ESET Endpoint Security

사용자 설명서

이 문서의 온라인 버전을 표시하려면 여기를 클릭

Digital Security
Progress. Protected.

ESET Endpoint Security은(는) ESET, spol. s r.o.에서 개발했습니다.

자세한 내용은 https://www.eset.com을 참조하십시오.

기술 지원: https://support.eset.com

REV. 2024년 4월 12일

ESET Endpoint Security

ESET Endpoint Security에는 완전히 통합된 컴퓨터 보안에 대한 새로운 접근 방식이 도입되었습니다. 사용자 지정 방화벽 및 이메일 클라이언트 안티스팸 모듈과 결합된 최신 버전의 ESET LiveGrid® 탐지 엔진이 빠르고 정밀하게 컴퓨터를 보호해 줍니다. 그 결과, 컴퓨터를 위험에 빠뜨리는 공격 및 악성 소프트웨어에 대해 끊임없이 경고하는 지능형 시스템이 탄생했습니다.

ESET Endpoint Security는 시스템 공간을 최소화하면서 보호 기능을 극대화하기 위한 장기간에 걸친 노력의 산물입니다. 인공 지능에 기반을 둔 이 고급 기술은 시스템 성능을 저해하거나 컴퓨터를 방해하지 않고 바이러스, 스파이웨어, 트로이목마, 웜, 애드웨어, 루트킷 및 기타 인터넷 기반 공격에 의한 침입을 사전에 제거할 수 있습니다.

ESET Endpoint Security 주로 중소기업 환경의 워크스테이션에서 사용하도록 고안되었습니다.

설치 섹션에서는 다운로드, 설치, 활성화 등의 여러 장과 하위 장으로 구분된 도움말 항목이 있어서 사용자가 필요한 내용을 쉽게 찾을 수 있습니다.

대기업 환경에서 ESET PROTECT와 함께 ESET Endpoint Security을(를) 사용하면 여러 클라이언트 워크스테이션을 쉽게 관리하고 정책과 규칙을 적용하며 검색을 모니터링할 수 있을 뿐만 아니라, 네트워크로 연결된 모든 컴퓨터에서 클라이언트를 원격으로 구성할 수 있습니다.

일반적인 질문 장에서는 몇 가지 자주 묻는 질문과 발생하는 문제에 대해 다룹니다.

기능 및 장점

새롭게 설계된 사용자 인터페이스	이 버전의 사용자 인터페이스가 유용성 테스트 결과를 바탕으로 완전히 새롭게 설계되고 간편해졌습니다. 모든 GUI 표현 및 알림이 검토되었으며 이제 인터페이스에서 히브리어, 아랍어 등과 같은 오른쪽에서 왼쪽으로 쓰는 언어도 지원됩니다. 이제 온라인 도움말이 ESET Endpoint Security로 통합되어 동적으로 업데이트된 지원 콘텐츠가 제공됩니다.
어두운 모드	화면을 어두운 테마로 빠르게 전환하는 데 도움이 되는 확장 프로그램입니다. 사용자 인터페이스 요소에서 원하는 색 구성표를 선택할 수 있습니다.
안티바이러스, 안티스파이웨어	잘 알려지거나 알려지지 않은 바이러스, 웜, 트로이 목마 및 루트킷을 사전에 검출하고 치료합니다. 고급 인공지능으로 이전에 발견된 적이 없는 맬웨어까지도 플래깅하여 해를 끼치기 전에 알 수 없는 위협으로부터 시스템을 보호하고 위협을 무력화합니다. 웹 브라우저 보호 및 안티피싱은 웹 브라우저와 원격 서버(SSL 포함) 간의 통신을 모니터링하는 방식으로 작동합니다. 이메일 클라이언트 보호는 POP3(S) 및 IMAP(S) 프로토콜을 통해 받은 이메일 통신을 제어합니다.
정기적 업데이트	검색 엔진(이전 명칭: 바이러스 시그니처 DB) 및 프로그램 모듈을 정기적으로 업데이트하는 것이 컴퓨터에서 최고 수준의 보안을 유지하는 가장 좋은 방법입니다.
ESET LiveGrid® (클라우드 기반 평판)	ESET Endpoint Security에서 직접 실행 중인 프로세스 및 파일의 평판을 확인할 수 있습니다.
원격 관리	ESET PROTECT에서 워크스테이션, 서버 및 중앙 위치 한 곳에서 네트워크로 연결된 환경의 모든 장치에 있는 ESET 제품을 관리할 수 있습니다. ESET PROTECT Web Console(ESET PROTECT Web Console)을 사용하여 ESET 솔루션을 배포하고 작업을 관리하며 보안 정책을 적용하고 시스템 상태를 모니터링할 뿐만 아니라, 원격 컴퓨터의 문제나 위협에 신속하게 대응할 수 있습니다.

네트워크 공격 보호	네트워크 트래픽의 내용을 분석하고 네트워크 공격으로부터 보호합니다. 유해한 것으로 간주되는 모든 트래픽이 차단됩니다.
웹 컨트롤(ESET Endpoint Security만 해당)	웹 컨트롤을 사용하면 잠재적으로 부적절한 자료가 포함되었을 수 있는 웹 페이지를 차단할 수 있습니다. 또한 고용주나 시스템 관리자는 27개가 넘는 미리 정의된 웹 사이트 범주 및 140개 이상의 하위 범주에 대한 접근을 금지할 수 있습니다.

새로운 기능

ESET Endpoint Security 버전 10.1의 새로운 기능

새 방화벽 규칙 편집기

방화벽 규칙 편집기가 더 많은 구성 옵션을 사용하여 방화벽 규칙을 더 쉽게 정의할 수 있도록 새롭게 설계되었습니다.

취약성 및 패치 관리

워크스테이션을 정기적으로 검사하여 보안 위험에 취약한 설치된 소프트웨어를 탐지하는 ESET PROTECT Cloud의 기능입니다. 패치 관리는 다운로드를 시작하기 전에 사용 가능한 공간이 일치하는지 확인하고(기본값 및 최소값은 2GB) 자동화된 소프트웨어 업데이트를 통해 이러한 위험을 수정하여 장치를 보다 안전하게 유지합니다.

수명 종료 제품 상태

이 버전의 ESET Endpoint Security에는 다양한 수명 종료 제품 상태가 표시될 수 있습니다. 알림에서 수명 종료 상태를 설정할 수 있습니다.

다양한 버그 수정 및 성능 개선 사항

시스템 요구 사항

ESET Endpoint Security의 원활한 작동을 위해서는 시스템이 다음 하드웨어 및 소프트웨어 요구 사항(기본 제품 설정)을 충족해야 합니다.

지원되는 프로세서

Intel 또는 AMD 데이터 처리자, SSE2 명령 집합이 포함된 32비트(x86) 또는 64비트(x64), 1GHz 이상
ARM64 기반 데이터 처리자, 1GHz 이상

운영 체제

Microsoft® Windows® 11

Microsoft® Windows® 10

> 지원되는 Microsoft® Windows® 10 그리고 Microsoft® Windows® 11 버전의 자세한 목록은 Windows 운영 체제 지원 정책을 참조하십시오.

운영 체제를 항상 최신 상태로 유지하도록 하십시오.

2023년 7월 이후에 릴리스된 ESET 제품을 설치하거나 업그레이드하려면 모든 Windows 운영 체제에 Azure Code Signing 지원 기능을 설치해야 합니다. 추가 정보.

ESET Endpoint Security 기능 요구 사항

아래 표에서 ESET Endpoint Security의 특정 기능에 대한 시스템 요구 사항을 참조하십시오:

기능	요구 사항
Intel® Threat Detection Technology	지원되는 프로세서를 참조하십시오.
안전한 브라우저	지원되는 웹 브라우저를 참조하십시오.
특수 클리너	비 ARM64 기반 프로세서
Exploit 차단	비 ARM64 기반 프로세서
심층 행위 검사	비 ARM64 기반 프로세서

ESET PROTECT에서 생성된 ESET Endpoint Security 설치 관리자는 가상 데스크톱용 Windows 10 Enterprise 및 Windows 10 다중 세션 모드를 지원합니다.

기타

- 컴퓨터에 설치된 운영 체제 및 기타 소프트웨어의 시스템 요구 사항 충족
- 사용 가능한 시스템 메모리 0.3GB(참고 1 참조)
- 사용 가능한 디스크 공간 1GB(참고 2 참조)
- 최소 디스플레이 해상도 1024x768
- 제품 업데이트 소스(참고 3 참조)에 대한 인터넷 연결 또는 로컬 영역 네트워크 연결
- 단일 장치에서 동시에 실행되는 두 개의 안티바이러스 프로그램은 시스템 속도를 저하시켜 작동을 불가능하게 하는 등 불가피한 시스템 리소스 충돌을 일으킵니다.

이러한 요구 사항을 충족하지 않는 시스템에 제품을 설치하고 실행할 수는 있지만, ESET에서는 사전에 성능 요구 사항에 따라 유용성을 테스트하는 것을 권장합니다.

(1):컴퓨터가 심각하게 감염되어 메모리가 달리 사용되지 않는 경우나 URL 허용 목록과 같은 대규모 데이터 목록을 제품으로 가져오는 경우에는 제품이 더 많은 메모리를 사용할 수도 있습니다.
(2) 설치 관리자 다운로드, 제품 설치, 프로그램 데이터에 설치 패키지 사본 보관 및 롤백 기능 지원을 위한 제품 업데이트 백업을 저장할 디스크 공간이 필요합니다. 제품은 다양한 설정(예: 더 많은 제품 업데이트 백업 버전, 메모리 덤프 또는 대용량 로그 레코드가 저장되는 경우)에 따라, 또는 감염된 컴퓨터의 경우 검역소 기능으로 인해 더 많은 디스크 공간을 사용할 수도 있습니다. 운영 체제 및 ESET 제품 업데이트를 지원하기 위해 사용 가능한 디스크 공간을 충분하게 확보하는 것이 좋습니다.
(3) 권장되지는 않지만 이동식 미디어에서 제품을 수동으로 업데이트할 수도 있습니다.

지원되는 언어

ESET Endpoint Security은(는) 다음 언어로 설치 및 다운로드할 수 있습니다.

언어	언어 코드	LCID
영어(미국)	en-US	1033

언어	언어 코드	LCID
아랍어(이집트)	ar-EG	3073
불가리아어	bg-BG	1026
중국어 간체	zh-CN	2052
중국어 번체	zh-TW	1028
크로아티아어	hr-HR	1050
체코어	cs-CZ	1029
에스토니아어	et-EE	1061
핀란드어	fi-FI	1035
프랑스어(프랑스)	fr-FR	1036
프랑스어(캐나다)	fr-CA	3084
독일어(독일)	de-DE	1031
그리스어	el-GR	1032
*히브리어	he-IL	1037
헝가리어	hu-HU	1038
*인도네시아어	id-ID	1057
이탈리아어	it-IT	1040
일본어	ja-JP	1041
카자흐어	kk-KZ	1087
한국어	ko-KR	1042
*라트비아어	lv-LV	1062
리투아니아어	lt-LT	1063
Nederlands	nl-NL	1043
노르웨이어	nb-NO	1044
폴란드어	pl-PL	1045
포르투갈어(브라질)	pt-BR	1046
루마니아어	ro-RO	1048
러시아어	ru-RU	1049
스페인어(칠레)	es-CL	13322
스페인어(스페인)	es-ES	3082
스웨덴어(스웨덴)	sv-SE	1053
슬로바키아어	sk-SK	1051
슬로베니아어	sl-SI	1060
태국어	th-TH	1054
터키어	tr-TR	1055
우크라이나어(우크라이나)	uk-UA	1058
*베트남어	vi-VN	1066

* ESET Endpoint Security은(는) 이 언어로 사용할 수 있지만, 온라인 사용자 설명서는 제공되지 않습니다(영어 버전으로 리디렉션됨).

이 온라인 사용자 설명서의 언어를 변경하려면 오른쪽 상단 모서리에 있는 언어 선택 상자를 사용합니다.

변경 로그

방지

컴퓨터를 사용할 때, 특히 인터넷을 검색할 때는 어떤 안티바이러스 시스템도 탐지 및 원격 공격의 위험을 완벽하게 제거할 수 없다는 점에 유의해야 합니다. 보호 기능을 극대화하면서 최대한 편리하게 사용하려면 안티바이러스 솔루션을 제대로 사용하고 다음과 같은 몇 가지 유용한 규칙을 준수해야 합니다.

정기적으로 업데이트

ESET LiveGrid®의 통계에 따르면 기존 보안 조치를 무시하고 다른 사용자에게 피해를 주면서 침입 작성자에게 이익을 가져다주는 것을 목적으로 하는 수천 개의 새로운 침입이 매일 생성된다고 합니다. ESET 바이러스 연구소의 전문가는 매일 이러한 위협을 분석하고 업데이트를 준비하여 발표함으로써 사용자를 위한 보안 수준을 지속적으로 향상시키고 있습니다. 이러한 업데이트의 효과를 극대화하려면 시스템에서 업데이트를 제대로 구성해야 합니다. 업데이트를 구성하는 방법에 대한 자세한 내용은 업데이트 설정 장을 참조하십시오.

보안 패치 다운로드

악성 소프트웨어 작성자는 대개 악성 코드를 더욱 효과적으로 유포하기 위해 다양한 시스템 취약성을 악용합니다. 이 때문에 소프트웨어 회사에서 자사 애플리케이션에 취약성이 나타나는지 면밀히 감시하고 잠재 위협을 제거하는 보안 업데이트를 정기적으로 공개합니다. 이러한 보안 업데이트가 공개되면 다운로드해야 합니다. Microsoft Windows 및 웹 브라우저(예: Microsoft Edge)는 보안 업데이트가 정기적으로 출시되는 두 가지 예입니다.

중요한 데이터 백업

일반적으로 악성코드 작성자는 사용자의 요구 사항에 신경 쓰지 않습니다. 따라서 종종 악성 프로그램 활동으로 인해 운영 체제가 전체적으로 작동하지 않거나 중요한 데이터가 손실됩니다. 중요한 데이터는 DVD 또는 외장 하드 드라이브와 같은 외부 소스에 정기적으로 백업해야 합니다. 이러한 예방 조치를 통해 시스템 오류 발생 시 데이터를 한층 쉽고 빠르게 복구할 수 있습니다.

컴퓨터에서 정기적으로 바이러스 검사

알려지거나 알려지지 않은 바이러스, 웜, 트로이목마 및 루트킷의 탐지는 실시간 파일 시스템 보호 모듈을 통해 처리됩니다. 즉, 파일을 접근하거나 열 때마다 맬웨어 활동이 있는지 검사됩니다. 맬웨어 시그니처는 다양하고 검색 엔진도 자체적으로 매일 업데이트되므로, 한 달에 1번 이상 전체 컴퓨터 검사를 실행하는 것이 좋습니다.

기본 보안 규칙 준수

무엇보다도 가장 유용하고 효과적인 규칙은 항상 조심하는 것입니다. 요즘에는 실행하고 배포하기 위해 사용자 개입을 요구하는 침입이 많이 있습니다. 따라서 새 파일을 열 때 주의를 기울이면 사용자가 부주의하

여 컴퓨터에 침입이 발생했을 때 치료하느라 소요되는 많은 시간과 노력이 절약됩니다. 다음은 유용한 몇 가지 지침입니다.

- 팝업 및 깜박이는 광고가 많은 의심스러운 웹 사이트를 방문하지 마십시오.
- 프리웨어 프로그램, 코덱 팩 등을 설치할 때 주의하십시오. 안전한 프로그램만 사용하고 안전한 인터넷 웹 사이트만 방문합니다.
- 이메일 첨부 파일을 열 때 주의하십시오. 특히 대량으로 발송된 메시지와 알 수 없는 사람이 보낸 메시지의 경우 더욱 조심합니다.
- 컴퓨터로 진행하는 일상적인 작업에 관리자 계정을 사용하지 마십시오.

수명 종료 상태

ESET Endpoint Security은(는) 기본 프로그램 창의 여러 위치에 자동 알림 또는 경고를 표시하여 예정된 수명 종료 정보를 알릴 수 있습니다.

다음에 대한 자세한 내용 읽기:
- 지원 종료 정책(비즈니스 제품)
- 제품 업데이트
- 보안 및 안정성 핫픽스

ESET Endpoint Security 변경 사항에 대한 자세한 내용은 다음의 ESET 지식베이스 문서를 참조하십시오.

아래 표는 범주에 따른 제품 상태 및 알림의 몇 가지 예를 관련 동작과 함께 보여 줍니다.

범주	알림 또는 경고 창	업데이트 페이지	도움말 및 지원 페이지
새로운 기능 또는 서비스 업데이트 사용 가능	ℹ 새 버전의 출시 ESET Endpoint Security에 요구되는 중요한 서비스 수정 사항이 포함된 업데이트를 사용할 수 있습니다. 최신 보호 기능을 사용하려면 지금 업데이트하십시오. **동작**: 자세히 알아보기	ℹ 새 버전의 ESET Endpoint Security 사용 가능. 새 버전의 ESET Endpoint Security 사용 가능. **동작**: 지금 업데이트/자동 업데이트 활성화	ℹ 새 버전의 ESET Endpoint Security 사용 가능. 새로운 기능과 개선 사항이 포함된 최신 버전을 사용하려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy
	ℹ 서비스 업데이트를 사용할 수 있음 새 버전의 ESET Endpoint Security 사용 가능. 새로운 기능과 개선 사항이 포함된 최신 버전을 사용하려면 지금 업데이트하십시오. **동작**: 자세히 알아보기	ℹ ESET Endpoint Security에 대한 서비스 업데이트를 사용할 수 있습니다. 설치된 버전 번호 지원 기간: mm/dd/yyyy **동작**: 자세히 알아보기	ℹ ESET Endpoint Security에 요구되는 중요한 서비스 수정 사항이 포함된 업데이트를 사용할 수 있습니다. 최신 보호 기능을 사용하려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy
	⚠ 장치를 다시 시작하는 것이 좋음 ESET Endpoint Security에 요구되는 중요한 서비스 수정 사항이 포함된 업데이트를 사용할 수 있습니다. 최신 보호 기능을 사용하려면 지금 업데이트하십시오. **동작**: 자세히 알아보기		지원 기간: mm/dd/yyyy
	⚠ 필수 서비스 업데이트를 사용할 수 있음 ESET Endpoint Security에 요구되는 필수 서비스 수정 사항이 포함된 업데이트를 사용할 수 있습니다. 최신 보호 기능을 사용하려면 지금 업데이트하십시오. **동작**: 자세히 알아보기	⚠ ESET Endpoint Security에 대한 필수 서비스 업데이트를 사용할 수 있습니다. 설치된 버전 번호 지원 기간: mm/dd/yyyy **동작**: 자세히 알아보기	⚠ ESET Endpoint Security에 요구되는 필수 서비스 수정 사항이 포함된 업데이트를 사용할 수 있습니다. 최신 보호 기능을 사용하려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy
	⚠ 장치를 다시 시작해야 함 버전 번호에 대한 업데이트가 다운로드되었으며, 여기에는 ESET Endpoint Security에 요구되는 중요한 서비스 및 안정성 수정 사항이 포함되어 있습니다. 최신 보호 기능을 사용하려면 지금 업데이트하십시오. **동작**: 자세히 알아보기		지원 기간: mm/dd/yyyy

범주	알림 또는 경고 창	업데이트 페이지	도움말 및 지원 페이지
애플리케이션 지원 만료 예정	설치된 애플리케이션 버전에 대한 지원이 mm/dd/yyyy에 종료되고, 곧 장치가 보호되지 않습니다. 계속 보호받으려면 지금 업데이트하십시오. **동작**: 지금 업데이트	설치된 버전 번호/지원 기간: mm/dd/yyyy **동작**: 지금 업데이트/자동 업데이트 활성화	설치된 ESET Endpoint Security 버전에 대한 지원이 곧 종료되어 컴퓨터가 보호되지 않습니다. 계속 보호받으려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy
	설치된 애플리케이션 버전에 대한 ESET 연장 지원이 mm/dd/yyyy에 종료되고, 곧 장치가 보호되지 않습니다. 계속 보호받으려면 지금 업데이트하십시오. **동작**: 지금 업데이트	설치된 버전 번호/지원 기간: mm/dd/yyyy **동작**: 지금 업데이트/자동 업데이트 활성화	설치된 ESET Endpoint Security 버전에 대한 ESET 연장 지원이 곧 종료되어 장치가 보호되지 않습니다. 계속 보호받으려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy
	오래된 운영 체제가 설치되어 있으며, 설치된 애플리케이션 버전에 대한 지원이 mm/dd/yyyy에 종료됩니다. 최신 애플리케이션 업데이트를 받고 계속 보호받으려면 운영 체제를 업그레이드하십시오. **동작**: 자세히 알아보기	설치된 버전 번호 지원 기간: mm/dd/yyyy **동작**: 자세히 알아보기	설치된 ESET Endpoint Security 버전에 대한 지원이 곧 종료되어 컴퓨터가 보호되지 않습니다. 계속 보호받으려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy
	설치된 애플리케이션 버전에 대한 ESET 연장 지원이 곧 종료됨 오래된 운영 체제가 설치되어 있으며, 설치된 애플리케이션 버전에 대한 지원이 mm/dd/yyyy에 종료됩니다. 최신 애플리케이션 업데이트를 받고 계속 보호받으려면 운영 체제를 업그레이드하십시오. **동작**: 자세히 알아보기	설치된 ESET Endpoint Security 버전에 대한 ESET 연장 지원이 곧 종료됩니다. 설치된 버전 번호 지원 기간: mm/dd/yyyy **동작**: 자세히 알아보기	설치된 ESET Endpoint Security 버전에 대한 ESET 연장 지원이 곧 종료되어 장치가 보호되지 않습니다. 계속 보호받으려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy

범주	알림 또는 경고 창	업데이트 페이지	도움말 및 지원 페이지
애플리케이션 버전이 더 이상 지원되지 않음	⚠ 설치된 애플리케이션 버전이 더 이상 지원되지 않음 설치된 애플리케이션 버전에 대한 지원이 종료되었으며, 장치가 보호되지 않을 수 있습니다. 보호를 받으려면 지금 업데이트하십시오. **동작**: 지금 업데이트	⚠ 설치된 ESET Endpoint Security 버전은 더 이상 지원되지 않습니다. 설치된 버전 번호/지원 기간: mm/dd/yyyy **동작**: 지금 업데이트/자동 업데이트 활성화	⚠ 지원 기간: mm/dd/yyyy
	⚠ 설치된 애플리케이션 버전이 더 이상 지원되지 않음 오래된 운영 체제가 설치되어 있으며, 설치된 애플리케이션 버전에 대한 지원이 종료되었습니다. 컴퓨터가 보호되지 않습니다. 최신 애플리케이션 업데이트를 받고 보호를 받으려면 운영 체제를 업그레이드하십시오. **동작**: 자세히 알아보기	⚠ 설치된 ESET Endpoint Security 버전은 더 이상 지원되지 않습니다. 설치된 버전 번호 지원 기간: mm/dd/yyyy **동작**: 자세히 알아보기	⚠ 설치된 ESET Endpoint Security 버전에 대한 지원이 종료되어 컴퓨터가 보호되지 않습니다. 보호를 받으려면 지금 업데이트하십시오. 지원 기간: mm/dd/yyyy
운영 체제 업데이트 필요	오래된 운영 체제가 설치되어 있음 오래된 운영 체제가 설치되어 있음. 최신 애플리케이션 업데이트를 받고 계속 보호받으려면 운영 체제를 업그레이드하십시오. **동작**: 자세히 알아보기	✔ ESET Endpoint Security 설치된 버전 번호	지원 기간: mm/dd/yyyy

도움말 페이지

ESET Endpoint Security 사용자 설명서입니다. 여기에 제공된 정보는 제품을 소개하고 컴퓨터를 보다 안전하게 만드는 데 도움이 됩니다.

시작

ESET Endpoint Security 사용을 시작하기 전에 ESET PROTECT를 사용하여 제품을 원격으로 관리할 수 있습니다. 또한 컴퓨터 사용 중 발생할 수 있는 다양한 검색 유형 및 원격 공격을 숙지하는 것이 좋습니다.

이 버전의 ESET Endpoint Security에 도입된 기능에 대한 자세한 내용은 새 기능을 참조하십시오. 또한 ESET Endpoint Security의 기본 설정을 정의하고 사용자 지정하는 데 도움이 되는 설명서도 준비되어 있습니다.

ESET Endpoint Security 도움말 페이지를 사용하는 방법

도움말 항목은 여러 개의 장과 하위 장으로 구분되어 있어 사용자가 필요한 내용을 쉽게 찾을 수 있습니다. 즉, 도움말 페이지 구조를 검색하여 관련 정보를 찾을 수 있습니다.

프로그램에서 자세히 알아보고 싶은 창이 있는 경우에는 **F1** 키를 누르십시오. 그러면 현재 표시된 창에 대한 도움말 페이지가 표시됩니다.

키워드를 사용하거나 단어 또는 구를 입력하여 도움말 페이지를 검색할 수 있습니다. 이러한 두 가지 방법의 차이는 키워드는 텍스트에 해당 특정 키워드가 포함되어 있지 않은 도움말 페이지와도 논리적으로 관련될 수 있다는 점입니다. 단어 및 구를 통한 검색은 모든 페이지의 내용을 검색하여 검색한 단어 또는 구가 포함된 페이지만 표시합니다.

일관성을 확보하고 혼동을 방지하기 위해 이 설명서에서 사용된 용어는 ESET Endpoint Security 파라미터 이름을 기준으로 합니다. 또한 특정 관심 분야의 항목이나 중요한 항목을 강조하기 위한 일련의 균일한 기호를 사용합니다.

참고는 잠깐 살펴보면 되는 내용입니다. 참고를 무시해도 되지만, 참고는 특정 기능이나 관련 항목의 링크와 같은 중요한 정보를 제공할 수 있습니다.

이 항목은 건너뛰지 말고 주의를 기울이는 것이 좋습니다. 일반적으로 중요 항목은 필수적이지는 않지만 상당히 중요한 정보를 제공합니다.

이는 특별히 주의해야 하는 정보입니다. 경고는 사용자가 유해한 실수를 저지르지 않도록 하기 위해 특별히 배치됩니다. 경고 괄호가 사용된 텍스트는 매우 중요한 시스템 설정이나 위험한 항목을 의미하므로 읽고 이해하십시오.

특정 기능을 사용하는 방법을 이해하는 데 도움이 되는 사용 사례나 실례입니다.

규칙	의미
굵은 글꼴	상자 및 옵션 버튼과 같은 인터페이스 항목의 이름입니다.
기울임꼴	사용자가 제공하는 정보의 자리 표시자입니다. 예를 들어 파일 이름 또는 경로는 사용자가 실제 경로나 파일 이름을 입력한다는 의미입니다.
Courier New	코드 샘플 또는 명령
하이퍼링크	교차 참조된 항목이나 외부 웹 위치에 쉽고 빠르게 접근할 수 있습니다. 하이퍼링크는 파란색으로 강조 표시되고 밑줄이 그어져 있을 수 있습니다.
%ProgramFiles%	Windows에 설치된 프로그램이 저장되어 있는 Windows 시스템 디렉터리입니다.

온라인 도움말은 도움말 콘텐츠의 기본 소스입니다. 인터넷에 연결되어 있는 경우에는 최신 버전의 온라인 도움말이 자동으로 표시됩니다.

원격으로 관리되는 엔드포인트에 대한 설명서

ESET Endpoint Security뿐만 아니라 ESET 비즈니스 제품은 클라이언트 워크스테이션과 서버, 중앙 위치 한 곳으로부터 네트워크로 연결된 환경의 모바일 장치에서 원격으로 관리할 수 있습니다. 10개가 넘는 클라이언트 워크스테이션을 관리하는 시스템 관리자는 ESET 원격 관리 도구 중 하나를 배포하여 ESET 솔루션을 배포하고, 작업을 관리하며, 보안 정책을 적용하고, 시스템 상태를 모니터링할 뿐만 아니라 중앙 위치 한 곳에서 원격 컴퓨터의 문제나 위협에 신속하게 대응할 수 있습니다.

ESET 원격 관리 도구

ESET Endpoint Security은(는) ESET PROTECT 또는 ESET PROTECT Cloud 중 하나를 통해 원격으로 관리할 수 있습니다.

- ESET PROTECT 소개

- ESET PROTECT Cloud 소개
- ESET HUB - ESET PROTECT 통합 보안 플랫폼의 중앙 게이트웨이입니다. 모든 ESET 플랫폼 모듈에 대한 중앙 집중식 ID, 구독 및 사용자 관리를 제공합니다. 제품을 활성화하기 위한 지침은 ESET PROTECT 라이선스 관리를 참조하십시오. ESET Business Account 및 ESET MSP Administrator가 ESET HUB로 완전히 대체될 예정입니다.
- ESET Business Account - ESET 비즈니스 제품용 라이선스 관리 포털입니다. 제품 활성화에 대한 지침은 ESET PROTECT 라이선스 관리를 참조하고, ESET Business Account 사용에 대한 자세한 내용은 ESET Business Account 온라인 도움말을 참조하십시오. 라이선스 키로 변환하려는 ESET 발급 사용자 이름 및 패스워드가 이미 있는 경우 레거시 라이선스 자격 증명 변환 섹션을 참조하십시오.

추가 보안 제품

- ESET Inspect - 사고 검색, 사고 관리 및 응답, 데이터 수집, 손상 검색, 비정상 검색, 동작 검색, 정책 위반 표시기 등의 기능을 포함하는 포괄적인 Endpoint Detection and Response 시스템입니다.
- ESET Endpoint Encryption - 유휴 및 전송 중 데이터를 보호하도록 설계된 포괄적인 보안 애플리케이션입니다. ESET Endpoint Encryption을 사용하여 파일, 폴더 및 이메일을 암호화하거나 암호화된 가상 디스크를 생성하고, 압축파일을 압축하고, 안전한 파일 제거를 위한 바탕 화면 보안 파일 제거 도구를 포함할 수 있습니다.

타사 원격 관리 도구

- 원격 모니터링 및 관리 (RMM)

모범 사례

- ESET Endpoint Security이(가) 있는 모든 엔드포인트를 ESET PROTECT에 연결
- 연결된 클라이언트 컴퓨터에서 고급 설정을 보호하여 무단 수정 방지
- 권장 정책을 적용하여 사용 가능한 보안 기능 적용
- 사용자 인터페이스를 최소화하여 ESET Endpoint Security(과)와의 사용자 상호 작용 제한 또는 감소

방법 설명서

- 재정의 모드 사용 방법
- GPO 또는 SCCM을 사용해 ESET Endpoint Security을(를) 배포하는 방법

ESET PROTECT 소개

ESET PROTECT에서 워크스테이션, 서버 및 중앙 위치 한 곳에서 네트워크로 연결된 환경의 모든 장치에 있는 ESET 제품을 관리할 수 있습니다.

ESET PROTECT 웹 콘솔을 사용하여 ESET 솔루션을 배포하고, 작업을 관리하며, 보안 정책을 적용하며, 시스템 상태를 모니터링할 뿐만 아니라 원격 컴퓨터의 문제 또는 위협에 신속하게 대응할 수 있습니다. ESET PROTECT 아키텍처 및 인프라 요소 개요, ESET PROTECT 웹 콘솔 시작하기 및 지원되는 데스크톱 프로비저닝 환경도 참조하십시오.

ESET PROTECT는 다음 구성 요소로 구성됩니다.

- ESET PROTECT 서버 - 이 서버는 에이전트와의 통신을 처리하며 DB에서 애플리케이션 데이터를 수집 및 저장합니다. ESET PROTECT 서버는 Windows 및 Linux 서버에 설치할 수 있으며 가상 어플라이언스로도 제공됩니다.
- ESET PROTECT 웹 콘솔 - 웹 콘솔은 사용자 환경에서 클라이언트 컴퓨터를 관리할 수 있도록 해 주는 기본 인터페이스입니다. 이 인터페이스는 네트워크상의 클라이언트 상태 개요를 표시하고, 이를 통해 관리되지 않는 컴퓨터에 ESET 솔루션을 원격으로 배포할 수 있습니다. ESET PROTECT 서버를 설치한 후에는 웹 브라우저를 사용하여 웹 콘솔에 접근할 수 있습니다. 인터넷에서 웹 서버에 접근할 수 있도록 선택하면 인터넷에 연결된 모든 장소 또는 장치에서 ESET PROTECT를 사용할 수 있습니다.
- ESET Management 에이전트 - ESET PROTECT 서버와 클라이언트 컴퓨터 간의 통신을 원활하게 해 줍니다. 에이전트는 컴퓨터와 ESET PROTECT 서버 간의 통신을 설정하려는 클라이언트 컴퓨터에 설치해야 합니다. 에이전트가 클라이언트 컴퓨터에 설치되고 여러 보안 시나리오가 저장될 수 있으므로 ESET Management 에이전트를 사용하면 새 감지에 대한 반응 시간이 대폭 줄어듭니다. ESET PROTECT 웹 콘솔을 사용하여 Active Directory나 ESET RD Sensor에서 식별된 관리되지 않는 컴퓨터에 ESET Management 에이전트를 배포할 수 있습니다. 또한 필요한 경우 클라이언트 컴퓨터에 ESET Management 에이전트를 수동으로 설치할 수 있습니다.
- ESET Rogue Detection Sensor - 는 네트워크에 있는 관리되지 않는 컴퓨터를 검색하며 관련 정보를 ESET PROTECT 서버에 전송합니다. 이를 통해 수동으로 검색하고 추가할 필요 없이 ESET PROTECT에서 새 클라이언트 컴퓨터를 관리할 수 있습니다. Rogue Detection Sensor는 검색된 컴퓨터를 저장하여 같은 정보를 두 번 전송하지 않습니다.
- ESET Bridge - ESET PROTECT와 함께 사용하여 다음을 수행할 수 있는 서비스입니다.
    - 클라이언트 컴퓨터 및 설치 패키지에 대한 업데이트를 ESET Management 에이전트로 배포.
    - ESET Management 에이전트의 통신을 ESET PROTECT 서버에 전달합니다.
- 모바일 장치 커넥터 - ESET PROTECT를 사용하여 모바일 장치를 관리할 수 있는 구성 요소로, 이를 통해 모바일 장치(Android 및 iOS)와 Android용 ESET Endpoint Security를 관리할 수 있습니다.
- ESET PROTECT 가상 어플라이언스 - 가상화된 환경에서 ESET PROTECT을(를) 실행하려는 사용자를 위해 제공됩니다.
- ESET PROTECT Virtual Agent Host - 에이전트가 없는 가상 컴퓨터를 관리할 수 있도록 에이전트 엔터티를 가상화하는 ESET PROTECT의 구성 요소입니다. 이 솔루션은 물리적 컴퓨터의 ESET Management 에이전트와 같은 작업 관리 수준, 동적 그룹 사용 및 자동화 기능을 활성화합니다. 가상 에이전트는 가상 컴퓨터에서 정보를 수집하여 ESET PROTECT 서버로 전송합니다.
- 미러 도구 - 오프라인 모듈 업데이트에 필요합니다. 클라이언트 컴퓨터가 인터넷에 연결되어 있지 않은 경우 미러 도구를 사용하여 ESET 업데이트 서버에서 업데이트 파일을 다운로드한 후 로컬로 저장할 수 있습니다.
- ESET Remote Deployment Tool - <%PRODUCT%> 웹 콘솔에서 생성된 통합형 패키지를 배포합니다. 이 도구를 통해 ESET Management 에이전트와 ESET 제품을 네트워크로 컴퓨터에 편리하게 배포할 수 있습니다.

ℹ 자세한 내용은 ESET PROTECT 온라인 도움말을 참조하십시오.

ESET PROTECT Cloud 소개

ESET PROTECT Cloud를 사용하면 ESET PROTECT 또는 의 경우처럼 물리 또는 가상 서버가 필요 없이 중앙 위치한 곳에서 네트워크로 연결된 환경의 워크스테이션과 서버에서 ESET 제품을 관리할 수 있습니다. ESET PROTECT Cloud 웹 콘솔을 사용하여 ESET 솔루션을 배포하고 작업을 관리하며 보안 정책을 적용하고 시스템 상태를 모니터링하며 원격 컴퓨터의 문제 또는 위협에 신속하게 대응할 수 있습니다.

ESET PROTECT Cloud는 다음 구성 요소로 구성됩니다.

- ESET PROTECT Cloud 인스턴스 - 이 서버는 에이전트와의 통신을 처리하며 DB에서 애플리케이션 데이터를 수집 및 저장합니다.
- ESET PROTECT Cloud 웹 콘솔 - 웹 콘솔은 사용자 환경에서 클라이언트 컴퓨터를 관리할 수 있도록 해 주는 기본 인터페이스입니다. 이 인터페이스는 네트워크상의 클라이언트 상태 개요를 표시하고, 이를 통해 관리되지 않는 컴퓨터에 ESET 솔루션을 원격으로 배포할 수 있습니다. 인터넷이 연결된 모든 장소 또는 장치에서 ESET PROTECT Cloud를 사용할 수 있습니다.
- ESET Management 에이전트 - ESET PROTECT Cloud와 클라이언트 컴퓨터 간의 통신을 원활하게 해 줍니다. 에이전트는 컴퓨터와 ESET PROTECT Cloud 간의 통신을 설정하려는 클라이언트 컴퓨터에 설치해야 합니다. 에이전트가 클라이언트 컴퓨터에 설치되고 여러 보안 시나리오가 저장될 수 있으므로 ESET Management 에이전트를 사용하면 새 감지에 대한 반응 시간이 대폭 줄어듭니다. ESET PROTECT Cloud 웹 콘솔을 사용하여 관리되지 않는 컴퓨터에 ESET Management 에이전트를 배포할 수 있습니다. 또한 필요한 경우 클라이언트 컴퓨터에 ESET Management 에이전트를 수동으로 설치할 수 있습니다.
- ESET Bridge - ESET PROTECT Cloud와 함께 사용하여 다음을 수행할 수 있는 서비스입니다.
    - 클라이언트 컴퓨터 및 설치 패키지에 대한 업데이트를 ESET Management 에이전트로 배포.
    - ESET Management 에이전트의 통신을 ESET PROTECT Cloud에 전달합니다.
- 모바일 장치 관리 - ESET PROTECT Cloud를 사용하여 모바일 장치를 관리할 수 있는 구성 요소로, 이를 통해 모바일 장치(Android 및 iOS)와 Android용 ESET Endpoint Security를 관리할 수 있습니다.
- 취약성 및 패치 관리 - 워크스테이션을 정기적으로 검사하여 보안 위험에 취약할 수 있는 설치된 소프트웨어를 탐지하는 ESET PROTECT Cloud의 기능입니다. 패치 관리는 자동화된 소프트웨어 업데이트를 통해 이러한 위험을 수정하여 장치를 보다 안전하게 유지하는 데 도움이 됩니다.

자세한 내용은 ESET PROTECT Cloud 온라인 도움말을 참조하십시오.

패스워드로 보호된 설정

시스템에 최대한의 보안 성능을 제공하려면 ESET Endpoint Security을(를) 올바르게 구성해야 합니다. 잘못 변경하거나 설정하면 클라이언트 보안 성능과 보호 수준이 저하될 수 있습니다. 고급 설정에 대한 사용자 접근을 제한하기 위해 관리자가 설정을 패스워드로 보호할 수 있습니다.

관리자는 연결된 클라이언트 컴퓨터에서 ESET Endpoint Security 고급 설정을 패스워드로 보호하기 위한 정책을 생성할 수 있습니다. 새 정책을 생성하려면:

1. ESET PROTECT 웹 콘솔의 왼쪽 기본 메뉴에 있는 **정책**을 클릭합니다.
2. **새 정책**을 클릭합니다.
3. 새 정책의 이름을 지정하고 간략한 설명을 제공합니다. **계속** 버튼을 클릭합니다.
4. 제품 목록에서 **Windows용 ESET Endpoint를** 선택합니다.
5. **설정** 목록에서 **사용자 인터페이스**를 클릭하고 **접근 설정**을 확장합니다.
6. ESET Endpoint Security 버전에 따라 토글을 클릭하여 **설정을 보호하기 위한 패스워드**를 활성화합니다. ESET Endpoint 제품 버전 7은 향상된 보호 기능을 제공합니다. 네트워크에 Endpoint 제품 버전 7과 버전 6이 모두 있는 경우 각 버전에 다른 패스워드를 사용하여 두 가지 별도 정책을 생성하는 것이 좋습니다.
7. 알림 창에서 새 패스워드를 생성하고 이를 확인한 후 **확인**을 클릭합니다. **계속**을 클릭합니다.
8. 클라이언트에 정책을 할당합니다. **할당**을 클릭하고 패스워드로 보호할 컴퓨터 또는 컴퓨터 그룹을 선택합니다. **확인**을 클릭하여 확인합니다.
9. 원하는 모든 클라이언트 컴퓨터에 대상 목록에 있는지 확인하고 **계속**을 클릭합니다.

10. 요약에서 정책 설정을 검토하고 **마침**을 클릭하여 새 정책을 저장합니다.

정책이란?

관리자는 ESET PROTECT 웹 콘솔의 정책을 사용하여 클라이언트 컴퓨터에서 실행되는 ESET 제품에 특정 구성을 푸시할 수 있습니다. 정책은 개별 컴퓨터와 컴퓨터 그룹에 직접 적용할 수 있습니다. 또한, 여러 정책을 하나의 컴퓨터 또는 그룹에 할당할 수 있습니다.

A user must have the following permissions to create a new policy: 사용자에게 정책 목록을 읽을 수 있는 **읽기** 권한, 대상 컴퓨터에 정책을 할당할 수 있는 **사용** 권한, 정책을 생성, 수정하거나 편집할 수 있는 **쓰기** 권한이 있어야 합니다.

정책은 정적 그룹의 순서로 적용됩니다. 동적 그룹의 경우 정책이 하위 동적 그룹에 먼저 적용됩니다. 따라서 최상위 수준의 그룹 트리에 더 큰 영향을 주는 정책을 적용하고 하위 그룹에 더 구체적인 정책을 적용할 수 있습니다. 트리 내 상위에 위치한 그룹에 접근할 수 있는 ESET Endpoint Security 사용자는 플래그를 이용하여 하위 그룹의 정책을 재정의할 수 있습니다. 알고리즘은 ESET PROTECT 온라인 도움말에 설명되어 있습니다.

> 그룹 트리 내 상위에 있는 그룹에 더 일반적인 정책(예: 업데이트 서버 정책)을 할당하는 것이 좋습니다. 더 구체적인 정책(예: 장치 제어 설정)은 그룹 트리의 하위 수준에 할당해야 합니다. 정책 플래그를 통해 별도로 정의하는 경우가 아니라면 병합 시 일반적으로 하위 정책이 상위 정책의 설정을 재정의합니다.

정책 병합

클라이언트에 적용된 정책은 일반적으로 여러 정책을 하나의 최종 정책으로 병합한 결과입니다. 정책은 하나씩 병합됩니다. 정책을 병합하는 경우 일반 규칙은 이후 정책이 항상 이전 정책에서 지정된 설정을 대체합니다. 이 동작을 변경하려면 정책 플래그를 사용하면 됩니다(설정별로 사용 가능).

정책을 생성할 때 일부 설정에서는 추가 규칙(대체/추가/앞에 추가)을 구성할 수 있습니다.

- **대체** - 전체 목록을 대체하고 새 값을 추가하며 이전의 모든 값을 제거합니다.
- **추가** - 현재 적용된 목록의 하단에 항목이 추가됩니다(다른 정책이어야 하며, 로컬 목록을 항상 덮어씀).
- **앞에 추가** - 목록의 상단에 항목이 추가됩니다(로컬 목록을 덮어씀).

ESET Endpoint Security은(는) 원격 정책이 포함된 로컬 설정의 병합을 새로운 방법으로 지원합니다. 설정이 목록(예: 차단된 웹 사이트 목록)이고 원격 정책이 기존 로컬 설정과 충돌하는 경우 원격 정책을 덮어씁니다. 서로 다른 병합 규칙을 선택하여 로컬 목록과 원격 목록을 결합하는 방법을 선택할 수 있습니다.

- 원격 정책에 대한 병합 설정
- 원격 및 로컬 정책의 병합 - 로컬 설정을 결과 원격 정책과 병합

정책 병합에 대해 자세히 알아보려면 ESET PROTECT 온라인 사용자 설명서에 따르고 예를 참조하십시오.

플래그의 작동 방식

클라이언트 컴퓨터에 적용되는 정책은 일반적으로 여러 정책을 하나의 최종 정책으로 병합한 결과입니다. 정책을 병합하는 경우 정책 플래그를 사용하면 적용된 정책의 순서로 인해 최종 정책의 예상되는 동작을 조정할 수 있습니다. 플래그는 정책에서 특정 설정을 처리하는 방법을 정의합니다.

각 설정에 대해 다음 플래그 중 하나를 선택할 수 있습니다.

적용되지 않음	적용되지 않음 - 이 플래그가 있는 모든 설정이 정책으로 설정되지 않습니다. 설정이 정책으로 설정되지 않으므로 나중에 적용되는 다른 정책에서 변경할 수 있습니다.
적용	**적용** 플래그가 있는 설정은 클라이언트 컴퓨터에 적용됩니다. 그러나 정책을 병합하는 경우 나중에 적용되는 다른 정책으로 덮어쓸 수 있습니다. 이 플래그로 표시된 설정을 포함하는 클라이언트 컴퓨터에 정책이 전송되면 해당 설정이 클라이언트 컴퓨터의 로컬 구성을 변경합니다. 설정은 강제 적용되지 않으므로 나중에 적용되는 다른 정책에서 변경할 수 있습니다.
강제 적용	**강제 적용** 플래그가 있는 설정은 우선적으로 적용되며 **강제 적용** 플래그가 있어도 나중에 적용되는 정책으로 덮어쓸 수 없습니다. 따라서 병합하는 동안 나중에 적용되는 다른 정책에서 이 설정을 변경할 수 없습니다. 이 플래그로 표시된 설정을 포함하는 클라이언트 컴퓨터에 정책이 전송되면 해당 설정이 클라이언트 컴퓨터의 로컬 구성을 변경합니다.

시나리오: 관리자가 사용자 *John*이 자신의 홈 그룹에서 정책을 생성하거나 편집하도록 허용하고, 강제 적용 플래그가 있는 정책을 포함하여 관리자가 생성한 모든 정책을 보도록 허용하려고 합니다. 관리자는 *John*이 모든 정책을 볼 수 있도록 하되 관리자가 생성한 기존 정책을 편집할 수는 없도록 하려고 합니다. *John*은 자신의 홈 그룹, San Diego 내에서만 정책을 생성하거나 편집할 수 있습니다.
솔루션:관리자는 다음 단계를 수행해야 합니다.
사용자 지정 정적 그룹 및 권한 집합 생성
1. 새 정적 그룹 *San Diego*를 생성합니다.
2. 모두 정적 그룹 접근 권한이 있고 **정책**에 대한 **읽기** 권한이 있는 새 권한 집합 정책 - 모두*(John)*를 생성합니다.
3. *San Diego* 정적 그룹 접근 권한이 있고 **그룹과 컴퓨터** 및 **정책**에 대한 **쓰기** 기능 접근 권한이 있는 새 권한 집합 정책*(John)*을 생성합니다. 이 권한 집합은 *John*이 자신의 홈 그룹 *San Diego*에서 정책을 생성하거나 편집하도록 허용합니다.
4. 새 사용자 *John*을 생성하고 **권한 집합** 섹션에서 정책 - 모두*(John)* 및 정책*(John)*을 선택합니다.
정책 생성
5. 새 정책 모두 - 방화벽 활성화를 생성하고 **설정** 섹션을 확장한 다음 **Windows용 ESET Endpoint**를 선택하고 **개인 방화벽 > 기본**으로 이동하여 **강제 적용** 플래그를 통해 모든 설정을 적용합니다. **할당** 섹션을 확장하고 정적 그룹 모두를 선택합니다.
6. 새 정책 *John* 그룹 - 방화벽 활성화를 생성하고 **설정** 섹션을 확장한 다음 **Windows용 ESET Endpoint**를 선택하고 **개인 방화벽 > 기본**으로 이동하여 **적용** 플래그를 통해 모든 설정을 적용합니다. **할당** 섹션을 확장하고 정적 그룹 *San Diego*를 선택합니다.
결과
관리자가 생성한 정책은 **강제 적용** 플래그가 정책 설정에 적용된 후 가장 먼저 적용됩니다. 강제 적용 플래그가 있는 설정은 우선적으로 적용되며 나중에 적용되는 다른 정책으로 덮어쓸 수 없습니다. 사용자 *John*이 생성한 정책은 관리자가 정책을 생성한 후에 적용됩니다.
최종 정책 순서를 확인하려면 **자세히 > 그룹 > San Diego**로 이동합니다. 컴퓨터를 선택하고 **상세 정보 표시**를 선택합니다. **구성** 섹션에서 **적용된 정책**을 클릭합니다.

설치

ESET PROTECT 또는 ESET PROTECT Cloud을(를) 통해 원격으로 클라이언트 워크스테이션에 ESET Endpoint Security을(를) 배포하지 않는 경우 클라이언트 워크스테이션에서의 ESET Endpoint Security 설치 방법이 몇

가지 있습니다.

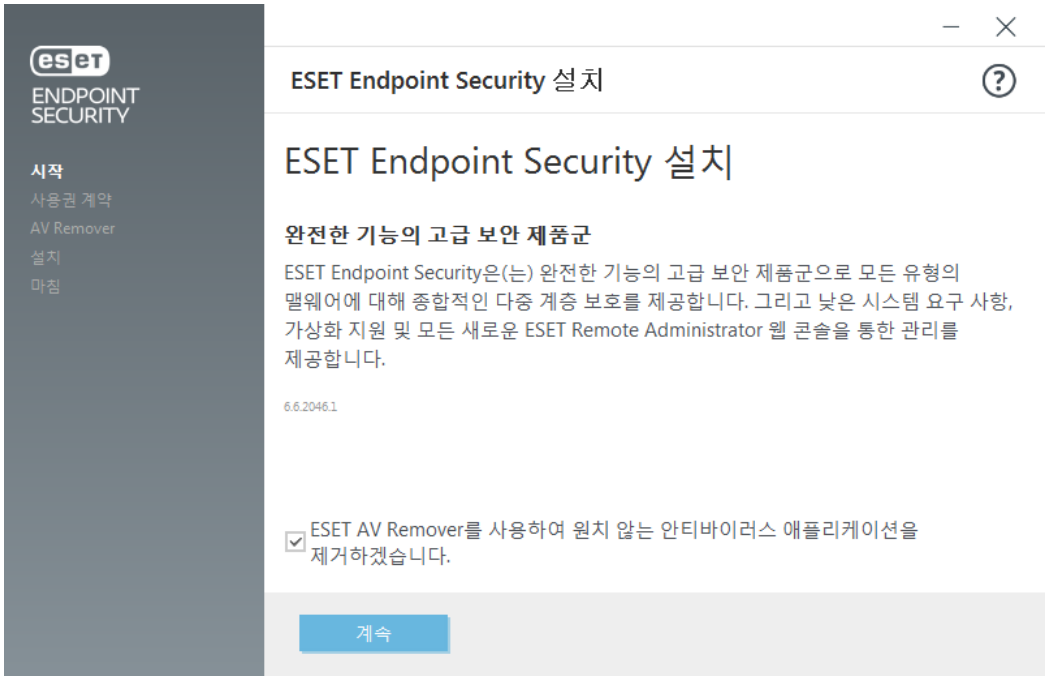
ESET Endpoint Security가 이미 설치된 상태에서 ESET Endpoint Antivirus 설치 관리자를 실행하여 ESET Endpoint Security에서 ESET Endpoint Antivirus로 다운그레이드할 수 있습니다. 그러나 동일한 버전 또는 이후 버전을 설치해야 합니다.

방법	목적	다운로드 링크
ESET AV Remover를 사용하여 설치	ESET AV Remover 도구를 통해 설치를 진행하기 전에 시스템에 이전에 설치된 거의 모든 안티바이러스 소프트웨어를 제거할 수 있습니다.	64비트 다운로드 32비트 다운로드
*** 설치(.exe)	ESET AV Remover 없는 설치 프로세스.	64비트 다운로드 32비트 다운로드
설치(.msi)	비즈니스 환경에서는 .msi 설치 관리자가 설치 패키지로 선호됩니다. 이것은 주로 ESET PROTECT 등의 다양한 도구를 사용하는 오프라인 및 원격 배포 때문입니다.	64비트 다운로드 32비트 다운로드
명령줄 설치	ESET Endpoint Security은(는) 명령줄을 사용하여 로컬로 설치하거나 ESET PROTECT의 클라이언트 작업을 사용하여 원격으로 설치할 수 있습니다.	해당 없음
GPO 또는 SCCM을 사용한 배포	GPO 또는 SCCM 같은 관리 도구를 사용하여 ESET Management Agent와 ESET Endpoint Security을(를) 클라이언트 워크스테이션에 배포합니다.	해당 없음
RMM 도구를 사용하여 배포	RMM(원격 관리 및 모니터링) 도구용 ESET DEM 플러그인을 사용하여 클라이언트 워크스테이션에 ESET Endpoint Security을(를) 배포할 수 있습니다.	해당 없음

ESET Endpoint Security에서는 30여 개의 언어를 사용할 수 있습니다.

ESET AV Remover를 사용하여 설치

설치 프로세스를 계속하기 전에 컴퓨터에서 기존의 보안 응용 프로그램을 모두 제거해야 합니다. **ESET AV Remover를 사용하여 원치 않는 안티바이러스 애플리케이션을 제거하겠습니다.** 옆의 확인란을 선택하여 ESET AV Remover가 시스템을 검색하고 지원되는 보안 응용 프로그램을 모두 제거하도록 합니다. ESET AV Remover를 실행하지 않고 ESET Endpoint Security을(를) 설치하려면 이 확인란을 선택하지 않은 상태로 두고 **계속**을 클릭합니다.

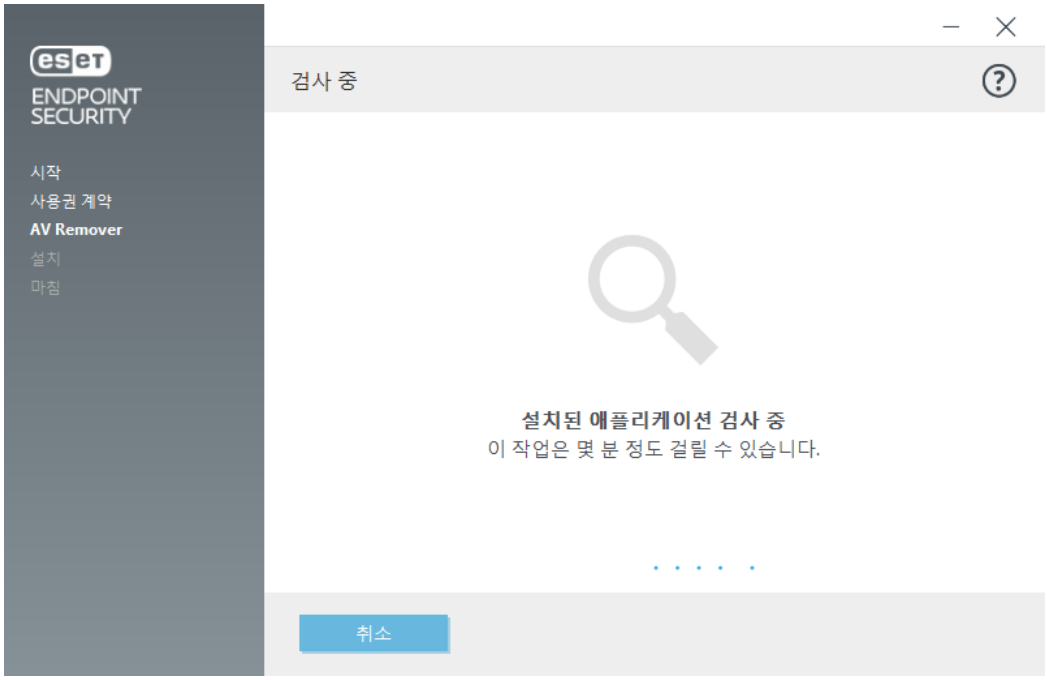


ESET AV Remover

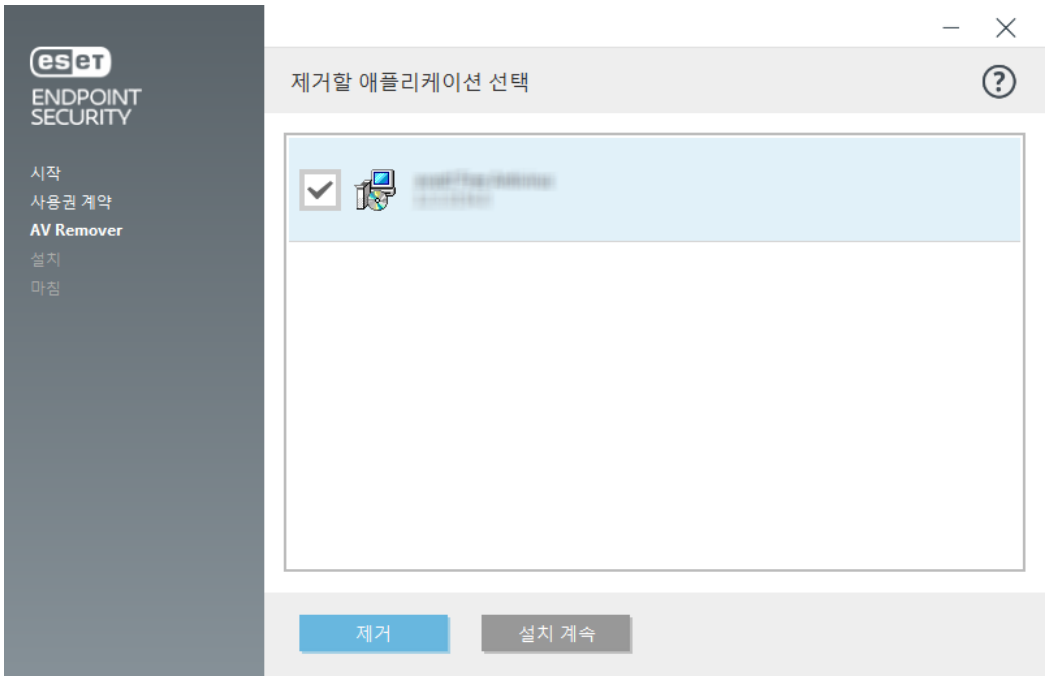
ESET AV Remover 도구를 통해 시스템에 이전에 설치된 거의 모든 안티바이러스 소프트웨어를 제거할 수 있습니다. ESET AV Remover를 사용하여 기존의 안티바이러스 프로그램을 제거하려면 아래 지침을 따르십시오.

1. ESET AV Remover를 통해 제거할 수 있는 안티바이러스 소프트웨어 목록을 보려면 ESET 지식 베이스 문서를 참조하십시오.
2. 최종 사용자 사용권 계약을 읽고 **동의**를 클릭하여 사용권 계약에 동의합니다. **동의 안 함**을 클릭하면 컴퓨터에서 기존의 보안 응용 프로그램이 제거되지 않은 상태에서 ESET Endpoint Security 설치가 진행됩니다.

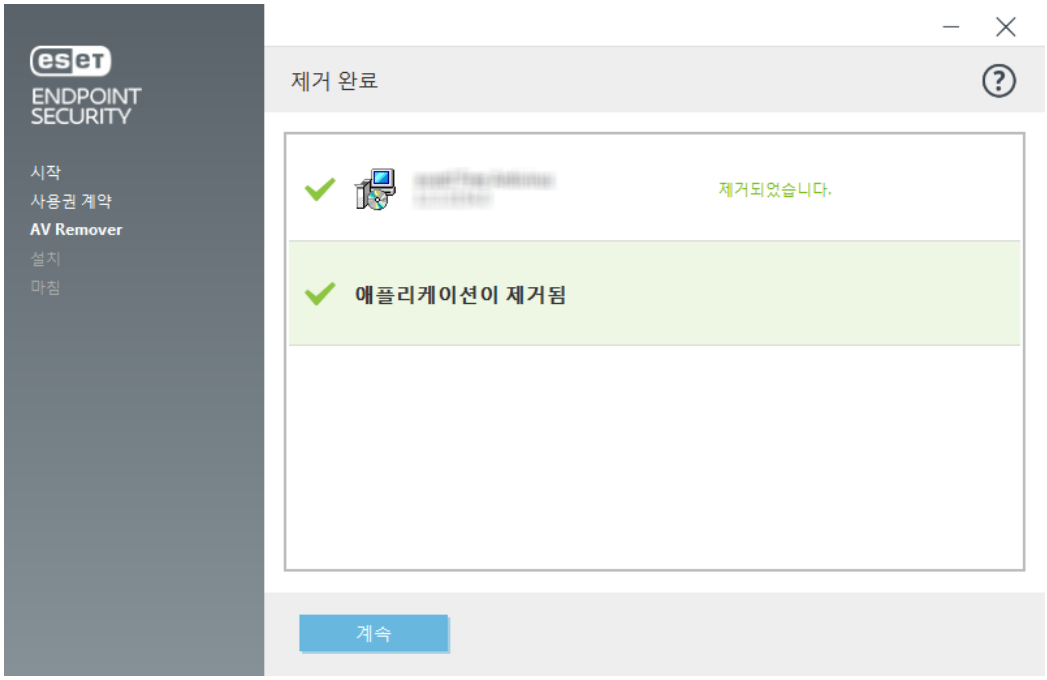
2. ESET AV Remover가 시스템에서 안티바이러스 소프트웨어 검색을 시작합니다.



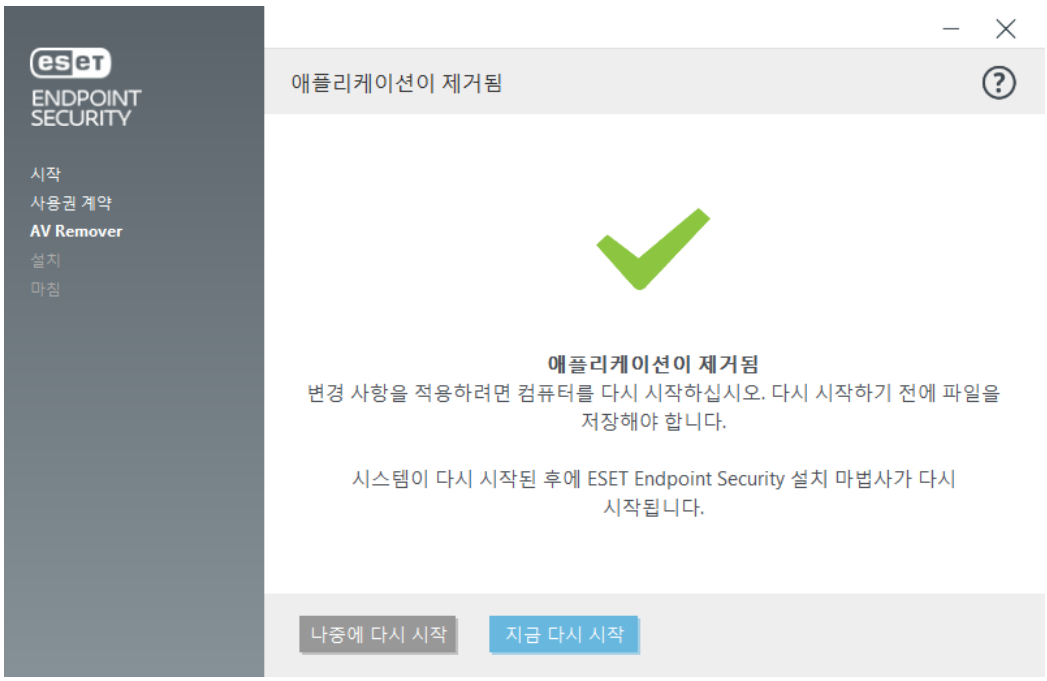
2. 목록에서 제거할 안티바이러스 애플리케이션을 선택하고 **제거**를 클릭합니다. 제거 작업은 다소 시간이 걸릴 수 있습니다.



2. 제거가 완료되면 **계속**을 클릭합니다.



6. 컴퓨터를 다시 시작하여 변경 내용을 적용하고 ESET Endpoint Security 설치를 계속합니다. 제거에 실패한 경우 이 설명서의 ESET AV Remover를 사용하여 제거가 완료되었지만 오류가 있음 섹션을 참조하십시오.



ESET AV Remover를 사용하여 제거가 완료되었지만 오류가 있음

ESET AV Remover를 사용하여 안티바이러스 프로그램을 제거할 수 없는 경우 제거하려는 응용 프로그램이 ESET AV Remover에서 지원되지 않을 수 있음을 나타내는 알림이 수신됩니다. 특정 프로그램을 제거할 수 있는지 여부를 확인하려면 ESET 지식 베이스에서 지원되는 제품 목록이나 일반 Windows 안티바이러스 소프트웨어 제거 관리자를 참조하십시오.

보안 제품을 제거하지 못했거나 구성 요소 일부가 부분적으로 제거된 경우 **다시 시작하여 다시 검색**하라는

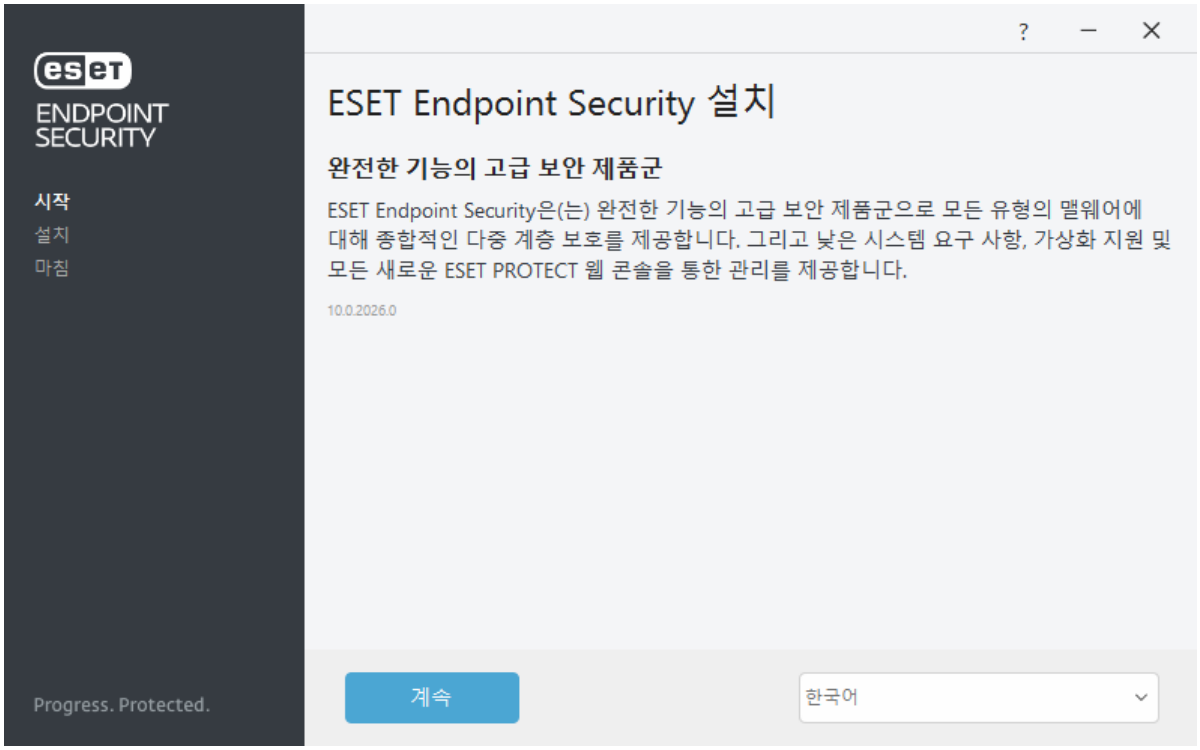
메시지가 표시됩니다. 시작 후 UAC를 확인하고 검사 및 제거 프로세스를 계속하십시오.

필요한 경우 ESET 기술 지원에 연락하여 지원 요청을 개설하고 **AppRemover.log** 파일을 ESET 기술 지원 담당자에게 제공하십시오. **AppRemover.log** 파일은 **eset** 폴더에 있습니다. Windows Explorer에서 *%TEMP%*로 이동하여 이 폴더에 접근합니다. ESET 기술 지원이 최대한 신속하게 응답하여 문제 해결을 지원할 것입니다.

설치(.exe)

.exe 설치 프로그램을 시작하면 설치 마법사가 설치 프로세스를 안내합니다.

컴퓨터에 다른 안티바이러스 프로그램이 설치되어 있지 않은지 확인합니다. 하나의 컴퓨터에 둘 이상의 안티바이러스 솔루션이 설치된 경우 서로 충돌할 수 있습니다. 따라서 시스템의 다른 안티바이러스 프로그램을 제거하는 것이 좋습니다. 일반 안티바이러스 소프트웨어에 대한 제거 도구 목록은 지식 베이스 문서를 참조하십시오(영어 및 기타 여러 언어로 제공).



1. 다음 기능에 대한 기본 설정을 선택하고 최종 사용자 사용권 계약 및 개인 정보 보호 정책을 읽은 후 **계속**을 클릭하거나, **모두 허용 후 계속**을 클릭하여 모든 기능을 활성화합니다.

- ESET LiveGrid® 피드백 시스템
- 사용자가 원치 않는 애플리케이션 탐지

계속 또는 **모두 허용 후 계속**을 클릭하면 최종 사용자 사용권 계약과 개인 정보 보호 정책에 동의하는 것입니다. 설치 폴더 변경을 클릭하면 특정 폴더에 ESET Endpoint Security을(를) 설치할 수 있습니다.

2. 설치가 완료되면 ESET Endpoint Security 활성화 여부를 묻는 메시지가 표시됩니다.

설치 폴더 변경(.exe)

설치 중에 **설치 폴더를 변경**할 수 있습니다. ESET Endpoint Security 설치 위치를 선택합니다. 기본적으로 프로그램은 다음 디렉터리에 설치됩니다.

C:\Program Files\ESET\ESET Security

프로그램 모듈 및 데이터의 위치를 지정할 수 있습니다. 기본적으로 프로그램 모듈 및 데이터는 각각 다음 디렉터리에 설치됩니다.

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

이러한 위치를 변경하려면 **찾아보기**를 클릭합니다(권장되지 않음).

뒤로를 클릭한 다음 설치 프로세스를 계속 진행합니다.

설치(.msi)

.msi 설치 프로그램을 실행하면 설치 마법사가 설치 프로세스를 안내합니다.

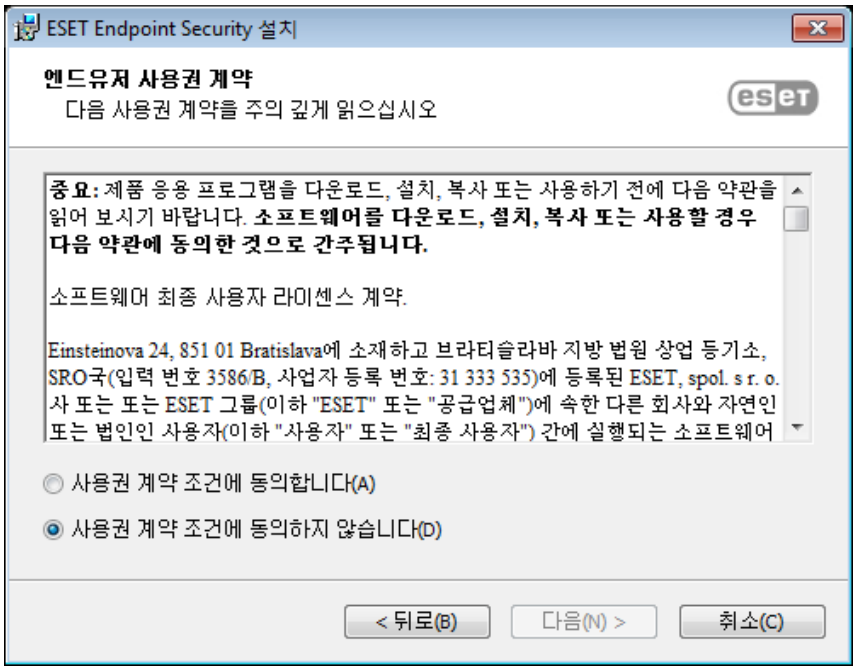
비즈니스 환경에서는 .msi 설치 관리자가 설치 패키지로 선호됩니다. 이것은 주로 ESET PROTECT 등의 다양한 도구를 사용하는 오프라인 및 원격 배포 때문입니다.

컴퓨터에 다른 안티바이러스 프로그램이 설치되어 있지 않은지 확인합니다. 하나의 컴퓨터에 둘 이상의 안티바이러스 솔루션이 설치된 경우 서로 충돌할 수 있습니다. 따라서 시스템의 다른 안티바이러스 프로그램을 제거하는 것이 좋습니다. 일반 안티바이러스 소프트웨어에 대한 제거 도구 목록은 지식 베이스 문서를 참조하십시오(영어 및 기타 여러 언어로 제공).

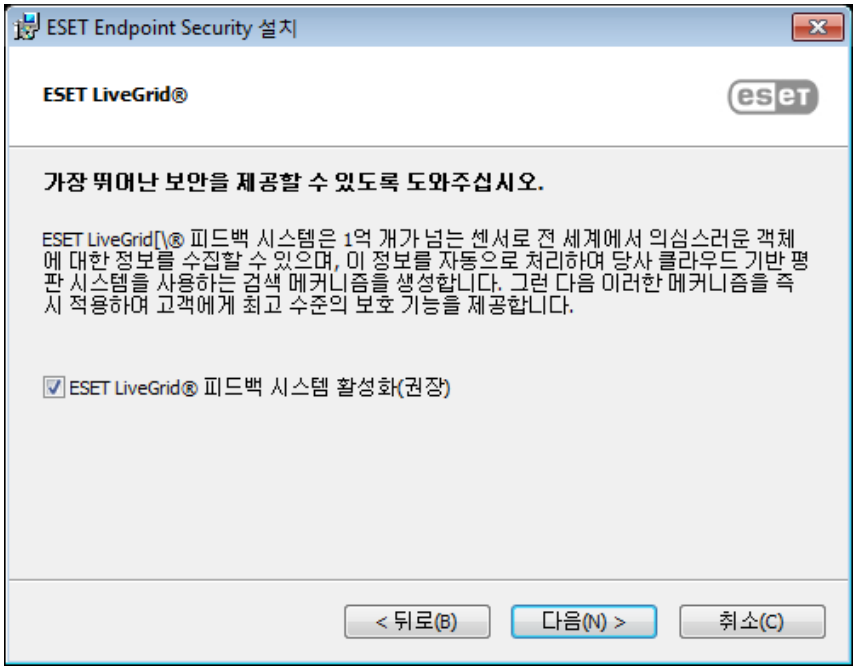
ESET PROTECT에서 생성된 ESET Endpoint Security 설치 관리자는 가상 데스크톱용 Windows 10 Enterprise 및 Windows 10 다중 세션 모드를 지원합니다.

1. 원하는 언어를 선택하고 **다음**을 클릭합니다.

2. 최종 사용자 사용권 계약을 읽고 **사용권 계약의 조건에 동의함**을 클릭하여 최종 사용자 사용권 계약에 동의합니다. 사용권 계약 조건에 동의한 후 **다음**을 클릭하여 설치를 계속합니다.



3. ESET LiveGrid® 피드백 시스템의 기본 설정을 선택합니다. ESET LiveGrid®에서는 ESET이 새로운 침입에 대한 정보를 즉각적이고 지속적으로 확인하여 고객을 더 잘 보호할 수 있도록 해줍니다. 이 시스템을 사용하면 ESET 바이러스 연구소에 새로운 위협을 전송할 수 있으며, 여기서 위협을 분석, 처리하고 탐지 엔진에 추가합니다. **고급 설정**을 클릭하여추가 설치 파라미터를 구성합니다.



4. 최종 단계에서는 **설치**를 클릭하여 설치를 확인합니다. 설치가 완료되면 ESET Endpoint Security 활성화 여부를 묻는 메시지가 표시됩니다.

고급 설치(.msi)

고급 설치에서는 표준 설치를 수행할 때 사용할 수 없는 설치 파라미터를 사용자 지정할 수 있습니다.

1. 설치 중에 **설치 폴더를 변경**할 수 있습니다. ESET Endpoint Security 설치 위치를 선택합니다. 기본적으로 프로그램은 다음 디렉터리에 설치됩니다.

C:\Program Files\ESET\ESET Security

프로그램 모듈 및 데이터의 위치를 지정할 수 있습니다. 기본적으로 프로그램 모듈 및 데이터는 각각 다음 디렉터리에 설치됩니다.

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

이러한 위치를 변경하려면 **찾아보기**를 클릭합니다(권장되지 않음).

2. 설치할 제품 구성 요소를 선택합니다. 컴퓨터 검사 및 사용 가능한 모든 보호 기능에 대한 기본 설정을 선택할 수 있습니다. 업데이트 미러 구성 요소는 네트워크의 다른 컴퓨터를 업데이트하는 데 사용할 수 있습니다. 원격 모니터링 및 관리(RMM)는 관리 서비스 공급자가 접근할 수 있는, 로컬에 설치된 에이전트를 사용하여 소프트웨어 시스템 을 감독하고 제어하는 프로세스입니다.

3. **설치**를 클릭하여 설치 프로세스를 시작합니다.

최소 모듈 설치

설치 관리자의 크기와 관련된 네트워크 트래픽을 줄이고 리소스를 절약하기 위해 ESET은 최소한의 모듈 설치 관리자를 함께 제공합니다. 설치 프로그램에는 필수 모듈만 포함되며, 다른 모든 모듈은 제품 활성화 후 초기 모듈을 업데이트하는 동안 다운로드됩니다. 주요 장점은 설치 프로그램이 훨씬 작아지고, ESET

Endpoint Security에서 제품을 활성화할 때 최신 애플리케이션 모듈만 다운로드할 수 있다는 점입니다.

최소 모듈 설치 관리자에는 계속해서 다음 모듈이 포함됩니다.

- 로더
- Direct Cloud 통신
- 변환 지원
- 구성
- SSL

제품 활성화 후 기능 초기화에 대해 알려 주는 **보호 초기화 중** 상태가 표시됩니다.

모듈 다운로드에 문제가 있는 경우(예: 프록시 설정, 네트워크 없음 등) 경고 애플리케이션 상태 **주의 필요**가 표시됩니다. 기본 프로그램 창에서 **업데이트** > **업데이트 확인**을 클릭하여 프로세스를 다시 시작합니다.

여러 번의 시도가 실패하면, 빨간색 애플리케이션 상태 **보호 설정 실패**가 표시됩니다. 다시 시도를 클릭하여 보호 설정을 다시 시작합니다. 초기화 프로세스에 실패한 후 여전히 모듈을 다운로드할 수 없으면 전체 MSI 설치 관리자를 다운로드하십시오.

클라이언트 컴퓨터가 인터넷에 연결되어 있지 않거나 오프라인으로 작동하여 업데이트가 필요한 경우, 다음 방법을 사용하여 ESET 업데이트 서버에서 업데이트 파일을 다운로드합니다.
- 미러에서 업데이트
- 미러 도구 사용

명령줄 설치

명령줄을 사용하여 ESET Endpoint Security을(를) 로컬로 설치하거나, ESET PROTECT에서 클라이언트 작업을 사용하여 원격으로 설치할 수 있습니다.

지원되는 파라미터

APPDIR=<path>

- 경로 - 유효한 디렉터리 경로
- 애플리케이션 설치 디렉터리입니다.

APPDATADIR=<path>

- 경로 - 유효한 디렉터리 경로
- 애플리케이션 데이터 설치 디렉터리입니다.

MODULEDIR=<path>

- 경로 - 유효한 디렉터리 경로
- 모듈 설치 디렉터리입니다.

ADDLOCAL=<list>

- 구성 요소 설치 - 로컬로 설치할 비필수 기능 목록입니다.
- ESET .msi 패키지에서 사용: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`

- **ADDLOCAL** 속성에 대한 자세한 내용은 http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx를 참조하십시오.

ADDEXCLUDE=<list>

- ADDEXCLUDE 목록은 설치되지 않은 모든 기능 이름이 쉼표로 구분된 목록으로, 더 이상 사용되지 않는 REMOVE 목록을 대체합니다.
- 설치하지 않은 기능을 선택할 때 전체 경로(예: 모든 하위 기능) 및 관련된 숨김 기능이 목록에 명시적으로 포함되어 있어야 합니다.
- ESET .msi 패키지에서 사용: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

ADDEXCLUDE는 **ADDLOCAL**과 함께 사용할 수 없습니다.

해당 명령줄 스위치에 사용되는 **msiexec** 버전의 설명서를 참조하십시오.

규칙

- **ADDLOCAL** list는 설치할 모든 기능 이름이 쉼표로 구분되어 있는 목록입니다.
- 설치할 기능 선택 시 전체 경로(모든 상위 기능)가 목록에 명시적으로 포함되어야 합니다.
- 정확한 사용에 대해서는 추가 규칙을 참조하십시오.

구성 요소 및 기능

ADDLOCAL/ADDEXCLUDE 파라미터를 사용하여 구성 요소를 설치하는 경우 ESET Endpoint Antivirus에서 작동하지 않습니다.

기능은 다음의 네 가지 범주로 나뉩니다.

- **필수** – 해당 기능은 항상 설치됩니다.
- **옵션** – 해당 기능은 설치되지 않도록 선택 취소할 수 있습니다.
- **숨김** - 다른 기능이 제대로 작동하기 위한 필수 논리 기능
- **자리 표시자** - 제품에 영향을 미치지 않는 기능이지만 하위 기능과 함께 목록에 나열되어야 합니다.

ESET Endpoint Security의 기능 집합은 다음과 같습니다.

설명	기능 이름	기능 부모	현재 상태
기본 프로그램 구성 요소	Computer		자리 표시자
탐지 엔진	Antivirus	Computer	필수
탐지 엔진/악성코드 검사	Scan	Computer	필수
탐지 엔진/실시간 파일 시스템 보호	RealtimeProtection	Computer	필수
탐지 엔진/악성코드 검사/문서 보호	DocumentProtection	Antivirus	옵션
장치 제어	DeviceControl	Computer	옵션
네트워크 보호	Network		자리 표시자
네트워크 보호/방화벽	Firewall	Network	옵션

설명	기능 이름	기능 부모	현재 상태
네트워크 보호/네트워크 공격 보호/...	IdsAndBotnetProtection	Network	옵션
안전한 브라우저	OnlinePaymentProtection	WebAndEmail	옵션
웹 및 이메일	WebAndEmail		자리 표시자
웹 및 이메일/프로토콜 필터링	ProtocolFiltering	WebAndEmail	숨김
웹 및 이메일/웹 브라우저 보호	WebAccessProtection	WebAndEmail	옵션
웹 및 이메일/이메일 클라이언트 보호	EmailClientProtection	WebAndEmail	옵션
웹 및 이메일/이메일 클라이언트 보호/이메일 클라이언트	MailPlugins	EmailClientProtection	숨김
웹 및 이메일/이메일 클라이언트 보호/이메일 클라이언트 안티스팸	Antispam	EmailClientProtection	옵션
웹 및 이메일/웹 컨트롤	WebControl	WebAndEmail	옵션
도구/ESET RMM	Rmm		옵션
업데이트/프로필/업데이트 미러	UpdateMirror		옵션
ESET Inspect 플러그인	EnterpriseInspector		숨김

그룹 기능 집합:

설명	기능 이름	기능 상태
모든 필수 기능	_Base	숨김
사용 가능한 모든 기능	ALL	숨김

추가 규칙

- **WebAndEmail** 기능 중 설치하도록 선택된 기능이 있는 경우 숨겨진 **ProtocolFiltering** 기능이 목록에 포함되어야 합니다.
- 모든 기능의 이름은 대소문자를 구분합니다(예: UpdateMirror는 UPDATEMIRROR와 같지 않음).

구성 속성 목록

속성	값	기능
CFG_POTENTIALLYUNWANTED_ENABLED=	0 - 비활성화됨 1 - 활성화됨	PUA 탐지
CFG_LIVEGRID_ENABLED=	아래 참조	아래의 LiveGrid 속성 참조
FIRSTSCAN_ENABLE=	0 - 비활성화됨 1 - 활성화됨	설치 후 컴퓨터 검사 예약 및 실행
CFG_PROXY_ENABLED=	0 - 비활성화됨 1 - 활성화됨	프록시 서버 설정
CFG_PROXY_ADDRESS=	<ip>	프록시 서버 IP 주소
CFG_PROXY_PORT=	<port>	프록시 서버 포트 번호
CFG_PROXY_USERNAME=	<username>	인증용 사용자 이름

속성	값	기능
CFG_PROXY_PASSWORD=	<password>	인증을 위한 비밀번호입니다
ACTIVATION_DATA=	아래 참조	제품 활성화, 라이선스 키 또는 오프라인 라이선스 파일
ACTIVATION_DLG_SUPPRESS=	0 - 비활성화됨 1 - 활성화됨	"1"로 설정하면 처음 시작한 후 제품 활성화 대화 상자가 표시되지 않음
ADMINCFG=	<path>	내보낸 XML 구성의 경로 (기본값 *cfg.xml*)

ESET Endpoint Security의 구성 속성만 해당

CFG_EPFW_MODE=	0 - 자동(기본값) 1 - 대화형 2 - 정책 기반 3 - 학습	방화벽 필터링 모드
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Unix 타임스탬프에 따른 학습 모드의 종료 날짜

LiveGrid® 속성

CFG_LIVEGRID_ENABLED를 사용하여 ESET Endpoint Security을(를) 설치하는 경우, 설치 후 제품 동작은 다음과 같습니다.

기능	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ESET LiveGrid® 평판 시스템	켜기	켜기
ESET LiveGrid® 피드백 시스템	끄기	켜기
익명 통계 전송	끄기	켜기

ACTIVATION_DATA 속성

형식	방법
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	ESET 라이선스 키를 사용하여 활성화(인터넷 연결이 활성화되어 있어야 함)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	오프라인 라이선스 파일을 사용하여 활성화

언어 속성

ESET Endpoint Security 언어(두 속성을 모두 지정해야 함)

속성	값
PRODUCT_LANG=	LCID 십진수(로캘 ID), 예: 영어(미국)의 경우 1033입니다. 언어 코드 목록을 참조하십시오.
PRODUCT_LANG_CODE=	소문자의 LCID 문자열(언어 문화 이름), 예: 영어-미국의 경우 en-us. 언어 코드 목록을 참조하십시오.

다시 시작 속성

설치 후 컴퓨터를 다시 시작하려면 다음 파라미터를 지정합니다.

속성	값	기능
REBOOT_WHEN_NEEDED=	0 - 비활성화됨 1 - 활성화됨	활성화된 경우 설치 후 컴퓨터가 다시 시작됩니다.
REBOOT_CANCELABLE=	0 - 비활성화됨 1 - 활성화됨	활성화된 경우 사용자가 컴퓨터 다시 시작을 취소할 수 있습니다.
REBOOT_POSTPONE=	값(초)	사용자가 컴퓨터 다시 시작을 연기하는 데 걸리는 최대 시간(초)입니다.

REBOOT_WHEN_NEEDED가 활성화된 경우에만 REBOOT_CANCELABLE 및 REBOOT_POSTPONE을 사용할 수 있습니다.

명령줄 설치 예

최종 사용자 사용권 계약을 읽어 보고 설치를 실행하기 전에 관리자 권한을 보유하고 있는지 확인하십시오.

설치에서 **NetworkProtection** 섹션 제외(하위 기능도 모두 지정해야 함):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

설치 후 ESET Endpoint Security을(를) 자동으로 구성되도록 하려면 설치 명령 내에서 기본 구성 파라미터를 지정해야 합니다.
ESET LiveGrid®가 활성화된 ESET Endpoint Security 설치:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

기본값 외에 다른 애플리케이션 설치 디렉터리를 설치합니다.
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

ESET 라이선스 키를 사용하여 ESET Endpoint Security을(를) 설치 및 활성화합니다.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

상세 로깅이 포함된 자동 설치(문제 해결 시 유용), 필수 구성 요소만 포함된 RMM:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

특정 언어를 사용하여 전체 자동 설치를 강제 적용합니다.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

설치 이후 명령줄 옵션

- ESET CMD – .xml 구성 파일 가져오기 또는 보안 기능 켜기/끄기
- 명령줄 검사기 – 명령줄에서 컴퓨터 검사 실행

GPO 또는 SCCM을 사용한 배포

클라이언트 워크스테이션에 ESET Endpoint Security을(를) 직접 설치하는 방법 외에, GPO(그룹 정책 개체), SCCM(Software Center Configuration Manager), Symantec Altiris 또는 Puppet 등의 관리 도구를 사용하여 설치

할 수도 있습니다.

관리됨(권장)

관리되는 컴퓨터의 경우 먼저 ESET Management 에이전트를 설치한 다음, ESET PROTECT를 통해 ESET Endpoint Security을(를) 설치합니다. ESET PROTECT가 네트워크에 설치되어 있어야 합니다.

1. ESET Management 에이전트용 독립 실행형 설치 관리자를 다운로드합니다.
2. GPO/SCCM 원격 배포 스크립트를 준비합니다.
3. GPO 또는 SCCM을 사용하여 ESET Management 에이전트를 배포합니다.
4. 클라이언트 컴퓨터가 ESET PROTECT에 추가되었는지 확인합니다.
5. 클라이언트 컴퓨터에 ESET Endpoint Security을(를) 배포 및 활성화합니다.

다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- SCCM 또는 GPO를 통해 ESET Management Agent 배포
- GPO(그룹 정책 개체)를 사용하여 ESET Management Agent 배포

등록 취소됨

관리되지 않는 컴퓨터의 경우 클라이언트 워크스테이션에 직접 ESET Endpoint Security을(를) 배포할 수 있습니다. 워크스테이션의 모든 ESET 엔드포인트 제품에 대한 정책을 모니터링하고 적용할 수 없으므로 권장되지는 않습니다.

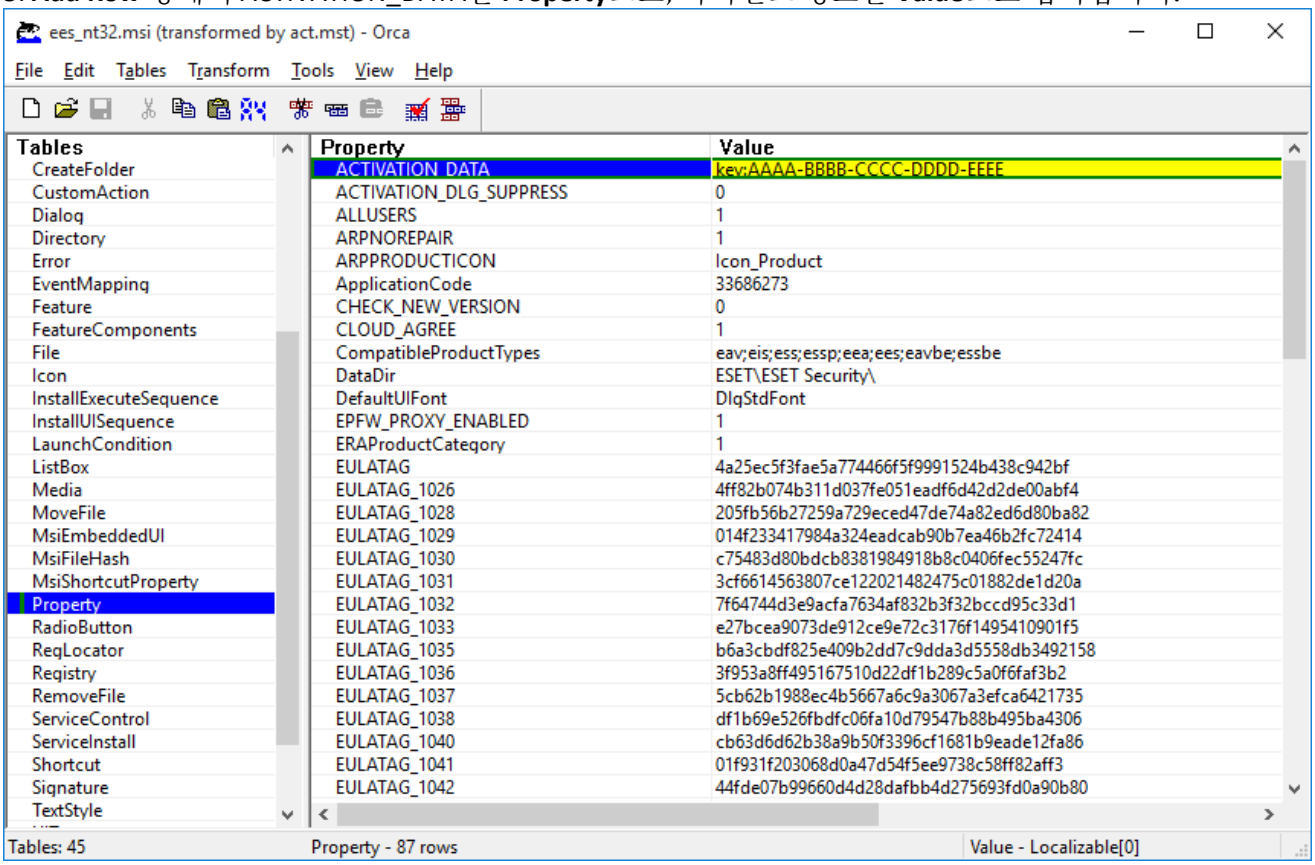
기본적으로 ESET Endpoint Security이(가) 설치 후 활성화되지 않아 작동되지 않습니다.

옵션 1(소프트웨어 설치)

1. ESET Endpoint Security용 .msi 설치 관리자를 다운로드합니다.
2. 제품 활성화 속성을 포함하도록 .msi 파일에서 .mst 변환 패키지를 생성(예: Orca .msi 편집기 사용)합니다(명령줄 설치에서 `ACTIVATION_DATA` 참조).

Orca에서 .mst를 생성하기 위한 단계 표시

1. 열기 Orca
2. **File** > **Open**를 클릭하여 .msi 설치 관리자를 로드합니다.
3. **Transform** > **New Transform**을 클릭합니다.
4. **Tables** 섹션에서 **Property**을 클릭한 다음 **Tables** 메뉴에서 > **Add row**를 클릭합니다.
5. **Add Row** 창에서 ACTIVATION_DATA를 **Property**으로, 라이선스 정보를 **Value**으로 입력합니다.



6. **변환** > **변환 생성**을 클릭하여 .mst 파일을 저장합니다.

1. 옵션: 사용자 지정된 ESET Endpoint Security .xml 구성 파일을 가져오려면(예: RMM을 활성화하거나 프록시 서버 설정을 구성하려면), cfg.xml 파일을 .msi 설치 관리자와 동일한 위치에 넣습니다.
2. GPO(소프트웨어 설치 사용) 또는 SCCM을 이용해 원격으로 .mst 파일을 사용하여 .msi 설치 관리자를 배포합니다.

옵션2(예약된 작업 사용)

1. ESET Endpoint Security용 .msi 설치 관리자를 다운로드합니다.
2. 제품 활성화 속성을 포함하도록 명령줄 설치를 준비합니다(ACTIVATION_DATA 참조).
3. 모든 워크스테이션용 네트워크에서 접근할 수 있는 .msi 설치 관리자와 .cmd 스크립트를 만듭니다.
4. 옵션: 사용자 지정된 ESET Endpoint Security .xml 구성 파일을 가져오려면(예: RMM을 활성화하거나 프록시 서버 설정을 구성하려면), cfg.xml 파일을 .msi 설치 관리자와 동일한 위치에 넣습니다.
5. GPO 또는 SCCM 중 하나를 사용하여 준비된 명령줄 설치 스크립트를 적용합니다.

    - GPO의 경우 그룹 정책 기본 설정 > 그룹 정책 예약 작업 > 즉시 실행 작업을 사용합니다.

ESET PROTECT을(를) 사용하여 ESET 엔드포인트 제품을 원격으로 관리하지 않으려는 경우, ESET Endpoint Security에 RMM용 ESET 플러그인을 포함하여 관리 서비스 공급업체에서 접근 가능한 로컬에 설치된 에이전트로 소프트웨어 시스템을 감독 및 제어할 수 있습니다. 자세한 정보 찾기

최신 버전으로 업그레이드

ESET Endpoint Security 최신 버전이 발표되어 제품을 개선하거나 프로그램 모듈의 자동 업데이트로 해결할 수 없는 문제를 해결할 수 있습니다.

최신 버전으로 업그레이드하는 것은 다음과 같은 여러 가지 방법으로 수행할 수 있습니다.

1. ESET PROTECT, 또는 ESET PROTECT Cloud을(를) 사용하여 자동으로
2. 자동으로 GPO 또는 SCCM 사용.
3. 프로그램 업데이트를 사용하여 자동으로.
   프로그램 업그레이드는 모든 사용자에게 배포되고 특정 시스템 구성에 영향을 미칠 수 있으므로 가능한 모든 시스템 구성에서 원활하게 작동되는지 오랜 시간 동안 테스트를 거친 후 발표됩니다. 최신 제품이 발표된 직후 최신 버전으로 업그레이드해야 하는 경우 다음 방법 중 하나를 사용합니다.
   고급 설정 > 업데이트 > **프로필** > **제품 업데이트**에서 **업데이트 모드**를 활성화했는지 확인하십시오..
4. 최신 버전을 다운로드한 후 이전 버전 위에 설치하는 방식을 통해 수동으로

권장 업그레이드 시나리오

ESET 제품을 원격으로 관리 또는 관리하려고 함

10개 이상의 ESET Endpoint 제품을 관리하는 경우 ESET PROTECT 또는 ESET PROTECT Cloud를 사용하여 업그레이드를 관리하는 것이 좋습니다. 다음 문서를 참조하십시오.

- ESET PROTECT | 클라이언트 작업을 통해 ESET 소프트웨어 업그레이드
- ESET PROTECT | 최대 250개의 Windows ESET 엔드포인트 제품을 관리하는 중소기업용 가이드
- ESET PROTECT Cloud 소개

클라이언트 워크스테이션에서 수동으로 업그레이드

개별 클라이언트 워크스테이션에서 수동으로 ESET Endpoint Security을(를) 업그레이드하려면:

1. 현재 설치한 버전이 지원되는지 확인합니다.
2. 사용하는 운영 체제가 지원되는지 확인합니다.

2. 최신 버전을 다운로드한 후 이전 버전 위에 설치합니다.

지원 수준이 "수명 종료"인 버전의 경우 이전 버전에 대한 최신 버전의 성공적인 설치가 보장되지 않습니다. 수명 종료 정책을 참조하여 ESET Endpoint Security 지원 수준을 검토합니다.
지원되지 않는 버전에서 업그레이드하려면 ESET Endpoint Security을(를) 먼저 제거하십시오. 클라이언트 워크스테이션에서 ESET Endpoint Security을(를) 업그레이드하는 방법에 대한 자세한 내용은 다음 ESET 지식베이스 문서를 읽어보십시오.

레거시 제품 자동 업그레이드

사용 중인 ESET 제품 버전은 더 이상 지원되지 않으며 해당 제품이 최신 버전으로 업그레이드되었습니다.

일반적인 설치 문제

각각의 새로운 ESET 제품 버전은 다양한 버그 수정 및 개선 사항을 갖추고 있습니다. ESET 제품에 유효한 라이선스를 보유한 기존 고객은 동일한 제품의 최신 버전으로 무료 업그레이드할 수 있습니다.

설치를 완료하려면 다음을 수행합니다.

1. **동의 후 계속**을 클릭하여 최종 사용자 사용권 계약에 동의하고 개인 정보 보호 정책을 승인합니다. 최종 사용자 사용권 계약에 동의하지 않는 경우 **제거**를 클릭합니다. 이전 버전으로 되돌릴 수 없습니다.
2. ESET LiveGrid® 피드백 시스템을 허용하려면 **모두 허용 후 계속**을 클릭하고, 참여하지 않으려면 **계속**을 클릭합니다.
3. 라이선스 키로 새 ESET 제품을 활성화하면 홈 페이지가 표시됩니다. 라이선스 정보를 찾을 수 없는 경우 새 평가판 라이선스를 계속 사용하십시오. 이전 제품에 사용된 라이선스가 유효하지 않은 경우 ESET 제품을 활성화합니다.
4. 설치를 완료하려면 장치를 다시 시작해야 합니다.

보안 및 안정성 업데이트

ESET Endpoint Security 업데이트는 악성 코드에 대해 완전한 보호를 유지하는 데 필수적인 부분입니다. ESET Endpoint Security의 각 새로운 버전에는 많은 개선 사항 및 버그 수정이 포함됩니다. 보안 취약점 및 위협으로부터 보호하기 위해서는 ESET Endpoint Security 제품을 정기적으로 업데이트하는 것이 좋습니다. ESET Endpoint Security 제품은 다른 ESET 제품처럼 제품 수명 주기의 특정 단계에 적합합니다.

다음에 대한 자세한 내용 읽기:
지원 종료 정책(비즈니스 제품)
제품 업데이트
보안 및 안정성 핫픽스
ESET Endpoint Security 변경 사항에 대한 추가 정보는 다음 ESET 지식베이스 문서를 읽어보십시오.

자동 업데이트는 제품의 최대 보안 성능과 안정성을 보장합니다. 보안 및 안정성 업데이트를 비활성화할 수는 없습니다.

제품 활성화

설치가 완료되면 제품을 활성화할 것인지 묻는 메시지가 표시됩니다.

제품을 활성화하는 방법에는 몇 가지가 있습니다. 제품 활성화 창의 특정 제품 활성화 시나리오 사용 가능 여부는 국가 및 배포 방법(ESET 웹 페이지, 설치 관리자 유형 .msi 또는 .exe 등)에 따라 달라질 수 있습니다.

기본 프로그램 창 > **도움말 및 지원** > **제품 활성화** 또는 **보호 상태** > **제품 활성화**에서 ESET Endpoint Security을(를) 활성화할 수 있습니다.

다음 방법 중 하나를 사용하여 ESET Endpoint Security를 활성화할 수 있습니다.

- **구입한 라이선스 키 사용** - 라이선스 소유자 식별과 라이선스 활성화에 사용되는, XXXX-XXXX-XXXX-XXXX-XXXX 형식의 고유한 문자열입니다.
- **ESET HUB** - 생성해야 하는 ESET HUB 계정입니다. ESET HUB는 ESET PROTECT 통합 보안 플랫폼의 중앙 게이트웨이입니다. 모든 ESET 플랫폼 모듈에 대한 중앙 집중식 ID, 구독 및 사용자 관리를 제공합니다. 이 옵션을 사용하여 ESET Endpoint Security을(를) 활성화할 수 있으며, 이전 라이선스 관리 도구(ESET Business Account 또는 ESET MSP Administrator)를 사용할 수도 있습니다.

- **오프라인 라이선스** - 라이선스 정보를 제공하기 위해 ESET 제품으로 전송되는, 자동으로 생성된 파일입니다. 라이선스를 사용하여 오프라인 활성화를 수행하는 데 사용할 수 있는 파일인 오프라인 라이선스 파일(.lf)을 다운로드할 수 있습니다. 오프라인 라이선스 수를 사용 가능한 총 라이선스 수에서 뺍니다. 오프라인 파일을 생성하는 방법에 대한 자세한 내용은 ESET Business Account 사용자 설명서를 참조하십시오.

컴퓨터가 관리되는 네트워크의 구성원일 경우 **나중에 활성화**를 클릭합니다. 관리자가 ESET PROTECT를 통해 원격 활성화를 수행합니다. 나중에 이 클라이언트를 활성화하려는 경우에도 이 옵션을 사용할 수 있습니다.

이전 ESET 제품의 활성화에 사용되는 사용자 이름과 패스워드가 있는 경우, 레거시 자격 증명을 라이선스 키로 변환하십시오.

기본 프로그램 창 > **도움말 및 지원** > **라이선스 변경**에서 언제든지 제품 라이선스를 변경할 수 있습니다. ESET 지원에 라이선스를 식별하는 데 사용되는 공개 라이선스 ID가 표시됩니다.

ESET PROTECT는 관리자가 사용할 수 있는 라이선스를 이용해 클라이언트 컴퓨터를 자동으로 활성화할 수 있습니다. ESET PROTECT 온라인 도움말에서 지침을 참조하십시오.

제품을 활성화하지 못하셨습니까?

활성화 중 라이선스 키 입력

자동 업데이트는 보안에 있어 중요한 요소입니다. ESET Endpoint Security은(는) **라이선스 키**를 사용하여 활성화된 업데이트만 받습니다.

설치 후 라이선스 키를 입력하지 않았다면 제품이 활성화되지 않습니다. 기본 프로그램 창에서 라이선스를 변경할 수 있습니다. 이렇게 하려면 **도움말 및 지원** > **라이선스 활성화**를 차례로 클릭하고 ESET 보안 제품과 함께 받은 라이선스 데이터를 제품 활성화 창에 입력합니다.

라이선스 키 입력 시 작성된 그대로 입력해야 합니다:

- 라이선스 키는 XXXX-XXXX-XXXX-XXXX-XXXX 형식의 고유한 문자열로, 라이선스 소유자 식별과 라이선스 활성화에 사용됩니다.

정확성을 위해 등록 이메일의 라이선스 키를 복사하여 붙여넣는 것이 좋습니다.

ESET HUB 계정

ESET HUB는 ESET PROTECT 통합 보안 플랫폼의 중앙 게이트웨이입니다. 모든 ESET 플랫폼 모듈에 대한 중앙 집중식 ID, 구독 및 사용자 관리를 제공합니다. ESET HUB를 사용하여 다음을 수행할 수 있습니다.

- 보안 구독 개요 보기
- 가입한 서비스 사용 현황 및 상태 확인
- 개별 ESET 플랫폼에 대한 세분화된 접근 권한 할당 및 제어
- 연결되고 접근 가능한 모든 ESET 플랫폼에 대한 단일 로그인

이 활성화 옵션을 사용하여 ESET Endpoint Security을(를) 활성화할 수 있으며, 이전 라이선스 관리 도구(ESET Business Account 또는 ESET MSP Administrator)를 사용할 수도 있습니다.

ESET HUB 계정을 생성하고 **이메일 주소**와 **패스워드**로 로그인할 수 있습니다.

패스워드를 잊어버린 경우 **패스워드를 잊어버림**을 클릭하면 ESET HUB로 리디렉션됩니다. 이메일 주소를 입력하고 **로그인**을 클릭하여 확인합니다. 그러고 나면 패스워드를 재설정하는 방법이 설명된 메시지를 받게 됩니다.

레거시 라이선스 자격 증명을 사용하여 ESET 엔드포인트 제품을 활성화하는 방법

이미 사용자 이름 및 비밀번호를 가지고 있는 경우 라이선스 키를 받으려면 자격 증명을 새 라이선스 키로 변환할 수 있는 ESET Business Account 포털을 방문하십시오.

제품 활성화 실패

ESET Endpoint Security 활성화에 성공하지 못하는 경우 가장 일반적인 시나리오는 다음과 같습니다.

- 라이선스 키가 이미 사용 중인 경우.
- 잘못된 라이선스 키를 입력했습니다.
- 활성화 양식의 정보가 없거나 올바르지 않습니다.
- 활성화 서버와의 통신에 실패했습니다.
- ESET 활성화 서버에 대한 연결이 없거나 비활성화되었습니다.

올바른 라이선스 키를 입력했거나 오프라인 라이선스를 연결했는지 확인하고 다시 활성화를 시도하십시오.

활성화할 수 없는 경우 시작 패키지에서 활성화 및 라이선스에 대한 일반적인 질문과 오류, 문제를 설명합니다(영어 및 기타 여러 언어로 제공).

- ESET 제품 활성화 문제 해결 시작

등록

등록 양식에 포함된 필드에 기재하고 **계속**을 클릭하여 라이선스를 등록하십시오. 괄호에 필수로 표시된 필드는 필수 항목입니다. 이 정보는 ESET 라이선스 관련 작업에만 사용됩니다.

활성화 진행률

ESET Endpoint Security을(를) 활성화 중입니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

제품 활성화 완료

활성화에 성공했으며, 이제 ESET Endpoint Security가 활성화되었습니다. 이제부터 ESET Endpoint Security는 정기 업데이트를 받아 최신 위협을 식별하고 컴퓨터를 안전하게 유지합니다. **완료**를 클릭하여 제품 활성화를 마칩니다.

일반적인 설치 문제

설치 중에 문제가 발생하면 가능한 경우 설치 마법사가 문제를 해결하는 문제 해결사를 제공합니다.

문제 해결사 실행을 클릭하여 문제 해결사를 시작합니다. 문제 해결사가 완료되면 권장 솔루션을 따르십시오.

문제가 지속되면 일반적인 설치 오류 및 해결 방법 목록을 참조하십시오.

초보자용 설명서

이 장에서는 ESET Endpoint Security의 초기 개요 및 해당 기본 설정에 대해 설명합니다.

시스템 트레이 아이콘

가장 중요한 몇 가지 설정 옵션 및 기능은 시스템 트레이 아이콘을 오른쪽 마우스 버튼으로 클릭하여 사용할 수 있습니다.

> 시스템 트레이(Windows 알림 영역) 아이콘 메뉴에 접근하려면 사용자 인터페이스 요소의 시작 모드가 전체로 설정되어 있는지 확인합니다.

보호 일시 중지 – 파일, 웹 및 이메일통신을 제어하여 공격으로부터 보호하는 검색 엔진을 비활성화하는 확인 대화 상자를 표시합니다. **시간 간격** 드롭다운 메뉴를 사용하면 보호를 비활성화할 기간을 지정할 수 있습니다.

방화벽 일시 중지(모든 트래픽 허용) - 방화벽을 비활성 상태로 전환합니다. 자세한 내용은 네트워크를 참조하십시오.

모든 네트워크 트래픽 차단 - 모든 네트워크 트래픽을 차단합니다. **모든 네트워크 트래픽 차단 중지**를 클릭하여 다시 활성화할 수 있습니다.

고급 설정 – ESET Endpoint Security 고급 설정을 엽니다. 기본 프로그램 창에서 고급 설정을 열려면 키보드에서 F5 키를 누르거나 **설정 > 고급 설정**을 클릭합니다.

로그 파일 - 로그 파일은 발생한 중요 프로그램 이벤트에 대한 정보를 포함하고 있으며 검색에 대한 개요를 제공합니다.

ESET Endpoint Security 열기 – 트레이(Windows 알림 영역) 아이콘에서 ESET Endpoint Security 기본 프로그램 창을 엽니다.

창 레이아웃 다시 설정 - ESET Endpoint Security의 창을 기본 크기로 다시 설정하고 화면에서의 위치를 다시 설정합니다.

색상 모드—GUI의 색상을 변경할 수 있는 사용자 인터페이스 설정을 엽니다.

업데이트 확인 – 사용자를 보호하기 위해 모듈 또는 제품 업데이트를 시작합니다. ESET Endpoint Security에서는 하루에 여러 번 업데이트를 자동으로 확인합니다.

정보 - 시스템 정보, 설치된 ESET Endpoint Security 버전에 대한 세부 정보, 설치된 프로그램 모듈 및 운영 체제 및 시스템 리소스에 대한 정보를 제공합니다.

키보드 바로 가기

ESET Endpoint Security에서 더 원활히 탐색하려면 다음과 같은 키보드 단축키를 사용하면 됩니다.

키보드 단축키	동작
F1	도움말 페이지 열기
F5	고급 설정 열기
위쪽 화살표/아래쪽 화살표	드롭다운 메뉴 항목 탐색
TAB	창에서 다음 GUI 요소로 이동
Shift+TAB	창에서 이전 GUI 요소로 이동
ESC	활성 대화 상자 창 닫기
Ctrl+U	ESET 라이선스 및 컴퓨터에 대한 정보(기술 지원 정보) 표시
Ctrl+R	화면에서 기본 크기 및 위치로 제품 창 다시 설정
ALT + 왼쪽 화살표	뒤로 탐색
ALT + 오른쪽 화살표	앞으로 탐색
ALT+Home	홈 탐색

탐색 시 마우스 버튼을 뒤로 또는 앞으로 사용할 수도 있습니다.

프로필

프로필 관리자는 ESET Endpoint Security 내에서 두 군데, 즉 **수동 검사** 섹션과 **업데이트** 섹션에서 사용됩니다.

컴퓨터 검사

ESET Endpoint Security에는 4개의 미리 정의된 검사 프로필이 있습니다.

- **스마트 검사** - 기본 고급 검사 프로필입니다. 스마트 검사 프로필은 이전 검사에서 깨끗한 것으로 확인되었고 검사 이후 수정되지 않은 파일을 제외하는 스마트 최적화 기술을 사용합니다. 이를 통해 시스템 보안에 최소한의 영향을 미치면서 검사 시간을 단축할 수 있습니다.
- **오른쪽 마우스 버튼 메뉴 검사** - 오른쪽 마우스 버튼 메뉴에서 모든 파일의 수동 검사를 시작할 수 있습니다. 오른쪽 마우스 버튼 메뉴 검사 프로필을 사용하면 이 방법으로 검사를 트리거할 때 사용할 검사 구성을 정의할 수 있습니다.
- **상세 검사** - 상세 검사 프로필은 기본적으로 스마트 최적화를 사용하지 않으므로 이 프로필을 사용하여 검사에서 파일이 제외되지 않습니다.
- **컴퓨터 검사** - 표준 컴퓨터 검사에 사용되는 기본 프로필입니다.

향후 검사를 위해 기본 설정 검사 파라미터를 저장할 수 있습니다. 정기적으로 사용되는 각 검사에 대해 서로 다른 프로필(다양한 검사 대상, 검사 방법 및 기타 파라미터 포함)을 생성하는 것이 좋습니다.

새 프로필을 생성하려면 고급 설정 > **탐지 엔진** > **악성코드 검사** > **수동 검사** > **프로필 목록** > **편집**을 엽니다. **프로필 관리자** 창에는 새 프로필을 생성할 수 있는 옵션 및 기존 검사 프로필이 있는 **선택한 프로필** 드롭다

운 메뉴가 포함되어 있습니다. 필요에 맞게 검사 프로필을 생성하는 데 도움을 받으려면 ThreatSense에서 검사 설정의 각 파라미터에 대한 설명을 참조하십시오.

고유한 검사 프로필을 생성하려는데 **컴퓨터 검사** 구성이 부분적으로 적합하지만 런타임 패커나 잠재적으로 안전하지 않은 애플리케이션은 검사하고 싶지 않고 **항상 탐지 수정**도 적용하고자 한다고 가정합니다. **프로필 관리자** 창에서 새 프로필의 이름을 입력하고 **추가**를 클릭합니다. **선택한 프로필** 드롭다운 메뉴에서 새 프로필을 선택하고 요구 사항을 충족하도록 나머지 파라미터를 조정한 다음 **확인**을 클릭하여 새 프로필을 저장합니다.

업데이트

업데이트 설정의 프로필 편집기를 사용하여 새로운 업데이트 프로필을 생성할 수 있습니다. 컴퓨터에서 여러 가지 방법으로 업데이트 서버에 연결하는 경우에만 사용자 지정 프로필(기본 **내 프로필** 이외 프로필)을 생성하여 사용합니다.

예로 랩톱을 들 수 있습니다. 랩톱은 일반적으로 로컬 네트워크를 통해 로컬 서버(미러)에 연결하지만, 출장으로 인해 로컬 네트워크와 연결이 끊기는 경우 ESET 업데이트 서버에서 직접 업데이트를 다운로드하며 로컬 서버에 연결하는 프로필과 ESET 서버에 연결하는 또 다른. 이러한 프로필이 구성되면 **도구 > 스케줄러**로 이동한 후 업데이트 작업 파라미터를 편집합니다. 하나의 프로필을 기본 프로필로 지정하고 다른 하나를 보조 프로필로 지정합니다.

업데이트 프로필 - 현재 사용 중인 프로필 업데이트입니다. 프로필을 변경하려면 드롭다운 메뉴에서 프로필을 선택합니다.

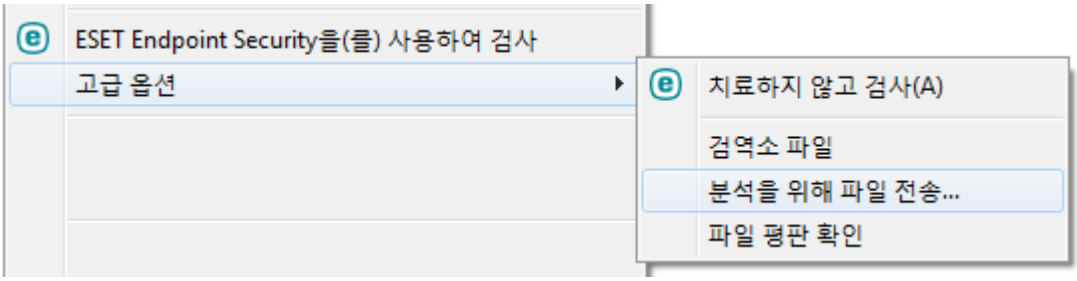
프로필 목록 - 새 업데이트 프로필을 생성하거나 기존의 업데이트 프로필을 제거합니다.

오른쪽 마우스 버튼 메뉴

개체(파일)를 오른쪽 마우스 버튼으로 클릭하면 오른쪽 마우스 버튼 메뉴가 표시됩니다. 메뉴에는 개체에 대해 수행할 수 있는 모든 동작이 나열됩니다.

ESET Endpoint Security 제어 요소를 오른쪽 마우스 버튼 메뉴에 통합할 수 있습니다. 이 기능의 설정 옵션은 고급 설정 > **사용자 인터페이스 > 사용자 인터페이스 요소**에서 사용할 수 있습니다.

오른쪽 마우스 버튼 메뉴로 통합 - ESET Endpoint Security 제어 요소를 오른쪽 마우스 버튼 메뉴로 통합합니다.



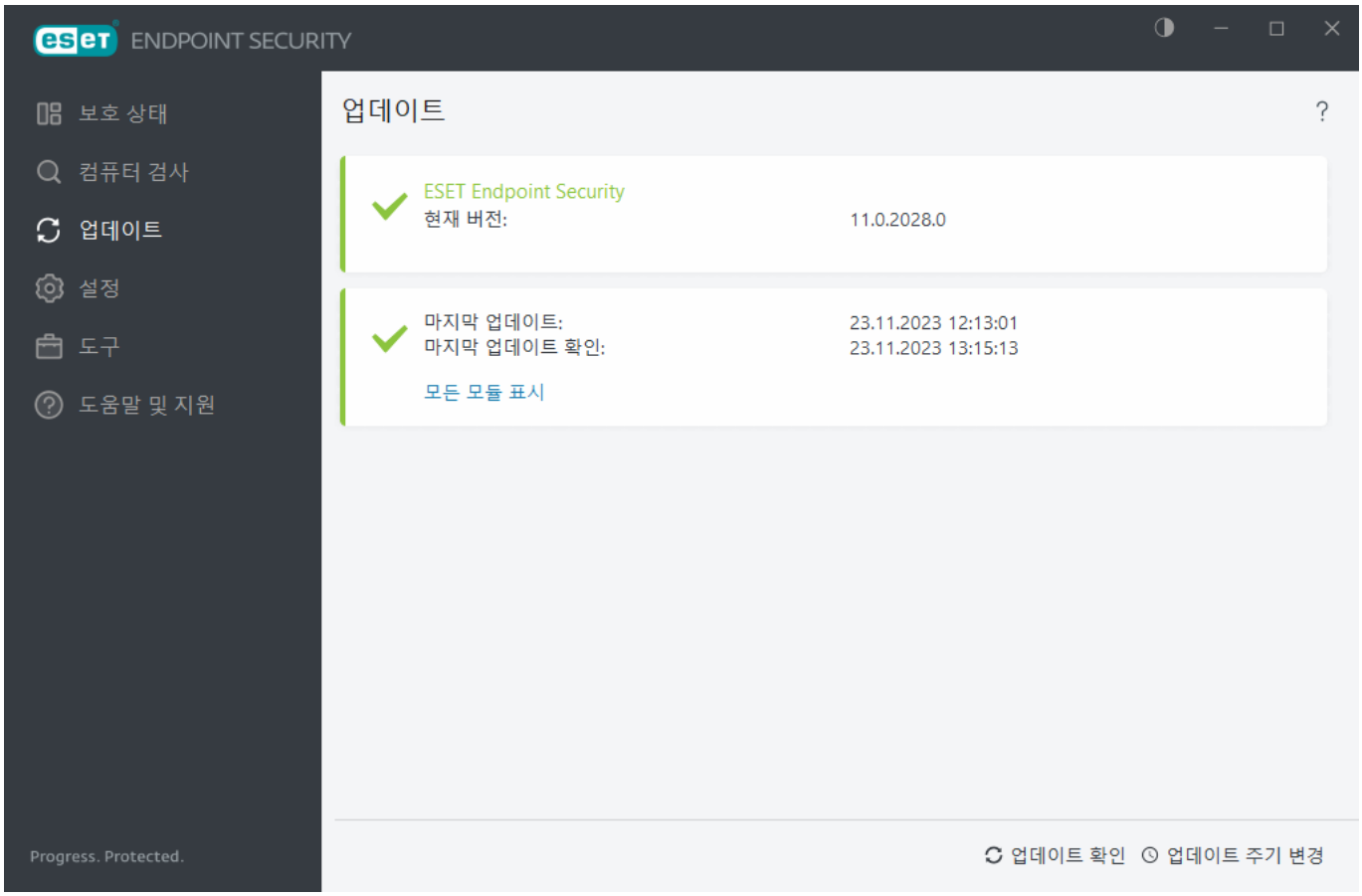
업데이트 설정

컴퓨터에 최대의 보안을 제공하는 가장 좋은 방법은 ESET Endpoint Security을(를) 정기적으로 업데이트하는 것입니다. 업데이트 모듈을 통해 프로그램 모듈과 시스템 구성 요소를 항상 최신 상태로 유지할 수 있습니

다.

