

## ESET PROTECT

### 설치 업그레이드 및 마이그레이션 설명서

[이 문서의 온라인 버전을 표시하려면 여기를 클릭](#)

Copyright ©2024 by ESET, spol. s r.o.

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

자세한 내용은 <https://www.eset.com>을 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. 2024년 4월 17일

1 도움말 정보 .....	1
2 설치/업그레이드/마이그레이션 .....	2
<b>2.1 ESET PROTECT 10.0의 새 기능</b> .....	2
<b>2.2 아키텍처</b> .....	3
2.2 서버 .....	4
2.2 웹 콘솔에 연결 .....	5
2.2 ESET Bridge HTTP 프록시 .....	5
2.2 에이전트 .....	6
2.2 Rogue Detection Sensor .....	7
2.2 모바일 장치 커넥터 .....	8
<b>2.3 ESET Bridge HTTP 프록시, 미러 도구 및 직접 연결 간의 차이</b> .....	9
2.3 ESET Bridge 다음의 사용 시작 시점(HTTP 프록시) .....	11
2.3 미러 도구 사용 시작 시점 .....	11
3 시스템 요구 사항 및 크기 조정 .....	12
<b>3.1 지원되는 운영 체제</b> .....	12
3.1 Windows .....	12
3.1 Linux .....	14
3.1 macOS .....	15
3.1 모바일 .....	15
<b>3.2 지원되는 워크스테이션 프로비저닝 환경</b> .....	17
<b>3.3 하드웨어 및 인프라 크기 조정</b> .....	18
3.3 배포 권장 사항 .....	19
3.3 10,000개의 클라이언트에 대한 배포 .....	21
<b>3.4 DB</b> .....	22
<b>3.5 지원되는 Apache Tomcat 및 Java 버전</b> .....	24
<b>3.6 지원되는 웹 브라우저, ESET 보안 제품 및 언어</b> .....	25
<b>3.7 네트워크</b> .....	27
3.7 사용되는 포트 .....	28
4 설치 프로세스 .....	30
<b>4.1 Windows에서의 통합형 설치</b> .....	31
4.1 ESET PROTECT 서버 설치 .....	32
4.1 ESET PROTECT 모바일 장치 커넥터(독립형) 설치 .....	43
<b>4.2 Windows의 구성 요소 설치</b> .....	49
4.2 서버 설치 - Windows .....	51
4.2 Microsoft SQL Server 요구 사항 .....	58
4.2 MySQL Server 설치 및 구성 .....	58
4.2 전용 DB 사용자 계정 .....	60
4.2 에이전트 설치 - Windows .....	61
4.2 서버 지원 에이전트 설치 .....	63
4.2 오프라인 에이전트 설치 .....	63
4.2 ESET Remote Deployment Tool .....	64
4.2 웹 콘솔 설치 - Windows .....	64
4.2 통합형 설치 관리자를 사용하여 웹 콘솔 설치 .....	64
4.2 웹 콘솔을 수동으로 설치 .....	70
4.2 RD Sensor 설치 - Windows .....	71
4.2 미러 도구 - Windows .....	72
4.2 모바일 장치 커넥터 설치 - Windows .....	80
4.2 모바일 장치 커넥터 필수 구성 요소 .....	82
4.2 모바일 장치 커넥터 활성화 .....	83
4.2 MDM iOS 라이선스 기능 .....	84

4.2 HTTPS 인증서 요구 사항	84
4.2 오프라인 저장소 - Windows	85
4.2 장애 조치(Failover) 클러스터 - Windows	87
<b>4.3 Linux의 구성 요소 설치</b>	88
4.3 Linux에 단계별 ESET PROTECT 설치	89
4.3 MySQL 설치 및 구성	90
4.3 ODBC 설치 및 구성	91
4.3 서버 설치 - Linux	94
4.3 서버 필수 구성 요소 - Linux	97
4.3 에이전트 설치 - Linux	99
4.3 웹 콘솔 설치 - Linux	103
4.3 Rogue Detection Sensor 설치 - Linux	105
4.3 모바일 장치 커넥터 설치 - Linux	106
4.3 모바일 장치 커넥터 필수 구성 요소 - Linux	109
4.3 미리 도구 - Linux	110
<b>4.4 macOS의 구성 요소 설치</b>	118
4.4 에이전트 설치 - macOS	118
<b>4.5 ISO 이미지</b>	119
<b>4.6 DNS 서비스 레코드</b>	119
<b>4.7 ESET PROTECT 오프라인 설치 시나리오</b>	120
<b>5 업그레이드 절차</b>	121
5.1 ESET PROTECT 구성 요소 업그레이드 작업	122
5.2 ESET PROTECT 10.0 통합형 설치 관리자를 사용하여 업그레이드	125
5.3 데이터베이스 서버 백업/업그레이드	127
5.3 DB 서버 백업 및 복원	128
5.3 DB 서버 업그레이드	130
5.4 Windows의 장애 조치(Failover) 클러스터에 설치된 ESMC/ESET PROTECT 업그레이드	131
5.5 Apache Tomcat 업그레이드	131
5.5 통합형 설치 관리자를 사용하여 Apache Tomcat 프록시 업그레이드(Windows)	132
5.5 Apache Tomcat 수동 업그레이드(Windows)	135
5.5 Apache Tomcat 및 Java 업그레이드(Linux)	137
<b>6 마이그레이션 및 다시 설치 절차</b>	138
6.1 서버 간 마이그레이션	139
6.1 새로 설치 - 동일한 IP 주소	139
6.1 마이그레이션된 DB - 동일한/다른 IP 주소	141
6.2 ESET PROTECT DB 마이그레이션	142
6.2 MS SQL Server의 마이그레이션 프로세스	142
6.2 MySQL Server의 마이그레이션 프로세스	150
6.2 ESET PROTECT 서버 또는 MDM을 DB에 연결	152
6.3 MDM 마이그레이션	153
6.4 마이그레이션 후 ESET PROTECT 서버의 IP 주소 또는 호스트 이름 변경	155
<b>7 ESET PROTECT 서버 및 해당 구성 요소 제거</b>	156
7.1 ESET Management 에이전트 제거	156
7.2 Windows - ESET PROTECT 서버 및 해당 구성 요소 제거	157
7.3 Linux - ESET PROTECT 구성 요소 업그레이드, 다시 설치 또는 제거	159
7.4 macOS - ESET Management Agent 및 ESET Endpoint 제품 제거	160
7.5 다른 서버로 마이그레이션한 후 이전 ESMC/ESET PROTECT/MDM 서버 해제	162
<b>8 문제 해결</b>	163
8.1 오프라인 환경에서 ESET PROTECT 구성 요소 업그레이드	163
8.2 일반적인 설치 문제에 대한 대답	164

8.3 로그 파일 .....	167
8.4 분석 도구 .....	168
8.5 ESET PROTECT 서버 업그레이드/마이그레이션 후 문제 .....	170
8.6 MSI 로깅 .....	171
9 ESET PROTECT API .....	172
10 FAQ .....	172
11 최종 사용자 사용권 계약 .....	179
12 개인 정보 보호 정책 .....	185

# 도움말 정보

이 설치 설명서는 ESET PROTECT 설치 및 업그레이드를 도와주기 위해 작성되었으며, 해당 프로세스에 대한 지침을 제공합니다.

일관성을 유지하고 혼동을 방지하기 위해 이 설명서 전체에서 사용된 용어는 ESET PROTECT 파라미터 이름을 기준으로 합니다. 또한 특정 관심 분야의 항목이나 중요한 항목을 강조하기 위해 일련의 기호를 사용합니다.

**i** 참고는 특정 기능이나 관련 항목의 링크와 같은 중요한 정보를 제공할 수 있습니다.

**!** 중요는 사용자의 주의가 필요하므로 건너뛰지 않는 것이 좋습니다. 일반적으로 중요는 절대적으로 중요하지는 않지만 상당히 중요한 정보를 제공합니다.

**!** 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.

**✓** 사용자 사례가 포함된 항목에 대해 해당 사용자 사례를 설명하는 예제 시나리오입니다. 예는 보다 복잡한 항목을 설명하는 데 사용됩니다.

규칙	의미
<b>굵은 글꼴</b>	상자 및 옵션 버튼과 같은 인터페이스 항목의 이름입니다.
기울임꼴	사용자가 제공하는 정보의 자리 표시자입니다. 예를 들어 파일 이름 또는 경로는 사용자가 실제 경로나 파일 이름을 입력한다는 의미입니다.
Courier New	코드 샘플 또는 명령.
<u>하이퍼링크</u>	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.

- [온라인 도움말](#)은 도움말 콘텐츠의 기본 소스입니다. 인터넷에 연결되어 있는 경우에는 최신 버전의 온라인 도움말이 자동으로 표시됩니다. ESET PROTECT 온라인 도움말 페이지에는 위쪽 탐색 헤더에 4개의 활성 탭, 즉 [설치/업그레이드](#), [관리](#), [VA 배포](#) 및 [SMB 설명서](#)가 있습니다.
- 이 설명서의 항목은 여러 장 및 하위 장으로 구성되어 있습니다. 상단의 검색 필드를 사용하여 관련 정보를 찾을 수 있습니다.

**!** 페이지 위쪽의 탐색 모음에서 사용자 설명서를 연 후에는 검색이 해당 설명서의 내용으로 제한됩니다. 예를 들어 관리자 설명서를 열면 설치/업그레이드 및 VA 배포 설명서의 항목은 검색 결과에 포함되지 않습니다.

- [ESET 지식 베이스](#)에는 가장 자주 묻는 질문에 대한 대답과 다양한 문제에 대한 권장 해결책이 포함되어 있습니다. 지식 베이스는 ESET 기술 전문가가 정기적으로 업데이트하기 때문에 다양한 유형의 문제를 해결하는 가장 강력한 도구입니다.
- [ESET 포럼](#)을 통해 ESET 사용자는 손쉽게 도움을 얻고 다른 사용자에게 도움을 제공할 수 있습니다. ESET 제품 관련 문제나 질문을 게시할 수 있습니다.

# 설치/업그레이드/마이그레이션

ESET PROTECT 는 중앙 위치 한 곳에서 네트워크로 연결된 환경에 있는 클라이언트 워크스테이션, 서버 및 모바일 장치에서 ESET 제품을 관리할 수 있게 해주는 애플리케이션입니다. ESET PROTECT의 기본 제공 작업 관리 시스템을 사용하면 원격 컴퓨터에서 ESET 보안 솔루션을 설치하고 새로운 문제 및 탐지에 신속하게 대응할 수 있습니다.

ESET PROTECT은(는) 악성 코드로부터 스스로 보호하지는 못합니다. 워크스테이션 및 모바일 장치의 ESET Endpoint Security 또는 서버 컴퓨터의 Windows 용 ESET Server Security와 같은 ESET 보안 솔루션으로 작업 환경을 보호할 수 있습니다.

ESET PROTECT은(는) 다음 두 가지 기본 원칙에 따라 구축되었습니다.

- **중앙 집중식 관리** - 전체 네트워크를 한 곳에서 구성, 관리 및 모니터링할 수 있습니다.
- **확장성** - 시스템을 대기업 환경뿐만 아니라 소규모 네트워크에도 배포할 수 있습니다. ESET PROTECT은(는) 증가하는 인프라를 수용할 수 있도록 설계되었습니다.

ESET PROTECT [은\(는\) 차세대 ESET 보안 제품을 지원](#)하며, 이전 세대의 제품과도 호환됩니다.

ESET PROTECT 도움말 페이지에는 완전한 설치 및 업그레이드 설명서가 있습니다:

- [ESET PROTECT의 아키텍처](#)
- [설치 프로세스](#)
- [업그레이드 절차](#)
- [마이그레이션 절차](#)
- [제거 절차](#)
- [라이선스 관리](#)
- [배포 프로세스 및 GPO 또는 SCCM을 사용한 에이전트 배포](#)
- [ESET PROTECT 설치 후 첫 번째 단계](#)
- [관리 설명서](#)

## ESET PROTECT 10.0 의 새 기능

### 향상된 VDI 지원

VDI 환경을 설정할 때 이제 컴퓨터 하드웨어 지문 인식뿐만 아니라 컴퓨터의 FQDN을 통해서도 컴퓨터 ID(새 ID 생성 및 기존 ID 갱신)를 처리할 수 있습니다. [자세히 알아보기](#)

## 어두운 테마

이제 ESET PROTECT에 추가된 새로운 어두운 테마를 사용해 볼 수 있습니다. 콘솔 사용자는 이제 사용자 설정에서 해당 기능을 활성화할 수 있습니다. [자세히 알아보기](#)

## Syslog용 CEF 형식

이제 로그를 CEF(Common Event Format) 형식으로 Syslog에 보낼 수 있습니다. [자세히 알아보기](#)

## 기타 개선사항 및 유용성 변경사항

[변경 로그](#)에서 자세한 내용을 확인할 수 있습니다.

## 아키텍처

ESET PROTECT은(는) 차세대 원격 관리 시스템입니다.

[ESET 보안 제품](#)의 배포를 완료하려면 다음 구성 요소(Windows 및 Linux 플랫폼)를 설치합니다.

- [ESET PROTECT 서버](#)
- [ESET PROTECT 웹 콘솔](#)
- [ESET Management 에이전트](#)

다음 지원 구성 요소는 옵션이지만 네트워크에서 최상의 애플리케이션 성능을 보장하려면 설치하는 것이 좋습니다.

- [RD Sensor](#)
- [ESET Bridge HTTP 프록시](#)
- [모바일 장치 커넥터](#)

ESET PROTECT 구성 요소는 인증서를 사용하여 ESET PROTECT 서버와 통신합니다. [지식베이스 문서](#)에서 ESET PROTECT의 인증서에 대해 자세히 알아보십시오.

## 인프라 요소 개요

아래 표에는 ESET PROTECT 인프라 요소와 해당 기본 기능에 대한 개요가 나와 있습니다.

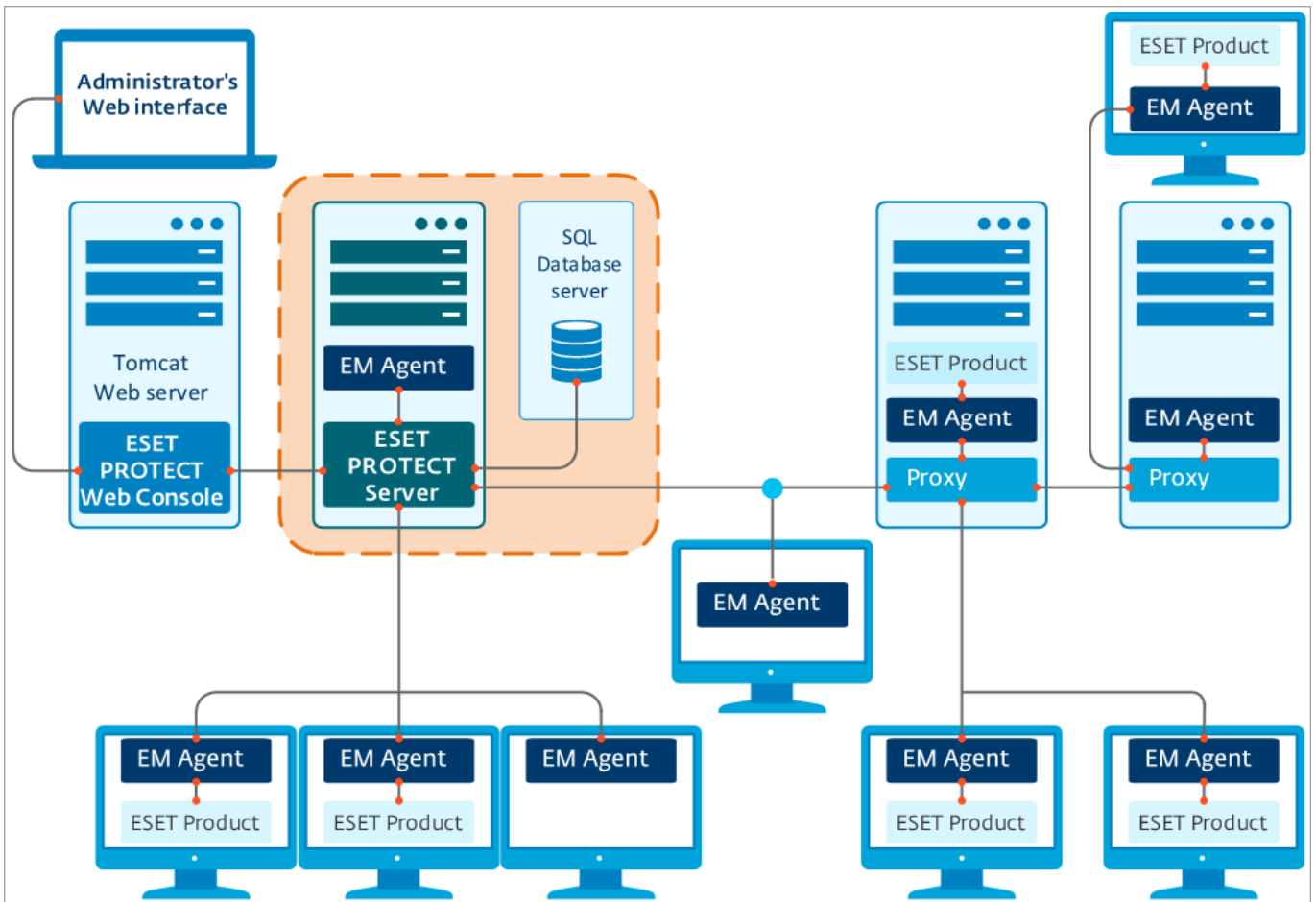
기능	ESET PROTECT 서버	ESET Management 에이전트	ESET 보안 제품	ESET Bridge HTTP 프록시	ESET 서버	모바일 장치 커넥터
ESET 보안 제품의 원격 관리(정책, 작업, 보고서 등의 생성)	✓	X	X	X	X	X



기능	ESET PROTECT 서버	ESET Management 에이전트	ESET 보안 제품	ESET Bridge HTTP 프록시	ESET 서버	모바일 장치 커넥터
ESET PROTECT 서버와의 통신 및 클라이언트 장치에서 ESET 보안 제품 관리	X	✓	X	X	X	✓
업데이트, 라이선스 유효성 검사 제공	X	X	X	X	✓	X
업데이트 캐시 및 전달(탐지 엔진, 설치 관리자, 모듈)	X	X	✓	✓	X	X
ESET Management Agent와 ESET PROTECT 서버 간 네트워크 트래픽 전달	X	X	X	✓	X	X
클라이언트 장치 보안	X	X	✓	X	X	X
모바일 장치의 원격 관리	X	X	X	X	X	✓

## 서버

ESET PROTECT 서버는 (ESET Management Agent 또는 [HTTP 프록시](#)를 통해) 서버에 연결된 클라이언트에서 수신되는 모든 데이터를 처리하는 실행 애플리케이션입니다. 데이터를 올바르게 처리하기 위해서는 이 서버에 네트워크 데이터가 저장된 DB 서버에 대한 안정적인 연결이 필요합니다. 더 나은 성능을 얻기 위해 DB 서버를 다른 컴퓨터에 설치하는 것이 좋습니다.

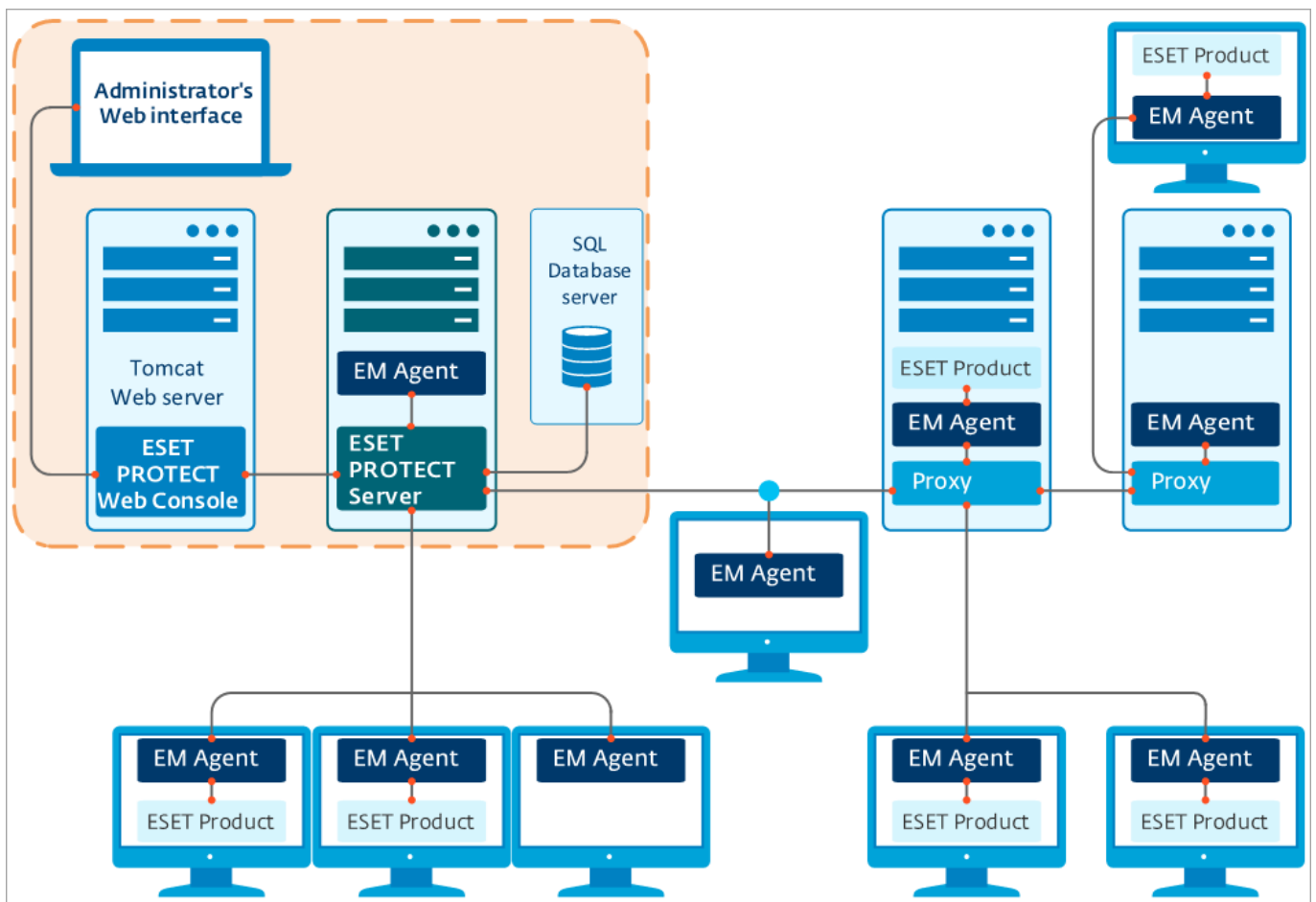


## 웹 콘솔에 연결

ESET PROTECT 웹 콘솔은 사용자 환경에서 ESET 보안 솔루션을 관리할 수 있는 웹 기반 사용자 인터페이스입니다. 이 인터페이스는 네트워크의 클라이언트 상태 개요를 표시하고, ESET 솔루션을 관리되지 않는 컴퓨터에 원격으로 배포하는 데 사용될 수 있습니다. 이 웹 콘솔에는 브라우저를 사용하여 접근합니다([지원되는 웹 브라우저](#) 참조). 인터넷에서 웹 서버에 접근할 수 있도록 선택하면 거의 모든 장소 및 장치에서 ESET PROTECT을(를) 사용할 수 있습니다.

웹 콘솔은 Apache Tomcat을 HTTP 웹 서버로 사용합니다. ESET 설치 관리자 또는 가상 어플라이언스와 함께 제공되는 Tomcat을 사용하는 경우 웹 콘솔에 대한 TLS 1.2 및 1.3 연결만 허용됩니다.

**i** ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다.



## ESET Bridge HTTP 프록시

ESET Bridge 및 ESET PROTECT을(를) 프록시 서비스로 사용하여 다음을 수행할 수 있습니다.

- 다음을 다운로드 및 캐시합니다: ESET 모듈 업데이트, ESET PROTECT(예: ESET Endpoint Security MSI 설치 관리자)에서 푸시된 설치 및 업데이트 패키지, ESET 보안 제품 업데이트(구성 요소 및 제품 업데이트), ESET LiveGuard 결과.
- ESET Management Agent에서 ESET PROTECT 서버로 통신을 전달합니다.

ESET Bridge 설치 및 구성에 대한 자세한 내용은 [ESET Bridge 온라인 도움말](#)에서 확인할 수 있습니다.

### Apache HTTP Proxy 사용자

- ! ESET PROTECT 10.0부터 ESET Bridge이(가) Apache HTTP Proxy를 대체합니다. Apache HTTP Proxy가 제한된 지원에 도달했습니다. Apache HTTP Proxy를 사용하는 경우, [ESET Bridge\(으\)로 마이그레이션](#)하는 것이 좋습니다.

## 에이전트

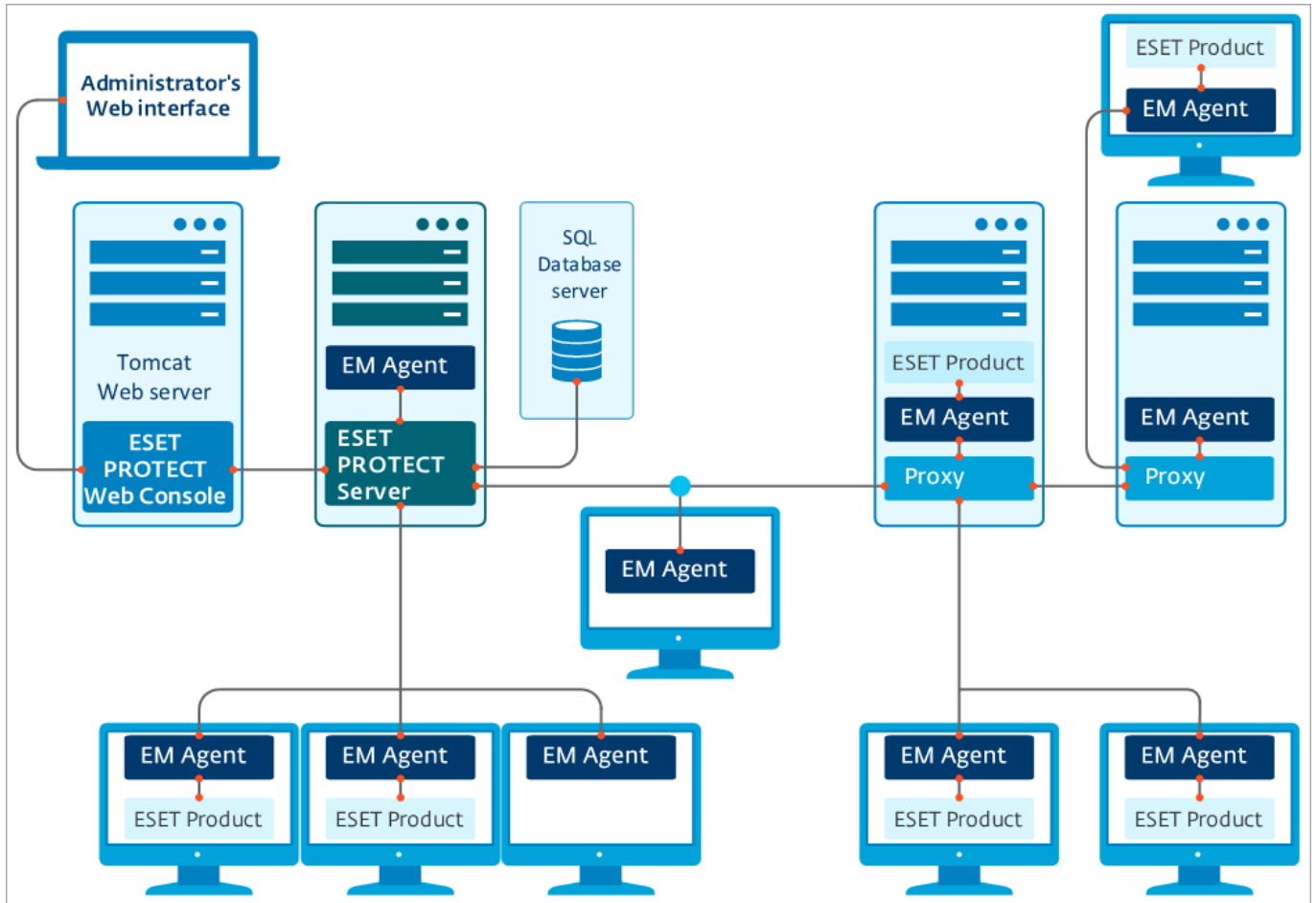
**ESET Management 에이전트**는 ESET PROTECT의 필수적인 부분입니다. 클라이언트는 ESET PROTECT 서버와 직접 통신하지 않으며 이 에이전트가 이 통신을 도와줍니다. 에이전트는 클라이언트에서 정보를 수집한 후 ESET PROTECT 서버로 전송합니다. ESET PROTECT 서버가 클라이언트에 대한 작업을 전송하면 클라이언트는 에이전트로 전송하고, 에이전트는 클라이언트로 이 작업을 전송합니다. ESET Management 에이전트는 새로운 향상된 [통신 프로토콜](#)을 사용합니다.

끝점 보호를 간편하게 구현하기 위해 독립 실행형 ESET Management 에이전트가 ESET PROTECT 제품군에 포함됩니다. 에이전트는 ESET PROTECT 서버와 ESET 제품 또는 운영 체제 간의 모든 통신을 처리하는 간단하고 고도로 모듈화된 경량 서비스입니다. ESET 제품은 ESET PROTECT 서버와 직접 통신하지 않고 에이전트를 통해 통신합니다. ESET Management 에이전트가 설치되고 ESET PROTECT 서버와 통신할 수 있는 클라이언트 컴퓨터는 '관리되는' 컴퓨터라고 합니다. 다른 ESET 소프트웨어가 설치되어 있는지 여부에 관계없이 어떤 컴퓨터에도 에이전트를 설치할 수 있습니다.

다음과 같은 장점이 있습니다.

- 쉬운 설정 - 에이전트를 표준 회사 설치의 일부로 배포할 수 있습니다.
- 즉각적인 보안 관리 - 여러 보안 시나리오를 저장하도록 에이전트를 구성할 수 있으므로 탐지에 대한 반응 시간이 크게 줄어듭니다.
- 오프라인 보안 관리 - 에이전트는 ESET PROTECT 서버에 연결되어 있지 않아도 이벤트에 반응할 수 있습니다.

- ! 에이전트와 ESET PROTECT 서버 간의 통신 프로토콜은 인증을 지원하지 않습니다. 인증을 요구하는 ESET PROTECT 서버에 에이전트 통신을 전달하는 데 사용되는 프록시 솔루션은 작동되지 않습니다. 웹 콘솔이나 에이전트에 대해 기본값이 아닌 포트를 사용하도록 선택하면 방화벽을 조정해야 할 수 있습니다. 조정하지 않으면 설치에 실패할 수 있습니다.



## Rogue Detection Sensor

**RD Sensor(Rogue Detection Sensor)**는 네트워크에서 컴퓨터를 검색하는 Rogue 시스템 검색기 도구입니다. 이 RD Sensor는 새 컴퓨터를 검색하여 수동으로 추가할 필요 없이 ESET PROTECT에서 새 컴퓨터를 찾을 수 있으므로 편리합니다. 검색된 컴퓨터는 바로 미리 정의된 보고서에서 검색되고 이 보고서에 보고되므로 이러한 컴퓨터를 특정 정적 그룹으로 이동하고 관리 작업을 계속 수행할 수 있습니다.

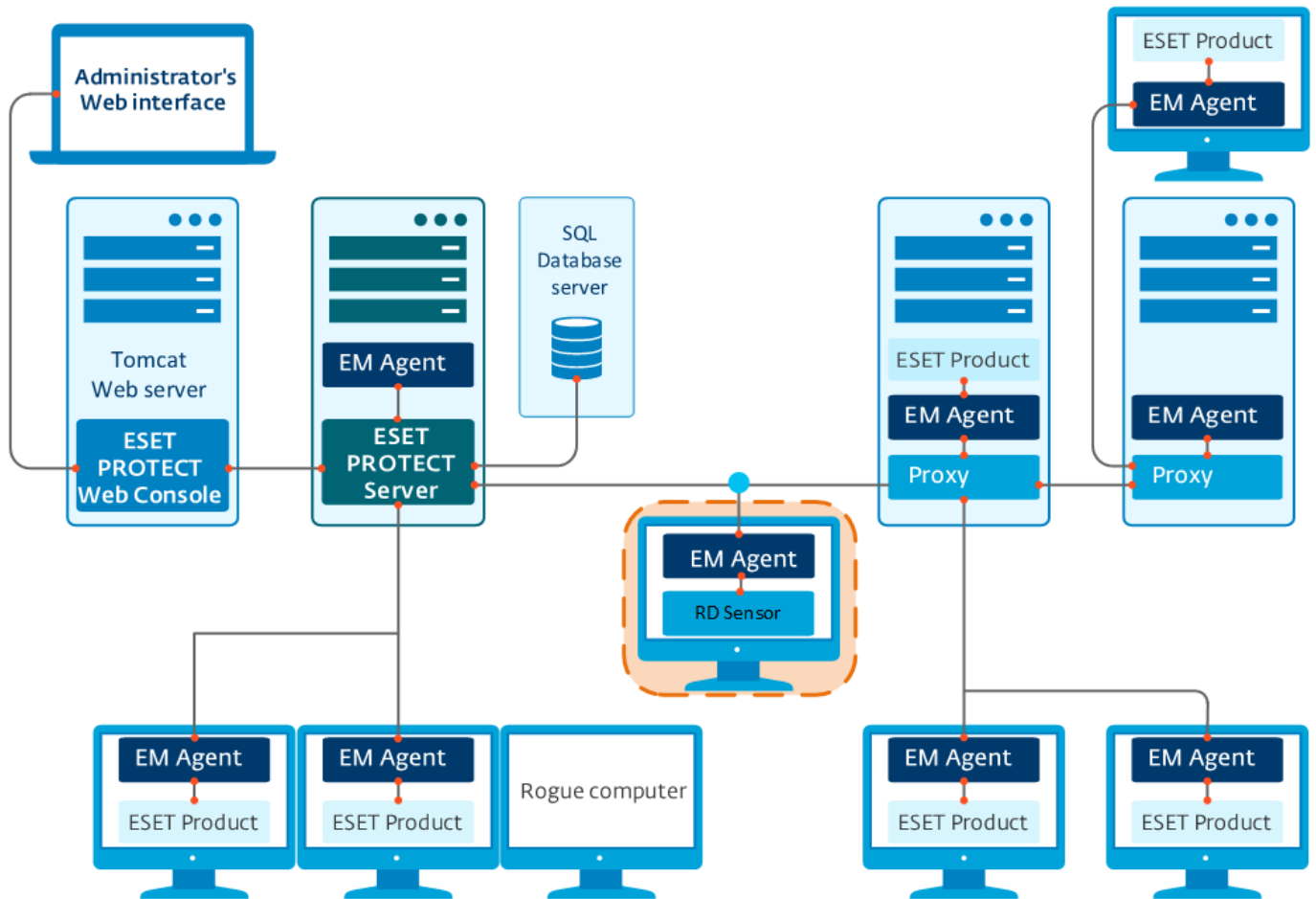
RD Sensor는 ARP 방송을 능동적으로 듣습니다. RD Sensor가 새로운 활성 네트워크 구성 요소를 감지하면 RD Sensor가 ARP 유니캐스트를 전송하고, ([여러 포트](#)를 사용해) 호스트 지문 채취를 수행하고, 감지된 컴퓨터에 관한 정보를 ESET PROTECT 서버에 전송합니다. ESET PROTECT 서버는 네트워크에서 찾은 PC가 ESET PROTECT 서버에 알려져 있지 않은 PC인지 또는 이미 관리되고 있는 PC인지를 평가합니다.

RD Sensor의 주요 기능이므로 호스트 지문 채취를 비활성화할 수 없습니다.



여러 네트워크 세그먼트가 있는 경우 전체 네트워크에 있는 모든 장치의 종합 목록을 생성하려면 각 네트워크 세그먼트에 Rogue Detection Sensor를 별도로 설치해야 합니다.

네트워크 구조(도메인, LDAP, Windows 네트워크) 내의 모든 컴퓨터는 서버 동기화 작업을 통해 자동으로 ESET PROTECT 서버의 컴퓨터 목록에 추가됩니다. RD Sensor는 도메인이나 다른 네트워크 구조에 없는 컴퓨터를 찾아 ESET PROTECT 서버에 추가하는 편리한 방법입니다. RD Sensor는 이미 검색된 컴퓨터를 기억해두고 동일한 정보를 두 번 전송하지 않습니다.



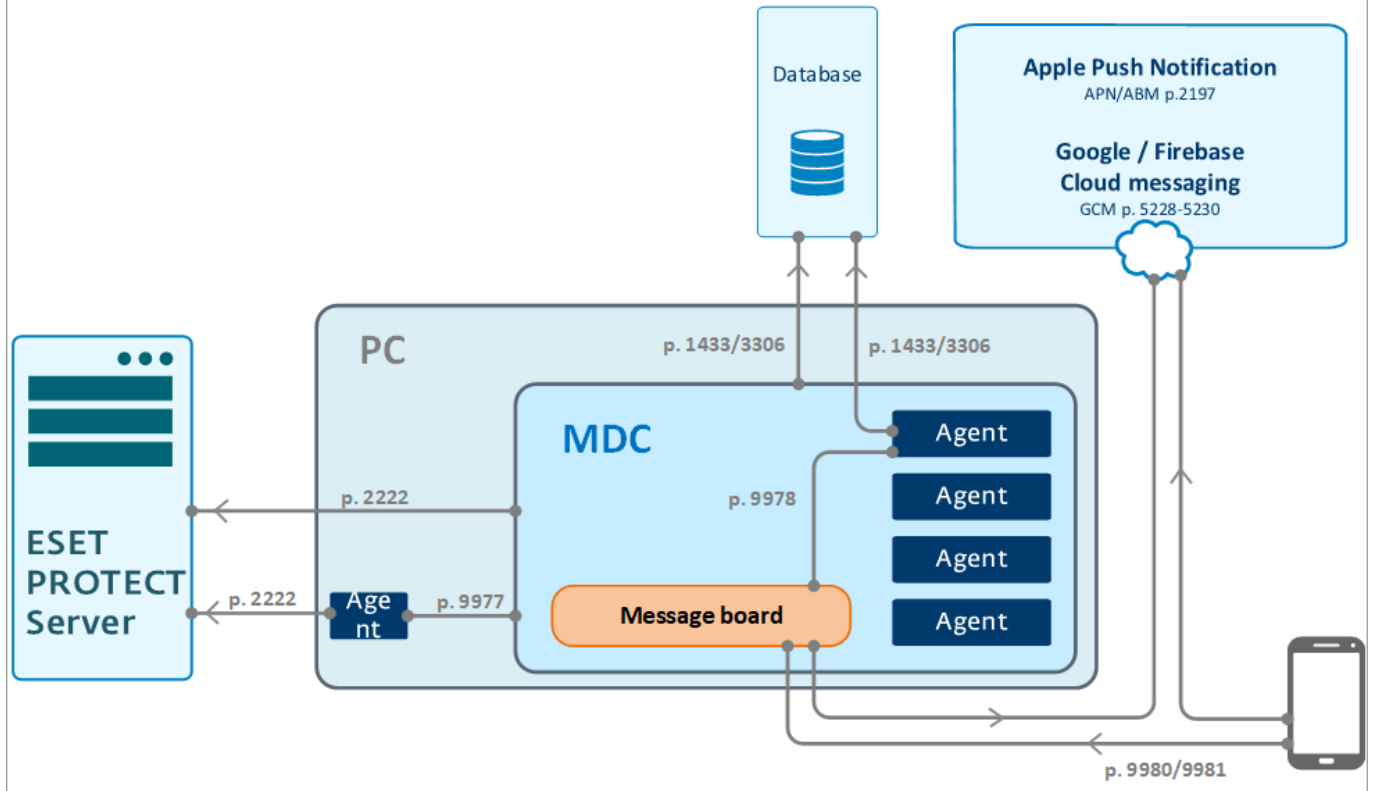
## 모바일 장치 커넥터

ESET PROTECT 모바일 장치 커넥터는 ESET PROTECT를 사용하여 모바일 장치를 관리할 수 있게 해주는 구성 요소로, 모바일 장치(Android 및 iOS)와 Android용 ESET Endpoint Security를 관리할 수 있습니다.



ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

## ESET PROTECT – MDC – Device Communication scheme



[이미지 크게 보기](#)

**i** ESET PROTECT 서버가 호스팅된 것과는 별도의 호스트 장치에 MDM 구성 요소를 배포하는 것이 좋습니다.

약 80개의 관리되는 모바일 장치에 대한 권장되는 하드웨어 전제 조건은 다음과 같습니다.

하드웨어	권장 구성
프로세서	4 코어, 2.5GHz
RAM	4GB(권장)
HDD	100 GB

80개가 넘는 관리되는 모바일 장치의 경우 하드웨어 요구 사항이 별로 높지 않습니다. ESET PROTECT에서 작업을 전송하는 시점과 모바일 장치에서 작업을 실행하는 시점 사이의 시간 지연은 작업 환경의 장치 수에 비례해서 증가합니다.

Windows([통합형 설치 관리자](#) 또는 [구성 요소 설치](#)) 또는 [Linux](#)용 MDM 설치 지침을 따르십시오.

## ESET Bridge HTTP 프록시, 미러 도구 및 직접 연결 간의 차이

ESET 제품 통신에는 탐지 엔진 및 프로그램 모듈 업데이트뿐만 아니라 [ESET LiveGrid®](#) 데이터(아래 [표](#) 참조) 및 라이선스 정보 교환도 포함됩니다.

ESET PROTECT는 배포할 최신 제품을 저장소의 클라이언트 컴퓨터에 다운로드합니다. 제품이 배포되었으면 대상 컴퓨터에 제품을 배포할 준비가 된 것입니다.

ESET 보안 제품이 설치되었으면 활성화해야 합니다. 즉, 제품에서 라이선스 서버에 대한 라이선스 정보를 확인해야 합니다. 활성화 후 검색 엔진 및 프로그램 모듈은 정기적으로 업데이트됩니다.

[ESET LiveGrid® 초기 정보 시스템](#)은 고객을 빠르게 보호하기 위해 ESET에 새로운 침입에 대한 정보가 지속적으로 즉시 제공되도록 도와줍니다. 이 시스템을 사용하면 새로운 탐지가 ESET 연구소로 전송되어 위협을 분석 및 처리할 수 있습니다.

대부분의 네트워크 트래픽은 제품 모듈 업데이트에 의해 생성됩니다. 일반적으로 ESET 보안 제품은 한 달 후에 약 23.9MB의 모듈 업데이트를 다운로드합니다.

[ESET LiveGrid®](#) 데이터(약 22.3MB) 및 업데이트 버전 파일(최대 11KB)은 캐시될 수 없는 유일한 배포 파일입니다.

업데이트에는 수준 업데이트와 nano 업데이트의 두 가지 유형이 있습니다. [업데이트 유형에 대한 자세한 내용은 지식 베이스 문서를 참조하십시오.](#)

업데이트를 컴퓨터 네트워크에 배포할 때 네트워크 부하를 줄이는 두 가지 방법은 [ESET Bridge HTTP 프록시](#) 또는 미러 도구([Windows](#) 및 [Linux](#)용)를 사용하는 것입니다.

**i** 미러 도구 연결(다른 미러 도구에서 업데이트를 다운로드하기 위해 미러 도구 구성)을 설정하려면 [이 지식 베이스 문서](#)를 참조하십시오.

## ESET 통신 유형

통신 유형	통신 빈도	네트워크 트래픽 영향	프록시 전달 통신	프록시 캐시 옵션1	미러링 옵션2	오프라인 환경 옵션
에이전트 배포(저장소에서 푸시/라이브 설치 관리자)	한 번	클라이언트마다 약 50MB	예	예3	아니요	예(GPO / SCCM, 편집된 라이브 설치 관리자)4
끝점 설치(저장소에서 소프트웨어 설치)	한 번	클라이언트마다 약 100MB	예	예3	아니요	예(GPO / SCCM, 패키지 URL을 통한 설치)4
검색 엔진 모듈/프로그램 모듈 업데이트	하루에 6회 이상	월간 23.9MB5	예	예	예	예(오프라인 Mirror Tool 및 사용자 지정 HTTP 서버)6
버전 파일 update.ver 업데이트	하루에 최대 8회	월간 2.6MB7	예	아니요	-	-
활성화/라이선스 확인	하루에 4회	무시할 수 있음	예	아니요	아니요	예(ESET Business Account에 생성된 오프라인 파일)8
ESET LiveGrid® 클라우드 기반 평판	즉시	월간 11MB	예	아니요	아니요	아니요

1.프록시 캐시 영향/이점에 대해서는 [HTTP 프록시 사용 시작 시점](#)을 참조하십시오.

2.미러링 영향에 대해서는 [미러 도구 사용 시작 시점](#)을 참조하십시오.

3.설치/업그레이드마다 하나의 에이전트(특정 버전마다 하나)/끝점을 처음에 배포하여 설치 관리자가 캐시되도록 하는 것이 좋습니다.

4.대규모 네트워크에 ESET Management 에이전트를 배포하려면 [GPO 및 SCCM을 사용한 에이전트 배포](#)를 참조하십시오.

5.초기 검색 엔진 업데이트는 새로운 모든 검색 엔진 업데이트 및 모듈 업데이트가 다운로드되므로 설치 패키지의 기간에 따라 평소 때보다 커질 수 있습니다. 처음에 하나의 클라이언트를 설치하고 업데이트되도록 하여, 필요한 검색 엔진 및 프로그램 모듈 업데이트가 캐시되도록 하는 것이 좋습니다.

6.인터넷 연결 없이 Mirror Tool에서 검색 엔진 업데이트를 다운로드할 수 없습니다. Apache Tomcat을 HTTP 서버로 이용하여 미러 도구([Windows](#) 및 [Linux](#)용)에 사용할 수 있는 디렉토리에 업데이트를 다운로드할 수 있습니다.



7. 검색 엔진 업데이트를 확인할 때 *update.ver* 파일이 항상 다운로드되고 구문 분석됩니다. 기본적으로 ESET 끝점 제품의 스케줄러는 시간마다 새 업데이트를 쿼리합니다. 클라이언트 워크스테이션이 하루에 8시간 켜져 있다고 가정합니다. *update.ver* 파일에는 약 11KB가 포함되어 있습니다.

8. [ESET Business Account에서 오프라인 라이선스 파일을 다운로드하십시오.](#)



ESET Bridge HTTP 프록시를 사용하여 버전 4와 5에 대한 업데이트를 캐시할 수 없습니다. 이러한 제품에 대한 업데이트를 배포하려면 [미러 도구](#)를 사용하십시오.

## ESET Bridge 다음의 사용 시작 시점(HTTP 프록시)

실제 테스트를 수행한 결과, 한 개 네트워크에 37개 이상의 컴퓨터가 있는 경우에는 ESET Bridge HTTP 프록시를 배포할 것을 권장합니다.



효과적으로 캐싱하려면 HTTP 프록시 서버의 날짜와 시간이 올바르게 설정되어 있어야 합니다. 몇 분 차이로 인해 캐싱 메커니즘이 효과적으로 작동하지 않고 필요 이상으로 많은 파일이 다운로드됩니다.

다음은 여러 설치 및 제거가 수행된 1,000대의 컴퓨터가 있는 테스트 네트워크에서 업데이트에만 사용된 네트워크 대역폭을 분석한 결과입니다.

- 인터넷에 직접 연결된 한 대의 컴퓨터에서 평균적으로 매달 23.9MB의 [업데이트](#)를 다운로드합니다(HTTP 프록시는 사용 안 함).
- HTTP 프록시를 사용하는 경우 전체 네트워크에 대해 매달 총 900MB를 다운로드합니다.

다음은 컴퓨터 네트워크에서 직접 인터넷 연결 또는 HTTP 프록시를 사용하여 한 달 동안 다운로드한 업데이트 데이터를 간단하게 비교한 것입니다.

회사 네트워크의 PC 수	25	36	50	100	500	1.000
인터넷에 직접 연결(MB/월)	375	900	1.250	2.500	12.500	25.000
ESET Bridge HTTP 프록시(MB/월)	30	50	60	150	600	900

## Mirror Tool 다음의 사용 시작 시점

미러 도구([Windows](#) 및 [Linux](#)에서 제공)는 사용 가능한 새 업데이트가 있는 경우 새로운 업데이트 요청이 있을 때마다 사용 가능한 모든 수준 및 Nano 업데이트를 다운로드하기 때문에 오프라인 환경이 있는 경우, 즉 네트워크에 있는 컴퓨터가 장기간(몇 개월, 1년) 인터넷에 연결되지 않은 경우 이 도구를 통해서만 제품 모듈 업데이트를 배포할 수 있습니다.



미러 도구 연결(다른 미러 도구에서 업데이트를 다운로드하기 위해 미러 도구 구성)을 설정하려면 [이 지식베이스 문서](#)를 참조하십시오.

ESET Bridge HTTP 프록시와 미러 도구의 주요 차이점은 ESET Bridge HTTP 프록시가 누락된 업데이트(예: Nano 업데이트 3)만 다운로드하는 반면, Mirror Tool은 특정 제품 모듈에 없는 업데이트와 관계없이 사용 가능한 모든 [수준 및 Nano 업데이트](#)(또는 지정된 경우 수준 업데이트만)를 다운로드한다는 것입니다.



**i** 스트리밍된 업데이트는 미리 도구에서 사용할 수 없습니다. 가능한 경우 ESET Bridge HTTP 프록시를 통해 미리에서 업데이트하는 것이 좋습니다. 컴퓨터가 오프라인 상태이지만 인터넷에 연결되어 있고 ESET Bridge HTTP 프록시를 실행하여 업데이트 파일을 캐시할 수 있는 다른 컴퓨터에 액세스할 수 있는 경우에도 이 옵션을 선택합니다.

1,000대의 컴퓨터가 있는 같은 네트워크에서 [ESET Bridge HTTP 프록시](#) 대신 미리 도구를 테스트했습니다. 분석에 따르면 그 달에 5,500MB의 업데이트를 다운로드했습니다. 다운로드한 업데이트 크기는 네트워크에 더 많은 컴퓨터를 추가하여 늘어나지 않았습니다. 이는 클라이언트가 인터넷에 직접 연결된 구성에 비해 부하가 크게 줄어든 것이지만, 성능은 HTTP 프록시를 사용할 때만큼 크게 향상되지 않았습니다.

회사 네트워크의 PC 수	25	36	50	100	500	1,000
인터넷에 직접 연결(MB/월)	375	900	1,250	2,500	12,500	25,000
미리 도구(MB/월)	5,500	5,500	5,500	5,500	5,500	5,500

**i** 네트워크에 1,000대 이상의 컴퓨터가 있더라도 업데이트와 관련하여 대역폭 사용량은 ESET Bridge HTTP 프록시나 미리 도구를 사용함으로써 크게 늘어나지 않았습니다.

## 시스템 요구 사항 및 크기 조정

시스템이 ESET PROTECT을(를) 설치 및 작동하기 위한 일련의 [하드웨어](#), [DB](#), [네트워크](#), [소프트웨어](#) 필수 구성 요소를 충족해야 합니다.

## 지원되는 운영 체제

다음 섹션에서는 [Windows](#), [Linux](#), [macOS](#) 및 [모바일](#) 운영 체제 버전에 대한 ESET PROTECT 구성 요소 지원을 설명합니다.

### Windows

다음 표에는 각 ESET PROTECT 구성 요소에 대해 지원되는 Windows 운영 체제가 표시되어 있습니다.

운영 체제	서버	에이전트	RD Sensor	MDM
<a href="#">KB4493730</a> 및 <a href="#">KB4039648</a> 이 포함된 Windows Server 2008 R2 x64 SP1이(가) 설치됨		✓	✓	
<a href="#">KB4493730</a> 및 <a href="#">KB4039648</a> 이 포함된 Windows Server 2008 R2 CORE x64이(가) 설치됨		✓	✓	
<a href="#">KB4493730</a> 및 <a href="#">KB4039648</a> 이 포함된 Windows Storage Server 2008 R2 x64이(가) 설치됨		✓	✓	
Microsoft SBS 2011 Standard x64		✓	✓	
Microsoft SBS 2011 Essentials x64		✓	✓	
Windows Server 2012 x64	✓	✓	✓	✓
Windows Server 2012 CORE x64	✓	✓	✓	✓

운영 체제	서버	에이전트	RD Sensor	MDM
Windows Server 2012 R2 x64	✓	✓	✓	✓
Windows Server 2012 R2 CORE x64	✓	✓	✓	✓
Windows Storage Server 2012 R2 x64	✓	✓	✓	✓
Windows Server 2016 x64	✓	✓	✓	✓
Windows Storage Server 2016 x64	✓	✓	✓	✓
Windows Server 2019 x64	✓	✓	✓	✓
Windows Server 2022 x64	✓	✓	✓	✓


운영 체제	서버	에이전트	RD Sensor	MDM
최신 Windows 업데이트( <a href="#">KB4474419</a> 및 <a href="#">KB4490628</a> 이상)가 포함된 Windows 7 x86 SP1		✓	✓	
최신 Windows 업데이트( <a href="#">KB4474419</a> 및 <a href="#">KB4490628</a> 이상)가 포함된 Windows 7 x64 SP1		✓	✓	
Windows 8 x86		✓	✓	
Windows 8 x64		✓	✓	❓*
Windows 8.1 x86		✓	✓	
Windows 8.1 x64		✓	✓	❓*
Windows 10 x86		✓	✓	
Windows 10 x64(모든 공식 릴리스)	❓*	✓	✓	❓*
ARM에 있는 Windows 10		✓		
Windows 11 x64 (21H2 및 22H2)	❓*	✓	✓	❓*
ARM에 있는 Windows 11		✓		

**!** ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

\* 클라이언트 OS에 ESET PROTECT 구성 요소를 설치하는 것은 Microsoft 라이선스 정책에 위배될 수 있습니다. 자세한 내용은 Microsoft 라이선스 정책을 확인하거나 소프트웨어 공급업체에 문의하십시오. SMB/소규모 네트워크 환경에서는 ESET PROTECT 설치 또는 [가상 어플라이언스](#)(해당하는 경우)를 고려하는 것이 좋습니다.

### 이전 Microsoft Windows 시스템

- ESET Management Agent 10.x는 [Windows 7/8.x](#) 및 [Windows Server 2008 R2/Microsoft SBS 2011](#)을 지원하는 최신 버전입니다.
- 항상 최신 서비스 팩을 설치하십시오. 특히 Server 2008 및 Windows 7와 같은 구형 시스템에서 이 작업이 필요합니다.
- !** • ESET PROTECT에서는 Windows 7(SP 미포함), Windows Vista 및 Windows XP를 실행하는 컴퓨터의 관리 기능을 지원하지 않습니다.
- 2020년 3월 24일부터 ESET은 Microsoft Windows 운영 체제 Windows 7, Windows Server 2008(모든 버전)에 설치된 ESET PROTECT(Server 및 MDM)에 대한 기술 지원을 더 이상 공식적으로 제공하지 않습니다. 불법 또는 불법 복제 운영 체제를 지원하지 않습니다.

 2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.


 ESXi가 없어도 서버가 아닌 OS에서 ESET PROTECT을(를) 실행할 수 있습니다. 데스크톱 운영 체제에 [VMware Player](#)를 설치하고 [ESET PROTECT 가상 어플라이언스](#)를 배포할 수 있습니다.

## Linux

다음 표에는 각 ESET PROTECT 구성 요소에 대해 지원되는 Linux 운영 체제가 표시되어 있습니다.

운영 체제	서버	에이전트	RD Sensor	MDM
Ubuntu 16.04.1 LTS x64 Desktop	✓	✓	✓	☒*
Ubuntu 16.04.1 LTS x64 Server	✓	✓	✓	☒*
Ubuntu 18.04.1 LTS x64 Desktop	✓	✓	✓	☒*
Ubuntu 18.04.1 LTS x64 Server	✓	✓	✓	☒*
Ubuntu 20.04 LTS x64	✓	✓	✓	☒*
Ubuntu 22.04 LTS x64		✓	✓	
Linux Mint 20		✓	✓	
RHEL Server 7 x64	✓	✓	✓	☒*
RHEL Server 8 x64	☒**	✓		☒**
RHEL Server 9 x64		✓	✓	
CentOS 7 x64	✓	✓	✓	☒*
SLED 15 x64		✓	✓	
SLES 12 x64		✓	✓	
SLES 15 x64		✓	✓	
Debian 9 x64		✓	✓	
Debian 10 x64	✓	✓	✓	☒*
Debian 11 x64		✓	✓	
Oracle Linux 8		✓	✓	
Amazon Linux 2		✓	✓	

\*

 ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

\*\* Red Hat Enterprise Linux Server 8.x은 .pdf 보고서 생성 작업을 지원하지 않습니다. [ESET PROTECT의 알려진 문제](#)에서 자세한 내용을 참조하십시오.

## macOS

운영 체제	에이전트
macOS Sierra (10.12)	✓
macOS High Sierra (10.13)	✓
macOS Mojave (10.14)	✓
macOS Catalina (10.15)	✓
macOS Big Sur (11.0)	✓
macOS Monterey (12.0)	✓
macOS Ventura (13.0)	✓

**i** macOS는 클라이언트로서만 지원됩니다. [ESET Management 에이전트](#) 및 [macOS용 ESET 제품](#)은 macOS에 설치할 수 있습니다. 그러나 ESET PROTECT 서버는 macOS에 설치할 수 없습니다.

## 모바일

**!** ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

운영 체제	EESA	EESA 장치 소유자	MDM iOS	MDM iOS ABM
Android 6.x+	✓			
Android 7.x+	✓	✓		
Android 8.x+	✓	✓		
Android 9.0	✓	✓		
Android 10.0	✓	✓		
Android 11	✓	✓		
Android 12	✓	✓		
Android 13	✓	✓		
iOS 9.x+			✓	?
iOS 10.x+			✓	?
iOS 11.x+			✓	?
iOS 12.0.x			✓	?
iOS 13.x+			✓	✓
iOS 14.x+			✓	✓
iOS 15			✓	✓
iOS 16			✓	✓
iPadOS 13.x+			✓	✓
iPadOS 14.x+			✓	✓
iPadOS 15			✓	✓
iPadOS 16			✓	✓

\* iOS DEP는 [선택한 국가](#)에서만 사용할 수 있습니다.



중요한 보안 패치를 계속해서 받으려면 모바일 장치 OS를 최신 버전으로 업데이트하는 것이 좋습니다.

### ^ iOS 10.3 이상의 요구 사항:

iOS 10.3 릴리스 이후에 등록 프로파일의 일부로 설치된 CA는 자동으로 신뢰할 수 없는 상태가 될 수 있습니다. 이 문제를 해결하려면 아래 단계를 따르십시오.

a) [Apple이 신뢰하는 인증서 발급자](#)가 발급한 인증서를 사용합니다.

b) 등록하기 전에 인증서 신뢰를 수동으로 설치합니다. 즉, 등록하기 전에 모바일 장치에 루트 CA를 수동으로 설치하고, 설치된 인증서에 대해 [전체 신뢰를 활성화](#)해야 합니다.

### ^ iOS 12D의 요구 사항:

iOS 10.3 이상의 요구 사항을 검토하십시오.

- 연결에는 **TLS 1.2** 이상을 사용해야 합니다.
- 연결에는 **AES-128** 또는 **AES-256 대칭 암호**를 사용해야 합니다. 협상된 TLS 연결 암호 그룹은 **ECDHE(Elliptic Curved Diffie-Hellman Ephemeral) 키 교환**을 통해 **PFS(Perfect Forward Secrecy)**를 지원해야 하며 다음 중 하나여야 합니다.

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

- 길이가 **2048비트 이상인 RSA 키**로 서명해야 합니다. 인증서의 해시 알고리즘은 **다이제스트 길이가 256자 이상인 SHA-2**("지문"이라고도 함)여야 합니다(즉, **SHA-256 이상**). [고급 보안](#)을 설정하여 ESET PROTECT에서 이러한 요구 사항이 있는 인증서를 생성할 수 있습니다.

- 인증서에는 **루트 CA를 포함하는 전체 인증서 체인**이 포함되어야 합니다. 인증서에 포함된 루트 CA는 장치와의 신뢰를 설정하는 데 사용되며 MDM 등록 프로파일의 일부로 설치됩니다.

### ^ iOS 12D의 요구 사항:

- iOS 13 모바일 장치를 관리하려면 새 Apple 통신 인증서(MDM HTTPS) [요구 사항](#)을 충족해야 합니다. 2019년 7월 1일 이전에 발급된 인증서도 이러한 기준을 충족해야 합니다.
- ESMC CA에서 서명한 HTTPS 인증서는 이러한 요구 사항을 충족하지 않습니다.



Apple 통신 인증서 [요구 사항](#)을 충족하기 전에 모바일 장치를 iOS 13으로 업그레이드하지 않는 것이 좋습니다. 업그레이드할 경우 ESET PROTECT MDM에 대한 장치의 연결이 중단됩니다.

- 적절한 인증서 없이 이미 업그레이드했으며 ESET PROTECT MDM에 대한 장치의 연결이 중단된 경우 먼저 iOS 장치와 통신하는 데 사용된 현재 HTTPS 인증서를 Apple 통신 인증서(MDM HTTPS) [요구 사항](#)을 충족하는 인증서로 변경한 후 iOS 장치를 다시 등록해야 합니다.

- iOS 13으로 업그레이드하지 않은 경우 iOS 장치와 통신하는 데 사용된 현재 MDM HTTPS 인증서가 Apple 통신 인증서(MDM HTTPS) [요구 사항](#)을 충족하는지 확인합니다. 충족하는 경우 iOS 장치를 iOS 13으로 계속 업그레이드할 수 있습니다. 요구 사항을 충족하지 않으면 현재 MDM HTTPS 인증서를 Apple 통신 인증서(MDM HTTPS) [요구 사항](#)을 충족하는 HTTPS 인증서로 변경한 다음 계속해서 iOS 장치를 iOS 13으로 업그레이드합니다.

# 지원되는 워크스테이션 프로비저닝 환경

워크스테이션 프로비저닝을 사용하면 장치를 더 쉽게 관리할 수 있으며 워크스테이션 컴퓨터를 최종 사용자에게 더 빨리 전달할 수 있습니다.

프로비저닝된 데스크톱은 일반적으로 실제 또는 가상입니다. 스트리밍된 OS(Citrix 프로비저닝 서비스)를 사용하는 가상화된 환경의 경우 [지원되는 하이퍼바이저](#) 목록을 참조하십시오.

ESET PROTECT [지원](#):

- 비영구 디스크가 있는 시스템
- VDI 환경
- 복제된 컴퓨터 식별

## 지원되는 하이퍼바이저 및 하이퍼바이저 확장

하이퍼바이저	ESET PROTECT	ESET Full Disk Encryption
Citrix XenServer	✓	X
Microsoft Hyper-V	✓	✓(보안 부팅은 지원되지 않음)
VMware vSphere	✓	✓ (7.0.3.00300)
VMware ESXi	✓	✓ (7.0)
VMware Workstation	✓	✓ (16.2.3)
VMware View	✓	X
Oracle VirtualBox	✓	X
VMware Fusion	X	✓ (12.2.3)
Parallels	X	✓

하이퍼바이저 확장	ESET PROTECT	ESET Full Disk Encryption
Citrix VDI-in-a-box	✓	X
Citrix XenDesktop	✓	X

## 도구

(가상 컴퓨터와 물리적 컴퓨터 둘 다에 적용됨)

- Microsoft SCCM
- Windows Server 2012/2016/2019/2022 서버 관리자
- Windows 관리 센터

# 하드웨어 및 인프라 크기 조정

ESET PROTECT 서버 컴퓨터는 아래 표의 다음 하드웨어 권장 사항을 충족해야 합니다.

클라이언트 수	ESET PROTECT 서버 + SQL DB 서버				
	CPU 코어	CPU 클럭 속도(GHz)	RAM(GB)	디스크 드라이브 <sup>1</sup>	디스크 IOPS <sup>2</sup>
최대 1,000개	4	2.1	4	단일	500
5,000	8	2.1	8		1,000
10,000 3	4	2.1	16	별도	2,000
20,000	4	2.1	16		4,000
50,000	8	2.1	32		10,000
100,000	16	2.1	64+		20,000

1 단일/별도 디스크 드라이브 - 클라이언트가 10,000개 이상인 시스템의 경우 별도 드라이브에 [DB](#)를 설치하는 것이 좋습니다.

2 IOPS(초당 총 I/O 작업) - 최소 필수 값입니다.

- 연결된 클라이언트(500개 정도)당 약 0.2 IOPS를 사용하는 것이 좋습니다.
- [diskspd](#) 도구를 사용하여 드라이브의 IOPS를 확인할 수 있습니다. 다음 명령을 사용하십시오.

클라이언트 수	명령
최대 5,000개 클라이언트	<code>diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat</code>
5,000개 이상의 클라이언트	<code>diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat</code>

3 10,000개의 클라이언트 환경에 대한 [예제 시나리오](#)를 참조하십시오.

## 디스크 드라이브 권장 사항

디스크 드라이브는 ESET PROTECT 성능에 영향을 미치는 중요한 요소입니다.

- SQL Server 인스턴스에서 리소스를 ESET PROTECT 서버와 공유하여 활용률을 극대화하고 지연을 최소화할 수 있습니다. 단일 컴퓨터에서 ESET PROTECT 서버 및 DB 서버를 실행하여 ESET PROTECT 성능을 향상시킵니다.
- 별도의 드라이브(가능하면 별도의 물리적 SSD 드라이브)에 DB 및 거래 로그 파일을 배치하는 경우 SQL 서버의 성능이 향상됩니다.
- 단일 디스크 드라이브가 있는 경우 SSD 드라이브를 사용하는 것이 좋습니다.
- 올플래시 아키텍처를 사용하는 것이 좋습니다. 반도체 디스크(SSD)가 표준 HDD보다 훨씬 더 빠릅니다.
- RAM 구성이 높은 경우 SAS를 R5로 설정하면 충분합니다. 테스트된 구성: R5의 10x 1.2TB SAS디스크 -

추가 캐싱 없이 4+1의 두 패리티 그룹.

- IOPS가 높은 엔터프라이즈급 SSD를 사용하면 성능이 향상되지 않습니다.
- 클라이언트의 수에 관계없이 100GB 용량이면 충분합니다. 종종 DB를 백업하는 경우 더 높은 용량이 필요할 수 있습니다.
- 네트워크 드라이브의 성능이 ESET PROTECT의 속도를 저하시키므로 네트워크 드라이브를 사용하지 마십시오.
- 온라인 저장소 마이그레이션을 허용하는 작업 다중 계층 저장소 인프라가 있는 경우, 속도가 더 느린 공유 계층으로 시작하여 ESET PROTECT 성능을 모니터링하는 것이 좋습니다. 읽기/쓰기 지연 시간이 20ms를 초과하면 저장소 계층에서 더 빠른 계층으로 무중단 이동하여 가장 비용 효율적인 백엔드를 사용할 수 있습니다. 하이퍼바이저에서 동일한 작업을 수행할 수 있습니다(ESET PROTECT을(를) 가상 컴퓨터로 사용하는 경우).

## 다양한 클라이언트 수에 대한 크기 권장 사항

아래에서 설정된 클라이언트 수로 1년간 실행되는 가상 환경의 성능 결과를 확인할 수 있습니다.

**i** DB와 ESET PROTECT이(가) 동일한 하드웨어 구성으로 별도의 가상 컴퓨터에서 실행됩니다.

CPU 코어	CPU 클럭 속도(GHz)	RAM(GB)	성능		
			클라이언트 10,000개	클라이언트 20,000개	클라이언트 40,000개
8	2.1	64	높음	높음	보통
8	2.1	32	보통	보통	보통
4	2.1	32	보통	보통	낮음
2	2.1	16	낮음	낮음	부족
2	2.1	8	매우 낮음 (권장되지 않음)	매우 낮음 (권장되지 않음)	부족

## 배포 권장 사항

### ESET PROTECT 배포에 대한 모범 사례

클라이언트 수	최대 1,000개	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100,000+
같은 컴퓨터에 있는 ESET PROTECT 서버 및 DB 서버	✓	✓	✓	X	X	X
Microsoft SQL Express 사용	✓	✗*	X	X	X	X
Microsoft SQL 사용	✓	✓	✓	✓	✓	✓
MySQL 사용	✓	✓	✓	X	X	X
ESET PROTECT 가상 어플라이언스 사용	✓	✓	권장되지 않음	X	X	X
VM 서버 사용	✓	✓	✓	옵션	X	X
권장 연결 간격(배포 단계 중)	60초	5분	10분	15분	20분	25분
권장 연결 간격(배포 후, 일반 사용 시)	10분	10분	20분	30분	40분	60분



\* ESET PROTECT 데이터베이스 작성을 피하기 위해, ESET Inspect도 사용하는 경우 이 시나리오를 권장하지 않습니다.

## 연결 간격

ESET PROTECT 서버는 영구 연결을 사용하여 ESET Management 에이전트에 연결되어 있습니다. 영구 연결에도 불구하고 데이터 전송은 연결 간격 동안 한 번만 발생합니다. 예를 들어 5,000개 클라이언트의 복제 간격이 8분으로 설정된 경우 480초 동안 5,000개의 전송(초당 10.4)이 발생합니다. 적합한 [클라이언트 연결 간격](#)을 설정해야 합니다. 고성능 하드웨어 구성을 위해서는 에이전트 - 서버 연결의 총 수를 초당 1,000개 미만으로 유지해야 합니다.

서버가 과부하되거나 댐웨어가 발생하는 경우(예: 10분당 10,000대의 클라이언트에만 서비스를 제공할 수 있는 서버에 20,000대의 클라이언트 연결) 연결된 클라이언트 중 일부는 건너뛰게 됩니다. 연결되지 않은 클라이언트는 나중에 ESET PROTECT 서버에 연결을 시도합니다.

## 단일 서버(중소기업)

소규모 네트워크(1,000개 이하 클라이언트)를 관리하려는 경우 ESET PROTECT 서버와 모든 ESET PROTECT 구성 요소가 설치되어 있는 단일 컴퓨터를 사용합니다. SMB/소규모 네트워크 환경에서는 ESET PROTECT 설치 또는 [가상 어플라이언스](#)(해당하는 경우)를 고려하는 것이 좋습니다.

## 프록시가 있는 원격 지사

클라이언트 컴퓨터를 ESET PROTECT 서버에서 직접 볼 수 없으면 [프록시](#)를 사용하여 ESET 제품 통신을 전달하십시오. HTTP 프록시는 통신을 집계하거나 복제 트래픽을 낮추지 않습니다.

## 고가용성(대기업)

엔터프라이즈 환경(10,000개 이상의 클라이언트)의 경우 다음을 고려하십시오.

- [RD Sensor](#)는 네트워크를 검색하고 새 컴퓨터를 찾는 데 도움이 됩니다.
- 장애 조치(Failover) 클러스터에 ESET PROTECT 서버를 설치할 수 있습니다.
- 많은 수의 클라이언트에 대해 HTTP 프록시를 구성하거나 더 많은 프록시를 사용하십시오.

## 엔터프라이즈 솔루션 또는 저성능 시스템용 웹 콘솔 구성

기본적으로 Windows용 통합형 설치 관리자를 통해 설치된 ESET PROTECT 웹 콘솔은 Apache Tomcat용으로 1024MB의 메모리 제한을 예약합니다.

인프라에 따라 기본 웹 콘솔 구성을 변경할 수 있습니다.

- 엔터프라이즈 환경에서 많은 수의 개체로 작업할 경우 기본 웹 콘솔 구성이 불안정해질 수 있습니다. 메모리 부족을 예방하기 위해 Tomcat 설정을 변경하십시오. 이와 같이 변경하기 전에 RAM이 충분(16GB 이상)한지 확인합니다.
- 하드웨어 리소스가 제한된 저성능 시스템이 있는 경우 Tomcat 메모리 사용량을 줄일 수 있습니다.



아래 제공된 메모리 값은 권장 사항입니다. 하드웨어 리소스에 따라 Tomcat 메모리 설정을 조정할 수 있습니다.

## Windows

1. `tomcat9w.exe`를 열거나 `Configure Tomcat` 응용 프로그램을 실행합니다.
2. **Java** 탭으로 전환합니다.
3. 메모리 사용량 변경:
  - a. 증가(엔터프라이즈): 초기 메모리 풀 값을 2048MB로 변경하고 최대 메모리 풀을 16384MB로 변경합니다.
  - b. 감소(저성능 시스템): 초기 메모리 풀 값을 2048MB로 변경하고 최대 메모리 풀을 16384MB로 변경합니다.
4. Tomcat 서비스를 다시 시작합니다.

## LINUX 및 ESET PROTECT 가상 어플라이언스

1. 루트 권한으로 터미널을 열거나 `sudo`를 사용하십시오.
2. 파일 열기:
  - a. ESET PROTECT 가상 어플라이언스/CentOS: `/etc/sysconfig/tomcat`
  - b. Debian: `/etc/default/tomcat9`
3. 파일에 다음 줄을 추가합니다.
  - a. 메모리 사용량 증가(엔터프라이즈): `JAVA_OPTS="-Xms2048m -Xmx16384m"`
  - b. 메모리 사용량 감소(저성능 시스템): `JAVA_OPTS="-Xms256m -Xmx2048m"`
4. 파일을 저장하고 Tomcat 서비스를 다시 시작하십시오.  
`service tomcat restart`

# 10,000개의 클라이언트에 대한 배포

아래에서 10,000개의 클라이언트가 1년 동안 실행되는 가상 환경의 성능 결과를 확인할 수 있습니다.

## 하이퍼바이저 서버 구성

구성 요소	값
VMware	ESXi 6.7 업데이트 2 이상(VM 버전 15)
하이퍼바이저	VMware ESXi, 6.7.0
논리 프로세서	112
프로세서 유형	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz



## 전용 컴퓨터에서 테스트 실행

DB와 ESET PROTECT이(가) 동일한 하드웨어 구성으로 별도의 가상 컴퓨터에서 실행됩니다.

## 가상 머신에 사용되는 소프트웨어

ESET PROTECT:

- OS: Microsoft Windows Server 2016 Standard (64-bit)

DB:

- Database server: Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- OS: Microsoft Windows Server 2016 Standard (64-bit)

## ESET PROTECT 환경 설명

- 10,000개의 연결된 클라이언트
- 동적 그룹을 위한 약 2,000개의 동적 그룹과 2,000개의 템플릿
- 약 255개의 정적 그룹
- 사용자 20명
- ESET Management 에이전트에 대한 15분 연결 간격
- 환경이 1년 동안 실행된 후 DB 크기는 15GB입니다.

CPU 수	RAM(GB)	성능
8	64	높음
4	32	보통
2	16	낮음
2	8	매우 낮음 (권장되지 않음)

## DB

ESET PROTECT 서버를 설치할 때 사용할 DB 서버 및 커넥터를 지정합니다. 사용자 환경에서 실행되고 있는 기존 DB 서버를 사용할 수 있지만 아래 요구 사항을 충족해야 합니다.

ESET PROTECT 10.0 [통합형 설치 관리자](#)는 기본적으로 Microsoft SQL Server Express 2019를 설치합니다.

0이전 Windows 버전(Server 2012 또는 SBS 2011)을 사용하는 경우 기본적으로 Microsoft SQL Server Express 2014가 설치됩니다.


o 설치 관리자는 데이터베이스 인증을 위해 임의의 패스워드를 자동으로 생성합니다(%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini에 저장됨).

Microsoft SQL Server Express는 각 관계형 DB의 크기가 10GB로 제한되어 있습니다. Microsoft SQL Server Express를 사용하지 않는 것이 좋습니다.

- 엔터프라이즈 환경 또는 대규모 네트워크에서.
- [ESET Inspect](#)과(와) 함께 ESET PROTECT을(를) 사용하려는 경우


## 지원되는 DB 서버 및 DB 커넥터

ESET PROTECT에서는 다음 두 가지 유형의 DB 서버가 지원됩니다. Microsoft SQL Server 및 MySQL.

 ESET PROTECT에서는 MariaDB를 지원하지 않습니다. MariaDB는 대부분의 현재 Linux 환경에서 기본 DB이며, MySQL을 설치하도록 선택하면 설치됩니다.

