

ESET NOD32 Antivirus

사용자 설명서

[이 문서의 온라인 버전을 표시하려면 여기를 클릭](#)

Copyright ©2022 by ESET, spol. s r.o.

ESET NOD32 Antivirus는 ESET, spol. s r.o.에서 개발했습니다.

자세한 내용을 보려면 www.nod32korea.co.kr을 방문하십시오.

All rights reserved. 이 설명서의 어떠한 부분도 작성자의 서면 허가 없이는 어떠한 형식이나 수단으로도 복제, 검색 시스템에 저장 또는 전자적, 기계적, 복사, 기록, 스캐닝 또는 기타 방식으로 전송할 수 없습니다.

ESET, spol. s r.o.는 상기 애플리케이션 소프트웨어를 사전 통지 없이 변경할 수 있는 권한을 가집니다.

고객 지원: www.eset.com/support

REV. 2022년 3월 22일

1 ESET NOD32 Antivirus	1
1.1 새로운 기능	2
1.2 내게 있는 제품	2
1.3 시스템 요구 사항	3
1.3 Windows 7 버전이 오래됨	4
1.3 Windows 7은 더 이상 Microsoft에서 지원되지 않습니다	4
1.3 Windows Vista가 더 이상 지원되지 않음	5
1.4 방지	6
1.5 도움말 페이지	7
2 설치	8
2.1 라이브 설치 관리자	9
2.2 오프라인 설치	10
2.3 제품 활성화	11
2.3 활성화 중 라이선스 키 입력	12
2.3 ESET HOME 계정 사용	13
2.3 평가판 라이선스 활성화	14
2.3 무료 ESET 라이선스 키	14
2.3 활성화 실패 - 일반적인 시나리오	15
2.3 초과 사용된 라이선스로 인해 활성화 실패	15
2.3 라이선스 업그레이드	16
2.3 제품 업그레이드	17
2.3 라이선스 다운그레이드	18
2.3 제품 다운그레이드	18
2.4 설치 문제 해결사	19
2.5 설치 후 첫 번째 검사	19
2.6 최신 버전으로 업그레이드	20
2.6 레거시 제품 자동 업그레이드	21
2.7 친구에게 ESET 제품 추천	21
2.7 ESET NOD32 Antivirus이(가) 설치됨	22
2.7 다른 제품군으로 변경	22
2.7 등록	22
2.7 제품 활성화 진행률	22
2.7 제품 활성화 완료	22
3 초보자용 설명서	23
3.1 ESET HOME에 연결합니다	23
3.1 ESET HOME에 로그인	24
3.1 로그인 실패 - 일반적인 오류	25
3.1 ESET HOME에 장치 추가	26
3.2 기본 프로그램 창	26
3.3 업데이트	29
4 ESET NOD32 Antivirus 운용	30
4.1 컴퓨터 보호	32
4.1 탐지 엔진	33
4.1 탐지 엔진 고급 옵션	37
4.1 침입이 검출됨	38
4.1 실시간 파일 시스템 보호	40

4.1 치료 수준	42
4.1 실시간 보호 설정을 변경하는 경우	43
4.1 실시간 보호 검사	43
4.1 실시간 보호가 작동하지 않는 경우 수행할 작업	43
4.1 프로세스 제외	44
4.1 프로세스 제외 추가 또는 편집	45
4.1 클라우드 기반 보호	45
4.1 클라우드 기반 보호를 위한 제외 필터	48
4.1 컴퓨터 검사	48
4.1 사용자 지정 검사 시작기	50
4.1 검사 진행률	52
4.1 컴퓨터 검사 로그	53
4.1 악성코드 검사	55
4.1 유틸리티 상태 검사	55
4.1 검사 프로필	56
4.1 검사 대상	56
4.1 장치 제어	57
4.1 장치 제어 규칙 편집	58
4.1 검색된 장치	59
4.1 장치 그룹	59
4.1 장치 제어 규칙 추가	60
4.1 HIPS(호스트 침입 방지 시스템)	63
4.1 HIPS 대화 창	66
4.1 잠재적인 랜섬웨어 동작이 검출됨	67
4.1 HIPS 규칙 관리	68
4.1 HIPS 규칙 설정	69
4.1 HIPS 애플리케이션/레지스트리 경로 추가	72
4.1 HIPS 고급 설정	72
4.1 드라이버 로드가 항상 허용됨	73
4.1 게이머 모드	73
4.1 시작 검사	74
4.1 자동 시작 파일 검사	74
4.1 문서 보호	75
4.1 제외	75
4.1 성능 제외	76
4.1 성능 제외 추가 또는 편집	77
4.1 경로 제외 형식	78
4.1 탐지 제외	79
4.1 탐지 제외 추가 또는 편집	81
4.1 탐지 제외 생성 마법사	82
4.1 HIPS 제외	83
4.1 ThreatSense 파라미터	83
4.1 검사에서 제외된 파일 확장명	87
4.1 추가 ThreatSense 파라미터	88
4.2 인터넷 보호	88
4.2 프로토콜 필터링	89
4.2 제외된 애플리케이션	90

4.2 제외된 IP 주소	91
4.2 IPv4 주소 추가	92
4.2 IPv6 주소 추가	92
4.2 SSL/TLS	93
4.2 인증서	94
4.2 암호화된 네트워크 트래픽	95
4.2 알려진 인증서 목록	95
4.2 SSL/TLS 필터링된 애플리케이션 목록	96
4.2 이메일 클라이언트 보호	97
4.2 이메일 프로토콜	98
4.2 POP3, POP3S 필터	99
4.2 이메일 경고 및 알림	100
4.2 이메일 클라이언트 통합	100
4.2 Microsoft Outlook 도구 모음	101
4.2 Outlook Express 및 Windows Mail 도구 모음	101
4.2 확인 대화 상자	102
4.2 메시지 다시 검사	102
4.2 웹 브라우저 보호	102
4.2 웹 브라우저 보호 고급 설정	105
4.2 웹 프로토콜	105
4.2 URL 주소 관리	106
4.2 URL 주소 목록	107
4.2 새 URL 주소 목록 생성	108
4.2 URL 마스크 추가 방법	109
4.2 안티피싱 보호	110
4.3 프로그램 업데이트	112
4.3 업데이트 설정	114
4.3 업데이트 롤백	116
4.3 롤백 시간 간격	118
4.3 프로그램 구성 요소 업데이트	119
4.3 연결 옵션	119
4.3 업데이트 작업을 생성하는 방법	120
4.3 시스템 업데이트	120
4.3 업데이트 정보	121
4.4 도구	121
4.4 ESET NOD32 Antivirus의 도구	121
4.4 로그 파일	122
4.4 로그 필터링	123
4.4 로깅 구성	125
4.4 실행 중인 프로세스	126
4.4 보안 보고서	128
4.4 ESET SysInspector	129
4.4 스케줄러	130
4.4 예약된 검사 옵션	133
4.4 예약된 작업 개요	134
4.4 작업 상세 정보	134
4.4 작업 타이밍	134

4.4	작업 타이밍 - 한 번	135
4.4	작업 타이밍 - 매일	135
4.4	작업 타이밍 - 매주	135
4.4	작업 타이밍 - 이벤트가 트리거됨	135
4.4	건너편 작업	136
4.4	작업 상세 정보 - 업데이트	136
4.4	작업 상세 정보 - 애플리케이션 실행	136
4.4	시스템 클리너	137
4.4	ESET SysRescue Live	138
4.4	검역소	139
4.4	프록시 서버	141
4.4	분석용 샘플 전송	143
4.4	분석용 샘플 선택 - 감염 의심 파일	144
4.4	분석용 샘플 선택 - 감염 의심 사이트	144
4.4	분석용 샘플 선택 - 가양성 파일	144
4.4	분석용 샘플 선택 - 가양성 사이트	145
4.4	분석용 샘플 선택 - 기타	145
4.4	Microsoft Windows® 업데이트	145
4.5	사용자 인터페이스	146
4.5	사용자 인터페이스 요소	146
4.5	접근 설정	147
4.5	고급 설정을 위한 패스워드	148
4.5	시스템 트레이 아이콘	149
4.5	화면 리더 지원	150
4.5	도움말 및 지원	150
4.5	ESET NOD32 Antivirus 정보	151
4.5	ESET 뉴스	151
4.5	시스템 구성 데이터 전송	152
4.5	기술 지원	153
4.6	알림	153
4.6	대화 상자 창 - 애플리케이션 상태	154
4.6	바탕 화면 알림	154
4.6	바탕 화면 알림 목록	156
4.6	대화형 경고	157
4.6	확인 메시지	159
4.6	이동식 미디어	160
4.6	전달	161
4.7	개인 정보 보호 설정	163
4.8	프로필	164
4.9	키보드 단축키	165
4.10	분석	166
4.10	기술 지원	167
4.10	설정 가져오기 및 내보내기	167
4.10	현재 섹션의 모든 설정 되돌리기	168
4.10	기본 설정으로 되돌리기	169
4.10	구성 저장 중 오류 발생	169
4.11	명령줄 검사기	169

4.12 ESET CMD	171
4.13 유틸리티 상태 탐지	173
5 일반적인 질문	173
5.1 ESET NOD32 Antivirus를 업데이트하는 방법	174
5.2 내 PC에서 바이러스를 제거하는 방법	175
5.3 스케줄러에서 새 작업을 생성하는 방법	175
5.4 주간 컴퓨터 검사를 예약하는 방법	176
5.5 고급 설정의 잠금 해제 방법	177
5.6 ESET HOME에서 제품 비활성화를 해결하는 방법	177
5.6 제품이 비활성화됨, 장치 연결 해제됨	178
5.6 제품이 활성화되지 않음	178
6 사용자 환경 개선 프로그램	178
7 최종 사용자 사용권 계약	179
8 개인 정보 보호 정책	191

ESET NOD32 Antivirus

ESET NOD32 Antivirus에는 완전히 통합된 컴퓨터 보안에 대한 새로운 접근 방식이 도입되었습니다. 최신 버전의 ESET LiveGrid® 검사 엔진이 속도와 정밀도를 활용하여 컴퓨터를 안전하게 보호합니다. 그 결과, 컴퓨터를 위협에 빠뜨릴 수 있는 공격 및 악성 소프트웨어에 대해 끊임없이 경고하는 지능형 시스템이 탄생했습니다.

ESET NOD32 Antivirus는 보호 성능은 최대화된 반면 시스템 공간은 최소화된 완벽한 보안 솔루션입니다. 이 고급 기술은 인공지능을 사용하여 시스템 성능을 저해하거나 컴퓨터를 방해하지 않고 바이러스, 스파이웨어, 트로이 목마, 웜, 애드웨어, 루트킷 및 기타 위협 요소의 침입을 방지합니다.

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 NOD32 Antivirus로 통합되어 동적으로 업데이트된 지원 콘텐츠가 제공됩니다.
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 NOD32 Antivirus에서 직접 실행 중인 프로세스 및 파일의 평판을 확인할 수 있습니다.
장치 제어	모든 USB 플래시 드라이브, 메모리 카드 및 CD/DVD를 자동으로 검사합니다. 미디어 종류, 제조업체, 크기 및 기타 속성에 따라 이동식 미디어를 차단합니다.
HIPS 기능	보다 자세하게 시스템 동작을 사용자 지정하고, 시스템 레지스트리, 활성 프로세스 및 프로그램에 대한 규칙을 지정하고, 보안 정책을 미세 조정할 수 있습니다.
게이머 모드	모든 팝업 창, 업데이트 또는 기타 시스템 집약적 활동을 연기하여 게임 및 기타 전체 화면 작업을 위한 시스템 리소스를 보존합니다.

ESET NOD32 Antivirus의 기능이 작동하려면 라이선스가 활성화되어야 합니다. ESET NOD32 Antivirus 라이선스가 만료되기 몇 주 전에 라이선스를 갱신하는 것이 좋습니다.

새로운 기능

ESET NOD32 Antivirus 15의 새로운 기능

ESET HOME(이전 이름: myESET)

가시성을 높여 주고 보안을 제어합니다. 새 장치에 대한 보호 기능을 설치하고, 라이선스를 추가 및 공유하며, 모바일 앱 및 웹 포털을 통해 중요한 알림을 받습니다. 자세한 내용은 [ESET HOME 온라인 도움말 가이드](#)에서 확인할 수 있습니다.

향상된 호스트 기반 침입 방지 시스템(HIPS)

정교한 악성코드 삽입 기술로 수정할 수 있는 메모리 영역을 검사합니다. 개선 기능이 가장 정교한 악성코드 침입을 탐지할 수 있는 기술적 기능을 확장합니다.

ESET NOD32 Antivirus의 새로운 기능에 대한 이미지와 추가 정보는 [ESET 홈 제품 최신 버전에 포함된 새로운 기능](#)을 참조하십시오.

i 새로운 기능 알림을 비활성화하려면 **고급 설정 > 알림 > 바탕 화면 알림**을 클릭합니다. **바탕 화면 알림** 옆의 **편집**을 클릭하고 **새로운 기능 알림 표시** 확인란을 선택 취소합니다. 알림에 대한 자세한 내용은 [알림](#) 섹션을 참조하십시오.

내게 있는 제품

ESET은 새 제품으로 강력하고 빠른 안티바이러스 솔루션에서 최소화된 시스템 공간이 포함된 올인원 보안 솔루션까지 여러 보안 기능을 제공합니다.

- ESET NOD32 Antivirus
- ESET Internet Security
- ESET Smart Security Premium

어떤 제품을 설치했는지 알아보기 위해 [기본 프로그램 창](#)을 열면 창의 상단([지식베이스 문서](#) 참조)에 제품의 이름이 표시됩니다.

아래의 표에는 각각의 특정 제품에서 사용할 수 있는 기능이 상세히 나와 있습니다.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
탐지 엔진	✓	✓	✓
고급 머신 러닝	✓	✓	✓
Exploit 차단	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
스크립트 기반 공격 보호	✓	✓	✓
안티피싱	✓	✓	✓
웹 브라우저 보호	✓	✓	✓
HIPS(랜섬웨어 보호 포함)	✓	✓	✓
안티스팸		✓	✓
방화벽		✓	✓
네트워크 검사		✓	✓
웹캠 보호		✓	✓
네트워크 공격 보호		✓	✓
봇넷 보호		✓	✓
뱅킹 및 지불 보호		✓	✓
청소년 보호		✓	✓
개인정보보호		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

i 사용자 언어/지역에 따라 위의 제품 중 일부를 사용하지 못할 수 있습니다.

시스템 요구 사항

시스템은 ESET NOD32 Antivirus이(가) 최적으로 수행될 수 있도록 다음 하드웨어 및 소프트웨어 요구 사항을 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

지원되는 운영 체제*

Microsoft® Windows® 11

Microsoft® Windows® 10

Microsoft® Windows® 8.1

Microsoft® Windows® 8

[최신 Windows 업데이트가 있는 Microsoft® Windows® 7 SP1](#)

Microsoft® Windows® Home Server 2011 64-bit

! 운영 체제를 항상 최신 상태로 유지하도록 하십시오.

기타

활성화하고 ESET NOD32 Antivirus이(가) 제대로 작동하도록 업데이트하려면 인터넷에 연결되어 있어야 합니다.

단일 장치에서 동시에 실행되는 두 개의 안티바이러스 프로그램은 시스템 속도를 저하시켜 작동을 불가능하게 하는 등 불가피한 시스템 리소스 충돌을 일으킵니다.

* ESET은 2021년 2월 이후 지원되지 않는 운영 체제에 대한 보호 기능을 제공할 수 없습니다.

Windows 7 버전이 오래됨

문제

오래된 운영 체제 버전을 실행 중입니다. 보호된 상태를 유지하려면 운영 체제를 항상 최신 상태로 유지하도록 하십시오.

솔루션

{GET_OSNAME} {GET_BITNESS}에서 실행되는 ESET NOD32 Antivirus을(를) 설치했습니다.

최신 Windows 업데이트([KB4474419](#) 및 [KB4490628 이상](#))를 사용하여 Windows 7 서비스 팩 1(SP1)을 설치했는지 확인합니다.

사용 중인 Windows 7이 자동으로 업데이트되도록 구성되지 않은 경우, **시작 메뉴 > 제어판 > 시스템 및 보안 > Windows Update > 업데이트 확인**을 클릭한 후 **업데이트 설치**를 클릭합니다.

또한 [Windows 7은 더 이상 Microsoft에서 지원되지 않음](#)을 참조하십시오.

Windows 7은 더 이상 Microsoft에서 지원되지 않습니다.

문제

Windows 7에 대한 Microsoft 지원이 2020년 1월 14일에 종료되었습니다. [자세한 설명](#)

지원이 종료된 후에도 Windows 7을 계속 사용하면 PC가 계속 작동하지만 보안 위험 및 바이러스에 더 취약해질 수 있습니다. PC에서 더 이상 Windows 업데이트(보안 업데이트 포함)를 수신하지 않습니다.

솔루션

Windows 7에서 Windows 10으로 업그레이드하시겠습니까? ESET 제품 업데이트

업그레이드 프로세스는 비교적 쉬우며 대부분의 경우 파일을 손실하지 않고 수행할 수 있습니다. Windows 10으로 업그레이드하기 전에 다음을 수행하십시오.

1. [ESET 제품 확인/업데이트](#)
2. 중요한 데이터 백업
3. Microsoft의 [Windows 10으로 업그레이드 FAQ](#)를 읽고 Windows OS 업데이트

새 컴퓨터 또는 장치를 가져오시겠습니까? ESET 제품 이전

새 컴퓨터 또는 장치를 가져오시겠습니까? 아니면 구매하셨습니까? [기존 ESET 제품을 새 장치로 이전하는 방법](#)에 대해 알아보십시오.

i Windows 7 지원이 종료되도 참조하십시오.

Windows Vista가 더 이상 지원되지 않음

문제

Windows Vista의 기술적 한계 때문에 ESET NOD32 Antivirus은(는) **2021년 2월** 이후 보호 기능을 제공할 수 없습니다. ESET 제품이 **작동하지 않게** 됩니다. 이로 인해 시스템이 취약해져 침입이 발생할 수 있습니다.

Windows Vista에 대한 Microsoft 지원은 2017년 4월 11일에 종료되었습니다. [자세한 설명](#)

지원이 종료된 후에도 Windows Vista를 계속 사용하면 PC가 계속 작동하지만 보안 위험 및 바이러스에 더 취약해질 수 있습니다. PC에서 더 이상 Windows 업데이트(보안 업데이트 포함)를 수신하지 않습니다.

솔루션

Windows Vista에서 Windows 10으로 업그레이드하시겠습니까? 새 컴퓨터나 장치를 가져와 ESET 제품을 이전하십시오.

Windows 10으로 업그레이드하기 전에:

1. 중요한 데이터 백업
2. Microsoft의 [Windows 10으로 업그레이드 FAQ](#)를 읽고 Windows OS 업데이트
3. [기존 ESET 제품을 새 장치에 이전](#)하거나 설치하십시오.

방지

컴퓨터를 사용할 때, 특히 인터넷을 검색할 때는 현존하는 어떤 안티바이러스 시스템도 [검출 및 원격 공격](#)의 위험을 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 연구소의 전문가는 매일 이러한 위협을 분석하고 업데이트를 준비하여 발표함으로써 사용자를 위한 보안 수준을 지속적으로 향상시키고 있습니다. 이러한 업데이트의 효과를 극대화하려면 시스템에서 업데이트를 제대로 구성하는 것이 중요합니다. 업데이트를 구성하는 방법에 대한 자세한 내용은 [업데이트 설정](#) 장을 참조하십시오.

보안 패치 다운로드

악성 소프트웨어 작성자는 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: Internet Explorer)는 보안 업데이트가 정기적으로 출시되는 프로그램의 좋은 예입니다.

중요한 데이터 백업

일반적으로 맬웨어 작성자는 사용자의 요구에 개의치 않습니다. 따라서 종종 악성 프로그램으로 인해 운영 체제가 전체적으로 작동하지 않거나 중요한 데이터가 손실됩니다. 중요한 데이터는 DVD 또는 외부 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

잘 알려지거나 알려지지 않은 바이러스, 웜, 트로잔 목마 및 루트킷의 검출은 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

가장 편리하고 효과적인 규칙은 항상 조심하는 것입니다. 요즘에는 실행하고 배포하기 위해 사용자 개입을 요구하는 침입이 많이 있습니다. 따라서 새 파일을 열 때 주의를 기울이면 사용자가 부주의하여 컴퓨터에 침입이 발생했을 때 치료하기 위해 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.

도움말 페이지

ESET NOD32 Antivirus 사용자 설명서입니다. 여기서 제공되는 정보를 활용하면 사용자가 제품에 익숙해지고 컴퓨터에서 보다 안전하게 작업할 수 있습니다.

시작

ESET NOD32 Antivirus을(를) 사용하기 전에 컴퓨터 사용 중 발생할 수 있는 다양한 [검색 유형](#) 및 [위협 공격](#)을 숙지하는 것이 좋습니다.

또한 ESET NOD32 Antivirus에 소개된 [새 기능](#) 목록 및 기본 설정을 구성할 수 있도록 도와주는 설명서를 컴파일했습니다.

ESET NOD32 Antivirus 도움말 페이지를 사용하는 방법

도움말 항목은 여러 장 및 하위 장으로 구성되어 있습니다. **F1** 키를 누르면 현재 있는 창에 관한 정보를 볼 수 있습니다.

프로그램을 사용하면 키워드로 도움말 항목을 검색하거나 단어 또는 구를 입력하여 내용을 검색할 수 있습니다. 이러한 두 가지 검색 방법의 차이는 다음과 같습니다. 키워드는 도움말 페이지의 텍스트에 해당 키워드가 포함되어 있지 않더라도 논리적으로 관련이 있는 페이지를 검색합니다. 단어 및 구를 통한 검색은 모든 페이지의 내용을 검색하여 실제 텍스트에 검색한 단어 또는 구가 포함된 페이지만 표시합니다.

일관성을 확보하고 혼동을 방지하기 위해 이 설명서에서 사용된 용어는 ESET NOD32 Antivirus 파라미터 이름을 기준으로 합니다. 또한 특정 관심 분야의 항목이나 중요한 항목을 강조하기 위한 일련의 균일한 기호를 사용합니다.

i 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.

설치

컴퓨터에 ESET NOD32 Antivirus를 설치하는 방법에는 여러 가지가 있습니다. 설치 방법은 국가 및 배포 방식에 따라 다를 수 있습니다.

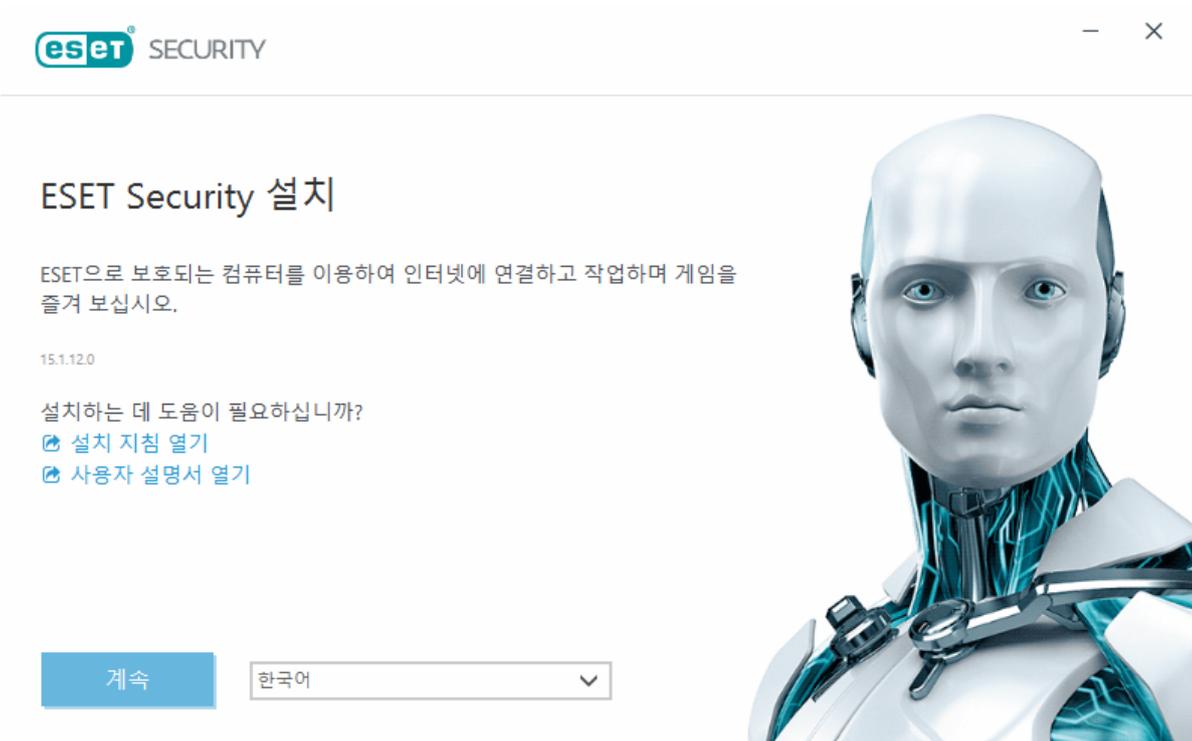
- **Live Installer** - ESET 웹 사이트나 CD/DVD에서 다운로드할 수 있습니다. 설치 패키지는 모든 언어가 동일하며 적절한 언어를 선택할 수 있습니다. Live Installer 파일 자체는 크기가 작으며 ESET NOD32 Antivirus 설치에 필요한 추가 파일은 자동으로 다운로드됩니다.
- **오프라인 설치** - Live Installer 파일보다 더 큰 .exe 파일이 사용되며 설치 완료를 위해 인터넷 연결이나 추가 파일이 필요하지 않습니다.

! ESET NOD32 Antivirus을 설치하기 전에 컴퓨터에 다른 안티바이러스 프로그램이 설치되어 있지 않은지 확인하십시오. 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 [ESET 지식 베이스 문서](#)를 참조하십시오(영어 및 기타 여러 언어로 제공).

라이브 설치 관리자

일단 [Live Installer 설치 패키지](#)를 다운로드한 후에는 설치 파일을 두 번 클릭하고 설치 관리자 마법사의 단계별 지침을 따릅니다.

! 이 유형의 설치를 사용하려면 인터넷에 연결되어 있어야 합니다.



1. 드롭다운 메뉴에서 해당 언어를 선택하고 **계속**을 클릭합니다. 설치 파일이 다운로드될 때까지 잠시 기다립니다.
2. 최종 사용자 사용권 계약을 읽고 **동의**를 클릭하여 계속 진행합니다.
3. ESET HOME 관리 포털을 사용하여 장치의 보안을 활성화하고 관리 및 확인하려면 [장치를 ESET HOME](#)합니다. ESET HOME에 연결하지 않고 계속하려면 **로그인 건너뛰기**를 클릭합니다.
4. [활성화 옵션](#)을 선택합니다. 이전 버전보다 더 최신 버전을 설치하는 경우 라이선스 키가 자동으로 입력됩니다.
5. 설치 마법사는 라이선스를 기반으로 설치할 ESET 제품을 결정합니다. 보안 기능이 가장 많은 버전이 항상 먼저 선택됩니다. [다른 버전의 ESET 제품을 설치](#)하려면 **제품 변경**을 클릭합니다.
6. 다음 기능에 대한 기본 설정을 선택하고 **계속**을 클릭하거나, **허용 후 계속**을 클릭하여 모든 기능을 활성화하고 설치 프로세스를 시작합니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

- [ESET LiveGrid® 피드백 시스템](#)
- [사용자가 원치 않는 애플리케이션](#)

- [사용자 환경 개선 프로그램](#)

7. **완료**를 클릭하여 설치 마법사를 종료합니다.

! [설치 문제 해결사](#)입니다.

i 제품이 설치되고 활성화되면 모듈이 다운로드를 시작합니다. 보호를 초기화하는 중이며 다운로드가 완료되지 않으면 일부 기능이 완전히 작동하지 않을 수 있습니다.

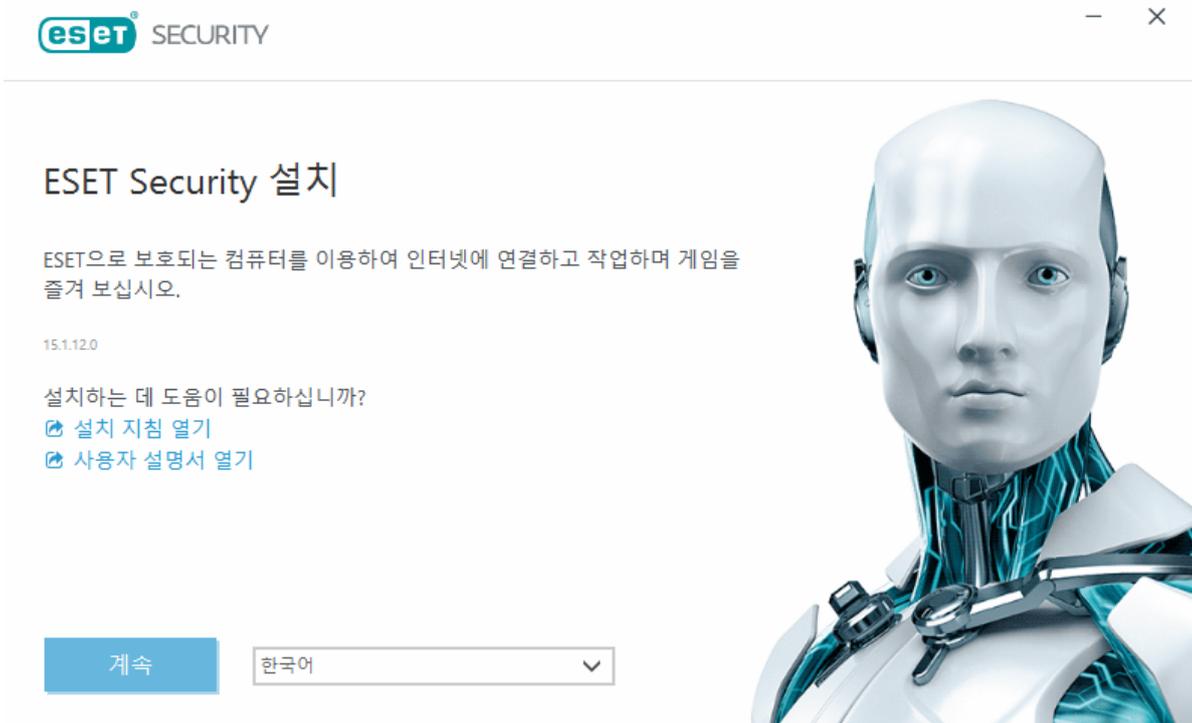
오프라인 설치

아래의 오프라인 설치 관리자(.exe)를 사용하여 ESET Windows 홈 제품을 다운로드하고 설치하십시오.

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
64비트 다운로드	64비트 다운로드	64비트 다운로드
32비트 다운로드	32비트 다운로드	32비트 다운로드
ARM 다운로드	ARM 다운로드	ARM 다운로드

! 인터넷에 연결되어 있는 경우, [Live Installer](#)를 사용하여 **ESET 제품을 설치**하십시오.

오프라인 설치 관리자(.exe)를 실행하면 설치 마법사가 설치 프로세스를 안내합니다.



1. 드롭다운 메뉴에서 적절한 언어를 선택하고 **계속**을 클릭합니다.
2. 최종 사용자 사용권 계약을 읽고 **동의**를 클릭하여 계속 진행합니다.
3. **로그인 건너뛰기**를 클릭합니다. 인터넷에 연결되어 있으면 [장치를 ESET HOME계정에 연결](#)할 수 있습니다.

4. **활성화 건너뛰기**를 클릭합니다. 제품이 완전히 작동하려면 설치 후 ESET NOD32 Antivirus 제품이 활성화되어야 합니다. [제품 활성화](#)에는 인터넷 연결이 필요합니다.
5. 설치 마법사는 다운로드한 오프라인 설치 관리자를 기반으로 설치할 ESET 제품을 표시합니다. **계속**을 클릭합니다.
6. 다음 기능에 대한 기본 설정을 선택하고 **계속**을 클릭하거나, **허용 후 계속**을 클릭하여 모든 기능을 활성화하고 설치 프로세스를 시작합니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.
 - [ESET LiveGrid® 피드백 시스템](#)
 - [사용자가 위치 않는 애플리케이션](#)
 - [사용자 환경 개선 프로그램](#)
7. **완료**를 클릭하여 설치 마법사를 종료합니다.

 [설치 문제 해결사](#)입니다.

제품 활성화

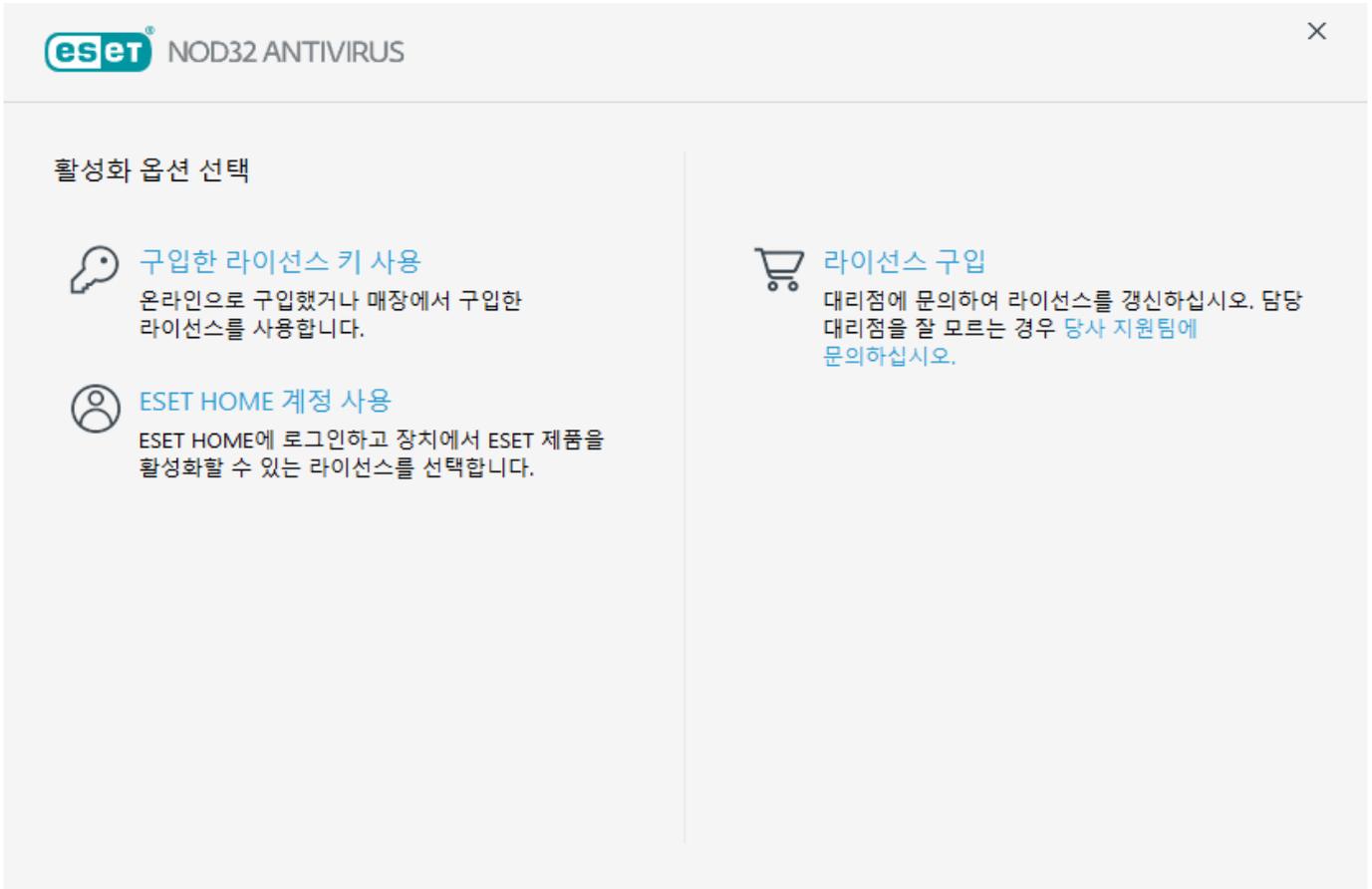
제품을 활성화하는 데 사용 가능한 방법에는 몇 가지가 있습니다. 활성화 창의 특정 활성화 시나리오 사용 가능 여부는 국가 및 배포 방법(CD/DVD, ESET 웹 페이지 등)에 따라 달라질 수 있습니다.

- 일반 정품 버전을 구매한 경우에는 **라이선스 키 입력**을 클릭하여 제품을 활성화합니다. 라이선스 키는 일반적으로 제품 패키지 안쪽이나 뒷면에 있습니다. 성공적으로 활성화하려면 제공된 그대로 라이선스 키를 입력해야 합니다. 라이선스 키 - 라이선스 소유자 식별과 라이선스 활성화에 사용되는 XXXX-XXXX-XXXX-XXXX-XXXX 또는 XXXX-XXXXXXXXX 형식의 고유한 문자열입니다.
- **ESET HOME 계정 사용**을 선택하면 ESET HOME 계정에 로그인하라는 메시지가 표시됩니다.
- 구입하기 전에 ESET NOD32 Antivirus을 평가하려면 **무료 평가판**을 선택합니다. 제한된 시간 동안 ESET NOD32 Antivirus을 활성화하려면 이메일 주소 및 국가를 입력합니다. 평가판 라이선스가 사용자에게 이메일로 전달됩니다. 평가판 라이선스는 고객당 한 번만 활성화할 수 있습니다.
- 라이선스가 없어 라이선스를 구입하려는 경우 **라이선스 구입**을 클릭합니다. 그러면 로컬 ESET 판매업체 웹 사이트로 리디렉션됩니다. ESET Windows 홈 제품 [정품 라이선스는 무료로 제공되지 않습니다](#).

언제든지 제품 라이선스를 변경할 수 있습니다. 라이선스를 변경하려면 [기본 프로그램](#) 창에서 **도움말 및 지원 > 라이선스 변경**을 클릭합니다. ESET 지원에 라이선스를 식별하는 데 사용되는 공개 라이선스 ID가 표시됩니다.

이전 ESET 제품의 활성화에 사용되는 사용자 이름과 패스워드가 있지만 ESET NOD32 Antivirus 활성화 방법을 모를 경우, [레거시 자격 증명을 라이선스 키로 변환하십시오.](#)

! [제품을 활성화하지 못하셨습니까?](#)



활성화 중 라이선스 키 입력

자동 업데이트는 보안에 있어 중요한 요소입니다. ESET NOD32 Antivirus은(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.

ESET Windows 홈 제품 [정품 라이선스는 무료로 제공되지 않습니다.](#)

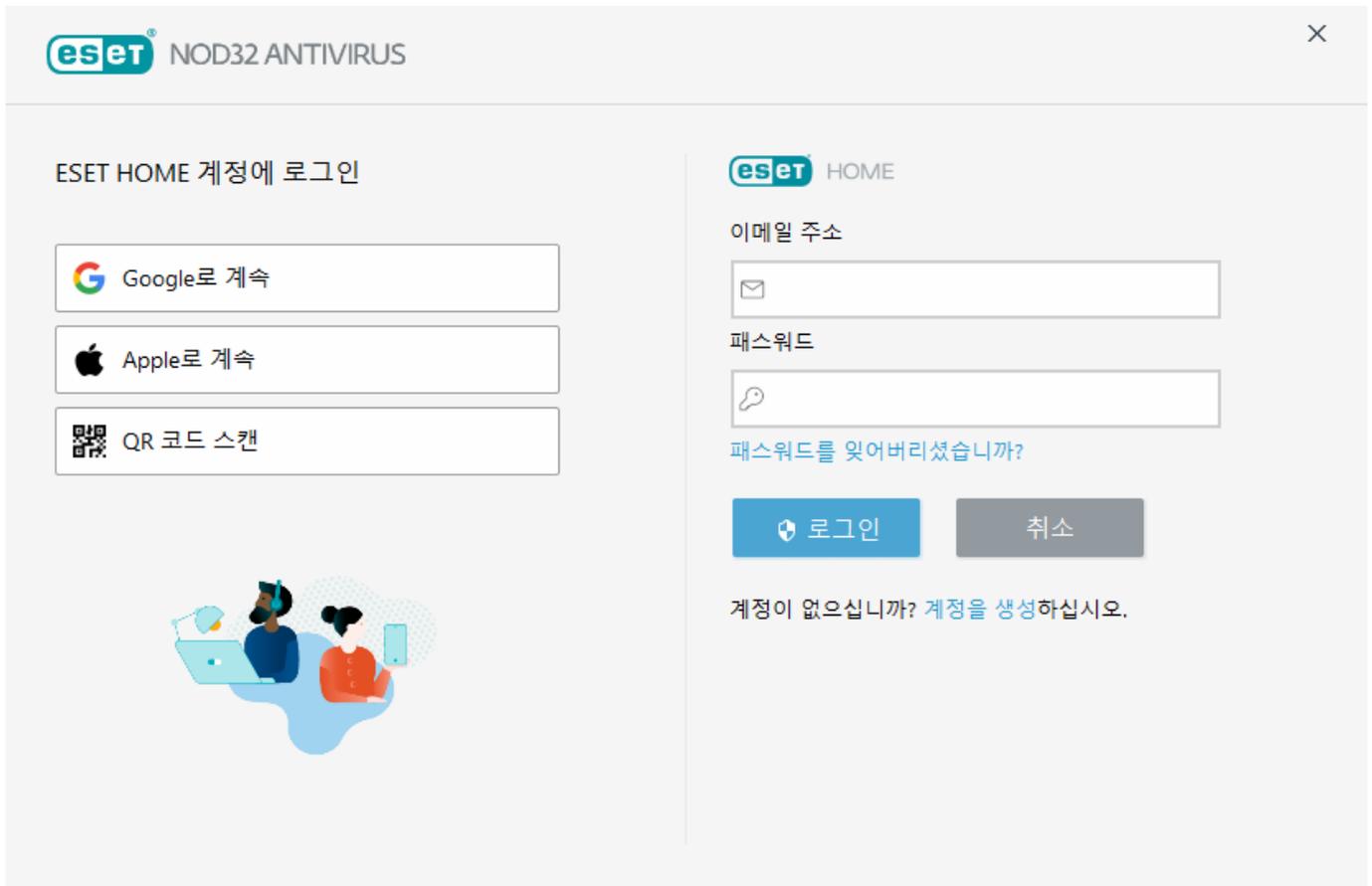
라이선스 키 입력 시 작성된 그대로 입력해야 합니다:

- 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 HOME 계정 사용

[ESET HOME](#)에 장치를 연결하여 활성화된 모든 ESET 라이선스 및 장치를 확인하고 관리하십시오. 라이선스를 갱신, 업그레이드하거나 연장하고 중요한 라이선스 상세 정보를 확인할 수 있습니다. ESET HOME 관리 포털 또는 모바일 앱에서 다른 라이선스를 추가하거나, 장치에 제품을 다운로드하거나, 제품 보안 상태를 확인하거나, 이메일을 통해 라이선스를 공유할 수 있습니다. 자세한 내용은 [ESET HOME 온라인 도움말 페이지](#)에서 확인할 수 있습니다.



활성화 방법으로 **ESET HOME 계정 사용**을 선택한 후, 또는 설치 중에 ESET HOME 계정에 연결하는 경우:

1. [ESET HOME 계정에 로그인](#)합니다.

i ESET HOME 계정이 없는 경우, **계정 생성**을 클릭하여 등록하거나 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.
패스워드를 잊어버린 경우 **패스워드를 잊어버림**을 클릭하고 화면의 단계를 따르거나 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.

2. 모든 ESET HOME 서비스에서 사용할 장치의 **장치 이름**을 설정하고 **계속**을 클릭합니다.
3. 활성화를 위한 라이선스를 선택하거나 **새 라이선스를 추가**합니다. **계속**을 클릭하여 ESET NOD32 Antivirus 제품을 활성화합니다.

평가판 라이선스 활성화

ESET NOD32 Antivirus 평가판 버전을 활성화하려면 유효한 이메일 주소를 **이메일 주소 및 이메일 주소 확인** 필드에 입력합니다. 활성화 후, ESET 라이선스가 생성되어 사용자의 이메일로 전송됩니다. 이 이메일 주소는 제품 만료 알림 및 ESET와의 기타 통신에도 사용됩니다. 평가판은 한 번만 활성화할 수 있습니다.

국가 드롭다운 메뉴에서 국가를 선택하여 기술 지원을 제공할 로컬 배포자에 ESET NOD32 Antivirus를 등록합니다.

무료 ESET 라이선스 키

전체 ESET NOD32 Antivirus 라이선스가 무료는 아닙니다.

ESET 라이선스 키는 [최종 사용자 사용권 계약](#)에 따라 ESET NOD32 Antivirus을(를) 합법적으로 사용할 수 있도록 ESET에서 제공하는, 대시로 구분된 문자 및 숫자의 고유한 시퀀스입니다. 모든 최종 사용자는 ESET이 부여한 라이선스 수에 따라 ESET NOD32 Antivirus을(를) 사용할 수 있는 권한 수준까지만 라이선스 키를 사용할 자격이 있습니다. 라이선스 키는 기밀로 취급되며 공유할 수 없지만, [ESET HOME을\(를\) 사용하여 라이선스 시트를 공유](#)할 수 있습니다.

인터넷상의 소스에서 "무료" ESET 라이선스 키를 제공할 수도 있지만 다음 사항을 기억하십시오.

- 무료 ESET 라이선스' 광고를 클릭하면 컴퓨터 또는 장치가 손상될 수 있으며 악성코드에 감염될 수 있습니다. 악성코드는 비공식 웹 콘텐츠(예: 비디오), 방문 횟수에 따라 수익을 얻기 위해 광고를 표시하는 웹 사이트 등에 숨겨져 있을 수 있습니다. 일반적으로 이를 트랩이라고 합니다.
- ESET은 불법 복제된 라이선스를 비활성화할 수 있습니다.
- 불법 복제된 라이선스 키를 보유하는 것은 ESET NOD32 Antivirus을(를) 설치하려면 동의해야 하는 [최종 사용자 사용권 계약](#)을 위반하는 행위입니다.
- www.eset.com, ESET 판매업체 또는 대리점 등 공식 채널을 통해서만 ESET 라이선스를 구입하십시오(eBay와 같은 비공식 타사 웹 사이트에서 라이선스를 구입하거나 타사에서 공유 라이선스를 구입하지 말 것).
- ESET NOD32 Antivirus [다운로드](#)는 무료이지만, 설치 중에 활성화하려면 유효한 ESET 라이선스 키가 필요합니다(다운로드하여 설치할 수는 있지만, 활성화하지 않으면 작동하지 않음).
- 인터넷 또는 소셜 미디어에 라이선스를 공유하지 마십시오(널리 유포될 수 있음).

불법 복제된 ESET 라이선스를 식별하고 보고하는 방법에 대한 지침은 [지식베이스 문서를 참조](#)하십시오.

ESET 보안 제품 구입에 대한 확신이 없는 경우 다음과 같은 방법으로 평가판 버전을 사용한 후 결정할 수 있습니다.

1. [무료 평가판 라이선스를 사용하여 ESET NOD32 Antivirus 활성화](#)
2. [ESET 베타 프로그램 참여](#)
3. Android 모바일 장치를 사용 중인 경우 무료인 [ESET Mobile Security](#)를 설치하십시오.

라이선스를 할인받거나 연장하려면:

- [친구에게 ESET NOD32 Antivirus 추천](#)
- [ESET 갱신](#)(이미 활성화 라이선스가 있는 경우) 또는 장기간 활성화

활성화 실패 - 일반적인 시나리오

ESET NOD32 Antivirus 활성화에 성공하지 못하는 경우 가장 일반적인 시나리오는 다음과 같습니다.

- 라이선스 키가 이미 사용 중인 경우
- 라이선스 키가 잘못되었습니다. 제품 활성화 양식 오류
- 제품 활성화에 필요한 추가 정보가 누락되었거나 잘못되었습니다.
- 제품 활성화 DB와의 통신에 실패했습니다. 15분 후에 다시 활성화해 보십시오.
- ESET 활성화 서버에 대한 연결이 없거나 비활성화되었습니다

적절한 라이선스 키를 입력했는지 확인하고 다시 활성화해 보십시오. 활성화하기 위해 ESET HOME 계정을 사용하는 경우 [ESET HOME 라이선스 관리 - 온라인 도움말](#)을 참조하십시오.

여전히 활성화할 수 없는 경우 [ESET 활성화 문제 해결사](#)에서 활성화 및 라이선스에 대한 일반적인 질문과 오류, 문제를 설명합니다(영어 및 기타 여러 언어로 제공).

초과 사용된 라이선스로 인해 활성화 실패

문제

- 라이선스가 초과 사용되거나 남용되고 있을 수 있음
- 초과 사용된 라이선스로 인해 활성화 실패

솔루션

이 라이선스를 사용 중인 장치 수가 허용 한도를 벗어났습니다. 소프트웨어 불법 복제나 위조를 당했을 수 있습니다. 이 라이선스는 다른 ESET 제품을 활성화하는 데 사용될 수 없습니다. 라이선스를 ESET HOME 계정에서 관리할 수 있거나 합법적인 경로로 구매한 경우 이 문제를 직접 해결할 수 있습니다. 아직 계정이 없는 경우 계정을 생성하십시오.

라이선스 소유자이고 이메일 주소를 입력하라는 메시지가 표시되지 않은 경우:

1. ESET 라이선스를 관리하려면, 웹 브라우저를 열고 <https://home.eset.com>으로 이동합니다. ESET License Manager에 접근하고 시트를 제거하거나 비활성화합니다. 자세한 내용은 [라이선스가 초과 사용된 경우 수행할 작업](#)을 참조하십시오.
2. 불법 복제된 ESET 라이선스를 식별하고 보고하는 방법에 대한 지침은 [불법 복제된 ESET 라이선스 식별 및 보고 문서를 참조](#)하십시오.
3. 잘 모르겠다면 뒤로를 클릭하고 [ESET 기술 지원으로 이메일을 보내 주십시오](#).

라이선스 소유자가 아니라면, 이 라이선스의 소유자에게 연락하여 라이선스 초과 사용으로 인해 ESET 제품을 활성화할 수 없다는 것을 알려주십시오. 라이선스 소유자는 [ESET HOME](#) 포털에서 이 문제를 해결할 수 있습니다.

이메일 주소를 확인하라는 메시지가 나타나면(일부 경우에 한함) ESET NOD32 Antivirus을(를) 구입하거나 활성화하기 위해 처음 사용한 이메일 주소를 입력합니다.

라이선스 업그레이드

이 알림은 ESET 제품을 활성화하는 데 사용되는 라이선스가 변경된 경우에 표시됩니다. 변경된 라이선스를 사용하면 보안 기능이 더 많은 제품을 활성화할 수 있습니다. 변경하지 않은 경우 ESET NOD32 Antivirus에서 **더 많은 기능을 갖춘 제품으로 변경**이라는 경고 창을 한 번 표시합니다.

예 (권장) – 보안 기능이 더 많은 제품을 자동으로 설치합니다.

아니요 – 변경되지 않으며 알림이 사라집니다.

나중에 제품을 변경하려면 [ESET 지식베이스 문서](#)를 참조하십시오. ESET 라이선스에 대한 자세한 내용은 [라이선스 FAQ](#)를 참조하십시오.

아래의 표에는 각각의 특정 제품에서 사용할 수 있는 기능이 상세히 나와 있습니다.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
탐지 엔진	✓	✓	✓
고급 머신 러닝	✓	✓	✓
Exploit 차단	✓	✓	✓
스크립트 기반 공격 보호	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
안티피싱	✓	✓	✓
웹 브라우저 보호	✓	✓	✓
HIPS(랜섬웨어 보호 포함)	✓	✓	✓
안티스팸		✓	✓
방화벽		✓	✓
네트워크 검사		✓	✓
웹캠 보호		✓	✓
네트워크 공격 보호		✓	✓
봇넷 보호		✓	✓
뱅킹 및 지불 보호		✓	✓
청소년 보호		✓	✓
개인정보보호		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

제품 업그레이드

기본 설치 관리자를 다운로드하고 활성화할 제품을 변경하기로 결정했거나 설치된 제품을 보안 기능이 더 많은 제품으로 변경하고자 합니다.

[설치 중에 제품을 변경](#)합니다.

아래의 표에는 각각의 특정 제품에서 사용할 수 있는 기능이 상세히 나와 있습니다.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
탐지 엔진	✓	✓	✓
고급 머신 러닝	✓	✓	✓
Exploit 차단	✓	✓	✓
스크립트 기반 공격 보호	✓	✓	✓
안티피싱	✓	✓	✓
웹 브라우저 보호	✓	✓	✓
HIPS(랜섬웨어 보호 포함)	✓	✓	✓
안티스팸		✓	✓
방화벽		✓	✓
네트워크 검사		✓	✓
웹캠 보호		✓	✓
네트워크 공격 보호		✓	✓
봇넷 보호		✓	✓
뱅킹 및 지불 보호		✓	✓
청소년 보호		✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
개인정보보호		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

라이선스 다운그레이드

이 대화 상자는 ESET 제품을 활성화하는 데 사용되는 라이선스가 변경된 경우에 표시됩니다. 변경된 라이선스는 보안 기능이 더 적은 다른 ESET 제품에서만 사용할 수 있습니다. 보호 기능의 손실을 방지하기 위해 제품이 자동으로 변경되었습니다.

ESET 라이선스에 대한 자세한 내용은 [라이선스 FAQ](#)를 참조하십시오.

아래의 표에는 각각의 특정 제품에서 사용할 수 있는 기능이 상세히 나와 있습니다.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
탐지 엔진	✓	✓	✓
고급 머신 러닝	✓	✓	✓
Exploit 차단	✓	✓	✓
스크립트 기반 공격 보호	✓	✓	✓
안티피싱	✓	✓	✓
웹 브라우저 보호	✓	✓	✓
HIPS(랜섬웨어 보호 포함)	✓	✓	✓
안티스팸		✓	✓
방화벽		✓	✓
네트워크 검사		✓	✓
웹캠 보호		✓	✓
네트워크 공격 보호		✓	✓
봇넷 보호		✓	✓
뱅킹 및 지불 보호		✓	✓
청소년 보호		✓	✓
개인정보보호		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

제품 다운그레이드

현재 설치된 제품에는 활성화하려는 제품보다 더 많은 보안 기능이 있습니다.