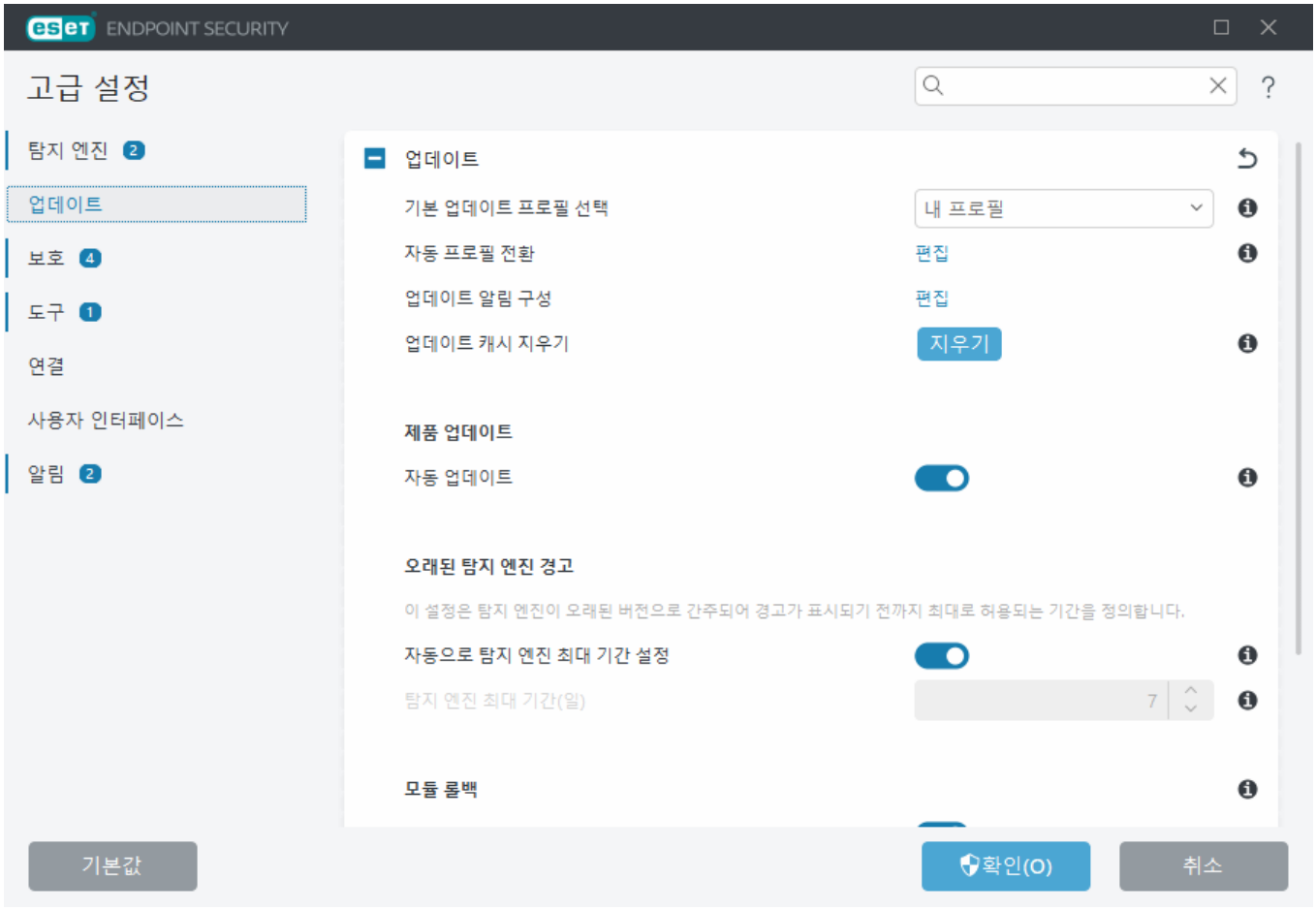
기본 프로그램 창에서 **업데이트**를 클릭하면 마지막으로 성공한 업데이트 날짜 및 시간, 업데이트가 필요한지 여부 등 현재 업데이트 상태를 확인할 수 있습니다.

자동 업데이트 외에도 **업데이트 확인**을 클릭하여 수동 업데이트를 트리거할 수 있습니다.



고급 설정 > **업데이트**에는 업데이트 모드, 프록시 서버 접근 및 LAN 연결과 같은 추가 업데이트 옵션이 포함되어 있습니다.

업데이트에 문제가 발생하는 경우 **지우기**를 클릭하여 업데이트 캐시를 지웁니다. 그래도 프로그램 모듈을 업데이트할 수 없는 경우 "모듈 업데이트 실패" 메시지에 대한 문제 해결 섹션을 참조하십시오.

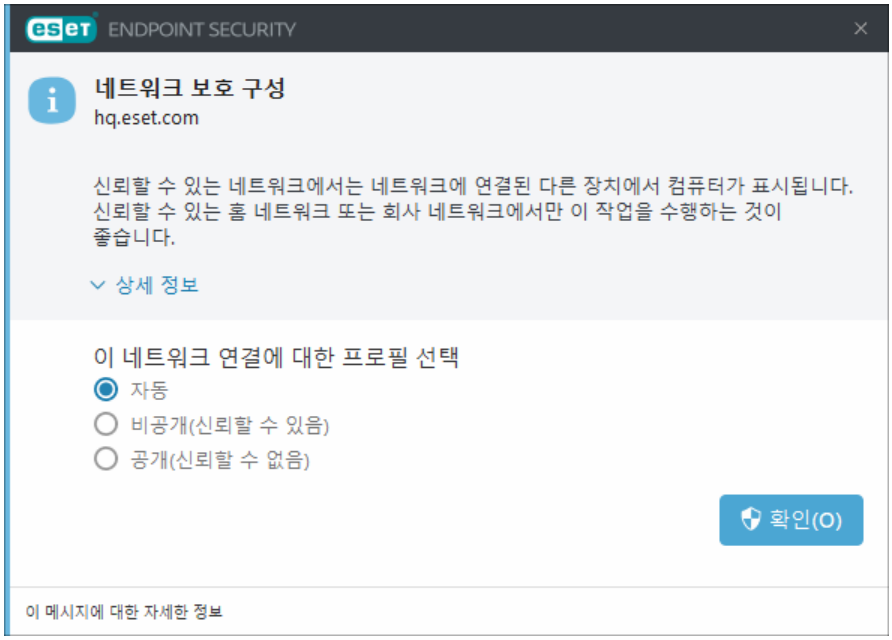


고급 설정 > **업데이트** > **프로필** > **업데이트** > **모듈 업데이트**의 **자동으로 선택** 옵션은 기본적으로 활성화되어 있습니다. 업데이트 수신에 ESET 업데이트 서버를 사용하는 경우에는 이 옵션 상태를 그대로 두는 것이 좋습니다.

최적의 기능을 위해서는 프로그램이 자동으로 업데이트되어야 합니다. 자동 업데이트는 **도움말 및 지원** > **제품 활성화**에 올바른 라이선스 키를 입력한 경우에만 실행됩니다. 설치 후 라이선스 키를 입력하지 않은 경우 언제든지 라이선스 키를 입력할 수 있습니다. 활성화에 대한 자세한 내용은 ESET Endpoint Security 을(를) 활성화하는 방법을 참조하십시오.

네트워크 보호 구성

기본적으로 새로운 네트워크 연결이 탐지되면 ESET Endpoint Security에서 Windows 설정을 사용합니다. 새 네트워크가 탐지될 때 대화 상자 창을 표시하려면 네트워크 보호 프로필 할당을 **확인**으로 변경합니다. 컴퓨터가 새로운 네트워크에 연결될 때마다 네트워크 보호 구성이 표시됩니다.



다음 네트워크 연결 프로필 중에서 선택할 수 있습니다.

자동 - 각 프로필에 구성된 활성화 도구에 따라 ESET Endpoint Security에서 프로필을 자동으로 선택합니다.

개인 – 신뢰할 수 있는 네트워크(홈 네트워크 또는 회사 네트워크). 컴퓨터에 저장된 공유 파일과 컴퓨터가 다른 네트워크 사용자에게 표시되며, 네트워크의 다른 사용자가 시스템 리소스에 접근할 수 있습니다(공유 파일 및 프린터에 대한 접근이 활성화되고 들어오는 RPC 통신이 활성화되며 원격 데스크톱 공유를 사용할 수 있음). 안전한 로컬 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성된 경우 네트워크 연결에 자동으로 할당됩니다.

공용 – 신뢰할 수 없는 네트워크(공용 네트워크). 시스템의 파일 및 폴더가 네트워크의 다른 사용자와 공유되거나 다른 사용자에게 표시되지 않으며, 시스템 리소스 공유가 비활성화됩니다. 무선 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성되지 않은 모든 네트워크 연결에 자동으로 할당됩니다.

사용자 정의 프로필 - 드롭다운 메뉴에서 생성한 프로필을 선택할 수 있습니다. 이 옵션은 사용자 지정 프로필을 하나 이상 생성한 경우에만 사용할 수 있습니다.

⚠ 네트워크를 잘못 구성하면 컴퓨터에 보안 위험을 유발할 수 있습니다.

웹 컨트롤 도구

ESET Endpoint Security에서 웹 컨트롤을 이미 활성화한 경우 웹 컨트롤이 제대로 작동하려면 원하는 사용자 계정에 대한 웹 컨트롤도 구성해야 합니다. 잠재적으로 부적절한 자료로부터 클라이언트 워크스테이션을 보호하기 위해 클라이언트 워크스테이션에 대한 특정 제한을 생성하는 방법과 관련된 지침을 확인하려면 웹 컨트롤 장을 참조하십시오.

차단된 해시

사용자 환경에서 ESET Inspect를 사용하면 관리자가 해시를 기반으로 지정된 실행 파일에 대한 접근을 차단할 수 있습니다. 관리자가 실행 파일에 대한 접근을 차단하고 사용자가 해당 파일에 접근하려고 하면 ESET

Endpoint Security에 다음 알림이 표시됩니다.

파일 접근 차단됨 - 관리자가 허용하지 않은 파일에 애플리케이션(애플리케이션 이름이 표시됨)이 접근하려고 했습니다.

관리자로서 알림에 명시된 애플리케이션에 대한 접근을 허용하려면 ESET Inspect 온라인 도움말의 차단된 해시를 참조하십시오. 애플리케이션의 동작을 변경하려는 사용자인 경우 관리자에게 문의하십시오.

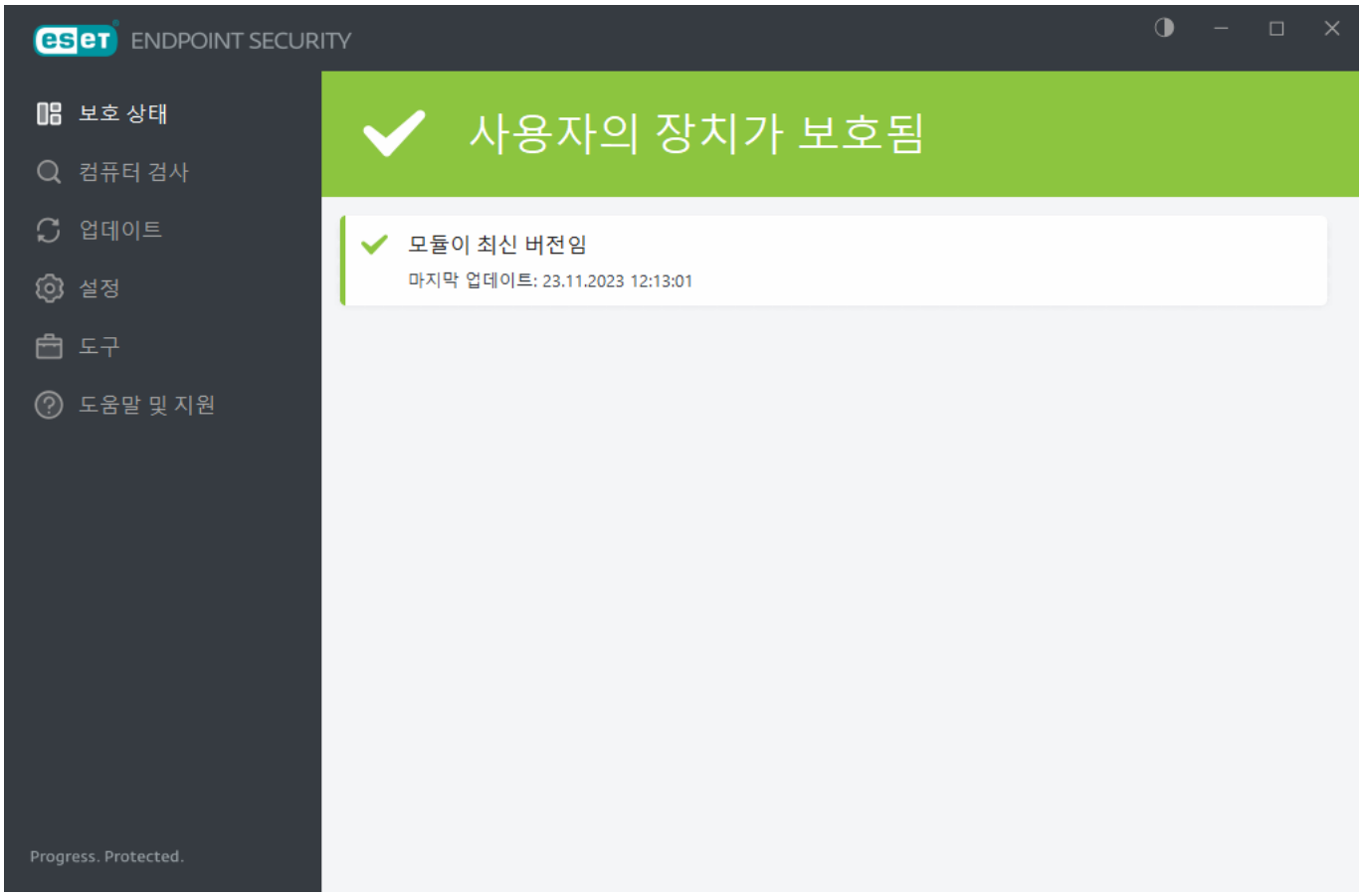
ESET Endpoint Security 운용

ESET Endpoint Security의 기본 프로그램 창은 두 섹션으로 나뉩니다. 오른쪽의 기본 창은 왼쪽의 기본 메뉴에서 선택한 옵션에 해당하는 정보를 표시합니다.

> **그림이 포함된 지침**
> 영어 및 기타 여러 언어로 제공되는 그림이 포함된 지침은 ESET Windows 제품의 기본 프로그램 창 열기를 참조하십시오.

기본 프로그램 창의 오른쪽 상단에서 ESET Endpoint Security GUI의 색 구성표를 선택할 수 있습니다. **최소화** 아이콘 옆에 있는 **색 구성표** 아이콘(아이콘은 현재 선택한 색 구성표에 따라 변경됨)을 클릭하고 드롭다운 메뉴에서 색 구성표를 선택합니다.

- **시스템 색상과 동일**—운영 체제 설정에 따라 ESET Endpoint Security의 색 구성표를 설정합니다.
- **어두운**—ESET Endpoint Security에서 어두운 색 구성표(어두운 모드)를 적용합니다.
- **밝은**—ESET Endpoint Security에서 표준적인 밝은 색 구성표를 적용합니다.



기본 메뉴 옵션:

보호 상태 - ESET Endpoint Security의 보호 상태에 대한 정보를 제공합니다.

컴퓨터 검사 - 컴퓨터 검사를 구성 및 시작하거나 사용자 지정 검사를 생성합니다.

업데이트 – 모듈 및 탐지 엔진 업데이트에 대한 정보를 표시합니다.

도구 - 기능(프로그램 관리를 단순화하고 고급 사용자를 위한 추가 옵션을 제공).

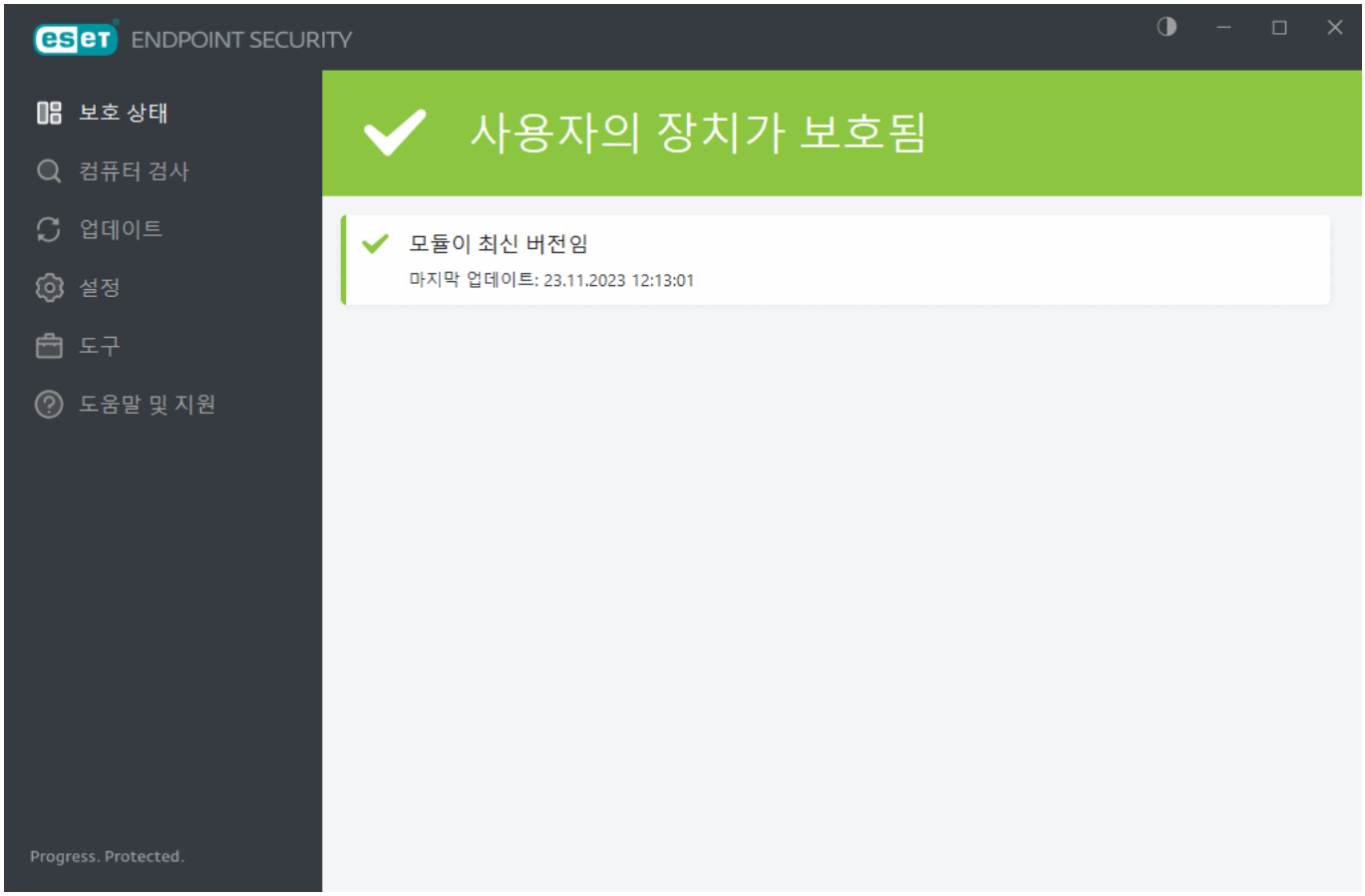
설정 - ESET Endpoint Security 보호 기능에 대한 구성 옵션 및 고급 설정에 대한 접근을 제공합니다.

도움말 및 지원 – 라이선스, 설치된 ESET 제품 및 온라인 도움말, ESET 지식베이스/기술 지원에 대한 링크를 표시합니다.

보호 상태

보호 상태 창에는 컴퓨터의 현재 보호 수준 및 마지막 업데이트에 대한 정보가 표시됩니다. 녹색 **최대 보호** 상태는 보호 수준이 최대임을 나타냅니다.

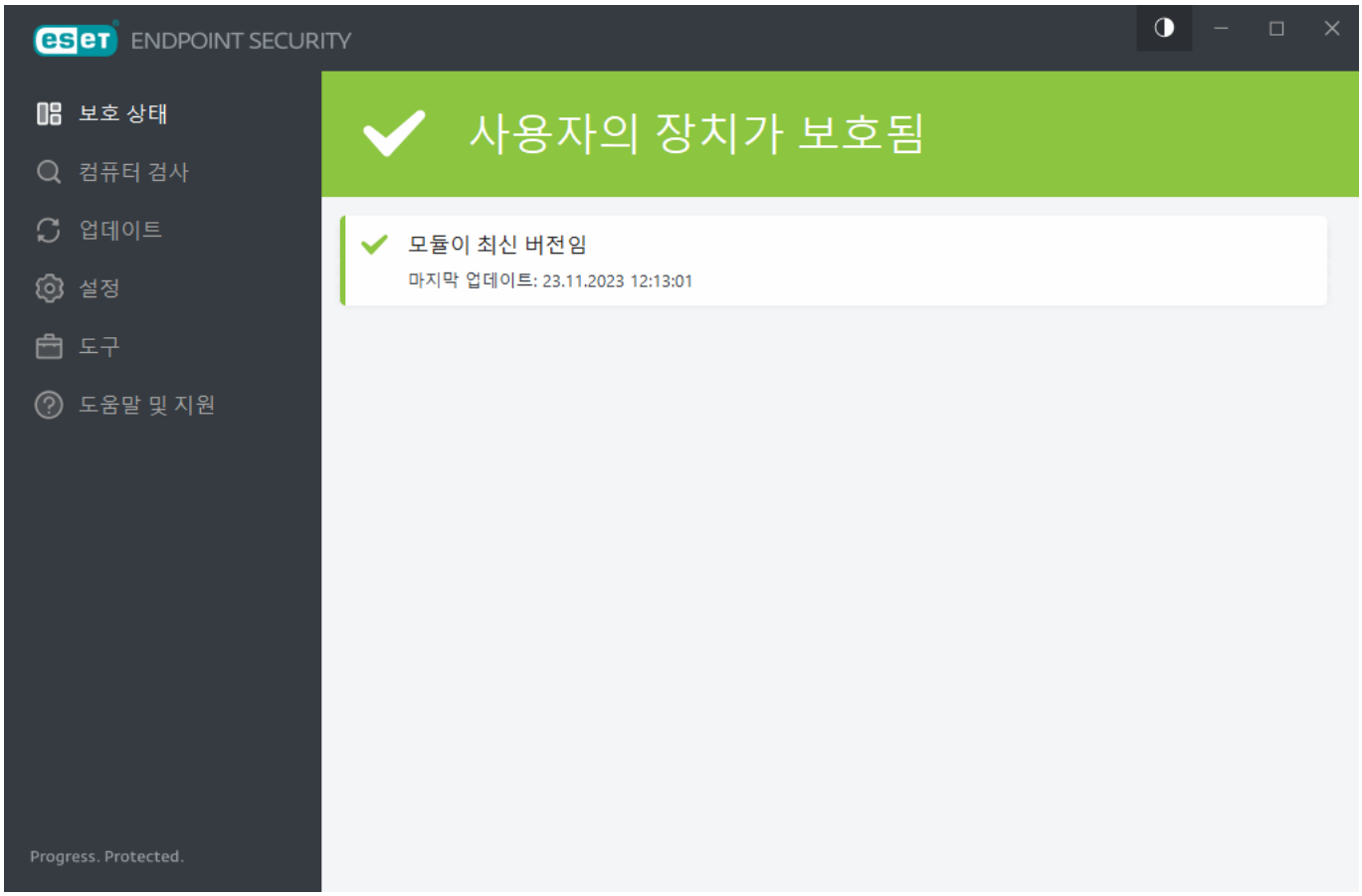
보호 상태 창에는 ESET Endpoint Security의 보안을 강화하거나 추가 기능을 켜거나 최대한의 보호를 보장하기 위한 자세한 정보와 권장 솔루션이 포함된 알림이 표시됩니다.



녹색 아이콘 및 녹색 **사용자의 장치가 보호됨** 상태는 최대 수준으로 보호됨을 나타냅니다.

프로그램이 제대로 작동하지 않는 경우 수행할 작업

녹색 확인 표시는 제대로 작동하고 있는 모든 프로그램 모듈 옆에 표시됩니다. 모듈에 주의가 필요한 경우에는 빨간색 느낌표나 주황색 알림 아이콘이 표시됩니다. 전체 기능을 복원하는 방법에 대한 ESET의 권장 사항을 비롯한, 모듈에 대한 추가 정보는 창의 상단에 표시됩니다. 모듈의 상태를 변경하려면 기본 메뉴에서 **설정**을 클릭한 다음 원하는 모듈을 클릭합니다.



빨간색 느낌표(!) 아이콘은 컴퓨터의 보호 수준이 최대가 아님을 나타냅니다. 다음 시나리오에서 이러한 알림 유형이 표시될 수 있습니다.

- **안티바이러스 및 안티스파이웨어 보호가 일시 중지됨** - **모든 안티바이러스, 안티스파이웨어 보호 모듈 시작**을 클릭하여 기본 프로그램 창의 **설정** 창에서 **안티바이러스, 안티스파이웨어 보호를 활성화**하거나 **보호 상태** 창에서 안티바이러스 및 안티스파이웨어 보호를 다시 활성화합니다.
- 안티바이러스 보호가 작동 안 함 - 바이러스 검사기를 초기화하지 못했습니다. 대부분의 ESET Endpoint Security 모듈이 제대로 작동하지 않습니다.
- **안티피싱 보호가 작동 안 함** - 다른 필수 프로그램 모듈이 활성 상태가 아니므로 이 기능이 작동하지 않습니다.
- **방화벽이 비활성화됨** - 이 문제는 빨간색 아이콘과 **네트워크** 항목 옆에 있는 보안 알림으로 표시됩니다. **필터링 모드 활성화**를 클릭하여 네트워크 보호를 다시 활성화합니다.
- **방화벽 초기화 실패** - 시스템 통합 문제로 인해 방화벽이 비활성화되었습니다. 최대한 빨리 컴퓨터를 다시 시작하십시오.
- **탐지 엔진이 오래된 버전임** – 탐지 엔진(이전 이름: 바이러스 지문 DB)을 업데이트하려는 시도에 여러 번 실패하면 이 오류가 나타납니다. 이 경우 업데이트 설정을 확인하는 것이 좋습니다. 이 오류가 발생하는 가장 일반적인 이유는 인증 데이터가 잘못 입력되거나, 연결 설정이 잘못 구성되었기 때문입니다.

- **제품이 활성화되지 않음** 또는 **라이선스가 만료됨** - 빨간색 보호 상태 아이콘으로 나타납니다. 라이선스가 만료되면 프로그램에서 업데이트를 수행할 수 없습니다. 라이선스를 갱신하려면 경고 창의 지침을 따르십시오.
- **HIPS(호스트 침입 방지 시스템)가 비활성화됨** - HIPS가 비활성화된 경우 이 문제가 표시됩니다. 컴퓨터가 일부 유형의 위협으로부터 보호되지 않으므로 **HIPS 활성화**를 클릭하여 즉시 보호를 다시 활성화해야 합니다.
- **예약된 정기적 업데이트 없음** - 업데이트 작업을 예약하지 않으면 ESET Endpoint Security에서 중요 업데이트를 확인하지 않거나 수신하지 않습니다.
- **네트워크 접근이 차단됨** – ESET PROTECT에서 이 워크스테이션의 **네트워크에서 컴퓨터 격리** 클라이언트 작업이 트리거되면 표시됩니다. 자세한 내용은 시스템 관리자에게 문의하십시오.
- **실시간 파일 시스템 보호가 일시 중지됨** - 사용자가 실시간 보호를 비활성화했습니다. 컴퓨터가 위협으로부터 보호되지 않습니다. 실시간 보호 활성화를 클릭하여 이 기능을 다시 활성화합니다.

주황색 "i"는 ESET 제품에 중요하지 않은 문제에 대한 주의가 필요함을 나타냅니다. 이는 다음과 같은 원인 때문일 수 있습니다.

- **웹 브라우저 보호가 비활성화됨** - 보안 알림을 클릭하고 **웹 브라우저 보호 활성화**를 클릭하여 웹 브라우저 보호를 다시 활성화할 수 있습니다.
- **라이선스가 곧 만료됨/라이선스가 오늘 만료됨** - 느낌표가 표시되는 보호 상태 아이콘이 나타납니다. 라이선스가 만료된 후에는 프로그램에서 업데이트할 수 없으며 보호 상태 아이콘이 빨간색으로 변합니다.
- **봇넷 보호가 일시 중지됨** - **봇넷 보호 활성화**를 클릭하여 이 기능을 다시 활성화합니다.
- **네트워크 공격 보호(IDS)가 일시 중지됨** - **네트워크 공격 보호(IDS) 활성화**를 클릭하여 이 기능을 다시 활성화합니다.
- **이메일 클라이언트 안티스팸이 일시 중지됨** - **이메일 클라이언트 안티스팸 활성화**를 클릭하여 이 기능을 다시 활성화합니다.
- **웹 컨트롤이 일시 중지됨** - **웹 컨트롤 활성화를 클릭하여 이 기능을 다시 활성화합니다.**
- **정책 재정의 활성화** - 문제가 해결될 때까지 정책에서 설정된 구성이 일시적으로 재정의됩니다. 권한이 있는 사용자만 정책 설정을 재정의할 수 있습니다. 자세한 내용은 재정의 모드 사용 방법을 참조하십시오.
- **장치 제어가 일시 중지됨** - **장치 제어 활성화**를 클릭하여 이 기능을 다시 활성화합니다.

ESET Endpoint Security의 첫 번째 창에서 제품 내 가시성 상태를 조정하려면 애플리케이션 상태를 참조하십시오.

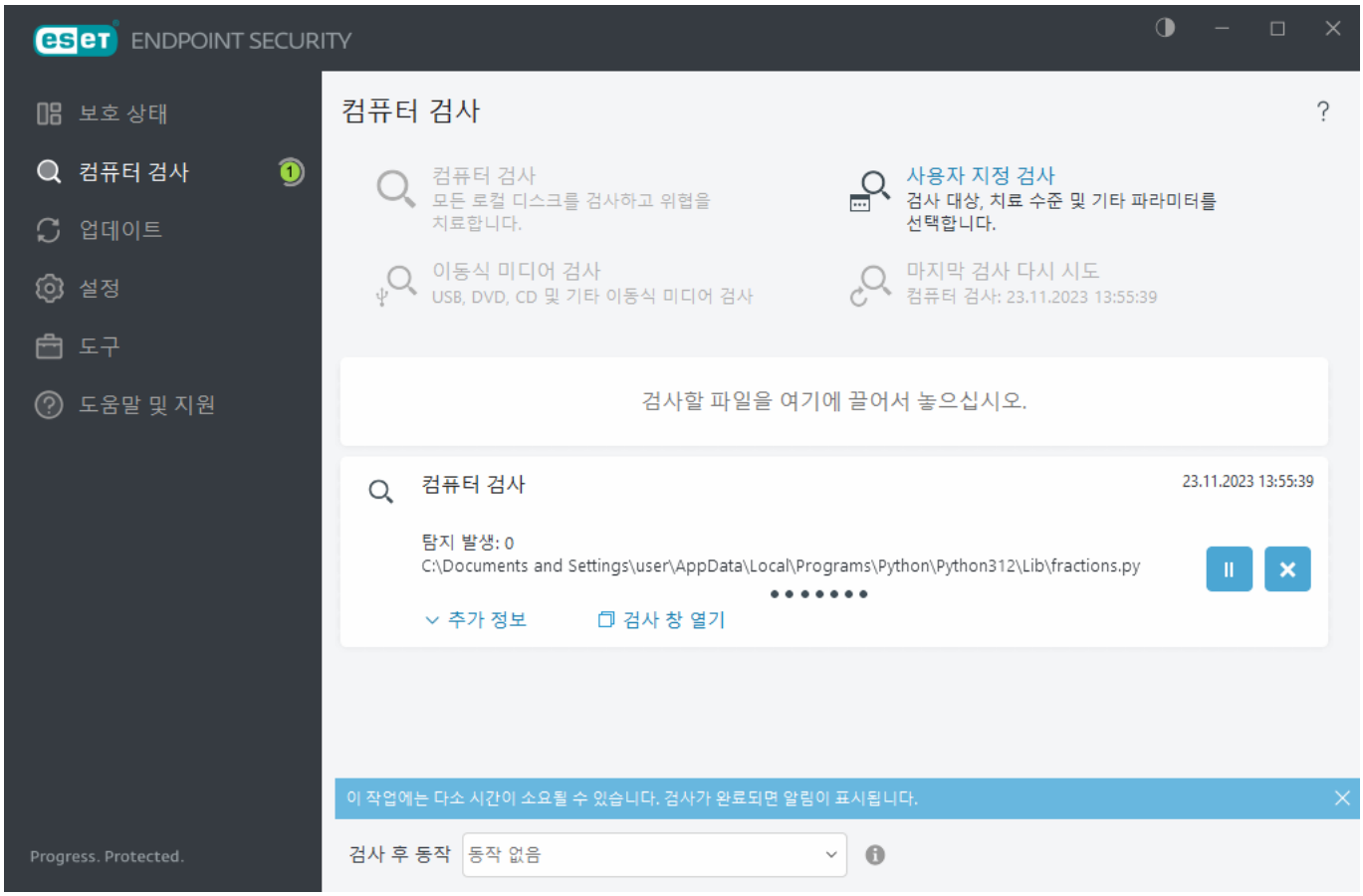
권장 해결 방법을 사용하여 문제를 해결할 수 없는 경우 **도움말 및 지원**을 클릭하여 도움말 파일에 접근하거나 ESET 지식베이스를 검색합니다. 계속해서 도움이 필요한 경우 ESET 기술 지원 요청을 전송할 수 있습니다. ESET 기술 지원은 사용자의 질문에 신속하게 응답하고 해결 방법을 찾는 데 도움을 줍니다.

상태가 ESET PROTECT 정책에 의해 차단된 기능에 속해 있는 경우 해당 링크는 클릭할 수 없습니다.

컴퓨터 검사

수동 검사기는 ESET Endpoint Security의 중요한 기능으로 컴퓨터에서 파일 및 폴더를 검사하는 데 사용됩니다. 보안 측면에서 볼 때 감염이 의심될 때만이 아니라 일상적인 보안 조치의 일환으로 정기적으로 컴퓨터 검사를 실행하는 것이 필수적입니다. 보안 측면에서 볼 때 감염이 의심될 때만이 아니라 일상적인 보안 조치의 일환으로 정기적으로 컴퓨터 검사를 실행하는 것이 필수적입니다. 실시간 파일 시스템 보호에서 검출

되지 않는 바이러스를 검출하기 위해 시스템 상세 검사를 정기적으로(예: 한 달에 한 번) 수행하는 것이 좋습니다. 그 당시 실시간 파일 시스템 보호가 비활성화되어 있었거나, 검색 엔진이 오래되었거나, 파일이 디스크에 저장될 때 바이러스로 검출되지 않은 경우가 여기에 해당합니다.



두 가지 유형의 **컴퓨터 검사**가 제공됩니다. **컴퓨터 검사**는 검사 파라미터를 더 구성할 필요 없이 시스템을 빠르게 검사합니다. **사용자 지정 검사**에서는 미리 정의된 검사 프로필을 선택하고 특정 검사 대상을 정의할 수 있습니다.

검사 프로세스에 대한 자세한 내용은 검사 진행률을 참조하십시오.

컴퓨터 검사

컴퓨터 검사를 사용하면 컴퓨터 검사를 빠르게 시작하고 사용자가 개입하지 않고도 감염된 파일을 치료할 수 있습니다. **컴퓨터 검사**의 장점은 작동하기 쉽고 검사를 상세하게 구성하지 않아도 된다는 것입니다. 이 검사에서는 로컬 드라이브에 있는 모든 파일을 검사하고, 탐지된 침입 항목을 자동으로 치료하거나 제거합니다. 치료 수준은 기본값으로 자동 설정됩니다. 치료 유형에 대한 자세한 내용은 치료를 참조하십시오.

끌어서 놓기를 통해 검사 기능을 사용하여 검사할 파일이나 폴더를 클릭하고 마우스 버튼을 누른 상태에서 마우스 포인터를 표시된 영역으로 이동한 후 버튼에서 손을 놓아 파일이나 폴더를 수동으로 검사할 수도 있습니다. 그런 다음 애플리케이션을 포그라운드로 이동합니다.

다음 검사 옵션은 **고급 검사**에서 사용할 수 있습니다.

사용자 지정 검사

사용자 지정 검사를 사용하면 검사 대상 및 검사 방법과 같은 검사 파라미터를 지정할 수 있습니다. **사용자**

지정 검사의 장점은 파라미터를 자세히 구성할 수 있다는 점입니다. 구성은 사용자 정의 검사 프로필에 저장할 수 있는데, 이는 동일한 파라미터로 검사를 반복 수행하는 경우에 유용할 수 있습니다.

이동식 미디어 검사

컴퓨터 검사와 유사하며, 현재 컴퓨터에 연결된 이동식 미디어(예: CD/DVD/USB)의 검사를 빠르게 시작합니다. 이 기능은 컴퓨터에 USB 플래시 드라이브 연결 시 콘텐츠에 악성코드 및 기타 잠재적 위협이 있는지 검사하고자 하는 경우에 유용할 수 있습니다.

이러한 유형의 검사는 **사용자 지정 검사**를 클릭하고 **검사 대상** 드롭다운 메뉴에서 **이동식 미디어**를 선택한 다음 **검사**를 클릭하여 시작할 수도 있습니다.

마지막 검사 다시 시도

이전 검사에서와 동일한 설정을 사용하여 이전에 수행한 검사를 빠르게 시작할 수 있습니다.

검사 후 동작 드롭다운 메뉴를 사용해 검사가 완료되면 자동으로 실행할 동작을 설정할 수 있습니다.

- **동작 없음** - 검사 완료 후 아무 동작도 수행되지 않습니다.
- **종료** - 검사가 완료되면 컴퓨터 전원이 꺼집니다.
- **필요한 경우 다시 시작** – 탐지된 위협 치료를 완료하기 위해 필요한 경우에만 컴퓨터가 다시 시작됩니다.
- **다시 부팅** - 검사가 완료되면 열려 있는 모든 프로그램이 닫히고 컴퓨터가 다시 시작됩니다.
- **필요한 경우 강제로 다시 시작** – 탐지된 위협 치료를 완료하기 위해 필요한 경우에만 컴퓨터가 강제로 다시 시작됩니다.
- **강제 재부팅** – 검사가 완료되면 사용자 상호 작용을 기다리지 않고 열려 있는 모든 프로그램을 강제로 닫은 후 컴퓨터를 다시 시작합니다.
- **절전 모드** - 작업을 빠르게 다시 시작할 수 있도록 사용자 세션을 저장하고 컴퓨터를 절전 상태로 설정합니다.
- **최대 절전 모드** - RAM에서 실행 중인 모든 항목을 하드 드라이브의 특수 파일로 이동합니다. 컴퓨터가 종료되지만 다음에 컴퓨터를 시작할 때 이전 상태에서 다시 시작됩니다.

> **절전 모드** 또는 **최대 절전 모드** 동작은 컴퓨터 전원과 절전 운영 체제 설정이나 컴퓨터/랩톱 기능에 따라 사용할 수 있습니다. 절전 모드 컴퓨터는 여전히 작동하는 컴퓨터입니다. 계속해서 기본 기능을 실행하고 컴퓨터가 배터리 전원으로 작동되는 경우 전기를 사용합니다. 외근 중일 때 등의 상황에서 배터리 수명을 보존하려면 최대 절전 모드를 사용하는 것이 좋습니다.

실행 중인 검사를 모두 완료하면 선택한 동작이 시작됩니다. **종료** 또는 **재부팅**을 선택하면 제품 확인 다이얼로그 창에 30초 카운트다운이 표시됩니다(요청된 동작을 비활성화하려면 **취소** 클릭).

> 컴퓨터 검사는 매월 1회 이상 실행하는 것이 좋습니다. **도구 > 스케줄러**에서 검사를 예약된 작업으로 구성할 수 있습니다. 주간 컴퓨터 검사를 예약하는 방법

사용자 지정 검사 시작기

사용자 지정 검사를 사용하여 전체 디스크가 아닌 디스크의 특정 부분이나 운영 메모리, 네트워크를 검사할 수 있습니다. 이렇게 하려면 **고급 검사 > 사용자 지정 검사**를 클릭하고 폴더(트리) 구조에서 특정 대상을 선택합니다.

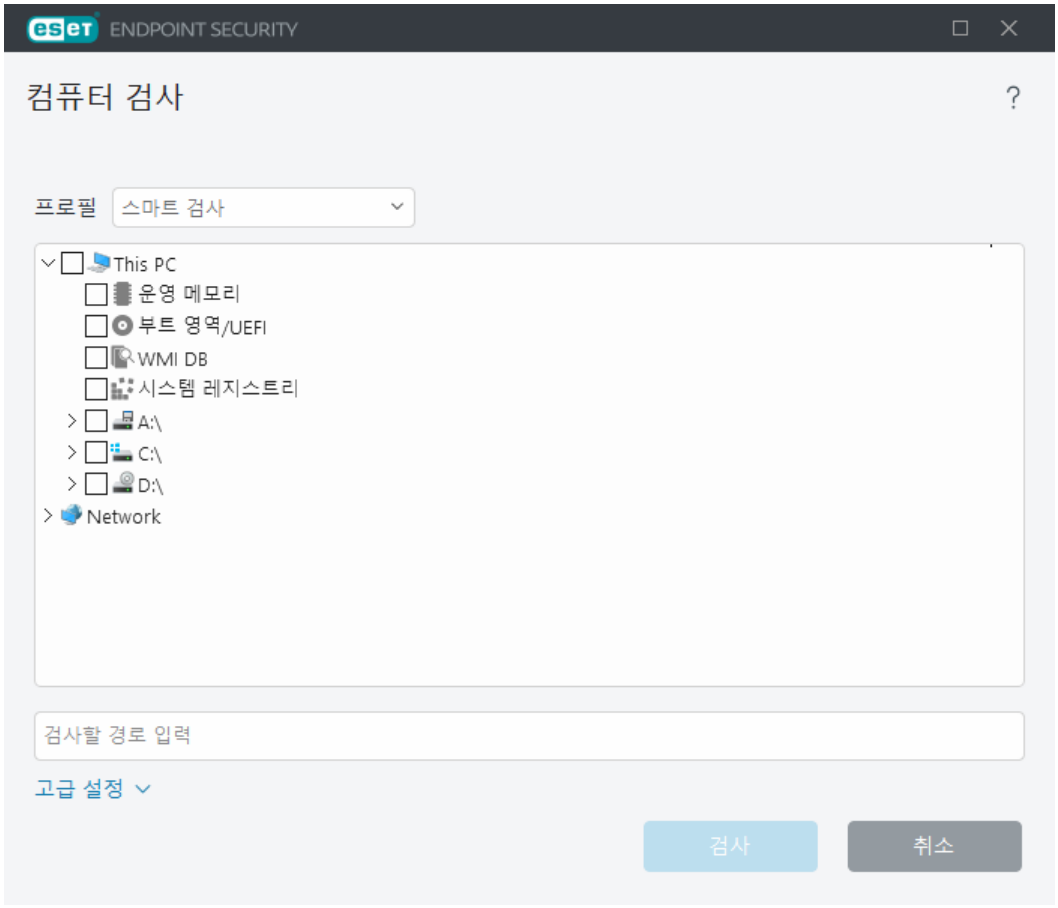
프로필 드롭다운 메뉴에서 특정 대상 검사에 사용할 프로필을 선택할 수 있습니다. 기본 프로필은 **스마트 검사**입니다. **상세 검사**, **오른쪽 마우스 버튼 메뉴 검사** 및 **컴퓨터 검사**의 세 가지 검사 프로필이 추가로 미리 정의되어 있습니다. 이러한 검사 프로필은 서로 다른 ThreatSense 파라미터를 사용합니다. 사용 가능한 옵션은 고급 설정 > **탐지 엔진** > **악성코드 검사** > **수동 검사** > ThreatSense에 설명되어 있습니다.

폴더(트리) 구조에는 특정 검사 대상도 포함되어 있습니다.

- **운영 메모리** – 운영 메모리에서 현재 사용되는 모든 프로세스와 데이터를 검사합니다.
- **부트 영역/UEFI** – 악성코드가 있는지 부트 영역과 UEFI를 검사합니다. UEFI 스캐너에 대한 자세한 내용은 용어집을 참조하십시오.
- **WMI 데이터베이스** – 전체 Windows Management Instrumentation WMI 데이터베이스, 모든 네임스페이스, 모든 클래스 인스턴스 및 모든 속성을 검사합니다. 감염된 파일 또는 데이터로 포함된 악성코드에 대한 참조를 검색합니다.
- **시스템 레지스트리** – 전체 시스템 레지스트리, 모든 키 및 하위 키를 검사합니다. 감염된 파일 또는 데이터로 포함된 악성코드에 대한 참조를 검색합니다. 탐지 항목을 치료할 때 참조 사항은 레지스트리에 남아 중요한 데이터가 손실되지 않도록 합니다.

검사 대상(파일 또는 폴더)으로 빠르게 이동하려면 트리 구조 아래의 텍스트 필드에 해당 경로를 입력합니다. 경로는 대소문자를 구분합니다. 검사에 대상을 포함하려면 트리 구조에서 대상 확인란을 선택합니다.

> **주간 컴퓨터 검사를 예약하는 방법**
> 정기적인 작업을 예약하려면 주간 컴퓨터 검사를 예약하는 방법 장을 참조하십시오.



고급 설정 > **탐지 엔진** > **악성코드 검사** > **수동 검사** > **ThreatSense** > **치료**에서 검사에 대한 치료 파라미터를 구성할 수 있습니다. 치료 동작 없이 검사를 실행하려면 **고급 설정**을 클릭하고 **치료하지 않고 검사**를 선택합니다. 검사 기록은 검사 로그에 저장됩니다.

제외 무시를 선택하면 이전에 제외된 확장명이 포함된 파일이 예외 없이 검사됩니다.

검사를 클릭하면 설정한 사용자 지정 파라미터로 검사를 실행할 수 있습니다.

관리자로 검사를 사용하면 관리자 계정에서 검사를 실행할 수 있습니다. 현재 사용자에게 검사할 파일에 대한 접근 권한이 없는 경우 이 옵션을 사용합니다. 현재 사용자가 관리자로서 UAC 작업을 호출할 수 없으면 이 버튼을 사용할 수 없습니다.

로그 표시를 클릭하여 검사 완료 시 컴퓨터 검사 로그를 볼 수 있습니다.

검사 진행률

검사 진행률 창에는 현재 검사 상태 및 악성 코드를 포함하는 것으로 밝혀진 파일 수에 대한 정보가 표시됩니다.

비밀번호로 보호되는 파일이나 시스템에서만 사용하는 파일(일반적으로 *pagefile.sys* 및 특정 로그 파일)과 같은 일부 파일의 경우 검색할 수 없는 것이 일반적입니다. 지식베이스 문서에서 자세한 내용을 확인할 수 있습니다.

주간 컴퓨터 검사를 예약하는 방법

정기적인 작업을 예약하려면 주간 컴퓨터 검사를 예약하는 방법 장을 참조하십시오.

검사 진행률 - 진행률 표시줄에 실행 중인 검사의 상태가 표시됩니다.

대상 - 현재 검사된 개체 이름 및 해당 위치입니다.

탐지 발생 - 검사한 파일, 발견된 위협, 검사 중에 치료된 위협의 총수를 표시합니다.

추가 정보를 클릭하면 다음 정보가 표시됩니다.

- **사용자** - 검사를 시작한 사용자 계정의 이름.
- **검사된 개체** - 이미 검사된 개체의 수.
- **기간** - 경과된 시간.

일시 중지 아이콘 - 검사를 일시 중지합니다.

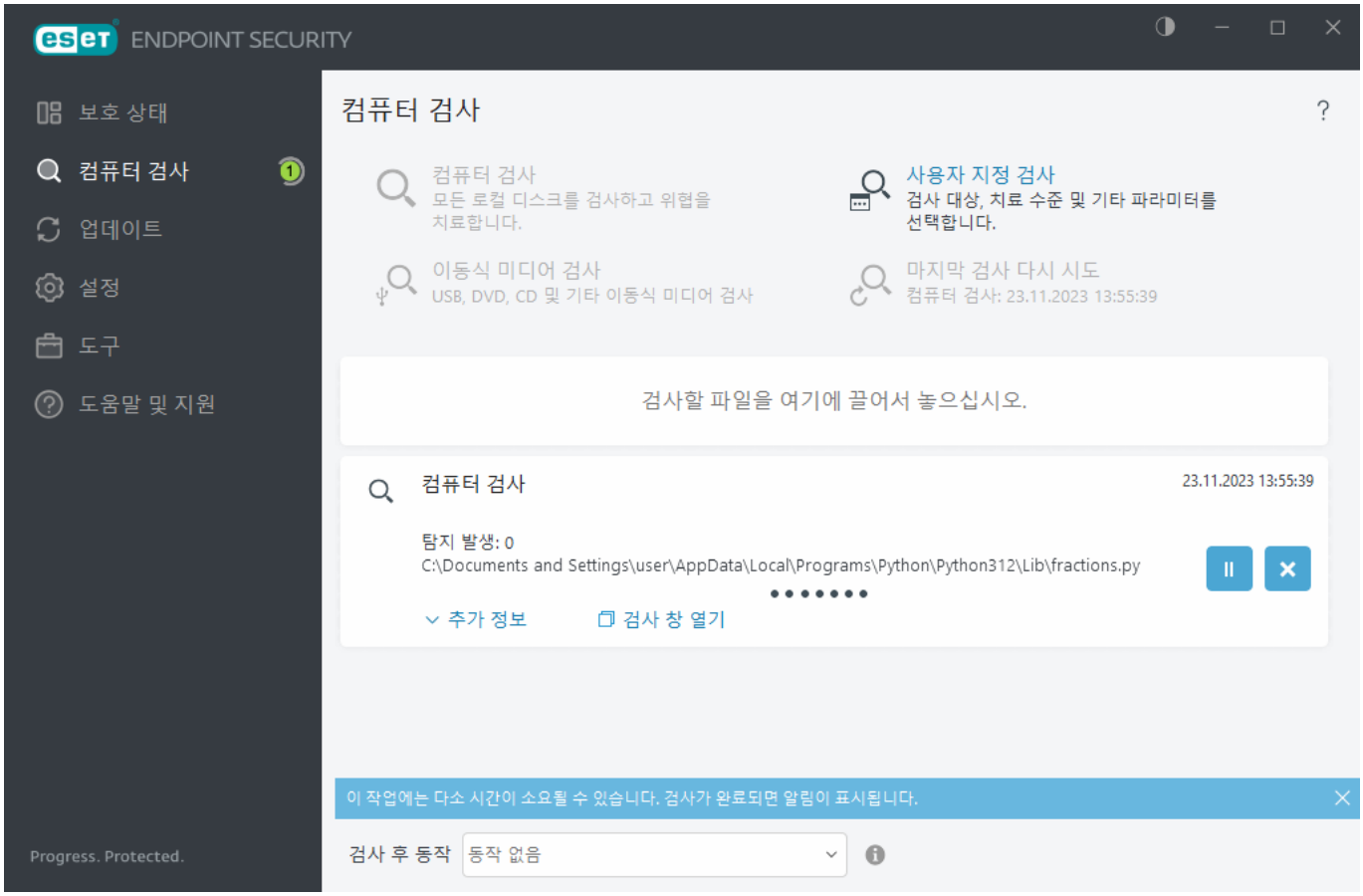
다시 시작 아이콘 - 이 옵션은 검사 진행을 일시 중지하면 표시됩니다. 아이콘을 클릭하면 검사가 계속 진행됩니다.

중지 아이콘 - 검사를 종료합니다.

검사에 대한 자세한 정보가 포함된 컴퓨터 검사 로그를 열려면 **검사 창 열기**를 클릭합니다.

검사 로그 스크롤 - 이 옵션을 활성화하면 새 항목이 추가됨에 따라 최신 항목이 표시되도록 검사 로그가 자동으로 아래로 스크롤됩니다.

현재 실행 중인 검사에 대한 상세 정보를 보려면 돋보기나 화살표를 클릭합니다. **컴퓨터 검사** 또는 **고급 검사 > 사용자 지정 검사**를 클릭하여 다른 검사를 동시에 실행할 수 있습니다.



검사 후 동작 드롭다운 메뉴를 사용해 검사가 완료되면 자동으로 실행할 동작을 설정할 수 있습니다.

- **동작 없음** - 검사 완료 후 아무 동작도 수행되지 않습니다.
- **종료** - 검사가 완료되면 컴퓨터 전원이 꺼집니다.
- **필요한 경우 다시 시작** – 탐지된 위협 치료를 완료하기 위해 필요한 경우에만 컴퓨터가 다시 시작됩니다.
- **다시 부팅** - 검사가 완료되면 열려 있는 모든 프로그램이 닫히고 컴퓨터가 다시 시작됩니다.
- **필요한 경우 강제로 다시 시작** – 탐지된 위협 치료를 완료하기 위해 필요한 경우에만 컴퓨터가 강제로 다시 시작됩니다.
- **강제 재부팅** – 검사가 완료되면 사용자 상호 작용을 기다리지 않고 열려 있는 모든 프로그램을 강제로 닫은 후 컴퓨터를 다시 시작합니다.
- **절전 모드** - 작업을 빠르게 다시 시작할 수 있도록 사용자 세션을 저장하고 컴퓨터를 절전 상태로 설정합니다.
- **최대 절전 모드** - RAM에서 실행 중인 모든 항목을 하드 드라이브의 특수 파일로 이동합니다. 컴퓨터가 종료되지만 다음에 컴퓨터를 시작할 때 이전 상태에서 다시 시작됩니다.

절전 모드 또는 **최대 절전 모드** 동작은 컴퓨터 전원과 절전 운영 체제 설정이나 컴퓨터/랩톱 기능에 따라 사용할 수 있습니다. 절전 모드 컴퓨터는 여전히 작동하는 컴퓨터입니다. 계속해서 기본 기능을 실행하고 컴퓨터가 배터리 전원으로 작동되는 경우 전기를 사용합니다. 외근 중일 때 등의 상황에서 배터리 수명을 보존하려면 최대 절전 모드를 사용하는 것이 좋습니다.

실행 중인 검사를 모두 완료하면 선택한 동작이 시작됩니다. **종료** 또는 **재부팅**을 선택하면 제품 확인 다이얼로그 창에 30초 카운트다운이 표시됩니다(요청된 동작을 비활성화하려면 **취소** 클릭).

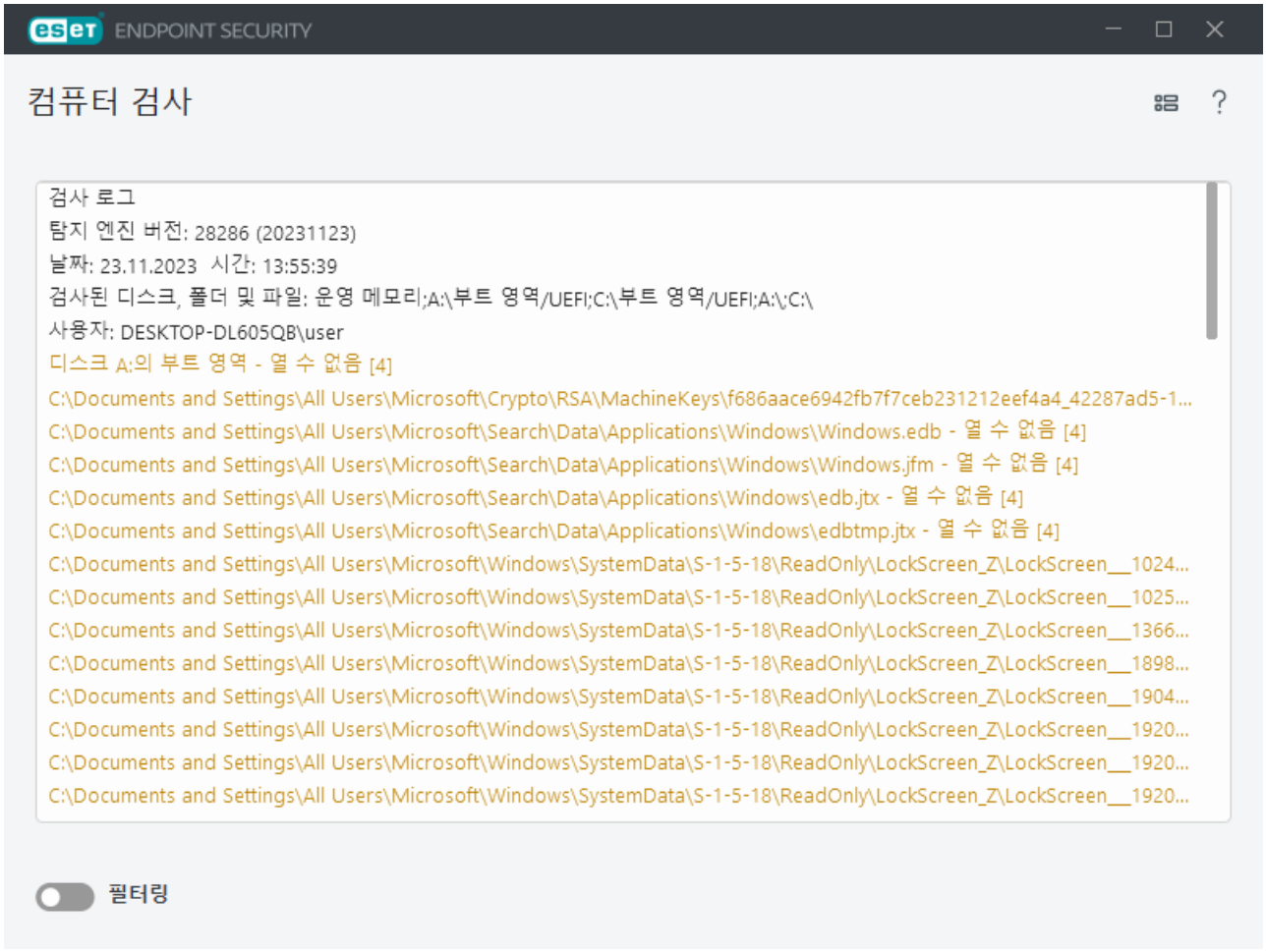
컴퓨터 검사 로그

로그 파일에서 특정 검사와 관련된 자세한 정보를 볼 수 있습니다. 검사 로그에 포함되는 정보는 다음과 같습니다.

- 검색 엔진 버전
- 시작 날짜 및 시간
- 검사된 디스크, 폴더 및 파일 목록
- 예약된 검사 이름(예약된 검사만 해당)
- 검사를 시작한 사용자.
- 검사 상태
- 검사된 개체 수
- 발견된 탐지 수
- 완료 시간
- 총 검사 시간

> 이전에 실행된, 똑같이 예약된 작업이 여전히 실행 중인 경우 예약된 컴퓨터 검사 작업을 새로 시작하는 단계를 건너뜁니다. 건너뛴 예약된 검사 작업은 검사된 개체가 0개인 컴퓨터 검사 로그와 **이전 검사가 여전히 실행 중이므로 검사가 시작되지 않았습니다.** 상태를 생성합니다.

이전 검사 로그를 찾으려면 기본 프로그램 창에서 **도구 > 로그 파일**을 선택합니다. 드롭다운 메뉴에서 **컴퓨터 검사**를 선택하고 원하는 레코드를 두 번 클릭합니다.



"열 수 없음", "여는 중 오류" 및/또는 "압축파일이 손상됨" 레코드에 대해 자세히 알아보려면, ESET 지식베이스 문서를 참조하십시오.

사용자 지정 기준을 정의하여 검색 범위를 좁힐 수 있는 로그 필터링 창을 열려면 **필터링** 토글 아이콘을 클릭합니다. 오른쪽 마우스 버튼 메뉴를 보려면 특정 로그 항목을 오른쪽 마우스 버튼으로 클릭하십시오.

동작	사용
같은 레코드 필터링	로그 필터링을 활성화합니다. 로그에는 선택한 유형과 동일한 유형의 레코드만 표시됩니다.
필터	이 옵션을 사용하여 로그 필터링 창을 열고 특정 로그 항목에 대한 기준을 정의할 수 있습니다. 바로 가기: `Ctrl+Shift+F`
필터 비활성화	필터 설정을 활성화합니다. 필터를 처음 활성화하는 경우 설정을 정의해야 하며, 로그 필터링 창이 열립니다.
필터 비활성화	필터를 끕니다(하단의 토글을 클릭하는 것과 같음).
복사	강조 표시된 레코드를 클립보드에 복사합니다. 바로 가기: `Ctrl+C`
모두 복사	모든 레코드를 창에 복사합니다.
내보내기	클립보드에 강조 표시된 레코드를 XML 파일로 내보냅니다.
모두 내보내기	이 옵션은 창에 있는 모든 레코드를 XML 파일로 내보냅니다.
탐지 설명	강조 표시된 침투의 위험과 증상에 대한 자세한 정보가 포함된 ESET 위협 백과사전을 엽니다.

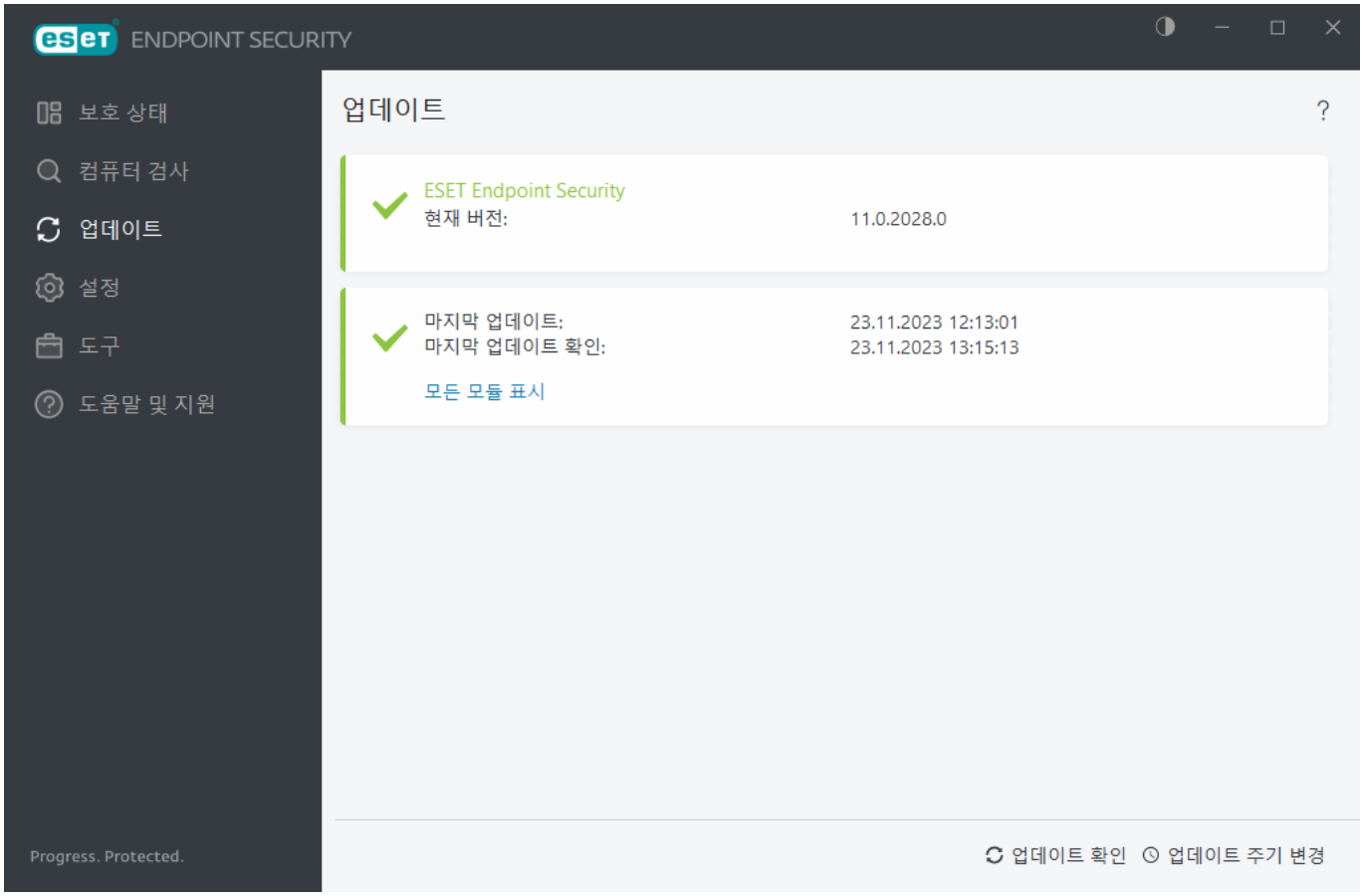
업데이트

컴퓨터의 보안 수준을 최대로 유지하기 위한 가장 좋은 방법은 ESET Endpoint Security를 정기적으로 업데이트하는 것입니다. 업데이트 모듈을 통해 프로그램 모듈과 시스템 구성 요소를 항상 최신 상태로 유지할 수 있습니다.

기본 프로그램 창에서 **업데이트**를 클릭하면 마지막으로 성공한 업데이트 날짜 및 시간, 업데이트가 필요한지 여부 등 현재 업데이트 상태를 확인할 수 있습니다.

자동 업데이트 외에도 **업데이트 확인**을 클릭하여 수동 업데이트를 트리거할 수 있습니다. 프로그램 모듈과 구성 요소를 정기적으로 업데이트하는 것은 악성 코드에 대해 완전한 보호 성능을 유지 관리하는 데 중요한 요소입니다. 제품 모듈 구성 및 작동에 주의를 기울여 주십시오. 업데이트를 수신하기 위한 라이선스 키를 사용하여 제품을 활성화해야 합니다. 설치 중에 활성화하지 않은 경우 ESET 업데이트 서버에 접근하려면 ESET Endpoint Security을(를) 활성화해야 합니다. 라이선스 키는 ESET Endpoint Security 구매 후 ESET에서 이메일로 보내 드렸습니다.

사용자 이름 및 패스워드 없이 오프라인 라이선스 파일로 ESET Endpoint Security를 활성화한 후 업데이트를 시도할 경우 빨간색 정보 **모듈 업데이트 실패**가 표시되며, 미러에서만 업데이트를 다운로드할 수 있습니다.



현재 버전 – ESET Endpoint Security 빌드 번호입니다.

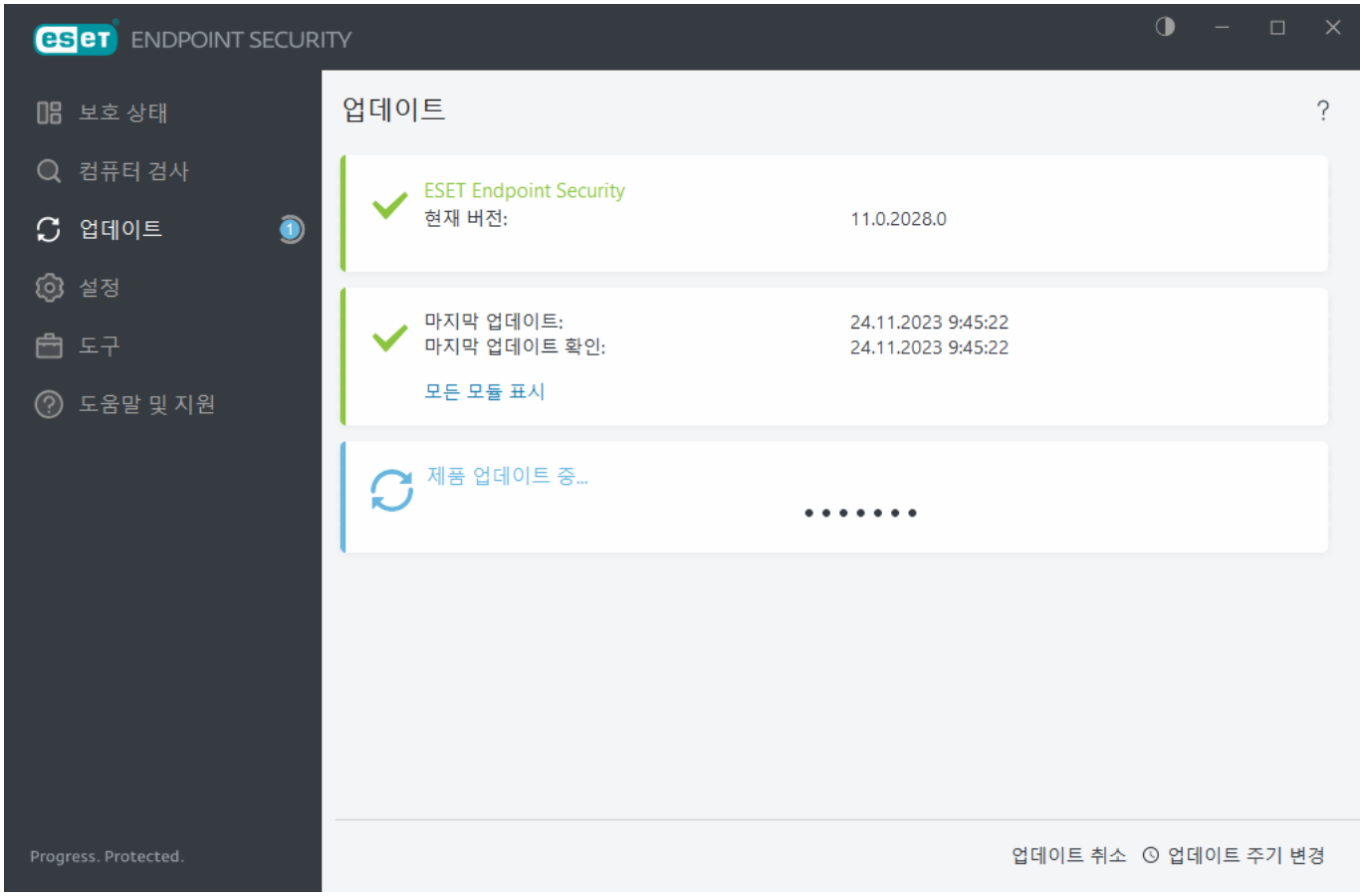
마지막으로 성공한 업데이트 – 마지막으로 성공한 업데이트의 날짜와 시간입니다. 이 날짜는 최신 날짜여야 합니다. 즉, 검색 엔진이 최신 상태여야 합니다.

마지막으로 성공한 업데이트 확인 – 마지막으로 성공한 모듈 업데이트 시도 날짜와 시간입니다.

모든 모듈 표시 – 설치된 모듈 목록을 열고 모듈 버전 및 마지막 업데이트 날짜를 확인하려면 이 링크를 클릭합니다.

업데이트 프로세스

업데이트 확인을 클릭하면 다운로드 프로세스가 시작됩니다. 다운로드 진행률 표시줄 및 남은 다운로드 시간이 표시됩니다. 업데이트를 중단하려면 **업데이트 취소**를 클릭합니다.



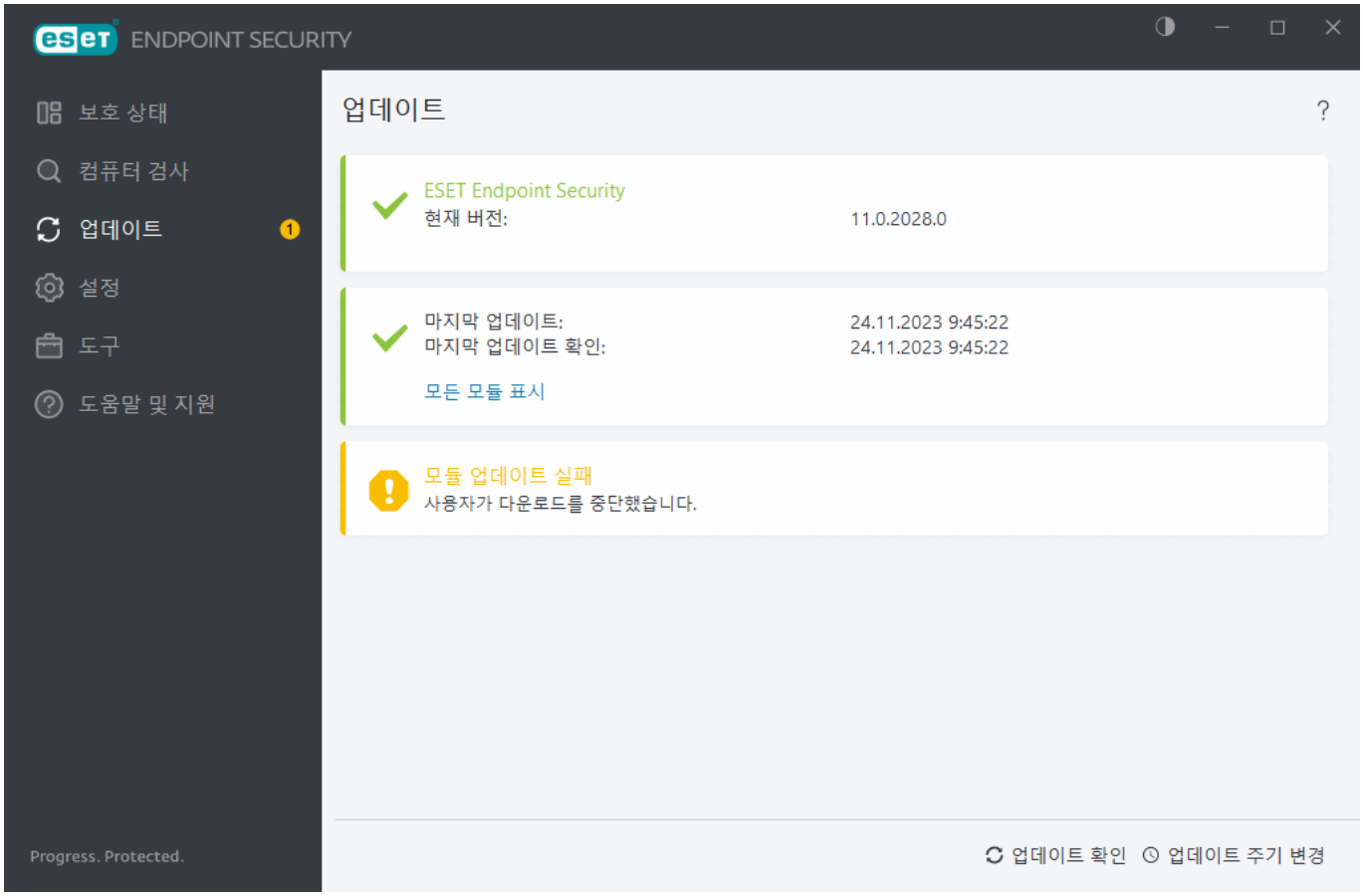
일반적인 상황에서는 **업데이트** 창에 녹색 확인 표시가 나타나며, 이는 프로그램이 최신 상태임을 의미합니다. 녹색 확인 표시가 나타나지 않는 경우 프로그램이 최신 상태가 아니므로 감염 위험이 증가합니다. 가급적 빨리 프로그램 모듈을 업데이트하십시오.

실패한 업데이트

탐지 엔진이 오래된 버전임 – 모듈을 업데이트하려는 시도에 여러 번 실패하면 이 오류가 나타납니다. 이 경우 업데이트 설정을 확인하는 것이 좋습니다. 이 오류가 발생하는 가장 일반적인 이유는 인증 데이터가 잘못 입력되거나, 연결 설정이 잘못 구성되었기 때문입니다.

이전 알림은 실패한 업데이트에 대한 다음 두 가지 메시지(**모듈 업데이트 실패**)와 관련이 있습니다.

1. **유효하지 않은 라이선스** - 라이선스가 활성화되지 않았습니다. 인증 데이터를 확인하는 것이 좋습니다. 새 라이선스 키를 입력하려면 기본 메뉴에서 **도움말 및 지원** > **라이선스 변경**을 클릭합니다.
2. **업데이트 파일을 다운로드하는 동안 오류 발생** - 오류의 가능한 원인은 잘못된 인터넷 연결 설정입니다. 이 경우 웹 브라우저에서 임의의 웹 사이트를 열어 인터넷 연결을 확인하는 것이 좋습니다. 웹 사이트가 열리지 않으면 인터넷 연결이 설정되어 있지 않거나 컴퓨터 관련 연결 문제가 있을 수 있습니다. ISP(인터넷 서비스 공급업체)를 통한 활성 인터넷 연결이 있는지 확인하십시오.



자세한 내용은 ESET 지식베이스 문서를 참조하십시오.

업데이트 작업을 생성하는 방법

기본 메뉴에서 **업데이트**를 클릭한 후 표시되는 기본 창에서 **업데이트 확인**을 클릭하여 수동으로 업데이트를 트리거할 수 있습니다.

또한 예약된 작업으로 업데이트를 실행할 수도 있습니다. 예약된 작업을 구성하려면 **도구 > 스케줄러**를 클릭합니다. 기본적으로 ESET Endpoint Security에는 다음과 같은 업데이트 작업이 활성화되어 있습니다.

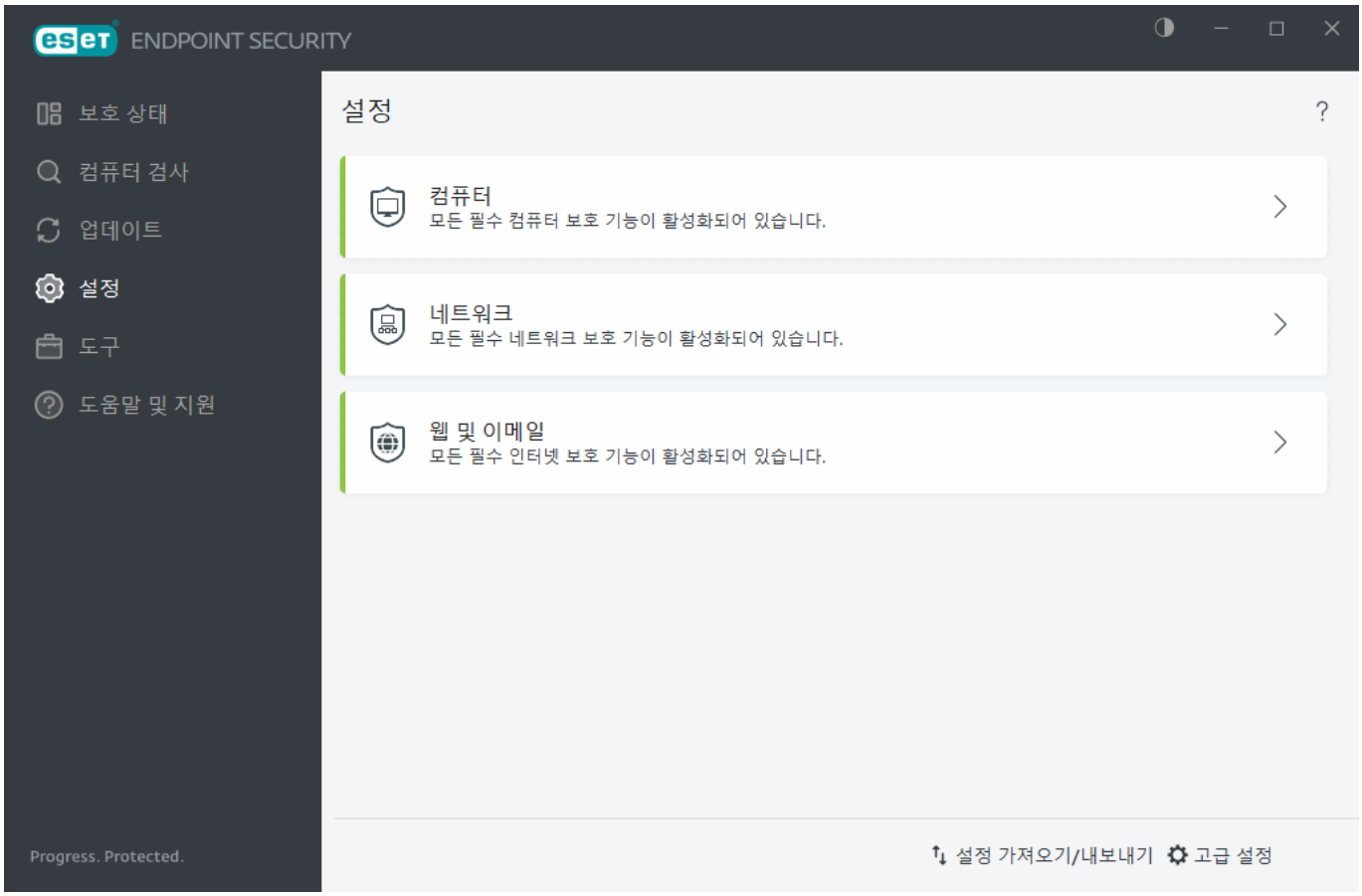
- **정기적 자동 업데이트**
- **사용자 로그온 후 자동 업데이트**

필요에 맞게 각 업데이트 작업을 수정할 수 있습니다. 기본 업데이트 작업 외에 사용자 정의 구성을 사용하여 새 업데이트 작업을 생성할 수 있습니다. 업데이트 작업 생성 및 구성에 대한 자세한 내용은 스케줄러 섹션을 참조하십시오.

설정

기본 프로그램 창 > **설정**에서 사용 가능한 보호 기능 그룹을 찾을 수 있습니다.

ESET PROTECT 웹 콘솔에서 정책을 생성할 때 설정별로 플래그를 선택할 수 있습니다. 강제 적용 플래그가 포함된 설정은 우선적으로 지정되며 이후 정책으로 덮어쓸 수 없습니다(이후 정책에 강제 적용 플래그가 포함된 경우에도 마찬가지임). 따라서 이 설정은 변경되지 않습니다(예를 들어 병합하는 동안 이후 정책 또는 또는 사용자에 의해 변경되지 않음). 자세한 내용은 ESET PROTECT 온라인 도움말의 플래그를 참조하십시오.



설정 메뉴에는 다음과 같은 섹션이 포함되어 있습니다.

컴퓨터

네트워크

웹 및 이메일

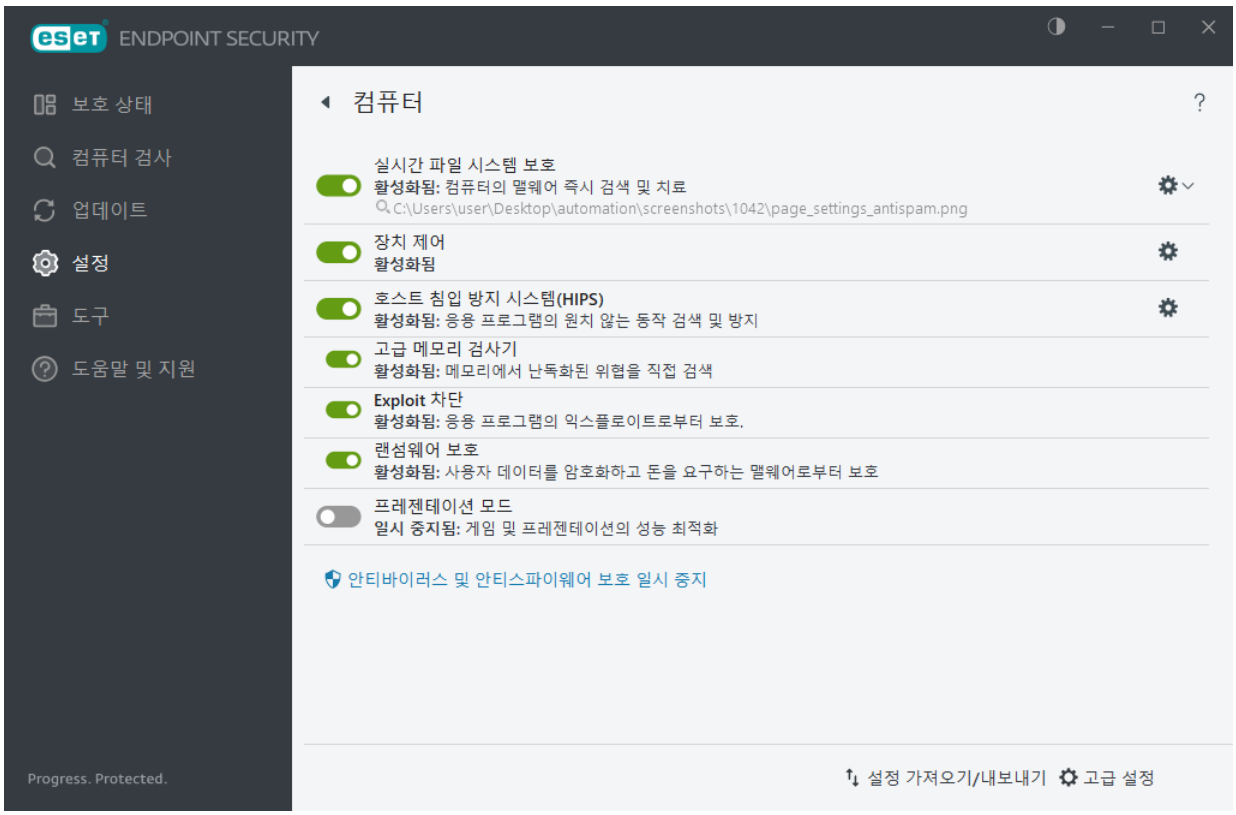
ESET PROTECT 정책이 적용되면 특정 구성 요소 옆에 잠금 아이콘이 표시됩니다. ESET PROTECT에서 적용된 정책은 로그인된 사용자(예: 관리자)에 의한 인증 후 로컬로 재정의할 수 있습니다. 자세한 내용은 ESET PROTECT 온라인 도움말을 참조하십시오.

이러한 방식으로 비활성화된 모든 보호 조치는 컴퓨터가 다시 시작되고 나면 다시 활성화됩니다.

설정 창 아래쪽에 추가 옵션이 있습니다. 고급 설정을 클릭하면 각 모듈에 대한 파라미터를 보다 상세하게 구성할 수 있습니다. 설정 가져오기/내보내기를 통해 .xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장할 수 있습니다.

컴퓨터

기본 프로그램 창 > **설정**에서 **컴퓨터**를 클릭하여 모든 보호 모듈에 대한 개요를 확인합니다.



컴퓨터 섹션에서는 다음 구성 요소를 활성화 또는 비활성화할 수 있습니다.

- 실시간 파일 시스템 보호 - 컴퓨터에서 모든 파일을 열거나 생성하거나 실행할 때 악성 코드가 있는지 검사합니다. 실시간 파일 시스템 보호 옆의 톱니바퀴 아이콘을 클릭하고 제외 편집을 클릭하여 파일 및 폴더를 검사에서 제외할 수 있는 제외 설정 창을 엽니다. 실시간 파일 시스템 보호 고급 설정을 열려면 구성을 클릭합니다.
- 장치 제어 – 자동 장치(CD/DVD/USB/...) 제어 기능을 제공합니다. 이 모듈에서는 확장 필터/권한을 차단하거나 조정하고, 사용자가 지정된 장치에 접근하여 사용하는 기능을 정의할 수 있습니다.
- Host Intrusion Prevention System (HIPS) - HIPS 시스템은 운영 체제 내에서 발생하는 이벤트를 모니터링하고 사용자 지정 규칙 집합에 따라 반응합니다.
- **고급 메모리 검사기** - 는 Exploit 차단과 함께 작동하여 난독화 또는 암호화를 사용한 맬웨어 방지 제품의 검색을 피하도록 설계된 맬웨어로부터 보호하는 기능을 강화합니다. 고급 메모리 검사기는 기본적으로 활성화되어 있습니다. 이러한 유형의 보호에 대한 자세한 내용은 용어집을 참조하십시오.
- **Exploit 차단** - 웹 브라우저, PDF 리더, 이메일 클라이언트 및 MS Office 구성 요소와 같은 일반적으로 악용되는 애플리케이션 유형을 강화하도록 설계되었습니다. Exploit 차단은 기본적으로 활성화되어 있습니다. 이러한 유형의 보호에 대한 자세한 내용은 용어집을 참조하십시오.
- **랜섬웨어 보호** - HIPS 기능의 일부로 작동하는 추가적인 보호 레이어입니다. 랜섬웨어 보호 기능이 작동하려면 ESET LiveGrid® 평판 시스템이 활성화되어 있어야 합니다. 이러한 유형의 보호에 대한 자세한 내용을 참조하십시오.
- 프레젠테이션 모드 - 소프트웨어를 중단 없이 사용하고 알림의 방해를 받지 않으며 CPU의 사용을 최소화하려는 사용자를 위한 기능입니다. 프레젠테이션 모드를 활성화하면 경고 메시지(잠재적 보안 위험)가 수신되며 기본 프로그램 창이 주황색으로 바뀝니다.

안티바이러스 및 안티스파이웨어 보호 일시 중지 - 안티바이러스 및 안티스파이웨어 보호를 일시적으로 비

활성화할 때마다 드롭다운 메뉴를 사용하여 선택한 구성 요소를 비활성화할 기간을 선택한 다음 **적용**을 클릭하여 보안 구성 요소를 비활성화할 수 있습니다. 보호 기능을 다시 활성화하려면 **안티바이러스, 안티스파이웨어 보호 활성화**를 클릭합니다.

개별 보호 모듈을 일시 중지하거나 비활성화하려면 토글 아이콘을 클릭합니다.

⚠ 보호 모듈을 끄면 컴퓨터의 보호 수준이 저하될 수 있습니다.

위협이 탐지됨

시스템의 여러 진입점(예: 웹 페이지, 공유 폴더, 이메일 또는 USB/외부 디스크/CD/DVD 등의 이동식 장치)에서 침입이 발생할 수 있습니다.

표준 동작

침입 항목이 ESET Endpoint Security에서 처리되는 방법에 대한 일반적인 예로, 다음 방법을 사용하여 침입을 검출할 수 있습니다.

- 실시간 파일 시스템 보호
- 웹 브라우저 보호
- 이메일 클라이언트 보호
- 수동 컴퓨터 검사

각 방법에서는 표준 치료 수준을 사용하며, 파일을 치료하고 검역소로 이동하거나 연결을 종료하려고 시도합니다. 화면의 오른쪽 하단에 있는 알림 영역에 알림 창이 표시됩니다. 탐지/치료된 개체에 대한 자세한 내용은 로그 파일을 참조하십시오. 치료 수준 및 동작에 대한 자세한 내용은 치료를 참조하십시오.

치료 및 삭제

실시간 파일 시스템 보호에 대해 수행할 동작이 미리 정의되어 있지 않으면 경고 창에 옵션을 선택하라는 메시지가 표시됩니다. 일반적으로 **치료**, **삭제** 및 **무시** 옵션을 사용할 수 있습니다. **무시** 옵션은 감염된 파일을 치료되지 않은 상태로 두기 때문에 선택하지 않는 것이 좋습니다. 단, 파일이 무해하며 잘못 검출된 것이 확실하다면 무시를 선택해도 됩니다.

파일이 악성 코드를 첨부한 바이러스에 의해 파일이 공격을 받았다면 치료를 적용합니다. 이 경우 먼저 감염된 파일을 치료해 원래 상태로 복원합니다. 악성 코드만 포함된 파일은 삭제됩니다.

감염된 파일이 "잠긴" 상태거나 시스템 프로세스에서 사용 중이면 일반적으로 시스템을 다시 시작하여 해제된 후에만 삭제됩니다.

검역소에서 복원

검역소는 ESET Endpoint Security 기본 프로그램 창에서 **도구** > **검역소**를 클릭하여 접근할 수 있습니다.

검역소로 보낸 파일은 원래 위치에 복원할 수도 있습니다.

- 이렇게 하려면 **복원** 기능을 사용합니다. 이 기능은 마우스 오른쪽 버튼 메뉴에서 검역소에 지정된 파일을 마우스 오른쪽 단추로 클릭하여 사용할 수 있습니다.
- 파일이 사용자가 원치 않는 애플리케이션으로 표시된 경우 **복원 후 검사에서 제외** 옵션이 활성화됩니다. 또한 제외를 참조하십시오.
- 마우스 오른쪽 버튼 메뉴에서는 **복원 대상** 옵션도 제공하여 제거된 위치가 아닌 위치로 파일을 복원할 수 있습니다.
- 예를 들어 읽기 전용 네트워크 공유에 있는 파일의 경우 복원 기능을 사용할 수 없습니다.

여러 위협

컴퓨터 검사 중 감염된 파일이 치료되지 않은 경우(또는 치료 수준이 **치료 안 함**으로 설정된 경우) 이러한 파일에 대한 동작을 선택하라는 경고 창이 표시됩니다.

압축파일의 파일 삭제

기본 치료 모드에서는 압축파일에 감염된 파일이 있고 감염되지 않은 파일은 없는 경우에만 전체 압축파일을 삭제합니다. 따라서 감염되지 않은 무해한 파일이 있는 압축파일은 삭제되지 않습니다. 단, 엄격한 치료 모드에서는 감염된 파일이 하나라도 포함되어 있으면 압축파일 내의 다른 파일 상태에 관계없이 압축파일을 삭제하므로 엄격한 치료 검사를 수행하는 경우에는 주의해야 합니다.

컴퓨터가 맬웨어에 감염된 증상(예: 속도가 느려짐, 작동이 자주 중단됨 등)을 보이면 다음을 수행하는 것이 좋습니다.

- ESET Endpoint Security을(를) 열고 컴퓨터 검사를 클릭합니다.
- **스마트 검사**를 클릭합니다(자세한 내용은 컴퓨터 검사 참조).
- 검사를 마치면 검사한 파일, 감염된 파일 및 치료된 파일 수가 표시된 로그를 검토합니다.

디스크의 특정 부분만 검사하려면 **사용자 지정 검사**를 클릭하고 바이러스를 검사할 대상을 선택합니다.

네트워크

기본 프로그램 창 > **설정** > **네트워크**를 열어 기본 네트워크 보호 설정을 구성하거나 네트워크 통신 문제를 해결합니다.

개별 보호 모듈을 일시 중지하거나 비활성화하려면  토글 아이콘을 클릭합니다.

⚠ 보호 모듈을 끄면 컴퓨터의 보호 수준이 저하될 수 있습니다.

보호 모듈 옆의 톱니바퀴 아이콘⚙을 클릭하여 고급 설정에 접근합니다.

방화벽 - ESET Endpoint Security 구성에 따라 모든 네트워크 통신을 필터링합니다.

구성 - 방화벽에서 네트워크 통신을 처리하는 방법을 정의할 수 있는 방화벽 고급 설정을 엽니다.

방화벽 일시 중지(모든 트래픽 허용) - 모든 네트워크 트래픽 차단과 반대됩니다. 이 옵션을 선택하면 방화벽의 모든 필터링 옵션이 꺼지고 나가는 연결 및 들어오는 연결이 모두 허용됩니다. 네트워크 트래픽 필터링이 이 모드로 설정된 경우 방화벽을 다시 활성화하려면 **방화벽 활성화**를 클릭합니다.

모든 트래픽 차단 - 들어오는 통신과 나가는 통신이 모두 방화벽에 의해 차단됩니다. 이 옵션은 심각한 보안 위험이 의심되어 네트워크에서 시스템 연결을 끊어야 하는 경우에만 사용합니다. 네트워크 트래픽 필터링이 **모든 트래픽 차단** 모드일 때 **모든 트래픽 차단 중지**를 클릭하면 방화벽이 정상 작동 상태로 복원됩니다.

자동 모드 - (다른 필터링 모드가 활성화된 경우) - 필터링 모드를 자동 필터링 모드(사용자 정의 규칙 포함)로 변경하려면 클릭합니다.

대화 모드 - (다른 필터링 모드가 활성화된 경우) - 필터링 모드를 대화 필터링 모드로 변경하려면 클릭합니다.

네트워크 공격 보호(IDS) - 네트워크 트래픽의 내용을 분석하고 네트워크 공격으로부터 보호합니다. 유해한 것으로 간주되는 트래픽이 차단되면 ESET Endpoint Security 제품이 보호되지 않은 무선 네트워크 또는 약한 보호 기능을 가진 네트워크에 연결되는 경우 알려줍니다.

봇넷 보호 - 시스템에서 악성코드를 빠르고 정확하게 식별합니다.

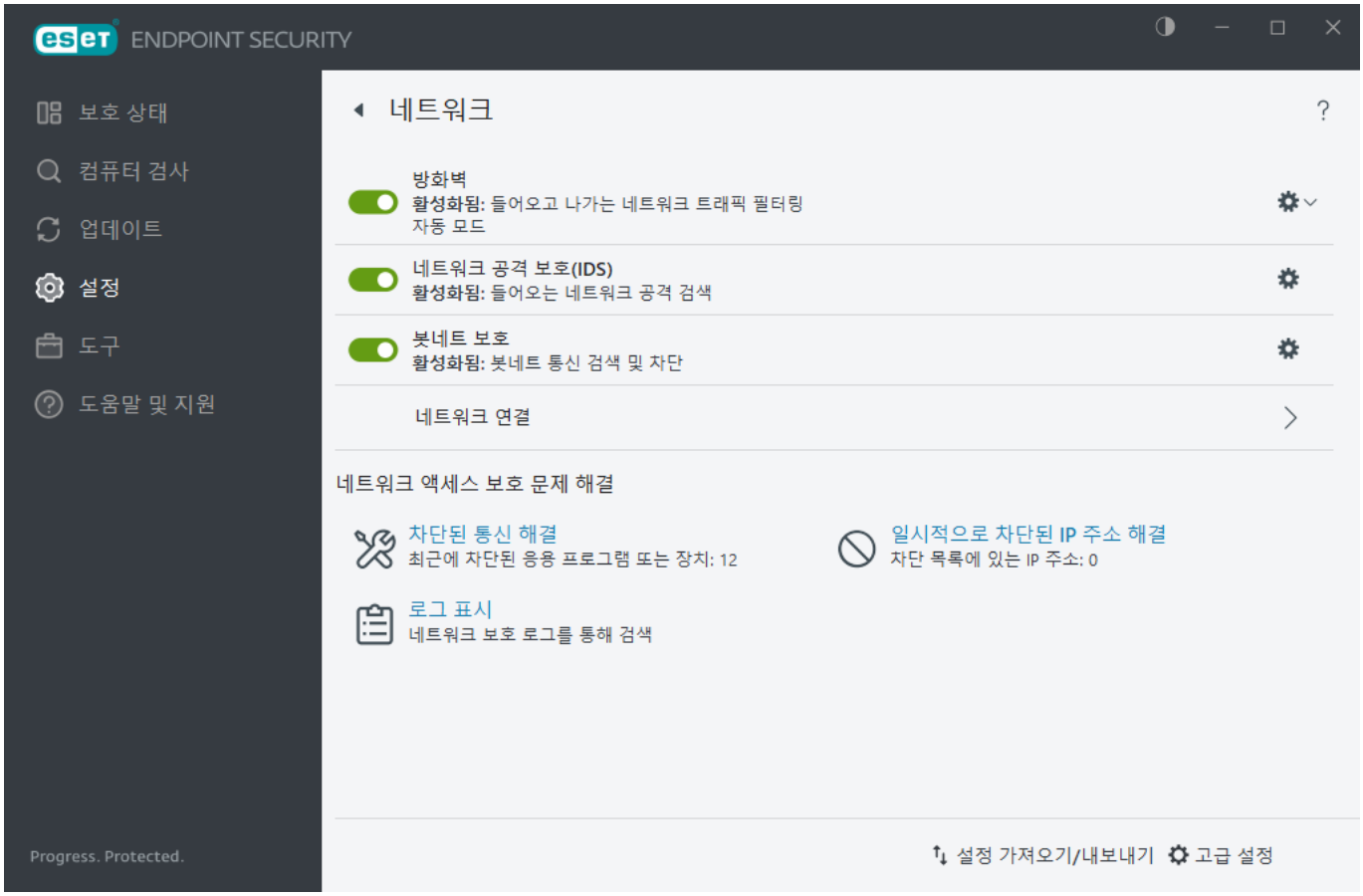
네트워크 연결 - 자세한 정보와 함께 네트워크 어댑터가 연결된 네트워크를 표시합니다.

차단된 통신 해결 - ESET 방화벽으로 인해 발생한 연결 문제를 해결하는 데 도움을 줍니다. 자세한 내용은 문제 해결 마법사를 참조하십시오.

임시 차단된 IP 주소 확인 - 일정 기간 연결을 차단하도록 차단 목록에 추가되고 공격의 근원지로 탐지된 IP

주소 목록을 확인합니다.

로그 표시 - 네트워크 보호 로그 파일을 엽니다.



네트워크 연결

네트워크 어댑터가 연결된 네트워크를 표시합니다. 네트워크 연결을 보려면 기본 프로그램 창 > **설정** > **네트워크** > **네트워크 연결**을 엽니다.

목록에서 연결을 두 번 클릭하여 연결 상세 정보와 네트워크 어댑터 상세 정보를 표시합니다.

특정 네트워크 연결 위로 마우스를 가져간 다음 **신뢰할 수 있음** 열의 ⋮ 메뉴 아이콘을 클릭하여 다음 옵션 중 하나를 선택합니다.

- **편집** - 특정 네트워크에 네트워크 보호 프로필을 할당할 수 있는 네트워크 보호 구성 창을 엽니다.
- **삭제** - 네트워크 연결 구성을 기본값으로 재설정합니다.

네트워크 연결 상세 정보

네트워크 연결 목록에서 연결을 두 번 클릭하여 네트워크 어댑터 상세 정보와 함께 연결 상세 정보를 표시할 수 있습니다. 네트워크 연결 및 어댑터 상세 정보는 네트워크 접근 보호에서 구성하려는 네트워크를 식별하는 데 도움이 될 수 있습니다.

네트워크 연결 상세 정보:

- 네트워크 연결 상태
- 처음 네트워크를 탐지한 날짜와 시간
- 네트워크가 마지막으로 활성화된 시간
- 이 네트워크에 연결된 총 시간
- 네트워크 연결 윤곽
- Windows에 정의된 네트워크 연결 프로필
- 네트워크 보호 구성(네트워크를 신뢰할 수 있는지 여부)

네트워크 어댑터 상세 정보:

- 연결 유형(유선, 가상 등)
- 네트워크 어댑터 이름
- 어댑터 설명
- IP 주소 (MAC 주소 포함)
- 서브넷이 있는 네트워크의 IPv4/IPv6 주소
- DNS 접미사
- DNS 서버 IP
- DHCP 서버 IP
- 기본 게이트웨이 IP 및 MAC 주소
- 어댑터 MAC 주소

네트워크 액세스 문제 해결

문제 해결 마법사는 방화벽으로 인해 발생한 연결 문제를 해결하는 데 도움을 줍니다. **네트워크 접근 문제 해결**은 기본 프로그램 창 > **설정** > **네트워크** > **차단된 통신 해결**에서 찾을 수 있습니다.

로컬 애플리케이션에 대해 차단된 통신을 표시하거나 **원격 장치**에서 차단된 통신을 표시하려면 선택합니다.

드롭다운 메뉴에서 통신이 차단되었던 기간을 선택합니다. 최근에 차단된 통신 목록에서는 애플리케이션이나 장치 유형, 평판 및 해당 기간 동안 차단된 총 애플리케이션 및 장치 수 등을 개략적으로 볼 수 있습니다. 차단된 통신에 대한 자세한 내용을 보려면 **상세 정보**를 클릭하십시오. 다음 단계는 연결 문제가 있는 장치나 애플리케이션의 차단을 해제하는 것입니다.

차단 해제를 클릭하면 이전에 차단된 통신이 허용됩니다. 애플리케이션 문제가 계속되거나 장치가 예상대로 작동하지 않으면 **다른 규칙 생성**을 클릭합니다. 그러면 해당 장치에 대해 이전에 차단된 모든 통신이 허용됩니다. 그래도 문제가 해결되지 않으면 컴퓨터를 다시 시작하십시오.

방화벽 규칙 열기를 클릭하면 마법사에서 생성된 규칙을 볼 수 있습니다. 또한 고급 설정 > **보호** > **네트워크 접근 보호** > **방화벽** > **규칙** > **편집**을 통해 마법사에서 생성된 규칙을 볼 수 있습니다.

다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- 문제 해결 마법사를 사용하여 방화벽 예외 추가

규칙을 생성할 수 없는 경우 오류 메시지가 표시됩니다. **다시 시도**를 클릭하고 프로세스를 반복하여 통신 차단을 해제하거나, 차단된 통신 목록에서 다른 규칙을 생성합니다.

임시 IP 주소 차단 목록

공격의 근원지로 탐지되었고 차단 목록에 추가되어 일정 기간 연결이 차단되는 IP 주소를 보려면 기본 프로그램 창 > **설정** > **네트워크 보호** > **임시 차단된 IP 주소 확인**을 엽니다. 임시 차단된 IP 주소는 1시간 동안 차단됩니다.

열

IP 주소 - 차단된 IP 주소를 표시합니다.

차단 이유 - 주소에서 차단된 공격 유형(예: TCP 포트 검사 공격)을 표시합니다.

시간 초과 - 차단 목록에서 주소가 만료되는 시간과 날짜를 표시합니다.

제어 요소

제거 - 만료되기 전에 차단 목록에서 주소를 제거하려면 클릭합니다.

모두 제거 - 차단 목록에서 모든 주소를 즉시 제거하려면 클릭합니다.

예외 추가 - 방화벽 예외를 IDS 필터링에 추가하려면 클릭합니다.

네트워크 보호 로그

ESET Endpoint Security 네트워크 보호는 중요한 모든 이벤트를 로그 파일에 저장합니다. 로그 파일을 보려면 기본 프로그램 창 > **설정** > **네트워크** > **로그 표시**를 엽니다.

로그 파일을 사용하여 오류를 검출하고 시스템에 대한 침입을 확인할 수 있습니다. 네트워크 보호 로그에 포함되는 데이터는 다음과 같습니다.

- 이벤트의 날짜 및 시간입니다
- 이벤트 이름
- 소스
- 대상 네트워크 주소
- 네트워크 통신 프로토콜
- 적용한 규칙 또는 웜 이름(식별된 경우)
- 애플리케이션 경로 및 이름
- 해시
- 사용자
- 애플리케이션 지문 생성자(게시자)
- 패키지 이름
- 서비스 이름

이 데이터를 철저하게 분석하면 시스템 보안을 손상시키려는 시도를 검출할 수 있습니다. 그 외에도 잠재적 보안 위험을 나타내는 많은 기타 요인을 통해 위험의 영향을 최소화할 수 있습니다. 이러한 요인으로는 알 수 없는 위치에서의 연결 빈도가 너무 높거나 여러 차례 연결 설정을 시도하는 경우, 애플리케이션 통신을 알 수 없거나 평소에는 사용되지 않는 포트 번호를 사용하는 경우 등이 있습니다.

보안 취약성 악용
실제 악용이 발생하기 전에 네트워크 수준에서 악용 시도가 탐지되고 차단되기 때문에 특정 취약성이 이미 패치된 경우에도 보안 취약성 악용 메시지가 기록됩니다.

ESET 네트워크 보호 문제 해결

설치된 ESET Endpoint Security에 연결 문제가 있는 경우 ESET 네트워크 보호 때문에 문제가 발생하는 것인지 여부를 알 수 있는 몇 가지 방법이 있습니다. 더욱이, ESET 네트워크 보호를 사용하면 연결 문제를 해결하기 위한 새 규칙 또는 예외를 생성하는 데 도움이 됩니다.

ESET 네트워크 보호 문제를 해결하는 데 도움이 되는 다음 항목을 참조하십시오.

- 네트워크 액세스 문제 해결
- 로그에서 규칙 또는 예외 로깅 및 생성
- 방화벽 알림에서 예외 생성
- 네트워크 보호 고급 로깅
- 네트워크 트래픽 검사기 문제 해결

로그에서 규칙 또는 예외 로깅 및 생성

기본적으로 ESET 방화벽은 차단된 모든 연결을 기록하지 않습니다. 네트워크 보호에서 차단된 내용을 보려면 고급 설정 > **도구** > **진단** > **고급 로깅**을 열고 **네트워크 보호 고급 로깅 활성화**를 활성화합니다. 방화벽에서 차단하고 싶지 않은 항목이 로그에 표시되는 경우 해당 항목을 오른쪽 마우스 버튼으로 클릭하고 **앞으로 유사한 이벤트 차단 안 함**을 선택하여 규칙 또는 IDS 규칙을 생성할 수 있습니다. 차단된 모든 연결 로그에는 수천 개의 항목이 포함될 수 있어 이 로그에서 특정 연결을 찾기가 어려울 수도 있습니다. 문제를 해결한 후에는 로깅을 끌 수 있습니다.

로그에 대한 자세한 내용은 로그 파일을 참조하십시오.

네트워크 보호에서 특정 연결을 차단한 순서를 보려면 로깅을 사용하십시오. 더욱이, 로그에서 규칙을 생성하면 정확히 원하는 바를 수행하는 규칙을 생성할 수 있습니다.

로그에서 규칙 생성

ESET Endpoint Security의 새 버전에서는 로그에서 규칙을 생성할 수 있습니다. 기본 메뉴에서 **도구** > **로그 파일**을 선택합니다. 드롭다운 메뉴에서 **네트워크 보호**를 선택하고 원하는 로그 항목을 오른쪽 마우스 버튼으로 클릭한 다음 오른쪽 마우스 버튼 메뉴에서 **앞으로 유사한 이벤트 차단 안 함**을 선택합니다. 알림 창에 새 규칙이 표시됩니다.

로그에서 새 규칙을 생성할 수 있으려면 ESET Endpoint Security을(를) 다음과 같은 설정으로 구성해야 합니다.

1. **고급 설정** > 도구 > **로그 파일**에서 최소 로그 기록 상세 수준을 **분석**으로 설정합니다.
2. 고급 설정 > **보호** > **네트워크 접근 보호** > **네트워크 공격 보호(IDS)** > **고급 옵션** > **침입 탐지**에서 **보안 허점에 대한 들어오는 공격에 대해 알림**을 활성화합니다.

방화벽 알림에서 예외 생성

ESET 방화벽이 악의적인 네트워크 활동을 탐지하면 해당 이벤트를 설명하는 알림 창이 표시됩니다. 이 알림에는 이벤트에 대한 자세한 내용을 살펴보고 원하는 경우 이 이벤트에 대한 예외를 설정할 수 있는 링크가 포함되어 있습니다.

네트워크 애플리케이션 또는 장치가 네트워크 표준을 올바르게 구현하지 않으면 반복적인 방화벽 IDS 알림이 트리거될 수 있습니다. 알림에서 직접 예외를 생성하여 ESET 방화벽이 이 애플리케이션 또는 장치를 검색하지 않도록 할 수 있습니다.

네트워크 보호 고급 로깅

이 기능은 ESET 기술 지원에 보다 복잡한 로그 파일을 제공하기 위해 마련되었습니다. 이 기능은 매우 큰 로그 파일을 생성하여 컴퓨터 성능을 저하시킬 수 있으므로 ESET 기술 지원에서 요청하는 경우에만 사용하십시오.

1. 고급 설정 > **도구** > **진단**으로 이동한 후 **네트워크 보호 고급 로깅 활성화**를 활성화합니다.
2. 발생한 문제를 재현하려고 시도합니다.
3. 네트워크 보호 고급 로깅 비활성화
4. 네트워크 보호 고급 로깅으로 생성된 PCAP 로그 파일은 진단 메모리 덤프가 생성되는 동일한 디렉터리에서 찾을 수 있습니다: *C:\ProgramData\ESET\ESET Security\Diagnostics*

네트워크 트래픽 검사기 문제 해결

브라우저 또는 이메일 클라이언트에 문제가 있는 경우 먼저 네트워크 트래픽 검사기가 그 원인인지 확인해야 합니다. 이렇게 하려면 고급 설정 > **탐지 엔진** > **네트워크 트래픽 검사기**에서 네트워크 트래픽 검사기를 일시적으로 비활성화해 보십시오. 이때 완료한 후에는 네트워크 트래픽 검사기를 다시 켜야 합니다. 그렇지 않으면 브라우저와 이메일 클라이언트가 보호되지 않는 상태로 유지됩니다. 프로토콜 필터링을 해제한 후에 문제가 사라지는 경우 일반적인 문제와 해결 방법 목록은 다음과 같습니다.

업데이트 또는 보안 통신 문제

애플리케이션에 업데이트할 수 없다거나 통신 채널이 안전하지 않다는 메시지가 표시되는 경우

- SSL/TLS가 활성화된 경우 일시적으로 끕니다. 이렇게 해서 도움이 되면 SSL/TLS를 계속 사용하고 문제가 있는 통신을 제외하는 방식으로 업데이트 작업을 만들 수 있습니다.
  비활성화 SSL/TLS. 업데이트를 다시 실행합니다. 암호화된 네트워크 트래픽에 대한 정보를 제공하는 대화 상자가 표시됩니다. 애플리케이션이 문제 해결 중인 애플리케이션과 일치하는지 확인하고, 인증서가 해당 업데이트 서버에서 제공된 것인지 확인합니다. 그런 다음 이 인증서에 대한 동작을 저장하도록 선택하고 [무시]를 클릭합니다. 관련 대화 상자가 더 이상 표시되지 않으면 필터링 모드를 다시 자동으로 전환할 수 있으며, 문제가 해결된 것입니다.
- 해당 애플리케이션이 브라우저 또는 이메일 클라이언트가 아닌 경우 웹 브라우저 보호에서 완전히 제외할 수 있습니다(브라우저 또는 이메일 클라이언트를 완전히 제외하면 보호되지 않음). 과거에 통신이 필터링된 모든 애플리케이션은 예외를 추가할 때 사용자에게 제공된 목록에 이미 있으므로 수동으로 해당 애플리케이션을 추가할 필요가 없습니다.

네트워크의 장치 접근 문제

네트워크에서 장치의 기능을 사용할 수 없는 경우(웹캠의 웹 페이지를 열거나 홈 미디어 플레이어에서 비디오를 재생하는 것을 의미할 수 있음) 해당 IPv4 및 IPv6 주소를 제외된 주소 목록에 추가해 보십시오.

특정 웹 사이트 문제

URL 주소 관리를 사용하여 웹 브라우저 보호에서 특정 웹 사이트를 제외할 수 있습니다. 예를 들어 https://www.gmail.com/intl/en/mail/help/about.html에 접근할 수 없는 경우 제외된 주소 목록에 *gmail.com*을 추가해 보십시오.

"루트 인증서를 가져올 수 있는 일부 애플리케이션이 아직 실행되고 있습니다." 오류

SSL/TLS를 활성화하면 ESET Endpoint Security에서 인증서 저장소로 인증서를 가져와 설치된 애플리케이션이 SSL 프로토콜을 필터링하는 방식을 신뢰하는지 확인합니다. 일부 애플리케이션은 인증서를 가져오기 위해 다시 시작해야 할 수 있습니다. 이러한 애플리케이션으로는 Firefox, Opera가 있습니다. 이러한 애플리케이션이 실행되고 있지 않은지 확인(확인하는 가장 좋은 방법은 작업 관리자를 열고 [프로세스] 탭에 firefox.exe 또는 opera.exe가 없는지 확인하는 것임)한 다음 [다시 시도]를 누르십시오.

신뢰할 수 없는 발급자 또는 잘못된 시그니처에 대한 오류

이 오류는 필시 위에 설명한 가져오기에 실패했다는 의미일 것입니다. 먼저, 언급한 애플리케이션이 실행되고 있지 않은지 확인하십시오. 그런 다음 SSL/TLS를 비활성화했다가 다시 활성화합니다. 그러면 가져오기가 다시 실행됩니다.

네트워크 위협 차단됨

이러한 상황은 컴퓨터의 애플리케이션에서 악의적인 트래픽을 해당 네트워크의 다른 장치에 전송을 시도하여 보안 허점을 악용하거나 시스템에서 포트 검사 시도가 감지되는 등과 같은 경우에 발생할 수 있습니다.

알림에서 위협 유형 및 관련 장치 IP 주소를 찾을 수 있습니다. **이 위협 처리 방법 변경**을 클릭하여 다음 옵션을 표시합니다.

차단 계속 - 탐지된 위협을 차단합니다. 특정 원격 주소에서 이러한 유형의 위협에 대한 알림 수신을 중지하려면 **계속 차단**을 클릭하기 전에 **알리지 않음** 옆에 있는 라디오 버튼을 선택합니다. 이렇게 하면 다음 구성으로 침입 탐지 서비스(IDS) 규칙이 생성됩니다. **차단** - 기본값, **알림** - 아니요, **로그** - 아니요

허용 - 탐지된 위협을 허용하는 침입 탐지 서비스(IDS) 규칙을 생성합니다. **허용**을 클릭하여 규칙 설정을 지정하기 전에 다음 옵션 중 하나를 선택합니다.

- **이 위협이 차단될 때만 알림** - 규칙 구성: **차단** - 아니요, **알림** - 아니요, **로그** - 아니요
- **이 위협이 발생할 때마다 알림** - 규칙 구성: **차단** - 아니요, **알림** - 기본값, **로그** - 기본값
- **알리지 않음** - 규칙 구성: **차단** - 아니요, **알림** - 아니요, **로그** - 아니요

> 이 알림 창에 표시되는 정보는 검출된 위협 유형에 따라 다를 수 있습니다.
> 위협 및 기타 관련 용어에 대한 자세한 내용은 원격 공격 유형이나 검색 유형을 참조하십시오.
> **네트워크에 중복된 IP 주소**를 해결하려면 ESET 지식베이스 문서를 참조하십시오.

연결 설정 - 검색

방화벽은 새로 생성한 각 네트워크 연결을 검색합니다. 활성 방화벽 모드에 따라 새 규칙에 대해 수행할 동작이 결정됩니다. **자동 모드** 또는 **정책 기반 모드**를 활성화한 경우 방화벽이 사용자 상호 작용 없이 미리 정의된 동작을 수행합니다.

대화 모드에서는 새 네트워크 연결을 탐지한 사실과 해당 연결에 대한 자세한 정보를 보고하는 정보 창이 표시됩니다. 연결을 **허용**하거나 **거부**(차단)하도록 선택할 수 있습니다. 대화 상자 창에서 같은 연결을 반복적으로 허용하는 경우에는 해당 연결에 대한 새 규칙을 생성하는 것이 좋습니다. 새 규칙을 생성하려면 **규칙 생성 및 영구 저장**을 선택하고 해당 동작을 방화벽에 대한 새 규칙으로 저장합니다. 그러면 방화벽에서 향후 같은 연결을 인식하는 경우 기존 규칙을 적용합니다. 이 경우 사용자 상호 작용을 필요로 하지 않습니다.

새 규칙을 생성할 때에는 안전한 것으로 알려진 연결만 허용합니다. 모든 연결을 허용하면 방화벽을 제대로

활용할 수 없습니다. 다음은 연결에 대한 중요한 파라미터입니다.

애플리케이션 – 실행 파일 위치와 프로세스 ID입니다. 알 수 없는 애플리케이션과 프로세스에 대한 연결을 허용하지 마십시오.

지문 생성자 - 애플리케이션의 게시자 이름입니다. 텍스트를 클릭하여 회사의 보안 인증서를 표시합니다.

평판 – 연결의 위험 수준입니다. 연결에는 정상(녹색), 알 수 없음(주황색) 또는위험(빨간색)의 위험 수준을 할당하기 위해, 각 연결의 특성, 사용자 수, 검색 시간을 검사하는 일련의 휴리스틱 규칙을 사용합니다. 이 정보는 ESET LiveGrid® 기술을 통해 수집됩니다.

서비스 – 애플리케이션이 Windows 서비스인 경우 해당 서비스의 이름입니다.

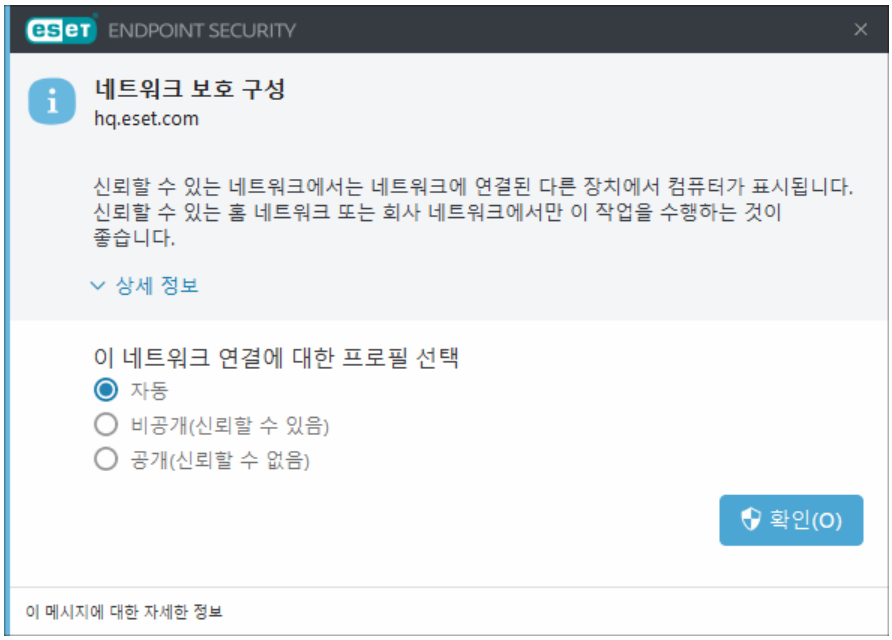
원격 컴퓨터 – 원격 장치의 주소입니다. 신뢰할 수 있는 주소와 알려진 주소에 대한 연결만 허용합니다.

원격 포트 – 통신 포트입니다. 일반 포트의 통신(예: 웹 트래픽 – 포트 번호 80,443)은 일반 환경에서 허용됩니다.

컴퓨터 침입은 원격 시스템을 감염시키기 위해 인터넷과 숨겨진 연결을 사용하는 경우가 많습니다. 규칙이 올바르게 구성되어 있으면 다양한 악성 코드 공격으로부터 보호하는 데 방화벽을 유용하게 사용할 수 있습니다.

새로운 네트워크가 검색됨

기본적으로 새로운 네트워크 연결이 탐지되면 ESET Endpoint Security에서 Windows 설정을 사용합니다. 새 네트워크가 탐지될 때 대화 상자 창을 표시하려면 네트워크 보호 프로필 할당을 **확인**으로 변경합니다. 컴퓨터가 새로운 네트워크에 연결될 때마다 네트워크 보호 구성이 표시됩니다.



다음 네트워크 연결 프로필 중에서 선택할 수 있습니다.

자동 - 각 프로필에 구성된 활성화 도구에 따라 ESET Endpoint Security에서 프로필을 자동으로 선택합니다.

개인 – 신뢰할 수 있는 네트워크(홈 네트워크 또는 회사 네트워크). 컴퓨터에 저장된 공유 파일과 컴퓨터가

다른 네트워크 사용자에게 표시되며, 네트워크의 다른 사용자가 시스템 리소스에 접근할 수 있습니다(공유 파일 및 프린터에 대한 접근이 활성화되고 들어오는 RPC 통신이 활성화되며 원격 데스크톱 공유를 사용할 수 있음). 안전한 로컬 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성된 경우 네트워크 연결에 자동으로 할당됩니다.

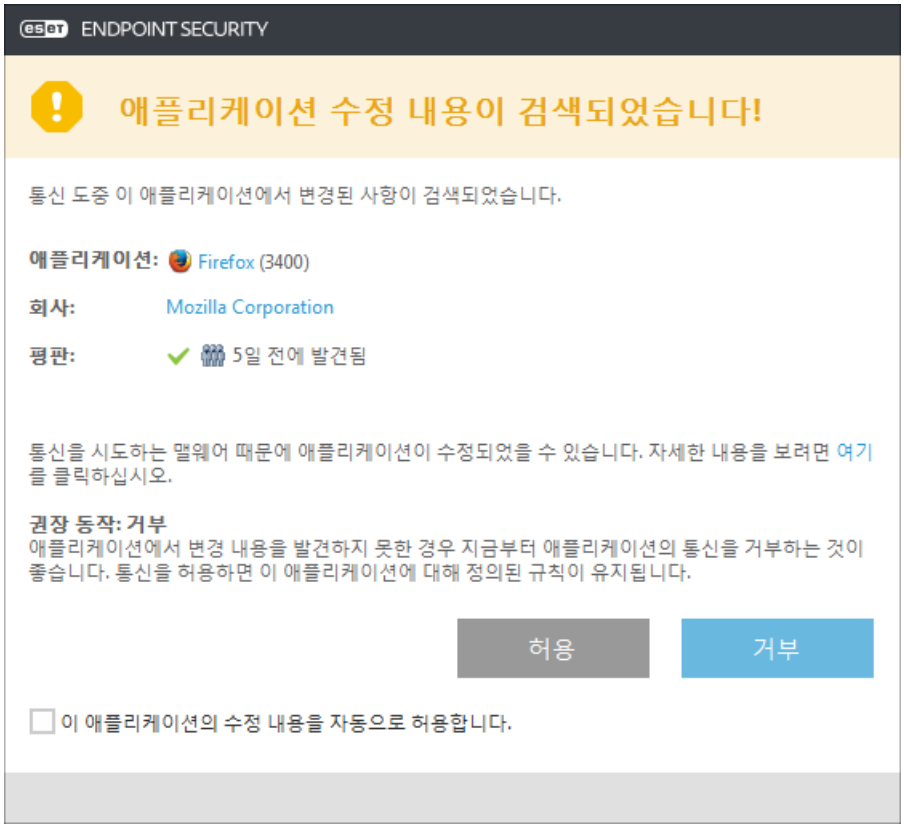
공용 – 신뢰할 수 없는 네트워크(공용 네트워크). 시스템의 파일 및 폴더가 네트워크의 다른 사용자와 공유되거나 다른 사용자에게 표시되지 않으며, 시스템 리소스 공유가 비활성화됩니다. 무선 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성되지 않은 모든 네트워크 연결에 자동으로 할당됩니다.

사용자 정의 프로필 - 드롭다운 메뉴에서 생성한 프로필 중 하나를 선택할 수 있습니다. 이 옵션은 사용자 지정 프로필을 하나 이상 생성한 경우에만 사용할 수 있습니다.

⚠ 네트워크를 잘못 구성하면 컴퓨터에 보안 위험을 유발할 수 있습니다.

애플리케이션 변경

방화벽에서 컴퓨터로부터 나가는 연결을 설정하는 데 사용되는 애플리케이션의 수정 내용을 검색했습니다. 애플리케이션을 새 버전으로 업데이트했기 때문일 수도. 있지만 악성 애플리케이션으로 인한 수정 내용일 수도 있습니다. 적법한 수정이 아니라고 생각되면 연결을 거부하고 최신 버전의 검색 엔진을 사용하여 컴퓨터 검사를 수행하는 것이 좋습니다. 애플리케이션이 확실히 수정되었으며, **이 애플리케이션의 수정 내용을 자동으로 허용합니다.** 확인란이 선택된 상태에서 통신을 허용할 경우 이 애플리케이션에 적용된 규칙이 유지됩니다.



신뢰할 수 있는 들어오는 통신

신뢰 영역 내의 들어오는 연결의 예로는
신뢰 영역 내의 원격 컴퓨터가 컴퓨터에서 실행되는 로컬 애플리케이션과 통신하려는 시도를 들 수 있습니다.

애플리케이션 - 원격 장치가 연결하는 애플리케이션입니다.

애플리케이션 경로 - 애플리케이션의 위치입니다.

Microsoft Store 애플리케이션 - Microsoft Store의 애플리케이션 이름입니다.

지문 생성자 - 애플리케이션의 게시자 이름입니다. 텍스트를 클릭하여 회사의 보안 인증서를 표시합니다.

평판 - ESET LiveGrid® 기술로 획득한 애플리케이션에 대한 평판입니다.

서비스 - 현재 컴퓨터에서 실행 중인 서비스의 이름입니다.

원격 컴퓨터 - 컴퓨터의 애플리케이션과 통신을 설정하려고 하는 원격 컴퓨터입니다.

원격 포트 - 통신에 사용되는 포트입니다.

매시간 확인 - 규칙의 기본 동작이 **확인**으로 설정된 경우 규칙이 트리거될 때마다 대화 상자 창이 표시됩니다.

애플리케이션이 종료될 때까지 저장 - ESET Endpoint Security에서 다음에 다시 시작될 때까지 선택한 동작을 기억합니다.

규칙 생성 및 영구 저장 - 통신을 허용하거나 거부하기 전에 이 옵션을 선택하면 ESET Endpoint Security에서 동작을 기억하여 원격 컴퓨터가 애플리케이션에 다시 연결하는 경우 해당 동작을 사용합니다.

허용 - 들어오는 통신을 허용합니다.

거부 - 들어오는 통신을 거부합니다.

규칙 편집 - 방화벽 규칙 편집기를 사용하여 규칙 속성을 사용자 지정할 수 있습니다.

신뢰할 수 있는 나가는 통신

신뢰 영역 내의 나가는 연결의 예로는
로컬 애플리케이션이 로컬 네트워크 내의 다른 컴퓨터 또는 신뢰 영역에 있는 네트워크 내의 다른 컴퓨터와 연결을 설정하려는 시도를 들 수 있습니다.

애플리케이션 - 원격 장치가 연결하는 애플리케이션입니다.

애플리케이션 경로 - 애플리케이션의 위치입니다.

Microsoft Store 애플리케이션 - Microsoft Store의 애플리케이션 이름입니다.

지문 생성자 - 애플리케이션의 게시자 이름입니다. 텍스트를 클릭하여 회사의 보안 인증서를 표시합니다.

평판 - ESET LiveGrid® 기술로 획득한 애플리케이션에 대한 평판입니다.

서비스 - 현재 컴퓨터에서 실행 중인 서비스의 이름입니다.

원격 컴퓨터 - 컴퓨터의 애플리케이션과 통신을 설정하려고 하는 원격 컴퓨터입니다.

원격 포트 - 통신에 사용되는 포트입니다.

매시간 확인 - 규칙의 기본 동작이 **확인**으로 설정된 경우 규칙이 트리거될 때마다 대화 상자 창이 표시됩니다.

애플리케이션이 종료될 때까지 저장 - ESET Endpoint Security에서 다음에 다시 시작될 때까지 선택한 동작을 기억합니다.

규칙 생성 및 영구 저장 - 통신을 허용하거나 거부하기 전에 이 옵션을 선택하면 ESET Endpoint Security에서 동작을 기억하여 원격 컴퓨터가 애플리케이션에 다시 연결하는 경우 해당 동작을 사용합니다.

허용 - 들어오는 통신을 허용합니다.

거부 - 들어오는 통신을 거부합니다.

규칙 편집 - 방화벽 규칙 편집기를 사용하여 규칙 속성을 사용자 지정할 수 있습니다.

들어오는 통신

들어오는 인터넷 연결의 예로는:
원격 컴퓨터가 컴퓨터에서 실행되는 애플리케이션과 통신하려는 시도를 들 수 있습니다.

애플리케이션 - 원격 장치가 연결하는 애플리케이션입니다.

애플리케이션 경로 - 애플리케이션의 위치입니다.

Microsoft Store 애플리케이션 - Microsoft Store의 애플리케이션 이름입니다.

지문 생성자 - 애플리케이션의 게시자 이름입니다. 텍스트를 클릭하여 회사의 보안 인증서를 표시합니다.

평판 - ESET LiveGrid® 기술로 획득한 애플리케이션에 대한 평판입니다.

서비스 - 현재 컴퓨터에서 실행 중인 서비스의 이름입니다.

원격 컴퓨터 - 컴퓨터의 애플리케이션과 통신을 설정하려고 하는 원격 컴퓨터입니다.

원격 포트 - 통신에 사용되는 포트입니다.

매시간 확인 - 규칙의 기본 동작이 **확인**으로 설정된 경우 규칙이 트리거될 때마다 대화 상자 창이 표시됩니다.

애플리케이션이 종료될 때까지 저장 - ESET Endpoint Security에서 다음에 다시 시작될 때까지 선택한 동작을 기억합니다.

규칙 생성 및 영구 저장 - 통신을 허용하거나 거부하기 전에 이 옵션을 선택하면 ESET Endpoint Security에서 동작을 기억하여 원격 컴퓨터가 애플리케이션에 다시 연결하는 경우 해당 동작을 사용합니다.

허용 - 들어오는 통신을 허용합니다.

거부 - 들어오는 통신을 거부합니다.

규칙 편집 - 방화벽 규칙 편집기를 사용하여 규칙 속성을 사용자 지정할 수 있습니다.

나가는 통신

나가는 인터넷 연결의 예로는:
로컬 애플리케이션이 인터넷 연결을 설정하려는 시도를 들 수 있습니다.

애플리케이션 - 원격 장치가 연결하는 애플리케이션입니다.

애플리케이션 경로 - 애플리케이션의 위치입니다.

Microsoft Store 애플리케이션 - Microsoft Store의 애플리케이션 이름입니다.

지문 생성자 - 애플리케이션의 게시자 이름입니다. 텍스트를 클릭하여 회사의 보안 인증서를 표시합니다.

평판 - ESET LiveGrid® 기술로 획득한 애플리케이션에 대한 평판입니다.

서비스 - 현재 컴퓨터에서 실행 중인 서비스의 이름입니다.

원격 컴퓨터 - 컴퓨터의 애플리케이션과 통신을 설정하려고 하는 원격 컴퓨터입니다.

원격 포트 - 통신에 사용되는 포트입니다.

매시간 확인 - 규칙의 기본 동작이 **확인**으로 설정된 경우 규칙이 트리거될 때마다 대화 상자 창이 표시됩니다.

애플리케이션이 종료될 때까지 저장 - ESET Endpoint Security에서 다음에 다시 시작될 때까지 선택한 동작을 기억합니다.

규칙 생성 및 영구 저장 - 통신을 허용하거나 거부하기 전에 이 옵션을 선택하면 ESET Endpoint Security에서 동작을 기억하여 원격 컴퓨터가 애플리케이션에 다시 연결하는 경우 해당 동작을 사용합니다.

허용 - 들어오는 통신을 허용합니다.

거부 - 들어오는 통신을 거부합니다.

규칙 편집 - 방화벽 규칙 편집기를 사용하여 규칙 속성을 사용자 지정할 수 있습니다.

연결 보기 설정

다음을 비롯한 추가 옵션을 보려면 연결을 오른쪽 마우스 버튼으로 클릭합니다.

호스트 이름 확인 - 가능한 경우 모든 네트워크 주소가 숫자 IP 주소 형식이 아닌 DNS 형식으로 표시됩니다.

TCP 연결만 표시 - TCP 프로토콜 제품군에 속하는 연결만 목록에 표시됩니다.

수신 중인 연결 표시 - 현재 통신이 설정되어 있지 않지만 시스템이 포트를 열고 연결을 대기 중인 연결만 표시하려면 이 옵션을 선택합니다.

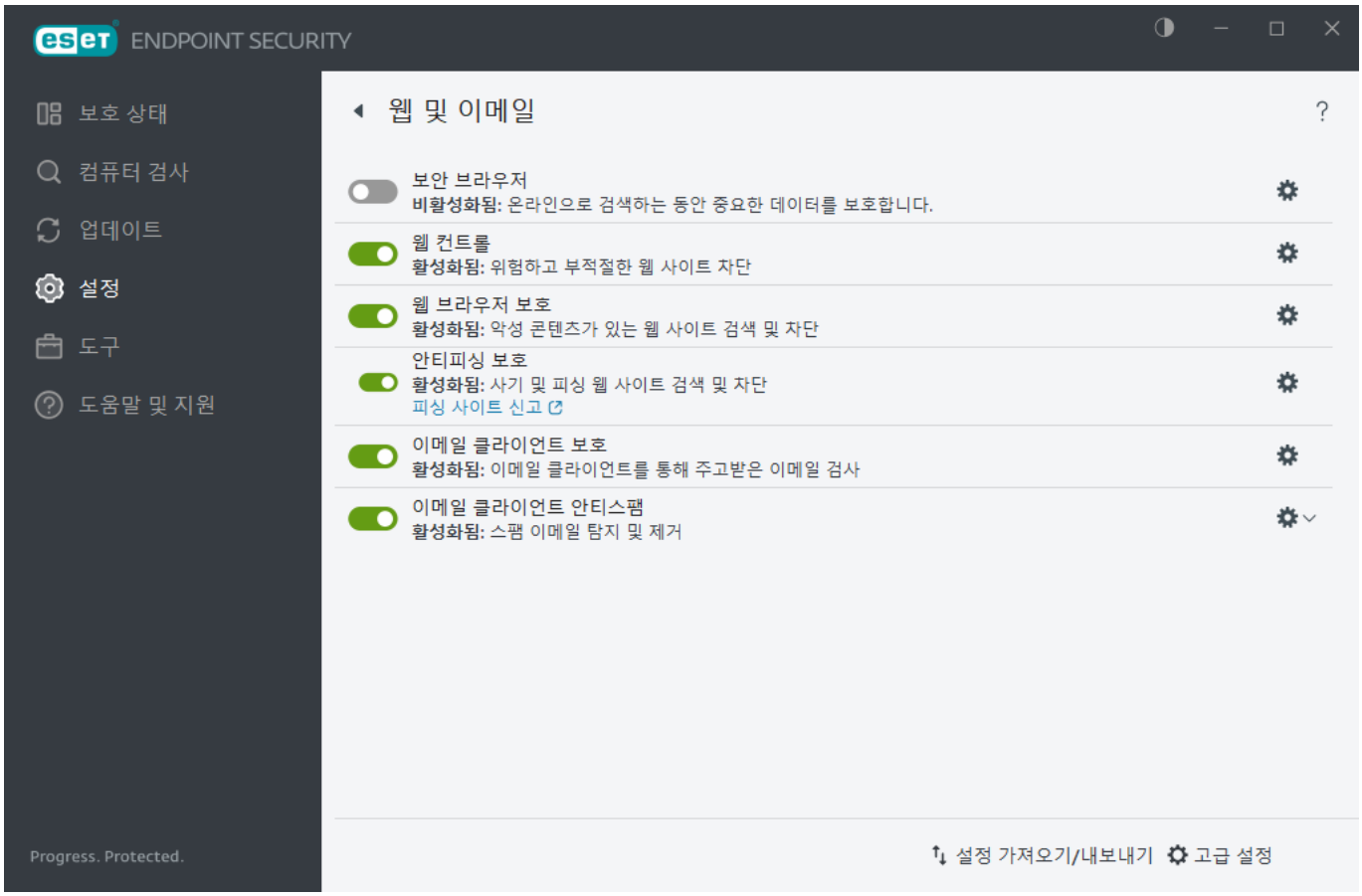
컴퓨터 내 연결 표시 - 원격 측이 로컬 시스템인 연결(localhost 연결)만 표시하려면 이 옵션을 선택합니다.

웹 및 이메일

인터넷 연결은 개인용 컴퓨터의 일반적인 기능일 뿐만 아니라 악성 코드를 전송하는 주된 수단이기도 합니다. 기본 프로그램 창 > **설정** > **웹 및 이메일**을 열어 인터넷 보호를 강화하는 ESET Endpoint Security 기능을 구성합니다.

개별 보호 모듈을 일시 중지하거나 비활성화하려면 토글 아이콘을 클릭합니다.

⚠ 보호 모듈을 끄면 컴퓨터의 보호 수준이 저하될 수 있습니다.



보호 모듈 옆의 톱니바퀴 아이콘을 클릭하여 모듈 고급 설정에 접근합니다.

안전한 브라우저 - 온라인으로 검색하는 동안 중요한 데이터를 보호합니다.

웹 컨트롤 모듈에서는 관리자에게 워크스테이션을 보호하고 인터넷 검색에 대한 제한을 설정하는 데 도움이 되는 자동화된 도구를 제공하는 설정을 구성할 수 있습니다. 웹 컨트롤 기능은 부적절하거나 유해한 콘텐츠가 포함된 페이지에 접근하지 못하도록 방지합니다. 자세한 내용은 웹 컨트롤을 참조하십시오.

웹 브라우저 보호는 HTTP/HTTPS 통신에서 악성코드와 피싱을 검사합니다. 웹 브라우저 보호는 문제를 해결하기 위한 경우에만 꺼야 합니다.

안티피싱 보호는 피싱 콘텐츠를 배포하는 것으로 알려진 웹 페이지를 차단할 수 있도록 합니다. 안티피싱을 활성화된 상태로 두는 것이 좋습니다.

피싱 사이트 보고 - 분석을 위해 ESET에 피싱/악성 웹 사이트를 보고합니다.

> 웹 사이트를 ESET로 전송하기 전에 다음 조건 중 하나 이상을 충족하는지 확인하십시오.
> • 웹 사이트가 검출되지 않음.
> • 웹 사이트가 위협으로 잘못 검출됨. 이 경우 잘못 차단된 페이지를 신고할 수 있습니다.

이메일 클라이언트 보호는 POP3(S) 및 IMAP(S) 프로토콜을 통해 받은 이메일 통신을 제어합니다. ESET Endpoint Security는 이메일 클라이언트용 플러그인 프로그램을 사용하여 이메일 클라이언트의 모든 통신을 제어합니다.

이메일 클라이언트 안티스팸은 원치 않는 이메일 메시지를 필터링합니다.

이메일 클라이언트 안티스팸의 경우 톱니바퀴 아이콘을 클릭하고 다음 옵션 중에서 선택합니다.

- **구성** - 이메일 클라이언트 안티스팸의 고급 설정을 엽니다.
- **사용자의 주소 목록**(활성화된 경우) - 대화 상자 창을 열고 주소를 추가, 편집, 제거하여 안티스팸 규칙을 정의합니다.
- **전체 주소 목록**(활성화된 경우) - 대화 상자 창을 열고 주소를 추가, 편집, 제거하여 안티스팸 규칙을 정의합니다. 이 목록의 규칙은 모든 사용자에게 적용됩니다.

안티피싱 보호

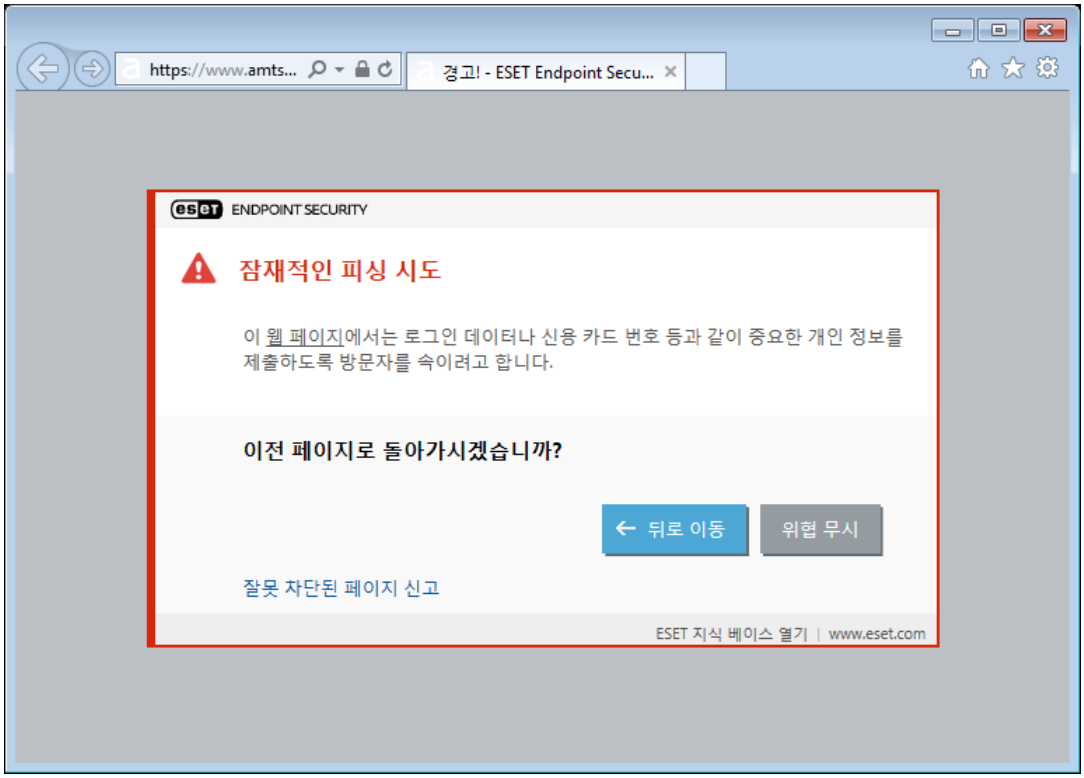
피싱은 소셜 엔지니어링(기밀 정보를 얻기 위해 사용자를 조작)을 사용하는 범죄 행위입니다. 피싱은 은행 계좌 번호, PIN 등과 같은 중요한 데이터에 액세스하는 데 사용됩니다. 자세한 내용은 용어집을 참조하십시오. ESET Endpoint Security에는 안티피싱 보호 기능이 포함되어 이러한 유형의 콘텐츠를 배포하는 것으로 알려진 웹 페이지를 차단합니다.

안티피싱 보호는 기본적으로 활성화되어 있습니다. 이 설정은 고급 설정 > **보호** > **웹 브라우저 보호**에서 구성할 수 있습니다.

ESET Endpoint Security의 안티피싱 보호에 대한 자세한 내용을 보려면 지식 베이스 문서를 참조하십시오.

피싱 웹 사이트 접근

인식된 피싱 웹 사이트에 액세스하면 웹 브라우저에 다음 대화 상자가 표시됩니다. 계속해서 이 웹 사이트에 접근하려면 **위협 무시**(권장되지 않음)를 클릭합니다.



허용 목록에 포함된 잠재적인 피싱 웹 사이트는 기본적으로 몇 시간 후에 만료됩니다. 웹 사이트를 영구히 허용하려면 URL 주소 관리 도구를 사용합니다. 고급 설정 > **보호** > **웹 브라우저 보호** > **URL 주소 관리** > **주소 목록** > **편집**에서 편집하려는 웹 사이트를 목록에 추가합니다.

피싱 사이트 신고

잘못 차단된 페이지 보고 링크를 사용하면 위협으로 잘못 탐지된 웹 사이트를 보고할 수 있습니다.

웹 사이트를 이메일로 전송할 수도 있습니다. samples@eset.com으로 이메일을 전송하십시오. 제목에 내용을 설명하고 이메일에 웹 사이트에 대한 정보(예: 이 웹 사이트를 소개받은 웹 사이트, 웹 사이트에 대한 소식을 들은 방식)를 최대한 많이 추가하십시오.

설정 가져오기 및 내보내기

설정 메뉴에서 사용자 지정된 ESET Endpoint Security.xml 구성 파일을 가져오거나 내보낼 수 있습니다.

그림이 포함된 지침

영어 및 기타 여러 언어로 제공되는 그림이 포함된 지침은 .xml 파일을 사용하여 ESET 구성 설정 가져오기 또는 내보내기를 참조하십시오.

구성 파일을 가져오고 내보내는 작업은 나중에 사용하기 위해 ESET Endpoint Security의 현재 구성을 백업해야 할 경우 도움이 됩니다. 또한 설정 내보내기 옵션은 여러 시스템에서 기본 설정 구성을 이용하려는 경우에 편리합니다. .xml 파일을 가져와서 이러한 설정을 전송할 수 있습니다.

구성을 가져오려면 기본 프로그램 창에서 **설정** > **설정 가져오기/내보내기**를 클릭한 다음 **설정 가져오기**를 선택합니다. 구성 파일의 이름을 입력하거나 **...** 버튼을 클릭하여 가져올 구성 파일을 찾습니다.

구성을 내보내려면 기본 프로그램 창에서 **설정** > **설정 가져오기/내보내기**를. 클릭하고 **설정 가져오기**를 선택한 다음, 전체 파일 경로를 이름과 함께 입력합니다. **...**를 클릭하여 구성 파일을 저장할 컴퓨터 위치로 이

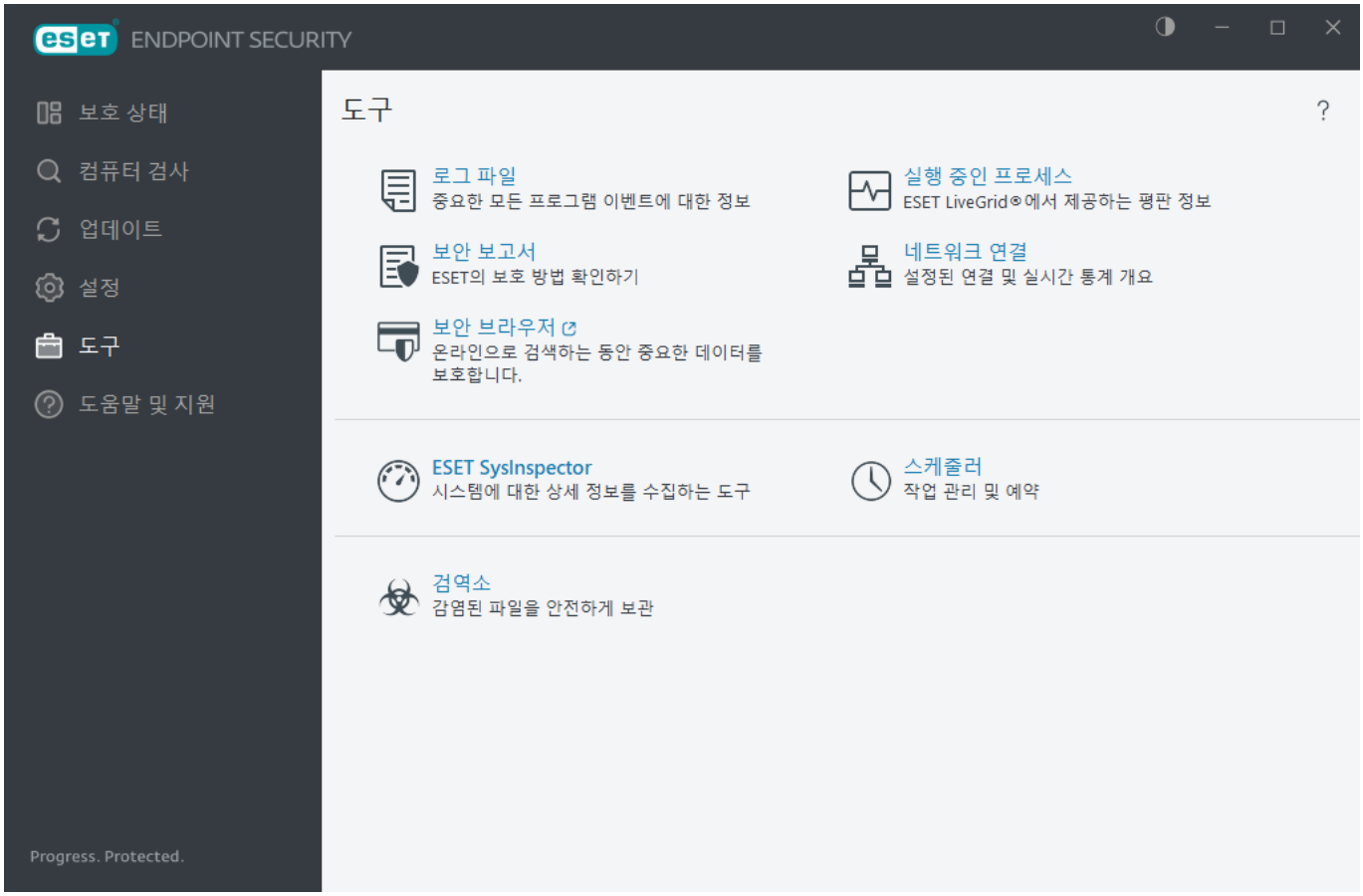
동합니다.

> 지정된 디렉터리에 내보낸 파일을 작성할 권한이 없으면 설정을 내보내는 동안 오류가 발생할 수 있습니다.

도구

도구 메뉴에는 프로그램을 간편하게 관리하는 데 도움이 되고 고급 사용자를 위한 추가 옵션을 제공하는 모듈이 포함되어 있습니다.

- 로그 파일
- 실행 중인 프로세스 (ESET LiveGrid®가 ESET Endpoint Security에서 활성화된 경우)
- 보안 보고서 (관리되지 않는 엔드포인트용)
- 네트워크 연결 (방화벽이 ESET Endpoint Security에서 활성화된 경우)
- ESET SysInspector
- 스케줄러
- 분석용 샘플 전송 – 분석하기 위해 감염 의심 파일을 ESET 연구소로 전송할 수 있습니다(ESET LiveGrid® 구성에 따라 사용하지 못할 수도 있음).
- 검역소



로그 파일

로그 파일은 발생한 모든 중요 프로그램 이벤트에 대한 정보를 포함하고 있고 검출된 위협에 대한 개요를 제공합니다. 로그는 시스템을 분석하고, 위협을 검출하고, 문제를 해결하는 데 사용하는 기본 도구입니다. 로깅은 사용자 상호 작용 없이 백그라운드에서 수행됩니다. 정보는 현재 로그 상세 수준 설정에 따라 기록됩니다. ESET Endpoint Security 환경에서 직접 텍스트 메시지 및 로그를 볼 수 있습니다. 로그 파일을 압축파일로 만들 수도 있습니다.

기본 프로그램 창에서 **도구** > **로그 파일**을 클릭하여 로그 파일에 접근할 수 있습니다. **로그** 드롭다운 메뉴에서 원하는 로그 유형을 선택합니다. 다음과 같은 로그를 사용할 수 있습니다.

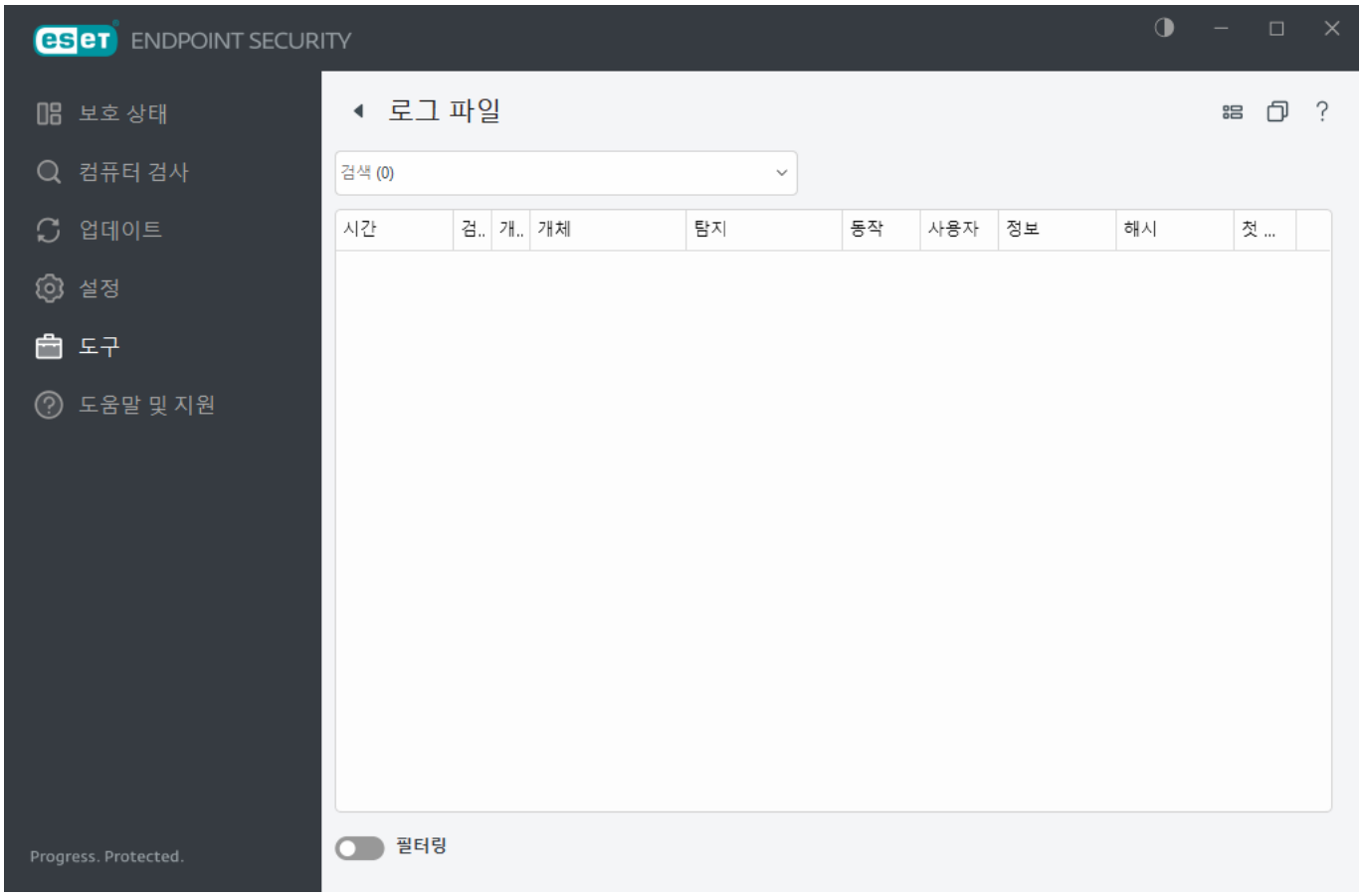
- **검출** - 이 로그는 검출 및 ESET Endpoint Security 모듈에서 검출된 침입에 대한 자세한 정보를 제공합니다. 정보에는 검출 시간, 검출 이름, 위치, 수행된 동작 및 침입 검출 시 로그인한 사용자 이름이 포함됩니다. 별도의 창에 자세한 내용을 표시하려면 로그 항목을 두 번 클릭합니다. 치료되지 않은 침입은 항상 연한 빨간색 배경에 빨간색 텍스트로 표시되며, 치료된 침입은 흰색 배경에 노란색 텍스트로 표시됩니다. 치료 안 된 PUA, 즉 잠재적으로 안전하지 않은 애플리케이션은 흰색 배경에 노란색 텍스트로 표시됩니다.
- **이벤트** - ESET Endpoint Security에서 수행된 중요한 모든 동작이 이벤트 로그에 기록됩니다. 이벤트 로그에는 프로그램에서 발생한 이벤트 및 오류에 대한 정보가 포함되어 있습니다. 이 로그는 시스템 관리자 및 사용자가 문제를 해결하는 데 도움이 되도록 설계되었습니다. 여기서 찾은 정보를 통해 프로그램에서 발생한 문제에 대한 해결책을 찾을 수 있도록 도움을 주기 위해 고안되었습니다.
- **컴퓨터 검사** - 모든 검사 결과가 이 창에 표시됩니다. 각 행은 단일 컴퓨터 제어에 해당됩니다. 각 검사의 상세 정보를 보려면 항목을 두 번 클릭합니다.
- **차단된 파일** – ESET Enterprise Inspector에 연결된 경우 접근할 수 없는 차단된 파일 기록을 포함합니다. 프로토콜에는 파일을 차단한 이유와 소스 모듈 및 파일을 실행한 애플리케이션과 사용자도 표시됩니

다. 자세한 내용은 ESET Enterprise Inspector 온라인 사용자 설명서를 참조하십시오.

- **전송된 파일** – 분석을 위해 ESET LiveGrid® 또는 ESET LiveGuard로 전송된 파일의 레코드를 포함합니다.
- **감사 로그** – 각 로그에는 변경이 수행된 날짜와 시간, 변경 유형, 설명, 소스 및 사용자에 대한 정보가 포함됩니다. 자세한 내용은 감사 로그를 참조하십시오.
- **HIPS** - 기록을 위해 지정된 특정 규칙의 레코드를 포함합니다. 이 프로토콜은 작업을 호출한 애플리케이션, 결과(규칙이 허용되는지 또는 금지되는지 여부) 및 생성된 규칙 이름을 표시합니다.
- **안전한 브라우저** - 브라우저에 로드된 확인되지 않은/신뢰할 수 없는 파일의 레코드를 포함합니다.
- **네트워크 보호** - 방화벽 로그에는 네트워크 공격 보호(IDS) 또는 방화벽을 통해 탐지된 모든 원격 공격이 표시됩니다. 이 로그에서는 컴퓨터의 모든 공격에 대한 정보를 찾을 수 있습니다. 이벤트 열에 검출된 공격이 나열됩니다. 소스 열에는 공격자에 대한 자세한 내용이 표시됩니다. 프로토콜 열에는 공격에 사용된 통신 프로토콜이 표시됩니다. 네트워크 보호 로그를 분석하면 시스템 침입 시도를 적시에 탐지하여 시스템에 대한 무단 접근을 방지하는 데 도움이 될 수 있습니다. 네트워크 공격에 대한 자세한 내용 IDS 및 고급 옵션을 참조하십시오.

- **필터링된 웹 사이트** - 이 목록은 웹 브라우저 보호 또는 웹 컨트롤에 의해 차단된 웹 사이트의 목록을 보려는 경우에 유용합니다. 이러한 로그에서 특정 웹 사이트에 대한 연결을 연 시간, URL, 사용자 및 애플리케이션을 확인할 수 있습니다.

- **이메일 클라이언트 안티스팸** - 스팸으로 표시된 이메일 메시지와 관련된 기록을 포함합니다.
- **웹 컨트롤** - 차단되거나 허용된 URL 주소와 해당 주소의 분류 방법에 대한 상세 정보를 표시합니다. 수행된 동작 열은 필터링 규칙이 적용된 방식을 보여줍니다.
- **장치 제어** - 컴퓨터에 연결된 이동식 미디어나 장치의 레코드를 포함합니다. 장치 제어 규칙이 있는 장치만 로그 파일에 기록됩니다. 규칙이 연결된 장치와 일치하지 않으면 연결된 장치의 로그 항목이 생성되지 않습니다. 여기에서 장치 유형, 일련 번호, 공급업체 이름, 미디어 크기(해당하는 경우) 등의 상세 정보도 확인할 수 있습니다.



로그의 내용을 선택하고 Ctrl + C**를 눌러 클립보드에 복사합니다.** 여러 항목을 선택하려면 Ctrl +

Shift를 누른 상태에서 선택합니다.

필터링을 클릭하여 필터링 기준을 정의할 수 있는 로그 필터링 창을 엽니다.

마우스 오른쪽 버튼으로 특정 레코드를 클릭하여 오른쪽 마우스 버튼 메뉴를 엽니다. 오른쪽 마우스 버튼 메뉴에서 사용할 수 있는 옵션은 다음과 같습니다.

- **표시** - 새 창에서 선택한 로그에 대한 보다 자세한 정보를 표시합니다.
- **같은 레코드 필터링** - 이 필터를 활성화하고 나면 같은 형식(분석, 경고 등)의 레코드만 표시됩니다.
- **필터링** - 이 옵션을 클릭하면 로그 필터링 창에서 특정 로그 항목에 대한 필터링 기준을 정의할 수 있습니다.
- **필터 활성화** - 필터 설정을 활성화합니다.
- **필터 비활성화** - 위에서 설명한 것처럼 모든 필터 설정을 지웁니다.
- **복사/모두 복사** - 창에 있는 모든 레코드에 대한 정보를 복사합니다.
- **셀 복사**—마우스 오른쪽 버튼을 클릭한 셀의 내용을 복사합니다.
- **삭제/모두 삭제** - 선택한 레코드를 삭제하거나 표시된 모든 레코드를 삭제합니다. 이 동작을 수행하려면 관리자 권한이 필요합니다.
- **내보내기** - 레코드에 대한 정보를 XML 형식으로 내보냅니다.
- **모두 내보내기** - 모든 레코드에 대한 정보를 XML 형식으로 내보냅니다.
- **찾기/다음 찾기/이전 찾기** – 이 옵션을 클릭하면 로그 필터링 창을 사용하여 특정 항목을 강조 표시할 필터링 기준을 정의할 수 있습니다.
- **제외 생성** – 마법사를 사용하여 새 탐지 제외를 생성합니다(악성코드 탐지에는 사용할 수 없음).

로그 필터링

도구 > 로그 파일의 **필터링**을 클릭하여 필터링 기준을 정의합니다.

로그 필터링 기능은 특히 레코드가 많은 경우, 정보를 찾는 데 도움이 됩니다. 예를 들어 특정 유형의 이벤트, 상태 또는 기간을 찾는 경우 필터링 기능으로 로그 레코드의 범위를 좁힐 수 있습니다. 특정 검색 옵션을 지정하여 로그 레코드를 필터링하면 관련된 레코드만 (이러한 검색 옵션에 따라) 로그 파일 창에 표시됩니다.

검색할 키워드를 **텍스트 찾기** 필드에 입력합니다. **열에서 검색** 드롭다운 메뉴를 사용하여 검색 범위를 좁힙니다. **레코드 로그 종류** 드롭다운 메뉴에서 하나 이상의 레코드를 선택합니다. 결과를 표시할 **기간**을 정의합니다. **단어 단위로** 또는 **대소문자 구분** 같은 추가 검색 옵션도 사용할 수 있습니다.

텍스트 찾기

문자열(단어 또는 단어의 일부)을 입력합니다. 이 문자열이 포함된 레코드만 표시됩니다. 다른 레코드는 생략됩니다.

열에서 검색

검색할 때 고려할 열을 선택합니다. 검색에 사용할 하나 이상의 열을 선택할 수 있습니다.

레코드 종류

드롭다운 메뉴에서 하나 이상의 로그 레코드 종류를 선택합니다.

- **분석** - 위의 프로그램과 모든 레코드를 미세 조정하는 데 필요한 정보를 기록합니다.

- **정보** - 성공한 업데이트 메시지를 포함한 정보 메시지와 위의 모든 레코드를 기록합니다.
- **경고** - 심각한 오류 및 경고 메시지를 기록합니다.
- **오류** - "파일을 다운로드하는 중 오류 발생"과 같은 오류 및 심각한 오류가 기록됩니다.
- **주요** - 심각한 오류(안티바이러스 보호

기간

결과를 표시할 기간을 정의합니다:

- **지정되지 않음**(기본값) - 기간 내에서 검색하지 않고 전체 로그를 검색합니다.
- **어제**
- **지난주**
- **지난달**
- **기간** - 정확한 기간(시작: 및 종료:)을 지정하여 지정된 기간의 레코드만 필터링할 수 있습니다.

단어 단위로

보다 정확한 결과를 위해 단어 전체를 검색하려는 경우 이 확인란을 사용합니다.

대소문자 구분

필터링할 때 대문자 또는 소문자의 사용이 중요하다면 이 옵션을 **활성화**합니다. 필터링/검색 옵션을 구성한 후 **확인**을 클릭하여 필터링된 로그 레코드를 표시하거나, 찾기를 클릭하여 검색을 시작합니다. 로그 파일은 현재 위치(강조 표시된 레코드)에서 시작해 위에서 아래로 검색됩니다. 해당하는 첫 번째 레코드를 찾으면 검색이 중지됩니다. **F3** 키를 눌러 다음 레코드를 검색하거나, 오른쪽 마우스 버튼 메뉴에서 **찾기**를 선택해 검색 옵션을 구체화합니다.

감사 로그

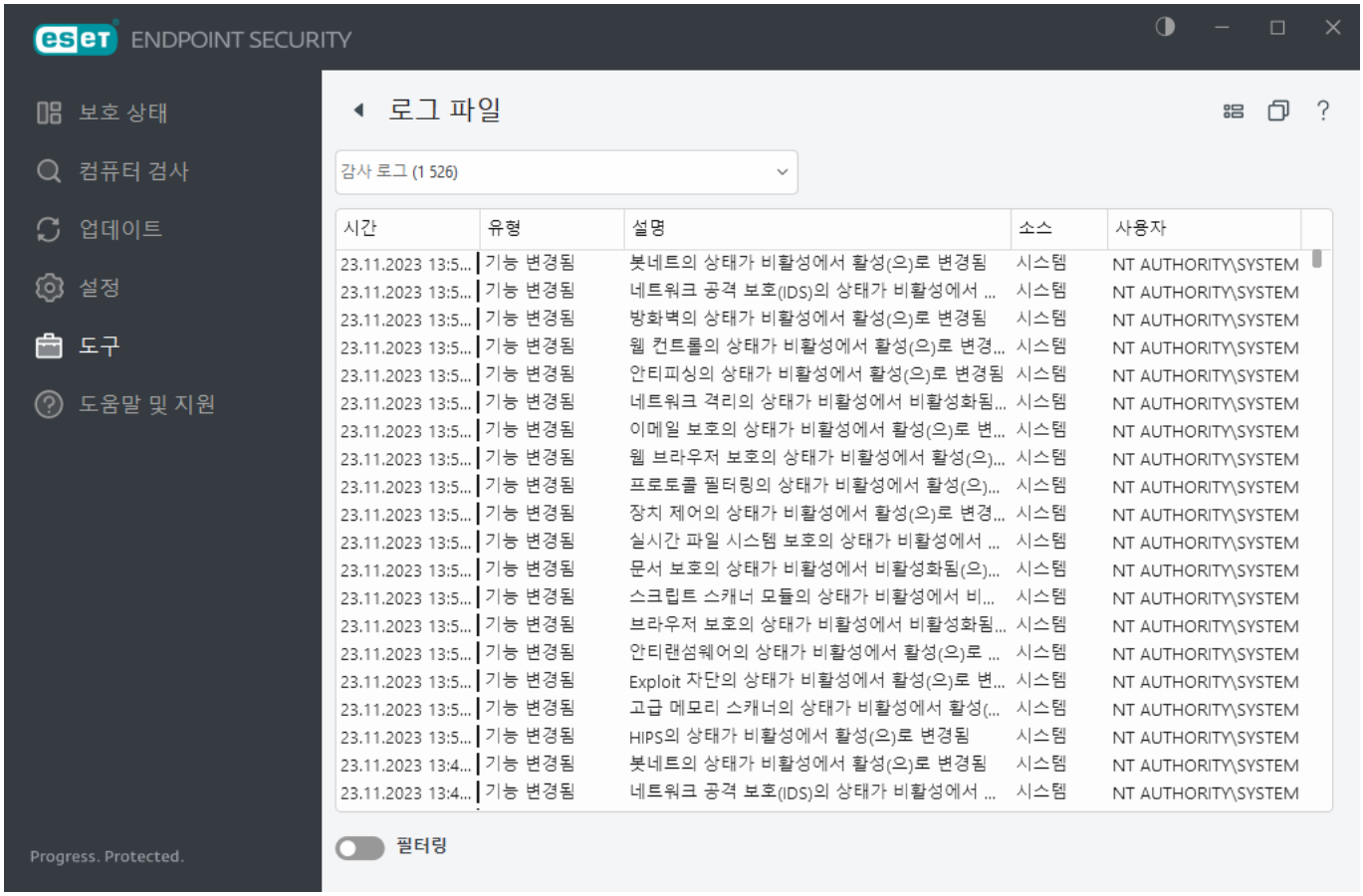
일반적으로 엔터프라이즈 환경에는 엔드포인트 구성을 위해 정의된 접근 권한이 있는 여러 사용자가 있습니다. 제품 구성을 수정하면 제품 작동 방식이 크게 달라질 수 있으므로 관리자는 사용자가 수행한 변경 사항을 추적하여 관리자가 나중에 동일하거나 유사한 문제를 신속하게 파악 및 해결하고, 문제 발생을 방지할 수 있도록 지원해야 합니다.

감사 로그는 문제의 원인을 식별하기 위한 새로운 로깅 유형입니다. 감사 로그는 구성 또는 보호 상태의 변경 사항을 추적하고 나중에 참조할 수 있도록 스냅숏을 기록합니다.

감사 로그를 보려면 기본 메뉴에서 **도구**를 클릭하고 **로그 파일**을 클릭하여 드롭다운 메뉴에서 **감사 로그**를 선택합니다.

감사 로그에는 다음에 관한 정보가 포함되어 있습니다.

- 시간 - 변경이 수행된 시간
- 유형 - 변경된 설정 또는 기능의 유형
- 설명 - 변경된 정확한 사항, 변경된 설정의 개수 및 변경된 설정 부분
- 소스 - 변경의 소스 위치
- 사용자 - 변경한 사람



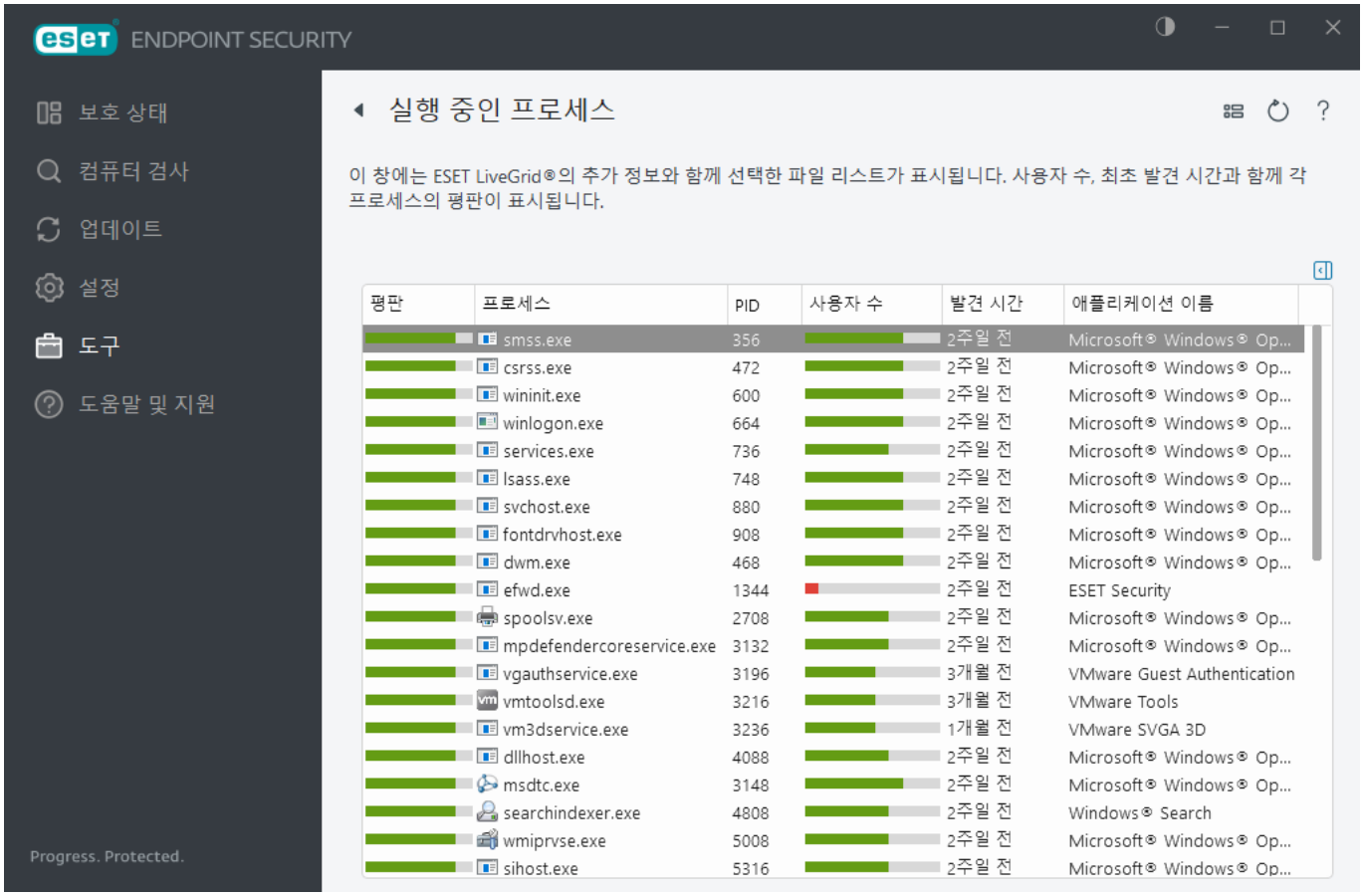
로그 파일 창에서 감사 로그의 **설정이 변경된** 유형을 오른쪽 마우스 버튼으로 클릭하고 오른쪽 마우스 버튼 메뉴에서 **변경 사항 표시**를 선택하면 수행된 변경에 관한 자세한 정보가 표시됩니다. 또한 오른쪽 마우스 버튼 메뉴에서 **복원**을 클릭하여 변경된 설정을 복원할 수 있습니다(ESET PROTECT에서 관리되는 제품에는 사용할 수 없음). 오른쪽 마우스 버튼 메뉴에서 **모두 삭제**를 선택하면 이 동작에 관한 정보가 포함된 로그가 생성됩니다.

고급 설정 > 도구 > **로그 파일**에서 **자동으로 로그 파일 최적화**가 활성화되면 감사 로그가 다른 로그로 자동 조각 모음됩니다.

고급 설정 > 도구 > **로그 파일**에서 **다음 기간이 지난 기록 자동 삭제**가 활성화되면 지정된 일수보다 오래된 로그 항목이 자동으로 삭제됩니다.

실행 중인 프로세스

실행 중인 프로세스는 컴퓨터에서 실행 중인 프로그램이나 프로세스를 표시하며, ESET가 새로운 침입에 대한 정보를 즉각적이고 지속적으로 확인할 수 있도록 해줍니다. ESET Endpoint Security는 ESET LiveGrid® 기술이 활성화된 상태로 사용자를 보호하기 위해 실행 중인 프로세스에 대한 자세한 정보를 제공합니다.



평판 - 대부분의 경우 ESET Endpoint Security 및 ESET LiveGrid® 기술에서는 각 개체의 특성을 파악한 다음 악의적인 활동의 잠재성에 대한 심각도를 매기는 일련의 인공지능 규칙을 사용하여 개체(파일, 프로세스, 레지스트리 키 등)에 위험 수준을 지정합니다. 이러한 인공지능 규칙을 바탕으로 개체에 9 - 최고의 평판(녹색)에서 0 - 최악의 평판(빨간색)까지 평판 수준이 지정됩니다.

프로세스 - 현재 컴퓨터에서 실행 중인 프로그램 또는 프로세스의 이미지 이름입니다. Windows 작업 관리자를 사용하여 컴퓨터에서 실행 중인 모든 프로세스를 볼 수도 있습니다. 작업 관리자는 작업 표시줄의 빈 영역을 오른쪽 마우스 버튼으로 클릭한 다음 [작업 관리자]를 클릭하거나, 키보드에서 **Ctrl+Shift+Esc**를 눌러 열 수 있습니다.

PID - Windows 운영 체제에서 실행 중인 프로세스의 ID입니다.

녹색으로 표시된 알려진 애플리케이션은 분명히 감염되지 않아(허용 목록에 포함됨) 검사에서 제외됩니다. 이로써 컴퓨터에서 실시간 파일 시스템 보호나 수동 컴퓨터 검사 시 검사 속도가 향상됩니다.

사용자 수 - 지정된 애플리케이션을 사용하는 사용자 수입니다. 이 정보는 ESET LiveGrid® 기술을 통해 수집됩니다.

검색 시간 - ESET LiveGrid® 기술에 의해 애플리케이션이 검색된 이후의 시간입니다.

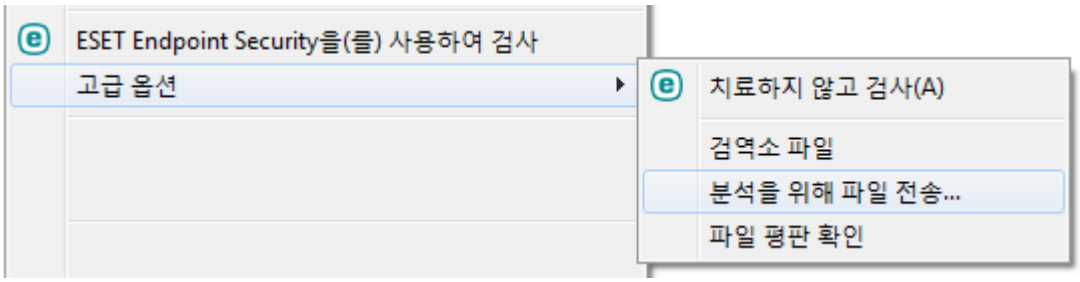
애플리케이션이 알 수 없음 (주황색) 보안 수준으로 지정된 경우 이 애플리케이션이 악성 소프트웨어가 아닐 수도 있습니다. 일반적으로 이 애플리케이션은 새로운 애플리케이션인 경우가 많습니다. 파일에 대해 확신이 서지 않는 경우 분석을 위해 파일 전송 기능을 사용하여 파일을 ESET 바이러스 연구소로 보냅니다. 이 파일이 악성 애플리케이션으로 확인되면 향후 검색 엔진 업데이트 중 하나에 해당 파일 검출이 추가됩니다.

애플리케이션 이름 - 프로그램 또는 프로세스의 지정된 이름입니다.

아래쪽에서 지정된 애플리케이션을 클릭하면 창 아래쪽에 다음 정보가 나타납니다.

- **경로** - 컴퓨터에서 애플리케이션의 위치입니다.
- **설명** - 운영 체제 설명에 따른 파일 특성입니다.
- **버전** - 애플리케이션 게시자의 정보입니다.
- **회사** - 공급업체 또는 애플리케이션 프로세스의 이름입니다.
- **제품** - 애플리케이션 이름 및/또는 회사 이름입니다.
- **크기** - 파일 크기는 kB(킬로바이트) 또는 MB(메가바이트)입니다.
- **생성 날짜** - 애플리케이션이 생성된 날짜와 시간입니다.
- **수정 날짜** - 애플리케이션이 마지막으로 수정된 날짜와 시간입니다.

평판은 실행 중인 프로그램/프로세스로 작동하지 않는 파일에서도 확인할 수 있습니다. 검사할 파일을 표시하고 파일을 오른쪽 마우스 버튼으로 클릭한 다음 오른쪽 마우스 버튼 메뉴에서 **고급 옵션** > **ESET LiveGrid®를 사용하여 파일 평판 검사**를 선택하면 됩니다.



보안 보고서

이 기능은 다음 범주에 대한 통계 개요를 제공합니다.

- **차단된 웹 페이지** – 차단된 웹 페이지의 수를 표시합니다(PUA의 차단 목록 URL, 피싱, 해킹된 라우터, IP 또는 인증서).
- **감염된 이메일 개체가 탐지됨** – 탐지된 감염 이메일 개체 수를 표시합니다.
- **웹 컨트롤에서 차단된 웹 페이지** – 웹 컨트롤에서 차단된 웹 페이지의 수를 표시합니다.
- **PUA가 감지됨** – PUA(사용자가 원치 않는 애플리케이션) 수를 표시합니다.
- **스팸 이메일이 감지됨** – 감지된 스팸 이메일 수를 표시합니다.
- **문서가 검사됨** - 검사된 문서 개체 수를 표시합니다.
- **애플리케이션이 검사됨** – 검사된 실행 파일 개체 수를 표시합니다.
- **기타 개체가 검사됨** – 검사된 기타 개체 수를 표시합니다.
- **웹 페이지 개체가 검사됨** – 검사된 웹 페이지 개체 수를 표시합니다.
- **이메일 개체가 검사됨** – 검사된 이메일 개체 수를 표시합니다.

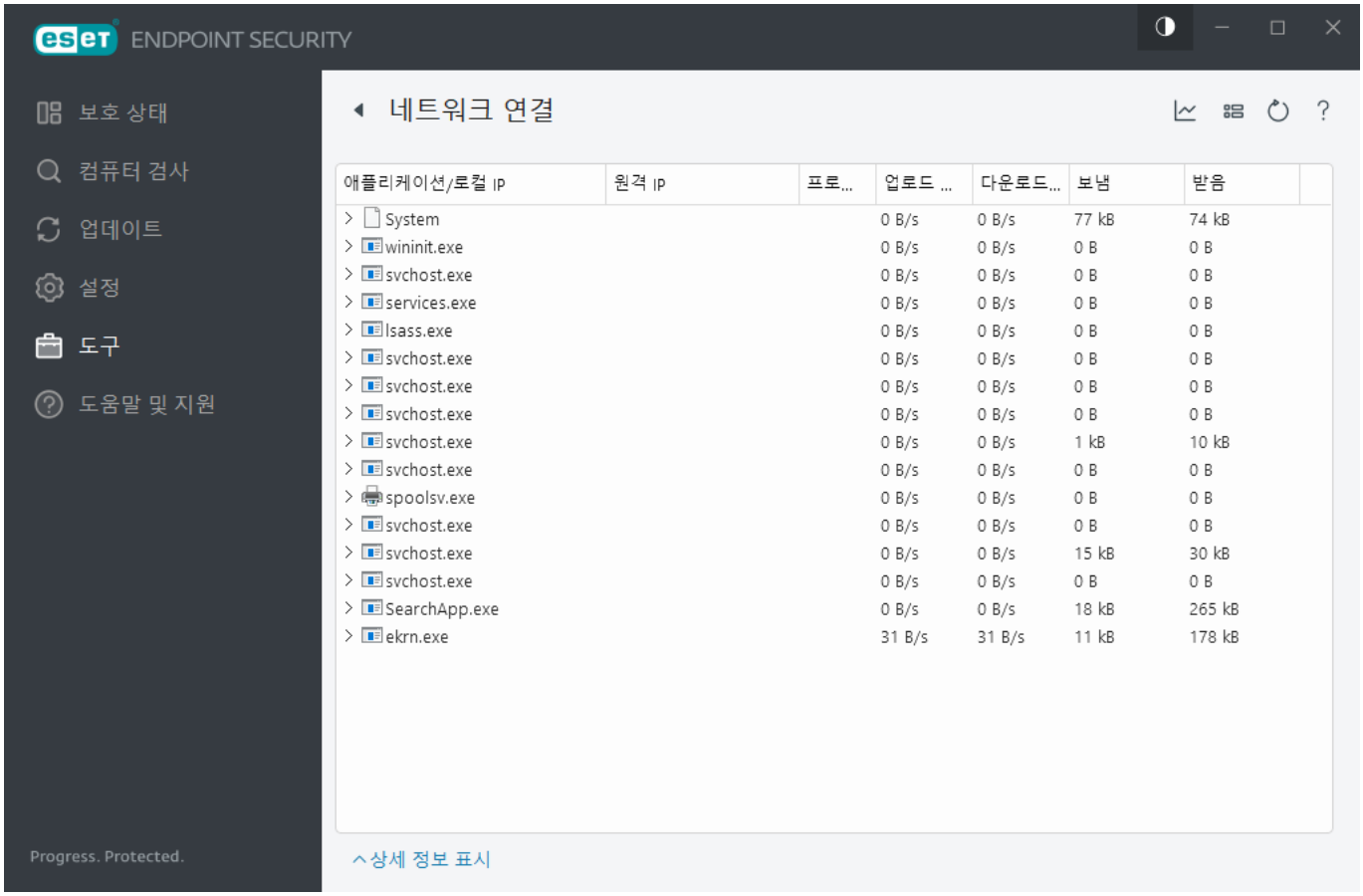
이러한 범주의 순서는 가장 높은 값부터 낮은 값 순서를 따릅니다. 값이 0인 범주는 표시되지 않습니다. 숨겨진 범주를 확장하여 표시하려면 **자세히 표시**를 클릭합니다.

오른쪽 상단 모서리에 있는 톱니바퀴⚙을 클릭하여 **보안 보고서 알림을 활성화/비활성화**하거나 지난 30일 동안 또는 제품이 활성화된 이후의 데이터를 표시할지 여부를 선택할 수 있습니다. ESET Endpoint Security를 30일 이내에 설치한 경우 설치한 날로부터의 기간(일)만 선택할 수 있습니다. 기본적으로 이 기간은 30일로 설정됩니다.

데이터 다시 설정을 선택하면 보안 보고서의 모든 통계가 지워지고 기존 데이터가 제거됩니다. **고급 설정** > 알림 > **대화형 경고** > **확인 메시지**에서 **통계를 다시 설정하기 전 확인** 옵션을 선택 취소한 경우를 제외하고는 항상 이 작업을 확인해야 합니다.

네트워크 연결

네트워크 연결 섹션에서 활성 연결과 대기 중인 연결 목록을 확인할 수 있습니다. 그러면 나가는 연결을 설정하는 모든 애플리케이션을 제어할 수 있습니다.



그래프 아이콘을 클릭하여 네트워크 활동을 엽니다.

첫 번째 줄에는 애플리케이션 이름과 해당 데이터 전송 속도가 표시됩니다. 애플리케이션이 설정하는 연결 목록과 보다 자세한 정보를 보려면 **>**를 클릭합니다.

열

애플리케이션/로컬 IP - 애플리케이션 이름, 로컬 IP 주소 및 통신 포트입니다.

원격 IP - 특정 원격 컴퓨터의 IP 주소 및 포트 번호입니다.

프로토콜 - 사용되는 전송 프로토콜입니다.

최고 속도/최저 속도 - 보내는 데이터와 받는 데이터의 현재 속도입니다.

보냄/받음 - 연결 내에서 교환한 데이터의 양입니다.

상세 정보 표시 - 선택한 연결에 대한 상세한 정보를 표시하려면 이 옵션을 선택합니다.

네트워크 연결 화면에서 애플리케이션 또는 IP 주소를 선택하고 오른쪽 마우스 버튼을 클릭하면 오른쪽 마우스 버튼 메뉴가 다음과 같은 구조로 표시됩니다.

호스트 이름 확인 - 가능한 경우 모든 네트워크 주소가 숫자 IP 주소 형식이 아닌 DNS 형식으로 표시됩니다.

TCP 연결만 표시 - TCP 프로토콜 제품군에 속하는 연결만 목록에 표시됩니다.

수신 중인 연결 표시 - 현재 통신이 설정되어 있지 않지만 시스템이 포트를 열고 연결을 대기 중인 연결만 표시하려면 이 옵션을 선택합니다.

컴퓨터 내 연결 표시 - 원격 측이 로컬 시스템인 연결(localhost 연결)만 표시하려면 이 옵션을 선택합니다.

다음을 비롯한 추가 옵션을 보려면 연결을 오른쪽 마우스 버튼으로 클릭합니다.

연결을 위한 통신 거부 - 설정된 통신을 종료합니다. 이 옵션은 활성 연결을 클릭한 후에만 사용할 수 있습니다.

새로 고침 속도 - 활성 연결을 새로 고칠 빈도를 선택합니다.

지금 새로 고침 - 네트워크 연결 창을 다시 로드합니다.

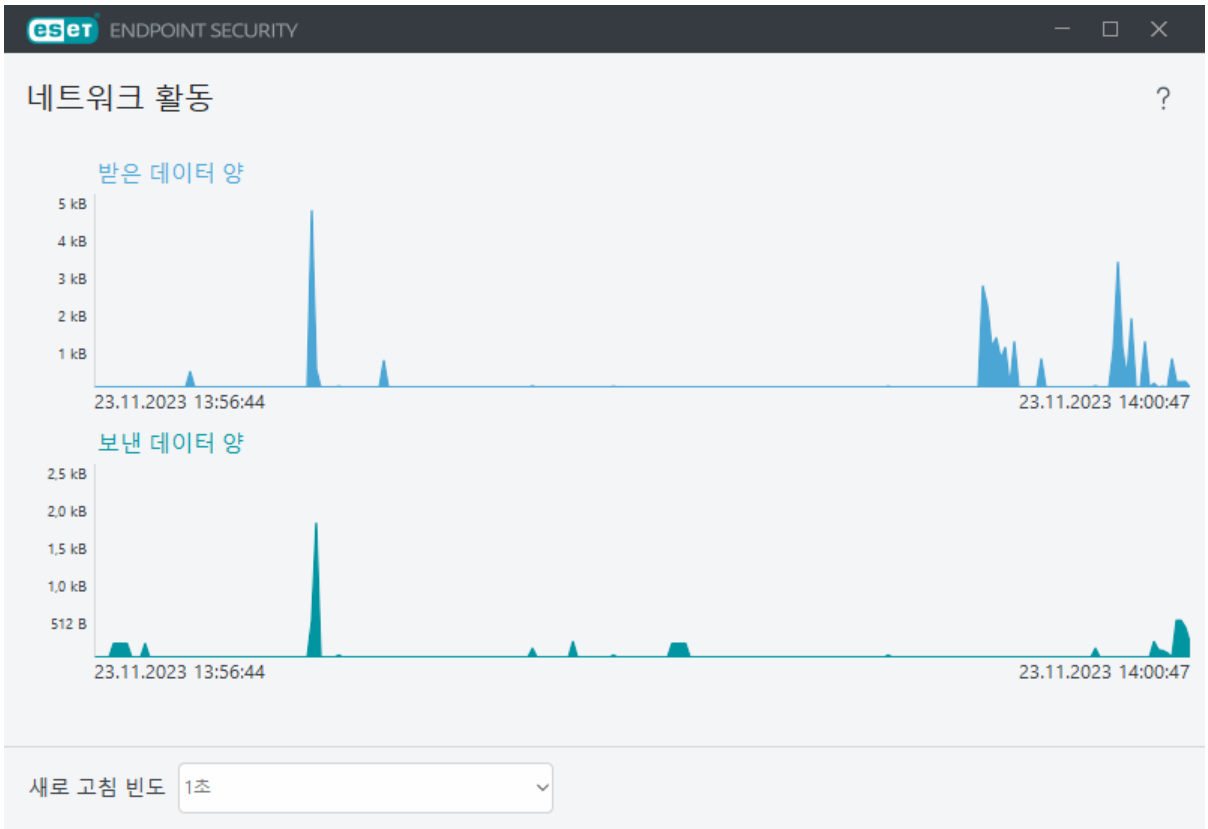
다음의 옵션은 활성 연결이 아닌 애플리케이션 또는 프로세스를 클릭한 후에만 사용할 수 있습니다.

일시적으로 프로세스를 위한 통신 거부 - 지정된 애플리케이션의 현재 연결을 거부합니다. 새 연결이 설정되면 방화벽이 미리 정의된 규칙을 사용합니다. 설정에 대한 설명은 방화벽 규칙 섹션에서 확인할 수 있습니다.

일시적으로 프로세스를 위한 통신 허용 - 지정된 애플리케이션의 현재 연결을 허용합니다. 새 연결이 설정되면 방화벽이 미리 정의된 규칙을 사용합니다. 설정에 대한 설명은 방화벽 규칙 섹션에서 확인할 수 있습니다.

네트워크 활동

현재 **네트워크 활동**을 그래프 양식으로 보려면 **도구 > 네트워크 연결**을 클릭하고 그래프 아이콘을 클릭합니다. 그래프 아래쪽에는 선택한 시간 범위에 따라 네트워크 활동을 실시간으로 기록하는 시간 표시줄이 있습니다. 시간 범위를 변경하려면 **새로 고침 빈도** 드롭다운 메뉴에서 해당하는 값을 선택합니다.



다음과 같은 옵션을 사용할 수 있습니다.

- **1초**- 그래프가 1초마다 새로 고쳐지고 시간 표시줄이 지난 4분을 나타냅니다.
- **1분(지난 24시간)** - 그래프가 1분마다 새로 고쳐지고 시간 표시줄이 지난 24시간을 나타냅니다.
- **1시간(지난달)** - 그래프가 1시간마다 새로 고쳐지고 시간 표시줄이 지난달을 나타냅니다.

그래프의 세로 축은 수신되거나 전송된 데이터의 양을 나타냅니다. 그래프 위에 마우스를 올리면 특정 시간에 수신/전송된 데이터의 정확한 양을 확인할 수 있습니다.

ESET SysInspector

ESET SysInspector는 컴퓨터를 철저히 검사하고, 시스템 구성 요소에 대한 자세한 정보(예: 드라이버 및 애플리케이션, 네트워크 연결 또는 중요한 레지스트리 항목)를 수집하고, 각 구성 요소의 위험 수준을 평가하는 애플리케이션입니다. 이러한 정보는 소프트웨어 또는 하드웨어 비호환성이나 악성코드 감염으로 인해 발생할 수 있는 감염 의심 시스템 동작의 원인을 확인하는 데 도움이 됩니다. ESET SysInspector 사용 방법에 대해 자세히 알아보려면 ESET SysInspector 온라인 도움말을 참조하십시오.

ESET SysInspector 창에는 다음과 같은 로그 정보가 표시됩니다.

- **시간** - 로그 생성 시간입니다.
- **설명** - 간단한 설명입니다.
- **사용자** - 로그를 생성한 사용자의 이름입니다.
- **상태** - 로그 생성 상태입니다.

다음과 같은 동작을 사용할 수 있습니다:

- **표시** – 선택한 로그를 ESET SysInspector에서 엽니다. 지정된 로그 파일을 오른쪽 마우스 버튼으로 클릭한 후 오른쪽 마우스 버튼 메뉴에서 **표시**를 선택할 수도 있습니다.
- **생성** - 새 로그를 생성합니다. 로그에 접근하려고 시도하기 전에 ESET SysInspector가 생성될 때(**생성됨** 상태)까지 기다리십시오. 로그는 C:\ProgramData\ESET\ESET Security\SysInspector에 저장됩니다.
- **삭제** - 목록에서 선택한 로그를 제거합니다.

하나 이상의 로그 파일을 선택하면 오른쪽 마우스 버튼 메뉴에 다음 항목이 표시됩니다:

- **표시** - 선택한 로그를 ESET SysInspector에서 엽니다(로그를 두 번 클릭하는 것과 같은 기능).
- **생성** - 새 로그를 생성합니다. 로그에 접근하려고 시도하기 전에 ESET SysInspector가 생성될 때(**생성됨** 상태)까지 기다리십시오.
- **삭제** - 목록에서 선택한 로그를 제거합니다.
- **모두 삭제** - 모든 로그를 삭제합니다.
- **내보내기** - 로그를 .xml 파일 또는 압축된 .xml로 내보냅니다.

스케줄러

스케줄러는 미리 정의된 구성 및 속성을 사용하여 예약된 작업을 관리하고 실행합니다.

스케줄러는 ESET Endpoint Security 기본 프로그램 창에서 **도구** > **스케줄러**를 클릭하여 접근할 수 있습니다. **스케줄러**에는 모든 예약된 작업 및 구성 속성(예: 미리 정의된 날짜, 시간 및 사용된 검사 프로필) 목록이 포함되어 있습니다.

스케줄러를 통해 검색 엔진 업데이트, 검사 작업, 시스템 시작 파일 검사 및 로그 유지 관리와 같은 작업을 예

약할 수 있습니다. 기본 스케줄러 창의 아래쪽에서 **작업 추가** 또는 **삭제**를 클릭하여 작업을 직접 추가하거나 삭제할 수 있습니다. 스케줄러 창에서 임의의 위치를 오른쪽 마우스 버튼으로 클릭하면 상세 정보 표시, 즉시 작업 수행, 새 작업 추가 및 기존 작업 삭제를 수행할 수 있습니다. 작업을 활성화/비활성화하려면 각 항목 시작 시 확인란을 사용합니다.

기본적으로 **스케줄러**에는 다음과 같은 예약된 작업이 표시됩니다:

- **로그 유지 관리**
- **정기적 자동 업데이트**
- **전화 접속 연결 후 자동 업데이트**
- **사용자 로그온 후 자동 업데이트**
- **자동 시작 파일 검사**(사용자 로그온 후)
- **자동 시작 파일 검사**(모듈 업데이트 후)

ESET PROTECT에서 임의 작업 실행 지연을 사용하여 작업을 실행할 때(특히 대규모 네트워크에서) 서버 로드를 줄일 수 있습니다. 이 옵션을 통해 전체 네트워크의 모든 워크스테이션에서 작업이 실행되는 것과는 달리 작업이 전체 네트워크에서 실행될 기간을 정의할 수 있습니다. 작업 실행 시 네트워크의 각 워크스테이션에 고유한 작업 실행 시간을 할당하기 위해 설정된 시간 값이 임의로 분할됩니다. 이로써 서버 오버로드 및 관련 문제를 방지할 수 있습니다(예: 전체 네트워크에서 동시 일괄 업데이트를 수행할 경우 일부 서버가 DoS 공격을 보고할 수 있습니다).

예약된 기존 작업(기본값 및 사용자 정의 모두)의 구성을 편집하려면 작업을 오른쪽 마우스 버튼으로 클릭하고 **편집**을 클릭하거나 수정하려는 작업을 선택하고 **편집** 버튼을 클릭합니다.

새 작업 추가

1. 창 아래쪽의 **작업 추가**를 클릭합니다.

2. 작업의 이름을 입력합니다.
3. 드롭다운 메뉴에서 원하는 작업을 선택합니다.

- **외부 애플리케이션 실행** - 외부 애플리케이션 실행을 예약합니다.
- **로그 유지 관리** - 로그 파일에는 삭제된 레코드의 잔여 레코드가 포함되어 있을 수도 있습니다. 이 작업에서는 효과적으로 작업하기 위해 정기적으로 로그 파일의 레코드를 최적화합니다.
- **시스템 시작 파일 검사** - 시스템 시작 또는 로그온 시 실행할 수 있는 파일을 검사합니다.
- **컴퓨터 상태 스냅숏 생성** - ESET SysInspector 컴퓨터 스냅숏을 생성합니다. 시스템 구성 요소(예: 드라이버, 애플리케이션)에 대한 자세한 정보를 수집하고 각 구성 요소의 위험 수준을 평가합니다.
- **수동 컴퓨터 검사** - 컴퓨터의 파일 및 폴더에 대한 검사를 수행합니다.
- **업데이트** - 검색 엔진 및 프로그램 모듈을 업데이트하여 업데이트 작업을 예약합니다.

4. 작업을 활성화하려면 **활성화됨** 스위치를 켜고(나중에 예약된 작업 목록에서 확인란을 선택/선택 취소하여 이렇게 할 수 있음), **다음**을 클릭하고 다음과 같은 타이밍 옵션 중 하나를 선택합니다.

- **한 번** - 미리 정의된 날짜 및 시간에 작업이 수행됩니다.
- **반복적으로** - 작업이 지정한 시간 간격으로 수행됩니다.
- **매일** - 매일 지정한 시간에 반복적으로 작업이 실행됩니다.
- **매주** - 선택한 날짜 및 시간에 작업이 실행됩니다.
- **이벤트가 트리거됨** - 지정한 이벤트에서 작업이 수행됩니다.

5. 랩톱을 배터리 전원으로 실행하는 동안 시스템 리소스를 최소화하려면 **배터리 전원으로 실행되는 작업 건너뛰기**를 선택합니다. 작업은 **작업 실행** 필드에 지정된 날짜 및 시간에 실행됩니다. 미리 정의된 시간에 작업을 실행할 수 없는 경우 해당 작업이 다시 수행될 시점을 지정할 수 있습니다.

- **다음 예약 시간에**
- **최대한 빨리**
- **마지막 실행 이후 시간이 지정된 값을 초과하는 경우 즉시**(간격은 **마지막 실행 후 시간** 스크롤 상자를 사용하여 정의할 수 있음)

예약된 작업을 검토하려면 작업을 마우스 오른쪽 단추로 클릭하고 **작업 상세 정보 표시**를 클릭합니다.

예약된 검사 옵션

이 창에서 예약된 컴퓨터 검사 작업에 대한 고급 옵션을 지정할 수 있습니다.

치료 동작 없이 검사를 실행하려면 **고급 설정**을 클릭하고**치료하지 않고 검사**를 선택합니다. 검사 기록은 검사 로그에 저장됩니다.

제외 무시가 선택된 경우 이전에 검사에서 제외된 확장명이 포함된 파일이 예외 없이 검사됩니다.

드롭다운 메뉴를 사용하여 검사를 완료하면 자동으로 수행될 동작을 설정할 수 있습니다.

- **동작 없음** - 검사 완료 후 아무 동작도 수행되지 않습니다.
- **종료** - 검사가 완료되면 컴퓨터 전원이 꺼집니다.
- **다시 부팅** - 검사가 완료되면 열려 있는 모든 프로그램이 닫히고 컴퓨터가 다시 시작됩니다.
- **필요한 경우 재부팅**– 탐지된 위협 치료를 완료하기 위해 필요한 경우에만 컴퓨터가 재부팅됩니다.
- **강제 재부팅** – 검사가 완료되면 사용자 상호 작용을 기다리지 않고 열려 있는 모든 프로그램을 강제로 닫은 후 컴퓨터를 다시 시작합니다.
- **필요한 경우 강제 재부팅**– 탐지된 위협 치료를 완료하기 위해 필요한 경우에만 컴퓨터가 재부팅됩니다.

- **절전 모드** - 작업을 빠르게 다시 시작할 수 있도록 사용자 세션을 저장하고 컴퓨터를 절전 상태로 설정합니다.
- **최대 절전 모드** - RAM에서 실행 중인 모든 항목을 하드 드라이브의 특수 파일로 이동합니다. 컴퓨터가 종료되지만 다음에 컴퓨터를 시작할 때 이전 상태에서 다시 시작됩니다.

절전 모드 또는 **최대 절전 모드** 동작은 컴퓨터 전원과 절전 운영 체제 설정이나 컴퓨터/랩톱 기능에 따라 사용할 수 있습니다. 절전 모드 컴퓨터는 여전히 작동하는 컴퓨터입니다. 계속해서 기본 기능을 실행하고 컴퓨터가 배터리 전원으로 작동되는 경우 전기를 사용합니다. 외근 중일 때 등의 상황에서 배터리 수명을 보존하려면 최대 절전 모드를 사용하는 것이 좋습니다.

권한 없는 사용자가 검사 후 수행되는 동작을 중지하지 못하도록 하려면 **검사를 취소할 수 없음**을 선택합니다.

제한된 사용자가 지정된 기간 동안 컴퓨터 검사를 일시 중지하도록 허용하려면 **다음 시간(분) 동안 사용자가 검사를 일시 중지할 수 있음** 옵션을 선택합니다.

검사 진행률도 참조하십시오.

예약된 작업 개요

사용자 지정 작업을 두 번 클릭하거나, 사용자 지정 스케줄러 작업을 오른쪽 마우스 버튼으로 클릭하고 **작업 상세 정보 표시**를 클릭하면 이 대화 상자 창에 선택한 예약된 작업에 대한 자세한 정보가 표시됩니다.

작업 상세 정보

작업 이름을 입력하고 **작업 유형** 옵션 중 하나를 선택한 후 **다음**을 클릭합니다.

- **외부 애플리케이션 실행** - 외부 애플리케이션 실행을 예약합니다.
- **로그 유지 관리** - 로그 파일에는 삭제된 레코드의 잔여 레코드가 포함되어 있을 수도 있습니다. 이 작업에서는 효과적으로 작업하기 위해 정기적으로 로그 파일의 레코드를 최적화합니다.
- **시스템 시작 파일 검사** - 시스템 시작 또는 로그온 시 실행할 수 있는 파일을 검사합니다.
- **컴퓨터 상태 스냅숏 생성** - ESET SysInspector 컴퓨터 스냅숏을 생성합니다. 시스템 구성 요소(예: 드라이버, 애플리케이션)에 대한 자세한 정보를 수집하고 각 구성 요소의 위험 수준을 평가합니다.
- **수동 컴퓨터 검사** - 컴퓨터의 파일 및 폴더에 대한 검사를 수행합니다.
- **업데이트** – 모듈을 업데이트하여 업데이트 작업을 예약합니다.

작업 타이밍

작업이 지정한 시간 간격으로 반복적으로 수행됩니다. 다음과 같은 타이밍 옵션 중 하나를 선택합니다.

- **한 번** - 미리 정의된 날짜 및 시간에 작업이 한 번만 수행됩니다.
- **반복적으로** - 작업이 지정한 간격(시)으로 수행됩니다.
- **매일** - 매일 지정한 시간에 작업이 실행됩니다.
- **매주** - 작업이 매주 한 번 이상 선택한 날짜 및 시간에 실행됩니다.
- **이벤트가 트리거됨** - 지정한 이벤트가 발생한 후에 작업이 수행됩니다.

배터리 전원으로 실행되는 작업 건너뛰기 - 작업이 시작될 때 컴퓨터가 배터리로 실행 중인 경우 작업이 시작되지 않습니다. UPS로 실행 중인 컴퓨터에서도 마찬가지입니다.

작업 타이밍 - 한 번

작업 실행 - 지정한 작업이 지정한 날짜 및 시간에 한 번만 실행됩니다.

작업 타이밍 - 매일

매일 지정한 시간에 작업이 실행됩니다.

작업 타이밍 - 매주

작업이 선택한 요일과 시간에 매주 반복적으로 실행됩니다.

작업 타이밍 - 이벤트가 트리거됨

다음 이벤트 중 하나에 의해 작업이 트리거됩니다.

- **컴퓨터를 시작할 때마다**
- **매일 컴퓨터를 처음 시작할 때**
- **인터넷/VPN에 전화 접속 연결**
- **모듈 업데이트 완료 시**
- **제품 업데이트 완료 시**
- **사용자 로그온**
- **위협 검출**

이벤트에 의해 트리거된 작업을 예약하면 두 작업 완료 간 최소 간격을 지정할 수 있습니다. 예를 들어, 하루에 여러 번 컴퓨터에 로그온하는 경우 하루 중 처음으로 로그온할 때에만 작업을 수행하고 다음 날도 동일한 패턴으로 작업을 수행하려면 24시간을 선택합니다.

건너뛴 작업

컴퓨터 전원이 차단되거나 컴퓨터가 배터리 전원으로 실행되는 경우 작업을 건너뛸 수 있습니다. 다음 옵션 중에서 작업을 실행할 시기를 선택하고 **다음**을 클릭합니다.

- **다음 예약 시간에** – 컴퓨터가 다음 예약 시간에 켜져 있으면 작업이 실행됩니다.
- **최대한 빨리** – 컴퓨터가 켜지면 작업이 실행됩니다.
- **마지막 예약 실행 이후 다음 시간이 초과되면 즉시** – 작업의 실행을 처음 건너뛴 이후로 경과된 시간을 나타냅니다. 이 시간이 초과되면 작업이 즉시 실행됩니다.

마지막으로 예약된 실행 이후 시간이 초과하는 경우 즉시(시간) - 예

예제 작업은 매시간 반복 실행되도록 설정되었습니다. **마지막 예약 실행 이후 다음 시간이 초과되면 즉시** 옵션을 선택하고 초과 시간은 2시간으로 설정합니다. 작업은 오후 1시에 실행되고, 완료되면 컴퓨터가 절전 모드로 전환됩니다.

- 컴퓨터는 오후 3시 30분에 깨어납니다. 작업의 실행을 처음 건너뛴 시간은 오후 2시였습니다. 오후 2시 이후 단 1.5시간이 경과했으므로, 작업은 오후 4시에 실행됩니다.
- 컴퓨터는 오후 4시 30분에 깨어납니다. 작업의 실행을 처음 건너뛴 시간은 오후 2시였습니다. 오후 2시 이후 2.5시간이 경과했으므로, 작업이 즉시 실행됩니다.

작업 상세 정보 - 업데이트

두 업데이트 서버에서 프로그램을 업데이트하려는 경우에는 서로 다른 두 프로필 업데이트를 생성해야 합니다. 첫 번째 프로필로 업데이트 파일을 다운로드하지 못하는 경우 프로그램은 자동으로 대체 프로필로 전환합니다. 이는 일반적으로 로컬 LAN 업데이트 서버로부터 업데이트하지만 소유자가 다른 네트워크의 인터넷에 연결하는 경우가 많은 노트북의 경우 적합합니다. 따라서 첫 번째 프로필이 실패하면 두 번째 프로필은 ESET의 업데이트 서버로부터 업데이트 파일을 자동으로 다운로드합니다.

작업 상세 정보 - 애플리케이션 실행

이 작업은 외부 애플리케이션의 실행을 예약합니다.

실행 파일 - 디렉터리 트리에서 실행 파일을 선택하고 **...** 옵션을 클릭하거나 수동으로 경로를 입력합니다.

작업 폴더 - 외부 애플리케이션의 작업 디렉터리를 정의합니다. 선택한 **실행 파일**의 모든 임시 파일이 이 디렉터리 내에 생성됩니다.

파라미터 - 애플리케이션의 명령줄 파라미터입니다(옵션).

작업을 적용하려면 **마침**을 클릭합니다.

분석용 샘플 전송

컴퓨터에서 감염 의심 파일을 찾았거나 인터넷에서 감염 의심 사이트를 찾은 경우 ESET 연구소로 전송하여 분석할 수 있습니다(ESET LiveGrid® 구성에 따라 사용하지 못할 수도 있음).

다음 기준 중 한 가지 이상을 충족하지 않을 경우 샘플을 전송하지 마십시오:

- 샘플이 ESET 제품에서 검출되지 않음
- 샘플이 위협으로 잘못 검출됨
- ESET을 통해 악성코드를 검색하려는 개인 파일은 샘플로 허용되지 않음(ESET 연구소에서는 사용자를 위한 수동 검사를 수행하지 않음)
- 설명이 포함된 제목 줄을 사용하고, 파일을 다운로드한 웹 사이트나 스크린샷 등의 파일 관련 정보를 최대한 많이 포함해 주십시오.

샘플 전송을 사용하면 다음 방법 중 하나로 파일 또는 사이트를 ESET에 전송할 수 있습니다.

1. 샘플 전송 대화 상자는 **도구 > 분석용 샘플 전송**에서 사용할 수 있습니다.
2. 파일을 이메일로 전송할 수도 있습니다. 이 옵션을 사용하려는 경우에는 WinRAR/ZIP을 사용하여 파일을 압축하고 "infected"라는 비밀번호로 압축파일을 보호한 후에 samples@eset.com으로 보내면 됩

니다.

3. 스팸, 스팸 오탐지 또는 웹 컨트롤 모듈이 잘못 분류한 웹 사이트를 보고하려면 ESET 지식베이스 문서를 참조하십시오.

분석용 샘플 전송이 열린 상태에서 **샘플 전송 사유** 드롭다운 메뉴에서 메시지에 가장 적합한 설명을 선택합니다.

- 감염 의심 파일
- 감염 의심 사이트(맬웨어에 감염된 웹 사이트)
- 가양성 파일(감염된 것으로 검출되었지만 실제로는 감염되지 않은 파일)
- 가양성 사이트
- 기타

파일/사이트 - 전송하려는 파일 또는 웹 사이트의 경로입니다.

담당자 이메일 - 이 담당자 이메일이 감염 의심 파일과 함께 ESET로 전송되며, 분석 시 추가 정보가 필요한 경우 사용자에게 연락하는 데 사용될 수 있습니다. 담당자 이메일 입력은 옵션입니다. 이를 비워 두려면 **익명으로 전송**을 선택하십시오.

추가 정보가 필요한 경우가 아니면 ESET에서는 응답 메시지를 보내지 않습니다. 매일 수만 개의 파일이 ESET 서버에 수신되기 때문에 모든 전송 항목에 대해 회신할 수는 없습니다.
샘플이 악성 애플리케이션 또는 웹 사이트로 확인되면 향후 ESET 업데이트에 해당 항목 검출 기능이 추가됩니다.

분석용 샘플 선택 - 감염 의심 파일

맬웨어 감염 증상 발견 - 컴퓨터에서 발견된 감염 의심 파일 동작에 대한 설명을 입력합니다.

원본 파일(URL 주소나 공급업체) - 원본 파일(소스) 및 이 파일을 발견한 방식을 입력하십시오.

메모 및 추가 정보 - 여기에 감염 의심 파일 식별 프로세스에 도움이 될 추가 정보나 설명을 입력할 수 있습니다.

첫 번째 파라미터 **맬웨어 감염 증상 발견**은 필수 사항이지만, 추가 정보를 입력하면 샘플 식별 프로세스에 있어 ESET 연구소에 많은 도움이 됩니다.

분석용 샘플 선택 - 감염 의심 사이트

사이트의 문제 드롭다운 메뉴에서 다음 중 하나를 선택하십시오.

- **감염됨** - 다양한 방법으로 배포된 바이러스나 기타 맬웨어가 포함되어 있는 웹 사이트입니다.
- **피싱** - 은행 계좌 번호, PIN 번호 등과 같은 중요한 데이터에 접근하는 데 자주 사용됩니다. 이러한 공격 유형에 대한 자세한 내용은 용어집을 참조하십시오.
- **사기** - 특히 빠른 수익을 얻기 위해 사용되는 사기 또는 사취성 웹 사이트입니다.
- 전송하려는 사이트가 앞서 언급된 옵션에 해당하지 않을 경우 **기타**를 선택합니다.

메모 및 추가 정보 - 여기에 감염 의심 웹 사이트를 분석하는 데 도움이 될 추가 정보나 설명을 입력할 수 있습니다.

분석용 샘플 선택 - 가양성 파일

사용자는 감염된 것으로 검출되었지만 실제로는 감염되지 않은 파일을 전송하여 안티바이러스 및 안티스파이웨어 엔진을 향상시키고 다른 사용자가 보호받을 수 있도록 해야 합니다. 가양성(FP)은 파일 패턴이 검색 엔진에 포함된 동일한 패턴과 일치하는 경우에 발생할 수 있습니다.

애플리케이션 이름 및 버전 - 프로그램 제목 및 해당 버전(예: 번호, 별칭 또는 코드 이름)입니다.

원본 파일(URL 주소나 공급업체) - 원본 파일(소스) 및 이 파일을 발견한 방식을 입력하십시오.

애플리케이션 용도 - 일반적인 애플리케이션 설명, 애플리케이션 유형(예: 브라우저, 미디어 플레이어 등) 및 해당 기능입니다.

메모 및 추가 정보 - 여기에 감염 의심 파일을 처리하는 동안 도움이 될 추가 정보나 설명을 추가할 수 있습니다.

i 처음 세 개의 파라미터는 적법한 애플리케이션을 식별하여 악성 코드와 구별하는 데 필요합니다. 추가 정보를 입력하면 샘플을 식별 및 처리하는 데 있어 ESET 연구소에 많은 도움이 됩니다.

분석용 샘플 선택 - 가양성 사이트

사용자는 감염된 상태이거나 사기, 피싱 사이트로 검출되었지만 실제로는 그렇지 않은 사이트를 전송해야 합니다. 가양성(FP)은 파일 패턴이 검색 엔진에 포함된 동일한 패턴과 일치하는 경우에 발생할 수 있습니다. 이 웹 사이트 정보를 제공하여 안티바이러스 및 안티피싱 엔진을 향상시키고 다른 사용자가 보호받을 수 있도록 해 주십시오.

메모 및 추가 정보 – 여기에 감염 의심 웹 사이트를 처리하는 동안 도움이 될 추가 정보나 설명을 추가할 수 있습니다.

분석용 샘플 선택 - 기타

파일을 **감염 의심 파일** 또는 **가양성**으로 분류할 수 없는 경우 이 양식을 사용합니다.

파일 전송 사유 - 파일을 보내는 이유와 자세한 설명을 입력하십시오.

검역소

검역소의 기본 기능은 보고된 개체(예: 악성코드, 감염된 파일 또는 사용자가 원치 않는 애플리케이션)를 안전하게 저장하는 것입니다.

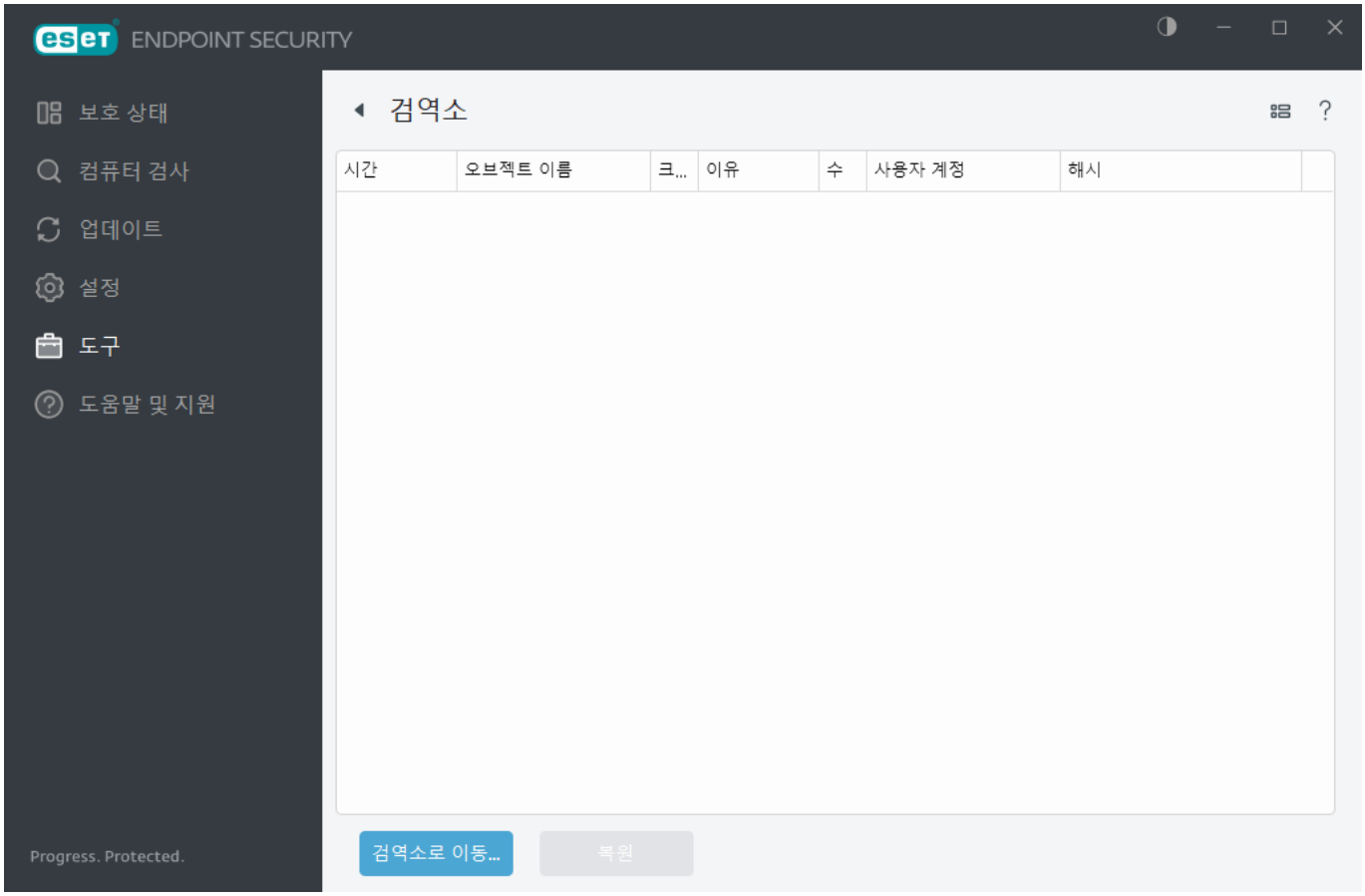
검역소는 ESET Endpoint Security 기본 프로그램 창에서 **도구 > 검역소**를 클릭하여 접근할 수 있습니다.

검역소 폴더에 저장된 파일은 다음을 표시하는 표에서 확인할 수 있습니다.

- 검역소 날짜 및 시간
- 파일의 원래 위치 경로
- 크기(바이트)

- 이유(예: 사용자가 추가한 개체)
- 및 탐지 수(예: 동일한 파일의 중복된 탐지 또는 여러 개의 침입이 포함된 압축파일인 경우).

클라이언트 워크스테이션에서 원격으로 검역소 관리



파일을 검역소로 보내기

ESET Endpoint Security에서는 제거된 파일을 자동으로 검역소로 보냅니다(경고 창에서 이 옵션을 취소하지 않은 경우).

다음과 같은 경우 추가 파일을 검역소로 보내야 합니다.

- 치료할 수 없는 경우
- 안전하지 않거나, 제거하는 것이 권장되지 않은 경우
- 해당 파일을 ESET Endpoint Security에서 잘못 탐지한 경우
- 또는 파일이 의심스럽게 동작하지만 검사기에서 탐지되지 않는 경우

파일을 검역소로 보내는 데에는 다음과 같은 여러 가지 옵션이 있습니다.

- 끌어서 놓기 기능을 사용하여 파일을 클릭하고 마우스 버튼을 누른 상태에서 마우스 포인터를 표시된 영역으로 이동한 후 손을 놓아 파일을 수동으로 검역소로 보낼 수 있습니다. 그런 다음 애플리케이션을 포그라운드로 이동합니다.
- 기본 프로그램 창에서 **검역소로 이동...**을 클릭합니다.
- 또한 오른쪽 마우스 버튼 메뉴을 사용하여 파일을 검역소로 보낼 수 있습니다. **검역소** 창에서 마우스 오른쪽 버튼을 클릭하고 **검역소**를 선택하면 됩니다.

검역소에서 복원

검역소로 보낸 파일은 원래 위치에 복원할 수도 있습니다.

- 이렇게 하려면 **복원** 기능을 사용합니다. 이 기능은 마우스 오른쪽 버튼 메뉴에서 검역소에 지정된 파일을 마우스 오른쪽 단추로 클릭하여 사용할 수 있습니다.
- 파일이 사용자가 원치 않는 애플리케이션으로 표시된 경우 **복원 후 검사에서 제외** 옵션이 활성화됩니다. 또한 제외를 참조하십시오.
- 마우스 오른쪽 버튼 메뉴에서는 **복원 대상** 옵션도 제공하여 제거된 위치가 아닌 위치로 파일을 복원할 수 있습니다.
- 예를 들어 읽기 전용 네트워크 공유에 있는 파일의 경우 복원 기능을 사용할 수 없습니다.

검역소에서 제거

지정된 항목을 오른쪽 마우스 버튼으로 클릭한 후 **검역소에서 제거**를 선택하거나, 제거할 항목을 선택한 후 키보드에서 **Delete** 키를 누릅니다. 또한 여러 항목을 선택하여 동시에 제거할 수 있습니다. 제거된 항목은 장치 및 검역소에서 영구적으로 제거됩니다.

검역소에서 파일 전송

프로그램에서 탐지되지 않은 감염 의심 파일을 검역소로 보낸 경우 또는 코드의 인공지능 분석 등을 통해 파일이 감염된 것으로 잘못 평가되어 검역소로 보내진 경우에는 분석용 샘플을 ESET 연구소로 보내 주십시오. 파일을 전송하려면 해당 파일을 오른쪽 마우스 버튼으로 클릭한 다음 오른쪽 마우스 버튼 메뉴에서 **분석을 위해 전송**을 선택합니다.

다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- ESET PROTECT 에서 검역소 관리
- 내 ESET 제품에서 탐지 정보를 알려 주었습니다. 어떻게 해야 합니까?

도움말 및 지원

발생할 수 있는 문제를 해결하는 데 도움이 되는 지원 정보와 문제 해결 도구를 표시하려면 기본 프로그램 창에서 **도움말 및 지원**을 클릭합니다.

설치된 제품

- ESET Endpoint Security 정보 - ESET Endpoint Security 복사본에 대한 정보를 표시합니다.
- 제품 문제 해결 – 가장 자주 발생하는 문제에 대한 해결 방법을 찾으려면 이 링크를 클릭합니다.
- 라이선스 문제 해결 – 활성화 또는 라이선스 변경 문제에 대한 해결 방법을 찾으려면 이 링크를 클릭합니다.
- 라이선스 변경 - 제품 활성화 창을 클릭하여 시작한 다음 제품을 활성화합니다.

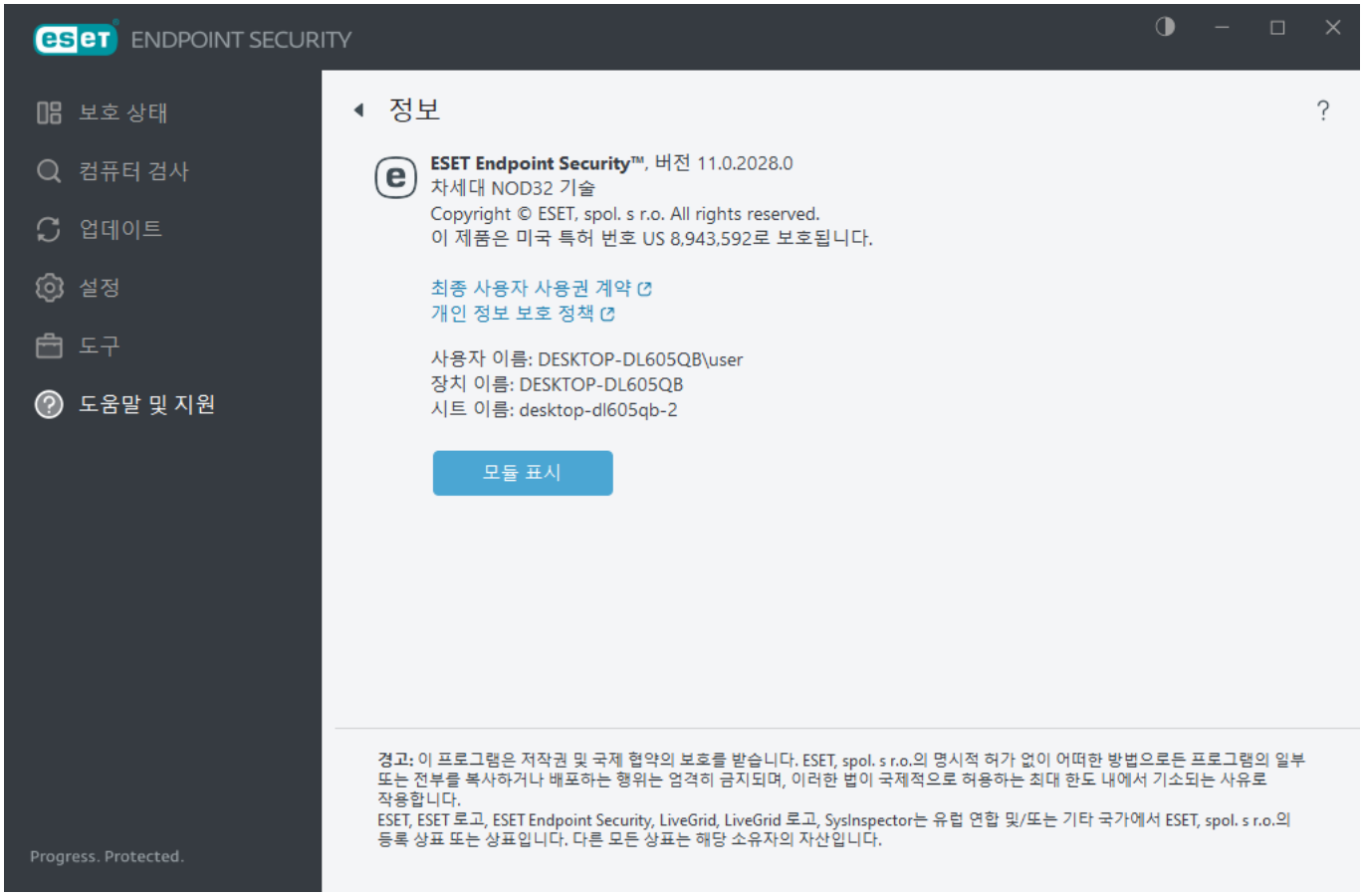
도움말 페이지 - ESET Endpoint Security 도움말 페이지를 실행하려면 이 링크를 클릭합니다.

기술 지원

지식베이스 - ESET 지식 베이스에는 다양한 문제에 대한 질문과 대답 및 권장 해결 방법이 포함되어 있습니다. 지식 베이스는 다양한 문제를 해결하는 가장 강력한 도구로, ESET 기술 전문가가 정기적으로 업데이트합니다.

ESET Endpoint Security 정보

이 창에서는 설치된 ESET Endpoint Security 버전과 컴퓨터에 대한 상세 정보를 제공합니다.



모듈 표시를 클릭하여 로드된 프로그램 모듈 목록에 대한 정보를 확인합니다.

- **복사**를 클릭하면 모듈에 대한 정보를 클립보드에 복사할 수 있습니다. 이는 문제 해결 중 또는 기술 지원에 문의할 때 유용할 수 있습니다.
- 모듈 창에서 **탐지 엔진**을 클릭하여 ESET 탐지 엔진의 각 버전에 대한 정보가 포함된 ESET Virus Radar를 엽니다.

시스템 구성 데이터 전송

ESET에서 최대한 빠르고 정확하게 지원을 제공하려면 ESET Endpoint Security 구성 정보, 상세한 시스템 정보, 실행 중인 프로세스(ESET SysInspector 로그 파일) 및 레지스트리 데이터가 필요합니다. ESET에서는 컴퓨터에 대한 기술적인 지원을 제공하는 용도로만 이 데이터를 사용합니다.

웹 양식 전송 시, 사용자의 시스템 구성 데이터가 ESET으로 전송됩니다. 이 프로세스에 대해 이 동작을 저장하려면 **항상 이 정보 전송**을 선택합니다. 데이터를 보내지 않고 웹 양식을 전송하려면 **데이터 전송 안 함**을 클릭하고 계속 진행합니다.

고급 설정 > **도구** > **진단** > 기술 지원에서 시스템 구성 데이터 전송을 구성할 수 있습니다.

시스템 구성 데이터를 전송하기로 결정한 경우 웹 양식을 작성하여 전송해야 합니다. 그렇지 않으면 티켓이 생성되지 않고 시스템 구성 데이터가 손실됩니다. 시스템 구성 데이터를 전송할 수 없는 경우 웹 양식을 작성하고 기술 지원 부서의 지침을 기다립니다.

기술 지원

기본 프로그램 창에서 **도움말 및 지원** > **기술 지원**을 클릭합니다.

기술 지원에 문의

지원 요청 – 문제에 대한 답을 찾을 수 없는 경우 ESET 웹 사이트에 있는 이 양식을 사용하여 ESET 기술 지원 부서에 신속하게 문의할 수 있습니다. 설정에 따라 웹 양식을 작성하기 전에시스템 구성 데이터 제출 창이 표시됩니다.

기술 지원에 대한 정보 얻기

기술 지원에 대한 상세 정보 – 메시지가 표시되면 정보(제품 이름, 제품 버전, 운영 체제 및 프로세서 유형 등)를 복사하여 ESET 기술 지원부에 보낼 수 있습니다.

ESET Log Collector – 보다 신속하게 문제를 해결하기 위해 컴퓨터에서 정보를 자동으로 수집하여 기록하는 ESET Log Collector 유틸리티를 다운로드할 수 있는 ESET 지식 베이스 문서로 연결됩니다. 자세한 내용을 보려면 ESET Log Collector여기를 클릭하십시오.

고급 로깅을 활성화하여 개발자가 이 문제를 분석하고 해결할 수 있도록 사용 가능한 모든 기능에 대해 고급 로그를 생성합니다. 최소 로그 기록 상세 수준은 **분석** 수준으로 설정되어 있습니다. **고급 로깅 중지**를 클릭하여 좀 더 일찍 중지한 경우를 제외하고 고급 로깅은 두 시간 뒤에 자동으로 비활성화됩니다. 모든 로그가 생성되면, 생성된 로그를 사용하여 분석 폴더에 직접 접근하라고 알려 주는 알림 창이 표시됩니다.

고급 설정

고급 설정을 사용하면 필요에 맞게 자세한 ESET Endpoint Security 설정을 구성할 수 있습니다.

고급 설정을 열려면 기본 프로그램 창을 열고 키보드에서 **F5** 키를 누르거나 **설정** > **고급 설정**을 클릭합니다.

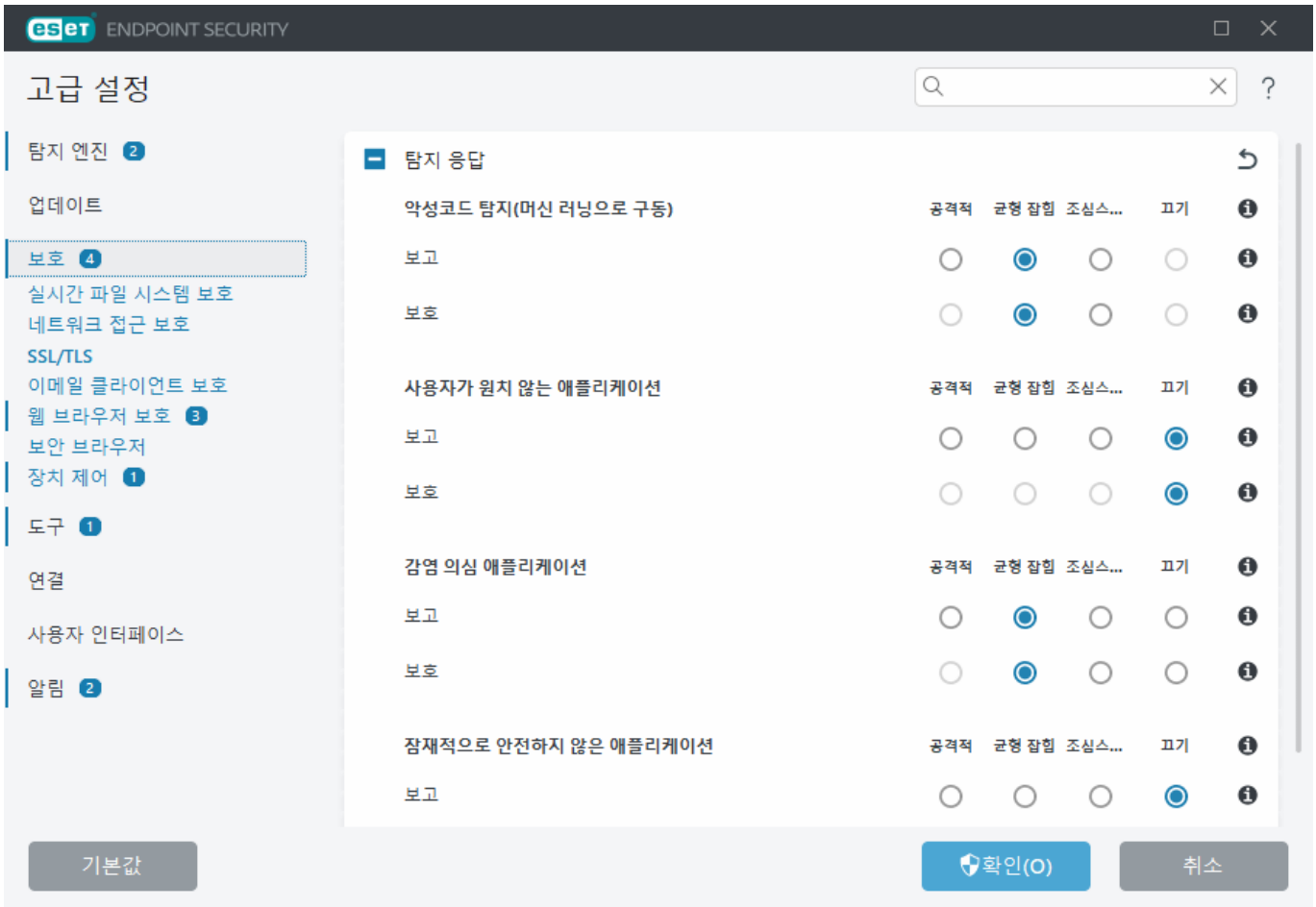
ESET PROTECT 웹 콘솔에서 정책을 생성할 때 설정별로 플래그를 선택할 수 있습니다. 강제 적용 플래그가 포함된 설정은 우선적으로 지정되며 이후 정책으로 덮어쓸 수 없습니다(이후 정책에 강제 적용 플래그가 포함된 경우에도 마찬가지임). 따라서 이 설정은 변경되지 않습니다(예를 들어 병합하는 동안 이후 정책 또는 또는 사용자에 의해 변경되지 않음). 자세한 내용은 ESET PROTECT 온라인 도움말의 플래그를 참조하십시오.

접근 설정에 따라 따라 고급 설정을 열려면 패스워드를 입력하라는 메시지가 표시될 수 있습니다.

고급 설정에서 다음 설정을 구성할 수 있습니다.

- 탐지 엔진
- 업데이트

- 보호
- 도구
- 연결
- 사용자 인터페이스
- 알림



탐지 엔진

고급 설정 > **탐지 엔진**을 사용하여 다음 옵션을 구성할 수 있습니다.

- 제외
- 고급 옵션
- 네트워크 트래픽 검사기

제외

제외에서는 개체를 탐지 엔진에서 제외할 수 있습니다. 모든 개체를 검사하려면 반드시 필요한 항목만 제외로 생성하는 것이 좋습니다. 검사 중 컴퓨터 속도를 저하시키는 대용량 DB 항목 또는 검사와 충돌하는 소프트웨어 등의 개체를 제외해야 하는 상황이 있을 수 있습니다.

성능 제외 – 파일 및 폴더를 검사에서 제외합니다. 성능 제외는 게임 애플리케이션의 파일 수준 검사를 제외하려는 경우나 비정상적인 시스템 동작을 유발하는 경우나 성능 향상을 위한 경우에 유용합니다.

탐지 제외 - 탐지 이름, 경로 또는 해당 해시를 사용하여 치료에서 개체를 제외할 수 있습니다. 탐지 제외는

성능 제외와 달리, 검사에서 파일 및 폴더를 제외하지 않습니다. 탐지 제외는 개체가 탐지 엔진에서 탐지되고 제외 목록에 해당 규칙이 있는 경우에만 개체를 제외합니다.

다음과 같은 다른 유형의 제외와 혼동하지 마십시오.

- 프로세스 제외 – 제외된 애플리케이션 프로세스에 관련된 모든 파일 작업이 검사에서 제외됩니다(백업 속도 및 서비스 가용성을 향상시키는 데 필요할 수 있음).
- 제외된 파일 확장명
- HIPS 제외
- 클라우드 기반 보호를 위한 제외 필터

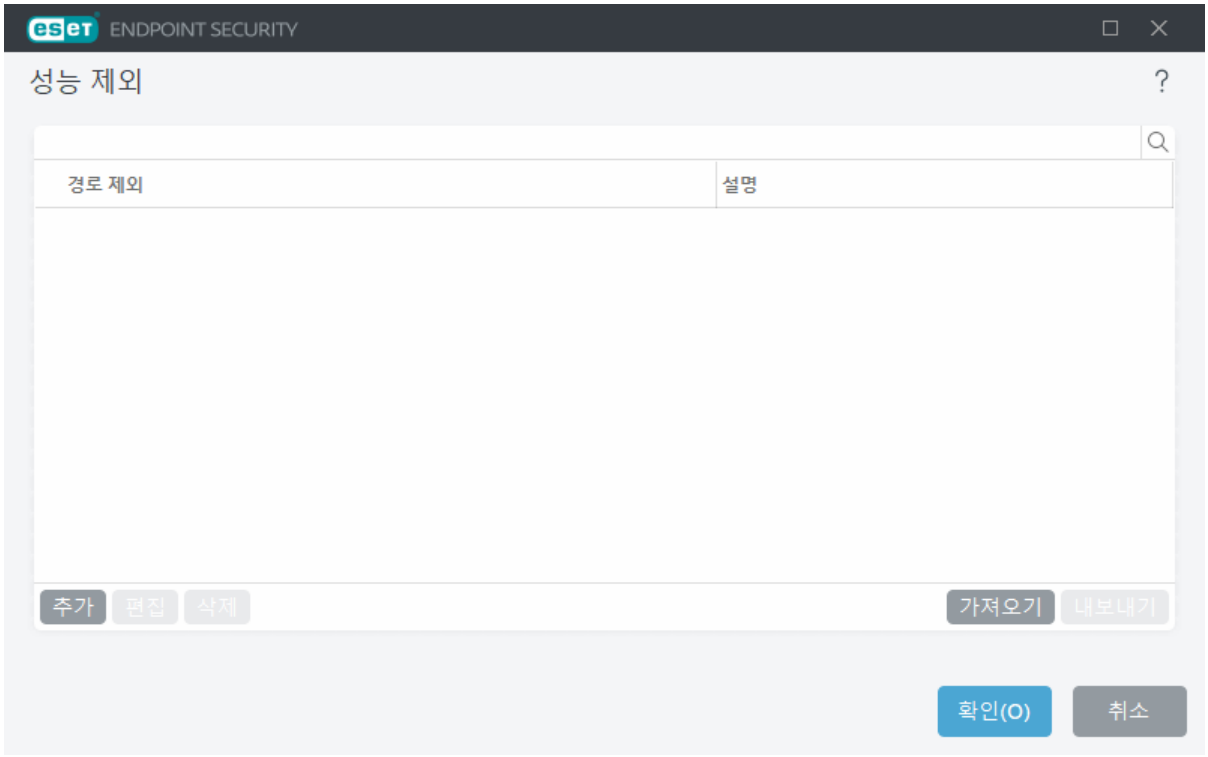
성능 제외

성능 제외를 사용하여 파일 및 폴더를 검사에서 제외할 수 있습니다.

모든 개체에서 위협 요소가 있는지 검사하려면 반드시 필요한 경우에만 성능 제외를 생성하는 것이 좋습니다. 그러나 검사 중 컴퓨터 속도를 저하시키는 대용량 DB 항목 또는 검사와 충돌하는 소프트웨어 등의 개체를 제외해야 할 수 있는 상황이 있습니다.

고급 설정 > **탐지 엔진** > **제외** > **성능 제외** > **편집**을 통해 검사에서 제외할 파일과 폴더를 제외 목록에 추가할 수 있습니다.