지원되는 DB 서버	지원되는 DB 버전	지원되는 DB 커넥터
Microsoft SQL Server	<ul style="list-style-type: none"> <li>• Express 및 Express 이외의 버전</li> <li>• 2014, 2016, 2017, 2019</li> </ul>	<ul style="list-style-type: none"> <li>• SQL 서버</li> <li>• SQL Server Native Client 10.0</li> <li>• SQL Server 11, 13, 17, 18용 ODBC 드라이버</li> </ul>
MySQL	<ul style="list-style-type: none"> <li>• 5.6*</li> <li>• 5.7</li> <li>• 8.0</li> </ul>	<p>MySQL ODBC 드라이버 버전:</p> <ul style="list-style-type: none"> <li>• 5.1, 5.2</li> <li>• 5.3.0-5.3.10</li> <li>• 8.0.16, 8.0.17</li> <li>• 8.0.27, 8.0.31 Windows만 해당</li> </ul>

\* MySQL 5.6은 2021년 2월에 종료되었습니다. MySQL DB 서버를 버전 5.7 이상으로 [업그레이드](#)하는 것이 좋습니다.

 다음 MySQL ODBC 드라이버 버전은 지원되지 않습니다.

- 5.3.11 이상 5.3.x
- 8.0.0-8.0.15
- 8.0.18 이상

## DB 서버 하드웨어 요구 사항

[하드웨어](#) 및 크기 조정 지침을 참조하십시오.

## 성능 권장 사항

최상의 성능을 얻으려면 지원되는 최신 Microsoft SQL Server를 ESET PROTECT DB로 사용하는 것이 좋습니다. ESET PROTECT는 MySQL과 호환되지만 MySQL을 사용하면 대량의 데이터로 작업할 경우 대시보드, 탐지, 클라이언트를 비롯하여 성능에 부정적인 영향을 미칠 수 있습니다. Microsoft SQL Server를 사용하는 동일한 하드웨어는 MySQL보다 훨씬 많은 클라이언트를 처리할 수 있습니다.

다음 위치에 SQL DB 서버를 설치할지 여부를 결정할 수 있습니다.

- ESET PROTECT 서버와 동일한 컴퓨터.

- 별도 디스크에 있지만 동일한 컴퓨터.
- SQL DB 서버를 설치하기 위한 전용 서버

10,000대 이상의 클라이언트를 관리하려는 경우 예약된 리소스가 있는 전용 컴퓨터를 사용하는 것이 좋습니다.

DB	SMB 고객	엔터프라이즈 고객	클라이언트 제한	Windows	Linux
Microsoft SQL Express	✓	(옵션)	5.000	✓	
Microsoft SQL Server	✓	✓	없음	✓	
MySQL	✓	✓	10.000	✓	✓

## 추가 정보



ESET PROTECT 서버는 통합 백업을 사용하지 않습니다. 데이터 손실을 방지하려면 DB 서버를 [백업](#)하는 것이 좋습니다.

- [도메인 컨트롤러에 SQL Server를 설치하지 마십시오](#)(예: Windows SBS/Essentials). ESET PROTECT 제품을 다른 서버에 설치하거나 설치 중에 SQL Server Express 구성 요소를 선택하지 않는 것이 좋습니다(이 경우 기존 SQL 또는 MySQL Server를 사용하여 ESET PROTECT DB를 실행해야 함).
- ESET PROTECT DB에만 접근할 수 있는 전용 DB 사용자 계정을 사용하려면 설치 전에 특정 권한을 가진 사용자 계정을 만들어야 합니다. 자세한 내용은 [전용 DB 사용자 계정](#)을 참조하십시오. 또한 ESET PROTECT에서 사용할 빈 DB를 만들어야 합니다.
- [Windows용 MySQL](#) 및 [Linux용 MySQL](#)을 설치하고 ESET PROTECT 제품과 제대로 작동하도록 구성하는 방법에 대한 지침을 참조하십시오.
- [Linux에서 Microsoft SQL Server](#)는 지원되지 않습니다. 그러나 [Linux의 ESET PROTECT 서버를 Windows의 Microsoft SQL Server에 연결](#)할 수 있습니다.
- [별도의 컴퓨터](#)에 ESET PROTECT 서버 및 Microsoft SQL Server를 설치하는 경우 [DB에 암호화된 연결을 활성화](#)할 수 있습니다.
- Windows 환경에서 DB의 클러스터 설정은 Microsoft SQL Server(MySQL 아님)에만 지원됩니다.

## 지원되는 Apache Tomcat 및 Java 버전

### Apache Tomcat

Apache Tomcat은 ESET PROTECT 웹 콘솔을 실행하는 데 필요한 필수 구성 요소입니다.

ESET PROTECT에서는 Apache Tomcat 9.x(64비트)만 지원합니다. 최신 Apache Tomcat 버전 9.x을 사용하는 것이 좋습니다.

ESET PROTECT는 Apache Tomcat의 알파/베타/RC 버전은 지원하지 않습니다.

## Java

Apache Tomcat에는 64비트 Java/OpenJDK가 필요합니다.

시스템에 여러 가지 Java 버전이 설치되어 있는 경우, 이전 Java 버전을 제거하고 [지원되는 Java](#) 최신 버전만 유지하는 것이 좋습니다.

**⚠** 2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.

## 지원되는 웹 브라우저, ESET 보안 제품 및 언어

ESET PROTECT는 다음 운영 체제를 지원합니다.

- [Windows](#), [Linux](#) 및 [macOS](#)

ESET PROTECT 웹 콘솔은 다음 웹 브라우저에서 실행됩니다.

웹 브라우저
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

ESET PROTECT 웹 콘솔을 최적으로 사용하려면 웹 브라우저를 최신 상태로 유지하는 것이 좋습니다.

## ESET PROTECT10.0를 통해 관리할 수 있는 최신 버전의 ESET 제

제품	제품 버전
ESET Endpoint Security for Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Antivirus for Windows	7.3, 8.x, 9.x, 10.x
macOS용 ESET Endpoint Security	6.10 이상
macOS용 ESET Endpoint Antivirus	6.10 이상
ESET Endpoint Security for Android	2.x, 3.x
Microsoft Windows Server용 ESET Server Security(이전의 Microsoft Windows Server용 ESET File Security)	7.3, 8.x, 9.x, 10.x
Microsoft Exchange Server용 ESET Mail Security	7.3, 8.x, 9.x, 10.x
ESET Security for Microsoft SharePoint Server	7.3, 8.x, 9.x, 10.x
IBM Domino용 ESET Mail Security	7.3, 8.x, 9.x

제품	제품 버전
Linux-용 ESET Server Security(이전의 Linux-용 ESET File Security)	7.2, 8.x, 9.x
ESET Endpoint Antivirus Linux의 경우	7.1, 8.x, 9.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.6+
ESET Full Disk Encryption for Windows	
macOS-용 ESET Full Disk Encryption	

## ESET PROTECT 10.0 을 통해 관리할 수 있는 이전 버전의 ESET 제품:

제품	제품 버전
ESET Endpoint Security for Windows	6.5
ESET Endpoint Antivirus for Windows	6.5
Microsoft Windows Server-용 ESET File Security	6.5
Microsoft Exchange Server-용 ESET Mail Security	6.5
IBM Domino-용 ESET Mail Security	6.5
ESET Security for Microsoft SharePoint Server	6.5

**i** 위의 표에 나온 버전보다 이전의 ESET 보안 제품 버전은 ESET PROTECT 10.0을(를) 사용하여 관리할 수 없습니다.  
호환성에 대한 자세한 내용은 [ESET 비즈니스 제품의 만료 정책](#)을 참조하십시오.

## 구독 라이선스를 통해 활성화를 지원하는 제품

ESET 제품	다음 제품 버전부터 사용 가능
ESET Endpoint Antivirus/Security for Windows	7.0
ESET Endpoint Antivirus/Security for macOS	6.8.x
ESET Endpoint Security for Android	2.0.158
ESET Mobile Device Management for Apple iOS	7.0
Microsoft Windows Server-용 ESET File Security	7.0
ESET Mail Security for Microsoft Exchange	7.0
Windows Server-용 ESET File Security	7.0
IBM Domino-용 ESET Mail Security	7.0
ESET Security for Microsoft SharePoint Server	7.0
ESET File Security Linux의 경우	7.0
ESET Endpoint Antivirus Linux의 경우	7.0
ESET Server Security 용 Windows	8.0
ESET Server Security 용 Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect(Windows 7.3 이상-용 ESET Endpoint 사용)	1.5

## 지원되는 언어

언어	코드
영어(미국)	en-US
아랍어(이집트)	ar-EG
중국어 간체	zh-CN
중국어 번체	zh-TW
크로아티아어(크로아티아)	hr-HR
체코어(체코 공화국)	cs-CZ
프랑스어(프랑스)	fr-FR
프랑스어(캐나다)	fr-CA
독일어(독일)	de-DE
그리스어(그리스)	el-GR
헝가리어(헝가리)*	hu-HU
인도네시아어(인도네시아)*	id-ID
이탈리아어(이탈리아)	it-IT
일본어(일본)	ja-JP
한국어(한국)	ko-KR
폴란드어(폴란드)	pl-PL
포르투갈어(브라질)	pt-BR
러시아어(러시아)	ru-RU
스페인어(칠레)	es-CL
스페인어(스페인)	es-ES
슬로바키아어(슬로바키아)	sk-SK
터키어(터키)	tr-TR
우크라이나어(우크라이나)	uk-UA

\* 제품만 이 언어로 제공되며 온라인 도움말은 제공되지 않습니다.

## 네트워크

ESET PROTECT에 의해 관리되는 ESET PROTECT 서버와 클라이언트 컴퓨터가 ESET 저장소 및 제품 활성화 서버에 연결할 수 있도록 ERA 서버와 클라이언트 컴퓨터 둘 다에는 작동하는 인터넷 연결이 필요합니다. 클라이언트가 인터넷에 직접 연결되지 않도록 하려는 경우 프록시 서버([ESET Bridge HTTP 프록시](#)와 동일하지 않음)를 사용하면 네트워크 및 인터넷과 원활하게 통신할 수 있습니다.

ESET PROTECT에 의해 관리되는 컴퓨터는 ESET PROTECT 서버와 동일한 LAN에 연결되거나 동일한 *Active Directory* 도메인에 있어야 합니다. 클라이언트 컴퓨터가 ESET PROTECT 서버를 볼 수 있어야 합니다. 또한 클라이언트 컴퓨터가 원격 배포 및 Wake-up call 기능을 사용하기 위해서는 ESET PROTECT 서버와 통신할 수 있어야 합니다.

Windows/Linux용 ESET PROTECT 제품은 IPv4 및 IPv6 인터넷 프로토콜과 모두 호환됩니다. ESET PROTECT 가상 어플라이언스는 IPv4와만 호환됩니다.



## 사용되는 포트

네트워크에서 방화벽을 사용하면, ESET PROTECT 및 해당 구성 요소가 인프라에 설치된 경우 사용되는 가능한 [네트워크 통신 포트](#) 목록을 참조하십시오.

## ESET PROTECT 서버 및 ESET Management 에이전트 통신이 네트워크 트래픽에 미치는 영향

클라이언트 컴퓨터의 애플리케이션은 ESET PROTECT 서버와 직접 통신하지 않으며, ESET Management 에이전트가 이 통신을 지원합니다. 이 솔루션을 사용하면 네트워크를 통해 전송되는 데이터를 보다 쉽게 관리하고 데이터 전송량을 줄일 수 있습니다. 네트워크 트래픽은 클라이언트에서 수행되는 작업 유형 및 클라이언트 연결 간격에 따라 결정됩니다. 클라이언트에서 실행되거나 예약된 작업이 없는 경우에도 ESET Management 에이전트는 연결 간격마다 한 번씩 ESET PROTECT 서버와 통신하며, 각 연결마다 트래픽이 생성됩니다. 트래픽 예는 아래 표를 참조하십시오.

동작 유형	단일 연결 간격에서의 트래픽
클라이언트 작업: 치료하지 않고 검사	4kB
클라이언트 작업: 모듈 업데이트	4kB
클라이언트 작업: SysInspector 로그 요청	300kB
정책 안티바이러스 - 최대 보안	144kB

ESET Management 에이전트 복제 간격	유휴 ESET Management 에이전트에서 생성된 일일 트래픽
1분	16MB
15분	1MB
30분	0.5MB
1시간	144kB
1일	12kB

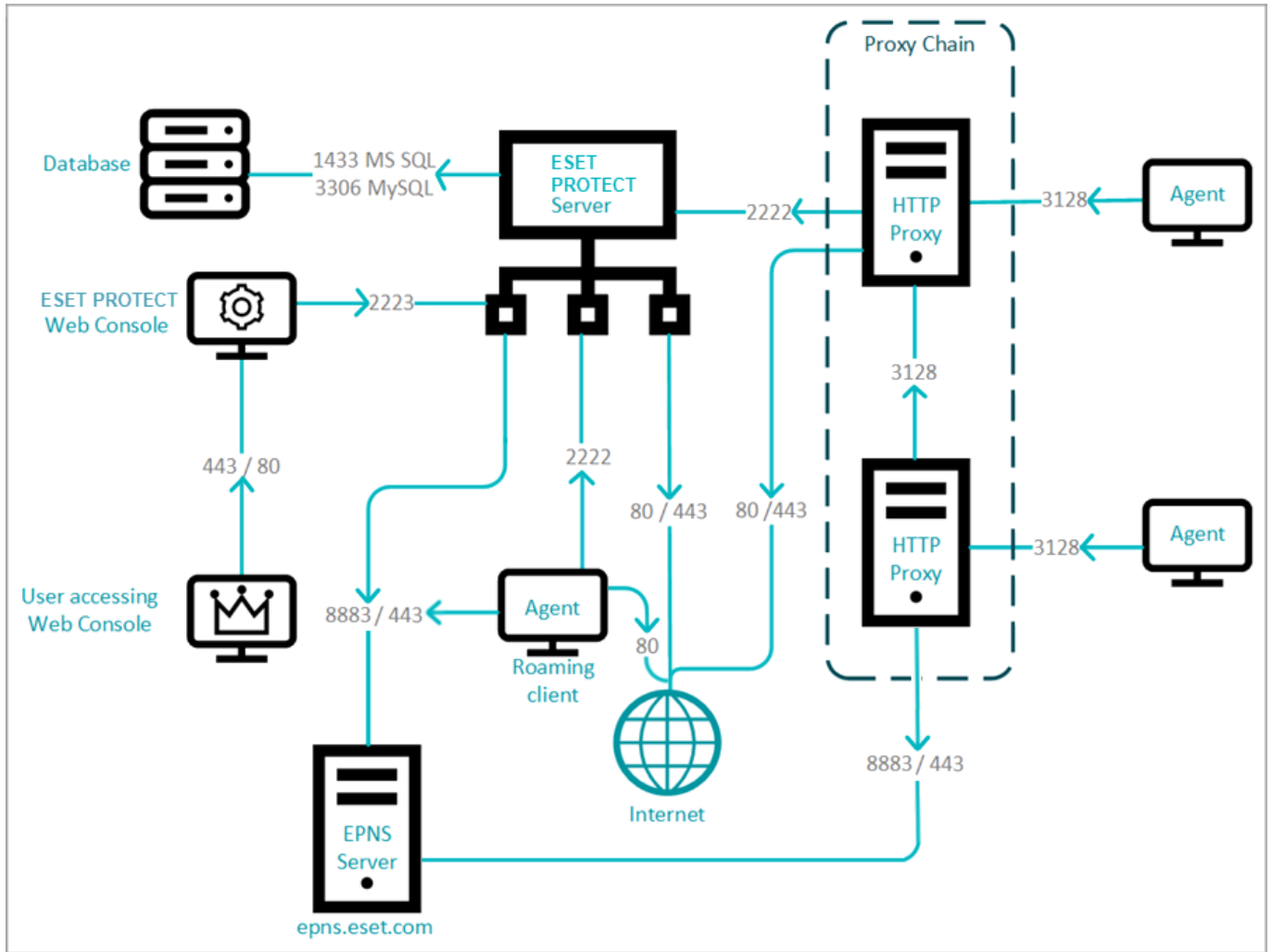
ESET Management 에이전트에서 생성된 전체 트래픽을 예상하려면 다음 공식을 사용하십시오.

클라이언트 수 \* (유휴 에이전트의 일일 트래픽 + (특정 작업의 트래픽 \* 작업의 일일 발생 수))

ESET Inspect을(를) 사용하는 경우 ESET Inspect Connector에서 매일 2~5MB의 트래픽을 생성합니다(이벤트 수에 따라 다름).

## 사용되는 포트

ESET PROTECT 서버는 데이터베이스, ESET PROTECT 웹 콘솔 및 HTTP 프록시와 동일한 컴퓨터에 설치할 수 있습니다. 아래 다이어그램에는 분리된 설치와 사용된 포트가 표시되어 있습니다(화살표는 네트워크 트래픽을 나타냄).



아래 테이블에는 ESET PROTECT 및 해당 구성 요소가 인프라에 설치된 경우 사용되는 가능한 모든 네트워크 통신 포트가 나열되어 있습니다. 다른 통신은 기본 운영 체제 프로세스를 통해 수행됩니다(예: 추가 통신은 기본 운영 체제 프로세스를 통해 수행됩니다(예: TCP/IP를 통한 NetBIOS)).

**!** ESET PROTECT이(가) 적절히 작동하려면 다른 애플리케이션에서 아래의 포트를 사용해서는 안 됩니다. 아래에 나열된 포트를 통한 통신을 허용하도록 네트워크 내의 모든 방화벽을 구성해야 합니다.

#### 클라이언트(ESET Management Agent) 또는 ESET Bridge HTTP 프록시 컴퓨터

프로토콜	포트	설명
TCP	2222	ESET Management 에이전트와 ESET PROTECT 서버 간 통신
TCP	80	ESET 저장소에 연결
MQTT	8883, 443	ESET Push Notification Service - ESET PROTECT 서버 및 ESET Management Agent 간의 Wake-Up Call인 443은 장애 조치(Failover) 포트입니다.
TCP	3128	ESET Bridge(HTTP 프록시)를 통한 통신
TCP	443	ESET LiveGuard Advanced(와) 통신(프록시만 해당)

ESET Management Agent - Windows OS를 포함한 대상 컴퓨터에 원격 배포 시 사용하는 포트:

프로토콜	포트	설명
TCP	139	공유 ADMIN\$ 사용
TCP	445	원격 설치 중에 TCP/IP를 사용하여 공유 리소스에 직접 접근(TCP 139의 대체 포트)
UDP	137	원격 설치 중 이름 해석
UDP	138	원격 설치 중 찾아보기

#### ESET PROTECT 웹 콘솔 컴퓨터(ESET PROTECT 서버 컴퓨터와 같지 않은 경우)

프로토콜	포트	설명
TCP	2223	ESET PROTECT 웹 콘솔과 ESET PROTECT 서버 간의 통신으로, 지원 설치에 사용됩니다.
TCP	443/80	웹 콘솔을 브로드캐스트하는 Tomcat.
TCP	443	지원뉴스를 위한 RSS 피드: • <a href="https://era.welivesecurity.com:443">https://era.welivesecurity.com:443</a> • <a href="https://support.eset.com:443/rss/news.xml">https://support.eset.com:443/rss/news.xml</a>

## ESET PROTECT 서버 컴퓨터

프로토콜	포트	설명
TCP	2222	ESET Management Agent와 ESET PROTECT 서버 간 통신
TCP	80	ESET 저장소에 연결
MQTT	8883	<a href="#">ESET Push Notification Service</a> - ESET PROTECT 서버 및 ESET Management Agent 간의 Wake-Up Call
TCP	2223	DNS 해결 및 MQTT 대체
TCP	3128	ESET Bridge(HTTP 프록시)을(를) 통한 통신
TCP	1433 (Microsoft SQL) 3306 (MySQL)	외부 데이터베이스에 대한 연결(데이터베이스가 다른 컴퓨터에 있는 경우에만).
TCP	389	LDAP 동기화. AD 컨트롤러에서도 이 포트를 엽니다.
UDP	88	<a href="#">Kerberos 티켓</a> (ESET PROTECT 가상 어플라이언스에만 적용)

## Rogue Detection(RD) Sensor

프로토콜	포트	설명
TCP	22, 139	SMB(TCP 139) 및 SSH(TCP 22) 프로토콜을 통한 운영 체제 탐지.
UDP	137	NetBIOS를 통한 컴퓨터 호스트 이름 해결

## ESET PROTECT MDC 컴퓨터

프로토콜	포트	설명
TCP	9977 9978	모바일 장치 커넥터와 ESET Management 에이전트 간의 내부 통신
TCP	9980	모바일 장치 등록
TCP	9981	모바일 장치 통신
TCP	2195	Apple Push Notification Service로 알림 보내기 ( <a href="#">gateway.push.apple.com</a> ) ESMC 버전 7.2.11.1까지
TCP	2196	Apple 피드백 서비스 ( <a href="#">feedback.push.apple.com</a> ) ESMC 버전 7.2.11.1까지
HTTPS	2197	• Apple 푸시 알림 및 피드백 ( <a href="#">api.push.apple.com</a> ) ESMC 버전 7.2.11.3 이상
TCP	2222	ESET Management Agent, MDC 및 ESET PROTECT 서버 간의 연결(복제)
TCP	1433 (Microsoft SQL) 3306 (MySQL)	외부 데이터베이스에 대한 연결(데이터베이스가 다른 컴퓨터에 있는 경우에만)

## MDM 관리되는 장치

프로토콜	포트	설명
TCP	9980	모바일 장치 등록
TCP	9981	모바일 장치 통신
TCP	5223	Apple Push Notification Service(iOS)와의 외부 통신
TCP	443	<ul style="list-style-type: none"> <li>Wi-Fi 전용에서의 대체(장치가 포트 5223에서 APNS에 연결할 수 없는 경우(iOS))</li> <li>GCM 서버와의 Android 장치 연결</li> <li>ESET 라이선스 포털에 대한 연결.</li> <li>ESET LiveGrid®(Android)(인바운드: <a href="https://l1.c.eset.com">https://l1.c.eset.com</a>, 아웃바운드: <a href="https://l3.c.eset.com">https://l3.c.eset.com</a>)</li> <li>ESET 연구소에 대한 익명 통계 정보(Android)(<a href="https://ts.eset.com">https://ts.eset.com</a>)</li> <li>장치에 앱 분류가 설치되었습니다. 일부 앱 분류 차단이 정의되었을 때 <a href="#">애플리케이션 제어</a>에 사용됩니다. (Android)(<a href="https://play.eset.com">https://play.eset.com</a>)</li> <li>지원 요청 기능을 사용하여 지원 요청을 보냄(Android)(<a href="https://suppreq.eset.eu">https://suppreq.eset.eu</a>)</li> </ul>
TCP	5228 5229 5230	Google Cloud Messaging으로 알림 전송(Android)* Firebase Cloud Messaging으로 알림 전송(Android)*
TCP	80	<ul style="list-style-type: none"> <li>모듈 업데이트(Android) (<a href="http://update.eset.com">http://update.eset.com</a>)</li> <li>웹 버전에서만 사용함. 최신 웹 버전 업데이트 및 새 버전 다운로드에 대한 정보. (Android)(<a href="http://go.eset.eu">http://go.eset.eu</a>)</li> </ul>

\* GCM(Google Cloud Messaging) 서비스는 더 이상 사용되지 않으며, 2019년 4월 11일부로 제거되었습니다. 이 서비스는 FCM(Firebase Cloud Messaging)으로 대체되었습니다. 위의 날짜까지 MDM v7에서는 GCM 서비스를 FCM 서비스로 대체했으며, 이 날짜부터 FCM 서비스에 대한 통신만 허용해야 합니다.

필요한 경우 미리 정의된 포트인 2222, 2223을 변경할 수 있습니다.

## 설치 프로세스



설치 설명서에는 ESET PROTECT 제품을 설치하는 여러 방법이 포함되어 있으며 일반적으로 엔터프라이즈 고객을 대상으로 합니다. 최대 250개의 Windows ESET 끝점 제품을 관리하기 위해 Windows 플랫폼에 ESET PROTECT를 설치하려는 경우 [중소기업용 설명서](#)를 참조하십시오.  
기존 ESET PROTECT 설치 업그레이드 지침을 보려면 [업그레이드 절차](#)를 참조하십시오.

ESET PROTECT 설치 관리자는 ESET 웹 사이트의 [ESET PROTECT 다운로드](#) 섹션에서 제공됩니다. 다양한 설치 방법을 지원하기 위해 여러 가지 형식으로 제공됩니다. 기본적으로 **통합형 설치 관리자** 탭이 선택됩니다. VA 또는 독립 실행형 설치 관리자를 다운로드하려면 적합한 탭을 클릭합니다. 사용할 수 있는 다운로드에는 다음과 같습니다.

- zip 형식의 Windows용 ESET PROTECT [통합형 설치 관리자](#) 패키지
- 모든 ESET PROTECT 설치 관리자를 포함하는 ISO 이미지(ESET PROTECT 가상 어플라이언스 제외)
- 가상 어플라이언스(OVA 파일). 가상화된 환경에서 ESET PROTECT를 실행하거나 보다 간편한 설치를 원하는 사용자에게는 ESET PROTECT 가상 어플라이언스 배포가 권장됩니다. 단계별 지침에 대해서는 전체 [ESET PROTECT 가상 어플라이언스 배포 설명서](#)를 참조하십시오.
- [Windows](#) 및 [Linux](#) 플랫폼용 각 구성 요소의 개별 설치 관리자

추가적인 설치 방법:

- 단계별 [Linux용 설치 지침](#)

**i** 2022년 11월부터 Azure Marketplace에서 ESET PROTECT 어플라이언스가 제공되지 않습니다. 그 대신에, [ESET PROTECT 클라우드](#)를 사용하여 모든 필수 인프라 구성 요소를 ESET에서 관리하도록 할 수 있습니다.

**!** 설치 후 ESET PROTECT 서버 컴퓨터의 컴퓨터 이름을 변경하지 마십시오. 자세한 내용은 [ESET PROTECT 서버의 IP 주소 또는 호스트 이름 변경](#)을 참조하십시오.

자신의 환경에 알맞은 ESET PROTECT 설치 방법을 알아보려면 다음 결정 표에서 가장 적절한 선택이 무엇인지 확인하십시오. 예를 들면 다음과 같습니다.

- 클라우드에서 ESET PROTECT에 속도가 느린 인터넷을 연결하지 마십시오.
- SMB 고객인 경우 통합형 설치 관리자를 선택하십시오.

[하드웨어 및 인프라 크기 조정](#)도 참조하십시오.

설치 방법	고객 유형		마이그레이션		ESET PROTECT 설치 환경					인터넷 연결		
	SMB	엔터프라이즈	예	아니요	서버 없음	전용 서버	공유 서버	가상화 플랫폼	클라우드 서버	없음	양호	나쁨
통합형 커집 Windows Server	✓	✓	✓			✓	✓		✓	✓	✓	✓
통합형 커집 Windows Desktop	✓		✓		✓					✓	✓	✓
가상 어플라이언스	✓		✓					✓		✓	✓	✓
구성 요소 Linux		✓	✓			✓	✓		✓	✓	✓	✓
구성 요소 Windows		✓	✓			✓	✓		✓	✓	✓	✓

## Windows에서의 통합형 설치

몇 가지 다른 방법으로 ESET PROTECT을(를) 설치할 수 있습니다. 사용자의 요구 사항과 환경에 가장 적합한 설치 유형을 선택합니다. 가장 간단한 방법은 ESET PROTECT 통합형 설치 관리자를 사용하는 것입니다. 이 방법을 사용하면 ESET PROTECT 및 해당 구성 요소를 단일 컴퓨터에 설치할 수 있습니다.

구성 요소 설치를 사용하면 시스템 요구 사항을 충족하는 경우 설치를 사용자 지정하고 별도의 컴퓨터에 각

ESET PROTECT 구성 요소를 설치할 수 있습니다.

다음은 사용하여 ESET PROTECT를 설치할 수 있습니다.

- [ESET PROTECT 서버](#), [ESET Bridge HTTP 프록시](#) 또는 [모바일 장치 커넥터](#)의 통합형 패키지 설치
- ESET PROTECT 구성 요소용 [독립 실행형 설치 관리자](#)(구성 요소 설치)

사용자 지정 설치 시나리오는 다음과 같습니다.

- [사용자 지정 인증서](#)를 사용한 설치
- [장애 조치\(Failover\) 클러스터](#)에서의 설치

많은 설치 시나리오에서는 여러 다른 네트워크 아키텍처를 수용하거나, 성능 요구를 충족하거나, 기타 이유로 인해 컴퓨터마다 다른 ESET PROTECT 구성 요소를 설치해야 합니다. 개별 ESET PROTECT 구성 요소에 대해 다음 설치 패키지를 사용할 수 있습니다.

핵심 구성 요소 설치:

- [ESET PROTECT 서버](#)
- [ESET PROTECT 웹 콘솔](#) - ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다.
- [ESET Management 에이전트](#)(클라이언트 컴퓨터에 설치되어야 하며, ESET PROTECT 서버에서의 설치 여부는 옵션임)

옵션 구성 요소 설치:

- [RD Sensor](#)
- [모바일 장치 커넥터](#)
- [ESET Bridge HTTP 프록시](#)
- [미러 도구](#)

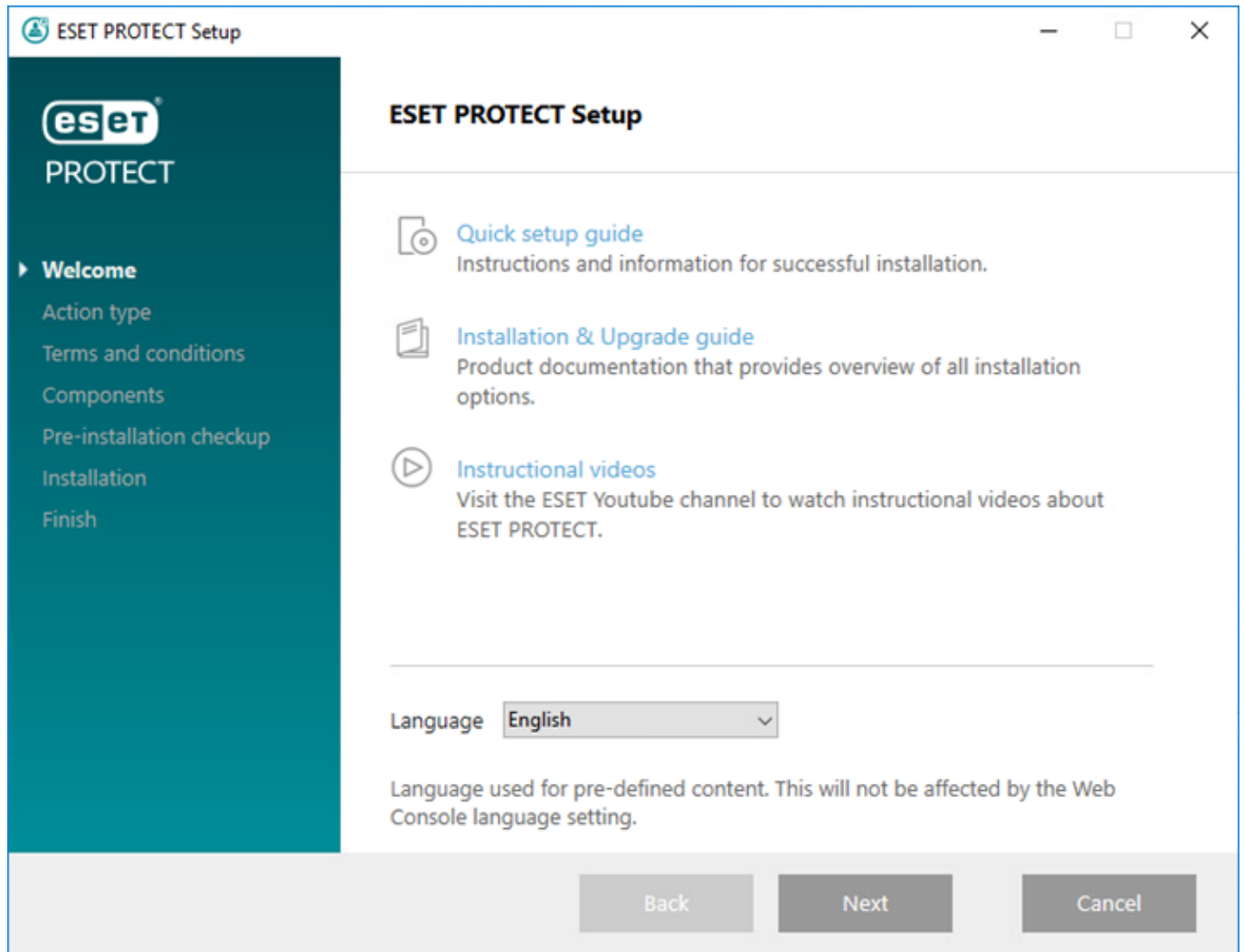
[ESET PROTECT 통합형 설치](#)도 참조하십시오.

ESMC를 최신 ESET PROTECT 10.0(으)로 업그레이드하는 지침을 보려면 [업그레이드 절차](#)를 참조하십시오.

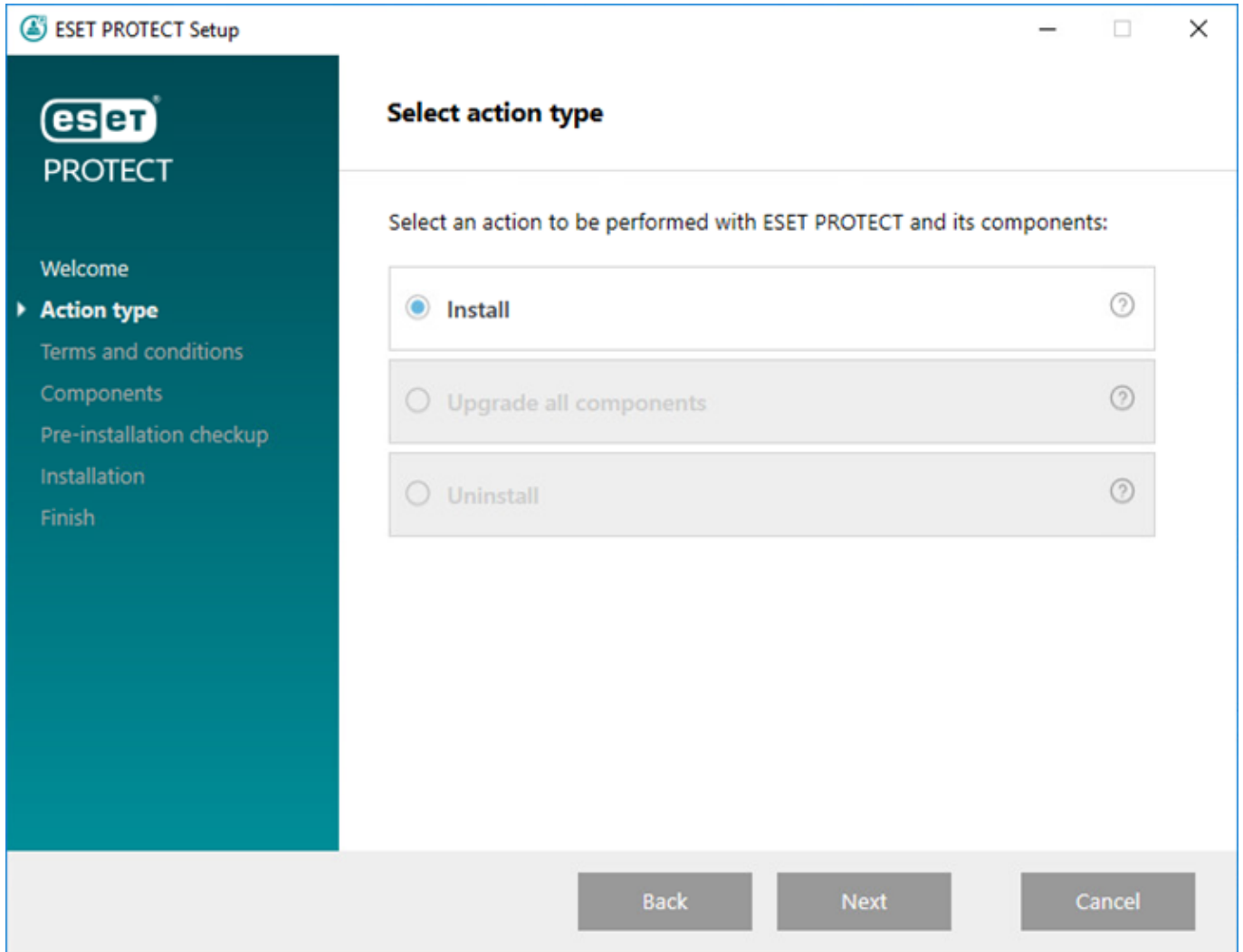
## ESET PROTECT 서버 설치

[ESET PROTECT 통합형 설치 관리자](#)는 Windows 운영 체제에만 사용할 수 있습니다. 통합형 설치 관리자로는 ESET PROTECT 설치 마법사를 사용하여 모든 ESET PROTECT 구성 요소를 설치할 수 있습니다.

1. 설치 패키지를 엽니다. 시작 화면에서 **언어** 드롭다운 메뉴를 사용하여 언어 설정을 지정합니다. 계속하려면 **다음**을 클릭합니다.



2. 설치를 선택하고 다음을 클릭합니다.




3. 제품 향상 프로그램에 참여 확인란을 선택하여 익명의 원격 측정 데이터 및 충돌 보고서(OS 버전 및 유형, ESET 제품 버전 및 기타 제품 특정 정보)를 ESET으로 보냅니다. EULA에 동의한 후에 다음을 클릭합니다.

4. 설치할 구성 요소를 선택하고 다음을 클릭합니다.

### [Microsoft SQL Server Express](#)

- ESET PROTECT 10.0 통합형 설치 관리자는 기본적으로 Microsoft SQL Server Express 2019를 설치합니다. 이전 Windows 버전(Server 2012 또는 SBS 2011)을 사용하는 경우 기본적으로 Microsoft SQL Server Express 2014가 설치됩니다.
- 설치 관리자는 데이터베이스 인증을 위해 임의의 패스워드를 자동으로 생성합니다(%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini에 저장됨).

-  Microsoft SQL Server Express는 각 관계형 DB의 크기가 10GB로 제한되어 있습니다. Microsoft SQL Server Express를 사용하지 않는 것이 좋습니다.
- 엔터프라이즈 환경 또는 대규모 네트워크에서.
  - ESET Inspect과(와) 함께 ESET PROTECT을(를) 사용하려는 경우

- 다른 지원되는 버전의 Microsoft SQL Server 또는 MySQL이 이미 설치되어 있거나 다른 SQL Server에 연결하려는 경우 **Microsoft SQL Server Express** 옆의 확인란을 선택 취소하십시오.
- 도메인 컨트롤러에 SQL Server를 설치하지 마십시오(예: Windows SBS/Essentials). ESET PROTECT 제품을 다른 서버에 설치하거나 설치 중에 SQL Server Express 구성 요소를 선택하지 않는 것이 좋습니다(이 경우 기존 SQL 또는 MySQL Server를 사용하여 ESET PROTECT DB를 실행해야 함).

### [웹 콘솔용 사용자 지정 HTTPS 인증서 추가](#)



- ESET PROTECT 웹 콘솔에 대한 사용자 지정 HTTPS 인증서를 사용하려면 이 옵션을 선택합니다.
- 이 옵션을 선택하지 않으면 설치 관리자가 새로운 Tomcat 키 저장소(자체 서명된 HTTPS 인증서)를 자동으로 생성합니다.

## ESET Bridge 프록시



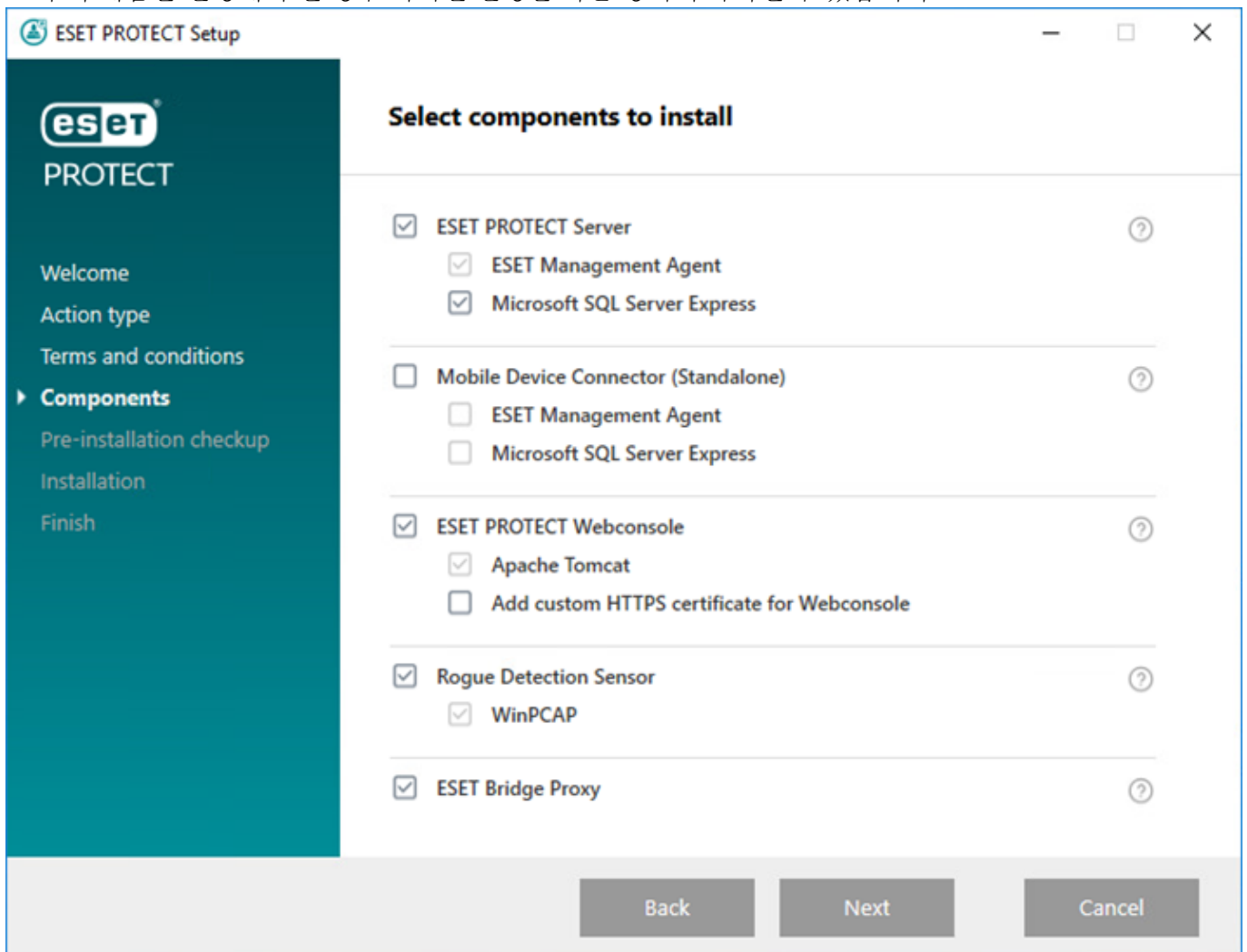
**ESET Bridge HTTP 프록시** 옵션은 로밍 클라이언트가 없는, 소규모 또는 중앙화된 네트워크에 사용하도록 설계되었습니다. 이 옵션을 선택하면 설치 관리자가 ESET PROTECT 서버와 동일한 컴퓨터에 설치된 프록시를 통해 ESET과의 통신을 터널링하도록 클라이언트를 구성합니다. 클라이언트와 ESET PROTECT 서버 간 직접적인 네트워크 포시가 없는 경우에는 이 연결이 설정되지 않습니다.

- HTTP 프록시를 사용하면 인터넷에서 다운로드되는 데이터에 대해 많은 양의 대역폭이 절감되며 제품 업데이트에 대한 다운로드 속도가 향상될 수 있습니다. ESET PROTECT에서 37개가 넘는 컴퓨터를 관리하려는 경우 **ESET Bridge 프록시** 옆에 있는 확인란을 선택하는 것이 좋습니다. [나중에 ESET Bridge를 설치](#)할 수도 있습니다.
- 자세한 내용은 [ESET Bridge\(HTTP 프록시\)](#) 및 [ESET Bridge\(HTTP 프록시\), 미리 도구 및 직접 연결 간의 차이](#)를 참조하십시오.



통합형 설치 관리자는 모든 정적 그룹에 적용되는, ESET Management Agent 및 ESET 보안 제품에 대한 기본 **HTTP Proxy 사용** 정책을 생성합니다. 이 정책은 업데이트 패키지 캐싱 프록시로 ESET Bridge을(를) 사용하도록 관리되는 컴퓨터에 ESET Management Agent 및 ESET 보안 제품을 자동으로 구성합니다.

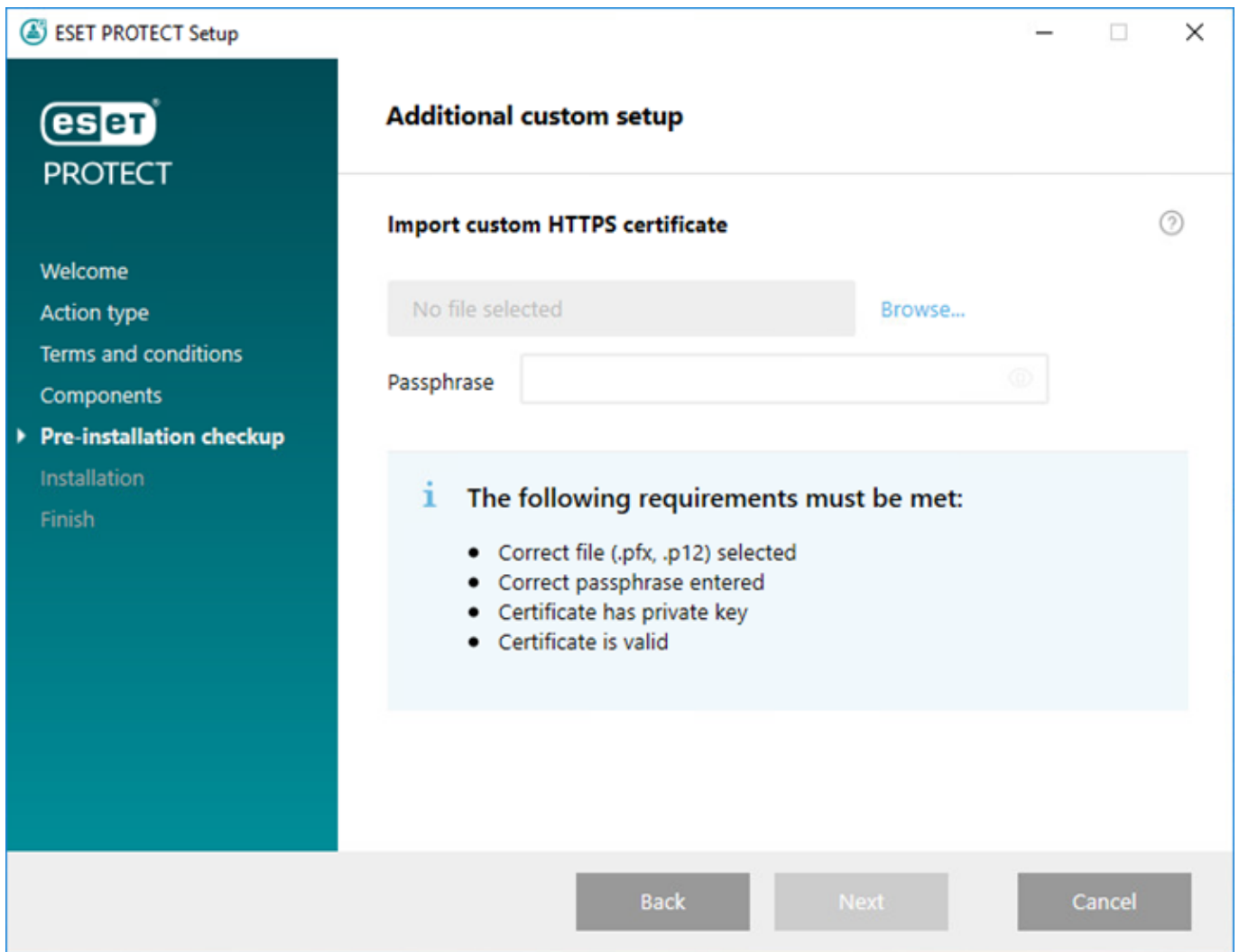
HTTP 프록시 호스트는 ESET PROTECT 서버의 로컬 IP 주소 및 포트 3128입니다. 인증이 비활성화됩니다. 추가 제품을 설정해야 할 경우 이러한 설정을 다른 정책에 복사할 수 있습니다.



5. 웹 콘솔용 사용자 지정 HTTPS 인증서 추가를 선택했으면 찾아보기를 클릭하고 올바른 인증서(.pfx 또는

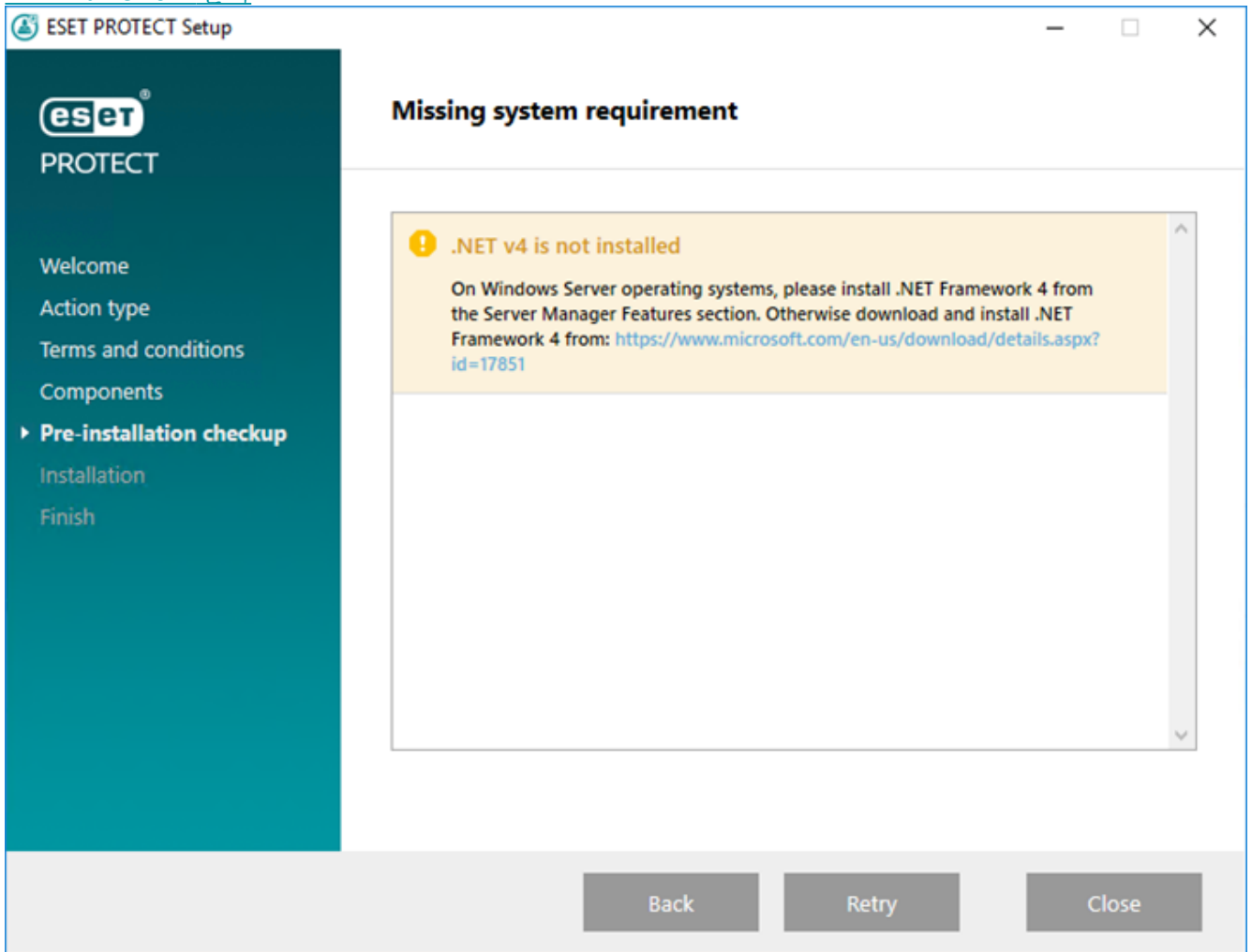


는 .p12 파일)를 선택한 후 해당하는 **비밀번호**를 입력합니다(또는 비밀번호가 없는 경우 필드를 공백으로 남김). 설치 관리자가 Tomcat 서버에 웹 콘솔 접근 인증서를 설치합니다. 계속하려면 **다음**을 클릭합니다.

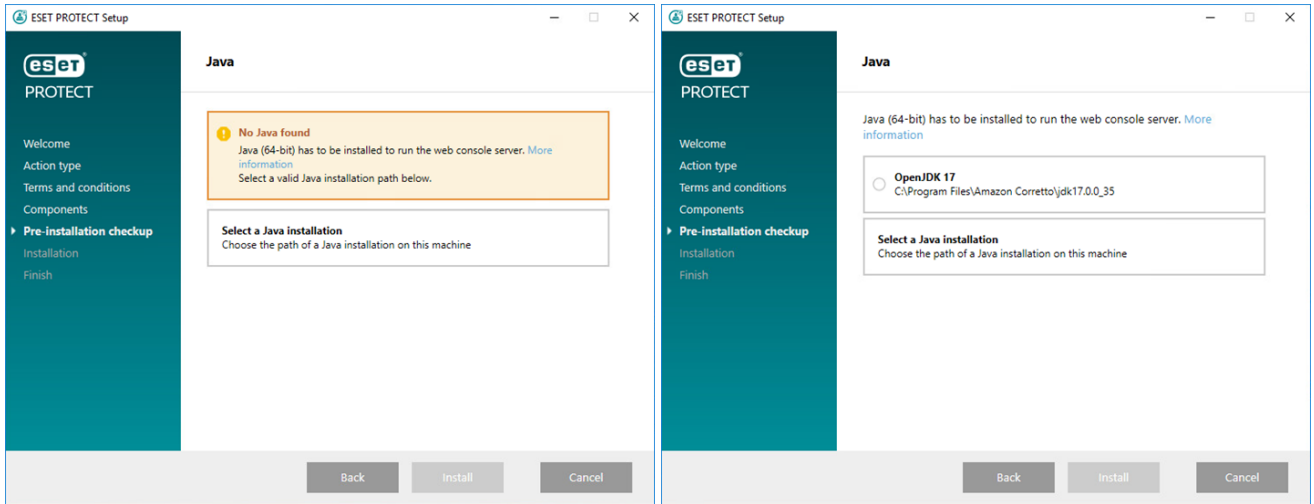


6. 필수 구성 요소 확인 중 오류가 발견되면 오류를 적절히 해결합니다. 시스템이 모든 [필수 구성 요소](#)를 충족하는지 확인합니다.

^ [.NET v4가 설치되어 있지 않습니다.](#)



Java를 찾을 수 없음/Java(64비트)가 검색됨



시스템에 여러 가지 Java 버전이 설치되어 있는 경우, 이전 Java 버전을 제거하고 [지원되는 Java](#) 최신 버전만 유지하는 것이 좋습니다.

**!** 2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.

- a) 이미 설치된 Java를 선택하려면 **Java 설치 선택**을 클릭하고 Java가 설치된 폴더(*bin* 하위 폴더가 있음, 예: *C:\Program Files\Amazon Corretto\jdk1.8.0\_212*)를 선택하고 **확인**을 클릭합니다. 잘못된 경로를 선택한 경우 설치 관리자에 메시지가 표시됩니다.
- b) 계속하려면 **설치**를 클릭하고 Java 설치 경로를 변경하려면 **변경**을 클릭합니다.

#### 사용 가능한 시스템 디스크 공간이 32MB만 남아 있습니다.

- 시스템에 ESET PROTECT을(를) 설치하기 위한 디스크 공간이 부족한 경우 이 알림이 표시될 수 있습니다.
- ESET PROTECT 및 해당하는 모든 구성 요소를 설치하려면 적어도 4,400MB의 사용 가능한 디스크 공간이 있어야 합니다.

#### ESET Remote Administrator 5.x 이전 버전이 컴퓨터에 설치되어 있습니다.

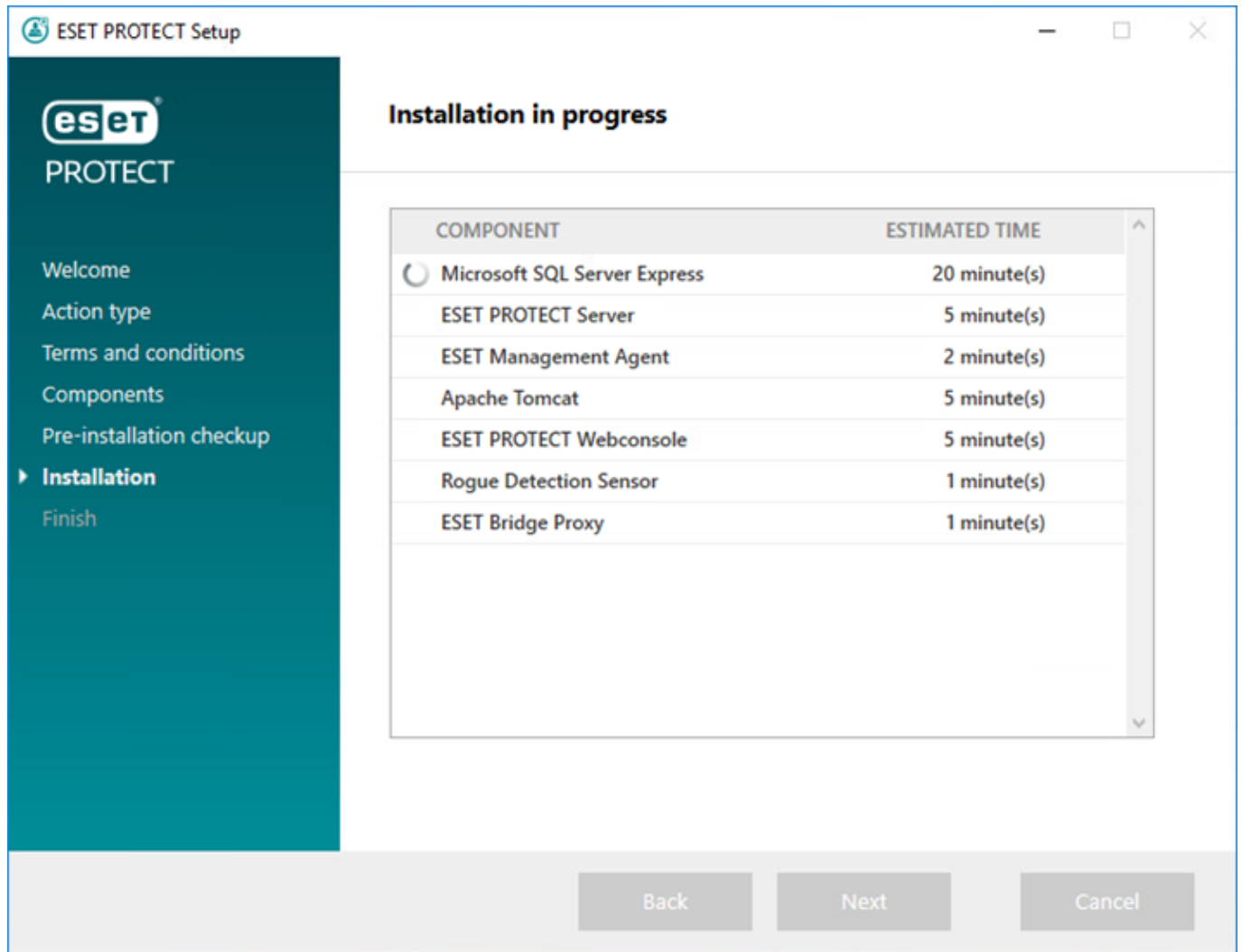
ERA 5.x/6.x 또는 ESMC 7.0/7.1이 있는 경우:

- ESET PROTECT 10.0(으)로 직접 업그레이드하는 것은 지원되지 않습니다.
- ESET PROTECT 10.0을(를) 새로 설치합니다.

ESMC 7.2에서 ESET PROTECT 10.0(으)로 직접 업그레이드할 수 있습니다.

7. 필수 구성 요소 확인을 마치고 사용자의 환경이 모든 [요구 사항](#)을 충족하면 설치가 시작됩니다. 시스템 및 네트워크 구성에 따라 설치 작업은 1시간 이상 소요될 수 있습니다.

**i** 설치가 진행 중이면 ESET PROTECT 설치 마법사가 응답하지 않습니다.



8. 4단계에서 **Microsoft SQL Server Express**를 설치하기로 선택한 경우 설치 관리자가 DB 연결을 확인합니다. 기존 DB 서버가 있는 경우 설치 관리자에서 DB 연결 상세 정보를 입력하라는 메시지를 표시합니다.

[SQL/MySQL Server에 대한 연결 구성](#)

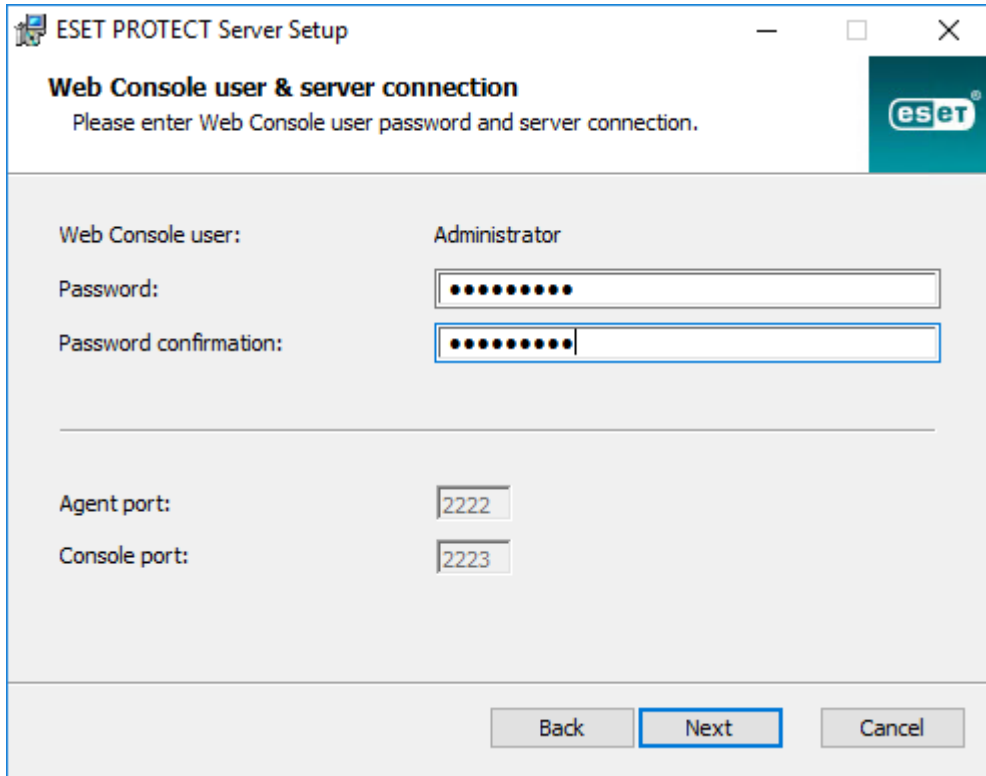
DB 이름, 호스트 이름, 포트 번호(Microsoft SQL Server 구성 관리자에서 이 정보를 찾을 수 있음) 및 DB 계정 상세 정보(사용자 이름 및 비밀번호)를 해당 필드에 입력하고 다음을 클릭합니다. 설치 관리자가 DB 연결을 확인합니다. DB 서버에 기존 DB(이전 ESMC/ESET PROTECT 설치)가 있는 경우 검색됩니다. 기존 DB를 사용하고 업그레이드 적용 또는 기존 DB를 제거하고 새 버전 설치 선택할 수 있습니다. 명령된 인스턴스 사용 - Microsoft SQL DB를 사용하는 경우 명령된 인스턴스 사용 확인란을 선택하여 사용자 지정 DB 인스턴스를 사용할 수 있습니다. 호스트 이름 필드에 HOSTNAME\DB\_INSTANCE 형식으로 설정할 수 있습니다(예: 192.168.0.10\ESMC75SQL). 클러스터된 DB의 경우 클러스터 이름만 사용합니다. 이 옵션을 선택하면 DB 연결 포트를 변경할 수 없으며, 시스템은 Microsoft에서 결정한 기본 포트를 사용하게 됩니다. ESET PROTECT 서버를 장애 조치(Failover) 클러스터에 설치된 Microsoft SQL DB와 연결하려면, 클러스터 이름을 호스트 이름 필드에 입력합니다.

DB 계정 정보 입력 시 두 가지 옵션이 있습니다. ESET PROTECT DB에만 접근할 수 있는 전용 DB 사용자 계정을 사용하거나 SA 계정(Microsoft SQL) 또는 루트 계정(MySQL)을 사용할 수 있습니다. 전용 사용자 계정을 사용하기로 결정한 경우 특정 권한을 갖는 계정을 만들어야 합니다. 자세한 내용은 전용 DB 사용자 계정을 참조하십시오. 전용 사용자 계정을 사용하지 않으려는 경우 관리자 계정(SA 또는 루트)을 입력합니다.

이전 창에서 SA 계정 또는 루트 계정을 입력한 경우 예를 클릭하여 SA/루트 계정을 ESET PROTECT의 DB 사용자로 계속 사용합니다.

아니요를 클릭하는 경우 새 사용자 생성(아직 사용자를 만들지 않은 경우) 또는 기존 사용자 사용(전용 DB 사용자 계정이 있는 경우)을 선택해야 합니다.

9. 설치 관리자에서 웹 콘솔 관리자 계정의 패스워드를 입력하라는 메시지를 표시합니다. 이 비밀번호는 [ESET PROTECT 웹 콘솔](#)에 로그인할 때 사용하므로 중요합니다. 다음을 클릭합니다.



**ESET PROTECT Server Setup**

**Web Console user & server connection**  
Please enter Web Console user password and server connection.

Web Console user: Administrator

Password: [Masked Password]

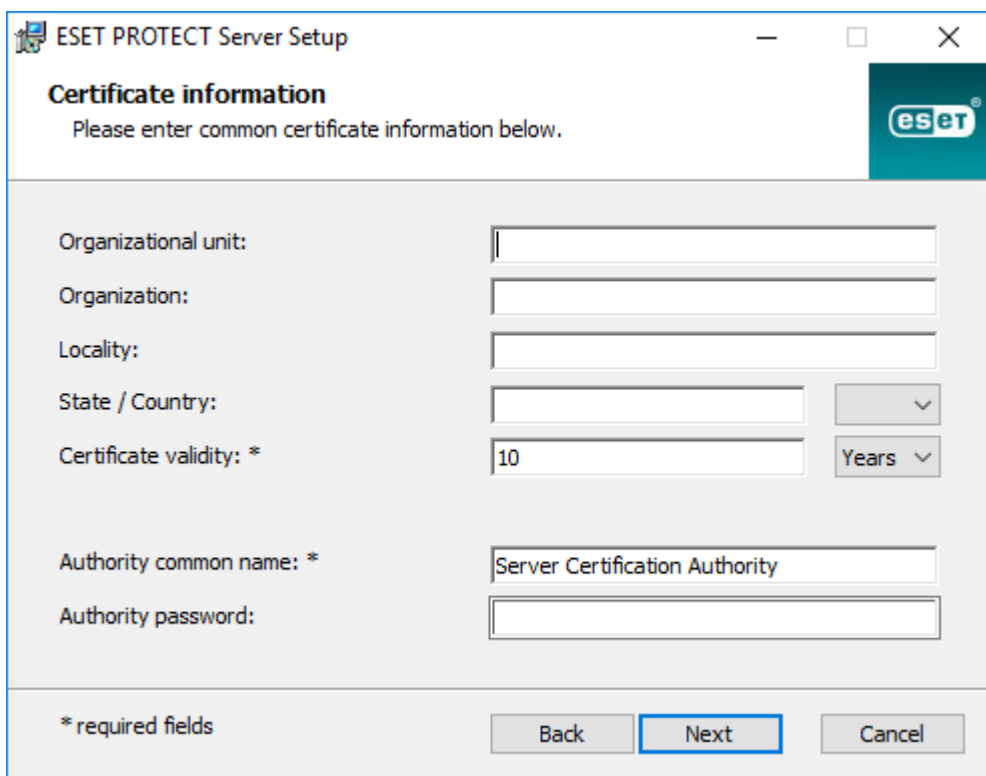
Password confirmation: [Masked Password]

Agent port: 2222

Console port: 2223

Back Next Cancel

10. 필드를 그대로 두거나 ESET Management Agent 및 ESET PROTECT 서버 인증서의 상세 정보에 표시할 회사 정보를 입력하십시오. **기관 패스워드** 필드에 패스워드를 입력하는 경우 이 패스워드를 기억해야 합니다. **다음**을 클릭합니다.



**ESET PROTECT Server Setup**

**Certificate information**  
Please enter common certificate information below.

Organizational unit: [Empty Field]

Organization: [Empty Field]

Locality: [Empty Field]

State / Country: [Empty Field] [Dropdown Arrow]

Certificate validity: \* 10 [Dropdown Arrow] Years [Dropdown Arrow]

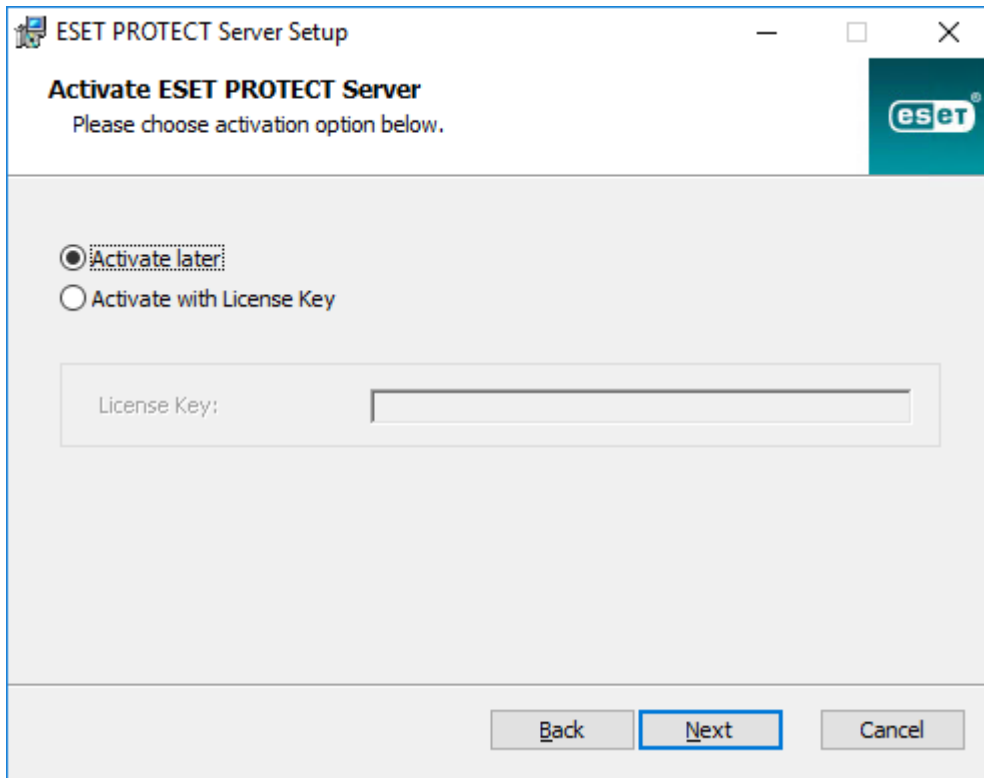
Authority common name: \* Server Certification Authority

Authority password: [Empty Field]

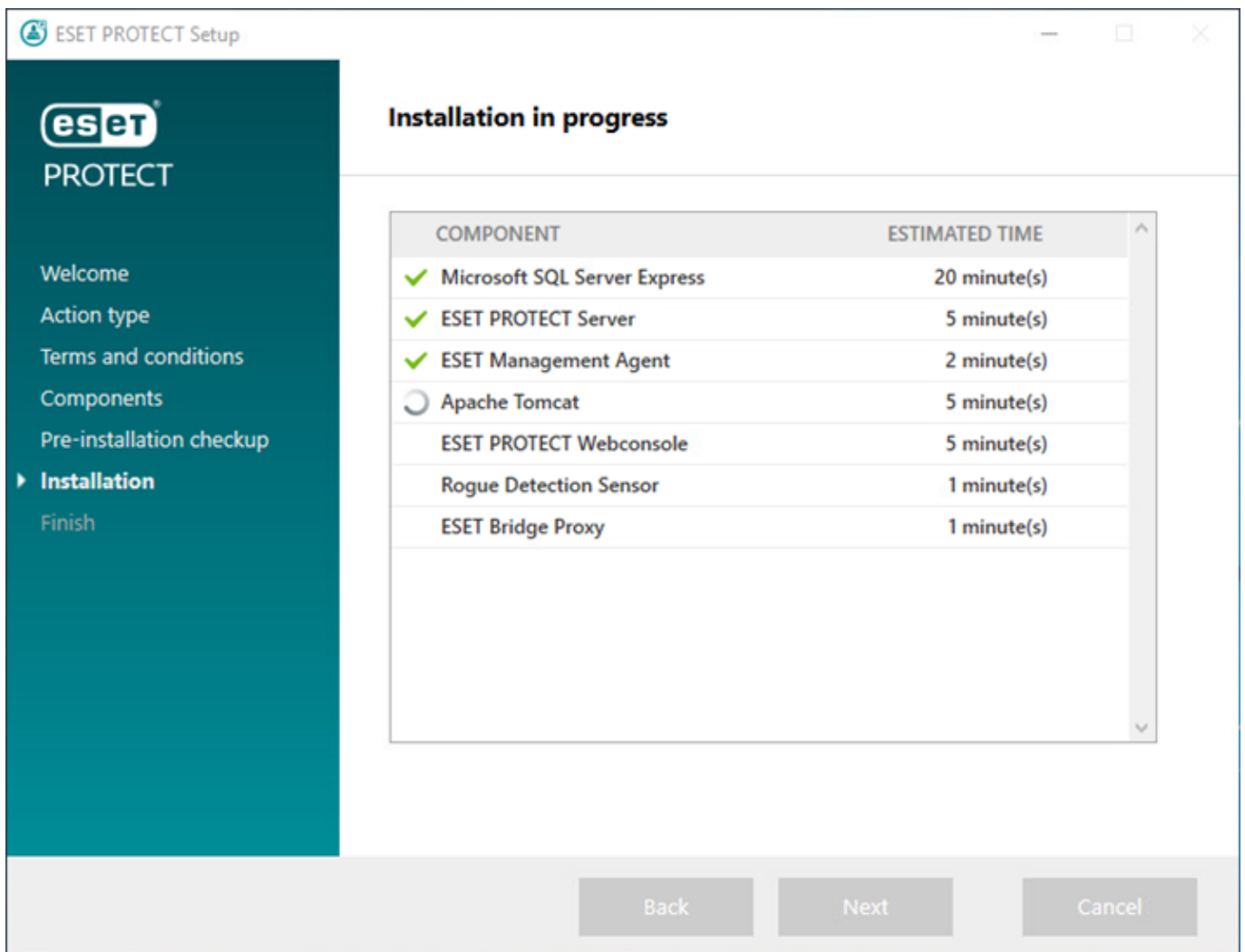
\* required fields

Back Next Cancel

11. 유효한 **라이선스 키**(제품 구입시 ESET에서 받은 이메일에 포함되어 있음)를 입력하고 **다음**을 클릭합니다. 레거시 라이선스 자격 증명(사용자 이름 및 비밀번호)을 사용하는 경우 이 자격 증명을 라이선스 키로 **변환**합니다. 또는 **나중에 활성화**하도록 선택할 수 있습니다(추가 지침은 [활성화](#) 장 참조).

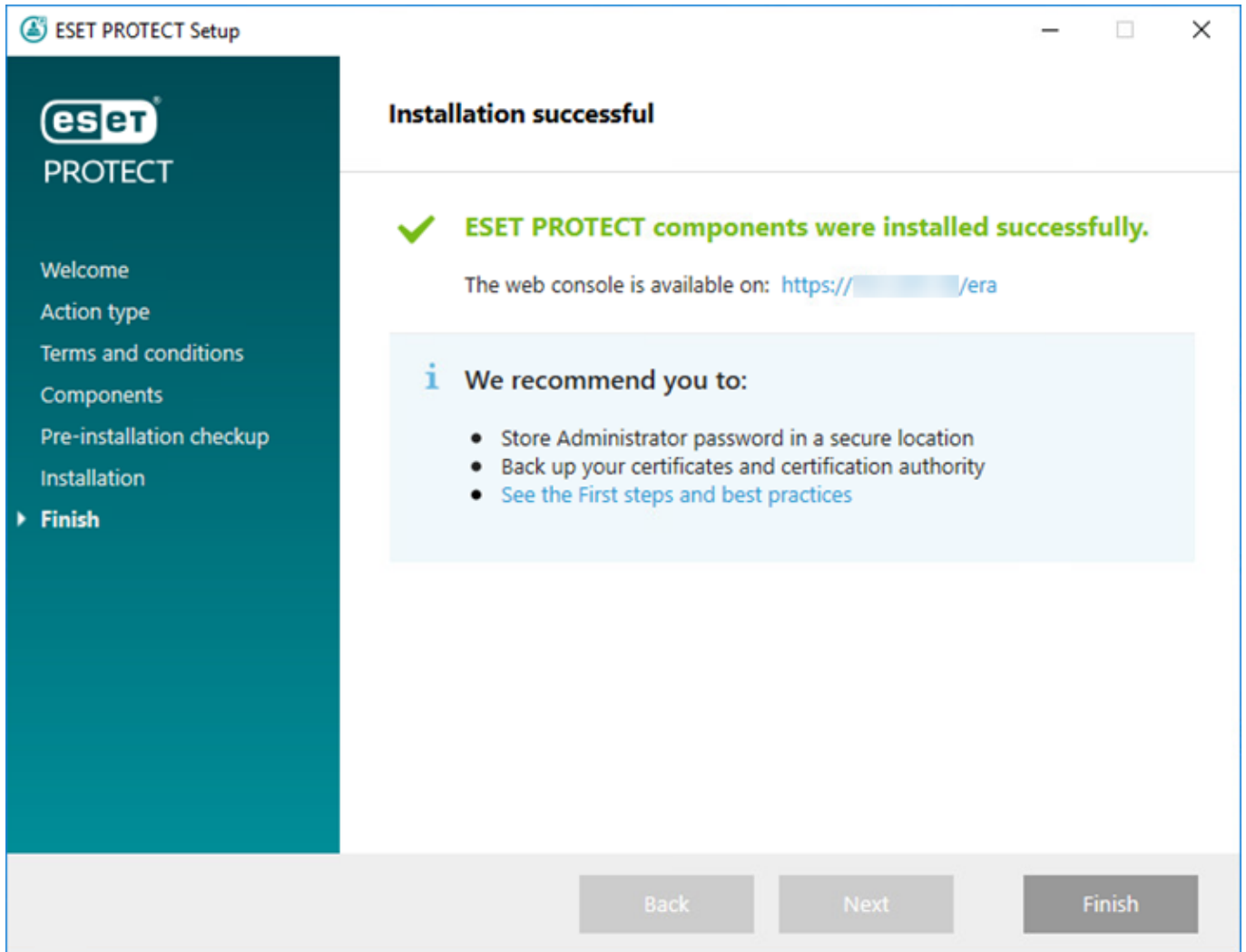


12. 설치 진행률이 표시됩니다.



13. **Rogue Detection Sensor**를 설치하도록 선택한 경우 WinPcap 드라이버에 대한 설치 창이 표시됩니다. 부팅 시 WinPcap 드라이버 자동 시작 확인란을 선택해야 합니다.

14. 설치가 완료되면 "ESET PROTECT 구성 요소 설치가 성공적으로 수행되었습니다."라는 메시지가 ESET PROTECT 웹 콘솔 URL 주소와 함께 표시됩니다. 라는 메시지가 ERA 웹 콘솔 URL 주소와 함께 표시됩니다. URL을 클릭하여 [웹 콘솔](#)을 열거나 [마침](#)을 클릭합니다.



설치가 실패한 경우:

- 통합형 설치 패키지의 설치 로그 파일을 검토합니다. 로그 디렉토리는 통합형 설치 관리자의 디렉토리입니다. 예를:  
C:\Users\Administrator\Downloads\x64\logs\
- 문제 해결을 위한 추가 단계에 대해서는 [문제 해결](#)을 참조하십시오.

## ESET PROTECT 모바일 장치 커넥터(독립형) 설치



ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

모바일 장치 커넥터를 ESET PROTECT 서버가 아닌 다른 컴퓨터에 독립 실행형 도구로 설치하려면 다음 단계를 완료하십시오.





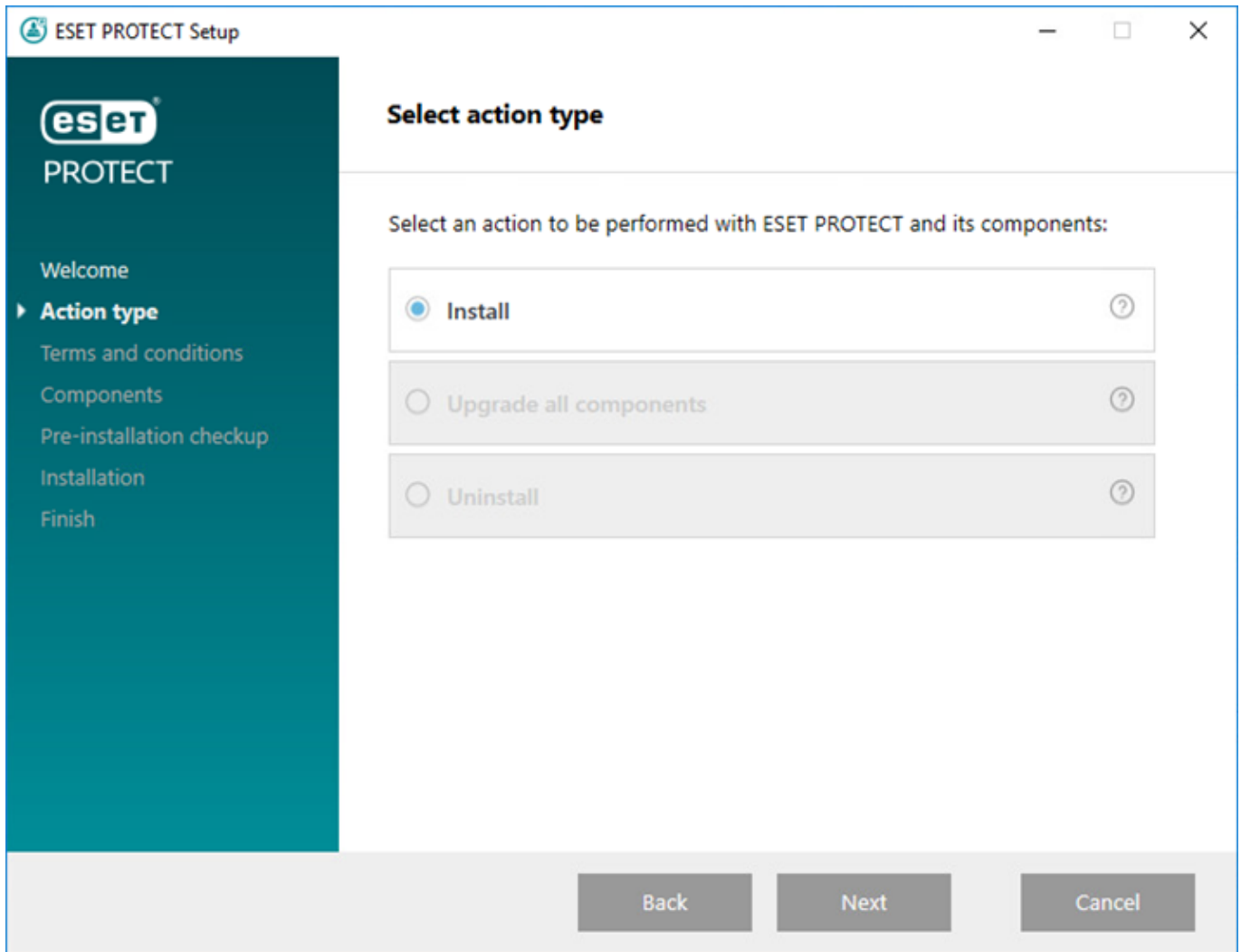
모바일 장치를 해당 위치와 관계없이 항상 관리할 수 있도록 인터넷에서 모바일 장치 커넥터에 접근할 수 있어야 합니다.



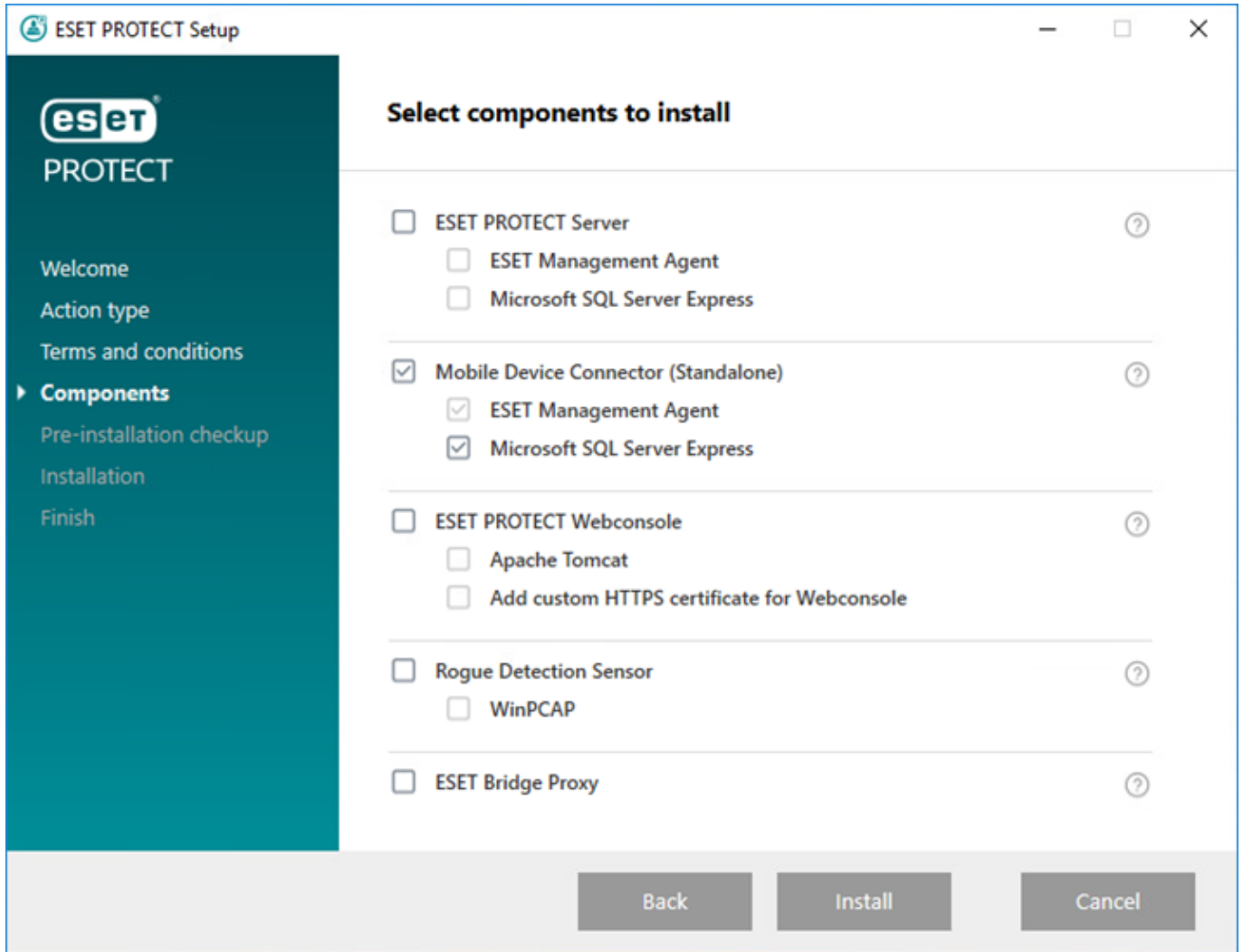
모바일 장치가 모바일 데이터의 사용에 영향을 줄 수 밖에 없는 모바일 장치 커넥터와 통신한다는 것을 고려하십시오. 로밍의 경우가 특히 여기에 해당합니다.

다음 단계에 따라 Windows에 모바일 장치 커넥터를 설치합니다.

1. 먼저 [필수 구성 요소](#)를 읽어 모든 사항이 충족되었는지 확인합니다.
2. 설치 패키지를 두 번 클릭하여 열고 **설치**를 선택한 후 **다음**을 클릭합니다.



3. **제품 향상 프로그램에 참여** 확인란을 선택하여 익명의 원격 측정 데이터 및 충돌 보고서(OS 버전 및 유형, ESET 제품 버전 및 기타 제품 특정 정보)를 ESET으로 보냅니다.
4. EULA에 동의한 후에 **다음**을 클릭합니다.
5. **Mobile Device Connector(독립 실행형)** 옆의 확인란만 선택합니다. ESET PROTECT 모바일 장치 커넥터의 작동을 위해 DB가 필요합니다. DB를 설치하려면 **Microsoft SQL Server Express**를 선택하고, 그렇지 않은 경우 이 확인란을 비워 둡니다. 기존 DB에 연결하려는 경우 설치 중에 이 작업을 위한 옵션을 사용합니다. **설치**를 클릭하여 설치를 계속 진행합니다.



6. 5단계에서 이 설치의 일부로 DB를 설치한 경우, 해당 DB가 자동으로 설치되므로 8단계로 건너뛸 수 있습니다. 5단계에서 DB를 설치하지 않도록 선택한 경우 이제 MDM 구성 요소를 기존 DB에 연결할지 묻는 메시지가 표시됩니다.

**i** ESET PROTECT DB에 사용하는 것과 동일한 DB 서버를 사용할 수도 있지만 80개보다 많은 모바일 장치를 등록하려는 경우에는 다른 DB 서버를 사용하는 것이 좋습니다.

7. 설치 관리자가 모바일 장치 커넥터에 사용될 기존 DB에 연결되어야 합니다. 다음 연결 세부 사항을 지정하십시오.

- **DB:** Windows 인증을 통한 MySQL Server/MS SQL Server/MS SQL Server
- **ODBC 드라이버:** MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 유니코드 드라이버/MySQL ODBC 5.3 유니코드 드라이버/MySQL ODBC 8.0 유니코드 드라이버/SQL Server/SQL Server Native Client 10.0/SQL Server용 ODBC Driver 11/SQL Server용 ODBC Driver 13/SQL Server용 ODBC Driver 17/SQL Server용 ODBC Driver 18
- **DB 이름:** 미리 정의된 이름을 사용하거나, 필요한 경우 이름을 변경하는 것이 좋습니다.
- **호스트 이름:** DB 서버의 호스트 이름 또는 IP 주소
- **포트:** DB 서버에 연결하는 데 사용됩니다.
- **DB 관리자 계정 사용자 이름/비밀번호**

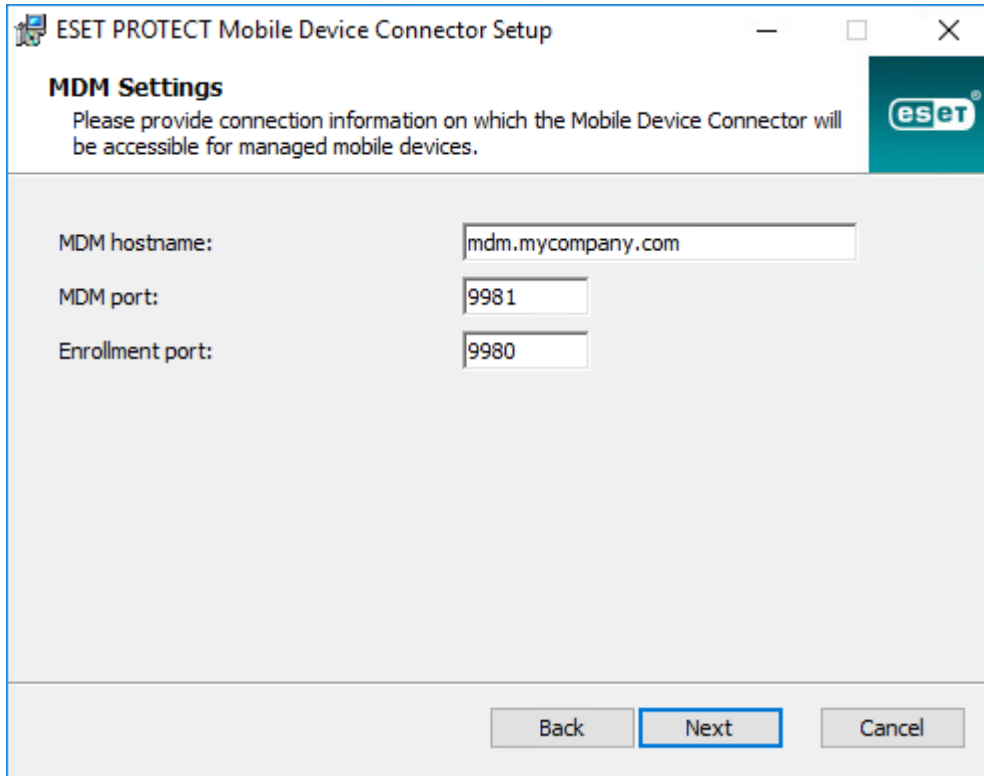
- **명명된 인스턴스 사용** - Microsoft SQL DB를 사용하는 경우 **명명된 인스턴스 사용** 확인란을 선택하여 사용자 지정 DB 인스턴스를 사용할 수 있습니다. **호스트 이름** 필드에 **HOSTNAME\DB\_INSTANCE** 형식으로 설정할 수 있습니다(예: **192.168.0.10\ESMC7SQL**). 클러스터된 DB의 경우 클러스터 이름만 사용합니다. 이 옵션을 선택하면 DB 연결 포트를 변경할 수 없으며, 시스템은 Microsoft에서 결정한 기본 포트를 사용하게 됩니다. ESET PROTECT 서버를 장애 조치(Failover) 클러스터에 설치된 Microsoft SQL DB와 연결하려면, 클러스터 이름을 **호스트 이름** 필드에 입력합니다.

8. 연결이 성공적으로 수행되면 제공된 사용자를 ESET PROTECT MDM에 대한 DB 사용자로 사용할지 묻는 메시지가 표시됩니다.

9. 새 DB가 성공적으로 설치되거나 설치 관리자가 기존 DB에 연결되면 MDM 설치를 계속 진행할 수 있습니다. **MDM 호스트 이름**을 지정합니다. 인터넷에서 모바일 장치가 연결할 수 있는 MDM 서버의 공용 도메인 또는 공용 IP 주소입니다.

MDM 호스트 이름은 **HTTPS 서버 인증서**에 표시되는 것과 같은 형식으로 입력해야 합니다. 그러지 않으면 iOS 모바일 장치가 **MDM 프로파일 설치**를 거부합니다. 예를 들어 HTTPS 인증서에 지정된 IP 주소가 있는 경우 **MDM 호스트 이름** 필드에 이 IP 주소를 입력합니다. HTTPS 인증서에 FQDN을 지정한 경우(예: **mdm.mycompany.com**) 이 FQDN을 **MDM 호스트 이름** 필드에 입력합니다. 또한 HTTPS 인증서에 와일드카드 \*를 사용한 경우(예: **\*.mycompany.com**) **MDM 호스트 이름** 필드에 **mdm.mycompany.com**을 사용할 수 있습니다.

**!** 이 설치 단계에서 **MDM 호스트 이름** 필드를 채울 때는 주의하십시오. 이 정보가 올바르지 않거나 형식이 잘못된 경우 MDM 커넥터가 제대로 작동하지 않으며, 구성 요소를 다시 설치해야만 이 문제를 해결할 수 있습니다.



10. 다음 단계에서는 **다음**을 클릭하여 DB에 대한 연결을 확인하십시오.

11. MDM 커넥터를 ESET PROTECT 서버에 연결합니다. ESET PROTECT 서버에 연결하는 데 필요한 **서버 호스트** 및 **서버 포트**를 채우고 **서버 지원 설치** 또는 **오프라인 설치**를 선택하여 계속 진행합니다.

- **서버 지원 설치** - ESET PROTECT 웹 콘솔 관리자 자격 증명을 제공하며, 설치 관리자가 자동으로 필요한 인증서를 다운로드합니다. 서버 지원 설치에 필요한 [권한](#)도 확인합니다.

1. **서버 호스트**(ESET PROTECT 서버의 이름 또는 IP 주소) 및 **웹 콘솔 포트**(사용자 지정 포트를 사용하지 않는 경우 기본 포트 2223을 그대로 둡)를 입력합니다. 또한 웹 콘솔 관리자 계정 자격 증명(**사용자 이름/비밀번호**)을 제공합니다.

2. 인증서를 수락할 것인지 물으면 **예**를 클릭합니다. 11단계를 계속합니다.

- **오프라인 설치** - ESET PROTECT에서 [내보낼 수 있는](#) 프록시 인증서 및 인증 기관을 제공합니다. 또는 [사용자 지정 인증서](#) 및 해당 인증 기관을 사용할 수도 있습니다.

1. 피어 인증서 옆에 있는 **찾아보기**를 클릭하고 **피어 인증서** 위치(ESET PROTECT에서 내보낸 프록시 인증서)로 이동합니다. 이 인증서에는 비밀번호가 필요하지 않으므로 **인증서 비밀번호** 텍스트 필드를 비웁니다.

2. 인증 기관에 대해 해당 절차를 반복하고 11단계를 계속 진행합니다.

**i** ESET PROTECT에서 ESET PROTECT 설치 중에 자동으로 생성된 기본 인증서 대신 사용자 지정 인증서를 사용하는 경우 이러한 인증서는 프록시 인증서를 제공하라는 메시지가 표시될 때 사용해야 합니다.

12. 모바일 장치 커넥터의 대상 폴더를 지정하고(기본값을 사용하는 것이 좋음) **다음 > 설치**를 클릭합니다.

MDM 설치가 완료된 후에 에이전트 설치를 수행할지 묻는 메시지가 표시됩니다. **다음**을 클릭하여 설치를 시작하고, EULA에 동의한 후 다음 단계를 따르십시오.

1. 서버 **호스트**(ESET PROTECT 서버의 호스트 이름 또는 IP 주소) 및 **서버 포트**(기본 포트는 2222임, 다른 포트를 사용하는 경우 기본 포트를 해당 사용자 지정 포트 번호로 바꿈)를 입력합니다.

**!** 서버 **호스트**가 서버 인증서의 **호스트** 필드에 정의된 하나 이상의 값(이상적으로는 FQDN)과 일치하는지 확인합니다. 일치하지 않을 경우 "받은 서버 인증서가 유효하지 않습니다." 오류가 발생합니다. 유일한 예외는 서버 인증서 호스트 필드에 와일드카드(\*)가 있는 경우입니다. 이 경우 모든 **서버 호스트**에서 작동한다는 것을 의미합니다.

2. 프록시를 사용하는 경우 **프록시 사용** 확인란을 선택합니다. 이 확인란을 선택하면 설치 관리자가 **오프라인** 설치를 계속합니다.

이 프록시 설정은 ESET Management 에이전트와 ESET PROTECT 서버 간의 (복제)에만 사용되며 업데이트 캐시에는 사용되지 않습니다.

- **프록시 호스트 이름**: HTTP 프록시 시스템의 호스트 이름 또는 IP 주소입니다.
  - **프록시 포트**: 기본값은 3182입니다.
  - **사용자 이름, 비밀번호**: 인증을 사용할 경우 프록시에 사용되는 자격 증명을 입력합니다.
- 나중에 [정책](#)에서 프록시 설정을 변경할 수 있습니다. [프록시](#)는 프록시를 통한 에이전트 - 서버 연결을 구성하려는 경우 먼저 설치해야 합니다.

3. 다음 설치 옵션 중 하나를 선택하고 아래 해당 섹션의 단계를 따르십시오.

**서버 지원 설치** - ESET PROTECT 웹 콘솔 관리자 자격 증명을 제공해야 합니다(설치 관리자가 자동으로 필요한 인증서를 다운로드함).

**오프라인 설치** - 에이전트 인증서 및 인증 기관(둘 다 ESET PROTECT에서 [내보낼](#) 수 있음)을 제공해야 합니다. 또는 [사용자 지정 인증서](#)를 사용할 수도 있습니다.

- **서버 지원 에이전트 설치를 계속하려면 다음 단계를 따르십시오.**

1. 서버 **호스트** 필드에 ESET PROTECT 웹 콘솔의 호스트 이름 또는 IP 주소(ESET PROTECT 서버와 동일)를 입력합니다. 사용자 지정 포트를 사용하지 않는 경우 **웹 콘솔 포트**를 기본 포트 2223으로 그대로 둡니다. 또는 **사용자 이름 및 비밀번호 필드**에 웹 콘솔 계정 자격 증명을 입력합니다. 도메인 사용자로 로그인하려면 **도메인에 로그인** 옆의 확인란을 선택합니다.

**!** 서버 **호스트**가 서버 인증서의 **호스트** 필드에 정의된 하나 이상의 값(이상적으로는 FQDN)과 일치하는지 확인합니다. 일치하지 않을 경우 "받은 서버 인증서가 유효하지 않습니다." 오류가 발생합니다. 유일한 예외는 서버 인증서 호스트 필드에 와일드카드(\*)가 있는 경우입니다. 이 경우 모든 **서버 호스트**에서 작동한다는 것을 의미합니다.

- 서버 지원 설치의 경우 사용자에게 [2단계 인증](#)을 사용할 수 없습니다.

2. 인증서를 수락할 것인지 묻는 메시지가 표시되면 **예**를 클릭합니다.

3. **컴퓨터를 생성하지 않음**(처음 연결할 때 컴퓨터가 자동으로 생성됨) 또는 **사용자 지정 정적 그룹** 선택을 선택합니다. **사용자 지정 정적 그룹** 선택을 클릭하는 경우 ESET PROTECT의 기존 정적 그룹 목록에서 선택할 수 있습니다. 선택한 그룹에 컴퓨터가 추가됩니다.

4. ESET Management 에이전트의 대상 폴더를 지정하고(기본 위치를 사용하는 것이 좋음) **다음**을 클릭한

후 설치를 클릭합니다.

• 오프라인 에이전트 설치를 계속하려면 다음 단계를 따르십시오.

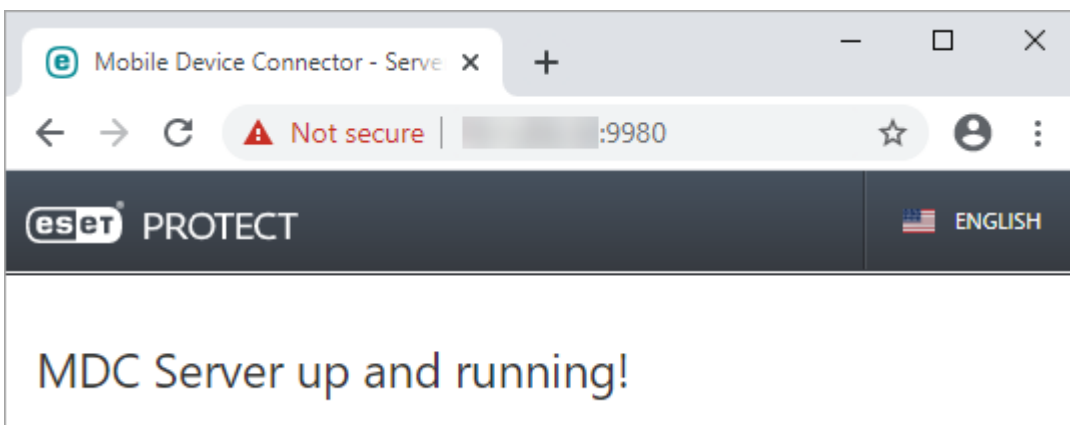
1. 이전 단계에서 **프록시 사용**을 선택한 경우 **프록시 호스트 이름**, **프록시 포트**(기본 포트는 3128), **사용자 이름** 및 **비밀번호**를 제공하고 **다음**을 클릭합니다.
2. **찾아보기**를 클릭하고 **피어 인증서**(ESET PROTECT에서 내보낸 에이전트 인증서임) 위치로 이동합니다. 이 인증서에는 비밀번호가 필요하지 않으므로 **인증서 비밀번호** 텍스트 필드를 비워둡니다. **인증 기관**을 찾을 필요가 없습니다. 이 필드를 비워둡니다.

**i** ESET PROTECT에서 ESET PROTECT 설치 중에 자동으로 생성된 기본 인증서 대신 사용자 지정 인증서를 사용하는 경우 적절하게 해당 사용자 지정 인증서를 사용합니다.

**!** 인증서 비밀번호에는 문자를 포함할 수 없습니다: " \ 이러한 문자를 사용하면 에이전트를 초기화하는 동안 심각한 오류가 발생합니다.

3. 기본 폴더에 설치하려면 **다음**을 클릭하고 다른 폴더를 선택하려면 **변경**을 클릭합니다(기본 위치를 사용하는 것이 좋음).

설치가 완료된 후 웹 브라우저 또는 모바일 장치에서 <https://your-mdm-hostname:enrollment-port>(예: <https://mdm.company.com:9980>)를 열어 모바일 장치 커넥터가 올바르게 실행되는지 확인합니다. 설치에 성공하면 다음과 같은 메시지가 표시됩니다.



이제 [ESET PROTECT에서 MDM을 활성화](#)할 수 있습니다.

## Windows의 구성 요소 설치

많은 설치 시나리오에서는 여러 다른 네트워크 아키텍처를 수용하거나, 성능 요구를 충족하거나, 기타 이유로 인해 컴퓨터마다 다른 ESET PROTECT 구성 요소를 설치해야 합니다. 개별 ESET PROTECT 구성 요소에 대해 다음 설치 패키지를 사용할 수 있습니다.

핵심 구성 요소 설치:

- [ESET PROTECT 서버](#)
- [ESET PROTECT 웹 콘솔](#) - ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다.
- [ESET Management 에이전트](#) (클라이언트 컴퓨터에 설치되어야 하며, ESET PROTECT 서버에서의 설치 여부는 옵션임)

옵션 구성 요소 설치:

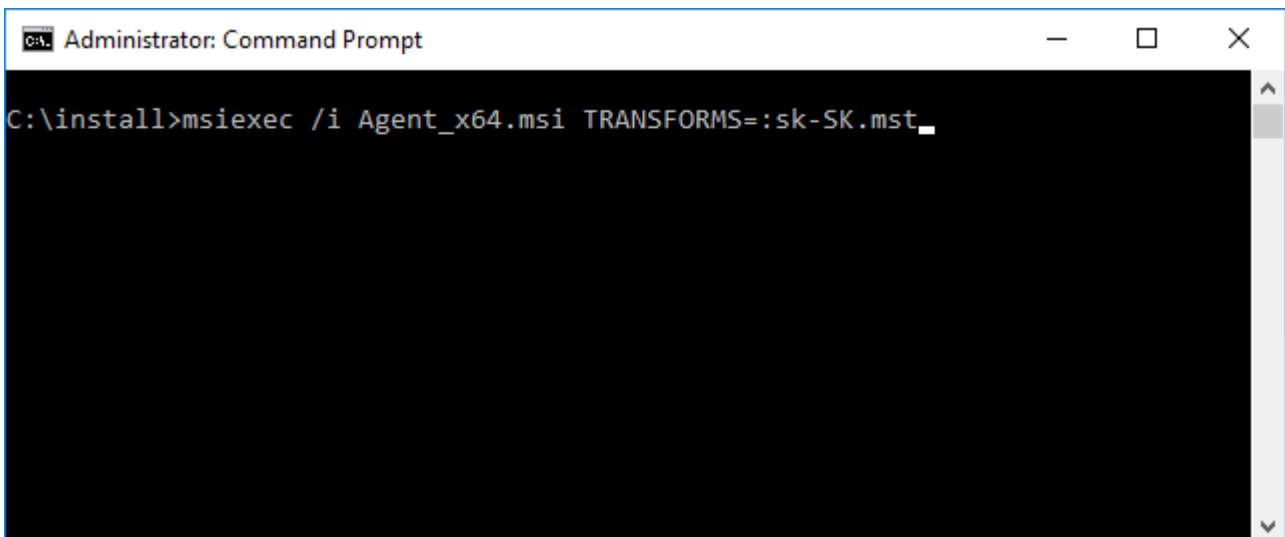
- [RD Sensor](#)
- [모바일 장치 커넥터](#)
- [ESET Bridge HTTP 프록시](#)
- [미러 도구](#)

[ESET PROTECT 통합형 설치](#)도 참조하십시오.

ESMC를 최신 ESET PROTECT 10.0(으)로 업그레이드하는 지침을 보려면 [업그레이드 절차](#)를 참조하십시오.

현지 언어로 설치를 실행하려면 명령줄을 통해 특정 ESET PROTECT 구성 요소의 MSI 설치 관리자를 시작해야 합니다.

다음은 슬로바키아 언어로 설치를 실행하는 방법에 대한 예입니다.



```
Administrator: Command Prompt
C:\install>msiexec /i Agent_x64.msi TRANSFORMS=:sk-SK.mst_
```

설치 관리자 실행 언어를 선택하려면 이 표에 따라 해당 TRANSFORMS 파라미터를 지정하십시오.

언어	코드
영어(미국)	en-US
아랍어(이집트)	ar-EG
중국어 간체	zh-CN
중국어 번체	zh-TW



언어	코드
크로아티아어(크로아티아)	hr-HR
체코어(체코 공화국)	cs-CZ
프랑스어(프랑스)	fr-FR
프랑스어(캐나다)	fr-CA
독일어(독일)	de-DE
그리스어(그리스)	el-GR
헝가리어(헝가리)*	hu-HU
인도네시아어(인도네시아)*	id-ID
이탈리아어(이탈리아)	it-IT
일본어(일본)	ja-JP
한국어(한국)	ko-KR
폴란드어(폴란드)	pl-PL
포르투갈어(브라질)	pt-BR
러시아어(러시아)	ru-RU
스페인어(칠레)	es-CL
스페인어(스페인)	es-ES
슬로바키아어(슬로바키아)	sk-SK
터키어(터키)	tr-TR
우크라이나어(우크라이나)	uk-UA

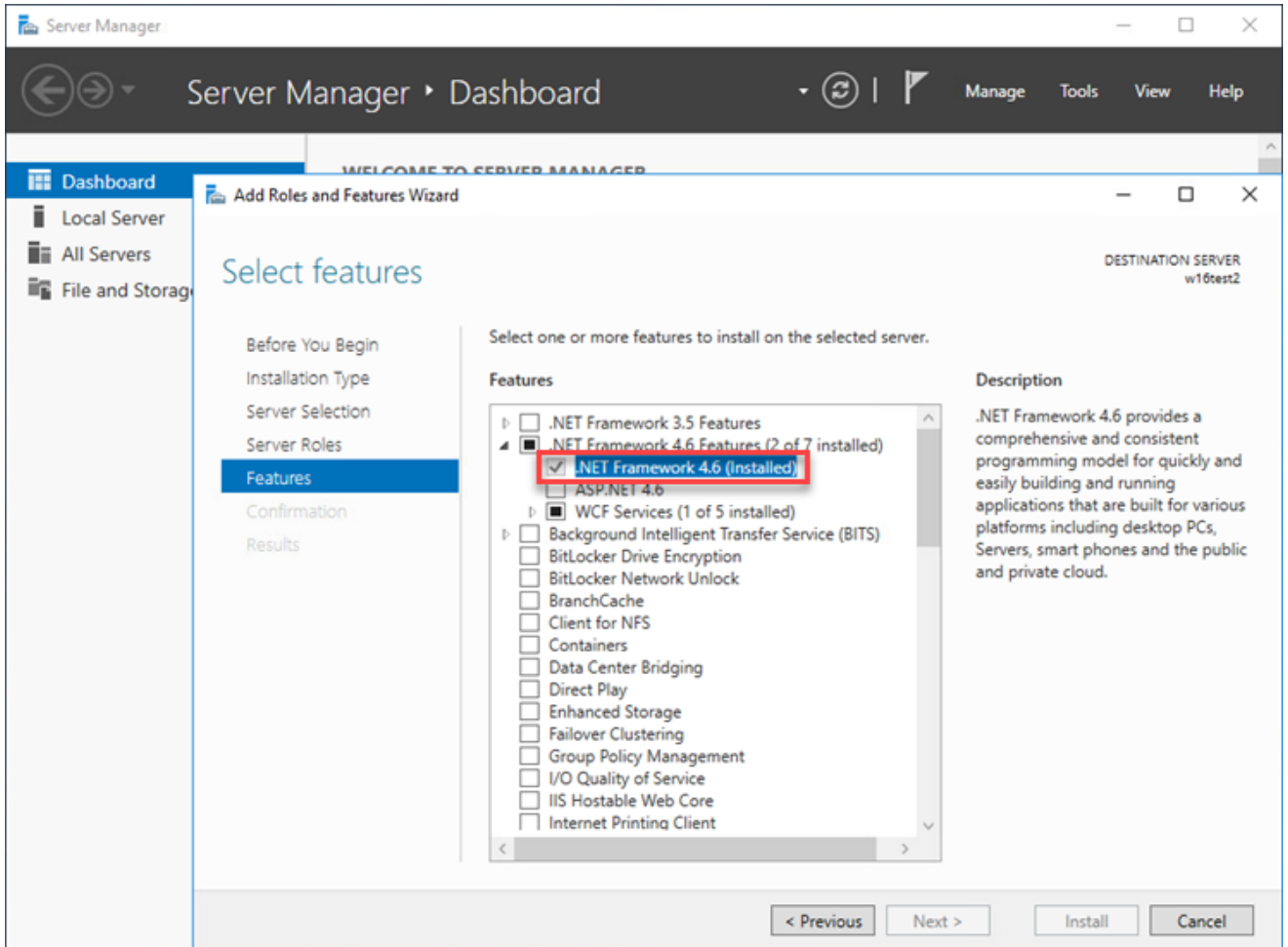
\* 제품만 이 언어로 제공되며 온라인 도움말은 제공되지 않습니다.

## 서버 설치 - Windows

### 필수 구성 요소

- 유효한 [라이선스 키](#)가 있어야 합니다.
- [지원되는 Windows 운영 체제](#)가 있어야 합니다.
- 필요한 포트가 열려 있고 사용 가능해야 함 - [전체 포트 목록은 여기](#)를 참조하십시오.
- [지원되는 DB 서버 및 커넥터](#)([Microsoft SQL Server](#) 또는 [MySQL](#))가 설치되어 있고 실행 중이어야 합니다. DB 서버 구성 상세 정보([Microsoft SQL Server](#) 또는 [MySQL](#))를 검토하여 ESET PROTECT에서 사용할 수 있도록 DB를 제대로 구성하는 것이 좋습니다. Microsoft SQL 또는 MySQL용 데이터베이스 및 데이터베이스 사용자를 설정하려면 [지식베이스 문서](#)를 읽어 보십시오.
- ESET PROTECT 서버를 관리하기 위해 [ESET PROTECT 웹 콘솔](#)이 설치되어 있어야 합니다.
- Microsoft SQL Server Express를 설치하려면 Microsoft .NET Framework 4가 필요합니다. **역할 및 기능 추가 마법사**를 사용하여 설치할 수 있습니다.





## 설치

Windows에 ESET PROTECT 서버 구성 요소를 설치하려면 다음 단계를 따릅니다.

! 위에 나열된 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

1. ESET PROTECT [다운로드 섹션](#)으로 이동하여 이 ESET PROTECT 구성 요소용 독립 실행형 설치 관리자를 다운로드합니다. (*server\_x64.msi*).
2. ESET PROTECT 서버 설치 관리자를 실행하고 EULA에 동의하는 경우 동의합니다.
3. **제품 향상 프로그램에 참여** 확인란을 선택하여 익명의 원격 측정 데이터 및 충돌 보고서(OS 버전 및 유형, ESET 제품 버전 및 기타 제품 특정 정보)를 ESET으로 보냅니다.
4. **클러스터 설치임** 옆의 확인란을 선택하지 않은 상태로 그대로 두고 **다음**을 클릭합니다. [클러스터 설치입니까?](#)

! 장애 조치(Failover) 클러스터에 ESET PROTECT 서버를 설치하는 경우 **클러스터 설치임** 옆의 확인란을 선택합니다. 클러스터의 공유 저장소를 가리키도록 **사용자 지정 애플리케이션 데이터 경로**를 지정합니다. 데이터는 클러스터 내의 모든 노드가 접근할 수 있는 한 위치에 저장해야 합니다.

5. **서비스 사용자 계정**을 선택합니다. 이 계정은 ESET PROTECT 서버 서비스를 실행하는 데 사용됩니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **네트워크 서비스 계정** - 도메인을 사용하지 않는 경우 이 옵션을 선택합니다.
- **사용자 지정 계정**: 도메인 사용자 자격 증명 제공: DOMAIN\USERNAME 및 패스워드.

6. DB에 연결합니다. 모든 데이터가 여기에 저장됩니다(ESET PROTECT 웹 콘솔 비밀번호, 클라이언트 컴퓨터 로그 등).

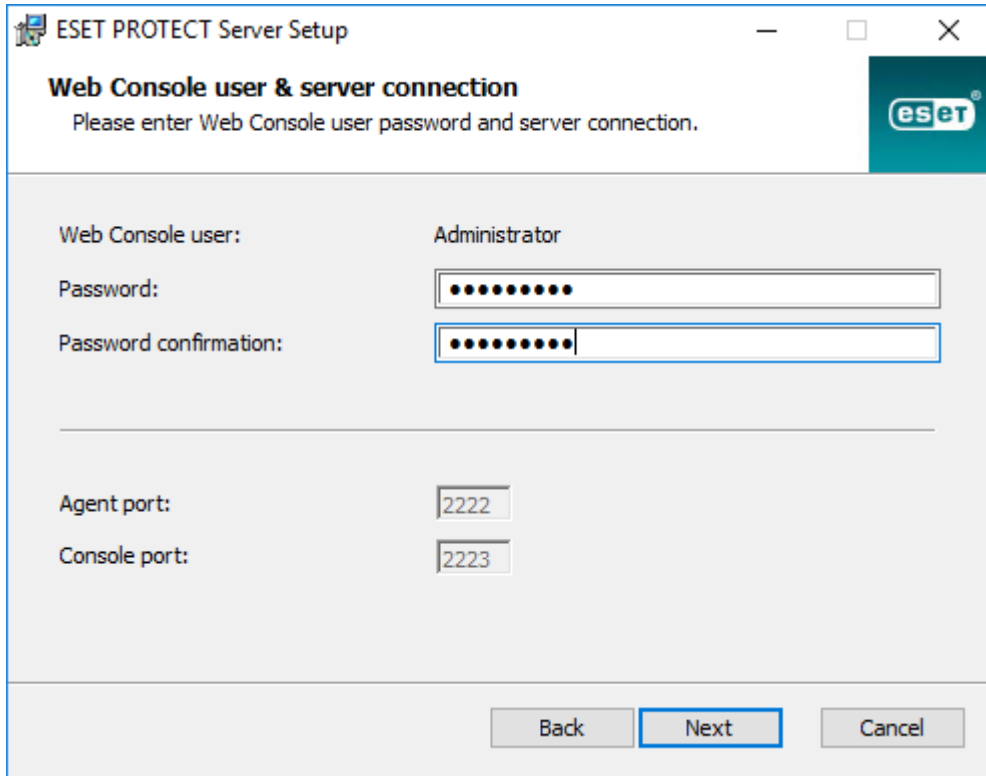
- **DB**: Windows 인증을 통한 MySQL Server/MS SQL Server/MS SQL Server
- **ODBC 드라이버**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 유니코드 드라이버/MySQL ODBC 5.3 유니코드 드라이버/MySQL ODBC 8.0 유니코드 드라이버/SQL Server/SQL Server Native Client 10.0/SQL Server-용 ODBC Driver 11/SQL Server-용 ODBC Driver 13/SQL Server-용 ODBC Driver 17/SQL Server-용 ODBC Driver 18
- **DB 이름**: 미리 정의된 이름을 사용하거나, 필요한 경우 이름을 변경하는 것이 좋습니다.
- **호스트 이름**: DB 서버의 호스트 이름 또는 IP 주소
- **포트**: DB 서버에 연결하는 데 사용됩니다.
- **DB 관리자 계정 사용자 이름/비밀번호**
- **명명된 인스턴스 사용** - Microsoft SQL DB를 사용하는 경우 **명명된 인스턴스 사용** 확인란을 선택하여 사용자 지정 DB 인스턴스를 사용할 수 있습니다. **호스트 이름** 필드에 **HOSTNAME\DB\_INSTANCE** 형식으로 설정할 수 있습니다(예: **192.168.0.10\ESMC7SQL**). 클러스터된 DB의 경우 클러스터 이름만 사용합니다. 이 옵션을 선택하면 DB 연결 포트를 변경할 수 없으며, 시스템은 Microsoft에서 결정한 기본 포트를 사용하게 됩니다. ESET PROTECT 서버를 장애 조치(Failover) 클러스터에 설치된 Microsoft SQL DB와 연결하려면, 클러스터 이름을 **호스트 이름** 필드에 입력합니다.

**i** ESET PROTECT 서버는 DB에 큰 데이터 Blob을 저장하므로 ESET PROTECT이(가) 제대로 실행되려면 [큰 패킷을 수용하도록 MySQL을 구성](#)해야 합니다.

이 단계는 DB에 대한 연결을 확인합니다. 연결 상태가 양호하면 다음 단계를 계속 진행합니다.

7. DB에 대한 접근 권한이 있는 ESET PROTECT의 사용자를 선택합니다. 기존 사용자를 사용할 수도 있고 설치 프로그램이 자동으로 사용자를 만들 수도 있습니다.

8. 웹 콘솔 접근을 위한 비밀번호를 입력합니다.



**ESET PROTECT Server Setup**

**Web Console user & server connection**  
Please enter Web Console user password and server connection.

Web Console user: Administrator

Password:

Password confirmation:

---

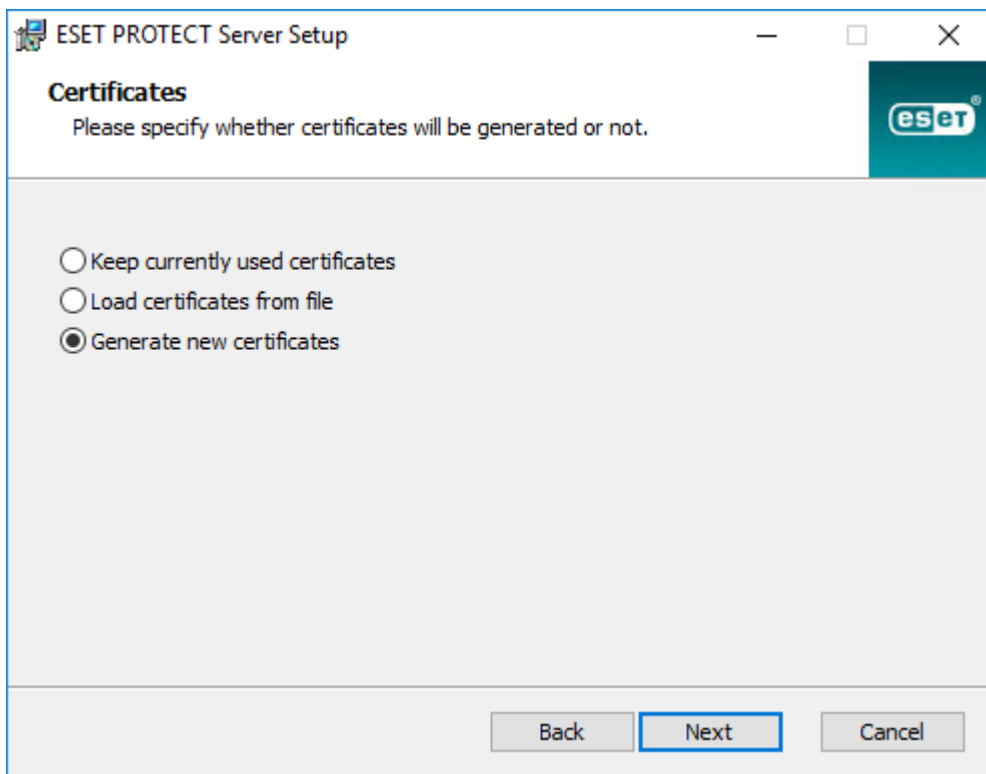
Agent port:

Console port:

Back Next Cancel

9. ESET PROTECT에서는 클라이언트-서버 통신을 위해 인증서를 사용합니다. 다음과 같은 옵션 중 하나를 선택합니다.

- **현재 사용된 인증서 유지** - 이 옵션은 DB가 이전에 이미 다른 ESET PROTECT Server와 함께 사용된 경우에만 사용할 수 있습니다.
- **파일에서 인증서 로드** - 기존 서버 인증서 및 인증 권한을 선택합니다.
- **새 인증서 생성** - 설치 관리자가 새 인증서를 생성합니다.



**ESET PROTECT Server Setup**

**Certificates**  
Please specify whether certificates will be generated or not.

☐ Keep currently used certificates

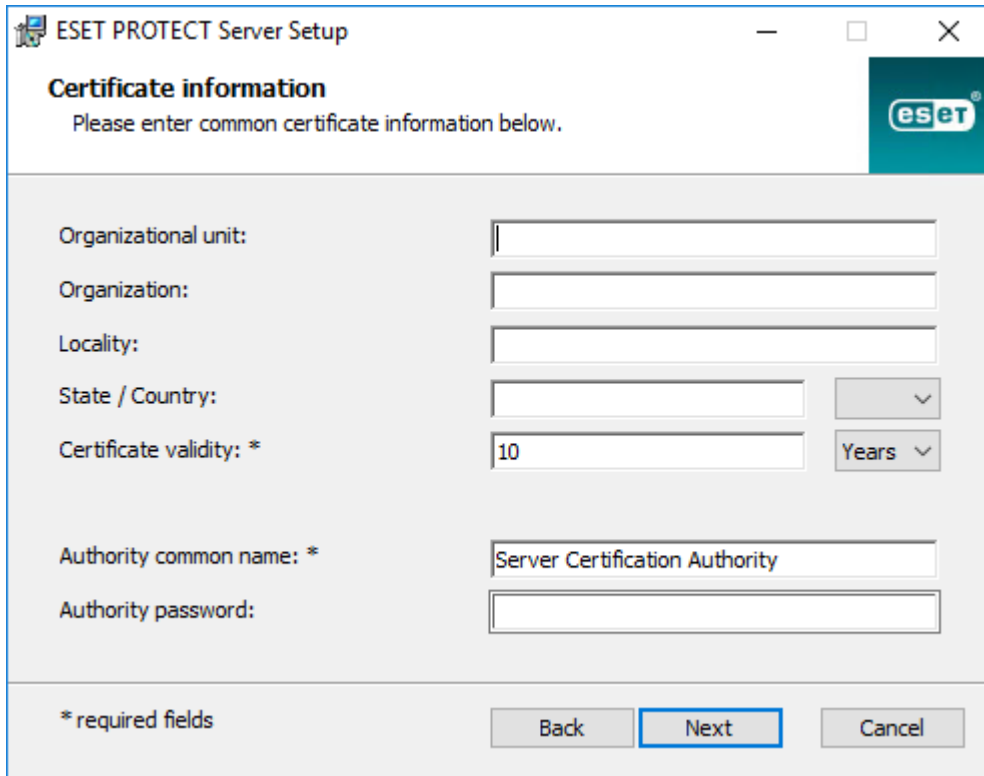
☐ Load certificates from file

☒ Generate new certificates

Back Next Cancel

10. 이전 단계에서 **새 인증서 생성** 옵션을 선택한 경우 다음 단계를 따르십시오.

a)인증서에 대한 추가 정보를 지정합니다(옵션). **기관 패스워드**를 입력하는 경우 패스워드를 꼭 기억해 두십시오.



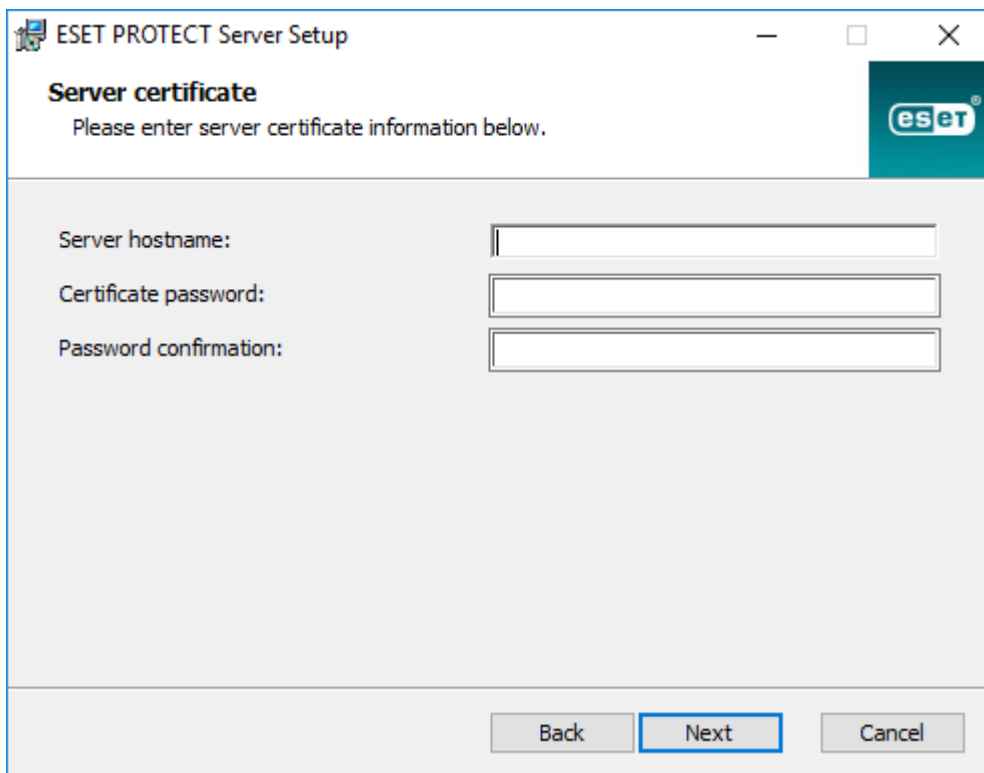
The dialog box is titled "ESET PROTECT Server Setup" and "Certificate information". It contains the following fields:

- Organizational unit: [Text box]
- Organization: [Text box]
- Locality: [Text box]
- State / Country: [Text box] [Dropdown arrow]
- Certificate validity: \* [Text box with "10"] [Dropdown arrow with "Years"]
- Authority common name: \* [Text box with "Server Certification Authority"]
- Authority password: [Text box]

At the bottom, there is a note "\* required fields" and three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

b)서버 인증서 필드에 서버 호스트 이름 및 인증서 패스워드(옵션)를 입력합니다.

**⚠ 서버 인증서의 서버 호스트 이름에는 키워드 server, proxy, agent를 사용할 수 없습니다.**

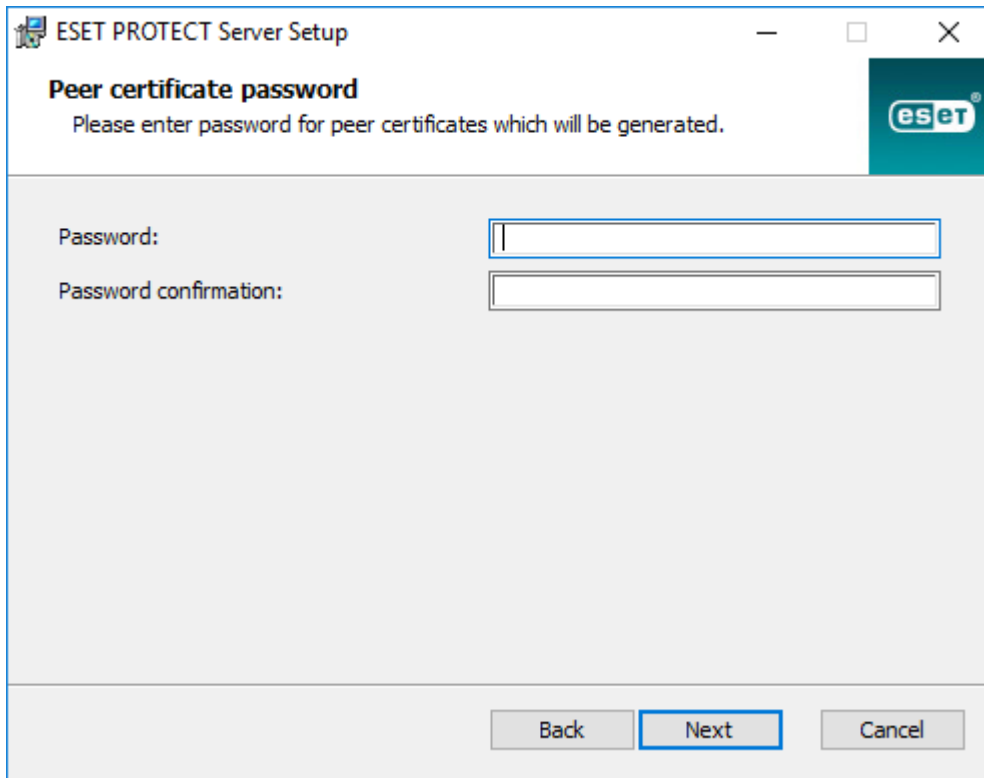


The dialog box is titled "ESET PROTECT Server Setup" and "Server certificate". It contains the following fields:

- Server hostname: [Text box]
- Certificate password: [Text box]
- Password confirmation: [Text box]

At the bottom, there are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

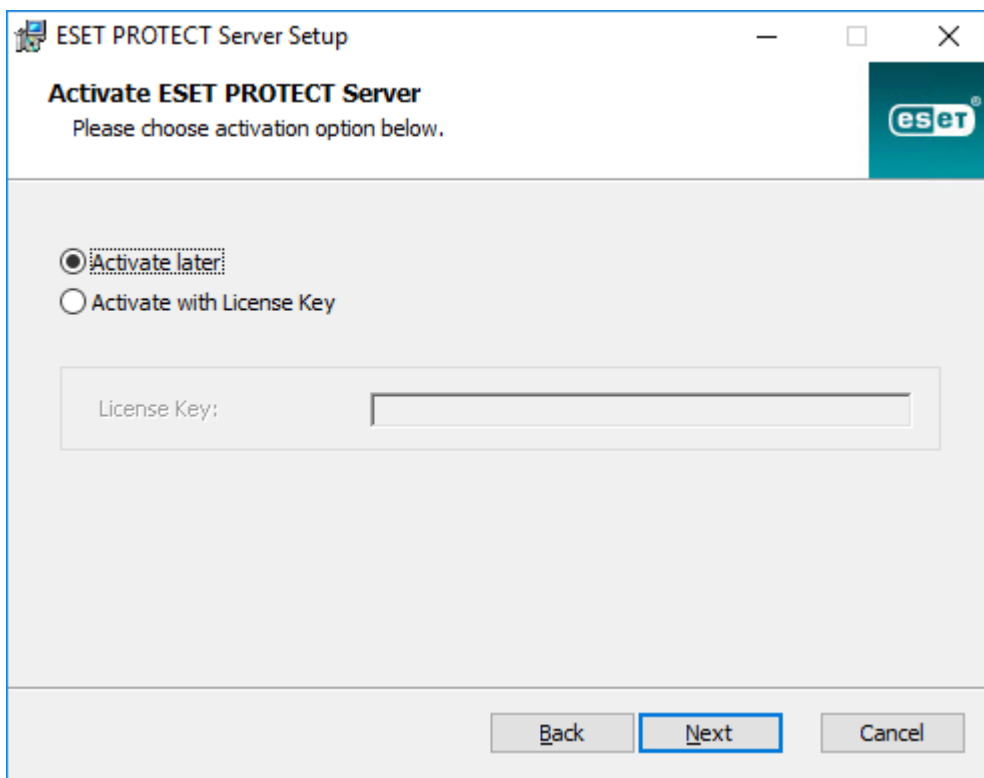
c) 피어 인증서 패스워드 필드에 에이전트 및 프록시 피어 인증서에 대한 패스워드를 입력합니다.



The screenshot shows the 'ESET PROTECT Server Setup' window. The title bar includes the ESET logo and standard window controls. The main heading is 'Peer certificate password' with a sub-instruction: 'Please enter password for peer certificates which will be generated.' Below this, there are two text input fields: 'Password:' and 'Password confirmation:'. At the bottom, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'.

11. 설치 프로그램은 초기 [정적 그룹 동기화](#) 작업을 수행할 수 있습니다. 방법(동기화 안 함, Windows 네트워크와 동기화, Active Directory와 동기화)을 선택하고 다음을 클릭합니다.

12. 유효한 [라이선스 키](#)를 입력하거나 나중에 활성화를 선택합니다.



The screenshot shows the 'ESET PROTECT Server Setup' window at the 'Activate ESET PROTECT Server' step. The title bar includes the ESET logo and standard window controls. The main heading is 'Activate ESET PROTECT Server' with a sub-instruction: 'Please choose activation option below.' There are two radio button options: 'Activate later' (which is selected) and 'Activate with License Key'. Below the 'Activate with License Key' option, there is a text input field labeled 'License Key:'. At the bottom, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'.

13. 서버의 설치 폴더를 확인하거나 변경하고 다음을 클릭합니다.

14. 설치를 클릭하여 ESET PROTECT Server를 설치합니다.

**i** ESET PROTECT 서버 설치를 완료했으면 동일한 컴퓨터(선택 사항)에 [ESET Management Agent](#)를 설치하여 클라이언트 컴퓨터를 관리하는 것과 동일한 방식으로 서버를 관리할 수 있습니다.

## Microsoft SQL Server 요구 사항

Microsoft SQL Server에 대한 다음 요구 사항이 충족되어야 합니다.

- [지원되는 Microsoft SQL Server 버전](#)을 설치합니다. 설치하는 동안 **혼합 모드** 인증을 선택하십시오.
- Microsoft SQL Server를 이미 설치한 경우 인증을 **혼합 모드(SQL Server 인증 및 Windows 인증)**로 설정하십시오. 이렇게 하려면 이 [지식 베이스 문서](#)의 지침을 따르십시오. **Windows 인증**을 사용하여 Microsoft SQL Server에 로그인하려면 이 [지식 베이스 문서](#)의 단계를 따르십시오.
- SQL Server에 대해 TCP/IP 연결을 허용합니다. 이렇게 하려면 이 [지식 베이스 문서II. SQL DB에 대해 TCP/IP 연결 허용](#)의 지침을 따르십시오.

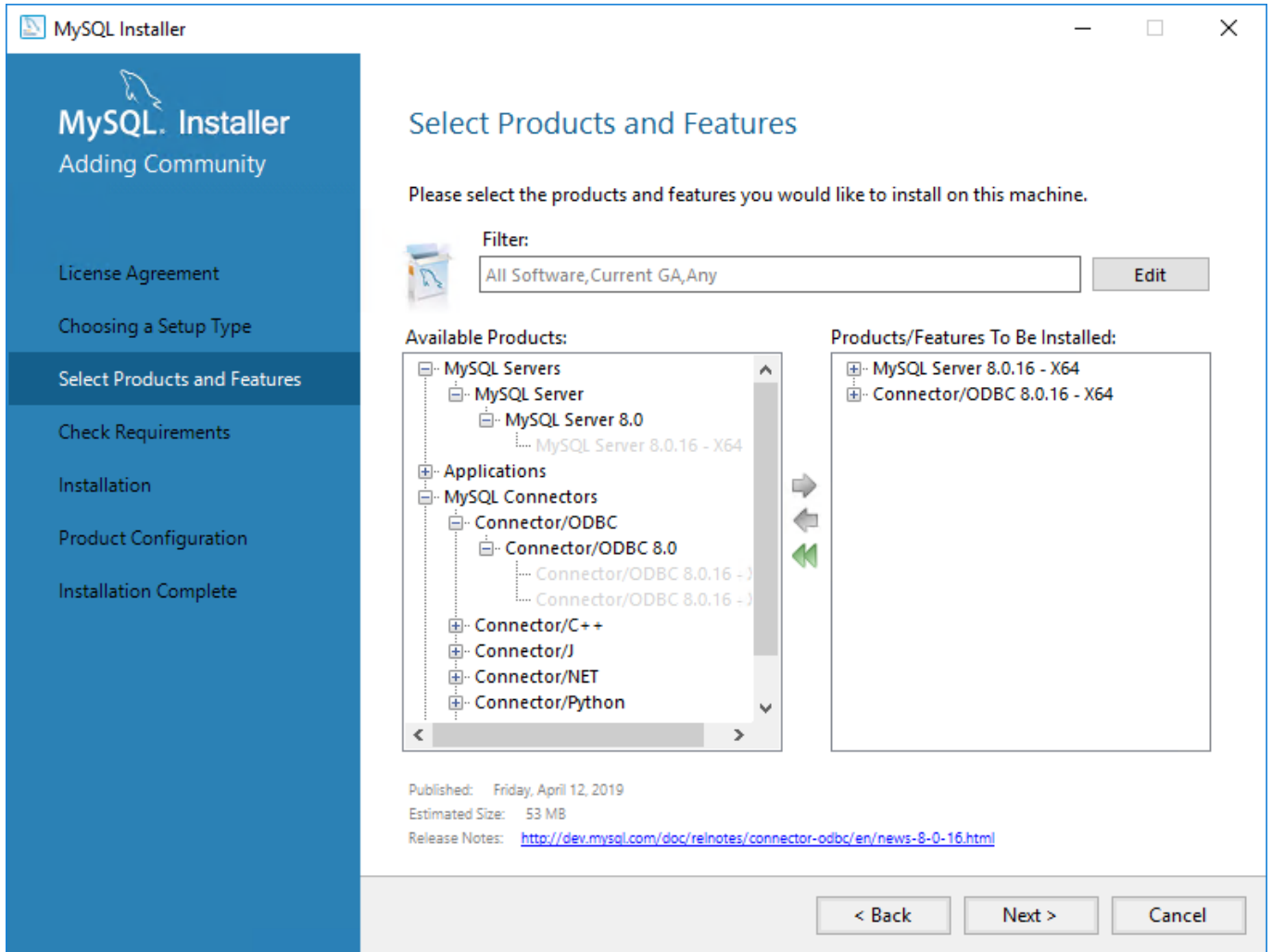
- i** Microsoft SQL Server(DB 및 사용자)를 구성하고 관리하려면 [SSMS\(SQL Server Management Studio\)](#)를 [다운로드](#)하십시오.
- [도메인 컨트롤러에 SQL Server를 설치하지 마십시오](#)(예: Windows SBS/Essentials). ESET PROTECT 제품을 다른 서버에 설치하거나 설치 중에 SQL Server Express 구성 요소를 선택하지 않는 것이 좋습니다(이 경우 기존 SQL 또는 MySQL Server를 사용하여 ESET PROTECT DB를 실행해야 함).

## MySQL Server 설치 및 구성

### 설치

지원되는 버전의 [MySQL Server 및 ODBC 커넥터](#)를 설치해야 합니다.

1. <https://dev.mysql.com/downloads/installer/>에서 MySQL 8 Windows Installer를 다운로드하고 실행합니다.
2. 라이선스 약관에 동의 확인란을 선택하고 다음을 클릭합니다.
3. 설치 설정 중에 사용자 지정을 선택하고 **MySQL Server**와 설치할 **커넥터/ODBC 커넥터**를 선택합니다. 설치된 MySQL Server의 비트 수와 ODBC 커넥터가 일치하는지 확인하십시오(x86 또는 x64).



4. 다음과 실행을 클릭하여 MySQL Server 및 ODBC 커넥터를 설치합니다.
5. 다음을 클릭합니다. 고가용성에서 독립 실행형 MySQL Server/클래식 MySQL 복제를 선택하고 다음을 클릭합니다.
6. 유형 및 네트워킹의 구성 유형 드롭다운 메뉴에서 서버 컴퓨터를 선택하고 다음을 클릭합니다.
7. 인증 방법에서 권장되는 인증 시 강력한 패스워드 암호화 사용 옵션을 선택하고 다음을 클릭합니다.
8. 계정 및 역할에서 MySQL 루트 패스워드를 두 번 입력합니다. [전용 DB 사용자 계정](#)도 생성하는 것이 좋습니다.
9. Windows 서비스에서 미리 선택된 값을 유지하고 다음을 클릭합니다.
10. 실행을 클릭하고 MySQL Server 설치가 완료될 때까지 기다립니다. 완료와 다음을 클릭한 후 마침을 클릭하여 설치 창을 닫습니다.

## 구성

1. 텍스트 편집기에서 다음 파일을 엽니다.

`C:\ProgramData\MySQL\MySQL Server 8.0\my.ini`

2. 다음 구성을 찾아 편집하거나 `[mysqld]` 파일의 `my.ini` 섹션에 추가합니다.





- 파일에 없는 경우 [mysqld] 섹션을 생성합니다.
- 파일에 파라미터가 없는 경우 [mysqld] 섹션에 추가합니다.
- MySQL 버전을 확인하려면 `mysql --version` 명령을 실행합니다.

파라미터	설명 및 권장 값	MySQL 버전으로 업그레이드
<code>max_allowed_packet=33M</code>		모든 <a href="#">지원되는 버전</a> .
<code>log_bin_trust_function_creators=1</code>	또는 <code>log_bin=0</code> 이전 로깅을 비활성화할 수 있습니다.	<a href="#">지원되는 8.x 버전</a>
<code>innodb_log_file_size=100M</code> <code>innodb_log_files_in_group=2</code>	이러한 두 파라미터 값의 곱셈은 <b>200</b> 이상이어야 합니다. <code>innodb_log_files_in_group</code> 의 최솟값은 <b>2</b> 이고 최댓값은 <b>100</b> ;이며, 이 값도 정수여야 합니다.	<a href="#">지원되는 8x 버전</a> 5.7 5.6.22 (이상 5.6.x)
<code>innodb_log_file_size=200M</code>	값을 <b>200M</b> 이상, <b>3000M</b> 이하로 설정합니다.	5.6.20 및 5.6.21

3. `my.ini` 파일을 저장하고 닫습니다.

4. 명령 프롬프트를 열고 다음 명령을 입력하여 MySQL Server를 재시작하고 구성을 적용합니다(프로세스 이름은 MySQL 버전에 따라 다름: 8.0 = `mysql80` 등).

```
net stop mysql80
net start mysql80
```

5. 명령 프롬프트에서 다음 명령을 입력하여 MySQL Server가 실행 중인지 확인합니다.

```
sc query mysql80
```

## 전용 DB 사용자 계정

**SA 계정**(Microsoft SQL) 또는 **루트 계정**(MySQL)을 사용하지 않으려는 경우 **전용 DB 사용자 계정**을 만들 수 있습니다. 이 전용 사용자 계정은 ESET PROTECT DB에 접근하는 데만 사용됩니다. ESET PROTECT 설치를 시작하기 전에 DB 서버 내에 전용 DB 사용자 계정을 만드는 것이 좋습니다. 또한 이 전용 사용자 계정을 사용하여 ESET PROTECT에서 접근하는 빈 DB를 만들어야 합니다.

전용 DB 사용자 계정에 부여해야 하는 최소 권한 집합이 있습니다:

- **MySQL 사용자 권한:** ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, SELECT, UPDATE, TRIGGER. - MySQL 권한에 대한 자세한 내용은 <http://dev.mysql.com/doc/refman/8.0/en/grant.html>을 참조하십시오.
- **Microsoft SQL Server DB 수준 역할:** ESET PROTECT DB 사용자는 `db_owner` DB 역할의 구성원이어야 합니다. Microsoft SQL Server DB 수준 역할에 대한 자세한 내용은 <https://msdn.microsoft.com/ko-kr/library/ms189121%28v=sql.100%29.aspx>를 참조하십시오.

ESET의 [지식 베이스 문서](#)에서 Microsoft SQL 및 MySQL 둘 다에 대해 DB 및 사용자 계정을 설정하는 방법에 대한 자세한 내용을 확인할 수 있습니다.

# 에이전트 설치 - Windows

## 사용 가능한 방법

Windows 워크스테이션에 ESET Management Agent 설치에 사용 가능한 다양한 설치 및 배포 방법이 있습니다.

방법	설명서	설명
.msi 설치 관리자에서 GUI 기반 설치	<ul style="list-style-type: none"><li>• <a href="#">이 장</a></li><li>• <a href="#">KB</a></li></ul>	<ul style="list-style-type: none"><li>• <b>표준</b> 설치 방법입니다.</li><li>• 이 방법은 <a href="#">서버 지원</a> 또는 <a href="#">오프라인</a> 설치로 실행할 수 있습니다.</li><li>• ESET PROTECT 서버 컴퓨터에 에이전트를 설치하는 경우 이 방법을 사용합니다.</li></ul>
ESET Remote Deployment Tool	<ul style="list-style-type: none"><li>• <a href="#">온라인 도움말</a></li></ul>	<ul style="list-style-type: none"><li>• 로컬 네트워크를 통한 대량 배포에 권장됩니다.</li><li>• 통합형 설치 관리자(에이전트 + ESET 보안 제품)를 배포하는 데 사용할 수 있음</li></ul>
통합형 에이전트 설치 관리자	<ul style="list-style-type: none"><li>• <a href="#">통합형 에이전트 설치 관리자 생성</a></li><li>• <a href="#">KB</a></li></ul>	<ul style="list-style-type: none"><li>• 설치 관리자에는 보안 제품 및 포함된 정책도 포함될 수 있습니다.</li><li>• 설치 관리자의 크기는 수백 MB입니다.</li></ul>
에이전트 스크립트 설치 관리자	<ul style="list-style-type: none"><li>• <a href="#">에이전트 스크립트 설치 관리자 생성</a></li><li>• <a href="#">KB</a></li></ul>	<ul style="list-style-type: none"><li>• 설치 관리자는 실행 가능한 스크립트입니다. 크기는 작지만 .msi 설치 관리자의 위치에 접근해야 합니다.</li><li>• 스크립트는 로컬 설치 관리자와 HTTP 프록시를 사용하도록 편집할 수 있습니다.</li></ul>
SCCM 및 GPO 배포	<ul style="list-style-type: none"><li>• <a href="#">SCCM</a></li><li>• <a href="#">GPO</a></li><li>• <a href="#">KB</a></li></ul>	<ul style="list-style-type: none"><li>• 원격 대량 배포의 고급 방법입니다.</li><li>• 작은 .ini 파일을 사용합니다.</li></ul>
서버 작업 - 에이전트 배포	<ul style="list-style-type: none"><li>• <a href="#">온라인 도움말</a></li><li>• <a href="#">KB</a></li></ul>	<ul style="list-style-type: none"><li>• SCCM 및 GPO에 대한 대체 방법입니다.</li><li>• HTTP 프록시를 통해서만 실행할 수 없습니다.</li><li>• ESET PROTECT 웹 콘솔에서 ESET PROTECT 서버로 실행됩니다.</li></ul>



에이전트와 ESET PROTECT 서버 간의 통신 프로토콜은 인증을 지원하지 않습니다. 인증을 요구하는 ESET PROTECT 서버에 에이전트 통신을 전달하는 데 사용되는 프록시 솔루션은 작동되지 않습니다. 웹 콘솔이나 에이전트에 대해 기본값이 아닌 포트를 사용하도록 선택하면 방화벽을 조정해야 할 수 있습니다. 조정하지 않으면 설치에 실패할 수 있습니다.

## GUI 기반 설치

Windows에 로컬로 ESET Management Agent 구성 요소를 설치하려면 다음 단계를 따릅니다.

1. ESET PROTECT [다운로드 섹션](#)으로 이동하여 이 ESET PROTECT 구성 요소용 독립 실행형 설치 관리자를 다운로드합니다. (*agent\_x86.msi* 또는 *agent\_x64.msi* 또는 *agent\_arm64.msi*).
2. ESET Management 에이전트 설치 관리자를 실행하고 EULA에 동의하는 경우 동의합니다.
3. **제품 향상 프로그램에 참여** 확인란을 선택하여 익명의 원격 측정 데이터 및 충돌 보고서(OS 버전 및 유형, ESET 제품 버전 및 기타 제품 특정 정보)를 ESET으로 보냅니다.
4. **서버 호스트**(ESET PROTECT 서버의 호스트 이름 또는 IP 주소) 및 **서버 포트**(기본 포트는 2222임, 다른 포트를 사용하는 경우 기본 포트를 해당 사용자 지정 포트 번호로 바꿈)를 입력합니다.



**서버 호스트**가 **서버 인증서**의 **호스트** 필드에 정의된 하나 이상의 값(이상적으로는 FQDN)과 일치하는지 확인합니다. 일치하지 않을 경우 "받은 서버 인증서가 유효하지 않습니다." 오류가 발생합니다. 서버 인증서 호스트 필드에서 와일드카드(\*)를 사용하면 인증서가 모든 **서버 호스트**에서 작동할 수 있습니다.

5. 에이전트 - 서버 연결용 프록시를 사용하는 경우 **프록시 사용** 옆의 확인란을 선택합니다. 이 확인란을 선택하면 설치 관리자가 [오프라인 설치](#)를 계속합니다.

이 프록시 설정은 ESET Management 에이전트와 ESET PROTECT 서버 간의 (복제)에만 사용되며 업데이트 캐시에는 사용되지 않습니다.

- **프록시 호스트 이름:** HTTP 프록시 시스템의 호스트 이름 또는 IP 주소입니다.
  - **프록시 포트:** 기본값은 3182입니다.
  - **사용자 이름, 비밀번호:** 인증을 사용할 경우 프록시에 사용되는 자격 증명을 입력합니다.
- 나중에 [정책](#)에서 프록시 설정을 변경할 수 있습니다. [프록시](#)는 프록시를 통한 에이전트 - 서버 연결을 구성하려는 경우 먼저 설치해야 합니다.

6. 다음 설치 옵션 중 하나를 선택하고 아래 해당 섹션의 단계를 따르십시오.

- [서버 지원 설치](#) - ESET PROTECT 웹 콘솔 관리자 자격 증명을 제공해야 합니다. 설치 관리자가 자동으로 필요한 인증서를 다운로드합니다.

❗ 서버 지원 설치의 경우 사용자에게 [2단계 인증](#)을 사용할 수 없습니다.

- [오프라인 설치](#) - 에이전트 인증서 및 인증 기관을 제공해야 합니다. 둘 다 ESET PROTECT에서 [내보낼](#) 수 있습니다. 또는 [사용자 지정 인증서](#)를 사용할 수도 있습니다.

## 명령줄 설치

MSI 설치 관리자를 로컬 또는 원격으로 실행할 수 있습니다. ESET [웹 사이트](#)에서 ESET Management Agent를 다운로드합니다.

파라미터	설명 및 허용된 값
P_HOSTNAME=	ESET PROTECT 서버의 호스트 이름 또는 IP 주소입니다.
P_PORT=	에이전트 연결에 대한 서버 포트(옵션, 지정하지 않으면 기본 포트 2222가 사용됨)입니다.
P_CERT_PATH=	.txt 파일의 Base64 형식 에이전트 인증서 경로입니다( <a href="#">ESET PROTECT 웹 콘솔</a> 에서 내보냄).
P_CERT_AUTH_PATH=	.txt 파일의 Base64 형식 인증 기관 경로입니다( <a href="#">ESET PROTECT 웹 콘솔</a> 에서 내보냄).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	YES, .txt 파일에 저장된 에이전트 인증서와 인증 기관을 참조하는 경우 이 파라미터를 사용합니다.
P_CERT_PASSWORD=	에이전트 인증서의 패스워드를 제공하려면 이 파라미터를 사용합니다.
P_CERT_CONTENT=	파일의 Base64 형식 에이전트 인증서 문자열입니다( <a href="#">ESET PROTECT 웹 콘솔</a> 에서 내보냄).
P_CERT_AUTH_CONTENT=	Base64 형식의 인증 기관 문자열입니다( <a href="#">ESET PROTECT 웹 콘솔</a> 에서 내보냄).
PASSWORD=	<a href="#">패스워드 보호된 에이전트</a> 를 제거하기 위한 패스워드입니다.
P_ENABLE_TELEMETRY=	0 - 비활성화됨(기본 옵션), 1 - 활성화됨 ESET에 충돌 보고서 및 원격측정 데이터를 보냅니다(옵션 파라미터).
P_INSTALL_MODE_EULA_ONLY=	1 ESET Management Agent 설치를 부분 자동으로 설치하는 경우 이 파라미터를 사용합니다. 에이전트 설치 창이 나타나고 최종 사용자 사용권 계약에 동의하여 원격측정을 활성화/비활성화하라는 메시지가 표시됩니다(지정된 경우에는 P_ENABLE_TELEMETRY가 무시됨). 다른 에이전트 설치 설정은 명령줄 파라미터에서 가져옵니다. 에이전트 설치 프로세스가 완료된 것을 확인할 수 있습니다.
P_USE_PROXY=	1, 이 파라미터를 사용하여 ESET Management Agent와 ESET PROTECT 서버 간의 복제를 위한 HTTP 프록시(네트워크에 이미 설치됨) 사용을 활성화할 수 있습니다(업데이트 캐시 사용 아님).
P_PROXY_HTTP_HOSTNAME=	HTTP 프록시의 호스트 이름 또는 IP 주소입니다.
P_PROXY_HTTP_PORT=	에이전트 연결용 HTTP 프록시 포트입니다.

## 명령줄 설치의 예

필요한 경우 아래의 주황색 코드를 바꿉니다.

- 다음과 같은 기본 포트 연결, 활성화된 원격측정, 파일에 저장된 에이전트 인증서 및 인증 기관을 사용하여 자동 설치(/q 파라미터)합니다.

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- 다음과 같은 에이전트 인증서 및 인증 기관에 제공된 문자열과 에이전트 인증서 패스워드 및 HTTP 프록시 파라미터를 사용하여 자동 설치합니다.

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=
CJfXtf1kZqLZKA19P48HymBHa3CKw P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvk
pqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_
HTTP_PORT=3128
```

- 부분 자동 설치:

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Users\
Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Deskt
op\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

## 서버 지원 에이전트 설치

서버 지원 에이전트 설치를 계속하려면 다음 단계를 따르십시오.

1. 서버 **호스트** 필드에 ESET PROTECT 웹 콘솔의 호스트 이름 또는 IP 주소(ESET PROTECT 서버와 동일)를 입력합니다. 사용자 지정 포트를 사용하지 않는 경우 **웹 콘솔 포트**를 기본 포트 2223으로 그대로 둡니다. 또는 **사용자 이름 및 비밀번호** 필드에 웹 콘솔 계정 자격 증명을 입력합니다. 도메인 사용자로 로그인하려면 **도메인에 로그인** 옆의 확인란을 선택합니다.

- 서버 호스트가 서버 인증서의 호스트 필드에 정의된 하나 이상의 값(이상적으로는 FQDN)과 일치하는지 확인합니다. 일치하지 않을 경우 "받은 서버 인증서가 유효하지 않습니다." 오류가 발생합니다. 유일한 예외는 서버 인증서 호스트 필드에 와일드카드(\*)가 있는 경우입니다. 이 경우 모든 서버 호스트에서 작동한다는 것을 의미합니다.
- 서버 지원 설치의 경우 사용자에게 **2단계 인증**을 사용할 수 없습니다.

2. 인증서를 수락할 것인지 묻는 메시지가 표시되면 **예**를 클릭합니다.
3. 컴퓨터를 생성하지 않음(처음 연결할 때 컴퓨터가 자동으로 생성됨) 또는 사용자 지정 정적 그룹 선택을 선택합니다. 사용자 지정 정적 그룹 선택을 클릭하는 경우 ESET PROTECT의 기존 정적 그룹 목록에서 선택할 수 있습니다. 선택한 그룹에 컴퓨터가 추가됩니다.
4. ESET Management 에이전트의 대상 폴더를 지정하고(기본 위치를 사용하는 것이 좋음) **다음**을 클릭한 후 **설치**를 클릭합니다.

## 오프라인 에이전트 설치

오프라인 에이전트 설치를 계속하려면 다음 단계를 따르십시오.

1. 이전 단계에서 **프록시 사용**을 선택한 경우 **프록시 호스트 이름**, **프록시 포트**(기본 포트는 3128), **사용자 이름 및 비밀번호**를 제공하고 **다음**을 클릭합니다.
2. **찾아보기**를 클릭하고 **피어 인증서**(ESET PROTECT에서 내보낸 에이전트 인증서임) 위치로 이동합니다. 이 인증서에는 비밀번호가 필요하지 않으므로 **인증서 비밀번호** 텍스트 필드를 비워둡니다. **인증 기관**을

찾을 필요가 없습니다. 이 필드를 비워둡니다.

**i** ESET PROTECT에서 ESET PROTECT 설치 중에 자동으로 생성된 기본 인증서 대신 사용자 지정 인증서를 사용하는 경우 적절하게 해당 사용자 지정 인증서를 사용합니다.

**!** 인증서 비밀번호에는 문자를 포함할 수 없습니다: " \ 이러한 문자를 사용하면 에이전트를 초기화하는 동안 심각한 오류가 발생합니다.

3. 기본 폴더에 설치하려면 **다음**을 클릭하고 다른 폴더를 선택하려면 **변경**을 클릭합니다(기본 위치를 사용하는 것이 좋음).

## ESET Remote Deployment Tool

ESET Remote Deployment Tool은 ESET PROTECT에서 생성된 [설치 관리자 패키지](#)를 배포하는 간편한 방법으로, ESET Management Agent와 ESET 보안 제품을 네트워크로 컴퓨터에 원격으로 배포할 수 있습니다.

ESET Remote Deployment Tool은 ESET [웹 사이트에서](#) 독립 실행형 ESET PROTECT 구성 요소로 무료로 이용할 수 있습니다. 배포 도구는 주로 중소 네트워크에서 배포하는 데 사용되며 관리자 권한으로 실행됩니다.

**i** ESET Remote Deployment Tool은 Microsoft Windows 운영 체제만 [지원되는](#) 클라이언트 컴퓨터에 ESET Management Agent를 배포하는 전용 도구입니다.

이 도구의 필수 구성 요소 및 사용에 대한 자세한 내용은 [ESET Remote Deployment Tool](#) 장을 참조하십시오.

## 웹 콘솔 설치 - Windows

다음 두 가지 방법으로 Windows에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다.

- [통합형 설치 관리자를 사용](#)하는 것이 좋습니다.
- 고급 사용자는 [수동 설치](#)를 수행할 수 있습니다.

**i** ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다.


## 통합형 설치 관리자를 사용하여 웹 콘솔 설치

### 필수 구성 요소

- ESET PROTECT 서버가 설치되었습니다.


**i** ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다. 이 절차를 수행하려면 [추가 단계](#)를 진행해야 합니다.

- Apache Tomcat은 ESET PROTECT 웹 콘솔을 실행하는 데 필요한 필수 구성 요소입니다.
- Apache Tomcat에는 64비트 Java/OpenJDK가 필요합니다. 시스템에 여러 가지 Java 버전이 설치되어 있는 경우, 이전 Java 버전을 제거하고 [지원되는 Java](#) 최신 버전만 유지하는 것이 좋습니다.

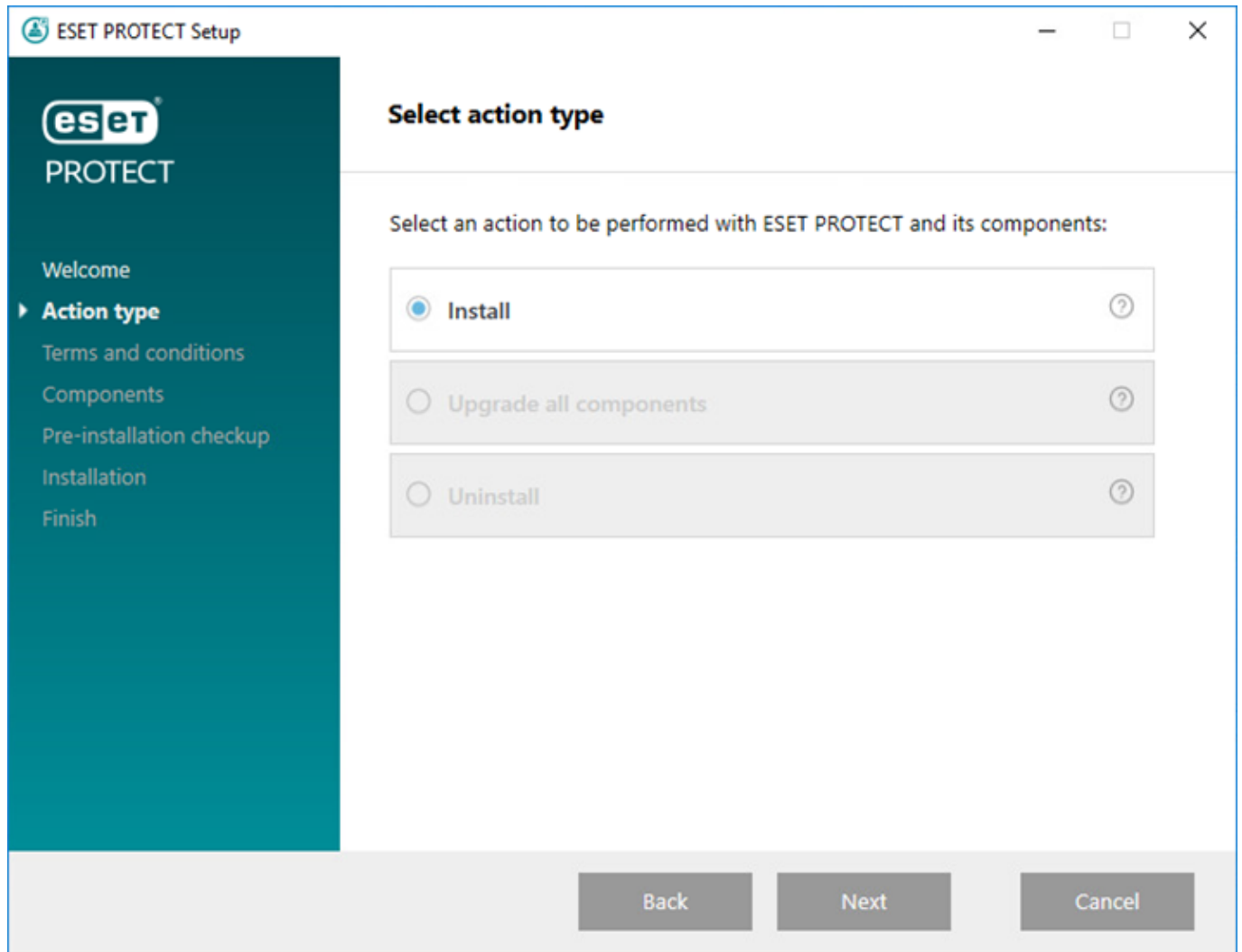
 2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.

## 설치

통합형 설치 관리자를 사용하여 Windows에 ESET PROTECT 웹 콘솔 구성 요소를 설치하려면 다음을 수행하십시오.

 위에 나열된 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

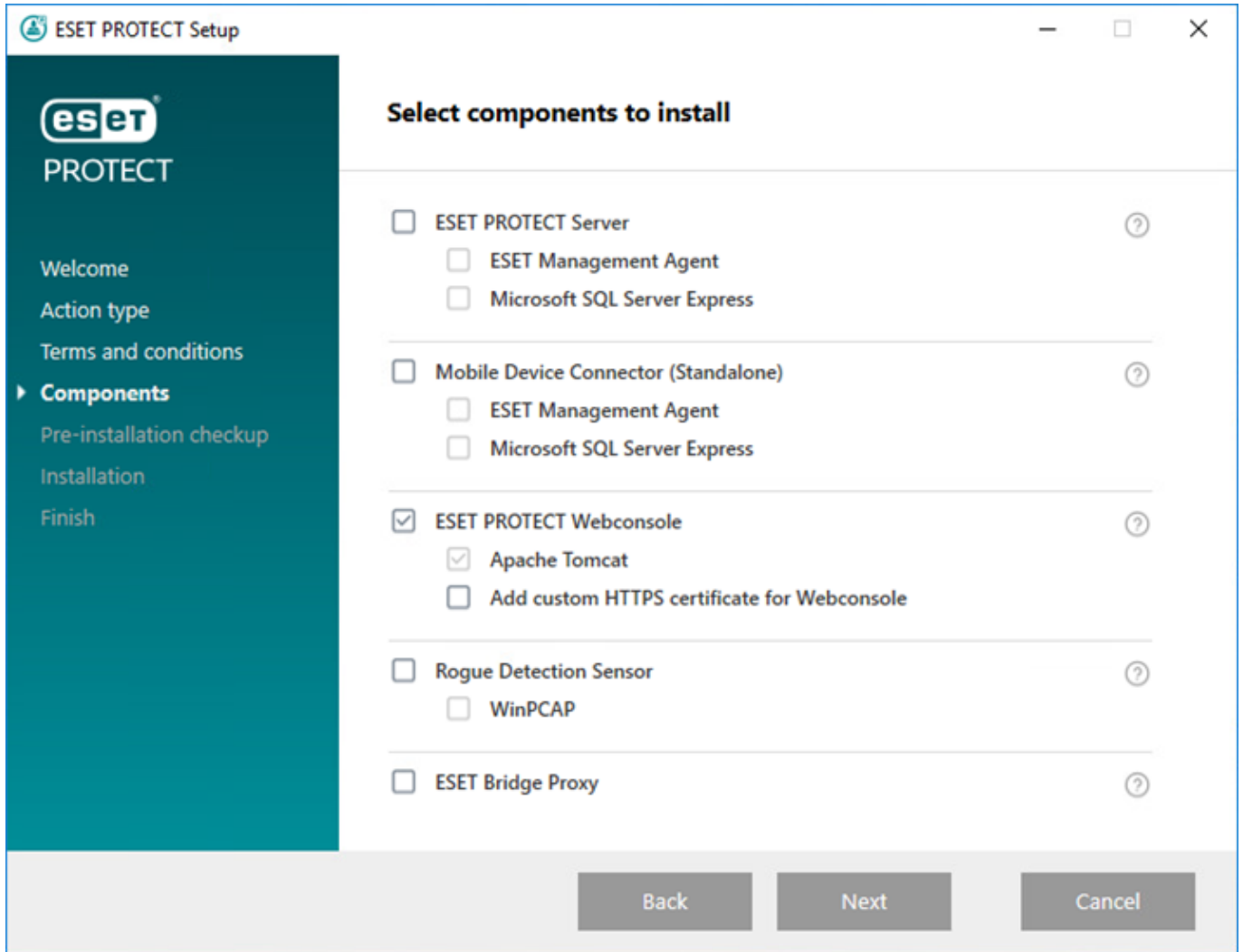
1. ESET 웹 사이트에서 [ESET PROTECT 통합형 설치 관리자](#)를 다운로드하고 다운로드한 파일의 압축을 풉니다.
2. 최신 버전의 Apache Tomcat을 설치하려고 하고 통합형 설치 관리자에 이전 버전의 Apache Tomcat이 포함되어 있는 경우(이 단계는 선택 사항임 - 최신 버전의 Apache Tomcat이 필요하지 않은 경우 4단계로 건너뛰):
  - a.x64 폴더를 열고 *installers* 폴더로 이동합니다.
  - b.*installers* 폴더에 있는 *apache-tomcat-9.0.x-windows-x64.zip* 파일을 제거합니다.
  - c.Apache Tomcat 9 [64비트 Windows 압축](#) 패키지를 다운로드합니다.
  - d.다운로드한 압축 패키지를 *installers* 폴더로 이동합니다.
3. 통합형 설치 관리자를 시작하려면 *Setup.exe* 파일을 두 번 클릭하고 **시작** 화면에서 **다음**을 클릭합니다.
4. **설치**를 선택하고 **다음**을 클릭합니다.



5. EULA에 동의한 후에 다음을 클릭합니다.

6. 설치할 구성 요소 선택에서 ESET PROTECT 웹 콘솔 확인란만 선택하고 다음을 클릭합니다.

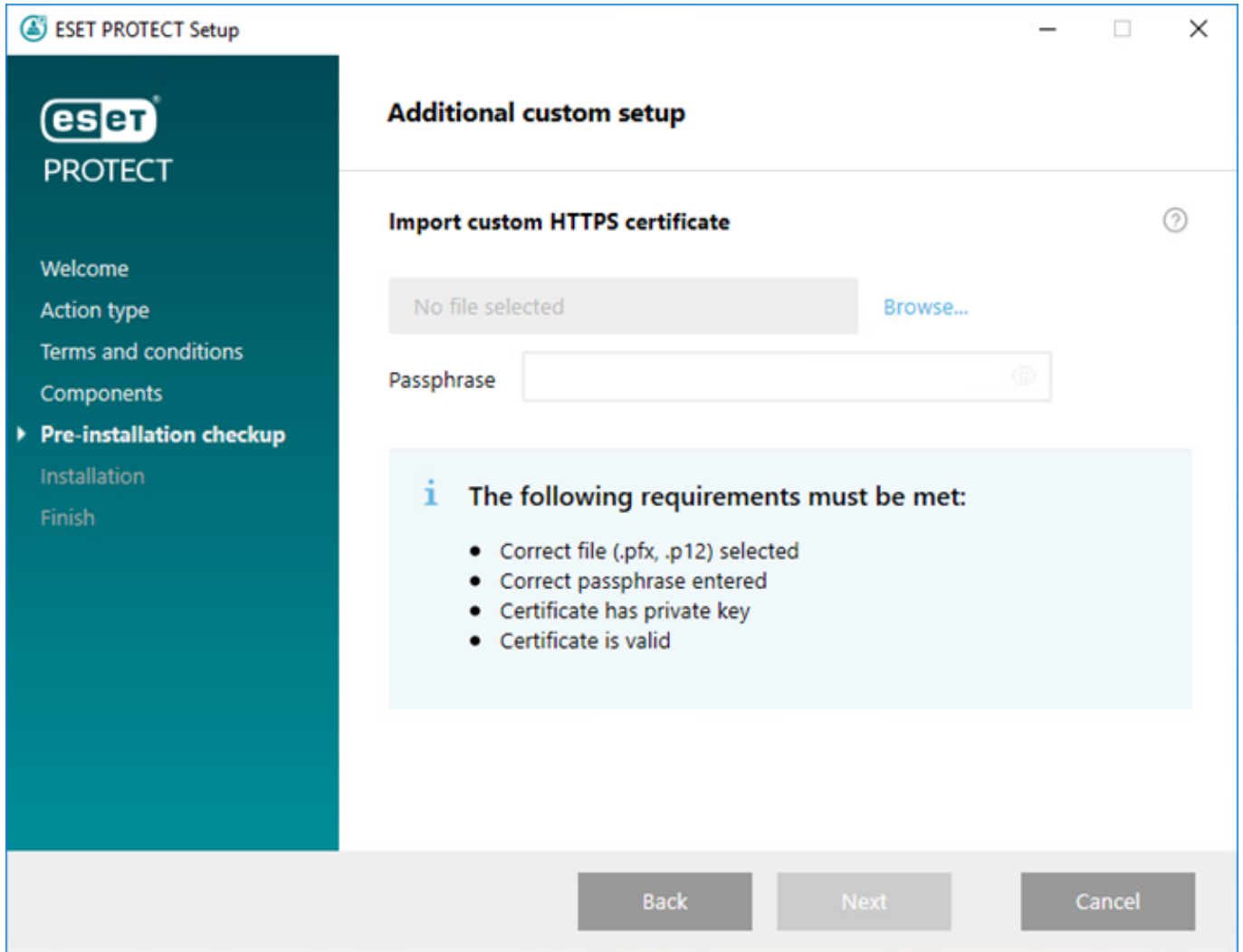




필요한 경우 **웹 콘솔용 사용자 지정 HTTPS 인증서 추가** 확인란을 선택합니다.

- ESET PROTECT 웹 콘솔에 대한 사용자 지정 HTTPS 인증서를 사용하려면 이 옵션을 선택합니다.
- 이 옵션을 선택하지 않으면 설치 관리자가 새로운 Tomcat 키 저장소(자체 서명된 HTTPS 인증서)를 자동으로 생성합니다.
- **웹 콘솔용 사용자 지정 HTTPS 인증서 추가**를 선택했으면 **찾아보기**를 클릭하고 올바른 인증서(.pfx 또는 .p12 파일)를 선택한 후 해당하는 **비밀번호**를 입력합니다(또는 비밀번호가 없는 경우 필드를 공백으로 남김). 설치 관리자가 Tomcat 서버에 웹 콘솔 접근 인증서를 설치합니다. 계속하려면 **다음**을 클릭합니다.

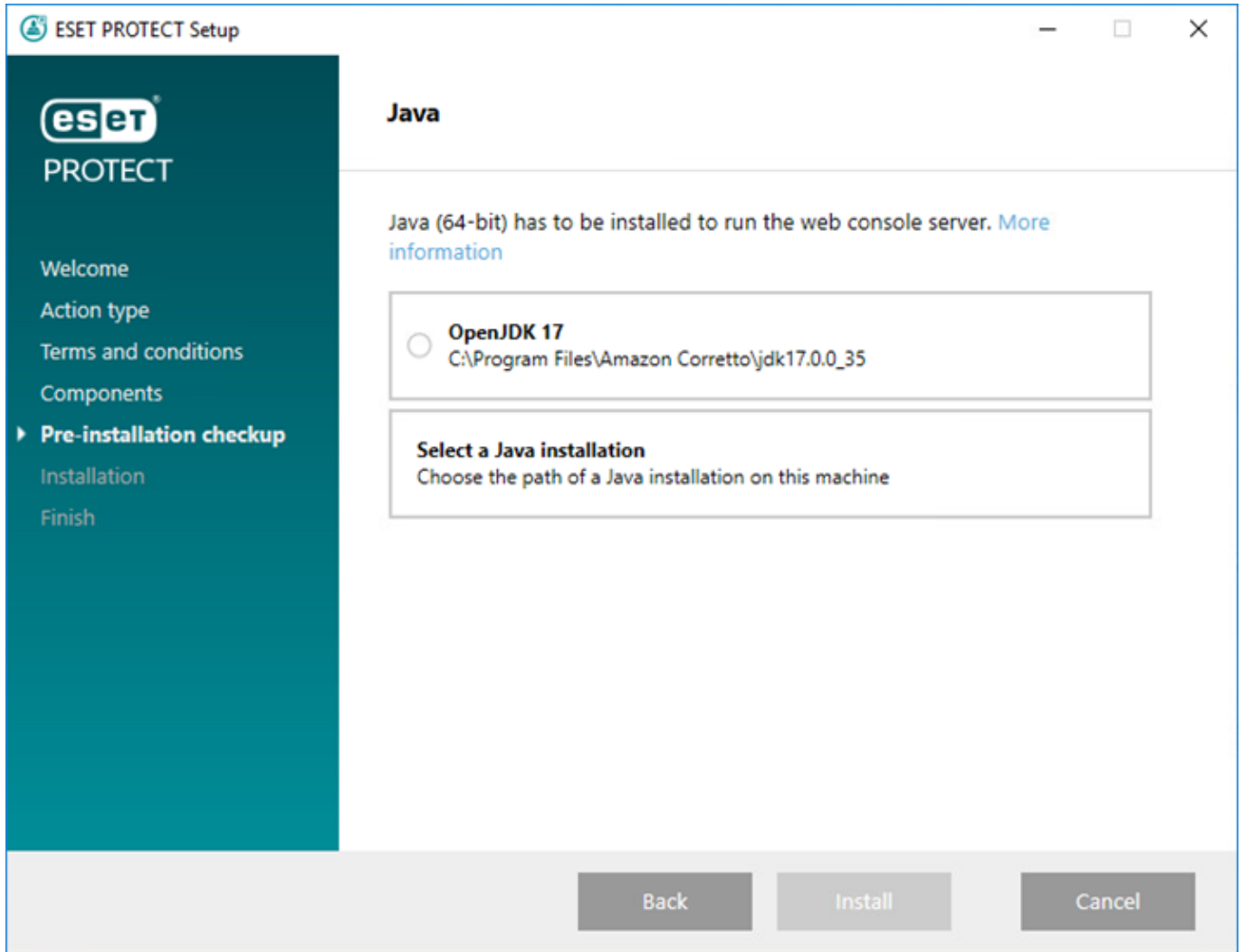




7. 컴퓨터에 Java 설치를 선택합니다. 최신 버전의 Java/OpenJDK를 사용하고 있는지 확인합니다.

a) 이미 설치된 Java를 선택하려면 **Java 설치 선택**을 클릭하고 Java가 설치된 폴더(*bin* 하위 폴더가 있음, 예: *C:\Program Files\Amazon Corretto\jdk1.8.0\_212*)를 선택하고 **확인**을 클릭합니다. 잘못된 경로를 선택한 경우 설치 관리자에 메시지가 표시됩니다.

b) 계속하려면 **설치**를 클릭하고 Java 설치 경로를 변경하려면 **변경**을 클릭합니다.



8. 설치가 완료되면 **완료**를 클릭합니다.

ESET PROTECT 서버와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치한 경우 다음 추가 단계를 수행하여 ESET PROTECT 웹 콘솔과 ESET PROTECT 서버 간의 통신을 활성화하십시오.

a) Apache Tomcat 서비스를 중지합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **중지**를 선택합니다.

**i** b) 메모장을 관리자 권한으로 실행하고 를 편집합니다. `C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.

c) `server_address=localhost`를 찾습니다.

d) `localhost`를 ESET PROTECT 서버의 IP 주소로 바꾸고 파일을 저장합니다.

e) Apache Tomcat 서비스를 시작합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택합니다.

9. 지원되는 웹 브라우저에서 ESET PROTECT 웹 콘솔을 열면 로그인 화면이 표시됩니다.

- ESET PROTECT 웹 콘솔을 호스팅하는 컴퓨터에서: `https://localhost/era`

- ESET PROTECT 웹 콘솔에 대한 인터넷 접근 권한이 있는 컴퓨터에서(`IP_ADDRESS_OR_HOSTNAME`을 ESET PROTECT 웹 콘솔의 IP 주소 또는 호스트 이름으로 대체): `https://IP_ADDRESS_OR_HOSTNAME/era`

**i** 엔터프라이즈 솔루션 또는 저성능 시스템에 대한 추가 웹 콘솔 구성도 참조하십시오.

# 웹 콘솔을 수동으로 설치



ESET PROTECT 웹 콘솔의 수동 설치의 고급 절차입니다. [통합형 설치 관리자](#)를 사용하여 ESET PROTECT 웹 콘솔을 설치하는 것이 좋습니다.

## 필수 구성 요소

- ESET PROTECT 서버가 설치되었습니다.



ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다. 이 절차를 수행하려면 [추가 단계](#)를 진행해야 합니다.

- Apache Tomcat은 ESET PROTECT 웹 콘솔을 실행하는 데 필요한 필수 구성 요소입니다. Apache Tomcat 설치:

a) <https://tomcat.apache.org>에서 [지원되는 최신 버전](#)의 Apache Tomcat 설치 관리자 파일(32비트/64비트 Windows Service Installer) *apache-tomcat-[버전].exe*를 다운로드합니다.

b) 설치 관리자를 실행합니다.

c) 설치하는 동안 Java의 경로(Java *bin* 및 *lib* 폴더의 상위 폴더)를 선택하고 **Run Apache Tomcat** 확인란을 선택합니다.

d) 설치 후에는 Apache Tomcat 서비스가 실행 중이고 그 시작 유형이 **자동**으로 설정되어 있어야 합니다(**services.msc**에서).

- Apache Tomcat에는 64비트 Java/OpenJDK가 필요합니다. 시스템에 여러 가지 Java 버전이 설치되어 있는 경우, 이전 Java 버전을 제거하고 [지원되는 Java](#) 최신 버전만 유지하는 것이 좋습니다.



2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.

## 설치

Windows에 ESET PROTECT 웹 콘솔 구성 요소를 설치하려면 다음 단계를 따르십시오.



위에 나열된 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

1. ESET PROTECT [다운로드 섹션](#)으로 이동하여 이 ESET PROTECT 구성 요소용 독립 실행형 설치 관리자를 다운로드합니다. (웹 콘솔에 연결 *era.war*).

2. *era.war*을 Apache Tomcat 웹 애플리케이션 폴더에 복사합니다.

`C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\webapps\`

3. Apache Tomcat이 자동으로 *era.war* 파일을 *era* 폴더에 추출하고 ESET PROTECT 웹 콘솔을 설치합니다. 추출이 완료될 때까지 몇 분간 기다립니다. 추출이 발생하지 않으면 [문제 해결 단계](#)를 따르십시오.

4. ESET PROTECT 서버와 동일한 컴퓨터에 ESET PROTECT 웹 콘솔을 설치한 경우, Apache Tomcat 서비스를 다시 시작합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **중지**를 선택합니다. 중지를 클릭하고 30초간 기다린 다음 **시작**을 클릭합니다.

ESET PROTECT 서버와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치한 경우 다음 추가 단계를 수행하여 ESET PROTECT 웹 콘솔과 ESET PROTECT 서버 간의 통신을 활성화하십시오.

a) Apache Tomcat 서비스를 중지합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **중지**를 선택합니다.

! b) 메모장을 관리자 권한으로 실행하고 를 편집합니다. `C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.

c) `server_address=localhost`를 찾습니다.

d) `localhost`를 ESET PROTECT 서버의 IP 주소로 바꾸고 파일을 저장합니다.

e) Apache Tomcat 서비스를 시작합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택합니다.

5. 지원되는 웹 브라우저에서 ESET PROTECT 웹 콘솔을 열면 로그인 화면이 표시됩니다.

- ESET PROTECT 웹 콘솔을 호스팅하는 컴퓨터에서: `http://localhost:8080/era`

- ESET PROTECT 웹 콘솔에 대한 인터넷 접근 권한이 있는 컴퓨터에서(`IP_ADDRESS_OR_HOSTNAME`을 ESET PROTECT 웹 콘솔의 IP 주소 또는 호스트 이름으로 대체):

`http://IP_ADDRESS_OR_HOSTNAME:8080/era`

6. 설치 후 웹 콘솔 구성:

- Apache Tomcat 수동 설치 중에 기본 HTTP 포트는 8080으로 설정됩니다. Apache Tomcat용 HTTPS 연결을 설정하는 것이 좋습니다.

- 엔터프라이즈 솔루션 또는 저성능 시스템에 대한 추가 웹 콘솔 구성도 참조하십시오.

## RD Sensor 설치 - Windows

### 필수 구성 요소

- WinPcap - 최신 버전의 WinPcap을 사용하십시오(4.1.0 이상).
- 네트워크가 올바르게 구성되어야 합니다(적절한 포트가 열려 있음, 들어오는 통신이 방화벽에 의해 차단되지 않음 등).
- ESET PROTECT Server에 연결할 수 있습니다.
- 모든 프로그램 기능을 완전히 지원하려면 ESET Management 에이전트가 로컬 컴퓨터에 설치되어야 합니다.
- `C:\ProgramData\ESET\Rogue Detection Sensor\Logs`에서 Rogue Detection Sensor 로그 파일을 찾을 수 있습니다.

### 설치

Windows에 RD Sensor 구성 요소를 설치하려면 다음 단계를 따릅니다.

! 위에 나열된 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

1. ESET PROTECT [다운로드 섹션](#)으로 이동하여 이 ESET PROTECT 구성 요소용 독립 실행형 설치 관리자를 다운로드합니다. (*rdsensor\_x86.msi* 또는 *rdsensor\_x64.msi*).
2. RD Sensor 설치 관리자 파일을 두 번 클릭하여 설치를 시작합니다.
3. EULA에 동의한 후 **다음**을 클릭합니다.
4. **제품 항상 프로그램에 참여** 확인란을 선택하여 익명의 원격 측정 데이터 및 충돌 보고서(OS 버전 및 유형, ESET 제품 버전 및 기타 제품 특정 정보)를 ESET으로 보냅니다.
5. RD Sensor의 설치 위치를 선택하고 **다음 > 설치**를 클릭합니다.

! 여러 네트워크 세그먼트가 있는 경우 전체 네트워크에 있는 모든 장치의 종합 목록을 생성하려면 각 네트워크 세그먼트에 Rogue Detection Sensor를 별도로 설치해야 합니다.

## 미러 도구 - Windows

### [Linux 사용자입니까?](#)

미러 도구는 오프라인 검색 엔진 업데이트에 필요합니다. 클라이언트 컴퓨터가 인터넷에 연결되어 있지 않고 검색 엔진 업데이트가 필요한 경우 미러 도구를 사용하여 ESET 업데이트 서버에서 업데이트 파일을 다운로드한 후 로컬로 저장할 수 있습니다.

미러 도구에는 다음과 같은 기능이 있습니다.

- 모듈 업데이트 - 탐지 엔진 업데이트 및 기타 프로그램 모듈을 다운로드하지만, [자동 업데이트](#) (uPCU)는 다운로드하지 않습니다.
  - 저장소 생성 - [자동 업데이트](#) (uPCU)를 포함한 전체 [오프라인 저장소](#)를 생성할 수 있습니다.
- 미러 도구는 ESET LiveGrid® 데이터를 다운로드하지 않습니다.

## 필수 구성 요소

! 미러 도구는 Windows XP 및 Windows Server 2003을 지원하지 않습니다.

- 대상 폴더는 업데이트에 접근하려는 방법에 따라 공유, Samba/Windows 또는 HTTP/FTP 서비스에 사용할 수 있어야 합니다.

oWindows용 ESET 보안 제품 - HTTP 또는 공유 폴더를 사용하여 원격으로 업데이트할 수 있습니다.

oLinux/macOS에 대한 ESET 보안 제품 - HTTP만을 사용해 원격으로 업데이트할 수 있습니다. 공유 폴더를 사용하는 경우 ESET 보안 제품과 동일한 컴퓨터에 있어야 합니다.

- 사용자 이름 및 비밀번호를 포함하는 유효한 [오프라인 라이선스](#) 파일이 있어야 합니다. 라이선스 파일 생성 시 **사용자 이름 및 비밀번호 포함** 옆의 확인란을 선택해야 합니다. 또한, 라이선스 이름도 입력해야 합니다. 미러 도구를 활성화하고 업데이트 미러를 생성하려면 오프라인 라이선스 파일이 필요합니다.

×

Create offline license file

Product

ESET Endpoint Security for Windows

Name

Test license

Units count

1

/3

Username and password

☒ Include Username and Password  
 When included it is possible to update from ESET servers

ESET PROTECT

☐ Allow management with ESET PROTECT

GENERATE

CANCEL

- 미리 도구를 실행하기 전에 다음 패키지를 설치해야 합니다.
- [Visual Studio 2010용 Visual C++ 재배포 가능 패키지](#)
- [Visual C++ 2015 재배포 가능 패키지 x86](#)

## 미리 도구를 사용하는 방법

1. [ESET 다운로드 페이지](#)(독립 실행형 설치 관리자 섹션)에서 미리 도구를 다운로드합니다.
2. 다운로드된 압축파일의 압축을 풉니다.
3. 명령 프롬프트를 열고 *MirrorTool.exe* 파일을 포함하는 폴더로 이동합니다.
4. 아래 명령을 실행하여 미리 도구 및 해당 버전에 사용 가능한 모든 파라미터를 봅니다.

```
MirrorTool.exe --help
```

```

C:\Users\ >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights
reserved.
Allowed options:
  --mirrorType arg                [required for module update]
                                  Type of mirror. Possible values (case
                                  insensitive): regular, pre-release,
                                  delayed.
  --intermediateUpdateDirectory arg [required for module update]
                                  Files will be downloaded to this
                                  directory to create mirror in output
                                  directory.
  --offlineLicenseFilename arg    [required for module update]
                                  Offline license file.
  --updateServer arg             [optional]
                                  Update server. (e.g.:
                                  http://update.eset.com/eset_upd/ep6/)
                                  Mirror will be created in output
                                  directory, only specified path in
                                  server will be mirrored.
  --outputDirectory arg          [required for module update]
                                  Directory where mirror will be created.
  --proxyHost arg                [optional]
                                  Http proxy address (fqdn or IP).
  --proxyPort arg                [optional]
                                  Http proxy port.
  --proxyUsername arg            [optional]
                                  Http proxy username.
  --proxyPassword arg            [optional]
                                  Http proxy password.
  --networkDriveUsername arg     [optional]
                                  Username used, when output directory is
                                  accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg     [optional]
                                  Password used, when output directory is
                                  accessed using smb(e.g:\\hostname).
  --excludedProducts arg         [optional]
                                  Disable creating mirror for specified
                                  products. Use --listUpdatableProducts
                                  to see possible values.
  --listUpdatableProducts        Show list of all products which modules
                                  are downloaded by default.
  --repositoryServer arg         [required for repository update]
                                  Repository server for repository
                                  creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                  Files will be downloaded to this
                                  directory to create offline mirror in
                                  output directory.
  --outputRepositoryDirectory arg [required for repository update]
                                  Directory where offline repository will
                                  be created.
  --trustDownloadedFilesInRepositoryTemp [optional]
                                  If set, hashes on already downloaded
                                  files are not checked.
  --mirrorOnlyLevelUpdates       [optional]
                                  If set, only level upgrades will be
                                  downloaded (nano/continuous updates
                                  will not be downloaded)
  --mirrorFileFormat arg        [optional]
                                  Specifies which type of update files
                                  will be downloaded. Possible values
                                  (case insensitive): dll, dat.
  --compatibilityVersion arg     [optional]
                                  Version of compatible products.
  --filterFilePath arg           [optional]
                                  Path to filter file in json format.
                                  Parameter compatibilityVersion has to
                                  be higher than 7.1.0.0 to run program.
  --dryRun arg                   [optional]
                                  Specifies dry run of program with path
                                  to csv file where will be saved list of
                                  products to be downloaded with current
                                  filter configuration.
  --help                         [optional]
                                  Display this help and exit

```



**i** 모든 필터는 대소문자를 구분합니다.

파라미터를 사용하여 저장소 미리 또는 모듈 미리를 생성할 수 있습니다.

#### 저장소 및 모듈 미리 모두에 대한 파라미터


<b>--proxyHost</b>
--proxyPort
--proxyUsername
--proxyPassword
--help

#### 저장소용 파라미터


<b>--repositoryServer</b>
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

#### 모듈용 파라미터

<b>--mirrorType</b>
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

파라미터	설명
--updateServer	Mirror Tool은 엔드포인트 미러에서와는 다른 <a href="#">폴더 구조</a> 를 생성합니다. 각 폴더에는 제품 그룹에 대한 업데이트 파일이 들어 있습니다. <div>  <b>미리를 사용하여 제품의 업데이트 설정에서 <a href="#">업데이트 서버 전체 링크</a>(올바른 폴더에 대한 전체 경로)를 지정해야 합니다.</b> </div>
--offlineLicenseFilename	오프라인 라이선스 파일의 경로를 지정해야 합니다(위에 설명됨).



파라미터	설명
--mirrorOnlyLevelUpdates	인수가 필요하지 않습니다. 설정하면 수준 업데이트만 다운로드됩니다(nano 업데이트는 다운로드되지 않음). <a href="#">지식베이스 문서에서</a> 업데이트 유형에 대해 자세히 알아보십시오.
--mirrorFileFormat	<div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;">  --mirrorFileFormat 파라미터를 사용하기 전, 환경에 이전(6.5 이상) 및 최신(6.6 이상) ESET 보안 제품 버전이 모두 포함되어 있는지 확인합니다. 이 파라미터를 잘못 사용하면 ESET 보안 제품이 잘못 업데이트될 수 있습니다. </div> <p>다운로드할 업데이트 파일 유형을 지정할 수 있습니다. 가능한 값(대소문자 구분):</p> <ul style="list-style-type: none"> <li>• dat - 환경에 ESET 보안 제품 버전 6.5 이상만 있는 경우 이 값을 사용합니다.</li> <li>• dll - 환경에 ESET 보안 제품 버전 6.6 이상만 있는 경우 이 값을 사용합니다.</li> </ul> <p>레거시 제품(ep4, ep5)에 대한 미러를 생성할 때 이 파라미터는 무시됩니다.</p>
--compatibilityVersion	<p>이 선택적 파라미터는 ESET PROTECT 8.1 이상에서 배포되는 미러 도구에 적용됩니다.</p> <p>미러 도구는 x.x 또는 x.x.x.x 형식으로 파라미터 인수에 지정한 ESET PROTECT 저장소 버전과 호환되는 업데이트 파일(예: --compatibilityVersion 10.0 또는 --compatibilityVersion 8.1.13.0)을 다운로드합니다.</p> <p>--compatibilityVersion 파라미터는 미러에서 <a href="#">자동 업데이트(uPCU)</a>를 제외합니다. 사용자 환경에서 자동 업데이트(uPCU)가 필요하고 미러 크기를 줄이고 싶다면, --filterFilePath 파라미터를 사용합니다.</p>

- ESET 저장소에서 다운로드되는 데이터의 양을 줄이려면 ESET PROTECT 9와 함께 배포된 미러 도구의 새 파라미터, --filterFilePath 및 --dryRun을 사용하는 것이 좋습니다.
1. **JSON** 형식으로 필터를 생성합니다(아래의 --filterFilePath 참조).
  2. --dryRun 파라미터(아래 참조)를 사용하여 테스트 미러 도구 실행을 수행하고 필요한 경우 필터를 조정합니다.
  3. --filterFilePath 파라미터 및 정의된 다운로드 필터와 함께 --intermediateRepositoryDirectory 및 --outputRepositoryDirectory 파라미터를 사용하여 미러 도구를 실행합니다.
  4. 미러 도구를 정기적으로 실행하여 항상 최신 설치 관리자를 사용합니다.

파라미터	설명
--filterFilePath	<p>이 선택적 파라미터를 사용하면 미러 도구와 동일한 폴더에 배치된 <b>JSON</b> 형식의 텍스트 파일을 기준으로 ESET 보안 제품을 필터링합니다(예: --filterFilePath filter.txt).</p> <p><b>필터 구성 설명:</b></p> <p>제품 필터링용 구성 파일 형식은 구조가 다음과 같은 <b>JSON</b>입니다.</p> <ul style="list-style-type: none"> <li>루트 <b>JSON</b> 개체: <ul style="list-style-type: none"> <li>use_legacy(부울, 옵션) - true이면 레거시 제품이 포함됩니다.</li> <li>defaults(<b>JSON</b> 개체, 옵션) - 모든 제품에 적용될 필터 속성을 정의합니다. <ul style="list-style-type: none"> <li>languages(목록) - 포함할 언어의 ISO 언어 코드(예: 프랑스어 형식 "fr_FR")를 지정합니다. 기타 언어 코드는 <a href="#">아래 표</a>에 나와 있습니다. 더 많은 언어를 선택하려면 쉼표와 공백으로 구분합니다(예: ("en_US", "zh_TW", "de_DE")).</li> <li>platforms(목록) - 포함할 플랫폼입니다(["x64", "x86", "arm64"]).</li> </ul> </li> </ul> </li> </ul> <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p><b>!</b> platforms 필터를 신중하게 사용하십시오. 예를 들어, 미러 도구가 64비트 설치 관리자만 다운로드하고 인프라에 32비트 컴퓨터가 있는 경우 64비트 ESET 보안 제품은 32비트 컴퓨터에 설치되지 않습니다.</p> </div> <ul style="list-style-type: none"> <li>os_types(목록) - 포함할 OS 유형입니다(["windows"], ["linux"], ["mac"]).</li> <li>oproducts(<b>JSON</b> 개체 목록, 옵션) - 특정 제품에 적용할 필터 - 지정된 제품에 대해 defaults를 재지정합니다. 개체에는 다음과 같은 속성이 있습니다. <ul style="list-style-type: none"> <li>app_id(문자열) - name이 지정되지 않은 경우 필요합니다.</li> <li>name(문자열) - app_id가 지정되지 않은 경우 필요합니다.</li> <li>version(문자열) - 포함할 버전 또는 버전 범위를 지정합니다.</li> <li>languages(목록) - 포함할 언어의 ISO 언어 코드입니다(<a href="#">아래 표</a> 참조).</li> <li>platforms(목록) - 포함할 플랫폼입니다(["x64", "x86", "arm64"]).</li> <li>os_types(목록) - 포함할 OS 유형입니다(["windows"], ["linux"], ["mac"]).</li> </ul> </li> </ul> <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p><b>i</b> 필터에 적합한 값을 확인하려면 시험 실행 모드에서 미러 도구를 실행하고 생성된 CSV 파일에서 관련 제품을 찾습니다.</p> </div> <p><b>버전 문자열 형식 설명</b></p> <p>모든 버전 번호는 점으로 구분된 네 개의 숫자로 구성됩니다(예: 7.1.0.0). 버전 필터를 작성할 때 더 적은 숫자를 지정(예: 7.1)할 수 있으며, 나머지 숫자는 0이 됩니다(7.1은 7.1.0.0과 동일).</p> <p>버전 문자열은 다음의 두 형식 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>[&gt; &lt; &gt;= &lt;= &lt;n&gt;.&lt;n&gt;.&lt;n&gt;.&lt;n&gt;)]</li> </ul> <p>o 지정된 버전보다 큰/작은 또는 같은/작은 또는 같은/같은 버전을 선택합니다.</p> <ul style="list-style-type: none"> <li>&lt;n&gt;.&lt;n&gt;.&lt;n&gt;.&lt;n&gt;)] - &lt;n&gt;.&lt;n&gt;.&lt;n&gt;.&lt;n&gt;)]</li> </ul> <p>o 하한보다 크거나 하한과 같고, 상한보다 작거나 상한과 같은 버전을 선택합니다. 비교는 버전 번호의 각 부분에 대한 숫자(왼쪽에서 오른쪽)로 나타냅니다.</p> <div style="border: 1px solid green; padding: 10px; margin: 10px 0;"> <p><b>JSON 예제</b></p> <pre> {   "use_legacy": true,   "defaults": {     "languages": [ "en_US" ],     "platforms": [ "x64", "x86" ]   },   "products": [     {       "app_id": "com.eset.apps.business.ees.windows",       "version": "7.1.0.0-8.0.0.0"     },     {       "app_id": "com.eset.apps.business.eea.windows",       "version": "&gt;7.1.0.0"     }   ] } </pre> </div> <p>--filterFilePath 파라미터는 이전 미러 도구 버전(ESET PROTECT 8.x에서 릴리스됨)에 사용된 --languageFilterForRepository, --productFilterForRepository, --downloadLegacyForRepository 파라미터를 대체합니다.</p>

파라미터	설명
--dryRun	<p>이 선택적 파라미터를 사용하면 미리 도구는 파일을 다운로드하지 않고 다운로드될 모든 패키지를 나열하는 .csv 파일을 생성합니다.</p> <p>필수 파라미터 --intermediateRepositoryDirectory 및 --outputRepositoryDirectory 없이 이 파라미터를 사용할 수 있습니다(예:)</p> <ul style="list-style-type: none"> <li>Windows: MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv</li> <li>Linux: sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv</li> </ul> <div style="border: 1px solid blue; padding: 5px;"> <p><b>i</b> 일부 ESET 설치 관리자는 언어 일반(multilang 언어 코드 포함)이며 미리 도구는 --filterFilePath에 언어를 지정하더라도 .csv 파일에 해당 설치 관리자를 나열합니다.</p> </div> <p>--dryRun 파라미터와 --intermediateRepositoryDirectory 및 --outputRepositoryDirectory 파라미터도 사용하는 경우 미리 도구는 outputRepositoryDirectory를 지우지 않습니다.</p>
--listUpdatableProducts	<p>(--excludedProducts을 사용하는 경우를 제외하고) Mirror Tool이 모듈 업데이트를 다운로드할 수 있는 모든 ESET 제품을 나열합니다.</p> <p>파라미터는 다음 Mirror Tool 버전으로부터 사용할 수 있습니다: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).</p>

## Mirror Tool 폴더 구조

기본적으로 --updateServer 파라미터를 지정하지 않으면 Mirror Tool은 HTTP 서버에 다음 폴더 구조를 만듭니다.

### HTTP 전용 미리 서버 사용 안 함

**!** 로컬 미리 서버가 HTTP 및 HTTPS 프로토콜을 사용하거나 HTTPS만 사용하는지 확인합니다. 미리 서버가 HTTP만 사용하는 경우 HTTP 서버에서 ESET 보안 제품의 최종 사용자 사용권 계약을 검색할 수 없으므로 소프트웨어 설치 클라이언트 작업을 사용할 수 없습니다.

Mirror Tool 기본 폴더	ESET 보안 제품	서버 업데이트(HTTP 서버 루트 위치에 따름)
mirror/eset_upd/era6	era6 미리 폴더는 다음 ESET 원격 관리 솔루션에 공통되는 사항입니다. ERA 6, ESMC 7 및 ESET PROTECT	미리에서 ESET PROTECT 10을(를) 업데이트하려면 <a href="#">업데이트 서버</a> 를 <code>http://your_server_address/mirror/eset_upd/era6</code> (으)로 설정합니다.
mirror/eset_upd/ep[버전으로 업그레이드]	Windows용 ESET Endpoint Antivirus/Security 버전 6.x(이상) 각 주 버전에는 해당 폴더가 있습니다(예: 10.x 버전의 경우 ep10).	<code>http://your_server_address/mirror/eset_upd/ep10</code> (버전 10.x의 예)
mirror/eset_upd/v5	Windows용 ESET Endpoint Antivirus/Security 버전 5.x	<code>http://your_server_address/mirror/eset_upd/v5</code>

### ESET 보안 제품 Linux/macOS

**!** HTTP 미리에서 Linux/macOS용 ESET 보안 제품을 업데이트하려면 --updateServer 파라미터를 지정하고 추가 폴더를 생성해야 합니다(아래 참조).

--updateServer	추가 Mirror Tool 폴더	ESET 보안 제품	서버 업데이트(HTTP 서버 루트 위치에 따름)
<code>http://update.eset.com/eset_upd/businesslinux</code>	mirror/eset_upd/BusinessLinux	ESET Endpoint Antivirus-용 Linux	<code>http://your_server_address/mirror/eset_upd/BusinessLinux</code>



# 모바일 장치 커넥터 설치 - Windows



ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.



모바일 장치를 해당 위치와 관계없이 항상 관리할 수 있도록 인터넷에서 모바일 장치 커넥터에 접근할 수 있어야 합니다.



ESET PROTECT 서버가 호스팅된 것과는 별도의 호스트 장치에 MDM 구성 요소를 배포하는 것이 좋습니다.

Windows에 ESET PROTECT 서버용 Mobile Device Connector 구성 요소를 설치하려면 다음 단계를 따릅니다.



설치 [필수 구성 요소](#)를 모두 충족하는지 확인합니다.

1. ESET PROTECT [다운로드 섹션](#)으로 이동하여 이 ESET PROTECT 구성 요소용 독립 실행형 설치 관리자를 다운로드합니다. (*mdmcore\_x64.msi*).
2. 모바일 장치 커넥터 설치 관리자를 실행하고 EULA에 동의하는 경우 동의합니다.
3. [찾아보기](#)를 클릭하고 HTTPS를 통한 통신에 사용할 [SSL 인증서](#)의 위치로 이동한 다음 이 인증서의 비밀번호를 입력합니다.
4. **MDM 호스트 이름**: 을 지정합니다. 인터넷에서 모바일 장치가 연결할 수 있는 MDM 서버의 공용 도메인 또는 공용 IP 주소입니다.



MDM 호스트 이름은 **HTTPS 서버 인증서**에 지정한 것과 같은 형식으로 입력해야 합니다. 그렇지 않으면 iOS 모바일 장치가 [MDM 프로파일](#) 설치를 거부합니다. 예를 들어 HTTPS 인증서에 지정된 IP 주소가 있는 경우 **MDM 호스트 이름** 필드에 이 IP 주소를 입력합니다. HTTPS 인증서에 FQDN을 지정한 경우(예: *mdm.mycompany.com*) 이 FQDN을 **MDM 호스트 이름** 필드에 입력합니다. 또한 HTTPS 인증서에 사용한 와일드카드 \*가 있는 경우(예: *\*.mycompany.com*) **MDM 호스트 이름** 필드에 *mdm.mycompany.com*을 사용할 수 있습니다.

5. 이제 설치 관리자가 모바일 장치 커넥터에 사용될 기존 DB에 연결되어야 합니다. 다음 연결 세부 사항을 지정하십시오.

- **DB**: Windows 인증을 통한 MySQL Server/MS SQL Server/MS SQL Server
- **ODBC 드라이버**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 유니코드 드라이버/MySQL ODBC 5.3 유니코드 드라이버/MySQL ODBC 8.0 유니코드 드라이버/SQL Server/SQL Server Native Client 10.0/SQL Server용 ODBC Driver 11/SQL Server용 ODBC Driver 13/SQL Server용 ODBC Driver 17/SQL Server용 ODBC Driver 18
- **DB 이름**: 미리 정의된 이름을 사용하거나, 필요한 경우 이름을 변경하는 것이 좋습니다.
- **호스트 이름**: DB 서버의 호스트 이름 또는 IP 주소
- **포트**: DB 서버에 연결하는 데 사용됩니다.
- **DB 관리자 계정 사용자 이름/비밀번호**
- **명명된 인스턴스 사용** - Microsoft SQL DB를 사용하는 경우 **명명된 인스턴스 사용** 확인란을 선택하

여 사용자 지정 DB 인스턴스를 사용할 수 있습니다. **호스트 이름** 필드에 `HOSTNAME\DB_INSTANCE` 형식으로 설정할 수 있습니다(예: `192.168.0.10\ESMC7SQL`). 클러스터된 DB의 경우 클러스터 이름만 사용합니다. 이 옵션을 선택하면 DB 연결 포트를 변경할 수 없으며, 시스템은 Microsoft에서 결정한 기본 포트를 사용하게 됩니다. ESET PROTECT 서버를 장애 조치(Failover) 클러스터에 설치된 Microsoft SQL DB와 연결하려면, 클러스터 이름을 **호스트 이름** 필드에 입력합니다.

**i** ESET PROTECT DB에 사용하는 것과 동일한 DB 서버를 사용할 수도 있지만 80개보다 많은 모바일 장치를 등록하려는 경우에는 다른 DB 서버를 사용하는 것이 좋습니다.

6. 새로 생성한 모바일 장치 커넥터 DB의 사용자를 지정합니다. **새 사용자 생성** 또는 **기존 DB 사용자 사용**이 가능합니다. DB 사용자의 비밀번호를 입력합니다.

7. **서버 호스트**(ESET PROTECT 서버의 이름 또는 IP 주소) 및 **서버 포트**(기본 포트는 2222임, 다른 포트를 사용하는 경우 기본 포트를 해당 사용자 지정 포트 번호로 바꿈)를 입력합니다.

8. MDM 커넥터를 ESET PROTECT 서버에 연결합니다. ESET PROTECT 서버에 연결하는 데 필요한 **서버 호스트** 및 **서버 포트**를 채우고 **서버 지원 설치** 또는 **오프라인 설치**를 선택하여 계속 진행합니다.

• **서버 지원 설치** - ESET PROTECT 웹 콘솔 관리자 자격 증명을 제공하며, 설치 관리자가 자동으로 필요한 인증서를 다운로드합니다. 서버 지원 설치에 필요한 [권한](#)도 확인합니다.

1. **서버 호스트**(ESET PROTECT 서버의 이름 또는 IP 주소) 및 **웹 콘솔 포트**(사용자 지정 포트를 사용하지 않는 경우 기본 포트 2223을 그대로 둠)를 입력합니다. 또한 웹 콘솔 관리자 계정 자격 증명(**사용자 이름/비밀번호**)을 제공합니다.

2. 인증서를 수락할 것인지 묻으면 **예**를 클릭합니다. 10단계를 계속합니다.

• **오프라인 설치** - ESET PROTECT에서 [내보낼 수 있는](#) **프록시 인증서** 및 **인증 기관**을 제공합니다. 또는 [사용자 지정 인증서](#) 및 해당 인증 기관을 사용할 수도 있습니다.

1. 피어 인증서 옆에 있는 **찾아보기**를 클릭하고 **피어 인증서** 위치(ESET PROTECT에서 내보낸 프록시 인증서)로 이동합니다. 이 인증서에는 비밀번호가 필요하지 않으므로 **인증서 비밀번호** 텍스트 필드를 비워둡니다.

2. 인증 기관에 대해 해당 절차를 반복하고 11단계를 계속 진행합니다.

**i** ESET PROTECT에서 ESET PROTECT 설치 중에 자동으로 생성된 기본 인증서 대신 사용자 지정 인증서를 사용하는 경우 이러한 인증서는 프록시 인증서를 제공하라는 메시지가 표시될 때 사용해야 합니다.


9. 모바일 장치 커넥터의 대상 폴더를 지정하고(기본값을 사용하는 것이 좋음) **다음**을 클릭한 후 **설치**를 클릭합니다.

10. 설치가 완료되면 웹 브라우저 또는 모바일 장치에서 `https://your-mdm-hostname:enrollment-port`(예: `https://mdm.company.com:9980`)를 열어 Mobile Device Connector가 올바르게 실행되는지 확인합니다. 설치에 성공하면 다음과 같은 메시지가 표시됩니다. MDM 서버가 시작되어 실행 중입니다.

11. 이제 [ESET PROTECT에서 MDM을 활성화](#)할 수 있습니다.




# 모바일 장치 커넥터 필수 구성 요소

 MDM 서버의 포트 또는 호스트 이름이 변경되면 모든 모바일 장치를 다시 등록해야 합니다. 이러한 이유로 MDM 서버에 전용 호스트 이름을 설정하는 것이 좋습니다. 따라서 MDM 서버의 호스트 장치를 변경해야 하는 경우 새 호스트 장치의 IP 주소를 DNS 설정의 MDM 호스트 이름에 다시 할당하여 변경할 수 있습니다.

Windows에서 모바일 장치 커넥터를 설치하려면 다음 필수 구성 요소가 충족되어야 합니다.

- 인터넷에서 접근할 수 있는 공용 IP 주소/호스트 이름 또는 공용 도메인


 MDM 서버의 호스트 이름을 변경해야 할 경우 MDC 구성 요소의 복구 설치를 실행해야 합니다. MDM 서버의 호스트 이름을 변경할 경우 MDM이 계속 제대로 작동하도록 하기 위해 이 새 호스트 이름을 포함하는 새 **HTTPS 서버 인증서**를 가져와야 합니다.

- 포트가 열려 있고 사용 가능해야 함 - [전체 포트 목록은 여기](#)를 참조하십시오. 기본 포트 번호 9981 및 9980을 사용하는 것이 좋지만, 필요한 경우 MDM 서버의 구성 파일에서 이를 변경할 수도 있습니다. 지정된 포트를 통해 모바일 장치가 연결할 수 있는지 확인합니다. 이러한 연결이 가능하도록 방화벽 및/또는 네트워크 설정(해당되는 경우)을 변경합니다. [MDM 아키텍처](#)에 대한 자세한 내용을 읽어 보십시오.
- 방화벽 설정 - 평가 목적으로 Windows 7 등 서버 이외의 OS에 모바일 장치 커넥터를 설치하는 경우 [방화벽 규칙](#)을 만들어 다음에 대해 통신 포트를 허용해야 합니다.

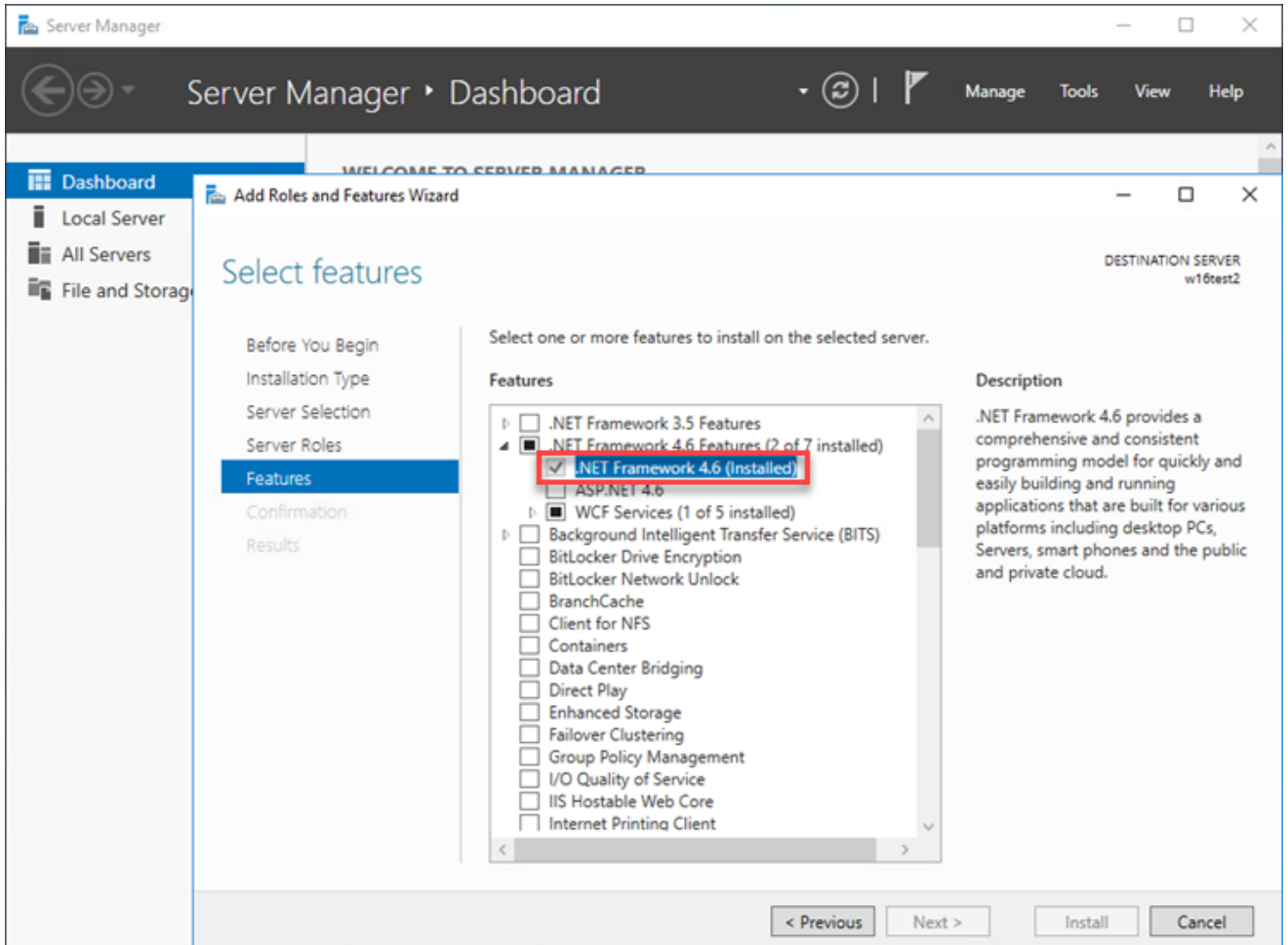
C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP 포트 9980

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP 포트 9981

C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP 포트 2222

 실제 .exe 파일 경로는 클라이언트 OS 시스템에 각 ESET PROTECT 구성 요소가 설치된 위치에 따라 다를 수 있습니다.

- 이미 설치 및 구성된 DB 서버. [Microsoft SQL](#) 또는 [MySQL](#) 요구 사항을 충족하는지 확인합니다.
- MDM 커넥터의 RAM 사용은 동시에 실행되는 "ESET PROTECT MDMCore 모듈" 프로세스 수가 최대 48개가 될 수 있도록 최적화되고, 사용자가 더 많은 장치를 연결할 경우 프로세스는 현재 리소스를 사용하여 하는 각 장치를 주기적으로 변경합니다.
- Microsoft SQL Server Express를 설치하려면 Microsoft .NET Framework 4가 필요합니다. **역할 및 기능 추가 마법사**를 사용하여 설치할 수 있습니다.



## 인증서 요구 사항

- HTTPS를 통한 보안 통신을 위해서는 **.pfx**형식의 **SSL 인증서**가 필요합니다. 타사 인증 기관에서 제공한 인증서를 사용하는 것이 좋습니다. 일부 모바일 장치에서는 사용자가 자체 서명한 인증서를 수락할 수 없으므로, 자체 서명한 인증서(ESET PROTECT CA에서 서명한 인증서 포함)는 권장되지 않습니다.
- CA에서 서명한 인증서 및 해당 개인 키가 있어야 하며, 표준 절차를 사용하여(기존에는 OpenSSL을 사용했음) 이를 다음과 같은 하나의 **.pfx** 파일로 병합합니다.  

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx
```

 SSL 인증서를 사용하는 대부분의 서버에서는 이 절차가 표준 절차입니다.
- **오프라인 설치**의 경우 피어 인증서(ESET PROTECT에서 **내보낸 에이전트 인증서**)도 필요합니다. 또는 ESET PROTECT에 **사용자 지정 인증서**를 사용할 수도 있습니다.

## 모바일 장치 커넥터 활성화

모바일 장치 커넥터를 설치했으면 ESET 끝점, 기업용 또는 사무용 라이선스로 이 커넥터를 활성화해야 합니다.

1. **ESET 엔드포인트, 기업용 또는 사무용 라이선스**를 ESET PROTECT 라이선스 관리에 추가합니다.
2. **제품 활성화** 클라이언트 작업을 사용하여 Mobile Device Connector를 활성화합니다. 이 절차는 클라



이언트 컴퓨터에서 모든 ESET 제품을 활성화할 때의 절차와 같습니다. 이 경우 모바일 장치 커넥터가 클라이언트 컴퓨터입니다.

## MDM iOS 라이선스 기능

ESET는 Apple App Store에서 애플리케이션을 제공하지 않으므로 ESET 모바일 장치 커넥터는 iOS 장치에 대한 모든 라이선스 정보를 저장합니다.

라이선스는 장치 단위로 적용되며 [제품 활성화 작업](#)(Android와 동일)을 사용하여 활성화할 수 있습니다.

iOS 라이선스는 다음과 같은 방법으로 비활성화할 수 있습니다.

- 관리 중단 작업을 통해 관리에서 장치 제거
- **DB 제거** 옵션을 통해 MDC 제거 수행
- 다른 방법으로 비활성화(ESET PROTECT 또는 [EBA 비활성화](#))

MDC는 iOS 장치 대신 ESET 라이선스 서버와 통신하므로 EBA 포털은 MDC의 상태를 반영하고 개별 장치의 상태는 반영하지 않습니다. 현재 장치 정보는 항상 ESET PROTECT 웹 콘솔에서 제공됩니다.

활성화되지 않은 장치나 라이선스가 만료된 장치에는 빨간색 보호 상태 및 "제품이 활성화되지 않음" 메시지가 표시됩니다. 이러한 장치는 작업 처리, 정책 설정 및 중요하지 않은 로그 제공을 거부합니다.

MDM 제거 중에 **DB 제거 안 함**을 선택한 경우 사용된 라이선스가 비활성화되지 않습니다. 이러한 라이선스는 MDM을 이 DB에 다시 설치하거나, ESET PROTECT 또는 [ESET 비활성화](#)를 통해 제거할 수 있습니다. 다른 MDM 서버로 이동할 때 [제품 활성화 작업을 다시](#) 수행해야 합니다.

## HTTPS 인증서 요구 사항

ESET 모바일 장치 커넥터에 모바일 장치를 등록하려면 HTTPS 서버가 전체 인증서 체인을 반환하는지 확인하십시오.

인증서가 제대로 작동하려면 이러한 요구 사항을 충족해야 합니다.

- HTTPS 인증서(pkcs#12/pfx 컨테이너)에 루트 CA를 포함하는 전체 인증서 체인이 있어야 합니다.
- 필수 기간 중에는 인증서가 유효해야 합니다(유효 기간 시작/유효 기간 종료).
- **CommonName** 또는 **subjectAltNames**는 MDM 호스트 이름과 일치해야 합니다.

예를 들어 **MDM 호스트 이름**이 hostname.mdm.domain.com이면 인증서에 다음과 같은 이름이 포함될 수 있습니다.

- hostname.mdm.domain.com
- \*.mdm.domain.com

**i** 하지만 다음과 같은 이름은 포함될 수 없습니다.

- \*
- \*.com
- \*.domain.com

기본적으로 "\*"가 "점"을 대체할 수 없습니다. iOS가 MDM에 대한 인증서를 수락하는 방법에 대해 이 동작이 확인됩니다.

**i** 인증서 유효성을 확인할 때 현재 표준 시간대를 고려하는 장치도 있고 그렇지 않은 장치도 있습니다. 현재 날짜 하루 또는 이틀 전에 인증서 유효성을 부여하여 문제 발생을 방지하십시오.

## 오프라인 저장소 - Windows

미러 도구를 사용하여 오프라인 저장소를 생성할 수 있습니다(Windows에서). 오프라인 저장소는 보통 인터넷 접근이 제한된 네트워크나 폐쇄 컴퓨터 네트워크에 필요합니다. 미러 도구를 사용하여 로컬 폴더에서 ESET 저장소의 복제본을 만들 수 있습니다. 복제된 이 저장소를 나중에 폐쇄된 네트워크의 특정 위치에 이동할 수 있으며(예: 외부 디스크), 로컬 네트워크의 안전한 위치로 복사한 후 HTTP 서버를 통해 사용할 수 있도록 설정할 수도 있습니다.

오프라인 저장소를 업데이트하려면 오프라인 저장소 생성에 사용된 것과 동일한 파라미터로 동일한 명령을 실행합니다. 중간 폴더의 이전 데이터가 사용되며 오래된 파일만 다운로드됩니다.

**!** 저장소의 크기는 증대되며 중간 디렉터리는 저장소와 동일한 크기가 됩니다. 이 절차를 시작하려면 사용 가능한 공간이 **1.2TB** 이상 있어야 합니다.

### 모범 사례

ESET 지식베이스 문서 [오프라인 환경에서 ESET PROTECT을\(를\) 사용하기 위한 모범 사례](#)도 참조하십시오.

## Windows용 예 시나리오

### I. 저장소 복제본 만들기

1. 미러 도구를 [다운로드](#)합니다.
2. 다운로드된 .zip 파일에서 미러 도구의 압축을 해제합니다.
3. 다음에 대해 폴더를 준비(생성)합니다.
  - 중간 파일
  - 최종 저장소
4. 명령 프롬프트를 열고 미러 도구의 압축이 해제된 폴더로 디렉터리를 변경합니다(cd 명령).
5. 다음 명령을 실행합니다(중간 및 출력 저장소 디렉터리를 3단계의 폴더로 변경).

```
MirrorTool.exe --repositoryServer AUTOSELECT ^  
--intermediateRepositoryDirectory C:\Intermediary ^  
--outputRepositoryDirectory C:\Repository
```

6. 저장소가 outputRepositoryDirectory 폴더에 복사되면 폴더 및 해당 내용을 폐쇄된 네트워크에서 접근 가능한 다른 컴퓨터로 이동합니다.

## II. HTTP 서버 설정

7. 폐쇄 네트워크의 컴퓨터에서 HTTP 서버가 실행되고 있어야 합니다. 다음 중 하나를 사용할 수 있습니다.

- ESET [다운로드 사이트](#)의 Apache HTTP Proxy(이 시나리오)
- 다른 HTTP 서버

8. *apachehttp.zip*을 열고 *C:\Program Files\Apache HTTP Proxy*에서 파일의 압축을 해제합니다.

9. 관리 명령 프롬프트를 열고 디렉터리를 *C:\Program Files\Apache HTTP Proxy\bin*으로 변경합니다(cd 명령).

10. 다음 명령을 실행합니다.

```
httpd.exe -k install -n ApacheHttpProxy
```

11. 간편한 텍스트 편집기를 사용하여 *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf* 파일을 열고 파일 끝 부분에 다음 줄을 추가합니다.

```
Listen 80  
ServerRoot "C:\Program Files\Apache HTTP Proxy"  
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"  
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">  
Options Indexes FollowSymLinks  
AllowOverride None  
Require all granted  
</Directory>  
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

12. 다음 명령을 사용하여 **ApacheHttpProxy** 서비스를 시작합니다.

```
sc start ApacheHttpProxy
```

13. 웹 브라우저에서 *http://YourIpAddress:80/index.html*을 열어 이 서비스가 실행 중인지 여부를 테스트합니다(*YourIpAddress*를 컴퓨터의 IP 주소로 바꿈).

## III. 오프라인 저장소 실행

14. 오프라인 저장소의 새 폴더를 만듭니다(예: *C:\Repository*).

15. `httpd.conf` 파일에서

```
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"  
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
```

위의 줄을 아래와 같이 저장소 폴더의 주소로 바꿉니다.

```
DocumentRoot "C:\Repository"  
<Directory "C:\Repository">
```

16. 다운로드된 저장소를 `C:\Repository`에 복사합니다.

17. 다음 명령을 사용하여 **ApacheHttpProxy** 서비스를 다시 시작합니다.

```
sc restart ApacheHttpProxy
```

18. 이제 오프라인 저장소가 `http://YourIpAddress` 주소에서 실행 중입니다(예: `http://10.1.1.10`).

19. ESET PROTECT 웹 콘솔을 사용하여 새 저장소 주소를 설정합니다.

a. [ESET PROTECT 서버](#) - 자세히 > 설정 > 고급 설정 > 저장소를 클릭하고 서버 필드에 오프라인 저장소 주소를 입력합니다.

b. [ESET Management 에이전트](#) - 정책을 클릭한 후 에이전트 정책 > 편집 > 설정 > 고급 설정 > 저장소를 클릭하고, 서버 필드에 오프라인 저장소 주소를 입력합니다.

c. ESET Endpoint 제품(Windows용) - 정책을 클릭한 후 **Windows용 ESET Endpoint** 정책 > 편집 > 설정 > 업데이트 > 프로필 > 업데이트 > 모듈 업데이트를 클릭하고, 자동으로 선택을 선택 취소한 다음 사용자 지정 서버 필드에 오프라인 저장소 주소를 입력합니다.

## 장애 조치(Failover) 클러스터 - Windows

장애 조치(Failover) 클러스터 환경에 ESET PROTECT를 설치하는 데 필요한 대략적인 단계는 다음과 같습니다.

**i** ESET PROTECT 서버의 클러스터 설치에 대해 이 [지식 베이스 문서](#)도 참조하십시오.

1. 공유 디스크가 있는 장애 조치(Failover) 클러스터를 만듭니다.

- [Windows Server 2016 및 2019에서 장애 조치\(Failover\) 클러스터를 만드는 지침](#)
- [Windows Server 2012 및 2012 R2에서 장애 조치\(Failover\) 클러스터를 만드는 지침](#)

2. 클러스터 만들기 마법사에서 원하는 호스트 이름(호스트 이름 구성) 및 IP 주소를 입력합니다.

3. 노드1에서 클러스터의 공유 디스크를 온라인 상태로 전환하고 이 공유 디스크에 [독립 실행형 설치 관리자를 사용하여 ESET PROTECT 서버를 설치](#)합니다. 설치 중에 클러스터 설치임을 선택하고 애플리케이션 데이터 저장소로 공유 디스크를 선택했는지 확인합니다. 호스트 이름을 구성하고 미리 채워진 호스트 이름 옆에 있는 ESET PROTECT Server의 서버 인증서에 대한 호스트 이름으로 입력합니다. 이 호스트 이름을 기억했다가 클러스터 관리자에서 ESET PROTECT 서버 역할을 만들 때 6단계에서 사용하십시오.

4. node1에서 ESET PROTECT Server를 중지하고 node2에서 클러스터 공유 디스크를 온라인 상태로 전환한 후 [독립 실행형 설치 관리자를 사용하여 ESET PROTECT 서버를 설치](#)합니다. 설치 중에 **클러스터 설치**임을 선택했는지 확인합니다. 애플리케이션 데이터 저장소로 공유 디스크를 선택합니다. DB 연결 및 인증서 정보는 노드1에서 ESET PROTECT Server 설치 중에 구성되었으므로 그대로 둡니다.

5. ESET PROTECT Server가 사용하는 모든 [포트](#)에서 들어오는 연결을 허용하도록 방화벽을 구성합니다.

6. 클러스터 구성 관리자에서 ESET PROTECT 서버 서비스에 대한 역할을 만들고 시작합니다(**역할 구성 > 역할 선택 > 일반 서버**). 사용 가능한 서비스 목록에서 **ESET PROTECT 서버** 서비스를 선택합니다. 역할에 대해 동일한 호스트 이름을 사용하는 것이 매우 중요한데, 이 호스트 이름이 서버 인증서와 관련하여 3단계에서 사용되었기 때문입니다.

7. 독립 실행형 설치 관리자를 사용하여 모든 클러스터 노드에 ESET Management 에이전트를 설치합니다. **에이전트 구성 및 ESET PROTECT 서버에 연결** 화면에서 6단계에서 사용한 호스트 이름을 사용합니다. 에이전트 데이터를 로컬 노드(클러스터 디스크 아님)에 저장합니다.

8. 웹 서버(Apache Tomcat)는 클러스터에서 지원되지 않으므로, 클러스터되지 않은 디스크나 다른 컴퓨터에 설치해야 합니다.

a. 별도의 컴퓨터에 [웹 콘솔을 설치](#)하고 ESET PROTECT 서버 클러스터 역할에 연결하도록 올바르게 구성합니다.

b. 웹 콘솔이 설치된 후 다음에서 해당 구성 파일을 찾습니다. `C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`

c. 메모장 또는 기타 간단한 텍스트 편집기에서 파일을 엽니다. `server_address=localhost` 줄에서 localhost를 ESET PROTECT 서버 클러스터 역할의 IP 주소 또는 호스트 이름으로 바꿉니다.

## Linux의 구성 요소 설치

대부분의 설치 시나리오에서는 여러 다른 네트워크 아키텍처를 수용하거나, 성능 요구를 충족하거나, 기타 이유로 인해 컴퓨터마다 다른 ESET PROTECT 구성 요소를 설치해야 합니다.

[단계별 ESET PROTECT 설치](#) 지침을 따릅니다.

### 핵심 구성 요소 설치

- [ESET PROTECT 서버](#)
- [ESET PROTECT 웹 콘솔](#) - ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다.
- [ESET Management 에이전트](#)
- [데이터베이스](#) 서버

### 옵션 구성 요소 설치

- [RD Sensor](#)

- [모바일 장치 커넥터](#)
- [ESET Bridge HTTP 프록시](#)
- [미러 도구](#)

Linux용 ESET PROTECT를 최신 버전으로 업그레이드하려면 [구성 요소 업그레이드 작업](#) 장 또는 ESET의 [지식 베이스 문서](#)를 참조하십시오.

## Linux에 단계별 ESET PROTECT 설치

이 설치 시나리오에서는 ESET PROTECT 서버 및 ESET PROTECT 웹 콘솔의 단계별 설치를 시뮬레이트합니다. MySQL을 사용하여 설치를 시뮬레이트합니다.

### 선택한 Linux 배포에 대한 설치 지침

배포별 지침이 포함된 당사 지식베이스 문서를 따를 수 있습니다.



- [CentOS 7](#)
- [Debian 10](#)
- [SUSE Linux Enterprise Server\(SLES\)](#)

## 설치 전

1. 네트워크에 [DB 서버](#)가 있는지 확인하고 로컬/원격 서버에서 이 서버에 접근할 수 있는지 확인합니다. DB 서버가 설치되어 있지 않은 경우 새 DB 서버를 [설치하고 구성합니다](#).
2. ESET PROTECT Linux 독립 실행형 구성 요소(에이전트, 서버, 웹 콘솔)를 다운로드합니다. ESET 웹 사이트에서 제공되는 [ESET PROTECT 독립 실행형 설치 관리자](#) 범주에서 이러한 설치 파일을 찾을 수 있습니다.

## 설치 프로세스

sudo 명령을 사용하거나 root 권한으로 설치하여 설치를 완료할 수 있어야 합니다.

1. ESET PROTECT 서버에 [필요한 패키지](#)를 설치합니다.
2. [MySQL 구성](#) 항목에 설명된 것처럼 MySQL Server에 대한 연결을 구성합니다.
3. MySQL ODBC 드라이버의 구성 확인. 자세한 내용은 [ODBC 설치 및 구성](#)을 참조하십시오.
4. 설치 파라미터를 사용자 지정하고 ESET PROTECT 서버 설치를 실행합니다. 자세한 내용은 [서버 설치 - Linux](#)를 참조하십시오.
5. 필요한 Java 및 Tomcat 패키지를 설치하고 [ESET PROTECT Web Console을 설치](#)합니다. ESET PROTECT Web Console에 대한 HTTPS 연결에 문제가 있는 경우 [HTTPS/SSL 연결 설정](#)을 참조하십시오.
6. 서버 컴퓨터에 [ESET Management 에이전트를 설치](#)합니다.

명령줄 기록에서 중요한 데이터(예: 패스워드)가 포함된 명령을 제거하는 것이 좋습니다.



- 1.history를 실행하여 기록에서 모든 명령 목록을 확인합니다.
- 2.history -d line\_number를 실행합니다(명령의 줄 수 지정). 또는 history -c를 실행하여 전체 명령줄 기록을 제거합니다.

# MySQL 설치 및 구성

## 설치

**!** 지원되는 버전의 [MySQL Server](#) 및 [ODBC 커넥터](#)를 설치해야 합니다.

이미 MySQL을 설치하고 구성한 경우 [구성](#)을 진행합니다.

### 1. MySQL 저장소 추가:

<b>Debian, Ubuntu</b>	터미널에서 다음 명령 실행: a) <code>wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb</code> b) <code>sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb</code> 패키지 설치 중에 설치할 구성 요소의 버전을 선택할 수 있습니다. 기본 옵션을 선택하는 것이 좋습니다. <a href="#">MySQL APT 저장소 추가</a> 도 참조하십시오.
<b>CentOS, Red Hat</b>	<a href="#">MySQL Yum 저장소 추가</a>
<b>SUSE Linux Enterprise Server</b>	<a href="#">MySQL SLES 저장소 추가</a>

### 2. 로컬 저장소 캐시 업데이트:

<b>Debian, Ubuntu</b>	<code>sudo apt-get update</code>
<b>CentOS, Red Hat</b>	<code>sudo yum update</code>
<b>SUSE Linux Enterprise Server</b>	<code>sudo zypper update</code>

### 3. MySQL 설치에 사용된 Linux 배포 및 버전에 따라 다릅니다.

Linux 배포:	MySQL 서버 설치 명령:	MySQL 서버 고급 설치:
<b>Debian, Ubuntu</b>	<code>sudo apt-get install mysql-server</code>	<a href="#">Installing MySQL from Source with the MySQL APT Repository</a>
<b>CentOS, Red Hat</b>	<code>sudo yum install mysql-community-server</code>	<a href="#">Installing MySQL on Linux Using the MySQL Yum Repository</a>
<b>SUSE Linux Enterprise Server</b>	<code>sudo zypper install mysql-community-server</code>	<a href="#">Steps for a Fresh Installation of MySQL</a>

수동으로 설치하려면 [MySQL 커뮤니티 서버를 다운로드](#)하십시오.

## 구성

### 1. 텍스트 편집기에서 `my.cnf` 구성 파일을 엽니다.

```
sudo nano /etc/my.cnf
```

파일이 없으면 `/etc/mysql/my.cnf` 또는 `/etc/my.cnf.d/community-mysql-server.cnf` 또는 `/etc/mysql/mysql.conf.d/mysqld.cnf`를 시도하십시오.



2. my.cnf 파일의 `[mysqld]` 섹션에서 다음 구성을 찾아서 값을 수정합니다.

- 파일에 없는 경우 `[mysqld]` 섹션을 생성합니다.
- 파일에 파라미터가 없는 경우 `[mysqld]` 섹션에 추가합니다.
- MySQL 버전을 확인하려면 `mysql --version` 명령을 실행합니다.

파라미터	설명 및 권장 값	MySQL 버전으로 업그레이드
<code>max_allowed_packet=33M</code>		모든 <a href="#">지원되는 버전</a> .
<code>log_bin_trust_function_creators=1</code>	또는 <code>log_bin=0</code> 이진 로깅을 비활성화할 수 있습니다.	<a href="#">지원되는 8.x 버전</a>
<code>innodb_log_file_size=100M</code> <code>innodb_log_files_in_group=2</code>	이러한 두 파라미터 값의 곱셈은 <b>200</b> 이상이어야 합니다. <code>innodb_log_files_in_group</code> 의 최솟값은 <b>2</b> 이고 최댓값은 <b>100</b> ;이며, 이 값도 정수여야 합니다.	<a href="#">지원되는 8x 버전</a> 5.7 5.6.22 (이상 5.6.x)
<code>innodb_log_file_size=200M</code>	값을 <b>200M</b> 이상, <b>3000M</b> 이하로 설정합니다.	5.6.20 및 5.6.21

3. **CTRL + X**를 누르고 **Y**를 입력하여 변경 내용을 저장한 후 파일을 닫습니다.

4. MySQL 서버를 다시 시작하고 구성을 적용합니다(경우에 따라 서비스 이름이 `mysqld`임).

```
sudo systemctl restart mysql
```

5. MySQL 권한과 패스워드를 설정합니다(이 단계는 선택 사항이며, 일부 Linux 배포에서 작동하지 않을 수 있음).

a)임시 MySQL 패스워드 공개: `sudo grep 'temporary password' /var/log/mysql/mysql.log`

b)패스워드를 복사 및 저장합니다.

c)다음 옵션 중 하나를 수행하여 새 패스워드를 설정합니다.

- `/usr/bin/mysql_secure_installation`을 실행하고 임시 패스워드를 입력합니다. 그러면 새 패스워드를 생성하라는 메시지가 표시됩니다.

- `mysql -u root -p`를 실행하고 임시 패스워드를 입력합니다. `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';`을 실행하여 루트 패스워드를 변경(`strong_new_password`를 사용자 패스워드로 바꾸기)하고 `Quit`를 입력합니다.

MySQL 참조 설명서에서 [MySQL 설치 보안 기능 향상](#)도 참조하십시오.

6. MySQL 서버 서비스가 실행 중인지 확인합니다.

```
sudo systemctl status mysql
```

## ODBC 설치 및 구성

**!** 지원되는 버전의 [MySQL Server](#) 및 [ODBC 커넥터](#)를 설치해야 합니다.



**i** Microsoft ODBC 드라이버(버전 13 이상)를 설치하면 Linux의 ESET PROTECT 서버를 Windows의 Microsoft SQL Server에 연결할 수 있습니다. 자세한 내용을 보려면 [이 지식베이스 문서](#)를 방문하십시오.

터미널을 사용하여 MySQL ODBC 드라이버를 설치합니다. Linux 배포 단계를 따릅니다.

- [Debian, Ubuntu](#)
- [CentOS 7](#)
- [기타 지원되는 Linux 배포판](#)

## Debian, Ubuntu

### 1. unixODBC 드라이버 설치:

```
sudo apt-get install unixodbc
```

### 2. ODBC 커넥터 다운로드:

Ubuntu 16	wget <a href="https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz">https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz</a>
Ubuntu 18	wget <a href="https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz">https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz</a>
Ubuntu 20	wget <a href="https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz">https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz</a>
Debian 10	wget <a href="https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz">https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz</a>

- Linux 배포 및 버전과 호환되는 버전을 선택하고 다운로드해야 합니다.
- [공식 MySQL 사이트](#)에서 MySQL용 ODBC 커넥터를 다운로드할 수 있습니다.

### 3. ODBC 드라이버 압축 파일의 압축 풀기(사용된 링크에 따라 패키지 이름이 변경됨):

```
gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
```

### 4. ODBC 드라이버 추출(사용된 링크에 따라 패키지 이름이 변경됨):

```
tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar
```

### 5. ODBC 드라이버 폴더로 이동(사용된 링크에 따라 패키지 이름이 변경됨):

```
cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit
```

### 6. ODBC 드라이버 파일 복사:

```
sudo cp bin/* /usr/local/bin
```

```
sudo cp lib/* /usr/local/lib
```

### 7. ODBC에 드라이버를 등록합니다.

- Ubuntu 20.x 같은 새로운 Linux 버전에서는 유니코드 드라이버를 사용하는 것이 좋습니다.

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t  
"Driver=/usr/local/lib/libmyodbc8w.so"
```

- 다른 시스템의 경우 또는 유니코드 드라이버가 작동하지 않는 경우 이 명령을 사용합니다.

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t  
"Driver=/usr/local/lib/libmyodbc8a.so"
```

#### 8. 설치된 드라이버 나열:

```
sudo myodbc-installer -d -l
```

자세한 내용은

<https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html>을 참조하십시오.

## CentOS 7

#### 1. unixODBC 드라이버 설치:

```
sudo yum install unixODBC -y
```

#### 2. ODBC 커넥터 다운로드:

```
wget  
https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-1.e  
17.x86_64.rpm
```



- YUM을 사용하여 ODBC 커넥터를 설치하지 마십시오. 호환되지 않는 최신 버전이 설치됩니다.
- Linux 배포 및 버전과 호환되는 버전을 선택하고 다운로드해야 합니다.
- [공식 MySQL 사이트](#)에서 MySQL용 ODBC 커넥터를 다운로드할 수 있습니다.

#### 3. ODBC 드라이버 설치:

```
sudo rpm -ivh mysql-connector-odbc-8.0.17-1.e17.x86_64.rpm --nodeps
```

#### 4. ODBC 드라이버 설정:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0.17" -t  
"Driver=/usr/lib64/libmyodbc8w.so"
```

#### 5. 설치된 드라이버 나열:

```
sudo myodbc-installer -d -l
```

## 기타 지원되는 Linux 배포판



- Linux 배포 및 버전과 호환되는 버전을 선택하고 다운로드해야 합니다.
- [공식 MySQL 사이트](#)에서 MySQL용 ODBC 커넥터를 다운로드할 수 있습니다.

#### 1. ODBC 드라이버를 설치하려면 다음 지침을 따릅니다.

- **SUSE Linux Enterprise Server:** `sudo zypper install unixODBC`.

<https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html>도 참조

- [이진 Tarball 배포에서 커넥터/ODBC 설치](#)

2. 다음 명령을 실행하여 텍스트 편집기에서 *odbcinst.ini* 파일을 엽니다.

```
sudo nano /etc/odbcinst.ini
```

또는 `sudo nano/etc/unixODBC/odbcinst.ini`

3. 다음 구성을 *odbcinst.ini* 파일에 복사한 다음(Driver 및 Setup 경로가 올바른지 확인) 파일을 저장하고 닫습니다.

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

일부 배포의 경우 Driver가 다른 위치에 있을 수 있습니다. 다음 명령을 사용하여 해당 파일을 찾을 수 있습니다.

```
sudo find /usr -iname "*libmyodbc*"
```

4. 다음 명령을 실행하여 현재 호스트의 DB 서버에 대한 ODBC 접근을 제어하는 구성 파일을 업데이트합니다.

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

또는 `sudo odbcinst -i -d -f /etc/unixODBC/odbcinst.ini`

## 서버 설치 - Linux

### 선택한 Linux 배포에 대한 설치 지침

배포별 지침이 포함된 당사 지식베이스 문서를 따를 수 있습니다.



- [CentOS 7](#)
- [Debian 10](#)
- [SUSE Linux Enterprise Server\(SLES\)](#)

## 설치

터미널 명령을 사용하여 Linux에 ESET PROTECT 서버 구성 요소를 설치하려면 다음 단계를 따릅니다.

**!** 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

1. 다음과 같이 ESET PROTECT Server 구성 요소를 다운로드합니다.

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server-linux-x86_64.sh
```

2. 다운로드한 파일을 실행 가능하게 합니다.

```
chmod +x server-linux-x86_64.sh
```

3. 설치 스크립트를 준비한 다음 `sudo`를 사용하여 실행할 수 있습니다.

아래 예에 따라 설치 스크립트를 실행합니다(전체 명령을 터미널에 복사할 수 있도록 새 줄은 "\"로 분리 됨).

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-hostname=localhost \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

다음 특성을 수정할 수 있습니다.

특성	설명	필수
--uninstall	제품을 <a href="#">제거</a> 합니다.	-
--keep-database	<a href="#">제거</a> 작업 동안 DB는 제거되지 않습니다.	-
--locale	설치된 서버의 로컬 식별자(LCID)(기본값:en_US). 사용 가능한 옵션에 대해서는 <a href="#">지원되는 언어</a> 를 참조하십시오. <div><b>i</b> --locale을 지정하지 않으면 ESET PROTECT 서버가 영어로 설치됩니다. ESET PROTECT 각 ESET PROTECT 웹 콘솔 세션의 언어를 설정할 수 있습니다. 웹 콘솔의 일부 요소는 언어를 바꿔도 변경되지 않습니다. 일부 요소(기본 대시보드, 정책, 작업 등)는 ESET PROTECT 설치 중에 생성되며 해당 언어를 변경할 수 없습니다.</div>	예
--skip-license	설치에서 사용권 계약 확인을 요구하는 메시지는 표시되지 않습니다.	-
--skip-cert	인증서 생성을 건너뜁니다(--server-cert-path 파라미터와 함께 사용).	-
--license-key	ESET 라이선스 키. 나중에 라이선스 키를 제공할 수 있습니다.	-
--server-port	ESET PROTECT 서버 포트(기본값: 2222).	-
--console-port	ESET PROTECT 콘솔 포트(기본값: 2223)	-
--server-root-password	"Administrator" 사용자의 웹 콘솔 로그인 비밀번호(8자 이상이어야 함).	예
--db-type	사용할 DB 유형(가능한 값: "MySQL Server", "MS SQL Server") <a href="#">Linux에서 Microsoft SQL Server</a> 는 지원되지 않습니다. 그러나 <a href="#">Linux의 ESET PROTECT 서버를 Windows의 Microsoft SQL Server에 연결</a> 할 수 있습니다.	-
--db-driver	<code>odbcinst.ini</code> 파일에 지정된 데이터베이스 연결에 사용되는 ODBC 드라이버( <code>odbcinst -q -d</code> 명령은 사용 가능한 드라이버 목록을 제공하며, --db-driver="MySQL ODBC 8.0 Driver", --db-driver="MySQL ODBC 8.0 Unicode Driver" 또는 --db-driver="MySQL ODBC 8.0.17" 등의 드라이버 중 하나를 사용함)입니다.	예

특성	설명	필수
--db-hostname	DB 서버의 컴퓨터 이름 또는 IP 주소 명명된 DB 인스턴스는 지원되지 않습니다.	예
--db-port	DB 서버의 포트(기본값: 3306)	예
--db-name	ESET PROTECT 서버 DB의 이름(기본값: era_db)	-
--db-admin-username	DB 관리자 사용자 이름(설치에서 DB 생성 및 수정에 사용). --db-user-username 및 --db-user-password에서 정의한 이전에 생성된 DB 사용자가 있는 경우 이 파라미터를 생략할 수 있습니다.	예
--db-admin-password	DB 관리자 비밀번호. --db-user-username 및 --db-user-password에서 정의한 이전에 생성된 DB 사용자가 있는 경우 이 파라미터를 생략할 수 있습니다.	예
--db-user-username	DB ESET PROTECT 서버 사용자 이름(ESET PROTECT 서버에서 DB에 연결하는 데 사용)으로, 16자 이하여야 합니다.	예
--db-user-password	DB ESET PROTECT 서버 사용자 비밀번호	예
--cert-hostname	가능한 ESET PROTECT 서버 컴퓨터의 이름 및/또는 IP를 모두 포함합니다. 서버에 연결하려고 하는 에이전트 인증서에 지정된 서버 이름과 일치해야 합니다.	예
--server-cert-path	서버 피어 인증서의 경로(--skip-cert도 함께 지정한 경우에 이 옵션 사용)	-
--server-cert-password	서버 피어 인증서의 비밀번호	-
--agent-cert-password	에이전트 피어 인증서의 비밀번호	-
--cert-auth-password	인증 기관 비밀번호	-
--cert-auth-path	서버 인증 기관 파일의 경로	-
--cert-auth-common-name	인증 기관 공용 이름(" " 사용)	-
--cert-organizational-unit	-	-
--cert-organization	-	-
--cert-locality	-	-
--cert-state	-	-
--cert-country	-	-
--cert-validity	인증서 유효성(일 또는 연 단위)(인수 --cert-validity-unit에 지정)	-
--cert-validity-unit	인증서 유효성의 단위로 가능한 값은 '연도' 또는 '일'(기본값: Years)	-
--ad-server	Active Directory 서버	-
--ad-user-name	AD 네트워크 검색 권한이 있는 사용자의 이름	-
--ad-user-password	Active Directory 사용자 비밀번호	-
--ad-cdn-include	동기화될 Active Directory 트리 경로, 전체 트리 경로를 동기화하려면 빈 괄호 ""를 사용합니다.	-
--enable-imp-program	제품 향상 프로그램을 켭니다.	-
--disable-imp-program	제품 향상 프로그램을 끕니다.	-

명령줄 기록에서 중요한 데이터(예: 패스워드)가 포함된 명령을 제거하는 것이 좋습니다.

- 1.history를 실행하여 기록에서 모든 명령 목록을 확인합니다.
- 2.history -d line\_number를 실행합니다(명령의 줄 수 지정). 또는 history -c를 실행하여 전체 명령줄 기록을 제거합니다.

4. 설치 작업을 수행하면 제품 향상 프로그램에 참여하라는 메시지가 표시됩니다. 충돌 보고서 및 원격측정 데이터를 ESET에 보내는 데 동의하면 **Y**를 누르고, ESET에 데이터를 보내지 않으려면 **N**을 누릅니다.

5. ESET PROTECT 서버 및 eraserver 서비스는 다음 위치에 설치됩니다.

`/opt/eset/RemoteAdministrator/Server`

설치가 **SELinux policy... failure**로 끝날 수 있습니다. SELinux를 사용하지 않은 경우 무시해도 됩니다.

6. 설치 후 아래 표시된 명령을 사용하여 ESET PROTECT 서버 서비스가 실행되고 있는지 확인합니다.

`sudo systemctl status eraserver`

```
root@protect:~  
[root@protect ~]# sudo systemctl status eraserver  
Last login: Wed Apr 27 16:35:14 CEST 2022 from [REDACTED] on pts/0  
● eraserver.service - ESET PROTECT Server  
   Loaded: loaded (/etc/systemd/system/eraserver.service; enabled; vendor preset: disabled)  
   Active: active (running) since Thu 2022-04-07 13:58:07 CEST; 2 weeks 6 days ago  
 Main PID: 3480 (ERAServer)  
   CGroup: /system.slice/eraserver.service  
           └─3480 /opt/eset/RemoteAdministrator/Server/ERAServer --daemon --pidfile /var/run/eraserver.pid...  
  
Apr 07 13:58:07 protect.local systemd[1]: Starting ESET PROTECT Server...  
Apr 07 13:58:07 protect.local systemd[1]: Started ESET PROTECT Server.  
[root@protect ~]#
```

## 설치 관리자 로그

설치 관리자 로그는 문제를 해결하는 데 도움이 될 수 있으며 [로그 파일](#)에서 찾을 수 있습니다.

## 서버 필수 구성 요소 - Linux

Linux에 ESET PROTECT 서버를 설치하려면 다음 필수 구성 요소를 충족해야 합니다.

- 유효한 [라이선스](#)가 있어야 합니다.
- [지원되는 Linux 운영 체제](#)가 있어야 합니다.
- 필요한 포트가 열려 있고 사용 가능해야 함 - [전체 포트 목록은 여기](#)를 참조하십시오.
- 루트 계정을 사용하여 [DB 서버가 설치되고 구성되어 있어야](#) 합니다. 설치 전에 사용자 계정을 생성할 필요가 없으며, 설치 관리자가 계정을 만들 수 있습니다. [Linux에서 Microsoft SQL Server](#)는 지원되지 않습니다. 그러나 [Linux의 ESET PROTECT 서버를 Windows의 Microsoft SQL Server에 연결](#)할 수 있습니다.

**i** ESET PROTECT 서버는 DB에 큰 데이터 Blob을 저장하므로 ESET PROTECT가 제대로 실행되려면 [큰 패키지](#)를 [수용](#)하도록 MySQL을 구성합니다.

- **ODBC 드라이버** - ODBC 드라이버는 [DB 서버](#)(My SQL)와의 연결을 설정하는 데 사용됩니다.

- 터미널 명령을 사용하여 서버 설치 파일을 실행 파일로 설정합니다.

```
chmod +x server-linux-x86_64.sh
```

- **최신 버전의 OpenSSL 1.1.1**를 사용하는 것이 좋습니다. ESET PROTECT 서버/MDM은 OpenSSL 3.x을(를) 지원하지 않습니다. ESET Management Agent는 OpenSSL 3.x을(를) 지원합니다. 지원되는 최소 Linux용 OpenSSL 버전은 openssl-1.0.1e-30입니다. 한 시스템에 여러 버전의 OpenSSL을 동시에 설치할 수 있습니다. 시스템에는 지원되는 버전이 하나 이상 있어야 합니다.

openssl version 명령을 사용하여 현재 기본 버전을 표시합니다.

o시스템에 있는 OpenSSL의 모든 버전을 나열할 수 있습니다. 명령 sudo find / -iname \*libcrypto.so\*를 사용하여 나열된 파일 이름의 끝 부분을 확인합니다.

o다음 명령을 사용하여 Linux 클라이언트가 호환되는지 확인할 수 있습니다: openssl s\_client -connect google.com:443 -tls1\_2

- **Xvfb** - 그래픽 인터페이스 없이 Linux 서버 시스템에서 적절한 보고 인쇄([보고서 생성](#))를 수행하는 데 필요합니다.
- **Xauth** - 패키지가 xvfb와 함께 설치됩니다. xvfb를 설치하지 않으면 xauth를 설치해야 합니다.
- **cifs-utils** - Windows OS에 대한 적절한 에이전트 배포에 필요합니다.
- **Qt4 WebKit 라이브러리** - 보고서를 PDF 및 PS 형식으로 인쇄하는 데 사용됩니다(버전 5가 아닌 4.8이어야 함). 기타 모든 Qt4 종속성은 자동으로 설치됩니다. 운영 체제 저장소에서 패키지를 사용할 수 없는 경우, 대상 컴퓨터에 직접 컴파일하거나 타사 저장소(예: [EPEL 저장소](#))에서 패키지를 설치할 수 있습니다. [CentOS 7 지침](#), [Ubuntu 20.04 지침](#).
- **kinit + klist** - Kerberos는 로그인 및 Active Directory 동기화 작업 시 도메인 사용자를 인증하는 데 사용됩니다. Kerberos를 올바르게 구성했는지 확인합니다(/etc/krb5.conf). ESET PROTECT 10.0에서는 여러 도메인과의 동기화를 지원합니다.
- **ldapsearch** - AD 동기화 작업과 인증에 사용됩니다.
- **snmptrapd** - 옵션으로, SNMP 트랩을 전송하는 데 사용됩니다. SNMP 구성도 필요합니다.
- **SELinux devel 패키지** - SELinux 정책 모듈을 작성하기 위해 제품 설치 중에 사용됩니다. SELinux가 활성화된 시스템(CentOS, RHEL)에서만 필요합니다. SELinux는 다른 애플리케이션과 문제를 발생시킬 수 있습니다. ESET PROTECT 서버의 경우 불필요합니다.
- **lshw** - ESET Management 에이전트가 [하드웨어 인벤토리](#)를 올바르게 보고하게 하려면 클라이언트/서버 Linux 컴퓨터에 lshw 패키지를 설치합니다.

아래 표에는 다양한 Linux 배포에 대해 위에서 설명한 각 패키지용으로 적합한 터미널 명령이 포함되어 있습니다(명령을 sudo 또는 root로 실행).

패키지	Debian 및 Ubuntu 배포	CentOS 및 Red Hat 배포
ODBC 드라이버	<a href="#">ODBC 설치 및 구성</a> 을 참조하십시오.	<a href="#">ODBC 설치 및 구성</a> 을 참조하십시오.
OpenSSL	apt-get install openssl	yum install openssl -y
xvfb	apt-get install xvfb	yum install xorg-x11-server-Xvfb -y
cifs-utils	apt-get install cifs-utils	yum install cifs-utils



패키지	Debian 및 Ubuntu 배포	CentOS 및 Red Hat 배포
Qt4 WebKit 라이브러리	apt-get install libqtwebkit4 <a href="#">Ubuntu 20.04 지침</a> 을 참조하십시오.	Qt4 WebKit는 표준 CentOS 저장소에 없습니다. 다음 패키지를 설치하십시오. yum install -y epel-release yum install qtwebkit-devel 또는 <a href="#">Fedora 저장소</a> 에서 패키지를 설치할 수 있습니다.
kinit+klint - 옵션(Active Directory 서비스에 필요함)	apt-get install krb5-user	yum install krb5-workstation
ldapsearch	apt-get install ldap-utils libsasl2-modules-gssapi-mit	yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y
snmptrap	apt-get install snmp	yum install net-snmp-utils net-snmp
SELinux devel 패키지(옵션 - ESET PROTECT 서버에 필요하지 않음, SELinux로 인해 다른 애플리케이션에서 문제가 발생할 수 있음).	apt-get install selinux-policy-dev	yum install policycoreutils-devel
samba(옵션, 원격 배포에만 필요함)	apt-get install samba	yum install samba samba-winbind-clients
lshw	apt-get install -y lshw	yum install -y lshw

## 에이전트 설치 - Linux

### 필수 구성 요소

- 최신 버전의 **OpenSSL1.1.1**를 사용하는 것이 좋습니다. ESET PROTECT 서버/MDM은 OpenSSL 3.x을(를) 지원하지 않습니다. ESET Management Agent는 OpenSSL 3.x을(를) 지원합니다. 지원되는 최소 Linux용 OpenSSL 버전은 openssl-1.0.1e-30입니다. 한 시스템에 여러 버전의 OpenSSL을 동시에 설치할 수 있습니다. 시스템에는 지원되는 버전이 하나 이상 있어야 합니다.

openssl version 명령을 사용하여 현재 기본 버전을 표시합니다.

시스템에 있는 OpenSSL의 모든 버전을 나열할 수 있습니다. 명령 sudo find / -iname \*libcrypto.so\*를 사용하여 나열된 파일 이름의 끝 부분을 확인합니다.

다음 명령을 사용하여 Linux 클라이언트가 호환되는지 확인할 수 있습니다: openssl s\_client -connect google.com:443 -tls1\_2

- ESET Management 에이전트가 [하드웨어 인벤토리](#)를 올바르게 보고하게 하려면 클라이언트/서버 Linux 컴퓨터에 lshw 패키지를 설치합니다.

Linux 배포	터미널 명령
Debian, Ubuntu	sudo apt-get install -y lshw
Red Hat, CentOS, RHEL	sudo yum install -y lshw
OpenSUSE	sudo zypper install lshw

- Linux CentOS의 경우 policycoreutils-devel 패키지를 설치하는 것이 좋습니다. 다음 명령을 실행하여 패키지를 설치합니다.

```
yum install policycoreutils-devel
```

- 서버 지원 에이전트 설치:

네트워크에서 서버 컴퓨터에 연결할 수 있어야 하고, 서버 컴퓨터에 [ESET PROTECT 서버](#) 및 [ESET](#)



[PROTECT 웹 콘솔](#)이 설치되어 있어야 합니다.

- 오프라인 에이전트 설치:

o네트워크에서 서버 컴퓨터에 연결할 수 있어야 하고, 서버 컴퓨터에 [ESET PROTECT 서버](#)가 설치되어 있어야 합니다.

o에이전트의 [인증서](#)가 있어야 합니다.

o서버의 [인증 기관](#) 공개 키 파일이 있어야 합니다.

## 설치

터미널 명령을 사용하여 Linux에 ESET Management Agent 구성 요소를 설치하려면 다음 단계를 따릅니다.

**!** 위에 나열된 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

1. 다음과 같이 에이전트 설치 스크립트를 다운로드합니다.

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. 파일을 실행 가능하게 합니다.

```
chmod +x agent-linux-x86_64.sh
```

3. 아래 예에 따라 설치 스크립트를 실행합니다(전체 명령을 터미널에 복사할 수 있도록 새 줄은 "\"로 분리됨).

**i** 자세한 내용은 아래의 [파라미터](#)를 참조하십시오.

서버 지원 설치:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.0.1 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

오프라인 설치:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
```

--port=2222

명령줄 기록에서 중요한 데이터(예: 패스워드)가 포함된 명령을 제거하는 것이 좋습니다.

- i 1.history를 실행하여 기록에서 모든 명령 목록을 확인합니다.  
2.history -d line\_number를 실행합니다(명령의 줄 수 지정). 또는 history -c를 실행하여 전체 명령줄 기록을 제거합니다.

4. 메시지가 표시되면 **y** 키를 눌러 인증서를 수락합니다. 설치 관리자가 반환한 SELinux 관련 오류는 무시해도 됩니다.

5. 설치 후 ESET Management Agent 서비스가 실행 중인지 확인합니다.

```
sudo systemctl status eraagent
```

6. 부팅 시 시작하도록 eraagent 서비스 설정:sudo systemctl enable eraagent

i **설치 관리자 로그**  
설치 관리자 로그는 문제를 해결하는 데 도움이 될 수 있으며, [로그 파일](#)에서 찾을 수 있습니다.

## 파라미터

ESET PROTECT 서버 연결은 파라미터(--hostname 및 --port)를 사용하여 확인합니다(SRV 레코드가 제공된 경우에는 포트가 사용되지 않음). [가능한 연결 형식은 다음과 같습니다.](#)

- 호스트 이름 및 포트
- IPv4 주소 및 포트
- IPv6 주소 및 포트
- 서비스 레코드(SRV 레코드) - Linux에서 DNS 리소스 레코드를 구성하려면 컴퓨터가 작업 DNS 서버가 있는 도메인에 있어야 합니다. [DNS 리소스 레코드](#)를 참조하십시오. SRV 레코드는 접두어 "\_NAME.\_tcp"로 시작해야 합니다. 여기서 'NAME'은 사용자 지정 이름을 나타냅니다(예:

특성	설명	필수
--hostname	연결할 ESET PROTECT 서버의 호스트 이름 또는 IP 주소	예
--port	ESET PROTECT() 서버 포트(기본값: 2222).	예
--cert-path	에이전트 인증서 파일의 로컬 경로( <a href="#">인증서</a> 에 대한 추가 정보)	예(오프라인)
--cert-auth-path	서버 인증 기관 파일의 경로( <a href="#">기관</a> 에 대한 추가 정보)	예(오프라인)
--cert-password	에이전트 인증서 패스워드	예(오프라인)
--cert-auth-password	인증 기관 비밀번호	예(사용하는 경우)
--skip-license	설치에서 사용권 계약 확인을 요구하는 메시지는 표시되지 않습니다.	아니요
--cert-content	서버 및 에이전트와의 안전한 통신 채널을 설정하는 데 사용되는, PKCS12 인코딩 공개 키 인증서 및 개인 키의 Base64 인코딩 콘텐츠. --cert-path 또는 --cert-content 옵션 중 하나만 사용하십시오.	아니요
--cert-auth-content	원격 피어(프로キシ 또는 서버)를 검증하는 데 사용되는, DER 인코딩 인증 기관 개인 키 인증서의 Base64 인코딩 콘텐츠. --cert-auth-path 또는 --cert-auth-content 옵션 중 하나만 사용하십시오.	아니요
--webconsole-hostname	서버에 연결하기 위해 웹 서버에서 사용하는 호스트 이름 또는 IP 주소(비어 있는 경우 설치 관리자가 'hostname'에서 값을 복사함)	아니요
--webconsole-port	서버에 연결하기 위해 웹 콘솔에서 사용하는 포트(기본값: 2223)	아니요
--webconsole-user	서버에 연결하기 위해 웹 콘솔에서 사용하는 사용자 이름(기본값: Administrator) <b>! 서버 지원 설치의 경우 사용자에게 2단계 인증을 사용할 수 없습니다.</b>	아니요
--webconsole-password	서버에 연결하기 위해 웹 콘솔에서 사용하는 비밀번호	예(서버 지원)
--proxy-hostname	HTTP 프록시 호스트 이름. 이 파라미터를 사용하여 ESET Management Agent와 ESET PROTECT 서버 간의 복제를 위한 HTTP 프록시(네트워크에 이미 설치됨) 사용을 활성화할 수 있습니다(업데이트 캐시용 아님).	프록시를 사용하는 경우
--proxy-port	서버 연결용 HTTP 프록시 포트	프록시를 사용하는 경우
--enable-imp-program	제품 향상 프로그램을 켭니다.	아니요
--disable-imp-program	제품 향상 프로그램을 끕니다.	아니요

## 연결 및 인증서

- **ESET PROTECT 서버 연결**을 제공해야 합니다. `--hostname`, `--port`(서비스 레코드가 제공된 경우 포트가 필요하지 않으며, 기본 포트 값은 2222임)
- **서버 지원 설치**를 위한 이 연결 정보 제공: `--webconsole-port`, `--webconsole-user`, `--webconsole-password`
- **오프라인 설치**를 위한 인증서 정보 제공: `--cert-path`, `--cert-password`. 설치 파라미터 `--cert-path` 및 `--cert-auth-path`에는 ESET PROTECT 웹 콘솔에서 내보낼 수 있는 인증 파일(`.pfx` 및 `.der`)이 필요합니다. ([.pfx 파일 내보내기](#) 및 [.der 파일 내보내기](#) 방법 참조).

## 비밀번호 유형 파라미터

비밀번호 유형 파라미터는 환경 변수, 파일로 제공될 수 있으며, `stdin`에서 읽거나 일반 텍스트로 제공될 수 있습니다. 즉 다음과 같습니다.

`--password=env:SECRET_PASSWORD`, 여기서 `SECRET_PASSWORD`는 패스워드가 포함된 환경 변수입니다.

`--password=file:/opt/secret`, 여기서 일반 파일 `/opt/secret`의 첫 번째 줄에 비밀번호가 포함됩니다.

`--password=stdin`은 설치 관리자에 표준 입력에서 비밀번호를 읽도록 지시합니다.

`--password="pass:PASSWORD"`는 `--password="PASSWORD"`와 같고 실제 패스워드가 `"stdin"`(표준 입력) 또는 `"env:"`, `"file:"`, `"pass:"`로 시작하는 문자열인 경우 필수 항목입니다.



인증서 비밀번호에는 문자를 포함할 수 없습니다: " \ 이러한 문자를 사용하면 에이전트를 초기화하는 동안 심각한 오류가 발생합니다.

## HTTP 프록시 연결

ESET Management Agent 및 ESET PROTECT 서버 간 복제를 위해 HTTP 프록시를 사용하는 경우(업데이트 캐싱 용이 아님) `--proxy-hostname` 및 `--proxy-port`에서 연결 파라미터를 지정할 수 있습니다.

예 - HTTP 프록시 연결을 사용하는 오프라인 에이전트 설치

```
./agent-linux-x86_64.sh \  
--skip-license \  
--cert-path=/home/admin/Desktop/agent.pfx \  
--cert-auth-path=/home/admin/Desktop/CA.der \  
--cert-password=N3lluI4#2aCC \  
--hostname=10.1.179.36 \  
--port=2222 \  
--proxy-hostname=10.1.180.3 \  
--proxy-port=3333 \  

```



에이전트와 ESET PROTECT 서버 간의 통신 프로토콜은 인증을 지원하지 않습니다. 인증을 요구하는 ESET PROTECT 서버에 에이전트 통신을 전달하는 데 사용되는 프록시 솔루션은 작동되지 않습니다. 웹 콘솔이나 에이전트에 대해 기본값이 아닌 포트를 사용하도록 선택하면 방화벽을 조정해야 할 수 있습니다. 조정하지 않으면 설치에 실패할 수 있습니다.

## Linux에서 에이전트 설치 업그레이드 및 복구

에이전트가 이미 설치된 시스템에서 에이전트 설치를 수동으로 실행하는 경우 다음 시나리오가 발생할 수 있습니다.

- **업그레이드** - 최신 버전의 설치 관리자를 실행합니다.
  - o 서버 지원 설치 - 응용 프로그램이 업그레이드되지만 이전 인증서가 계속 사용됩니다.
  - o 오프라인 설치 - 응용 프로그램이 업그레이드되고 새 인증서가 사용됩니다.
- **복구** - 동일한 버전의 설치 프로그램을 실행합니다. 이 옵션을 사용하여 에이전트를 다른 ESET PROTECT 서버로 마이그레이션할 수 있습니다.
  - o 서버 지원 설치 - 응용 프로그램이 다시 설치되고 ESET PROTECT 서버에서 현재 인증서를 가져옵니다(hostname 파라미터로 정의됨).
  - o 오프라인 설치 - 응용 프로그램이 다시 설치되고 새 인증서가 사용됩니다.

이전 서버에서 다른 새 ESET PROTECT 서버로 에이전트를 수동으로 마이그레이션하고 서버 지원 설치를 사용하는 경우 설치 명령을 두 번 실행합니다. 첫 번째 실행 시 에이전트를 업그레이드하고, 두 번째 실행 시 에이전트가 ESET PROTECT 서버에 연결할 수 있도록 새 인증서를 가져옵니다.

## 웹 콘솔 설치 - Linux

다음 단계에 따라 ESET PROTECT 웹 콘솔을 설치합니다.



ESET PROTECT 서버가 설치된 컴퓨터와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치할 수 있습니다. 이 절차를 수행하려면 [추가 단계](#)를 진행해야 합니다.

1. Apache Tomcat 및 Java 패키지를 설치합니다.



아래 패키지 이름의 예는 Linux 배포 저장소 패키지과 다를 수 있습니다. Linux 배포본의 기본 저장소에 [지원되는 최신 버전의 Apache Tomcat 및 Java](#)가 포함되어 있지 않을 수 있습니다.

Linux 배포	터미널 명령
Debian 및 Ubuntu 배포	sudo apt-get update sudo apt-get install openjdk-17-jdk tomcat9
CentOS 및 Red Hat 배포	yum update yum install java-17-openjdk tomcat
SUSE Linux	zypper refresh sudo zypper install java-17-openjdk tomcat9

2. 웹 콘솔 파일(*era.war*) 다운로드:

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. *era.war* 파일을 Tomcat 폴더에 복사:

Debian, Ubuntu	<code>sudo cp era.war /var/lib/tomcat9/webapps/</code>
CentOS, Red Hat	<code>sudo cp era.war /var/lib/tomcat/webapps/</code>
SUSE Linux Enterprise Server	<code>sudo cp era.war /usr/share/tomcat/webapps/</code>

4. Tomcat 서비스를 다시 시작하여 *era.war* 파일 배포:

Debian, Ubuntu	<code>sudo systemctl restart tomcat9</code>
CentOS, Red Hat	<code>sudo systemctl restart tomcat</code>
SUSE Linux Enterprise Server	<code>sudo systemctl restart tomcat</code>

5. *era* 폴더가 Tomcat 폴더에 있는지 확인합니다.

Debian, Ubuntu	<code>ls /var/lib/tomcat9/webapps</code>
CentOS, Red Hat	<code>ls /var/lib/tomcat/webapps</code>
SUSE Linux Enterprise Server	<code>ls /usr/share/tomcat/webapps</code>

출력은 *era era.war*와 같아야 합니다.

6. 부팅 시 시작하도록 Tomcat 서비스 설정: `sudo systemctl enable tomcat`(또는 서비스 이름에 따라 `tomcat9`)

7. ESET PROTECT 서버와는 다른 컴퓨터에 ESET PROTECT 웹 콘솔을 설치한 경우 다음 추가 단계를 수행하여 ESET PROTECT 웹 콘솔과 ESET PROTECT 서버 간의 통신을 활성화하십시오.

a) Tomcat 서비스를 중지합니다: `sudo systemctl stop tomcat`

b) *EraWebServerConfig.properties* 파일을 편집합니다:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties
```

*EraWebServerConfig.properties* 파일이 위 경로에 없으면 다음 명령을 사용하여 시스템에서 파일을 찾을 수 있습니다.

```
find / -iname "EraWebServerConfig.properties"
```

c) `server_address=localhost`를 찾습니다

d) `localhost`를 ESET PROTECT 서버의 IP 주소로 바꾸고 파일을 저장합니다.

e) Tomcat 서비스 다시 시작: `sudo systemctl restart tomcat`(또는 서비스 이름에 따라 `tomcat9`)

f)부팅 시 시작하도록 Tomcat 서비스 설정: `sudo systemctl enable tomcat`(또는 서비스 이름에 따라 `tomcat9`)


8. [지원되는 웹 브라우저](#)에서 ESET PROTECT 웹 콘솔을 열면 로그인 화면이 표시됩니다.

- ESET PROTECT 웹 콘솔을 호스팅하는 컴퓨터에서: `http://localhost:8080/era`
- ESET PROTECT 웹 콘솔에 대한 인터넷 접근 권한이 있는 컴퓨터에서(`IP_ADDRESS_OR_HOSTNAME`을 ESET PROTECT 웹 콘솔의 IP 주소 또는 호스트 이름으로 대체):  
`http://IP_ADDRESS_OR_HOSTNAME:8080/era`

9. 설치 후 웹 콘솔 구성:

- Apache Tomcat 수동 설치 중에 기본 HTTP 포트는 8080으로 설정됩니다. [Apache Tomcat용 HTTPS 연결](#)을 설정하는 것이 좋습니다.
- [엔터프라이즈 솔루션 또는 저성능 시스템에 대한 추가 웹 콘솔 구성](#)도 참조하십시오.

## Rogue Detection Sensor 설치 - Linux

 여러 네트워크 세그먼트가 있는 경우 전체 네트워크에 있는 모든 장치의 종합 목록을 생성하려면 각 네트워크 세그먼트에 Rogue Detection Sensor를 별도로 설치해야 합니다.

### 필수 구성 요소

- 네트워크는 검색 가능해야 합니다(포트가 열려 있으며 방화벽이 수신 통신을 차단하지 않아야 함).
- 서버 컴퓨터에 연결할 수 있습니다.
- 모든 프로그램 기능을 완전히 지원하려면 [ESET Management 에이전트](#)가 로컬 컴퓨터에 설치되어야 합니다.
- 터미널이 열려 있습니다.
- RD Sensor 설치 파일을 실행 파일로 설정합니다.

```
chmod +x rdsensor-linux-x86_64.sh
```

### 설치

터미널 명령을 사용하여 Linux에 RD Sensor 구성 요소를 설치하려면 다음 단계를 따릅니다.

 위에 나열된 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

1. 다음 명령을 사용하여 설치 파일을 `sudo`로 실행합니다.

```
sudo ./rdsensor-linux-x86_64.sh
```

2. 최종 사용자 사용권 계약을 읽어 보십시오. EULA의 다음 페이지로 이동하려면 **스페이스바**를 사용합니다.

설치 관리자가 계약에 동의하는지 여부를 지정하라는 메시지를 표시합니다. 동의하면 키보드에서 **Y** 키를 누르고, 그렇지 않으면 **N** 키를 누릅니다.

3. 제품 항상 프로그램에 참여하는 데 동의하면 **Y** 키를 누르고, 그렇지 않으면 **N** 키를 누릅니다.

4. 설치가 완료되면 ESET Rogue Detection Sensor가 시작됩니다.

5. 제대로 설치되었는지 확인하려면 다음 명령을 실행하여 서비스가 실행되고 있는지 확인하십시오.

```
sudo systemctl status rdsensor
```

6. [로그 파일](#)에서 Rogue Detection Sensor 로그 파일을 찾을 수 있습니다.

```
/var/log/eset/RogueDetectionSensor/trace.log
```

## 모바일 장치 커넥터 설치 - Linux

**!** ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

ESET PROTECT 서버가 실행되고 있는 서버와 다른 서버에 모바일 장치 커넥터를 설치할 수 있습니다. 예를 들어 이 설치 시나리오를 사용하여 인터넷에서 Mobile Device Connector에 접근하여 항상 사용자의 모바일 장치를 관리하도록 할 수 있습니다.

터미널 명령을 사용하여 Linux에 Mobile Device Connector 구성 요소를 설치하려면 다음 단계를 따릅니다.

**!** 설치 [필수 구성 요소](#)를 모두 충족하는지 확인합니다.

1. Mobile Device Connector 설치 스크립트를 다운로드합니다.

```
wget https://download.eset.com/com/eset/apps/business/era/mdm/latest/mdmcore-linux-x86_64.sh
```

2. 아래 예에 따라 설치 스크립트를 실행합니다(전체 명령을 터미널에 복사할 수 있도록 새 줄은 "\"로 분리됨).

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

사용 가능한 파라미터의 전체 목록을 보려면(도움말 메시지 출력) 다음을 사용:

--help

명령줄 기록에서 중요한 데이터(예: 패스워드)가 포함된 명령을 제거하는 것이 좋습니다.

- i 1.history를 실행하여 기록에서 모든 명령 목록을 확인합니다.
- 2.history -d line\_number를 실행합니다(명령의 줄 수 지정). 또는 history -c를 실행하여 전체 명령줄 기록을 제거합니다.

## 필수 설치 명령 파라미터

옵션 설치 파라미터가 많이 있지만 이 중 일부는 필수입니다:

- **피어 인증서** - ESET PROTECT [피어 인증서](#)를 가져올 수 있는 방법은 다음의 두 가지가 있습니다.
  - **서버 지원 설치** - ESET PROTECT 웹 콘솔 관리자 자격 증명을 제공해야 합니다(설치 관리자가 필요한 인증서를 자동으로 다운로드함).
  - **오프라인 설치** - 피어 인증서(ESET PROTECT에서 [내보낸](#) 프록시 인증서)을 제공해야 합니다. 또는 [사용자 지정 인증서](#)를 사용할 수도 있습니다.

0**서버 지원 설치**의 경우 최소 다음을 포함:

--webconsole-password=

0**오프라인 설치**의 경우 다음을 포함:

--cert-path=  
--cert-password=

(ESET PROTECT 서버 설치 중에 생성된 기본 에이전트 인증서에는 패스워드가 필요하지 않음)

- **HTTPS(프록시) 인증서:**

0이미 HTTPS 인증서가 있는 경우:

--https-cert-path=  
--https-cert-password=

0**새 HTTPS 인증서**를 생성하려면 다음을 수행합니다.

--https-cert-generate  
--mdm-hostname=

- **ESET PROTECT 서버에 대한 연결(이름 또는 IP 주소):**



--hostname=

- DB 연결:

oMySQL DB의 경우 다음을 포함:

```
--db-type="MySQL Server"  
--db-driver=  
--db-admin-username=  
--db-admin-password=  
--db-user-password=
```

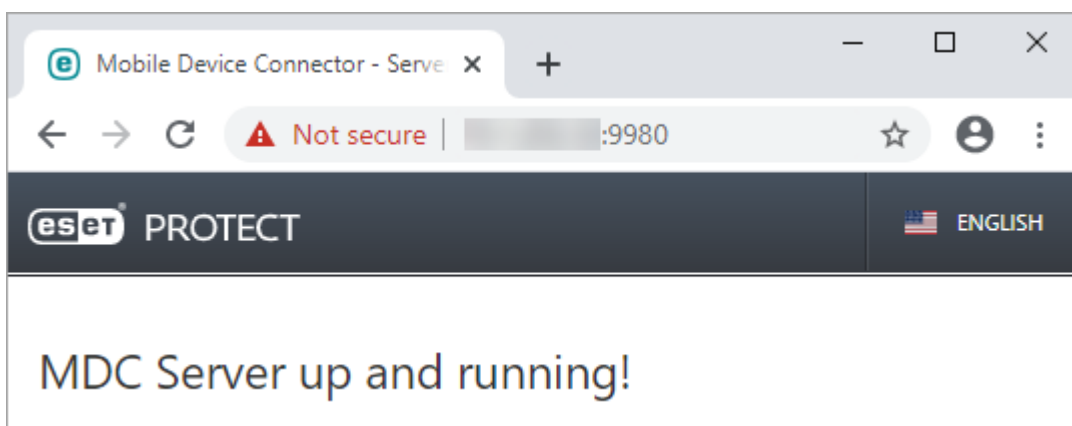
oMicrosoft SQL 데이터베이스의 경우 다음이 포함됩니다.

```
--db-type="Microsoft SQL Server"  
--db-driver=  
--db-admin-username=  
--db-admin-password=  
--db-user-password=
```

## 설치 관리자 로그

설치 관리자 로그는 문제를 해결하는 데 도움이 될 수 있으며 [로그 파일](#)에서 찾을 수 있습니다.

설치가 완료된 후 웹 브라우저에서 *https://your-mdm-hostname:enrollment-port*(예: *https://eramdm:9980*)를 열어 모바일 장치 커넥터가 제대로 실행되는지 확인합니다. 설치에 성공하면 다음과 같은 메시지가 표시됩니다.



또한 모바일 장치에서 이 URL을 방문하여 인터넷(이러한 방식으로 구성된 경우)에서 모바일 장치 커넥터 서버의 가용성을 확인할 수도 있습니다. 이 페이지에 연결할 수 없는 경우 방화벽과 네트워크 인프라 구성을 확인하십시오.

# 모바일 장치 커넥터 필수 구성 요소 - Linux

Linux에서 모바일 장치 커넥터를 설치하려면 다음 필수 구성 요소가 충족되어야 합니다.

- 루트 계정을 사용하여 DB 서버가 이미 설치되고 구성되어 있어야 합니다(설치 관리자가 사용자 계정을 만들 수 있으므로 설치 전에 미리 만들 필요가 없음).
- [DB 서버](#)(MySQL/Microsoft SQL) 연결용 ODBC 드라이버가 컴퓨터에 설치되어 있습니다. [ODBC 설치 및 구성](#) 장을 참조하십시오.

**i** 문제 없이 MDC를 MySQL DB에 연결하려면 기본 unixODBC가 아니라 unixODBC\_23 패키지를 사용해야 합니다. 특히, SUSE Linux의 경우 그렇습니다.

**i** ESET PROTECT 서버가 호스팅된 것과는 별도의 호스트 장치에 MDM 구성 요소를 배포하는 것이 좋습니다.

- MDMCore 설치 파일이 실행 파일로 설정되어 있어야 합니다.

```
chmod +x mdmcore-linux-x86_64.sh
```

- 설치 후 MDMCore 서비스가 실행 중인지 확인합니다.

```
sudo systemctl status eramdmcore
```

- **최신 버전의 OpenSSL 1.1.1**를 사용하는 것이 좋습니다. ESET PROTECT 서버/MDM은 OpenSSL 3.x을(를) 지원하지 않습니다. ESET Management Agent는 OpenSSL 3.x을(를) 지원합니다. 지원되는 최소 Linux용 OpenSSL 버전은 openssl-1.0.1e-30입니다. 한 시스템에 여러 버전의 OpenSSL을 동시에 설치할 수 있습니다. 시스템에는 지원되는 버전이 하나 이상 있어야 합니다.

openssl version 명령을 사용하여 현재 기본 버전을 표시합니다.

시스템에 있는 OpenSSL의 모든 버전을 나열할 수 있습니다. 명령 `sudo find / -iname *libcrypto.so*`를 사용하여 나열된 파일 이름의 끝 부분을 확인합니다.

다음 명령을 사용하여 Linux 클라이언트가 호환되는지 확인할 수 있습니다: `openssl s_client -connect google.com:443 -tls1_2`

**i** MySQL의 MDM DB가 너무 크면(수천 대의 장치) 기본 `innodb_buffer_pool_size` 값이 너무 작아집니다. DB 최적화에 대한 자세한 내용은 <http://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html>을 참조하십시오.

## 인증서 요구 사항

- HTTPS를 통한 보안 통신을 위해서는 .pfx형식의 **SSL 인증서**가 필요합니다. 타사 인증 기관에서 제공한 인증서를 사용하는 것이 좋습니다. 일부 모바일 장치에서는 사용자가 자체 서명한 인증서를 수락할 수 없으므로, 자체 서명한 인증서(ESET PROTECT CA에서 서명한 인증서 포함)는 권장되지 않습니다.

- CA에서 서명한 인증서 및 해당 개인 키가 있어야 하며, 표준 절차를 사용하여(기존에는 OpenSSL을 사용했음) 이를 다음과 같은 하나의 .pfx 파일로 병합합니다.

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx
```

SSL 인증서를 사용하는 대부분의 서버에서는 이 절차가 표준 절차입니다.

- [오프라인 설치](#)의 경우 피어 인증서(ESET PROTECT에서 [내보낸 에이전트 인증서](#))도 필요합니다. 또는 ESET PROTECT에 [사용자 지정 인증서](#)를 사용할 수도 있습니다.

## 미러 도구 - Linux

### [Windows 사용자입니까?](#)

미러 도구는 오프라인 검색 엔진 업데이트에 필요합니다. 클라이언트 컴퓨터가 인터넷에 연결되어 있지 않고 검색 엔진 업데이트가 필요한 경우 미러 도구를 사용하여 ESET 업데이트 서버에서 업데이트 파일을 다운로드한 후 로컬로 저장할 수 있습니다.

미러 도구에는 다음과 같은 기능이 있습니다.

- 모듈 업데이트 - 탐지 엔진 업데이트 및 기타 프로그램 모듈을 다운로드하지만, [자동 업데이트](#)(uPCU)는 다운로드하지 않습니다.
  - 저장소 생성 - [자동 업데이트](#)(uPCU)를 포함한 전체 [오프라인 저장소](#)를 생성할 수 있습니다.
- 미러 도구는 ESET LiveGrid® 데이터를 다운로드하지 않습니다.

## 필수 구성 요소

- 미러가 생성되는 저장소에는 모든 사용자에게 읽기 및 실행 권한이 있어야 합니다. 권한이 있는 사용자로 이 명령을 실행하여 권한을 부여합니다. `chmod 755`

`mirror/folder/path`(`mirror/folder/path`를 미러 폴더 경로로 대체).

- 대상 폴더는 업데이트에 접근하려는 방법에 따라 공유, Samba/Windows 또는 HTTP/FTP 서비스에 사용할 수 있어야 합니다.

OWindows용 ESET 보안 제품 - HTTP 또는 공유 폴더를 사용하여 원격으로 업데이트할 수 있습니다.

OLinux/macOS에 대한 ESET 보안 제품 - HTTP만을 사용해 원격으로 업데이트할 수 있습니다. 공유 폴더를 사용하는 경우 ESET 보안 제품과 동일한 컴퓨터에 있어야 합니다.

- 사용자 이름 및 비밀번호를 포함하는 유효한 [오프라인 라이선스](#) 파일이 있어야 합니다. 라이선스 파일 생성 시 **사용자 이름 및 비밀번호 포함** 옆의 확인란을 선택해야 합니다. 또한, 라이선스 이름도 입력해야 합니다. 미러 도구를 활성화하고 업데이트 미러를 생성하려면 오프라인 라이선스 파일이 필요합니다.

×

Create offline license file

Product

ESET Endpoint Security for Windows

Name

Test license

Units count

1

/3

Username and password

☒ Include Username and Password  
When included it is possible to update from ESET servers

ESET PROTECT

☐ Allow management with ESET PROTECT

GENERATE

CANCEL

## 미러 도구를 사용하는 방법

- 1.[ESET 다운로드 페이지](#)(독립 실행형 설치 관리자 섹션)에서 미러 도구를 다운로드합니다.
- 2.다운로드된 압축파일의 압축을 풉니다.
- 3.*MirrorTool* 파일이 있는 폴더에서 터미널을 열고 파일을 실행 파일로 만듭니다.

```
chmod +x MirrorTool
```

- 4.아래 명령을 실행하여 미러 도구 및 해당 버전에 사용 가능한 모든 파라미터를 봅니다.

```
./MirrorTool --help
```

```

root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights reserved.
Allowed options:
--mirrorType arg                [required for module update]
                                Type of mirror. Possible values (case
                                insensitive): regular, pre-release,
                                delayed.
--intermediateUpdateDirectory arg [required for module update]
                                Files will be downloaded to this
                                directory to create mirror in output
                                directory.
--offlineLicenseFilename arg     [required for module update]
                                Offline license file.
--updateServer arg              [optional]
                                Update server. (e.g.:
                                http://update.eset.com/eset_upd/ep6/)
                                Mirror will be created in output
                                directory, only specified path in
                                server will be mirrored.
--outputDirectory arg           [required for module update]
                                Directory where mirror will be created.
--proxyHost arg                 [optional]
                                Http proxy address (fqdn or IP).
--proxyPort arg                 [optional]
                                Http proxy port.
--proxyUsername arg             [optional]
                                Http proxy username.
--proxyPassword arg             [optional]
                                Http proxy password.
--networkDriveUsername arg      [optional]
                                Username used, when output directory is
                                accessed using smb(e.g:\\hostname).
--networkDrivePassword arg      [optional]
                                Password used, when output directory is
                                accessed using smb(e.g:\\hostname).
--excludedProducts arg          [optional]
                                Disable creating mirror for specified
                                products. Use --listUpdatableProducts
                                to see possible values.
--listUpdatableProducts         Show list of all products which modules
                                are downloaded by default.
--repositoryServer arg          [required for repository update]
                                Repository server for repository
                                creation.
--intermediateRepositoryDirectory arg [required for repository update]
                                Files will be downloaded to this
                                directory to create offline mirror in
                                output directory.
--outputRepositoryDirectory arg [required for repository update]
                                Directory where offline repository will
                                be created.
--trustDownloadedFilesInRepositoryTemp [optional]
                                If set, hashes on already downloaded
                                files are not checked.
--mirrorOnlyLevelUpdates        [optional]
                                If set, only level upgrades will be
                                downloaded (nano/continuous updates
                                will not be downloaded)
--mirrorFileFormat arg          [optional]
                                Specifies which type of update files
                                will be downloaded. Possible values
                                (case insensitive): dll, dat.
--compatibilityVersion arg      [optional]
                                Version of compatible products.
--filterFilePath arg            [optional]
                                Path to filter file in json format.
                                Parameter compatibilityVersion has to
                                be higher than 7.1.0.0 to run program.
--dryRun arg                    [optional]
                                Specifies dry run of program with path
                                to csv file where will be saved list of
                                products to be downloaded with current
                                filter configuration.
--help                          [optional]
                                Display this help and exit

```

**i** 모든 필터는 대소문자를 구분합니다.

파라미터를 사용하여 저장소 미리 또는 모듈 미러를 생성할 수 있습니다.

### 저장소 및 모듈 미리 모두에 대한 파라미터


<b>--proxyHost</b>
--proxyPort
--proxyUsername
--proxyPassword
--help


### 저장소용 파라미터

<b>--repositoryServer</b>
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

### 모듈용 파라미터

<b>--mirrorType</b>
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

파라미터	설명
--updateServer	Mirror Tool은 엔드포인트 미러에서와는 다른 <a href="#">폴더 구조</a> 를 생성합니다. 각 폴더에는 제품 그룹에 대한 업데이트 파일이 들어 있습니다. <div>  <b>미러를 사용하여 제품의 업데이트 설정에서 <a href="#">업데이트 서버 전체 링크</a>(올바른 폴더에 대한 전체 경로)를 지정해야 합니다.</b> </div>
--offlineLicenseFilename	오프라인 라이선스 파일의 경로를 지정해야 합니다(위에 설명됨).
--mirrorOnlyLevelUpdates	인수가 필요하지 않습니다. 설정하면 수준 업데이트만 다운로드됩니다(nano 업데이트는 다운로드되지 않음). <a href="#">지식베이스 문서에서</a> 업데이트 유형에 대해 자세히 알아보십시오.

파라미터	설명
--mirrorFileFormat	<div>  <p>--mirrorFileFormat 파라미터를 사용하기 전, 환경에 이전(6.5 이상) 및 최신(6.6 이상) ESET 보안 제품 버전이 모두 포함되어 있지 않은지 확인합니다. 이 파라미터를 잘못 사용하면 ESET 보안 제품이 잘못 업데이트될 수 있습니다.</p> </div> <p>다운로드할 업데이트 파일 유형을 지정할 수 있습니다. 가능한 값(대소문자 구분):</p> <ul style="list-style-type: none"> <li>• dat - 환경에 ESET 보안 제품 버전 6.5 이상만 있는 경우 이 값을 사용합니다.</li> <li>• dll - 환경에 ESET 보안 제품 버전 6.6 이상만 있는 경우 이 값을 사용합니다.</li> </ul> <p>레거시 제품(ep4, ep5)에 대한 미러를 생성할 때 이 파라미터는 무시됩니다.</p>
--compatibilityVersion	<p>이 선택적 파라미터는 ESET PROTECT 8.1 이상에서 배포되는 미러 도구에 적용됩니다.</p> <p>미러 도구는 x.x 또는 x.x.x.x 형식으로 파라미터 인수에 지정한 ESET PROTECT 저장소 버전과 호환되는 업데이트 파일(예: --compatibilityVersion 10.0 또는 --compatibilityVersion 8.1.13.0)을 다운로드합니다.</p> <p>--compatibilityVersion 파라미터는 미러에서 <a href="#">자동 업데이트(uPCU)</a>를 제외합니다. 사용자 환경에서 자동 업데이트(uPCU)가 필요하고 미러 크기를 줄이고 싶다면, --filterFilePath 파라미터를 사용합니다.</p>

ESET 저장소에서 다운로드되는 데이터의 양을 줄이려면 ESET PROTECT 9와 함께 배포된 미러 도구의 새 파라미터, --filterFilePath 및 --dryRun을 사용하는 것이 좋습니다.



1. JSON 형식으로 필터를 생성합니다(아래의 --filterFilePath 참조).
2. --dryRun 파라미터(아래 참조)를 사용하여 테스트 미러 도구 실행을 수행하고 필요한 경우 필터를 조정합니다.
3. --filterFilePath 파라미터 및 정의된 다운로드 필터와 함께 --intermediateRepositoryDirectory 및 --outputRepositoryDirectory 파라미터를 사용하여 미러 도구를 실행합니다.
4. 미러 도구를 정기적으로 실행하여 항상 최신 설치 관리자를 사용합니다.



파라미터	설명
--filterFilePath	<p>이 선택적 파라미터를 사용하면 미러 도구와 동일한 폴더에 배치된 <b>JSON</b> 형식의 텍스트 파일을 기준으로 ESET 보안 제품을 필터링합니다(예: --filterFilePath filter.txt).</p> <p><b>필터 구성 설명:</b></p> <p>제품 필터링용 구성 파일 형식은 구조가 다음과 같은 <b>JSON</b>입니다.</p> <ul style="list-style-type: none"> <li>루트 <b>JSON</b> 개체: <ul style="list-style-type: none"> <li>use_legacy(부울, 옵션) - true이면 레거시 제품이 포함됩니다.</li> <li>defaults(<b>JSON</b> 개체, 옵션) - 모든 제품에 적용될 필터 속성을 정의합니다. <ul style="list-style-type: none"> <li>languages(목록) - 포함할 언어의 ISO 언어 코드(예: 프랑스어 형식 "fr_FR")를 지정합니다. 기타 언어 코드는 <a href="#">아래 표</a>에 나와 있습니다. 더 많은 언어를 선택하려면 쉼표와 공백으로 구분합니다(예: ("en_US", "zh_TW", "de_DE")).</li> <li>platforms(목록) - 포함할 플랫폼입니다(["x64", "x86", "arm64"]).</li> </ul> </li> </ul> </li> </ul> <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p><b>!</b> platforms 필터를 신중하게 사용하십시오. 예를 들어, 미러 도구가 64비트 설치 관리자만 다운로드하고 인프라에 32비트 컴퓨터가 있는 경우 64비트 ESET 보안 제품은 32비트 컴퓨터에 설치되지 않습니다.</p> </div> <ul style="list-style-type: none"> <li>os_types(목록) - 포함할 OS 유형입니다(["windows"], ["linux"], ["mac"]).</li> <li>oproducts(<b>JSON</b> 개체 목록, 옵션) - 특정 제품에 적용할 필터 - 지정된 제품에 대해 defaults를 재지정합니다. 개체에는 다음과 같은 속성이 있습니다. <ul style="list-style-type: none"> <li>app_id(문자열) - name이 지정되지 않은 경우 필요합니다.</li> <li>name(문자열) - app_id가 지정되지 않은 경우 필요합니다.</li> <li>version(문자열) - 포함할 버전 또는 버전 범위를 지정합니다.</li> <li>languages(목록) - 포함할 언어의 ISO 언어 코드입니다(<a href="#">아래 표</a> 참조).</li> <li>platforms(목록) - 포함할 플랫폼입니다(["x64", "x86", "arm64"]).</li> <li>os_types(목록) - 포함할 OS 유형입니다(["windows"], ["linux"], ["mac"]).</li> </ul> </li> </ul> <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p><b>i</b> 필터에 적합한 값을 확인하려면 시험 실행 모드에서 미러 도구를 실행하고 생성된 CSV 파일에서 관련 제품을 찾습니다.</p> </div> <p><b>버전 문자열 형식 설명</b></p> <p>모든 버전 번호는 점으로 구분된 네 개의 숫자로 구성됩니다(예: 7.1.0.0). 버전 필터를 작성할 때 더 적은 숫자를 지정(예: 7.1)할 수 있으며, 나머지 숫자는 0이 됩니다(7.1은 7.1.0.0과 동일).</p> <p>버전 문자열은 다음의 두 형식 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>[&gt; &lt; = &lt;= &gt;= &lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))</li> </ul> <p>o 지정된 버전보다 큰/작은 또는 같은/작은 또는 같은/같은 버전을 선택합니다.</p> <ul style="list-style-type: none"> <li>&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;))) - &lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))</li> </ul> <p>o 하한보다 크거나 하한과 같고, 상한보다 작거나 상한과 같은 버전을 선택합니다. 비교는 버전 번호의 각 부분에 대한 숫자(왼쪽에서 오른쪽)로 나타냅니다.</p> <div style="border: 1px solid green; padding: 10px; margin: 10px 0;"> <p><b>JSON 예제</b></p> <pre> {   "use_legacy": true,   "defaults": {     "languages": [ "en_US" ],     "platforms": [ "x64", "x86" ]   },   "products": [     {       "app_id": "com.eset.apps.business.ees.windows",       "version": "7.1.0.0-8.0.0.0"     },     {       "app_id": "com.eset.apps.business.eea.windows",       "version": "&gt;7.1.0.0"     }   ] } </pre> </div> <p>--filterFilePath 파라미터는 이전 미러 도구 버전(ESET PROTECT 8.x에서 릴리스됨)에 사용된 --languageFilterForRepository, --productFilterForRepository, --downloadLegacyForRepository 파라미터를 대체합니다.</p>



파라미터	설명
--dryRun	<p>이 선택적 파라미터를 사용하면 미리 도구는 파일을 다운로드하지 않고 다운로드될 모든 패키지를 나열하는 .csv 파일을 생성합니다.</p> <p>필수 파라미터 --intermediateRepositoryDirectory 및 --outputRepositoryDirectory 없이 이 파라미터를 사용할 수 있습니다(예:)</p> <ul style="list-style-type: none"> <li>Windows: MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv</li> <li>Linux: sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv</li> </ul> <div style="border: 1px solid blue; padding: 5px;"> <p><b>i</b> 일부 ESET 설치 관리자는 언어 일반(multilang 언어 코드 포함)이며 미리 도구는 --filterFilePath에 언어를 지정하더라도 .csv 파일에 해당 설치 관리자를 나열합니다.</p> </div> <p>--dryRun 파라미터와 --intermediateRepositoryDirectory 및 --outputRepositoryDirectory 파라미터도 사용하는 경우 미리 도구는 outputRepositoryDirectory를 지우지 않습니다.</p>
--listUpdatableProducts	<p>(--excludedProducts을 사용하는 경우를 제외하고) Mirror Tool이 모듈 업데이트를 다운로드할 수 있는 모든 ESET 제품을 나열합니다.</p> <p>파라미터는 다음 Mirror Tool 버전으로부터 사용할 수 있습니다: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).</p>

## Mirror Tool 폴더 구조

기본적으로 --updateServer 파라미터를 지정하지 않으면 Mirror Tool은 HTTP 서버에 다음 폴더 구조를 만듭니다.

### HTTP 전용 미리 서버 사용 안 함

**!** 로컬 미리 서버가 HTTP 및 HTTPS 프로토콜을 사용하거나 HTTPS만 사용하는지 확인합니다. 미리 서버가 HTTP만 사용하는 경우 HTTP 서버에서 ESET 보안 제품의 최종 사용자 사용권 계약을 검색할 수 없으므로 소프트웨어 설치 클라이언트 작업을 사용할 수 없습니다.

Mirror Tool 기본 폴더	ESET 보안 제품	서버 업데이트(HTTP 서버 루트 위치에 따름)
mirror/eset_upd/era6	era6 미리 폴더는 다음 ESET 원격 관리 솔루션에 공통되는 사항입니다. ERA 6, ESMC 7 및 ESET PROTECT	미리에서 ESET PROTECT 10을(를) 업데이트하려면 <a href="#">업데이트 서버</a> 를 <code>http://your_server_address/mirror/eset_upd/era6</code> (으)로 설정합니다.
mirror/eset_upd/ep[버전으로 업그레이드]	Windows용 ESET Endpoint Antivirus/Security 버전 6.x(이상) 각 주 버전에는 해당 폴더가 있습니다(예: 10.x 버전의 경우 ep10).	<code>http://your_server_address/mirror/eset_upd/ep10</code> (버전 10.x의 예)
mirror/eset_upd/v5	Windows용 ESET Endpoint Antivirus/Security 버전 5.x	<code>http://your_server_address/mirror/eset_upd/v5</code>

### ESET 보안 제품 Linux/macOS

**!** HTTP 미리에서 Linux/macOS용 ESET 보안 제품을 업데이트하려면 --updateServer 파라미터를 지정하고 추가 폴더를 생성해야 합니다(아래 참조).

--updateServer	추가 Mirror Tool 폴더	ESET 보안 제품	서버 업데이트(HTTP 서버 루트 위치에 따름)
<code>http://update.eset.com/eset_upd/businesslinux</code>	mirror/eset_upd/BusinessLinux	ESET Endpoint Antivirus-용 Linux	<code>http://your_server_address/mirror/eset_upd/BusinessLinux</code>

--updateServer	추가 Mirror Tool 폴더	ESET 보안 제품	서버 업데이트(HTTP 서버 루트 위치에 따름)
<a href="http://update.eset.com/eset_upd/serverlinux">http://update.eset.com/eset_upd/serverlinux</a>	<a href="mirror/eset_upd/LinuxServer">mirror/eset_upd/LinuxServer</a>	ESET Server Security 용 Linux	<a href="http://your_server_address/mirror/eset_upd/LinuxServer">http://your_server_address/mirror/eset_upd/LinuxServer</a>
<a href="http://update.eset.com/eset_upd/businessmac">http://update.eset.com/eset_upd/businessmac</a>	<a href="mirror/eset_upd/BusinessMac">mirror/eset_upd/BusinessMac</a>	macOS용 ESET Endpoint Security 버전 7.x+	<a href="http://your_server_address/mirror/eset_upd/BusinessMac">http://your_server_address/mirror/eset_upd/BusinessMac</a>

## 언어 코드 표

언어	코드	언어	코드	언어	코드	언어	코드
한국어	ko	영어	en	러시아어	ru	일본어	ja
중국어	cn	프랑스어	fr	독일어	de	스페인어	es
히브리어	il	이탈리아어	it	포르투갈어	pt	그리스어	gr
폴란드어	pl	네덜란드어	nl	체코어	cz	헝가리어	hu
슬로바키아어	sk	크로아티아어	hr	슬로베니아어	sl	세르비아어	sr
루마니아어	ro	불가리아어	bg	마케도니아어	mk	알바니아어	al
우크라이나어	ua	벨라루스어	by	리투아니아어	lt	라트비아어	lv
에스토니아어	ee	레토니아어	lv	몰도바어	md	우즈베크어	uz
타지크어	tg	키르기스어	kg	카자흐어	kz	아제르바이잔어	az
아제르바이잔어	az	조지아어	ge	아르메니아어	am	벨라루스어	by
우크라이나어	ua	러시아어	ru	우크라이나어	ua	러시아어	ru

```
sudo ./MirrorTool --mirrorType regular \
--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \
--offlineLicenseFilename /tmp/mirrorTool/offline.lf \
--outputDirectory /tmp/mirrorTool/mirror
```

다음은 선택한 제품, 언어 및 *filter.txt* 파일에 정의된 레거시 파일의 다운로드를 활성화한 오프라인 저장소에 대한 고급 구성의 예입니다(위의 세부 정보에서 --filterFilePath 파일 내용 예제 참조).

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--filterFilePath filter.txt
```

- i** 명령줄 기록에서 중요한 데이터(예: 패스워드)가 포함된 명령을 제거하는 것이 좋습니다.
- 1.history를 실행하여 기록에서 모든 명령 목록을 확인합니다.
  - 2.history -d line\_number를 실행합니다(명령의 줄 수 지정). 또는 history -c를 실행하여 전체 명령줄 기록을 제거합니다.

## 미러 도구 및 업데이트 설정

- 모듈 업데이트에 대한 다운로드를 자동화하려면 미러 도구 실행을 예약하면 됩니다. 이렇게 하려면 웹 콘솔을 열고 **클라이언트 작업 > 운영 체제 > 명령 실행**으로 이동합니다. 실행할 명령줄(MirrorTool.exe 경로 포함)과 적절한 트리거를 선택합니다(예: CRON, 다음 시간 간격일 경우 00 \*\*\*? \*). 또는 Windows 작업 스케줄러 또는 Linux의 Cron을 사용할 수 있습니다.
- 클라이언트 컴퓨터에서 업데이트를 구성하려면 새 정책을 만들고 미러 주소 또는 공유 폴더를 가리키도록 **업데이트 서버**를 구성하십시오.

# macOS의 구성 요소 설치

대부분의 설치 시나리오에서는 여러 다른 네트워크 아키텍처를 수용하거나, 성능 요구를 충족하거나, 기타 이유로 인해 컴퓨터마다 다른 ESET PROTECT 구성 요소를 설치해야 합니다.

**i** macOS는 클라이언트로서만 지원됩니다. [ESET Management 에이전트](#) 및 [macOS용 ESET 제품](#)은 macOS에 설치할 수 있습니다. 그러나 ESET PROTECT 서버는 macOS에 설치할 수 없습니다.

## 에이전트 설치 - macOS

다음의 두 가지 방법으로 ESET Management Agent를 macOS에 설치할 수 있습니다.

- 원격 - 서버 작업 **에이전트 배포** 사용. ESET Management 에이전트를 원격으로 배포할 때 문제가 발생하는 경우(서버 작업 **에이전트 배포**가 실패 상태로 끝남) [에이전트 배포 문제 해결](#)을 참조하십시오.
- 로컬 - 아래의 지침을 참조하십시오.

### 필수 구성 요소

- 서버 컴퓨터에 ESET PROTECT 서버 및 ESET PROTECT 웹 콘솔이 설치되어 있어야 합니다.
- 로컬 드라이브에 에이전트 [인증서](#)가 생성되고 준비되어 있어야 합니다.
- 로컬 드라이브에 [인증 기관](#)이 준비되어 있어야 합니다(서명되지 않은 인증서에만 필요함).

### 설치

macOS에 로컬로 ESET Management Agent 구성 요소를 설치하려면 다음 단계를 따릅니다.

**!** 위에 나열된 설치 필수 구성 요소를 모두 충족하는지 확인합니다.

1. [ESET 다운로드 사이트](#) 또는 시스템 관리자로부터 설치 파일(독립 실행형 에이전트 설치 관리자 *.dmg*)을 가져옵니다.
2. *Agent-MacOSX-x86\_64.dmg* 파일을 두 번 클릭한 다음 *.pkg* 파일을 두 번 클릭하여 설치를 시작합니다.
3. 설치를 계속 진행합니다. 메시지가 표시되면 **서버 연결** 데이터를 입력합니다.
  - **서버 호스트 이름:** ESET PROTECT 서버의 호스트 이름이나 IP 주소
  - **서버 포트:** 에이전트 - 서버 통신을 위한 포트, 기본값: 2222
  - **프록시 사용:** 에이전트 - 서버 연결용 HTTP 프록시를 사용하려는 경우 클릭합니다.

이 프록시 설정은 ESET Management 에이전트와 ESET PROTECT 서버 간의 (복제)에만 사용되며 업데이트 캐시에는 사용되지 않습니다.

- **프록시 호스트 이름:** HTTP 프록시 시스템의 호스트 이름 또는 IP 주소입니다.
  - **프록시 포트:** 기본값은 3182입니다.
  - **사용자 이름, 비밀번호:** 인증을 사용할 경우 프록시에 사용되는 자격 증명을 입력합니다.
- 나중에 [정책](#)에서 프록시 설정을 변경할 수 있습니다. [프록시](#)는 프록시를 통한 에이전트 - 서버 연결을 구성하려는 경우 먼저 설치해야 합니다.

4. 피어 [인증서](#)와 이 인증서의 비밀번호를 선택합니다. 경우에 따라 [인증 기관](#)을 추가할 수도 있습니다.

**A** 인증서 비밀번호에는 문자를 포함할 수 없습니다: " \ 이러한 문자를 사용하면 에이전트를 초기화하는 동안 심각한 오류가 발생합니다.

5. 설치 위치를 검토하고 **설치**를 클릭합니다. 컴퓨터에 에이전트가 설치됩니다.

6. ESET Management 에이전트 로그 파일은 다음 경로에서 찾을 수 있습니다.

```
/Library/Application Support/com.eset.remoteadministrator.agent/Logs/  
/Users/%user%/Library/Logs/EraAgentInstaller.log
```

**!** 에이전트와 ESET PROTECT 서버 간의 통신 프로토콜은 인증을 지원하지 않습니다. 인증을 요구하는 ESET PROTECT 서버에 에이전트 통신을 전달하는 데 사용되는 프록시 솔루션은 작동되지 않습니다. 웹 콘솔이나 에이전트에 대해 기본값이 아닌 포트를 사용하도록 선택하면 방화벽을 조정해야 할 수 있습니다. 조정하지 않으면 설치에 실패할 수 있습니다.

## ISO 이미지

ISO 이미지 파일은 ESET PROTECT 설치 관리자를 [다운로드](#)할 수 있는 형식 중 하나입니다(일체형 설치 관리자 범주). ISO 이미지에는 다음이 포함되어 있습니다.

- ESET PROTECT 설치 관리자 패키지
- 각 구성 요소의 별도 설치 관리자

ISO 이미지는 모든 ESET PROTECT 설치 관리자를 한 곳에 모아두려는 경우에 유용합니다. 또한 ISO 이미지를 사용하면 설치를 실행해야 할 때마다 ESET 웹 사이트에서 설치 관리자를 다운로드할 필요도 없습니다. ISO 이미지는 가상 컴퓨터에 ESET PROTECT를 설치하려는 경우에도 유용합니다.

## DNS 서비스 레코드

### DNS 리소스 레코드를 설정하려면

1. DNS 서버(도메인 컨트롤러의 DNS 서버)에서 **제어판 > 관리 도구**로 이동합니다.
2. DNS 값을 선택합니다.
3. DNS 관리자의 트리에서 **\_tcp**를 선택하고 새 **서비스 위치(SRV)** 레코드를 생성합니다.
4. DNS 표준 규칙에 따라 **서비스** 필드에 서비스 이름을 입력하고 서비스 이름 앞에 밑줄(\_)을 입력합

니다(\_era와 같은 자체 서비스 이름 사용).

5. **프로토콜** 필드에 `_tcp` 형식으로 tcp 프로토콜을 입력합니다.

6. **포트 번호** 필드에 포트 2222를 입력합니다.

7. 이 서비스를 제공하는 **호스트** 필드에 ESET PROTECT 서버의 FQDN(정규화된 도메인 이름)을 입력합니다.

8. **확인** > **완료**를 클릭하여 레코드를 저장합니다. 레코드가 목록에 표시됩니다.

## DNS 레코드를 확인하려면

1. 도메인의 아무 컴퓨터에나 로그인한 후 명령 프롬프트(cmd.exe)를 엽니다.

2. 명령 프롬프트에 `nslookup`을 입력하고 **Enter** 키를 누릅니다.

3. `set querytype=srv`를 입력하고 **Enter** 키를 누릅니다.

4. `_era._tcp.domain.name`을 입력하고 **Enter** 키를 누릅니다. 서비스 위치가 올바르게 표시됩니다.

**i** 다른 컴퓨터에 ESET PROTECT 서버를 설치할 때 "이 서비스를 제공하는 호스트:" 값을 새 서버의 FQDN으로 반드시 변경해야 합니다.

## ESET PROTECT 오프라인 설치 시나리오

인터넷에 접속할 수 없는 환경에서 ESET PROTECT 및 해당 구성 요소를 설치하려면 (Windows에 ESET PROTECT 제품을 설치한 상태에서) 고급 설치 지침을 따르십시오.

### 인터넷에 연결된 컴퓨터에서

1. 공유 네트워크 폴더를 생성합니다.
2. 다음 설치 관리자를 공유 폴더에 다운로드합니다.
  - [ESET PROTECT 통합형 설치 관리자를 사용하여 업그레이드](#)
  - [지원되는 JDK 패키지](#)(웹 콘솔에 필요)
  - ESET Management Agent 설치 관리자
  - ESET 보안 제품 설치 관리자(예: ESET Endpoint Security)

### 동일한 로컬 네트워크에 있는 오프라인 상태의 Windows 컴퓨터에서

1. 네트워크 공유 폴더의 설치 관리자를 ESET PROTECT 제품이 설치될 오프라인 Windows 컴퓨터에 복사합니다.

2. JDK 패키지를 설치합니다.
3. 통합형 설치 관리자를 사용하여 Windows에 [ESET PROTECT을\(를\) 설치](#)합니다. 설치하는 동안 **나중에 활성화**를 선택합니다.
4. [오프라인 라이선스](#)로 ESET PROTECT 제품을 활성화합니다.
5. [에이전트 설치 관리자 스크립트](#)를 통해 오프라인 환경의 컴퓨터에 ESET Management 에이전트를 배포합니다. 새 URL을 사용하도록 설치 스크립트를 수정하여 공유 네트워크 폴더의 에이전트 설치 패키지에 접근할 수 있게 만듭니다.
6. [소프트웨어 설치 작업](#)을 사용하여 ESET 보안 제품을 워크스테이션에 배포합니다. <Choose package>을 선택하고 로컬 저장소에서 설치 패키지를 사용자 지정 URL을 입력합니다.
7. [오프라인 라이선스로 관리되는 엔드포인트를 활성화](#)합니다.
8. [ESET LiveGrid®](#)를 비활성화합니다.



로컬 업데이트 저장소를 사용하여 [오프라인 ESET 인프라를 최신 업데이트 상태로 유지](#)하는 것이 좋습니다. ESET 보안 제품 모듈을 정기적으로 업데이트합니다. 모듈이 업데이트되지 않은 경우 ESET PROTECT 웹 콘솔은 컴퓨터를 **업데이트되지 않음**으로 플래그 지정합니다. 이 웹 콘솔 경고를 일시 중지하려면 목록에서 컴퓨터를 클릭하고 오른쪽 마우스 버튼 메뉴에서 **음소거**를 선택합니다.

ESET PROTECT 업그레이드에 대한 지침은 [오프라인 환경에서 ESET PROTECT 구성 요소 업그레이드](#)를 참조하십시오.

## 업그레이드 절차

ESET PROTECT 서버 및 기타 ESET PROTECT 구성 요소를 업그레이드하는 다양한 방법이 있습니다. [마이그레이션 및 다시 설치 절차](#)도 참조하십시오.



ESET PROTECT 10.0(으)로 업그레이드하기 전에 [지원되는 운영 체제](#)가 있는지 확인하십시오. 지원되지 않는 이전 DB를 설치한 경우(MySQL 5.5 또는 Microsoft SQL 2008/2012) ESET PROTECT 서버를 업그레이드하기 전에 [DB를 호환되는 DB 버전](#)으로 업그레이드합니다.

### 이전 ERA 5.x/6.5 또는 ESMC 7.0/7.1

ERA 5.x/6.x 또는 ESMC 7.0/7.1이 있는 경우:

- ESET PROTECT 10.0(으)로 직접 업그레이드하는 것은 지원되지 않습니다.
- ESET PROTECT 10.0을(를) 새로 설치합니다.

ESMC 7.2에서 ESET PROTECT 10.0(으)로 직접 업그레이드할 수 있습니다.

### ESMC 7.2 또는 이전 ESET PROTECT 버전을 ESET PROTECT 10.0 버전으로 업그레이드

업그레이드 절차 중 하나를 선택합니다.



업그레이드 절차	운영 체제	설명
웹 콘솔의 <a href="#">구성 요소 업그레이드</a> 작업	Windows/Linux	
<a href="#">ESET PROTECT 10.0 통합형 설치 관리자를 사용하여 업그레이드</a>	Windows	통합형 설치 관리자는 기존 버전을 통합형 설치 관리자를 통해 설치한 경우에 권장되는 업그레이드 옵션입니다(Microsoft SQL DB 및 Apache Tomcat 기본 설치가 있는 경우).
<a href="#">수동 구성 요소 기반 업그레이드</a>	Linux	고급 사용자용 Linux 지침.
<a href="#">ESET PROTECT 가상 어플라이언스 업그레이드</a>	Linux (가상 어플라이언스)	

**i** 실행 중인 각 ESET PROTECT 구성 요소의 버전을 조회하려면 ESET PROTECT 서버 버전을 확인합니다. ESET PROTECT 웹 콘솔의 [정보](#) 페이지로 이동하여 [전체 ESET PROTECT 구성 요소 버전 목록](#)을 참조하십시오.

## ESET PROTECT 구성 요소 업그레이드 작업

### 업그레이드하기 전 권장 사항

ESET PROTECT 웹 콘솔에서 사용할 수 있는 [ESET PROTECT 구성 요소 업그레이드](#) 작업을 사용하여 ESET PROTECT 인프라를 업그레이드하는 것이 좋습니다. 업그레이드하기 전에 여기에서 지침을 주의 깊게 검토하십시오.

**A** ESET PROTECT 서버 또는 웹 콘솔을 실행하는 컴퓨터에서 구성 요소 업그레이드에 실패할 경우 웹 콘솔에 원격으로 로그인하지 못할 수 있습니다. 따라서 이 업그레이드를 수행하기 전에 서버 컴퓨터에 대해 물리적 접근을 구성하는 것이 좋습니다. 컴퓨터에 대해 물리적 접근을 구성할 수 없는 경우 원격 워크스테이션을 사용하여 관리 권한으로 컴퓨터에 로그인할 수 있는지 확인합니다. 이 작업을 수행하기 전에 ESET PROTECT 서버 및 모바일 장치 커넥터 DB를 [백업](#)하는 것이 좋습니다. 가상 어플라이언스를 백업하려면 스냅샷을 생성하거나 가상 컴퓨터를 복제합니다.

[ESMC 가상 어플라이언스에서 업그레이드하십니까?](#)

[ESET PROTECT 서버 인스턴스가 장애 조치\(Failover\) 클러스터에 설치되어 있습니까?](#)

ESET PROTECT 서버 인스턴스가 장애 조치(Failover) 클러스터에 설치된 경우 각 클러스터 노드에서 ESET PROTECT 서버 구성 요소를 수동으로 업그레이드해야 합니다. ESET PROTECT 서버를 업그레이드한 후 [구성 요소 업그레이드](#) 작업을 실행하여 인프라 나머지 항목(예: 클라이언트 컴퓨터의 ESET Management Agent)을 업그레이드합니다.

ESMC 버전 7.2 이상에서만 ESET PROTECT 10.0(으)로 업그레이드할 수 있습니다.

ESET PROTECT에서는 [새 버전의 ESET PROTECT 서버를 사용할 수 있게 되면](#) 자동으로 알립니다.

업그레이드를 실행하기 전에 먼저 다음 데이터를 백업합니다.

- 모든 인증서(인증 기관, 서버 인증서, 프록시 및 에이전트 인증서)
- [인증 기관 인증서](#)를 이전 ESET PROTECT 서버에서 `.der` 파일로 내보내고 외부 저장소에 저장합니다.
- [피어 인증서](#)(ESET Management Agent, ESET PROTECT 서버용) 및 개인 키 `.pfx` 파일을 이전 ESET PROTECT 서버에서 내보내고 외부 저장소에 저장합니다.

**!** [ESMC/ESET PROTECT 데이터베이스](#) 지원되지 않는 이전 DB를 설치한 경우(MySQL 5.5 또는 Microsoft SQL 2008/2012) ESET PROTECT 서버를 업그레이드하기 전에 [DB를 호환되는 DB 버전](#)으로 업그레이드합니다.

ESET PROTECT 10.0(으)로 업그레이드하기 전에 [지원되는 운영 체제](#)가 있는지 확인하십시오.

ESET 보안 제품을 업그레이드하려면 최신 설치 관리자 패키지를 사용해 [소프트웨어 설치 작업](#)을 실행하여 기존 제품 위에 최신 버전을 설치합니다.

### 권장 업그레이드 절차

1. ESET PROTECT 서버 업그레이드 - [ESET PROTECT 구성 요소 업그레이드](#) 작업의 대상으로 ESET PROTECT

서버를 사용하는 컴퓨터만 선택합니다.

2. 일부 클라이언트 컴퓨터(테스트 샘플로 운영 체제 및 비트 수마다 클라이언트 하나 이상)를 선택하여 **ESET PROTECT 구성 요소 업그레이드** 작업을 실행합니다.

네트워크 부하를 제한하려면 [ESET Bridge HTTP 프록시](#) (또는 캐시가 활성화된 다른 투명한 웹 프록시)를 사용하는 것이 좋습니다. 테스트 클라이언트 컴퓨터가 설치 관리자의 다운로드/캐시를 트리거합니다. 작업을 다시 실행하면 설치 관리자가 캐시에서 바로 클라이언트 컴퓨터에 배포됩니다.

3. ESET Management Agent를 업그레이드한 컴퓨터가 ESET PROTECT 서버에 연결되면 나머지 클라이언트의 업그레이드를 진행합니다.

**i** 네트워크에서 관리되는 모든 컴퓨터에서 ESET Management Agent를 업그레이드하려면 정적 그룹 모두를 **ESET PROTECT 구성 요소 업그레이드** 작업의 대상으로 선택합니다. 작업은 이미 최신 ESET Management 에이전트를 실행한 컴퓨터를 건너뛵니다. ESET PROTECT 은(는) 관리되는 컴퓨터에서 [ESET Management 에이전트의 자동 업그레이드](#)를 지원합니다.

**구성 요소가 자동으로 업그레이드됩니다.**

- ESET PROTECT 서버
- ESET Management 에이전트
- ESET PROTECT 웹 콘솔 - Apache Tomcat이 ESET PROTECT 가상 어플라이언스를 포함하여 Windows 및 Linux 배포 모두에서 기본 설치 폴더에 설치된 경우에만 적용됩니다(예: `/var/lib/tomcat8/webapps/`, `/var/lib/tomcat7/webapps/`, `/var/lib/tomcat/webapps/`).

### 웹 콘솔 업그레이드 제한 사항

○ Apache Tomcat은 구성 요소 업그레이드 작업을 통한 ESET PROTECT 웹 콘솔 업그레이드 동안 업그레이드되지 않습니다.

**!** ○ ESET PROTECT 웹 콘솔 업그레이드는 Apache Tomcat이 사용자 지정 위치에 설치된 경우에는 작동하지 않습니다.

○ 사용자 지정 버전의 Apache Tomcat이 설치(Tomcat 서비스 수동 설치)된 경우 통합형 설치 관리자 또는 구성 요소 업그레이드 작업을 통한 후속 ESET PROTECT 웹 콘솔 업그레이드는 지원되지 않습니다.

- ESET PROTECT 모바일 장치 커넥터

**수동으로 업그레이드해야 하는 구성 요소:**

### ESET 구성 요소

- [ESET Rogue Detection Sensor](#) - 업그레이드 시 [소프트웨어 설치 작업](#)을 사용합니다. 또는 이전 버전 위에 최신 버전을 설치합니다([Windows](#) 또는 [Linux](#)의 설치 지침을 따름). ESMC 7.2 이상을 사용하는 RD Sensor를 설치한 경우 새 RD Sensor 릴리스가 없으므로 업그레이드할 필요가 없습니다.

### 타사 구성 요소

ESET 구성 요소 외에도 ESET PROTECT에서는 수동 업그레이드가 필요한 타사 구성 요소를 사용합니다.

ESET PROTECT 웹 콘솔에서 **빠른 링크 > 서버 구성 요소**를 클릭하여 사용할 수 있는 최신 버전의 타사 구성 요소를 확인합니다.



- 최대한 빨리 최신 버전의 타사 구성 요소를 설치하는 것이 좋습니다. 사용할 수 있는 최신 버전은 ESET PROTECT 서버 실행에 사용되는 운영 체제에 따라 다를 수 있습니다.
- ESET PROTECT 가상 어플라이언스는 타사 구성 요소에 대해 사용 가능한 업그레이드를 보고하지 않습니다.

ESET PROTECT 웹 콘솔은 아래 나열된 버전보다 이전 버전에 대한 업그레이드를 권장합니다.

타사 구성 요소:	버전:	참고:
Microsoft SQL Server	2019 (빌드 15.0.4261.0)	<a href="#">SQL Server 데이터베이스 엔진의 버전과 에디션</a> 을 확인하고 최신 <a href="#">누적 업데이트</a> 를 설치합니다.
MySQL	8.0.0.0	ESET PROTECT 웹 콘솔에서 <b>도움말 &gt; 정보</b> 를 클릭하여 설치된 데이터베이스 버전을 확인합니다.
운영 체제	Windows Server 2016	ESET PROTECT은(는) Linux에 대해 사용 가능한 업데이트를 보고하지 않습니다.
Apache Tomcat	9.0.65	설치된 Apache Tomcat 버전을 확인합니다. <ul style="list-style-type: none"> <li>• Windows - C:\Program Files\Apache Software Foundation\[Tomcat 폴더] \텍스트 편집기의 <b>RELEASE-NOTES</b> 파일을 찾아서 열고 버전 번호를 확인합니다.</li> <li>• Linux - 터미널 명령 <code>tomcat version</code>을 실행합니다.</li> </ul>
Java	17.0	설치된 Java 버전을 확인합니다. <ul style="list-style-type: none"> <li>• Windows - 명령 프롬프트를 열고 <code>java -version</code>을 실행합니다.</li> <li>• Linux - 터미널 명령 <code>java -version</code>을 실행합니다.</li> </ul>

- ! ESET PROTECT 모바일 장치 관리/커넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

타사 구성 요소에 대한 업그레이드 지침을 따릅니다.

- [DB 서버](#)
- [운영 체제](#)
- [Apache Tomcat](#)
- [Java Runtime Environment](#)

### Apache HTTP Proxy 사용자

- ! ESET PROTECT 10.0부터 ESET Bridge이(가) Apache HTTP Proxy를 대체합니다. Apache HTTP Proxy가 제한된 지원에 도달했습니다. Apache HTTP Proxy를 사용하는 경우, [ESET Bridge\(으\)로 마이그레이션](#)하는 것이 좋습니다.

## 문제 해결

- 업그레이드된 컴퓨터에서 [ESET PROTECT 저장소에 접근](#)할 수 있는지 확인합니다.
- 이미 최신 버전으로 업그레이드된 구성 요소가 하나 이상 있는 경우 ESET PROTECT 구성 요소 업그레이드 작업을 재실행하면 작업이 수행되지 않습니다.
- ESET PROTECT 웹 콘솔이 로드되지 않거나 로그인 중에 오류가 표시되면 [웹 콘솔 문제 해결](#)을 참조하십시오.

- 명확한 실패 사유가 없는 경우 구성 요소를 수동으로 업그레이드할 수 있습니다. [Windows](#) 또는 [Linux](#)에 대한 지침을 참조하십시오.
- 업그레이드 문제 해결에 대한 추가 제안 사항은 [일반 문제 해결 정보](#)를 참조하십시오.

## ESET PROTECT 10.0 통합형 설치 관리자를 사용하여 업그레이드

ESET PROTECT 10.0 통합형 설치 관리자를 사용하여 ESMC 7.2 또는 이전 ESET PROTECT 버전을 최신 ESET PROTECT 10.0 버전으로 업그레이드합니다.

통합형 설치 관리자는 기존 버전을 통합형 설치 관리자를 통해 설치한 경우에 권장되는 업그레이드 옵션입니다(Microsoft SQL DB 및 Apache Tomcat 기본 설치가 있는 경우).

ESET PROTECT 10.0 [통합형 설치 관리자](#)는 기본적으로 Microsoft SQL Server Express 2019를 설치합니다.

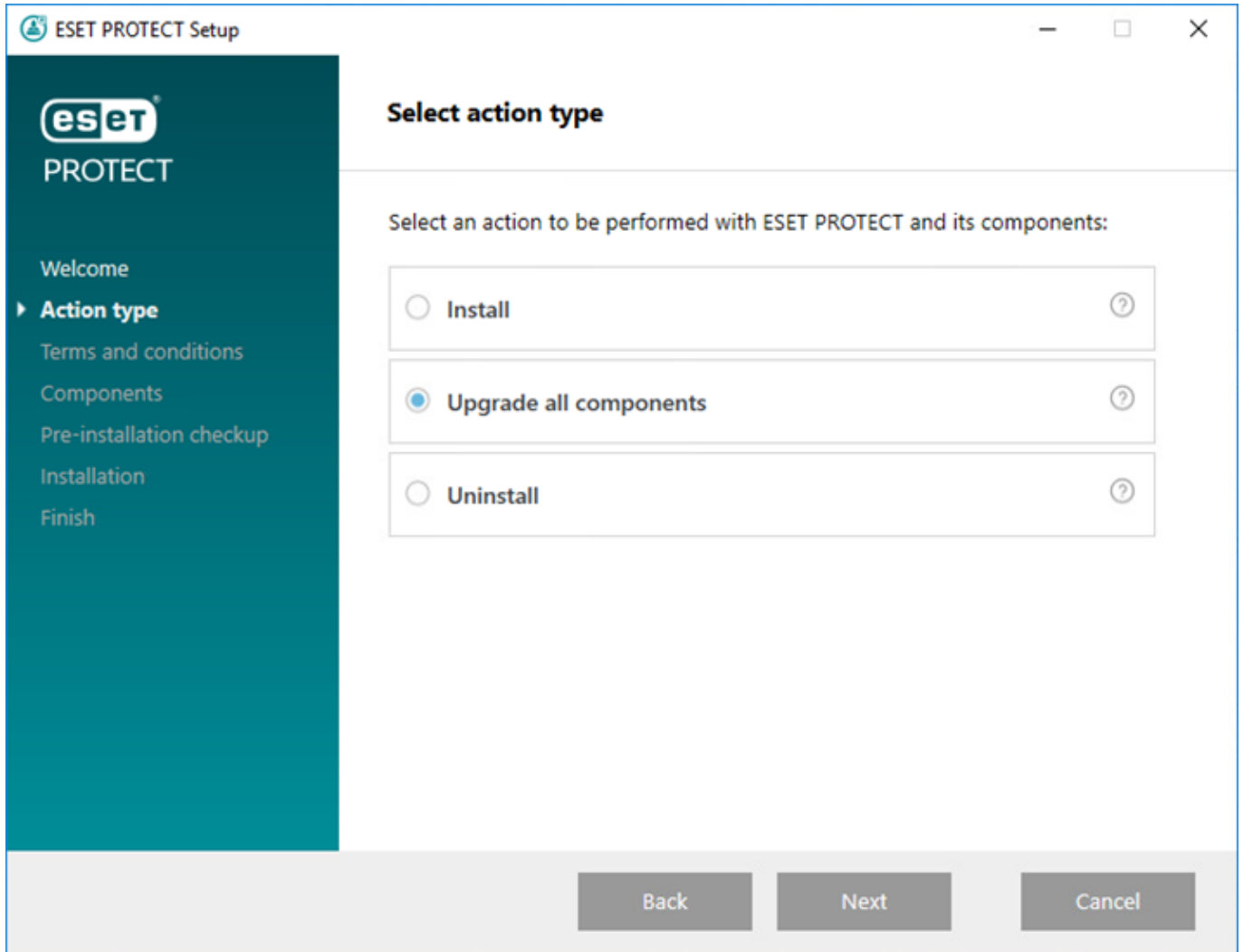
이전 Windows 버전(Server 2012 또는 SBS 2011)을 사용하는 경우 기본적으로 Microsoft SQL Server Express 2014가 설치됩니다.

설치 관리자는 데이터베이스 인증을 위해 임의의 패스워드를 자동으로 생성합니다(%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini에 저장됨).

- Microsoft SQL Server Express는 각 관계형 DB의 크기가 10GB로 제한되어 있습니다. Microsoft SQL Server Express를 사용하지 않는 것이 좋습니다.
- 엔터프라이즈 환경 또는 대규모 네트워크에서.
  - [ESET Inspect](#)과(와) 함께 ESET PROTECT을(를) 사용하려는 경우

- ESMC 버전 7.2 이상에서만 ESET PROTECT 10.0(으)로 업그레이드할 수 있습니다. 업그레이드를 실행하기 전에 먼저 다음 데이터를 백업합니다.
- 모든 인증서(인증 기관, 서버 인증서, 프록시 및 에이전트 인증서)
  - [인증 기관 인증서](#)를 이전 ESET PROTECT 서버에서 .der 파일로 내보내고 외부 저장소에 저장합니다.
  - [피어 인증서](#)(ESET Management Agent, ESET PROTECT 서버용) 및 개인 키 .pfx 파일을 이전 ESET PROTECT 서버에서 내보내고 외부 저장소에 저장합니다.
  - [ESMC/ESET PROTECT 데이터베이스](#) 지원되지 않는 이전 DB를 설치한 경우(MySQL 5.5 또는 Microsoft SQL 2008/2012) ESET PROTECT 서버를 업그레이드하기 전에 [DB를 호환되는 DB 버전](#)으로 업그레이드합니다.
- ESET PROTECT 10.0(으)로 업그레이드하기 전에 [지원되는 운영 체제](#)가 있는지 확인하십시오.

1. Setup.exe를 실행합니다.
2. 언어를 선택하고 다음을 클릭합니다.
3. 모든 구성 요소 업그레이드를 선택하고 다음을 클릭합니다.



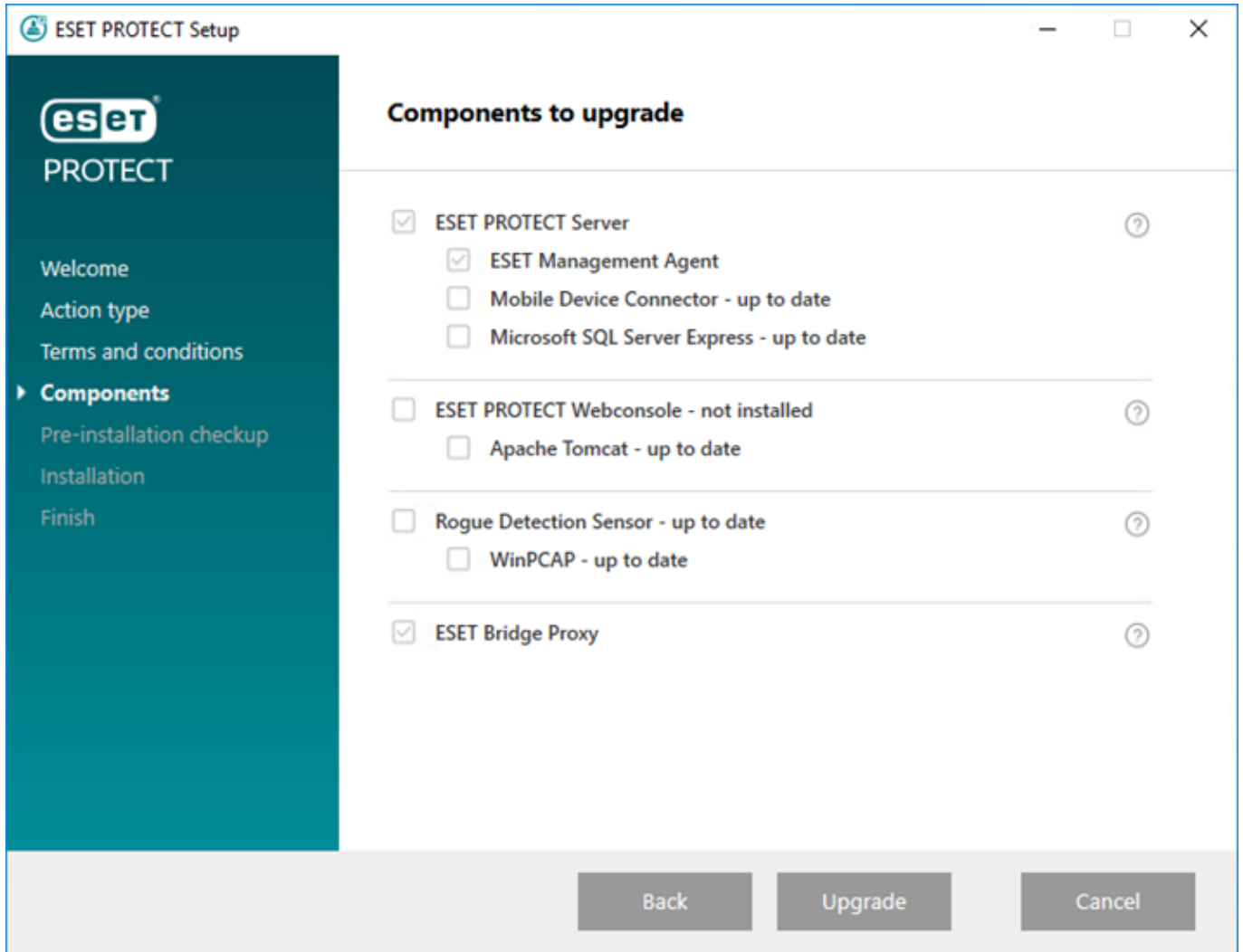
4. 최종 사용자 사용권 계약을 읽어보고 동의한 후 다음을 클릭합니다.

5. 구성 요소에서 업그레이드할 수 있는 ESET PROTECT 구성 요소를 검토하고 다음을 클릭합니다.

### Apache Tomcat 및 웹 콘솔 업그레이드 제한 사항

- 사용자 지정 버전의 Apache Tomcat이 설치(Tomcat 서비스 수동 설치)된 경우 통합형 설치 관리자 또는 구성 요소 업그레이드 작업을 통한 후속 ESET PROTECT 웹 콘솔 업그레이드는 지원되지 않습니다.
- Apache Tomcat을 업그레이드하면 다음에 있는 *era* 폴더가 제거됩니다. *C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\webapps\era* 폴더를 사용하여 추가 데이터를 저장하려면 업그레이드 전에 데이터를 백업해야 합니다.
- 이때 *C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\webapps*는 추가 데이터를 포함하고(*era* 및 *ROOT* 폴더 아님) Apache Tomcat 업그레이드가 실행되지 않으며 웹 콘솔만 업그레이드됩니다.
- 웹 콘솔 및 Apache Tomcat 업그레이드 시 [오프라인 도움말](#) 파일이 지워집니다. ESMC 또는 이전 ESET PROTECT 버전에서 오프라인 도움말을 사용한 경우, 업그레이드한 후 ESET PROTECT 10.0용으로 다시 생성하여 ESET PROTECT 버전과 일치하는 최신 오프라인 도움말이 있는지 확인하십시오.

⚠ Apache HTTP Proxy가 설치된 Windows 컴퓨터에서 통합형 설치 관리자를 실행하면, 설치 관리자가 자동으로 Apache HTTP Proxy를 제거하고 대신 [ESET Bridge](#)을(를) 설치합니다.



6.사전 설치 점검에 따라 시스템이 모든 필수 구성 요소를 충족하는지 확인합니다.

7.업그레이드를 클릭하여 ESET PROTECT 업그레이드를 시작합니다. 시스템 및 네트워크 구성에 따라 업그레이드에 다소 시간이 걸릴 수 있습니다.

8.업그레이드가 완료되면 **완료**를 클릭합니다.

9.ESET PROTECT 업그레이드 후 구성 요소 업그레이드 작업을 사용하여 관리되는 컴퓨터에서 ESET Management 에이전트를 업그레이드합니다. ESET PROTECT 은(는) 관리되는 컴퓨터에서 [ESET Management 에이전트의 자동 업그레이드](#)를 지원합니다.

## 데이터베이스 서버 백업/업그레이드

ESET PROTECT에서는 DB를 사용하여 클라이언트 데이터를 저장합니다. 다음 섹션에서는 ESET PROTECT 서버(나 ESMC 서버) 데이터베이스 또는 MDM 데이터베이스의 [백업](#)과 [업그레이드](#)에 대해 자세히 설명합니다.

- ESET PROTECT 서버에서 사용하도록 구성된 DB가 없는 경우 **Microsoft SQL Server Express**가 설치 관리자에 포함됩니다. ESET PROTECT 10.0 [통합형 설치 관리자](#)는 기본적으로 Microsoft SQL Server Express 2019를 설치합니다.

0이전 Windows 버전(Server 2012 또는 SBS 2011)을 사용하는 경우 기본적으로 Microsoft SQL Server Express 2014가 설치됩니다.

o 설치 관리자는 데이터베이스 인증을 위해 임의의 패스워드를 자동으로 생성합니다(%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini에 저장됨).

Microsoft SQL Server Express는 각 관계형 DB의 크기가 10GB로 제한되어 있습니다. Microsoft SQL Server Express를 사용하지 않는 것이 좋습니다.

- 엔터프라이즈 환경 또는 대규모 네트워크에서.
- [ESET Inspect](#)과(와) 함께 ESET PROTECT을(를) 사용하려는 경우

- 지원되지 않는 이전 DB를 설치한 경우(MySQL 5.5 또는 Microsoft SQL 2008/2012) ESET PROTECT 서버를 업그레이드하기 전에 [DB를 호환되는 DB 버전](#)으로 업그레이드합니다.

[ESET PROTECT 데이터베이스 마이그레이션](#)도 참조하십시오.

Microsoft SQL Server에 대한 다음 요구 사항이 충족되어야 합니다.

- [지원되는 Microsoft SQL Server 버전](#)을 설치합니다. 설치하는 동안 **혼합 모드** 인증을 선택하십시오.
- Microsoft SQL Server를 이미 설치한 경우 인증을 **혼합 모드(SQL Server 인증 및 Windows 인증)**로 설정하십시오. 이렇게 하려면 이 [지식 베이스 문서](#)의 지침을 따르십시오. **Windows 인증**을 사용하여 Microsoft SQL Server에 로그인하려면 이 [지식 베이스 문서](#)의 단계를 따르십시오.
- SQL Server에 대해 TCP/IP 연결을 허용합니다. 이렇게 하려면 이 [지식 베이스 문서 II. SQL DB에 대해 TCP/IP 연결 허용](#)의 지침을 따르십시오.

- Microsoft SQL Server(DB 및 사용자)를 구성하고 관리하려면 [SSMS\(SQL Server Management Studio\)](#)를 [다운로드](#)하십시오.

**i** • [도메인 컨트롤러에 SQL Server를 설치하지 마십시오](#)(예: Windows SBS/Essentials). ESET PROTECT 제품을 다른 서버에 설치하거나 설치 중에 SQL Server Express 구성 요소를 선택하지 않는 것이 좋습니다(이 경우 기존 SQL 또는 MySQL Server를 사용하여 ESET PROTECT DB를 실행해야 함).

## DB 서버 백업 및 복원

모든 ESET PROTECT 정보와 설정은 DB에 저장됩니다. 데이터 손실을 방지하려면 정기적으로 DB를 백업하는 것이 좋습니다. 나중에 ESET PROTECT을(를) 새 서버로 마이그레이션할 때 백업을 사용할 수 있습니다. DB에 대해서는 아래의 해당 섹션을 참조하십시오.

- DB 및 로그 파일 이름은 제품 이름을 ESET Security Management Center에서 ESET PROTECT로 변경한 후에도 그대로 유지됩니다.
- ESET PROTECT 가상 어플라이언스를 사용하는 경우 [VA 데이터베이스 백업 지침](#)을 따르십시오.

## Microsoft SQL 백업 예제

Microsoft SQL DB를 파일에 백업하려면 아래 표시된 예제를 따르십시오.



이러한 예제는 기본 설정(예:기본 DB 이름 및 DB 연결 설정)에서 사용하기 위한 것입니다. 기본 설정의 변경 사항을 적용하려면 백업 스크립트를 사용자 지정해야 합니다.  
아래 명령을 실행하려면 충분한 권한이 있어야 합니다. 로컬 관리자 사용자 계정을 사용하지 않는 경우 백업 경로(예: 'C:\USERS\PUBLIC\BACKUPFILE')를 변경해야 합니다.

## 한 번 DB 백업

Windows 명령 프롬프트에서 이 명령을 실행하여 **BACKUPFILE** 파일에 백업을 만듭니다.

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE' "
```



이 예제에서 **HOST**는 IP 주소 또는 호스트 이름을 나타내고 **ERASQL**은 Microsoft SQL 서버 인스턴스의 이름을 나타냅니다. 사용자가 지정한 이름의 SQL 인스턴스에 ESET PROTECT 서버를 설치할 수 있습니다(Microsoft SQL DB 사용 시). 이 시나리오의 경우 백업 스크립트를 상황에 맞게 수정하십시오.

## SQL 스크립트를 사용하여 정기적 DB 백업

다음 SQL 스크립트 중 하나를 선택합니다.

a)정기적인 백업을 만들어서 만든 날짜를 기준으로 하여 저장:

```
@ECHO OFF
```

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

WITH NOFORMAT, INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHECKSUM, STATS=10"
```

```
REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)백업을 한 개 파일에 추가:

```
@ECHO OFF
```

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHECKSUM, STATS=10"
```

## Microsoft SQL 복원

파일에서 Microsoft SQL DB를 복원하려면 아래 표시된 예제를 따르십시오.

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE' "
```

## MySQL 백업

MySQL DB를 파일에 백업하려면 아래 표시된 예제를 따르십시오.

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -p DBNAME -r BACKUPFILE
```

**i** 이 예제에서 **HOST**는 MySQL Server의 IP 주소 또는 호스트 이름을, **ROOTLOGIN**은 MySQL Server의 루트 계정을, **DBNAME**은 ESET PROTECT DB 이름을 나타냅니다.

## MySQL 복원

파일에서 MySQL DB를 복원하려면 아래 표시된 예제를 따르십시오.

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

**i** Microsoft SQL Server 백업에 대한 자세한 내용을 보려면 [Microsoft TechNet 웹사이트](#)를 방문하십시오. MySQL Server 백업에 대한 자세한 내용을 보려면 [MySQL 문서 웹사이트](#)를 방문하십시오.

## DB 서버 업그레이드

ESET PROTECT 서버 데이터베이스에서 사용하기 위해 기존의 데이터베이스 서버 인스턴스를 최신 버전으로 업그레이드하려면 아래 지침을 따르십시오.

1. 업그레이드할 DB 서버에 연결되어 있는 실행 중인 모든 ESMC/ESET PROTECT 프록시 서비스를 중지합니다. 또한 데이터베이스 서버 인스턴스에 연결될 수 있는 다른 애플리케이션도 모두 중지합니다.
2. 계속하기 전에 관련 DB를 모두 안전하게 [백업](#)합니다.
3. DB 서버 업그레이드를 수행합니다.

### [SQL Server\(Windows\):](#)

- [Microsoft SQL Express DB를 최신 버전으로 업그레이드하려면 지식베이스 문서](#)를 따르십시오.
- 또는 DB 공급업체 지침(<https://msdn.microsoft.com/en-us/library/bb677622.aspx>)을 따릅니다.
- [Linux에서 Microsoft SQL Server](#)는 지원되지 않습니다. 그러나 [Linux의 ESET PROTECT 서버를 Windows의 Microsoft SQL Server에 연결](#)할 수 있습니다.

### [MySQL Server\(Windows 및 Linux\):](#)

- [MySQL 5.6에서 버전 5.7로 업그레이드](#)
- [MySQL 5.7에서 버전 8로 업그레이드](#)

4. ESET PROTECT 서버 서비스를 시작하고 [추적 로그](#)를 확인하여 데이터베이스가 제대로 연결되었는지 확인합니다.



# Windows의 장애 조치(Failover) 클러스터에 설치된 ESMC/ESET PROTECT 업그레이드

Windows의 [장애 조치\(Failover\) 클러스터](#)에 ESMC/ESET PROTECT 서버가 설치되어 있는 경우 아래의 단계에 따라 최신 ESET PROTECT(으)로 업그레이드합니다.

**! 지원되는 운영 체제**가 있는지 확인합니다.

1. 클러스터 관리자에서 ESMC/ESET PROTECT 서버 클러스터 역할을 중지합니다. 모든 클러스터 노드에서 서비스(**ESET Security Management Center Server** 또는 **ESET PROTECT Server**)가 중지되었는지 확인합니다.
2. node1의 클러스터 공유 디스크를 온라인 상태로 전환하고 [구성 요소를 설치](#)하는 경우처럼 최신 .msi 설치 관리자를 실행하여 서버 구성 요소를 수동으로 업그레이드합니다.
3. 설치(업그레이드)가 완료된 후 **ESET PROTECT Server** 서비스가 중지되었는지 확인합니다.
4. node2의 클러스터 공유 디스크를 온라인 상태로 전환하고 2단계와 동일한 방법으로 서버 구성 요소를 업그레이드합니다.
5. 모든 클러스터 노드에서 ESET PROTECT 서버가 업데이트된 후 클러스터 관리자에서 **ESET PROTECT 서버** 역할을 시작합니다.
6. 모든 클러스터 노드에서 최신 .msi 설치 관리자를 실행하여 수동으로 ESET Management 에이전트를 업그레이드합니다.
7. ESET PROTECT 웹 콘솔에서 모든 노드의 에이전트 및 서버 버전이 업그레이드한 최신 버전을 보고하는지 확인합니다.

## Apache Tomcat 업그레이드

Apache Tomcat은 ESET PROTECT 웹 콘솔을 실행하는 데 필요한 필수 구성 요소입니다.

최신 버전의 ESET PROTECT로 업그레이드하거나, 오랫동안 Apache Tomcat을 업그레이드하지 않은 경우 Apache Tomcat을 최신 버전으로 업그레이드하는 것을 고려해야 합니다. Apache Tomcat 및 해당 종속성을 비롯한 일반 공개용 서비스를 최신 상태로 유지하면 사용자 환경에 대한 보안 위험이 줄어듭니다.

Apache Tomcat을 업그레이드하려면 다음 지침을 따릅니다.

- [Windows 지침\(최신 ESET PROTECT 통합형 설치 관리자\)](#) - 통합형 설치 관리자를 통해 기존 Apache Tomcat을 설치한 경우에 권장되는 업그레이드 옵션입니다.
- [Windows 지침\(수동 설치\)](#) - 기존 Apache Tomcat을 수동으로 설치했거나 최신 ESET PROTECT 통합형 설치 관리자가 없는 경우 Apache Tomcat을 수동으로 업그레이드합니다.
- [Linux 지침](#)

# 통합형 설치 관리자를 사용하여 Apache Tomcat 프록시 업그레이드(Windows)

Apache Tomcat은 ESET PROTECT 웹 콘솔을 실행하는 데 필요한 필수 구성 요소입니다. 이 방법으로 최신 [ESET PROTECT 10.0 통합형 설치 관리자](#)를 사용하여 Apache Tomcat을 업그레이드합니다. 통합형 설치 관리자를 통해 기존 Apache Tomcat을 설치한 경우에 권장되는 업그레이드 옵션입니다. 또는 [Apache Tomcat을 수동으로 업그레이드](#)할 수 있습니다.

## 업그레이드하기 전에

다음 파일을 백업합니다.

```
C:\Program Files\Apache Software Foundation\[ Tomcat 폴더 ]\.keystore  
C:\Program Files\Apache Software Foundation\[ Tomcat 폴더 ]\conf\server.xml  
C:\Program Files\Apache Software Foundation\[ Tomcat 폴더 ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties
```

Tomcat 폴더에 사용자 지정 SSL 인증서 저장소를 사용하는 경우 해당 인증서도 백업합니다.

### Apache Tomcat 및 웹 콘솔 업그레이드 제한 사항

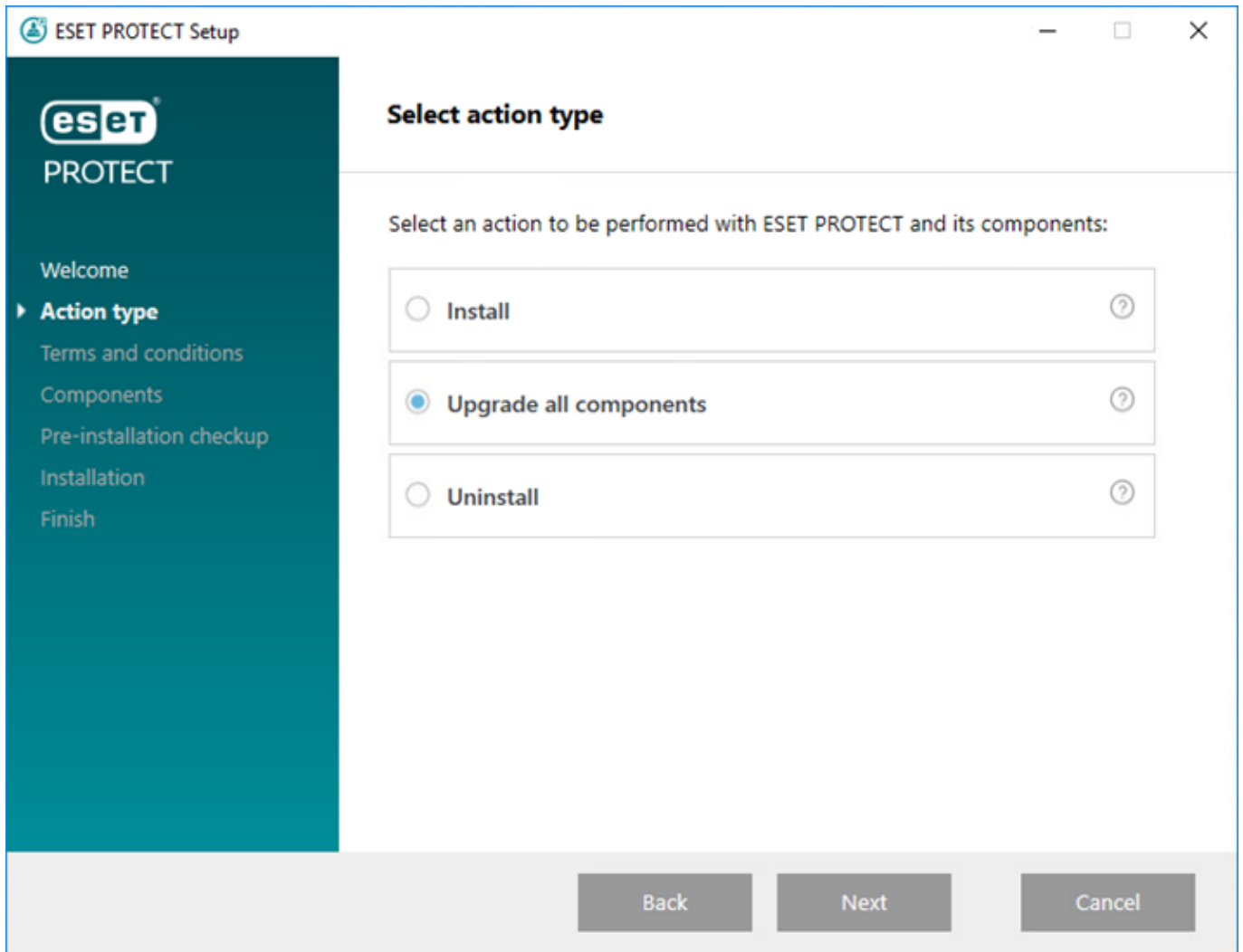
- 사용자 지정 버전의 Apache Tomcat이 설치(Tomcat 서비스 수동 설치)된 경우 통합형 설치 관리자 또는 구성 요소 업그레이드 작업을 통한 후속 ESET PROTECT 웹 콘솔 업그레이드는 지원되지 않습니다.
- Apache Tomcat을 업그레이드하면 다음에 있는 *era* 폴더가 제거됩니다. *C:\Program Files\Apache Software Foundation\[ Tomcat 폴더 ]\webapps\era* 폴더를 사용하여 추가 데이터를 저장하려면 업그레이드 전에 데이터를 백업해야 합니다.
- 이때 *C:\Program Files\Apache Software Foundation\[ Tomcat 폴더 ]\webapps\era*는 추가 데이터를 포함하고(*era* 및 *ROOT* 폴더 아님) Apache Tomcat 업그레이드가 실행되지 않으며 웹 콘솔만 업그레이드됩니다.
- 웹 콘솔 및 Apache Tomcat 업그레이드 시 [오프라인 도움말](#) 파일이 지워집니다. ESMC 또는 이전 ESET PROTECT 버전에서 오프라인 도움말을 사용한 경우, 업그레이드한 후 ESET PROTECT 10.0용으로 다시 생성하여 ESET PROTECT 버전과 일치하는 최신 오프라인 도움말이 있는지 확인하십시오.

## 업그레이드 절차

1. ESET 웹 사이트에서 [ESET PROTECT 통합형 설치 관리자](#)를 다운로드하고 다운로드한 파일의 압축을 풉니다.
2. 최신 버전의 Apache Tomcat을 설치하려고 하고 통합형 설치 관리자에 이전 버전의 Apache Tomcat이 포함되어 있는 경우(이 단계는 선택 사항임 - 최신 버전의 Apache Tomcat이 필요하지 않은 경우 4단계로 건너뛰기):
  - a.x64 폴더를 열고 *installers* 폴더로 이동합니다.
  - b.*installers* 폴더에 있는 *apache-tomcat-9.0.x-windows-x64.zip* 파일을 제거합니다.
  - c.Apache Tomcat 9 [64비트 Windows 압축](#) 패키지를 다운로드합니다.
  - d.다운로드한 압축 패키지를 *installers* 폴더로 이동합니다.

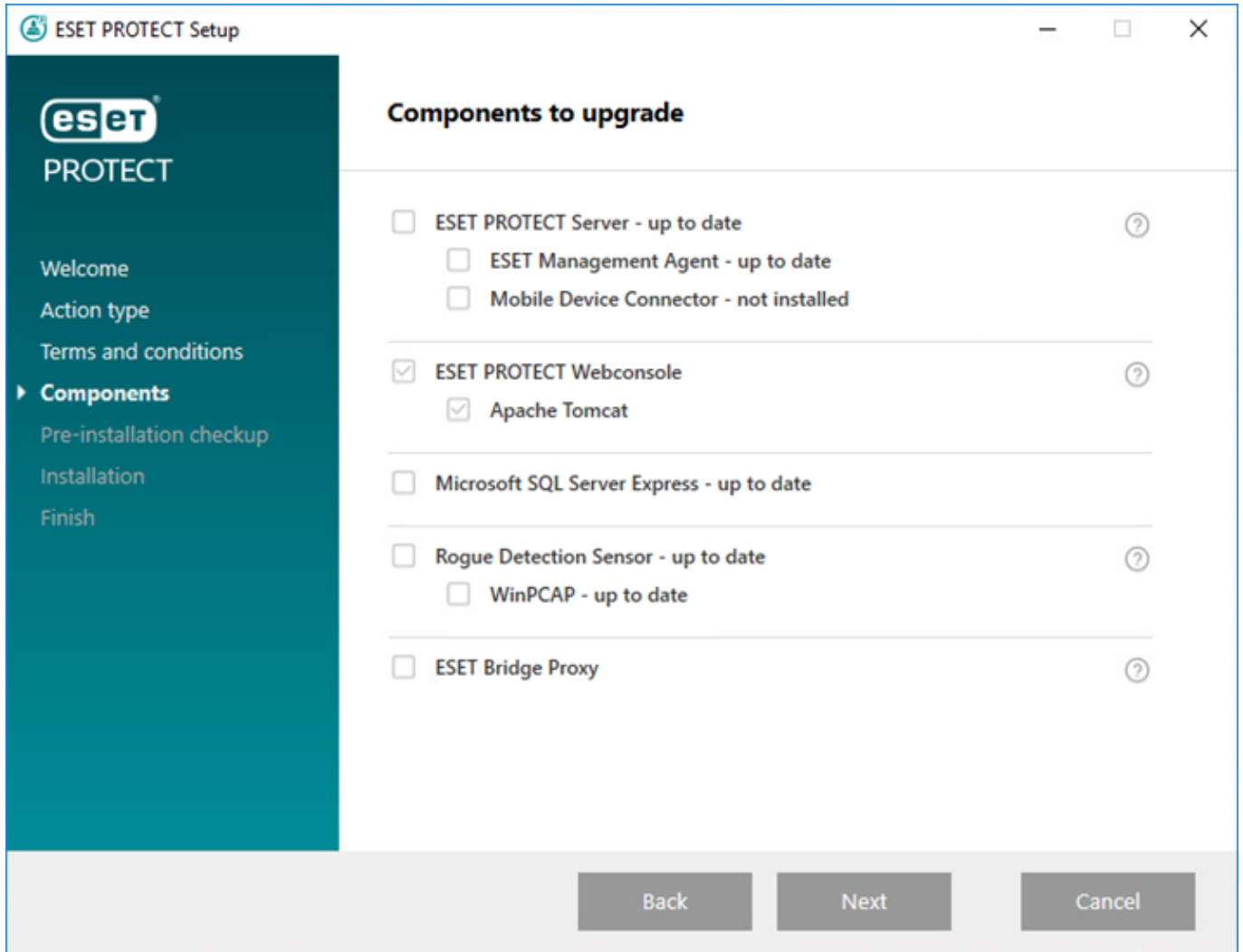
3. 통합형 설치 관리자를 시작하려면 *Setup.exe* 파일을 두 번 클릭하고 **시작** 화면에서 **다음**을 클릭합니다.

4. 모든 구성 요소 업그레이드를 선택하고 **다음**을 클릭합니다.



5. EULA에 동의한 후에 **다음**을 클릭합니다.

6. 통합형 설치 관리자가 업그레이드가 사용 가능한지 자동으로 감지합니다. 업그레이드할 수 있는 ESET PROTECT 구성 요소 옆에 확인란이 있습니다. **다음**을 클릭합니다.



7. 컴퓨터에 Java 설치를 선택합니다. Apache Tomcat에는 64비트 Java/OpenJDK가 필요합니다. 시스템에 여러 가지 Java 버전이 설치되어 있는 경우, 이전 Java 버전을 제거하고 [지원되는 Java](#) 최신 버전만 유지하는 것이 좋습니다.

**!** 2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.

8. **업그레이드**를 클릭하여 업그레이드를 완료한 후 **마침**을 클릭합니다.

9. ESET PROTECT 서버가 아닌 컴퓨터에 웹 콘솔을 설치한 경우:

a. Apache Tomcat 서비스를 중지합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **중지**를 선택합니다.

b. *EraWebServerConfig.properties* 파일(1단계)을 원래 위치로 복원합니다.

c. Apache Tomcat 서비스를 시작합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **시작**을 선택합니다.

10. [ESET PROTECT 웹 콘솔에 연결](#)하고 웹 콘솔이 올바르게 로드되는지 확인합니다.

**i** [엔터프라이즈 솔루션 또는 저성능 시스템에 대한 추가 웹 콘솔 구성도](#) 참조하십시오.

## 문제 해결

Apache Tomcat 업그레이드가 실패하면 Apache Tomcat을 제거한 다음 다시 설치하고 1단계의 구성을 적용합니다.

## Apache Tomcat 수동 업그레이드(Windows)

Apache Tomcat은 ESET PROTECT 웹 콘솔을 실행하는 데 필요한 필수 구성 요소입니다. 기존 Apache Tomcat을 수동으로 설치했거나 최신 ESET PROTECT 통합형 설치 관리자가 없는 경우 Apache Tomcat을 수동으로 업그레이드합니다.



사용자 지정 버전의 Apache Tomcat이 설치(Tomcat 서비스 수동 설치)된 경우 통합형 설치 관리자 또는 구성 요소 업그레이드 작업을 통한 후속 ESET PROTECT 웹 콘솔 업그레이드는 지원되지 않습니다.

### 업그레이드하기 전에

- Apache Tomcat에는 64비트 Java/OpenJDK가 필요합니다. 시스템에 여러 가지 Java 버전이 설치되어 있는 경우, 이전 Java 버전을 제거하고 [지원되는 Java](#) 최신 버전만 유지하는 것이 좋습니다.



2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.

- 현재 사용되는 Apache Tomcat 버전을 확인합니다.

a. Apache Tomcat 설치 폴더로 이동:

`C:\Program Files\Apache Software Foundation\[Tomcat 폴더]`

b. 텍스트 편집기에서 RELEASE-NOTES 파일을 열고 버전 번호(예: 9.0.34)를 확인합니다.

c. [지원되는 최신 버전](#)을 사용할 수 있는 경우 업그레이드를 수행합니다.

### 업그레이드 절차

1. Apache Tomcat 서비스를 중지합니다. **시작 > 서비스**로 이동하여 Apache Tomcat 서비스를 마우스 오른쪽 버튼으로 클릭하고 **중지**를 선택합니다.

Windows 알림 영역에서 실행 중인 경우 `Tomcat7w.exe`를 닫습니다.

2. 다음 파일을 백업합니다.

`C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\.keystore`

`C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\conf\server.xml`

`C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`

Tomcat 폴더에 사용자 지정 SSL 인증서 저장소를 사용하는 경우 해당 인증서도 백업합니다.

3. 현재 Apache Tomcat 버전을 제거합니다.

4. 시스템에 아직 다음 폴더가 있는 경우 삭제합니다.

C:\Program Files\Apache Software Foundation\[Tomcat 폴더]

5. <https://tomcat.apache.org>에서 **지원되는 최신 버전**의 Apache Tomcat 설치 관리자 파일(32비트/64비트 Windows Service Installer) `apache-tomcat-[버전].exe`를 다운로드합니다.

6. 다운로드한 최신 버전의 Apache Tomcat을 설치합니다.

- Java 버전이 더 설치되어 있는 경우 설치하는 동안 최신 Java 경로를 선택합니다.
- 설치가 완료되면 **Apache Tomcat 실행** 옆에 있는 확인란을 선택 취소합니다.

7. `.keystore`, `server.xml` 및 사용자 지정 인증서를 원래 위치에 복원합니다.

8. `server.xml` 파일을 열고 `keystoreFile` 경로가 올바른지 확인합니다(Apache Tomcat의 상위 주 버전으로 업그レード한 경우 경로 업데이트).

`keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\.keystore"`

9. ESET PROTECT 웹 콘솔에서 [Apache Tomcat용 HTTPS 연결](#)이 올바르게 구성되어 있는지 확인합니다.

10. ESET PROTECT 웹 콘솔을 배포합니다([웹 콘솔 설치 - Windows](#)).

11. `EraWebServerConfig.properties`를 원래 위치로 복원합니다.

12. Apache Tomcat을 실행하고 올바른 Java VM을 설정합니다.

a. 폴더 C:\Program Files\Apache Software Foundation\[Tomcat 폴더]\bin으로 이동하고 `Tomcat9w.exe`를 실행합니다.

b. 일반 탭에서 시작 유형을 자동으로 설정하고 시작을 누릅니다.

c. Java 탭을 클릭하고 기본값 사용을 선택 취소하고 Java 가상 컴퓨터에 `jvm.dll` 파일의 경로가 포함되어 있는지 확인([설명된 지식베이스 지식 참조](#))한 다음 확인을 클릭합니다.

13. [ESET PROTECT 웹 콘솔에 연결](#)하고 웹 콘솔이 올바르게 로드되는지 확인합니다.

**i** 엔터프라이즈 솔루션 또는 저성능 시스템에 대한 추가 웹 콘솔 구성도 참조하십시오.

## 문제 해결

- Apache Tomcat용 HTTPS 연결 설정에 실패할 경우 이 단계를 건너뛰고 일시적으로 HTTP 연결을 사용할 수 있습니다.
- Apache Tomcat 업그레이드에 실패한 경우 원래 버전을 설치하고 2단계의 구성을 적용하십시오.
- 웹 콘솔 및 Apache Tomcat 업그레이드 시 [오프라인 도움말](#) 파일이 지워집니다. ESMC 또는 이전 ESET PROTECT 버전에서 오프라인 도움말을 사용한 경우, 업그레이드한 후 ESET PROTECT 10.0용으로 다시 생성하여 ESET PROTECT 버전과 일치하는 최신 오프라인 도움말이 있는지 확인하십시오.

# Apache Tomcat 및 Java 업그레이드(Linux)

Apache Tomcat은 ESET PROTECT 웹 콘솔을 실행하는 데 필요한 필수 구성 요소입니다.

## 업그레이드하기 전에

1. 다음 명령을 실행하여 설치된 Apache Tomcat 버전을 확인합니다(경우에 따라 폴더 이름이 tomcat7 또는 tomcat8임).

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. 최신 버전을 사용할 수 있는 경우:

- a. 최신 버전이 [지원](#)되는지 확인하십시오.

- b. Tomcat 구성 파일(/etc/tomcat7/server.xml)을 백업합니다.

## 업그레이드 절차

1. 다음 명령을 실행하여 Apache Tomcat 서비스를 중지합니다(경우에 따라 서비스 이름은 tomcat7임).

```
sudo systemctl stop tomcat
```

2. Apache Tomcat 및 Java를 업그레이드합니다.



아래 패키지 이름의 예는 Linux 배포 저장소 패키지와 다를 수 있습니다. Linux 배포본의 기본 저장소에는 [지원되는 최신 버전의 Apache Tomcat 및 Java](#)가 포함되어 있지 않을 수 있습니다.

Linux 배포	터미널 명령
Debian 및 Ubuntu 배포	sudo apt-get update sudo apt-get install openjdk-17-jdk tomcat9
CentOS 및 Red Hat 배포	yum update yum install java-17-openjdk tomcat
SUSE Linux	zypper refresh sudo zypper install java-17-openjdk tomcat9

3. 백업에서 /etc/tomcat9/server.xml 파일을 server.xml 파일로 대체합니다.

4. server.xml 파일을 열고 keystoreFile 경로가 올바른지 확인합니다.

5. [Apache Tomcat용 HTTPS 연결](#)이 올바르게 구성되어 있는지 확인합니다.

[엔터프라이즈 솔루션 또는 저성능 시스템에 대한 추가 웹 콘솔 구성](#)도 참조하십시오.

6. Java를 업그레이드한 경우 아래 단계에 따라 시스템에 설치된 최신Java 패키지를 사용하도록 Apache Tomcat을 구성합니다.

- a. Apache Tomcat 구성 폴더로 이동합니다.

```
cd /usr/share/tomcat/conf/
```



b. 텍스트 편집기에서 `tomcat.conf` 파일을 엽니다.

```
nano tomcat.conf
```

c. `JAVA_HOME` 변수에서 설치된 최신 Java 패키지로 경로를 업데이트합니다(이 경로는 시스템에 설치된 Java 패키지에 따라 다름).

```
JAVA_HOME="/usr/lib/jvm/jre-11-openjdk"
```

d. 파일을 저장하고 닫습니다: **CTRL+X**를 누른 다음 **Y** 및 **ENTER**를 누릅니다.

e. **tomcat** 서비스를 다시 시작합니다:

```
sudo systemctl restart tomcat
```

f. 아래 명령을 실행하여 Apache Tomcat에서 사용되는 Java 패키지를 확인합니다.

```
sudo systemctl status tomcat
```

Apache Tomcat을 이후 주 버전으로 업그레이드한 후(예: Apache Tomcat 버전 7.x를 9.x로):

1. ESET PROTECT 웹 콘솔을 다시 배포합니다([ESET PROTECT 웹 콘솔 설치 - Linux 참조](#)).

2. ESET PROTECT 웹 콘솔의 모든 사용자 지정 설정을 유지하려면 `%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties`을 재사용합니다.

⚠ 웹 콘솔 및 Apache Tomcat 업그레이드 시 [오프라인 도움말](#) 파일이 지워집니다. ESMC 또는 이전 ESET PROTECT 버전에서 오프라인 도움말을 사용한 경우, 업그레이드한 후 ESET PROTECT 10.0용으로 다시 생성하여 ESET PROTECT 버전과 일치하는 최신 오프라인 도움말이 있는지 확인하십시오.

## 마이그레이션 및 다시 설치 절차

ESET PROTECT 서버 및 기타 ESET PROTECT 구성 요소를 업그레이드, 마이그레이션 및 다시 설치하는 다양한 방법이 있습니다.

- 한 서버의 ESET PROTECT 10을(를) 다른 서버로 [마이그레이션 또는](#) 다시 설치.

⚠ 한 ESET PROTECT 서버에서 새로운 서버 컴퓨터로 마이그레이션하려면 모든 인증 기관과 ESET PROTECT 서버 인증서를 내보내고 백업합니다. 그렇지 않으면 ESET PROTECT 구성 요소가 새 ESET PROTECT 서버와 통신할 수 없게 됩니다.

- [ESET PROTECT DB 마이그레이션](#)
- [MDM 마이그레이션](#)
- ESET PROTECT 서버의 [IP 주소 또는 호스트 이름을 변경](#)합니다.

[업그레이드 절차](#)를 참조하십시오.

# 서버 간 마이그레이션

다음과 같은 여러 가지 방법으로 한 서버에서 다른 서버로 ESET PROTECT를 마이그레이션할 수 있습니다(이러한 시나리오는 ESET PROTECT Server를 다시 설치할 때 사용할 수 있음).

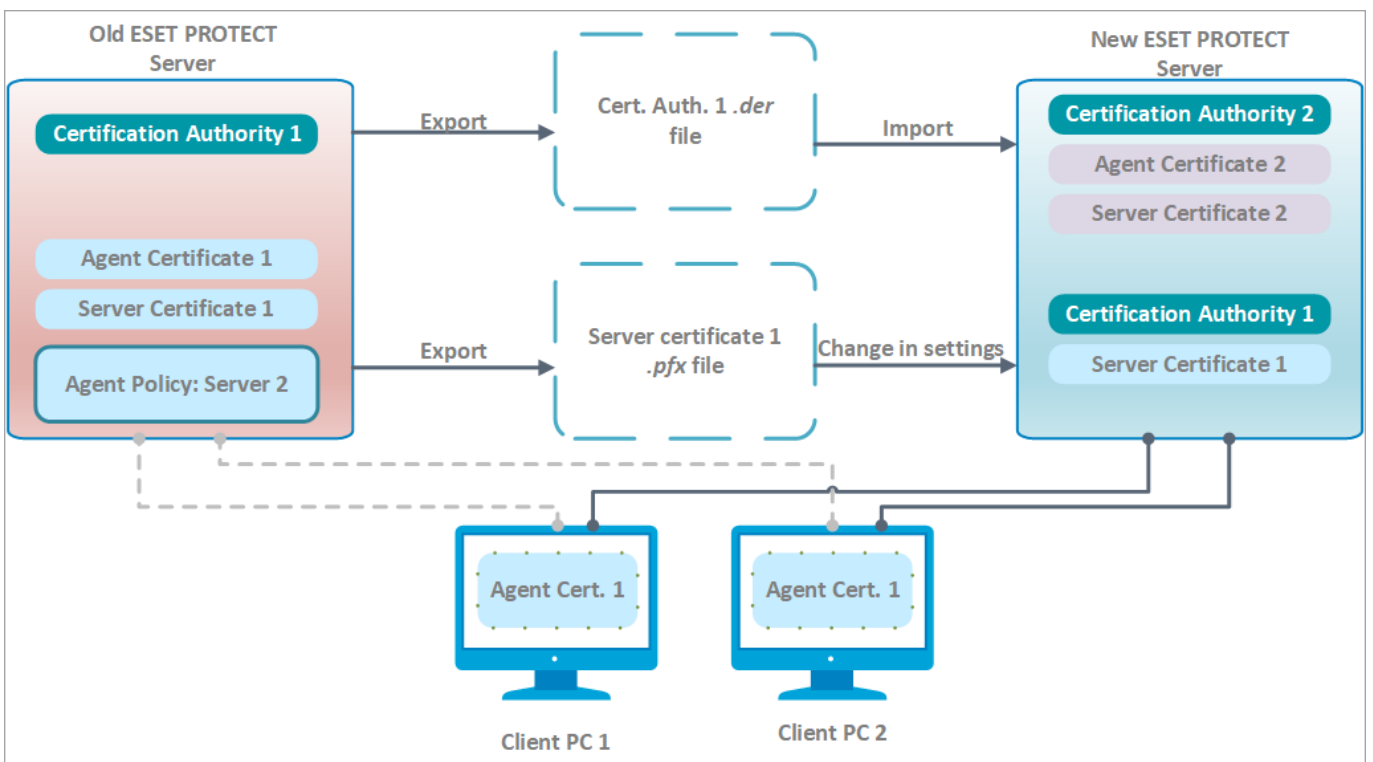
- [새로 설치 - 동일한 IP 주소](#) - 새 설치에서는 이전 ESET PROTECT 서버의 이전 DB를 사용하지 않으며 원래 IP 주소를 유지합니다.
- [새로 설치 - 다른 IP 주소](#)(지식베이스 문서) - 새 설치에서는 이전 ESET PROTECT 서버의 이전 DB를 사용하지 않으며 다른 IP 주소를 사용합니다.
- [마이그레이션된 DB - 동일한/다른 IP 주소](#) - DB 마이그레이션은 두 가지 유사한 DB 유형(MySQL에서 MySQL로 또는 Microsoft SQL에서 Microsoft SQL로)과 두 가지 유사한 버전의 ESET PROTECT 사이에서만 수행할 수 있습니다.

## 새로 설치 - 동일한 IP 주소

이 절차의 목표는 이전 DB를 사용하지 않도록 ESET PROTECT 서버의 완전히 새로운 인스턴스를 설치하는 것입니다. 이 새 ESET PROTECT 서버는 이전 서버와 **동일한 IP 주소**를 갖지만 이전 ESET PROTECT 서버의 DB를 사용하지 않습니다.

아래 지침에 따라 액세스 가능한 웹 콘솔과 함께 이전 ESET PROTECT 서버가 실행 중이어야 합니다. 이전 ESET PROTECT 서버에 액세스할 수 없는 경우:

1. [통합형 패키지 설치 관리자](#)(Windows)를 사용하여 ESET PROTECT 서버/MDM을 설치하거나 [다른 설치 방법](#)(Windows 수동 설치, Linux 또는 가상 어플라이언스)을 선택합니다.
2. ESET PROTECT 웹 콘솔에 [연결](#)합니다.
3. [ESET PROTECT 인프라에 클라이언트 컴퓨터를 추가하고 ESET Management Agent를 로컬 또는 원격으로 배포할 수 있습니다.](#)



□ 현재(이전) ESET PROTECT 서버에서:

[ESET Full Disk Encryption](#)로 암호화된 장치를 관리하는 경우 다음 단계에 따라 [복구 데이터](#)의 손실을 피하십시오.

1. 마이그레이션 전 - **상태 개요 > 암호화**로 이동합니다. 여기에서 현재 **ESET Full Disk Encryption 복구 데이터를 내보낼** 수 있습니다.
2. 마이그레이션 후 - 새 관리 콘솔에서 **ESET Full Disk Encryption 복구 데이터를 가져옵니다**. 이러한 단계를 수행할 수 없는 경우 마이그레이션하기 전에 [관리되는 장치를 복호화](#)해야 합니다. 마이그레이션 후 ESET PROTECT 웹 콘솔에서 [관리되는 장치를 암호화](#)할 수 있습니다.

1. 현재 ESET PROTECT 서버에서 서버 인증서를 내보내고 외부 저장소에 저장합니다.
  - ESET PROTECT 서버에서 [인증 기관 인증서](#)를 모두 내보내고 각 CA 인증서를 .der 파일로 저장합니다.
  - ESET PROTECT 서버에서 .pfx 파일로 [서버 인증서](#)를 내보냅니다. 내보낸 .pfx에는 개인 키도 포함됩니다.
2. ESET PROTECT 서버 서비스를 중지합니다.
3. 사용 중인 ESET PROTECT 서버 컴퓨터를 해제합니다.

! 아직 이전 ESET PROTECT 서버를 제거/해제하지 마십시오.

□ 새 ESET PROTECT 서버에서:

! 동일한 IP 주소로 새 ESET PROTECT Server를 사용하려면 새 ESET PROTECT Server의 네트워크 구성(IP 주소, FQDN, 컴퓨터 이름, DNS SRV 레코드)이 이전 ESET PROTECT Server의 네트워크 구성과 일치해야 합니다.

1. [통합형 패키지 설치 관리자](#)(Windows)를 사용하여 ESET PROTECT 서버/MDM을 설치하거나 [다른 설치 방법](#)(Windows 수동 설치, Linux 또는 가상 어플라이언스)을 선택합니다.
2. ESET PROTECT 웹 콘솔에 [연결](#)합니다.
3. 이전 ESET PROTECT 서버에서 내보낸 모든 CA 가져오기를 수행합니다. 이렇게 하려면 [공개 키 가져오기](#) 지침을 따릅니다.
4. 이전 ESET PROTECT 서버의 서버 인증서를 사용하도록 **자세히 > 서버 설정**에서 ESET PROTECT 서버 인증서를 변경합니다.
5. ESET PROTECT로 [필요한 모든 ESET 라이선스를 가져옵니다](#).
6. ESET PROTECT 서버 서비스를 다시 시작합니다(자세한 내용은 ESET의 [지식 베이스 문서](#) 참조).

하나 또는 두 [에이전트 연결 간격](#) 후에 클라이언트 컴퓨터는 원래 ESET PROTECT Agent 에이전트 인증서를 사용하여 새 ESET Management 서버에 연결되어야 하며, 원래 Agent 인증서는 이전 ESET PROTECT 서버에서 가져온 CA에 의해 인증됩니다. 클라이언트가 연결되지 않는 경우 [ESET PROTECT 서버 업그레이드/마이그레이션 후 문제](#)를 참조하십시오.

**i** 새 클라이언트 컴퓨터를 추가할 경우 새 인증 기관을 사용하여 에이전트 인증서에 서명합니다. 가져온 CA는 새 피어 인증서에 서명하는 데 사용될 수 없으며 마이그레이션된 클라이언트 컴퓨터의 ESET Management 에이전트만 인증할 수 있으므로 이렇게 합니다.

#### □ 이전 ESET PROTECT 서버/MDM 제거:

새 ESET PROTECT 서버에서 모든 항목이 올바르게 실행되도록 한 후 [단계별 지침](#)을 사용하여 이전 ESET PROTECT 서버/MDM을 주의해서 해제하십시오.

## 마이그레이션된 DB - 동일한/다른 IP 주소

이 절차의 목표는 ESET PROTECT 서버의 완전히 새로운 인스턴스를 설치하고 기존 클라이언트 컴퓨터를 포함하여 기존 ESET PROTECT DB를 유지하는 것입니다. 새 ESET PROTECT Server는 이전 ESET PROTECT 서버와 동일하거나 다른 IP 주소를 사용하게 되며, 설치 전에 이전 서버의 DB를 새 서버 컴퓨터로 가져옵니다.

- [DB 마이그레이션](#)은 동일한 DB 유형 간(MySQL에서 MySQL로 또는 Microsoft SQL에서 Microsoft SQL로)에만 지원됩니다.
- DB를 마이그레이션할 때는 동일한 ESET PROTECT 버전의 인스턴스 간에 마이그레이션해야 합니다. ESET PROTECT 구성 요소의 버전을 확인하는 지침은 ESET의 [지식 베이스 문서](#)를 참조하십시오. DB 마이그레이션을 완료한 후 필요한 경우 업그레이드를 수행하여 최신 버전의 ESET PROTECT를 사용할 수 있습니다.

#### □ 현재(이전) ESET PROTECT 서버에서:

- 고급 사용자에게 한해서만 다른 IP 주소로 마이그레이션하는 것을 권장합니다. 새 ESET PROTECT Server의 IP 주소가 다른 경우 현재(이전) ESET PROTECT Server에서 다음과 같은 추가 단계를 수행합니다.
- !** a) 새 ESET PROTECT 서버에 대한 연결 정보를 사용하여 [새 ESET PROTECT 서버 인증서](#)를 생성합니다. 호스트 필드의 기본값(별표)을 그대로 두어 특정 DNS 이름 또는 IP 주소와 연결하지 않고 이 인증서를 배포할 수 있습니다.
- !** b) [새 ERA ESET PROTECT IP 주소](#)를 정의하고 이를 모든 컴퓨터에 할당하기 위한 정책을 생성합니다. 정책이 모든 클라이언트 컴퓨터에 배포될 때까지 기다립니다(컴퓨터가 새 서버 정보를 받기 때문에 보고를 중지함).

1. ESET PROTECT 서버 서비스를 중지합니다.
2. [ESET PROTECT DB를 내보내기/백업](#)합니다.
3. 현재 ESET PROTECT Server 컴퓨터를 끕니다(새 서버의 IP 주소가 다른 경우의 옵션).

**!** 아직 이전 ESET PROTECT 서버를 제거/해제하지 마십시오.

#### □ 새 ESET PROTECT 서버에서:

**!** 동일한 IP 주소로 새 ESET PROTECT Server를 사용하려면 새 ESET PROTECT Server의 네트워크 구성(IP 주소, FQDN, 컴퓨터 이름, DNS SRV 레코드)이 이전 ESET PROTECT Server의 네트워크 구성과 일치해야 합니다.

1. [지원되는](#) ESET PROTECT DB를 설치/실행합니다.
2. 이전 ESET PROTECT 서버에서 [ESET PROTECT DB](#)를 가져오기/복원합니다.

3. [통합형 패키지 설치 관리자](#)(Windows)를 사용하여 ESET PROTECT 서버/MDM을 설치하거나 [다른 설치 방법](#)(Windows 수동 설치, Linux 또는 가상 어플라이언스)을 선택합니다. ESET PROTECT 서버 설치 중에 DB 연결 설정을 지정합니다.
4. ESET PROTECT 웹 콘솔에 [연결](#)합니다.
5. **자세히 > 설정 > 연결**로 이동합니다. **인증서 변경 > 인증서 목록 열기**를 클릭하고 이전 ESET PROTECT 서버의 **서버 인증서**를 선택한 다음 **확인**을 두 번 클릭합니다.
6. [ESET PROTECT 서버 서비스를 다시 시작합니다](#).
7. ESET PROTECT 웹 콘솔에 [로그인](#)하고 **컴퓨터**를 클릭합니다.

하나 또는 두 [에이전트 연결 간격](#) 후에 클라이언트 컴퓨터는 원래 ESET PROTECT Agent 에이전트 인증서를 사용하여 새 ESET Management 서버에 연결되어야 합니다. 클라이언트가 연결되지 않는 경우 [ESET PROTECT 서버 업그레이드/마이그레이션 후 문제](#)를 참조하십시오.

#### □ 이전 ESET PROTECT 서버/MDM 제거:

새 ESET PROTECT 서버에서 모든 항목이 올바르게 실행되도록 한 후 [단계별 지침](#)을 사용하여 이전 ESET PROTECT 서버/MDM을 주의해서 해제하십시오.

## ESET PROTECT DB 마이그레이션

이러한 지침은 서로 다른 SQL Server 인스턴스 간 ESET PROTECT DB 마이그레이션에 적용됩니다(서로 다른 SQL Server 버전으로 마이그레이션할 때나 다른 컴퓨터에서 호스팅된 SQL Server로 마이그레이션할 때에도 적용됨).

- [Microsoft SQL Server에 대한 마이그레이션 프로세스](#)
- [MySQL Server의 마이그레이션 프로세스](#)

## Microsoft SQL Server에 대한 마이그레이션 프로세스

이 마이그레이션 프로세스는 **Microsoft SQL Server**와 **Microsoft SQL Server Express**에 대해 동일하게 적용됩니다.

자세한 내용은 다음 Microsoft 기술 자료 문서를 참조하십시오.

<https://msdn.microsoft.com/en-us/library/ms189624.aspx>

### 필수 구성 요소

- 소스 및 대상 SQL Server 인스턴스가 설치되어 있어야 하며, 이러한 인스턴스는 서로 다른 컴퓨터에서 호스팅될 수 있습니다. 이러한 인스턴스는 서로 다른 컴퓨터에서 호스팅될 수 있습니다.
- 소스 인스턴스와 같은 버전의 대상 SQL Server 인스턴스가 하나 이상 있어야 합니다. **다운그레이드는 지원되지 않습니다!**
- **SQL Server Management Studio**가 설치되어 있어야 합니다. SQL Server 인스턴스가 서로 다른 컴퓨터

에 있는 경우 SQL Server Management Studio는 인스턴스가 있는 모든 컴퓨터에 있어야 합니다.

## SQL Server Management Studio를 사용하여 마이그레이션

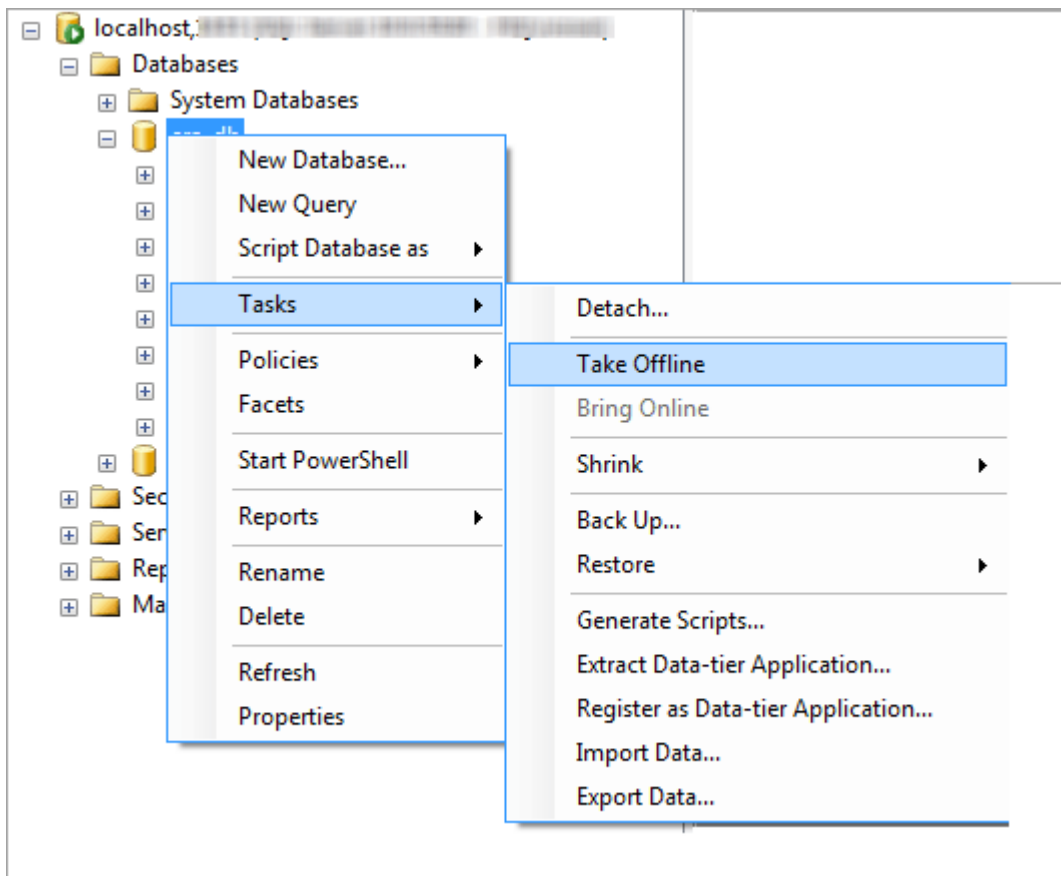
1. ESET PROTECT 서버 서비스(ESMC 서버 서비스) 또는 ESET PROTECT MDM 서비스를 중지합니다.

**!** 아래의 모든 단계를 완료하기 전에 ESET PROTECT 서버 또는 ESET PROTECT MDM을 시작하지 마십시오.

2. SQL Server Management Studio를 통해 소스 SQL Server 인스턴스에 로그인합니다.

3. 마이그레이션할 DB의 전체 DB 백업을 생성합니다. 이때 새로운 백업 집합 이름을 지정하는 것이 좋습니다. 그렇지 않으면 백업 집합이 이미 사용된 경우 새 백업이 기존 백업에 추가되며, 이로 인해 백업 파일 크기가 불필요하게 커집니다.

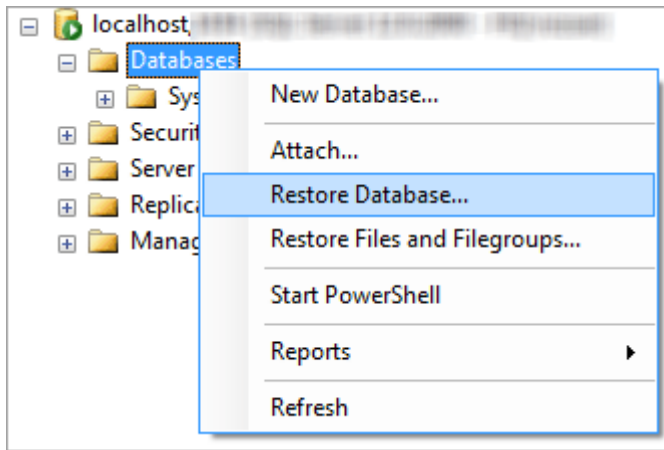
4. 소스 DB를 오프라인으로 가져오고 **작업 > 오프라인으로 가져오기**를 선택합니다.



5. 3단계에서 생성한 백업 파일(.bak)을 대상 SQL Server 인스턴스에서 접근 가능한 위치에 복사합니다. DB 백업 파일의 접근 권한을 편집해야 할 수 있습니다.

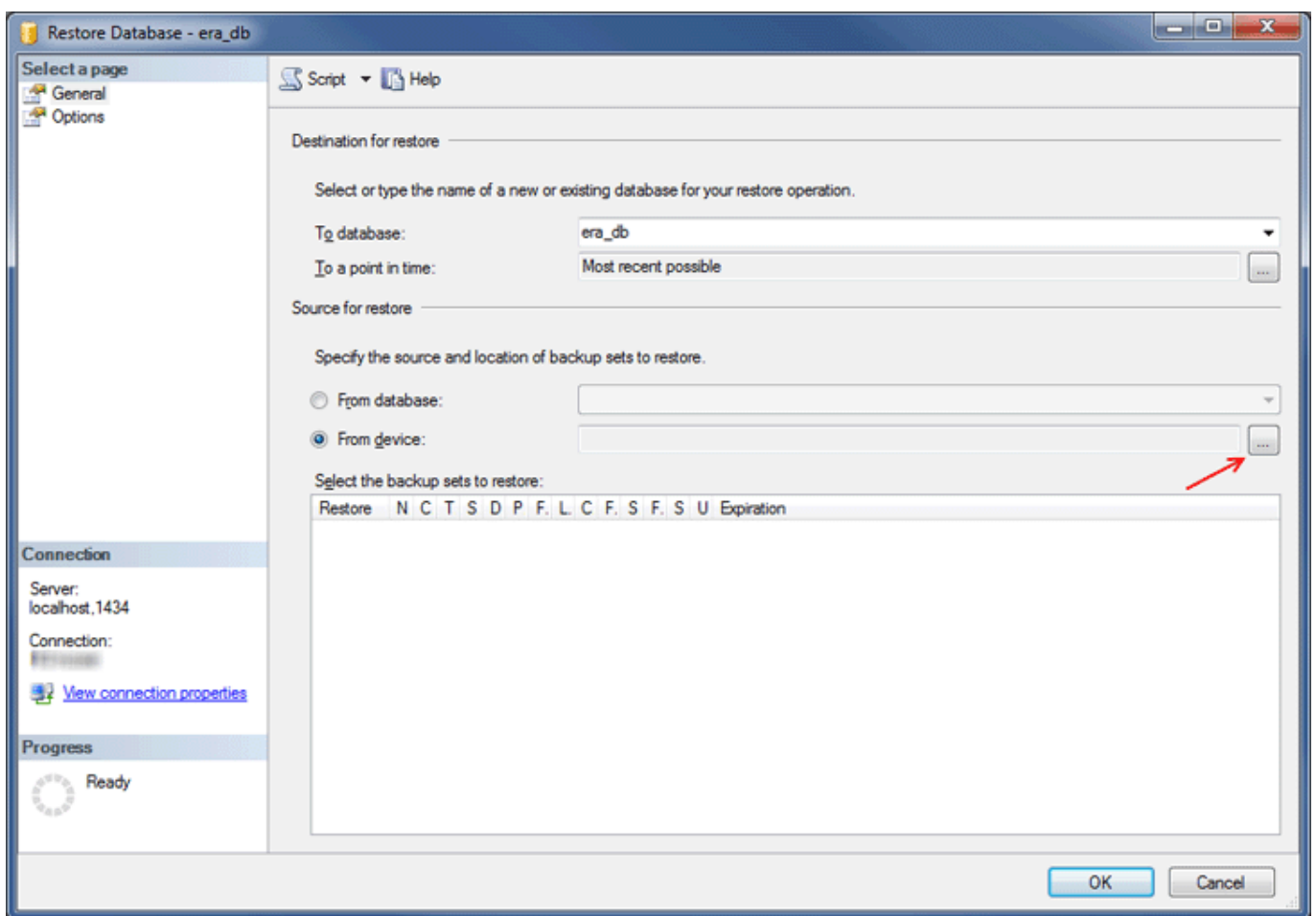
6. SQL Server Management Studio를 통해 대상 SQL Server 인스턴스에 로그인합니다.

7. 대상 SQL Server 인스턴스에서 DB를 복원합니다.



8. 복원 후 DB 필드에 새 DB의 이름을 입력합니다. 원할 경우 기존 DB와 같은 이름을 사용할 수 있습니다.

9. 복원할 백업 집합의 소스 및 위치 지정에서 [장치에서]를 선택한 후 [...]를 클릭합니다.



10. 추가를 클릭하고 백업 파일로 이동하여 이 파일을 엽니다.

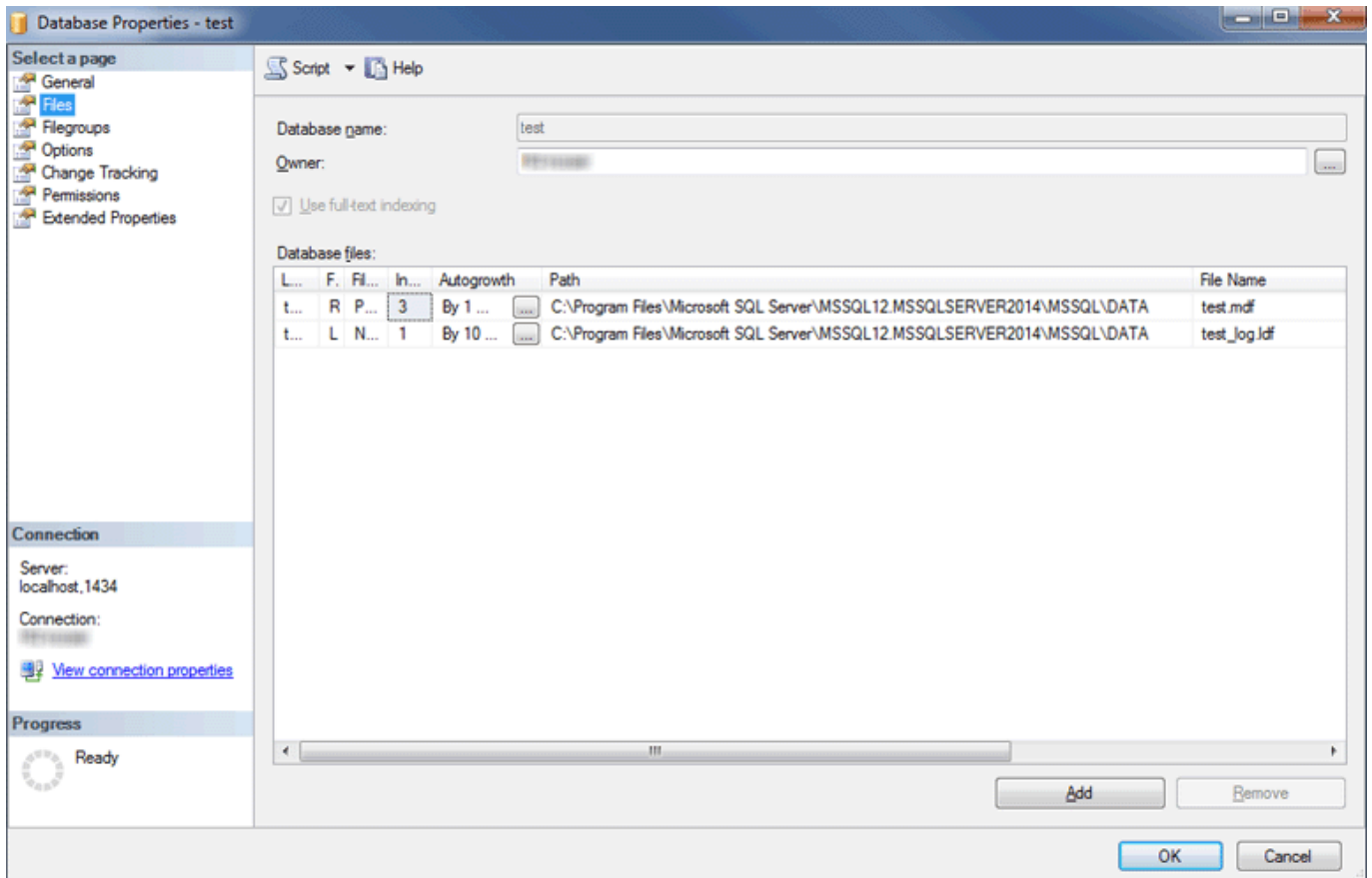
11. 복원할 가장 최근 백업을 선택합니다(백업 집합에 여러 백업이 포함될 수 있음).

12. 복원 마법사의 옵션 페이지를 클릭합니다. 경우에 따라 기존 DB 덮어쓰기를 선택하고 DB(.mdf) 및 로그(.ldf)에 대한 복원 위치가 올바른지 확인합니다. 기본값을 변경하지 않은 상태로 두면 소스 SQL Server의 경로가 사용됩니다. 따라서 이 값을 확인하십시오.

- DB 파일이 대상 SQL Server 인스턴스에 저장되는 위치를 모를 경우 기존 DB를 오른쪽 마우스 버튼으로 클릭하고 속성을 선택한 후 파일 탭을 클릭합니다. DB가 저장되는 디렉터리가 아래 표시된 테이블



의 경로 열에 표시됩니다.

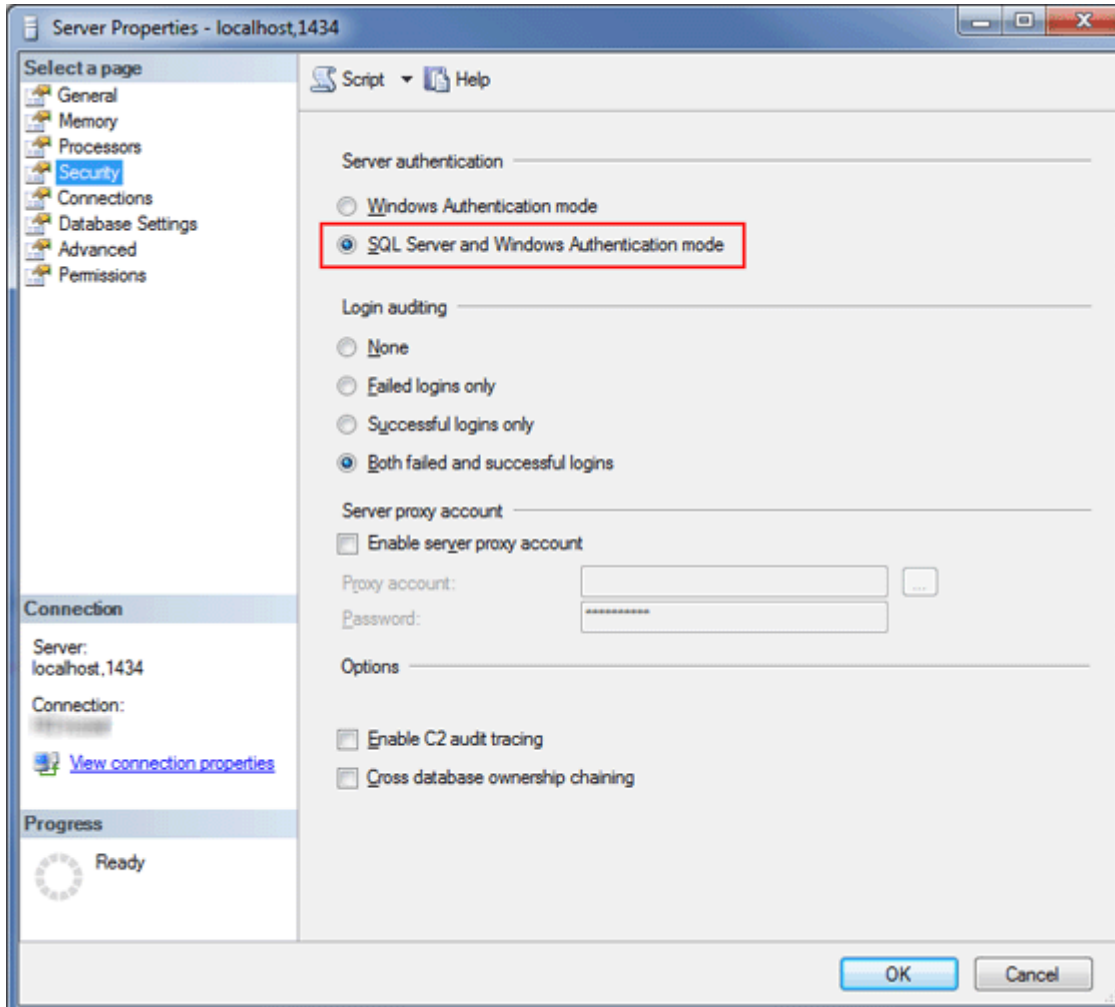


13. 복원 마법사 창에서 **확인**을 클릭합니다.

14. **era\_db** DB를 마우스 오른쪽 버튼으로 클릭하고, **새 쿼리**를 선택한 후 아래의 쿼리를 실행하여 **tbl\_authentication\_certificate** 표의 콘텐츠를 삭제합니다(삭제하지 않으면 에이전트가 새 서버에 연결되지 않을 수 있음).

```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. 새 DB 서버에서 **SQL Server 인증**이 **활성화**되었는지 확인합니다. 서버를 오른쪽 마우스 버튼으로 클릭하고 **속성**을 클릭합니다. **보안**으로 이동한 후 **SQL Server 및 Windows 인증 모드**가 선택되었는지 확인합니다.



16. SQL Server 인증으로 대상 SQL Server에서 새 **SQL Server 로그인**을 생성(ESET PROTECT 서버/ESET PROTECT MDM용)하고 로그인을 복원된 DB의 사용자에게 매핑합니다.

o비밀번호 만료를 적용하지 마십시오!

o사용자 이름에 권장되는 문자:

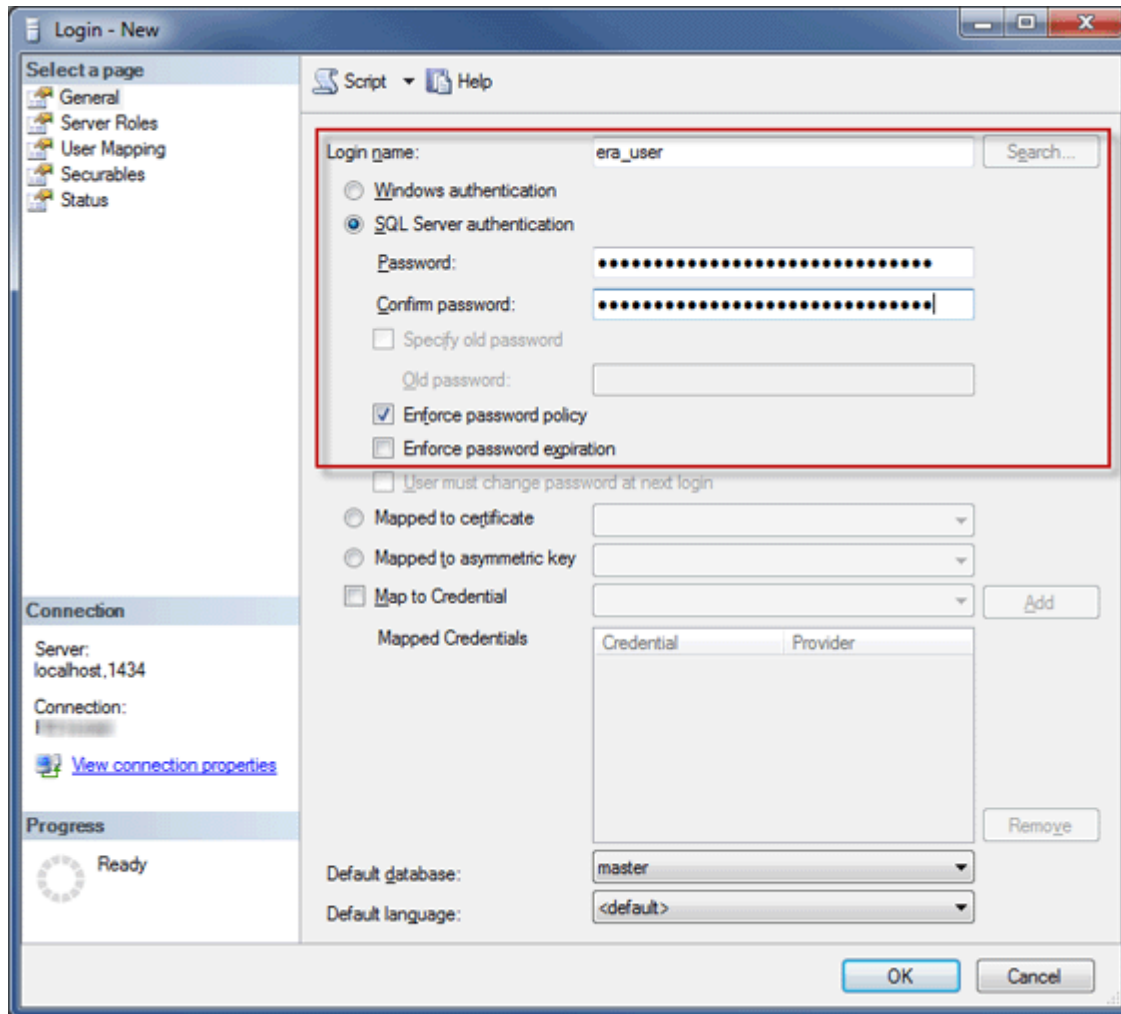
■소문자 ASCII 문자, 숫자 및 밑줄 문자("\_")

o비밀번호에 권장되는 문자:

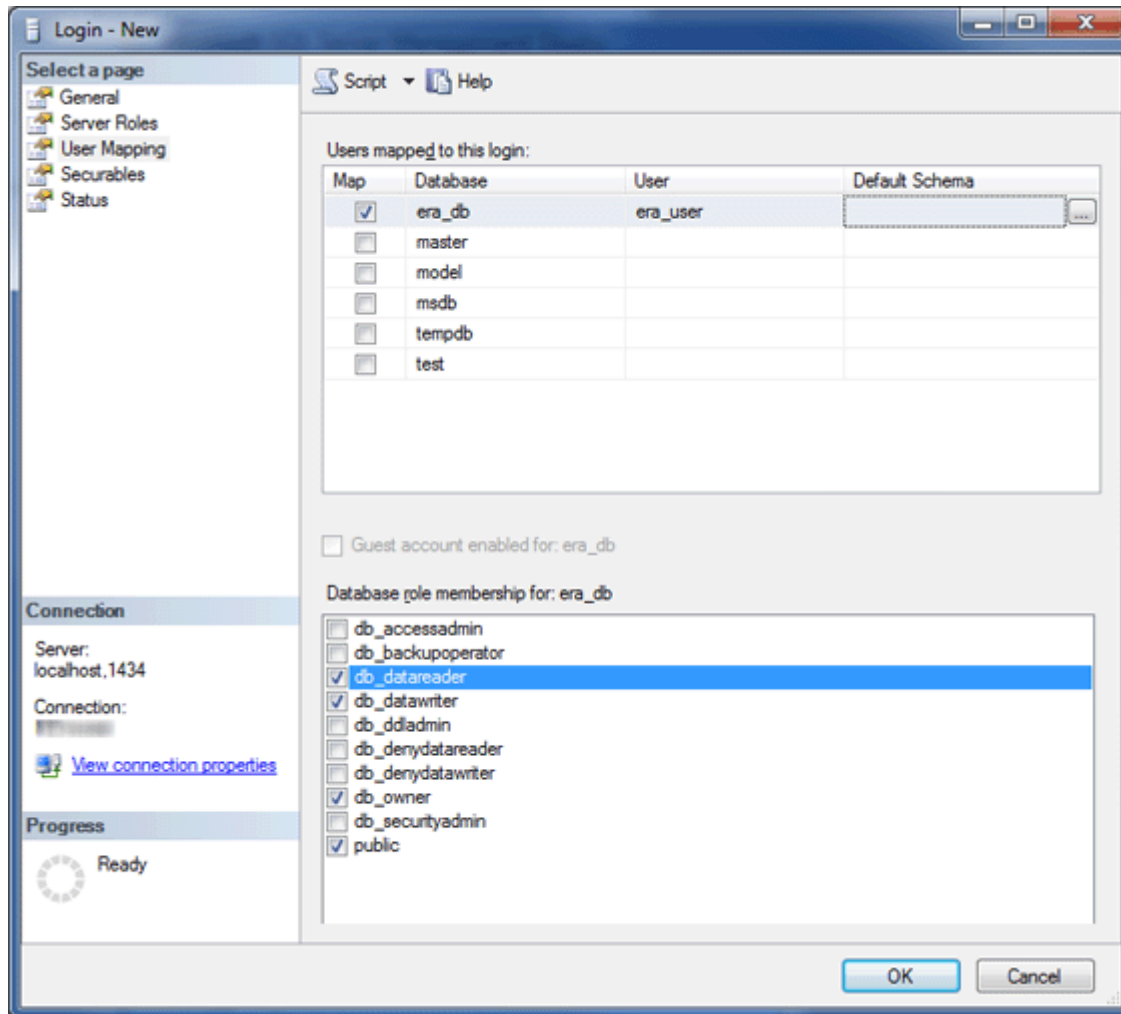
■ASCII 문자만(대문자 및 소문자 ASCII 문자, 숫자, 공백, 특수 문자 포함)

oASCII 이외의 문자는 사용하지 마십시오(예: 중괄호({})나 @).

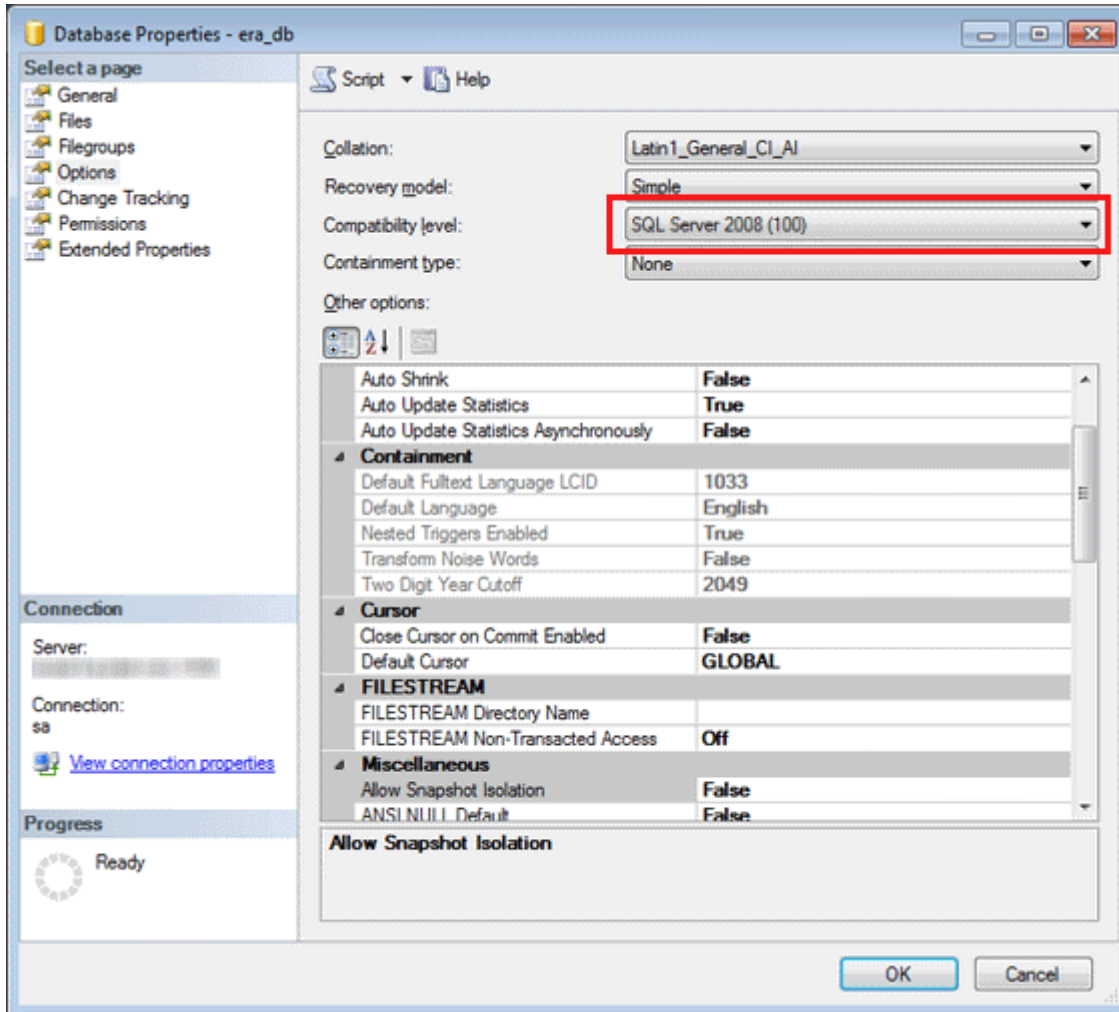
o위의 문자 권장 사항을 따르지 않을 경우 DB 연결에 문제가 발생하거나 DB 연결 문자열을 수정하는 동안 나중의 단계에서 특수 문자를 이스케이프해야 할 수 있습니다. 이 문서에는 문자 이스케이프 규칙이 포함되어 있지 않습니다.



17. 로그인 대상 DB의 사용자에게 매핑합니다. **사용자 매핑** 탭에서 DB 사용자에게 **db\_datareader**, **db\_datawriter**, **db\_owner** 역할이 포함되는지 확인합니다.

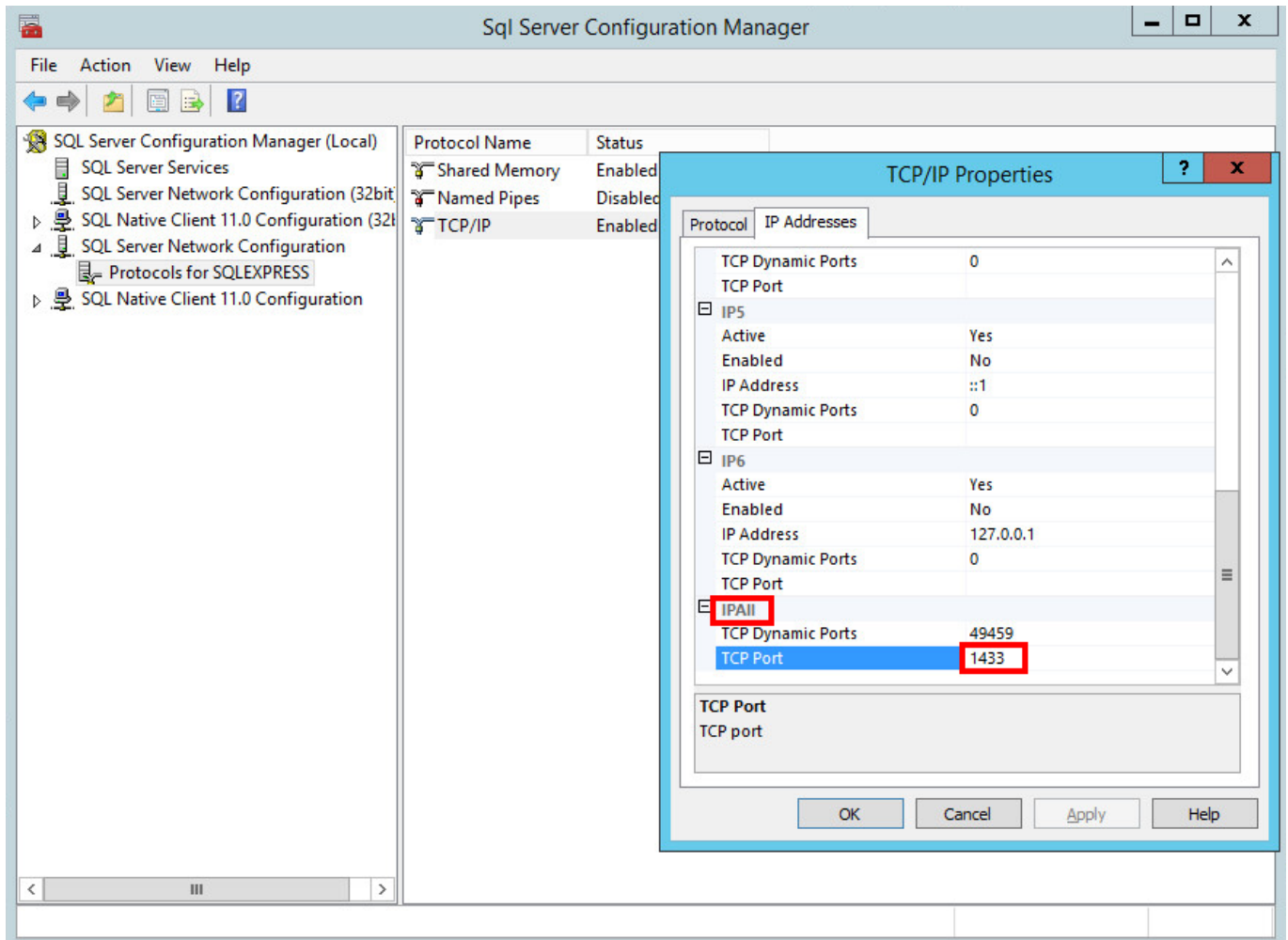


18. 최신 DB 서버 기능을 사용하려면 복원된 DB의 **호환성 수준**을 최신으로 변경합니다. 새 DB를 오른쪽 마우스 버튼으로 클릭하고 DB의 속성을 엽니다.



**i** SQL Server Management Studio에서는 사용 중인 버전보다 높은 버전의 호환성 수준은 정의할 수 없습니다. 예를 들어 SQL Server Management Studio 2014에서는 SQL Server 2019의 호환성 수준을 설정할 수 없습니다.

19. **TCP/IP** 연결 프로토콜이 "db\_instance\_name"(예: SQLEXPRESS 또는 MSSQLSERVER)에 대해 **사용** 상태이고 **TCP/IP 포트**가 **1433**으로 설정되어 있는지 확인합니다. 이렇게 하려면 **Sql Server 구성 관리자**를 열고 **SQL Server 네트워크 구성 > db\_instance\_name용 프로토콜**로 이동한 후 **TCP/IP**를 마우스 오른쪽 버튼으로 클릭하고 **활성화됨**을 선택합니다. **TCP/IP**를 두 번 클릭하고 **프로토콜** 탭으로 전환한 다음 **IPAll**이 나올 때까지 아래로 스크롤하고 **TCP 포트** 필드에 **1433**을 입력합니다. **확인**을 클릭하고 **SQL Server** 서비스를 다시 시작합니다.



20. [ESET PROTECT 서버 또는 MDM을 DB에 연결](#)합니다.

## MySQL Server의 마이그레이션 프로세스

### 필수 구성 요소

- 소스 및 대상 SQL Server 인스턴스가 설치되어 있어야 하며, 이러한 인스턴스는 서로 다른 컴퓨터에서 호스팅될 수 있습니다. 이러한 인스턴스는 서로 다른 컴퓨터에서 호스팅될 수 있습니다.
- MySQL 도구를 하나 이상의 컴퓨터(mysqlump 및 mysql 클라이언트)에서 사용할 수 있어야 합니다.

### 유용한 링크

- <https://dev.mysql.com/doc/refman/5.6/en/copying-databases.html>
- <https://dev.mysql.com/doc/refman/5.6/en/mysqldump.html>
- <https://dev.mysql.com/doc/refman/5.6/en/mysql.html>

### 마이그레이션 프로세스

명령에서 아래 구성 파일이나 SQL 문을 항상 다음 항목으로 바꾸십시오.

- **SRCHOST**를 소스 DB 서버의 주소로 바꿉니다.
- **SRCROOTLOGIN**을 소스 MySQL Server 루트 사용자 로그인으로 바꿉니다.
- **SRCDBNAME**을 백업할 소스 ESET PROTECT DB의 이름으로 바꿉니다.
- **BACKUPFILE**을 백업이 저장되는 파일의 경로로 바꿉니다.
- **TARGETROOTLOGIN**을 대상 MySQL Server 루트 사용자 로그인으로 바꿉니다.
- **TARGETHOST**를 대상 DB 서버의 주소로 바꿉니다.
- **TARGETDBNAME**을 대상 ESET PROTECT DB(마이그레이션 후)의 이름으로 바꿉니다.
- **TARGETLOGIN**을 대상 DB 서버의 새 ESET PROTECT DB 사용자의 로그인 이름으로 바꿉니다.
- **TARGETPASSWD**를 대상 DB 서버의 새 ESET PROTECT DB 사용자의 패스워드로 바꿉니다.

명령줄을 통해 아래 SQL 문을 실행하지 않아도 됩니다. 사용 가능한 GUI 도구가 있는 경우 기존에 알고 있던 애플리케이션을 사용해도 됩니다.

1. ESET PROTECT 서버/MDM 서비스를 중지합니다.
2. 소스 ESET PROTECT DB(마이그레이션할 DB)의 전체 DB 백업을 생성합니다.

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -  
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. 대상 MySQL Server에서 빈 DB를 준비합니다.

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

**i** Linux 시스템에서는 따옴표(") 대신 아포스트로피(')를 사용하십시오.

4. 대상 MySQL Server의 DB를 이전에 준비한 빈 DB로 복원합니다.

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. 대상 MySQL Server에서 ESET PROTECT DB 사용자를 생성합니다.

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

**TARGETLOGIN**에 권장되는 문자:

- 소문자 ASCII 문자, 숫자 및 밑줄("\_")

**TARGETPASSWD**에 권장되는 문자:

- ASCII 문자만(대문자 및 소문자 ASCII 문자, 숫자, 공백, 특수 문자 포함)
- ASCII 이외의 문자는 사용하지 마십시오(예: 중괄호({})나 @).



위의 문자 권장 사항을 따르지 않을 경우 DB 연결에 문제가 발생하거나 DB 연결 문자열을 수정하는 동안 나중의 단계에서 특수 문자를 이스케이프해야 할 수 있습니다. 이 문서에는 문자 이스케이프 규칙이 포함되어 있지 않습니다.

6. 대상 MySQL Server에서 ESET PROTECT DB 사용자에게 적절한 접근 권한을 부여합니다.

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

**i** Linux 시스템에서는 따옴표(") 대신 아포스트로피(')를 사용하십시오.

7. **tbl\_authentication\_certificate** 표의 콘텐츠를 제거합니다(삭제하지 않으면 에이전트가 새 서버에 연결되지 않을 수 있음).

```
mysql --host TARGETHOST -u root -p "--  
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. [ESET PROTECT 서버 또는 MDM을 DB에 연결](#)합니다.

## ESET PROTECT 서버 또는 MDM을 DB에 연결

ESET PROTECT 서버 또는 ESET PROTECT MDM이 설치되어 있는 컴퓨터에서 아래 단계에 따라 DB에 연결합니다.

1. ESET PROTECT 서버/MDM 서비스를 중지합니다.

2. *startupconfiguration.ini* 찾기

- Windows:

서버:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration\startupconfiguration.ini
```

- Linux:

서버:

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore:

```
/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini
```

3. ESET PROTECT 서버/MDM *startupconfiguration.ini*에서 DB 연결 문자열을 변경합니다.

o 새 DB 서버의 주소와 포트를 설정합니다.

o 연결 문자열에 새 ESET PROTECT 사용자 이름 및 패스워드를 설정합니다.

최종 결과의 형식은 다음과 같습니다.

- Microsoft SQL:

```
DatabaseType=MSSQL0dbc
```

```
DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pwd={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySQL0dbc
```

```
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETLOGIN;Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

위의 구성에서는 항상 다음을 교체하십시오.

- **TARGETHOST**를 대상 DB 서버의 주소로 바꿉니다.
- **TARGETDBNAME**을 대상 ESET PROTECT DB(마이그레이션 후)의 이름으로 바꿉니다.
- **TARGETLOGIN**을 대상 DB 서버의 새 ESET PROTECT DB 사용자의 로그인 이름으로 바꿉니다.
- **TARGETPASSWD**를 대상 DB 서버의 새 ESET PROTECT DB 사용자의 패스워드로 바꿉니다.

4. ESET PROTECT 서버 또는 ESET PROTECT MDM을 시작하고 서비스가 제대로 실행되고 있는지 확인합니다.

## MDM 마이그레이션

**i** ESET PROTECT 모바일 장치 관리/컨넥터(MDM/MDC) 구성 요소(온-프레미스 전용)가 수명 종료될 예정입니다. [자세한 내용](#). [클라우드 모바일 장치 관리로 마이그레이션](#)하는 것이 좋습니다.

모바일 장치 관리(온-프레미스)를 한 서버에서 다른 서버로 마이그레이션하려면 아래 지침을 따르십시오.

### 한 서버에서 다른 서버로의 모바일 장치 관리 마이그레이션(온-프레미스)

이 절차의 목표는 ESET PROTECT MDM의 기존 인스턴스를 마이그레이션하고 등록된 모바일 장치를 포함하는 기존 **ESET PROTECT MDM DB**를 유지하는 것입니다. 마이그레이션된 ESET PROTECT MDM은 이전 ESET

PROTECT MDM과 동일한 IP 주소/호스트 이름을 사용하게 되며, 설치 전에 이전 ESET PROTECT MDM의 DB를 새 MDM 호스트로 가져옵니다.

- [DB 마이그레이션](#)은 동일한 DB 유형 간(MySQL에서 MySQL로 또는 Microsoft SQL에서 Microsoft SQL로)에만 지원됩니다.
- DB를 마이그레이션할 때는 동일한 ESET PROTECT 버전의 인스턴스 간에 마이그레이션해야 합니다. ESET PROTECT 구성 요소의 버전을 확인하는 지침은 ESET의 [지식 베이스 문서](#)를 참조하십시오. DB 마이그레이션을 완료한 후 필요한 경우 업그레이드를 수행하여 최신 버전의 ESET PROTECT를 사용할 수 있습니다.

#### □ 현재(이전) ESET PROTECT MDM 서버에서:

1. MDM 구성의 백업을 생성합니다.

a)컴퓨터에서 MDM 서버를 클릭하고 **상세 정보**를 선택합니다.

b)구성 > 구성 요청을 클릭합니다. 요청된 구성이 생성될 때까지 에이전트 연결 간격에 따라 잠시 기다려야 할 수 있습니다.

c)ESET PROTECT Mobile Device Connector를 클릭하고 **구성 열기**를 선택합니다.

d)구성에서 외부 저장소로 다음 항목을 내보냅니다.

oMDM 서버의 정확한 호스트 이름.

o피어 인증서 - 내보낸 .pfx 파일에는 개인 키가 포함됩니다.



Linux에서 ESET PROTECT MDM 서버를 실행하는 경우, MDM 구성 정책에서 HTTPS 인증서를 내보내야 합니다.

I.HTTPS 인증서 옆에 있는 **보기**를 클릭합니다.

II. **다운로드**를 클릭하고 PFX 형식으로 HTTPS 인증서를 다운로드합니다.

e)다음과 같은 인증서 및 토큰을 내보낼 수도 있습니다(있는 경우).

o등록 프로필 서명 인증서.

oAPNS 인증서(APNS 인증서 및 APNS 개인 키 둘 다 내보내기)

oApple DEP(Device Enrollment Program) 인증 토큰

2. ESET PROTECT MDM 서비스를 중지합니다.

3. [ESET PROTECT MDM DB를 내보내고 백업합니다](#).

4. 현재 ESET PROTECT MDM 컴퓨터를 끕니다.



아직 이전 ESET PROTECT MDM을 제거/해제하지 마십시오.

## □ 새 ESET PROTECT MDM 서버에서:

**!** 새 ESET PROTECT MDM 서버의 네트워크 구성("이전" MDM 서버의 구성에서 내보낸 호스트 이름)이 이전 ESET PROTECT MDM과 일치하는지 확인하십시오.

1. 지원되는 ESET PROTECT MDM DB를 설치/실행합니다.
2. 이전 ESET PROTECT MDM에서 ESET PROTECT MDM DB를 가져오기/복원합니다.
3. 통합형 패키지 설치 관리자(Windows)를 사용하여 ESET PROTECT 서버/MDM을 설치하거나 다른 설치 방법(Windows 수동 설치, Linux 또는 가상 어플라이언스)을 선택합니다. ESET PROTECT MDM 설치 중에 DB 연결 설정을 지정합니다.

**!** Linux에 ESET PROTECT MDM을 설치할 때 백업에서 HTTPS 인증서를 사용합니다.

4. ESET PROTECT 웹 콘솔에 연결합니다.
5. ESET PROTECT MDM 서비스를 다시 시작합니다.

이제 관리되는 모바일 장치가 원래 인증서를 사용해서 새 ESET PROTECT MDM 서버에 연결됩니다.

## □ 이전 ESET PROTECT 서버/MDM 제거:

새 ESET PROTECT 서버에서 모든 항목이 올바르게 실행되도록 한 후 단계별 지침을 사용하여 이전 ESET PROTECT 서버/MDM을 주의해서 해제하십시오.

# 마이그레이션 후 ESET PROTECT 서버의 IP 주소 또는 호스트 이름 변경

ESET PROTECT 서버의 IP 주소 또는 호스트 이름을 변경하려면 다음 단계를 따르십시오.

1. ESET PROTECT 서버 인증서에 특정 IP 주소 및/또는 호스트 이름이 포함된 경우 새 서버 인증서를 생성하고 전환하려는 새 IP 주소 또는 호스트 이름을 포함합니다. 그러나 서버 인증서의 호스트 필드에 와일드카드 \*가 있는 경우 2단계로 건너뛰십시오. 와일드카드 \*가 없는 경우 새 IP 주소 및 호스트 이름을 쉼표로 구분해서 추가하여 새 서버 인증서를 생성하고 이전 IP 주소 및 호스트 이름도 포함합니다.
2. ESET PROTECT 서버 인증 기관을 사용하여 새 서버 인증서에 서명합니다.
3. 새 IP 주소 또는 호스트 이름(가능하면 IP 주소)에 대한 클라이언트 연결을 변경하는 정책을 만들되, 이전 IP 주소 또는 호스트 이름에 대한 두 번째(대체) 연결을 포함하여 ESET Management 에이전트에 두 서버에 모두 연결할 기회를 제공합니다. 자세한 내용은 ESET Management 에이전트를 새 ESET PROTECT 서버에 연결하는 정책 만들기를 참조하십시오.
4. 이 정책을 클라이언트 컴퓨터에 적용하고 ESET Management 에이전트가 복제할 수 있도록 합니다. 정책에서 클라이언트를 새 서버(실행되고 있지 않음)로 리디렉션하더라도 ESET Management 에이전트는 대체 서버 정보를 사용하여 원래 IP 주소에 연결합니다.
5. 추가 > 설정에서 새 서버 인증서를 설정합니다.

6. ESET PROTECT 서버 서비스를 다시 시작하고 IP 주소 또는 호스트 이름을 변경합니다.

ESET PROTECT 서버 주소 변경에 대한 지침은 [지식 베이스 문서](#)를 참조하십시오.

## ESET PROTECT 서버 및 해당 구성 요소 제거

ESET PROTECT 서버 및 해당 구성 요소를 제거하려면 아래의 장 중 하나를 선택합니다.

- [ESET Management 에이전트 제거](#)
- [Windows - ESET PROTECT 서버 및 해당 구성 요소 제거](#)
- [Linux - ESET PROTECT 구성 요소 업그레이드, 다시 설치 또는 제거](#)
- [macOS - ESET Management Agent 및 ESET Endpoint 제품 제거](#)
- [다른 서버로 마이그레이션한 후 이전 ESMC/ESET PROTECT/MDM 서버 해제](#)

## ESET Management 에이전트 제거

ESET Management 에이전트는 여러 가지 방법으로 제거할 수 있습니다.

### ESET PROTECT 웹 콘솔을 사용한 원격 제거


1. [ESET PROTECT 웹 콘솔에 로그인](#)합니다.
2. 컴퓨터 창에서 ESET Management 에이전트를 제거할 컴퓨터를 선택하고 **새 작업**을 클릭합니다.  
또는 해당 확인란을 선택하여 여러 컴퓨터를 선택한 다음 **컴퓨터 > 작업 > 새 작업**을 클릭합니다.
3. 작업 이름을 입력합니다.
4. 작업 범주 드롭다운 메뉴에서 **ESET PROTECT**를 선택합니다.
5. 작업 드롭다운 메뉴에서 [관리 중단\(ESET Management 에이전트 제거\)](#)을 선택합니다.

클라이언트 컴퓨터에서 ESET Management Agent를 제거하면 ESET PROTECT에서 더 이상 해당 장치를 관리하지 않습니다.

- ESET Management Agent를 제거한 후에 ESET 보안 제품에 일부 설정이 남아 있을 수 있습니다.
- 에이전트가 패스워드로 보호되고 있다면, 이를 제거할 수 없습니다. 관리에서 장치를 제거하기 전에 **정책**을 사용하여 유지하지 않으려는 일부 설정(예: 비밀번호 보호)을 기본 설정으로 다시 설정하는 것이 좋습니다.
- 또한 에이전트에서 실행 중인 모든 작업이 중단됩니다. 복제에 따라서는 ESET PROTECT 웹 콘솔에 이 작업의 **실행 중**, **마침** 또는 **실패** 실행 상태가 정확하게 표시되지 않을 수도 있습니다.
- 에이전트를 제거한 후에는 통합 EGUI 또는 [eShell](#)을 통해 보안 제품을 관리할 수 있습니다.


6. 작업 **요약**을 검토하고 **마침**을 클릭합니다.
7. [트리거 생성](#)을 클릭하여 이 클라이언트 작업을 실행해야 하는 시기와 **대상**을 지정합니다.

## 로컬 제거 - Windows


 [Linux](#) 또는 [macOS](#)에서 ESET Management 에이전트 로컬 제거 지침도 참조하십시오.  
에이전트 제거 문제를 해결하려면 [ESET Management 에이전트 제거 문제 해결](#)을 참조하십시오.

1. ESET Management 에이전트를 제거할(예: RDP를 통해) 끝점 컴퓨터에 연결합니다.
2. 제어판 > 프로그램 및 기능으로 이동하여 **ESET Management 에이전트**를 두 번 클릭합니다.
3. 다음 > 제거를 클릭하고 제거 지침을 따릅니다.

ESET Management 에이전트 정책을 사용하여 패스워드를 설정한 경우 다음 옵션이 제공됩니다.

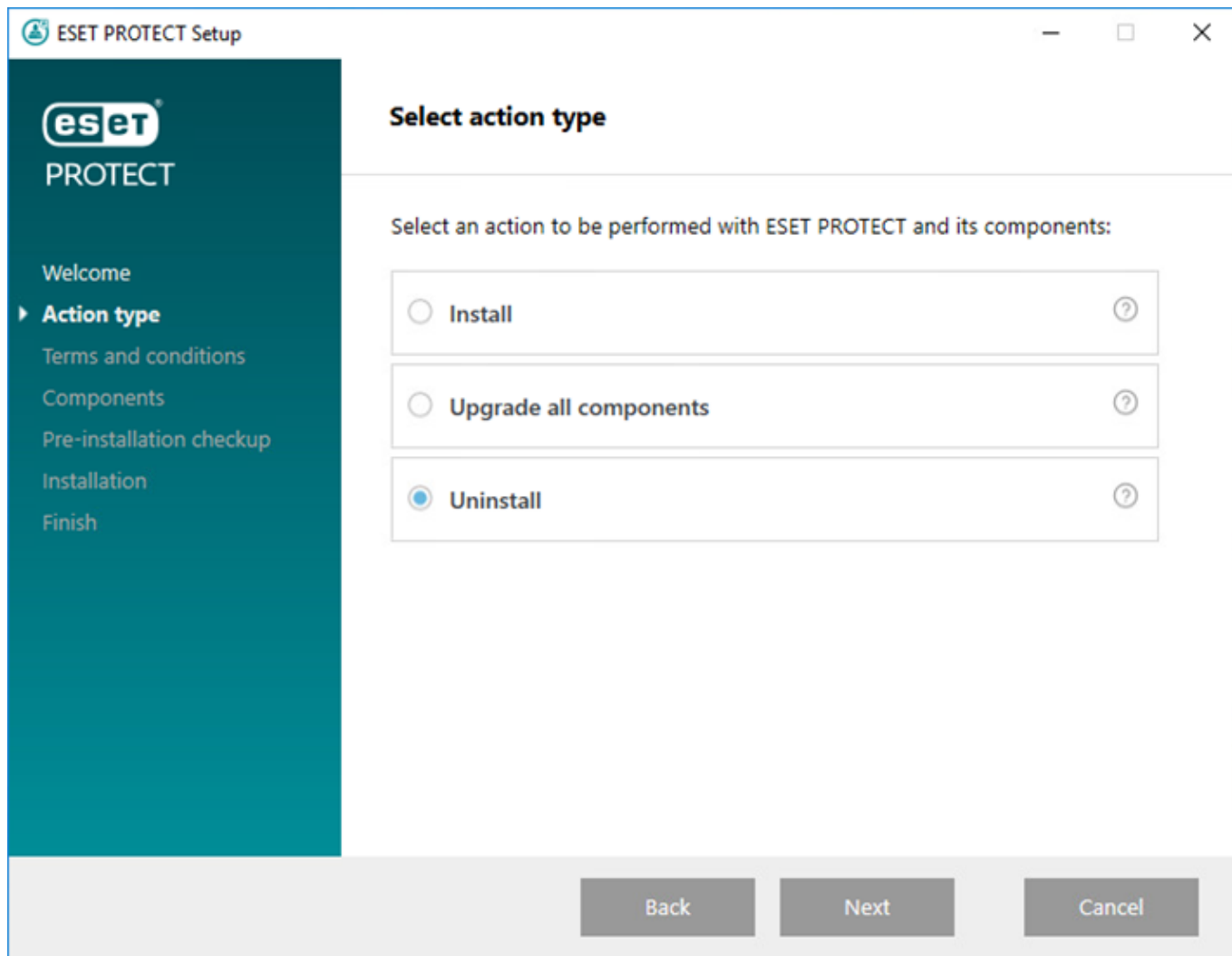
- 제거 중에 패스워드를 입력해야 합니다.
-  • ESET Management 에이전트를 제거하기 전에 먼저 정책을 할당 취소합니다.
- [패스워드로 보호되는 기존 에이전트 위에 ESET Management 에이전트를 재배포합니다](#)(지식베이스 문서).

## Windows - ESET PROTECT 서버 및 해당 구성 요소 제거

 ESET PROTECT을(를) 제거하기 전에 [관리되는 컴퓨터에서 에이전트를 제거](#)합니다.  
모바일 장치 커넥터를 제거하기 전에 [MDM iOS 라이선스 기능](#)을 읽어 보십시오.

다음 단계를 수행하여 Windows에서 ESET PROTECT 서버와 해당 구성 요소를 제거합니다.

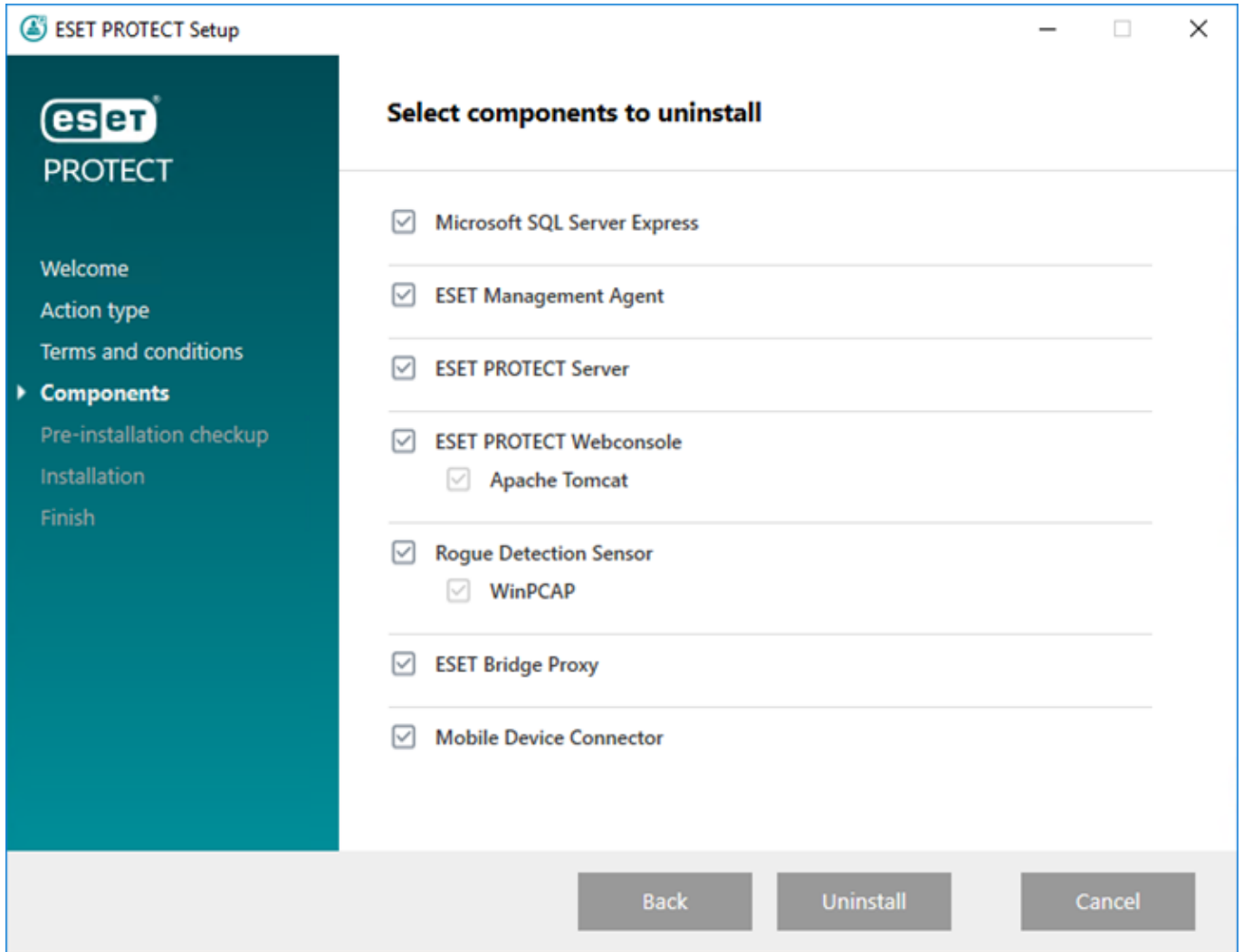
1. [ESET PROTECT 통합형 설치 관리자](#)를 다운로드하고 패키지의 압축을 풉니다.
2. *Setup.exe*를 실행합니다. 드롭다운 메뉴에서 언어를 선택할 수 있습니다. 다음을 클릭합니다.
3. 제거를 선택하고 다음을 클릭합니다.



4. EULA에 동의한 후 **다음**을 클릭합니다.

5. 제거하려는 구성 요소를 선택하고 **제거**를 클릭합니다.





6. 특정 구성 요소 제거를 완료하기 위해 컴퓨터를 다시 시작해야 할 수 있습니다.

**i** 다른 서버로 마이그레이션한 후 이전 ESMC/ESET PROTECT/MDM 서버 해제도 참조하십시오.

## Linux - ESET PROTECT 구성 요소 업그레이드, 다시 설치 또는 제거

최신 버전으로 다시 설치하거나 업그레이드하려면 설치 스크립트를 다시 실행하십시오.

구성 요소를 제거하려면(이 경우 ESET PROTECT 서버) 여기에 표시된 것처럼 `--uninstall` 파라미터를 사용하여 설치 관리자를 실행하십시오.

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

다른 구성 요소를 제거하려면 명령에서 해당 패키지 이름을 사용합니다. 예: ESET Management 에이전트:

```
sudo ./agent-linux-x86_64.sh --uninstall
```



제거 중에 구성 및 DB 파일이 제거됩니다. DB 파일을 보존하려면 DB의 SQL 덤프를 만들거나 --keep-database 파라미터를 사용합니다.

제거 후

- eraserver 서비스가 삭제되었는지 확인합니다.
- /etc/opt/eset/RemoteAdministrator/Server/ 폴더가 삭제되었는지 확인합니다.



데이터를 복원해야 할 경우 제거를 수행하기 전에 DB 덤프 백업을 만드는 것이 좋습니다. 에이전트 재설치에 대한 자세한 내용은 관련 [장](#)을 참조하십시오. 에이전트 제거 문제를 해결하려면 [ESET Management 에이전트 제거 문제 해결](#)을 참조하십시오.

## macOS - ESET Management Agent 및 ESET Endpoint 제품 제거

ESET Management을(를) 통해 로컬 또는 원격으로 ESET PROTECT Agent 및 ESET Endpoint 제품을 제거합니다.

ESET Management Agent 및 ESET Endpoint 제품의 로컬 제거에 대한 자세한 지침은 당사 [지식베이스 문서](#)에서 확인할 수 있습니다.



ESET Endpoint 제품을 원격으로 제거하려면, ESET Management Agent를 제거하기 전에 제거해야 합니다.

### ESET Management Agent를 로컬에서 제거

1. 찾기를 클릭하여 새 찾기 창을 엽니다.
2. 애플리케이션을 클릭하고 > CTRL을 누른 상태에서 > ESET Management Agent를 클릭한 후 오른쪽 마우스 버튼 메뉴에서 패키지 내용 표시를 선택합니다.
3. 내용 > 스크립트로 이동한 후 Uninstaller.command를 두 번 클릭하여 제거 관리자를 실행합니다.
4. 관리자 패스워드를 입력하고, 패스워드를 입력하라는 메시지가 표시되면 Enter를 누릅니다.
5. ESET Management Agent가 제거되면 프로세스 완료됨 메시지가 표시됩니다.

### 터미널을 통해 ESET Management Agent를 로컬에서 제거

1. 찾기 > 애플리케이션 > 유틸리티 > 터미널을 엽니다.
2. 다음 코드를 입력하고 Enter 키를 누릅니다.

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;
exit;
```

3. 관리자 패스워드를 입력하고, 패스워드를 입력하라는 메시지가 표시되면 Enter를 누릅니다.

4. ESET Management Agent가 제거되면 **프로세스 완료됨** 메시지가 표시됩니다.

## ESET Management을(를) 통해 ESET PROTECT 에이전트를 원격으로 제거

컴퓨터에서 클라이언트 macOS 컴퓨터를 클릭하고 [제거](#)를 선택하여 ESET Management Agent를 제거한 후 관리에서 컴퓨터를 제거합니다.

에이전트 제거 문제를 해결하려면 [ESET Management 에이전트 제거 문제 해결](#)을 참조하십시오.

## 로컬에서 ESET Endpoint 제품 제거

1. 찾기를 클릭하여 새 찾기 창을 엽니다.
2. 애플리케이션을 클릭하고 > CTRL을 누른 상태에서 > **ESET Endpoint Security** 또는 **ESET Endpoint Antivirus**를 클릭한 후 오른쪽 마우스 버튼 메뉴에서 **패키지 내용 표시**를 선택합니다.
3. **내용 > 헬퍼**로 이동한 후 **Uninstaller.app**을 두 번 클릭하여 제거 관리자를 실행합니다.
4. **제거**를 클릭합니다.
5. 관리자 패스워드를 입력하고, 패스워드를 입력하라는 메시지가 표시되면 **확인**을 누릅니다.
6. ESET Endpoint Security 또는 ESET Endpoint Antivirus가 제거되었으면 **제거 성공** 메시지가 표시됩니다. 닫기를 클릭합니다.

## 터미널을 통해 로컬에서 ESET Endpoint 제품 제거

1. **찾기 > 애플리케이션 > 유틸리티 > 터미널**을 엽니다.
2. 다음 코드를 입력하고 **Enter** 키를 누릅니다.

- 제거 ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app/  
Contents/Scripts/uninstall.sh
```

- 제거 ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/  
Contents/Scripts/uninstall.sh
```

3. 관리자 패스워드를 입력하고, 패스워드를 입력하라는 메시지가 표시되면 **Enter**를 누릅니다.
4. ESET Endpoint 제품이 제거되면 **프로세스 완료됨** 메시지가 표시됩니다.

## ESET PROTECT을(를) 통해 원격으로 ESET Endpoint 제품 제거

ESET Management을(를) 통해 원격으로 ESET PROTECT Agent를 제거하려면 다음 옵션 중 하나를 사용하면 됩니다

니다.

- 컴퓨터에서 클라이언트 macOS 컴퓨터를 설치하고 **상세 정보 > 설치된 애플리케이션**을 선택한 후 > **ESET Endpoint Security** 또는 **ESET Endpoint Antivirus**를 선택하고 **제거** 버튼을 클릭합니다.
- [소프트웨어 제거 작업](#)을 사용합니다.

## 다른 서버로 마이그레이션한 후 이전 ESMC/ESET PROTECT/MDM 서버 해제

**!** 새 ESET PROTECT 서버/MDM이 실행 중이며 클라이언트 컴퓨터 및 모바일 장치가 새 ESET PROTECT에 올바르게 연결되어 있는지 확인합니다.

다른 서버로 마이그레이션한 후 이전 ESMC/ESET PROTECT 서버/MDM을 해제할 경우 몇 가지 옵션이 있습니다.

### I. 서버 컴퓨터 OS를 유지하고 재사용

1. [이전 ESMC/ESET PROTECT 서버 서비스를 중지합니다.](#)
2. 이전 ESMC/ESET PROTECT 서버 데이터베이스 인스턴스(Microsoft SQL 또는 MySQL)를 제거합니다(DROP DATABASE).

**!** 데이터베이스를 새 ESET PROTECT 서버로 마이그레이션한 경우 새 ESMC 서버 데이터베이스에서 라이선스가 연결 해제(제거)되지 않도록 하려면 이전 ESET PROTECT/ESET PROTECT 서버를 제거하기 전에 해당 데이터베이스를 제거해야 합니다.

3. 이전 ESET PROTECT/MDM 서버와 모든 구성 요소(ESET Management Agent, Rogue Detection Sensor, MDM 등 포함)를 제거합니다.

o [ESET PROTECT 제거 - Windows](#)

o [ESET PROTECT 제거 - Linux](#)

**!** DB에 종속된 다른 소프트웨어가 있는 경우 DB를 제거하지 마십시오.

4. 제거 후 서버의 운영 체제 다시 시작을 계획합니다.

### II. 서버 컴퓨터 유지

ESMC/ESET PROTECT/MDM을 제거하는 가장 쉬운 방법은 설치되어 있는 디스크를 포맷하는 것입니다.

**!** 이렇게 하면 OS를 포함하여 디스크에 있는 모든 것이 지워집니다.

# 문제 해결

ESET PROTECT는 여러 타사 도구를 사용하고 많은 OS 플랫폼을 지원하는 복잡한 제품이므로 문제 해결이 필요한 문제가 발생할 수 있습니다.

ESET 문서에는 ESET PROTECT 문제를 해결하기 위한 여러 가지 방법이 포함되어 있습니다. ESET PROTECT에서 발생하는 일반적인 몇 가지 문제를 해결하려면 [일반적인 설치 문제에 대한 대답](#)을 참조하십시오. [ESET 비즈니스 제품에 대한 알려진 문제](#)도 참조하십시오.

## 문제를 해결할 수 없습니까?

- 각 ESET PROTECT 구성 요소에는 상세 수준이 높아지거나 낮아지도록 구성할 수 있는 [로그 파일](#)이 있습니다. 로그를 검토하여 현재 있는 문제를 설명할 수 있는 오류를 식별하십시오.
- 각 구성 요소의 로그 기록 상세 수준은 해당 [정책](#) > [고급 설정](#) > [로깅](#) > [추적 로그 상세 수준](#) - [추적](#)(정보)부터 [중요](#)(가장 중요한 정보) 수준까지 수집되어 로깅되는 정보 수준을 결정하도록 로그 상세 수준을 설정할 수 있습니다.

o [ESET Management Agent 정책](#) - 이 정책을 실행하려면 장치에 적용해야 합니다. *trace.log* 파일에서 전체 ESET Management 에이전트 로깅을 활성화하려면, *trace.log*와 동일한 폴더에서 확장명 없이 *traceAll*이라는 이름의 더미 파일을 생성한 후 컴퓨터를 다시 시작(하여 ESET Management 에이전트 서비스를 다시 시작)합니다.

### o [ESET PROTECT 서버 설정](#)

o ESET Mobile Device Connector 정책 - 이 정책을 실행하려면 장치에 적용해야 합니다. [MDM 문제 해결](#)도 참조.

- 문제를 해결할 수 없는 경우 [ESET 보안 포럼](#)을 방문하여 ESET 커뮤니티에 발생할 수 있는 문제에 대한 정보를 문의할 수 있습니다.
- [ESET 기술 지원](#)에 문의하면 [ESET Log Collector](#) 또는 [진단 도구](#)를 사용하여 로그 파일을 수집해 달라는 요청을 받을 수 있습니다. 고객 지원 서비스 요청을 빠르게 진행하려면 지원에 문의 시 로그를 포함하는 것이 좋습니다.

## 오프라인 환경에서 ESET PROTECT 구성 요소 업그레이드

다음 단계에 따라 인터넷에 액세스하지 않고 ESET PROTECT 구성 요소와 ESET 끝점 제품을 업그레이드합니다.

다음 조건이 충족되면 오프라인 환경에 [구성 요소 업그레이드 작업](#)을 사용할 수 있습니다.



- 사용 가능한 [오프라인 저장소](#)가 있을 경우
- ESET Management 에이전트 저장소의 위치가 [정책](#)을 사용하여 접근 가능한 위치에 구성된 경우

## 먼저 ESET PROTECT 서버와 웹 콘솔을 업그레이드합니다

1. 서버에서 실행 중인 [ESET 관리 콘솔의 버전을 확인](#)합니다.
2. 최신 [Windows용 통합형 설치 관리자](#)를 다운로드하거나, ESET 다운로드 사이트에서 최신 [Linux용 독립 실행형 ESET PROTECT 구성 요소 설치 관리자](#)를 다운로드합니다.
3. ESET PROTECT 서버와 ESET PROTECT 웹 콘솔을 업그레이드합니다.
  - Windows - [통합형 설치 관리자를 사용하여 업그레이드](#)
  - Linux - [수동 구성 요소 기반 업그레이드](#)

**i** 웹 콘솔 및 Apache Tomcat 업그레이드 시 [오프라인 도움말](#) 파일이 지워집니다. ESMC 또는 이전 ESET PROTECT 버전에서 오프라인 도움말을 사용한 경우, 업그레이드한 후 ESET PROTECT 10.0용으로 다시 생성하여 ESET PROTECT 버전과 일치하는 최신 오프라인 도움말이 있는지 확인하십시오.

## ESET 끝점 제품의 오프라인 업그레이드를 계속 진행합니다

1. 클라이언트에 설치된 ESET 제품을 확인합니다. ESET PROTECT 웹 콘솔을 열고 **대시보드 > ESET 애플리케이션**으로 이동합니다.
2. [최신 버전의 ESET Endpoint 제품](#)이 있는지 확인합니다.
3. [ESET 다운로드 사이트](#)로부터 [오프라인 설치](#) 동안 구성된 로컬 저장소로 설치 관리자를 다운로드합니다.
4. ESET PROTECT 웹 콘솔에서 [소프트웨어 설치 작업](#)을 실행합니다.

## 일반적인 설치 문제에 대한 대답

해결할 오류 메시지에 대한 섹션을 확장합니다.

 [ESET PROTECT 서버](#)

ESET PROTECT 서버 서비스가 시작되지 않음:

## 손상된 설치

- 이 오류는 레지스트리 키나 파일이 누락되거나 파일 권한이 잘못되어 발생할 수 있습니다.
- ESET 통합형 설치 관리자에는 [자체 로그 파일](#)이 있습니다. 수동으로 구성 요소를 설치할 경우 [MSI 로깅](#) 방법을 사용하십시오.

## 수신 대기 포트가 이미 사용되고 있음(주로 2222 및 2223)

해당 OS에 적합한 명령을 사용합니다.

- Windows:

```
netstat -an | find "2222"
```

```
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
```

```
netstat | grep 2223
```

## DB가 실행되지 않음/DB에 연결할 수 없음

- Microsoft SQL Server: DB 서버에서/DB 서버에 대해 포트 1433을 사용할 수 있는지 확인하거나 SQL Server Management Studio에 로그인해 보십시오.
- MySQL: DB 서버에서/DB 서버에 대해 포트 3306을 사용할 수 있는지 확인하거나 DB 인터페이스에 로그인해 보십시오(예: MySQL 명령줄 인터페이스 또는 phpmyadmin 사용).

## 손상된 DB

여러 SQL 오류가 ESET PROTECT 서버 로그 파일에 표시됩니다. 백업에서 DB를 복원하는 것이 좋습니다. 백업이 없는 경우 ESET PROTECT을(를) 다시 설치합니다.

## 시스템 리소스(RAM, 디스크 공간) 부족

실행 중인 프로세스 및 시스템 성능을 검토합니다.

- Windows 사용자: 작업 관리자 또는 이벤트 뷰어를 실행하여 정보를 검토합니다.
- Linux 사용자: 다음 명령 중 하나를 실행합니다.

```
df -h(디스크 공간 정보 검토)
```

```
cat /proc/meminfo(메모리 공간 정보 검토)
```

```
dmesg(Linux 시스템 상태 검토)
```

## ESET PROTECT 서버 설치 중에 ODBC 커넥터와 관련하여 발생하는 오류

Error: (Error 65533) ODBC connector compatibility check failed.

Please install ODBC driver with support for multi-threading.

다중 스레딩을 지원하는 ODBC 드라이버 버전을 다시 설치하거나 [ODBC 구성 섹션](#)에 설명된 대로 *odbcinst.ini*를 다시 구성하십시오.

## ESET PROTECT 서버 설치 중에 DB 연결과 관련하여 발생하는 오류

ESET PROTECT 서버 설치를 완료한 후 다음과 같은 오류 메시지가 표시됩니다.

The database server is not configured correctly.

Please check the documentation and reconfigure the database server as needed.

설치 로그의 오류 메시지:

Error: Execution test of long statement failed with exception:

CMysqlCodeTokenExecutor: CheckVariableInnodbLogFileSize:

Server variables innodb\_log\_file\_size\*innodb\_log\_files\_in\_group

value 100663296 is too low.

DB 드라이버 구성이 [ODBC 구성 섹션](#)에 설명된 DB 드라이버 구성과 일치하는지 확인하십시오.



## ESET Management 에이전트 제거 문제 해결

• ESET Management 에이전트의 [로그 파일](#)을 참조하십시오.

• [ESET 제거 도구](#)를 사용하거나 비표준 방법(예: 파일 제거, ESET Management 에이전트 서비스 및 레지스트리 항목 제거)을 사용하여 ESET Management 에이전트를 제거할 수 있습니다. 같은 컴퓨터에 ESET 끝점 제품이 있는 경우에는 [활성화된 자기 보호](#)로 인해 에이전트를 제거할 수 없습니다.

• 에이전트 제거 중에 "DB를 업그레이드할 수 없습니다. 먼저 제품을 제거하십시오."라는 메시지가 표시됩니다. ESET Management 에이전트 수리:

1. 제어판 > 프로그램 및 기능을 클릭하고 ESET Management 에이전트를 두 번 클릭합니다.

2. 다음 > 복구를 클릭하고 지침을 따릅니다.

ESET Management 에이전트를 제거하는 가능한 모든 방법이 [제거 섹션](#)에 설명되어 있습니다.

### 에이전트 설치 중에 오류 코드 1603 발생

이 오류는 설치 관리자 파일이 로컬 디스크에 없는 경우 발생할 수 있습니다. 이 문제를 해결하려면 설치 관리자 파일을 로컬 디렉터리에 복사하고 설치를 다시 실행합니다. 파일이 이미 있는 경우 또는 이 오류가 계속 발생하는 경우 [지식 베이스 지침](#)을 따르십시오.

### Linux에 에이전트를 설치하는 동안 오류 메시지가 표시됨

오류 메시지:

```
Checking certificate ... failed
```

```
Error checking peer certificate: NOT_REGULAR_FILE
```

이 오류는 설치 명령에서 잘못된 파일 이름이 사용되어 발생했을 수 있습니다. 콘솔은 대소문자를 구분합니다. 예를 들어 Agent.pfx는 agent.pfx와 다릅니다.

### Linux - Windows 8.1(32-비트) 원격 배포 실패

이 문제는 Microsoft의 KB3161949로 인해 발생한 인증 문제입니다. 이 문제는 배포가 실패한 호스트에서 해당 업데이트를 제거하는 방법으로만 해결할 수 있습니다.

### ESET Management 에이전트는 ESET PROTECT 서버에 연결할 수 없습니다.

[에이전트 연결 문제 해결](#) 및 [지식 베이스 문서](#)를 참조하십시오.

### 에이전트 스크립트 설치 관리자가 종료되었습니다(코드 30).

사용자 지정 설치 관리자 위치가 있는 에이전트 스크립트 설치 관리자를 사용하여 스크립트를 올바르게 편집하지 못했습니다. [도움말 페이지](#)를 검토하고 다시 시도하십시오.

#### [웹 콘솔에 연결](#)

#### [ESET Bridge HTTP 프로토콜](#)

#### [ESET Rogue Detector Sensor](#)

### ESET Rogue Detector trace.log에 다음 오류 메시지가 계속 기록되는 이유는 무엇입니까?

```
Information: CPCAPDeviceSniffer [Thread 764]:
```

```
CPCAPDeviceSniffer on rpcap://\Device\NPF_{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} threw error:
```

```
Device open failed with error:Error opening adapter:
```

```
The system cannot find the device specified. (20)
```

이 문제는 WinPcap 관련 문제입니다. ESET Rogue Detector Sensor 서비스를 중지하고 최신 버전의 WinPcap(4.1.0 이상)을 다시 설치한 후 ESET Rogue Detector Sensor 서비스를 다시 시작하십시오.

#### [Linux](#)

## CentOS Linux에 libQtWebKit 종속성이 없음

다음 오류가 표시되는 경우:

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
ESET의 지식 베이스 문서 지침을 따르십시오.
```

## CentOS 7에서 ESET PROTECT 서버 설치가 실패함

다음 오류가 표시되는 경우:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
이 문제는 환경/로컬 설정으로 인해 발생할 수 있습니다. 다음 명령을 실행하여 서버 설치 관리자 스크립트를 활용하십시오.
export LC_ALL="en_US.UTF-8"
```

## Microsoft SQL Server

### Microsoft SQL Server 설치 중에 오류 코드 2068052081이 표시됩니다.

컴퓨터를 다시 시작한 후 다시 설치하십시오. 문제가 계속되면 SQL Server Native Client를 제거한 후 다시 설치하십시오. 계속해서 문제가 해결되지 않으면 모든 Microsoft SQL Server 제품을 제거한 후 컴퓨터를 다시 시작하고 다시 설치하십시오.

### Microsoft SQL Server 설치 중에 오류 코드 2067922943이 표시됩니다.

시스템이 ESET PROTECT의 [DB 요구 사항](#)을 충족하는지 확인하십시오.

### Microsoft SQL Server 설치 중에 오류 코드 2067922934가 표시됩니다.

[사용자 계정 권한](#)이 올바른지 확인하십시오.

### 웹 콘솔에서 "데이터 로드 실패했습니다"라는 메시지가 나타납니다.

Microsoft SQL Server는 거래 로그에서 최대한 많은 디스크 공간을 사용하려고 합니다. 이를 정리하려면 [공식 Microsoft 웹사이트](#)를 방문하십시오.

### Microsoft SQL Server 설치 중 오류 코드 -2067919934가 표시됨

이전 단계가 모두 정상적으로 완료되었는지 확인합니다. 이 오류는 잘못된 구성된 시스템 파일로 인해 발생한 것입니다. 컴퓨터를 다시 시작한 후 다시 설치하십시오.

## 로그 파일

각 ESET PROTECT 구성 요소는 로깅을 수행합니다. ESET PROTECT 구성 요소는 특정 이벤트에 대한 정보를 로그 파일에 기록합니다. 로그 파일의 위치는 구성 요소에 따라 다릅니다. 로그 파일 위치 목록은 다음과 같습니다.

## Windows

ESET PROTECT 구성 요소	로그 파일 위치
ESET PROTECT 서버	C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\
ESET Management 에이전트	C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\ <a href="#">에이전트 연결 문제 해결</a> 도 참조하십시오.
ESET PROTECT 웹 콘솔 및 Apache Tomcat	C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs\ <a href="https://tomcat.apache.org/tomcat-9.0-doc/logging.html">https://tomcat.apache.org/tomcat-9.0-doc/logging.html</a> 도 참조
모바일 장치 커넥터	C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs\ <a href="#">MDM 문제 해결</a> 도 참조.

ESET PROTECT 구성 요소	로그 파일 위치
Rogue Detection Sensor	C:\ProgramData\ESET\Rogue Detection Sensor\Logs\
ESET Bridge HTTP 프록시	<a href="#">ESET Bridge 온라인 도움말</a> 을 참조하십시오.

- i** C:\ProgramData는 기본적으로 숨겨져 있습니다. 이 폴더를 표시하려면:
1. 시작 > 제어판 > 폴더 옵션 > 보기로 이동합니다.
  2. 숨김 파일, 폴더 및 드라이브 표시를 선택하고 **확인**을 클릭합니다.

## Linux

ESET PROTECT 구성 요소	로그 파일 위치
ESET PROTECT 서버	/var/log/eset/RemoteAdministrator/Server/ /var/log/eset/RemoteAdministrator/EraServerInstaller.log
ESET Management 에이전트	/var/log/eset/RemoteAdministrator/Agent/ /var/log/eset/RemoteAdministrator/EraAgentInstaller.log
모바일 장치 커넥터	/var/log/eset/RemoteAdministrator/MDMCore/ /var/log/eset/RemoteAdministrator/MDMCore/Proxy/ <a href="#">MDM 문제 해결</a> 도 참조.
ESET Bridge HTTP 프록시	<a href="#">ESET Bridge 온라인 도움말</a> 을 참조하십시오.
ESET PROTECT 웹 콘솔 및 Apache Tomcat	/var/log/tomcat/ <a href="https://tomcat.apache.org/tomcat-9.0-doc/logging.html">https://tomcat.apache.org/tomcat-9.0-doc/logging.html</a> 도 참조
ESET RD Sensor	/var/log/eset/RogueDetectionSensor/

## ESET PROTECT 가상 어플라이언스

ESET PROTECT 구성 요소	로그 파일 위치
ESET PROTECT VA 구성	/root/appliance-configuration-log.txt
ESET PROTECT 서버	/var/log/eset/RemoteAdministrator/EraServerInstaller.log
Apache HTTP 프록시	/var/log/httpd

## macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

## 분석 도구

분석 도구는 모든 ESET PROTECT 구성 요소에 포함되어 있습니다. 이 도구는 기술 지원 에이전트와 개발자가 제품 구성 요소의 문제를 해결하는 데 사용할 수 있는 로그를 수집하고 압축하는 데 사용됩니다.

## 분석 도구 위치

## Windows

폴더 `C:\Program Files\ESET\RemoteAdministrator\<product>\Diagnostic.exe`

## Linux

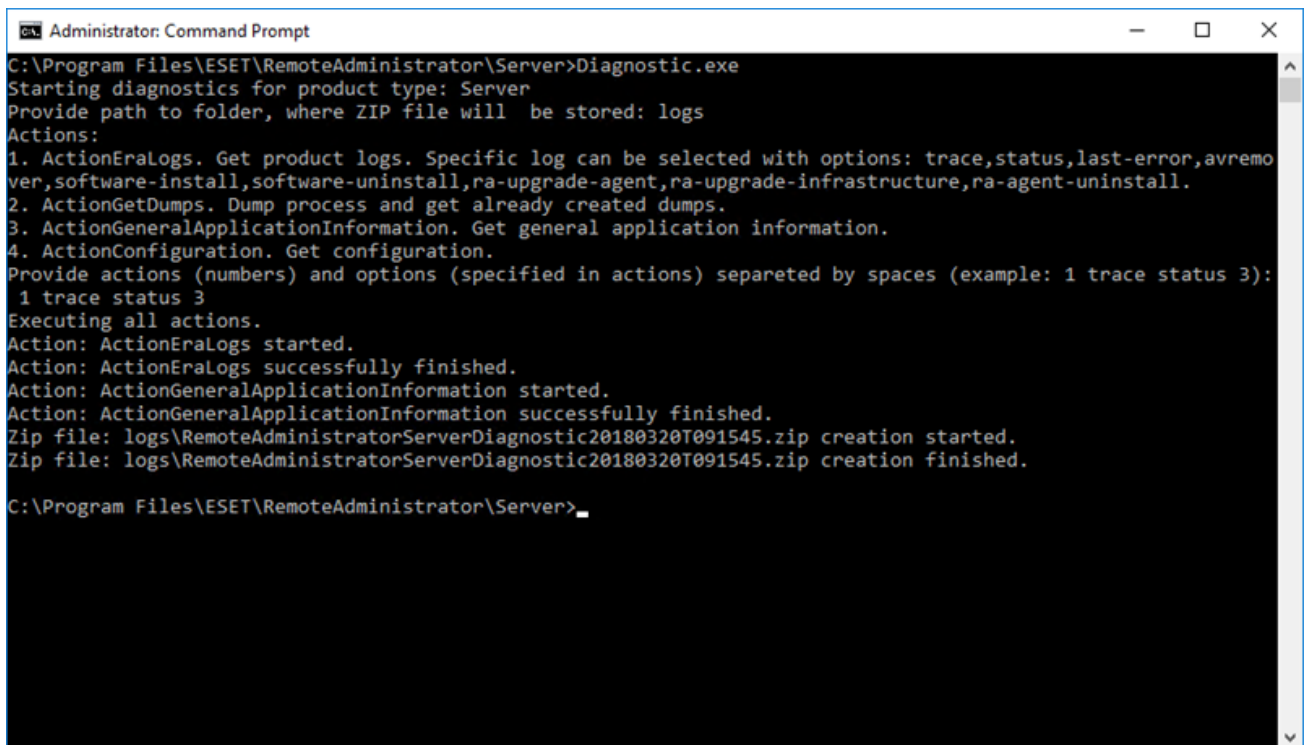
서버의 다음 디렉터리에 있음: `/opt/eset/RemoteAdministrator/<product>/`, **Diagnostics<product>** 실행 파일(**DiagnosticsServer**, **DiagnosticsAgent**등과 같이 한 단어로 구성)이 있습니다.

## 사용법(Linux)

터미널에서 진단 실행 파일을 루트 권한으로 실행하고 화면에 표시되는 지침을 따릅니다.

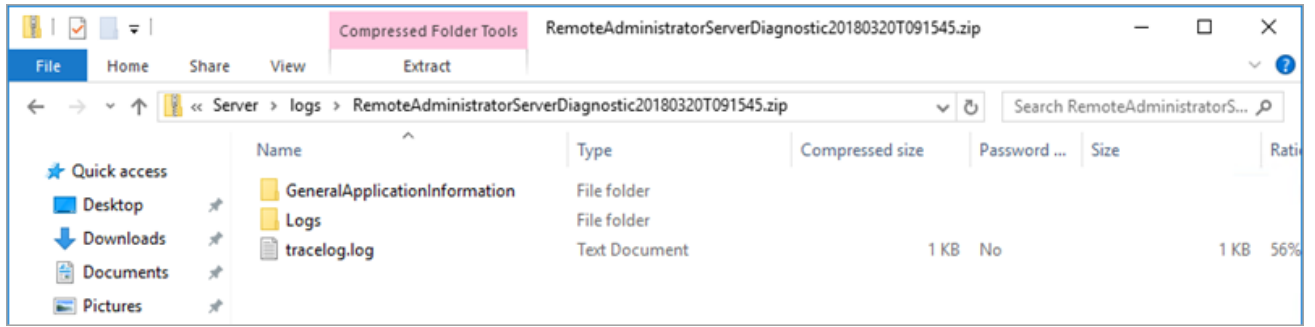
## 사용법(Windows)

1. 명령 프롬프트를 사용하여 도구를 실행합니다.
2. 로그 파일을 저장할 위치를 입력하고(이 예에서는 "logs") **Enter** 키를 누릅니다.
3. 수집할 정보를 입력합니다(이 예에서는 `1 trace status 3`). 자세한 내용은 아래 **동작**을 참조하십시오.



```
Administrator: Command Prompt
C:\Program Files\ESET\RemoteAdministrator\Server>Diagnostic.exe
Starting diagnostics for product type: Server
Provide path to folder, where ZIP file will be stored: logs
Actions:
1. ActionEraLogs. Get product logs. Specific log can be selected with options: trace,status,last-error,avremo
ver,software-install,software-uninstall,ra-upgrade-agent,ra-upgrade-infrastructure,ra-agent-uninstall.
2. ActionGetDumps. Dump process and get already created dumps.
3. ActionGeneralApplicationInformation. Get general application information.
4. ActionConfiguration. Get configuration.
Provide actions (numbers) and options (specified in actions) separated by spaces (example: 1 trace status 3):
1 trace status 3
Executing all actions.
Action: ActionEraLogs started.
Action: ActionEraLogs successfully finished.
Action: ActionGeneralApplicationInformation started.
Action: ActionGeneralApplicationInformation successfully finished.
Zip file: logs\RemoteAdministratorServerDiagnostic20180320T091545.zip creation started.
Zip file: logs\RemoteAdministratorServerDiagnostic20180320T091545.zip creation finished.
C:\Program Files\ESET\RemoteAdministrator\Server>
```

4. 작업을 마쳤으면 분석 도구 위치의 **"logs"** 디렉터리에서 **..zip** 파일로 압축된 로그 파일을 찾을 수 있습니다.



## 동작

- **ActionEraLogs** - 모든 로그가 저장되는 로그 폴더가 생성됩니다. 특정 로그만 지정하려면 공백을 사용하여 각 로그를 구분합니다.
- **ActionGetDumps** - 새 폴더가 생성됩니다. 문제가 탐지되면 프로세스 덤프 파일이 일반적으로 생성됩니다. 심각한 문제가 검색되면 시스템에서 덤프 파일이 생성됩니다. 수동으로 이를 확인하려면 %temp%(Windows) 또는 /tmp/(Linux) 폴더로 이동한 후 덤프 파일을 삽입합니다.

**i** 구성 요소 서비스(Agent, , Server, RD Sensor, )가 실행되고 있어야 합니다.

- **ActionGeneralApplicationInformation** - GeneralApplicationInformation 폴더가 생성되고 이 폴더 내에 GeneralApplicationInformation.txt 파일이 생성됩니다. 이 파일에는 현재 설치된 제품의 제품 이름과 제품 버전이 들어 있는 텍스트 정보가 포함됩니다.
- **ActionConfiguration** - storage.lua 파일이 저장되는 구성 폴더가 생성됩니다.

## ESET PROTECT 서버 업그레이드/마이그레이션 후 문제

설치가 손상되거나 알 수 없는 로그 파일 오류 메시지로 인해 ESET PROTECT 서버 서비스를 시작할 수 없는 경우 아래 표시된 단계를 사용하여 복구 작업을 수행합니다.

**!** 복구 작업을 시작하기 전에 [DB 서버 백업](#)을 수행하는 것이 좋습니다.

1. 시작 > 제어판 > 프로그램 및 기능으로 이동하여 **ESET PROTECT** 서버를 두 번 클릭합니다.
2. 복구를 선택하고 다음을 클릭합니다.
3. 기존 DB 연결 설정을 재사용하고 다음을 클릭합니다. 확인 메시지가 표시되면 예를 클릭합니다. 데이터베이스 연결 정보는 여기(%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini)에서 확인할 수 있습니다.
4. 이미 DB에 저장된 비밀번호 사용을 선택하고 다음을 클릭합니다.
5. 현재 기존 인증서 유지를 선택하고 다음을 클릭합니다.
6. 유효한 라이선스 키로 ESET PROTECT 서버를 활성화하거나, 나중에 활성화를 선택(추가 지침은 [라이선스](#)

[스 관리](#) 참조)하고 **다음**을 클릭합니다.

7. **복구**를 클릭합니다.

8. 다시 [웹 콘솔에 연결](#)하고 모든 것이 정상인지 확인합니다.

기타 문제 해결 시나리오:

## ESET PROTECT 서버가 실행되고 있지 않지만 DB 백업이 있음:

1. [DB 백업](#)을 복원합니다.
2. 새 컴퓨터가 이전 설치와 동일한 IP 주소 또는 호스트 이름을 사용하는지 확인하여 에이전트가 연결되도록 합니다.
3. ESET PROTECT 서버를 복구하고 복원한 데이터베이스를 사용합니다.

## ESET PROTECT 서버가 실행되고 있지 않지만 해당 서버에서 서버 인증서 및 인증 기관을 내보냈음:

1. 새 컴퓨터가 이전 설치와 동일한 IP 주소 또는 호스트 이름을 사용하는지 확인하여 에이전트가 연결되도록 합니다.
2. 백업 인증서를 사용하여 ESET PROTECT Server를 복구합니다(복구 시 **파일에서 인증서 로드**를 선택하고 지침을 따름).

## ESET PROTECT 서버가 실행되고 있지 않고 DB 백업 또는 ESET PROTECT 서버 인증서 및 인증 기관이 없음:

1. ESET PROTECT 서버를 복구합니다.
2. 다음 방법 중 하나를 사용하여 ESET Management 에이전트를 복구합니다.
  - 에이전트 설치 관리자 스크립트
  - 원격 배포(이 방법을 사용하려면 대상 컴퓨터에서 방화벽을 비활성화해야 함)
  - 수동 에이전트 구성 요소 설치 관리자

## MSI 로깅

Windows에서 ESET PROTECT 구성 요소(예: ESET Management 에이전트)를 제대로 설치할 수 없는 경우 유용합니다.

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```



# ESET PROTECT API

ESET PROTECT ServerApi(*ServerApi.dll*)는 애플리케이션 프로그래밍 인터페이스로, 사용자의 요구 및 사양을 충족하는 사용자 지정 소프트웨어 애플리케이션을 작성하기 위한 기능 및 도구 집합입니다. ServerApi를 사용하여 애플리케이션은 사용자 지정 인터페이스, 기능 및 일반적으로 ESET PROTECT 웹 콘솔을 통해 수행하는 작업(ESET PROTECT 관리, 보고서 생성 및 수신 등)을 제공할 수 있습니다.


C 언어에 대한 자세한 내용 및 예제와 사용 가능한 JSON 메시지 목록을 보려면 다음 온라인 도움말을 참조하십시오.

[ESET PROTECT 10 API](#)

## FAQ

**서버에 Java를 설치하는 이유는 무엇입니까? 이렇게 하면 보안 위험이 발생하지 않습니까? 모든 보안 회사 및 보안 프레임워크 대다수는 컴퓨터 특히, 서버에서 Java를 제거하도록 권장합니다.**

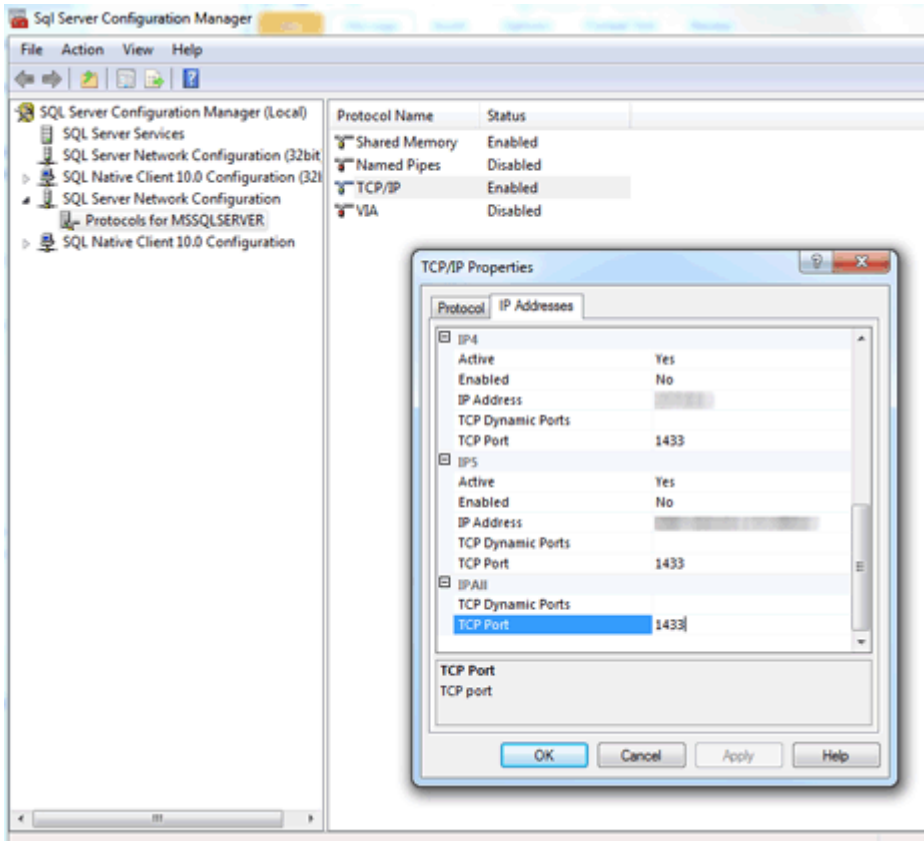
ESET PROTECT 웹 콘솔을 작동하려면 Java/OpenJDK가 필요합니다. Java는 웹 기반 콘솔에 대한 업계 표준입니다. 모든 주요 웹 콘솔은 작동을 위해 Java 및 웹 서버(Apache Tomcat)를 사용합니다. Java는 다중 플랫폼 웹 서버를 지원하는 데 필요합니다. 보안상의 이유로 전용 컴퓨터에 웹 서버를 설치할 수 있습니다.

 2019년 1월부터 비즈니스, 상업 또는 프로덕션 용도의 Oracle JAVA SE 8 공개 업데이트에는 상용 라이선스가 필요합니다. JAVA SE 구독을 구매하지 않은 경우 무료 대안으로 전환할 수 없습니다. [지원되는 버전의 JDK](#)를 참조하십시오.

## SQL Server가 사용 중인 포트를 확인하려면 어떻게 해야 하나요?

SQL Server에서 사용되는 포트는 여러 가지 방법으로 확인할 수 있습니다. SQL Server 구성 관리자를 통해 가장 정확한 결과를 얻을 수 있습니다. SQL Server 구성 관리자에서 이 정보를 찾는 위치의 예를 보려면 아래 그림을 참조하십시오.





Windows Server 2012에서 SQL Server Express(ESET PROTECT 패키지에 포함)를 설치했는데도 표준 SQL 포트에서 수신 대기 중인 것으로 나타나지 않습니다. 기본 포트인 1433 이외의 포트에서 수신 대기할 가능성이 높습니다.

## 큰 패킷 크기를 수용하도록 MySQL을 구성하려면 어떻게 합니까?

[Windows](#) 또는 [Linux](#)용 MySQL 설치 및 구성을 참조하십시오.

## SQL을 직접 설치하는 경우ESET PROTECT?

직접 만들 필요가 없습니다. 데이터베이스는 ESET PROTECT 설치 관리자가 아니라 *Server.msi* 설치 관리자에 의해 생성됩니다. ESET PROTECT 설치 관리자는 간편한 작업 진행을 위해 제공되며 SQL Server를 설치합니다. 그런 다음, *Server.msi* 설치 관리자를 통해 DB가 생성됩니다.


## 적절한 Microsoft SQL Server 연결 상세 정보와 자격 증명을 제공한다면 ESET PROTECT 설치 관리자를 통해 기존 Microsoft SQL Server 설치에서 새 DB를 생성할 수 있습니까? 설치 관리자가 다른 버전의 SQL Server(2014, 2019 등)를 지원한다면 편리할 것입니다.

DB는 *Server.msi*를 통해 생성됩니다. 통해 생성되므로 개별적으로 설치된 SQL Server 인스턴스에 ESET PROTECT DB를 만들 수 있습니다. 지원되는 Microsoft SQL Server 버전은 2014 이상입니다.

ESET PROTECT 10.0 [통합형 설치 관리자](#)는 기본적으로 Microsoft SQL Server Express 2019를 설치합니다.

0이전 Windows 버전(Server 2012 또는 SBS 2011)을 사용하는 경우 기본적으로 Microsoft SQL Server Express 2014가 설치됩니다.

0설치 관리자는 데이터베이스 인증을 위해 임의의 패스워드를 자동으로 생성합니다(%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini에 저장됨).

-  Microsoft SQL Server Express는 각 관계형 DB의 크기가 10GB로 제한되어 있습니다. Microsoft SQL Server Express를 사용하지 않는 것이 좋습니다.
- 엔터프라이즈 환경 또는 대규모 네트워크에서.
  - [ESET Inspect](#)과(와) 함께 ESET PROTECT을(를) 사용하려는 경우

---

## 기존 SQL Server에 설치하는 경우 SQL Server에서 기본적으로 기본 제공 Windows 인증 모드를 사용합니까?

그렇지 않습니다. Windows 인증 모드는 SQL Server에서 비활성화될 수 있으므로 로그인하는 유일한 방법은 SQL Server 인증을 사용하는 것입니다(사용자 이름 및 비밀번호 입력). ESET PROTECT 서버를 설치하는 동안에는 혼합 모드 인증(SQL Server 인증 및 Windows 인증)이 필요합니다. SQL Server를 수동으로 설치할 경우에는 루트 비밀번호(루트 사용자 이름은 보안 관리자를 의미하는 "sa"임)를 만든 후 나중에 사용할 수 있도록 안전한 장소에 보관하는 것이 좋습니다. ESET PROTECT 서버를 업그레이드할 때 루트 비밀번호가 필요할 수 있습니다. ESET PROTECT 서버를 설치한 후에는 [Windows 인증](#)을 설정할 수 있습니다.

---

## MySQL 대신 MariaDB를 사용할 수 있습니까?

아니요, MariaDB는 지원되지 않습니다. 지원되는 버전의 [MySQL Server 및 ODBC 커넥터](#)를 설치해야 합니다. [MySQL 설치 및 구성](#)을 참조하십시오.

---

## ESET PROTECT 설치 관리자에서 이 페이지

지(<http://www.microsoft.com/en-us/download/details.aspx?id=17851>)를 안내해서 Microsoft .NET Framework 4를 설치해야 했지만, 새로 설치한 Windows Server 2012 R2(SP1 포함)에서 작동하지 않았습니다.

Windows Server 2012 보안 정책으로 인해 Windows Server 2012에서는 이 설치 관리자를 사용할 수 없습니다. Microsoft .NET Framework는 역할 및 기능 추가 마법사를 통해 설치해야 합니다.

---


## SQL Server 설치가 실행되고 있는지를 확인하기가 매우 어렵습니다. 설치에 10분 넘게 걸릴 경우 어떤 문제가 있는지 어떻게 알 수 있습니까?

드문 경우지만 SQL Server 설치에 최대 1시간이 걸릴 수 있습니다. 설치 시간은 시스템 성능에 따라 좌우됩니다.

---

## 설치 중에 입력한 웹 콘솔의 관리자 비밀번호를 다시 설정하려면 어떻게 합니까?

서버 설치 관리자를 실행하고 복구를 선택하여 비밀번호를 다시 설정할 수 있습니다. DB 생성 중에 Windows 인증을 사용하지 않은 경우, ESET PROTECT DB에 접근하려면 비밀번호가 필요할 수 있습니다.

-  • 일부 복구 옵션의 경우 잠재적으로 저장된 데이터가 제거될 수 있으므로 주의를 기울여야 합니다.  
• 패스워드를 재설정하면 다음 항목이 비활성화됩니다. [2FA](#).

---

## ESET PROTECT에 추가할 컴퓨터 목록이 있는 파일을 가져올 경우 파일의 형식은 어떤 형식이어야 합니까?

형식은 다음 줄과 같습니다.

*All\Group1\GroupN\Computer1*

*All\Group1\GroupM\ComputerX*

All은 루트 그룹의 필수 이름입니다.

---

## Apache Tomcat대신 IIS를 사용할 수 있습니까? 다른 HTTP 서버는 어떻습니까?

IIS는 HTTP 서버입니다. 웹 콘솔을 실행하려면 Java 서블릿 컨테이너(예: Apache Tomcat)가 필요하며 HTTP 서버만으로는 충분하지 않습니다. IIS를 Java 서블릿 컨테이너로 변경하는 방법이 있지만 일반적으로는 지원되지 않습니다.

**i** ESET에서는 Apache HTTP 서버를 사용하지 않으며, 다른 제품인 Apache Tomcat을 사용합니다.

---

## ESET PROTECT에 명령줄 인터페이스가 있습니까?

예, ESET PROTECT [ServerApi](#)가 있습니다.

---

## 도메인 컨트롤러에 ESET PROTECT을(를) 설치할 수 있습니까?

[도메인 컨트롤러에 SQL Server를 설치하지 마십시오](#)(예: Windows SBS/Essentials). ESET PROTECT 제품을 다른 서버에 설치하거나 설치 중에 SQL Server Express 구성 요소를 선택하지 않는 것이 좋습니다(이 경우 기존 SQL 또는 MySQL Server를 사용하여 ESET PROTECT DB를 실행해야 함).

---

## 시스템에 SQL이 이미 설치되어 있는 경우 ESET PROTECT 서버 설치에서 검색됩니까? 검색될 경우에는 어떻게 됩니까? MySQL의 경우는 어떻습니까?

ESET PROTECT는 사용자가 설치 마법사를 사용하고 SQL Express가 설치되도록 선택한 경우 시스템에서 실행되는 SQL을 확인합니다. 시스템에서 이미 실행되는 SQL이 있는 경우 마법사는 기존 SQL을 제거하고 설치를 다시 실행하거나 SQL Express를 제외하고 ESET PROTECT를 설치하라는 알림을 표시합니다. ESET PROTECT에 대한 [DB 요구 사항](#)을 참조하십시오.

## 릴리스 버전별로 매핑된 ESET PROTECT 구성 요소는 어디서 찾을 수 있습니까?

ESET의 [지식 베이스 문서](#)를 참조하십시오.

---

## ESET PROTECT에서 최신 버전으로 업그레이드를 수행하려면 어떻게 해야 합니까?

[업그레이드 절차](#)를 참조하십시오.

---

## 인터넷 연결 없이 시스템을 업데이트하려면 어떻게 합니까?

ESET 업데이트 서버에 연결할 수 있는 컴퓨터(업데이트 파일이 캐시됨)에 설치된 [ESET BridgeHTTP 프록시](#)를 사용하고 로컬 네트워크의 해당 HTTP 프록시로 끝점을 가리킵니다. 서버가 인터넷에 연결되어 있지 않으면 한 대의 컴퓨터에서 끝점 제품의 미러 기능을 활성화하고, USB 드라이브를 사용하여 이 컴퓨터에 업데이트 파일을 제공하고, 다른 모든 오프라인 컴퓨터가 이 컴퓨터를 업데이트 서버로 사용하도록 구성할 수 있습니다.

오프라인 설치를 수행하는 방법에 대한 자세한 내용을 보려면 [이 지침을 따르십시오](#).

---

## 초기 ESET PROTECT 설치 시 SQL Server가 자동으로 설정된 경우 ESET PROTECT 서버를 다시 설치하고 기존 SQL Server에 연결하려면 어떻게 해야 합니까?

원래 ESET PROTECT 서버를 설치한 것과 동일한 사용자 계정(예: 도메인 관리자 계정)을 사용하여 ESET PROTECT 서버의 새 인스턴스를 설치하는 경우 **Windows 인증을 통해 MS SQL Server**를 사용할 수 있습니다.

---

## Linux의 Active Directory 동기화 문제를 해결하려면 어떻게 합니까?

도메인 이름을 모두 대문자로 입력했는지 확인합니다(administrator@TEST.LOCAL 대신 administrator@test.local).

---

## 저장소 대신 자체 네트워크 리소스(예: SMB 공유)를 사용하는 방법이 있습니까?

패키지가 있는 직접 URL을 제공하도록 선택할 수 있습니다. 파일 공유를 사용하는 경우 다음과 같이 file://를 입력하고 뒤에 파일의 전체 네트워크 경로를 입력하십시오.

`file://\\\eraserver\\install\\ees_nt64_ENU.msi`

---

## 비밀번호를 다시 설정하거나 변경하려면 어떻게 합니까?

관리자 계정은 개별 관리자의 계정을 만드는 데만 사용해야 합니다. [관리자 계정](#)이 생성되면 관리자 비밀번호를 저장해야 하고 해당 관리자 계정은 사용하지 말아야 합니다. 이렇게 하면 관리자 계정을 비밀번호 다시 설정/계정 상세 정보에만 사용할 수 있습니다.

기본 제공 ESET PROTECT 관리자 계정의 비밀번호를 다시 설정하는 방법:

1. **프로그램 및 기능**을 열고(appwiz.cpl 실행) ESET PROTECT 서버를 찾은 다음 오른쪽 마우스 버튼을 클릭합니다.
2. 오른쪽 마우스 버튼 메뉴에서 **변경**을 선택합니다.
3. **복구**를 선택합니다.
4. DB 연결 상세 정보를 지정합니다.
5. **기존 DB를 사용하고 업그레이드 적용**을 선택합니다.
6. 이미 DB에 저장된 비밀번호 사용을 선택 취소하고 새 비밀번호를 입력합니다.
7. 새 비밀번호를 사용하여 ESET PROTECT 웹 콘솔에 로그인합니다.

**i** 원하는 계정 권한에 따라 특정 접근 권한을 갖는 추가 계정을 만드는 것이 좋습니다.

---

## ESET PROTECT 서버 및 ESET PROTECT 웹 콘솔 포트를 변경하려면 어떻게 합니까?

새 포트에 대한 웹 서버 연결을 허용하려면 웹 서버 구성에서 포트를 변경해야 합니다. 이렇게 하려면 아래

단계를 따릅니다.

1. 웹 서버 종료
2. 웹 서버 구성에서 포트 수정
  - a) `webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties` 파일 열기
  - b) 새 포트 번호 설정(예: `server_port=44591`)
3. 웹 서버 다시 시작

---

## 통합형 설치 관리자를 통해 ERA 5.x/6.x 또는 ESMC 7.x에서 ESET PROTECT 10.0(으)로 직접 업그레이드할 수 있습니까?

ERA 5.x/6.x 또는 ESMC 7.0/7.1이 있는 경우:

- ESET PROTECT 10.0(으)로 직접 업그레이드하는 것은 지원되지 않습니다.
- ESET PROTECT 10.0을(를) 새로 설치합니다.

ESMC 7.2에서 ESET PROTECT 10.0(으)로 직접 업그레이드할 수 있습니다.

---

## 오류 메시지를 수신하거나 ESET PROTECT에서 문제가 발생하는 경우 어떻게 해야 합니까?

[문제 해결 FAQ](#)를 참조하십시오.

## 최종 사용자 사용권 계약

2021년 10월 19일부로 효력이 발생합니다.

**중요:** 제품 응용 프로그램을 다운로드, 설치, 복사 또는 사용하기 전에 다음 약관을 읽어 보시기 바랍니다. 소프트웨어를 다운로드, 설치, 복사하거나 사용할 경우 다음 약관에 동의하며 다음을 인정하는 것으로 간주됩니다. [개인 정보 보호 정책](#).

최종 사용자 사용권 계약

Einsteinova 24, 85101 Bratislava, Slovak Republic에 소재하고 브라티슬라바 지방 법원 상업 등기소 SRO국(입력 번호 3586/B, 사업자 등록 번호: 31333532)에 등록된 ESET, spol. s r. o.사("ESET" 또는 "공급업체")와 자연인 또는 법인("귀하" 또는 "최종 사용자") 간에 작성된 본 최종 사용자 사용권 계약("계약")의 약관에 따라 사용자는 본 계약 1조에 정의된 소프트웨어를 사용할 수 있는 권한을 보유합니다. 아래 설명되어 있는 약관



을 전제로 본 계약 1조에 정의된 소프트웨어를 데이터 저장 미디어에 저장하거나, 이메일을 통해 전송하거나, 인터넷 또는 공급업체의 서버에서 다운로드하거나, 다른 공급원으로부터 얻을 수 있습니다.

본 계약은 구매 계약이 아닌 최종 사용자의 권한에 대한 계약입니다. 공급업체는 여전히 소프트웨어 복사본 및 구매 패키지에 포함된 물리적 미디어 및 본 계약에 따라 최종 사용자가 권한을 가진 기타 모든 복사본에 대한 소유권을 가지고 있습니다.

소프트웨어를 설치, 다운로드, 복사 또는 사용하는 중에 "동의함" 또는 "동의함..."을 클릭하면 본 계약의 사용 약관에 동의하고 개인 정보 보호 정책을 인정하는 것입니다. 본 계약의 모든 사용 약관 및/또는 개인 정보 보호 정책에 동의하지 않는 경우 즉시 취소 옵션을 클릭하거나, 설치 또는 다운로드를 취소하거나, 소프트웨어와 설치 미디어, 기본 설명서 및 구매 영수증을 폐기하거나 소프트웨어를 구매한 판매점에 반납하시기 바랍니다.

소프트웨어를 사용할 경우 본 계약서를 읽고 본 계약서 약관을 이해하며 준수할 것을 동의하는 것으로 인정됩니다.

**1. 소프트웨어.** 본 계약서에 명시된 "소프트웨어"는 (i) 본 계약서에 따른 컴퓨터 프로그램 및 해당 구성 요소를 모두 포함하거나, (ii) 디스크, CD-ROM, DVD, 이메일 및 모든 첨부 파일 또는 본 계약서가 제공된 기타 미디어의 모든 내용(이메일이나 인터넷에서의 다운로드를 통해 데이터 저장 미디어에서 제공되는 소프트웨어의 개체 코드 형태 포함), (iii) 소프트웨어와 관련된 모든 설명 자료나 기타 가능한 모든 설명서, 상기 소프트웨어에 대한 모든 설명, 해당 사양, 소프트웨어 특성이나 작동 설명, 소프트웨어가 사용되는 작동 환경 설명, 소프트웨어의 사용 또는 설치 지침, 소프트웨어의 사용 방법에 대한 모든 설명("설명서"), (iv) 본 계약서 3조에 따라 공급업체가 사용자에게 라이선스를 제공한 경우 소프트웨어와 관련하여 해당 소프트웨어의 복사본, 소프트웨어에서 발생 가능한 오류 해결을 위한 패치, 소프트웨어에 대한 추가 사항, 소프트웨어 확장 프로그램, 수정된 소프트웨어 버전, 소프트웨어 구성 요소 업데이트를 의미합니다. 소프트웨어는 실행 개체 코드 형태로만 제공됩니다.

**2. 설치, 컴퓨터 및 라이선스 키.** 데이터 저장 미디어를 통해 제공되거나, 이메일을 통해 전송되거나, 인터넷 또는 공급업체의 서버에서 다운로드하거나, 다른 공급원으로부터 얻은 소프트웨어는 설치해야 합니다. 소프트웨어는 설명서에 명시된 최소한의 요구 사항에 따라 올바르게 구성된 컴퓨터에 설치해야 합니다. 설치 방법은 설명서에 나와 있습니다. 소프트웨어에 악영향을 줄 수 있는 컴퓨터 프로그램이나 하드웨어는 소프트웨어를 설치한 컴퓨터에 설치할 수 없습니다. 컴퓨터는 개인용 컴퓨터, 랩톱, 워크스테이션, 팜톱 컴퓨터, 스마트폰, 핸드헬드 전자 장치 또는 소프트웨어가 해당 용도로 디자인되고 설치 및/또는 사용되는 기타 전자 장치를 포함하나 이에 국한되지 않는 하드웨어를 의미합니다. 라이선스 키는 소프트웨어의 합법적인 사용과 본 계약에 따라 라이선스 조항의 특정 버전 또는 확장을 허용하기 위해 최종 사용자에게 제공되는 기호, 문자, 숫자 또는 특수 기호의 고유한 시퀀스를 의미합니다.

**3. 라이선스.** 본 계약서의 약관에 동의한 조건에 따라 사용자가 여기에 약정된 모든 약관을 준수하는 경우 공급업체는 다음과 같은 권한("라이선스")을 사용자에게 부여합니다.

**a) 설치 및 사용.** 컴퓨터의 하드 디스크나 데이터를 영구 저장하기 위한 기타 미디어에 소프트웨어를 설치하거나, 컴퓨터 시스템의 메모리에 소프트웨어를 설치 및 저장하거나, 컴퓨터 시스템에 소프트웨어를 구현, 저장 및 표시할 수 있는 비독점적이고 양도 불가능한 권한을 사용자에게 제공합니다.

**b) 라이선스 수 관련 조항.** 소프트웨어 사용 권한은 최종 사용자의 수에 따라 제한됩니다. 1명의 최종 사용자 수는 (i) 1대의 컴퓨터 시스템에 소프트웨어 설치를 의미하거나, (ii) 라이선스 범위가 사서함 수로 제한된 경우 1명의 사용자는 메일 사용자 에이전트("MUA")를 통해 이메일을 수신하는 1명의 컴퓨터 사용자를 의미합니다. MUA가 이메일을 수신하여 여러 사용자에게 자동으로 배포할 경우 이메일이 배포되는 실제 사용자 수에 따라 해당 최종 사용자 수가 결정됩니다. 메일 서버가 메일 게이트 기능을 수행할 경우, 최종 사용자 수는 해당 게이트가 서비스를 제공하는 메일 서버 사용자 수와 같습니다. 개수에 상관없이 이메일 주소가 예를

들어 별칭을 통해 한 명의 사용자에게 연결되고 한 명의 사용자가 이 주소를 수락하며, 클라이언트에서 더 많은 사용자에게 메시지를 자동으로 배포하지 않을 경우, 1대의 컴퓨터에 대한 라이선스만 필요합니다. 둘 이상의 컴퓨터에서 동일한 라이선스를 동시에 사용할 수는 없습니다. 최종 사용자는 공급업체가 부여한 라이선스의 수로 인해 발생하는 제한에 따라 최종 사용자가 소프트웨어를 사용할 수 있는 권한 범위까지만 소프트웨어에 라이선스 키를 입력할 수 있습니다. 본 계약 또는 공급업체가 허가하지 않는 한, 라이선스 키를 제3자와 공유할 수 없으며 제3자가 라이선스 키를 사용하도록 허용할 수 없습니다. 라이선스 키가 손상되면 공급업체에 즉시 알려주세요.

c) **Home/Business Edition.** Home Edition 버전의 소프트웨어는 가정/가족 전용으로 비공개 및/또는 비상업적 환경에서만 사용해야 합니다. 상업적 환경과 메일 서버, 메일 릴레이, 메일 게이트웨이 또는 인터넷 게이트웨이에서 사용하려면 Business Edition 버전의 소프트웨어를 구입해야 합니다.

d) **라이선스 기간.** 소프트웨어 사용 권한에 대한 기간은 제한됩니다.

e) **OEM 소프트웨어.** "OEM"으로 분류된 소프트웨어는 귀하가 구입한 컴퓨터에서만 사용할 수 있습니다. 다른 컴퓨터에 양도할 수 없습니다.

f) **증정용("NFR") 및 평가판 소프트웨어.** 증정용("NFR") 또는 평가판으로 분류된 소프트웨어는 판매될 수 없으며, 소프트웨어 기능을 검증 및 테스트하는 데만 사용할 수 있습니다.

g) **라이선스 종료.** 라이선스 기간이 만료되면 라이선스가 자동으로 해제됩니다. 또한 사용자가 본 계약서의 조항을 위배한 경우 공급업체는 이러한 만일의 사태에 공급업체에 제공되는 자격이나 법적제재를 침해하지 않고 계약을 철회할 수 있습니다. 라이선스 취소 시 소프트웨어와 모든 백업 복사본을 사용자 자비로 즉시 삭제 또는 폐기하거나, 소프트웨어를 구입한 매장이거나 ESET으로 반납해야 합니다. 라이선스가 종료되면 공급업체는 소프트웨어 기능 사용(공급업체 서버나 타사 서버에 연결되어야 함)과 관련하여 최종 사용자의 자격을 취소할 수 있는 권한도 지닙니다.

4. **데이터 수집의 기능 및 인터넷 연결 요구 사항.** 소프트웨어를 제대로 작동하려면 인터넷에 연결되어 있어야 하며, 개인 정보 보호 정책에 따라 정기적으로 공급업체 서버 또는 제3자 서버와 해당 데이터 수집에 연결되어야 합니다. 소프트웨어 기능을 사용하고 소프트웨어를 업데이트 및 업그레이드하려면 인터넷과 해당 데이터 수집 기능에 연결되어 있어야 합니다. 공급업체가 소프트웨어 업데이트 또는 업그레이드("업데이트")를 발표할 수는 있지만, 업데이트를 제공할 의무는 없습니다. 이 기능은 소프트웨어의 표준 설정에 따라 활성화되므로, 최종 사용자가 업데이트 자동 설치를 비활성화하지 않는 한 업데이트가 자동으로 설치됩니다. 업데이트를 제공하려면 개인 정보 보호 정책에 따라 소프트웨어가 설치되는 컴퓨터 및/또는 플랫폼에 대한 정보 등 라이선스 정품 확인이 필요합니다.

업데이트 조항에는 [https://go.eset.com/eol\\_business](https://go.eset.com/eol_business)에서 확인 가능한 만료 정책("EOL 정책")이 적용될 수 있습니다. 소프트웨어 또는 해당 기능이 EOL 정책에 정의된 만료 날짜에 도달한 후에는 업데이트가 제공되지 않습니다.

본 계약의 목적에 따라, 공급업체가 개인 정보 보호 정책에 따라 사용자를 식별할 수 있도록 하는 데이터를 수집, 처리 및 저장해야 합니다. 사용자는 공급업체가 자체적인 방식을 통해 사용자가 본 계약의 조항에 따라 소프트웨어를 사용하는지 확인하는 데 동의해야 합니다. 사용자는 본 계약의 목적에 따라, 소프트웨어와 공급업체 컴퓨터 시스템 또는 공급업체 유통 및 지원 네트워크에 속하는 비즈니스 파트너의 컴퓨터 시스템 간 통신 중에 소프트웨어의 기능 및 소프트웨어를 사용하고, 공급업체의 권리를 보호하기 위한 승인을 보장하기 위해 사용자의 데이터가 전송되어야 한다는 데 동의해야 합니다.

본 계약의 체결에 따라, 공급업체 또는 공급업체의 유통 및 지원 네트워크에 속하는 비즈니스 파트너는 대금 청구 목적, 본 계약의 이행 및 컴퓨터에서 알림 전송을 위해 사용자를 식별하는 필수 데이터를 전송, 처리 및 저장할 자격을 갖습니다.

개인 정보, 개인 데이터 보호 및 데이터 주체로서의 사용자 권한에 대한 자세한 내용은 공급업체의 웹 사이트에서 확인할 수 있으며, 설치 프로세스를 통해 직접 접근할 수 있습니다. 또한 소프트웨어의 도움말 섹션에서 방문할 수도 있습니다.

**5. 최종 사용자의 권리 실행.** 최종 사용자의 권리는 직접 또는 직원을 통해 실행해야 합니다. 사용자는 라이선스를 얻은 컴퓨터 시스템을 보호하고 사용자의 활동을 보장하는 목적으로만 소프트웨어를 사용할 수 있습니다.

**6. 권한 제한.** 소프트웨어의 일부를 복사, 배포 또는 분리하거나 소프트웨어의 파생된 버전을 만들 수 없습니다. 다음은 예외입니다.

a) 아카이브 백업 복사본을 다른 컴퓨터에 설치하거나 사용하지 않을 경우 데이터를 백업 복사본으로 영구 저장하기 위해 미디어에 소프트웨어 복사본을 하나 직접 만들 수 있습니다. 이 외에 다른 소프트웨어 복사본을 만들 경우 본 계약서를 위반하는 것이 됩니다.

b) 소프트웨어 또는 소프트웨어 복사본을 사용할 수 있는 권리를 본 계약서에서 기술한 방식 외에 다른 방식으로 사용, 수정, 해석, 복제 또는 양도할 수 없습니다.

c) 소프트웨어를 다른 개인에게 판매, 재배포 또는 임대하거나, 다른 개인으로부터 소프트웨어를 임차 또는 대여할 수 없으며, 상업적 서비스 제공을 위해 사용할 수 없습니다.

d) 소프트웨어를 역엔지니어링, 역컴파일 또는 디어셈블하거나 소프트웨어의 소스 코드를 검색할 수 없습니다. 그러나 이러한 제한이 명시적으로 법에 의해 금지된 경우는 제외합니다.

e) 저작권법이나 다른 지적 재산권으로 인한 해당 제한 사항에 따르되 제한 없이 이를 포함하여, 소프트웨어 사용에 관한 모든 해당 법률 규정에 따른 방식으로만 소프트웨어를 사용할 것을 동의합니다.

f) 이러한 서비스에 접근하는 다른 최종 사용자의 기회를 제한하지 않는 방식으로만 소프트웨어 및 해당 기능을 사용할 것을 동의합니다. 공급업체는 최대한 많은 최종 사용자가 서비스를 사용할 수 있도록, 개별 사용자에게 제공되는 서비스 범위를 제한할 권리를 보유합니다. 서비스 범위를 제한하는 것은 소프트웨어 기능 사용 기회 종료 및 소프트웨어의 특정 기능과 관련한 제3자의 서버나 공급업체 서버에 대한 데이터 및 정보 삭제를 의미하기도 합니다.

g) 사용자는 본 계약의 조항에 반하여 라이선스 키를 사용하거나, 복제 또는 생성된 라이선스 키의 무단 복제나 배포뿐만 아니라 임의의 형태로 사용했거나 사용하지 않은 라이선스 키의 전송과 같이 소프트웨어 사용자 자격이 없는 사람에게 라이선스 키를 제공하거나, 공급업체 이외의 출처에서 얻은 라이선스 키를 사용하여 소프트웨어를 사용하는 모든 활동을 이행하지 않는다는 데 동의합니다.

**7. 저작권.** 소프트웨어의 법적 권리와 지적 재산권을 포함하되 제한 없이 소프트웨어와 소프트웨어의 모든 권한은 ESET 및/또는 해당 라이선스 공급업체의 자산입니다. 이들은 소프트웨어를 사용하고 있는 국가의 다른 모든 해당 법률과 국제 협약의 규정에 의해 보호를 받습니다. 소프트웨어의 구조, 구성 및 코드는 ESET 및/또는 해당 라이선스 공급업체의 업무상 비밀이며 기밀 정보입니다. 소프트웨어를 복사할 수 없지만 6(a)조에 지정된 경우는 예외입니다. 이에 따라 작성한 복사본에는 소프트웨어에 지정된 것과 동일한 저작권 및 법적 권한에 대한 고지 사항이 포함되어야 합니다. 본 계약서의 위반과 관련한 공급업체 권한에도 불구하고 본 계약서의 조항을 위반하여 소프트웨어의 소스 코드를 역엔지니어링, 역컴파일, 디어셈블하거나 소스 코드를 검색한 경우 이로 인해 획득한 모든 정보는 그 시점부터 모두 공급업체에게 자동으로 그리고 취소 불가능하게 양도되거나 공급업체가 소유한 것으로 간주됩니다.

**8. 권리 유보.** 본 계약서에서 소프트웨어의 최종 사용자에게 명시적으로 부여한 권리를 제외한 소프트웨어의 모든 권리는 공급업체가 단독으로 유보하고 있습니다.

**9. 복수의 언어 버전, 이중 미디어 소프트웨어, 복수의 복사본.** 소프트웨어에서 복수의 플랫폼이나 언어를 지원하거나 복수의 소프트웨어 복사본을 얻은 경우, 라이선스를 획득한 컴퓨터 시스템 수 및 버전에 해당하는 소프트웨어만 사용할 수 있습니다. 사용자가 이용하지 않은 소프트웨어의 버전이나 복사본은 판매, 대여, 임대, 임차, 재허여하거나 양도할 수 없습니다.

**10. 계약의 시작 및 종료.** 본 계약서는 본 계약서에 동의한 날부터 유효합니다. 소프트웨어, 모든 백업 복사본 및 공급업체나 공급업체의 비즈니스 파트너로부터 획득한 모든 관련 자료를 사용자가 비용을 부담하여 영구적으로 삭제, 폐기 또는 반납할 경우 본 계약을 종료할 수 있습니다. 소프트웨어와 해당 기능의 사용 권한에는 EOL 정책이 적용될 수 있습니다. 소프트웨어 또는 해당 기능이 EOL 정책에 정의된 만료 날짜에 도달하면 소프트웨어 사용 권한이 종료됩니다. 본 계약의 종료 방법과 상관없이 7, 8, 11, 13, 19 및 21조의 조항은 시간 제한 없이 계속 유효합니다.

**11. 최종 사용자 선언.** 최종 사용자로서 소프트웨어는 어떤 유형의 명시적 또는 암시적 보증 없이 해당 법률에서 허용하는 최대 한도까지 "있는 그대로" 제공되며, 공급업체, 라이선스 공급업체 또는 자회사가 특히 판매 보증이나 특수 목적에의 적합성 또는 소프트웨어가 제3자의 특허권, 저작권, 상표권 또는 기타 권리를 위반하지 않는다는 보증을 포함한 어떤 명시적이거나 묵시적인 보증이나 표명을 제공하지 않음을 인정합니다. 소프트웨어에 포함된 기능이 사용자 요구 사항을 충족하거나 소프트웨어 작동이 원활하고 오류 없음을 보장하는 공급업체나 다른 당사자의 보증은 제공되지 않습니다. 의도한 결과를 달성하기 위해 또는 소프트웨어 선택, 설치 및 사용에 따른 책임과 위험은 전적으로 사용자가 부담합니다.

**12. 추가 책임 없음.** 본 계약서에 명시적으로 열거된 책임을 제외한 다른 추가 책임이 공급업체 및 라이선스 공급업체에게 부과되지 않습니다.

**13. 책임 제한.** 준거법에 따라 허용되는 최대 범위까지 공급업체, 해당 공급업체 직원 또는 라이선스 공급업체는 모든 수익, 매출, 판매, 데이터 손실이나 대체품 또는 서비스 조달 비용, 재산상의 손해, 인적 상해, 비즈니스 중단, 비즈니스 정보 손실 혹은 계약, 고의적인 위법 행위, 태만 또는 설치, 제품의 사용/사용 불능으로 인해 제기되는 기타 책임론의 원인과 그 발생 여부에 상관없이 특수하거나 직간접적, 우발적, 경제적, 외과성, 범죄적, 특별 손해 또는 결과적 손해에 대해 공급업체나 해당 라이선스 공급업체 또는 자회사가 이러한 손해 가능성을 통보받은 경우에도 이에 대해 책임지지 않습니다. 특정 국가와 관할지에서 책임의 제외는 허용하지 않지만 책임의 제한은 허용할 수도 있기 때문에 공급업체, 공급업체 직원 또는 라이선스 공급업체, 자회사의 책임은 사용자가 라이선스를 위해 지불한 가격으로 제한됩니다.

**14.** 본 계약서에 포함된 어떠한 규정도 이에 어긋나는 경우 소비자의 입장을 인정한 당사자의 법적 권한을 침해하지 않습니다.

**15. 기술 지원.** ESET나 ESET에서 위탁한 제3자는 보증이나 선언 없이 단독 재량으로 기술 지원을 제공합니다. 소프트웨어 또는 해당 기능이 EOL 정책에 정의된 만료 날짜에 도달한 후에는 기술 지원이 제공되지 않습니다. 최종 사용자는 기술 지원을 제공받기 전에 기존의 모든 데이터, 소프트웨어 및 프로그램 기능을 백업해야 합니다. ESET나 ESET에서 위탁한 제3자는 기술 지원 제공으로 인한 데이터 손실, 재산상 손해, 소프트웨어나 하드웨어 손실 또는 수익 손실에 대해서는 어떤 법적 책임도 지지 않습니다. ESET나 ESET에서 위탁한 제3자는 기술 지원 범위를 벗어난 문제 해결과 관련하여 결정권을 가지고 있습니다. ESET는 단독 재량으로 기술 지원 제공을 거부, 연기 또는 종료할 권리를 보유합니다. 개인 정보 보호 정책을 준수하는 라이선스 정보, 정보 및 기타 데이터는 기술 지원을 제공하기 위해 필요할 수 있습니다.

**16. 라이선스 양도.** 공급업체의 동의를 받은 경우 컴퓨터 시스템 간 소프트웨어를 양도할 수 있습니다. 공급업체의 동의를 받은 경우 컴퓨터 시스템 간 소프트웨어를 양도할 수 있습니다. 공급업체의 동의를 받은 경우, 그리고 다음의 조건을 충족하는 경우에 한해 본 계약서의 모든 권한 및 라이선스를 다른 최종 사용자에게 영구적으로 양도할 수 있습니다. (i) 원래 최종 사용자가 소프트웨어 복사본을 가지고 있지 않아야 합니다. (ii) 권한은 원래 최종 사용자에게서 새로운 최종 사용자에게로 직접 양도되어야 합니다. (iii) 새로운 최종 사용자가 본 계약서의 원래 최종 사용자와 관련된 모든 권리와 책임을 맡기로 표명해야 합니다. (iv) 원래 최종

사용자가 17조에 지정된 대로 소프트웨어 정품을 확인할 수 있도록 설명서를 새로운 최종 사용자에게 제공해야 합니다.

**17. 소프트웨어 정품 확인.** 최종 사용자는 다음 방법 중 하나로 소프트웨어 사용 자격을 증명할 수 있습니다. (i) 공급업체에서 지정한 제3자나 공급업체에서 발행한 라이선스 인증서를 통해, (ii) 서면으로 작성된 라이선스 계약을 통해(이러한 계약이 체결된 경우), (iii) 라이선스 정보(사용자 이름 및 비밀번호)가 포함된 이메일을 공급업체로 전송하는 방법을 통해. 개인 정보 보호 정책에 따른 라이선스 정보 및 최종 사용자 식별 데이터는 소프트웨어 정품 확인에 필요할 수 있습니다.

**18. 미국 정부 및 공공 기관을 위한 라이선스.** 본 계약서에 설명된 라이선스 권한과 제한 사항이 적용된 소프트웨어가 미국 정부를 비롯한 공공 기관에 제공됩니다.

**19. 무역 관리 규정 준수.**

a) 귀하는 소프트웨어를 다른 사람에게 직간접적으로 수출, 재수출, 양도 또는 달리 제공하거나, 어떠한 방식으로든 소프트웨어를 사용하거나, ESET 또는 해당 지주 회사, 자회사 및 지주 회사의 자회사와 지주 회사가 관리하는 회사("계열사")가 다음을 포함하는 무역관리법에 의거하여 부정적인 결과를 초래하게 되거나 관련 법을 위반하게 될 수 있는 어떠한 행위에도 관여하지 않습니다.

i. 미국, 싱가포르, 영국, 유럽 연합이나 그 회원국 또는 본 계약에 따른 의무가 이행될 국가 또는 ESET이나 해당 계열사가 통합 또는 운영되는 국가의 정부, 주 또는 규제 기관에서 발표하거나 채택한 물품, 소프트웨어, 기술, 서비스의 수출, 재수출 또는 양도에 관한 라이선스 요구 사항을 규제, 제한하거나 부과하는 모든 법

ii. 경제, 금융, 무역 또는 기타 제재, 제한, 금수 조치, 수출입 제한, 자금이나 자산의 양도 혹은 서비스 수행 금지 또는 미국, 싱가포르, 영국, 유럽 연합이나 그 회원국 또는 본 계약에 따른 의무가 이행될 국가 또는 ESET이나 해당 계열사가 통합 또는 운영되는 국가의 정부, 주 또는 규제 기관에서 부과한 동등한 조치.

(법적 조치는 상기 i, ii항에 "무역관리법"으로 함께 언급되어 있음)

b) ESET은 다음과 같은 경우 본 약관에 따른 의무를 즉시 유예하거나 종료할 수 있는 권한을 보유합니다.

i. ESET이 합리적인 의견에 따라 사용자가 본 계약의 조항 19 a)조를 위반했거나 위반할 가능성이 있는 것으로 판단하는 경우

ii. 최종 사용자 및/또는 소프트웨어가 무역관리법의 적용을 받게 되어 결과적으로 ESET이 합당한 의견에 따라 본 계약의 의무를 계속 이행하면 ESET 또는 해당 계열사가 무역관리법에 의거하여 관련 법을 위반하게 되거나 부정적인 결과를 초래하게 될 수 있다고 판단하는 경우

c) 본 계약의 어떠한 조항도 해당 무역관리법과 상반되거나, 관련 법에 따라 처벌 또는 금지되는 방식으로 행동하거나 행동을 삼가도록(또는 행동하거나 행동을 삼가는 데 동의하도록) 유도 또는 요구하기 위한 것이 아니며, 이와 같이 해석되거나 이해되어서는 안 됩니다.

**20. 고지 사항.** 소프트웨어 및 설명서의 모든 고지 사항과 반납은 계약 22조에 따라 본 계약, 개인 정보 보호 정책, EOL 정책 및 설명서에 대한 변경 사항을 사용자에게 전달할 ESET의 권리를 침해하지 않고 ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic으로 전달되어야 합니다. ESET은 소프트웨어를 통해 사용자에게 이메일, 앱 내 알림을 보낼 수 있으며 당사 웹 사이트에 통신 사항을 게시할 수 있습니다. 사용자는 약관, 특별 약관 또는 개인 정보 보호 정책의 변경 사항과 취급, 고지 사항 또는 기타 법적 통신에 대한 계약상의 제언/수락이나 초대 등의 법적 통신을 온라인 형태로 ESET으로부터 수신하는 데 동의합니다. 준거법에 따라 다른 형태의 통신이 특별히 요구되지 않는 한, 이러한 전자 통신은 서면으로 수신된 것으로 간주됩니다.

**21. 준거법.** 본 계약서는 슬로바키아 법률에 따라 관리 및 해석됩니다. 최종 사용자와 공급업체는 준거법과 국제 물품 매매 계약에 관한 국제연합 협약 간의 상충되는 규정은 적용하지 않을 것을 동의합니다. 공급업체 또는 소프트웨어 사용과 관련된 손해 배상이나 분쟁에 대한 전속 사법권은 슬로바키아 브라티슬라바 지방 법원에 있으며, 관할권 행사는 브라티슬라바 지방 법원에 있음을 명시적으로 동의하는 바입니다.

**22. 일반 조항.** 본 계약서의 특정 규정이 유효하지 않거나 실행 불가능할 경우 계약의 나머지 규정의 유효성에 영향을 미치지 않습니다. 본 계약서에 규정된 약관에 따라 나머지 규정은 여전히 유효하고 실행 가능합니다. 본 계약서는 영어로 작성되었습니다. 편의상 또는 다른 목적상 본 계약서의 번역본을 준비하거나 본 계약서의 언어 버전 간에 불일치 항목이 있는 경우 영어 버전이 우선합니다.

ESET은 (i) 소프트웨어 또는 ESET의 비즈니스 수행 방법에 대한 변경 사항을 반영하거나, (ii) 법규 또는 보안상의 이유가 있거나, (iii) 남용 또는 피해를 방지하기 위해 관련 문서를 업데이트하여 언제든지 본 계약서와 해당 부속서, 부록, 개인 정보 보호 정책, EOL 정책 및 설명서 또는 그 일부를 개정할 수 있고 소프트웨어를 변경할 수 있는 권리를 보유합니다. 사용자에게는 이메일, 앱 내 알림 또는 기타 전자적 수단을 통해 본 계약서의 개정 사항이 통지됩니다. 본 계약서에 제시된 변경 사항에 동의하지 않을 경우 10조에 따라 변경 사항을 통지받은 후 30일 이내에 계약을 해지할 수 있습니다. 이 기한 내에 계약을 해지한 경우 외에는 제시된 변경 사항을 수락한 것으로 간주하며, 변경 사항을 통지받은 날짜를 기준으로 귀하에 대한 효력이 발생합니다.

사용자와 공급업체 간에 체결한 본 계약은 소프트웨어와 관련된 전체 계약을 나타내고, 소프트웨어 관련 정보에 대한 이전의 진술, 토론, 약정, 의사 전달 또는 공지를 완전히 대체합니다.

## 계약 부록

**공급업체에 정보 전송.** 추가 조항은 다음과 같이 공급업체에 정보 전송에 적용됩니다.

소프트웨어에는 설치 프로세스, 소프트웨어가 설치된 컴퓨터 및/또는 플랫폼에 대한 데이터, 소프트웨어의 작동 및 기능에 대한 정보와 관리되는 장치에 대한 정보(이하 "정보")를 수집한 후 공급업체에 전송하는 기능이 포함되어 있습니다. 해당 정보에는 관리되는 장치에 대한 데이터(무작위로 또는 우연히 획득한 개인 데이터 포함)가 포함될 수 있습니다. 소프트웨어의 이 기능을 활성화하는 경우, 개인 정보 보호 정책에 명시된 대로 관련 법률 규정에 따라 정보를 수집하고 공급업체에서 처리할 수 있습니다.

소프트웨어를 사용하려면 관리되는 컴퓨터에 구성 요소가 설치되어 있어야 관리되는 컴퓨터와 원격 관리 소프트웨어 간에 정보를 전송할 수 있습니다. 전송 대상 정보에는 관리되는 컴퓨터의 하드웨어 및 소프트웨어 정보와 원격 관리 소프트웨어의 관리 지침과 같은 관리 데이터가 포함됩니다. 관리되는 컴퓨터에서 전송되는 다른 데이터 콘텐츠는 관리되는 컴퓨터에 설치된 소프트웨어의 설정에 따라 결정됩니다. 관리 소프트웨어의 지침 콘텐츠는 원격 관리 소프트웨어의 설정에 따라 결정됩니다.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

## 개인 정보 보호 정책

Einsteinova 24, 851 01 Bratislava, Slovak Republic에 소재하고 브라티슬라바 지방 법원 상업 등기소, SRO국(입력 번호 3586/B, 데이터 통제자로서의 사업자 등록 번호: 31333532)에 등록된 ESET, spol. 사("ESET" 또는 "당사")는 고객들의 개인 데이터 및 개인 정보 처리 작업이 투명하게 이루어지기를 원합니다. 이러한 목표를 달성하기 위한 일환으로 ESET에서는 본 개인 정보 보호 정책을 게시하며, 이 정책은 고객("최종 사용자" 또는 "귀하")에게 다음과 같은 내용을 알리기 위한 목적으로만 사용됩니다.

- 개인 데이터 처리,
- 데이터 기밀성,



- 데이터 주체 권한

## 개인 데이터 처리

ESET에서 제공하는 서비스는 최종 사용자 사용권 계약("EULA")에 따라 제품 내에서 구현되지만 일부 서비스에는 특별한 주의가 필요할 수 있습니다. 당사의 서비스 제공과 관련된 데이터 수집에 대한 자세한 내용을 알려드리고자 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.

- ESET 보안 제품의 관리 시 사용자 ID/이름, 제품 이름, 라이선스 정보, 활성화/만료 정보, ESET 보안 제품이 설치된 관리되는 컴퓨터에 대한 하드웨어/소프트웨어 정보 등의 정보가 필요하며 로컬에 저장됩니다. 관리되는 ESET 보안 제품 및 장치의 활동에 관한 로그는 기능과 서비스를 원활하게 관리, 감독하기 위해 수집 및 사용될 수 있으며 ESET에 자동으로 전송되지 않습니다.
- 제품이 설치된 플랫폼 및 하드웨어 지문, 설치 ID, 크래시 덤프, 라이선스 ID, IP 주소, MAC 주소, 관리되는 장치도 포함될 수 있는 제품 구성 설정 등 제품의 작동과 기능에 대한 정보를 비롯한 설치 프로세스 관련 정보
- 라이선스 ID 및 개인 데이터(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. 보다 원활한 지원 서비스를 제공하기 위해 생성된 로그 파일 또는 덤프와 같은 기타 정보를 제공할 수도 있습니다.
- 서비스 사용에 관한 데이터는 세션이 끝날 때까지 완전히 익명으로 처리됩니다. 세션이 끝난 후 개인 식별 정보는 저장되지 않습니다.

## 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 권리가 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