



ENDPOINT PROTECTOR

사용 설명서 버전 5.4.0.0

사용자 매뉴얼



목 차

1. 소개	1
1.1. 주요 구성요소	2
2. 서버 기능	4
2.1. Endpoint Protector 설정 마법사	5
2.2. 통합 대시보드	6
2.3. 시스템 상태	7
2.4. Live Update	8
2.5. 유효 권한	9
3. 매체 제어	10
3.1. 대시보드	10
3.2. 장치	11
3.2.1. 장치 권한	13
3.2.2. 장치 기록	15
3.3. 컴퓨터	15
3.3.1. 컴퓨터 권한	17
3.3.2. 컴퓨터 설정	18
3.3.3. 컴퓨터 기록	19
3.3.4. 터미널 서버 및 씬 클라이언트	19
3.4. 사용자	23
3.4.1. 사용자 권한	24
3.4.2. 사용자 설정	26
3.4.3. 사용자 기록	26
3.5. 그룹	27
3.5.1. 그룹 유형	28

3.5.2. 그룹 권한	3 3
3.5.3. 그룹 설정	3 4
3.6. 전체	3 5
3.6.1. 전체 권한	3 5
3.6.2. 전체 설정	4 1
3.7. 파일 허용목록	5 8
3.8. 사용자 클래스	5 9
3.9. 장치 권한 우선순위	6 1
3.9.1. 매체 제어 정책 우선순위	6 2

4. 콘텐츠 인식 보호 6 4

4.1. 콘텐츠 인식 보호 활성화	6 5
4.2. 대시보드	6 6
4.3. 콘텐츠 인식 정책	6 6
4.3.1. 콘텐츠 인식 정책 만들기	6 7
4.3.2. 미리 설정된 정책	7 5
4.3.3. 차단 및 조치 정책	7 5
4.3.4. 다중 콘텐츠 인식 정책 적용	7 7
4.3.4. HIPAA 준수	7 9
4.4. 심층 패킷 검사(DPI)	8 2
4.4.1. 심층 패킷 검사(DPI) 포트 및 설정	8 5
4.4.2. 심층 패킷 검사(DPI) 응용프로그램	8 7

5. eDiscovery 8 8

5.1. eDiscovery 활성화	8 8
5.2. 대시보드	8 9
5.3. eDiscovery 정책 및 검색	9 0
5.3.1. eDiscovery 정책 및 검색 만들기	9 2

5.4. eDiscovery 검색 결과 및 액션.....	9 5
5.4.1. 검색 결과 보기 및 조치 하기.....	9 6
6. 거부목록 및 허용목록	9 7
6.1. 파일 유형 거부목록	9 8
6.2. 개인정보 거부목록.....	9 9
6.3. 사용자 키워드 거부목록	1 0 0
6.4. 파일 이름 거부목록	1 0 1
6.5. 파일 위치 거부목록	1 0 3
6.6. 검색위치 거부목록.....	1 0 4
6.7. 정규식 거부목록	1 0 5
6.8. 도메인 및 URL 거부목록	1 0 7
6.9. MIME 유형 허용목록	1 0 8
6.10. 허용된 파일 허용목록	1 1 0
6.11. 파일 위치 허용목록.....	1 1 1
6.12. 네트워크 공유 허용목록.....	1 1 2
6.13. 이메일 도메인 허용목록	1 1 4
6.14. URL 주소 허용목록	1 1 5
6.15. 심층 패킷 검사 허용목록	1 1 6
6.16. URL 범주	1 1 8
7. 암호화 정책	1 2 0
7.1. EasyLock	1 2 0
7.1.1. EasyLock 배포	1 2 1
7.1.2. EasyLock 설정	1 2 2
7.1.3. EasyLock 클라이언트.....	1 2 4
8. 오프라인 임시 암호	1 2 6

8.1. 오프라인 임시 암호 만들기	1 2 8
---------------------------	-------

9. 보고 및 분석 1 3 1

9.1. 로그 보고서	1 3 2
9.2. 파일 추적	1 3 3
9.3. 파일 사본보관	1 3 4
9.4. 콘텐츠 인식 보고	1 3 4
9.5. 콘텐츠 인식 파일 사본 보관	1 3 5
9.6. 관리자 작업	1 3 6
9.7. 온라인 컴퓨터	1 3 6
9.8. 온라인 사용자	1 3 7
9.9. 온라인 장치	1 3 7
9.10. 통계	1 3 8

10. 경고 1 3 9

10.1. 시스템 경고	1 4 1
10.1.1. 시스템 경고 만들기	1 4 1
10.1.2. 시스템 경고 기록	1 4 3
10.2. 매체 제어 경고	1 4 3
10.2.1. 매체 제어 경고 만들기	1 4 4
10.2.2. 매체 제어 경고 기록	1 4 5
10.3. 콘텐츠 인식 경고 정의	1 4 5
10.3.1. 콘텐츠 인식 경고 만들기	1 4 6
10.3.2. 콘텐츠 인식 경고 기록	1 4 7
10.4. EasyLock 경고	1 4 7
10.4.1 EasyLock 경고 만들기	1 4 8
10.4.2 EasyLock 경고 기록	1 4 9

11. 디렉터리 서비스 1 5 0

11.1. Microsoft Active Directory	1 5 1
11.2. Azure Active Directory	1 5 3
12. 장비	1 6 9
12.1. 서버 정보	1 6 9
12.2. 서버 유지보수	1 6 9
12.2.1. 시간대 설정	1 7 0
12.2.2. 네트워크 설정	1 7 1
12.2.3. 공장 초기화 어플라이언스 재설정	1 7 1
12.2.4. SSH 서버	1 7 1
12.3. SIEM 연결	1 7 1
13. 시스템 유지 관리.....	1 7 4
13.1. 파일 유지 관리	1 7 4
13.2. 객체 내보내기	1 7 5
13.3. 시스템 스냅숏	1 7 6
13.4. 감사 로그 백업	1 7 8
13.4.1. 감사 로그 백업 스케줄러	1 7 9
13.5. 외부 저장장치	1 8 0
14.5.1. FTP 서버	1 8 0
13.5.2. SFTP 서버	1 8 1
13.5.3. Samba / 네트워크 공유	1 8 2
13.6. 시스템 백업	1 8 3
13.6.1. 시스템 백업 (웹 인터페이스)	1 8 3
13.6.2. 시스템 백업 (콘솔)	1 8 6
13.7. 시스템 백업 v2	1 8 7
13.7.1. 시스템 백업 v2 만들기 (마이그레이션)	1 8 9
13.7.2. 가져오기 및 복원 (마이그레이션)	1 8 9

13.8. 사본 보관 저장소	190
-----------------------	-----

14. 시스템 구성 192

14.1. 클라이언트 소프트웨어	192
14.2. 클라이언트 업그레이드	193
14.3. 클라이언트 삭제	193
14.4. 시스템 관리자	194
14.5. 관리자 그룹	197
14.6. 시스템 구분	199
14.7. 시스템 보안	201
14.8. 시스템 설정	202
14.8.1. 권한 기능	202
14.8.2. 로그 설정	203
14.8.3. 심층 패킷 검사 (DPI) 인증서	203
14.8.4. Active Directory 인증	203
14.8.5. 프록시 서버 설정	205
14.9. 시스템 라이선스	205
14.9.1. 무료 평가 라이선스	206
14.9.2. 라이선스 가져오기 및 관리	207
14.10. SSO (Single Sign On)	208

15. 시스템 매개 변수 222

15.1. 장치 유형 및 알림	222
15.1.1. Trusted Devices	224
15.2. 문맥 감지	227
15.2.1. XML 만들기	227
15.2.2. XML 업로드	229
15.3. 고급 스캐닝 예외	232

15.4. 권한	2 3 3
15.5. 이벤트	2 3 3
15.6. 사용자 조치	2 3 4

16. Endpoint Protector 클라이언트 2 3 8

16.1. 클라이언트 설치.....	2 3 9
16.1.1. DPI 및 VPN 트래픽 가로채기 사용을 위한 macOS Endpoint Protector 클라이언트 설치	2 4 0
16.1.2. Debian 기반 배포	2 4 6
16.1.3. RedHat 기반 배포	2 4 9

17. 지원 2 5 2

18. 중요 공지 사항 / 책임의 한계 2 5 3

1. 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 맴출 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 보존된 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.

정보

Endpoint Protector는 완전한 자료유출방지 (Data Loss Prevention) 솔루션을 제공합니다. DLP 기능은 아래에 기술했습니다. Endpoint Protector 서버 배포 정보는 <https://cososys.kr> 을 참조 하시기 바랍니다.

1.1. 주요 구성요소

Endpoint Protector는 여러 물리적 객체로 설계되었습니다.

- 컴퓨터

Endpoint Protector 클라이언트가 설치된 Windows, Mac 및 Linux 워크스테이션

- 장치

현재 Endpoint Protector가 지원하는 장치

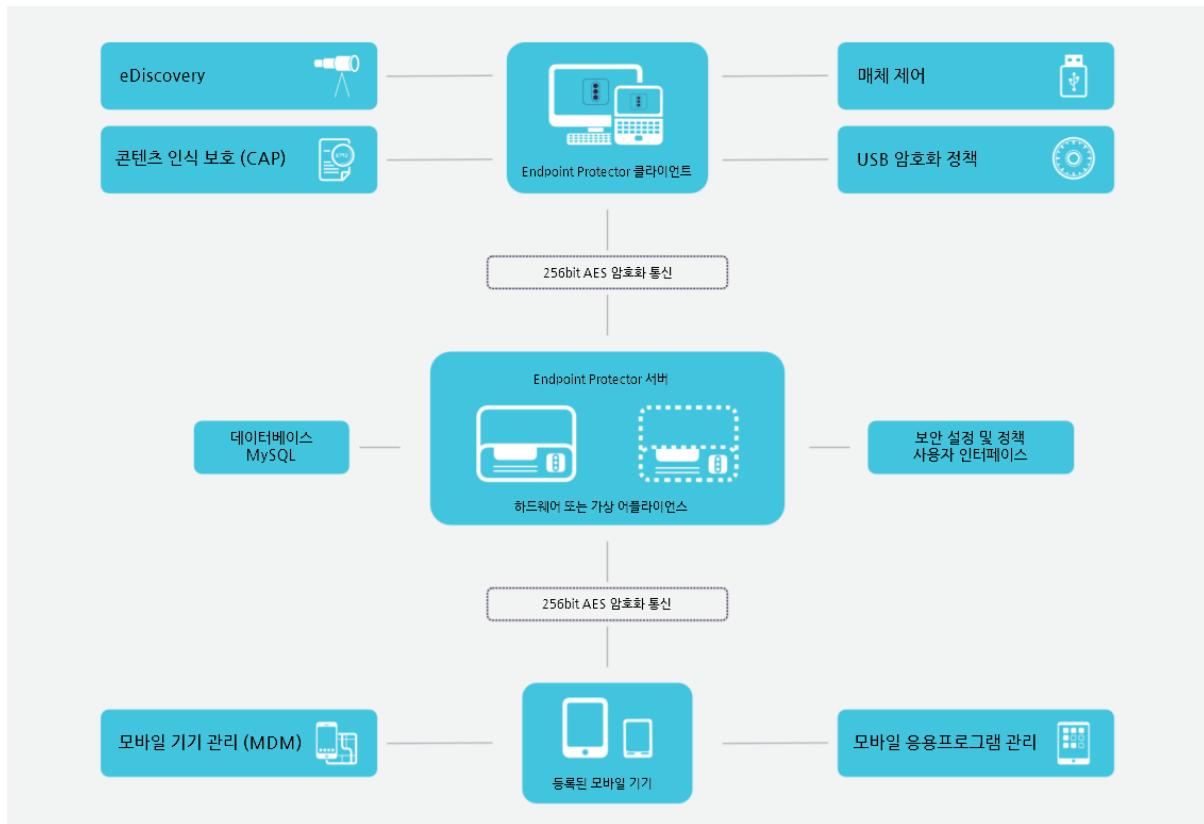
예: USB 장치, PTP 장치, USB 메모리 카드 등

- 사용자

장치와 컴퓨터를 다룰 사용자

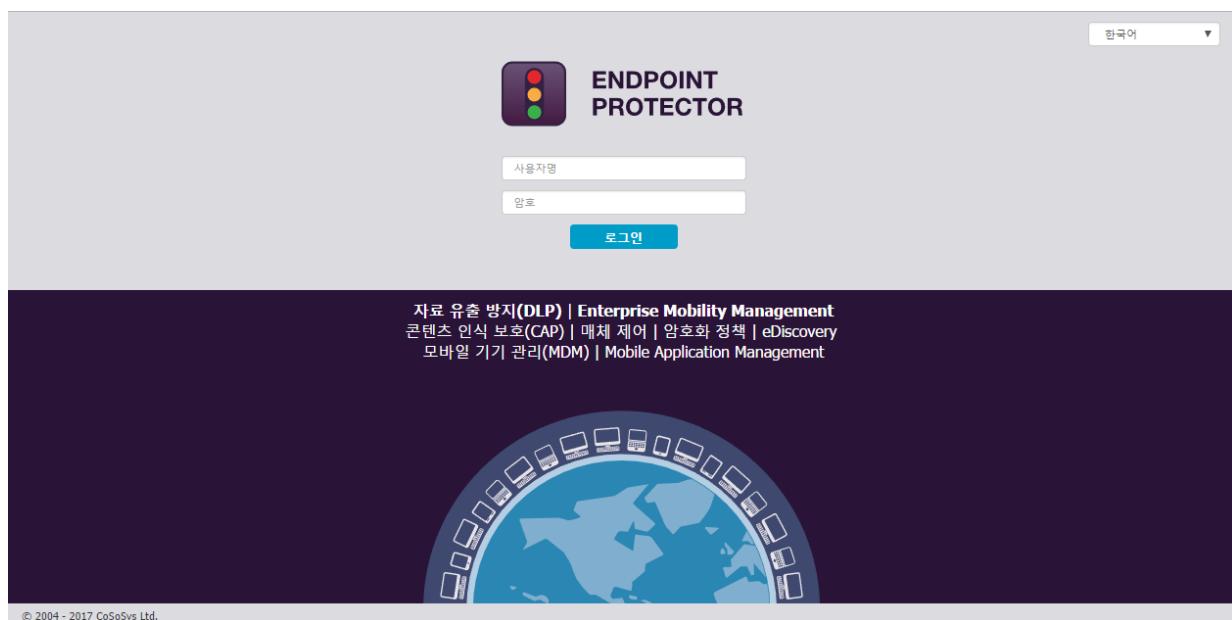
Endpoint Protector의 서버는 밀접하게 같이 동작하는 다른 부분이 있습니다.

- 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



2. 서버 기능

Endpoint Protector 하드웨어 또는 가상 어플라이언스 설정을 마치면 지정된 IP 주소를 입력하여 사용자 인터페이스에 접근할 수 있습니다. Endpoint Protector 기본 IP 주소는 <https://192.168.0.201>입니다.



정보

Endpoint Protector 기본 로그인 계정:

- 사용자명: root
- 암호: epp2011

이 설정을 변경 또는 관리자를 추가하려면 '14.4 시스템 관리자' 섹션을 참조 바랍니다.

참고

IP 주소 입력 시 HTTPS (Hypertext Transfer Protocol Secure)를 반드시 사용해야 합니다.

2.1. Endpoint Protector 설정 마법사

설정 마법사는 관리자가 일부 기본 설정을 정의하기 위한 단순한 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.

정보

설정 마법사는 Endpoint Protector의 기본 설정이 없는 경우에만 표시가 됩니다.

 ENDPOINT
PROTECTOR





« Endpoint Protector Appliance Configuration

1
2
3
4
5
6

[Next](#)

Welcome to Endpoint Protector Appliance Configuration!

Please finalize the configuration by defining the essential settings and default device control policies (Global Settings and Global Rights)

Time Zone

Please select your timezone
Europe 
Bucharest 

[Next](#)
[skip this step now - remind me later](#)

2.2. 통합 대시보드

이 섹션은 Endpoint Protector의 가장 중요한 활동 로그를 한 눈에 볼 수 있도록 시각화와 차트를 제공합니다. 라이선스 또는 최신 뉴스에 대한 일반 시스템 정보도 여기서 확인 할 수 있습니다. 매체 제어, 콘텐츠 인식 보호, 모바일 기기 관리에 대한 추가 정보가 표시 됩니다.

정보

매체 제어, 콘텐츠 인식 보호, eDiscovery에서 더 상세한 대시보드를 사용할 수 있습니다.

2.3. 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 하위 섹션에서 Endpoint Protector의 매체 제어, 콘텐츠 인식 보호, eDiscovery 모듈을 ON / OFF 할 수 있습니다.

시스템 상태 하위 섹션에서 HDD 디스크 공간과 로그 회전을 ON / OFF 할 수 있습니다.

정보

이 설정이 ON으로 되어 있으면 서버 디스크 공간이 설정된 특정 퍼센트에 다다르면 오래된 로그는 자동으로 새로운 로그로 덮어쓰기가 됩니다.

퍼센트 설정은 50%, 60%, 70%, 80%, 90%로 설정이 가능합니다.

시스템 경고 하위 섹션에서 중요 경고는 APNS, 업데이트, 지원 또는 비밀번호 만료를 알 수 있도록 ON / OFF 설정이 가능합니다.

시스템 백업 하위 섹션에서 시스템 백업은 ON / OFF로 설정할 수 있습니다.

2.4. Live Update

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

참고

이 기능은 80번 포트를 통해서 통신합니다.

Live Update 구성은 업데이트를 수행하는 두 가지 옵션 중 하나인 자동으로 업데이트 확인 및 수동으로 업데이트 확인을 선택할 수 있습니다. 그리고 Live Update 서버에 현재 시스템 상태 보고를 사용 또는 사용 중지할 수 있습니다.



'지금 확인' 버튼을 누르면 Endpoint Protector 서버 업데이트 검색을 시작합니다.

새로운 업데이트가 발견되면 사용 가능한 업데이트 섹션 아래에 표시가 되고 'Apply all update' 버튼을 눌러서 바로 설치할 수 있습니다. '적용된 업데이트 보기' 버튼을 눌러서 설치된 최신 업데이트를 확인할 수 있습니다.

오프라인 패치 업로드로 인터넷 통신을 사용할 수 없는 경우에도 업데이트를 할 수 있습니다.

참고

오프라인 패치 요청은 support@cososys.co.kr로 연락 주시기 바랍니다.

2.5. 유효 권한

이 섹션은 현재 적용된 매체 제어 또는 콘텐츠 인식 보호 정책을 보여 줍니다. 드롭 다운 메뉴를 이용하여 권한, 사용자 컴퓨터, 장치 유형, 특정 장치, 보고서 유형 (PDF 또는 XLS), 근무 외 시간 및 외부 네트워크 등의 정보를 표시할 수 있습니다.

The screenshot shows the 'Effective Rights Criteria' section where various parameters like media type, rights, device type, device, user, and location are selected. Below this is the 'Effective Rights List' table, which displays five entries of generated rights, each with columns for session, computer, user, device type, device, right, policy, duration, status, and action. The table includes filters (10, 항목), export options (Excel, PDF, CSV), and a download button.

섹션	컴퓨터	사용자	장치 유형	장치	권한	정책	만든 시간	상태	작업
매체 제어	전부	support	Bluetooth Radio	전부	Deny Access	N/A	2017-06-19 13:24:52	Generating report	
매체 제어	admin's MacBook Pro	전부	전부	전부	Read Only Access	N/A	2017-06-01 09:58:11	Ready to download	
매체 제어	전부	전부	전부	전부	Read Only Access	N/A	2017-06-01 09:57:59	Ready to download	
매체 제어	전부	전부	전부	전부	Read Only Access	N/A	2017-05-26 16:42:20	Ready to download	
매체 제어	전부	전부	전부	전부	Allow Access	N/A	2017-05-26 16:42:07	Ready to download	

한 번 생성되면 보고서는 다운로드 준비가 되어 원하는 곳에 사용할 수 있습니다.

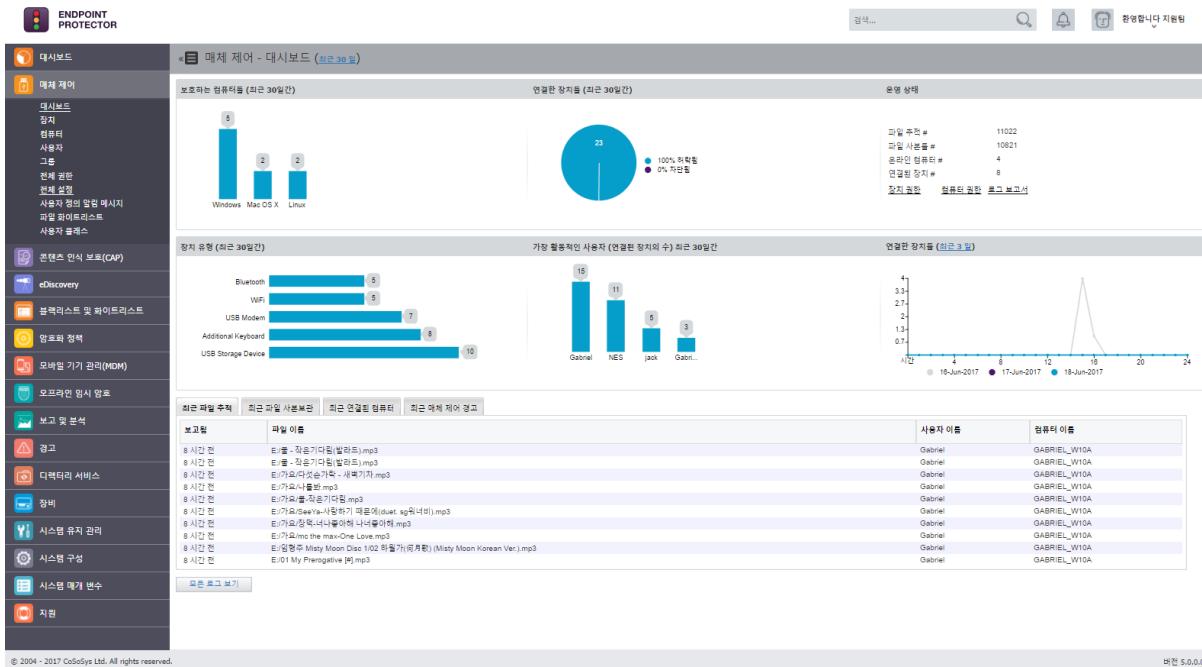
3. 매체 제어

이 섹션에서 관리자는 시스템의 모든 객체, 하위 권한 및 설정을 관리할 수 있습니다. 하위 섹션은 대시보드, 장치, 컴퓨터, 사용자, 그룹, 전체 권한, 전체 설정, 사용자 정의 알림 메시지, 파일 허용목록, 사용자 클래스가 있습니다.

일부 추가적인 세팅이 포함되면서 이 섹션은 매체 제어 모듈이라고 생각하시면 될 것입니다. Endpoint Protector의 첫 번째 보안 계층으로 모든 설정이 기본으로 활성화되어 제공됩니다.

3.1. 대시보드

이 섹션은 Endpoint Protector 객체를 한 눈에 볼 수 있도록 그래픽과 차트 형태로 제공합니다. 최근 파일 추적, 최근 파일 사본 보관, 최근 연결된 컴퓨터, 최근 매체 제어 경고의 추가 정보를 확인 할 수 있습니다.



3.2. 장치

이 섹션에서 관리자는 시스템의 모든 장치를 관리할 수 있습니다. 보호되는 컴퓨터에 연결된 새로운 장치가 자동으로 데이터베이스에 추가되어서 관리가 가능합니다.

The screenshot shows the device management interface with the following details:

장치 이름	장치 유형	설명	VID	PID	일련 번호	장치 코드	구분	최종 사용자	마지막 접속일	마지막 확인일	작업
Bluetooth Host Controller	Bluetooth	Bluetooth Host Controller/Apple, Inc.	5ac	8286		-	Default Department	GABRIEL_W10A	2021-03-05 17:35:56	i	
FaceTime HD Camera (Built-in)	Webcam	FaceTime HD Camera (Built-in)/Apple, Inc.	5ac	8510	0000	-	Default Department	GABRIEL_W10A	2021-03-05 17:35:56	i	
HID Keyboard Device	Additional Keyboard	HID Keyboard Device/(Standard keyboards)	45e	773	HID-VID_045E&PID_0773&REV_0674&MI_00/HID-VID_045E&PID_0773&MI_00/HID-VID_045E&UP_0001_U0006/HID_DEVICE_SYSTEM_KEYBOARD/HID_DEVICE_UP_0001_U0006/HID_DEVICE/	-	Default Department	GABRIEL_W10A	2021-03-05 17:35:56	i	
HID Keyboard Device	Additional Keyboard	HID Keyboard Device/(Standard keyboards)	5ac	262	HID-VID_05AC&PID_0262&REV_0222&MI_00&Co01/HID-VID_05AC&PID_0262&MI_00&Co01/HID-VID_05AC&UP_0001_U0006/HID_DEVICE_SYSTEM_KEYBOARD/HID_DEVICE_UP_0001_U0006/HID_DEVICE/	-	Default Department	GABRIEL_W10A	2021-03-05 17:35:56	i	
SDA Standard Compliant SD Host Controller	Internal Card Reader	SDA Standard Compliant SD Host Controller/SDA Standard Compliant SD Host Controller Vendor	14e4	16bc	96BC14E4_10_4_1A0B740B_0_01E0	-	Default Department	GABRIEL_W10A	2021-03-05 17:35:56	i	

장치는 장치 매개 변수 (Vendor ID, Product ID, Serial Number)로 확인하지만 장치 이름과 설명과 같은 정보 역시 사용할 수 있습니다. 장치는 처음 사용자의 기본값으로

할당되지만 차후에 변경할 수 있습니다.

관리자는 위에서 언급한 장치 매개 변수와 정보를 이용해서 언제든지 수동으로 새로운 장치를 만들 수 있습니다. 장치는 또한 Active Directory에서 Endpoint Protector로 가져올 수 있습니다.

정보

Active Directory 상세 정보는 '11 디렉토리 서비스' 섹션을 참조하시기 바랍니다.

'작업' 열을 보면 수정, 권한 관리, 장치 기록 보기, 장치 기록 내보내기, 삭제 옵션이 있습니다.

정보

장치의 '상태' 열은 아래와 같은 의미를 가지고 있습니다.

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

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

정보

장치 유형의 상세 정보는 '3.6.1.1 장치 유형' 을 참조하시기 바랍니다.

참고

장치 권한이 모든 객체에 세밀하게 설정이 되었다면 우선 순위는 아래와 같습니다. 가장 높은 우선 순위로 시작합니다.

장치 > 컴퓨터 | 사용자 > 그룹 > 전체

예제

전체 권한이 특정 장치에 컴퓨터가 접근하지 못하도록 설정되어 있고 한 컴퓨터는 이 장치 접근 허용이 되었다면 이 컴퓨터는 장치를 사용할 수 있습니다.

정보

장치 가져오기 / 내보내기 옵션은 JSON 포맷으로 또한 사용 할 수 있습니다. 이는 하나의 Endpoint Protector 서버에서 장치 목록을 내보내고 다른 Endpoint Protector 서버에서 이 목록을 가져와서 사용할 수 있습니다.

이 기능은 장치 권한과 그룹에 연관성을 가져가는 것에 있습니다. 그래서 두 서버에 같은 그룹이 있다면 가져온 장치 또한 같은 접근 권한을 유지할 것입니다. 그룹이 존재하지 않으면 장치 목록은 가져오지만 접근 권한은 무시됩니다.

3.2.1. 장치 권한

장치 권한은 특정 장치의 작업 열에서 권한 관리 선택해서 접근할 수 있습니다. 이 섹션에서 관리자는 특정 컴퓨터, 그룹 또는 사용자가 사용 또는 사용할 수 없음으로 설정할 수 있습니다.

The screenshot shows the Endpoint Protector interface. On the left, there's a sidebar with various icons and sections like '대시보드', '매체 제어', '장치', '컴퓨터', etc. The main area is titled 'Device Control - Device Rights - Apple Broadcom Built-in Bluetooth'. It has a search bar at the top right and a toolbar with Excel, PDF, CSV, and other export options. Below that is a table header with columns for Entity Type, Entity Name, 고친 시간 (Last Accessed), 고친 사람 (Last Accessed By), 권한 (Permissions), and 작업 (Actions). A note says '일치하는 레코드 찾지 못함' (No matching records found). At the bottom of the table area is a '다음' (Next) button.

장치를 선택한 후에 원하는 사용자, 컴퓨터 또는 그룹에 특정 권한을 2 가지 단계의 마법사를 사용하여 바로 할당할 수 있습니다.

- 객체와 장치 권한 선택

This is a screenshot of the 'Device Control' section under 'Device Rights'. It shows a table with columns for Entity (선택한 장치), 고친 시간 (Last Accessed), 고친 사람 (Last Accessed By), 권한 (Permissions), and 작업 (Actions). The table is currently empty with the message '선택된 항목이 없습니다' (No selected items).

- 객체 선택 (컴퓨터, 그룹 또는 사용자)

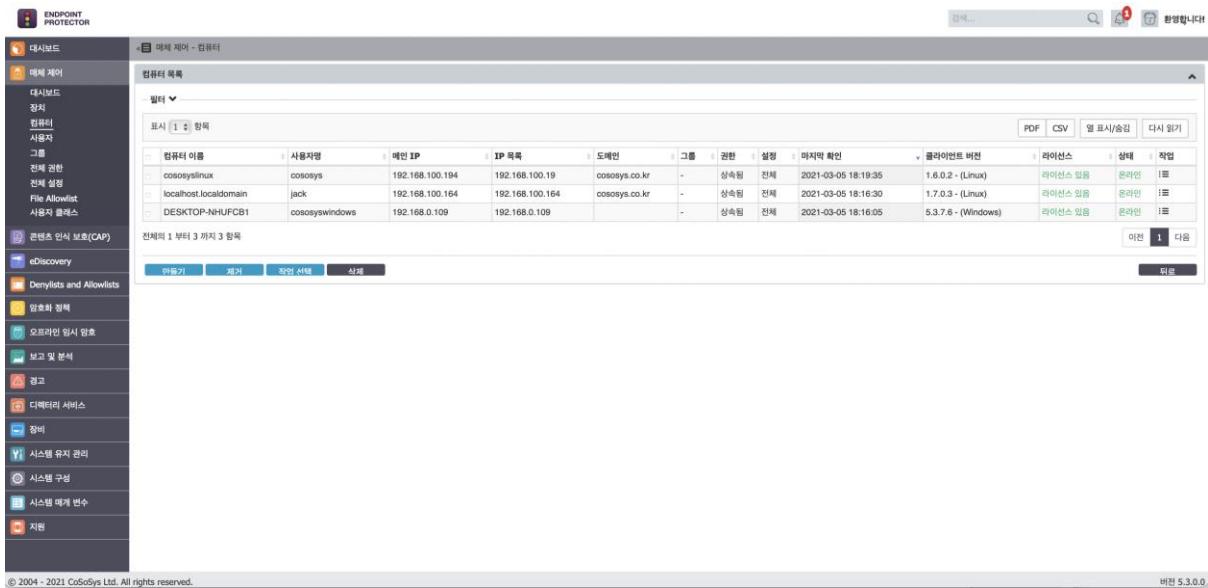
This is a screenshot of the 'Device Control' section under 'Device Rights'. It shows a table with columns for Computer Name, IP Address, MAC Address, and Group. The table lists three devices: 'PC-000000000000', 'PC-000000000001', and 'PC-000000000002'. At the bottom, there are buttons for '이전' (Previous) and '다음' (Next).

3.2.2. 장치 기록

컴퓨터 및 사용자 기록과 비슷하게 서버에 한 번이라도 연결된 장치는 여기서 찾을 수 있습니다. 로그는 “내보내기” 버튼을 누르면 .csv 파일로 저장됩니다. 반면에 “장치 보기”는 개별 장치의 로그 리포트 페이지로 필터링 됩니다.

3.3. 컴퓨터

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



Endpoint Protector 클라이언트는 자체 등록 메커니즘을 가지고 있습니다. 이 프로세스는 클라이언트 소프트웨어가 클라이언트 컴퓨터에 설치된 후에 한 번 작동됩니다. 서버는 데이터베이스에서 컴퓨터 관련 정보를 저장하고 라이선스를 할당합니다.

참고

자체 등록 메커니즘은 컴퓨터 라이선스 모듈이 변경 될 때 마다 동작합니다. 그 때마다 응용 프로그램 클라이언트는 재설치 됩니다. 컴퓨터 소유자는 자체 등록에 저장되지 않습니다.

정보

라이선스에 대한 상세 정보는 '14.9 시스템 라이선스'를 참조 바랍니다.

컴퓨터는 컴퓨터 매개 변수 (메인 IP, IP 목록, MAC, 도메인 또는 워크그룹)으로 확인되지만 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 수도 있습니다.

관리자는 위에서 언급한 컴퓨터 매개 변수와 정보를 이용해서 수동으로 새로운 컴퓨터를 만들 수 있습니다. 컴퓨터는 또한 Active Directory에서 Endpoint Protector로 가져올 수 있습니다.

정보

Active Directory에 대한 상세 정보는 '11 디렉토리 서비스'를 참조 바랍니다.

팁

효율적인 조직화를 위해서 컴퓨터는 아래와 같이 할당:

- 그룹 (예: 같은 사무실의 여러 컴퓨터)

그룹의 상세 정보는 '3.5 그룹'을 참조하시기 바랍니다.

- 구분 (그룹의 대안 조직)

구분의 상세 정보는 '14.6 시스템 구분'을 참조하시기 바랍니다.

3.3.1. 컴퓨터 권한

컴퓨터 권한은 특정 컴퓨터의 작업 열에서 권한 관리를 선택하면 이용할 수 있습니다. 이 섹션은 관리자가 특정 장치 유형에 권한을 부여할 수 있습니다.

장치 유형	제어 수준	장치 유형	제어 수준	장치 유형	제어 수준
미확인 저장장치	사용 허용	SATA 컨트롤러(eSATA)	사용 허용	사용 허용	사용 허용
USB 저장장치	사용 허용	WiFi	사용 허용	사용 허용	사용 허용
내장 CD/DVD/BR 드라이브	사용 허용	Bluetooth	사용 허용	사용 허용	사용 허용
내장 카드 리더	사용 허용	FireWire(1394) 저장장치	사용 허용	사용 허용	사용 허용
내장 플로피 드라이브	사용 허용	시리얼 포트	사용 허용	사용 허용	사용 허용
네트워크 프린터	사용 허용	PCMCIA 장치	사용 허용	사용 허용	사용 허용
로컬 프린터	사용 허용	MTD 밍식 카드 리더	사용 허용	사용 허용	사용 허용
Windows 스마트 기기 (MTP)	사용 허용	SCSI 밍식 카드 리더	사용 허용	사용 허용	사용 허용
디지털 카메라	사용 허용	ZIP 드라이브	사용 허용	사용 허용	사용 허용
블랙박스	사용 허용	ADB 및 Teensy Board	사용 허용	사용 허용	사용 허용
휴대폰 (Sony Ericsson, etc.)	사용 허용	Thunderbolt	사용 허용	사용 허용	사용 허용
스마트폰 (USB 동기화)	사용 허용	네트워크 공유	사용 허용	사용 허용	사용 허용
스마트폰 (Windows CE)	사용 허용	적외선 통신	사용 허용	사용 허용	사용 허용
노키아폰 (Symbian)	사용 허용	병렬 포트 (LPT)	사용 허용	사용 허용	사용 허용
웹캠 (Webcam)	사용 허용	썬 플레이언트 저장소 (RDP 저장소)	사용 허용	사용 허용	사용 허용
iPhone	사용 허용	추가 키보드 (혹 BadUSB)	사용 허용	사용 허용	사용 허용
iPad	사용 허용	USB 모뎀	사용 허용	사용 허용	사용 허용

팁

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 관리자는 여기에서 업무 시간 및 외부 네트워크 정책을 만들 수 있습니다.

정보

매체 유형 및 특정 장치 (표준, 외부 네트워크, 업무 시간)의 상세 정보는 '3.6.1 전체 권한' 을 참조 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.

3.3.2. 컴퓨터 설정

이 섹션은 관리자가 각 컴퓨터의 설정을 편집할 수 있습니다.

The screenshot shows the 'Computer Control' section of the Endpoint Protector software. On the left, there's a sidebar with icons for Dashboard, Computer Control (selected), Denylists and Allowlists, Encryption, Offline Temporary Encryption, Reporting and Analysis, and Audit. The main panel title is 'Computer Control - General Settings'. It contains several configuration fields:

- Cloud Client Mode: Set to 'Normal Mode'.
- User Language: Set to 'English'.
- Log File Size (bytes): 300, 30, 60, 3.
- Log File Size (MB): 512, 512, 0, 512, 5000.
- Log File Size (KB): 512, 512, 0, 512, 5000.
- Log File Size (bytes): 300, 30, 60, 3.
- Log File Size (MB): 512, 512, 0, 512, 5000.
- Log File Size (KB): 512, 512, 0, 512, 5000.
- User Message Setting: Enabled.
- OTP Usage: Enabled.
- Screen Rotation Detection (DPI): Enabled.
- Bluetooth File Transfer: Enabled.

At the bottom, it says '© 2004 - 2021 CoSoSys Ltd. All rights reserved.' and 'Version 5.3.0.0'.

모든 컴퓨터를 사용자 정의 설정하는 것은 불필요합니다. 컴퓨터는 수정 설정 정의가 없어도 완벽하고 정확하게 기능을 수행하기 때문입니다. 그룹이 가지고 있는 설정을 받아 오거나 아니면 시스템에 기본값으로 되어 있는 전체 설정을 받아 올 수 있습니다. 전체 설정 역시 추후에 변경이 가능합니다.

3.3.3. 컴퓨터 기록

이 모듈은 서버에 한 번이라도 연결된 모든 컴퓨터를 보여줍니다. '내보내기' 버튼을 누르면 .csv 파일로 저장하고 반면에 '컴퓨터 기록 보기'는 각 컴퓨터로 필터링 된 로그 보고서를 보여줍니다.

이벤트	컴퓨터	메인 IP	사용자명	장치 유형	장치	날짜/시간 (서버)	날짜/시간 (클라이언트)	작업
정책 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-08 10:52:25	2021-03-08 10:52:25	-
정책 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-08 10:37:24	2021-03-08 10:37:24	-
정책 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-08 10:07:24	2021-03-08 10:07:24	-
정책 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-05 17:26:30	2021-03-05 17:26:30	-
정책 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-05 11:01:39	2021-03-05 11:01:39	-
정책 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-05 10:54:51	2021-03-05 10:54:51	-
사용자 로그인	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-05 10:49:57	2021-03-04 20:47:18	-
정책 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-05 10:49:36	2021-03-05 10:49:36	-

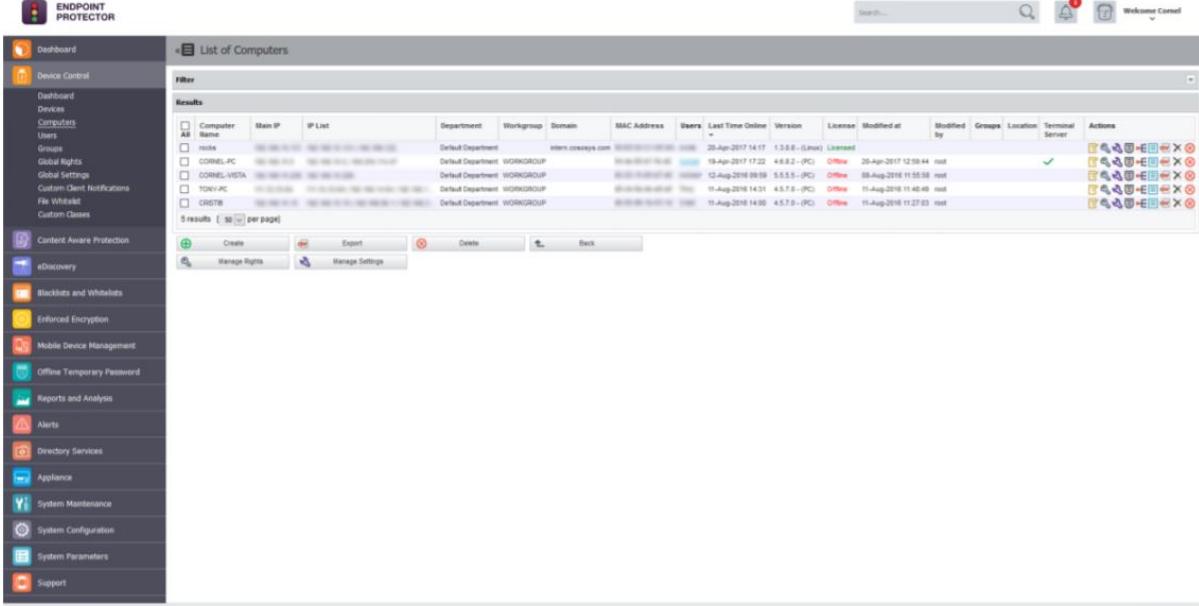
3.3.4. 터미널 서버 및 씬 클라이언트

씬 클라이언트와 Windows 터미널 서버 사이의 RDP 스토리지에 파일 전송을 제어가 Endpoint Protector를 통해서 가능합니다.

3.3.4.1. 초기 설정

프로세스는 매체 제어 > 컴퓨터에서 '터미널 서버로 지정'  으로 시작됩니다

성공적으로 시스템에서 원하는 컴퓨터를 지정하면 아래 이미지와 같이 쉽게 구별할 수 있도록  마크가 표시됩니다.



Computer Name	Main IP	IP List	Department	Workgroup	Domain	MAC Address	Users	Last Time Online	Version	License	Modified at	Modified by	Groups	Location	Terminal Server	Actions
CORNEL-PC	192.168.1.100		Default Department	WORKGROUP	intern.corneys.local	00:0C:29:4D:0A:00	1	18-Aug-2017 11:17	1.0.0.0 - (None)	Unlimited	20-Aug-2017 12:19:44	out				        
CORNEL-VISTA	192.168.1.101		Default Department	WORKGROUP	intern.corneys.local	00:0C:29:4D:0B:00	1	12-Aug-2016 09:59	4.5.5.5 - (PC)	Online	08-Aug-2016 11:55:55	out				        
TONY-PC	192.168.1.102		Default Department	WORKGROUP	intern.corneys.local	00:0C:29:4D:0C:00	1	11-Aug-2016 14:31	4.5.7.8 - (PC)	Online	11-Aug-2016 11:45:40	out				        
GHSTB	192.168.1.103		Default Department	WORKGROUP	intern.corneys.local	00:0C:29:4D:0D:00	1	15-Aug-2016 14:00	4.5.7.9 - (PC)	Online	11-Aug-2016 11:27:03	out				        

참고

이 액션으로 선택할 수 있는 컴퓨터는 엄격하게 터미널 서버 역할을 수행하는 Windows 서버입니다.

정보

터미널 서버로 이 액션 마크가 수행되려면 적어도 하나의 터미널 서버 라이선스가 있어야 합니다.

터미널 서버로 성공적으로 설정되었으면 '매체 제어 > 컴퓨터 > 컴퓨터 권한'에서 편집할 때 새로운 장치 유형이 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 권한 사용 옵션은 '시스템 구성 > 시스템 설정 > Endpoint Protector 권한 기능 사용'의 설정에서 사용자 권한 우선순위로 사용자 로그인 적용이 되어 있어야 합니다.

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

장치 유형	설정
Thin Client Storage (RDP Storage)	<input checked="" type="checkbox"/> 허용
내장 CD/DVD/BR 드라이브	<input type="checkbox"/> 허용
내장 카드 리더	<input type="checkbox"/> 허용
내장 플로피 드라이브	<input type="checkbox"/> 허용
로컬 프린터	<input type="checkbox"/> 허용
마이크로 저장장치	<input type="checkbox"/> 허용
USB 저장장치	<input type="checkbox"/> 허용
Windows 스마트 기기 (MTP)	<input type="checkbox"/> 허용
디지털 카메라	<input type="checkbox"/> 허용
블루투스	<input type="checkbox"/> 허용
휴대폰 (Sony Ericsson, etc.)	<input type="checkbox"/> 허용
오프라인 할인 암호	<input type="checkbox"/> 허용
스마트폰 (USB 충전기)	<input type="checkbox"/> 허용
스마트폰 (Windows CE)	<input type="checkbox"/> 허용
노트북 (Symbian)	<input type="checkbox"/> 허용
웹캠 (Webcam)	<input type="checkbox"/> 허용
iPhone	<input type="checkbox"/> 허용
iPad	<input type="checkbox"/> 허용
Pod	<input type="checkbox"/> 허용
SATA 인터페이스(eSATA)	<input type="checkbox"/> 허용
WiFi	<input type="checkbox"/> 허용
Bluetooth	<input type="checkbox"/> 허용
FireWire(1394) 저장장치	<input type="checkbox"/> 허용
시리얼 포트	<input type="checkbox"/> 허용
PONDA 장치	<input type="checkbox"/> 허용
MFD 등의 카드 리더	<input type="checkbox"/> 허용
SCSI 등의 카드 리더	<input type="checkbox"/> 허용
ZIP 드라이브	<input type="checkbox"/> 허용
ADB 및 Teeny Board	<input type="checkbox"/> 허용
Thunderbolt	<input type="checkbox"/> 허용
네트워크 드라이버	<input type="checkbox"/> 허용
PCI Express槽	<input type="checkbox"/> 허용
PCI Express槽	<input type="checkbox"/> 허용
Bluetooth (LPT)	<input type="checkbox"/> 허용
신 플레이어드 저장소 (RDP 저장소)	<input type="checkbox"/> 허용
주가 키보드 (혹은 BadUSB)	<input type="checkbox"/> 허용
USB 카메라	<input type="checkbox"/> 허용
USB 콘솔	<input type="checkbox"/> 허용
안드로이드 스마트폰 (Mac MTP)	<input type="checkbox"/> 허용
Chip Card Device	<input type="checkbox"/> 허용

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

2.2 | Endpoint Protector | 사용 설명서

□	192.168.0.149	Default Department	Administrator	00-25-90-d5-50-32	noUser	14-May-2015 18:21	4.4.2.9 - (PC)	Licensed	13-May-2015 17:43:06	root	ThinGroup ✓	☒ 🔍 🌐 🌐 🌐 🌐
□	192.168.0.19	Default Department		08-00-27-00-94-38		14-May-2015 17:28	4.4.2.4 - (PC)	Offline			☒ 🔍 🌐 🌐 🌐 🌐	
□	111.33.33.12	Default Department	WORKGROUP	00-19-86-d5-8d-0f		13-May-2015 16:49:45	4.4.2.9 - (PC)	Unlicensed	13-May-2015 16:49:26	root	✓	☒ 🔍 🌐 🌐 🌐 🌐

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

Endpoint Protector Client Version

ENDPOINT PROTECTOR by CoSoSys

Device Control Content Aware Protection Settings

Search

Device	VID	PID	Serial Number	Device Code
SanDisk / Ultra T C	781	5596	4C5300000...	D0D5
HP LaserJet Pro MFP M225-M226	0	0	ipp://192.16...	685E
Generic PostScript Printer	0	0	ipp://192.16...	74C8
Generic PostScript Printer	0	0	ipp://192.19...	7A9C
HP LaserJet 200 color MFP M276. Fax	0	0	hpfax://HPD...	3EC4
Apple / Wireless Network Adapter (802.11 a/b/g/n/ac)	14E4	43A3	88-e9-fe-79...	7077

To authorize a blocked device, please Request Access from your administrator.

Request Access

Last server connection: 2021-07-22 19:13:20

3.4. 사용자

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

장치 이름	장치 유형	설명	VID	PID	일련 번호	장치 코드	최종 사용자	마지막 컴퓨터	마지막 확인	작업
Apple iPhone	iPhone	Apple iPhone/Apple Inc.	5Ac	12a8	6DDAD3B9BDAC9A0BF89B57D2F1D2A00D38537A25	A6E9	cososyswindows	DESKTOP-NHUFBC1	2021-07-15 11:06:02	⋮
ASIX AX88772B USB2.0 to Fast Ethernet Adapter	USB Modem	ASIX AX88772B USB2.0 to Fast Ethernet Adapter/ASIX	b95	7e2b	04AA28	F11E	cososyswindows	DESKTOP-NHUFBC1	2021-09-01 09:35:03	⋮
Bluetooth Device	Bluetooth	Bluetooth Device/Broadcom	5Ac	98	AO-78-17-7A-06-99	-	cososysjack	JackJung@ MacBook Pro	2021-07-27 09:19:55	⋮
Bluetooth Device	Bluetooth	Bluetooth Device/Broadcom	8294	28-F0-76-44-5E-4B		F7D6	macadmin	cososy-iMac	2021-06-21 17:03:13	⋮
Bluetooth Device	Bluetooth	Bluetooth Device/Broadcom	5Ac	8289	AC-BC-32-EF-26-38	-	macminil	코리아의 Mac mini	2021-06-15 13:32:49	⋮
Bluetooth Device (Personal Area Network)	USB Modem	Bluetooth Device (Personal Area Network)/Microsoft	0	0	Net_9_1076F190_0_2	-	cososyswindows	DESKTOP-NHUFBC1	2021-09-01 09:35:03	⋮
Bluetooth Host		Bluetooth Host						DESKTOP-	2021-09- -	⋮

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

정보

Active Directory의 상세 정보는 '11 디렉터리 서비스'를 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.

정보

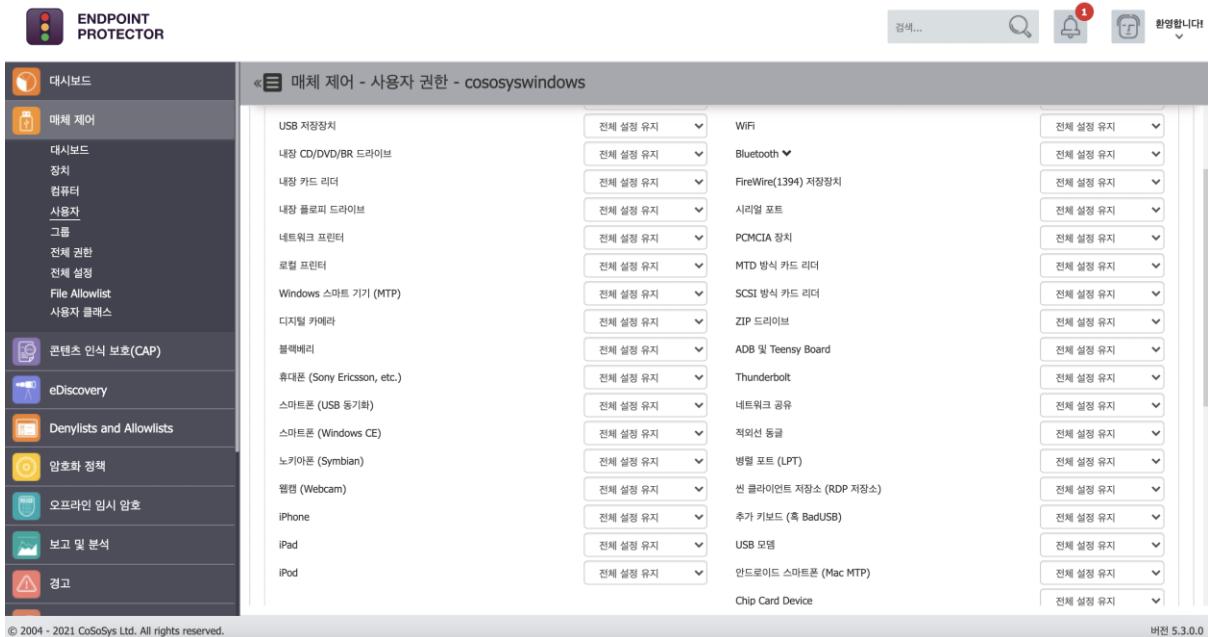
OS에 따라서 추가 시스템 사용자가 다음과 같이 나타날 수 있습니다:

- _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.

3.4.1. 사용자 권한

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



팁

표준 매체 제어 권한에는 '장치 유형'과 '이미 있는 장치'가 포함되어 있습니다. 일반적으로 사용되는 유일한 장치 권한입니다.

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

정보

장치 유형 및 특정 장치 (표준, 외부 네트워크, 업무 시간)에 대한 자세한 내용은 '3.6.1 전체 권한'을 참조하시기 바랍니다.

참고

전체 권한 복원 버튼은 권한을 전체 권한을 따르도록 만드는데 사용할 수 있습니다. 이 버튼은 전체 권한 뿐만 아니라 전체 설정도 따릅니다.

해당 수준에 설정된 이미 존재하는 장치는 복원 버튼을 누르면 삭제됩니다.

3.4.2. 사용자 설정

이 섹션에서 관리자는 각 사용자 설정을 편집할 수 있습니다.

대시보드

매체 제어

대시보드
장치
컴퓨터
사용자
그룹
전체 권한
전체 설정
파일 허용목록
사용자 클래스

콘텐츠 인식 보호(CAP)

eDiscovery

거부목록 및 허용목록

암호화 정책

오프라인 임시 암호

보고 및 분석

경고

데이터리 서비스

장비

Endpoint Protector 클라이언트

로그 간격(초): 300
로그 크기(MB): 512
사본보관 간격(분): 30
사본보관 크기(MB): 512
사본보관의 최소 파일(KB): 0
사본보관의 최대 파일(KB): 512
복구 폴더의 보존 기간(일): 3
복구 폴더 풀어 최대 크기 (MB): 5000
사용자 정보 입력: 자동
OTP 사용 이유 제출 필수: 자동
확장된 소스 코드 길지: 자동
사용자 정의 알림 메시지: 자동
광학 인식 문자: 자동
위험 암생코드에서 충단: 자동
심층 패킷 검사(DPI): Beta
보안 안 된 연결 차단: 자동
블루투스 파일 전송 충단: 자동

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.

3.4.3. 사용자 기록

이 섹션에서 관리자는 사용자 기록 활동 보기通过对 사용자 기록을 볼 수 있습니다. 각 사용자에 대한 로그 리포트를 보여줍니다.

The screenshot shows the 'Report and Analysis - Log Report' section. On the left, there's a sidebar with various navigation options like Dashboard, Device Management, Content Protection, eDiscovery, Asset Inventory, Encryption Policies, Offline Instant Recovery, and Reporting. The main area displays a table of log entries with columns for Event Type, Computer, External IP, Username, Device Type, Device, Log Date, Log Date (Client), and Action. There are filters at the top and buttons for Excel, PDF, CSV, and Print at the bottom right.

이벤트	컴퓨터	예인 IP	사용자명	장치 유형	장치	날짜/시간 (서버)	날짜/시간 (클라이언트)	작업
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 17:16:44	2021-09-01 17:16:44	-
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 15:41:23	2021-09-01 15:41:23	-
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 15:36:22	2021-09-01 15:36:22	-
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 10:10:11	2021-09-01 10:10:11	-
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 09:32:27	2021-09-01 09:32:27	-
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 09:27:26	2021-09-01 09:27:26	-
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 09:22:25	2021-09-01 09:22:25	-
사용자 로그인	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-09-01 09:17:32	2021-09-01 09:17:10	-
사용자 로그아웃	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-08-31 18:46:21	2021-08-31 18:46:10	-
정책 수령	DESKTOP-NHUFBCB1	10.37.13.35	cososyswindows	-	-	2021-08-31 18:23:41	2021-08-31 18:23:41	-

3.5. 그룹

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

The screenshot shows the 'Device Management - Groups' section. The sidebar includes options like Device Management, Locations, Computers, Users, Groups, Full Control, Full Settings, File Backup Log, and User Classes. The main area shows a table of groups with columns for Group Name, Description, Group Type, Location, and Priority. There are buttons for Create, Select, and Delete at the bottom right.

그룹 이름	그룹 설명	그룹 유형	도메인	우선 순위	작업
Group1 - TEST		각각	-	999	
Default Group - Computers	Default Group for Computers	기본값	-	2	

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.

정보

Active Directory의 상세 정보는 '11 디렉터리 서비스'를 참조하시기 바랍니다.

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

3.5.1. 그룹 유형

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

스마트 그룹

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

스마트 그룹은 '시스템 구성 > 시스템 설정 > 스마트 그룹'에서 사용할 수 있습니다.

Smart Groups

Enable Smart Groups:



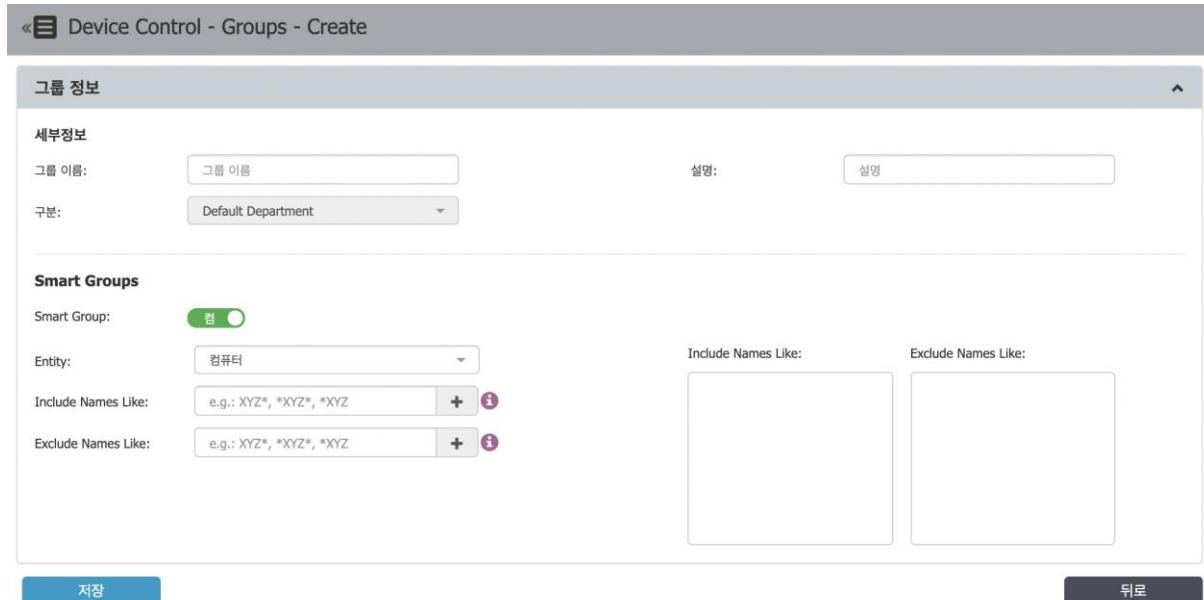
Enable Default Group for Computers:



Enable Default Group for Users:



스마트 그룹은 ‘매체 제어 > 그룹 > 만들기 > 스마트 그룹 콤 > 객체 선택 > 컴퓨터 / 사용자 이름 규칙 설정’을 통해서 만들 수 있고 이름 규칙은 포함 및 제외로 설정이 가능합니다.



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

참고

규칙은 대소문자 구분이 필요합니다.

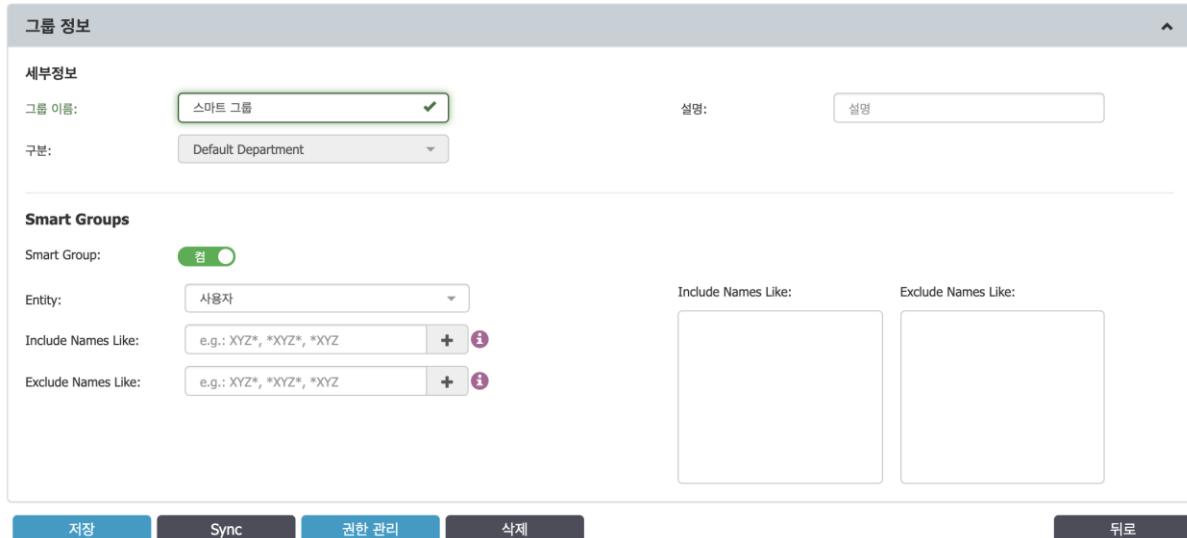
스마트 그룹은 스마트 그룹에 할당된 일반 그룹의 항목을 삭제하지 않습니다.

객체는 동기화로 스마트 그룹에 추가됩니다. 동기화를 하려면 관리자는 저장을 누르고 동기화 버튼을 눌러야 합니다. 동기화 버튼이 눌러지면 매 1분의 간격으로 운영됩니다. 새로운 스마트 그룹이 저장된 후에만 동기화를 찾을 수 있습니다.

동기화는 일반 그룹에 어떤 것도 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.



스마트 그룹은 일부 제한을 가지고 있습니다: 할당된 컴퓨터 또는 사용자는 표시되지 않습니다. 스마트 그룹은 수동 선택이 불가능하고 구분을 사용하지 않지만 기본 구분의 부분입니다.

시스템 설정에서 스마트 그룹을 사용하지 않으면 스마트 그룹은 설정, 권한 등을 가지고 있는 일반 그룹이 되지만 객체는 사라지고 컴퓨터의 기본 그룹과 사용자의 기본 그룹은 삭제됩니다.

스마트 그룹은 삭제할 수 있습니다.

사용자 객체만 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).

기본 그룹은 스마트 그룹을 사용할 때만 사용할 수 있는 새로운 범주의 그룹입니다. 이는 '시스템 구성 > 시스템 설정 > 스마트 그룹 > 컴퓨터 기본 그룹 사용 / 사용자 기본

그룹 사용' 을 통해서 사용할 수 있습니다.

Smart Groups

Enable Smart Groups:

Enable Default Group for Computers:

Enable Default Group for Users:

컴퓨터 기본 그룹 사용과 사용자 기본 그룹 사용을 활성화하면 두 그룹은 자동으로 생성됩니다.

그룹 목록

필터	표시	10 항목	Excel	PDF	CSV	열 표시/숨김	다시 읽기
<input type="checkbox"/>	그룹 이름	그룹 설명	Group Type	도메인	우선 순위	작업	
<input type="checkbox"/>	Default Group - Computers	Default Group for Computers	기본값	-	1	:≡	
<input type="checkbox"/>	Default Group - Users	Default Group for Users	기본값	-	2	:≡	

전체의 1 부터 2 까지 2 항목

이전 1 다음

만들기 작업 선택 삭제 뒤로

기본 그룹은 스마트 그룹에 속하지 않는 컴퓨터와 사용자의 그룹입니다. 여기에는 스마트 그룹에서 설정한 이름 패턴을 따르지 않는 컴퓨터와 사용자가 있습니다.

컴퓨터와 사용자를 기본 그룹에 할당하기 위해서는 다음 단계를 거쳐야 합니다. '매체 제어' -> 그룹 -> 기본 그룹 수정 -> 저장 버튼 누르기 -> 동기화 버튼 누르기' 입니다.

Device Control - Groups - Edit Default Group - Computers

그룹 정보

세부정보

그룹 이름: Default Group - Computers 설명: Default Group for Computers

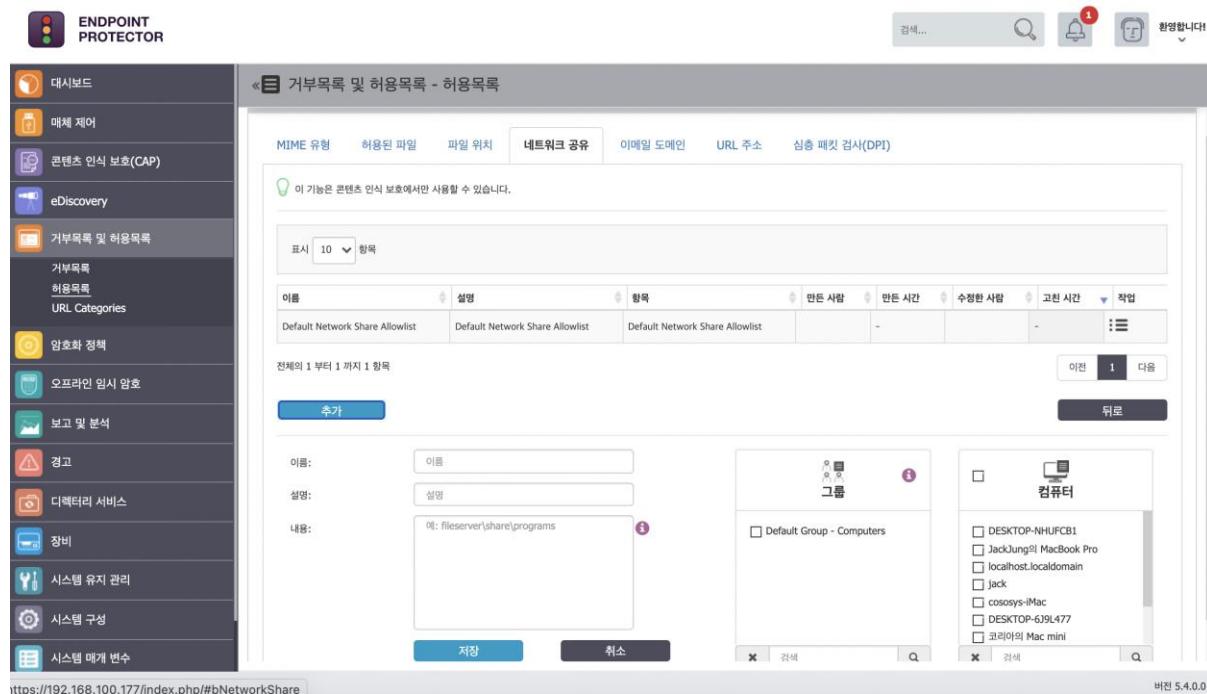
구분: Default Department

저장 동기화 권한 관리 뒤로

기본 그룹에는 제한이 있습니다: 기본 그룹의 이름은 수정할 수 없고 설명만 수정이 가능합니다. 이 그룹들은 삭제가 안되고 사용하지 않음으로만 할 수 있습니다. 기본 그룹을 사용하지 않으면 모든 의존성 (dependencies)이 삭제됩니다.

컴퓨터 그룹의 허용목록

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



The screenshot shows the 'Network Share Allowlist' configuration page within the Endpoint Protector web interface. The left sidebar contains navigation links such as Dashboard, Audit Log, Content Protection (CAP), eDiscovery, Network Share & Allowlist, Group Policy, Offline Access, Reporting, and Notifications. The main content area has tabs for MIME Type, Shared File, File Location, Network Share (selected), Email Domain, URL Address, and Advanced Search. A message indicates that this feature is available only in Content Protection mode. The table lists a single entry: 'Default Network Share Allowlist' under 'Name', 'Default Network Share Allowlist' under 'Description', and 'Default Network Share Allowlist' under 'Share'. The right side shows a list of computers: DESKTOP-NHUFBCB1, JackJung's MacBook Pro, localhost.localdomain, jack, cososys-iMac, DESKTOP-639L477, and 코리아의 Mac mini. The bottom status bar shows the URL https://192.168.100.177/index.php/#bNetworkShare and the version 5.4.0.0.

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 동기화합

니다. 허용목록 또는 거부목록에 선택된 그룹은 매 15분마다 동기화합니다.

3.5.2. 그룹 권한

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

The screenshot shows the 'Group Permissions' section for 'Computers' in the Endpoint Protector software. The left sidebar includes icons for Device Board, Computer, User, Group (selected), Full Settings, File Allowlist, and User Classes. The main panel displays a list of hardware components with dropdown menus for permission settings:

장치 유형	설정	설정 유지
미확인 저장장치	전체 설정 유지	SATA 컨트롤러(eSATA)
USB 저장장치	전체 설정 유지	WiFi
내장 CD/DVD/BR 드라이브	전체 설정 유지	Bluetooth
내장 카드 리더	전체 설정 유지	FireWire(1394) 저장장치
내장 플로피 드라이브	전체 설정 유지	시리얼 포트
네트워크 프린터	전체 설정 유지	PCMCIA 장치
로컬 프린터	전체 설정 유지	MTD 방식 카드 리더
Windows 스마트 기기 (MTP)	전체 설정 유지	SCSI 방식 카드 리더
디지털 카메라	전체 설정 유지	ZIP 드라이브
블랙박스	전체 설정 유지	ADB 및 Teensy Board
휴대폰 (Sony Ericsson, etc.)	전체 설정 유지	Thunderbolt
스마트폰 (USB 동기화)	전체 설정 유지	네트워크 공유
스마트폰 (Windows CE)	전체 설정 유지	적외선 동글
노키아폰 (Symbian)	전체 설정 유지	병렬 포트 (LPT)
웹캠 (Webcam)	전체 설정 유지	썬 클라이언트 저장소 (RDP 저장소)
iPhone	전체 설정 유지	추가 키보드 (속 BadUSB)
iPad	전체 설정 유지	USB 모델

© 2004 - 2021 CoSoSys Ltd. All rights reserved. 버전 5.3.0.0

컴퓨터 권한 섹션과 유사합니다. 그룹으로 설정된 모든 컴퓨터에 적용됩니다.

팁

표준 매체 제어 권한에는 '장치 유형'과 '이미 있는 장치'가 포함되어 있습니다. 일반적으로 사용되는 유일한 장치 권한입니다.

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

정보

장치 유형 및 특정 장치 (표준, 외부 네트워크, 업무 시간)에 대한 자세한 내용은 '3.6.1 전체 권한'을 참조하시기 바랍니다.

참고

전체 권한 복원 버튼은 권한을 전체 권한을 따르도록 만드는데 사용할 수 있습니다. 이 버튼은 전체 권한 뿐만 아니라 전체 설정도 따릅니다.

해당 수준에 설정된 이미 존재하는 장치는 복원 버튼을 누르면 삭제됩니다.

3.5.3. 그룹 설정

이 섹션에서 관리자는 각 그룹의 설정을 편집할 수 있습니다.

The screenshot shows the 'Endpoint Protector' web interface. On the left, there's a sidebar with icons for Dashboard, Device Manager, eDiscovery, and other features. The main content area is titled 'Endpoint Protector 클라이언트' (Endpoint Protector Client) and shows 'Group Settings'. It includes fields for log rotation (e.g., log size, log count), password complexity (e.g., length, uppercase/lowercase, numbers, symbols), and file transfer limits (e.g., maximum file size, maximum log size). There are also sections for user authentication (OTP, two-factor authentication) and reporting (reporting frequency). At the bottom right, it says '버전 5.4.0.0' (Version 5.4.0.0).

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.

3.6. 전체

이 섹션에서 관리자는 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:

장치 > 컴퓨터 | 사용자 > 그룹 > 전체

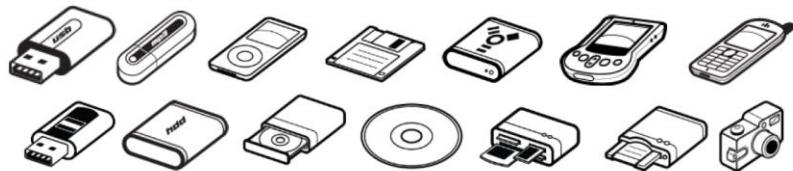
3.6.1. 전체 권한

이 섹션은 전체 시스템과 관련이 있고 관리자는 장치 유형과 이미 있는 장치에 권한을 부여할 수 있습니다.

장치 유형	권한
미확인 저장장치	사용 허용
USB 저장장치	사용 허용
내장 CD/DVD/BR 드라이브	사용 허용
내장 카드 리더	사용 허용
내장 플로피 드라이브	사용 허용
네트워크 프린터	사용 허용
로컬 프린터	사용 허용
Windows 스마트 기기 (MTP)	사용 허용
디지털 카메라	사용 허용
블랙베리	사용 허용
휴대폰 (Sony Ericsson, etc.)	사용 허용
스마트폰 (USB 동기화)	사용 허용
스마트폰 (Windows CE)	사용 허용
노키아폰 (Symbian)	사용 허용
웹캠 (Webcam)	사용 허용
iPhone	사용 허용
SATA 컨트롤러(eSATA)	사용 허용
WiFi	사용 허용
Bluetooth	사용 허용
FireWire(1394) 저장장치	사용 허용
シリ얼 포트	사용 허용
PCMCIA 장치	사용 허용
MTD 방식 카드 리더	사용 허용
SCSI 방식 카드 리더	사용 허용
ZIP 드라이브	사용 허용
ADB 및 Teensy Board	사용 허용
Thunderbolt	사용 허용
네트워크 공유	사용 허용
적외선 동글	사용 허용
병렬 포트 (LPT)	사용 허용
scn 클라이언트 저장소 (RDP 저장소)	사용 허용
추가 키보드 (혹 BadUSB)	사용 허용

3.6.1.1. 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/Paralled 포트는 스토리지 장치에만 적용
- 플로피 디스크 드라이브
- 시리얼 ATA 컨트롤러

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

정보

Endpoint Protector의 TrustedDevicesTM 기술은 4단계의 보안을 사용합니다. 이것은 장치에 제공된 보호 수준에 따릅니다. (EasyLockTM은 TD 레벨1입니다.)

TrustedDevicesTM과 EasyLockTM의 더 자세한 정보는 '15.1.1 Trusted Devices'를 참조 바랍니다.

팁

'유선 네트워크가 있으면 WiFi 차단' 권한이 있습니다.

이 옵션은 관리자가 유선 네트워크 통신이 있으면 WiFi 연결을 사용할 수 없도록 만듭니다. WiFi 연결은 유선 네트워크 연결이 없으면 사용 가능합니다.

참고

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.

3.6.1.2. 이미 있는 장치 (표준)

이 옵션은 관리자가 특정 장치에 접근 권한을 부여할 수 있도록 합니다. 전체 또는 그룹, 사용자 또는 컴퓨터에 설정할 수 있는 섬세한 기능입니다.

정보

각각의 섹션 및 객체에서 관리 권한 액션을 사용하여 전체, 그룹, 사용자, 컴퓨터 별로 장치 권한을 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.

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

장치 마법사 (단계 2/2)							
필터를 사용하여 원하는 장치를 표시하세요.							
	장치 유형	장치 이름	설명	VID	PID	일련 번호	장치 코드
<input type="checkbox"/>	USB Storage Device	USB_FLASH_DISK	USB_FLASH_DISK/GENERAL	90c	1000	0423340000006813	9E16 DESKTOP-HOBPV3K
<input type="checkbox"/>	USB Storage Device	USB Attached SCSI (UAS) Mass Storage Device	USB Attached SCSI (UAS) Mass Storage Device/JMicron Technology Corp. / JMicron USA Technology Corp.	152d	583	0123456789ABC	EA3D DESKTOP-HOBPV3K

전체의 1 부터 2 까지 2 항목

이전 1 다음

[뒤로](#) [저장](#)

- **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.

장치 마법사 (단계 2/2)			
<input type="button" value="VID"/>	<input type="button" value="PID"/>	<input type="button" value="일련번호 범위의 첫 번째"/>	<input type="button" value="일련번호 범위의 마지막"/>
<input type="button" value="설명"/>			

[뒤로](#) [저장](#)

참고

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

- **장치의 벌크 리스트** – 2단계에서 2개에서 500까지의 장치를 동시에 입력할 수 있습니다. 가져오기와 단순히 붙여넣기 두 가지 방법을 사용할 수 있습니다.

장치 마법사 (단계 2/2)	
등록 옵션:	<input checked="" type="radio"/> 콘텐츠 붙여넣기 혹은 입력 <input type="radio"/> 콘텐츠 가져오기
장치:	<input type="text" value="e.g.: Sac, Sb9, BB4001110130000001, STORAGE_MEDIA"/> !

[뒤로](#) [저장](#)

정보

파일 허용목록 기능은 USB 저장 장치의 사용 허용 권한에서 사용할 수 있습니다. 더 자세한 정보는 '3.7 파일 허용목록' 섹션을 참조하시기 바랍니다.

3.6.1.3. 외부 네트워크

참고

이 기능을 사용하려면 '전체 설정' 섹션에서 설정이 필요합니다.

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

Category	Setting	Value
사용 거부	WIFI	사용 거부
	Bluetooth	사용 거부
사용 허용	FireWire(1394) 저장장치	사용 거부
	사용 거부	사용 허용
사용 거부	사리얼 포트	사용 거부
	사용 거부	사용 거부
사용 허용	PCMCIA 장치	사용 거부
	사용 거부	사용 거부
사용 거부	MTD 방식 카드 리더	사용 거부
	SCSI 방식 카드 리더	사용 거부
사용 허용	ZIP 드라이브	사용 거부
	AIO 및 Teensy Board	사용 거부
사용 거부	Thunderbolt	사용 거부
	네트워크 공유	사용 허용
사용 허용	제이션 동글	사용 거부
	병렬 포트 (LPT)	사용 거부
사용 거부	센 클라이언트 저장소 (RDP 저장소)	사용 허용
	추가 키보드 (혹 BadUSB)	사용 허용
사용 허용	USB 모뎀	사용 허용
	안드로이드 스마트폰 (Mac MTP)	사용 거부
사용 거부	Chip Card Device	사용 허용
	모든 장치 허용	모든 장치 차단

3.6.1.4. 근무 외 시간

참고

이 기능을 사용하려면 '전체 설정' 섹션에서 설정이 필요합니다.

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

The screenshot shows the Endpoint Protector software interface. The left sidebar contains a navigation menu with various icons and labels: 대시보드 (Dashboard), 매체 제어 (Media Control), 대시보드 (Dashboard), 장치 (Device), 컴퓨터 (Computer), 사용자 (User), 그룹 (Group), 전체 권한 (Full Access), 전체 설정 (Full Settings), 사용자 경의 알림 메시지 (User Alert Message), 파일 하이트리스토 (File Hierarchy), 사용자 클러스터 (User Cluster), 페렌트 인식 보호(CAP), eDiscovery, 블랙리스트 및 회이트리스토 (Blacklist and Whitelist), 암호화 정책 (Encryption Policy), 모바일 기기 관리(MDM), 오프라인 일자 읽기 (Offline Read), 보고 및 분석 (Report and Analysis), 경고 (Warning), 디렉토리 서비스 (Directory Service), 정비 (Maintenance), 시스템 유지 관리 (System Maintenance). The main content area displays a table of connected devices with columns: 장치 유형 (Device Type), 사용 거부 (Block Usage), WiFi, 사용 허용 (Allow Usage), 사용 허용 (Allow Usage). The table includes rows for various devices: USB 저장장치 (USB Storage Device), 내장 CD/DVD/BR 드라이브 (Internal CD/DVD/BR Drive), 내장 카드 리더 (Internal Card Reader), 내장 플로피 드라이브 (Internal Floppy Drive), 로컬 프린터 (Local Printer), Windows 스마트 기기 (MTP) (Windows Smart Device (MTP)), 디지털 카메라 (Digital Camera), 블랙리스트 (Blacklist), 휴대폰 (Sony Ericsson, etc.), 스마트폰 (USB 동기화) (Smartphone (USB Sync)), 스마트폰 (Windows CE), 노사파운 (Symbian), 웹캠 (Webcam), iPhone, iPad, iPod, SATA 컨트롤러(eSATA), WiFi, Bluetooth, FireWire(1394) 저장장치, 시리얼 포트, PCMCIA 카드, MTD 방식 카드 리더, SCSI 방식 카드 리더, ZIP 드라이브, ADB 및 Teensy Board, Thunderbolt, 네트워크 공유, 적외선 등록, 병렬 포트 (LPT), 씬 클라이언트 저장소 (RDP 저장소), 추가 카보드 (혹 BadUSB), USB 모뎀, 안드로이드 스마트폰 (Mac MTP), Chip Card Device. At the bottom right are buttons for 모든 장치 사용 (All Device Use) and 모든 장치 차단 (All Device Block).

3.6.2. 전체 설정

이 섹션은 시스템의 모든 컴퓨터에 영향을 주는 글로벌 설정을 다룹니다. 컴퓨터에 대해 세밀하게 정의된 설정이 없고 그룹에 속해 있지 않다면 설정은 상속이 됩니다. 만약 컴퓨터가 그룹에 있다면 그룹의 설정을 상속받습니다.

« 매체 제어 - 전체 설정

클라이언트 에이전트 모드:	정상모드	알림 언어:	영어
정책 경신 주기 (초):	300	로그 크기 (MB):	512
로그 간격(분):	30	사본보관 크기(MB):	512
사본보관 간격(분):	60	사본보관의 최소 파일 크기(KB):	0
복구 풀러의 보존 기간(일):	3	사본보관의 최대 파일 크기(KB):	512
		장치 복구 폴더 최대 크기 (MB):	5000
사용자 정의 알림 메시지:		사용자의 정보 입력:	<input type="checkbox"/>
OTP 사용 이유 제출 필수:		광학 인식 문자:	<input type="checkbox"/>
심층 패킷 검사(DPI):		위협 임계값에서 중단:	<input type="checkbox"/>
확장된 소스 코드 감지:			
Disable Bluetooth File Transfer:			

클라이언트 모드, 파일 추적, 파일 사본 보관, 사용자 저의 클라이언트 알림 뿐만 아니라 근무와 시간 정책, 외부 네트워크 정책, 전송 제한 등은 이 섹션에서 설정할 수 있는 강력한 기능입니다. 아래에서 더 자세히 살펴보겠습니다.

팁

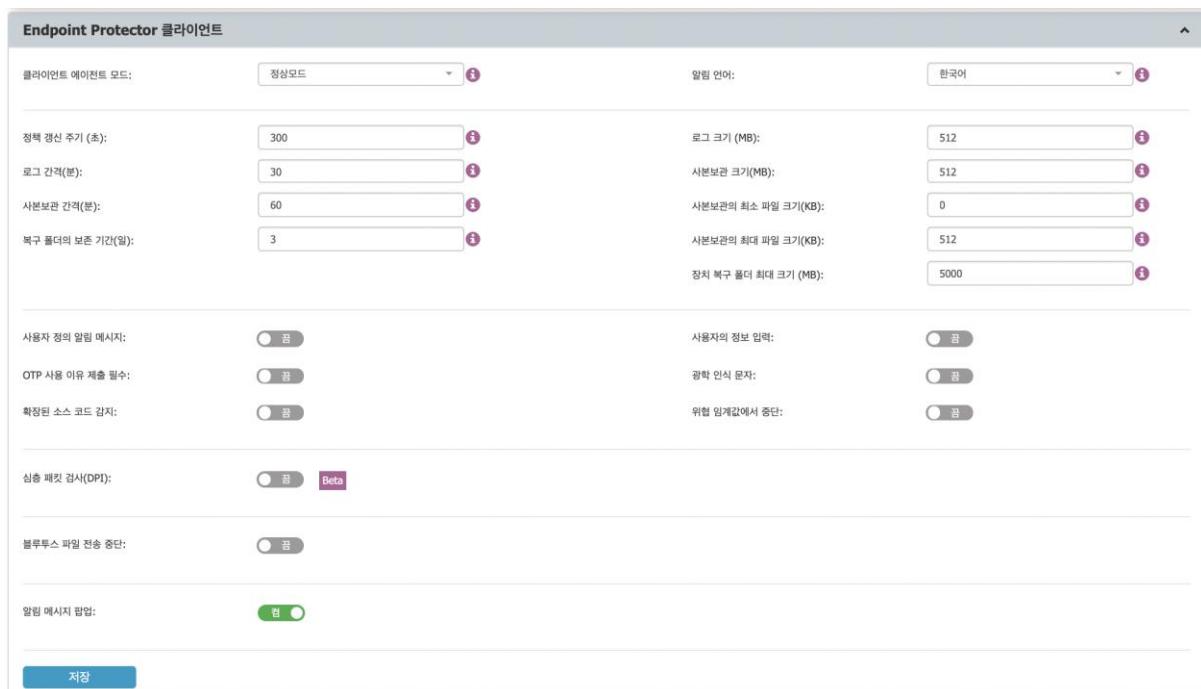
위협 임계값 중단이 활성화 되어 있으면 보고만 정책의 위협 임계값에 도달한 후에 발견된 정 보는 더 이상 로그로 남지 않습니다. 상당한 로그 수를 줄일 수 있어서 할당된 저장 공간을 최적화합니다.

참조

이 섹션의 일부 설정은 다른 모듈 (예: 콘텐츠 인식 보고 및 eDiscovery 등)과 관련이 있습니다. 매체 제어 모듈에만 관련이 없습니다.

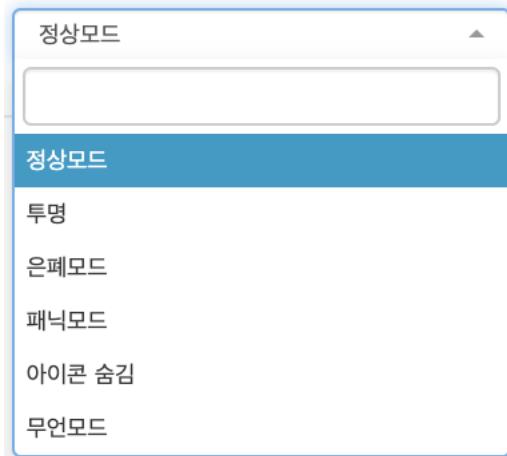
3.6.2.1. Endpoint Protector 클라이언트 설정

Endpoint Protector 클라이언트는 사용자, 컴퓨터, 그룹 별로 여러가지 모드를 제공합니다. 이 모드는 사용자, 컴퓨터, 그룹에서 모두 사용이 가능합니다.



클라이언트 모드

Endpoint Protector 클라이언트는 여러가지 모드를 제공합니다.



위와 같이 선택할 수 있는 6가지 모드가 있습니다.

▪ 정상모드 (Endpoint Protector 기본 설정)

참고

다른 모드에 대한 완전한 이해 없이 정상모드 변경을 권장하지 않습니다.

정상모드가 사내 정책에 적절하지 않다면 온폐모드 또는 무언모드가 일반적으로 가장 적절한 선택입니다.

▪ 투명모드

정보

이 모드는 아래와 같이 동작합니다:

- 시스템 트레이 아이콘 보이지 않음
- 시스템 트레이 알림 보이지 않음
- 설정된 권한에 관계없이 모두 차단
- 관리자는 모든 활동의 경고 알림을 받음

팁

이 모드는 모든 장치를 차단하는데 유용하지만 사용자는 Endpoint Protector 클라이언트의 모든 사용 제한 또는 존재를 인지하지 못합니다.

▪ 은폐모드**정보**

이 모드는 아래와 같이 동작합니다:

- 시스템 트레이 아이콘 보이지 않음
- 시스템 트레이 알림 보이지 않음
- 설정 권한에 관계없이 모두 허용
- 모든 사용자 활동을 모니터링하기 위해서 파일 추적 및 사본 보관 허용
- 관리자는 모든 활동의 경고 알림 받음

팁

이 모드는 모든 사용자와 컴퓨터를 모니터링하는데 유용하지만 사용자는 Endpoint Protector 클라이언트의 존재와 활동을 인지하지 못합니다. 모든 활동이 허용되고 사용자를 방해하지 않습니다.

▪ 패닉모드**정보**

이 모드는 아래와 같이 동작합니다:

- 시스템 트레이 아이콘 보임
- 시스템 트레이 알림 보임
- 설정된 권한에 관계없이 모두 차단
- 모든 사용자 활동을 모니터링하기 위해서 파일 추적 및 사본 보관 허용
- 관리자는 패닉모드로 들어가고 나올 때 경고 알림을 받음

참고

이 모드는 사용자의 악의적인 의도 및 활동이 탐지되는 극단적인 상황에서 자동으로 동작이 될 수도 있습니다.

특정한 상황에서 관리자는 또한 모든 장치 차단을 위해서 수동으로 설정할 수 있습니다. 그러나 이런 식으로 모드를 설정하는 것을 권장하지 않습니다.

■ 아이콘 숨김 모드

정보

이 모드는 아래와 같이 동작합니다:

- 시스템 트레이 아이콘 보이지 않음
- 시스템 트레이 알림 보이지 않음
- 모든 권한 및 설정은 유지됨

팁

이 모드는 정상모드와 비슷합니다. 다른 점은 Endpoint Protector 클라이언트가 사용자에게 보이지 않는 것입니다.

■ 무언모드

정보

이 모드는 아래와 같이 동작합니다:

- 시스템 트레이 아이콘 보임
- 시스템 트레이 알림 보이지 않음
- 모든 권한 및 설정은 유지됨

팁

이 모드는 정상모드와 비슷합니다. 다른 점은 트레이 팝업 알림이 사용자에게 보이지 않는 것입니다.

클라이언트 언어

Endpoint Protector 클라이언트 언어

정책 갱신 간격(sec)

최신 설정, 권한 정책 업데이트를 하는 클라이언트와 서버 사이의 시간 간격

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.

로그 간격 (min)

클라이언트가 로그를 서버로 보내는 시간 간격

사본 보관 크기 (MB)

클라이언트의 모든 파일 사본 보관 최대 크기. 이 값에 도달하면 가장 오래된 사본 보관은 삭제되고 새로운 사본 보관으로 덮어씁니다.. 클라이언트와 서버가 통신하지 않는 최대 시간 동안 사용이 됩니다.

사본 보관 간격 (min)

클라이언트가 사본 보관을 서버로 보내는 시간 간격

사본 보관의 최소 파일 크기 (KB)

파일 사본 보관을 만드는 최소 파일 크기

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.

사본 보관의 최대 파일 크기 (KB)

파일 사본 보관을 만드는 최대 파일 크기

복구 폴더의 최대 크기 (MB)

Mac과 Linux 컴퓨터에 해당됩니다. 격리 폴더의 최대 크기입니다. 이 값에 도달하면 새로운 파일이 가장 오래된 파일을 덮어쓰기 합니다.

사용자 정의 알림 메시지

사용으로 되어 있으면 클라이언트 알림은 사용자가 정의한 것으로 나타납니다.

사용자 정보 편집

사용으로 되어 있으면 사용자가 Endpoint Protector 클라이언트의 사용자와 컴퓨터 정보를 편집할 수 있습니다.

OTP 요청 이유 의무화

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.

심층 패킷 검사

이 옵션을 켜면 콘텐츠의 네트워크 트래픽을 검사할 수 있습니다. 이 옵션은 심층 패킷 검사 허용목록과 URL 및 도메인 거부목록을 수행합니다.

심층 패킷 검사

이 옵션을 켜면 콘텐츠의 네트워크 트래픽을 검사할 수 있습니다. 이 옵션은 심층 패킷 검사 허용목록과 URL 및 도메인 거부목록을 수행합니다.

보안 안 된 연결 차단

이 옵션을 켜면 HTTP를 통한 보안이 없는 접근은 차단되고 사용자 접근은 제한됩니다.

정보

보안 안 된 연결 차단 기능은 심층 패킷 검사 기능이 사용 중일 때만 동작합니다.

VPN 트래픽 가로채기

이 옵션을 켜면 Endpoint Protector 클라이언트는 네트워크 확장 프레임워크를 사용하여 macOS의 VPN 트래픽을 가로챕니다.

정보

'VPN 트래픽 가로채기' 기능은 '심층 패킷 검사 (DPI)' 기능이 활성화 되어 있을 때만 사용할 수 있습니다. macOS 11.0 이전 버전에서만 사용이 가능하고 DPI 인증서가 추가되어 있는 경우에만 사용할 수 있습니다.

이 기능을 사용하려면 아래 단계를 반드시 따라야 합니다.

1. 심층 패킷 검사 (DPI) 활성화하기
2. VPN 트래픽 가로채기 활성화하기
3. '네트워크 확장을 사용하지 않을 때 EPP 동작'에 대한 옵션을 선택하기

참고

-**심층 패킷 검사 임시 사용하지 않음:** DPI를 임시로 사용하지 않습니다.

-**인터넷 접근 차단:** 최종 사용자가 Endpoint Protector 프록시 설정을 허용할 때까지 인터넷 연결을 차단합니다.

4.9 | Endpoint Protector | 사용 설명서

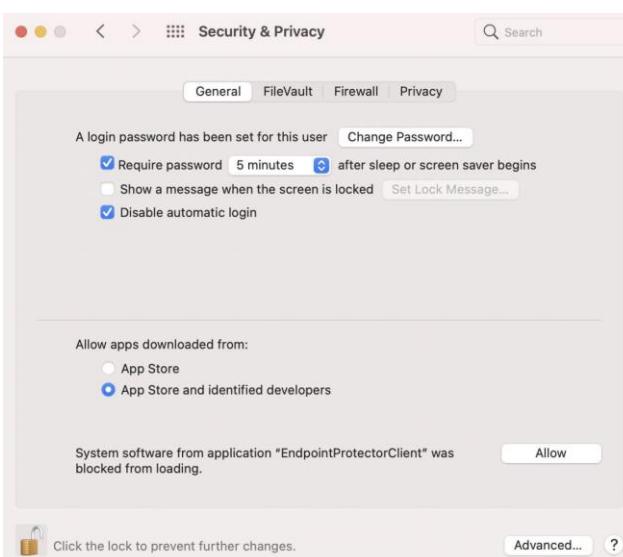
The screenshot shows the Endpoint Protector software interface. The left sidebar contains navigation links such as Dashboard, Audit Log, Device Board, Computer, User, Group, Network Control, General Settings, File Allowlist, User Classes, Content Protection (CAP), eDiscovery, Denylists and Allowlists, IP Blocking, Offline Temporary Blocking, Reporting and Analysis, and Alerts. The main panel displays the 'General - Full Settings' configuration page. It includes various configuration options like log retention, audit log size, and network extension behavior. A dropdown menu under 'EPP behaviour when network extension is disabled' lists 'Temporary Disable Deep P...', 'Temporary Disable Deep Packet Inspection', and 'Block Internet access'. The bottom right corner indicates the version '버전 5.3.0.5'.

4. 변경 내용 저장하기

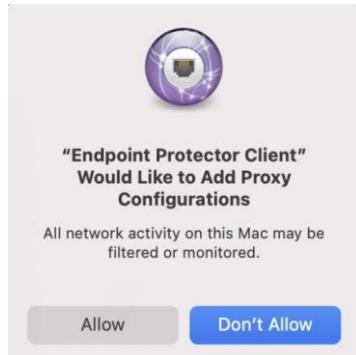
5. 최종 사용자에게 시스템 확장이 차단되었다는 정보가 표시된 아래 팝업이 나타나면 허용하기



6. '시스템 환경 설정 -> 보안 및 개인 정보 보호 -> 일반' 탭으로 이동 후 Endpoint Protector Client 확장 허용하기



7. 아래 화면이 표시되면 Endpoint Protector 프록시 설정을 허용하기

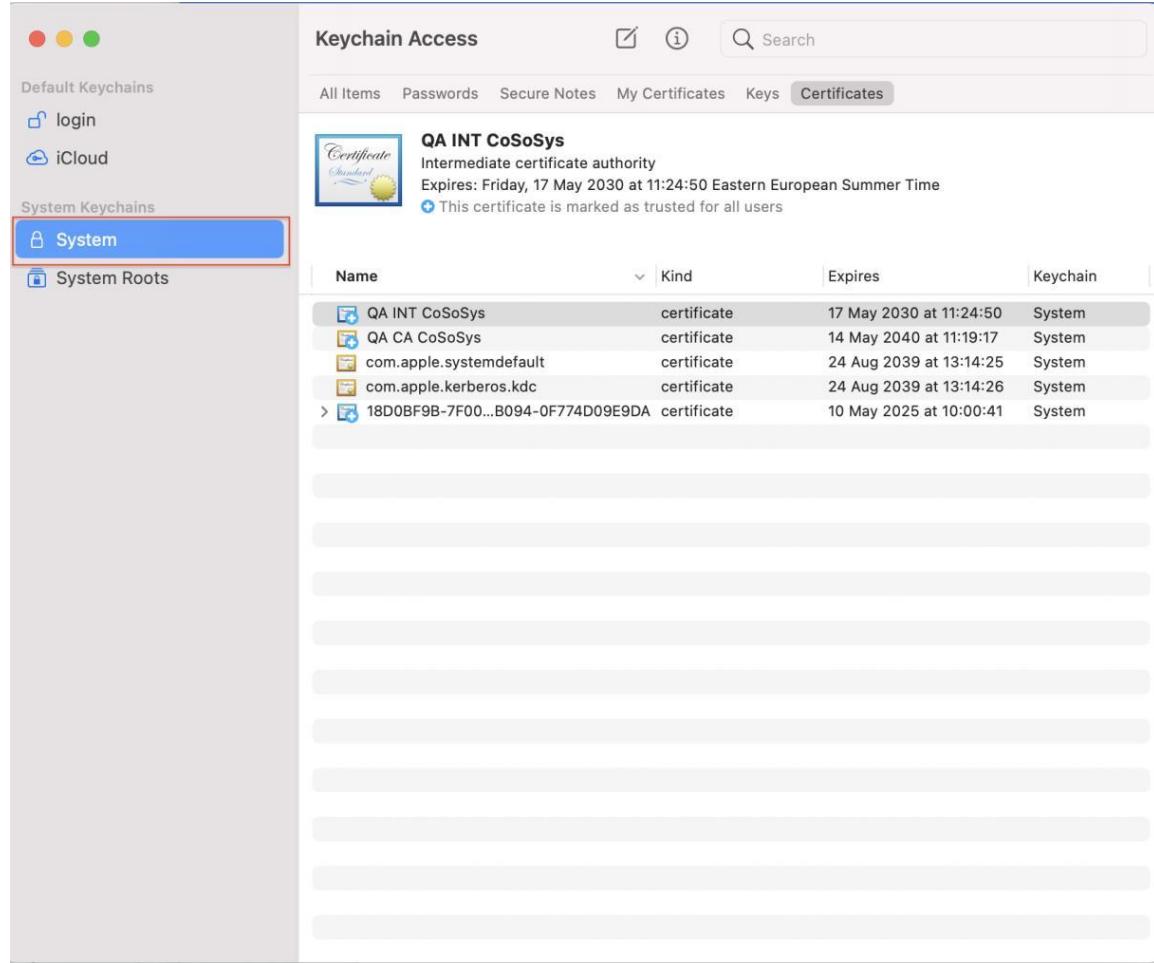


정보

네트워크 확장을 성공적으로 사용되면 '클라이언트 무결성 OK' 로그가 생성됩니다.

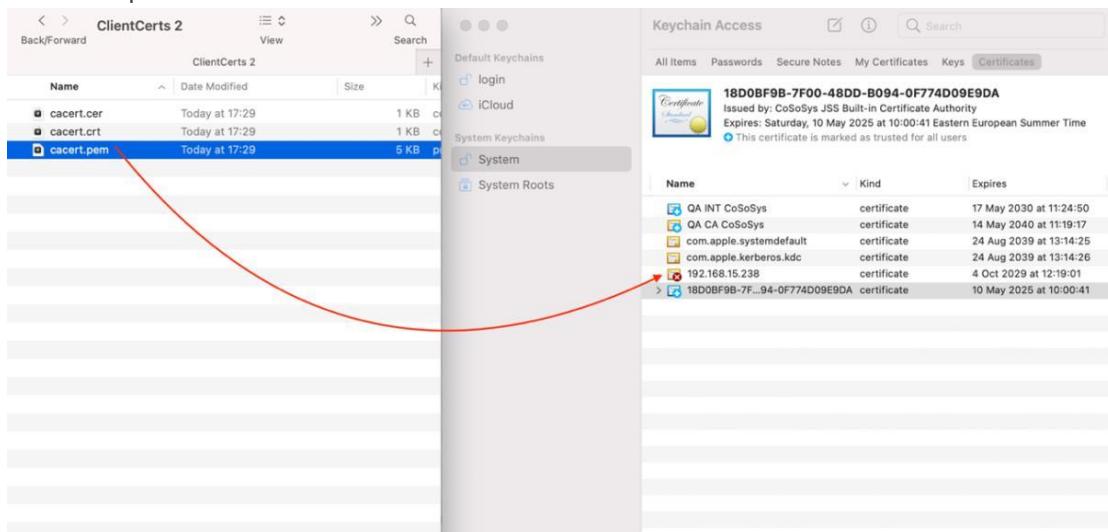
8. '시스템 구성 > 시스템 설정 > DPI 인증서'로 이동해서 CA 인증서 다운로드 하기

9. macOS에서 '키체인 접근' 응용프로그램은 열고 '시스템' 선택을 확인하기

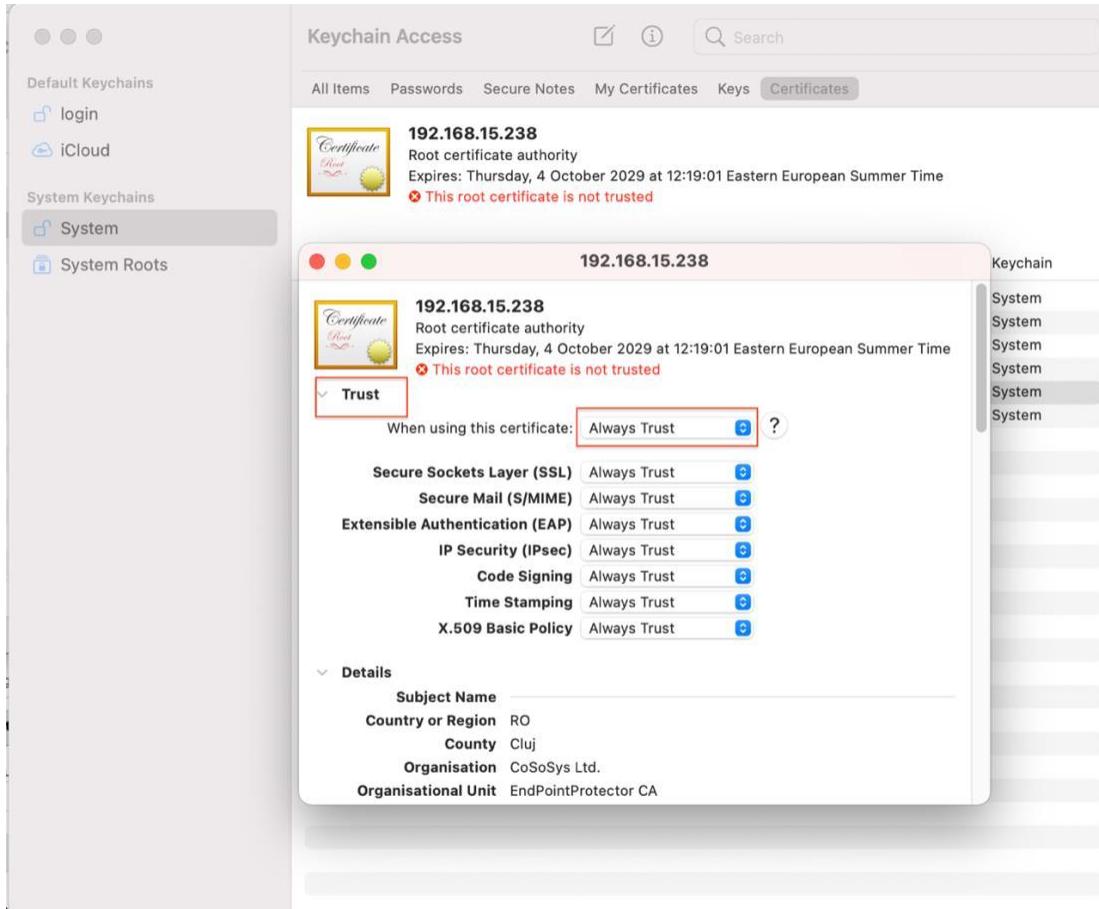


10. 다운로드한 ClientCerts 파일의 압축을 해제하기

11. cacert.pem 파일을 선택하고 '키체인 접근 -> 시스템'에 드래그 앤 드롭하기



12. 새롭게 추가된 인증서는 'x' 표시가 됨. 더블 클릭 후 신뢰 섹션에서 '항상 신뢰' 선택하기



13. 변경 저장하기

확장된 소스 코드 감지

이 옵션을 켜면 ngram 탐지가 확장되어서 PDF, docx 등과 같은 파일 유형에 있는 소스 코드를 감지합니다.

Bluetooth 파일 전송 사용하지 않음

이 옵션을 켜면 Bluetooth 장치의 전송을 허용하지 않습니다. 이는 엔드포인트의 페어링 여부와 관계가 없습니다. Windows에서만 사용이 가능합니다.

팝업 알림

관리자는 팝업 알림을 선택할 수 있습니다.

사용자 조치 팝업

이 설정은 사용자 조치 기능이 활성화 시 사용할 수 있습니다. 관리자가 최종 사용자에 대한 사용자 조치 팝업 알림을 사용할 수 있는 옵션입니다.

강제 사용자 조치 팝업

이 설정은 사용자 조치 팝업 설정이 활성화 될 때만 사용할 수 있습니다. 이 설정이 활성화되면 최종 사용자는 사용자 조치 팝업 알림을 중단할 수 없습니다.

3.6.2.2. 파일 추적과 사본 보관

파일 추적 기능은 보호되는 클라이언트와 휴대용 저장 장치, 내부 eSATA 하드드라이브 및 네트워크 공유 사이의 데이터 트래픽 모니터링을 허용합니다. 누가 언제 어디서 어떤 파일을 복사했는지 보여줍니다. 파일 이름 변경, 삭제, 읽기, 수정 등의 활동도 볼 수 있습니다. 그룹 또는 컴퓨터 별로 설정이 가능하며 매체 제어 > 전체 설정에서 설정할 수 있습니다.

정보

'매체 제어 > 전체 설정'에서 사용하거나 그룹 또는 컴퓨터에서 따로 설정이 가능합니다.

파일 추적 및 사본보관

파일 추적:

- 전부
- 이동식 장치
- eSATA HDD 혹은 티임마신
- 네트워크 공유

파일 사본보관:

- 전부
- 이동식 장치 및 다른 저장장치
- 콘텐츠 인식 보호(CAP)
- 이메일 본문

추적에서 제외된 확장자: e.g.: .mp3;.vob;.exe;

검색에서 제외할 확장자: e.g.: .mp3;.vob;.exe;

파일 추적 방향: Both (Outgoing & Incoming)

사본보관에서 제외된 확장자: e.g.: .mp3;.vob;.exe;

입출 파일 속의 암축 파일 검색: 8회

Block Time Machine: 허용 금지

메타데이터 검색: 허용 금지

개선된 프린터 및 MTP 검색: 허용 금지

파일 해시: 허용 금지

인쇄된 문서 스캔: 각 문서

저장

파일 추적은 파일 추적에서 제외된 확장자 옵션을 사용하여 특정 파일 유형을 추적하지 않을 수 있습니다.

참고

Time Machine 차단 옵션을 체크해서 macOS에서 Time Machine 백업을 차단할 수 있습니다.

파일 추적 경로는 관리자가 전송 경로를 기반으로 파일 전송을 모니터링 할 수 있습니다
– 나가는 경로, 들어오는 경로, 모든 경로.

나가는 파일 추적 경로는 로컬 머신에서 휴대용 저장 장치로 전송하는 것으로 정의합니다.

들어오는 파일 추적 경로는 휴대용 저장 장치에서 로컬 머신으로 전송하는 것을 가리킵니다.

모든 경로 설정을 선택하면 관리자는 휴대용 저장 장치와 로컬 머신 사이의 모든 전송 유형을 모니터링 할 수 있습니다.

참고

파일 전송 경로는 휴대용 장치, 컴퓨터와 네트워크 공유 사이의 전송에서만 적용됩니다.
Windows와 macOS (버전 11.0 이상)에서만 사용이 가능합니다.

파일 사본 보관 기능은 파일 추적으로 제공되는 정보를 더 확장합니다. 사용자가 접근한 파일의 정확한 사본을 만듭니다. 사본 보관은 파일 복사, 파일 쓰기, 파일 읽기의 이벤트가 일어나면 만들어집니다. 파일 삭제, 파일 이름변경 등의 이벤트는 사본 보관을 하지 않습니다.

각 관리자의 필요에 따라서 파일 사본 보관은 지원하는 모든 휴대용 장치 (선택한다면 eSATA HDD 및 네트워크 공유 포함) 또는 콘텐츠 인식 보호 (온라인 응용프로그램, 프린터, 클립보드 등을 통한 파일 전송) 그리고 이메일 본분에서 사용 가능합니다.

정보

파일 추적 기능이 설정되지 않으면 파일 사본 보관은 사용할 수 없습니다.

파일 사본 보관은 파일 사본 보관에서 제외된 확장자 옵션을 사용해서 특정 파일 유형을 사본 보관하지 않을 수 있습니다.

참고

파일 사본 보관은 네트워크 트래픽, 다른 컴퓨터 또는 파일 크기에 대한 Endpoint Protector 설정으로 자연이 될 수 있습니다. 일반적으로 파일 사본 보관은 몇 분이 지나서 확인할 수 있습니다.

팁

250 ~ 1000 엔드포인트와 같은 시스템에서 가상 또는 하드웨어 어플라이언스의 전체 엔드포인트 용량의 15%까지만 파일 사본 보관 기능을 활성화 시키는 것을 강력하게 권장합니다.

(예: 1000 사용자 하드웨어 어플라이언스를 사용하고 있다면 파일 사본 보관은 최대 150 엔드포인트로 설정해야 최적화된 성능을 사용할 수 있습니다.)

3.6.2.3. 근무 외 시간과 외부 네트워크

이 섹션은 관리자가 '매체 유형 - 근무 외 시간 정책' 및 '매체 유형 - 외부 네트워크 정책'을 사용할 수 있도록 설정합니다.



근무 외 시간 정책 – 출퇴근 시간을 기준으로 필요한 시작 및 끝나는 시간 설정을 합니다.

외부 네트워크 정책 – DNS FQDN (Fully Qualified Domain Name)과 DNS IP 주소 기준으로 필요한 설정을 합니다.

한 번 설정을 하면 이 정책을 전제, 그룹, 사용자 또는 컴퓨터에서 사용할 수 있습니다.

참고

정책이 시작되면 이 대체 정책은 기본 정책을 대신합니다.

대체 정책에서 외부 네트워크 정책은 업무시간 정책을 대신합니다.

정보

콘텐츠 인식 보호 정책에서 외부 네트워크 및 업무시간 정책을 선택할 수 있습니다.

3.6.2.4. 전송 제한

이 섹션에서 관리자는 특정 시간 간격 (시간) 내에서 전송 제한을 설정할 수 있습니다. 한 번 제한에 도달하면 휴대용 매체 (매체 제어) 또는 제어되는 응용프로그램 (콘텐츠 인식 보호)를 통한 파일 전송은 이 시간 간격이 만료되거나 콘텐츠 수가 재설정 되기 전까지 사용이 불가능합니다. 네트워크 공유를 통한 파일 전송에서 또한 전송 제한 옵션을 사용할 수 있습니다.



참고

전송 제한에 도달을 체크하는 메커니즘은 컴퓨터 성능에 영향을 주지 않도록 설계되었습니다.

그러므로 제한에 도달하는 정확한 시각과 전송 제한 시행 사이에 약간의 지연이 발생할 수 있습니다. 일반적으로 몇 초 정도이지만 네트워크 환경에 따라서 몇 분이 될 수 도 있습니다.

전송 제한에 도달했을 때 선택할 수 있는 세가지 옵션이 있습니다.

- **보고만:** 전송 제한에 도달하면 보고만 합니다.
- **제한:** 매체 제어 정책에 정의된 장치 및 응용프로그램을 차단합니다.
- **잠금:** 매체 제어 정책에 관계없이 모든 장치를 차단합니다. 네트워크 인터페이스를 포함하기 때문에 모든 전송이 차단됩니다.

정보

전송 제한 시간 주기 만료 전에 서버와 클라이언트 통신을 다시 연결하기 위해서 전송 제한 도달 오프라인 임시 암호를 사용할 수 있습니다. 더 자세한 내용은 '8 오프라인 임시 암호'를 참조 하시기 바랍니다.

전송 제한 도달 경고를 또한 사용할 수 있습니다. 추가적으로 전송 제한 도달 보고서는 매일, 매주, 매달 기준으로 예약할 수 있습니다.



3.7. 파일 허용목록

이 섹션에서 관리자는 이미 허가된 휴대용 저장 장치에 허용된 파일만 전송하도록 제어 할 수 있습니다.

휴대용 저장 장치에 어떤 파일이 복사될 수 있고 복사 될 수 없는지 관리하는 것은 Endpoint Protector 서버에 허용목록 파일을 업로드하면서 정할 수 있습니다. 파일이 한번 업로드 되면 특정 파일 액션은 활성화 또는 비활성화 할 수 있습니다.



정보

파일 허용목록에 업로드 할 수 있는 최대 파일 크기는 190 MB 입니다.

참고

파일 허용목록은 컴퓨터 외부 소스에서 복사된 파일에는 적용되지 않습니다. 게다가 콘텐츠 인식 보호 (CAP) 모듈이 활성화되고 설정되면 매체 제어 모듈의 파일 허용목록보다 더 우선합니다.

3.8. 사용자 클래스

이 섹션은 관리자에게 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 '새로 추가' 버튼을 누르거나 정책 만들기를 더블 클릭해서 만들 수 있습니다.

정보

정책을 설정한 후에 편집, 복사, 삭제 옵션을 사용할 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** – 팝업이 열리고 보호되는 컴퓨터에 전에 연결된 장치와 그 후에 Endpoint Protector 데이터베이스에서 이미 사용 가능한 장치들을 선택할 수 있습니다.

장치 마법사 (단계 2/2)										
💡 필터를 사용하여 원하는 장치를 표시하세요.										
	장치 유형	장치 이름	식별 이름	설명	VID	PID	일련 번호	장치 코드	마지막 컴퓨터	🔍
<input type="checkbox"/>	USB Storage Device	External	GLOTRENDS External	External/GLOTRENDS	152d	583	0123456789ABC	EA3D	(주)코소시스코리아의 MacBook Pro	
<input type="checkbox"/>	USB Storage Device	CRUZER_BLADE	SanDisk Cruzer Blade USB Device	CRUZER_BLADE/SANDISK	781	5567	20044324321DF5C2F712	9C08	PTS-NI-KIMY	
<input type="checkbox"/>	USB Storage Device	STORAGE_DEVICE	Mass Storage Device USB Device	STORAGE_DEVICE/MASS	14cd	1212	121220160204	ECEF	PTS-NI-KIMY	
<input type="checkbox"/>	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	
<input type="checkbox"/>	USB Storage Device	STORAGE_DEVICE	n/a	STORAGE_DEVICE/GENERIC	5e3	736	000000000272	93A5	n/a	
<input type="checkbox"/>	USB Storage Device	STORAGE_DEVICE	n/a	STORAGE_DEVICE/GENERIC	5e3	716	000000009744	3E35	n/a	
<input type="checkbox"/>	USB Storage Device	ULTRA_USB_3.0	n/a	ULTRA_USB_3.0/SANDISK	781	5591	4C530001120206114085	3D5A	n/a	
<input type="checkbox"/>	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 지정해서 한 번에 추가할 수 있습니다. 이 기능의 권장 사용은 연속되는 범위와 명확한 패턴의 일련번호를 가진 장치에 사용하는 것입니다.

장치 마법사 (단계 2/2)

뒤로 저장

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 마법사 (단계 2/2)

등록 옵션: 콘텐츠 붙여넣기 혹은 입력 콘텐츠 가져오기

장치: e.g.: Sac, 5b9, BB4001110130000001, STORAGE_MEDIA

뒤로 저장

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

장치 마법사 (단계 1/2)

장치 유형:	내장 CD/DVD/BR 드라이브	✓ ▾
장치 권한:	사용 거부	✓ ▾
추가:	장치 클래스 (장치 유형)	✓ ▾

다음

예제

사용자 클래스로 CD-ROM 허용을 만들고 매체제어에서 CD-ROM / DVD-ROM 사용 허용 정책을 설정합니다. 클라이언트 PC는 CD-ROM 사용 거부가 설정되어 있어도 모든 CD / DVD - ROM은 사용 가능합니다. 사용자 클래스가 우선이기 때문입니다.

3.9. 장치 권한 우선순위

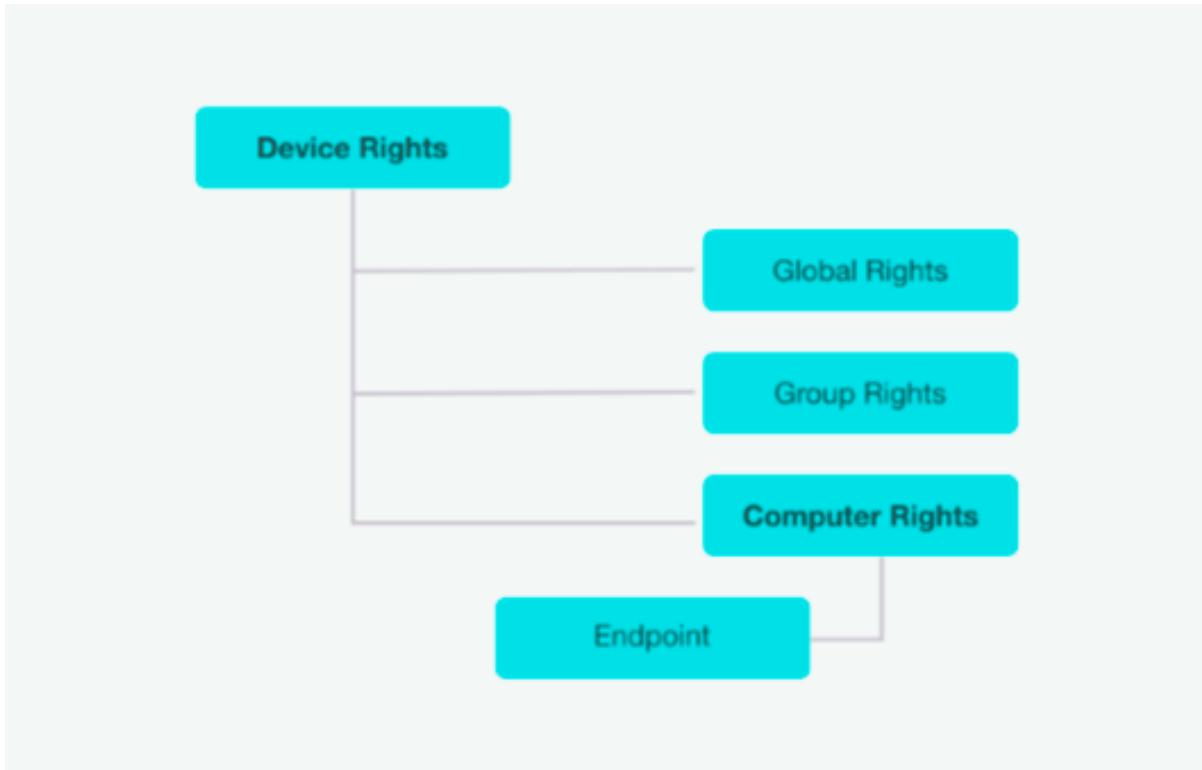
컴퓨터 권한, 그룹 권한, 정체 권한은 단일 설정이고 각각 다른 설정을 상속합니다. 이것은 하나가 변경되면 다른 설정에 영향을 미치는 것을 의미합니다.

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

정보

장치 권한은 모든 컴퓨터, 그룹, 전체 권한보다 우선합니다.

사용자 권한과 컴퓨터 권한은 우선순위가 동일합니다. 우선순위는 시스템 설정 섹션에서 조정이 가능합니다. 더 자세한 내용은 '14.8.1 Endpoint Protector 권한'을 참조하시기 바랍니다.



예제

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.

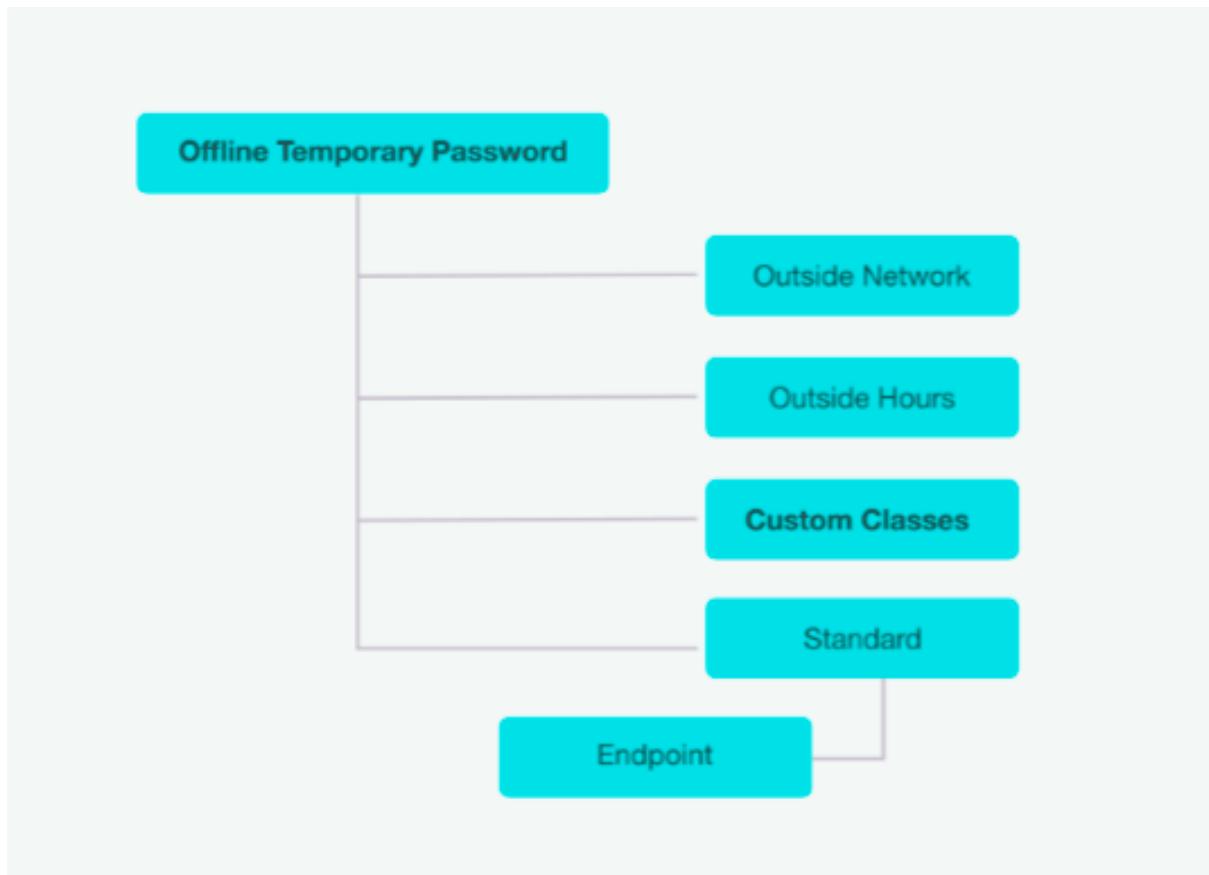
3.9.1. 매체 제어 정책 우선순위

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.



4. 콘텐츠 인식 보호

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.

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

4.1. 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.

정보

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

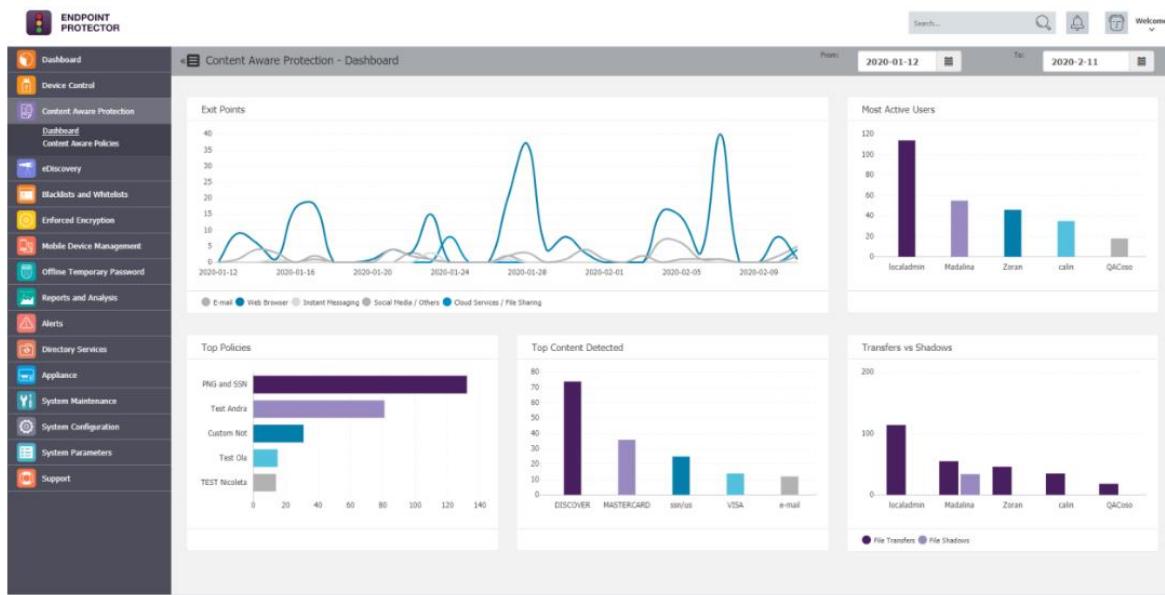
The screenshot displays the 'Content Aware Protection - Activation' page within the Endpoint Protector web interface. The left sidebar lists several modules: Dashboard, Device Control, Content Aware Protection (which is currently selected), eDiscovery, Blacklists and Whitelists, Enforced Encryption, Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, and Appliance. The main content area is titled 'Activate Content Aware Protection' and contains a section for 'Endpoint Protector Content Aware Protection'. It includes a note that the Endpoint Protector Client version 4.3.0.0 or higher is required for Content Aware Protection. Below this, there's a 'Live Update Server Information' section with fields for Company (CoSoSys), Administrator (Admin), E-mail (aaa@bbb.cc), and Phone (+123123). A large blue 'Enable' button is at the bottom of this section. At the very bottom of the page, there's a copyright notice for CoSoSys Ltd. and a version number (Version 5.1.0.0).

참고

콘텐츠 인식 보호 모듈은 매체 제어 또는 eDiscovery 모듈과 분리가 되어 있습니다. 각각 라이선스가 필요합니다.

4.2. 대시보드

이 섹션은 콘텐츠 인식 보호 모듈과 관련된 정보를 그래프과 차트의 형태로 빠르게 현황을 볼 수가 있도록 제공합니다. 최근의 파일 전송, 차단된 파일 종류, 가장 활동적인 정책 내용, 가장 많이 차단된 응용프로그램, 가장 활동적인 사용자, 최근 알림 및 정책 적용이 없는 컴퓨터 및 사용자와 같은 정보를 보여줍니다.



4.3. 콘텐츠 인식 정책

콘텐츠 인식 정책은 민감한 콘텐츠 탐지에 대한 규칙 설정이고 이 규칙들은 선택된 각 객체들 (사용자, 컴퓨터, 그룹, 구분)에 대한 파일 전송 관리를 합니다. 콘텐츠 인식 정책은 4가지 요소로 구성되어 있습니다.

- **OS 유형:** Windows, macOS, Linux 중 어느 OS 유형에 적용할 것인지 정의합니다.
- **정책 액션:** 민감한 콘텐츠 전송의 보고만과 차단 및 보고로 수행하는 액션의 유형을 정의합니다.
- **정책 유형:** 정책 유형 정의 – 표준, 근문 시간 또는 외부네트워크
- **엔드포인트:** 모니터링하는 전송 목적지를 설정합니다.

- 정책 거부목록 및 허용목록:** 탐지되는 특정 콘텐츠를 지정합니다. 파일 종류 필터, 개인정보 콘텐츠 필터, 사용자 키워드 필터, 도메인 허용목록, 파일 허용목록, 정규식, HIPAA, DPI (Deep Packet Inspection) 등이 포함됩니다.

예제

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 보고를하도록 정책을 설정할 수 있습니다.

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.

참고

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

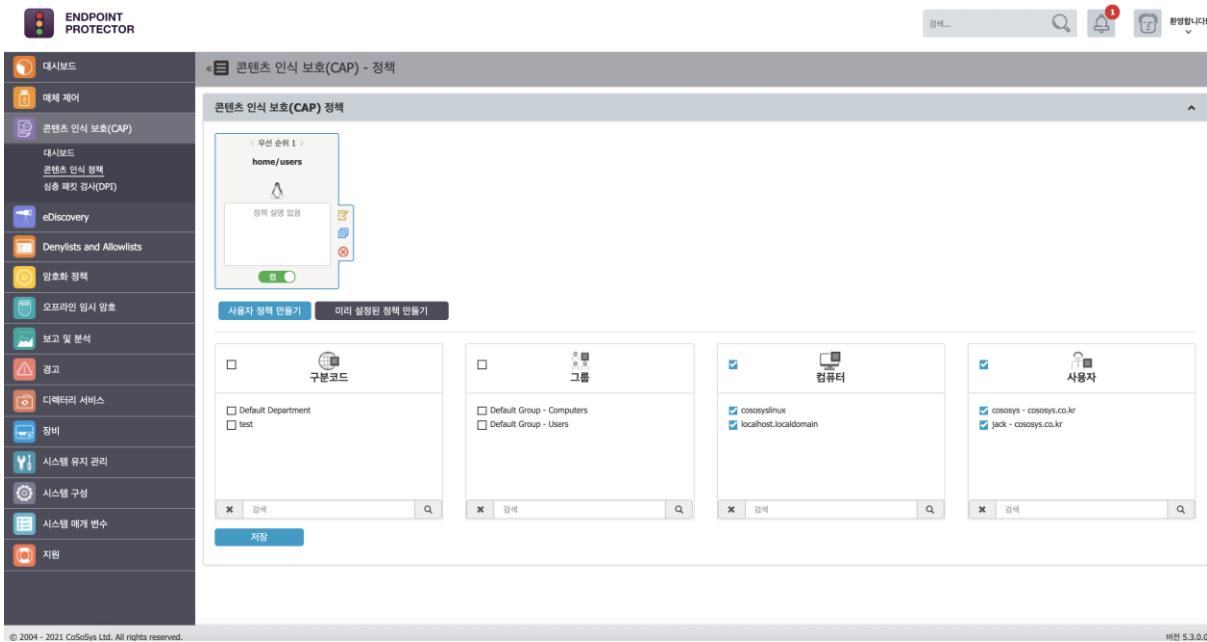
정보

매체 제어 정책과 똑같이 콘텐츠 인식 보호 정책은 회사 네트워크에서 벗어난 후에도 컴퓨터를 계속 보호합니다.

콘텐츠 인식 정책은 오프라인 상황에서도 컴퓨터의 에이전트가 민감한 콘텐츠를 계속 보호합니다.

4.3.1. 콘텐츠 인식 정책 만들기

관리자는 “콘텐츠 인식 보호(CAP) > 콘텐츠 인식 정책” 섹션에서 콘텐츠 인식 정책을 쉽게 만들고 관리할 수 있습니다.



새로운 정책은 정책 새로 만들기 아이콘을 클릭해서 만들 수 있습니다. 존재하는 정책은 그 정책 아이콘을 더블 클릭하면 편집할 수 있습니다.

정보

원하는 정책을 먼저 선택해야 편집, 복사, 삭제 옵션을 사용할 수 있습니다.

팁

하나 또는 그 이상의 콘텐츠 인식 정책은 같은 컴퓨터, 사용자, 그룹, 구분에 적용될 수 있습니다. 적용된 규칙들 사이에 충돌을 피하기 위해서 왼쪽에서 오른쪽 순서로 정책의 우선 순위를 설정합니다. 가장 왼쪽의 정책은 가장 높은 우선 순위를 가지고 반대로 오른쪽은 가장 낮은 우선 순위가 됩니다. 하나 또는 그 이상 정책의 우선 순위를 변경하는 것은 정책 아이콘의 화살표를 왼쪽 또는 오른쪽을 클릭해서 원하는 우선 순위로 가져가면 됩니다.

새로운 정책을 만들 때 정책 정보 (OS 유형, 정책 이름 및 설명), 정책 거부목록, 정책 허용목록, 정책 객체들 (구분, 그룹, 컴퓨터)는 반드시 선택이 되어야 합니다.

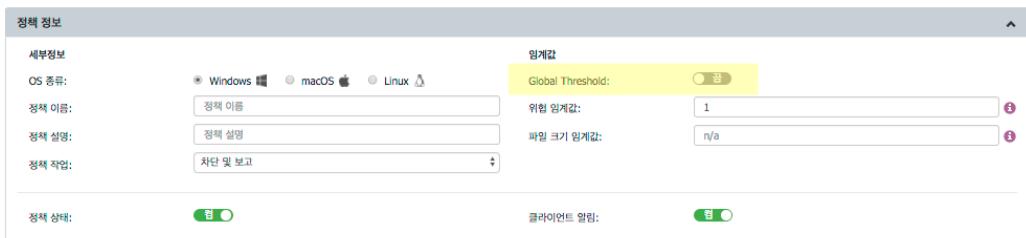
정책 상태는 민감한 콘텐츠가 포함된 모든 데이터 전송을 보고만 또는 차단 및 보고로 설정할 수 있습니다.

팁

초기에는 데이터 전송 차단이 아니라 탐지를 위한 보고만 옵션 사용을 권장합니다. 이 방법으로 사용자는 활동의 제약이 없어지므로 네트워크를 통해서 데이터가 사용되는 현황을 더 잘 파악할 수 있습니다.

전체 임계값을 사용할 수 있습니다.

- 전체 임계값 (ON 또는 OFF)
- 만약 전체 임계값이 OFF로 설정되어 있으면 일반 임계값으로 동작합니다.

**예제**

일부 인터넷 브라우저 유형에 주민등록번호 전송 차단 및 보고 정책을 설정했다고 가정합니다. 임계값 4 설정은 4개 이상의 주민등록번호가 포함된 콘텐츠의 모든 전송을 차단하지만 3개의 주민등록번호가 포함된 콘텐츠 전송은 차단하지 않습니다.

전체 임계값 옵션을 사용하면 4개 이상의 서로 다른 유형의 개인정보가 포함된 콘텐츠 전송을 차단합니다. 예를 들어 2개의 주민등록번호와 2개의 전화번호는 차단합니다. 반면에 일반 임계값 4는 차단하지 못합니다.

팁

임계값 옵션은 개인정보 콘텐츠 필터, 사용자 키워드 필터, 정규식에서만 적용됩니다. 일반적으로 임계값을 사용하는 차단 및 보고 정책이 보고만 정책보다 더 높은 우선 순위에서 사용되는 것을 권장합니다.

- 파일 크기 임계값

파일 크기 임계값은 위에서 언급된 각각 및 전체 임계값과는 관련이 없습니다. 파일 크기 임계값은 파일 전송의 차단 및 보고를 시작하는 크기(MB)로 정의 됩니다.

니다.

파일 크기 임계값:



파일 크기 임계값 사용은 반드시 값이 0보다 커야합니다.

파일 크기 임계값 사용하지 않음은 값이 0이거나 값이 없어야 합니다.

참고

파일 크기 임계값을 설정하면 정책 내에 파일 유형 또는 키워드 정책에 상관없이 모든 정책에 적용됩니다. 파일 크기 임계값은 양수가 사용되어야 합니다.

정보

특정 응용프로그램 및 OS에 따라서 제한적으로 적용될 수 있습니다.

- 파일 크기 임계값이 일치하는 경우 정책 적용

이 기능을 사용하면 정책은 임계값과 결합하여 적용됩니다. 거부목록에 체크된 모든 것이 임계값을 고려하여 차단될 것입니다.

참고

이 설정은 파일 이름과 파일 위치에는 적용되지 않습니다.

아래는 제어되는 전송으로 모니터링하는 엔드포인트입니다.

- 응용프로그램

웹 브라우저	이메일	엔스턴트 메시징	파일 공유	미디어 / 기타
<input type="checkbox"/> Internet Explorer <input type="checkbox"/> Chrome <input type="checkbox"/> Mozilla Firefox <input type="checkbox"/> Opera <input type="checkbox"/> Safari <input type="checkbox"/> AOL Desktop 9.6 <input type="checkbox"/> Aurora Firefox <input type="checkbox"/> FrontMotion Firefox <input type="checkbox"/> K-Meleon	<input type="checkbox"/> Outlook (Attachments) <input type="checkbox"/> Outlook (Body) <input type="checkbox"/> Mozilla Thunderbird <input type="checkbox"/> Mozilla Thunderbird (Body) <input type="checkbox"/> IBM Lotus Notes (Attachments) <input type="checkbox"/> IBM Lotus Notes (Body) <input type="checkbox"/> Windows Live Mail <input type="checkbox"/> GroupWise Client <input type="checkbox"/> Outlook Express	<input type="checkbox"/> ICQ <input type="checkbox"/> AIM <input type="checkbox"/> Skype <input type="checkbox"/> Windows Live Messenger <input type="checkbox"/> Yahoo! Messenger <input type="checkbox"/> Gain <input type="checkbox"/> HanbitTalk <input type="checkbox"/> Pidgin <input type="checkbox"/> Trillian	<input type="checkbox"/> Google Drive Client <input type="checkbox"/> iCloud Drive <input type="checkbox"/> uTorrent <input type="checkbox"/> BitComet <input type="checkbox"/> Daum Cloud <input type="checkbox"/> KT Ollleh uCloud <input type="checkbox"/> Naver N Drive <input type="checkbox"/> Azureus <input type="checkbox"/> OneDrive (Skydrive)	<input type="checkbox"/> EasyLock <input type="checkbox"/> Windows DVD Maker <input type="checkbox"/> ALFTP <input type="checkbox"/> ADB <input type="checkbox"/> AI-Drive <input type="checkbox"/> AnyDesk <input type="checkbox"/> Blizz <input type="checkbox"/> FileZilla <input type="checkbox"/> GoToAssist

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

- 인스턴트 메시징 (예> Skype, Pidgin, Google Talk 등)
- 파일 공유 (예> Google Drive Client, iCloud, Dropbox, DC++ 등)
- 기타 (예> iTunes, Total Commander, GoToMeeting 등)

참고

Adobe Flash Active X를 사용하는 사이트를 차단하려면 반드시 웹 브라우저 범주에서 Adobe Flash Player를 체크해야 합니다.

정보

제어되는 응용프로그램의 완전한 목록은 Endpoint Protector 사용자 인터페이스에서 직접 확인 할 수 있습니다.

- 저장 장치 (시스템 매개 변수 > 장치 유형 > 콘텐츠 인식 보호(CAP) 에서 지원하는 모든 장치 유형 목록을 볼 수 있습니다.)

참고

Windows에서 휴대용 저장 장치의 파일 전송은 모두 모니터링 됩니다.

정보

제어되는 응용프로그램의 완전한 목록은 Endpoint Protector 사용자 인터페이스에서 직접 확인 할 수 있습니다.

- 네트워크 공유

정보

Mac 네트워크 공유에서 Endpoint Protector 보고만 정책으로 모든 이벤트를 보고합니다. 로컬 공유의 차단 및 보고 정책은 제어되는 저장 장치 유형 및 제어되는 응용프로그램으로 차단됩니다.

- 씬 클라이언트
- 클립보드 (복사 및 붙여넣기 또는 잘라내기 및 붙여넣기를 통한 모든 콘텐츠 캡쳐를 참조 바랍니다.)

정보

클립보드 기능은 세분화 시켜서 사용할 수 있습니다.

- 클립보드: 감시되는 응용프로그램에 관계없이 컴퓨터에 적용됩니다.
- 정책에 정의된 소스코드 탐지
- 감시되는 응용프로그램들에 붙여 넣기 제한 적용: 감시되는 응용프로그램에만 붙여 넣기가 제한됩니다.
- 아래 응용프로그램들로 붙여 넣기 제한 확장: Word, Excel, Notepad++ 등과 같이 정의된 응용 프로그램에 대해서 붙여 넣기가 제한됩니다.

- 프린트 스크린 (스크린 캡쳐 옵션을 참조 바랍니다.)
- 프린터 (로컬 및 네트워크 공유 프린터를 참조 바랍니다.)

사용되는 거부목록은 아래와 같습니다.

- 파일 유형

팁

대부분의 프로그램 파일은 실제로 .txt 파일이기 때문에 원하지 않은 결과를 피하기 위해서 이 파일 유형을 선택할 때 더 주의 하기를 권장합니다.

- 소스 코드

팁

N-gram 기반 탐지 방법은 이러한 파일 유형의 정확성을 높이는데 사용됩니다. 그러나 다양한 소스 코드가 비슷하게 연결되어 있어서 (예: C, C++ 등) 세부적인 구분 체크가 필요합니다. 이러한 점을 더 쉽게 다루기 위해서 Endpoint Protector는 자동으로 연관성을 가진 유형을 함께 마크합니다.

정보

심층 패킷 검사를 사용할 때 Git를 감시하는 확장된 방법을 사용할 수 있습니다. 제한된 응용프로그램으로 Git가 선택되어 있으면 Git 관련 액션 (fetch, clone, push, pull)은 Git 응용프로그램 사용과 관계없이 차단됩니다. 이 활동을 Git를 완전하게 차단하는 것입니다.

그러나 심층 패킷 검사 허용목록에 특정 도메인과 연결된 특정 Git 사용을 허용합니다. (예: internalgiit.mydomain.com)

참고

모든 Git 트래픽은 암호화됩니다. 그러므로 특정 도메인 허용은 콘텐츠 또는 다른 제한 정책과 관계없이 모든 파일 전송을 허용합니다.

참고

Git가 제한된 응용프로그램으로 선택되면 Endpoint Protector 클라이언트 알림과 로그는 Git 관련 액션 (fetch, clone, push, pull)에 관련해서 생성되지 않습니다.

- 개인 정보 콘텐츠 필터

팁

개인정보 콘텐츠 필터 목록은 대부분 특정 국가 (예: 호주, 캐나다, 독일, 대한민국, 영국, 미국 등)의 패턴을 가지고 있습니다. 너무나 많은 로그 및 잠재적 과탐을 줄이기 위해서 해당 지역의 패턴만 사용하시기 바랍니다.

- 사용자 키워드 필터
- 파일 이름
- 파일 위치
- 정규식
- HIPAA
- URL 및 도메인

사용되는 허용목록은 아래와 같습니다.

- MIME 유형
- 허용되는 파일
- 파일 위치
- 네트워크 공유
- 이메일 도메인
- URL 주소
- 심층 패킷 검사

정보

거부목록 및 허용목록의 상세한 정보는 섹션 “6 거부목록 및 허용목록”을 참조하시기 바랍니다.

참고

콘텐츠 인식 정책은 심지어 에이전트가 설치된 컴퓨터가 사내 네트워크와 연결이 끊어져도 전송되는 민감한 데이터에 대해서 보고만 / 차단 및 보고 정책을 계속 수행합니다. 로그는 Endpoint Protector 클라이언트에 저장되고 사내 네트워크와 연결되면 바로 서버로 전송됩니다.

만들어진 정책의 마지막 단계는 적용하려는 객체를 선택하는 것입니다. 아래의 객체를 선택할 수 있습니다.

- 구분
- 그룹
- 컴퓨터
- 사용자

팁

컴퓨터, 사용자, 그룹 또는 구분이 콘텐츠 인식 정책에 적용되고 이 정책을 클릭하면 적용된 네트워크에 응답하는 객체는 하이라이트 처리가 될 것입니다.

4.3.2. 미리 설정된 정책

두 번째 옵션은 미리 설정된 정책을 사용하는 것입니다. 관리자는 Windows 및 macOS에 기본으로 보고 및 차단 정책으로 미리 설정된 정책 두 가지 목록을 사용할 수 있습니다. 관리자는 정책 설명을 읽고 원하는 정책을 선택한 다음 아래에 “정책 만들기” 버튼을 이용하여 정책을 만들 수 있습니다.

이 정책들은 이름에 따라 각각의 임계값이 부여되어 있습니다. 이름 및 임계값 열에서 확인 할 수 있습니다.

정책 이름	설명	임계값
파일 종류 - 아카이브 파일	모든 목적지로 압축 파일 전송을 차단	3 전체
파일 종류 - 그레픽 파일	모든 목적지로 그레픽 파일 전송을 차단	3 전체
파일 종류 - 오피스 문서 파일	모든 목적지로 오피스 파일의 전송을 차단	3 전체
파일 종류 - 기타 파일	모든 목적지로 기타 파일의 전송을 차단	3 전체
파일 종류 - 프로그램 소스 파일	모든 목적지로 프로그래밍 파일의 전송을 차단	3 전체
파일 종류 - 미디어 파일	모든 목적지로 미디어 파일의 전송을 차단	3 전체
HIPAA - 진단 용어	모든 목적지로 ICD 코드 및 진단 용어 전송을 차단	5 전체
HIPAA - 개인 식별 정보	모든 목적지로 ICD 코드, 진단 용어 및 개인 식별 정보 전송을 차단	10 전체
HIPAA - 개인 식별 정보	모든 목적지로 개인 식별 정보 전송을 차단	5 전체
HIPAA - 제약 회사	모든 목적지로 FDA 등록 제약 회사 이름 전송을 차단	5 전체

4.3.3. 차단 및 조치 정책

차단 및 조치 정책은 프리미엄 라이선스로만 사용할 수 있는 콘텐츠 인식 정책의 범주입니다.

이 정책은 최종 사용자가 정당한 사유를 사용하여 콘텐츠 인식 위협을 해결하는 기회를 제공합니다.

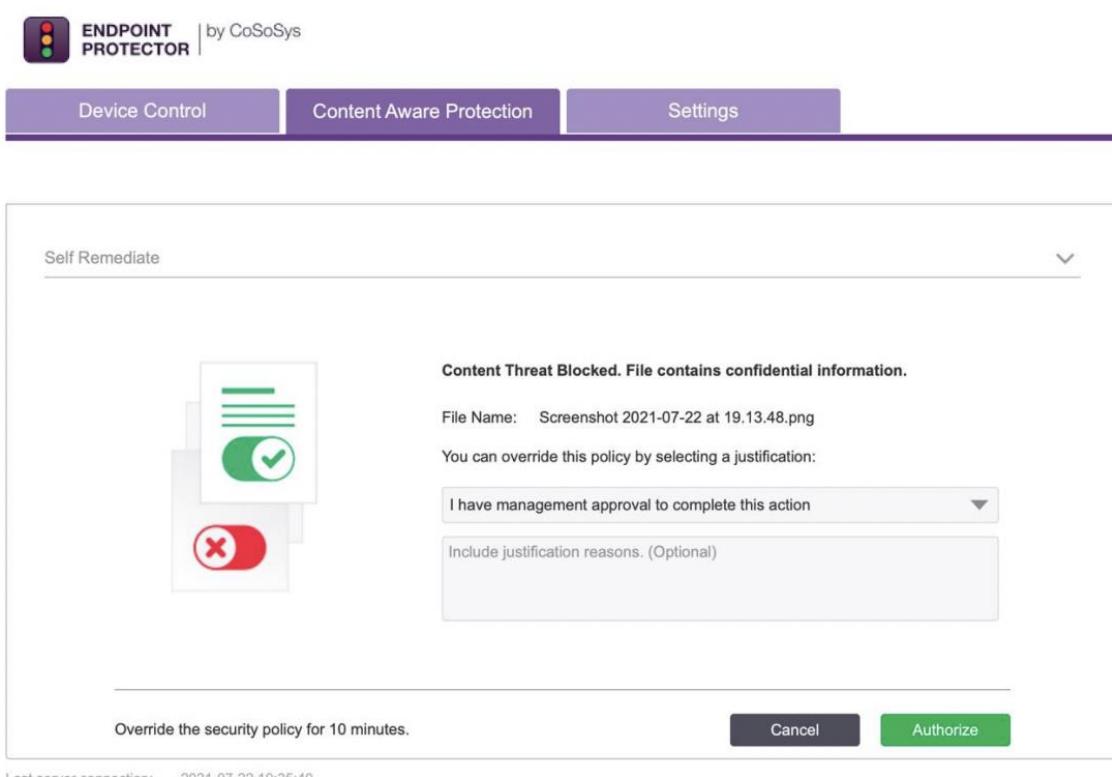
'관리자는 콘텐츠 인식 보호 섹션 -> 콘텐츠 인식 정책 만들기 -> 정책 작업 -> 차단 및 조치'에서 쉽게 콘텐츠 인식 정책의 차단 및 조치 정책을 설정할 수 있습니다.

콘텐츠 인식 위협이 일어나면 최종 사용자는 Endpoint Protector 알림 창의 콘텐츠 인식 탭에서 확인하거나 설정 섹션의 옵션에 따라 파일 알림으로 확인할 수 있습니다.

이 위협을 조치하기 위해서 최종 사용자는 콘텐츠 인식 보호 탭에서 원하는 조치가 필요한 파일을 선택해야 합니다.

The screenshot shows the Endpoint Protector application window. At the top, there is a logo for 'ENDPOINT PROTECTOR by CoSoSys'. Below the logo, there are three tabs: 'Device Control', 'Content Aware Protection' (which is highlighted in purple), and 'Settings'. A search bar with a magnifying glass icon is positioned above the main content area. The main content area has a table header with columns: 'File name', 'Threat', and 'Application'. Below the header, there is one row of data: 'Screenshot 2021-07-22 at 19.13.48.png', 'file-type', and 'com.apple....'. At the bottom of the main content area, there is a message: 'To authorize the data transfer, please Request Access from your administrator or click Self Remediate.' Below this message are two buttons: a blue 'Request Access' button and a green 'Self Remediate' button. At the very bottom of the window, there is a small note: 'Last server connection: 2021-07-22 19:38:42'.

그리고 나서 자가 조치 버튼을 누르고 정당한 사유를 선택하고 인가 버튼을 누릅니다.



이 기능의 추가적인 설정은 '시스템 매개 변수 -> 사용자 조치'에서 찾을 수 있습니다.

4.3.4. 다음 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

참고

정책을 만들 때 체크하지 않은 정보는 허용이 아니라 무시로 간주됩니다.

참고

DPI (Deep Packet Inspection) 기능은 도메인 허용목록 기반의 이메일 검사로 확장 되었습니다.

4.3.4. HIPAA 준수

HIPAA 탭의 옵션이 선택되면 콘텐츠 인식 보호 정책은 자동으로 HIPAA 정책이 됩니다. 사용 관련 옵션은 FDA 허용 목록 및 ICD 코드를 참조하시기 바랍니다.

HIPAA 정책은 반드시 주소, 전화 및 팩스 번호, 이메일 및 사용자 키워드 등 개인정보를 포함해야합니다. 이전 탭에서 확실하게 이 정보를 가져오세요.

FDA가 인정한 제약 회사들

FDA가 인정한 치료용 처방 약품 (일반 의약품)

ICD-10 코드들 및 진단 용어

ICD-9 코드들 및 진단 용어집

그러나 HIPAA 정책을 사용하려면 개인정보 콘텐츠 필터 및 사용자 키워드 필터를 또한 사용해야 합니다. 주민등록번호, 건강보험번호, 주소 등과 같은 개인정보를 자동으로 보고 또는 차단합니다.

내에 표시되는 개인 식별 정보가 포함되어 있습니다. 적절하게 선택되면 개인정보보호법, PCI DSS, GDPR 및 HIPAA와 같은 다양한 규정 및 규제를 준수하는 데 도움이 됩니다. 현실적으로 백화점은 정확성을 보장 할 수 없으며, *로 표시된 항목들은 과정 및 모판이 있을 것입니다.

신용카드

- AMEX
- Discover
- Maestro
- Diners (Carte Blanche)
- JCB
- VISA
- Diners
- Mastercard
- China UnionPay
- MIR

개인 식별 정보

- IBAN
- ISBN
- SWIFT
- 날짜
- 이메일

주소

- 미국
- 일본
- 독일
- 중국
- 캐나다
- 그리스
- 일본
- 스위스
- 사이프리스
- 헝가리
- 대한민국
- 우리나라
- 스위스
- 포르투갈
- 인도네시아
- 대만

주민등록번호

- 오스트리아
- 러시아
- 아일랜드
- 네덜란드
- 스페인
- 영국
- 캐나다
- 그리스
- 일본
- 폴란드
- 스웨덴
- 미국
- 사이프리스
- 헝가리
- 대한민국
- 우리나라
- 스위스
- 포르투갈
- 인도네시아 *
- 라트비아
- 노르웨이
- 싱가포르

ID

- 알바니아
- 칠레
- 에콰도르
- 독일
- 이스라엘
- 리투아니아
- 파루
- 불가리아
- 멕시코
- 프랑스
- 페루
- 그리스
- 이탈리아
- 말레이시아
- 폴란드
- 보라질
- 코모에
- 에스토니아
- 페루
- 아일랜드
- 카자흐스탄
- 맥시코
- 터키

권장하는 HIPAA는 HIPAA 탭 옵션 이외에 아래의 구성을 가지는 콘텐츠 인식 정책이 됩니다.

- 인식되는 모든 파일 유형 포함
- 미국의 모든 개인 정보 (주소, 전화번호/팩스, 사회보장번호) 포함
- IP4/6 인터넷 프로토콜 주소 선택

- URL 및 도메인 허용목록 옵션 체크

HIPAA 정책은 만들면 네트워크 내에서 더 제어를 잘하기 위해서 이 정책 하나 또는 일반 정책과 함께 사용할 수 있습니다. Windows, macOS, Linux 컴퓨터에서 사용이 가능합니다.



4.3.4.1. 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 있는 것을 알기 때문에 관리자는 아래와 같은 HIPAA 정책을 만들 수 있습니다.

The screenshot shows the 'Content Integrity Protection (CAP) - Policy Creation' screen in the Endpoint Protector application. The left sidebar includes options like Dashboard, Audit, CAP, eDiscovery, Denylists and Allowlists, and more. The main area has tabs for File Type, Source Code, Malicious Content, User Keyword, File Name, Regular Expression, HIPAA (selected), and Domain and URL.

Policy Denylists:

- File Type: FDA가 인정한 제약 회사들, FDA가 인정한 치료용 처방 약품 (일반 의약품)
- Source Code: ICD-9 코드들 및 진단 용어집
- Malicious Content: FDA가 인정한 치료용 처방 약품 (보편도)

Policy Allowlists:

Category	Item	Action
Group Code	구분코드	<input type="checkbox"/> Default Department, <input type="checkbox"/> test
Group	그룹	<input type="checkbox"/> Default Group - Computers, <input type="checkbox"/> Default Group - Users
Computer	컴퓨터	<input type="checkbox"/> DESKTOP-NHUFBCB1
User	사용자	<input type="checkbox"/> coscowsindows - DESKTOP-NHUFBCB1

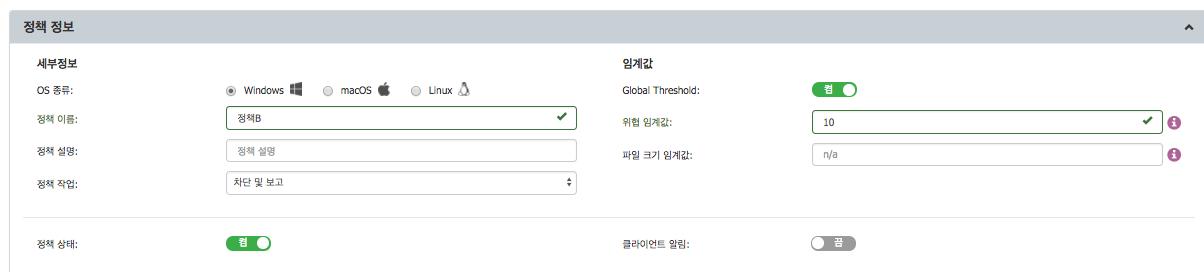
Buttons at the bottom include '저장' (Save) and '뒤로' (Back).

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).

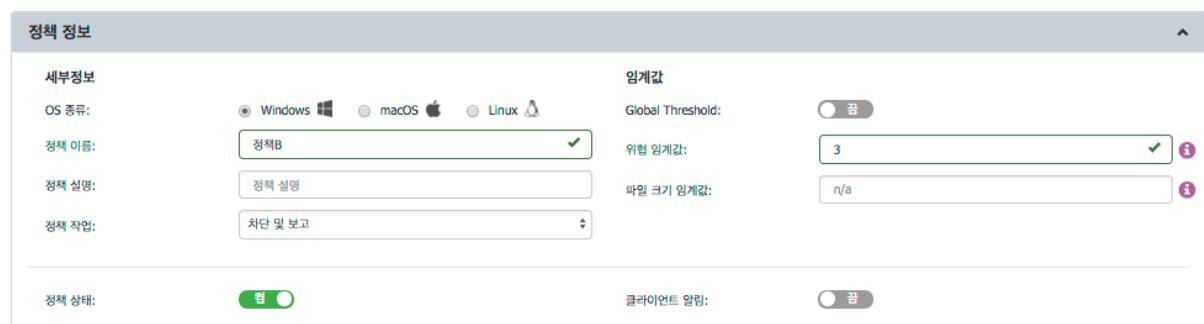
4.3.4.2. 사례 #2

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 전송 차단을 설정할 수 있습니다.



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



정보

앞에서 언급했지만 차단 및 보고 정책은 우선 순위가 보고만 정책보다 더 앞에 있어야 합니다.

4.4. 심층 패킷 검사(DPI)

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

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

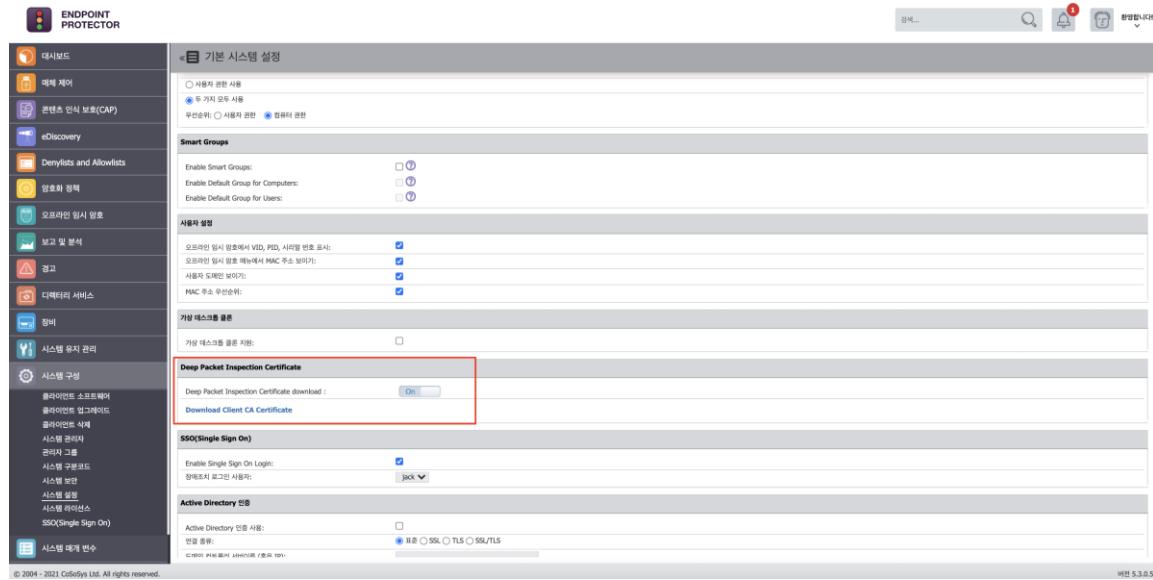
DPI 인증서가 Endpoint Protector 클라이언트를 위해 추가되면 DPI 검사는 macOS 11.0+ 에서만 동작합니다.

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

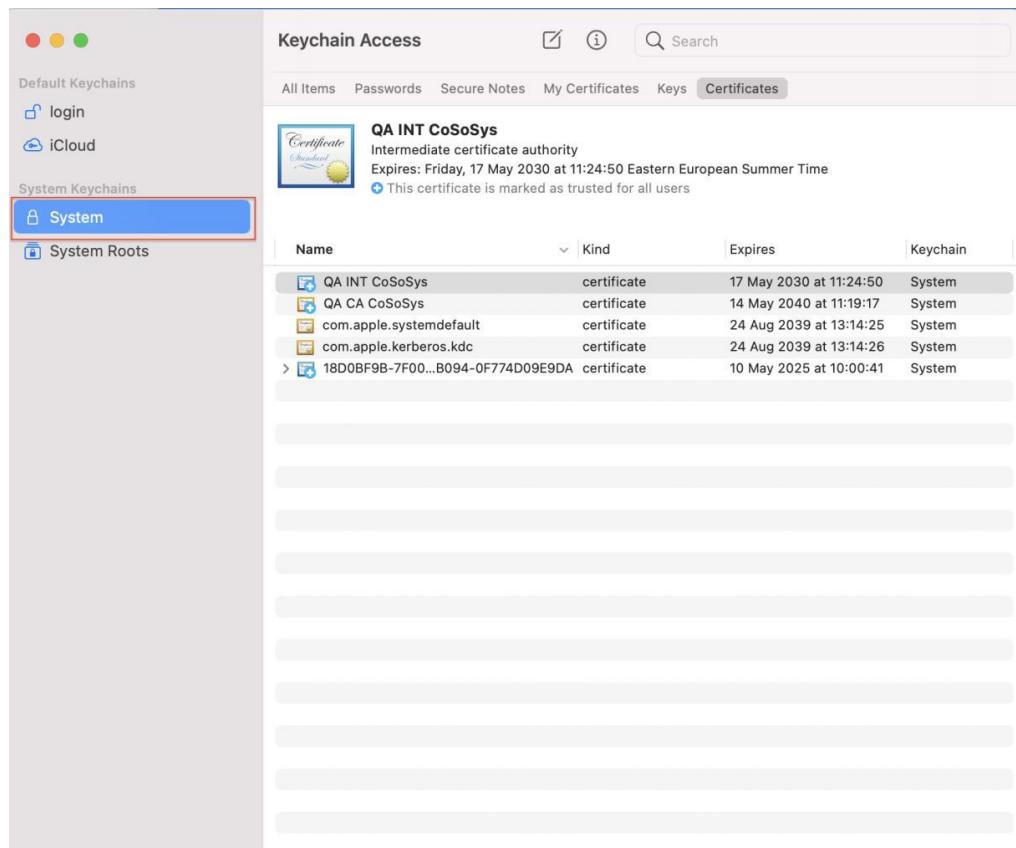
수동으로 추가하려면 아래 단계를 참조하시기 바랍니다:

- '시스템 구성 > 시스템 설정 > DPI 인증서'로 이동해서 CA 인증서를 다운로드합니다.

8.3 | Endpoint Protector | 사용 설명서

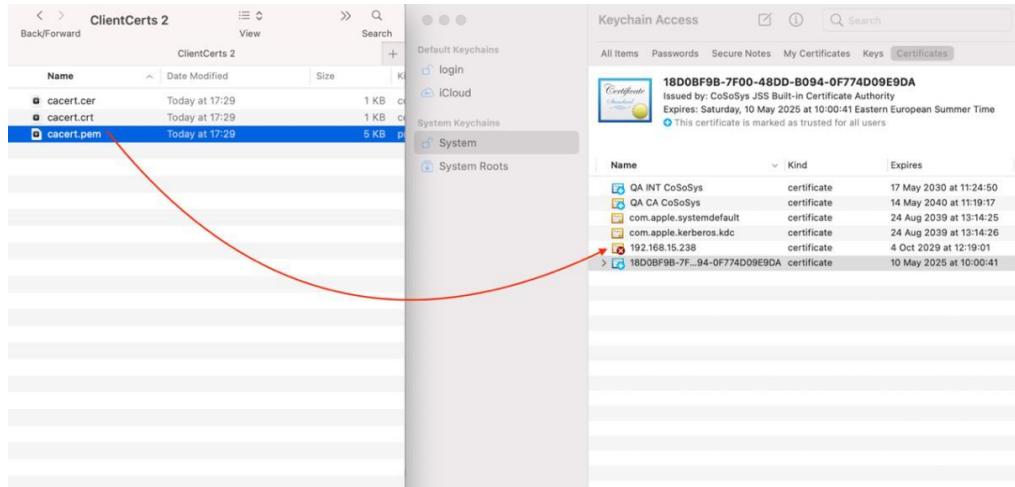


2. macOS에서 '키체인 접근' 응용프로그램을 열고 '시스템'을 선택합니다.

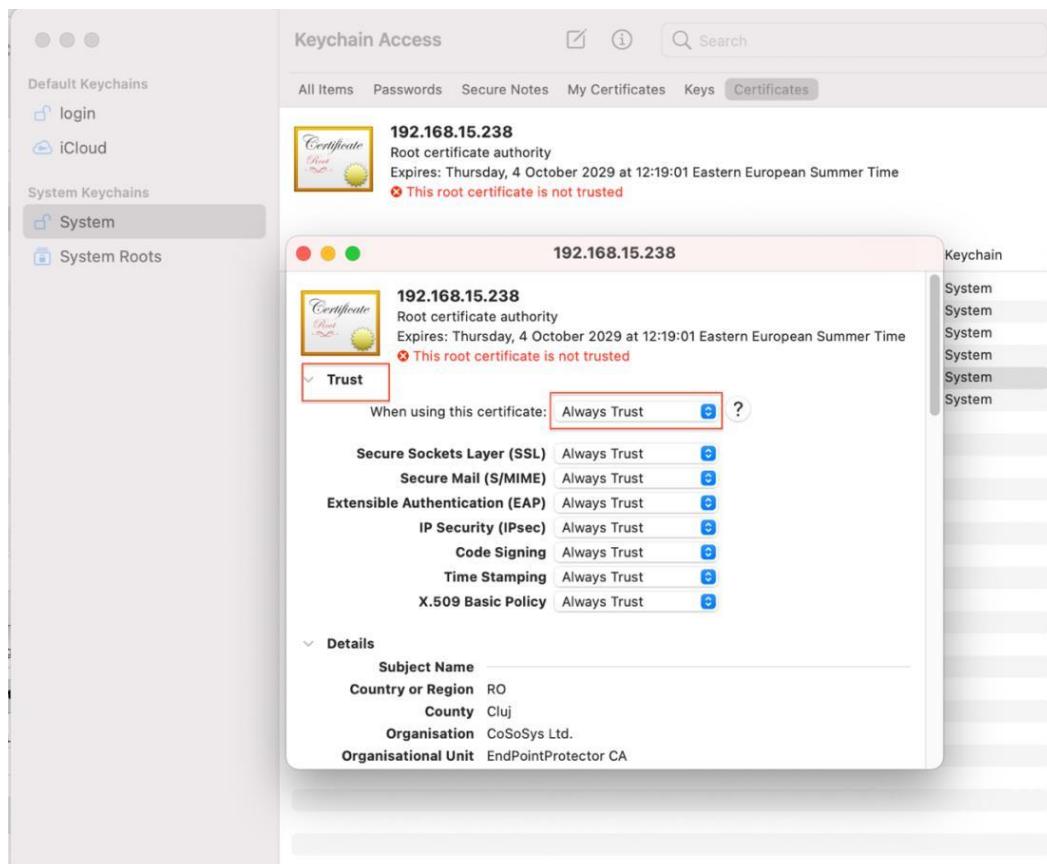


3. 다운로드한 ClientCerts 파일 압축을 해제합니다.

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 저장합니다.

4.4.1. 심층 패킷 검사(DPI) 포트 및 설정

이 섹션에서 관리자는 각 네트워크에 사용되는 포트와 감시되는 응용프로그램을 연계할 수 있습니다.

미리 정의된 포트	사용자 지정 포트
포트: 80 트래픽 유형: HTTP	사용자 지정 포트 사용: [Green Circle] (선택)
포트: 443 트래픽 유형: HTTPS	포트: [] 트래픽 유형: [HTTP] [+]
포트: 8080 트래픽 유형: Proxy	포트: [] 트래픽 유형: [HTTP] [-]
포트: 587 트래픽 유형: HTTP	포트: [] 트래픽 유형: [HTTP] [-]
포트: 465 트래픽 유형: SMTP	포트: [] 트래픽 유형: [HTTP] [-]
포트: 25 트래픽 유형: SMTP	포트: [] 트래픽 유형: [HTTP] [-]

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 보호정책으로 정의된 감시되는 응용프로그램이 연결되어 있다면 이 포트는 이 섹션에서 추가할 수 있습니다.

정보

텍스트 검사 설정을 켜면 Teams, Skype, Slack, Mattermost로 타이핑 되는 기밀 콘텐츠는 감시됩니다.

참고

텍스트 검사 설정은 또한 다음의 브라우저에도 적용됩니다: Google Spreadsheet, Facebook Post, Facebook Comment, Instagram Comment. 그러나 이러한 설정은 전체적으로 적용되고 DPI가 기본적으로 사용되어야 합니다.

피어 인증서 검증 설정은 관리자가 DPI 기능이 활성화 되어 있을 때 사용자가 접근하는 웹 사이트의 Endpoint Protector 인증서 검증을 사용하지 않는 가능성을 제공합니다.

참고

이 설정은 주의해서 변경해야 하며 웹 사이트 인증서를 검증하는 또 다른 네트워크 트래픽 검사 제품 (예: Secure Web Gateway Solution)이 있는 경우에만 사용해야 합니다.

예제

심층 패킷 검사와 피어 인증서 검증이 모두 켜져 있을 때 badssl.com 접근: "여러분의 연결은 비공개가 아닙니다." 그리고 다른 인증서 경고가 있습니다.

심층 패킷 검사 켜 그리고 피어 인증서 검증이 끄져 있을 때 badssl.com 접근: Endpoint Protector 클라이언트는 서버 인증서 검증을 하지 않고 브라우저는 사용자가 경고 없이 사이트를 방문하도록 허용합니다.

상황에 따른 예제 사용:

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.

4.4.2. 심층 패킷 검사(DPI) 응용프로그램

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

정보

DPI를 지원하는 응용프로그램은 오직 아래 목록에서만 가능합니다.

The screenshot shows the 'Endpoint Protector' software interface. On the left is a sidebar with various icons and menu items: 대시보드, 매체 제어, 콘텐츠 인식 보호(CAP), 대시보드, 콘텐츠 인식 정책, 심층 패킷 검사(DPI), eDiscovery, Denylists and Allowlists, 암호화 정책, 오프라인 임시 암호, 보고 및 분석, 경고, 디렉터리 서비스, 정비, 시스템 유지 관리, 시스템 구성, 시스템 매개 변수, 지원. The main area is titled '콘텐츠 인식 보호(CAP) - 심층 패킷 검사(DPI)' and contains a table titled '심층 패킷 검사(DPI) 응용프로그램'. The table has columns: 이름 (Name), 종류 (Type), OS 종류 (OS Type), DPI (DPI), and 작업 (Action). The table lists several applications: Microsoft Teams, Cloud Services / File Sharing, Mac, 사용 중지 (Blocked); Microsoft Teams, Cloud Services / File Sharing, Linux, 사용 중지 (Blocked); OneDrive for Business, Cloud Services / File Sharing, Mac, 사용 가능 (Allowed); OneDrive (Skydrive), Cloud Services / File Sharing, Mac, 사용 중지 (Blocked); OneDrive for Business, Cloud Services / File Sharing, Windows, 사용 중지 (Blocked); Microsoft Teams, Cloud Services / File Sharing, Windows, 사용 중지 (Blocked); OneDrive (Skydrive), Cloud Services / File Sharing, Windows, 사용 중지 (Blocked); Sparrow, E-mail, Mac, 사용 가능 (Allowed); Sparrow Lite, E-mail, Mac, 사용 가능 (Allowed); Sylphred, E-mail, Linux, 사용 가능 (Allowed). At the bottom of the table, it says '전체의 1 부터 10 까지 89 항목' (Total of 1 to 10 of 89 items) and has a page navigation bar from 1 to 9. The top right of the interface includes a search bar, a refresh button, a help button, and a '환영합니다' (Welcome) message.

참고

심층 패킷 검사 기능은 '매체 제어 > 설정 (전체, 그룹, 컴퓨터 등)'에서 활성화해야 합니다.
더 자세한 내용은 '3.6.2 전체 설정'을 참조하시기 바랍니다.

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

5.1. 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.

정보

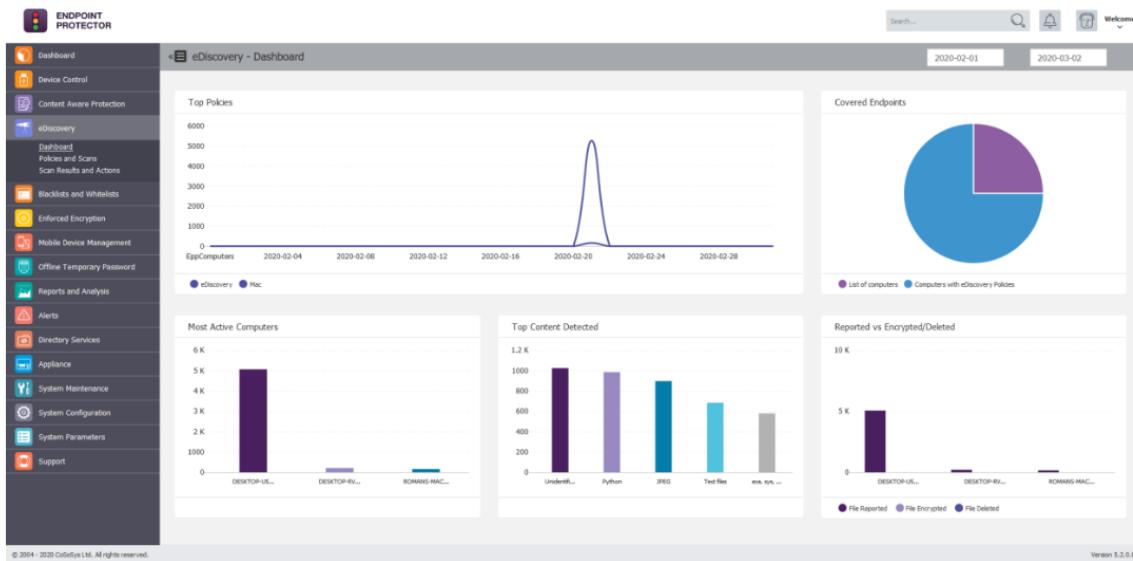
연락처 정보는 Live Update 서버가 정확하게 구성되고 eDiscovery 모듈이 성공적으로 사용되는지 확인 목적으로만 사용됩니다.

참고

eDiscovery 모듈은 매체 제어 또는 콘텐츠 인식 보호 모듈과 분리되어 있어서 별도의 라이선스가 필요합니다.

5.2. 대시보드

이 섹션은 eDiscovery 모듈에 관련된 그래프과 차트 형태로 빠르게 보여줍니다.



5.3. eDiscovery 정책 및 검색

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

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

정보

eDiscovery 정책을 만들면 원하는 eDiscovery 검색 유형을 선택해야 합니다.

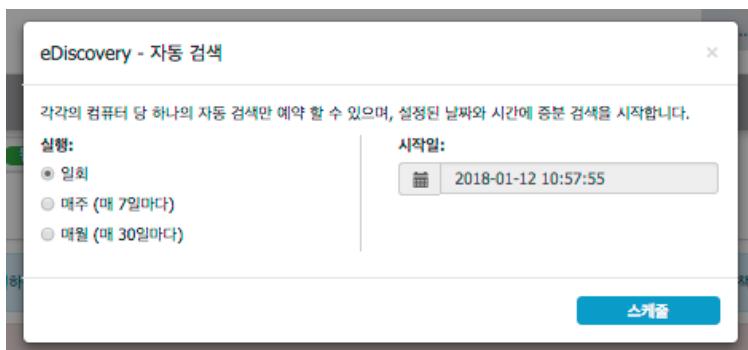
eDiscovery 검색은 정책에서 설정하고 데이터 디스커버리 시작할 때 정의됩니다. 아래 검색을 참조 바랍니다.

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

팁

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 원활 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 스캔을 정지하고 모든 로그를 삭제할 때 사용합니다.

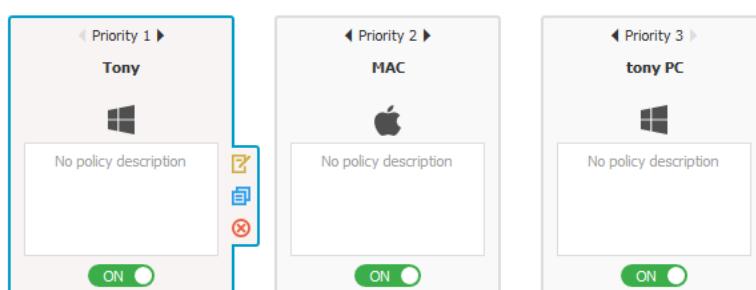
5.3.1. eDiscovery 정책 및 검색 만들기

관리자는 “eDiscovery > 정책 및 검색”에서 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.

정보

정책 수정, 복사, 삭제 옵션은 원하는 정책을 선택한 후에 사용 가능합니다.



새로운 정책을 만들 때 정책 정보 (예> OS 유형, 정책 이름, 정책 설명), 정책 거부목록, 정책 허용목록, 정책 객체 (구분, 그룹, 컴퓨터)를 선택해야 합니다.

아래와 같이 임계값을 사용할 수 있습니다.

- 위협 임계값에서 중단
- 위협 임계값
- 파일 크기 임계값

정보

임계값의 더 자세한 정보는 Endpoint Protector 사용자 인터페이스에서 바로 찾을 수 있습니다.

거부목록을 다음과 같이 사용할 수 있습니다.

- 파일 유형

팁

대부분의 프로그래밍 파일은 실제로 .txt 파일이기 때문에 원하지 않는 검색을 피하려면 파일 유형을 더 신중하게 선택하시기 바랍니다.

- 소스 코드

팁

N-gram 기반 탐지 방법은 이러한 파일 유형의 정확성을 높이는데 사용됩니다. 그러나 다양한 소스 코드가 비슷하게 연결이 되어 있어서 (예: C, C++ 등) 세부적으로 구분 체크가 필요합니다. 이러한 부분을 더 쉽게 만들기 위해서 Endpoint Protector는 연관성 있는 소스 코드를 자동으로 마킹합니다.

- 개인 정보 콘텐츠

팁

개인 정보 항목의 대부분은 국가 유형을 따릅니다 (예: 호주, 캐나다, 독일, 대한민국, 영국, 미국 등). 과탐을 줄이기 위해서 지역 또는 국가 유형에 적용되는 여권 번호만 사용할 수 있습니다.

- 사용자 키워드 콘텐츠
- 파일 이름
- 정규식
- HIPAA

허용 목록은 다음과 같이 사용할 수 있습니다.

- MIME 유형
- 허용된 파일

정보

거부 목록 및 허용 목록의 자세한 정보는 '6 거부 목록 및 허용 목록'을 참조 바랍니다.

eDiscovery 정책을 만든 후에 검색 액션을 선택할 수 있습니다 – 전체 검색 시작, 증분 검색 시작, 중단, 검색 중지 및 로그 삭제.

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.

5.4. 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.

The screenshot shows the Endpoint Protector software interface. The left sidebar contains navigation links such as Dashboard, Audit Log, System Health (CAP), eDiscovery (selected), File Types and Search, Search Results, and more. The main area is titled 'eDiscovery - 검색 결과 및 작업' (eDiscovery - Search Results and Tasks). It displays a table of search results with columns for Computer, Type, Location Type, Location Path, Address, Creation Time, Current Status, Last Task Status, Task Status, and Task. The table lists five entries for 'eDiscovery' type, word search, on 'JACK-WIN10' computer, with various status and task details. At the bottom, there are buttons for 'Print Selection' and 'Next'.

컴퓨터	유형	위치 유형	위치 경로	주소	발행된 시간	현재 상태	마지막 작업	작업 상태	작업
JACK-WIN10	eDiscovery	word	coseosyscoseosy11	C:/Users/jack/Desktop/eDiscovery/Test/eD01.txt	2017-06-14 18:25:23	실행됨	대상에서 실행	완료됨	
JACK-WIN10	eDiscovery	word	coseosyscoseosy11	C:/Users/jack/Desktop/eDiscovery/Test/eD02.txt	2017-06-14 18:25:23	실행됨	대상에서 알트파일 처리	완료됨	
JACK-WIN10	eDiscovery	word	coseosyscoseosy11	C:/Users/jack/Desktop/eDiscovery/Test/eD04.txt	2017-06-14 18:25:23	보고됨	n/a	n/a	
JACK-WIN10	eDiscovery	word	coseosyscoseosy11	C:/Users/jack/Desktop/eDiscovery/Test/eD03.txt	2017-06-14 18:25:23	보고됨	n/a	n/a	
JACK-WIN10	eDiscovery	word	coseosyscoseosy11	C:/Users/jack/Desktop/eDiscovery/Test/eD05.txt	2017-06-14 18:25:23	보고됨	n/a	n/a	

四

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

eDiscovery 검색

검색

결과 10 | 정렬

정렬	OS 종류	검색 유형	검색 범위	검색 상태	시작 시간	발견된 파일	작업
JACK-DESKTOP	eDiscovery	Windows	수동	진행 중인	2017-06-14 12:48:49	5	<ul style="list-style-type: none">Start clean scanStop manual scanStop scanStop scan and clear logsFind expected file

페이지 1 총 1 총 1 항목

수동 관리 | 현재 경지 볼 세부

5.4.1. 검색 결과 보기 및 조치 하기

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

컴퓨터	정책	설치된 유형	설치된 항목	파스	발견된 시간	현재 상태	마지막 작업	작업 상태	작업
JACK-WIN10	eDiscovery	word	cososyccosy11	C:/Users/jackj/Desktop/eDiscovery/Test/eD01.txt	2017-06-14 18:25:23	삭제됨	대상에서 삭제	삭제	Delete on target
JACK-WIN10	eDiscovery	word	cososyccosy11	C:/Users/jackj/Desktop/eDiscovery/Test/eD02.txt	2017-06-14 18:25:23	복호화됨	대상에서 암호화 해제	복호화됨	Decrypt on target
JACK-WIN10	eDiscovery	word	cososyccosy11	C:/Users/jackj/Desktop/eDiscovery/Test/eD04.txt	2017-06-14 18:25:23	복구됨	n/a	복구됨	Restore on target
JACK-WIN10	eDiscovery	word	cososyccosy11	C:/Users/jackj/Desktop/eDiscovery/Test/eD03.txt	2017-06-14 18:25:23	복구됨	n/a	복구됨	Restore on target
JACK-WIN10	eDiscovery	word	cososyccosy11	C:/Users/jackj/Desktop/eDiscovery/Test/eD05.txt	2017-06-14 18:25:23	복구됨	n/a	복구됨	Restore on target

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

6. 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.

참고

일부 거부목록 및 허용목록은 OS와 연관이 있습니다 (예: 이메일 도메인 및 URL 이름은 Windows에서만 사용 가능합니다.). 또는 두 모듈에서 모두 사용할 수 없습니다.

6.1. 파일 유형 거부목록

Endpoint Protector의 기능적인 콘텐츠 검사는 여러 파일 유형을 확인 할 수 있습니다. Endpoint Protector 업데이트에서 사용 가능한 목록을 확장하기 때문에 파일 유형은 계속해서 추가됩니다. 관리자는 콘텐츠 인식 보호 또는 eDiscovery 정책 스캔의 파일 유형을 정의 할 수 있지만 지원하는 파일 유형 목록을 직접 확장할 수는 없습니다. 미리 정의된 목록 때문에 관리자는 정책의 파일 유형 콘텐츠 탭에서 원하는 파일 유형을 선택해야 합니다. 이러한 과정은 이미 앞에서 자세하게 다루었습니다.

파일 종류	소스 코드	미리 정의된 콘텐츠	사용자 키워드	파일 이름	규칙	HIPAA	도메인 및 URL
<small>정액 설정에 따라서, 이 옵션을 선택하면 아래에 나열된 파일 종류들이 자동으로 보고만 혹은 차단 및 보고 됩니다.</small>							
그림 파일							
<input type="checkbox"/> JPEG	<input type="checkbox"/> PNG	<input type="checkbox"/> GIF	<input type="checkbox"/> ICO				
<input type="checkbox"/> BMP	<input type="checkbox"/> TIFF	<input type="checkbox"/> GEM	<input type="checkbox"/> COREL PHOTO-PAINT				
<input type="checkbox"/> CORELDRAW	<input type="checkbox"/> DJV	<input type="checkbox"/> EPS	<input type="checkbox"/> ADOBE ILLUSTRATOR				
<input type="checkbox"/> ADOBE INDESIGN	<input type="checkbox"/> BPF	<input type="checkbox"/> PSD					
오피스 파일							
<input type="checkbox"/> 워드	<input type="checkbox"/> 엑셀	<input type="checkbox"/> POWERPOINT	<input type="checkbox"/> PDF				
<input type="checkbox"/> INFOPATH	<input type="checkbox"/> OUTLOOK	<input type="checkbox"/> PUBLISHER	<input type="checkbox"/> INWORK FILES				
<input type="checkbox"/> OFFICE2007+/PASSWORD							
압축 파일							
<input type="checkbox"/> ZIP	<input type="checkbox"/> ZIP/PASSWORD	<input type="checkbox"/> 7Z	<input type="checkbox"/> 7Z/PASSWORD				
<input type="checkbox"/> RAR	<input type="checkbox"/> ACE	<input type="checkbox"/> TAR	<input type="checkbox"/> XZ				
<input type="checkbox"/> XAR	<input type="checkbox"/> ACE/PASSWORD	<input type="checkbox"/> RAR/PASSWORD	<input type="checkbox"/> ASIC CONTAINER				
<input type="checkbox"/> BZ2	<input type="checkbox"/> GZ						
기타 파일							
<input type="checkbox"/> TEXT FILES	<input type="checkbox"/> XML / DTD	<input type="checkbox"/> DRM FILES	<input type="checkbox"/> EXE, SYS, DLL				
<input type="checkbox"/> FASOO FILES	<input type="checkbox"/> JOURNAL FILES	<input type="checkbox"/> SO	<input type="checkbox"/> UNIDENTIFIED				
<input type="checkbox"/> ACCDB	<input type="checkbox"/> BDF	<input type="checkbox"/> CSR	<input type="checkbox"/> DTA				
<input type="checkbox"/> EPB, ENCRYPTED FILES	<input type="checkbox"/> FDL	<input type="checkbox"/> HUE STREAMS	<input type="checkbox"/> NASCA DRM				
<input type="checkbox"/> P12	<input type="checkbox"/> PGP	<input type="checkbox"/> PGP	<input type="checkbox"/> RODE				
<input type="checkbox"/> SEGD	<input type="checkbox"/> SEGY	<input type="checkbox"/> SGWGC	<input type="checkbox"/> SID				
<input type="checkbox"/> SSD	<input type="checkbox"/> VMDK	<input type="checkbox"/> XIA					
미디어 파일							
<input type="checkbox"/> MOV	<input type="checkbox"/> MP3	<input type="checkbox"/> M4A, MP4	<input type="checkbox"/> WAV				
<input type="checkbox"/> WMA	<input type="checkbox"/> AVI	<input type="checkbox"/> AIFF	<input type="checkbox"/> M3U				
<input type="checkbox"/> MATROSKA	<input type="checkbox"/> MXF						
CAD 파일							
<input type="checkbox"/> AUTOCAD FILES	<input type="checkbox"/> I-DEAS 3D CAD	<input type="checkbox"/> JGS	<input type="checkbox"/> IPT				
<input type="checkbox"/> JT	<input type="checkbox"/> PRO-E CAD	<input type="checkbox"/> PRT	<input type="checkbox"/> REVIT				
<input type="checkbox"/> SMG	<input type="checkbox"/> SOLID EDGE	<input type="checkbox"/> SOLIDWORKS FILES	<input type="checkbox"/> STL				

정보

파일 유형 거부목록은 콘텐츠 인식 보호 및 eDiscovery 모듈에서 사용 가능합니다.

참고

파일 유형 거부목록은 실제 파일 유형을 참조합니다. 만약 사용자가 임의로 파일 확장자를 변경해서 콘텐츠 탐지를 피하려고 해도 Endpoint Protector는 해당 파일을 탐지합니다.

6.2. 개인정보 거부목록

개인정보 거부목록은 Endpoint Protector로 탐지되는 민감한 콘텐츠의 용어 및 표현 목록이 미리 정의되어 있습니다. 목록이 미리 정의가 되어서 관리자는 정책의 개인정보 콘텐츠 탭에서 원하는 콘텐츠를 선택하면 됩니다.

The screenshot shows the '정책 블랙리스트' (Policy Blacklist) configuration interface. It includes tabs for '파일 종류' (File Types), '개인정보' (Personal Information), '사용자 키워드' (User Keywords), '파일 이름' (File Name), '정규식' (Regular Expression), and 'HIPAA'. The '개인정보' tab is selected. The interface lists several categories of sensitive information with checkboxes for inclusion in the blacklist:

- 신용 카드:** Amex, Mastercard, Diners, VISA, Discover, XE
- Personal Identifiable Information:** IBAN, 닉네임, 이메일, Germany, United States
- 주민등록번호:** Austria, 德國, Romania, United Kingdom, Canada, 대한민국, Spain, United States, France, Netherlands, Switzerland, Germany, Poland, Taiwan
- ID:** Belgium, Denmark, Poland, Taiwan, Hong Kong, Italy, Poland, Singapore, Turkey, India, Germany, South Africa, China Mainland, Macau, Sweden, Austria, Kazakhstan, Hong Kong
- 여행면적:** Poland, United Kingdom, France, China Mainland, Macao, 대만, Hong Kong
- 전화 번호:** Germany, Turkey, International, China Mainland, 대만, Macao, 대만, Hong Kong
- 세금 ID:** International, Italy, Poland, United States
- VAT ID:** Germany
- 관련면적:** 대만, 대만
- 간접면적:** Australia, 대한민국, United Kingdom
- 인터넷 프로토콜 주소:** IPv4, IPv6

정보

개인 정보 거부목록은 콘텐츠 인식 보호 및 eDiscovery 모듈에서 모두 사용 가능합니다.

미리 정의된 콘텐츠 거부목록은 아래와 같습니다.

- 신용카드
Amex, Diners, China UnionPay, Discovery, JCB, MasterCard, MIR, Maestro, Visa
- 개인 식별 정보 (PII, Personal Identifiable Information)

IBAN, 날짜, 이메일, 주소 등

- 사회보장번호(SSN), 주민등록번호
- ID
- 여권번호
- 세금 ID
- 운전면허번호
- 건강보험번호

팁

개인정보 항목의 대부분은 국가 유형을 따릅니다 (예: 호주, 캐나다, 독일, 대한민국, 영국, 미국 등). 과탐을 줄이기 위해서 지역 또는 국가 유형에 적용되는 여권번호만 사용할 수 있습니다.

6.3. 사용자 키워드 거부목록

사용자 키워드 거부목록은 Endpoint Protector가 탐지하는 민감한 콘텐츠에 대한 용어 및 표현 목록을 사용자가 정의합니다. 사용자 키워드 목록은 “거부목록 및 허용목록 > 거부목록 > 사용자 키워드 탭”에서 확인합니다.

The screenshot shows the 'Denylists' tab in the Endpoint Protector interface. The main panel displays a table of denylist entries:

이름	설명	횟수	만든 사람	만든 시간	수정한 사람	고친 시간	작업
Confidential Dictionary	List of Confidential Terms	108	root	-	root	-	수정
US Driving License	List for Contextual Detection	10	root	-	root	-	수정

Below the table, there is a note: '전체의 1 부터 2 까지 2 항목' (2 items from 1 to 2) and two buttons: '추가' (Add) and '다음' (Next).

정보

사용자 키워드 거부목록은 콘텐츠 인식 보호 및 eDiscovery 모듈에서 사용 가능합니다.

각 사용자 키워드는 편지, 내보내기, 삭제가 가능합니다. ☐☒×

"추가" 버튼을 클릭해서 새로운 사용자 키워드를 만들 수 있습니다. 새로 만들어진 키워드의 콘텐츠 추가는 수동 (타이핑 또는 붙여넣기) 또는 가져오기로 적어도 3자 이상의 키워드를 입력할 수 있습니다.

추가

이름: 이름

설명: 설명

콘텐츠 옵션들:

콘텐츠 붙여넣기 혹은 입력 콘텐츠 가져오기

내용: 예 : 대외비, 반출금지, 일급 비밀 등 세글자 이상 추천

저장 취소

새로운 키워드가 만들어지면 즉시 자동으로 사용자 키워드 탭에서 확인됩니다. 콘텐츠 인식 보호 또는 eDiscovery 정책을 편집 또는 만들 때 사용 가능합니다.

6.4. 파일 이름 거부목록

파일 이름 거부목록은 Endpoint Protector가 탐지하는 파일 이름의 사용자 정의 목록입니다. 파일 이름의 목록은 "거부목록 및 허용목록 > 거부목록 > 파일 이름 탭"에서 사용 가능합니다.

이름	설명	항목	만든 사람	만든 시간	수정한 사람	고친 시간	작업
Filename Denylist	Default Empty List	0	root	-	root	-	삭제

페이지... 검색... 알림 1 활성화합니다

이전 1 다음

추가

다음

_filename

© 2004 - 2021 Cetisys Ltd. All rights reserved. 버전 5.3.0.0

정보

파일 이름 거부목록은 콘텐츠 인식 보호 및 eDiscovery 모듈에서 사용 가능합니다.

각 파일 이름은 편지, 내보내기, 삭제가 가능합니다. 📈✉️✖

"추가" 버튼을 클릭해서 새로운 사용자 키워드를 만들 수 있습니다. 새로 만들어진 파일 이름 콘텐츠 추가는 수동 (타이핑 또는 붙여넣기) 또는 가져오기로 적어도 2자 이상의 키워드를 입력할 수 있습니다.

추가

이름:

설명:

콘텐츠 옵션들:

콘텐츠 붙여넣기 혹은 입력 콘텐츠 가져오기

내용:
예: example, example.png, png, .png, 등. ?

저장 취소

콘텐츠는 여러 방법으로 정의 될 수 있습니다. 파일 이름만, 파일 이름 및 확장자, 확장자로만 할 수 있습니다.

예제

"example.pdf" 파일 이름으로 설정하면 example.pdf 이름으로 끝나는 모든 파일이 차단됩니다
(예: example.pdf, myexample.pdf, test1example.pdf).

".epp" 확장자로 설정하면 .epp 확장자의 모든 파일이 차단됩니다.

(예: test.epp, mail.epp, 123.epp)

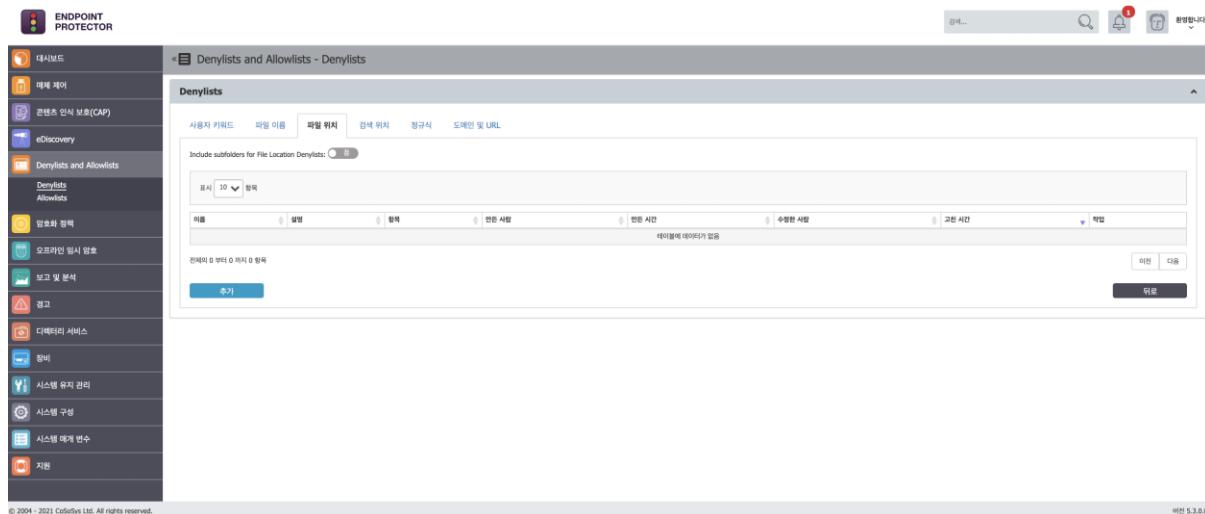
새로운 파일 이름이 만들어지면 즉시 자동으로 사용자 키워드 탭에서 확인됩니다. 콘텐츠 인식 보호 또는 eDiscovery 정책을 편집 또는 만들 때 사용 가능합니다.

참고

콘텐츠 인식 보호에서 파일 이름 거부목록은 차단 및 보고 정책에서만 동작합니다. 대소문자 구분 및 단어 단위 기능은 적용되지 않습니다.

6.5. 파일 위치 거부목록

파일 위치 거부목록은 Endpoint Protector로 확인되는 사용자 정의 위치입니다. 이 위치의 파일 전송은 여러 정책에서 정의된 콘텐츠 검사 규칙 및 허용에 관계없이 자동으로 차단됩니다. 위치 목록은 “거부목록 및 허용목록 > 거부목록 > 파일 위치 탭”에서 확인 합니다.



참고

파일 위치 거부목록 정의에서 파일 전송에 사용되는 브라우저 또는 응용프로그램은 콘텐츠 인식 보호 정책에서 선택해야 합니다.

팁

기본적으로 파일 위치 거부목록은 특정 폴더에 위치한 모든 파일 뿐만 아니라 하위 폴더의 다른 파일에도 적용됩니다. “파일 위치 하위 폴더를 포함” 옵션을 OFF로 하면 시스템을 통하여 모든 다른 파일 위치 거부목록과 허용목록에 영향을 줍니다.

정보

파일 위치 거부목록은 콘텐츠 인식 보호 모듈에서만 사용 가능합니다.

각 파일 위치는 편지, 내보내기, 삭제가 가능합니다.

"추가" 버튼을 클릭해서 새로운 파일 위치를 만들 수 있습니다. 새로 만들어진 파일 위치 추가는 수동 (타이핑 또는 붙여넣기) 또는 가져오기로 입력할 수 있습니다. 오른쪽 사이드에 적용하는 그룹 또는 컴퓨터를 선택해야 합니다.



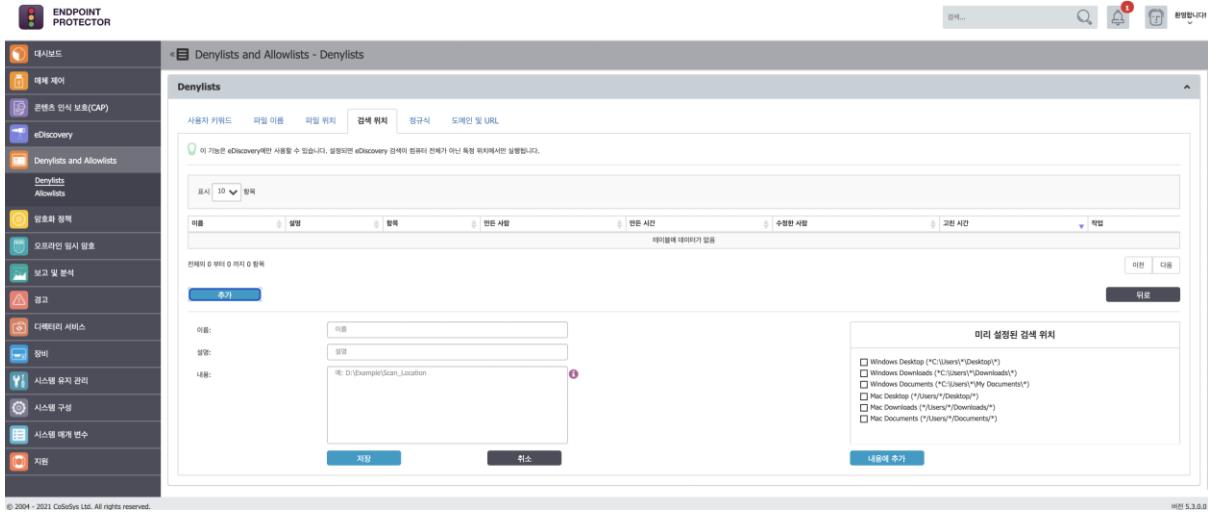
참고

파일 위치 거부목록은 사용자 그룹에 적용되지 않고 컴퓨터에만 적용됩니다.

파일 위치 거부목록은 15분 후에 선택된 컴퓨터 그룹에 적용될 것입니다.

6.6. 검색위치 거부목록

검색위치 거부목록은 eDiscovery 모듈에서 사용하는 위치 목록을 사용자가 정의하는 것입니다. 이렇게 정의된 경로에 있는 저장 데이터 (Data at rest)는 다양하게 정의된 정책에 따라서 콘텐츠를 자동으로 검사합니다. 이 옵션은 거부목록 및 허용목록 > 거부목록 > 검색위치에서 설정할 수 있습니다.



정보

몇 가지 미리 정의된 검색위치를 사용할 수 있습니다. 이렇게 정의된 검색위치는 원하는 결과를 더 잘 볼 수 있도록 조정되어 있습니다 (예: 전체 데스크톱 검색보다는 오히려 특정 패턴이 정의될 수 있는 일부 경로를 검색하는 것이 효율적입니다.).

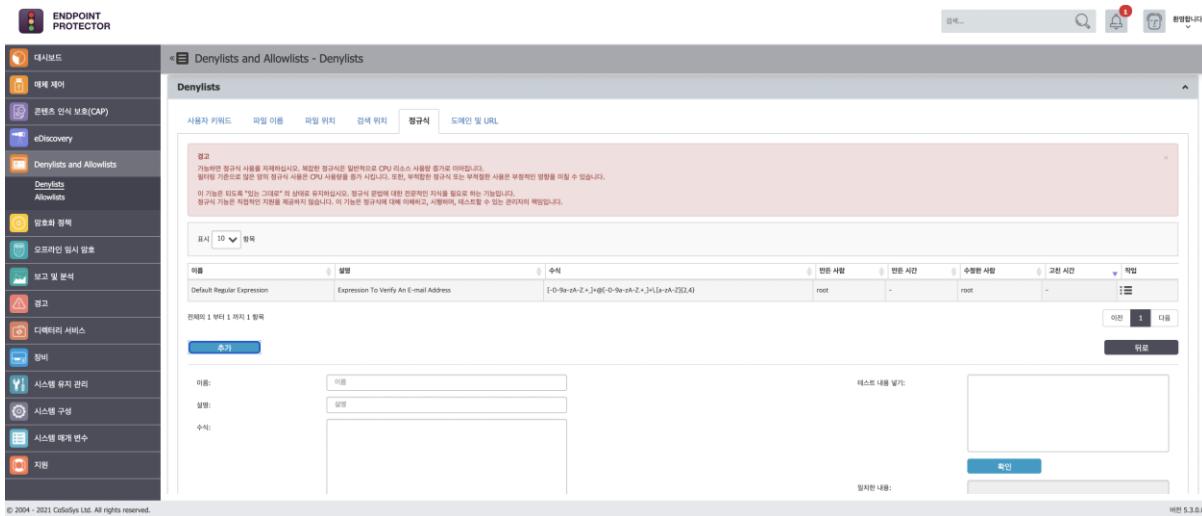
검사 위치를 정의 할 때 일부 특수 문자를 경로에 사용할 수 있습니다.

" * " – 모든 단어를 대체할 때 사용합니다.

" ? " – 모든 문자를 대체할 때 사용합니다.

6.7. 정규식 거부목록

정의에 따르면 정규식 표현은 주로 string 값과 매치되는 패턴에 사용되는 문자열의 검색 패턴 형태입니다. 관리자는 보호되는 네트워크에 전송되는 데이터의 특정 패턴을 찾기 위해서 정규식 표현을 만들 수 있습니다.



정보

정규식 거부목록은 콘텐츠 인식 보호 및 eDiscovery 모듈에서 사용 가능합니다.

각 정규식은 편지, 내보내기, 삭제가 가능합니다.

“추가” 버튼을 클릭해서 새로운 정규식 거부목록을 만들 수 있습니다. 정규식 표현은 정확성을 테스트할 수도 있습니다. “테스트 내용 넣기”에 정규식이 적용되는 예를 입력하고 “확인” 버튼을 누릅니다. 정규식 표현에 문제가 없다면 “일치한 내용” 박스에서 정규식이 찾아낸 콘텐츠가 나타나야 합니다.

예제

이메일 패턴과 매치되는 정규식

`[-0-9a-zA-Z.+]+@[-0-9a-zA-Z.+]+\W[a-zA-Z]{2,4}`

예제

IP 패턴과 매치되는 정규식

`(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

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 기능은 고급 정규식 문법을 알아야 합니다. 직접적으로 지원을 제공하지 않습니다. 정규식 표현을 배우고 실행하는 것은 고객의 책임입니다.

6.8. 도메인 및 URL 거부목록

도메인 및 URL 거부목록은 Endpoint Protector로 식별되는 웹 주소 목록을 사용자가 정의하는 것입니다. 이 목록에 있는 도메인 및 URL에 접근하면 사용 거부가 될 것입니다. 도메인 및 URL 목록은 '거부목록 및 허용목록 > 거부목록 > 도메인 및 URL' 탭에서 사용 가능합니다.

추가 버튼을 클릭해서 도메인 및 URL 거부목록을 만들 수 있습니다. 각 URL 또는 도메인은 수동으로 입력 또는 붙여넣기 아니면 가져오기를 선택할 수 있습니다.

이름:

설명:

콘텐츠 옵션들:

콘텐츠 붙여넣기 혹은 입력
 콘텐츠 가져오기

내용:

e.g.: *endpointprotector.com, *endpointprotector*,
<https://endpointprotector.com>, <http://endpointprotector.com> etc.

저장
취소

여러가지 방법으로 도메인 및 URL 콘텐츠를 만들 수 있습니다. 아래 예제를 참조 하시기 바랍니다.

예제

pdf, test1example.pdf, example.endpointprotector.com, *example.com, *example*example,
<https://website.com>

새로운 도메인 및 URL 거부목록이 만들어지면 자동으로 도메인 및 URL 탭에 나타납니다. 또한 콘텐츠 인식 보호 (CAP) 정책을 만들거나 수정할 때도 사용할 수 있습니다.

6.9. MIME 유형 허용목록

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 등을 포함할 수 없어서 콘텐츠 필터 사용으로 이러한 파일을 탐지하는 것은 무의미합니다.

MIME 유형	허용된 파일	파일 위치	네트워크 공유	이메일 도메인	URL 주소	심층 패킷 분석(DPI)
그림 파일	<input checked="" type="checkbox"/> JPG <input checked="" type="checkbox"/> BMP <input checked="" type="checkbox"/> COREL PHOTO-PAINT <input type="checkbox"/> GIF	<input checked="" type="checkbox"/> PNG <input checked="" type="checkbox"/> TIFF <input checked="" type="checkbox"/> COM <input checked="" type="checkbox"/> ADOBE INDESIGN	<input checked="" type="checkbox"/> GIF	<input checked="" type="checkbox"/> EPS	<input checked="" type="checkbox"/> PSD	<input checked="" type="checkbox"/> PCD <input checked="" type="checkbox"/> CORELDRAW <input checked="" type="checkbox"/> ADOBE ILLUSTRATOR
문서 파일	<input type="checkbox"/> DOC <input type="checkbox"/> INFORPATH <input type="checkbox"/> INWORD FILES	<input type="checkbox"/> 워드 <input type="checkbox"/> OUTLOOK		<input type="checkbox"/> POWERPOINT	<input type="checkbox"/> PUBLISHER	<input type="checkbox"/> PDF <input type="checkbox"/> OFFICE2007+/PASSWORD
압축 파일	<input type="checkbox"/> ZIP <input type="checkbox"/> RAR <input checked="" type="checkbox"/> ACI/PASSWORD <input checked="" type="checkbox"/> 822	<input checked="" type="checkbox"/> ZIP/PASSWORD <input checked="" type="checkbox"/> ACE <input checked="" type="checkbox"/> RAR/PASSWORD <input checked="" type="checkbox"/> GZ	<input type="checkbox"/> ZIP/PASSWORD <input checked="" type="checkbox"/> TAR <input checked="" type="checkbox"/> XAR	<input type="checkbox"/> 7Z <input checked="" type="checkbox"/> XZ		<input checked="" type="checkbox"/> ASIC CONTAINER
소스 코드	<input type="checkbox"/> C <input type="checkbox"/> C/C++ HEADER <input type="checkbox"/> TEX <input type="checkbox"/> MAKEFILE <input type="checkbox"/> CSS <input type="checkbox"/> OCAML <input type="checkbox"/> R <input type="checkbox"/> BACKUP	<input type="checkbox"/> C++ <input type="checkbox"/> BATCH FILE <input type="checkbox"/> FORTRAN <input type="checkbox"/> DMP <input type="checkbox"/> HTML <input type="checkbox"/> HASKELL <input type="checkbox"/> OBJECTIVE-C <input type="checkbox"/> RUBY <input type="checkbox"/> SWIFT	<input type="checkbox"/> JAVA <input type="checkbox"/> PYTHON <input type="checkbox"/> SHELL SCRIPT <input type="checkbox"/> ANDROID PACKAGE <input type="checkbox"/> JAVASCRIPT <input type="checkbox"/> LISP <input type="checkbox"/> PERL <input type="checkbox"/> SCALA <input type="checkbox"/> MATLAB	<input type="checkbox"/> UNIDENTIFIED	<input type="checkbox"/> UNIDENTIFIED	<input type="checkbox"/> POWERSHELL <input type="checkbox"/> PASCAL <input type="checkbox"/> ASSEMBLY <input type="checkbox"/> IOS APPLICATION <input type="checkbox"/> C# <input type="checkbox"/> LUA <input type="checkbox"/> PHP <input type="checkbox"/> SQL <input type="checkbox"/> VISUAL BASIC SCRIPT
기타 파일	<input type="checkbox"/> TEXT FILES <input type="checkbox"/> JOURNAL FILES <input type="checkbox"/> BMP_UNCRYPTED FILES <input type="checkbox"/> PGP <input type="checkbox"/> SEGY <input type="checkbox"/> BDF <input type="checkbox"/> ...	<input type="checkbox"/> XML / DTD <input checked="" type="checkbox"/> DLL, SHV, DLL <input type="checkbox"/> FOL <input type="checkbox"/> CSR <input type="checkbox"/> SID <input type="checkbox"/> SGWGC	<input type="checkbox"/> UNIDENTIFIED <input type="checkbox"/> CRW FILES <input type="checkbox"/> HUE STREAMS <input type="checkbox"/> RODE <input checked="" type="checkbox"/> VMDK <input type="checkbox"/> DTA	<input type="checkbox"/> UNIDENTIFIED	<input type="checkbox"/> UNIDENTIFIED	<input type="checkbox"/> FAX FILES <input checked="" type="checkbox"/> GO <input type="checkbox"/> MASCA DBM <input type="checkbox"/> SEQD <input type="checkbox"/> ACCDB <input type="checkbox"/> PIZ

© 2004 - 2021 Colodys Ltd. All rights reserved. 버전 5.3.0.0

정보

MIME 유형 허용목록은 콘텐츠 인식 보호 및 eDiscovery 모듈에서 사용 가능하고 사용자 키워드, 개인정보 및 정규식에 적용됩니다.

팁

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 유형에 깊은 이해를 가진 후에 변경하시기를 권장합니다.

MIME 유형 목록은 "거부목록 및 허용목록 > 허용목록 > MIME 유형 탭"에서 확인합니다.

6.10. 허용된 파일 허용목록

허용된 파일 허용목록은 Endpoint Protector가 탐지하는 민감한 콘텐츠 탐지에서 관리자가 제외하고 싶은 사용자 정의 파일 그룹입니다. 허용된 파일 그룹은 “거부목록 및 허용목록 > 허용목록 > 허용된 파일 탭”에서 확인합니다.

이름	설명	작업
Default File Allowlist	Default File Allowlist	root

정보

허용된 파일 허용목록은 콘텐츠 인식 보호 및 eDiscovery 모듈에서 사용 가능합니다.

각 허용된 파일은 편지, 내보내기, 삭제가 가능합니다. 📎✉️✖️

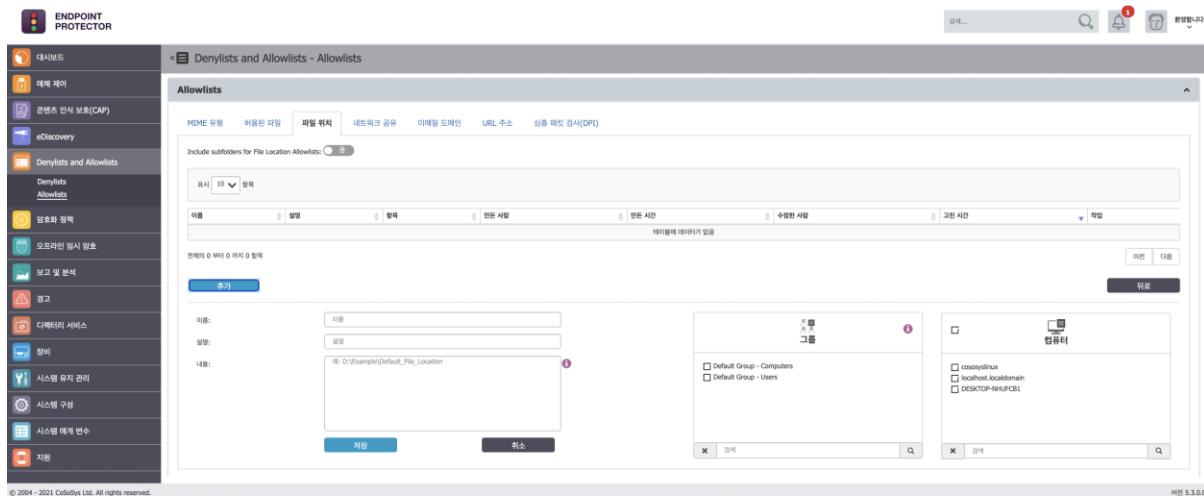
“추가” 버튼을 클릭해서 새로운 허용된 파일을 만들 수 있습니다. 새로 만들어진 허용목록에 콘텐츠 추가는 Endpoint Protector 서버에 업로드 된 허용된 파일이 필요합니다. 파일이 업로드 되면 여러 허용목록에서 사용할 수 있습니다.

작업	파일 이름	확장명	크기	해시
✖️	Dad.bmp	bmp	2 MB	055796e2067320abbff8c579e0fb55
✖️	sample.tif	tif	27 MB	d3dbb3d0b4d155859b1ede6e13b34d54

새로운 허용목록이 만들어지면 즉시 자동으로 허용된 파일 탭에서 확인됩니다. 콘텐츠 인식 보호 또는 eDiscovery 정책을 편집 또는 만들 때 사용 가능합니다.

6.11. 파일 위치 허용목록

파일 위치 허용목록은 Endpoint Protector에서 확인 할 수 있는 사용자 정의 파일 위치 목록입니다. 다양한 정책에 정의된 콘텐츠 검색 규칙 및 허용 정책에 상관없이 이 위치에 있는 파일 전송은 자동으로 허용됩니다. 위치 목록은 “거부목록 및 허용목록 > 허용 목록 > 파일 위치 탭”에서 확인합니다.



참고

파일 위치 허용목록 정의에서 파일 전송에 사용되는 브라우저 또는 응용프로그램은 콘텐츠 인식 보호 정책에서 선택해야 합니다.

팁

기본적으로 파일 위치 허용목록은 특정 폴더에 위치한 모든 파일 뿐만 아니라 하위 폴더의 다른 파일에도 적용됩니다. “파일 위치 하위 폴더를 포함” 옵션을 OFF로 하면 시스템을 통하여 모든 다른 파일 위치 거부목록과 허용목록에 영향을 줍니다.

정보

파일 위치 허용목록은 콘텐츠 인식 보호 모듈에서만 사용 가능합니다.

각 정규식은 편지, 내보내기, 삭제가 가능합니다.

“추가” 버튼을 클릭해서 새로운 파일 위치를 만들 수 있습니다. 새로 만들어진 파일 위치 추가는 수동 (타이핑 또는 붙여넣기) 또는 가져오기로 입력할 수 있습니다. 오른쪽 사이

드에 적용하는 컴퓨터를 선택해야 합니다.

참고

파일 위치 허용목록은 사용자 그룹에 적용되지 않고 컴퓨터 그룹에만 적용됩니다.

파일 위치 허용목록은 15분 후에 선택된 컴퓨터 그룹에만 적용됩니다.

The screenshot shows the 'Allowlists' configuration screen. On the left, there are input fields for 'Name' (Name), 'Description' (Description), and 'Content' (e.g.: D:\Example\Default_File_Location). Below these are 'Save' and 'Cancel' buttons. To the right, there are two sections: 'Groups' and 'Computers'. The 'Groups' section lists several computer groups: Default Group - Computers, Default Group - Users, Smart Group, and Test Group. The 'Computers' section lists individual computer names: RGyp3Fh9eHIM, ADIzBEQUOzYc, OFW4fD76vGwy, INIAvgm63HFE, lvza5yrUJNy2, 869DMGc8tVIZ, i4SpMK48gEil, and cGf0ze28kcM7. Both sections have search bars at the bottom.

6.12. 네트워크 공유 허용목록

네트워크 공유 허용목록은 Endpoint Protector로 기밀 정보 전송을 허용하는 사용자 정의 네트워크 공유 주소입니다. 허용목록 네트워크 공유는 "거부목록 및 허용목록 > 허용목록 > 네트워크 공유 탭"에서 확인합니다.

The screenshot shows the 'Allowlists' configuration screen under the 'Denylists and Allowlists' module. On the left, there is a sidebar with various security modules like Firewall, Antivirus, Content Protection, eDiscovery, Denylists, Allowlists, and more. The main area is titled 'Allowlists' and shows a table of existing allowlists: 'Default Network Share Allowlist' (설명: Default Network Share Allowlist, 그룹: Default Group - Computers). Below this is a 'New' button and a form for creating a new allowlist, including fields for '이름' (Name), '설명' (Description), and '내용' (Content) which contains the value '제거: Reserv/share/programs'. To the right, there are two sections: 'Groups' and 'Computers', each with a list of items and a search bar.

정보

네트워크 공유 허용목록은 콘텐츠 인식 보호 모듈에서만 사용 가능합니다.

참고

이 기능을 사용하려면 네트워크 공유를 사용 허용으로 설정해야 하고 콘텐츠 인식 보호 정책에서 네트워크 공유 스캔을 체크해야 합니다.

각 네트워크 공유는 편지, 내보내기, 삭제가 가능합니다.

“추가” 버튼을 클릭해서 새로운 네트워크 공유 허용목록을 만들 수 있습니다. 새로운 화이트 리스트에 내용을 추가하려면 네트워크 공유 경로로 서버 이름 또는 IP를 사용할 수 있습니다.

참고

네트워크 공유 허용목록은 사용자 그룹에 적용되지 않고 컴퓨터 그룹에서만 사용 가능합니다.

네트워크 공유 허용목록은 15분 후에 선택된 컴퓨터 그룹에만 적용됩니다.

추가

이름:

이름

설명:

설명

내용:

예: fileserver\share\programs

**참고**

네트워크 공유 경로는 백슬래시로(\\) 시작하면 안 됩니다.

예제

192.168.0.1\public\users\test; fileserver\documents\example

새로운 허용목록이 만들어지면 즉시 자동으로 네트워크 공유 탭에서 확인됩니다. 콘텐츠 인식 보호 또는 eDiscovery 정책을 편집 또는 만들 때 사용 가능합니다.

6.13. 이메일 도메인 허용목록

이메일 도메인 허용목록은 Endpoint Protector로 기밀 정보를 보낼 수 있는 사용자 정의 이메일 주소입니다. 이메일 도메인 목록은 “거부목록 및 허용목록 > 허용목록 > 이메일 도메인 탭”에서 확인합니다.

정보

이메일 도메인 허용목록은 콘텐츠 인식 보호 모듈에서만 사용 가능합니다.

이름	설명	등록	한은 사람	한은 시간	수정한 사람	고친 시간	작업
Default Domain Allowlist	Default Domain Allowlist	2	root	-	root	-	수정

각 네트워크 공유는 편지, 내보내기, 삭제가 가능합니다. ✉️✉️✖️

추가

이름:

설명:

콘텐츠 옵션들:

콘텐츠 복여넣기 혹은 입력 콘텐츠 가져오기

내용:

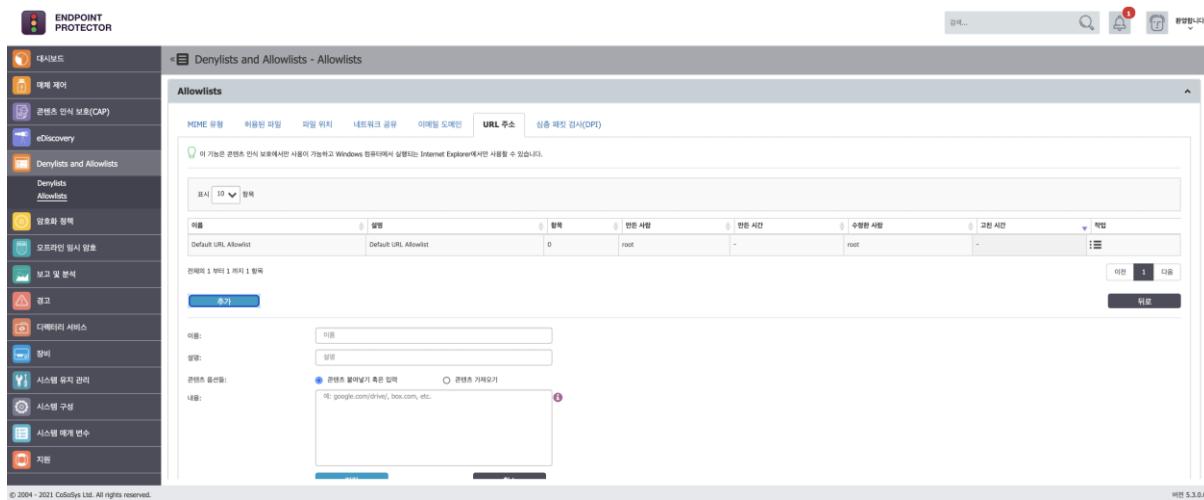
예: support@cososys.kr, endpointprotector.com, etc.

저장 취소

새로운 이메일 도메인 허용목록이 추가되면 바로 이메일 도메인 허용목록 탭에서 자동으로 확인됩니다. 콘텐츠 인식 보호 정책을 만들거나 수정할 때 또한 사용 가능합니다.

6.14. URL 주소 허용목록

URL 주소 허용목록은 Endpoint Protector가 기밀 정보 업로드를 허용하는 사용자 정의 웹 주소 목록입니다. URL 주소 목록은 “거부목록 및 허용목록 > 허용목록 > URL 주소 탭”에서 사용 가능합니다.



정보

URL 주소 허용목록은 콘텐츠 인식 보호 모듈에서만 사용 가능합니다.

각 URL 주소는 편지, 내보내기, 삭제가 가능합니다.

“추가” 버튼을 클릭해서 새로운 URL 주소 허용목록을 만들 수 있습니다. 새로운 화이트 리스트에 내용을 추가하려면 URL 주소를 수동 (타이핑 또는 붙여넣기) 또는 가져오기로 입력할 수 있습니다.

추가

이름:

설명:

콘텐츠 옵션들:

콘텐츠 업로드 혹은 입력 콘텐츠 가져오기

내용:
e.g.: google.com/drive/, box.com, etc.

저장 취소

새로운 허용목록이 만들어지면 즉시 자동으로 네트워크 공유 탭에서 확인됩니다. 콘텐츠 인식 보호 정책을 편집 또는 만들 때 사용 가능합니다.

참고

URL은 주소와 도메인만 사용해야 합니다, www.* , www2.* , en.* 등으로 시작해서는 안 됩니다.

예제

endpointprotector.com (www.endpointprotector.com 은 사용 불가)

새로운 URL 주소 허용목록이 추가되면 바로 URL 주소 허용목록 탭에서 자동으로 확인됩니다. 콘텐츠 인식 보호 정책을 만들거나 수정할 때 또한 사용 가능합니다.

6.15. 심층 패킷 검사 허용목록

심층 패킷 검사 허용목록은 Endpoint Protector에서 기밀 정보 업로드를 허용하는 웹 주소 목록을 사용자가 정의할 수 있습니다. 심층 패킷 검사 목록은 거부목록 및 허용목록 > 허용목록 > 심층 패킷 검사 (DPI) 탭에서 확인할 수 있습니다.

117 | Endpoint Protector | 사용 설명서

정보

심층 패킷 검사 허용목록은 콘텐츠 인식 보호 모듈에서만 사용 가능합니다.

심층 패킷 검사 허용목록은 추가 버튼을 클릭해서 만들 수 있습니다. 새롭게 만들어진 심층 패킷 검사 허용목록에 컨텐츠를 입력하려면 타이핑 또는 붙여넣기 같은 수동 입력이나 파일 가져오기로 입력이 가능합니다.

추가

이름:

설명:

콘텐츠 옵션들:

콘텐츠 붙여넣기 혹은 입력 콘텐츠 가져오기

내용: i

저장 취소

예제

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

참고

“ ? ”는 문자를 대체하는데 사용할 수 없습니다.

참고

Gmail에서 원하는 결과를 얻으려면 아래 내용을 고려해야 합니다.

- mail.google.com 화이트리스팅은 이메일 첨부 또는 드래그앤파울을 사용 가능
- doc.google.com 화이트리스팅은 이메일 본문에 이미지 삽입 시 필요

새로운 심층 패킷 검사 허용목록이 추가되면 자동으로 심층 패킷 검사 허용목록 탭에 등록이 되어 볼 수 있습니다. 콘텐츠 인식 보호(CAP) 정책 만들기 또는 수정할 때 사용할 수 있습니다.

6.16. URL 범주

URL 범주는 웹 트래픽을 모니터링하는 DPI 제한을 위한 콘텐츠 인식 정책을 설정하는 웹 주소 목록의 사용자 정의입니다. 정책에 URL 범주로 모니터링하는 DPI가 설정되어 있지 않으면 Endpoint Protector 클라이언트는 기본적으로 모든 웹 주소를 모니터링합니다.

이름	설명	항목	만든 사람	만든 시간	수정한 사람	고친 시간	작업
전체의 0 부터 0 까지 0 항목 데이터에 데이터가 없음							

© 2004 - 2021 CoSoSys Ltd. All rights reserved.

버전 5.4.0.0

정보

URL 범주는 DPI 기능이 활성화 될 때만 적용됩니다.

참고

URL 범주 기반 콘텐츠 차단은 브라우저가 아닌 URL 기반으로 차단되기 때문에 보안 위반입니다. 정책은 새로운 범주 발견 시 업데이트가 항상 필요 합니다.

각 URL 범주는 수정, 내보내기, 삭제 액션이 가능합니다.

추가 버튼을 클릭해서 새로운 URL 범주를 만들 수 있습니다. 새로운 URL 범주 내용을 만들기 위해서 수동 (타이핑 또는 붙여넣기) 또는 가져오기 옵션을 사용할 수 있습니다.

이름:	<input type="text" value="이름"/>
설명:	<input type="text" value="설명"/>
콘텐츠 옵션들: <input checked="" type="radio"/> 콘텐츠 붙여넣기 혹은 입력 <input type="radio"/> 콘텐츠 가져오기	
내용: <div style="border: 1px solid #ccc; padding: 5px; width: 100%;"> E.g.: http://domain.com domain.com - monitors the main domain including all its subdomains *.domain.com - monitors only subdomains, excluding the main domain www.domain.com subdomain1.domain.com - monitors the subdomain1 and any of its subdomains like subdomain2.subdomain1.domain.com i </div>	
<input type="button" value="저장"/> <input type="button" value="취소"/>	

7. 암호화 정책

7.1. EasyLock

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.

The screenshot shows the Endpoint Protector software interface with the following details:

- Left Sidebar:** A vertical menu bar with various icons and labels, including "데시보드", "매체 제어", "콘텐츠 인식 보호(CAP)", "eDiscovery", "블랙리스트 및 화이트리스트", "암호화 정책", "EasyLock" (selected), "모바일 기기 관리(MDM)", "오프라인 임시 암호", "보고 및 분석", "경고", "디렉터리 서비스", "장비", "시스템 유지 관리", "시스템 구성", "시스템 매개 변수", and "지원".
- Top Bar:** Includes a search bar ("검색..."), a notification icon with a red dot ("1"), and a "환영합니다" (Welcome) message.
- Main Content Area:**
 - Header:** "암호화 정책 - EasyLock 보안USB".
 - Section 1: 배포**
 - Sub-section: 수동 배포**

EasyLock을 수동 배포하고 보안USB 관리 기능을 이용하려면 아래 단계를 실행:
① USB 저장장치를 선택하세요.
② 선택한 USB 저장 장치의 루트에 EasyLock 패키지를 직접 다운로드하거나 복사하세요.
 - Buttons:** "장치 선택" dropdown, "운영체제 선택" dropdown, and a blue "다운로드" button.
 - Text:** "EasyLock이 지원하는 모든 장치에 자동으로 또는 특정 장치에 배포하려면 USB 저장장치에서 "TD 레벨 1+ 장치 사용 허용"을 선택해야만 합니다. USB 저장장치가 Endpoint Protector 클라이언트가 배포된 컴퓨터에 꽂히면 EasyLock이 그 장치 속으로 자동으로 설치됩니다."
 - Section 2: 설정**
 - Sub-section: Update EasyLock**

Automatically:
 - Sub-section: EasyLock 설치 및 실행**

Endpoint Protector Client presence required:
 - Master Password Settings:**
 - 암호 복잡성 설정:
 - Minimum password length: 6
 - Minimum password upper case characters: 0
 - Minimum password lower case characters: 0
 - User Password Settings:**
 - 암호 복잡성 설정:
 - Minimum password length: 6
 - Minimum password upper case characters: 0
 - Minimum password lower case characters: 0

정보

EasyLock 자체 사용에 대한 더 많은 정보는 홈페이지를 참조하시기 바랍니다.

Endpoint Protector와 연동해서 EasyLock은 "TD 레벨1"로 확인되어 USB 저장 장치를 허용합니다. 보호되는 컴퓨터에서 USB 암호화 정책을 확실히 할 수 있습니다. 즉 사용자가 설정한 암호로 저장 데이터에 접근하거나 Endpoint Protector 관리자가 설정한 마스터 암호로 접근이 가능합니다. 암호화된 데이터는 복호화 후에만 열 수 있습니다.

참고

Endpoint Protector는 TD 레벨 1로 모든 EasyLock USB 장치를 탐지하지만 암호화 정책 기능을 사용하려면 특정 EasyLock 버전이 필요합니다. 이 버전은 Endpoint Protector 사용자 인터페이스에서 받을 수 있습니다.

7.1.1. EasyLock 배포

정보

EasyLock 암호화 정책은 macOS 및 Windows 컴퓨터를 모두 지원합니다.

배포

수동 배포 ⓘ

EasyLock을 수동 배포하고 보안USB 관리 기능을 이용하려면 아래 단계를 실행:

- ① USB 저장장치를 선택하세요.
- ② 선택한 USB 저장 장치의 루트에 EasyLock 페키지를 직접 다운로드하거나 복사하세요.
- ③ 간단한 설정 절차를 따르고 암호를 설정합니다.
- ④ 암호화 및 보호를 할 파일들을 EasyLock을 통해서 복사 & 붙여넣기 혹은 끌어서 & 놓기 합니다.

장치 선택:

운영체제 선택:

다운로드

자동 배포 ⓘ

EasyLock이 지원하는 모든 장치에 자동으로 또는 특정 장치에 배포하려면 USB 저장장치에서 "TD 레벨 1+ 장치 사용 허용"을 선택해야만 합니다. USB 저장장치가 Endpoint Protector 클라이언트가 배포된 컴퓨터에 꽂히면 EasyLock이 그 장치 속으로 자동으로 설치됩니다.

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 확인하거나 위의 이미지에서 제공하는 링크를 통해서 확인

합니다.

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.

팁

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).

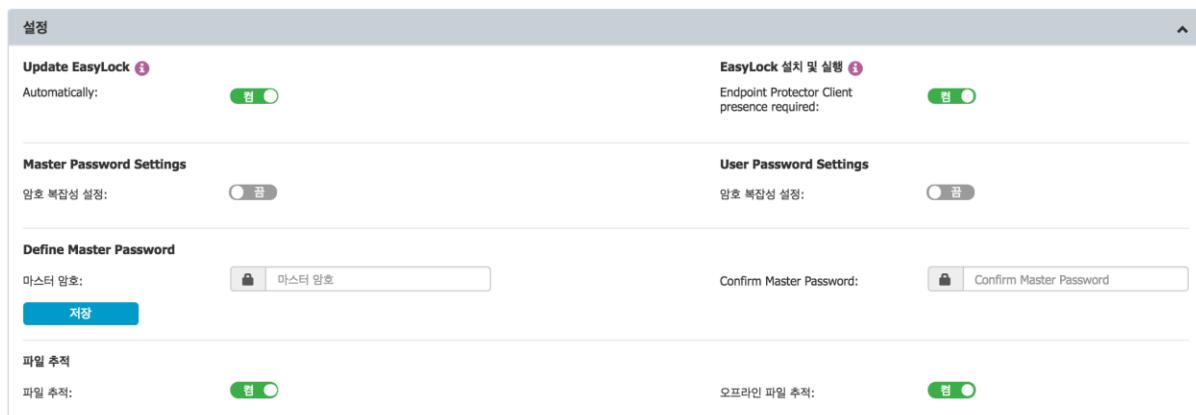
두 가지 방법은 모두 배포가 간단하고 사용자는 암호만 설정하면 됩니다.

참고

macOS에서 여러 파티션을 가진 USB 저장 장치는 EasyLock 및 TD 레벨 1을 지원하지 않습니다.

7.1.2. EasyLock 설정

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



정보

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.

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

Master Password Settings	User Password Settings
암호 복잡성 설정: <input checked="" type="radio"/>	암호 복잡성 설정: <input checked="" type="radio"/>
Minimum password length: 6	Minimum password length: 6
Minimum password upper case characters: 0	Minimum password upper case characters: 0
Minimum password lower case characters: 0	Minimum password lower case characters: 0
Minimum password numbers: 0	Minimum password numbers: 0
Minimum password special characters: 0	Minimum password special characters: 0
Consecutive and ascending characters: cannot be used	Consecutive and ascending characters: cannot be used
Password Validity: Never expires	Password Validity: Never expires
암호 기록: 1	암호 기록: 1
Password Retries: 10	Password Retries: 10
저장	

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

파일 추적

파일 추적:

오프라인 파일 추적:

파일 추적 옵션을 체크해서 EasyLock을 사용하는 장치로 전송된 모든 데이터가 기록되고 차후 감사를 위한 로그가 됩니다. 로그 정보는 Endpoint Protector 클라이언트가 컴퓨터

에 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 옵션을 활성화하지 않습니다. 그 반대도 동일합니다.

7.1.3. EasyLock 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.

1 2 5 | Endpoint Protector | 사용 설명서

표시 10 ▼ 항목									Excel	PDF	CSV	열 브이기/슬기기	다시 읽기
	이름	장치	설명	일련 번호	최종 사용자	마지막 컴퓨터	마지막 확인	최근 주 IP	작업				
■	Jack	Patriot Memory	Patriot Memory /	07014A1892CE6E17	jackjung	YoungHo@ MacBook Pro	2017-03-27 19:28:00	192.168.100.190	Manage Delete				
■	Jack	DataTraveler 3.0	DataTraveler 3.0 / Kingston	08606E6B66FB85B0C7107941	jackjung	YoungHo@ MacBook Pro	2017-03-27 19:26:51	192.168.100.190	Manage Delete				
■	cotosys-Win10	Patriot Memory	Patriot Memory /	07014A1892279805	cotosys-Win10	DESKTOP-NG69592	2017-03-14 15:08:35	220.118.0.30	Manage Delete				
■	Jack	Ultra	Ultra / SanDisk	4C530123181206116342	jackj	JACK-WIN10	2016-12-30 10:40:10	192.168.100.190	Manage Delete				
■	mandol	HMCUSB	HMCUSB / HDCAR	SZSUEB0000000002487	PARK	DESKTOP-D9QFJMH	2016-12-08 13:48:06	121.140.122.141	Manage Delete				
■	Jack	Patriot Memory	Patriot Memory /	070147B273279C36	Jack	JACK-WIN10	2016-10-18 11:10:37	192.168.100.147	Manage Delete				

표시줄 1 부터 6 까지 6 항목

이전 1 다음

메시지 보내기 마스터 암호 다시보냄 사용자 암호 변경 장치 초기화 모든 대기 중인 작업 취소

뒤로

« 암호화 정책 - 장치 관리

기기 정보

Jack	식별 정보:	Jack	마지막 확인:	2017-03-27 19:28:00	만든 사용자:	jackjung
	설명:	Patriot Memory /	최근 위치 IP:	192.168.0.105 192.168.100.190	만든 시간:	2017-03-27 19:28:00
	번더 ID:	13PE	컴퓨터:	YoungHo@ MacBook Pro	수정한 사용자:	jackjung
	제품 ID:	SS500	사용자:	jackjung	수정한 시간:	2017-03-27 19:28:00
	일련 번호:	07014A1892CE6E17	상태:	활성		

저장 메시지 보내기 마스터 암호 다시보냄 사용자 암호 변경 장치 초기화

작업 기록

표시 10 ▼ 항목									Excel	PDF	CSV	열 브이기/슬기기	다시 읽기
종류	상태	세부정보	만든 사람	만든 시간	고친 사람	고친 시간	작업						
데이터베이스에 데이터가 없습니다									이전	다음			

표시줄 0 부터 0 까지 0 항목

8. 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.

- 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.

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.

정보

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 서버 시간 및 클라이언트 시간을 고려해야 합니다.

예제

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 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.

정보

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.

8.1. 오프라인 임시 암호 만들기

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

The screenshot shows the Endpoint Protector software interface with the following details:

- Left Sidebar:** Includes icons for Dashboard, Device List, Group Policy, eDiscovery, Assets & Inventories, Key Management, Mobile Device Management, Offline Temporary Passwords, and Help.
- Top Bar:** Includes search, notifications, and a language switcher (한국어/Korean).
- Main Content Area - 'Create Offline Temporary Password' Screen:**
 - Header:** 오프라인 임시 암호
 - Text:** 모든 기능을 최대한 활용하려면, 최소로 필요한 Endpoint Protector Client 버전은 Windows는 4.7.3.5, Mac은 1.5.5.8 그리고 Linux는 1.3.1.2입니다.
 - Section: Create Offline Temporary Password**
 - Toggle:** 비밀번호 오프라인 임시 암호:
 - Text:** 비밀번호 오프라인 임시 암호는 모든 컴퓨터, 모든 사용자, 모든 장치 또는 파일 전송에 사용될 수 있습니다. 이것은 한 시간 동안 보안 세션을 일으킵니다.
 - Section: Offline Temporary Password Settings**
 - Form:**

장치 (특정 장치) 매체 제어:	Bluetooth Device
기간:	30분
장치 이름 혹은 코드:	BD04
컴퓨터 이름 혹은 사용자 이름:	JACK-WIN10
정답한 이유:	Bluetooth 파일 전송 필요 - 세밀조차로 받아야 함
 - Form (Right):**

유용한 정보:	
컴퓨터 이름:	JACK-WIN10
예인 IP:	192.168.100.211
MAC 주소:	40:6c:8f:32:65:a0
도메인:	
작업 그룹:	WORKGROUP
사용자명:	jack(정도영)
이름:	jack(정도영)
성:	jack(정도영)
 - Buttons:** 생성 (Create), 보내기 (Send), 취소 (Cancel).

장치에 대한 OTP를 만들 때 관리자는 사용자와 연락을 통해서 장치 코드를 받아서 입력하거나 Endpoint Protector 데이터베이스의 장치 검색을 위한 마법사를 사용할 수 있습니다.

팁

오프라인 임시 암호를 설정하는 또 다른 방법은 매체 제어 > 컴퓨터 섹션의 액션 컬럼에서 오프라인 임시 암호 옵션을 선택하는 것입니다.

정보

특정 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.

정보

오프라인 임시 암호에 대한 더 자세한 정보는 '17.4.1 오프라인 임시 암호의 요청 및 사용'을 참조 하시기 바랍니다.

참고

관리자 연락처 정보는 사용자에게 노출됩니다. 이것은 '시스템 구성 > 시스템 설정' 섹션에서 변경할 수 있습니다. 여기에 주요 관리자 연락처를 입력하시면 됩니다.

정보

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.

9. 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.

정보

추가적인 데이터 보안 조치로 이 섹션은 최고 관리자가 설정한 암호를 통해서 보호 할 수 있습니다. '시스템 구성 > 시스템 보안' 섹션에서 설정 할 수 있습니다.

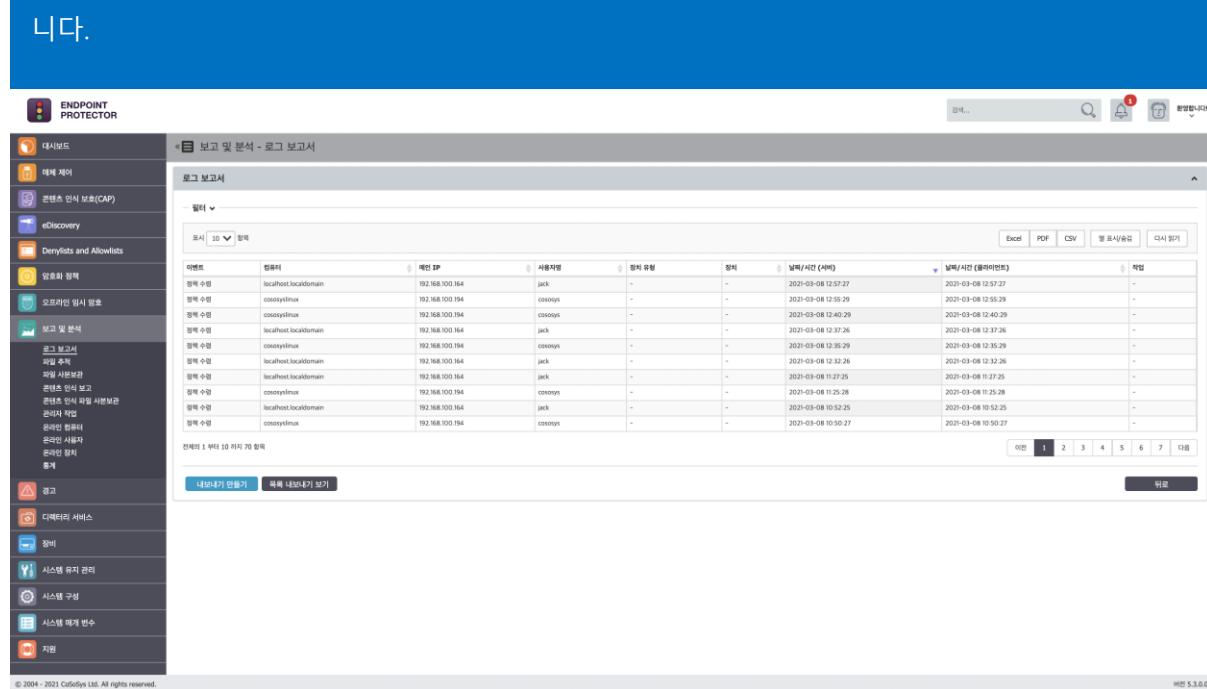
시스템 보안에 대한 자세한 정보는 14.7 시스템 보안을 참조 하시기 바랍니다.

9.1. 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.

팁

이 섹션에서 로그 유형의 완전한 항목은 필터의 이벤트 드롭 다운 목록에서 확인 할 수 있습니다.



The screenshot shows the 'Logging and Analysis - Log Reporting' section of the Endpoint Protector interface. On the left, there's a sidebar with various system monitoring and protection features like Firewall, eDiscovery, Denylists and Allowlists, and Endpoint Protection. The main area has a search bar and a table displaying log entries. The table columns include: 이벤트 (Event), 컴퓨터 (Computer), 배인 IP (External IP), 사용자명 (User Name), 장치 유형 (Device Type), 장치 (Device), 날짜/시간 (날짜/시간) (Date/Time (Date/Time)), 날짜/시간 (로그아웃) (Date/Time (Logout)), and 작업 (Action). The table lists several log entries for different users (jack, cososys) on the same computer (localhost.localdomain) at various dates and times. At the bottom, there are buttons for '내보내기 만들기' (Create Export) and '파일 내보내기 보기' (View File Export), along with a page navigation bar.

이벤트	컴퓨터	배인 IP	사용자명	장치 유형	장치	날짜/시간 (날짜/시간)	날짜/시간 (로그아웃)	작업
정체 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-08 12:57:27	2021-03-08 12:57:27	-
정체 수령	cososyslinux	192.168.100.194	cososys	-	-	2021-03-08 12:55:29	2021-03-08 12:55:29	-
정체 수령	cososyslinux	192.168.100.194	cososys	-	-	2021-03-08 12:40:29	2021-03-08 12:40:29	-
정체 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-08 12:37:26	2021-03-08 12:37:26	-
정체 수령	cososyslinux	192.168.100.194	cososys	-	-	2021-03-08 12:35:29	2021-03-08 12:35:29	-
정체 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-08 12:32:26	2021-03-08 12:32:26	-
정체 수령	localhost.beatdomen	192.168.100.164	jack	-	-	2021-03-08 11:27:25	2021-03-08 11:27:25	-
정체 수령	cososyslinux	192.168.100.194	cososys	-	-	2021-03-08 11:25:28	2021-03-08 11:25:28	-
정체 수령	localhost.localdomain	192.168.100.164	jack	-	-	2021-03-08 10:52:25	2021-03-08 10:52:25	-
정체 수령	cososyslinux	192.168.100.194	cososys	-	-	2021-03-08 10:50:27	2021-03-08 10:50:27	-

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

9.2. 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.

로그 보고서 섹션과 마찬가지로 파일 목록에 액세스하려면 관리자가 설정한 추가 암호를 입력해야 할 수도 있습니다.

정보

“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.

9.3. 파일 사본보관

이 섹션은 보호되는 컴퓨터에서 이동식 저장 장치로 전송된 파일 사본 보관에 대한 정보를 보여줍니다. 파일 목록은 관리자가 설정한 추가 암호로 보호될 수 있습니다. 이 경우 이 섹션에 들어갈 때 추가 암호를 입력해야 바로 사용할 수 있습니다.

또한 파일 보관은 Endpoint Protector 관리자가 서버에 로컬로 저장할 수 있습니다.

9.4. 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. 또한 컴퓨터 이름, 사용자 및 전송 대상 유형, 수행된 동작, 검사된 파일이 이러한 정보에 포함됩니다. 포함된 세분화 필터를 통해 정보를 빠르고 쉽게 찾을 수 있습니다.

1 3 5 | Endpoint Protector | 사용 설명서

The screenshot shows the 'Content Analysis - Content Scan Report' section of the Endpoint Protector interface. It features a search bar at the top right and a sidebar on the left with various navigation links. The main area contains a table of scanned files with the following columns: 파일 이름 (File Name), 컴퓨터 (Computer), 사용자명 (User), 접두어 이름 (Prefix Name), 대상 유형 (Target Type), 대상 (Target), 파일 이름 (File Name), 파일 확장 (File Extension), 파일 사이즈 (File Size), 날짜/시간(시작) (Start Date/Time), 날짜/시간(종료) (End Date/Time), 파일 유형 (File Type), 파일 확장 (File Extension), OS 종류 (OS Type), 사용자 (User), 날짜/시간(시작) (Start Date/Time), 날짜/시간(종료) (End Date/Time), 파일 유형 (File Type), 파일 확장 (File Extension), OS 종류 (OS Type), 사용자 (User), and 작업 (Action). The table lists numerous entries, each with a timestamp ranging from 2021-03-05 11:02:10 to 2021-03-04 21:01:00.

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

9.5. 콘텐츠 인식 파일 사본 보관

콘텐츠 인식 정책으로 탐지된 파일 및 파일 보관 리스트를 보여줍니다. 파일 리스트는 보고 및 분석 섹션의 관리자가 설정한 추가 암호로 보호 할 수 있습니다. 이 경우 이 섹션에 들어 갈 때 추가 암호를 입력해야 합니다.

The screenshot shows the 'Content Analysis - Content File Backup' section of the Endpoint Protector interface. It features a search bar at the top right and a sidebar on the left with various navigation links. The main area contains a table of backed-up files with the following columns: 파일 이름 (File Name), 파일 크기 (File Size), 컴퓨터 (Computer), 사용자 (User), 날짜/시간 (Date/Time), and 작업 (Action). The table lists entries such as '파일 이름: 파일 이름' (File Name: File Name), '파일 크기: 0 B', '컴퓨터: 컴퓨터', '사용자: 사용자', '날짜/시간(시작) (Start Date/Time): 2021-03-05 11:02:10', and '날짜/시간(종료) (End Date/Time): 2021-03-04 21:01:00'. A note at the bottom states '일치하는 레코드 찾지 못함' (No matching records found).

9.6. 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. 변경 전후의 상태를 보여 줍니다.

관리자	작업	작업	한은 시간	액션
root	로그인	로그인	2021-03-08 15:01:35	
root	로그인	로그인	2021-03-08 14:35:55	
root	로그인	로그인	2021-03-08 13:58:54	
root	로그인	로그인	2021-03-08 13:40:13	
root	로그	선택 항목 삭제 / 모두	제거됨	2021-03-08 13:55:58
root	구성	수정됨	2021-03-08 12:53:55	
root	구성	저장됨	2021-03-08 12:33:55	
root	저장	저장됨	2021-03-08 12:29:32	
root	로그인	로그인	2021-03-08 12:29:03	
root	구성	수정됨	2021-03-08 11:22:50	

9.7. 온라인 컴퓨터

컴퓨터 이름	사용자명	예전 IP	MAC 주소	도메인	작업그룹	액션
cosemyslum	cosemys	192.168.100.194	00-0C-29-7F-82-06	cosemys.co.kr		
localhost.localdomain	jack	192.168.100.194	00-0C-29-42-22-08	cosemys.co.kr		

서버와 연결이 설정된 시스템에 등록된 클라이언트 컴퓨터를 실시간으로* 모니터링할 수 있습니다.

정보

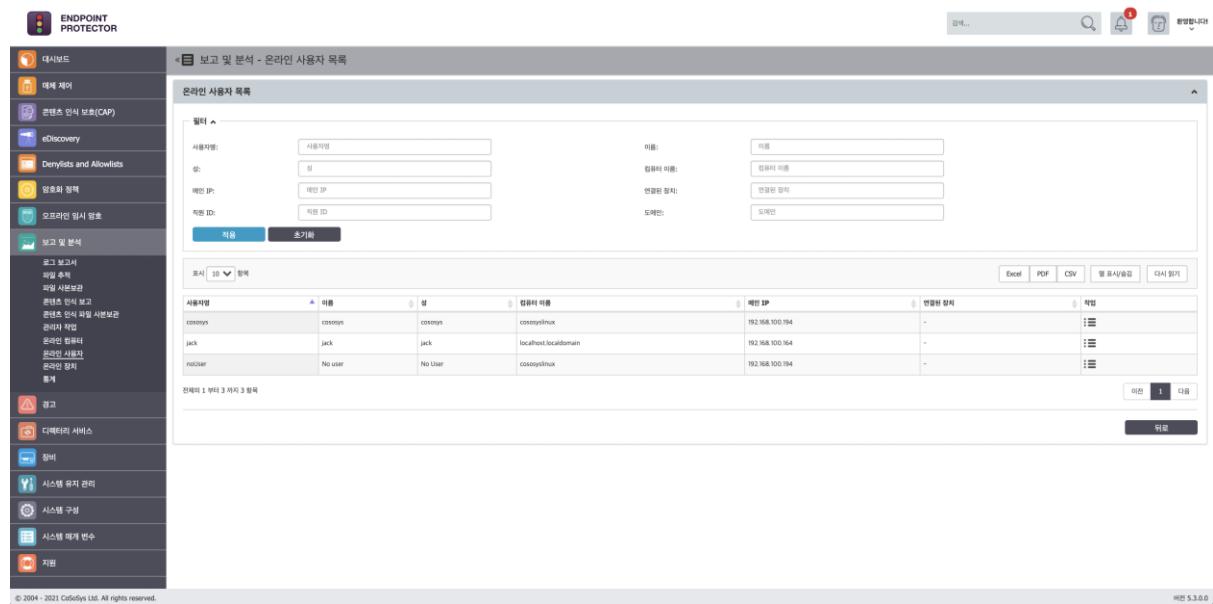
컴퓨터 X의 새로 고침 간격이 1분이면 컴퓨터 X는 지난 1분 전에 서버와 통신 중이었습니다.

관리자는 "로그 보기" 작업 버튼을 눌러 특정 컴퓨터의 로그에 액세스할 수 있습니다.

 이 버튼을 누르면 해당하는 특정 컴퓨터의 작업만이 표시되는 로그 보고서로 이동합니다.

9.8. 온라인 사용자

Endpoint Protector 서버에 연결된 사용자 목록이 실시간으로 표시됩니다.



사용자명	이름	성	컴퓨터 이름	예전 IP	연결된 장치	작업
cosys	cosys	cosys	cosyslinux	192.168.100.194	-	
jack	jack	jack	localhost.localdomain	192.168.100.164	-	
nouser	No user	No User	cosyslinux	192.168.100.194	-	

9.9. 온라인 장치

시스템의 컴퓨터에 연결된 장치 관련 정보를 제공합니다.

1 3 8 | Endpoint Protector | 사용 설명서

The screenshot shows the 'Endpoint Protector' interface with the 'Reporting and Analysis - Online Device List' report selected. The left sidebar includes sections like Dashboard, Device Management, eDiscovery, Denylists and Allowlists, and Reporting & Analysis. The main area displays a table of online devices with columns for Computer Name, User Name, Device Type, VID, and MAC Address. Filter options and export buttons (Excel, PDF, CSV) are available at the top of the table.

관리자는 어떤 장치가 어느 컴퓨터에 연결되어 있고 이 장치에 액세스하고 있는 클라이언트 사용자가 누구인지 확인할 수 있습니다. 또한 "로그 보기" 및 "권한 관리" 작업 버튼을 사용하여 장치를 신속하게 관리할 수 있습니다.

9.10. 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.

The screenshot shows the 'Endpoint Protector' interface with the 'Statistics' report selected. The left sidebar includes sections like Dashboard, Device Management, eDiscovery, Denylists and Allowlists, and Reporting & Analysis. The main area displays a table with columns for Report Type (Report Type: Current Active Devices), Date (Date: Yesterday), and Device (Device). A search bar and a 'Filter Apply' button are present above the table.

10. 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.

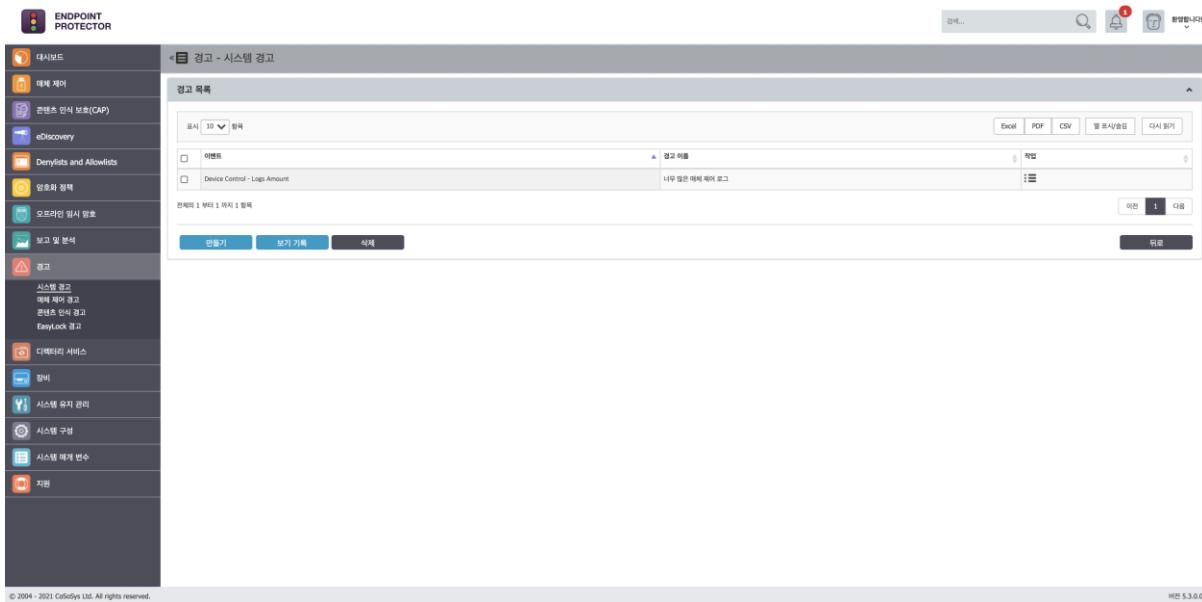
이메일 서버 설정		
<small>*참고: 관리자 계정에 이메일 정보가 없습니다. 다음 메뉴에서 이메일 주소 설정을 해야만 합니다. 시스템 관리자 > 동작 > 수정.</small>		
이메일 유형:	SMTP	
호스트 이름:	localhost	예: smtp.cososys.com
SMTP 포트:	25	예: 25 (Gmail은 SSL의 경우 포트 465를 사용하고 TLS/STARTTLS의 경우 포트 587를 사용합니다)
SMTP 인증 필요:	<input type="checkbox"/>	
사용자명:		
암호:		
암호화 형식:	None 예: 없음, SSL, TLS/STARTTLS.	
내 계정으로 테스트 이메일 보내기:	<input type="checkbox"/>	
<small>*참고: Endpoint Protector 서버는 이 기능을 위해서 작동하는 인터넷 연결을 필요로 합니다.</small>		

프록시 서버 설정		
프록시 유형:	없음	
인증 방식:	Basic	
IP 및 포트:	예: 192.168.0.1:8080	
사용자명:		
암호:		
<small>*참고: 이 정보는 프록시 서버가 구성된 네트워크를 참조하여 Endpoint Protector Live Update로의 액세스를 허용합니다.</small>		
<input type="button" value="Test"/>		

정보

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

10.1. 시스템 경고

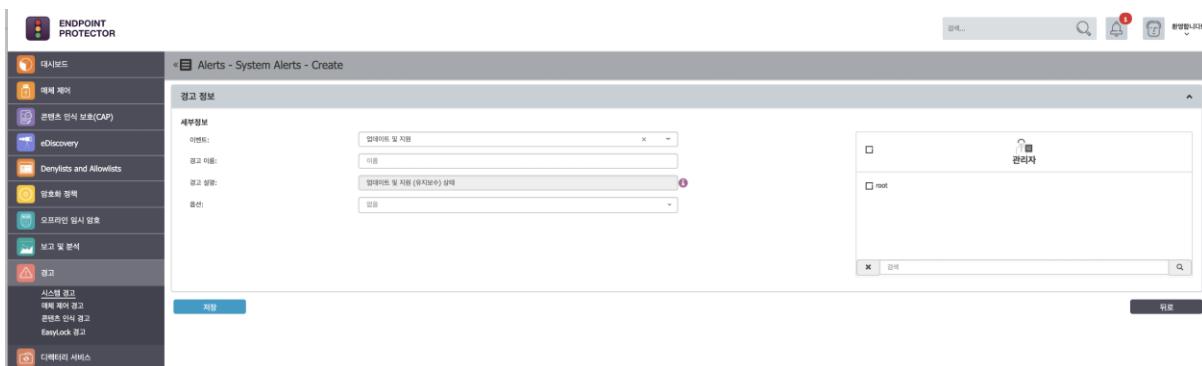


새 경고를 생성하려면 "시스템 경고 정의"로 이동한 후 "생성"을 클릭합니다.

10.1.1. 시스템 경고 만들기

시스템 경고를 새로 만들 때 아래 정보가 정의되어야 합니다.

- 이벤트** – 경고를 만드는 이벤트 유형 (APNS 인증서, 업데이트 및 지원, 클라이언트 삭제 등)



- 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.

- **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 때마다 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 확인하기 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.
- **온라인에서 안 보임** – 보호되는 엔드포인트가 특정 시간 동안 온라인에서 보이지 않으면 경고가 각 관리자에게 보내집니다. 이것은 또한 Endpoint Protector 클라이언트가 삭제될 수 있는 컴퓨터를 식별하는데 사용할 수 있습니다.

참고

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

10.1.2. 시스템 경고 기록

시스템 경고 기록은 감사에 사용할 수 있습니다. 시스템 경고가 일어나 이벤트는 모두 여기에 저장 됩니다. 관리자는 필터를 이용하여 더 쉽게 검색할 수 있습니다. 더 이상 로그가 필요 없다면 “기록 삭제” 버튼을 누릅니다.

10.2. 매체 제어 경고

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

새로운 경고를 생성하기 위해서는 “경고 정의”로 가서 “만들기” 버튼을 클릭하시기 바랍니다.

10.2.1. 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
- 모니터링 객체** – 이벤트를 만드는 그룹, 컴퓨터 또는 사용자
- 수신자** – 경고를 수신해야 하는 관리자

10.2.2. 매체 제어 경고 기록

매체 제어 경고 기록은 감사에 사용할 수 있습니다. 시스템 경고가 일어나 이벤트는 모두 여기에 저장 됩니다. 관리자는 필터를 이용하여 더 쉽게 검색할 수 있습니다. 더 이상 로그가 필요 없다면 “기록 삭제” 버튼을 누릅니다.

10.3. 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.

10.3.1. 콘텐츠 인식 경고 만들기

새로운 콘텐츠 인식 경고를 만들기 위해서는 아래 정보가 정의되어야 합니다.

- 이벤트** – 경고를 만드는 이벤트 유형 (콘텐츠 위협 탐지 또는 콘텐츠 위협 차단)
- 경고 이름** – 경고의 이름
- 모니터링 객체** – 이벤트를 만드는 그룹, 컴퓨터 또는 사용자
- 수신자** – 경고를 받아야 하는 관리자

참고

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

10.3.2. 콘텐츠 인식 경고 기록

콘텐츠 인식 경고 기록은 감사에 사용할 수 있습니다. 콘텐츠 인식 경고가 일어나 이벤트는 모두 여기에 저장 됩니다. 관리자는 필터를 이용하여 더 쉽게 검색할 수 있습니다. 더 이상 로그가 필요 없다면 “기록 삭제” 버튼을 누릅니다.

The screenshot shows the Endpoint Protector software interface. On the left is a sidebar with various icons and sections: Dashboard, Device, Content Awareness (selected), eDiscovery, File Locks & Hashes, Password Protection, Mobile Device Management, Offline Emergency Lock, and Reporting. Below these are sections for Alerts, Directories, Configuration, System Metrics, System Settings, Support, and Help. The main area is titled 'Content Awareness' and contains a search bar, a bell icon, and a refresh button. A message at the top right says '환영합니다' and '자원팀'. The main content area has a table header with columns: 이벤트 이름, 컴퓨터, 플레이언트 이름, 콘텐츠 정책, 대상 유형, 대상, 파일 이름, 일치한 항목, 항목 세부정보, 이벤트 시간, 날짜/시간 (플레이언트), 생성된 경고, and 세부정보 보기. Below the table is a search bar with placeholder '결과 찾기' and a '검색...' button. At the bottom are buttons for '이전' and '다음' pages, and a total count of '1 of 1'.

10.4. EasyLock 경고

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



새 EasyLock 경고를 생성하려면 “경고 > EasyLock 경고” 이동한 후 “만들기” 버튼을 클릭 합니다.

10.4.1 EasyLock 경고 만들기

새로운 EasyLock 경고를 만들 때 아래 정보 정의가 필요합니다.

- 이벤트** – 경고가 만들어지는 이벤트 유형 (메시지 보내기, 마스터 암호 변경, 장치 초기화, 설정 변경 등)
- 경고 이름** – 경고의 이름
- 수신자** – 경고를 받아야 하는 관리자



10.4.2 EasyLock 경고 기록

EasyLock 경고 기록은 감사에 사용할 수 있습니다. EasyLock 경고가 일어나 이벤트는 모두 여기에 저장 됩니다. 관리자는 필터를 이용하여 더 쉽게 검색할 수 있습니다. 더 이상 로그가 필요 없다면 “기록 삭제” 버튼을 누릅니다

The screenshot shows the Endpoint Protector software interface. On the left is a vertical navigation menu with icons and labels for various features: 대시보드 (Dashboard), 새제 제이 (New Agent), 콘텐츠 인식 보호(CAP), eDiscovery, 블랙리스트 및 화이트리스트, 암호화 검색, 모바일 기기 관리(MDM), 오프라인 임시 암호, 보고 및 분석, 경고. The '경고' section is currently selected. On the right, the main window title is 'EasyLock 경고 기록'. It includes a search bar, a filter button, and a message '결과 없음'. Below the search bar are buttons for '검색...' (Search...), '닫기' (Close), and '활용합니다' (Useful). A '지원팀' (Support Team) link is also present. At the bottom of the window, there is a footer with copyright information: '© 2004 - 2017 CoSoSys Ltd. All rights reserved.' and '버전 5.0.0.0'.

11. 디렉터리 서비스

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

The screenshot shows the Endpoint Protector web interface. On the left is a sidebar with various icons and sections: 대시보드, 매체 제어, 콘텐츠 인식 보호(CAP), eDiscovery, 거부목록 및 허용목록, 암호화 정책, 오프라인 임시 암호, 보고 및 분석, 경고, 디렉터리 서비스 (selected), Microsoft Active Directory, Azure Active Directory, 장비, 시스템 유지 관리, 시스템 구성, 시스템 메개 변수, and 지원. The main content area has a header '« ■ 디렉터리 서비스 - 동기화'. Below it is a '새 연결' (New Connection) form with fields for '이름:' (Name: 동기화 이름), '설명:' (Description: 동기화 설명), '연결 종류:' (Connection Type: 표준), '서버:' (Server: 예: WServer2018 또는 192.168.0.2), '포트:' (Port: 예: 389), '기본 검색 경로:' (Default Search Path: 예: OU=Deployed,DC=cososys,DC=cor), '사용자명:' (Username: 사용자명), and '암호:' (Password: 암호). There are '만들기' (Create) and '확인' (Confirm) buttons. Below this is a '동기화' (Sync) section with a table header: 표시 (10), 항목 (Items), 설명 (Description), 연결 종류 (Connection Type), 서버 (Server), 포트 (Port), 기본 검색 경로 (Default Search Path), 사용자명 (Username), 마지막 동기화 (Last Sync), and 작업 (Action). A note says '테이블에 데이터가 없음' (No data in the table). At the bottom are '이전' (Previous) and '다음' (Next) buttons, and a large '삭제' (Delete) button.

11.1. 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.

팁

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.

1 5 2 | Endpoint Protector | 사용 설명서

The screenshot shows the 'Endpoint PROTECTOR' application interface. On the left is a sidebar with various menu items: Dashboard, Device Control, Content Aware Protection, eDiscovery, Blacklists and Whitelists, Enforced Encryption, Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Synchronization, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main area is titled 'Directory Services - Edit Synchronization - qaapp'. It contains two tabs: 'Connection Details & Synchronization Options' and 'Advanced Groups Filter'. The 'Connection Details & Synchronization Options' tab shows fields for Name (qaapp), Connection Type (Standard), Port (389), Username (qaapp\qaoff), New Password (New Password), Synchronization Interval (6 hours), Description (Description 5), Server (192.168.7.182), Base Search Path (DC=qaapp,DC=com), Current Password (Current Password), and Confirm Password (Confirm Password). The 'Advanced Groups Filter' tab has an 'On' switch for 'Group Filter' and a 'Save' button. Below these tabs is a 'Directory Browser' section with a search bar and a tree view of directory objects like BuiltIn, Computers, Domain Controllers, ForeignSecurityPrincipals, Groups, Infrastructure, Keys, LostAndFound, and Managed Service Accounts. To the right of the browser is an 'Entity Details' panel with fields for Name (LostAndFound), Type (Container), Path (CN=LostAndFound,DC=qaapp,DC=com), and Description (Default container for orphaned objects). The bottom right corner of the main window displays 'Version 5.2.0.0'.

팁

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

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

The screenshot shows the 'Directory Browser' page. On the left is a tree view of directory objects under 'Search'. The 'LostAndFound' node is selected and highlighted with a blue background. To the right is an 'Entity Details' panel with fields for Name (LostAndFound), Type (Container), Path (CN=LostAndFound,DC=qaapp,DC=com), and Description (Default container for orphaned objects). At the bottom left of the browser area is a 'Save to Sync' button.

객체를 선택하고 동기화 저장을 할 수 있습니다.

Synchronized Entities					
Filters ▾					
	Server	User	Synchronization Interval	Path	Actions
■	192.168.7.182	qaeppliosif	6 hours	OU=Groups,DC=qaapp,DC=com	☰
■	192.168.7.182	qaeppliosif	6 hours	CN=ForeignSecurityPrincipals,DC=qaapp,DC=com	☰
■	192.168.7.182	qaeppliosif	6 hours	CN=Schema Admins,CN=Users,DC=qaapp,DC=com	☰
■	192.168.7.182	qaeppliosif	6 hours	CN=Enterprise Admins,CN=Users,DC=qaapp,DC=com	☰

Showing 1 to 4 of 4 entries

Previous 1 Next

[Delete](#)

11.2. 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.

예제:

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;

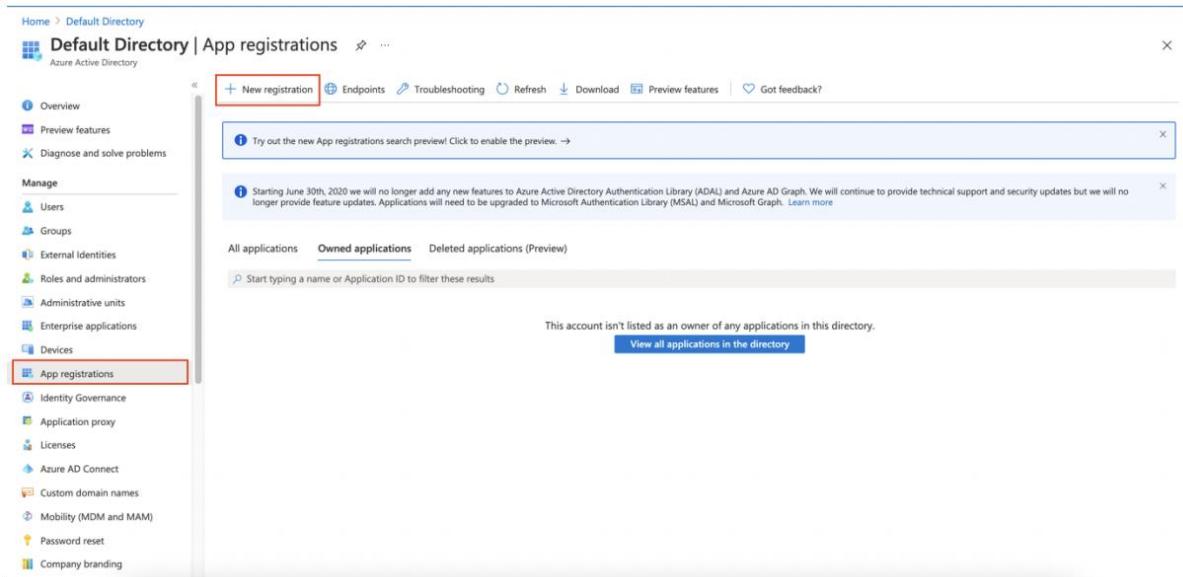
Azure Active Directory 설정을 위한 구성 단계:

I. Azure Active Directory에서 응용프로그램 만들기

1. Azure Portal 로그인

2. Azure Active Directory 탐색

3. 왼쪽의 Active Directory 메뉴에서 Manage 섹션의 App Registrations을 클릭 후 New Registration을 클릭합니다.



4. Registration 페이지가 열리면 아래 내용을 나옵니다:

4.1. 이름

4.2. 지원되는 계정 유형: Selected Default Directory

! Redirect URI 완성하지 마세요.

4.3. Register 버튼 클릭

Home > Default Directory >

Register an application

Name
The user-facing display name for this application (this can be changed later).
[]

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 Web e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the Microsoft Platform Policies [\[?\]](#)

Register

5. Essentials 섹션에서 다음 정보를 저장합니다:

5.1. Application (client) ID는 Endpoint Protector 서버에서 Application (client) ID 항목에 추가할 때 필요할 것입니다.

5.2. Directory (tenant) ID는 Endpoint Protector 서버에서 Tenant ID 항목에 추가할 때 필요할 것입니다.

Home > Default Directory >

Test Application

Search (Cmd+ /) < Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

- Application (client) ID : be17afc-c92c-4ef4-b861-678448f3ec19
- Object ID : 4861ffb5-fdf3-4ab2-ba34-3af5906c2a901
- Directory (tenant) ID : 1def8742-8c49-497a-a304-1019540da191

Client credentials : Add a certificate or secret.
 Redirect URIs : Add a Redirect URI
 Application ID URI : Add an Application ID URI
 Managed application in ... : Test Application

Supported account types : My organization only

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

II. 응용프로그램의 비밀 ID 만들기

정보

비밀 ID는 Graph API로 응용프로그램에 접근하는 인가 방법으로 사용됩니다.

1. 관리 섹션의 측면에 있는 Certificates & Secrets 클릭

The screenshot shows the Azure portal's 'Default Directory' section for a 'Test Application'. The 'Certificates & secrets' link in the left sidebar is highlighted with a red box. The main pane displays the application's details, including its display name, client ID, object ID, and directory ID. A note at the bottom states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph.' Below this note, there are 'Get Started' and 'Documentation' links, and a section titled 'Build your application with the Microsoft identity platform'.

2. Certificates & Secrets 페이지에 New client secret 버튼 클릭

The screenshot shows the 'Certificates & Secrets' page for the 'Test Application'. The '+ New client secret' button in the 'Client secrets' section is highlighted with a red box. The page also includes sections for 'Certificates' and 'Client secrets', both of which are currently empty. The left sidebar shows the 'Certificates & secrets' link is also highlighted with a red box.

3. secret ID의 Enter a Description

The screenshot shows the Azure portal's 'Certificates & secrets' page for a 'Test Application'. On the left, there's a sidebar with various management options like Overview, Quickstart, Integration assistant, Manage, and Certificates & secrets (which is currently selected). The main area displays sections for 'Certificates' and 'Client secrets'. Under 'Client secrets', there's a table with one row: '+ New client secret'. A modal window titled 'Add a client secret' is overlaid on the page. It contains fields for 'Description' (with placeholder 'Enter a description for this client secret') and 'Expires' (set to 'Recommended: 6 months'). At the bottom of the modal are 'Add' and 'Cancel' buttons.

4. Add 및 Add a client secret section 클릭

This screenshot is similar to the previous one, showing the 'Certificates & secrets' page for the 'Test Application'. The 'Certificates & secrets' section is selected in the sidebar. A modal window titled 'Add a client secret' is open, with the 'Add' button highlighted by a red box. The fields for 'Description' and 'Expires' are visible but not filled in this view.

5. 나중에 더 필요하기 때문에 Secret ID 값을 기록하고 클립보드에 복사하고 안전하게 저장합니다.

정보

뒤로 가기를 하면 secret ID는 마스팅 처리될 것입니다.

158 | Endpoint Protector | 사용 설명서

The screenshot shows the Azure portal interface for managing a 'Test Application'. The left sidebar has a 'Certificates & secrets' section selected. The main area displays a table for client secrets. One row is highlighted with a red box around the 'Value' column, which contains the value '3yAk-9je7Env-xaV.Gm1N43VB1.hgp6AOI'. The table columns are: Description, Expires, Value, and Secret ID.

Description	Expires	Value	Secret ID
Client Secret Description	1/22/2022	3yAk-9je7Env-xaV.Gm1N43VB1.hgp6AOI	644ff38a-b82e-4873-9a6d-e9b43f5dff0

III. Graph API 를 사용하여 사용자 / 그룹 만들기

1. Home 클릭 -> Azure Active Directory

This screenshot is identical to the one above, showing the 'Certificates & secrets' section for the 'Test Application'. The 'Value' column of the client secret table is again highlighted with a red box, containing the value '3yAk-9je7Env-xaV.Gm1N43VB1.hgp6AOI'.

Welcome to Azure!

Don't have a subscription? Check out the following options:

- Start with an Azure free trial**: Get \$200 free credit toward Azure products and services, plus 12 months of popular free services. [Start](#) [Learn more](#)
- Manage Azure Active Directory**: Manage access, set smart policies, and enhance security with Azure Active Directory. [View](#) [Learn more](#)
- Access student benefits**: Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status. [Explore](#) [Learn more](#)

Azure services

- Create a resource**
- Azure Active Directory** (highlighted with a red box)
- App Services**
- All resources**
- Azure Cosmos DB**
- Quickstart Center**
- Virtual machines**
- Storage accounts**
- SQL databases**
- More services**

Navigate

- Subscriptions**
- Resource groups**
- All resources**
- Dashboard**

2. Default Directory | Overview 페이지에서 Add 버튼 클릭

Home > Default Directory | Overview

Add (highlighted with a red box) | Manage tenants | What's new | Preview features | Got feedback?

User

Tutorials

Name	Default Directory	Users	49,471
Tenant ID	1def8742-8c49-497a-a304-1019540da191	Groups	122
Primary domain	testazureqendpointprotect.onmicrosoft.com	Applications	45
License	Azure AD Free	Devices	0

My feed

- Julia Stoica**: 928bdadf-b139-467e-8029-c513dced3e96 (Global administrator and 5 other roles) [More info](#)
- TLS 1.0, 1.1 and 3DES deprecation**: Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients/applications/platform to avoid any service impact.
- Azure AD Connect**: Enabled (Last sync was more than 1 day ago)
- Secure Score for Identity**: 3.85% (Secure score updates can take up to 48 hours.)

3. Add User 클릭

The screenshot shows the Azure Active Directory Default Directory Overview page. On the left, there's a navigation sidebar with various options like Overview, Preview features, Diagnose and solve problems, Manage, Users, Groups, External identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, and Company branding. A red box highlights the 'User' option under the 'Add' dropdown menu at the top center. The main area displays statistics: Name (Default Directory), Tenant ID (1def8742-8c49-497a-a304-1019540da191), Primary domain (testazureqendpointproto.onmicrosoft.com), License (Azure AD Free). Below this is a 'My feed' section with items for Julia Stoica and Azure AD Connect, followed by a warning about TLS deprecation and a secure score summary.

3.1. Create User 선택

3.2. Username에서 Domain 선택

3.3. Name 들어가기

3.4. Auto-generate password 를 클릭하거나 직접 만들기

3.5. Department 추가

3.6. Create 클릭

The screenshot shows the 'New user' creation form. It has two radio button options: 'Create user' (selected) and 'Invite user'. The 'Create user' section contains instructions: 'Create a new user in your organization, have a user name like alice@testazureqendpointproto.on' and 'I want to create users in bulk'. Below this is a 'Help me decide' link. The 'Identity' section requires filling in 'User name*' (set to 'User'), 'Name*', 'First name' (set to 'Test'), and 'Last name'. The 'Password' section includes an 'Auto-generate password' checkbox and a 'Create' button at the bottom.

4. 스텝 1과 2를 반복하고 Group 클릭

- 4.1. 그룹 보안 유형 선택
- 4.2. 그룹 이름으로 가기
- 4.3. 멤버쉽 추가를 위해 선택된 멤버 없음 클릭
- 4.4. 새롭게 만들어진 사용자 검색 그리고 Select 클릭

The screenshot shows a 'New Group' creation form. At the top, there are navigation links: 'Home > Default Directory > New Group ...'. On the right side, there is a close button (X). The form fields are as follows:

- Group type ***: A dropdown menu showing 'Security'.
- Group name ***: An input field containing 'Group'.
- Group description**: An input field containing 'description'.
- Membership type**: A dropdown menu showing 'Assigned'.
- Owners**: A note stating 'No owners selected'.
- Members**: A note stating 'No members selected'.

At the bottom left, there is a blue 'Create' button.

IV. 응용프로그램 승인 추가하기

응용프로그램에 추가되는 승인:

- ⑩ Directory.ReadWrite.All
- ⑩ Group.ReadWrite.All
- ⑩ User.ReadWrite.All

만들어진 응용프로그램이 열리는지 확인하고 다음을 진행합니다:

1. API Permissions 클릭

1 6 2 | Endpoint Protector | 사용 설명서

The screenshot shows the Microsoft Azure portal interface for a 'Test Application'. The left sidebar includes links for Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions), App roles, Owners, Roles and administrators, Manifest, Support + Troubleshooting (Troubleshooting, New support request), and Get Started Documentation.

The main content area displays the application's details under the 'Essentials' tab:

Display name	: Test Application	Client credentials	: Add a certificate or secret
Application (client) ID	: f8935dbb-e249-4bdf-98a0-2ab2419126e1	Redirect URIs	: Add a Redirect URI
Object ID	: 851abdff-907d-4f93-9d90-950201b7c214	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 1def8742-8c49-497a-a304-1019540da191	Managed application in L...	: Test Application
Supported account types	: My organization only		

A note at the bottom states: "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more".

The right side features a section titled 'Build your application with the Microsoft identity platform' with icons for various Microsoft services like Excel, SharePoint, OneDrive, and Power BI.

2. Add a Permission 클릭

The screenshot shows the 'Test Application | API permissions' page. The left sidebar is identical to the previous screenshot.

The main content area shows the 'Configured permissions' section:

The 'Admin consent required' column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

Add a permission button (highlighted with a red box)

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

To view and manage permissions and user consent, try Enterprise applications.

3. Microsoft Graph 클릭

1 6 3 | Endpoint Protector | 사용 설명서

The screenshot shows the Azure portal interface. On the left, the 'Test Application' blade is open, specifically the 'API permissions' section under 'Manage'. It displays a table with one row: 'No permissions added'. A button '+ Add a permission' is visible. To the right, a modal window titled 'Request API permissions' is displayed. The 'Microsoft APIs' tab is selected. Under 'Commonly used Microsoft APIs', the 'Microsoft Graph' card is highlighted with a red border. Other cards include 'Azure Service Management', 'Azure Storage', 'Dynamics 365 Business Central', 'Office 365 Management APIs', 'SharePoint', and 'Skype for Business'. Below this section, there are more cards for 'Azure Batch', 'Azure Cosmos DB', and 'Azure Data Catalog'. At the bottom of the modal, there are buttons for 'Add permissions' and 'Discard'.

4. Application Permissions 클릭

This screenshot is similar to the previous one, showing the 'Test Application | API permissions' page and the 'Request API permissions' modal. The 'Microsoft Graph' card in the modal is also highlighted with a red border. The 'Application permissions' section is visible, stating: 'Your application needs to access the API as the signed-in user.' At the bottom of the modal, there are buttons for 'Add permissions' and 'Discard'.

5. 위에서 언급된 승인을 검색하고 각각의 승인을 확인합니다. (Directory.ReadWrite.All, Group.ReadWrite.All, User.ReadWrite.All)

1 6 4 | Endpoint Protector | 사용 설명서

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Test Application | API permissions' page is displayed. It includes a sidebar with options like Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration), API permissions (selected), and Support + Troubleshooting. The main area shows 'Configured permissions' with a note about admin consent required. A table lists 'API / Permissions name', 'Type', and 'Description'. Below it, a note says 'To view and manage permissions and user consent, try Enterprise applications.' On the right, a 'Request API permissions' dialog box is open for 'Microsoft Graph'. It shows 'Delegated permissions' and 'Application permissions' sections. Under 'Select permissions', 'direc' is typed into a search bar. The results show two options under 'Directory (I)': 'Directory.Read.All' (radio button) and 'Directory.ReadWrite.All' (checkbox checked). Both have 'Yes' next to them. At the bottom of the dialog are 'Add permissions' and 'Discard' buttons.

6. Add Permissions 클릭

This screenshot is similar to the one above, showing the 'Test Application | API permissions' page and the 'Request API permissions' dialog box for Microsoft Graph. The 'Add permissions' button at the bottom of the dialog box is highlighted with a red border.

7. API Permission 페이지에서 Grant admin consent for Default Directory 버튼을 클릭

The screenshot shows the 'Test Application | API permissions' page in the Azure portal. On the left, there's a sidebar with options like Overview, Quickstart, Integration assistant, Manage (selected), API permissions (selected), Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main area is titled 'Configured permissions' and lists three permissions under 'Microsoft Graph (3)': Directory.ReadWrite.All, Group.ReadWrite.All, and User.ReadWrite.All. Each permission has a 'Type' (Application), 'Description', 'Admin consent req...', and 'Status' (Not granted for Default...). A note at the bottom says 'To view and manage permissions and user consent, try Enterprise applications.'

V. Endpoint Protector 서버에 Graph Application 추가하기

1. 'Endpoint Protector 서버 -> 디렉터리 서비스 -> Azure Active Directory' 이동
2. API Consumer 추가를 위해 추가 버튼 클릭

정보

하나의 API Consumer는 다중 동기화 작업에 사용될 수 있습니다.

The screenshot shows the 'Directory Services - Azure Active Directory' page in the Endpoint Protector web interface. The left sidebar includes options like Dashboard, Device Control, Content Aware Protection, eDiscovery, Denylists and Allowlists, Enforced Encryption, Offline Temporary Password, Reports and Analysis, Alerts, and several items under 'Directory Services' (highlighted with a red box) such as Microsoft Active Directory and Azure Active Directory. The main content area is titled 'API Consumers' and shows a table with columns: Name, Description, Tenant ID, Client ID, and Actions. A large 'Add' button is highlighted with a red box. Below the table, there are input fields for Name, Description, Tenant ID, Application (Client) ID, and Client Secret Value, along with Test and Cancel buttons. At the bottom, there's a 'Synchronization jobs' section with a 'Filters' dropdown and a table with columns: Show, Name, Description, Tenant ID, Client ID, and Actions.

3. 상세 정보 완성하기

3.1 이름 추가

3.2 설명 추가

3.3 Tenant ID 영역에 미리 저장한 Directory (tenant) ID 추가

3.4 Application (Client) ID 영역에 미리 저장한 Application (client) ID 추가

3.5 Client Secret Value 영역에 미리 저장한 Secret ID 추가

The screenshot shows the 'API Consumers' section of the Endpoint Protector interface. On the left sidebar, 'Directory Services' is selected under 'Microsoft Active Directory'. The main area displays a table with columns: Name, Description, Tenant ID, Client ID, and Actions. A new entry is being added with the following values:

Name	Description	Tenant ID	Client ID	Actions
Test	Description	1def8742-8c49-497a-a304-1019540da191	beta7afc-c92c-4ef4-b861-67b448f3ec19	<button>Test</button> <button>Cancel</button>

Below the table, there is a 'Synchronization jobs' section with a 'Filters' dropdown and a table with columns: Name, Description, Status, Last Sync, and Actions.

4. 테스트 버튼 클릭

5. 저장 버튼 클릭

The screenshot shows the 'API Consumers' section of the Endpoint Protector interface. A new consumer is being created with the following details:

Name:	Test
Description:	Description
Tenant ID:	1def8742-8c49-497a-a304-1019540da191
Application (Client) ID:	be1a7afc-c92c-4ef4-b861-678448f3ec19
Client Secret Value:	3yA6-9y7Em:xaV.Gm1N43V81.hg06AOI

Buttons at the bottom of the form include 'Save', 'Test', and 'Cancel'. The 'Save' button is highlighted with a red box.

VI. Endpoint Protector 서버에서 동기화 작업 만들기

1. 동기화 작업 만들기 클릭

The screenshot shows the 'Synchronization jobs' section of the Endpoint Protector interface. A new sync job is being created with the following details:

Name:	Test
Description:	
API Consumer:	Test
Synchronization Interval:	
Last Synchronization:	

Buttons at the bottom of the form include 'Create Sync Job' and 'Delete'. The 'Create Sync Job' button is highlighted with a red box.

2. 동기화 옵션 완성하기

2.1. 이름 입력

2.2. 설명 입력

2.3. 만들어진 API Consumer 선택

2.4. 동기화 간격 선택

3. 저장 버튼 클릭

The screenshot shows the 'Azure Active Directory - Synchronization Job' configuration screen. On the left, a sidebar lists various features like Dashboard, Device Control, Content Aware Protection, eDiscovery, Denylists and Allowlists, Enforced Encryption, Reports and Analysis, Alerts, and more. The main area has two tabs: 'Synchronization Options' and 'Directory Browser'. Under 'Synchronization Options', there are fields for 'Name' (set to 'Test'), 'API Consumer' (set to 'GraphAPI Consumer'), and 'Synchronization Interval' (set to '6 hours'). A prominent red box highlights the 'Save' button. Below this is the 'Directory Browser' tab, which displays a table for 'Synchronized Entities'. The table has columns for Entity Name, Description, Entity Id, Synchronization Interval, Last Synchronization, and Actions. A note at the bottom says 'No matching records found'. At the bottom right of the browser section is a 'Delete' button.

12. 장비

12.1. 서버 정보

이 화면은 관리자에게 서버, 장애 조치, 총 디스크 사용 및 동작 시간 등의 일반 정보를 제공 합니다.

The screenshot shows the 'Endpoint Protector' interface with the following details:

- Endpoint Protector 장비 - 시스템 정보**
- 시스템 상태(Poller) 상태:** N/A
- 디스크 공간**

시스템 디스크 공간:	3.6G - 4% - 99%
EPP 디스크 공간:	7.7G - 2% - 681G
디스크의 폴더:	4.0K 파일 위치 /var/zeppfiles/logo
디스크의 사용:	8.0K 파일 위치 /var/zeppfiles/shadows
- 디스크 공간 경고**

경고에서 제공하는 스토리지 자원의 95% 까지 사용한 경우면 시스템 유지 관리 범위에서 다음 작업 중 하나의 실행을 고려합니다. 시스템 유지 관리 범위는 하드웨어 및 하드웨어 부품을 고려합니다. 그 외에는 시스템 유지 관리 범위에서 다음 작업 중 하나의 실행을 고려합니다.

 - 오늘은 파일 체크 혹은 디스크 사용률을 통해 일부 문제를 해결하고 적절한 충전을 선택합니다.
 - 오늘은 파일 체크 혹은 디스크 사용률을 통해 일부 문제를 해결하고 적절한 충전을 선택합니다.
- 데이터베이스**

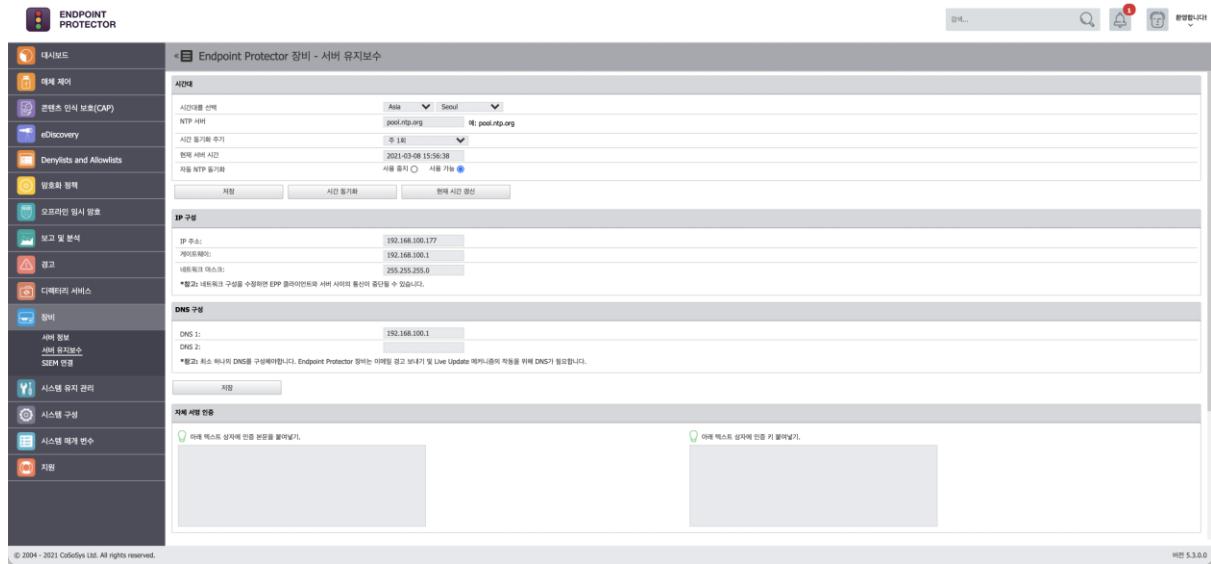
데이터 디스크 공간에 사용량:	19M 파일 위치 /var/lib/mysql/zeppdatabase
SQL 데이터 폴더 수:	70
수집된 파일의 수:	0
보관된 파일의 수:	0
- 시스템**

작동 시간:	15:50:02 up 4 days, 5:24, 0 users, load average: 0.07, 0.06, 0.09 - 1%, 5%, 15분 전
Linux 버전:	Ubuntu 14.04 LTS
시스템 정보 업데이트:	2021-Mar-08 15:50:02

底部信息: © 2004 - 2021 Cellebrite Ltd. All rights reserved. 版權所有 © 2004 - 2021 Cellebrite Ltd. All rights reserved.

12.2. 서버 유지보수

이 화면에서 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.



12.2.1. 시간대 설정

이 메뉴는 관리자가 선호 시간대와 기기의 NTP 서버 동기화 설정을 할 수 있도록 합니다.

저장 버튼을 누르면 모든 변경된 설정이 저장됩니다. 그러나 동기화 프로세스가 시작되지는 않습니다!

시간 동기화 버튼을 누르면 5분 후에 동기화가 시작됩니다. 5분 후에 여러분이 선택한 형식으로 경고 및 로그가 보고 됩니다.

시간 동기화 버튼을 누르면 아래 화면이 업데이트 됩니다.

현재 서버 시간

2018-01-12 16:09:15

참고

어플라이언스는 pool.ntp.org로 일주일에 한 번 동기화 되도록 기본 설정되어 있습니다.

12.2.2. 네트워크 설정

어플라이언스와 정확하게 통신하도록 네트워크 설정을 여기서 바꿀 수 있습니다.

주의

IP 주소를 변경한 후에 인터넷 브라우저를 닫고 새로운 창을 여시기 바랍니다. 그러면 Endpoint Protector 관리 및 보고 도구는 새로운 IP 주소로 액세스를 시도합니다.

12.2.3. 공장 초기화 어플라이언스 재설정

공장 초기화는 어플라이언스의 모든 설정, 정책, 인증 및 다른 데이터를 지웁니다. 공장 초기화가 되면 어플라이언스와 Endpoint Protector 클라이언트 사이의 모든 설정 및 통신이 차단됩니다.

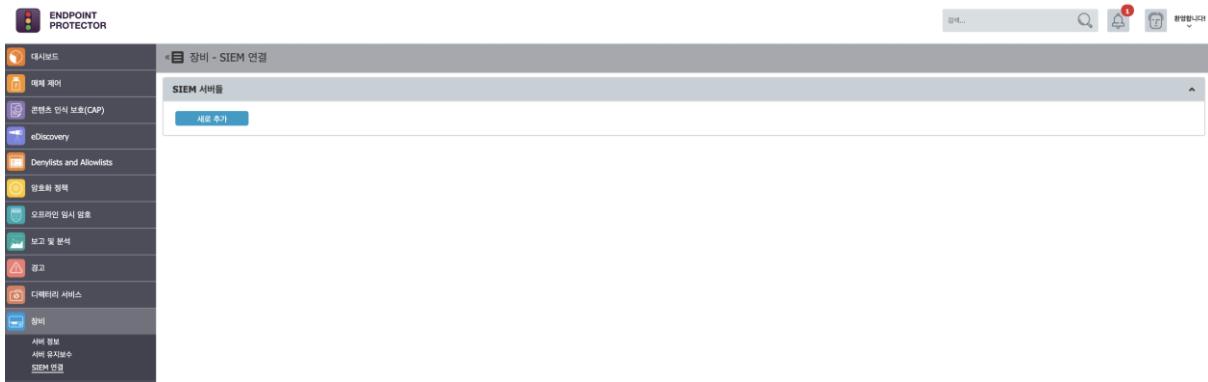
12.2.4. SSH 서버

이 옵션은 SSH 프로토콜을 통해서 어플라이언스에 접근을 사용 또는 사용하지 않음으로 설정할 수 있습니다. 지원 액세스 요청 전에는 "사용"을 선택하시기 바랍니다.

12.3. 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.

관리자는 장비 > SIEM 연결에서 관리할 수 있습니다.



새로운 SIEM 서버는 새로 추가 버튼을 클릭해서 추가할 수 있습니다. 이미 존재하는 정책은 더블 클릭으로 편집이 가능합니다.

정보

SIEM 서버 편집 또는 삭제 옵션은 원하는 정책을 선택한 후에 가능합니다.

SIEM 서버 설정에는 아래의 정보가 필요합니다.

서버 이름

서버 설명

서버 프로토콜 – UDP 또는 TCP

서버 포트

서버 IP

로그 유형 – SIEM 서버로 보내는 로그 유형

참고

로깅 사용 중지 옵션은 관리자가 Endpoint Protector에 로그를 보관하거나 SIEM 서버에만 보관할 때 사용합니다.

173 | Endpoint Protector | 사용 설명서

SIEM 연결 - 새로운 서버 추가

서버 정보

서버 상태: SIEM 상태:

서버 설정

서버 이름: [] 서버 IP: [] 서버 포트: []

서버 설명: [] 서버 포트: []

서버 포트번호: UDP 서버 포트: []

로그 정보 유형

SIEM 서버로 보내길 원하는 로그 유형을 선택하세요.

제작자 챠어: 시안팀 언급팀 TD 미니 설치 TD 설치 사용 허지 언급 참여팀 EasyLock - 베로 설치됨 TD 제작 1 사용 TD 제작 2 사용 TD 제작 3 사용

관련한 미시 보호(CAP): 혁신 혁신팀

eDiscovery: 보고된 파일

관련 모니터링 프로그램: AD 통지됨 관리자 작업 APNS 인증 클라이언트 정보 생산 클라이언트 무결성 생산 클라이언트 삭제 관리자 헬스 - 로그의 양 디제 혁신 챠어 - 로그 양 혁신모듈 리마인드 외부 저장소 접근도

저장

뒤로

© 2004 - 2021 Colodgy Ltd. All rights reserved. 버전 5.2.0.0

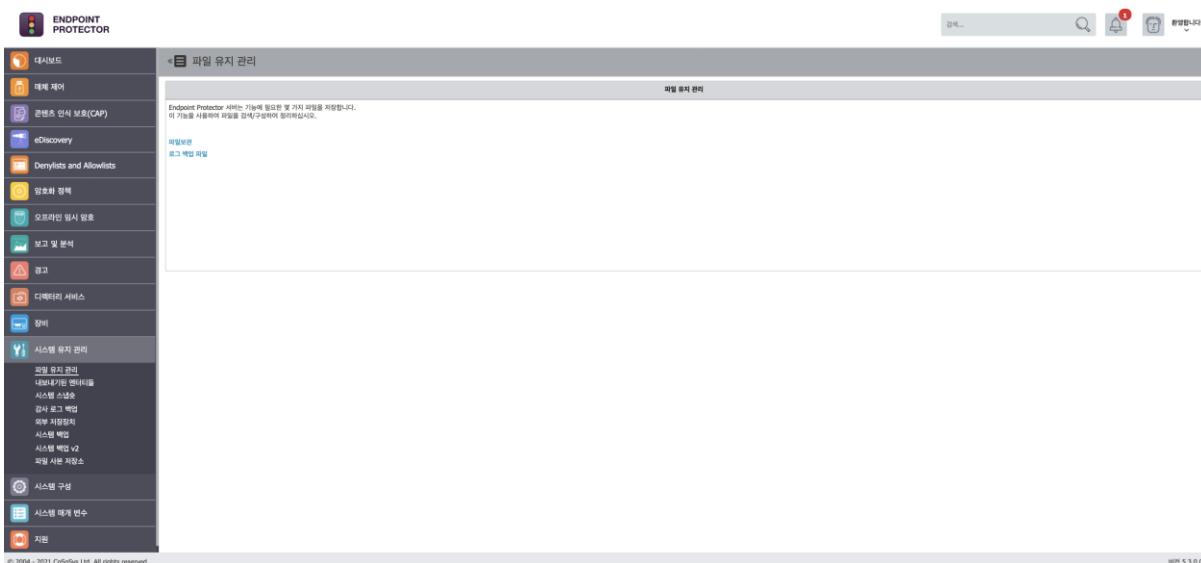
정보

SIEM 호스트의 최대 수는 4입니다.

13. 시스템 유지 관리

13.1. 파일 유지 관리

이 모듈은 관리자가 Endpoint Protector 서버에 사용된 파일을 검색/구성 및 정리할 수 있습니다.



- 임시 로그 파일:** 선택한 클라이언트 컴퓨터에서 로그 파일을 보관 및 삭제 할 수 있습니다.
- 파일 보관:** 선택한 클라이언트 컴퓨터에서 보관 파일을 보관 및 삭제 할 수 있습니다.
- 로그 백업 파일:** 이전에 백업된 로그 파일을 보관 및 삭제 할 수 있습니다.

이전에 선택한 파일 세트를 보관하려면 “Zip으로 저장” 버튼을 클릭하고, 파일 세트를 Endpoint Protector 서버에서 영구 삭제하려면 “삭제” 버튼을 사용합니다.

13.2. 객체 내보내기

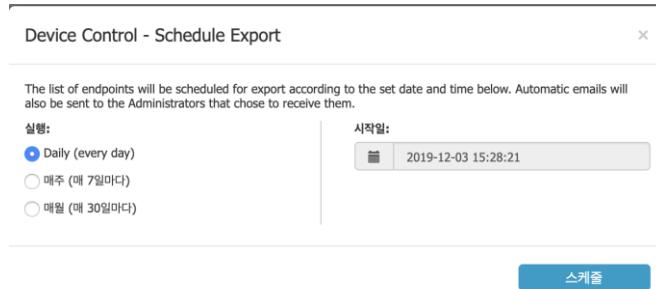
이 섹션에서 관리자는 내보낸 객체의 목록을 볼 수 있고 다운로드 또는 삭제 할 수도 있을 뿐만 아니라 시스템에서 내보내기 목록을 예약할 수 있습니다.

The screenshot shows the 'Endpoint PROTECTOR' dashboard. On the left sidebar, under 'System Usage Management', there is a 'Devices' section. The main content area is titled 'System Usage Management - Exported Entities'. It contains a sub-section 'Export' with a table header: 'Name', 'Type', 'Entity Name', 'Last Modified', and 'Actions'. There are filters for 'Name', 'Type', 'Entity Name', and 'Last Modified'. At the bottom right of the table, there are buttons for 'Excel', 'PDF', 'CSV', and 'Scheduled Export'.

정보

'매체 제어 > 장치 목록 / 컴퓨터 목록 / 사용자 목록 / 그룹 목록' 을 수동으로 만들거나 예약 설정으로 만들 수 있습니다.

The screenshot shows the 'Media Control' section of the 'Device' page. The left sidebar has a 'Media Control' section. The main content area is titled 'Media Control - Device'. It shows a table of devices with columns: 'Name', 'Type', 'Manufacturer', 'ID', 'Last Modified', and 'Actions'. A context menu is open over a device entry, showing options: 'Device Export (JSON)', 'Device Schedule Export (JSON)', and 'Delete'. At the bottom right of the table, there are buttons for 'Excel', 'PDF', 'CSV', and 'Scheduled Export'.

**팁**

예약 내보내기는 예약 내보내기 경고가 설정된 모든 관리자의 이메일에 자동으로 보내집니다.

참고

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.

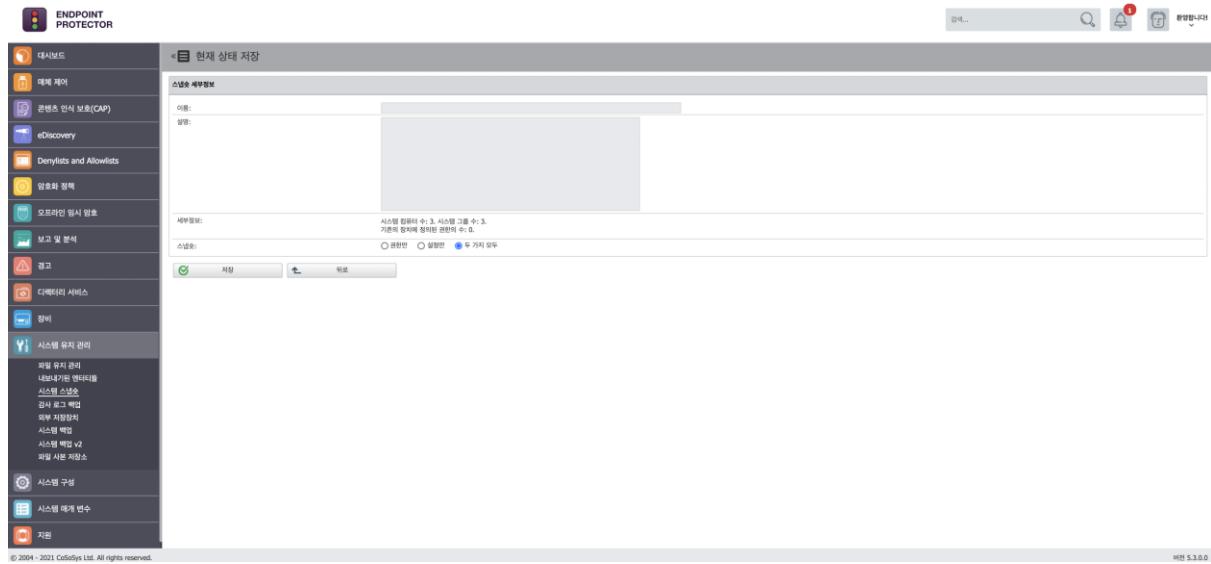
성능 관리 목적으로 예약된 내보내기와 로깅 사용 중지 옵션은 관리자가 Endpoint Protector 서버에 로그를 보관할 것인지 아니면 SIEM 서버에만 보관할지 결정할 수 있습니다.

13.3. 시스템 스냅숏

시스템 스냅샷 모듈에서는 모든 장치 제어 권한 및 설정을 시스템에 저장했다가 나중에 필요할 때 복원할 수 있습니다.

Endpoint Protector 5 서버를 설치한 후 변경하기 전에 시스템 스냅샷을 생성하는 것이 좋습니다. 그러면 서버를 잘못 구성하더라도 원래 설정으로 되돌릴 수 있습니다.

시스템 스냅샷을 생성하려면 "시스템 구성"에서 시스템 스냅샷 모듈로 이동한 후 "스냅숏 만들기"를 클릭합니다.

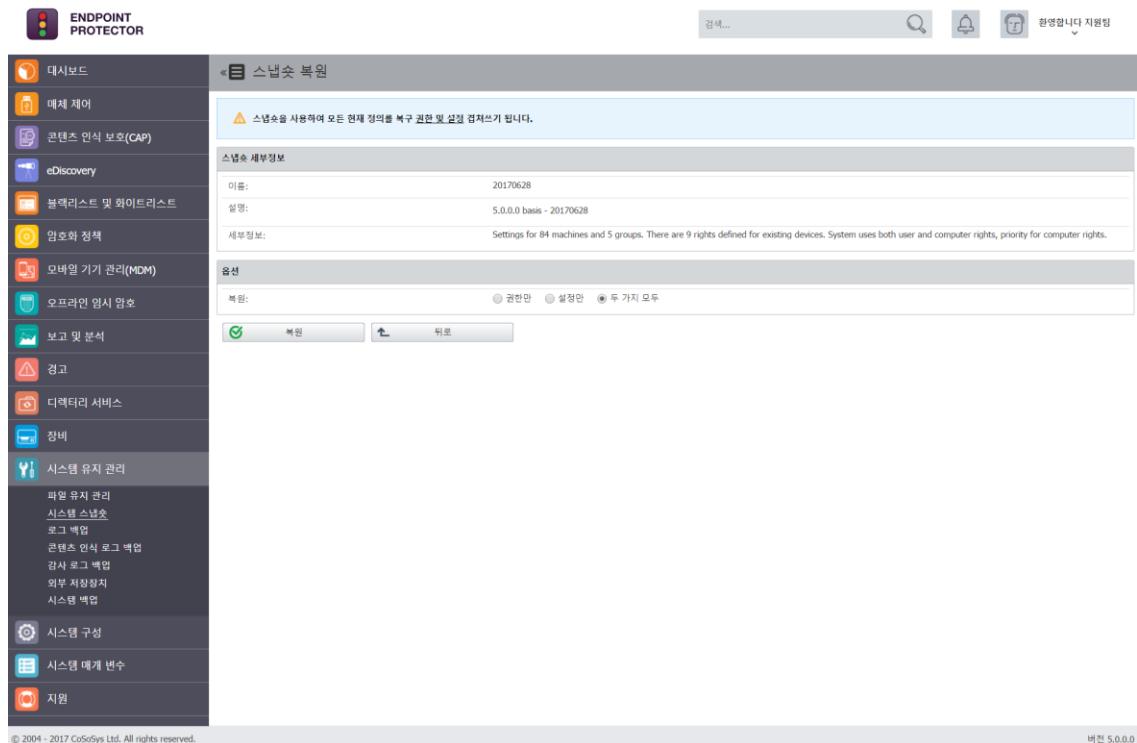


스냅샷 이름과 설명을 입력합니다. 또한 스냅샷에 저장할 항목을 권한만, 설정만 또는 둘 다 중에서 선택합니다.

시스템 스냅샷에 생성된 스냅샷이 나타납니다.

이전에 생성된 스냅샷을 복원하려면 원하는 스냅샷 옆에 있는 "복원" 버튼을 클릭합니다.

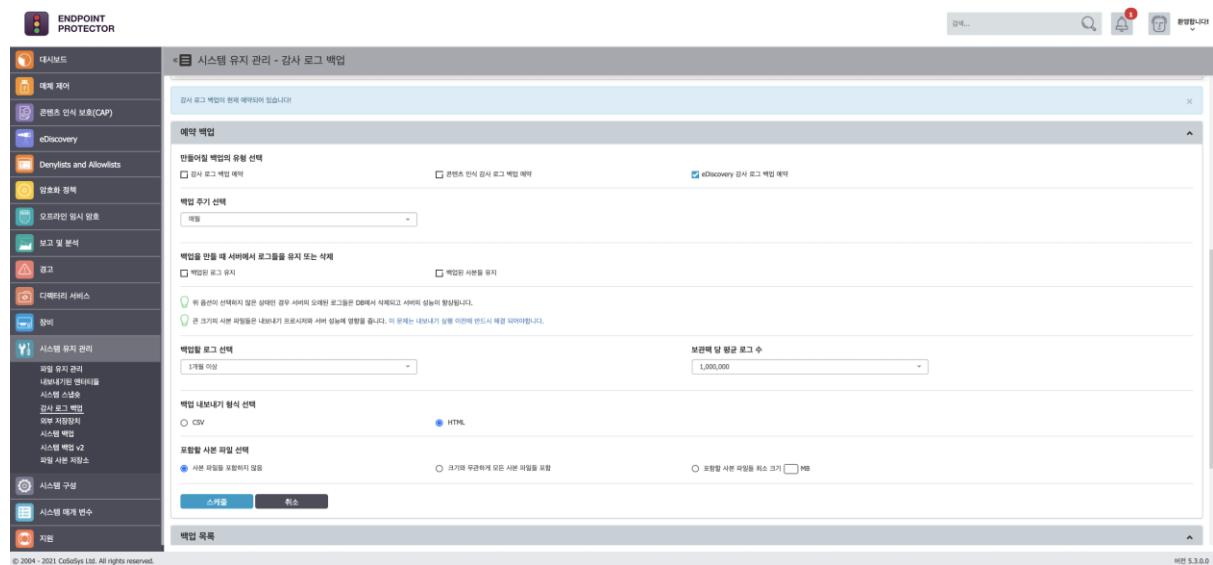
다음 창에서 "복원" 버튼을 다시 클릭하여 복원을 확인합니다.



13.4. 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 사실입니다. 이는 임원들이 쉽게 감사할 수 있는 리포트로 만듭니다.

179 | Endpoint Protector | 사용 설명서

ENDPOINT PROTECTOR | Logs Report

Logs | Filetrace | Shadows

Collection Shadow: 2019-01-28 17:22:13 - 2019-01-28 17:22:07

Show 25 entries

Username	Machine Name	Machine Ip	Filename	Filehash	FileSize(kb)	FileType	Event Time	Log	Action									
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:13	3701560558413078842										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078843										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078844										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078845										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078846										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078847										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078848										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078849										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078850										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078851										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078852										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078853										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078854										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078855										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078856										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078857										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078858										
andrei	ANDREIP-WIN10	192.168.15.34	1~ Copy (10) - Copy - Copy.txt	15530fb1a715e170e2235be14b0f71e	0.01		2019-01-28 17:22:14	3701560558413078859										
Showing 1 to 25 of 828 entries	Search Username	Search Machine Name	Search machine Ip	Search Filenames	Search Filehash	Search Filesize(kb)	Search FileType	Search Event Time	Search Log	Previous	1	2	3	4	5	...	34	Next

13.4.1. 감사 로그 백업 스케줄러

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)

예약 백업

만들어질 백업의 유형 선택

감사 로그 백업 예약 eDiscovery 감사 로그 백업 예약

백업 주기 선택

백업을 만들 때 서버에서 로그들을 유지 또는 삭제

백업된 로그 유지 백업된 사본을 유지

위 품신이 선택하지 않은 상태면 경우 서버의 모래된 로그들은 DB에서 삭제되고 서버의 성능이 영향을 줍니다.

온 크기의 사본 파일들은 내보내기 프로시저와 서버 성능에 영향을 줍니다. 이 문제는 내보내기 실행 이전에 반드시 해결되어야 합니다.

백업할 로그 선택

보관해 당 평균 로그 수
1,000,000

백업 내보내기 형식 선택

CSV HTML

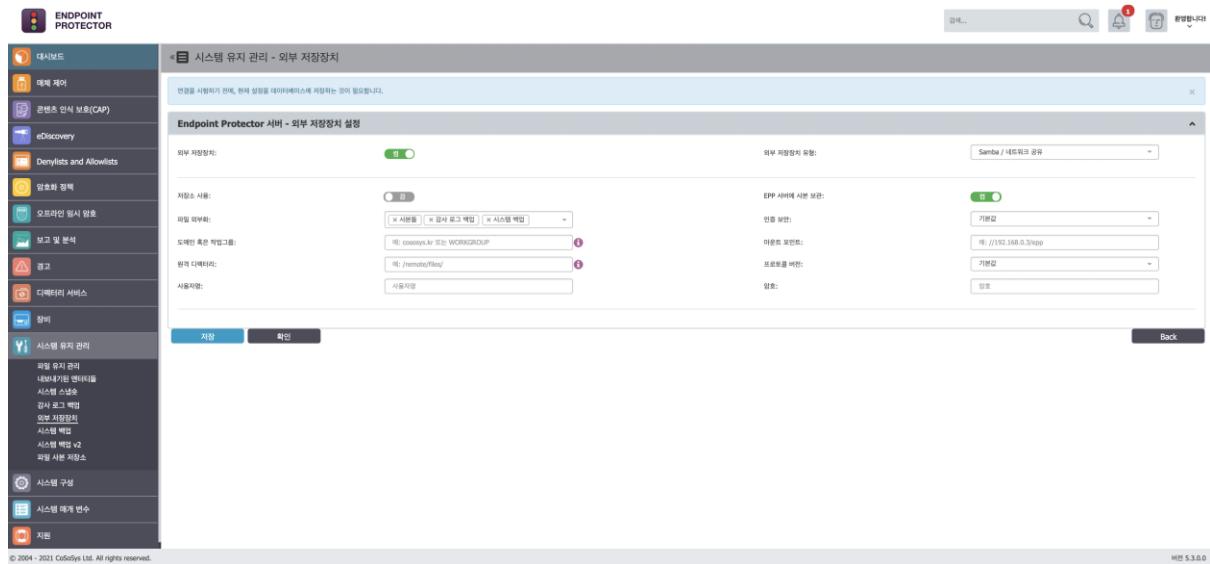
포함할 사본 파일 선택

기본 파일을 포함하지 않음 크기와 무관하게 모든 사본 파일을 포함 포함할 사본 파일을 최소 크기 MB

스케줄 **취소**

13.5. 외부 저장장치

외부 저장장치 옵션은 관리자가 Endpoint Protector로 만들어진 로그 백업 파일과 보관 파일을 네트워크를 통해서 특정 저장 디스크에 저장 할 수 있습니다. FTP 서버, Samba / 네트워크 공유, SFTP 서버를 지원 합니다.



참고

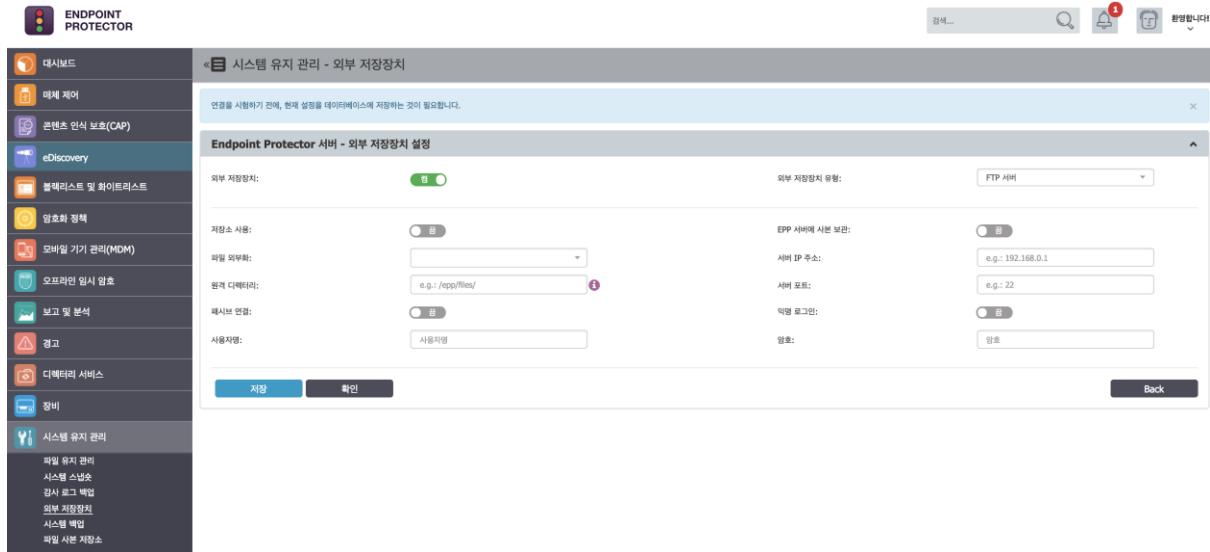
Endpoint Protector 서버에서 파일 복사를 유지하는 옵션은 모든 외부 저장 장치 유형에서 ON/OFF 할 수 있습니다.

14.5.1. FTP 서버

FTP 서버를 설정하기 위해서 다음의 매개 변수가 필요합니다.

- 파일 외부화** – Endpoint Protector 파일: 사본 보관, 감사 로그 백업 또는 시스템 백업
- 인증 보안** – 보안 프로토콜: 기본값, NTLM, NTLMv2, NTLMSSP
- 도메인 또는 작업그룹** – 적용될 때만 사용
- 서버 IP 주소** – 외부 서버 IP
- 원격 디렉토리** – 외부 디렉토리의 특정 위치

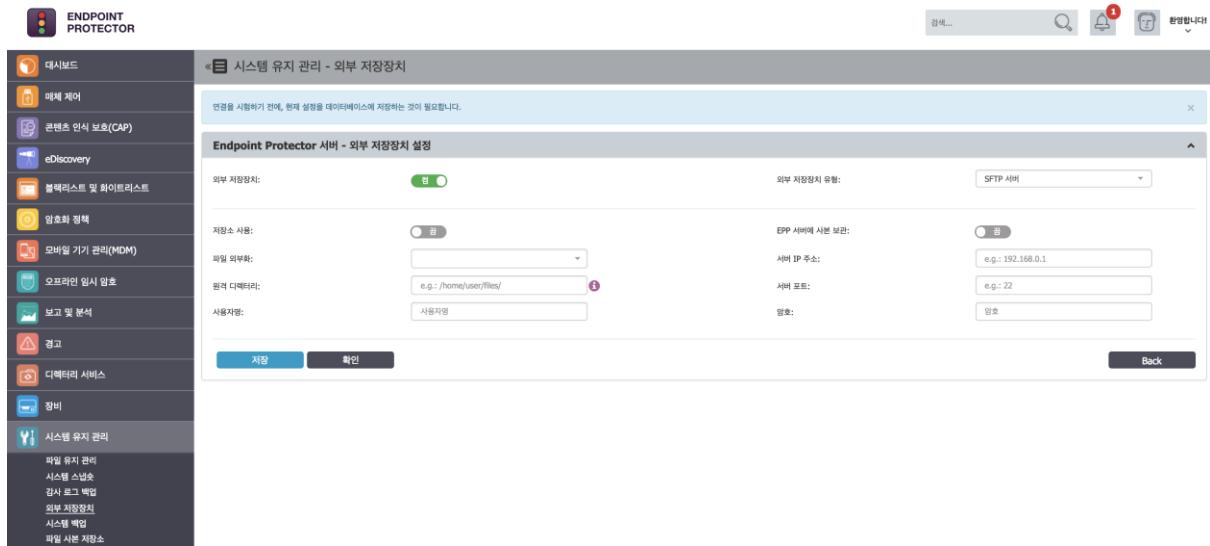
- **사용자명** – 외부 서버의 사용자 이름
- **암호** – 관련 암호



13.5.2. SFTP 서버

SFTP 서버를 설정하기 위해서 다음의 매개 변수가 필요합니다.

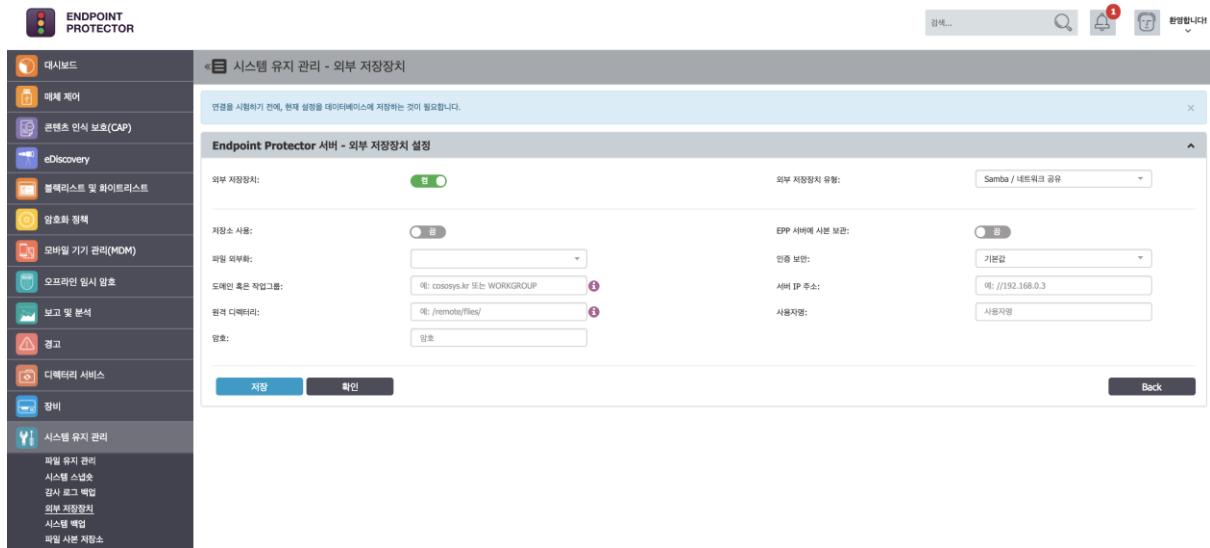
- **파일 외부화** – Endpoint Protector 파일: 사본 보관, 감사 로그 백업 또는 시스템 백업
- **서버 IP 주소** – 외부 서버 IP
- **원격 디렉토리** – 외부 디렉토리의 특정 위치
- **서버 포트** – 외부 저장 서버의 포트
- **사용자명** – 외부 서버의 사용자 이름
- **암호** – 관련 암호



13.5.3. Samba / 네트워크 공유

Samba / 네트워크 공유 서버를 설정하기 위해서 다음의 매개 변수가 필요합니다.

- 파일 외부화** – Endpoint Protector 파일: 사본 보관, 감사 로그 백업 또는 시스템 백업
- 인증 보안** – 보안 프로토콜: 기본값, NTLM, NTLMv2, NTLMSSP
- 도메인 또는 작업그룹** – 적용될 때만 사용
- 서버 IP 주소** – 외부 서버 IP
- 원격 디렉토리** – 외부 디렉토리의 특정 위치
- 사용자명** – 외부 서버의 사용자 이름
- 암호** – 관련 암호



13.6. 시스템 백업

13.6.1. 시스템 백업 (웹 인터페이스)

이 모듈은 관리자가 완전하게 시스템 백업을 할 수 있도록 도와줍니다.

이름	버전	내용	설명	만든 시간	작업
auto_backup_24Mar2018	5.1.0.1	데이터베이스 내용, 응용프로그램 원본	Scheduled System Backup on 24-Mar-2018	24-Mar-2018 11:06:01	
auto_backup_22Feb2018	5.1.0.1	데이터베이스 내용, 응용프로그램 원본	Scheduled System Backup on 22-Feb-2018	22-Feb-2018 11:05:01	

"시스템 유지 관리 > 시스템 백업" 메뉴에서 현재 존재하는 백업 목록을 볼 수 있습니다.

관리자는 복원, 다운로드, 삭제 액션을 취할 수 있습니다.

초기 단계에서 복원하는 것은 간단히 원하는 시스템 백업 옆에 있는 복원  버튼을 클릭하면 됩니다. 이 액션은 창 옆에 버튼을 다시 클릭해서 확정합니다.

다운로드 버튼을 클릭하면 관리자는 .eppb 백업 파일을 로컬 드라이브에 즉시 저장할 수 있습니다. 이 파일이 저장된 장소를 잘 기억하시기를 권장합니다.

참고

한 번 삭제하면 백업은 복원되지 않습니다.

"시스템 유지 관리 > 시스템 백업" 하위 메뉴에서 백업 만들기, 상태, 업로드, 백업 스케줄러를 사용할 수 있습니다.

첫 번째 옵션인 백업 만들기는 아래 메뉴를 사용합니다:



관리자는 아래 두 옵션을 선택할 수 있습니다:

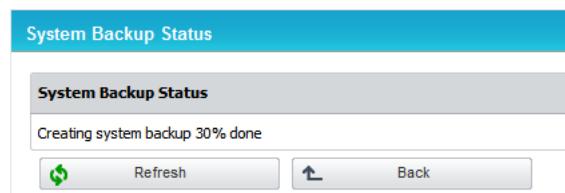
- **데이터베이스 내용 저장** – 이 옵션은 EPP 서버있는 모든 장치, 권한, 로그, 설정, 정책의 백업 파일을 포함합니다.
- **응용프로그램 소스 저장** – 이 옵션은 EPP 클라이언트 및 서버의 적절한 다른 기

능과 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.



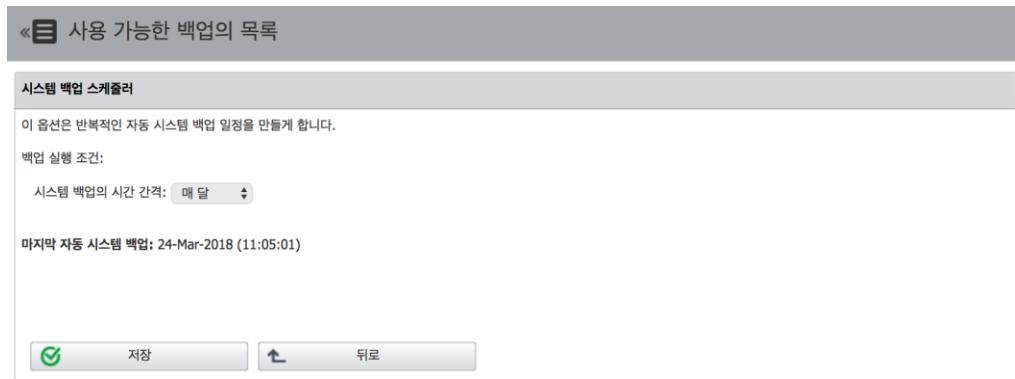
다음 메뉴인 **업로드**로 관리자는 로컬 파일 시스템에서 .eppb 파일을 올릴 수 있습니다. 이 기능은 서버 이관 또는 손상 복원에 매우 유용합니다. 아래와 같은 화면을 볼 수 있습니다.



참고

200 MB 가 넘는 Endpoint Protector 백업 파일 (.eppb)은 어플라이언스 콘솔로만 업로드가 가능합니다. .eppb 파일이 200 MB 넘으면 담당 지원팀에 연락하시기 바랍니다.

마지막 메뉴는 **백업 스케줄러**입니다.



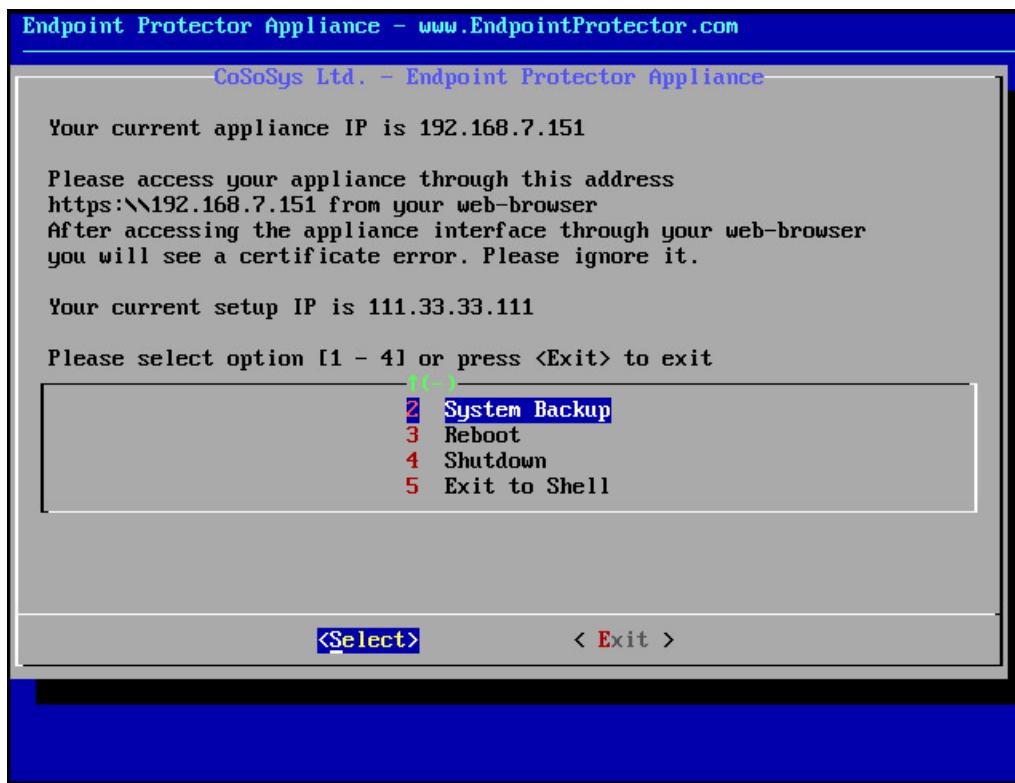
관리자는 자동 백업 스케줄을 설정할 수 있습니다. 시스템 백업 간격은 매일, 매주, 매달 등으로 설정이 가능합니다.

참고

자동 백업 스케줄은 원하지 않은 손실을 막기 위해서 권장합니다.

13.6.2. 시스템 백업 (콘솔)

Endpoint Protector는 초기 구성하는 관리자 콘솔에서 이전 상태로 시스템을 돌리는 옵션을 제공합니다.

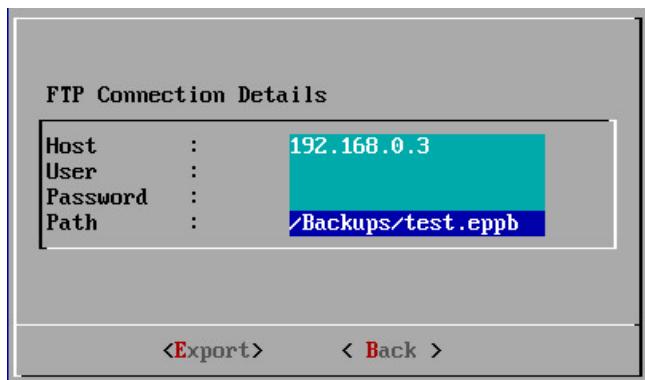


2번 메뉴를 통해 관리자는 다음 옵션을 사용할 수 있습니다.

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.



13.7. 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.

정보

오래된 서버와 새로운 서버 버전이 같아야 합니다. 마이그레이션 전에 같은 버전이 되도록 맞추어야 합니다. (예: 5206으로 오래된 서버를 업그레이드해서 막 배포된 새로운 서버와 버전을 맞추어야 합니다.).

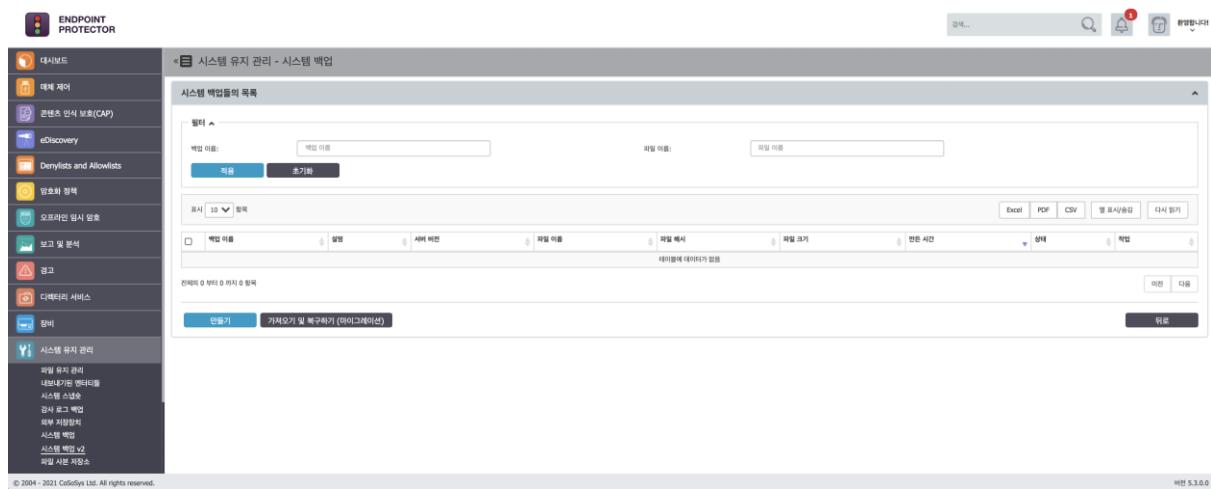
참고

로그, 감사 로그 또는 시스템 백업은 여기에 포함되지 않습니다. 필요하다면 시작하기 전에 다운로드 하시기 바랍니다.

예제

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.



13.7.1. 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.



13.7.2. 가져오기 및 복원 (마이그레이션)

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 파일과 시스템 백업 키가 필요합니다.

시스템 백업 - 가져오기 및 복구하기 (마이그레이션)

This is intended as a migration tool to a newer Endpoint Protector Appliance

If needed, make sure to use the Audit Log Backup before proceeding as Logs will not be kept. Previous System Backups should also be downloaded beforehand as only the System Backup you are about to import and restore will remain.

가져오기: 파일 선택...

시스템 백업 키: 시스템 백업 키

가져오기

참고

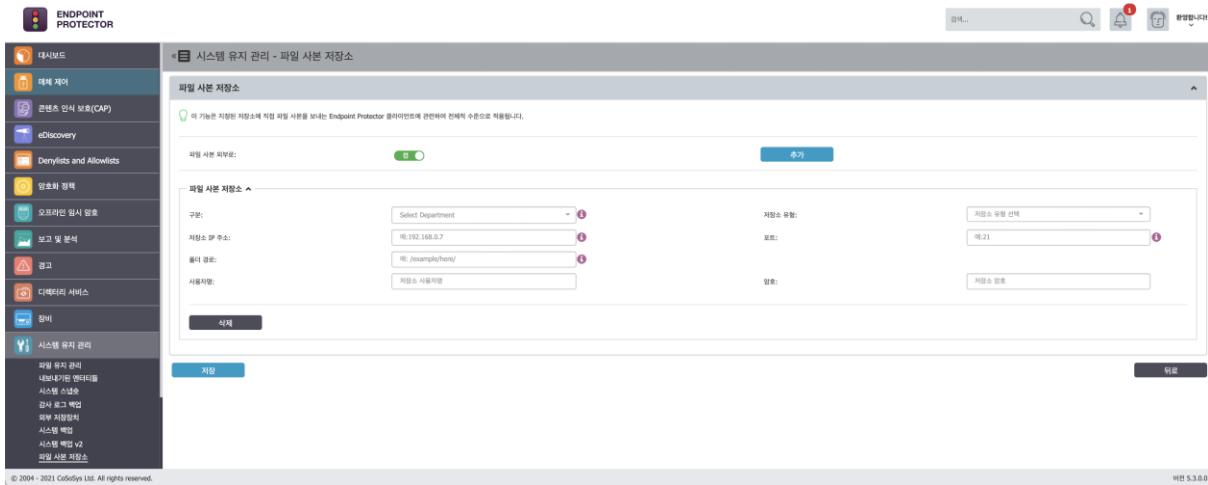
필요하다면 시작 전에 시스템 백업 또는 감사 로그 백업을 다운로드해야 합니다. 이 프로세스에서는 포함되지 않습니다.

정보

새로운 어플라이언스에 가져오기 및 복원 (마이그레이션)을 만든 후에 오래된 어플라이언스 전원을 내려야 합니다. 배포된 Endpoint Protector 클라이언트가 새로운 어플라이언스와 통신을 시작하기 위해서 IP가 새로운 어플라이언스에 재할당 되기를 기다려야 하기 때문입니다.

13.8. 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.

정보

Endpoint Protector에서 구분은 같은 속성에서 객체 모음으로 정의됩니다. 조직도의 부서와 혼동해서는 안됩니다.

파일 사본 보관 저장소를 추가하기 위해서는 구분, 저장소 IP 주소, 포트, 폴더 경로, 사용자 이름 및 비밀 번호가 설정되어야 합니다.

정보

FTP 또는 Samba 저장소 유형에 따라서 포트는 필요하지 않을 수 있고 비활성화 처리됩니다.

14. 시스템 구성

이 모듈에도 시스템의 기능과 안정성에 영향을 미치는 고급 설정이 포함되어 있습니다.

14.1. 클라이언트 소프트웨어

이 섹션에서 관리자는 사용 중인 운영 체제에 해당하는 Endpoint Protector 클라이언트를 다운로드 하여 설치할 수 있습니다. 서버와 클라이언트는 **443** 포트로 통신하는 것을 유의 하시기 바랍니다.

The screenshot shows the Endpoint Protector software interface. On the left, there's a sidebar with various icons and sections like 'ediscovery', '기부목록 및 허용목록', '암호화 정책', '오프라인 임시 암호', '보고 및 분석', '경고', '디렉터리 서비스', '장비', '시스템 유지 관리', and '시스템 구성'. Under '시스템 구성', there are sub-options for '클라이언트 소프트웨어', '클라이언트 업그레이드', '클라이언트 삭제', '시스템 관리자', '관리자 그룹', '시스템 구분코드', '시스템 보안', '시스템 설정', '시스템 라이선스', and 'SSO(Single Sign On)'. The main content area is titled 'Endpoint Protector 클라이언트 설치' and shows 'Endpoint Protector 클라이언트 설치 운영 체제:' dropdown menus for Windows, MAC, and Linux. The Windows menu lists: Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2003/2008/2012/2016/2019. The MAC menu lists: macOS 11.0 (Big Sur), macOS 10.15 (Catalina), macOS 10.14 (Mojave), macOS 10.13 (High Sierra), macOS 10.12 (Sierra), macOS X 10.11 (El Capitan), macOS X 10.10 (Yosemite), macOS X 10.9 (Mavericks), macOS X 10.8 (Mountain Lion), macOS X 10.7 (Lion). The Linux menu lists: Debian, Ubuntu, Linux Mint, RHEL, CentOS, Fedora, openSUSE, SUSE Enterprise. Below these are notes about Linux support and a download button. The bottom of the screen shows copyright information: '© 2004 - 2021 CoSoSys Ltd. All rights reserved.' and '버전 5.4.0.0'.

팁

Windows 클라이언트 인스톨러는 add-on 이 있거나 없는 다운로든 패키지를 제공합니다. 이 옵션은 Endpoint Protector와 특정 솔루션 사이의 호환성 이슈를 해결합니다.

14.2. 클라이언트 업그레이드

이 섹션에서는 설치된 Endpoint Protector 클라이언트 버전의 자동 업데이트를 선택하고 수행할 수 있습니다.

참고

이 기능은 Linux 클라이언트에서 사용할 수 없습니다. 또한 정말 오래된 클라이언트 (예: Windows 클라이언트 4.0.1.4 이하 버전)에서도 사용할 수 없습니다.

OS 종류	기본값	버전	필터스 정보	버전별로 적용	작업
Windows	Yes	5.3.7.6		4.0.1.5	✖
Mac OS X 10.5+ (Snow Leopard)	Yes	2.1.1.3		1.0.8.5	✖
Mac OS X 10.4 (Tiger)	Yes	1.0.5.0		none	✖
Ubuntu 14.04 LTS	Yes	1.0.5.1		none	✖
Ubuntu 12.04 LTS	Yes	1.0.5.1		none	✖
Ubuntu 10.4 LTS	Yes	1.0.5.1		none	✖
OpenSUSE 11.4	Yes	1.0.5.1		none	✖
Windows	No	5.3.7.0		4.0.1.5	✖
Windows	No	5.3.4.1		4.0.1.5	✖
Windows	No	5.2.3.9		4.0.1.5	✖
Windows	No	5.1.2.0		4.0.1.5	✖
Windows	No	4.8.8.9		4.0.1.5	✖
Windows	No	4.8.5.4		4.0.1.5	✖
Windows	No	4.4.5.3		4.0.1.5	✖
Windows	No	4.4.4.5		4.0.1.5	✖
Mac OS X 10.5+ (Snow Leopard)	No	2.0.3.7		1.0.8.5	✖
Mac OS X 10.4	No	2.0.3.3		1.0.8.5	✖
Mac OS X 10.5+ (Snow Leopard)	No	2.0.2.9		1.0.8.5	✖
Mac OS X 10.5+ (Snow Leopard)	No	1.9.3.2		1.0.8.5	✖
Mac OS X 10.5+ (Snow Leopard)	No	1.8.1.3		1.0.8.5	✖
Mac OS X 10.5+ (Snow Leopard)	No	1.6.8.9		1.0.8.5	✖
Mac OS X 10.5+ (Snow Leopard)	No	1.5.1.8		1.0.8.5	✖
Mac OS X 10.5+ (Snow Leopard)	No	1.5.0.6		1.0.8.5	✖

작업 열 아래의 버튼을 사용하여 클라이언트 소프트웨어 섹션에서 다운로드 할 수 있는 Endpoint Protector 클라이언트 버전을 설정할 수 있습니다.

14.3. 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 회색으로 처리됩니다. 이미 실행된 것이 아니라면 삭제 명령은

취소 할 수 있습니다.

The screenshot shows the 'Computer List' section of the Endpoint Protector application. The left sidebar contains navigation links such as eDiscovery, Denylists and Allowlists, Firewall Policy, Endpoint Protection, Diagnostics Services, and System Configuration. The main area displays a table of computer details:

컴퓨터 이름	IP	구분	작업 그룹	도메인	GROUPS	기본 사용자	마지막 확인	비전	라이선스	작업
cossyslinux	192.168.100.194	Default Department		cossys.co.kr	-	cossys	2021-03-08 16:05:32	1.6.0.2 - (Linux)	라이선스 있음	<i>(edit)</i>
localhost.localdomain	192.168.100.164	Default Department		cossys.co.kr	-	jack	2021-03-08 16:07:29	1.7.0.3 - (Linux)	라이선스 있음	<i>(edit)</i>
DESKTOP-NHUFICB	192.168.100.106	Default Department	WORKGROUP		-	cossywindows	2021-03-08 09:36:07	5.3.7.6 - (Windows)	라이선스 있음	<i>(edit)</i>

At the bottom of the table, there are buttons for '전체' (All), '1' (Page 1), and '다음' (Next). Below the table, there are buttons for '제거' (Delete) and '뒤로' (Back).

14.4. 시스템 관리자

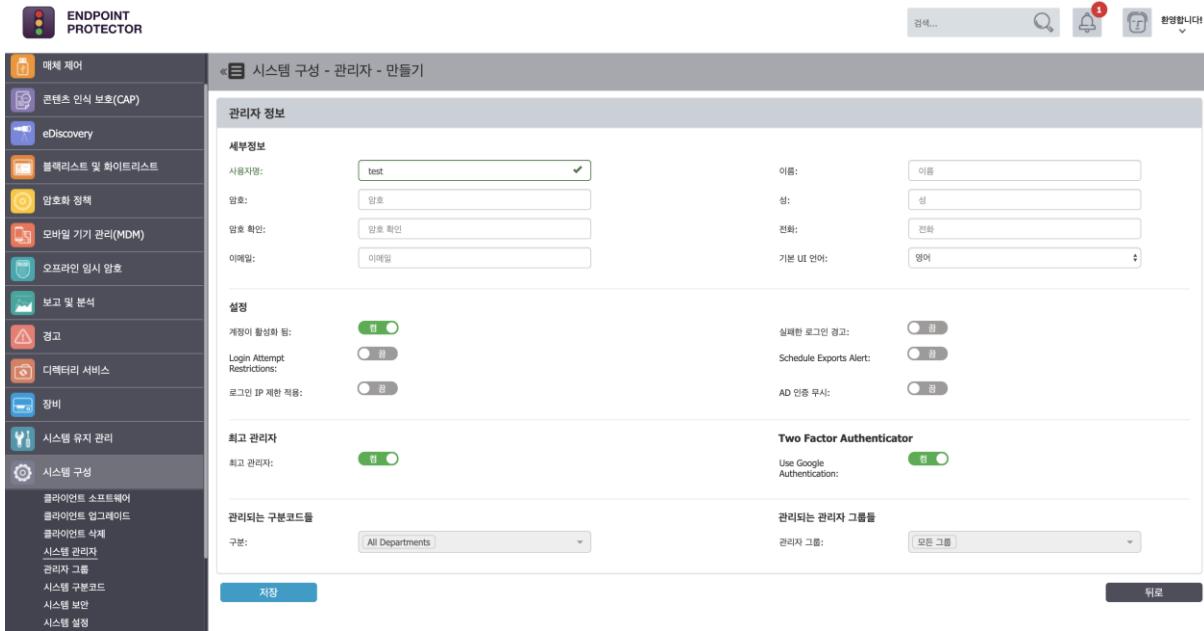
이 섹션은 새로운 관리자를 만듭니다. 관리자가 만들어지면 모든 관리자를 포함하는 목록에 표시됩니다. 상세 정보 편집 및 설정 옵션 또는 원하지 않는 관리자를 삭제하는 옵션 또한 가능합니다. 일반 관리자는 몇 가지 제한을 가지고 있고 최고 관리자는 모든 시스템에 접근이 가능하고 고급 기능을 사용할 수 있습니다. 이것이 가장 큰 점입니다.

관리자를 만드는 중간에 여러 관리자 상세 정보 및 관리자 설정을 구성할 수 있습니다. 이메일 경고 수신, 구분 관리, 특정 IP 로그인 제한 및 UI 언어 기본값 등을 변경할 수 있습니다. 이러한 설정은 나중에 다시 할 수 있습니다.

The screenshot shows the 'System Manager' section of the Endpoint Protector application. The left sidebar contains the same navigation links as the previous screenshot. The main area displays a table of manager details:

관리자 이름	이름	성	전화	이메일	관리자 그룹	관리자 역할	구분	마지막 확인	2FA	AD 사용자	AD 인증 주사	작업
root	-	-	-	n/a	최고 관리자	전부	2021-03-08 15:01:35	아니오	아니오	예	<i>(edit)</i>	

At the bottom of the table, there are buttons for '만들기' (Create), '삭제' (Delete), '전체' (All), '1' (Page 1), and '다음' (Next). Below the table, there are buttons for '만들기' (Create) and '삭제' (Delete).



계정이 활성화 됨

만약 겸으로 되어 있으면 계정을 사용할 수 있습니다.

최고 관리자

만약 겸으로 되어 있으면 해당 계정으로 최고 관리자로 간주가 되어서 모든 구분 및 Endpoint Protector의 모든 섹션에 접근할 수 있습니다.

AD인증 무시

만약 겸으로 되어 있으면 AD 계정을 Endpoint Protector 로그인에 사용할 수 있습니다.

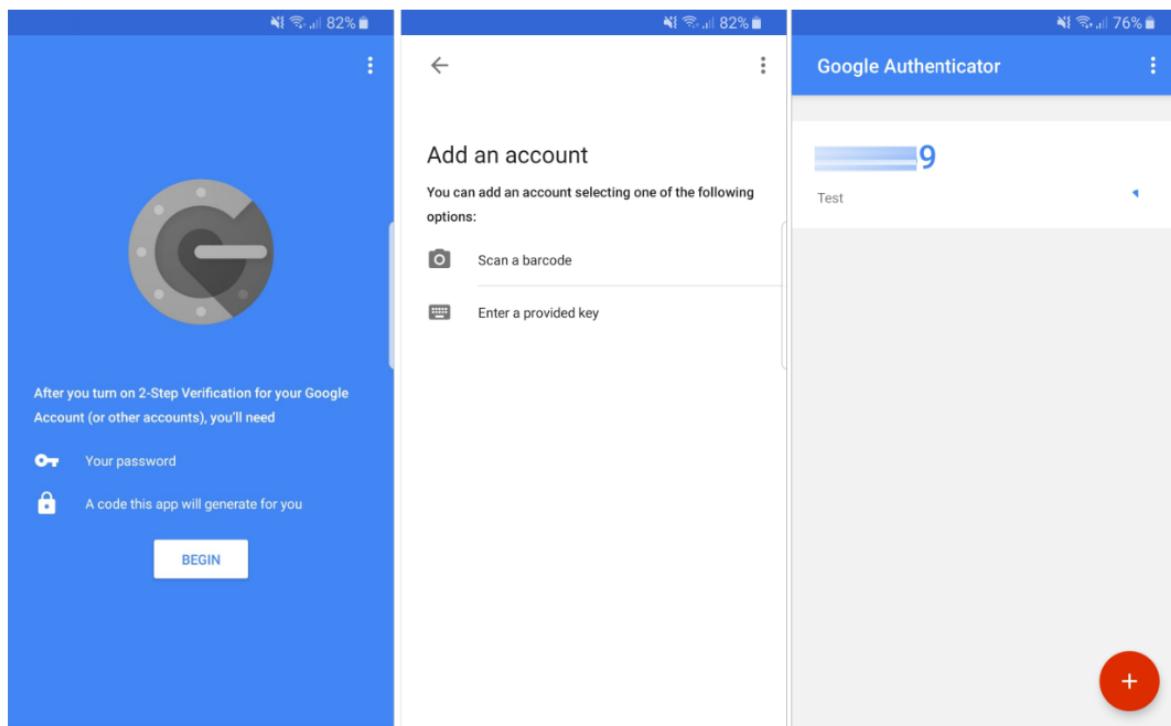
이중 인증 (Two Factor Authentication)

만약 겸으로 되어 있으면 2FA는 Google 인증을 사용하여 보안을 강화할 수 있습니다.

이중 인증 (Two Factor Authentication, 2FA)은 Google 인증 앱을 통해서 생성된 임시 코드를 요청해서 로그인 프로세스에 추가적인 단계를 포함합니다. 만약 겸으로 되어있고 저장을 누르면 관리자는 인증 화면을 아래와 같이 볼 수 있습니다.

The screenshot shows the 'Google 2FA Validation' configuration page within the Endpoint Protector web interface. On the left, there's a sidebar with various navigation options like Dashboard, Audit, Content Protection, eDiscovery, and System Configuration. The main panel is titled 'Google 2FA Validation' and contains three steps: 1) Scan the QR code with the Google Authenticator app. 2) Continue configuration in the app. 3) Enter the authentication code from the app into the provided field. A 'Validate' button is at the bottom.

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.



정보

최고 관리자 옵션이 활성화되면 관리자는 전체 시스템의 모든 권한을 가지게 됩니다.

최고 관리자 옵션이 비활성화 되면 관리자는 일반 권한을 가지고 시스템의 특정 부분 접근이 제한 될 수 있습니다 (예: 관리자는 관리하는 시스템 구분의 객체만 관리할 수 있습니다.). 즉 일반 관리자입니다.

일반 관리자는 특정 역할에 따라서 분류되어 관리자 그룹을 통해서 해당 역할만 수행 할 수 있습니다. (예: 오프라인 임시 암호, 보고 및 분석, EasyLock, 유지 관리, 헬프 데스크, 매체 제어, 읽기만, 콘텐츠 인식 보호, eDiscovery).

참고

AD Admin 그룹에서 가져온 모든 관리자는 자동으로 최고 관리자가 됩니다. 그렇기 때문에 필요에 따라 동기화 후에 역할을 변경해야 합니다.

관리자 AD 인증에 대한 자세한 정보는 '14.8.2 Active Directory 인증' 을 참조하시기 바랍니다.

14.5. 관리자 그룹

이 섹션에서 관리자 그룹 만들기와 관리를 할 수 있습니다. 일반 관리자에게 다양한 접근 권한을 제공합니다 – 오프라인 임시 암호 관리자, EasyLock 관리자, 보고 및 분석 관리자, 유지보수 관리자 등.

198 | Endpoint Protector | 사용 설명서

시스템 구성 - 관리자 그룹

관리자 그룹	설명	역할	고친 시간	고친 사람	만든 시간	만든 사람	작업
오프라인 임시 암호	이 그룹의 관리자에게는 오프라인 임시 암호 섹션 사용이 허용됨	오프라인 임시 암호 관리자	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
보고 및 분석	이 그룹의 관리자에게는 보고 및 분석 섹션 사용이 허용됨	보고 및 분석 관리자	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
EasyLock	이 그룹의 관리자에게는 EasyLock 섹션 사용이 허용됨	EasyLock 관리자	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
유지 관리	Administrators from this Group will be granted access to the Directory Services, Appliance and System Maintenance section	시스템 유지 관리자	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
헬프 데스크	이 그룹의 관리자에게는 EasyLock, 오프라인 임시 암호 섹션 사용이 허용됨	EasyLock 관리자, 오프라인 임시 암호 관리자	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
매체 제어	이 그룹의 관리자에게는 매체 제어 관리 섹션 사용이 허용됨	Device Control Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
Read Only	Administrators from this Group will only be able to view the UI. It cannot be combined with other Roles.	Read Only Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
콘텐츠 인식 보호 (CAP)	Administrators from this Group will only be granted access to the Content Aware Protection sections.	Content Aware Protection Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...
eDiscovery	Administrators from this Group will only be granted access to the eDiscovery sections.	eDiscovery Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	...

전체의 1 부터 9 까지 9 항목

이전 1 다음

뒤로

이러한 그룹을 생성하는 주요 정보는 이름, 설명, 역할 선택 및 관리자 선택을 통해서 수행이 됩니다.

시스템 구성 - 관리자 그룹 - 수정 오프라인 임시 암호

그룹 정보

세부정보	이름: 오프라인 임시 암호	설명: 이 그룹의 관리자에게는 오프라인 임시 암호 섹션 사용이 허용됨
역할	역할 선택: 오프라인 임시 암호 관리자	관리자 선택: 관리자 선택
추가적인 정보	만든 시간: 2017-09-25 15:19:57	만든 사람: root
	고친 시간: 2017-09-25 15:19:57	고친 사람: root

저장

뒤로

팁

역할이 부여된 관리자 그룹을 만들 수 있습니다.

예: 헬프데스크 그룹에 두 가지 역할을 부여할 수 있습니다 – 오프라인 임시 암호 관리자 / EasyLock 관리자.

14.6. 시스템 구분

이 섹션에서 시스템 구분을 만들고 관리할 수 있습니다.

참고

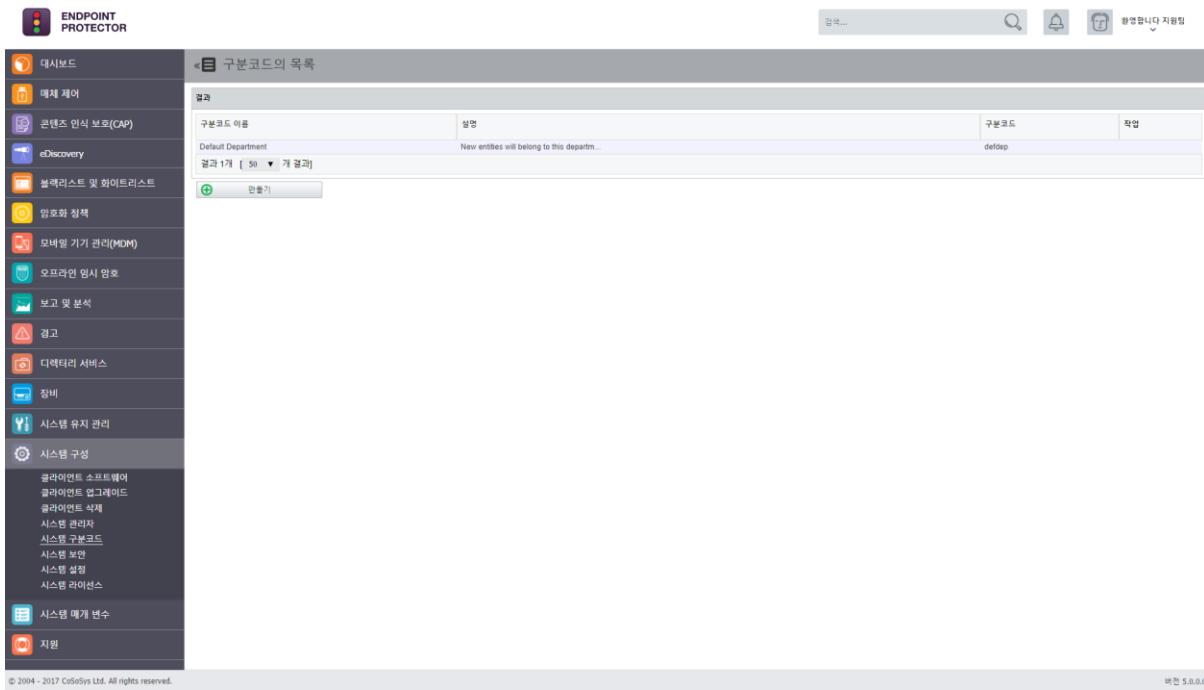
클라이언트를 설치하는 경우 구분 코드를 할당하지 않거나 잘못된 코드를 넣으면 구분 코드는 유효하지 않은 것으로 인식되고 기본 구분코드 (defdep)가 할당됩니다.

정보

시스템 구분 사용은 옵션입니다. Endpoint Protector는 기본 구분인 defdep로 완벽하게 동작합니다. 게다가 대부분의 시나리오는 장치, 컴퓨터, 사용자 및 그룹으로 적용할 수 있습니다. 이 객체는 AD에서도 사용할 수 있습니다.

이 기능은 많은 관리자가 필요하고 역할이 다른 대규모 네트워크에서 유용합니다. 이러한 환경에서 구분 코드를 만들어서 일반 관리자들에게 각각의 고유한 역할을 부여합니다.

이 기능을 컴퓨터 및 사용자 그룹 또는 관리자의 역할과 혼동하지 마시기 바랍니다.



"생성" 버튼을 사용하여 새 구분을 정의할 수 있습니다.



Endpoint Protector와 Active Directory(또는 기타 디렉토리 서비스 소프트웨어) 사이의 유사성을 확보를 위해 '구분' 용어와 동등한 용어는 '조직 단위'입니다. 물론 조직 단위는 구분과 동일하지 않고 하나 이상의 조직 단위를 Endpoint Protector 부서에 연결하는 것은 실제 최고 관리자의 몫입니다.

아래에는 구분에 관한 다양한 설명이 자세히 나와 있습니다.

- 최고 관리자가 기본 구분을 삭제하는 시나리오 외에 모든 주 개체는 반드시 구분에 속해야 합니다. 컴퓨터 등록 시 구분 코드를 입력합니다. 해당 코드를 가진 구분이 발견되면 컴퓨터가 등록되고 해당 구분에 속하게 됩니다. 구분 X 의 컴퓨터에서 받은 모든

주 개체 정보는 구분 X에 속합니다.

예제

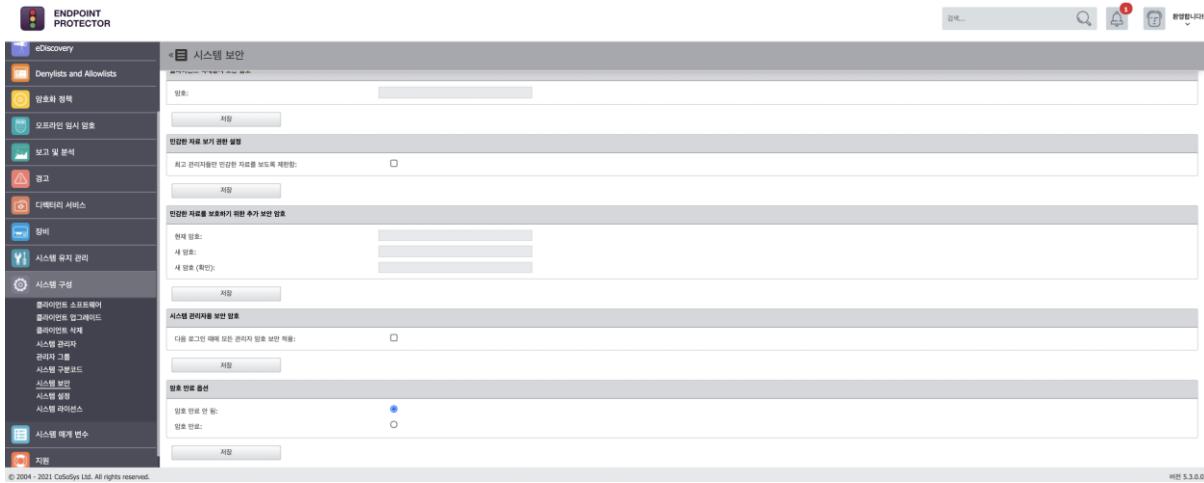
Test-PC 컴퓨터가 "개발자" 구분에 등록되어 있습니다. 이 경우 해당 컴퓨터에 로그온한 Test 사용자를 Test-PC 컴퓨터에 연결된 장치와 함께 동일한 구분에 할당합니다.

2. 최고 관리자(예: 루트)는 구분에 상관없이 모든 주 개체에 계속 액세스할 수 있으며 부서를 변경할 수 있습니다. 최고 관리자로 로그온 하면 웹 인터페이스 기본 콘텐츠 레이아웃의 오른쪽 상단에 "모든 구분 표시" 텍스트가 표시됩니다.
3. 최고 관리자만 일반 사용자를 생성할 수 있으므로 하나 이상의 구분을 처리할 일반 관리자를 할당하는 것도 최고 관리자의 책임입니다. 일반 관리자는 웹 인터페이스에서 할당된 구분에 속하는 주 개체만 확인하고 관리할 수 있습니다.
4. 보안상 이유로 일반 관리자는 자신의 구분 개체만 볼 수 있습니다. 일반 관리자는 자신의 구분 개체만 제어할 수 있습니다.

14.7. 시스템 보안

클라이언트 삭제 방지 기능은 암호 기반의 메커니즘을 사용하여 Endpoint Protector 클라이언트가 삭제되는 것을 방지합니다. 시스템 관리자는 Endpoint Protector의 보고 및 관리 도구에서 이 암호를 정의합니다. 다른 사람이 Endpoint Protector 클라이언트를 삭제하려고 시도하면 암호를 입력하라는 메시지가 표시됩니다. 암호를 모르면 클라이언트 제거가 계속되지 않습니다.

"시스템 구성" -> "시스템 보안"에 액세스한 후 "암호" 영역에 암호를 입력하고 "저장"을 클릭하여 암호를 설정할 수 있습니다.



참고

한 번 “다음 로그인 때에 모든 관리자 암호 보안 적용”을 체크하면 이 기능을 다시 비활성화 할 수 없습니다.

활성화되면 아래의 규칙에 따라 복잡한 암호를 설정해야 합니다.

- 암호 최소 길이 9자
- 대문자, 소문자, 숫자, 특수기호 반드시 포함
- 오름차순으로 연속되는 숫자 및 문자 사용 금지

14.8. 시스템 설정

이 섹션에서 관리자는 전체 시스템에 적용하는 일반 설정을 구성할 수 있습니다. 이러한 설정의 대부분은 이미 초기 Endpoint Protector 마법사에 포함이 되어있습니다.

14.8.1. 권한 기능

시스템 설정 기능에서 사용자 권한과 컴퓨터 권한 중에 우선 순위를 설정하여 Endpoint Protector의 서버 권한 기능을 설정할 수 있습니다.

더 많은 정보를 원하시는 경우에는 "정책 설정" 부분을 참조 바랍니다.



14.8.2. 로그 설정

이 섹션에서 관리자는 CSV 로그 보고서에 대한 백만 단위 행을 설정할 수 있습니다. 모든 로그 행은 하나의 로그입니다. 예를 들어 1.0으로 설정되면 CSV 내보내기에 1백만 로그가 내보내기 될 것입니다.

정보

서버에서 로그 파티션을 가지면 내보내기 할 때 날짜가 선택되는 것을 확인하시기 바랍니다.

14.8.3. 심층 패킷 검사 (DPI) 인증서

더 자세한 정보는 DPI (Deep Packet Inspection) 섹션을 참조하시기 바랍니다.

14.8.4. Active Directory 인증

이 섹션에서 AD 그룹 관리자를 Endpoint Protector 최고 관리자로 가져올 수 있습니다. Active Directory 인증 사용을 체크하면 여기에 속한 관리자는 Endpoint Protector 로그인 시 그들의 AD 계정을 사용할 수 있습니다.

이 진행 과정은 간단하면 아래 4가지로 요약할 수 있습니다.

- 모든 계정 및 요청 정보 입력

정보

필요한 설정은 디렉토리 서비스 섹션과 동일합니다. 자세한 내용은 '11 디렉토리 서비스'를 참조하시기 바랍니다.

- 이 페이지 아래 부분으로 스크롤해서 변경 저장

팁

페이지 상단 녹색 박스로 완료 메시지가 나타나면 성공적으로 저장이 완료된 것을 확인할 수 있습니다.

- 페이지의 Active Directory 인증으로 돌아와서 시험 연결 확인
- AD 관리자 동기화 버튼 누름

참고

Active Directory 관리자 그룹이 한 번 정의되면 이 AD 그룹의 사용자만 동기화되고 Endpoint Protector 최고 관리자가 됩니다. 추가적인 접근 제어 관리자 설정은 시스템 관리자 섹션에서 수동으로 만들 수 있습니다.

The screenshot shows the 'Basic System Settings' configuration page of the Endpoint Protector software. The left sidebar contains various management icons: Dashboard, Audit Log, CAP, eDiscovery, Blacklist/Whitelist, Encryption Policies, MDM, Offline Emergency, Reporting, Alerts, Discovery Services, Groups, System Configuration, Software Updates, System Health, System Groups, Administrators Groups, System Profiles, System Monitoring, System Settings, and System Backup. The main panel has several sections:

- Storage Paths:** Log directory: /var/epprofiles/logs/, Shadow directory: /var/epprofiles/shadows/.
- Group Policy:** Radio buttons for using a group policy with a logon script or using a group policy without a logon script.
- Endpoint Protector Permissions:** Radio buttons for computer permission, user permission, or both.
- User Settings:** Options for displaying VID, PID, and Serial Number for Offline Temporary Password, displaying offline emergency menu MAC address, and displaying user domain password.
- Active Directory Authentication:** A section for configuring Active Directory authentication, including selecting the authentication type (Basic, SSL/TLS), IP for the Active Directory controller, domain controller port, domain name, account name, and account password. Buttons for 'AD 관리자 등기화' (Sync AD Manager) and '시험 연결' (Test Connection) are also present.
- Additional Settings:** An 'Email Server Settings' section.

At the bottom of the interface, there is a copyright notice: © 2004 - 2018 CoSoSys Ltd. All rights reserved. and a version number: 버전 5.1.0.0.

14.8.5. 프록시 서버 설정

Endpoint Protector는 아래와 같이 프록시의 구성 옵션을 제공합니다.



필요한 구성의 자세한 내용은 다음과 같습니다.

- IP 및 포트 – 프록시 서버 IP 및 포트
- 사용자 이름 / 암호 – 프록시 접근 인증 (필수 사항 아님)

참고

프록시 서버가 설정되지 않으면 Endpoint Protector는 바로 liveupdate.endpointprotector.com으로 연결됩니다.

14.9. 시스템 라이선스

이 모듈에서 관리자는 Endpoint Protector 의 라이선스를 관리할 수 있으며 최신 라이선스 상태에 대한 간략한 정보가 제공됩니다.

Module	Usage
EasyLock	50
Windows eDiscovery	6
MDM	4
Mobile Device Management	5
Temporary User	1
Total	1

Licensed Endpoints

Type	Total	Used	Online
Computers	50	6	4
Mobile Device	5	1	1

Note: Terminal Server and EasyLock Enforced Encrypted Devices relate also to the number of users.

Terminal Server Users: 0
EasyLock Enforced Encrypted Devices: 2

참고

Endpoint Protector 버전 5.2.0.7에서 라이선스는 구독 시스템으로 변경되었습니다. 레거시 라이선스 유형을 가지고 있는 고객은 새로운 계약 전까지 라이선스 조건 등의 대상입니다.

** 대한민국은 레거시 라이선스를 유지합니다.

Endpoint Protector 라이선스는 아래 2가지를 기반으로 합니다.

- **모듈** – 모든 모듈 라이선스는 분리가 되어있고 (콘텐츠 인식 보호, eDiscovery 등) 매체 제어 모듈을 필요로 합니다.
- **엔드포인트** – 보호가 필요한 Windows, Mac, Linux 컴퓨터를 참조하여 Endpoint Protector 클라이언트가 설치됩니다. 특히 이러한 엔드포인트는 모바일 기기 관리 (MDM) 모듈이 연결된 모바일 엔드포인트를 포함할 수 있습니다. 원하는 모듈과 엔드포인트를 기반으로 라이선스 파일이 제공됩니다.

정보

Endpoint Protector 서버 ID는 각각의 서버를 식별하는 고유 ID이고 라이선스 파일과 연결됩니다. 라이선스 구매 전에 이 정보가 전달되어야 합니다.

라이선스 만료 날짜는 이 시스템의 라이선스 만료일을 표시합니다.

지원은 구매한 지원 레벨 (표준 또는 프리미엄)을 나타냅니다.

14.9.1. 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.

14.9.2. 라이선스 가져오기 및 관리

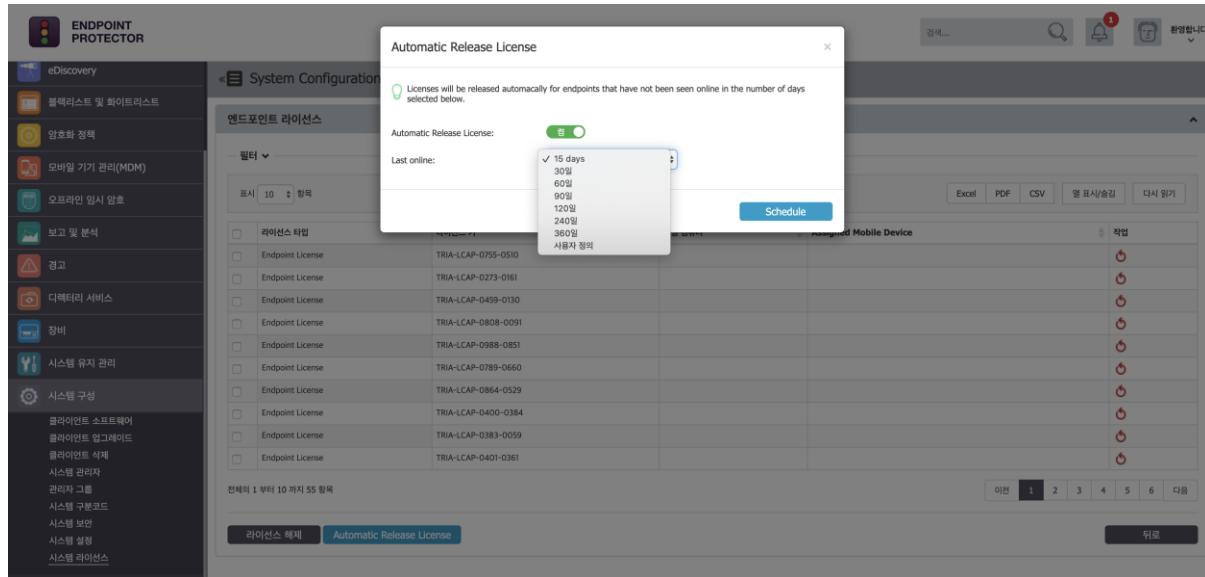
라이선스 가져오기 버튼은 라이선스 파일을 검색합니다. 이 파일은 모든 관련 정보가 포함되어 있습니다 (모듈, 엔드포인트 수, 만료일, 지원 유형 등).

라이선스 보기 버튼으로 엔드포인트 라이선스 관리를 할 수 있습니다.

Licenses Type	License Key	Assigned Mobile Device	Action
Endpoint License	TRIA-LCAP-0755-0510		Red
Endpoint License	TRIA-LCAP-0273-0161		Red
Endpoint License	TRIA-LCAP-0459-0130		Red
Endpoint License	TRIA-LCAP-0808-0091		Red
Endpoint License	TRIA-LCAP-0588-0851		Red
Endpoint License	TRIA-LCAP-0789-0660		Red
Endpoint License	TRIA-LCAP-0864-0529		Red
Endpoint License	TRIA-LCAP-0400-0384		Red
Endpoint License	TRIA-LCAP-0383-0059		Red
Endpoint License	TRIA-LCAP-0401-0361		Red

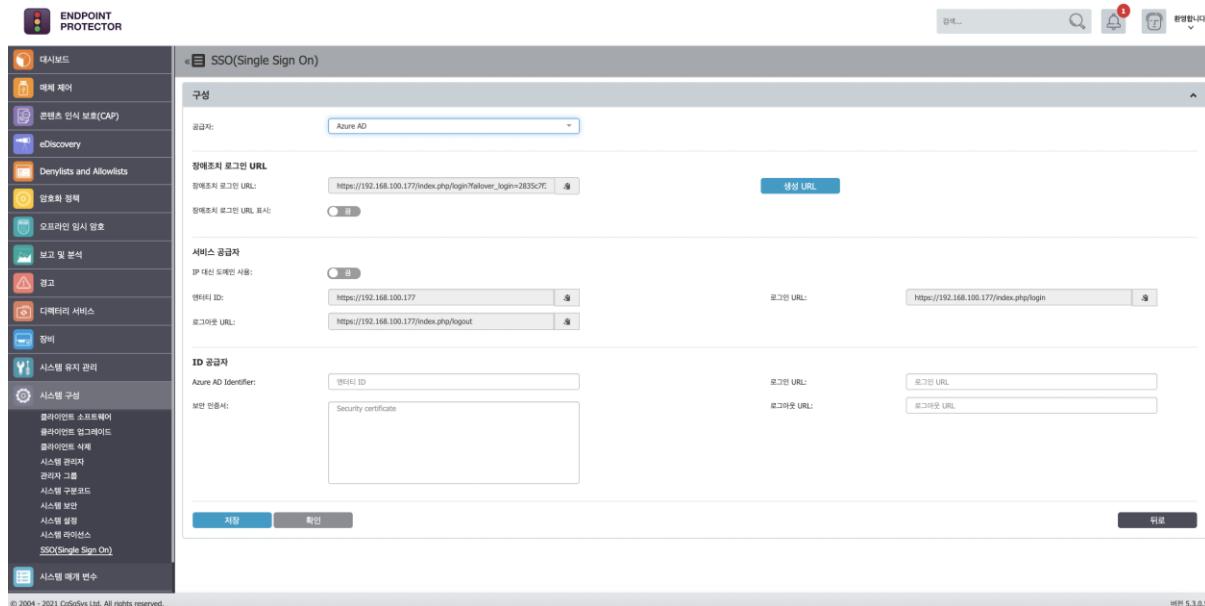
하나 또는 그 이상의 라이선스가 할당된 엔드포인트가 비활성화되고 재할당이 필요한 경우에 관리자는 이러한 라이선스를 다른 온라인 컴퓨터에 자동으로 재할당할 수 있습니다.

자동 라이선스 배포 기능을 사용하면 라이선스는 특정 기간 (15일, 30일, 90일 등 또는 사용자 정의) 동안 온라인으로 표시가 되지 않은 엔드포인트에 자동으로 배포될 것입니다.



14.10. SSO (Single Sign On)

SSO (Single Sign On) 기능은 관리자가 Azure AD 계정으로 Endpoint Protector 서버에 로그인 할 수 있도록 지원합니다.



SSO는 도메인 또는 IP 기반으로 만들 수 있습니다. 이 옵션은 '서비스 공급자' 하위 섹션에서 선택할 수 있습니다.

SSO 섹션은 아래 영역으로 구성되어 있습니다.

공급자는 구성을 시작을 위해서 첫 번째로 선택되어야 합니다.

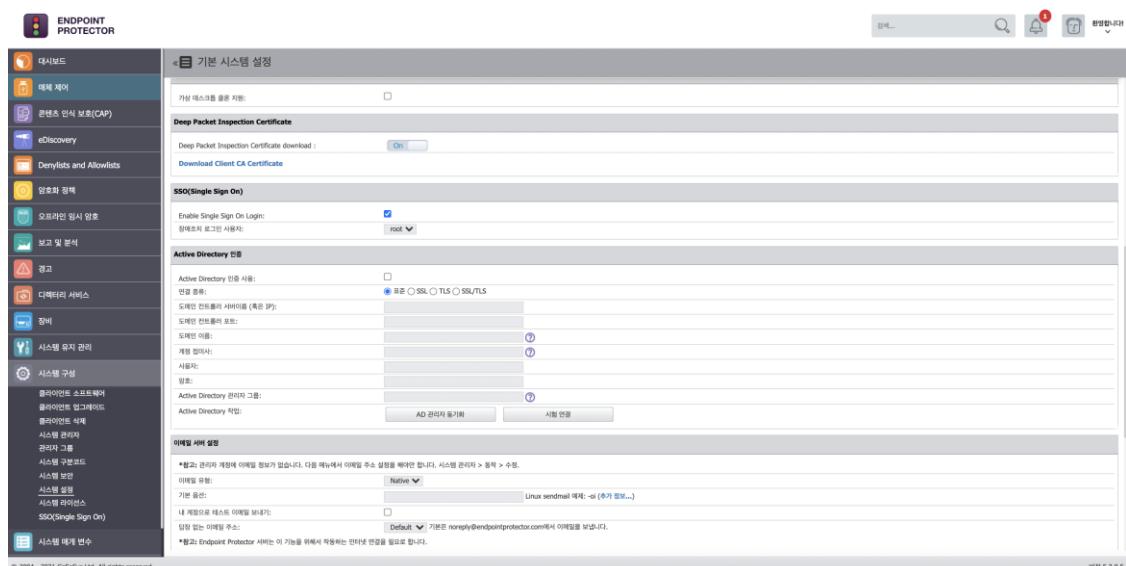
장애조치 로그인 URL은 Endpoint Protector 최고 관리자로 로컬 로그인이 허용되는 페이지의 링크를 제공하기 위해서 만들 수 있습니다. 이 URL은 동작이 멈추는 상황에서 Azure SSO (Single Sign On) 로그인을 우회합니다.

서비스 공급자 하위 섹션은 Endpoint Protector 서버 식별을 나타냅니다. 이 하위 섹션의 데이터는 Azure에서 Endpoint Protector 응용프로그램을 구성할 때 필요합니다. 로그인은 IP 또는 도메인 기반으로 할 수 있습니다.

ID 공급자는 Azure 쪽을 나타냅니다. Azure에서 만들어진 데이터가 입력되어야 하는 영역이고 관리자는 Endpoint Protector 서버에 로그인할 수 있습니다.

Azure로 SSO (Single Sign On) 구성

- SSO를 사용하려면 '시스템 구성 > 시스템 설정 > SSO(Single Sign On)' 으로 이동합니다. 활성화하면 '장애조치 로그인 사용자' 를 선택할 수 있도록 드롭다운으로 표시됩니다. root 사용자가 기본으로 선택될 것입니다.



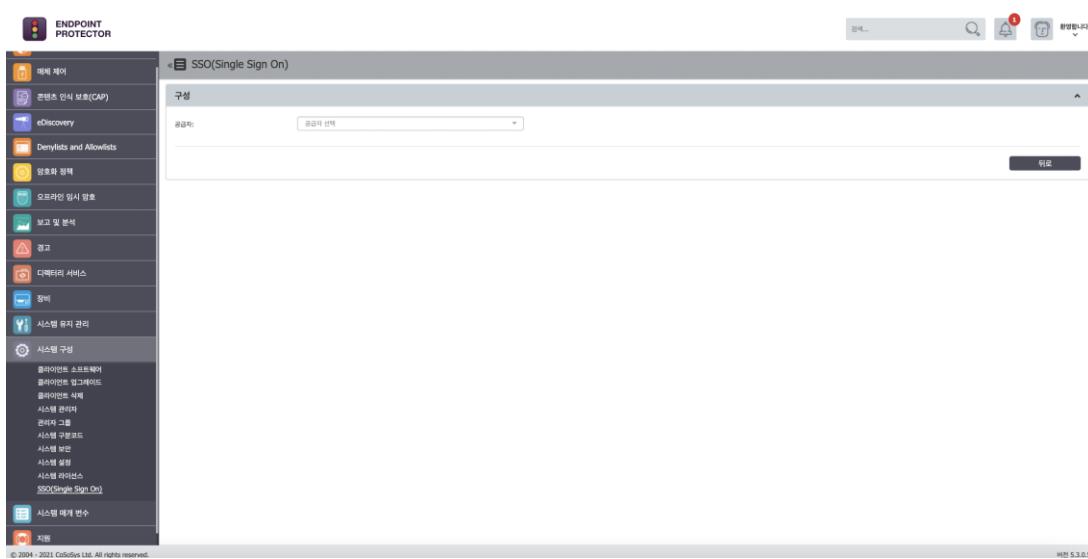
위의 단계가 완료되면 SSO(Single Sign On) 하위 섹션이 시스템 구성 섹션에 표시가 됩니다.

참고

선택된 장애조치 로그인 사용자는 선택된 동안 Endpoint Protector 서버에서 삭제할 수 없습니다.

장애조치 로그인 사용자가 없으면 SSO(Single Sign On)은 활성화되지 않습니다.

- SSO(Single Sign On) 하위 섹션이 나타나면 공급자를 선택합니다.



- portal.azure.com 이동 후 로그인합니다.
- Azure Active Directory로 이동합니다.
- 새로운 엔터프라이즈 애플리케이션을 만듭니다: 새로운 애플리케이션 추가 -> 자신만의 애플리케이션 만들기 -> 애플리케이션 이름 부여하기 -> '갤러리에서 찾지 못하는 다른 모든 애플리케이션 통합' 선택 -> 만들기

2.1.1 | Endpoint Protector | 사용 설명서

The screenshot shows the Microsoft Azure Default Directory Overview page. On the left, there's a navigation sidebar with links like Overview, Getting started, Preview features, Diagnose and solve problems, Manage (Users, Groups, External identities, Roles and administrators), and various Azure services. The main area displays a chart titled "Sign-ins" showing activity from March 28 to April 18, with a count of 67. Below the chart, there's a "Create" section with icons for User, Guest user, Group, and Enterprise application (which is highlighted with a red box). There are also sections for Featured services like Identity Secure Score, Policies, Privileged Identity Management, Tenant restrictions, Azure AD Domain Services, and Access reviews.

The screenshot shows the Azure AD Gallery interface. At the top, there's a header with a search bar and filter options for Single Sign-on: All, User Account Management: All, and Categories: All. Below the header, there's a message: "You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience." The main area is titled "Cloud platforms" and shows cards for Amazon Web Services (AWS), Google Cloud Platform, Oracle, and SAP. Each card has a logo and a link to the service's page.

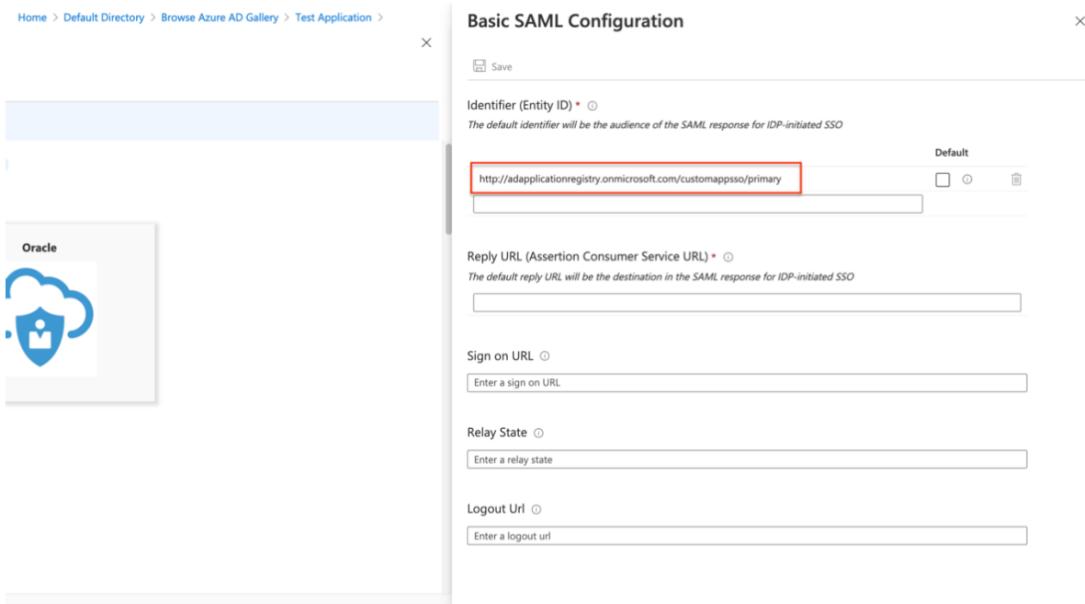
The screenshot shows the legacy Azure AD Gallery experience. It has a similar header and search/filter functionality. A message at the top says: "You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience." The main area is titled "Browse Azure AD Gallery" and shows the same "Cloud platforms" section with cards for AWS, Google Cloud, and SAP. To the right, there's a "Create your own application" overlay window. It asks for the name of the app and provides options for what to do with it: "Configure Application Proxy for secure remote access to an on-premises application", "Register an application to integrate with Azure AD (App you're developing)", and "Integrate any other application you don't find in the gallery (Non-gallery)" (which is selected and highlighted with a red box). A "Create" button is at the bottom of the overlay.

6. 새롭게 만들어진 애플리케이션을 선택하고 Single Sign On 이동 후 SAML을 선택합니다.

The screenshot shows the Microsoft Azure Test Application Overview page. The left sidebar has 'Single sign-on' selected. The main area shows 'Properties' with application details and a 'Getting Started' section with four steps: 1. Assign users and groups, 2. Set up single sign on (which is highlighted with a red box), 3. Provision User Accounts, and 4. Self-service. Below this is a 'What's New' section.

The screenshot shows the 'Select a single sign-on method' page. It offers three options: 'Disabled' (not enabled), 'SAML' (selected and highlighted with a red box), and 'Password-based'. The 'SAML' option is described as rich and secure authentication using the SAML protocol.

7. 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.
8. 기본 SAML 구성 페이지에서 기본으로 식별 완성된 데이터를 삭제합니다 (객체 편집).



9. Endpoint Protector 서버의 SSO(Single Sign On) 페이지로 가서 '서비스 공급자 -> 객체 ID' 데이터를 복사해서 기본 SAML 구성에서 식별자 (객체 ID) 영역과 URL 응답하기 (Assertion Consumer Service URL) 붙여 넣기를 하고 기본 설정(Default)에 체크합니다.

10. Endpoint Protector 서버의 '서비스 공급자 -> SSO(Single Sign On) 페이지에서 '로 그인 URL'을 복사하고 기본 SAML 구성 페이지의 'URL 서명'에 붙여 넣기 합니다.

The screenshot shows two side-by-side configuration interfaces. On the left is the 'Single Sign On' configuration for Endpoint Protector, where the 'Logout URL' field contains 'https://192.168.15.238/index.php/logout'. On the right is the 'Basic SAML Configuration' in Microsoft Azure, where the 'Sign on URL' field also contains 'https://192.168.15.238/index.php/login'. A red arrow highlights the connection between these two fields.

11. Endpoint Protector 서버의 '서비스 공급자 -> SSO(Single Sign On)' 페이지에서 '로그아웃 URL'을 복사하고 기본 SAML 구성 페이지의 '로그아웃 URL'에 붙여 넣기합니다.

This screenshot shows the same two configuration pages as the previous one. The 'Logout URL' field in the Endpoint Protector config has been updated to 'https://192.168.15.238/index.php/logout', and a red arrow points from this field to the 'Logout Url' field in the Microsoft Azure config, which now also contains 'https://192.168.15.238/index.php/logout'.

12. Single Sign On 테스트없이 설정을 저장합니다.

13. 페이지의 3번 단계인 SAML 서명 인증서와 편집으로 이동합니다.

215 | Endpoint Protector | 사용 설명서

Home > Default Directory > Browse Azure AD Gallery > Test Application >

Test Application | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan Manage Properties Owners Roles and administrators (Preview) Users and groups Single sign-on Provisioning Application proxy Self-service Security Conditional Access Permissions Token encryption Activity Sign-ins Usage & insights Audit logs Provisioning logs (Preview) Access reviews

Upload metadata file Change single sign-on mode Test this application Got feedback?

3 SAML Signing Certificate

Status: Active Expiration Date: 4/21/2024, 8:34:21 PM
Thumbprint: https://login.microsoftonline.com/1def8742-8c49-497a-a30...
Expiration: https://sts.windows.net/1def8742-8c49-497a-a30...
Notification Email: https://login.microsoftonline.com/1def8742-8c49-497a-a30...
App Federation Metadata Url: Download
Certificate (Base64): Download
Certificate (Raw): Download
Federation Metadata XML: Download

4 Set up Test Application

You'll need to configure the application to link with Azure AD.

Login URL: https://login.microsoftonline.com/1def8742-8c49-497a-a30...
Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a30...
Logout URL: https://login.microsoftonline.com/1def8742-8c49-497a-a30...
View step-by-step instructions

5 Test single sign-on with Test Application

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

14. 서명 알고리즘을 SHA-1으로 변경하고 저장합니다.

SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save + New Certificate Import Certificate

Status	Expiration Date	Thumbprint
Active	4/21/2024, 8:34:21 PM	...

Signing Option: Sign SAML assertion

Signing Algorithm: SHA-1

Notification Email Addresses:

15. 3번 단계인 SAML 서명 인증서에서 인증서 (Base64)를 다운로드합니다.

The screenshot shows the 'Test Application | SAML-based Sign-on' configuration page in the Azure AD portal. In the 'Single sign-on' section, there is a 'SAML Signing Certificate' card. This card displays the certificate status as 'Active', its thumbprint, expiration date (4/21/2024, 8:34:21 PM), and a 'Notification Email' field containing 'https://login.microsoftonline.com/1def8742-8c49...'. Below these fields are three download links: 'Certificate (Base64)', 'Certificate (Raw)', and 'Federation Metadata XML'. The 'Certificate (Base64)' link is highlighted with a red box. The entire 'SAML Signing Certificate' card is also highlighted with a larger red box.

16. 텍스트 편집기에서 다운로드한 인증서를 열고 콘텐츠를 복사합니다.

17. Endpoint Protector 서버의 '시스템 구성' -> SSO(Single Sign On) -> ID 공급자 -> 보안 인증서'로 이동해서 복사한 콘텐츠를 붙여 넣기 합니다.

The screenshot shows the 'Single Sign On' configuration page in the Endpoint Protector web interface. In the 'Identity Provider' section, there is a 'Security Certificate:' input field. A large blue box highlights the copied SAML certificate content, which starts with '-----BEGIN CERTIFICATE-----' and ends with '-----END CERTIFICATE-----'. A red arrow points from this highlighted area to the 'Security Certificate:' input field. The 'Save' and 'Test' buttons are visible at the bottom of the form.

18. Azure SAML 기반 서명 페이지로 돌아와서 4번 단계 -> "당신의 애플리케이션" 설정으로 이동하고 Azure AD 식별자를 복사합니다.

19. Endpoint Protector 서버의 '시스템 구성' -> SSO(Single Sign On) -> ID 공급자 -> Azure AD 식별자'로 이동해서 복사한 데이터를 붙여 넣기 합니다.

The screenshot shows two overlapping web pages. The left page is titled 'Single Sign On' under 'Service Provider' and lists Entity ID, Login URL, and Logout URL. The right page is titled 'SAML-based Sign-on' and shows Azure AD Identifier, Login URL, and Logout URL. A red arrow points from the 'Azure AD Identifier' field on the right to the 'Identity Provider' section on the left.

20. Azure SAML 기반 서명 페이지로 돌아와서 4번 단계 -> “당신의 애플리케이션” 설정으로 가서 로그인 URL을 복사합니다.

21. Endpoint Protector 서버에서 ‘시스템 구성’ -> SSO(Single Sign On) -> ID 공급자 -> 로그인 URL’로 이동 후 복사한 데이터를 붙여 넣기 합니다.

The screenshot shows the same two pages as above. The 'Identity Provider' section on the left now has 'https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2' selected in the dropdown. A red arrow points from the 'Logout URL' field on the right to the 'Logout URL' field on the left.

22. Azure SAML 기반 서명 페이지로 돌아와서 4번 단계 -> “당신의 애플리케이션” 설정으로 이동해서 로그아웃 URL을 복사합니다.

23. Endpoint Protector 서버의 ‘시스템 구성’ -> SSO(Single Sign On) -> ID 공급자 -> 로그아웃 URL’로 이동 후 복사한 데이터를 붙여 넣기 합니다.

SAML-based Sign-on

Service Provider

- Entity ID: https://192.168.15.238
- Login URL: https://192.168.15.238/index.php/login
- Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

- Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a304-1019540da191/
- Login URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2
- Security Certificate: (Redacted)
- Logout URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191/saml2

Test

Set up Test Application

Test single sign-on with Test Application

Test

© 2004 - 2021 CoSoSys Ltd. All rights reserved. Version 5.3.0.5

24. Endpoint Protector 서버의 ‘시스템 구성 -> SSO(Single Sign On) -> 장애조치 로그인 URL 및 URL 저장’에서 장애조치 로그인 URL 만들기를 합니다.

Single Sign On

Configuration

Provider: Azure AD

Failover Login URL

Failover Login URL: https://192.168.15.238/index.php/login?failover_log

Display Failover Login URL: ON

Service Provider

Use Domain instead of IP: OFF

Entity ID: https://192.168.15.238

Logout URL: https://192.168.15.238/index.php/logout

Identity Provider

Azure AD Identifier: https://sts.windows.net/1def8742-8c49-497a-a304-11

Security Certificate: (Redacted)

Logout URL: https://login.microsoftonline.com/1def8742-8c49-497a-a304-1019540da191

Save

© 2004 - 2021 CoSoSys Ltd. All rights reserved. Version 5.3.0.5

25. Endpoint Protector 서버의 SSO 페이지에서 설정을 저장합니다.

26. Azure -> 왼쪽 메뉴의 사용자 및 그룹을 선택합니다.

219 | Endpoint Protector | 사용 설명서

The screenshot shows the Azure AD Test Application configuration page. On the left, there's a navigation sidebar with sections like Overview, Deployment Plan, Manage (Properties, Owners, Roles and administrators (Preview), **Users and groups**, Single sign-on, Provisioning, Application proxy, Self-service), Security (Conditional Access, Permissions, Token encryption), Activity (Sign-ins, Usage & insights, Audit logs, Provisioning logs (Preview)), and a bottom section for Activity (Sign-ins, Usage & insights, Audit logs, Provisioning logs (Preview)). The 'Users and groups' link is highlighted with a red box. The main content area has three numbered steps: 3. SAML Signing Certificate, 4. Set up Test Application, and 5. Test single sign-on with Test Application. Step 3 shows details like Status (Active), Thumbprint, Expiration (4/21/2024, 8:34:21 PM), Notification Email (iulia@testazureendpointprotecto.onmicrosoft.com), App Federation Metadata Url (https://login.microsoftonline.com/1def8742-8c49...), Certificate (Base64), Certificate (Raw), and Federation Metadata XML. Step 4 shows Login URL (https://login.microsoftonline.com/1def8742-8c49...), Azure AD Identifier (https://sts.windows.net/1def8742-8c49-497a-a30...), and Logout URL (https://login.microsoftonline.com/1def8742-8c49...). Step 5 shows a 'Test' button.

27. '사용자/그룹 추가 -> 선택 없음 -> 원하는 Azure 사용자 검색 -> 선택 -> 할당'으로 이동합니다.

The screenshot shows the 'Users and groups' list page for the Test Application. The left sidebar is identical to the previous screenshot. The main area shows a table with columns: Display Name, Object Type, and Role assigned. A note says 'First 100 shown, to search all users & groups, enter a display name.' Below the table, it says 'No application assignments found'. At the top of the list area, there's a button labeled '+ Add user/group' which is highlighted with a red box. Other buttons in the header include Edit, Remove, Update Credentials, Columns, and Got feedback?.

220 | Endpoint Protector | 사용 설명서

The image consists of three vertically stacked screenshots from the Azure AD portal, illustrating the process of adding a user assignment to a test application.

Screenshot 1: The 'Add Assignment' screen shows the 'Users and groups' section with a red box around the 'None Selected' link. Below it are 'Select a role' and 'Default Access' buttons. At the bottom is an 'Assign' button.

Screenshot 2: A modal window titled 'Users and groups' is open. It includes a search bar, a list of service accounts (AAD DC Service Accounts), and a 'Selected items' section. The 'Select' button at the bottom right is highlighted with a red box. The main 'Add Assignment' screen is visible in the background.

Screenshot 3: The 'Add Assignment' screen again, but now the 'Users and groups' section shows '1 user selected.' with a red box around it. The 'Assign' button at the bottom is highlighted with a red box.

28. 사용자는 애플리케이션에 할당되고 Azure로 Endpoint Protector 로그인을 할 수 있습니다.
29. Endpoint Protector 서버에서 로그인하고 다시 접근하면 관리자는 Azure 로그인 프로세스를 위해서 <http://login.microsoftonline.com>으로 리다이렉트 되어야 합니다.

15. 시스템 매개 변수

15.1. 장치 유형 및 알림

이 섹션에서 관리자는 각 운영 체제에 따라서 사용 가능한 매체 유형을 전반적으로 볼 수 있습니다. 게다가 이러한 장치가 콘텐츠 인식 보호 모듈로 검사가 가능한지 여부를 이 테이블에서 확인 할 수 있습니다.

추가적으로 이 섹션은 관리자가 Endpoint Protector 클라이언트에서 보여주는 알림 메시지를 편집 할 수 있습니다.

The screenshot shows the Endpoint Protector software interface. On the left, there is a sidebar with various menu items: 메체 제어, 콘텐츠 인식 보호(CAP), eDiscovery, 거부목록 및 허용목록, 암호화 정책, 오프라인 임시 암호, 보고 및 분석, 경고, 디렉토리 서비스, 장비, 시스템 유지 관리, 시스템 구성, 시스템 매개 변수 (selected), 장치 유형 및 알림 (selected), 문맥 감지, 고급 스캔ning 예외 권한, 이벤트, User Remediation, and 지원. The main content area has a title '시스템 매개 변수 - 장치 유형 및 알림' and a sub-section title '장치 유형 및 알림의 목록'. It includes a filter dropdown, a table with columns: 장치 유형, 설명, 장치 제어 알림, 콘텐츠 인식 보호(CAP) 알림, 사용자 정의 알림, and 작업. The table lists various device types like USB 저장장치, 디지털 키예라, 스마트폰, 노키아폰, 내장 카드 리더, PCMCIA 장치, FireWire(1394) 저장장치, ZIP 드라이브, and 내장 CD/DVD/BR 드라이브, along with their descriptions and system compatibility. At the bottom, there are buttons for 사용자 정의 알림 사용 and 사용자 정의 알림 사용 중지, and a navigation bar with 이전, 뒤로, and 버전 5.4.0.0.

사용자 정의 알림 목록을 확장하고 원하는 언어를 선택 함으로써 표시된 메시지를 수정할 수 있습니다. 게다가 관리자가 일부 알림 표시를 원하지 않는 경우에 체크하지 않을 수 있습니다.

정보

사용자 정의 클라이언트 알림은 '매체 제어 > 전체 설정'에서 전체적으로 사용할 수 있습니다. 또한 컴퓨터 또는 그룹에 개별적으로 사용할 수도 있습니다.

제작 장치	구형 노트북 모델과 같은 PCMCIA 인터페이스에 연결된 장치	Windows	n/a	사용 중지
PCMCIA 장치				
FireWire(1394) 저장장치	FireWire 버스에 연결된 저장장치	Windows, MAC	Windows, MAC	사용 중지
ZIP 드라이브	ZIP 드라이브 플로피 디스크 저장 장치	Windows	Windows	사용 중지
내장 CD/DVD/BR 드라이브	CD, DVD, Blu-ray 드라이브 같은 내장 광학 디스크 드라이브 장치	Windows, MAC, Linux	n/a	사용 중지

List of Default Notifications

Custom Content Aware Protection Notifications

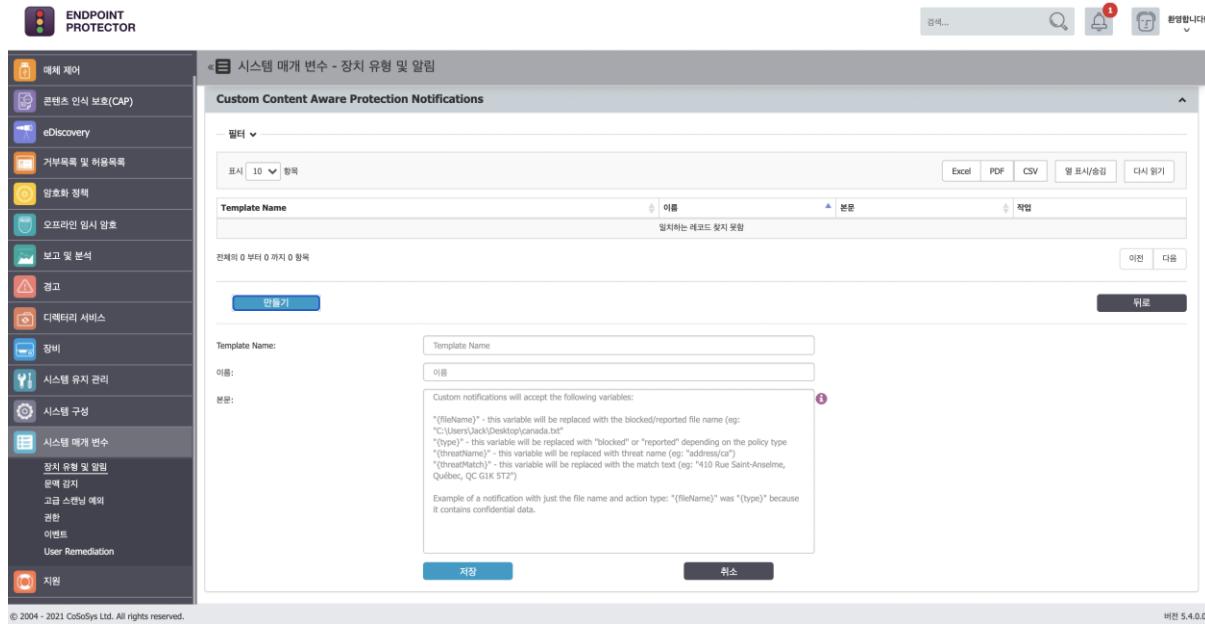
만들기

버전 5.4.0.0

사용자 정의 콘텐츠 인식 보호 알림에서 관리자는 사용자 정의 알림을 만들 수 있습니다. 이 알림은 이 알림은 콘텐츠 인식 정책마다 설정이 가능해서 특정 콘텐츠 인식 정책에 특정한 클라이언트 알림이 가능합니다.

새로운 알림을 추가하기 위해서 만들기 버튼을 누르고 템플레이트 이름, 제목, 본문 텍스트를 설정하시기 바랍니다. 본문 텍스트는 몇 가지 변수를 허용합니다:

- ⑩ "{filename)": 차단 및 보고되는 파일 이름을 대체함;
- ⑩ "{type)": 정책 유형에 따라서 차단 및 보고를 대체함;
- ⑩ "{threatName)": 위협 이름을 대체함;
- ⑩ "{threatMatch)": 일치하는 텍스트를 대체함;



예제:

파일 이름과 액션 유형이 포함된 알림 예제입니다:

기밀 데이터가 포함되어 있어서 "{fileName}"은 "{type}" 입니다.

알림이 만들어진 후에 이 알림이 필요한 콘텐츠 인식 정책으로 가서 해당 정책에 원하는 알림을 알림 템플레이트에서 선택하시기 바랍니다.

15.1.1. Trusted Devices

전송 데이터를 보호하는 것은 필수적입니다. 장치가 분실 및 도난이 되었을 때 제 3가 데이터에 접근을 못하도록 해야 합니다. 암호화 정책 솔루션으로 관리자는 휴대용 저장 장치의 기밀 데이터를 도난 및 분실에서 보호할 수 있습니다.

Endpoint Protector가 설치된 컴퓨터에서 암호화된 장치만 사용할 수 있는 것은 Trusted Devices를 활용할 수 있습니다. Trusted Devices는 Endpoint Protector 서버에서 인가를 받아야합니다. 그렇지 않으면 사용할 수 없습니다. Trusted Devices는 보안 4단계로 나뉩니다.

- **레벨1** – 오피스와 개인을 위한 최소한의 보안으로 데이터 보안 암호화 기반 소프트웨어에 초점을 맞추어 사용합니다. 모든 USB 플래시 드라이브와 대부분의 휴대용 저장 장치는 Trusted Device 레벨1으로 변경할 수 있습니다. 특정 하드웨어 장치가 필요 없고 EasyLock과 같은 암호화 솔루션을 사용합니다.
- **레벨2** – 데이터 암호화 기반의 생체 데이터 보호 또는 고급 소프트웨어의 중간 보안 레벨입니다. 보안 소프트웨어가 포함된 특별한 하드웨어가 필요하며 Trusted Device 레벨2로 테스트 됩니다.
- **레벨3** – SOX, HIPAA, GBLA, PIPED, Basel II, DPA 또는 PCI 95/46/EC와 같은 규정 준수를 위해 의무화된 암호화 기반의 강력한 하드웨어를 가진 높은 보안 레벨입니다. Trusted Device Level 3에서 테스트된 사전 보안 소프트웨어와 하드웨어 기반 암호화를 포함하는 특별한 하드웨어가 필요합니다.
- **레벨4** – 군대 또는 정부에서 사용하는 최고 보안 레벨입니다. 레벨4 Trusted Devices는 데이터 보호 암호화 기반의 강력한 하드웨어를 포함하고 독립적인 인증 (예> FIPS140)을 가집니다. 이 장치는 소프트웨어 및 하드웨어의 철저한 검사를 성공적으로 받은 것입니다. 보안에 집중한 대리점을 통하여 주로 얻을 수 있는 특정 하드웨어를 요구합니다.
- **레벨1+** - 레벨1의 확장으로 마스터 암호를 가진 EasyLock은 Endpoint Protector가 설치된 컴퓨터에 USB 저장 장치를 연결하면 자동으로 배포됩니다. 현재 이 서비스는 제공하고 있습니다.

정보

TD 레벨 1이 사용 가능하고 TD 레벨 2, 3 또는 4가 연결되어 있으면 권한은 그에 맞춰서 적용됩니다.

아래 테이블에서 TrustedDevices 목록을 참조 바랍니다.

장치 이름	TrustedDevices 레벨
EasyLock 장치	1
AT1177	2
UT169	2
UT176	2
Trek ThumbDrive	2
BitLocker 암호화 장치	3
FileVault 암호화 장치	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 DataTraveler Locker+	3
Lexar 1 (Locked 1 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

15.2. 문맥 감지

이 섹션에서 관리자는 전체 시스템에 대한 문맥 감지를 관리할 수 있습니다. 실행을 하면 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).

팁

탐지된 민감한 정보는 맥락에 맞게 검색이 되어 이 기능은 오탐을 줄이는데 도움이 됩니다.

참조

이 기능은 콘텐츠 인식 보호 및 eDiscovery 정책에 모두 적용됩니다. 실행하면 맥락 탐지가 시스템을 통해 콘텐츠 탐지를 대신합니다.

이 기능을 실행하기 전에 여러분의 시나리오 규칙과 관련성을 확인하시기 바랍니다.

문맥 감지가 실행되면 Contextual XML에 정의된 규칙을 기반으로 전체 수준으로 적용됩니다. 이 설정은 콘텐츠 인식 보호 및 eDiscovery 정책에 모두 영향을 줍니다.

문맥 규칙을 만드는 두 가지 옵션이 있습니다.

- Endpoint Protector 서버에서 직접 만들기
- 수동으로 문맥 XML을 편집 후 Endpoint Protector 서버에 업로드 하기

15.2.1. XML 만들기

정보

이 방법은 가장 쉬운 방법으로 대부분의 사용자 케이스를 다룰 수 있어서 권장합니다.

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):** 관련된 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)

참조

문맥 규칙을 만들거나 변경한 후에 Contextual XML 만들기 버튼을 누르는 것을 잊지 마시기 바랍니다.

15.2.2. XML 업로드

정보

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 함수를 결정하는 추가적인 함수가 고려됩니다.

팁

Contextual XML에 필요한 문법을 이해하는 가장 좋은 방법은 여러가지 예제가 포함된 Endpoint Protector에서 사용할 수 있는 샘플을 보는 것입니다.

아래 샘플을 참조하여 명확한 방향성을 이해하시기 바랍니다.

예제

```
<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 -->
```

예제

```
<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">
```

```

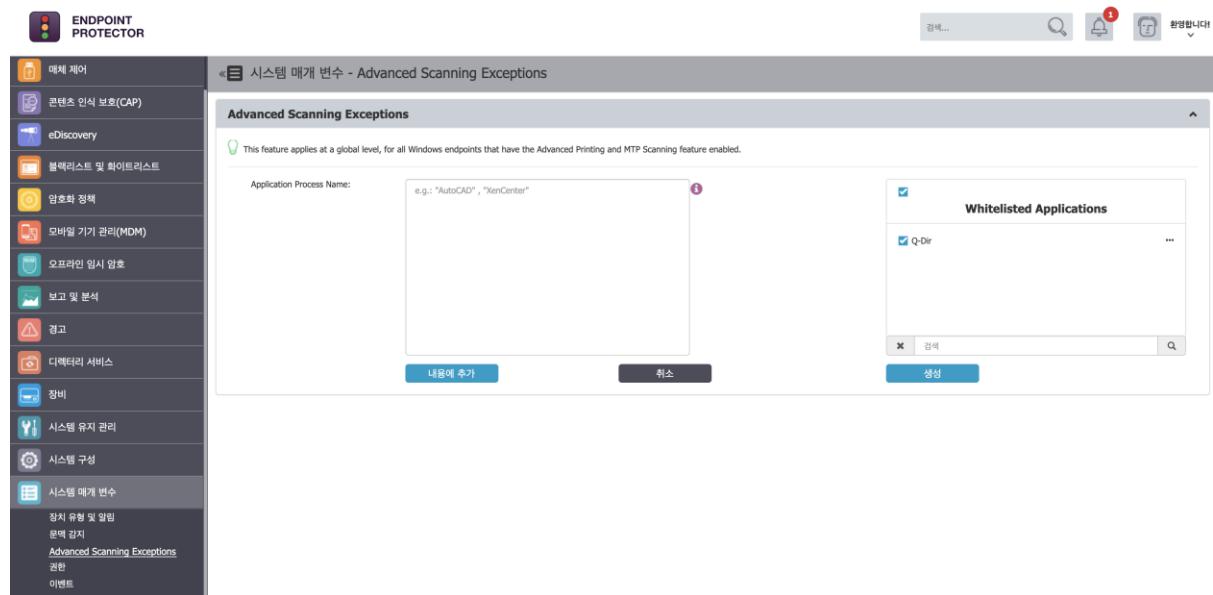
<Group matchStyle="word">
    <Term>random word</Term>
</Group>
</Keyword>
<Regex id="regex_email_id">[-0-9a-zA-Z.+_]+@[ -0-9a-zAZ.+_]+[a-zA-Z]{2,4}</Regex>
</Rules>
</RulePackage>

```

15.3. 고급 스캐닝 예외

Windows 환경은 고정적이고 보안 업데이트와 설치된 응용프로그램은 계속해서 발전합니다. Endpoint Protector 클라이언트 간섭을 피하기 위해서 응용프로그램과 프로세스의 허용목록이 가능합니다.

엔드포인트 컴퓨터에 향상된 프린터 및 MTP 검색 기능이 활성화 되어 있을 때 고급 스캐닝 예외 기능은 이러한 검색에서 원하는 응용프로그램을 예외처리 합니다.



정보

이 기능은 글로벌 레벨로 '향상된 프린터 및 MTP 검색 기능'이 활성화된 모든 Windows 엔드포인트 컴퓨터에 적용됩니다.

15.4. 권한

이 섹션은 장치에 적용할 수 있는 모든 접근 권한 목록을 보여줍니다.

이름	설명
사용 허용	사용 허용
사용 허용 및 CAP 검색 제외	사용 허용 및 CAP 검색 제외
사용 허용 및 CAP 검색에 사용자 클래스 포함	사용 허용 및 CAP 검색에 사용자 클래스 포함
TD 레벨 1 허용	TD 레벨 1 장치 사용 허용
TD 레벨 1+ 허용	TD 레벨 1+ 장치 사용 허용
TD 레벨 1+ 허용, 그 외 읽기만	TD 레벨 1+ 장치 사용 허용, 그 외 읽기만
TD 레벨 2 허용	TD 레벨 2 장치 사용 허용
TD 레벨 3 허용	TD 레벨 3 장치 사용 허용
TD 레벨 3 허용, 그 외 읽기만	TD 레벨 3 장치 사용 허용, 그 외 읽기만
TD 레벨 4 허용	TD 레벨 4 장치 사용 허용

15.5. 이벤트

이 섹션은 Endpoint Protector 로그의 이벤트 목록을 보여줍니다. 추가적으로 액션 컬럼은 이벤트 이름과 설명을 편집 또는 특정 이벤트 로그를 사용하지 못하게 하는 옵션을 제공합니다.

이 섹션에서 관리자는 Endpoint Protector 이벤트 목록을 관리할 수 있습니다. 이벤트 이름 및 설명 편집 또는 특정 이벤트를 사용하지 못하게 하는 옵션을 사용할 수 있습니다.

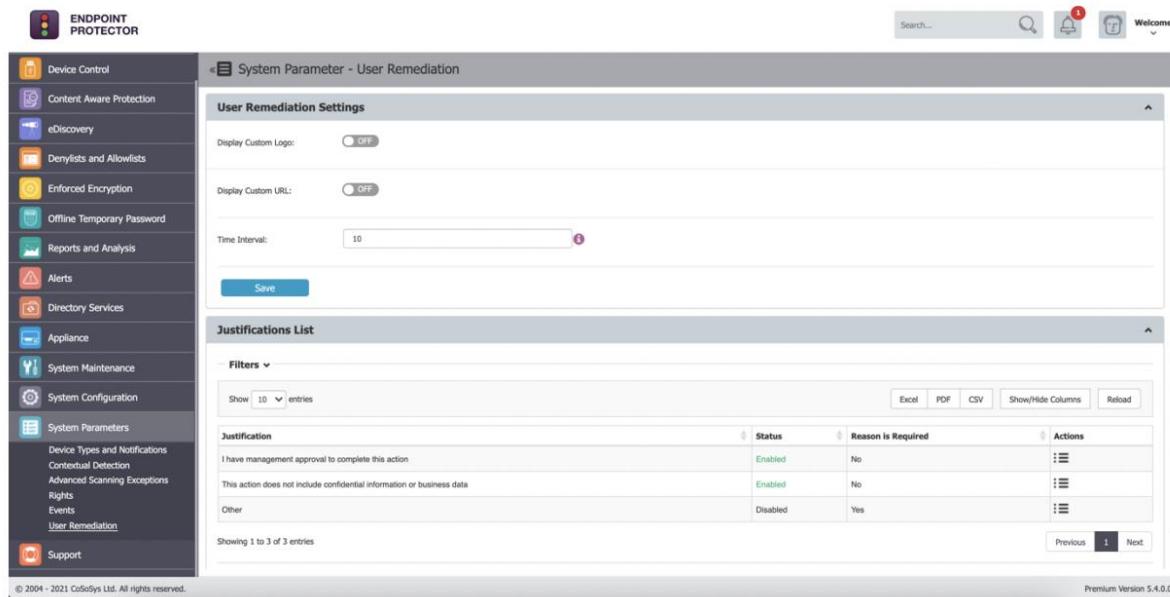
The screenshot shows the 'System Event' section of the Endpoint Protector interface. On the left, there's a sidebar with various icons and labels: 매체 제어, 콘텐츠 인식 보호(CAP), eDiscovery, 블랙리스트 및 화이트리스트, 암호화 정책, 모바일 기기 관리(MDM), 오프라인 임시 암호, 보고 및 분석, 경고, 디렉터리 서비스, 장비, 시스템 유지 관리, 시스템 구성, 시스템 메개 변수, 장치 유형 및 알림, 문의 감지, Advanced Scanning Exceptions, 권한, 이벤트, and 지원. The '이벤트' item in the sidebar is underlined, indicating it's the current section. The main area has a title '시스템 메개 변수 - 이벤트' and a sub-title '연결됨'. It includes a search bar, a notification bell icon with a red '1', and a '환영합니다!' message. Below these are buttons for Excel, PDF, CSV, 열 표시/숨김, and 다시 읽기. A table lists system events with columns for 이름 (Name), 설명 (Description), 상태 (Status), and 작업 (Actions). The table includes rows for '연결됨' (Device Connected) and '연결 끊어짐' (Device Disconnected), both marked as '사용 가능' (Available). There are also sections for '로그 작성' (Log Writing) and '저장' (Save), along with a detailed table of file-related events like 파일 읽기, 파일 쓰기, 파일 읽기/쓰기, 파일 이름 바꾸기, 파일 삭제, TD 장치, 삭제됨, and 읽기 전용 사용. At the bottom, there are navigation links for 이전 (Previous), 1 (Current page), 2, 3, 4, 다음 (Next), and a '뒤로' (Back) button.

15.6. 사용자 조치

참고

이 섹션은 서버에 프리미엄 라이선스가 있어야 사용할 수 있습니다.

이 섹션에서 관리자는 사용자 조치 알림을 사용자 정의할 수 있습니다.



사용자 정의 로고 보이기

이 설정에서 관리자는 팝업 알림에 나오는 원하는 로고를 업로드 할 수 있습니다.

사용자 정의 URL 보이기

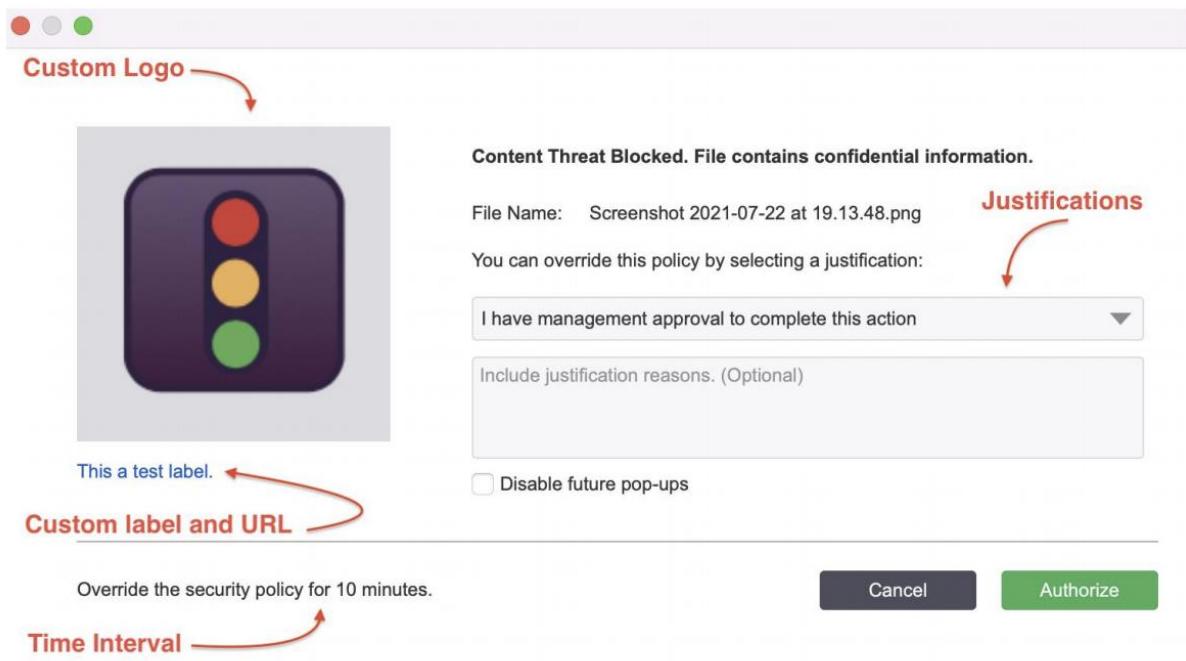
최종 사용자의 특정 웹 페이지 URL을 이 하위 섹션에서 설정할 수 있습니다.

사용자 정의 URL 레이블

이 설정은 '사용자 정의 URL 보이기' 가 활성화 될 때만 사용할 수 있습니다. 관리자는 이전에 추가한 사용자 정의 URL 레이블을 설정할 수 있습니다.

시간 간격

최종 사용자가 차단 및 조치된 위협을 조치할 수 있는 시간 간격을 설정할 수 있습니다.



정당한 사유 항목

정당한 사유는 위협이 조치된 이유입니다. 최종 사용자는 위협 조치를 위해서 정당한 사유를 반드시 선택해야 합니다.

이 섹션에서 정당한 사유를 관리합니다: 사용함, 사용할 수 없음 또는 사용자 정의로 만들 수 있습니다.

일부 정당한 사유는 기본적으로 서버에 이미 추가되어 있습니다. 그러나 새로운 정당한 사유는 추가 버튼을 클릭해서 만들 수 있습니다.

Justification	Status	Reason is Required	Actions
I have management approval to complete this action	Enabled	No	
This action does not include confidential information or business data	Enabled	No	
Other	Disabled	Yes	

Justification:

Status:

Reason is Required:

사용자 조치 팝업 알림은 'Endpoint Protector 클라이언트 설정 -> 사용자 조치 팝업'에서 활성화, 비활성화 또는 강제화 할 수 있습니다.

참고

테이블에 최소한 정당한 사유가 항상 사용할 수 있도록 되어 있어야 합니다.

16. Endpoint Protector 클라이언트

Endpoint Protector 클라이언트는 Windows, macOS, Linux의 엔드포인트를 보호하는 Endpoint Protector 서버에서 권한 및 설정을 받아서 제어합니다.

Endpoint Protector 클라이언트는 Endpoint Protector UI에서 직접 다운로드 받을 수 있습니다.

정보

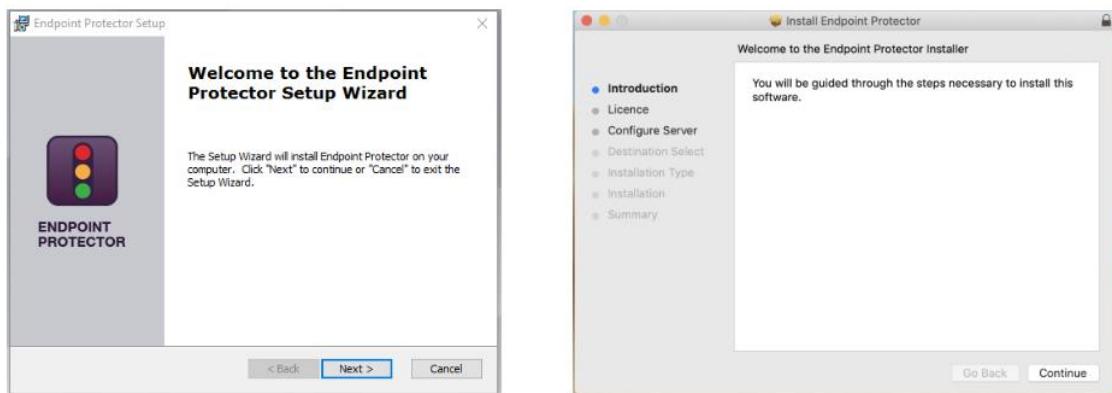
Endpoint Protector 클라이언트 다운로드에 대한 자세한 내용은 '14.1 클라이언트 소프트웨어'를 참조하시기 바랍니다.

팁

Active Directory 또는 Jamf 같은 도구는 Endpoint Protector 클라이언트를 대규모 네트워크에 배포하는데 사용할 수 있습니다.

16.1. 클라이언트 설치

Windows와 Mac용 Endpoint Protector 클라이언트는 설치가 쉬워서 누구나 따라 할 수 있습니다. 설치 풀더와 서버 정보를 설정해야 하지만 이미 미리 설정이 되어 있어서 '다음' 버튼만 클릭하시면 됩니다.

**참고**

Linux 클라이언트 설치는 `readmeLinux.txt` 파일을 참조하시기 바랍니다.

팁

Endpoint Protector Linux 클라이언트 1.4.0.4 버전에서는 레포지토리에서 클라이언트를 설치할 수 있는 옵션이 있습니다. 아래 내용을 참조하시기 바랍니다.

이 옵션은 Ubuntu 14.04+, Mint 18.X, CentOS 7.X, Fedora 29, OpenSUSE 42.2 /42.3 에서 사용 할 수 있습니다.

16.1.1. 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.

The screenshot shows the 'Endpoint Protector 클라이언트 설치' section of the web interface. It lists download links for various operating systems:

- Windows:** Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2003/2008/2012/2016/2019
- MAC:** macOS 11.0 (Big Sur), macOS 10.15 (Catalina), macOS 10.14 (Mojave), macOS 10.13 (High Sierra), macOS 10.12 (Sierra), macOS X 10.11 (El Capitan), macOS X 10.10 (Yosemite), macOS X 10.9 (Mavericks), macOS X 10.8 (Mountain Lion), macOS X 10.7 (Lion)
- Linux:** Debian, Ubuntu, Linux Mint, RHEL, CentOS, Fedora, openSUSE, SUSE Enterprise

Below the MAC section, it says: "Clients for Unix distributions are only available on request due to different kernel versions and dependencies." and "Endpoint Protector는 CentOS 6.5 이상의 최신 패치를 지원합니다."

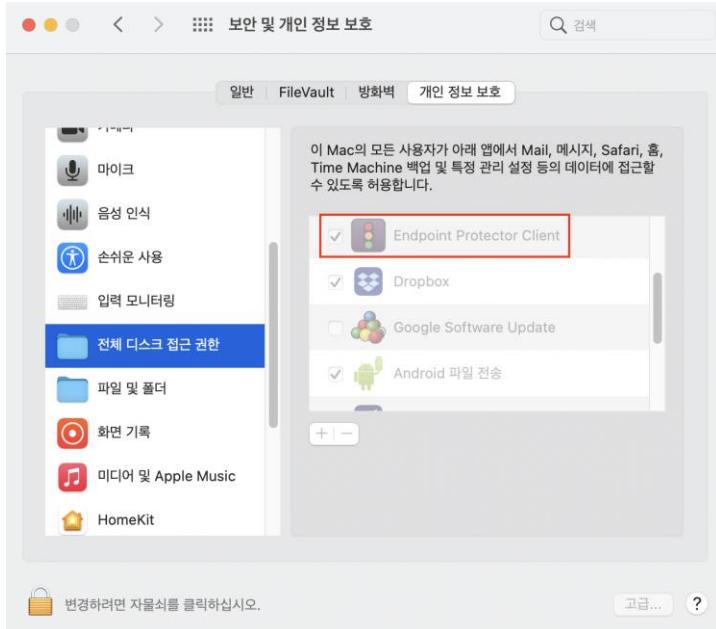
At the bottom, there is a '다운로드' (Download) button.

3. 다운로드 파일 압축을 해제합니다.

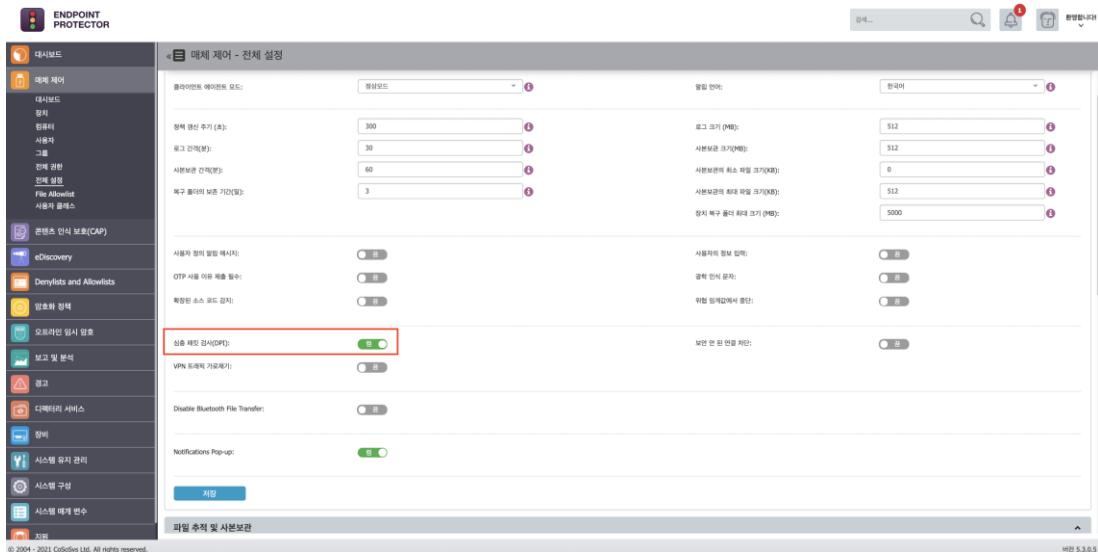
4. .pkg 파일을 열고 설치 단계를 따릅니다. 권한을 허용합니다.

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.

2 4 1 | Endpoint Protector | 사용 설명서

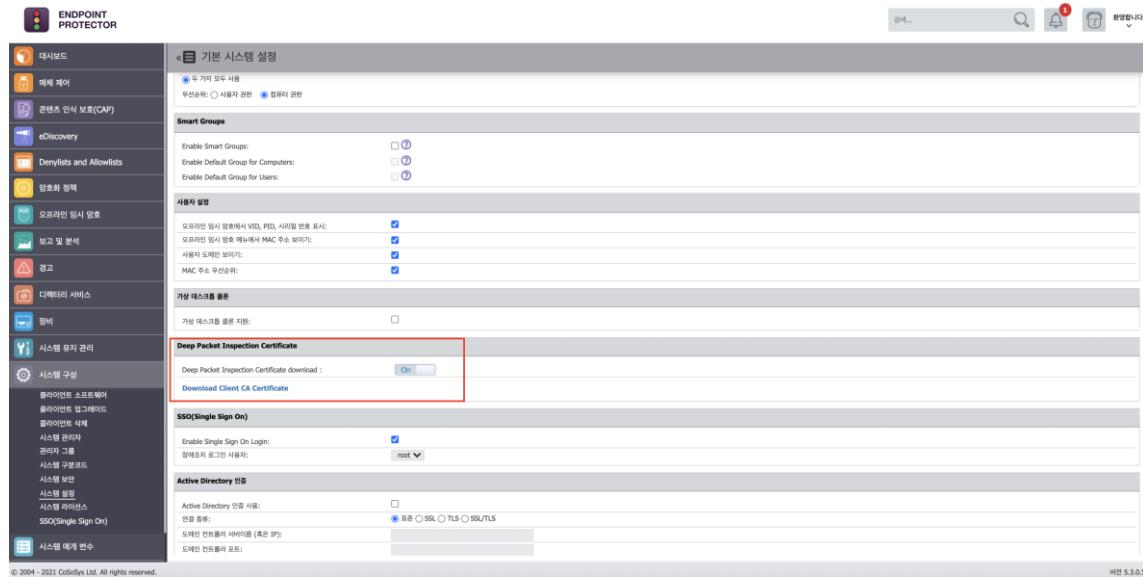


6. Endpoint Protector 서버로 이동해서 매체 제어 하위 섹션에서 심층 패킷 검사(DPI) 기능을 활성화합니다: 사용자/컴퓨터/그룹/전체 설정 -> 설정 관리 -> Endpoint Protector 클라이언트 -> 심층 패킷 검사(DPI).

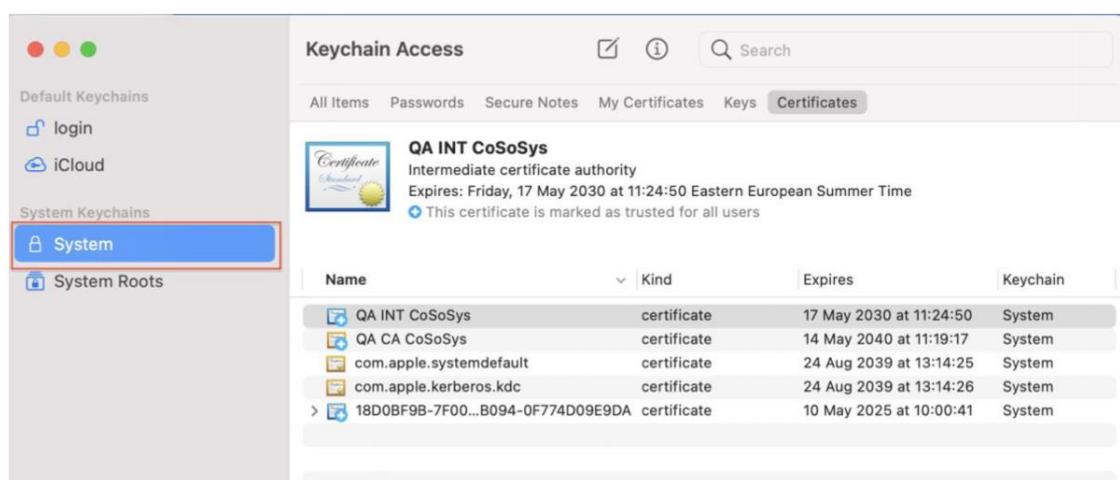


2 4 2 | Endpoint Protector | 사용 설명서

7. 시스템 구성 -> 시스템 설정 -> DPI 인증서에서 CA 인증서를 다운로드합니다.



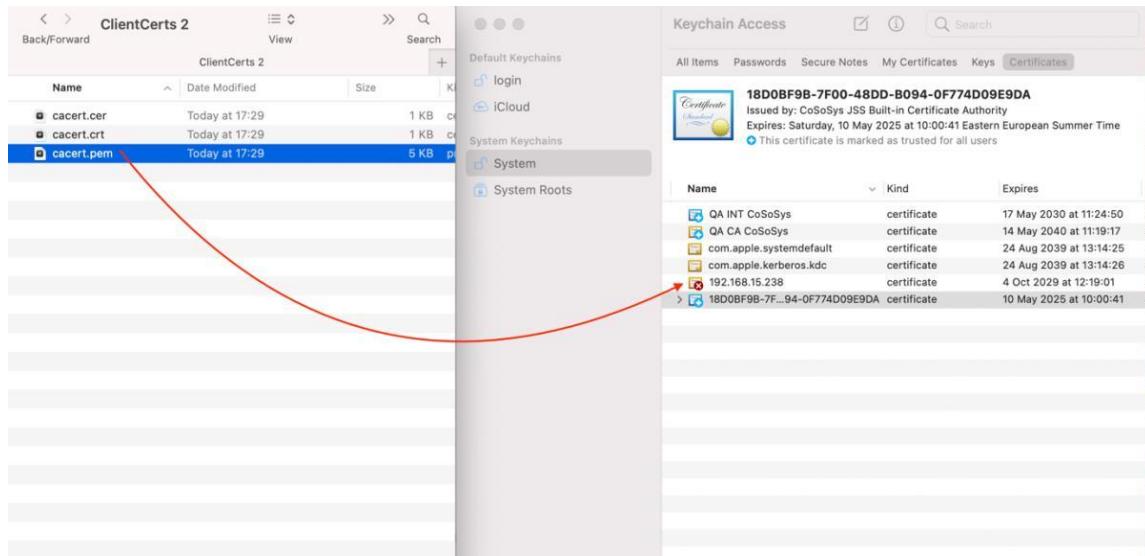
8. macOS에서 키 체인 접근 응용프로그램을 열고 시스템을 선택합니다.



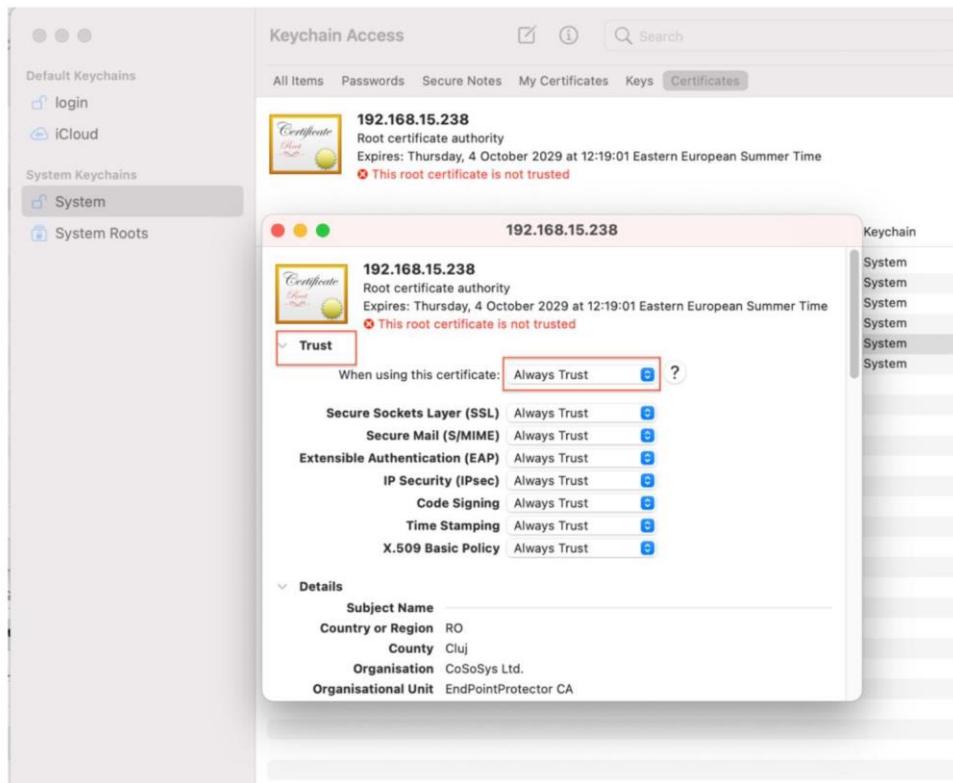
9. 다운로드된 ClientCert 파일 압축을 해제합니다.

10. cacert.pem 파일을 선택하고 '키 체인 접근' -> '시스템'에 드래그 앤 드롭합니다.

2 4 3 | Endpoint Protector | 사용 설명서



11. 새롭게 추가된 인증서에 'x' 표시가 됩니다. 더블 클릭하고 신뢰 섹션에서 '항상 신뢰'를 선택합니다.



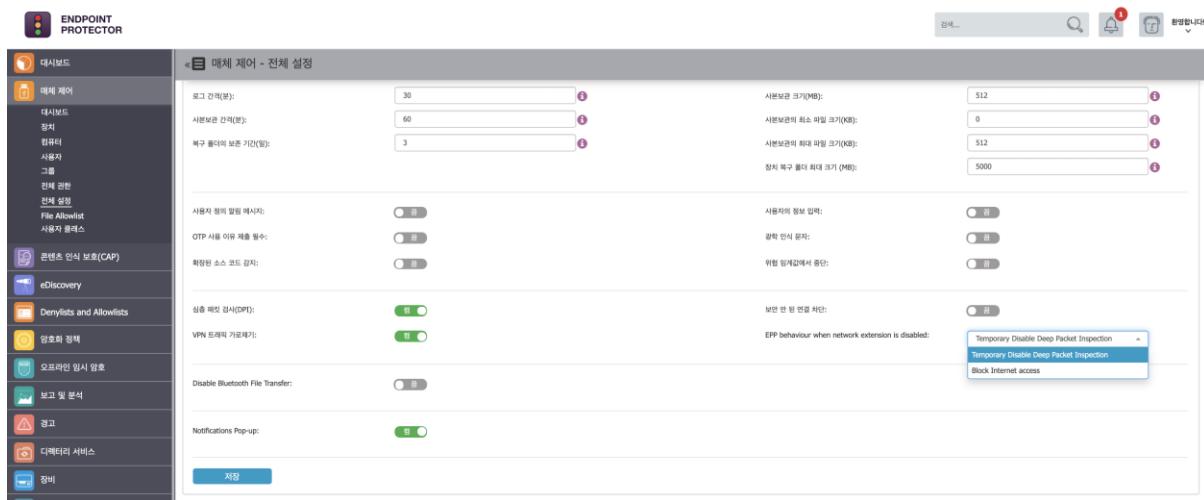
12. 변경 내용을 저장합니다.

13. VPN 트래픽 가로채기를 활성화합니다.

14. 네트워크 확장을 사용할 수 없을 때 EPP 동작 옵션을 선택합니다.

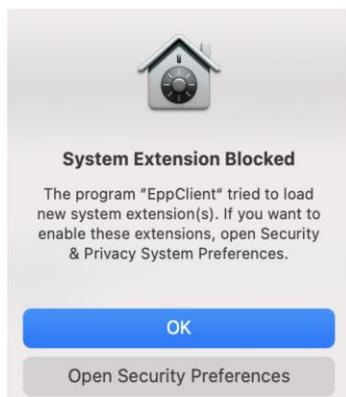
참고

- **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.

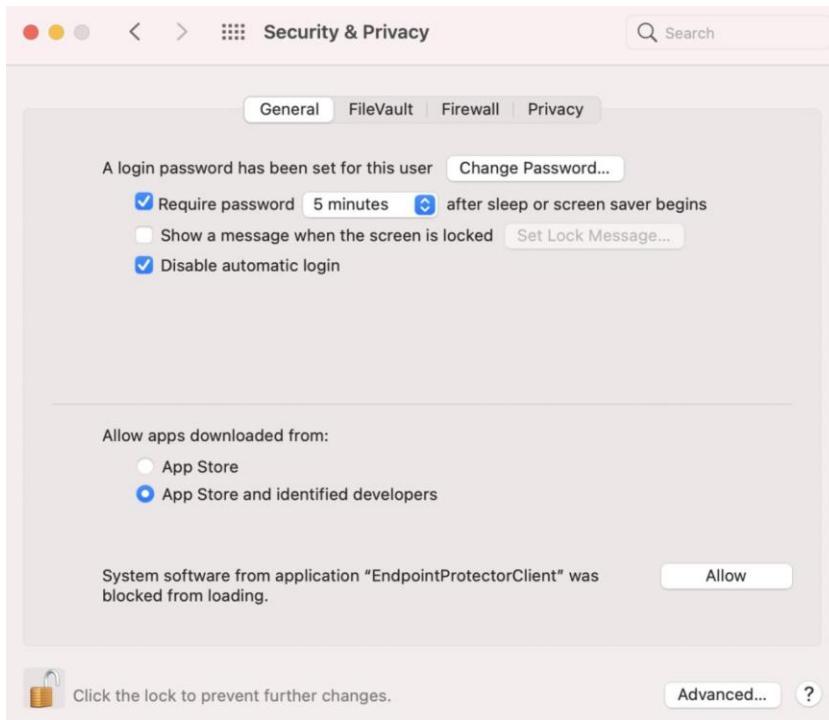


15. 변경 내용을 저장합니다.

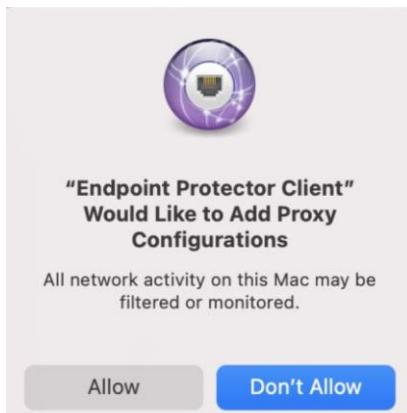
16. 시스템 확장 차단과 허용이 필요하다는 것을 최종 사용자에게 알려주는 다음 팝업이 표시됩니다.



17. '시스템 환경설정 -> 보안 및 개인 정보 보호 -> 일반 탭에서 Endpoint Protector Client 확장 허용' 을 합니다.



18. 다음 화면이 표시되면 Endpoint Protector 프록시 설정을 허용합니다.



정보

네트워크 확장이 성공적으로 사용 가능하면 클라이언트 무결성 OK 로그가 생성됩니다.

19. macOS 클라이언트 설치를 완료합니다.

16.1.2. Debian 기반 배포

방법은 비슷하지만 각 배포 버전마다 차이가 있습니다.

Ubuntu 19 – amd64

```
# echo "deb
https://download.endpointprotector.com/repo/deb/Ubuntu/19.04/amd64/ /"
> /etc/apt/sources.list.d/epprepo.list

# wget -q -O -
https://download.endpointprotector.com/repo/deb/Ubuntu/19.04/amd64/KEY.
gpg | apt-key

# apt update

# apt-get install epp-client
```

Ubuntu 18 – amd64

```
# echo "deb
https://download.endpointprotector.com/repo/deb/Ubuntu/18.04/amd64/ /"
> /etc/apt/sources.list.d/epprepo.list

# wget -q -O -
https://download.endpointprotector.com/repo/deb/Ubuntu/18.04/amd64/KEY.
gpg | apt-key add -

# apt update

# apt-get install epp-client
```

Ubuntu 16 – amd64

```
# echo "deb
https://download.endpointprotector.com/repo/deb/Ubuntu/16.04/amd64/ /"
> /etc/apt/sources.list.d/epprepo.list

# wget -q -O -
https://download.endpointprotector.com/repo/deb/Ubuntu/16.04/amd64/KEY.
gpg | apt-key add -

# apt update

# apt-get install epp-client
```

Ubuntu 16 – i386

```
# echo "deb
https://download.endpointprotector.com/repo/deb/Ubuntu/16.04/i386/ /" >
/etc/apt/sources.list.d/epprepo.list

# wget -q -O -
https://download.endpointprotector.com/repo/deb/Ubuntu/16.04/i386/KEY.gp
g | apt-key add -

# apt update

# apt-get install epp-client
```

Ubuntu 14 – amd64

```
# echo "deb
https://download.endpointprotector.com/repo/deb/Ubuntu/14.04/amd64/ /"
> /etc/apt/sources.list.d/epprepo.list

# wget -q -O -
https://download.endpointprotector.com/repo/deb/Ubuntu/14.04/amd64/KEY.gpg | apt-key add -

# apt update

# apt-get install epp-client
```

Linux Mint – amd64

```
# echo "deb
https://download.endpointprotector.com/repo/deb/LinuxMint/18.x/amd64/ /"
> /etc/apt/sources.list.d/epprepo.list

# wget -q -O -
https://download.endpointprotector.com/repo/deb/LinuxMint/18.x/amd64/KEY.gpg | apt-key add -

# apt update

# apt-get install epp-client
```

16.1.3. RedHat 기반 배포

방법은 비슷하지만 각 배포 버전마다 차이가 있습니다.

CentOS 7.x

```
# sudo sh -c 'echo -e "[epp-client]\nname=Endpoint Protector\nClient\nbaseurl=https://download.endpointprotector.com/repo/rpm/CentOS/7.x/\nenabled=1\ntype=rpm-md\nngpgcheck=1\nngpgkey=https://download.endpointprotector.com/repo/rpm/CentOS/7.x/repo/repodata/repo-md.xml.key" > /etc/yum.repos.d/eppclient.repo'

# rpm --import
https://download.endpointprotector.com/repo/rpm/CentOS/7.x/repo/repodata/repo-md.xml.key
```

Fedora 29

```
# sudo sh -c 'echo -e "[epp-client]\nname=Endpoint Protector\nClient\nbaseurl=https://download.endpointprotector.com/repo/rpm/Fedora/29/\nenabled=1\ntype=rpm-md\nngpgcheck=1\nngpgkey=https://download.endpointprotector.com/repo/rpm/Fedora/29/repo/repodata/repo-md.xml.key" > /etc/yum.repos.d/eppclient.repo'

# rpm --import
https://download.endpointprotector.com/repo/rpm/Fedora/29/repo/repodata/repo-md.xml.key
```

OpenSUSE 42.3

참고

Endpoint Protector 퍼블릭 키는 SUSE와 openSUSE 버전에서 반드시 필요합니다.

```
# sudo sh -c 'echo -e "[epp-client]\nname=Endpoint Protector\nClient\nbaseurl=https://download.endpointprotector.com/repo/rpm/openSUSE/42.3/\nenabled=1\ntype=rpm-\nmd\nngpgcheck=1\nngpgkey=https://download.endpointprotector.com/repo/rpm/openSUSE/43.2/repo/repodata/repomd.xml.key" >\n/etc/yum.repos.d/eppclient.repo'
```

```
# rpm --import\nhttps://download.endpointprotector.com/repo/rpm/openSUSE/42.3/keys/repo\nmd.xml.key
```

```
# rpm --import\nhttps://download.endpointprotector.com/repo/rpm/openSUSE/42.3/keys/coso\nsys_gpg2_public.key
```

참고

모든 RedHat 기반 배포 버전은 위의 커맨드 실행 후 추가적인 단계가 필요합니다.

프로세스 상호작용이 완료된 것이 아니고 Endpoint Protector 서버 IP를 이 단계에서 설정할 수 없습니다.

아래와 같이 두 가지 방법이 있고 각 버전마다 차이가 있습니다.

Method 1.

Step 1: Define the Endpoint Protector Server IP

```
#EPPCLIENT_WS_SERVER=[the desired IP]
#export EPPCLIENT_WS_SERVER
```

Step 2: Install the Endpoint Protector Client

- for SUSE and openSUSE: #zypper install epp-client
- for CentOS, RedHat, Fedora: #yum install epp-client

Method 2.

Step 1: Install the Endpoint Protector Client

- for SUSE and openSUSE: #zypper install epp-client
- for CentOS, RedHat, Fedora: #yum install epp-client

Step 2: Run bash file to define the Endpoint Protector Server IP

```
#bash '/opt/cososys/share/apps/epp-client/scripts/set_epp_client_server.sh'
```

정보

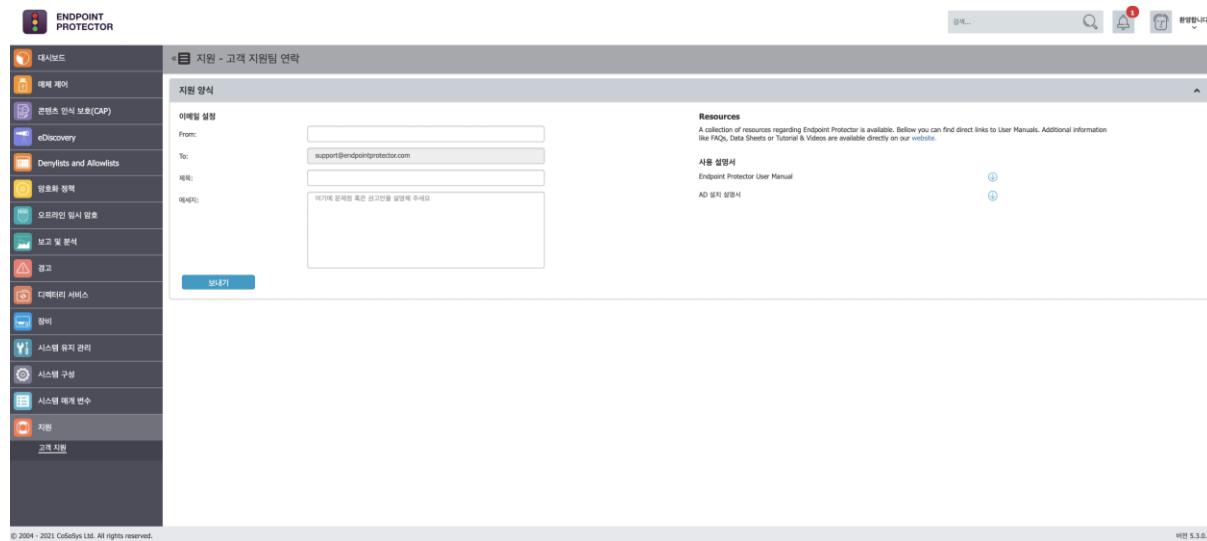
모든 클라이언트 레포지토리는 다음의 경로에서 찾을 수 있습니다.

<https://download.endpointprotector.com/repo/>

17. 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.



저희 지원 팀 직원이 가능한 한 빨리 연락을 드리도록 하겠습니다.

제품 이용 중에 문제가 없어도 원하는 기능이 있으시거나, 일반적인 의견을 남기는 거라면 언제든 환영입니다. 휴대용 장치를 안전하고 편리하게 사용하는 것과 관련된 의견이라면 어떤 것이라도 저희에게는 소중한 의견입니다.

18. 중요 공지 사항 / 책임의 한계

Endpoint Protector 어플라이언스는 liveupdate.endpointprotector.com과 clould.endpointprotector.com을 제외하고 외부 네트워크와 통신하지 않습니다.

Endpoint Protector는 악성 소프트웨어를 포함하고 있지않고 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.

© 2004 – 2021 CoSoSys Ltd. Endpoint Protector Basic, Endpoint Protector, My Endpoint Protector 는 CoSoSys Ltd.의 상표입니다. All rights reserved. Windows 는 Microsoft Corporation 의 등록 상표입니다. Macintosh, macOS 는 Apple Corporation 의 상표입니다. 다른 모든 이름과 상표는 해당 소유자의 재산입니다.