아래의 표에는 각각의 특정 제품에서 사용할 수 있는 기능이 상세히 나와 있습니다.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
탐지 엔진	✓	✓	✓
고급 머신 러닝	✓	✓	✓
Exploit 차단	✓	✓	✓
스크립트 기반 공격 보호	✓	✓	✓
안티피싱	✓	✓	✓
웹 브라우저 보호	✓	✓	✓
HIPS(랜섬웨어 보호 포함)	✓	✓	✓
안티스팸		✓	✓
방화벽		✓	✓
네트워크 검사		✓	✓
웹 캠 보호		✓	✓
네트워크 공격 보호		✓	✓
봇넷 보호		✓	✓
뱅킹 및 지불 보호		✓	✓
청소년 보호		✓	✓
개인정보보호		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

설치 문제 해결사

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

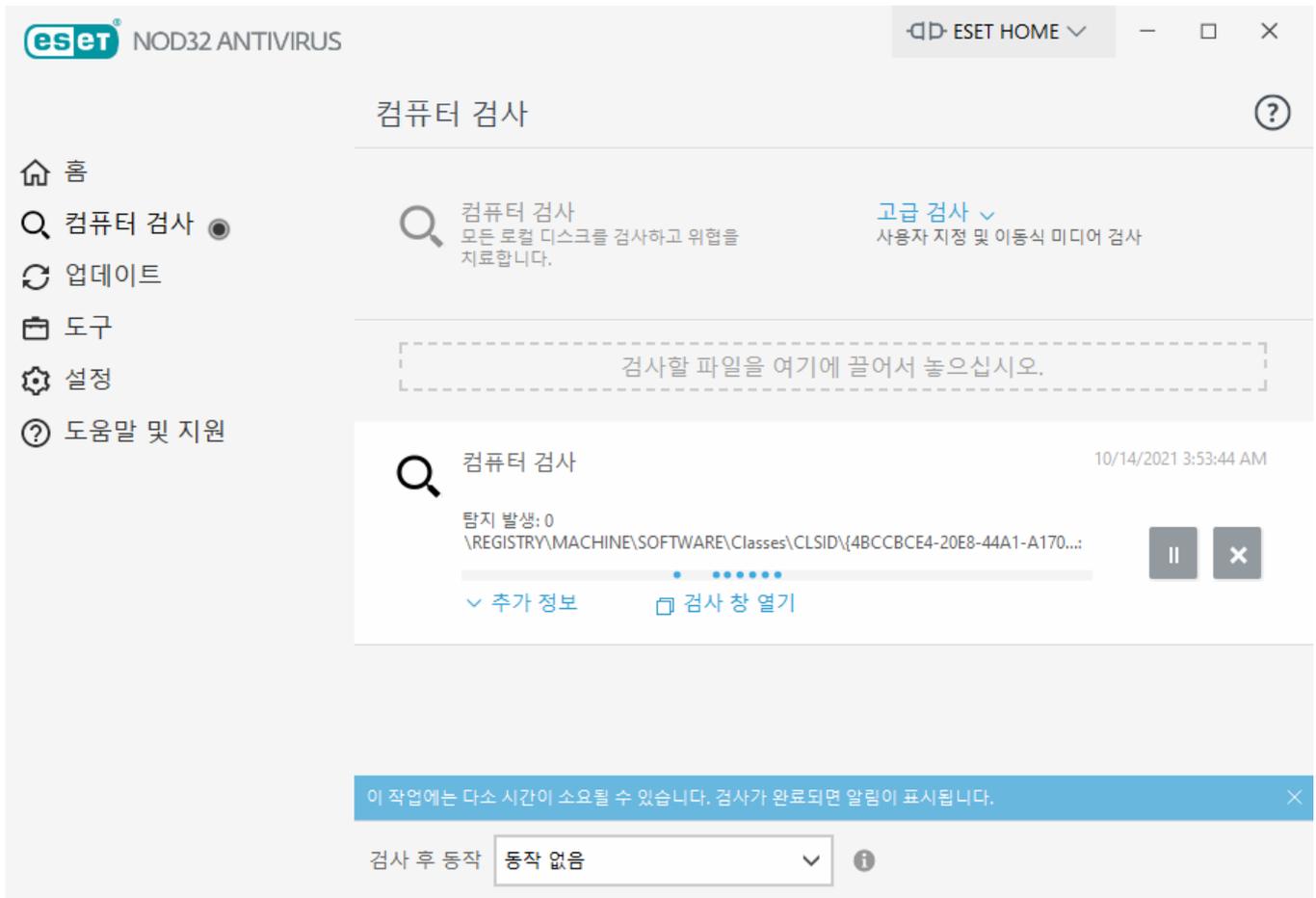
문제 해결사 실행을 클릭하여 문제 해결사를 시작합니다. 문제 해결사가 완료되면 권장 솔루션을 따르십시오.

문제가 지속되면 [일반적인 설치 오류 및 해결 방법](#) 목록을 참조하십시오.

설치 후 첫 번째 검사

ESET NOD32 Antivirus 설치 후 악성 코드를 확인하기 위해 처음 업데이트하면 컴퓨터 검사가 자동으로 시작됩니다.

컴퓨터 검사 > 컴퓨터 검사를 클릭하여 [기본 프로그램](#) 창에서 컴퓨터 검사를 수동으로 시작할 수도 있습니다. 컴퓨터 검사에 대한 자세한 내용은 [컴퓨터 검사](#) 섹션을 참조하십시오.



최신 버전으로 업그레이드

최신 버전의 ESET NOD32 Antivirus이(가) 발표되어 제품을 개선하거나 프로그램 모듈의 자동 업데이트로 해결할 수 없는 문제를 해결할 수 있습니다. 최신 버전으로의 업그레이드는 다음과 같은 몇 가지 방법으로 수행할 수 있습니다.

1. 프로그램 업데이트를 통해 자동으로
프로그램 업그레이드는 모든 사용자에게 배포되고 특정 시스템 구성에 영향을 줄 수 있으므로, 가능한 모든 시스템 구성에서 원활하게 작동되는지 오랜 기간 테스트를 거친 후 발표됩니다. 최신 제품이 발표된 직후 최신 버전으로 업그레이드해야 하는 경우 다음 방법 중 하나를 사용합니다.
고급 설정(F5) > 업데이트에서 **애플리케이션 업데이트**를 활성화했는지 확인합니다.
2. [기본 프로그램](#) 창의 **업데이트** 섹션에서 **업데이트 확인**을 클릭하여 수동으로
3. 최신 버전을 다운로드한 후 이전 버전 위에 [설치](#)하는 방식을 통해 수동으로

자세한 내용 및 그림이 포함된 지침은 다음을 참조하십시오.

- [ESET 제품 업데이트 - 최신 제품 모듈 확인](#)
- [다른 ESET 제품 업데이트 및 릴리스 유형](#)

레거시 제품 자동 업그레이드

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

⚠ 일반적인 설치 문제

i 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 계약](#)에 동의하고 [개인 정보 보호 정책](#)을 승인합니다. 최종 사용자 사용권 계약에 동의하지 않는 경우 **제거**를 클릭합니다. 이 경우 이전 버전으로 되돌릴 수 없습니다.
2. [ESET LiveGrid® 피드백 시스템](#) 및 [사용자 환경 개선 프로그램](#)을 모두 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 활성화](#)합니다.
4. 설치를 완료하려면 장치를 다시 시작해야 합니다.

친구에게 ESET 제품 추천

이 ESET NOD32 Antivirus 버전부터 ESET 제품의 사용 경험을 가족이나 친구와 공유할 수 있도록 추천 보너스를 제공합니다. 평가판 라이선스로 활성화한 제품의 추천도 공유할 수 있습니다. 평가판 사용자인 경우 추천을 보내서 실제로 제품이 활성화될 때마다 귀하와 친구들 다 평가판 라이선스에 추가 기간이 부여됩니다.

설치된 ESET NOD32 Antivirus을(를) 사용하여 추천할 수 있습니다. 추천 가능한 제품은 현재 추천을 보내는 제품입니다. 아래 표를 참조하십시오.

내가 설치한 제품	추천 가능한 제품
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

제품 추천

추천 링크를 보내려면 ESET NOD32 Antivirus 기본 메뉴에서 **친구 추천**을 클릭합니다. [추천 링크](#)

공유를 클릭합니다. 사용 중인 제품에서 추천 링크를 생성하여 새 창에 표시합니다. 해당 링크를 복사하여 가족과 친구에게 보냅니다. **Facebook**에서 공유, **Gmail** 연락처 추천 및 **Twitter**에서 공유 옵션을 사용하여 ESET 제품에서 바로 추천 링크를 공유할 수 있습니다.

친구에게 보낸 추천 링크를 친구가 클릭하면, 제품을 다운로드하고 무료 보호 기능을 1개월 더 사용할 수 있는 웹 페이지로 리디렉션됩니다. 평가판 사용자인 경우 각 추천 링크가 활성화될 때마다 알림이 표시되고, 무료 보호 기능을 1개월 더 사용할 수 있도록 라이선스가 자동 연장됩니다. 이렇게 하면 최대 5개월까지 무료 보호 기능을 연장할 수 있습니다. ESET 제품의 친구 추천 창에서 활성화된 추천 링크 수를 확인할 수 있습니다.

i 추천 기능은 해당 언어/지역에서 제공되지 않을 수 있습니다.

ESET NOD32 Antivirus이(가) 설치됨

ESET NOD32 Antivirus 설치를 계속하려면 **계속**을 클릭하십시오.

제품 변경 옵션을 사용하면 ESET 라이선스에 따라 ESET Windows 홈 제품 간에 전환할 수 있습니다. 자세한 내용은 [사용 중인 제품](#)을 참조하십시오.

다른 제품군으로 변경

ESET 라이선스에 따라 ESET Windows 홈 제품 간에 전환할 수 있습니다. 자세한 내용은 [사용 중인 제품](#)을 참조하십시오.

등록

등록 양식에 포함된 필드에 기재하고 활성화를 클릭하여 라이선스를 등록하십시오. 괄호가 표시된 필드는 필수 항목입니다. 이 정보는 ESET 라이선스 관련 작업에만 사용됩니다.

활성화 진행률

활성화 프로세스가 완료되는 데 몇 초 정도 걸릴 수 있습니다(필요한 시간은 인터넷 연결 속도 또는 컴퓨터에 따라 다를 수 있음).

제품 활성화 완료

활성화 프로세스가 완료되었습니다.

모듈 업데이트는 몇 초 후에 시작되며, ESET NOD32 Antivirus의 정기 업데이트는 즉시 시작됩니다.

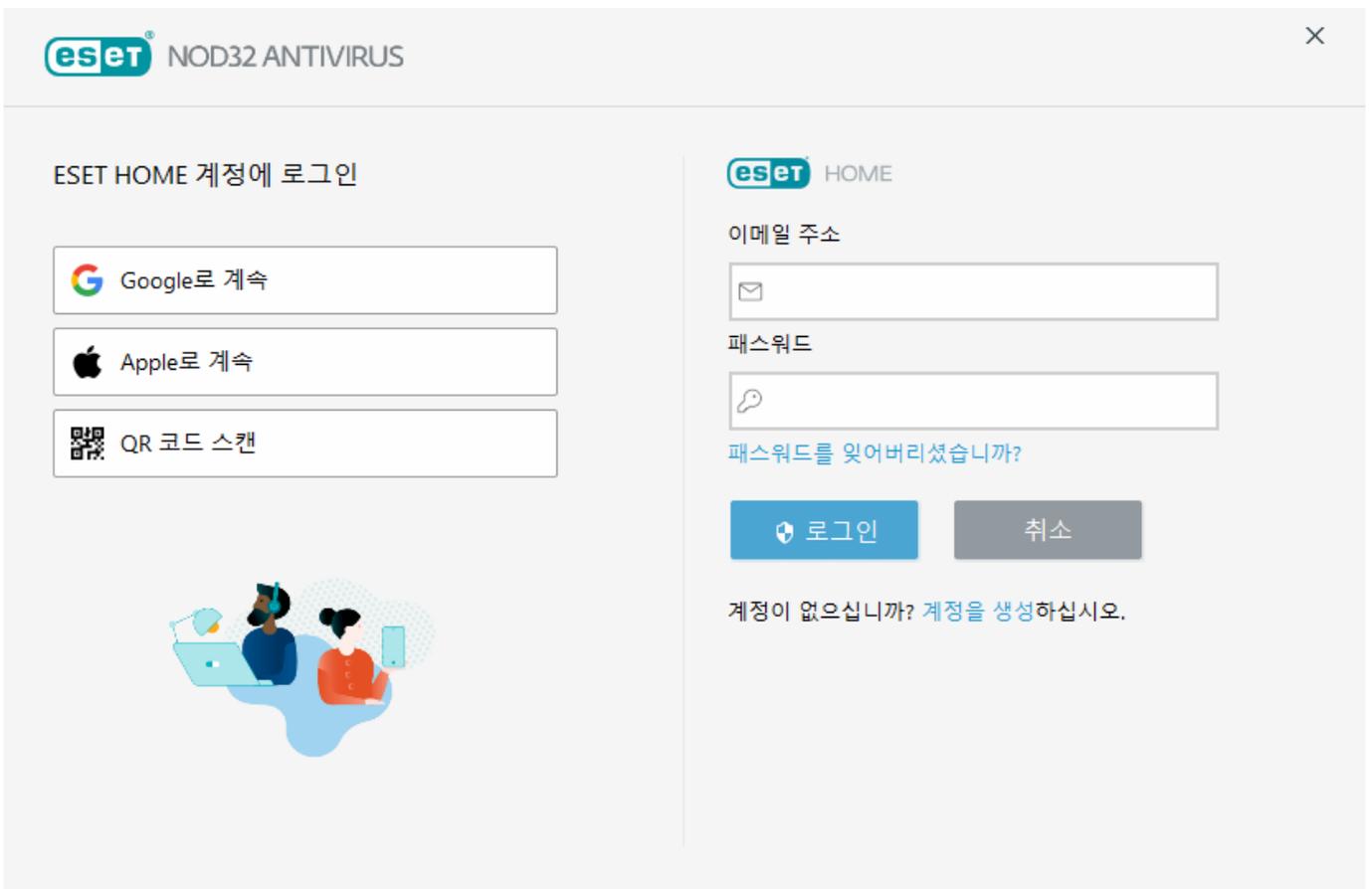
모듈 업데이트 후 20분 이내에 첫 번째 검사가 자동으로 시작됩니다.

초보자용 설명서

이 장에서는 ESET NOD32 Antivirus의 초기 개요 및 해당 기본 설정에 대해 설명합니다.

ESET HOME에 연결합니다

[ESET HOME](#)에 장치를 연결하여 활성화된 모든 ESET 라이선스 및 장치를 확인하고 관리하십시오. 라이선스를 갱신, 업그레이드하거나 연장하고 중요한 라이선스 상세 정보를 확인할 수 있습니다. ESET HOME 관리 포털 또는 모바일 앱에서 다른 라이선스를 추가하거나, 장치에 제품을 다운로드하거나, 제품 보안 상태를 확인하거나, 이메일을 통해 라이선스를 공유할 수 있습니다. 자세한 내용은 [ESET HOME 온라인 도움말 페이지](#)에서 확인할 수 있습니다.



ESET HOME 에 장치 연결:

설치 중에 ESET HOME에 연결하거나 활성화 방법으로 **ESET HOME 계정 사용**을 선택한 경우, 프로세스가 다릅니다. [ESET HOME 계정 사용](#) 항목에서 지침을 참조하십시오.

i 이미 ESET NOD32 Antivirus이(가) 설치되어 있고 ESET HOME 계정에 추가된 라이선스로 활성화된 경우, ESET HOME 포털을 사용하여 장치를 ESET HOME에 연결할 수 있습니다. [ESET HOME 온라인 도움말 가이드](#)의 지침에 따라 [ESET NOD32 Antivirus에서 연결을 허용하십시오](#).

1. [기본 프로그램 창](#)에서, **ESET HOME > ESET HOME** 연결을 클릭하거나 이 장치를 **ESET HOME** 계정 알림에 연결에서 **ESET HOME**에 연결을 클릭합니다.
2. [ESET HOME 계정에 로그인합니다.](#)

i ESET HOME 계정이 없는 경우, **계정 생성**을 클릭하여 등록하거나 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.
 패스워드를 잊어버린 경우 **패스워드를 잊어버림**을 클릭하고 화면의 단계를 따르거나 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.

3. 장치 이름을 설정하고 **계속**을 클릭합니다.
4. 연결되면 상세 정보 창이 표시됩니다. **완료**를 클릭합니다.

ESET HOME에 로그인

ESET HOME 계정에 로그인하기 위해 사용할 수 있는 방법이 몇 가지 있습니다.

- **ESET HOME 이메일 주소 및 패스워드 사용** - ESET HOME 계정 생성에 사용한 **이메일 주소**와 **패스워드**를 입력하고 **로그인**을 클릭합니다.
- **Google 계정/AppleID 사용** - **Google**로 계속하거나 **Apple**로 계속하고 적절한 계정에 로그인합니다. 로그인되면, ESET HOME 확인 웹 페이지로 리디렉션됩니다. 계속하려면 ESET 제품 창으로 다시 전환합니다. Google 계정/AppleID 로그인에 대한 자세한 내용은 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.
- **QR 코드 스캔** - **QR 코드 스캔**을 클릭하여 QR 코드를 표시합니다. ESET HOME 모바일 앱을 열고 QR 코드를 스캔하거나 장치의 카메라로 QR 코드를 가리킵니다. 자세한 내용은 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.

i ESET HOME 계정이 없는 경우, **계정 생성**을 클릭하여 등록하거나 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.
 패스워드를 잊어버린 경우 **패스워드를 잊어버림**을 클릭하고 화면의 단계를 따르거나 [ESET HOME 온라인 도움말](#)의 지침을 참조하십시오.

⚠ [로그인 실패 - 일반적인 오류.](#)

ESET HOME 계정에 로그인



eSet HOME

이메일 주소

패스워드

패스워드를 잊어버리셨습니까?

계정이 없으십니까? [계정을 생성하십시오.](#)

로그인 실패 - 일반적인 오류

이러한 자격 증명을 갖는 계정이 없음

입력한 이메일 주소나 패스워드가 ESET HOME 계정과 일치하지 않습니다. **다시 시도**를 클릭하고 올바른 이메일 주소와 패스워드를 입력하십시오.

로그인하려면, ESET HOME 계정을 생성해야 합니다. ESET HOME 계정이 없는 경우, **다시 시도 > 계정 생성**을 클릭하거나 [새 ESET HOME 계정 생성](#)을 참조하십시오.

패스워드를 잊어버린 경우, **다시 시도 > 패스워드를 잊어버림**을 클릭하고 화면의 단계를 따르거나 [ESET HOME 패스워드를 잊어버림](#)을 참조하십시오.

잘못된 비밀번호

이 오류는 ESET NOD32 Antivirus이(가) 이미 ESET HOME에 연결되어 있고 로그인해야 하는 변경(예: Anti-Theft 비활성화)을 수행하고 입력한 패스워드가 계정과 일치하지 않는 경우에 발생할 수 있습니다. 올바른 패스워드를 입력하고 **다시 시도**를 클릭합니다. 여전히 로그인할 수 없는 경우 **다시 시도 > 패스워드를 잊어버림**을 클릭하여 패스워드를 다시 설정하고 화면의 단계를 따르거나 [ESET HOME 패스워드 잊어버림](#)을 참조하십시오.

선택한 로그인 옵션이 계정과 일치하지 않습니다.

계정이 소셜 미디어 계정에 연결되어 있습니다. ESET HOME에 로그인하려면 **Google로 계속** 또는 **Apple로 계속**을 클릭하고 해당 계정에 로그인합니다. 로그인에 성공하면 ESET HOME 확인 웹 페이지로 리디렉션됩니다. ESET HOME 포털의 ESET HOME계정에서 소셜 미디어 계정의 연결을 해제할 수 있습니다.

ESET HOME에 장치 추가

이미 ESET NOD32 Antivirus이(가) 설치되어 있고 ESET HOME 계정에 추가된 라이선스로 활성화된 경우 ESET HOME 포털을 사용하여 장치를 ESET HOME에 연결할 수 있습니다.

1. [장치에 연결 요청을 보냅니다.](#)
2. ESET NOD32 Antivirus에서 ESET HOME 계정 이름과 함께 **ESET HOME 계정에 이 장치 연결** 대화 상자 창을 표시합니다. **허용**을 클릭하여 언급된 ESET HOME 계정에 장치를 연결합니다.

i 상호 작용이 없는 경우 약 30분 후에 연결 요청이 자동으로 취소됩니다.

기본 프로그램 창

ESET NOD32 Antivirus의 기본 프로그램 창은 두 개의 기본 섹션으로 구분됩니다. 오른쪽의 기본 창은 왼쪽의 기본 메뉴에서 선택한 옵션에 해당하는 정보를 표시합니다.

그림이 포함된 지침

i 영어 및 기타 여러 언어로 제공되는 그림이 포함된 지침은 [ESET Windows 제품의 기본 프로그램 창 열기](#)를 참조하십시오.

ESET HOME - [ESET HOME에 장치를 연결](#)합니다. **ESET HOME**을(를) 사용하여 활성화된 ESET 라이선스 및 장치를 확인하고 관리합니다.

다음은 기본 메뉴 내의 옵션에 대한 설명입니다.

홈 - ESET NOD32 Antivirus의 보호 상태에 대한 정보를 제공합니다.

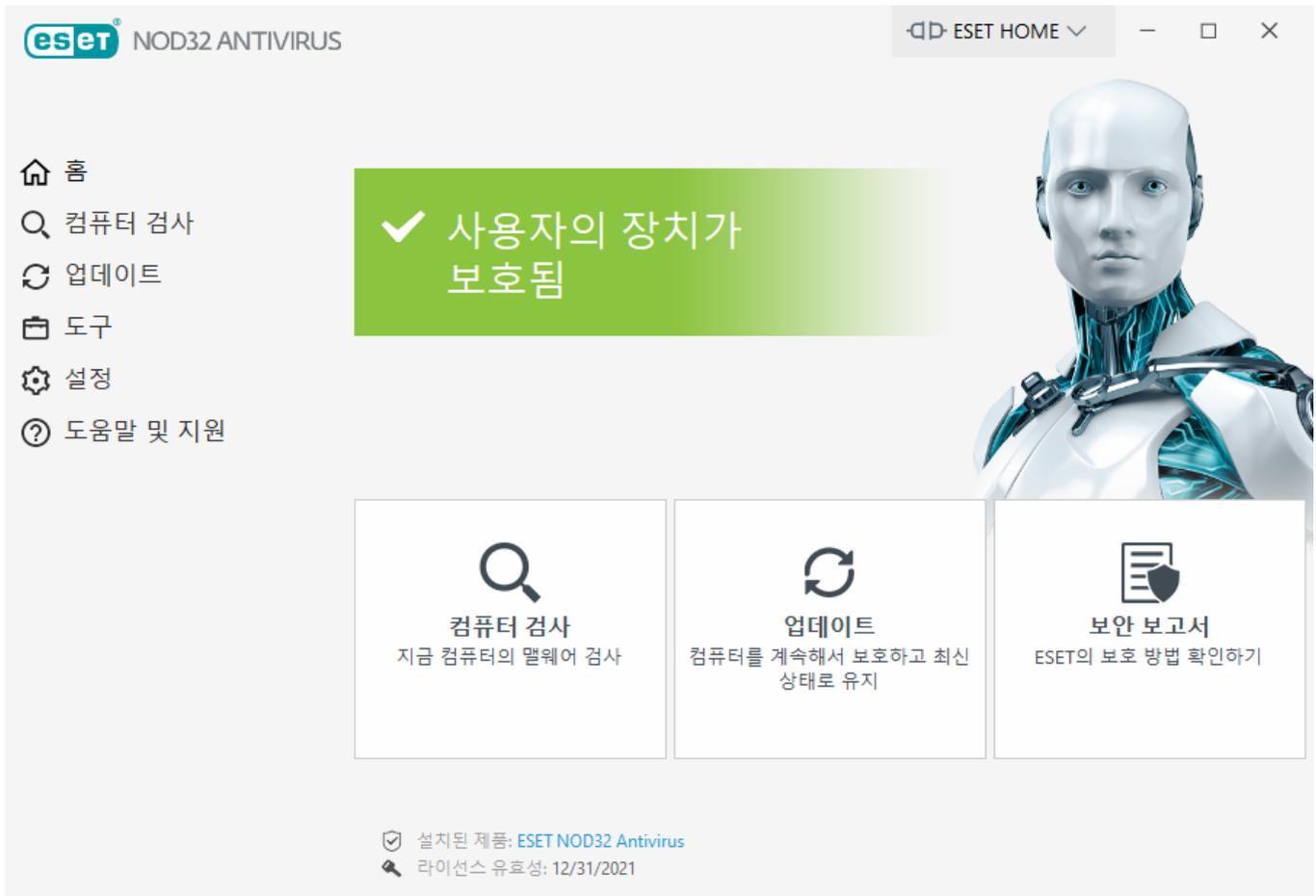
컴퓨터 검사 - 컴퓨터 검사를 구성 및 시작하거나 사용자 지정 검사를 생성합니다.

업데이트 - 검색 엔진 업데이트에 대한 정보를 표시합니다.

도구 - 프로그램 관리를 간소화하고 고급 사용자용 추가 옵션을 제공하는 데 도움이 되는 모듈에 대한 액세스 권한을 제공합니다. 자세한 내용은 [ESET NOD32 Antivirus의 도구](#)를 참조하십시오.

설정 - 컴퓨터, 인터넷.

도움말 및 지원 - 도움말 파일, [ESET 지식 베이스](#), ESET 웹 사이트 및 지원 요청을 전송할 수 있는 링크에 접근할 수 있습니다.

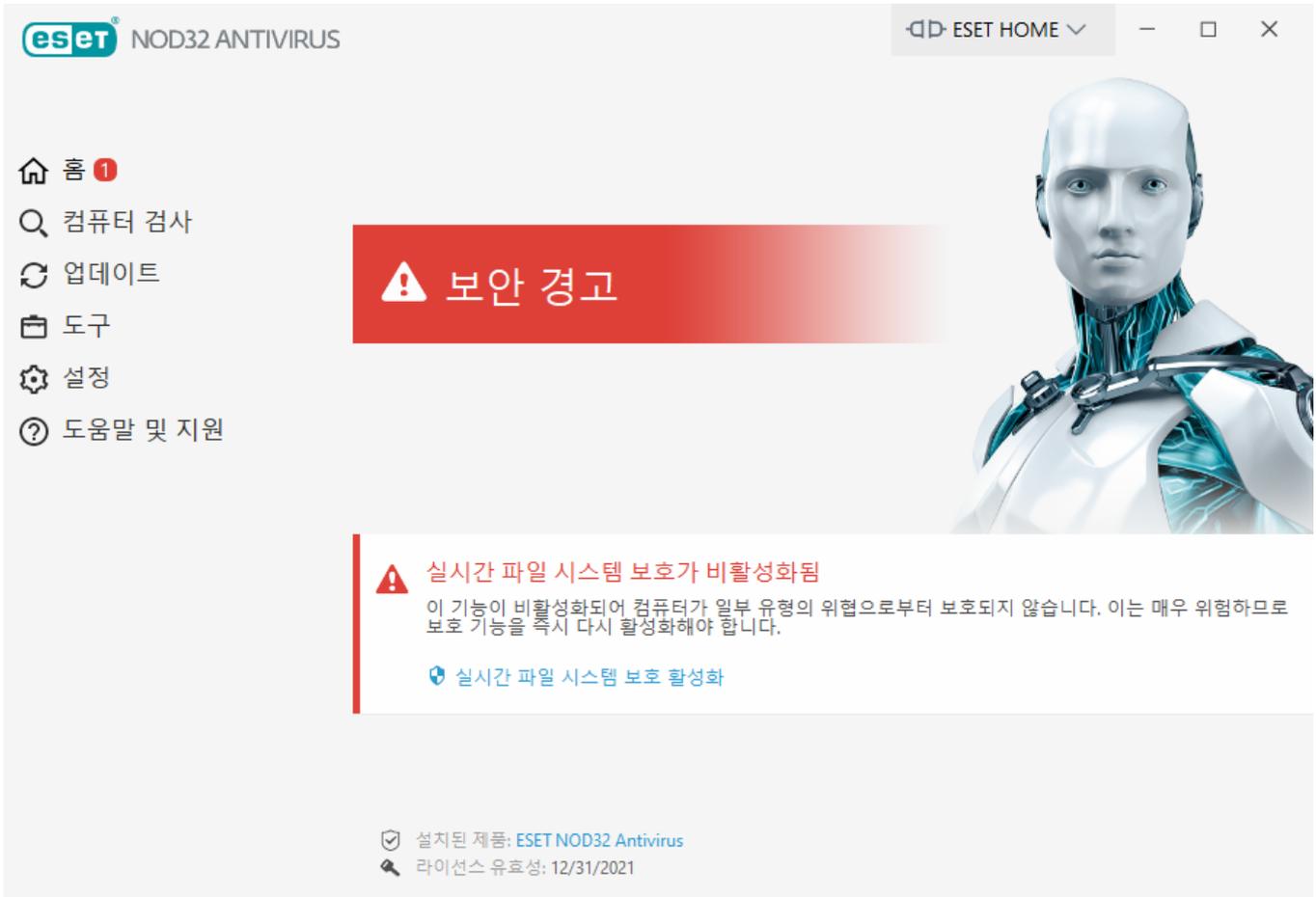


홈 화면에는 컴퓨터의 현재 보호 수준에 대한 중요한 정보가 포함됩니다. 상태 창에는 자주 사용하는 ESET NOD32 Antivirus 기능이 표시됩니다. 설치된 제품과 라이선스 만료 날짜에 대한 정보도 여기에서 확인할 수 있습니다. 다른 버전의 ESET 제품을 설치하고 싶다면 **ESET NOD32 Antivirus**을(를) 클릭하십시오. [각 특정 제품의 기능에 대한 자세한 내용을 확인](#)하십시오.

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

프로그램이 제대로 작동하지 않는 경우 수행할 작업

활성 보호 모듈이 제대로 작동하고 있으면 보호 상태 아이콘이 녹색으로 표시됩니다. 빨간색 느낌표나 주황색 알림 아이콘이 있으면 최대 보호가 적용되지 않음을 나타냅니다. 각 모듈의 보호 상태에 대한 자세한 정보와 최대 보호를 복원할 때 제안되는 해결 방법이 **홈** 아래에 표시됩니다. 개별 모듈의 상태를 변경하려면 **설정**을 클릭하고 원하는 모듈을 선택합니다.



! 빨간색 아이콘과 빨간색 **보안 경고** 상태는 심각한 문제를 나타냅니다. 이 상태는 다음과 같은 몇 가지 이유 때문에 표시될 수 있습니다.

- **제품이 활성화되지 않음** 또는 **라이선스 만료됨** - 빨간색 보호 상태 아이콘으로 나타납니다. 라이선스가 만료되면 프로그램에서 업데이트를 수행할 수 없습니다. 라이선스를 갱신하려면 경고 창의 지침을 따르십시오.
- **검색 엔진이 오래된 버전임** - 검색 엔진을 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 설정**이 잘못 구성되었기 때문입니다.
- **실시간 파일 시스템 보호가 비활성화됨** - 사용자가 실시간 보호를 비활성화했습니다. 컴퓨터가 위협으로부터 보호되지 않습니다. **실시간 파일 시스템 보호 활성화**를 클릭하여 이 기능을 다시 활성화합니다.
- **안티바이러스, 안티스파이웨어 보호 비활성화됨** - **안티바이러스, 안티스파이웨어 보호 활성화**를 클릭하여 안티바이러스 및 안티스파이웨어 보호를 다시 활성화할 수 있습니다.

! 주황색 아이콘은 제한된 보호를 나타냅니다 (예: 프로그램을 업데이트하는 중 문제 발생 또는 라이선스 만료일 임박). 이 상태는 다음과 같은 몇 가지 이유 때문에 표시될 수 있습니다.

- **게이머 모드 활성화** - **게이머 모드**를 활성화하면 보안상 위협할 수 있습니다. 이 기능을

활성화하면 모든 팝업 창이 비활성화되고 예약된 모든 작업이 중지됩니다.

- **라이선스가 곧 만료됨** - 보호 상태 아이콘이 표시되고 시스템 시계 옆에 느낌표가 표시됩니다. 라이선스가 만료된 후에는 프로그램이 업데이트할 수 없으며 보호 상태 아이콘이 빨간색으로 변합니다.

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

업데이트

컴퓨터의 보안 수준을 최대로 유지하기 위한 가장 좋은 방법은 ESET NOD32 Antivirus를 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.

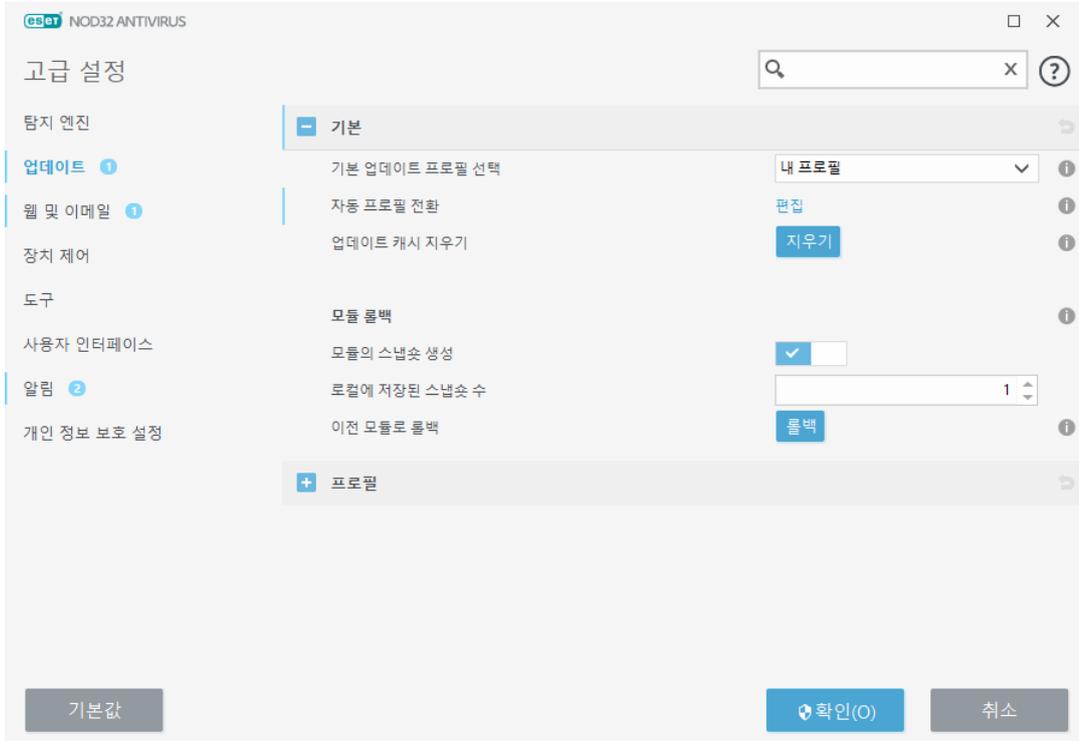
자동 업데이트 외에도 **업데이트 확인**을 클릭하여 수동 업데이트를 트리거할 수 있습니다.

항목	상태	정보
ESET NOD32 Antivirus	✓	현재 버전: 15.0.15.0
마지막 업데이트:	✓	10/14/2021 2:23:41 AM
마지막 업데이트 확인:	✓	10/14/2021 3:27:17 AM

고급 설정 창(기본 메뉴에서 **설정**을 클릭한 다음 **고급 설정**을 클릭하거나 키보드에서 **F5** 키를 누

름)에는 추가 업데이트 옵션이 포함되어 있습니다. 업데이트 모드, 프록시 서버 접근, LAN 연결 등의 고급 업데이트 옵션을 구성하려면 고급 설정 트리에서 **업데이트**를 클릭합니다.

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.



ESET NOD32 Antivirus 운용

ESET NOD32 Antivirus 설정 옵션을 사용하면 컴퓨터와 네트워크에 대한 보호 수준을



설정 메뉴는 다음과 같은 섹션으로 구분되어 있습니다.

 컴퓨터 보호

 인터넷 보호

해당 보호 모듈의 고급 설정을 조정하려면 구성 요소를 클릭합니다.

컴퓨터 보호 설정을 통해 다음 구성 요소를 활성화 또는 비활성화할 수 있습니다.

- **실시간 파일 시스템 보호** - 모든 파일을 열거나 생성하거나 실행할 때 악성 코드가 있는지 검사합니다.
- **장치 제어** - 이 모듈에서는 확장 필터/권한을 검사, 차단하거나 조정하고 사용자가 지정된 장치(CD/DVD/USB...)에 접근하여 사용할 수 있는 방식을 선택할 수 있습니다.
- **HIPS** - **HIPS** 시스템은 운영 체제 내의 이벤트를 모니터링하고 사용자 지정 규칙 집합에 따라 반응합니다.
- **게이머 모드** - **게이머 모드**를 활성화하거나 비활성화합니다. 게이머 모드를 활성화하면 경고 메시지(잠재적 보안 위험)가 수신되며 기본 창이 주황색으로 바뀝니다.

인터넷 보호 설정을 통해 다음 구성 요소를 활성화 또는 비활성화할 수 있습니다.

- **웹 브라우저 보호** - 이 옵션을 활성화하면 HTTP 또는 HTTPS를 통한 모든 트래픽에 악성 소프트웨어가 있는지 검사합니다.
- **이메일 클라이언트 보호** - POP3(S) 및 IMAP(S) 프로토콜을 통해 받은 통신을 모니터링합니다.
- **안티피싱 보호** - 기밀 정보를 얻기 위해 사용자를 조정하기 위해 고안된 콘텐츠를 배포하는 것으로 의심되는 웹 사이트를 필터링합니다.

비활성화된 보안 구성 요소를 다시 활성화하려면 슬라이더  를 클릭하여 녹색 확인 표시  가 나타나도록 합니다.

i 이 방법을 사용하여 보호를 비활성화하면 컴퓨터 다시 시작 후 비활성화된 모든 보호 모듈이 활성화됩니다.

설정 창 아래쪽에 추가 옵션이 있습니다. **고급 설정** 링크를 통해 각 모듈에 대해 파라미터를 상세하게 설정할 수 있습니다. **설정 가져오기/내보내기**를 통해 .xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장할 수 있습니다.

컴퓨터 보호

모든 보호 모듈의 개요를 보려면 **설정** 창에서 **컴퓨터 보호**를 클릭합니다:

- [실시간 파일 시스템 보호](#)
- [장치 제어](#)
- [HIPS\(호스트 침입 방지 시스템\)](#)
- [게이머 모드](#)

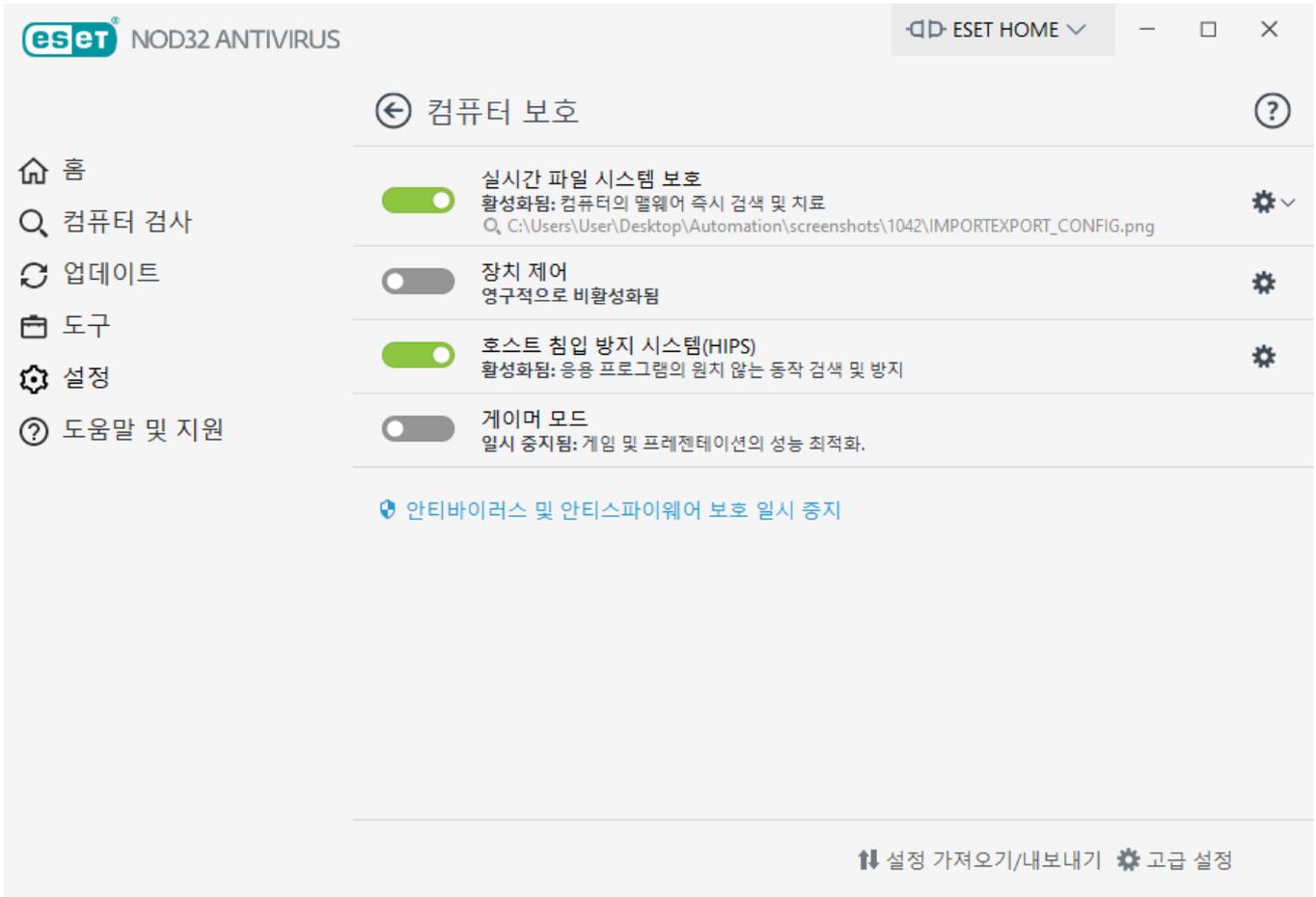
개별 보호 모듈을 일시 중지하거나 비활성화하려면 슬라이더 막대 아이콘  을 클릭합니다.

⚠ 보호 모듈을 끄면 컴퓨터의 보호 수준이 저하될 수 있습니다.

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

실시간 파일 시스템 보호의 경우 톱니바퀴 아이콘  을 클릭하고 다음 옵션 중에서 선택합니다.

- **구성** - 실시간 파일 시스템 보호 고급 설정을 엽니다.
- **제외 편집** - 검사에서 파일과 폴더를 제외할 수 있도록 [제외 설정 창](#)을 엽니다.



안티바이러스 및 안티스파이웨어 보호 일시 중지 - 모든 안티바이러스 및 안티스파이웨어 보호 모듈을 비활성화합니다. 보호를 비활성화하면 **시간 간격** 드롭다운 메뉴를 사용하여 보호 비활성화 기간을 결정할 수 있는 창이 열립니다. 숙련된 사용자이거나 ESET 기술 지원의 지시가 있는 경우에만 사용하십시오.

탐지 엔진

탐지 엔진은 파일, 이메일 및 인터넷 통신을 제어하여 악의적인 시스템 공격으로부터 보호합니다. 예를 들어 악성코드로 분류된 개체가 탐지되면 수정이 시작됩니다. 탐지 엔진은 먼저 해당 개체를 차단한 다음, 치료하거나, 삭제하거나, 검역소로 이동하여 제거할 수 있습니다.

탐지 엔진 설정을 자세히 구성하려면 **고급 설정**을 클릭하거나 **F5** 키를 누릅니다.

⚠ 탐지 엔진 설정은 숙련된 사용자만 변경해야 합니다. 설정을 잘못 구성하면 보호 수준이 저하될 수 있습니다.

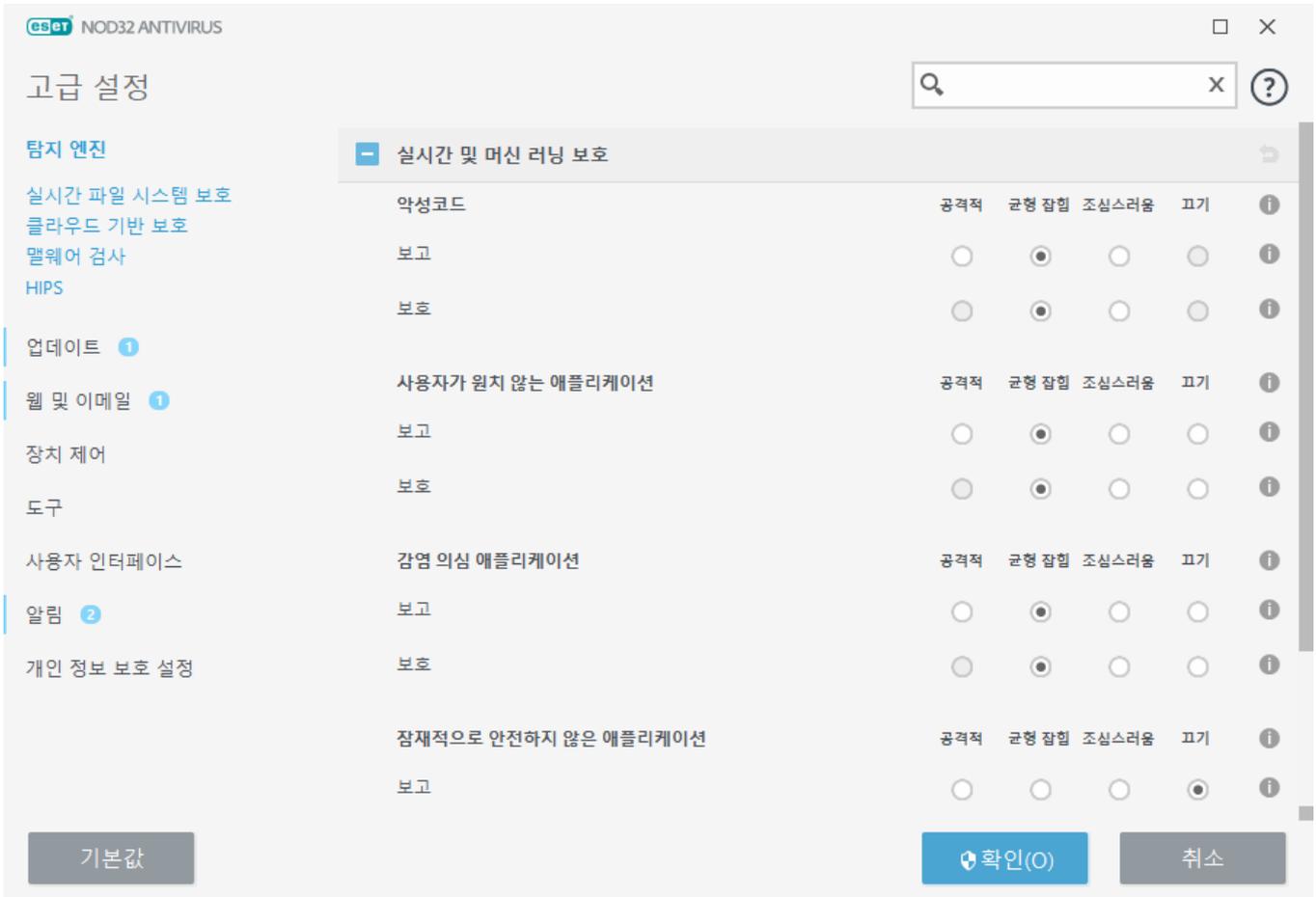
이 섹션의 내용:

- [실시간 및 머신 러닝 보호 범주](#)
- [악성코드 검사](#)
- [보고 설정](#)

실시간 및 머신 러닝 보호 범주

모든 보호 모듈(예: 실시간 파일 시스템 보호, 웹 브라우저 보호 등)에 대한 **실시간 및 머신 러닝 보호**를 사용하여 다음 범주의 보고 및 보호 수준을 구성할 수 있습니다.

- **악성코드** – 컴퓨터 바이러스는 컴퓨터에 있는 기존 파일 앞뒤에 붙는 악성 코드의 일종입니다. 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 [용어집](#)을 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 [용어집](#)을 참조하십시오.
- **감염 의심 응용 프로그램**에는 [패키](#) 또는 보호기로 압축된 프로그램이 포함됩니다. 이러한 유형의 보호기는 맬웨어에서 검출을 회피하기 위해 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 [용어집](#)을 참조하십시오.



개선된 보호

i 고급 머신 러닝이 이제 머신 러닝에 기반을 두고 탐지 성능을 개선하는 고급 보호 계층으로 탐지 엔진에 포함되어 있습니다. 이 보호 유형에 대한 자세한 내용은 [용어집](#)을 읽어 보십시오.

악성코드 검사

검사기 설정은 실시간 검사기 및 [수동 검사기](#)와는 별도로 구성할 수 있습니다. 기본적으로 **실시간 보호 설정 사용**은 활성화됩니다. 활성화되면 관련 수동 검사 설정이 **실시간 및 머신 러닝 보호** 섹션에서 상속됩니다. 자세한 내용은 [악성코드 검사](#)를 참조하십시오.

보고 설정

탐지가 발생하면(예: 위협이 발견된 후 악성코드로 분류됨), 정보가 [탐지 로그](#)에 기록되고 [바탕 화면 알림](#)이 발생합니다(ESET NOD32 Antivirus에서 구성된 경우).

각 범주에 대해 다음과 같은 보고 한계("범주"라고도 함)가 구성됩니다.

1. 악성코드

- 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 [개체](#) 차단, [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.
균형 잡힘	균형 잡힘으로 구성된 범주 보고입니다. 이 설정은 성능과 탐지율의 정확도 및 잘못 보고된 개체의 수가 균형을 이루도록 하는데 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 NOD32 Antivirus 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

* ESET NOD32 Antivirus 버전 13.1 이상에서 사용 가능합니다.

** 권장되지 않음

✓ [제품 버전, 프로그램 모듈 버전 및 빌드 날짜 확인](#)

1. [도움말 및 지원](#) > **ESET NOD32 Antivirus** 정보를 클릭합니다.
2. 정보 화면의 첫 번째 텍스트 줄에는 ESET 제품의 버전 번호가 표시됩니다.
3. 설치된 구성 요소를 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 이전 버전의 ESET NOD32 Antivirus(13.0 이하)와 비슷한 수준의 보호를

AMSI를 통해 고급 검사 활성화 - 애플리케이션 개발자의 새 맬웨어 방어를 허용하는 Microsoft Antimalware Scan Interface 도구입니다(Windows 10만 해당).

침입이 검출됨

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 NOD32 Antivirus에서 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 [검역소](#)로 이동하거나 연결을 종료하려고 시도합니다. 화면의 오른쪽 하단에 있는 알림 영역에 알림 창이 표시됩니다. 탐지/치료된 개체에 대한 자세한 내용은 [로그 파일](#)을 참조하십시오. 치료 수준 및 동작에 대한 자세한 내용은 [치료 수준](#)을 참조하십시오.



감염된 파일에 대해 컴퓨터 검사

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

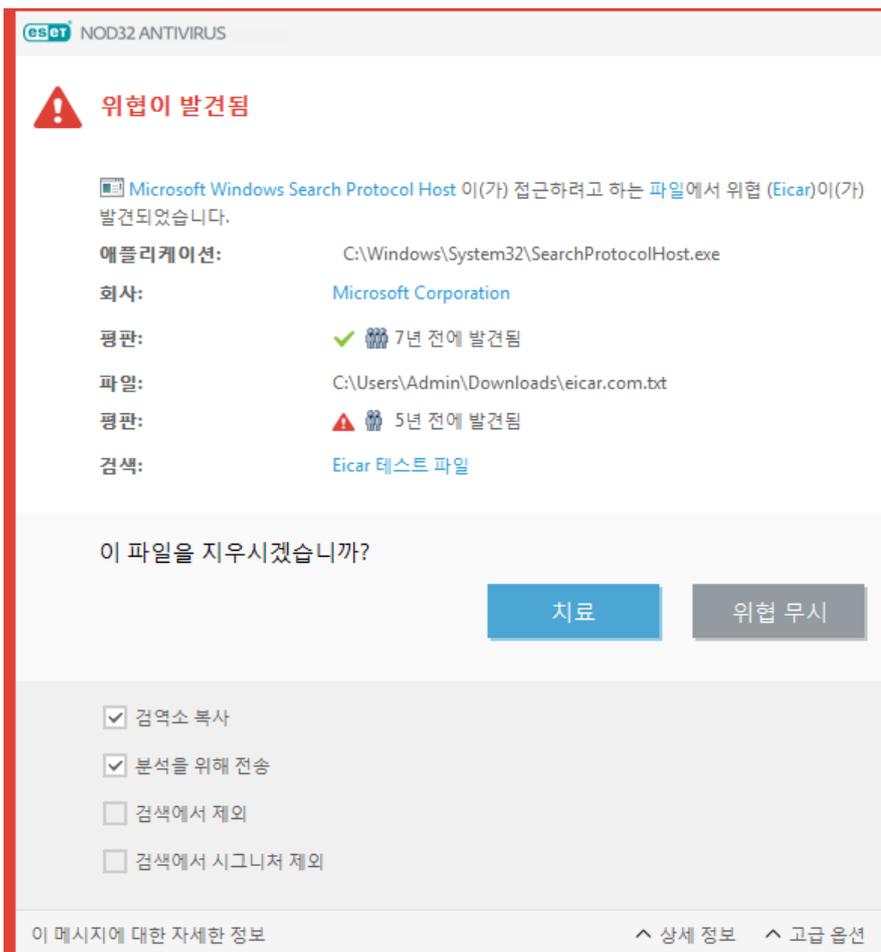
1. ESET NOD32 Antivirus을(를) 열고 [컴퓨터 검사](#)를 클릭합니다.
2. [컴퓨터 검사](#)를 클릭합니다(자세한 내용은 [컴퓨터 검사](#) 참조).

3.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.

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 NOD32 Antivirus [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 위치 않는 애플리케이션](#)으로 표시된 경우 **복원 후 검사에서 제외** 옵션이 활성화됩니다. 또한 [제외](#)를 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 위험

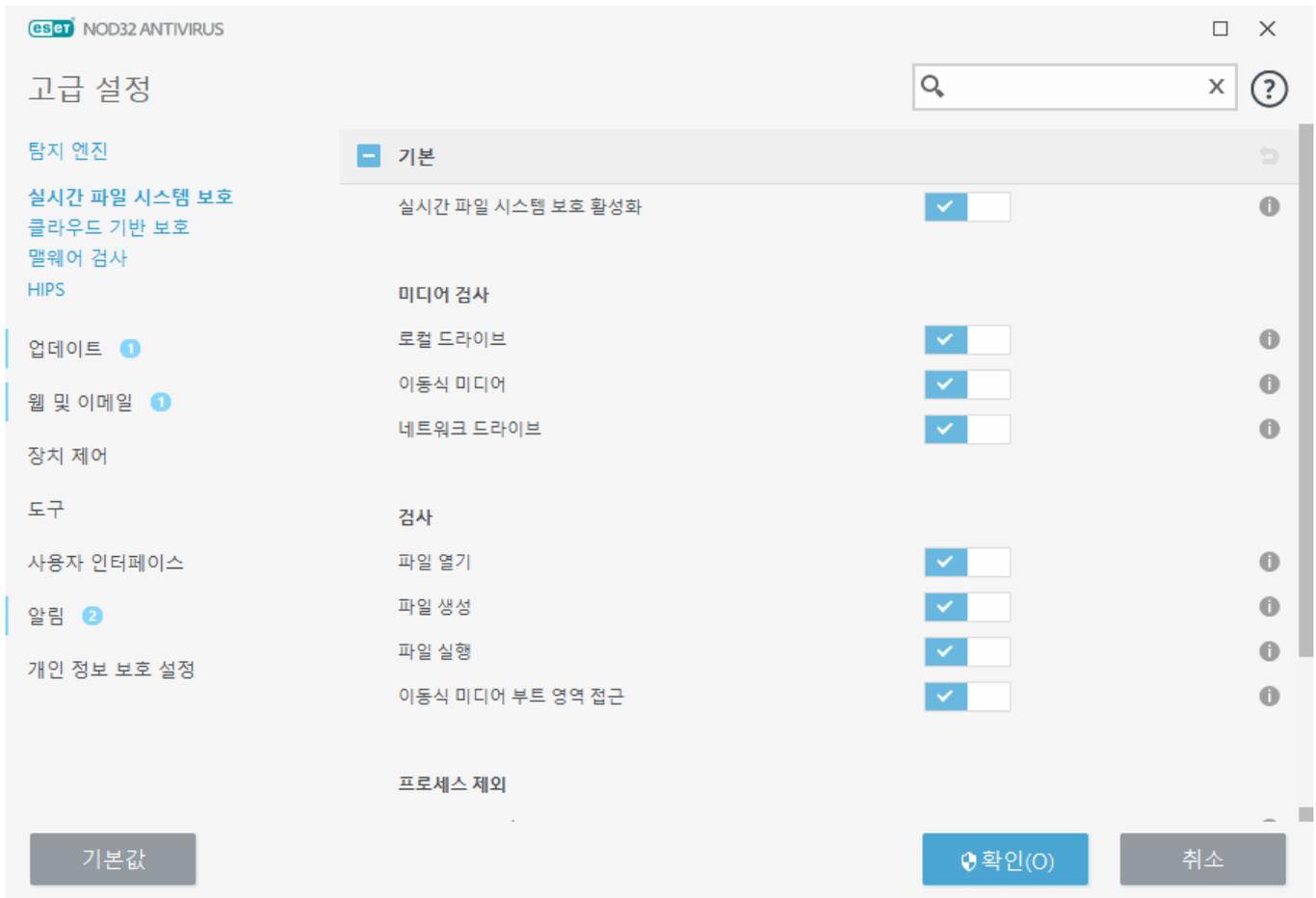
컴퓨터 검사 중 감염된 파일이 치료되지 않은 경우(또는 [치료 수준](#)이 **치료 안함**으로 설정된 경우) 이러한 파일에 대한 동작을 선택할지를 묻는 경고 창이 표시됩니다. 파일에 대해 수행할 동작을 선택한 다음(목록의 각 파일에 대해 개별적으로 동작 설정) **마침**을 클릭합니다.

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.

실시간 파일 시스템 보호

실시간 파일 시스템 보호는 파일을 열거나 생성하거나 실행할 때 시스템의 모든 파일에 포함된 악의적인 코드를 제어합니다.



기본적으로 실시간 파일 시스템 보호가 시스템 시작 시 시작되며 중단 없이 검사를 수행합니다. 탐지 엔진 > 실시간 파일 시스템 보호 > 기본의 고급 설정에서 실시간 파일 시스템 보호 활성화를 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: \\store04로서 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 모든 파일은 열거나 생성하거나 실행할 때 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 ThreatSense 파라미터에서 **부트 영역/UEFI**를 활성화 상태로 유지해야 합니다.

모든 유형의 미디어를 검사하는 실시간 파일 시스템 보호는 파일에 접근하는 등의 다양한 시스템 이벤트가 발생하면 트리거됩니다. [ThreatSense 엔진 파라미터 설정](#) 섹션에 설명되어 있는 ThreatSense 기술 검출 방법을 사용한 실시간 파일 시스템 보호 기능은 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 **F5** 키를 눌러 **고급 설정**을 열고 **검색 엔진 > 실시간 파일 시스템 보호**를 확장합니다. **ThreatSense 파라미터 > 기타**를 클릭한 후 **스마트 최적화 활성화**를 선택하거나 선택 취소합니다.

치료 수준

원하는 보호 모듈의 치료 수준 설정에 접근하려면 **ThreatSense 파라미터**(예: **실시간 파일 시스템 보호**)를 확장한 다음 **치료 > 치료 수준**을 클릭합니다.

ThreatSense 파라미터는 다음 수정(예: 치료) 수준으로 제공됩니다.

ESET NOD32 Antivirus의 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.
안전하면 탐지 수정, 그렇지 않으면 유지	최종 사용자가 개입하지 않고 개체 를 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 대화형 창이 나타나면 수정 동작(예: 제거 또는 무시)를 선택해야 합니다. 이 수준은 탐지 이벤트에서 취해야 할 단계를 알고 있는 고급 사용자를 위한 것입니다.

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 NOD32 Antivirus을(를) 설치하고 나면 모든 설정이 최적화되어 사용자에게 최대 수준의 시스템 보호 성능을 제공합니다. 기본 설정을 복원하려면 창에서 각 탭 옆에 있는 을 클릭합니다(고급 설정 > 검색 엔진 > 실시간 파일 시스템 보호).

실시간 보호 검사

실시간 보호가 작동 중이며 바이러스를 검출하는지 확인하려면 www.eicar.com에서 제공하는 테스트 파일을 사용합니다. 이 테스트 파일은 모든 안티바이러스 프로그램에서 검출할 수 있는 무해한 파일입니다. 이 파일은 EICAR (European Institute for Computer Antivirus Research) 회사에서 안티바이러스 프로그램의 기능을 테스트하기 위해 생성한 것입니다. 이 파일은 <http://www.eicar.org/download/eicar.com>에서 다운로드할 수 있습니다.

파일은 <http://www.eicar.org/download/eicar.com>에서 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 보호 > 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(F5 키)**로 이동하여 **검색 엔진 > 실시간 파일 시스템 보호**를 클릭합니다.

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

실시간 보호가 시스템을 시작할 때 시작되지 않고 실시간 파일 시스템 보호 활성화가 활성화되어 있으면 다른 프로그램과 충돌하기 때문일 수 있습니다. 이 문제를 해결하려면 [SysInspector 로그](#)를 생성하여 분석을 위해 [ESET 기술 지원에 제출](#)하십시오.

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.

i 제외된 파일 확장명, HIPS 제외, 탐지 제외 또는 성능 제외와 혼동하지 마십시오.

프로세스 제외는 잠재적 충돌 위험을 최소화하고 제외된 응용 프로그램의 성능을 개선하는 데 도움이 되며, 결과적으로 운영 체제의 전반적 성능 및 안정성에 긍정적 효과를 미칩니다. 프로세스/응용 프로그램 제외는 그 실행 파일(.exe)을 제외하는 것입니다.

고급 설정(F5) > 탐지 엔진 > 실시간 파일 시스템 보호 > 프로세스 제외를 통해 실행 파일을 제외된 프로세스 목록에 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 제외된 실행 파일(예 *Backup-tool.exe*)을 탐색할 수 있습니다.

.exe 파일이 제외에 추가되는 즉시 ESET NOD32 Antivirus가 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 올바르게 작동하지 않으며 HIPS가 오류를 보고할 수 있습니다.

기존 프로세스를 편집하거나 제외 목록에서 삭제할 수도 있습니다.

i 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 추가할 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 NOD32 Antivirus가 이 프로세스의 활동을 모니터링 되지 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 올바르게 작동하지 않으며 HIPS가 오류를 보고할 수 있습니다.

기존 프로세스를 편집하거나 제외 목록에서 삭제할 수도 있습니다.

클라우드 기반 보호

ESET LiveGrid®(ESET ThreatSense.Net 고급 조기 경고 시스템에 구축)에서는 ESET 사용자가 전 세계적으로 제출한 데이터를 활용하고 해당 데이터를 ESET 연구소로 보냅니다. ESET LiveGrid®에서는 현장의 감염 의심 샘플과 메타데이터를 제공하여 ESET에서 고객의 요구 사항에 즉각 반응하고 ESET이 최신 위협에 대한 대응력을 유지할 수 있도록 합니다.

다음과 같은 옵션을 사용할 수 있습니다.

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 프로세스](#)와 파일의 평판을 확인하십시오.

ESET LiveGrid® 피드백 시스템 활성화

ESET LiveGrid® 평판 시스템뿐만 아니라 ESET LiveGrid® 피드백 시스템에서는 새로 탐지된 위협과 관련된 사용자 컴퓨터의 정보를 수집합니다. 수집하는 정보는 다음과 같습니다.

- 위협이 나타난 파일의 샘플 또는 사본
- 파일 경로
- 파일 이름

- 날짜 및 시간
- 컴퓨터에 위협이 나타난 프로세스
- 컴퓨터의 운영 체제에 대한 정보

기본적으로 ESET NOD32 Antivirus는 자세한 분석을 위해 ESET 바이러스 연구소로 감염 의심 파일을 전송하도록 구성되어 있습니다. .doc 또는 .xls와 같은 특정 확장명의 파일은 항상 제외됩니다. 또한 사용자 또는 사용자의 조직에서 전송하지 않으려는 특정 파일이 있는 경우 해당 파일의 확장명을 추가할 수도 있습니다.

i 관련 데이터 전송에 대한 자세한 내용은 [개인 정보 보호 정책](#)을 참조하십시오.

ESET LiveGrid®를 활성화하지 않도록 선택할 수 있음

소프트웨어에서 사용하지 못하는 기능은 없지만 경우에 따라서는 ESET LiveGrid®이(가) 활성화된 경우, ESET NOD32 Antivirus이(가) 새로운 위협에 더 빨리 대응할 수도 있습니다. 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.

ESET LiveGrid®에 대한 자세한 내용은 [용어집](#)을 참조하십시오.
i ESET NOD32 Antivirus에서 ESET LiveGrid®을(를) 활성화 또는 비활성화하는 방법은 영어 및 기타 여러 언어로 제공되는 [그림이 포함된 지침](#)을 참조하십시오.

고급 설정 내 클라우드 기반 보호 구성

ESET LiveGrid® 설정에 접근하려면 **고급 설정(F5) > 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.
- **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, [검색소](#) 또는 [도구](#)에서 ESET에 수동으로 샘플을 전송하는 옵션을 활성화합니다.

탐지된 샘플 자동 전송

분석 및 향후 탐지 성능 개선을 위해 ESET에 전송할 샘플 종류를 선택합니다(기본 최대 샘플 크기는 64MB). 사용할 수 있는 옵션은 다음과 같습니다.

- **탐지된 모든 샘플** - [탐지 엔진](#)(검사기 설정에 활성화된 경우 사용자가 원치 않은 애플리케이션 포함)에서 탐지된 모든 [개체](#)입니다.
- **문서를 제외한 모든 샘플** - 문서를 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 NOD32 Antivirus [보호 모듈](#) 중 하나는 이러한 샘플을 감염이 의심되거나 명확하지 않은 동작을 하는 것으로 간주합니다(기본 최대 샘플 크기는 64MB).

- **실행 파일** - .exe, .dll, .sys 등의 실행 파일을 포함합니다.
- **압축파일** - .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab 등의 압축파일 형식을 포함합니다.
- **스크립트** - .bat, .cmd, .hta, .js, .vbs, .ps1 등의 스크립트 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 목록을 확인하려면 확장](#)

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWF, 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 필터](#)를 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 포함되어 있어도 분석하기 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 > 탐지 엔진 > 클라우드 기반 보호 > 샘플 제출**로 이동하여 **제외** 옆에 있는 **편집**을 클릭합니다. 제외를 추가합니다 (.download.domain.com).

샘플의 최대 크기(MB) – 샘플의 최대 크기(1-64MB)를 정의합니다.

클라우드 기반 보호를 위한 제외 필터

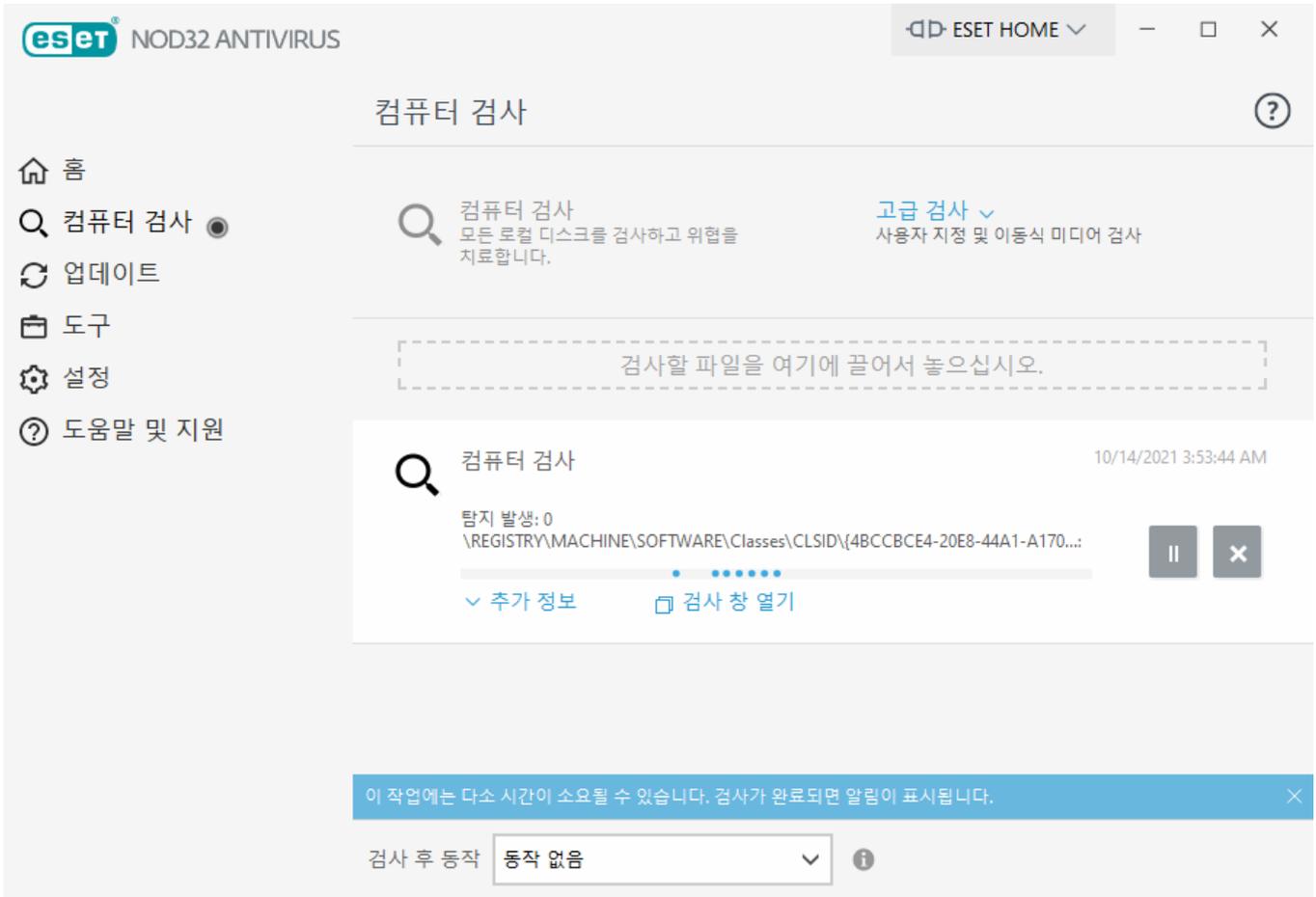
제외 필터를 사용하면 샘플 전송 시 특정 파일이나 폴더를 제외할 수 있습니다. 나열된 파일에 감염 의심 코드가 있어도 분석을 위해 ESET 연구소로 보내지 않습니다. 일반적인 파일 형식(.doc 등)은 기본적으로 제외됩니다.

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

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

컴퓨터 검사

수동 검사기는 안티바이러스 솔루션의 중요한 기능으로 컴퓨터에서 파일 및 폴더를 검사하는 데 사용됩니다. 보안 측면에서 볼 때 감염이 의심될 때뿐만 아니라 일상적인 보안 조치의 일환으로 정기적으로 컴퓨터 검사를 실행하는 것이 필수적입니다. 바이러스가 디스크에 기록될 때 [실시간 파일 시스템 보호](#)에서 검출되지 않은 바이러스를 검출하려면 시스템 상세 검사를 정기적으로 수행하는 것이 좋습니다. 당시 실시간 파일 시스템 보호가 비활성화되었거나, 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 지정하지 않아도 시스템을 빠르게 검사합니다. **사용자 지정 검사**(고급 검사 아래)를 사용하면 특정 위치를 대상으로 하도록 설계된 미리 정의된 검사 프로파일 중에서 선택할 수 있으며, 특정 검사 대상을 선택할 수도 있습니다.

검사 프로세스에 대한 자세한 내용은 [검사 진행률](#)을 참조하십시오.

i 기본적으로 ESET NOD32 Antivirus에서는 컴퓨터 검사 중에 발견된 탐지 항목을 자동으로 치료하거나 제거하려고 시도합니다. 경우에 따라 수행할 수 있는 동작이 없으면 대화형 경고가 표시되고 치료 동작(예: 제거 또는 무시)을 선택해야 합니다. 치료 수준을 변경하고 자세한 내용을 알아보려면 [치료](#)를 참조하십시오. 이전 검사를 검토하려면 [로그 파일](#)을 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 되는 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 [치료](#)를 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 대상과 검사 방법 같은 검사 파라미터를 지정할 수 있습니다. **사용자 지정 검사**의 장점은 파라미터를 상세히 구성할 수 있다는 것입니다. 파라미터를 설정하려면 톱니바퀴를 클릭하십시오. 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 메뉴에서 **동작 없음**, **종료**, **필요한 경우 재부팅**, **재부팅**, **필요한 경우 강제 재부팅** 또는 **강제 재부팅**을 선택할 수 있습니다. **절전 모드** 또는 **최대 절전 모드**는 컴퓨터 전원과 절전 운영 체제 설정이나 컴퓨터/랩톱 기능에 따라 사용할 수 있습니다. 실행 중인 검사를 모두 완료하면 선택한 동작이 시작됩니다. **종료**를 선택하면 종료 확인 대화 상자 창에 30초 카운트다운이 표시됩니다(요청된 종료를 비활성화하려면 **취소** 클릭). 자세한 내용은 [고급 검사 옵션](#)을 참조하십시오.

i 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 파라미터**를 사용합니다. 사용 가능한 옵션은 **고급 설정 (F5) > 탐지 엔진 > 악성코드 검사 > 수동 검사 > ThreatSense 파라미터**에 설명되어 있습니다.

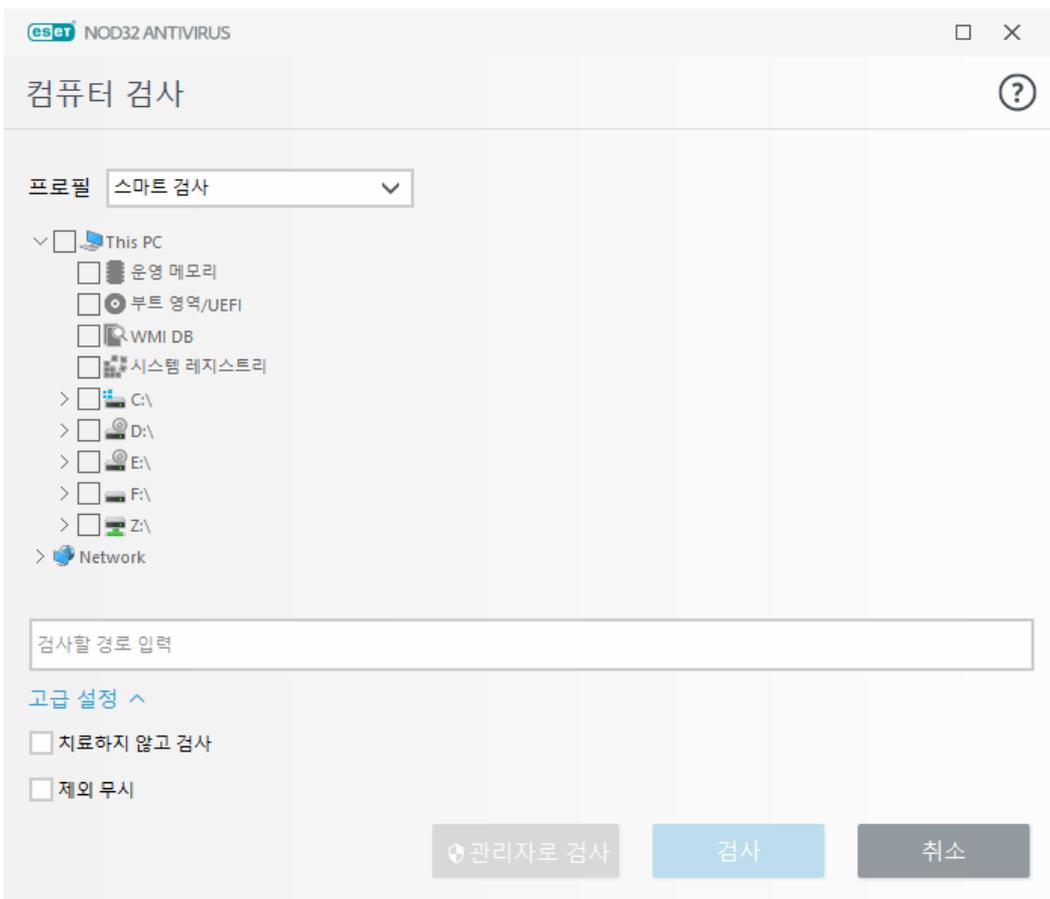
폴더(트리) 구조에는 특정 검사 대상도 포함되어 있습니다.

- **운영 메모리** – 운영 메모리에서 현재 사용되는 모든 프로세스와 데이터를 검사합니다.
- **부트 영역/UEFI** – 악성코드가 있는지 부트 영역과 UEFI를 검사합니다. UEFI 스캐너에 대한 자세한 내용은 [용어집](#)을 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 대상으로 신속하게 이동하거나 대상 폴더 또는 파일을 추가하려면 폴더 목록 아래의 빈 필드에 대상 디렉토리를 입력합니다.

i 주간 컴퓨터 검사를 예약하는 방법

정기적인 작업을 예약하려면 [주간 컴퓨터 검사를 예약하는 방법](#) 장을 참조하십시오.



고급 설정(F5 키) > 탐지 엔진 > 수동 검사 > **ThreatSense** 파라미터 > 치료에서 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.

i [로그 표시](#)를 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.

i 비밀번호로 보호되는 파일이나 시스템에서만 사용하는 파일(일반적으로 *pagefile.sys* 및 특정 로그 파일)과 같은 일부 파일의 경우 검색할 수 없는 것이 일반적입니다. 자세한 내용은 [지식 베이스 문서](#)에서 확인할 수 있습니다.

i [주간 컴퓨터 검사를 예약하는 방법](#)
정기적인 작업을 예약하려면 [주간 컴퓨터 검사를 예약하는 방법](#) 장을 참조하십시오.

검사 진행률 - 진행률 표시줄에는 아직 검사 대기 중인 개체와 비교하여 이미 검사된 개체의 상태가 표시됩니다. 검사 진행률 상태는 검사에 포함된 전체 개체 수에서 파생됩니다.

대상 - 현재 검사된 개체 이름 및 해당 위치입니다.

위험 발견됨 - 검사한 파일, 발견된 위험, 검사 중에 치료된 위험의 총 수를 표시합니다.

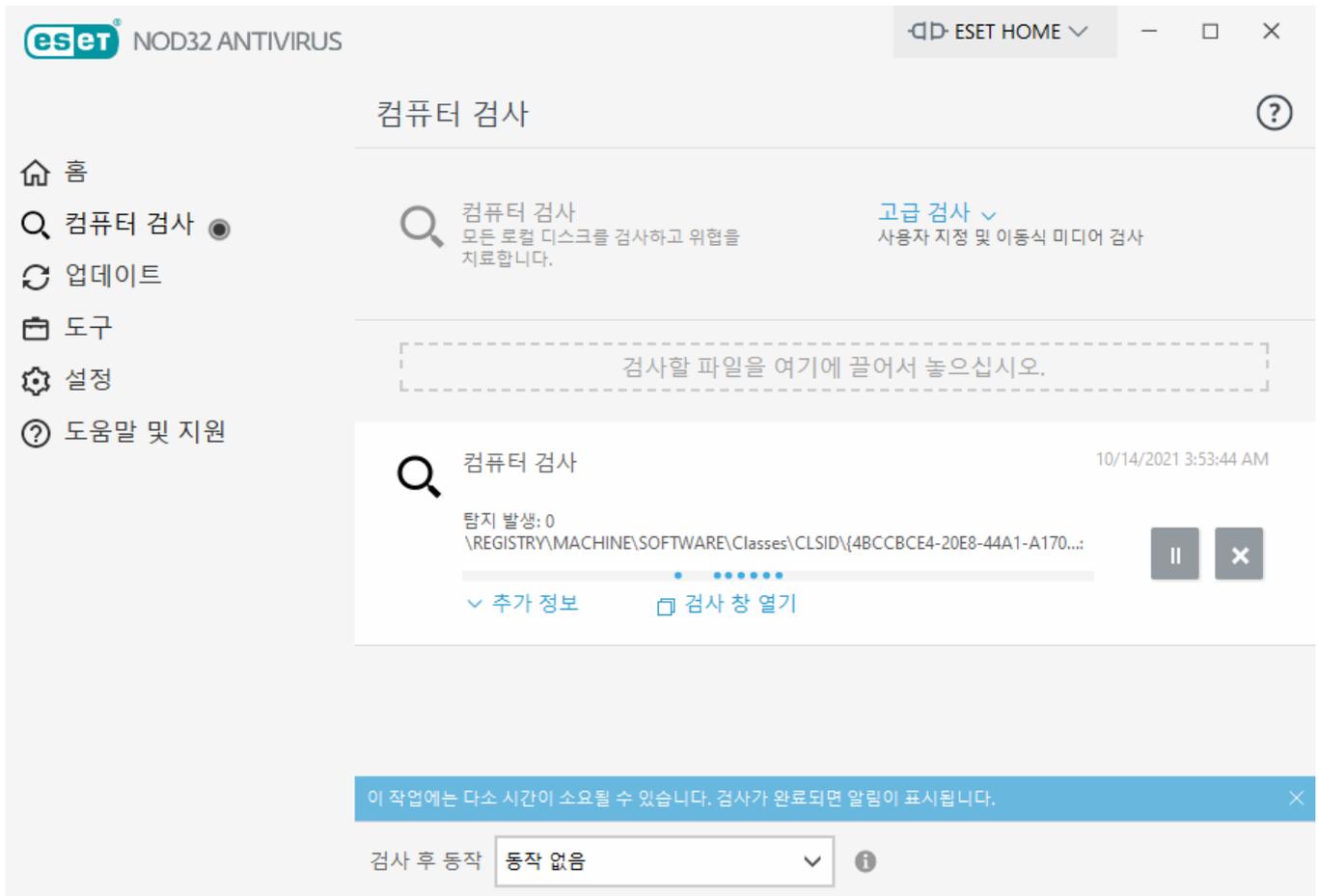
일시 중지 - 검사를 일시 중지합니다.

다시 시작 - 이 옵션은 검사 진행을 일시 중지한 경우 표시됩니다. 검사를 계속하려면 **다시 시작**을 클릭합니다.

중지 - 검사를 종료합니다.

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

i 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 - 검사 후 동작 드롭다운 메뉴에서 동작 없음, 종료, 필요한 경우 재부팅, 재부팅, 필요한 경우 강제 재부팅 또는 강제 재부팅을 선택할 수 있습니다. 절전 모드 또는 최대 절전 모드는 컴퓨터 전원과 절전 운영 체제 설정이나 컴퓨터/랩톱 기능에 따라 사용할 수 있습니다. 실행 중인 검사를 모두 완료하면 선택한 동작이 시작됩니다. 종료를 선택하면 종료 확인 대화 상자 창에 30초 카운트다운이 표시됩니다(요청된 종료를 비활성화하려면 취소 클릭). 자세한 내용은 [고급 검사 옵션](#)을 참조하십시오.

컴퓨터 검사 로그

검사가 완료되면 특정 검사와 연관 있는 관련 정보가 모두 포함된 [컴퓨터 검사 로그](#)가 열립니다. 검사 로그는 다음과 같은 정보를 제공합니다.

- 검색 엔진 버전
- 시작 날짜 및 시간
- 검사된 디스크, 폴더 및 파일 목록
- 총 검사 시간
- 검사된 개체 수
- 발견된 탐지 수

- 완료 시간
- 총 검사 시간

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



i "열 수 없음", "여는 중 오류" 및/또는 "압축파일이 손상됨" 레코드에 대해 자세히 알아보려면, [ESET 지식베이스 문서](#)를 참조하십시오.

필터링 전환 아이콘을 클릭하여 사용자 지정 기준에 따라 검색 범위를 좁혀 정의할 수 있는 **로그 필터링**을 엽니다. 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 스위치를 클릭하는 것과 같음).

동작	사용
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.

악성코드 검사

악성코드 검사 섹션은 **고급 설정(F5 키) > 탐지 엔진 > 악성코드 검사**에서 액세스할 수 있으며 검사 파라미터를 선택하는 옵션이 제공됩니다. 이 섹션에는 다음 항목이 포함됩니다.

선택한 프로필 - 수동 검사기에서 사용하는 특정 파라미터 집합입니다. 새 프로필을 생성하려면 **프로필 목록** 옆의 **편집**을 클릭합니다. 자세한 내용은 [검사 프로필](#)을 참조하십시오.

대상 검사 - 특정 대상만 검사하려면 **대상 검사** 옆의 **편집**을 클릭하고 드롭다운 메뉴에서 옵션을 선택하거나 폴더(트리) 구조에서 특정 대상을 선택하면 됩니다. 자세한 내용은 [대상 검사](#)을 참조하십시오.

ThreatSense 파라미터 - 이 섹션에는 제어하려는 파일 확장명, 사용되는 검출 방법 등의 고급 설정 옵션이 있습니다. 고급 검사기 옵션이 포함된 탭을 클릭하여 엽니다.

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 슬라이더 막대를 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 슬라이더 막대를 활성화하면 이 설정을 재정의할 수 있습니다.

[로그 파일](#) 섹션에서 컴퓨터 검사 결과를 기록하려면 고급 설정에서 **로깅 활성화** 옆의 슬라이더 막대를 활성화합니다([기본 프로그램 창](#)에서 **도구 > 로그 파일**을 클릭한 다음 **로그** 드롭다운 메뉴에서 **컴퓨터 검사** 선택).

유휴 상태 탐지

유휴 상태 검사기를 트리거하기 위해 충족되어야 하는 전체 조건 목록을 보려면 [유휴 상태 탐지 트리거](#)를 참조하십시오.

유휴 상태 검사기의 검사 파라미터(예: 검출 방법)를 수정하려면 [ThreatSense 엔진 파라미터 설정](#)을 클릭합니다.

검사 프로필

ESET NOD32 Antivirus에는 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 창(F5 키)을 열고 **검색 엔진 > 맬웨어 검사 > 수동 검사 > 프로필 목록**을 클릭합니다. **프로필 관리자** 창에는 새 프로필을 생성할 수 있는 옵션 및 기존 검사 프로필이 있는 **선택한 프로필** 드롭다운 메뉴가 포함되어 있습니다. 필요에 맞게 검사 프로필을 생성하려면 [ThreatSense 엔진 파라미터 설정](#) 섹션에서 검사 설정의 각 파라미터 설명을 참조하십시오.

i 고유한 검사 프로필을 생성하려는데 **컴퓨터 검사** 구성이 부분적으로 적합하지만 **런타임 패커**나 **잠재적으로 안전하지 않은 애플리케이션**은 검사하고 싶지 않고 **항상 탐지** 수정도 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 [용어집](#)을 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 대상으로 신속하게 이동하거나 대상 폴더 또는 파일을 추가하려면 폴더 목록 아래의 빈 필드에 대상 디렉토리를 입력합니다.

장치 제어

ESET NOD32 Antivirus은(는) 자동 장치(CD/DVD/USB/...) 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
- 모든 장치 유형

장치 제어 설정 옵션은 **고급 설정(F5 키) > 장치 제어**에서 수정할 수 있습니다.

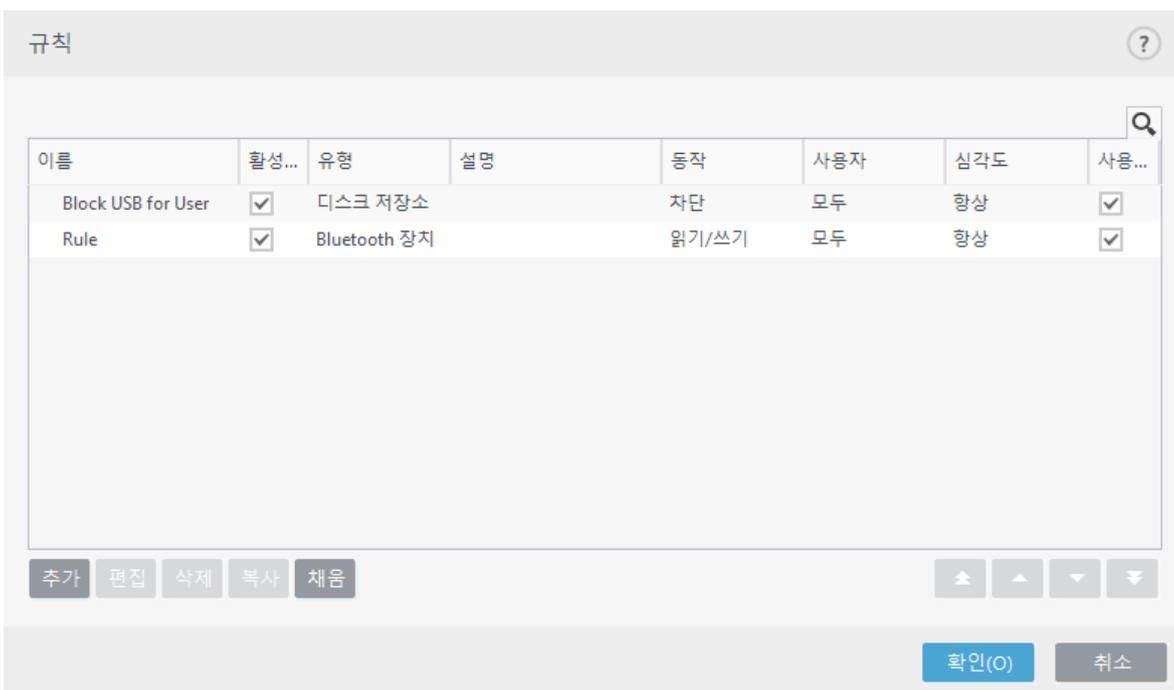
장치 제어 활성화 옆에 있는 스위치를 켜면 ESET NOD32 Antivirus의 장치 제어 기능이 활성화됩니다. 이 변경 내용을 적용하려면 컴퓨터를 다시 시작해야 합니다. 장치 제어가 활성화되면 **규칙**이 활성화되어 **규칙 편집** 창을 열 수 있습니다.

i 서로 다른 규칙이 적용되는 여러 장치 그룹을 생성할 수 있습니다. 또한 **읽기/쓰기** 또는 **읽기 전용** 동작을 포함한 규칙이 적용되는 하나의 장치 그룹만 생성할 수도 있습니다. 그러면 컴퓨터에 연결 시 장치 제어에 의해 인식되지 않는 장치가 차단됩니다.

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 연결한 외부 장치를 정밀하게 제어할 수 있습니다.



특정 장치는 규칙 구성에서 지정할 수 있는 추가 장치 파라미터를 기준으로 사용자 또는 사용자 그룹별로 허용하거나 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. 또한 [장치 제어 규칙 추가](#)를 참조하십시오.

추가 또는 **편집**을 클릭하면 규칙을 관리할 수 있습니다. **복사**를 클릭하면 선택된 다른 규칙에 사용되는 미리 정의된 옵션으로 새 규칙을 생성할 수 있습니다. 규칙을 클릭하면 표시되는 XML 문자열은 클립보드에 복사되어 시스템 관리자가 등에서 이러한 데이터를 내보내거나 가져오고 사용할 수 있습니다.

Ctrl 키를 누른 상태에서 클릭하면 여러 규칙을 선택하고, 선택된 모든 규칙에 규칙을 삭제하거나 규칙을 목록 위아래로 이동하는 등의 동작을 적용할 수 있습니다. **활성화됨** 확인란을 사용하면 규칙을 활성화 또는 비활성화할 수 있습니다. 이 옵션은 규칙을 나중에 사용할 수 있도록 영구적으로 삭제하지 않으려는 경우에 유용합니다.

이 제어 작업은 순위를 결정하는 순서(순위가 높은 규칙이 상단에 정렬)로 정렬된 규칙에 따라 수행됩니다.

로그 항목은 ESET NOD32 Antivirus 기본 창의 **도구 > 로그 파일**에서 볼 수 있습니다.

장치 제어 로그에는 장치 제어가 트리거된 모든 항목이 기록됩니다.

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 클릭하면 미리 정의된 정보가 포함된 상태로 규칙 편집 창이 표시됩니다(모든 설정을 조정할 수 있음).

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 부분에 표시할 장치 목록이 포함된 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 - 장치 이름을 입력하여 그룹을 추가하거나, 기존 그룹에 장치를 추가할 수 있습니다. 또는 창에서 버튼을 클릭한 위치에 따라 공급업체 이름, 모델 및 일련 번호 등과 같은 상세 정보를 지정할 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.

사용자 지정을 완료했다면 **확인**을 클릭합니다. 변경 내용을 저장하지 않고 **장치 그룹** 창을 벗어나려면 **취소**를 클릭합니다.

i 서로 다른 규칙이 적용되는 여러 장치 그룹을 생성할 수 있습니다. 또한 **읽기/쓰기** 또는 **읽기 전용** 동작을 포함한 규칙이 적용되는 하나의 장치 그룹만 생성할 수도 있습니다. 그러면 컴퓨터에 연결 시 장치 제어에 의해 인식되지 않는 장치가 차단됩니다.

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 **읽기 전용**을 사용할 수 없으므로 Bluetooth 장치를 허용, 차단하거나 이 장치에 경고만 할 수 있음).

장치 제어 규칙 추가

장치 제어 규칙은 규칙 기준을 충족하는 장치가 컴퓨터에 연결된 경우 수행할 동작을 정의합니다.

규칙 편집
?

이름

규칙이 활성화됨

장치 유형

동작

기준 유형

공급업체

모델

일련 번호

로그 심각도

사용자 목록 편집

사용자에게 알림

좀 더 쉽게 식별할 수 있도록 이름 필드에 규칙 설명을 입력합니다. 규칙이 활성화됨 옆의 슬라이더 막대를 클릭하여 이 규칙을 비활성화하거나 활성화할 수 있습니다. 이 옵션은 규칙을 영구적으로 삭제하지 않으려는 경우에 유용합니다.

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 제공하고 사용자에 대한 정보는 제공하지 않으므로 이미징 장치는 전체적으로만 차단할 수 있습니다.

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.

- 읽기/쓰기 - 장치에 대한 모든 접근이 허용됩니다.
- 차단 - 장치에 대한 접근이 차단됩니다.
- 읽기 전용 - 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 **읽기 전용**을 사용할 수 없으므로 Bluetooth 장치를 허용, 차단하거나 이 장치에 경고만 할 수 있음).

기준 유형

장치 그룹이나 장치를 선택합니다.

규칙을 미세 조정하고 장치에 맞게 조정하는 데 아래와 같은 추가 파라미터를 사용할 수 있습니다. 모든 파라미터는 대소문자를 구분하지 않습니다.

- **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.

i 이러한 파라미터가 정의되지 않은 경우 일치 작업 동안 규칙에서 이러한 필드를 무시합니다. 모든 텍스트 필드의 필터링 파라미터는 대소문자를 구분하지 않으며 와일드카드(*, ?)는 지원되지 않습니다.

i 장치에 대한 정보를 보려면 해당 유형의 장치에 대한 규칙을 생성하고 장치를 컴퓨터에 연결한 후 [장치 제어 로그](#)에서 장치 상세 정보를 확인합니다.

로그 심각도

ESET NOD32 Antivirus는 로그 파일에 중요한 모든 이벤트를 저장합니다. 로그 파일은 기본 메뉴에서 직접 확인할 수 있습니다. **도구 > 로그 파일**을 클릭한 다음 **로그** 드롭다운 메뉴에서 **장치 제어**를 선택합니다.

- **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 오류 및 경고 메시지를 기록합니다.
- **없음** - 로그가 기록되지 않습니다.

사용자 목록

사용자 목록 옆의 편집을 클릭하여, 규칙을 사용자 목록에 추가하면 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 유형**이 있는 규칙에 대해 정의할 수 없습니다.

- USB 프린터
- Bluetooth 장치
- 스마트 카드 리더
- 이미징 장치
- 모뎀
- LPT/COM 포트

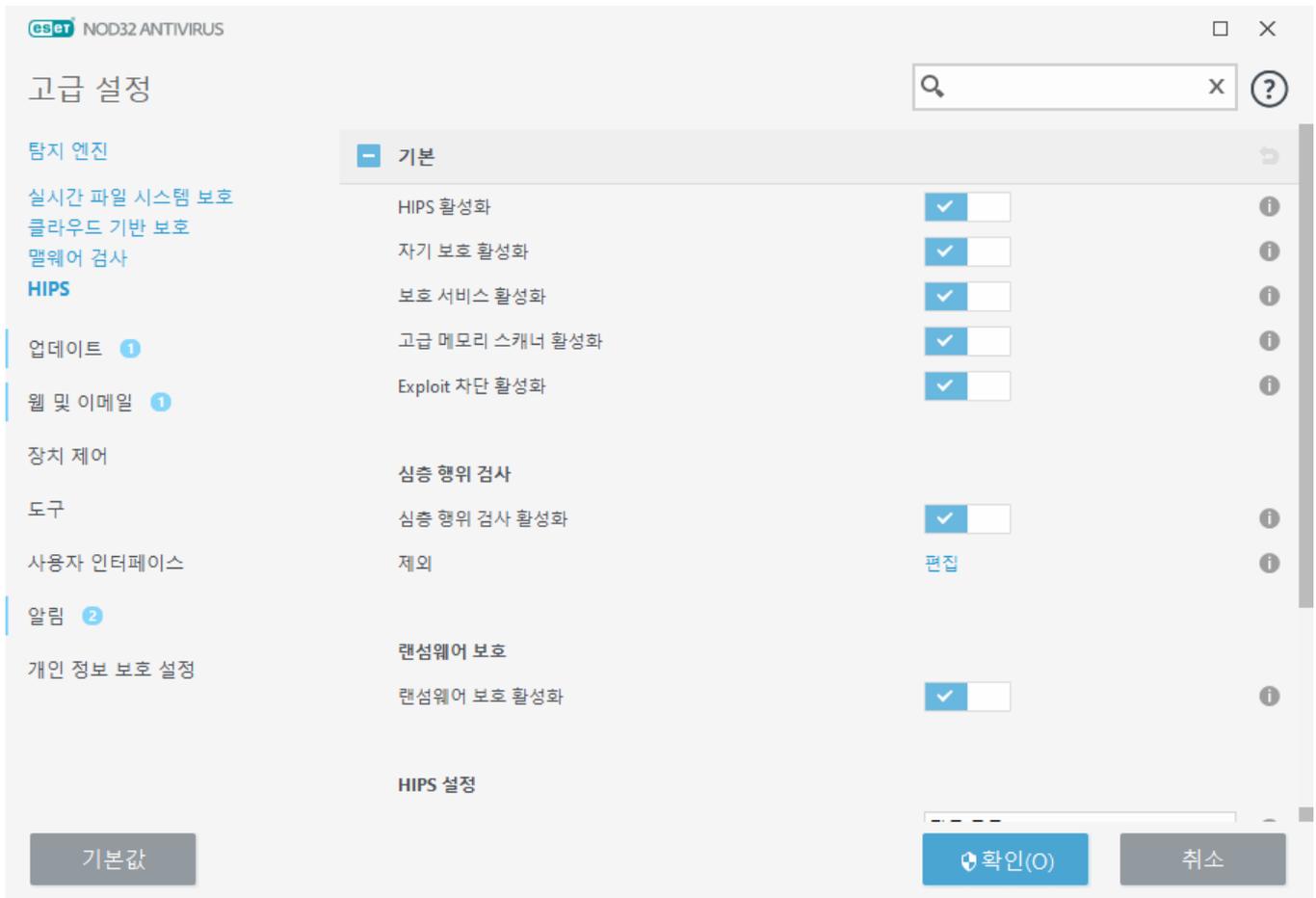
사용자에게 알림 - 기존 규칙에 의해 차단된 장치를 삽입하면 알림 창이 표시됩니다.

HIPS(호스트 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. 따라서 운영 체제 내에서 실행 중인 프로세스만 모니터링합니다.

HIPS 설정은 **고급 설정(F5) 키 > 검색 엔진 > HIPS > 기본**에서 찾을 수 있습니다. HIPS 상태(활성화됨/비활성화됨)는 ESET NOD32 Antivirus **기본 프로그램 창의 설정 > 컴퓨터 보호**에 표시됩니다.



기본

HIPS 활성화 - HIPS는 ESET NOD32 Antivirus에서 기본적으로 활성화되어 있습니다. HIPS를 끄면 Exploit 차단 같은 나머지 HIPS 기능이 비활성화됩니다.

자기 방어 활성화 - ESET NOD32 Antivirus에는 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.

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 이상에서 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 [용어집](#)을 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 [용어집](#)을 참조하십시오.

심층 행위 검사

깊은 동작 검사 활성화 - HIPS 기능의 일부로 작동하는 추가적인 보호 기능입니다. 이 HIPS 확장 기능은 컴퓨터에서 실행 중인 모든 프로그램의 동작을 분석하고 프로세스의 동작이 악의적인 경우 경고를 표시합니다.

[깊은 동작 검사에서 HIPS 제외](#)에서는 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.](#)

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 후에 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 편집](#)에서 확인할 수 있습니다.

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 순위](#)를 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.

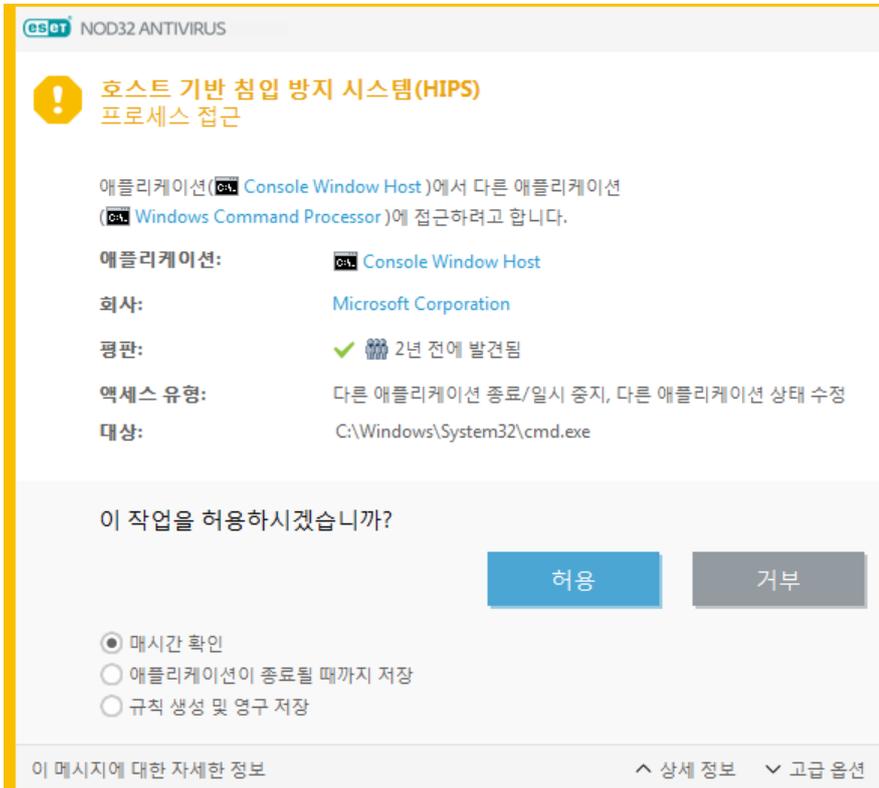
작업을 트리거한 애플리케이션, 파일의 평판 또는 허용 또는 거부를 요청 받은 작업의 종류를 보려면 아래쪽의 **상세 정보**를 클릭합니다.

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.

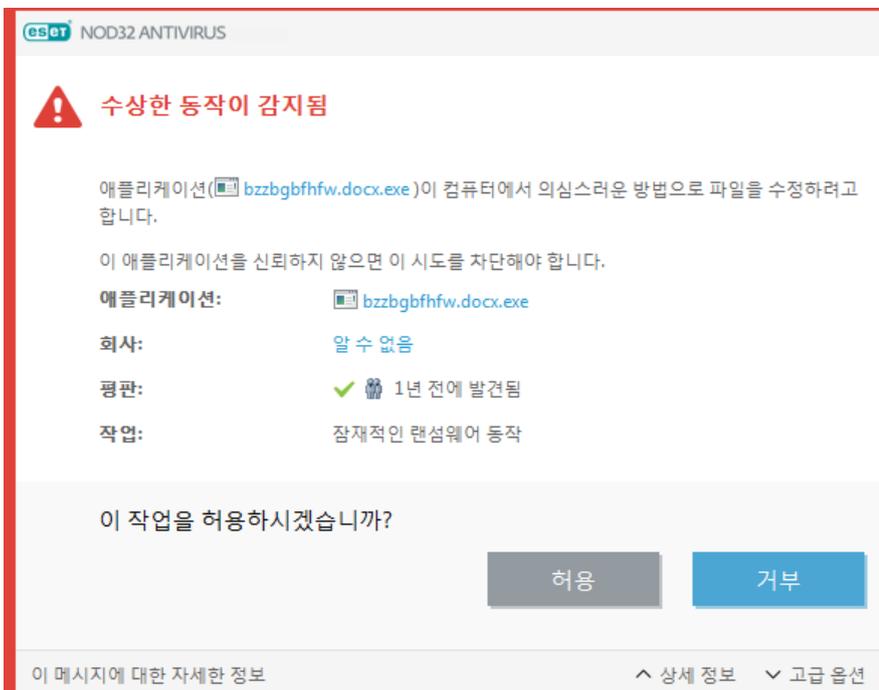
무한 HIPS 알림?

- ! 알림이 표시되는 것을 중지하려면 **고급 설정(F5 키) > 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 허용하도록 선택할 수 있습니다.



특정 검색 파라미터를 보려면 상세 정보를 클릭합니다. 대화 상자 창을 통해 분석을 위해 전송 또는 검색에서 제외를 선택할 수 있습니다.

❗ ESET LiveGrid®를 올바르게 작동하려면 [래쉬웨어 보호](#)에 대해 활성화해야 합니다.

HIPS 규칙 관리

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 원칙](#)도 참조하십시오.

열

규칙 - 사용자가 정의하거나 자동으로 선택된 규칙 이름입니다.

활성화됨 - 목록에서 규칙을 유지하되 사용하지 않으려면 슬라이더 막대를 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 로그](#)에 기록됩니다.

알림 - 이벤트가 트리거되면 오른쪽 아래의 모서리에 작은 팝업 창이 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 우선 순위 수준을 조정하는 옵션은 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 편집

먼저 [HIPS 규칙 관리](#)를 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 슬라이더 막대를 비활성화합니다.

로깅 심각도 - 이 옵션을 활성화하면 이 규칙에 대한 정보가 [HIPS 로그](#)에 기록됩니다.

사용자에게 알림 - 이벤트가 트리거되면 오른쪽 아래 모서리에 작은 팝업 창이 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 파일을 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 수동으로 항목을 입력하거나 **레지스트리 편집기 열기**를 클릭하여 레지스트리에서 키를 선택합니다. 드롭다운 메뉴에서 **모든 항목**을 선택하여 모든 애플리케이션을 추가할 수도 있습니다.

i 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.

중요한 작업에 대한 설명:

파일 작업

- **파일 삭제** - 애플리케이션에서 대상 파일을 삭제할 권한이 있는지 여부를 확인합니다.
- **파일에 작성** - 애플리케이션에서 대상 파일에 작성할 권한이 있는지 여부를 확인합니다.
- **디스크에 직접 접근** - 애플리케이션이 일반적인 Windows 절차를 회피하는 표준 이외의 방법으로 디스크에서 읽거나 디스크에 씁니다. 이로 인해 해당 규칙이 적용되지 않은 상태에서 파일이 수정될 수 있습니다. 이 작업은 검출을 회피하려고 하는 맬웨어, 디스크의 정확한 복사본을 생성하려는 백업 소프트웨어 또는 디스크 볼륨을 인식하려는 파티션 관리자가 원인일 수 있습니다.
- **전체 후크 설치** - MSDN 라이브러리에서 SetWindowsHookEx 함수 호출을 참조합니다.
- **드라이버 로드** - 시스템에 드라이버를 설치 및 로드합니다.

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.

i 64비트 버전의 Windows XP에서는 프로세스 작업을 가로챌 수 없습니다.

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.

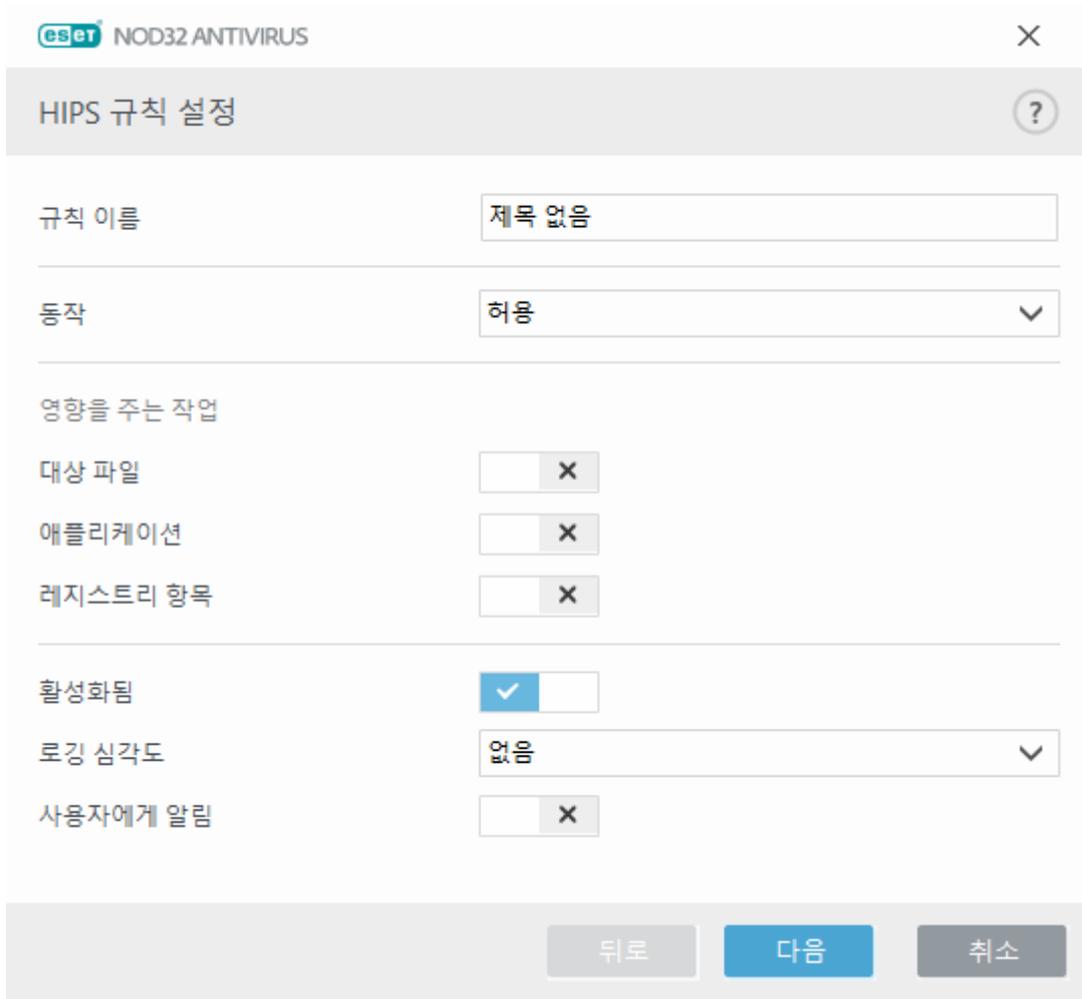
- **레지스트리 수정** - 레지스트리 키에 대한 새 값을 생성하거나 기존의 값을 변경하거나 DB 트리의 데이터를 이동하거나 레지스트리 키에 대한 사용자나 그룹 권한을 설정합니다.

대상 입력 시 특정 제한 사항으로 와일드카드를 사용할 수 있습니다. 레지스트리 경로에 특정 키 대신 *(별표) 기호를 사용할 수 있습니다. 예를 들어 `HKEY_USERS*\software`는 `HKEY_USER\default\software`를 의미할 수 있지만 `HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\default\software`를 의미할 수는 없습니다. `HKEY_LOCAL_MACHINE\system\ControlSet*`는 유효한 레지스트리 키 경로가 아닙니다. *가 있는 레지스트리 키 경로는 "이 경로 또는 해당 기호 뒤에 있는 모든 수준의 모든 경로"를 정의합니다. 이 방법은 파일 대상에 와일드카드를 사용하는 유일한 방법입니다. 먼저 경로의 특정 부분이 평가된 다음 와일드카드 기호(*) 뒤에 있는 경로가 평가됩니다.

⚠ 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** 옆의 슬라이더 막대를 활성화하면 규칙이 적용될 때마다 알림을 표시할 수 있습니다.
3. 규칙이 적용될 **하나 이상의 작업**을 **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. **C추가**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`

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.

i 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.

게이머 모드

게이머 모드는 소프트웨어를 중단 없이 사용하고 팝업 창의 방해받지 않으며 CPU의 사용을 최소화하려는 사용자를 위한 기능입니다. 게이머 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 보호**에서  을 클릭하거나 **게이머 모드** 옆에 있는  을 클릭하여 게이머 모드를 활성화하거나 비활성화할 수 있습니다. 게이머 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 **게이머 모드 활성화**가 주황색으로 표시됩니다.

전체 화면 애플리케이션을 시작할 때마다 게이머 모드가 시작되고 애플리케이션을 종료하면 게이머 모드가 중지되도록 하려면 **고급 설정(F5 키) > 도구 > 게이머 모드**에서 **전체 화면 모드로 애플리케이션을 실행할 때 자동으로 게이머 모드 활성화**를 활성화합니다.

게이머 모드가 자동으로 비활성화되는 시간을 정의하려면 **다음 시간 후 자동으로 게이머 모드 비활성화**를 활성화합니다.

시작 검사

기본적으로 자동 시작 파일 검사는 시스템을 시작할 때와 검색 엔진을 업데이트하는 동안 수행됩니다. 이 검사는 [스케줄러 구성 및 작업](#)에 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(자세한 내용은 다음 장 참조).

스케줄러 작업 생성 및 관리에 대한 자세한 내용은 [새 작업 생성](#)을 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 로그인하기 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 로그인한 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.

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(F5) > 탐지 엔진 > 악성코드 검사 > 문서 보호**를 열고 **문서 보호 활성화** 옆의 슬라이더 막대를 클릭합니다.

i 이 기능은 Microsoft Office 2000 이상 또는 Microsoft Internet Explorer 5.0 이상 등 Microsoft Antivirus API를 사용하는 애플리케이션에 의해 활성화됩니다.

제외

제외에서는 **개체**를 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 제외에서는 검사에서 파일 및 폴더를 제외할 수 있습니다. 성능 제외는 게임 애플리케이션의 파일 수준 검사를 제외하려는 경우나 비정상적인 시스템 동작을 유발하는 경우나 성능 향상을 위한 경우에 유용합니다.

탐지 제외에서는 탐지 이름, 경로 또는 해당 해시를 사용하여 탐지에서 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

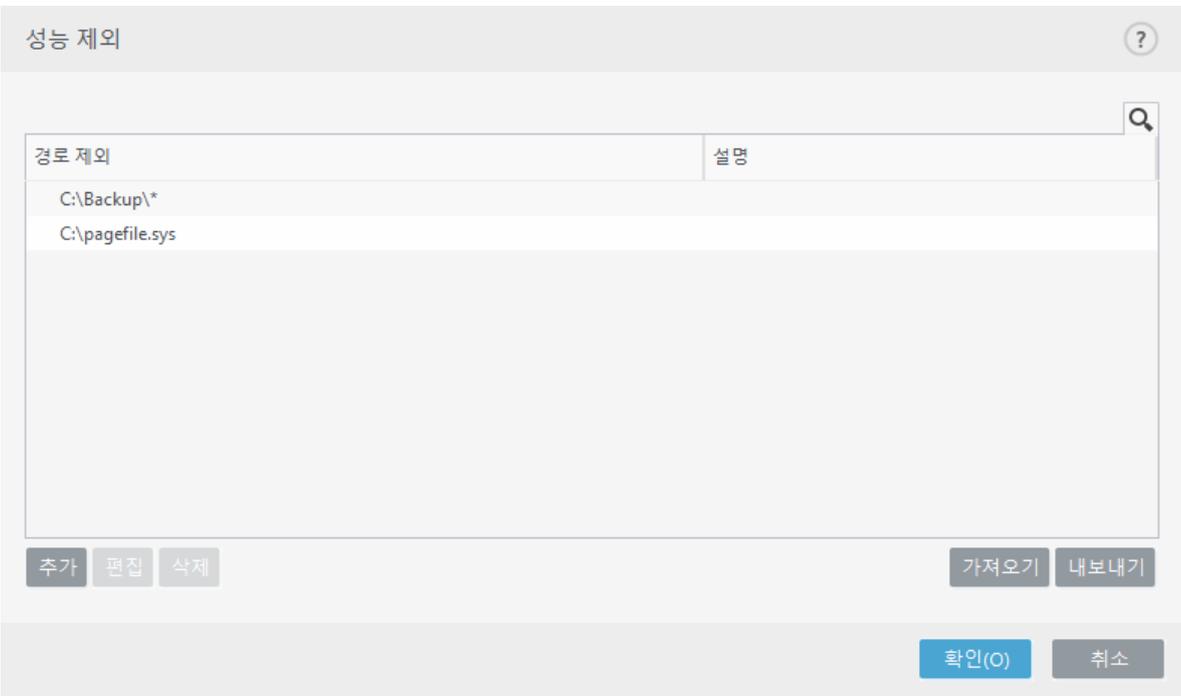
성능 제외를 사용하여 파일 및 폴더를 검사에서 제외할 수 있습니다.

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(F5 키) > 탐지 엔진 > 제외 > 성능 제외 > 편집을 통해 검사에서 제외할 파일 및 폴더를 제외 목록에 추가할 수 있습니다.

i 탐지 제외, 제외된 파일 확장명, HIPS 제외 또는 프로세스 제외와 혼동하지 마십시오.

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



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

제어 요소

- **추가** - 개체를 검색에서 제외합니다.
- **편집** - 선택한 항목을 편집할 수 있습니다.
- **삭제** - 선택한 항목을 제거합니다(여러 항목을 선택하려면 CTRL + 클릭).

성능 제외 추가 또는 편집

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

경로를 선택하거나 수동으로 입력

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

제외 항목 편집

경로 C:\Backup* ...

설명

확인 취소

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

제외 형식

- 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 Tools도 파일 이름일 수 있습니다.
- C:\Tools*.dat - Tools 폴더에서 .dat 파일을 제외합니다.
- C:\Tools\sg.dat - 정확한 경로에 있는 이 특정 파일을 제외합니다.

제외 항목의 시스템 변수

%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 와일드카드는 지원되지 않음

경로 중간에 와일드카드를 사용(예: C:\Tools*\Data\file.dat)하면 작동할 수는 있지만 성능 제외 시 공식적으로 지원되지 않습니다. 자세한 내용은 다음 [지식베이스 문서](#)를 참조하십시오.

탐지 제외를 사용할 때는 경로 중간에 자유롭게 와일드카드를 사용할 수 있습니다.

제외 순서

- 맨 위로/맨 아래로 버튼을 사용하여 제외 우선 순위 수준을 조정하는 옵션은 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.

제외 형식

- 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)



- 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 Tools도 파일 이름일 수 있습니다.
- C:\Tools*.dat - Tools 폴더에서 .dat 파일을 제외합니다.
- C:\Tools\sg.dat - 정확한 경로에 있는 이 특정 파일을 제외합니다.

제외 항목의 시스템 변수

%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.

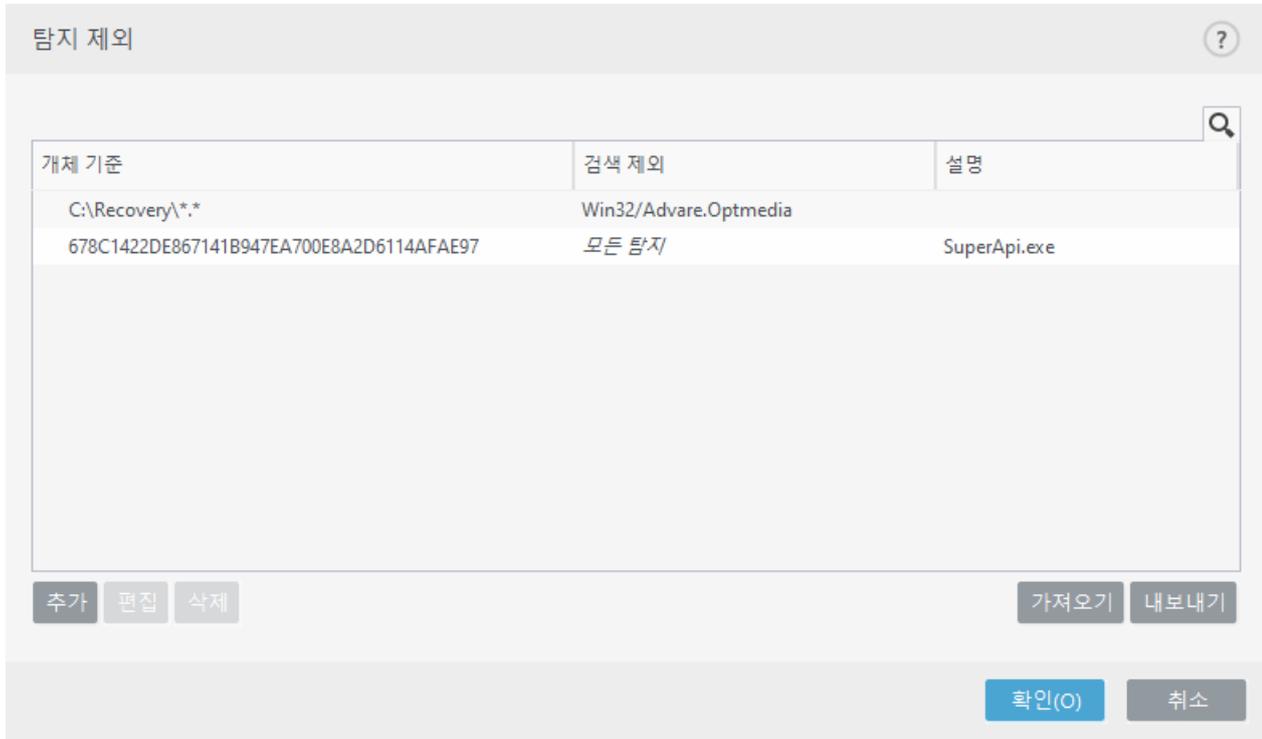
탐지 제외

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

탐지 제외 작동 방식



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.exe인 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 (F5 키) > 탐지 엔진 > 제외 > 탐지 제외 > 편집**을 클릭합니다.

i 성능 제외, 제외된 파일 확장명, HIPS 제외 또는 프로세스 제외와 혼동하지 마십시오.

탐지 엔진에서 개체(해당 탐지 이름 또는 해시에 따라)를 제외하려면 **추가**를 클릭합니다.

사용자가 위치 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 마법사**를 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**를 선택하여 생성할 수 있습니다.

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.

탐지 제외 추가 또는 편집

검색 제외

유효한 ESET 탐지 이름을 입력해야 합니다. 유효한 탐지 이름의 경우 [로그 파일](#)을 참조한 다음 로그 파일 드롭다운 메뉴에서 **검색**을 선택합니다. 이는 ESET NOD32 Antivirus에서 [가양성 샘플](#)이 탐지되는 경우 유용합니다. 실제 침입에 대한 제외는 매우 위험하므로, **경로** 필드에서 ...를 클릭하여 영향을 받는 파일/디렉토리를 제외하거나 일시적으로만 제외하는 것이 좋습니다. 제외는 [사용자가 위치 않는 애플리케이션](#), 잠재적으로 안전하지 않은 애플리케이션 및 감염 의심 애플리케이션에도 적용됩니다.

[경로 제외 형식](#)도 참조하십시오.

제외 항목 편집	
경로	C:\Recovery**
해시	
검색 이름	Win32/Advare.Optmedia
설명	

확인 취소

아래에서 [탐지 제외 예](#)를 참조하십시오.

해시 제외

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

제외 항목 편집	
경로	
해시	678C1422DE867141B947EA700E8A...
검색 이름	
설명	SuperApi.exe

확인 취소

탐지 이름별 제외

이름을 기준으로 특정 위협을 제외하려면 다음과 같이 유효한 탐지 이름을 입력합니다.
Win32/Adware.Optmedia

- ✓ ESET NOD32 Antivirus 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).

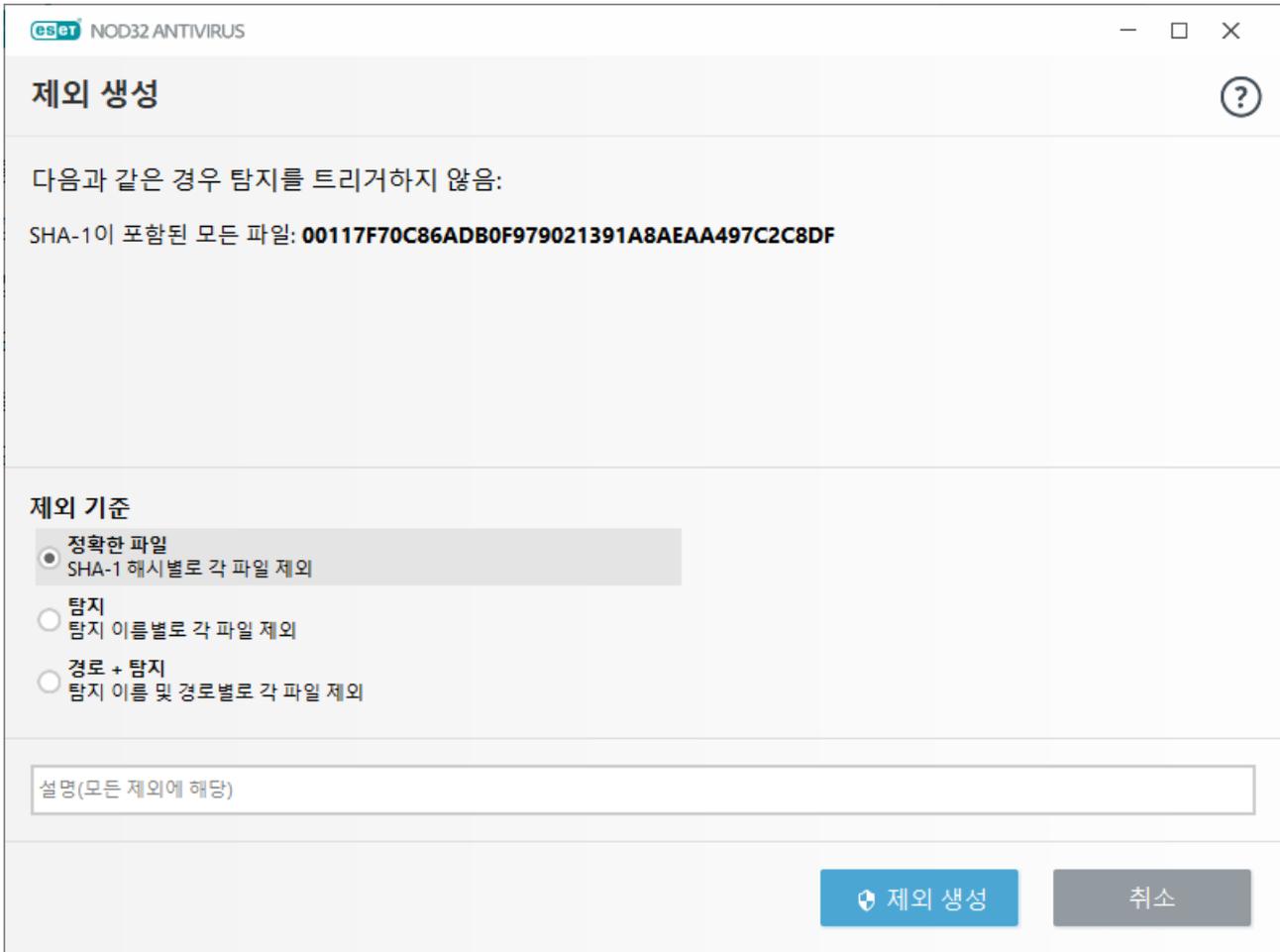
1. [기본 프로그램 창](#)에서 다음을 클릭합니다. **도구 > 로그 파일**.
2. **탐지 로그**에서 탐지를 마우스 오른쪽 버튼으로 클릭합니다.
3. **제외 생성**을 클릭합니다.

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.



HIPS 제외

제외를 사용하면 HIPS 깊은 동작 검사에서 프로세스를 제외할 수 있습니다.

HIPS 제외를 편집하려면 **고급 설정(F5 키) > 탐지 엔진 > HIPS > 기본 > 제외 > 편집**으로 이동합니다.

i 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.

ThreatSense 파라미터

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 사용하면 여러 검사 파라미터를 지정할 수 있습니다.

- 검사할 파일 형식 및 확장명
- 다양한 검출 방법의 조합
- 치료 수준 등

설정 창으로 들어가려면 ThreatSense 기술을 사용하는 모듈(아래 참조)의 고급 설정 창에 있는 **ThreatSense 파라미터**를 클릭합니다. 각 보안 시나리오에 따라서 다른 구성이 필요할 수 있습니다. 이를 염두에 두고, 다음 보호 모듈에 대해 ThreatSense를 개별적으로 구성할 수 있습니다.

- 실시간 파일 시스템 보호
- 유틸리티 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.

휴리스틱 - 휴리스틱은 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 워 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 NOD32 Antivirus의 동작이 결정됩니다. 치료 수준에는 다음의 4가지가 있습니다.

ThreatSense 파라미터는 다음 수정(예: 치료) 수준으로 제공됩니다.

ESET NOD32 Antivirus의 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.
안전하면 탐지 수정, 그렇지 않으면 유지	최종 사용자가 개입하지 않고 개체 를 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 대화형 창이 나타나면 수정 동작(예: 제거 또는 무시)을 선택해야 합니다. 이 수준은 탐지 이벤트에서 취해야 할 단계를 알고 있는 고급 사용자를 위한 것입니다.

제외

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로, 파일의 형식과 내용을 정의합니다. ThreatSense 파라미터 설정의 이 섹션에서는 검사할 파일 형식을 정의할 수 있습니다.

기타

수동 컴퓨터 검사에 대해 ThreatSense 엔진 파라미터 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 로그 - [검사 로그](#)는 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 압축 파일 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 검사

가 중지되지는 않습니다(예: 사용자 정의 변수가 3초이지만 파일 압축 해제에는 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 위협으로 인해 권장되지 않음).
기본값은 제한 없음입니다.

압축파일 검사 설정

다중 압축 수준 - 최대 압축파일 검사 수준을 지정합니다. 기본값은 10.

압축파일 내 파일의 최대 크기 - 이 옵션을 사용하면 검사할 압축파일에 포함된 파일의 최대 파일 크기(압축 해제 시)를 지정할 수 있습니다. 최대값은 **3GB**입니다.

i 일반적인 상황에서는 기본값을 수정할 필요가 없으므로 기본값을 변경하지 않는 것이 좋습니다.

검사에서 제외된 파일 확장명

제외된 파일 확장명은 **ThreatSense 파라미터**의 일부입니다. 제외된 파일 확장명을 구성하려면 고급 설정 창에서 **ThreatSense 기술을 사용하는 모듈**에 대한 **ThreatSense 파라미터**를 클릭합니다.

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로, 파일의 형식과 내용을 정의합니다. ThreatSense 파라미터 설정의 이 섹션에서는 검사할 파일 형식을 정의할 수 있습니다.

i 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;tmp를 입력).
특수 기호?(물음표)를 사용할 수 있습니다. 물음표는 임의의 기호를 나타냅니다(예: ?db).

i Windows 운영 체제에 있는 파일의 정확한 확장명을 확인(해당하는 경우)하려면 **제어판 > 폴더 옵션 > 보기(탭)의 알려진 파일 형식의 파일 확장명 숨기기** 옵션을 선택 취소하고 이 변경 사항을 적용해야 합니다.

추가 ThreatSense 파라미터

이러한 설정을 편집하려면 **고급 설정(F5 키) > 탐지 엔진 > 실시간 파일 시스템 보호 > 추가 ThreatSense 파라미터**로 이동합니다.

새로 생성 및 수정한 파일에 대한 추가 ThreatSense 파라미터

새로 생성하거나 수정한 파일의 감염 가능성은 기존 파일보다 비교적 더 높습니다. 이 같은 이유로 프로그램에서 추가 검사 파라미터를 통해 이러한 파일을 확인합니다. ESET NOD32 Antivirus에서는 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 인공지능**이 사용됩니다. 활성화된 경우 **스마트 최적화** 및 **ESET LiveGrid®**를 활성화된 상태로 유지하여 시스템 성능에 미치는 영향을 완화하는 것이 좋습니다.

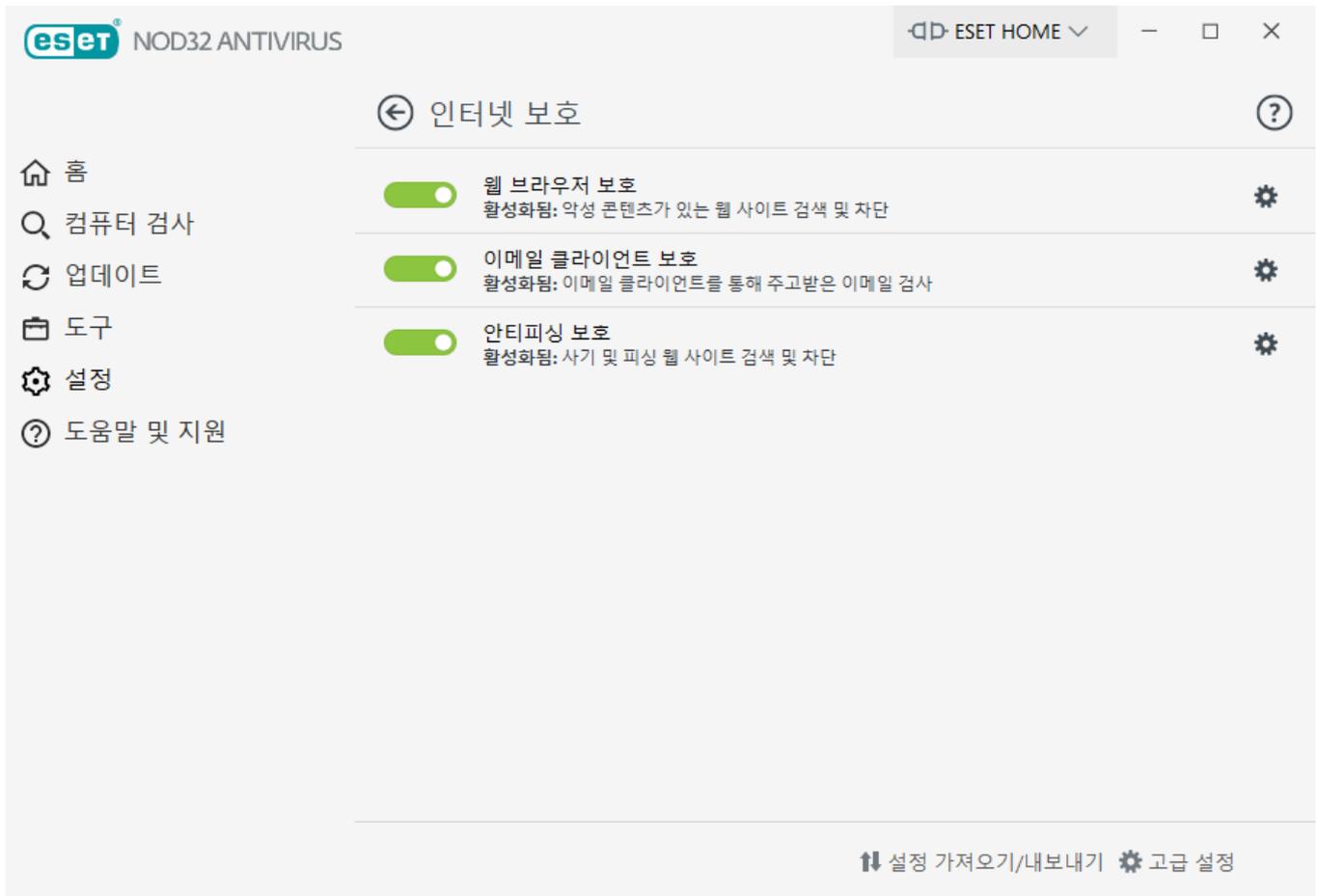
이동식 미디어에서 파일 실행 시 고급 인공지능 - 고급 인공지능은 가상 환경에서 코드를 에뮬레이션하고 이동식 미디어로부터의 코드 실행이 허용되기 전에 동작을 평가합니다.

인터넷 보호

웹 및 이메일 구성은 **인터넷 보호**를 클릭하여 **설정** 창에서 찾을 수 있습니다. 여기서 보다 상세한 프로그램 설정에 접근할 수 있습니다.

개별 보호 모듈을 일시 중지하거나 비활성화하려면 슬라이더 막대 아이콘 을 클릭합니다.

⚠ 보호 모듈을 끄면 컴퓨터의 보호 수준이 저하될 수 있습니다.



⚙️을 클릭하여 고급 설정에서 웹/이메일/안티피싱 보호 설정을 엽니다.

인터넷 연결은 PC의 표준 기능입니다. 그렇지만 인터넷은 악성 코드를 배포하는 기본 매개체로 변질되었습니다. 따라서 [웹 브라우저 보호](#) 설정에 특별한 주의를 기울여야 합니다.

[이메일 클라이언트 보호](#)는 POP3(S) 및 IMAP(S) 프로토콜을 통해 받은 이메일 통신을 제어합니다. ESET NOD32 Antivirus는 이메일 클라이언트용 플러그인 프로그램을 사용하여 이메일 클라이언트의 모든 통신을 제어합니다.

[안티피싱 보호](#)는 피싱 콘텐츠를 배포하는 것으로 알려진 웹 페이지를 차단할 수 있도록 합니다. 안티피싱을 활성화된 상태로 두는 것이 좋습니다.

프로토콜 필터링

애플리케이션 프로토콜에 대한 안티바이러스 보호 기능은 ThreatSense 탐지 엔진에서 제공됩니다. 이 탐지 엔진은 모든 고급 악성코드 검사 기술을 원활하게 통합합니다. 프로토콜 필터링은 사용되는 인터넷 브라우저 또는 이메일 클라이언트에 상관없이 자동으로 작동합니다. 암호화된(SSL/TLS) 설정을 편집하려면 **고급 설정(F5 키) > 웹 및 이메일 > SSL/TLS**로 이동합니다.

애플리케이션 프로토콜 콘텐츠 필터링 활성화 - 프로토콜 필터링을 비활성화하는 데 사용할 수 있습니다. 많은 ESET NOD32 Antivirus 구성 요소(웹 브라우저 보호, 이메일 프로토콜 보호, 안티피싱, 자녀 보호)가 이 옵션을 사용하며 이 옵션 없이는 작동하지 않습니다.

제외된 애플리케이션 - 프로토콜 필터링에서 특정 애플리케이션을 제외할 수 있습니다. 프로토콜 필터링으로 인해 호환성 문제가 발생하는 경우 유용합니다.

제외된 IP 주소 - 프로토콜 필터링에서 특정 원격 주소를 제외할 수 있습니다. 프로토콜 필터링으로 인해 호환성 문제가 발생하는 경우 유용합니다.

추가(예: 2001:718:1c01:16:214:22ff:fec9:ca5)합니다.

서브넷 - 서브넷(컴퓨터 그룹)은 IP 주소 및 마스크로 정의됩니다(예: 2002:c0a8:6301:1::1/64).

제외된 IP 주소의 예

IPv4 주소 및 마스크:

- 192.168.0.10 - 규칙을 적용할 개별 컴퓨터의 IP 주소를 추가합니다.
- 192.168.0.1~192.168.0.99 - 규칙을 적용할 여러 컴퓨터의 IP 범위를 지정하려면 시작 IP 주소와 끝 IP 주소를 입력합니다.
- IP 주소 및 마스크로 정의된 서브넷(컴퓨터 그룹)입니다. 예를 들어, 255.255.255.0은
- ✓ 192.168.1.0/24 접두어(192.168.1.1 ~ 192.168.1.254 주소 범위를 의미)에 대한 네트워크 마스크입니다.

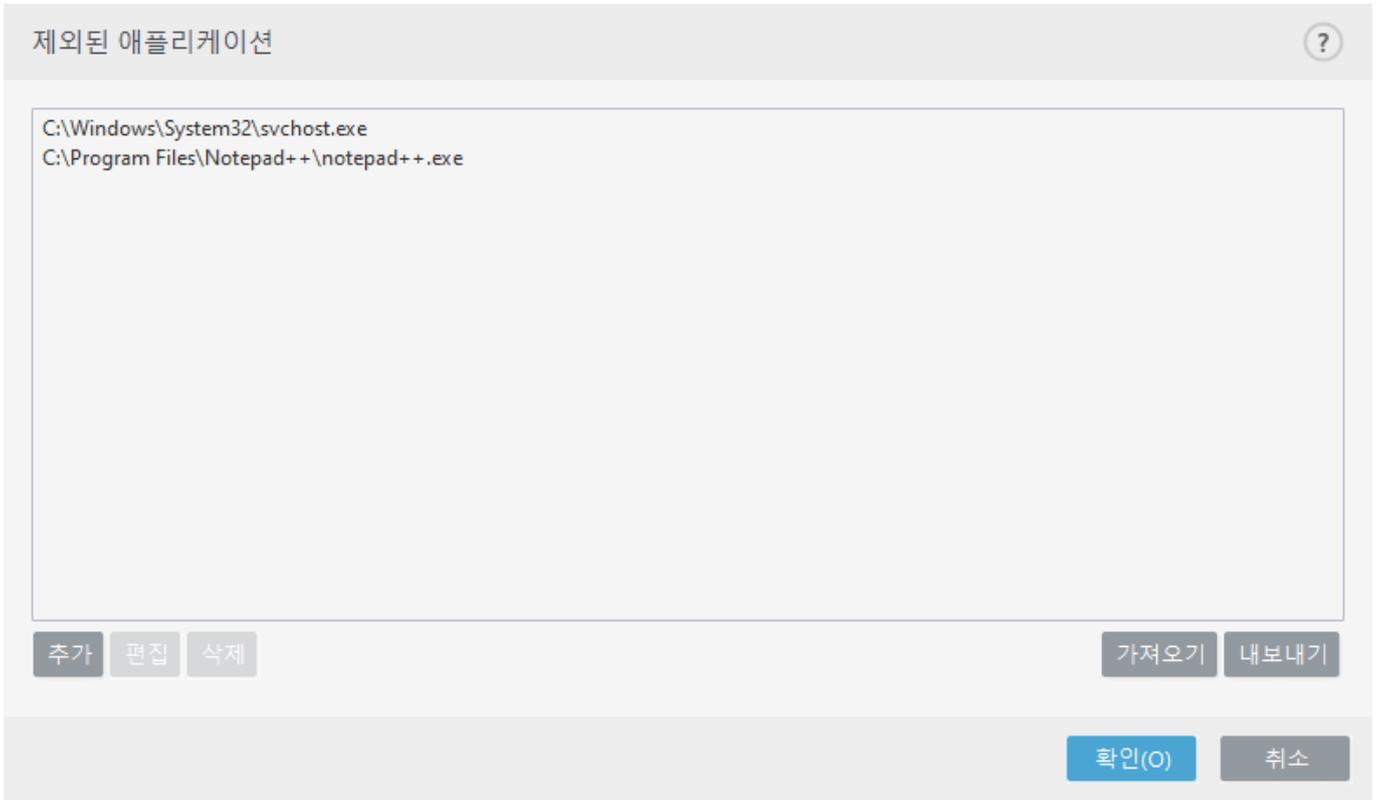
IPv6 주소 및 마스크:

- 2001:718:1c01:16:214:22ff:fec9:ca5 - 규칙을 적용할 개별 컴퓨터의 IPv6 주소입니다.
- 2002:c0a8:6301:1::1/64 - 접두어 길이가 64비트(2002:c0a8:6301:0001:0000:0000:0000:0000 ~ 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff를 의미)인 IPv6 주소입니다.

제외된 애플리케이션

콘텐츠 필터링에서 특정 네트워크 인식 애플리케이션의 통신을 제외하려면 목록에서 해당 애플리케이션을 선택합니다. 선택한 애플리케이션의 HTTP/POP3/IMAP 통신은 위협에 대해 검사되지 않습니다. 이 옵션은 통신 검사 도중 제대로 작동하지 않는 애플리케이션에 대해서만 사용하는 것이 좋습니다.

실행 중인 애플리케이션 및 서비스는 여기서 자동으로 사용할 수 있습니다. 프로토콜 필터링 목록에 애플리케이션이 표시되지 않는 경우 애플리케이션을 수동으로 추가하려면 **추가**를 클릭합니다.

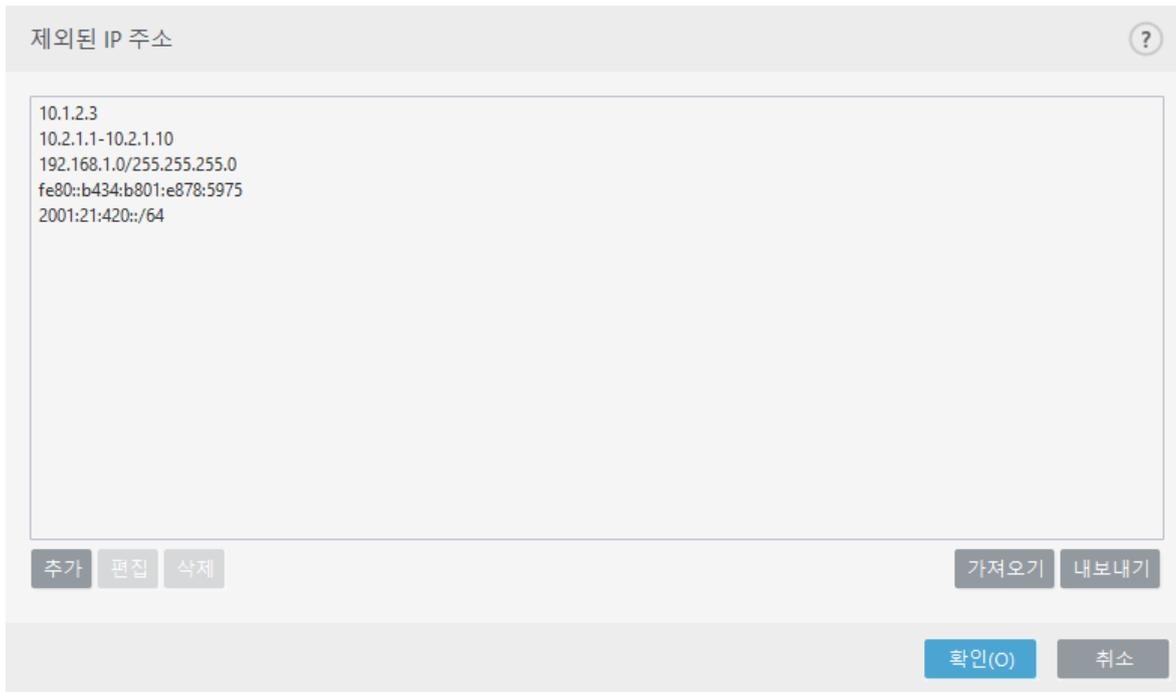


제외된 IP 주소

목록의 항목은 프로토콜 콘텐츠 필터링에서 제외됩니다. 선택한 주소와의 HTTP/POP3/IMAP 통신은 위협에 대해 검사되지 않습니다. 신뢰할 수 있는 것으로 알려진 주소에 한해서만 이 옵션을 사용하는 것이 좋습니다.

추가를 클릭하여 프로토콜 필터링 목록에 표시되지 않은 원격 지점의 IP 주소/주소 범위/서브넷을 제외할 수 있습니다.

제거를 클릭하여 목록에서 선택한 항목을 제거할 수 있습니다.



IPv4 주소 추가

이 옵션을 사용하면 규칙이 적용되는 원격 지점의 IP 주소/주소 범위/서브넷을 추가할 수 있습니다. 인터넷 프로토콜 버전 4는 이전 버전이지만 여전히 가장 널리 사용되고 있습니다.

단일 주소 - 규칙을 적용할 개별 컴퓨터의 IP 주소(예: **192.168.0.10**)를 추가합니다.

주소 범위 - 규칙을 적용할 여러 컴퓨터의 IP 범위를 지정하려면 시작 IP 주소와 끝 IP 주소를 입력합니다(예: **192.168.0.1~192.168.0.99**).

서브넷 - IP 주소 및 마스크에서 정의된 서브넷(컴퓨터 그룹)입니다.

예를 들어 **255.255.255.0** 은 **192.168.1.0/24** 접두어 (**192.168.1.1~192.168.1.254** 주소 범위를 의미)에 대한 네트워크 마스크입니다.

IPv6 주소 추가

이 옵션을 사용하면 규칙이 적용되는 원격 지점의 IPv6 주소/서브넷을 추가할 수 있습니다. IPv6은 최신 인터넷 프로토콜 버전으로, 이전 버전인 4를 대체할 예정입니다.

단일 주소 - 규칙을 적용할 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**).

SSL/TLS

ESET NOD32 Antivirus은(는) SSL 프로토콜을 사용하는 통신에서 위협 요소를 검사할 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 프로토콜 필터링 활성화 - 프로토콜 필터링이 비활성화된 경우 SSL을 통한 통신이 검사되지 않습니다.

SSL/TLS 프로토콜 필터링 모드는 다음과 같은 옵션에서 사용할 수 있습니다.

필터링 모드	설명
자동 모드	기본 모드는 웹 브라우저 및 이메일 클라이언트 등과 같은 해당 애플리케이션만 검사합니다. 통신을 검사할 애플리케이션을 선택하여 재정의할 수 있습니다.
대화 모드	알 수 없는 인증서를 사용하여 SSL로 보호된 새로운 사이트에 들어가면 동작 선택 대화 상자 가 표시됩니다. 이 모드를 사용하면 검사에서 제외될 SSL 인증서/애플리케이션 목록을 생성할 수 있습니다.
정책 모드	정책 모드 - 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.

SSL/TLS 필터링된 애플리케이션 목록은 특정 애플리케이션의 ESET NOD32 Antivirus 동작을 사용자 지정하는 데 사용할 수 있습니다.

알려진 인증서 목록 - 특정 SSL 인증서에 대한 ESET NOD32 Antivirus 동작을 사용자 지정할 수 있습니다.

신뢰할 수 있는 도메인과의 통신 제외 - 이 기능을 활성화하면 신뢰할 수 있는 도메인과의 통신은 검사에서 제외됩니다. 도메인 신뢰도는 기본 제공 허용 목록에 따라 결정됩니다.

구식 프로토콜 SSL v2를 사용하여 암호화된 통신 차단 - 이전 버전의 SSL 프로토콜을 사용하는 통신을 자동으로 차단합니다.

루트 인증서

알려진 브라우저에 루트 인증서 추가 - 브라우저/이메일 클라이언트에서 SSL 통신이 제대로 작동하려면 ESET에 대한 루트 인증서를 알려진 루트 인증서(게시자) 목록에 추가해야 합니다. 활성화하면 ESET NOD32 Antivirus에서 ESET SSL Filter CA 인증서를 알려진 브라우저(예: Opera)에 자동으로 추가합니다. 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 유효성

인증서 신뢰를 설정할 수 없는 경우 - 경우에 따라 TRCA(신뢰할 수 있는 루트 인증 기관) 저장소를 사용하여 웹 사이트 인증서를 확인하지 못할 수 있습니다. 따라서 누군가(예: 웹 서버 또는 소기업 관리자) 인증서에 서명했으며 이 인증서를 신뢰할 수 있는 것으로 간주하는 일이 항상 위험하지는 않습니다. 은행 등 대부분의 대기업은 TRCA에서 서명한 인증서를 사용합니다. **인증서 유효성에 대해 확인**(기본적으로 선택됨)을 선택한 경우 사용자에게 암호화된 통신이 설정되면 수행할 동작을 선택하라는 메시지가 표시됩니다. **인증서를 사용하는 통신 차단**을 선택하여 확인되지 않은 인증서를 사용하는 사이트에 대해 암호화된 연결을 항상 종료할 수 있습니다.

인증서가 손상된 경우 - 인증서가 잘못 서명되었거나 손상되었음을 의미합니다. 이 경우 ESET은 **인증서를 사용하는 통신 차단**을 선택한 상태로 유지하는 것을 권장합니다. **인증서 유효성 확인**을 선택한 경우 사용자에게 암호화된 통신이 설정되면 수행할 동작을 선택하라는 메시지가 표시됩니다.

예(그림 포함)

i 다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.

- [ESET Windows 홈 제품의 인증서 알림](#)
- [웹 페이지에 방문하면 "암호화된 네트워크 트래픽: 신뢰할 수 없는 인증서"가 표시됨](#)

인증서

브라우저/이메일 클라이언트에서 SSL 통신이 제대로 작동하려면 ESET에 대한 루트 인증서를 알려진 루트 인증서(게시자) 목록에 추가해야 합니다. **알려진 브라우저에 루트 인증서 추가**를 활성화해야 합니다. Opera, Firefox 등의 알려진 브라우저에 ESET 루트 인증서를 자동으로 추가하려면 이 옵션을 선택합니다. Internet Explorer와 같이 시스템 인증서 저장소를 사용하는 브라우저의 경우에는 인증서가 자동으로 추가됩니다. 지원되지 않는 브라우저에 인증서를 적용하려면 **인증서 보기 > 상세 정보 > 파일에 복사...**를 클릭한 다음 수동으로 인증서를 브라우저로 가져옵니다.

VeriSign 등의 신뢰할 수 있는 루트 인증 기관 저장소를 사용하여 인증서를 확인할 수 없는 경우가 있습니다. 이는 인증서가 누군가(예: 웹 서버 또는 소기업의 관리자)에 의해 자체적으로 지문이 생성되었으며 이 인증서를 신뢰할 수 있는 것으로 간주하는 것이 항상 위험한 것은 아님을 의미합니다. 은행 등 대부분의 대기업은 TRCA에서 지문이 생성된 인증서를 사용합니다. **인증서 유효성에 대해 확인**(기본값)을 선택한 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 확인되지 않은 인증서를 사용하는 사이트에 암호화된 연결을 항상 종료할 수 있습니다.

인증서가 잘못되었거나 손상된 경우 이는 인증서가 만료되었거나 자체적으로 지문이 잘못 생성되었음을 의미합니다. 이 경우 인증서를 사용하는 통신을 차단하는 것이 좋습니다.

암호화된 네트워크 트래픽

시스템이 SSL 프로토콜 검사를 사용하도록 구성된 경우 다음과 같은 두 가지 상황에서 동작을 선택하라는 메시지를 표시하는 대화 상자 창이 표시됩니다.

첫째, 웹 사이트에서 확인할 수 없거나 잘못된 인증서를 사용하는 경우 ESET NOD32 Antivirus 이(가) 이러한 경우에 사용자에게 확인(기본적으로 확인할 수 없는 인증서의 경우 "예", 잘못된 인증서의 경우 "아니요")하도록 구성되어 있으면, 연결을 허용할지 아니면 차단할지 확인하는 대화 상자가 표시됩니다. 인증서가 Trusted Root Certification Authorities store(TRCA)에 없으면 신뢰할 수 없는 인증서로 간주됩니다.

둘째, SSL 프로토콜 필터링 모드가 대화 모드로 설정된 경우 트래픽을 검사할지 아니면 무시할지 확인하는 대화 상자가 웹 사이트별로 표시됩니다. 일부 애플리케이션에서는 SSL 트래픽이 다른 사용자에게 의해 수정되거나 검사되지 않았는지 확인합니다. 이러한 경우 애플리케이션이 계속 작동되도록 하려면 ESET NOD32 Antivirus 이(가) 해당 트래픽을 무시해야 합니다.

예(그림 포함)

i 다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.

- [ESET Windows 홈 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 [알려진 인증서 목록](#)에 저장됩니다.

알려진 인증서 목록

알려진 인증서 목록을 사용하여 특정 SSL 인증서에 대한 ESET NOD32 Antivirus 동작을 사용자 지정하고, SSL/TLS 프로토콜 필터링 모드에서 대화 모드를 선택한 경우 선택한 동작을 저장할 수 있습니다. 고급 설정(F5 키) > 웹 및 이메일 > SSL/TLS > 알려진 인증서 목록에서 목록을 보고 편집할 수 있습니다.

알려진 인증서 목록 창은 다음으로 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.

SSL/TLS 필터링된 애플리케이션 목록

SSL/TLS 필터링된 애플리케이션 목록을 사용하여 특정 애플리케이션에 대한 ESET NOD32 Antivirus 동작을 사용자 지정하고 **SSL/TLS 프로토콜 필터링 모드**가 **대화 모드**일 때 선택한 동작을 저장할 수 있습니다. 목록은 **고급 설정(F5 키) > 웹 및 이메일 > SSL/TLS > SSL/TLS 필터링된 애플리케이션 목록**에서 확인 및 편집할 수 있습니다.

SSL/TLS 필터링된 애플리케이션 목록 창은 다음으로 구성됩니다.

열

애플리케이션 - 애플리케이션의 이름입니다.

검사 동작 - **검사**나 **무시**를 선택하여 통신을 검사하거나 무시합니다. 자동 모드에서 검사하고 대화 모드에서 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.

이메일 클라이언트 보호

ESET NOD32 Antivirus이(가) 이메일 클라이언트와 통합되면 이메일 메시지의 악성 코드에 대한 활성 보호 수준이 높아집니다. 사용자의 이메일 클라이언트가 지원되면 ESET NOD32 Antivirus에서 통합을 활성화할 수 있습니다. 이메일 클라이언트로 통합되면 ESET NOD32 Antivirus 도구 모음이 이메일 클라이언트에 직접 삽입되어 이메일을 보다 효율적으로 보호할 수 있습니다. 통합 설정은 **고급 설정(F5) > 웹 및 이메일 > 이메일 클라이언트 보호 > 이메일 클라이언트**에 있습니다.

이메일 클라이언트 통합

현재 지원되는 이메일 클라이언트로는 [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#), [Windows Live Mail](#) 등이 있습니다. 이메일 보호는 이러한 프로그램의 플러그인으로 작동합니다. 플러그인의 주된 장점은 사용되는 프로토콜과 무관하다는 점입니다. 이메일 클라이언트는 암호화된 메시지를 받으면 메시지 암호를 해독해 바이러스 검사기로 보냅니다. 지원되는 이메일 클라이언트, 해당 버전에 대한 전체 목록은 [ESET 지식 베이스 문서](#)를 참조하십시오.

이메일을 검색할 때 시스템의 속도가 느려지면 **받은 편지함 내용 변경 시 확인 비활성화**를 켭니다.

검사할 이메일

클라이언트 플러그인으로 이메일 보호 활성화 - 비활성화된 경우 이메일 클라이언트 플러그인으로 보호 기능이 꺼집니다.

받은 이메일 - 활성화된 경우 받은 이메일 메시지를 확인합니다.

보낸 이메일 - 활성화된 경우 보낸 이메일 메시지를 확인합니다.

읽은 이메일 - 활성화된 경우 읽은 이메일 메시지를 확인합니다.

i 클라이언트 플러그인으로 이메일 보호 활성화를 활성화된 상태로 유지하는 것이 좋습니다. 통합이 활성화되어 있지 않거나 작동하지 않는 경우에도 이메일 통신은 계속해서 [프로토콜 필터링](#)(IMAP/IMAPS 및 POP3/POP3S)에 의해 보호됩니다.

감염된 이메일에 수행할 동작

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.

업데이트 후 검사 재실행 - 활성화된 경우 탐지 엔진 업데이트 후 감염된 이메일을 다시 검사합니다.

다른 모듈의 검사 결과 수락 - 이메일 보호 모듈에서 다시 검사하는 대신 다른 보호 모듈로부터 받은 검사 결과를 사용하도록 허용합니다.

이메일 프로토콜

IMAP 및 POP3 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.

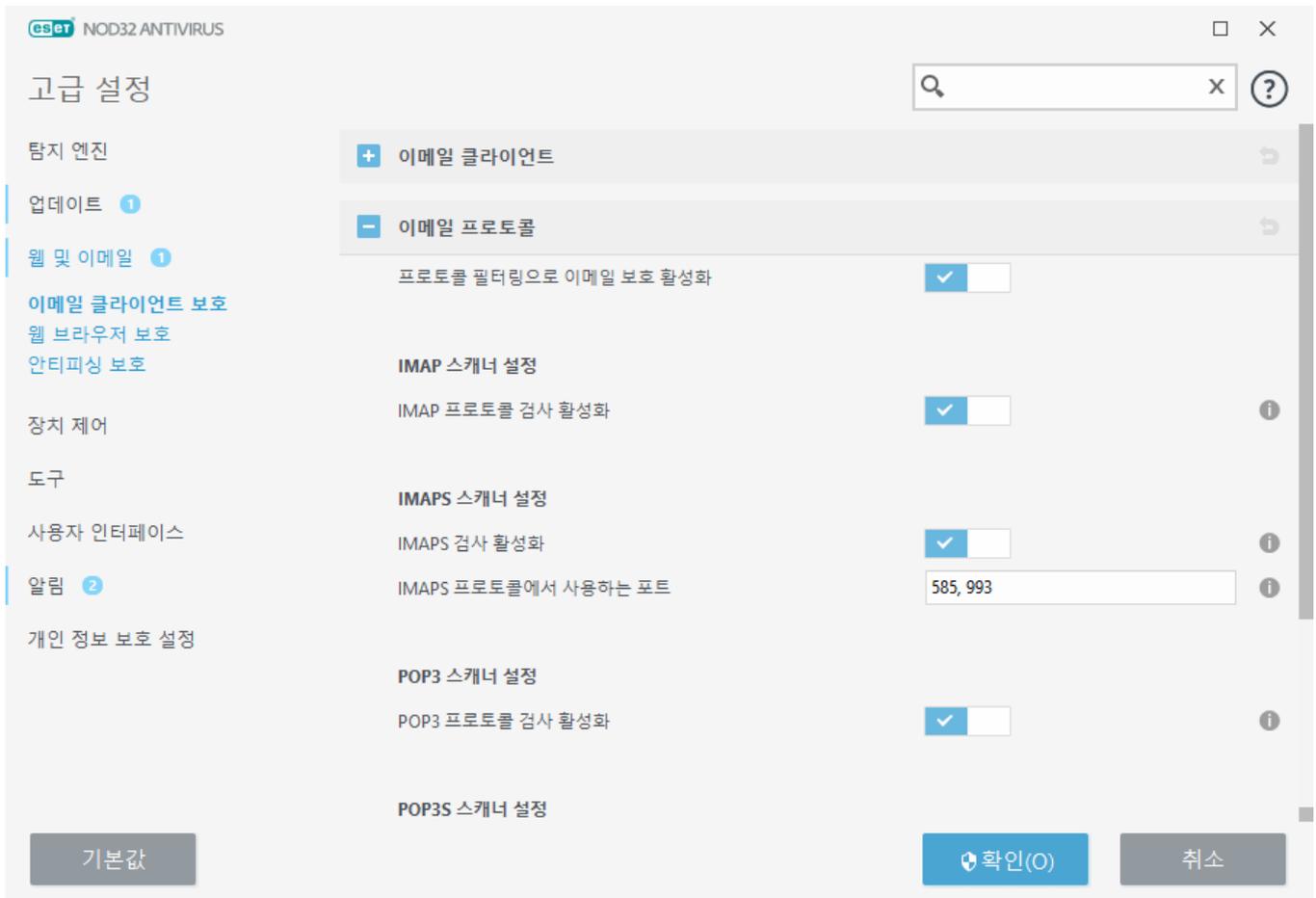
ESET NOD32 Antivirus은(는) 사용된 이메일 클라이언트에 상관없이 이러한 프로토콜에 대한 보호 기능을 제공하며, 이메일 클라이언트를 다시 구성할 필요가 없습니다. 기본적으로 POP3 및 IMAP 프로토콜을 통한 모든 통신은 기본 POP3/IMAP 포트 번호에 상관없이 검사됩니다. IMAP 프로토콜은 검사되지 않습니다. 그러나 Microsoft Exchange 서버와의 통신은 Microsoft Outlook 같은 이메일 클라이언트의 [통합 모듈](#)에 의해 검사될 수 있습니다.

프로토콜 필터링에 의한 이메일 보호 활성화를 활성화된 상태로 유지하는 것이 좋습니다.

IMAP/IMAPS 및 POP3/POP3S 프로토콜 검사를 구성하려면 **고급 설정 > 웹 및 이메일 > 이메일 클라이언트 보호 > 이메일 프로토콜**로 이동하십시오.

ESET NOD32 Antivirus에서는 암호화된 채널을 사용하여 서버와 클라이언트 간에 정보를 전송하는 IMAPS(585, 993) 및 POP3S(995) 프로토콜의 검사도 지원합니다. ESET NOD32 Antivirus에서는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 프로토콜을 사용하여 통신을 검사합니다. 이 프로그램은 운영 체제 버전과 관계없이 **IMAPS/POP3S 프로토콜에서 사용되는 포트**에 정의된 포트의 트래픽만 검사합니다. 필요한 경우 다른 통신 포트를 추가할 수 있습니다. 여러 포트 번호는 쉼표로 구분해야 합니다.

암호화된 통신은 기본적으로 검사됩니다. 검사기 설정을 보려면, **고급 설정 > 웹 및 이메일 > [SSL/TLS](#)**를 엽니다.



POP3, POP3S 필터

POP3 프로토콜은 이메일 클라이언트 애플리케이션에서 이메일 통신을 받는 데 가장 널리 사용되는 프로토콜입니다. ESET NOD32 Antivirus는 사용되는 이메일 클라이언트에 관계없이 이 프로토콜에 대한 보호 기능을 제공합니다.

이 제어를 제공하는 보호 모듈은 시스템 시작 시 자동으로 시작된 다음 메모리에서 활성화됩니다. 이 모듈이 제대로 작동하도록 하려면 모듈이 활성화되어 있는지 확인합니다. POP3 프로토콜 검사는 이메일 클라이언트를 다시 구성하지 않아도 자동으로 수행됩니다. 기본적으로 포트 110의 모든 통신을 검사하지만 필요한 경우 다른 통신 포트도 추가할 수 있습니다. 포트 번호는 쉼표로 분리해야 합니다.

암호화된 통신은 기본적으로 검사됩니다. 검사기 설정을 보려면, 고급 설정 > 웹 및 이메일 > [SSL/TLS](#)를 엽니다.

이 섹션에서는 POP3 및 POP3S 프로토콜 검사를 구성할 수 있습니다.

POP3 프로토콜 검사 활성화 - 이 옵션을 활성화하면 POP3를 통한 모든 트래픽에 악성 소프트웨어가 있는지 모니터링합니다.

POP3 프로토콜이 사용하는 포트 - POP3 프로토콜이 사용하는 포트(기본값: 110) 목록입니다.

ESET NOD32 Antivirus는 POP3S 프로토콜 검사도 지원합니다. 이러한 유형의 통신에서는 암호화

된 채널을 사용하여 서버와 클라이언트 간에 정보를 전송합니다. ESET NOD32 Antivirus는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 암호화 방식을 사용하여 통신을 검사합니다.

POP3S 검사 사용 안 함 - 암호화된 통신을 검사하지 않습니다.

선택한 포트에 POP3S 프로토콜 검사 사용 - POP3S 프로토콜이 사용하는 포트에 정의된 포트에 대해서만 POP3S 검사를 활성화하려면 이 옵션을 선택합니다.

POP3S 프로토콜이 사용하는 포트 - 검사할 POP3S 포트(기본값: 995) 목록입니다.

이메일 경고 및 알림

이 기능에 대한 옵션은 **고급 설정의 웹 및 이메일 > 이메일 클라이언트 보호 > 경고 및 알림**에서 사용할 수 있습니다.

이메일을 검사한 후에 검사 결과가 포함된 알림을 메시지에 추가할 수 있습니다. **받아서 읽은 이메일에 태그 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. 사용할 수 있는 옵션은 다음과 같습니다.

- **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.

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.

이메일 클라이언트 통합

현재 지원되는 이메일 클라이언트로는 [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#), [Windows Live Mail](#) 등이 있습니다. 이메일 보호는 이러한 프로그램의 플러그인으로 작동합니다. 플러그인의 주된 장점은 사용되는 프로토콜과 무관하다는 점입니다. 이메일 클라이언트는 암호화된 메시지를 받으면 메시지 암호를 해독해 바이러스 검사기로 보냅니다. 지원되는 이메일 클라이언트, 해당 버전에 대한 전체 목록은 [ESET 지식 베이스 문서](#)를 참조하십시오.

Microsoft Outlook 도구 모음

Microsoft Outlook 보호는 플러그인 모듈로 작동합니다. ESET NOD32 Antivirus를 설치하면 안티바이러스/안티스팸 포함된 도구 모음이 Microsoft Outlook에 추가됩니다.

ESET NOD32 Antivirus - ESET NOD32 Antivirus의 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 [이메일 클라이언트 보호](#)를 참조하십시오.

검사기 설정 - [이메일 클라이언트 보호](#) 설정 옵션을 표시합니다.

Outlook Express 및 Windows Mail 도구 모음

Outlook Express 및 Windows Mail 보호는 플러그인 모듈로 작동합니다. ESET NOD32 Antivirus를 설치하면 안티바이러스/안티스팸 포함된 도구 모음이 Outlook Express 또는 Windows Mail에 추가됩니다.

ESET NOD32 Antivirus - ESET NOD32 Antivirus의 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 [이메일 클라이언트 보호](#)를 참조하십시오.

검사기 설정 - [이메일 클라이언트 보호](#) 설정 옵션을 표시합니다.

사용자 인터페이스

모양 사용자 지정 - 이메일 클라이언트의 도구 모음 모양을 수정할 수 있습니다. 이메일 프로그램 파라미터와 관계없이 모양을 사용자 지정하려면 이 옵션의 선택을 취소합니다.

텍스트 표시 - 아이콘에 대한 설명을 표시합니다.

텍스트를 오른쪽으로 - 옵션 설명의 위치를 아래쪽에서 아이콘의 오른쪽으로 이동합니다.

큰 아이콘 - 메뉴 옵션의 큰 아이콘을 표시합니다.

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 NOD32 Antivirus 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.

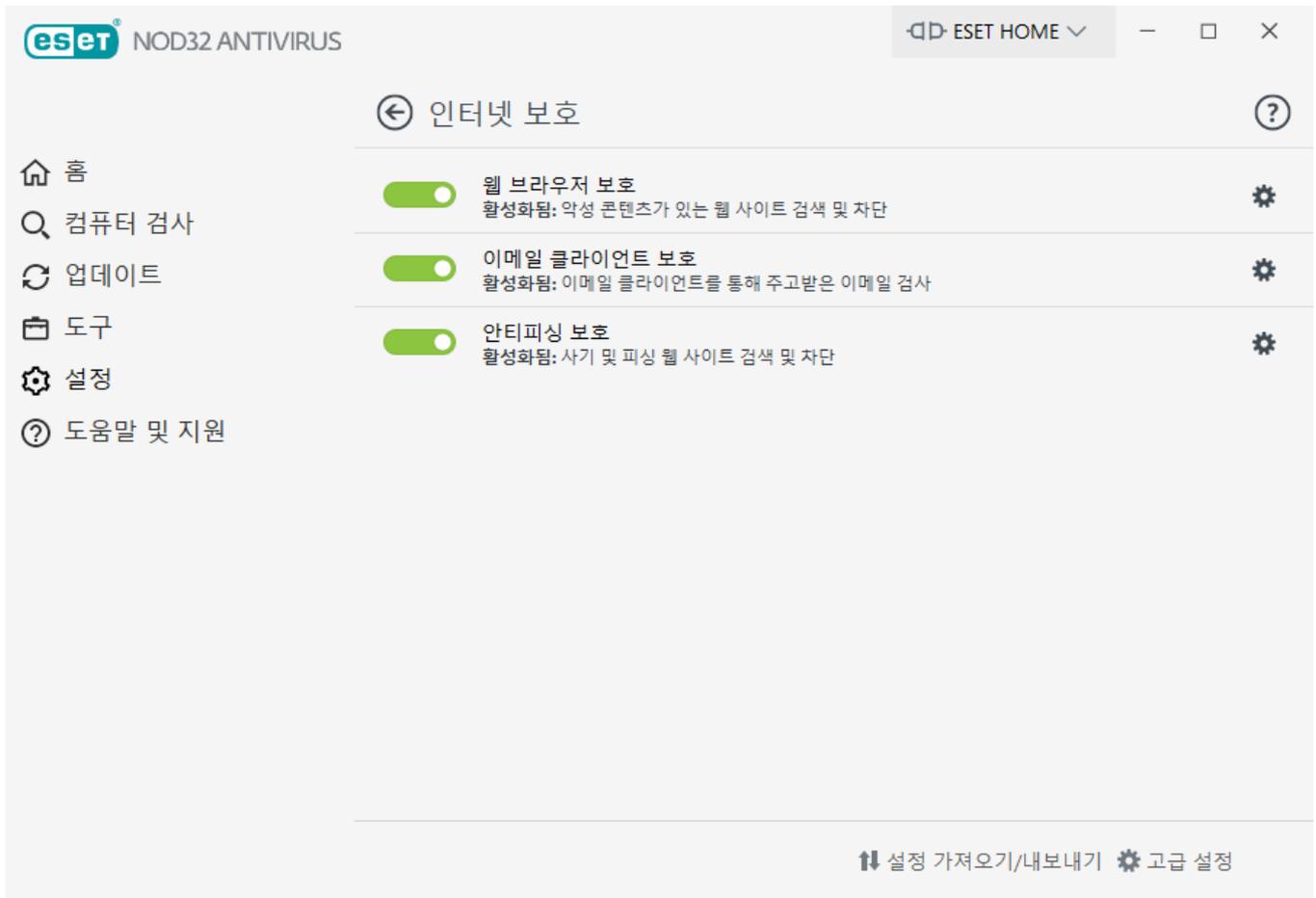
이미 검사한 메시지 다시 검사 확인란을 선택하면 이전에 검사한 메시지를 다시 검사할 수 있습니다.

웹 브라우저 보호

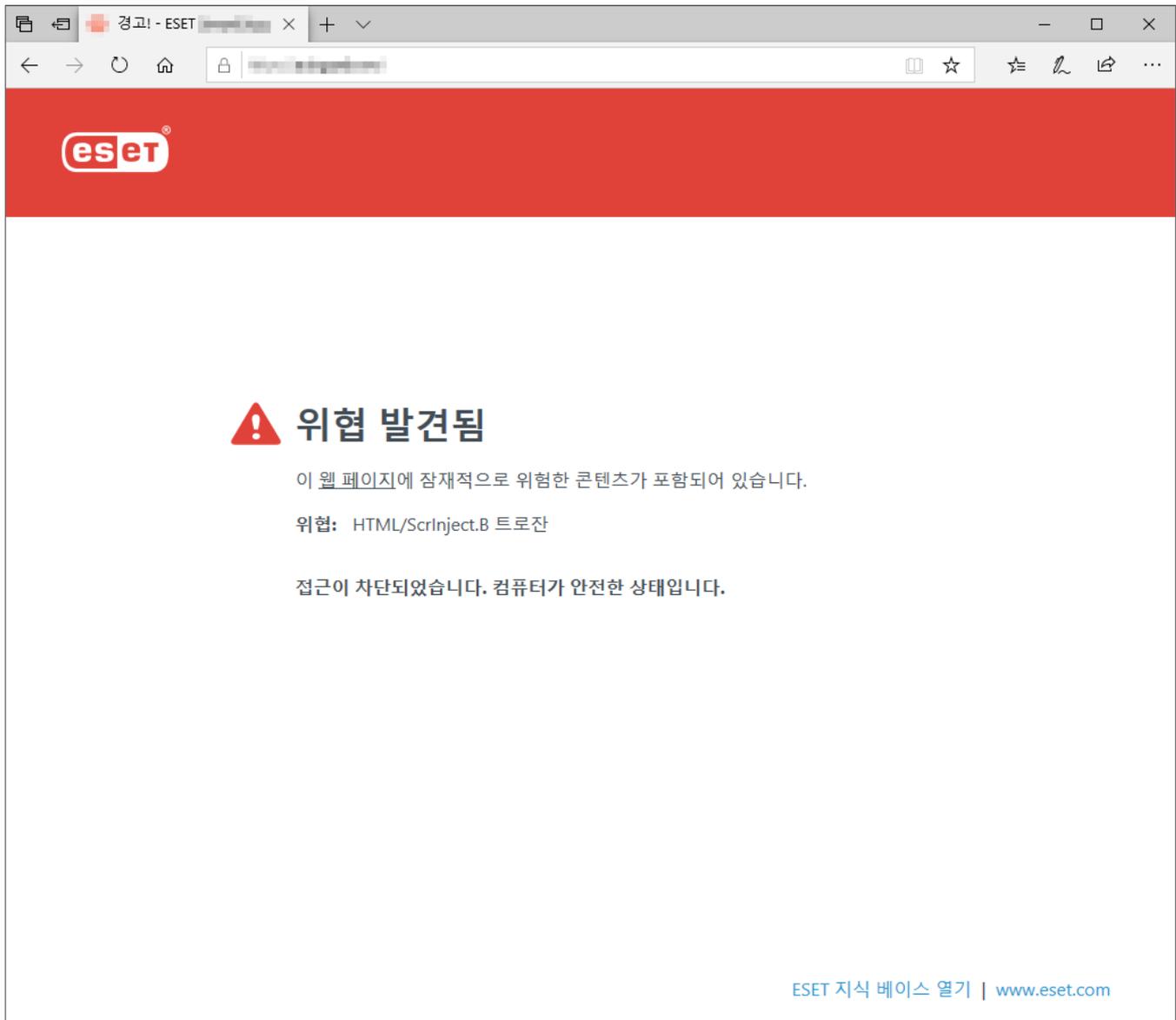
인터넷 연결은 PC의 표준 기능입니다. 그러나 안타깝게도 인터넷 연결은 악성 코드를 전송하는 기본 미디어가 되었습니다. 웹 브라우저 보호는 웹 브라우저와 원격 서버 간의 통신을 모니터링하는 방식으로 작동하며, HTTP(Hypertext Transfer Protocol) 및 HTTPS(암호화된 통신) 규칙을 따릅니다.

악성 콘텐츠가 있는 것으로 알려진 웹 페이지의 접근은 콘텐츠가 다운로드되기 전에 차단됩니다. 다른 모든 웹 페이지는 로드 시 ThreatSense 검사 엔진에서 검사되어 악성 콘텐츠가 검출되면 차단됩니다. 웹 브라우저 보호는 두 가지 수준의 보호 즉, 차단 목록에 의한 차단 및 콘텐츠에 의한 차단 기능을 제공합니다.

웹 브라우저 보호를 활성화하는 것이 좋습니다. 이 옵션은 [기본 프로그램 창](#) > **설정** > **인터넷 보호** > **웹 브라우저 보호**에서 접근할 수 있습니다.



웹 브라우저 보호는 웹 사이트가 차단될 때 브라우저에 다음 메시지를 표시합니다.

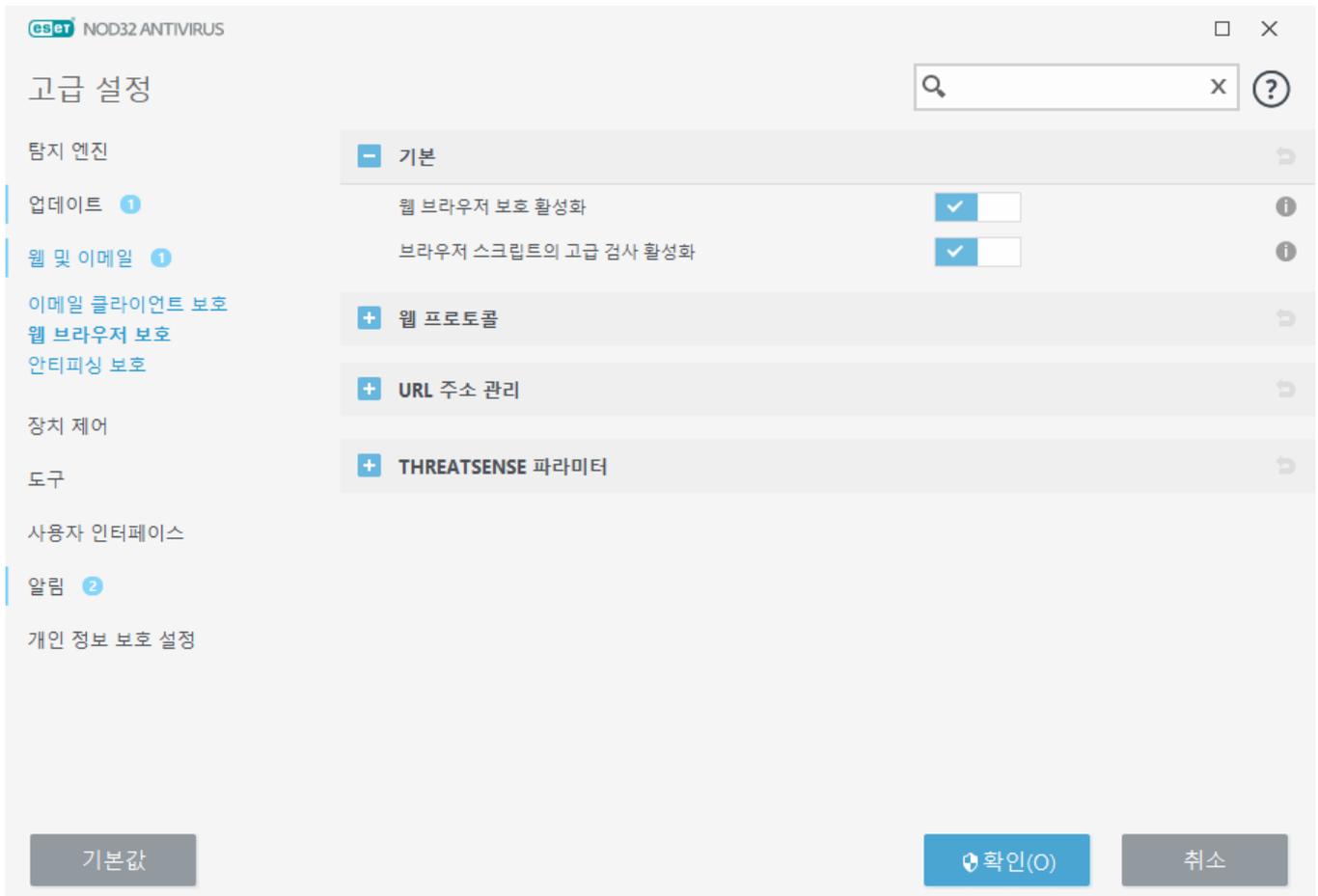


그림이 포함된 지침

- i** 다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.
- [안전한 웹 사이트를 웹 브라우저 보호에 의한 차단에서 제외](#)
 - [ESET NOD32 Antivirus\(를\) 사용하여 웹 사이트 차단](#)

고급 설정(F5 키) > 웹 및 이메일 > 웹 브라우저 보호에서 다음과 같은 옵션을 사용할 수 있습니다.

- **기본** - 고급 설정에서 이 기능을 활성화하거나 비활성화합니다.
- **웹 프로토콜** - 대부분의 인터넷 브라우저에서 사용되는 이러한 표준 프로토콜에 대한 모니터링을 구성할 수 있습니다.
- **URL 주소 관리** - 검사에서 차단, 허용 또는 제외할 URL 주소를 지정할 수 있습니다.
- **ThreatSense 파라미터** - 고급 바이러스 검사기 설정 - 웹 브라우저 보호 등의 검사할 오브젝트 유형(이메일, 압축파일 등), 검출 방법 등의 설정을 구성할 수 있습니다.



웹 브라우저 보호 고급 설정

고급 설정(F5) > 웹 및 이메일 > 웹 브라우저 보호 > 기본에서 다음과 같은 옵션을 사용할 수 있습니다.

웹 브라우저 보호 활성화 - 비활성화하면 [웹 브라우저 보호](#) 및 [안티피싱 보호](#)가 실행되지 않습니다. 이 옵션은 SSL/TLS 프로토콜 필터링이 활성화된 경우에만 사용할 수 있습니다.

브라우저 스크립트의 고급 검사 활성화 - 활성화하면 웹 브라우저로 실행된 모든 JavaScript 프로그램을 탐지 엔진에서 검사합니다.

i 웹 브라우저 보호를 활성화된 상태로 두는 것이 좋습니다.

웹 프로토콜

기본적으로 ESET NOD32 Antivirus는 대부분의 인터넷 브라우저에서 사용되는 HTTP 프로토콜을 모니터링하도록 구성됩니다.

HTTP 검사기 설정

HTTP 트래픽은 항상 모든 애플리케이션의 모든 포트에서 모니터링됩니다.

HTTPS 검사기 설정

ESET NOD32 Antivirus에서는 HTTPS 프로토콜 검사도 지원합니다. HTTPS 통신에서는 암호화된 채널을 사용하여 서버와 클라이언트 간에 정보를 전송합니다. ESET NOD32 Antivirus에서는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 프로토콜을 사용하여 통신을 검사합니다. 이 프로그램은 운영 체제 버전과 관계없이 **HTTPS 프로토콜에서 사용되는 포트에 정의된 포트 (443, 0-65535)의 트래픽만 검사합니다.**

암호화된 통신은 기본적으로 검사됩니다. 검사기 설정을 보려면, 고급 설정 > **웹 및 이메일** > **SSL/TLS**를 엽니다.

URL 주소 관리

URL 주소 관리 섹션에서는 콘텐츠 검사에서 차단, 허용 또는 제외할 HTTP 주소를 지정할 수 있습니다.

HTTPS 웹 페이지 외에 HTTP 주소도 필터링하려면 **SSL/TLS 프로토콜 필터링 활성화**를 선택해야 합니다. 그렇지 않으면 방문한 HTTPS 사이트의 도메인만 추가되고 전체 URL은 추가되지 않습니다.

차단된 주소 목록의 웹 사이트는 허용된 주소 목록에도 포함되지 않는 한 접근할 수 없습니다. 콘텐츠 검사에서 제외된 주소 목록의 웹 사이트는 접근 시 악성 코드가 있는지 검사되지 않습니다.

활성 허용된 주소 목록에 있는 주소를 제외하고 모든 HTTP 주소를 차단하려면 활성 차단된 주소 목록에 *를 추가합니다.

목록에서 특수 기호 *(별표) 및 ?(물음표)를 사용할 수 있습니다. 별표는 모든 문자열을 대체하고 물음표는 모든 기호를 대체합니다. 제외된 주소 목록에는 신뢰할 수 있고 안전한 주소만 포함되어야 하므로 제외된 주소를 지정할 때는 특히 주의해야 합니다. 마찬가지로 이 목록에서 * 및 ? 기호가 올바르게 사용되는지 확인해야 합니다. 모든 하위 도메인을 비롯한 전체 도메인을 안전하게 일치시키는 방법은 **HTTP 주소/도메인 마스크 추가**를 참조하십시오. 목록을 활성화하려면 **목록 활성화**를 선택합니다. 현재 목록에서 주소를 입력할 때 알림을 받으려면 **적용 시 알림**을 선택합니다.

신뢰할 수 있는 도메인

i 웹 및 이메일 > **SSL/TLS** > 신뢰할 수 있는 도메인과의 통신 제외 설정이 활성화되어 있고 도메인이 신뢰할 수 있는 것으로 간주되는 경우 주소가 필터링되지 않습니다.

주소 목록 ?

Q

목록 이름	주소 유형	목록 설명
허용된 주소 목록	허용됨	
차단된 주소 목록	차단됨	
콘텐츠 검사에서 제외된 주소 목록	발견된 악성코드가 무시됨	

추가 편집 삭제
가져오기 내보내기

허용된 주소 목록에 포함된 주소를 제외한 모든 URL을 차단하려면 차단된 주소 목록에 와일드카드(*)를 추가하십시오.

확인(O)
취소

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.

URL 주소 목록

이 섹션에서는 검사에서 차단, 허용 또는 제외할 HTTP 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.

주소 목록 ?

목록 이름	주소 유형	목록 설명
허용된 주소 목록	허용됨	
차단된 주소 목록	차단됨	
콘텐츠 검사에서 제외된 주소 목록	발견된 악성코드가 무시됨	

추가 편집 삭제 가져오기 내보내기

허용된 주소 목록에 포함된 주소를 제외한 모든 URL을 차단하려면 차단된 주소 목록에 와일드카드(*)를 추가하십시오.

확인(O) 취소

그림이 포함된 지침

i 다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.

- [안전한 웹 사이트를 웹 브라우저 보호에 의한 차단에서 제외](#)
- [ESET Windows 휴 제품을 사용하여 웹 사이트 차단](#)

자세한 내용은 [URL 주소 관리](#)를 참조하십시오.

새 URL 주소 목록 생성

이 섹션에서는 검사에서 차단, 허용 또는 제외할 URL 주소/마스킹 목록을 지정할 수 있습니다.

새 목록을 생성할 때 다음과 같은 옵션을 구성하는 데 사용할 수 있습니다.

주소 목록 유형 - 다음과 같은 세 가지 목록 유형을 사용할 수 있습니다.

- **검사에서 제외됨** - 이 목록에 추가된 주소에 대해서는 악성 코드 검사를 수행하지 않습니다.
- **차단됨** - 사용자는 이 목록에 지정된 주소에 접근할 수 없습니다.
- **허용됨** - [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.

목록 이름 - 목록 이름을 지정합니다. 이 필드는 미리 정의된 세 목록 중 하나를 편집할 때 회색으로 표시됩니다.

목록 설명 - 목록에 대한 간단한 설명을 입력합니다(옵션). 미리 정의된 세 목록 중 하나를 편집할 때 회색으로 표시됩니다.

목록을 활성화하려면 해당 목록 옆의 **목록 활성화**를 선택합니다. 방문한 HTTP 사이트 평가에 특정 목록이 사용될 경우 알림을 받으려면 **적용 시 알림**을 선택합니다. 예를 들어 웹 사이트가 차단된 주소 목록이나 허용된 주소 목록에 포함되어 있어 차단되거나 허용되는 경우 알림이 발생합니다. 이 알림에는 지정된 웹 사이트를 포함하는 목록의 이름이 포함됩니다.

제어 요소

추가 - 목록에 새 URL 주소를 추가합니다(여러 값은 분리 기호를 사용하여 입력).

편집 - 목록의 기존 주소를 수정합니다. **추가**를 사용하여 생성한 주소에 대해서만 가능합니다.

제거 - 목록에서 기존 주소를 삭제합니다. **추가**를 사용하여 생성한 주소에 대해서만 가능합니다.

가져오기 - URL 주소가 포함된 파일을 가져옵니다(줄 바꿈으로 값이 구분됨, 예: 인코딩 UTF-8을 사용하는 *.txt).

URL 마스크 추가 방법

원하는 주소/도메인 마스크로 들어가기 전에 이 대화 상자의 지침을 참조하십시오.

ESET NOD32 Antivirus에서는 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.

맨 앞의 "*" 시퀀스는 도메인 이름 앞에 사용될 경우 특수하게 취급됩니다. 첫째, 이 경우에는 *와 일드카드가 슬래시 문자('/')와 일치하지 않습니다. 이를 통해 마스크 회피를 방지할 수 있습니다. 예를 들어 마스크 *.domain.com은 <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 마스크 *.domain.com은 <http://domain.com>과도 일치합니다. *domain.com을 사용하면 <http://anotherdomain.com>과도 일치하게 되므로 올바르지 않습니다.

안티피싱 보호

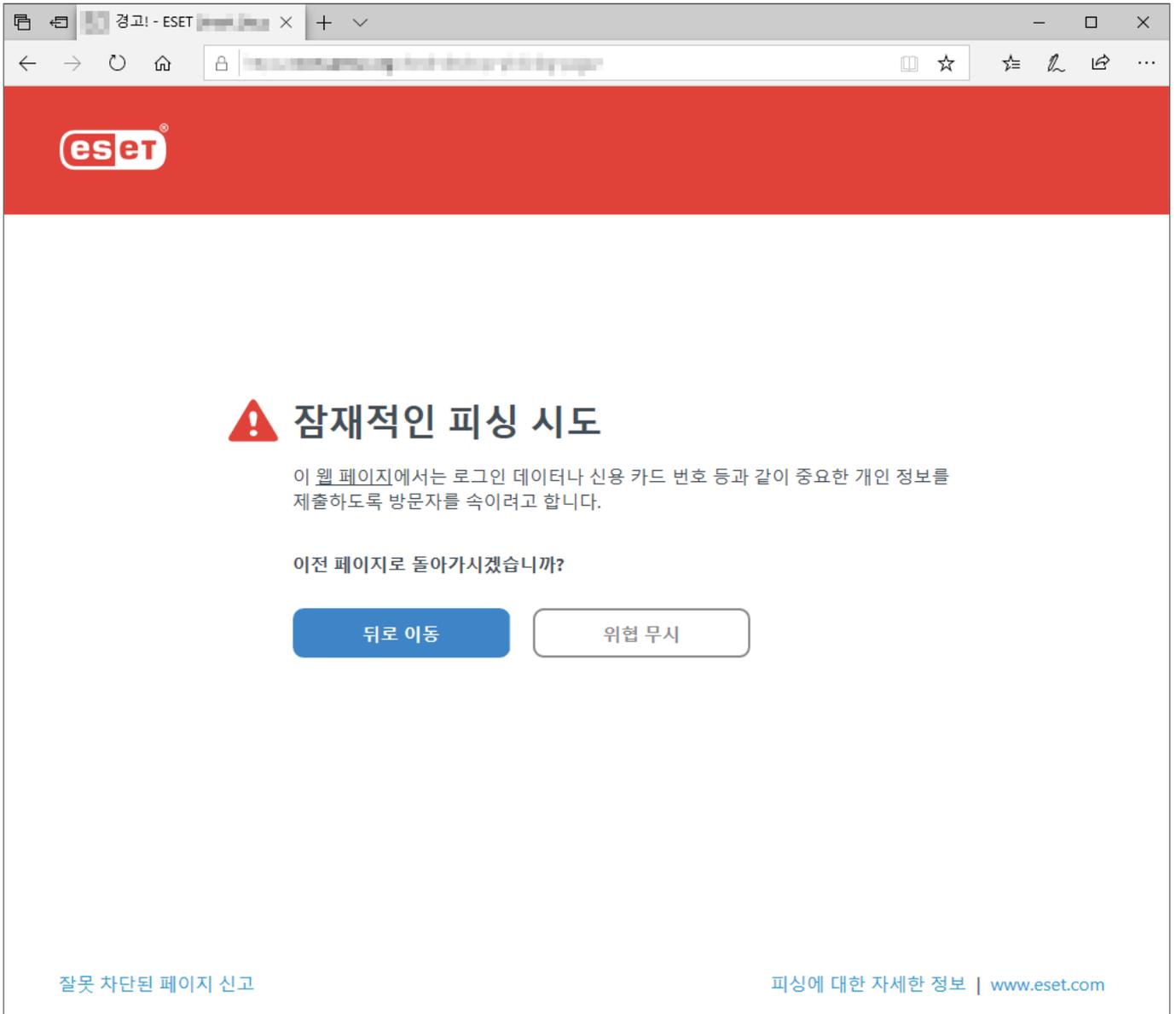
피싱이라는 용어는 사회 공학(기밀 정보를 얻기 위해 사용자를 조종하는 방법)을 사용한 범죄 행위를 의미합니다. 피싱은 종종 은행 계좌 번호, PIN 코드 등과 같은 중요한 데이터에 접근하기 위해 사용됩니다. 이러한 활동에 대한 자세한 내용은 [용어집](#)을 참조하십시오. ESET NOD32 Antivirus에는 안티피싱 보호 기능이 포함되어 이러한 유형의 콘텐츠를 배포하는 것으로 알려진 웹 페이지를 차단합니다.

ESET NOD32 Antivirus에서 안티피싱을 활성화할 것을 강력히 권장합니다. 이렇게 하려면 **고급 설정(F5)**을 열고 **웹 및 이메일 > 안티피싱 보호**로 이동하십시오.

ESET NOD32 Antivirus의 안티피싱 보호에 대한 자세한 내용을 보려면 [지식 베이스 문서](#)를 참조하십시오.

피싱 웹 사이트 접근

인식된 피싱 웹 사이트에 접근하면 웹 브라우저에 다음 대화 상자가 나타납니다. 계속해서 이 웹 사이트에 접근하려면 **위험 무시(권장되지 않음)**를 클릭합니다.



i 허용 목록에 포함된 잠재적인 피싱 웹 사이트는 기본적으로 몇 시간 후에 만료됩니다. 웹 사이트를 영구히 허용하려면 [URL 주소 관리](#) 도구를 사용합니다. **고급 설정(F5)**에서 **웹 및 이메일 > 웹 브라우저 보호 > URL 주소 관리 > 주소 목록**을 확장하고 **편집**을 클릭한 후 편집하려는 웹 사이트를 목록에 추가하십시오.

피싱 사이트 보고

보고 링크에서는 분석을 위해 ESET으로 피싱/악성 웹 사이트를 보고할 수 있습니다.

i 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 신고](#)할 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.

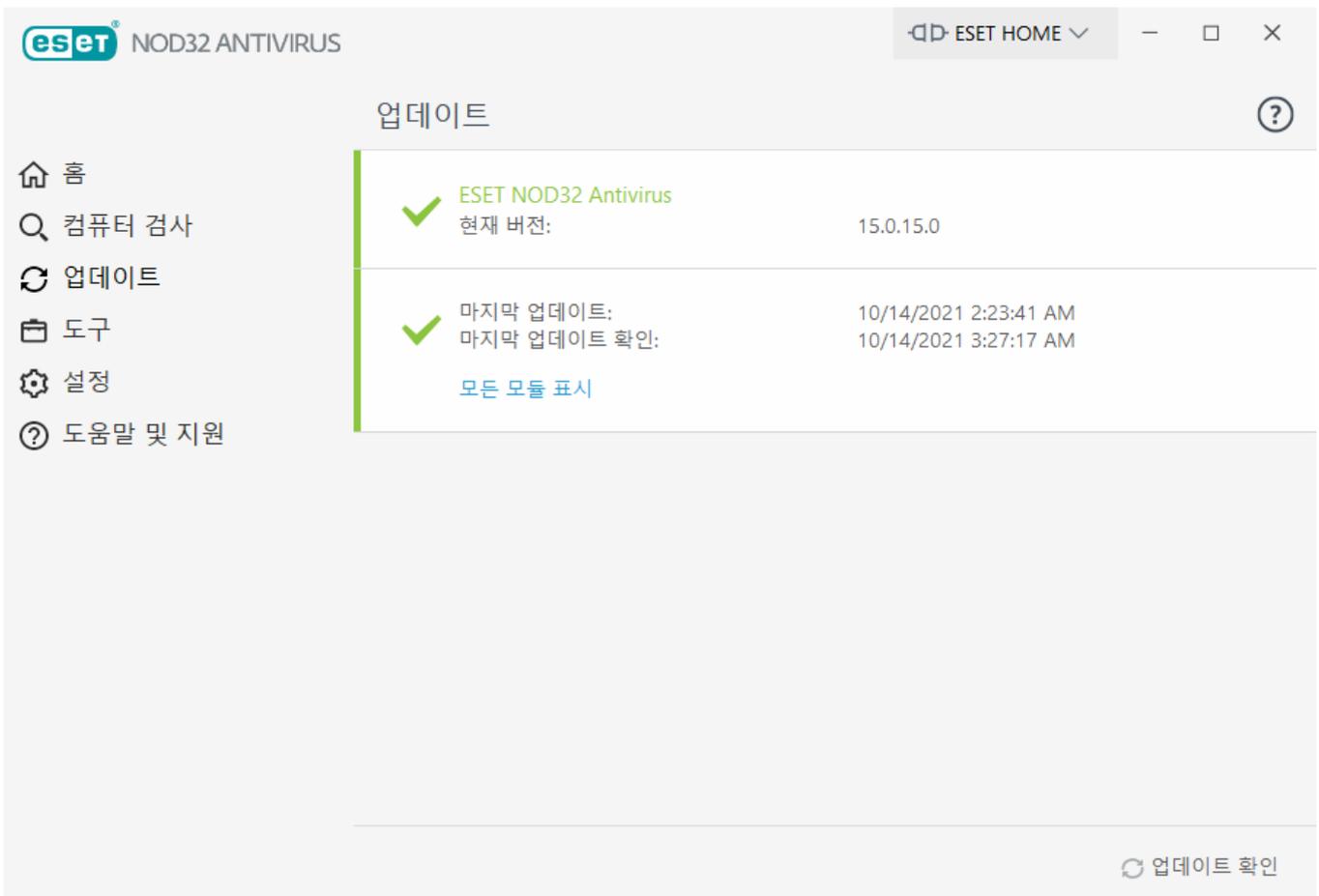
프로그램 업데이트

컴퓨터의 보안 수준을 최대로 유지하기 위한 가장 좋은 방법은 ESET NOD32 Antivirus를 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 업데이트뿐만 아니라 **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. 설치하는 동안 이와 같이 하지 않은 경우 업데이트할 때 ESET 업데이트 서버에 접근하려면 라이선스 키를 입력하여 제품을 활성화하면 됩니다.

i 라이선스 키는 ESET NOD32 Antivirus 구매 후 ESET에서 이메일로 보내 드립니다.



현재 버전 – 설치한 현재 제품 버전의 버전 번호를 표시합니다.

마지막으로 성공한 업데이트 – 마지막으로 성공한 업데이트 날짜를 표시합니다. 최근 날짜가 없으면 제품 모듈이 최신 버전이 아닐 수 있습니다.

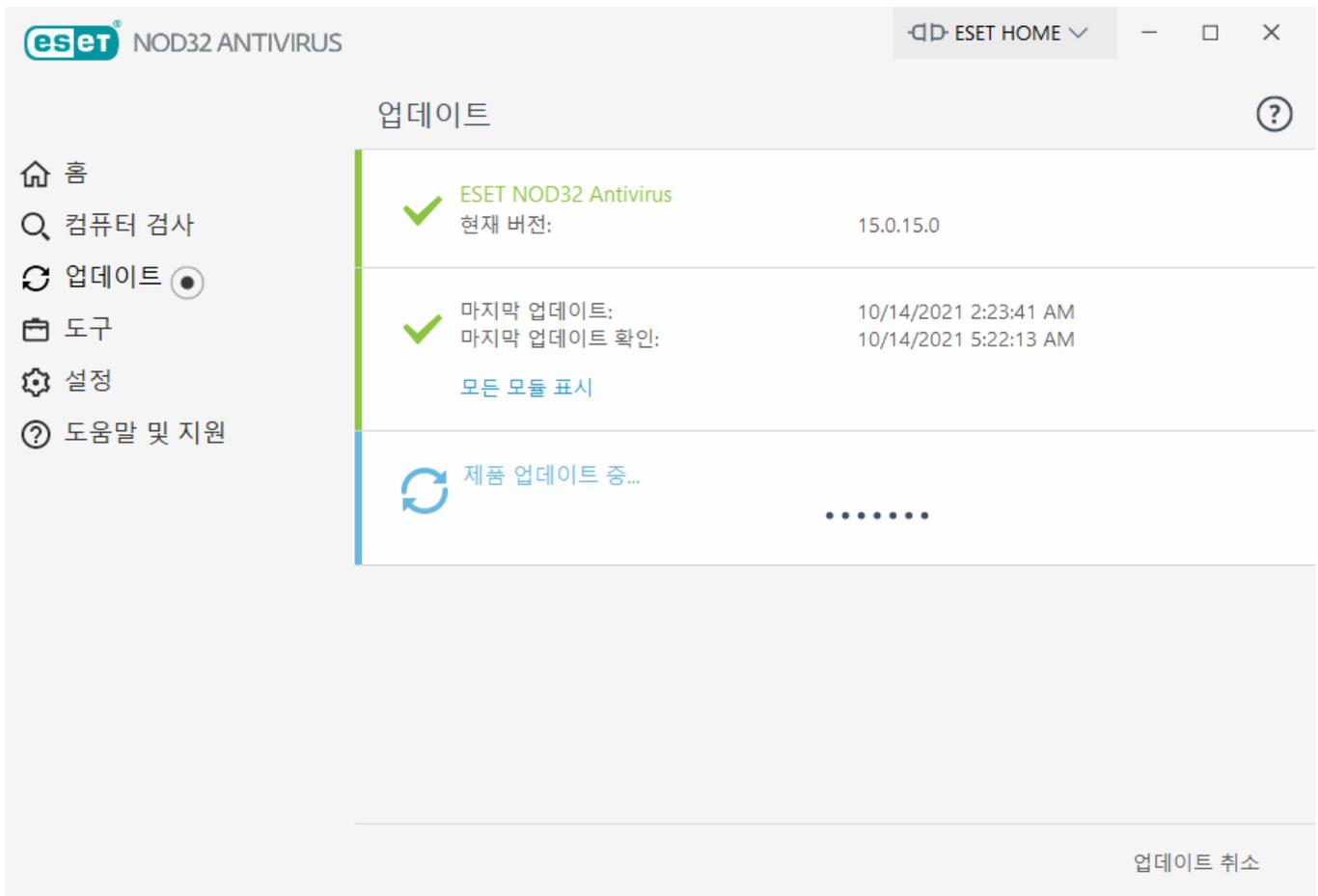
마지막으로 성공한 업데이트 확인 – 마지막으로 성공한 업데이트 확인 날짜를 표시합니다.

모든 모듈 표시 – 설치된 프로그램 모듈의 목록을 표시합니다.

사용 가능한 ESET NOD32 Antivirus의 최신 버전을 검색하려면 **업데이트 확인**을 클릭합니다.

업데이트 프로세스

업데이트 확인을 클릭하면 다운로드가 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.

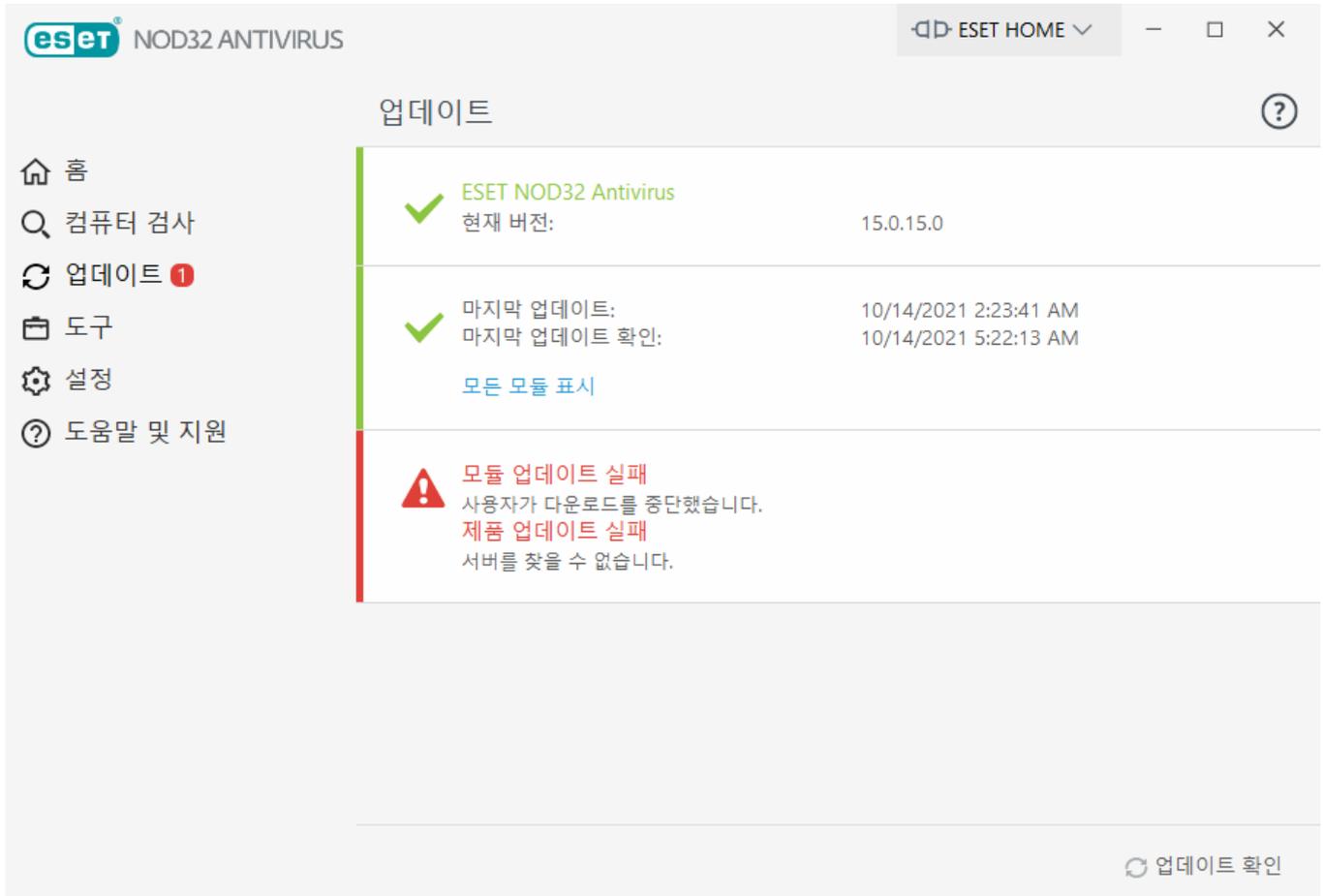
실패한 업데이트

실패한 모듈 업데이트 메시지를 받은 경우 다음과 같은 문제가 원인일 수 있습니다.

1. 잘못된 라이선스 – 활성화에 사용된 라이선스가 잘못되었거나 만료되었습니다. [기본 프로그램](#)

랜 창에서 **도움말 및 지원 > 라이선스 변경**을 클릭하고 새 라이선스 키를 입력합니다.

2. **업데이트 파일을 다운로드하는 동안 오류가 발생했습니다.** - 이 오류는 잘못된 [인터넷 연결 설정](#)으로 인해 발생할 수 있습니다. 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. 활성 인터넷 연결이 없는 경우 ISP(인터넷 서비스 공급자)에 문의하십시오.



모든 프로그램 모듈이 올바르게 업데이트되도록 ESET NOD32 Antivirus 업데이트에 성공한 후에는 컴퓨터를 최신 제품 버전으로 다시 시작하는 것이 좋습니다. 정기적인 모듈 업데이트 후에는 컴퓨터를 다시 시작할 필요가 없습니다.

i 자세한 내용은 "[모듈 업데이트 실패](#)" 메시지에 대한 문제 해결을 참조하십시오.

업데이트 설정

설정 업데이트 옵션은 **고급 설정** 트리(F5 키)의 **업데이트 > 기본**에서 사용할 수 있습니다. 이 섹션에서는 사용되는 업데이트 서버 및 이러한 서버에 대한 인증 데이터와 같은 업데이트 소스 정보를 지정합니다.

기본

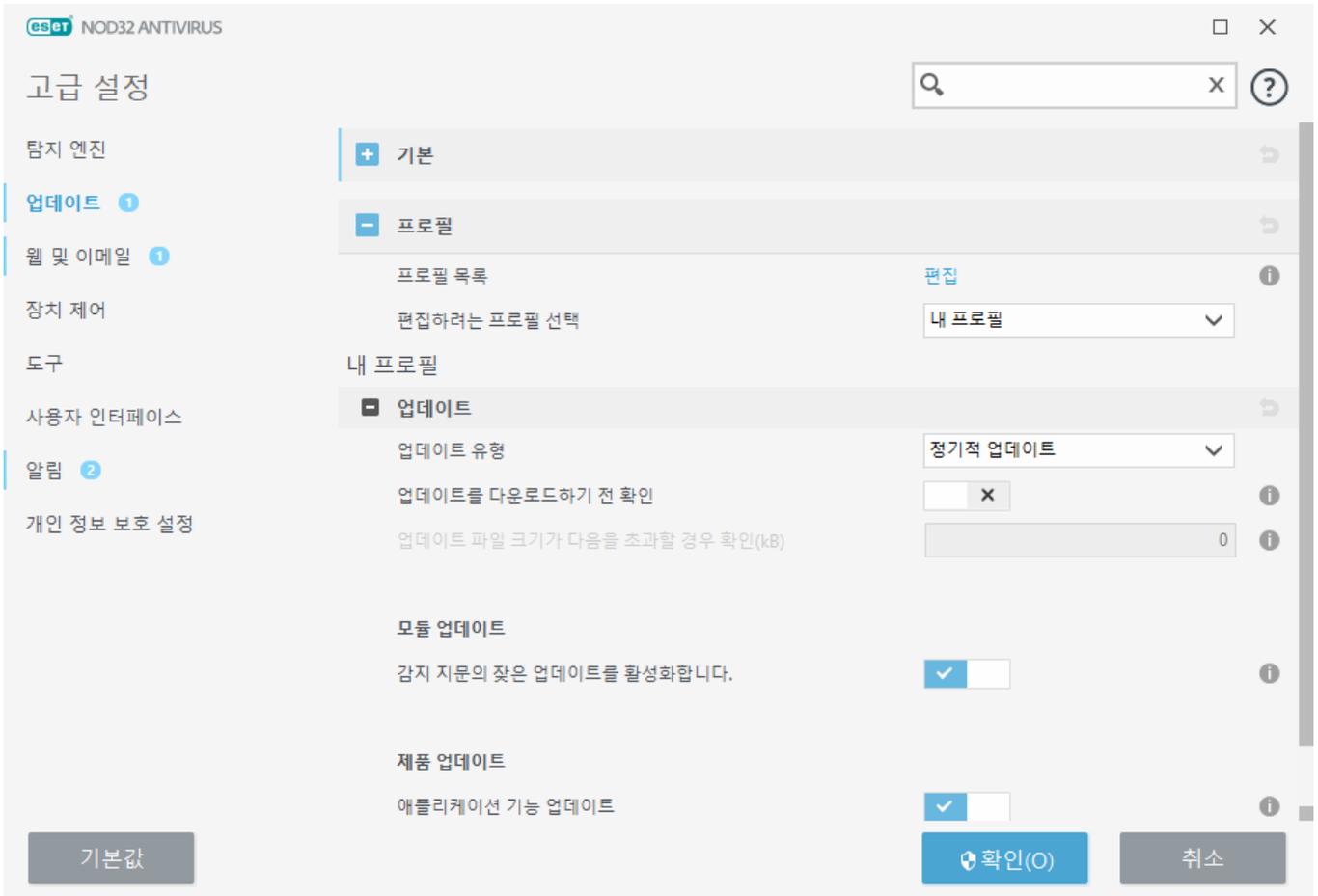
현재 사용 중인 업데이트 프로파일(특정 프로파일의 **고급 설정 > 방화벽 > 알려진 네트워크**에서 설정된 경우는 제외)이 **기본 업데이트 프로파일 선택** 드롭다운 메뉴에 표시됩니다.

새 프로파일을 생성하려면 [업데이트 프로파일](#) 섹션을 참조하십시오.

탐지 엔진 또는 모듈 업데이트를 다운로드하려고 할 때 문제가 발생하는 경우 **지우기**를 클릭하여 임시 업데이트 파일/캐시를 지웁니다.

모듈 롤백

검색 엔진 및/또는 프로그램 모듈의 새 업데이트가 불안정하거나 손상되었다고 의심되면 [이전 버전으로 롤백](#)한 후 설정된 기간에 대해 업데이트를 비활성화할 수 있습니다.



업데이트를 제대로 다운로드하려면 모든 업데이트 파라미터를 올바르게 입력해야 합니다. 방화벽을 사용하는 경우에는 ESET 프로그램이 인터넷과 통신(예: HTTP 통신)할 수 있는지 확인합니다.

- 프로파일

다양한 업데이트 구성 및 작업을 위해 프로파일 업데이트를 생성할 수 있습니다. 프로파일 업데이트를 생성하는 경우 정기적으로 변경되는 인터넷 연결 속성에 대한 대체 프로파일이 필요한 모바일 사용자에게 특히 유용합니다.

편집할 프로필 선택 드롭다운 메뉴에는 현재 선택한 프로필이 표시되는데, 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.

업데이트를 다운로드하기 전 확인 - 프로그램에서 업데이트 파일 다운로드를 확인할 것인지, 거절할 것인지 선택할 수 있는 알림이 표시됩니다.

업데이트 파일 크기가 다음을 초과할 경우 확인(KB) - 업데이트 파일 크기가 지정된 값보다 큰 경우 프로그램에서 확인 대화 상자를 표시합니다. 업데이트 파일 크기를 0KB로 설정하면 프로그램에서 항상 확인 대화 상자를 표시합니다.

성공한 업데이트에 대한 알림 비활성화 - 화면 오른쪽 아래의 시스템 트레이 알림을 해제합니다. 전체 화면 애플리케이션이나 게임을 실행 중인 경우 이 옵션을 선택하는 것이 유용합니다. 게이머 모드는 모든 알림을 해제합니다.

모듈 업데이트

감지 지문의 잦은 업데이트 활성화 - 감지 지문이 더 짧은 간격으로 업데이트됩니다. 이 설정을 비활성화하면 감지 속도에 부정적인 영향을 미칠 수도 있습니다.

프로그램 구성 요소 업데이트

애플리케이션 업데이트 - 재설치해야 하는 경우 확인 대화 상자가 표시됩니다.

- 연결 옵션

프록시 서버를 사용하여 업데이트를 다운로드하려면 [연결 옵션](#) 섹션을 참조하십시오.

업데이트 롤백

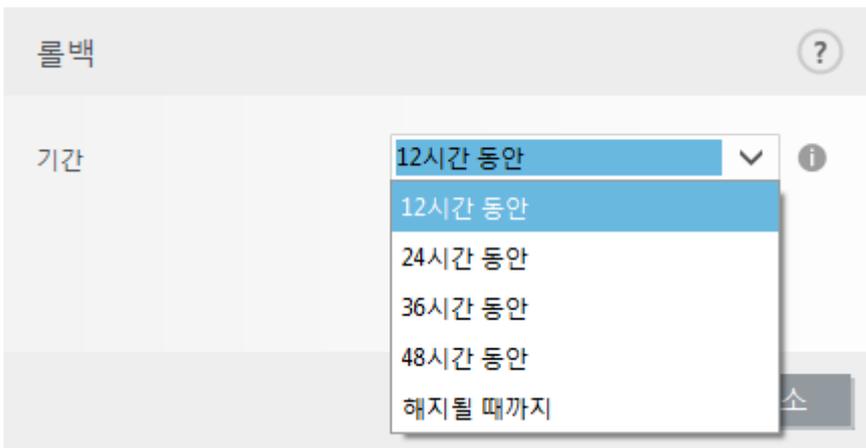
새로운 탐지 엔진 업데이트 또는 프로그램 모듈이 불안정하거나 손상되었을 수 있다고 의심되면 이전 버전으로 롤백한 후 업데이트를 일시적으로 비활성화할 수 있습니다. 또는 업데이트를 무기한 연기한 경우 이전에 비활성화한 업데이트를 활성화할 수 있습니다.

ESET NOD32 Antivirus에서는 롤백 기능과 함께 사용할 수 있는 탐지 엔진 및 프로그램 모듈의 스

냅shots을 기록합니다. 바이러스 DB 스냅shots을 생성하려면 **모듈의 스냅shots 생성**이 활성화된 상태로 유지합니다. **모듈의 스냅shots 생성**이 활성화된 경우 첫 번째 업데이트 중에 첫 번째 스냅shots이 생성됩니다. 다음 스냅shots은 48시간 후에 생성됩니다. **로컬에 저장된 스냅shots 수** 필드는 저장된 탐지 엔진 스냅shots의 수를 정의합니다.

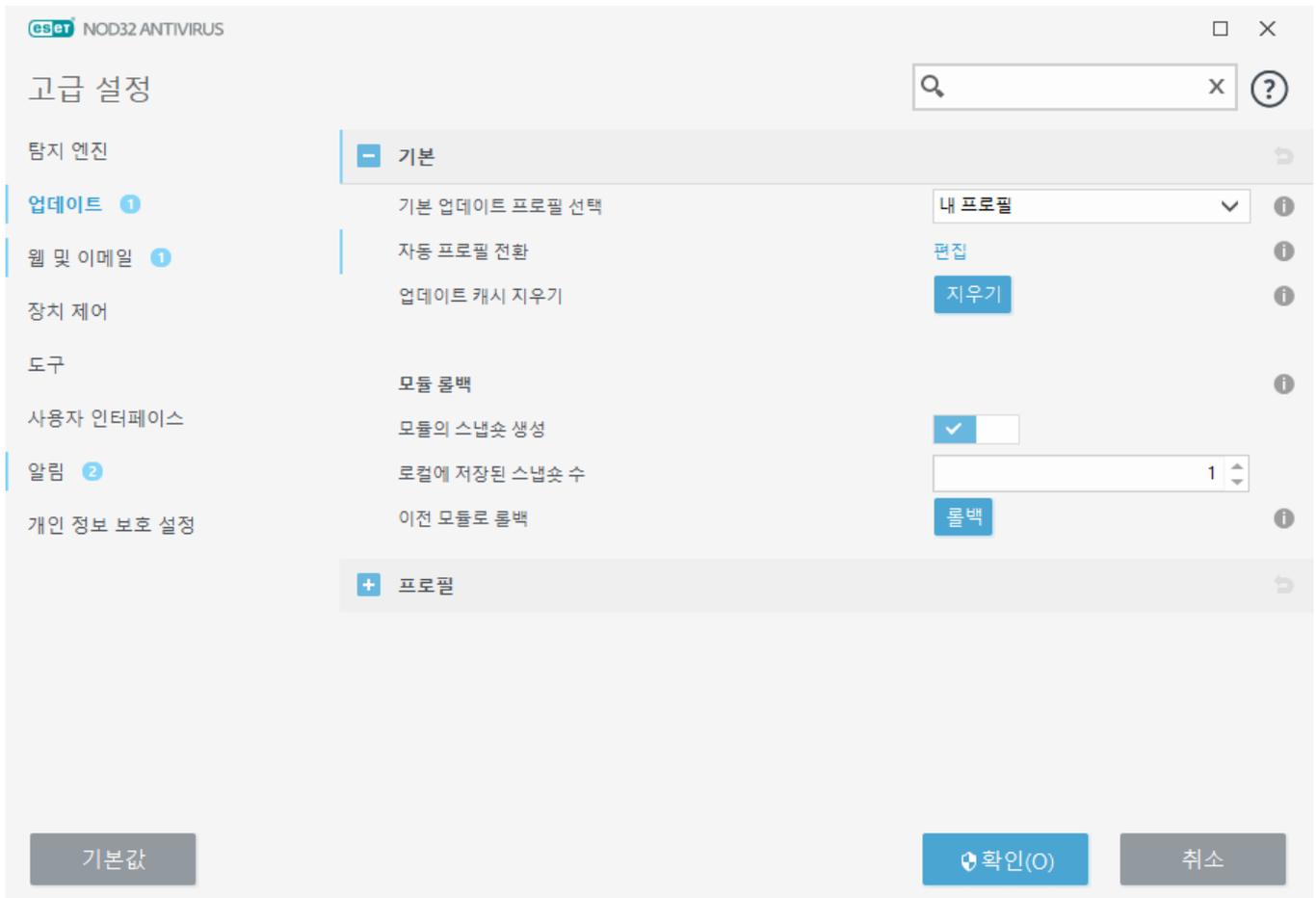
i 최대 스냅shots 수(예: 세 개)에 도달하면 가장 오래된 스냅shots이 48시간마다 새 스냅shots으로 대체됩니다. ESET NOD32 Antivirus에서는 가장 오래된 스냅shots으로 탐지 엔진 및 프로그램 모듈 업데이트 버전을 롤백합니다.

롤백(고급 설정(F5 키) > 업데이트 > 기본)을 클릭한 경우 검색 엔진 및 프로그램 모듈 업데이트가 일시 중지되는 기간을 나타내는 시간 간격을 **기간** 드롭다운 메뉴에서 선택해야 합니다.



업데이트 기능을 수동으로 복원할 때까지 정기 업데이트를 무기한 연기하려면 **해지될 때까지**를 선택합니다. 잠재적 보안 위험을 나타내므로 ESET에서는 이 옵션을 선택하는 것을 권장하지 않습니다.

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 스냅shots으로 저장됩니다.



✓ 22700이 최신 탐지 엔진 버전 번호이고, 22698과 22696이 탐지 엔진 스냅샷으로 저장되었다고 가정합니다. 22697은 사용할 수 없습니다. 이 예에서는 22697 업데이트 중에 컴퓨터가 꺼졌고, 22697을 다운로드하기 전에 최신 업데이트가 제공되었습니다. **로컬에 저장된 스냅샷 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.

롤백 시간 간격

롤백(고급 설정(F5 키) > 업데이트 > 기본)을 클릭한 경우 검색 엔진 및 프로그램 모듈 업데이트가 일시 중지되는 기간을 나타내는 시간 간격을 **기간** 드롭다운 메뉴에서 선택해야 합니다.



업데이트 기능을 수동으로 복원할 때까지 정기 업데이트를 무기한 연기하려면 **해지될 때까지**를 선택합니다. 잠재적 보안 위험을 나타내므로 ESET에서는 이 옵션을 선택하는 것을 권장하지 않습니다.

프로그램 구성 요소 업데이트

프로그램 구성 요소 업데이트 섹션에는 프로그램 구성 요소 업데이트와 관련된 옵션이 있습니다. 새 프로그램 구성 요소 업그레이드를 사용할 수 있는 경우 프로그램의 동작을 미리 정의할 수 있습니다.

프로그램 구성 요소 업데이트는 새로운 기능을 제공하거나 이전 버전에 이미 있었던 기능을 변경합니다. 업그레이드는 사용자 개입 없이 자동으로 수행될 수도 있고, 알림이 표시되도록 선택할 수도 있습니다. 프로그램 구성 요소 업데이트를 설치한 후에는 컴퓨터를 재시작해야 할 수 있습니다.

애플리케이션 업데이트 - 활성화하면 전체 제품 업그레이드가 수행되지 않고 각 프로그램 구성 요소 업그레이드가 자동으로 수행됩니다.

연결 옵션

지정된 업데이트 프로파일에 대한 프록시 서버 설정 옵션에 접근하려면 **고급 설정** 트리(F5 키)에서 **업데이트**를 클릭한 다음 **프로파일 > 업데이트 > 연결 옵션**을 클릭합니다. **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

글로벌 프록시 서버 설정 사용을 선택하면 고급 설정 트리의 **도구 > 프록시 서버** 분기에 이미 지정되어 있는 프록시 서버 구성 옵션을 사용하게 됩니다.

ESET NOD32 Antivirus을(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 NOD32 Antivirus을(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 NOD32 Antivirus이(가) 업데이트를 위해 프록시 서버에 연결하는 경우.
- 컴퓨터가 프록시 서버를 통해 인터넷에 연결되어 있는 경우. 프로그램을 설치하는 동안

Internet Explorer에서 설정을 가져오지만 이러한 설정이 변경된 경우(예: 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.

i 이 섹션에 있는 **사용자 이름** 및 **패스워드** 필드는 프록시 서버에 적용됩니다. 사용자 이름 및 패스워드가 프록시 서버에 접근하는 데 필요한 경우에만 이러한 필드를 완료하십시오. 이러한 필드는 프록시 서버를 통해 인터넷에 접근하기 위해 패스워드가 필요한 경우에만 내용을 입력해야 합니다.

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 NOD32 Antivirus에는 다음과 같은 작업이 활성화됩니다.

- 정기적 자동 업데이트
- 전화 접속 연결 후 자동 업데이트
- 사용자 로그인 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.

시스템 업데이트

몇 가지 운영 체제 업데이트를 사용할 수 있는 경우 ESET NOD32 Antivirus 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.

운영 체제 업데이트 다운로드 및 설치를 시작하려면 **시스템 업데이트 실행**을 클릭합니다.

업데이트 정보

Windows 업데이트에 대한 정보입니다. 이 창의 맨 위에는 업데이트 이름 및 번호가 표시되고 그 다음에 업데이트 순위와 해당 업데이트를 통해 해결된 문제에 대한 설명이 표시됩니다.

도구

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

자세한 내용은 [ESET NOD32 Antivirus의 도구](#)를 참조하십시오.

ESET NOD32 Antivirus의 도구

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

이 메뉴에는 다음 도구가 포함되어 있습니다.

 [로그 파일](#)

 [보안 보고서](#)

 [실행 중인 프로세스](#)(ESET LiveGrid®가 ESET NOD32 Antivirus에서 활성화된 경우)

 [ESET SysInspector](#)

 [ESET SysRescue Live](#) - ESET SysRescue Live .iso CD/DVD 이미지를 다운로드할 수 있는 ESET SysRescue Live 웹 사이트로 리디렉션됩니다.

 [스케줄러](#)

 [시스템 클리너](#) - 위협을 치료한 후 컴퓨터를 사용 가능한 상태로 복원하는 데 도움이 됩니다.

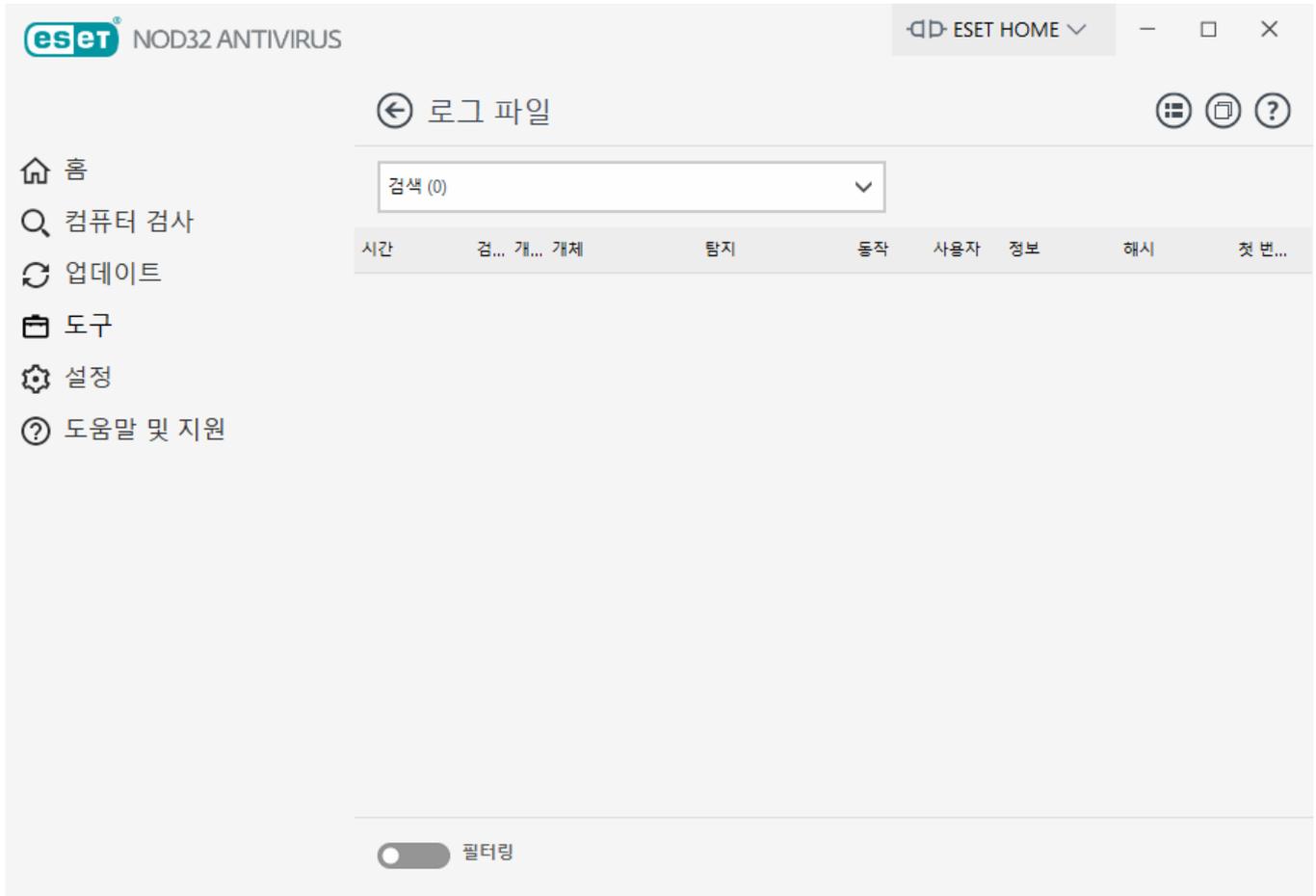
 [분석용 샘플 전송](#) - 분석하기 위해 감염 의심 파일을 ESET 연구소로 전송할 수 있습니다(ESET LiveGrid® 구성에 따라 사용하지 못할 수도 있음).

 [검역소](#)



로그 파일

로그 파일은 발생한 중요 프로그램 이벤트에 대한 정보를 포함하고 있고 검출된 위협에 대한 개요를 제공합니다. 로깅은 시스템 분석, 위협 검출 및 문제 해결에서 중요한 부분입니다. 로깅은 사용자 상호 작용 없이 백그라운드에서 수행됩니다. 정보는 현재 로그 상세 수준 설정에 따라 기록됩니다. ESET NOD32 Antivirus 환경에서 직접 텍스트 메시지 및 로그뿐만 아니라 압축파일 로그를 볼 수 있습니다.



로그 파일은 [기본 프로그램 창](#)에서 **도구 > 로그 파일**을 클릭하여 접근할 수 있습니다. **로그** 드롭다운 메뉴에서 원하는 로그 유형을 선택합니다. 다음과 같은 로그를 사용할 수 있습니다.

- **탐지** - 이 로그는 탐지 및 ESET NOD32 Antivirus에서 탐지된 침입에 대한 자세한 정보를 제공합니다. 로그 정보에는 탐지 시간, 검사기 유형, 개체 유형, 개체 위치, 탐지 이름, 수행된 동작 및 침입 탐지 시 로그인한 사용자 이름, 해시 및 첫 번째 발생 내용이 포함됩니다. 치료되지 않은 침입은 항상 열린 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 NOD32 Antivirus에서 수행된 중요한 모든 동작이 이벤트 로그에 기록됩니다. 이벤트 로그에는 프로그램에서 발생한 이벤트 및 오류에 대한 정보가 포함되어 있습니다. 이 로그는 시스템 관리자 및 사용자가 여기서 찾은 정보를 통해 프로그램에서 발생한 문제에 대한 해결책을 찾을 수 있도록 도움을 주기 위해 고안되었습니다.
- **컴퓨터 검사** - 모든 완료된 수동 검사 또는 계획 검사의 결과가 이 창에 표시됩니다. 각 행은 단일 컴퓨터 제어에 해당됩니다. 각 검사의 상세 정보를 보려면 항목을 두 번 클릭합니다.

로그 필터링

다음에서 **필터링**을 클릭하여 **도구 > 로그 파일** 필터링 기준을 정의합니다.

로그 필터링 기능은 특히 레코드가 많은 경우, 정보를 찾는 데 도움이 됩니다. 예를 들어 특정 유형

의 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 소문자 사용이 중요하다면 이 옵션을 활성화합니다. 필터링/검색 옵션을 구성한 다음 **확인**을 클릭하여 필터링된 로그 레코드를 표시하거나 **찾기**를 클릭하여 검색을 시작합니다. 로그 파일은 현재 위치(강조 표시된 레코드)에서 시작해 위에서 아래로 검색됩니다. 해당하는 첫 번째 레코드를 찾으면 검색이 중지됩니다. **F3**을 눌러 다음 레코드를 검색하거나 오른쪽 마우스 버튼 메뉴에서 **찾기**를 선택해 검색 옵션을 구체화합니다.

로깅 구성

[기본 프로그램](#) 창에서 ESET NOD32 Antivirus의 로깅 구성에 접근할 수 있습니다. **설정 > 고급 설정 > 도구 > 로그 파일**을 클릭합니다. 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.
- **주요** - 심각한 오류(안티바이러스 보호등)만 기록합니다.

i 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 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. 이 프로세스가 진행되는 동안 빈 로그 항목이 모두 제거되어 성능과 로그 처리 속도가 향상됩니다. 이러한 향상은 특히 로그에 포함된 항목 수가 매우 클 경우 관찰할 수 있습니다.

텍스트 프로토콜 활성화를 통해 [로그 파일](#)과 별도로 다른 파일 형식으로 로그를 저장할 수 있습니다.

- **대상 디렉터리** - 로그 파일이 저장되는 디렉터리입니다(텍스트/CSV에만 적용됨). 각 로그 섹션에는 파일 이름이 미리 정의된 고유한 파일이 있습니다(예: 로그를 저장하는 데 일반 텍스트 파일 형식을 사용하는 경우 로그 파일 **탐지** 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.

i 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 지식 베이스](#) 문서를 참조하십시오.

실행 중인 프로세스

실행 중인 프로세스는 컴퓨터에서 실행 중인 프로그램이나 프로세스를 표시하며, ESET이 새로운 침입 정보를 즉각적이고 지속적으로 확인할 수 있도록 해줍니다. ESET NOD32 Antivirus은(는) [ESET LiveGrid®](#) 기술로 사용자를 보호하기 위해 실행 중인 프로세스에 대한 자세한 정보를 제공합니다.

실행 중인 프로세스

이 창에는 ESET LiveGrid®의 추가 정보와 함께 선택한 파일 리스트가 표시됩니다. 사용자 수, 최초 발견 시간과 함께 각 프로세스의 평판이 표시됩니다.

평판	프로세스	PID	사용자 수	검색 시간	응용 프로그램 이름
●●●●●●●●	smss.exe	356	3개월 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	csrss.exe	452	1년 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	wininit.exe	524	1개월 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	services.exe	572	6개월 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	winlogon.exe	616	1개월 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	lsass.exe	660	6개월 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	svchost.exe	748	1년 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	fontdrvhost.exe	760	1개월 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	dwm.exe	980	6개월 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	vboxservice.exe	1412	1년 전	●●●●●●●●	Oracle VM VirtualBox Guest A...
●●●●●●●●	wudfhost.exe	1472	1년 전	●●●●●●●●	Microsoft® Windows® Oper...
●●●●●●●●	spoolsv.exe	2400	1개월 전	●●●●●●●●	Microsoft® Windows® Oper...

경로: c:\windows\system32\smss.exe
 크기: 152.3 kB
 설명: Windows Session Manager
 회사: Microsoft Corporation
 버전: 10.0.19041.1 (WinBuild.160101.0800)
 제품: Microsoft® Windows® Operating System
 생성 날짜: 5/12/2021 12:02:49 AM
 수정 날짜: 5/12/2021 12:02:49 AM

▼ 상세 정보 숨기기

평판 - 대부분의 경우 ESET NOD32 Antivirus 및 ESET LiveGrid® 기술에서는 각 개체의 특성을 파악한 다음 악의적인 활동의 잠재성을 평가하는 일련의 휴리스틱 규칙을 사용하여 개체(파일, 프로세스, 레지스트리 키 등)에 위험 수준을 지정합니다. 이러한 휴리스틱을 기준으로 개체에 1 - 양호(녹색)에서 9 - 위험(빨간색)까지 위험 수준을 지정합니다.

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

i 정상(녹색)으로 표시된 잘 알려진 애플리케이션은 확실히 문제가 없으므로(허용 목록에 표시) 성능이 개선되도록 검색에서 제외됩니다.

PID - 프로세스 식별자 숫자는 프로세스의 우선 순위를 조정하는 등 다양한 함수 호출에서 파라미터로 사용할 수 있습니다.

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

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

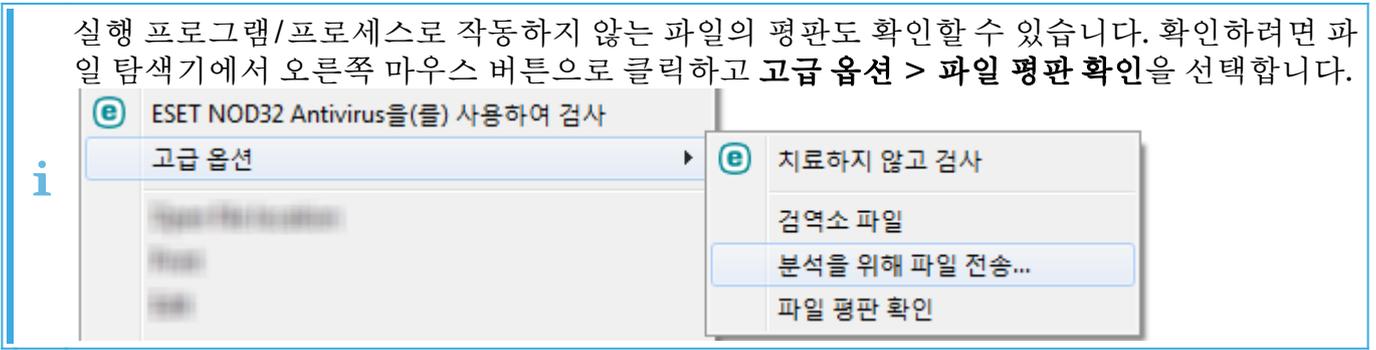
i 알 수 없음(주황색)으로 표시된 애플리케이션이라고 반드시 악성 소프트웨어는 아닙니다. 일반적으로 이 애플리케이션은 새로운 애플리케이션인 경우가 많습니다. 파일에 대해 확신이 서지 않는 경우 ESET 연구소로 [분석을 위해 파일을 전송](#)할 수 있습니다. 이 파일이 악성 애플리케이션으로 확인되면 향후 업데이트에 해당 검출 정보가 추가됩니다.

애플리케이션 이름 - 프로그램 또는 프로세스의 지정된 이름입니다.

애플리케이션을 클릭하여 해당 애플리케이션의 다음 세부 정보를 표시합니다.

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

실행 프로그램/프로세스로 작동하지 않는 파일의 평판도 확인할 수 있습니다. 확인하려면 파일 탐색기에서 오른쪽 마우스 버튼으로 클릭하고 **고급 옵션 > 파일 평판 확인**을 선택합니다.



보안 보고서

이 기능은 다음 범주에 대한 통계 개요를 제공합니다.

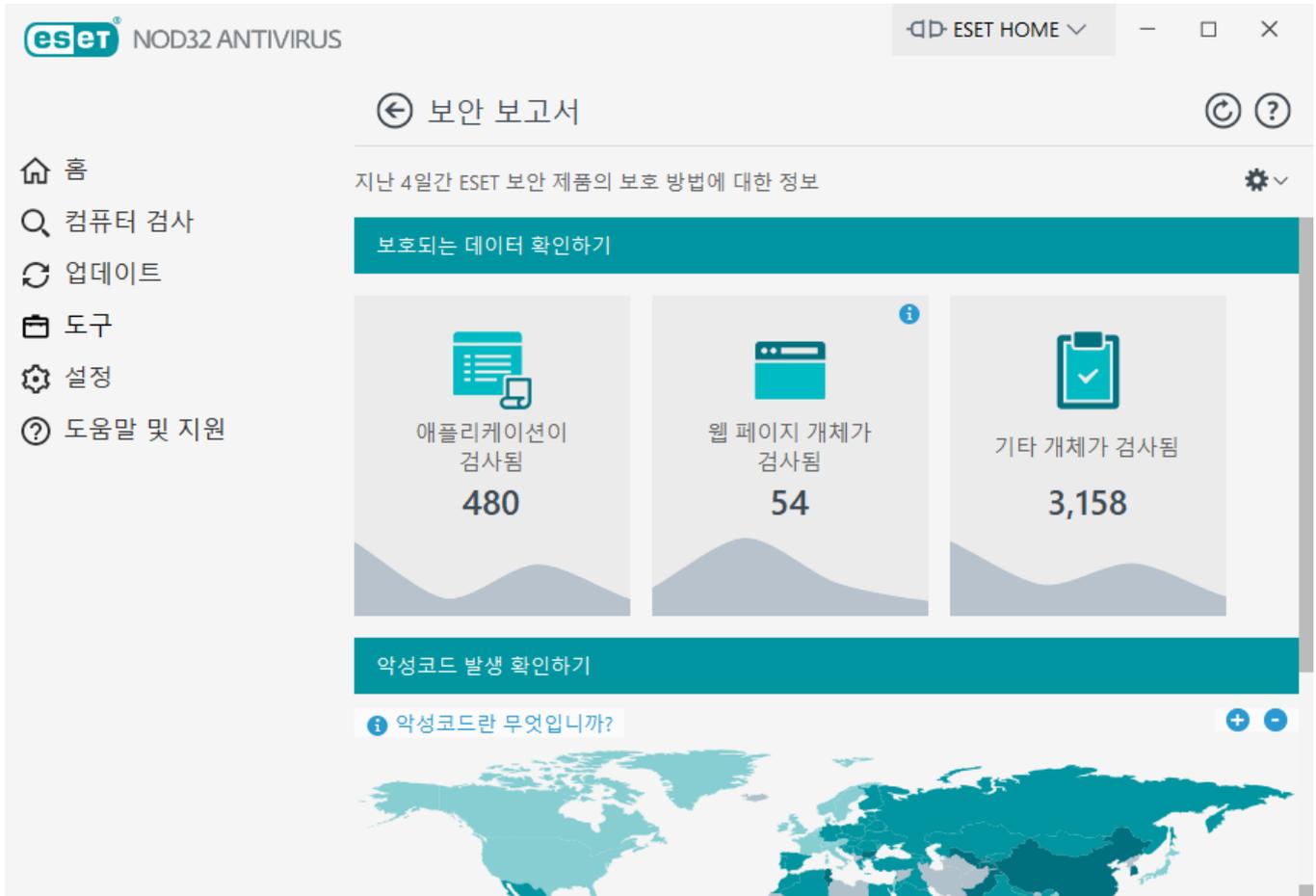
- **차단된 웹 페이지** – 차단된 웹 페이지의 수를 표시합니다(PUA의 차단 목록 URL, 피싱, 해킹된 라우터, IP 또는 인증서).
- **감염된 이메일 개체가 탐지됨** – 탐지된 감염 이메일 **개체** 수를 표시합니다.
- **PUA가 감지됨** - PUA(**사용자가 원치 않는 애플리케이션**) 수를 표시합니다.
- **문서가 검사됨** – 검사된 문서 개체 수를 표시합니다.
- **애플리케이션이 검사됨** – 검사된 실행 파일 개체 수를 표시합니다.
- **기타 개체가 검사됨** – 검사된 기타 개체 수를 표시합니다.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

범주 아래에서는 세계 지도에 표시된 실제 바이러스 상황을 볼 수 있습니다. 각 국가에 바이러스가 있으면 색으로 구분됩니다(색이 진할수록 수치가 높은 것임). 데이터가 없는 국가는 회색으로 표시됩니다. 국가 위로 마우스를 가져가면 선택한 국가의 데이터가 표시됩니다. 특정 대륙을 선택하면 자동으로 확대/축소됩니다.

기능이 활성화되면 보안 보고서에서 더 이상 작동하지 않는 상태로 표시되지 않습니다.

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 NOD32 Antivirus를 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 > 사용자 인터페이스 > 경고 및 메시지 상자 > 확인 메시지에서 통계를 다시 설정하기 전 확인 옵션을 선택 취소한 경우를 제외하고는 항상 이 동작을 확인해야 합니다.

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 SysInspector의 온라인 사용자 설명서도 참조하십시오.](#)

SysInspector 창에는 생성된 로그에 대한 다음과 같은 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** - 생성된 로그를 엽니다. 지정된 로그 파일을 오른쪽 마우스 버튼으로 클릭한 후 오른쪽 마우스 버튼 메뉴에서 **표시**를 선택할 수도 있습니다.
- **비교** - 기존의 두 로그를 비교합니다.
- **생성** - 새 로그를 생성합니다. 로그에 접근하기 전에 ESET SysInspector가 완료(로그 상태가 "생성됨"으로 표시됨)될 때까지 기다리십시오.
- **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).
- **비교** - 기존의 두 로그를 비교합니다.
- **생성** - 새 로그를 생성합니다. 로그에 접근하기 전에 ESET SysInspector가 완료(로그 상태가 "생성됨"으로 표시됨)될 때까지 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 NOD32 Antivirus [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 업데이트 모듈, 검사 작업, 시스템 시작 파일 검사 및 로그 유지 관리와 같은 작업을 예약할 수 있습니다. 기본 스케줄러 창의 아래쪽에서 **작업 추가** 또는 **삭제**를 클릭하여 작업을 직접 추가하거나 삭제할 수 있습니다. **기본값**을 클릭하여 예약된 작업 목록을 기본값으로 되돌리고 모든 변경 사항을 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 로그인 후 자동 업데이트
- 자동 시작 파일 검사(사용자 로그인 후)
- 자동 시작 파일 검사(검색 엔진 업데이트 후)

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

The screenshot shows the '스케줄러' (Scheduler) window in ESET NOD32 ANTIVIRUS. The window title is 'ESET HOME'. On the left, there is a navigation menu with icons for Home, Computer Scan, Update, Tools, Settings, and Help. The main area displays a table of tasks with columns for '작업' (Task), '이름' (Name), '트리거' (Trigger), '다음 실행' (Next Run), and '마지막 실행' (Last Run). Below the table are buttons for '작업 추가(A)', '편집(E)', '삭제(D)', and '기본값(E)'.

작업	이름	트리거	다음 실행	마지막 실행
<input checked="" type="checkbox"/>	로그 유지 관리	로그 유지 관리	작업이 매일 2:00:00 AM... 10/15/2021 2:00:00 AM	10/14/2021 2:01:00 AM
<input checked="" type="checkbox"/>	업데이트	정기적 자동 업데이트	작업이 60분마다에 반복... 10/14/2021 4:27:46 AM	10/14/2021 3:27:46 AM
<input checked="" type="checkbox"/>	업데이트	전화 접속 연결 후 자동 ...	인터넷/VPN에 전화 접... 이벤트가 트리거됨	
<input type="checkbox"/>	업데이트	사용자 로그인 후 자동 ...	사용자 로그인 시 (최대 ... 이벤트가 트리거됨	
<input checked="" type="checkbox"/>	시스템 시작 파일 ...	자동 시작 파일 검사	사용자 로그인 시 컴퓨터... 이벤트가 트리거됨	10/14/2021 3:50:47 AM
<input checked="" type="checkbox"/>	시스템 시작 파일 ...	자동 시작 파일 검사	모듈 업데이트 완료 시 (... 이벤트가 트리거됨	10/14/2021 3:50:38 AM

새 작업 추가

1. 창 아래쪽의 **작업 추가**를 클릭합니다.
2. 작업 이름을 입력합니다.
3. 풀다운 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 로그인 시 실행할 수 있는 파일을 검사합니다.
- **컴퓨터 상태 스냅샷 생성** - [ESET SysInspector](#) 컴퓨터 스냅샷을 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.

4. 작업을 활성화하려면 **활성화됨** 옆의 슬라이더 막대를 클릭하고(나중에 예약된 작업 목록에서 확인란을 선택/선택 취소하여 이렇게 할 수 있음), **다음**을 클릭한 후 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)

오른쪽 마우스 버튼을 클릭하고 **작업 상세 정보 표시**를 클릭하면 예약된 작업을 검토할 수 있습니다.

작업 이름

로그 유지 관리

작업 유형

로그 유지 관리

작업 실행

작업이 매일 3:00:00 AM에 실행됩니다.

지정된 시간에 작업이 실행되지 않을 경우 수행할 동작

최대한 빨리

확인

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.

i 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 진행률](#)도 참조하십시오.

예약된 작업 개요

사용자 지정 작업을 두 번 클릭하거나, 사용자 지정 스케줄러 작업을 오른쪽 마우스 버튼으로 클릭하고 **작업 상세 정보** 표시를 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 로그인 시 실행할 수 있는 파일을 검사합니다.
- **컴퓨터 상태 스냅샷 생성** - [ESET SysInspector](#) 컴퓨터 스냅샷을 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 로그인
- 위협 검출

이벤트에 의해 트리거된 작업을 예약하면 두 작업 완료 간 최소 간격을 지정할 수 있습니다. 예를 들어, 하루에 여러 번 컴퓨터에 로그인하는 경우 하루 중 처음으로 로그인할 때에만 작업을 수행하

고 다음 날도 동일한 패턴으로 작업을 수행하려면 24시간을 선택합니다.

건너뛰기 작업

컴퓨터가 배터리 전원으로 실행되거나 전원이 차단된 경우 작업을 건너뛸 수 있습니다. 다음 옵션 중에서 작업을 실행할 시기를 선택하고 다음을 클릭합니다.

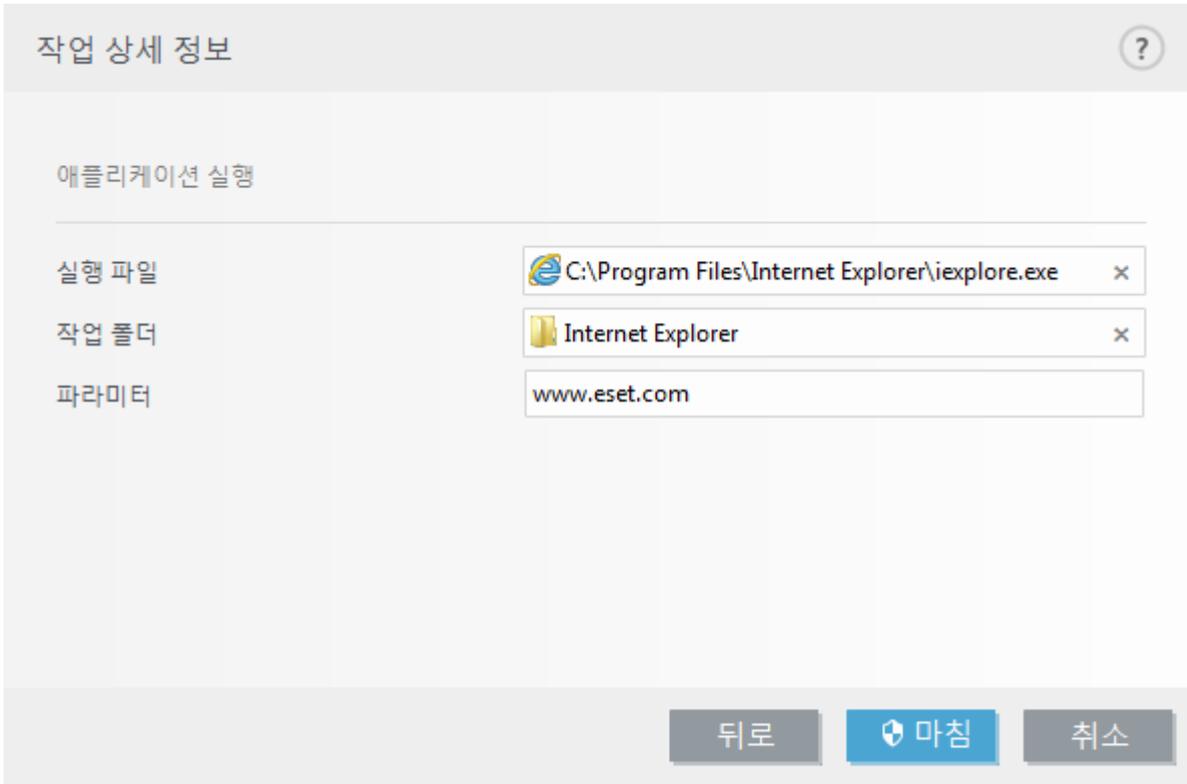
- 다음 예약 시간에
- 최대한 빨리
- 마지막으로 예약된 실행 이후 시간이 초과하는 경우 즉시(시간)

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 사용자가 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 디렉터를 정의합니다. 선택한 **실행 파일**의 모든 임시 파일이 이 디렉터리 내에 생성됩니다.

파라미터 - 애플리케이션의 명령줄 파라미터입니다(옵션).

작업을 적용하려면 **마침**을 클릭합니다.

시스템 클리너

시스템 클리너는 위협을 치료한 후 컴퓨터를 사용 가능한 상태로 복원하는 데 도움이 되는 도구입니다. 맬웨어는 레지스트리 편집기, 작업 관리자 또는 Windows 업데이트와 같은 시스템 유틸리티를 비활성화할 수 있습니다. 시스템 클리너는 기본값과 단 한 번의 클릭에 지정된 시스템 설정을 복원합니다.

시스템 클리너는 다음의 다섯 가지 설정 범주에서 문제를 보고합니다.

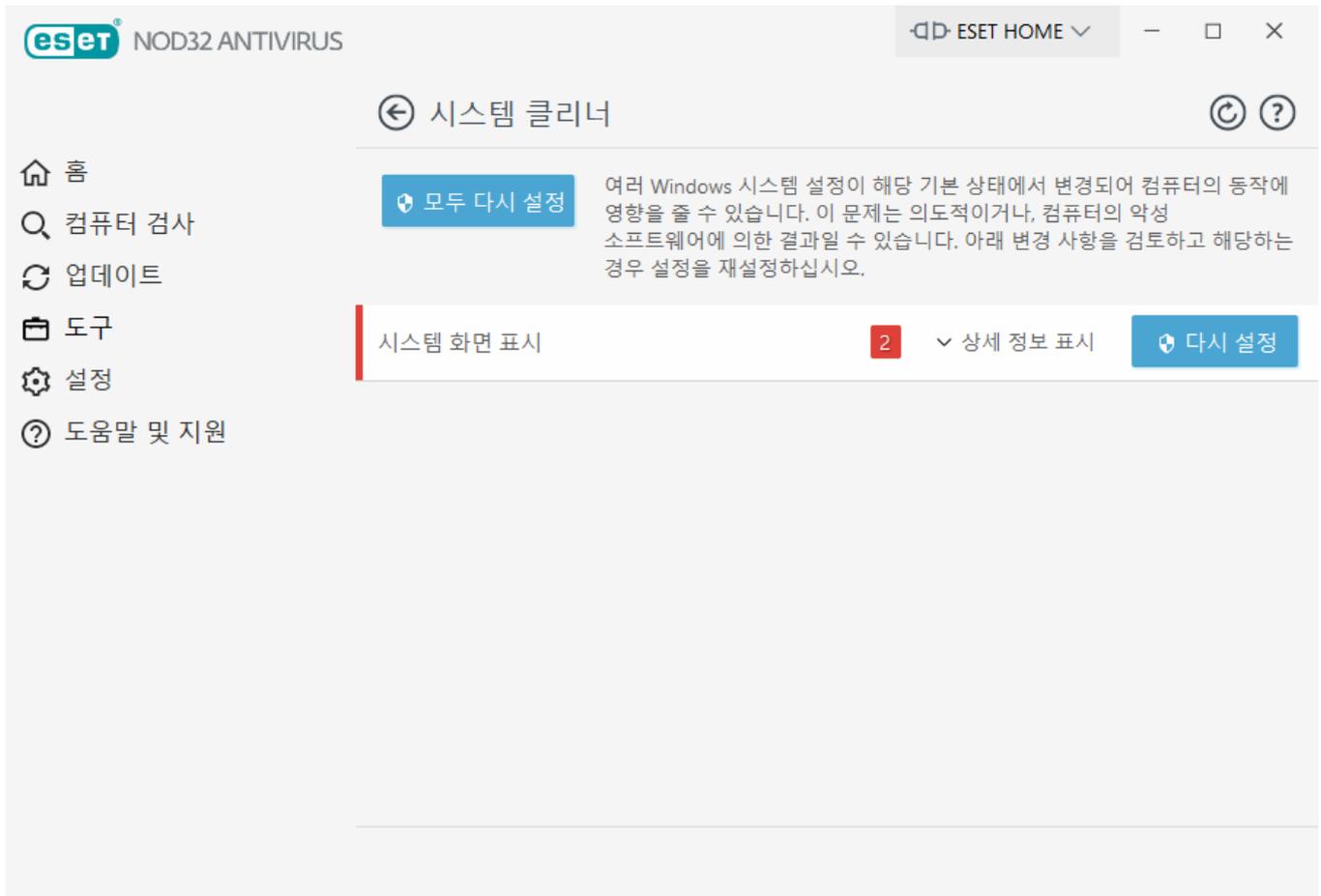
- **보안 설정:** Windows Update 등과 같이 컴퓨터 취약성을 증가시킬 수 있는 설정의 변경 사항
- **시스템 설정:** 파일 연결 등과 같이 컴퓨터 동작을 변경할 수 있는 시스템 설정 변경의 변경 사항
- **시스템 화면 표시:** 바탕 화면 배경 무늬 등과 같이 시스템 외관에 영향을 주는 설정
- **비활성화된 기능:** 비활성화되어 있을 수 있는 중요한 기능과 애플리케이션

- **Windows 시스템 복원:** 시스템을 이전 상태로 되돌릴 수 있는 Windows 시스템 복원 기능에 대한 설정

다음과 같은 경우 시스템 치료를 요청할 수 있습니다.

- 위협이 발견된 경우
- 사용자가 **다시 설정**을 클릭한 경우

변경 내용을 검토하고 해당하는 경우 설정을 다시 지정할 수 있습니다.



i 관리자 권한이 있는 사용자만 시스템 클리너에서 작업을 수행할 수 있습니다.

ESET SysRescue Live

ESET SysRescue Live는 부팅 가능한 복구 CD/DVD 또는 USB 드라이브를 생성할 수 있는 무료 유틸리티입니다. 복구 미디어에서 감염된 컴퓨터를 부팅하여 악성코드를 검사하고 감염된 파일을 치료할 수 있습니다.

ESET SysRescue Live는 호스트 운영 체제와 독립적으로 실행되지만 디스크 및 파일 시스템에 직접 접근할 수 있다는 것이 가장 큰 장점입니다. 따라서 정상적인 운영 조건에서는 제거하지 못할 수도 있는 위협을 제거할 수 있습니다(예: 운영 체제가 실행 중인 경우 등).

- [ESET SysRescue Live 온라인 도움말](#)

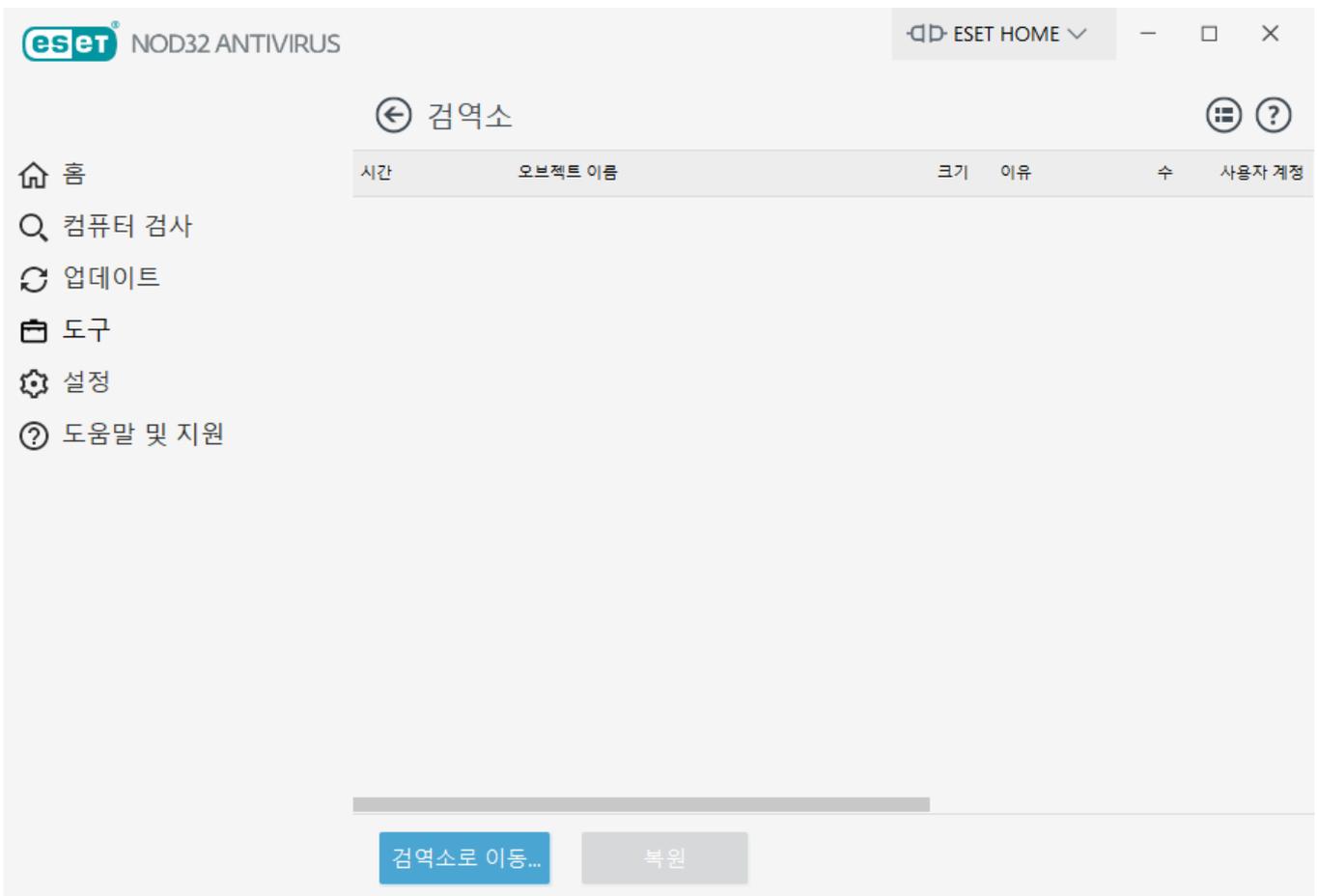
검역소

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

검역소는 ESET NOD32 Antivirus [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).



파일을 검역소로 보내기

ESET NOD32 Antivirus에서는 제거된 파일을 자동으로 검역소로 보냅니다([경고](#) 창에서 이 옵션을 취소하지 않은 경우).

다음과 같은 경우 추가 파일을 검역소로 보내야 합니다.

- a. 치료할 수 없는 경우
- b. 안전하지 않거나, 제거하는 것이 권장되지 않은 경우
- c. 해당 파일을 ESET NOD32 Antivirus에서 잘못 탐지한 경우
- d. 또는 파일이 의심스럽게 동작하지만 [검사기](#)에서 탐지되지 않는 경우

파일을 검역소로 보내는 데에는 다음과 같은 여러 가지 옵션이 있습니다.

- a. 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.
- b. 해당 파일을 오른쪽 마우스 버튼으로 클릭하고 > **고급 옵션** > **파일을 검역소로 보내기**를 클릭합니다.
- c. **검역소** 창에서 **검역소로 이동**을 클릭합니다.
- d. 또한 오른쪽 마우스 버튼 메뉴를 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 위치 않는 애플리케이션](#)으로 표시된 경우 **복원 후 검사에서 제외** 옵션이 활성화됩니다. 또한 [제외](#)를 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.

탐지 설명

항목을 마우스 오른쪽 버튼으로 클릭하고 **탐지 설명**을 클릭하여 기록된 침투의 위험과 증상에 대한 자세한 정보가 포함된 ESET 위협 백과사전을 엽니다.

그림이 포함된 지침

다음 ESET 지식 베이스 문서는 영어로만 제공됩니다.

- [ESET NOD32 Antivirus에서 검역소로 보내 파일 복원](#)
- [ESET NOD32 Antivirus에서 검역소로 보내 파일 제거](#)
- [내 ESET 제품에서 탐지 정보를 알려 주었습니다. 어떻게 해야 하나요?](#)

검역소 보내기 실패

특정 파일을 검역소로 이동할 수 없는 이유는 다음과 같습니다.

- **읽기 권한 없음** - 파일 내용을 읽을 수 없다는 뜻입니다.
- **쓰기 권한 없음** - 파일 내용을 수정할 수 없다는 뜻입니다. 즉, 새로운 내용을 추가하거나 기존 내용을 삭제할 수 없습니다.
- **검역소로 보내려는 파일이 너무 큼** - 파일 크기를 줄여야 합니다.

"검역소 보내기 실패" 오류 메시지를 받으면, **추가 정보**를 클릭합니다. 검역소 보내기 오류 목록 창이 표시되고, 파일 이름과 해당 파일을 검역소로 보내지 못한 이유를 확인할 수 있습니다.

프록시 서버

대규모 LAN 네트워크에서는 컴퓨터와 인터넷 간 통신이 프록시 서버를 통해 조정될 수 있습니다. 이 구성 사용 시 다음 설정을 정의해야 합니다. 그렇지 않으면 프로그램이 자동으로 업데이트될 수 없습니다. ESET NOD32 Antivirus에서 프록시 서버 설정은 고급 설정 트리 내의 서로 다른 두 섹션에서 사용할 수 있습니다.

먼저, 프록시 서버 설정은 **도구 > 프록시 서버** 아래의 **고급 설정**에서 구성할 수 있습니다. 이 수준에서 프록시 서버를 지정하면 모든 ESET NOD32 Antivirus에 대한 전체 프록시 서버 설정이 정의됩니다. 여기의 파라미터는 인터넷 연결이 필요한 모든 모듈에서 사용됩니다.

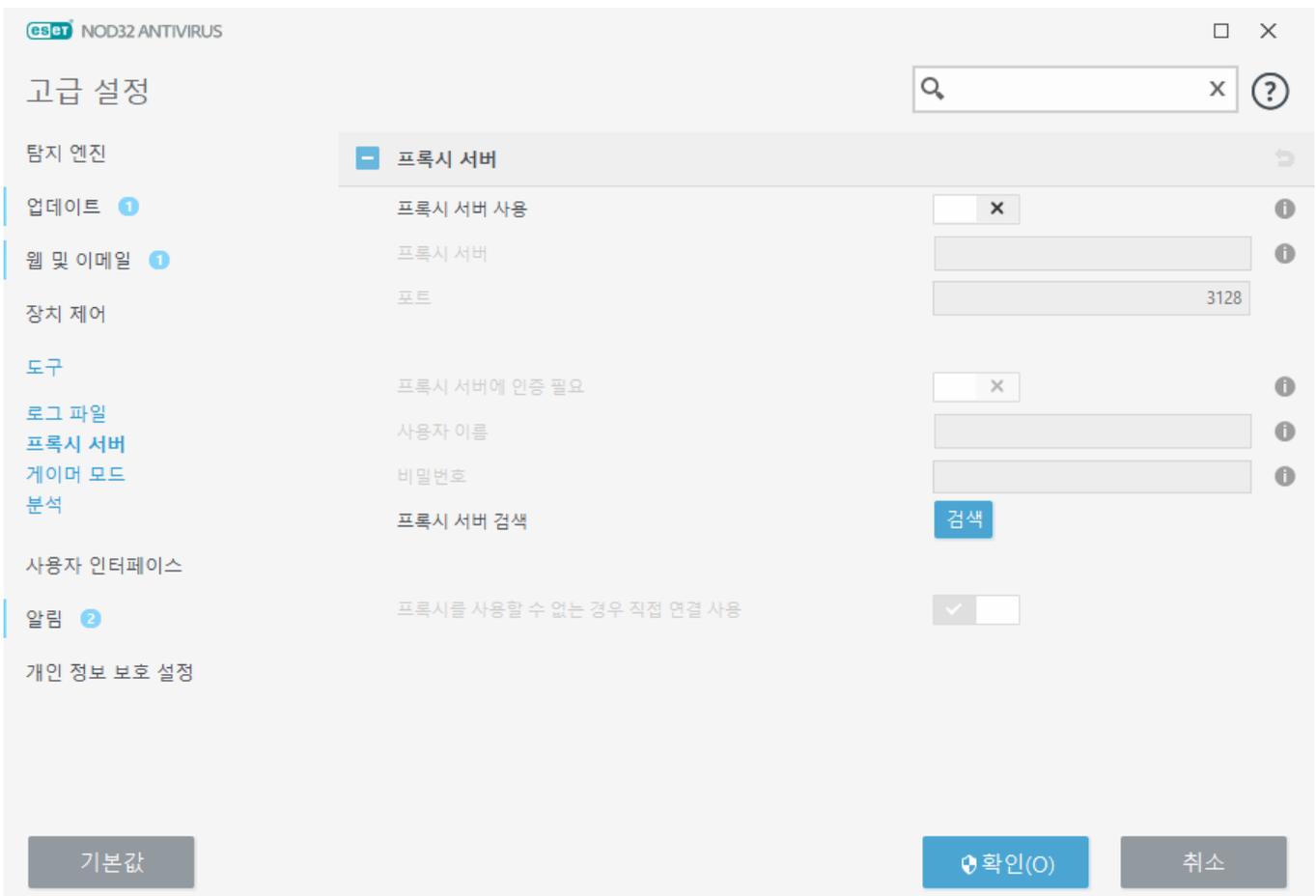
이 수준에 대한 프록시 서버 설정을 지정하려면 **프록시 서버 사용**을 선택한 다음 **프록시 서버 필드**에 프록시 서버 주소와 프록시 서버의 **포트** 번호를 입력합니다.

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. Internet Explorer 또는 Google Chrome의 인터넷 옵션에 지정된 파라미터가 복사됩니다.

i **프록시 서버** 설정에 사용자 이름 및 비밀번호를 수동으로 입력해야 합니다.

프록시를 사용할 수 없는 경우 직접 연결 사용 - ESET NOD32 Antivirus이(가) 프록시를 통해 연결하도록 구성되어 있는데 프록시에 연결할 수 없는 경우 ESET NOD32 Antivirus은(는) 프록시를 우회하고 ESET 서버와 직접 통신합니다.

프록시 서버 설정은 고급 업데이트 설정(**프록시 모드** 드롭다운 메뉴에서 **프록시 서버를 통해 연결**을 선택하면 표시되는 **고급 설정 > 업데이트 > 프로필 > 업데이트 > 연결 옵션**)에서도 설정할 수 있습니다. 이 설정은 지정한 업데이트 프로필에 적용되고, 원격 위치에서 바이러스 시그니처 업데이트를 자주 받는 랩톱에 권장됩니다. 이 설정에 대한 자세한 내용은 [고급 업데이트 설정](#)을 참조하십시오.



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).

ESET에 샘플을 전송하기 전에

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 연구소에서 사용하는 사용자들을 위한 수동 검사를 수행하지 않음)
- 설명이 포함된 제목 줄을 사용하고, 파일을 다운로드한 웹 사이트나 스크린샷 등의 파일 관련 정보를 최대한 많이 포함해 주십시오.

다음 방법 중 하나를 사용하여 분석용 샘플(파일 또는 웹 사이트)을 ESET에 전송할 수 있습니다.

1. 제품에 있는 샘플 전송 양식을 사용하십시오. 이 양식은 **도구 > 분석용 샘플 전송**에 있습니다. 전송된 샘플의 최대 크기는 256MB입니다.
2. 파일을 이메일로 전송할 수도 있습니다. 이 옵션을 사용하려는 경우에는 WinRAR/WinZIP을 사용하여 파일을 압축하고 "infected"라는 비밀번호로 압축파일을 보호한 후에 samples@eset.com으로 보내면 됩니다. 설명이 포함된 이메일 제목을 사용하고, 파일을 다운로드한 웹 사이트 등 파일에 대한 정보를 최대한 많이 포함해 주십시오.
3. 스팸 또는 스팸 가양성을 보고하려면 [ESET 지식베이스 문서](#)를 참조하십시오.

분석용 샘플 선택 양식의 **샘플 전송 사유** 드롭다운 메뉴에서 메시지의 목적에 가장 부합하는 설명을 선택합니다.

- [감염 의심 파일](#)
- [감염 의심 사이트](#)(맬웨어에 감염된 웹 사이트)
- [가양성 사이트](#)
- [가양성 파일](#)(감염된 것으로 검출되었지만 실제로는 감염되지 않은 파일)
- [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.

ESET에서 응답 메시지를 받지 못할 수도 있음

i 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 식별을 처리하는 동안 도움이 될 추가 정보나 설명을 입력할 수 있습니다.

i 첫 번째 파라미터 **맬웨어 감염 증상 발견**은 필수 사항이지만, 추가 정보를 입력하면 샘플을 식별 및 처리하는 데 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 [용어집](#)을 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 탐지 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 적절한 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 가양성으로 분류할 수 없는 경우 이 양식을 사용합니다.

파일 전송 사유 - 파일을 보내는 이유와 자세한 설명을 입력하십시오.

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 NOD32 Antivirus에서는 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.

사용자 인터페이스

프로그램의 그래픽 사용자 인터페이스(GUI) 동작을 구성하려면 [기본 프로그램 창](#)에서 **설정 > 고급 설정(F5 키) > 사용자 인터페이스**를 클릭합니다.

[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.

i 시스템 알림, 탐지 경고 및 애플리케이션 상태의 동작을 구성하려면 [알림](#) 섹션을 참조하십시오.

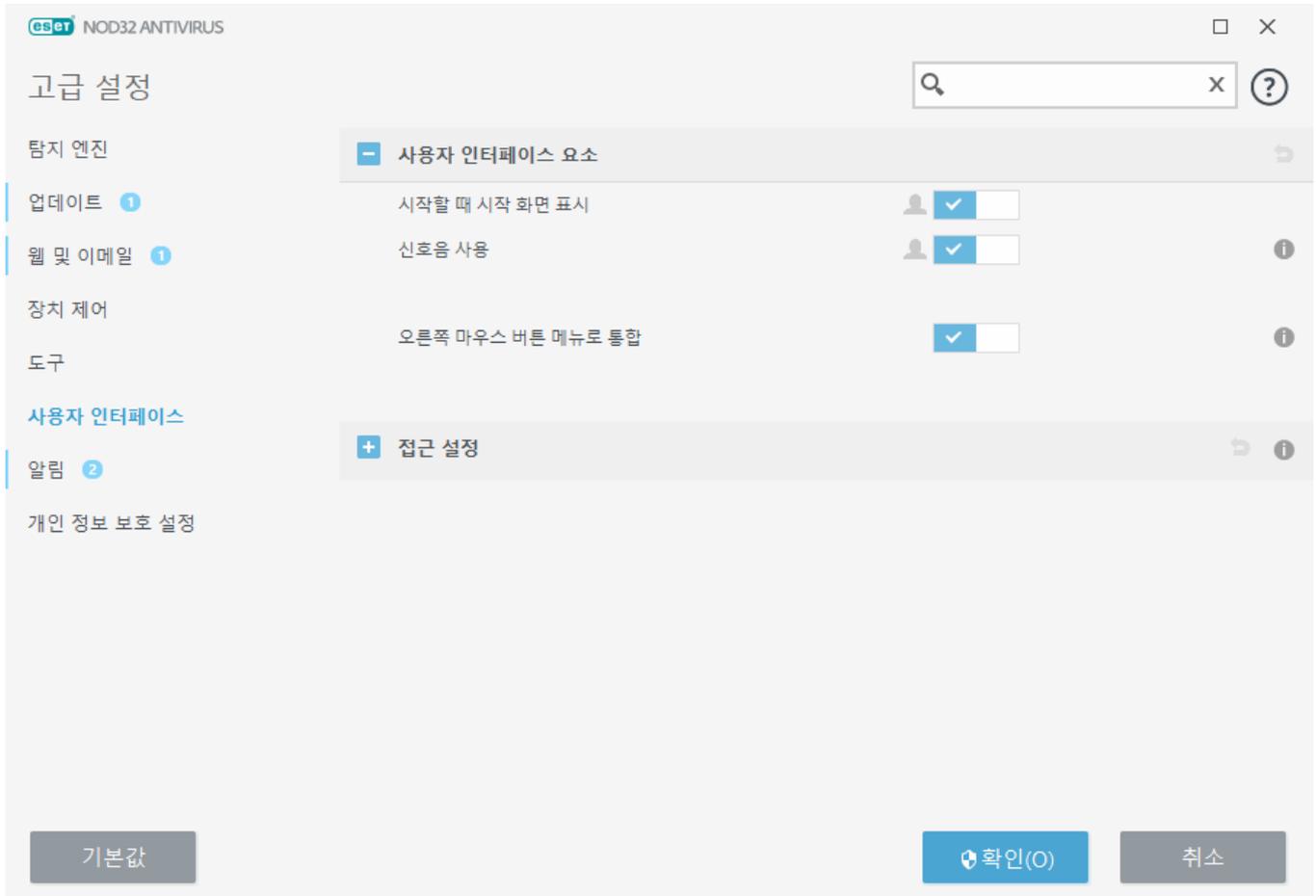
사용자 인터페이스 요소

ESET NOD32 Antivirus의 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.

ESET NOD32 Antivirus 시작 화면을 비활성화하려면 **시작할 때 시작 화면 표시** 옵션을 선택 취소합니다.

신호음 사용 - 검사 중에 중요한 이벤트가 발생(예: 위협이 발견되거나 검사가 완료된 경우)하면 ESET NOD32 Antivirus에서 신호음을 울립니다.

오른쪽 마우스 버튼 메뉴로 통합 - ESET NOD32 Antivirus 제어 요소를 오른쪽 마우스 버튼 메뉴로 통합합니다.



접근 설정

ESET NOD32 Antivirus 설정은 보안 정책의 중요한 부분입니다. 무단 수정은 잠재적으로 시스템의 안정성과 보호 상태를 위험에 빠뜨릴 수 있습니다. 무단 수정을 방지하기 위해 ESET NOD32 Antivirus의 제거 및 설정 파라미터를 패스워드로 보호할 수 있습니다.

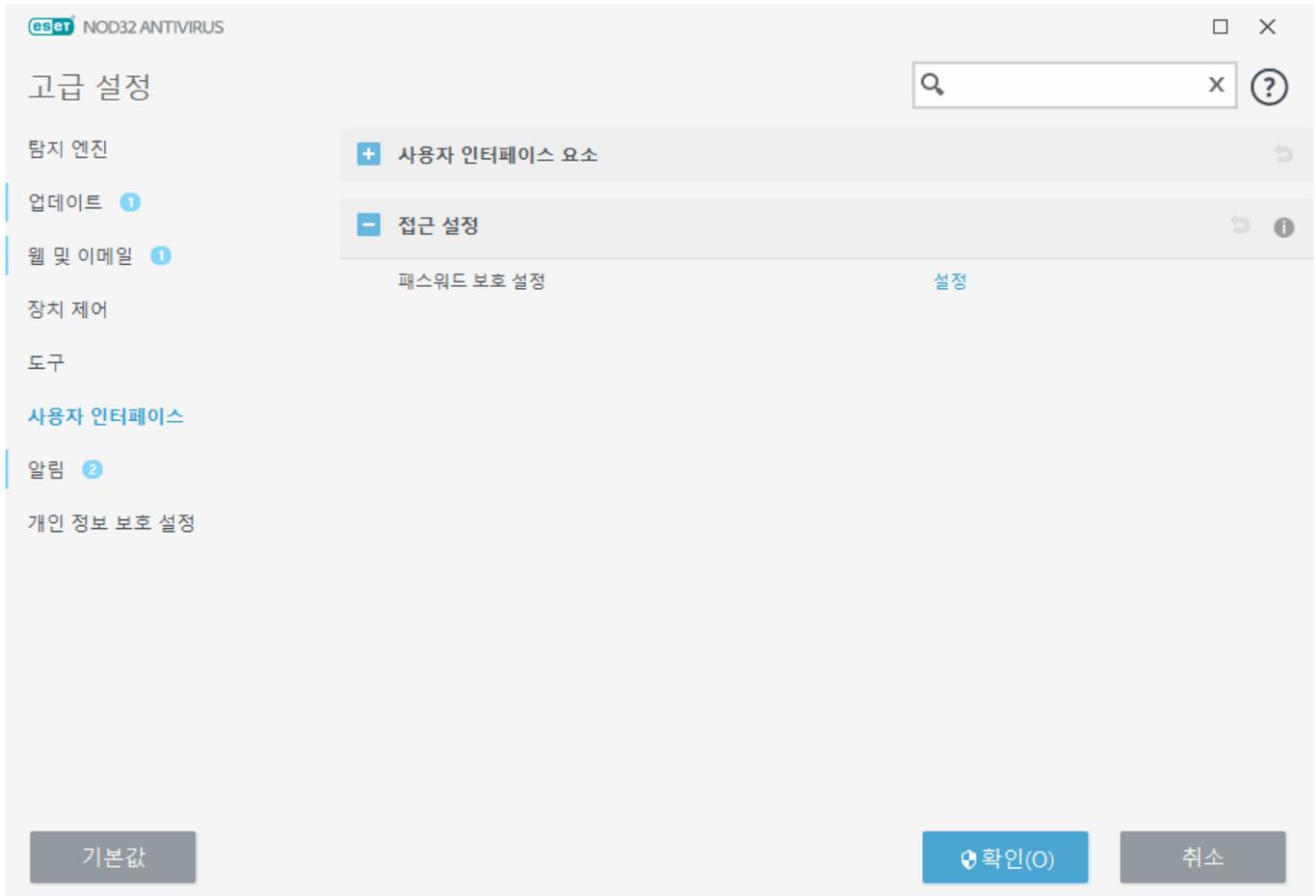
ESET NOD32 Antivirus의 제거 및 설정 파라미터를 보호하기 위한 패스워드를 설정하려면 **패스워드 보호 설정** 옆에 있는 **설정**을 클릭합니다.

i 보호된 고급 설정에 접근하려는 경우 패스워드를 입력하는 창이 표시됩니다. 패스워드를 잊어버린 경우 아래의 **패스워드 복원** 옵션을 클릭하고 라이선스 등록에 사용한 이메일 주소를 입력합니다. ESET에서 확인 코드와 패스워드를 다시 설정하는 방법에 대한 지침이 있는 이메일을 보내드립니다.

- [고급 설정의 잠금 해제 방법](#)

패스워드를 변경하려면 **패스워드 보호 설정** 옆에 있는 **패스워드 변경**을 클릭합니다.

패스워드를 제거하려면 **패스워드 보호 설정** 옆에 있는 **제거**를 클릭합니다.



고급 설정을 위한 패스워드

무단 수정을 방지하기 위해 ESET NOD32 Antivirus의 고급 설정을 보호하려면 새 패스워드를 설정해야 합니다.

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.

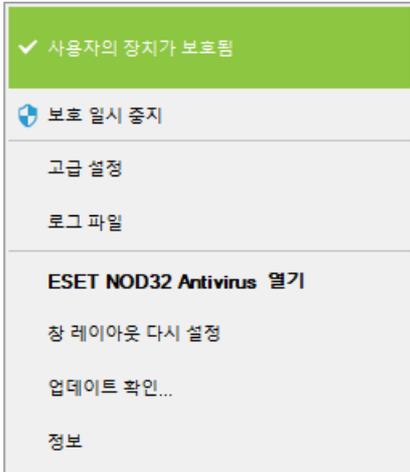
이 패스워드는 나중에 ESET NOD32 Antivirus 수정 시 필요합니다.

패스워드를 잊어버린 경우 고급 설정에 접근하여 ["패스워드 복원" 방법을 사용해 복원](#)할 수 있습니다.

잃어버린 ESET 라이선스 키, 라이선스 만료 날짜 또는 기타 ESET NOD32 Antivirus 라이선스 정보를 복구하려면 [지식베이스 문서](#)를 참조하십시오.

시스템 트레이 아이콘

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



보호 일시 중지 - 파일, 웹 및 이메일 통신을 제어하여 악의적인 시스템 공격으로부터 보호하는 [탐색 엔진](#)을 비활성화하는 확인 대화 상자를 표시합니다.

시간 간격 드롭다운 메뉴는 보호가 비활성화되는 시간을 나타냅니다.



안티바이러스, 안티스파이웨어 보호를 비활성화하시겠습니까?

안티바이러스 및 안티스파이웨어 보호를 비활성화하면 실시간 파일 시스템 보호, 웹 브라우저 보호, 이메일 클라이언트 보호는 물론 안티피싱 보호가 비활성화됩니다. 이렇게 되면 컴퓨터가 다양한 위협에 취약해집니다.

10분 동안 일시 중지 ▼

적용

취소

고급 설정 - 고급 설정 트리로 들어가려면 이 옵션을 선택합니다. F5 키를 누르거나 **설정 > 고급 설정**으로 이동하는 등의 다른 방법으로도 고급 설정을 열 수 있습니다.

로그 파일 - [로그 파일](#)은 발생한 중요 프로그램 이벤트에 대한 정보를 포함하고 있으며 검색에 대한 개요를 제공합니다.

열기 ESET NOD32 Antivirus - 트레이 아이콘에서 ESET NOD32 Antivirus [기본 프로그램](#) 창을 엽니다.

창 레이아웃 다시 설정 - ESET NOD32 Antivirus의 창을 기본 크기로 다시 설정하고 화면에서의 위치를 다시 설정합니다.

업데이트 확인 - 검색 엔진(이전 명칭: 바이러스 시그니처 DB) 업데이트를 시작하여 악성 코드에 대한 보호 수준을 보장합니다.

정보 - 시스템 정보, 설치된 ESET NOD32 Antivirus 버전과 설치된 프로그램 모듈에 대한 상세 정보를 제공합니다. 여기서 운영 체제 및 시스템 리소스에 대한 정보와 라이선스 만료일도 확인할 수 있습니다.

화면 리더 지원

ESET NOD32 Antivirus을(를) 화면 리더와 함께 사용하면 시각 장애가 있는 ESET 사용자가 제품을 탐색하거나 설정을 구성할 수 있습니다. 다음의 화면 리더는 (JAWS, NVDA, Narrator)를 지원합니다.

화면 리더 소프트웨어가 ESET NOD32 Antivirus GUI에 올바르게 접근할 수 있도록 하려면 [지식베이스 문서](#)의 지침을 따르십시오.

도움말 및 지원

ESET NOD32 Antivirus에는 발생할 수 있는 문제를 해결하는 데 도움을 주는 문제 해결 도구 및 지원 정보가 포함되어 있습니다.

라이선스

- [라이선스 문제 해결](#) - 이 링크를 클릭하여 활성화 또는 라이선스 변경 문제에 대한 해결 방법을 찾습니다.
- [라이선스 변경](#) - 활성화 창을 클릭하여 시작한 다음 제품을 활성화합니다. 장치가 [ESET HOME에 연결되었다면](#), ESET HOME 계정에서 라이선스를 선택하거나 새로운 라이선스를 추가합니다.

설치된 제품

- [새로운 기능](#) - 새롭고 향상된 기능에 대한 정보 창을 열려면 여기를 클릭합니다.
- [ESET NOD32 Antivirus 정보](#) - ESET NOD32 Antivirus 복사본에 대한 정보를 표시합니다.
- [제품 문제 해결](#) - 이 링크를 클릭하여 가장 자주 발생하는 문제에 대한 해결 방법을 찾습니다.
- [제품 변경](#) - 현재 라이선스로 ESET NOD32 Antivirus을 [다른 제품군으로](#) 변경할 수 있는지 여부를 확인하려면 클릭합니다.

 [도움말 페이지](#) - ESET NOD32 Antivirus 도움말 페이지를 실행하려면 이 링크를 클릭합니다.

기술 지원

 [지식베이스](#) - [ESET 지식 베이스](#)에는 다양한 문제에 대한 질문과 대답 및 권장 해결 방법이 포

함되어 있습니다. 지식 베이스는 다양한 문제를 해결하는 가장 강력한 도구로, ESET 기술 전문가가 정기적으로 업데이트합니다.

ESET NOD32 Antivirus 정보

이 창에서는 설치된 ESET NOD32 Antivirus 버전과 컴퓨터에 대한 상세 정보를 제공합니다.

모듈 표시를 클릭하여 로드된 프로그램 모듈 목록에 대한 정보를 확인합니다.

- 복사를 클릭하여 모듈에 대한 정보를 클립보드에 복사할 수 있습니다. 이 기능은 문제 해결 및 고객 지원부에 문의할 때 유용할 수 있습니다.
- 모듈 창에서 탐지 엔진을 클릭하여 ESET 탐지 엔진의 각 버전에 대한 정보가 포함된 ESET Virus Radar를 엽니다.

ESET 뉴스

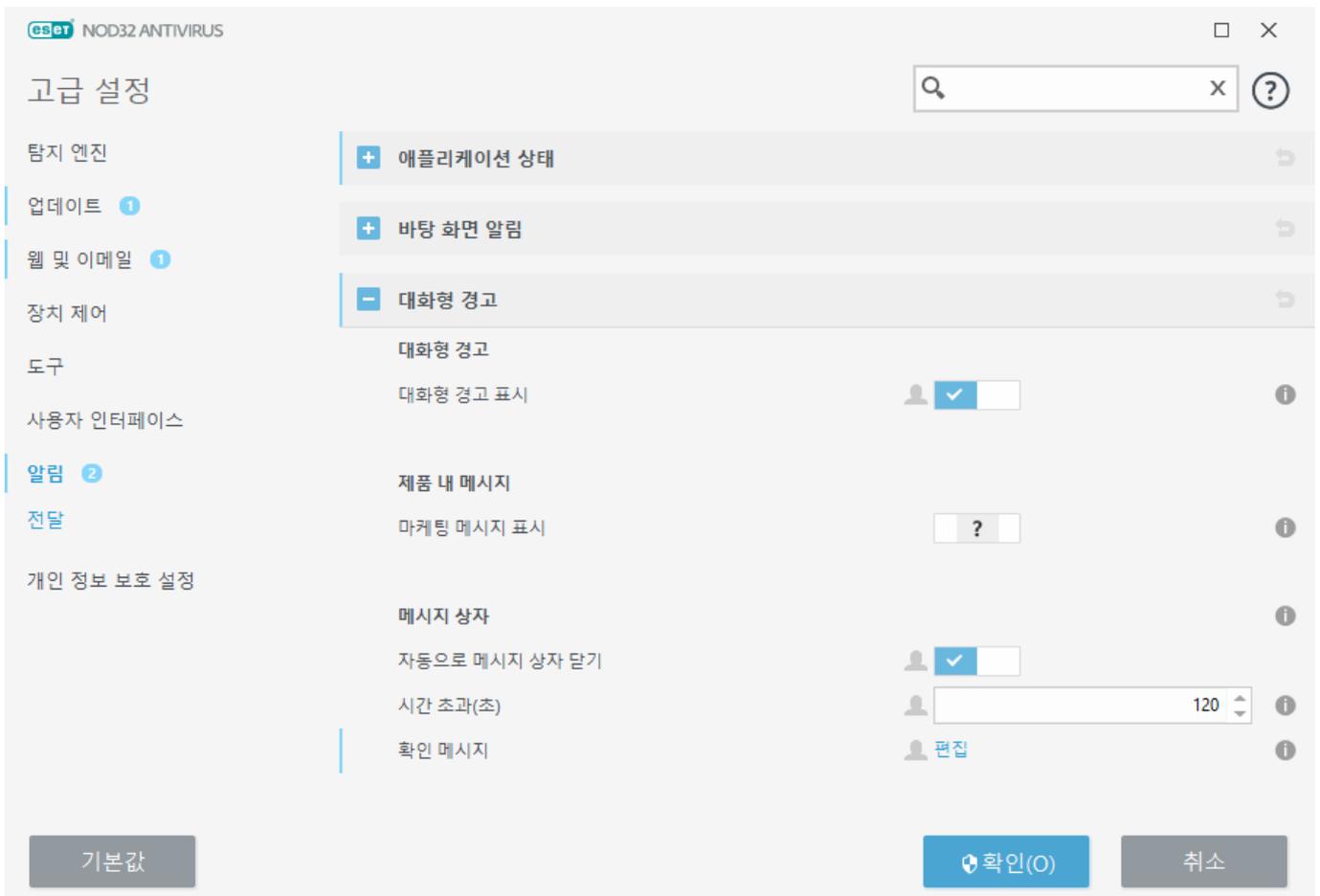
이 창에서 정기적으로 ESET NOD32 Antivirus은(는) ESET 뉴스를 알려줍니다.

제품 내 메시지는 사용자에게 ESET 관련 뉴스 및 기타 의견을 알려주기 위해 설계되었습니다. 마케팅 메시지를 보내려면 사용자의 동의가 있어야 합니다. 그러므로 마케팅 메시지는 기본적으로 사용자에게 전송되지 않습니다(물음표로 표시됨). 이 옵션을 활성화하면 ESET 마케팅 메시지 수

신에 동의하게 됩니다. ESET 마케팅 자료를 수신하지 않으려면 **마케팅 메시지 표시** 옵션을 비활성화하십시오.

팝업 창을 통한 마케팅 메시지 수신을 활성화하거나 비활성화하려면 아래 지침을 따르십시오.

1. ESET 제품의 기본 창을 엽니다.
2. **F5** 키를 눌러 **고급 설정**에 접근합니다.
3. **사용자 인터페이스 > 경고 및 메시지 상자**를 클릭합니다.
4. **마케팅 메시지 표시** 옵션을 수정합니다.



시스템 구성 데이터 전송

ESET에서 최대한 빠르고 정확하게 지원을 제공하려면 ESET NOD32 Antivirus 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 양식을 전송하려면 **데이터 전송 안 함**을 클릭하고 온라인 지원 양식을 사용하여 ESET 기술 지원에 문의할 수 있습니다.

이 설정은 [고급 설정 > 도구 > 분석 > 기술 지원](#)에서도 구성할 수 있습니다.

i 시스템 데이터를 전송하도록 결정했으면 웹 양식을 입력하고 전송해야 합니다. 그렇지 않으면 티켓이 생성되지 않으며 시스템 데이터가 손실됩니다.

기술 지원

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 전에 [시스템 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.

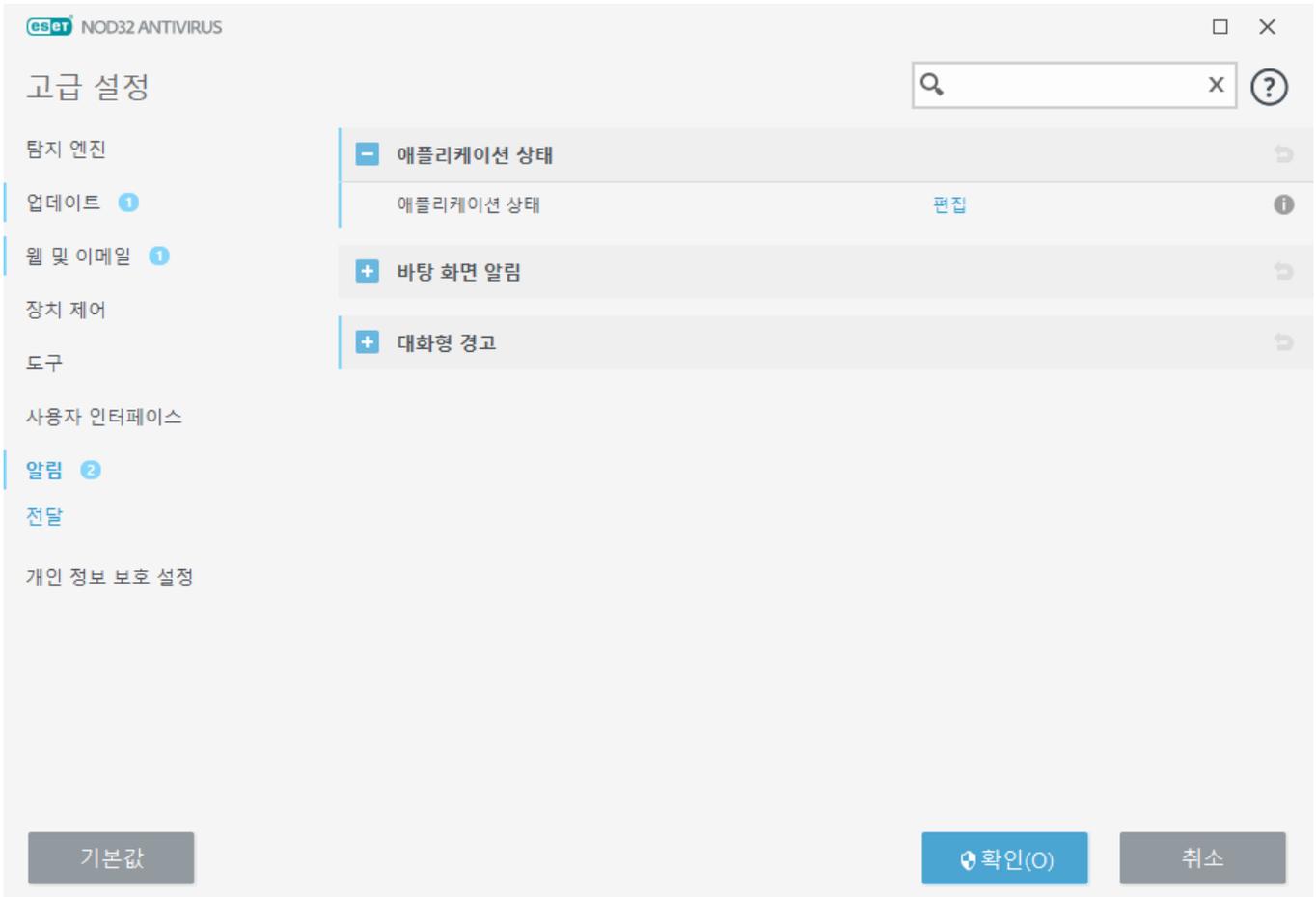
ESET Log Collector - 보다 신속하게 문제를 해결하기 위해 컴퓨터에서 정보를 자동으로 수집하여 기록하는 애플리케이션인 로그 수집기 유틸리티를 다운로드할 수 있는 [ESET 지식 베이스](#) 문서로 연결됩니다. 자세한 내용을 보려면 [ESET Log Collector](#) 여기를 클릭하십시오.

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 알려주는 알림 창이 표시됩니다.

알림

ESET NOD32 Antivirus 알림을 관리하려면 **고급 설정(F5 키) > 알림**을 엽니다. 다음과 같은 유형의 알림을 구성할 수 있습니다.

- 애플리케이션 상태 - [기본 프로그램 창](#)의 홈 섹션에 표시되는 알림입니다.
- [바탕 화면 알림](#) - 시스템 작업 표시줄 옆에 있는 작은 팝업 창입니다.
- [대화형 경고](#) - 사용자 상호 작용이 필요한 경고 창과 메시지 상자입니다.
- [전달](#) (이메일 알림) - 지정된 이메일 주소로 이메일 알림이 전송됩니다.



- 애플리케이션 상태

애플리케이션 상태 - 편집을 클릭하여 [기본 프로그램 창](#)의 홈 섹션에 표시되는 애플리케이션 상태를 선택합니다.

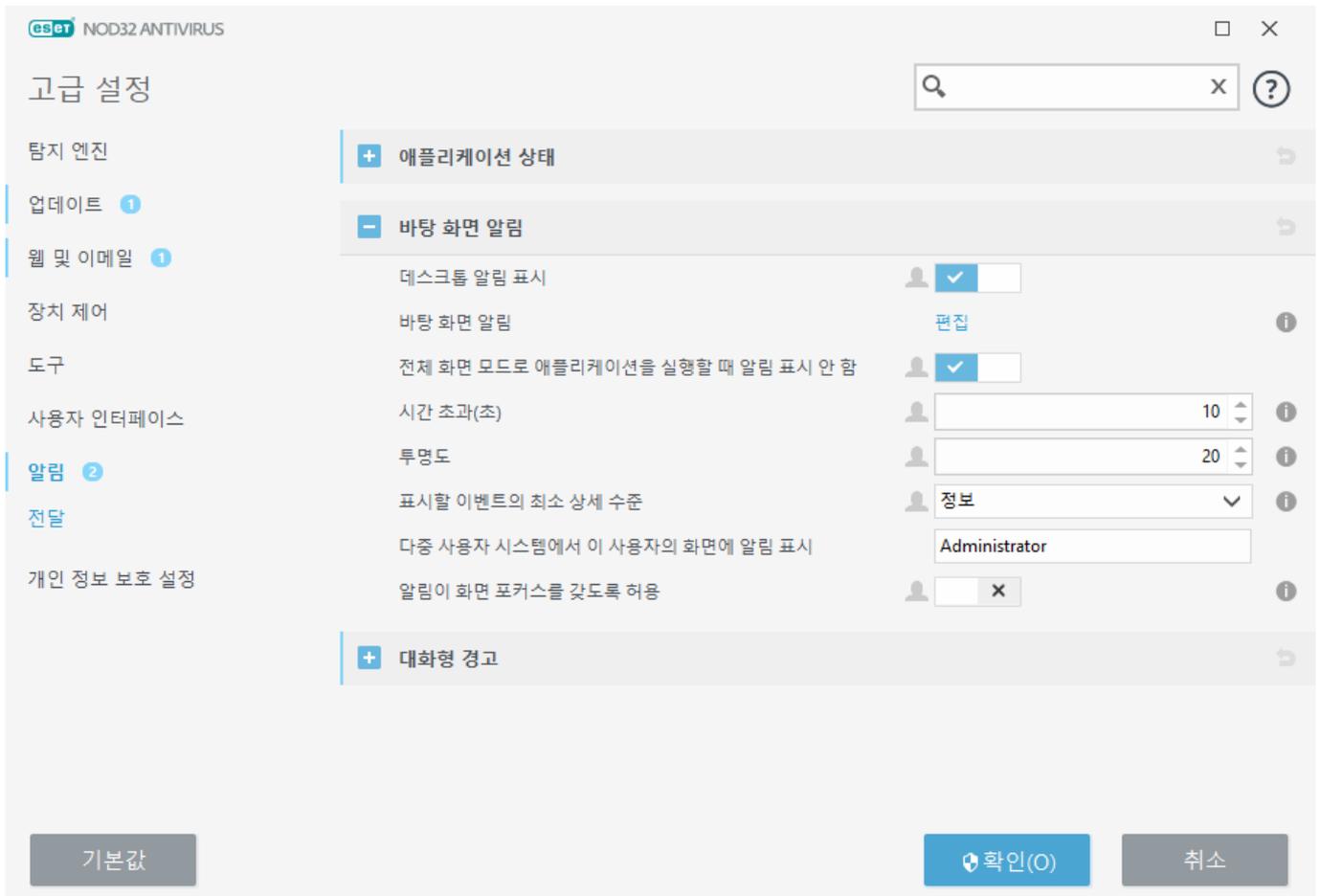
대화 상자 창 - 애플리케이션 상태

이 대화 상자 창에서 표시될 애플리케이션 상태를 선택할 수 있습니다. 예로, 안티바이러스 및 안티스파이웨어 보호를 일시 중지하거나 게이머 모드를 활성화하는 경우를 들 수 있습니다.

제품이 활성화되지 않았거나 라이선스가 만료된 경우에도 애플리케이션 상태가 표시됩니다.

바탕 화면 알림

바탕 화면 알림은 시스템 작업 표시 줄 옆에 있는 작은 팝업 창으로 표시됩니다. 기본적으로 10초 동안 표시되며 서서히 사라집니다. 알림에는 성공적인 제품 업데이트, 연결된 새 장치, 바이러스 검사 작업 완료 또는 새로운 위협 요소 발견이 포함됩니다.



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 알림](#)을 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.

0분석 - 위의 프로그램과 모든 레코드를 미세 조정하는 데 필요한 정보를 표시합니다.

0정보 - 성공한 업데이트 메시지를 포함한 정보 메시지(예: 비표준 네트워크 이벤트)와 위의 모든 레코드를 표시합니다.

0경고 - 경고 메시지, 오류 및 심각한 오류(예: 안티스텔스가 제대로 실행되지 않거나 업데이트가 실패함)를 표시합니다.

○오류 - 오류(예: 문서 보호가 시작되지 않음) 및 심각한 오류를 표시합니다.

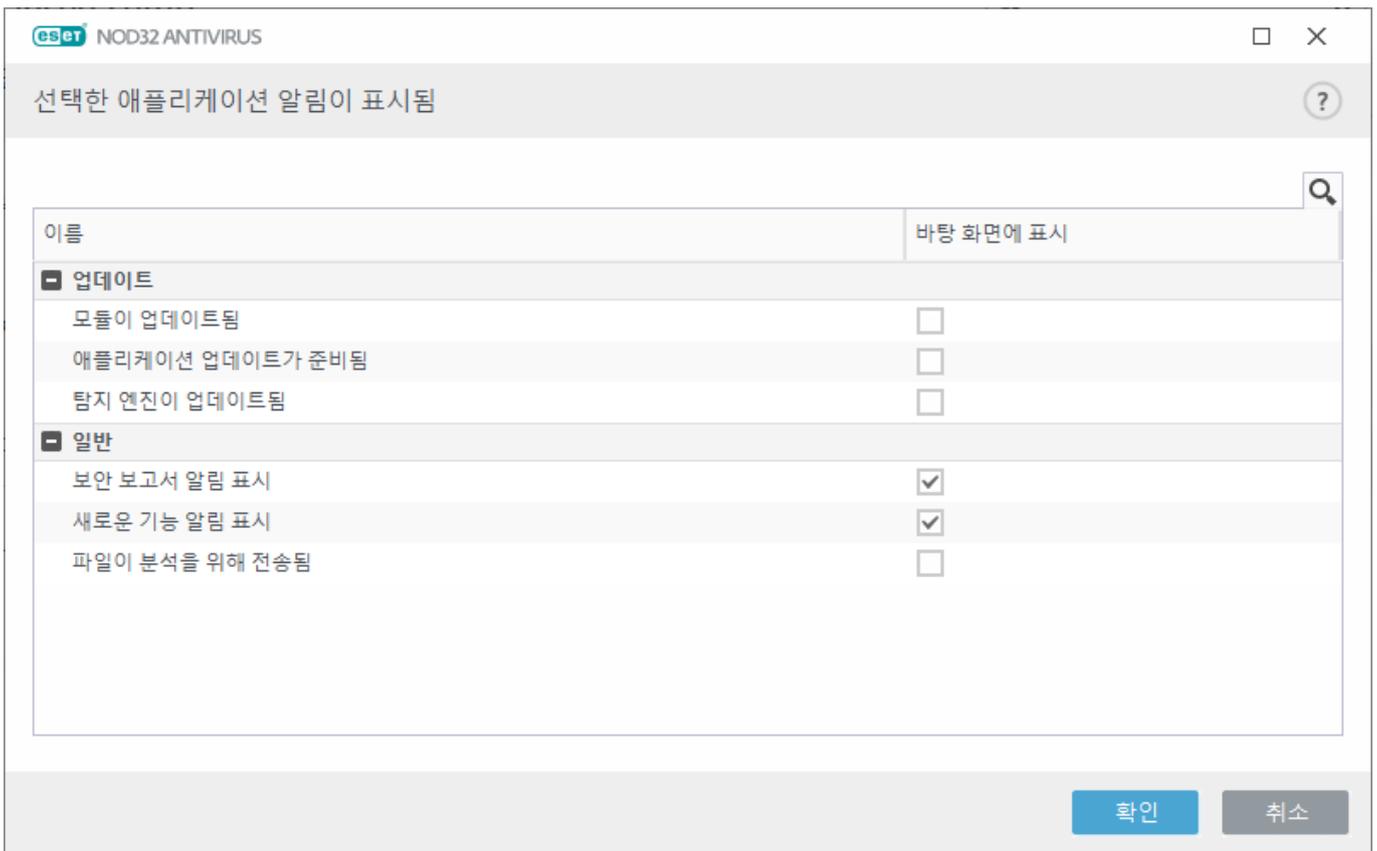
○주요 - 심각한 오류(안티바이러스 보호를 시작할 때 오류 발생, 시스템 감염 등)만 표시합니다.

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 - 알림이 화면 포커스를 갖고 **ALT + Tab** 메뉴에서 접근할 수 있도록 합니다.

바탕 화면 알림 목록

화면 오른쪽 하단에 표시되는 바탕 화면 알림의 표시 기능을 조정하려면 **고급 설정(F5 키) > 알림 > 바탕 화면 알림**을 엽니다. **바탕 화면 알림** 옆의 **편집**을 클릭하고 적절한 **표시** 확인란을 선택합니다.



일반

보안 보고서 알림 표시 - 새로운 [보안 보고서](#)가 생성되면 알림을 받습니다.

새로운 기능 알림 표시 - 최신 제품 버전의 새롭고 향상된 모든 기능에 대한 알림을 받습니다.

파일이 분석을 위해 전송됨 - ESET NOD32 Antivirus이(가) 분석을 위해 파일을 보낼 때마다 알림을 받습니다.

업데이트

애플리케이션 업데이트가 준비됨 - ESET NOD32 Antivirus 새 버전 업데이트가 준비되면 알림을 받습니다.

탐지 엔진이 업데이트됨 - 제품이 탐지 엔진 모듈을 업데이트하면 알림을 받습니다.

모듈이 업데이트됨 - 제품이 프로그램 구성 요소를 업데이트하면 알림을 받습니다.

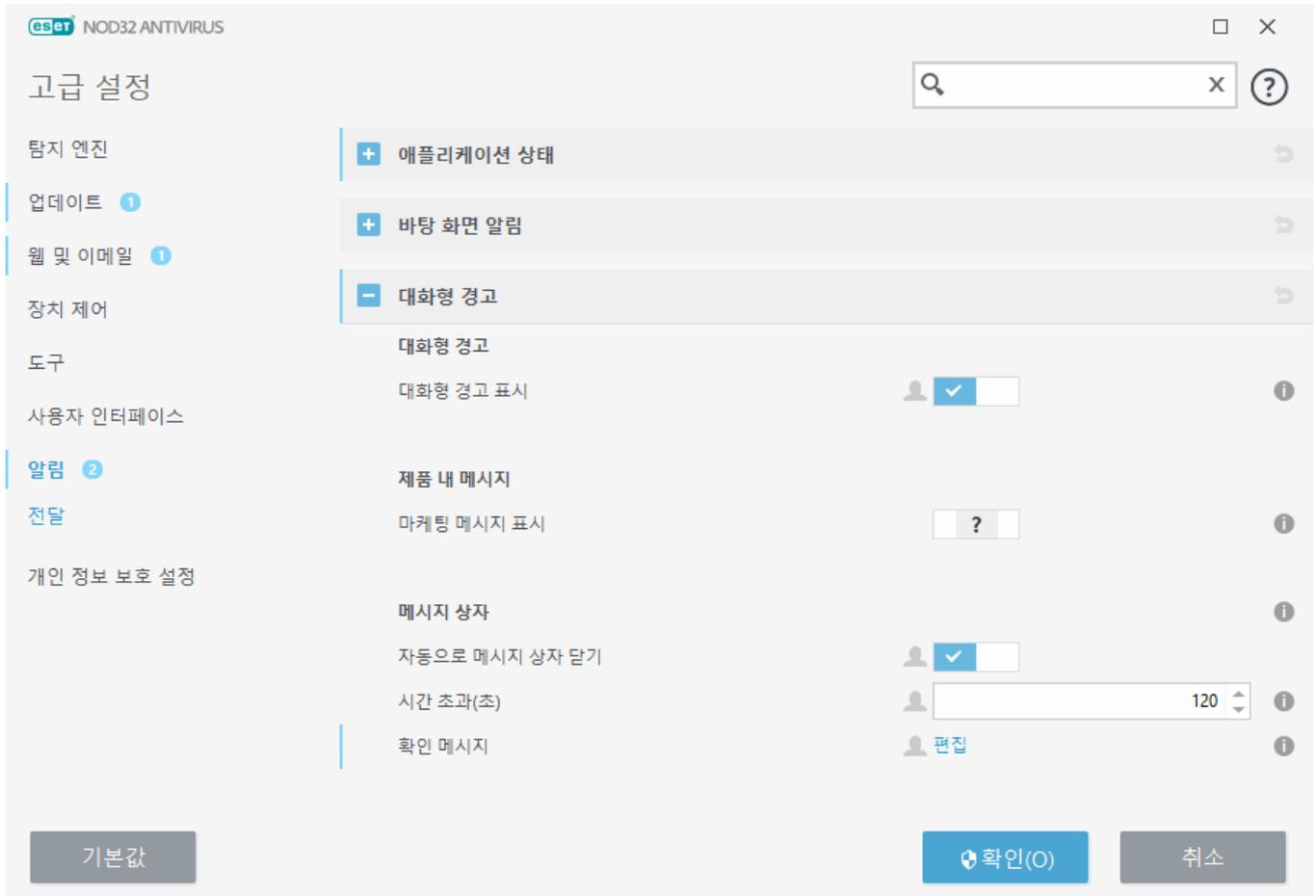
바탕 화면 알림의 일반 설정을 설정하려면(예: 표시할 메시지의 길이 또는 표시할 이벤트의 최소 상세 수준) **고급 설정 (F5) > 알림의 [바탕 화면 알림](#)**을 참조하십시오.

대화형 경고

일반 경고 및 알림에 대한 정보를 원하십니까?

- [위협이 발견됨](#)
- [주소가 차단됨](#)
- [제품이 활성화되지 않음](#)
- [더 많은 기능을 갖춘 제품으로 변경](#)
- [더 적은 기능을 갖춘 제품으로 변경](#)
- [업데이트 사용 가능](#)
- [업데이트 정보가 일치하지 않습니다](#)
- ["모듈 업데이트 실패" 메시지에 대한 문제 해결](#)
- [모듈 업데이트 오류 해결](#)
- [웹 사이트 인증서가 해지됨](#)

고급 설정(F5 키) > 알림의 대화형 경고 섹션에서는 사용자가 결정을 내려야 하는 경우(예: 잠재적 피싱 웹 사이트) ESET NOD32 Antivirus에서 탐지에 대한 메시지 상자 및 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. ESET은 이 옵션을 활성화해 두는 것을 권장합니다.

제품 내 메시지

제품 내 메시지는 사용자에게 ESET 관련 뉴스 및 기타 의견을 알려주기 위해 설계되었습니다. 마케팅 메시지를 보내려면 사용자의 동의가 있어야 합니다. 그러므로 마케팅 메시지는 기본적으로 사용자에게 전송되지 않습니다(물음표로 표시됨). 이 옵션을 활성화하면 ESET 마케팅 메시지 수신에 동의하게 됩니다. ESET 마케팅 자료를 수신하지 않으려면 **마케팅 메시지 표시** 옵션을 비활성화하십시오.

메시지 상자

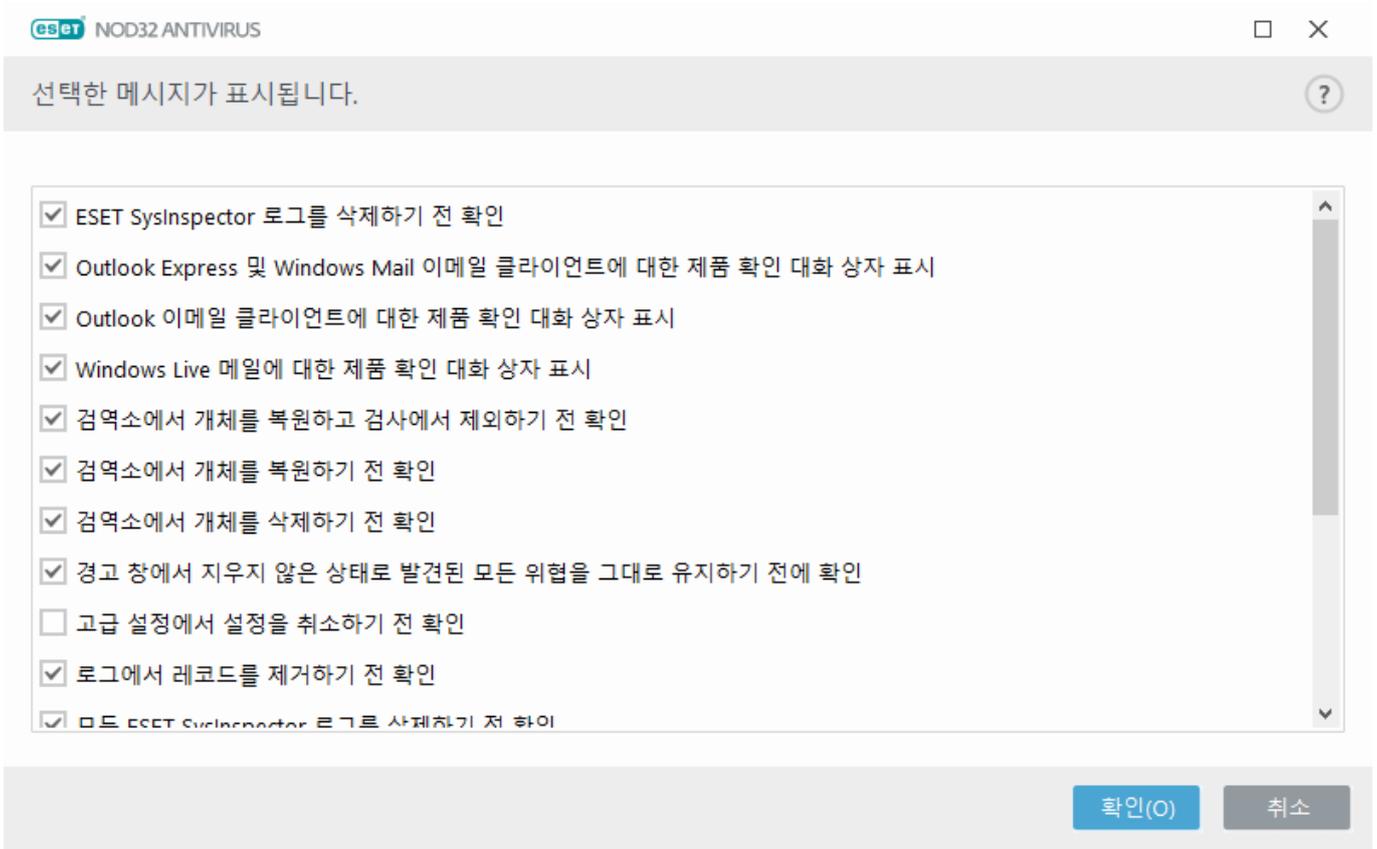
일정 시간 후에 메시지 상자를 자동으로 닫으려면 **자동으로 메시지 상자 닫기**를 선택합니다. 수동으로 닫지 않은 경우 지정된 시간이 경과하면 경고 창이 자동으로 닫힙니다.

시간 초과(초) – 경고 표시 지속 시간을 설정합니다. 값은 10~999초 사이여야 합니다.

확인 메시지 – 표시하거나 표시하지 않도록 선택할 수 있는 **확인 메시지 목록**을 표시하려면 **편집**을 클릭합니다.

확인 메시지

확인 메시지를 조정하려면 **고급 설정(F5 키) > 알림 > 대화형 경고**로 이동한 다음 **확인 메시지** 옆의 **편집**을 클릭합니다.



이 대화 상자 창에는 어떠한 동작이 수행되기 전에 ESET NOD32 Antivirus에서 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 전 확인](#)
- [모든 ESET SysInspector 로그를 삭제하기 전 확인](#)
- [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](#)
- [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](#)

이동식 미디어

ESET NOD32 Antivirus에서는 컴퓨터에 연결 시 자동 이동식 미디어(CD/DVD/USB/...) 검사 기능을 제공합니다. 이 기능은 컴퓨터 관리자가 원치 않는 콘텐츠가 포함된 이동식 미디어를 사용자가 연결하지 못하도록 하려는 경우에 유용할 수 있습니다.

이동식 미디어를 연결하고 ESET NOD32 Antivirus에서 **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 설정 섹션을 엽니다.
- **선택한 옵션 항상 사용** - 이후에 이동식 미디어가 삽입될 때마다 같은 작업이 수행됩니다.

이외에도 ESET NOD32 Antivirus에는 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.

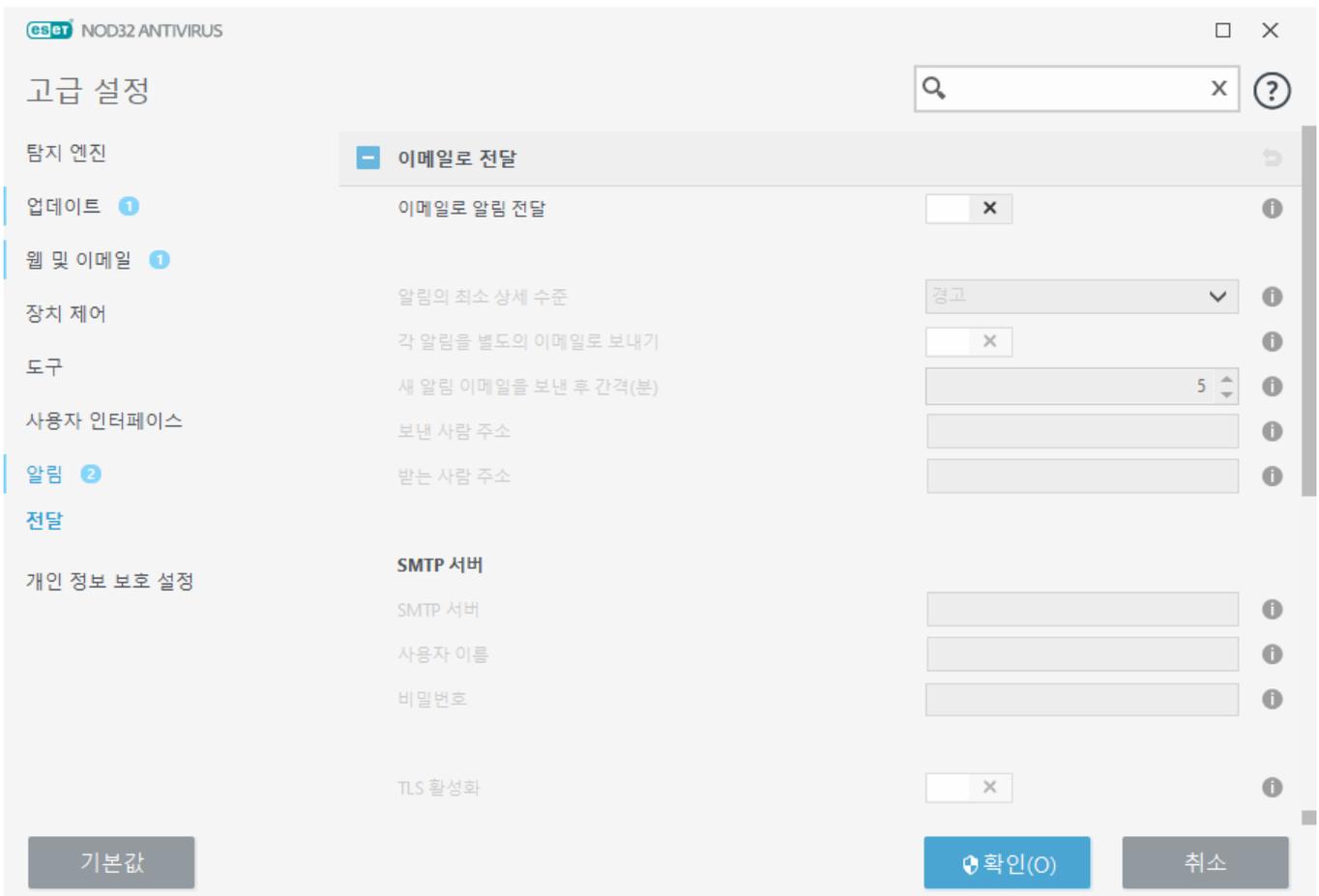
이동식 미디어 검사 설정에 접근하려면 고급 설정(F5 키) > 탐지 엔진 > 악성코드 검사 > 이동식 미디어를 엽니다.

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.
- **검사 옵션 표시** - 이동식 미디어 설정 섹션을 엽니다.

전달

ESET NOD32 Antivirus에서는 선택한 상세 수준의 이벤트가 발생하면 알림 이메일을 자동으로 보낼 수 있습니다. 고급 설정(F5 키) > 알림 > 전달을 열고 **이메일로 알림 전달**을 활성화하여 이메일 알림을 활성화합니다.



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 메시지를 기록합니다(안티스텔스가 제대로 실행되지 않거나 업데이트가 실패함).
- **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).

i TLS 암호화를 사용하는 SMTP 서버는 ESET NOD32 Antivirus에서 지원됩니다.

사용자 이름 및 비밀번호 - SMTP 서버에 인증이 필요한 경우 SMTP 서버에 접근하기 위한 유효한 사용자 이름 및 비밀번호를 이 필드에 입력합니다.

TLS 활성화 - TLS 암호화를 사용하는 Secure Alert 및 알림입니다.

SMTP 연결 테스트 - 테스트 이메일이 받는 사람의 이메일 주소로 전송됩니다. SMTP 서버, 사용자 이름, 패스워드, 보낸 사람 주소 및 받는 사람 주소를 입력해야 합니다.

메시지 형식

프로그램과 원격 사용자 또는 시스템 관리자 간의 통신은 Windows 메시징 서비스를 사용하여 이메일 또는 LAN 메시지를 통해 수행됩니다. 대부분의 경우 경고 메시지 및 알림에 대해 **기본 메시지 형식을 사용하는 것이 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. ESET은

미리 정의된 형식을 유지할 것을 권장합니다. 그러나 일부 경우(예: 자동화된 이메일 처리 시스템을 사용하는 경우), 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.

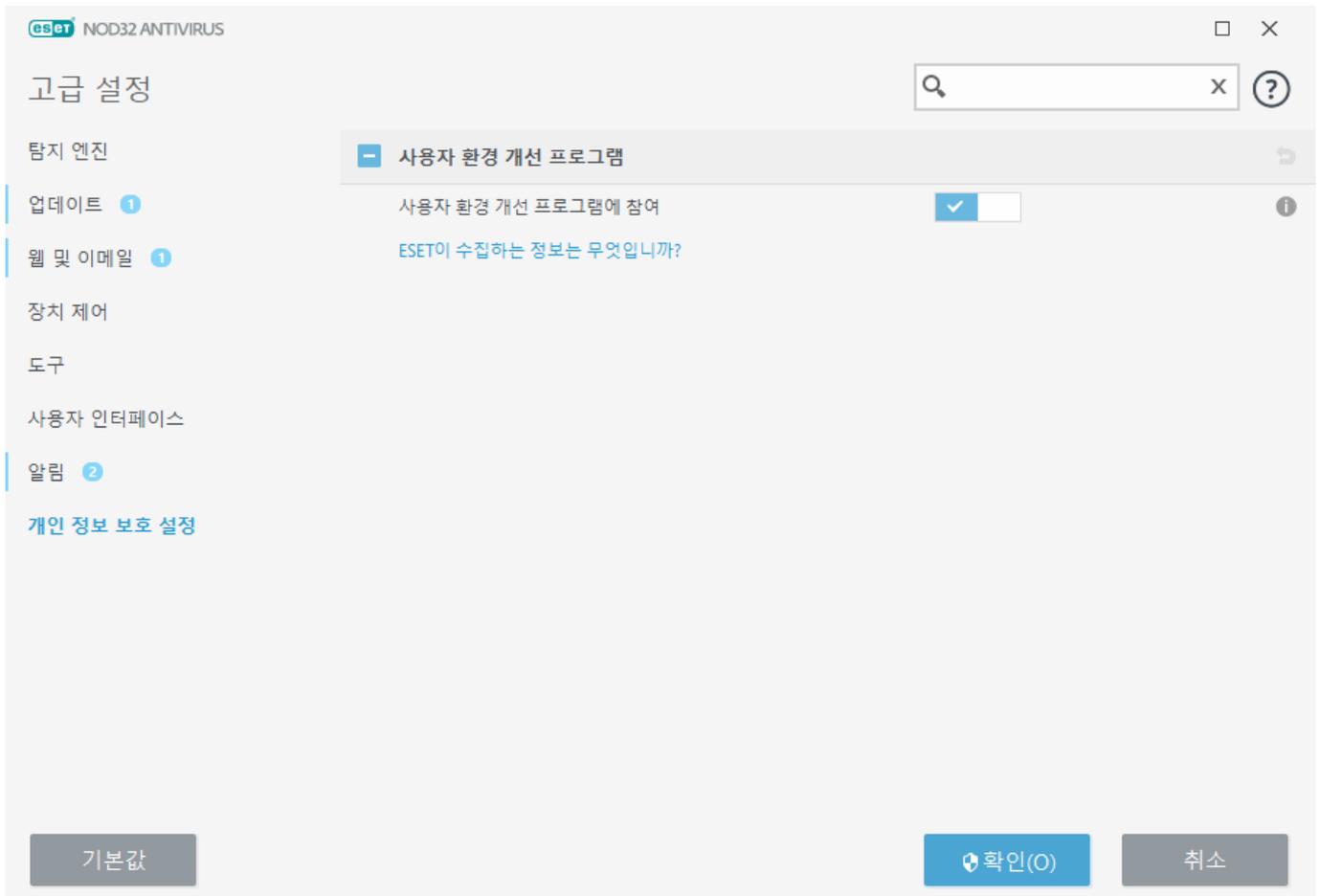
QP(Quoted-Printable) 인코딩 사용 - 이메일 메시지 소스가 (QP)(Quoted Printable) 형식으로 인코딩됩니다. 이 형식은 ASCII 문자를 사용하며, 8비트 형식(áéíóú)의 이메일로 특수 국가 표준 문자를 제대로 전송할 수 있습니다.

- **%TimeStamp%** - 이벤트의 날짜 및 시간입니다.
- **%Scanner%** - 관련 모듈입니다.
- **%ComputerName%** - 경고가 발생한 컴퓨터의 이름입니다.
- **%ProgramName%** - 경고를 생성한 프로그램입니다.
- **%InfectedObject%** - 감염된 파일, 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.

개인 정보 보호 설정

[기본 프로그램 창](#)에서 **설정 > 고급 설정(F5 키) > 개인 정보 보호 설정**을 클릭합니다.



사용자 환경 개선 프로그램

사용자 환경 개선 프로그램에 참여하려면 **사용자 환경 개선 프로그램에 참여** 옆의 슬라이더 막대를 활성화합니다. 참여하면 ESET 제품 사용과 관련된 익명의 정보를 ESET에 제공하게 됩니다. 수집된 데이터는 사용자 환경을 개선하는 데 도움이 되며, 제3자와 공유되지 않습니다. [ESET에서 수집하는 정보는 무엇입니까?](#)

프로필

프로필 관리자는 ESET NOD32 Antivirus 내에서 두 군데 즉, **수동 컴퓨터 검사** 섹션과 **업데이트** 섹션에서 사용됩니다.

컴퓨터 검사

ESET NOD32 Antivirus에는 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 트리거

할 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 창(F5 키)을 열고 **검색 엔진 > 맬웨어 검사 > 수동 검사 > 프로필 목록**을 클릭합니다. **프로필 관리자** 창에는 새 프로필을 생성할 수 있는 옵션 및 기존 검사 프로필이 있는 **선택한 프로필** 드롭다운 메뉴가 포함되어 있습니다. 필요에 맞게 검사 프로필을 생성하려면 **ThreatSense 엔진 파라미터 설정** 섹션에서 검사 설정의 각 파라미터 설명을 참조하십시오.

i 고유한 검사 프로필을 생성하려는데 **컴퓨터 검사** 구성이 부분적으로 적합하지만 **런타임 패어나 잠재적으로 안전하지 않은 애플리케이션**은 검사하고 싶지 않고 **항상 탐지** 수정도 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 설정 섹션의 프로필 편집기를 사용하여 새 프로필 업데이트를 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 프로필의 두 프로필을 사용할 수 있습니다. 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.

키보드 바로 가기

다음과 같은 단축키를 사용하면 ESET NOD32 Antivirus을 보다 잘 탐색할 수 있습니다.

키보드 단축키	수행된 동작
F1	도움말 페이지 열기
F5	고급 설정 열기
Up/Down	제품에서 항목을 통해 탐색
TAB	창에서 커서 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

분석

분석은 ESET 프로세스의 애플리케이션 크래시 덤프(예: ekrn)를 제공합니다. 애플리케이션이 충돌하면 덤프가 생성됩니다. 따라서 개발자는 다양한 ESET NOD32 Antivirus 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 중인 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 중인 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 디렉터리에서 분석 덤프 파일을 생성하려면 **생성**을 클릭합니다.

고급 로깅

마케팅 메시지에 고급 로깅 활성화 - 제품 내 마케팅 메시지와 관련된 모든 이벤트를 기록합니다.

컴퓨터 검사기 고급 로깅 활성화 - 컴퓨터 검사를 통해 파일과 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.

직접 클라우드 고급 로깅 활성화 - ESET LiveGrid®에서 발생하는 모든 이벤트를 기록합니다. 이

기록은 개발자들이 ESET LiveGrid® 관련 문제를 분석하고 수정하는 데 도움이 됩니다.

문서 보호 고급 로깅 활성화 - 문제를 진단하고 해결할 수 있도록 문서 보호에서 발생하는 모든 이벤트를 기록합니다.

커널 고급 로깅 활성화 - ESET 커널(ekrn)에서 발생하는 모든 이벤트를 기록합니다.

라이선싱 고급 로깅 활성화 - ESET 활성화 또는 ESET License Manager 서버와의 모든 제품 통신을 기록합니다.

메모리 추적 활성화 - 개발자가 메모리 누수를 진단하는 데 도움이 되는 모든 이벤트를 기록합니다.

운영 체제 고급 로깅 활성화 - 실행 중인 프로세스, CPU 활동, 디스크 작동 같은 운영 체제에 대한 추가 정보를 기록합니다. 이 정보는 개발자가 운영 체제에서 실행 중인 ESET 제품과 관련된 문제를 진단하고 수정하는 데 도움이 됩니다.

프로토콜 필터링 고급 로깅 활성화 - 개발자들이 프로토콜 필터링 관련 문제를 분석 및 수정할 수 있도록 프로토콜 필터링 엔진을 통과하는 모든 데이터를 PCAP 형식으로 기록합니다.

푸시 메시징 고급 로깅 활성화 - 푸시 메시징 중에 발생하는 모든 이벤트를 기록합니다.

실시간 파일 시스템 보호 고급 로깅 활성화 - 실시간 파일 시스템 보호를 통해 파일과 폴더를 검사하는 동안 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.

로그 파일은 `C:\ProgramData\ESET\ESET Security\Diagnostics\`에 있습니다.

기술 지원

ESET NOD32 Antivirus에서 [ESET 기술 지원에 문의](#)할 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.

설정 가져오기 및 내보내기

설정 메뉴에서 사용자 지정된 ESET NOD32 Antivirus.xml 구성 파일을 가져오거나 내보낼 수 있습니다.

그림이 포함된 지침

i 영어 및 기타 여러 언어로 제공되는 그림이 포함된 지침은 [.xml 파일을 사용하여 ESET 구성 설정 가져오기 또는 내보내기](#)를 참조하십시오.

구성 파일을 가져오고 내보내는 작업은 나중에 사용하기 위해 ESET NOD32 Antivirus의 현재 구성

을 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 창](#)에서 **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 창](#)에서 **설정 > 설정 가져오기/내보내기**를 클릭하고 **설정 가져오기**를 선택한 다음, 전체 파일 경로를 이름과 함께 입력합니다. ... 버튼을 클릭하여 구성 파일을 저장할 컴퓨터 위치를 찾습니다.

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



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 내보내기](#)도 참조하십시오.

기본 설정으로 되돌리기

모든 모듈의 모든 프로그램 설정을 되돌리려면 고급 설정(F5)에서 **기본값**을 클릭합니다. 이렇게 하면 모든 모듈의 모든 프로그램 설정이 새로 설치한 이후의 상태로 다시 설정됩니다.

[설정 가져오기 및 내보내기](#)도 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 NOD32 Antivirus의 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

스캐너 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	<p>감염된 개체에 치료 MODE 사용</p> <p>다음과 같은 옵션을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> • 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 Windows 시스템 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

i 100보다 큰 종료 코드는 해당 파일이 검사되지 않았으므로 감염되었을 수 있음을 나타냅니다.

ESET CMD

이 기능은 고급 `ecmd` 명령을 활성화하는 기능으로, 이 기능을 통해 명령줄(`ecmd.exe`)을 사용하여 설정을 내보내고 가져올 수 있습니다. 지금까지는 [GUI](#)를 사용해서만 설정을 내보낼 수 있었습니다.

이제 ESET NOD32 Antivirus 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 설정](#)에 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 NOD32 Antivirus 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.

✓ 설정 내보내기 명령:
ecmd /getcfg c:\config\settings.xml

✓ 설정 가져오기 명령:
ecmd /setcfg c:\config\settings.xml

 고급 ecmd 명령은 로컬로만 실행할 수 있습니다.

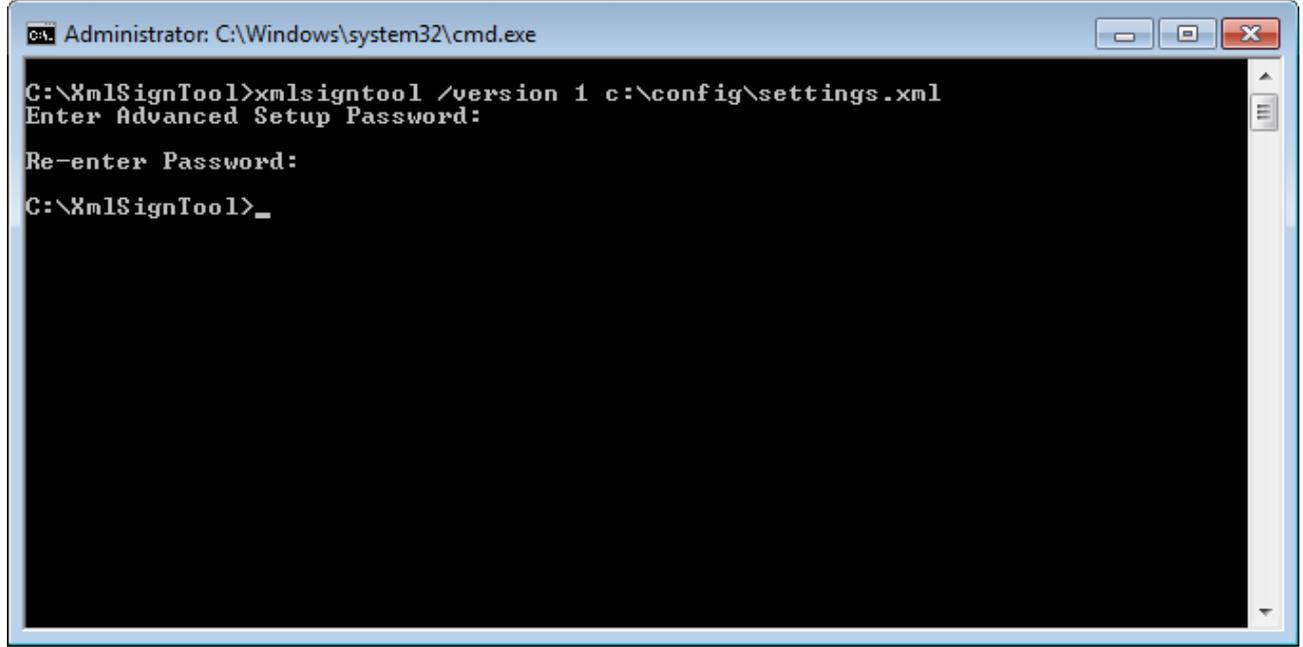
.xml 구성 파일에 지문 생성:

1. [XmlSignTool](#) 실행 파일을 다운로드합니다.
2. **관리자 권한으로 실행**을 사용하여 Windows 명령 프롬프트(cmd)를 엽니다.
3. xmlsigttool.exe의 저장 위치로 이동합니다.
4. 명령을 실행하여 .xml 구성 파일에 지문을 생성합니다(사용법: xmlsigttool /version 1|2 <xml_file_path>

 /version 파라미터 값은 사용 중인 ESET NOD32 Antivirus 버전에 따라 다릅니다. 11.1보다 이전 버전의 ESET NOD32 Antivirus용 /version 1을 사용합니다. 현재 버전의 ESET NOD32 Antivirus용 /version 2를 사용합니다.

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 NOD32 Antivirus 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 NOD32 Antivirus을 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. 사용자에게 의한 무단 수정을 방지하려면 **고급 설정 > 사용자 인터페이스 > 접근 설정**에서 비밀번호를 설정합니다.

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 검사**에 대한 트리거를 지정합니다.

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

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

일반적인 질문

이 장에서는 몇 가지 자주 묻는 질문과 발생하는 문제에 대해 다룹니다. 장 제목을 클릭하면 문제 해결 방법을 확인할 수 있습니다.

- [ESET NOD32 Antivirus을\(를\) 업데이트하는 방법](#)
- [내 PC에서 바이러스를 제거하는 방법](#)
- [스케줄러에서 새 작업을 생성하는 방법](#)
- [검사 작업을 예약하는 방법\(매주\)](#)
- [고급 설정의 잠금 해제 방법](#)
- [ESET HOME에서 제품 비활성화를 해결하는 방법](#)

문제가 위의 도움말 페이지 목록에 포함되지 않으면 ESET NOD32 Antivirus 도움말 페이지 내에서 검색해 보십시오.

도움말 페이지에서 문제/질문에 대한 해결 방법이나 대답을 찾을 수 없는 경우에는 정기적으로 업데이트되는 ESET 온라인의 [ESET 지식 베이스](#)를 확인해 보시기 바랍니다. 가장 인기 있는 지식 베이스 문서의 링크에는 일반적인 문제를 해결하는 데 도움을 주는 다음 내용이 포함되어 있습니다.

- [내 라이선스를 갱신하는 방법](#)
- [ESET 제품을 설치하는 동안 활성화 오류가 발생했습니다. 어떤 의미입니까?](#)
- [내 사용자 이름, 비밀번호 또는 라이선스 키를 사용하여 내 ESET Windows 홈 제품 활성화](#)
- [내 ESET 홈 제품 제거 또는 다시 설치](#)
- [ESET 설치가 중단되었다는 메시지가 표시되었습니다.](#)
- [라이선스를 갱신한 후에는 어떻게 해야 \(홈 사용자\)합니까?](#)
- [이메일 주소를 변경하면 어떻게 됩니까?](#)
- [내 ESET 제품을 새 컴퓨터 또는 장치로 이전](#)
- [Windows를 안전 모드 또는 안전 모드\(네트워크 사용\)을 시작하려면 어떻게 해야 합니까?](#)
- [안전한 웹 사이트를 차단에서 제외](#)
- [화면 리더 소프트웨어가 ESET GUI에 접근하도록 허용](#)

필요한 경우 [ESET의 기술 지원](#)에 질문이나 문제를 직접 문의할 수 있습니다.

ESET NOD32 Antivirus를 업데이트하는 방법

ESET NOD32 Antivirus를 수동으로 업데이트하거나 자동으로 업데이트할 수 있습니다. 업데이트를 트리거하려면 [기본 프로그램](#) 창에서 업데이트를 클릭한 다음 업데이트 확인을 클릭합니다.

기본 설치 설정에서는 매 시간 수행되는 자동 업데이트 작업을 생성합니다. 작업 수행 간격을 변경해야 하는 경우에는 **도구 > 스케줄러**로 이동하십시오.

내 PC에서 바이러스를 제거하는 방법

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

1. [기본 프로그램 창](#)에서 **컴퓨터 검사**를 클릭합니다.
2. **컴퓨터 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 문서](#)를 참조하십시오.

스케줄러에서 새 작업을 생성하는 방법

도구 > 스케줄러에서 새 작업을 생성하려면 **추가**를 클릭하거나, 마우스 오른쪽 버튼을 클릭하고 오른쪽 마우스 버튼 메뉴에서 **추가...**를 선택합니다. 5가지 유형의 예약된 작업:

- **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 로그인 시 실행할 수 있는 파일을 검사합니다.
- **컴퓨터 상태 스냅샷 생성** - ESET SysInspector 컴퓨터 스냅샷을 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 다음을 클릭합니다. 작업 수행 빈도를 선택합니다. 사용할 수 있는 옵션은 **한 번**, **반복적으로**, **매일**, **매주** 및 **이벤트가 트리거됨** 랩톱을 배터리 전원으로 실행하는 동안 시스템 리소스를 최소화하려면

배터리 전원으로 실행되는 작업 건너뛰기를 선택합니다. 작업은 **작업 실행** 필드에 지정된 날짜 및 시간에 실행됩니다. 그런 다음 예약된 시간에 작업을 수행하거나 완료할 수 없는 경우 수행할 동작을 정의합니다. 사용할 수 있는 옵션은 다음과 같습니다.

- 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 완료했다면 **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

정기 작업을 예약하려면 기본 프로그램 창을 열고 **도구 > 스케줄러**를 클릭합니다. 다음은 매주 로컬 드라이브를 검사하는 작업을 예약하는 방법에 대한 간단한 설명입니다. 자세한 내용은 [ESET의 지식베이스 문서](#)를 참조하십시오.

검사 작업을 예약하려면 다음을 수행합니다.

1. 기본 스케줄러 화면에서 **추가**를 클릭합니다.
2. 작업 이름을 입력하고 **작업 유형** 드롭다운 메뉴에서 **수동 컴퓨터 검사**를 선택합니다.
3. 작업 빈도로 **매주**를 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.

패스워드로 보호된 고급 설정의 잠금 해제 방법

보호된 고급 설정에 접근하려는 경우 패스워드를 입력하는 창이 표시됩니다. 패스워드를 잊어버린 경우 **패스워드 복원**을 클릭하고 라이선스 등록에 사용한 이메일 주소를 입력합니다. ESET에서 확인 코드가 있는 이메일을 보내드립니다. 확인 코드를 입력한 후 새 패스워드를 입력하여 확인합니다. 확인 코드는 7일 동안 유효합니다.

ESET HOME 계정을 통한 패스워드 복원 - 활성화에 사용되는 라이선스가 ESET HOME 계정에 연결되어 있는 경우에 이 옵션을 사용하십시오. [ESET HOME](#) 계정에 로그인하는 데 사용하는 이메일 주소를 입력하십시오.

이메일 주소가 기억나지 않거나 패스워드 복원에 문제가 있으면, **기술 지원 문의**를 클릭하십시오. 기술 지원 부서에 문의할 수 있는 ESET 웹 사이트로 리디렉션됩니다.

기술 지원용 코드 생성 - 이 옵션을 사용하면 기술 지원용 코드가 생성됩니다. 기술 지원에서 제공한 코드를 복사하고 **확인 코드가 있습니다.**를 클릭합니다. 확인 코드를 입력한 다음 새 패스워드를 입력하여 확인합니다. 확인 코드는 7일 동안 유효합니다.

자세한 내용은 [ESET Windows 홈 제품에서 설정 패스워드 잠금 해제](#)를 참조하십시오.

ESET HOME에서 제품 비활성화를 해결하는 방법

제품이 활성화되지 않음

이 오류 메시지는 라이선스 소유자가 ESET HOME 포털에서 ESET NOD32 Antivirus을(를) 비활성화하거나 ESET HOME 계정과 공유된 라이선스가 더 이상 공유되지 않는 경우에 표시됩니다. 이 문제를 해결하려면 다음을 수행합니다.

- **활성화**를 클릭하고 [활성화 방법](#) 중 하나를 사용하여 ESET NOD32 Antivirus을(를) 활성화합니다.
- 귀하의 ESET NOD32 Antivirus을(를) 라이선스 소유자가 비활성화했거나 라이선스가 더 이상 귀하와 공유되지 않는다는 정보를 이용해 라이선스 소유자에게 문의하십시오. 소유자는 [ESET HOME](#)에서 문제를 해결할 수 있습니다.

제품이 비활성화됨, 장치 연결 해제됨

이 오류 메시지는 [ESET HOME 계정에서 장치를 제거](#)하면 표시됩니다. 이 문제를 해결하려면 다음을 수행합니다.

- **활성화**를 클릭하고 [활성화 방법](#) 중 하나를 사용하여 ESET NOD32 Antivirus을(를) 활성화합니다.

- ESET NOD32 Antivirus이(가) 비활성화되었고 장치가 ESET HOME에서 연결 해제되었다는 정보를 이용해 라이선스 소유자에게 문의하십시오.
- 귀하가 라이선스 소유자이고 이러한 변경 내용을 모르는 경우 [ESET HOME 활동 피드](#)를 검토합니다. 의심스러운 활동이 발견되면 [ESET HOME 계정 패스워드를 변경](#)하고 [ESET 기술 지원에 문의](#)하십시오.

제품이 비활성화됨, 장치 연결 해제됨

이 오류 메시지는 [ESET HOME 계정에서 장치를 제거](#)하면 표시됩니다. 이 문제를 해결하려면 다음을 수행합니다.

- **활성화**를 클릭하고 [활성화 방법](#) 중 하나를 사용하여 ESET NOD32 Antivirus을(를) 활성화합니다.
- ESET NOD32 Antivirus이(가) 비활성화되었고 장치가 ESET HOME에서 연결 해제되었다는 정보를 이용해 라이선스 소유자에게 문의하십시오.
- 귀하가 라이선스 소유자이고 이러한 변경 내용을 모르는 경우 [ESET HOME 활동 피드](#)를 검토합니다. 의심스러운 활동이 발견되면 [ESET HOME 계정 패스워드를 변경](#)하고 [ESET 기술 지원에 문의](#)하십시오.

제품이 활성화되지 않음

이 오류 메시지는 라이선스 소유자가 ESET HOME 포털에서 ESET NOD32 Antivirus을(를) 비활성화하거나 ESET HOME 계정과 공유된 라이선스가 더 이상 공유되지 않는 경우에 표시됩니다. 이 문제를 해결하려면 다음을 수행합니다.

- **활성화**를 클릭하고 [활성화 방법](#) 중 하나를 사용하여 ESET NOD32 Antivirus을(를) 활성화합니다.
- 귀하의 ESET NOD32 Antivirus을(를) 라이선스 소유자가 비활성화했거나 라이선스가 더 이상 귀하와 공유되지 않는다는 정보를 이용해 라이선스 소유자에게 문의하십시오. 소유자는 [ESET HOME](#)에서 문제를 해결할 수 있습니다.

사용자 환경 개선 프로그램

사용자 환경 개선 프로그램에 참여하면 ESET 제품의 사용과 관련된 익명의 정보를 제공하게 됩니다. 데이터 처리에 대한 자세한 정보는 당사 개인 정보 보호 정책에서 확인할 수 있습니다.

사용자 동의

프로그램 참여는 자발적이며 귀하의 동의를 기반으로 합니다. 참여 후에는 수동적 참여가 되며, 이는 어떠한 추가 조치도 취할 필요가 없다는 뜻입니다. 언제든지 제품 설정을 변경하여 동의를 철회할 수 있습니다. 이렇게 하면 ESET에서 귀하의 익명 데이터를 더 이상 처리할 수 없게 됩니다.

언제든지 제품 설정을 변경하여 동의를 철회하실 수 있습니다:

- [ESET Windows 홈 제품에서 사용자 환경 개선 프로그램 설정 변경](#)

ESET은 어떤 유형의 정보를 수집합니까?

제품과의 상호 작용에 대한 데이터

당사는 이 정보를 통해 당사 제품이 사용되는 방식에 대해 자세히 파악할 수 있습니다. 이 덕분에 당사는 자주 사용되는 기능, 사용자가 수정하는 설정 또는 사용자가 제품 이용에 할애하는 시간 등의 정보를 알 수 있습니다.

장치에 대한 데이터

당사는 당사 제품이 사용되는 장치와 위치를 파악하기 위해 이 정보를 수집합니다. 관련 정보의 일반적인 예로는 장치 모델, 국가, 버전 및 운영 체제 이름 등이 있습니다.

오류 분석 데이터

오류 및 충돌 상황에 대한 정보도 수집됩니다. 예를 들면, 발생한 오류와 원인이 된 동작 등의 정보가 해당됩니다.

ESET이 이 정보를 수집하는 이유

당사는 이 같은 익명의 정보를 통해 당사의 사용자인 귀하를 위해 제품을 개선할 수 있습니다. 이 정보는 가장 적절하고, 사용하기 쉬우며, 가급적 결점 없는 제품을 만드는 데 도움을 줍니다.

이 정보를 제어하는 사람

ESET, spol. s r.o.가 프로그램에서 수집된 데이터의 유일한 관리자입니다. 이 정보는 제3자와 공유되지 않습니다.

최종 사용자 사용권 계약

2021년 10월 19일부로 효력이 발생합니다.

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 인정

하는 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 연결

되어 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_home에서 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 사용자에게 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 사용자에게 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 보유하고 있습니다. 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.

다. 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 보유하고 있습니다. 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 라이선스 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 삼가는데 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 웹사이트에 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 수신하는데 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 보유하고 있습니다. 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 발생합니다.

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.

계약 부록

네트워크 연결 장치 보안 평가. 추가 조항은 다음과 같이 네트워크 연결 장치 보안 평가에 적용됩니다.

소프트웨어에는 최종 사용자의 로컬 네트워크 보안 및 로컬 네트워크에 있는 장치의 보안을 확인하는 기능이 포함되어 있으며, 이 경우 라이선스 정보와 관련된 로컬 네트워크의 장치 존재 여부, 유형, 이름, IP 주소 및 MAC 주소와 같은 로컬 네트워크의 장치에 대한 정보 및 로컬 네트워크 이름이 필요합니다. 이 정보에는 라우터 장치에 대한 무선 암호화 유형 및 무선 보안 유형도 포함됩니다. 또한 이 기능은 로컬 네트워크에서 장비를 안전하게 보호하기 위한 보안 소프트웨어 솔루션의 가용성에 관한 정보를 제공할 수도 있습니다.

데이터 악용으로부터 보호. 추가 조항은 다음과 같이 데이터 악용으로부터 보호에 적용됩니다.

소프트웨어에는 컴퓨터의 도난과 직접적으로 관련된 중요한 데이터의 손실이나 악용으로부터 보호해 주는 기능이 포함되어 있습니다. 이 기능은 소프트웨어의 기본 설정에 따라 해제되어 있습니다. 기능을 활성화하려면 ESET HOME 계정을 생성해야 하며, 이 계정이 있어야 컴퓨터 도난 시에 데이터 수집이 활성화됩니다. 소프트웨어의 이 기능을 활성화하도록 선택한 경우 도난당한 컴퓨터에 대한 데이터가 수집되어 공급업체로 전송되며, 공급업체에서는 컴퓨터 네트워크 위치, 컴퓨터 화면에 표시되는 콘텐츠에 대한 데이터, 컴퓨터의 구성에 대한 데이터 및/또는 컴퓨터에 연결된 카메라에 기록된 데이터(이하 "데이터")가 포함될 수 있습니다. 컴퓨터 도난으로 인해 발생한 불리한 상황을 시정하기 위한 용도에 한해, 최종 사용자는 이 기능으로 획득하고 ESET HOME 계정을 통해 제공된 데이터를 사용할 권한을 갖습니다. 이 기능을 사용하려는 경우에만, 공급업체는 개인 정보 보호 정책에 명시된 대로 관련 법규 규정에 따라 데이터를 처리합니다. 공급업체는 최종 사용자가 개인 정보 보호 정책에 지정된 보존 기간을 초과하지 않으면서 데이터를 입수한 목적을 달성하는 데 필요한 기간 동안 데이터에 접근하도록 허용해야 합니다. 악용으로부터 데이터를 보호하는 기능은 최종 사용자에게 합법적 접근 권한이 있는 컴퓨터 및 계정에서만 사용해야 합니다. 모든 불법적인 사용은 관할당국에 신고됩니다. 공급업체는 관련 법률을 준수하고 데이터가 악용된 경우 사법당국에 협조합니다. 사용자는 ESET HOME 계정에 접근하는 패스워드를 보호할 책임이 있으며, 패스워드를 제3자에게 유출하지 않을 것에 동의합니다. 최종 사용자는 권한이 있는지 여부와 관계 없이 데이터 악용으로부터 보호 기능 및 ESET HOME 계정을 사용한 모든 활동과 관련하여 책임을 집니다. ESET HOME 계정이 손상된 경우 공급업체에 즉시 알려주세요. 데이터 악용으로부터 보호에 대한 추가 조항은 ESET Internet Security 및 ESET Smart Security Premium 최종 사용자에게만 적용됩니다.

ESET Secure Data. 추가 조항은 다음과 같이 ESET Secure Data에 적용됩니다.

1. 정의. ESET Secure Data 에 대한 이러한 추가 조항에서 아래 단어의 의미는 다음과 같습니다.

- a) "정보" 소프트웨어를 사용하여 암호화되었거나 암호가 해독된 모든 정보 또는 데이터
- b) "제품" ESET Secure Data 소프트웨어 및 설명서
- c) "ESET Secure Data" 전자 데이터의 암호화 및 암호 해독에 사용되는 소프트웨어

복수형에 대한 모든 언급은 단수형도 포함하고, 남성성에 대한 모든 언급은 여성과 중성을 포함하며

그 반대도 마찬가지입니다. 달리 정의되지 않은 단어는 본 계약에서 규정한 정의에 따라 사용해야 합니다.

2. 추가 최종 사용자 선언. 사용자는 다음을 승인하고 동의합니다.

a) 정보를 보호하고, 유지 관리하고, 백업하는 것은 사용자의 책임입니다.

b) ESET Secure Data를 설치하기 전에 컴퓨터의 모든 정보 및 데이터(중요한 정보 및 데이터를 포함하나 이에 국한되지 않음)를 완전히 백업해야 합니다.

c) ESET Secure Data를 설치하고 사용하는 데 사용되는 패스워드 또는 기타 정보를 안전하게 보관해야 하며 모든 암호화 키, 라이선스 코드, 키 파일 및 별도의 저장소 미디어로 생성된 기타 데이터의 백업 복사본을 만들어야 합니다.

d) 제품 사용에 대한 책임은 사용자에게 있습니다. 공급업체는 정보 또는 기타 데이터가 저장되는 위치 및 방법에 관계없이 정보 또는 기타 데이터의 허가되지 않았거나 잘못 수행된 암호화 또는 암호 해독의 결과로 인한 손실, 손해 또는 손상을 책임지지 않습니다.

e) 공급업체가 ESET Secure Data의 무결성 및 보안 보장을 위해 적절한 모든 조치를 취하는 동안, 안전 수준의 보안에 의존하거나 핵 시설, 항공기 탐사, 제어 또는 통신 시스템, 무기 및 방어 시스템, 생명 유지 또는 생명 감시 시스템을 포함하여 이에 국한되지 않는 잠재적으로 해롭거나 위험한 지역에서 제품을 사용하지 않아야 합니다.

f) 제품이 사용자의 요구 사항에 적합하다고 가정할 경우 보안 및 암호화 수준을 유지하는 것은 최종 사용자의 책임입니다.

g) 슬로바키아 또는 제품이 사용되는 기타 국가, 지역 또는 주의 모든 관련 법률 및 규정을 준수하도록 하는 것을 포함하여 이에 국한되지 않는 모든 제품 사용은 사용자의 책임입니다. 모든 제품을 사용하기 전에 제품이 모든 정부(슬로바키아 또는 기타 국가)의 금수 조치에 위반되지 않음을 보장했는지 확인해야 합니다.

h) ESET Secure Data는 라이선스 정보, 사용 가능한 패치, 서비스 팩 및 ESET Secure Data의 작동을 개선하거나, 유지 관리하거나, 수정하거나, 향상시킬 수 있는 기타 업데이트를 확인하기 위해 때때로 공급업체 서버에 연결할 수 있으며, 개인 정보 보호 정책에 따라 작동과 관련된 일반 시스템 정보를 전송할 수 있습니다.

i) 공급업체는 소프트웨어 사용 중에 생성되거나 저장된 비밀번호, 설치 정보, 암호화 키, 라이선스 활성화 코드 및 기타 데이터의 분실, 도난, 남용, 손상 또는 파괴로 인해 야기되는 어떤 손실, 손상, 비용 또는 손해 배상 청구도 책임지지 않습니다.

ESET Secure Data에 대한 추가 조항은 ESET Smart Security Premium 최종 사용자에게만 적용됩니다.

Password Manager 소프트웨어. 추가 조항은 다음과 같이 Password Manager 소프트웨어에 적용됩니다:

1. 추가 최종 사용자 선언. 사용자는 다음을 승인하고 이행하지 않을 것에 동의합니다.

a) Password Manager Software를 사용하여 인간 생활 또는 자산이 위협해질 수 있는 업무에 중대한 애플리케이션을 작동할 수 없습니다. 귀하는 Password Manager Software가 이러한 용도로 고안되지 않았으며, 이러한 경우에 발생하는 문제로 인해 공급업체가 책임질 수 없는 사망, 상해 또는 심각한 재산상 또는 환경 손상을 가져올 수 있다는 사실을 이해해야 합니다.

Password Manager Software는 핵 시설, 항공 탐사 또는 통신 시스템, 항공 교통 관제 및 생명 유지 시스템 또는 무기 시스템의 설계, 구성, 유지 보수 또는 작동을 포함하여 이에 국한되지 않는 이중 안전 제어가 요구되는 위험한 환경에서 사용되도록 설계, 의도 또는 사용 허가되지 않았습니다. 공급업체는 이러한 목적에의 적합성에 대해 명시적이거나 암시적인 어떤 보증도 분명히 거부합니다.

b) 본 계약이나 슬로바키아 또는 사용자의 관할권 법률을 위반하는 방식으로 Password Manager Software를 사용할 수 없습니다. 특히 유해한 콘텐츠의 데이터 또는 위법 활동에 사용될 수 있거나 법을 위반하거나 제3자의 권리(지적 재산권 포함)를 침해하는 콘텐츠의 데이터를 업로드하는 것을 포함하여 위법 활동을 행하거나 조장하는 데 Password Manager Software를 사용할 수 없습니다. 이러한 위법 활동에는 저장소>Password Manager Software 추가 약관의 목적에 따라 "저장소"는 공급업체 또는 공급업체 이외의 제3자와 사용자가 사용자 데이터를 동기화 및 백업할 수 있도록 하기 위해 관리하는 데이터 저장소 공간을 나타냄)의 계정 또는 다른 Password Manager Software나 저장소 사용자의 계정과 데이터에 대한 접근 권한을 얻으려는 시도가 포함되며 이에 국한되지 않습니다. 이러한 규정을 위반하는 경우 공급업체는 본 계약을 즉시 중단하며 필요한 구제 비용을 청구할 수 있으며, 환불 없이는 Password Manager Software를 추가로 사용하지 못하도록 하는 데 필요한 모든 조치를 취할 수 있습니다.

2. 책임 제한. Password Manager Software는 "있는 그대로" 제공됩니다. 어떠한 종류의 명시적이거나 암시적인 보증도 없습니다. 소프트웨어 사용에 따른 책임은 모두 사용자에게 있습니다. 제작업체는 데이터 동기화 및 백업 목적으로 Password Manager Software에서 외부 저장소로 전송된 데이터를 포함한 데이터 손실, 손상, 서비스 가용성 제한을 책임지지 않습니다. Password Manager Software를 사용해서 암호화한다고 해서 데이터 보안과 관련된 문제를 공급업체가 책임진다는 것을 의미하지는 않습니다. Password Manager Software를 통해 획득되거나 사용되거나 암호화되거나 저장되거나 동기화되거나 전송된 데이터가 제3자 서비스에도 저장될 수 있다는 것에 명시적으로 동의해야 합니다(동기화 및 백업 서비스가 사용되도록 설정된 경우에 Password Manager Software를 사용할 때만 적용됨). 공급업체가 독자적 판단에 따라 이러한 제3자 저장소, 웹 사이트, 웹 포털, 서버 또는 서비스를 선택하는 경우 공급업체는 이러한 제3자 서비스의 품질, 보안 또는 가용성을 책임지지 않으며 제3자의 계약 또는 법적 의무 위반 또는 소프트웨어를 사용하는 동안 발생하는 손상, 수익 손실, 금융 및 금융 외적 손상 또는 다른 종류의 손실에 대해서도 어떠한 책임도 지지 않습니다. 공급업체는 Password Manager Software 또는 저장소를 사용하여 획득하거나 사용하거나 암호화하거나 저장하거나 동기화하거나 전송되는 데이터에 대해 아무런 책임도 지지 않습니다. 귀하는 공급업체가 저장된 데이터 콘텐츠에 액세스할 수 없으며 법적으로 유해한 콘텐츠를 모니터링하거나 제거하지 않는다는 데 동의해야 합니다.

Password Manager Software와 관련된 개선, 업그레이드 및 수정(□개선)이 어떤 형식으로든 귀하가 제출한 피드백, 아이디어 또는 제안을 기반으로 작성된 경우에도 이러한 모든 권리는 공급업체가 보유하고 있습니다. 귀하는 이러한 개선과 관련된 로열티를 비롯한 어떤 보상도 받을 자격이 없습니다.

공급업체 법인 및 라이선스 소유자는 귀하 또는 제3자의 Password Manager Software 사용, 중개

회사 또는 중개인의 사용이나 미사용, 보안의 판매나 구입에 의해 야기되거나 관련해서 발생하는 어떤 종류의 손해 배상 청구 및 책임을 귀하에게 부과하지 않습니다. 이러한 손해 배상 청구 및 책임이 법적 또는 형평성 원칙을 따르는 경우에도 마찬가지입니다.

공급업체 법인 및 라이선스 소유자는 제3자 소프트웨어, Password Manager Software를 통해 액세스된 모든 데이터, Password Manager Software 또는 Password Manager Software를 통해 제공된 데이터의 사용 또는 사용이나 액세스할 수 없음으로 인해 야기되거나 이러한 데이터와 관련된 직접적, 우발적, 특수적, 간접적 또는 인과적 손해를 전혀 책임지지 않으며, 이러한 손해 배상 청구가 법률 또는 형평성 원칙에 따라 제기되어도 마찬가지입니다. 이 절에 명시되지 않은 손상에는 업무 수익의 손실, 개인이나 자산의 상해, 업무 중단, 업무 또는 개인 정보 손실이 포함되며 이에 국한되지 않습니다. 일부 관할권에서는 우발적이거나 인과적인 손상의 제한을 허용하지 않으므로 이러한 제한이 적용될 수도 있습니다. 이러한 경우 공급업체의 책임 한도는 관련 법률에 따라 허용되는 최소 수준이 됩니다.

주식 시세, 분석, 시장 정보, 뉴스 및 재무 데이터를 비롯하여 Password Manager Software를 통해 제공된 정보는 지연되거나, 부정확하거나, 오류 또는 누락을 포함할 수 있으며, 공급업체 주체 및 라이선스 소유자는 이와 관련해서 어떤 책임도 지지 않습니다. 공급업체는 Password Manager Software의 속성이나 Password Manager Software의 기능 또는 기술의 전체나 일부를 사전 예고 없이 변경하거나 중단할 수 있습니다.

본 문서의 조항이 여타의 이유로 인해 무효가 되거나 공급업체가 관련 법률에 따라 손실, 손상 등을 책임지게 될 경우, 계약 상대방은 공급업체의 책임이 귀하가 지불한 총 라이선스 비용으로 제한된다는 데 동의해야 합니다.

귀하는 이러한 계약 상대방이 Password Manager Software를 사용하여 발생할 수 있는 제3자(해당 권리가 Password Manager Software 또는 저장소에 사용된 데이터의 영향을 받는 장치 소유자 또는 계약 상대방 포함) 손해 배상 청구, 의무, 손상, 손실, 비용, 경비, 수수료에 대해 악의가 없는 공급업체 및 해당 직원, 자회사, 계열사, 리브랜딩 및 기타 계약 상대방을 면제하고, 방어하고, 보호한다는 데 동의해야 합니다.

3. Password Manager Software의 데이터. 명시적으로 귀하가 선택하지 않는 한, 귀하가 입력했으며 Password Manager Software 데이터베이스에 저장되는 모든 데이터는 사용자 컴퓨터에 암호화 형식으로 저장되거나 귀하가 지정한 다른 저장 장치에 저장됩니다. Password Manager Software 데이터베이스 또는 기타 파일이 삭제되거나 손상되는 경우 포함된 모든 데이터는 복구 불가능한 방식으로 손실된다는 사실과 이러한 손실에 대한 위험을 수락한다는 데 동의해야 합니다. 개인 데이터가 컴퓨터에 암호화된 형식으로 저장된다고 해서 데이터베이스를 열기 위해 마스터 패스워드를 알아내거나 고객이 정의한 활성화 장치에 액세스할 수 있게 된 누군가가 해당 정보를 훔치거나 남용할 수 없다는 것을 의미하지는 않습니다. 모든 액세스 방법의 보안 유지 관리에 대한 책임은 사용자에게 있습니다.

4. 공급업체 또는 저장소에 개인 데이터 전송. 시기 적절한 데이터 동기화 및 백업만을 위해 이렇게 하기로 선택하면 Password Manager Software는 Password Manager Software 데이터베이스에서 비밀번호, 로그인 정보, 계정 및 ID와 같은 개인 데이터를 인터넷을 통해 저장소로 전송하거나 보냅니다. 데이터는 암호화된 형식으로 단독 전송됩니다. 비밀번호, 로그인 또는 기타 데이터로 온라인 양식을 채우기 위해 Password Manager Software를 사용하면 해당 정보가 인터넷을 통해 사용자가 식별한 웹 사이트로 전송되어야 할 수 있습니다. 이러한 데이터 전송은 Password Manager

Software에 의해 시작되지 않으므로 공급업체가 여러 공급업체에서 지원하는 웹 사이트와의 이러한 상호 작용에 대한 보안을 책임지지 않을 수 있습니다. Password Manager Software 사용 여부에 관계없이 인터넷을 통해 진행되는 모든 트랜잭션은 사용자의 단독 책임이며 이러한 자료나 서비스의 다운로드 및/또는 사용으로 인한 컴퓨터 시스템의 손상이나 데이터의 손실에 대한 책임은 전적으로 사용자에게 있습니다. 귀중한 데이터를 손실할 위험을 최소화하기 위해 공급업체는 고객이 데이터베이스 및 기타 중요한 파일을 외부 드라이브에 주기적으로 백업할 것을 권장합니다. 공급업체는 손실되거나 손상된 데이터의 복구를 지원할 수 없습니다. 공급업체가 사용자 PC에 있는 파일이 손상되었거나 삭제된 경우 사용자 데이터베이스 파일의 백업 서비스를 제공하는 경우 이러한 백업 서비스에 대해 어떤 보증도 제공되지 않으며 이러한 제공이 공급업체의 의무는 아닙니다.

Password Manager Software를 사용할 경우 이 소프트웨어가 라이선스 정보, 사용 가능한 패치, 서비스 팩 및 Password Manager Software의 작동을 개선하거나, 유지 관리하거나, 수정하거나, 향상시킬 수 있는 기타 업데이트를 확인하기 위해 때때로 공급업체 서버에 연결할 수 있다는 데 동의하는 것으로 간주됩니다. 이 소프트웨어는 개인 정보 보호 정책에 따라 Password Manager Software의 작동과 관련된 일반 시스템 정보를 보낼 수 있습니다.

5. 제거 정보 및 지침. 데이터베이스에서 보존하려는 모든 정보는 Password Manager Software를 제거하기 전에 내보내야 합니다.

Password Manager Software에 대한 추가 조항은 ESET Smart Security Premium 최종 사용자에게만 적용됩니다.

ESET LiveGuard. 추가 조항은 다음과 같이 ESET LiveGuard에 적용됩니다.

소프트웨어는 최종 사용자가 제출한 파일의 추가 분석 기능을 포함합니다. 공급업체는 개인 정보 보호 정책 및 관련 법규에 따라 최종 사용자가 제출한 파일과 분석 결과만 사용해야 합니다.

ESET LiveGuard에 대한 추가 조항은 ESET Smart Security Premium 최종 사용자에게만 적용됩니다.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

개인 정보 보호 정책

개인 데이터 보호는 데이터 관리자인 ESET, spol. s r. o.(등록 사무소 소재지 Einsteinova 24, 851 01 Bratislava, Slovak Republic, 브라티슬라바 지방 법원 상업 등기소 등기, Sro국, 등기 번호: 3586/B, 사업자 등록 번호: 31333532) ('ESET' 또는 '당사')에 특히 중요합니다. 당사는 EU 일반 데이터 보호 규정('GDPR')에 따라 법적으로 표준화된 투명성 요건을 준수하고자 합니다. 당사는 이러한 목표를 달성하기 위해 데이터 주체인 고객('최종 사용자' 또는 '귀하')에게 아래의 개인 데이터 보호 주제에 관해 알리는 것을 유일한 목적으로 하는 본 개인 정보 보호 정책을 게시합니다.

- 개인 데이터 처리의 법적 근거
- 데이터 공유 및 기밀성
- 데이터 보안

- 데이터 주체의 권리
- 개인 데이터 처리
- 연락처 정보.

개인 데이터 처리의 법적 근거

개인 데이터의 보호와 관련된 해당 법률 프레임워크에 따라 당사가 데이터 처리에 사용하는 법적 근거는 단 몇 가지뿐입니다. ESET에서는 주로 다음을 이행하기 위해 개인 데이터를 처리합니다. [최종 사용자 사용권 계약](#) ('최종 사용자 사용권 계약'): 최종 사용자와 체결하며(6 (1) (b)항 GDPR), ESET 제품 또는 서비스의 제공에 적용됩니다(달리 명시적으로 언급한 경우 제외). 예:

- 합법적 이익 법적 근거(6 (1) (f)항 GDPR): 고객이 당사 서비스를 사용하는 방식과 고객 만족도에 대한 데이터를 처리하여 사용자에게 당사가 제공할 수 있는 최상의 보호 기능과 지원 서비스, 경험을 제공할 수 있도록 합니다. 마케팅도 해당 법률에서 합법적 이익으로 인정되므로, 당사는 고객과의 마케팅 통신 시 일반적으로 이를 사용합니다.
- 동의(6 (1) (a)항 GDPR): 당사가 이 법적 근거를 가장 적합한 근거로 간주하는 특정 상황이나 법률에서 요구하는 경우 귀하에게 요청할 수 있습니다.
- 법적 의무 준수(6 (1) (c)항 GDPR)(예: 전자 통신, 송장 또는 청구 문서 보관 요건 규정)

데이터 공유 및 기밀성

당사는 귀하의 데이터를 제3자와 공유하지 않습니다. 그러나 ESET은 영업, 서비스 및 지원 네트워크의 일환인 계열사 또는 파트너를 통해 전 세계적으로 운영되는 회사입니다. 라이선스, 청구 및 ESET에서 처리한 기술 지원 정보는 서비스 또는 지원 제공과 같은 최종 사용자 사용권 계약 이행을 목적으로 계열사 또는 파트너와 주고받을 수 있습니다.

ESET은 유럽 연합(EU) 내에서 데이터를 처리하는 것을 선호합니다. 그러나 귀하의 위치(EU 외부의 제품 및/또는 서비스 사용) 및/또는 귀하가 선택한 서비스에 따라 귀하의 데이터를 EU 외부의 국가로 전송해야 할 수 있습니다. 예를 들어 당사는 클라우드 컴퓨팅과 관련하여 제3자 서비스를 사용합니다. 이러한 경우 서비스 공급업체를 신중하게 선택하고 기술 및 조직적인 조치 외에도 계약상 조치를 통해 적절한 수준의 데이터 보호를 보장합니다. 당사는 일반적으로 EU 표준 계약 조항(필요한 경우 추가 계약 규정 포함)에 동의합니다.

영국, 스위스와 같이 EU에 가입하지 않은 일부 국가에 대해 EU는 이미 비슷한 수준의 데이터 보호를 결정했습니다. 데이터 보호 수준이 비슷하기 때문에 이들 국가로 데이터를 전송하는 데 특별한 승인이나 계약이 필요하지 않습니다.

데이터 보안

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 데이터 주체에 해당하는 침해 당사자인 최종 사용자뿐만 아니라 관련 감독 기관에 통지할 준비가 되어 있습니다.

데이터 주체 권한

모든 최종 사용자의 권리는 중요하며 당사는 모든 최종 사용자(EU 또는 EU 외 국가에 거주)가 ESET에서 보장되는 다음과 같은 권리를 보유하고 있음을 알려드리고자 합니다. 데이터 주체의 권리를 행사하기 위해 귀하는 지원 양식을 이용하거나 이메일(dpo@eset.sk)로 당사에 연락할 수 있습니다. 신원 확인을 위해 다음 정보를 요청합니다. 이름, 이메일 주소 및 사용 가능한 경우 라이선스 키 또는 고객 번호 및 소속 회사. 생년월일과 같은 다른 모든 개인 데이터 전송은 삼가주시기 바랍니다. 신원을 확인하고 귀하의 요청을 처리할 수 있도록 귀하의 개인 데이터를 처리할 것임을 알려드리고자 합니다.

동의를 철회할 권리. 동의를 철회할 권리는 동의를 기반으로 하는 처리인 경우에만 적용됩니다. 당사가 귀하의 동의를 근거로 귀하의 개인 데이터를 처리하는 경우, 귀하는 이유를 제시하지 않고 언제든지 동의를 철회할 권리가 있습니다. 동의 철회는 이후에 한해 유효하며 동의를 철회하기 전에 처리된 데이터의 적법성에는 영향을 미치지 않습니다.

이의 제기 권리. 처리에 반대할 수 있는 권리는 ESET 또는 제3자의 합법적 이익을 근거로 하는 처리인 경우에 적용됩니다. 당사가 합법적 이익을 보호하기 위해 개인 데이터를 처리하는 경우, 귀하는 데이터 주체로서 언제든지 당사가 주장하는 합법적 이익 및 귀하의 개인 데이터 처리에 이의를 제기할 권리가 있습니다. 이의 제기는 이후에 한해 유효하며 이의를 제기하기 전에 처리된 데이터의 적법성에는 영향을 미치지 않습니다. 당사가 다이렉트 마케팅 목적으로 귀하의 개인 데이터를 처리하는 경우 이의 제기 사유를 제시할 필요가 없습니다. 이는 다이렉트 마케팅과 관련이 있는 한 프로파일링에도 적용됩니다. 다른 모든 경우에 당사는 귀하의 개인 데이터 처리를 통한 ESET의 합법적 이익에 대한 귀하의 불만 사항을 간략하게 전달해 줄 것을 요청합니다.

경우에 따라 귀하가 동의를 철회했음에도 불구하고 당사는 계약의 이행과 같은 다른 법적 근거를 바탕으로 귀하의 개인 데이터를 추가로 처리할 권리가 있습니다.

정보 열람 권리. 귀하는 데이터 주체로서 언제든지 ESET에 저장된 귀하의 데이터에 대한 정보를 무료로 제공받을 권리가 있습니다.

데이터 수정 권리. 당사가 귀하에 대한 잘못된 개인 데이터를 실수로 처리하는 경우, 귀하는 수정을 요구할 권리가 있습니다.

삭제 권리 및 처리 제한 권리. 귀하는 데이터 주체로서 귀하의 개인 데이터 제거 또는 처리 제한을 요청할 권리가 있습니다. 예를 들어, 당사가 귀하의 동의를 얻어 귀하의 개인 데이터를 처리하는데 귀하가 동의를 철회하고 계약과 같은 다른 법적 근거가 없는 경우 당사는 즉시 귀하의 개인 데이터를 제거합니다. 귀하의 개인 데이터는 또한 보존 기간이 끝나 더 이상 명시된 목적을 위해 필요하지 않게 되는 즉시 제거됩니다.

당사가 다이렉트 마케팅 목적으로만 귀하의 개인 데이터를 사용하고 귀하가 동의를 철회하거나 근거가 되는 ESET의 합법적 이익에 이의를 제기한 경우, 당사는 원치 않는 접촉을 피하고자 귀하의 연락처 데이터를 내부 차단 목록에 포함하는 정도로만 귀하의 개인 데이터 처리를 제한할 것입니다. 그렇지 않으면 귀하의 개인 데이터를 제거합니다.

당사는 입법자 또는 감독 당국에서 발표한 보존 의무 및 기간이 만료될 때까지 귀하의 데이터를 보관해야 할 수 있음을 참고하시기 바랍니다. 보존 의무와 기간은 또한 슬로바키아 법률에 따라 발생 할 수도 있습니다. 그 후에는 해당 데이터가 정상적으로 제거됩니다.

데이터 이동성에 대한 권리. 데이터 주체인 귀하에게 ESET에서 처리한 귀하의 개인 데이터를 xls 형식으로 제공하게 되어 기쁘게 생각합니다.

불만 사항을 제기할 수 있는 권리. 귀하는 데이터 주체로서 언제든지 감독 기관에 불만 사항을 제기 할 권리가 있습니다. ESET은 슬로바키아 법률의 적용을 받으며 유럽 연합의 일원으로 데이터 보호 법을 준수해야 합니다. 관련 데이터 감독 당국은 슬로바키아의 개인 데이터 보호국(Hraničná 12, 82007 Bratislava 27, Slovak Republic 소재)입니다.

개인 데이터 처리

ESET에서 제공하는 서비스는 [EULA](#) 약관에 따라 당사의 제품 내에서 구현되지만 일부 서비스에는 특별한 주의가 필요할 수 있습니다. 당사의 서비스 제공과 관련된 데이터 수집에 대한 자세한 내용을 알려드리고자 합니다. 당사는 최종 사용자 사용권 계약과 제품 해당 [설명서](#)에서 각각의 자세한 사양의 작동 및 기능에 대한 정보 등)를 포함하되 이에 국한되지 않는 정보를 공급업체에 보냅니다. 모든 서비스를 제공하기 위해서는 다음 정보를 수집해야 합니다.

라이선스 및 청구 데이터. 이름, 이메일 주소, 라이선스 키와 (해당하는 경우) 주소, 소속 회사 및 지불 데이터는 라이선스 활성화, 라이선스 키 제공, 만료 시 알림, 지원 요청, 라이선스 정품 인증, 당사 서비스 및 관련 법률 또는 귀하의 동의에 따라 마케팅 메시지를 포함한 기타 알림의 제공이 가능 하도록 ESET에서 수집 및 처리합니다. ESET은 법적으로 10년 동안 청구 정보를 보관할 의무가 있지만 라이선스 정보는 라이선스 만료 후 12개월 이내에 익명화됩니다.

업데이트 및 기타 통계. 설치 프로세스 및 제품이 설치된 플랫폼을 비롯한 컴퓨터에 대한 정보가 처리 정보에 포함되며 운영 체제, 하드웨어 정보, 설치 ID, 라이선스 ID, IP 주소, MAC 주소, 제품 구성 설정 등과 같은 제품의 작동 및 기능에 대한 정보가 업데이트 및 업그레이드 서비스 제공 및 백엔드 인프라의 유지 관리, 보안 및 개선을 목적으로 처리됩니다.

이 정보는 최종 사용자 확인이 필요하지 않기 때문에 라이선스 및 청구 목적으로 필요한 신원 정보와 별도로 보관됩니다. 보존 기간은 최대 4년입니다.

ESET LiveGrid® 평판 시스템. 검사된 파일을 클라우드의 허용 목록 및 차단 목록 항목 DB와 비교하여 안티 맬웨어 솔루션의 효율성을 향상시키는 ESET LiveGrid® 평판 시스템을 실행하기 위해 침입 관련 단방향 해시를 처리합니다. 이 과정에서 최종 사용자를 식별하지 않습니다.

ESET LiveGrid® 피드백 시스템. 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, 스파이로 보고되었거나 당사 제품에 의해 플래그가 지정된 이메일 메시지)의 잠재적 샘플 등과 같은 침입 사항

- 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.

ESET LiveGrid® 피드백 시스템을 통해 수집 및 처리된 모든 정보는 최종 사용자 확인 없이 사용하도록 되어 있습니다.

네트워크 연결 장치 보안 평가. 당사는 보안 평가 기능을 제공하기 위해 로컬 네트워크 이름 및 로컬 네트워크 내 장치에 대한 정보(예: 로컬 네트워크에서 라이선스 정보와 연결된 장치의 존재 여부, 종류, 이름, IP 주소 및 MAC 주소)를 처리합니다. 이 정보에는 라우터 장치에 대한 무선 암호화 유형 및 무선 보안 유형도 포함됩니다. 최종 사용자를 확인하는 라이선스 정보는 라이선스 만료 후 12개월 이내에 익명화됩니다.

기술 지원. 지원 요청에 포함된 연락처 및 라이선스 정보와 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. 보다 원활한 지원 서비스를 제공하기 위해 그 이외의 정보를 제공해야 할 수도 있습니다. 기술 지원을 위해 처리된 데이터는 4년 동안 보관됩니다.

데이터 악용으로부터 보호. ESET HOME 계정을 <https://home.eset.com>에서 만들고 컴퓨터 도용 관련 기능을 최종 사용자가 활성화하는 경우 위치 데이터, 스크린샷, 컴퓨터 구성 데이터 및 컴퓨터 카메라에 기록된 데이터 정보가 수집 및 처리됩니다. 수집된 데이터는 보존 기간 3개월로 당사 서버 또는 당사 서비스 공급업체의 서버에 저장됩니다.

Password Manager. Password Manager 기능을 활성화하기로 하면 로그인 세부 정보 관련 데이터가 귀하의 컴퓨터 또는 다른 지정된 장치에만 암호화된 형식으로 저장됩니다. 동기화 서비스를 활성화하면 암호화된 데이터가 ESET의 서버 또는 서비스 공급자의 서버에 저장되어 이러한 서비스가 보장됩니다. ESET이나 서비스 공급자는 암호화된 데이터에 접근할 수 없습니다. 데이터를 복호화할 수 있는 키는 귀하에게만 제공됩니다. 기능을 비활성화하면 데이터가 제거됩니다.

ESET LiveGuard. ESET LiveGuard 기능을 활성화하려면 최종 사용자가 미리 정의하고 선택한 파일과 같은 샘플을 제출해야 합니다. 원격 분석을 위해 선택한 샘플은 ESET 서비스에 업로드되고 분석 결과가 귀하의 컴퓨터로 다시 전송됩니다. 감염 의심 샘플은 ESET LiveGrid® 피드백 시스템에서 수집한 정보의 방식으로 처리됩니다.

사용자 환경 개선 프로그램. 활성화를 선택한 경우 [사용자 환경 개선 프로그램](#), 당사의 제품 사용과 관련된 익명의 원격 분석 정보는 귀하의 동의에 따라 수집 및 사용됩니다.

당사의 제품 및 서비스를 사용하는 사람이 제품 또는 서비스를 구매하고 당사와 최종 사용자 사용권 계약을 체결한 최종 사용자가 아닌 경우(예: 최종 사용자의 직원, 가족 또는 달리 최종 사용자 사용권 계약에 따라 제품 또는 서비스를 사용하도록 최종 사용자의 허가를 받은 자) 6 (1) (f)항 GDPR

의 의미 범위 내에서 ESET의 합법적 이익을 위해 데이터 처리: 최종 사용자의 허가를 받은 사용자는 최종 사용자 사용권 계약에 따라 당사에서 제공하는 제품 및 서비스를 사용할 수 있습니다.

연락처 정보

데이터 주체로서 권한을 행사하고 싶거나 질문 또는 우려 사항이 있는 경우 다음 주소로 관련 내용을 보내 주십시오.

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk