ESET File Security

사용자 설명서

이 문서의 온라인 버전을 표시하려면 여기를 클릭

Digital Security
Progress. Protected.

Copyright ©2023 by ESET, spol. s r.o.

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

자세한 내용은 https://www.eset.com을 참조하십시오.

모든 권리 보유. 이 문서의 어떤 부분도 작성자의 서면 허가 없이 복제하거나, 검색 시스템에 저장하거나, 전자/기계적, 복사, 기록, 검사 등의 어떠한 수단 또는 형식으로 전송할 수 없습니다.

ESET, spol. s r.o.는 사전 통지 없이 설명된 애플리케이션 소프트웨어를 변경할 수 있는 권리를 보유합니다.

기술 지원: https://support.eset.com

REV. 2023년 3월 19일

1 서문 1
2 개요 2
2.1 주요 기능 2
2.2 새로운 기능 3
2.3 보호 유형 3
3 설치 준비 4
3.1 시스템 요구 사항 5
3.2 SHA-2 필수 호환성 6
3.3 ESET File Security 설치 단계 7
3.3 기존 설치 수정 10
3.4 자동/무인 설치 12
3.4 명령줄 설치 13
3.5 제품 활성화 15
3.5 ESET Business Account 17
3.5 제품 활성화 완료 17
3.5 활성화 오류 17
3.5 라이선스 17
3.6 최신 버전으로 업그레이드 18
3.6 ESMC를 통해 업그레이드 18
3.6 ESET 클러스터를 통해 업그레이드 21
3.7 클러스터 환경에서 설치 24
3.8 터미널 서버 24
4 시작 24
4.1 ESET Security Management Center를 통해 관리됨 25
4.2 모니터링 25
4.2 상태 27
4.2 Windows 업데이트 사용 가능 28
4.2 네트워크 격리 28
5 명령과 함께 ESET File Security 29
5.1 검사 30
5.1 검사 창 및 검사 로그 31
5.2 로그 파일 33
5.2 로그 필터링 36
5.3 업데이트 38
5.4 설정 40
5.4 서버 41
5.4 컴퓨터 42
5.4 네트워크 43
5.4 네트워크 문제 해결 마법사 44
5.4 웹 및 이메일 44
5.4 도구 - 진단 로깅 45
5.4 설정 가져오기 및 내보내기 46
5.5 도구 47
5.5 실행 중인 프로세스 48
5.5 감시 활동 50
5.5 보호 통계 51
5.5 클러스터 52
5.5 클러스터 마법사 - 노드 선택 54
5.5 클러스터 마법사 - 클러스터 설정 56
5.5 클러스터 마법사 - 클러스터 설정 56

5.5 클러스터 마법사 - 노드 확인 56
5.5 클러스터 마법사 - 노드 설치 58
5.5 ESET Shell 61
5.5 사용 63
5.5 명령 68
5.5 배치 파일/스크립팅 71
5.5 ESET SysInspector 72
5.5 ESET SysRescue Live 73
5.5 스케줄러 73
5.5 스케줄러 - 작업 추가 74
5.5 작업 유형 76
5.5 작업 타이밍 77
5.5 이벤트가 트리거됨 77
5.5 애플리케이션 실행 77
5.5 건너뛴 작업 78
5.5 예약된 작업 개요 78
5.5 분석용 샘플 전송 78
5.5 감염 의심 파일 79
5.5 감염 의심 사이트 79
5.5 가양성 파일 80
5.5 가양성 사이트 80
5.5 기타 81
5.5 검역소 81
5.6 OneDrive 검사 설정 82
5.6 ESET OneDrive 스캐너 등록 85
5.6 ESET OneDrive 스캐너 등록 취소 89
6 일반 설정 93
6.1 진단 엔진 94
6.1 머신 러닝 탐지 96
6.1 제외 98
6.1 성능 제외 98
6.1 탐지 제외 99
6.1 제외 생성 마법사 101
6.1 고급 옵션 101
6.1 자동 제외 항목 102
6.1 공유 로컬 캐시 102
6.1 침입이 검출됨 102
6.1 실시간 파일 시스템 보호 103
6.1 ThreatSense 파라미터 105
6.1 추가 ThreatSense 파라미터 109
6.1 검사에서 제외된 파일 확장명 109
6.1 프로세스 제외 109
6.1 클라우드 기반 보호 111
6.1 제외 필터 112
6.1 맬웨어 검사 113
6.1 프로필 관리자 115
6.1 프로필 대상 115
6.1 검사 대상 117
6.1 유휴 상태 검사 119
6.1 시작 검사 119
6.1 자동 시작 파일 검사 119

6.1 이동식 미디어 120
6.1 문서 보호 121
6.1 Hyper-V 검사 121
6.1 OneDrive 검사 123
6.1 HIPS 124
6.1 HIPS 규칙 설정 126
6.1 HIPS 고급 설정 129
6.2 업데이트 구성 129
6.2 업데이트 롤백 133
6.2 예약된 작업 - 업데이트 133
6.2 업데이트 미러 133
6.3 네트워크 보호 135
6.3 IDS 예외 137
6.3 일시적인 IP 주소 차단 목록 137
6.4 웹 및 이메일 137
6.4 프로토콜 필터링 138
6.4 웹 및 이메일 클라이언트 139
6.4 SSL/TLS 139
6.4 알려진 인증서 목록 140
6.4 암호화된 SSL 통신 141
6.4 이메일 클라이언트 보호 142
6.4 이메일 프로토콜 143
6.4 경고 및 알림 143
6.4 MS Outlook 도구 모음 144
6.4 Outlook Express 및 Windows Mail 도구 모음 144
6.4 확인 대화 상자 145
6.4 메시지 다시 검사 145
6.4 웹 브라우저 보호 145
6.4 URL 주소 관리 146
6.4 새 목록 생성 147
6.4 안티피싱 웹 보호 149
6.5 장치 제어 150
6.5 장치 규칙 150
6.5 장치 그룹 152
6.6 도구 구성 153
6.6 시간 슬롯 154
6.6 Microsoft Windows 업데이트 154
6.6 ESET CMD 154
6.6 ESET RMM 156
6.6 라이선스 157
6.6 WMI 공급자 157
6.6 제공된 데이터 158
6.6 제공된 데이터 접근 165
6.6 ERA/ESMC 검사 대상 166
6.6 재정의 모드 166
6.6 로그 파일 170
6.6 프록시 서버 171
6.6 알림 172
6.6 애플리케이션 알림 172
6.6 바탕 화면 알림 173
6.6 이메일 알림 173

6.6 사용자 지정 175
6.6 프레젠테이션 모드 176
6.6 분석 176
6.6 기술 지원 177
6.6 클러스터 177
6.7 사용자 인터페이스 179
6.7 경고 및 메시지 상자 180
6.7 접근 설정 180
6.7 ESET Shell 181
6.7 터미널 서버에서 GUI 비활성화 182
6.7 비활성화된 메시지 및 상태 182
6.7 애플리케이션 상태 설정 182
6.7 시스템 트레이 아이콘 183
6.8 기본 설정으로 되돌리기 184
6.9 도움말 및 지원 185
6.9 지원 요청 전송 186
6.9 ESET File Security 정보 187
6.10 용어집 187
7 최종 사용자 사용권 계약 187
8 개인정보처리방침 193

서문

이 설명서는 ESET File Security를 가장 효율적으로 사용할 수 있도록 하기 위해 작성되었습니다. 프로그램의 모든 창에 대해 자세히 알아보려면 해당 창이 열려 있는 동안 키보드에서 **F1** 키를 누르십시오. 그러면 현재 보고 있는 창에 대한 도움말 페이지가 표시됩니다.

일관성을 확보하고 혼동을 방지하기 위해 이 설명서 전체에서 사용된 용어는 ESET File Security 파라미터 이름을 기준으로 합니다. 또한 특정 관심 분야의 항목이나 중요한 항목을 강조하기 위해 일련의 균일한 기호가 사용되었습니다.

참고
참고는 잠깐 살펴보면 되는 내용입니다. 참고를 생략할 수는 있지만, 참고는 특정 기능이나 일부 관련 항목의 링크와 같은 중요한 정보를 제공할 수 있습니다.

중요
중요는 사용자의 주의가 필요하며 건너뛰지 않는 것이 좋습니다. 중요 메모에는 절대적으로 중요하지는 않지만 상당히 중요한 정보가 포함됩니다.

경고
많은 주의를 기울여 살펴봐야 할 중요한 정보입니다. 경고는 특히 사용자가 유해한 실수를 저지르지 않도록 배치되어 있습니다. 경고 괄호가 사용된 텍스트는 매우 중요한 시스템 설정이나 위험한 항목을 의미하므로 읽고 이해하십시오.

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

도움말 페이지의 오른쪽 위에 다음 요소가 보이면, 이는 ESET File Security 그래픽 사용자 인터페이스(GUI) 창 내의 탐색을 나타냅니다. 이러한 지침을 사용하여 각 도움말 페이지에서 설명하는 창으로 이동하십시오.

ESET File Security 열기
설정 > 서버 > *OneDrive* 검사 설정 > 등록 클릭

서식 지정 규칙:

규칙	의미
굵은 글꼴	섹션 제목, 기능 이름 또는 사용자 인터페이스 항목(예: 버튼)입니다.
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

규칙	의미
하이퍼링크	교차 참조된 항목이나 외부 웹 위치에 쉽고 빠르게 접근할 수 있습니다. 하이퍼링크는 파란색으로 강조 표시되고 밑줄이 그어져 있을 수 있습니다.
%ProgramFiles%	Windows 및 기타 설치된 프로그램이 저장된 Windows 시스템 디렉터리입니다.

ESET File Security 온라인 도움말 페이지는 여러 장과 하위 장으로 구성되어 있습니다. 도움말 페이지의 목차를 검색하여 관련 정보를 찾을 수 있습니다. 또는 단어나 구를 입력하여 전체 텍스트 검색을 사용할 수 있습니다.

개요

ESET File Security는 Microsoft Windows Server 환경용으로 특수 설계된 통합 솔루션입니다. ESET File Security에서는 다양한 유형의 악성코드를 강력하고 효율적으로 차단하며, 악성코드 방지 및 안티스파이웨어의 두 가지 보호 유형을 제공합니다.

주요 기능

다음 표에는 ESET File Security에서 사용할 수 있는 기능 목록이 나와 있습니다. ESET File Security는 독립 실행형 및 클러스터 환경에서 Microsoft Windows Server 2008 R2 SP1, 2012, 2016 및 2019의 대다수 버전을 지원합니다. 대규모 네트워크에서는 ESET Security Management Center를 사용하여 ESET File Security을(를) 원격으로 관리할 수 있습니다.

트루 64비트 제품 핵심	제품 핵심 구성 요소의 성능과 안정성을 더욱 높여 줍니다.
악성코드 방지	수상 경력에 빛나는() 악성코드에 대한 혁신적인 방어 수단인 이 첨단 기술()은 바이러스, 랜섬웨어, 루트킷, 웜 및 탐지율을 더 높이기 위한 클라우드 기반 검사 기능을 갖춘 스파이웨어 등 모든 유형의 위협을 제거하고 공격을 방지합니다. 공간은 적게 차지하면서도 성능은 저하시키지 않는 시스템 리소스에 적합합니다. 이 기술을 계층화된 보안 모델을 사용합니다. 각각의 계층 또는 단계에는 여러 핵심 기술이 내장되어 있습니다. 실행 전 단계에는 *UEFI* 스캐너, 네트워크 공격 보호, 평판 및 캐시, 제품 내장 샌드박스, *DNA* 탐지 등의 기술이 포함되어 있습니다. 실행 단계 기술로는 *Exploit* 차단, 랜섬웨어 보호, 고급 메모리 스캐너, 스크립트 스캐너*(AMSI)*가 있고, 실행 후 단계에서는 봇네트 보호, 클라우드 악성코드 보호 시스템, 샌드박싱을 사용합니다. 풍부한 기능을 갖춘 이 핵심 기술은 타의 추종을 불허하는 수준의 보호 능력을 보여줍니다.
OneDrive 검사	OneDrive 클라우드 저장 장치에 있는 파일을 검사할 수 있는 기능이 새로 추가되었습니다. Office 365 비즈니스 계정용 기능입니다.
Hyper-V 검사	특정 가상 컴퓨터(VM)에 "에이전트"를 설치하지 않고도 Microsoft Hyper-V Server에서 VM 디스크를 검사할 수 있는 새로운 기술입니다.
EDTD(ESET Dynamic Threat Defense)	클라우드 기반 서비스입니다. ESET File Security에서는 감염 의심 코드나 동작을 검출하면 이를 일시적으로 ESET Dynamic Threat Defense 검역소로 보내 추가적인 위협 활동을 방지합니다. 감염 의심 샘플은 ESET Dynamic Threat Defense 서버에 자동으로 전송되어 최신 악성코드 진단 엔진으로 분석됩니다. 그러면 ESET File Security에서 분석 결과를 받게 됩니다. 감염 의심 파일은 결과에 따라 처리됩니다.

트루 64비트 제품 핵심	제품 핵심 구성 요소의 성능과 안정성을 더욱 높여 줍니다.
ESET 클러스터	ESET 클러스터를 사용하면 한 위치에서 여러 서버를 관리할 수 있습니다. Microsoft Windows Server용 ESET File Security 6와 유사하며, 워크스테이션을 노드에 가입하면 모든 클러스터 구성원 전체에 걸쳐 하나의 구성 정책을 배포할 수 있으므로 추가로 관리를 자동화할 수 있게 됩니다. 클러스터 자체 생성은 설치된 노드를 사용하여 수행되며, 클러스터가 생성되고 나면 모든 노드를 원격으로 설치 및 시작할 수 있습니다. ESET 서버 제품은 서로 통신하며 구성 및 알림 등의 데이터를 교환할 수 있을 뿐 아니라, 제품 인스턴스 그룹의 적절한 작업에 필요한 데이터를 동기화할 수 있습니다. 이로써 클러스터의 모든 구성원에 대해 동일한 제품 구성을 적용할 수 있습니다. ESET File Security에서는 Windows 장애 조치(Failover) 클러스터 및 NLB(네트워크 부하 분산) 클러스터를 지원합니다. 또한 특정 Windows 클러스터 없이 ESET 클러스터 구성원을 수동으로 추가할 수 있습니다. ESET 클러스터는 도메인 환경과 작업 그룹 환경에서 모두 작동합니다.
자동 제외 항목	원활한 작동과 성능을 제공하기 위해 중요한 애플리케이션과 서버 파일을 자동으로 검출 및 제외합니다.
프로세스 제외	악성코드 방지 접근 시 검사에서 특정 프로세스를 제외합니다. 악성코드 방지 접근 시 검사는 백업 프로세스 또는 가상 컴퓨터의 실시간 마이그레이션 작업 중과 같은 특정 상황에서 충돌할 수 있습니다. 프로세스를 제외하면 이러한 잠재적 충돌 위험을 최소화하고 제외된 애플리케이션의 성능을 향상시켜 전체 시스템의 전반적인 성능과 안정성에 긍정적인 효과를 가져다줄 수 있습니다. 프로세스/애플리케이션을 제외하면 실행 파일(*.exe*)이 제외됩니다.
eShellESET Shell	eShell 2.0은 고급 사용자와 관리자에게 ESET 서버 제품을 관리하는 더욱 포괄적인 옵션을 제공하는 명령줄 인터페이스입니다.
ESET Security Management Center	수동 검사 예약 기능을 포함하여 ESET Security Management Center와의 통합 성능이 향상됩니다. 자세한 내용은 ESET Security Management Center 온라인 도움말을 참조하십시오.
구성 요소 기반 설치	설치 시 선택한 제품 부분만 포함하도록 사용자 지정할 수 있습니다.

새로운 기능

ESET File Security에 새로 추가된 기능은 다음과 같습니다.

- 트루 64비트 제품 핵심
- OneDrive 검사
- EDTD(ESET Dynamic Threat Defense)
- ESET Enterprise Inspector 지원
- ESET RMM
- 머신 러닝 탐지

보호 유형

다음과 같은 두 가지 보호 유형이 있습니다.

- 악성코드 방지 보호
- 안티스파이웨어 보호

악성코드 방지, 안티스파이웨어 보호는 ESET File Security 제품의 기본적인 기능 중 하나로, 파일, 이메일 및 인터넷 통신을 제어하여 악의적인 시스템 공격으로부터 보호합니다. 위협이 발견되면 탐지 모듈은 위협을

차단한 후 치료, 삭제하거나 검역소로 보내 위협을 제거할 수 있습니다.

설치 준비

제품 설치를 준비하는 데 권장되는 몇 가지 단계가 있습니다.

- ESET File Security를 구입한 후 ESET 웹 사이트에서 .msi 설치 패키지를 다운로드합니다.
- ESET File Security를 설치할 계획인 서버가 시스템 요구 사항을 충족하는지 확인합니다.
- 관리자 계정을 사용하여 서버에 로그온합니다.

> 참고
> 기본 제공 관리자 계정 또는 도메인 관리자 계정(로컬 기관리자 계정이 비활성화된 경우)에서 설치 프로그램을 실행해야 합니다. 다른 사용자의 경우 관리자 그룹 구성원이더라도 해당하는 접근 권한이 없습니다. 따라서 로컬 또는 도메인 관리자 이외의 다른 사용자 계정으로는 설치를 완료할 수 없으므로 기본 제공 관리자 계정을 사용해야 합니다.

- 기존 ESET File Security 설치에서 업그레이드하려는 경우 설정 내보내기 기능을 사용하여 현재 구성을 백업하는 것이 좋습니다.
- 해당하는 경우 시스템에서 타사 안티바이러스 소프트웨어를 제거합니다. ESET AV Remover를 사용하는 것이 좋습니다. ESET AV Remover를 사용하여 제거할 수 있는 타사 안티바이러스 소프트웨어 목록은 이 KB 문서를 참조하십시오.
- ESET File Security을 Windows Server 2016에 설치하는 경우 Microsoft에서는 시스템에 안티바이러스 제품이 여러 개 설치되어 발생하는 문제를 막으려면 Windows Defender 기능을 제거하고 Windows Defender ATP 등록에서 철회하는 것을 권장합니다.

두 가지 설치 모드에서 ESET File Security 설치 관리자를 실행할 수 있습니다.

- GUI(그래픽 사용자 인터페이스)
  설치 마법사에서 권장되는 설치 유형입니다.
- 자동/무인 설치
  설치 마법사 이외에도 명령줄을 통해 ESET File Security를 자동으로 설치하도록 선택할 수 있습니다.

> 중요
> 가능한 경우 ESET File Security를 새로 설치 및 구성한 OS에 설치하는 것이 좋습니다. 기존 시스템에 설치해야 하는 경우 이전 버전의 ESET File Security를 제거하고 서버를 다시 시작한 후 새 ESET File Security를 설치하는 것이 좋습니다.

- 최신 버전으로 업그레이드
  이전 버전의 ESET File Security를 사용하는 경우 적절한 업그레이드 방법을 선택할 수 있습니다.

ESET File Security를 설치 또는 업그레이드한 후의 추가 동작은 다음과 같습니다.

- 제품 활성화
  활성화 창에서 특정 활성화 시나리오를 사용할 수 있는지 여부는 국가와 배포 방법에 따라 달라질 수 있습니다.

- 일반 설정 구성

필요에 맞게 각 기능의 고급 설정을 수정하여 ESET File Security를 미세 조정할 수 있습니다.

시스템 요구 사항

지원되는 운영 체제:

- Microsoft Windows Server 2019(Server Core 및 데스크톱 환경)
- Microsoft Windows Server 2016 (Server Core 및 데스크톱 환경)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- KB4474419 및 KB4490628이 설치된 Microsoft Windows Server 2008 R2 SP1
- Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2, 2016)

> 참고
> Microsoft Windows Server 2008 R2 SP1을 실행 중인 경우 SHA-2 필수 호환성을 읽고 운영 체제에 필요한 모든 패치가 적용되었는지 확인하십시오.

Storage, Small Business 및 MultiPoint Server:

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2012

- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation
- KB4474419 및 KB4490628이 설치된 Microsoft Windows Small Business Server 2011 SP1 (x64)

- Microsoft Windows MultiPoint Server 2012
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2010

Hyper-V 역할이 있는 지원되는 호스트 운영 체제:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 - 가상 컴퓨터는 오프라인 상태에서만 검사할 수 있습니다.

하드웨어 요구 사항은 사용 중인 운영 체제 버전에 따라 다릅니다. Microsoft Windows Server 제품 설명서에서 하드웨어 요구 사항에 대한 자세한 내용을 읽어 보는 것이 좋습니다.

참고
ESET 보안 제품을 설치하기 전에 Microsoft Server 운영 체제 및 서버 애플리케이션용 최신 서비스 팩을 설치하는 것이 좋습니다. 또한 사용 가능한 경우 항상 최신 Windows 업데이트와 핫픽스를 설치하는 것이 좋습니다.

최소 하드웨어 요구 사항:

구성 요소	요구 사항
프로세서	Intel 또는 AMD 단일 코어 x86 또는 x64
메모리	사용 가능한 메모리 256MB
하드 드라이브	사용 가능한 디스크 공간 700MB
화면 해상도	800 x 600픽셀 이상

SHA-2 필수 호환성

Microsoft는 SHA-1(Secure Hash Algorithm 1)의 사용 중단을 발표하고 2019년 초 SHA-2로의 마이그레이션 프로세스를 시작했습니다. 그러므로 SHA-1 알고리즘을 사용해 서명한 모든 인증서가 더 이상 인식되지 않고 보안 경고가 발생하게 됩니다. 그러나 안타깝게도 SHA-1 해시 알고리즘의 보안 성능은 알고리즘에서 발견된 약점과 향상된 프로세서 성능, 클라우드 컴퓨팅의 출현으로 인해 시간이 지남에 따라 약화되었습니다.

SHA-1의 후속 버전인 SHA-2 해시 알고리즘은 현재 SSL 보안 내구성을 보장하기 위해 선호되는 방법이 되었습니다. 자세한 내용은 해시 및 서명 알고리즘()에 대한 Microsoft 문서를 참조하십시오.

참고
이 같은 변화는 SHA-2 지원이 없는 운영 체제에서 ESET 보안 솔루션이 더 이상 탐지 엔진 등의 모듈을 업데이트할 수 없게 되어 결국 ESET File Security이(가) 완전히 기능하지 않고 충분한 보호 성능을 제공할 수 없게 됨을 의미한다.

Microsoft Windows Server 2008 R2 SP1 또는 **Microsoft Windows Small Business Server 2011 SP1**을 실행하는 경우 시스템이 SHA-2와 호환되는지 확인하십시오. 다음과 같이 특정 운영 체제 버전에 따라 패치를 적용합니다.

- **Microsoft Windows Server 2008 R2 SP1** — KB4474419 또는 KB4490628(추가로 시스템을 다시 시작해야 할 수 있음) 적용
- **Microsoft Windows Small Business Server 2011 SP1**(x64) — KB4474419 및 KB4490628(추가로 시스템을 다시 시작해야 할 수 있음) 적용

중요
업데이트를 설치하고 시스템을 다시 시작한 후 ESET File Security GUI를 열어 상태를 확인합니다. 상태가 주황색인 경우 추가로 시스템을 다시 시작합니다. 그러면 상태가 최대 보호 성능을 나타내는 녹색으로 바뀝니다.

참고
Microsoft Server 운영 체제 및 서버 애플리케이션용 최신 서비스 팩을 설치하는 것이 좋습니다. 또한 사용 가능한 경우 항상 최신 Windows 업데이트와 핫픽스를 설치하는 것이 좋습니다.

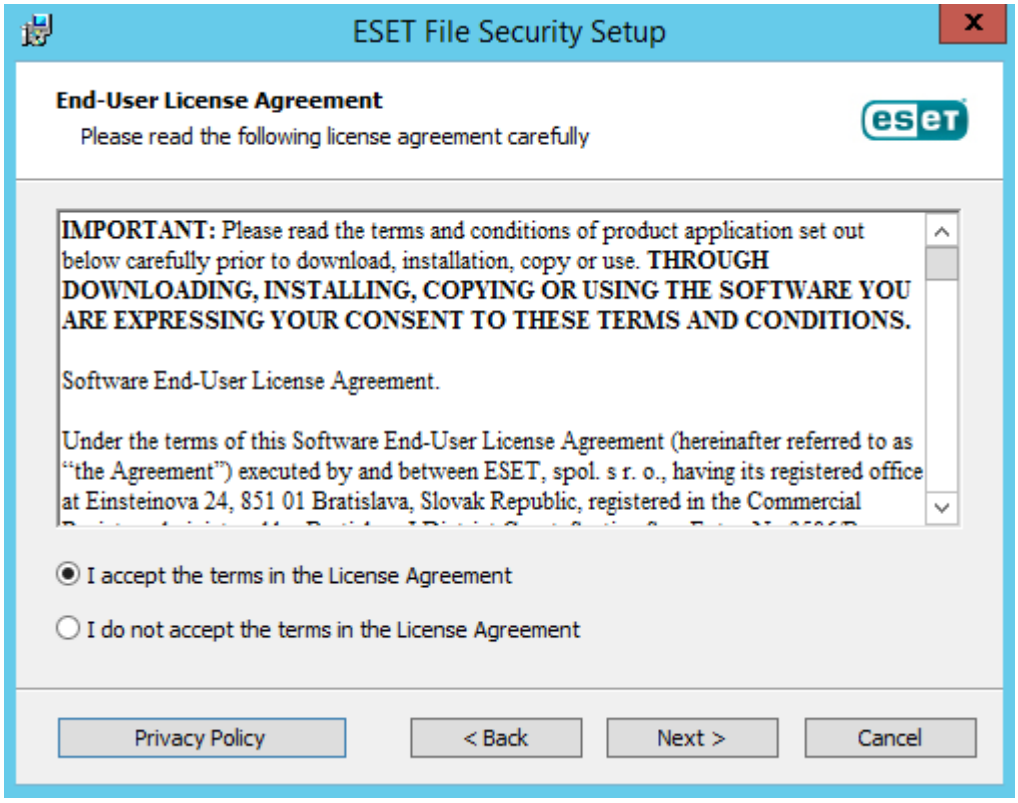
ESET File Security 설치 단계

일반적인 GUI 설치 마법사입니다. ESET File Security를 설치하려면 `.msi` 패키지를 두 번 클릭하고 아래 단계를 따릅니다.

1. 계속하려면 **다음**을 클릭하고 설치를 종료하려면 **취소**를 클릭합니다.

2. 설치 마법사는 사용 중인 운영 체제의 **지역 > 위치** 설정 중 **홈 위치**(또는 기존 시스템의 **지역 및 언어 > 위치** 중 **현재 위치**)로 지정되어 있는 언어로 실행됩니다. 드롭다운 메뉴를 사용하여 ESET File Security를 설치할 **제품 언어**를 선택합니다. 선택한 ESET File Security 언어는 설치 마법사에 표시되는 언어와 무관합니다.

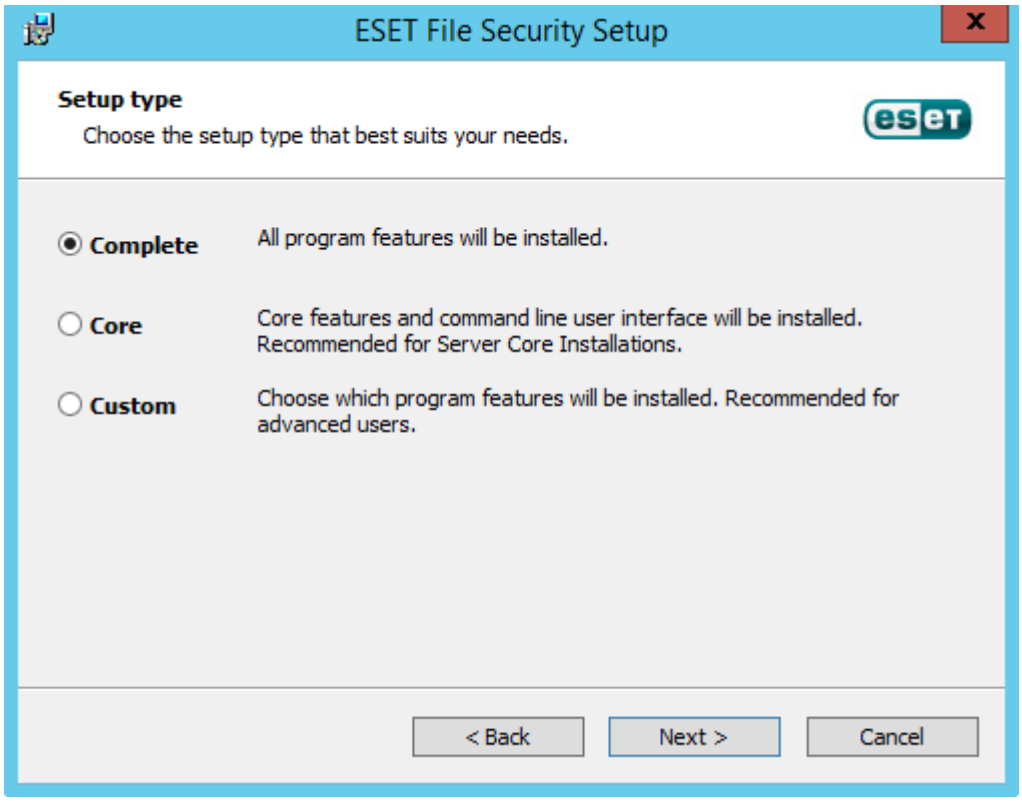
3. **다음**을 클릭하면 최종 사용자 사용권 계약이 표시됩니다. **최종 사용자 사용권 계약**(EULA)과 개인정보 보호 정책의 수락을 확인하고 **다음**을 클릭합니다.



4.사용 가능한 설치 유형 중 하나를 선택합니다(사용 가능 여부는 운영 체제에 따라 다름).

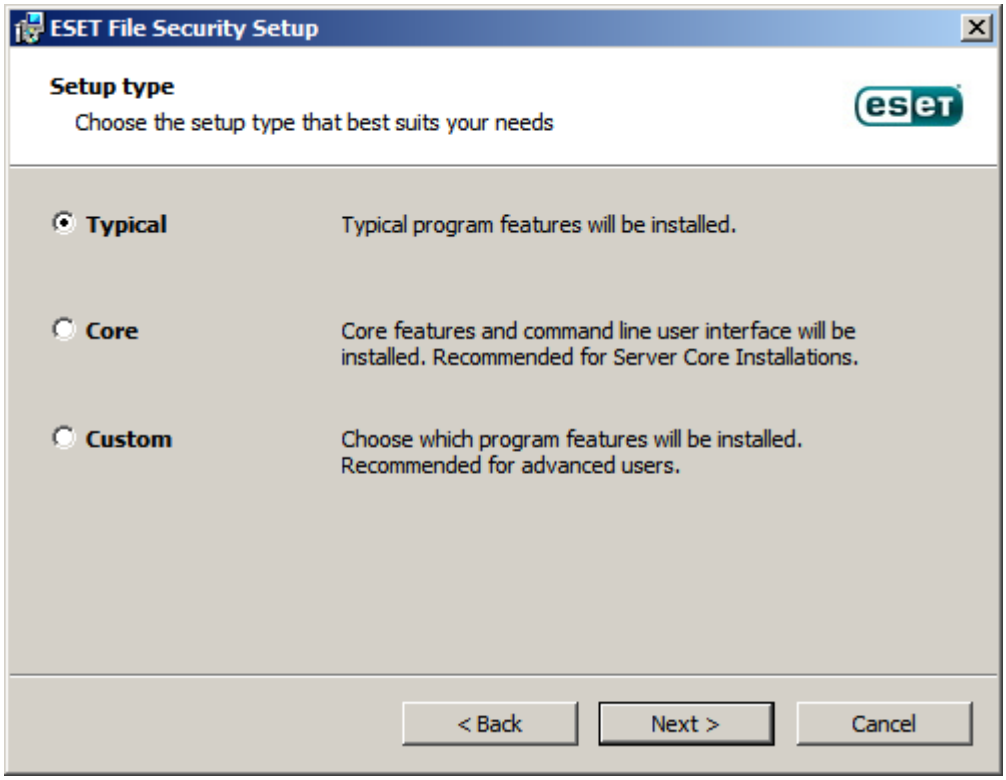
전체

모든 ESET File Security 기능을 설치합니다. 전체 설치(full installation)라고도 합니다. 권장되는 설치 유형으로, **Windows Server 2012, 2012 R2, 2016, 2019, Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials 및 2019 Essentials**에서 사용할 수 있습니다.



표준

권장되는 ESET File Security 기능을 설치합니다. 2008 R2 SP1 및 2011에서 사용할 수 있습니다.



주요

이 설치 유형은 Windows Server Core Edition용입니다. 설치 단계는 전체 설치와 동일하지만, 주요 기능만 제공되며 명령줄 사용자 인터페이스가 설치됩니다. 주요 설치는 주로 Windows Server Core에서 사용되지만, 원하는 경우 일반적인 Windows Server에도 이를 설치할 수 있습니다. 주요 설치를 사용하여 설치된 ESET 보안 제품에는 GUI가 포함되지 않습니다. 즉, ESET File Security로 작업할 때에는 명령줄 사용자 인터페이스만 사용할 수 있습니다. 자세한 내용과 기타 특수 파라미터에 대해서는 명령줄 설치 섹션을 참조하십시오.

예
명령줄을 통해 주요 설치를 실행하려면 다음 샘플 명령을 사용합니다.

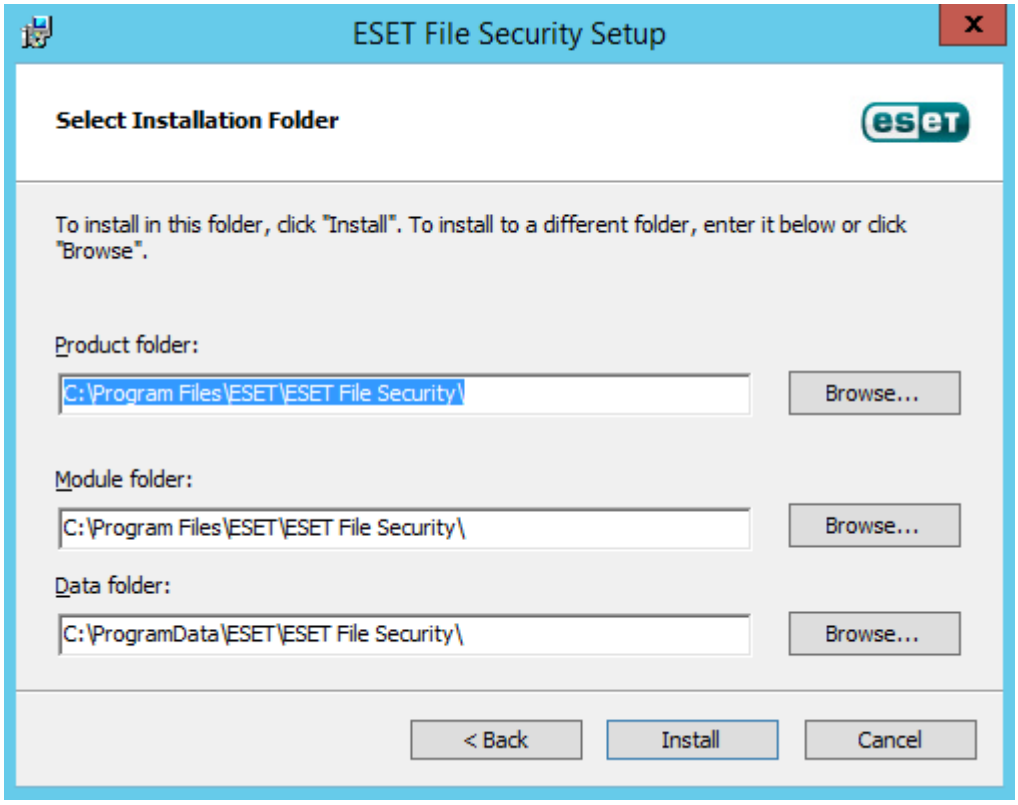
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base
```

사용자 지정

시스템에 설치할 ESET File Security 기능을 선택할 수 있습니다. 설치를 시작하기 전에 제품 모듈 및 기능 목록이 표시됩니다. 필요한 구성 요소만 포함하도록 ESET File Security를 사용자 지정하려는 경우에 유용합니다.

참고
Windows Server 2008 R2 SP1에서 **네트워크 보호** 구성 요소의 설치는 기본적으로 비활성화됩니다(**표준** 설치). 이 구성 요소를 설치하려면 **사용자 지정** 설치 유형을 선택합니다.

5.ESET File Security가 설치될 위치를 선택하라는 메시지가 표시됩니다. 기본적으로 이 프로그램은 C:*Program Files**ESET**ESET File Security*에 설치됩니다. 이 위치를 변경하려면 **찾아보기**를 설치합니다(권장되지 않음).



6. 설치를 시작하려면 **설치**를 클릭합니다. 설치를 완료하면 ESET GUI가 시작되고 알림 영역(시스템 트레이)에 트레이 아이콘 이 표시됩니다.

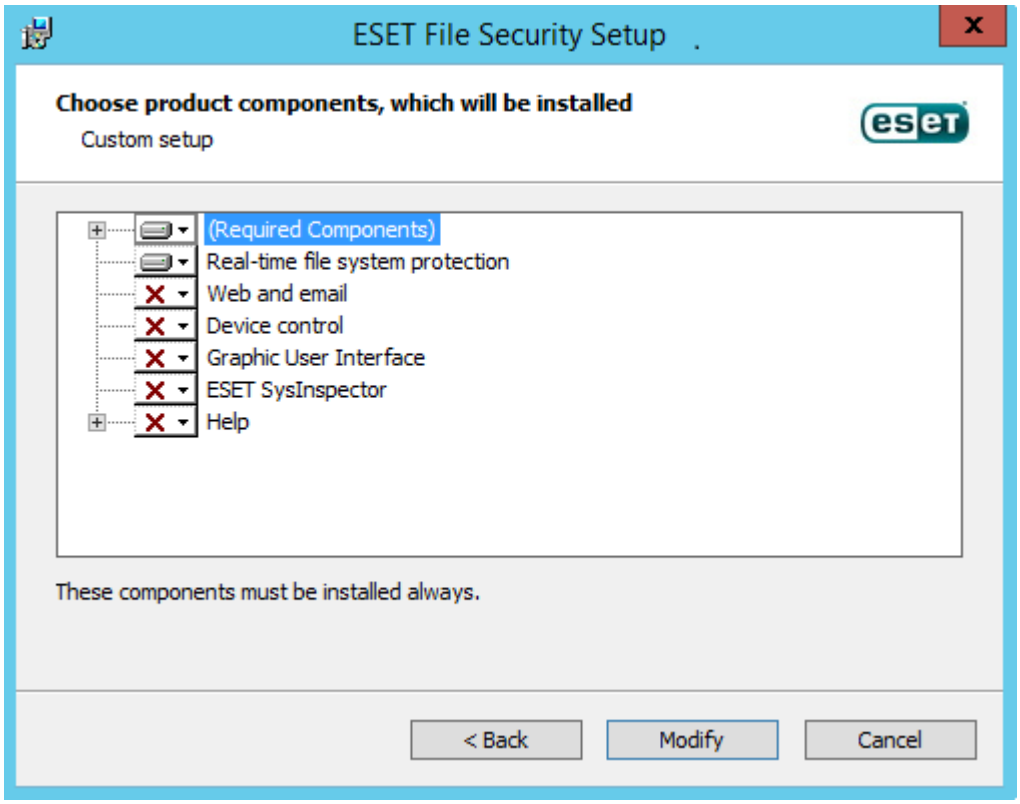
기존 설치 수정

설치에 포함된 구성 요소를 추가하거나 제거할 수 있습니다. 이렇게 하려면 초기 설치 중에 사용한 `.msi` 설치 관리자 패키지를 실행하거나, **프로그램 및 기능**(Windows 제어판에서 접근 가능)으로 이동한 후 ESET File Security를 오른쪽 마우스 버튼으로 클릭하고 **변경**을 선택합니다. 아래 단계에 따라 구성 요소를 추가하거나 제거합니다.

세 가지 옵션을 사용할 수 있습니다. 즉, 설치된 구성 요소를 **수정**하거나, 설치된 ESET File Security를 **복구**하거나, 완전히 **제거**할 수 있습니다.

수정을 선택하면 사용 가능한 프로그램 구성 요소 목록이 표시됩니다.

추가하거나 제거할 구성 요소를 선택합니다. 여러 구성 요소를 한꺼번에 추가/제거할 수 있습니다. 다음 그림과 같이 구성 요소를 클릭한 다음 드롭다운 메뉴에서 옵션을 선택합니다.



옵션을 선택했으면 **수정**을 클릭하여 수정 작업을 수행합니다.

참고
언제든지 설치 관리자를 실행하여 설치된 구성 요소를 수정할 수 있습니다.대다수 구성 요소의 경우 변경 사항을 적용하기 위해 서버를 다시 시작하지 않아도 됩니다. GUI가 다시 시작되고 설치하도록 선택한 구성 요소만 표시됩니다. 서버를 다시 시작해야 하는 구성 요소의 경우 Windows 설치 관리자에서 서버를 다시 시작하라는 메시지를 표시하며, 서버가 온라인 상태로 바뀌면 새 구성 요소가 사용 가능한 상태가 됩니다.

자동/무인 설치

다음 명령을 실행하여 명령줄을 통해 설치를 완료합니다. `msiexec /i <packagename> /qn /l*xv msi.log`

참고
Windows Server 2008 R2 SP1에는 **네트워크 보호** 기능이 설치되지 않습니다.

정상적으로 설치되었는지 확인하려는 경우 또는 설치 문제가 발생한 경우에는Windows 이벤트 뷰어를 사용해 **애플리케이션 로그**(소스: MsiInstaller에서 레코드 검색)를 확인합니다.

예
64비트 시스템에 **전체 설치**:
```
msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

설치를 완료하면 ESET GUI가 시작되고 알림 영역(시스템 트레이)에 트레이 아이콘 이 표시됩니다.

예
특정 언어(독일어)로 제품 설치:
```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
자세한 내용과 언어 코드 목록은 명령줄 설치에서 **언어 파라미터**를 참조하십시오.

중요
`REINSTALL` 파라미터 값을 지정할 때 `ADDLOCAL` 또는 `REMOVE` 파라미터 값으로 사용되지 않는 나머지 기능을 나열해야 합니다. `REINSTALL`, `ADDLOCAL`, `REMOVE` 파라미터 값으로 모든 기능을 나열하려면 명령줄 설치를 제대로 실행해야 합니다. `REINSTALL` 파라미터 값을 사용하지 않으면 추가 또는 제거가 완료되지 않을 수 있습니다.
전체 기능 목록은 명령줄 설치 섹션을 참조하십시오.

예
64비트 시스템에서 **전체 제거**(제거):
```
msiexec /x efsw_nt64.msi /qn /l*xv msi.log
```

참고
정상적으로 제거되면 서버가 자동으로 재부팅됩니다.

명령줄 설치

다음 설정은 사용자 인터페이스의 **감소**, **기본** 및 **없음** 수준으로만 사용해야 합니다. 해당 명령줄 스위치에 사용되는 **msiexec** 버전에 대해서는 설명서를 참조하십시오.

지원되는 파라미터:

APPDIR=<path>

- 경로 - 유효한 디렉터리 경로
- 애플리케이션 설치 디렉터리입니다.
- 예를 들어 다음과 같습니다. `efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

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

MODULEDIR=<path>

- 경로 - 유효한 디렉터리 경로
- 모듈 설치 디렉터리입니다.

ADDLOCAL=<list>

- 구성 요소 설치 - 로컬로 설치할 비필수 기능 목록입니다.
- ESET `.msi` 패키지에서 사용: `efsw_nt64.msi /qn ADDLOCAL=<list>`
- `ADDLOCAL` 속성에 대한 자세한 내용은 https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal를 참조하십시오.
- `ADDLOCAL` 목록은 설치할 모든 기능이 쉼표로 구분된 목록입니다.
- 설치된 기능을 선택하면 전체 경로(모든 상위 기능)가 목록에 명시적으로 포함되어야 합니다.

REMOVE=<list>

- 구성 요소 설치 - 로컬에 설치하지 않으려는 상위 기능.
- ESET `.msi` 패키지에서 사용: `efsw_nt64.msi /qn REMOVE=<list>`
- `REMOVE` 속성에 대한 자세한 내용은 https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal를 참조하십시오.
- `REMOVE` 목록은 설치하지 않을(또는 기존 설치인 경우 제거할) 상위 기능을 쉼표로 구분한 목록입니다.
- 상위 기능만 지정하는 것으로 충분합니다. 목록에 모든 하위 기능을 명시적으로 포함할 필요는 없습니다.

ADDEXCLUDE=<list>

- `ADDEXCLUDE` 목록은 설치되지 않은 모든 기능 이름을 쉼표로 구분한 목록입니다.
- 설치되지 않은 기능을 선택한 경우 전체 경로(즉, 모든 하위 기능) 및 표시되지 않은 관련 기능이 목록에 명시적으로 포함되어야 합니다.
- ESET `.msi` 패키지에서 사용: `efsw_nt64.msi /qn ADDEXCLUDE=<list>`

> 참고
> ADDEXCLUDE는 ADDLOCAL과 함께 사용할 수 없습니다.

기능 상태

- **필수** - 해당 기능이 항상 설치됩니다.
- **옵션** - 해당 기능을 설치하지 않도록 선택을 취소할 수 있습니다.
- **숨김** - 다른 기능이 제대로 작동하기 위한 필수 논리 기능입니다.

ESET File Security 기능 목록:

> 중요
> 모든 기능 이름은 대소문자를 구분합니다. 예를 들어 RealtimeProtection은 REALTIMEPROTECTION과 같지 않습니다.

기능 이름	기능 상태
SERVER	필수
RealtimeProtection	필수
WMIProvider	필수
HIPS	필수
Updater	필수
eShell	필수
UpdateMirror	필수
DeviceControl	옵션
DocumentProtection	옵션
WebAndEmail	옵션
ProtocolFiltering	숨김
NetworkProtection	옵션
IdsAndBotnetProtection	옵션
Rmm	옵션
WebAccessProtection	옵션
EmailClientProtection	옵션
MailPlugins	숨김
Cluster	옵션
_Base	필수
eula	필수
ShellExt	옵션
_FeaturesCore	필수
GraphicUserInterface	옵션
SysInspector	옵션
SysRescue	옵션
EnterpriseInspector	옵션

다음 기능 중 하나를 제거하려면 해당 그룹에 속하는 모든 그룹을 지정해서 전체 그룹을 제거해야 합니다.

그렇지 않으면 해당 기능이 제거되지 않습니다. 여기에는 두 그룹이 나와 있습니다(각 줄이 하나의 그룹을 나타냄).

```
GraphicUserInterface,ShellExt

NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

예
REMOVE 파라미터를 사용하고 상위 기능만 지정하여 설치에서 **NetworkProtection** 섹션(하위 기능 포함)을 제외합니다.
```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```
또는 ADDEXCLUDE 파라미터를 사용할 수 있지만 모든 하위 기능도 지정해야 합니다.
```
msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

예
주요 설치 예:
```
msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm
```

설치 후 ESET File Security를 자동으로 구성되도록 하려면 설치 명령 내에서 기본 구성 파라미터를 지정할 수 있습니다.

예
ESET File Security 설치 및 ESET LiveGrid® 비활성화:
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

모든 구성 속성 목록:

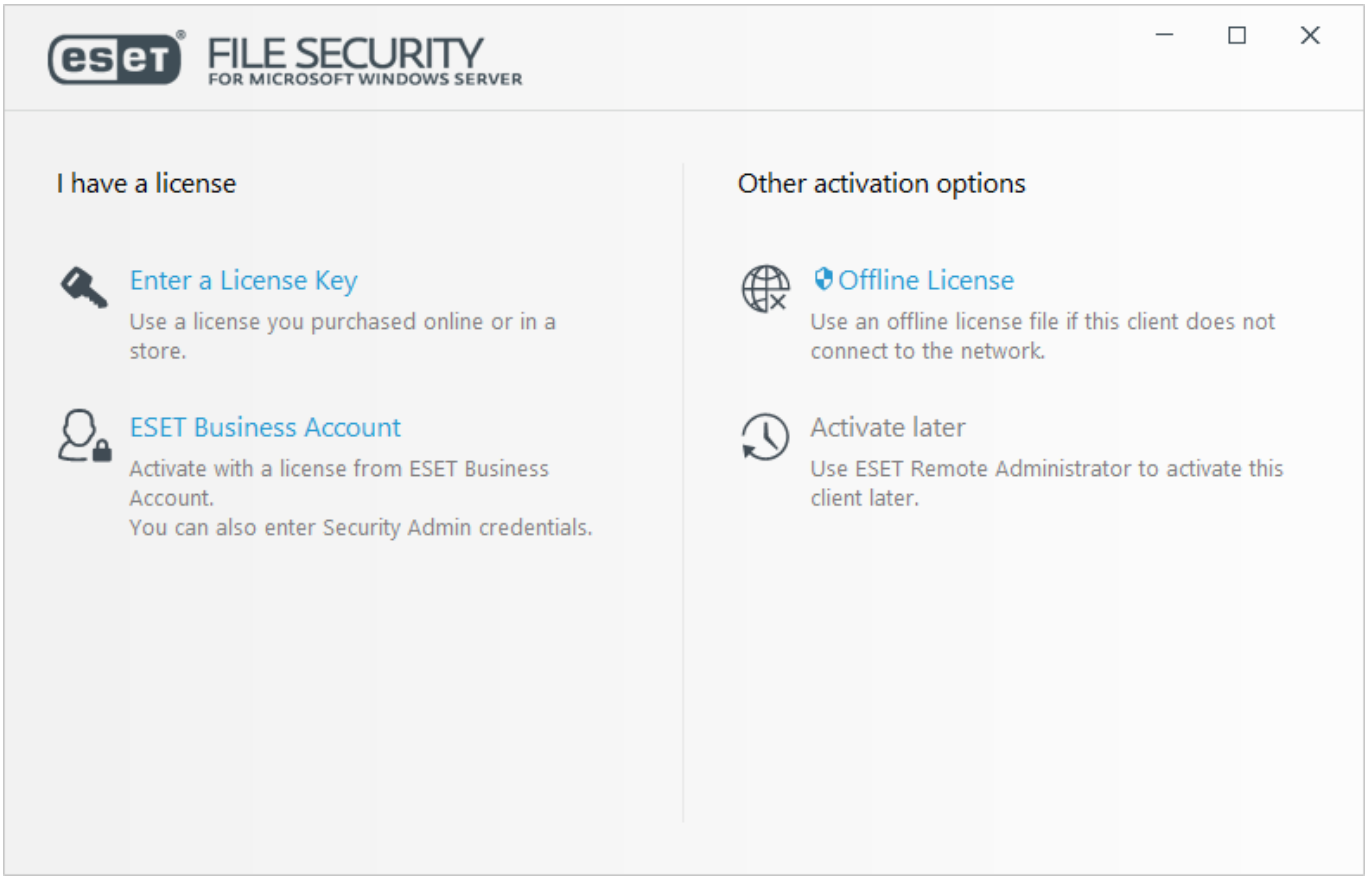
스위치	값
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 - 비활성화됨, 1 - 활성화됨
CFG_LIVEGRID_ENABLED=1/0	0 - 비활성화됨, 1 - 활성화됨
FIRSTSCAN_ENABLE=1/0	0 - 비활성화, 1 - 활성화
CFG_PROXY_ENABLED=0/1	0 - 비활성화됨, 1 - 활성화됨
CFG_PROXY_ADDRESS=<ip>	프록시 IP 주소입니다.
CFG_PROXY_PORT=<port>	프록시 포트 번호입니다.
CFG_PROXY_USERNAME=<user>	인증을 위한 사용자 이름입니다.
CFG_PROXY_PASSWORD=<pass>	인증을 위한 비밀번호입니다.

언어 파라미터: 제품 언어(두 파라미터를 모두 지정해야 함)

스위치	값
PRODUCT_LANG=	LCID 십진수(로캘 ID, 예: *English - United States*의 경우 1033)는 언어 코드 목록을 참조하십시오.
PRODUCT_LANG_CODE=	소문자의 LCID 문자열(언어 문화권 이름, 예: *English - United States*의 경우 en-us)은 언어 코드 목록을 참조하십시오.

제품 활성화

완료되면 제품을 활성화할 것인지 묻는 메시지가 표시됩니다.



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

라이선스 키 입력

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

ESET Business Account

사용자가 등록되어 있고 ESET File Security 라이선스를 가져온 EBA(ESET Business Account)를 보유하고 있는 경우 이 옵션을 사용합니다. ESET 라이선스 관리자 포털에서 사용하는 **보안 관리** 자격 증명을 입력할 수도 있습니다.

오프라인 라이선스 파일

라이선스 정보를 제공하기 위해 ESET 제품으로 전송될 자동 생성 파일입니다. 오프라인 라이선스 파일은 라이선스 포털에서 생성되며, 애플리케이션이 라이선스 기관에 연결할 수 없는 환경에서 사용됩니다.

컴퓨터가 관리되는 네트워크의 구성원이고 관리자가 ESET Security Management Center를 통해 원격 활성화를 수행할 경우 ESET Security Management Center로 **나중에 활성화**를 클릭합니다. 나중에 이 클라이언트를 활성화하려는 경우에도 이 옵션을 사용할 수 있습니다.

언제든지 기본 프로그램 창에서 **도움말 및 지원** > **라이선스 관리**를 선택하여 라이선스 정보를 관리할 수 있습니다. ESET의 제품 및 라이선스를 식별하는 데 사용되는 공개 라이선스 ID가 표시됩니다. 컴퓨터가 등록되는 사용자 이름은 시스템 트레이 아이콘 ⓔ을 오른쪽 마우스 버튼으로 클릭하면 표시되는 정보 섹션 내에 저장됩니다.

ESET File Security를 활성화하면 기본 프로그램 창이 열리고 모니터링 페이지에 현재 상태가 표시됩니다. 처음에는 몇 가지 주의를 기울여야 할 수도 있습니다. 예를 들면 ESET LiveGrid®에 참가할지 묻는 메시지가 표시됩니다.

기본 프로그램 창에는 시스템 업데이트(Windows Update) 또는 탐지 엔진 업데이트 같은 다른 항목에 대한 알림도 표시됩니다. 주의해야 하는 모든 항목을 확인하면 모니터링 상태가 녹색으로 바뀌고 **사용자의 장치가 보호됨** 상태가 표시됩니다.

기본 메뉴의 **도움말 및 지원** > **제품 활성화** 또는 **모니터링 상태** > **제품이 활성화되지 않음**에서 제품을 활성화할 수도 있습니다.

> 참고
> ESET Security Management Center는 관리자가 사용할 수 있는 라이선스를 이용해 자동으로 클라이언트 컴퓨터를 활성화할 수 있습니다.

ESET Business Account

ESET Business Account를 사용하여 여러 라이선스를 관리할 수 있습니다. ESET Business Account가 없는 경우 **계정 생성**을 클릭하면 등록할 수 있는 ESET Business Account 포털로 리디렉션됩니다.

> 참고
> 자세한 내용은 EBA(ESET Business Account) 사용자 가이드를 참조하십시오.

보안 관리자 자격 증명을 사용하고 있으며 패스워드를 잊은 경우 **패스워드를 잊어버리셨나요?**를 클릭하면 ESET License Administrator 포털로 리디렉션됩니다. 이메일 주소를 입력하고 **전송**을 클릭하여 확인합니다. 그러고 나면 비밀번호를 다시 설정하는 지침이 포함된 메시지를 받게 됩니다.

제품 활성화 완료

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

활성화 오류

ESET File Security를 활성화하지 못했습니다. 올바른 **라이선스 키**를 입력했는지, **오프라인 라이선스**를 연결했는지 확인하십시오. 다른 **오프라인 라이선스**가 있으면 다시 입력하십시오. 입력한 라이선스 키를 확인하려면 **라이선스 키 다시 확인** 또는 **다른 라이선스를 입력**하십시오.

라이선스

ESET File Security에 사용할 계정과 연결된 라이선스를 선택하라는 메시지가 표시됩니다. 활성화를 계속 진행하려면 **계속**을 클릭합니다.

최신 버전으로 업그레이드

최신 버전의 ESET File Security가 발표되어 제품을 개선하거나 프로그램 모듈의 자동 업데이트로 해결할 수 없는 문제를 해결할 수 있습니다.

업그레이드 방법:

- **제거/설치** - 새 버전을 설치하기 전에 이전 버전을 제거합니다. 최신 버전의 ESET File Security를 다운로드합니다. 구성을 유지하려는 경우 기존 ESET File Security에서 설정을 내보냅니다. ESET File Security를 제거한 후 서버를 다시 시작합니다. 다운로드한 설치 관리자로 설치 새로 고침을 수행합니다. 구성을 로드할 설정을 가져옵니다. ESET File Security를 실행하는 서버가 한 개 있는 경우에 이 절차를 사용하는 것이 좋습니다.

- **현재 위치** - 기전 버전을 제거하고 그 위에 새 ESET File Security를 설치하지 않고 업그레이드하는 방법입니다.

중요
Windows Update 또는 다른 이유로 인해 서버에서 **보류 중인 Windows Update가 없고 보류 중인 다시 시작이 없어야** 합니다. 보류 중인 Windows Update 또는 다시 시작이 있는 상태에서 현재 위치에 업그레이드하려고 하면 기존 ESET File Security 버전이 제대로 제거되지 않을 수 있습니다. 또한 이후에 이전 버전의 ESET File Security를 수동으로 제거하려고 하면 문제가 발생할 수 있습니다.

참고
ESET File Security를 업그레이드하는 동안 서버를 다시 시작해야 합니다.

- 원격 - ESET Security Management Center에서 관리되는 대규모 네트워크 환경에서 사용합니다. 기본적으로 새로 설치하는 업그레이드 방법이지만, 원격으로 수행됩니다. 이 방법은 ESET File Security를 실행하는 서버가 여러 개 있는 경우에 유용합니다.

- ESET 클러스터 마법사 - 업그레이드 방법으로도 사용할 수 있습니다. ESET File Security가 있는 2개 이상의 서버가 있는 경우 이 방법을 사용하는 것이 좋습니다. 기본적으로 현재 위치 업그레이드 방법이지만, ESET 클러스터를 통해 수행됩니다. 업그레이드가 완료되어도 ESET 클러스터를 계속 사용하면서 클러스터의 기능을 활용할 수 있습니다.

참고
ESET File Security를 업그레이드한 후에는 모든 설정을 살펴보면서 올바르게 구성되었는지와 요구에 적합한지 확인하는 것이 좋습니다.

ESMC를 통해 업그레이드

ESET Security Management Center를 통해 이전 버전의 ESET File Security를 실행하는 여러 서버를 업그레이드할 수 있습니다. 이 방법을 사용하면 각 ESET File Security를 동일하게 구성하면서(원하는 경우) 대량의 서버를 업그레이드할 수 있습니다.

이 절차는 다음과 같은 단계로 구성됩니다.

- 규칙, 여러 허용 목록 및 차단 목록 등을 비롯하여 모든 구성을 보존하기 위해 기존 버전 위에 최신 버전의 ESET File Security를 설치하여 수동으로 **첫 번째 서버를 업그레이드**합니다. 이 단계는 ESET File Security를 실행하는 서버에서 로컬로 수행됩니다.

• 버전 7.x로 새롭게 업그레이드된 ESET File Security **구성을 요청**하고 ESET Security Management Center에서 **정책으로 변환**합니다. 이 정책은 나중에 업그레이드된 모든 서버에 적용됩니다. 이 단계는 ESMC와 다음 단계를 사용하여 원격으로 수행됩니다.

• 이전 버전의 ESET File Security를 실행하는 모든 서버에서 **소프트웨어 제거 작업을 실행**합니다.

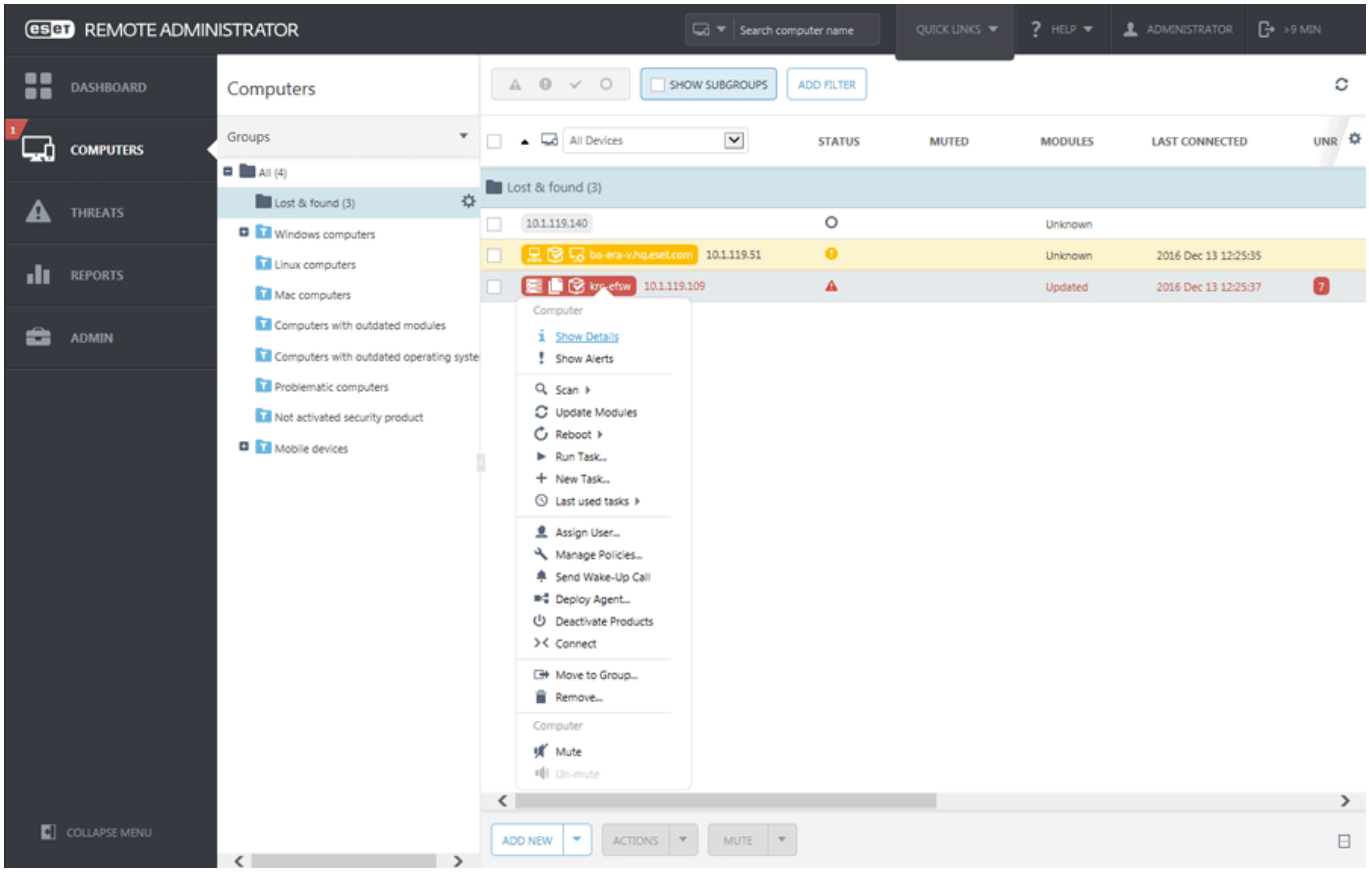
• 최신 버전의 ESET File Security를 실행할 모든 서버에서 **소프트웨어 설치 작업을 실행**합니다.

• 최신 버전의 ESET File Security를 실행하는 모든 서버에 **구성 정책을 할당**합니다.

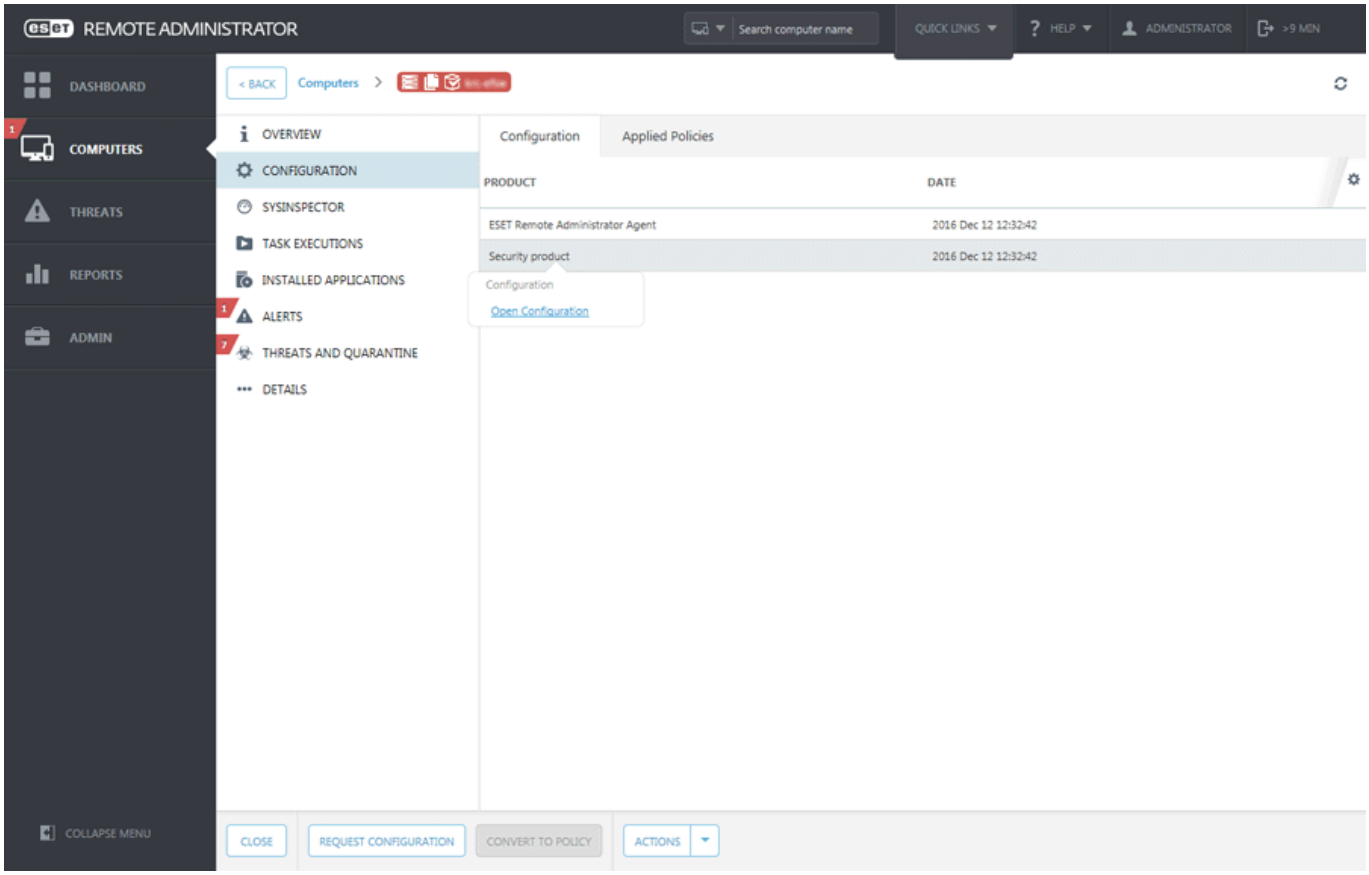
단계별 절차:

1.최신 버전의 ESET Mail Security를 다운로드하고 기존 버전 위에 설치하여 ESET File Security를 실행하는 서버 중 하나에 로그온하고 서버를 업그레이드합니다. 일반적인 설치 단계를 따르십시오. 설치하는 동안 이전 ESET File Security의 모든 원래 구성은 보존됩니다.

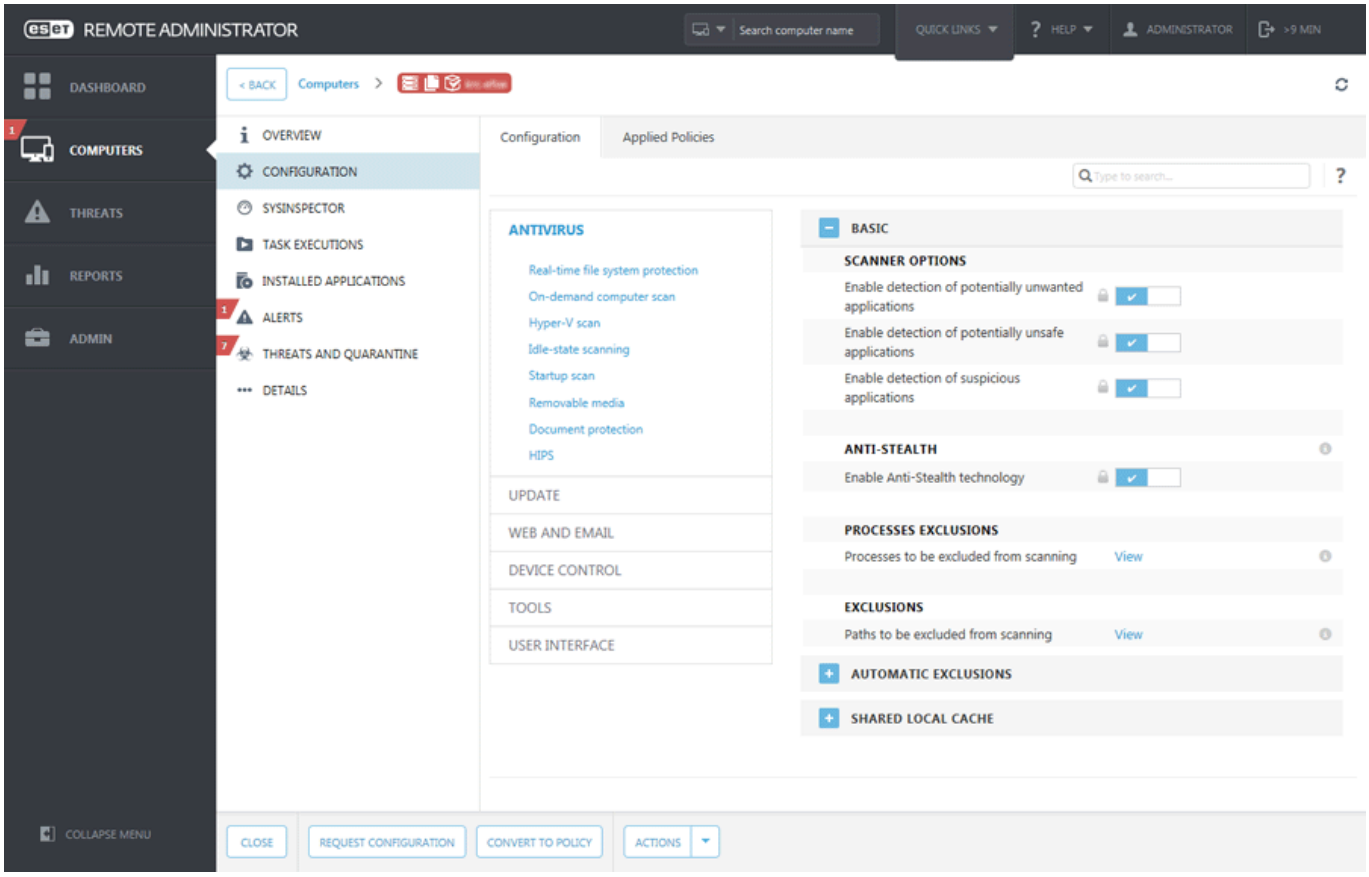
2.**ESET Security Management Center 웹 콘솔**을 열고 정적 또는 동적 그룹에서 클라이언트 컴퓨터를 선택한 후 **상세 정보 표시**를 선택합니다.



3.구성 탭으로 이동하고 **구성 요청** 버튼을 클릭하여 관리되는 제품의 모든 구성을 수집합니다. 구성을 가져오는 작업은 몇 분 정도 소요됩니다. 최신 구성이 목록에 표시되면 **보안 제품**을 클릭하고 **구성 열기**를 선택합니다.



4.**정책으로 변환** 버튼을 클릭하여 구성 정책을 생성합니다. 새 정책의 **이름**을 입력하고 **마침**을 클릭합니다.



5.**클라이언트 작업**으로 이동하여 소프트웨어 제거 작업을 선택합니다. 제거 작업 생성 시 **필요한 경우 자동으로 다시 부팅** 확인란을 선택하여 제거 후 서버를 다시 부팅하는 것이 좋습니다. 작업이

생성되면 제거할 모든 대상 컴퓨터를 추가합니다.

6.모든 대상에서 ESET File Security가 제거되었는지 확인합니다.

7.최신 버전의 ESET File Security를 원하는 모든 대상에 설치하려면 소프트웨어 설치 작업을 생성합니다.

8.ESET File Security를 실행하는 모든 서버(그룹 권장)에 **구성 정책을 할당**합니다.

ESET 클러스터를 통해 업그레이드

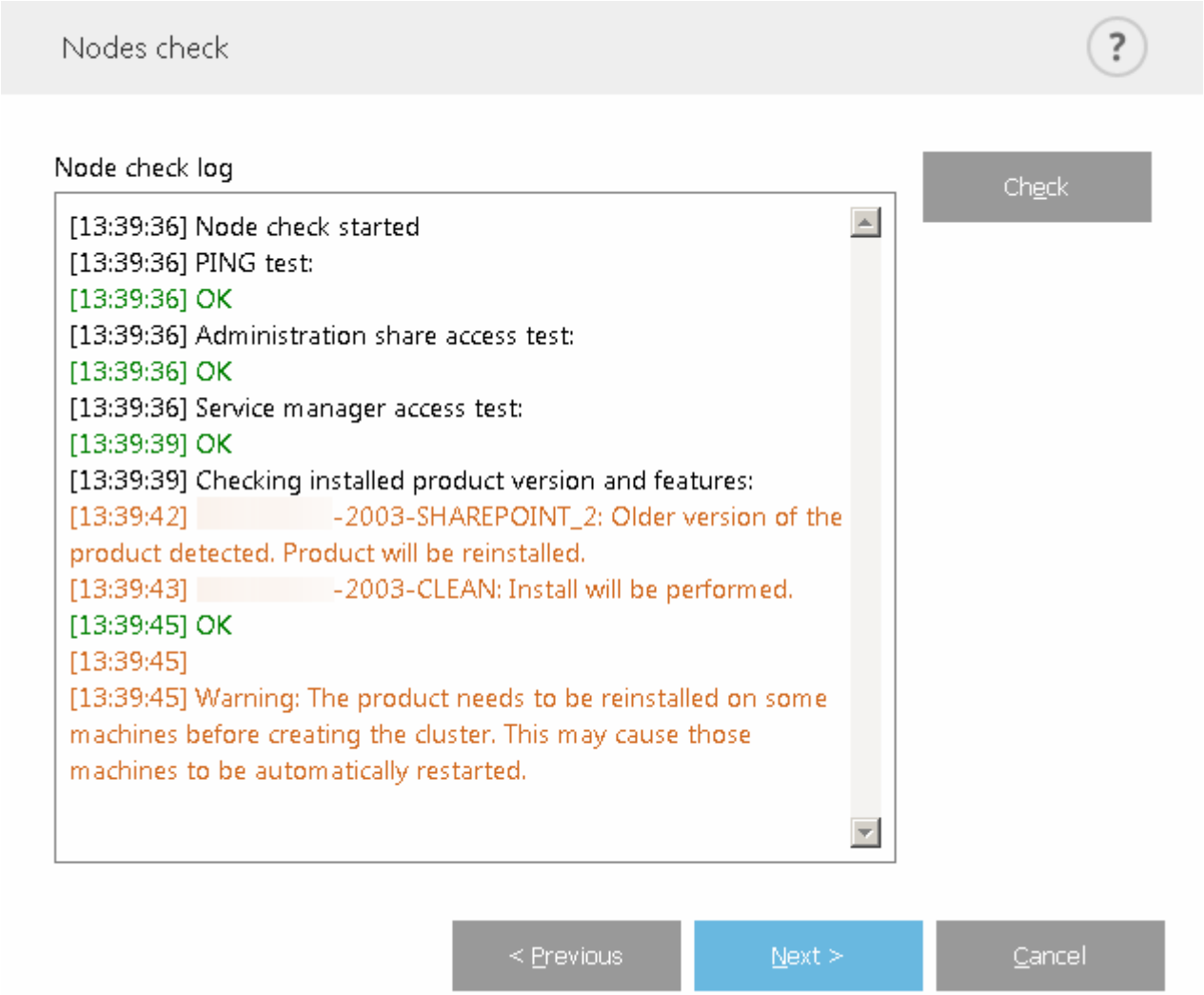
ESET 클러스터를 생성하면 이전 버전의 ESET File Security를 사용하는 여러 서버를 업그레이드할 수 있습니다. 이는 ESMC 업그레이드에 대한 대체 방법입니다. 사용자 환경에 ESET File Security가 있는 서버가 둘 이상인 경우 ESET 클러스터 방법을 사용하는 것이 좋습니다. 이 업그레이드 방법의 또 다른 장점은 ESET 클러스터를 계속 사용할 수 있어 모든 구성원 노드에서 ESET File Security 구성이 동기화된다는 점입니다.

이 방법을 사용하여 업그레이드하려면 아래 단계를 따르십시오.

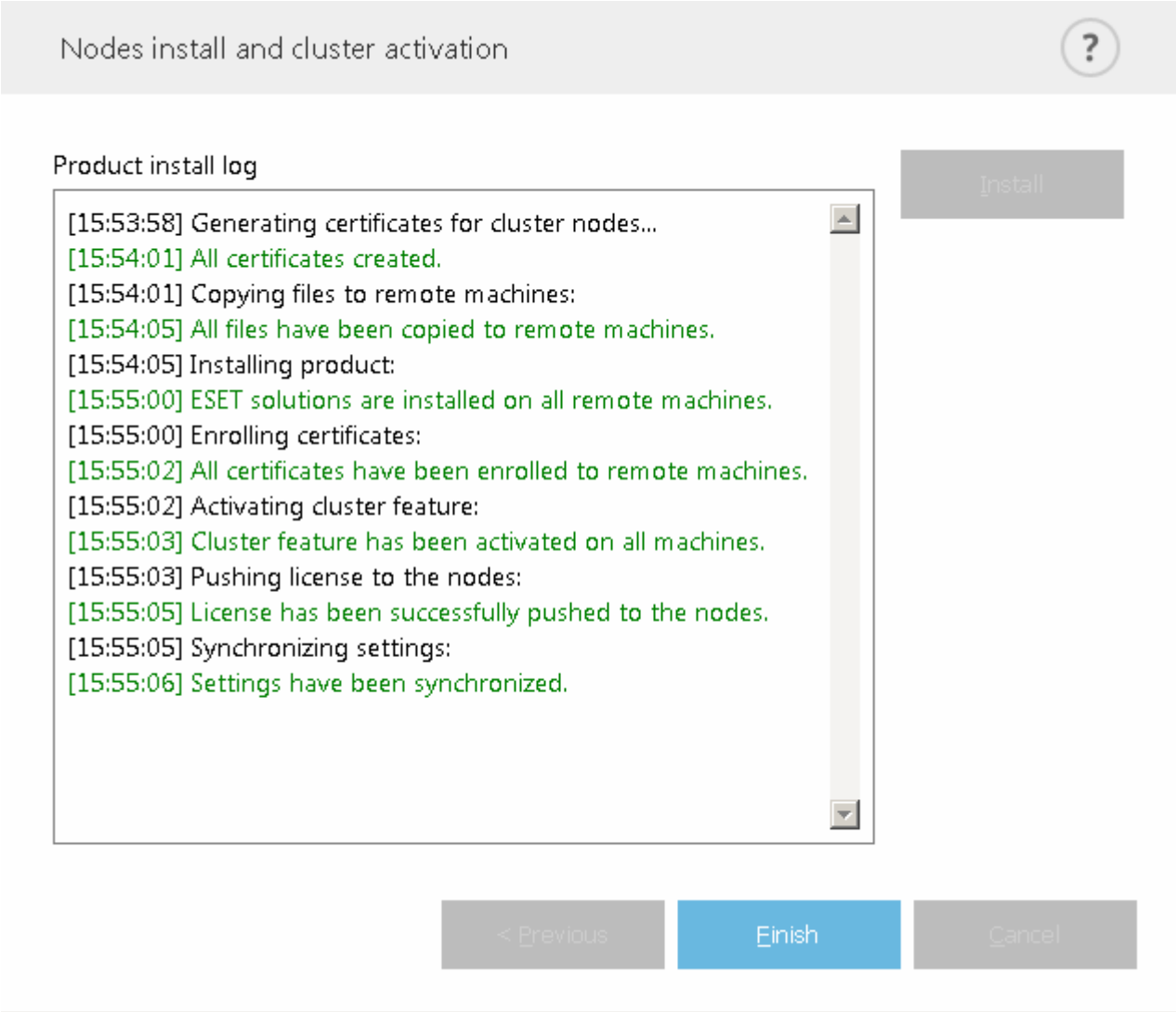
1.최신 버전의 ESET Mail Security를 다운로드하고 기존 버전 위에 설치하여 ESET File Security를 실행하는 서버 중 하나에 로그온하고 서버를 업그레이드합니다. 일반적인 설치 단계를 따르십시오. 설치하는 동안 이전 ESET File Security의 모든 원래 구성은 보존됩니다.

2.ESET 클러스터 마법사를 실행하고 클러스터 노드를 추가합니다(ESET File Security를 업그레이드할 서버). 필요한 경우 아직 ESET File Security가 실행되고 있지 않은 다른 서버를 추가할 수 있습니다(이 서버에서 설치가 수행됨). 클러스터 이름 및 설치 유형 지정 시 기본 설정을 유지하는 것이 좋습니다(**제품을 활성화하지 않고 노드에 라이선스 푸시**가 선택되어 있어야 함).

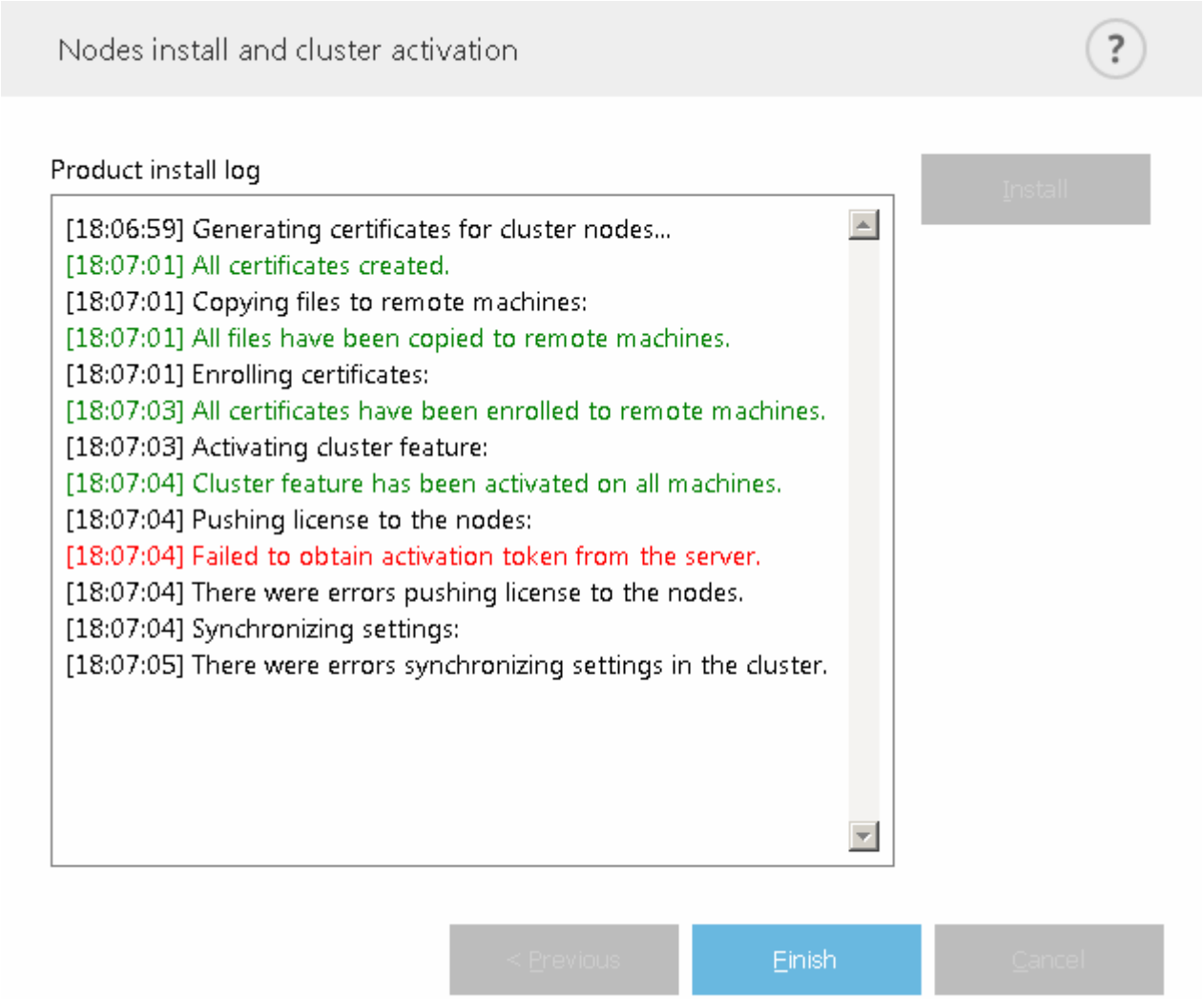
3.**노드 확인 로그** 화면을 검토합니다. 이전 제품 버전이 설치된 서버와 제품이 다시 설치되는 서버가 표시됩니다. 또한 추가된 서버 중 ESET File Security가 설치되지 않은 모든 서버에 ESET File Security가 설치됩니다.



4.**노드 설치 및 클러스터 활성화** 화면에 설치 진행률이 표시됩니다. 설치가 완료되면 다음과 같은 형식의 결과가 표시됩니다.



네트워크나 DNS가 제대로 구성되지 않은 경우 **서버에서 활성화 토큰을 가져오지 못했습니다.** 오류 메시지가 표시될 수 있습니다. ESET 클러스터 마법사를 다시 실행해 보십시오. 클러스터가 폐기되고 새 클러스터가 생성되며(제품을 다시 설치하지는 않음) 활성화가 완료됩니다. 문제가 계속되면 네트워크 및 DNS 설정을 확인하십시오.



클러스터 환경에서 설치

클러스터 환경에서 ESET File Security를 배포할 수 있습니다(예: 장애 조치(Failover) 클러스터). 활성 노드에 ESET File Security를 설치한 다음 ESET File Security의 ESET 클러스터 기능을 사용하여 수동 노드에서 설치를 재배포하는 것이 좋습니다. 설치와 별개로, ESET 클러스터는 올바른 작동에 필요한 클러스터 노드 간 일관성을 보장하기 위해 ESET File Security 구성의 복제로 작동합니다.

터미널 서버

터미널 서버 역할을 하는 Windows Server에 ESET File Security를 설치할 경우 사용자가 로그인할 때마다 ESET File Security GUI가 시작되지 않도록 비활성화하는 것이 좋을 수도 있습니다. GUI를 비활성화하는 구체적인 단계는 터미널 서버에서 GUI 비활성화를 참조하십시오.

시작

다음 부분에서 ESET File Security를 시작하는 데 도움을 받을 수 있습니다.

모니터링

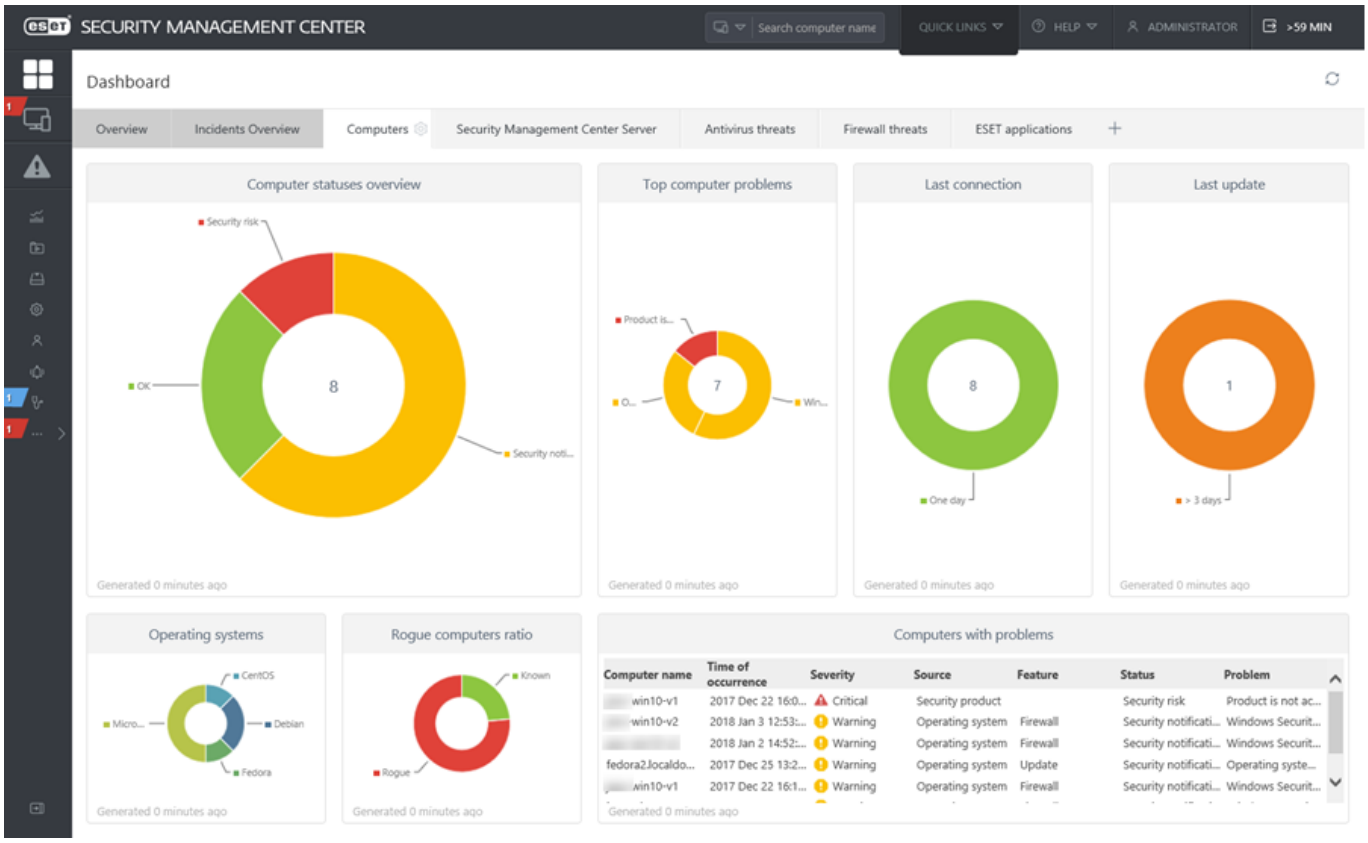
ESET File Security의 현재 상태를 즉각적으로 간략하게 보여 줍니다. 처음에 주의를 기울여야 하는 문제가 있는지 표시됩니다.

ESET Security Management Center를 통해 관리됨

ESET Security Management Center를 사용하여 ESET File Security를 원격으로 관리할 수 있습니다.

ESET Security Management Center를 통해 관리됨

ESMC(ESET Security Management Center)는 중앙 위치 한 곳에서 네트워크로 연결된 환경에 있는 ESET 제품을 관리할 수 있도록 해주는 애플리케이션입니다. ESET Security Management Center 작업 관리 시스템을 통해 원격 컴퓨터에 ESET 보안 솔루션을 설치하고 새로운 문제와 위협에 신속하게 대응할 수 있습니다. ESET Security Management Center는 악성 코드로부터 보호하는 기능을 자체적으로 제공하지는 않으며 각 클라이언트에 있는 ESET 보안 솔루션을 활용합니다. ESET 보안 솔루션은 여러 플랫폼 유형이 포함된 네트워크를 지원합니다. 네트워크에는 현재 Microsoft, Linux 기반, Mac OS 및 모바일 운영 체제가 조합되어 포함돼 있을 수 있습니다.



ESMC에 대한 자세한 내용은 ESET Security Management Center 온라인 도움말을 참조하십시오.

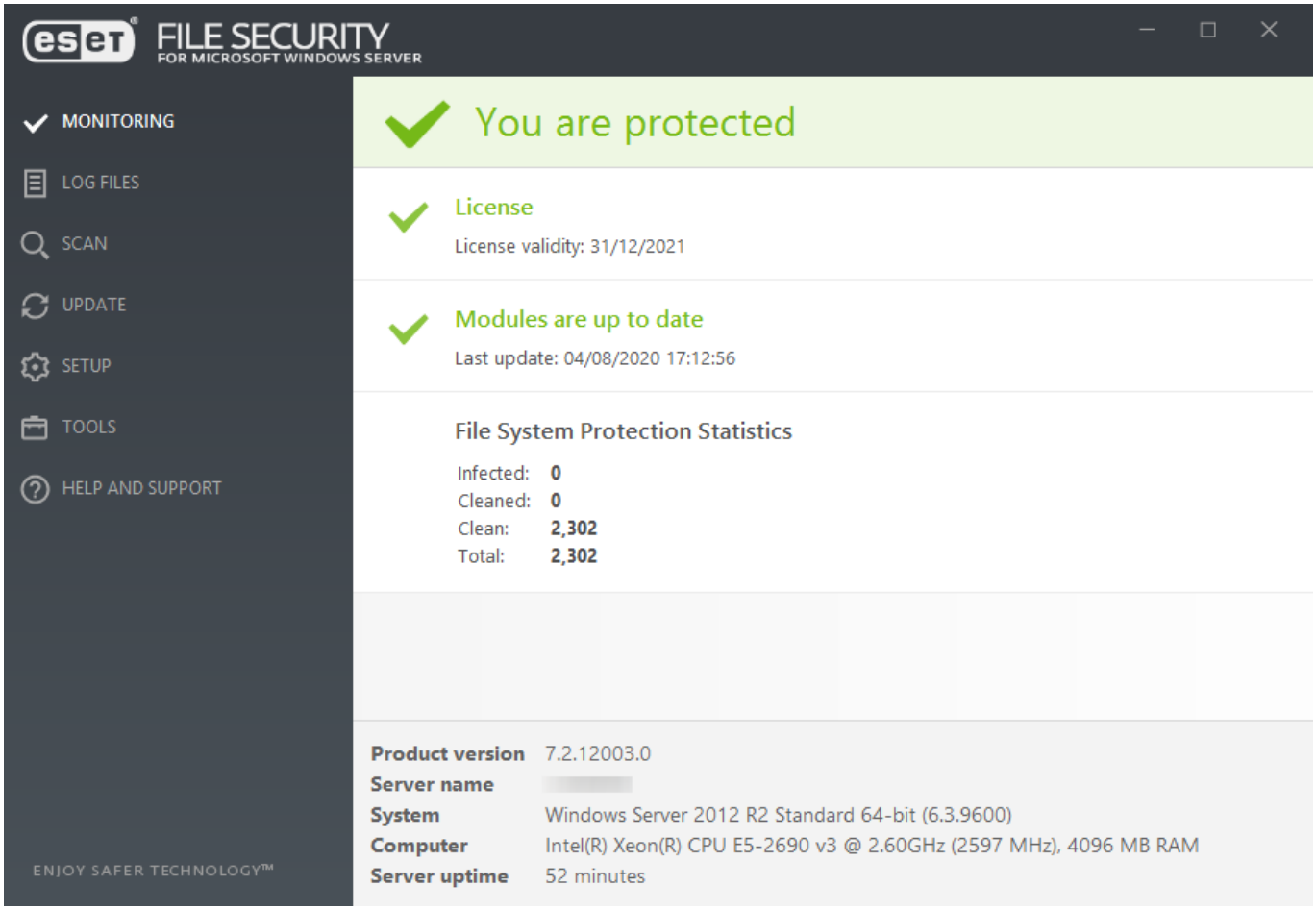
모니터링

모니터링 섹션에 표시되는 보호 상태는 컴퓨터의 현재 보호 수준에 대한 정보를 알려 줍니다. 기본 창에 ESET File Security 모듈 작동에 대한 상태 요약이 표시됩니다.

✔ 녹색 **사용자의 장치가 보호됨** 상태는 보호 수준이 최대임을 나타냅니다.

빨간색 아이콘은 주요 문제가 있음을 나타냄 - 컴퓨터의 보호 수준이 최대가 아닙니다. 가능한 보호 상태 목록은 상태 섹션을 참조하십시오.

주황색 아이콘은 ESET 제품에 중요하지 않은 문제에 대한 주의가 필요함을 나타냅니다.



제대로 작동하는 모듈에는 녹색 확인 표시가 지정됩니다. 제대로 작동하지 않는 모듈에는 빨간색 느낌표 또는 주황색 알림 아이콘이 지정됩니다. 모듈에 대한 추가 정보가 창의 위쪽 부분에 표시됩니다. 모듈 해결에 대한 권장 해결 방법도 표시됩니다. 개별 모듈의 상태를 변경하려면 기본 메뉴에서 설정을 클릭한 다음 원하는 모듈을 클릭합니다.

모니터링 페이지에는 다음을 비롯한, 시스템에 대한 정보도 포함되어 있습니다.

- **제품 버전** - ESET File Security의 버전 번호입니다.
- **서버 이름** - 컴퓨터 호스트 이름 또는 FQDN입니다.
- **시스템** - 운영 체제 상세 정보입니다.
- **컴퓨터** - 하드웨어 상세 정보입니다.
- **서버 가동 시간** - 시스템이 작동되고 실행되는 시간을 표시합니다. 기본적으로 가동 중지 시간과 반대입니다.

권장 해결 방법을 사용하여 문제를 해결할 수 없는 경우 **도움말 및 지원**을 클릭하여 도움말 파일에 접근하거나 ESET 지식베이스를 검색합니다. 그래도 계속해서 지원이 필요한 경우 지원 요청을 전송할 수 있습니다. ESET 기술 지원은 사용자의 질문에 신속하게 응답하고 해결 방법을 찾을 수 있도록 도와줍니다.

상태

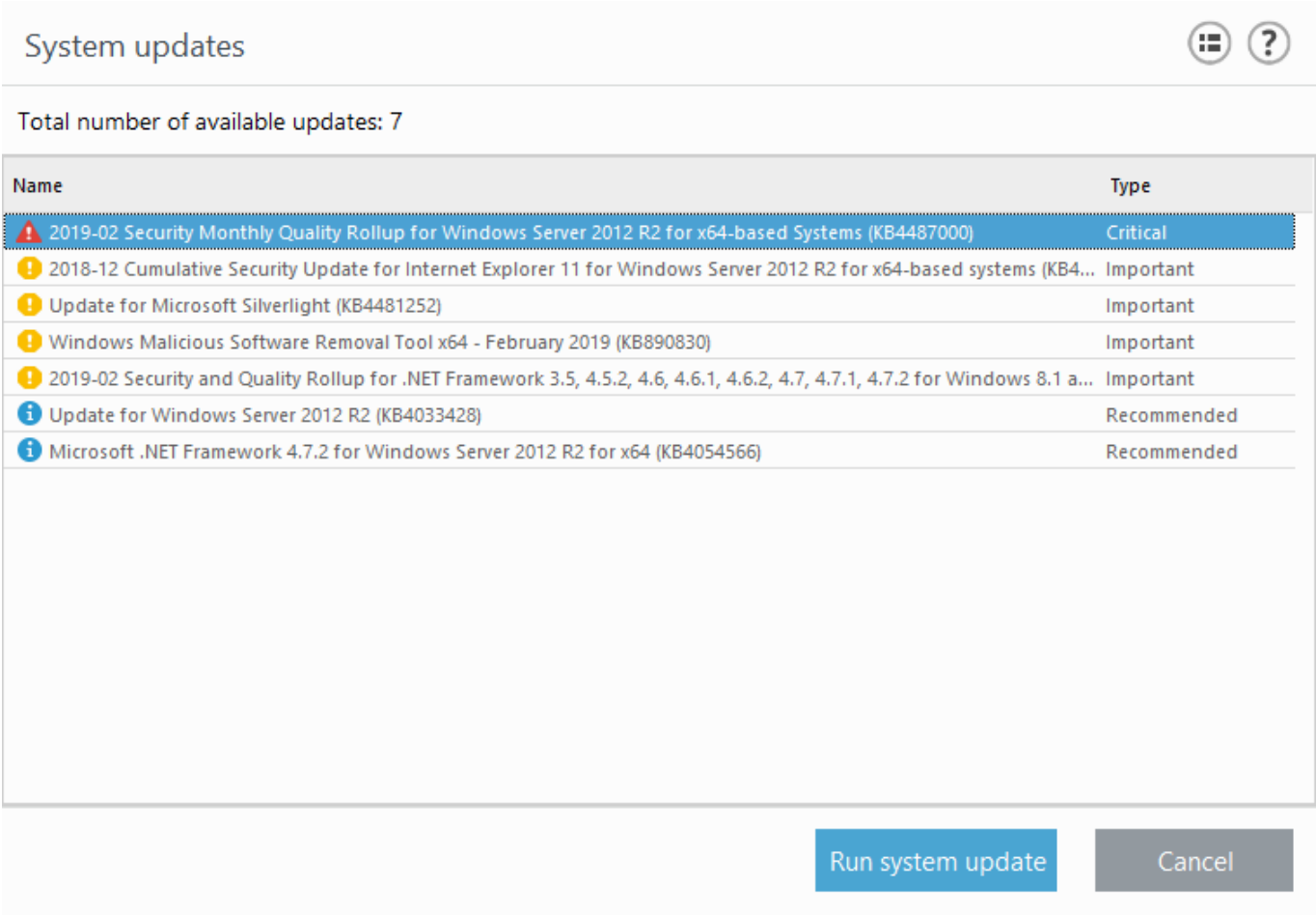
ESET File Security의 상태 요약이 시스템에 대한 상세 정보와 함께 기본 창에 표시됩니다. 일반적으로 모든 기능이 문제 없이 작동할 때에는 보호 상태가 ✔ 녹색입니다. 그러나 특정 상황에서는 보호 상태가 바뀔 수 있습니다. 다음 중 하나가 발생하는 경우 경고 메시지가 표시되는 ! 주황색 또는 ⚠ 빨간색으로 보호 상태가 바뀝니다.

경고 메시지	경고 메시지 상세 정보
사용자가 원치 않는 애플리케이션 검색이 구성되지 않음	사용자가 원치 않는 애플리케이션(PUA)은 애드웨어를 포함하거나, 도구 모음을 설치하거나, 기타 목적이 불분명한 프로그램입니다. 사용자가 원치 않는 애플리케이션의 경우 위험에 비해 이 애플리케이션의 이점이 훨씬 더 많다고 느껴지는 경우가 더러 있습니다.
실시간 파일 시스템 보호가 일시 중지됨	모니터링 탭에서 **실시간 보호 활성화**를 클릭하거나 기본 프로그램 창의 설정 탭에서 **실시간 파일 시스템 보호**를 다시 활성화합니다.
안티피싱 보호가 작동 안 함	필요한 기타 프로그램 모듈이 활성화되어 있지 않아 이 기능이 작동하지 않습니다.
ESET LiveGrid®가 비활성화됨	이 문제는 ESET LiveGrid®가 **고급 설정**에서 비활성화되어 있을 때 나타납니다.
프로토콜 필터링이 비활성화됨	이 기능을 다시 활성화하려면 프로토콜 필터링 활성화를 클릭합니다.
운영 체제가 최신 버전이 아님	시스템 창에는 다운로드하여 설치할 수 있는 업데이트 목록이 표시됩니다.
장치의 보호 기능이 곧 종료됨	Microsoft Windows 버전을 업데이트하는 방법에 대한 자세한 내용은 옵션 참조를 클릭하십시오. **Microsoft Windows Server 2008 R2 SP1** 또는 **Microsoft Windows Small Business Server 2011 SP1**을 실행하는 경우 시스템이 SHA-2와 호환되는지 확인하십시오. 다음과 같이 특정 운영 체제 버전에 따라 패치를 적용합니다.
프리젠테이션 모드 활성화됨	모든 팝업 창이 숨겨지고 예약된 작업이 일시 중지됩니다.
네트워크 공격 보호(IDS)가 일시 중지됨	이 기능을 다시 활성화하려면 네트워크 공격 보호(IDS) 활성화를 클릭합니다.
봇네트 보호가 일시 중지됨	이 기능을 다시 활성화하려면 봇네트 보호 활성화를 클릭합니다.
웹브라우저 보호가 일시 중지됨	모니터링에서 **웹 브라우저 보호 활성화**를 클릭하거나 기본 프로그램 창의 설정 창에서 **웹 브라우저 보호**를 다시 활성화합니다.
장치 제어가 일시 중지됨	이 기능을 다시 활성화하려면 장치 제어 활성화를 클릭합니다.
제품이 활성화되지 않음 또는 라이선스가 만료됨	보호 상태 아이콘이 빨간색으로 변하여 이 문제를 나타냅니다. 라이선스가 만료되면 프로그램에서 업데이트할 수 없습니다. 라이선스를 갱신하려면 경고 창의 지침을 따르십시오.
정책 무시 활성화	문제가 해결될 때까지 정책에서 설정한 구성이 일시적으로 재정의됩니다. ESMC를 사용하여 ESET File Security를 관리 중이고 여기에 할당된 정책이 있는 경우, 정책에 속하는 기능에 따라 상태 링크가 잠깁니다(회색으로 표시됨).

문제를 해결할 수 없는 경우 ESET 지식베이스를 검색합니다. 그래도 계속해서 지원이 필요한 경우 지원 요청을 전송할 수 있습니다. ESET 기술 지원은 사용자의 질문에 신속하게 응답하고 해결 방법을 찾을 수 있도록 도와줍니다.

Windows 업데이트 사용 가능

시스템 업데이트 창에는 다운로드하여 설치할 수 있는 업데이트 목록이 표시됩니다. 업데이트 이름 옆에는 업데이트 순위 수준이 표시됩니다. 추가 정보가 포함된 팝업 창을 표시하려면 업데이트 행을 오른쪽 마우스 버튼으로 클릭하고 **추가 정보**를 클릭합니다.



시스템 업데이트 실행을 클릭하여 **Windows 업데이트** 창을 열고 시스템 업데이트를 계속 진행합니다.

네트워크 격리

ESET File Security에서는 네트워크 격리라고 하는 서버의 네트워크 연결을 차단하는 옵션을 제공합니다. 일부 극단적인 시나리오에서는 예방 조치로 네트워크의 서버를 격리하고자 할 수 있습니다. 그 예로 서버가 악성코드에 감염되었거나 컴퓨터가 달리 손상되었음을 알게 되는 경우를 들 수 있습니다.

네트워크 격리를 활성화하면 다음과 같은 경우를 제외하고 모든 네트워크 트래픽이 차단됩니다.

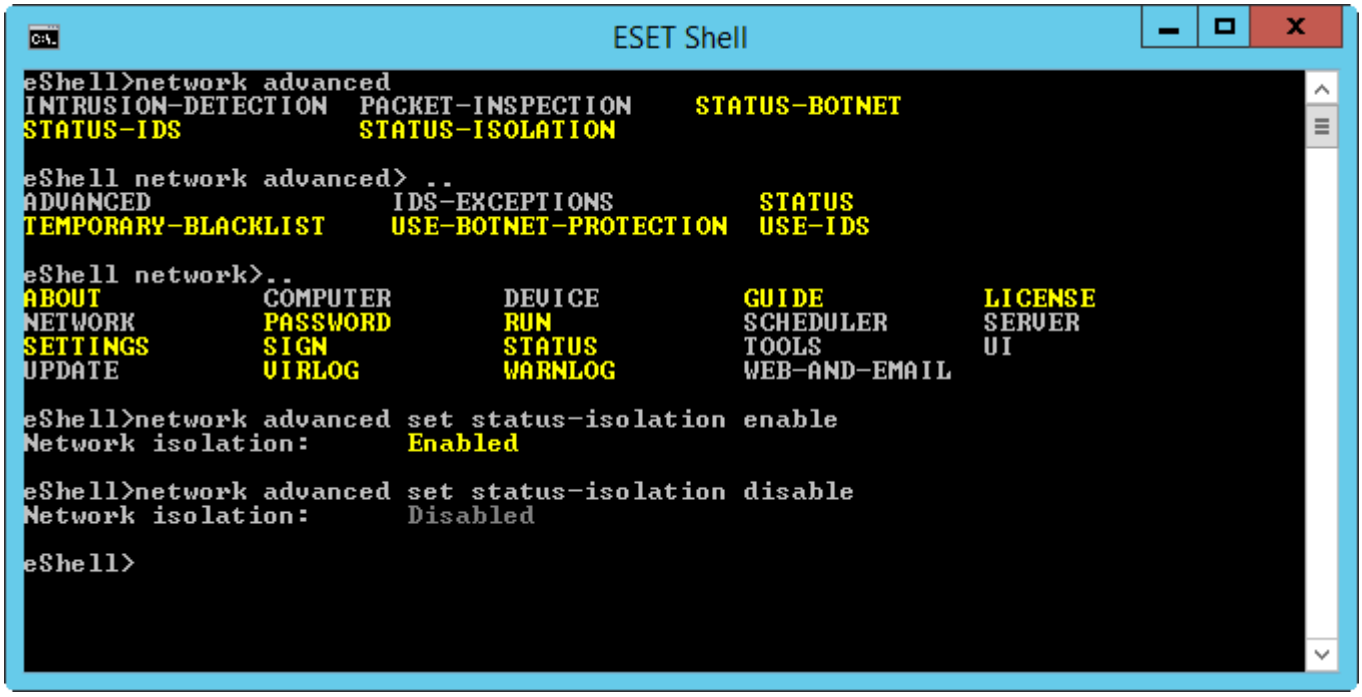
- 도메인 컨트롤러에 대한 연결이 유지되는 경우
- ESET File Security에서 계속 통신할 수 있는 경우
- 있다면 ESET Management Agent와 ESET Enterprise Inspector Agent가 네트워크를 통해 통신할 수 있는 경우

eShell 명령 또는 ESET Security Management Center 클라이언트 작업을 사용해 네트워크 격리를 활성화/비활성화하는 경우

eShell

대화 모드의 경우:

- 네트워크 격리 활성화: `network advanced set status-isolation enable`
- 네트워크 격리 비활성화: `network advanced set status-isolation disable`



또는 배치/스크립트 모드를 사용하여 배치 파일을 생성 및 실행할 수 있습니다.

ESET Security Management Center

- 클라이언트 작업을 통해 네트워크 격리를 활성화합니다.
- 클라이언트 작업을 통해 네트워크 격리를 비활성화합니다.

네트워크 격리가 활성화되면 **네트워크 접근이 차단됨**이라는 메시지와 함께 ESET File Security 상태가 빨간색으로 변경됩니다.

명령과 함께 ESET File Security

이 부분에는 프로그램의 사용자 인터페이스에 대한 상세 설명이 수록되어 있으며, 이는 ESET File Security의 사용 방법을 설명하는 데 목적을 두고 있습니다.

사용자 인터페이스를 통해 일반적으로 사용되는 기능에 빠르게 접근할 수 있습니다.

- 모니터링
- 로그 파일
- 검사
- 업데이트
- 설정
- 도구

검사

수동 스캐너는 ESET File Security의 중요한 기능으로 컴퓨터에서 파일 및 폴더를 검사하는 데 사용됩니다. 네트워크 보안을 위해 감염이 의심될 때뿐만 아니라 일상적인 보안 조치의 일환으로 정기적으로 컴퓨터 검사를 실행해야 합니다. 실시간 파일 시스템 보호에서 검출되지 않는 바이러스를 검출하기 위해 시스템 상세 검사를 정기적으로(예: 한 달에 한 번) 수행하는 것이 좋습니다. 실시간 파일 시스템 보호가 비활성화되었을 때 위협이 검출되었거나, 진단 엔진이 업데이트되지 않았거나, 파일이 처음 디스크에 저장될 때 파일이 검색되지 않은 경우에 이를 실행할 수 있습니다.

ESET File Security에서 사용할 수 있는 수동 검사를 선택합니다.

저장소 검사

로컬 서버의 모든 공유 폴더를 검사합니다. 저장소 검사를 사용할 수 없으면 서버에 공유 폴더가 없는 것입니다.

컴퓨터 검사

컴퓨터 검사를 빠르게 시작하고 사용자가 상호 작용하지 않고도 감염된 파일을 치료할 수 있습니다. 컴퓨터 검사의 장점은 작동이 간편하고 검사를 상세하게 검사를 구성하지 않아도 된다는 점입니다. 검사에서는 로컬 드라이브에 있는 모든 파일을 검사하고 검색된 침입 항목을 자동으로 치료하거나 제거합니다. 치료 수준은 기본값으로 자동 설정됩니다. 치료 유형에 대한 자세한 내용은 치료를 참조하십시오.

> 참고
> 컴퓨터 검사는 매월 1회 이상 실행하는 것이 좋습니다. 검사를 예약된 작업으로 구성할 수 있습니다.

사용자 지정 검사

검사 대상 및 검사 방법과 같은 검사 파라미터를 지정하려는 경우에는 사용자 지정 검사가 가장 적합합니다. 사용자 지정 검사의 장점은 검사 파라미터를 상세히 구성할 수 있다는 점입니다. 사용자 정의 검사 프로필에 구성을 저장할 수 있는데 이는 동일한 파라미터를 사용하여 검사를 반복적으로 수행하는 경우에 유용합니다.

이동식 미디어 검사

스마트 검사와 유사하며, 컴퓨터에 연결된 이동식 미디어(예: CD/DVD/USB)의 검사를 빠르게 시작합니다. 이 기능은 컴퓨터에 USB 플래시 드라이브 연결 시 콘텐츠의 악성코드와 다른 잠재적 위협을 검사하는 데 유용합니다. 이 유형의 검사는 **사용자 지정 검사**를 클릭한 다음 **검사 대상** 드롭다운 목록에서 **이동식 미디어**를 선택하고 **검사**를 클릭하여 시작할 수도 있습니다.

Hyper-V 검사

이 옵션은 ESET File Security를 실행하는 서버에 Hyper-V Manager가 설치된 경우에만 메뉴에 표시됩니다. Hyper-V 검사를 통해 특정 VM에 "에이전트"를 설치하지 않고도 Microsoft Hyper-V Server에서 가상 컴퓨터(VM) 디스크를 검사할 수 있습니다.

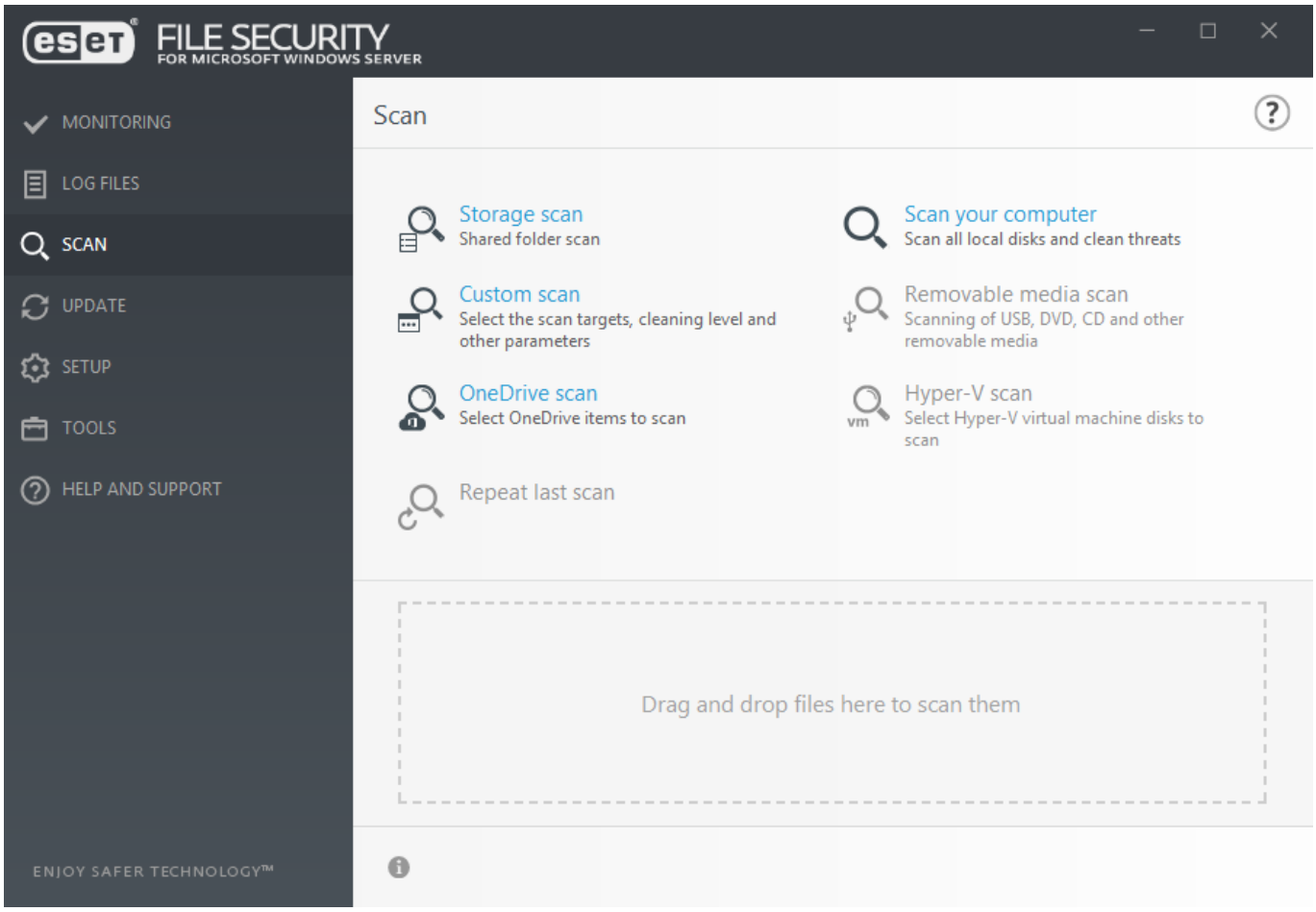
OneDrive 검사

OneDrive 클라우드 저장 장치에 있는 사용자의 파일을 검사하려면 활성화합니다.

마지막 검사 다시 시도

정확하게 동일한 설정을 사용하여 마지막 검사 작업을 다시 실행합니다.

> 참고
> 수동 DB 검사가 있는 경우 [마지막 검사 다시 시도] 기능을 사용할 수 없습니다.



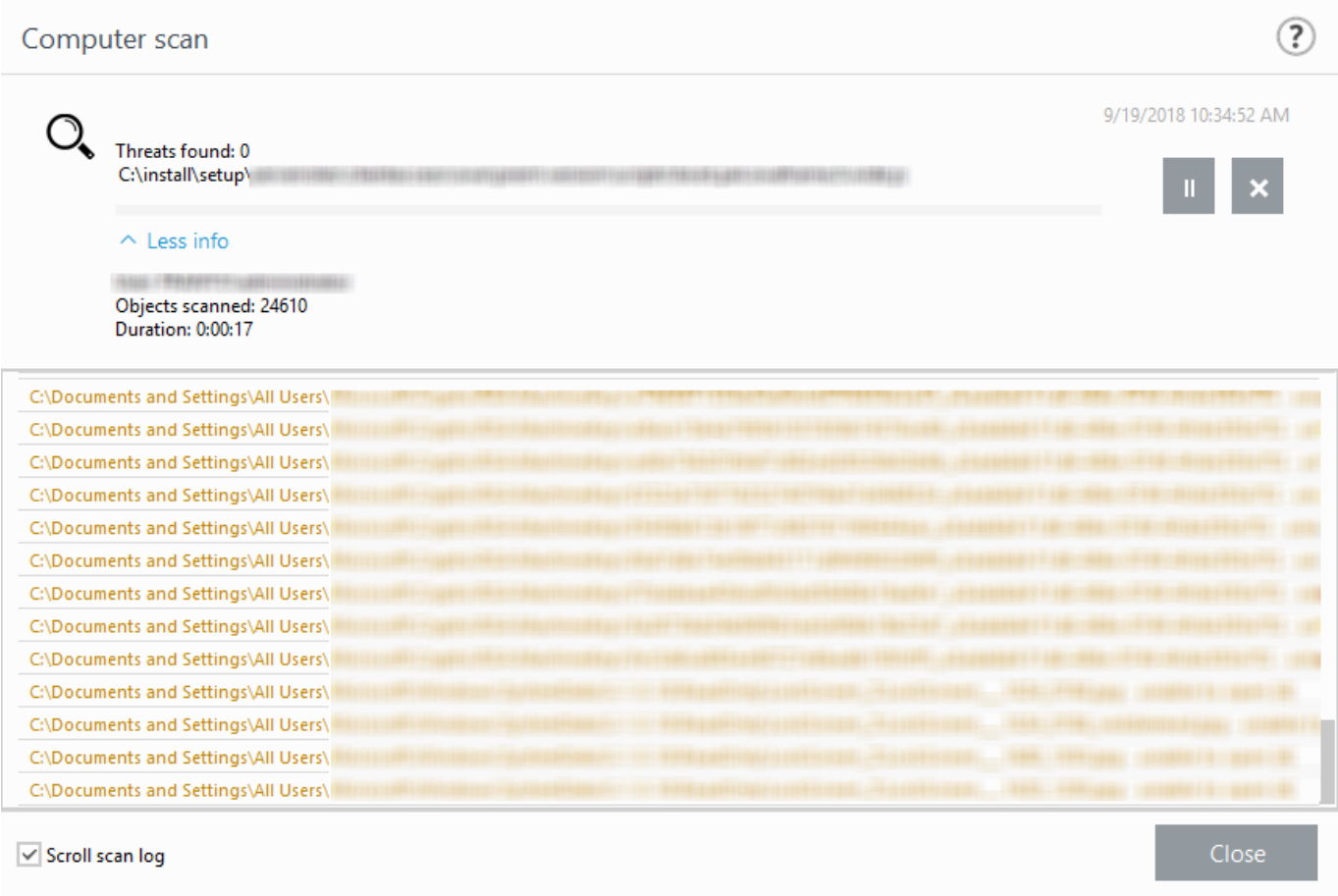
옵션을 사용하고 검사 상태에 대한 자세한 정보를 표시할 수 있습니다.

파일 끌어다 놓기	**ESET File Security 검사 창에도 파일을 끌어다 놓을 수 있습니다. 이러한 파일에서는 바이러스가 즉시 검사됩니다.**
삭제/모두 삭제	지정된 메시지를 삭제합니다.
검사 상태	첫 번째 검사 상태를 표시합니다. 이 검사는 사용자가 완료했거나 중단했습니다.
로그 표시	자세한 정보를 표시합니다.
추가 정보	검사하는 동안 검사를 실행한 **사용자**, **검사된 개체** 수 및 검사 **기간** 같은 상세 정보를 볼 수 있습니다.
검사 창 열기	검사 진행률 창에는 현재 검사 상태 및 악성 코드를 포함하는 것으로 밝혀진 파일 수에 대한 정보가 표시됩니다.

검사 창 및 검사 로그

검사 창에는 개체 위치, 발견된 위협의 수(해당하는 경우), 검사한 개체의 수 및 검사 기간 등 현재 검사한 개체가 표시됩니다. 창 아래쪽에는 진단 엔진 버전 번호, 검사를 시작한 날짜/시간 및 대상 선택 항목을 표시하는 검사 로그가 있습니다.

검사가 진행 중이면 검사를 일시적으로 중단하고 싶은 경우 **일시 중지**를 클릭할 수 있습니다. 검사 프로세스를 일시 중지한 경우에는 **다시 시작** 옵션을 사용할 수 있습니다.

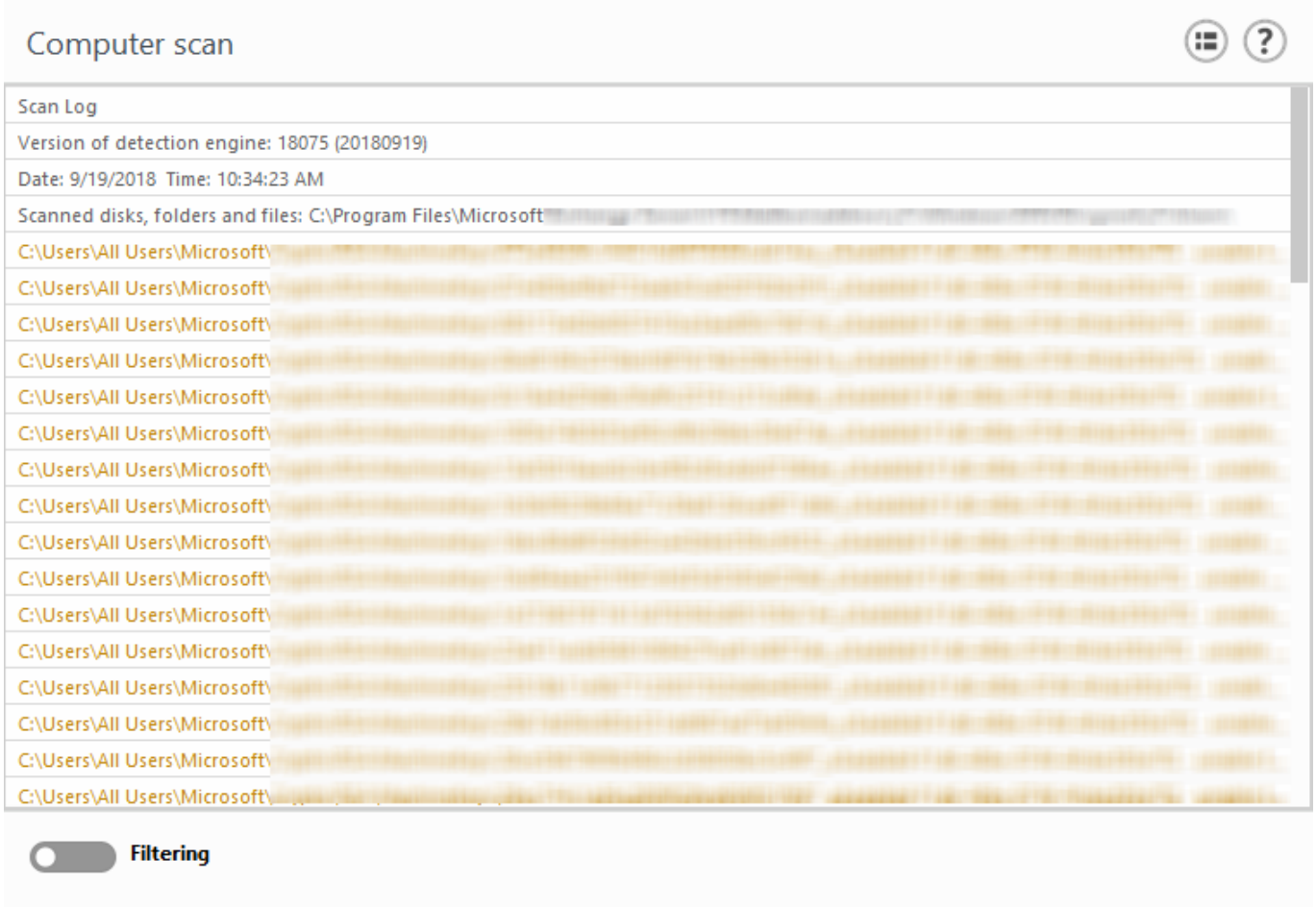


검사 로그 스크롤

로그 파일 창에서 이전 로그를 자동으로 스크롤하고 활성 로그를 보려면 이 옵션을 활성화된 상태로 둡니다.

> 참고
> 비밀번호로 보호되는 파일이나 시스템에서만 사용하는 파일(일반적으로 *pagefile.sys* 및 특정 로그 파일)과 같은 일부 파일의 경우 검색할 수 없는 것이 일반적입니다.

검사가 완료된 후에는 특정 검사와 연관 있는 관련 정보가 모두 포함된 검사 로그가 표시됩니다.



필터링 또는 검색 조건을 정의할 수 있는 로그 필터링 창을 열려면 전환 아이콘 **필터링**을 클릭합니다. 오른쪽 마우스 버튼 메뉴를 보려면 특정 로그 항목을 오른쪽 마우스 버튼으로 클릭합니다.

동작	사용	바로가기	추가 참조
같은 레코드 필터링	선택한 레코드와 같은 형식의 레코드만 표시하는 로그 필터링을 활성화합니다.	Ctrl + Shift + F 키	
필터링...	이 옵션을 클릭하면 로그 필터링 창에서 특정 로그 항목에 대한 필터링 기준을 정의할 수 있습니다.		로그 필터링
필터 활성화	필터 설정을 활성화합니다. 필터링을 처음 활성화할 때에는 설정을 정의해야 합니다.		
필터 비활성화	필터링을 끕니다(맨 아래의 전환 아이콘을 클릭한 것과 같음).		
복사	선택/강조 표시된 레코드의 정보를 클립보드에 복사합니다.	Ctrl + C 키	
모두 복사	창에 있는 모든 레코드의 정보를 복사합니다.		
내보내기...	선택/강조 표시된 레코드의 정보를 XML 파일로 내보냅니다.		
모두 내보내기...	창의 모든 정보를 XML 파일로 내보냅니다.		

로그 파일

로그 파일은 발생한 중요 프로그램 이벤트에 대한 정보를 포함하며 검사 결과, 검출된 위협 등에 대한 개요를 제공합니다. 로그는 시스템을 분석하고, 위협을 검출하고, 문제를 해결하는 데 반드시 필요한 도구입니다. 로깅은 사용자 상호 작용 없이 백그라운드에서 수행됩니다. 정보는 현재 로그 상세 수준 설정에 따라 기

록됩니다. ESET File Security 환경에서 직접 텍스트 메시지와 로그를 보거나, 이를 내보내 다른 환경에서 볼 수 있습니다.

드롭다운 메뉴에서 적합한 로그 유형을 선택합니다. 사용할 수 있는 로그는 다음과 같습니다.

검색

탐지 로그는 ESET File Security 모듈에서 탐지된 침입에 대한 자세한 정보를 제공합니다. 이 정보에는 탐지 시간, 침입 이름, 위치, 수행된 조치 및 침입 탐지 시 로그인한 사용자 이름이 포함됩니다. 별도의 창에 자세한 내용을 표시하려면 로그 항목을 두 번 클릭합니다. 필요한 경우, 탐지 제외를 생성할 수 있습니다. 로그 기록(탐지)를 마우스 오른쪽 버튼으로 클릭하고 **제외 생성**을 클릭합니다. 그러면 미리 정의된 기준이 있는 제외 마법사가 열립니다. 제외된 파일 옆에 탐지 이름이 있으면 파일이 지정된 탐지에 대해서만 제외된다는 의미입니다. 해당 파일이 나중에 다른 악성코드에 감염되면 탐지됩니다.

이벤트

ESET File Security에서 수행된 중요한 모든 동작이 이벤트 로그에 기록됩니다. 이벤트 로그에는 프로그램에서 발생한 이벤트 및 오류에 대한 정보가 포함되어 있습니다. 이 로그는 시스템 관리자 및 사용자가 문제를 해결하는 데 도움이 되도록 설계되었습니다. 여기서 찾은 정보를 통해 프로그램에서 발생한 문제에 대한 해결책을 찾을 수 있도록 도움을 주기 위해 고안되었습니다.

컴퓨터 검사

모든 검사 결과가 이 창에 표시됩니다. 각 행은 단일 컴퓨터 검사에 해당됩니다. 각 검사의 상세 정보를 보려면 항목을 두 번 클릭합니다.

차단된 파일

차단되어 접근할 수 없는 파일 레코드를 포함합니다. 프로토콜에는 파일을 차단한 이유와 소스 모듈뿐만 아니라, 파일을 실행한 애플리케이션과 사용자도 표시됩니다.

파일 보냄

클라우드 기반 보호, ESET Dynamic Threat Defense 및 ESET LiveGrid®의 파일 레코드를 포함합니다.

HIPS

기록을 위해 지정된 특정 규칙의 레코드를 포함합니다. 이 프로토콜은 작업을 호출한 애플리케이션, 결과(규칙이 허용되는지, 금지되는지 여부) 및 생성된 규칙 이름을 표시합니다.

네트워크 보호

봇네트 보호 및 IDS(네트워크 공격 보호)에서 차단된 파일 레코드를 포함합니다.

필터링된 웹 사이트

웹 브라우저 보호 및 . 이러한 로그는 특정 웹 사이트에 대한 연결을 연 시간, URL, 사용자 및 애플리케이션을 표시합니다.

장치 제어

컴퓨터에 연결된 이동식 미디어나 장치의 레코드를 포함합니다. 장치 제어 규칙이 포함된 장치만 로그

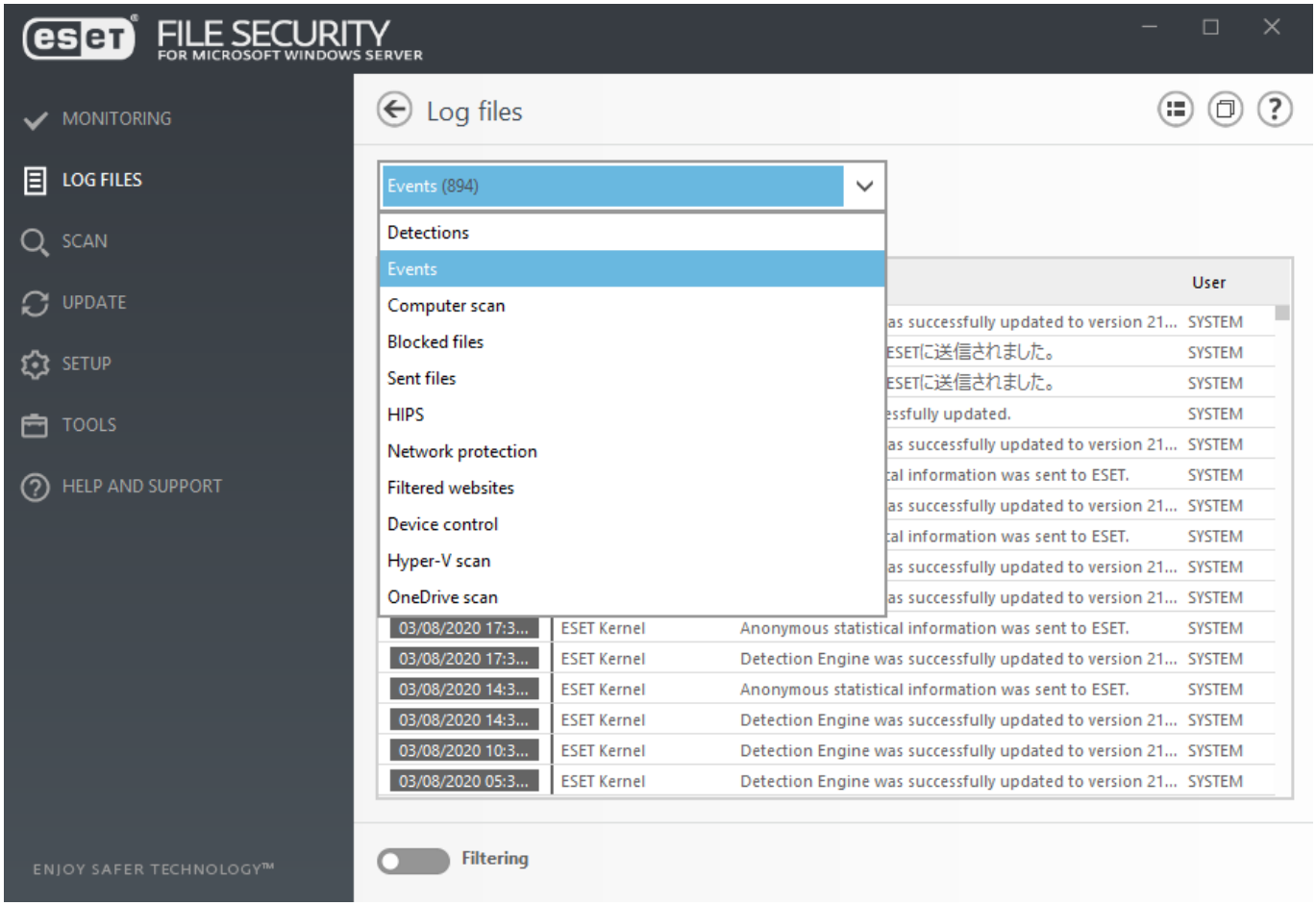
파일에 기록됩니다. 규칙이 연결된 장치와 일치하지 않으면 연결된 장치의 로그 항목이 생성되지 않습니다. 여기에서 장치 유형, 일련 번호, 공급업체 이름 및 미디어 크기(해당하는 경우) 등의 상세 정보도 확인할 수 있습니다.

Hyper-V 검사

Hyper-V 검사 결과의 목록을 포함합니다. 각 검사의 상세 정보를 보려면 항목을 두 번 클릭합니다.

OneDrive 검사

OneDrive 검사 결과의 목록을 포함합니다.



오른쪽 마우스 버튼 메뉴를 사용하면 선택한 로그 레코드 관련 동작을 선택할 수 있습니다.

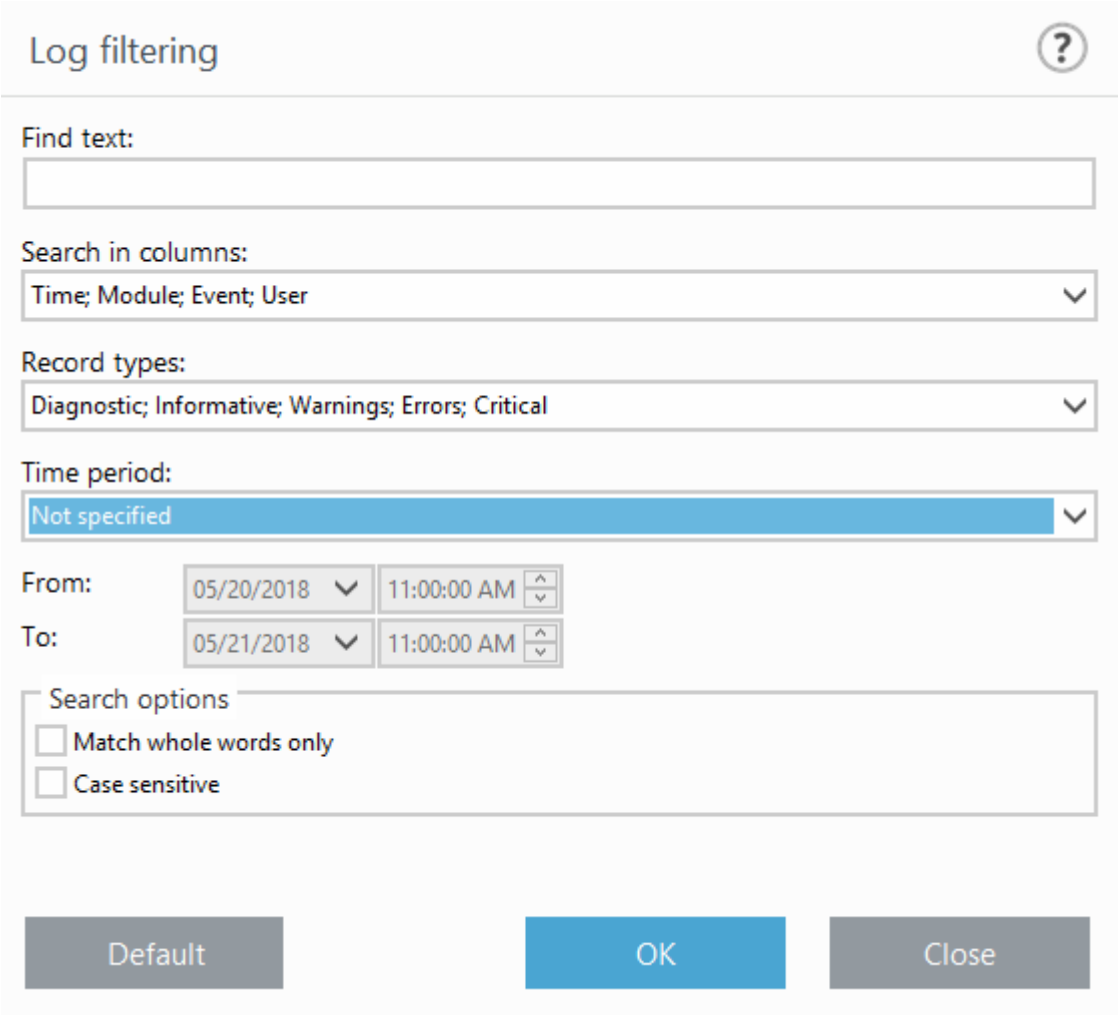
동작	사용	바로가기	추가 참조
표시	선택한 로그에 대한 자세한 정보를 새 창에 표시합니다(두 번 클릭한 것과 같음).		
같은 레코드 필터링	선택한 레코드와 같은 형식의 레코드만 표시하는 로그 필터링을 활성화합니다.	Ctrl + Shift + F 키	
필터링...	이 옵션을 클릭하면 로그 필터링 창에서 특정 로그 항목에 대한 필터링 기준을 정의할 수 있습니다.		로그 필터링
필터 활성화	필터 설정을 활성화합니다. 필터링을 처음 활성화할 때에는 설정을 정의해야 합니다.		
필터 비활성화	필터링을 끕니다(맨 아래의 전환 아이콘을 클릭한 것과 같음).		

동작	사용	바로가기	추가 참조
복사	선택/강조 표시된 레코드의 정보를 클립보드에 복사합니다.	Ctrl + C 키	
모두 복사	창에 있는 모든 레코드의 정보를 복사합니다.		
삭제	선택/강조 표시된 레코드 제거 - 이 동작을 수행하려면 관리자 권한이 필요합니다.		
모두 삭제	창에 있는 모든 레코드를 제거 - 이 동작을 수행하려면 관리자 권한이 필요합니다.		
내보내기...	선택/강조 표시된 레코드의 정보를 XML 파일로 내보냅니다.		
모두 내보내기...	창의 모든 정보를 XML 파일로 내보냅니다.		
찾기...	로그에서 찾기 창을 열어 검색 기준을 정의할 수 있습니다. 필터링이 켜져 있는 동안에도 기능 찾기를 사용하여 특정 레코드를 찾을 수 있습니다.	Ctrl + F 키	로그에서 찾기
다음 찾기	정의한 검색 기준에 일치하는 다음 항목을 찾습니다.	F3	
이전 찾기	이전 항목을 찾습니다.	Shift + F3 키	
제외 생성	탐지 이름, 경로 또는 해시를 사용하여 치료에서 개체를 제외합니다.		제외 생성

로그 필터링

로그 필터링 기능을 사용하면 특히 레코드가 많을 때 원하는 정보를 찾을 수 있습니다. 이 기능을 통해 예컨대 특별한 이벤트, 상태 또는 기간 유형을 찾는 경우 로그 레코드 범위를 좁힐 수 있습니다. 특정 검색 옵션을 지정하여 로그 레코드를 필터링할 수 있어 해당 검색 옵션에 따라 관련 있는 레코드만 로그 파일 창에 표시됩니다.

텍스트 찾기 필드에 검색할 키워드를 입력합니다. **열에서 검색** 드롭다운 메뉴를 사용하여 검색을 구체화합니다. **레코드 로그 종류** 드롭다운 메뉴에서 레코드를 하나 이상 선택합니다. 결과를 표시할 **기간**을 정의합니다. 또한 **단어 단위로** 또는 **대소문자 구분** 등의 추가 검색 옵션을 사용할 수 있습니다.



텍스트 찾기

문자열(단어 또는 단어의 일부분)을 입력합니다. 그러면 해당 문자열을 포함하는 레코드만 표시됩니다. 다른 레코드는 생략됩니다.

열에서 검색

검색 시 고려할 열을 선택합니다. 검색에 사용할 열을 하나 이상 선택할 수 있습니다.

레코드 종류

드롭다운 메뉴에서 레코드 로그 종류를 하나 이상 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.
- **중요** - 심각한 오류만 기록합니다.

기간

결과를 표시할 기간을 정의합니다.

- **지정되지 않음**(기본값) - 특정 기간 내에서 검색하지 않고 전체 로그를 검색합니다.
- **어제**

- **지난 주**
- **지난 달**
- **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.

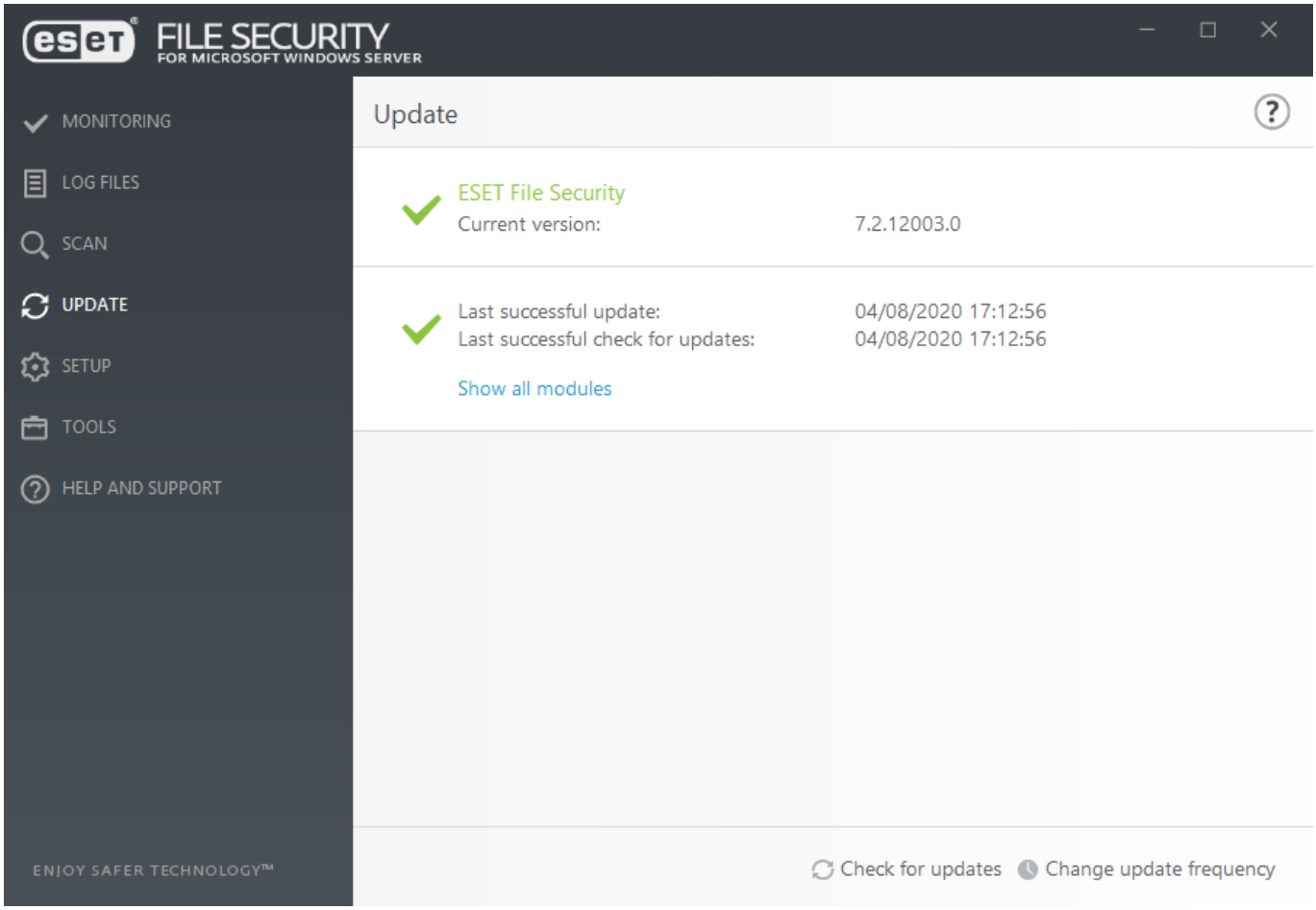
대소문자 구분

필터링하는 동안 대문자나 소문자를 사용하는 것이 중요한 경우 이 옵션을 활성화합니다. 필터링/검색 옵션을 구성한 후 필터링된 로그 레코드를 표시하려면 **확인**을 클릭하고, 검색을 시작하려면 **찾기**를 클릭합니다. 현재 위치(강조 표시된 레코드)를 시작으로 위에서 아래로 로그 파일을 검색합니다. 해당하는 첫 번째 레코드를 찾으면 검색이 중지됩니다. 다음 레코드를 검색하려면 **F3** 키를 누르고, 검색 옵션을 구체화하려면 **찾기**를 선택합니다.

업데이트

업데이트 섹션에서 마지막으로 성공한 업데이트 날짜와 시간 등 ESET File Security의 현재 업데이트 상태를 볼 수 있습니다. 서버의 보안 수준을 최대로 유지하기 위한 가장 좋은 방법은 ESET File Security를 정기적으로 업데이트하는 것입니다. 업데이트 모듈은 진단 엔진과 시스템 구성 요소를 업데이트하여 프로그램을 항상 최신 상태로 유지해 줍니다. 진단 엔진과 프로그램 구성 요소 업데이트는 악성 코드로부터 완벽히 보호하는 데 중요한 부분을 차지합니다.

> 참고
> 아직 라이선스 키를 입력하지 않았다면 업데이트를 수신할 수 없고 제품을 활성화하라는 메시지가 표시됩니다. 제품을 활성화하려면 **도움말 및 지원** > **제품 활성화**로 이동합니다.



현재 버전

ESET File Security 빌드 버전입니다.

마지막 업데이트

마지막 업데이트 날짜입니다. 이 날짜는 최근 날짜여야 합니다. 즉 모듈이 최신 상태여야 합니다.

마지막 업데이트 확인

마지막으로 모듈 업데이트를 시도한 날짜입니다.

모든 모듈 표시

설치된 모듈의 목록을 열 수 있습니다.

업데이트 확인

모듈 업데이트는 악성 코드로부터 완벽한 보호 성능을 유지하는 데 중요한 부분을 차지합니다.

업데이트 주기 변경

스케쥴러 작업 정기 자동 업데이트의 작업 타이밍을 편집할 수 있습니다.

최대한 빨리 업데이트를 확인하지 않으면 다음 메시지 중 하나가 표시됩니다.

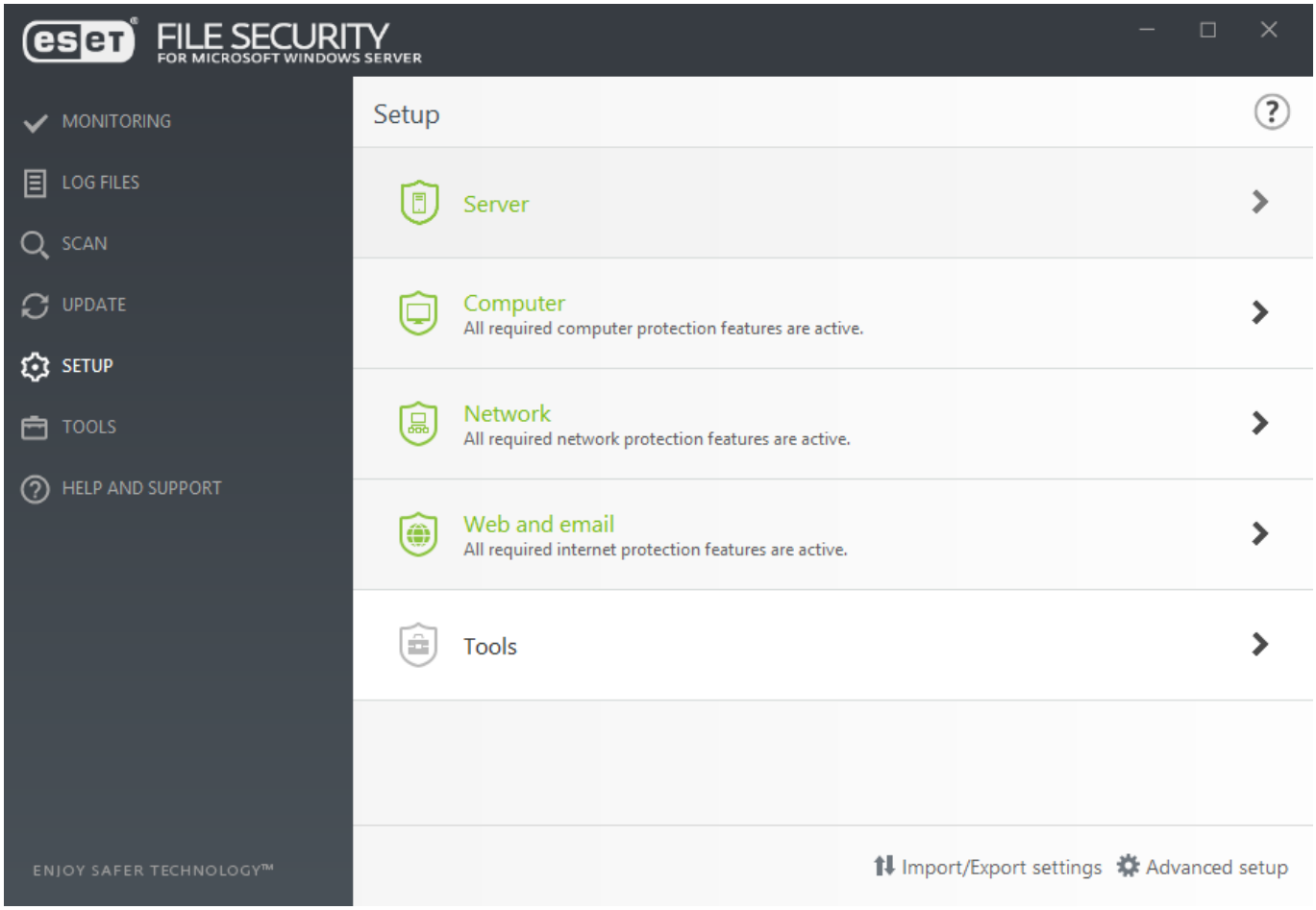
오류 메시지	설명
모듈 업데이트가 오래된 버전임	모듈 업데이트 시도에 여러 번 실패하면 이 오류가 나타납니다. 이 경우 업데이트 설정을 확인하는 것이 좋습니다. 이 오류가 발생하는 가장 일반적인 이유는 인증 데이터가 잘못 입력되거나, 연결 설정이 잘못 구성되었기 때문입니다.
모듈 업데이트 실패 - 제품이 활성화되지 않음	업데이트 설정에서 라이선스 키를 잘못 입력했습니다. 이 경우 인증 데이터를 확인하는 것이 좋습니다. **고급 설정**(**F5** 키)에는 추가 업데이트 옵션이 포함되어 있습니다. 새 라이선스 키를 입력하려면 기본 메뉴에서 **도움말 및 지원** > 라이선스 관리를 클릭합니다.
업데이트 파일을 다운로드하는 동안 오류가 발생했습니다	이 오류는 인터넷 연결 설정으로 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.
모듈 업데이트 실패 오류 0073	**업데이트** > **업데이트 확인**을 클릭합니다. 자세한 내용은 이 지식베이스 문서를 참조하십시오.

참고
다양한 업데이트 프로필의 프록시 서버 옵션은 서로 다를 수 있습니다. 프록시 서버 옵션이 서로 다른 경우 **업데이트** > 프로필을 클릭하여 **고급 설정**(**F5** 키)에서 다른 업데이트 프로필을 구성합니다.

설정

설정 메뉴 창에는 다음과 같은 섹션이 포함되어 있습니다.

- 서버
- 컴퓨터
- 네트워크
- 웹 및 이메일
- 도구 - 진단 로깅



개별 모듈을 일시적으로 비활성화하려면 해당하는 모듈 옆의 녹색 슬라이드 바를 클릭합니다. 그러면 서버의 보호 수준을 낮출 수 있습니다.

비활성화된 보안 구성 요소의 보호 기능을 다시 활성화하려면 해당하는 모듈 옆의 빨간색 슬라이드바를 클릭합니다. 구성 요소가 활성화된 상태로 반환됩니다.

특정 보안 구성 요소의 세부 설정에 접근하려면 톱니바퀴 아이콘을 클릭합니다.

설정 가져오기/내보내기

.xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장합니다.

고급 설정

필요에 따라 고급 설정과 옵션을 구성합니다. 프로그램의 어느 위치에서나 **고급 설정** 화면에 접근하려면 **F5** 키를 누릅니다.

서버

슬라이더 바를 사용하여 활성화/비활성화할 수 있는 구성 요소 목록이 표시됩니다. 특정 항목에 대한 설정을 구성하려면 톱니바퀴 아이콘을 클릭합니다.

자동 제외 항목

중요한 서버 애플리케이션과 서버 운영 체제를 확인하여 제외 항목 목록에 자동으로 추가합니다. 이 기능을 통해 위협 탐지 소프트웨어 실행 시의 잠재적 충돌 위험을 최소화하고 전반적인 서버 성능을 높일 수 있습니다.

클러스터

ESET 클러스터를 구성하고 활성화할 수 있습니다.

OneDrive 검사 설정

Microsoft OneDrive에서 ESET OneDrive 스캐너 애플리케이션을 등록하거나 등록 취소할 수 있습니다.

개별 모듈을 일시적으로 비활성화하려면 해당하는 모듈 옆의 녹색 슬라이드 바를 클릭합니다. 그러면 서버의 보호 수준을 낮출 수 있습니다.

비활성화된 보안 구성 요소의 보호 기능을 다시 활성화하려면 해당하는 모듈 옆의 빨간색 슬라이드바를 클릭합니다. 구성 요소가 활성화된 상태로 반환됩니다.

특정 보안 구성 요소의 세부 설정에 접근하려면 톱니바퀴 아이콘을 클릭합니다.

설정 가져오기/내보내기

.xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장합니다.

고급 설정

필요에 따라 고급 설정과 옵션을 구성합니다. 프로그램의 어느 위치에서나 **고급 설정** 화면에 접근하려면 **F5** 키를 누릅니다.

컴퓨터

ESET File Security에는 컴퓨터로 중요한 서버 보호 기능을 제공하는 데 필요한 모든 구성 요소가 있습니다. 이 모듈을 통해 다음 구성 요소를 활성화/비활성화하고 구성할 수 있습니다.

실시간 파일 시스템 보호

컴퓨터에서 모든 파일을 열거나 생성하거나 실행할 때 악성 코드가 있는지 검사합니다. 실시간 파일 시스템 보호의 경우 **구성** 또는 **제외 항목 편집** 옵션도 제공됩니다. 이 옵션을 클릭하면 검사에서 파일과 폴더를 제외할 수 있는 제외 설정 창이 열립니다.

장치 제어

이 모듈에서는 확장 필터/권한을 검사, 차단 또는 조정하고 사용자가 지정된 장치에 접근하여 사용하는 기능을 정의할 수 있습니다.

HIPS(호스트 침입 방지 시스템)

시스템은 운영 체제 내에서 발생하는 이벤트를 모니터링하고 사용자 지정 규칙 집합에 따라 반응합니다.

- 고급 메모리 스캐너
- Exploit 차단
- 랜섬웨어 보호

프레젠테이션 모드

소프트웨어를 중단 없이 사용하고 팝업 창의 방해를 받지 않으며 CPU의 사용을 최소화하려는 사용자를 위한 기능입니다. 프리젠테이션 모드를 활성화하면 경고 메시지(잠재적 보안 위험)가 수신되며 기본 프로그램 창이 주황색으로 바뀝니다.

안티바이러스 및 안티스파이웨어 보호 일시 중지

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

개별 모듈을 일시적으로 비활성화하려면 해당하는 모듈 옆의 녹색 슬라이드 바를 클릭합니다. 그러면 서버의 보호 수준을 낮출 수 있습니다.

비활성화된 보안 구성 요소의 보호 기능을 다시 활성화하려면 해당하는 모듈 옆의 빨간색 슬라이드바를 클릭합니다. 구성 요소가 활성화된 상태로 반환됩니다.

특정 보안 구성 요소의 세부 설정에 접근하려면 톱니바퀴 아이콘을 클릭합니다.

설정 가져오기/내보내기

.xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장합니다.

고급 설정

필요에 따라 고급 설정과 옵션을 구성합니다. 프로그램의 어느 위치에서나 **고급 설정** 화면에 접근하려면 **F5** 키를 누릅니다.

네트워크

이 작업은 필터링 규칙을 기준으로 개별 네트워크 연결을 허용하거나 거부하는 방식으로 수행됩니다. 방화벽은 원격 컴퓨터의 공격으로부터 보호하고 잠재적으로 위험한 일부 서비스를 차단합니다.

네트워크 모듈을 통해 다음 구성 요소를 활성화/비활성화하거나 구성할 수 있습니다.

네트워크 공격 보호(IDS)

네트워크 트래픽의 콘텐츠를 분석하고 네트워크 공격에서 보호합니다. 유해한 것으로 간주되는 트래픽이 차단됩니다.

봇넷 보호

봇넷 통신을 검색하고 차단합니다. 시스템에서 악성코드를 빠르고 정확하게 식별합니다.

일시적인 IP 주소 차단 목록(차단된 주소)

공격의 근원지로 검색되고 특정 기간 동안 연결을 차단하도록 차단 목록에 추가된 IP 주소 목록 보기

문제 해결 마법사(최근에 차단된 애플리케이션 또는 장치)

네트워크 공격 보호로 인한 연결 문제를 해결하도록 도와줍니다.

개별 모듈을 일시적으로 비활성화하려면 해당하는 모듈 옆의 녹색 슬라이드 바를 클릭합니다. 그러면 서버의 보호 수준을 낮출 수 있습니다.

비활성화된 보안 구성 요소의 보호 기능을 다시 활성화하려면 해당하는 모듈 옆의 빨간색 슬라이드바를 클릭합니다. 구성 요소가 활성화된 상태로 반환됩니다.

특정 보안 구성 요소의 세부 설정에 접근하려면 톱니바퀴 아이콘을 클릭합니다.

설정 가져오기/내보내기

.xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장합니다.

고급 설정

필요에 따라 고급 설정과 옵션을 구성합니다. 프로그램의 어느 위치에서나 **고급 설정** 화면에 접근하려면 **F5** 키를 누릅니다.

네트워크 문제 해결 마법사

문제 해결 마법사는 차단된 모든 연결을 모니터링하고 특정 애플리케이션 또는 장치에 있는 네트워크 공격 보호 문제를 해결하기 위한 문제 해결 프로세스를 안내합니다. 그런 다음 마법사는 사용자가 승인할 경우 적용할 새 규칙 집합을 제안합니다.

웹 및 이메일

웹 및 이메일을 통해 다음 구성 요소를 활성화/비활성화하고 구성할 수 있습니다.

웹 브라우저 보호

활성화하면 모든 HTTP 또는 HTTPS 트래픽에 악성 소프트웨어가 있는지 검사합니다.

이메일 클라이언트 보호

POP3 및 IMAP 프로토콜을 통해 받은 통신을 모니터링합니다.

안티피싱 보호

적법한 웹 사이트로 가장한 불법 웹 사이트를 통해 패스워드, 뱅킹 데이터 및 기타 중요한 정보를 획득하려는 시도로부터 보호해 줍니다.

개별 모듈을 일시적으로 비활성화하려면 해당하는 모듈 옆의 녹색 슬라이드 바를 클릭합니다. 그러면 서버의 보호 수준을 낮출 수 있습니다.

비활성화된 보안 구성 요소의 보호 기능을 다시 활성화하려면 해당하는 모듈 옆의 빨간색 슬라이드바를 클릭합니다. 구성 요소가 활성화된 상태로 반환됩니다.

특정 보안 구성 요소의 세부 설정에 접근하려면 톱니바퀴 아이콘을 클릭합니다.

설정 가져오기/내보내기

.xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장합니다.

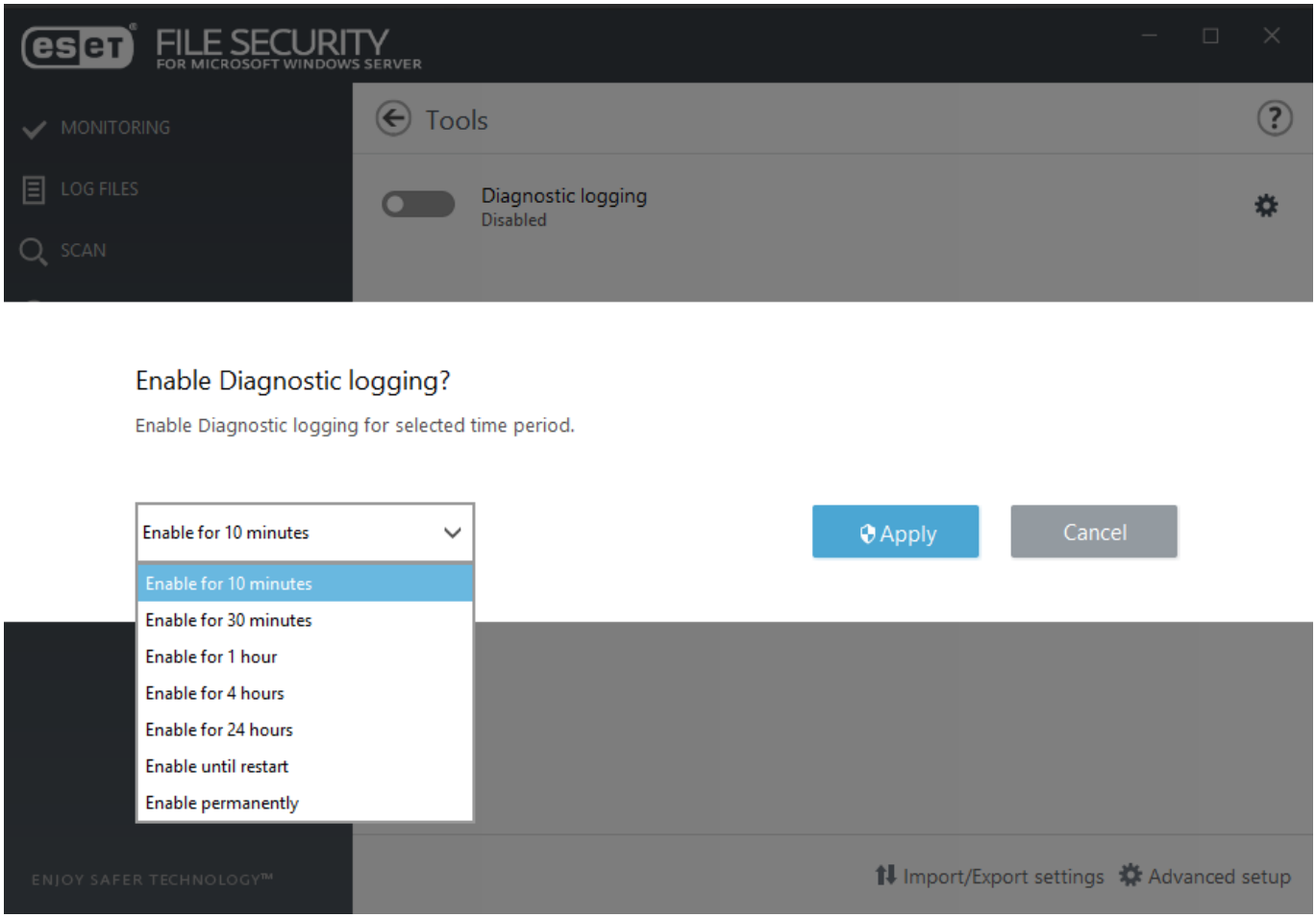
고급 설정

필요에 따라 고급 설정과 옵션을 구성합니다. 프로그램의 어느 위치에서나 **고급 설정** 화면에 접근하려면 **F5** 키를 누릅니다.

도구 - 진단 로깅

예를 들면 문제 해결 시 같은 특정 ESET File Security 기능의 동작에 대한 상세 정보가 필요한 경우 진단 로깅을 활성화할 수 있습니다. 톱니바퀴 아이콘을 클릭하면 진단 로그를 수집하는 기능을 구성할 수 있습니다.

활성화 기간(10분, 30분, 1시간, 4시간, 24시간, 다음에 서버를 다시 시작할 때까지 또는 영구적으로)을 선택합니다. 진단 로깅을 켜면 ESET File Security에서 활성화된 기능에 따라 상세 로그를 수집하게 됩니다.



개별 모듈을 일시적으로 비활성화하려면 해당하는 모듈 옆의 녹색 슬라이드 바를 클릭합니다. 그러면 서버의 보호 수준을 낮출 수 있습니다.

비활성화된 보안 구성 요소의 보호 기능을 다시 활성화하려면 해당하는 모듈 옆의 빨간색 슬라이드바를 클릭합니다. 구성 요소가 활성화된 상태로 반환됩니다.

특정 보안 구성 요소의 세부 설정에 접근하려면 톱니바퀴 아이콘을 클릭합니다.

설정 가져오기/내보내기

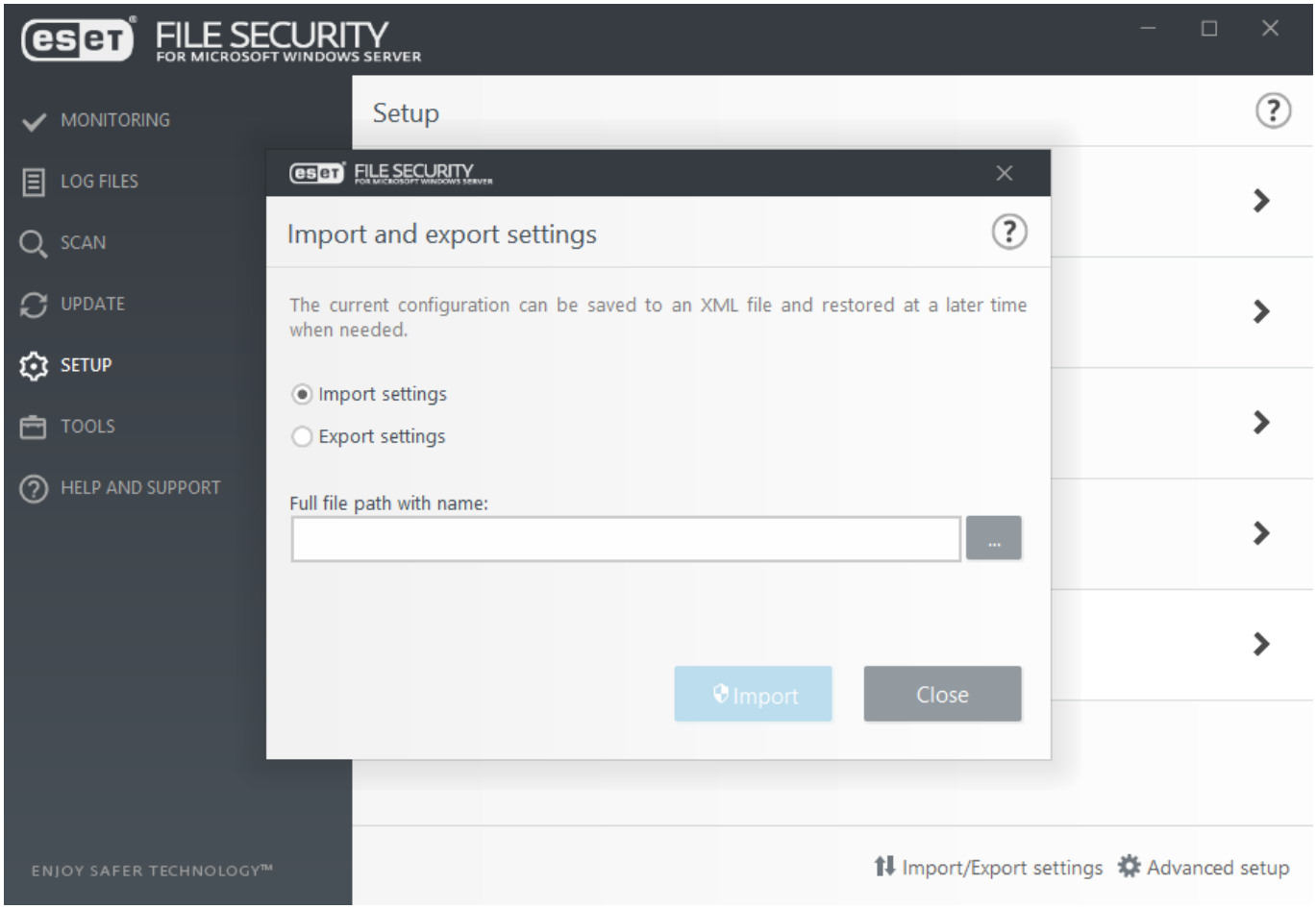
.xml 구성 파일을 사용하여 설정 파라미터를 로드하거나 현재 설정 파라미터를 구성 파일에 저장합니다.

고급 설정

필요에 따라 고급 설정과 옵션을 구성합니다. 프로그램의 어느 위치에서나 **고급 설정** 화면에 접근하려면 **F5** 키를 누릅니다.

설정 가져오기 및 내보내기

가져오기/내보내기 설정 기능은 현재 ESET File Security 구성을 백업해야 할 경우에 유용합니다. 또한 가져오기 기능을 사용하여 ESET File Security가 있는 다른 서버에 동일한 설정을 배포/적용할 수 있습니다. 설정은 *.xml* 파일로 내보내집니다.

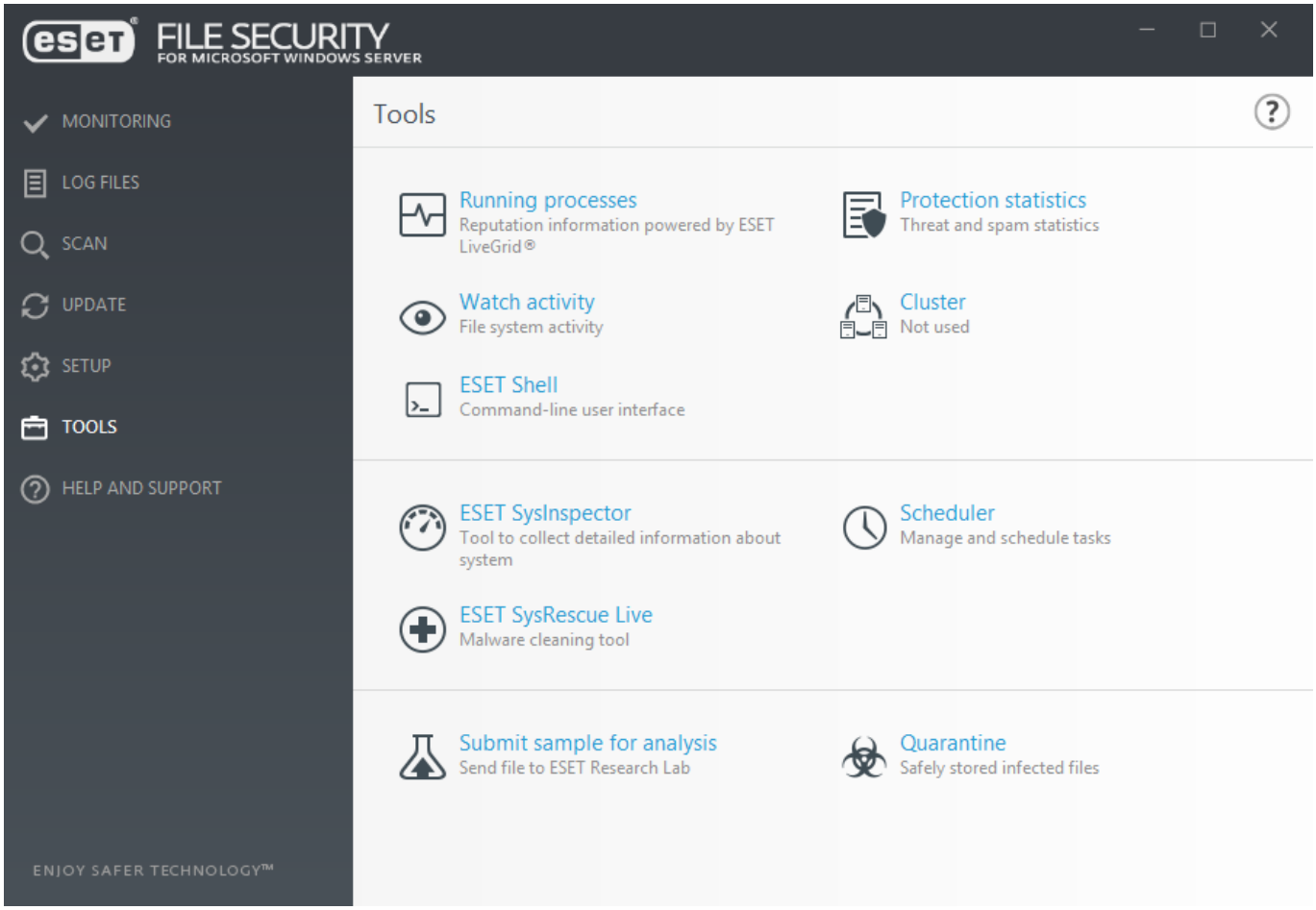


참고
지정된 디렉터리에 내보낸 파일을 작성할 권한이 없으면 설정을 내보내는 동안 오류가 발생할 수 있습니다.

도구

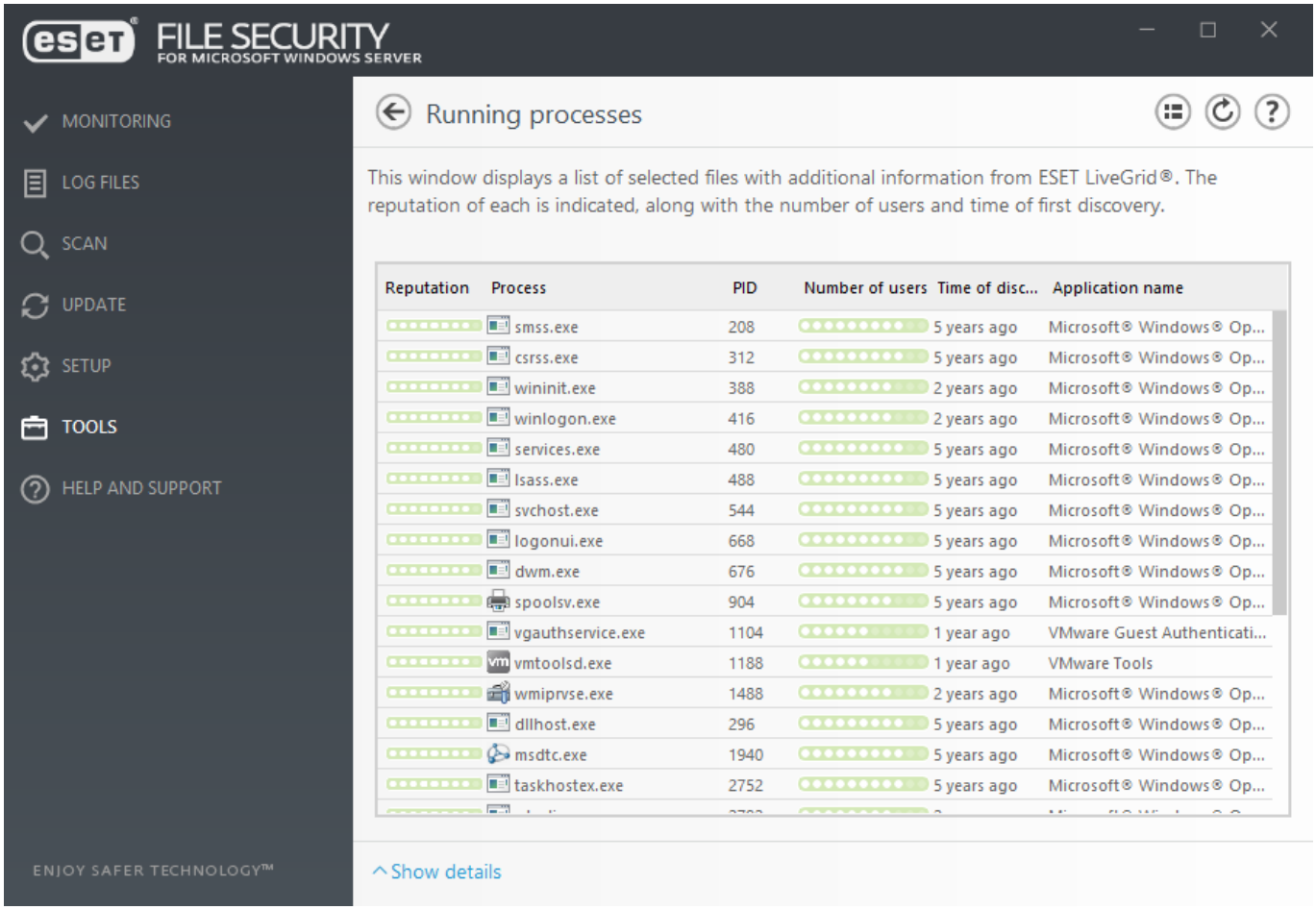
ESET File Security 관리에서 사용할 수 있는 기능은 다음과 같습니다.

- 실행 중인 프로세스
- 감시 활동
- 보호 통계
- 클러스터
- ESET Shell
- ESET Dynamic Threat Defense
- ESET SysInspector
- ESET SysRescue Live
- 스케줄러
- 분석을 위해 샘플 전송
- 검역소



실행 중인 프로세스

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



참고
최고 평판(녹색)으로 지정된 알려진 애플리케이션은 감염되지 않아(허용 목록에 포함됨) 검사에서 제외됩니다. 그래서 컴퓨터에서 실시간 파일 시스템 보호나 수동 검사 시 검사 속도가 향상됩니다.

평판	**대부분의 경우 ESET File Security 및 ESET LiveGrid® 기술에서는 각 개체의 특성(파일, 프로세스, 레지스트리 키 등)을 검사하고 악의적인 활동의 잠재성에 대한 심각도를 매기는 일련의 휴리스틱 규칙을 사용하여 개체 평판을 결정합니다. 휴리스틱을 기준으로 개체에 9 - 최고 평판(녹색)에서 0 - 최악 평판(빨간색)까지의 평판 수준이 지정됩니다.**
프로세스	현재 컴퓨터에서 실행 중인 프로그램 또는 프로세스의 이미지 이름입니다. Windows 작업 관리자를 사용하여 컴퓨터에서 실행 중인 프로세스를 모두 볼 수도 있습니다. 작업 관리자는 작업 표시줄의 빈 영역을 오른쪽 마우스 버튼으로 클릭한 다음 작업 관리자를 클릭하거나, 키보드에서 Ctrl + Shift + Esc 키를 눌러 열 수 있습니다.
PID	Windows 운영 체제에서 실행 중인 프로세스의 ID입니다.
사용자 수	지정된 애플리케이션을 이용하는 사용자 수입니다. 이 정보는 ESET LiveGrid® 기술을 통해 수집됩니다.
검색 시간	ESET LiveGrid® 기술에 의해 애플리케이션이 발견된 이후의 시간입니다.
애플리케이션 이름	이 프로세스가 속한 프로그램에 대해 지정된 이름입니다.

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

상세 정보 표시

창 아래쪽에 다음 정보가 나타납니다.

- **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.
- **생성 날짜** - 애플리케이션이 생성된 날짜와 시간입니다.
- **수정 날짜** - 애플리케이션이 마지막으로 수정된 날짜와 시간입니다.

프로세스 제외 항목에 추가

검사에서 항목을 제외하려면 실행 중인 프로세스 창에서 프로세스를 마우스 오른쪽 버튼으로 클릭합니다. 해당 경로는 프로세스 제외 목록에 추가됩니다.

감시 활동

그래픽 형식의 활동이 포함된 활동을 감시하려면 드롭 다운 메뉴에서 다음 활동을 선택합니다.

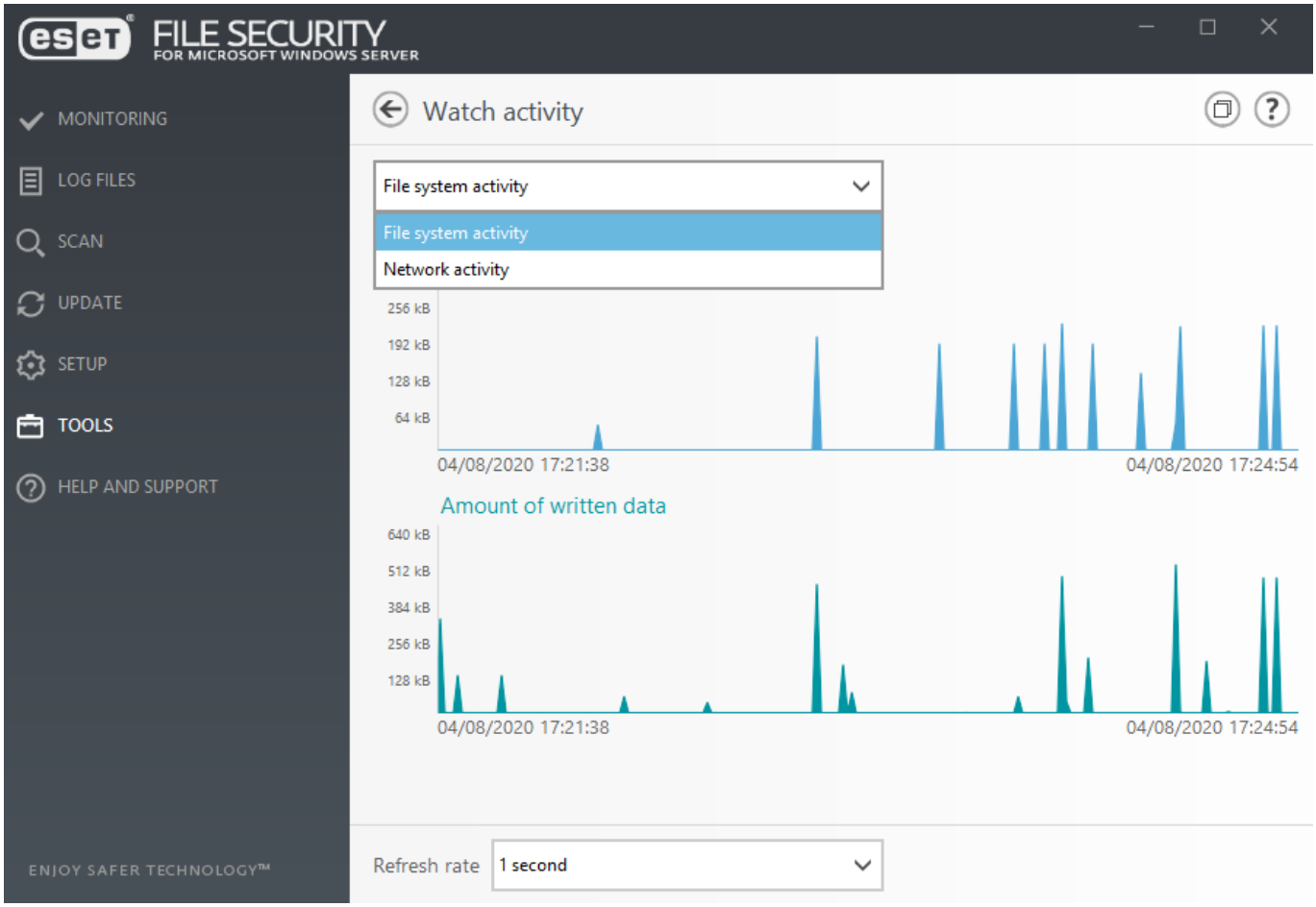
파일 시스템 활동

읽거나 기록한 데이터의 양입니다. 그래프의 세로 축은 읽은 데이터(파란색)와 기록한 데이터(녹색)를 나타냅니다.

네트워크 활동

받거나 보낸 데이터의 양입니다. 그래프의 세로 축은 받은 데이터(파란색)와 보낸 데이터(녹색)를 나타냅니다.

그래프 아래쪽에는 선택한 시간 범위를 기준으로 파일 시스템 활동을 실시간으로 기록하는 시간 표시줄이 있습니다. **새로 고침 빈도** 드롭다운 메뉴를 사용하여 업데이트 빈도를 변경합니다.

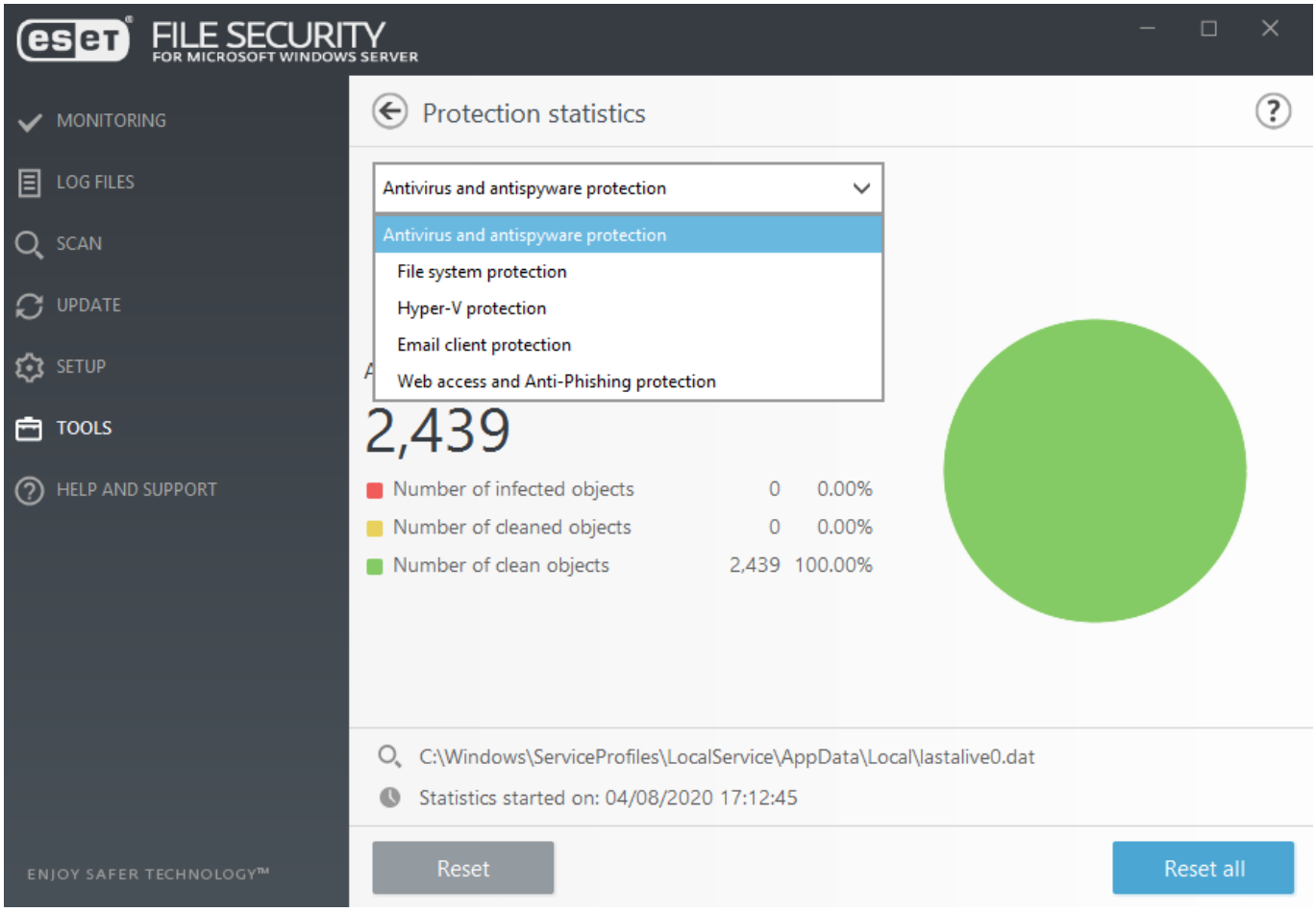


다음과 같은 옵션을 사용할 수 있습니다.

1초	**그래프가 1초마다 새로 고쳐지고 시간 표시줄이 지난 10분을 나타냅니다.**
1분(지난 24시간)	그래프가 1분마다 새로 고쳐지고 시간 표시줄이 지난 24시간을 나타냅니다.
1시간(지난 달)	그래프가 1시간마다 새로 고쳐지고 시간 표시줄이 지난달을 나타냅니다.
1시간(선택한 달)	그래프가 1시간마다 새로 고쳐지고 시간 표시줄이 선택한 달을 나타냅니다. 활동을 보려면 드롭다운 메뉴에서 한 달(1년)을 선택합니다. **변경**을 클릭합니다.

보호 통계

ESET File Security의 보호 모듈과 관련된 통계 데이터를 보려면 드롭다운 메뉴에서 해당하는 보호 모듈을 선택합니다. 통계에는 검사한 모든 개체 수, 감염된 개체 수, 치료된 개체 수, 감염되지 않은 개체 수 등의 정보가 포함됩니다. 그래프 옆에 있는 개체 위에 올려 놓으면 특정 개체의 데이터만 그래프에 표시됩니다. 현재 보호 모듈의 통계 정보를 지우려면 **다시 설정**을 클릭합니다. 모듈 모듈의 데이터를 지우려면 **모두 다시 설정**을 클릭합니다.



ESET File Security에서는 다음의 통계 그래프를 사용할 수 있습니다.

안티바이러스, 안티스파이웨어 보호

감염된 개체와 치료된 개체의 전체 수를 표시합니다.

파일 시스템 보호

파일 시스템에서 읽었거나 파일 시스템에 기록한 개체만 표시합니다.

Hyper-V 보호

감염된 개체와 치료된 개체, 감염되지 않은 개체의 전체 수를 표시합니다.

이메일 클라이언트 보호

이메일 클라이언트를 통해 주고받은 개체만 표시합니다.

웹 브라우저 및 안티피싱 보호

웹 브라우저를 통해 다운로드한 개체만 표시합니다.

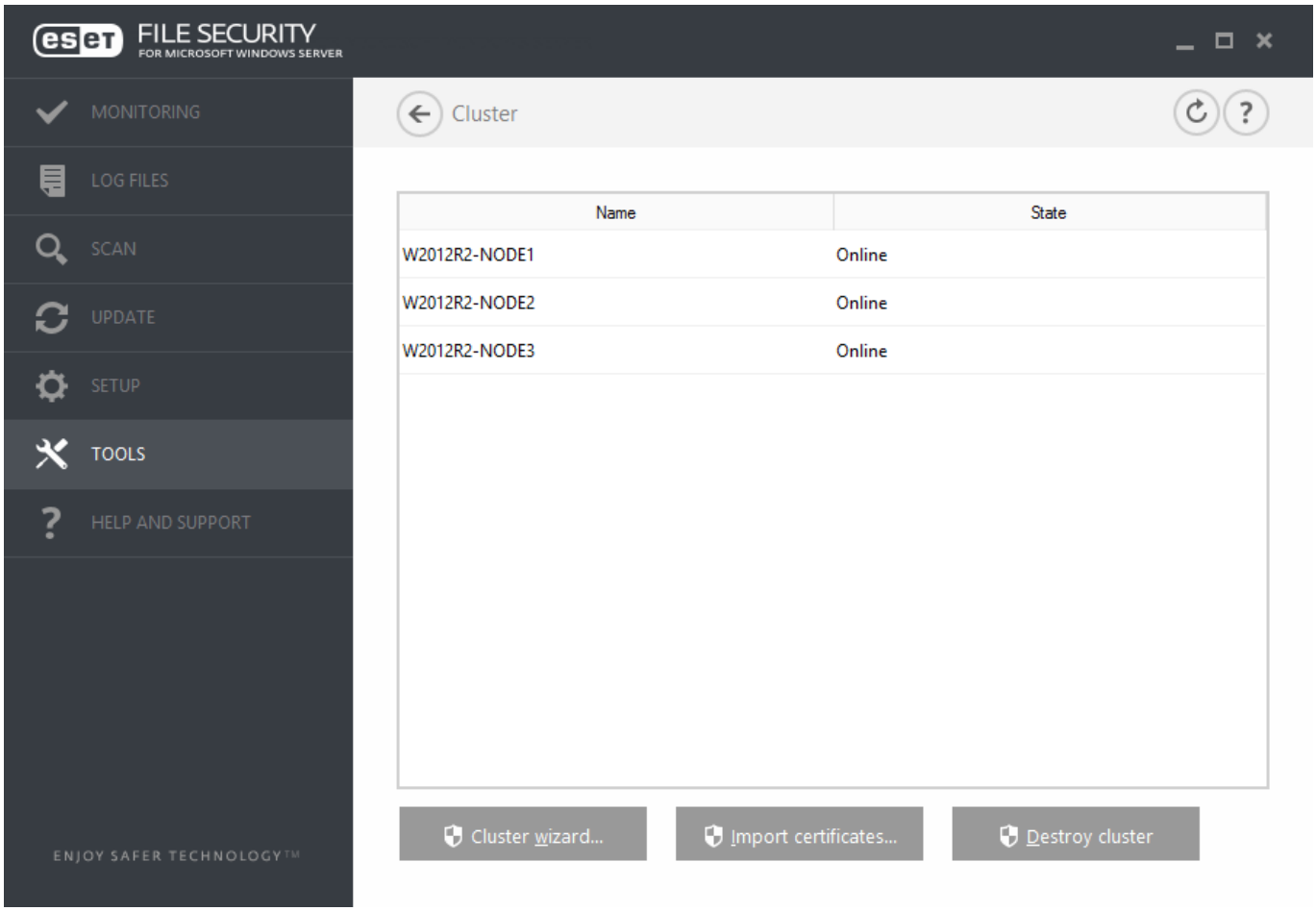
클러스터

ESET 클러스터는 Microsoft Windows Server용 ESET 제품군의 P2P 통신 인프라입니다.

이 인프라를 통해 ESET 서버 제품은 서로 통신하며 구성 및 알림 등의 데이터를 교환할 수 있고 제품 인스턴스 그룹의 올바른 작업에 필요한 데이터를 동기화할 수 있습니다. 예를 들어 ESET 제품이 설치되어 있으며, 클러스터 전반에 같은 제품 구성을 사용해야 하는 Windows 장애 조치(Failover) 클러스터 또는 NLB(네트워크 부하 분산) 클러스터의 노드 그룹이 이러한 그룹에 해당합니다. ESET 클러스터를 통해 인스턴스 간의 일관성이 유지됩니다.

참고
사용자 인터페이스 설정은 ESET 클러스터 노드 간에 동기화되지 않습니다.

ESET 클러스터 상태 페이지는 **도구 > 클러스터**의 기본 메뉴에서 접근할 수 있습니다. 올바르게 구성된 경우 상태 페이지는 아래 그림과 같이 나타납니다.



참고
ESET File Security와 Linux용 ESET File Security 간에는 ESET 클러스터를 생성할 수 없습니다.

ESET 클러스터를 설정할 때 두 가지 방식으로 노드를 추가할 수 있습니다.

자동 검색

기존 Windows 장애 조치(Failover) 클러스터/NLB 클러스가 있는 경우 자동 검색에서 해당 구성원 노드를 ESET 클러스터에 자동으로 추가합니다.

찾아보기

서버 이름(동일한 작업 이름 또는 동일한 도메인의 구성원)을 입력하여 노드를 수동으로 추가할 수 있습니다.

참고
서버가 ESET 클러스터 기능을 사용하기 위해 Windows 장애 조치(Failover) 클러스터/NLB 클러스터의 구성원일 필요는 없습니다. Windows 장애 조치(Failover) 클러스터 또는 NLB 클러스터가 사용자 환경에 없어도 ESET 클러스터를 사용할 수 있습니다.

노드를 ESET 클러스터에 추가한 후 다음 단계에서 각 노드에 ESET File Security를 설치합니다. 이 작업은 ESET 클러스터를 설정하는 동안 자동으로 수행됩니다. 다른 클러스터 노드에 ESET File Security를 원격으로 설치하려면 다음 자격 증명이 필요합니다.

도메인 시나리오

도메인 관리자 자격 증명입니다.

작업 그룹 시나리오

모든 노드에서 동일한 로컬 관리자 계정 자격 증명을 사용해야 합니다.

ESET 클러스터에서는 기존 Windows 장애 조치(Failover) 클러스터/NLB 클러스터의 구성원으로 자동 추가된 노드를 같은 도메인의 구성원으로 수동 추가된 노드와 함께 사용할 수도 있습니다.

중요
도메인 노드와 작업 그룹 노드를 결합할 수는 없습니다.

ESET 클러스터를 사용하기 위한 또 다른 요구 사항은 ESET File Security를 ESET 클러스터 노드로 부시하기 전에 **파일 및 프린터 공유**가 Windows 방화벽에서 활성화되어 있어야 한다는 점입니다.

클러스터 마법사를 실행해서 언제든지 기존 ESET 클러스터에 새 노드를 추가할 수 있습니다.

인증서 가져오기

자격 증명은 HTTPS이 사용될 때 컴퓨터 인증에 강력한 컴퓨터를 제공하는 데 사용할 수 있습니다. 각 ESET 클러스터에 독립적인 인증서 계층이 있습니다. 계층에는 루트 인증서 한 개와 루트 인증서에 의해 지문이 생성된 노드 인증서 집합 한 개가 있습니다. 루트 인증서의 개인 키는 모든 노드 인증서가 생성된 후에 폐기됩니다. 새 노드를 클러스터에 추가하면 새 인증서 계층이 생성됩니다. 클러스터 마법사를 실행하는 동안 생성된 인증서를 포함하는 폴더로 이동합니다. 인증서 파일을 선택하고 **열기**를 클릭합니다.

클러스터 폐기

ESET 클러스터는 구성을 해제할 수 있습니다. 각 노드는 해당 이벤트 로그에 폐기 중인 ESET 클러스터 관련 레코드를 기록합니다. 그러고 나면 모든 ESET 방화벽 규칙이 Windows 방화벽에서 제거됩니다. 이전 노드는 해당 노드의 이전 상태로 되돌아가고, 필요한 경우 다른 ESET 클러스터에 다시 사용될 수 있습니다.

클러스터 마법사 - 노드 선택

ESET 클러스터를 설정하는 첫 단계는 노드를 추가하는 것입니다. **자동 검색** 옵션을 사용하거나 **찾아보기**를 사용하여 노드를 추가할 수 있습니다. 또는 서버 이름을 텍스트 상자에 입력한 다음 **추가**를 클릭합니다.

자동 검색

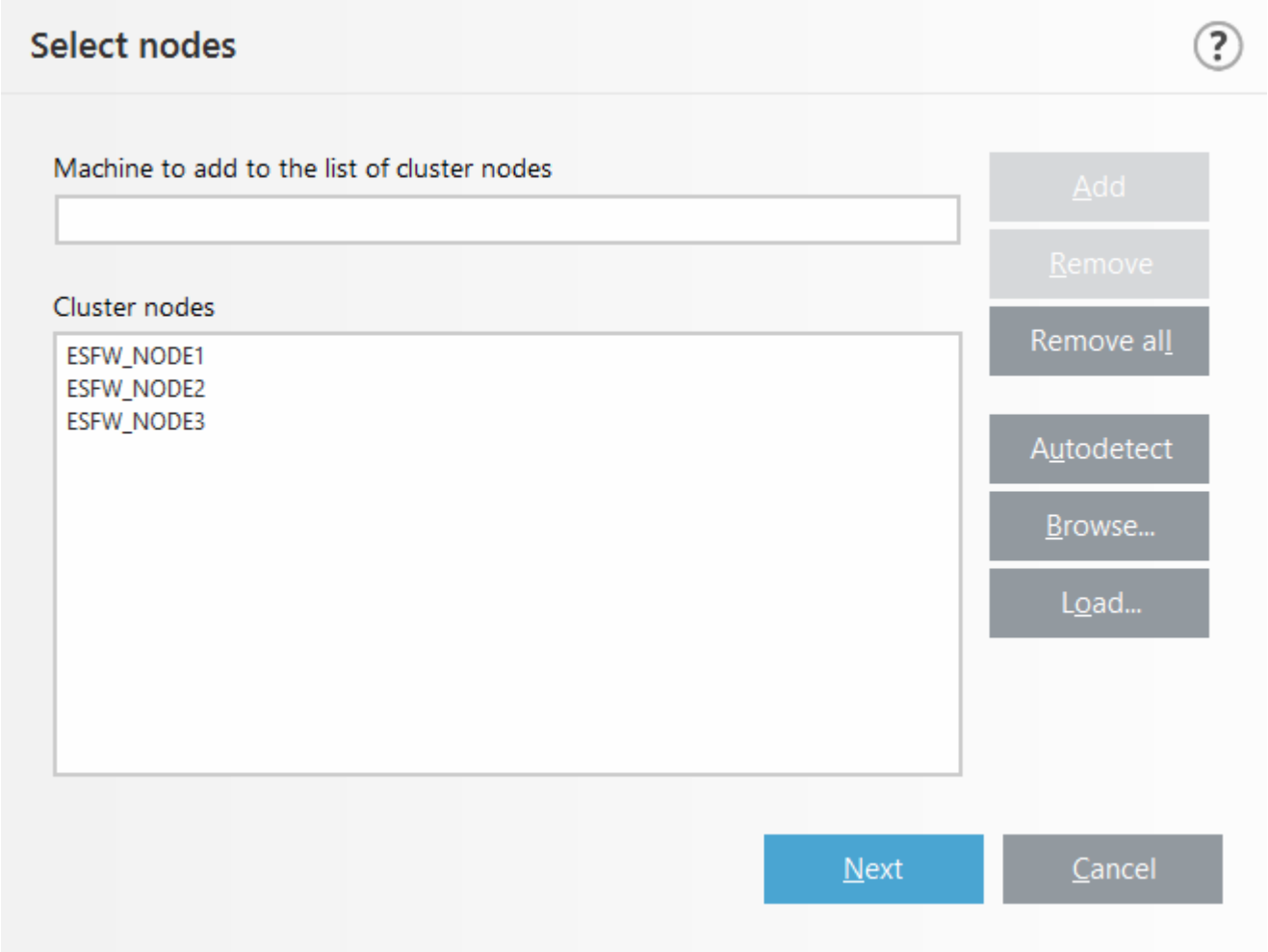
기존 Windows 장애 조치(Failover) 클러스터/NLB(네트워크 부하 분산) 클러스터에서 노드를 자동으로 추가합니다. 노드를 자동으로 추가하려면 ESET 클러스터를 만드는 데 사용할 서버가 이 Windows 장애 조치(Failover) 클러스터/NLB 클러스터의 구성원이어야 합니다. NLB 클러스터의 경우 **원격 검사 허용** 기능이 ESET 클러스터의 클러스터 속성에서 활성화되어 있어야 노드를 올바르게 검색할 수 있습니다. 새로 추가된 노드 목록이 표시되면 원치 않는 노드를 제거할 수 있습니다.

찾아보기

도메인이나 작업 그룹에 있는 컴퓨터를 찾아서 선택할 수 있습니다. 이 방법을 사용하면 ESET 클러스터에 노드를 수동으로 추가할 수 있습니다. 노드를 추가하는 또 다른 방법으로, 추가할 서버의 호스트 이름을 입력한 다음 **추가**를 클릭하는 방법이 있습니다.

로드

파일에서 노드 목록을 가져옵니다.



클러스터 노드 목록을 수정하려면 제거할 노드를 선택한 다음 **제거**를 클릭하거나, **모두 제거**를 클릭하여 전체 목록을 지웁니다.

기존 ESET 클러스터가 이미 있는 경우 언제든지 새 노드를 추가할 수 있습니다. 위와 같은 방식으로 노드를 새로 추가할 수 있습니다.

> 참고
> 목록에 남아 있는 모든 노드는 온라인 상태로 연결 가능해야 합니다. Localhost는 기본적으로 클러스터 노드에 추가됩니다.

클러스터 마법사 - 클러스터 설정

클러스터 이름과 네트워크 사양(필요한 경우)을 정의합니다.

클러스터 이름

클러스터 이름을 입력하고 **다음**을 클릭합니다.

수신 대기 포트(기본 포트: 9777)

네트워크 환경에서 포트 9777을 이미 사용 중인 경우 사용하고 있지 않은 다른 포트 번호를 지정합니다.

Windows 방화벽에서 포트 열기

선택한 규칙이 Windows 방화벽에 생성됩니다.

클러스터 마법사 - 클러스터 설정

인증서 배포 모드를 정의하고 제품을 다른 노드에 설치할지 여부를 정의합니다.

인증서 배포

- **자동 원격** - 인증서가 자동으로 설치됩니다.
- **수동** - **생성**을 클릭하고 인증서를 저장하기에 적합한 폴더를 선택합니다. ESET 클러스터를 설정할 노드(로컬 컴퓨터)를 비롯해 각 노드에 대한 인증서와 루트 인증서가 생성됩니다. 로컬 컴퓨터에 인증서를 등록하려면 **예**를 클릭합니다.

다른 노드에 제품 설치

- **자동 원격** - ESET File Security가 각 노드에 자동으로 설치됩니다(설치되는 노드의 운영 체제 아키텍처가 모두 같은 경우).
- **수동** - ESET File Security를 수동으로 설치합니다(예: 일부 노드의 OS 아키텍처가 다른 경우).

제품을 활성화하지 않고 노드에 라이선스 푸시

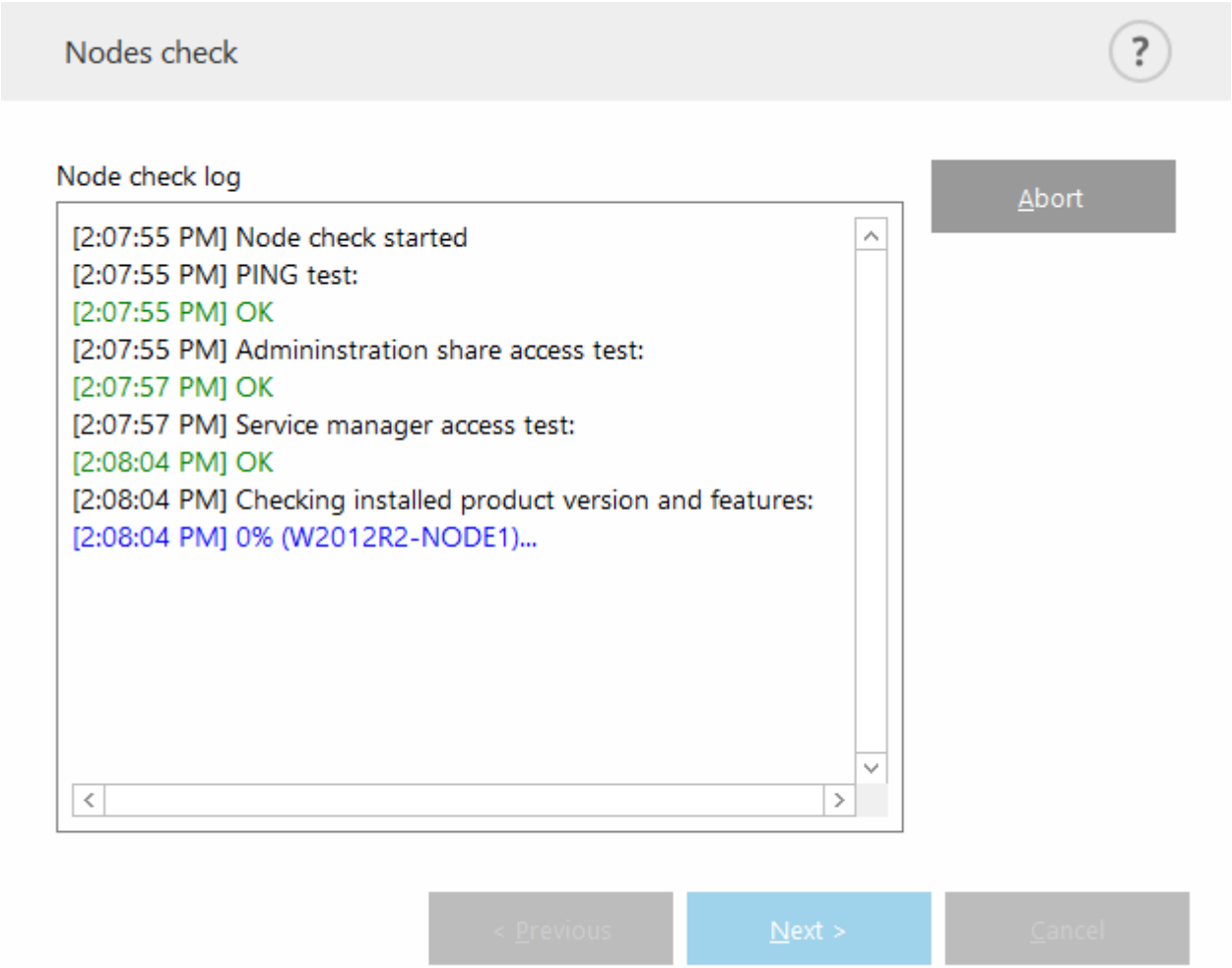
ESET Security가 라이선스 없이 노드에 설치된 ESET 솔루션을 자동으로 활성화합니다.

> 참고
> 운영 체제 아키텍처가 혼합(32비트, 64비트)된 ESET 클러스터를 생성하려면 ESET File Security를 수동으로 설치합니다. 사용 중인 운영 체제가 다음 단계에서 검색되어 로그 창에서 이 정보를 확인할 수 있습니다.

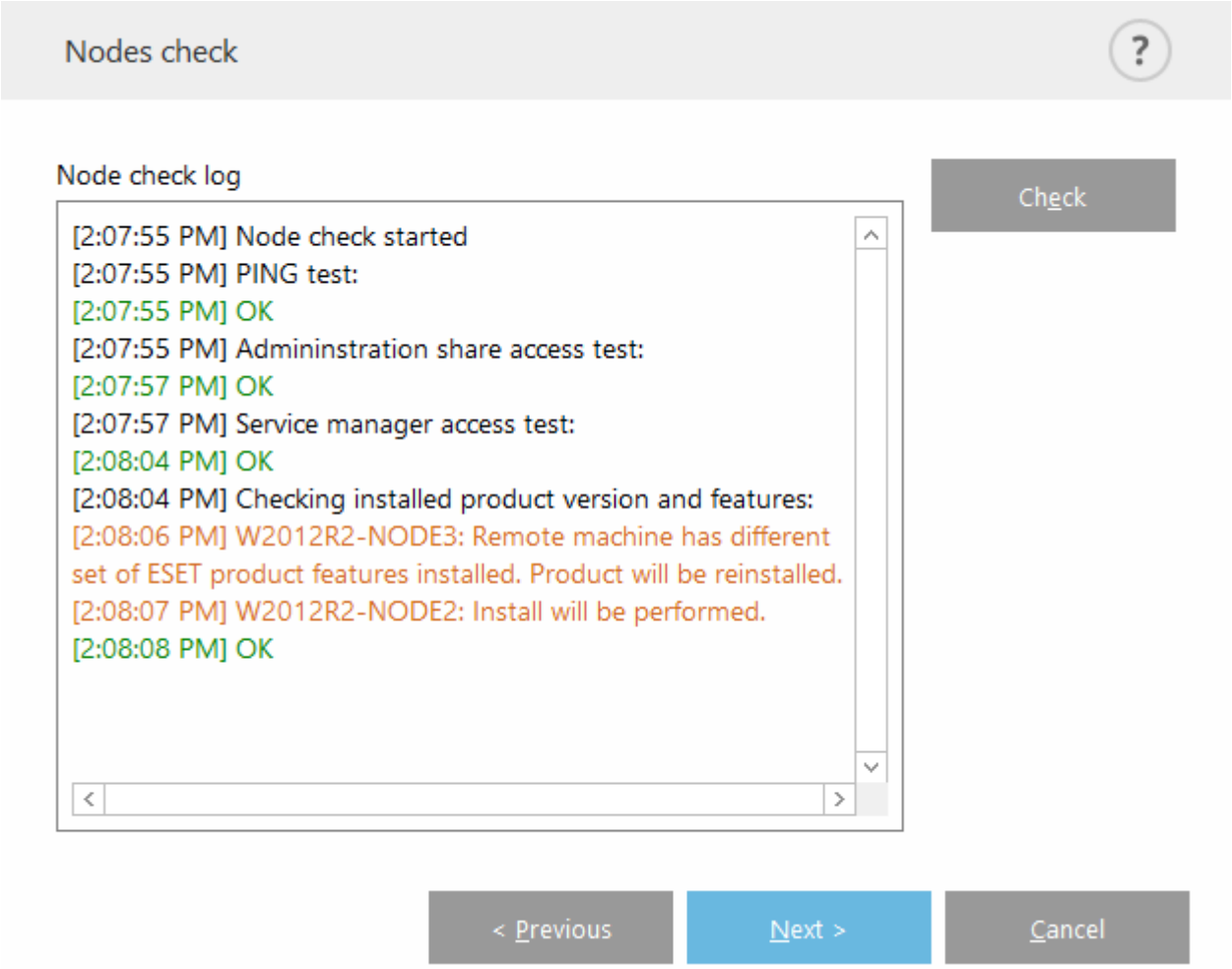
클러스터 마법사 - 노드 확인

설치 상세 정보를 지정한 후에는 노드 확인이 실행됩니다. **노드 확인 로그**에 표시되는 정보는 다음과 같습니다.

- 기존 노드가 모두 온라인 상태인지 확인
- 새 노드가 접근 가능한 상태인지 확인
- 노드가 온라인 상태임
- 관리자 공유가 접근 가능한 상태임
- 원격 실행이 가능함
- 올바른 제품 버전(또는 제품이 없음)이 설치됨
- 새 인증서가 있는지 확인

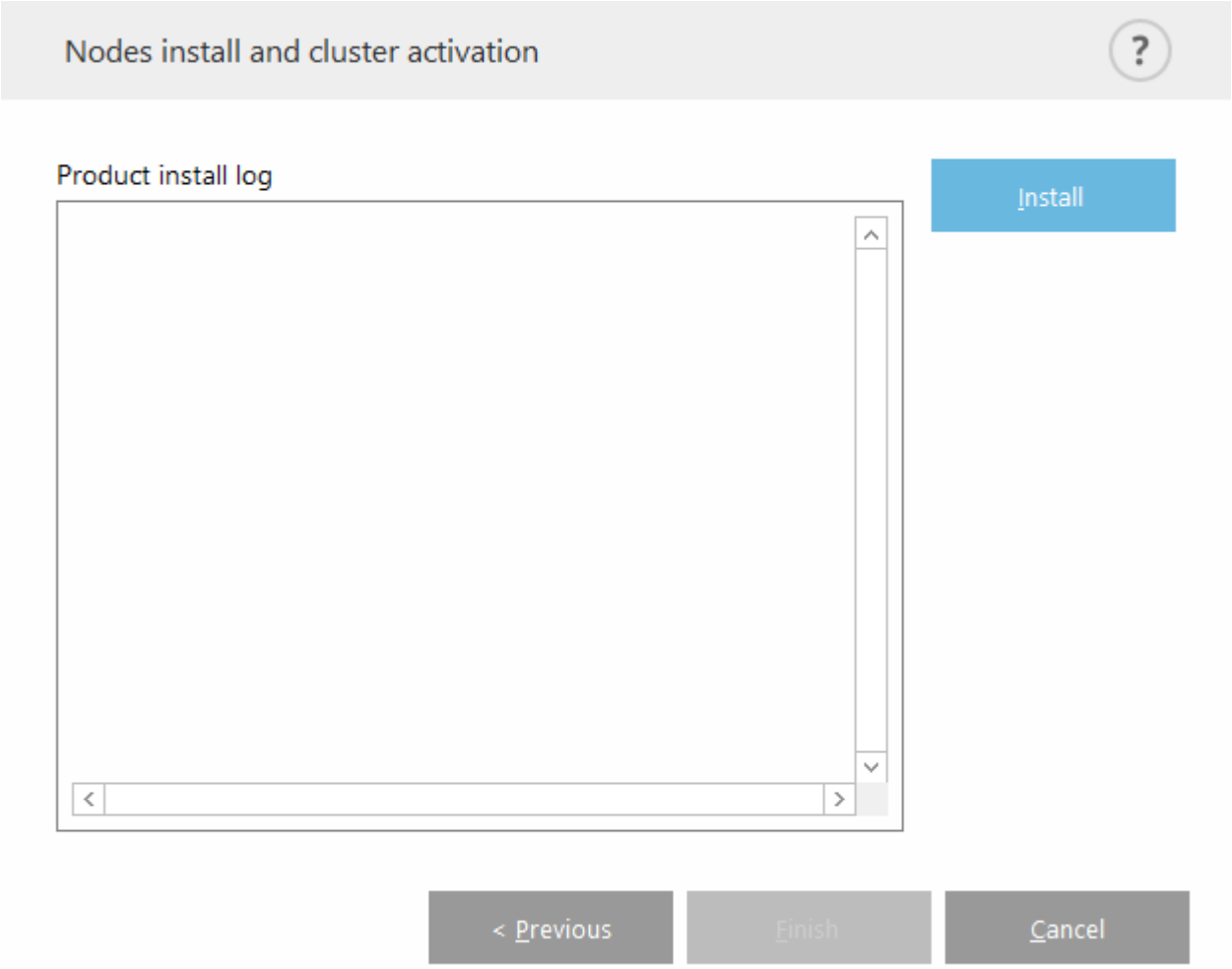


노드 확인이 완료되면 보고서를 확인할 수 있습니다.

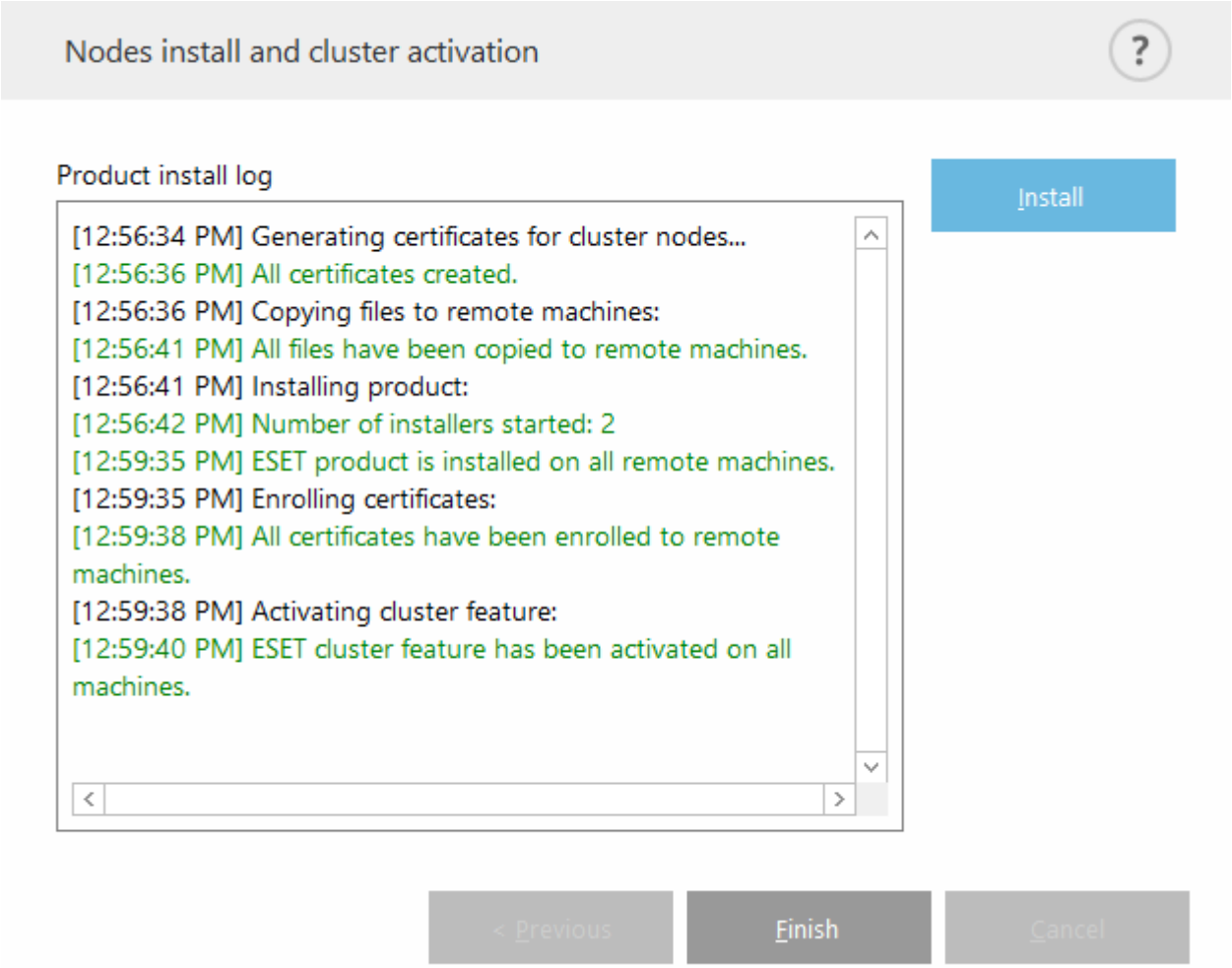


클러스터 마법사 - 노드 설치

ESET 클러스터를 초기화하는 중에 원격 컴퓨터에 설치하는 경우 마법사가 *%ProgramData%\ESET\ESET Security\Installer* 디렉터리에서 설치 프로그램을 검색합니다. 설치 프로그램 패키지를 이 디렉터리에 없는 경우 설치 프로그램 파일을 찾으라는 메시지가 표시됩니다.

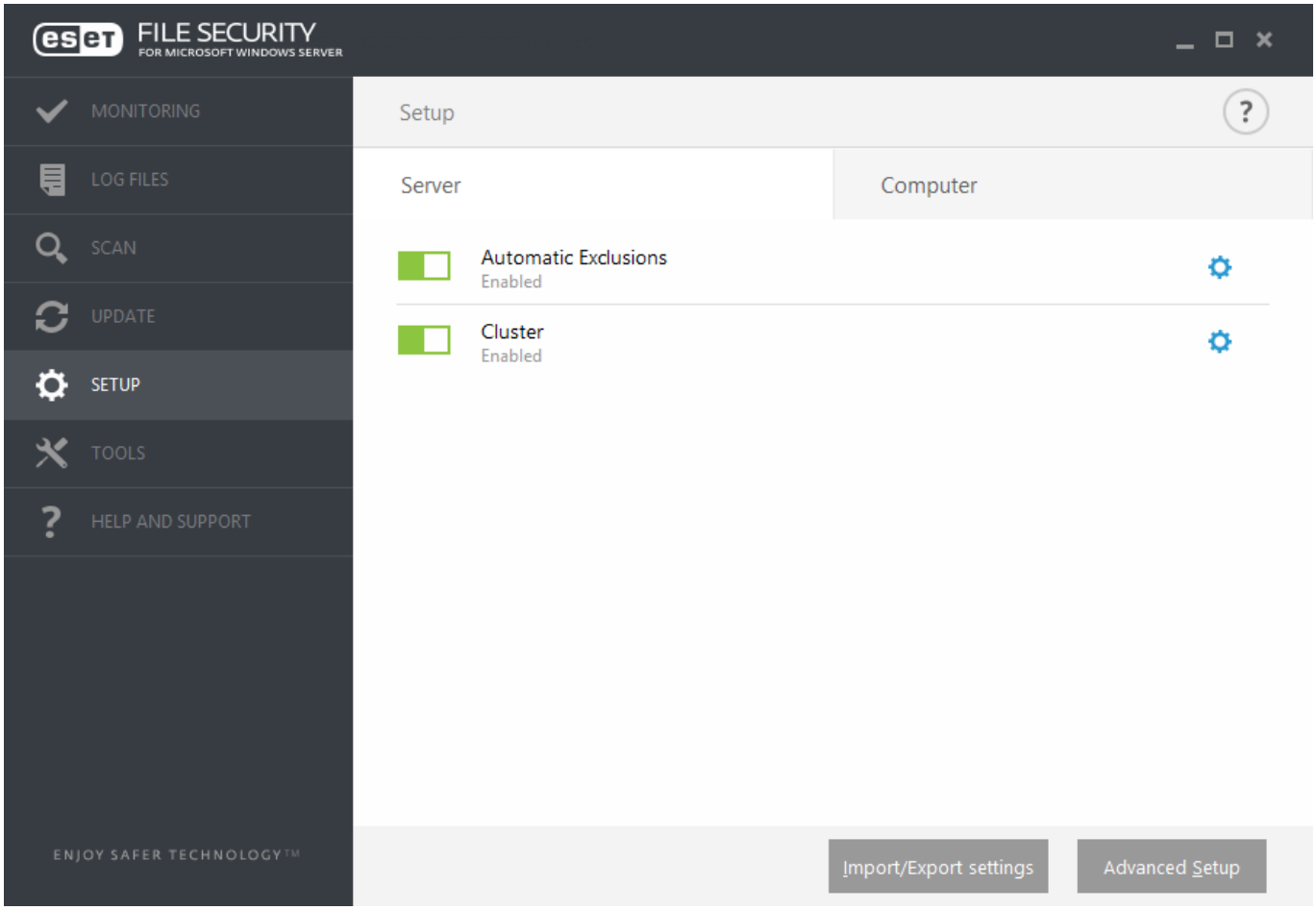


참고
아키텍처가 다른(32비트 및 64비트) 노드에 대해 자동 원격 설치를 사용하려는 경우, 아키텍처가 다른 노드가 검출되어 수동 설치를 권장하는 메시지가 표시됩니다.



ESET 클러스터를 올바르게 구성하고 나면 **설정** > **서버** 페이지에 활성화된 상태로 표시됩니다.

> 참고
> 일부 노드에 이전 버전의 ESET File Security가 이미 설치된 경우 이 컴퓨터에 최신 버전이 필요하다는 알림이 수신됩니다. ESET File Security를 업데이트하면 해당 컴퓨터가 자동으로 다시 시작될 수 있습니다.



또한 클러스터 상태 페이지(**도구 > 클러스터**)에서 현재 상태를 확인할 수 있습니다.

ESET Shell

eShell(ESET Shell의 약어)은 ESET File Security용 명령줄 인터페이스로, GUI(그래픽 사용자 인터페이스)의 대체 인터페이스입니다. eShell에는 일반적으로 GUI가 제공하는 모든 기능과 옵션이 포함됩니다. eShell을 통해 GUI를 사용하지 않고도 전체 프로그램을 구성하고 관리할 수 있습니다.

GUI에서 사용할 수 있는 모든 기능 외에도 eShell을 통해 스크립트를 실행하여 구성을 설정 또는 수정하거나 동작을 수행하는 작업을 자동화할 수도 있습니다. 또한 eShell은 GUI를 통해 명령줄을 사용하려는 사용자에게 유용할 수 있습니다.

> 참고
> 완전한 기능을 사용하려면 관리자 권한으로 실행을 사용하여 eShell을 여는 것이 좋습니다. 이는 Windows 명령 프롬프트(cmd)를 통해 단일 명령을 실행하는 경우에도 마찬가지입니다. 관리자 권한으로 실행을 사용하여 프롬프트를 여십시오. 관리자 권한으로 명령 프롬프트를 실행하지 못하면 권한 부족으로 인해 명령을 실행할 수 없게 됩니다.

eShell은 다음과 같은 두 가지 모드로 실행할 수 있습니다.

1. **대화 모드** - 구성 변경, 로그 보기 등과 같은 작업을 수행하기 위해 단일 명령을 실행할 때뿐만 아니라 eShell을 사용할 때 유용합니다. 일부 명령이 아직 익숙하지 않은 경우 대화 모드를 사용할 수 있습니다. 대화 모드를 사용하면 eShell을 보다 쉽게 탐색할 수 있으며, 이 모드에는 특정 컨텍스트에서 사용할 수 있는 명령도 표시됩니다.

2. **단일 명령/배치 모드 -** 대화 모드의 eShell로 전환하지 않고 명령만 실행해야 하는 경우 이 모드를 사용할 수 있습니다. 이 작업은 Windows 명령 프롬프트에 적합한 파라미터와 함께 eshell을 입력하여 수행할 수 있습니다.

예
`eshell get status` 또는 `eshell computer set real-time status disabled 1h`

배치/스크립트 모드에서 위의 두 번째 예와 같은 특정 명령을 실행하려면 먼저 몇 가지 설정을 구성해야 합니다. 그렇지 않으면 **접근이 거부됨** 메시지가 수신됩니다. 이는 보안상의 이유에 기인합니다.

참고
Windows 명령 프롬프트에서 eShell 명령을 사용하려면 설정을 변경해야 합니다. 배치 파일을 실행하는 방법에 대한 자세한 내용을 보려면 여기를 클릭하십시오.

eShell에서는 다음과 같은 두 가지 방법으로 대화 모드로 설정할 수 있습니다.

1. **Windows 시작 메뉴** 사용: 시작 > 모든 프로그램 > ESET > ESET File Security > ESET Shell

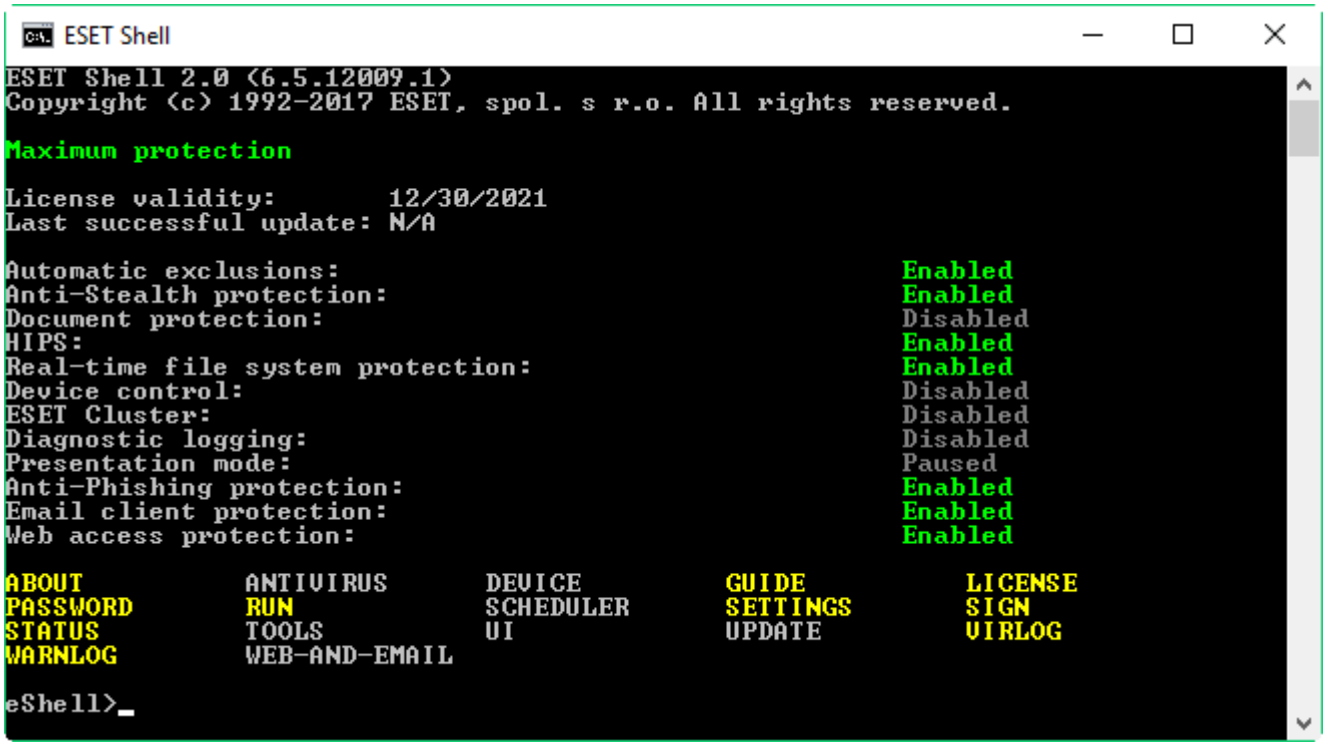
2. **Windows 명령 프롬프트**에서 `eshell`을 입력하고 Enter 키를 누릅니다.

중요
`'eshell' is not recognized as an internal or external command` 오류가 발생했다면 ESET File Security 설치 후 시스템에서 새로운 환경 변수를 로드하지 않았기 때문입니다. 새 명령 프롬프트를 열고 eShell을 다시 시작해 보십시오. 여전히 오류가 발생하거나 ESET File Security가 주요 설치되어 있는 경우 `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"` 등의 절대 경로를 사용하여 eShell을 시작하십시오(명령이 정상적으로 작동하려면 ""를 사용해야 함).

eShell을 대화 모드로 처음 실행하는 경우 첫 번째 실행(안내) 화면이 표시됩니다.

참고
앞으로 첫 번째 실행 화면을 표시하려면 `guide` 명령을 입력합니다. 이 화면에는 구문, 접두어, 명령 경로, 단축 형식, 별칭 등과 함께 eShell을 사용하는 방법에 대한 기본적인 몇 가지 예가 나와 있습니다.

다음번에 eShell을 실행하면 아래 화면이 표시됩니다.



> 참고
> 명령은 대소문자를 구분하지 않으므로 대문자나 소문자 모두 사용할 수 있으며, 대소문자에 상관없이 명령이 실행됩니다.

eShell 사용자 지정

`ui eshell` 컨텍스트에서 eShell을 사용자 지정할 수 있습니다. 스크립트에 대한 실행 정책, 언어, 색상 및 별칭과 숨겨진 명령에 대한 설정 등을 구성할 수 있습니다.

사용

구문

명령이 제대로 작동하려면 올바른 구문으로 작성되어야 하며, 명령은 접두어, 컨텍스트, 인수, 옵션 등으로 구성될 수 있습니다. 다음은 eShell 전체에서 사용되는 일반적인 구문입니다.

[<접두어>] [<명령 경로>] <명령> [<인수>]

예(이 예는 문서 보호를 활성화함):

`SET COMPUTER SCANS DOCUMENT REGISTER ENABLED`

- `SET` - 접두어
- `COMPUTER SCANS DOCUMENT` - 특정 명령, 이 명령이 속한 컨텍스트 경로
- `REGISTER` - 명령 자체
- `ENABLED` - 명령에 대한 인수

`?`를 명령 인수로 사용하면 해당 특정 명령에 대한 구문이 표시됩니다. 예를 들어 `STATUS ?` 는 `STATUS` 명령의 구문을 표시합니다.

구문:

```
[get] status
```

작업:

```
get - 모든 보호 모듈의 상태 표시
```

이 구문에서 대괄호로 묶인 [get]은 접두어 get이 status 명령의 기본값임을 나타냅니다. 즉, 접두어를 지정하지 않고 status를 실행하면 실제로 기본 접두어가 사용됨을 의미합니다(이 경우 get status). 접두어 없이 명령을 사용하면 입력 시간이 절약됩니다. 보통 get은 대부분의 명령에 대한 기본 접두어이지만 특정 명령에 대해 기본 접두어가 무엇인지 그리고 실행하려는 접두어가 맞는지 확인해야 합니다.

> 참고
> 명령은 대소문자를 구분하지 않으므로 대문자나 소문자 모두 사용할 수 있으며, 대소문자에 상관없이 명령이 실행됩니다.

접두어/작업

접두어는 작업 역할을 합니다. GET 접두어는 ESET File Security의 특정 기능을 구성하는 방식에 대한 정보를 제공하거나 상태를 보여줍니다(예: GET COMPUTER REAL-TIME STATUS는 실시간 모듈의 현재 보호 상태를 보여줌). SET 접두어는 기능을 구성하거나 해당 상태를 변경합니다(SET COMPUTER REAL-TIME STATUS ENABLED는 실시간 보호를 활성화함).

다음은 eShell을 통해 사용할 수 있는 접두어이며, 명령에서 이러한 접두어를 지원할 수도 있으며, 지원하지 않을 수도 있습니다.

GET	현재 설정/상태 반환
SET	값/상태 설정
SELECT	항목 선택
ADD	항목 추가
REMOVE	항목 제거
CLEAR	모든 항목/파일 제거
START	동작 시작
STOP	동작 중지
PAUSE	동작 일시 중지
RESUME	동작 다시 시작
RESTORE	기본 설정/개체/파일 복원
SEND	개체/파일 전송
IMPORT	파일에서 가져오기
EXPORT	파일로 내보내기

> 참고
> GET, SET 같은 접두어는 여러 명령에 사용되지만, 일부 명령(예: EXIT)에서는 접두어를 사용하지 않습니다.

명령 경로/컨텍스트

명령은 트리 구조를 형성하는 컨텍스트에 배치됩니다. 트리의 최상위 수준은 루트입니다. eShell을 실행하면 루트 수준에 설정됩니다.

eShell>

여기에서 명령을 실행하거나 컨텍스트 이름을 입력하여 트리 내에서 이동할 수 있습니다. 예를 들어, TOOLS 컨텍스트를 입력하면 여기에서 사용할 수 있는 모든 명령과 하위 컨텍스트가 표시됩니다.

노란색 항목은 실행할 수 있는 명령이며, 회색 항목은 입력할 수 있는 하위 컨텍스트입니다. 하위 컨텍스트에는 추가 명령이 포함됩니다.

상위 수준으로 다시 되돌아가야 하는 경우 ..(점 두 개)을 사용합니다.

> 예
> 예를 들어
> eShell computer real-time>
> ..를 입력하면 다음과 같이 한 수준 위로 이동됩니다.
> eShell computer>

만약 eShell computer real-time> (루트보다 두 수준 아래임)에서 다시 루트로 돌아오려면 .. ..(공백으로 구분된 두 개의 점 2개)을 입력하면 됩니다. 이렇게 하면 두 수준 위로 이동되며, 이 예의 경우 루트로 돌아오게 됩니다. 백슬래시 \를 사용하면 컨텍스트 내 위치에 상관없이 모든 수준에서 루트로 바로 돌아올 수 있습니다. 상위 수준의 특정 컨텍스트로 이동하려면 원하는 수준에 맞도록 해당 개수의 .. 명령을 사용하면 됩니다(구분 기호로 공백 사용). 예를 들어, 세 수준 위로 이동하려면 .. .. ..을 사용합니다.

경로는 현재 컨텍스트에 상대적입니다. 명령이 현재 컨텍스트에 포함된 경우 경로를 입력하지 마십시오. 예를 들어 GET COMPUTER REAL-TIME STATUS를 실행하려면 다음을 입력하십시오:

GET COMPUTER STATUS - 루트 컨텍스트에 있는 경우(명령줄에eShell>
GET STATUS - COMPUTER 컨텍스트에 있는 경우(명령줄에 eShell computer> 표시)
.. GET STATUS - COMPUTER REAL-TIME 컨텍스트에 있는 경우(명령줄에 eShell computer real-time> 표시)

단일 점은 두 개의 점의 약어이므로 두 개의 점 `..` 대신 단일 점 `.`을 사용할 수 있습니다.

```
예
. GET STATUS - COMPUTER REAL-TIME 컨텍스트에 있는 경우(명령줄에 eShell computer real-time> 표시)
```

인수

인수는 특정 명령에 대해 수행되는 동작입니다.`CLEAN-LEVEL` 예를 들어, `COMPUTER REAL-TIME ENGINE`에 있는 명령은 다음 인수와 함께 사용할 수 있습니다.

- `rigorous` - 항상 탐지 치료
- `safe` - 안전하면 탐지 치료, 그렇지 않으면 유지
- `normal` - 안전하면 탐지 치료, 그렇지 않으면 확인
- `none` - 최종 사용자에게 항상 확인

또 다른 인수의 예로는 `ENABLED`나 `DISABLED`가 있으며, 이러한 인수는 특정 기능을 활성화하거나 비활성화하는 데 사용됩니다.

단축 형식/축소된 명령

eShell을 통해 컨텍스트, 명령 및 인수(인수가 스위치나 대체 옵션인 경우)를 축소할 수 있습니다. 숫자, 이름 또는 경로 등과 같이 구체적인 값인 접두어나 인수는 축소할 수 없습니다. enabled 또는 disabled 인수 대신 숫자 `1`과 `0`을 사용할 수 있습니다.

```
예
computer set real-time status enabled    =>   com set real stat 1
computer set real-time status disabled    =>   com set real stat 0
```

단축 형식 예는 다음과 같습니다.

```
예
computer set real-time status enabled    =>   com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext    =>   com excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1    =>   com excl rem det 1
```

두 개의 명령이나 컨텍스트가 같은 문자로 시작하는 경우(예: `ADVANCED` 및 `AUTO-EXCLUSIONS`, 그리고 `A`를 축약 명령으로 입력) eShell은 두 개의 명령 중 사용자가 실행하려는 명령을 결정할 수 없습니다. 이 경우 오류 메시지가 표시되고 "A"로 시작하는 명령이 표시되어 실행할 명령을 선택할 수 있습니다.

```
eShell>a

The following command is not unique: a
```

`COMPUTER` 컨텍스트에서는 다음과 같은 하위 컨텍스트를 사용할 수 있습니다:

- `ADVANCED`
- `AUTO-EXCLUSIONS`

하나 이상의 문자(예: A 대신 AD)를 추가하면 eShell은 이제 고유하므로 ADVANCED 하위 컨텍스트를 입력합니다. 단축 명령에도 똑같이 적용됩니다.

> 참고
> 명령이 원하는 방식으로 정확하게 실행되도록 하려면 단축 명령, 인수 등을 사용하지 말고 전체 형식을 사용하는 것이 좋습니다. 그러면 eShell이 필요한 명령을 정확하게 실행하며, 원치 않는 실수도 방지할 수 있습니다. 배치 파일/스크립트의 경우 특히 전체 형식을 사용하는 것이 좋습니다.

자동 완성

이 새로운 기능은 eShell 2.0에 도입되었으며, Windows 명령 프롬프트의 자동 완성 기능과 매우 비슷합니다. Windows 명령 프롬프트는 파일 경로를 완성하는 한편, eShell은 명령, 컨텍스트 및 작업 이름을 완성합니다. 인수 완성은 지원되지 않습니다. 명령을 입력할 때 Tab 키를 누르면 사용 가능한 변수를 완성하거나 사용 가능한 변수를 돌아가면서 선택할 수 있습니다. Shift + Tab 키를 누르면 반대 방향으로 변수를 돌아가면서 선택할 수 있습니다. 약어와 자동 완성을 함께 사용할 수는 없습니다. 둘 중 하나만 사용하십시오. 예를 들어, computer real-time additional을 입력한 경우, Tab 키를 눌러도 아무 동작이 수행되지 않습니다. 대신 com을 입력한 다음 Tab 키를 눌러 computer를 완성한 후 real을 입력하고 Tab 키를 누르고 add를 입력하고 ab 키를 누른 후 Enter 키를 누릅니다. on을 입력하고 Tab 키를 계속해서 누르면 on-execute-ah, on-execute-ah-removable, on-write-ah, on-write-archive-default 등의 사용할 수 있는 모든 변수가 돌아가며 표시됩니다.

별칭

별칭은 명령을 실행하는 데 사용할 수 있는 대체 이름입니다(명령에 별칭이 지정된 경우). 다음은 몇 가지 기본 별칭입니다.

(global) close - 종료
(global) quit - 종료
(global) bye - 종료
warnlog - 도구 로그 이벤트
virlog - 도구 로그 검출

"(global)"은 현재 컨텍스트에 관계없이 어디에서나 사용할 수 있는 명령을 의미합니다. 하나의 명령에 여러 별칭이 할당될 수 있습니다. 예를 들어, EXIT의 별칭은 CLOSE, QUIT 및 BYE입니다. eShell을 종료하려면 EXIT 명령을 사용하거나 별칭 중 원하는 별칭을 사용하면 됩니다. 별칭 VIRLOG는 DETECTIONS 컨텍스트에 있는 TOOLS LOG 명령의 별칭입니다. 이 방법으로 ROOT 컨텍스트에서 탐지 명령을 사용할 수 있으며, 명령에 보다 쉽게 접근할 수 있습니다(TOOLS를 입력한 다음 LOG 컨텍스트를 입력하고 ROOT에서 직접 실행할 필요가 없음).

eShell을 통해 자신만의 별칭을 정의할 수 있습니다. ALIAS 명령은 UI ESHELL 컨텍스트에 있습니다.

비밀번호로 보호된 설정

ESET File Security 설정은 패스워드로 보호할 수 있습니다. GUI를 사용하여 패스워드를 설정하거나 set ui access lock-password 명령을 사용하여 eShell에서 패스워드를 설정할 수 있습니다. 특정 명령의 경우 이 패스워드를 대화형으로 입력해야 합니다(설정을 변경하거나 데이터를 수정하는 명령 등). eShell을 장기간 사용할 예정인데 쉘을 사용할 때마다 패스워드를 입력하는 것이 싫다면, set password(root에서 실행) 명령으로 eShell에서 패스워드를 기억하게 할 수 있습니다. 그러면 패스워드가 필요한 명령을 실행할 때마다 패스워드가 자동으로 입력됩니다. 이 설정은 eShell을 종료할 때까지 유지됩니다. 즉, 새 세션을 시작하고 eShell에서 패스워드를 기억하게 하고 싶다면, set password 명령을 다시 사용해야 한다는 뜻입니다.

Guide/Help

GUIDE 또는 HELP 명령을 실행하면, eShell 사용 방법을 설명하는 "첫 번째 실행" 화면이 표시됩니다. 이 명령은 ROOT 컨텍스트(eShell>)에서만 사용할 수 있습니다.

명령 기록

eShell은 이전에 실행된 명령의 기록을 보관합니다. 단, 현재 eShell 대화형 세션에만 해당됩니다. eShell을 종료하면 명령 기록이 삭제됩니다. 키보드의 위쪽 및 아래쪽 화살표 키를 사용하여 기록 사이를 이동할 수 있습니다. 원하는 명령을 찾았으면 처음부터 전체 명령을 다시 입력할 필요 없이 해당 명령을 다시 실행하거나 수정할 수 있습니다.

CLS/화면 지우기

CLS 명령은 화면을 지우는 데 사용할 수 있으며, Windows 명령 프롬프트나 유사한 명령줄 인터페이스와 같은 방식으로 작동됩니다.

EXIT/CLOSE/QUIT/BYE

eShell을 닫거나 종료하려면, EXITCLOSE, QUIT 또는BYE 명령 중 하나를 사용하면 됩니다.

명령

이 섹션에는 기본적인 몇몇 eShell 명령과 해당 설명이 나와 있습니다.

> 참고
> 명령은 대소문자를 구분하지 않으므로 대문자나 소문자 모두 사용할 수 있으며, 대소문자에 상관없이 명령이 실행됩니다.

예 명령(ROOT 컨텍스트에 포함됨):

ABOUT

프로그램에 대한 정보가 나열되며, 다음과 같은 정보를 표시합니다.

- 설치된 ESET 보안 제품 이름과 해당 버전 번호.
- 운영 체제 및 기본 하드웨어 상세 정보.
- 사용자 이름(도메인 포함), 전체 컴퓨터 이름(FQDN, 서버가 도메인의 구성원인 경우) 및 시트 이름.
- 각 구성 요소의 버전 번호를 포함하여 설치된 ESET 보안 제품의 구성 요소.

컨텍스트 경로:

```
root
```

PASSWORD

일반적으로 비밀번호로 보호된 명령을 실행하려면 보안상의 이유로 패스워드를 입력하라는 메시지가 표시되며, 이러한 명령으로는 보호를 비활성화하는 명령 및 ESET File Security 구성에 영향을 줄 수 있는 명령 등이 포함됩니다. 이러한 명령은 실행할 때마다 패스워드를 입력하라는 메시지가 표시됩니다. 매번 비밀번호

를 입력하지 않도록 하려면 이 비밀번호를 정의하면 됩니다. 그러면 eShell에서 비밀번호를 저장하여 비밀번호로 보호된 명령을 실행할 때 자동으로 이 비밀번호가 입력됩니다.

> 참고
> 비밀번호는 현재 eShell 대화 세션에 한해서만 작동됩니다. eShell을 종료하면 정의된 이 비밀번호가 삭제되며, eShell을 다시 시작할 때 비밀번호를 다시 정의해야 합니다.

정의된 비밀번호는 지문이 생성되지 않은 배치 파일이나 스크립트를 실행할 때 사용할 수도 있습니다. 서명되지 않은 배치 파일을 실행할 때는 ESET Shell 실행 정책을 전체 권한으로 설정해야 합니다. 다음은 이러한 배치 파일의 예입니다.

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

위의 연결된 이 명령은 비밀번호를 정의하고 보호를 비활성화합니다.

> 중요
> 가능한 경우 언제나 서명한 배치 파일을 사용하는 것이 좋습니다. 이렇게 하면 배치 파일에 일반 텍스트 비밀번호를 포함하지 않게 됩니다(위에 설명된 방법을 사용하는 경우). 자세한 내용은 배치 파일/스크립팅(서명한 배치 파일 섹션)을 참조하십시오.

컨텍스트 경로:

`root`

구문:

`[get] | restore password`

`set password [plain <password>]`

작업:

- `get` - 비밀번호 표시
- `set` - 패스워드- 비밀번호 설정 또는 지우기
- `restore` - 비밀번호 지우기

인수:

- `plain` - 비밀번호를 파라미터로 입력하도록 전환
- `password` - 비밀번호

예:

- `set password plain <yourpassword>` - 비밀번호로 보호된 명령에 사용되는 비밀번호 설정
- `restore password` - 비밀번호 지우기

예:

- `get password` - 비밀번호가 구성되었는지 여부를 확인하려면 이 명령을 사용합니다(이 명령은 비밀번호 자체가 아닌 "*"만 표시함). "*"가 표시되지 않으면 비밀번호가 설정되지 않은 것입니다.

`set password plain <yourpassword>` - 정의된 패스워드를 설정하려면 이 명령을 사용합니다.

`restore password` - 이 명령은 정의된 비밀번호를 지웁니다.

STATUS

ESET File Security의 현재 실시간 보호 상태에 대한 정보를 표시하며, 보호를 일시 중지/다시 시작할 수 있습니다(GUI와 비슷함).

컨텍스트 경로:

```
computer real-time
```

구문:

```
[get] status
set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]
restore status
```

작업:

`get` - 현재 설정/상태 반환

`set` - 값/상태 설정

`restore` - 기본 설정/개체/파일 복원

인수:

`enabled` - 보호/기능 활성화

`disabled` - 보호/기능 비활성화

`10m` - 10분 동안 비활성화

`30m` - 30분 동안 비활성화

`1h` - 1시간 동안 비활성화

`4h` - 4시간 동안 비활성화

`temporary` - 다시 부팅할 때까지 비활성화

> 참고
> 단일 명령으로 모든 보호 기능을 비활성화할 수 없습니다. `status` 명령을 사용하여 보호 기능 및 모듈을 하나씩 관리할 수 있습니다. 각 보호 기능 또는 모듈에는 자체적인 `status` 명령이 있습니다.

`status` 명령이 있는 기능 목록은 다음과 같습니다.

기능	컨텍스트 및 명령
자동 제외 항목	`COMPUTER AUTO-EXCLUSIONS STATUS`

기능	컨텍스트 및 명령
HIPS(호스트 침입 방지 시스템)	COMPUTER HIPS STATUS
실시간 파일 시스템 보호	COMPUTER REAL-TIME STATUS
장치 제어	DEVICE STATUS
봇네트 보호	NETWORK ADVANCED STATUS-BOTNET
네트워크 공격 보호(IDS)	NETWORK ADVANCED STATUS-IDS
네트워크 격리	NETWORK ADVANCED STATUS-ISOLATION
ESET 클러스터	TOOLS CLUSTER STATUS
진단 로깅	TOOLS DIAGNOSTICS STATUS
프레젠테이션 모드	TOOLS PRESENTATION STATUS
안티피싱 보호	WEB-AND-EMAIL ANTIPHISHING STATUS
이메일 클라이언트 보호	WEB-AND-EMAIL MAIL-CLIENT STATUS
웹 브라우저 보호	WEB-AND-EMAIL WEB-ACCESS STATUS

VIRLOG

DETECTIONS 명령의 별칭입니다. 탐지된 침입 항목에 대한 정보를 확인해야 할 때 유용합니다.

WARNLOG

EVENTS 명령의 별칭입니다. 다양한 이벤트에 대한 정보를 확인해야 할 때 유용합니다.

배치 파일/스크립팅

강력한 자동화 스크립팅 도구로 eShell을 사용할 수 있습니다. eShell과 함께 배치 파일을 사용하려면 eShell 및 이 쉘에 포함된 명령을 사용하여 배치 파일을 생성합니다.

```
예
eshell get computer real-time status
```

가끔 필요한 명령을 묶을 수도 있습니다. 예를 들어 예약된 특정 작업의 유형을 가져오려면 다음을 입력합니다.

```
eshell select scheduler task 4 "&" get scheduler action
```

선택한 항목(이 경우 작업 번호 4)은 일반적으로 현재 실행 중인 eShell의 인스턴스에만 적용됩니다. 이러한 두 개의 명령을 교대로 실행할 경우 두 번째 명령이 실패하게 되며 "작업을 선택하지 않았거나 선택한 작업이 더 이상 존재하지 않습니다." 오류가 표시됩니다.

보안상의 이유로 실행 정책은 기본적으로 **제한된 스크립팅**으로 설정됩니다. 이 설정에서는 eShell을 모니터링 도구로 사용할 수 있지만 스크립트를 실행하여 ESET File Security의 구성을 변경할 수는 없습니다. 보호 기능을 비활성화하는 등 보안에 영향을 줄 수 있는 명령을 사용하여 스크립트를 실행하려고 하면 **접근이 거부됨** 메시지가 수신됩니다. 구성을 변경하는 명령을 실행하려면 지문이 생성된 배치 파일을 사용하는 것이 좋습니다.

Windows 명령 프롬프트에 직접 단일 명령을 입력하여 구성을 변경하려면 eShell에 전체 권한을 부여해야 합니다(권장되지 않음). eShell 자체의 대화 모드에서 ui eshell shell-execution-policy를 사용하거나, **고급 설정**(**F5** 키) > **사용자 인터페이스** > ESET Shell의 GUI를 통해 전체 권한을 부여할 수 있습니다.

지문이 생성된 배치 파일

eShell을 통해 시그니처가 있는 일반 배치 파일(*.bat)을 보호할 수 있습니다. 스크립트의 지문은 설정 보호에 사용된 패스워드와 같은 패스워드를 통해 생성됩니다. 스크립트의 지문을 생성하려면 먼저 설정 보호를 활성화해야 합니다. 이 작업은 GUI를 통해 수행하거나 eShell에서 `set ui access lock-password` 명령으로 수행할 수 있습니다. 설정 보호 패스워드가 설정되면 배치 파일에 대해 지문을 생성하는 작업을 시작할 수 있습니다.

> 참고
> 설정 보호 비밀번호를 변경할 경우 모든 스크립트에 대해 지문을 다시 생성해야 합니다. 그렇지 않으면 보호 비밀번호를 변경한 시점부터 스크립트를 실행하지 못하게 됩니다. 스크립트 지문 생성 시 입력한 비밀번호가 대상 시스템의 설정 보호 비밀번호와 일치해야 합니다.

배치 파일에 대해 지문을 생성하려면 `sign <script.bat>`를 eShell의 루트 컨텍스트에서 실행합니다. 여기서 *script.bat*는 지문을 생성할 스크립트의 경로입니다. 지문 생성 시 사용할 패스워드를 입력하고 확인합니다. 이 패스워드는 설정 보호 패스워드와 일치해야 합니다. 시그니처는 설명 형식으로 배치 파일 끝부분에 배치됩니다. 이 스크립트의 지문이 이미 생성된 경우 이 시그니처는 새로운 시그니처로 대체됩니다.

> 참고
> 이전에 지문이 생성된 배치 파일을 수정하려면 지문을 다시 생성해야 합니다.

Windows 명령 프롬프트에서 또는 예약된 작업으로 지문이 생성된 배치 파일을 실행하려면 다음 명령을 사용합니다.

```
eshell run <script.bat>
```

여기서 script.bat은 배치 파일의 경로입니다.

> 예
> `eshell run d:\myeshellscript.bat`

ESET SysInspector

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

생성을 클릭하고 생성할 로그를 설명하는 간단한 **설명**을 입력합니다. ESET SysInspector 로그가 생성될 때까지 (상태가 생성됨으로 표시됨) 기다려 주십시오. 하드웨어 구성 및 시스템 데이터에 따라 로그를 생성하는 데 약간의 시간이 걸릴 수 있습니다.

ESET 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:

- **열기** - 생성된 로그를 엽니다. 로그를 오른쪽 마우스 버튼으로 클릭한 후 오른쪽 마우스 버튼 메뉴에서 표시를 선택할 수도 있습니다.
- **비교** - 기존의 두 로그를 비교합니다.
- **생성** - 새 로그를 생성합니다. 생성할 로그에 대한 간단한 설명을 입력하고 생성을 클릭합니다. ESET SysInspector 로그가 완성될 때까지 기다려 주십시오(상태가 생성됨으로 표시됨).
- **삭제** - 선택한 로그를 목록에서 제거합니다.

선택한 하나 이상의 로그를 오른쪽 마우스 버튼으로 클릭한 후 오른쪽 마우스 버튼 메뉴에서 다음과 같은 옵션을 사용할 수 있습니다:

- **표시** - 선택한 로그를 ESET SysInspector에서 엽니다(로그를 두 번 클릭하는 것과 같은 기능).
- **비교** - 기존의 두 로그를 비교합니다.
- **생성 -** 새 로그를 생성합니다. 생성할 로그에 대한 간단한 설명을 입력하고 **생성**을 클릭합니다. ESET SysInspector 로그가 완성될 때까지 기다려 주십시오(**상태**가 생성됨으로 표시됨).
- **삭제** - 선택한 로그를 목록에서 제거합니다.
- **모두 삭제** - 모든 로그를 삭제합니다.
- **내보내기** - 로그를 .xml 파일 또는 압축된 .xml로 내보냅니다.

ESET SysRescue Live

ESET SysRescue Live은 부팅 가능한 복구 CD/DVD나 USB 드라이브를 만들 수 있는 무료 유틸리티입니다. 복구 미디어로 감염된 컴퓨터를 부팅한 다음 악성코드를 검사하고 감염된 파일을 치료할 수 있습니다.

ESET SysRescue Live의 가장 큰 장점은 ESET Security 솔루션이 호스트 운영 체제와 독립적으로 실행되면서도 디스크 및 파일 시스템에 직접 접근할 수 있다는 점입니다. 따라서 운영 체제가 실행 중일 때 등에 일반적으로 제거할 수 없는 위협을 제거할 수 있습니다.

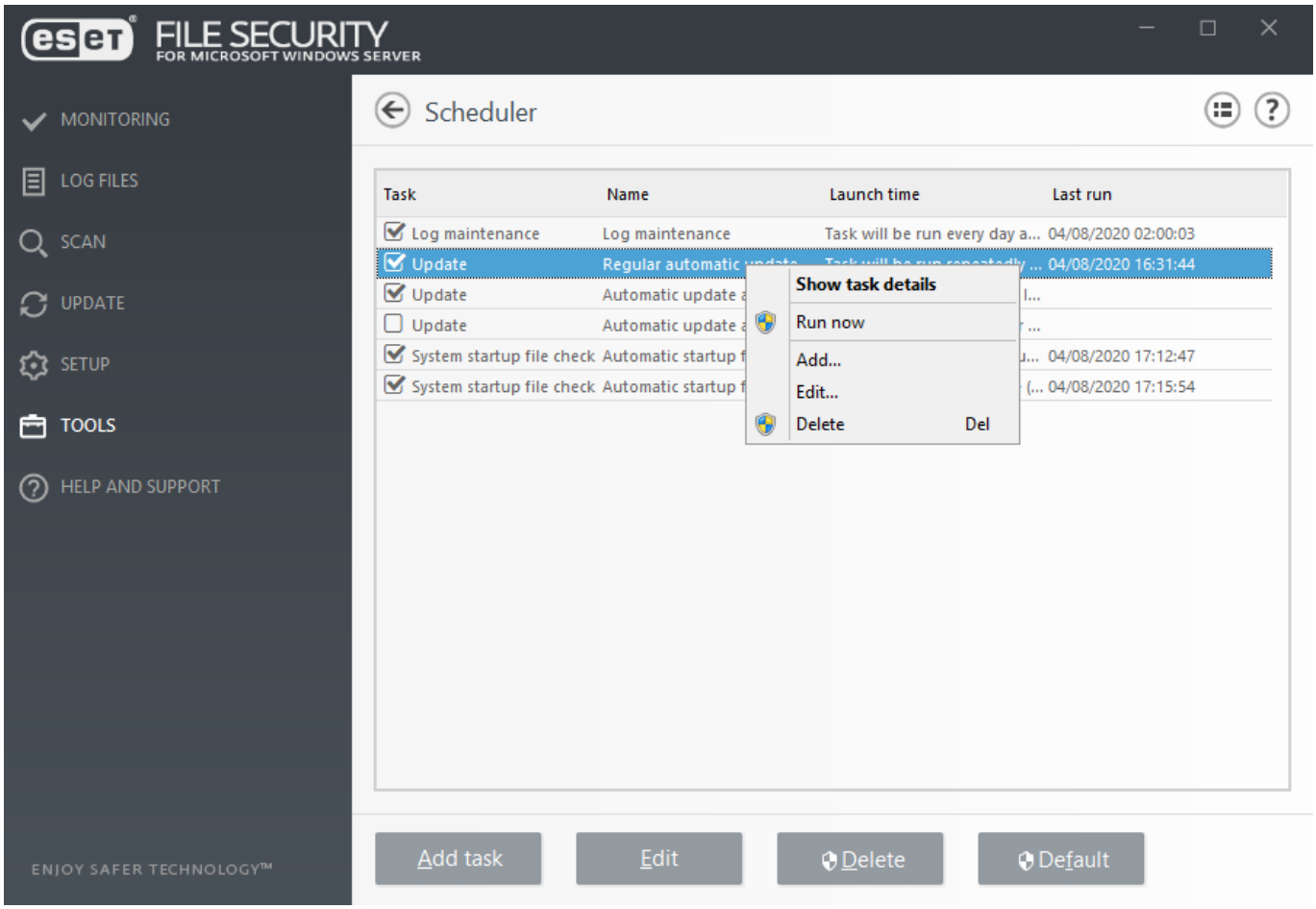
스케줄러

스케쥴러는 정의된 파라미터에 따라 예약된 작업을 관리하고 시작합니다. 작업 유형과 이름, 시작 시간과 수행된 마지막 실행 등 각각의 파라미터를 보여주는 표 형식으로 예약된 모든 작업의 목록을 볼 수 있습니다. 작업 추가를 클릭하여 새로 예약된 작업을 생성할 수도 있습니다. 예약된 기존 작업의 구성을 편집하려면 **편집** 버튼을 클릭합니다. 예약된 작업 목록을 기본 설정으로 되돌리고 **기본값**을 클릭한 후 수행된 모든 변경 사항을 **기본값으로 되돌리기**를 클릭하면 실행 취소할 수 없습니다.

미리 정의된 기본 작업 집합은 다음과 같습니다.

- 로그 유지 관리
- 정기적 자동 업데이트(이 작업을 업데이트 빈도에 사용)
- 전화 접속 연결 후 자동 업데이트
- 사용자 로그온 후 자동 업데이트
- 자동 시작 파일 검사(사용자 로그인 후)
- 자동 시작 파일 검사(모듈 업데이트 후)

참고
작업을 활성화 또는 비활성화하려면 해당하는 확인란을 선택합니다.



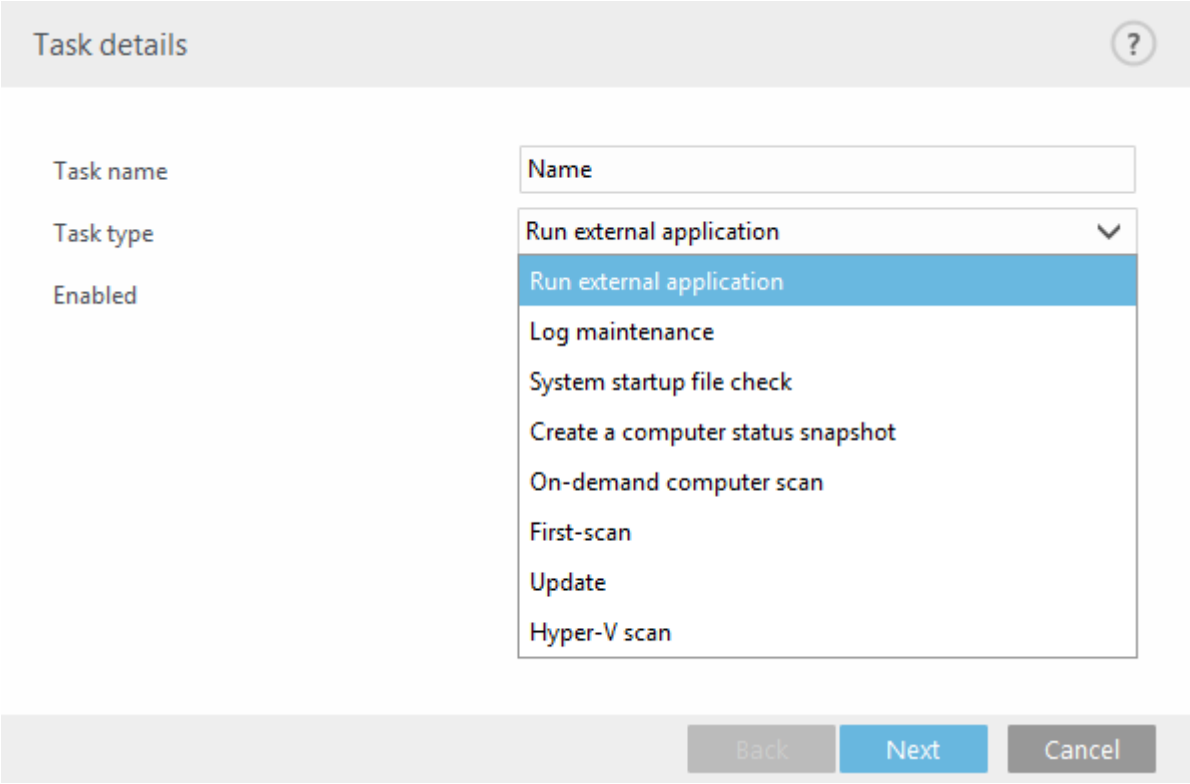
다음 동작을 수행하려면 작업을 오른쪽 마우스 버튼으로 클릭합니다.

작업 상세 정보 표시	예약된 작업을 두 번 클릭하거나 오른쪽 마우스 버튼으로 클릭하면 예약된 작업에 대한 상세 정보가 표시됩니다.
지금 실행	선택한 스케쥴러 작업을 실행하고 작업을 즉시 수행합니다.
추가...	새 스케쥴러 작업을 생성할 수 있는 마법사를 시작합니다.
편집...	예약된 기존 작업의 구성을 편집합니다(기본 작업과 사용자 정의 작업 모두).
삭제	기존 작업을 제거합니다.

스케줄러 - 작업 추가

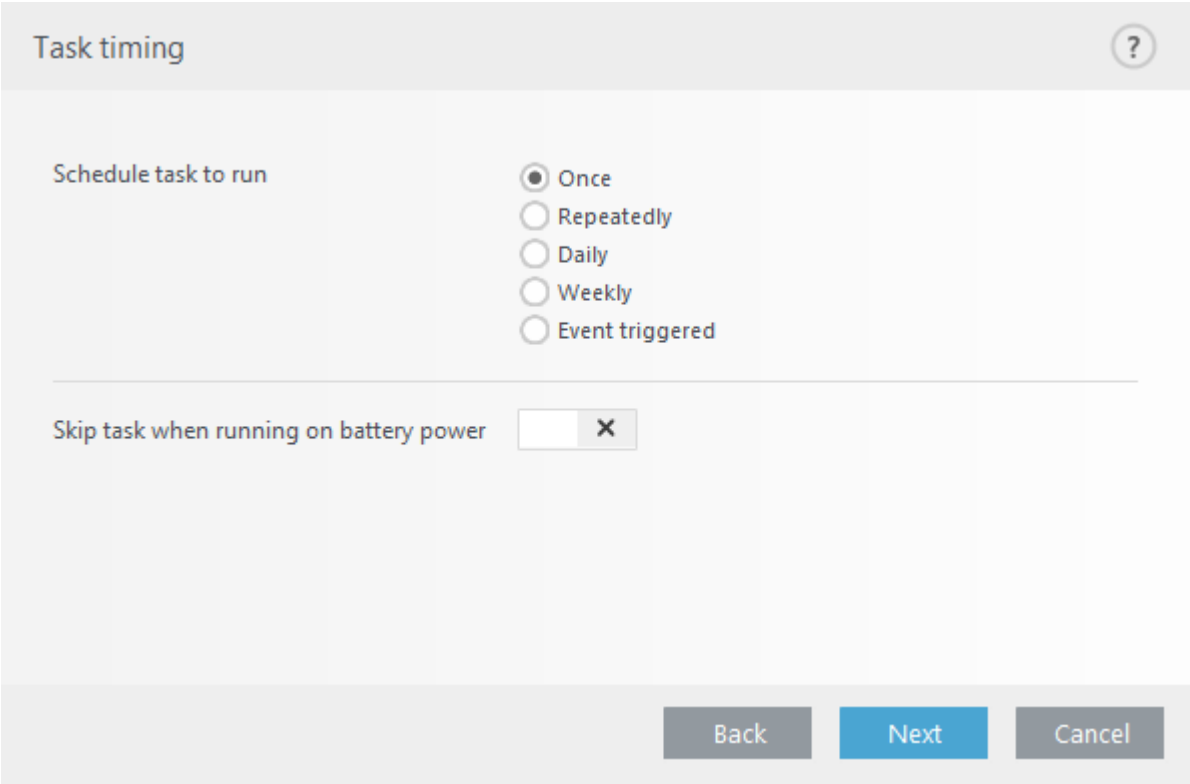
예약된 새 작업을 생성하려면:

1. **작업 추가**를 클릭합니다.
2. **작업 이름**을 입력하고 사용자 지정 예약 작업을 구성합니다.
3. 작업 유형 - 드롭다운 메뉴에서 해당하는 **작업 유형**을 선택합니다.

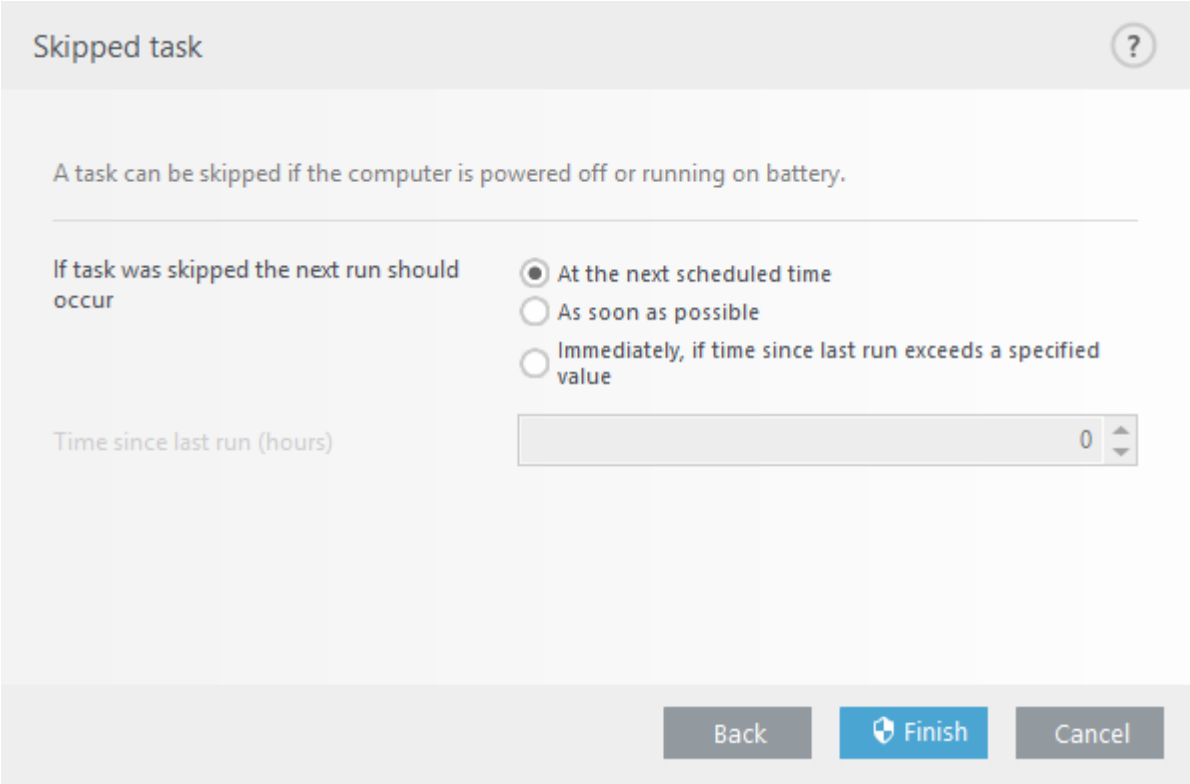


참고
작업을 비활성화하려면 **활성화됨** 옆에 있는 슬라이드 바를 클릭합니다. 나중에 작업을 활성화하려면 스케쥴러 보기에 있는 확인란을 클릭합니다.

4. 작업 타이밍 - 작업을 실행하려는 때 정의할 옵션 중 하나를 선택합니다. 선택에 따라 특정 시간, 날짜, 간격 또는 이벤트를 선택하라는 메시지가 표시됩니다.



5. 건너뛴 작업 - 미리 정의된 시간에 작업을 실행할 수 없는 경우 해당 작업이 수행될 시점을 지정할 수 있습니다.



6. 애플리케이션 실행 - 작업이 외부 애플리케이션을 실행하도록 예약된 경우 디렉터리 트리에서 실행 파일을 선택합니다.

7.내용을 변경해야 하는 경우 **뒤로**를 클릭하여 이전 단계로 돌아가 파라미터를 수정할 수 있습니다.

8.작업을 생성하거나 변경 내용을 적용하려면 **마침**을 클릭합니다.

예약된 새 작업이 스케쥴러 보기에 표시됩니다.

작업 유형

예약된 작업의 작업 유형별로 구성 마법사가 다릅니다. **작업 이름**을 입력하고 드롭다운 메뉴에서 원하는 **작업 유형**을 선택합니다.

- **외부 애플리케이션 실행** - 외부 애플리케이션 실행을 예약합니다.
- **로그 유지 관리 -** 로그 파일에는 삭제된 레코드의 잔여 레코드도 포함됩니다. 이 작업에서는 효과적으로 작업하기 위해 정기적으로 로그 파일의 레코드를 최적화합니다.
- **시스템 시작 파일 검사 -** 시스템 시작 또는 로그온 시 실행할 수 있는 파일을 검사합니다.
- **컴퓨터 상태 스냅숏 생성 -** ESET SysInspector 컴퓨터 스냅숏을 생성합니다. 시스템 구성 요소(예: 드라이버, 애플리케이션)에 대한 자세한 정보를 수집하고 각 구성 요소의 위험 수준을 평가합니다.
- **수동 컴퓨터 검사 -** 컴퓨터의 파일 및 폴더에 대한 검사를 수행합니다.
- **업데이트 -** 진단 엔진 및 프로그램 모듈을 업데이트하도록 업데이트 작업을 예약합니다.
- **Hyper-V 검사** - Hyper-V에서 가상 디스크 검사를 예약합니다.
- **OneDrive 검사** - OneDrive에 저장된 파일 검사를 예약합니다.

작업이 생성된 후에 비활성화하려면 **활성화됨** 옆에 있는 스위치를 클릭합니다. 나중에 작업을 활성화하려면 스케쥴러 보기에 있는 확인란을 클릭합니다. 다음 단계를 계속 진행하려면 **다음**을 클릭합니다.

작업 타이밍

다음의 타이밍 옵션 중 하나를 선택합니다.

- **한 번 -** 작업이 지정한 날짜와 시간에 한 번만 수행됩니다. 지정된 시간에 한 번만 작업을 실행할 수 있습니다. **작업 실행**에서 작업 한 번의 시작 날짜와 시간을 지정합니다.
- **반복적으로 -** 작업이 지정한 시간 간격(분)으로 수행됩니다. **작업 실행**에서 작업이 매일 실행되는 시간을 지정합니다.
- **매일** - 작업이 지정한 시간에 매일 반복적으로 실행됩니다.
- **매주 -** 작업이 선택한 날짜와 시간에 매주 한 번 이상 실행됩니다. 특정 요일에만 지정된 날짜와 시간에 시작되는 작업을 반복적으로 실행할 수 있습니다. 작업 실행 시간에서 시작 시간을 지정합니다. 작업이 실행되어야 하는 요일을 선택합니다.
- 이벤트가 트리거됨 - 지정된 이벤트가 발생한 후에 작업이 수행됩니다.

배터리 전원으로 실행되는 작업 건너뛰기를 활성화하면 작업이 시작될 때 시스템이 배터리로 실행 중인 경우 작업이 시작되지 않습니다. 예로 UPS에서 실행되는 컴퓨터를 들 수 있습니다.

이벤트가 트리거됨

이벤트에 의해 트리거된 작업을 예약하면 두 작업 완료 시간 사이의 최소 간격을 지정할 수 있습니다.

작업은 다음과 같은 이벤트에 의해 트리거될 수 있습니다.

- **컴퓨터를 시작할 때마다**
- **매일 컴퓨터를 처음 시작할 때**
- **인터넷/VPN에 전화 접속 연결**
- **모듈 업데이트 완료 시**
- **제품 업데이트 완료 시**
- **사용자 로그인** - 사용자가 시스템에 로그온하면 작업이 배포됩니다. 하루에 여러 번 컴퓨터에 로그온하는 경우 하루 중 처음으로 로그온할 때에만 작업을 수행하고 다음 날에도 동일한 패턴으로 작업을 수행하려면 24시간을 선택합니다.
- **위협 검출**

애플리케이션 실행

이 작업은 외부 애플리케이션 실행을 예약합니다.

- **실행 파일** - 디렉터리 트리에서 실행 파일을 선택하고 **찾아보기(...)**를 클릭하거나 수동으로 경로를 입력합니다.
- **작업 폴더** - 외부 애플리케이션의 작업 디렉터리를 정의합니다. 선택한 **실행 파일**의 모든 임시 파일이 이 디렉터리 내에 생성됩니다.
- **파라미터** - 애플리케이션의 명령줄 파라미터입니다(옵션).

건너뛴 작업

미리 정의된 시간에 작업을 실행할 수 없는 경우 해당 작업이 수행될 시점을 지정할 수 있습니다.

- **다음 예약 시간에** - 작업이 지정된 시간(예: 24시간 후)에 실행됩니다.
- **최대한 빨리** - 작업이 실행되지 않도록 하는 동작이 더 이상 유효하지 않을 때 작업이 최대한 빨리 실행됩니다.
- **마지막 실행 이후 시간이 지정된 값을 초과하는 경우 즉시 - 마지막 실행 후 시간(시)** - 이 옵션을 선택하면 지정된 시간(시)이 지난 후 작업이 항상 반복됩니다.

예약된 작업 개요

스케줄러 보기에서 작업을 두 번 클릭하거나 예약된 작업을 마우스 오른쪽 버튼으로 클릭하고 **작업 상세 정보 표시**를 선택하면 이 대화 상자 창에는 예약된 작업에 대한 자세한 정보가 표시됩니다.

분석용 샘플 전송

샘플 전송 대화 상자는 파일 또는 사이트를 ESET으로 보내 분석하도록 할 수 있습니다. 컴퓨터에서 동작이 의심스러운 파일을 찾았거나 인터넷에서 감염이 의심되는 사이트를 찾은 경우, 이를 ESET 바이러스 연구소로 보내 분석할 수 있습니다. 파일이 악성 애플리케이션이나 웹 사이트로 확인되면 향후 업데이트에 해당 파일 검출 기능이 추가됩니다.

파일을 이메일로 전송하려면 WinRAR 또는 WinZip과 같은 프로그램을 사용해 파일을 압축하고, *infected*라는 패스워드로 압축파일을 보호하여 samples@eset.com으로 전송합니다. 설명이 포함된 제목을 사용하고, 파일에 대한 정보(예: 파일을 다운로드한 웹 사이트)를 최대한 많이 포함해 주십시오.

샘플을 ESET으로 전송하기 전에 다음 조건 중 한두 가지를 충족하는지 확인하십시오.

- 파일 또는 웹 사이트가 전혀 검출되지 않는 경우
- 파일 또는 웹 사이트가 위협으로 잘못 검출되는 경우

위의 요구 사항 중 한 가지 이상을 충족하지 않을 경우 추가 정보를 제공할 때까지 응답이 전송되지 않습니다.

샘플 전송 사유 드롭다운 메뉴에서 메시지에 가장 적합한 설명을 선택합니다.

- 감염 의심 파일
- 감염 의심 사이트(맬웨어에 감염된 웹 사이트)

- 가양성 파일(감염된 것으로 검출되었지만 실제로는 감염되지 않은 파일)
- 가양성 사이트
- 기타

파일/사이트

전송하려는 파일 또는 웹 사이트의 경로입니다.

담당자 이메일

이 담당자 이메일이 감염 의심 파일과 함께 ESET으로 전송되며, 분석 시 추가 정보가 필요한 경우 사용자에게 연락하는 데 사용될 수 있습니다. 담당자 이메일 입력 항목은 옵션입니다. 추가 정보가 필요한 경우 외에는 ESET에서 답장을 전송하지 않습니다. 당사 서버에서는 매일 수만 개의 파일을 수신하기 때문에 모든 전송에 회신할 수가 업습니다.

익명으로 전송

익명으로 전송 옆의 확인란을 사용하여 이메일 주소를 입력하지 않고도 감염 의심 파일 또는 웹 사이트를 전송할 수 있습니다.

감염 의심 파일

맬웨어 감염 증상 발견

컴퓨터에서 발견된 감염 의심 파일 동작에 대한 설명을 입력합니다.

원본 파일(URL 주소나 공급업체)

파일 원본(소스)과 이 파일을 발견한 방법을 입력합니다.

메모 및 추가 정보

여기에 감염 의심 파일 식별 프로세스에 도움이 될 추가 정보나 설명을 입력할 수 있습니다.

> 참고
> 첫 번째 파라미터인 **맬웨어 감염 증상 발견**은 필수 사항이며, 이 파라미터 외에도 추가 정보를 입력하면 샘플 식별 프로세스에 있어 ESET 연구소에 많은 도움이 됩니다.

감염 의심 사이트

사이트의 문제 드롭다운 메뉴에서 다음 중 하나를 선택합니다.

감염됨

다양한 방법으로 배포된 바이러스나 기타 악성코드가 포함되어 있는 웹 사이트입니다.

피싱

은행 계좌 번호, PIN 번호 등과 같은 중요한 데이터에 접근하는 데 자주 사용됩니다. 이러한 공격 유형에 대한 자세한 내용은 용어집을 참조하십시오.

사기

사기성 또는 사취성 웹 사이트입니다.

기타

위의 옵션 중 하나도 전송하려는 사이트에 적용되지 않는 경우 이 옵션을 사용합니다.

메모 및 추가 정보

감염 의심 웹 사이트를 분석하는 데 도움이 될 추가 정보나 설명을 입력할 수 있습니다.

가양성 파일

사용자는 감염된 것으로 검출되지만 실제로는 감염되지 않은 파일을 전송하여 탐지 엔진을 향상시키고 다른 사용자가 보호받을 수 있도록 해 주시기 바랍니다. 오탐지(FP)는 파일의 패턴이 진단 엔진에 포함된 동일한 패턴과 일치하는 경우 발생할 수 있습니다.

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

응용 프로그램 이름 및 버전

프로그램 제목과 해당 버전(예: 번호, 별칭 또는 코드 이름)입니다.

원본 파일(URL 주소나 공급업체)

파일 원본(소스)와 이 파일을 발견한 방법을 입력합니다.

애플리케이션 용도

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

메모 및 추가 정보

여기에 감염 의심 파일을 처리할 때 도움이 될 추가 정보나 설명을 입력할 수 있습니다.

가양성 사이트

감염, 사기 또는 피싱 사이트로 검출되었지만 실제로는 그렇지 않은 사이트를 전송해 주시기 바랍니다. 오탐지(FP)는 파일의 패턴이 진단 엔진에 포함된 동일한 패턴과 일치하는 경우 발생할 수 있습니다. 이 웹 사이트 정보를 제공하여 탐지 엔진을 향상시키고 다른 사용자가 보호받을 수 있도록 해주십시오.

메모 및 추가 정보

여기에 감염 의심 파일을 처리할 때 도움이 될 추가 정보나 설명을 입력할 수 있습니다.

기타

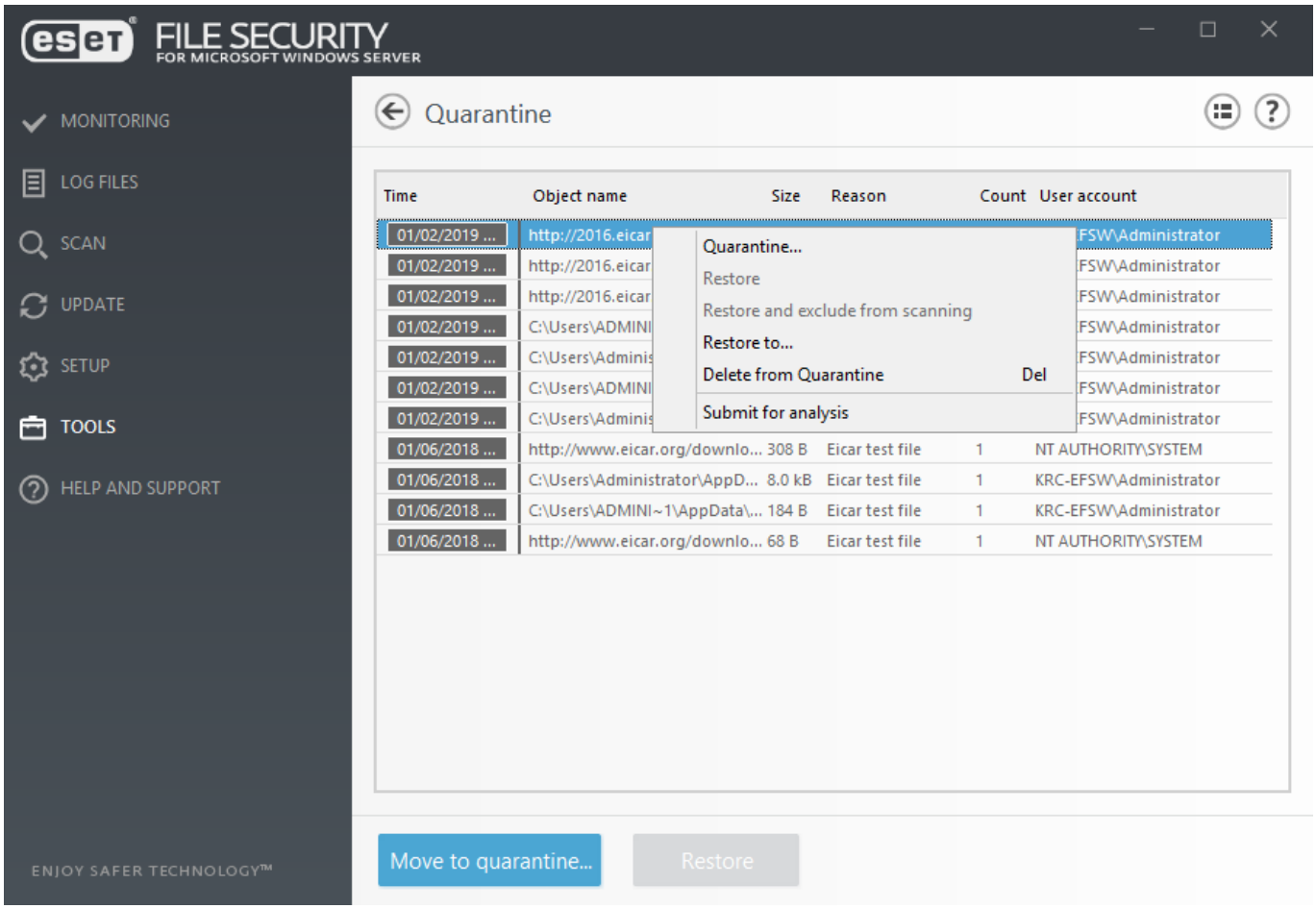
파일을 **감염 의심 파일** 또는 **가양성**으로 분류할 수 없는 경우 이 양식을 사용합니다.

파일 전송 사유

파일을 보내는 이유와 자세한 설명을 입력합니다.

검역소

검역소의 기본 기능은 감염된 파일을 안전하게 저장하는 것입니다. 치료할 수 없는 파일, 제거하는 것이 안전하지 않거나 권장되지 않는 파일 또는 ESET File Security에서 잘못 검출된 파일은 검역소로 보내야 합니다. 모든 파일을 검역소로 보내도록 선택할 수 있습니다. 동작이 의심스럽지만 악성코드 검사기에서 검색되지 않는 파일은 검역소로 보내는 것이 좋습니다. 검역소로 보낸 파일은 분석하기 위해 ESET 바이러스 연구소로 전송할 수 있습니다.



검역소 폴더에 저장된 파일은 표로 볼 수 있습니다. 이 표에는 검역소로 보낸 날짜와 시간, 감염된 파일의 원래 위치 경로, 파일 크기(바이트), 이유(예: 사용자가 추가한 개체) 및 위협 수(예: 해당 파일이 여러 침입이 포함된 압축파일인 경우)가 표시됩니다.

이메일 메시지 개체를 파일 검역소에 보내면 사서함/폴더/파일 이름 경로가 표시됩니다.

파일을 검역소로 보내기

ESET File Security는 제거된 파일을 자동으로 검역소에 보냅니다(경고 창에서 이 옵션을 비활성화하지 않은 경우). 감염 의심 파일을 수동으로 검역소에 보내려면 **검역소**를 클릭합니다. 검역소에 있는 파일은 원래 위치에서 제거됩니다. 또한 오른쪽 마우스 버튼 메뉴를 사용하여 수동으로 검역소에 보낼 수 있습니다. **검역소** 창에서 오른쪽 마우스 버튼을 클릭하고 **검역소**를 선택하면 됩니다.

검역소에서 복원

검역소에 있는 파일을 원래 위치로 복원할 수도 있습니다. **복원** 기능은 검역소 창에서 지정된 파일을 오른쪽 마우스 버튼으로 클릭하여 오른쪽 마우스 버튼 메뉴를 통해 사용할 수 있습니다. 파일이 사용자가 원치 않는 애플리케이션으로 표시되면 **복원 후 검사에서 제외** 옵션을 사용할 수 있습니다. 오른쪽 마우스 버튼 메뉴에는 파일이 제거된 위치가 아닌 다른 위치로 파일을 복원할 수 있는 **복원 대상...** 옵션도 있습니다.

> 참고
> 프로그램에서 실수로 아무 문제가 없는 파일을 검역소로 보낸 경우 해당 파일을 복원한 후 검사에서 파일을 제외한 다음 ESET 고객 지원으로 전송합니다.

검역소에서 파일 전송

프로그램에서 검색되지 않은 감염 의심 파일을 검역소에 보낸 경우 또는 코드의 휴리스틱 분석 등을 통해 파일이 감염된 것으로 잘못 평가되어 검역소로 보내진 경우에는 해당 파일을 ESET 바이러스 연구소로 전송하시기 바랍니다. 검역소에서 파일을 전송하려면 해당 파일을 오른쪽 마우스 버튼으로 클릭한 다음 표시되는 메뉴에서 분석을 위해 전송을 선택합니다.

검역소에서 제거

지정된 항목을 오른쪽 마우스 버튼으로 클릭한 후 **검역소에서 제거**를 선택합니다. 또는 해당 항목을 선택한 후 키보드에서 **delete** 키를 누릅니다.

OneDrive 검사 설정

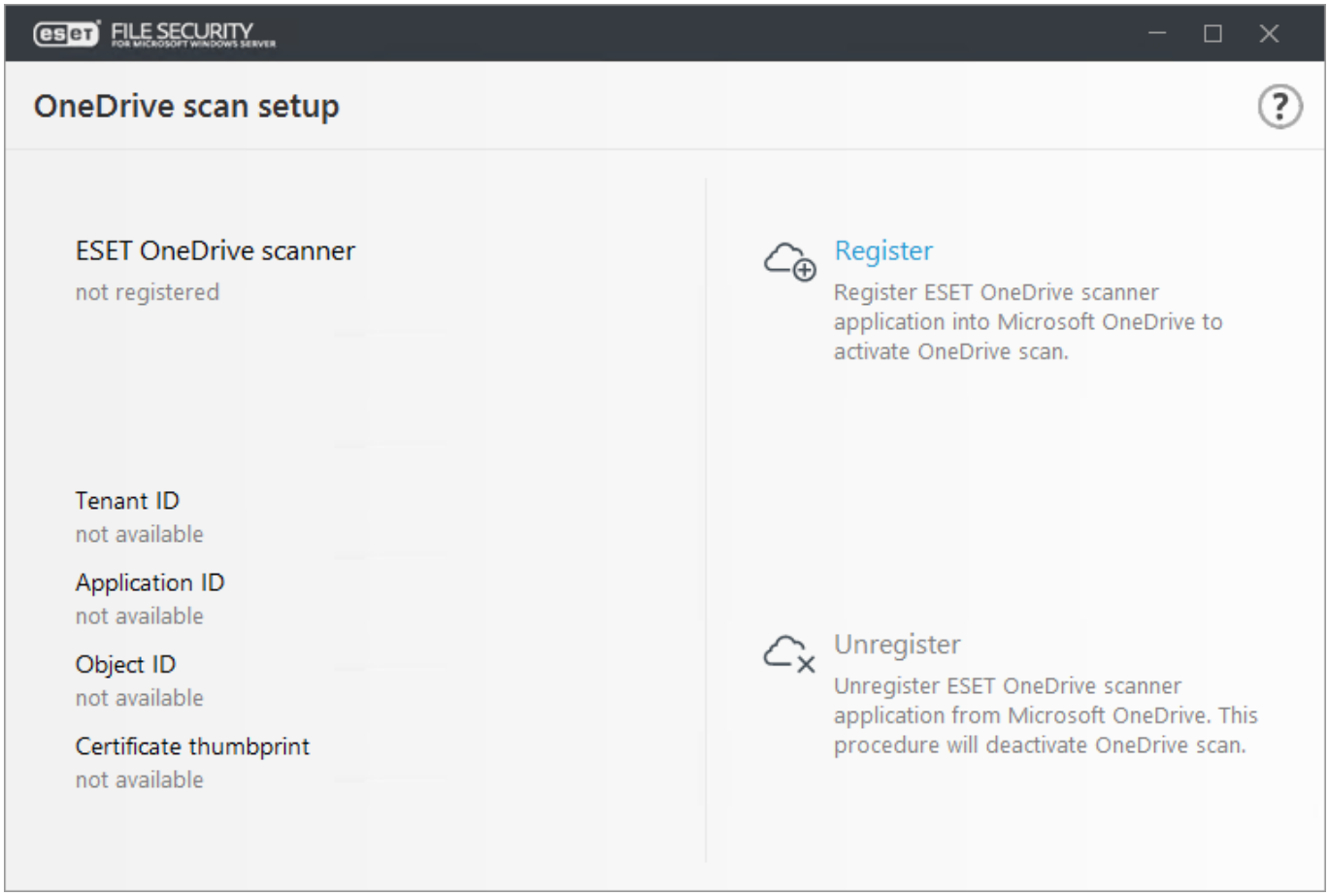
ESET File Security 열기
설정 > 서버 > *OneDrive* 검사 설정

이 기능을 사용하여 Microsoft 비즈니스용 OneDrive 클라우드 저장소에 파일을 저장할 수 있습니다. ESET File Security OneDrive 검사 프로세스 파일과 폴더만 필요하며, 이메일이나 SharePoint 파일, 연락처, 달력 같은 다른 유형의 데이터는 검사하지 않습니다.

빠른 링크

ESET OneDrive 스캐너 등록
ESET OneDrive 스캐너 등록 취소

ESET File Security OneDrive 검사를 사용하여 시작하려면 ESET OneDrive 스캐너 등록 애플리케이션을 Microsoft OneDrive/Microsoft Office 365/Microsoft Azure에 등록합니다. OneDrive 검사 설정 페이지에는 등록 상태가 표시되고(이미 등록된 경우), 등록 상세 정보(테넌트 ID, 애플리케이션 ID, 개체 ID 및 인증서 지문)가 나타납니다.



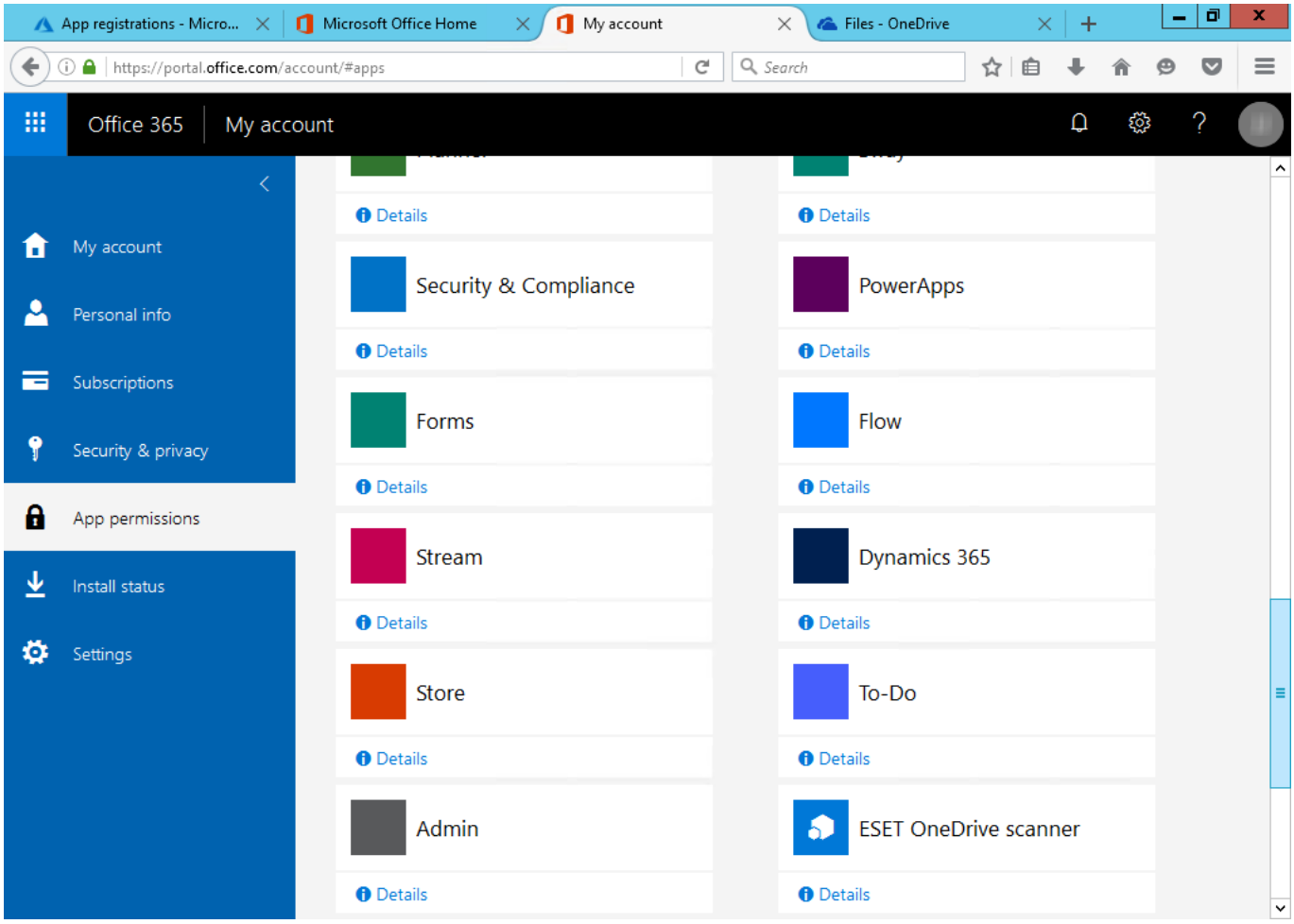
등록을 완료하면 검사를 위해 선택할 수 있는 파일과 폴더 구조를 갖춘 사용자 목록을 표시하는 검사 메뉴에서 OneDrive 검사를 사용할 수 있게 됩니다. ESET File Security OneDrive 검사에서는 사용자가 비즈니스용 OneDrive에 저장된 파일을 검사할 수 있습니다.

> 참고
> ESET File Security OneDrive 검사는 비즈니스용 OneDrive 클라우드 저장소에서 파일을 다운로드하고 로컬에서 검사를 수행합니다. 검사가 완료되면 다운로드한 파일이 제거됩니다. OneDrive에서 데이터를 대량 다운로드하면 네트워크 트래픽에 영향을 줍니다.

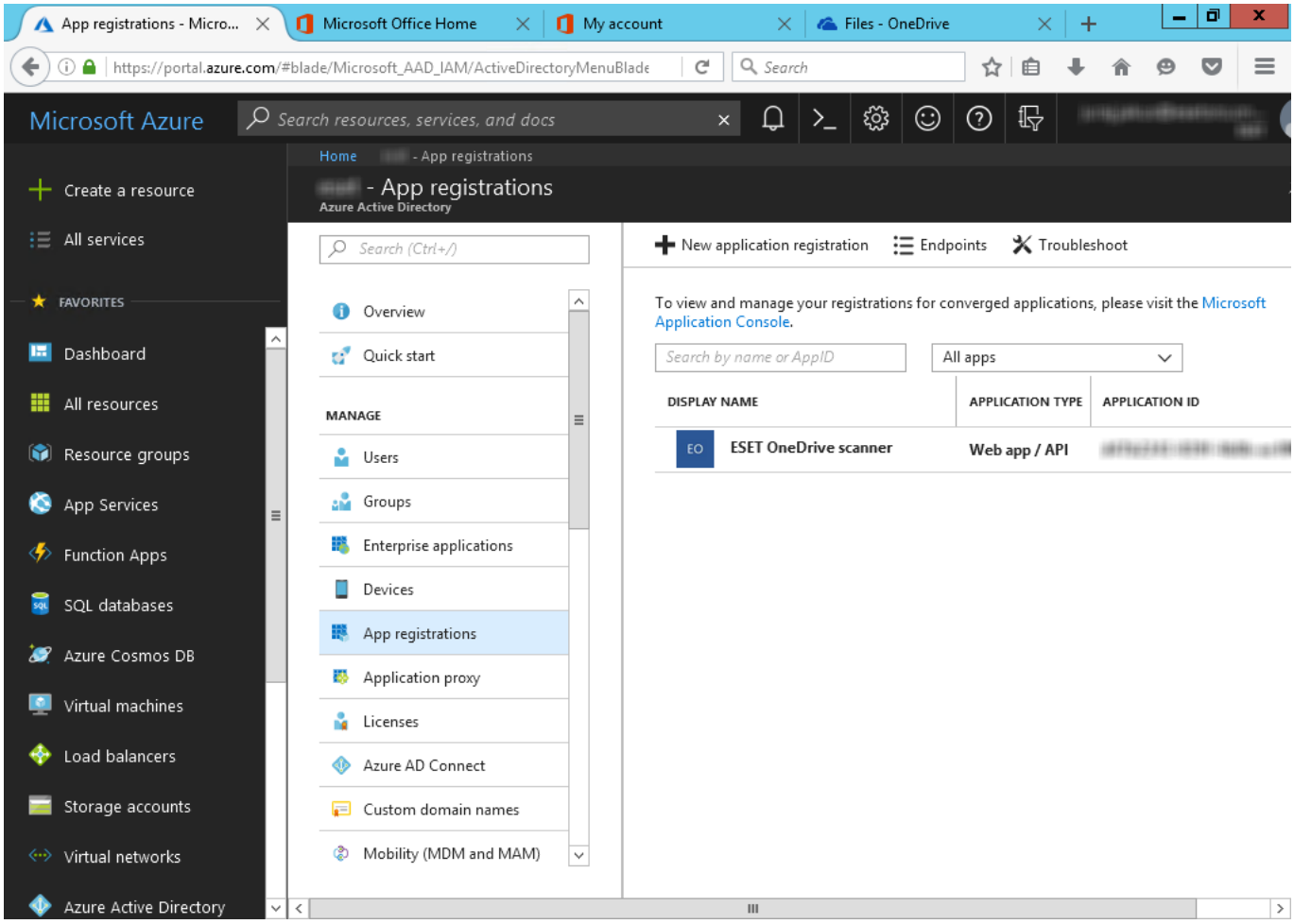
> 참고
> 다른 계정으로 다시 등록: 새로운 Microsoft 비즈니스용 OneDrive/Office 365 계정이 있는 ESET File Security OneDrive 스캐너를 등록하려면 이전 계정으로 사용 중인 ESET OneDrive 스캐너를 등록 취소하고 새로운 Microsoft 비즈니스용 OneDrive/Office 365 관리자 계정으로 등록을 수행해야 합니다.

Office 365와 Azure에서는 애플리케이션으로 등록된 ESET OneDrive 스캐너를 찾을 수 있습니다.

Office 365 포털 - 내 계정 페이지에서 **앱 권한**을 클릭하면 목록에 있는 ESET OneDrive 스캐너 앱이 표시됩니다.



Azure - **Azure Active Directory** > **앱 등록**으로 이동하여 **모든 애플리케이션 보기**를 클릭하면 목록에 있는 ESET OneDrive 스캐너 앱이 표시됩니다. 상세 정보를 확인하려면 앱을 클릭합니다.

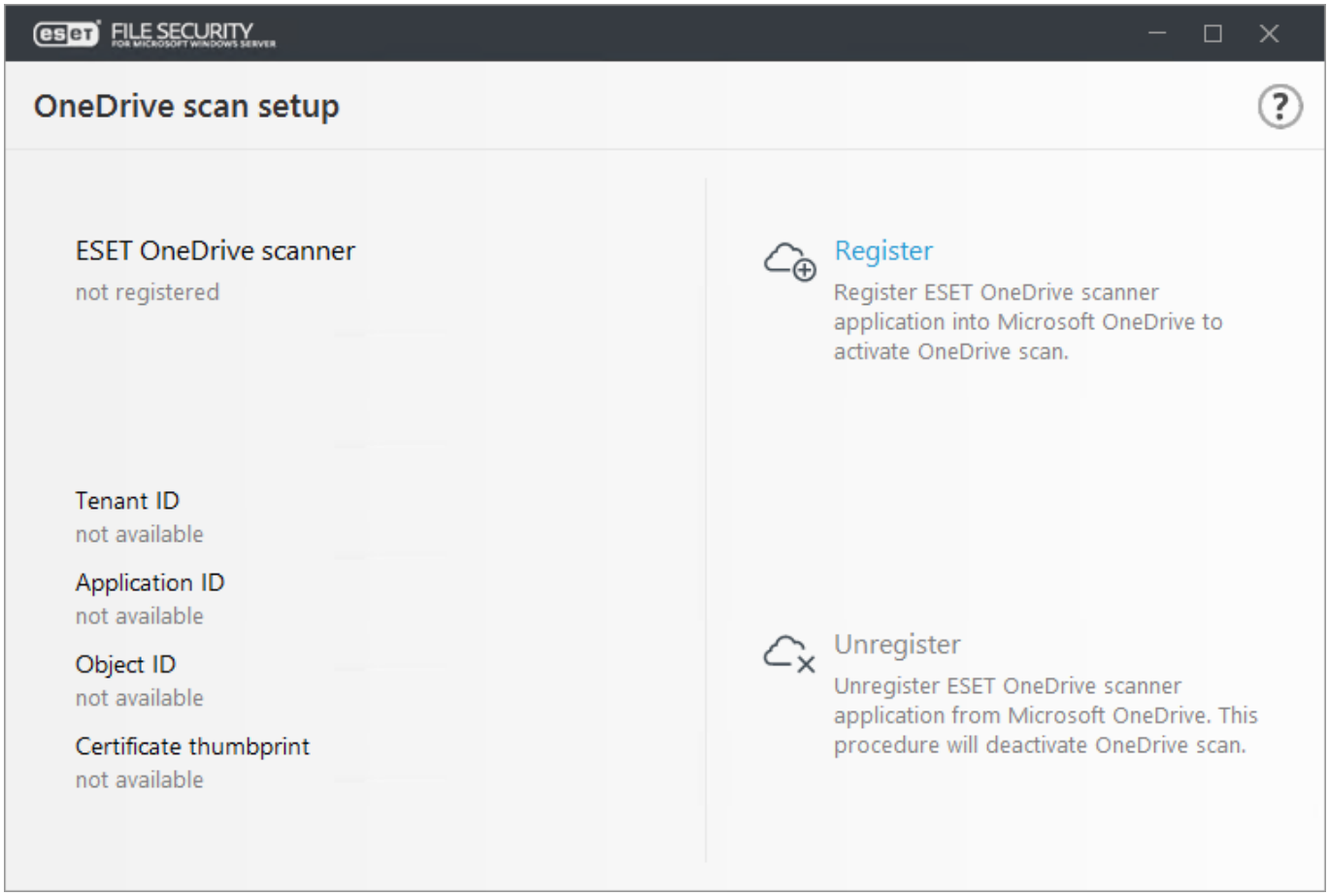


ESET OneDrive 스캐너 등록

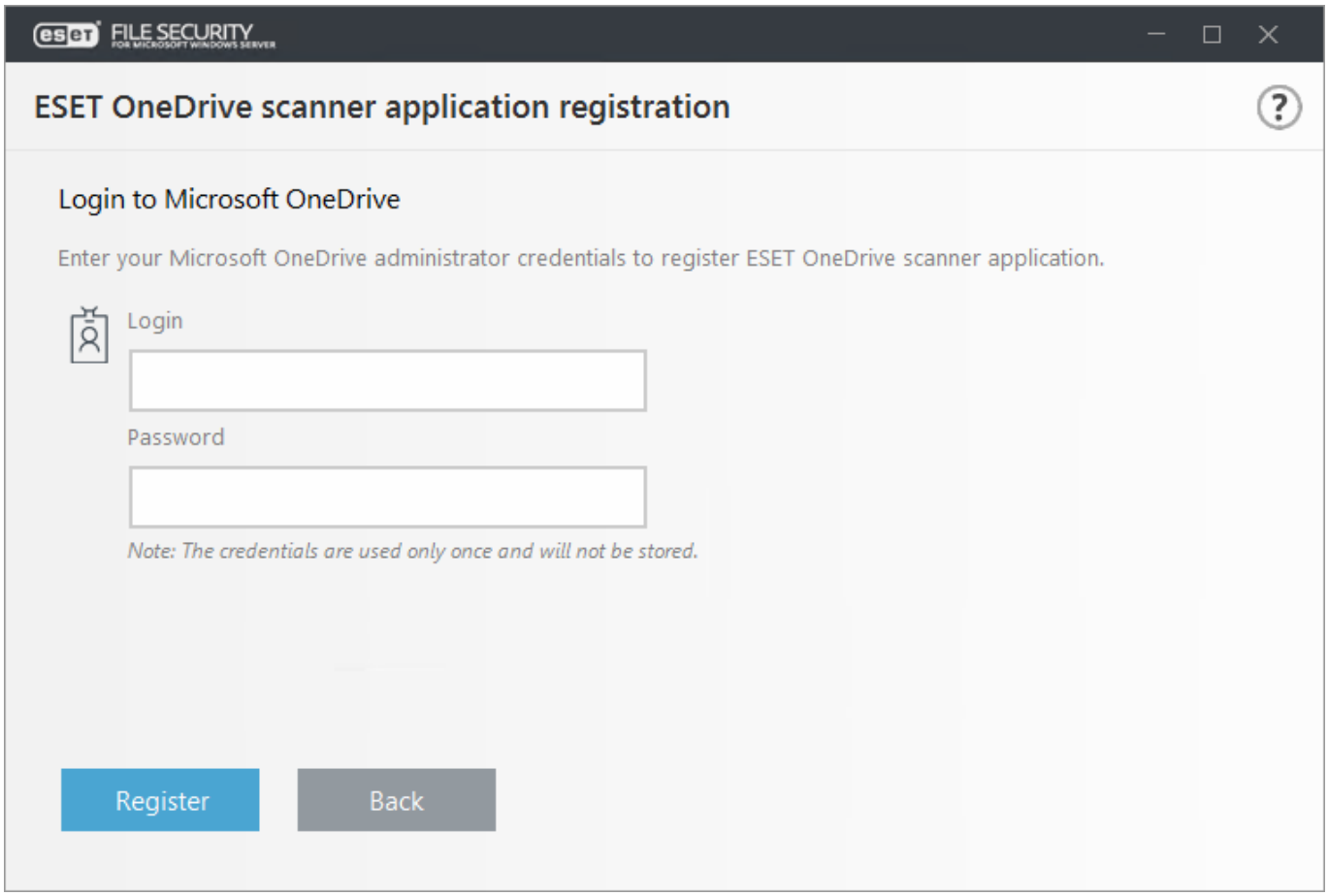
ESET File Security 열기
설정 > 서버 > *OneDrive* 검사 설정 > 등록 클릭

Microsoft OneDrive/Office 365/Azure에 ESET OneDrive 스캐너 앱을 등록하는 프로세스는 다음과 같습니다.

- **등록**을 클릭하여 ESET OneDrive 스캐너 등록을 시작하면 등록 마법사가 열립니다.

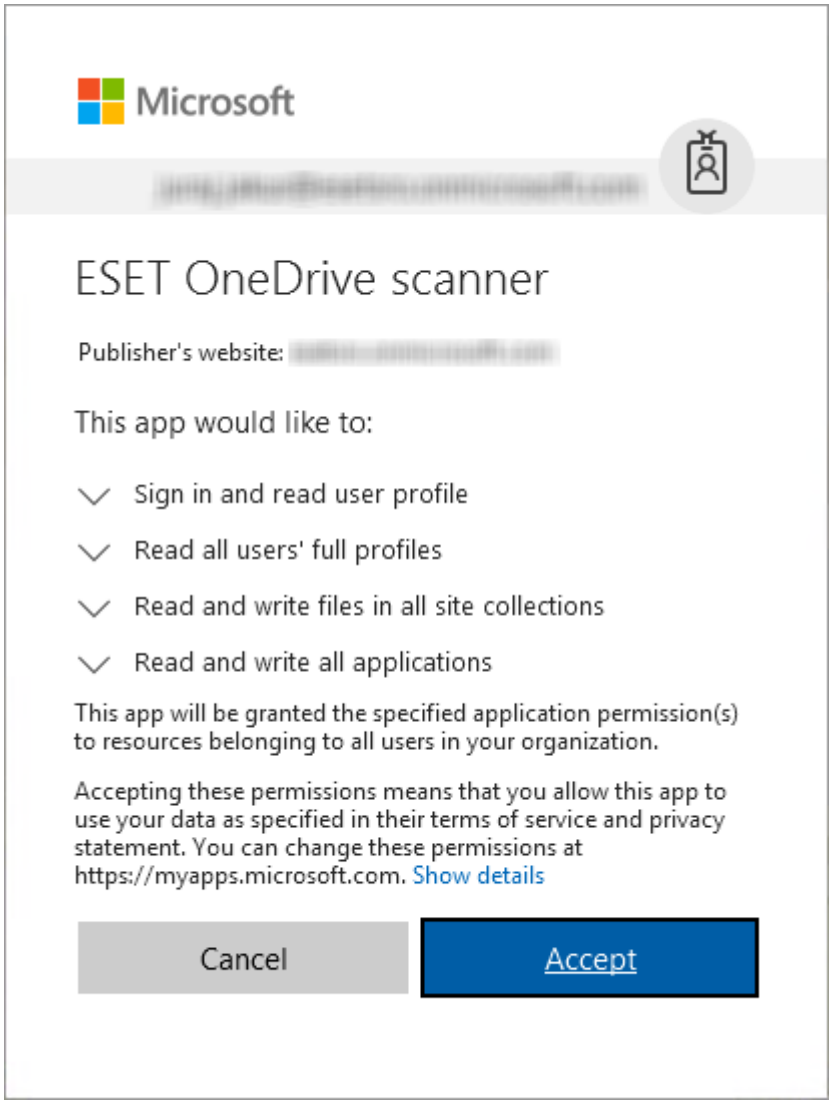


- Microsoft OneDrive/Office 365 관리자 계정 자격 증명을 입력합니다. Microsoft OneDrive에서 애플리케이션 등록을 완료할 때까지 기다립니다.



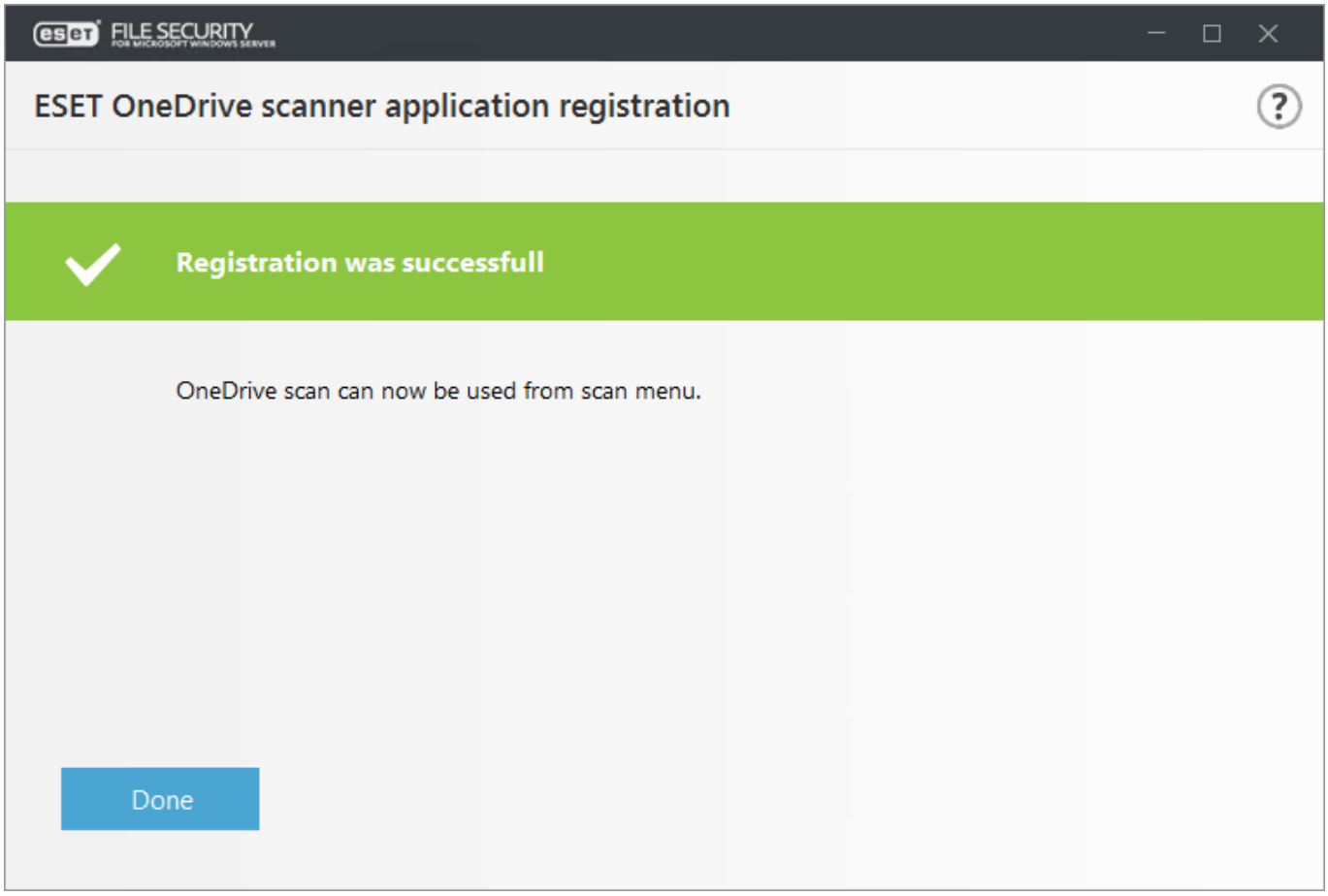
• Microsoft **계정 선택** 페이지가 있는 웹 브라우저가 열립니다. 해당하는 경우 사용 중인 계정을 클릭하거나, Microsoft OneDrive/Office 365 관리자 계정 자격 증명을 입력하고 **로그인**을 클릭합니다.

• ESET OneDrive 스캐너 앱에서는 동의 메시지에 나열된 네 가지 유형의 권한이 필요합니다. ESET File Security OneDrive 스캐너에서 OneDrive 클라우드 저장소에 있는 데이터에 접근할 수 있도록 하려면 **동의**를 클릭합니다.



• 웹 브라우저에 이 정보를 보낼 것인지(ESET File Security에서 앱이 등록되었는지 알 수 있도록 localhost로만 보내짐) 묻는 메시지가 표시되면 **계속**을 클릭합니다.

• 웹 브라우저를 닫은 후 ESET OneDrive 스캐너 등록 마법사에서 등록 완료 메시지를 표시하면 **완료**를 클릭합니다.



참고
관리자 계정 자격 증명을 사용하여 Microsoft 포털(OneDrive, Office 365, Azure 등)에 로그인했는지 여부 등에 따라 특정 환경에서는 ESET OneDrive 스캐너 등록 프로세스가 다를 수 있습니다. 화면의 지침과 등록 마법사 창의 메시지를 따릅니다.

ESET OneDrive 스캐너를 등록하는 동안 다음과 같은 오류 메시지가 나타나는 경우 권장되는 해결 방법에 대해서는 오류 메시지 상세 정보를 참조하십시오.

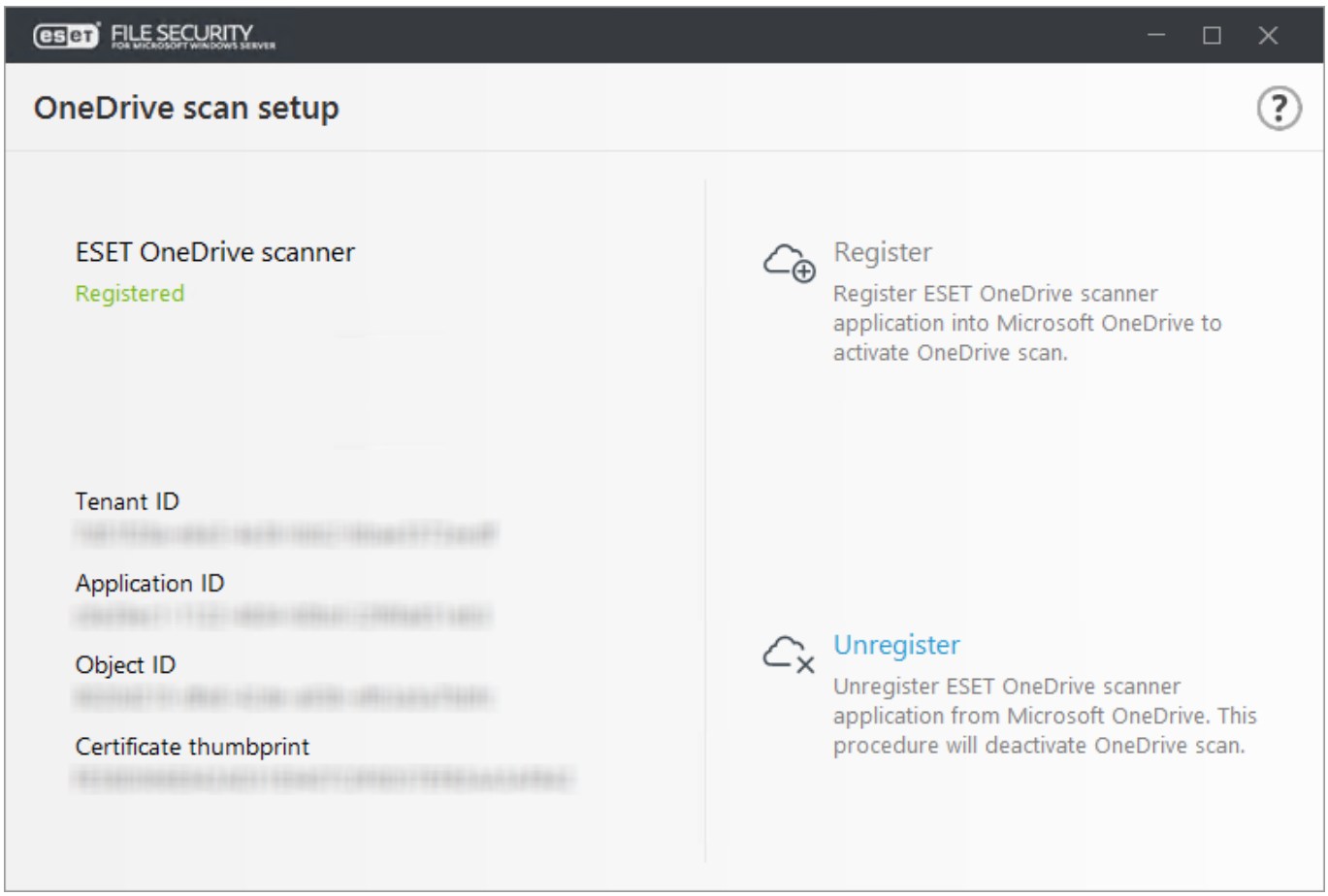
오류 메시지	오류 메시지 상세 정보
예기치 않은 오류가 발생했습니다.	ESET File Security에서 문제가 발생했을 수 있습니다. ESET OneDrive 스캐너 등록을 나중에 다시 실행하십시오. 문제가 계속되면 ESET 기술 지원에 문의하시기 바랍니다.
Microsoft OneDrive에 연결할 수 없습니다.	네트워크/인터넷 연결을 확인하고 ESET OneDrive 스캐너 등록을 다시 실행하십시오.
Microsoft Onedrive에서 예기치 않은 오류가 수신되었습니다.	오류 메시지 응답에 대한 답변이 없는 HTTP 4xx 오류가 반환되었습니다. 이 문제가 계속되면 ESET 기술 지원에 문의하시기 바랍니다.
Microsoft Onedrive에서 다음과 같은 오류가 수신되었습니다.	Microsoft OneDrive 서버에서 특정 오류 코드/이름이 있는 오류가 반환되었습니다. **오류 표시**를 클릭합니다.
설정 작업의 시간이 초과되었습니다.	ESET OneDrive 스캐너 등록 설정 작업이 너무 오래 걸립니다. ESET OneDrive 스캐너 등록을 나중에 다시 실행하십시오.
설정 작업이 취소되었습니다.	실행 중인 등록 작업을 취소했습니다. 등록을 완료하려면 ESET OneDrive 스캐너 등록을 다시 실행하십시오.
다른 설정 작업이 이미 진행 중입니다.	이미 실행 중인 등록 작업이 있습니다. 첫 번째 등록 프로세스가 완료될 때까지 기다리십시오.

ESET OneDrive 스캐너 등록 취소

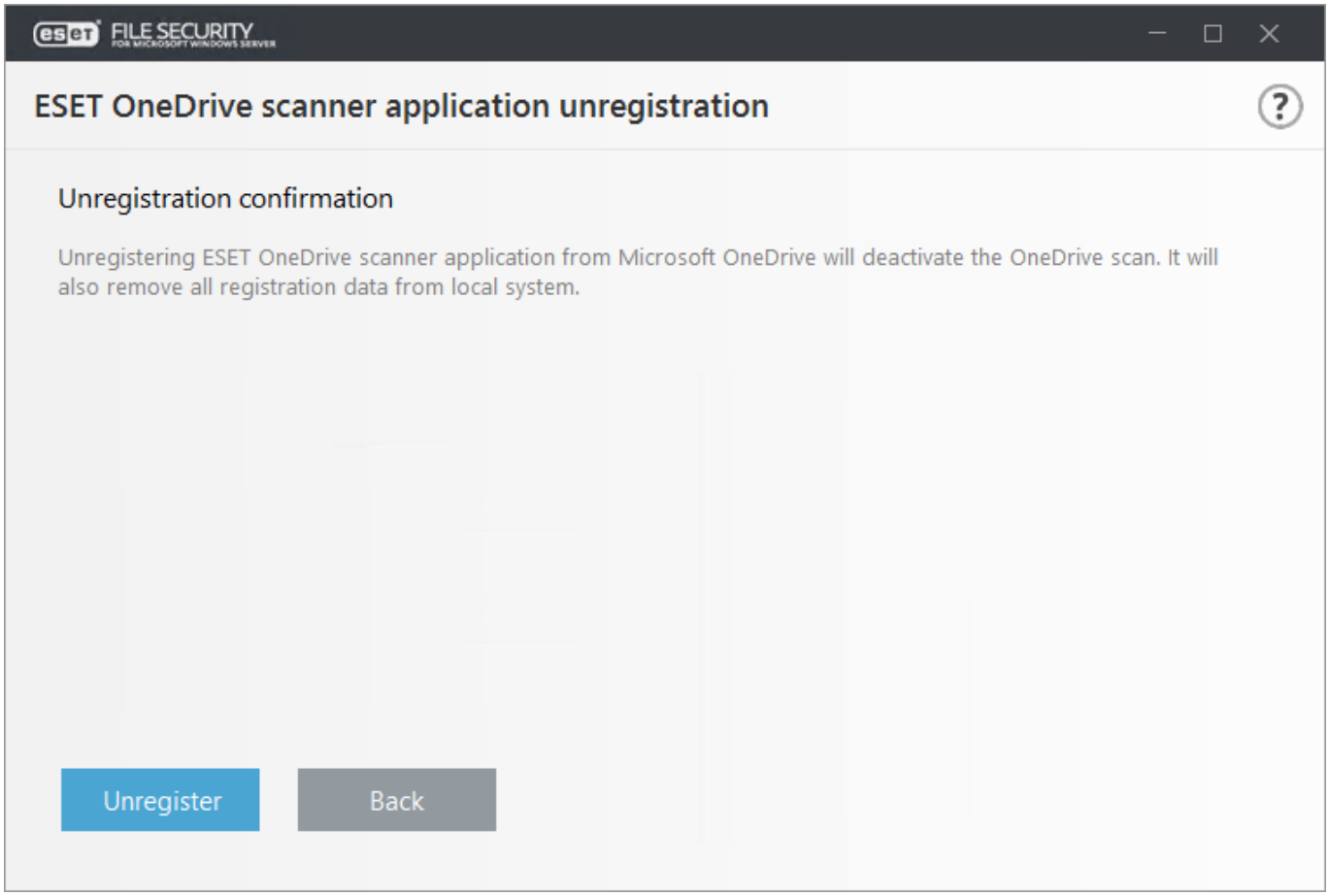
ESET File Security 열기
설정 > 서버 > *OneDrive* 검사 설정 > 등록 취소 클릭

프로세스를 등록 취소하면 인증서와 ESET OneDrive 스캐너 앱을 Microsoft OneDrive/Office 365/Azure에서 제거할 수 있습니다. 또한 이 프로세스에서는 로컬 종속성을 제거하고 등록 옵션을 다시 사용할 수 있게 해 줍니다.

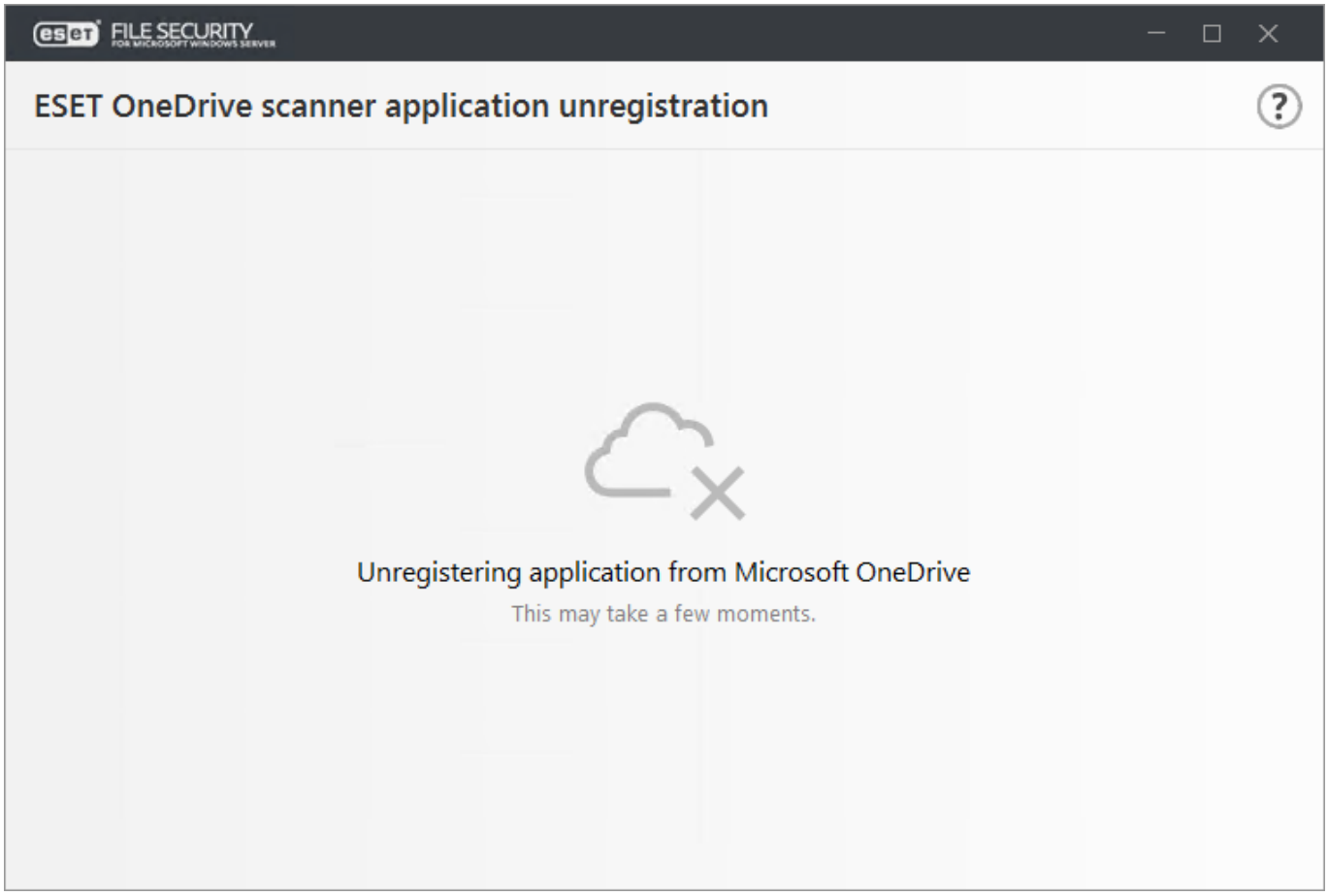
- **등록 취소**를 클릭하여 ESET OneDrive 스캐너 등록 취소/제거 프로세스를 시작하면 등록 취소 마법사가 열립니다.



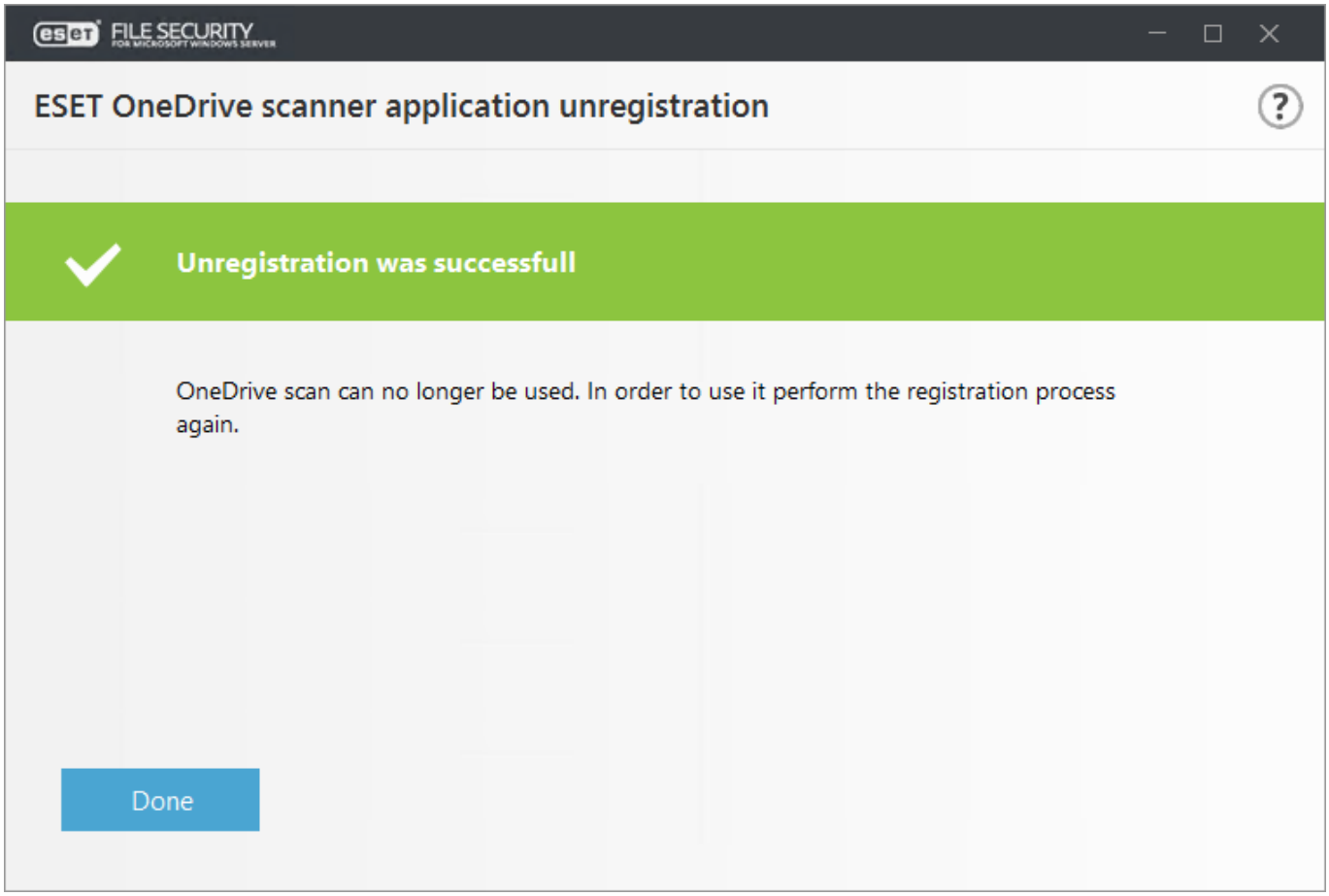
- **등록 취소**를 클릭하여 ESET OneDrive 스캐너를 제거할 것인지 확인합니다.



- Microsoft OneDrive에서 등록 취소를 완료할 때까지 기다립니다.



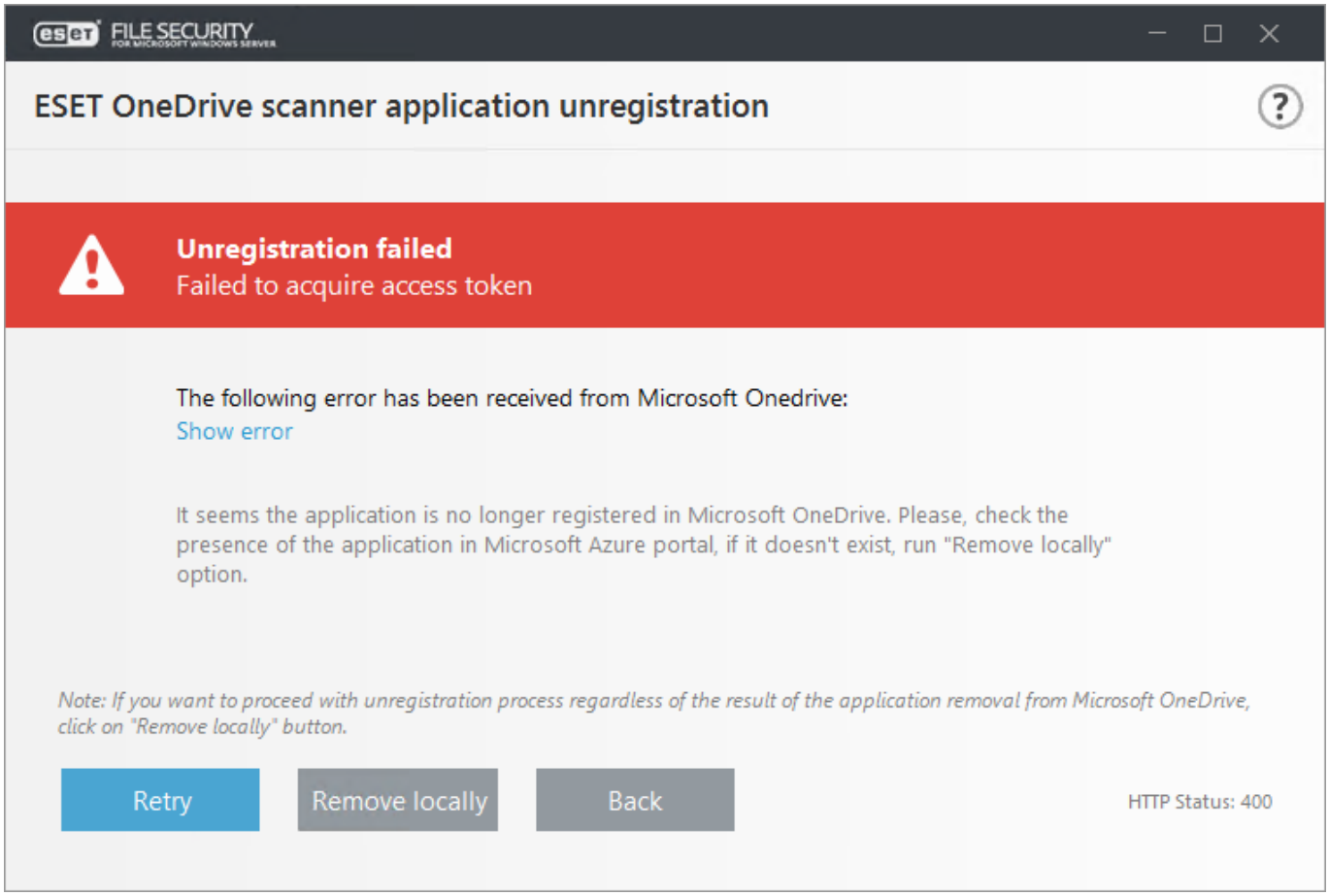
- 등록 취소 프로세스가 완료되면 등록 취소 마법사가 관련 메시지를 표시합니다.



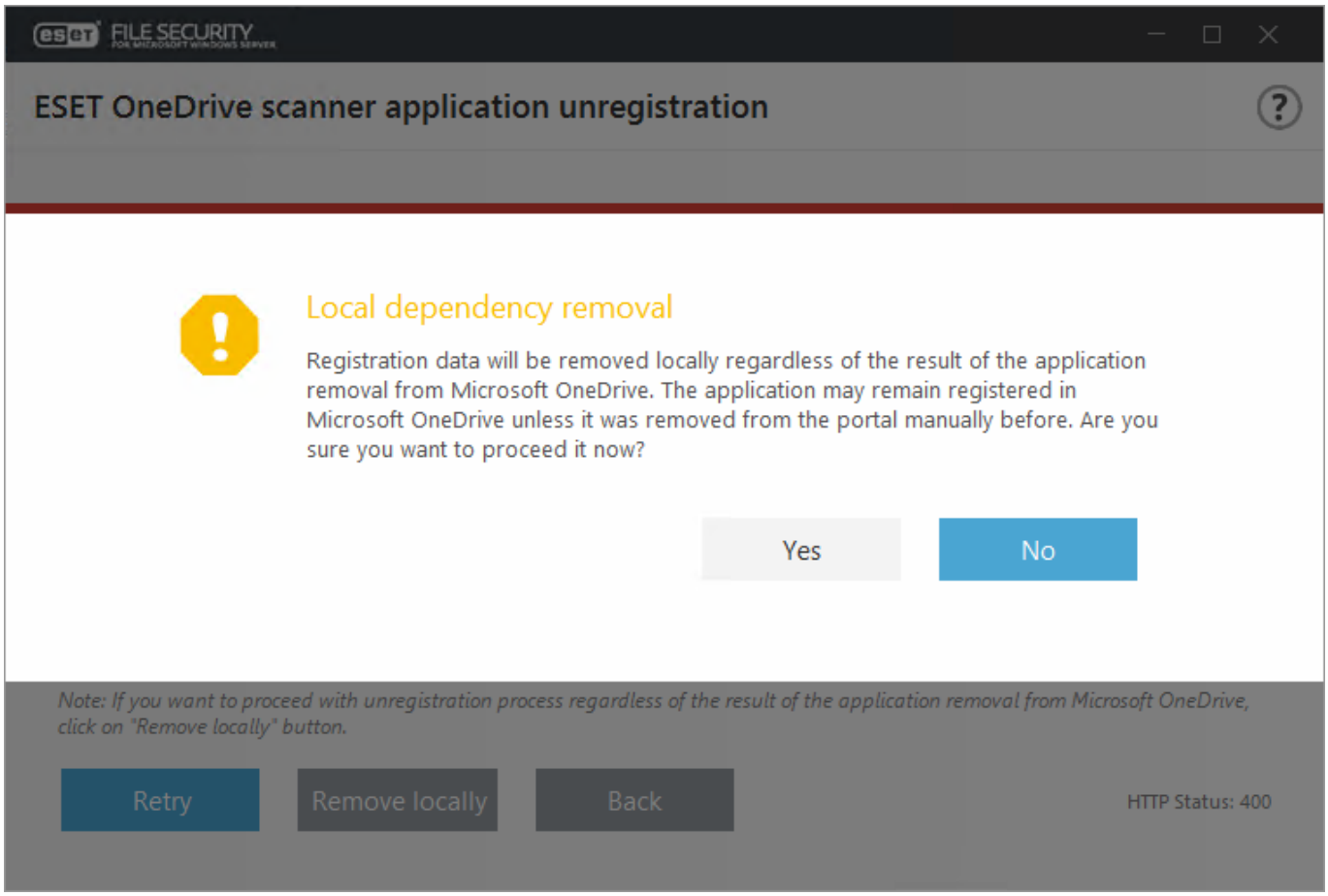
참고
등록 취소 실패 같은 오류 메시지가 표시되는 경우 Microsoft OneDrive 서버에서 나타나는 일반적인 네트워크나 인터넷 연결 문제 또는 ESET OneDrive 스캐너가 Microsoft OneDrive에 더 이상 등록되어 있지 않은 등의 여러 가지 이유가 있을 수 있습니다. 오류 메시지 목록과 이를 처리하는 방법에 대해서는 아래 표를 참조하십시오.

일부 오류 대화 상자에서는 로컬 종속성(연결 문제, Microsoft OneDrive에 존재하지 않는 앱 등)을 제거할 수 있는 옵션을 제공합니다. ESET OneDrive 스캐너를 로컬에서 제거하려면 다음을 수행하십시오.

- **다시 시도** 버튼이 작동하지 않고 문제가 계속되면 **로컬에서 제거**를 클릭하여 ESET OneDrive 스캐너 로컬 종속성을 제거할 등록 취소 프로세스를 계속 진행합니다.



- 계속해서 ESET OneDrive 스캐너를 로컬에서 제거하려면 **예**를 클릭합니다. ESET OneDrive 검사는 더 이상 사용할 수 없게 되며, 등록 프로세스를 다시 실행해야 합니다.



중요
로컬 종속성을 제거하면 Azure 포털의 앱 등록을 변경할 수 없게 되며, Office 365 포털에서 앱 권한도 변경할 수 없게 됩니다. Microsoft OneDrive 서버에서 나타나는 네트워크나 연결 문제 때문에 ESET OneDrive 스캐너를 로컬에서 제거한 경우 Azure의 앱 등록에서 ESET OneDrive 스캐너 앱을 수동으로 제거해야 합니다. Azure 포털에서 ESET OneDrive 스캐너를 찾고 수동으로 제거하는 방법에 대해서는 OneDrive 검사 설정을 참조하십시오.

ESET OneDrive 스캐너를 등록 취소하는 동안 다음과 같은 오류 메시지가 나타나는 경우 권장 해결 방법에 대해서는 오류 메시지 상세 정보를 참조하십시오.

오류 메시지	오류 메시지 상세 정보
Azure 애플리케이션에 연결하지 못했습니다. 인터넷에 연결되어 있지 않습니다.	네트워크/인터넷 연결을 확인하고 등록 취소를 다시 실행합니다. Microsoft OneDrive에서 ESET OneDrive 스캐너 앱을 제거하지 않고 등록 취소 프로세스를 계속 진행하려면 **로컬에서 제거**를 클릭합니다.
접근 토큰을 가져오지 못했습니다. Microsoft Onedrive에서 예기치 않은 오류가 수신되었습니다.	ESET OneDrive 스캐너 앱이 Microsoft OneDrive에 더 이상 등록되어 있지 않은 것 같습니다. ESET OneDrive 스캐너 앱은 Azure 포털에서 수동으로 제거할 수 있습니다. Microsoft OneDrive 또는 Azure 포털에 ESET OneDrive 스캐너 앱이 있는지 확인하십시오. 앱이 나열되지 않으면 **로컬에서 제거**를 클릭하여 등록 취소 프로세스를 계속 진행합니다.
접근 토큰을 가져오지 못했습니다. Microsoft Onedrive에서 서버 오류가 수신되었습니다.	Microsoft OneDrive에서 HTTP 5xx 오류가 반환되었습니다. 지금은 등록 취소 작업을 완료할 수 없습니다. 나중에 다시 등록 취소를 실행하십시오.
Microsoft Onedrive에서 다음과 같은 오류가 수신되었습니다.	Microsoft OneDrive 서버에서 특정 오류 코드/이름이 있는 오류가 반환되었습니다. **오류 표시**를 클릭합니다.
다른 설정 작업이 이미 진행 중입니다.	이미 실행 중인 등록 취소 작업이 있습니다. 첫 번째 등록 취소 프로세스가 완료될 때까지 기다리십시오.

일반 설정

필요에 따라 일반 설정과 옵션을 구성할 수 있습니다. 왼쪽의 메뉴는 다음 범주를 포함합니다.

진단 엔진

잠재적으로 원치 않고 안전하지 않으며 감염이 의심되는 애플리케이션 및 안티스텔스 보호의 검색 기능을 활성화 또는 비활성화합니다. 프로세스나 파일/폴더 제외 항목을 지정합니다. 실시간 파일 시스템 보호, ThreatSense 파라미터, 클라우드 기반 보호(ESET LiveGrid®), 악성코드 검사(수동 컴퓨터 검사와 기타 검사 옵션), Hyper-V 검사 및 HIPS를 구성합니다.

업데이트

프로필, 진단 엔진 기간, 모듈 롤백 스냅숏, 업데이트 유형, 사용자 지정 업데이트 서버, 연결/프록시 서버, 업데이트 미러, 업데이트 파일 접근, HTTP 서버, 네트워크 연결에 대한 사용자 계정 상세 정보 등의 업데이트 옵션을 구성합니다.

웹 및 이메일

프로토콜 필터링과 제외 항목(제외된 플리케이션 및 IP 주소), SSL/TLS 프로토콜 필터링 옵션, 이메일 클라이언트 보호(통합, 이메일 프로토콜, 경고 및 알림), 웹 브라우저 보호(HTTP/HTTPS 웹 프로토콜 및 URL 주소 관리), 이메일 클라이언트 안티피싱 보호를 구성할 수 있습니다.

장치 제어

통합을 활성화하고 장치 제어 규칙 및 그룹을 구성합니다.

도구 구성

ESET CMD, ESET RMM, WMI 공급자, ESET Security Management Center 검사 대상, Windows 업데이트 알림, 로그 파일, 프록시 서버, 이메일 알림, 분석, 클러스터 등의 도구를 사용자 지정할 수 있습니다.

사용자 인터페이스

프로그램 GUI의 동작, 상태, 라이선스 정보, 경고 및 알림, 패스워드 보호, eShell 실행 정책 등을 구성합니다.

진단 엔진

탐지 엔진이 파일, 이메일 및 네트워크 통신을 검사하여 악의적인 시스템 공격으로부터 보호합니다. 악성코드로 분류된 개체가 탐지되면 수정이 시작됩니다. 탐지 엔진은 먼저 개체를 차단한 다음 치료, 제거하거나 검역소로 이동하는 등의 조치를 수행하여 해당 개체를 제거할 수 있습니다.

실시간 및 머신 러닝 보호

고급 머신 러닝은 이제 고급 보호 계층인 탐지 엔진의 일부로, 머신 러닝을 기반으로 하는 탐지를 개선합니다. 용어집에서 이 보호 유형에 대해 자세히 알아보십시오. 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. 용어집에서 해당 애플리케이션 유형에 대해 자세히 알아보십시오.

사용자가 원치 않는 애플리케이션(PUA)

사용자가 원치 않는 애플리케이션은 명백하게 악의적이지는 않지만 원치 않는 소프트웨어를 추가로 설치하거나, 디지털 장치의 동작을 변경하거나, 사용자가 승인하지 않거나 사용자에게 필요하지 않은 활동을 수행할 수 있으며 기타 명확하지 않은 목적을 포함합니다.
이 범주에는 광고 표시 소프트웨어, 래퍼 다운로드, 여러 브라우저 도구 모음, 잘못된 동작을 포함한 소프트웨어, 번들웨어, 트랙웨어 등이 포함됩니다.
이러한 유형의 애플리케이션에 대한 자세한 내용은 용어집을 참조하십시오.

잠재적인 감염 의심 애플리케이션

패커나 보호기로 압축된 소프트웨어로, 독점적인 압축 및/또는 암호화 방법을 사용하여 리버스 엔지니어링을 방지하거나 실행 파일의 내용(예: 악성코드의 존재 숨기기 등)을 난독화하는 데 주로 사용됩니다.
이 범주에는 악성코드를 압축하는 데 주로 사용되는 패커나 보호기로 압축된, 알 수 없는 모든 애플리케이션이 포함됩니다.

사용자에게 안전하지 않은 애플리케이션

이 분류는 악의적으로 잘못 사용될 수 있는 적법한 상용 소프트웨어에 지정됩니다. 안전하지 않은 애플리케이션은 악의적으로 잘못 사용될 가능성이 있는 적법한 상용 소프트웨어를 일컫습니다.
이 범주에는 도구, 라이선스 키 생성기 크랙, 도구, 원격 접근 또는 검사 도구 해킹, 패스워드 크랙 애플리케이션 및 키로거(사용자가 입력한 각 키 입력을 기록하는 프로그램)가 포함됩니다. 이 옵션은 기본적으로 비활성화되어 있습니다.
이러한 유형의 애플리케이션에 대한 자세한 내용은 용어집을 참조하십시오.

범주 보고 또는 보호에 대한 한계치(또는 수준)를 수정하기 전에 다음을 읽어보십시오.

보고

보고는 탐지 엔진과 머신 러닝 구성 요소에 의해 수행됩니다. 사용자 환경과 요구 사항에 더 부합하도록 보고 한계치를 설정할 수 있습니다. 올바른 구성이 하나도 없습니다. 따라서 환경 내에서 동작을 모니터링하고 다른 보고 설정이 더 적합한지 결정하는 것이 좋습니다.

보고는 개체에 대한 조치를 수행하지 않고 정보를 각 보호 계층에 전달하며 보호 계층이 그에 따라 조치를 수행합니다.

공격적	**최대 민감도로 구성된 보고입니다. 자세한 탐지 사항이 보고됩니다. 공격적 설정이 가장 안전한 것처럼 보일 수 있지만 간혹 너무 민감하여 역효과가 발생할 수도 있습니다.** 참고 공격적 설정에서는 개체를 악성으로 잘못 식별하여 해당 개체에 조치를 수행할 수 있습니다(보호 설정에 따라).
균형 잡힘	이 설정은 성능과 탐지율의 정확도 및 잘못 보고된 개체 수 사이의 최적화된 균형입니다.
조심스러움	충분한 보호 수준을 유지하면서 잘못 식별된 개체를 최소화하도록 구성된 보고입니다. 개체는 가능성이 분명히 있고 악의적인 동작과 일치하는 경우에만 보고됩니다.
끄기	보고가 활성화되어 있지 않습니다. 탐지 사항이 발견, 보고 또는 치료되지 않았습니다. 참고 악성코드 보고를 비활성화할 수 없으므로 악성코드에 대해 ***끄기*** 설정을 사용할 수 없습니다.

이 섹션의 설정을 기본값으로 되돌리려면 섹션 헤더 옆에 있는 "유턴" 화살표를 클릭합니다. 이 섹션에서 변경한 모든 내용이 손실됩니다.

보호

위의 구성과 머신 러닝 결과에 따라 개체가 보고되면 개체가 차단되고 조치가 수행됩니다(치료, 제거되거나 검역소로 이동).

공격적	**공격적(또는 이보다 낮은) 수준으로 보고된 탐지가 차단되고, 자동 수정(즉 치료)이 시작됩니다.**
균형 잡힘	균형 잡힌(또는 이보다 낮은) 수준으로 보고된 탐지가 차단되고, 자동 수정(즉 치료)이 시작됩니다.
조심스러움	조심스러운 수준으로 보고된 탐지가 차단되고, 자동 수정(즉 치료)이 시작됩니다.

공격적	공격적(또는 이보다 낮은) 수준으로 보고된 탐지가 차단되고, 자동 수정(즉 치료)이 시작됩니다.
끄기	보고가 활성화되지 않았거나 탐지 사항이 발견, 보고 또는 치료되지 않았습니다. 참고 악성코드 보고를 비활성화할 수 없으므로 악성코드에 대해 **끄기** 설정을 사용할 수 없습니다.

이 섹션의 설정을 기본값으로 되돌리려면 섹션 헤더 옆에 있는 "유턴" 화살표를 클릭합니다. 이 섹션에서 변경한 모든 내용이 손실됩니다.

> 참고
> 기본적으로 위의 머신 러닝 보호 설정은 수동 컴퓨터 검사에도 적용됩니다. 필요한 경우 **수동 및 머신 러닝 보호** 설정을 별도로 구성할 수 있습니다. 전환 아이콘을 클릭하여 **실시간 보호 설정 사용**을 비활성화하고 구성을 진행합니다.

머신 러닝 탐지

탐지 엔진이 파일, 이메일 및 네트워크 통신을 검사하여 악의적인 시스템 공격으로부터 보호합니다. 악성코드로 분류된 개체가 탐지되면 수정이 시작됩니다. 탐지 엔진은 먼저 개체를 차단한 다음 치료, 제거하거나 검역소로 이동하는 등의 조치를 수행하여 해당 개체를 제거할 수 있습니다.

실시간 및 머신 러닝 보호

고급 머신 러닝은 이제 고급 보호 계층인 탐지 엔진의 일부로, 머신 러닝을 기반으로 하는 탐지를 개선합니다. 용어집에서 이 보호 유형에 대해 자세히 알아보십시오. 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. 용어집에서 해당 애플리케이션 유형에 대해 자세히 알아보십시오.

사용자가 원치 않는 애플리케이션(PUA)

사용자가 원치 않는 애플리케이션은 명백하게 악의적이지는 않지만 원치 않는 소프트웨어를 추가로 설치하거나, 디지털 장치의 동작을 변경하거나, 사용자가 승인하지 않거나 사용자에게 필요하지 않은 활동을 수행할 수 있으며 기타 명확하지 않은 목적을 포함합니다.
이 범주에는 광고 표시 소프트웨어, 래퍼 다운로드, 여러 브라우저 도구 모음, 잘못된 동작을 포함한 소프트웨어, 번들웨어, 트랙웨어 등이 포함됩니다.
이러한 유형의 애플리케이션에 대한 자세한 내용은 용어집을 참조하십시오.

잠재적인 감염 의심 애플리케이션

패커나 보호기로 압축된 소프트웨어로, 독점적인 압축 및/또는 암호화 방법을 사용하여 리버스 엔지니어링을 방지하거나 실행 파일의 내용(예: 악성코드의 존재 숨기기 등)을 난독화하는 데 주로 사용됩니다.
이 범주에는 악성코드를 압축하는 데 주로 사용되는 패커나 보호기로 압축된, 알 수 없는 모든 애플리케

이션이 포함됩니다.

사용자에게 안전하지 않은 애플리케이션

이 분류는 악의적으로 잘못 사용될 수 있는 적법한 상용 소프트웨어에 지정됩니다. 안전하지 않은 애플리케이션은 악의적으로 잘못 사용될 가능성이 있는 적법한 상용 소프트웨어를 일컫습니다.
이 범주에는 도구, 라이선스 키 생성기 크랙, 도구, 원격 접근 또는 검사 도구 해킹, 패스워드 크랙 애플리케이션 및 키로거(사용자가 입력한 각 키 입력을 기록하는 프로그램)가 포함됩니다. 이 옵션은 기본적으로 비활성화되어 있습니다.
이러한 유형의 애플리케이션에 대한 자세한 내용은 용어집을 참조하십시오.

범주 보고 또는 보호에 대한 한계치(또는 수준)를 수정하기 전에 다음을 읽어보십시오.

보고

보고는 탐지 엔진과 머신 러닝 구성 요소에 의해 수행됩니다. 사용자 환경과 요구 사항에 더 부합하도록 보고 한계치를 설정할 수 있습니다. 올바른 구성이 하나도 없습니다. 따라서 환경 내에서 동작을 모니터링하고 다른 보고 설정이 더 적합한지 결정하는 것이 좋습니다.

보고는 개체에 대한 조치를 수행하지 않고 정보를 각 보호 계층에 전달하며 보호 계층이 그에 따라 조치를 수행합니다.

공격적	**최대 민감도로 구성된 보고입니다. 자세한 탐지 사항이 보고됩니다. 공격적 설정이 가장 안전한 것처럼 보일 수 있지만 간혹 너무 민감하여 역효과가 발생할 수도 있습니다.** 참고 공격적 설정에서는 개체를 악성으로 잘못 식별하여 해당 개체에 조치를 수행할 수 있습니다(보호 설정에 따라).
균형 잡힘	이 설정은 성능과 탐지율의 정확도 및 잘못 보고된 개체 수 사이의 최적화된 균형입니다.
조심스러움	충분한 보호 수준을 유지하면서 잘못 식별된 개체를 최소화하도록 구성된 보고입니다. 개체는 가능성이 분명히 있고 악의적인 동작과 일치하는 경우에만 보고됩니다.
끄기	보고가 활성화되어 있지 않습니다. 탐지 사항이 발견, 보고 또는 치료되지 않았습니다. 참고 악성코드 보고를 비활성화할 수 없으므로 악성코드에 대해 **끄기** 설정을 사용할 수 없습니다.

이 섹션의 설정을 기본값으로 되돌리려면 섹션 헤더 옆에 있는 "유턴" 화살표를 클릭합니다. 이 섹션에서 변경한 모든 내용이 손실됩니다.

OneDrive 및 머신 러닝 보호

보고

탐지 엔진과 머신 러닝 구성 요소에 의해 수행됩니다. 보고는 개체에 대해 조치를 수행하지 않습니다(이 조치는 각 보호 계층에서 수행함).

보호

보고된 개체에 대해 수행할 조치에 영향을 주도록 OneDrive 섹션에서 파라미터를 구성합니다.

이 섹션의 설정을 기본값으로 되돌리려면 섹션 헤더 옆에 있는 "유턴" 화살표를 클릭합니다. 이 섹션에서 변경한 모든 내용이 손실됩니다.

eShell을 사용하여 머신 러닝 보호를 구성합니다. eShell의 컨텍스트 이름은 **MLP**입니다. eShell을 대화 모드로 열고 다음 MLP로 이동:

```
computer onedrive mlp
```

감염 의심 애플리케이션에 대한 현재 보고 설정 확인:

```
get suspicious-reporting
```

덜 엄격한 보고를 원하는 경우 설정을 조심스러움으로 변경:

```
set suspicious-reporting cautious
```

제외

제외를 사용하여 파일 및 폴더를 검사에서 제외할 수 있습니다. 모든 개체에서 위협 요소가 있는지 검사하려면 반드시 필요한 항목만 제외로 생성하는 것이 좋습니다. 검사 중 서버 속도를 저하시키는 대용량 데이터베이스 항목 또는 검사와 충돌하는 소프트웨어(예: 백업 소프트웨어)와 같은 개체를 제외해야 하는 상황이 있을 수 있습니다.

> 경고
> 제외된 확장명, 프로세스 제외 또는 제외 필터와 혼동하지 않도록 유의하십시오.

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

제외 유형을 선택하고 **편집**을 클릭하여 새 유형을 추가하거나 다음과 같은 기존 유형을 수정합니다.

- 성능 제외 - 검사에서 파일 및 폴더를 제외합니다.
- 탐지 제외 - 경로, 파일 해시 또는 검색 이름 등의 특정 기준을 사용하여 검사에서 개체를 제외합니다.

성능 제외

이 기능을 사용하면 검사에서 파일 및 폴더를 제외할 수 있습니다. 성능 제외는 업무에 중대한 애플리케이션의 파일 수준 검사를 제외하거나, 검사 시 비정상적인 시스템 동작이 발생하거나 성능이 저하되는 경우에 유용합니다.

경로

이 컴퓨터에 대한 특정 경로(파일 또는 디렉토리)를 제외합니다. 경로 중간에 와일드카드, 즉 별표(*)를 사용하지 마십시오. 자세한 내용은 지식베이스 문서(↗)를 참조하십시오.

참고
폴더 콘텐츠를 제외하려면 경로 끝에 별표(*)를 추가(*C:\Tools**)하는 것을 잊지 마십시오. 검사기 관점에서 볼 때 *Tools*도 파일 이름일 수 있으므로, *C:\Tools*는 제외되지 않습니다.

설명

선택적 **설명**을 추가하면 향후에 제외를 쉽게 인식할 수 있습니다.

예
별표를 사용하여 경로 제외:
*C:\Tools** - 한 폴더와 모든 폴더 콘텐츠(파일 및 하위 폴더)가 제외됨을 나타내려면 경로가 백슬래시(\)와 별표(*)로 끝나야 합니다.
C:\Tools.** - *C:\Tools**와 같은 동작입니다. 즉, 재귀적으로 작동합니다.
C:\Tools.dat* - 도구 폴더의 *dat* 파일을 제외함
C:\Tools\sg.dat - 정확한 경로에 있는 이 특정 파일을 제외함

예
폴더의 모든 파일을 제외하려면 폴더 경로를 입력하고 *.* 마스크를 사용합니다.
• 모든 파일 및 하위 폴더를 비롯한 전체 드라이브를 제외하려면*D:** 마스크를 사용합니다.
• doc 파일만 제외하려면 *.doc* 마스크를 사용합니다.
• 실행 파일 이름에 각각 다른 문자가 특정 개수 포함되어 있으며 그 중 첫 문자(예: "D")만 알고 있는 경우에는 다음 형식을 사용합니다.
D????.exe(여기서 물음표는 누락된/알 수 없는 문자를 대체함)

예
%PROGRAMFILES% 같은 시스템 변수를 사용하여 검사에서 제외할 항목을 정의할 수 있습니다.
• 이 시스템 변수를 사용하여 Program Files 폴더를 제외하려면, *%PROGRAMFILES%* 경로를 사용합니다(제외 항목에 추가할 때 경로 끝에 백슬래시를 붙여야 합니다).
• *%HOMEDRIVE%* 하위 디렉토리에 있는 모든 파일을 제외하려면 *%HOMEDRIVE%\Excluded_Directory*.** 경로를 사용합니다.
다음 변수를 경로 제외 형식에 사용할 수 있습니다.
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%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 이름, 경로 또는 해시를 사용하여 검사에서 개체를 제외하는 다른 방법입니다. 탐지 제외는 검사에서 파일 및 폴더를 제외하지 않습니다(예: 성능 제외). 탐지 제외는 개체가 탐지 엔진에서 탐지되고 제외 목록에 해당 규칙이 있는 경우에만 개체를 제외합니다.

탐지 기반 제외를 생성하는 가장 쉬운 방법은 **로그 파일** > 탐지에서 기존 탐지를 사용하는 것입니다. 로그 기록을 마우스 오른쪽 버튼으로 클릭하고 **제외 생성**을 클릭합니다. 그러면 미리 정의된 기준이 있는 제외 마법사가 열립니다.

탐지 제외를 수동으로 생성하려면 **편집** > **추가**(또는 기존 항목을 수정하는 경우 **편집**)를 클릭하고 다음 기준 중 하나 이상을 지정합니다(결합 가능).

경로

특정 경로(파일 또는 디렉토리)를 제외합니다. 특정 위치/파일을 찾거나 문자열을 수동으로 입력할 수 있습니다. 경로 중간에 와일드카드, 즉 별표(*)를 사용하지 마십시오. 자세한 내용은 지식베이스 문서를 참조하십시오.

> 참고
> 폴더 콘텐츠를 제외하려면 경로 끝에 별표(*)를 추가(*C:\Tools**)하는 것을 잊지 마십시오. 검사기 관점에서 볼 때 *Tools*도 파일 이름일 수 있으므로, *C:\Tools*는 제외되지 않습니다.

해시

파일 형식, 위치, 이름 또는 해당 확장자에 관계없이 지정된 해시(SHA1)에 따라 파일을 제외합니다.

탐지 이름

유효한 탐지(위협) 이름을 입력합니다. 탐지 이름만 기반으로 하여 제외를 생성하면 보안 위험이 발생할 수 있습니다. 탐지 이름과 경로를 결합하는 것이 좋습니다. 이 제외 기준은 특정 유형의 탐지에만 사용할 수 있습니다.

설명

선택적 **설명**을 추가하면 향후에 제외를 쉽게 인식할 수 있습니다.

ESET Security Management Center에는 탐지 제외 관리가 포함되어 있어 탐지 제외를 생성하고 더 많은 컴퓨터/그룹에 적용할 수 있습니다.

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

> 예
> 별표를 사용하여 경로 제외:
> *C:\Tools** - 한 폴더와 모든 폴더 콘텐츠(파일 및 하위 폴더)가 제외됨을 나타내려면 경로가 백슬래시(\)와 별표(*)로 끝나야 합니다.
> *C:\Tools*.** - *C:\Tools**와 같은 동작입니다. 즉, 재귀적으로 작동합니다.
> *C:\Tools*.dat* - 도구 폴더의 *dat* 파일을 제외함
> *C:\Tools\sg.dat* - 정확한 경로에 있는 이 특정 파일을 제외함

> 예
> 위협을 제외하려면 올바른 탐지 이름을 다음 형식으로 입력합니다.
> *@NAME=Win32/Adware.Optmedia*
> *@NAME=Win32/TrojanDownloader.Delf.QQI*
> *@NAME=Win32/Bagle.D*

예
폴더의 모든 파일을 제외하려면 폴더 경로를 입력하고 *.* 마스크를 사용합니다.
• 모든 파일 및 하위 폴더를 비롯한 전체 드라이브를 제외하려면 *D:** 마스크를 사용합니다.
• doc 파일만 제외하려면 **.doc* 마스크를 사용합니다.
• 실행 파일 이름에 각각 다른 문자가 특정 개수 포함되어 있으며 그 중 첫 문자(예: "D")만 알고 있는 경우에는 다음 형식을 사용합니다.
D????.exe(여기서 물음표는 누락된/알 수 없는 문자를 대체함)

예
%PROGRAMFILES% 같은 시스템 변수를 사용하여 검사에서 제외할 항목을 정의할 수 있습니다.
• 이 시스템 변수를 사용하여 Program Files 폴더를 제외하려면, *%PROGRAMFILES%* 경로를 사용합니다(제외 항목에 추가할 때 경로 끝에 백슬래시를 붙여야 합니다).
• *%HOMEDRIVE%* 하위 디렉토리에 있는 모든 파일을 제외하려면 *%HOMEDRIVE%\Excluded_Directory*.** 경로를 사용합니다.
다음 변수를 경로 제외 형식에 사용할 수 있습니다.
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
사용자별 시스템 변수(*%TEMP%* 또는 *%USERPROFILE%* 등) 또는 환경 변수(*%PATH%* 등)는 지원되지 않습니다.

제외 생성 마법사

권장 제외는 탐지 유형에 따라 미리 선택되어 있지만 탐지에 대한 제외 기준을 추가로 지정할 수 있습니다. **기준 변경** 클릭:

- **정확한 파일** - SHA-1 해시별로 각 파일을 제외합니다.
- **탐지** - 해당 탐지가 포함된 각 파일을 제외하도록 탐지 이름을 지정합니다.
- **경로 + 검색** - 지정된 위치에 탐지가 있는 각 파일을 제외하도록 탐지 이름과 경로(파일 이름 포함)를 지정합니다.

선택적 **설명**을 추가하면 향후에 제외를 쉽게 인식할 수 있습니다.

고급 옵션

안티스텔스 기술

운영 체제 내에 숨길 수 있는 루트킷 등의 위험한 프로그램을 검출하는 기능을 제공하는 고급 시스템입니다. 일반적인 테스트 기술로는 이러한 위험 프로그램을 검출할 수 없습니다.

AMSI

AMSI(Microsoft Antimalware Scan Interface)를 사용하여 Windows 스크립트 호스트에서 실행한 Powershell 스크립트를 검사할 수 있습니다.

자동 제외 항목

서버 애플리케이션 및 운영 체제 개발자는 대부분의 제품에 대해 중요한 작업 파일 및 폴더 집합을 악성코드 검사에서 제외할 것을 권장합니다. 악성코드 검사는 서버 성능을 저하시키고 충돌을 발생시킬 수 있으며 일부 애플리케이션이 서버에서 실행되는 것을 방해할 수도 있습니다. 제외 항목을 통해 악성코드 방지 소프트웨어 실행 시의 잠재적 충돌 위험을 최소화하고 전반적인 서버 성능을 높일 수 있습니다. ESET 서버 제품 검사에서 완전한 제외된 파일 목록을 참조하십시오.

ESET File Security는 중요한 서버 애플리케이션과 서버 운영 체제를 확인하여 제외 항목 목록에 자동으로 추가합니다. 모든 자동 제외 항목은 기본적으로 활성화됩니다. 다음 결과가 나타나는 슬라이더 막대를 사용하여 각 서버 애플리케이션 제외를 활성화/비활성화할 수 있습니다.

- 활성화되면, 중요 파일과 폴더가 검사에서 제외되는 파일 목록에 추가됩니다. 서버를 다시 시작할 때마다 시스템은 자동으로 제외 항목을 확인하고 시스템이나 애플리케이션이 변경된 경우(예: 새로운 서버 애플리케이션 설치) 목록을 업데이트합니다. 이 설정을 사용하면 권장 자동 제외 항목이 항상 적용됩니다.

- 비활성화하면 제외된 파일과 폴더가 목록에서 자동으로 제거됩니다. 수동으로 입력한 사용자 정의 제외 항목에는 영향이 없습니다.

자동 제외 항목을 식별하고 생성하기 위해 ESET File Security는 설치 폴더에 있는 전용 애플리케이션인 *eAutoExclusions.exe*를 사용합니다. 사용자가 상호 작용할 필요는 없지만, 명령줄을 사용하여 `eAutoExclusions.exe -servers`을 실행하여 시스템에서 감지된 서버 애플리케이션을 나열할 수 있습니다. 전체 구문을 표시하려면 `eAutoExclusions.exe -?`를 사용합니다.

공유 로컬 캐시

ESET 공유 로컬 캐시는 네트워크에서 중복 검사를 없애 가상화된 환경에서 성능을 향상시킵니다. 따라서 각 파일이 한 번만 검사되고 공유 캐시에 저장됩니다. 네트워크의 파일 및 폴더 검사에 대한 정보를 로컬 캐시에 저장하려면 **캐시 옵션** 스위치를 켭니다. 새로운 검사를 수행하면 ESET File Security가 캐시에서 검사된 파일을 검색합니다. 파일이 일치하면 해당 파일은 검사에서 제외됩니다.

캐시 서버 설정에는 다음 옵션이 포함되어 있습니다.

- **호스트 이름** - 캐시가 있는 컴퓨터의 이름 또는 IP 주소입니다.
- **포트** - 통신에 사용되는 포트 번호입니다(공유 로컬 캐시에 설정된 것과 같음).
- **비밀번호** - 필요한 경우 공유 로컬 캐시 비밀번호를 지정합니다.

침입이 검출됨

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

표준 동작

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

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

각 방법에서는 표준 치료 수준을 사용하며 파일을 치료하고 검역소로 옮기거나 연결을 종료합니다. 화면의 오른쪽 하단에 있는 알림 영역에 알림 창이 표시됩니다. 치료 수준 및 동작에 대한 자세한 내용은 치료를 참조하십시오.

치료 및 삭제

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

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

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

여러 위협

컴퓨터 검사 중 감염된 파일이 치료되지 않은 경우(또는 치료 수준이 **치료 안 함**으로 설정된 경우) 이러한 파일에 대한 동작을 선택할지를 묻는 경고 창이 표시됩니다. 목록의 각 위협에 대해 개별적으로 동작을 선택하거나 **나열된 모든 위협에 대한 동작 선택**을 사용하여 목록의 모든 위협에 대해 수행할 하나의 동작을 선택한 다음 **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 시스템에서 악성코드와 관련된 모든 이벤트를 검사합니다. 컴퓨터에서 모든 파일을 열거나, 생성하거나, 실행할 때 악성코드가 있는지 검사합니다. 기본적으로 시스템 시작 시 실시간 파일 시스템 보호가 시작되며 중단 없이 검사를 수행합니다. 다른 실시간 스캐너와 충돌하는 등의 특수한 경우에는 **고급 설정**(**F5** 키)의 **실시간 파일 시스템 보호** > **기본**에서 **자동으로 실시간 파일 시스템 보호 시작**을 취소하여 실시간 보호 기능을 비활성화할 수 있습니다.

미디어 검사

기본적으로 모든 미디어 유형은 잠재적 위협에 대해 검사됩니다.

- **로컬 드라이브** - 모든 시스템 하드 드라이브를 검사합니다.
- **이동식 미디어**- CD/DVD, USB 저장 장치, Bluetooth 장치 등을 검사합니다.
- **네트워크 드라이브** - 매핑된 모든 드라이브를 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 열려 있거나 파일에 접근한 경우 검사합니다.
- **파일 생성** - 파일이 생성/수정된 경우 검사합니다.
- **파일 실행** - 파일이 실행된 경우 검사합니다.
- **이동식 미디어 접근** - 이동식 저장소에 접근하는 경우 검사합니다. 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 접근이 제대로 작동하려면 ThreatSense 파라미터에서 **부트 영역/UEFI**를 활성화 상태로 유지해야 합니다.

프로세스 제외

특정 프로세스를 제외할 수 있습니다. 백업 솔루션 프로세스를 예로 들면, 이러한 제외 프로세스에 관련된 모든 파일 작업은 안전하다고 판단되어 무시되므로 백업 프로세스에서의 간섭을 최소화할 수 있습니다.

ThreatSense 파라미터

모든 유형의 미디어를 검사하는 실시간 파일 시스템 보호는 파일에 접근하는 등의 다양한 시스템 이벤트가 발생하면 트리거됩니다. 실시간 파일 시스템 보호는 새로 생성된 파일을 기존 파일과 다르게 처리하도록 구성될 수 있습니다. 예를 들면 실시간 파일 시스템 보호를 구성하여 새로 생성된 파일을 더욱 면밀히 모니터링할 수 있습니다.

실시간 보호 기능을 사용할 때 시스템 공간을 최소화하기 위해 이미 검사한 파일이 수정된 경우를 제외하고는 반복적으로 검사하지 않습니다. 각 탐지 엔진 DB 업데이트 직후에 파일을 다시 검사합니다. 이 동작은 **스마트 최적화**를 사용하여 검사됩니다. 이 **스마트 최적화**가 비활성화된 경우 모든 파일에 접근할 때마다 해당 파일이 검사됩니다. 이 설정을 수정하려면 **F5** 키를 눌러 **고급 설정**을 열고 **진단 엔진** > **실시간 파일 시스템 보호**를 확장합니다. **ThreatSense 파라미터** > **기타**를 클릭하고 **스마트 최적화 활성화**를 선택하거나 선택 취소합니다.

추가 ThreatSense 파라미터

새로 생성 및 수정한 파일에 대한 추가 ThreatSense 파라미터 또는 **실행된 파일에 대한 추가 ThreatSense 파라미터**의 세부 옵션을 수정할 수 있습니다.

ThreatSense 파라미터

ThreatSense는 복잡한 위협 검출 방법으로 구성된 기술로. 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. 또한 ThreatSense 기술은 루트킷도 제거합니다.

> 참고
> 자동 시작 파일 검사에 대한 자세한 내용은 시작 검사를 참조하십시오.

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(F5** 키) 창에서 **ThreatSense 엔진 파라미터 설정**을 클릭합니다. 각 보안 시나리오에 따라 서로 다른 구성이 필요할 수 있습니다. 이를 염두에 두고, 다음 보호 모듈에 대해 ThreatSense를 개별적으로 구성할 수 있습니다.

- Hyper-V 검사
- OneDrive 검사
- 실시간 파일 시스템 보호
- 맬웨어 검사
- 유휴 상태 검사
- 시작 검사
- 문서 보호
- 이메일 클라이언트 보호
- 웹 브라우저 보호

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 휴리스틱을 활성화하면 시스템 속도가 느려질 수 있습니다. 일반적으로 새로 생성된 파일만 이러한 방법을 사용하여 검사합니다. 따라서 컴퓨터 검사를 제외한 모든 모듈에 대해서는 기본 ThreatSense 파라미터를 변경하지 않는 것이 좋습니다.

⊟ 검사할 개체

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

MBR(마스터 부트 레코드)에 바이러스가 있는지 부트 영역을 검사합니다. Hyper-V 가상 컴퓨터의 경우 해당 디스크 MBR가 읽기 전용 모드에서 검사됩니다.

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 압축을 푸는 데 특별한 압축파일용 프로그램이 필요하지 않은 압축파일입니다.

런타임 패커

런타임 패커는 표준 압축파일 형식과 달리 실행 후에 메모리에 압축이 풀립니다. 스캐너는 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 탐지 엔진 생성 당시 존재하지 않았거나 해당 DB에서 인식하지 못한 악성 소프트웨어를 식별할 수 있다는 것입니다.

고급 휴리스틱/DNA 시그니처

고급 휴리스틱은 컴퓨터 웜 및 트로이목마 검출용으로 최적화되고 높은 수준의 프로그래밍 언어로 작성된, ESET에서 개발한 고유 휴리스틱 알고리즘으로 구성됩니다. 고급 휴리스틱을 사용하면 ESET 제품의 위협 검출 기능이 크게 향상됩니다. 시그니처는 바이러스를 안정적으로 검출 및 식별할 수 있습니다. 자동 업데이트 시스템을 통해 위협 검출 후 몇 시간 이내에 새 시그니처를 사용할 수 있습니다. 그러나 시그니처는 인식 가능한 바이러스 또는 이러한 바이러스의 약간 수정된 버전만 검출할 수 있다는 단점이 있습니다.

치료

치료 설정에 따라 감염된 파일을 치료하는 중에 실행되는 검사기 동작이 결정됩니다. 치료 수준에는 다음과 같은 세 가지가 있습니다.

치료 않음

감염된 파일을 자동으로 치료하지 않습니다. 프로그램에 표시되는 경고 창을 통해 사용자가 동작을 선택할 수 있습니다. 이 수준은 침입이 발생할 경우 수행해야 할 단계를 알고 있는 고급 사용자를 위한 것입니다.

일반 치료

침입 유형에 따라 미리 정의된 동작을 기반으로 프로그램이 감염된 파일 자동 치료 또는 제거를 시도합니다. 화면 오른쪽 아래에 있는 알림에 감염된 파일 검출 및 제거가 표시됩니다. 적절한 동작을 자동으로 선택할 수 없는 경우에는 선택 가능한 후속 동작이 제공됩니다. 미리 정의된 동작을 완료할 수 없는 경우에도 마찬가지입니다.

엄격한 치료

프로그램이 감염된 모든 파일을 치료 또는 제거합니다. 단, 시스템 파일의 경우는 예외입니다. 파일을 치료할 수 없는 경우 어떤 유형의 동작을 수행해야 하는지 사용자에게 묻습니다.

경고
압축파일에 감염된 파일이 들어 있는 경우 두 가지 옵션을 사용하여 압축파일을 처리할 수 있습니다. 기본 모드인 **일반 치료**에서는 압축파일에 포함된 모든 파일이 감염된 경우 전체 압축파일이 삭제됩니다. **엄격한 치료** 모드에서는 압축파일에 포함된 파일 중 하나 이상이 감염된 경우 압축파일의 나머지 파일 상태에 관계없이 압축파일이 삭제됩니다.

중요
Hyper-V 호스트가 Windows Server 2008 R2 SP1 에서 실행되고 있는 경우 **일반 치료** 및 **엄격한 치료**가 지원되지 않습니다. 가상 컴퓨터 디스크 검사는 읽기 전용 모드, 즉 치료 안 함 상태로 수행됩니다. 선택한 치료 수준에 관계없이 검사는 항상 읽기 전용 모드로 수행됩니다.

제외

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

기타

수동 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

이 옵션을 선택하면 로그 파일에 검사된 모든 파일(감염되지 않은 파일도 포함)이 표시됩니다.

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.

기본 개체 설정

- 기본 설정을 사용할 수 있습니다(무제한). ESET File Security에서 사용자 지정 설정은 무시합니다.

최대 개체 크기

검사할 개체의 최대 크기를 정의합니다. 그러면 지정된 보호 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)

개체를 검사하는 최대 시간 값을 정의합니다. 여기에 사용자 정의 값을 입력한 경우 해당 시간이 지나면 검사 완료 여부에 관계없이 보호 모듈이 개체 검사를 중지합니다. 기본값은 제한 없음입니다.

압축파일 검사 설정

압축파일 검사 설정을 수정하려면 **기본 압축파일 검사 설정**을 선택 취소합니다.

다중 압축 수준

최대 압축파일 검사 수준을 지정합니다. 기본값은 10입니다. 사서함 전송 보호에서 검출된 개체의 경우 실제 다중 압축 수준은 +1입니다. 이메일의 압축 첨부 파일이 최상위 수준으로 간주되기 때문입니다.

> 예
> 다중 압축 수준이 3으로 설정된 경우 다중 압축 수준이 3인 압축파일은 전송 계층에서 실제 수준 2까지만 검사됩니다. 따라서 사서함 전송 보호에서 압축 파일을 수준 3까지 검사하려면 **다중 압축 수준** 값을 4로 설정하십시오.

압축파일 내 파일의 최대 크기

이 옵션을 사용하면 검사할 압축파일에 포함된 파일의 최대 파일 크기(압축 해제 시)를 지정할 수 있습니다. 기본값은 제한 없음입니다.

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

추가 ThreatSense 파라미터

새로 생성한 파일과 수정한 파일에 대한 추가 ThreatSense 파라미터

새로 생성하거나 수정한 파일은 기존 파일보다 비교적 감염 가능성이 높습니다. 이러한 이유 때문에 프로그램에서 추가 검사 파라미터로 이러한 파일을 검사합니다. 일반적인 시그니처 기반 검사 방법과 함께, 모듈 업데이트가 공개되기 전에 새 위협을 검출할 수 있는 고급 휴리스틱도 사용됩니다. 새로 생성된 파일 외에 자체 압축 해제 파일(.sfx) 및 런타임 패커(내부적으로 압축된 실행 파일)에 대해 검사가 수행됩니다. 기본적으로 압축파일은 최대 10번째 다중 압축 수준까지 검사되며, 실제 크기에 관계없이 검사됩니다. 압축파일 검사 설정을 수정하려면 **기본 압축파일 검사 설정**을 비활성화합니다.

실행된 파일에 대한 추가 ThreatSense 파라미터

파일이 실행될 때는 기본적으로 고급 휴리스틱이 사용됩니다. 활성화된 경우 스마트 최적화 및 ESET LiveGrid®를 활성화된 상태로 유지하여 시스템 성능에 미치는 영향을 완화하는 것이 좋습니다.

검사에서 제외된 파일 확장명

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로, 파일 형식을 정의합니다. 일반적으로 모든 파일을 검사합니다. 그러나 특정 확장명이 포함된 파일을 제외해야 하는 경우 ThreatSense 파라미터 설정을 통해 해당 확장자를 기준으로 검사에서 파일을 제외할 수 있습니다. 제외는 특정 파일 형식을 검사할 때 애플리케이션이 제대로 실행되지 않는 경우에 유용할 수 있습니다.

예
목록에 새 확장명을 추가하려면 **추가**를 클릭합니다. 텍스트 필드에 확장명을 입력(예: `tmp`)하고 **확인**을 클릭합니다. **여러 값 입력**을 선택하면 여러 파일 확장명을 줄, 쉼표 또는 세미콜론으로 분리하여 추가할 수 있습니다(예: 드롭다운 메뉴에서 **세미콜론**을 분리 기호로 선택하고 `edb;eml;tmp` 입력).
특수 기호 ?(물음표)를 사용할 수 있습니다. 물음표는 임의의 기호(예: `?db`)를 나타냅니다.

참고
Windows 운영 체제에 있는 모든 파일의 확장명(파일 형식)을 표시하려면 **제어판** > **폴더 옵션** > **보기**의 **알려진 파일 형식의 확장명 숨기기**를 선택 취소합니다.

프로세스 제외

프로세스 제외 기능을 사용하면 악성코드 방지 접근 시 검사에서만 애플리케이션 프로세스를 제외할 수 있습니다. 전용 서버(애플리케이션 서버, 저장소 서버 등)의 주요 역할로 인해 문제가 발생할 경우 적시에 복구하려면 정기적인 백업이 필수입니다. 백업 속도를 높이기 위해 백업하는 동안 파일 수준 악성코드 보호와 충돌한다고 알려진 일부 기술, 서비스 가용성 및 프로세스 무결성이 사용됩니다. 가상 컴퓨터를 실시한 마이그레이션할 때에도 비슷한 문제가 발생할 수 있습니다. 이러한 문제를 방지할 수 있는 유일하게 효과적인 방법은 악성코드 방지 소프트웨어를 비활성화하는 것입니다. 특정 프로세스(예: 백업 솔루션 프로세스)를 제외하면 해당 제외 프로세스에 관련된 모든 파일 작업이 안전하다고 판단되어 무시되므로, 백업 프로세스

에서의 간섭을 최소화할 수 있습니다. 제외를 생성할 때에는 주의하는 것이 좋습니다. 제외된 백업 도구는 경고를 트리거하지 않고 감염 파일에 접근할 수 있습니다. 이러한 문제 때문에 실시간 보호 모듈에서만 확장된 권한이 허용됩니다.

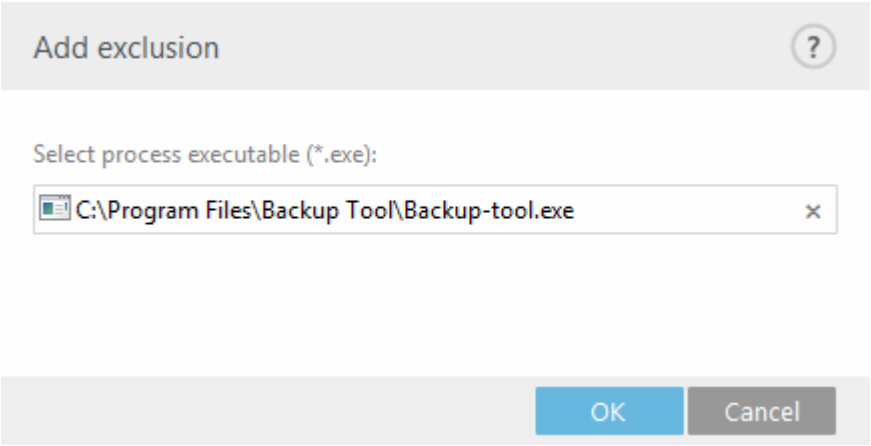
프로세스 제외를 통해 잠재적인 충돌 위험을 최소화하고 제외된 애플리케이션의 성능을 향상시켜 운영 체제의 전반적인 성능 및 안정성에 긍정적인 효과를 가져다줄 수 있습니다. 프로세스/애플리케이션을 제외하면 실행 파일(*.exe*)이 제외됩니다.

고급 설정(**F5** 키) > **진단 엔진** > **실시간 파일 시스템 보호** > **기본** > **프로세스 제외** 또는 기본 메뉴 **도구** > **실행 중인 프로세스**에서 실행 중인 프로세스 목록을 사용하여 제외된 프로세스 목록에 실행 파일을 추가할 수 있습니다.

이 기능은 백업 도구를 제외하도록 설계되었습니다. 검사에서 백업 도구의 프로세스를 제외하면 시스템 안정성이 보장될 뿐만 아니라, 백업이 실행되는 동안 백업 속도가 저하되지 않아 백업 성능에 영향을 주지 않습니다.

예
제외 항목을 **추가**하고 검사에서 제외할 실행 파일(예: *Backup-tool.exe*)을 찾을 수 있는 **프로세스 제외** 관리 창을 열려면 편집을 클릭합니다.
.exe 파일이 제외에 추가되는 즉시 이 프로세스의 활동이 ESET File Security에서 모니터링되지 않고 이 프로세스에서 수행되는 모든 파일 작업에 대해 검사가 수행되지 않습니다.

중요
프로세스 실행 파일을 선택할 때 찾아보기 기능을 사용하지 않는 경우 실행 파일의 전체 경로를 수동으로 입력해야 합니다. 그렇지 않으면 제외 기능이 올바로 작동하지 않고 HIPS에서 오류를 보고할 수 있습니다.



또한 기존 프로세스를 **편집**하거나 제외에서 이를 **제거**할 수 있습니다.

참고
웹 브라우저 보호에는 이 제외가 적용되지 않습니다. 따라서 웹 브라우저의 실행 파일을 제외해도 다운로드된 파일이 계속해서 검사됩니다. 이 경우 침입도 계속 검출할 수 있습니다. 이 시나리오는 단지 예제로 제공되며, 웹 브라우저의 제외를 생성하지 않는 것이 좋습니다.

클라우드 기반 보호

ESET LiveGrid®는 여러 클라우드 기반 기술로 구성된 고급 조기 경보 시스템으로, 평판을 기반으로 최근 발생한 위협을 감지하고 허용 목록을 통해 검사 성능을 향상시킵니다. 새 위협 정보가 클라우드에 실시간으로 스트리밍되기 때문에 ESET 악성코드 연구소에서 적절한 조치와 일관된 보호를 항상 제공할 수 있습니다. 사용자는 ESET LiveGrid®에서 제공되는 추가 정보로 프로그램 인터페이스나 오른쪽 마우스 버튼 메뉴에서 직접 실행 중인 프로세스와 파일에 대한 평판을 확인할 수 있습니다.

ESET File Security를 설치할 때 다음 옵션 중 하나를 선택합니다.

- ESET LiveGrid®를 활성화하지 않도록 설정할 수 있습니다. 소프트웨어에서 손실되는 기능은 없지만 경우에 따라 ESET File Security가 탐지 엔진 DB 업데이트보다 새로운 위협에 더 느리게 대응할 수 있습니다.

- 새로운 위협, 위협이 되는 새 코드가 감지된 위치에 대한 익명 정보를 전송하도록 ESET LiveGrid®를 구성할 수 있습니다. 자세한 분석을 위해 이 파일을 ESET으로 전송할 수 있습니다. 이러한 위협에 대한 연구를 바탕으로 ESET은 위협 검출 기능을 업데이트합니다.

ESET LiveGrid®는 새로 감지된 위협과 관련된 사용자의 컴퓨터 정보를 수집합니다. 이 정보에는 위협이 나타난 파일의 샘플 또는 복사본, 해당 파일의 경로, 파일 이름, 날짜 및 시간, 해당 위협이 사용자 컴퓨터에 나타난 과정, 사용자 컴퓨터의 운영 체제 관련 정보가 포함될 수 있습니다.

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

ESET LiveGrid® 평판 시스템 활성화(권장)

ESET LiveGrid® 평판 시스템은 검사한 파일을 클라우드의 허용 목록 및 차단 목록 항목에 있는 DB와 비교하여 ESET 악성코드 방지 솔루션의 효율성을 향상시킵니다.

ESET LiveGrid® 피드백 시스템 활성화

추가 분석을 위해 ESET 연구소로 데이터가 전송됩니다.

충돌 보고서 및 분석 데이터 전송

충돌 보고서, 모듈 또는 메모리 덤프와 같은 데이터를 전송합니다.

익명 통계 전송

ESET은 새로 검색된 위협(위협 이름, 검색 날짜 및 시간, 검색 방법과 관련 메타데이터), 검사된 파일(해시, 파일 이름, 파일 출처, 원격측정), 차단된 감염 의심 URL, 제품 버전 및 시스템 정보를 포함한 구성 등의 정보를 수집할 수 있습니다.

담당자 이메일(옵션)

감염 의심 파일과 함께 담당자 이메일을 제공하여 분석을 위해 추가 정보가 필요한 경우 연락을 받을 수 있습니다. 추가 정보가 필요하지 않으면 ESET에서 회신이 발송되지 않습니다.

샘플 전송

감염된 샘플 자동 전송

감염된 모든 샘플이 분석 및 향후 검색 개선을 위해 ESET으로 전송됩니다.

- 감염된 모든 샘플
- 문서를 제외한 모든 샘플
- 전송하지 않음

감염 의심 샘플 자동 전송

위협이 있는 것으로 보이는 감염 의심 샘플 및/또는 비정상적인 특징이나 동작이 있는 샘플은 분석을 위해 ESET으로 전송됩니다.

- **실행 파일** - *.exe, .dll, .sys* 등의 실행 파일을 포함합니다.
- **압축파일** - *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab* 등의 압축파일 유형을 포함합니다.
- **스크립트** - *.bat, .cmd, .hta, .js, .vbs, .js, .ps1* 등의 스크립트 파일 유형을 포함합니다.
- **기타** - *.jar, .reg, .msi, .swf, .lnk* 등의 파일 유형을 포함합니다.
- **스팸 의심 이메일** - 스팸의 전체 검색 기능이 향상됩니다.
- **문서** - Microsoft Office 문서 또는 액티브 콘텐츠가 있는 PDF를 포함합니다.

제외

ESET LiveGrid®에서 제외 옆에 있는 편집 옵션을 클릭하여 위협을 분석하기 위해 ESET 바이러스 연구소로 전송하는 방식을 구성할 수 있습니다.

샘플의 최대 크기(MB)

검사할 샘플의 최대 크기를 정의합니다.

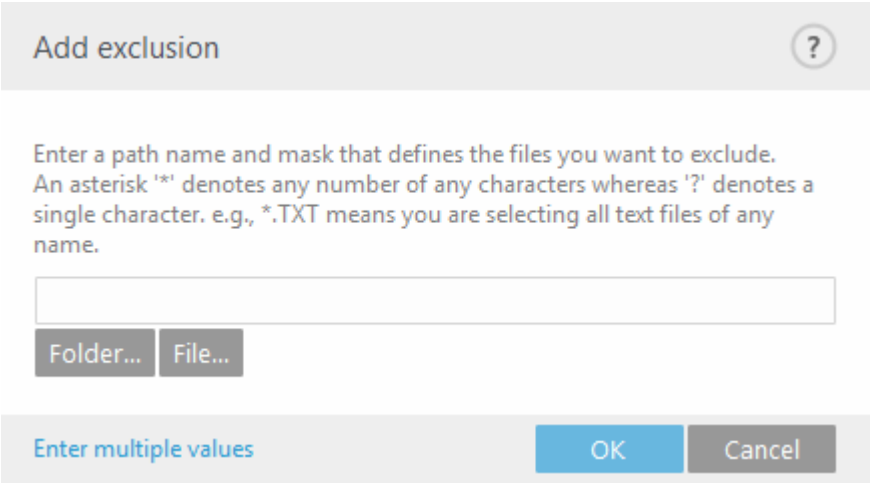
ESET Dynamic Threat Defense

클라이언트 컴퓨터에서 ESMC 웹 콘솔을 이용하여 ESET Dynamic Threat Defense 서비스를 활성화하려면, ESET Security Management Center 웹 콘솔에서 새 정책을 생성하거나 기존 정책을 편집한 후 ESET Dynamic Threat Defense를 사용하려는 컴퓨터에 할당합니다.

제외 필터

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

ESET LiveGrid®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.



감염 의심 파일을 발견하는 경우 파일을 당사 위협 연구소로 보내 분석할 수 있습니다. 해당 파일이 악성 애플리케이션이라면 이 검출 사항이 다음 검색 모듈 업데이트에 추가됩니다.

맬웨어 검사

이 섹션에서는 검사 파라미터를 선택할 수 있는 옵션을 제공합니다.

> 참고
> 이 검사 프로필 선택기는 **수동 검사**와 Hyper-V 검사, OneDrive 검사에 적용됩니다.

선택한 프로필

특정 파라미터 집합은 수동 스캐너에서 사용됩니다. 미리 정의된 검사 프로필 중 하나를 사용하거나, 새 프로필을 생성할 수 있습니다. 검사 프로필은 다른 ThreatSense 엔진 파라미터를 사용합니다.

프로필 목록

새 프로필을 생성하려면 **편집**을 클릭합니다. 프로필 이름을 입력하고 **추가**를 클릭합니다. 새 프로필이 기존 검사 프로필이 나열되는 **선택한 프로필** 드롭다운 메뉴에 표시됩니다.

검사 대상

특정 대상을 검사하려면 **편집**을 클릭하고 드롭다운 메뉴에서 옵션을 선택하거나, 폴더(트리) 구조에서 특정 대상을 선택합니다.

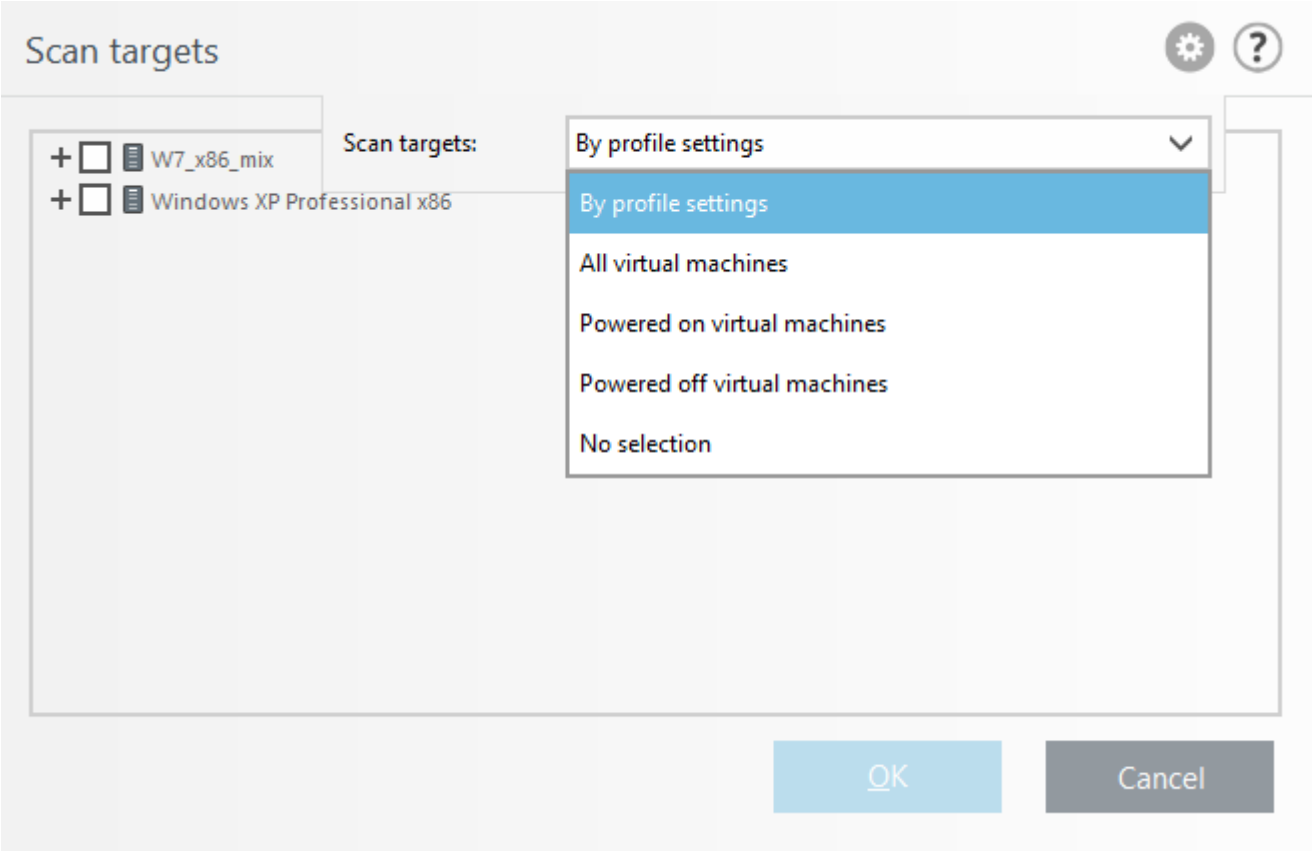
ThreatSense 파라미터

수동 컴퓨터 검사의 검사 파라미터를 수정합니다.

수동 및 머신 러닝 보호

보고는 탐지 엔진과 머신 러닝 구성 요소에 의해 수행됩니다.

Hyper-V 검사 팝업 창:



Hyper-V 검사 대상 드롭다운 메뉴에서 미리 정의된 검사 대상을 선택할 수 있습니다.

프로필 설정으로	선택한 검사 프로필에 설정된 대상을 선택합니다.
모든 가상 컴퓨터	모든 가상 컴퓨터를 선택합니다.
전원이 켜져 있는 가상 컴퓨터	온라인 상태인 모든 가상 컴퓨터를 선택합니다.
전원이 꺼져 있는 가상 컴퓨터	오프라인 상태인 모든 가상 컴퓨터를 선택합니다.

프로필 설정으로	선택한 검사 프로필에 설정된 대상을 선택합니다.
선택 안 함	선택한 모든 항목을 지웁니다.

검사를 클릭하면 설정한 사용자 지정 파라미터로 검사를 실행할 수 있습니다. 모든 검사가 완료되면 **로그 파일** > Hyper-V 검사를 확인합니다.

프로필 관리자

검사 프로필 드롭다운 메뉴에서 미리 정의된 검사 프로필을 선택할 수 있습니다.

- **스마트 검사**
- **오른쪽 마우스 버튼 메뉴 검사**
- **상세 검사**
- **내 프로필**(Hyper-V 검사, 프로필 업데이트 및 OneDrive 검사에 적용)

필요에 맞게 검사 프로필을 생성하려면 ThreatSense 엔진 파라미터 설정 섹션에서 검사 설정의 각 파라미터 설명을 참조하십시오.

프로필 관리자는 ESET File Security 내 세 가지 위치에서 사용됩니다.

수동 검사

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.

업데이트

프로필 편집기를 사용하여 새 프로필 업데이트를 생성할 수 있습니다. 컴퓨터에서 여러 가지 방법으로 업데이트 서버에 연결하는 경우 사용자 지정 업데이트 프로필을 생성하기만 하면 됩니다.

Hyper-V 검사

새 프로필을 생성하려면 **프로필 목록** 옆의 **편집**을 선택합니다. 새 프로필이 기존 검사 프로필이 나열되는 **선택한 프로필** 드롭다운 메뉴에 표시됩니다.

OneDrive 검사

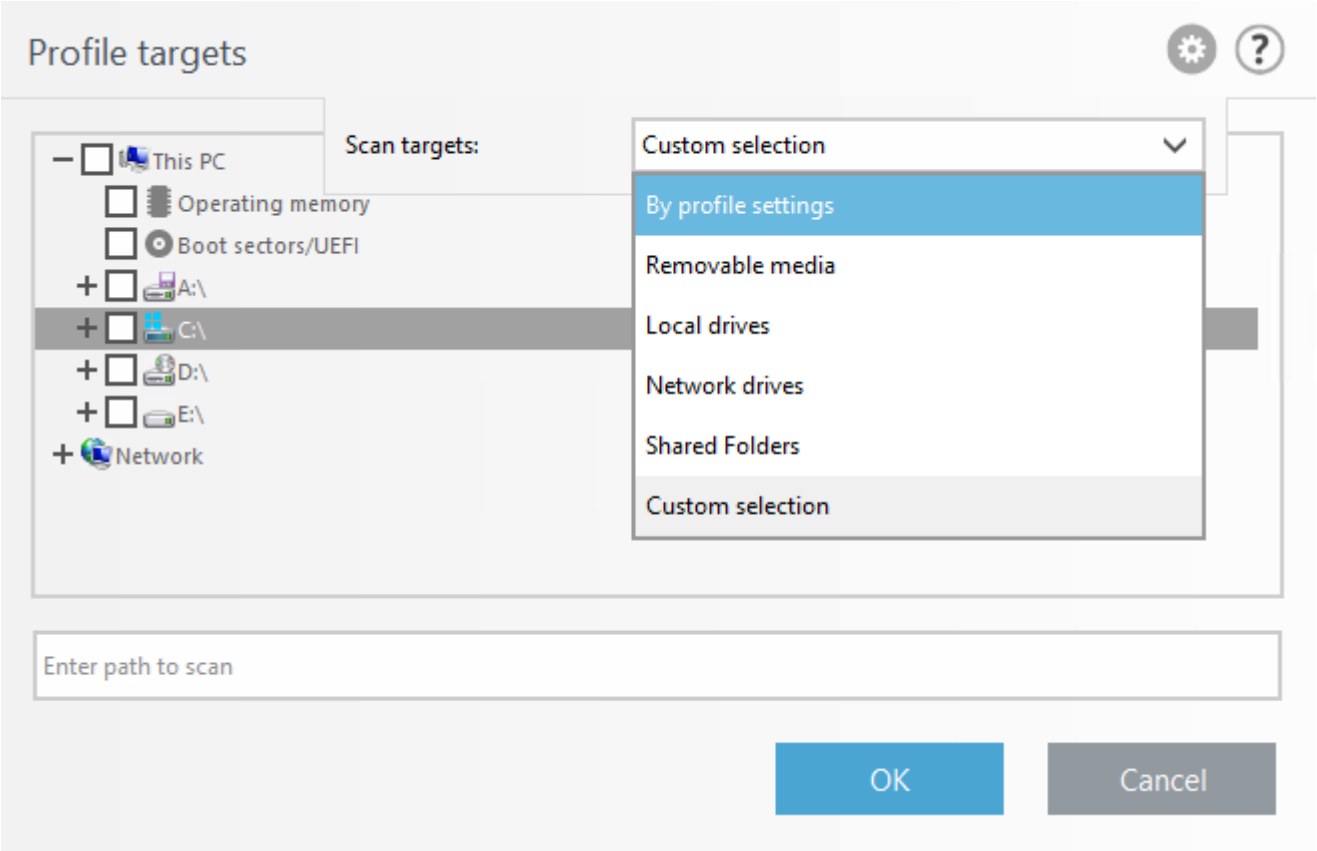
새 프로필을 생성하려면 **프로필 목록** 옆의 **편집**을 선택합니다. 새 프로필이 기존 검사 프로필이 나열되는 **선택한 프로필** 드롭다운 메뉴에 표시됩니다.

프로필 대상

침입을 검사할 대상을 지정할 수 있습니다. 시스템에서 사용 가능한 대상을 모두 나열하는 트리 구조에서 개체(메모리, 부트 영역과 UEFI, 드라이브, 파일과 폴더 또는 네트워크)를 선택합니다.

> 참고
> 이 검사 프로필 선택기는 **수동 검사**와 Hyper-V 검사, OneDrive 검사에 적용됩니다.

검사 대상과 **검사 프로필** 드롭다운 메뉴에 접근하려면 왼쪽 상단에 있는 톱니바퀴 아이콘을 클릭합니다.



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

프로필 설정으로	선택한 검사 프로필에 설정된 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.
공유 폴더	로컬 서버에서 공유되는 모든 폴더를 선택합니다.
사용자 지정 선택	선택한 모든 항목을 지웁니다. 지워진 이후 사용자 지정 선택이 가능합니다.

검사에 대상을 포함하기 위해 검사 대상(파일 또는 폴더)으로 빠르게 이동하려면 트리 구조 아래의 텍스트 필드에 해당 경로를 입력합니다. 경로 입력 시 대소문자를 구분합니다.

검사 프로필 드롭다운 메뉴에서 미리 정의된 검사 프로필을 선택할 수 있습니다.

- **스마트 검사**
- **오른쪽 마우스 버튼 메뉴 검사**
- **상세 검사**

다양한 ThreatSense 엔진 파라미터를 사용하는 프로필을 검사합니다.

검사 진행률 표시

추가 치료 동작 없이 시스템을 검사만 하려면 **치료하지 않고 검사**를 선택합니다. 이 옵션은 감염된 항목이 있는지를 대략적으로 파악하고, 있는 경우에만 이러한 감염에 대한 자세한 정보를 보려는 경우에 유용합니다. **설정** > **ThreatSense 파라미터** > **치료**를 클릭하여 세 가지 치료 수준 중에서 선택할 수 있습니다. 검사에 대한 정보가 검사 로그에 저장됩니다.

제외 무시

제외 무시를 선택하면, 무시하지 않으면 적용될 예외를 무시하면서 검사를 수행할 수 있습니다.

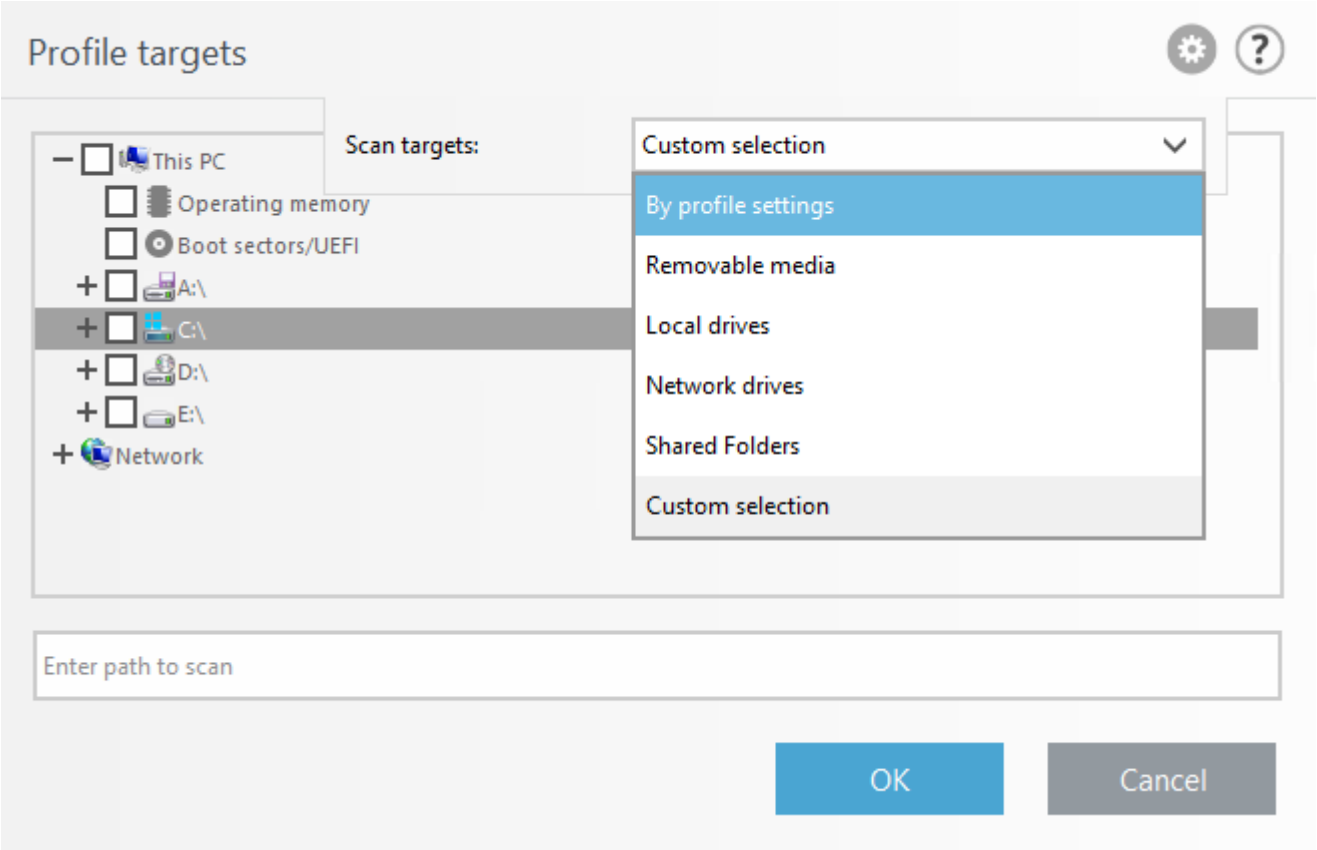
검사 대상

특정 대상만 검사하려면 **사용자 지정 검사**를 사용하여 **검사 대상** 드롭다운 메뉴에서 옵션을 선택하거나 폴더(트리) 구조에서 특정 대상을 선택하면 됩니다.

검사 대상 프로필 선택기의 적용 대상은 다음과 같습니다.

- 수동 검사
- Hyper-V 검사
- OneDrive 검사

검사 대상으로 신속하게 이동하거나 새 대상 파일이나 폴더를 추가하려면 폴더 목록 아래의 빈 필드에 해당 대상을 입력합니다. 단, 트리 구조 나열에서 선택된 대상이 없고 **검사 대상** 메뉴가 **선택 안 함**으로 설정된 경우에만 입력할 수 있습니다.



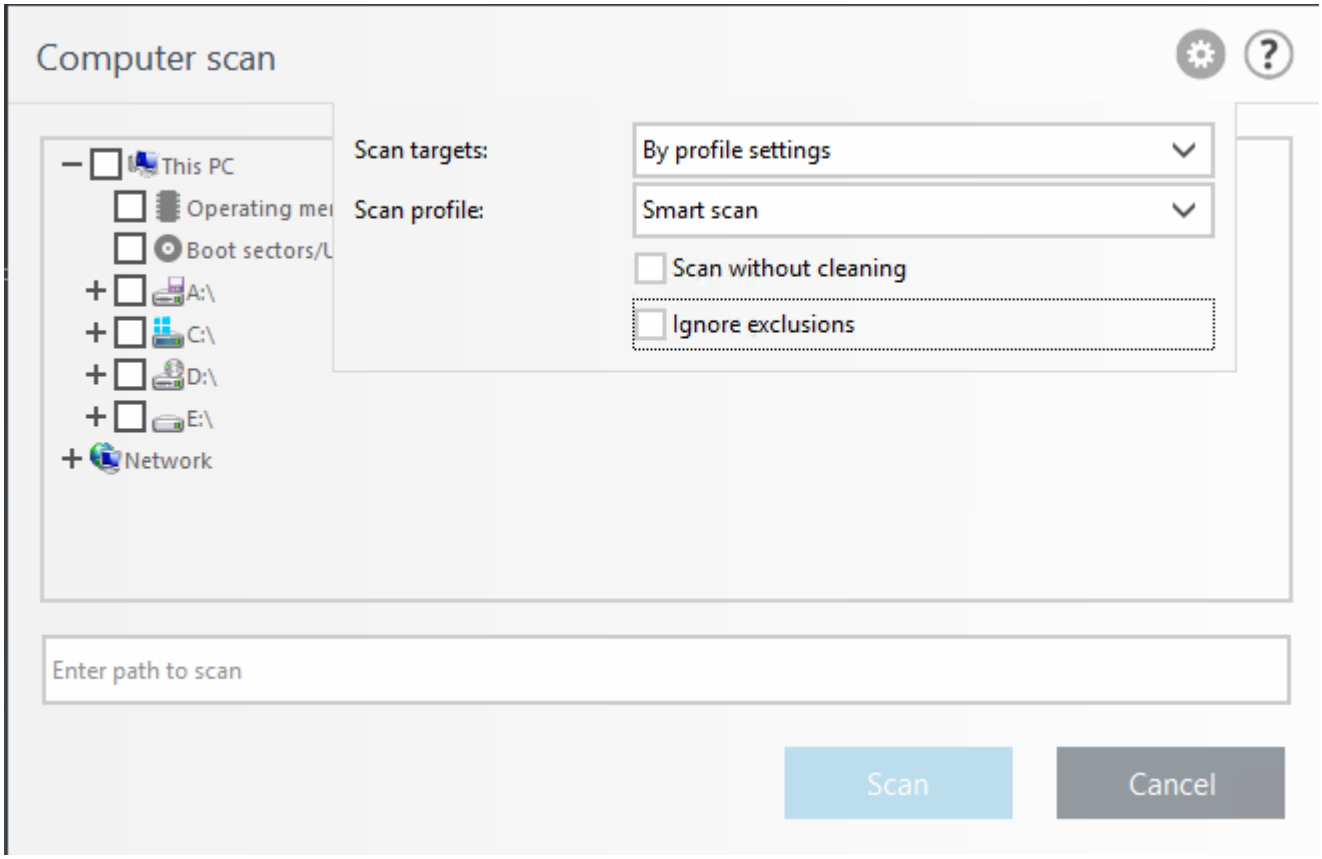
검사 대상 드롭다운 메뉴에서 미리 정의된 검사 대상을 선택할 수 있습니다.

프로필 설정으로	선택한 검사 프로필에 설정된 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.
공유 폴더	로컬 서버에서 공유되는 모든 폴더를 선택합니다.
사용자 지정 선택	선택한 모든 항목을 지웁니다. 지워진 이후 사용자 지정 선택이 가능합니다.

검사 프로필 드롭다운 메뉴에서 선택한 대상 검사에 사용할 프로필을 선택할 수 있습니다. 기본 프로필은

스마트 검사입니다. **상세 검사**와 **오른쪽 마우스 버튼 메뉴 검사**의 두 가지 검사 프로필이 추가로 미리 정의되어 있습니다. 이러한 검사 프로필은 다른 여러 가지 ThreatSense 엔진 파라미터를 사용합니다.

사용자 지정 검사 팝업 창:



검사 진행률 표시

추가 치료 동작 없이 시스템을 검사만 하려면 **치료하지 않고 검사**를 선택합니다. 이 옵션은 감염된 항목이 있는지를 대략적으로 파악하고, 있는 경우에만 이러한 감염에 대한 자세한 정보를 보려는 경우에 유용합니다. **설정** > **ThreatSense 파라미터** > **치료**를 클릭하여 세 가지 치료 수준 중에서 선택할 수 있습니다. 검사에 대한 정보가 검사 로그에 저장됩니다.

제외 무시

무시하지 않으면 적용되는 제외를 무시하면서 검사를 수행할 수 있습니다.

검사

설정한 사용자 지정 파라미터로 검사를 실행할 수 있습니다.

관리자로 검사

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

유휴 상태 검사

컴퓨터가 유휴 상태이면 모든 로컬 드라이브에서 자동 컴퓨터 검사가 수행됩니다. **유휴 상태 검색**은 컴퓨터가 다음 상태일 때 실행됩니다.

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

컴퓨터의 전원이 배터리로 공급되더라도 실행

기본적으로 컴퓨터(노트북)가 배터리 전원으로 작동될 때에는 유휴 상태 검사기가 실행되지 않습니다.

로깅 활성화

로그 파일 섹션(기본 프로그램 창에서 로그 파일을 클릭하고 드롭다운 메뉴에서 컴퓨터 검사 로그 유형 선택)에서 컴퓨터 검사를 기록할 수 있습니다.

ThreatSense 파라미터

유휴 상태 스캐너의 검사 파라미터를 수정합니다.

시작 검사

기본적으로 자동 시작 파일 검사는 시스템을 시작할 때(사용자 로그온)와 모듈을 업데이트한 후에 수행됩니다. 이 검사는 스케쥴러 구성 및 작업에서 검사됩니다.

시작 검사 옵션은 **시스템 시작 파일 검사** 스케쥴러 작업의 일부입니다.

시작 검사 설정을 수정하려면 **도구** > **스케쥴러**로 이동하여 **자동 시작 파일 검사**(사용자 로그온 또는 모듈 업데이트)라는 이름의 작업 중 하나를 선택하고 **편집**을 클릭합니다. 마법사를 계속 클릭하여 마지막 단계에서 자동 시작 파일 검사의 세부 옵션을 수정할 수 있습니다.

자동 시작 파일 검사

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

검사 대상 드롭다운 메뉴는 시스템 시작 시 실행되는 파일에 대한 검사 수준을 지정합니다. 파일은 다음 기준에 따라 오름차순으로 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 검사 대상 그룹도 포함됩니다:

사용자 로그온 전에 실행된 파일

사용자가 로그인하지 않은 상태에서도 접근할 수 있는 위치의 파일을 포함합니다(서비스, 브라우저 헬퍼 개체, winlogon 알림, Windows 스케쥴러 항목, 알려진 dll 등 포함).

사용자 로그온 후에 실행된 파일

사용자가 로그인한 후에만 접근할 수 있는 위치의 파일을 포함합니다(특정 사용자만 실행하는 파일, 일반적으로 *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*의 파일 포함).

앞서 언급한 각 그룹에 대해 검사할 파일 목록은 정해져 있습니다.

검사 순위

검사 시작 시기를 결정하는 데 사용되는 우선 순위는 다음과 같습니다.

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

이동식 미디어

ESET File Security는 자동 이동식 미디어(CD/DVD/USB) 검사 기능을 제공합니다. 이 모듈을 통해 넣은 미디어를 검사할 수 있습니다. 이 모듈은 컴퓨터 관리자가 원치 않는 콘텐츠가 포함된 이동식 미디어를 사용자가 넣지 못하도록 하려는 경우 유용할 수 있습니다.

이동식 미디어를 연결 후 수행할 동작

이동식 미디어 장치를 컴퓨터에 연결할 때 수행할 기본 동작을 선택합니다(CD/DVD/USB).

- **검사 안 함** - 아무런 동작이 수행되지 않으며 **새 장치가 검색됨** 창이 닫힙니다.
- **자동 장치 검사** - 넣은 이동식 미디어 장치에 대한 수동 검사가 수행됩니다.
- **검사 옵션 표시** - 이동식 미디어 설정 섹션을 엽니다.

이동식 미디어를 삽입하면 다음 대화 상자가 표시됩니다.

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

또한 ESET File Security는 지정된 컴퓨터에서 외부 장치 사용 규칙을 정의할 수 있는 장치 제어 기능을 제공합니다. 장치 제어에 대한 자세한 내용은 장치 제어 섹션에서 확인할 수 있습니다.

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 대용량 Microsoft Office 문서를 열 때 시스템의 성능을 향상시키기 위해 비활성화할 수 있습니다.

시스템으로 통합

이 옵션은 Microsoft Office 문서의 보호를 강화합니다(정상 상황에서는 필요하지 않음).

ThreatSense 파라미터

문서 보호 파라미터를 수정합니다.

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

Hyper-V 검사

현재 Hyper-V 검사 버전은 온라인 또는 오프라인 상태의 Hyper-V 가상 컴퓨터에 대한 검사를 지원합니다. 호스트된 Windows Hyper-V 컴퓨터와 가상 컴퓨터의 상태에 따라 지원되는 검사 유형이 여기에 표시됩니다.

Hyper-V 기능을 갖춘 가상 컴퓨터	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V
온라인 VM	검사 안 함	읽기 전용	읽기 전용	읽기 전용	읽기 전용
오프라인 VM	읽기 전용/치료	읽기 전용/치료	읽기 전용/치료	읽기 전용/치료	읽기 전용/치료

하드웨어 요구 사항

서버에 가상 컴퓨터 실행과 관련한 성능 문제가 없어야 합니다. 활동 검사는 주로 CPU 리소스를 사용합니다. 온라인으로 VM을 검사하려면 사용 가능한 디스크 공간이 있어야 합니다. 디스크 공간은 검사점/스냅숏 및 가상 디스크에서 사용하는 공간의 두 배 이상이어야 합니다.

특정 제한 사항

- 동적 디스크의 특성 때문에 RAID 저장소 검사, 검사된 볼륨 및 동적 디스크는 지원되지 않습니다. 따라서 가능한 경우 VM에서는 동적 디스크 유형을 사용하지 않는 것이 좋습니다.
- 검사는 항상 최신 VM에서 수행되며 검사점/스냅숏에는 영향을 주지 않습니다.
- 클러스터의 호스트에서 실행되는 Hyper-V는 현재 ESET File Security에서 지원되지 않습니다.
- Windows Server 2008 R2 SP1에서 실행되는 Hyper-V 호스트의 가상 컴퓨터는 ThreatSense 파라미터에서 선택한 치료 수준에 관계없이 읽기 전용 모드(치료 안 함)에서만 검사될 수 있습니다.

참고
ESET Security는 가상 디스크 MBR 검사를 지원하지만 이러한 대상에 지원되는 검사 방법은 읽기 전용 검사뿐입니다. 이 설정은 **고급 설정(F5 키)** > **진단 엔진** > **Hyper-V 검사** > ThreatSense 파라미터 > **부트 영역**에서 변경할 수 있습니다.

검사할 가상 컴퓨터가 "오프라인"임 - 꺼짐 상태로 전환

ESET File Security는 Hyper-V 관리를 사용하여 가상 디스크를 검색하고 연결합니다. 이러한 방식으로 ESET File Security에서는 일반 드라이브의 데이터 및 파일에 접근하는 경우와 동일한 방식으로 가상 디스크의 내용에 접근합니다.

검사할 가상 컴퓨터가 "온라인"임 - 실행 중, 일시 중지됨, 저장됨 상태

ESET File Security는 Hyper-V 관리를 사용하여 가상 디스크를 검색합니다. 이러한 디스크에 대한 실제 연결은 가능하지 않습니다. 따라서 ESET File Security는 가상 컴퓨터의 검사점/스냅숏을 만든 후 해당 검사점/스냅숏에 연결합니다. 검사가 완료되면 검사점/스냅숏은 삭제됩니다. 즉, 실행 중인 가상 컴퓨터는 검사 활동의 영향을 받지 않으므로 읽기 전용 검사가 수행될 수 있습니다.

검사하는 동안 ESET File Security에서 최대 1분 동안 스냅숏이나 검사점을 생성할 수 있습니다. 더 많은 가상 컴퓨터에서 Hyper-V 검사를 실행하려는 경우에는 이 점을 고려해야 합니다.

명명 규칙

Hyper-V 검사 모듈에는 다음과 같은 명명 규칙이 사용됩니다.

```
VirtualMachineName\DiskX\VolumeY
```

여기서 X는 디스크 번호이고 Y는 볼륨 번호입니다. 예를 들면 다음과 같습니다.

```
Computer\Disk0\Volume1
```

숫자 접미사는 검색 순서를 기준으로 추가되며, 이는 VM의 디스크 관리자에 표시되는 순서와 동일합니다. 이 명명 규칙은 검사할 대상의 트리 구조 목록, 진행률 표시줄 및 로그 파일에서 사용됩니다.

검사 실행

- 수동 - 검사에 사용할 수 있는 가상 컴퓨터 및 볼륨 목록을 보려면 **Hyper-V 검사**를 클릭합니다. 검사할 가상 컴퓨터, 디스크 또는 볼륨을 선택하고 **검사**를 클릭합니다.
- 다음 방법으로 스케줄러 작업을 생성할 수 있습니다.
- 서버 검사라고 하는 클라이언트 작업인 ESET Security Management Center를 통해.
- Hyper-V 검사는 eShell을 통해 관리하고 시작할 수 있습니다.

여러 Hyper-V 검사를 동시에 실행할 수 있습니다. 검사가 완료되면 로그 파일 링크가 포함된 알림이 수신됩니다.

발생 가능한 문제

- 온라인 가상 컴퓨터 검사를 실행할 때 특정 가상 컴퓨터의 검사점/스냅숏을 생성해야 하며, 검사점/스냅숏을 생성하는 동안 가상 컴퓨터의 일반적인 동작 몇 가지가 제한되거나 비활성화될 수 있습니다.

- 오프라인 가상 컴퓨터를 검사하는 경우 검사가 완료될 때까지 가상 컴퓨터 전원을 켤 수 없습니다.
- Hyper-V Manager를 통해 두 개의 서로 다른 가상 컴퓨터의 이름을 동일하게 지정할 수 있으며, 이 경우 검사 로그를 검토하는 동안 이러한 컴퓨터를 구분할 때 문제가 발생합니다.

OneDrive 검사

기본

동작 및 검역소를 구성할 수 있습니다.

파일이 감염된 경우 수행할 작업

- **동작 없음** - 파일의 변경 사항이 적용되지 않습니다.
- **제거** - 검역소로 이동한 후 OneDrive에서 파일을 제거합니다. 그러나, OneDrive 휴지통에서 파일을 계속 사용할 수 있습니다.

감염된 파일을 검역소로 보내기

활성화된 경우 제거하도록 표시된 파일이 격리 상태로 전환됩니다. 파일이 검역소에 누적되지 않도록 이 설정을 선택 취소하여 검역소를 비활성화합니다.

고급

이 부분에는 OneDrive 검사 등록에 대한 정보(애플리케이션 ID, Azure 포털의 개체 ID, 인증서 지문)가 포함됩니다. 시간 초과 및 동시 다운로드 제한을 구성할 수 있습니다.

프로필

새 프로필을 생성하려면 **프로필 목록** 옆의 **편집**을 선택하고 자신의 **프로필 이름**을 입력한 다음 **추가**를 클릭합니다. 새 프로필은 기존 검사 프로필이 나열되는 **선택한 프로필** 드롭다운 메뉴에 표시됩니다.

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

- **프로필로** - 선택한 검사 프로필에 설정된 대상을 선택합니다.
- **모든 사용자** - 모든 사용자를 선택합니다.
- **선택 안 함** - 현재 선택을 지웁니다.

검사를 클릭하면 설정한 사용자 지정 파라미터로 검사를 실행할 수 있습니다. 모든 검사가 완료되면 **로그 파일** > OneDrive 검사를 확인합니다.

ThreatSense 파라미터

OneDrive 스캐너의 검사 파라미터를 수정합니다.

OneDrive 검사 및 머신 러닝 보호

보고는 탐지 엔진과 머신 러닝 구성 요소에 의해 수행됩니다.

HIPS

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.

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

자기 보호 활성화

ESET File Security에는 악성 소프트웨어가 악성코드 방지 기능을 손상시키거나 비활성화하지 못하도록 하는 기본 제공 자기 보호 기술이 포함되어 있으므로 시스템이 항상 보호됨을 확신할 수 있습니다. HIPS 활성화 및 SD(자기 보호) 활성화 설정에 대한 변경 내용은 Windows 운영 체제를 다시 시작한 후 적용됩니다. 전체 HIPS 시스템을 비활성화할 때에도 컴퓨터를 다시 시작해야 합니다.

보호 서비스 활성화

Microsoft는 Microsoft Windows Server 2012 R2로 보호되는 서비스 개념을 도입했습니다. 이 제품은 악성코드 공격으로부터 서버를 보호합니다. ESET File Security의 커널은 기본적으로 보호되는 서비스로 실행됩니다. 이 기능은 Microsoft Windows Server 2012 R2 이상의 서버 운영 체제에서 사용할 수 있습니다.

사용 Advanced Memory Scanner

Exploit 차단과 함께 작동하여 난독화 또는 암호화를 사용한 악성코드 방지 제품의 검색을 피하도록 설계된 악성코드로부터 보호하는 기능을 강화합니다. 고급 메모리 스캐너는 기본적으로 활성화되어 있습니다. 이 유형의 보호에 대한 자세한 내용은 용어집을 참조하십시오.

Exploit 차단 활성화

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

랜섬웨어 보호 활성화

이 기능을 사용하려면 HIPS 및 ESET Live Grid를 활성화합니다. 랜섬웨어에 대한 자세한 내용은 용어집을 참조하십시오.

필터링 모드

다음 필터링 모드 중 하나를 선택할 수 있습니다.

- **자동 모드** - 시스템을 보호하는 미리 정의된 규칙에 의해 차단된 규칙을 제외한 작업이 활성화됩니다. 규칙에 의해 차단된 동작을 제외하고 모두 허용됩니다.
- **스마트 모드** - 매우 의심스러운 이벤트에 한해 사용자에게 알림을 표시합니다.
- **대화 모드** - 사용자가 작업을 확인하는 메시지가 표시됩니다. 접근을 허용/거부하고, 규칙을 생성하

며, 이 동작을 일시적으로 저장합니다.

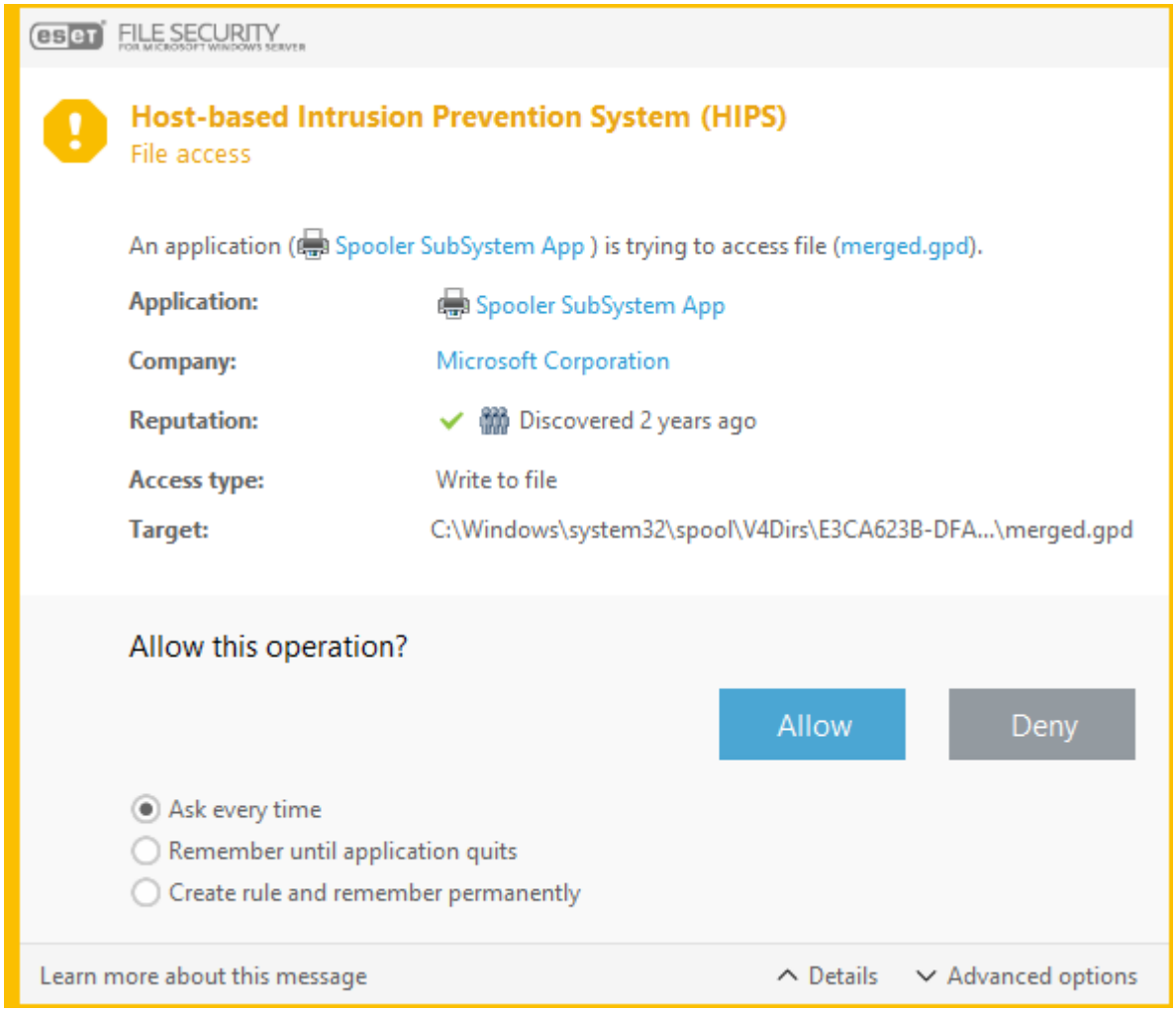
- **정책 기반 모드** - 작업이 차단됩니다. 사용자/사전 정의된 규칙만 허용됩니다.

- **학습 모드** - 작업이 활성화되고 각 작업 후 규칙이 생성됩니다. 이 모드에서 생성된 규칙은 규칙 편집에서 볼 수 있지만, 해당 순위는 수동으로 생성한 규칙이나 자동 모드에서 생성한 규칙의 순위보다 낮습니다. HIPS 필터링 모드 드롭다운 메뉴에서 **학습 모드**를 선택하면 **학습 모드 종료** 설정을 사용할 수 있게 됩니다. 학습 모드를 선택할 기간을 선택합니다(최대 기간 14일). 지정된 기간이 경과하면 HIPS에서 생성된 규칙을 편집하라는 메시지가 표시됩니다(학습 모드 상태임). 다른 필터링 모드를 선택하거나, 선택을 연기하고 학습 모드를 계속 사용할 수 있습니다.

규칙

규칙은 파일, 레지스트리 일부 또는 기타 애플리케이션에 접근할 수 있는 애플리케이션을 결정합니다. HIPS 시스템은 운영 체제 내의 이벤트를 모니터링하고 개인 방화벽에서 사용되는 규칙과 유사한 규칙에 따라 적절하게 반응합니다. HIPS 규칙 관리 창을 열려면 편집을 클릭합니다. 규칙의 기본 동작이 **확인**으로 설정된 경우 규칙이 트리거될 때마다 대화 상자 창이 표시됩니다. 여기에서 작업을 **차단**하거나 **허용**하도록 선택할 수 있습니다. 지정된 시간 내에 동작을 선택하지 않으면 규칙에 따라 새 동작이 선택됩니다.

이 대화 상자 창에서 HIPS가 검출하는 모든 새 동작을 기준으로 규칙을 생성한 다음, 해당 동작을 **허용**하거나 **차단**할 조건을 정의할 수 있습니다. **세부 정보**를 클릭하여 추가 정보를 확인합니다. 이렇게 생성된 규칙은 수동으로 생성된 규칙과 동일하게 간주되므로 대화 상자 창에서 생성한 규칙이 대화 상자 창을 트리거한 규칙보다 덜 구체적일 수 있습니다. 이는 이러한 규칙 생성 후 동일한 작업에서 같은 창을 트리거할 수 있음을 의미합니다.



매시간 확인

규칙이 트리거될 때마다 대화 상자 창이 표시됩니다. 여기에서 작업을 **차단** 또는 **허용**하도록 선택할 수 있습니다.

응용 프로그램이 종료될 때까지 저장

차단 또는 **허용** 작업을 선택하면 임시 HIPS 규칙이 생성되고 해당 애플리케이션이 닫힐 때까지 사용됩니다. 또한 필터링 모드를 변경하는 경우, 규칙을 변경하는 경우, 또는 HIPS 모듈이 업데이트되어 시스템을 다시 시작하는 경우 임시 규칙이 제거됩니다.

규칙 생성 및 영구 저장

새 HIPS 규칙을 생성합니다. 나중에 HIPS 규칙 관리 섹션에서 이 규칙을 수정할 수 있습니다.

HIPS 규칙 설정

이 창에서 기존 HIPS 규칙에 대한 개요를 확인할 수 있습니다.

규칙	사용자가 정의하거나 자동으로 선택된 규칙 이름입니다.
활성화됨	목록에서 규칙을 유지하되 사용하지 않으려면 이 스위치를 비활성화합니다.
동작	규칙은 조건이 충족되면 수행되어야 하는 동작, 즉 **허용**, **차단** 또는 **확인**을 지정합니다.
소스	애플리케이션에서 이벤트를 트리거한 경우에만 규칙이 사용됩니다.

규칙	사용자가 정의하거나 자동으로 선택된 규칙 이름입니다.
대상	작업이 특정 파일, 애플리케이션 또는 레지스트리 항목과 관련된 경우에만 규칙이 사용됩니다.
로그 심각도	이 옵션을 활성화하면 이 규칙에 대한 정보가 HIPS 로그에 기록됩니다.
알림	이벤트가 트리거되면 오른쪽 아래의 모서리에 작은 팝업 창이 나타납니다.

새 규칙을 생성하고, 새 HIPS 규칙 **추가** 또는 선택한 항목 **편집**을 클릭합니다.

규칙 이름

사용자가 정의하거나 자동으로 선택된 규칙 이름입니다.

동작

규칙은 조건을 충족하면 수행되어야 하는 **허용**, **차단** 또는 **확인** 동작을 지정합니다.

영향을 주는 작업

규칙이 적용되는 작업 유형을 선택해야 합니다. 이 유형의 작업과 선택한 대상에 한해 규칙이 사용됩니다. 규칙은 이 규칙을 트리거링하는 조건에 대해 설명하는 부분을 구성합니다.

소스 애플리케이션

이 애플리케이션에서 이벤트를 트리거한 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 애플리케이션**을 선택하고 **추가**를 클릭하여 새 파일 또는 폴더를 추가하거나, 드롭다운 메뉴에서 **모든 애플리케이션**을 선택하여 모든 애플리케이션을 추가할 수 있습니다.

> 참고
> 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 제거할 권한이 있는지 확인합니다.
파일에 작성	애플리케이션에서 대상 파일에 작성할 권한이 있는지 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 악성코드, 디스크의 정확한 복사본을 생성하려는 백업 소프트웨어 또는 디스크 볼륨을 인식하려는 파티션 관리자가 원인일 수 있습니다.
전체 후크 설치	MSDN 라이브러리에서 SetWindowsHookEx 함수에 대한 호출을 참조합니다.
드라이버 로드	시스템에 드라이버를 설치 및 로드하고 있습니다.

작업이 이 대상과 관련 있는 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 파일**을 선택하고 **추가**를 클릭하여 새 파일이나 폴더를 추가합니다. 또는 드롭다운 메뉴에서 **모든 파일**을 선택하여 모든 애플리케이션을 추가할 수 있습니다.

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(예: 키로거가 브라우저 이벤트를 캡처하려고 함).
다른 애플리케이션 종료/일시 중지	프로세스를 일시 중지하거나 다시 시작하거나 종료합니다(프로세스 탐색기 또는 프로세스 창에서 직접 접근할 수 있음).
새 애플리케이션 시작	새 애플리케이션이나 프로세스 시작.
다른 애플리케이션 상태 수정	소스 애플리케이션이 대상 애플리케이션의 메모리에 작성하려고 하거나 대신해서 코드를 실행하려고 합니다. 이 기능은 이 작업의 사용을 차단하는 규칙에서 필수 애플리케이션을 대상 애플리케이션으로 구성하여 필수 애플리케이션을 보호할 때 유용할 수 있습니다.

작업이 이 대상과 관련 있는 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 애플리케이션**을 선택하고 **추가**를 클릭하여 새 파일이나 폴더를 추가합니다. 또는 드롭다운 메뉴에서 **모든 애플리케이션**을 선택하여 모든 애플리케이션을 추가할 수 있습니다.

레지스트리 작업:

시작 설정 수정	Windows 시작 시 실행되는 애플리케이션을 정의하는 설정에 대한 모든 변경 사항입니다. 이러한 변경 사항은 예컨대 Windows 레지스트리에서 실행 키를 검색하여 확인할 수 있습니다.
레지스트리에서 삭제	레지스트리 키 또는 해당 값을 제거합니다.
레지스트리 키 이름 바꾸기	레지스트리 키 이름을 바꿉니다.
레지스트리 수정	새로운 레지스트리 키 값을 생성하거나, 기존 값을 변경하거나, DB 트리의 데이터를 이동하거나, 레지스트리 키에 대한 사용자나 그룹 권한을 설정합니다.

작업이 이 대상과 관련된 경우에만 규칙이 사용됩니다. 드롭다운 메뉴에서 **특정 항목**을 선택하고 **추가**를 클릭하여 새 파일이나 폴더를 추가합니다. 또는 드롭다운 메뉴에서 **모든 항목**을 선택하여 모든 애플리케이션을 추가할 수 있습니다.

참고
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 can mean HKEY_USER\.default\software*만, *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 포함된 레지스트리 키 경로는 "이 경로 또는 해당 기호 뒤에 있는 모든 수준의 경로"를 정의합니다. 이 방법은 파일 대상에 와일드카드를 사용하는 유일한 방법입니다. 먼저 경로의 특정 부분을 평가한 다음 와일드카드 기호(*) 뒤에 있는 경로를 평가합니다.

경고
너무 일반적인 규칙을 생성하면 알림이 수신될 수 있습니다.

HIPS 고급 설정

다음 옵션은 애플리케이션의 동작을 디버깅하고 분석하는 데 유용합니다.

드라이버 로드가 항상 허용됨

선택한 드라이버는 사용자 규칙에 따라 명백하게 차단되는 경우를 제외하고 구성된 필터링 모드에 상관없이 항상 로드할 수 있습니다. 이 목록에 표시된 드라이버는 사용자 규칙에 따라 명백하게 차단된 경우를 제외하고 HIPS 필터링 모드에 상관없이 항상 로드할 수 있습니다. 새 드라이버를 **추가**하거나, 목록에서 선택한 드라이버를 **편집** 또는 **제거**할 수 있습니다.

> 참고
> 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.

차단된 모든 작업 기록

차단된 모든 작업은 HIPS 로그에 기록됩니다.

시작 애플리케이션에서 변경사항 발생 시 알림

시스템 시작 시 애플리케이션이 추가되거나 제거될 때마다 바탕 화면 알림을 표시합니다.

업데이트 구성

이 섹션에서는 사용된 업데이트 서버와 이러한 서버의 인증 데이터 같은 업데이트 소스 정보를 지정합니다.

> 참고
> 업데이트를 제대로 다운로드하려면 모든 업데이트 파라미터를 올바르게 입력해야 합니다. 방화벽을 사용하는 경우 ESET 프로그램이 인터넷과 통신(예: HTTP 통신)할 수 있어야 합니다.

기본

기본 업데이트 프로필 선택

업데이트에 기본적으로 적용할 기존 프로필을 선택하거나 새 프로필을 생성합니다.

업데이트 캐시 지우기

업데이트 중에 문제가 발생하면 **지우기**를 클릭하여 임시 업데이트 캐시를 지웁니다.

자동으로 진단 엔진 최대 기간 설정/진단 엔진 최대 기간(일)

진단 엔진 기간이 오래된 것으로 보고되는 최대 기간(일)을 설정할 수 있습니다. 기본값은 7입니다.

모듈 롤백

진단 엔진 및/또는 프로그램 모듈의 새 업데이트가 불안정하거나 손상되었다고 의심되면 이전 버전으로 롤백한 후 설정된 기간 동안 업데이트를 비활성화할 수 있습니다. 또는 업데이트를 무기한 연기한 경

우 이전에 비활성화한 업데이트를 활성화할 수 있습니다. ESET File Security는 롤백 기능과 함께 사용하기 위해 진단 엔진 및 프로그램 모듈의 스냅숏을 기록합니다. 진단 엔진 스냅숏을 생성하려면 **모듈 스냅숏 생성이 활성화**된 상태로 둡니다.

로컬에 저장된 스냅숏 수

저장되는 이전 모듈 스냅숏의 수를 정의합니다.

프로필

사용자 지정 업데이트 프로필을 생성하려면 **프로필 목록** 옆의 **편집**을 선택하고 자신의 **프로필 이름**을 입력한 다음 **추가**를 클릭합니다. **편집할 프로필을 선택**하고 **모듈 업데이트** 유형에 대한 파라미터를 수정하고 **업데이트 미러**를 생성합니다.

업데이트

드롭다운 메뉴에서 사용할 업데이트 유형을 선택합니다.

- **정기적 업데이트** - 기본적으로 업데이트 유형은 정기적 업데이트로 설정되어 있어 업데이트 파일을 ESET 서버에서 최소 네트워크 트래픽으로 자동으로 다운로드할 수 있습니다.
- **테스트 모드** - 테스트 모드는 철저한 내부 테스트를 거친 업데이트로, 곧 일반 사용자에게 제공될 예정입니다. 최신 검출 방법 및 수정 프로그램에 접근하여 테스트 모드를 활성화하여 이 기능을 사용할 수 있습니다. 단, 테스트 모드는 항상 안정적인 상태인 것은 아니므로 최대 가용성 및 안정성이 필요한 프로덕션 서버 및 워크스테이션에서는 사용하면 안 됩니다.
- **지연된 업데이트** - 이 유형을 통해 X시간 이상 지연된 새 버전의 바이러스 DB(즉 실제 환경에서 테스트되어 안정적이라고 간주되는 DB)를 제공하는 특수 업데이트 서버에서 업데이트할 수 있습니다.

업데이트를 다운로드하기 전 확인

새 업데이트를 사용할 수 있는 경우 업데이트를 다운로드하기 전에 메시지가 표시됩니다.

업데이트 파일 크기가 다음을 초과할 경우 확인(kB)

업데이트 파일 크기가 필드에 지정된 값보다 큰 경우 알림이 표시됩니다.

성공한 업데이트에 대한 알림 비활성화

화면 오른쪽 아래의 시스템 트레이 알림을 해제합니다. 전체 화면 애플리케이션을 실행 중인 경우 이 옵션을 선택하는 것이 유용합니다. 프리젠테이션 모드는 모든 알림을 해제합니다.

모듈 업데이트

모듈 업데이트는 기본적으로 **자동으로 선택**으로 설정되어 있습니다. 업데이트 서버는 업데이트가 저장되는 위치입니다. ESET 서버를 사용할 경우 기본 옵션이 선택된 상태로 그대로 두는 것이 좋습니다.

로컬 HTTP 서버(미러라고도 함)를 사용할 때 업데이트 서버를 다음과 같이 설정해야 합니다. ***http://***컴퓨터_이름_또는_해당***_IP_***주소:2221
SSL을 사용한 로컬 HTTP 서버를 사용할 때는 업데이트 서버를 다음과 같이 설정해야 합니다. https://컴퓨터_이름_또는_해당_*IP*_주소:2221

로컬 HTTP 서버(미러라고도 함)를 사용할 때 업데이트 서버를 다음과 같이 설정해야 합니다.
http://컴퓨터_이름_또는_해당***_IP_***주소:2221

로컬 공유 폴더를 사용할 때는 업데이트 서버를 다음과 같이 설정해야 합니다.
\\컴퓨터_이름_또는_해당_*IP* 주소\공유_폴더

감지 지문의 잦은 업데이트를 활성화합니다

진단 엔진은 더 짧은 간격으로 업데이트됩니다. 이 옵션을 비활성화하면 감지 속도에 부정적인 영향을 줄 수 있습니다.

이동식 미디어에서 업데이트 허용

생성된 미러가 포함되어 있는 경우 이동식 미디어에서 업데이트합니다. **자동**이 선택된 경우 업데이트가 백그라운드에서 실행됩니다. 업데이트 대화 상자를 표시하려면 **항상 확인**을 선택합니다.

프로그램 구성 요소 업데이트

업데이트 모드 드롭다운 메뉴를 이용하여 사용 가능한 업데이트가 있을 때 ESET File Security 구성 요소 업데이트가 적용되는 방법을 선택할 수 있습니다. 구성 요소 업데이트는 일반적으로 기존 기능을 수정하지만, 새 기능도 포함할 수 있습니다. 선택한 업데이트 모드에 따라 간섭이나 확인 없이 구성 요소 업데이트를 자동으로 수행할 수 있습니다. 또는 업데이트를 설치하기 전에 알림이 표시되도록 선택할 수 있습니다. 구성 요소 업데이트 후에는 서버를 다시 시작해야 할 수도 있습니다. 선택할 수 있는 업데이트 모드는 다음과 같습니다.

- **업데이트 전 확인** - 사용 가능한 업데이트가 있을 때 제품 업데이트를 확인할지, 거부할지 묻는 메시지가 표시됩니다. 기본 옵션이며, 구성 요소 업데이트 후에는 서버를 다시 시작해야 할 수도 있습니다.
- **자동 업데이트** - 구성 요소 업데이트가 자동으로 다운로드 및 설치됩니다.
- **업데이트 안 함** - 구성 요소 업데이트가 수행되지 않습니다. 구성 요소 업데이트를 수동으로 수행하고 예약된 유지 관리 창에서 서버를 다시 시작할 수 있으므로 옵션을 권장합니다.

중요
자동 업데이트 모드에서는 구성 요소 업데이트가 완료된 후에 서버를 자동으로 다시 시작합니다.

연결 옵션

프록시 서버

지정된 업데이트 프로필에 대한 프록시 서버 설정 옵션에 접근하는 방법 **프록시 모드**를 클릭하고 다음 세 가지 옵션 중 하나를 선택합니다.

- **프록시 서버 사용 안 함** - 업데이트할 때 ESET File Security에서 프록시 서버를 사용하지 않습니다.
- **글로벌 프록시 서버 설정 사용** - **고급 설정(F5** 키)> **도구** > 프록시 서버에 지정된 프록시 서버 구성이 사용됩니다.
- **프록시 서버를 통해 연결** - 다음의 경우 이 옵션을 사용합니다.

프록시 서버를 사용하여 ESET File Security를 업데이트해야 하고 이 프록시 서버가 전체 설정(도구 > 프록시 서버)에 지정된 프록시 서버와 다른 경우. 이 경우 프록시 서버 주소, 통신 포트(기본적으로 3128) 및 필요한 경우 프록시 서버의 사용자 이름 및 비밀번호와 같은 설정을 지정해야 합니다.
프록시 서버 설정이 전체적으로 설정되어 있지 않지만 ESET File Security가 업데이트를 위해 프록시 서버에 연결하는 경우
컴퓨터가 프록시 서버를 통해 인터넷에 연결되어 있는 경우. 프로그램을 설치하는 동안 Internet Explorer에서 설정을 가져오지만 이후에 이러한 설정이 변경된 경우(예: ISP를 변경한 경우), 이 창에 나열된 HTTP 프록시 설정이 올바른지 확인하십시오. 그렇지 않으면 프로그램이 업데이트 서버에 연결할 수 없습니다.

참고
사용자 이름 및 **비밀번호**와 같은 인증 데이터는 프록시 서버에 접근하기 위한 것입니다. 사용자 이름과 비밀번호가 필요한 경우에만 이 필드에 내용을 입력합니다. 이러한 필드는 ESET File Security의 사용자 이름/비밀번호를 입력하는 곳이 아닙니다. 프록시 서버를 통해 인터넷에 접근하는 데 비밀번호가 필요한 경우에만 이 필드에 내용을 입력해야 합니다.

프록시를 사용할 수 없는 경우 직접 연결 사용

제품이 HTTP 프록시를 활용하도록 구성되어 있는데 프록시에 연결할 수 없는 경우 제품은 프록시를 우회하고 ESET 서버와 직접 통신합니다.

Windows 공유

Windows를 실행하는 로컬 서버에서 업데이트하는 경우 기본적으로 각 네트워크에 연결해야 합니다.

다음 계정으로 LAN 연결

계정을 구성하려면 다음 옵션 중 하나를 선택합니다.

- **시스템 계정(기본값)** - 인증에 시스템 계정을 사용합니다. 일반적으로 기본 업데이트 설정 섹션에 인증 데이터를 입력하지 않으면 인증 프로세스가 수행되지 않습니다.
- **현재 사용자** - 현재 로그인한 사용자 계정을 이용해 프로그램에서 인증하도록 하려면 이 옵션을 선택합니다. 이 방법은 현재 로그인한 사용자가 없는 경우 프로그램에서 업데이트 서버에 연결할 수 없다는 단점이 있습니다.
- **지정한 사용자** - 인증에 특정 사용자 계정을 사용하려면 이 옵션을 선택합니다. 기본 시스템 계정에 연결하지 못한 경우 이 방법을 사용합니다. 지정한 사용자 계정이 로컬 서버의 업데이트 파일 디렉터리에 접근할 수 있어야 합니다. 사용자에게 접근 권한이 없으면 프로그램에서 연결하여 업데이트를 다운로드할 수 없습니다.

경고
현재 사용자 또는 **지정한 사용자**가 선택되어 있는 경우 프로그램 ID를 원하는 사용자로 변경하면 오류가 발생할 수 있습니다. LAN 인증 데이터를 기본 업데이트 설정 섹션에 입력하는 것이 좋습니다. 이 업데이트 설정 섹션에서 인증 데이터는 *domain_name\user*(작업 그룹인 경우 *workgroup_name\name* 입력) 및 패스워드와 같이 입력해야 합니다. 로컬 서버의 HTTP 버전에서 업데이트하는 경우에는 인증이 필요하지 않습니다.

업데이트 후 서버 연결 끊기

업데이트를 다운로드한 후에도 서버 연결이 활성 상태로 유지되는 경우 강제로 연결을 끊습니다.

업데이트 미러

로컬 미러 서버의 구성 옵션은 **고급 설정**(**F5** 키)의 **업데이트** > **프로필** > 업데이트 미러 탭에 있습니다.

업데이트 롤백

롤백을 클릭한 경우 탐지 엔진 DB 및 프로그램 모듈 업데이트가 일시 중지되는 기간을 나타내는 시간 간격을 드롭다운 메뉴에서 선택해야 합니다.

업데이트 기능을 수동으로 복원할 때까지 정기 업데이트를 무기한 연기하려면 **취소될 때까지**를 선택합니다. 이 경우 잠재적 보안 위험이 발생하므로 이 옵션은 선택하지 않는 것이 좋습니다.

탐지 엔진 DB 버전이 사용 가능한 가장 낮은 버전으로 다운그레이드되며 로컬 컴퓨터 파일 시스템에 스냅숏으로 저장됩니다.

예약된 작업 - 업데이트

두 업데이트 서버에서 프로그램을 업데이트하려면 서로 다른 두 프로필 업데이트를 생성해야 합니다. 첫 번째 프로필로 업데이트 파일을 다운로드하지 못하면 프로그램에서 대체 프로필로 자동 전환합니다. 이는 일반적으로 로컬 LAN 업데이트 서버에서 업데이트하지만 소유자가 다른 네트워크의 인터넷에 연결하는 경우가 많은 노트북의 경우 적합합니다. 따라서 첫 번째 프로필이 실패하면 두 번째 프로필이 ESET 업데이트 서버에서 업데이트 파일을 자동으로 다운로드합니다.

예
아래 단계에서는 기존의 **정기적 자동 업데이트**를 편집하는 작업을 설명합니다.
1. 기본 **스케쥴러** 화면에서 이름이 **정기적 자동 업데이트**인 작업 **업데이트**를 선택하고 구성 마법사가 열리는 **편집**을 클릭합니다.
2. 실행할 스케쥴러 작업을 설정하고, 예약된 작업을 실행할 시기를 정의하려면 다음 타이밍 옵션 중 하나를 선택합니다.
3. 시스템이 배터리로 실행될 때(예: UPS) 작업이 실행되지 않도록 하려면 **배터리 전원으로 실행되는 작업 건너뛰기** 옆의 스위치를 클릭합니다.
4. 업데이트에 사용할 업데이트 프로필을 선택합니다. 어떠한 이유로든 예약된 작업을 실행하지 못한 경우 실행할 동작을 선택합니다.
5. **마침**을 클릭하여 작업을 적용합니다.

업데이트 미러

ESET File Security 열기
F5 키를 누름 > 업데이트 > 프로필 > 업데이트 미러

ESET File Security를 사용하면 네트워크에 있는 다른 워크스테이션을 업데이트하는 데 사용할 수 있는 업데이트 파일의 복사본을 생성할 수 있습니다. "미러"(LAN 환경의 업데이트 파일 복사본)를 사용하면 각 워크스테이션별로 공급업체 업데이트 서버에서 업데이트 파일을 반복적으로 다운로드하지 않아도 되므로 편리합니다. 업데이트는 로컬 미러 서버에 다운로드된 후에 모든 워크스테이션으로 배포되므로 네트워크 트래픽 오버로드가 발생하는 위험도 방지할 수 있습니다. 미러에서 클라이언트 워크스테이션을 업데이트하면 네트워크 부하 분산이 최적화되고 인터넷 연결 대역폭이 절감됩니다.

⊟ 업데이트 미러

업데이트 미러 생성

미러 구성 옵션을 활성화합니다.

저장 폴더

미러링된 파일 *C:\ProgramData\ESET\ESET Security\mirror*를 저장할, 정의된 기본 폴더를 변경하려면 지우기를 클릭합니다. 로컬 컴퓨터 또는 공유 네트워크 폴더에서 폴더를 찾으려면 **편집**을 클릭합니다. 지정한 폴더에 대한 인증이 필요한 경우 사용자 이름 및 패스워드 필드에 인증 데이터를 입력해야 합니다. 선택한 대상 폴더가 Windows NT/2000/XP 운영 체제를 실행하는 네트워크 디스크에 있는 경우에는 여기서 지정하는 사용자 이름 및 패스워드에 선택한 폴더에 대한 쓰기 권한이 있어야 합니다.
사용자 이름 및 패스워드는 *Domain/User* 또는 *Workgroup/User* 형식으로 입력해야 합니다. 해당되는 패스워드를 입력할 수 있도록 기억해 두십시오.

프로그램 구성 요소 업데이트

파일

미러를 구성할 때 사용자가 다운로드하려는 업데이트의 언어 버전을 지정할 수 있습니다. 선택된 언어는 사용자가 구성한 미러 서버에서 지원되어야 합니다.

자동으로 구성 요소 업데이트

새 기능과 기존 기능의 업데이트를 설치할 수 있습니다. 업데이트는 사용자 개입 없이 자동으로 수행될 수도 있고, 알림이 표시되도록 선택할 수도 있습니다. 제품 업데이트를 설치한 후에는 컴퓨터를 다시 시작해야 할 수 있습니다.

구성 요소 지금 업데이트

프로그램 구성 요소를 최신 버전으로 업데이트합니다.

HTTP 서버

서버 포트

기본 포트는 2221로 설정되어 있습니다. 다른 포트를 사용하는 경우 이 값을 변경하십시오.

인증

업데이트 파일에 접근하는 데 사용되는 인증 방법을 정의합니다. 사용할 수 있는 옵션은 **없음**, **기본** 및 **NTLM**입니다.

- 기본 사용자 이름 및 비밀번호 인증과 함께 base64 인코딩을 사용하려면 **기본**을 선택합니다.
- **NTLM** 옵션을 선택하면 안전 인코딩 방법을 사용하는 인코딩을 사용할 수 있습니다. 인증을 위해 업데이트 파일을 공유하는 워크스테이션에서 생성된 사용자가 사용됩니다.
- 기본 설정은 **없음**이며, 이 옵션은 인증할 필요 없이 업데이트 파일에 대한 접근 권한을 부여합니다.

경고
HTTP 서버를 통해 업데이트 파일에 접근할 수 있도록 하려면 미러 폴더가 자신을 생성한 ESET File Security 인스턴스와 동일한 컴퓨터에 있어야 합니다.

HTTP 서버용 SSL

HTTPS(SSL)가 지원되는 HTTP 서버를 실행하려면 **인증서 체인 파일**을 추가하거나 자체적으로 지문이 생성된 인증서를 생성합니다. 사용 가능한 인증서 유형은 PEM, PFX 및 ASN입니다. 보안 강화를 위해 HTTPS 프로토콜을 사용하여 업데이트 파일을 다운로드할 수 있습니다. 이 프로토콜을 사용하여 데이터 전송 및 로그인 자격 증명을 추적한다는 것은 거의 불가능합니다.
개인 키 유형은 기본적으로 **통합**으로 설정됩니다(따라서 개인 키 파일 옵션이 기본적으로 비활성화됨). 즉, 개인 키가 선택된 인증서 체인 파일의 일부입니다.

연결 옵션

Windows 공유

Windows를 실행하는 로컬 서버에서 업데이트하는 경우 기본적으로 각 네트워크에 연결해야 합니다.

다음 계정으로 LAN 연결

계정을 구성하려면 다음 옵션 중 하나를 선택합니다.

- **시스템 계정(기본값)** - 인증에 시스템 계정을 사용합니다. 일반적으로 기본 업데이트 설정 섹션에 인증 데이터를 입력하지 않으면 인증 프로세스가 수행되지 않습니다.
- **현재 사용자** - 현재 로그인한 사용자 계정을 사용하여 프로그램이 인증하도록 하려면 이 옵션을 선택합니다. 이 방법은 현재 로그인한 사용자가 없는 경우 프로그램에서 업데이트 서버에 연결할 수 없다는 단점이 있습니다.
- **지정한 사용자** - 인증에 특정 사용자 계정을 사용하려면 이 옵션을 선택합니다. 기본 시스템 계정 연결에 실패한 경우 이 방법을 사용합니다. 지정한 사용자 계정이 로컬 서버의 업데이트 파일 디렉터리에 접근할 수 있어야 합니다. 사용자에게 접근 권한이 없으면 프로그램에서 연결하여 업데이트를 다운로드할 수 없습니다.

경고
현재 사용자 또는 **지정한 사용자**가 선택되어 있는 경우 프로그램 ID를 원하는 사용자로 변경하면 오류가 발생할 수 있습니다. LAN 인증 데이터를 기본 업데이트 설정 섹션에 입력하는 것이 좋습니다. 이 업데이트 설정 섹션에서 인증 데이터는 *domain_name\user*(작업 그룹인 경우 *workgroup_name\name* 입력) 및 패스워드와 같이 입력해야 합니다. 로컬 서버의 HTTP 버전에서 업데이트하는 경우에는 인증이 필요하지 않습니다.

업데이트 후 서버 연결 끊기

업데이트를 다운로드한 후에도 서버 연결이 활성 상태로 유지되는 경우 강제로 연결을 끊습니다.

네트워크 보호

네트워크 공격 보호(IDS) 활성화

신뢰 영역의 컴퓨터에서 실행 중인 일부 서비스에 대한 접근 권한을 구성하고, 컴퓨터에 해를 끼치는 데 사용될 수 있는 여러 공격 및 익스플로이트 유형의 검출을 활성화/비활성화할 수 있습니다.

봇네트 보호 활성화

컴퓨터가 감염되고 봇이 통신하려고 할 때 일반적인 패턴을 기준으로 악성 명령과 검사 서버가 포함된 통신을 검출하고 차단합니다.

IDS 예외

IDS(Intrusion Detection System) 예외를 네트워크 보호 규칙으로 간주할 수 있습니다. 편집을 클릭하여 IDS 예외를 정의합니다.

침입 검출:

프로토콜 SMB - SMB 프로토콜에서 다양한 보안 문제를 검출하고 차단합니다.
프로토콜 RPC - DCE(Distributed Computing Environment)용으로 개발된 원격 프로시저 호출 시스템에서 다양한 CVE를 검출하고 차단합니다.
프로토콜 RDP - RDP 프로토콜에서 다양한 CVE를 검출하고 차단합니다(상기 참조).
공격 검출 후 안전하지 않은 주소 차단 - 공격의 근원지로 검출되고 특정 기간 동안 연결하지 못하도록 차단 목록에 추가됩니다.
공격 검출 후 알림 표시 - 화면 오른쪽 아래의 시스템 트레이 알림을 켭니다.
보안 허점을 통해 들어오는 공격도 알림 표시 - 보안 허점을 통한 공격이 감지되었거나 이러한 방식으로 위협이 시스템에 침투하려는 경우 경고합니다.

패킷 검사:

SMB 프로토콜에서 관리자 공유에 대해 들어오는 연결 허용 - 관리 공유는 시스템의 하드 드라이브 파티션(C$, D$ 등)을 시스템 폴더(ADMIN$)와 공유하는 기본 네트워크 공유입니다. 관리 공유에 대한 연결을 비활성화하면 많은 보안 위험이 경감됩니다. 예를 들어 Conficker 웜은 관리 공유에 연결하기 위해 사전 공격을 수행합니다.
이전(지원되지 않는) SMB 언어 거부 - IDS에서 지원하지 않는 이전 SMB 언어를 사용하는 SMB 세션을 거부합니다. 최신 Windows 운영 체제는 Windows 95와 같은 이전 운영 체제와의 호환성 문제 때문에 이전 SMB 언어를 지원합니다. 공격자는 트래픽 조사를 회피하기 위해 SMB 세션에 이전 언어를 사용할 수 있습니다. 컴퓨터가 이전 버전의 Windows를 사용하는 컴퓨터와 파일을 공유(또는 일반적으로 SMB 통신 사용)할 필요가 없으면 이전 SMB 언어를 거부하십시오.
확장된 보안이 없는 SMB 세션 거부 - LM(LAN Manager) Challenge/Response 인증보다 안전한 인증 메커니즘을 제공하기 위해 SMB 세션 협상 중에 확장된 보안이 사용될 수 있습니다. LM 체계는 약한 것으로 간주되므로 사용하지 않는 것이 좋습니다.
Security Account Manager 서비스와의 통신 허용 - 이 서비스에 대한 자세한 내용은 [MS-SAMR]를 참조하십시오.
Local Security Authority service 서비스와의 통신 허용 - 이 서비스에 대한 자세한 내용은 [MS-LSAD] 및 [MS-LSAT]를 참조하십시오.
Remote Registry 서비스와의 통신 허용 - 이 서비스에 대한 자세한 내용은 [MS-RRP]를 참조하십시오.
Service Control Manager 서비스와의 통신 허용 - 이 서비스에 대한 자세한 내용은 [MS-SCMR]를 참조하십시오.
Server 서비스와의 통신 허용 - 이 서비스에 대한 자세한 내용은 [MS-SRVS]를 참조하십시오.
기타 서비스와의 통신 허용 - 기타 MSRPC 서비스입니다.

IDS 예외

IDS(Intrusion Detection System) 예외는 기본적으로 네트워크 보호 규칙입니다. 예외는 위에서 아래로 평가됩니다. IDS 예외 편집기를 사용하여 다양한 IDS 예외에 대한 네트워크 보호 동작을 사용자 지정할 수 있습니다. 각 동작 유형(차단, 알림, 로그)에 일치하는 첫 번째 예외가 각기 적용됩니다. **맨 위로/위로/아래로/맨 아래로**를 사용하여 예외의 순위 수준을 조정할 수 있습니다. 새 IDS 예외를 생성하려면 **추가**를 클릭합니다. **편집**을 클릭하여 기존 IDS 예외를 수정하거나 **제거**를 클릭하여 제거합니다.

드롭다운 목록에서 **경고** 유형을 선택합니다. **위협 이름** 및 **지침**을 지정합니다. 예외를 생성하고자 하는 **애플리케이션**을 찾습니다. IP 주소(IPv4 또는 IPv6) 또는 서브넷 목록을 지정합니다. 항목이 여러 개일 경우 쉼표를 분리 기호로 사용합니다.

드롭다운 메뉴에 있는 옵션 중 하나(**기본값**, **예**, **아니요**)를 선택하여 IDS 예외에 대한 **동작**을 구성합니다. 각 동작 유형(**차단**, **알림**, **로그**)에 대해 이를 수행합니다.

> 예
> IDS 예외 경고 발생 시 알림을 표시하고 로그된 이벤트의 시간을 표시하고자 하는 경우 **차단** 동작 유형을 **기본값**으로 두고 다른 두 작업 유형(**알림** 및 **로그**)의 경우 드롭다운 메뉴에서 **예**를 선택합니다.

일시적인 IP 주소 차단 목록

공격의 근원지로 검색되고 특정 기간 동안 연결을 차단하도록 차단 목록에 추가된 IP 주소 목록을 확인합니다. 잠긴 **IP 주소**를 표시합니다.

차단 사유

주소에서 차단된 공격 유형을 표시합니다(예: TCP 포트 검사 공격).

시간 초과

차단 목록에서 주소가 만료되는 시간과 날짜를 표시합니다.

제거/모두 제거

차단되기 전에 선택한 IP 주소를 임시 차단 목록에서 제거하거나, 모든 주소를 차단 목록에서 즉시 제거합니다.

예외 추가

선택한 IP 주소에 대한 방화벽 예외를 IDS 필터링에 추가합니다.

웹 및 이메일

프로토콜 필터링, 이메일 클라이언트 보호, 웹 브라우저 보호 및 안티피싱을 구성하여 인터넷 통신 중에 서버를 보호할 수 있습니다.

이메일 클라이언트 보호

이메일 클라이언트 보호는 모든 이메일 통신을 제어하고 악성 코드로부터 보호하며 감염 검출 시 수행할 동작을 선택할 수 있도록 합니다.

웹 브라우저 보호

웹 브라우저와 원격 서버 간의 통신을 모니터링하고 HTTP 및 HTTPS 규칙을 따릅니다. 이 기능을 사용하여 특정 URL 주소를 차단, 허용하거나 제외할 수 있습니다.

프로토콜 필터링

애플리케이션 프로토콜에 대한 고급 보호 기능을 제공하며, ThreatSense 검사 엔진에서 제공됩니다. 이 검사는 웹 브라우저 또는 이메일 클라이언트 사용 여부에 관계없이 자동으로 작동합니다. 또한 암호화된 (SSL/TLS) 통신에서도 작동합니다.

안티피싱 보호

피싱 콘텐츠를 배포하는 것으로 알려진 웹 페이지를 차단할 수 있습니다.

프로토콜 필터링

애플리케이션 프로토콜에 대한 악성코드 보호 기능은 ThreatSense 탐지 엔진에서 제공합니다. 이 검사 엔진은 여러 고급 악성코드 검사 기술을 통합합니다. 프로토콜 필터링은 사용하는 인터넷 브라우저 또는 이메일 클라이언트와 관계없이 자동으로 작동합니다. 프로토콜 필터링이 활성화된 경우 ESET File Security는 SSL/TLS 프로토콜을 사용하는 통신을 검사합니다. **웹 및 이메일** > SSL/TLS로 이동합니다.

애플리케이션 프로토콜 콘텐츠 필터링 활성화

프로토콜 필터링을 비활성화하면 많은 ESET File Security 구성 요소(**웹 브라우저 보호**, **이메일 프로토콜 보호**, **안티피싱 보호**)에서 이 옵션을 사용하며 이들 기능의 일부는 사용할 수 없습니다.

제외된 애플리케이션

콘텐츠 필터링에서 특정 네트워크 인식 애플리케이션의 통신을 제외하려면 목록에서 해당 애플리케이션을 선택합니다. 선택한 애플리케이션의 HTTP/POP3 통신에서는 위협을 검사하지 않습니다. 프로토콜 필터링에서 특정 애플리케이션을 제외할 수 있습니다. 프로토콜 필터링에서 제외할 애플리케이션 목록의 실행 파일을 선택하려면 **편집**과 **추가**를 클릭합니다.

> 중요
> 이 옵션은 통신 검사 도중 제대로 작동하지 않는 애플리케이션에 대해서만 사용하는 것이 좋습니다.

제외된 IP 주소

프로토콜 필터링에서 특정 원격 주소를 제외할 수 있습니다. 이 목록의 IP 주소는 프로토콜 콘텐츠 필터링에서 제외됩니다. 선택한 주소와의 HTTP/POP3/IMAP 통신에서는 위협을 검사하지 않습니다.

> 중요
> 신뢰할 수 있는 것으로 알려진 주소에 한해서만 이 옵션을 사용하는 것이 좋습니다.

제외할 IP 주소, 주소 범위 또는 서브넷을 지정하려면 **편집**과 **추가**를 클릭합니다. **여러 값 입력**을 선택하면 여러 IP 주소를 새 줄, 쉼표 또는 세미콜론으로 구분하여 추가할 수 있습니다. 여러 선택 항목을 활성화하면

제외된 IP 주소 목록에 주소가 표시됩니다.

> 참고
> 제외는 프로토콜 필터링으로 인해 호환성 문제가 발생하는 경우 유용합니다.

웹 및 이메일 클라이언트

인터넷에는 매우 많은 악성 코드가 있으므로 컴퓨터를 보호하는 데 있어 안전한 인터넷 탐색은 매우 중요한 요소입니다. 웹 브라우저의 취약점과 위조된 링크로 인해 사용자가 모르는 사이에 악성 코드가 시스템에 저장될 수 있습니다. 이러한 이유 때문에 ESET File Security는 웹 브라우저 보안에 중점을 둡니다. 네트워크에 접근하는 각 애플리케이션을 인터넷 브라우저로 표시할 수 있습니다. 선택한 경로의 통신 또는 애플리케이션에 이미 프로토콜을 사용하는 애플리케이션을 웹 및 이메일 클라이언트 목록에 추가할 수 있습니다.

SSL/TLS

ESET File Security에서는 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 프로토콜을 사용하는 통신에서 위협을 검사할 수 있습니다.

다양한 검사 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 프로그램에서 SSL/TLS를 통한 통신을 검사하지 않습니다. SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 프로토콜 필터링 모드는 다음 옵션에서 사용할 수 있습니다.

- **자동 모드** - 검사에서 제외된 인증서로 보호되는 통신을 제외한 SSL/TLS로 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.
- **대화 모드** - 알 수 없는 인증서를 사용하여 SSL/TLS로 보호된 새로운 사이트에 들어가면 동작 선택 대화 상자가 표시됩니다. 이 모드를 사용하면 검사에서 제외할 SSL/TLS 인증서 목록을 생성할 수 있습니다.
- **정책 모드** - 모든 SSL/TLS 연결이 필터링됩니다(구성된 제외 예외).

SSL/TLS 필터링된 애플리케이션 목록

필터링된 애플리케이션을 추가하고 검사 동작 중 하나를 설정합니다. SSL/TLS 필터링된 애플리케이션 목록을 사용하여 특정 애플리케이션에 대한 ESET File Security 동작을 사용자 지정하고, **SSL/TLS 프로토콜 필터링 모드**에서 **대화 모드**를 선택한 경우 선택한 동작을 저장할 수 있습니다.

알려진 인증서 목록

특정 SSL 인증서에 대한 ESET File Security 동작을 사용자 지정할 수 있습니다. **알려진 인증서 목록** 옆의 편집을 클릭하여 목록을 보고 관리할 수 있습니다.

신뢰할 수 있는 도메인과의 통신 제외

프로토콜 검사에서 연장된 유효성 검사 인증서를 사용하여 통신을 제외할 수 있습니다(인터넷 뱅킹).

오래된 프로토콜 SSL v2를 사용하여 암호화된 통신 차단

이 SSL 프로토콜의 이전 버전을 사용하는 통신은 자동으로 차단됩니다.

루트 인증서

브라우저/이메일 클라이언트에서 SSL/TLS 통신이 제대로 작동하려면 ESET에 대한 루트 인증서를 알려진 루트 인증서(게시자) 목록에 추가해야 합니다. 알려진 브라우저에 루트 인증서 추가를 활성화해야 합니다. Opera, Firefox 등의 알려진 브라우저에 ESET 루트 인증서를 자동으로 추가하려면 이 옵션을 선택합니다. Internet Explorer와 같이 시스템 인증서 저장소를 사용하는 브라우저의 경우 인증서가 자동으로 추가됩니다.

지원되지 않는 브라우저에 인증서를 적용하려면 **인증서 보기** > **상세 정보** > **파일에 복사...**를 클릭하고 수동으로 인증서를 브라우저로 가져옵니다.

인증서 유효성

TRCA 인증서 저장소를 사용하여 인증서를 확인할 수 없는 경우

일부 경우 TRCA(**신뢰할 수 있는 루트 인증 기관**) 저장소를 사용하여 웹 사이트 인증서를 확인할 수 있습니다. 이는 인증서가 누군가(예: 웹 서버 또는 소기업의 관리자)에 의해 지문이 생성되었으며 이 인증서를 신뢰할 수 있는 것으로 간주하는 경우 항상 위험이 따르지는 않음을 의미합니다. 은행 등 대부분의 대기업은 TRCA에서 지문이 생성된 인증서를 사용합니다. **인증서 유효성에 대해 확인**(기본값)을 선택한 경우 암호화된 통신이 설정되면 사용자에게 수행할 동작을 선택하라는 메시지가 표시됩니다. **인증서를 사용하는 통신 차단**을 선택하여 확인되지 않은 인증서를 사용하는 사이트에 대해 암호화된 연결을 항상 종료할 수 있습니다.

인증서가 잘못되었거나 손상된 경우

이는 인증서가 만료되었거나 지문이 잘못 생성되었음을 의미합니다. 이 경우 **인증서를 사용하는 통신 차단**을 선택된 상태로 두는 것이 좋습니다.

알려진 인증서 목록

특정 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 인정서에 대한 ESET File Security 동작을 사용자 지정할 수 있으며, **대화 모드**를 SSL/TLS 프로토콜 필터링 모드에서 선택한 경우 선택한 동작을 저장할 수 있습니다. 선택한 인증서를 구성하거나, URL 또는 파일에서 인증서를 **추가**할 수 있습니다. 인증서 추가 창에서 URL 또는 파일을 클릭하고 인증서 URL을 지정하거나 인증서 파일을 찾습니다. 인증서의 데이터를 사용하여 자동으로 입력되는 필드는 다음과 같습니다.

- **인증서 이름** - 인증서의 이름입니다.
- **인증서 발급자** - 인증서 생성자의 이름입니다.
- **인증서 제목** - 제목 필드는 제목 공개 키 필드에 저장된 공개 키와 연결된 엔터티를 식별합니다.

접근 동작

- **자동** - 신뢰할 수 있는 인증서 허용, 신뢰할 수 없는 인증서 확인
- **허용 또는 차단** - 인증서의 신뢰성과 관계없이 이 인증서로 보호되는 통신 허용/차단
- **확인** - 특정 인증서가 검색될 때 메시지 표시

검사 동작

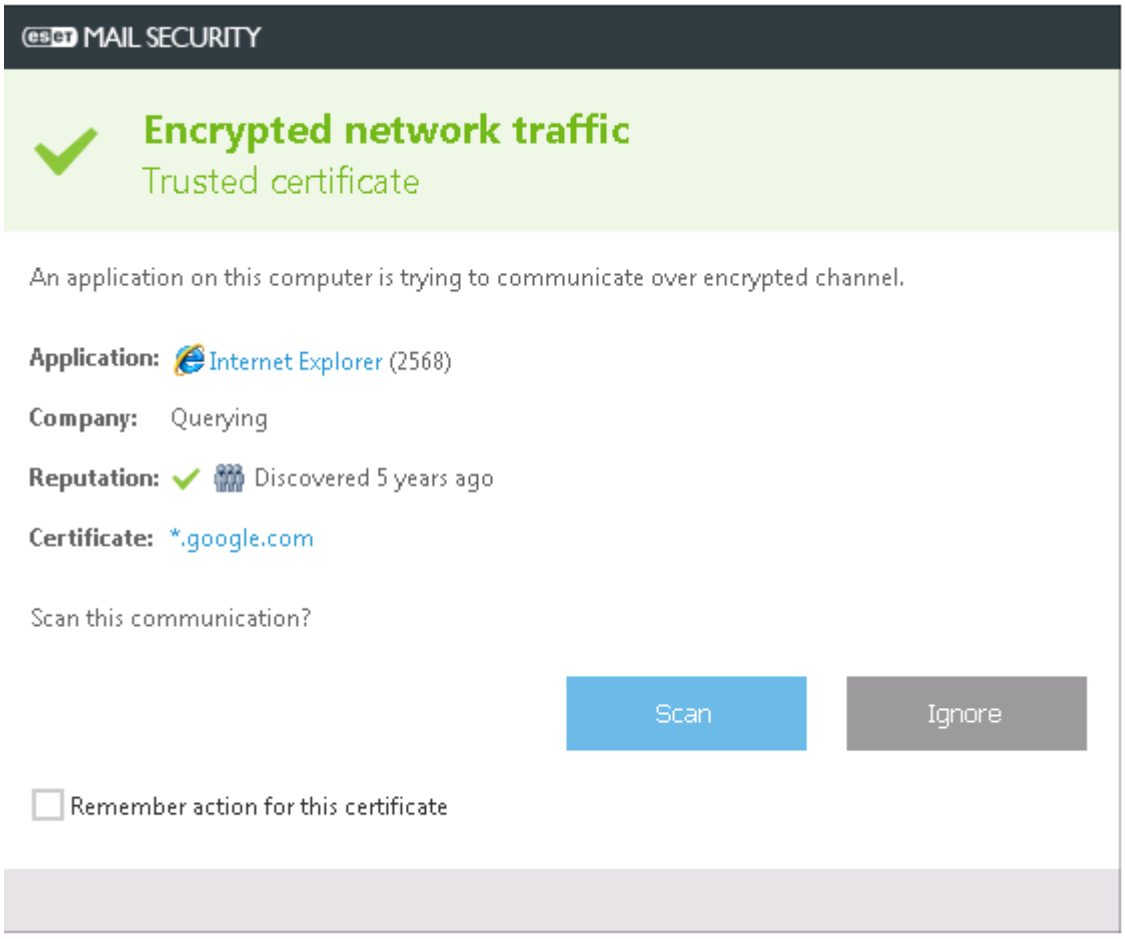
- **자동** - 자동 모드일 때 검사하고 대화 모드일 때 확인
- **검사 또는 무시** - 이 인증서로 보호되는 통신을 검사 또는 무시
- **확인** - 특정 인증서가 검색될 때 메시지 표시

암호화된 SSL 통신

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 File Security가 이러한 경우에 사용자에게 확인(기본적으로 확인할 수 없는 인증서는 "예", 잘못된 인증서는 "아니요")하도록 구성되어 있으면, 연결을 **허용**할지 아니면 **차단**할지 확인하는 대화 상자가 표시됩니다.

둘째, **SSL 프로토콜 필터링 모드**가 **대화 모드**로 설정된 경우 트래픽을 **검사**할지 아니면 **무시**할지 확인하는 대화 상자가 웹 사이트별로 표시됩니다. 일부 애플리케이션에서는 SSL 트래픽이 다른 사용자에 의해 수정되거나 검사되지 않았는지 확인합니다. 이러한 경우 애플리케이션이 계속 작동되도록 하려면 ESET File Security가 해당 트래픽을 **무시**해야 합니다.



이러한 두 가지 경우에서 사용자는 선택한 동작을 저장하도록 선택할 수 있습니다. 저장된 동작은 알려진 인증서 목록에 저장됩니다.

이메일 클라이언트 보호

ESET File Security를 이메일 클라이언트와 통합하면 이메일 메시지의 악성 코드에 대한 활성 보호 수준이 높아집니다. 사용자의 이메일 클라이언트가 지원되면 ESET File Security에서 통합을 활성화할 수 있습니다. 통합이 활성화되면 ESET File Security 도구 모음이 이메일 클라이언트에 직접 삽입되어(최신 버전의 Windows Live Mail 도구 모음은 삽입되지 않음) 이메일을 보다 효율적으로 보호할 수 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 스캐너로 보냅니다. 통합이 활성화되어 있지 않은 경우라도 이메일 통신은 이메일 클라이언트 보호 모듈(POP3, IMAP)의 보호를 계속 받습니다. 지원되는 이메일 클라이언트, 해당 버전에 대한 전체 목록은 지식베이스 문서를 참조하십시오.

받은 편지함 내용 변경 시 확인 비활성화

이메일 클라이언트를 사용할 때 시스템의 속도가 느려지면 이 옵션을 설정합니다(MS Outlook에만 해당). 이러한 상황은 Kerio Outlook Connector Store에서 이메일을 검색할 때 발생할 수 있습니다.

클라이언트 플러그인으로 이메일 보호 활성화

이메일 클라이언트로의 통합을 제거하지 않고도 이메일 클라이언트 보호를 비활성화할 수 있습니다. 모든 플러그인을 한 번에 비활성화하거나, 다음과 같이 선택적으로 비활성화할 수 있습니다.

- **받은 이메일** - 받은 메시지 검사를 전환합니다.
- **보낸 이메일** - 보낸 메시지 검사를 전환합니다.
- **읽은 이메일** - 읽은 메시지 검사를 전환합니다.

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** - 감염된 이메일을 자동으로 지정된 폴더로 이동합니다.
- **폴더** - 검출 시 감염된 이메일을 이동할 사용자 지정 폴더를 지정합니다.

업데이트 후 검사 재실행

탐지 엔진 업데이트 후의 다시 검사를 전환합니다.

다른 모듈의 검사 결과 수락

이 옵션을 선택하면 이메일 보호 모듈에서 다른 보호 모듈(POP3, IMAP 프로토콜 검사)의 검사 결과를 수락합니다.

이메일 프로토콜

프로토콜 필터링으로 이메일 보호 활성화

IMAP 및 POP3 프로토콜은 이메일 클라이언트 애플리케이션에서 이메일 통신을 받는 데 가장 널리 사용되는 프로토콜입니다. ESET File Security는 사용되는 이메일 클라이언트에 관계없이 이 프로토콜에 대한 보호 기능을 제공합니다.

ESET File Security는 암호화된 채널을 사용하여 서버와 클라이언트 간에 정보를 전송하는 IMAPS 및 POP3S 프로토콜의 검사도 지원합니다. ESET File Security는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 프로토콜을 사용하여 통신을 검사합니다. 이 프로그램은 운영 체제 버전과 관계없이 **IMAPS/POP3S 프로토콜**에서 사용되는 포트에 정의된 포트의 트래픽만 검사합니다.

IMAPS / POP3S 스캐너 설정

기본 설정을 사용 중인 경우 암호화된 통신이 검사되지 않습니다. 암호화된 통신 검사를 활성화하려면 SSL/TLS 프로토콜 검사로 이동합니다.

포트 번호는 포트 유형이 무엇인지를 알려 줍니다. 다음은 해당 항목에 대한 기본 이메일 포트입니다.

포트 이름	포트 번호	설명
POP3	110	암호화되지 않은 기본 POP3 포트
IMAP	143	암호화되지 않은 기본 IMAP 포트
보안 IMAP(IMAP4-SSL)	585	SSL/TLS 프로토콜 필터링을 활성화합니다. 포트 번호는 쉼표로 분리해야 합니다.
SSL을 통한 IMAP4(IMAPS)	993	SSL/TLS 프로토콜 필터링을 활성화합니다. 포트 번호는 쉼표로 분리해야 합니다.
보안 POP3(SSL-POP)	995	SSL/TLS 프로토콜 필터링을 활성화합니다. 포트 번호는 쉼표로 분리해야 합니다.

경고 및 알림

이메일 보호는 POP3 및 IMAP 프로토콜을 통해 받은 이메일 통신을 제어합니다. ESET File Security는 Microsoft Outlook용 플러그인 및 기타 이메일 클라이언트를 사용하여 이메일 클라이언트의 모든 통신(POP3, MAPI, IMAP, HTTP)을 제어합니다. 받는 메시지를 검사할 때는 ThreatSense 검사 엔진에 포함된 고급 검사 방법이 모두 사용됩니다. 즉, 바이러스 검출 DB에 일치하는 항목이 있는지 확인하기 전에 악성 프로그램 검출을 수행합니다. POP3 및 IMAP 프로토콜 통신 검사는 사용되는 이메일 클라이언트와 무관합니다.

이메일을 검사한 후에 검사 결과가 포함된 알림을 메시지에 추가할 수 있습니다. **받아서 읽은 메일에 태그 메시지 추가**, **감염된 이메일을 받아서 읽은 경우 이메일 제목에 메모 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 다)에 추가할 수 있습니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **안 함** - 태그 메시지를 추가하지 않습니다.
- **감염된 이메일에만** - 악성 소프트웨어가 포함된 메시지만 검사한 것으로 표시됩니다(기본값).
- **검사한 모든 이메일에** - 검사한 모든 이메일에 메시지를 추가합니다.

감염된 이메일을 보낸 경우 이메일 제목에 메모 추가

이메일 보호 기능을 통해 감염된 이메일의 제목에 바이러스 경고를 포함하지 않으려면 이 옵션을 비활성화합니다. 이 기능을 사용하면 감염된 이메일을 제목에 따라 간편하게 필터링할 수 있습니다(이메일 프로그램에서 지원하는 경우). 또한 받는 사람의 신뢰도가 높아지고 침입이 검출되는 경우, 해당 이메일이나 보낸 사람의 위협 수준에 대한 유용한 정보를 제공합니다.

감염된 이메일의 제목에 추가된 템플릿

감염된 이메일의 제목 접두어 형식을 수정하려면 이 템플릿을 편집합니다. 이 기능은 메시지 제목 `Hello`과 지정된 접두어 값 `[virus]`를 `[virus] Hello` 형식으로 바꿉니다. `%VIRUSNAME%` 변수는 탐지된 위협을 나타냅니다.

MS Outlook 도구 모음

Microsoft Outlook 보호는 플러그인 모듈로 작동합니다. ESET File Security를 설치하면 다음과 같은 악성코드 보호 옵션이 포함된 도구 모음이 Microsoft Outlook에 추가됩니다.

ESET File Security

아이콘을 클릭하면 ESET File Security의 기본 프로그램 창이 열립니다.

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 보호를 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 File Security를 설치하면 다음과 같은 악성코드 보호 옵션이 포함된 도구 모음이 Outlook Express 또는 Windows Mail에 추가됩니다.

ESET File Security

아이콘을 클릭하면 ESET File Security의 기본 프로그램 창이 열립니다.

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 보호를 참조하십시오.

검사기 설정

이메일 클라이언트 보호 설정 옵션을 표시합니다.

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. 이 대화 상자에는 확인을 비활성화하는 옵션도 제공됩니다.

메시지 다시 검사

이메일 클라이언트에 통합된 ESET File Security 도구 모음을 통해 다양한 이메일 검사 옵션을 지정할 수 있습니다. **메시지 다시 검사** 옵션은 다음과 같은 두 가지 검사 모드를 제공합니다.

- **현재 폴더의 모든 메시지** - 현재 표시된 폴더의 메시지를 검사합니다.
- **선택한 메시지만** - 사용자가 지정한 메시지만 검사합니다.
- **이미 검사한 메시지 다시 검사** - 이전에 검사한 메시지를 다시 검사할 수 있습니다.

웹 브라우저 보호

웹 브라우저 보호는 온라인 위협으로부터 사용자를 보호하기 위해 웹 브라우저와 원격 서버 간의 통신을 모니터링하는 방식으로 작동하며, HTTP(Hypertext Transfer Protocol) 및 HTTPS(암호화된 통신) 규칙을 따릅니다.

악성 콘텐츠가 포함된 것으로 알려진 웹 페이지로의 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 차단과 콘텐츠에 의한 차단 기능을 제공합니다.

기본

웹 브라우저 보호를 활성화된 상태로 두는 것이 좋습니다. 이 옵션은 **설정** > **웹 및 이메일** > **웹 브라우저 보호**로 이동하여 ESET File Security의 기본 프로그램 창에서 접근할 수도 있습니다.

브라우저 스크립트의 고급 검사 활성화

기본적으로 웹 브라우저에서 실행되는 모든 JavaScript 프로그램은 탐지 엔진으로 확인됩니다.

웹 프로토콜

대부분의 인터넷 브라우저에서 사용되는 이러한 표준 프로토콜에 대한 모니터링을 구성할 수 있습니다. 기본적으로 ESET File Security는 대부분의 인터넷 브라우저에서 사용되는 HTTP 프로토콜을 모니터링하도록 구성됩니다.

ESET File Security는 HTTPS 프로토콜 검사도 지원합니다. HTTPS 통신에서는 암호화된 채널을 사용하여 서버

와 클라이언트 간에 정보를 전송합니다. ESET File Security는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 프로토콜을 사용하여 통신을 검사합니다. 이 프로그램은 운영 체제 버전과 관계없이 **HTTPS 프로토콜에서 사용되는 포트**에 정의된 포트의 트래픽만 검사합니다.

기본 설정을 사용 중인 경우 암호화된 통신이 검사되지 않습니다. 암호화된 통신 검사를 활성화하려면 **고급 설정**(**F5** 키) > **웹 및 이메일** > SSL/TLS를 선택합니다.

ThreatSense 파라미터

웹 브라우저 보호에서 검사 유형(이메일, 압축파일, 제외, 제한 등)과 검출 방법 등의 설정을 구성합니다.

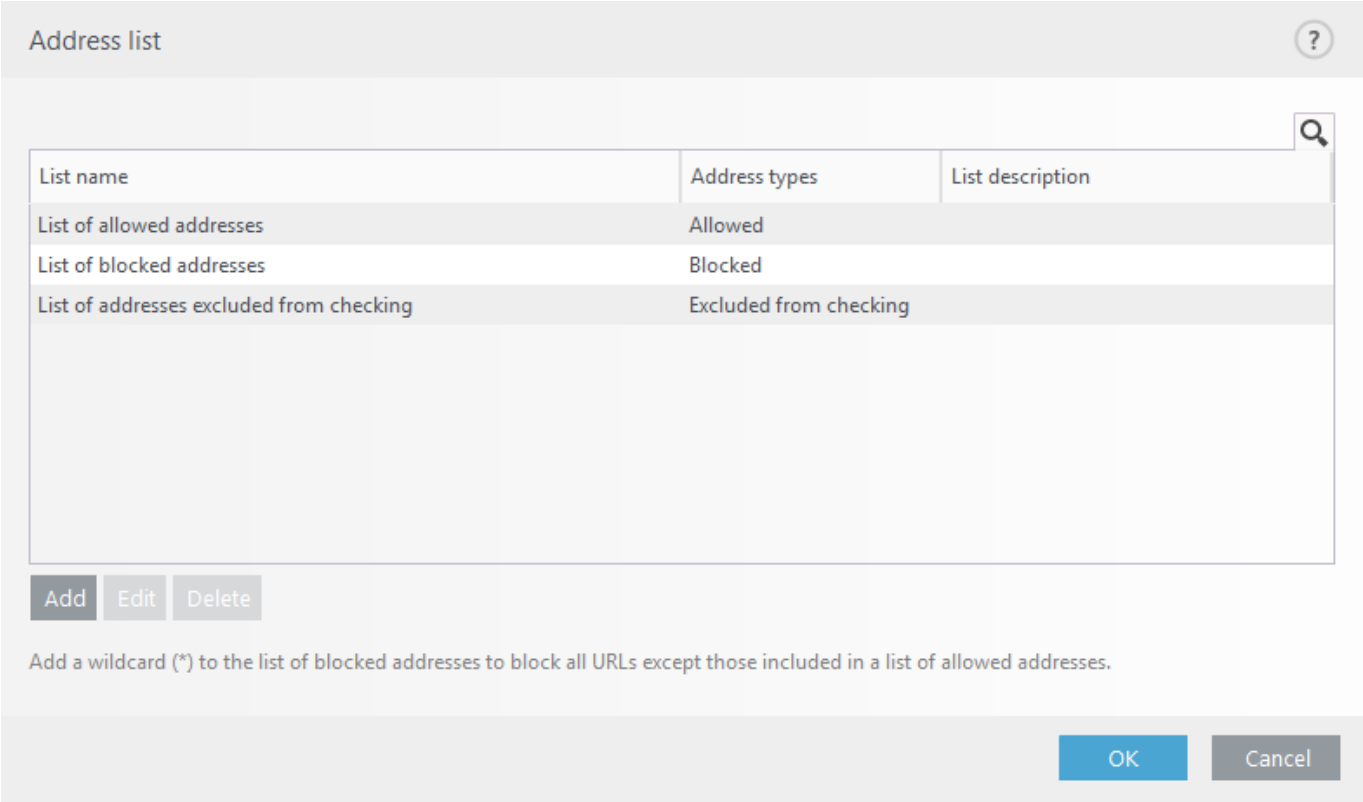
URL 주소 관리

URL 주소 관리에서는 검사에서 차단, 허용 또는 제외할 HTTP 주소를 지정할 수 있습니다. 차단된 주소 목록의 웹 사이트는 허용된 주소 목록에도 포함되지 않는 한 접근할 수 없습니다. 검사에서 제외된 주소 목록의 웹 사이트는 접근 시 악성 코드가 있는지 검사되지 않습니다. HTTP 웹 페이지 외에 HTTPS 주소도 필터링하려면SSL/TLS 프로토콜 필터링을 활성화해야 합니다. 그렇지 않으면 방문한 HTTPS 사이트의 도메인만 추가되고 전체 URL은 추가되지 않습니다.

차단된 주소 목록 하나에는 일부 외부 공개 차단 목록의 주소가 포함될 수 있으며, 다른 차단된 주소 목록에는 자체 차단 목록이 포함될 수 있어 사용자의 차단 목록을 그대로 유지하면서 외부 목록을 쉽게 업데이트할 수 있습니다.

미리 정의된 주소 외에 새 주소를 생성하려면 **편집**과 **추가**를 클릭합니다. 이 옵션은 다양한 주소 그룹을 논리적으로 분할하려는 경우 유용합니다. 기본적으로 다음의 세 목록을 사용할 수 있습니다.

- **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** - 주소가 허용된 주소 목록에도 포함되지 있지 않으면 사용자는 이 목록에서 지정된 주소에 접근할 수 없습니다.



새 URL 주소를 목록에 **추가**할 수 있습니다. 또한 분리 기호를 사용하여 여러 값을 입력할 수 있습니다. 목록에서 기존 주소를 수정하려면 **편집**을 클릭하고, 주소를 제거하려면 **제거**를 클릭합니다. **추가**를 사용하여 생성한 주소만 제거할 수 있고 가져온 목록은 제거할 수 없습니다.

모든 목록에서 특수 기호 *(별표) 및 ?(물음표)를 사용할 수 있습니다. 별표는 임의의 숫자 또는 문자를 나타내고, 물음표는 임의의 한 문자를 나타냅니다. 제외된 주소를 지정할 때는 목록에 신뢰할 수 있는 주소와 안전한 주소만 포함해야 하므로 특히 주의해야 합니다. 마찬가지로 이 목록에서 * 및 ? 기호가 올바르게 사용되는지 확인해야 합니다.

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

새 목록 생성

이 목록에는 검사에서 차단, 허용 또는 제외할, 원하는 URL 주소/도메인 마스크가 포함됩니다. 새 목록 생성 시 다음을 지정합니다.

- **주소 목록 유형** - 드롭다운 목록에서 유형(검사에서 제외됨, 차단됨 또는 허용됨)을 선택합니다.
- **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.
- **목록 활성화** - 스위치를 사용하여 목록을 비활성화합니다. 필요한 경우 나중에 활성화할 수 있습니다.

- **적용 시 알림** - 방문한 HTTP/HTTPS 사이트 평가에 특정 목록이 사용되는 경우 알림을 받으려면 이 옵션을 선택합니다. 웹 사이트가 차단된 주소 목록이나 허용된 주소 목록에 포함되어 있어 차단되거나 허용되는 경우 알림이 발생합니다. 이 알림에는 지정된 웹 사이트를 포함하는 목록의 이름이 포함됩니다.

- **로깅 심각도** - 드롭다운 목록에서 로깅 심각도(없음, 분석, 정보 또는 경고)를 선택합니다. ESET Security Management Center에서 **경고** 상세 수준이 포함된 레코드를 수집할 수 있습니다.

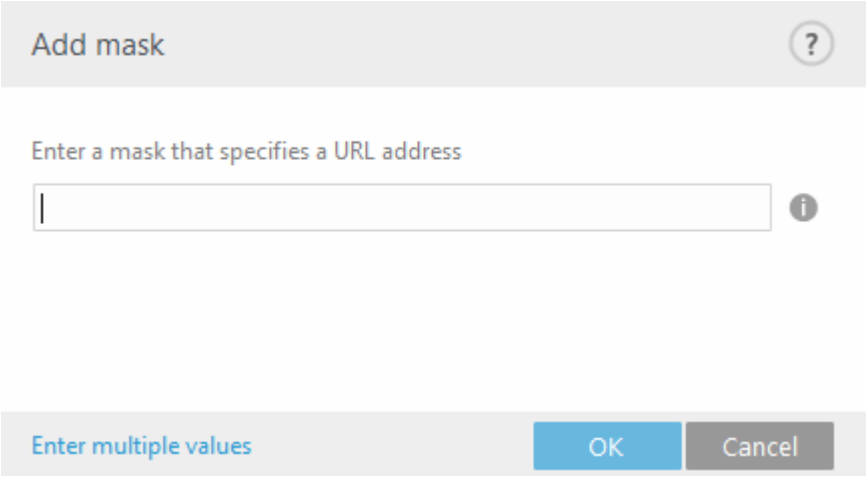
ESET File Security에서는 사용자가 지정한 웹 사이트에 대한 접근을 차단하고 인터넷 브라우저에 해당 웹 사이트의 콘텐츠가 표시되지 않도록 할 수 있습니다. 또한 검사에서 제외할 주소를 지정할 수 있습니다. 원격 서버의 전체 이름을 모르거나 전체 원격 서버 그룹을 지정하려는 경우에는 마스크를 사용하여 해당 그룹을 표시할 수 있습니다.

마스크에는 ? 및 * 기호가 포함됩니다.

- 기호를 대체하려면 ?를 사용합니다.
- 텍스트 문자열을 대체하려면 * 기호를 사용합니다.

예
**.c?m*은 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 특수 취급됩니다. 첫째, 이 경우에는 * 와일드카드가 슬래시 문자(('/'))를 나타내지 않습니다. 이를 통해 마스크 회피를 방지할 수 있습니다. 예를 들어 마스크 **.domain.com*은 *https://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.com*은 *https://domain.com*과도 일치합니다. **domain.com*을 사용하면 *https://anotherdomain.com*과도 일치하게 되므로 올바르지 않습니다.

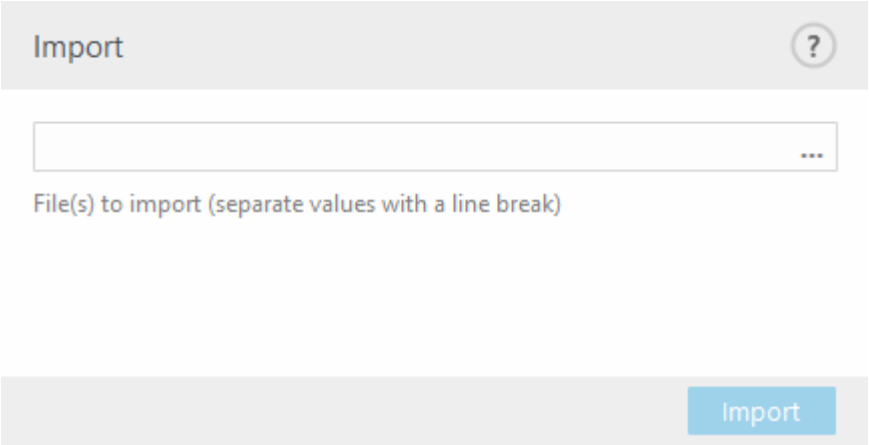


여러 값 입력

여러 URL 주소를 새 줄, 쉼표 또는 세미콜론으로 구분하여 추가합니다. 여러 선택 항목을 활성화하면 주소가 목록에 표시됩니다.

가져오기

가져올 URL 주소가 포함된 텍스트 파일(줄 바꿈으로 값이 구분됨, 예: 인코딩 UTF-8을 사용하는 `*.txt`).

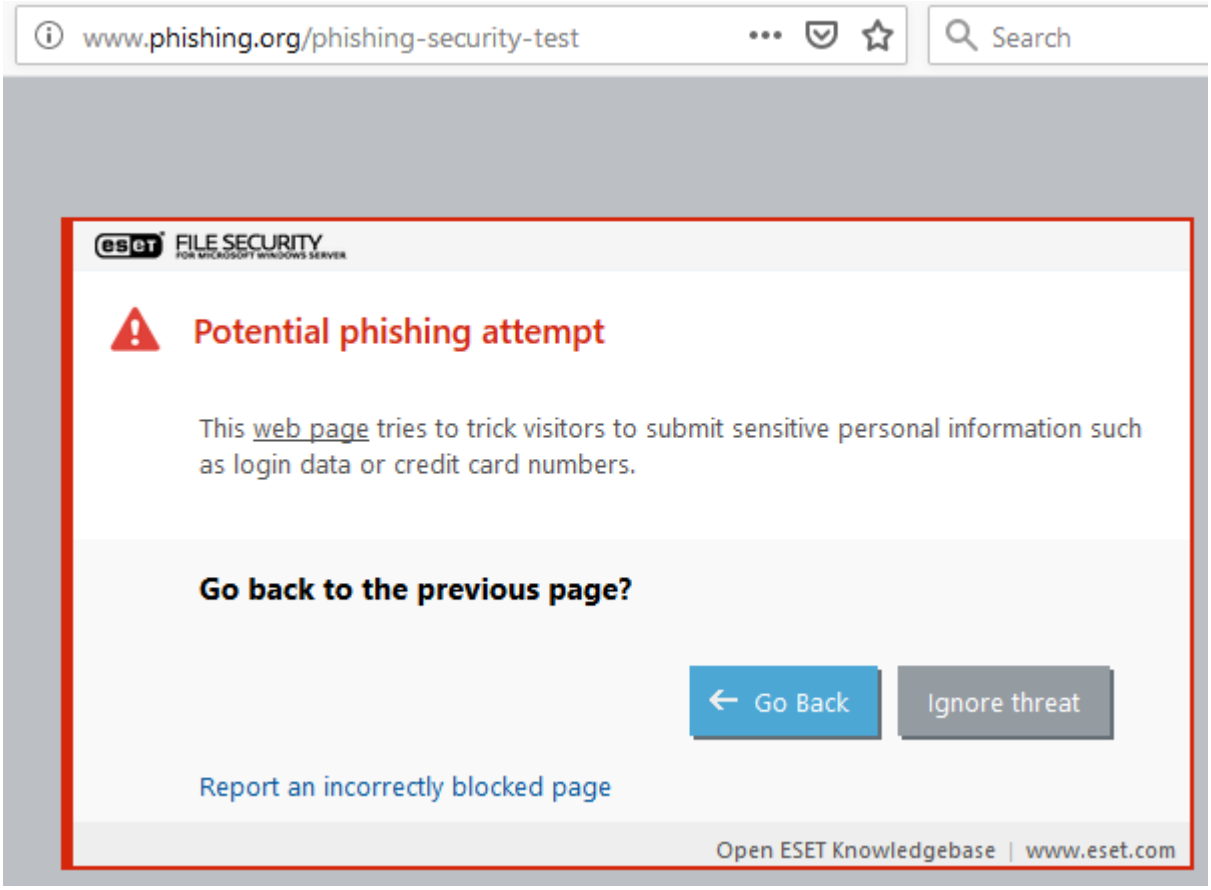


안티피싱 웹 보호

피싱이라는 용어는 사회 공학(기밀 정보를 얻기 위해 사용자를 조종하는 방법)을 사용한 범죄 행위를 의미합니다. 피싱은 은행 계좌 번호, PIN 코드 등과 같은 중요한 데이터에 접근하기 위해 사용되는 경우가 많습니다.

ESET File Security에는 안티피싱 보호 기능이 포함되어 이 유형의 콘텐츠를 배포하는 것으로 알려진 웹 페이지를 차단합니다. ESET File Security에서 안티피싱을 활성화하는 것이 좋습니다. ESET File Security의 안티피싱 보호에 대한 자세한 내용은 지식베이스 문서를 참조하십시오.

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



> 참고
> 허용 목록에 포함된 잠재적인 피싱 웹 사이트는 기본적으로 몇 시간 후에 만료됩니다. 웹 사이트를 영구히 허용하려면 URL 주소 관리 도구를 사용합니다.

피싱 사이트 신고

피싱 사이트 또는 다른 악성 사이트인 것으로 나타나는 감염 의심 웹 사이트를 발견하게 되면 분석하기 위해 ESET에 이를 보고할 수 있습니다. 웹 사이트를 ESET에 전송하기 전에 이 사이트가 다음 조건을 하나 이상 충족하는지 확인하십시오.

- 웹 사이트가 검출되지 않음
- 웹 사이트가 위협으로 잘못 검출됨. 이 경우 가양성 피싱 사이트를 보고할 수 있습니다.

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

장치 제어

ESET File Security에는 자동 장치(CD/DVD/USB) 검사 기능이 포함됩니다. 이 모듈에서는 확장 필터/권한을 검사, 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.

> 참고
> **시스템으로 통합** 스위치를 사용한 장치 제어를 활성화하면 ESET File Security의 장치 제어 기능이 활성화됩니다. 그러나 이 변경 사항을 적용하려면 시스템을 다시 시작해야 합니다.

장치 제어가 활성화되면 각각의 설정을 편집할 수 있습니다. 기존 규칙에 의해 차단된 장치가 검색되면 알림 창이 표시되고 해당 장치에 대한 접근 권한이 부여되지 않습니다.

규칙

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

그룹

편집을 클릭하면 장치 그룹을 관리할 수 있습니다. 새 장치 그룹을 생성하거나 기존 장치 그룹을 선택하여 목록에서 장치를 추가하거나 제거할 수 있습니다.

> 참고
> 로그 파일의 장치 제어 로그 항목을 볼 수 있습니다.

장치 규칙

특정 장치를 사용자, 사용자 그룹 또는 규칙 구성에서 지정할 수 있는 여러 추가 파라미터별로 허용 또는 차단할 수 있습니다. 규칙 목록에는 이름, 외부 장치 유형, 장치가 검색된 경우에 수행할 동작 및 로그 심각도 등과 같은 여러 규칙 설명이 포함됩니다.

새 규칙을 **추가**하거나 기존 규칙의 설정을 수정할 수 있습니다. 좀 더 쉽게 식별할 수 있도록 **이름** 필드에 규칙 설명을 입력합니다. **규칙이 활성화됨** 옆의 스위치를 클릭하여 이 규칙을 비활성화하거나 활성화할 수 있습니다. 이 옵션은 규칙을 영구적으로 제거하지 않으려는 경우에 유용합니다.

다음 기간 중에 적용

시간 슬롯을 사용하여 규칙을 제한할 수 있습니다. 시간 슬롯을 먼저 생성하면 드롭다운 메뉴에 시간 슬롯이 표시됩니다.

장치 유형

드롭다운 메뉴에서 외부 장치 유형(디스크 저장소/휴대용 장치/Bluetooth/FireWire 등)을 선택합니다. 장치 유형은 운영 체제에서 상속되며, 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 장치의 예로는 스캐너나 카메라를 들 수 있습니다. 이러한 장치는 사용자 관련 정보는 제공하지 않고 동작에 대한 정보만 제공합니다. 즉, 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.

> 참고
> 모든 장치 유형에서 모든 권한(동작)을 사용할 수 있는 것은 아닙니다. 장치에 저장 공간이 있는 경우 네 가지 동작을 모두 사용할 수 있습니다. 비저장 장치의 경우 두 가지 동작만 제공됩니다(예: Bluetooth의 경우 **읽기 전용**을 사용할 수 없기 때문에 Bluetooth 장치를 허용하거나 차단할 수만 있음).

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.

> 참고
> 이 세 개의 설명자가 비어 있는 경우 일치 작업 동안 규칙에서 이러한 필드를 무시합니다. 모든 텍스트 필드의 필터링 파라미터는 대소문자를 구분하지 않으며 와일드카드(*, ?)는 지원되지 않습니다.

장치 파라미터를 확인하려면 해당 장치 유형을 허용하는 규칙을 생성하고 이 장치를 컴퓨터에 연결한 다음 장치 제어 로그에서 장치 상세 정보를 확인합니다.

드롭다운 목록에서 **로깅 심각도**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.

규칙을 **사용자 목록**에 추가하여 특정 사용자나 사용자 그룹으로 제한할 수 있습니다. **편집**을 클릭하여 사용자 목록을 관리합니다.

- **추가** - 원하는 사용자를 선택할 수 있는 **개체 유형**: 사용자 또는 그룹 대화 상자 창을 엽니다.
- **제거** - 선택한 사용자를 필터에서 제거합니다.

> 참고
> 모든 장치를 사용자 규칙으로 필터링할 수 있습니다(예: 이미징 장치는 사용자 관련 정보는 제공하지 않고 호출된 동작에 대한 정보만 제공).

사용할 수 있는 기능은 다음과 같습니다.

편집

선택한 규칙 이름이나 해당 그룹에 속한 장치의 파라미터(공급업체, 모델, 일련 번호)를 수정할 수 있습니다.

복사

선택한 규칙의 파라미터를 기반으로 새 규칙을 생성합니다.

삭제

선택한 규칙을 제거하려는 경우 사용합니다. 또는 지정된 규칙 옆의 확인란을 사용하여 규칙을 비활성화할 수 있습니다. 이 옵션은 나중에 규칙을 사용하게 될 경우를 대비하여 규칙을 영구적으로 제거하지 않으려는 경우에 유용합니다.

채움

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 있는 규칙 편집 창이 표시됩니다(모든 설정을 조정할 수 있음).

규칙은 우선 순위 순서대로 나열되며, 규칙의 우선 순위가 높을수록 상단에 나열됩니다. 여러 규칙을 선택하고 동작을 적용할 수 있습니다. 예를 들어 선택한 규칙을 제거하거나 **맨 위로/위로/아래로/맨 아래로**(화살표 버튼)를 클릭하여 목록에서 위 또는 아래로 이동할 수 있습니다.

장치 그룹

장치 그룹 창은 두 부분으로 나뉘어 있습니다. 창의 오른쪽에는 각 그룹에 속한 장치 목록이 표시되고 창의 왼쪽에는 기존 그룹 목록이 표시됩니다. 오른쪽 창에 표시할 장치가 포함된 그룹을 선택합니다.

서로 다른 규칙이 적용되는 여러 장치 그룹을 생성할 수 있습니다. 또한 **읽기/쓰기**나 **읽기 전용**으로 설정된 하나의 장치 그룹을 생성할 수 있습니다. 그러면 컴퓨터에 연결할 때 장치 제어에서 인식되지 않는 장치가 차단됩니다.

> 경고
> 컴퓨터에 외부 장치가 연결되면 보안 위험을 유발할 수 있습니다.

사용할 수 있는 기능은 다음과 같습니다.

추가

장치 이름을 입력하여 새 장치 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 해당 그룹에 속한 장치의 파라미터(공급업체, 모델, 일련 번호)를 수정할 수 있습니다.

삭제

창에서 클릭한 위치에 따라 선택한 그룹 또는 장치를 제거합니다. 또는 지정된 규칙 옆의 확인란을 사용하여 규칙을 비활성화할 수 있습니다. 이 옵션은 나중에 규칙을 사용하게 될 경우를 대비하여 규칙을 영구적으로 제거하지 않으려는 경우에 유용할 수 있습니다.

가져오기

파일에서 장치의 일련 번호 목록을 가져옵니다.

채움

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 있는 규칙 편집 창이 표시됩니다(모든 설정을 조정할 수 있음).

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

> 참고
> 모든 장치 유형에서 모든 권한(동작)을 사용할 수 있는 것은 아닙니다. 장치에 저장 공간이 있는 경우 네 가지 동작을 모두 사용할 수 있습니다. 비저장 장치의 경우 두 가지 동작만 제공됩니다(예: Bluetooth의 경우 읽기 전용을 사용할 수 없기 때문에 Bluetooth 장치를 허용하거나 차단할 수만 있음).

도구 구성

다음에 대한 고급 설정을 사용자 지정할 수 있습니다.

- 시간 슬롯
- ERA/ESMC 검사 대상

- 재정의 모드
- ESET CMD
- ESET RMM
- 라이선스
- WMI 공급자
- 로그 파일
- 프록시 서버
- 이메일 알림
- 프레젠테이션 모드
- 분석
- 클러스터

시간 슬롯

시간 슬롯은 해당 시간 슬롯이 적용되는 규칙을 제한하는 장치 제어 규칙 내에서 사용됩니다. 시간 슬롯을 생성하고, 새 규칙을 추가하거나 기존 규칙을 수정할 때(**다음 기간 중에 적용** 파라미터) 시간 슬롯을 선택합니다. 그러면 일반적으로 사용되는 시간 슬롯(작업 시간, 주말 등)을 정의하고 모든 규칙의 시간 범위를 구체화하지 않고 쉽게 다시 사용할 수 있습니다. 시간 슬롯은 시간 기반 검사를 지원하는 관련 규칙 유형에 모두 적용되어야 합니다.

Microsoft Windows 업데이트

Windows 업데이트는 잠재적으로 위험한 취약점에 중요한 수정 프로그램을 제공하며, 컴퓨터의 일반적인 보안 수준을 향상시킵니다. 이러한 이유로 Microsoft Windows 업데이트를 사용할 수 있게 되는 즉시 설치해야 합니다. ESET File Security는 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 후 시스템 업데이트 정보가 즉시 표시되지 않을 수 있습니다.

ESET CMD

이는 고급 ecmd 명령을 활성화하는 기능으로, 여기에서 명령줄을 사용하여 설정을 내보내고 가져올 수 있습니다(ecmd.exe). 지금까지는 GUI를 사용해야만 설정을 내보낼 수 있었습니다. 이제 ESET File Security 구성을 *.xml* 파일로 내보낼 수 있습니다.

ESET CMD를 활성화하면 다음과 같은 두 개의 인증 방법을 사용할 수 있습니다.

- **없음** - 인증하지 않습니다. 이 방법을 사용하면 지문이 없는 구성을 가져올 수 있으며, 이 경우 잠재적인 위험이 뒤따르므로 권장하지 않습니다.

- **고급 설정 패스워드** - *.xml* 파일에서 구성을 가져오려면 패스워드가 필요하며, 이 경우 파일에 지문이 있어야 합니다(자세한 내용은 *.xml* 구성 파일 지문 생성 참조). 새 구성을 가져오려면 접근 설정에 지정된 패스워드를 입력해야 합니다. 접근 설정이 활성화되지 않은 경우 패스워드가 일치하지 않거나, *.xml* 구성 파일에 지문이 생성되지 않거나, 구성을 가져오지 않게 됩니다.

ESET CMD가 활성화되면 명령줄을 사용하여 ESET File Security 구성을 내보내거나 가져올 수 있습니다. 자동화를 위해 이 작업을 수동으로 수행하거나 스크립트를 생성할 수 있습니다.

중요
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.

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

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

참고
고급 ecmd 명령은 로컬로만 실행할 수 있습니다. ESET Security Management Center를 사용하여 클라이언트 작업인 **명령 실행**을 실행할 수 없습니다.

.xml 구성 파일에 지문 생성:

1. XmlSignTool 실행 파일을 다운로드합니다.

2. **관리자 권한으로 실행**을 사용하여 Windows 명령 프롬프트(cmd)를 엽니다.

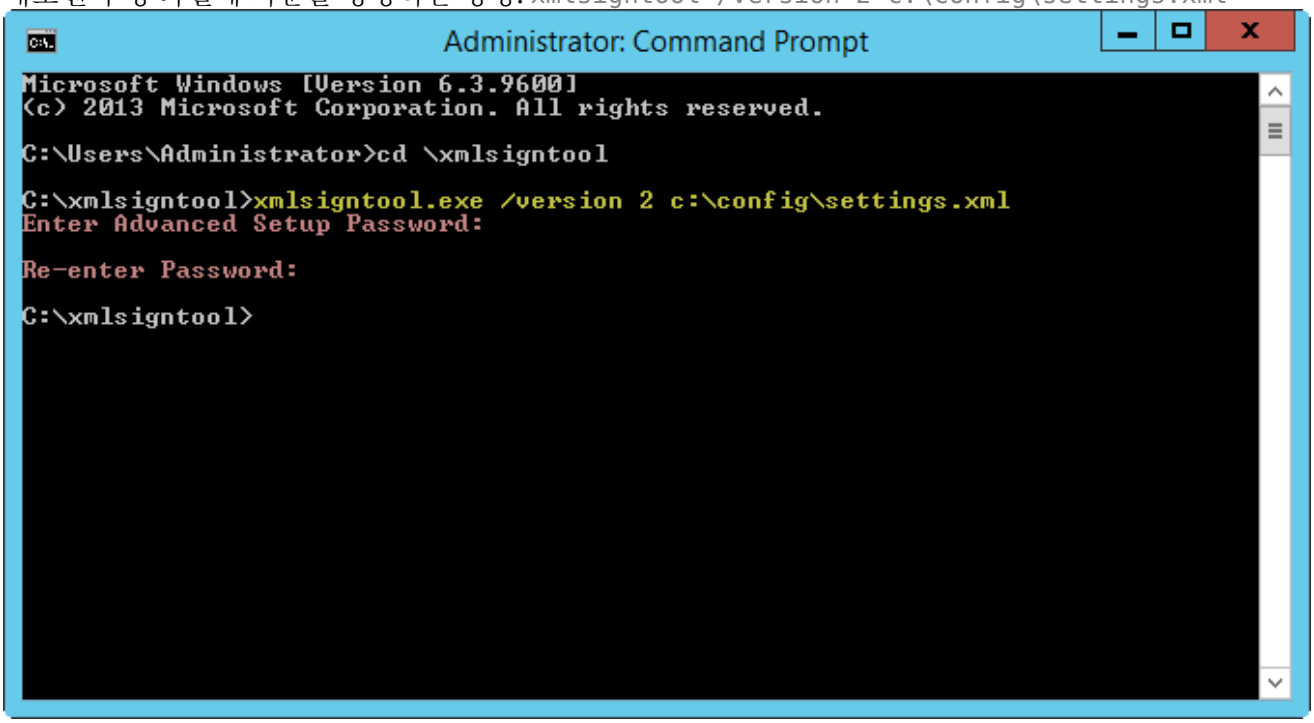
3. `xmlsigntool.exe` 위치로 이동

4. 명령을 실행하여 *.xml* 구성 파일에 지문을 생성합니다(사용: `xmlsigntool /version 1|2 <xml_file_path>`).

중요
`/version` 파라미터 값은 ESET File Security 버전에 따라 다릅니다. ESET File Security 7 이상의 경우 `/version 2`를 사용합니다.

5. XmlSignTool에 패스워드를 입력하라는 메시지가 표시되면 고급 설정 패스워드를 입력하고 확인 패스워드를 다시 입력합니다. 이제 *.xml* 구성 파일에 지문이 생성되었으며, 이 구성 파일을 통해 패스워드 인증 방법을 사용하여 ESET CMD로 다른 ESET File Security 인스턴스에서 설정을 가져올 수 있습니다.

예
내보낸 구성 파일에 지문을 생성하는 명령: `xmlsigntool /version 2 c:\config\settings.xml`



참고
접근 설정 패스워드가 변경되고 이전 패스워드로 이전에 지문이 생성된 구성을 가져오려면 현재 패스워드를 사용하여 *.xml* 구성 파일에 다시 지문을 생성하면 됩니다. 그러면 구성을 가져오기 전에 ESET File Security를 실행하는 다른 컴퓨터에서 구성을 내보내지 않고도 이전 구성 파일을 사용할 수 있습니다.

ESET RMM

원격 모니터링 및 관리(RMM)는 관리 서비스 공급자가 접근할 수 있는 로컬에 설치된 에이전트를 사용하여 소프트웨어 시스템(예: 데스크톱, 서버 및 모바일 장치)을 감독하고 검사하는 프로세스입니다.

RMM 활성화

원격 모니터링 및 관리 명령을 활성화하면 기능이 작동합니다. RMM 유틸리티를 사용하려면 관리자 권한이 있어야 합니다.

작동 모드

드롭다운 메뉴에서 RMM 작동 모드를 선택합니다.

- **안전 작업만 -** 안전한 읽기 전용 작업에 대해 RMM 인터페이스를 사용하려는 경우
- **모든 작업 -** 모든 작업에 대해 RMM 인터페이스를 활성화하려는 경우

인증 방법

드롭다운 메뉴에서 RMM 인증 방법을 선택합니다.

- **없음** - 애플리케이션 경로 확인 작업이 수행되지 않아 모든 애플리케이션에서 *ermm.exe*를 실행할 수 있습니다.
- **애플리케이션 경로** - *ermm.exe*를 실행할 수 있는 애플리케이션을 지정합니다.

기본 ESET Endpoint Security 설치에는 ESET File Security(기본 경로 c:*Program Files\ESET\ESET File Security*)에 있는 *ermm.exe* 파일이 포함됩니다. *ermm.exe*는 RMM 플러그인과 데이터를 교환하며, RMM 플러그인은 RMM 서버와 연결된 RMM 에이전트와 통신합니다.

- *ermm.exe* - ESET에서 개발한 명령줄 유틸리티로, Endpoint 제품을 관리하고 RMM 플러그인과 통신할 수 있습니다.
- RMM 플러그인 - Endpoint Windows 시스템에서 로컬로 실행되는 타사 애플리케이션입니다. 플러그인은 특정 RMM 에이전트(예: Kaseya만 해당) 및 *ermm.exe*와 통신하도록 설계되었습니다.
- RMM 에이전트 - Endpoint Windows 시스템에서 로컬로 실행되는 타사 애플리케이션(예: Kaseya 제품)입니다. 에이전트는 RMM 플러그인 및 RMM 서버와 통신합니다.
- RMM 서버 - 타사 서버에서 서비스로 실행됩니다. 지원되는 RMM 시스템으로는 Kaseya, Labtech, Autotask, Max Focus 및 Solarwinds N-able 등이 있습니다.

ESET File Security의 ESET RMM에 대한 자세한 내용은 지식베이스 문서를 참조하십시오.

타사 RMM 솔루션용 ESET 엔드포인트 직접 관리 플러그인

RMM 서버는 타사 서버에서 서비스로 실행됩니다. 자세한 내용은 다음 ESET 엔드포인트 직접 관리 온라인 사용자 설명서를 참조하십시오.

- ConnectWise Automate용 ESET 엔드포인트 직접 관리 플러그인
- DattoRMM용 ESET 엔드포인트 직접 관리 플러그인
- Solarwinds N-Central용 ESET 엔드포인트 직접 관리
- NinjaRMM용 ESET 엔드포인트 직접 관리

라이선스

ESET File Security은 시간당 몇 차례 ESET 라이선스 서버에 연결하여 확인을 수행합니다. 기본적으로 **간격 확인** 파라미터는 **자동**으로 설정되어 있습니다. 라이선스 확인으로 인한 네트워크 트래픽을 줄이려면 간격 확인을 **제한됨**으로 변경하여 라이선스 확인을 하루에 한 번만 수행합니다(서버 재시작 후에도 해당).

간격 확인을 **제한됨**으로 설정하면 ESET Business Account 및 ESET MSP Administrator를 통해 이루어진 모든 라이선스 관련 변경 사항이 ESET File Security에 적용되는 데 최대 1일이 걸릴 수 있습니다.

WMI 공급자

WMI(Windows Management Instrumentation)는 엔터프라이즈 환경에서 관리 정보에 접근하는 표준 기술을 개발하기 위한 산업 이니셔티브인 WBEM(웹 기반 엔터프라이즈 관리)의 Microsoft 구현입니다.

WMI에 대한 자세한 내용은 http://msdn.microsoft.com/ko-kr/library/windows/desktop/aa384642(v=vs.85).aspx를 참조하십시오.

ESET WMI 공급자

ESET WMI 공급자는 ESET 관련 소프트웨어나 도구 없이도 엔터프라이즈 환경에서 ESET 제품을 원격 모니터링할 수 있도록 지원하기 위해 제공됩니다. ESET에서는 WMI를 통해 기본 제품, 상태 및 통계를 제공함으로

써 엔터프라이즈 관리자의 ESET 제품 모니터링 기능을 크게 확장합니다. 관리자는 WMI에서 제공하는 여러 가지 접근 방법(명령줄, 스크립트 및 타사 엔터프라이즈 모니터링 도구)을 활용하여 ESET 제품의 상태를 모니터링할 수 있습니다.

현재 구현에서는 기본 제품 정보, 설치된 기능 및 해당 보호 상태, 개별 검사기의 통계 및 제품 로그 파일에 대한 읽기 전용 접근을 제공합니다.

WMI 공급자를 통해 표준 Windows WMI 인프라 및 도구를 사용하여 제품의 상태 및 제품 로그를 읽을 수 있습니다.

제공된 데이터

ESET 제품과 관련된 모든 WMI 클래스는 “root\ESET“ 네임스페이스에 있습니다. 현재 구현된 클래스에 대한 자세한 설명은 다음과 같습니다.

일반

- **ESET_Product**
- **ESET_Features**
- **ESET_Statistics**

로그

- **ESET_ThreatLog**
- **ESET_EventLog**
- **ESET_ODFileScanLogs**
- **ESET_ODFileScanLogRecords**
- **ESET_ODServerScanLogs**
- **ESET_ODServerScanLogRecords**
- **ESET_HIPSLog**
- **ESET_URLLog**
- **ESET_DevCtrlLog**
- **ESET_GreylistLog**
- **ESET_MailServeg**
- **ESET_HyperVScanLogs**
- **ESET_HyperVScanLogRecords**

ESET_Product 클래스

ESET_Product 클래스는 인스턴스가 하나만 있을 수 있습니다. 이 클래스의 속성은 설치된 ESET 제품에 대한 기본 정보를 참조합니다.

- **ID** - 제품 유형 식별자(예: “emsl”)
- **Name** - 제품의 이름(예: "ESET Mail Security")
- **FullName** - 제품의 전체 이름(예: "ESET Mail Security for IBM Domino")
- **Version** - 제품 버전(예: "6.5.14003.0")
- **VirusDBVersion** - 바이러스 DB의 버전(예: "14533 (20161201)")
- **VirusDBLastUpdate** - 바이러스 DB의 마지막 업데이트에 대한 타임스탬프. 이 문자열은 WMI 날짜/시간 형식(예: “20161201095245.000000+060”)의 타임스탬프를 포함합니다.

- **LicenseExpiration** - 라이선스 만료 시간. 이 문자열은 WMI 날짜/시간 형식의 타임스탬프를 포함합니다.
- **KernelRunning** - ekrn 서비스가 컴퓨터에서 실행 중인지 여부를 나타내는 부울 값(예: “TRUE”)
- **StatusCode** - 제품의 보호 상태를 나타내는 숫자. 0 - 녹색(정상), 1 - 노란색(경고), 2 - 빨간색(오류)
- **StatusText** - 0이 아닌 상태 코드에 대한 이유를 설명하는 메시지. 상태 코드가 0인 경우 null

ESET_Features 클래스

ESET_Features 클래스는 제품 기능 수에 따라 여러 인스턴스가 있습니다. 각 인스턴스는 다음 정보를 포함합니다.

- **Name** - 기능의 이름(아래에 이름 목록 제공)
- **Status** - 기능의 상태. 0 - 비활성, 1 - 비활성화됨, 2 - 활성화됨

현재 인식된 제품 기능을 나타내는 문자열 목록:

- **CLIENT_FILE_AV** - 실시간 파일 시스템 안티바이러스 보호
- **CLIENT_WEB_AV** - 클라이언트 웹 안티바이러스 보호
- **CLIENT_DOC_AV** - 클라이언트 문서 안티바이러스 보호
- **CLIENT_NET_FW** - 클라이언트 개인 방화벽
- **CLIENT_EMAIL_AV** - 클라이언트 이메일 안티바이러스 보호
- **CLIENT_EMAIL_AS** - 클라이언트 이메일 안티스팸 보호
- **SERVER_FILE_AV** - 보호된 파일 서버 제품에 있는 파일(예: ESET File Security의 경우 SharePoint 콘텐츠 데이터베이스에 있는 파일)에 대한 실시간 안티바이러스 보호
- **SERVER_EMAIL_AV** - 보호된 서버 제품의 이메일(예: MS Exchange 또는 IBM Domino의 이메일)에 대한 안티바이러스 보호
- **SERVER_EMAIL_AS** - 보호된 서버 제품의 이메일(예: MS Exchange 또는 IBM Domino의 이메일)에 대한 안티스팸 보호
- **SERVER_GATEWAY_AV** - 게이트웨이의 보호된 네트워크 프로토콜에 대한 안티바이러스 보호
- **SERVER_GATEWAY_AS** - 게이트웨이의 보호된 네트워크 프로토콜에 대한 안티스팸 보호

ESET_Statistics 클래스

ESET_Statistics 클래스는 제품의 검사기 수에 따라 여러 인스턴스가 있습니다. 각 인스턴스는 다음 정보를 포함합니다.

- **Scanner** - 특정 검사기에 대한 문자열 코드(예: “CLIENT_FILE”)
- **Total** - 검사한 전체 파일 수
- **Infected** - 발견한 감염된 파일 수
- **Cleaned** - 치료된 파일 수
- **Timestamp** - 이 통계의 마지막 변경에 대한 타임스탬프(예: WMI 날짜/시간 형식의 경우 “20130118115511.000000+060”)
- **ResetTime** - 통계 카운터가 마지막으로 다시 설정된 타임스탬프(예: WMI 날짜/시간 형식의 경우 “20130118115511.000000+060”)

현재 인식된 검사기를 나타내는 문자열 목록:

- **CLIENT_FILE**
- **CLIENT_EMAIL**
- **CLIENT_WEB**

- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog 클래스

ESET_ThreatLog 클래스는 인스턴스가 여러 개이며, 각각 "검출된 위협" 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 검사 로그 기록의 고유 ID
- **Timestamp** - 로그 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Scanner** - 이 로그 이벤트를 생성한 검사기의 이름
- **ObjectType** - 이 로그 이벤트를 생성한 개체의 유형
- **ObjectName** - 이 로그 이벤트를 생성한 개체의 이름
- **Threat** - 개체(ObjectName 및 ObjectType 속성으로 설명됨)에서 발견된 위협의 이름
- **Action** - 위협이 식별된 이후에 수행된 동작
- **User** - 이 로그 이벤트를 생성한 사용자 계정
- **Information** - 이벤트에 대한 추가 설명
- **Hash** - 이 로그 이벤트를 생성한 개체의 해시

ESET_EventLog

ESET_EventLog 클래스는 인스턴스가 여러 개이며, 각각 "이벤트" 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 검사 로그 기록의 고유 ID
- **Timestamp** - 로그 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8] 간격의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Module** - 이 로그 이벤트를 생성한 모듈의 이름
- **Event** - 이벤트에 대한 설명
- **User** - 이 로그 이벤트를 생성한 사용자 계정

ESET_ODFileScanLogs

ESET_ODFileScanLogs 클래스는 인스턴스가 여러 개이며, 각각 수동 파일 검사 기록을 나타냅니다. 이는 GUI "수동 검사" 로그 목록에 해당합니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 검사 로그 기록의 고유 ID
- **Timestamp** - 로그 생성 타임스탬프(WMI 날짜/시간 형식)
- **Targets** - 검사 대상 폴더/개체
- **TotalScanned** - 검사한 전체 개체 수
- **Infected** - 발견한 감염된 개체 수
- **Cleaned** - 치료된 개체 수
- **Status** - 검사 프로세스의 상태

ESET_ODFileScanLogRecords

ESET_ODFileScanLogRecords 클래스는 인스턴스가 여러 개이며, 각각 ESET_ODFileScanLogs 클래스의 인스턴스가 나타내는 검사 로그 중 하나에 있는 로그 기록을 나타냅니다. 이 클래스의 인스턴스는 모든 수동 검사/로그의 로그 기록을 제공합니다. 특정 검사 로그의 인스턴스만 필요한 경우 LogID 속성으로 필터링해야 합니다. 각 클래스 인스턴스는 다음 정보를 포함합니다.

- **LogID** - 이 기록이 속한 검사 로그의 ID(ESET_ODFileScanLogs 클래스 인스턴스 중 하나의 ID)
- **ID** - 이 검사 로그 기록의 고유 ID
- **Timestamp** - 로그 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Log** - 실제 로그 메시지

ESET_ODServerScanLogs

ESET_ODServerScanLogs 클래스는 인스턴스가 여러 개이며, 각각 수동 서버 검사 실행을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 검사 로그 기록의 고유 ID
- **Timestamp** - 로그 생성 타임스탬프(WMI 날짜/시간 형식)
- **Targets** - 검사 대상 폴더/개체
- **TotalScanned** - 검사한 전체 개체 수
- **Infected** - 발견한 감염된 개체 수
- **Cleaned** - 치료된 개체 수
- **RuleHits** - 전체 규칙 적중 횟수
- **Status** - 검사 프로세스의 상태

ESET_ODServerScanLogRecords

ESET_ODServerScanLogRecords 클래스는 인스턴스가 여러 개이며, 각각 ESET_ODServerScanLogs 클래스의 인스턴스가 나타내는 검사 로그 중 하나에 있는 로그 기록을 나타냅니다. 이 클래스의 인스턴스는 모든 수동 검사/로그의 로그 기록을 제공합니다. 특정 검사 로그의 인스턴스만 필요한 경우 LogID 속성으로 필터링해야 합니다. 각 클래스 인스턴스는 다음 정보를 포함합니다.

- **LogID** - 이 기록이 속한 검사 로그의 ID(ESET_ ODServerScanLogs 클래스 인스턴스 중 하나의 ID)
- **ID** - 이 검사 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8] 간격의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Log** - 실제 로그 메시지

ESET_SmtpProtectionLog

ESET_SmtpProtectionLog 클래스는 인스턴스가 여러 개이며, 각각 “Smtp 보호” 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 검사 로그 기록의 고유 ID

- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **HELODomain** - HELO 도메인의 이름
- **IP** - 소스 IP 주소
- **Sender** - 이메일 보낸 사람
- **Recipient** - 이메일 받는 사람
- **ProtectionType** - 사용된 보호 유형
- **Action** - 수행된 동작
- **Reason** - 동작 이유
- **TimeToAccept** - 이메일을 수락하기까지의 경과 시간(분)

ESET_HIPSLog

ESET_HIPSLog 클래스는 인스턴스가 여러 개이며, 각각 “HIPS” 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8] 간격의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Application** - 소스 애플리케이션
- **Target** - 작업 유형
- **Action** - HIPS에서 수행된 동작(예: 허용, 거부 등)
- **Rule** - 동작을 담당하는 규칙의 이름
- **AdditionalInfo**

ESET_URLLog

ESET_URLLog 클래스는 인스턴스가 여러 개이며, 각각 “필터링된 웹 사이트” 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **URL** - URL
- **Status** - URL에 발생한 상황("웹 컨트롤에 의해 차단됨")
- **Application** - URL에 접근하기 위해 시도하는 애플리케이션
- **User** - 애플리케이션이 실행 중이었던 사용자 계정

ESET_DevCtrlLog

ESET_DevCtrlLog 클래스는 인스턴스가 여러 개이며, 각각 “장치 제어” 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 로그 기록의 고유 ID

- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Device** - 장치 이름
- **User** - 사용자 계정 이름
- **UserSID** - 사용자 계정 SID
- **Group** - 사용자 그룹 이름
- **GroupSID** - 사용자 그룹 SID
- **Status** - 장치에 발생한 상황(예: "쓰기 차단됨")
- **DeviceDetails** - 장치에 관한 추가 정보
- **EventDetails** - 이벤트에 관한 추가 정보

ESET_MailServerLog

ESET_MailServerLog 클래스는 인스턴스가 여러 개이며, 각각 "메일 서버" 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **IPAddr** - 소스 IP 주소
- **HELODomain** - HELO 도메인의 이름
- **Sender** - 이메일 보낸 사람
- **Recipient** - 이메일 받는 사람
- **Subject** - 이메일 제목
- **ProtectionType** - 현재 로그 기록에서 설명하는 동작을 수행하는 보호 유형(예: 악성코드, 안티스팸 또는 규칙)
- **Action** - 수행된 동작
- **Reason** - 지정된 보호 유형에서 개체에 동작을 수행한 이유

ESET_HyperVScanLogs

ESET_HyperVScanLogs 클래스는 인스턴스가 여러 개이며, 각각 Hyper-V 파일 검사의 실행을 나타냅니다. 이는 GUI "Hyper-V 검사" 로그 목록에 해당합니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **Targets** - 대상 컴퓨터/디스크/검사 볼륨
- **TotalScanned** - 검사한 전체 개체 수
- **Infected** - 발견한 감염된 개체 수
- **Cleaned** - 치료된 개체 수
- **Status** - 검사 프로세스의 상태

ESET_HyperVScanLogRecords

ESET_HyperVScanLogRecords 클래스는 인스턴스가 여러 개이며, 각각 ESET_HyperVScanLogs 클래스의 인스턴스가 나타내는 검사 로그 중 하나에 있는 로그 기록을 나타냅니다. 이 클래스의 인스턴스는 모든 Hyper-V 검

사/로그의 로그 기록을 제공합니다. 특정 검사 로그의 인스턴스만 필요한 경우 LogID 속성으로 필터링해야 합니다. 각 클래스 인스턴스는 다음 정보를 포함합니다.

- **LogID** - 이 기록이 속한 검사 로그의 ID(ESET_HyperVScanLogs 클래스 인스턴스 중 하나의 ID)
- **ID** - 이 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Log** - 실제 로그 메시지

ESET_NetworkProtectionLog

ESET_NetworkProtectionLog 클래스는 인스턴스가 여러 개이며, 각각 "네트워크 보호" 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Event** - 네트워크 보호 동작을 트리거하는 이벤트
- **Action** - 네트워크 보호에 의해 수행된 동작
- **Source** - 네트워크 장치의 소스 주소
- **Target** - 네트워크 장치의 대상 주소
- **Protocol** - 네트워크 통신 프로토콜
- **RuleOrWormName** - 이벤트와 관련된 규칙 또는 웜 이름
- **Application** - 네트워크 통신을 시작한 애플리케이션
- **User** - 이 로그 이벤트를 생성한 사용자 계정

ESET_SentFilesLog

ESET_SentFilesLog 클래스는 인스턴스가 여러 개이며, 각각 "보낸 파일" 로그의 로그 기록을 나타냅니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 로그 기록의 고유 ID
- **Timestamp** - 로그 기록 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Sha1** - 보낸 파일의 Sha-1 해시
- **File** - 보낸 파일
- **Size** - 보낸 파일 크기
- **Category** - 보낸 파일 범주
- **Reason** - 파일 전송 이유
- **SentTo** - 파일이 전송된 ESET 부서
- **User** - 이 로그 이벤트를 생성한 사용자 계정

ESET_OneDriveScanLogs

ESET_OneDriveScanLogs 클래스는 인스턴스가 여러 개이며, 각각 OneDrive 검사의 실행을 나타냅니다. 이는 GUI "OneDrive 검사" 로그 목록에 해당합니다. 각 인스턴스는 다음 정보를 포함합니다.

- **ID** - 이 OneDrive 로그의 고유 ID
- **Timestamp** - 로그 생성 타임스탬프(WMI 날짜/시간 형식)
- **Targets** - 검사 대상 폴더/개체
- **TotalScanned** - 검사한 전체 개체 수
- **Infected** - 발견한 감염된 개체 수
- **Cleaned** - 치료된 개체 수
- **Status** - 검사 프로세스의 상태

ESET_OneDriveScanLogRecords

ESET_OneDriveScanLogRecords 클래스는 인스턴스가 여러 개이며, 각각 ESET_OneDriveScanLogs 클래스의 인스턴스가 나타내는 검사 로그 중 하나에 있는 로그 기록을 나타냅니다. 이 클래스의 인스턴스는 모든 OneDrive 검사/로그의 로그 기록을 제공합니다. 특정 검사 로그의 인스턴스만 필요한 경우 LogID 속성으로 필터링해야 합니다. 각 인스턴스는 다음 정보를 포함합니다.

- **LogID** - 이 기록이 속한 검사 로그의 ID(ESET_OneDriveScanLogs 클래스 인스턴스 중 하나의 ID)
- **ID** - 이 OneDrive 로그의 고유 ID
- **Timestamp** - 로그 생성 타임스탬프(WMI 날짜/시간 형식)
- **LogLevel** - [0-8]의 숫자로 표현되는 로그 기록의 심각도. 값은 명명된 수준인 Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical에 해당합니다.
- **Log** - 실제 로그 메시지

제공된 데이터 접근

다음은 모든 최신 Windows 운영 체제에서 작업해야 하는 Windows 명령줄 및 PowerShell에서 ESET WMI 데이터에 접근하는 방법에 대한 몇 가지 예입니다. 그러나 다른 스크립팅 언어 및 도구에서 데이터에 접근할 수 있는 여러 가지 방법도 있습니다.

스크립트 없는 명령줄

`wmic` 명령줄 도구를 사용하여 여러 가지 미리 정의된 WMI 클래스 또는 모든 사용자 지정 WMI 클래스에 접근할 수 있습니다.

로컬 컴퓨터에 제품에 대한 전체 정보를 표시하려면

```
wmic /namespace:\\root\ESET Path ESET_Product
```

로컬 컴퓨터에 제품의 버전 번호만 표시하려면

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

IP 10.1.118.180을 사용하여 원격 컴퓨터에 제품에 대한 전체 정보를 표시하려면

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

제품에 대한 전체 정보를 가져와 로컬 컴퓨터에 표시하려면

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

IP 10.1.118.180을 사용하여 제품에 대한 전체 정보를 가져와 원격 컴퓨터에 표시하려면

```
$cred = Get-Credential # promts the user for credentials and stores it in the
variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred
$cred
```

ERA/ESMC 검사 대상

이 기능을 통해 ESET File Security가 설치된 서버에서 **서버 검사** 클라이언트 작업을 실행할 때 ESET Security Management Center에서 검사 대상(수동 사서함 데이터베이스 검사 및 Hyper-V 검사)을 사용합니다. ESET Management Agent가 설치되어 있는 경우에만 ERA/ESMC 검사 대상 설정을 사용할 수 있으며, 그렇지 않은 경우에는 회색으로 표시됩니다.

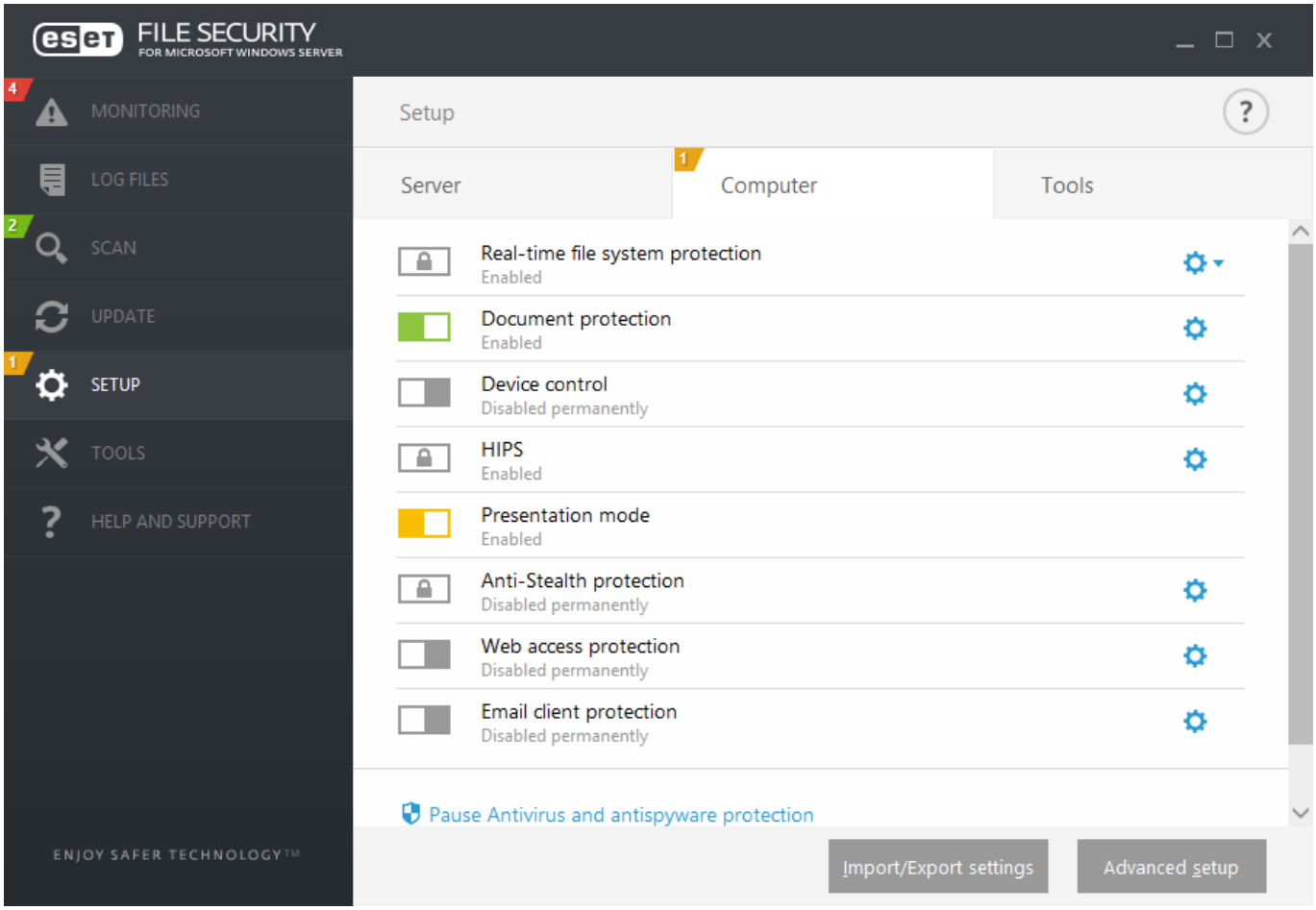
대상 목록 생성을 활성화하면 ESET File Security에서 사용할 수 있는 검사 대상 목록을 생성합니다. 이 목록은 **업데이트 기간**에 따라 주기적으로 생성됩니다.

> 참고
> **대상 목록 생성**을 처음 활성화한 경우 지정된 **업데이트 기간**의 반 정도가 경과되면 ESET Security Management Center에서 해당 작업을 수행할 수 있습니다. 따라서 **업데이트 기간**이 60분으로 설정된 경우 ERA에서 검사 대상 목록을 수신하는 데 약 30분이 걸립니다. ESET Security Management Center에서 더 일찍 목록을 수집해야 할 경우에는 업데이트 기간을 더 작은 값으로 설정하십시오. 이 값은 나중에 늘릴 수 있습니다.

ESET Security Management Center에서 **서버 검사** 클라이언트 작업을 실행하면 목록이 수집됩니다. 그러면 해당 특정 서버에서 Hyper-V 검사의 검사 대상을 선택하라는 메시지가 표시됩니다.

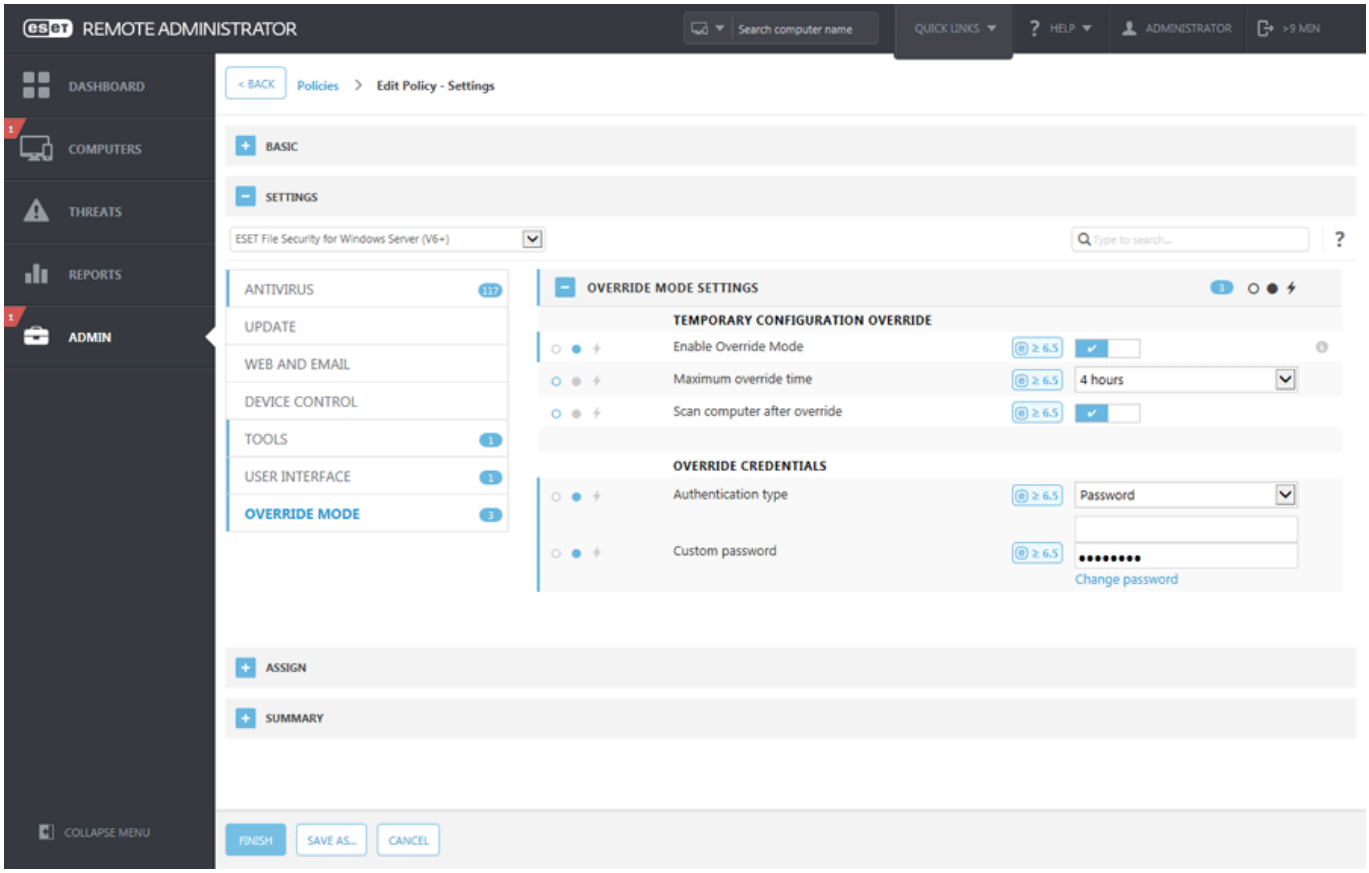
재정의 모드

ESET File Security에 ESET Security Management Center 정책이 적용된 경우 설정 페이지에 활성화/비활성화 스위치 대신 잠금 아이콘 이 표시되며, **고급 설정** 창에서는 스위치 옆에 잠금 아이콘이 표시됩니다.

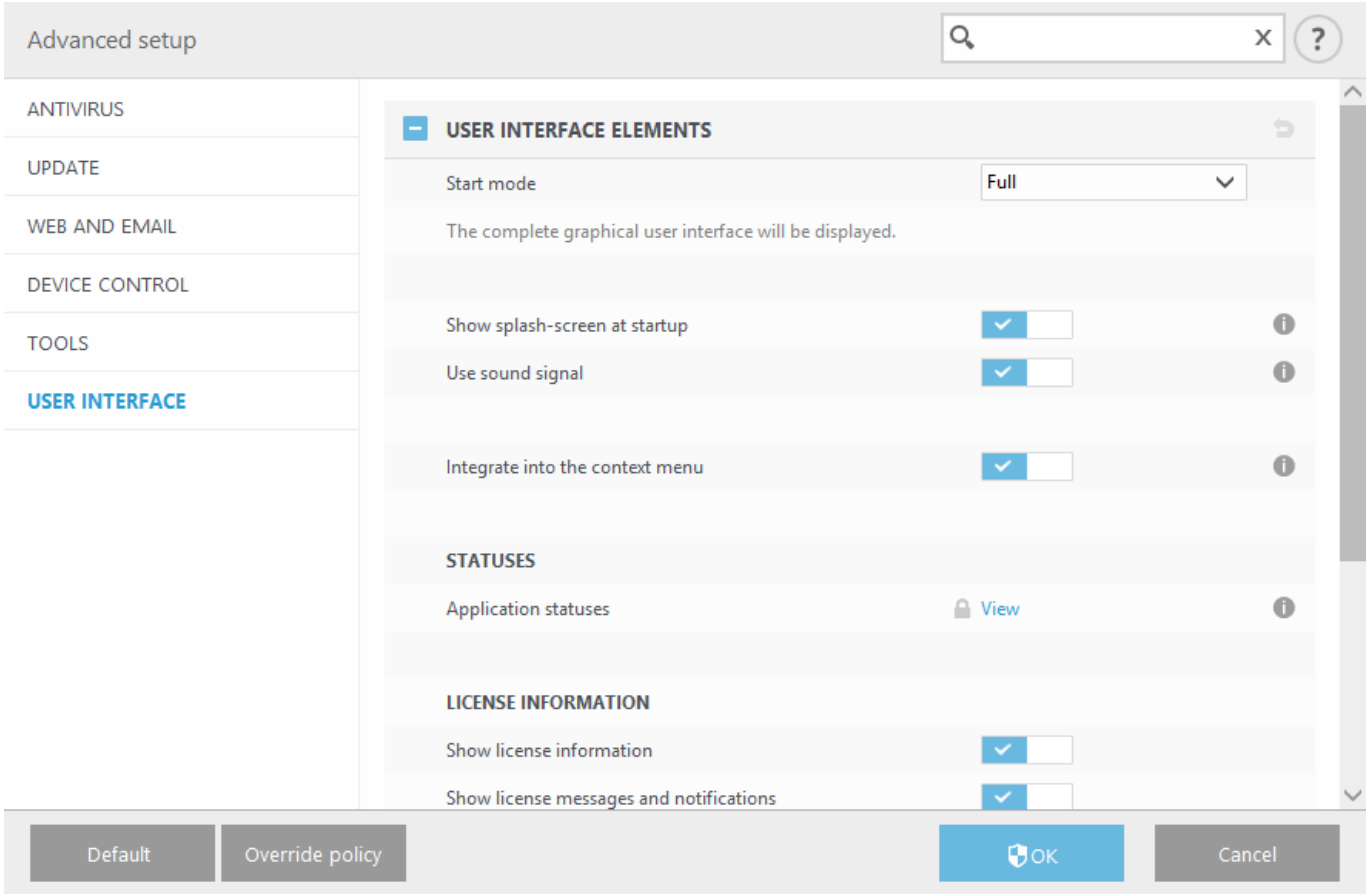


보통 ESET Security Management Center 정책을 통해 구성된 설정은 수정할 수 없습니다. 재정의 모드를 통해 이 설정을 일시적으로 잠금 해제할 수 있습니다. 단, ESET Security Management Center 정책을 사용하여 **재정의 모드**를 활성화해야 합니다.

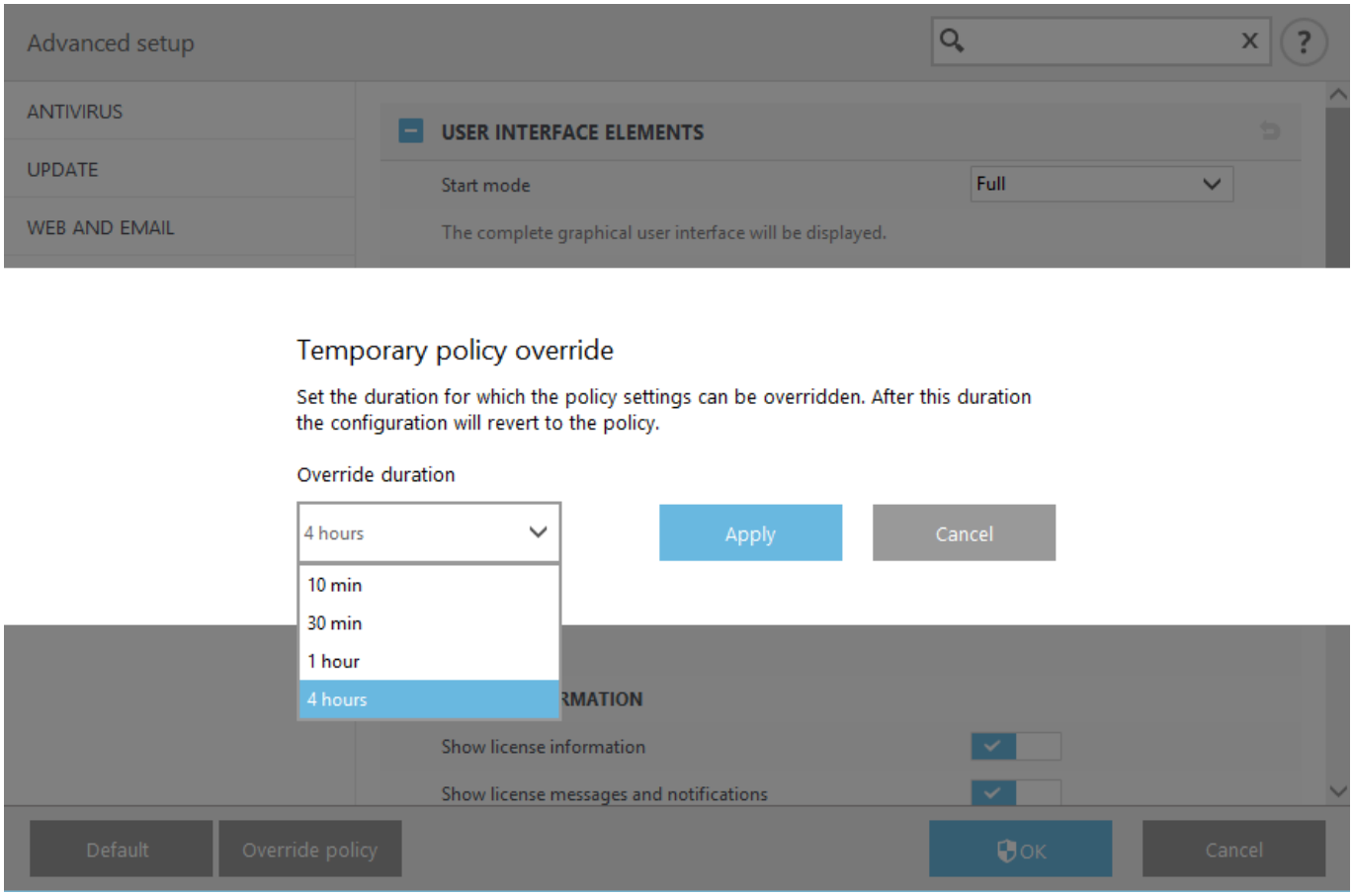
ESMC 웹 콘솔에 로그인한 후 **정책**으로 이동하고 ESET File Security에 적용된 기존 정책을 선택한 뒤 편집하거나 새 정책을 생성합니다. **설정**에서 **재정의 모드**를 클릭하고 활성화한 후 인증 유형(**Active Directory 사용자** 또는 **패스워드**)을 비롯한 나머지 설정을 구성합니다.



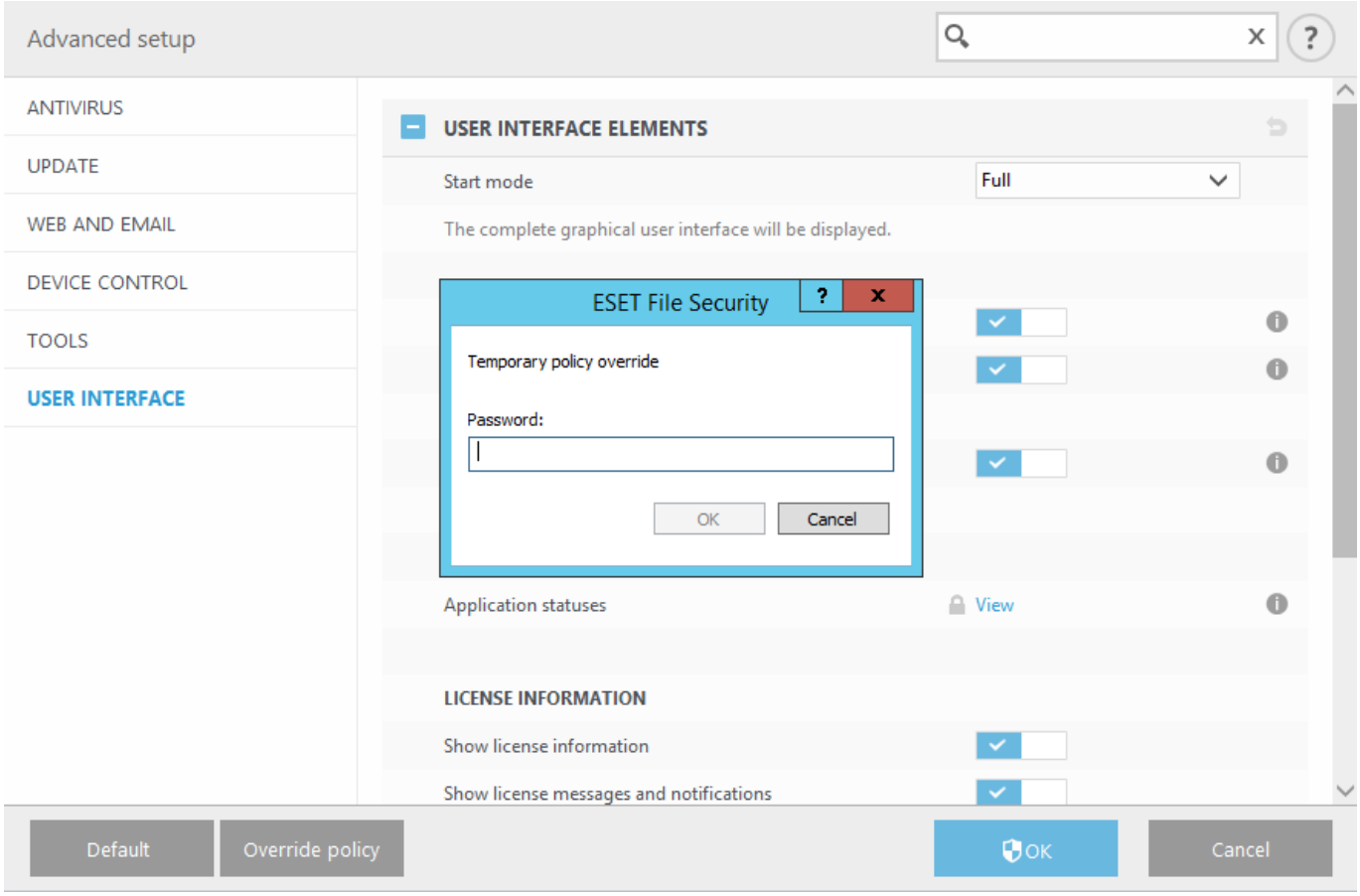
정책이 수정되거나 새 정책이 ESET File Security에 적용되면 고급 설정 창에 재정의 정책 버튼이 표시됩니다.



재정의 정책 버튼을 클릭하고 기간을 설정한 후 **적용**을 클릭합니다.



인증 유형으로 **비밀번호**를 선택한 경우 정책 재정의 비밀번호를 입력합니다.



재정의 모드가 만료되면 변경한 모든 구성이 다시 원래 ESET Security Management Center 정책 설정으로 바

뀝니다. 재정의가 만료되기 전에 알림이 표시됩니다.

재정의가 만료되기 전에 모니터링 페이지나 **고급 설정** 창에서 언제든지 **재정의 모드를 종료**할 수 있습니다.

로그 파일

이 섹션에서는 ESET File Security 로깅 구성을 수정할 수 있습니다.

로깅 필터

기본적으로 모든 로깅 옵션이 활성화되어 있기 때문에 많은 양의 데이터가 생성됩니다. 유용하지 않거나 문제와 관련이 없는 구성 요소에 대해서는 선택적으로 로깅을 비활성화하는 것이 좋습니다.

> 참고
> 실제 로깅을 시작하려면 기본 메뉴 **설정** > 도구에서 제품 수준에 대한 일반 **진단 로깅**을 켜야 합니다. 로깅이 켜져 있으면 ESET File Security에서 이 섹션에 활성화된 기능에 따라 상세 로그를 수집합니다.

스위치를 사용하여 특정 기능을 활성화하거나 비활성화할 수 있습니다. 이 옵션은 ESET File Security에서 개별 구성 요소의 가용성에 따라 결합할 수도 있습니다.

- **클러스터 진단 로깅** - 클러스터 로깅이 일반 진단 로깅에 포함됩니다.

로그 파일

로그 관리 방법을 정의합니다. 이는 디스크가 완전히 소모되지 않도록 하는 데 중요합니다. 기본 설정을 통해 오래된 로그를 자동으로 제거하여 디스크 공간을 절약할 수 있습니다.

다음 기간이 지난 기록 자동 삭제

지정된 기간(일)보다 오래된 로그 항목이 제거됩니다.

로그 크기를 초과하면 이전 기록을 자동으로 삭제

로그 크기가 **최대 로그 크기[MB]**를 초과하면 **로그 크기가 줄어듦[MB]**에 도달할 때까지 이전 로그 기록이 제거됩니다.

삭제된 기록을 자동으로 백업

로그 기록을 자동으로 제거하고 지정된 디렉터리에 파일을 백업한 후 ZIP을 사용해 압축합니다(옵션).

진단 로그 백업

제거된 진단 로그를 자동으로 백업합니다. 이 옵션을 활성화하지 않으면 진단 로그 기록이 백업되지 않습니다.

백업 폴더

로그 백업이 저장되는 폴더입니다. ZIP을 사용하여 압축된 로그 백업을 활성화할 수 있습니다.

자동으로 로그 파일 최적화

이 옵션을 선택하면 조각화 비율이 **사용되지 않는 기록 수가 (%)을(를) 초과하는 경우** 필드에 지정된 값보다 크면 로그 파일이 자동으로 조각 모음됩니다. 로그 파일 조각 모음을 시작하려면 **최적화**를 클릭합니다. 빈 로그 항목이 모두 제거되어 성능과 로그 처리 속도가 향상됩니다. 이러한 향상은 특히 로그에 포함된 항목 수가 상당히 많은 경우에 확인할 수 있습니다.

텍스트 프로토콜 활성화

로그 파일과 별도로 다른 파일 형식으로 로그를 저장할 수 있습니다.

- **대상 디렉터리** - 로그 파일이 저장되는 디렉터리입니다(**텍스트/CSV**에만 적용됨). 각 로그 섹션에는 파일 이름이 미리 정의된 고유한 파일이 포함되어 있습니다(예: 로그를 저장하는 데 일반 텍스트 파일 형식을 사용하는 경우 검출된 로그 파일 위협 섹션의 경우 *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.

참고
문제를 더 빨리 해결하는 데 도움이 되도록 ESET 기술 지원에서 컴퓨터의 로그를 제공하도록 요청할 수 있습니다. ESET Log Collector를 사용하면 필요한 정보를 쉽게 수집할 수 있습니다. ESET Log Collector에 대한 자세한 내용은 ESET의 지식베이스 문서를 참조하십시오.

프록시 서버

대규모 LAN 네트워크에서는 컴퓨터의 인터넷 연결이 프록시 설정을 통해 조정될 수 있습니다. 이 경우에는 다음 설정을 정의해야 합니다. 설정을 정의하지 않으면 프로그램을 자동으로 업데이트할 수 없습니다. ESET File Security에서 프록시 서버 설정은 **고급 설정** 창(**F5** 키) 내의 서로 다른 두 섹션에서 사용할 수 있습니다.

1. **고급 설정**(**F5** zl) > **업데이트** > **프로필** > **업데이트** > **옵션 연결** > HTTP 프록시
   이 설정은 지정한 프로필 업데이트에 적용되고, 일반적으로 다양한 위치에서 모듈을 받는 랩톱에 권장됩니다.

2. **고급 설정**(**F5** 키) > **도구** > **프록시 서버**
   이 수준에서 프록시 서버를 지정하면 모든 ESET File Security에 대한 전체 프록시 서버 설정이 정의됩니다. 여기의 파라미터는 인터넷에 연결되는 모든 모듈에서 사용됩니다.

이 수준에 대한 프록시 서버 설정을 지정하려면 **프록시 서버 사용** 스위치를 켠 다음 **프록시 서버** 필드에 프록시 서버 주소와 프록시 서버의 **포트** 번호를 입력합니다.

프록시 서버에 인증 필요

프록시 서버를 통한 네트워크 통신에 인증이 필요한 경우 이 옵션을 활성화하고 **사용자 이름**과 **패스워드**를 지정합니다.

프록시 서버 검색

프록시 서버 설정을 자동으로 검색하여 입력하려면 **검색**을 클릭합니다. Internet Explorer에 지정된 파라미터가 복사됩니다.

> 참고
> 이 기능은 인증 데이터(사용자 이름과 패스워드)를 검색하지 않으므로 사용자가 입력해야 합니다.

프록시를 사용할 수 없는 경우 직접 연결 사용

제품이 HTTP 프록시를 활용하도록 구성되어 있는데 프록시에 연결할 수 없는 경우 제품은 프록시를 우회하고 ESET 서버와 직접 통신합니다.

알림

바탕 화면의 알림과 풍선 팁은 정보를 제공하기 위한 것일 뿐이며, 사용자 상호 작용이 필요하지 않습니다. 이들 항목은 화면 오른쪽 아래의 알림 영역에 표시됩니다. 알림 표시 시간 및 창 투명도 등의 자세한 옵션은 아래에서 수정할 수 있습니다. 모든 비대화 알림이 표시되지 않도록 하려면 **전체 화면 모드로 애플리케이션을 실행할 때 알림 표시 안 함** 스위치를 켭니다.

성공한 업데이트에 대한 알림 표시

업데이트가 완료되면 팝업 알림이 표시됩니다.

이메일로 이벤트 알림 보내기

이메일 알림을 활성화할 수 있습니다.

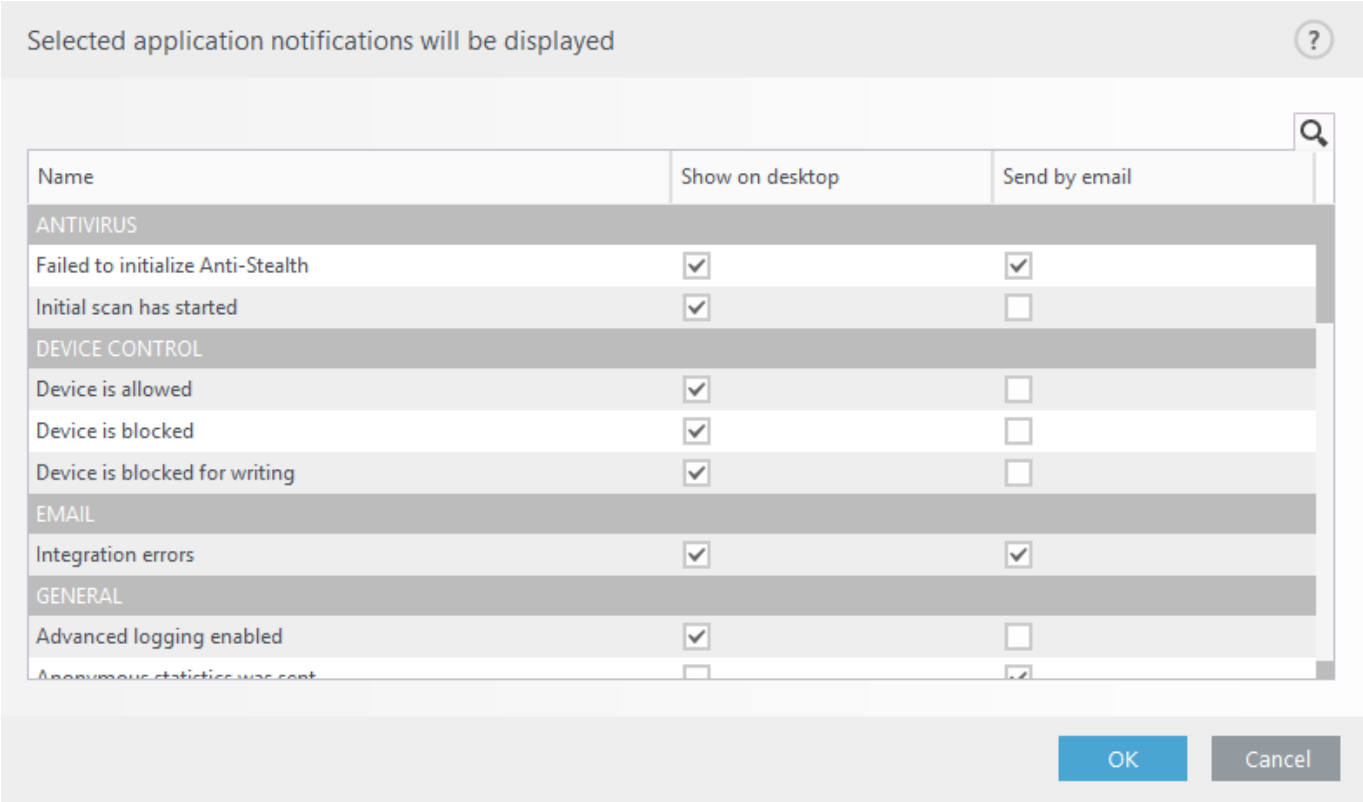
애플리케이션 알림

편집을 클릭하여 애플리케이션 알림 표시를 활성화하거나 비활성화할 수 있습니다.

애플리케이션 알림

바탕 화면에 표시 및/또는 이메일로 보낼 ESET File Security 알림을 구성할 수 있습니다.

> 참고
> 이메일 알림의 경우 **기본** 섹션에서 **이메일로 이벤트 알림 보내기**를 활성화한 다음 SMTP 서버 구성 및 기타 세부 정보(필요한 경우)를 활성화해야 합니다.



바탕 화면 알림

위협 경고 및 시스템 알림(예: 업데이트 성공 메시지)이 ESET File Security에서 처리되는 방식을 구성할 수 있습니다. 예로 시스템 트레이 알림의 표시 시간 **기간**과 **투명도**를 들 수 있습니다. 이러한 설정은 시스템 트레이 알림을 지원하는 시스템에만 적용됩니다.

표시할 이벤트의 최소 상세 수준 드롭다운 메뉴에서 경고 및 알림의 심각도 수준을 선택할 수 있습니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **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.
- **중요** - 심각한 오류만 기록합니다.

다중 사용자 시스템에서 이 사용자의 화면에 알림 표시 필드에 여러 사용자가 동시에 연결할 수 있도록 허용하는 시스템에서 시스템 및 기타 알림을 받을 사용자를 지정합니다. 일반적으로 이 사용자는 시스템 및 네트워크 관리자가 됩니다. 이 옵션은 모든 시스템 알림을 관리자에게 보내는 경우의 터미널 서버에 특히 유용합니다.

이메일 알림

선택한 상세 수준의 이벤트가 발생하는 경우 ESET File Security에서 알림 이메일을 자동으로 보낼 수 있습니다.

> 참고
> TLS 암호화를 사용하는 SMTP 서버는 ESET File Security에서 지원됩니다.

SMTP 서버

경고 및 알림을 보내는 데 사용되는 SMTP 서버의 이름입니다. 일반적으로 Microsoft Exchange Server의 이름입니다.

사용자 이름 및 패스워드

SMTP 서버에 인증이 필요한 경우 SMTP 서버에 접근하는 데 유효한 사용자 이름과 패스워드를 이러한 필드에 입력해야 합니다.

보낸 사람 주소

알림 이메일 헤더에 나타나는 보낸 사람 주소를 입력합니다. 받는 사람 입장에서 **보낸 사람** 필드에 표시되는 항목입니다.

받는 사람 주소

알림이 전달되는 **받는 사람** 이메일 주소를 지정합니다.

TLS 활성화

TLS 암호화에서 지원되는 경고 및 알림 메시지를 활성화합니다.

이메일 설정

알림의 최소 상세 수준

보낼 알림의 최소 상세 수준을 지정합니다.

새 알림 이메일을 보낸 후 간격(분)

새 알림이 이메일을 통해 전송되는 간격(분)입니다. 이러한 알림을 즉시 전송하려면 이 값을 0으로 설정합니다.

각 알림을 별도의 이메일로 보내기

활성화된 경우 받는 사람은 각 개별 알림에 대해 새 이메일을 수신하게 됩니다. 따라서 짧은 시간에 여러 이메일이 수신될 수 있습니다.

메시지 형식

프로그램과 원격 사용자 또는 시스템 관리자 간의 통신은 Windows 메신저 서비스를 사용하여 이메일 또는 LAN 메시지를 통해 수행됩니다. 대부분의 경우 기본 경고 메시지 및 알림 형식을 사용하면 가장 적합합니다. 일부 경우 이벤트 메시지의 메시지 형식을 변경해야 할 수 있습니다.

이벤트 메시지 형식

원격 컴퓨터에 표시되는 이벤트 메시지의 형식입니다.

위협 경고 메시지 형식

위협 경고 및 알림 메시지에는 미리 정의된 기본 형식이 있습니다. 이 형식은 변경하지 않는 것이 좋습니다. 그러나 자동화된 이메일 처리 시스템을 사용하는 등의 일부 경우에는 메시지 형식을 변경해야 할 수 있습니다.

% 기호로 구분되는 문자열인 키워드는 메시지에서 지정된 실제 정보로 바뀝니다. 다음과 같은 키워드를 사용할 수 있습니다.

- **%TimeStamp%** - 이벤트의 날짜 및 시간입니다.
- **%Scanner%** - 관련 모듈입니다.
- **%ComputerName%** - 경고가 발생한 컴퓨터의 이름입니다.
- **%ProgramName%** - 경고를 생성한 프로그램입니다.
- **%InfectedObject%** - 감염된 파일이나 메시지 등의 이름입니다.
- **%VirusName%** - 감염 ID입니다.
- **%ErrorDescription%** - 바이러스가 아닌 이벤트의 설명입니다.

키워드 **%InfectedObject%** 및 **%VirusName%**은 위협 경고 메시지에만 사용되고 **%ErrorDescription%**은 이벤트 메시지에만 사용됩니다.

문자 집합

드롭다운 메뉴에서 인코딩을 선택할 수 있습니다. 이메일 메시지는 선택한 문자 인코딩에 따라 변환됩니다.

QP(Quoted-Printable) 인코딩 사용

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

사용자 지정

이 메시지는 선택된 모든 알림의 꼬리말에 표시됩니다.

기본 알림 메시지

알림 바닥글에 표시되는 기본 메시지입니다.

위협

맬웨어 알림을 자동으로 닫지 않음

화면을 수동으로 닫을 때까지 화면에 유지할 악성코드 알림을 활성화합니다.

기본 메시지 사용

기본 메시지를 해제하고 위협을 차단하면 표시될 사용자 지정 **위협 알림 메시지**를 지정할 수 있습니다.

위협 알림 메시지

위협이 차단될 때 표시할 사용자 지정 메시지를 입력하십시오.

프레젠테이션 모드

프리젠테이션 모드는 소프트웨어를 중단 없이 사용하고 팝업 창의 방해를 받지 않으며 CPU의 사용을 최소화하려는 사용자를 위한 기능입니다. 프리젠테이션 모드는 ESET File Security 활동으로 중단될 수 없는 프리젠테이션 동안 사용할 수도 있습니다. 프리젠테이션 모드를 활성화하면 모든 팝업 창이 비활성화되고 예약된 작업이 실행되지 않습니다. 시스템 보호 기능은 백그라운드에서 계속해서 실행되지만, 사용자 상호 작용을 필요로 하지 않습니다.

전체 화면 모드로 애플리케이션을 실행할 때 자동으로 프레젠테이션 모드 활성화

전체 화면 애플리케이션을 실행할 때마다 프리젠테이션 모드가 자동으로 활성화됩니다. 프리젠테이션 모드를 사용하면 알림 또는 ESET File Security의 상태 변화를 볼 수 없습니다.

다음 시간 후 자동으로 프레젠테이션 모드 비활성화

프리젠테이션 모드가 자동으로 비활성화되는 시간(분)을 정의할 수 있습니다.

분석

분석은 ESET 프로세스의 애플리케이션 크래시 덤프(예: *ekrn*)를 제공합니다. 애플리케이션이 충돌하면 덤프가 생성됩니다. 따라서 개발자는 다양한 ESET File Security 문제를 디버깅하고 해결할 수 있습니다.

덤프 유형 옆의 드롭다운 메뉴를 클릭하고 다음의 사용 가능한 세 가지 옵션 중 하나를 선택합니다.

- **비활성화** - 이 기능을 비활성화합니다.
- **일부**(기본값) - 애플리케이션이 예기치 않게 충돌한 이유를 식별하는 데 도움이 될 수 있는 유용한 정보의 최소 집합을 기록합니다. 이 덤프 파일 종류는 공간이 제한되어 있을 때 유용할 수 있습니다. 그러나 포함된 정보가 제한되어 있어 이 파일을 분석할 때 문제 발생 시 실행 중이던 스레드에 의해 직접적으로 유발되지 않은 오류는 발견되지 않을 수 있습니다.
- **전체** - 애플리케이션이 예기치 않게 중지되면 시스템 메모리의 전체 내용을 기록합니다. 메모리 덤프 완료에는 메모리 덤프가 수집될 때 실행 중이던 프로세스의 데이터가 포함될 수 있습니다.

대상 디렉터리

충돌 중 덤프가 생성되는 디렉터리입니다.

분석 폴더 열기

새 *Windows* 탐색기 창에서 이 디렉터리를 열려면 **열기**를 클릭합니다.

분석 덤프 생성

생성을 클릭하여 대상 디렉터리에 분석 덤프 파일을 생성합니다.

고급 로깅

장치 제어 고급 로깅 활성화

장치 제어에서 발생하는 모든 이벤트를 기록하여 진단 및 문제 해결을 가능하게 합니다.

커널 고급 로깅 활성화

문제를 진단하고 해결할 수 있도록 ESET 커널 서비스(ekrn)에서 발생하는 모든 이벤트를 기록합니다.

라이선스 고급 로깅 활성화

라이선스 서버와의 모든 제품 통신을 기록합니다.

네트워크 보호 고급 로깅 활성화

개발자들이 네트워크 보호와 관련된 문제를 진단하고 해결하는 데 도움이 될 수 있도록 네트워크 보호를 통과하는 모든 네트워크 데이터를 PCAP 형식으로 기록합니다.

운영 체제 고급 로깅 활성화

실행 중인 프로세스, CPU 활동, 디스크 작동과 같은 운영 체제에 대한 추가 정보가 수집됩니다.

프로토콜 필터링 고급 로깅 활성화

개발자들이 프로토콜 필터링과 관련된 문제를 진단하고 해결하는 데 도움이 될 수 있도록 프로토콜 필터링 엔진을 통과하는 모든 데이터를 PCAP 형식으로 기록합니다.

업데이트 엔진 고급 로깅 활성화

개발자들이 업데이트 엔진과 관련된 문제를 진단하고 해결하는 데 도움이 될 수 있도록 업데이트 프로세스 중에 발생하는 모든 이벤트를 기록합니다.

기술 지원

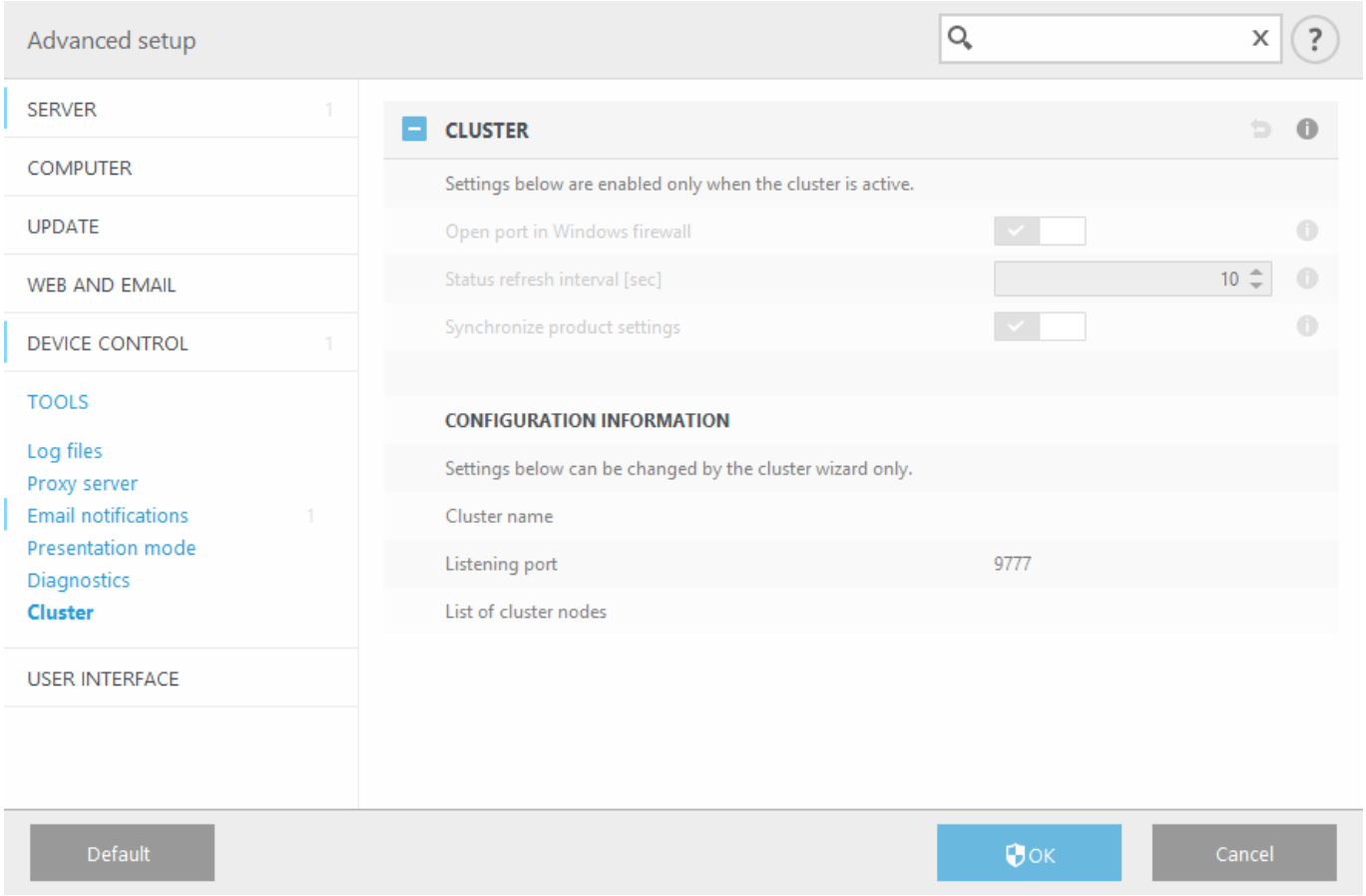
시스템 구성 데이터 전송

ESET File Security 구성 데이터를 고객 지원에 전송하기 전에 메시지를 표시하지 않는 **항상 전송**을 선택하거나, **제출 전 확인**을 사용합니다.

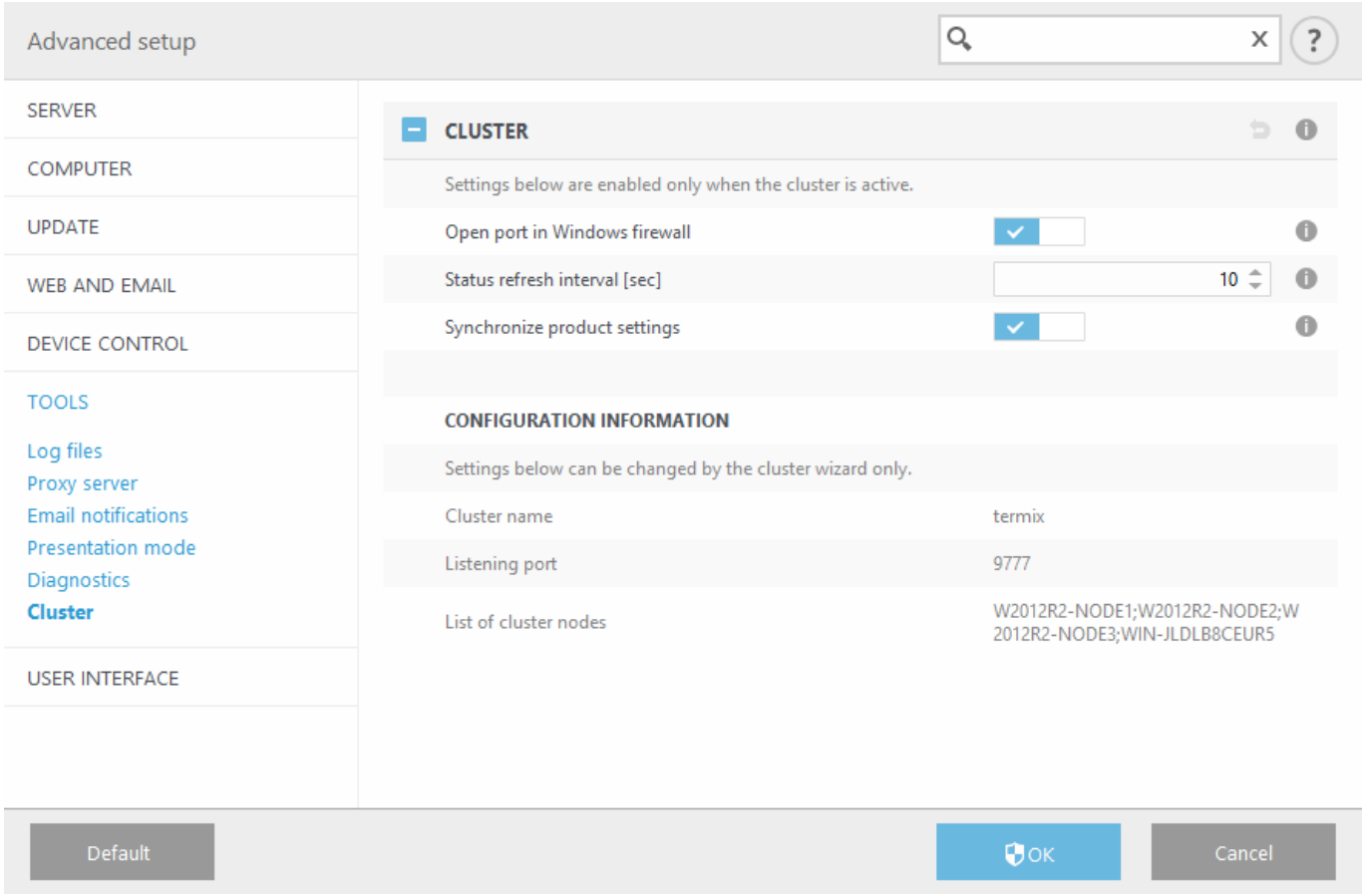
클러스터

ESET 클러스터가 구성되면 클러스터 활성화가 자동으로 활성화됩니다. 이 옵션은 전환 아이콘을 클릭하여 **고급 설정**(**F5** 키) 창에서 수동으로 비활성화할 수 있습니다(예: ESET 클러스터의 다른 노드에 영향을 주지 않고 구성을 변경해야 할 경우). 이 전환은 ESET 클러스터 기능을 활성화하거나 비활성화하기만 합니다. 클러스터를 설정 또는 폐기하려면 클러스터 마법사를 사용하거나 기본 프로그램 창의 **도구 > 클러스터** 섹션에 있는 클러스터 **폐기**를 사용합니다.

다음 그림은 ESET 클러스터가 구성되어 있지 않고 비활성화된 경우를 나타냅니다.



다음 그림은 ESET 클러스터가 상세 정보와 옵션으로 올바르게 구성된 경우입니다.



사용자 인터페이스

ESET File Security의 GUI(그래픽 사용자 인터페이스) 동작을 구성합니다. 프로그램의 시각적 모양 및 효과를 조정할 수 있습니다.

사용자 인터페이스 요소

GUI 시작 모드 드롭다운 메뉴를 사용하여 다음 GUI(그래픽 사용자 인터페이스) 시작 모드 중에서 선택합니다.

- **전체** - 완전한 GUI가 표시됩니다.
- **터미널** - 알림이나 경고가 표시되지 않습니다. 관리자만 GUI를 시작할 수 있습니다. 그래픽 요소가 컴퓨터 성능을 저해하거나 다른 문제를 유발하는 경우 사용자 인터페이스를 터미널로 설정해야 합니다. 터미널 서버에서도 GUI를 끌 수 있습니다. 터미널 서버에 설치된 ESET File Security에 대한 자세한 내용은 터미널 서버에서 GUI 비활성화 항목을 참조하십시오.

시작할 때 시작 화면 표시

ESET File Security의 GUI가 시작할 때(예: 시스템에 로그인할 때) 시작 화면이 표시되는 것을 원하지 않는 경우 이 옵션을 비활성화합니다.

신호음 사용

검사 중에 중요한 이벤트가 발생할 경우(예: 위협이 검색되거나 검사가 완료된 경우) ESET File Security에서 신호음을 울립니다.

오른쪽 마우스 버튼 메뉴로 통합

활성화하면 ESET File Security 검사 요소가 오른쪽 마우스 버튼 메뉴로 통합됩니다. 개체(파일)를 오른쪽 마우스 버튼으로 클릭하면 오른쪽 마우스 버튼 메뉴가 표시됩니다. 메뉴에는 개체에서 수행할 수 있는 모든 동작이 나열됩니다.

애플리케이션 상태

편집을 클릭하여 모니터링 창에 표시되는 상태를 선택합니다. 또는 ESET Security Management Center 정책을 사용하여 애플리케이션 상태를 구성할 수 있습니다. 애플리케이션 상태는 제품이 활성화되어 있지 않거나 라이선스가 만료된 경우에도 표시됩니다.

라이선스 정보/라이선스 정보 표시

활성화하면 라이선스에 대한 메시지와 알림이 표시됩니다.

경고 및 메시지 상자

경고 및 알림을 구성하여 검출된 위협 경고 및 시스템 알림의 동작을 변경할 수 있습니다. 필요에 맞게 이러한 동작을 사용자 지정할 수 있습니다. 일부 알림을 표시하지 않도록 선택하면 이러한 알림은 비활성화된 메시지 및 상태 영역에 표시됩니다. 여기서 해당 알림 상태를 확인하고 상세 정보를 표시하거나 이 창에서 해당 알림을 제거할 수 있습니다.

접근 설정

최대 보안 성능을 제공하도록 접근 설정 도구를 사용하여 무단 변경을 방지할 수 있습니다.

ESET Shell

ESET Shell 실행 정책을 변경하여 eShell을 통해 제품 설정, 기능 및 데이터에 대한 접근 권한을 구성할 수 있습니다.

시스템 트레이 아이콘

이 섹션의 모든 설정 되돌리기

경고 및 메시지 상자

위협 경고 및 시스템 알림(예: 업데이트 성공 메시지)이 ESET File Security에서 처리되는 방식을 구성할 수 있습니다. 예로 시스템 트레이 알림의 표시 시간 **기간**과 **투명도**를 들 수 있습니다. 이러한 설정은 시스템 트레이 알림을 지원하는 시스템에만 적용됩니다.

대화형 경고 표시

ESET File Security가 Windows 알림 영역에 알림을 표시하지 않게 하려면 이 기능을 비활성화하십시오.

대화형 경고 목록

자동화에 유용합니다. 자동화할 항목은 **사용자에게 요청**을 선택 해제하고, 상호작용을 기다리는 경고 창 대신 수행할 작업을 선택합니다.

메시지 상자에는 짧은 텍스트 메시지나 질문이 표시됩니다.

자동으로 메시지 상자 닫기

일정 시간이 경과하면 팝업 창을 자동으로 닫을 수 있습니다. 팝업 창을 수동으로 닫지 않은 경우 지정된 시간이 경과하면 경고 창이 자동으로 닫힙니다.

확인 메시지

편집을 클릭하면 동작을 수행하기 전에 ESET File Security에서 표시되는 확인 메시지 목록과 함께 팝업 창이 열립니다. 확인란을 사용하여 확인 메시지의 기본 설정을 사용자 지정할 수 있습니다.

접근 설정

시스템을 최대한 보호하기 위해서는 ESET File Security를 올바로 구성해야 합니다. 잘못 수정하면 문제가 발생하거나 중요한 데이터가 손실될 수도 있습니다. 잘못 수정하는 일을 방지하기 위해 ESET File Security 구성을 패스워드로 보호할 수 있습니다.

> 중요
> 접근 설정 패스워드 보호를 사용하는 중에 ESET File Security를 제거하면 패스워드를 입력하라는 메시지가 표시됩니다. 그렇지 않으면 ESET File Security를 제거할 수 없습니다.

비밀번호 보호 설정

프로그램의 설정 파라미터를 잠금/잠금 해제합니다. **패스워드 설정** 창을 열려면 클릭합니다.

비밀번호 설정

설정 파라미터를 보호하기 위한 패스워드를 설정하거나 변경하려면 **설정**을 클릭합니다. 무단 수정을 방지하기 위해 ESET File Security의 설정 파라미터를 보호하려면 새 패스워드를 설정해야 합니다. 기존 패스워드를 변경하려면 **현재 패스워드** 필드에 현재 패스워드를 입력하고 **새 패스워드** 및 **패스워드 확인** 필드에 새 패스워드를 입력한 다음 **확인**을 클릭합니다. 이 패스워드는 나중에 ESET File Security를 수정할 때 필요합니다.

제한된 관리자 계정을 사용하려면 전체 관리자 권한 필요

현재 사용자(관리자 권한이 없는 경우)에게 보호 모듈을 비활성화하는 등의 특정 파라미터를 수정할 때 관리자 계정 자격 증명을 입력하라는 메시지를 표시하려면 이 옵션을 선택합니다.

> 참고
> 접근 설정 비밀번호가 변경되고 ESET CMD 명령줄을 사용하여 기존의 *.xml* 구성 파일을 가져오려면(비밀번호가 변경되기 전에 지문이 생성된 구성 파일) 현재 비밀번호를 사용하여 이 구성 파일에 대해 다시 지문을 생성해야 합니다. 그러면 구성을 가져오기 전에 ESET File Security를 실행하는 다른 컴퓨터에서 구성을 내보내지 않고도 이전 구성 파일을 사용할 수 있습니다.

ESET Shell

ESET Shell 실행 정책을 변경하여 eShell을 통해 제품 설정, 기능 및 데이터에 대한 접근 권한을 구성할 수 있습니다. 기본 설정은 **제한된 스크립팅**이지만 필요한 경우 비활성화됨, 읽기 전용 또는 전체 권한으로 설정을 변경할 수 있습니다.

비활성화됨

eShell을 전혀 사용할 수 없습니다. eShell 자체 구성만 허용됩니다(`ui eshell` 컨텍스트). eShell의 모양을 사용자 지정할 수 있지만 제품 설정이나 데이터에는 접근할 수 없습니다.

읽기 전용

eShell을 모니터링 도구로 사용할 수 있습니다. 대화 모드 및 배치 모드 둘 다에서 모든 설정을 볼 수 있지만 설정이나 기능 또는 데이터를 수정할 수는 없습니다.

제한된 스크립팅

대화 모드에서 모든 설정, 기능 및 데이터를 보고 수정할 수 있습니다. 배치 모드에서 eShell은 읽기 전용 모드에 있는 것처럼 작동하지만 지문이 생성된 배치 파일을 사용하는 경우 설정을 편집하고 데이터를 수정할 수 있습니다.

전체 권한

대화 모드 및 배치 모드 둘 다에서(배치 파일을 실행할 때) 제한 없이 모든 설정에 접근할 수 있습니다. 또한 모든 설정을 보고 수정할 수 있습니다. 전체 권한으로 eShell을 실행하려면 관리자 계정을 사용해야 합니다. UAC가 활성화된 경우 권한 상승도 필요합니다.

터미널 서버에서 GUI 비활성화

이 장에서는 사용자 세션의 Windows 터미널 서버에서 실행되는 ESET File Security의 GUI를 비활성화하는 방법을 설명합니다.

보통 ESET File Security GUI는 원격 사용자가 서버에 로그온하여 터미널 세션을 생성할 때마다 시작됩니다. 이는 터미널 서버에 적합하지 않은 경우가 대부분입니다. 터미널 세션 GUI를 끄려면 eShell을 사용하여 `set ui ui gui-start-mode none` 명령을 실행할 수 있습니다. 그러면 GUI가 터미널 모드로 설정됩니다. GUI 시작 시 다음과 같은 두 가지 모드를 사용할 수 있습니다.

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

현재 사용되고 있는 모드를 확인하려면 `get ui ui gui-start-mode` 명령을 실행합니다.

> 참고
> Citrix 서버에 ESET File Security를 설치한 경우 ESET의 지식 베이스 문서에 설명된 설정을 사용하는 것이 좋습니다.

비활성화된 메시지 및 상태

확인 메시지

표시하거나 표시하지 않도록 선택할 수 있는 확인 메시지 목록을 표시합니다.

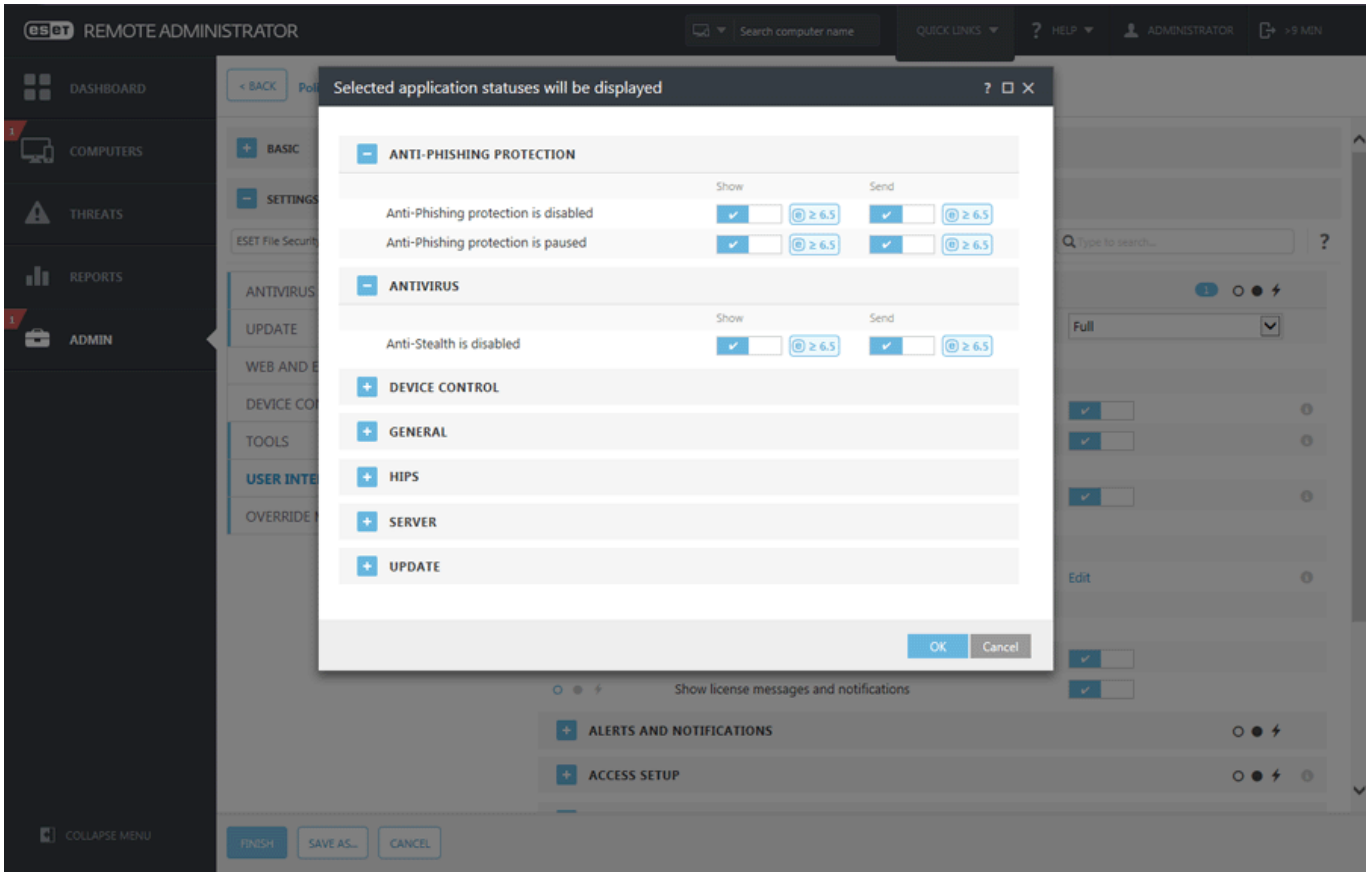
애플리케이션 상태 설정

기본 메뉴의 모니터링 페이지에서 표시 상태를 활성화하거나 비활성화할 수 있습니다.

애플리케이션 상태 설정

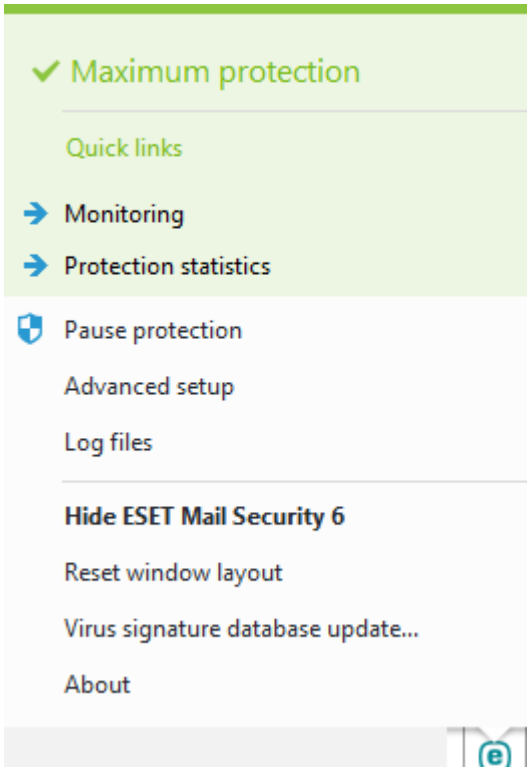
이 대화 상자 창에서는 표시하거나 표시하지 않을 애플리케이션 상태를 선택하거나 선택 취소할 수 있습니다. 예를 들어 안티바이러스 및 안티스파이웨어 보호를 일시 중지하면 모니터링 페이지에 표시되는 보호 상태가 바뀝니다. 애플리케이션 상태는 제품이 활성화되지 않았거나 라이선스가 만료된 경우에도 표시됩니다.

애플리케이션 상태는 ESET Security Management Center 정책을 통해 관리할 수 있습니다. 범주와 상태가 목록에 표시되며 이 목록에는 상태를 **표시**하는 옵션 및 **보내는** 옵션 등 두 개의 옵션이 있습니다. 애플리케이션 상태의 보내기 열은 ESET Security Management Center 정책 구성에만 표시됩니다. ESET File Security에는 잠금 아이콘이 포함된 설정이 표시됩니다. 재정의 모드를 사용하여 애플리케이션 상태를 일시적으로 변경할 수 있습니다.



시스템 트레이 아이콘

ESET File Security에서 자주 사용되는 항목과 기능에 빠르게 접근할 수 있도록 해 줍니다. 시스템 트레이 아이콘을 마우스 오른쪽 버튼으로 클릭하여 사용할 수 있습니다.



추가 정보

현재 보호 상태와 메시지를 표시하려면 모니터링 페이지를 엽니다.

보호 일시 중지

파일,웹 및 이메일 통신을 검사하여 공격으로부터 보호하는 안티바이러스 및 안티스파이웨어 보호를 비활성화하는 확인 대화 상자를 표시합니다. 시스템 트레이 아이콘ⓔ을 사용하여 안티바이러스 및 안티스파이웨어 보호를 일시 중지하면 **보호 일시 중지** 대화 상자가 나타납니다. 이를 통해 선택한 기간 동안 악성코드 관련 보호 기능을 비활성화할 수 있습니다. 보호를 영구적으로 비활성화하려는 경우**고급 설정**에서 이 작업을 수행할 수 있습니다. 보호를 비활성화할 경우 주의하십시오. 시스템이 위협에 노출됩니다.

고급 설정

고급 설정을 실행하려면 이 옵션을 사용합니다.

로그 파일

발생한 모든 중요 프로그램 이벤트에 대한 정보를 포함하며 검출된 위협에 대한 개요를 제공합니다.

ESET File Security 숨기기

화면에서 ESET File Security 창을 숨깁니다.

창 레이아웃 초기화

ESET File Security 창을 기본 크기로 다시 설정하고 화면에서의 위치를 다시 설정합니다.

업데이트 확인

모듈 업데이트를 시작하여 악성 코드에 대한 보호 수준을 보장합니다.

정보

시스템 정보, 설치된 ESET File Security 버전과 설치된 프로그램 모듈에 대한 상세 정보 및 라이선스 만료 날짜를 제공합니다. 운영 체제와 시스템 리소스에 대한 정보는 페이지 아래쪽에서 찾을 수 있습니다.

기본 설정으로 되돌리기

고급 설정 내에 해당하는 기본값으로 설정을 복원할 수 있습니다. 여기에는 두 가지 옵션이 있습니다. 모든 설정을 기본값으로 되돌리거나, 특정 섹션의 설정(변경되지 않은 상태로 남아 있게 되는 다른 섹션의 설정)만 되돌릴 수 있습니다.

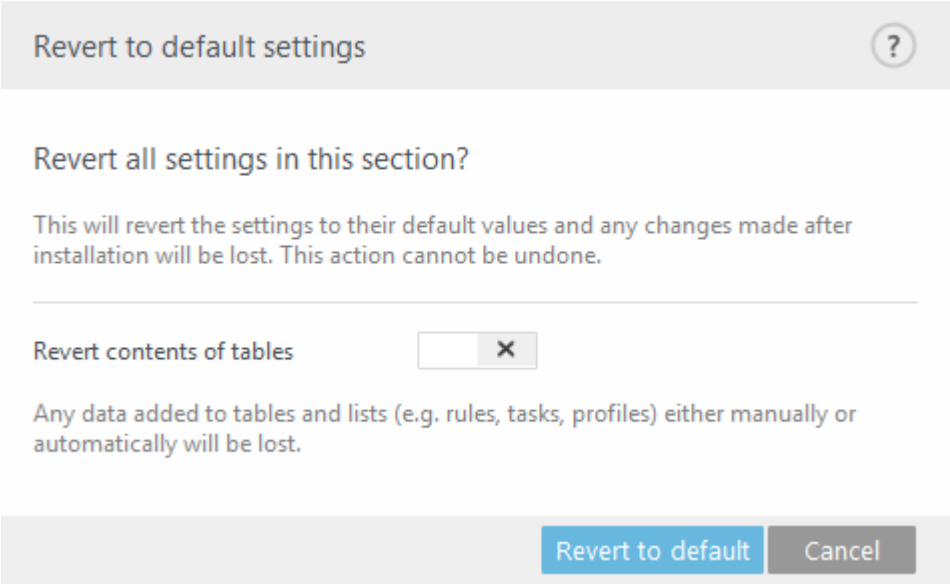
모든 설정 되돌리기

고급 설정의 모든 섹션에 있는 전체 설정이 ESET File Security를 설치한 후에 설정되었던 상태로 복원됩니다. 기본 설정으로 복원으로 생각할 수 있습니다.

> 참고
> **기본값으로 되돌리기**를 클릭하면 변경한 모든 내용이 손실됩니다. 이 동작은 실행 취소할 수 없습니다.

이 섹션의 모든 설정 되돌리기

선택한 섹션의 모듈 설정을 값으로 되돌립니다. 이 섹션에서 변경한 모든 내용이 손실됩니다.



테이블 내용 되돌리기

활성화하면 수동 또는 자동으로 추가한 규칙이나 작업, 프로필이 손실됩니다.

도움말 및 지원

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

도움말

ESET 지식베이스 검색

ESET 지식베이스에는 다양한 문제에 대한 질문과 대답 및 권장 해결 방법이 포함되어 있습니다. 지식베이스는 ESET 기술 전문가가 정기적으로 업데이트하기 때문에 다양한 유형의 문제를 해결하는 가장 강력한 도구입니다.

도움말 열기

ESET File Security에 대한 온라인 도움말 페이지를 시작합니다.

빠른 해결 찾기

가장 자주 발생하는 문제의 해결책을 찾으려면 이 옵션을 선택합니다. 기술 지원부에 문의하기 전에 이 섹션을 읽어보는 것이 좋습니다.

기술 지원

지원 요청 전송

문제에 대한 답변을 찾지 못한 경우 ESET 웹 사이트에 있는 이 양식을 사용하여 기술 지원부로 신속하게

문의할 수도 있습니다.

기술 지원에 대한 상세 정보

기술 지원에 필요한 상세 정보(제품 이름, 제품 버전 등)를 표시합니다.

지원 도구

위협 백과 사전

ESET 위협 백과 사전으로 연결되는 링크이며, 이 백과 사전에는 다양한 유형의 침입에 대한 위험 및 증상과 관련된 정보가 수록되어 있습니다.

ESET Log Collector

ESET Log Collector 다운로드 페이지에 연결됩니다. Log Collector는 더욱 신속하게 문제를 해결하기 위해 서버에서 구성 및 로그와 같은 정보를 자동으로 수집하는 애플리케이션입니다.

탐지 엔진 기록

ESET 검색 모듈 버전에 대한 정보가 포함된 ESET 바이러스 레이더에 연결됩니다.

ESET Specialized Cleaner

ESET 특수 클리너는 Conficker, Sirefef, Necurs 등의 일반적인 악성코드 감염을 제거하는 도구입니다.

제품 및 라이선스 정보

제품 활성화 / 라이선스 변경

제품 활성화 창을 시작하려면 클릭합니다. ESET File Security를 활성화하는 데 사용할 수 있는 방법 중 하나를 선택합니다.

ESET File Security 정보

ESET File Security 복사본에 대한 정보를 표시합니다.

지원 요청 전송

ESET에서 최대한 빠르고 정확하게 지원을 제공하려면 ESET File Security 구성 정보, 상세한 시스템 정보, 실행 중인 프로세스(ESET SysInspector 로그 파일) 및 레지스트리 데이터가 필요합니다. ESET에서는 고객에게 기술적인 지원을 제공하는 용도로만 이 데이터를 사용합니다. 이 설정은 **고급 설정**(**F5** 키) > **도구** > **진단** > **기술 지원**에서도 구성할 수 있습니다.

> 참고
> 시스템 데이터를 전송하도록 선택했으면 웹 양식을 입력하고 전송해야 합니다. 그렇지 않으면 티켓이 생성되지 않으며 시스템 데이터가 손실됩니다.

웹 양식 전송 시 시스템 구성 데이터가 ESET으로 전송됩니다. 이 프로세스에 대해 이 동작을 저장하려면 **항상 이 정보 전송**을 선택합니다.

데이터 전송 안 함

데이터를 전송하지 않으려면 이 옵션을 사용합니다. ESET 기술 지원 웹 페이지로 리디렉션됩니다.

ESET File Security 정보

이 창에는 설치된 ESET File Security 버전에 대한 세부 정보가 제공되며 창의 상단에서는 운영 체제와 시스템 리소스에 대한 정보, 현재 사용자와 전체 컴퓨터 이름을 볼 수 있습니다.

설치된 구성 요소

모듈에 대한 정보를 포함하여 설치된 구성 요소의 목록과 각각의 상세 정보를 볼 수 있습니다. 클립보드에 목록을 복사하려면 **복사**를 클릭합니다. 이 기능은 문제 해결 시 또는 기술 지원부에 문의할 때 유용할 수 있습니다.

용어집

기술 용어, 위협 및 인터넷 보안에 대한 자세한 내용은 용어집 페이지를 참조하세요.

최종 사용자 사용권 계약

중요: 제품 응용 프로그램을 다운로드, 설치, 복사 또는 사용하기 전에 다음 약관을 읽어 보시기 바랍니다. **소프트웨어를 다운로드, 설치, 복사하거나 사용할 경우 다음 약관에 동의하며 다음을 인정하는 것으로 간주됩니다.** 개인 정보 보호 정책.

최종 사용자 사용권 계약

Einsteinova 24, 85101 Bratislava, Slovak Republic에 소재하고 브라티슬라바 지방 법원 상업 등기소, SRO국(입력 번호 3586/B, 사업자 등록 번호: 31333532)에 등록된 ESET, spol. s r. o.사 또는 ESET 그룹(이하 "ESET" 또는 "공급업체")과 자연인 또는 법인인 사용자(이하 "사용자" 또는 "최종 사용자") 간에 실행되는 최종 사용자 라이선스 계약(이하 "계약")에 따라 사용자는 본 계약 1조에 정의된 소프트웨어를 사용할 수 있는 권한을 갖습니다. 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 다운로드, 설치, 복사 또는 사용하는 중에 "동의함"을 클릭하면 본 계약의 약관에 동의한 것이 됩니다. 본 계약의 약관에 동의하지 않을 경우 즉시 취소 옵션을 클릭하거나, 다운로드 또는 설치를 취소하거나 소프트웨어, 설치 미디어, 기본 설명서 및 구매 영수증을 폐기하거나, 소프트웨어를 구매한 매장이나 ESET로 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 요소

를 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(이하 "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 계약의 약관에 동의한 조건에 따라 사용자가 여기에 약정된 모든 약관을 준수하는 경우 공급업체는 다음과 같은 권한(이하 "라이선스")을 사용자에게 부여해야 합니다.

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(이하 "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 라이선스 수의 제한에 따라 소프트웨어를 사용할 수 있는 권한 수준까지만 소프트웨어에 라이선스 키를 입력할 자격이 있습니다. 라이선스 키는 기밀로 취급됩니다. 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) **Business Edition.** 메일 서버, 메일 릴레이, 메일 게이트웨이 또는 인터넷 게이트웨이에서 소프트웨어를 사용하려면 Business Edition 버전의 소프트웨어를 구입해야 합니다.

d) **라이선스 기간.** 소프트웨어 사용 권한에 대한 기간은 제한됩니다.

e) **OEM 소프트웨어.** OEM 소프트웨어는 구입한 해당 컴퓨터에서만 사용할 수 있으며, 다른 컴퓨터에 양도할 수 없습니다. 다른 컴퓨터에 양도할 수 없습니다.

f) **증정용("NFR") 및 평가판 소프트웨어.** 증정용("NFR") 또는 평가판으로 분류된 소프트웨어는 판매될 수 없

으며, 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. 이 경우 소프트웨어, 모든 백업 복사본을 사용자 비용 부담으로 즉시 삭제 또는 폐기하거나 또는 소프트웨어를 구입한 매장이나 ESET로 반납해야 합니다. 라이선스가 종료되면 공급업체는 소프트웨어 기능 사용(공급업체 서버나 타사 서버에 연결되어야 함)과 관련하여 최종 사용자의 자격을 취소할 수 있는 권한도 지닙니다.

4. **데이터 수집의 기능 및 인터넷 연결 요구 사항.** 소프트웨어를 제대로 작동하려면 인터넷에 연결되어 있어야 하며, 개인 정보 보호 정책에 따라 정기적으로 공급업체 서버 또는 제3자 서버와 해당 데이터 수집에 연결되어야 합니다. 인터넷 및 해당 데이터 수집에 대한 연결은 다음과 같은 소프트웨어 기능에 필요합니다.

a) **소프트웨어 업데이트.** 공급업체는 소프트웨어 업데이트("업데이트")를 발표할 자격이 있지만 업데이트를 제공할 의무는 없습니다. 이 기능은 소프트웨어의 표준 설정에 따라 활성화되므로 최종 사용자가 자동 업데이트 설치를 비활성화하지 않는 한 업데이트가 자동으로 설치됩니다. 업데이트를 제공하기 위해서는 개인 정보 보호 정책에 따라 소프트웨어가 설치되는 컴퓨터 및/또는 플랫폼에 대한 정보를 비롯한 라이선스 정품 확인이 필요합니다.

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)(이하 "침입 사항")의 샘플을 수집한 뒤 이를 설치 프로세스, 컴퓨터, 소프트웨어가 설치된 컴퓨터 및/또는 플랫폼에 대한 정보, 소프트웨어의 작동 및 기능에 대한 정보, 로컬 네트워크의 장치에 대한 정보(예: 유형, 공급업체, 모델 및/또는 장치 이름)(이하 "정보")를 포함하되 이에 국한되지 않은 정보와 함께 공급업체에 전송하는 기능이 포함되어 있습니다. 해당 정보 및 침입 사항에는 소프트웨어가 설치된 컴퓨터의 최종 사용자 및/또는 다른 사용자에 대한 데이터(무작위로 또는 우연히 획득한 개인 데이터 포함), 관련 메타데이터를 포함한 침입 사항의 영향을 받은 파일에 대한 데이터가 포함될 수 있습니다.

정보 및 침입 사항은 다음 소프트웨어 기능에 의해 수집될 수 있습니다.

i. LiveGrid 평판 시스템 기능에는 침입 사항 관련 단방향 해시를 수집하고 이를 공급업체에 보내는 기능이 포함됩니다. 이 기능은 소프트웨어의 표준 설정에서 활성화할 수 있습니다.

ii. LiveGrid 피드백 시스템 기능에는 관련 메타데이터를 포함한 침입 사항 및 정보를 수집하고 이를 공급업체에 보내는 기능이 포함됩니다. 이 기능은 소프트웨어를 설치하는 동안 최종 사용자에 의해 활성화될 수 있습니다.

공급업체는 침입 사항에 대한 분석 및 조사, 소프트웨어 및 라이선스 정품 확인 개선 목적에 한해, 이러한 수신된 정보와 침입 사항을 사용하고 수신된 정보 및 침입 사항을 안전하게 보호하기 위해 적절한 조치를 취해야 합니다. 소프트웨어의 이 기능을 활성화하는 경우, 개인 정보 보호 정책에 명시된 대로 관련 법률 규정에 따라 침입 사항과 정보를 수집하고 공급업체에서 처리할 수 있습니다. 이러한 기능은 언제든지 비활성화할 수 있습니다.

본 계약의 목적에 따라, 공급업체가 개인 정보 보호 정책에 따라 사용자를 식별할 수 있도록 하는 데이터를 수집, 처리 및 저장해야 합니다. 사용자는 공급업체가 자체적인 방식을 통해 사용자가 본 계약의 조항에 따라 소프트웨어를 사용하는지 확인하는 데 동의해야 합니다. 사용자는 본 계약의 목적에 따라, 소프트웨어와 공급업체 컴퓨터 시스템 또는 공급업체 유통 및 지원 네트워크에 속하는 비즈니스 파트너의 컴퓨터 시스템 간 통신 중에 소프트웨어의 기능 및 소프트웨어를 사용하고, 공급업체의 권리를 보호하기 위한 승인을 보장하기 위해 사용자의 데이터가 전송되어야 한다는 데 동의해야 합니다.

본 계약의 체결에 따라, 공급업체 또는 공급업체의 유통 및 지원 네트워크에 속하는 비즈니스 파트너는 대

금 청구 목적, 본 계약의 이행 및 컴퓨터에서 알림 전송을 위해 사용자를 식별하는 필수 데이터를 전송, 처리 및 저장할 자격을 갖습니다. 사용자는 마케팅 정보를 포함하되 이에 국한되지 않는 알림 및 메시지를 수신하는 데 동의합니다.

개인 정보, 개인 데이터 보호 및 데이터 주체로서의 사용자 권한에 대한 자세한 내용은 공급업체의 웹 사이트에서 확인할 수 있으며, 설치 프로세스를 통해 직접 접근할 수 있습니다. 또한 소프트웨어의 도움말 섹션에서 방문할 수도 있습니다.

5. **최종 사용자의 권리 실행**. 최종 사용자의 권리는 직접 또는 직원을 통해 실행해야 합니다. 사용자는 라이선스를 얻은 컴퓨터 시스템을 보호하고 사용자의 활동을 보장하는 목적으로만 소프트웨어를 사용할 수 있습니다.

6. **권한 제한.** 소프트웨어의 일부를 복사, 배포 또는 분리하거나 소프트웨어의 파생된 버전을 만들 수 없습니다. 다음은 예외입니다.

a) 아카이브 백업 복사본을 다른 컴퓨터에 설치하거나 사용하지 않을 경우 데이터를 백업 복사본으로 영구 저장하기 위해 미디어에 소프트웨어 복사본을 하나 직접 만들 수 있습니다. 이 외에 다른 소프트웨어 복사본을 만들 경우 본 계약서를 위반하는 것이 됩니다.

b) 소프트웨어 또는 소프트웨어 복사본을 사용할 수 있는 권리를 본 계약서에서 기술한 방식 외에 다른 방식으로 사용, 수정, 해석, 복제 또는 양도할 수 없습니다.

c) 소프트웨어를 다른 개인에게 판매, 재배포 또는 임대하거나, 다른 개인으로부터 소프트웨어를 임차 또는 대여할 수 없으며, 상업적 서비스 제공을 위해 사용할 수 없습니다.

d) 소프트웨어를 역엔지니어링, 역컴파일 또는 디어셈블하거나 소프트웨어의 소스 코드를 검색할 수 없습니다. 그러나 이러한 제한이 명시적으로 법에 의해 금지된 경우는 제외합니다.

e) 저작권법이나 다른 지적 재산권으로 인한 해당 제한 사항에 따르되 제한 없이 이를 포함하여, 소프트웨어 사용에 관한 모든 해당 법률 규정에 따른 방식으로만 소프트웨어를 사용할 것을 동의합니다.

f) 이러한 서비스에 접근하는 다른 최종 사용자의 기회를 제한하지 않는 방식으로만 소프트웨어 및 해당 기능을 사용할 것을 동의합니다. 공급업체는 최대한 많은 최종 사용자가 서비스를 사용할 수 있도록, 개별 사용자에게 제공되는 서비스 범위를 제한할 권리를 보유합니다. 서비스 범위를 제한하는 것은 소프트웨어 기능 사용 기회 종료 및 소프트웨어의 특정 기능과 관련한 제3자의 서버나 공급업체 서버에 대한 데이터 및 정보 삭제를 의미하기도 합니다.

g) 사용자는 본 계약의 조항에 반하여 라이선스 키를 사용하거나, 복제 또는 생성된 라이선스 키의 무단 복제나 배포뿐만 아니라 임의 형태로 사용했거나 사용하지 않은 라이선스 키의 전송과 같이 소프트웨어 사용 자격이 없는 사람에게 라이선스 키를 제공하거나, 공급업체 이외의 출처에서 얻은 라이선스 키를 사용하여 소프트웨어를 사용하는 모든 활동을 이행하지 않는다는 데 동의합니다.

7. **저작권**. 소프트웨어의 법적 권리와 지적 재산권을 포함하되 제한 없이 소프트웨어와 소프트웨어의 모든 권한은 ESET 및/또는 해당 라이선스 공급업체의 자산입니다. 이들은 소프트웨어를 사용하고 있는 국가의 다른 모든 해당 법률과 국제 협약의 규정에 의해 보호를 받습니다. 소프트웨어의 구조, 구성 및 코드는 ESET 및/또는 해당 라이선스 공급업체의 업무상 비밀이며 기밀 정보입니다. 소프트웨어를 복사할 수 없지만 6(a) 조에 지정된 경우는 예외입니다. 이에 따라 작성한 복사본에는 소프트웨어에 지정된 것과 동일한 저작권 및 법적 권한에 대한 고지 사항이 포함되어야 합니다. 본 계약서의 위반과 관련한 공급업체 권한에도 불구하고 본 계약서의 조항을 위반하여 소프트웨어의 소스 코드를 역엔지니어링, 역컴파일, 디어셈블하거나 소스 코드를 검색한 경우 이로 인해 획득한 모든 정보는 그 시점부터 모두 공급업체에게 자동으로 그리고 취소 불가능하게 양도되거나 공급업체가 소유한 것으로 간주됩니다.

8. **권리 유보**. 본 계약서에서 소프트웨어의 최종 사용자에게 명시적으로 부여한 권리를 제외한 소프트웨어의 모든 권리는 공급업체가 단독으로 유보하고 있습니다.

9. **복수의 언어 버전, 이중 미디어 소프트웨어, 복수의 복사본**. 소프트웨어에서 복수의 플랫폼이나 언어를 지원하거나 복수의 소프트웨어 복사본을 얻은 경우, 라이선스를 획득한 컴퓨터 시스템 수 및 버전에 해당하는 소프트웨어만 사용할 수 있습니다. 사용자가 이용하지 않은 소프트웨어의 버전이나 복사본은 판매, 대여, 임대, 임차, 재허여하거나 양도할 수 없습니다.

10. **계약의 시작 및 종료**. 본 계약서는 본 계약서에 동의한 날부터 유효합니다. 소프트웨어, 모든 백업 복사본 및 공급업체나 공급업체의 비즈니스 파트너로부터 획득한 모든 관련 자료를 사용자가 비용을 부담하여 영구적으로 삭제, 폐기 또는 반납할 경우 본 계약을 종료할 수 있습니다. 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**. 해당 법률에서 허용하는 최대 한도까지 공급업체, 공급업체 직원 또는 라이선스 공급업체는 모든 수익, 매출 또는 판매 손실이나 데이터, 대체품이나 서비스 조달 비용, 재산상 손해, 인적 상해, 비즈니스 중단, 비즈니스 정보 손실 또는 계약, 고의적인 위법 행위, 태만 또는 책임 발생이 성립되는 기타 사건으로 인해 방식에 상관없이 발생한 특수하거나 직접, 간접, 우발적, 경제적, 외피성, 범죄적, 특수한 손해나 수반되는 손해에 대해 공급업체나 해당 라이선스 공급업체 또는 자회사가 이러한 손해 가능성을 통보받은 경우에도 이에 대한 책임을 지지 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. 최종 사용자는 기술 지원을 제공받기 전에 기존의 모든 데이터, 소프트웨어 및 프로그램 기능을 백업해야 합니다. ESET나 ESET에서 위탁한 제3자는 기술 지원 제공으로 인한 데이터 손실, 재산상 손해, 소프트웨어나 하드웨어 손실 또는 수익 손실에 대해서는 어떤 법적 책임도 지지 않습니다. ESET나 ESET에서 위탁한 제3자는 기술 지원 범위를 벗어난 문제 해결과 관련하여 결정권을 가지고 있습니다. ESET는 단독 재량으로 기술 지원 제공을 거부, 연기 또는 종료할 권리를 보유합니다. 개인 정보 보호 정책을 준수하는 라이선스 정보, 정보 및 기타 데이터는 기술 지원을 제공하기 위해 필요할 수 있습니다

16. **라이선스 양도**. 공급업체의 동의를 받은 경우 컴퓨터 시스템 간 소프트웨어를 양도할 수 있습니다. 공급업체의 동의를 받은 경우 컴퓨터 시스템 간 소프트웨어를 양도할 수 있습니다. 공급업체의 동의를 받은 경우, 그리고 다음의 조건을 충족하는 경우에 한해 본 계약서의 모든 권한 및 라이선스를 다른 최종 사용자에게 영구적으로 양도할 수 있습니다. (i) 원래 최종 사용자가 소프트웨어 복사본을 가지고 있지 않아야 합니다. (ii) 권한은 원래 최종 사용자에게서 새로운 최종 사용자에게로 직접 양도되어야 합니다. (iii) 새로운 최종 사용자가 본 계약서의 원래 최종 사용자와 관련된 모든 권리와 책임을 맡기로 표명해야 합니다. (iv) 원래 최종

사용자가 17조에 지정된 대로 소프트웨어 정품을 확인할 수 있도록 설명서를 새로운 최종 사용자에게 제공해야 합니다.

17. **소프트웨어 정품 확인**. 최종 사용자는 다음 방법 중 하나로 소프트웨어 사용 자격을 증명할 수 있습니다. (i) 공급업체에서 지정한 제3자나 공급업체에서 발행한 라이선스 인증서를 통해, (ii) 서면으로 작성된 라이센스 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(이하 "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(이하 "수출관리법")

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(이하 "제재법")

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.a조를 위반했거나 위반할 가능성이 있는 것으로 판단하는 경우

ii. 최종 사용자 및/또는 소프트웨어가 무역관리법의 적용을 받게 되어 결과적으로 ESET이 합당한 의견에 따라 본 계약의 의무를 계속 이행하면 ESET 또는 해당 계열사가 무역관리법에 의거하여 관련 법을 위반하게 되거나 부정적인 결과를 초래하게 될 수 있다고 판단하는 경우

c) 본 계약의 어떠한 조항도 해당 무역관리법과 상반되거나, 관련 법에 따라 처벌 또는 금지되는 방식으로 행동하거나 행동을 삼가도록(또는 행동하거나 행동을 삼가는 데 동의하도록) 유도 또는 요구하기 위한 것이 아니며, 이와 같이 해석되거나 이해되어서는 안 됩니다.

20. **고지 사항**. 모든 고지 사항, 반품 소프트웨어 및 설명서는: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

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 유효성

에 영향을 미치지 않습니다. 본 계약서에 규정된 약관에 따라 나머지 규정은 여전히 유효하고 실행 가능합니다. 본 계약서의 언어 버전 간에 불일치 항목이 있는 경우 영어 버전이 우선합니다. 본 계약서의 수정은 서면으로만 가능하며 인증된 공급업체 대리인이나 직원이 공급업체를 대신하여 해당 수정 사항에 서명을 해야 합니다.

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.

EULA ID: BUS-STANDARD-20-01

개인 정보 보호 정책

Einsteinova 24, 851 01 Bratislava, Slovak Republic에 소재하고 브라티슬라바 지방 법원 상업 등기소, SRO국(입력 번호 3586/B, 데이터 통제자로서의 사업자 등록 번호: 31333532)에 등록된 ESET, spol. 사("ESET" 또는 "당사")는 고객들의 개인 데이터 및 개인 정보 처리 작업이 투명하게 이루어지기를 원합니다. 이러한 목표를 달성하기 위한 일환으로 ESET에서는 본 개인 정보 보호 정책을 게시하며, 이 정책은 고객("최종 사용자" 또는 "귀하")에게 다음과 같은 내용을 알리기 위한 목적으로만 사용됩니다.

- 개인 데이터 처리,
- 데이터 기밀성,
- 데이터 주체 권한

개인 데이터 처리

ESET에서 제공하는 서비스는 최종 사용자 사용권 계약("EULA")에 따라 제품 내에서 구현되지만 일부 서비스에는 특별한 주의가 필요할 수 있습니다. 당사의 서비스 제공과 관련된 데이터 수집에 대한 자세한 내용을 알려 드리고자 합니다. 당사는 업데이트/업그레이드 서비스, ESET LiveGrid®, 데이터 악용으로부터 보호, 지원 등 EULA와 제품 관련 문서에 설명된 다양한 서비스를 제공합니다. 모든 서비스를 제공하기 위해서는 다음 정보를 수집해야 합니다.

- 업데이트/기타 통계 - 설치 프로세스 및 제품이 설치된 플랫폼을 비롯한 컴퓨터에 대한 정보, 운영 체제, 하드웨어 정보, 설치 ID, 라이선스 ID, IP주소, MAC 주소, 제품 구성 설정 등과 같은 제품의 작동 및 기능에 대한 정보 포함
- ESET LiveGrid® 평판 시스템의 일부로 침입과 관련된 단방향 해시 - 검출된 파일을 클라우드의 허용 목록 및 차단 목록 항목 DB와 비교하여 악성코드 방지 솔루션의 효율성을 향상시킵니다.
- ESET LiveGrid® 피드백 시스템의 일부로 현장의 감염 의심 샘플과 메타데이터 - ESET에서 최종 사용자의 요구 사항에 즉각 반응하고 최신 위협에 대한 대응력을 유지합니다. 귀하께서는 아래 내용을 보내주시면 됩니다.
  - 바이러스 및 기타 악성 프로그램, 감염이 의심되거나 문제가 있거나, 사용자가 원치 않거나 사용자에게 안전하지 않은 오브젝트(예: 실행 파일, 스팸으로 보고되었거나 당사 제품에 의해 플래그가 지정된 이메일 메시지)의 잠재적 샘플 등과 같은 침입 사항
  - 로컬 네트워크의 장치에 대한 정보(예: 장치의 유형, 공급업체, 모델 및/또는 이름 등)
  - 인터넷 사용에 관한 정보(예: IP 주소 및 지리적 정보, IP 패킷, URL 및 이더넷 프레임 등)
  - 충돌 덤프 파일 및 포함된 정보

당사에서는 이 범위 외의 데이터를 수집하기를 원치 않지만 간혹 수집되는 경우가 있을 수 있습니다. 우발적으로 수집된 데이터는 악성코드 자체(사용자 모르게 또는 사용자 승인 없이)에 포함되었을 수 있거나 파일 이름 또는 URL의 일부로 포함되었을 수 있으며, 당사에서는 본 개인 정보 보호 정책에 명시된 목적에 따라 수집된 이 데이터로 당사 시스템의 일부를 구성하거나 이를 처리하지 않습니다.

- 라이선스 ID와 개인 데이터(예: 이름, 성, 주소, 이메일 주소 등)와 같은 라이선스 정보는 청구 용도, 라이선스 정품 확인 및 서비스 제공을 위해 필요합니다.
- 지원 요청에 포함된 연락처 정보 및 데이터는 지원 서비스에 필요할 수 있습니다. 연락받기로 선택한 채널을 기반으로 이메일 주소, 전화번호, 라이선스 정보, 제품 세부 사항 및 지원 사례 설명을 수집할 수 있습니다. 지원 서비스를 원활하게 제공하기 위해 기타 정보를 당사에 제공해야 할 수도 있습니다.

데이터 기밀성

ESET은 배포, 서비스 및 지원 네트워크의 일부로 계열사 또는 파트너를 통해 전 세계적으로 운영되는 회사입니다. ESET에서 처리한 정보는 서비스 제공, 지원 또는 청구 등과 같은 EULA 이행을 위해 계열사 또는 파트너와 주고받을 수 있습니다. 귀하가 사용하도록 선택한 지역 및 서비스에 따라 당사는 유럽 연합 집행 기관(European Commission)의 적절한 결정이 없는 국가로 귀하의 데이터를 전송해야 할 수도 있습니다. 이 경우에도 모든 정보의 전송은 데이터 보호법의 규제를 받으며 필요한 경우에만 수행됩니다. 표준 계약 조항, 구속력 있는 기업 규칙(BCR: Binding Corporate Rules), 또는 다른 적절한 보호 장치는 예외 없이 설정되어야 합니다.

당사는 EULA에 따라 서비스를 제공하는 동안 데이터가 필요 이상으로 오래 보관되지 않도록 최선을 다하고 있습니다. 당사의 보존 기간이 귀하의 라이선스 유효 기간보다 길기 때문에 라이선스를 갱신하는 데 아무런 문제가 없습니다. ESET LiveGrid®의 최소 및 익명화된 통계 및 기타 데이터를 추가로 처리할 수 있습니다(통계용).

ESET에서는 잠재적 위험에 적절한 수준의 보안을 보장하기 위해 적합한 기술적/조직적 조치를 구현합니다. 당사는 처리 시스템과 서비스에 대해 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장하기 위해 최선을 다하고 있습니다. 단, 데이터 위반으로 인해 귀하의 권리와 자유가 침해되는 경우 당사는 감독 기관과 데이터 주체에 이를 알릴 준비가 되어 있습니다. 데이터 주체로서 귀하는 감독 기관에 불만 사항을 제기할 권한이 있습니다.

데이터 주체 권한

ESET은 슬로바키아 법률의 적용을 받으며 유럽 연합의 일원으로 데이터 보호법을 준수해야 합니다. 해당 데이터 보호법에 규정된 조건에 따라 귀하는 데이터 주체로서 다음과 같은 권리를 부여받습니다.

- ESET의 개인 데이터에 접근을 요청할 수 있는 권리,
- 개인 데이터가 부정확한 경우 데이터를 수정할 수 있는 권리(불완전한 개인 데이터를 완료할 수 있는 권리도 부여됨),
- 개인 데이터 삭제를 요청할 수 있는 권리,
- 개인 데이터 처리에 대한 제한을 요청할 수 있는 권리
- 처리에 반대할 수 있는 권리
- 불만 사항을 제기할 수 있는 권리
- 데이터 이동성에 대한 권리.

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