검사에서 개체를 제외(경로: 파일 또는 폴더)하려면 **추가**를 클릭하고 해당 경로를 입력하거나 트리 구조에서 선택합니다.



파일이 검사 제외 조건을 충족할 경우 파일 내 위협 요소는 **실시간 파일 시스템 보호** 모듈이나 **컴퓨터 검사** 모듈을 통해 검색되지 않습니다.

제어 요소

- **추가** – 검사에서 개체를 제외할 새 항목을 추가합니다.
- **편집** - 선택한 항목을 편집할 수 있습니다.
- **삭제** - 선택한 항목을 제거합니다(여러 항목을 선택하려면 CTRL + 클릭).
- **가져오기/내보내기** – 성능 제외 가져오기 및 내보내기는 나중에 사용하기 위해 현재 제외 항목을 백업해야 하는 경우 유용합니다. 또한 내보내기 설정 옵션은 여러 시스템에서 기본 구성을 사용하려는 관리되지 않는 환경의 사용자에게 편리합니다. .txt 파일을 쉽게 가져와 이러한 설정을 전송할 수 있기 때문입니다.

  ^ 파일 가져오기/내보내기 형식의 예 표시

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

성능 제외 추가 또는 편집

이 대화 상자 창에서는 이 컴퓨터의 특정 경로(파일 또는 디렉토리)를 제외합니다.

적절한 경로를 선택하려면 **경로** 필드에서 **...**를 클릭합니다.
수동으로 입력할 경우 아래의 추가 제외 형식 예를 참조하십시오.

와일드카드를 사용하여 파일 그룹을 제외할 수 있습니다. 물음표(?)는 단일 문자를 나타내고 별표(*)는 0개 이상의 문자로 구성된 문자열을 나타냅니다.

• 폴더에 있는 모든 파일과 하위 폴더를 제외하려면 폴더 경로를 입력하고 *마스크를 사용합니다.
• doc 파일만 제외하려면 **.doc* 마스크를 사용합니다.
• 실행 파일 이름에 각각 다른 문자가 특정 개수 포함되어 있고 그중 첫 문자(예: "D")만 알고 있는 경우에는
D????.exe(물음표는 누락되거나 알 수 없는 문자를 대체)
예:
• *C:\Tools** – 폴더와 폴더 콘텐츠(파일 및 하위 폴더)가 제외됨을 나타내려면 경로가 백슬래시 (\)와 (*) 별표로 끝나야 합니다.
• *C:\Tools*.** – *C:\Tools**와 동일한 동작입니다.
• *C:\Tools* – *Tools* 폴더는 제외되지 않습니다. 검사기 관점에서 볼 때는 *Tools*도 파일 이름일 수 있습니다.
• *C:\Tools*.dat* – *Tools* 폴더에서 .dat 파일을 제외합니다.
• *C:\Tools\sg.dat* - 정확한 경로에 있는 이 특정 파일을 제외합니다.

%PROGRAMFILES% 등의 시스템 변수를 사용하여 검사 제외 항목을 정의할 수 있습니다.
• 이 시스템 변수를 사용하여 프로그램 파일 폴더를 제외하려면 제외 항목 추가 시 *%PROGRAMFILES%**(경로 끝에 백슬래시 및 별표를 추가해야 함) 경로 사용.
• *%PROGRAMFILES%* 하위 디렉토리의 모든 파일 및 폴더를 제외하려면 *%PROGRAMFILES%\Excluded_Directory** 경로 사용

지원되는 시스템 변수 목록 확장

경로 제외 형식에 다음 변수를 사용할 수 있습니다.
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
사용자별 시스템 변수(*%TEMP%* 또는 *%USERPROFILE%* 등) 또는 환경 변수(*%PATH%* 등)는 지원되지 않습니다.

경로 중간에 와일드카드를 사용(예: *C:\Tools*\Data\file.dat*)하면 작동할 수는 있지만 성능 제외 시 공식적으로 지원되지 않습니다. 자세한 내용은 다음 지식베이스 문서를 참조하십시오.
탐지 제외를 사용할 때는 경로 중간에 자유롭게 와일드카드를 사용할 수 있습니다.

제외 순서:
• 맨 위로/맨 아래로 버튼을 사용하여 제외 우선순위 수준을 조정하는 옵션(규칙이 위에서 아래 순서로 실행되는 방화벽 규칙의 경우)은 없습니다.
• 첫 번째 적용 규칙이 검사기와 일치하는 경우 두 번째 규칙은 평가되지 않습니다.
• 규칙이 적을수록 검사 결과가 더 좋아집니다.
• 동시 규칙 생성 피하기.

경로 제외 형식

와일드카드를 사용하여 파일 그룹을 제외할 수 있습니다. 물음표(*?*)는 단일 문자를 나타내고 별표(*)는 0개 이상의 문자로 구성된 문자열을 나타냅니다.

• 폴더에 있는 모든 파일과 하위 폴더를 제외하려면 폴더 경로를 입력하고 *마스크를 사용합니다.
• doc 파일만 제외하려면 **.doc* 마스크를 사용합니다.
• 실행 파일 이름에 각각 다른 문자가 특정 개수 포함되어 있고 그중 첫 문자(예: "D")만 알고 있는 경우에는
D????.exe(물음표는 누락되거나 알 수 없는 문자를 대체)
예:
• *C:\Tools** – 폴더와 폴더 콘텐츠(파일 및 하위 폴더)가 제외됨을 나타내려면 경로가 백슬래시 (\)와 (*) 별표로 끝나야 합니다.
• *C:\Tools*.** – *C:\Tools** 와 동일한 동작입니다.
• *C:\Tools* – *Tools* 폴더는 제외되지 않습니다. 검사기 관점에서 볼 때는 *Tools*도 파일 이름일 수 있습니다.
• *C:\Tools*.dat* – *Tools* 폴더에서 .dat 파일을 제외합니다.
• *C:\Tools\sg.dat* - 정확한 경로에 있는 이 특정 파일을 제외합니다.

%PROGRAMFILES% 등의 시스템 변수를 사용하여 검사 제외 항목을 정의할 수 있습니다.
• 이 시스템 변수를 사용하여 프로그램 파일 폴더를 제외하려면 제외 항목 추가 시 *%PROGRAMFILES%** (경로 끝에 백슬래시 및 별표를 추가해야 함) 경로 사용.
• *%PROGRAMFILES%* 하위 디렉토리의 모든 파일 및 폴더를 제외하려면 *%PROGRAMFILES%\Excluded_Directory** 경로 사용

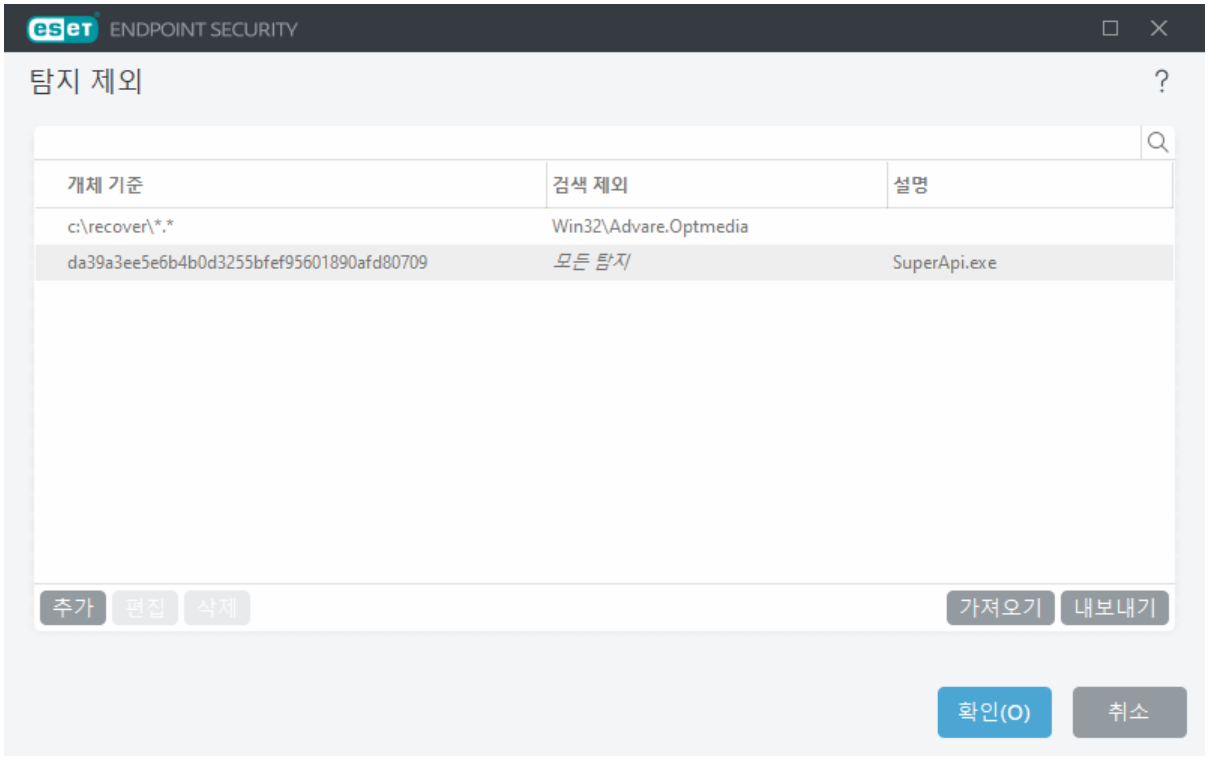
지원되는 시스템 변수 목록 확장

경로 제외 형식에 다음 변수를 사용할 수 있습니다.
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
사용자별 시스템 변수(*%TEMP%* 또는 *%USERPROFILE%* 등) 또는 환경 변수(*%PATH%* 등)는 지원되지 않습니다.

탐지 제외

탐지 제외에서는 탐지 이름, 개체 경로 또는 해당 해시를 필터링하여 치료에서 개체를 제외할 수 있습니다.

탐지 제외는 성능 제외와 달리, 검사에서 파일 및 폴더를 제외하지 않습니다. 탐지 제외는 개체가 탐지 엔진에서 탐지되고 제외 목록에 해당 규칙이 있는 경우에만 개체를 제외합니다.
예를 들어(아래 이미지의 첫 번째 행 참조), 개체가 Win32/Adware.Optmedia로 탐지되며 탐지된 파일이 *C:\Recovery\file.exe*인 경우입니다. 두 번째 행에서 해당 SHA-1 해시가 있는 각 파일은 탐지 이름과 관계없이 항상 제외됩니다.



모든 위협을 탐지하려면 반드시 필요할 때만 탐지 제외를 생성하는 것이 좋습니다.

파일 또는 폴더를 제외 목록에 추가하려면 고급 설정 > **탐지 엔진** > **제외** > **탐지 제외** > **편집**을 엽니다.

치료에서 개체를 제외(해당 탐지 이름 또는 해시별로)하려면 **추가**를 클릭합니다.

사용자가 원치 않는 애플리케이션과 잠재적으로 안전하지 않은 애플리케이션의 경우 다음과 같이 탐지 이름별로도 제외를 생성할 수 있습니다.

- 탐지를 보고하는 경고 창(**고급 옵션 표시**를 클릭한 다음 **탐지에서 제외** 선택)
- 탐지 제외 생성 마법사를 사용하여 로그 파일 오른쪽 마우스 버튼 메뉴에서 선택
- **도구** > **검역소**를 클릭하고 검역소에 있는 파일을 오른쪽 마우스 버튼으로 클릭한 다음 오른쪽 마우스 버튼 메뉴에서 **복원 후 검사에서 제외** 선택

탐지 제외 개체 기준

- **경로** – 지정된 경로(또는 임의 경로)로 탐지 제외를 제한합니다.
- **탐지 이름** – 제외된 파일 옆에 탐지 이름이 있는 경우 해당 파일은 완전히 제외된 것이 아니라 지정된 탐지에 한해 제외된 것입니다. 해당 파일이 나중에 다른 악성코드에 감염되면 이 파일은 탐지됩니다.
- **해시** – 파일 형식, 위치, 이름 또는 해당 확장명에 상관없이 지정된 해시SHA-1에 따라 파일을 제외합니다.

제어 요소

- **추가** – 치료에서 개체를 제외할 새 항목을 추가합니다.
- **편집** - 선택한 항목을 편집할 수 있습니다.
- **삭제** - 선택한 항목을 제거합니다(여러 항목을 선택하려면 CTRL + 클릭).

- **가져오기/내보내기** – 탐지 제외 가져오기 및 내보내기는 나중에 사용하기 위해 현재 제외 항목을 백업해야 하는 경우 유용합니다. 또한 내보내기 설정 옵션은 여러 시스템에서 기본 구성을 사용하려는 관리되지 않는 환경의 사용자에게 편리합니다. .txt 파일을 쉽게 가져와 이러한 설정을 전송할 수 있기 때문입니다.

  ^ 파일 가져오기/내보내기 형식의 예 표시

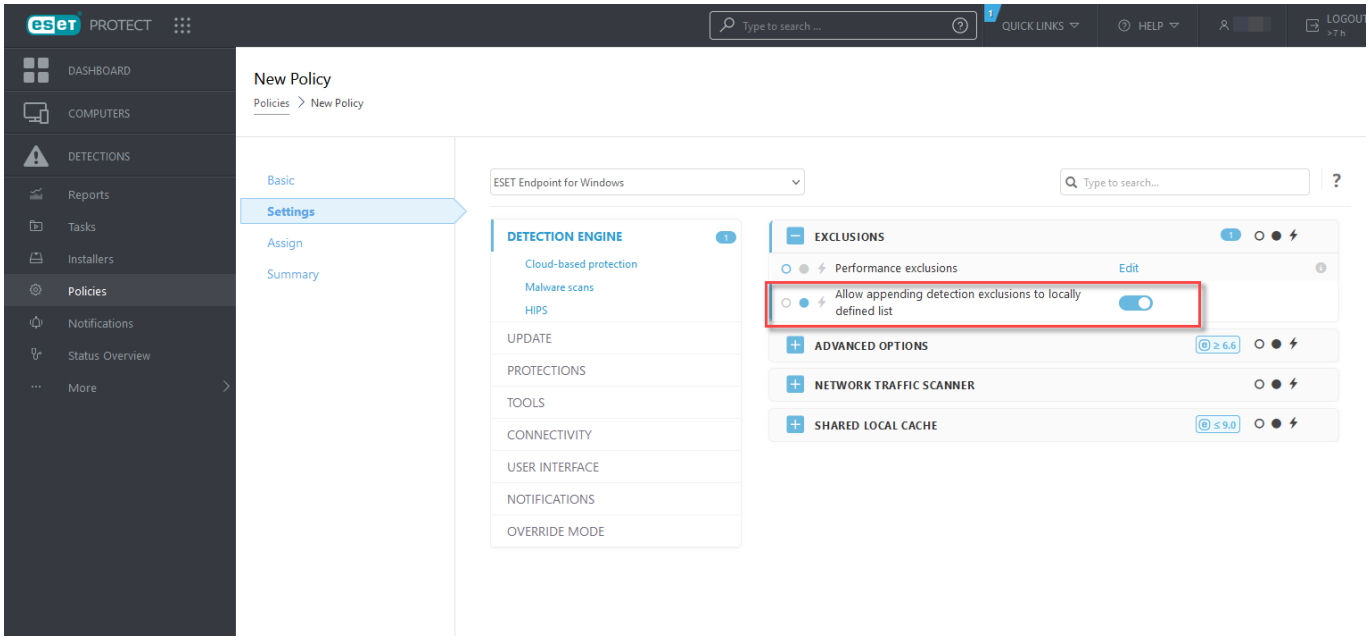
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

ESET PROTECT에서의 탐지 제외 설정

ESET PROTECT 탐지 제외 관리 마법사 - 탐지 제외를 생성하고 추가 컴퓨터/그룹에 적용합니다.

ESET PROTECT에서 탐지 제외 재정의 가능

기존에 탐지 제외 로컬 목록이 있는 경우 관리자는 **로컬로 정의된 목록에 탐지 제외 추가 허용**을 사용해서 정책을 적용해야 합니다. 그러면 ESET PROTECT에서 탐지 제외 추가가 예상대로 작동합니다.



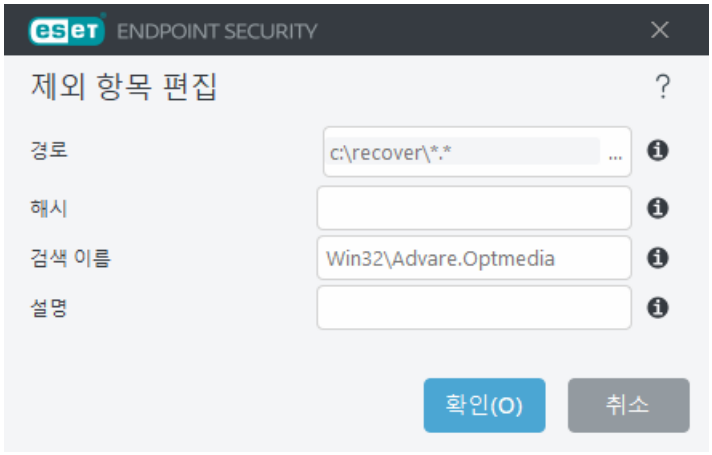
탐지 제외 추가 또는 편집

검색 제외

유효한 ESET 탐지 이름을 입력해야 합니다. 유효한 탐지 이름의 경우 로그 파일을 참조한 다음 로그 파일 드롭다운 메뉴에서 **검색**을 선택합니다. 이는 ESET Endpoint Security에서 가양성 샘플이 탐지되는 경우 유용합니다. 실제 침입에 대한 제외는 매우 위험하므로, **경로** 필드에서 **...**를 클릭하여 영향을 받는 파일/디렉토리

를 제외하거나 일시적으로만 제외하는 것이 좋습니다. 를 클릭하여 영향을 받는 파일/디렉토리를 제외하거나 일시적으로만 제외하는 것이 좋습니다. 제외는 사용자가 원치 않는 애플리케이션, 잠재적으로 안전하지 않은 애플리케이션 및 감염 의심 애플리케이션에도 적용됩니다.

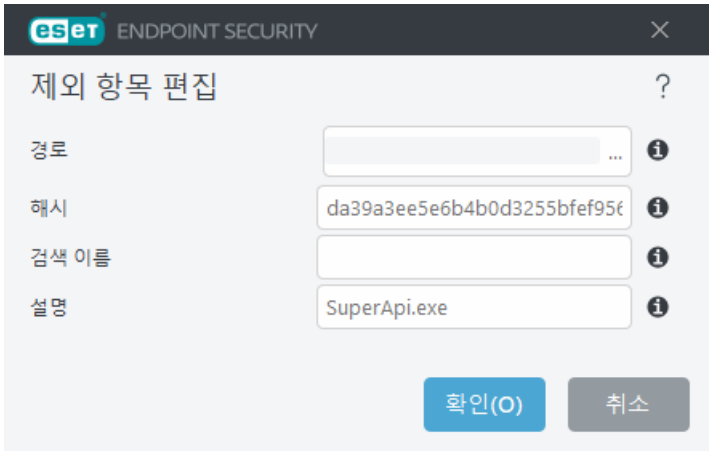
경로 제외 형식도 참조하십시오.



아래에서 탐지 제외 예를 참조하십시오.

해시 제외

파일 형식, 위치, 이름 또는 해당 확장명에 상관없이 지정된 해시SHA-1에 따라 파일을 제외합니다.



이름을 기준으로 특정 위협을 제외하려면 다음과 같이 유효한 탐지 이름을 입력합니다.
Win32/Adware.Optmedia
ESET Endpoint Security 경고 창에서 탐지를 제외할 때 다음 형식도 사용할 수 있습니다.
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

제어 요소

- **추가** - 개체를 검색에서 제외합니다.
- **편집** - 선택한 항목을 편집할 수 있습니다.

- **삭제** - 선택한 항목을 제거합니다(여러 항목을 선택하려면 CTRL + 클릭).

탐지 제외 생성 마법사

탐지 제외를 로그 파일 오른쪽 마우스 버튼 메뉴에서도 생성할 수 있습니다(악성코드 탐지에서는 사용할 수 없음).

1. 기본 프로그램 창에서 **도구** > **로그 파일**을 클릭합니다.
2. **탐지 로그**에서 탐지를 마우스 오른쪽 버튼으로 클릭합니다.
3. **제외 생성**을 클릭합니다.

제외 기준을 토대로 하나 이상의 탐지를 제외하려면 **기준 변경**을 클릭합니다.

- **정확한 파일** - SHA-1 해시별로 각 파일을 제외합니다.
- **탐지** - 탐지 이름별로 각 파일을 제외합니다.
- **경로 + 탐지** - 파일 이름을 포함하여 탐지 이름 및 경로별로 각 파일을 제외합니다(예: *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

권장 옵션은 탐지 유형에 따라 미리 선택됩니다.

경우에 따라 **제외 생성**을 클릭하기 전에 **설명**을 추가할 수 있습니다.

탐지 엔진 고급 옵션

AMSI를 통한 고급 검사 활성화는 PowerShell 스크립트, Windows Script Host에서 실행된 스크립트 및 AMSI SDK를 사용하여 검사한 데이터를 검사할 수 있는 Microsoft AMSI(Antimalware Scan Interface) 도구입니다.

네트워크 트래픽 검사기

네트워크 트래픽 검사기는 여러 고급 악성코드 검사 기술을 통합하는 애플리케이션 프로토콜에 대한 악성코드 방지 기능을 제공합니다. 네트워크 트래픽 검사기는 인터넷 브라우저나 이메일 클라이언트에 관계없이 HTTP(S), POP3(S) 및 IMAP(S) 프로토콜을 자동으로 검사합니다. 고급 설정 > **탐지 엔진** > **네트워크 트래픽 검사기**에서 네트워크 트래픽 검사기를 활성화/비활성화할 수 있습니다.

네트워크 트래픽 검사기 활성화 - 이 옵션을 비활성화하면 HTTP(S), POP3(S) 및 IMAP(S) 프로토콜이 검사되지 않습니다. 다음 ESET Endpoint Security 기능을 사용하려면 네트워크 트래픽 검사기가 활성화되어 있어야 합니다.

- 웹 브라우저 보호
- 웹 컨트롤
- 안전한 브라우저
- SSL/TLS
- 안티피싱 보호
- 이메일 클라이언트 보호

클라우드 기반 보호

ESET LiveGrid®(ESET ThreatSense.Net고급 조기 경보 시스템에 구축)에서는 ESET 사용자가 전 세계적으로 제출한 데이터를 활용하고 해당 데이터를 ESET 연구소로 보냅니다. 의심스러운 샘플과 메타데이터를 제공하면 ESET LiveGrid®에서 고객의 요구 사항에 즉각 대응하고 ESET이 최신 위협에 끊임없이 대처하도록 유지할 수 있습니다.

다음과 같은 옵션을 사용할 수 있습니다.

옵션 1: ESET LiveGrid® 평판 시스템 활성화

ESET LiveGrid® 평판 시스템은 클라우드 기반 허용 목록과 차단 목록을 제공합니다.

ESET LiveGrid®에서 제공되는 추가 정보를 사용하여 프로그램 인터페이스나 오른쪽 마우스 버튼 메뉴에서 직접 실행 중인 프로세스와 파일의 평판을 확인하십시오.

옵션 2: ESET LiveGrid® 피드백 시스템 활성화

ESET LiveGrid® 평판 시스템뿐만 아니라 ESET LiveGrid® 피드백 시스템에서는 새로 검출된 위협과 관련된 사용자 컴퓨터의 정보를 수집합니다. 이 정보에는 위협이 나타난 파일의 샘플 또는 복사본, 해당 파일의 경로, 파일 이름, 날짜 및 시간, 해당 위협이 사용자 컴퓨터에 나타난 과정, 사용자 컴퓨터의 운영 체제 관련 정보가 포함될 수 있습니다.

기본적으로 ESET Endpoint Security는 자세한 분석을 위해 ESET 바이러스 연구소로 감염 의심 파일을 전송하도록 구성되어 있습니다. *.doc* 또는 *.xls*와 같은 특정 확장명의 파일은 항상 제외됩니다. 또한 사용자 또는 사용자의 조직에서 전송하지 않으려는 특정 파일이 있는 경우 해당 파일의 확장명을 추가할 수도 있습니다.

옵션 3: ESET LiveGrid®를 활성화하지 않도록 선택

소프트웨어에서 사용하지 못하는 기능은 없지만 일부 경우 ESET LiveGrid®가 활성화되어 있으면 ESET Endpoint Security가 검색 엔진 업데이트보다 새로운 위협에 더 빨리 대응할 수 있습니다.

ESET LiveGrid®에 대한 자세한 내용은 용어집을 참조하십시오.
ESET Endpoint Security에서 ESET LiveGrid®를 활성화 또는 비활성화하는 방법은 영어를 비롯한 여러 국가의 언어로 제공되는 그림이 포함된 지침을 참조하십시오.

고급 설정 내 클라우드 기반 보호 구성

ESET LiveGrid® 설정에 접근하려면 고급 설정 > **탐지 엔진** > **클라우드 기반 보호**를 엽니다.

ESET LiveGrid®에 평판 시스템 활성화(권장) - ESET LiveGrid® 평판 시스템은 검사한 파일을 클라우드의 허용 목록 및 차단 목록 항목에 있는 DB와 비교하여 ESET 맬웨어 방지 솔루션의 효율성을 향상시킵니다.

ESET LiveGrid® 피드백 시스템 활성화 – 추가 분석을 위해 ESET 연구소로 충돌 보고서 및 통계와 함께 관련 전송 데이터(아래 **샘플 전송 섹션**에 설명됨)를 보냅니다.

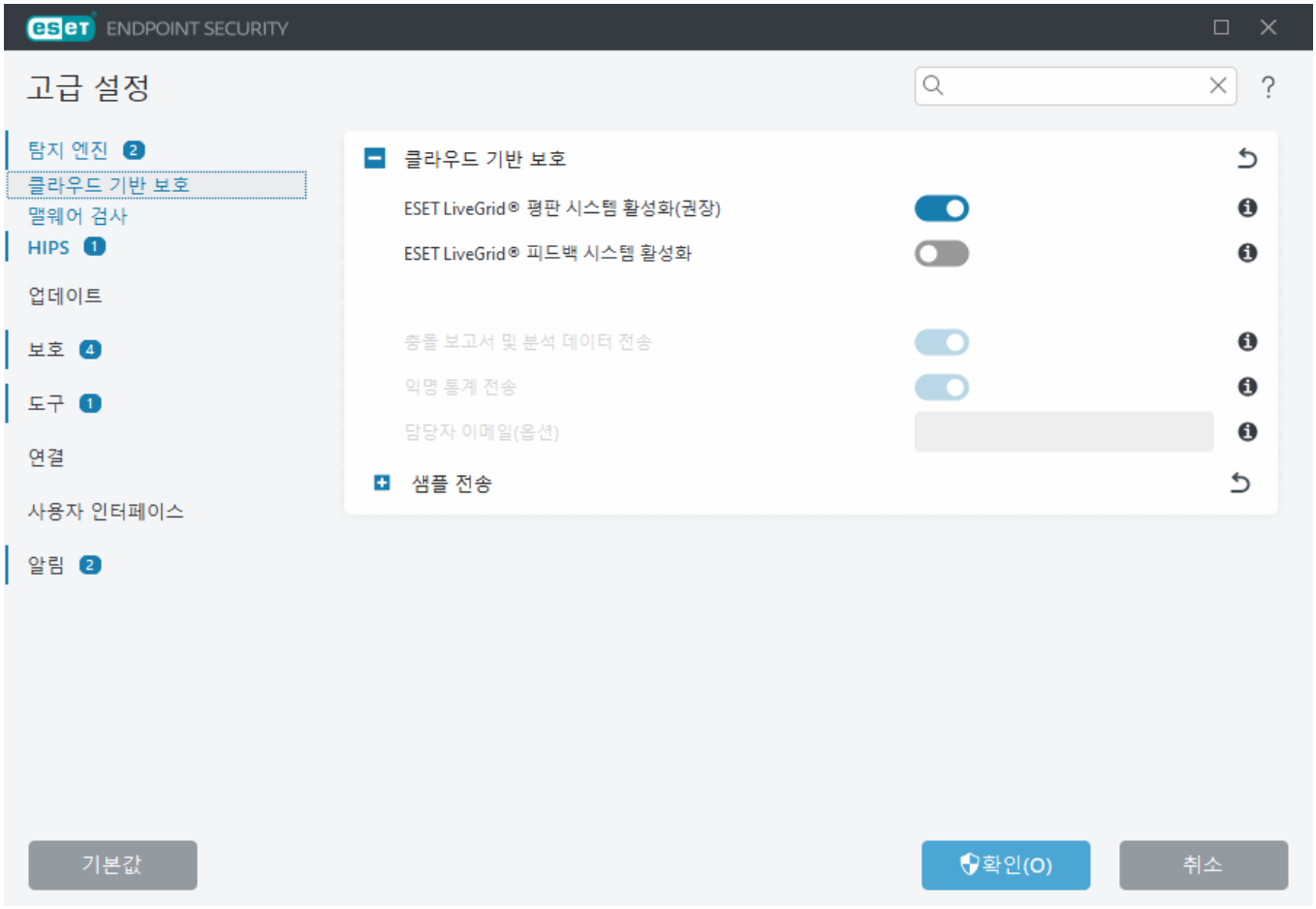
ESET LiveGuard 활성화(ESET LiveGuard는 ESET에서 판매하는 추가 기능이며 기본적으로 제공되지 않음) -

ESET LiveGuard는 ESET에서 제공하는 유료 서비스입니다. 이 서비스의 목적은 발견된 적 없는 위협을 완화하도록 특별히 설계된 보호 계층을 추가하는 데 있습니다. 감염 의심 파일은 ESET 클라우드에 자동으로 전송됩니다. 클라우드에서 해당 파일은 고급 악성코드 탐지 엔진을 통해 분석됩니다. 샘플을 제공한 사용자는 관찰된 '샘플'의 동작이 요약되어 있는 동작 보고서를 받게 됩니다.

충돌 보고서 및 분석 데이터 전송 – 충돌 보고서 및 모듈 메모리 덤프와 같은 ESET LiveGrid® 관련 분석 데이터를 전송합니다. ESET에서 문제를 분석하고, 제품을 개선하며, 최종 사용자 보호 성능을 향상시키도록 하는 데 도움을 주려면 이 기능이 활성화된 상태를 유지하는 것이 좋습니다.

익명 통계 전송 - ESET이 새로 검색된 위협에 대한 정보(위협 이름, 검색 날짜 및 시간, 검색 방법과 관련 메타데이터, 제품 버전 및 시스템 정보를 포함한 구성 등)를 수집하도록 허용합니다.

담당자 이메일(옵션) - 담당자 이메일이 감염 의심 파일에 포함될 수 있으며, 분석 시 추가 정보가 필요한 경우 사용자에게 연락하는 데 사용될 수 있습니다. 추가 정보가 필요한 경우가 아니면 ESET에서는 응답 메시지를 발송하지 않습니다.



샘플 전송

수동 샘플 전송 – 오른쪽 마우스 버튼 메뉴, 검역소 또는 도구에서 ESET에 수동으로 샘플을 전송하는 옵션을 활성화합니다.

탐지된 샘플 자동 전송

분석 및 향후 탐지 성능 개선을 위해 ESET에 전송할 샘플 종류를 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **탐지된 모든 샘플** – 탐지 엔진(검사기 설정에 활성화된 경우 사용자가 원치 않는 애플리케이션 포함)에서 탐지된 모든 개체입니다.
- **문서를 제외한 모든 샘플 – 문서**를 제외하고 탐지된 모든 개체입니다(아래 참조).
- **전송 안 함** – 탐지된 개체를 ESET에 전송하지 않습니다.

감염 의심 샘플 자동 전송

이러한 샘플은 탐지 엔진에서 탐지하지 못하는 경우에도 ESET에 전송됩니다. 예를 들어 탐지를 거의 놓친 샘플 또는 ESET Endpoint Security 보호 모듈 중 하나는 이러한 샘플을 감염이 의심되거나 명확하지 않은 동작을 포함한 것으로 간주합니다.

- **실행 파일** – .exe, .dll, .sys 등의 파일을 포함합니다.
- **압축파일** – .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab 등의 파일 형식을 포함합니다.
- **스크립트** – .bat, .cmd, .hta, .js, .vbs, .ps1 등의 파일 형식을 포함합니다.
- **기타** – .jar, .reg, .msi, .sfw, .lnk 등의 파일 형식을 포함합니다.
- **스팸 의심 이메일** – 이렇게 하면 스팸이 의심되는 부분과 스팸이 의심되는 전체 이메일을 첨부 파일로 ESET에 전송하여 추가 분석할 수 있습니다. 이 옵션을 사용하면 추후 사용자의 스팸 검색 개선을 비롯하여 스팸의 전체 검색 기능이 향상됩니다.
- **문서** – 액티브 콘텐츠가 있거나 없는 Microsoft Office 또는 PDF 문서를 포함합니다.

  포함된 모든 문서 파일 형식의 목록 확장

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

제외

제외 필터를 사용하면 전송 시 특정 파일/폴더를 제외할 수 있습니다. 예를 들어 문서나 스프레드시트와 같은 기밀 정보를 포함할 수 있는 파일을 제외하는 데 유용할 수 있습니다. 나열된 파일에 감염 의심 코드가 있어도 분석을 위해 ESET 연구소로 보내지 않습니다. 가장 일반적인 파일 형식.doc 등)은 기본적으로 제외됩니다. 원하는 경우 제외된 파일 목록에 추가할 수 있습니다.

download.domain.com에서 다운로드한 파일을 제외하려면 고급 설정 > **클라우드 기반 보호** > **샘플 제출** > **제외**로 이동하여 제외를 추가합니다(*download.domain.com*).

샘플의 최대 크기(MB) – 자동으로 제출되는 샘플의 최대 크기(1~64MB)를 정의합니다.

ESET LiveGuard

ESET LiveGuard 웹 콘솔을 사용하여 클라이언트 컴퓨터에서 ESET PROTECT 서비스를 활성화하려면 ESET Endpoint Security에 대한 ESET LiveGuard 구성을 참조하십시오.

ESET LiveGrid®을(를) 이전에 사용하다가 비활성화한 경우 보낼 데이터 패키지가 남아 있을 수 있습니다. 비활성화한 후에도 이러한 패키지는 ESET으로 전송됩니다. 현재 정보가 모두 전송되고 나면 추가 패키지가 생성되지 않습니다.

클라우드 기반 보호를 위한 제외 필터

제외 필터를 사용하면 샘플 전송 시 특정 파일이나 폴더를 제외할 수 있습니다. 나열된 파일에 감염 의심 코드가 있어도 분석을 위해 ESET 연구소로 보내지 않습니다. 일반적인 파일 형식(.doc 등)은 기본적으로 제외됩니다.

이 기능은 문서나 스프레드시트 등 기밀 정보를 포함할 수 있는 파일을 제외하는 데 유용합니다.

download.domain.com에서 다운로드한 파일을 제외하려면 고급 설정 > **탐지 엔진** > **클라우드 기반 보호** > **샘플 제출** > **제외**를 열고 제외(*download.domain.com*)를 추가합니다.

악성코드 검사

악성코드 검사 섹션은 고급 설정 > **탐지 엔진** > **악성코드 검사**에서 접근할 수 있으며, 여기에서 검사 프로필용 검사 파라미터를 구성할 수 있습니다.

수동 검사

선택한 프로필 – 수동 검사기에서 사용되는 특정 파라미터 집합입니다. 새 프로필을 생성하려면 **프로필 목록** 옆의 **편집**을 클릭합니다. 자세한 내용은 검사 프로필을 참조하십시오.

검사 프로필을 선택하면 다음 옵션을 구성할 수 있습니다.

검사 대상 – 특정 대상 또는 대상 그룹을 검사하려면 **검사 대상** 옆의 **편집**을 클릭하고 폴더(트리) 구조에서 옵션을 선택합니다. 자세한 내용은 검사 대상을 참조하십시오.

수동 검사 및 탐지 응답 - 각 검사 프로필에 대한 보고 및 보호 수준을 구성할 수 있습니다. 기본적으로 검사 프로필은 실시간 파일 시스템 보호에 정의된 것과 동일한 설정을 사용합니다. 사용자 지정 보고 및 보호 수준을 구성하려면 **실시간 보호 설정을 사용** 옆의 토글을 비활성화합니다. 보고 및 보호 수준에 대한 자세한 설명은 보호를 참조하십시오.

ThreatSense - 고급 설정 옵션(예: 제어하려는 파일 확장명 및 사용되는 탐지 방법). 자세한 내용은 ThreatSense을(를) 참조하십시오.

검사 프로필

ESET Endpoint Security에는 4개의 미리 정의된 검사 프로필이 있습니다.

- **스마트 검사** - 기본 고급 검사 프로필입니다. 스마트 검사 프로필은 이전 검사에서 깨끗한 것으로 확인되었고 검사 이후 수정되지 않은 파일을 제외하는 스마트 최적화 기술을 사용합니다. 이를 통해 시스템 보안에 최소한의 영향을 미치면서 검사 시간을 단축할 수 있습니다.
- **오른쪽 마우스 버튼 메뉴 검사** - 오른쪽 마우스 버튼 메뉴에서 모든 파일의 수동 검사를 시작할 수 있습니다. 오른쪽 마우스 버튼 메뉴 검사 프로필을 사용하면 이 방법으로 검사를 트리거할 때 사용할 검사 구성을 정의할 수 있습니다.
- **상세 검사** - 상세 검사 프로필은 기본적으로 스마트 최적화를 사용하지 않으므로 이 프로필을 사용하여 검사에서 파일이 제외되지 않습니다.
- **컴퓨터 검사** - 표준 컴퓨터 검사에 사용되는 기본 프로필입니다.

향후 검사를 위해 기본 설정 검사 파라미터를 저장할 수 있습니다. 정기적으로 사용되는 각 검사에 대해 서로 다른 프로필(다양한 검사 대상, 검사 방법 및 기타 파라미터 포함)을 생성하는 것이 좋습니다.

새 프로필을 생성하려면 고급 설정 > **탐지 엔진** > **악성코드 검사** > **수동 검사** > **프로필 목록** > **편집**을 엽니다. **프로필 관리자** 창에는 새 프로필을 생성할 수 있는 옵션 및 기존 검사 프로필이 있는 **선택한 프로필** 드롭다운 메뉴가 포함되어 있습니다. 필요에 맞게 검사 프로필을 생성하는 데 도움을 받으려면 ThreatSense에서 검사 설정의 각 파라미터에 대한 설명을 참조하십시오.

> 고유한 검사 프로필을 생성하려는데 **컴퓨터 검사** 구성이 부분적으로 적합하지만 런타임 패커나 잠재적으로 안전하지 않은 애플리케이션은 검사하고 싶지 않고 **항상 탐지 수정**도 적용하고자 한다고 가정합니다. **프로필 관리자** 창에서 새 프로필의 이름을 입력하고 **추가**를 클릭합니다. **선택한 프로필** 드롭다운 메뉴에서 새 프로필을 선택하고 요구 사항을 충족하도록 나머지 파라미터를 조정한 다음 **확인**을 클릭하여 새 프로필을 저장합니다.

검사 대상

검사 대상 드롭다운 메뉴에서 미리 정의된 검사 대상을 선택할 수 있습니다.

- **프로필 설정으로** - 선택한 검사 프로필에 지정된 대상을 선택합니다.
- **이동식 미디어** - 디스켓, USB 저장 장치, CD/DVD를 선택합니다.
- **로컬 드라이브** - 모든 시스템 하드 드라이브를 선택합니다.
- **네트워크 드라이브** - 매핑된 모든 네트워크 드라이브를 선택합니다.
- **사용자 지정 선택** - 이전 선택 항목을 모두 취소합니다.

폴더(트리) 구조에는 특정 검사 대상도 포함되어 있습니다.

- **운영 메모리** – 운영 메모리에서 현재 사용되는 모든 프로세스와 데이터를 검사합니다.
- **부트 영역/UEFI** – 악성코드가 있는지 부트 영역과 UEFI를 검사합니다. UEFI 스캐너에 대한 자세한 내용은 용어집을 참조하십시오.
- **WMI 데이터베이스** – 전체 Windows Management Instrumentation WMI 데이터베이스, 모든 네임스페이스, 모든 클래스 인스턴스 및 모든 속성을 검사합니다. 감염된 파일 또는 데이터로 포함된 악성코드에 대한 참조를 검색합니다.
- **시스템 레지스트리** – 전체 시스템 레지스트리, 모든 키 및 하위 키를 검사합니다. 감염된 파일 또는 데이터로 포함된 악성코드에 대한 참조를 검색합니다. 탐지 항목을 치료할 때 참조 사항은 레지스트리에 남아 중요한 데이터가 손실되지 않도록 합니다.

검사 대상(파일 또는 폴더)으로 빠르게 이동하려면 트리 구조 아래의 텍스트 필드에 해당 경로를 입력합니다. 경로는 대소문자를 구분합니다. 검사에 대상을 포함하려면 트리 구조에서 대상 확인란을 선택합니다.

유휴 상태 검사

고급 설정의 **탐지 엔진** > **맬웨어 검사** > **유휴 상태 검사**에서 유휴 상태 검사기를 활성화할 수 있습니다.

유휴 상태 검사

이 기능을 활성화하려면 **유휴 상태 검사 활성화** 옆의 토글을 활성화합니다. 컴퓨터가 유휴 상태이면 모든 로컬 드라이브에서 자동 컴퓨터 검사가 수행됩니다.

기본적으로 컴퓨터(노트북)가 배터리 전원으로 작동될 때에는 유휴 상태 검사기가 실행되지 않습니다. 고급 설정에서 **컴퓨터의 전원이 배터리로 공급되더라도 실행** 옆의 토글을 활성화하면 이 설정을 재정의할 수 있습니다.

로그 파일 섹션(기본 프로그램 창에서 **도구 > 로그 파일**을 클릭하고 **로그** 드롭다운 메뉴에서 **컴퓨터 검사** 선택)에서 컴퓨터 검사 결과를 기록하려면 고급 설정에서 **로깅 활성화** 옆의 토글을 활성화합니다.

유휴 상태 탐지

유휴 상태 검사기를 트리거하기 위해 충족되어야 하는 전체 조건 목록을 보려면 유휴 상태 탐지 트리거를 참조하십시오.

ThreatSense - 고급 설정 옵션(예: 제어하려는 파일 확장명 및 사용되는 탐지 방법). 자세한 내용은 ThreatSense를 참조하십시오.

유휴 상태 탐지

유휴 상태 탐지 설정은 고급 설정의 **탐지 엔진 > 맬웨어 검사 > 유휴 상태 검사 > 유휴 상태 탐지**에서 구성할 수 있습니다. 이러한 설정은 다음 경우에 유휴 상태 검사에 대한 트리거를 지정합니다.

- **화면 또는 화면 보호기가 꺼짐**
- **컴퓨터 잠금**
- **사용자 로그오프**

다른 유휴 상태 탐지 트리거를 활성화하거나 비활성화하려면 해당하는 각 상태의 토글을 사용합니다.

시작 검사

기본적으로 자동 시작 파일 검사는 시스템을 시작할 때와 검색 엔진을 업데이트하는 동안 수행됩니다. 이 검사는 스케줄러 구성 및 작업에 종속됩니다.

시작 검사 옵션은 **시스템 시작 파일 검사** 스케줄러 작업의 일부로. 설정을 수정하려면 **도구 > 스케줄러**로 이동하고 **자동 시작 파일 검사**를 클릭한 후 **편집**을 클릭합니다. 마지막 단계에 자동 시작 파일 검사 창이 나타납니다. 스케줄러 작업 생성 및 관리에 대한 자세한 내용은 새 작업 생성을 참조하십시오.

ThreatSense - 고급 설정 옵션(예: 제어하려는 파일 확장명 및 사용되는 탐지 방법). 자세한 내용은 ThreatSense를 참조하십시오.

자동 시작 파일 검사

시스템 시작 파일 검사 예약 작업을 생성할 경우 다음 파라미터를 조정하기 위한 몇 가지 옵션이 제공됩니다:

검사 대상 드롭다운 메뉴는 고급 알고리즘을 기반으로 시스템 시작 시 실행되는 파일의 검사 수준을 지정합니다. 파일은 다음 기준에 따라 내림차순으로 정렬됩니다:

- **등록된 모든 파일**(대부분의 파일이 검사됨)

- **거의 사용하지 않는 파일**
- **일반적으로 사용하는 파일**
- **자주 사용하는 파일**
- **가장 자주 사용하는 파일만**(최소의 파일이 검사됨)

두 개의 특정 그룹도 포함됩니다:

- **사용자가 로그온하기 전 실행된 파일** - 사용자가 로그인하지 않은 경우에도 접근할 수 있는 위치의 파일을 포함합니다(서비스, 브라우저 헬퍼 개체, Winlogon 알림, Windows 스케줄러 항목, 알려진 dll 등과 같은 모든 거의 모든 시작 위치 포함).
- **사용자가 로그온한 후 실행된 파일** -사용자가 로그인한 경우에만 접근할 수 있는 위치의 파일을 포함합니다(특정 사용자에 대해서만 실행되는 파일, 일반적으로 *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*의 파일 포함).

위의 각 그룹에서 검사할 파일 목록은 정해져 있습니다. 시스템 시작 시 실행되는 파일에 대해 더 낮은 검사 깊이를 선택하면 검사되지 않은 파일을 열거나 실행할 때 검사합니다.

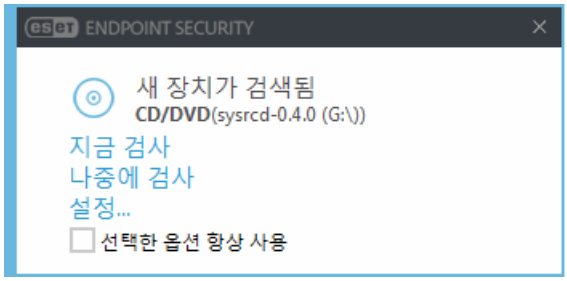
검사 순위 - 검사 시작 시기를 결정하는 데 사용할 우선 순위입니다:

- **유휴 상태일 때** - 시스템이 유휴 상태일 때만 작업이 수행됩니다.
- **가장 낮음** - 시스템 로드가 가장 낮을 경우.
- **더 낮음** - 시스템 로드가 낮을 경우.
- **보통** - 시스템 로드가 평균일 경우.

이동식 미디어

ESET Endpoint Security에서는 컴퓨터에 삽입하면 자동 이동식 미디어(CD/DVD/USB/...) 검사 기능을 제공합니다. 검사 기능을 제공합니다. 이 기능은 컴퓨터 관리자가 원치 않는 콘텐츠가 포함된 이동식 미디어를 사용자가 연결하지 못하도록 하려는 경우에 유용할 수 있습니다.

이동식 미디어를 삽입하고 고급 설정 > **탐지 엔진** > **악성코드 검사** > **이동식 미디어**에서 **검사 옵션 표시**를 설정하면 다음 대화 상자가 표시됩니다.



이 대화 상자의 옵션:

- **지금 검사** - 이동식 미디어에 대한 검사를 트리거합니다.
- **검사 안 함** - 이동식 미디어가 검사되지 않습니다.
- **설정** - 고급 설정을 엽니다.
- **선택한 옵션 항상 사용** - 이후에 이동식 미디어가 삽입될 때마다 같은 작업이 수행됩니다.

이외에도 ESET Endpoint Security에는 지정된 컴퓨터에서 외부 장치 사용을 위한 규칙을 정의할 수 있는 장치

제어 기능이 제공됩니다. 장치 제어에 대한 자세한 내용은 장치 제어 섹션에서 확인할 수 있습니다.

이동식 미디어 검사 설정에 접근하려면 고급 설정 > **탐지 엔진** > **악성코드 검사** > **이동식 미디어**를 엽니다.

이동식 미디어 연결 후 수행할 동작 – 이동식 미디어 장치를 컴퓨터에 연결(CD/DVD/USB)한 경우 수행할 기본 동작을 선택합니다. 이동식 미디어를 컴퓨터에 연결할 때 원하는 동작을 선택합니다.

- **검사 안 함** – 아무런 동작이 수행되지 않고, **새 장치가 탐지됨** 창이 열리지 않습니다.
- **자동 장치 검사** - 연결한 이동식 미디어 장치에 대한 컴퓨터 검사가 수행됩니다.
- **강제 장치 검사** - 삽입된 이동식 미디어 장치에 대한 컴퓨터 검사가 수행되며 취소할 수 없습니다.
- **검사 옵션 표시** - **이동식 미디어** 설정 섹션을 엽니다.

문서 보호

문서 보호 기능을 사용하면 Microsoft Office 문서를 열기 전에 검사하며, Microsoft ActiveX 요소와 같이 Internet Explorer를 통해 자동으로 다운로드한 파일도 검사합니다. 문서 보호 기능은 실시간 파일 시스템 보호 외에 추가적인 보호를 제공하며 대량의 Microsoft Office 문서를 처리하지 않는 시스템의 성능을 향상시키기 위해 비활성화할 수 있습니다.

문서 보호 기능을 활성화하려면 고급 설정 > **탐지 엔진** > **악성코드 검사** > **문서 보호**를 열고 **문서 보호 활성화** 옆의 토글을 클릭합니다.

ThreatSense - 고급 설정 옵션(예: 제어하려는 파일 확장명 및 사용되는 탐지 방법). 자세한 내용은 ThreatSense를 참조하십시오.

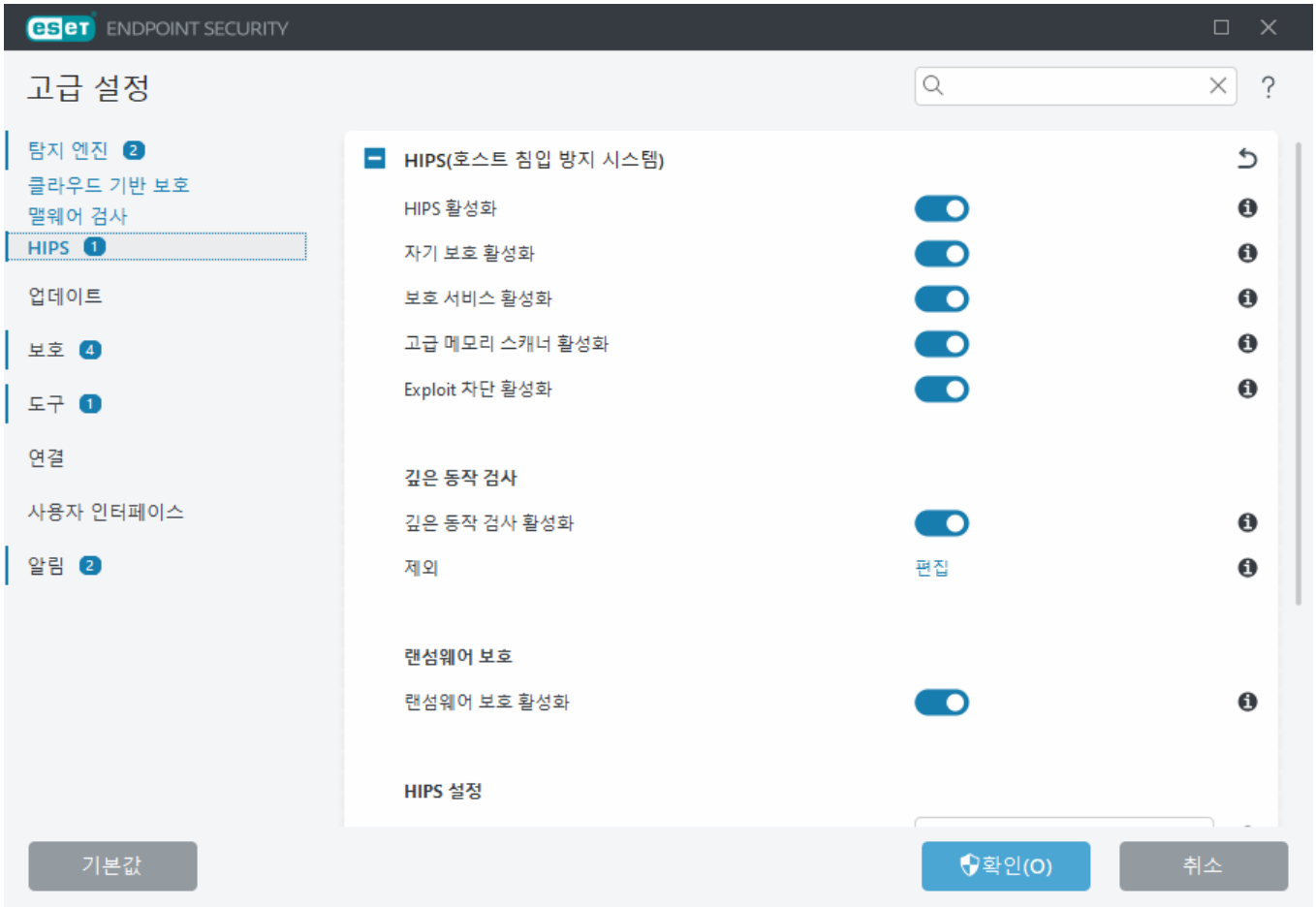
> 이 기능은 Microsoft Antivirus API(예: Microsoft Office 2000 이상 또는 Microsoft Internet Explorer 5.0 이상)를 사용하는 애플리케이션에 의해 활성화됩니다.

HIPS - 호스트 기반 침입 방지 시스템)

> HIPS 설정은 숙련된 사용자만 변경해야 합니다. HIPS 설정을 잘못 구성하면 시스템이 불안정해질 수 있습니다.

HIPS(호스트 기반 침입 방지 시스템)는 컴퓨터에 부정적인 영향을 주려고 시도하는 맬웨어 또는 원치 않는 활동으로부터 시스템을 보호합니다. HIPS는 네트워크 필터링의 검출 기능과 고급 동작 분석 기능을 함께 사용하여 실행 중인 프로세스, 파일 및 레지스트리 키를 모니터링합니다. HIPS는 실시간 파일 시스템 보호와는 별도로 작동하며 방화벽이 아닙니다.

고급 설정 > **탐지 엔진** > **HIPS** > **HIPS**에서 HIPS 설정을 구성할 수 있습니다. HIPS 상태(활성화됨/비활성화됨)는 ESET Endpoint Security 기본 프로그램 창 > **설정** > **컴퓨터**에 표시됩니다.



HIPS(호스트 침입 방지 시스템)

HIPS 활성화 – HIPS는 ESET Endpoint Security에서 기본적으로 활성화되어 있습니다. HIPS를 끄면 Exploit 차단 같은 나머지 HIPS 기능이 비활성화됩니다.

자기 방어 활성화 – ESET Endpoint Security에는 HIPS의 일부로 악의적인 소프트웨어가 안티바이러스 및 안티스파이웨어 보호를 손상시키거나 비활성화하지 못하게 하는 **자기 방어** 기술이 내장되어 있습니다. 자기 방어는 중요한 시스템과 ESET의 프로세스, 레지스트리 키 및 파일이 조작되지 않도록 보호해 줍니다. 설치하는 경우 ESET Management Agent도 보호됩니다.

보호 서비스 활성화 – ESET 서비스(ekrn.exe)에 대한 보호를 활성화합니다. 활성화하면 서비스가 악성코드의 공격을 방어하기 위한 보호 Windows 프로세스로 시작됩니다. 이 옵션은 Windows 8.1 및 Windows 10에서 사용할 수 있습니다.

고급 메모리 검사기 활성화 - Exploit 차단과 함께 작동하여 난독화 또는 암호화를 사용한 맬웨어 방지 제품의 검색을 피하도록 설계된 맬웨어로부터 보호하는 기능을 강화합니다. 고급 메모리 검사기는 기본적으로 활성화되어 있습니다. 이러한 유형의 보호에 대한 자세한 내용은 용어집을 참조하십시오.

Exploit 차단 - 웹 브라우저, PDF 리더, 이메일 클라이언트 및 MS Office 구성 요소와 같은 일반적으로 악용되는 애플리케이션 유형을 강화하도록 설계되었습니다. Exploit 차단은 기본적으로 활성화되어 있습니다. 이러한 유형의 보호에 대한 자세한 내용은 용어집을 참조하십시오.

심층 행위 검사

깊은 동작 검사 활성화 - HIPS 기능의 일부로 작동하는 추가적인 보호 기능입니다. 이 HIPS 확장 기능은 컴퓨

터에서 실행 중인 모든 프로그램의 동작을 분석하고 프로세스의 동작이 악의적인 경우 경고를 표시합니다.

깊은 동작 검사에서 HIPS 제외에서는 프로세스를 분석에서 제외할 수 있습니다. 모든 프로세스에서 가능한 위협이 있는지 검사하려면 반드시 필요한 항목만 제외로 생성하는 것이 좋습니다.

랜섬웨어 쉴드

랜섬웨어 보호 활성화 – HIPS 기능의 일부로 작동하는 추가적인 보호 레이어입니다. 랜섬웨어 보호 기능이 작동하려면 ESET LiveGrid® 평판 시스템이 활성화되어 있어야 합니다. 이러한 유형의 보호에 대한 자세한 내용을 참조하십시오.

Intel® Threat Detection Technology 활성화 – 고유한 Intel CPU 원격 측정을 활용하여 탐지 효율성을 높이고, 오탐지 경고를 낮추며, 가시성을 확장하여 고급 회피 기술을 포착함으로써 랜섬웨어 공격을 탐지하는 데 도움이 됩니다. 지원되는 프로세서를 참조하십시오.

감사 모드 활성화 – 랜섬웨어 보호에서 탐지된 모든 항목이 자동으로 차단되지는 않지만, 보호 심각도를 포함하여 기록되고 "감사 모드" 플래그와 함께 관리 콘솔로 전송됩니다. 관리자는 향후 탐지되지 않도록 해당 탐지를 제외할 것인지, 아니면 활성 상태를 유지할 것인지 결정할 수 있습니다. 이는 곧 감사 모드가 종료되면 해당 항목이 차단 및 제거된다는 뜻입니다. 감사 모드를 활성화/비활성화하면 ESET Endpoint Security에도 기록됩니다. 이 옵션은 ESET PROTECT 정책 구성 편집에서만 사용할 수 있습니다.

HIPS 설정

필터링 모드는 다음 모드 중 하나로 수행할 수 있습니다.

필터링 모드	설명
자동 모드	시스템을 보호하는 미리 정의된 규칙에 의해 차단된 규칙을 제외한 작업이 활성화됩니다.
스마트 모드	매우 의심스러운 이벤트에 한해 사용자에게 알림을 표시합니다.
대화 모드	작업을 확인하라는 메시지가 표시됩니다.
정책 기반 모드	작업을 허용하는 특정 규칙에 의해 정의되지 않은 모든 작업을 차단합니다.
학습 모드	작업이 활성화되고 각 작업 후 규칙이 생성됩니다. 이 모드에서 생성된 규칙은 **HIPS 규칙** 편집기에서 볼 수 있지만, 해당 우선 순위는 수동으로 생성한 규칙이나 자동 모드에서 생성한 규칙의 우선 순위보다 낮습니다. **필터링 모드** 드롭다운 메뉴에서 **학습 모드**를 선택하면 **학습 모드 종료** 설정을 사용할 수 있게 됩니다. 학습 모드를 사용할 시간 범위를 선택합니다. 최대 기간은 14일입니다. 지정된 기간이 경과하면 HIPS에서 생성한 규칙을 편집하라는 메시지가 표시됩니다(학습 모드 상태임). 또한 다른 필터링 모드를 선택하거나, 결정을 미루고 학습 모드를 계속 사용할 수 있습니다.

학습 모드 만료 후에 설정된 모드 - 학습 모드 만료 후에 사용할 필터링 모드를 선택합니다. 만료 후 **사용자에게 요청** 옵션을 사용하려면 HIPS 필터링 모드를 변경할 수 있는 관리자 권한이 필요합니다.

HIPS 시스템은 운영 체제 내의 이벤트를 모니터링하고 규칙(방화벽에서 사용된 규칙과 유사)에 따라 적절하게 반응합니다. **규칙** 옆의 **편집**을 클릭하여 **HIPS 규칙** 편집을 엽니다. HIPS 규칙 창에서 규칙을 선택, 추가, 편집하거나 제거할 수 있습니다. 규칙 생성과 HIPS 작업에 대한 자세한 내용은 HIPS 규칙 편집에서 확인할 수 있습니다.

HIPS 제외

제외를 사용하면 HIPS 깊은 동작 검사에서 프로세스를 제외할 수 있습니다.

HIPS 제외를 편집하려면 고급 설정 > **탐지 엔진** > **HIPS** > **HIPS** > **제외** > **편집**을 엽니다.

> 제외된 파일 확장명, 탐지 제외, 성능 제외 또는 프로세스 제외와 혼동하지 마십시오.

특정 개체를 검사에서 제외하려면 **추가**를 클릭하고 개체 경로를 입력하거나 트리 구조에서 선택합니다. 선택한 항목을 편집 또는 삭제할 수도 있습니다.

HIPS 고급 설정

다음 옵션은 애플리케이션의 동작을 디버깅하고 분석하는 데 유용합니다.

드라이버 로드가 항상 허용됨 - 선택한 드라이버는 사용자가 명백하게 차단한 경우를 제외하고 구성된 필터링 모드에 상관없이 항상 로드할 수 있습니다.

차단된 모든 작업 기록 - 차단된 모든 작업이 HIPS 로그에 기록됩니다. 이 기능은 매우 큰 로그 파일을 생성하여 컴퓨터 속도가 저하될 수 있으므로, ESET 기술 지원 부서에서 요청하거나 문제를 해결하는 경우에만 사용하십시오.

시작 애플리케이션에서 변경사항 발생 시 알림 - 시스템 시작 시 애플리케이션이 추가되거나 제거될 때마다 바탕 화면 알림을 표시합니다.

드라이버 로드가 항상 허용됨

이 목록에 표시된 드라이버는 사용자 규칙에 의해 명백하게 차단된 경우를 제외하고 HIPS 필터링 모드에 상관없이 항상 로드할 수 있습니다.

추가 - 새 드라이버를 추가합니다.

편집 - 선택한 드라이버를 편집합니다.

제거 - 목록에서 드라이버를 제거합니다.

다시 설정 - 시스템 드라이버 집합을 다시 로드합니다.

> 수동으로 추가한 드라이버를 포함하지 않으려면 **다시 설정**을 클릭합니다. 이 작업은 여러 개의 드라이버를 추가하고 목록에서 이 드라이버를 수동으로 삭제할 수 없는 경우 유용할 수 있습니다.

> 설치 후에는 드라이버 목록이 비어 있습니다. 시간이 지남에 따라 ESET Endpoint Security이(가) 목록을 자동으로 채웁니다.

> 항상 로드할 수 있는 드라이버는 장치마다 다르며 ESET PROTECT 정책을 사용하여 편집할 수 없습니다. 설치 후에는 드라이버 목록이 비어 있습니다. 시간이 지남에 따라 ESET Endpoint Security이(가) 목록을 자동으로 채웁니다.

HIPS 대화 창

HIPS 알림 창에서 HIPS가 검출하는 새로운 동작을 기반으로 하여 규칙을 생성한 다음 해당 동작을 허용하거나 거부할 조건을 정의할 수 있습니다.

알림 창에서 생성된 규칙은 수동으로 생성된 규칙과 동일하게 간주되므로. 대화 상자 창에서 생성한 규칙은 대화 상자 창을 트리거한 규칙보다 덜 구체적일 수 있습니다. 이는 이러한 규칙 생성 후 동일한 작업이 같은 창을 트리거할 수 있음을 의미합니다. 자세한 내용은 HIPS 규칙 우선 순위를 참조하십시오.

규칙의 기본 동작이 **매시간 확인**으로 설정된 경우 규칙이 트리거될 때마다 대화 상자 창이 표시됩니다. 여기에서 작업을 **거부** 또는 **허용**하도록 선택할 수 있습니다. 지정된 시간 내에 동작을 선택하지 않으면 규칙에 따라 새 동작이 선택됩니다.

애플리케이션이 종료될 때까지 저장을 사용하면 규칙 또는 필터링 모드가 변경되거나, HIPS 모듈이 업데이트되거나, 시스템이 다시 시작될 때까지 동작(**허용/거부**)을 계속 사용할 수 있습니다. 이러한 세 가지 동작 중 하나가 발생하면 임시 규칙이 삭제됩니다.

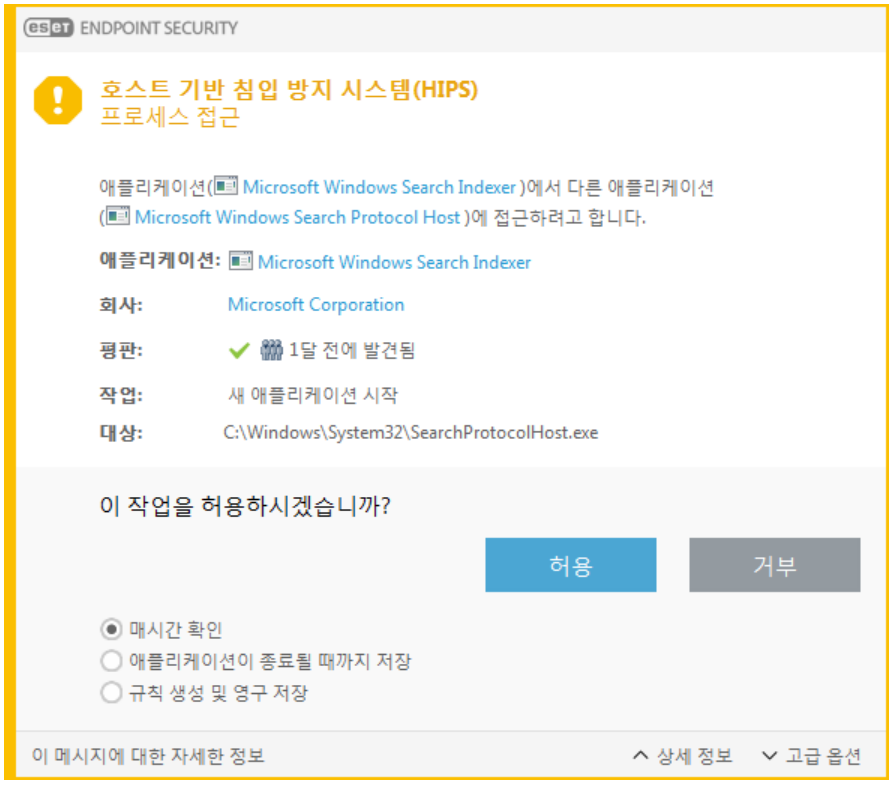
규칙 생성 및 영구 저장 옵션은 나중에 HIPS 규칙 관리 섹션에서 변경할 수 있는(관리자 권한 필요) 새 HIPS 규칙을 생성합니다.

작업을 트리거한 애플리케이션, 파일의 평판 또는 허용 또는 거부를 요청 받은 작업의 종류를 보려면 아래쪽의 **상세 정보**를 클릭합니다.

더 자세한 규칙 파라미터 설정은 **고급 옵션**을 클릭하면 접근할 수 있습니다. 아래 옵션은 **규칙 생성 및 영구 저장**을 선택하는 경우 사용할 수 있습니다.

- **이 애플리케이션에만 유효한 규칙 생성** – 이 확인란 선택을 취소하면 모든 소스 애플리케이션에 대해 규칙이 생성됩니다.
- **작업에만 유효** – 규칙 파일/애플리케이션/레지스트리 작업을 선택합니다. 모든 HIPS 작업의 설명을 참조하십시오.
- **대상에만 유효** – 규칙 파일/애플리케이션/레지스트리 대상을 선택합니다.

> 알림이 표시되는 것을 중지하려면 **고급 설정** > 검색 엔진 > **HIPS** > **기본**에서 필터링 모드를 **자동 모드**로 변경합니다.



잠재적인 랜섬웨어 동작이 검출됨

이 대화 창은 잠재적인 랜섬웨어 동작이 검출될 때 표시됩니다. 여기에서 작업을 **거부** 또는 **허용**하도록 선택할 수 있습니다.

특정 검색 파라미터를 보려면 **상세 정보**를 클릭합니다. 대화 상자 창을 통해 **분석을 위해 전송** 또는 **검색에서 제외**를 선택할 수 있습니다.

ESET LiveGrid®를 올바르게 작동하려면 랜섬웨어 보호에 대해 활성화해야 합니다.

HIPS 규칙 관리

이것은 HIPS 시스템에서 사용자가 정의하고 자동으로 추가된 규칙의 목록입니다. 규칙 생성 및 HIPS 작업에 대한 자세한 내용은 HIPS 규칙 설정 장에서 확인할 수 있습니다. HIPS 일반 원칙도 참조하십시오.

열

규칙 - 사용자가 정의하거나 자동으로 선택된 규칙 이름입니다.

활성화됨 - 목록에서 규칙을 유지하되 사용하지 않으려면 이 스위치를 비활성화합니다.

동작 – 규칙은 조건이 충족되면 수행되어야 하는 동작, 즉 **허용**, **차단** 또는 **확인**을 지정합니다.

소스 - 이 애플리케이션에서 이벤트를 트리거한 경우에만 규칙이 사용됩니다.

대상 - 작업이 특정 파일, 애플리케이션 또는 레지스트리 항목과 관련된 경우에만 규칙이 사용됩니다.

로깅 심각도 - 이 옵션을 활성화하면 이 규칙에 대한 정보가 HIPS 로그에 기록됩니다.

알림 – 이벤트가 트리거되면 오른쪽 아래의 모서리에 알림이 나타납니다.

제어 요소

추가 - 새 규칙을 생성합니다.

편집 - 선택한 항목을 편집할 수 있습니다.

제거 - 선택한 항목을 제거합니다.

HIPS 규칙 우선 순위

맨 위로/맨 아래로 버튼을 사용하여 HIPS 규칙의 우선순위 수준을 조정하는 옵션(규칙이 위에서 아래 순서로 실행되는 방화벽 규칙의 경우)은 없습니다.

- 생성하는 모든 규칙의 우선 순위는 동일합니다
- 규칙이 구체적일수록 우선 순위가 높아집니다(예를 들어 특정 애플리케이션에 대한 규칙은 모든 애플리케이션에 대한 규칙보다 우선 순위가 높습니다)
- 내부적으로 HIPS에는 사용자가 접근할 수 없는 보다 우선 순위가 높은 규칙이 포함되어 있습니다(예를 들어 자기 방어 정의 규칙은 재정의할 수 없습니다)
- 생성하는 규칙 중 운영 체제를 동결할 수 있는 규칙은 적용되지 않습니다(가장 낮은 우선 순위를 갖게 됨)

HIPS 규칙 설정

먼저 HIPS 규칙 관리를 참조하십시오.

규칙 이름 - 사용자 정의 규칙 이름이거나 자동으로 선택된 규칙 이름입니다.

동작 - 조건이 충족되면 수행되어야 하는 동작, 즉 **허용**, **차단** 또는 **확인**을 지정합니다.

영향을 주는 작업 - 규칙이 적용되는 작업 유형을 선택해야 합니다. 이 유형의 작업 및 선택한 대상에 대해서만 규칙이 사용됩니다.

활성화됨 - 목록에서 규칙을 유지하되 적용하지 않으려면 토글을 비활성화합니다.

로깅 심각도 - 이 옵션을 활성화하면 이 규칙에 대한 정보가 HIPS 로그에 기록됩니다.

사용자에게 알림 - 이벤트가 트리거되면 오른쪽 아래 모서리에 알림이 나타납니다.

규칙은 이 규칙을 트리거하는 조건을 설명하는 부분으로 구성됩니다.

소스 애플리케이션 - 이 애플리케이션에서 이벤트를 트리거한 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 애플리케이션**을 선택하고 **추가**를 클릭하여 새 파일을 추가하거나 드롭다운 메뉴에서 **모든 애플리케이션**을 선택하여 모든 애플리케이션을 추가할 수 있습니다.

대상 파일 – 작업이 이 대상과 관련 있는 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 파일**을 선택하고 **추가**를 클릭하여 새 파일 또는 폴더를 추가하거나, 드롭다운 메뉴에서 **모든 파일**을 선택하여 모든 파

일을 추가할 수 있습니다.

애플리케이션 - 작업이 이 대상에 관련된 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 애플리케이션**을 선택하고 **추가**를 클릭하여 새 파일이나 폴더를 추가하거나 드롭다운 메뉴에서 **모든 애플리케이션**을 선택하여 모든 애플리케이션을 추가할 수 있습니다.

레지스트리 항목 - 작업이 이 대상에 관련된 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 항목**을 선택하고 **추가**를 클릭하여 새 파일이나 폴더를 추가하거나 드롭다운 메뉴에서 **모든 항목**을 선택하여 모든 애플리케이션을 추가할 수 있습니다.

HIPS에서 미리 정의된 특정 규칙 중 일부 작업은 차단할 수 없으며, 기본적으로 허용됩니다. 또한 일부 시스템 작업은 HIPS에서 모니터링됩니다. HIPS는 안전하지 않다고 간주될 수 있는 작업을 모니터링합니다.

경로를 지정할 때 C:\example은 폴더 자체의 작업에 영향을 주고 C:\example*.* 폴더의 파일에 영향을 줍니다.

애플리케이션 작업

- **다른 애플리케이션 디버그** - 디버거를 프로세스에 연결합니다. 애플리케이션을 디버깅하는 동안 동작의 여러 상세 정보를 보고 수정할 수 있으며, 해당 데이터에 접근할 수 있습니다.
- **다른 애플리케이션에서 이벤트 가로채기** - 소스 애플리케이션이 특정 애플리케이션에 대상으로 지정된 이벤트를 캐치하려고 합니다(예를 들어 키로거가 브라우저 이벤트를 캡처하려고 함).
- **다른 애플리케이션 종료/일시 중지** - 프로세스를 일시 중지하거나 다시 시작하거나 종료합니다(프로세스 탐색기나 프로세스 창에서 직접 접근할 수 있음).
- **새 애플리케이션 시작** - 새 애플리케이션이나 프로세스를 시작합니다.
- **다른 애플리케이션 상태 수정** - 소스 애플리케이션이 대상 애플리케이션의 메모리에 작성하려고 하거나 대신해서 코드를 실행하려고 합니다. 이 기능은 필수 애플리케이션을 이 작업의 사용을 차단하는 규칙에 있는 대상 애플리케이션으로 구성하여 필수 애플리케이션을 보호할 때 유용할 수 있습니다.

레지스트리 작업

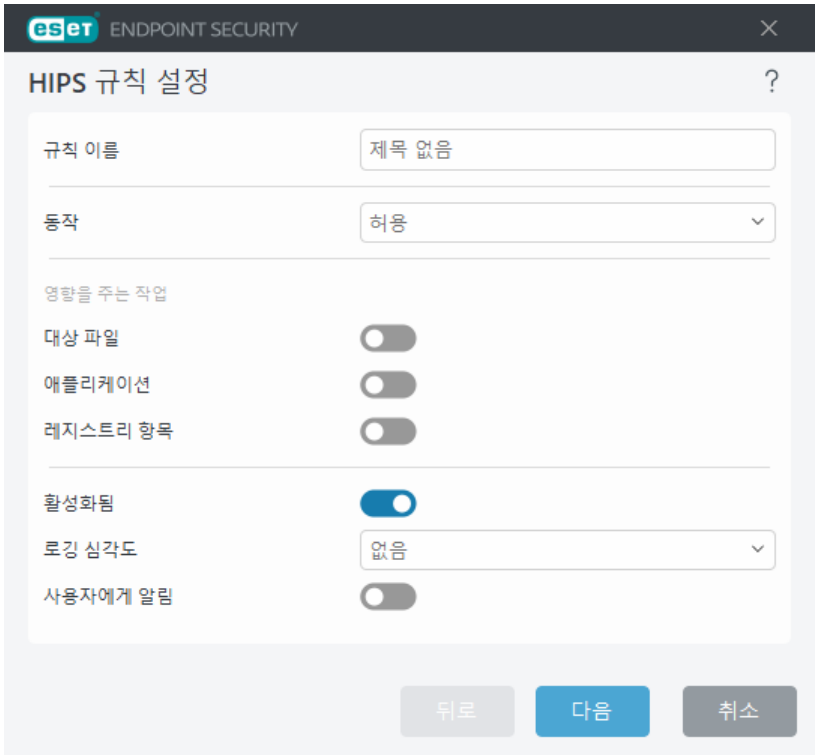
- **시작 설정 수정** - Windows 시작 시 실행되는 애플리케이션을 정의하는 설정의 모든 변경 내용입니다. 예를 들어 이러한 변경 내용은 Windows 레지스트리에서 Run 키를 검색하여 확인할 수 있습니다.
- **레지스트리에서 삭제** - 레지스트리 키나 해당 값을 삭제합니다.
- **레지스트리 키 이름 바꾸기** - 레지스트리 키 이름을 바꿉니다.
- **레지스트리 수정** - 레지스트리 키에 대한 새 값을 생성하거나 기존의 값을 변경하거나 DB 트리의 데이터를 이동하거나 레지스트리 키에 대한 사용자나 그룹 권한을 설정합니다.

규칙에 와일드카드 사용
규칙에 별표를 사용하여 특정 키(예: “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start”)를 대체할 수 있습니다. 와일드카드를 사용하는 다른 방법은 지원되지 않습니다.
대상이 지정된 HKEY_CURRENT_USER 키 규칙 생성
이 키는 SID(보안 식별자)로 식별된 사용자와 관련된 적절한 HKEY_USERS 하위 키 링크입니다. 현재 사용자 전용 규칙을 생성하려면 HKEY_CURRENT_USER 경로를 사용하는 대신 HKEY_USERS\%SID%를 가리키는 경로를 사용합니다. SID는 별표를 이용해 모든 사용자에게 적용되는 규칙을 만들 수 있습니다.

매우 일반적인 규칙을 생성한 경우 이 유형의 규칙에 대한 경고가 표시됩니다.

다음 예에서는 특정 애플리케이션의 원치 않는 동작을 제한하는 방법을 설명합니다.

1. 규칙 이름을 지정하고 **동작** 드롭다운 메뉴에서 **차단**을 선택합니다(또는 나중에 선택하려는 경우 **확인**).
2. **사용자에게 알림** 스위치를 활성화하여 규칙이 적용될 때마다 알림을 표시할 수 있습니다.
3. 규칙이 적용될 하나 이상의 작업을 **영향을 주는 작업** 섹션에서 선택합니다.
4. **다음**을 클릭합니다.
5. **소스 애플리케이션** 창의 드롭다운 메뉴에서 **특정 애플리케이션**을 선택하여 지정한 애플리케이션에서 선택된 모든 애플리케이션 작업을 수행하려고 하는 모든 애플리케이션에 새 규칙을 적용합니다.
6. **추가**를 클릭한 다음 **...**를 클릭하여 특정 애플리케이션 경로를 선택한 후 **확인**을 클릭합니다. 원한다면 더 많은 애플리케이션을 추가합니다.
   예를 들면 다음과 같습니다. *C:\Program Files (x86)\Untrusted application\application.exe*
7. **파일에 작성** 작업을 선택합니다.
8. 드롭다운 메뉴에서 **모든 파일**을 선택합니다. 이렇게 하면 이전 단계에서 선택한 애플리케이션이 파일에 쓰려는 모든 시도가 차단됩니다.
9. **마침**을 클릭하여 새 규칙을 저장합니다.



HIPS 애플리케이션/레지스트리 경로 추가

... 옵션을 클릭하여 파일 애플리케이션 경로를 선택합니다. 폴더를 선택하는 동안 이 위치의 모든 애플리케이션이 포함됩니다.

레지스트리 편집기 열기 옵션을 선택하면 Windows 레지스트리 편집기(regedit)가 시작됩니다. 레지스트리 경로를 추가하는 동안 **값** 필드에 올바른 위치를 입력합니다.

파일 또는 레지스트리 경로 예:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

업데이트

업데이트 설정 옵션은 고급 설정 > **업데이트**에서 사용할 수 있습니다. 이 섹션에서는 사용되는 업데이트 서버 및 이러한 서버에 대한 인증 데이터와 같은 업데이트 소스 정보를 지정합니다.

업데이트를 제대로 다운로드하려면 모든 업데이트 파라미터를 올바르게 입력해야 합니다. 방화벽을 사용하는 경우에는 ESET 프로그램이 인터넷과 통신(예: HTTPS 통신)할 수 있는지 확인합니다.

업데이트

현재 사용 중인 업데이트 프로필이 **기본 업데이트 프로필 선택** 드롭다운 메뉴에 표시됩니다.

새 프로필을 생성하려면 업데이트 프로필 섹션을 참조하십시오.

자동 프로필 전환 - 특정 네트워크 연결 프로필에 대한 업데이트 프로필을 설정할 수 있습니다.

업데이트 알림 구성 – 표시되는 애플리케이션 알림을 선택하려면 편집을 클릭합니다. 알림 표시는 바탕화면에 표시 및/또는 이메일로 보내기로 선택할 수 있습니다.

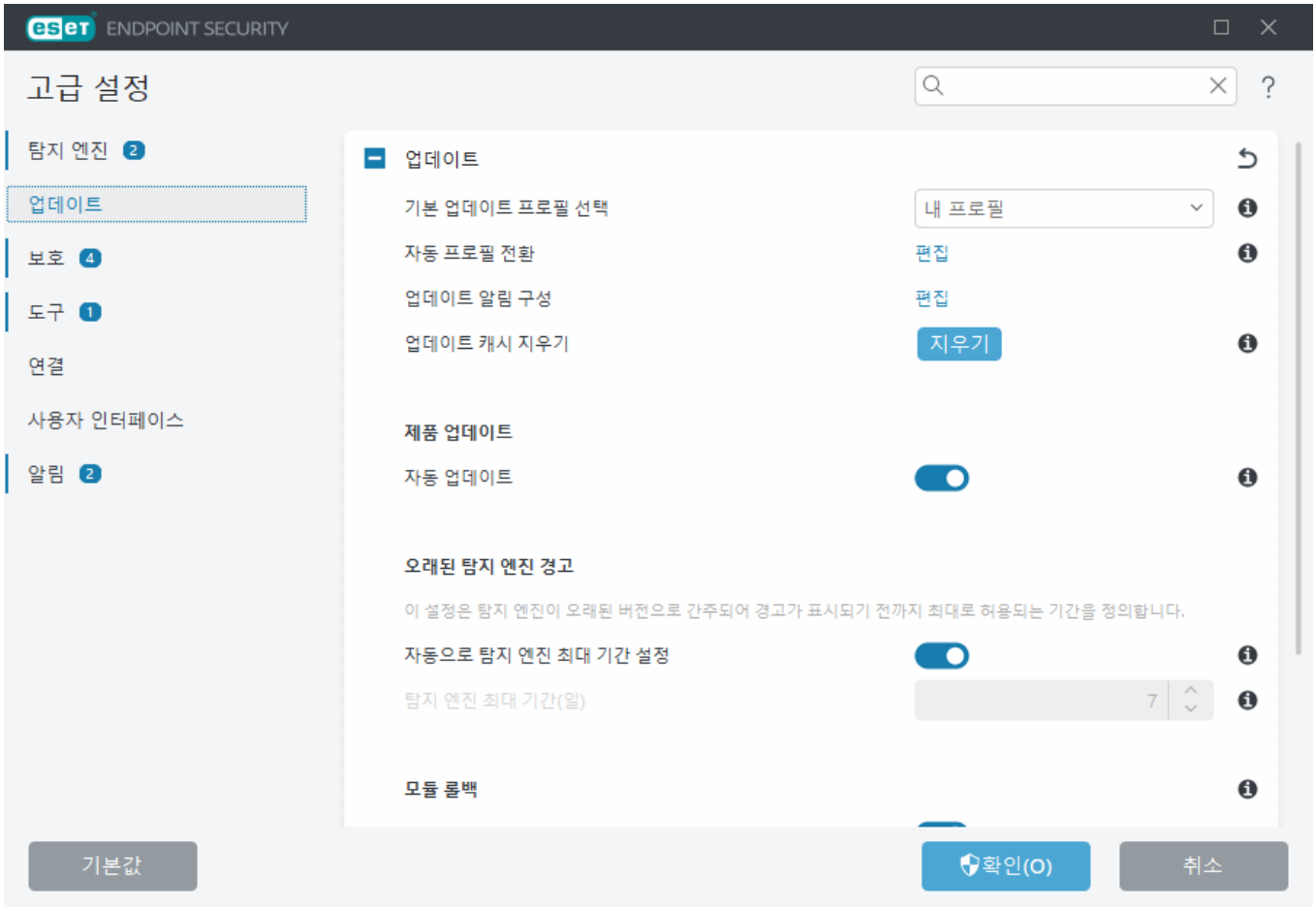
모듈 업데이트를 다운로드하려고 할 때 문제가 발생하는 경우 **업데이트 캐시 지우기** 옆의 **지우기**를 클릭하여 임시 업데이트 파일/캐시를 지웁니다.

오래된 탐지 엔진 경고

자동으로 검색 엔진 최대 기간 설정 – 검색 엔진이 오래된 것으로 보고되는 최대 시간(일수)을 설정할 수 있습니다. **검색 엔진 최대 기간(일수)** 기본값은 7일입니다.

모듈 롤백

검색 엔진 및/또는 프로그램 모듈의 새 업데이트가 불안정하거나 손상되었다고 의심되면 이전 버전으로 롤백한 후 설정된 기간에 대해 업데이트를 비활성화할 수 있습니다.



프로필

다양한 업데이트 구성 및 작업을 위해 프로필 업데이트를 생성할 수 있습니다. 프로필 업데이트를 생성하는 경우 정기적으로 변경되는 인터넷 연결 속성에 대한 대체 프로필이 필요한 모바일 사용자에게 특히 유용합니다.

편집할 프로필 선택 드롭다운 메뉴에는 현재 선택한 프로필이 표시되며, 기본적으로 **내 프로필**로 설정되어 있습니다.

새 프로필을 생성하려면 **프로필 목록** 옆의 **편집**을 클릭한 다음 자신의 **프로필 이름**을 입력하고 **추가**를 클릭합니다.

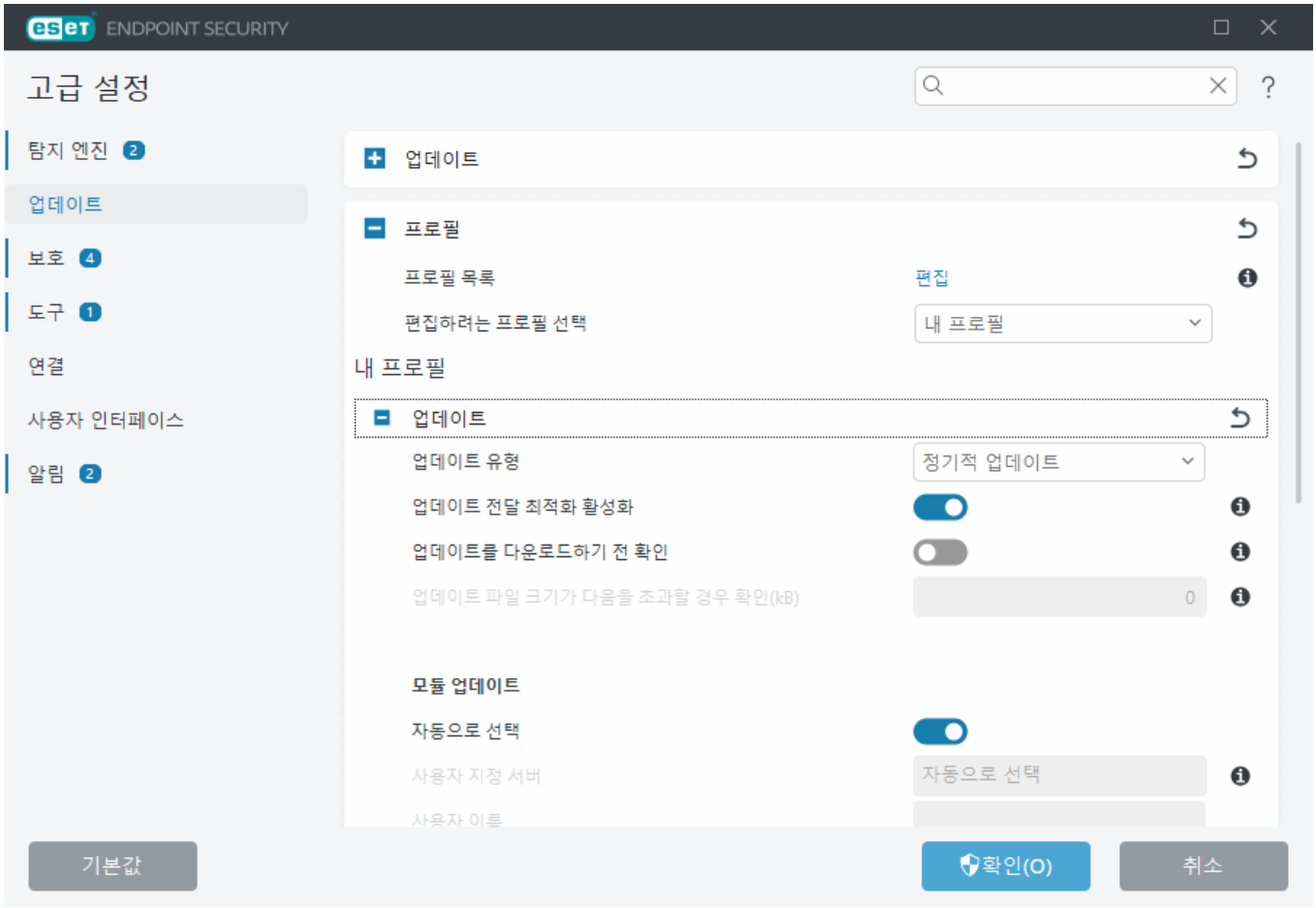
업데이트

기본적으로 **업데이트 유형**은 **정기적 업데이트**로 설정되어 있어 업데이트 파일을 최소한의 네트워크 트래픽으로 ESET 서버에서 자동 다운로드할 수 있습니다. 테스트 모드(**테스트 모드 업데이트** 옵션)는 내부 테스트를 통해 수행되는 업데이트로, 곧 일반 사용자에게 제공될 예정입니다. 최신 검출 방법 및 수정 프로그램에 접근하여 테스트 모드를 활성화함으로써 이 기능을 사용할 수 있습니다. 단, 테스트 모드는 항상 안정적인 상태가 아니므로 최대 가용성 및 안정성이 필요한 프로덕션 서버 및 워크스테이션에서는 사용하면 안 됩니다. 지연된 업데이트를 통해 X시간 이상 지연된 새 버전의 바이러스 DB(즉 실제 환경에서 테스트되어 안정적이라고 간주되는 DB)를 제공하는 특수 업데이트 서버에서 업데이트할 수 있습니다.

업데이트 전달 최적화 활성화 – 활성화되면 업데이트 파일을 CDN(콘텐츠 전달 네트워크)에서 다운로드할 수 있습니다. 이 설정을 비활성화하면 전용 ESET 업데이트 서버가 오버로드될 때 다운로드가 중단되거나 느려질 수 있습니다. 방화벽이 ESET 업데이트 서버 IP 주소에만 접근하도록 제한되는 경우 또는 CDN 서비스에

대한 연결이 작동하지 않는 경우에 비활성화하면 유용합니다.

업데이트를 다운로드하기 전 확인 – 프로그램에서 업데이트 파일 다운로드를 확인할 것인지, 거절할 것인지 선택할 수 있는 알림을 표시합니다. 업데이트 파일 크기가 업데이트 파일 크기가 다음(kB)을 초과할 경우 확인에 지정된 값보다 큰 경우, 프로그램에서 확인 대화 상자를 표시합니다. 업데이트 파일 크기가 0kB로 설정된 경우, 프로그램에서 항상 확인 대화 상자를 표시합니다.



모듈 업데이트

자동으로 선택 옵션이 기본적으로 활성화되어 있습니다. **사용자 지정 서버** 옵션은 업데이트가 저장되는 위치입니다. ESET 업데이트 서버를 사용하는 경우 기본 옵션이 선택된 상태로 두는 것이 좋습니다.

감지 지문의 잦은 업데이트 활성화 – 감지 지문이 더 짧은 간격으로 업데이트됩니다. 이 설정을 비활성화하면 감지 속도에 부정적인 영향을 미칠 수도 있습니다.

이동식 미디어에서 모듈 업데이트 허용 - 생성된 미러가 포함되어 있는 경우 이동식 미디어에서 업데이트할 수 있습니다. 자동이 선택된 경우 업데이트가 백그라운드에서 실행됩니다. 업데이트 대화 상자가 표시되도록 하려면 항상 확인을 선택합니다.

로컬 HTTP 서버(미러라고도 함)를 사용할 때 업데이트 서버를 다음과 같이 설정해야 합니다.
*http://*컴퓨터_이름_또는_*IP*주소:2221

SSL을 사용한 로컬 HTTP 서버를 사용할 때는 업데이트 서버를 다음과 같이 설정해야 합니다.
*https://*컴퓨터_이름_또는_*IP*주소:2221

로컬 공유 폴더를 사용할 때는 업데이트 서버를 다음과 같이 설정해야 합니다.
\\컴퓨터_이름_또는_*IP*주소\공유폴더

위의 예에서 지정된 HTTP 서버 포트 번호는 HTTP/HTTPS 서버가 수신하는 포트에 따라 다릅니다.

제품 업데이트

제품 업데이트를 참조하십시오.

연결 옵션

연결 옵션을 참조하십시오.

업데이트 미러

업데이트 미러를 참조하십시오.

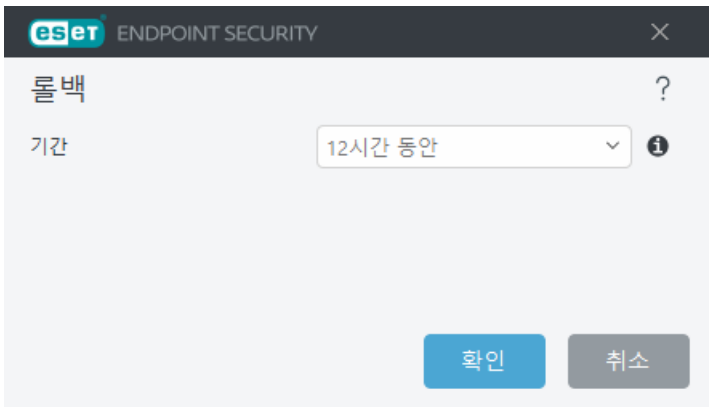
업데이트 롤백

새로운 탐지 엔진 업데이트 또는 프로그램 모듈이 불안정하거나 손상되었을 수 있다고 의심되면 이전 버전으로 롤백한 후 업데이트를 일시적으로 비활성화할 수 있습니다. 또는 업데이트를 무기한 연기한 경우 이전에 비활성화한 업데이트를 활성화할 수 있습니다.

ESET Endpoint Security에서는 롤백 기능과 함께 사용할 수 있는 탐지 엔진 및 프로그램 모듈의 스냅숏을 기록합니다. 바이러스 DB 스냅숏을 생성하려면 **모듈의 스냅숏 생성**이 활성화된 상태로 유지합니다. **모듈의 스냅숏 생성**이 활성화된 경우 첫 번째 업데이트 중에 첫 번째 스냅숏이 생성됩니다. 다음 스냅숏은 48시간 후에 생성됩니다. **로컬에 저장된 스냅숏 수**필드는 저장된 탐지 엔진 스냅숏의 수를 정의합니다.

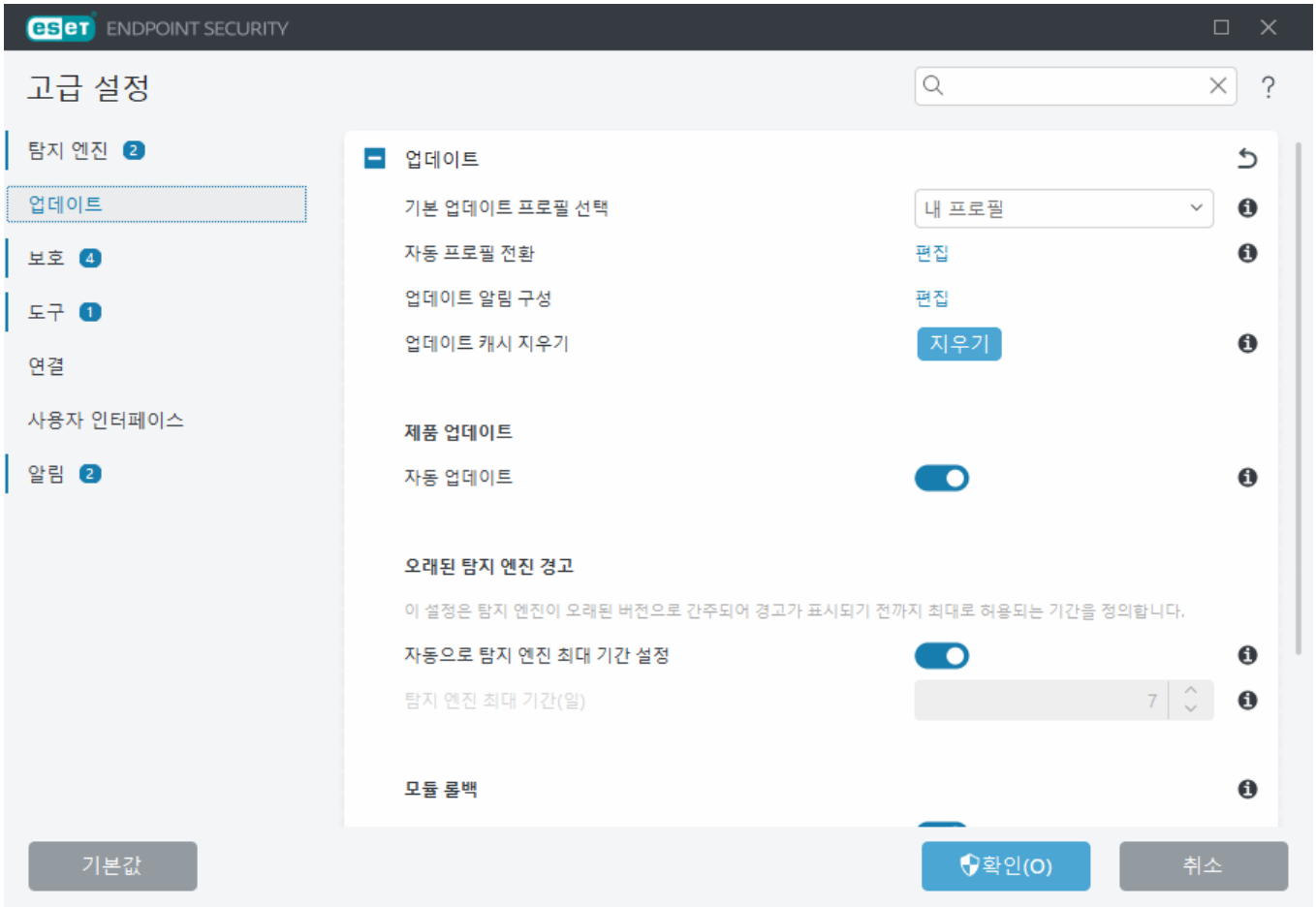
최대 스냅숏 수(예: 세 개)에 도달하면 가장 오래된 스냅숏이 48시간마다 새 스냅숏으로 대체됩니다. ESET Endpoint Security에서는 가장 오래된 스냅숏으로 탐지 엔진 및 프로그램 모듈 업데이트 버전을 롤백합니다.

고급 설정 > **업데이트** > **업데이트** > **모듈 롤백** > **롤백**을 열고 **기간** 드롭다운 메뉴에서 시간 간격을 선택합니다.



업데이트 기능을 수동으로 복원할 때까지 정기 업데이트를 무기한 연기하려면 **해지될 때까지**를 선택합니다. 이 경우 잠재적 보안 위험이 발생하므로 이 옵션은 선택하지 않는 것이 좋습니다.

롤백이 수행되면 **롤백** 버튼이 **업데이트 허용**으로 변경됩니다. **업데이트 일시 중지** 드롭다운 메뉴에서 선택된 시간 간격에 대해서는 업데이트가 허용되지 않습니다. 탐지 엔진 버전이 사용 가능한 가장 낮은 버전으로 다운그레이드되며 로컬 컴퓨터 파일 시스템에 스냅숏으로 저장됩니다.



22700이 최신 탐지 엔진 버전 번호이고, 22698과 22696이 탐지 엔진 스냅숏으로 저장되었다고 가정합니다. 22697은 사용할 수 없습니다. 이 예에서는 22697 업데이트 중에 컴퓨터가 꺼졌고, 22697을 다운로드하기 전에 최신 업데이트가 제공되었습니다. **로컬에 저장된 스냅숏 수** 필드가 2인 경우 **롤백**을 클릭하면 탐지 엔진(프로그램 모듈 포함)이 버전 번호 22696으로 저장됩니다. 이 프로세스는 시간이 다소 걸릴 수 있습니다. 탐지 엔진 버전이 업데이트 화면에 다운그레이드되었는지 확인합니다.

제품 업데이트

제품 업데이트 섹션에는 제품 업데이트와 관련된 옵션이 포함되어 있습니다. 해당 프로그램을 통해 새 제품 업데이트를 사용할 수 있는 경우 해당 동작을 미리 정의할 수 있습니다.

제품 업데이트는 새로운 기능을 제공하거나 이전 버전에 이미 있었던 기능을 변경합니다. 이는 사용자 개입 없이 자동으로 수행될 수도 있고, 알림이 표시되도록 선택할 수도 있습니다. 제품 업데이트를 설치한 후에는 컴퓨터를 다시 시작해야 할 수도 있습니다.

자동 업데이트 - 특정 업데이트 프로필에 대한 자동 업데이트를 일시 중지하면 다른 네트워크 또는 데이터 통신 연결을 사용하여 인터넷에 연결되어 있는 동안 자동 제품 업데이트가 일시적으로 비활성화됩니다. 이 설정을 활성화하여 최신 기능과 가능한 최고 보호 기능에 지속적으로 접근할 수 있습니다. 자동 업데이트에 대한 자세한 내용은 자동 업데이트 FAQ를 참조하십시오.

기본적으로 제품 업데이트는 ESET 저장소 서버에서 다운로드됩니다. 대규모 또는 오프라인 환경에서 트래픽을 배포하여 제품 파일의 내부 캐시를 허용할 수 있습니다.

프로그램 구성 요소 업데이트에 대한 사용자 지정 서버 정의

1. **사용자 지정 서버** 필드에서 제품 업데이트 경로를 정의합니다.
경로는 HTTP(S) 링크, SMB 네트워크 공유 경로, 로컬 디스크 드라이브 또는 이동식 미디어 경로일 수 있습니다. 네트워크 드라이브의 경우 매핑된 드라이브 문자 대신 UNC 경로를 사용합니다.
2. 필요하지 않은 경우 **사용자 이름** 및 **패스워드**를 비워 둡니다.
필요한 경우 사용자 지정 웹 서버에서 HTTP 인증을 위해 적절한 자격 증명을 여기에 정의합니다.
3. 변경 사항을 확인하고 표준 ESET Endpoint Security 업데이트를 사용하여 제품 업데이트가 있는지 테스트합니다.

가장 적절한 옵션을 선택하는 일은 설정이 적용되는 워크스테이션에 따라 다릅니다. 워크스테이션과 서버 간에는 차이가 있습니다. 예를 들어 제품 업데이트 후 서버를 자동으로 다시 시작하면 회사에 심각한 피해를 줄 수 있습니다.

연결 옵션

특정 업데이트 프로필에 대한 프록시 서버 설정 옵션에 접근하려면 고급 설정 > **업데이트** > **프로필** > **업데이트** > **연결 옵션**을 엽니다.

프록시 서버

프록시 모드 드롭다운 메뉴를 클릭하고 다음 세 가지 옵션 중 하나를 선택합니다.

- 프록시 서버 사용 안 함
- 프록시 서버를 통해 연결
- 글로벌 프록시 서버 설정 사용

고급 설정 > 연결 > 프록시 서버에 이미 지정된 프록시 서버 구성을 사용하려면 **글로벌 프록시 서버 설정 사용**을 선택합니다.

ESET Endpoint Security을(를) 업데이트하는 데 프록시 서버를 사용하지 않도록 지정하려면 **프록시 서버 사용 안 함**을 선택합니다.

다음의 경우에 **프록시 서버를 통해 연결** 옵션을 선택해야 합니다.

- **도구** > **프록시 서버**에 정의된 서버와는 다른 프록시 서버가 ESET Endpoint Security을(를) 업데이트하는 데 사용됩니다. 이 구성에서 새 프록시의 정보는 **프록시 서버** 주소, 통신 **포트**(기본적으로 3128), 그리고 필요한 경우 프록시 서버의 **사용자 이름**과 **비밀번호** 아래에 지정되어야 합니다.
- 프록시 서버 설정이 전체적으로 설정되어 있지 않지만 ESET Endpoint Security이(가) 업데이트를 위해 프록시 서버에 연결하는 경우.
- 컴퓨터가 프록시 서버를 통해 인터넷에 연결되어 있는 경우. 프로그램을 설치하는 동안 브라우저에서 설정을 가져오지만 이러한 설정이 변경된 경우(예: ISP를 변경한 경우) 이 창에 나열된 프록시 설정이 올바른지 확인해야 합니다. ISP를 변경한 경우) 이 창에 나열된 프록시 설정이 올바른지 확인해야 합니다. 그렇지 않으면 프로그램이 업데이트 서버에 연결할 수 없습니다.

프록시 서버의 기본 설정은 **글로벌 프록시 서버 설정 사용**입니다.

프록시를 사용할 수 없는 경우 직접 연결 사용 - 프록시에 연결할 수 없는 경우 업데이트 중에 프록시가 우회됩니다.

Windows 공유

Windows NT 운영 체제 버전으로 로컬 서버에서 업데이트하는 경우 기본적으로 네트워크에 연결할 때마다 인증이 필요합니다.

이러한 계정을 구성하려면 **다음 계정으로 LAN 연결** 드롭다운 메뉴에서 선택합니다.

- **시스템 계정(기본값)**
- **현재 사용자**
- **지정한 사용자**

인증에 시스템 계정을 사용하려면 **시스템 계정(기본값)**을 선택합니다. 일반적으로 기본 업데이트 설정 섹션에 인증 데이터를 입력하지 않으면 인증 프로세스가 수행되지 않습니다.

현재 로그인한 사용자 계정을 사용하여 프로그램이 인증하도록 하려면 **현재 사용자**를 선택합니다. 이 방법은 현재 로그인한 사용자가 없는 경우 프로그램에서 업데이트 서버에 연결할 수 없다는 단점이 있습니다.

프로그램에서 인증에 특정 사용자 계정을 사용하도록 하려면 **지정한 사용자**를 선택합니다. 기본 시스템 계정 연결이 실패한 경우 이 방법을 사용합니다. 지정한 사용자 계정이 로컬 서버의 업데이트 파일 디렉터리에 접근할 수 있어야 합니다. 그렇지 않으면 프로그램이 연결을 설정해 업데이트를 다운로드할 수 없습니다.

사용자 이름 및 **비밀번호** 설정은 옵션입니다.

현재 사용자 또는 **지정한 사용자**가 선택되어 있는 경우 프로그램 ID를 원하는 사용자로 변경하면 오류가 발생할 수 있습니다. LAN 인증 데이터를 기본 업데이트 설정 섹션에 입력하는 것이 좋습니다. 업데이트 설정 섹션에서 인증 데이터는 다음과 같이 입력해야 합니다. 도메인_이름\사용자(작업 그룹인 경우 작업 그룹_이름\이름 입력) 및 비밀번호. 로컬 서버의 HTTP 버전에서 업데이트하는 경우에는 인증이 필요하지 않습니다.

업데이트를 다운로드한 후에도 서버 연결이 활성 상태로 유지되는 경우 업데이트 후 서버 **연결 끊기**를 선택하여 강제로 연결을 끊습니다.

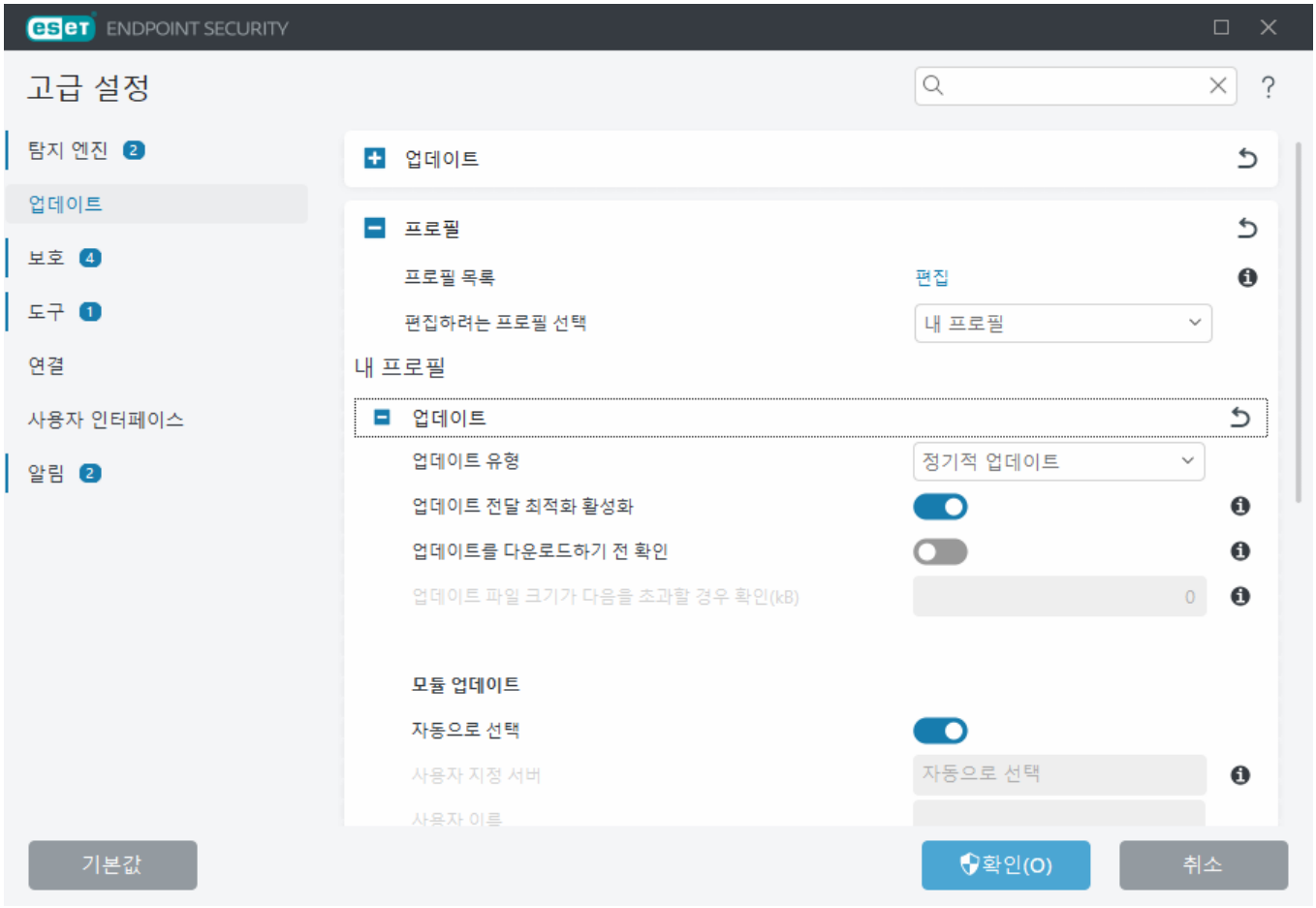
업데이트 미러

ESET Endpoint Security를 사용하면 네트워크에 있는 다른 워크스테이션을 업데이트하는 데 사용할 수 있는 업데이트 파일의 복사본을 생성할 수 있습니다. "미러"(LAN 환경의 업데이트 파일 복사본)를 사용하면 각 워크스테이션별로 공급업체 업데이트 서버에서 업데이트 파일을 반복적으로 다운로드하지 않아도 되므로 편리합니다. 업데이트는 로컬 미러 서버에 다운로드된 후에 모든 워크스테이션으로 배포되므로 네트워크 트래픽 오버로드가 발생하는 위험도 방지할 수 있습니다. 미러에서 클라이언트 워크스테이션을 업데이트하면 네트워크 부하 분산이 최적화되고 인터넷 연결 대역폭이 절감됩니다.

업데이트 미러는 동일한 세대의 Windows용 ESET Endpoint Security을(를) 실행하는 워크스테이션을 업데이트하는 데 사용할 수 있는 업데이트 파일의 복사본을 생성합니다. (예를 들어, Windows용 ESET Endpoint Security 버전 10.x는 Windows용 ESET Endpoint Security 및 Windows용 ESET Endpoint Antivirus 10.x 버전에 대해서만 업데이트 파일을 생성함)

ESET PROTECT가 다수의 클라이언트를 관리하는 데 사용되는 네트워크의 인터넷 트래픽을 최소화하려면, 클라이언트를 미러로 구성하는 대신 ESET Bridge을(를) 사용하는 것이 좋습니다. ESET Bridge은(는) 통합형 설치 관리자를 사용하여 ESET PROTECT와 함께 설치하거나 독립 실행형 구성 요소로 설치할 수 있습니다. ESET Bridge, Apache HTTP 프록시, 미러 도구 및 직접 연결 간의 차이점과 자세한 내용은 ESET PROTECT 온라인 도움말 페이지를 참조하십시오.

로컬 미러 서버의 구성 옵션은 고급 설정 > **업데이트** > **프로필** > **업데이트 미러**에 있습니다.



클라이언트 워크스테이션에서 미러를 생성하려면 **업데이트 미러 생성**을 활성화합니다. 이 옵션을 활성화하면 다른 미러 구성 옵션(예: 업데이트 파일에 접근하는 방식 및 미러링된 파일에 대한 업데이트 경로 등)이 활성화됩니다.

업데이트 파일 접근

HTTP 서버 활성화 – 활성화하면 업데이트 파일에 HTTP를 통해 접근할 수 있으며, 자격 증명이 필요하지 않습니다.

미러 서버에 접근하는 방법은 미러에서 업데이트에 자세히 설명되어 있습니다. 미러에 접근하는 기본 방법은 두 가지입니다. 즉, 업데이트 파일이 포함된 폴더를 공유 네트워크 폴더로 제공하거나 클라이언트가 HTTP 서버에 있는 미러에 접근할 수 있습니다.

미러에 필요한 업데이트 파일을 저장하는 전용 폴더는 **미러 파일을 저장할 폴더**에서 정의합니다. 다른 폴더를 선택하려면 **지우기**를 클릭하여 미리 정의된 폴더(*C:\ProgramData\ESET\ESET Endpoint Security\mirror*)를 삭제하고 **편집**을 클릭하여 로컬 컴퓨터나 공유 네트워크 폴더에서 원하는 폴더를 찾습니다. 지정한 폴더에 대한 인증이 필요한 경우 **사용자 이름** 및 **비밀번호** 필드에 인증 데이터를 입력해야 합니다. 선택한 대상 폴더가 Windows NT/2000/XP 운영 체제를 실행하는 네트워크 디스크에 있는 경우에는 여기서 지정하는 사용

자 이름 및 비밀번호에 선택한 폴더에 대한 쓰기 권한이 있어야 합니다. 사용자 이름은 도메인/사용자 또는 작업 그룹/사용자 형식으로 입력해야 합니다. 해당되는 비밀번호를 입력할 수 있도록 기억해 두십시오.

미러용 HTTP 서버 및 SSL

미러 탭의 **HTTP 서버** 섹션에서 HTTP 서버가 수신할 **서버 포트**와 HTTP 서버에서 사용하는 **인증** 유형을 지정할 수 있습니다. 기본적으로 서버 포트는 **2221**로 설정됩니다.

인증 - 업데이트 파일에 접근하는 데 사용되는 인증 방법을 정의합니다. 다음과 같은 옵션을 사용할 수 있습니다. **없음**, **기본** 및 **NTLM**. 기본 사용자 이름 및 비밀번호 인증과 함께 base64 인코딩을 사용하려면 **기본**을 선택합니다. **NTLM** 옵션을 선택하면 안전 인코딩 방법을 사용하는 인코딩을 사용할 수 있습니다. 인증을 위해 업데이트 파일을 공유하는 워크스테이션에서 생성된 사용자가 사용됩니다. 기본 설정은 **없음**이며, 이 옵션은 인증할 필요 없이 업데이트 파일에 대한 접근 권한을 부여합니다.

사용자 이름과 **패스워드** 같은 인증 데이터는 미러 HTTP 서버에 접근하기 위한 용도로만 사용됩니다. 사용자 이름과 패스워드가 필요한 경우에만 이 필드에 내용을 입력합니다.

HTTPS(SSL)가 지원되는 HTTP 서버를 실행하려면 **인증서 체인 파일**을 추가하거나 자체적으로 지문이 생성된 인증서를 생성합니다. 다음과 같은 **인증서 유형**을 사용할 수 있습니다. ASN, PEM 및 PFX. 보안을 강화하기 위해 HTTPS 프로토콜을 사용하여 다운로드할 업데이트 파일을 제공할 수 있습니다. 이 프로토콜을 사용하여 데이터 전송 및 로그인 자격 증명을 추적하는 것은 거의 불가능합니다. **개인 키 유형** 옵션은 기본적으로 **통합**으로 설정됩니다(따라서 **개인 키 파일** 옵션은 기본적으로 비활성화되어 있음). 즉, 개인 키는 선택한 인증서 체인 파일의 일부입니다.

자체적으로 지문이 생성된 HTTPS 미러용 인증서
HTTPS 미러 서버를 사용하는 경우 모든 클라이언트 컴퓨터의 신뢰할 수 있는 루트 저장소로 인증서를 가져와야 합니다. Windows에서 신뢰할 수 있는 루트 인증서 설치를 참조하십시오.

미러에서 업데이트

클라이언트가 업데이트 파일을 다운로드할 수 있는, 실질적으로 저장소인 미러를 구성하는 기본 방법으로 두 가지가 있습니다. 즉 업데이트 파일이 포함된 폴더를 공유 네트워크 폴더나 HTTP 서버로 제공하여 구성할 수 있습니다.

업데이트 미러는 동일한 세대의 Windows용 ESET Endpoint Security을(를) 실행하는 워크스테이션을 업데이트하는 데 사용할 수 있는 업데이트 파일의 복사본을 생성합니다. (예를 들어, Windows용 ESET Endpoint Security 버전 10.x는 Windows용 ESET Endpoint Security 및 Windows용 ESET Endpoint Antivirus 10.x 버전에 대해서만 업데이트 파일을 생성함)

내부 HTTP 서버를 사용하여 미러에 접근

이 설정은 미리 정의된 프로그램 구성에 지정된 기본 구성입니다. HTTP 서버를 사용하여 미러에 접근할 수 있도록 하려면 고급 설정 > **업데이트** > **프로필** > **업데이트 미러**로 이동하여 **업데이트 미러 생성**을 선택합니다.

미러 탭의 **HTTP 서버** 섹션에서 HTTP 서버가 수신할 **서버 포트**와 HTTP 서버에서 사용하는 **인증** 유형을 지정할 수 있습니다. 기본적으로 서버 포트는 **2221**로 설정됩니다.

인증 - 업데이트 파일에 접근하는 데 사용되는 인증 방법을 정의합니다. 다음과 같은 옵션을 사용할 수 있습니다. **없음**, **기본** 및 **NTLM**. 기본 사용자 이름 및 비밀번호 인증과 함께 base64 인코딩을 사용하려면 **기본**을 선택합니다. **NTLM** 옵션을 선택하면 안전 인코딩 방법을 사용하는 인코딩을 사용할 수 있습니다. 인증을 위해 업데이트 파일을 공유하는 워크스테이션에서 생성된 사용자가 사용됩니다. 기본 설정은 **없음**이며, 이 옵션은 인증할 필요 없이 업데이트 파일에 대한 접근 권한을 부여합니다.

HTTP 서버를 통해 업데이트 파일에 접근하려면 미러 폴더가 자신을 생성한 ESET Endpoint Security 인스턴스와 동일한 컴퓨터에 있어야 합니다.

미러에서 업데이트 시도에 여러 번 실패하면 기본 메뉴의 업데이트 패널에 **잘못된 사용자 이름 및/또는 패스워드**라는 오류가 표시됩니다. 고급 설정 > **업데이트** > **프로필** > **업데이트 미러**로 이동하여 사용자 이름과 패스워드를 확인하는 것이 좋습니다. 이 오류는 대부분 인증 데이터를 잘못 입력한 경우 표시됩니다.

미러 서버가 구성된 후에는 클라이언트 워크스테이션에 새 업데이트 서버를 추가해야 합니다. 이렇게 하려면 아래 단계를 따릅니다.

- 고급 설정을 열고**업데이트** > **프로필** > **업데이트** > **모듈 업데이트**를 클릭합니다.
- **자동으로 선택**을 선택 취소하고 다음 형식 중 하나를 사용하여 새 서버를 **업데이트 서버** 필드에 추가합니다.
  http://IP_address_of_your_server:2221
  https://IP_address_of_your_server:2221(SSL이 사용된 경우)

시스템 공유를 통해 미러에 접근

먼저, 로컬 또는 네트워크 장치에서 공유 폴더를 생성합니다. 미러에 필요한 폴더를 생성하면 이 폴더에 업데이트 파일을 저장할 사용자에게 "쓰기" 접근 권한을 부여하고 미러 폴더에서 ESET Endpoint Security를 업데이트할 모든 사용자에게 "읽기" 접근 권한을 부여해야 합니다.

그런 다음 고급 설정 > **업데이트** > **프로필** > **업데이트 미러** 탭에서 **HTTP 서버 활성화**를 비활성화하여 미러에 대한 접근을 구성합니다. 이 옵션은 프로그램 설치 패키지에서 기본적으로 활성화되어 있습니다.

공유 폴더가 네트워크의 다른 컴퓨터에 있는 경우, 인증 데이터를 입력해야 다른 컴퓨터에 접근할 수 있습니다. 인증 데이터를 입력하려면 고급 설정을 열고 **업데이트** > **프로필** > **업데이트** > **연결 옵션** > **Windows 공유** > **다음 계정으로 LAN 연결**을 클릭합니다. 이 설정은 다음 계정으로 LAN 연결 섹션에 설명된 업데이트에 사용되는 설정과 동일합니다.

미러 폴더에 접근하려면 미러가 생성된 컴퓨터에 로그인하는 데 사용되는 것과 동일한 계정에서 설정해야 합니다. 컴퓨터가 도메인에 있는 경우 "domain\user" 사용자 이름을 사용해야 합니다. 컴퓨터가 도메인에 없는 경우에는 "IP_address_of_your_server\user" 또는 "hostname\user"를 사용해야 합니다.

미러 구성이 완료되면 클라이언트 워크스테이션에서 아래 단계를 사용하여 *\\UNC\PATH*를 업데이트 서버로 설정합니다.

1. 고급 설정을 열고**업데이트** > **프로필** > **업데이트**를 클릭합니다.
2. **모듈 업데이트** 옆의 **자동으로 선택**을 선택 취소하고 *\\UNC\PATH* **형식을 사용하여 새 서버를 업데이트 서버** 필드에 추가합니다.

업데이트가 제대로 작동하도록 하려면 미러 폴더의 경로를 UNC 경로로 지정해야 합니다. 매핑된 드라이브에서는 업데이트하지 못할 수 있습니다.

미러 도구를 사용하여 미러 생성
미러 도구는 엔드포인트 미러가 생성하는 것과는 다른 폴더 구조를 생성합니다. 각 폴더는 제품 그룹에 대한 업데이트 파일을 갖고 있습니다. 미러를 사용해 제품 업데이트 설정 시 올바른 폴더에 전체 경로를 지정해야 합니다.
예를 들어 미러에서 ESET PROTECT을 업데이트하려면 업데이트 서버를 다음으로(HTTP 서버 루트 위치에 따름) 설정합니다.
`http://your_server_address/mirror/eset_upd/ep10`

마지막 섹션은 프로그램 구성 요소(PCU)를 제어합니다. 기본적으로 다운로드된 프로그램 구성 요소는 로컬 미러에 복사되도록 준비됩니다. **제품 업데이트**가 활성화된 경우 파일이 사용 가능할 때 로컬 미러에 자동으로 복사되므로 **업데이트**를 클릭하지 않아도 됩니다. 제품 업데이트에 대한 자세한 내용은 업데이트 모드를 참조하십시오.

미러 업데이트 문제 해결

대부분의 경우 미러 서버에서 업데이트하는 중 발생하는 문제의 원인은 잘못 지정된 미러 폴더 옵션, 미러 폴더에 대한 잘못된 인증 데이터, 미러에서 업데이트 파일을 다운로드하려는 로컬 워크스테이션의 잘못된 구성 중 하나 이상으로 인한 것일 수 있습니다. 또는 이러한 원인이 두 가지 이상 조합되어 문제가 발생하기도 합니다. 여기서는 미러에서 업데이트하는 동안 발생할 수 있는 문제 중 가장 자주 일어나는 문제에 대해 간략하게 설명합니다.

ESET Endpoint Security에서 미러 서버에 대한 연결 오류 보고 – 이 문제는 로컬 워크스테이션이 업데이트를 다운로드하는 업데이트 서버(미러 폴더에 대한 네트워크 경로)가 잘못 지정된 경우 발생할 수 있습니다. 미러 폴더를 확인하려면 Windows **시작** 메뉴, **실행**을 차례로 클릭한 다음 폴더 이름을 입력하고 **확인**을 클릭합니다. 그러면 폴더의 내용이 표시됩니다.

ESET Endpoint Security에 사용자 이름 및 비밀번호가 필요함 - 이 문제는 업데이트 섹션에 인증 데이터(사용자 이름 및 비밀번호)를 잘못 입력하여 발생할 수 있습니다. 사용자 이름 및 비밀번호는 프로그램이 자신을 업데이트할 업데이트 서버에 대한 접근 권한을 부여하는 데 사용됩니다. 인증 데이터가 정확하고 올바른 형식으로 입력되어 있는지 확인합니다. 예를 들어, 인증 데이터의 형식은 도메인/사용자 이름 또는 작업 그룹/사용자 이름이어야 하고 이에 해당하는 비밀번호를 입력해야 합니다. "모두"가 미러 서버에 접근할 수 있도록 허용된 경우, 이는 단순하게 모든 사용자에게 접근 권한이 부여되었다는 의미가 아닙니다. "모두"는 권한이 없는 모든 사용자도 포함해서 말하는 것이 아니라 모든 도메인 사용자에게 폴더에 대한 접근 권한이 있다는 의미입니다. 따라서 "모두"가 폴더에 접근할 수 있도록 설정된 경우에도 여전히 도메인 사용자 이름 및 비밀번호를 업데이트 설정 섹션에 입력해야 합니다.

ESET Endpoint Security에서 미러 서버에 대한 연결 오류 보고 - HTTP 버전의 미러에 접근하도록 정의된 포트에서 통신이 차단되었습니다.

ESET Endpoint Security에서 업데이트 파일을 다운로드하는 중에 오류 보고 – 이 문제는 로컬 워크스테이션이 업데이트를 다운로드하는 업데이트 서버(미러 폴더에 대한 네트워크 경로)가 잘못 지정된 경우 발생할 수 있습니다.

보호

보호 기능은 파일, 이메일 및 인터넷 통신을 제어하여 악의적인 시스템 공격에 대비합니다. 예를 들어 악성 코드로 분류된 개체가 탐지되면 수정이 시작됩니다. 보호 기능은 해당 개체를 차단한 후 치료, 삭제하거나 검역소로 이동하여 제거할 수 있습니다.

보호 기능을 자세히 구성하려면 고급 설정 > **보호**를 엽니다.

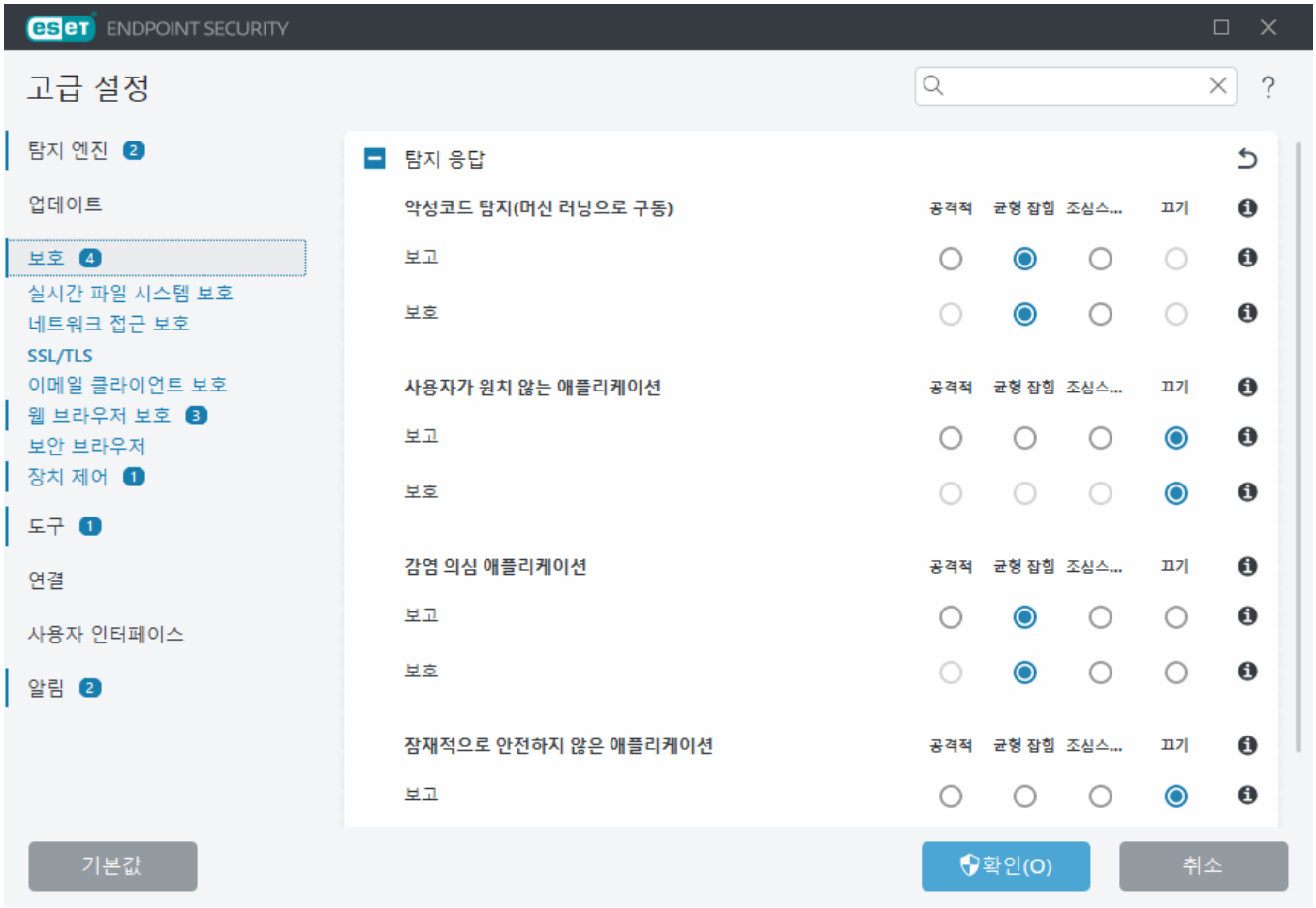
보호 설정은 숙련된 사용자만 변경해야 합니다. 설정을 잘못 구성하면 보호 수준이 저하될 수 있습니다.

이 섹션의 내용:

탐지 응답

탐지 응답을 사용하여 다음 범주에 대한 보고 및 보호 수준을 구성할 수 있습니다.

- **악성코드 탐지(머신 러닝으로 구동)** - 컴퓨터 바이러스는 컴퓨터의 기존 파일 앞뒤에 붙는 악성 코드의 한 종류입니다. 그러나 "바이러스"라는 용어는 잘못 사용되는 경우가 많습니다. "악성코드"(악의적인 소프트웨어)가 더 정확한 용어입니다. 악성코드 탐지는 머신 러닝 구성 요소와 결합된 탐지 엔진 모듈에서 수행됩니다. 이러한 애플리케이션 유형에 대한 자세한 내용은 용어집을 참조하십시오.
- **사용자가 원치 않는 애플리케이션** – 그레이웨어 또는 사용자가 원치 않는 애플리케이션(PUA)은 광범위한 소프트웨어 범주로, 바이러스나 트로이목마 등의 다른 악성코드 유형과 같이 명백하게 악의적이지는 않습니다. 그러나 원치 않는 추가 소프트웨어를 설치하거나, 디지털 장치의 동작을 변경하거나, 사용자가 승인 또는 예상하지 않은 활동을 수행할 수 있습니다. 이러한 애플리케이션 유형에 대한 자세한 내용은 용어집을 참조하십시오.
- **감염 의심 애플리케이션**에는 패커 또는 보호기로 압축된 프로그램이 포함됩니다. 이러한 유형의 보호기는 맬웨어 작성자가 검출을 회피하는 데 악용되는 경우가 많습니다.
- **잠재적으로 안전하지 않은 애플리케이션** – 악의적으로 잘못 사용될 수 있는 적법한 상용 소프트웨어를 나타냅니다. 잠재적으로 안전하지 않은 애플리케이션(PUA)에는 원격 접근 도구, 패스워드 크랙 애플리케이션, 키로거(사용자가 입력하는 각 키 입력을 기록하는 프로그램) 등이 포함됩니다. 이러한 애플리케이션 유형에 대한 자세한 내용은 용어집을 참조하십시오.



개선된 보호

고급 머신 러닝은 이제 머신 러닝에 기반을 두고 탐지 성능을 개선하는 고급 보호 계층으로 보호 기능의 일부입니다. 이 보호 유형에 대한 자세한 내용은 용어집을 읽어 보십시오.

보고 설정

탐지가 발생하면(예: 위협이 발견된 후 악성코드로 분류됨), 정보가 탐지 로그에 기록되고 바탕 화면 알림이 발생합니다(ESET Endpoint Security에서 구성된 경우).

각 범주에 대해 다음과 같은 보고 한계("범주"라고도 함)가 구성됩니다.

1. 악성코드 탐지
2. 사용자가 원치 않는 애플리케이션
3. 잠재적으로 안전하지 않음
4. 감염 의심 응용 프로그램

머신 러닝 구성 요소를 포함하여 탐지 엔진으로 수행되는 보고 작업입니다. 보호 한계를 현재 보호 한계보다 더 높게 설정할 수 있습니다. 이러한 보고 설정은 개체차단, 치료 또는 삭제에 영향을 주지 않습니다.

범주 보고의 한계(또는 수준)를 수정하기 전에 다음 내용을 읽어보십시오.

한계	설명
공격적	최대 민감도로 구성된 범주 보고입니다. 자세한 탐지 사항이 보고됩니다. **공격적** 설정에서는 개체를 범주로 잘못 식별할 수 있습니다.

한계	설명
균형 잡힘	균형 잡힘으로 구성된 범주 보고입니다. 이 설정은 성능과 탐지율의 정확도 및 잘못 보고된 개체의 수가 균형을 이루도록 하는 데 최적화되어 있습니다.
조심스러움	충분한 보호 수준을 유지하면서 잘못 식별된 개체를 최소화하도록 구성된 범주 보고입니다. 개체는 가능성이 분명히 있고 범주의 동작과 일치하는 경우에만 보고됩니다.
끄기	범주에 대한 보고가 활성화되어 있지 않으며 이 유형의 탐지를 찾거나, 보고하거나, 치료하지 않습니다. 그 결과 이 설정은 이 탐지 유형에서 보호를 비활성화합니다. 끄기는 악성코드 보고에는 사용할 수 없으며 잠재적으로 안전하지 않은 애플리케이션에 대한 기본값입니다.

^ ESET Endpoint Security 보호 모듈의 가용성

선택한 범주 한계에 대한 보호 모듈의 가용성(활성화됨 또는 비활성화됨)은 다음과 같습니다.

	공격적	균형 잡힘	조심스러움	끄기*
고급 머신 러닝 모듈	✓ (공격적 모드)	✓ (일반 모드)	X	X
탐지 엔진 모듈	✓	✓	✓	X
기타 보호 모듈	✓	✓	✓	X

* 권장되지 않음.

^ 제품 버전, 프로그램 모듈 버전 및 빌드 날짜 확인

1. **도움말 및 지원** > **ESET Endpoint Security 정보**를 클릭합니다.
2. **정보** 화면의 첫 번째 텍스트 줄에는 ESET 제품의 버전 번호가 표시됩니다.
3. **설치된 구성 요소**를 클릭하여 특정 모듈에 대한 정보에 접근합니다.

기본 방침

환경에 적절한 한계를 설정할 때의 몇 가지 기본 방침은 다음과 같습니다.

- **균형 잡힘** 한계는 대부분의 설정에 권장됩니다.
- **조심스러움** 한계는 보안 소프트웨어에서 잘못 식별된 개체를 최소화하는 것을 가장 우선시하는 환경에서 권장됩니다.
- 보고 한계가 높을수록 탐지율은 높지만 잘못 식별되는 개체가 많아질 수 있습니다.
- 실질적 관점에서 볼 때, 탐지율은 100%로 유지하면서 감염되지 않은 개체를 악성코드로 잘못 분류할 가능성을 0%로 유지할 수는 없습니다.
- ESET Endpoint Security 및 해당 모듈을 최신 상태로 유지하여 성능과 탐지율의 정확도 및 잘못 보고되는 개체 수가 최대한 균형을 이루도록 하십시오.

보호 설정

범주로 분류된 개체가 보고될 경우 프로그램은 해당 개체를 차단한 후 치료하거나, 삭제하거나, 검역소로 이동합니다.

범주 보호의 한계(또는 수준)를 수정하기 전에 다음 내용을 읽어보십시오.

한계	설명
공격적	공격적(또는 이보다 낮은) 수준으로 보고된 탐지가 차단되고, 자동 수정(즉 치료)이 시작됩니다. 이 설정은 모든 엔드포인트를 공격적 설정으로 검사하고 잘못 보고된 개체를 탐지 제외에 추가한 경우에 권장됩니다.
균형 잡힘	균형 잡힘(또는 이보다 낮은) 수준으로 보고된 탐지가 차단되고, 자동 수정(즉 치료)이 시작됩니다.
조심스러움	조심스러움 수준으로 보고된 탐지가 차단되고, 자동 수정(즉 치료)이 시작됩니다.
끄기	잘못 보고된 개체를 식별하고 제외하는 데 유용합니다. 끄기는 악성코드 보호에는 사용할 수 없으며 잠재적으로 안전하지 않은 애플리케이션에 대한 기본값입니다.

모범 사례

관리되지 않음(개별 클라이언트 워크스테이션)

기본 권장 값을 그대로 유지합니다.

관리되는 환경

이러한 설정은 일반적으로 정책을 통해 워크스테이션에 적용됩니다.

1. 초기 단계

이 단계는 최대 1주일이 소요될 수 있습니다.

- 모든 **보고** 한계를 **균형 잡힘**으로 설정합니다.
  참고: 필요한 경우 **공격적**으로 설정합니다.
- 악성코드에 대한 **보호**를 **균형 잡힘**으로 설정하거나 유지합니다.
- 다른 범주에 대한 **보호**를 **조심스러움**으로 설정합니다.
  참고: 잘못 식별된 경우를 포함하여 찾은 모든 탐지가 수정되므로 이 단계에서 **보호** 한계를 **공격적**으로 설정하는 것은 권장되지 않습니다.
- 탐지 로그에서 잘못 식별된 개체를 식별한 후 탐지 제외 목록에 먼저 추가합니다.

2. 전환 단계

- 일부 워크스테이션에 대해 테스트로서 "프로덕션 단계"를 구현합니다(네트워크의 모든 워크스테이션은 아님).

3. 프로덕션 단계

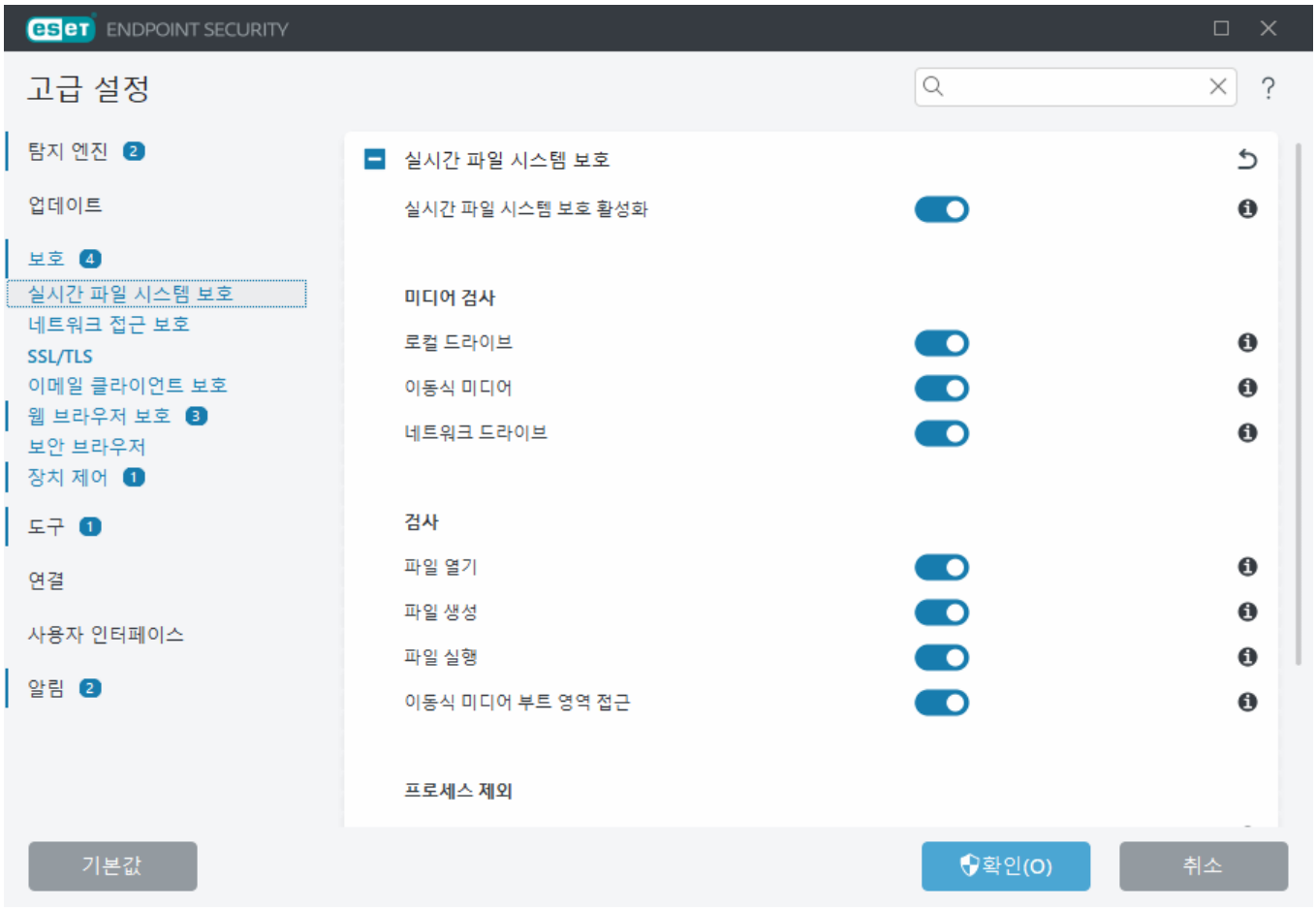
- 모든 **보호** 한계를 **균형 잡힘**으로 설정합니다.
- 원격으로 관리되는 경우 ESET Endpoint Security에 대해 해당 안티바이러스 미리 정의된 정책을 사용합니다.
- **공격적** 보호 한계는 가장 높은 탐지율이 필요하고 잘못 식별된 개체를 허용하는 경우에 설정할 수 있

습니다.

- 누락되었을 수 있는 탐지에 대해서는 탐지 로그 또는 ESET PROTECT 보고서를 확인합니다.

실시간 파일 시스템 보호

실시간 파일 시스템 보호는 파일을 열거나 생성하거나 실행할 때 시스템의 모든 파일에 포함된 악의적인 코드를 제어합니다.



기본적으로 시스템 시작 시 실시간 파일 시스템 보호가 시작되며 중단 없이 검사를 수행합니다. 고급 설정 > **보호** > **실시간 파일 시스템 보호** > **실시간 파일 시스템 보호**에서 **실시간 파일 시스템 보호 활성화**를 비활성화하지 않는 것이 좋습니다.

미디어 검사

기본적으로 모든 미디어 유형은 잠재적 위협에 대해 검사됩니다.

- **로컬 드라이브** – 모든 시스템 및 고정 하드 드라이브(예: *C:*, *D:*)를 검사합니다.
- **이동식 미디어** – CD/DVD, USB 저장소, 메모리 카드 등을 검사합니다.
- **네트워크 드라이브** – 매핑된 모든 네트워크 드라이브(예: *\\store04*로서 *H:*) 또는 직접 접근 네트워크 드라이브(예: *\\store08*)를 검사합니다.

기본 설정을 사용하고 특정 미디어를 검사할 때 데이터 전송 속도가 크게 느려지는 등의 특수한 상황에서만 이러한 설정을 수정하는 것이 좋습니다.

검사

기본적으로 열거나 만들거나 실행할 때 모든 파일이 검사됩니다. 컴퓨터에 최대 수준의 실시간 보호 기능을 제공하는 기본 설정을 유지하는 것이 좋습니다.

- **파일 열기** – 파일이 열릴 때 검사합니다.
- **파일 생성** – 생성되었거나 수정된 파일을 검사합니다.
- **파일 실행** – 파일이 실행될 때 검사합니다.
- **이동식 미디어 부트 영역 접근** – 부트 영역을 포함하는 이동식 미디어를 장치에 삽입하면 부트 영역이 즉시 검사됩니다. 이 옵션을 선택해도 이동식 미디어 파일 검사는 활성화되지 않습니다. 이동식 미디어 파일 검사는 **미디어 검사** > **이동식 미디어**에 있습니다. **이동식 미디어 부트 영역 접근**이 제대로 작동하려면 ThreatSense에서 **부트 영역/UEFI**를 활성화 상태로 유지해야 합니다.

프로세스 제외

프로세스 제외를 참조하십시오.

ThreatSense

모든 유형의 미디어를 검사하는 실시간 파일 시스템 보호는 파일에 접근하는 등의 다양한 시스템 이벤트가 발생하면 트리거됩니다. ThreatSense에 설명된 ThreatSense 기술 탐지 방법을 사용하면 실시간 파일 시스템 보호 기능을 통해 새로 생성된 파일을 기존 파일과 다르게 처리하도록 구성할 수 있습니다. 예를 들면 실시간 파일 시스템 보호를 구성하여 새로 생성된 파일을 좀 더 면밀히 모니터링할 수 있습니다.

실시간 보호 기능을 사용할 때 시스템 공간을 최소화하기 위해 이미 검사한 파일이 수정된 경우를 제외하고는 반복적으로 검사하지 않습니다. 각 검색 엔진 업데이트 직후 파일이 다시 검사됩니다. 이 동작은 **스마트 최적화**를 통해 제어됩니다. 이 **스마트 최적화**가 비활성화된 경우 모든 파일에 접근할 때마다 모든 파일이 검사됩니다. 이 설정을 수정하려면 고급 설정 > **보호** > **실시간 파일 시스템 보호**를 엽니다. **ThreatSense** > **기타**를 클릭하고 **스마트 최적화 활성화**를 선택하거나 선택 취소합니다.

또한 실시간 파일 시스템 보호를 통해 추가 ThreatSense 파라미터를 구성할 수 있습니다.

프로세스 제외

프로세스 제외 기능을 사용하면 애플리케이션 프로세스를 실시간 파일 시스템 보호에서 제외할 수 있습니다. 백업 속도, 프로세스 무결성 및 서비스 가용성을 개선하기 위해 백업 도중 파일 수준 악성코드 탐지와 충돌을 일으키는 것으로 알려진 일부 기술이 사용됩니다. 두 상황을 효과적으로 방지할 수 있는 유일한 방법은 악성코드 방지 소프트웨어를 비활성화하는 것입니다. 특정 프로세스(예: 백업 솔루션의 프로세스)를 제외함으로써 그러한 제외된 프로세스에 관련된 모든 파일 작업은 무시되고 안전한 것으로 간주되므로 백업 프로세스에서의 간섭이 최소화됩니다. 제외된 백업 도구가 경고를 트리거하지 않고 감염된 파일에 접근할 수 있으므로 제외를 생성할 때 주의하는 것이 좋습니다. 이러한 문제 때문에 실시간 보호 모듈에서만 확장된 권한이 허용됩니다.

> 제외된 파일 확장명, HIPS 제외, 탐지 제외 또는 성능 제외와 혼동하지 마십시오.

프로세스 제외는 잠재적 충돌 위험을 최소화하고 제외된 애플리케이션의 성능을 개선하는 데 도움이 되며, 결과적으로 운영 체제의 전반적 성능 및 안정성에 긍정적 효과를 미칩니다. 프로세스/애플리케이션 제외는 그 실행 파일(*.exe*)을 제외하는 것입니다.

고급 설정 > **보호** > **실시간 파일 시스템 보호** > **실시간 파일 시스템 보호** > **프로세스 제외**에서 제외된 프로세스의 목록에 실행 파일을 추가할 수 있습니다.

이 기능은 백업 도구를 제외하기 위해 설계된 것입니다. 백업 도구의 프로세스를 검사에서 제외하면 시스템 안정성이 확보될 뿐 아니라 백업 실행 시 속도가 저하되지 않아 백업 성능에도 영향을 미치지 않습니다.

편집을 클릭하여 **프로세스 제외** 관리 창을 엽니다. 이 창에서 제외를 추가하고 검사에서 제외될 실행 파일(예 *Backup-tool.exe*)을 탐색할 수 있습니다.
.exe 파일이 제외에 추가되는 즉시 ESET Endpoint Security가 이 프로세스의 활동을 모니터링되지 않으며 이 프로세스가 수행하는 모든 파일 작업에서 검사를 실행하지 않습니다.

프로세스 실행 파일을 선택할 때 탐색 기능을 사용하지 않을 경우 수동으로 전체 실행 파일 경로를 입력해야 합니다. 그렇지 않을 경우 제외가 올바로 작동하지 않으며 HIPS가 오류를 보고할 수 있습니다.

기존 프로세스를 **편집**하거나 제외 목록에서 **삭제**할 수도 있습니다.

웹 브라우저 보호는 이 제외를 고려하지 않습니다. 그러므로 웹 브라우저의 실행 파일을 제외하더라도 다운로드된 파일은 계속 검사됩니다. 이러한 방식으로 여전히 모든 침투를 탐지할 수 있습니다. 이 시나리오는 하나의 예일 뿐이며 웹 브라우저에 대해 제외를 생성하지 않는 것이 좋습니다.

프로세스 제외 추가 또는 편집

이 대화 상자 창에서는 탐지 엔진에서 제외된 프로세스를 **추가**할 수 있습니다. 프로세스 제외는 잠재적 충돌 위험을 최소화하고 제외된 애플리케이션의 성능을 개선하는 데 도움이 되며, 결과적으로 운영 체제의 전반적 성능 및 안정성에 긍정적 효과를 미칩니다. 프로세스/애플리케이션 제외는 그 실행 파일(*.exe*)을 제외하는 것입니다.

... 를 클릭하여 예외 애플리케이션의 파일 경로를 선택합니다(예: *C:\Program Files\Firefox\Firefox.exe*). 애플리케이션의 이름을 입력하지 마십시오.
.exe 파일이 제외에 추가되는 즉시 ESET Endpoint Security가 이 프로세스의 활동을 모니터링되지 않으며 이 프로세스가 수행하는 모든 파일 작업에서 검사를 실행하지 않습니다.

프로세스 실행 파일을 선택할 때 탐색 기능을 사용하지 않을 경우 수동으로 전체 실행 파일 경로를 입력해야 합니다. 그렇지 않을 경우 제외가 올바로 작동하지 않으며 HIPS가 오류를 보고할 수 있습니다.

기존 프로세스를 **편집**하거나 제외 목록에서 **삭제**할 수도 있습니다.

실시간 보호 설정을 변경하는 경우

실시간 보호는 보안 시스템을 유지 관리하는 데 있어 가장 중요한 구성 요소입니다. 따라서 해당 파라미터를 수정할 때는 주의해야 합니다. 다른 안티바이러스 프로그램의 실시간 검사기나 특정 애플리케이션과.

ESET Endpoint Security을 설치하고 나면 사용자에게 최대 시스템 보호 수준을 제공하기 위해 모든 설정이 최적화됩니다. 기본 설정을 복원하려면 고급 설정 > **보호** > **탐지 응답** 옆에 있는 ↺을 클릭합니다.

실시간 보호 검사

실시간 보호가 작동 중이며 바이러스를 탐지하는지 확인하려면 eicar.com에서 제공하는 테스트 파일을 사용합니다. 이 테스트 파일은 모든 안티바이러스 프로그램에서 탐지할 수 있는 무해한 파일입니다. 이 파일은 EICAR(European Institute for Computer Antivirus Research)이라는 회사에서 안티바이러스 프로그램의 기능을 테스트하기 위해 마련했습니다.

파일은 http://www.eicar.org/download/eicar.com에서 다운로드할 수 있습니다.
이 URL을 브라우저에 입력하면 위협이 제거되었다는 메시지가 표시됩니다.

실시간 보호가 작동하지 않는 경우 수행할 작업

이 장에서는 실시간 보호를 사용할 때 발생할 수 있는 문제와 이러한 문제를 해결하는 방법을 설명합니다.

실시간 보호가 비활성화됨

사용자가 실수로 실시간 보호를 비활성화한 경우 기능을 다시 활성화해야 합니다. 실시간 보호를 다시 활성화하려면 기본 프로그램 창에서 **설정**으로 이동하여 **컴퓨터 > 실시간 파일 시스템 보호**를 클릭합니다.

시스템을 시작할 때 실시간 보호가 시작되지 않으면, 일반적으로 **실시간 파일 시스템 보호 활성화**가 비활성화되어 있기 때문입니다. 이 옵션이 활성화되어 있는지 확인하려면 고급 설정 > **보호** > **실시간 파일 시스템 보호**를 엽니다.

실시간 보호가 침입을 검출 및 치료하지 않는 경우

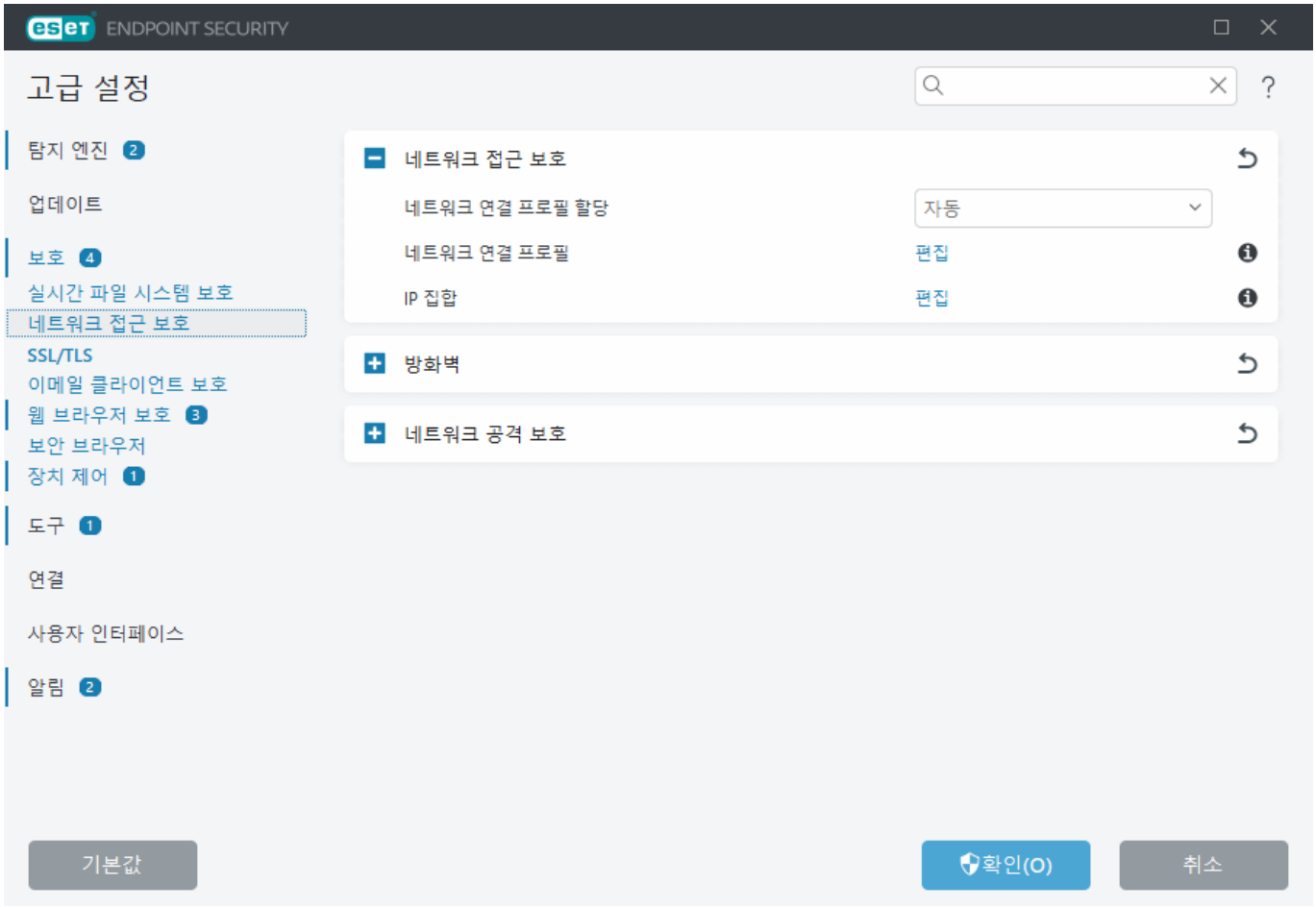
컴퓨터에 다른 안티바이러스 프로그램이 설치되어 있지 않은지 확인합니다. 두 개의 안티바이러스 프로그램이 동시에 설치되어 있는 경우 서로 충돌할 수 있습니다. ESET 제품을 설치하기 전에 시스템에 있는 모든 안티바이러스 프로그램을 제거하는 것이 좋습니다.

실시간 보호가 시작되지 않음

시스템 시작 시 실시간 보호가 시작되지 않고 **실시간 파일 시스템 보호 활성화**가 활성화된 경우, 다른 프로그램과 충돌하기 때문일 수 있습니다. 이 문제를 해결하려면 ESET SysInspector 로그를 생성하여 분석을 위해 ESET 기술 지원에 제출하십시오.

네트워크 접근 보호

네트워크 접근 보호를 사용하면 모든 네트워크 연결을 세부적으로 구성할 수 있습니다. 구성에 따라 특정 네트워크에서 컴퓨터에 대한 접근을 허용/거부하고, 컴퓨터에서 네트워크 장치에 대한 접근을 허용/거부할 수 있습니다. 기본적으로 ESET Endpoint Security에는 보안 성능을 극대화하도록 미리 구성된 방화벽 규칙과 네트워크 접근 보호 기능이 있습니다. 그러나 특정 환경에서는 사용자 지정 구성이 필요할 수 있습니다. 기본 설정은 숙련된 사용자만 변경해야 합니다.



고급 설정 > **보호** > **네트워크 접근 보호**에서 다음 설정을 구성할 수 있습니다(각 네트워크 접근 보호 옵션에 대한 자세한 설명은 아래 링크 클릭).

네트워크 접근 보호

네트워크 연결 프로필 - 프로필을 사용하여 특정 네트워크 연결에 대한 네트워크 접근 보호 기능 및 방화벽을 제어할 수 있습니다.

IP 집합 - 하나의 논리 IP 주소 그룹을 생성하는 IP 주소 모음을 정의한 다음 방화벽 및 무차별 공격 보호 규칙에 사용할 수 있습니다.

방화벽

네트워크 공격 보호

네트워크 연결 프로필

프로필을 사용하여 특정 네트워크 연결에 대한 ESET Endpoint Security 네트워크 접근 보호 동작을 제어할 수 있습니다. 방화벽 규칙, IDS 규칙 또는 무차별 공격 보호 규칙을 생성하거나 편집할 때 규칙을 특정 프로필에 할당하거나 모든 프로필에 적용할 수 있습니다. 프로필이 네트워크 연결에서 활성화된 경우 전역 규칙(프로필이 지정되지 않은 규칙) 및 해당 프로필에 할당된 규칙만 프로필에 적용됩니다. 네트워크 연결에 할당된 여러 규칙을 사용해 프로필을 여러 개 생성하여 방화벽 동작을 쉽게 변경할 수 있습니다.

고급 설정 > **보호** > **네트워크 접근 보호** > **네트워크 접근 보호**에서 네트워크 연결 프로필과 할당을 구성할 수 있습니다.

네트워크 연결 프로필 할당 - 새로 검색된 네트워크 연결에서 네트워크 연결 프로필에 구성된 활성화 도구를 기준으로 미리 정의된 프로필이나 사용자 지정 프로필을 자동(드롭다운 메뉴에서 **자동** 선택)으로 할당할 것인지, 아니면 새 네트워크 연결이 탐지될 때마다 네트워크 보호를 구성하고 프로필을 수동으로 할당하기 위해 확인(드롭다운 메뉴에서 **확인** 선택)받을 것인지 선택할 수 있습니다.

또한 기본 프로그램 창 > **설정** > **네트워크** > **네트워크 연결**에서 특정 네트워크 연결 프로필을 수동으로 할당할 수 있습니다. 특정 네트워크 연결을 마우스로 가리키고 ⋮ 메뉴 아이콘 > **편집**을 클릭하여 네트워크 보호 구성 창을 열고 프로필을 선택합니다.

네트워크 연결 프로필 - **편집**을 클릭하여 네트워크 연결 프로필을 추가 또는 편집합니다.

다음 프로필은 미리 정의되어 있으며 편집/제거할 수 없습니다.

개인 – 신뢰할 수 있는 네트워크(홈 네트워크 또는 회사 네트워크). 컴퓨터에 저장된 공유 파일과 컴퓨터가 다른 네트워크 사용자에게 표시되며, 네트워크의 다른 사용자가 시스템 리소스에 접근할 수 있습니다(공유 파일 및 프린터에 대한 접근이 활성화되고 들어오는 RPC 통신이 활성화되며 원격 데스크톱 공유를 사용할 수 있음). 안전한 로컬 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성된 경우 네트워크 연결에 자동으로 할당됩니다.

공용 – 신뢰할 수 없는 네트워크(공용 네트워크). 시스템의 파일 및 폴더가 네트워크의 다른 사용자와 공유되거나 다른 사용자에게 표시되지 않으며, 시스템 리소스 공유가 비활성화됩니다. 무선 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성되지 않은 모든 네트워크 연결에 자동으로 할당됩니다.

네트워크 연결이 다른 프로필로 전환되면 화면 오른쪽 하단에 알림이 표시됩니다.

네트워크 연결 프로필 추가 또는 편집

고급 설정 > **보호** > **네트워크 접근 보호** > **네트워크 접근 보호** > **네트워크 연결 프로필** > **편집**에서 네트워크 연결 프로필을 추가하거나 편집할 수 있습니다. 프로필을 편집하려면 **네트워크 연결 프로필** 창 목록에서 프로필을 선택해야 합니다.

다음 프로필은 미리 정의되어 있으며 편집/제거할 수 없습니다.

개인 – 신뢰할 수 있는 네트워크(홈 네트워크 또는 회사 네트워크). 컴퓨터에 저장된 공유 파일과 컴퓨터가 다른 네트워크 사용자에게 표시되며, 네트워크의 다른 사용자가 시스템 리소스에 접근할 수 있습니다(공유 파일 및 프린터에 대한 접근이 활성화되고 들어오는 RPC 통신이 활성화되며 원격 데스크톱 공유를 사용할 수 있음). 안전한 로컬 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성된 경우 네트워크 연결에 자동으로 할당됩니다.

공용 – 신뢰할 수 없는 네트워크(공용 네트워크). 시스템의 파일 및 폴더가 네트워크의 다른 사용자와 공유되거나 다른 사용자에게 표시되지 않으며, 시스템 리소스 공유가 비활성화됩니다. 무선 네트워크에 접근하는 경우 이 설정을 사용하는 것이 좋습니다. 이 프로필은 Windows에서 도메인 또는 개인 네트워크로 구성되지 않은 모든 네트워크 연결에 자동으로 할당됩니다.

맨 위로/위로/아래로/맨 아래로  - 네트워크 연결 프로필의 우선순위 수준을 조정할 수 있습니다(네트워크 연결 프로필은 우선순위에 따라 평가 및 적용됨. 일치하는 첫 번째 프로필이 항상 적용됨).

프로필 추가 또는 편집

사용자 지정 네트워크 연결 프로필을 사용하여 방화벽 규칙, 무차별 공격 보호 규칙을 적용하고 특정 네트워크 연결에 대한 추가 설정을 정의할 수 있습니다. 활성화 도구 섹션에서 사용자 지정 프로필을 할당할 네트워크 연결을 지정합니다.

프로필 편집기를 열려면 **네트워크 연결 프로필** 창에서 다음을 수행합니다.

- **추가**를 클릭합니다.
- 기존 프로필 중 하나를 선택하고 **편집**을 클릭합니다.
- 기존 프로필 중 하나를 선택하고 **복사**를 클릭합니다.

이름 - 프로필의 사용자 지정 이름입니다.

설명 - 프로필을 식별하는 데 도움이 되는 프로필 설명입니다.

신뢰할 수 있는 추가 주소 - 여기에 정의된 주소는 네트워크의 보호 유형에 상관없이 이 프로필이 적용되는 네트워크 연결의 신뢰 영역에 추가됩니다.

신뢰할 수 있는 연결 - 컴퓨터에 저장된 공유 파일과 컴퓨터가 다른 네트워크 사용자에게 표시되며, 네트워크의 다른 사용자가 시스템 리소스에 접근할 수 있습니다(공유 파일 및 프린터에 대한 접근이 활성화되고 들어오는 RPC 통신이 활성화되며 원격 데스크톱 공유를 사용할 수 있음). 보안 로컬 네트워크 연결용 프로필을 생성할 때 이 설정을 사용하는 것이 좋습니다. 직접 연결된 모든 네트워크 서브넷도 신뢰할 수 있는 것으로 간주됩니다. 예를 들어, 네트워크 어댑터가 IP 주소 192.168.1.5로 이 네트워크에 연결되어 있고 서브넷 마스크가 255.255.255.0인 경우 서브넷 192.168.1.0/24가 해당 네트워크 연결의 신뢰 영역에 추가됩니다. 어댑터에 추가 주소/서브넷이 있는 경우 모두 신뢰할 수 있습니다.

약한 Wi-Fi 암호화 보고 - 보호되지 않는 무선 네트워크 또는 보호 성능이 약한 네트워크에 연결하면 ESET Endpoint Security에서 데스크톱 알림을 표시합니다.

활성화 도구 - 이 네트워크 연결 프로필을 네트워크 연결에 할당하려면 충족해야 하는 사용자 지정 조건입니다. 자세한 설명은 활성화 도구를 참조하십시오.

활성화 도구

활성화 도구는 네트워크 연결 프로필을 네트워크 연결에 할당하기 위해 충족되어야 하는 사용자 지정 조건입니다. 연결된 네트워크 프로필에 대한 활성화 도구에 정의된 것과 동일한 특성이 연결된 네트워크에 있는 경우 해당 프로필이 네트워크에 적용됩니다. 네트워크 연결 프로필에는 하나 이상의 활성화 도구가 있을 수 있습니다. 활성화 도구가 여러 개 있는 경우 OR 논리가 적용됩니다(하나 이상의 조건이 충족되어야 함). 네트워크 연결 프로필 편집기에서 활성화 도구를 정의할 수 있습니다. 사용자 지정 네트워크 연결 프로필 생성 작업은 숙련된 사용자가 수행해야 합니다.

다음 활성화 도구를 사용할 수 있습니다(현재 연결되어 있는 네트워크에 대한 상세 정보를 알고 싶다면 네트워크 연결 참조).

어댑터

어댑터 유형 - 선택한 어댑터 유형에 네트워크 연결이 설정된 경우 프로필을 적용합니다.
어댑터 이름 - 네트워크 어댑터 이름이 일치하는 경우 프로필을 적용합니다.
어댑터 IP - 네트워크 어댑터의 IP 주소가 일치하는 경우 프로필을 적용합니다.

DNS

DNS 접미사 - 도메인 이름이 일치하는 경우 프로필을 적용합니다.
DNS IP - DNS 서버 IP 주소가 일치하는 경우 프로필을 적용합니다.

WINS

Windows Internet Name Service (WINS) 매핑된 IP 주소가 일치하는 경우 프로필을 적용합니다.

DHCP

DHCP IP - DHCP 서버 IP 주소와 일치합니다.

기본 게이트웨이

IP - 기본 게이트웨이 IP 주소가 일치하는 경우 프로필을 적용합니다.
MAC 주소 - 기본 게이트웨이 MAC 주소가 일치하는 경우 프로필을 적용합니다.

Wi-Fi

SSID - SSID(Wi-Fi 이름)가 일치하는 경우 프로필을 적용합니다.
프로필 이름 - Wi-Fi 프로필 이름이 일치하는 경우 프로필을 적용합니다.
보안 유형 - 보안 유형이 드롭다운 메뉴에서 선택한 보안 유형과 일치하는 경우 프로필을 적용합니다(둘 이상을 일치시키려면 다른 활성화 도구 생성).
암호화 유형 - 암호화 유형이 드롭다운 메뉴에서 선택한 것과 일치하는 경우 프로필을 적용합니다(둘 이상을 일치시키려면 다른 활성화 도구 생성.
네트워크 보안 - 네트워크가 **개방형/보안형**인 경우 프로필을 적용합니다.

Windows 프로필

네트워크가 Windows에서 **도메인/개인/공용**으로 구성된 경우 프로필을 적용합니다.

인증

네트워크 인증은 네트워크에서 특정 서버를 검색하고 비대칭 암호화(RSA)를 사용하여 해당 서버를 인증합니다. 인증되는 네트워크의 이름은 인증 서버 설정에 지정된 이름과 일치해야 합니다. 이름은 대소문자를 구분합니다. 서버 이름은 IP 주소, DNS 또는 NetBios 이름으로 입력할 수 있습니다.
ESET 인증 서버 다운로드
공개 키는 다음과 같은 파일 형식 중 하나를 사용하여 가져올 수 있습니다.
• PEM 암호화 공개 키(.pem), ESET 인증 서버를 사용하여 이 키를 생성할 수 있습니다
• 암호화된 공개 키
• 공개 키 인증서(.crt)
설정을 테스트하려면 **테스트**를 클릭합니다. 인증에 성공하면 서버 인증이 완료되었습니다.라고 표시됩니다. 인증이 올바르게 구성되지 않으면 다음 오류 메시지 중 하나가 나타납니다:
서버 인증에 실패했습니다. 서명이 올바르지 않거나 일치하지 않습니다.
서버 서명이 입력한 공개 키와 일치하지 않습니다.
서버 인증에 실패했습니다. 네트워크 이름이 일치하지 않습니다.
구성된 네트워크 이름이 인증 서버 네트워크 이름과 일치하지 않습니다. 두 이름을 모두 검토하고 동일한지 확인합니다.
서버 인증에 실패했습니다. 서버의 응답이 올바르지 않거나 없습니다.
서버가 실행 중이지 않거나 접근할 수 없으면 응답이 수신되지 않습니다. 지정된 주소에서 다른 HTTP 서버가 실행 중이면 잘못된 응답이 수신될 수 있습니다.
잘못된 공개 키를 입력했습니다.
입력한 공개 키 파일이 손상되지 않았는지 확인하십시오.

IP 집합

IP 집합은 하나의 논리 IP 주소 그룹을 생성하는 IP 주소 모음으로, 여러 방화벽 규칙 또는 무차별 공격 보호 규칙에서 동일한 주소 집합을 재사용하는 경우에 유용합니다. 또한 ESET Endpoint Security에는 내부 규칙이 적용되는 미리 정의된 IP 집합이 포함됩니다. 이러한 그룹의 일례로 **신뢰 영역**을 들 수 있습니다. 신뢰 영역은 컴퓨터에 저장된 공유 파일과 컴퓨터가 다른 네트워크 사용자에게 표시되며 네트워크의 다른 사용자가 시스템 리소스에 접근할 수 있는 네트워크 주소 그룹을 나타냅니다.

IP 집합을 추가하려면 다음을 수행합니다.

1. 고급 설정 > **보호** > **네트워크 접근 보호** > **IP 집합** > **편집**을 엽니다.
2. **추가**를 클릭하고 영역의 **이름**과 **설명**을 입력한 후 **원격 컴퓨터 주소(IPv4/IPv6, 범위, 마스크)**에 원격 IP 주소를 입력합니다.
3. **확인**을 클릭합니다.

자세한 내용은 IP 집합 편집을 참조하십시오.

IP 집합 편집

IP 집합에 대한 자세한 내용은 IP 집합을 참조하십시오.

열

이름 - 원격 컴퓨터 그룹의 이름입니다.

설명 - 그룹에 대한 일반 설명입니다.

IP 주소 - IP 집합에 속하는 원격 IP 주소입니다.

제어 요소

IP 집합을 **추가**하거나 **편집**하면 다음 필드를 사용할 수 있습니다.

이름 - 원격 컴퓨터 그룹의 이름입니다.

설명 - 그룹에 대한 일반 설명입니다.

원격 컴퓨터 주소(IPv4, IPv6, 범위, 마스크) – 원격 주소, 주소 범위 또는 서브넷을 추가할 수 있습니다.

삭제 - 목록에서 영역을 제거합니다.

미리 정의된 IP 집합은 제거할 수 없습니다.

IP 주소 예제

IPv4 주소 추가:

단일 주소 - 개별 컴퓨터의 IP 주소(예: *192.168.0.10*)를 추가합니다.

주소 범위 - 시작 IP 주소와 끝 IP 주소를 입력하여 여러 컴퓨터의 IP 범위(예: *192.168.0.1~192.168.0.99*)를 지정합니다.

서브넷 - IP 주소 및 마스크에서 정의된 서브넷(컴퓨터 그룹)입니다. 예를 들어 255.255.255.0은 192.168.1.0 서브넷의 네트워크 마스크입니다. 전체 서브넷 유형을 제외하려면 *192.168.1.0/24*를 입력합니다.

IPv6 주소 추가:

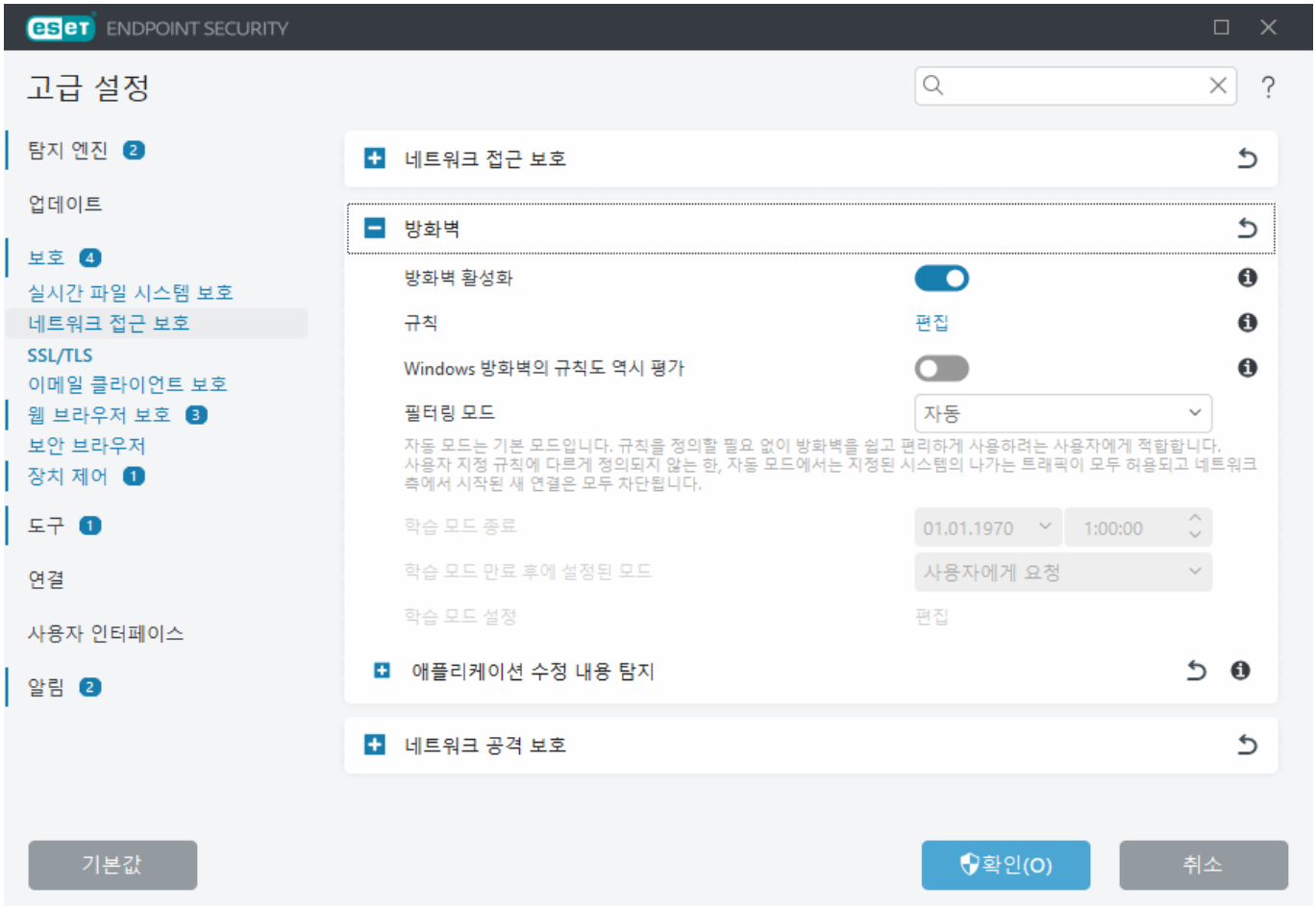
단일 주소 - 개별 컴퓨터의 IP 주소(예: *2001:718:1c01:16:214:22ff:fec9:ca5*)를 추가합니다.

서브넷 - 서브넷(컴퓨터 그룹)은 IP 주소 및 마스크로 정의됩니다(예: *2002:c0a8:6301:1::1/64*).

방화벽

방화벽은 내부 규칙과 사용자가 정의한 규칙에 따라 컴퓨터의 모든 인바운드/아웃바운드 네트워크 트래픽을 제어합니다. 이는 개별 네트워크 연결을 허용하거나 거부하는 방식으로 수행됩니다. 방화벽은 원격 장치의 공격으로부터 보호하고 잠재적으로 위협이 되는 서비스를 차단할 수 있습니다.

방화벽을 구성하려면 고급 설정 > **보호** > **네트워크 접근 보호** > **방화벽**을 엽니다.



방화벽

방화벽 활성화

시스템의 보안을 위해 이 기능을 활성화된 상태로 두는 것이 좋습니다. 방화벽을 활성화하면 네트워크 트래픽이 양방향으로 검사됩니다.

규칙

규칙 설정에서는 신뢰 영역 및 인터넷 내에서 개별 애플리케이션이 생성하는 트래픽에 적용되는 모든 규칙을 보고 편집할 수 있습니다.

GPO(그룹 정책)를 사용하여 구성된 Windows 방화벽의 규칙은 평가되지 않습니다.

봇넷가 컴퓨터를 공격한 경우 IDS 규칙을 생성할 수 있습니다. 규칙은 **편집**을 클릭하여 고급 설정 > **보호** > **네트워크 접근 보호** > **네트워크 공격 보호(IDS)** > **IDS 규칙**에서 수정할 수 있습니다.

Windows 방화벽의 규칙도 역시 평가

ESET 규칙에 따라 명시적으로 차단되지 않은 한, 자동 필터링 모드에서는 Windows 방화벽의 규칙에 의해 허용되는 들어오는 트래픽이 평가 및 처리됩니다.

필터링 모드

방화벽의 동작은 필터링 모드에 따라 달라집니다. 필터링 모드는 필요한 사용자 상호 작용 수준에도 영향을 줍니다.

방화벽의 동작은 필터링 모드에 따라 달라집니다. 필터링 모드는 필요한 사용자 상호 작용 수준에도 영향을 줍니다. ESET Endpoint Security 방화벽에서는 다음과 같은 필터링 모드를 사용할 수 있습니다.

필터링 모드	설명
자동 모드	기본 모드로서, 규칙을 정의할 필요 없이 방화벽을 쉽고 편리하게 사용하려는 사용자에게 적합합니다. 사용자 지정, 사용자 정의 규칙을 생성할 수 있지만 자동 모드에는 필요하지 않습니다. 사용자 지정, 사용자 정의 규칙을 생성할 수 있지만 **자동 모드**에는 필요하지 않습니다. 자동 모드에서는 지정된 시스템에서 나가는 모든 트래픽을 허용하고 들어오는 대부분의 트래픽을 차단합니다(IDS 및 고급 옵션/허용된 서비스에서 지정된 신뢰 영역의 일부 트래픽과 최근 나가는 통신에 응답하는 들어오는 트래픽은 예외임).
대화 모드	대화 모드 – 사용자가 개인 방화벽에 원하는 구성을 작성할 수 있습니다. 통신이 검색되었지만 해당 통신에 적용되는 기존 규칙이 없는 경우 알 수 없는 연결을 보고하는 대화 상자 창이 표시됩니다. 이 대화 상자 창에서는 해당 통신을 허용하거나 거부하는 옵션이 제공되며, 이 허용 또는 거부 결정을 새로운 방화벽 규칙으로 저장할 수 있습니다. 새 규칙을 생성하도록 선택하면 이 유형의 향후 모든 연결이 해당 규칙에 따라 허용되거나 차단됩니다.
정책 기반 모드	연결을 허용하는 특정 규칙에 의해 정의되지 않은 모든 연결이 차단됩니다. 고급 사용자는 이 모드에서 자신이 원하는 안전한 연결만 허용하는 규칙을 정의할 수 있습니다. 지정되지 않은 다른 모든 연결은 방화벽에 의해 차단됩니다.
학습 모드	규칙을 자동으로 생성 및 저장하는 이 모드는 방화벽의 초기 구성에 가장 효과적으로 사용되지만 오랫동안 그대로 계속 사용해서는 안 됩니다. ESET Endpoint Security에서 미리 정의된 파라미터에 따라 규칙을 저장하므로 사용자 상호 작용이 필요하지 않습니다. 보안 위험을 방지하기 위해 학습 모드는 필요한 통신에 대한 모든 규칙을 생성할 때까지만 사용해야 합니다.

학습 모드 종료 시간 - 학습 모드가 자동으로 종료되는 날짜와 시간을 설정합니다. 원할 때마다 학습 모드를 수동으로 끌 수도 있습니다.

학습 모드 만료 후에 설정된 모드 – 학습 모드 기간이 종료된 후 방화벽에 대해 다시 설정되는 필터링 모드를 정의합니다. 위 표에서 필터링 모드에 대한 자세한 내용을 읽어보십시오. 완료된 경우 **사용자에게 요청** 옵션을 사용하려면 방화벽 필터링 모드를 변경할 수 있는 관리자 권한이 필요합니다.

학습 모드 설정 - **편집**을 클릭하여 학습 모드에서 생성된 규칙을 저장하기 위한 파라미터를 구성합니다.

애플리케이션 수정 내용 검색

애플리케이션 수정 탐지 기능은 방화벽 규칙이 있는 수정된 애플리케이션에서 연결하려고 시도하는 알림을 표시합니다.

학습 모드 설정

학습 모드에서는 시스템에 설정된 각 통신에 대한 규칙이 자동으로 생성되어 저장됩니다. ESET Endpoint Security에서 미리 정의된 파라미터에 따라 규칙을 저장하므로 사용자 상호 작용이 필요하지 않습니다.

이 모드는 시스템을 위험에 노출시킬 수 있으므로 방화벽의 초기 구성에만 사용하는 것이 좋습니다.

고급 설정 > **보호** > **네트워크 접근 보호** > **방화벽** > **방화벽** > **필터링 모드**의 드롭다운 메뉴에서 **학습**을 선택하여 학습 모드 옵션을 활성화합니다. **학습 모드 설정** 옆의 **편집**을 클릭하여 다음 옵션을 구성합니다.

⚠ 학습 모드 중에는 방화벽이 통신을 필터링하지 않습니다. 즉, 나가는 통신과 들어오는 통신이 모두 허용됩니다. 따라서 이 모드에서는 컴퓨터가 방화벽에 의해 완전하게 보호되지 않습니다.

신뢰 영역으로부터 들어오는 트래픽 - 신뢰 영역 내의 들어오는 연결의 예로는 신뢰 영역 내의 원격 장치가 컴퓨터에서 실행되는 로컬 애플리케이션과 통신하려는 시도를 들 수 있습니다.

신뢰 영역으로 나가는 트래픽 - 예로는 로컬 애플리케이션이 로컬 네트워크 내의 다른 장치 또는 신뢰 영역에 있는 네트워크 내의 다른 장치와 연결을 설정하려는 시도를 들 수 있습니다.

들어오는 인터넷 트래픽 - 예로는 원격 장치가 컴퓨터에서 실행되는 애플리케이션과 통신하려는 시도를 들 수 있습니다.

나가는 인터넷 트래픽 - 예로는 로컬 애플리케이션이 다른 장치와 연결을 설정하려는 시도를 들 수 있습니다.

각 섹션에서 새로 생성된 규칙에 추가할 파라미터를 정의할 수 있습니다.

로컬 포트 추가 - 네트워크 통신의 로컬 포트 번호를 포함합니다. 나가는 통신의 경우에는 보통 임의의 번호가 생성됩니다. 따라서 이 옵션은 들어오는 통신에 대해서만 활성화하는 것이 좋습니다.

애플리케이션 추가 - 로컬 애플리케이션의 이름을 포함합니다. 이 옵션은 향후의 애플리케이션 수준 규칙(전체 애플리케이션의 통신을 정의하는 규칙)에 적합합니다. 예를 들어 웹 브라우저나 이메일 클라이언트에 대해서만 통신을 활성화할 수 있습니다.

원격 포트 추가 - 네트워크 통신의 원격 포트 번호를 포함합니다. 예를 들어 표준 포트 번호(HTTP - 80, POP3 - 110 등)와 연결된 특정 서비스를 허용하거나 거부할 수 있습니다.

원격 IP 주소/신뢰 영역 추가 - 원격 IP 주소 또는 영역을 로컬 시스템과 해당 원격 주소/영역 간의 모든 네트워크 연결을 정의하는 새 규칙의 파라미터로 사용할 수 있습니다. 이 옵션은 특정 장치 또는 네트워크 장치 그룹에 대해 동작을 정의하는 경우에 적합합니다.

애플리케이션의 서로 다른 최대 규칙 수 - 애플리케이션이 서로 다른 포트나 여러 IP 주소 등을 통해 통신하는 경우, 학습 모드의 방화벽에서 이 애플리케이션에 적절한 수의 규칙을 생성합니다. 이 옵션을 사용하면 한 애플리케이션에 생성할 수 있는 규칙의 수를 제한할 수 있습니다.

대화 상자 창 - 학습 모드 종료

학습 모드의 사용 기간이 경과되면 **대화** 또는 **정책 기반** 필터링 모드로 전환하라는 메시지가 표시됩니다. 방화벽이 학습 모드이면 사용자 개입 없이 새 규칙이 생성됩니다.

각 필터링 모드에 대한 자세한 내용은 필터링 모드를 참조하십시오.

규칙 편집 열기를 클릭하여 학습 모드에서 생성된 규칙을 검토하는 것이 좋습니다.

방화벽 규칙

방화벽 규칙은 모든 네트워크 연결을 유의미하게 테스트하는 데 사용되는 조건 집합과 이러한 조건에 할당된 모든 동작을 나타냅니다. 방화벽 규칙을 사용하면 다양한 유형의 네트워크 연결이 설정될 때 수행할 동작을 정의할 수 있습니다.

규칙은 위에서 아래 순서로 평가되며, 첫 번째 열에서 우선순위를 확인할 수 있습니다. 일치하는 첫 번째 규

칙의 동작이 평가되는 각 네트워크 연결에 사용됩니다.

연결은 들어오는 연결과 나가는 연결로 구분할 수 있습니다. 들어오는 연결은 로컬 시스템과 연결하려고 시도하는 원격 장치에서 시작됩니다. 나가는 연결은 반대 방향으로 작동합니다. 즉, 로컬 시스템이 원격 장치에 연결합니다.

알 수 없는 새로운 통신이 검색되면 통신을 허용할지 또는 거부할지를 주의해서 고려해야 합니다. 원치 않거나 안전하지 않거나 알 수 없는 연결은 시스템에 보안 위험을 유발합니다. 이러한 연결이 설정된 경우에는 사용자의 컴퓨터에 연결하려고 시도하는 원격 장치와 애플리케이션에 주의를 기울이는 것이 좋습니다. 대부분의 침입은 개인적인 데이터를 획득하여 보내거나 호스트 워크스테이션으로 기타 악성 애플리케이션을 다운로드하려고 합니다. 방화벽을 사용하면 그러한 연결을 검출해 종료할 수 있습니다.

고급 설정 > **보호** > **네트워크 접근 보호** > **방화벽** > **규칙** > **편집**에서 방화벽 규칙을 보고 편집할 수 있습니다.

방화벽 규칙이 많은 경우 필터를 사용하여 특정 규칙만 표시할 수 있습니다. 방화벽 규칙을 필터링하려면 방화벽 규칙 목록 위에 있는**추가 필터**를 클릭합니다. 다음 기준에 따라 규칙을 필터링할 수 있습니다.

- 원본
- 방향
- 동작
- 사용 가능 여부

기본적으로 미리 정의된 방화벽 규칙은 숨겨져 있습니다. 미리 정의된 모든 규칙을 표시하려면 **기본 제공(미리 정의된) 규칙 숨기기** 옆의 토글을 비활성화합니다. 미리 정의된 규칙을 비활성화할 수 있지만 삭제할 수는 없습니다.

오른쪽 위에 있는 검색 아이콘을 클릭하여 규칙을 검색할 수 있습니다.

열

우선순위 - 규칙은 위에서 아래 순서로 평가되며, 첫 번째 열에서 우선순위를 확인할 수 있습니다.

활성화됨 - 규칙의 활성화 또는 비활성화 여부를 표시합니다. 규칙을 활성화하려면 해당 확인란을 선택해야 합니다.

애플리케이션 - 규칙이 적용되는 애플리케이션입니다.

방향 - 통신 방향입니다(들어오는/나가는/둘 다).

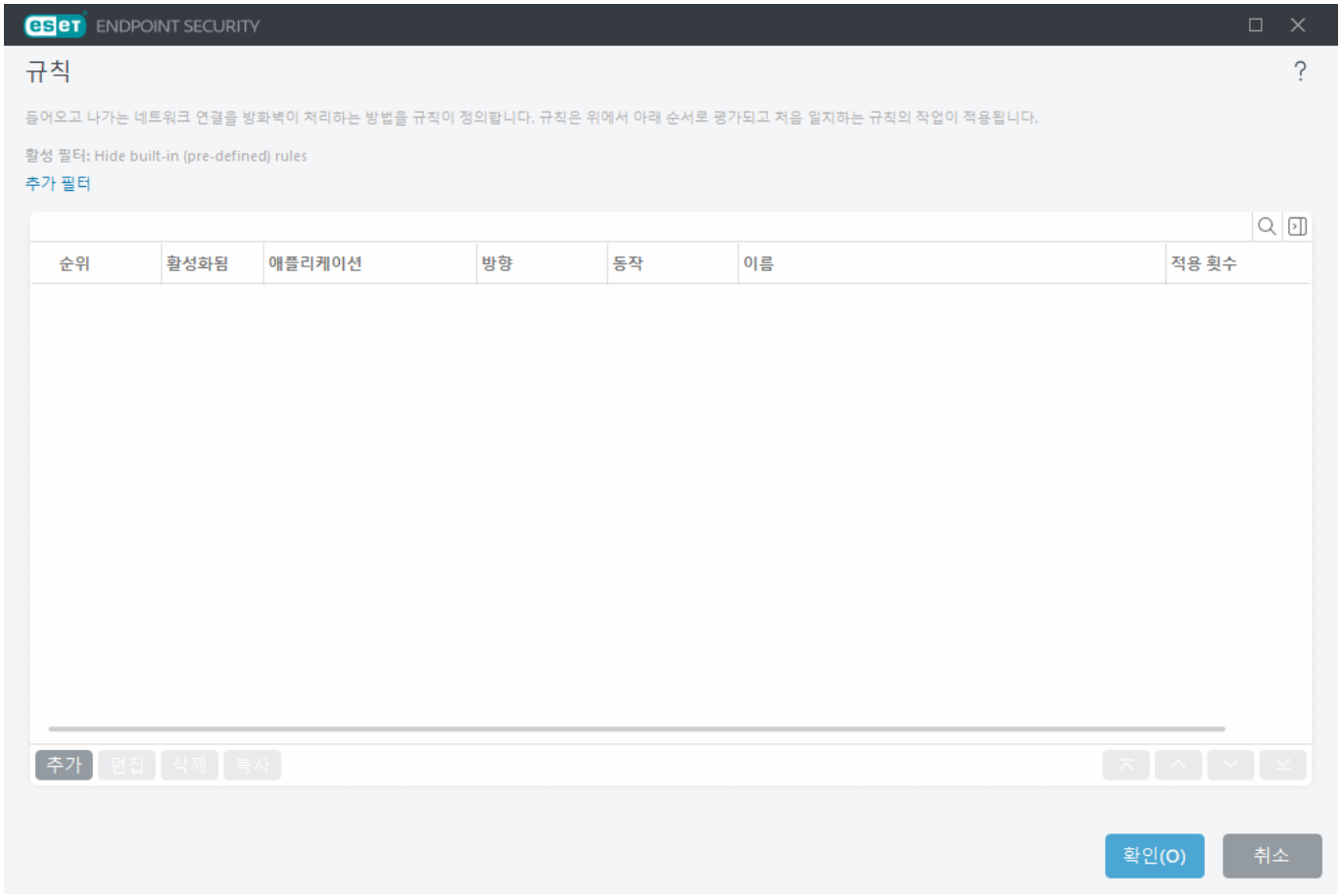
동작 - 통신 상태를 표시합니다(차단/허용/확인).

이름 - 규칙의 이름입니다. ESET 아이콘은 미리 정의된 규칙을 나타냅니다.

적용 횟수 - 규칙이 적용된 총 횟수입니다.

확장 아이콘을 클릭하여 규칙 상세 정보를 표시합니다.

표 머리글을 마우스 오른쪽 버튼으로 클릭하여 표시할 열을 선택할 수 있습니다.



제어 요소

추가 - 새 규칙을 생성합니다.

편집 - 기존 규칙을 수정합니다.

제거 – 기존 규칙을 제거합니다.

복사 - 선택한 규칙의 복사본을 생성합니다.

맨 위로/위로/아래로/맨 아래로 - 규칙의 우선 순위 수준을 조정할 수 있습니다(규칙은 위에서 아래로 실행됨).

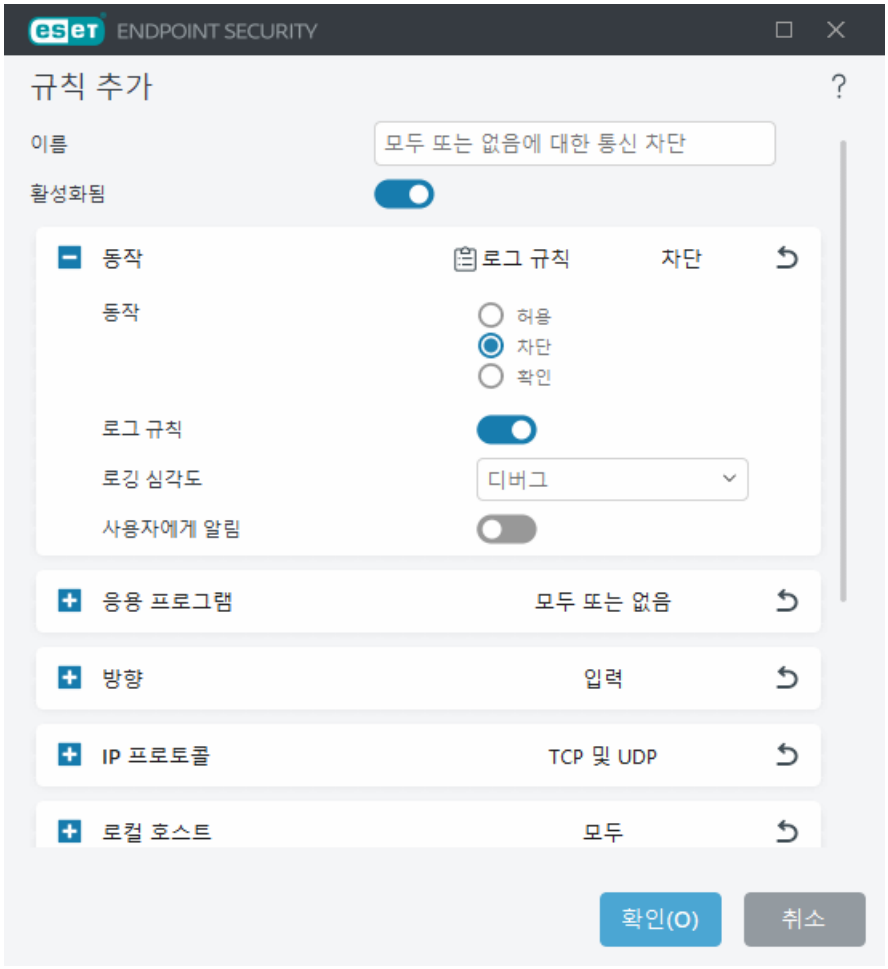
방화벽 규칙 추가 또는 편집

방화벽 규칙은 모든 네트워크 연결을 유의미하게 테스트하는 데 사용되는 조건과 이러한 조건에 할당된 동작을 나타냅니다. 규칙의 영향을 받는 애플리케이션의 올바른 작동을 보장하기 위해 네트워크 설정이 변경될 때(예: 원격 측의 네트워크 주소 또는 포트 번호가 변경된 경우) 방화벽 규칙을 편집하거나 추가해야 할 수 있습니다. 숙련된 사용자는 사용자 지정 방화벽 규칙을 생성해야 합니다.

다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- ESET Endpoint Security에서 방화벽 규칙 생성 또는 편집
- ESET PROTECT에서 클라이언트 워크스테이션에 대한 방화벽 규칙 생성 또는 편집

방화벽 규칙을 추가하거나 편집하려면 고급 설정 > **보호** > **네트워크 접근 보호** > **방화벽** > **규칙** > **편집**을 엽

니다. 방화벽 규칙 창에서 **추가** 또는 **편집**을 클릭합니다.



이름 - 규칙의 이름을 입력합니다.

활성화됨 - 규칙을 활성화하려면 토글을 클릭합니다.

방화벽 규칙에 대한 동작과 조건을 추가합니다.

동작

동작 - 이 규칙에 정의된 조건과 일치하는 통신을 **허용/차단**할 것인지, ESET Endpoint Security에서 통신이 연결될 때마다 **확인**할 것인지 선택합니다.
로그 규칙 - 규칙이 적용되면 로그 파일에 기록됩니다.
로깅 심각도 - 이 규칙에 대한 로그 기록의 심각도를 선택합니다.
사용자에게 알림은 규칙이 적용될 때 알림을 표시합니다.

응용 프로그램

이 규칙을 적용할 애플리케이션을 지정합니다.
애플리케이션 경로 - **...** 기호를 클릭하여 애플리케이션으로 이동하거나 애플리케이션의 전체 경로(예: C:\Program Files\Firefox\Firefox.exe)를 입력합니다. 애플리케이션의 이름만 입력해서는 안 됩니다.
애플리케이션 시그니처 - 시그니처(게시자의 이름)를 기준으로 애플리케이션에 규칙을 적용할 수 있습니다. **유효한 모든 시그니처**가 있는 애플리케이션 또는 **특정 지문 생성자가 지문을 생성한** 애플리케이션에 규칙을 적용하려면 드롭다운 메뉴에서 선택합니다. **특정 지문 생성자가 지문을 생성한** 애플리케이션을 선택하는 경우 **지문 생성자 이름** 필드에서 지문 생성자를 정의해야 합니다.
Microsoft Store 애플리케이션 - Microsoft Store에서 설치한 애플리케이션을 드롭다운 메뉴에서 선택합니다.
서비스 - 애플리케이션 대신 시스템 서비스를 선택할 수 있습니다. 드롭다운 메뉴를 열어 서비스를 선택합니다.
하위 프로세스에 적용 - 일부 애플리케이션은 하나의 애플리케이션 창만 표시되는 동안 더 많은 프로세스를 실행할 수 있습니다. 이 토글을 활성화하면 지정된 애플리케이션의 모든 프로세스에 규칙이 적용됩니다.

방향

이 규칙을 적용할 통신 **방향**을 선택합니다.
- **양방향** - 들어오는 통신/나가는 통신
- **인** - 들어오는 통신만
- **아웃** - 나가는 통신만

IP 프로토콜

이 규칙을 특정 프로토콜에만 적용하려면 드롭다운 메뉴에서 **프로토콜**을 선택합니다.

로컬 호스트

이 규칙을 적용할 로컬 주소, 주소 범위 또는 서브넷입니다. 지정된 주소가 없으면 규칙이 로컬 호스트와 주고받는 모든 통신에 적용됩니다. IP 주소, 주소 범위 또는 서브넷을 **IP** 텍스트 필드에 직접 추가하거나, **IP 집합** 옆의 **편집**을 클릭하여 기존 IP 집합에서 선택할 수 있습니다.

로컬 포트

로컬 **포트** 번호. 번호를 입력하지 않으면 모든 포트에 규칙이 적용됩니다. 단일 통신 포트 또는 통신 포트 범위를 추가할 수 있습니다.

원격 호스트

이 규칙을 적용할 원격 주소, 주소 범위 또는 서브넷입니다. 지정된 주소가 없으면 원격 호스트와 주고받는 모든 통신에 규칙이 적용됩니다. IP 주소, 주소 범위 또는 서브넷을 **IP** 텍스트 필드에 직접 추가하거나, **IP 집합** 옆의 **편집**을 클릭하여 기존 IP 집합에서 선택할 수 있습니다.

원격 포트

원격 **포트** 번호. 번호를 입력하지 않으면 모든 포트에 규칙이 적용됩니다. 단일 통신 포트 또는 통신 포트 범위를 추가할 수 있습니다.

프로필

방화벽 규칙은 특정 네트워크 연결 프로필에 적용할 수 있습니다.
모두 - 사용된 프로필에 관계없이 규칙이 모든 네트워크 연결에 적용됩니다.
선택됨 - 선택한 프로필을 기준으로 규칙이 특정 네트워크 연결에 적용됩니다. 선택하려는 프로필 옆에 있는 확인란을 선택합니다.

Firefox 웹 브라우저 애플리케이션이 인터넷/로컬 네트워크 웹 사이트에 접근할 수 있도록 허용하는 새 규칙을 생성합니다.
1. **동작** 섹션에서 **동작** > **허용**을 선택합니다.
2. **애플리케이션** 섹션에서 웹 브라우저의 **애플리케이션 경로**(예: C:\Program Files\Firefox\Firefox.exe)를 지정합니다. 애플리케이션의 이름만 입력해서는 안 됩니다.
3. **방향** 섹션에서 **방향** > **아웃**을 선택합니다.
4. **IP 프로토콜** 섹션의 **프로토콜** 드롭다운 메뉴에서 **TCP 및 UDP**를 선택합니다.
5. **원격 포트** 섹션에서 **포트** 번호: *80,443*을 추가하여 표준 브라우징을 허용합니다.

미리 정의된 규칙은 제한된 방식으로 수정할 수 있습니다.

애플리케이션 수정 내용 검색

애플리케이션 수정 탐지 기능은 방화벽 규칙이 있는 수정된 애플리케이션에서 연결하려고 시도하는 경우 알림을 표시합니다. 애플리케이션 수정은 다른 애플리케이션에서 원래 애플리케이션을 다른 실행 파일과 일시적으로 또는 영구적으로 바꾸는 메커니즘입니다(방화벽 규칙의 오용으로부터 보호).

이 기능이 일반적으로 모든 애플리케이션에 대한 수정 내용을 검색하는 것은 아니라는 사실에 주의하십시오. 목표는 기존 방화벽 규칙을 오용하는 것을 방지하는 것이며, 특정 방화벽 규칙이 있는 애플리케이션만 모니터링됩니다.

애플리케이션 수정 내용 탐지를 편집하려면 고급 설정 > **속성** > **네트워크 접근 보호** > **방화벽** > **애플리케이션 수정 내용 탐지**를 엽니다.

애플리케이션 수정 내용 검색 활성화 - 이 옵션을 선택하면 프로그램이 애플리케이션 변경 내용(업데이트, 감염, 기타 수정 내용)을 모니터링합니다. 수정된 애플리케이션이 연결을 시도하면 방화벽에서 알림을 표시합니다.

지문이 있는(신뢰할 수 있는) 애플리케이션의 수정 허용 - 애플리케이션에 수정 전후 동일하고 유효한 디지털 지문이 있는 경우 알리지 않습니다.

탐지에서 제외된 애플리케이션 목록 – 이 창에서 알림 없이 수정이 허용되는 개별 애플리케이션을 추가하거나 제거할 수 있습니다.

탐지에서 제외된 애플리케이션 목록

ESET Endpoint Security의 방화벽은 규칙이 있는 애플리케이션에 대한 변경 내용을 검색합니다(애플리케이션 수정 내용 검색 참조).

그러나 일부 애플리케이션이 방화벽에 의해 검사되지 않도록 제외하려는 경우 해당 애플리케이션에 이 기능을 사용하지 않을 수 있습니다.

추가 – 수정 탐지에서 제외된 애플리케이션 목록에 추가할 애플리케이션을 선택할 수 있는 창을 엽니다. 방화벽 규칙이 있는 개방형 네트워크 통신으로 실행 중인 애플리케이션 목록에서 선택하거나, 특정 애플리케이션을 추가할 수 있습니다.

편집 – 수정 탐지에서 제외된 애플리케이션 목록에 있는 애플리케이션의 위치를 변경할 수 있는 창을 엽니다. 방화벽 규칙이 있는 개방형 네트워크 통신으로 실행 중인 애플리케이션 목록에서 선택하거나, 위치를 수동으로 변경할 수 있습니다.

제거 - 수정 내용 검색에서 제외되는 애플리케이션 목록에서 항목을 제거합니다.

네트워크 공격 보호(IDS)

네트워크 공격 보호(IDS)는 알려진 취약성에 대한 악용 탐지를 향상시킵니다. 용어집에서 네트워크 공격 보호에 대해 자세히 알아보십시오. 네트워크 공격 보호를 구성하려면 고급 설정 > **보호** > **네트워크 액세스 보호** > **네트워크 공격 보호(IDS)**를 엽니다.

네트워크 공격 보호(IDS) 활성화 – 네트워크 트래픽의 내용을 분석하고 네트워크 공격으로부터 보호합니다. 유해한 것으로 간주되는 모든 트래픽이 차단됩니다.

봇넷 보호 활성화 - 컴퓨터가 감염되고 봇이 통신하려고 할 때 일반적인 패턴을 기준으로 악성 명령과 제어 서버를 포함한 통신을 검출하고 차단합니다. 봇넷 보호에 대한 자세한 내용은 용어집을 참조하십시오.

IDS 규칙 - 이 옵션을 사용하여 컴퓨터에 해를 끼치는 데 사용될 수 있는 여러 가지 공격 및 익스플로이트 유형을 검출하기 위한 고급 필터링 옵션을 구성할 수 있습니다.

네트워크 보호로 감지되는 모든 중요한 이벤트는 로그 파일에 저장됩니다. 자세한 내용은네트워크 보호 로그를 참조하십시오.

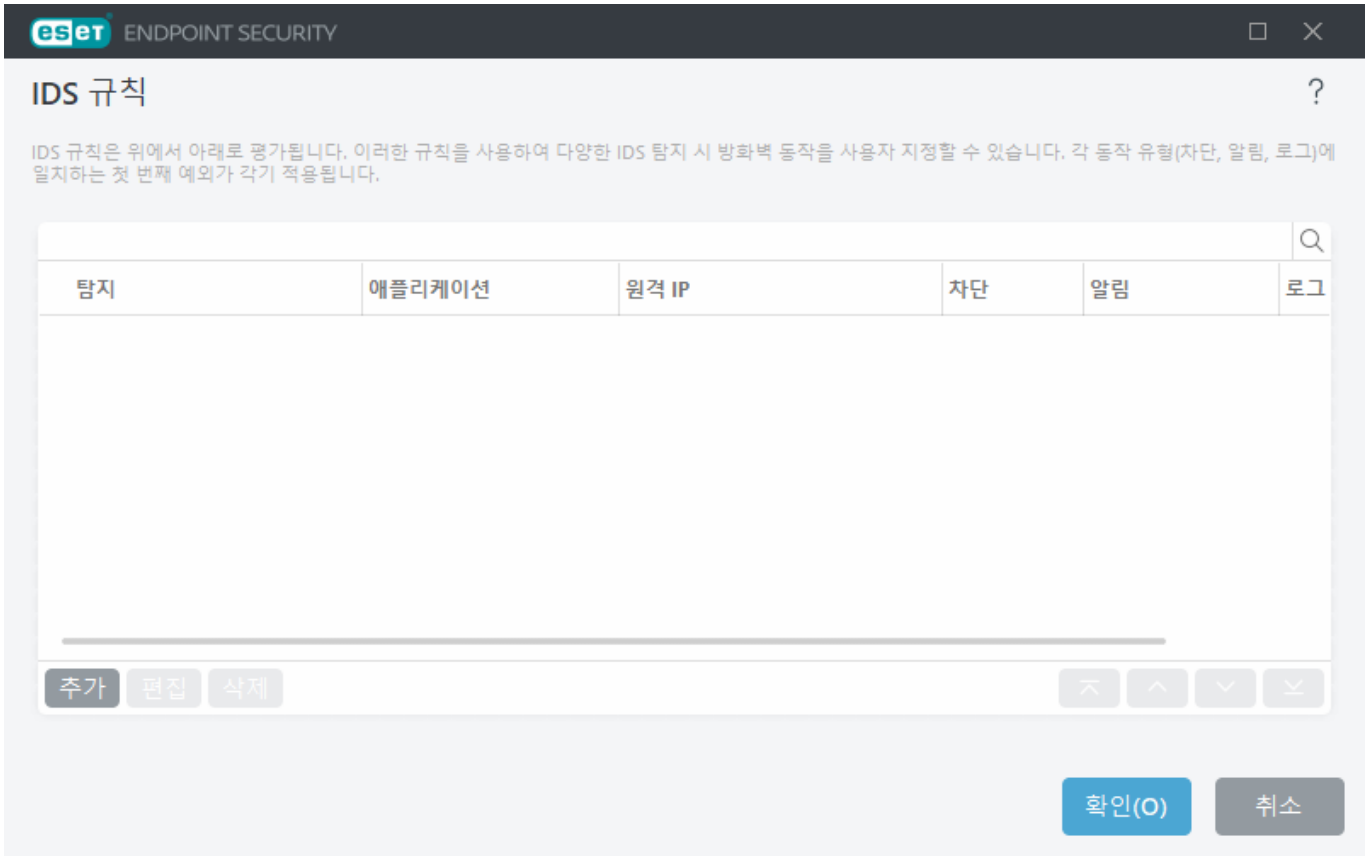
IDS 규칙

상황에 따라 IDS(침입 탐지 서비스)에서 라우터 또는 기타 내부 네트워킹 장치 간의 통신을 잠재적 공격으로 탐지할 수 있습니다. 예를 들면, 알려진 안전한 주소를 IDS에서 제외된 주소 영역에 추가하여 IDS를 우회할 수 있습니다.

다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- ESET Endpoint Security에서 클라이언트 워크스테이션에 대한 IDS 규칙 생성
- ESET PROTECT에서 클라이언트 워크스테이션에 대한 IDS 규칙 생성

IDS 규칙 관리

- **추가** - 새 IDS 규칙을 생성하려면 클릭합니다.
- **편집** - 기존 IDS 규칙을 편집하려면 클릭합니다.
- **제거** - IDS 규칙 목록에서 기존 규칙을 제거하려면 선택 및 클릭합니다.
-  **맨 위로/위로/아래로/맨 아래로** - 규칙의 우선 순위 수준을 조정할 수 있습니다(예외는 위에서 아래로 평가됨).



관리자가 ESET PROTECT 웹 콘솔에서 IDS 제외를 생성하면 탭 **제외가** 표시됩니다. IDS 제외에는 허용 규칙만 포함될 수 있으며 IDS 규칙보다 먼저 평가됩니다.

규칙 편집

탐지 – 탐지 유형.

위협 이름 - 사용 가능한 일부 탐지에 대해 위협 이름을 지정할 수 있습니다.

응용 프로그램 – ... 를 클릭하여 예외 애플리케이션의 파일 경로를 선택합니다(예: *C:\Program Files\Firefox\Firefox.exe*). 애플리케이션의 이름을 입력하지 마십시오.

원격 IP 주소 - 원격 IPv4 또는 IPv6 주소/범위/서브넷의 목록입니다. 여러 주소는 쉼표로 구분해야 합니다.

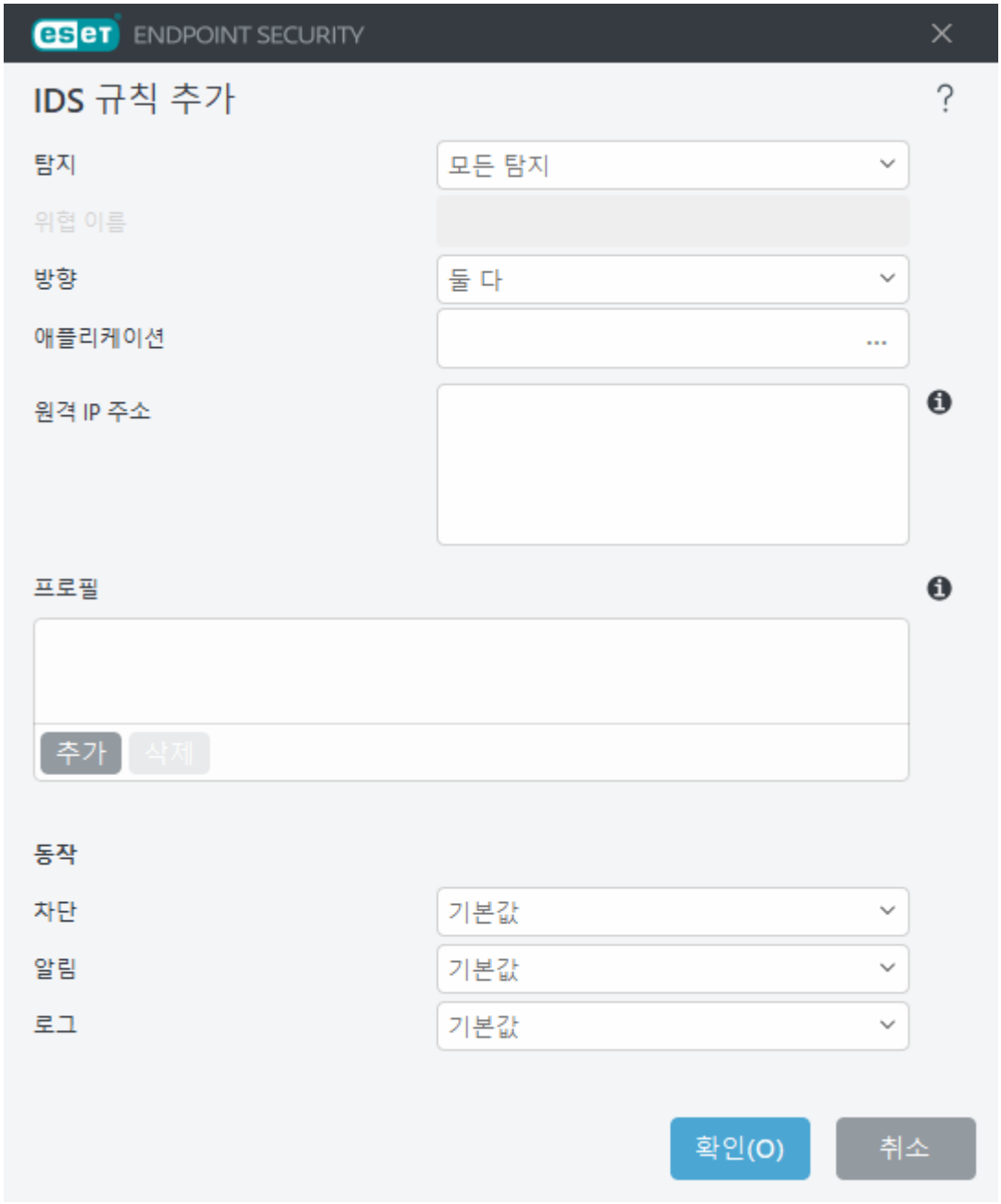
프로필 - 이 규칙을 적용할 네트워크 연결 프로필을 선택할 수 있습니다.

동작

차단 - 각 시스템 프로세스에는 고유한 기본 동작 및 할당된 동작(차단 또는 허용)이 있습니다. ESET Endpoint Security의 기본 동작을 재정의하려면 드롭다운 메뉴를 사용하여 해당 프로세스를 차단할지 아니면 허용할지 선택할 수 있습니다.

알림 – 컴퓨터에 바탕 화면 알림을 표시하려면 예를 선택합니다. 바탕 화면 알림을 원치 않을 경우아니요를 선택합니다. 사용 가능한 값은 기본값/예/아니요입니다.

로그 – 이벤트를 ESET Endpoint Security 로그 파일에 기록하려면 **예**를 선택합니다. 이벤트를 기록하지 않으려면 **아니요**를 선택합니다. 사용 가능한 값은 **기본값/예/아니요**입니다.



이벤트가 발생할 때마다 알림을 표시하고 로그를 수집하려는 경우:
1. **추가**를 클릭하여 새 IDS 규칙을 추가합니다.
2. **탐지** 드롭다운 메뉴에서 특정 경고를 선택합니다.
3. **...**를 클릭하고 알림을 적용하려는 애플리케이션의 파일 경로를 선택합니다.
4. **차단** 드롭다운 메뉴에서 **기본값**을 그대로 둡니다. 그러면 ESET Endpoint Security가 적용하는 기본 동작이 상속됩니다.
5. **알림** 및 **로그** 드롭다운 메뉴를 모두 **예**로 설정합니다.
6. **확인**을 클릭하여 이 알림을 저장합니다.

위협으로 간주되지 않는 특정 유형의 탐지에 대해 반복적 알림을 제거하려는 경우:
1. **추가**를 클릭하여 새 IDS 예외를 추가합니다.
2. **탐지** 드롭다운 메뉴에서 특정 경고(예: **보안 확장이 없는 SMB 세션** 또는 **TCP(Transmission Control Protocol) 포트 스캐닝 공격**)를 선택합니다.
3. 인바운드 통신에 적용되는 경우 방향 드롭다운 메뉴에서 **In**을 선택합니다.
4. **알림** 드롭다운 메뉴를 **아니요**로 설정합니다.
5. **로그** 드롭다운 메뉴를 **예**로 설정합니다.
6. **애플리케이션**을 공백으로 둡니다.
7. 통신이 특정 IP 주소로부터 들어오지 않는 경우 **원격 IP 주소**를 공백으로 둡니다.
8. **확인**을 클릭하여 이 알림을 저장합니다.

무차별 공격 보호

무차별 대입 공격 보호는 RDP/SMB 서비스에 대한 패스워드 추측 공격을 차단합니다. 무차별 대입 공격은 모든 문자, 숫자, 기호 조합을 체계적으로 시도하여 대상 패스워드를 알아내는 방법입니다. 무차별 공격 보호를 구성하려면 고급 설정 > **보호** > **네트워크 접근 보호** > **네트워크 공격 보호(IDS)** > **무차별 공격 보호**를 엽니다.

무차별 공격 보호 활성화 - ESET Endpoint Security에서 네트워크 트래픽의 내용을 검사하고 패스워드 추측 공격의 시도를 차단합니다.

규칙 – 들어오고 나가는 네트워크 연결 규칙을 생성, 편집하고 볼 수 있습니다. 자세한 내용은 규칙을 참조하십시오.

제외 – IP 주소 또는 애플리케이션 경로를 기준으로 정의된 제외 탐지 목록입니다. ESET PROTECT에서 제외를 생성 및 편집할 수 있습니다. 자세한 내용은 제외를 참조하십시오.

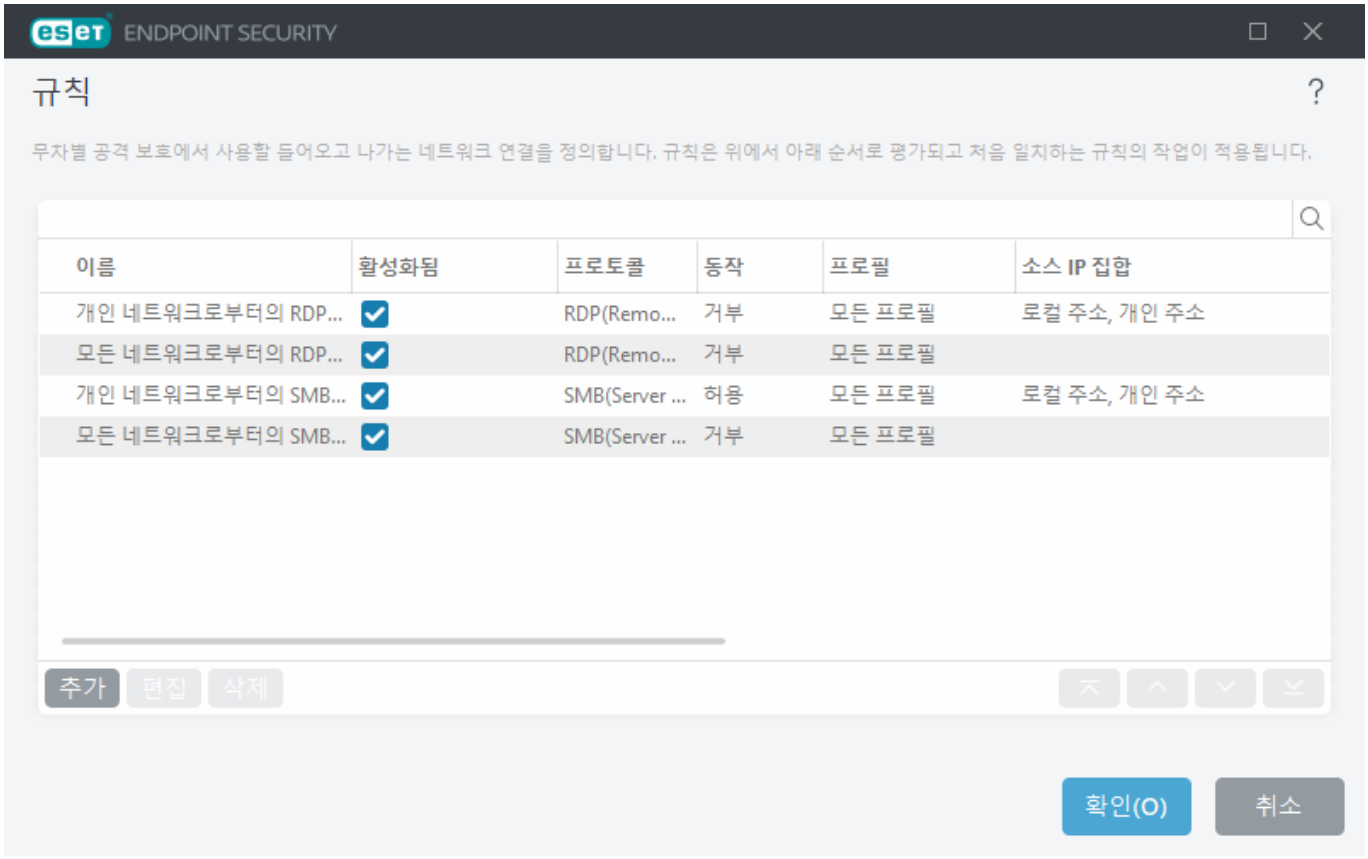
무차별 공격 보호에 대한 자세한 내용은 ESET Digital Security 설명서를 참조하십시오.

규칙

무차별 공격 보호 규칙을 사용하면, 들어오고 나가는 네트워크 연결에 적용할 규칙을 생성, 편집하고 볼 수 있습니다. 미리 정의된 규칙을 편집하거나 제거할 수는 없습니다.

무차별 공격 보호 규칙 관리

- **추가** - 새로운 무차별 공격 보호 규칙을 생성하려면 클릭합니다.
- **편집** - 기존 무차별 공격 보호 규칙을 편집하려면 클릭합니다.
- **제거** - IDS 규칙 목록에서 기존 예외를 제거하려면 선택 및 클릭합니다.
- **맨 위로/위로/아래로/맨 아래로** – 규칙의 우선 순위를 조정합니다.



가능한 가장 높은 보호를 보장하기 위해 여러 차단 규칙이 탐지 조건과 일치하는 경우 규칙이 규칙 목록에서 낮은 위치에 있더라도 **최대 시도** 값이 가장 낮은 차단 규칙이 적용됩니다.

규칙 편집

이름 - 규칙의 이름입니다.

활성화됨 - 목록에서 규칙을 유지하되 적용하지 않으려면 토글을 비활성화합니다.

동작 – 규칙 설정이 충족되면 연결을 **거부**할지, **허용**할지 선택합니다.

프로토콜 – 이 규칙이 검사하는 통신 프로토콜입니다.

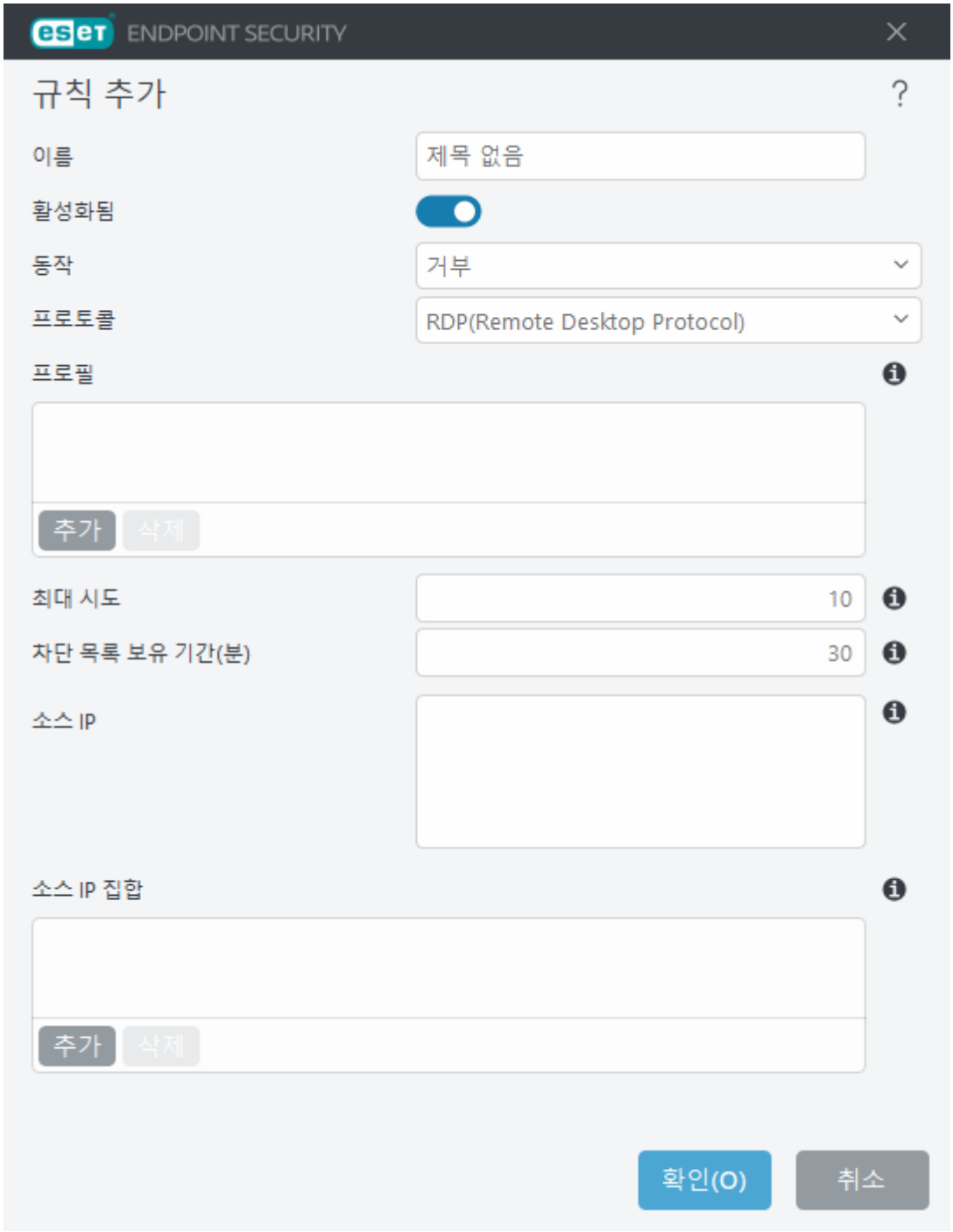
프로필 - 이 규칙을 적용할 네트워크 연결 프로필을 선택할 수 있습니다.

최대 시도 - IP 주소가 차단되고 차단 목록에 추가될 때까지 허용되는 최대 공격 반복 시도 수입니다.

차단 목록 보존 기간(최소) - 차단 목록에서 주소 만료 시간을 설정합니다.

소스 IP - IP 주소/범위/서브넷 목록입니다. 여러 주소는 쉼표로 구분해야 합니다.

소스 IP 집합 - IP 집합에 이미 정의한 IP 주소 집합입니다.



제외

무차별 제외를 사용하여 특정 기준에 대한 무차별 탐지를 억제할 수 있습니다. 이러한 제외는 무차별 탐지를 기반으로 ESET PROTECT에서 생성됩니다.

열

- **탐지** – 탐지 유형.
- **응용 프로그램** – ... 를 클릭하여 예외 애플리케이션의 파일 경로를 선택합니다(예: *C:\Program Files\Firefox\Firefox.exe*). 애플리케이션의 이름을 입력하지 마십시오.
- **원격 IP** - 원격 IPv4 또는 IPv6 주소/범위/서브넷의 목록입니다. 여러 주소는 쉼표로 구분해야 합니다.

제외 관리

관리자가 ESET PROTECT 웹 콘솔에서 무차별 제외를 생성하면 제외가 표시됩니다. 제외는 허용 규칙만 포함할 수 있으며 IDS 규칙보다 먼저 평가됩니다.

고급 옵션

고급 설정 > **보호** > **네트워크 접근 보호** > **네트워크 공격 보호(IDS)** > **고급 옵션**에서 컴퓨터를 손상시킬 수 있는 여러 유형의 공격 및 악용 탐지를 활성화하거나 비활성화할 수 있습니다.

차단된 통신에 대한 위협 알림을 수신하지 못하는 경우도 있습니다. 방화벽 로그에서 차단된 모든 통신을 보는 방법과 관련된 지침을 확인하려면 로그에서 규칙 또는 예외 로깅 및 생성 섹션을 참조하십시오.

이 창에서 특정 옵션의 사용 가능 여부는 ESET 제품 및 방화벽 모듈의 유형이나 버전 그리고 운영 체제 버전에 따라 다를 수 있습니다.

침입 검출

- **프로토콜 SMB** - SMB 프로토콜에서 다양한 보안 문제를 검출하고 차단합니다.
- **Rogue 서버 인증 시도 공격 검출** - 사용자 자격 증명을 얻기 위해 인증 시 Rogue 인증을 사용하는 공격으로부터 보호합니다.
- **명명된 파이프를 여는 동안 IDS 우회 검색** - SMB 프로토콜에서 MSRPCS 명명된 파이프를 여는 데 사용되는 알려진 우회 기술을 검색합니다.
- **CVE(일반적인 취약성 및 노출) 검출** - 다양한 공격, 양식, 보안 헛점 및 SMB 프로토콜을 통한 익스플로이트에 대해 구현된 검출 방법입니다. CVE 식별자에 대한 자세한 내용을 검색하고 보려면 CVE 웹 사이트(cve.mitre.org)를 참조하십시오.
- **프로토콜 RPC** - DCE(Distributed Computing Environment)용으로 개발된 원격 프로시저 호출 시스템에서 다양한 CVE를 검출하고 차단합니다.
- **프로토콜 RDP** - RDP 프로토콜에서 다양한 CVE를 검출하고 차단합니다(위 참조).
- **ARP 악성 공격 검출** - "메시지 가로채기" 공격으로 트리거되는 ARP 악성 공격이나 네트워크 스위치의 스니핑을 검출합니다. ARP (주소 해석 프로토콜)은 네트워크 애플리케이션이나 장치가 이더넷 주소를 확인하는 데 사용됩니다.
- **TCP/UDP 포트 검사 공격 검출** - 활성 포트를 찾고 서비스 취약점을 악용하려는 목적으로 다양한 포트 주소에 클라이언트 요청을 보내 열린 포트에 대한 호스트를 조사하도록 고안된 애플리케이션인 포트 검사 소프트웨어의 공격을 검출합니다. 이러한 공격 유형에 대한 자세한 내용은 용어집을 참조하십시오.
- **공격 검출 후 안전하지 않은 주소 차단** - 공격의 근원지로 검출된 IP 주소는 특정 기간 동안 연결하지 못하도록 차단 목록에 추가됩니다. 공격 탐지 후 주소가 차단되는 기간을 설정하는 **차단 목록 보존 기간**을 정의할 수 있습니다.
- **공격 탐지에 대해 알림** – 화면 오른쪽 하단에 있는 Windows 알림 영역의 알림을 켭니다.
- **보안 허점을 통해 들어오는 공격도 알림 표시** - 보안 허점을 통한 공격이 감지되었거나 이러한 방식으로 위협이 시스템에 침투하려는 경우 경고합니다.

패킷 검사

- **SMB 프로토콜에서 관리자 공유에 대해 들어오는 연결 허용** - 관리 공유는 시스템의 하드 드라이브 파티션(*C$*, *D$* 등)을 시스템 폴더(*ADMIN$*)와 공유하는 기본 네트워크 공유입니다. 관리 공유에 대한 연결을 비활성화하면 많은 보안 위험이 줄어듭니다. 예를 들어 Conficker 웜은 관리 공유에 연결하기 위해 사전 공격을 수행합니다.

- **이전(지원되지 않는) SMB 언어 거부** - IDS에서 지원하지 않는 이전 SMB 언어를 사용하는 SMB 세션을 거부합니다. 최신 Windows 운영 체제는 Windows 95와 같은 이전 운영 체제와의 호환성 문제 때문에 이전 SMB 언어를 지원합니다. 공격자는 트래픽 조사를 회피하기 위해 SMB 세션에 이전 언어를 사용할 수 있습니다. 컴퓨터가 이전 버전의 Windows를 사용하는 컴퓨터와 파일을 공유(또는 일반적으로 SMB 통신을 사용)할 필요가 없으면 이전 SMB 언어를 거부하십시오.
- **확장된 보안이 없는 SMB 세션 거부** - LM(LAN Manager) Challenge/Response 인증보다 안전한 인증 메커니즘을 제공하기 위해 SMB 세션 협상 중에 확장된 보안이 사용될 수 있습니다. LM 체계는 약한 것으로 간주되므로 사용하지 않는 것이 좋습니다.
- **신뢰 영역 외부에 있는 서버에 대해 SMB 프로토콜에서 실행 파일 열기 거부** - 방화벽의 신뢰 영역에 속해 있지 않은 서버의 공유 폴더에서 실행 파일(.exe, .dll, .. 신뢰할 수 있는 소스의 실행 파일을 복사하는 것은 적법할 수 있지만, 이 검출에서는 악의적인 서버에 있는 파일을 원치 않는 방식으로 열 때(예: 공유 악성 실행 파일의 하이퍼링크를 클릭하여 파일이 열림) 발생하는 위험을 완화해야 합니다.
- **신뢰 영역에서 서버 연결 시 SMB 프로토콜의 NTLM 인증 거부** - NTLM(두 버전 모두 해당) 인증 체계를 사용하는 프로토콜은 자격 증명 전달 공격(SMB 프로토콜의 경우 SMB 릴레이 공격으로 알려져 있음)을 받기 쉽습니다. 신뢰 영역 외부에 있는 서버의 NTLM 인증을 거부하면 신뢰 영역 밖에 있는 악의적인 서버에서 자격 증명을 전달하여 발생하는 위험이 줄어듭니다. 마찬가지로 신뢰 영역의 서버를 통한 NTLM 인증을 거부할 수 있습니다.

- **Security Account Manager 서비스와의 통신 허용** - 이 서비스에 대한 자세한 내용은 [MS-SAMR]을 참조하십시오.

- **Local Security Authority 서비스와의 통신 허용** - 이 서비스에 대한 자세한 내용은 [MS-LSAD] 및 [MS-LSAT]를 참조하십시오.

- **Remote Registry 서비스와의 통신 허용** - 이 서비스에 대한 자세한 내용은 [MS-RRP]를 참조하십시오.

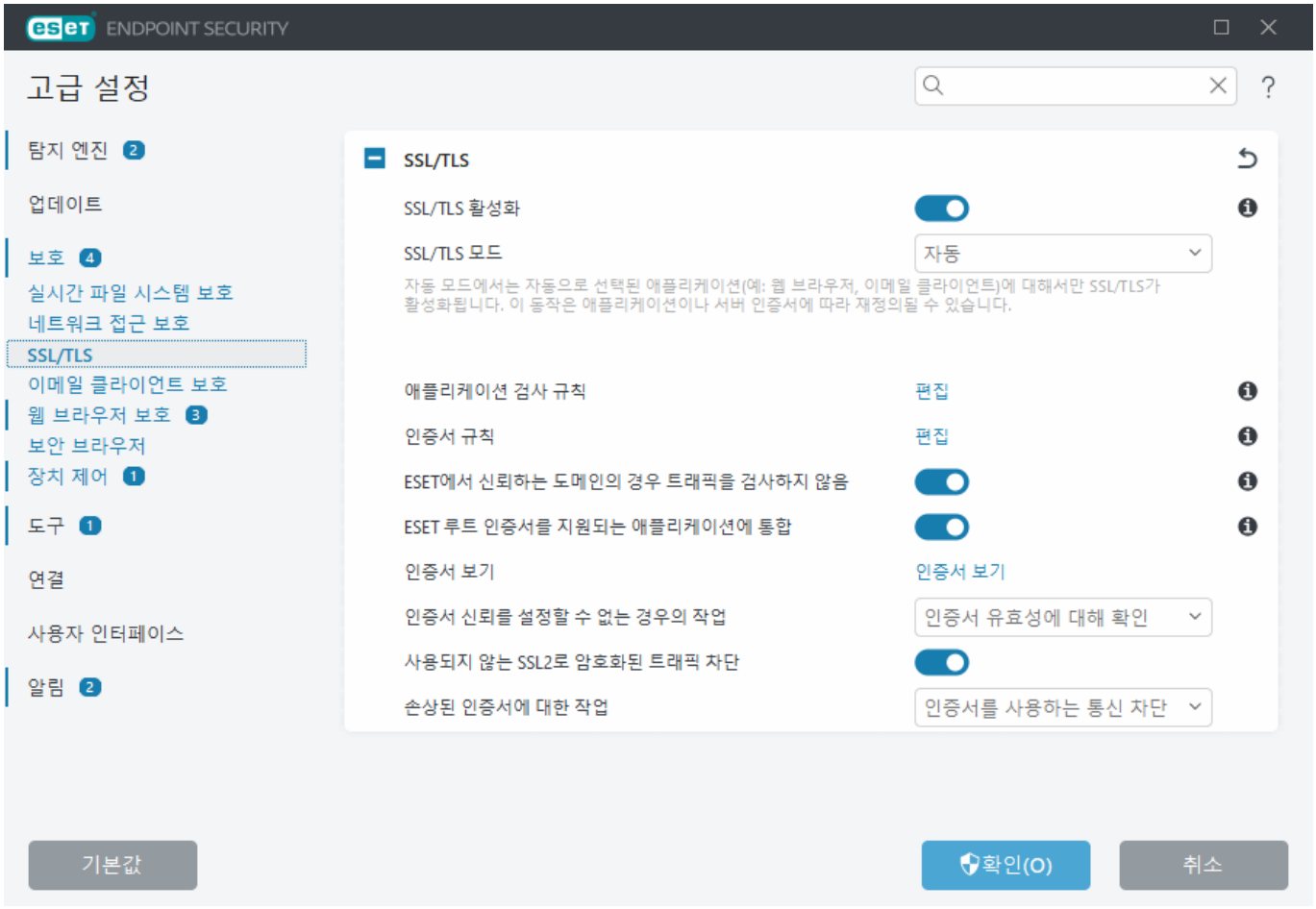
- **Service Control Manager 서비스와의 통신 허용** - 이 서비스에 대한 자세한 내용은 [MS-SCMR]을 참조하십시오.

- **Server 서비스와의 통신 허용** - 이 서비스에 대한 자세한 내용은 [MS-SRVS]를 참조하십시오.
- **기타 서비스와의 통신 허용** - MSRPC는 Microsoft에서 구현한 DCE RPC 메커니즘입니다. 더욱이 MSRPC에서는 전송(ncacn_np 전송)용 SMB(네트워크 파일 공유) 프로토콜로 이동되는 명명된 파이프를 사용할 수 있습니다. MSRPC 서비스는 Windows 시스템을 원격으로 접근 및 관리하기 위한 인터페이스를 제공합니다. Windows MSRPC 시스템에서는 몇 가지 보안 취약점(Conficker 웜, Sasser 웜 등)이 검색되고 악용되었습니다. 많은 보안 위험(예: 원격 코드 실행 또는 서비스 실패 공격)을 줄이려면 제공할 필요가 없는 MSRPC 서비스와의 통신 기능은 비활성화하십시오.

SSL/TLS

ESET Endpoint Security에서 SSL 프로토콜을 사용하는 통신 위협을 확인할 수 있습니다. 다양한 필터링 모드를 사용하여 신뢰할 수 있는 인증서, 알 수 없는 인증서 또는 SSL로 보호된 통신 검사에서 제외된 인증서를 통해 SSL로 보호된 통신을 검사할 수 있습니다. SSL/TLS 설정을 편집하려면 고급 설정 > **보호** > **SSL/TLS**를 엽

니다.



SSL/TLS 활성화 - 비활성화된 경우 ESET Endpoint Security에서 SSL/TLS를 통한 통신을 검사하지 않습니다.

SSL/TLS 모드는 다음과 같은 옵션에서 사용할 수 있습니다.

필터링 모드	설명
자동	기본 모드는 웹 브라우저 및 이메일 클라이언트 등과 같은 해당 애플리케이션만 검사합니다. 통신이 검사되는 애플리케이션을 선택하여 이를 재정의할 수 있습니다.
대화형	알 수 없는 인증서를 사용하여 SSL로 보호된 새로운 사이트에 들어가면 동작 선택 대화 상자가 표시됩니다. 이 모드를 사용하면 검사에서 제외될 SSL 인증서/애플리케이션 목록을 생성할 수 있습니다.
정책 기반	검사에서 제외된 인증서로 보호되는 통신을 제외한 SSL로 보호된 모든 통신을 검사하려면 이 옵션을 선택합니다. 지문이 있는 알 수 없는 인증서를 사용하여 새 통신을 설정한 경우 이러한 사실에 대한 알림이 표시되지 않으며 통신이 자동으로 필터링됩니다. 사용자가 신뢰할 수 있다고 표시(신뢰할 수 있는 인증서 목록에 있음)한 신뢰할 수 없는 인증서로 서버에 접근하면 서버에 대한 통신이 허용되고 통신 채널의 콘텐츠가 필터링됩니다.

애플리케이션 검사 규칙 - 특정 애플리케이션에 대한 ESET Endpoint Security 동작을 사용자 지정할 수 있습니다.

인증서 규칙 - 특정 SSL 인증서에 대한 ESET Endpoint Security 동작을 사용자 지정할 수 있습니다.

ESET이 신뢰하는 도메인에서 트래픽 검사 안 함 - 활성화된 경우 신뢰할 수 있는 도메인과의 통신은 검사에서 제외됩니다. ESET에서 관리하는 기본 제공 허용 목록이 도메인의 신뢰성을 결정합니다.

지원되는 애플리케이션에 ESET 루트 인증서 통합 - SSL 통신이 브라우저/이메일 클라이언트에서 제대로 작동하려면, ESET 루트 인증서를 알려진 루트 인증서(게시자) 목록에 추가해야 합니다. 활성화하면 ESET Endpoint Security에서 ESET SSL Filter CA 인증서를 알려진 브라우저(예: Opera). 시스템 인증서 저장소를 사용하는 브라우저의 경우 인증서가 자동으로 추가됩니다. 예를 들어 Firefox는 시스템 인증서 저장소에서 루트 인증서를 신뢰하도록 자동으로 구성됩니다.

지원되지 않는 브라우저에 인증서를 적용하려면 **인증서 보기** > **상세 정보** > **파일에 복사**를 클릭하고 수동으로 인증서를 브라우저로 가져옵니다.

인증서 신뢰를 설정할 수 없는 경우의 동작 - 경우에 따라서는 TRCA(신뢰할 수 있는 루트 인증 기관) 저장소를 사용하여 웹 사이트 인증서를 확인할 수 없습니다(예: 만료된 인증서, 신뢰할 수 없는 인증서, 특정 도메인에 유효하지 않은 인증서 또는 구문 분석할 수 있지만 인증서에 올바르게 서명하지 않은 서명). 합법적인 웹 사이트는 항상 신뢰할 수 있는 인증서를 사용합니다. 인증서를 제공하지 않는 경우, 이는 곧 공격자가 통신을 복호화하거나 웹 사이트에 기술적인 문제가 있음을 의미할 수 있습니다.

인증서 유효성에 대해 확인을 선택(기본적으로 선택됨)한 경우 암호화된 통신이 설정되면 수행할 동작을 선택하라는 메시지가 표시됩니다. 인증서를 신뢰할 수 있음으로 표시할지, 제외됨으로 표시할지를 결정할 수 있는 동작 선택 대화 상자가 표시됩니다. 인증서가 TRCA 목록에 없는 경우 창이 빨간색으로 표시되고. TRCA 목록에 있는 경우에는 녹색으로 표시됩니다.

인증서를 사용하는 통신 차단을 선택하여 신뢰할 수 없는 인증서를 사용하는 사이트에 대해 암호화된 연결을 항상 종료할 수 있습니다.

사용되지 않는 SSL2로 암호화된 트래픽 차단 - 이전 버전의SSL 프로토콜을 사용하는 통신이 자동으로 차단됩니다.

손상된 인증서에 대한 동작 - 손상된 인증서란, 인증서가 ESET Endpoint Security에서 인식하지 못하는 형식을 사용하거나 손상된 상태로 수신(예: 임의의 데이터로 덮어쓴 경우)되었음을 의미합니다. 이 경우 **인증서를 사용하는 통신 차단**을 선택한 상태로 유지하는 것이 좋습니다. **인증서 유효성 확인**을 선택한 경우 사용자에게 암호화된 통신이 설정되면 수행할 동작을 선택하라는 메시지가 표시됩니다.

i 다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- ESET 제품의 인증서 알림
- 웹 페이지에 방문하면 "암호화된 네트워크 트래픽: 신뢰할 수 없는 인증서"가 표시됨

애플리케이션 검사 규칙

애플리케이션 검사 규칙을 사용하여 특정 애플리케이션에 대한 ESET Endpoint Security 동작을 사용자 지정하고 **SSL/TLS 모드**가 **대화 모드**일 때 선택한 동작을 저장할 수 있습니다. 이 목록은 고급 설정 > **보호** > **SSL/TLS** > **애플리케이션 검사 규칙** > **편집**에서 보고 편집할 수 있습니다.

애플리케이션 검사 규칙 창은 다음과 같이 구성됩니다.

열

애플리케이션 - 디렉터리 트리에서 실행 파일을 선택하고 **...** 옵션을 클릭하거나 수동으로 경로를 입력합니다.

검사 동작 - **검사**나 **무시**를 선택하여 통신을 검사하거나 무시합니다. 자동 모드에서 검사하고 대화 모드에

서 확인하려면 **자동**을 선택합니다. 항상 어떤 동작을 수행할지 사용자에게 확인하려면 **확인**을 선택합니다.

제어 요소

추가 - 필터링된 애플리케이션을 추가합니다.

편집 - 구성하려는 애플리케이션을 선택하고 **편집**을 클릭합니다.

제거 - 제거하려는 애플리케이션을 선택하고 **제거**를 클릭합니다.

가져오기/내보내기 - 파일에서 애플리케이션을 가져오거나 현재 애플리케이션 목록을 파일에 저장합니다.

확인/취소 - 변경 내용을 저장하려면 **확인**을 클릭하고, 저장하지 않고 종료하려면 **취소**를 클릭합니다.

인증서 규칙

인증서 규칙을 사용하여 특정 SSL 인증서에 대한 ESET Endpoint Security 동작을 사용자 지정하고 **SSL/TLS 모드**가 **대화 모드**일 때 선택한 동작을 저장할 수 있습니다. 이 목록은 고급 설정 > **보호** > **SSL/TLS** > **인증서 규칙** > **편집**에서 보고 편집할 수 있습니다.

인증서 규칙 창은 다음과 같이 구성됩니다.

열

이름 - 인증서의 이름입니다.

인증서 발급자 - 인증서 생성자의 이름입니다.

인증서 제목 - 제목 필드는 제목 공개 키 필드에 저장된 공개 키와 연결된 엔터티를 식별합니다.

접근 - 인증서의 신뢰성과 관계없이 이 인증서로 보호되는 통신을 허용/차단하기 위한 **접근 동작**으로 **허용** 또는 **차단**을 선택합니다. 신뢰할 수 있는 인증서를 허용하고 신뢰할 수 없는 인증서에 대해서는 확인하려면 **자동**을 선택합니다. 항상 어떤 동작을 수행할지 사용자에게 확인하려면 **확인**을 선택합니다.

검사 - 이 인증서로 보호되는 통신을 검사하거나 무시하기 위한 **검사 동작**으로 **검사** 또는 **무시**를 선택합니다. 자동 모드에서 검사하고 대화 모드에서 확인하려면 **자동**을 선택합니다. 항상 어떤 동작을 수행할지 사용자에게 확인하려면 **확인**을 선택합니다.

제어 요소

추가 - 새 인증서를 추가하고 접근 및 검사 옵션에 대한 해당 설정을 조정합니다.

편집 - 구성하려는 인증서를 선택하고 **편집**을 클릭합니다.

삭제 - 삭제하려는 인증서를 선택하고 **삭제**를 클릭합니다.

확인/취소 - 변경 내용을 저장하려면 **확인**을 클릭하고, 저장하지 않고 종료하려면 **취소**를 클릭합니다.

암호화된 네트워크 트래픽

시스템이 SSL/TLS 검사를 사용하도록 구성된 경우 다음과 같은 두 가지 상황에서 동작을 선택하라는 메시지를 표시하는 대화 상자 창이 나타납니다.

첫째, 웹 사이트에서 확인할 수 없거나 잘못된 인증서를 사용하는 경우 ESET Endpoint Security이(가) 이러한 경우에 사용자에게 확인(기본적으로 확인할 수 없는 인증서의 경우 "예", 잘못된 인증서의 경우 "아니요")하도록 구성되어 있으면, 연결을 **허용**할지 아니면 **차단**할지 확인하는 대화 상자가 표시됩니다. 인증서가 Trusted Root Certification Authorities store(TRCA)에 없으면 신뢰할 수 없는 인증서로 간주됩니다.

둘째, **SSL/TLS 모드**가 **대화 모드**로 설정된 경우 각 웹 사이트의 대화 상자에 트래픽을 **검사**할지, **무시**할지 묻는 메시지가 표시됩니다. 일부 애플리케이션에서는 SSL 트래픽이 다른 사용자에 의해 수정되거나 검사되지 않았는지 확인합니다. 이러한 경우 애플리케이션이 계속 작동되도록 하려면 ESET Endpoint Security이(가) 해당 트래픽을 **무시**해야 합니다.

> 예(그림 포함)
> 다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
> • ESET Windows 제품의 인증서 알림
> • 웹 페이지에 방문하면 "암호화된 네트워크 트래픽: 신뢰할 수 없는 인증서"가 표시됨

이러한 두 가지 경우에서 사용자는 선택한 동작을 저장하도록 선택할 수 있습니다. 저장된 동작은 인증서 규칙에 저장됩니다.

이메일 클라이언트 보호

이메일 클라이언트 보호를 구성하려면 고급 설정 > **보호** > **이메일 클라이언트 보호**를 열고 다음 구성 옵션 중에서 선택합니다.

- 메일 전송 보호
- 사서함 보호
- 주소 목록 관리
- ThreatSense

메일 전송 보호

IMAP(S) 및 POP3(S) 프로토콜은 이메일 클라이언트 애플리케이션에서 이메일 통신을 수신하는 데 가장 널리 사용되는 프로토콜입니다. IMAP(Internet Message Access Protocol)는 또 다른 이메일 검색용 인터넷 프로토콜입니다. IMAP는 POP3와 비교했을 때 여러 클라이언트가 동시에 동일한 사서함에 연결하여 메시지를 읽었는지, 회신했는지 또는 제거했는지 여부와 같은 메시지 상태 정보를 유지 관리할 수 있는 등의 장점이 있습니다. 이 제어 기능을 제공하는 보호 모듈은 시스템 시작 시 자동으로 시작된 후 메모리에서 활성화됩니다.

ESET Endpoint Security은(는) 사용된 이메일 클라이언트에 상관없이 이러한 프로토콜에 대한 보호 기능을 제공하며, 이메일 클라이언트를 다시 구성할 필요가 없습니다. 기본적으로 POP3 및 IMAP 프로토콜을 통한 모든 통신은 기본 POP3/IMAP 포트 번호에 상관없이 검사됩니다.
MAPI 프로토콜은 검사되지 않습니다. 그러나 Microsoft Exchange 서버와의 통신은 Microsoft Outlook 같은 이메일 클라이언트의 통합 모듈에 의해 검사될 수 있습니다.

ESET Endpoint Security에서는 암호화된 채널을 사용하여 서버와 클라이언트 간에 정보를 전송하는 IMAPS(585, 993) 및 POP3S(995) 프로토콜의 검사도 지원합니다. ESET Endpoint Security에서는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 프로토콜을 사용하여 통신을 검사합니다. 암호화된 통신은 기본적으로 검사됩니다. 검사기 설정을 보려면 고급 설정 > 보호 > **SSL/TLS**를 엽니다.

메일 전송 보호를 구성하려면 고급 설정 > **보호** > **이메일 클라이언트 보호** > **메일 전송 보호**를 엽니다.

메일 전송 보호 활성화 - 활성화된 경우 ESET Endpoint Security에서 메일 전송 통신을 검사합니다.

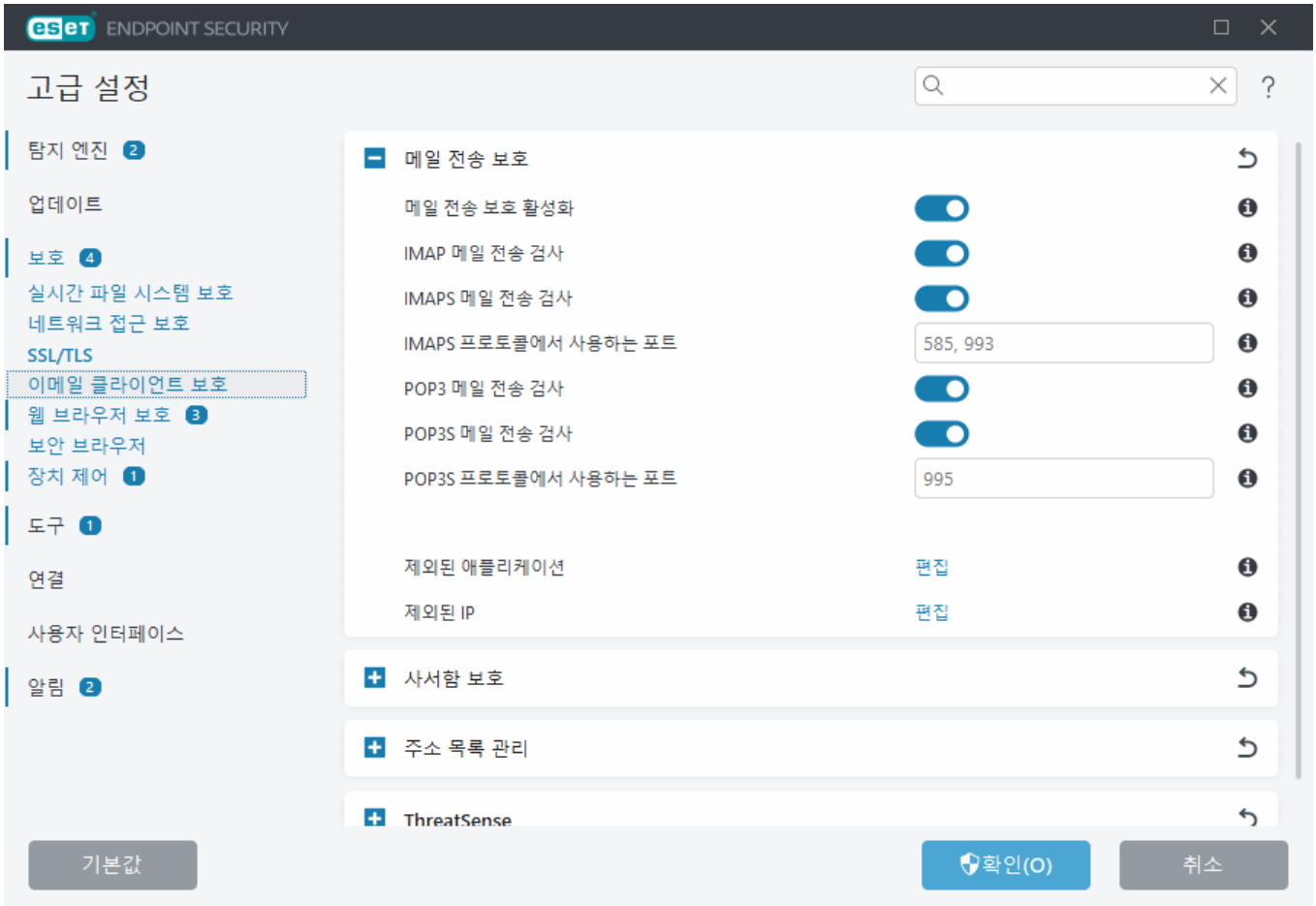
다음 옵션 옆에 있는 토글을 클릭하여 검사할 메일 전송 프로토콜을 선택할 수 있습니다(기본적으로 모든 프로토콜 검사가 활성화됨).

- **IMAP 메일 전송 검사**
- **IMAPS 메일 전송 검사**
- **POP3S 메일 전송 검사**
- **POP3S 메일 전송 검사**

기본적으로 ESET Endpoint Security은(는) 표준 포트에서 IMAPS 및 POP3S 통신을 검색합니다. IMAPS 및 POP3S 프로토콜에 대한 사용자 지정 포트를 추가하려면 **IMAPS 프로토콜에서 사용하는 포트** 또는 **POP3S 프로토콜에서 사용하는 포트** 옆의 텍스트 필드에 추가합니다. 여러 포트 번호는 쉼표로 구분해야 합니다.

제외된 애플리케이션 - 특정 애플리케이션을 메일 전송 보호에서 검사하지 않도록 제외할 수 있습니다. 웹 브라우저 보호로 인해 호환성 문제가 발생할 때 유용합니다.

제외된 IP - 특정 원격 주소를 메일 전송 보호에서 검사하지 않도록 제외할 수 있습니다. 웹 브라우저 보호로 인해 호환성 문제가 발생할 때 유용합니다.



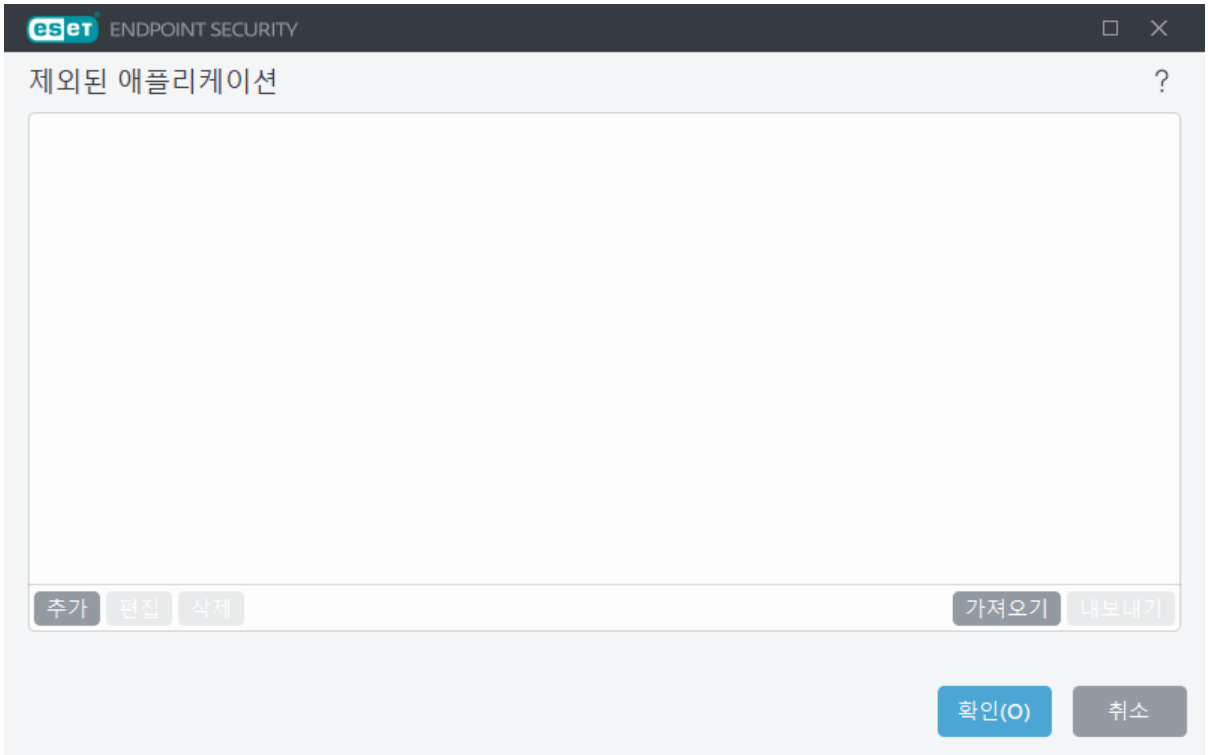
제외된 애플리케이션

특정 애플리케이션에 대한 통신 검사를 제외하려면 해당 애플리케이션을 목록에 추가합니다. 선택한 애플리케이션의 HTTP(S)/POP3(S)/IMAP(S) 통신은 위협에 대해 검사되지 않습니다. 이 옵션은 통신 검사 도중 제대로 작동하지 않는 애플리케이션에 대해서만 사용하는 것이 좋습니다.

실행 중인 애플리케이션과 서비스는 **추가**를 클릭하면 여기에서 자동으로 사용할 수 있습니다. **...**를 클릭하고 수동으로 제외를 추가할 애플리케이션으로 이동합니다.

편집 - 목록에서 선택한 항목을 편집합니다.

제거 - 목록에서 선택한 항목을 제거합니다.



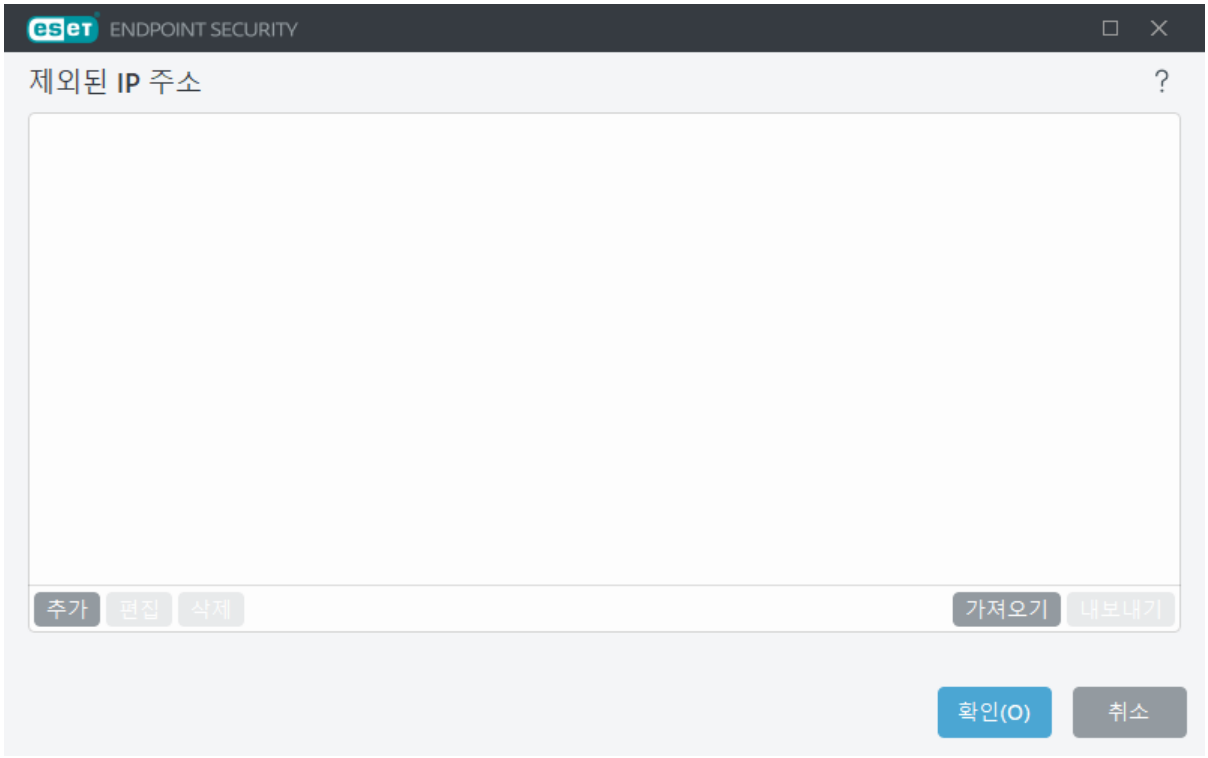
제외된 IP

목록의 항목은 검사에서 제외됩니다. 선택한 주소와의 HTTP(S)/POP3(S)/IMAP(S) 통신은 위협에 대해 검사되지 않습니다. 신뢰할 수 있는 것으로 알려진 주소에 한해서만 이 옵션을 사용하는 것이 좋습니다.

추가 - 규칙이 적용되는 원격 지점의 IP 주소/주소 범위/서브넷을 추가하려면 클릭합니다.

편집 - 목록에서 선택한 항목을 편집합니다.

제거 - 목록에서 선택한 항목을 제거합니다.



IP 주소 예제

IPv4 주소 추가:

단일 주소 - 개별 컴퓨터의 IP 주소(예: *192.168.0.10*)를 추가합니다.

주소 범위 - 시작 IP 주소와 끝 IP 주소를 입력하여 여러 컴퓨터의 IP 범위(예: *192.168.0.1~192.168.0.99*)를 지정합니다.

서브넷 - IP 주소 및 마스크에서 정의된 서브넷(컴퓨터 그룹)입니다. 예를 들어 255.255.255.0은 192.168.1.0 서브넷의 네트워크 마스크입니다. 전체 서브넷 유형을 제외하려면 *192.168.1.0/24*를 입력합니다.

IPv6 주소 추가:

단일 주소 - 개별 컴퓨터의 IP 주소(예: *2001:718:1c01:16:214:22ff:fec9:ca5*)를 추가합니다.

서브넷 - 서브넷(컴퓨터 그룹)은 IP 주소 및 마스크로 정의됩니다(예: *2002:c0a8:6301:1::1/64*).

사서함 보호

ESET Endpoint Security을(를) 사서함과 통합하면 이메일 메시지에서 악성 코드에 대한 활성 보호 수준이 높아집니다.

사서함 보호를 구성하려면 고급 설정 > **보호** > **이메일 클라이언트 보호** > **사서함 보호**를 엽니다.

클라이언트 플러그인으로 이메일 보호 활성화 – 비활성화된 경우 이메일 클라이언트 플러그인으로 보호 기능이 꺼집니다.

검사할 이메일 선택:

- **받은 이메일**
- **보낸 이메일**
- **읽은 이메일**
- **수정된 이메일**

클라이언트 플러그인으로 이메일 보호 활성화를 활성화된 상태로 유지하는 것이 좋습니다. 통합이 활성화되어 있지 않거나 작동하지 않는 경우에도 이메일 통신은 계속해서 메일 전송 보호(IMAP/IMAPS 및 POP3/POP3S)에 의해 보호됩니다.

스팸 검사

원치 않는 이메일, 즉 스팸은 전자 통신의 가장 큰 문제로 꼽힙니다. 스팸은 전체 이메일 통신의 50%를 차지합니다. 이메일 클라이언트 안티스팸은 이 문제를 방지하는 역할을 합니다. 몇 가지 이메일 보안 원칙이 결합된 이메일 클라이언트 안티스팸은 탁월한 필터링 기능을 제공하여 사서함을 정리된 상태로 유지해 줍니다. 스팸 탐지에서 한 가지 중요한 원칙은 미리 정의한 신뢰할 수 있는 주소(허용됨)와 스팸 주소(차단됨)를 토대로 원치 않는 이메일을 파악하는 것입니다.

스팸을 탐지하는 주요 방법은 이메일 메시지 속성 검사입니다. 즉, 받은 메시지를 기본 안티스팸 기준(메시지 정의, 통계 인공지능, 알고리즘 인식 및 기타 고유 방법)에 따라 검사한 다음 결과 색인 값을 사용해 메시지가 스팸인지 여부를 결정합니다.

이메일 클라이언트 안티스팸 활성화 - 활성화하면 수신된 메일에서 스팸이 있는지 검사합니다.

고급 스팸 검사기 사용 - 추가 안티스팸 데이터가 주기적으로 다운로드되어 안티스팸 기능을 향상시킴으로써 더 나은 결과를 얻을 수 있습니다.

스팸 점수 로깅 – ESET Endpoint Security 안티스팸 엔진은 검사한 모든 메시지에 스팸 점수를 지정합니다. 메시지는 안티스팸 보호 로그(기본 프로그램 창 > **도구** > **로그 파일** > **이메일 클라이언트 안티스팸**)에 기록됩니다.

- **없음** - 안티스팸 검사 점수가 기록되지 않습니다.
- **다시 분류되어 스팸으로 표시됨** - SPAM으로 지정된 메시지에 대한 스팸 점수를 기록하려면 이 옵션을 선택합니다.
- **모두** - 모든 메시지가 스팸 점수와 함께 로그에 기록됩니다.

정크 이메일 폴더에서 메시지를 클릭하고 **선택한 메시지를 스팸 아님으로 다시 분류**를 선택할 수 있으며 메시지가 받은 편지함으로 이동됩니다. 받은 편지함에서 스팸으로 간주되는 메시지를 클릭하고 **메시지를 스팸으로 다시 분류**를 선택하면 메시지가 받은 편지함으로 이동됩니다. 여러 메시지를 선택하고 해당 메시지에 동시 적용할 수 있습니다.

통합 - 사서함 보호를 이메일 클라이언트에 통합할 수 있습니다. 자세한 내용은 통합을 참조하십시오.

응답 - 스팸 메시지 처리를 사용자 지정할 수 있습니다. 자세한 내용은 응답을 참조하십시오.

통합

ESET Endpoint Security을(를) 이메일 클라이언트와 통합하면 이메일 메시지에서 악성 코드에 대한 활성 보호 수준이 높아집니다. 이메일 클라이언트가 지원되는 경우 ESET Endpoint Security에서 통합을 활성화할 수 있습니다. 이메일 클라이언트로 통합되면 ESET Endpoint Security 도구 모음이 이메일 클라이언트에 직접 삽입되어 이메일을 보다 효율적으로 보호할 수 있습니다. 통합 설정을 편집하려면 고급 설정 > **보호** > **이메일 클라이언트 보호** > **사서함 보호** > **통합**을 엽니다.

Microsoft Outlook으로 통합 - Microsoft Outlook이 현재 지원되는 유일한 이메일 클라이언트입니다. 이메일 보호는 플러그인으로 작동합니다. 플러그인의 주된 장점은 사용되는 프로토콜과 무관하다는 점입니다. 이메일 클라이언트는 암호화된 메시지를 받으면 메시지 암호를 해독해 바이러스 검사기로 보냅니다. 지원되는 Microsoft Outlook 버전의 전체 목록은 이 ESET 지식베이스 문서를 참조하십시오.

고급 이메일 클라이언트 처리 - 다음의 추가 Outlook Messaging API (MAPI) 이벤트, 즉 수정된 개체(`fnevObjectModified`)와 생성된 개체(`fnevObjectCreated`)를 처리합니다. 이메일 클라이언트를 사용하여 작업할 때 시스템이 느려지면 이 옵션을 비활성화 하십시오.

Microsoft Outlook 도구 모음

Microsoft Outlook 보호는 플러그인 모듈로 작동합니다. ESET Endpoint Security을(를) 설치하면 안티바이러스 보호 및 이메일 클라이언트 안티스팸 옵션이 포함된 이 도구 모음이 Microsoft Outlook에 추가됩니다.

스팸 - 선택한 메시지를 스팸으로 지정합니다. 지정하면 메시지의 "지문"이 스팸 지문을 저장하는 중앙 서버로 전송됩니다. 서버가 여러 사용자로부터 좀 더 유사한 "지문"을 받으면 이후에 해당 메시지가 스팸으로 분류됩니다.

스팸 아님 - 선택한 메시지를 스팸 아님으로 지정합니다.

스팸 주소(차단됨, 스팸 주소 목록) – 주소 목록에 새 보낸 사람 주소를 차단됨으로 추가합니다. 이 목록에 있는 주소로부터 받은 모든 메시지가 스팸으로 자동 분류됩니다.

> ⚠ 스푸핑 주의 - 이메일 메시지에서 보낸 사람의 주소를 위조해 이메일 받는 사람을 속여 이메일을 읽고 응답하도록 합니다.

신뢰할 수 있는 주소(허용됨, 신뢰할 수 있는 주소 목록) – 주소 목록에새 보낸 사람 주소를 허용됨으로 추가합니다. 허용된 주소에서 받은 모든 메시지는 자동으로 스팸으로 분류되지 않습니다.

ESET Endpoint Security – ESET Endpoint Security의 기본 창을 열려면 아이콘을 두 번 클릭합니다.

메시지 다시 검사 - 이메일 검사를 수동으로 실행할 수 있습니다. 검사할 메시지를 지정하고 받은 이메일을 다시 검사할 수 있는 기능을 활성화할 수 있습니다. 자세한 내용은 사서함 보호를 참조하십시오.

검사기 설정 - 사서함 보호 설정 옵션을 표시합니다.

안티스팸 설정 - 사서함 보호 설정 옵션을 표시합니다.

안티스팸 주소 목록 - 제외된 주소, 신뢰할 수 있는 주소, 스팸 주소의 목록에 접근할 수 있는 주소 목록 관리 창을 엽니다.

확인 대화 상자

이 알림은 실수 가능성을 없애기 위해 사용자가 선택한 동작을 수행할 것인지를 확인하는 역할을 합니다.

한편 이 대화 상자에는 확인을 비활성화하는 옵션도 있습니다.

메시지 다시 검사

이메일 클라이언트에 통합된 ESET Endpoint Security 도구 모음을 통해 다양한 이메일 검사 옵션을 지정할 수 있습니다. **메시지 다시 검사** 옵션은 다음과 같은 두 가지 검사 모드를 제공합니다.

현재 폴더의 모든 메시지 - 현재 표시된 폴더의 메시지를 검사합니다.

선택한 메시지만 - 사용자가 지정한 메시지만 검사합니다.

이미 검사한 메시지 다시 검사 확인란을 선택하면 이전에 검사한 메시지를 다시 검사할 수 있습니다.

응답

메시지 검사 결과에 따라 ESET Endpoint Security에서 검사한 메시지를 이동하거나 제목에 사용자 지정 텍스트를 추가할 수 있습니다. 고급 설정 > **보호** > **이메일 클라이언트 보호** > **사서함 보호** > **응답**에서 이러한 설정을 구성할 수 있습니다.

ESET Endpoint Security에서 이메일 클라이언트 안티스팸을 사용하면 다음과 같은 메시지 파라미터를 구성할 수 있습니다.

이메일 제목에 텍스트 추가 - 스팸으로 분류된 메시지의 제목 줄에 사용자 지정 접두어 문자열을 추가할 수 있습니다. 기본 **텍스트**는 "[SPAM]"입니다.

스팸 폴더로 이동 - 활성화된 경우 스팸 메시지가 기본 정크 이메일 폴더로 이동되고, 스팸 아님으로 다시 분류된 메시지가 사서함으로 이동됩니다. 이메일 메시지를 오른쪽 마우스 버튼으로 클릭하고 오른쪽 마우스 버튼 메뉴에서 ESET Endpoint Security을(를) 선택하면 표시되는 옵션에서 원하는 옵션을 선택할 수 있습니다.

사용자 지정 폴더로 이동 - 활성화된 경우 스팸 메시지가 아래에 지정된 폴더로 이동됩니다.

폴더 - 검출 시 감염된 이메일을 이동할 사용자 지정 폴더를 지정합니다.

탐지 항목이 포함된 메시지가 있는 경우 기본적으로 ESET Endpoint Security에서 메시지를 치료하려고 시도합니다. 메시지를 치료할 수 없는 경우 **치료할 수 없는 경우 수행할 동작**을 선택할 수 있습니다.

- **무시** - 이 옵션을 활성화하면 프로그램이 감염된 첨부 파일을 확인은 하지만 아무런 동작을 수행하지 않고 이메일을 그대로 둡니다.
- **이메일 삭제** - 프로그램에서 침입에 대해 사용자에게 알리고 메시지를 삭제합니다.
- **이메일을 지운 편지함 폴더로 이동** - 감염된 이메일을 자동으로 지운 편지함 폴더로 이동합니다.
- **이메일을 폴더로 이동**(기본 동작) – 감염된 이메일을 자동으로 지정된 폴더로 이동합니다.

폴더 - 검출 시 감염된 이메일을 이동할 사용자 지정 폴더를 지정합니다.

스팸 메시지를 읽은 것으로 지정 - 스팸 메시지를 읽은 것으로 자동 지정하려면 이 옵션을 활성화합니다. 그러면 사용자는 "감염되지 않은" 메시지만 확인할 수 있습니다.

다시 분류한 메시지를 읽지 않은 것으로 지정 - 원래 스팸으로 분류되었으나 나중에 "감염되지 않음"으로 지정된 메시지를 읽지 않은 것으로 표시합니다.

이메일을 검사한 후에 검사 결과가 포함된 알림을 메시지에 추가할 수 있습니다. **받아서 읽은 이메일에 태**

그 메시지 추가 또는 **보낸 이메일에 태그 메시지 추가**를 선택할 수 있습니다. 드문 경우이지만 태그 메시지가 문제 있는 HTML 메시지에서 누락되거나, 메시지가 악성코드에 의해 위조될 수 있습니다. 태그 메시지는 받아서 읽은 이메일이나 보낸 이메일 또는 둘 다에 추가할 수 있습니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **사용 안 함** - 태그 메시지를 추가하지 않습니다.
- **탐지가 발생하는 경우** – 악성 소프트웨어가 포함된 메시지만 검사한 상태로 표시됩니다(기본값).
- **검사한 경우 모든 이메일에** – 프로그램에서 검사한 모든 이메일에 메시지를 추가합니다.

받아서 읽은 이메일의 제목 업데이트/보낸 이메일의 제목 업데이트 - 아래에 지정된 사용자 지정 텍스트를 메시지에 추가하려면 이 옵션을 활성화합니다.

탐지된 이메일의 제목에 추가할 텍스트 - 감염된 이메일의 제목 접두어 형식을 수정하려면 이 템플릿을 편집합니다. 이 기능은 메시지 제목 "Hello"를 "[detection %DETECTIONNAME%] Hello" 형식으로 대체합니다. %DETECTIONNAME% 변수는 탐지 항목을 나타냅니다.

주소 목록 관리

ESET Endpoint Security의 이메일 클라이언트 안티스팸 기능을 사용하면 주소 목록에 다양한 파라미터를 구성할 수 있습니다. 주소 목록을 구성하려면 고급 설정 > **보호** > **이메일 클라이언트 보호** > **주소 목록 관리**를 엽니다.

사용자의 주소 목록 활성화 – 이 옵션을 활성화하여 사용자의 주소 목록을 활성화합니다.

사용자의 주소 목록 – 안티스팸 규칙을 정의하기 위해 주소를 추가, 편집, 제거할 수 있는 이메일 주소 목록입니다. 이 목록의 규칙은 현재 사용자에게 적용됩니다.

전체 주소 목록 활성화 – 이 장치의 모든 사용자가 공유하는 전체 주소 목록을 활성화하려면 이 옵션을 활성화합니다.

전체 주소 목록 – 안티스팸 규칙을 정의하기 위해 주소를 추가, 편집, 제거할 수 있는 이메일 주소 목록입니다. 이 목록의 규칙은 모든 사용자에게 적용됩니다.

자동으로 허용되어 사용자의 주소 목록에 추가

주소록의 주소를 신뢰할 수 있는 항목으로 처리 - 연락처 목록의 주소가 사용자의 주소 목록에 추가되지 않고 신뢰할 수 있는 항목으로 처리됩니다.

보내는 메시지의 받는 사람 주소 추가 – 메시지를 받는 사람 주소를 사용자의 주소 목록에 허용됨으로 추가합니다.

스팸 아님으로 다시 분류된 메시지의 주소 추가 – 스팸 아님으로 다시 분류된 메시지를 보낸 사람 주소를 사용자의 주소 목록에 허용됨으로 추가합니다.

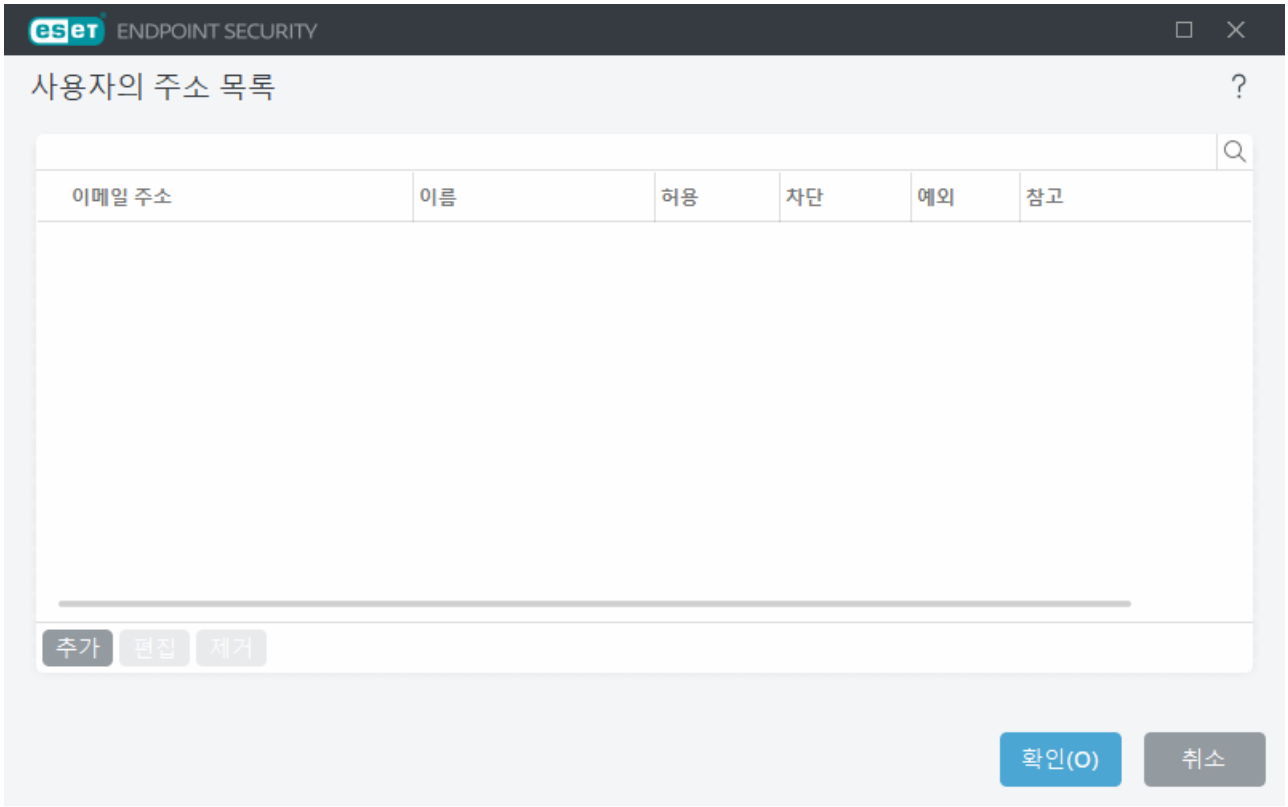
사용자의 주소 목록에 예외로 자동 추가

자신의 계정에서 주소 추가 – 기존 이메일 클라이언트 계정의 주소를 사용자의 주소 목록에 예외로 추가합니다.

주소 목록

원치 않는 이메일로부터 보호하기 위해 ESET Endpoint Security을(를) 사용하여 주소 목록에서 이메일 주소를 분류할 수 있습니다.

주소 목록을 편집하려면 고급 설정 > **보호** > **이메일 클라이언트 보호** > **주소 목록 관리**를 열고 **사용자의 주소 목록** 또는 **전체 주소 목록** 옆에 있는 **편집**을 클릭합니다.



열

이메일 주소 – 규칙이 적용될 주소입니다.

이름 – 사용자 지정 규칙 이름입니다.

허용/차단/예외 – 이메일 주소에 수행할 동작을 결정하는 데 사용되는 라디오 버튼입니다(동작을 빠르게 변경하려면 원하는 열의 라디오 버튼 클릭).

- **허용** - 안전한 것으로 간주되는 주소로, 사용자가 메시지를 수신할 주소입니다.
- **차단** - 안전하지 않거나 스팸으로 간주되고, 사용자가 메시지를 수신하지 않을 주소입니다.
- **예외** - 항상 스팸을 확인하는 주소로, 스푸핑되어 스팸 전송에 사용되고 있을 수 있는 주소입니다.

참고 – 규칙이 생성된 방법과 전체 도메인/하위 수준 도메인에 적용되는지 여부를 알려주는 정보입니다.

주소 관리

- **추가** – 새 주소에 규칙을 추가하려면 클릭합니다.
- **편집** – 기존 규칙을 편집하려면 선택 및 클릭합니다.
- **제거** – 주소 목록에서 규칙을 제거하려면 선택 및 클릭합니다.

주소 추가/편집

이 창에서 주소 목록 관리의 주소를 추가 또는 편집하고 수행할 동작을 구성할 수 있습니다.

이메일 주소 – 규칙이 적용될 주소입니다. 와일드카드는 지원되지 않습니다.

이름 – 사용자 지정 규칙 이름입니다.

동작 – 연락처의 이메일 주소가 **이메일 주소** 필드에 지정된 주소와 일치하는 경우 수행할 동작입니다.

- **허용** - 안전한 것으로 간주되는 주소로, 사용자가 메시지를 수신할 주소입니다.
- **차단** - 안전하지 않거나 스팸으로 간주되고, 사용자가 메시지를 수신하지 않을 주소입니다.
- **예외** - 항상 스팸을 확인하는 주소로, 스푸핑되어 스팸 전송에 사용되고 있을 수 있는 주소입니다.

전체 도메인 – 연락처의 전체 도메인(**이메일 주소** 필드에 지정된 주소뿐만 아니라 *address.info* 도메인의 모든 이메일 주소 포함)에 적용할 규칙의 경우 이 옵션을 선택합니다.

하위 수준 도메인 – 연락처의 하위 수준 도메인에 적용할 규칙의 경우 이 옵션을 선택합니다(*address.info*는 도메인을 나타내고, *my.address.info*는 하위 도메인을 나타냄).

주소 처리 결과

새 주소를 추가하거나 이메일 주소에 수행된 동작을 변경할 때 ESET Endpoint Security에서 알림 메시지를 표시합니다. 알림 메시지의 내용은 수행하려는 동작에 따라 다릅니다.

다음번에 메시지를 표시하지 않고 동작을 자동으로 수행하려면 **이 메시지를 다시 표시 안 함** 확인란을 선택합니다.

ThreatSense

ThreatSense는 복잡한 위협 검출 방법으로 구성되어 있습니다. 사전 예방 방식으로 검사를 수행합니다. 즉, 새로운 위협의 확산 초기에도 보호 기능을 제공합니다. 또한 함께 작동하여 시스템 보안 성능을 크게 향상시켜 주는 코드 분석, 코드 에뮬레이션, 일반 시그니처, 바이러스 시그니처 등의 방법을 조합해 사용합니다. 검사 엔진은 여러 데이터 스트림을 동시에 제어하여 효율성과 검출 비율을 최대화할 수 있습니다. ThreatSense 기술은 루트킷도 제거할 수 있습니다.

ThreatSense 엔진 설정 옵션을 사용하여 다음과 같은 여러 가지 검사 파라미터를 지정할 수 있습니다.

- 검사할 파일 형식 및 확장명
- 다양한 검출 방법의 조합
- 치료 수준 등

설정 창에 들어가려면 ThreatSense 기술을 사용하는 모듈(아래 참조)에 대한 고급 설정에서 **ThreatSense**을(를) 클릭합니다. 각 보안 시나리오에 따라 서로 다른 구성이 필요할 수 있습니다. 이를 염두에 두고, 다음 보호 모듈에 대해 ThreatSense를 개별적으로 구성할 수 있습니다.

- 실시간 파일 시스템 보호
- 유휴 상태 검사

- 시작 검사
- 문서 보호
- 이메일 클라이언트 보호
- 웹 브라우저 보호
- 컴퓨터 검사

ThreatSense 파라미터는 각 모듈에 맞게 고도로 최적화되어 있으므로 이를 수정하면 시스템 작동에 큰 영향을 줄 수 있습니다. 예를 들어 항상 런타임 패커를 검사하도록 파라미터를 변경하거나 실시간 파일 시스템 보호 모듈에서 고급 인공지능을 활성화하면 시스템 속도가 느려질 수 있습니다. 일반적으로 새로 생성된 파일에만 이러한 방법을 사용하여 검사합니다. 따라서 컴퓨터 검사를 제외한 모든 모듈에 대해서는 기본 ThreatSense 파라미터를 변경하지 않는 것이 좋습니다.

오브젝트 검사

이 섹션에서는 침입에 대해 검사할 컴퓨터 구성 요소 및 파일을 정의할 수 있습니다.

운영 메모리 - 시스템의 운영 메모리를 공격하는 위협이 있는지 검사합니다.

부트 영역/UEFI – 마트터 부트 레코드에 악성코드가 있는지 부트 영역을 검사합니다. UEFI에 대한 자세한 내용은 용어집을 참조하십시오.

이메일 파일 - 프로그램에서 지원되는 확장명은 DBX (Outlook Express) 및 EML입니다.

압축파일 – 프로그램에서 지원되는 확장명은 ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE 등입니다.

자체 압축 해제 파일 - 자체 압축 해제 파일(SFX)은 자체적으로 압축을 해제할 수 있는 파일입니다.

런타임 패커 - 런타임 패커는 표준 압축파일 형식과 달리 실행 후에 메모리에 압축이 풀립니다. 검사기는 표준 정적 패커(UPX, yoda, ASPack, FSG 등) 외에도 코드 에뮬레이션을 통해 몇 가지 추가 패커 유형을 인식할 수 있습니다.

검사 옵션

시스템에서 침입을 검사할 때 사용할 방법을 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.

인공지능 - 인공지능은 프로그램의 악의적 활동을 분석하는 알고리즘입니다. 이 기술의 가장 큰 장점은 이전 버전의 검색 엔진 생성 당시 존재하지 않았거나 해당 엔진에서 인식하지 못한 악성 소프트웨어를 식별할 수 있다는 것입니다. 그러나 악성이 아닌 소프트웨어를 악성으로 보고할 수 있다는 단점이 있습니다(가능성은 매우 낮음).

고급 휴리스틱/DNA 시그니처 - 고급 인공지능은 ESET에서 개발한 고유 인공지능 알고리즘으로, 컴퓨터 웜 및 트로이 목마 검출용으로 최적화되고 높은 수준의 프로그래밍 언어로 작성되었습니다. 고급 인공지능을 사용하면 ESET 제품의 위협 검출 기능이 크게 향상됩니다. 시그니처는 바이러스를 안정적으로 검출 및 식별할 수 있습니다. 자동 업데이트 시스템을 통해 위협 검출을 위해 새 시그니처를 몇 시간 이내에 사용할 수 있습니다. 그러나 시그니처는 인식 가능한 바이러스 또는 이러한 바이러스의 약간 수정된 버전만 검출할 수 있다는 단점이 있습니다.

치료

치료 설정에 따라 개체 치료 중 ESET Endpoint Security의 동작이 결정됩니다.

제외

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로. 파일의 형식과 내용을 정의합니다. 이 ThreatSense 설정 섹션에서는 검사할 파일 형식을 정의할 수 있습니다.

기타

수동 컴퓨터 검사에 대해 ThreatSense 엔진 설정을 구성할 때 **기타** 섹션에서 다음과 같은 옵션도 제공됩니다.

ADS(대체 데이터 스트림) 검사 - NTFS 파일 시스템에서 사용하는 대체 데이터 스트림은 일반 검사 기술로는 표시되지 않는 파일 및 폴더 연결입니다. 대체 데이터 스트림으로 가장하여 검출을 피하려고 하는 침입이 많이 있습니다.

순위가 낮은 백그라운드 검사 실행 - 각 검사 시퀀스는 일정량의 시스템 리소스를 사용합니다. 시스템 리소스에 대한 로드가 높은 프로그램을 사용하는 경우에는 순위가 낮은 백그라운드 검사를 활성화하여 리소스를 절약하고 이러한 절약된 리소스를 애플리케이션에 사용할 수 있습니다.

모든 개체 기록 – 검사 로그는 감염되지 않았더라도 자체 압축 해제 파일의 검사된 모든 파일을 표시합니다(이로 인해 검사 로그 데이터가 많이 생성되고 검사 로그 파일 크기가 커질 수 있음).

스마트 최적화 활성화 - 스마트 최적화를 활성화하면 가장 효율적인 검사 수준을 유지하는 동시에 최고 검사 속도를 유지하기 위한 최적의 설정이 사용됩니다. 다양한 보호 모듈이 다양한 검사 방법을 활용하고 해당 방법을 특정 파일 형식에 적용하는 방식으로 지능적 검사를 수행합니다. 스마트 최적화를 비활성화하면 검사를 수행할 때 특정 모듈의 ThreatSense 코어에서 사용자가 정의한 설정만 적용됩니다.

마지막 접근시의 타임스탬프 유지 - 검사한 파일의 원래 접근 시간을 데이터 백업 시스템 등에 사용할 수 있도록 업데이트하지 않고 그대로 유지하려면 이 옵션을 선택합니다.

제한

제한 섹션에서는 최대 개체 크기와 검사할 중복 압축 수준을 지정할 수 있습니다.

개체 설정

최대 개체 크기 - 검사할 개체의 최대 크기를 정의합니다. 그러면 지정된 안티바이러스 모듈에서 지정한 크기보다 작은 개체만 검사합니다. 큰 개체를 검사에서 제외해야 하는 특별한 이유가 있는 고급 사용자만 이 옵션을 변경해야 합니다. 기본값은 제한 없음입니다.

최대 개체 검사 시간(초) – 컨테이너 개체의 파일을 검사하기 위한 최대 시간 값(예: RAR/ZIP 압축파일 또는 첨부 파일이 여러 개 있는 이메일)을 정의합니다. 이 설정은 독립 실행형 파일에 적용되지 않습니다. 사용자 정의 값을 입력하고 해당 시간이 경과한 경우, 컨테이너 개체에서 각 파일 검사가 완료되었는지 여부에 관계없이 가능한 한 빨리 검사가 중지됩니다. 대용량 파일이 있는 압축파일의 경우, 압축파일에서 파일이 압축 해제되는 시간보다 더 빨리 검사가 중지되지는 않습니다(예: 사용자 정의 변수가 3초이지만 파일 압축 해제는 5초가 소요되는 경우). 압축파일의 나머지 파일은 해당 시간이 경과하면 검사되지 않습니다. 더 큰 압축파일 등의 검사 시간을 제한하려면 **최대 개체 크기**와 **압축파일 내 파일의 최대 크기**를 사용합니다(가능한

보안 위험으로 인해 권장되지 않음). 기본값은 제한 없음입니다.

압축파일 검사 설정

다중 압축 수준 - 최대 압축파일 검사 수준을 지정합니다. 기본값: 10.

압축파일 내 파일의 최대 크기 - 이 옵션을 사용하면 검사할 압축파일에 포함된 파일의 최대 파일 크기(압축 해제 시)를 지정할 수 있습니다. 최대값은 3GB입니다.

> 일반적인 상황에서는 기본값을 수정할 필요가 없으므로 기본값을 변경하지 않는 것이 좋습니다.

웹 브라우저 보호

웹 브라우저 보호를 사용하면 고급 인터넷 보호 모듈 설정을 구성할 수 있습니다. 다음 옵션은 고급 설정 > **보호 > 웹 브라우저 보호 > 웹 브라우저 보호**에서 사용할 수 있습니다.

웹 브라우저 보호 활성화 - 비활성화하면 웹 브라우저 보호 및 안티피싱 보호가 실행되지 않습니다.

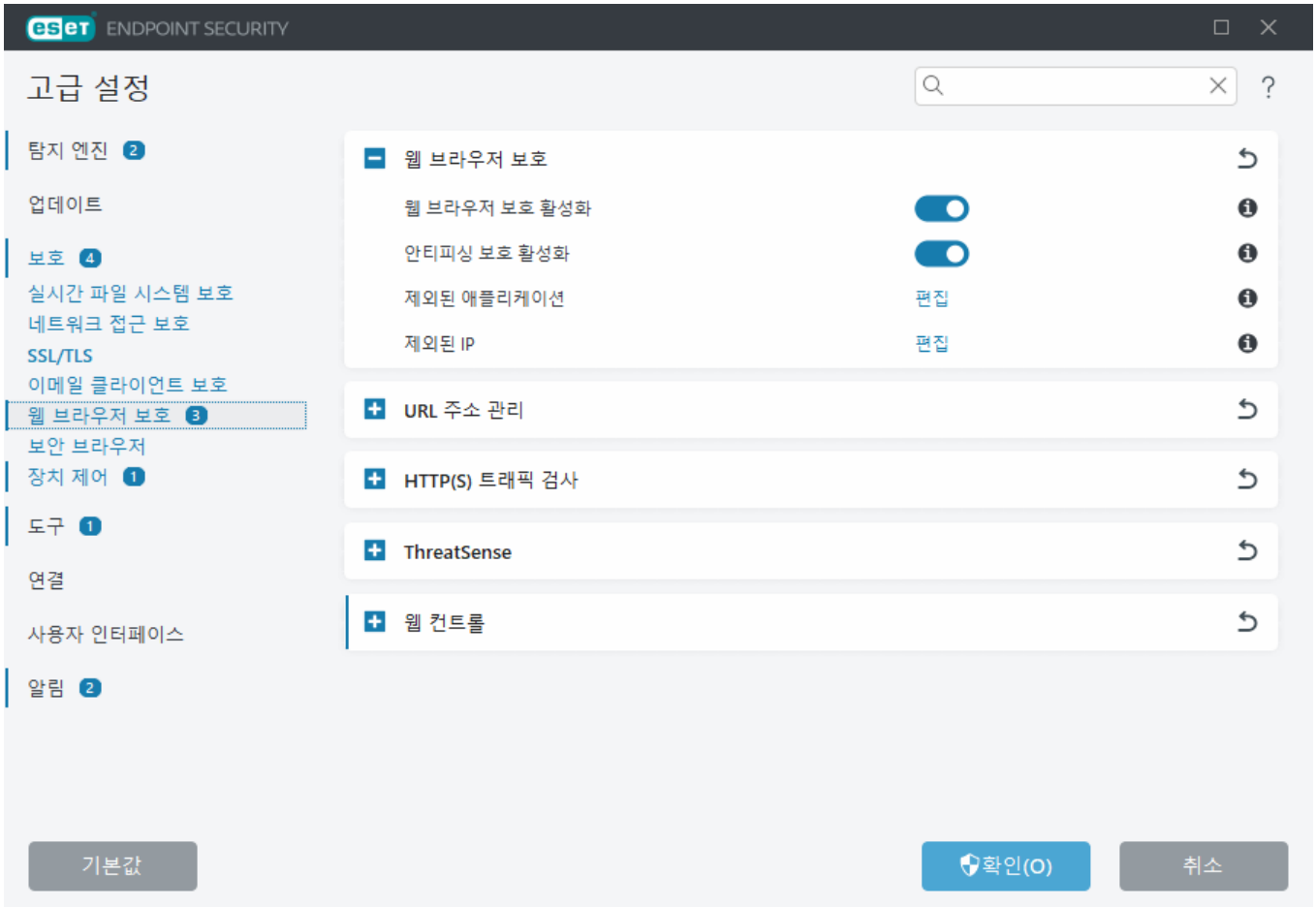
> 기본적으로 어떠한 애플리케이션이나 IP 주소도 제외하지 않고 웹 브라우저 보호가 활성화된 상태를 유지하는 것이 좋습니다.

브라우저 스크립트 검사 - 활성화된 경우 탐지 엔진이 웹 브라우저에서 실행되는 모든JavaScript 프로그램을 검사합니다.

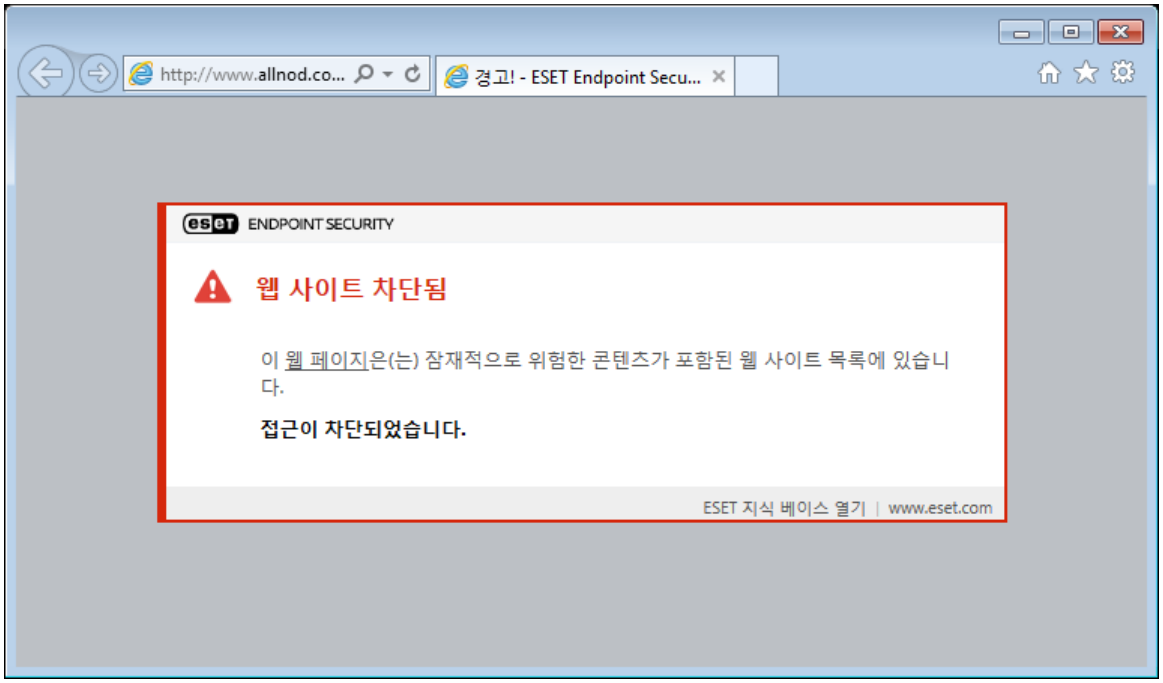
안티피싱 보호 활성화 - 활성화된 경우 피싱 웹 페이지가 차단됩니다. 자세한 내용은 안티피싱 보호를 참조하십시오.

제외된 애플리케이션 - 특정 애플리케이션을 웹 브라우저 보호에서 검사하지 않도록 제외할 수 있습니다. 웹 브라우저 보호로 인해 호환성 문제가 발생할 때 유용합니다.

제외된 IP - 특정 원격 주소를 웹 브라우저 보호에서 검사하지 않도록 제외할 수 있습니다. 웹 브라우저 보호로 인해 호환성 문제가 발생할 때 유용합니다.



웹 브라우저 보호는 웹 사이트가 차단될 때 브라우저에 다음 메시지를 표시합니다.



다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- ESET Endpoint Security의 개별 워크스테이션에서 안전한 웹 사이트 차단 해제

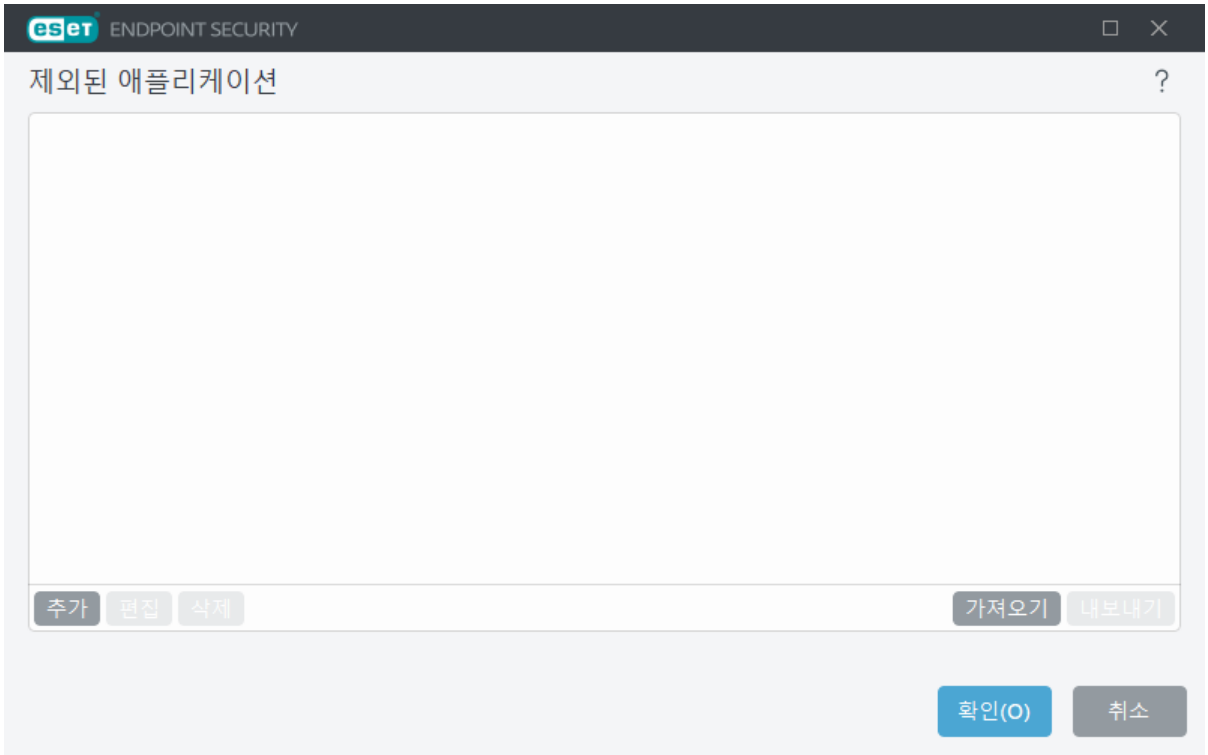
제외된 애플리케이션

특정 애플리케이션에 대한 통신 검사를 제외하려면 해당 애플리케이션을 목록에 추가합니다. 선택한 애플리케이션의 HTTP(S)/POP3(S)/IMAP(S) 통신은 위협에 대해 검사되지 않습니다. 이 옵션은 통신 검사 도중 제대로 작동하지 않는 애플리케이션에 대해서만 사용하는 것이 좋습니다.

실행 중인 애플리케이션과 서비스는 **추가**를 클릭하면 여기에서 자동으로 사용할 수 있습니다. **...**를 클릭하고 수동으로 제외를 추가할 애플리케이션으로 이동합니다.

편집 - 목록에서 선택한 항목을 편집합니다.

제거 - 목록에서 선택한 항목을 제거합니다.



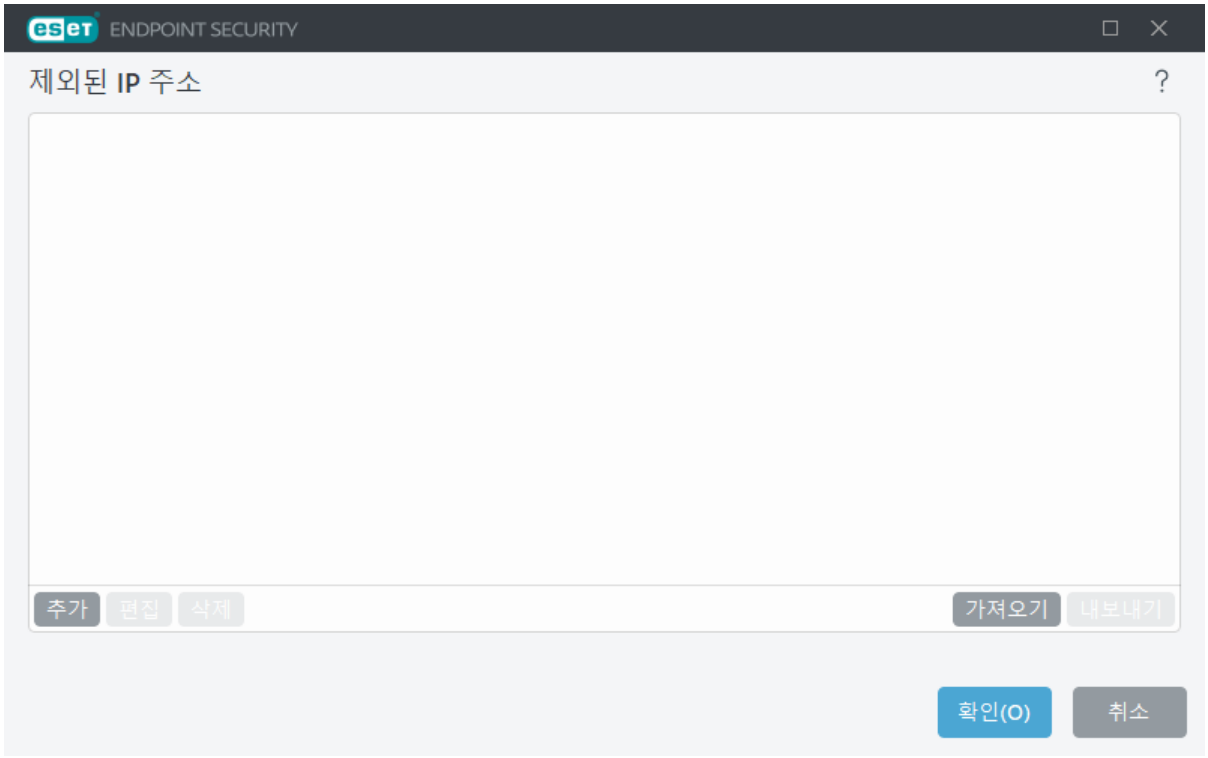
제외된 IP

목록의 항목은 검사에서 제외됩니다. 선택한 주소와의 HTTP(S)/POP3(S)/IMAP(S) 통신은 위협에 대해 검사되지 않습니다. 신뢰할 수 있는 것으로 알려진 주소에 한해서만 이 옵션을 사용하는 것이 좋습니다.

추가 - 규칙이 적용되는 원격 지점의 IP 주소/주소 범위/서브넷을 추가하려면 클릭합니다.

편집 - 목록에서 선택한 항목을 편집합니다.

제거 - 목록에서 선택한 항목을 제거합니다.



IP 주소 예제

IPv4 주소 추가:

단일 주소 - 개별 컴퓨터의 IP 주소(예: *192.168.0.10*)를 추가합니다.

주소 범위 - 시작 IP 주소와 끝 IP 주소를 입력하여 여러 컴퓨터의 IP 범위(예: *192.168.0.1~192.168.0.99*)를 지정합니다.

서브넷 - IP 주소 및 마스크에서 정의된 서브넷(컴퓨터 그룹)입니다. 예를 들어 255.255.255.0은 192.168.1.0 서브넷의 네트워크 마스크입니다. 전체 서브넷 유형을 제외하려면 *192.168.1.0/24*를 입력합니다.

IPv6 주소 추가:

단일 주소 - 개별 컴퓨터의 IP 주소(예: *2001:718:1c01:16:214:22ff:fec9:ca5*)를 추가합니다.

서브넷 - 서브넷(컴퓨터 그룹)은 IP 주소 및 마스크로 정의됩니다(예: *2002:c0a8:6301:1::1/64*).

URL 주소 관리

고급 설정 > **보호** > **웹 브라우저 보호**에서 **URL 목록 관리**를 사용하면 콘텐츠 검사를 차단, 허용하거나 제외할 HTTP 주소를 지정할 수 있습니다.

HTTP뿐만 아니라 HTTPS 주소도 필터링하려면 SSL/TLS를 활성화해야 합니다. 그렇지 않으면 방문한 HTTPS 사이트의 도메인만 추가되고 전체 URL은 추가되지 않습니다.

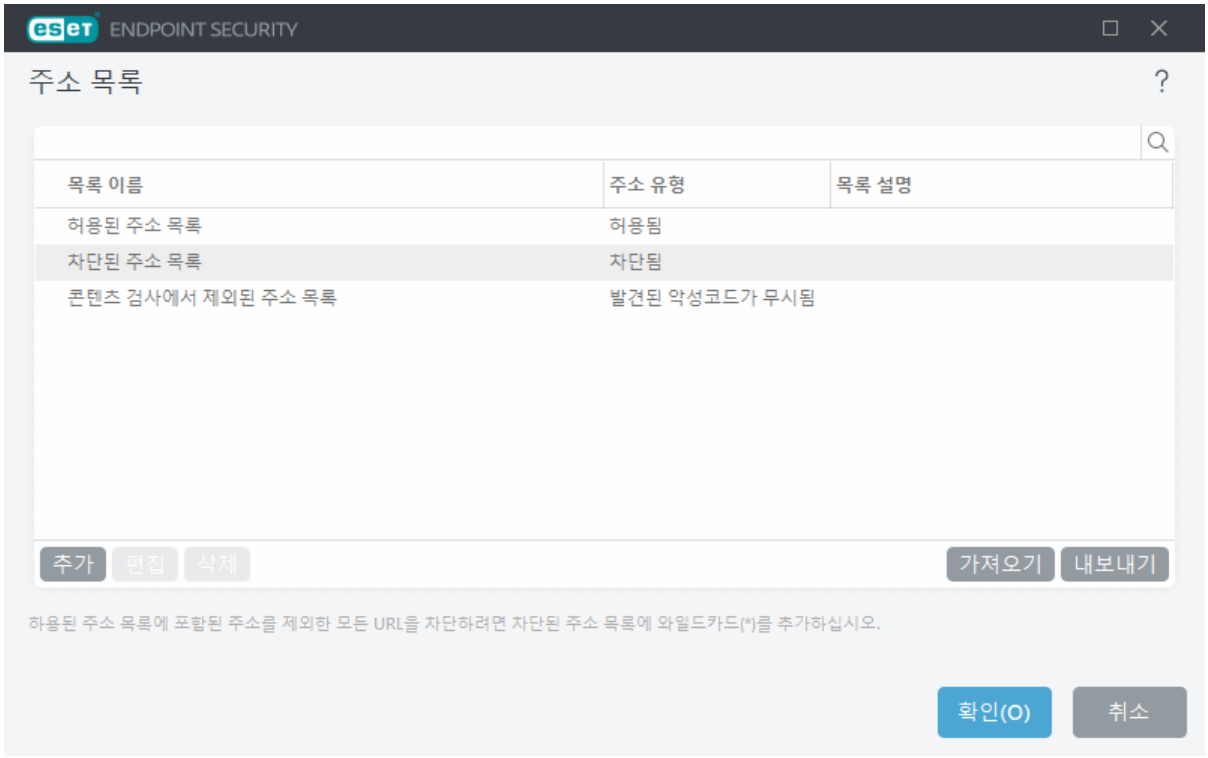
차단된 주소 목록의 웹 사이트는 **허용된 주소 목록**에도 포함되지 않는 한 접근할 수 없습니다. **콘텐츠 검사에서 제외된 주소 목록**의 웹 사이트는 접근 시 악성 코드가 있는지 검사되지 않습니다.

활성 **허용된 주소 목록**에 있는 주소를 제외하고 모든 HTTP 주소를 차단하려면 활성 **차단된 주소 목록**에 *를 추가합니다.

목록에서 특수 기호 *(별표) 및 ?(물음표)를 사용할 수 있습니다. 별표는 모든 문자열을 대체하고 물음표는 모든 기호를 대체합니다. 목록에는 신뢰할 수 있고 안전한 주소만 포함되어야 하므로 제외된 주소를 지정할 때 주의하십시오. 마찬가지로 이 목록에서 * 및 ? 기호가 올바르게 사용되는지 확인해야 합니다. 모든 하위 도메인을 비롯한 전체 도메인을 안전하게 일치시키는 방법은 HTTP 주소/도메인 마스크 추가를 참조하십시

오. 목록을 활성화하려면 **목록 활성화**를 선택합니다. 현재 목록에서 주소를 입력할 때 알림을 받으려면 **적용 시 알림**을 선택합니다.

> **ESET이 신뢰하는 주소**
> **ESET이 신뢰하는 도메인에서 트래픽 검사 안 함**이 활성화된 경우 SSL/TLS, 즉 ESET이 관리하는 허용 목록의 도메인은 URL 목록 관리 구성의 영향을 받지 않습니다.



제어 요소

추가 - 미리 정의된 목록 외에 새 목록을 생성합니다. 이 옵션은 다양한 주소 그룹을 논리적으로 분할하려는 경우 유용합니다. 예를 들어 차단된 주소 목록 하나에는 외부 공개 차단 목록의 주소가 포함될 수 있으며, 또 다른 차단된 주소 목록에는 자체 차단 목록이 포함될 수 있어 사용자의 차단 목록을 그대로 유지하면서 외부 목록을 쉽게 업데이트할 수 있습니다.

편집 - 기존 목록을 수정합니다. 이 옵션을 사용하여 주소를 추가하거나 제거할 수 있습니다.

삭제 – 기존 목록을 삭제합니다. **추가**를 사용하여 생성한 목록만 제거할 수 있고 기본 목록은 제거할 수 없습니다.

주소 목록

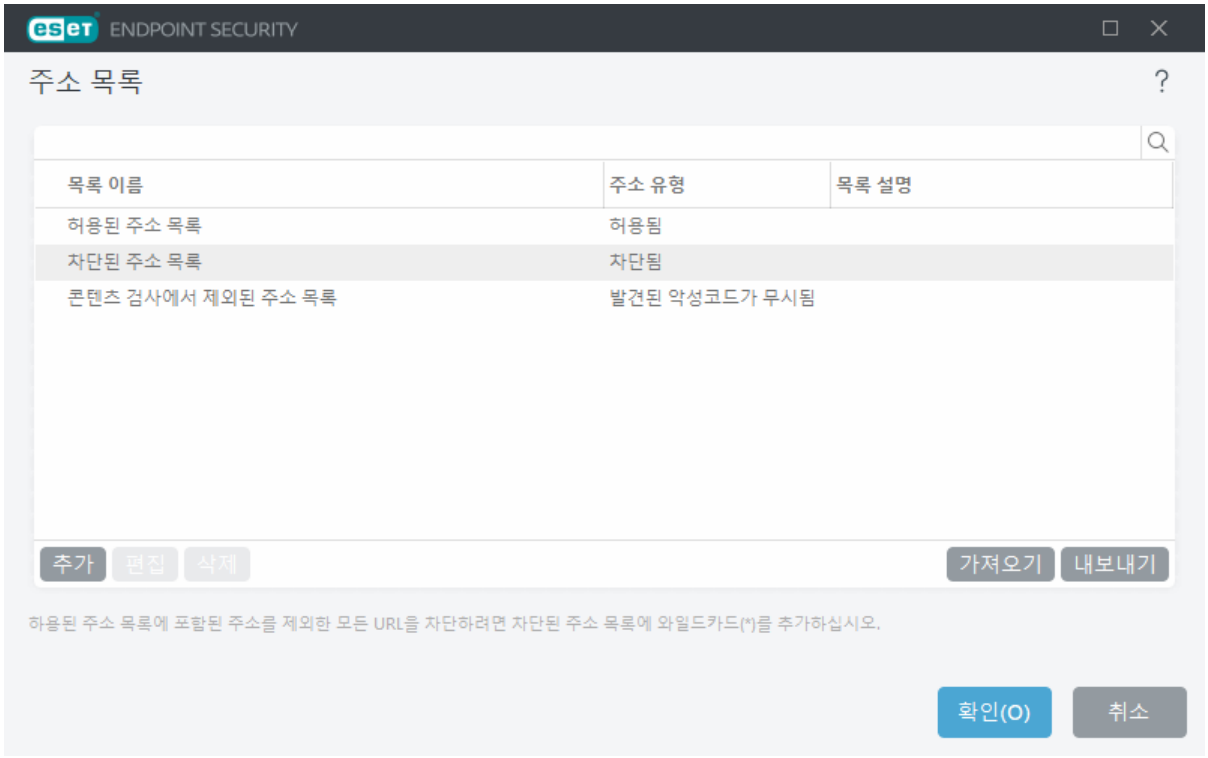
이 섹션에서는 검사에서 차단, 허용 또는 제외할 HTTP(S) 주소 목록을 지정할 수 있습니다.

기본적으로 다음의 세 가지 목록을 사용할 수 있습니다.

- **콘텐츠 검사에서 제외된 주소 목록** - 이 목록에 추가된 주소에 대해서는 악성 코드 검사를 수행하지 않습니다.
- **허용된 주소 목록** - 허용된 주소 목록에서 HTTP 주소에만 접근 허용 옵션이 활성화되고 차단된 주소 목록에 *(모든 항목 일치)가 포함된 경우 사용자는 이 목록에서 지정된 주소에만 접근할 수 있습니다.

주소가 차단된 주소 목록에 포함된 경우에도 이 목록에 포함되어 있으면 이 주소는 허용됩니다.
- **차단된 주소 목록** - 사용자는 주소가 허용된 주소 목록에도 포함된 경우가 아니라면 이 목록에서 지정된 주소에 접근할 수 없습니다.

새 목록을 생성하려면 **추가**를 클릭합니다. 선택한 목록을 제거하려면 **제거**를 클릭합니다.



다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- ESET Endpoint Security의 개별 워크스테이션에서 안전한 웹 사이트 차단 해제

자세한 내용은 URL 주소 관리를 참조하십시오.

새 주소 목록 생성

이 대화 상자 창에서는 검사에서 차단, 허용 또는 제외될 URL 주소/마스크의 새 목록을 구성할 수 있습니다.

다음 옵션을 구성할 수 있습니다.

주소 목록 유형 - 다음과 같은 세 가지 목록 유형을 사용할 수 있습니다.

- **발견된 악성코드가 무시됨** - 이 목록에 추가된 주소에 대해서는 악성 코드 검사를 수행하지 않습니다.
- **차단됨** - 이 목록에 지정된 주소에 대한 액세스가 차단됩니다.
- **허용됨** – 이 목록에 지정된 주소에 대한 액세스가 허용됩니다. 이 목록의 주소는 차단된 주소 목록과 일치하더라도 허용됩니다.

목록 이름 - 목록 이름을 지정합니다. 이 필드는 미리 정의된 목록 중 하나를 편집할 때 사용할 수 없습니다.

목록 설명 - 목록에 대한 간단한 설명을 입력합니다(옵션). 미리 정의된 목록 중 하나를 편집할 때 사용할 수 없습니다.

목록을 활성화하려면 해당 목록 옆의 **목록 활성화**를 선택합니다. 웹 사이트에 액세스할 경우에 특정 목록을

사용할 때 알림을 받으려면 **적용 시 알림**을 선택합니다. 예를 들어 웹 사이트가 차단된 주소 목록이나 허용된 주소 목록에 포함되어 있어 차단되거나 허용되는 경우 알림을 받게 됩니다. 이 알림에는 해당 목록의 이름이 포함됩니다.

로깅 심각도 - 드롭다운 메뉴에서 로깅 심각도를 선택합니다. 경고 상세 수준이 포함된 레코드는 ESET PROTECT에 의해 수집될 수 있습니다.

정보 및 경고 로깅 상세 수준은 도메인 내에 와일드카드가 없는 구성 요소가 두 개 이상 포함된 규칙에만 사용할 수 있습니다. 예를 들면 다음과 같습니다.
- *.domain.com/*
- *www.domain.com/*

제어 요소

추가 - 목록에 새 URL 주소를 추가합니다(여러 값은 분리 기호를 사용하여 입력).

편집 - 목록의 기존 주소를 수정합니다. **추가**를 사용하여 생성된 주소에만 사용할 수 있습니다.

제거 - 목록에서 기존 주소를 삭제합니다. **추가**를 사용하여 생성된 주소에만 사용할 수 있습니다.

가져오기 - URL 주소가 포함된 파일을 가져옵니다(줄 바꿈으로 값이 구분됨, 예: 인코딩 UTF-8을 사용하는 *.txt).

자세한 내용은 URL 마스크 추가 방법 장을 참조하십시오.

URL 마스크 추가 방법

원하는 주소/도메인 마스크를 입력하기 전에 이 대화 상자의 지침을 참조하십시오.

ESET Endpoint Security에서는 사용자가 지정한 웹 사이트에 대한 접근을 차단하고 인터넷 브라우저에 해당 웹 사이트의 콘텐츠가 표시되지 않도록 할 수 있습니다. 또한 검사에서 제외할 주소를 지정할 수도 있습니다. 원격 서버의 전체 이름을 모르거나 전체 원격 서버 그룹을 지정하려는 경우에는 '마스크'를 사용해 해당 그룹을 표시할 수 있습니다. 마스크에는 "?" 및 "*"가 있습니다.

- 기호를 대체하려면 ?를 사용합니다.
- 텍스트 문자열을 대체하려면 *를 사용합니다.

예를 들어 *.c?m은 마지막 부분이 c로 시작하고 m으로 끝나며 중간에 알 수 없는 기호가 포함된 모든 주소(.com, .cam 등)에 적용됩니다.

예를 들어 *x? 마스크는 끝에서 두 번째 문자인 x로 주소를 나타냅니다. 전체 도메인을 일치시키려면 **.domain.com/** 형식으로 입력합니다. 마스크에 *http://*, *https://* 프로토콜 접두어를 지정하는 일은 옵션입니다. 생략하면 마스크가 모든 프로토콜과 일치합니다. 맨 앞의 "*." 시퀀스는 도메인 이름 앞에 사용될 경우 특수하게 취급됩니다. 첫째, 이 경우에는 * 와일드카드가 슬래시 문자('/')와 일치하지 않습니다. 이를 통해 마스크 회피를 방지할 수 있습니다. 예를 들어 마스크 **.domain.com*은 *http://anydomain.com/anypath#.domain.com*과 일치하지 않습니다(이러한 접미사는 다운로드에 영향을 주지 않으면서 모든 URL에 추가할 수 있음). 둘째, 이와 같이 특수한 경우에는 "*."이 빈 문자열과도 일치합니다. 이를 통해 단일 마스크를 사용하여 하위 도메인이 포함된 전체 도메인과 일치시킬 수 있습니다. 예를 들어 **.domain.com* 마스크는 *http://domain.com*과도 일치합니다. **domain.com*을 사용하면

*http://anotherdomain.com*과도 일치하게 되므로 올바르지 않습니다.

정보 및 경고 로깅 상세 수준은 도메인 내에 와일드카드가 없는 구성 요소가 두 개 이상 포함된 규칙에만 사용할 수 있습니다. 예를 들면 다음과 같습니다.
- *.domain.com/*
- *www.domain.com/*

HTTP(S) 트래픽 검사

기본적으로 ESET Endpoint Security은(는) 인터넷 브라우저와 기타 애플리케이션에서 사용되는 HTTP 및 HTTPS 트래픽을 검사하도록 구성됩니다. 타사 소프트웨어에 문제가 있고, 이 문제가 ESET Endpoint Security에서 비롯된 것인지 알고 싶은 경우에만 트래픽 검사를 비활성화해야 합니다.

HTTP 트래픽 검사 활성화 - HTTP 트래픽은 항상 모든 애플리케이션의 모든 포트에서 모니터링됩니다.

HTTPS 트래픽 검사 활성화 - HTTPS 트래픽은 암호화된 채널을 사용하여 서버와 클라이언트 간에 정보를 전송합니다. ESET Endpoint Security에서는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 프로토콜을 활용하여 통신을 검사합니다. 이 프로그램은 운영 체제 버전과 관계없이 **HTTPS 프로토콜에서 사용되는 포트**에 정의된 포트의 트래픽만 검사합니다(미리 정의된 443 및 0~65535에 포트 추가 가능).

ThreatSense

ThreatSense는 복잡한 위협 검출 방법으로 구성되어 있습니다. 사전 예방 방식으로 검사를 수행합니다. 즉, 새로운 위협의 확산 초기에도 보호 기능을 제공합니다. 또한 함께 작동하여 시스템 보안 성능을 크게 향상시켜 주는 코드 분석, 코드 에뮬레이션, 일반 시그니처, 바이러스 시그니처 등의 방법을 조합해 사용합니다. 검사 엔진은 여러 데이터 스트림을 동시에 제어하여 효율성과 검출 비율을 최대화할 수 있습니다. ThreatSense 기술은 루트킷도 제거할 수 있습니다.

ThreatSense 엔진 설정 옵션을 사용하여 다음과 같은 여러 가지 검사 파라미터를 지정할 수 있습니다.

- 검사할 파일 형식 및 확장명
- 다양한 검출 방법의 조합
- 치료 수준 등

설정 창에 들어가려면 ThreatSense 기술을 사용하는 모듈(아래 참조)에 대한 고급 설정에서 **ThreatSense**을(를) 클릭합니다. 각 보안 시나리오에 따라 서로 다른 구성이 필요할 수 있습니다. 이를 염두에 두고, 다음 보호 모듈에 대해 ThreatSense를 개별적으로 구성할 수 있습니다.

- 실시간 파일 시스템 보호
- 유휴 상태 검사
- 시작 검사
- 문서 보호
- 이메일 클라이언트 보호
- 웹 브라우저 보호
- 컴퓨터 검사

ThreatSense 파라미터는 각 모듈에 맞게 고도로 최적화되어 있으므로 이를 수정하면 시스템 작동에 큰 영향을 줄 수 있습니다. 예를 들어 항상 런타임 패커를 검사하도록 파라미터를 변경하거나 실시간 파일 시스템

보호 모듈에서 고급 인공지능을 활성화하면 시스템 속도가 느려질 수 있습니다. 일반적으로 새로 생성된 파일에만 이러한 방법을 사용하여 검사합니다. 따라서 컴퓨터 검사를 제외한 모든 모듈에 대해서는 기본 ThreatSense 파라미터를 변경하지 않는 것이 좋습니다.

오브젝트 검사

이 섹션에서는 침입에 대해 검사할 컴퓨터 구성 요소 및 파일을 정의할 수 있습니다.

운영 메모리 - 시스템의 운영 메모리를 공격하는 위협이 있는지 검사합니다.

부트 영역/UEFI – 마트터 부트 레코드에 악성코드가 있는지 부트 영역을 검사합니다. UEFI에 대한 자세한 내용은 용어집을 참조하십시오.

이메일 파일 - 프로그램에서 지원되는 확장명은 DBX (Outlook Express) 및 EML입니다.

압축파일 – 프로그램에서 지원되는 확장명은 ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE 등입니다.

자체 압축 해제 파일 - 자체 압축 해제 파일(SFX)은 자체적으로 압축을 해제할 수 있는 파일입니다.

런타임 패커 - 런타임 패커는 표준 압축파일 형식과 달리 실행 후에 메모리에 압축이 풀립니다. 검사기는 표준 정적 패커(UPX, yoda, ASPack, FSG 등) 외에도 코드 에뮬레이션을 통해 몇 가지 추가 패커 유형을 인식할 수 있습니다.

검사 옵션

시스템에서 침입을 검사할 때 사용할 방법을 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.

인공지능 - 인공지능은 프로그램의 악의적 활동을 분석하는 알고리즘입니다. 이 기술의 가장 큰 장점은 이전 버전의 검색 엔진 생성 당시 존재하지 않았거나 해당 엔진에서 인식하지 못한 악성 소프트웨어를 식별할 수 있다는 것입니다. 그러나 악성이 아닌 소프트웨어를 악성으로 보고할 수 있다는 단점이 있습니다(가능성은 매우 낮음).

고급 휴리스틱/DNA 시그니처 - 고급 인공지능은 ESET에서 개발한 고유 인공지능 알고리즘으로, 컴퓨터 웜 및 트로이 목마 검출용으로 최적화되고 높은 수준의 프로그래밍 언어로 작성되었습니다. 고급 인공지능을 사용하면 ESET 제품의 위협 검출 기능이 크게 향상됩니다. 시그니처는 바이러스를 안정적으로 검출 및 식별할 수 있습니다. 자동 업데이트 시스템을 통해 위협 검출을 위해 새 시그니처를 몇 시간 이내에 사용할 수 있습니다. 그러나 시그니처는 인식 가능한 바이러스 또는 이러한 바이러스의 약간 수정된 버전만 검출할 수 있다는 단점이 있습니다.

치료

치료 설정에 따라 개체 치료 중 ESET Endpoint Security의 동작이 결정됩니다.

제외

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로. 파일의 형식과 내용을 정의합니다. 이 ThreatSense 설정 섹션에서는 검사할 파일 형식을 정의할 수 있습니다.

기타

수동 컴퓨터 검사에 대해 ThreatSense 엔진 설정을 구성할 때 **기타** 섹션에서 다음과 같은 옵션도 제공됩니다.

ADS(대체 데이터 스트림) 검사 - NTFS 파일 시스템에서 사용하는 대체 데이터 스트림은 일반 검사 기술로는 표시되지 않는 파일 및 폴더 연결입니다. 대체 데이터 스트림으로 가장하여 검출을 피하려고 하는 침입이 많이 있습니다.

순위가 낮은 백그라운드 검사 실행 - 각 검사 시퀀스는 일정량의 시스템 리소스를 사용합니다. 시스템 리소스에 대한 로드가 높은 프로그램을 사용하는 경우에는 순위가 낮은 백그라운드 검사를 활성화하여 리소스를 절약하고 이러한 절약된 리소스를 애플리케이션에 사용할 수 있습니다.

모든 개체 기록 – 검사 로그는 감염되지 않았더라도 자체 압축 해제 파일의 검사된 모든 파일을 표시합니다(이로 인해 검사 로그 데이터가 많이 생성되고 검사 로그 파일 크기가 커질 수 있음).

스마트 최적화 활성화 - 스마트 최적화를 활성화하면 가장 효율적인 검사 수준을 유지하는 동시에 최고 검사 속도를 유지하기 위한 최적의 설정이 사용됩니다. 다양한 보호 모듈이 다양한 검사 방법을 활용하고 해당 방법을 특정 파일 형식에 적용하는 방식으로 지능적 검사를 수행합니다. 스마트 최적화를 비활성화하면 검사를 수행할 때 특정 모듈의 ThreatSense 코어에서 사용자가 정의한 설정만 적용됩니다.

마지막 접근시의 타임스탬프 유지 - 검사한 파일의 원래 접근 시간을 데이터 백업 시스템 등에 사용할 수 있도록 업데이트하지 않고 그대로 유지하려면 이 옵션을 선택합니다.

제한

제한 섹션에서는 최대 개체 크기와 검사할 중복 압축 수준을 지정할 수 있습니다.

개체 설정

최대 개체 크기 - 검사할 개체의 최대 크기를 정의합니다. 그러면 지정된 안티바이러스 모듈에서 지정한 크기보다 작은 개체만 검사합니다. 큰 개체를 검사에서 제외해야 하는 특별한 이유가 있는 고급 사용자만 이 옵션을 변경해야 합니다. 기본값은 제한 없음입니다.

최대 개체 검사 시간(초) – 컨테이너 개체의 파일을 검사하기 위한 최대 시간 값(예: RAR/ZIP 압축파일 또는 첨부 파일이 여러 개 있는 이메일)을 정의합니다. 이 설정은 독립 실행형 파일에 적용되지 않습니다. 사용자 정의 값을 입력하고 해당 시간이 경과한 경우, 컨테이너 개체에서 각 파일 검사가 완료되었는지 여부에 관계없이 가능한 한 빨리 검사가 중지됩니다. 대용량 파일이 있는 압축파일의 경우, 압축파일에서 파일이 압축 해제되는 시간보다 더 빨리 검사가 중지되지는 않습니다(예: 사용자 정의 변수가 3초이지만 파일 압축 해제는 5초가 소요되는 경우). 압축파일의 나머지 파일은 해당 시간이 경과하면 검사되지 않습니다. 더 큰 압축파일 등의 검사 시간을 제한하려면 **최대 개체 크기**와 **압축파일 내 파일의 최대 크기**를 사용합니다(가능한 보안 위험으로 인해 권장되지 않음). 기본값은 제한 없음입니다.

압축파일 검사 설정

다중 압축 수준 - 최대 압축파일 검사 수준을 지정합니다. 기본값: 10.

압축파일 내 파일의 최대 크기 - 이 옵션을 사용하면 검사할 압축파일에 포함된 파일의 최대 파일 크기(압축 해제 시)를 지정할 수 있습니다. 최대값은 3GB입니다.

일반적인 상황에서는 기본값을 수정할 필요가 없으므로 기본값을 변경하지 않는 것이 좋습니다.

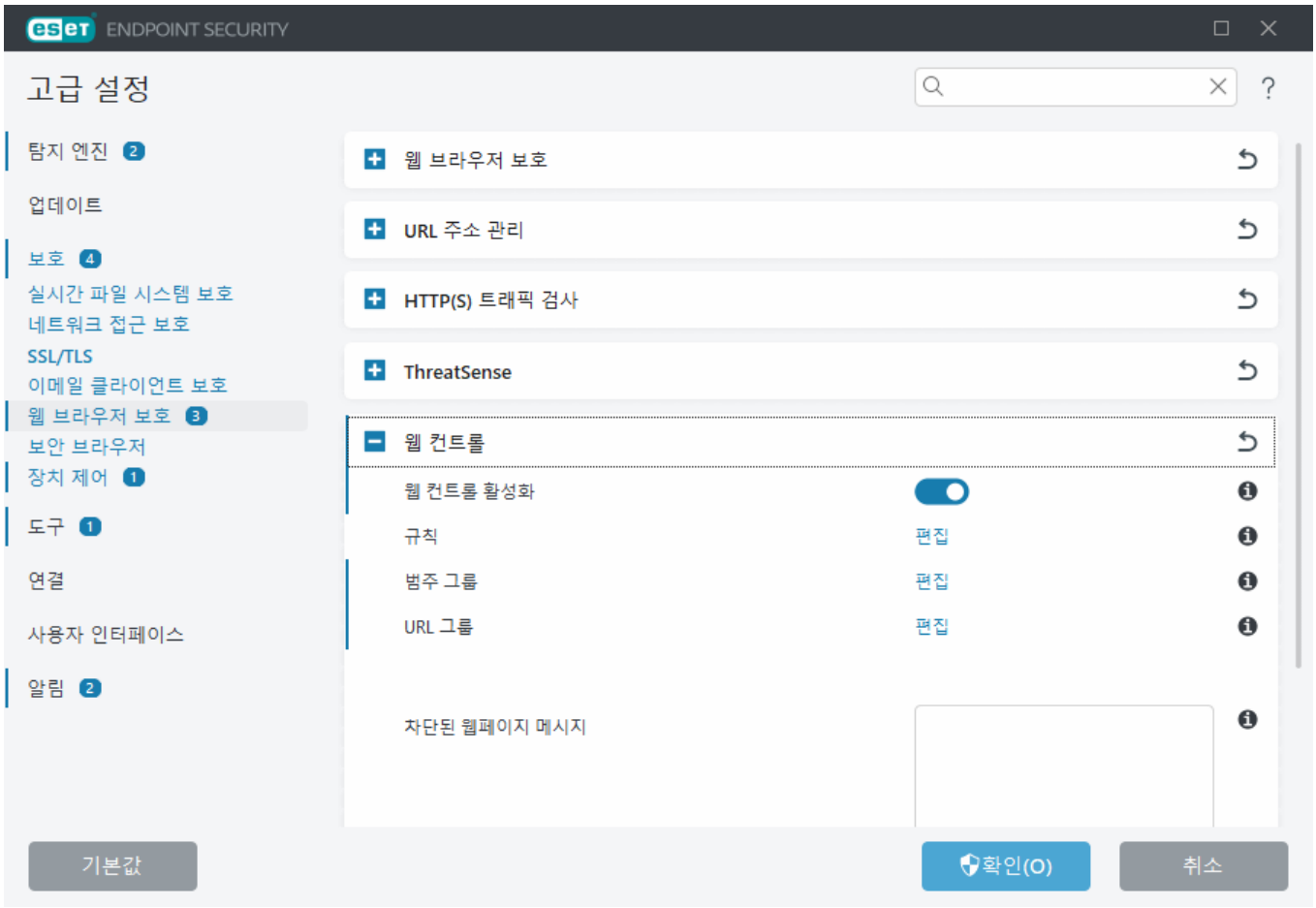
웹 컨트롤

웹 컨트롤 섹션에서는 법적 책임 위험으로부터 회사를 보호하는 설정을 구성할 수 있습니다. 웹 컨트롤은 지적재산권을 위반하는 웹 사이트에 대한 접근을 규제할 수 있습니다. 이 모듈의 목적은 직원들이 부적합하거나 유해한 콘텐츠가 있는 페이지나 생산성을 떨어뜨릴 수 있는 페이지에 접근하지 못하도록 하는 것입니다.

웹 컨트롤을 사용하면 잠재적으로 부적절한 자료가 포함되었을 수 있는 웹 페이지를 차단할 수 있습니다. 또한 고용주나 시스템 관리자는 27개가 넘는 미리 정의된 웹 사이트 범주 및 140개 이상의 하위 범주에 대한 접근을 금지할 수 있습니다.

웹 컨트롤은 기본적으로 비활성화되어 있습니다. 웹 컨트롤을 활성화하려면 다음을 수행합니다.

1. 고급 설정 > **보호** > **웹 브라우저 보호** > **웹 컨트롤**을 엽니다.
2. **웹 컨트롤 활성화** 토글을 활성화하여 ESET Endpoint Security에서 웹 컨트롤을 활성화합니다.
3. 특정 웹 페이지에 대한 접근을 구성합니다. 웹 컨트롤 규칙 편집 창에 접근하려면 **규칙** 옆의 **편집**을 클릭합니다.

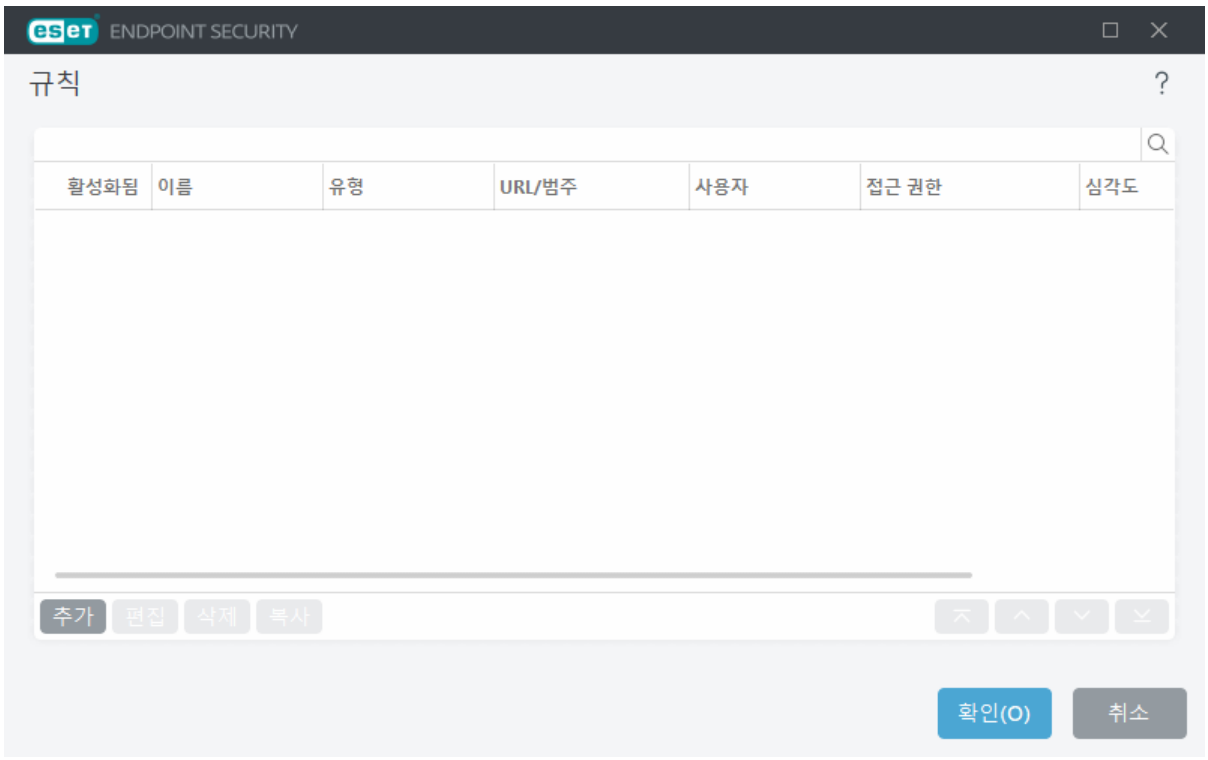


차단된 웹 페이지 메시지 및 **차단된 웹 페이지 그래픽** 필드를 사용하면 웹 사이트가 차단된 경우 표시되는 메시지를 사용자 지정할 수 있습니다.

모든 웹 페이지를 차단하고 특정 웹 페이지만 허용하려면 URL 주소 관리를 사용합니다.

웹 컨트롤 규칙

규칙 편집 창에는 기존 URL 기반 규칙이나 범주 기반 규칙이 표시됩니다.



규칙 목록에는 이름, 차단 유형, 웹 컨트롤 규칙을 일치시킨 후 수행할 동작 및 로그 심각도 등과 같은 여러 규칙 설명이 포함되어 있습니다.

추가 또는 **편집**을 클릭하면 규칙을 관리할 수 있습니다. **복사**를 클릭하면 선택된 다른 규칙에 사용되는 미리 정의된 옵션으로 새 규칙을 생성할 수 있습니다. **Ctrl** 키를 누른 상태에서 클릭하면 여러 규칙을 선택하여 선택한 모든 규칙을 삭제할 수 있습니다. **활성화됨** 확인란을 사용하면 규칙을 활성화 또는 비활성화할 수 있습니다. 이 옵션은 규칙을 나중에 사용할 수도 있어 영구적으로 삭제하지 않으려는 경우에 유용합니다.

규칙은 순위를 결정하는 순서로 정렬되며 순위가 높은 규칙이 맨 위에 정렬됩니다. 규칙의 순위를 변경하려면 규칙을 선택하고 화살표 버튼을 클릭하여 규칙 순위를 높이거나 낮춥니다. 규칙을 목록의 상단 또는 하단으로 이동하려면 이중 화살표를 클릭합니다.

규칙 생성도 참조하십시오.

웹 컨트롤 규칙 추가

웹 컨트롤 규칙 창에서 수동으로 웹 컨트롤 규칙을 생성하거나 기존 웹 컨트롤 규칙을 수정할 수 있습니다.

이름

좀 더 쉽게 식별할 수 있도록 **이름** 필드에 규칙 설명을 입력합니다.

활성화됨

규칙을 비활성화하거나 활성화하려면 **활성화됨** 스위치를 클릭합니다. 이 옵션은 규칙을 영구적으로 삭제하지 않으려는 경우에 유용합니다.

동작

URL 기반 동작 또는 **범주 기반 동작** 중에서 선택합니다.

URL 기반 동작

지정된 웹 사이트에 대한 접근을 제어하는 규칙의 경우 **URL** 필드에 URL을 입력합니다.
특수 기호 *(별표)와 ?(물음표)는 URL 주소 목록에서 사용할 수 없습니다. 여러 TLD(최상위 도메인)를 포함한 웹 사이트가 있는 URL 그룹을 생성할 경우 각 TLD를 별도로 추가해야 합니다. 그룹에 도메인을 추가할 때 이 도메인 및 모든 하위 도메인(예: *sub.examplepage.com*)에 있는 모든 콘텐츠는 사용자가 선택한 URL 기반 동작에 따라 차단되거나 허용됩니다.
URL 또는 **URL 그룹 사용** - URL 링크 또는 URL 링크 그룹을 정의하여 이러한 URL 중 하나에 접근하려는 사용자를 허용 또는 차단하거나 경고를 표시합니다.

범주 기반 동작

규칙은 웹 사이트 범주에 따라 적용됩니다.
URL 범주 또는 **그룹 사용** - 웹 사이트 범주 또는 범주 그룹을 선택하여 이러한 범주 중 하나가 탐지되면 사용자를 허용 또는 차단하거나 경고를 표시합니다.

접근 권한

- **허용** - URL 주소/범주에 대한 접근을 허용합니다.
- **경고** - URL 주소/범주에 대한 접근을 차단합니다. **뒤로 이동**을 클릭하여 이전 웹 사이트로 돌아가거나 **계속**을 클릭하여 웹 사이트에 접근할 수 있습니다. **계속**을 클릭하면 다음에 웹 사이트를 방문할 때 차단 페이지가 표시되지 않습니다.
- **항상 경고**: URL 주소/범주에 대한 접근을 차단합니다. **뒤로 이동**을 클릭하여 이전 웹 사이트로 돌아가거나 **계속**을 클릭하여 웹 사이트에 접근할 수 있습니다. 웹 사이트를 방문할 때마다 차단 페이지가 표

시됩니다.
- **차단** - URL 주소/범주에 대한 접근을 차단합니다. **뒤로 이동**을 클릭하여 이전 웹 사이트로 돌아갈 수 있습니다.

다음 기간 중에 적용

특정 시간 동안 생성된 규칙을 적용할 수 있습니다. **다음 기간 중에 적용** 드롭다운 메뉴에서 생성된 시간 슬롯을 선택합니다. 시간 슬롯에 대한 자세한 내용

로깅 심각도

- **항상** - 모든 온라인 통신을 기록합니다.
- **분석** - 프로그램을 미세 조정하는 데 필요한 로그 정보입니다.
- **정보** - 성공한 업데이트 메시지를 포함한 정보 메시지와 위의 모든 레코드를 기록합니다.
- **경고** - 심각한 오류 및 경고 메시지를 기록합니다.
- **없음** - 로그가 생성되지 않습니다.

> 각 목록에 대해 로깅 심각도를 별도로 구성할 수 있습니다. **경고** 상태의 로그는 ESET PROTECT에 의해 수집될 수 있습니다.

사용자 목록

- **추가** - 원하는 사용자를 선택할 수 있는 **사용자 또는 그룹 선택** 대화 상자 창을 엽니다. 사용자를 입력하지 않으면 규칙이 모든 사용자에게 적용됩니다.
- **제거** - 선택한 사용자를 필터에서 제거합니다.

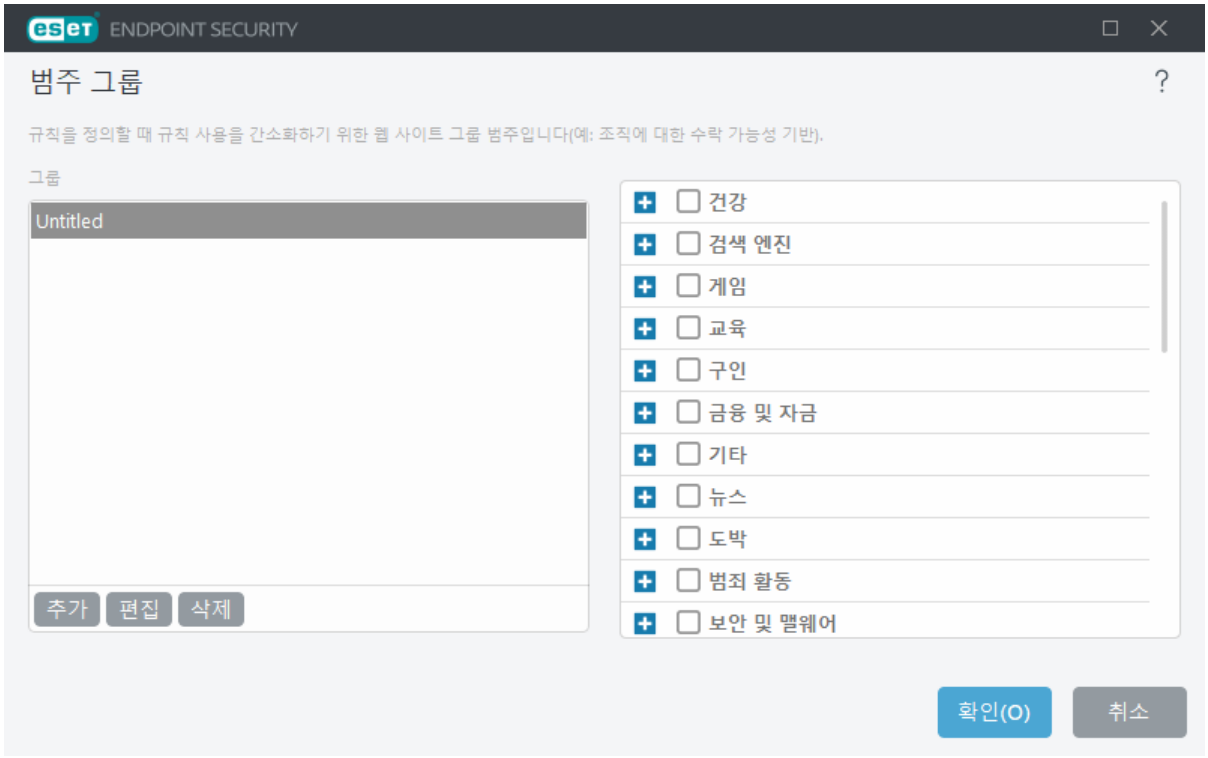
범주 그룹

범주 그룹 창은 두 부분으로 나뉘어 있습니다. 창의 왼쪽 부분에는 범주 그룹 목록이 포함됩니다.

- **추가** – 새 범주 그룹을 생성하려면 클릭합니다.
- **편집** – 기존 범주 그룹을 편집하려면 클릭합니다.
- **제거** – 범주 그룹 목록에서 기존 범주 그룹을 제거하려면 선택 및 클릭합니다.

창의 오른쪽에는 범주 및 하위 범주 목록이 포함됩니다. 범주 목록에서 범주를 선택하여 하위 범주를 표시할 수 있습니다. 각 그룹에는 일반적으로 허용되는 것으로 간주되는 범주와 일반적으로 부적절한 하위 범주 및/또는 성인이 포함됩니다. 범주 그룹 창을 열고 첫 번째 그룹을 클릭하면 적절한 그룹 목록에서 범주/하위 범주를 추가하거나 제거할 수 있습니다(예: 폭력 또는 무기). 부적절한 콘텐츠가 포함된 웹 페이지를 차단할 수 있으며 차단된 웹 페이지에 접근할 때 사용자에게 알릴 수 있습니다.

특정 그룹에 하위 범주를 추가하거나 특정 그룹에서 하위 범주를 제거하려면 확인란을 선택합니다.



다음은 사용자에게 생소할 수 있는 몇 가지 범주의 예입니다.

- **기타** - 주로 개인(로컬) IP 주소(예: 인트라넷 192.168.0.0/16 등)입니다. 403 또는 404 오류 코드가 나타나면 웹 사이트가 이 범주에 해당하는 것입니다.
- **해결 안 됨** - 이 범주에는 웹 컨트롤 DB 엔진에 연결할 때 발생한 오류 때문에 해결되지 않은 웹 페이지가 포함됩니다.
- **분류되지 않음** - 아직 웹 컨트롤 DB에 없는 알 수 없는 웹 페이지입니다.
- **프록시** - 익명 서비스, 리디렉터 또는 공용 프록시 서버와 같은 웹 페이지를 사용하여 일반적으로 웹 컨트롤 필터로 금지되지 않는 웹 페이지에 익명으로 접근할 수 있습니다.
- **파일 공유** - 이러한 웹 페이지에는 사진, 비디오 또는 전자책 같은 대량의 데이터가 포함되어 있습니다. 이러한 사이트에는 잠재적으로 부적절한 자료나 성인용 콘텐츠가 포함되어 있을 수 있습니다.

URL의 잘못된 분류를 보고할 수 있습니다.

하위 범주는 어떤 그룹에도 속할 수 있습니다. 미리 정의된 그룹에 포함되지 않은 일부 하위 범주도 있습니다(예: 게임). 웹 컨트롤 필터를 사용하여 원하는 하위 범주와 일치시키려면 해당 하위 범주를 원하는 그룹에 추가합니다.

URL 그룹

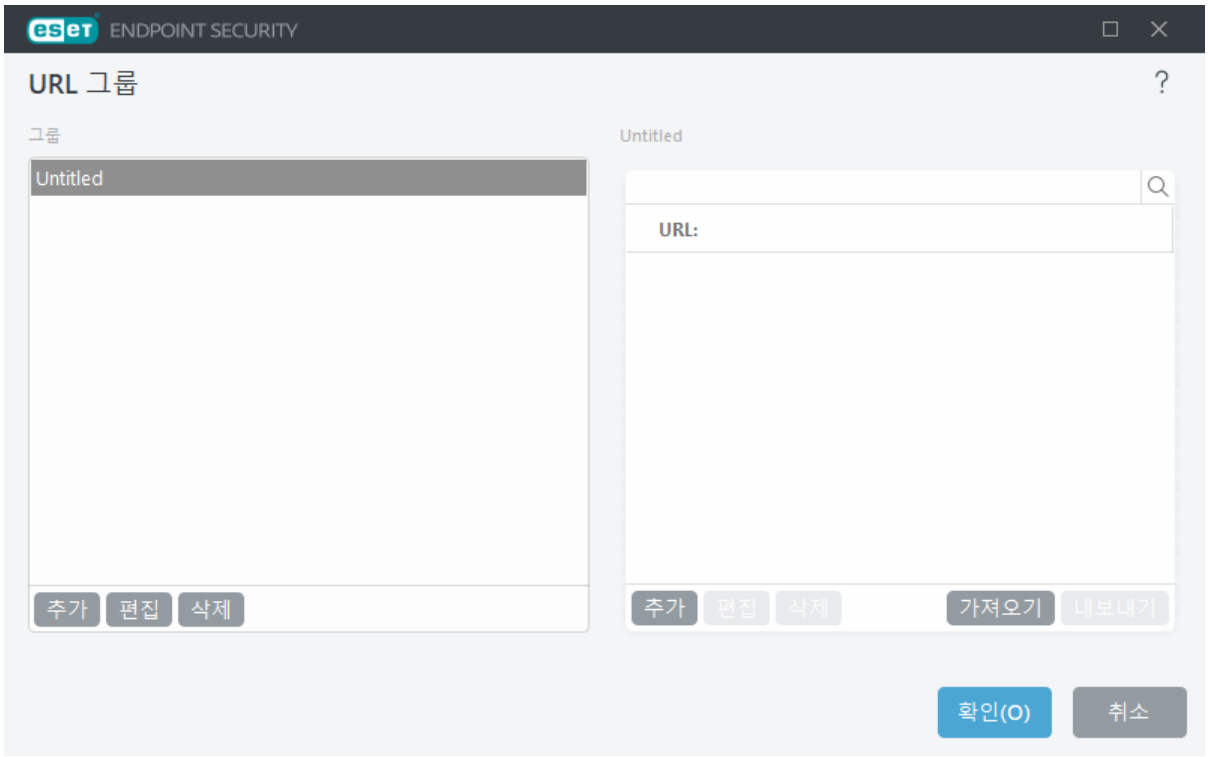
URL 그룹을 통해 규칙(특정 웹 사이트 허용/차단)을 생성할 여러 URL 링크가 포함된 그룹을 만들 수 있습니다.

새 URL 그룹 생성

새 URL 그룹을 생성하려면 **추가**를 클릭하고 새 URL 그룹의 이름을 입력합니다.

URL 그룹을 사용하면 관리자가 더 많은 웹 페이지에 대한 규칙을 생성하고자 할 때 유용할 수 있습니다(선택에 따라 차단되거나 허용됨).

URL 주소를 URL 그룹 목록에 추가 - 수동



새 URL 주소를 목록에 추가하려면 URL 그룹을 선택하고 창 오른쪽 아래의 **추가**를 클릭합니다.

특수 기호 *(별표)와 ?(물음표)는 URL 주소 목록에서 사용할 수 없습니다.

http:// 또는 https://가 포함된 도메인의 전체 이름을 입력하지 않아도 없습니다.

도메인을 그룹에 추가하는 경우, 이 도메인에 있는 모든 콘텐츠와 모든 하위 도메인(예: *sub.examplepage.com*)이 선택한 URL 기반 동작에 따라 차단되거나 허용됩니다.

도메인을 차단하는 첫 번째 규칙의 의미에 대해 두 규칙 간에 충돌이 발생하는 경우, 동일한 도메인, 특정 도메인 또는 IP 주소를 허용하는 두 번째 규칙이 차단됩니다. 규칙 생성에 대한 자세한 정보는 URL 기반 동작을 참조하십시오.

URL 그룹 목록에 URL 주소 추가 - .txt 파일을 사용하여 가져오기

URL 주소 목록이 포함된 파일(줄 바꿈으로 값 구분, 예: 인코딩 UTF-8을 사용하는 .txt 파일)을 가져오려면 **가져오기**를 클릭합니다. 특수 기호 *(별표)와 ?(물음표)는 URL 주소 목록에서 사용할 수 없습니다.

웹 컨트롤에서 URL 그룹 사용

특정 URL 그룹에 대해 수행할 동작을 설정하려는 경우, 웹 컨트롤 규칙 편집을 열고, 드롭다운 메뉴를 사용하여 URL 그룹을 선택하고, 기타 파라미터를 조정한 후 **확인**을 클릭합니다.

> 전체 웹 페이지 범주를 차단하거나 허용하는 것보다 특정 웹 페이지를 차단하거나 허용하는 것이 더 정확할 수 있습니다. 이러한 설정을 변경하고 목록에 범주/웹 페이지를 추가할 때는 주의하십시오.

차단된 웹 페이지 메시지 사용자 지정

차단된 웹 페이지 메시지 및 **차단 웹 페이지 그래픽** 필드에서는 웹 사이트가 차단된 경우 표시되는 메시지를 쉽게 사용자 지정할 수 있습니다.

사용

"무기" 웹 사이트 범주를 차단해 보겠습니다.

차단된 웹 페이지 메시지의 예:

```
웹 페이지 %URL_OR_CATEGORY%은(는) 부적절하거나 유해한 콘텐츠를 포함하는 것으로 간주되므
로 차단되었습니다.
자세한 내용은 관리자에게 문의하십시오.
```

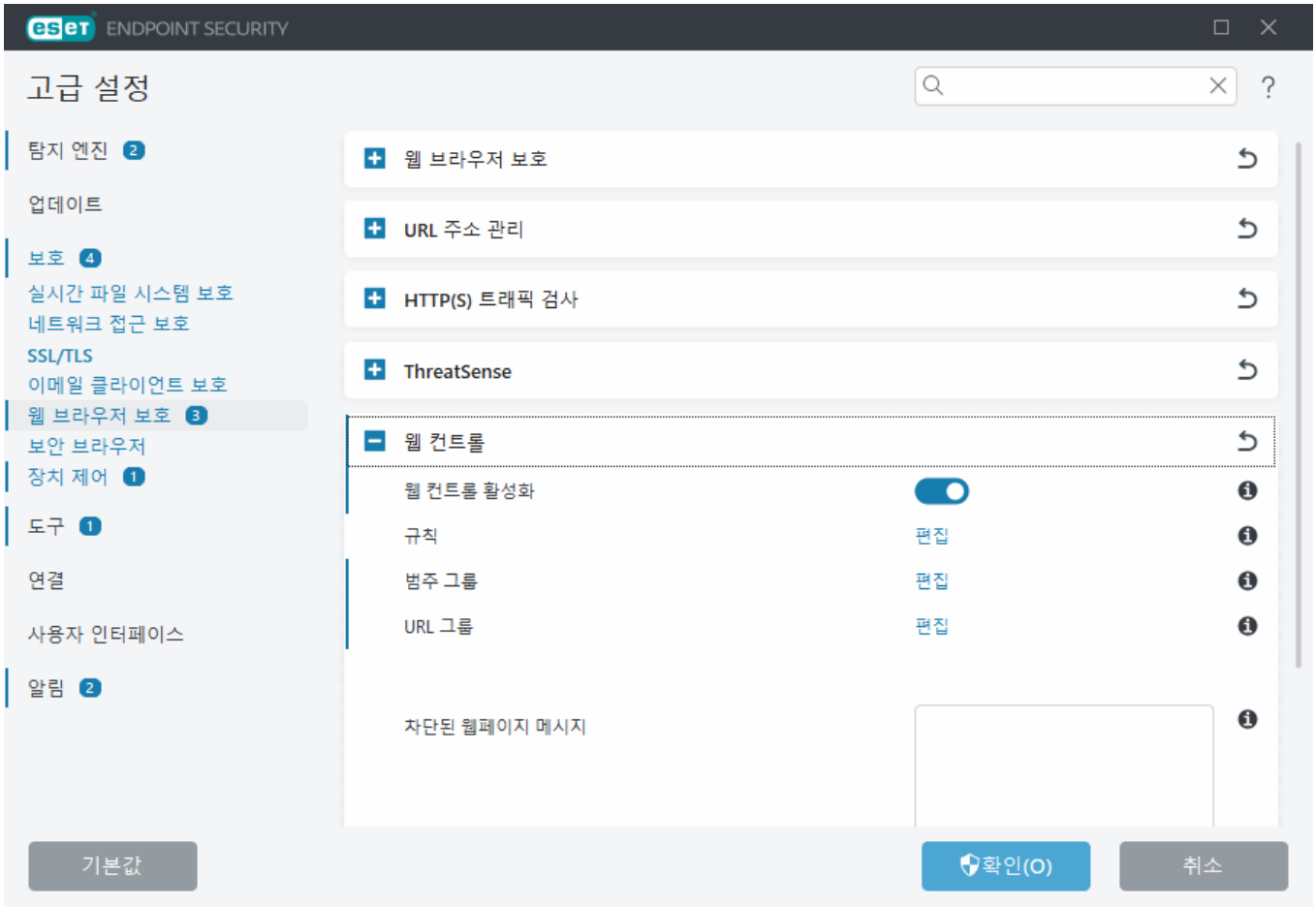
변수	설명
%CATEGORY%	차단된 웹 컨트롤 범주입니다.
%URL_OR_CATEGORY%	차단된 웹 컨트롤 웹 사이트 또는 범주입니다(웹 컨트롤 차단 규칙에 따라 다름).
%STR_GOBACK%	"뒤로 이동" 버튼 값입니다.
%product_name%	ESET 제품의 이름입니다(ESET Endpoint Security).
%product_version%	ESET 제품의 버전입니다.

차단된 웹 페이지 그래픽의 예:

```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

이미지 크기(너비/높이)가 너무 크면 자동으로 조정됩니다.

ESET Endpoint Security의 구성은 다음과 같습니다.



대화 상자 창 - 웹 컨트롤

웹 컨트롤의 기본 기능은 회사 네트워크에서 각 사용자가 접근하는 웹 사이트를 제어하는 것입니다. 네트워크 관리자는 사용자별 또는 사용자 그룹별로 사용자가 접근할 수 있는 웹 사이트의 범주를 정의할 수 있어야 합니다. 디렉터리 서비스와 통합하면 Active Directory 그룹을 웹 컨트롤 구성에 사용할 수 있습니다. 기본적으로 이 기능은 비활성화되어 있습니다. 이 기능을 활성화하려면 **웹 컨트롤 활성화**를 [켜기]로 설정합니다. **편집**을 클릭하여 규칙 편집에 접근합니다. 미리 정의된 그룹을 수정하려면 범주 그룹 옆의 **편집**을 클릭하고, 새 URL 그룹을 추가하려면 URL 그룹 편집 옆의 **편집**을 클릭합니다.

안전한 브라우저

안전한 브라우저는 온라인 거래를 하는 동안 금융 데이터를 보호하도록 설계된 추가 보호 기능입니다.

ESET LiveGrid® 평판 시스템은 안전한 브라우저 보호가 제대로 작동하도록 하기 위해 활성화(기본적으로 활성화)되어야 합니다.

보안 브라우저 동작을 구성하려면 고급 설정 > **보호** > **보안 브라우저**를 엽니다.

다음의 보안 브라우저 구성 옵션을 선택할 수 있습니다.

- **모든 브라우저 보호** – 지원되는 모든 웹 브라우저는 보안 모드에서 시작합니다. 이를 통해 리디렉션 없이 하나의 보안 브라우저 창에서 인터넷을 검색하고, 인터넷 뱅킹에 접근하며, 온라인으로 구매 및 거래할 수 있습니다.

기본

브라우저 보호

모든 브라우저 보호를 활성화하여 모든 지원되는 웹 브라우저를 보안 모드로 시작합니다. 이를 통해 리디렉션 없이 하나의 보안 브라우저 창에서 인터넷을 검색하고, 인터넷 뱅킹에 접근하며, 온라인으로 구매 및 거래할 수 있습니다.

확장 설치 모드 – 드롭다운 메뉴에서 ESET로 보호되는 브라우저에 설치할 수 있는 확장을 선택할 수 있습니다. 확장 설치 모드를 변경해도 이전에 설치한 브라우저 확장에는 영향이 없습니다.

- **필수 확장** – 특정 브라우저 제조업체에서 개발한 가장 필수적인 확장만 해당
- **모든 확장** – 특정 브라우저에서 지원하는 모든 확장

보안되는 브라우저

향상된 메모리 보호 – 활성화되면 보안되는 브라우저의 메모리가 다른 프로세스에 따른 검사에서 보호됩니다.

키보드 보호 – 활성화된 경우, 키보드를 통해 보안 브라우저에 입력된 정보가 다른 애플리케이션에서 숨겨집니다. 이렇게 하면 키로거에 대한 보호 수준이 높아집니다.

브라우저의 녹색 프레임 – 비활성화된 경우, 정보를 제공하는 브라우저 내 알림과 브라우저 주변의 녹색 프레임이 숨겨집니다.

안전한 브라우저 대화형 경고 구성 – 대화형 경고 창을 열 수 있습니다.

> 경우에 따라서는 안전한 브라우저를 올바르게 시작하는 데 오류가 발생한 때에만 특정 대화형 경고가 표시됩니다. 자세한 내용은 대화형 경고를 참조하십시오.

브라우저 내 알림

보안 브라우저는 브라우저 내 알림 및 브라우저 프레임의 색상을 통해 현재 상태에 대해 알려줍니다.

브라우저 내 알림은 오른쪽 탭에 표시됩니다.

브라우저 내 알림을 확장하려면 ESET 아이콘을 클릭합니다. 알림을 최소화하려면 알림 텍스트를 클릭합니다. 알림과 녹색 브라우저 프레임을 닫으려면 닫기 아이콘을 클릭합니다.

> 정보를 제공하는 알림 및 녹색 브라우저 프레임만 닫을 수 있습니다.

브라우저 내 알림

알림 유형	상태
정보 알림 및 녹색 브라우저 프레임	최대 보호 성능이 보장되고, 브라우저 내 알림이 기본적으로 최소화됩니다.
경고 및 주황색 브라우저 프레임	보안 브라우저에서는 중요하지 않은 문제에 주의를 기울여야 합니다. 문제 또는 솔루션에 대한 자세한 내용은 브라우저 내 알림의 지침을 따르십시오.
보안 경고 및 빨간색 브라우저 프레임	브라우저가 보호되지 않습니다. 보호가 활성화되어 있는지 확인하려면 브라우저를 다시 시작합니다. 브라우저에 로드된 파일과의 충돌을 해결하려면 로그 파일 > **보안 브라우저** 보호를 열고 다음에 브라우저를 시작할 때 기록된 파일이 로드되지 않도록 하십시오. 문제가 지속되면 지식베이스 문서의 지침에 따라 ESET 기술 지원에 문의하십시오.

장치 제어

ESET Endpoint Security에서는 자동 장치(CD/DVD/USB 등) 제어 기능을 제공합니다. 이 모듈에서는 확장 필터/권한을 차단하거나 조정하고, 사용자가 지정된 장치에 접근하여 사용하는 기능을 정의할 수 있습니다. 이 모듈은 컴퓨터 관리자가 원치 않는 콘텐츠가 포함된 장치를 사용하지 못하도록 하려는 경우에 유용합니다.

지원되는 외부 장치:

- 디스크 저장소(HDD, USB 이동식 디스크)
- CD/DVD
- USB 프린터
- FireWire 저장소
- Bluetooth 장치
- 스마트 카드 리더
- 이미징 장치
- 모뎀
- LPT/COM 포트
- 휴대용 장치(미디어 플레이어, 스마트폰, 플러그 앤 플레이 장치 등과 같은 배터리 구동 장치)
- 모든 장치 유형

장치 제어 설정 옵션은 고급 설정 > **보호** > **장치 제어**에서 수정할 수 있습니다.

장치 제어 활성화 토글을 클릭하여 ESET Endpoint Security에서 장치 제어 기능을 활성화합니다. 이 변경 사항을 적용하려면 컴퓨터를 다시 시작해야 합니다. 장치 제어가 활성화되면 규칙 편집기 창에서 **규칙**을 정의할 수 있습니다.

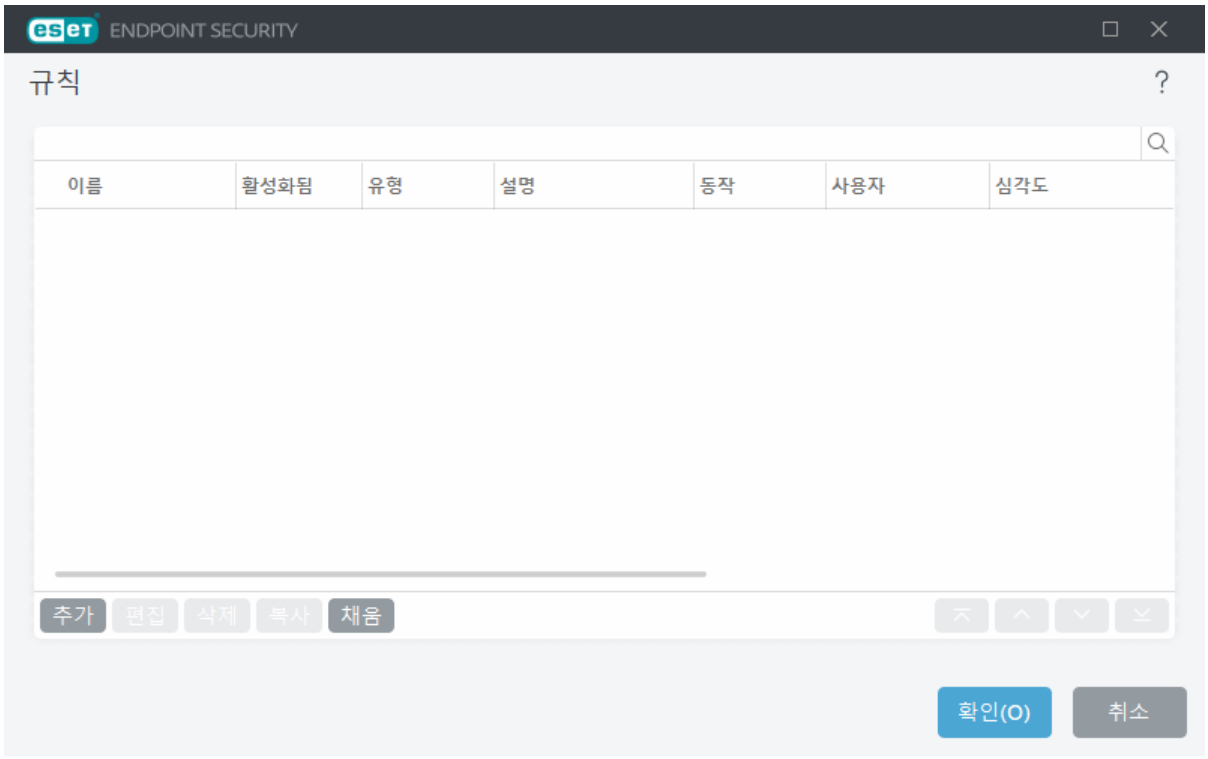
> 스케줄러를 사용하여 xml 파일에서 규칙이 있는 장치 제어 그룹을 가져올 수 있습니다. 자세한 내용과 단계별 가이드는 ESET 지식베이스 문서를 참조하십시오.

기존 규칙에 의해 차단된 장치를 삽입하면 알림 창이 표시되고 해당 장치에 대한 접근 권한이 부여되지 않습니다.

장치 제어 규칙 편집

장치 제어 규칙 편집 창에는 기존 규칙이 표시되며, 이 창에서 사용자가 컴퓨터에 연결할 외부 장치를 정밀하게 제어할 수 있습니다. 또한 장치 제어 규칙 추가를 참조하십시오.

다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
ESET 엔드포인트 제품을 사용하여 장치 제어 규칙 추가 및 수정



특정 장치를 사용자, 사용자 그룹 또는 규칙 구성에서 지정할 수 있는 여러 추가 파라미터에 따라 허용 또는 차단할 수 있습니다. 규칙 목록에는 이름, 외부 장치 유형, 컴퓨터에 외부 장치를 연결한 후 수행할 동작 및 로그 심각도 같은 규칙 설명이 여러 개 포함됩니다.

추가 또는 **편집**을 클릭하면 규칙을 관리할 수 있습니다. 규칙을 나중에 사용할 때까지 비활성화하려면 규칙 옆의 **활성화됨** 확인란을 선택 취소합니다. 규칙을 영구적으로 삭제하려면 규칙을 하나 이상 선택한 후 **삭제**를 클릭합니다.

복사 - 선택된 다른 규칙에 사용되는 미리 정의된 옵션으로 새 규칙을 생성합니다.

컴퓨터에 연결된 장치의 경우 이동식 미디어 장치 파라미터를 자동으로 채우려면 **채움**을 클릭합니다.

규칙은 우선 순위 순서대로 나열되며, 규칙의 우선 순위가 높을수록 맨 위에 가까이 나열됩니다. 규칙은 **맨 위로/위로/아래로/맨 아래로**를 클릭하여 이동할 수 있으며, 규칙을 개별적으로 또는 그룹으로 이동할 수 있습니다.

장치 제어 로그에는 장치 제어가 트리거된 모든 항목이 기록됩니다. 로그 항목은 ESET Endpoint Security 기본 프로그램 창의 **도구** > 로그 파일에서 볼 수 있습니다.

검색된 장치

채움 버튼은 장치 유형, 장치 공급업체, 모델 및 일련 번호(사용 가능한 경우)에 대한 정보와 함께 현재 연결된 모든 장치의 개요를 제공합니다.

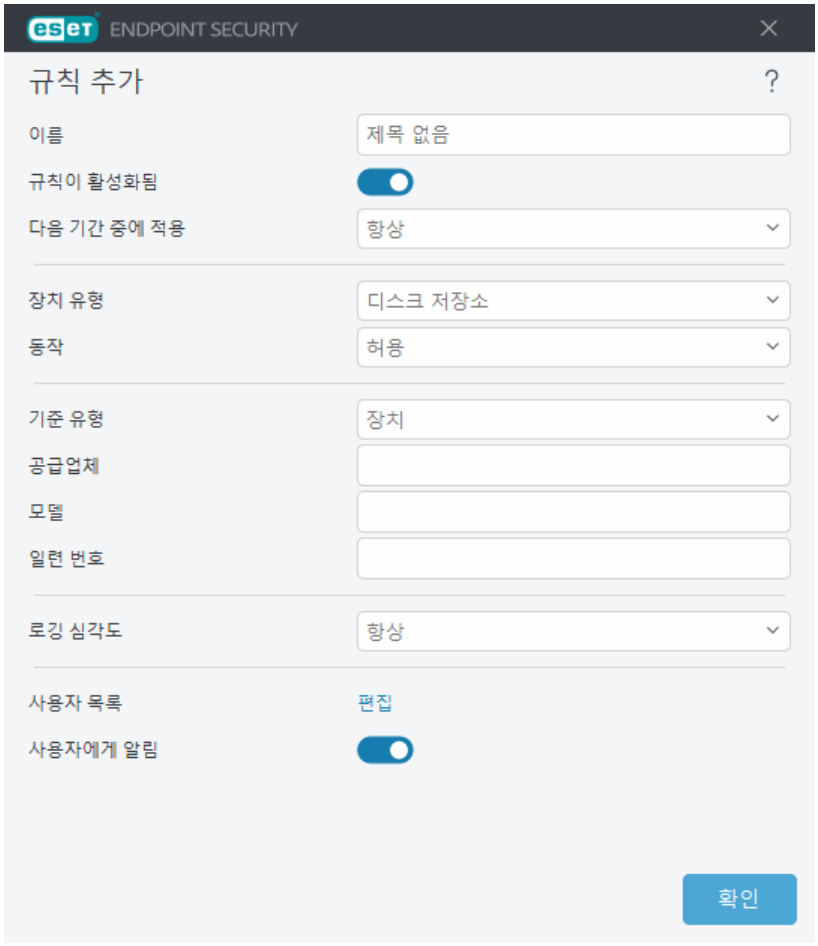
검색된 장치 목록에서 장치를 선택하고 **확인**을 클릭하여 정보가 미리 정의된 장치 제어 규칙을 추가합니다(모든 설정을 조정할 수 있음).

저전력(절전) 모드의 장치는 경고 아이콘으로 표시됩니다. **확인** 버튼을 활성화하고 이 장치에 대한 규칙을 추가하려면 다음을 수행합니다.

- 장치를 다시 연결합니다.
- 장치를 사용합니다(예: Windows에서 카메라 앱을 시작하여 웹캠의 절전 모드 해제).

장치 제어 규칙 추가

장치 제어 규칙은 규칙 기준을 충족하는 장치가 컴퓨터에 연결될 때 수행할 동작을 정의합니다.



좀 더 쉽게 식별할 수 있도록 **이름** 필드에 규칙 설명을 입력합니다. **규칙이 활성화됨** 옆에 있는 토글을 클릭하여 이 규칙을 비활성화하거나 활성화합니다. 이 옵션은 규칙을 영구적으로 제거하지 않으려는 경우에 유용할 수 있습니다.

다음 기간 중에 적용 – 특정 기간에 생성된 규칙을 적용할 수 있습니다. 드롭다운 메뉴에서 생성된 시간 슬롯을 선택합니다. 시간 슬롯에 대한 자세한 내용을 확인하십시오.

장치 유형

드롭다운 메뉴에서 외부 장치 유형을 선택합니다(디스크 저장소/휴대용 장치/Bluetooth/FireWire 등). 장치 유형 정보는 운영 체제에서 수집되며, 장치가 컴퓨터에 연결된 경우 시스템의 장치 관리자에서 확인할 수 있습니다. 저장 장치에는 USB나 FireWire를 통해 연결된 기존 메모리 카드 리더 또는 외부 디스크가 포함되며. 스마트 카드 리더에는 SIM 카드나 인증 카드처럼 내장된 통합 회로가 있는 모든 스마트 카드 리더가 포함됩니다. 이미징 장치 예로는 검사기나 카메라 등이 있습니다. 이러한 장치는 장치 동작에 대한 정보만 제

공하고 사용자에 대한 정보는 제공하지 않으므로 이미징 장치는 전체적으로만 차단할 수 있습니다.

사용자 목록 기능은 모뎀 장치 유형에는 사용할 수 없습니다. 규칙은 모든 사용자에게 적용되며 현재 사용자 목록은 삭제됩니다.

동작

비저장 장치에 대한 접근은 허용하거나 차단할 수만 있습니다. 이에 반해 저장 장치의 경우 해당 규칙을 통해 다음 권한 설정 중 하나를 선택할 수 있습니다.

- **허용** - 장치에 대한 모든 접근이 허용됩니다.
- **차단** - 장치에 대한 접근이 차단됩니다.
- **쓰기 블록** - 장치에 대한 읽기 접근만 허용됩니다.
- **경고** - 장치가 연결될 때마다 사용자는 장치가 허용되었는지 차단되었는지에 대한 알림을 수신하며, 로그 항목이 만들어집니다. 장치는 저장되지 않으므로 동일한 장치의 다음 연결 시 알림이 계속 표시됩니다.

모든 장치 유형에서 모든 동작(권한)을 사용할 수 있는 것은 아닙니다. 저장 유형의 장치일 경우 4개의 동작을 모두 사용할 수 있습니다. 하지만 비저장 장치의 경우 3개의 동작만 사용할 수 있습니다(예를 들어 Bluetooth의 경우 **쓰기 블록**을 사용할 수 없으므로 Bluetooth 장치를 허용, 차단하거나 이 장치에 경고만 할 수 있음).

기준 유형

장치 그룹이나 **장치**를 선택합니다.

아래에 표시된 추가 파라미터를 사용하여 여러 장치에 대한 규칙을 미세 조정할 수 있습니다. 모든 파라미터는 대/소문자를 구분하며 와일드카드(*, ?)를 지원합니다.

- **공급업체** - 공급업체 이름 또는 ID를 기준으로 필터링합니다.
- **모델** - 지정된 장치 이름입니다.
- **일련 번호** - 일반적으로 외부 장치에는 고유한 일련 번호가 있습니다. CD/DVD의 경우 CD 드라이브가 아닌 지정된 미디어의 일련 번호입니다.

이러한 파라미터가 정의되지 않은 경우 일치 작업 동안 규칙에서 이러한 필드를 무시합니다. 모든 텍스트 필드의 필터링 파라미터는 대/소문자를 구분하며 와일드카드를 지원합니다(물음표(?)는 단일 문자를 나타내고 별표(*)는 0개 이상의 문자로 구성된 문자열을 나타냄).

장치에 대한 정보를 보려면 해당 유형의 장치에 대한 규칙을 생성하고 장치를 컴퓨터에 연결한 후 장치 제어 로그에서 장치 상세 정보를 확인합니다.

로깅 심각도

- **항상** - 모든 이벤트를 기록합니다.
- **분석** - 프로그램을 미세 조정하는 데 필요한 로그 정보입니다.
- **정보** - 성공한 업데이트 메시지를 포함한 정보 메시지와 위의 모든 레코드를 기록합니다.
- **경고** - 심각한 오류와 경고 메시지를 기록하여 ERA Server에 전송합니다.
- **없음** - 로그가 기록되지 않습니다.

규칙을 **사용자 목록**에 추가하여 특정 사용자나 사용자 그룹으로 제한할 수 있습니다.

- **추가** - 원하는 사용자를 선택할 수 있는 **개체 유형: 사용자 또는 그룹** 대화 상자 창을 엽니다.
- **제거** - 선택한 사용자를 필터에서 제거합니다.

> **사용자 목록 제한 사항**
> 사용자 목록은 다음과 같은 특정 장치 유형이 있는 규칙에 대해 정의할 수 없습니다.
> - USB 프린터
> - Bluetooth 장치
> - 스마트 카드 리더
> - 이미징 장치
> - 모뎀
> - LPT/COM 포트

사용자에게 알림 – 기존 규칙에 의해 차단된 장치를 삽입하면 알림 창이 표시됩니다.

장치 그룹

> ⚠ 컴퓨터에 연결된 장치는 보안 위험을 유발할 수 있습니다.

장치 그룹 창은 두 부분으로 나뉘어 있습니다. 창의 오른쪽에는 각 그룹에 속한 장치 목록이 표시되고 창의 왼쪽에는 생성된 그룹이 표시됩니다. 오른쪽 창에 장치를 표시할 그룹을 선택합니다.

장치 그룹 창을 열고 그룹을 선택하면 목록에서 장치를 추가하거나 제거할 수 있습니다. 그룹에 장치를 추가하는 또 다른 방법은 파일에서 장치를 가져오는 것입니다. 또는 **채움** 버튼을 클릭하면 컴퓨터에 연결된 모든 장치가 **검색된 장치** 창에 나열됩니다. 채워진 목록에서 장치를 선택하고 **확인**을 클릭하여 그룹에 장치를 추가합니다.

제어 요소

추가 – 창에서 버튼을 클릭한 위치에 따라 기존 그룹에 이름이나 장치를 입력하여 그룹을 추가할 수 있습니다.

편집 - 선택한 그룹의 이름이나 장치 파라미터(공급업체, 모델, 일련 번호)를 수정할 수 있습니다.

삭제 - 버튼을 클릭한 창의 부분에 따라 선택한 그룹이나 장치를 삭제합니다.

가져오기 – 텍스트 파일에서 장치 목록을 가져옵니다. 텍스트 파일에서 장치를 가져오려면 올바른 서식이 필요합니다.

- 각 장치는 새 줄에서 시작됩니다.
- 각 장치에 대한 **공급업체**, **모델** 및 **일련 번호**가 있어야 하며, 쉼표로 분리되어야 합니다.

> ✓ 다음은 텍스트 파일 콘텐츠의 예입니다.
> ```
> Kingston,DT 101 G2,001CCE0DGRFC0371
> 04081-0009432,USB2.0 HD WebCam,20090101
> ```

내보내기 – 파일로 장치 목록을 내보냅니다.

채움 버튼은 장치 유형, 장치 공급업체, 모델 및 일련 번호(사용 가능한 경우)에 대한 정보와 함께 현재 연결된 모든 장치의 개요를 제공합니다.

스케줄러를 사용하여 xml 파일에서 규칙이 있는 장치 제어 그룹을 가져올 수 있습니다. 자세한 내용과 단계별 가이드는 ESET 지식베이스 문서를 참조하십시오.

장치 추가

오른쪽 창에서 추가를 클릭하여 기존 그룹에 장치를 추가합니다. 아래에 표시된 추가 파라미터를 사용하여 여러 장치에 대한 규칙을 미세 조정할 수 있습니다. 모든 파라미터는 대/소문자를 구분하며 와일드카드(*, ?)를 지원합니다.

- **공급업체** - 공급업체 이름 또는 ID를 기준으로 필터링합니다.
- **모델** - 지정된 장치 이름입니다.
- **일련 번호** - 일반적으로 외부 장치에는 고유한 일련 번호가 있습니다. CD/DVD의 경우 CD 드라이브가 아닌 지정된 미디어의 일련 번호입니다.
- **설명**—더 나은 구성을 위한 장치에 대한 설명입니다.

이러한 파라미터가 정의되지 않은 경우 일치 작업 동안 규칙에서 이러한 필드를 무시합니다. 모든 텍스트 필드의 필터링 파라미터는 대/소문자를 구분하며 와일드카드를 지원합니다(물음표(?)는 단일 문자를 나타내고 별표(*)는 0개 이상의 문자로 구성된 문자열을 나타냄).

확인을 클릭하여 변경 사항을 저장합니다. 변경 내용을 저장하지 않고 **장치 그룹** 창을 벗어나려면 **취소**를 클릭합니다.

장치 그룹을 생성한 후에는 생성한 장치 그룹에 대한 새 장치 제어 규칙을 추가하고 수행할 동작을 선택해야 합니다.

모든 장치 유형에서 모든 동작(권한)을 사용할 수 있는 것은 아닙니다. 저장 유형의 장치일 경우 4개의 동작을 모두 사용할 수 있습니다. 하지만 비저장 장치의 경우 3개의 동작만 사용할 수 있습니다(예를 들어 Bluetooth의 경우 **쓰기 블록**을 사용할 수 없으므로 Bluetooth 장치를 허용, 차단하거나 이 장치에 경고만 할 수 있음).

ThreatSense

ThreatSense는 복잡한 위협 검출 방법으로 구성되어 있습니다. 사전 예방 방식으로 검사를 수행합니다. 즉, 새로운 위협의 확산 초기에도 보호 기능을 제공합니다. 또한 함께 작동하여 시스템 보안 성능을 크게 향상시켜 주는 코드 분석, 코드 에뮬레이션, 일반 시그니처, 바이러스 시그니처 등의 방법을 조합해 사용합니다. 검사 엔진은 여러 데이터 스트림을 동시에 제어하여 효율성과 검출 비율을 최대화할 수 있습니다. ThreatSense 기술은 루트킷도 제거할 수 있습니다.

ThreatSense 엔진 설정 옵션을 사용하여 다음과 같은 여러 가지 검사 파라미터를 지정할 수 있습니다.

- 검사할 파일 형식 및 확장명
- 다양한 검출 방법의 조합
- 치료 수준 등

설정 창에 들어가려면 ThreatSense 기술을 사용하는 모듈(아래 참조)에 대한 고급 설정에서 **ThreatSense**을(를) 클릭합니다. 각 보안 시나리오에 따라 서로 다른 구성이 필요할 수 있습니다. 이를 염두에 두고, 다음 보호 모듈에 대해 ThreatSense를 개별적으로 구성할 수 있습니다.

- 실시간 파일 시스템 보호

- 유휴 상태 검사
- 시작 검사
- 문서 보호
- 이메일 클라이언트 보호
- 웹 브라우저 보호
- 컴퓨터 검사

ThreatSense 파라미터는 각 모듈에 맞게 고도로 최적화되어 있으므로 이를 수정하면 시스템 작동에 큰 영향을 줄 수 있습니다. 예를 들어 항상 런타임 패커를 검사하도록 파라미터를 변경하거나 실시간 파일 시스템 보호 모듈에서 고급 인공지능을 활성화하면 시스템 속도가 느려질 수 있습니다. 일반적으로 새로 생성된 파일에만 이러한 방법을 사용하여 검사합니다. 따라서 컴퓨터 검사를 제외한 모든 모듈에 대해서는 기본 ThreatSense 파라미터를 변경하지 않는 것이 좋습니다.

오브젝트 검사

이 섹션에서는 침입에 대해 검사할 컴퓨터 구성 요소 및 파일을 정의할 수 있습니다.

운영 메모리 - 시스템의 운영 메모리를 공격하는 위협이 있는지 검사합니다.

부트 영역/UEFI – 마트터 부트 레코드에 악성코드가 있는지 부트 영역을 검사합니다. UEFI에 대한 자세한 내용은 용어집을 참조하십시오.

이메일 파일 - 프로그램에서 지원되는 확장명은 DBX (Outlook Express) 및 EML입니다.

압축파일 – 프로그램에서 지원되는 확장명은 ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE 등입니다.

자체 압축 해제 파일 - 자체 압축 해제 파일(SFX)은 자체적으로 압축을 해제할 수 있는 파일입니다.

런타임 패커 - 런타임 패커는 표준 압축파일 형식과 달리 실행 후에 메모리에 압축이 풀립니다. 검사기는 표준 정적 패커(UPX, yoda, ASPack, FSG 등) 외에도 코드 에뮬레이션을 통해 몇 가지 추가 패커 유형을 인식할 수 있습니다.

검사 옵션

시스템에서 침입을 검사할 때 사용할 방법을 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.

인공지능 - 인공지능은 프로그램의 악의적 활동을 분석하는 알고리즘입니다. 이 기술의 가장 큰 장점은 이전 버전의 검색 엔진 생성 당시 존재하지 않았거나 해당 엔진에서 인식하지 못한 악성 소프트웨어를 식별할 수 있다는 것입니다. 그러나 악성이 아닌 소프트웨어를 악성으로 보고할 수 있다는 단점이 있습니다(가능성은 매우 낮음).

고급 휴리스틱/DNA 시그니처 - 고급 인공지능은 ESET에서 개발한 고유 인공지능 알고리즘으로, 컴퓨터 웜 및 트로이 목마 검출용으로 최적화되고 높은 수준의 프로그래밍 언어로 작성되었습니다. 고급 인공지능을 사용하면 ESET 제품의 위협 검출 기능이 크게 향상됩니다. 시그니처는 바이러스를 안정적으로 검출 및 식별할 수 있습니다. 자동 업데이트 시스템을 통해 위협 검출을 위해 새 시그니처를 몇 시간 이내에 사용할 수 있습니다. 그러나 시그니처는 인식 가능한 바이러스 또는 이러한 바이러스의 약간 수정된 버전만 검출할 수 있다는 단점이 있습니다.

치료

치료 설정에 따라 개체 치료 중 ESET Endpoint Security의 동작이 결정됩니다.

제외

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로. 파일의 형식과 내용을 정의합니다. 이 ThreatSense 설정 섹션에서는 검사할 파일 형식을 정의할 수 있습니다.

기타

수동 컴퓨터 검사에 대해 ThreatSense 엔진 설정을 구성할 때 **기타** 섹션에서 다음과 같은 옵션도 제공됩니다.

ADS(대체 데이터 스트림) 검사 - NTFS 파일 시스템에서 사용하는 대체 데이터 스트림은 일반 검사 기술로는 표시되지 않는 파일 및 폴더 연결입니다. 대체 데이터 스트림으로 가장하여 검출을 피하려고 하는 침입이 많이 있습니다.

순위가 낮은 백그라운드 검사 실행 - 각 검사 시퀀스는 일정량의 시스템 리소스를 사용합니다. 시스템 리소스에 대한 로드가 높은 프로그램을 사용하는 경우에는 순위가 낮은 백그라운드 검사를 활성화하여 리소스를 절약하고 이러한 절약된 리소스를 애플리케이션에 사용할 수 있습니다.

모든 개체 기록 – 검사 로그는 감염되지 않았더라도 자체 압축 해제 파일의 검사된 모든 파일을 표시합니다(이로 인해 검사 로그 데이터가 많이 생성되고 검사 로그 파일 크기가 커질 수 있음).

스마트 최적화 활성화 - 스마트 최적화를 활성화하면 가장 효율적인 검사 수준을 유지하는 동시에 최고 검사 속도를 유지하기 위한 최적의 설정이 사용됩니다. 다양한 보호 모듈이 다양한 검사 방법을 활용하고 해당 방법을 특정 파일 형식에 적용하는 방식으로 지능적 검사를 수행합니다. 스마트 최적화를 비활성화하면 검사를 수행할 때 특정 모듈의 ThreatSense 코어에서 사용자가 정의한 설정만 적용됩니다.

마지막 접근시의 타임스탬프 유지 - 검사한 파일의 원래 접근 시간을 데이터 백업 시스템 등에 사용할 수 있도록 업데이트하지 않고 그대로 유지하려면 이 옵션을 선택합니다.

제한

제한 섹션에서는 최대 개체 크기와 검사할 중복 압축 수준을 지정할 수 있습니다.

개체 설정

최대 개체 크기 - 검사할 개체의 최대 크기를 정의합니다. 그러면 지정된 안티바이러스 모듈에서 지정한 크기보다 작은 개체만 검사합니다. 큰 개체를 검사에서 제외해야 하는 특별한 이유가 있는 고급 사용자만 이 옵션을 변경해야 합니다. 기본값은 제한 없음입니다.

최대 개체 검사 시간(초) – 컨테이너 개체의 파일을 검사하기 위한 최대 시간 값(예: RAR/ZIP 압축파일 또는 첨부 파일이 여러 개 있는 이메일)을 정의합니다. 이 설정은 독립 실행형 파일에 적용되지 않습니다. 사용자 정의 값을 입력하고 해당 시간이 경과한 경우, 컨테이너 개체에서 각 파일 검사가 완료되었는지 여부에 관계없이 가능한 한 빨리 검사가 중지됩니다. 대용량 파일이 있는 압축파일의 경우, 압축파일에서 파일이 압축 해제되는 시간보다 더 빨리 검사가 중지되지는 않습니다(예: 사용자 정의 변수가 3초이지만 파일 압축 해제는 5초가 소요되는 경우). 압축파일의 나머지 파일은 해당 시간이 경과하면 검사되지 않습니다. 더 큰 압축파일 등의 검사 시간을 제한하려면 **최대 개체 크기**와 **압축파일 내 파일의 최대 크기**를 사용합니다(가능한

보안 위험으로 인해 권장되지 않음). 기본값은 제한 없음입니다.

압축파일 검사 설정

다중 압축 수준 - 최대 압축파일 검사 수준을 지정합니다. 기본값: 10.

압축파일 내 파일의 최대 크기 - 이 옵션을 사용하면 검사할 압축파일에 포함된 파일의 최대 파일 크기(압축 해제 시)를 지정할 수 있습니다. 최대값은 3GB입니다.

> 일반적인 상황에서는 기본값을 수정할 필요가 없으므로 기본값을 변경하지 않는 것이 좋습니다.

치료 수준

원하는 보호 모듈에 대한 치료 수준 설정을 변경하려면 **ThreatSense**(예: **실시간 파일 시스템 보호**)을(를) 확장한 다음 드롭다운 메뉴에서 **치료 수준**을 선택합니다.

ThreatSense의 수정(즉, 치료) 수준은 다음과 같습니다.

ESET Endpoint Security의 수정 사항

치료 수준	설명
항상 탐지 수정	최종 사용자가 개입하지 않고 개체를 치료하는 동안 탐지를 수정하려고 시도합니다. 드물게(예: 시스템 파일) 탐지를 수정할 수 없는 경우 보고된 개체가 원래 위치에 남아 있게 됩니다. **항상 탐지 수정**은 관리되는 환경에서 권장되는 기본 설정입니다.
안전하면 탐지 수정, 그렇지 않으면 유지	최종 사용자가 개입하지 않고 개체를 치료하는 동안 탐지를 수정하려고 시도합니다. 경우(예: 치료된 파일과 감염된 파일이 모두 있는 시스템 파일 또는 압축파일)에 따라 탐지를 수정할 수 없는 경우 보고된 개체가 원래 위치에 남아 있게 됩니다.
안전하면 탐지 수정, 그렇지 않으면 확인	개체를 치료하는 동안 탐지를 수정하려고 시도합니다. 경우에 따라 동작을 수행할 수 없는 경우 최종 사용자는 대화형 경고를 수신한 후 수정 동작(예: 삭제 또는 무시)을 선택해야 합니다. 이 설정은 대부분의 경우에 권장됩니다.
최종 사용자에게 항상 확인	최종 사용자는 개체를 치료하는 동안 대화 창을 수신한 후 수정 동작(예: 삭제 또는 무시)을 선택해야 합니다. 이 수준은 탐지 이벤트에서 취해야 할 단계를 알고 있는 고급 사용자를 위한 것입니다.

검사에서 제외된 파일 확장명

제외된 파일 확장명은 ThreatSense 파라미터의 일부입니다. 제외된 파일 확장명을 구성하려면 ThreatSense 기술을 사용하는 모듈에 대한 고급 설정에서 **ThreatSense**를 클릭합니다.

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로. 파일의 형식과 내용을 정의합니다. 이 ThreatSense 설정 섹션에서는 검사할 파일 형식을 정의할 수 있습니다.

> 프로세스 제외, HIPS 제외 또는 파일/폴더 제외를 혼동하지 마십시오.

기본적으로 모든 파일이 검사됩니다. 검사에서 제외되는 파일 목록에 원하는 확장명을 추가할 수 있습니다.

특정 파일 형식을 검사할 때 특정 확장명을 사용 중인 프로그램이 제대로 실행되지 않으면 파일을 검사에서 제외해야 하는 경우가 있습니다. 예를 들어 Microsoft Exchange 서버를 사용할 때는 `.edb`, `.eml` 및 `.tmp` 확장명을 제외하는 것이 좋습니다.

새 확장명을 목록에 추가하려면 **추가**를 클릭합니다. 빈 필드에 확장명(예 tmp)을 입력하고 **확인**을 클릭합니다. **여러 값 입력**을 선택하면 여러 파일 확장명을 줄, 쉼표 또는 세미콜론으로 구분하여 추가할 수 있습니다(예: 드롭다운 메뉴에서 분리 기호로 **세미콜론**을 선택하고 `edb;eml;tmp`를 입력).
특수 기호 ?(물음표)를 사용할 수 있습니다. 물음표는 임의의 기호를 나타냅니다(예: `?db`).

Windows 운영 체제에서 파일의 정확한 확장명(있는 경우)을 보려면 **Windows 탐색기 > 보기**(탭)에서 **파일 이름 확장명** 확인란을 선택해야 합니다.

추가 ThreatSense 파라미터

이러한 설정을 편집하려면 고급 설정 > **보호 > 실시간 파일 시스템 보호 > 추가 ThreatSense 파라미터**를 엽니다.

새로 생성 및 수정한 파일에 대한 추가 ThreatSense 파라미터

새로 생성 및 수정한 파일의 감염 가능성은 기존 파일보다 비교적 높습니다. 이 같은 이유로 프로그램에서 추가 검사 파라미터를 통해 이러한 파일을 확인합니다. ESET Endpoint Security에서는 탐지 엔진 업데이트를 공개하기 전에 시그니처 기반 검사 방법과 결합하여 새로운 위협을 탐지할 수 있는 고급 휴리스틱을 사용합니다.

새로 생성한 파일뿐만 아니라 **자체 압축 해제 파일**(.sfx) 및 **런타임 패커**(내부적으로 압축된 실행 파일)에서도 검사가 수행됩니다. 기본적으로 압축 파일은 10번째 다중 압축 수준까지 검사되며, 실제 크기에 관계없이 확인됩니다. 압축 파일 검사 설정을 수정하려면 **기본 압축 파일 검사 설정**을 선택 취소합니다.

실행된 파일에 대한 추가 ThreatSense 파라미터

파일 실행 시 고급 인공지능 - 기본적으로 파일이 실행될 때 고급 인공지능이 사용됩니다. 활성화된 경우 스마트 최적화 및 ESET LiveGrid®를 활성화된 상태로 유지하여 시스템 성능에 미치는 영향을 완화하는 것이 좋습니다.

이동식 미디어에서 파일 실행 시 고급 인공지능 - 고급 인공지능은 가상 환경에서 코드를 에뮬레이트하고 이동식 미디어로부터의 코드 실행이 허용되기 전에 동작을 평가합니다.

도구

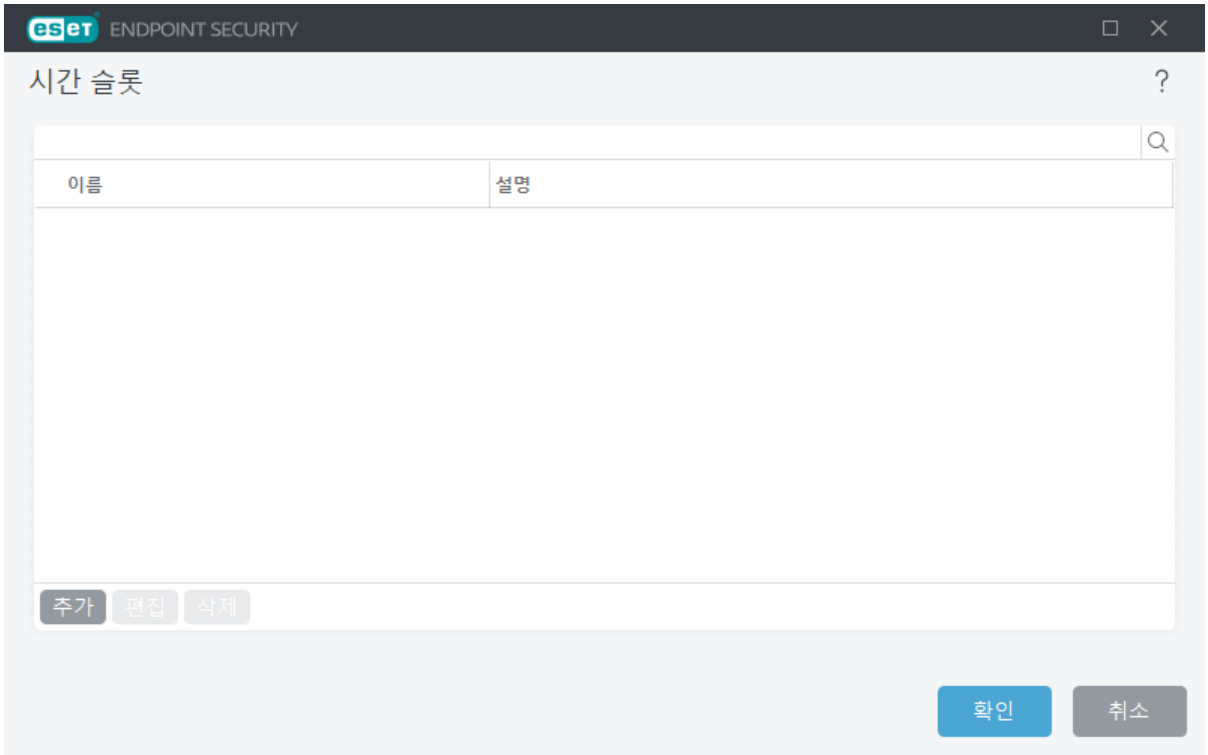
고급 설정 > **도구**에서 추가 보안 성능을 제공하고 ESET Endpoint Security 관리를 간소화하는 데 도움이 되는 기능에 대한 고급 설정을 구성할 수 있습니다.

- 시간 슬롯
- Microsoft Windows 업데이트
- ESET CMD
- 원격 모니터링 및 관리
- 라이선스 갱신 확인
- 로그 파일

- 프레젠테이션 모드
- 분석

시간 슬롯

시간 슬롯을 생성한 다음 **장치 제어** 및 **웹 컨트롤**에 대한 규칙에 할당할 수 있습니다. **시간 슬롯** 설정은 고급 설정 > **도구**에서 확인할 수 있습니다. 여기에서 일반적으로 사용되는 시간 슬롯(예: 작업 시간, 주말 등)을 정의할 수 있습니다. 시간 기반 검사를 지원하는 관련된 모든 규칙 유형에 적용할 수 있습니다.



시간 슬롯을 생성하려면 다음 단계를 완료합니다.

1. **편집** > **추가**를 클릭합니다.
2. 시간 슬롯의 이름과 **설명**을 입력하고 **추가**를 클릭합니다.
3. 요일과 시간 슬롯의 시작/종료 시간을 지정하거나 **종일**을 선택합니다.
4. **확인**을 클릭하여 확인합니다.

단일 시간 슬롯은 요일과 시간에 따라 하나 이상의 시간 범위로 지정할 수 있습니다. 시간 슬롯이 생성되면 장치 제어 규칙 편집 창 또는 웹 컨트롤 규칙 편집 창의 **다음 기간 중에 적용** 드롭다운 메뉴에 표시됩니다.

Microsoft Windows 업데이트

Windows 업데이트 기능은 사용자를 악성 소프트웨어로부터 보호하기 위한 중요한 구성 요소입니다. 이러한 이유로 Microsoft Windows 업데이트를 사용할 수 있게 되는 즉시 설치해야 합니다. ESET Endpoint Security에서는 지정한 수준에 따라 누락된 업데이트를 알려 줍니다. 다음과 같은 수준을 사용할 수 있습니다.

- **업데이트 확인 안함** - 시스템 업데이트를 다운로드할 수 없습니다.
- **옵션 업데이트** - 낮은 순위 이상으로 지정된 업데이트를 다운로드할 수 있습니다.
- **권장 업데이트** - 일반 수준 이상으로 지정된 업데이트를 다운로드할 수 있습니다.

- **중요 업데이트** - 주요 수준 이상으로 지정된 업데이트를 다운로드할 수 있습니다.
- **필수 업데이트** - 필수 업데이트만 다운로드할 수 있습니다.

변경 내용을 저장하려면 **확인**을 클릭합니다. 업데이트 서버의 상태를 확인한 후 시스템 업데이트 창이 표시됩니다. 따라서 변경 내용을 저장한 후에 시스템 업데이트 정보가 즉시 표시되지 않을 수 있습니다.

대화 상자 창 - 운영 체제 업데이트

몇 가지 운영 체제 업데이트를 사용할 수 있는 경우 ESET Endpoint Security 홈 창에 알림이 표시됩니다. 시스템 업데이트 창을 열려면 **추가 정보**를 클릭합니다.

시스템 업데이트 창에는 다운로드하여 설치할 수 있는 업데이트 목록이 표시됩니다. 업데이트 이름 옆에는 업데이트 유형이 표시됩니다.

추가 정보가 있는 업데이트 정보 창을 표시하려면 아무 업데이트 행이나 두 번 클릭합니다.

시스템 업데이트 실행을 클릭하여 나열된 모든 운영 체제 업데이트를 다운로드하고 설치합니다.

업데이트 정보

시스템 업데이트 창에는 다운로드하여 설치할 수 있는 업데이트 목록이 표시됩니다. 업데이트 이름 옆에는 업데이트 순위 수준이 표시됩니다.

운영 체제 업데이트 다운로드 및 설치를 시작하려면 **시스템 업데이트 실행**을 클릭합니다.

추가 정보가 포함된 새로운 창을 표시하려면 업데이트 행을 오른쪽 마우스 버튼으로 클릭하고 **정보 표시**를 클릭합니다.

ESET CMD

이 기능은 고급 ecmd 명령을 활성화하는 기능으로. 명령줄(ecmd.exe)을 사용하여 설정을 내보내고 가져올 수 있습니다. 지금까지는 GUI를 사용해서만 설정을 내보낼 수 있었습니다. 이제 ESET Endpoint Security 구성을 *.xml* 파일로 내보낼 수 있습니다.

ESET CMD를 활성화하면 다음과 같은 두 개의 인증 방법을 사용할 수 있습니다.

- **없음** – 인증하지 않습니다. 이 방법을 사용하면 지문이 없는 구성을 가져올 수 있으며, 이 경우 잠재적인 위험이 뒤따르므로 이 방법은 권장되지 않습니다.
- **고급 설정 비밀번호** – *.xml* 파일에서 구성을 가져오려면 비밀번호가 필요하며, 이 경우 .xml 파일에 지문이 있어야 합니다(자세한 내용은 *.xml* 구성 파일 지문 생성 참조). 새 구성을 가져오려면 접근 설정에 지정된 비밀번호를 입력해야 합니다. 접근 설정이 활성화되지 않은 경우 비밀번호가 일치하지 않거나 *.xml* 구성 파일에 지문이 생성되지 않거나 구성을 가져오지 않게 됩니다.

ESET CMD가 활성화되면 명령줄을 사용하여 ESET Endpoint Security 구성을 내보내거나 가져올 수 있습니다. 자동화를 위해 이 작업을 수동으로 수행하거나 스크립트를 생성할 수 있습니다.

고급 ecmd 명령을 사용하려면 관리자 권한으로 이 명령을 실행하거나 **관리자 권한으로 실행**을 사용하여 Windows 명령 프롬프트(cmd)를 열어야 합니다. 그렇지 않으면 **Error executing command** 메시지가 수신됩니다. 또한 구성을 내보낼 때 대상 폴더가 있어야 합니다. 내보내기 명령은 ESET CMD 설정이 해제된 상태에서도 작동합니다.

고급 ecmd 명령은 로컬에서만 실행할 수 있습니다. ecmd 명령을 일시 중지하는 것은 ESET PROTECT를 사용하여 클라이언트 작업 **명령 실행**을 통해서만 실행할 수 있습니다.

설정 내보내기 명령:
`ecmd /getcfg c:\config\settings.xml`
설정 가져오기 명령:
`ecmd /setcfg c:\config\settings.xml`

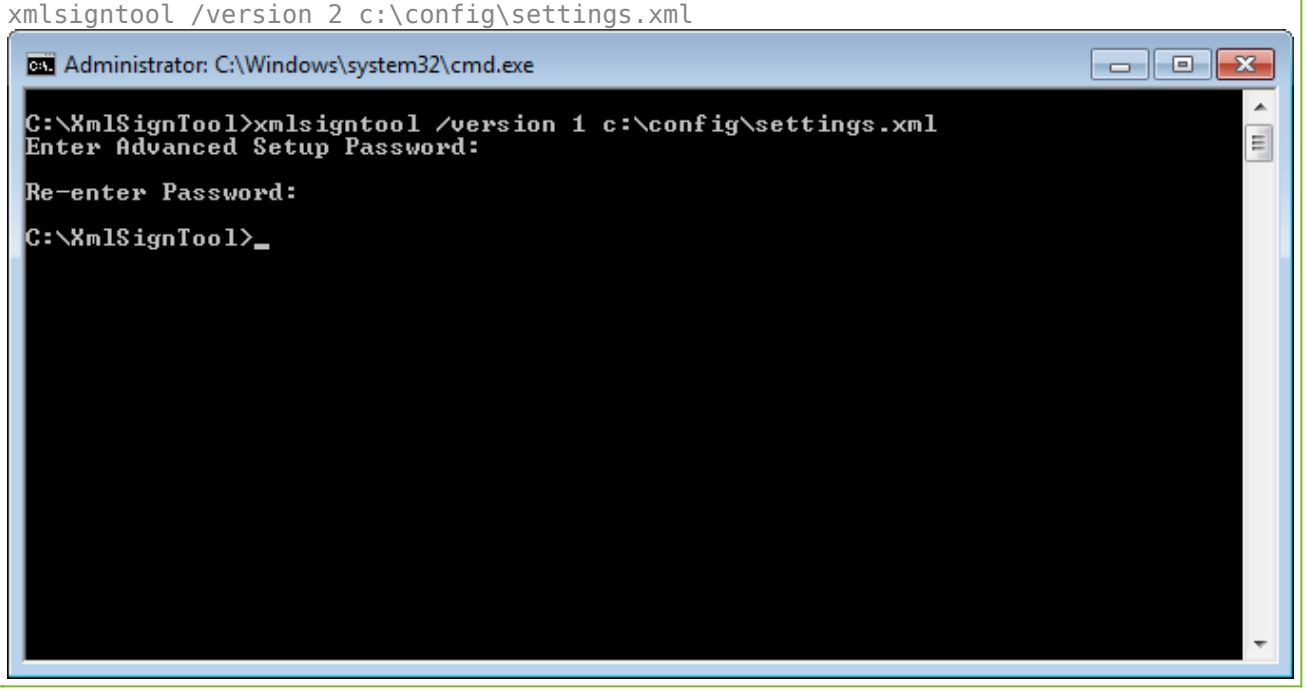
.xml 구성 파일에 지문 생성:

1. XmlSignTool 실행 파일을 다운로드합니다.
2. **관리자 권한으로 실행**을 사용하여 Windows 명령 프롬프트(cmd)를 엽니다.
3. `xmlsigntool.exe`의 저장 위치로 이동합니다.
4. 명령을 실행하여 *.xml* 구성 파일에 지문을 생성합니다(사용법: `xmlsigntool /version 1|2 <xml_file_path>`

`/version` 파라미터의 값은 ESET Endpoint Security의 버전에 따라 다릅니다. 버전 7 이상인 경우 `/version 2`를 사용하십시오.

5. XmlSignTool에 비밀번호를 입력하라는 메시지가 표시되면 고급 설정 비밀번호를 입력하고 확인 비밀번호를 다시 입력합니다. 이제 *.xml* 구성 파일에 지문이 생성되었으며, 이 구성 파일을 통해 비밀번호 인증 방법을 사용하여 ESET CMD로 다른 ESET Endpoint Security 인스턴스를 가져올 수 있습니다.

내보낸 구성 파일에 지문을 생성하는 명령:
`xmlsigntool /version 2 c:\config\settings.xml`



접근 설정 비밀번호가 변경되고 이전 비밀번호로 이전에 지문이 생성된 구성을 가져오려면 현재 비밀번호를 사용하여 *.xml* 구성 파일에 다시 지문을 생성해야 합니다. 그러면 구성을 가져오기 전에 ESET Endpoint Security을 실행하는 다른 컴퓨터에서 구성을 내보내지 않고도 이전 구성 파일을 사용할 수 있습니다.

⚠ 인증을 사용하지 않고 ESET CMD를 활성화할 경우 지문이 없는 구성을 가져올 수 있으므로 이 작업은 권장되지 않습니다. 사용자에 의한 무단 수정을 방지하려면 고급 설정 > **사용자 인터페이스** > **접근 설정**에서 비밀번호를 설정합니다.

ecmd 명령 목록

개별 보안 기능은 ESET PROTECT 클라이언트 작업 실행 명령을 사용하여 활성화하고 일시적으로 비활성화할 수 있습니다. 명령은 정책 설정을 재정의하지 않으며 일시 중지된 설정은 명령이 실행된 후 또는 장치 재부팅 후 원래 상태로 되돌아갑니다. 이 기능을 사용하려면 명령줄이 동일한 이름의 필드에서 실행되도록 지정하십시오.

다음은 각 보안 기능에 대한 명령 목록입니다.

보안 기능	임시 일시 중지 명령	활성화 명령
실시간 파일 시스템 보호	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
문서 보호	ecmd /setfeature document pause	ecmd /setfeature document enable
장치 제어	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
프리젠테이션 모드	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
개인 방화벽	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
네트워크 공격 보호(IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
봇넷 보호	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
웹 컨트롤	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
웹 브라우저 보호	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
이메일 클라이언트 보호	ecmd /setfeature email pause	ecmd /setfeature email enable
이메일 클라이언트 안티스팸	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
안티피싱 보호	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

원격 모니터링 및 관리

원격 모니터링 및 관리(RMM)는 관리 서비스 공급자가 접근할 수 있는, 로컬에 설치된 에이전트를 사용하여 소프트웨어 시스템 을 감독하고 제어하는 프로세스입니다.

ERMM - RMM용 ESET 플러그인

- 기본 ESET Endpoint Security 설치에는 디렉터리 내 엔드포인트 애플리케이션에 있는 `ermm.exe` 파일이 포함됩니다.
  C:\Program Files\ESET\ESET Security\ermm.exe
- `ermm.exe`는 RMM 플러그인과의 통신 및 엔드포인트 제품 관리를 수월하게 하도록 설계된 명령줄 유틸리티입니다.
- `ermm.exe`는 RMM 서버에 연결된 RMM 에이전트와 통신하는 RMM 플러그인과 데이터를 교환합니다. 기본적으로 ESET RMM 도구는 비활성화되어 있습니다.

추가 리소스

- ERMM 명령줄
- ERMM JSON 명령 목록

- 원격 모니터링 및 관리를 활성화하는 방법ESET Endpoint Security

타사 RMM 솔루션용 ESET Direct Endpoint Management 플러그인

RMM 서버는 타사 서버에서 서비스로 실행됩니다. 자세한 정보는 다음과 같은 ESET Direct Endpoint Management 온라인 사용자 설명서를 참조하십시오.

- ConnectWise Automate용 ESET Direct Endpoint Management 플러그인
- DattoRMM용 ESET Direct Endpoint Management 플러그인
- Solarwinds N-Central용 ESET Direct Endpoint Management
- NinjaRMM용 ESET Direct Endpoint Management

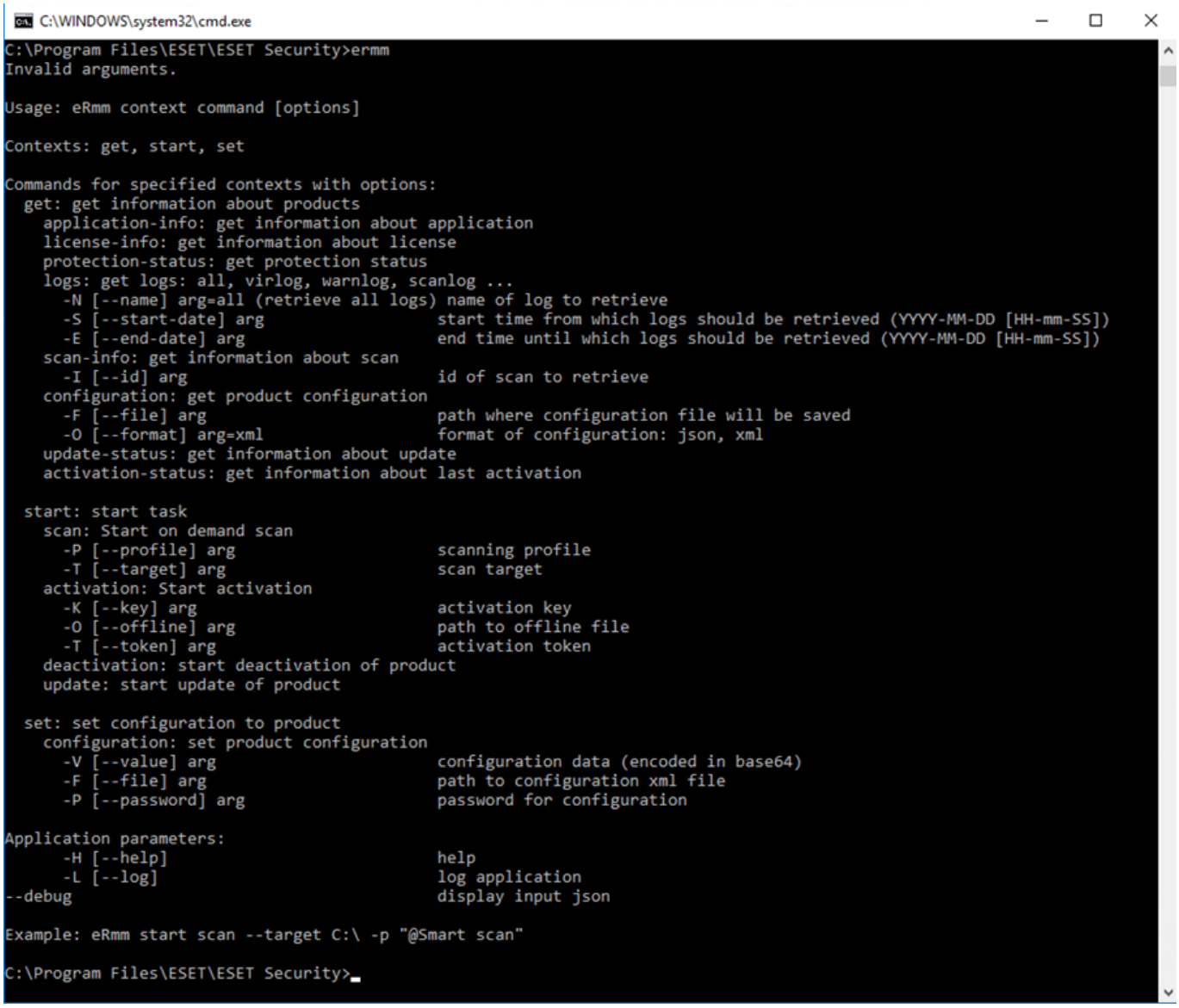
ERMM 명령줄

원격 모니터링 관리는 명령줄 인터페이스를 사용하여 실행됩니다. 기본 ESET Endpoint Security 설치에는 *c:\Program Files\ESET\ESET Security* 디렉터리 내 엔드포인트 애플리케이션에 있는 ermm.exe 파일이 포함됩니다.

관리자 권한으로 명령 프롬프트(cmd.exe)를 실행하고 앞서 언급한 경로로 이동합니다(명령 프롬프트를 열려면 키보드에서 Windows 버튼 + R을 누른 다음 실행 창에 cmd를 입력하고 Enter 키를 누름).

명령 구문은 `ermm context command [options]`입니다.

로그 파라미터는 대/소문자를 구분합니다.



ermm.exe는 Get, Start 및 Set의 세 가지 기본 컨텍스트를 사용합니다. 아래 표에서 명령 구문의 예를 확인할 수 있습니다. 명령 열의 링크를 클릭하여 추가 옵션, 파라미터 및 사용 예를 확인합니다. 명령이 성공적으로 실행되면 출력 부분(결과)이 표시됩니다. 입력 부분을 보려면 명령의 끝에 `--debug` 파라미터를 추가합니다.

컨텍스트	명령	설명
get		**제품 정보 가져오기**
	application-info	제품 정보 가져오기
	license-info	라이선스 정보 가져오기
	protection-status	보호 상태 가져오기
	logs	로그 가져오기
	scan-info	검사 실행에 대한 정보 가져오기
	configuration	제품 구성 가져오기
	update-status	업데이트에 대한 정보 가져오기
	activation-status	마지막 활성화에 대한 정보 가져오기
start		**시작 작업**
	scan	요청 시 검사 시작
	activation	제품 활성화 시작

컨텍스트	명령	설명
	deactivation	제품 비활성화 시작
	update	제품 업데이트 시작
set		**제품 옵션 설정**
	configuration	제품 구성 설정

모든 명령의 출력 결과에서 가장 먼저 표시되는 정보는 결과 ID입니다. 결과 정보를 더 잘 이해하려면 아래 ID 표를 확인하십시오.

오류 ID	오류	설명
0	Success	
1	Command node not present	"명령" 노드가 입력 json에 존재하지 않음
2	Command not supported	명령이 지원되지 않습니다.
3	General error executing the command	명령 실행 중 오류 발생
4	Task already running	요청한 작업이 이미 실행 중이라 시작되지 않았습니다.
5	Invalid parameter for command	잘못된 사용자 입력입니다.
6	Command not executed because it's disabled	RMM이 고급 설정에서 사용하도록 설정되지 않았거나 관리자로 시작되지 않음

ERMM JSON 명령 목록

get protection-status

Get the list of application statuses and the global application status

명령줄

```
ermm.exe get protection-status
```

파라미터

None

예

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

Get information about the installed application

명령줄

```
ermm.exe get application-info
```

파라미터

None

예

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

명령줄

```
ermm.exe get license-info
```

파라미터

None

예

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

명령줄

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

파라미터

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

예

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

명령줄

```
ermm.exe get activation-status
```

파라미터

None

예

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

실행 중인 검사에 대한 정보를 가져옵니다.

명령줄

```
ermm.exe get scan-info
```

파라미터

없음

예

호출

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

결과

```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

명령줄

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

파라미터

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

예

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

명령줄

```
ermm.exe get update-status
```

파라미터

None

예

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

명령줄

```
ermm.exe start scan --profile "profile name" --target "path"
```

파라미터

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

예

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

명령줄

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

파라미터

Name	Value
key	Activation key

offline	Path to offline file

예

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

명령줄

```
ermm.exe start deactivation
```

파라미터

None

예

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

명령줄

```
ermm.exe start update
```

파라미터

None

예

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

명령줄

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

파라미터

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

예

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

라이선스 간격 확인

ESET Endpoint Security 제품은 ESET 라이선스 서버에 자동으로 연결해야 합니다. 고급 설정 > **도구** > **라이선스**에서 ESET 라이선스 서버에 대한 연결 수를 제한할 수 있습니다. 기본적으로 **간격 확인**은 **자동**으로 설정되어 있으며, 연결은 매시간 몇 번씩 설정됩니다. 네트워크 트래픽이 증가하는 경우 **간격 확인**을 **제한됨**으로 변경하여 오버로드를 줄입니다. **제한됨**이 선택되면 ESET Endpoint Security에서 하루에 한 번만 또는 컴퓨터가 재시작될 때만 라이선스 서버를 확인합니다.

간격 확인 설정이 **제한됨**으로 설정되면 ESET HUB/ESET MSP Administrator를 통해 완료된 모든 라이선스 관련 변경이 ESET Endpoint Security 설정에 적용되는 데 최대 1일이 걸릴 수 있습니다.

로그 파일

고급 설정 > **도구** > **로그 파일**에서 ESET Endpoint Security 로깅 구성에 접근할 수 있습니다. 로그 섹션에서는 로그 관리 방법을 정의합니다. 프로그램에서는 하드 디스크 공간을 절약하기 위해 오래된 로그를 자동으로 삭제합니다. 다음과 같은 옵션을 지정하여 로그 파일에 사용할 수 있습니다.

최소 로그 기록 상세 수준 - 기록할 이벤트의 최소 상세 수준을 지정합니다.

- **분석** - 위의 프로그램과 모든 레코드를 미세 조정하는 데 필요한 정보를 기록합니다.
- **정보** - 성공한 업데이트 메시지를 포함한 정보 메시지와 위의 모든 레코드를 기록합니다.
- **경고** - 심각한 오류 및 경고 메시지를 기록합니다.
- **오류** - "파일을 다운로드하는 중 오류 발생"과 같은 오류 및 심각한 오류가 기록됩니다.
- **위험** - 심각한 오류(안티바이러스 보호, 기본 제공 방화벽 시작 오류 등)만 기록합니다.

분석 상세 수준을 선택하면 차단된 모든 연결이 기록됩니다.

다음 기간이 지난 기록 자동 삭제 필드에 지정된 일수보다 오래된 로그 항목이 자동으로 삭제됩니다.

자동으로 로그 파일 최적화 - 이 옵션을 선택하면 조각화 비율이 **사용되지 않는 기록 수가 (%)을(를) 초과하는 경우** 필드에 지정된 비율보다 높으면 로그 파일이 자동으로 조각 모음됩니다.

로그 파일 조각 모음을 시작하려면 **최적화**를 클릭합니다. 비어 있는 모든 로그 항목은 제거되므로 성능 및 로그 처리 속도가 향상됩니다. 로그에 많은 수의 항목이 포함되어 있는 경우에 이러한 향상이 두드러지게 나타날 수 있습니다.

텍스트 프로토콜 활성화를 통해 로그 파일과 별도로 다른 파일 형식으로 로그를 저장할 수 있습니다.

- **대상 디렉터리** - 로그 파일이 저장되는 디렉터리를 선택합니다(텍스트/CSV에만 적용됨). 경로를 복사하거나 **지우기**를 클릭하여 다른 디렉터리를 선택할 수 있습니다. 각 로그 섹션에는 파일 이름이 미리 정의된 고유한 파일이 포함되어 있습니다(예: 로그를 저장하는 데 일반 텍스트 파일 형식을 사용하는 경우 로그 파일의 **검출된 위협** 섹션의 *virlog.txt*).
- **유형** - **텍스트** 파일 형식을 선택하면 로그가 텍스트 파일로 저장되고 데이터는 탭으로 구분됩니다. 쉼표로 구분된 **CSV** 파일 형식에도 동일하게 적용됩니다. **이벤트**를 선택하면 로그가 파일과 달리 Windows 이벤트 로그(제어판에서 이벤트 뷰어를 사용하여 볼 수 있음)에 저장됩니다.
- **모든 로그 파일 삭제** - **유형** 드롭다운 메뉴에 현재 선택되어 있는 저장된 로그를 모두 지웁니다. 로그 삭제 성공과 관련된 알림이 표시됩니다.

감사 로그에서 구성 변경 내용 추적 활성화 – 각 구성 변경 내용에 대한 정보를 제공합니다. 자세한 내용은 감사 로그를 참조하십시오.

문제를 더 빨리 해결하는 데 도움이 되도록 ESET에서는 컴퓨터의 로그를 제공하도록 요청할 수 있습니다. ESET Log Collector를 사용하면 필요한 정보를 쉽게 수집할 수 있습니다. ESET Log Collector에 대한 자세한 내용은 ESET 지식베이스 문서를 참조하십시오.

프레젠테이션 모드

프리젠테이션 모드는 소프트웨어를 중단 없이 사용하고 알림/경고 창의 방해를 받지 않으며 CPU의 사용을 최소화하려는 사용자를 위한 기능입니다. 프레젠테이션 모드는 안티바이러스 활동으로 중단될 수 없는 프레젠테이션 동안 사용할 수도 있습니다. 이 기능을 활성화하면 모든 팝업 창이 비활성화되고 스케줄러의 활동이 완전히 중지됩니다. 시스템 보호 기능은 백그라운드에서 계속해서 실행되지만 사용자 상호 작용을 요구하지 않습니다.

기본 프로그램 창의 **설정** > **컴퓨터**에서 **프리젠테이션 모드** 옆에 있는  또는  아이콘을 클릭하여 프리젠테이션 모드를 활성화하거나 비활성화할 수 있습니다. 프레젠테이션 모드를 활성화하면 잠재적인 보안 위험이 발생할 수 있으므로 작업 표시줄의 보호 상태 아이콘이 주황색 경고 상태로 바뀝니다. 이 경고는 기본 프로그램 창에서도 볼 수 있으며 여기서는 **프리젠테이션 모드 활성화**가 주황색으로 표시됩니다.

전체 화면 애플리케이션을 시작할 때마다 프리젠테이션 모드가 시작되고 애플리케이션을 종료하면 프리젠테이션 모드가 중지되도록 하려면 **고급 설정** > 도구 > **프리젠테이션 모드**에서 **전체 화면 모드로 애플리케이션을 실행할 때 자동으로 프리젠테이션 모드 활성화**를 활성화합니다.

프리젠테이션 모드가 자동으로 비활성화되는 시간을 정의하려면 **다음 시간 후 자동으로 프리젠테이션 모드 비활성화**를 활성화합니다.

방화벽이 대화 모드이고 프레젠테이션 모드가 활성화되어 있으면 인터넷에 연결하는 데 문제가 있을 수 있습니다. 이는 인터넷에 연결하는 게임을 시작하는 경우 문제가 될 수 있습니다. 일반적으로 이러한 동작을 확인하는 메시지가 표시되지만(통신 규칙이나 예외가 정의되지 않은 경우) 프레젠테이션 모드에서 사용자 상호 작용이 비활성화됩니다. 해결 방법은 이 동작과 충돌할 수 있는 모든 애플리케이션에 대해 통신 규칙을 정의하거나 방화벽에서 다른 필터링 모드를 사용하는 것입니다. 프레젠테이션 모드가 활성화되어 있고 보안 위험이 발생할 수 있는 웹 페이지나 애플리케이션으로 이동하면 이러한 웹 페이지나 애플리케이션이 차단될 수 있습니다. 그러나 사용자 상호 작용이 비활성화되어 있기 때문에 설명이나 경고는 표시되지 않습니다.

분석

분석은 ESET 프로세스의 애플리케이션 크래시 덤프(예: ekrn)를 제공합니다. 애플리케이션이 충돌하면 덤프가 생성됩니다. 따라서 개발자는 다양한 ESET Endpoint Security 문제를 디버깅하고 해결할 수 있습니다.

덤프 유형 옆의 드롭다운 메뉴를 클릭하고 3개의 사용 가능한 옵션 중에서 하나를 선택합니다.

- 이 기능을 비활성화하려면 **비활성화**를 선택합니다.
- **일부** (기본값) - 애플리케이션이 예기치 않게 충돌한 이유를 식별하는 데 도움이 될 수 있는 유용한 정보의 최소 집합을 기록합니다. 이 덤프 파일 종류는 공간이 제한되어 있을 때 유용할 수 있습니다. 그러나 포함된 정보가 제한되어 있어 이 파일을 분석할 때 문제 발생 시 실행 중이던 스레드에 의해 직접적으로 유발되지 않은 오류는 발견되지 않을 수 있습니다.
- **전체** - 애플리케이션이 예기치 않게 중지되면 시스템 메모리의 전체 내용을 기록합니다. 메모리 덤프 완료에는 메모리 덤프가 수집될 때 실행 중이던 프로세스의 데이터가 포함될 수 있습니다.

대상 디렉터리 - 충돌 중 덤프가 생성되는 디렉터리입니다.

분석 폴더 열기 - 새 *Windows* 탐색기 창에서 이 디렉터리를 열려면 **열기**를 클릭합니다.

분석 덤프 생성 - **대상 디렉터리**에서 분석 덤프 파일을 생성하려면 **생성**을 클릭합니다.

고급 로깅

안티스팸 엔진 고급 로깅 활성화 – 안티스팸 검사 중에 발생하는 모든 이벤트를 기록합니다. 이 기록은 개발자들이 ESET 안티스팸 엔진 관련 문제를 분석하고 수정하는 데 도움이 됩니다.

브라우저 보호 고급 로깅 활성화화 - 문제를 진단하고 해결할 수 있도록 안전한 브라우저에서 발생하는 모든 이벤트를 기록합니다.

컴퓨터 검사기 고급 로깅 활성화 – 컴퓨터 검사 또는 실시간 파일 시스템 보호 기능을 통해 파일 및 폴더를 검사하는 동안 발생하는 모든 이벤트를 기록합니다.

장치 제어 고급 로깅 활성화 – 장치 제어에서 발생하는 모든 이벤트를 기록합니다. 이 기록은 개발자들이 장치 제어 관련 문제를 분석하고 수정하는 데 도움이 됩니다.

Direct Cloud 고급 로깅 활성화 - 제품과 Direct Cloud 서버 간의 모든 제품 통신을 기록합니다.

문서 보호 고급 로깅 활성화 – 문제를 진단하고 해결할 수 있도록 문서 보호에서 발생하는 모든 이벤트를 기록합니다.

이메일 클라이언트 보호 고급 로깅 활성화 – 이메일 클라이언트 보호 및 이메일 클라이언트 플러그인에서 발생하는 모든 이벤트를 기록하여 문제를 진단하고 해결할 수 있도록 합니다.

커널 고급 로깅 활성화 – ESET 커널 서비스(ekrn)에서 발생하는 모든 이벤트를 기록하여 문제를 진단 및 해결할 수 있도록 합니다.

라이선싱 고급 로깅 활성화 - ESET 활성화 및 라이선싱 서버와의 모든 제품 통신을 기록합니다.

메모리 추적 활성화 - 개발자가 메모리 누수를 진단하는 데 도움이 되는 모든 이벤트를 기록합니다.

네트워크 보호 고급 로깅 활성화 – 개발자들이 방화벽 관련 문제를 분석 및 수정할 수 있도록 방화벽을 통과하는 모든 네트워크 데이터를 PCAP 형식으로 기록합니다.

네트워크 트래픽 검사기 고급 로깅 활성화 - 개발자가 네트워크 트래픽 검사기와 관련된 문제를 진단하고 해결할 수 있도록 네트워크 트래픽 검사기를 통과하는 모든 데이터를 PCAP 형식으로 기록합니다.

운영 체제 고급 로깅 활성화 – 실행 중인 프로세스, CPU 활동, 디스크 작동과 같은 운영 체제에 대한 추가 정보가 수집됩니다. 이 정보는 개발자들이 사용 중인 운영 체제에서 실행하는 ESET 제품 관련 문제를 분석하고 수정하는 데 도움이 됩니다.

푸시 메시징 고급 로깅 활성화 - 푸시 메시징 중에 발생하는 모든 이벤트를 기록하여 진단 및 문제 해결을 허용합니다.

실시간 파일 시스템 보호 고급 로깅 – 문제를 진단하고 해결할 수 있도록 실시간 파일 시스템 보호에서 발생하는 모든 이벤트를 기록합니다.

업데이트 엔진 고급 로깅 활성화 – 업데이트 프로세스 중에 발생하는 모든 이벤트를 기록합니다. 이 기록은 개발자들이 업데이트 엔진 관련 문제를 분석하고 수정하는 데 도움이 됩니다.

취약성 및 패치 관리 고급 로깅 활성화 - 취약성 및 패치 관리의 모든 이벤트를 기록합니다. 이 설정은 사용자 환경에서 취약성 및 패치 관리가 활성화된 경우에만 표시됩니다(ESET PROTECT Cloud에서 활성화됨).

웹 컨트롤 고급 로깅 활성화 – 웹 컨트롤에서 발생하는 모든 이벤트를 기록합니다. 이 기록은 개발자들이 웹 컨트롤 관련 문제를 분석하고 수정하는 데 도움이 됩니다.

로그 파일은 *C:\ProgramData\ESET\ESET Security\Diagnostics*에 있습니다.

기술 지원

ESET Endpoint Security에서 ESET 기술 지원에 문의할 때 시스템 구성 데이터를 제출할 수 있습니다. **시스템 구성 데이터 제출** 드롭다운 메뉴에서 **항상 제출**을 선택하여 데이터를 자동으로 제출하거나, **제출 전 확인**을 선택하여 데이터를 제출하기 전에 메시지를 표시합니다.

연결

특정 네트워크에서는 프록시 서버가 컴퓨터와 인터넷 간의 통신을 조정할 수 있습니다. 프록시 서버를 사용하는 경우 다음 설정을 정의해야 합니다. 그렇지 않으면 ESET Endpoint Security 및 해당 모듈을 자동으로 업데이트할 수 없습니다. ESET Endpoint Security에서 프록시 서버 설정은 고급 설정의 두 가지 다른 섹션에서 사용할 수 있습니다.

전체 프록시 서버 설정은 고급 설정 > **연결** > **프록시 서버**에서 구성할 수 있습니다. 이 수준에서 프록시 서버를 지정하면 모든 ESET Endpoint Security에 대한 전체 프록시 서버 설정이 정의됩니다. 여기의 파라미터는 인터넷 연결이 필요한 모든 모듈에서 사용됩니다.

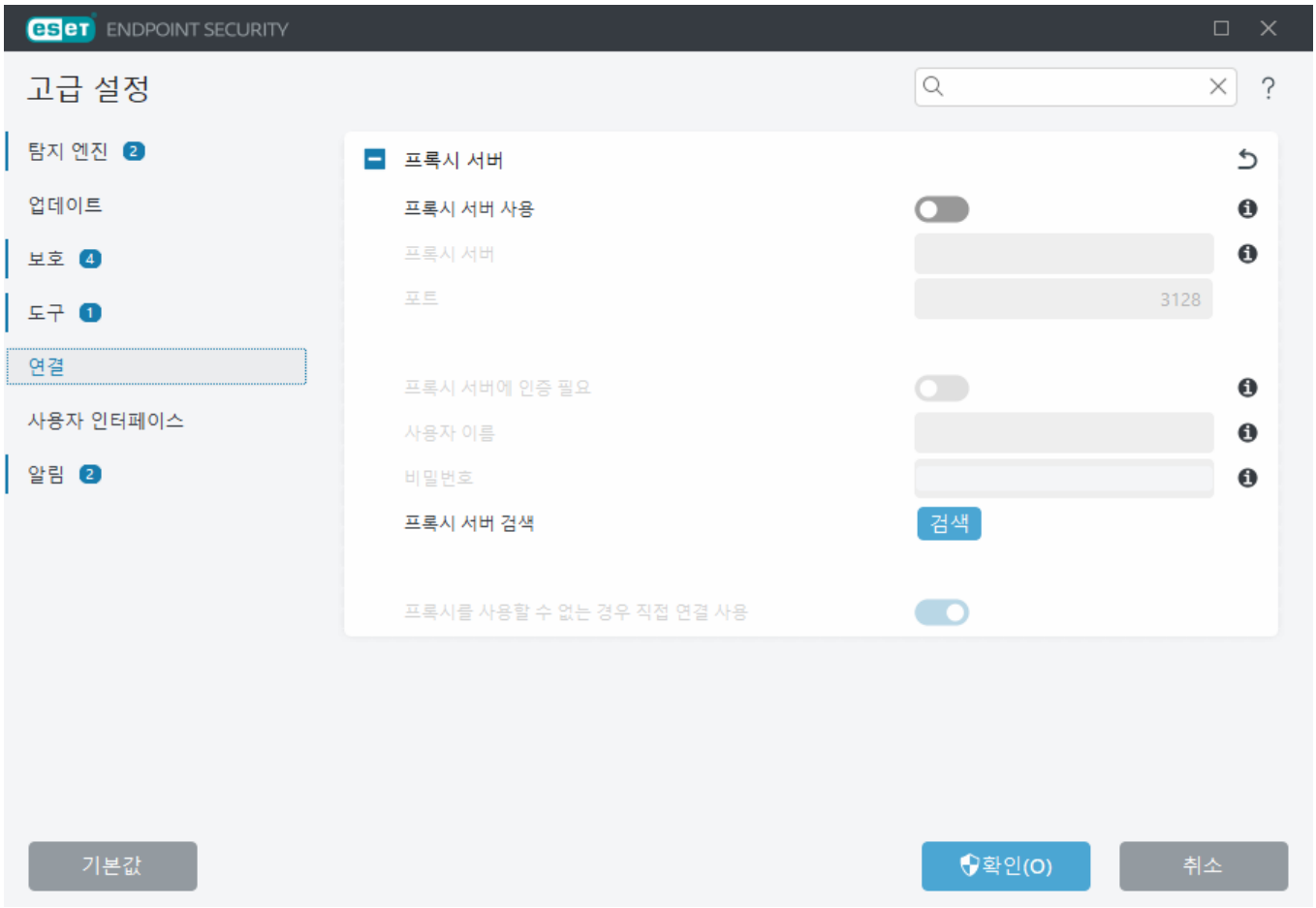
전체 프록시 서버 설정을 지정하려면 **프록시 서버 사용**을 활성화하고 프록시 서버의 **포트** 번호와 함께 **프록시 서버** 주소를 입력합니다.

프록시 서버와의 통신에 인증이 필요한 경우 **프록시 서버에 인증 필요**를 선택한 다음 각 필드에 올바른 **사용자 이름** 및 **패스워드**를 입력합니다. 프록시 서버 설정을 자동으로 검색하여 입력하려면 **프록시 서버 검색**을 클릭합니다. 운영 체제에서 프록시 설정을 찾으려면 **Windows + I** 바로 가기 키를 누르고 **네트워크 및 인터넷** > **프록시**를 클릭합니다. ESET Endpoint Security은(는) Internet Explorer 또는 Google Chrome의 인터넷 옵션에 지정된 파라미터를 복사합니다.

프록시 서버 설정에 사용자 이름 및 비밀번호를 수동으로 입력해야 합니다.

프록시를 사용할 수 없는 경우 직접 연결 사용 - ESET Endpoint Security이(가) 프록시를 통해 연결하도록 구성되어 있는데 프록시에 연결할 수 없는 경우 ESET Endpoint Security은(는) 프록시를 우회하고 ESET 서버와 직접 통신합니다.

또한 프록시 서버 설정은 **프록시 모드** 드롭다운 메뉴에서 **프록시 서버를 통해 연결**을 선택하여 고급 설정 > **업데이트** > **프로필** > **업데이트** > **연결 옵션**에서도 구성할 수 있습니다. 이 구성은 업데이트에 한해 적용되며 원격 위치에서 모듈 업데이트를 받는 랩톱에서 사용하는 것이 좋습니다. 자세한 내용은 고급 업데이트 설정을 참조하십시오.



사용자 인터페이스

프로그램의 그래픽 사용자 인터페이스(GUI) 동작을 구성하려면 고급 설정 > **사용자 인터페이스**를 엽니다.

사용자 인터페이스 요소 고급 설정 화면에서 프로그램의 시각적 모양과 효과를 조정할 수 있습니다.

보안 소프트웨어의 최고 보안 성능을 제공하기 위해 접근 설정 도구를 사용하여 패스워드로 설정을 보호하면 제거 또는 무단 변경을 방지할 수 있습니다.

시스템 알림, 탐지 경고 및 애플리케이션 상태의 동작을 구성하려면 알림섹션을 참조하십시오.

프레젠테이션 모드는 팝업 창, 예약된 작업 및 프로세서와 RAM을 로드할 수 있는 모든 구성 요소의 방해를 받지 않고 응용 프로그램을 사용하려는 사용자들에게 유용합니다.

ESET Endpoint Security 사용자 인터페이스를 최소화하는 방법(관리되는 환경에 유용함)도 참조하십시오.

사용자 인터페이스 요소

ESET Endpoint Security의 사용자 인터페이스 구성 옵션을 통해 필요에 따라 작업 환경을 조정할 수 있습니다. 이러한 구성 옵션은 **고급 설정** > **사용자 인터페이스** (F5) > **사용자 인터페이스 요소**에서 접근할 수 있습니다.

사용자 인터페이스 요소 섹션에서 작업 환경을 조정할 수 있습니다. **시작 모드** 드롭다운 메뉴를 사용하여 다음 GUI(그래픽 사용자 인터페이스) 시작 모드 중에서 선택합니다.

전체 - 완전한 GUI가 표시됩니다.

최소 - GUI가 실행되지만 사용자에게 알림만 표시됩니다.

수동 – 로그온해도 GUI가 자동으로 시작되지 않습니다. 어느 사용자든 수동으로 시작할 수 있습니다.

숨김 - 알림 또는 경고가 표시되지 않습니다. 관리자만 GUI를 시작할 수 있습니다. 이 모드는 관리되는 환경 또는 시스템 리소스를 보존해야 하는 상황에서 유용할 수 있습니다.

최소 GUI 시작 모드가 선택되고 컴퓨터가 다시 시작되면 알림이 표시되지만 그래픽 인터페이스는 표시되지 않습니다. 전체 그래픽 사용자 인터페이스 모드로 되돌리려면 관리자 권한으로 시작 메뉴의 **모든 프로그램** > **ESET** > ESET Endpoint Security에서 GUI를 실행하거나 정책을 사용하여 ESET PROTECT를 통해 수행할 수 있습니다.

색상 모드—드롭다운 메뉴에서 ESET Endpoint Security GUI의 색 구성표를 선택합니다.

- **시스템 색상과 동일** - 운영 체제 설정에 따라 ESET Endpoint Security의 색 구성표를 설정합니다.
- **어두운**—ESET Endpoint Security에서 어두운 색 구성표(어두운 모드)를 적용합니다.
- **밝은**—ESET Endpoint Security에서 표준적인 밝은 색 구성표를 적용합니다.

기본 프로그램 창의 오른쪽 상단에서 ESET Endpoint Security GUI의 색 구성표를 선택할 수도 있습니다.

ESET Endpoint Security 시작 화면을 비활성화하려면 **시작할 때 시작 화면 표시** 옵션을 선택 취소합니다.

검사 중에 중요한 이벤트가 발생할 경우(예: 위협이 검색되거나 검사가 완료된 경우) ESET Endpoint Security

에서 신호음을 울리도록 하려면 **신호음 사용**을 선택합니다.

오른쪽 마우스 버튼 메뉴로 통합 - ESET Endpoint Security 제어 요소를 오른쪽 마우스 버튼 메뉴로 통합합니다.

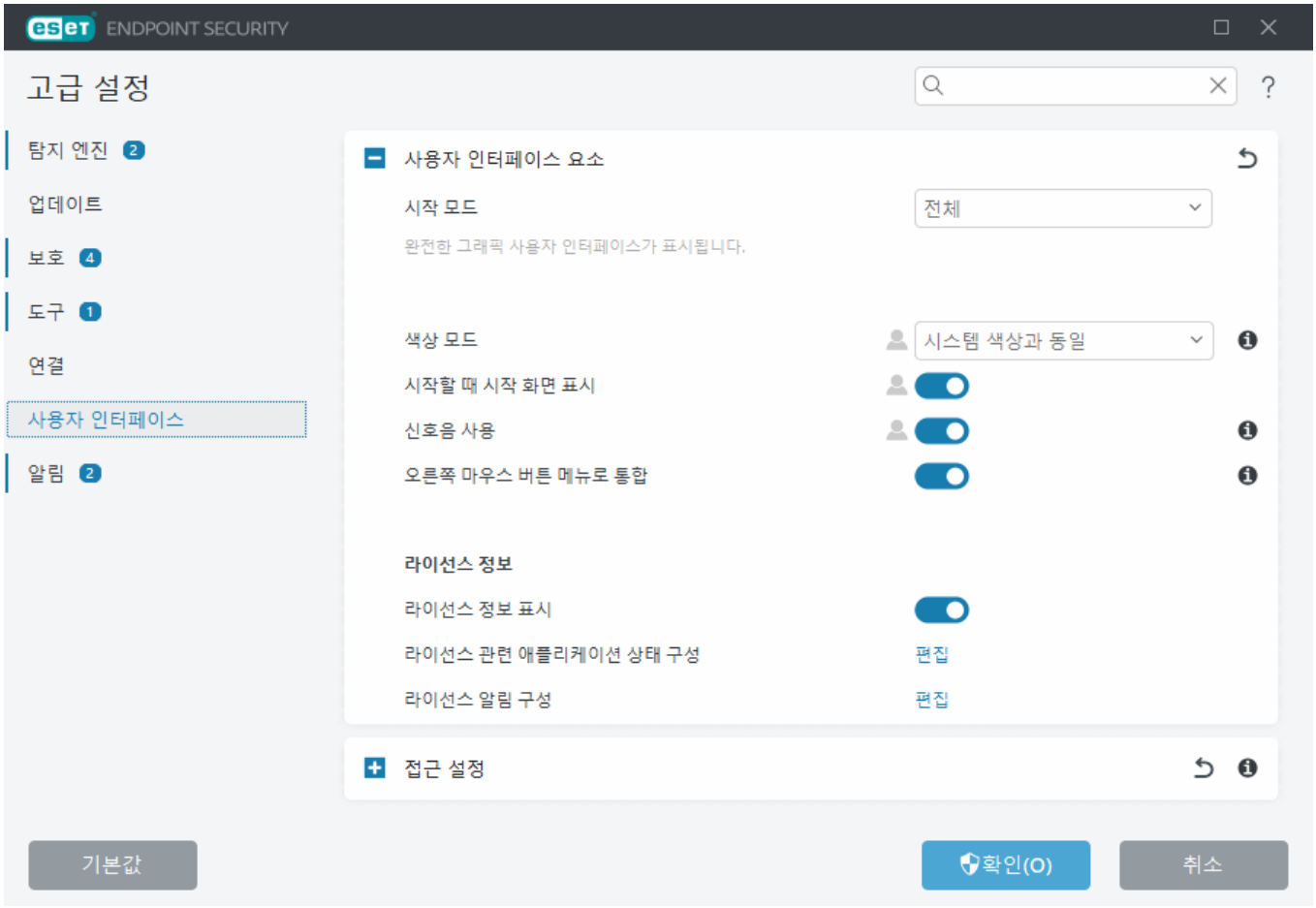
라이선스 정보

라이선스 정보 표시 - 비활성화하면 **보호 상태** 및 **도움말 및 지원** 화면의 라이선스 만료 날짜가 표시되지 않습니다.

라이선스 관련 애플리케이션 상태 구성 - 라이선스 관련 애플리케이션 상태 목록을 엽니다.

라이선스 알림 구성 - 라이선스 관련 알림 목록을 엽니다.

활성화된 MSP 라이선스를 사용하면 라이선스 정보 설정은 적용되지만 ESET Endpoint Security에 접근할 수 없습니다.



접근 설정

ESET Endpoint Security 설정은 보안 정책의 중요한 부분입니다. 무단 수정은 잠재적으로 시스템의 안정성과 보호 상태를 위험에 빠뜨릴 수 있습니다. 무단 수정을 방지하기 위해 ESET Endpoint Security의 제거 및 설정 파라미터를 패스워드로 보호할 수 있습니다. 접근 설정은 고급 설정 > **사용자 인터페이스** > **액세스 설정**에서 구성할 수 있습니다.

ESET Endpoint Security의 제거 및 설정 파라미터를 보호하기 위한 패스워드를 설정하려면 **패스워드 보호 설**

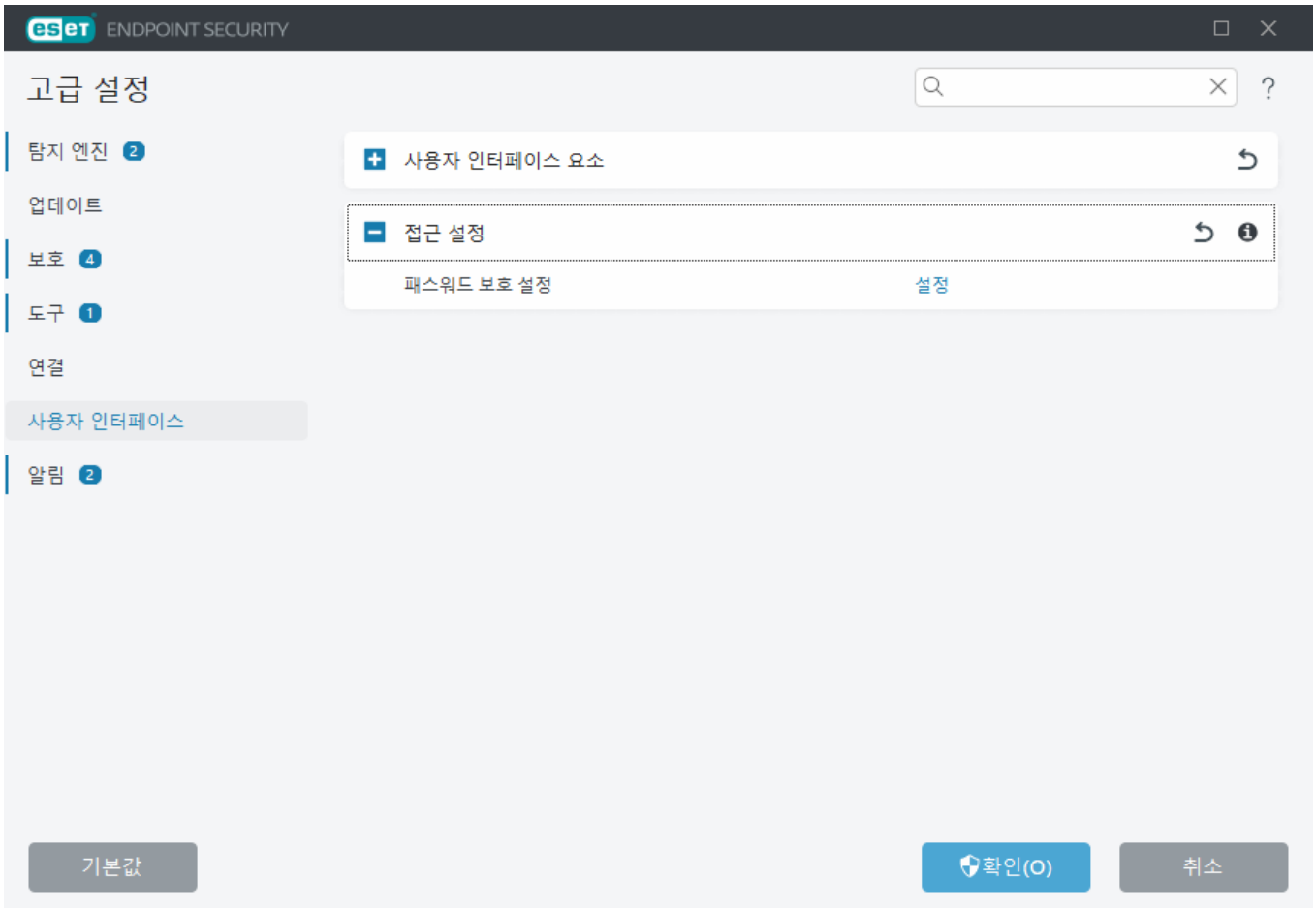
정 옆에 있는 **설정**을 클릭합니다.

패스워드를 변경하려면 **패스워드 보호 설정** 옆에 있는 **패스워드 변경**을 클릭합니다.

패스워드를 제거하려면 **패스워드 보호 설정** 옆에 있는 **제거**를 클릭합니다.

관리되는 환경

관리자는 연결된 클라이언트 컴퓨터에서 ESET Endpoint Security 설정을 패스워드로 보호하기 위한 정책을 생성할 수 있습니다. 새 정책을 생성하려면 패스워드로 보호된 설정을 참조하십시오.



고급 설정을 위한 패스워드

ESET Endpoint Security 고급 설정을 보호하고 무단 수정을 방지하려면 **새 패스워드** 및 **패스워드 확인** 필드에 새 패스워드를 입력합니다. **확인**을 클릭합니다.

관리되는 환경

관리자는 연결된 클라이언트 컴퓨터에서 ESET Endpoint Security 설정을 패스워드로 보호하기 위한 정책을 생성할 수 있습니다. 새 정책을 생성하려면 패스워드로 보호된 설정을 참조하십시오.

등록 취소됨

기존 패스워드를 변경하려면 다음을 수행합니다.

1. **현재 패스워드** 필드에 현재 패스워드를 입력합니다.
2. **새 패스워드** 및 **패스워드 확인** 필드에 새 패스워드를 입력합니다.
3. **확인**을 클릭합니다.

이 패스워드는 나중에 ESET Endpoint Security 수정 시 필요합니다.

패스워드를 잊어버린 경우 ESET 엔드포인트 제품에서 설정 패스워드 잠금 해제를 참조하십시오.

분실한 ESET 라이선스 키, 라이선스 만료 날짜 또는 ESET Endpoint Security에 대한 기타 라이선스 정보를 복구하려면 사용자 이름 및 패스워드/라이선스 키를 분실했습니다를 참조하십시오.

패스워드

무단 수정을 방지하기 위해 ESET Endpoint Security의 설정 파라미터를 비밀번호로 보호할 수 있습니다.

안전 모드

ESET Endpoint Security의 그래픽 인터페이스가 안전 모드에서 실행되면 해당 애플리케이션이 안전 모드에서 실행됨을 알리는 대화 상자 창이 표시됩니다. 안전 모드에서는 모든 프로그램 작동이 제한되므로 표준 모드에서처럼 ESET Endpoint Security의 그래픽 인터페이스를 열 수 없습니다.

표시된 창에서 컴퓨터 검사를 실행할 수 있습니다. 컴퓨터에 악성 코드가 있는지 검사하려면 옵션 **예**를 선택합니다.

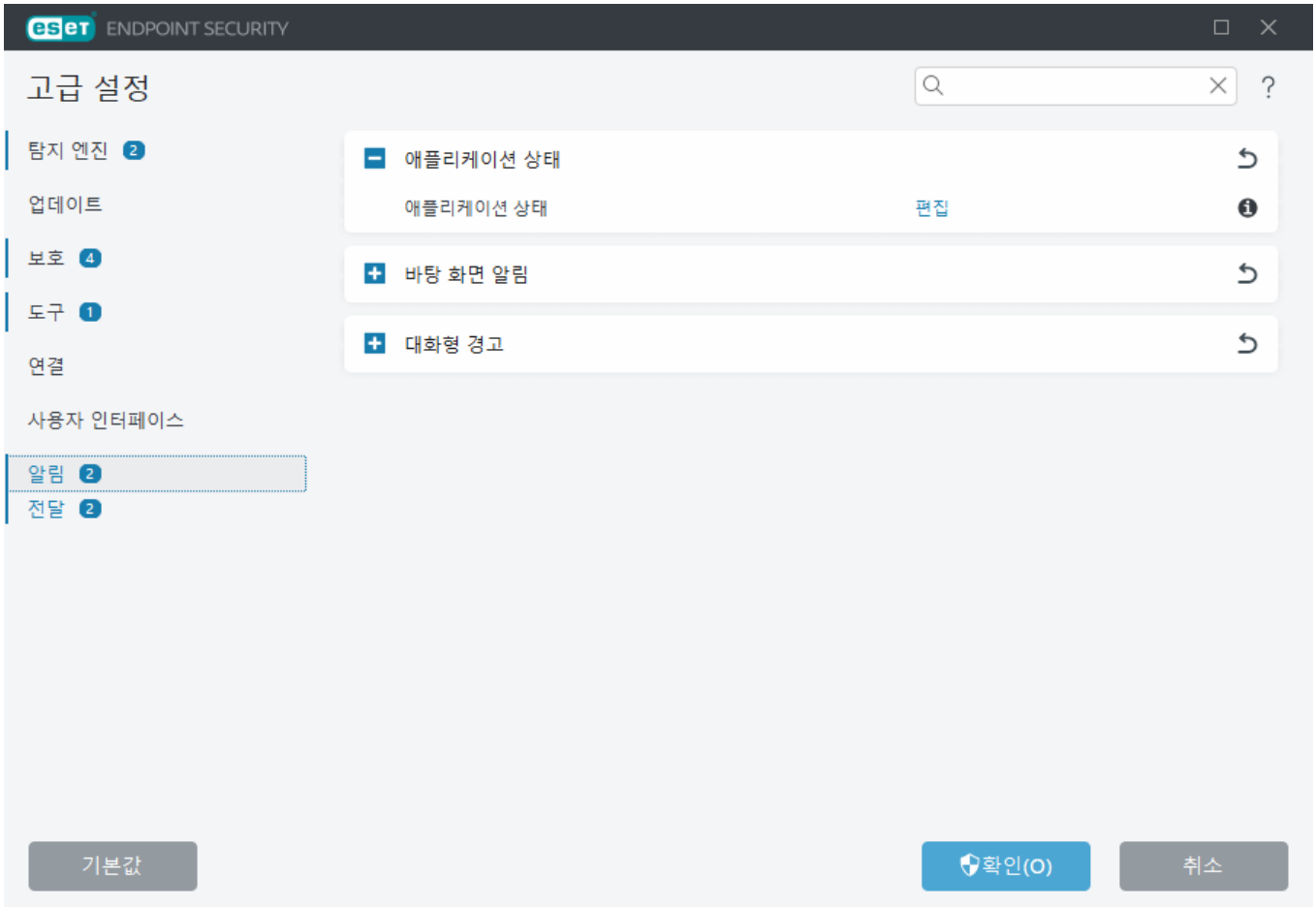
그러면 ESET Endpoint Security 설치 후 기본 컴퓨터 검사 프로필과 동일한 파라미터를 사용하여 별도의 창에서 검사가 시작됩니다.

대화 상자 창을 닫으려면 **아니요** 옵션을 선택합니다. 그러면 ESET Endpoint Security에서 아무런 동작도 수행하지 않습니다.

알림

ESET Endpoint Security 알림을 관리하려면 고급 설정 > **알림**을 엽니다. 다음과 같은 유형의 알림을 구성할 수 있습니다.

- 애플리케이션 상태 – 기본 프로그램 창의 홈 섹션에 표시되는 알림입니다.
- 바탕 화면 알림 – 시스템 작업 표시줄 옆에 있는 작은 알림 창입니다.
- 대화형 경고 – 사용자 상호 작용이 필요한 경고 창과 메시지 상자입니다.
- 전달 (이메일 알림) - 지정된 이메일 주소로 이메일 알림이 전송됩니다.
- 알림 사용자 지정 - 예를 들어 바탕 화면 알림에 사용자 정의 메시지를 추가합니다.



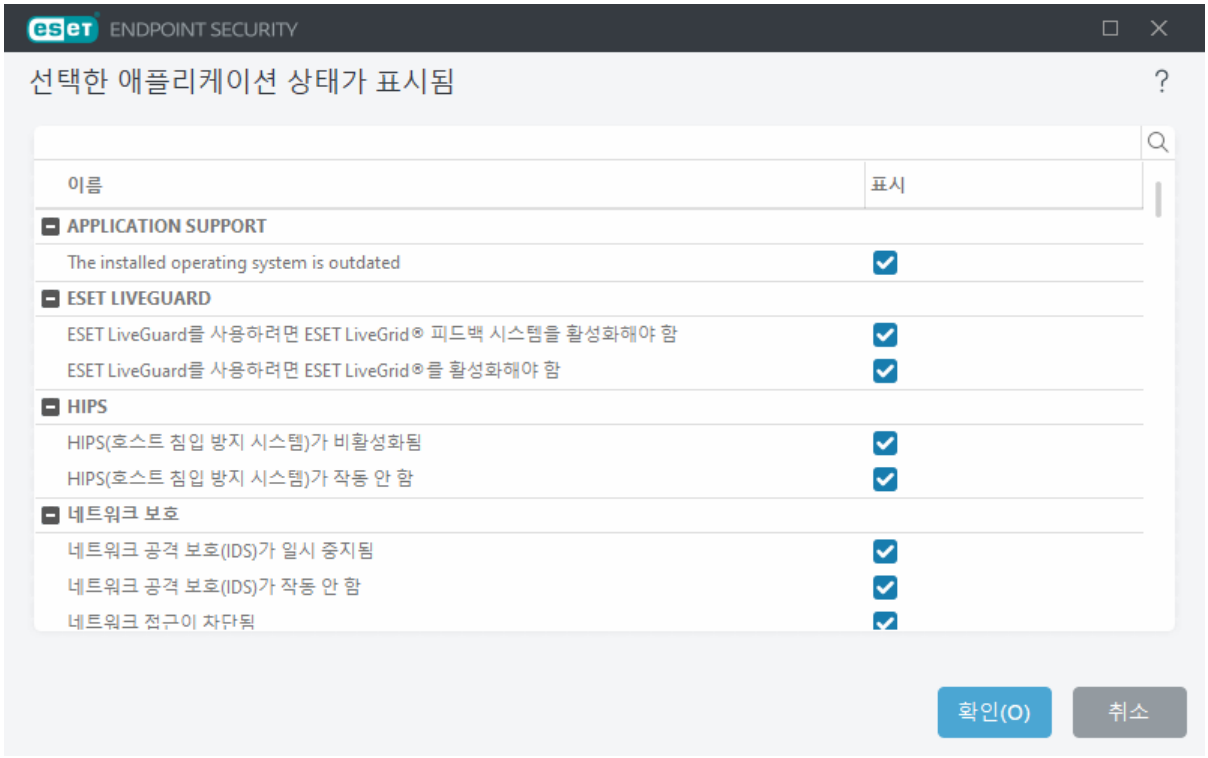
애플리케이션 상태

애플리케이션 상태 – 편집을 클릭하여 기본 프로그램 창의 홈 섹션에 표시되는 애플리케이션 상태를 선택합니다.

애플리케이션 상태

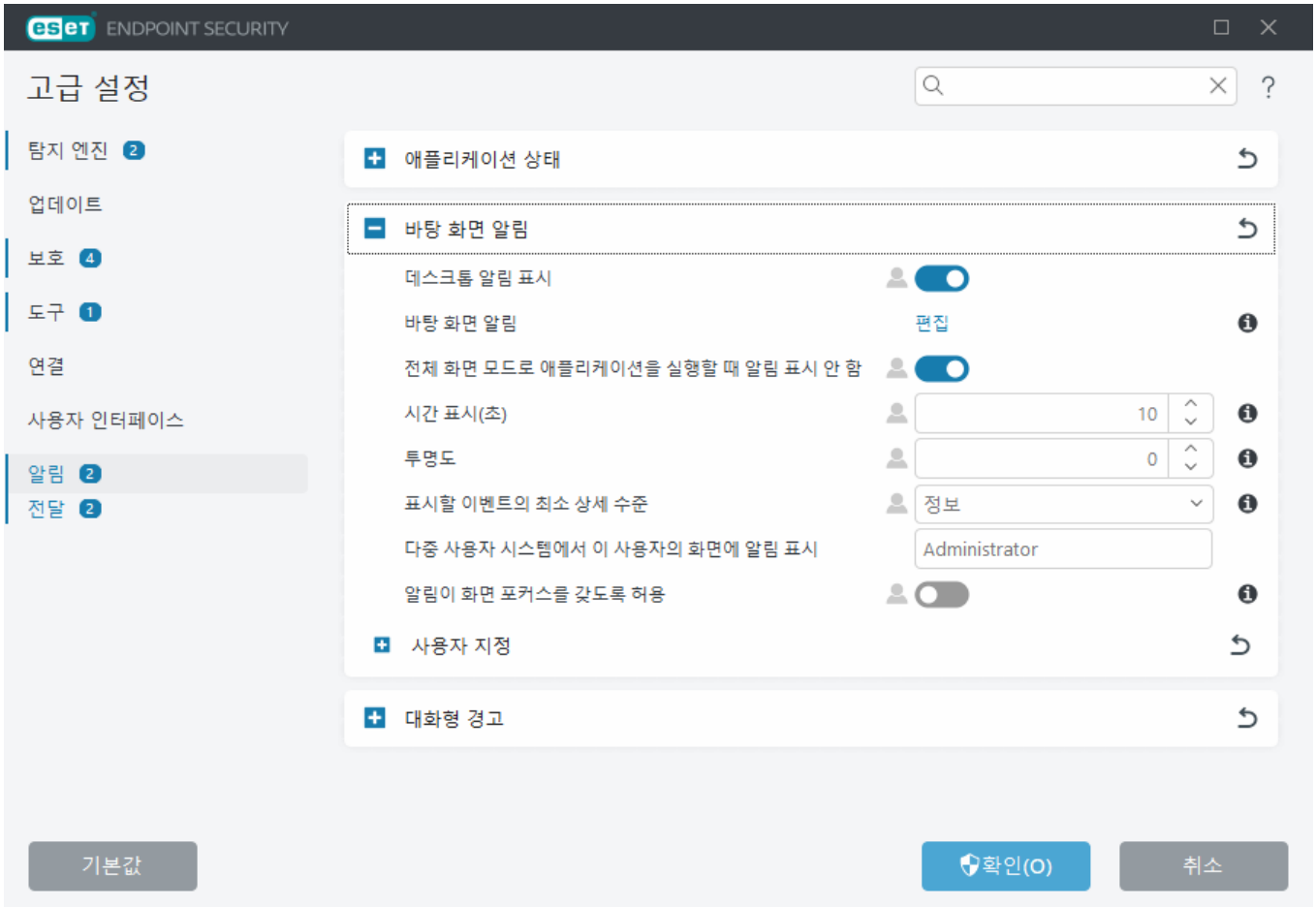
표시할 애플리케이션 상태(예: 안티바이러스 및 안티스파이웨어 보호를 일시 중지하거나 프리젠테이션 모드를 활성화하는 경우)를 구성하려면 고급 설정 > **알림**을 열고 **애플리케이션 상태** 옆에 있는 **편집**을 클릭합니다.

제품이 활성화되지 않았거나 라이선스가 만료된 경우에도 애플리케이션 상태가 표시됩니다. 이 설정은 ESET PROTECT 정책을 통해 변경될 수 있습니다.



바탕 화면 알림

바탕 화면 알림은 시스템 작업 표시 줄 옆에 있는 작은 알림 창으로 표시됩니다. 기본적으로 10초 동안 표시되도록 설정되어 있으며 서서히 사라집니다. 이는 사용자와 ESET Endpoint Security 제품이 통신하는 방식, 성공적인 제품 업데이트 알림, 연결된 새 장치, 바이러스 검사 작업 완료 또는 새로운 위협 요소 발견을 알리는 주요 방법입니다.



바탕 화면에 알림 표시 - 새 이벤트가 발생할 때 제품에서 알릴 수 있도록 이 옵션을 활성화된 상태로 유지하는 것이 좋습니다.

바탕 화면 알림 – 편집을 클릭하여 특정 바탕 화면 알림을 활성화하거나 비활성화합니다.

전체 화면 모드로 애플리케이션을 실행할 때 알림 표시 안 함 - 전체 화면 모드에서 애플리케이션을 실행할 때 모든 비대화 알림이 표시되지 않도록 합니다.

시간 초과(초) - 알림 표시 지속 시간을 설정합니다. 값은 3~30초 사이여야 합니다.

투명도 - 알림의 투명도를 백분율로 설정합니다. 지원되는 범위는 0(투명도 없음)~80(매우 높은 투명도)입니다.

표시할 이벤트의 최소 상세 수준 - 표시할 알림의 시작 심각도 수준을 설정합니다. 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.

- **분석** - 위의 프로그램과 모든 레코드를 미세 조정하는 데 필요한 정보를 기록합니다.
- **정보** - 성공한 업데이트 메시지를 포함한 정보 메시지(예: 비표준 네트워크 이벤트)와 위의 모든 레코드를 기록합니다.
- **경고** - 심각한 오류 및 경고 메시지(예: 업데이트 실패)를 기록합니다.
- **오류** - 오류(문서 보호가 시작되지 않음) 및 심각한 오류가 기록됩니다.
- **주요** - 심각한 오류(안티바이러스 보호를 시작할 때 오류 발생, 시스템 감염 등)만 기록합니다.

다중 사용자 시스템에서 이 사용자의 화면에 알림 표시 – 선택한 계정에서 바탕 화면 알림을 받도록 허용합니다. 예를 들어, 관리자 계정을 사용하지 않는 경우 전체 계정 이름을 입력하면 특정 계정에 대한 바탕 화면 알림이 표시됩니다. 하나의 사용자 계정에서만 바탕 화면 알림을 받을 수 있습니다.

알림이 화면 포커스를 갖도록 허용 - 알림은 화면 포커스를 가지며 Alt+Tab을 통해 접근할 수 있도록 합니다.

알림 사용자 지정

이 창에서는 알림에 사용되는 메시지를 사용자 지정할 수 있습니다.

기본 알림 메시지 - 알림 바닥글에 표시되는 기본 메시지입니다.

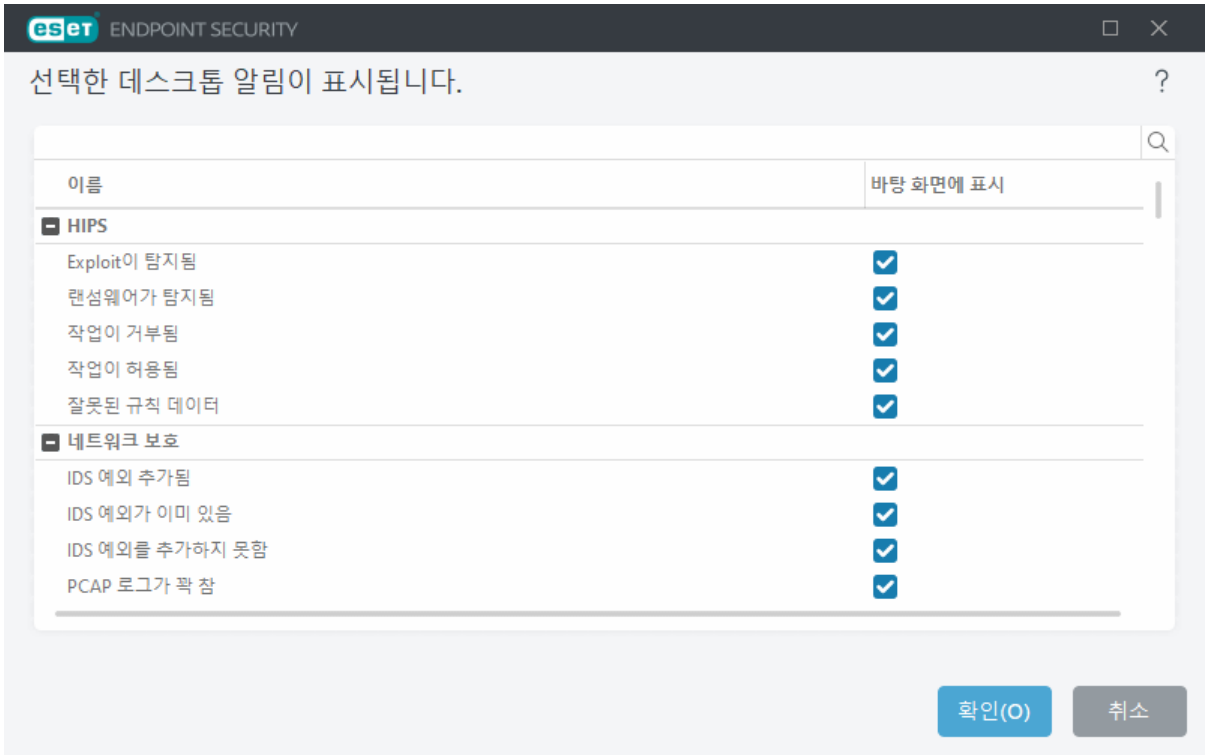
탐지

맬웨어 알림을 자동으로 닫지 않음을 활성화하면 맬웨어 알림을 수동으로 닫을 때까지 알림이 화면에 계속 표시됩니다.

사용자 지정된 알림 메시지를 사용하려면 **기본 메시지 사용**을 비활성화하고 **탐지 알림 메시지** 필드에 원하는 메시지를 입력합니다.

대화 상자 창 - 데스크톱 알림

화면 오른쪽 하단에 표시되는 바탕 화면 알림의 표시 기능을 조정하려면 고급 설정 > **알림** > **바탕 화면 알림**을 엽니다. **애플리케이션 알림** 옆에 있는 **편집**을 클릭한 다음 적절한 **바탕 화면에 표시** 확인란을 선택합니다.

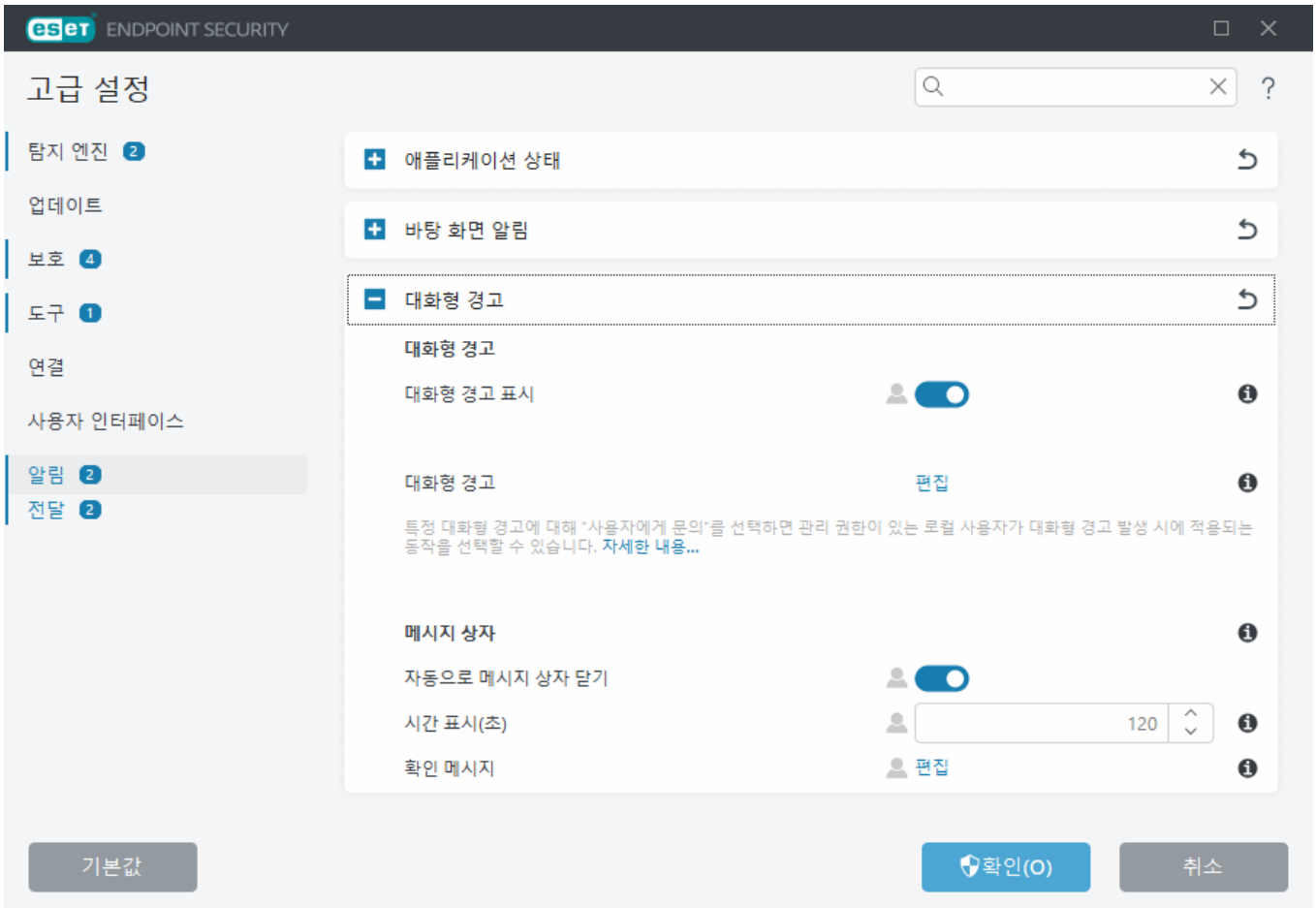


ESET LiveGuard를 사용하는 동안 **파일이 분석됨** 및 **파일이 분석되지 않음** 알림을 설정하려면 사전 보호를 **분석 결과를 받을 때까지 실행 차단**을 설정해야 합니다.

대화형 경고

일반 경고 및 알림에 대한 정보를 원하십니까?
- 위협이 발견됨
- 주소가 차단됨
- 제품이 활성화되지 않음
- 업데이트 사용 가능
- 업데이트 정보가 일치하지 않습니다
- "모듈 업데이트 실패" 메시지에 대한 문제 해결
- '파일이 손상됨' 또는 '파일 이름을 바꾸지 못함'
- 웹 사이트 인증서가 해지됨
- 네트워크 위협 차단됨
- 분석 때문에 파일 차단

고급 설정 > 알림의 **대화형 경고** 섹션에서는 사용자가 결정을 내려야 하는 경우(예: 잠재적 피싱 웹 사이트) ESET Endpoint Security에서 탐지에 대한 메시지 상자와 대화형 경고를 처리하는 방법을 구성할 수 있습니다.



대화형 경고

대화형 경고 표시를 비활성화하면 모든 경고 창과 브라우저 내 대화 상자가 숨겨지므로 이는 제한된 특정 상황에 한해 적합합니다.

- 관리되지 않는 사용자의 경우 이 옵션을 기본 설정(활성화됨) 상태로 두는 것이 좋습니다.
- 관리된 사용자의 경우 이 설정을 활성화된 상태로 두고 대화형 경고 목록에서 사용자에 대해 미리 정의된 동작을 선택합니다.

대화형 경고 - **편집**을 클릭하여 표시할 대화형 경고를 선택합니다.

메시지 상자

일정 시간 후에 메시지 상자를 자동으로 닫으려면 **자동으로 메시지 상자 닫기**를 선택합니다. 수동으로 닫지 않은 경우 지정된 시간이 경과하면 경고 창이 자동으로 닫힙니다.

시간 초과(초) – 경고 표시 지속 시간을 설정합니다. 값은 10~999초 사이여야 합니다.

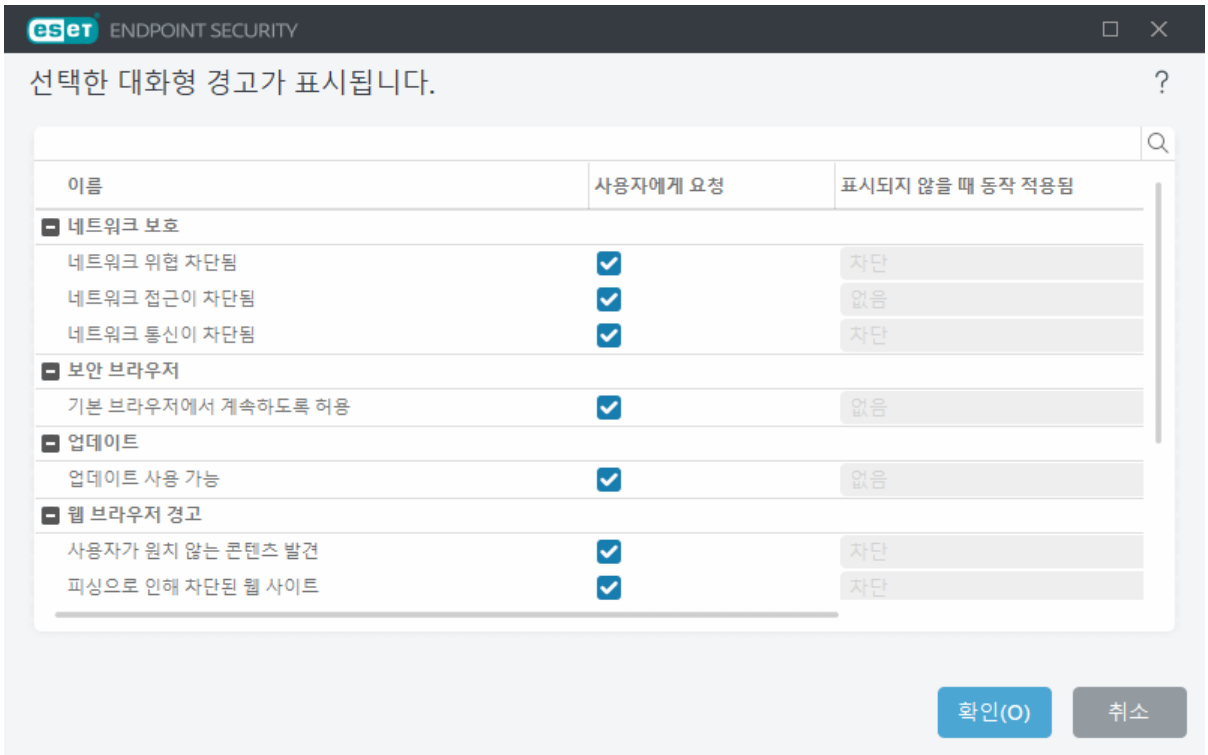
확인 메시지 – 표시하거나 표시하지 않도록 선택할 수 있는 확인 메시지 목록을 표시하려면 **편집**을 클릭합니다.

대화형 경고 목록

이 섹션에서는 동작이 수행되기 전에 ESET Endpoint Security에서 표시하는 몇 가지 대화형 경고 창에 대해 간단히 설명합니다.

구성 가능한 대화형 경고의 동작을 조정하려면 고급 설정 > **알림** > **대화형 경고**를 열고 **대화형 경고** 옆의 **편집**을 클릭합니다.

관리자가 어디에서든지 **사용자에게 요청**을 선택 취소하고, 대화형 경고 창이 표시될 때 적용되는 미리 정의된 동작을 선택할 수 있는 관리되는 환경에 유용합니다.



특정 대화형 경고 창에 대한 참조를 보려면 기타 도움말 섹션을 확인하십시오.

이동식 미디어

- 새 장치가 탐지됨

안전한 브라우저

- 기본 브라우저에서 계속하도록 허용

네트워크 보호

- 네트워크 접근이 차단됨은 ESET PROTECT에서 이 워크스테이션의 **네트워크에서 컴퓨터 격리** 클라이언트 작업이 트리거되면 표시됩니다.
- 네트워크 통신이 차단됨
- 네트워크 위협 차단됨

웹 브라우저 경고

- 사용자가 원치 않는 콘텐츠 발견
- 피싱으로 인해 차단된 웹 사이트

컴퓨터

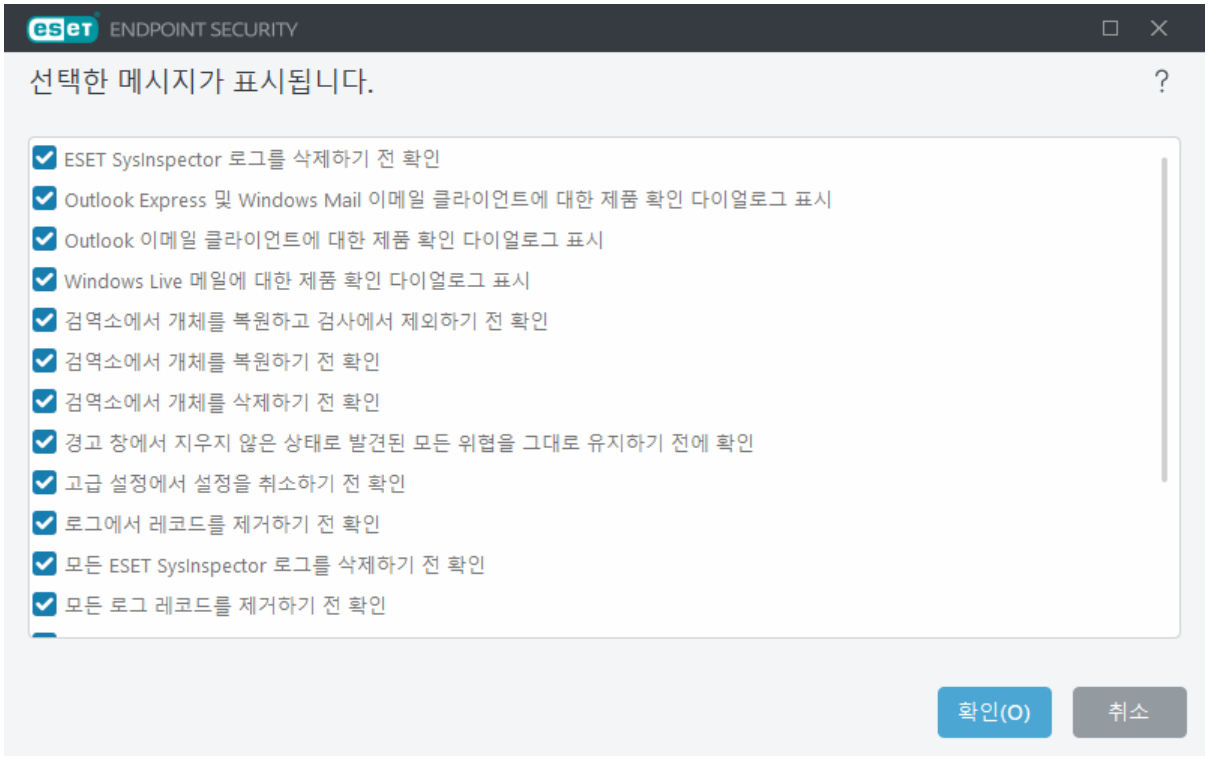
다음과 같은 경고가 있으면 사용자 인터페이스 색상이 변경됩니다.

- 컴퓨터 재시작(필수)
- 컴퓨터 재시작(권장)

> 대화형 경고의 동작은 특정 기능에서 개별적으로 구성할 수 있으므로 대화형 경고에는 탐지 엔진, HIPS 또는 방화벽 대화형 창이 포함되지 않습니다.

확인 메시지

확인 메시지를 조정하려면 고급 설정 > **알림** > **대화형 경고**로 이동한 다음 **확인 메시지** 옆의 **편집**을 클릭합니다.



이 대화 상자 창에는 어떠한 동작이 수행되기 전에 ESET Endpoint Security에서 표시하는 확인 메시지가 표시됩니다. 각 확인 메시지를 허용 또는 비활성화하려면 해당 메시지 옆의 확인란을 선택 또는 선택 취소합니다.

확인 메시지와 관련된 특정 기능에 대해 자세히 알아보십시오.

- ESET SysInspector 로그를 삭제하기 전에 묻기
- 모든 ESET SysInspector 로그를 삭제하기 전에 묻기
- 검역소에서 개체를 삭제하기 전 확인
- 고급 설정에서 설정을 취소하기 전 확인
- 경고 창에서 지우지 않은 상태로 발견된 모든 위협을 그대로 유지하기 전에 확인
- 로그에서 레코드를 제거하기 전 확인
- 스케줄러에서 예약된 작업을 제거하기 전 확인
- 모든 로그 레코드를 제거하기 전 확인
- 통계를 다시 설정하기 전 확인
- 검역소에서 개체를 복원하기 전 확인
- 검역소에서 개체를 복원하고 검사에서 제외하기 전 확인
- 스케줄러에서 예약된 작업을 실행하기 전 확인
- 안티스팸 처리 결과 알림 표시
- 이메일 클라이언트에 대한 안티스팸 처리 결과 알림 표시
- Outlook Express 및 Windows Mail 이메일 클라이언트에 대한 제품 확인 대화 상자 표시
- Windows Live 메일에 대한 제품 확인 대화 상자 표시
- Outlook 이메일 클라이언트에 대한 제품 확인 대화 상자 표시

고급 설정 충돌 오류

일부 구성 요소(예: HIPS 또는 방화벽)와 사용자가 대화 모드나 학습 모드에서 동시에 규칙을 생성할 경우 오류가 발생할 수 있습니다.

자체 규칙을 생성할 경우 필터링 모드를 기본값인 **자동 모드**로 변경하는 것이 좋습니다. ESET 방화벽 학습 모드에 대해 자세히 알아보십시오. HIPS 및 HIPS 필터링 모드에 대해 자세히 알아보십시오.

기본 브라우저에서 계속하도록 허용

특정 대화형 경고는 안전한 브라우저를 올바르게 시작하는 데 오류가 있는 경우에만 표시됩니다.

다시 시작해야 함

ESET Endpoint Security을(를) 새 버전으로 업그레이드하거나 취약성 및 패치 관리를 통해 애플리케이션에 패치를 적용한 후에는 컴퓨터를 다시 시작해야 합니다. ESET Endpoint Security의 새 버전이 발표되었으며, 프로그램 모듈의 자동 업데이트로 해결할 수 없던 문제를 개선하거나 해결할 수 있습니다.

지금 다시 시작을 클릭하여 컴퓨터를 다시 시작합니다. 나중에 컴퓨터를 다시 시작할 계획이라면 **나중에 알림**을 클릭합니다. 나중에 기본 프로그램 창의 **보호 상태** 섹션에서 컴퓨터를 수동으로 다시 시작할 수 있습니다.

"다시 시작해야 함" 또는 "다시 시작 권장" 경고를 비활성화하려면 아래 단계를 따르십시오.

1. **고급 설정**(F5) > **알림** > **대화형 경고**를 엽니다.
2. **대화형 경고** 옆에 있는 **편집**을 클릭합니다. **컴퓨터** 섹션에서 **컴퓨터 재시작(필수)** 및 **컴퓨터 재시작(권장)** 옆에 있는 확인란을 선택 취소합니다.
3. 열려 있는 두 창에서 **확인**을 클릭하여 변경 사항을 저장합니다.
4. 엔드포인트 컴퓨터에서 더 이상 경고가 표시되지 않습니다.
5. (옵션) ESET Endpoint Security의 기본 프로그램 창에서 애플리케이션 상태를 비활성화하려면 애플리케이션 상태 창에서 **컴퓨터를 다시 시작해야 함** 및 **컴퓨터 다시 시작 권장** 옆에 있는 확인란을 선택 취소합니다.

다시 시작하는 것이 좋음

ESET Endpoint Security을(를) 새 버전으로 업그레이드한 후 컴퓨터를 다시 시작해야 합니다. ESET Endpoint Security의 새 버전이 발표되었으며, 프로그램 모듈의 자동 업데이트로 해결할 수 없던 문제를 개선하거나 해결할 수 있습니다.

지금 다시 시작을 클릭하여 컴퓨터를 다시 시작합니다. 나중에 컴퓨터를 다시 시작할 계획이라면 **나중에 알림**을 클릭합니다. 나중에 기본 프로그램 창의 **보호 상태** 섹션에서 컴퓨터를 수동으로 다시 시작할 수 있습니다.

"다시 시작해야 함" 또는 "다시 시작 권장" 경고를 비활성화하려면 아래 단계를 따르십시오.

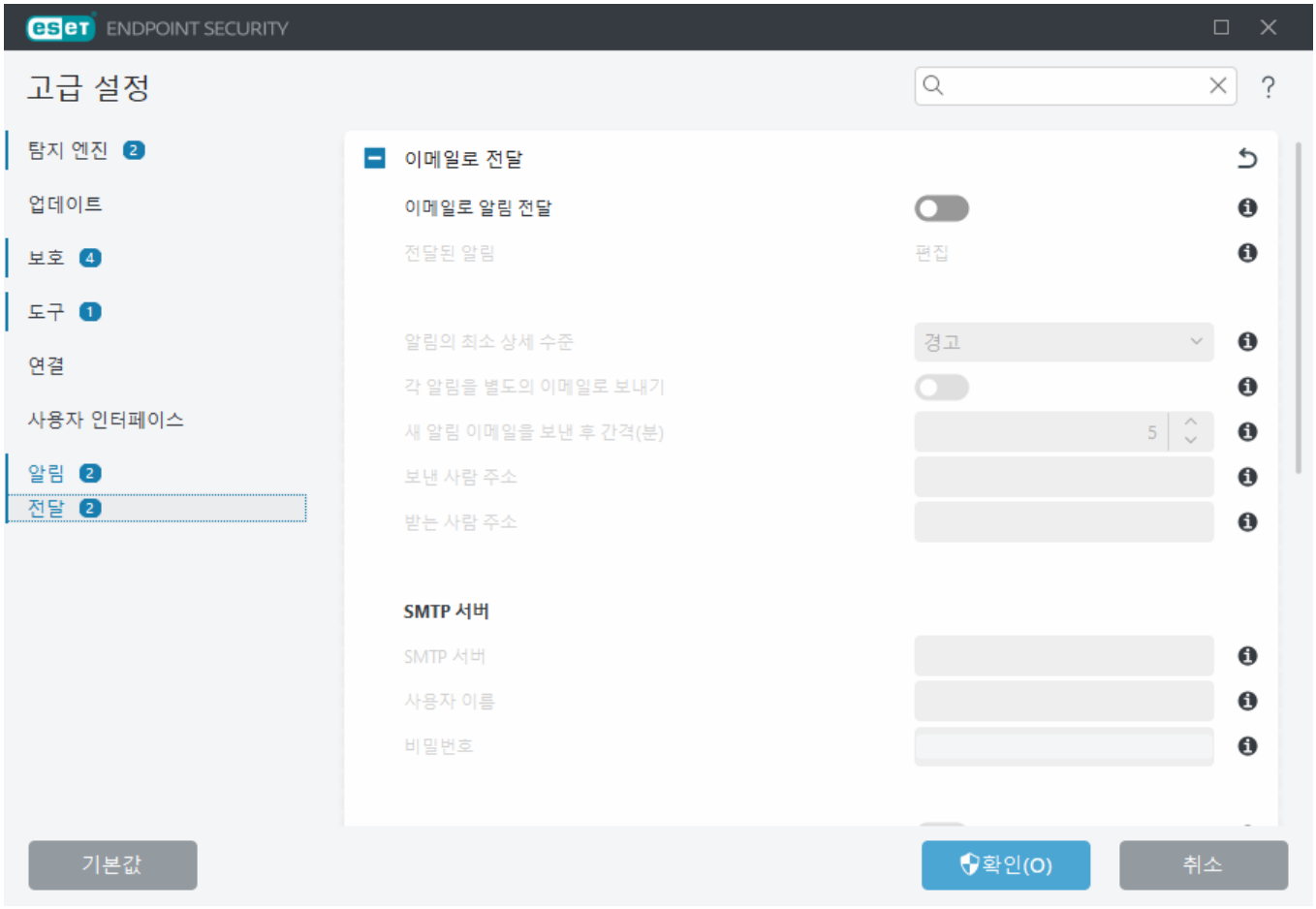
1. **고급 설정**(F5) > **알림** > **대화형 경고**를 엽니다.
2. **대화형 경고** 옆에 있는 **편집**을 클릭합니다. **컴퓨터** 섹션에서 **컴퓨터 재시작(필수)** 및 **컴퓨터 재시작(권장)** 옆에 있는 확인란을 선택 취소합니다.
3. 열려 있는 두 창에서 **확인**을 클릭하여 변경 사항을 저장합니다.
4. 엔드포인트 컴퓨터에서 더 이상 경고가 표시되지 않습니다.
5. (옵션) ESET Endpoint Security의 기본 프로그램 창에서 애플리케이션 상태를 비활성화하려면 애플리케이션 상태 창에서 **컴퓨터를 다시 시작해야 함** 및 **컴퓨터 다시 시작 권장** 옆에 있는 확인란을 선택 취

소합니다.

전달

ESET Endpoint Security에서는 선택한 상세 수준의 이벤트가 발생하면 알림 이메일을 자동으로 보낼 수 있습니다. 고급 설정 > **알림** > **전달** > **이메일로 전달** 섹션에서 **이메일로 알림 전달**을 활성화하여 이메일 알림을 활성화합니다.

전달되는 알림 – 이메일로 전달되는 바탕 화면 알림을 선택합니다.



알림의 최소 상세 수준 드롭다운 메뉴에서 전송할 알림의 시작 심각도 수준을 선택할 수 있습니다.

- **분석** - 위의 프로그램과 모든 레코드를 미세 조정하는 데 필요한 정보를 기록합니다.
- **정보** - 성공한 업데이트 메시지를 포함한 정보 메시지(예: 비표준 네트워크 이벤트)와 위의 모든 레코드를 기록합니다.
- **경고** - 심각한 오류 및 경고 메시지(예: 업데이트 실패)를 기록합니다.
- **오류** - 오류(문서 보호가 시작되지 않음) 및 심각한 오류가 기록됩니다.
- **중요** – 심각한 오류(예: 안티바이러스 보호 시작 오류 또는 위협 발견)만 기록합니다.

각 알림을 별도의 이메일로 보내기 – 활성화된 경우 받는 사람이 각 알림이 발생하면 새로운 이메일을 수신하게 됩니다. 이에 따라 짧은 시간 안에 여러 이메일을 수신할 수 있습니다.

새 알림 이메일을 보낸 후 간격(분) - 새 알림이 이메일로 전송되는 간격(분)입니다. 이 값을 0으로 설정하면 알림이 즉시 전송됩니다.

보낸 사람 주소 - 알림 이메일 헤더에 표시할 보낸 사람 주소를 정의합니다.

받는 사람 주소 – 알림 이메일 헤더에 표시되는 받는 사람 주소를 정의합니다. 값이 여러 개 지원됩니다. 구분 기호로 세미콜론을 사용하십시오.

SMTP 서버

SMTP 서버 - 알림을 보내는 데 사용되는 SMTP 서버입니다(예: *smtp.provider.com:587*, 미리 정의된 포트는 25임).

TLS 암호화를 사용하는 SMTP 서버는 ESET Endpoint Security에서 지원됩니다.

사용자 이름 및 비밀번호 - SMTP 서버에 인증이 필요한 경우 SMTP 서버에 접근하기 위한 유효한 사용자 이름 및 비밀번호를 이 필드에 입력합니다.

보낸 사람 주소 - 이 필드에 알림 이메일 헤더에 표시할 보낸 사람 주소를 지정합니다.

받는 사람 주소 - 이 필드에 알림 이메일 헤더에 표시할 받는 사람 주소를 지정합니다. 세미콜론(;)을 사용하여 여러 이메일 주소를 구분합니다.

TLS 활성화 - TLS 암호화에서 지원되는 경고 및 알림 메시지 보내기를 활성화합니다.

메시지 형식

프로그램과 원격 사용자 또는 시스템 관리자 간의 통신은 Windows 메시징 서비스를 사용하여 이메일 또는 LAN 메시지를 통해 수행됩니다. 대부분의 경우에는 기본 경고 메시지 및 알림 형식을 사용하면 가장 적합합니다. 일부 경우 이벤트 메시지의 메시지 형식을 변경해야 할 수 있습니다.

이벤트 메시지 형식 - 원격 컴퓨터에 표시되는 이벤트 메시지의 형식입니다.

위협 경고 메시지 형식 - 위협 경고 및 알림 메시지에는 미리 정의된 기본 형식이 있습니다. 이 형식은 변경하지 않는 것이 좋습니다. 그러나 자동화된 이메일 처리 시스템을 사용하는 등의 일부 경우에는 메시지 형식을 변경해야 할 수 있습니다.

문자 집합 – 이메일 메시지를 Windows 국가별 설정(예: windows-1250, Unicode (UTF-8), ACSII 7-bit 또는 일본어 (ISO-2022-JP))을 기준으로 ANSI 문자 인코딩으로 변환합니다. 따라서 "á"는 "a"로 변경되고 알 수 없는 기호는 "?"로 변경됩니다.

QP(Quoted-Printable) 인코딩 사용 - 이메일 메시지 소스가 (QP)(Quoted Printable) 형식으로 인코딩됩니다. 이 형식은 ASCII 문자를 사용하며, 8비트 형식(áéíóú)의 이메일로 특수 국가 표준 문자를 제대로 전송할 수 있습니다.

% 기호로 구분되는 문자열인 키워드는 메시지에서 지정된 실제 정보로 바뀝니다. 다음과 같은 키워드를 사용할 수 있습니다.

- **%TimeStamp%** - 이벤트의 날짜 및 시간입니다.
- **%Scanner%** - 관련 모듈입니다.
- **%ComputerName%** - 경고가 발생한 컴퓨터의 이름입니다.
- **%ProgramName%** - 경고를 생성한 프로그램입니다.
- **%InfectedObject%** - 감염된 파일이나 메시지 등의 이름입니다.

- **%VirusName%** - 감염 ID입니다.
- **%Action%** – 침입을 받은 동작입니다.
- **%ErrorDescription%** - 바이러스가 아닌 이벤트의 설명입니다.

키워드 **%InfectedObject%** 및 **%VirusName%**은(는) 위협 경고 메시지에만 사용되고 **%ErrorDescription%**은(는) 이벤트 메시지에만 사용됩니다.

모든 설정을 기본값으로 되돌리기

모든 모듈의 모든 프로그램 설정을 되돌리려면 **고급 설정**에서 기본값을 클릭합니다. 이렇게 하면 모든 모듈의 모든 프로그램 설정이 새로 설치한 이후의 상태로 다시 설정됩니다.

설정 가져오기 및 내보내기도 참조하십시오.

현재 섹션의 모든 설정 되돌리기

현재 섹션의 모든 설정을 ESET에서 정의된 기본 설정으로 되돌리려면 구부러진 화살표 ⮌를 클릭합니다.

기본값으로 되돌리기를 클릭하고 나면 변경한 모든 내용이 손실됩니다.

테이블 내용 되돌리기 - 이 옵션을 활성화하면 수동이나 자동으로 추가된 규칙, 작업 또는 프로필이 손실됩니다.

설정 가져오기 및 내보내기도 참조하십시오.

구성 저장 중 오류 발생

이 오류 메시지는 오류로 인해 설정이 제대로 저장되지 않았음을 나타냅니다.

이것은 일반적으로 프로그램 파라미터를 수정하려고 하는 사용자가 다음과 같음을 의미합니다.

- 접근 권한이 충분하지 않거나 구성 파일 및 시스템 레지스트리를 수정하는 데 필요한 운영 체제 권한이 없습니다.
  > 원하는 수정 작업을 수행하려면 시스템 관리자가 로그인해야 합니다.
- 최근에 HIPS 또는 방화벽에서 학습 모드를 활성화했으며 고급 설정을 변경하려고 했습니다.
  > 구성을 저장하고 구성 충돌을 피하려면 고급 설정을 저장하지 않고 닫은 후 원하는 항목을 다시 변경해 보십시오.

두 번째로 흔히 나타나는 원인은 프로그램이 손상되어 더 이상 제대로 작동하지 않으므로 재설치해야 하는 경우입니다.

명령줄 검사기

ESET Endpoint Security의 안티바이러스 모듈은 명령줄("ecls" 명령 사용)을 통해 수동으로 실행하거나 배치 파일("bat")을 사용하여 실행할 수 있습니다.

ESET 명령줄 검사기 사용 현황:

```
ecls [OPTIONS..] FILES..
```

명령줄에서 수동 검사기를 실행하는 동안 다음 파라미터 및 스위치를 사용할 수 있습니다.

옵션

/base-dir=폴더	FOLDER에서 모듈 로드
/quar-dir=폴더	검역소 FOLDER
/exclude=마스크	MASK가 일치하는 파일을 검사에서 제외
/subdir	하위 폴더 검사(기본값)
/no-subdir	하위 폴더 검사 안 함
/max-subdir-level=수준	검사할 폴더 내에 있는 폴더의 최대 하위 수준
/symlink	기호화된 링크를 따라 이동(기본값)
/no-symlink	기호화된 링크 건너뛰기
/ads	ADS 검사(기본값)
/no-ads	ADS 검사 안 함
/log-file=파일	FILE에 출력 기록
/log-rewrite	출력 파일 덮어쓰기(기본값 - 추가)
/log-console	콘솔에 출력 기록(기본값)
/no-log-console	콘솔에 출력 기록 안 함
/log-all	감염되지 않은 파일도 기록
/no-log-all	감염되지 않은 파일 기록 안 함(기본값)
/aind	활동 표시기 표시
/auto	모든 로컬 디스크 검사 및 자동 치료

검사기 옵션

/files	파일 검사(기본값)
/no-files	파일 검사 안 함
/memory	메모리 검사
/boots	부트 영역 검사
/no-boots	부트 영역 검사 안 함(기본값)
/arch	압축파일 검사(기본값)
/no-arch	압축파일 검사 안 함
/max-obj-size=크기	SIZEMB 미만의 파일만 검사(기본값 0 = 제한 없음)
/max-arch-level=수준	검사할 압축파일(다중 압축파일) 내에 있는 압축파일의 최대 하위 수준
/scan-timeout=제한	최대 LIMIT초 동안 압축파일 검사
/max-arch-size=크기	압축파일 내의 파일이 SIZE미만일 경우에만 해당 파일 검사(기본값 0 = 제한 없음)
/max-sfx-size=크기	자체 압축 해제 파일에 포함된 파일이 SIZEMB 미만일 경우에만 해당 파일 검사(기본값 0 = 제한 없음)
/mail	이메일 파일 검사(기본값)
/no-mail	이메일 파일 검사 안 함

/mailbox	사서함 검사(기본값)
/no-mailbox	사서함 검사 안 함
/sfx	자체 압축 해제 파일 검사(기본값)
/no-sfx	자체 압축 해제 파일 검사 안 함
/rtp	런타임 패커 검사(기본값)
/no-rtp	런타임 패커 검사 안 함
/unsafe	사용자에게 안전하지 않은 애플리케이션 검사
/no-unsafe	사용자에게 안전하지 않은 애플리케이션 검사 안 함(기본값)
/unwanted	사용자가 원치 않는 애플리케이션 검사
/no-unwanted	사용자가 원치 않는 애플리케이션 검사 안 함(기본값)
/suspicious	감염 의심 애플리케이션 검사(기본값)
/no-suspicious	감염 의심 애플리케이션 검사 안 함
/pattern	지문 사용(기본값)
/no-pattern	지문 사용 안 함
/heur	인공지능 활성화(기본값)
/no-heur	인공지능 비활성화
/adv-heur	고급 인공지능 활성화(기본값)
/no-adv-heur	고급 인공지능 비활성화
/ext-exclude=확장명	콜론으로 분리된 파일 확장명을 검사에서 제외
/clean-mode=모드	감염된 개체에 치료 MODE 사용 다음과 같은 옵션을 사용할 수 있습니다. • none (기본값) - 자동 치료가 실행되지 않습니다. • standard - ecls.exe가 감염된 파일을 자동으로 치료하거나 삭제하려고 합니다. • 엄격한 치료 - ecls.exe가 사용자 개입 없이 감염된 파일을 자동으로 치료하거나 삭제하려고 합니다(파일을 삭제하기 전에는 메시지가 표시되지 않음). • 정밀한 치료 - ecls.exe가 파일이 무엇이든 상관없이 치료하려고 하지 않고 파일을 삭제합니다. • 삭제 - ecls.exe가 치료하려고 하지 않고 파일을 삭제하지만 Windows시스템 파일과 같은 중요한 파일은 삭제하지 않습니다.
/quarantine	감염된 파일이 치료된 경우 검역소에 복사 (치료하는 동안 수행된 작업 추가)
/no-quarantine	감염된 파일을 검역소에 복사 안 함

일반 옵션

/help	도움말 표시 및 종료
/version	버전 정보 표시 및 종료
/preserve-time	마지막 접근시의 타임스탬프 유지

종료 코드

0	위협을 찾을 수 없음
1	위협을 찾아서 치료함

10	일부 파일을 검사하지 못함(위협일 수 있음)
50	위협을 찾음
100	오류

100보다 큰 종료 코드는 해당 파일이 검사되지 않았으므로 감염되었을 수 있음을 나타냅니다.

일반적인 질문

이 장에서는 몇 가지 자주 묻는 질문과 발생하는 문제에 대해 다룹니다. 장 제목을 클릭하면 문제 해결 방법을 확인할 수 있습니다.

- ESET Endpoint Security을(를) 업데이트하는 방법
- ESET Endpoint Security을(를) 활성화하는 방법
- ESET Endpoint Security에서 위협 탐지
- 내 PC에서 바이러스를 제거하는 방법
- 특정 애플리케이션에 대한 통신을 허용하는 방법
- 스케줄러에서 새 작업을 생성하는 방법
- 주간 컴퓨터 검사를 예약하는 방법
- 알림 및 대화형 경고를 관리하는 방법
- 제품을 ESET PROTECT에 연결하는 방법
  - 재정의 모드 사용 방법
  - ESET Endpoint Security에 권장되는 정책을 적용하는 방법
- 미러를 구성하는 방법
- ESET Endpoint Security에서 Windows 10으로 업그레이드하는 방법
- 원격 모니터링 및 관리를 활성화하는 방법
- 인터넷에서 특정 파일 유형의 다운로드를 차단하는 방법
- ESET Endpoint Security 사용자 인터페이스를 최소화하는 방법

문제가 위의 도움말 페이지 목록에 포함되지 않으면 ESET Endpoint Security 도움말 페이지에서 문제를 설명하는 키워드 또는 구를 검색하십시오.

도움말 페이지 내에서 문제/질문에 대한 해결 방법을 찾을 수 없는 경우, 일반적인 질문과 문제에 대한 답변을 찾을 수 있는 ESET 지식 베이스를 방문하십시오.

- ESET Endpoint Security 설치 방법
- 파일코더(랜섬웨어) 악성코드로부터 보호하기 위한 모범 사례
- ESET Endpoint Security 및 ESET Endpoint Antivirus FAQ
- ESET 제품이 완전히 작동하도록 하려면 타사 방화벽에서 어떤 주소와 포트를 열어야 합니까?

필요한 경우 ESET 온라인 기술 지원 센터에 질문이나 문제를 문의할 수 있습니다. ESET의 온라인 고객 지원 양식에 대한 링크는 기본 프로그램 창의 **도움말 및 지원** 창에 있습니다.

자동 업데이트 FAQ

ESET Endpoint Security의 제품 업데이트에 대한 자세한 내용은 ESET 지식베이스 문서를 읽어 보십시오.
- 다른 ESET 제품 업데이트 및 릴리스 유형

컴퓨터가 자동으로 업데이트됩니까? 다시 시작 전후로 업데이트가 다운로드됩니까?

다시 시작하기 전에 다운로드되므로 업데이트된 파일도 이 단계에서 준비됩니다. 다시 시작한 후에도 업데이트된 파일은 여전히 사용할 수 있도록 준비되어 있으며 현재 설치된 버전은 중단 없는 보호를 제공합니다. 변경 사항은 ESET Endpoint Security을(를) 다음 번에 시작하면 적용됩니다.

제게는 약 3,000대의 컴퓨터가 있습니다. 모든 컴퓨터가 동시에 업데이트를 다운로드합니까? 이렇게 많은 컴퓨터에서 자동 업데이트 시 프록시를 사용할 수 있습니까?

ESET은 대규모 네트워크용 미러 도구와 프록시 솔루션을 제공하므로, 업데이트는 인터넷에서 한 번만 다운로드하면 로컬로 배포됩니다. 업데이트는 일반적으로 5~10MB로 크기가 더 작고, ESET에서는 사용 가능한 처음 몇 주간 업데이트를 스로틀링합니다. 따라서 ESET 서버에 직접 연결된 경우 모든 클라이언트가 동시에 다운로드를 시작하지는 않습니다.

어떤 컴퓨터를 업데이트할지 또는 얼마나 많은 컴퓨터를 업데이트할지 정할 수 있습니까? 시간당 10대 이상의 컴퓨터를 다운로드하고 싶지 않을 수도 있고, 지금 10대의 컴퓨터를 업데이트하고 며칠 후에 다른 컴퓨터를 업데이트하고 싶을 수도 있으니까요.

관리되는 환경에는 원하는 최신 버전을 지정할 수 있는 자동 업데이트 정책이 있습니다. 와일드카드(예: 9.0.2032.*)도 지원됩니다. 자세한 내용은 ESET PROTECT 또는 ESET PROTECT Cloud에 대한 온라인 도움말에서 자동 업데이트 장을 참조하십시오. 죄송하지만, 현재 자동 업데이트를 제한하는 데 사용할 수 있는 다른 옵션은 없습니다. 여러 그룹에 다양한 정책을 할당할 수 있습니다.

자동 업데이트는 정책에 따라서만 구성됩니까? ESET 제품을 업데이트하고 싶지 않은 경우, 정책을 비활성화할 수 있습니까?

ESET 엔드포인트 제품용 보안 및 안정성 핫픽스가 있는 경우, 해당 최종 사용자 사용권 계약에 규정된 약관에 따라 자동 업데이트를 비활성화한 경우에도 제품이 업데이트됩니다. ESET은 보안 및 안정성 핫픽스를 사용하여 중요한 문제를 해결하고 ESET 제품에 최대한의 보안 성능과 안정성을 보장합니다.

현재 자동 업데이트 구성과 관계없이 모든 엔드포인트 그룹에 자동 업데이트 정책을 할당할 수 있습니다. 관리되지 않는 환경에서 사용자는 ESET 엔드포인트 제품의 고급 설정 화면에서 자동 업데이트를 로컬로 구성할 수 있습니다.

사용 가능한 가장 초기 버전을 사용하도록 정책을 구성하면 어떻게 됩니까? 그렇게 해도 ESET이 제 제품을 업데이트합니까?

핫픽스와 중요 핫픽스(보안 및 안정성 업데이트)는 업데이트 범주가 약간 다릅니다. 사용자 설정 승인 시, 일반 핫픽스는 표준 우선순위의 자동 업데이트에 할당됩니다. 중요 핫픽스는 사용자 설정과 관계없이 최우선순위로 적용됩니다.

오프라인 시나리오에서는 업데이트가 어떻게 작동합니까? 사용자는 언제 오프라인 저장소를 사용합니까?

오프라인 저장소에는 .dup 및 .fup 파일도 포함되어 있습니다. 저장소 섹션은 모듈 업데이트가 아니라 미러 도구에서 다운로드해야 합니다. 자세한 내용은 ESET PROTECT에 대한 온라인 도움말의 오프라인 저장소 항목을 참조하십시오.

ESET 제품은 업데이트가 필요하다는 것을 어떻게 알 수 있습니까? 저장소에서? 서버로 전송되는 데이터가 있습니까? ESET이 버전을 릴리스한 지 한 달 후에 업데이트할 계획인 경우 ESET 서버에서 전 세계 릴리스를 처리할 수 있습니까?

ESET 제품은 저장소에서 자동 업데이트를 다운로드합니다. 필수 업데이트는 단 몇 KB에 불과한 크기이므로, 서버가 이에 대비할 수 있습니다. ESET은 저장소 서버에서 필수 업데이트를 스로틀링하지 않습니다. 그러나 자동 업데이트 크기가 더 큰 경우, 서버 업데이트를 제한할 수 있는 옵션이 있습니다. 아래 표에는 차등 자동 업데이트 발생 시 핫픽스 크기의 예가 나와 있습니다.

이전 버전	새 버전	크기
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

차등 자동 업데이트에 실패하면 ESET 제품이 전체 업데이트를 시작할 수 있습니다. 여전히 기능이 보장되는 자동 업데이트이지만, .dup 파일 대신 더 큰 .fup 파일이 다운로드됩니다. 버전 9.0.2032.2의 경우 27MB입니다. 그러나 이러한 시나리오는 드뭅니다.

ESET Endpoint Security 업데이트가 스로틀링 상태로 릴리스됩니까? 그렇다면 릴리스 후 업데이트 스로틀링 기간은 어떻게 됩니까?

ESET은 새 버전이 릴리스된 후 처음 몇 주간 업데이트를 스로틀링하여 서버의 부하를 줄이고 새 버전을 균등하게 배포합니다.

자동 업데이트가 기본 업그레이드 방법 중 하나가 됩니다. 자동 업데이트는 업그레이드의 기본 방법 중 하나가 됩니다. 자세한 작동 방식은 어떻게 됩니까?

ESET은 가능한 한 많은 고객이 자동 업데이트를 사용해 업데이트하도록 하는 데 목표를 두고 있습니다. 사용할 수 있는 이전 버전이 너무 많으면 지원하기 어렵습니다. 자동 업데이트 기능은 작동 방식이 간단합니다. 첫 번째 모듈 업데이트 확인 중에 .dup 파일이 다운로드되며, 업데이트 절차 중에 제품이 완전히 작동하고 컴퓨터를 보호합니다. 업데이트 절차 중에 제품은 완벽하게 작동하며 항상 컴퓨터를 보호합니다. 새 버전은 다시 시작한 후 활성화됩니다. ESET PROTECT(서버 측)에서 정책을 사용하여 업데이트할 최고 버전을 지정하거나, 와일드카드를 사용할 수 있습니다. 자세한 내용은 ESET PROTECT 또는 ESET PROTECT Cloud에 대한 온라인 도움말에서 자동 업데이트 장을 참조하십시오.

자동 업데이트가 1/10에서 작동하는 것이 맞습니까? 현재 ESET Endpoint Security 8.0.2028.1을 사용하고 있습니다. 자동 업데이트가 실행되면 어떤 버전으로 업데이트됩니까?

저장소 서버의 스로틀링 때문에 자동 업데이트를 사용한 제품 업데이트가 지연될 수 있습니다. 스로틀링과 함께 제품 업데이트가 릴리스되면, 자동 업데이트 확인에서 이를 즉시 수신하지 못할 수 있습니다. 업데이트가 안전하고 안정적이라고 간주되면, 나머지 모든 클라이언트가 업데이트를 수신할 수 있도록 스로틀링을 완전히 제거하거나 줄일 수 있습니다.

스로틀링 절차는 업데이트할 때마다 소요 시간이 다를 수 있습니다. 업데이트를 요청하는 클라이언트 수, 서버의 트래픽, 기타 요인에 따라 소요 시간이 달라집니다. 이 절차는 항상 발전하며 언제나 변경 사항이 발생합니다.

오전 8시 45분에 컴퓨터를 시작해서 오후 5시에 종료하면 자동 업데이트가 언제 실행됩니까?

자동 업데이트는 24시간마다 최대 한 번, 다음으로 예정된 모듈 업데이트가 성공할 때 실행됩니다.

자동 업데이트가 실행되는 동안 컴퓨터를 종료하면 다음에 언제 업데이트가 실행됩니까?

업데이트는 다음 예약된 업데이트 창에서 실행됩니다. 자동 업데이트(구 uPCU) 절차에 대한 강력한 안전장치 메커니즘이 있습니다. 업데이트를 다운로드하고 컴퓨터를 다시 시작한 후에도 업데이트된 파일이 여전히 사용할 수 있도록 준비되며, 현재 설치된 버전이 중단 없는 보호 기능을 제공합니다. 변경 사항은 ESET 엔드포인트 제품을 다음번 시작한 후에 적용됩니다.

24시간마다 정기적으로 연결되기를 기다리지 않고 자동 업데이트를 즉시 실행할 수 있습니까? 업데이트 확인을 클릭하는 다른 방법이 있습니까?

기본 프로그램 창을 열고 **업데이트** > **업데이트 확인**을 클릭해야만 자동 업데이트 절차를 수동으로 시작할 수 있습니다. 모듈 업데이트를 시작하는 다른 모든 방법에는 24시간 자동 업데이트 스케줄러 정책이 반영됩니다. 현재는 자동 업데이트 다운로드를 원격으로 시작할 수 없습니다. 향후 업데이트에 이 기능을 추가할 예정입니다.

ESET Endpoint Security을(를) 업데이트하는 방법

ESET Endpoint Security를 수동으로 업데이트하거나 자동으로 업데이트할 수 있습니다. 업데이트를 트리거하려면 기본 프로그램 창에서 **업데이트**를 클릭한 다음 **업데이트 확인**을 클릭합니다.

기본 설치 설정에서는 매시간 수행되는 자동 업데이트 작업을 생성합니다. 간격을 변경하려면 **도구** > 스케줄러로 이동합니다.

내 PC에서 바이러스를 제거하는 방법

컴퓨터가 맬웨어에 감염된 증상(예: 속도가 느려짐, 작동이 자주 중단됨)을 보이면 다음을 수행하는 것이 좋습니다.

1. 기본 프로그램 창에서 **컴퓨터 검사**를 클릭합니다.
2. **스마트 검사**를 클릭하여 시스템 검사를 시작합니다.
3. 검사를 마치면 검사한 파일, 감염된 파일 및 치료된 파일 수가 표시된 로그를 검토합니다.
4. 디스크의 특정 부분만 검사하려면 **사용자 지정 검사**를 클릭하고 바이러스를 검사할 대상을 선택합니다.

자세한 내용은 정기적으로 업데이트되는 ESET 지식 베이스 문서를 참조하십시오.

특정 애플리케이션에 대한 통신을 허용하는 방법

대화 모드에서 새 연결이 검색되었으나 일치하는 규칙이 없는 경우 해당 연결을 허용 또는 거부할지를 묻는 메시지가 나타납니다. 애플리케이션에서 연결을 설정하도록 시도할 때마다 ESET Endpoint Security에서 동일한 동작이 수행되도록 하려면 **작업 저장(규칙 생성)** 확인란을 선택합니다.

애플리케이션에 대한 방화벽 규칙이 ESET Endpoint Security의 기본 프로그램 창을 열고 **설정** > **네트워크** > **방화벽** > 톱니바퀴 > **구성** > **고급** > **규칙**을 클릭하면 나타나는 방화벽 설정 창에서 감지되려면 먼저 **편집**을 클

릭하여 새 규칙을 생성해야 합니다.

추가를 클릭하여 규칙을 추가합니다. 추가 버튼과 **일반** 탭을 클릭하고 규칙의 이름, 방향 및 통신 프로토콜을 입력합니다. 이 창에서 규칙이 적용되면 실행할 동작을 정의할 수 있습니다.

로컬 탭에 애플리케이션의 실행 파일에 대한 경로 및 로컬 통신 포트를 입력합니다. **원격** 탭을 클릭하여 원격 주소 및 포트를 입력합니다(해당되는 경우). 애플리케이션에서 통신을 다시 시도하면 새로 생성된 규칙이 바로 적용됩니다.

스케줄러에서 새 작업을 생성하는 방법

도구 > 스케줄러에서 새 작업을 생성하려면 **작업 추가**를 클릭하거나, 오른쪽 마우스 버튼을 클릭하고 오른쪽 마우스 버튼 메뉴에서 **추가**를 선택합니다. 예약된 작업 유형에는 다음과 같이 다섯 가지가 있습니다.

- **외부 애플리케이션 실행** - 외부 애플리케이션 실행을 예약합니다.
- **로그 유지 관리** - 로그 파일에는 삭제된 레코드의 잔여 레코드가 포함되어 있을 수도 있습니다. 이 작업에서는 효과적으로 작업하기 위해 정기적으로 로그 파일의 레코드를 최적화합니다.
- **시스템 시작 파일 검사** - 시스템 시작 또는 로그온 시 실행할 수 있는 파일을 검사합니다.
- **컴퓨터 상태 스냅숏 생성** - ESET SysInspector 컴퓨터 스냅숏을 생성합니다. 시스템 구성 요소(예: 드라이버, 애플리케이션)에 대한 자세한 정보를 수집하고 각 구성 요소의 위험 수준을 평가합니다.
- **수동 컴퓨터 검사** - 컴퓨터의 파일 및 폴더에 대한 검사를 수행합니다.
- **업데이트** – 모듈을 업데이트하여 업데이트 작업을 예약합니다.

업데이트는 가장 자주 사용되는 예약된 작업 중 하나이므로 아래에서는 새 업데이트 작업을 추가하는 방법에 대해 설명하도록 하겠습니다.

예약된 작업 드롭다운 메뉴에서 **업데이트**를 선택합니다. **작업 이름** 필드에 작업 이름을 입력하고 **다음**을 클릭합니다. 작업 수행 빈도를 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다. **한 번**, **반복적으로**, **매일**, **매주** 및 **이벤트가 트리거됨**. **랩톱을 배터리 전원으로 실행하는 동안 시스템 리소스를 최소화하려면 배터리 전원으로 실행되는 작업 건너뛰기**를 선택합니다. 작업은 **작업 실행** 필드에 지정된 날짜 및 시간에 실행됩니다. 그런 다음 예약된 시간에 작업을 수행하거나 완료할 수 없는 경우 수행할 동작을 정의합니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **다음 예약 시간에**
- **최대한 빨리**
- **마지막 실행 이후 시간이 지정된 값을 초과하는 경우 즉시**(간격은 **마지막 실행 후 시간** 스크롤 상자를 사용하여 정의할 수 있음)

다음 단계에서는 현재 예약된 작업에 대한 정보가 포함된 요약 창이 표시됩니다. 변경 수행을 완료했으면 **마침**을 클릭합니다.

예약된 작업에 사용할 프로필을 선택할 수 있는 대화 상자 창이 표시됩니다. 여기서 기본 프로필과 대체 프로필을 설정할 수 있습니다. 대체 프로필은 기본 프로필을 사용하여 작업을 완료할 수 없는 경우 사용됩니다. **마침**을 클릭하여 확인하면, 새로 예약된 작업이 현재 예약된 작업 목록에 추가됩니다.

주간 컴퓨터 검사를 예약하는 방법

전기 작업을 예약하려면 기본 프로그램 창을 열고 **도구 > 스케줄러**를 클릭합니다. 다음은 매주 로컬 드라이브를 검사하는 작업을 예약하는 방법에 대한 간단한 설명입니다. 자세한 지침을 알아보려면 ESET의 지식베이스 문서를 참조하십시오.

검사 작업을 예약하려면 다음을 수행합니다.

1. 기본 스케줄러 화면에서 **작업 추가**를 클릭합니다.
2. 드롭다운 메뉴에서 **수동 검사**를 선택합니다.
3. 작업 이름을 입력하고 작업 수행 빈도에 대해 **매주를 선택합니다**.
4. 작업 실행 날짜 및 시간을 설정합니다.
5. 어떤 이유로든(예: 컴퓨터가 꺼져 있음) 예약된 작업이 실행되지 않을 경우 나중에 작업을 수행하려면 **최대한 빨리 작업 실행**을 선택합니다.
6. 예약된 작업의 요약 내용을 검토하고 **마침**을 클릭합니다.
7. **대상** 드롭다운 메뉴에서 **로컬 드라이브**를 선택합니다.
8. 작업을 적용하려면 **마침**을 클릭합니다.

ESET Endpoint Security를 ESET PROTECT에 연결하는 방법

컴퓨터에 ESET Endpoint Security을(를) 설치하고 나서 ESET PROTECT를 통해 연결하려면 클라이언트 워크스테이션에 ESET Management 에이전트도 설치되어 있어야 합니다. 이는 ESET PROTECT 서버와 통신하는 모든 클라이언트 솔루션의 필수 요소입니다.

- 클라이언트 워크스테이션에 ESET Management 에이전트 설치 또는 배포

또한 다음을 참조하십시오.

- 원격으로 관리되는 엔드포인트에 대한 설명서
- 재정의 모드 사용 방법
- ESET Endpoint Security에 권장되는 정책을 적용하는 방법

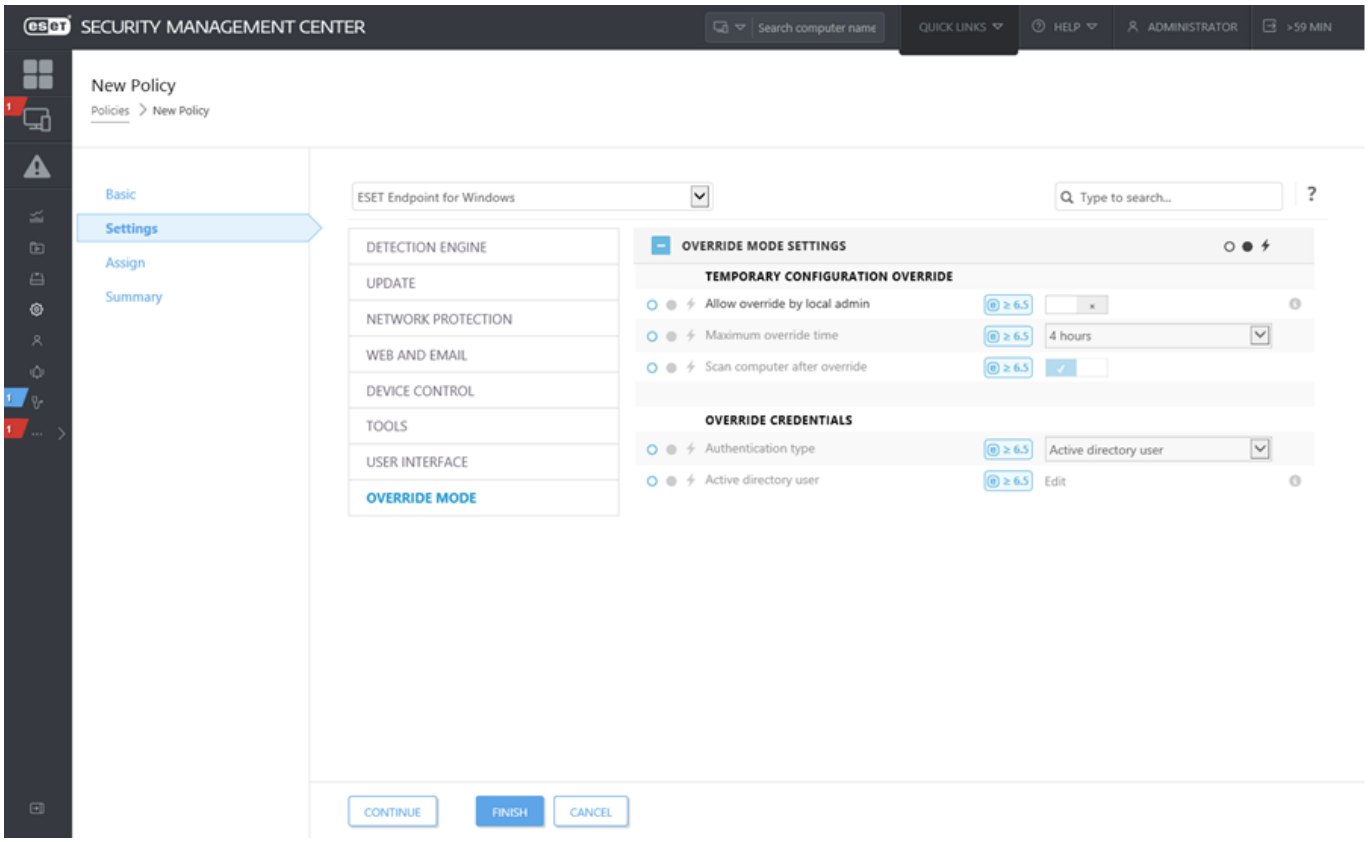
재정의 모드 사용 방법

컴퓨터에 Windows용 ESET Endpoint 제품(6.5 이상 버전)이 설치되어 있는 사용자는 재정의 기능을 사용할 수 있습니다. 재정의 모드를 통해 클라이언트-컴퓨터 수준의 사용자는 이 설정보다 우선 적용되는 정책이 있더라도 설치된 ESET 제품의 설정을 변경할 수 있습니다. 재정의 모드는 특정 AD 사용자에 대해 활성화하거나 비밀번호로 보호할 수 있습니다. 단, 이 기능은 한 번에 최대 4시간 동안만 활성화할 수 있습니다.

⚠ 재정의 모드가 활성화된 경우 ESET PROTECT 웹 콘솔에서 이 모드를 중지할 수 없습니다. 재정의 기간이 만료되면 재정의 모드가 자동으로 비활성화됩니다. 또한 이 기능을 클라이언트 컴퓨터에서 끌 수 있습니다.
재정의 모드를 이용 중인 사용자는 Windows 관리자 권한도 있어야 합니다. 그렇지 않으면 사용자가 ESET Endpoint Security의 설정 변경 내용을 저장할 수 없습니다.
Active Directory 그룹 인증이 지원됩니다.

재정의 모드를 설정하려면:

1. **정책** > **새 정책**으로 이동합니다.
2. **기본** 섹션에서 이 정책의 **이름**과 **설명**을 입력합니다.
3. **설정** 섹션에서 **Windows용 ESET Endpoint**를 선택합니다.
4. **재정의 모드**를 클릭하고 재정의 모드에 대한 규칙을 구성합니다.
5. **할당** 섹션에서 이 정책을 적용할 컴퓨터나 컴퓨터 그룹을 선택합니다.
6. **요약** 섹션에서 설정을 검토하고 **마침**을 클릭하여 정책을 적용합니다.



*John*이 자신의 컴퓨터에서 일부 중요한 기능이나 웹 브라우저를 차단하는 Endpoint 설정에 문제를 겪고 있는 경우 관리자는 *John*이 기존의 Endpoint 정책을 재정의하고 컴퓨터에서 설정을 수동으로 수정할 수 있도록 할 수 있습니다. 이후 관리자가 새 정책을 생성할 수 있도록 ESET PROTECT에서 새로운 이 설정을 요청할 수 있습니다.
이렇게 하려면 아래 단계를 따릅니다.
1. **정책** > **새 정책**으로 이동합니다.
2. **이름**과 **설명** 필드에 내용을 작성합니다. **설정** 섹션에서 **Windows용 ESET Endpoint**를 선택합니다.
3. **재정의 모드**를 클릭하고 1시간 동안 재정의 모드를 활성화한 후 AD 사용자로 *John*을 선택합니다.
4. 정책을 *John* 컴퓨터에 할당하고 **마침**을 클릭하여 정책을 저장합니다.
5. *John*은 자신의 ESET Endpoint에서 **재정의 모드**를 활성화하고 컴퓨터에서 설정을 수동으로 변경해야 합니다.
6. ESET PROTECT 웹 콘솔에서 **컴퓨터**로 이동한 후 *John* 컴퓨터를 선택하고 **상세 정보 표시**를 클릭합니다.
7. **구성** 섹션에서 **구성 요청**을 클릭하여 최대한 빨리 클라이언트에서 구성을 가져오는 클라이언트 작업을 예약합니다.
8. 잠시 후 새 구성이 표시됩니다. 설정을 저장할 제품을 클릭하고 **구성 열기**를 클릭합니다.
9. 설정을 검토한 후 **정책으로 변환**을 클릭할 수 있습니다.
10. **이름**과 **설명** 필드에 내용을 작성합니다.
11. **설정** 섹션에서 필요에 따라 설정을 수정할 수 있습니다.
12. **할당** 섹션에서 이 정책을 *John* 컴퓨터(또는 다른 사람의 컴퓨터)에 할당할 수 있습니다.
13. **마침**을 클릭하여 설정을 저장합니다.
14. 더는 필요 없는 재정의 정책은 제거해야 합니다.

ESET Endpoint Security에 권장되는 정책을 적용하는 방법

ESET Endpoint Security을(를) ESET PROTECT에 연결한 후의 모범 사례는 권장되는 정책 또는 사용자 지정 정책을 적용하기 위한 것입니다.

ESET Endpoint Security용 기본 제공 정책은 여러 가지가 있습니다.

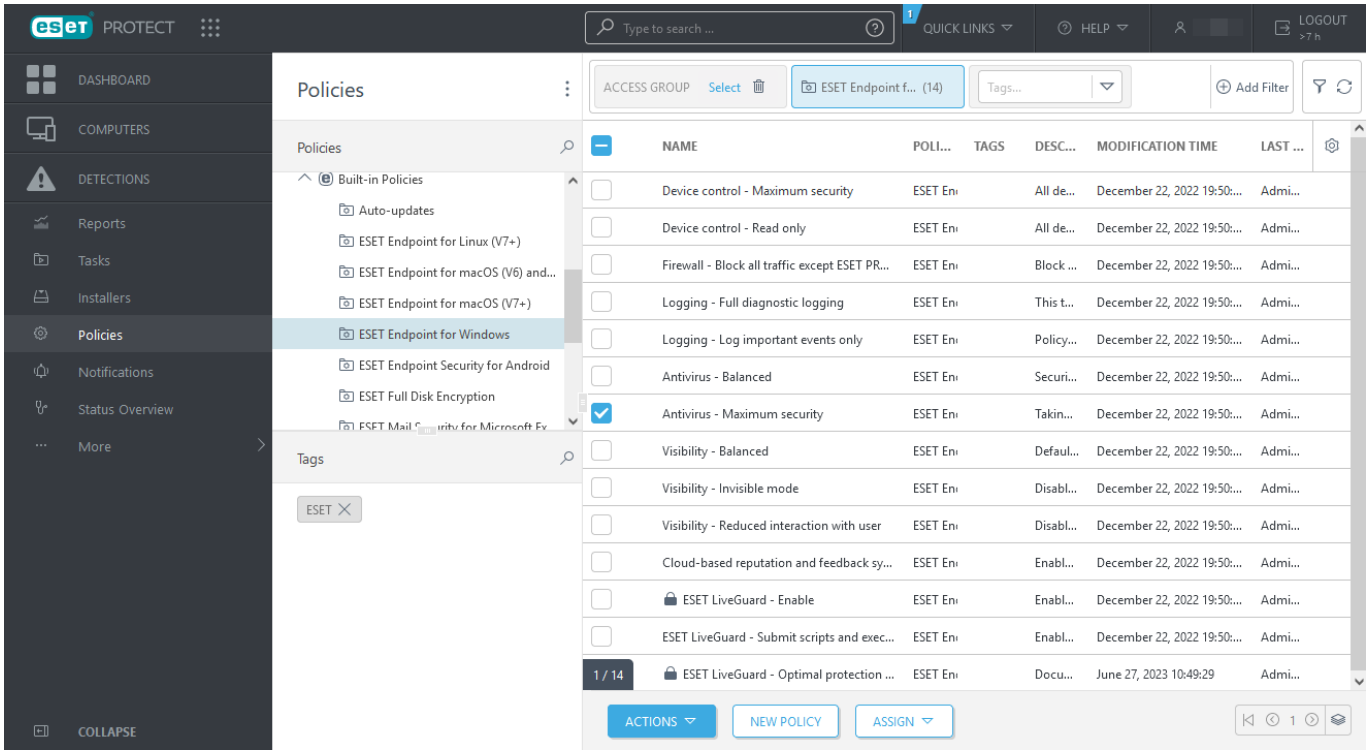
정책	설명
안티바이러스 - 균형	대부분의 설정에 권장되는 보안 구성입니다.
안티바이러스 - 최대 보안	머신 러닝, 깊은 동작 검사 및 SSL 필터링 기능을 활용합니다. 잠재적으로 안전하지 않고 원치 않는 감염 의심 애플리케이션의 탐지에 영향을 줍니다.
클라우드 기반 평판 및 피드백 시스템	최신 위협 탐지를 개선하고 향후 분석을 위해 악의적이거나 알 수 없는 잠재적 위협을 공유할 수 있도록 피드백 시스템 뿐만 아니라 ESET LiveGrid® 클라우드 기반 평판을 활성화합니다.
장치 제어 - 최대 보안	모든 장치가 차단됩니다. 장치를 연결하려면 관리자가 허용해야 합니다.
장치 제어 - 읽기 전용	모든 장치는 읽기만 가능합니다. 쓰기가 허용되지 않습니다.
방화벽 - ESET PROTECT 및 ESET Inspect 연결을 제외한 모든 트래픽 차단	ESET PROTECT 및 ESET Inspect 서버(ESET Endpoint Security만 해당) 연결을 제외한 모든 트래픽을 차단합니다.
로깅 - 전체 분석 로깅	이 템플릿을 통해 관리자는 필요 시 모든 로그를 확인할 수 있습니다. HIPS 및 ThreatSense, 방화벽을 포함한 최소 상세 수준으로 모든 항목이 기록됩니다. 로그는 90일 후에 자동으로 삭제됩니다.
로깅 - 중요한 이벤트만 기록	정책에 따라 경고, 오류 및 주요 이벤트가 기록됩니다. 로그는 90일 후에 자동으로 삭제됩니다.

정책	설명
표시 여부 - 균형	표시 여부 기본 설정. 상태 및 알림이 활성화되어 있습니다.
표시 여부 - 숨김 모드	비활성화된 알림, 경고, GUI, 상황에 맞는 메뉴에 통합. egui.exe가 실행되지 않습니다. ESET PROTECT Cloud에서의 관리 용도로만 적합합니다.
표시 여부 - 사용자와의 상호 작용 감소	상태, 알림이 비활성화되고 GUI는 표시됩니다.

워크스테이션에 설치된 ESET Endpoint Security용 권장 설정을 50개 넘게 적용하는 **안티바이러스 - 최대 보호** 라는 정책을 설정하려면 다음 단계를 따르십시오.

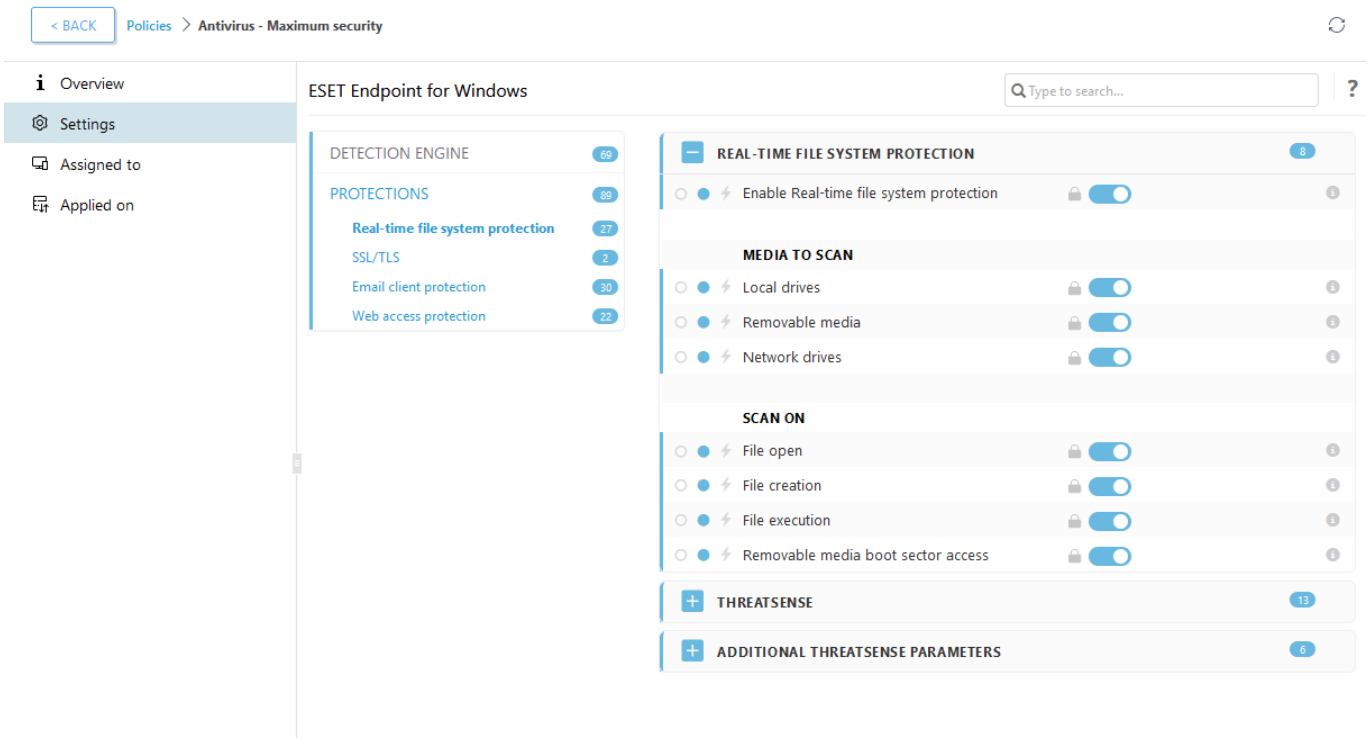
> 다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
> ESET PROTECT를 사용하여 ESET Endpoint Security에 권장되거나 미리 정의된 정책 적용

1. ESET PROTECT 웹 콘솔을 엽니다.
2. **정책**으로 이동하여 **기본 제공 정책** > **Windows용 ESET Endpoint**를 확장합니다.
3. **안티바이러스 - 최대 보안 - 권장**을 클릭합니다.
4. **할당 대상** 탭에서 **클라이언트 할당** 또는 **그룹 할당**을 클릭하고 이 정책을 적용하려는 해당 컴퓨터를 선택합니다.



이 정책에 적용되는 설정을 확인하려면 **설정** 탭을 클릭하고 고급 설정 트리를 확장합니다.

- 파란색 점은 이 정책에서 변경된 설정을 나타냄
- 파란색 프레임에 적힌 숫자는 이 정책에서 변경된 설정의 개수를 나타냄
- 여기에서 ESET PROTECT 정책에 대해 자세히 읽어 보기



미러를 구성하는 방법

ESET Endpoint Security은(는) 탐지 엔진 업데이트 파일의 복사본을 저장하고 ESET Endpoint Antivirus 또는 ESET Endpoint Security을(를) 실행하는 다른 워크스테이션에 업데이트를 배포하도록 구성될 수 있습니다.

업데이트 미러는 동일한 세대의 Windows용 ESET Endpoint Security을(를) 실행하는 워크스테이션을 업데이트하는 데 사용할 수 있는 업데이트 파일의 복사본을 생성합니다. (예를 들어, Windows용 ESET Endpoint Security 버전 10.x는 Windows용 ESET Endpoint Security 및 Windows용 ESET Endpoint Antivirus 10.x 버전에 대해서만 업데이트 파일을 생성함)

내부 HTTP 서버를 통해 업데이트를 제공하도록 ESET Endpoint Security를 미러 서버로 구성

1. **F5**를 눌러 고급 설정에 액세스하고 **업데이트 > 프로파일 > 업데이트 미러**를 확장합니다.
2. **업데이트**를 확장하고 **모듈 업데이트** 아래에서 **자동으로 선택** 옵션이 활성화되었는지 확인합니다.
3. **업데이트 미러**를 확장하고 **업데이트 미러 생성** 및 **HTTP 서버 활성화**를 활성화합니다.

자세한 내용은 다음을 참조하십시오.
- 업데이트 미러
- 미러에서 업데이트

공유 네트워크 폴더를 통해 업데이트를 제공하도록 미러 서버 구성

1. 로컬 또는 네트워크 장치에 공유 폴더를 생성합니다. 이 폴더는 ESET 보안 솔루션을 실행ESET하는 모든 사용자가 읽을 수 있고 로컬 SYSTEM 계정에서 쓸 수 있어야 합니다.
2. **고급 설정 > 업데이트 > 프로파일 > 업데이트 미러** 아래에서 **업데이트 미러 설정**을 활성화합니다.
3. **지우기**를 클릭하고 **편집**을 클릭하여 적절한 **스토리지 폴더**를 선택합니다. 생성된 공유 폴더를 찾아 선택합니다.

내부 HTTP 서버를 통해 모듈 업데이트를 제공하지 않으려면 **HTTP 서버 활성화**를 비활성화합니다.

ESET Endpoint Security에서 Windows 10으로 업그레이드하는 방법

최신 버전의 ESET 제품으로 업그레이드하고 최신 모듈 업데이트를 다운로드한 후 Windows 10으로 업그레이드하는 것이 좋습니다. 그러면 Windows 10으로 업그레이드하는 동안 최대 보호가 제공되며 프로그램 설정 및 라이선스 정보가 유지됩니다.

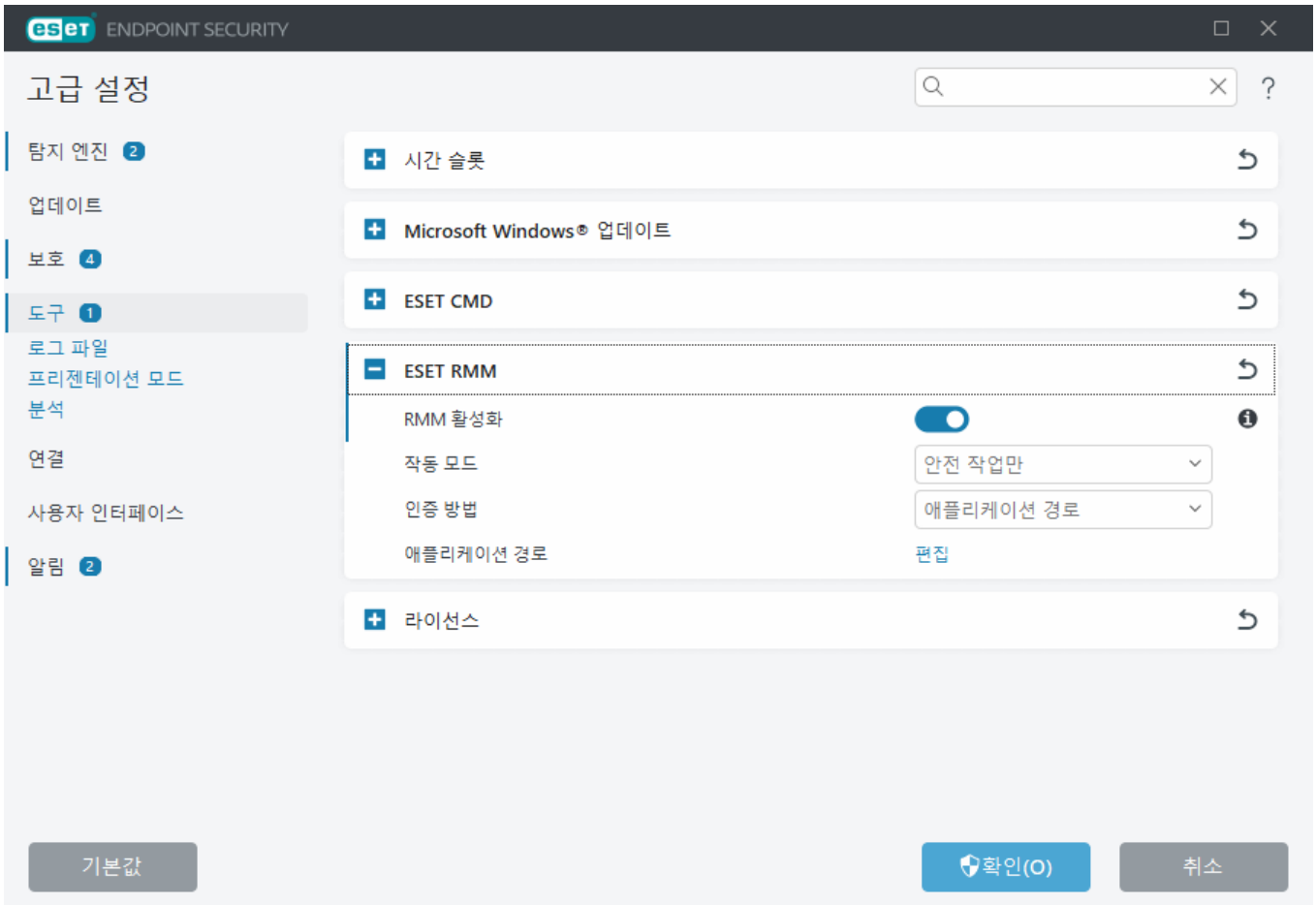
기타 언어 버전:

다른 언어 버전의 ESET 끝점 제품을 찾는 경우 ESET의 다운로드 페이지를 참조하십시오.

Windows 10과 ESET 비즈니스 제품의 호환성에 대한 자세한 내용.

원격 모니터링 및 관리를 활성화하는 방법

원격 모니터링 및 관리(RMM)는 관리 서비스 공급자가 접근할 수 있는, 로컬에 설치된 에이전트를 사용하여 소프트웨어 시스템(예: 데스크톱, 서버 및 모바일 장치의 소프트웨어 시스템)을 감독하고 제어하는 프로세스입니다. ESET Endpoint Security은(는) 버전 6.6.2028.0부터 RMM으로 관리할 수 있습니다.



ESET RMM은 기본적으로 비활성화되어 있습니다. ESET RMM을 활성화하려면 고급 설정 > **도구** > **ESET RMM**을 열고 **RMM 활성화** 옆의 토글을 활성화합니다.

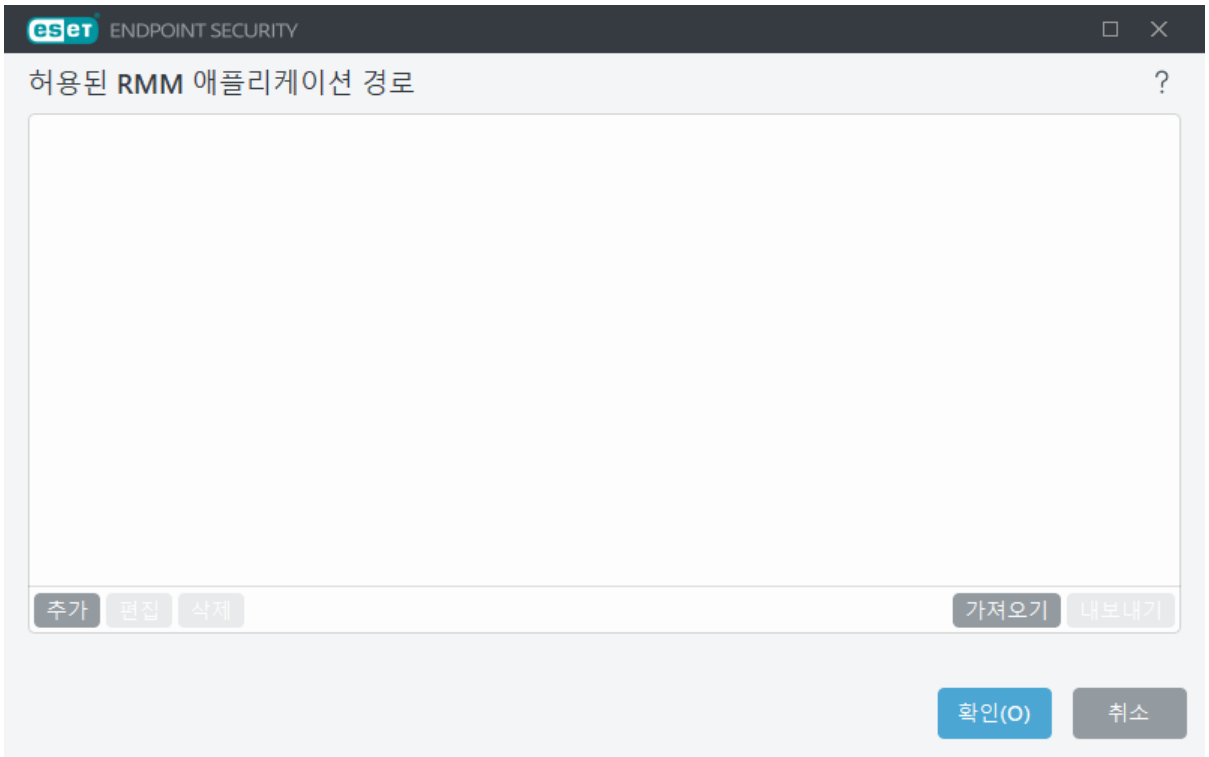
작동 모드 – 안전한 읽기 전용 작업을 위해 RMM 인터페이스를 사용하려면 **안전 작업만**을 선택합니다. 모든 작업에 대해 RMM 인터페이스를 활성화하려면 **모든 작업**을 선택합니다.

작업	안전 작업만 모드	모든 작업 모드
애플리케이션 정보 가져오기	✔	✔
구성 가져오기	✔	✔
라이선스 정보 가져오기	✔	✔
로그 가져오기	✔	✔
보호 상태 가져오기	✔	✔
업데이트 상태 가져오기	✔	✔
구성 설정		✔
활성화 시작		✔
검사 시작	✔	✔
업데이트 시작	✔	✔

인증 방법 – RMM 인증 방법을 설정합니다. 인증을 사용하려면 드롭다운 메뉴에서 **애플리케이션 경로**를 선택합니다. 인증을 사용하지 않으려면 **없음**을 선택합니다.

RMM에서는 악의적인 소프트웨어가 ESET Endpoint 보호를 비활성화하거나 회피하지 못하도록 항상 인증을 사용해야 합니다.

애플리케이션 경로 – RMM을 실행할 수 있는 특정 애플리케이션입니다. 인증 방법으로 **애플리케이션 경로**를 선택한 경우 **편집**을 클릭하여 **허용되는 RMM 애플리케이션 경로** 구성 창을 엽니다.



추가 – 허용되는 RMM 애플리케이션 경로를 새로 생성합니다. 경로를 입력하거나 **...** 버튼을 클릭하여 실행

파일을 선택합니다.

편집 – 기존의 허용되는 경로를 수정합니다. 실행 파일 위치가 다른 폴더로 바뀐 경우에는 **편집**을 사용합니다.

삭제 – 허용되는 기존 경로를 삭제합니다.

기본 ESET Endpoint Security 설치 시 Endpoint 애플리케이션 디렉터리에 ermm.exe 파일(기본 경로 *C:\Program Files\ESET\ESET Security*)이 포함됩니다. ermm.exe는 RMM 플러그인과 데이터를 교환하며, RMM 플러그인은 RMM 서버에 연결된 RMM 에이전트와 통신합니다.

- ermm.exe – ESET에서 개발한 명령줄 유틸리티로, Endpoint 제품을 관리하고 모든 RMM 플러그인과 통신할 수 있도록 해줍니다.
- RMM 플러그인은 Endpoint Windows 시스템에서 로컬로 실행되는 타사 애플리케이션입니다. Kaseya에만 해당) 및 ermm.exe와 통신하도록 설계되었습니다.
- RMM 에이전트는 Endpoint Windows 시스템에서 로컬로 실행되는 타사 애플리케이션(예: Kaseya 제품)입니다. 에이전트는 RMM 플러그인 및 RMM 서버와 통신합니다.

인터넷에서 특정 파일 유형의 다운로드를 차단하는 방법

인터넷에서 특정 파일 유형(예: exe, pdf 또는 zip)을 다운로드할 수 없도록 하려면 와일드카드가 조합된 URL 주소 관리를 사용합니다. F5 키를 눌러 **고급 설정**에 접근합니다. **웹 및 이메일** > **웹 브라우저 보호**를 클릭하고 **URL 주소 관리**를 확장합니다. **주소 목록** 옆에 있는 **편집**을 클릭합니다.

주소 목록 창에서 **차단된 주소 목록**을 선택하고 **편집** 또는 **추가**를 클릭하여 목록을 생성/편집합니다. 새 창이 열립니다. 새 목록을 생성하는 경우 **주소 목록 유형** 드롭다운 메뉴에서 **차단됨**을 선택하고 목록의 이름을 지정합니다. 현재 목록에 있는 파일 유형에 접근할 때 알림을 받으려면 **적용할 때 알림** 토글을 활성화합니다. 드롭다운 메뉴에서 **로깅 심각도**를 선택합니다. ESET PROTECT는 **경고** 상세 수준으로 레코드를 수집할 수 있습니다.

정보 및 경고 로깅 상세 수준은 도메인 내에 와일드카드가 없는 구성 요소가 두 개 이상 포함된 규칙에만 사용할 수 있습니다. 예를 들면 다음과 같습니다.
- *.domain.com/*
- *www.domain.com/*

다운로드를 차단할 파일 유형을 지정하는 마스크를 입력하려면 **추가**를 클릭합니다. 특정 웹 사이트(예: *http://example.com/file.exe*에서 특정 파일의 다운로드를 차단하려면 전체 URL을 입력합니다. 와일드카드를 사용하여 파일 그룹을 포함할 수 있습니다. 물음표(?)는 단일 변수 문자를 나타내고, 별표(*)는 0개 이상의 문자로 구성된 변수 문자열을 나타냅니다. 예를 들어, **/*.zip* 마스크는 압축된 모든 zip 파일이 다운로드되지 않도록 차단합니다.

파일 확장명이 파일 URL의 일부일 때에는 이 방법을 사용해 특정 파일 유형의 다운로드만 차단할 수 있습니다. 웹 페이지에서 파일 다운로드 URL을 사용하는 경우(예: *www.example.com/download.php?fileid=42*), 차단된 확장명이 포함되어 있더라도 이 링크에 있는 파일이 다운로드됩니다.

ESET Endpoint Security 사용자 인터페이스를 최소화하는 방법

원격으로 관리하는 경우 미리 정의된 "가시성" 정책을 적용할 수 있습니다.

그렇지 않은 경우 다음 단계를 수동으로 수행하십시오.

1. **F5** 키를 눌러 고급 설정에 접근한 후 **사용자 인터페이스 > 사용자 인터페이스 요소**를 확장합니다.
2. **시작 모드**를 원하는 값으로 설정합니다. 시작 모드에 대한 자세한 정보.
3. **시작할 때 시작 화면 표시** 및 **신호음 사용**을 비활성화합니다.
4. 알림을 구성합니다.
5. 애플리케이션 상태를 구성합니다.
6. 확인 메시지를 구성합니다.
7. 경고 및 메시지 상자를 구성합니다.

최종 사용자 사용권 계약

2021년 10월 19일부로 효력이 발생됩니다.

중요: 제품 응용 프로그램을 다운로드, 설치, 복사 또는 사용하기 전에 다음 약관을 읽어 보시기 바랍니다. **소프트웨어를 다운로드, 설치, 복사하거나 사용할 경우 다음 약관에 동의하며 다음을 인정하는 것으로 간주됩니다. 개인 정보 보호 정책.**

최종 사용자 사용권 계약

Einsteinova 24, 85101 Bratislava, Slovak Republic에 소재하고 브라티슬라바 지방 법원 상업 등기소 SRO국(입력 번호 3586/B, 사업자 등록 번호: 31333532)에 등록된 ESET, spol. s r. o.사("ESET" 또는 "공급업체")와 자연인 또는 법인("귀하" 또는 "최종 사용자") 간에 작성된 본 최종 사용자 사용권 계약("계약")의 약관에 따라 사용자는 본 계약 1조에 정의된 소프트웨어를 사용할 수 있는 권한을 보유합니다. 아래 설명되어 있는 약관을 전제로 본 계약 1조에 정의된 소프트웨어를 데이터 저장 미디어에 저장하거나, 이메일을 통해 전송하거나, 인터넷 또는 공급업체의 서버에서 다운로드하거나, 다른 공급원으로부터 얻을 수 있습니다.

본 계약은 구매 계약이 아닌 최종 사용자의 권한에 대한 계약입니다. 공급업체는 여전히 소프트웨어 복사본 및 구매 패키지에 포함된 물리적 미디어 및 본 계약에 따라 최종 사용자가 권한을 가진 기타 모든 복사본에 대한 소유권을 가지고 있습니다.

소프트웨어를 설치, 다운로드, 복사 또는 사용하는 중에 "동의함" 또는 "동의함…"을 클릭하면 본 계약의 사용 약관에 동의하고 개인 정보 보호 정책을 인정하는 것입니다. 본 계약의 모든 사용 약관 및/또는 개인 정보 보호 정책에 동의하지 않는 경우 즉시 취소 옵션을 클릭하거나, 설치 또는 다운로드를 취소하거나, 소프트웨어와 설치 미디어, 기본 설명서 및 구매 영수증을 폐기하거나 소프트웨어를 구매한 판매점에 반납하시기 바랍니다.

소프트웨어를 사용할 경우 본 계약서를 읽고 본 계약서 약관을 이해하며 준수할 것을 동의하는 것으로 인정됩니다.

1. **소프트웨어.** 본 계약서에 명시된 "소프트웨어"는 (i) 본 계약서에 따른 컴퓨터 프로그램 및 해당 구성 요소를 모두 포함하거나, (ii) 디스크, CD-ROM, DVD, 이메일 및 모든 첨부 파일 또는 본 계약서가 제공된 기타 미디어의 모든 내용(이메일이나 인터넷에서의 다운로드를 통해 데이터 저장 미디어에서 제공되는 소프트웨어의 개체 코드 형태 포함), (iii) 소프트웨어와 관련된 모든 설명 자료나 기타 가능한 모든 설명서, 상기 소프트웨어에 대한 모든 설명, 해당 사양, 소프트웨어 특성이나 작동 설명, 소프트웨어가 사용되는 작동 환경 설명, 소프트웨어의 사용 또는 설치 지침, 소프트웨어의 사용 방법에 대한 모든 설명("설명서"), (iv) 본 계약서 3조에 따라 공급업체가 사용자에게 라이선스를 제공한 경우 소프트웨어와 관련하여 해당 소프트웨어의 복사본, 소프트웨어에서 발생 가능한 오류 해결을 위한 패치, 소프트웨어에 대한 추가 사항, 소프트웨어 확장 프로그램, 수정된 소프트웨어 버전, 소프트웨어 구성 요소 업데이트를 의미합니다. 소프트웨어는 실행 개체 코드 형태로만 제공됩니다.

2. **설치, 컴퓨터 및 라이선스 키.** 데이터 저장 미디어를 통해 제공되거나, 이메일을 통해 전송되거나, 인터넷 또는 공급업체의 서버에서 다운로드하거나, 다른 공급원으로부터 얻은 소프트웨어는 설치해야 합니다. 소프트웨어는 설명서에 명시된 최소한의 요구 사항에 따라 올바르게 구성된 컴퓨터에 설치해야 합니다. 설치 방법은 설명서에 나와 있습니다. 소프트웨어에 악영향을 줄 수 있는 컴퓨터 프로그램이나 하드웨어는 소프트웨어를 설치한 컴퓨터에 설치할 수 없습니다. 컴퓨터는 개인용 컴퓨터, 랩톱, 워크스테이션, 팜톱 컴퓨터, 스마트폰, 핸드헬드 전자 장치 또는 소프트웨어가 해당 용도로 디자인되고 설치 및/또는 사용되는 기타 전자 장치를 포함하나 이에 국한되지 않는 하드웨어를 의미합니다. 라이선스 키는 소프트웨어의 합법적인 사용과 본 계약에 따라 라이선스 조항의 특정 버전 또는 확장을 허용하기 위해 최종 사용자에게 제공되는 기호, 문자, 숫자 또는 특수 기호의 고유한 시퀀스를 의미합니다.

3. **라이선스**. 본 계약서의 약관에 동의한 조건에 따라 사용자가 여기에 약정된 모든 약관을 준수하는 경우 공급업체는 다음과 같은 권한("라이선스")을 사용자에게 부여합니다.

a) **설치 및 사용.** 컴퓨터의 하드 디스크나 데이터를 영구 저장하기 위한 기타 미디어에 소프트웨어를 설치하거나, 컴퓨터 시스템의 메모리에 소프트웨어를 설치 및 저장하거나, 컴퓨터 시스템에 소프트웨어를 구현, 저장 및 표시할 수 있는 비독점적이고 양도 불가능한 권한을 사용자에게 제공합니다.

b) **라이선스 수 관련 조항.** 소프트웨어 사용 권한은 최종 사용자의 수에 따라 제한됩니다. 1명의 최종 사용자 수는 (i) 1대의 컴퓨터 시스템에 소프트웨어 설치를 의미하거나, (ii) 라이선스 범위가 사서함 수로 제한된 경우 1명의 사용자는 메일 사용자 에이전트("MUA")를 통해 이메일을 수신하는 1명의 컴퓨터 사용자를 의미합니다. MUA가 이메일을 수신하여 여러 사용자에게 자동으로 배포할 경우 이메일이 배포되는 실제 사용자 수에 따라 해당 최종 사용자 수가 결정됩니다. 메일 서버가 메일 게이트 기능을 수행할 경우, 최종 사용자 수는 해당 게이트가 서비스를 제공하는 메일 서버 사용자 수와 같습니다. 개수에 상관없이 이메일 주소가 예를 들어 별칭을 통해 한 명의 사용자에게 연결되고 한 명의 사용자가 이 주소를 수락하며, 클라이언트에서 더 많은 사용자에게 메시지를 자동으로 배포하지 않을 경우, 1대의 컴퓨터에 대한 라이선스만 필요합니다. 둘 이상의 컴퓨터에서 동일한 라이선스를 동시에 사용할 수는 없습니다. 최종 사용자는 공급업체가 부여한 라이선스의 수로 인해 발생하는 제한에 따라 최종 사용자가 소프트웨어를 사용할 수 있는 권한 범위까지만 소프트웨어에 라이선스 키를 입력할 수 있습니다. 본 계약 또는 공급업체가 허가하지 않는 한, 라이선스 키를 제3자와 공유할 수 없으며 제3자가 라이선스 키를 사용하도록 허용할 수 없습니다. 라이선스 키가 손상되면 공급업체에 즉시 알리십시오.

c) **Home/Business Edition.** Home Edition 버전의 소프트웨어는 가정/가족 전용으로 비공개 및/또는 비상업적 환경에서만 사용해야 합니다. 상업적 환경과 메일 서버, 메일 릴레이, 메일 게이트웨이 또는 인터넷 게이트웨이에서 사용하려면 Business Edition 버전의 소프트웨어를 구입해야 합니다.

d) **라이선스 기간.** 소프트웨어 사용 권한에 대한 기간은 제한됩니다.

e) **OEM 소프트웨어.** "OEM"으로 분류된 소프트웨어는 귀하가 구입한 컴퓨터에서만 사용할 수 있습니다. 다른 컴퓨터에 양도할 수 없습니다.

f) **증정용("NFR") 및 평가판 소프트웨어.** 증정용("NFR") 또는 평가판으로 분류된 소프트웨어는 판매될 수 없으며, 소프트웨어 기능을 검증 및 테스트하는 데만 사용할 수 있습니다.

g) **라이선스 종료.** 라이선스 기간이 만료되면 라이선스가 자동으로 해제됩니다. 또한 사용자가 본 계약서의 조항을 위배한 경우 공급업체는 이러한 만일의 사태에 공급업체에 제공되는 자격이나 법적제재를 침해하지 않고 계약을 철회할 수 있습니다. 라이선스 취소 시 소프트웨어와 모든 백업 복사본을 사용자 자비로 즉시 삭제 또는 폐기하거나, 소프트웨어를 구입한 매장이나 ESET으로 반납해야 합니다. 라이선스가 종료되면 공급업체는 소프트웨어 기능 사용(공급업체 서버나 타사 서버에 연결되어야 함)과 관련하여 최종 사용자의 자격을 취소할 수 있는 권한도 지닙니다.

4. **데이터 수집의 기능 및 인터넷 연결 요구 사항.** 소프트웨어를 제대로 작동하려면 인터넷에 연결되어 있어야 하며, 개인 정보 보호 정책에 따라 정기적으로 공급업체 서버 또는 제3자 서버와 해당 데이터 수집에 연결되어야 합니다. 인터넷 및 해당 데이터 수집에 대한 연결은 다음과 같은 소프트웨어 기능에 필요합니다.

a) **소프트웨어 업데이트.** 공급업체가 경우에 따라 소프트웨어 업데이트 또는 업그레이드("업데이트")를 발표할 수는 있지만, 업데이트를 제공할 의무는 없습니다. 이 기능은 소프트웨어의 표준 설정에 따라 활성화되므로, 최종 사용자가 업데이트 자동 설치를 비활성화하지 않는 한 업데이트가 자동으로 설치됩니다. 업데이트를 제공하려면 개인 정보 보호 정책에 따라 소프트웨어가 설치되는 컴퓨터 및/또는 플랫폼에 대한 정보 등 라이선스 정품 확인이 필요합니다.

업데이트 조항에는 https://go.eset.com/eol_business에서 확인 가능한 만료 정책("EOL 정책")이 적용될 수 있습니다. 소프트웨어 또는 해당 기능이 EOL 정책에 정의된 만료 날짜에 도달한 후에는 업데이트가 제공되지 않습니다.

b) **공급업체에 침입 사항 및 정보 전송.** 소프트웨어에는 컴퓨터 바이러스 및 기타 유해한 컴퓨터 프로그램 및 감염이 의심되거나 문제가 있거나, 사용자가 원치 않거나 사용자에게 안전하지 않은 개체(예: 파일, URL, IP 패킷 및 이더넷 프레임)("침입 사항")의 샘플을 수집한 뒤 이를 설치 프로세스, 소프트웨어가 설치된 컴퓨터 및/또는 플랫폼에 대한 정보, 소프트웨어의 작동 및 기능에 대한 정보("정보")를 포함하되 이에 국한되지 않은 정보와 함께 공급업체에 전송하는 기능이 포함되어 있습니다. 해당 정보 및 침입 사항에는 소프트웨어가 설치된 컴퓨터의 최종 사용자 및/또는 다른 사용자에 대한 데이터(무작위로 또는 우연히 획득한 개인 데이터 포함), 관련 메타데이터를 포함한 침입 사항의 영향을 받은 파일에 대한 데이터가 포함될 수 있습니다.

정보 및 침입 사항은 다음 소프트웨어 기능에 의해 수집될 수 있습니다.

i. LiveGrid 평판 시스템 기능에는 침입 사항 관련 단방향 해시를 수집하고 이를 공급업체에 보내는 기능이 포함됩니다. 이 기능은 소프트웨어의 표준 설정에서 활성화할 수 있습니다.

ii. LiveGrid 피드백 시스템 기능에는 관련 메타데이터를 포함한 침입 사항 및 정보를 수집하고 이를 공급업체에 보내는 기능이 포함됩니다. 이 기능은 소프트웨어를 설치하는 동안 최종 사용자에 의해 활성화될 수 있습니다.

공급업체는 침입 사항에 대한 분석 및 조사, 소프트웨어 및 라이선스 정품 확인 개선 목적에 한해, 이러한 수신된 정보와 침입 사항을 사용하고 수신된 정보 및 침입 사항을 안전하게 보호하기 위해 적절한 조치를 취해야 합니다. 소프트웨어의 이 기능을 활성화하는 경우, 개인 정보 보호 정책에 명시된 대로 관련 법률 규정에 따라 침입 사항과 정보를 수집하고 공급업체에서 처리할 수 있습니다. 이러한 기능은 언제든지 비활성화할 수 있습니다.

본 계약의 목적에 따라, 공급업체가 개인 정보 보호 정책에 따라 사용자를 식별할 수 있도록 하는 데이터를 수집, 처리 및 저장해야 합니다. 사용자는 공급업체가 자체적인 방식을 통해 사용자가 본 계약의 조항에 따라 소프트웨어를 사용하는지 확인하는 데 동의해야 합니다. 사용자는 본 계약의 목적에 따라, 소프트웨어와 공급업체 컴퓨터 시스템 또는 공급업체 유통 및 지원 네트워크에 속하는 비즈니스 파트너의 컴퓨터 시스템 간 통신 중에 소프트웨어의 기능 및 소프트웨어를 사용하고, 공급업체의 권리를 보호하기 위한 승인을 보장하기 위해 사용자의 데이터가 전송되어야 한다는 데 동의해야 합니다.

본 계약의 체결에 따라, 공급업체 또는 공급업체의 유통 및 지원 네트워크에 속하는 비즈니스 파트너는 대금 청구 목적, 본 계약의 이행 및 컴퓨터에서 알림 전송을 위해 사용자를 식별하는 필수 데이터를 전송, 처리 및 저장할 자격을 갖습니다.

개인 정보, 개인 데이터 보호 및 데이터 주체로서의 사용자 권한에 대한 자세한 내용은 공급업체의 웹 사이트에서 확인할 수 있으며, 설치 프로세스를 통해 직접 접근할 수 있습니다. 또한 소프트웨어의 도움말 섹션에서 방문할 수도 있습니다.

5. **최종 사용자의 권리 실행**. 최종 사용자의 권리는 직접 또는 직원을 통해 실행해야 합니다. 사용자는 라이선스를 얻은 컴퓨터 시스템을 보호하고 사용자의 활동을 보장하는 목적으로만 소프트웨어를 사용할 수 있습니다.

6. **권한 제한.** 소프트웨어의 일부를 복사, 배포 또는 분리하거나 소프트웨어의 파생된 버전을 만들 수 없습니다. 다음은 예외입니다.

a) 아카이브 백업 복사본을 다른 컴퓨터에 설치하거나 사용하지 않을 경우 데이터를 백업 복사본으로 영구 저장하기 위해 미디어에 소프트웨어 복사본을 하나 직접 만들 수 있습니다. 이 외에 다른 소프트웨어 복사본을 만들 경우 본 계약서를 위반하는 것이 됩니다.

b) 소프트웨어 또는 소프트웨어 복사본을 사용할 수 있는 권리를 본 계약서에서 기술한 방식 외에 다른 방식으로 사용, 수정, 해석, 복제 또는 양도할 수 없습니다.

c) 소프트웨어를 다른 개인에게 판매, 재배포 또는 임대하거나, 다른 개인으로부터 소프트웨어를 임차 또는 대여할 수 없으며, 상업적 서비스 제공을 위해 사용할 수 없습니다.

d) 소프트웨어를 역엔지니어링, 역컴파일 또는 디어셈블하거나 소프트웨어의 소스 코드를 검색할 수 없습니다. 그러나 이러한 제한이 명시적으로 법에 의해 금지된 경우는 제외합니다.

e) 저작권법이나 다른 지적 재산권으로 인한 해당 제한 사항에 따르되 제한 없이 이를 포함하여, 소프트웨어 사용에 관한 모든 해당 법률 규정에 따른 방식으로만 소프트웨어를 사용할 것을 동의합니다.

f) 이러한 서비스에 접근하는 다른 최종 사용자의 기회를 제한하지 않는 방식으로만 소프트웨어 및 해당 기능을 사용할 것을 동의합니다. 공급업체는 최대한 많은 최종 사용자가 서비스를 사용할 수 있도록, 개별 사용자에게 제공되는 서비스 범위를 제한할 권리를 보유합니다. 서비스 범위를 제한하는 것은 소프트웨어 기능 사용 기회 종료 및 소프트웨어의 특정 기능과 관련한 제3자의 서버나 공급업체 서버에 대한 데이터 및 정보 삭제를 의미하기도 합니다.

g) 사용자는 본 계약의 조항에 반하여 라이선스 키를 사용하거나, 복제 또는 생성된 라이선스 키의 무단 복제나 배포뿐만 아니라 임의 형태로 사용했거나 사용하지 않은 라이선스 키의 전송과 같이 소프트웨어 사용 자격이 없는 사람에게 라이선스 키를 제공하거나, 공급업체 이외의 출처에서 얻은 라이선스 키를 사용하여 소프트웨어를 사용하는 모든 활동을 이행하지 않는다는 데 동의합니다.

7. **저작권**. 소프트웨어의 법적 권리와 지적 재산권을 포함하되 제한 없이 소프트웨어와 소프트웨어의 모든 권한은 ESET 및/또는 해당 라이선스 공급업체의 자산입니다. 이들은 소프트웨어를 사용하고 있는 국가의 다른 모든 해당 법률과 국제 협약의 규정에 의해 보호를 받습니다. 소프트웨어의 구조, 구성 및 코드는 ESET 및/또는 해당 라이선스 공급업체의 업무상 비밀이며 기밀 정보입니다. 소프트웨어를 복사할 수 없지만 6(a)조에 지정된 경우는 예외입니다. 이에 따라 작성한 복사본에는 소프트웨어에 지정된 것과 동일한 저작권 및 법적 권한에 대한 고지 사항이 포함되어야 합니다. 본 계약서의 위반과 관련한 공급업체 권한에도 불구하고 본 계약서의 조항을 위반하여 소프트웨어의 소스 코드를 역엔지니어링, 역컴파일, 디어셈블하거나 소스 코드를 검색한 경우 이로 인해 획득한 모든 정보는 그 시점부터 모두 공급업체에게 자동으로 그리고 취소 불가능하게 양도되거나 공급업체가 소유한 것으로 간주됩니다.

8. **권리 유보**. 본 계약서에서 소프트웨어의 최종 사용자에게 명시적으로 부여한 권리를 제외한 소프트웨어의 모든 권리는 공급업체가 단독으로 유보하고 있습니다.

9. **복수의 언어 버전, 이중 미디어 소프트웨어, 복수의 복사본**. 소프트웨어에서 복수의 플랫폼이나 언어를 지원하거나 복수의 소프트웨어 복사본을 얻은 경우, 라이선스를 획득한 컴퓨터 시스템 수 및 버전에 해당하는 소프트웨어만 사용할 수 있습니다. 사용자가 이용하지 않은 소프트웨어의 버전이나 복사본은 판매, 대여, 임대, 임차, 재허여하거나 양도할 수 없습니다.

10. **계약의 시작 및 종료.** 본 계약서는 본 계약서에 동의한 날부터 유효합니다. 소프트웨어, 모든 백업 복사본 및 공급업체나 공급업체의 비즈니스 파트너로부터 획득한 모든 관련 자료를 사용자가 비용을 부담하여 영구적으로 삭제, 폐기 또는 반납할 경우 본 계약을 종료할 수 있습니다. 소프트웨어와 해당 기능의 사용 권한에는 EOL 정책이 적용될 수 있습니다. 소프트웨어 또는 해당 기능이 EOL 정책에 정의된 만료 날짜에 도달하면 소프트웨어 사용 권한이 종료됩니다. 본 계약의 종료 방법과 상관없이 7, 8, 11, 13,19 및 21조의 조항은 시간 제한 없이 계속 유효합니다.

11. **최종 사용자 선언**. 최종 사용자로서 소프트웨어는 어떤 유형의 명시적 또는 암시적 보증 없이 해당 법률에서 허용하는 최대 한도까지 "있는 그대로" 제공되며, 공급업체, 라이선스 공급업체 또는 자회사가 특히 판매 보장이나 특수 목적에의 적합성 또는 소프트웨어가 제3자의 특허권, 저작권, 상표권 또는 기타 권리를 위반하지 않는다는 보증을 포함한 어떤 명시적이거나 묵시적인 보증이나 표명을 제공하지 않음을 인정합니다. 소프트웨어에 포함된 기능이 사용자 요구 사항을 충족하거나 소프트웨어 작동이 원활하고 오류 없음을 보장하는 공급업체나 다른 당사자의 보증은 제공되지 않습니다. 의도한 결과를 달성하기 위해 또는 소프트웨어 선택, 설치 및 사용에 따른 책임과 위험은 전적으로 사용자가 부담합니다.

12. **추가 책임 없음**. 본 계약서에 명시적으로 열거된 책임을 제외한 다른 추가 책임이 공급업체 및 라이선스 공급업체에게 부과되지 않습니다.

13. **책임 제한**. 준거법에 따라 허용되는 최대 범위까지 공급업체, 해당 공급업체 직원 또는 라이선스 공급업체는 모든 수익, 매출, 판매, 데이터 손실이나 대체품 또는 서비스 조달 비용, 재산상의 손해, 인적 상해, 비즈니스 중단, 비즈니스 정보 손실 혹은 계약, 고의적인 위법 행위, 태만 또는 설치, 제품의 사용/사용 불능으로 인해 제기되는 기타 책임론의 원인과 그 발생 여부에 상관없이 특수하거나 직간접적, 우발적, 경제적, 외피성, 범죄적, 특별 손해 또는 결과적 손해에 대해 공급업체나 해당 라이선스 공급업체 또는 자회사가 이러한 손해 가능성을 통보받은 경우에도 이에 대해 책임지지 않습니다. 특정 국가와 관할지에서 책임의 제외는 허용하지 않지만 책임의 제한은 허용할 수도 있기 때문에 공급업체, 공급업체 직원 또는 라이선스 공급업체, 자회사의 책임은 사용자가 라이선스를 위해 지불한 가격으로 제한됩니다.

14. 본 계약서에 포함된 어떠한 규정도 이에 어긋나는 경우 소비자의 입장을 인정한 당사자의 법적 권한을 침해하지 않습니다.

15. **기술 지원**. ESET나 ESET에서 위탁한 제3자는 보증이나 선언 없이 단독 재량으로 기술 지원을 제공합니다. 소프트웨어 또는 해당 기능이 EOL 정책에 정의된 만료 날짜에 도달한 후에는 기술 지원이 제공되지 않습니다. 최종 사용자는 기술 지원을 제공받기 전에 기존의 모든 데이터, 소프트웨어 및 프로그램 기능을 백업해야 합니다. ESET나 ESET에서 위탁한 제3자는 기술 지원 제공으로 인한 데이터 손실, 재산상 손해, 소프트웨어나 하드웨어 손실 또는 수익 손실에 대해서는 어떤 법적 책임도 지지 않습니다. ESET나 ESET에서 위탁한 제3자는 기술 지원 범위를 벗어난 문제 해결과 관련하여 결정권을 가지고 있습니다. ESET는 단독 재량으로 기술 지원 제공을 거부, 연기 또는 종료할 권리를 보유합니다. 개인 정보 보호 정책을 준수하는 라이선스 정보, 정보 및 기타 데이터는 기술 지원을 제공하기 위해 필요할 수 있습니다

16. **라이선스 양도**. 공급업체의 동의를 받은 경우 컴퓨터 시스템 간 소프트웨어를 양도할 수 있습니다. 공급업체의 동의를 받은 경우 컴퓨터 시스템 간 소프트웨어를 양도할 수 있습니다. 공급업체의 동의를 받은 경우, 그리고 다음의 조건을 충족하는 경우에 한해 본 계약서의 모든 권한 및 라이선스를 다른 최종 사용자에게 영구적으로 양도할 수 있습니다. (i) 원래 최종 사용자가 소프트웨어 복사본을 가지고 있지 않아야 합니다. (ii) 권한은 원래 최종 사용자에게서 새로운 최종 사용자에게로 직접 양도되어야 합니다. (iii) 새로운 최종 사용자가 본 계약서의 원래 최종 사용자와 관련된 모든 권리와 책임을 맡기로 표명해야 합니다. (iv) 원래 최종 사용자가 17조에 지정된 대로 소프트웨어 정품을 확인할 수 있도록 설명서를 새로운 최종 사용자에게 제공해야 합니다.

17. **소프트웨어 정품 확인.** 최종 사용자는 다음 방법 중 하나로 소프트웨어 사용 자격을 증명할 수 있습니다. (i) 공급업체에서 지정한 제3자나 공급업체에서 발행한 라이선스 인증서를 통해, (ii) 서면으로 작성된 라이센

스 계약을 통해(이러한 계약이 체결된 경우), (iii) 라이선스 정보(사용자 이름 및 비밀번호)가 포함된 이메일을 공급업체로 전송하는 방법을 통해. 개인 정보 보호 정책에 따른 라이선스 정보 및 최종 사용자 식별 데이터는 소프트웨어 정품 확인에 필요할 수 있습니다.

18. **미국 정부 및 공공 기관을 위한 라이선스**. 본 계약서에 설명된 라이선스 권한과 제한 사항이 적용된 소프트웨어가 미국 정부를 비롯한 공공 기관에 제공됩니다.

19. **무역 관리 규정 준수**.

a) 귀하는 소프트웨어를 다른 사람에게 직간접적으로 수출, 재수출, 양도 또는 달리 제공하거나, 어떠한 방식으로든 소프트웨어를 사용하거나, ESET 또는 해당 지주 회사, 자회사 및 지주 회사의 자회사와 지주 회사가 관리하는 회사("계열사")가 다음을 포함하는 무역관리법에 의거하여 부정적인 결과를 초래하게 되거나 관련 법을 위반하게 될 수 있는 어떠한 행위에도 관여하지 않습니다.

i. 미국, 싱가포르, 영국, 유럽 연합이나 그 회원국 또는 본 계약에 따른 의무가 이행될 국가 또는 ESET이나 해당 계열사가 통합 또는 운영되는 국가의 정부, 주 또는 규제 기관에서 발표하거나 채택한 물품, 소프트웨어, 기술, 서비스의 수출, 재수출 또는 양도에 관한 라이선스 요구 사항을 규제, 제한하거나 부과하는 모든 법

ii. 경제, 금융, 무역 또는 기타 제재, 제한, 금수 조치, 수출입 제한, 자금이나 자산의 양도 혹은 서비스 수행 금지 또는 미국, 싱가포르, 영국, 유럽 연합이나 그 회원국 또는 본 계약에 따른 의무가 이행될 국가 또는 ESET이나 해당 계열사가 통합 또는 운영되는 국가의 정부, 주 또는 규제 기관에서 부과한 동등한 조치.

(법적 조치는 상기 i, ii항에 "무역관리법"으로 함께 언급되어 있음)

b) ESET은 다음과 같은 경우 본 약관에 따른 의무를 즉시 유예하거나 종료할 수 있는 권한을 보유합니다.

i. ESET이 합리적인 의견에 따라 사용자가 본 계약의 조항 19 a)조를 위반했거나 위반할 가능성이 있는 것으로 판단하는 경우

ii. 최종 사용자 및/또는 소프트웨어가 무역관리법의 적용을 받게 되어 결과적으로 ESET이 합당한 의견에 따라 본 계약의 의무를 계속 이행하면 ESET 또는 해당 계열사가 무역관리법에 의거하여 관련 법을 위반하게 되거나 부정적인 결과를 초래하게 될 수 있다고 판단하는 경우

c) 본 계약의 어떠한 조항도 해당 무역관리법과 상반되거나, 관련 법에 따라 처벌 또는 금지되는 방식으로 행동하거나 행동을 삼가도록(또는 행동하거나 행동을 삼가는 데 동의하도록) 유도 또는 요구하기 위한 것이 아니며, 이와 같이 해석되거나 이해되어서는 안 됩니다.

20. **고지 사항**. 소프트웨어 및 설명서의 모든 고지 사항과 반납은 계약 22조에 따라 본 계약, 개인 정보 보호 정책, EOL 정책 및 설명서에 대한 변경 사항을 사용자에게 전달할 ESET의 권리를 침해하지 않고 ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic으로 전달되어야 합니다. ESET은 소프트웨어를 통해 사용자에게 이메일, 앱 내 알림을 보낼 수 있으며 당사 웹 사이트에 통신 사항을 게시할 수 있습니다. 사용자는 약관, 특별 약관 또는 개인 정보 보호 정책의 변경 사항과 취급, 고지 사항 또는 기타 법적 통신에 대한 계약상의 제안/수락이나 초대 등의 법적 통신을 온라인 형태로 ESET으로부터 수신하는 데 동의합니다. 준거법에 따라 다른 형태의 통신이 특별히 요구되지 않는 한, 이러한 전자 통신은 서면으로 수신된 것으로 간주됩니다.

21. **준거법**. 본 계약서는 슬로바키아 법률에 따라 관리 및 해석됩니다. 최종 사용자와 공급업체는 준거법과 국제 물품 매매 계약에 관한 국제연합 협약 간의 상충되는 규정은 적용하지 않을 것을 동의합니다. 공급업체 또는 소프트웨어 사용과 관련된 손해 배상이나 분쟁에 대한 전속 사법권은 슬로바키아 브라티슬라바 지방 법원에 있으며, 관할권 행사는 브라티슬라바 지방 법원에 있음을 명시적으로 동의하는 바입니다.

22. **일반 조항**. 본 계약서의 특정 규정이 유효하지 않거나 실행 불가능할 경우 계약의 나머지 규정의 유효성에 영향을 미치지 않습니다. 본 계약서에 규정된 약관에 따라 나머지 규정은 여전히 유효하고 실행 가능합니다. 본 계약서는 영어로 작성되었습니다. 편의상 또는 다른 목적상 본 계약서의 번역본을 준비하거나 본 계약서의 언어 버전 간에 불일치 항목이 있는 경우 영어 버전이 우선합니다.

ESET은 (i) 소프트웨어 또는 ESET의 비즈니스 수행 방법에 대한 변경 사항을 반영하거나, (ii) 법규 또는 보안상의 이유가 있거나, (iii) 남용 또는 위해를 방지하기 위해 관련 문서를 업데이트하여 언제든지 본 계약서와 해당 부속서, 부록, 개인 정보 보호 정책, EOL 정책 및 설명서 또는 그 일부를 개정할 수 있고 소프트웨어를 변경할 수 있는 권리를 보유합니다. 사용자에게는 이메일, 앱 내 알림 또는 기타 전자적 수단을 통해 본 계약서의 개정 사항이 통지됩니다. 본 계약서에 제시된 변경 사항에 동의하지 않을 경우 10조에 따라 변경 사항을 통지받은 후 30일 이내에 계약을 해지할 수 있습니다. 이 기한 내에 계약을 해지한 경우 외에는 제시된 변경 사항을 수락한 것으로 간주하며, 변경 사항을 통지받은 날짜를 기준으로 귀하에 대한 효력이 발생됩니다.

사용자와 공급업체 간에 체결한 본 계약은 소프트웨어와 관련된 전체 계약을 나타내고, 소프트웨어 관련 정보에 대한 이전의 진술, 토론, 약정, 의사 전달 또는 공지를 완전히 대체합니다.

EULAID: EULA-PRODUCT-LG; 3537.0

개인 정보 보호 정책

Einsteinova 24, 851 01 Bratislava, Slovak Republic에 소재하고 브라티슬라바 지방 법원 상업 등기소, SRO국(입력 번호 3586/B, 데이터 통제자로서의 사업자 등록 번호: 31333532)에 등록된 ESET, spol. 사("ESET" 또는 "당사")는 고객들의 개인 데이터 및 개인 정보 처리 작업이 투명하게 이루어지기를 원합니다. 이러한 목표를 달성하기 위한 일환으로 ESET에서는 본 개인 정보 보호 정책을 게시하며, 이 정책은 고객("최종 사용자" 또는 "귀하")에게 다음과 같은 내용을 알리기 위한 목적으로만 사용됩니다.

- 개인 데이터 처리,
- 데이터 기밀성,
- 데이터 주체 권한

개인 데이터 처리

ESET에서 제공하는 서비스는 최종 사용자 사용권 계약("EULA")에 따라 제품 내에서 구현되지만 일부 서비스에는 특별한 주의가 필요할 수 있습니다. 당사의 서비스 제공과 관련된 데이터 수집에 대한 자세한 내용을 알려 드리고자 합니다. 당사는 업데이트/업그레이드 서비스, ESET LiveGrid®, 데이터 악용으로부터 보호, 지원 등 EULA와 제품 관련 문서에 설명된 다양한 서비스를 제공합니다. 모든 서비스를 제공하기 위해서는 다음 정보를 수집해야 합니다.

- 업데이트/기타 통계 - 설치 프로세스 및 제품이 설치된 플랫폼을 비롯한 컴퓨터에 대한 정보, 운영 체제, 하드웨어 정보, 설치 ID, 라이선스 ID, IP주소, MAC 주소, 제품 구성 설정 등과 같은 제품의 작동 및 기능에 대한 정보 포함
- ESET LiveGrid® 평판 시스템의 일부로 침입과 관련된 단방향 해시 - 검출된 파일을 클라우드의 허용 목록 및 차단 목록 항목 DB와 비교하여 악성코드 방지 솔루션의 효율성을 향상시킵니다.
- ESET LiveGrid® 피드백 시스템의 일부로 현장의 감염 의심 샘플과 메타데이터 - ESET에서 최종 사용자의 요구 사항에 즉각 반응하고 최신 위협에 대한 대응력을 유지합니다. 귀하께서는 아래 내용을 보내주시면 됩니다.

- 바이러스 및 기타 악성 프로그램, 감염이 의심되거나 문제가 있거나, 사용자가 원치 않거나 사용자에게 안전하지 않은 오브젝트(예: 실행 파일, 스팸으로 보고되었거나 당사 제품에 의해 플래그가 지정된 이메일 메시지)의 잠재적 샘플 등과 같은 침입 사항
- 로컬 네트워크의 장치에 대한 정보(예: 장치의 유형, 공급업체, 모델 및/또는 이름 등)
- 인터넷 사용에 관한 정보(예: IP 주소 및 지리적 정보, IP 패킷, URL 및 이더넷 프레임 등)
- 충돌 덤프 파일 및 포함된 정보

당사에서는 이 범위 외의 데이터를 수집하기를 원치 않지만 간혹 수집되는 경우가 있을 수 있습니다. 우발적으로 수집된 데이터는 악성코드 자체(사용자 모르게 또는 사용자 승인 없이)에 포함되었을 수 있거나 파일 이름 또는 URL의 일부로 포함되었을 수 있으며, 당사에서는 본 개인 정보 보호 정책에 명시된 목적에 따라 수집된 이 데이터로 당사 시스템의 일부를 구성하거나 이를 처리하지 않습니다.

- 라이선스 ID와 개인 데이터(예: 이름, 성, 주소, 이메일 주소 등)와 같은 라이선스 정보는 청구 용도, 라이선스 정품 확인 및 서비스 제공을 위해 필요합니다.
- 지원 요청에 포함된 연락처 정보 및 데이터는 지원 서비스에 필요할 수 있습니다. 연락받기로 선택한 채널을 기반으로 이메일 주소, 전화번호, 라이선스 정보, 제품 세부 사항 및 지원 사례 설명을 수집할 수 있습니다. 지원 서비스를 원활하게 제공하기 위해 기타 정보를 당사에 제공해야 할 수도 있습니다.

데이터 기밀성

ESET은 배포, 서비스 및 지원 네트워크의 일부로 계열사 또는 파트너를 통해 전 세계적으로 운영되는 회사입니다. ESET에서 처리한 정보는 서비스 제공, 지원 또는 청구 등과 같은 EULA 이행을 위해 계열사 또는 파트너와 주고받을 수 있습니다. 귀하가 사용하도록 선택한 지역 및 서비스에 따라 당사는 유럽 연합 집행 기관(European Commission)의 적절한 결정이 없는 국가로 귀하의 데이터를 전송해야 할 수도 있습니다. 이 경우에도 모든 정보의 전송은 데이터 보호법의 규제를 받으며 필요한 경우에만 수행됩니다. 표준 계약 조항, 구속력 있는 기업 규칙(BCR: Binding Corporate Rules), 또는 다른 적절한 보호 장치는 예외 없이 설정되어야 합니다.

당사는 EULA에 따라 서비스를 제공하는 동안 데이터가 필요 이상으로 오래 보관되지 않도록 최선을 다하고 있습니다. 당사의 보존 기간이 귀하의 라이선스 유효 기간보다 길기 때문에 라이선스를 갱신하는 데 아무런 문제가 없습니다. ESET LiveGrid®의 최소 및 익명화된 통계 및 기타 데이터를 추가로 처리할 수 있습니다(통계용).

ESET에서는 잠재적 위험에 적절한 수준의 보안을 보장하기 위해 적합한 기술적/조직적 조치를 구현합니다. 당사는 처리 시스템과 서비스에 대해 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장하기 위해 최선을 다하고 있습니다. 단, 데이터 위반으로 인해 귀하의 권리와 자유가 침해되는 경우 당사는 감독 기관과 데이터 주체에 이를 알릴 준비가 되어 있습니다. 데이터 주체로서 귀하는 감독 기관에 불만 사항을 제기할 권한이 있습니다.

데이터 주체 권한

ESET은 슬로바키아 법률의 적용을 받으며 유럽 연합의 일원으로 데이터 보호법을 준수해야 합니다. 해당 데이터 보호법에 규정된 조건에 따라 귀하는 데이터 주체로서 다음과 같은 권리를 부여받습니다.

- ESET의 개인 데이터에 접근을 요청할 수 있는 권리,
- 개인 데이터가 부정확한 경우 데이터를 수정할 수 있는 권리(불완전한 개인 데이터를 완료할 수 있는 권리도 부여됨),

- 개인 데이터 삭제를 요청할 수 있는 권리,
- 개인 데이터 처리에 대한 제한을 요청할 수 있는 권리
- 처리에 반대할 수 있는 권리
- 불만 사항을 제기할 수 있는 권리
- 데이터 이동성에 대한 권리.

ESET은 당사에서 처리하는 모든 정보가 소중하며 고객에게 서비스와 제품을 제공하는 합리적인 이해의 목적상 필요하다고 생각합니다.

데이터 주체로서 권한을 행사하고 싶거나 질문 또는 우려 사항이 있는 경우 다음 주소로 관련 내용을 보내주십시오.

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk