

ESET PROTECT

Installations- Upgrade- und Migrationsanleitung

[Klicken Sie hier um die Hilfe-Version dieses Dokuments anzuzeigen](#)

Copyright ©2023 by ESET, spol. s r.o.

ESET PROTECT wurde entwickelt von ESET, spol. s r.o.

Weitere Informationen finden Sie unter <https://www.eset.com>.

Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnahmen, Scannen oder auf andere Art.

ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung Änderungen an allen hier beschriebenen Software-Anwendungen vorzunehmen.

Technischer Support: <https://support.eset.com>

REV. 19.03.2023

1 Über die Hilfe	1
2 Installation/Upgrade/Migration	2
2.1 Neue Funktionen in ESET PROTECT 9.1	2
2.2 Architektur	4
2.2 Server	5
2.2 Web-Konsole	5
2.2 HTTP-Proxy	6
2.2 Apache HTTP-Proxy	8
2.2 Agent	12
2.2 Rogue Detection Sensor	13
2.2 Mobile Device Connector	14
2.3 Unterschiede zwischen Apache HTTP Proxy, Mirror-Tool und Direktverbindung	15
2.3 Wann sollte ich den Apache HTTP Proxy verwenden	17
2.3 Wann sollte ich das Mirror-Tool verwenden	18
3 Systemanforderungen und Größenbemessung	18
3.1 Unterstützte Betriebssysteme	18
3.1 Windows	19
3.1 Linux	20
3.1 macOS	21
3.1 Mobilgerät	21
3.2 Unterstützte Umgebungen für die Desktopbereitstellung	24
3.3 Größenbemessung für Hardware und Infrastruktur	25
3.3 Bereitstellungsempfehlungen	26
3.3 Bereitstellung für 10.000 Clients	29
3.4 Datenbank	30
3.5 Unterstützte Versionen von Apache Tomcat und Java	32
3.6 Unterstützte Webbrowser, ESET-Sicherheitsprodukte und Sprachen	32
3.7 Netzwerk	35
3.7 Verwendete Ports	36
4 Installationsprozedur	40
4.1 All-in-One-Installation unter Windows	41
4.1 Installieren des ESET PROTECT Servers	42
4.1 Installation des ESET PROTECT Mobile Device Connector (Standalone)	54
4.2 Installation in Microsoft Azure	61
4.3 Komponenteninstallation unter Windows	61
4.3 Serverinstallation - Windows	63
4.3 Microsoft SQL Server - Anforderungen	70
4.3 MySQL Server - Installation und Konfiguration	71
4.3 Speziell eingerichtetes Datenbankkonto	73
4.3 Installation des Agenten - Windows	73
4.3 Servergestützte Installation des Agenten	76
4.3 Offline-Installation des Agenten	77
4.3 ESET Remote Deployment Tool	77
4.3 Installation der Web-Konsole - Windows	78
4.3 Web-Konsole mit dem All-in-One-Installationsprogramm installieren	78
4.3 Web-Konsole manuell installieren	83
4.3 Installation des HTTP-Proxy	84
4.3 RD Sensor-Installation - Windows	85
4.3 Mirror-Tool - Windows	86
4.3 Mobile Device Connector-Installation - Windows	93

4.3 Mobile Device Connector-Voraussetzungen	95
4.3 Mobile Device Connector-Aktivierung	97
4.3 MDM iOS-Lizenzierungsfunktion	97
4.3 HTTPS-Zertifikatanforderungen	98
4.3 Apache HTTP Proxy - Installation und Cache	98
4.3 Konfiguration von Apache HTTP Proxy	99
4.3 Squid-Installation - Windows (HTTP Proxy Cache)	103
4.3 Offline-Repository - Windows	103
4.3 Failover-Cluster - Windows	106
4.4 Komponenteninstallation unter Linux	107
4.4 ESET PROTECT Schritt-für-Schritt-Installation unter Windows	108
4.4 MySQL - Installation und Konfiguration	109
4.4 ODBC - Installation und Konfiguration	111
4.4 Serverinstallation - Linux	113
4.4 Servervoraussetzungen - Linux	117
4.4 Agenten-Installation - Linux	119
4.4 Installation der Web-Konsole - Linux	124
4.4 Rogue Detection Sensor-Installation - Linux	126
4.4 Mobile Device Connector-Installation - Linux	127
4.4 Voraussetzungen für den Mobile Device Connector - Linux	130
4.4 Apache HTTP Proxy-Installation - Linux	131
4.4 Squid HTTP Proxy-Installation auf Ubuntu Server	140
4.4 Mirror-Tool - Linux	141
4.5 Komponenteninstallation unter macOS	147
4.5 Agenten-Installation - macOS	147
4.6 ISO-Abbild	149
4.7 DNS-Diensteintrag	149
4.8 Offline-Installation von ESET PROTECT	150
5 Upgradeprozeduren	151
5.1 Task „ESET PROTECT Komponenten-Upgrade“	152
5.2 Verwenden Sie das ESET PROTECT 9.1 All-in-One-Installationsprogramm für Ihr Upgrade	156
5.3 Upgrade von ERA 6.5	159
5.4 Datenbankserver sichern/aktualisieren	159
5.4 Datenbankserver-Sicherung und Wiederherstellung	160
5.4 Datenbankserver-Upgrade	162
5.5 Upgrade einer ESMC/ESET PROTECT-Installation in einem Failover-Cluster unter Windows	162
5.6 Apache HTTP-Proxy aktualisieren	163
5.6 Apache HTTP-Proxy mit dem All-in-One-Installationsprogramm aktualisieren (Windows)	163
5.6 Apache HTTP Proxy manuell aktualisieren (Windows)	166
5.7 Apache Tomcat aktualisieren	168
5.7 Apache Tomcat mit dem All-in-One-Installationsprogramm aktualisieren (Windows)	168
5.7 Apache Tomcat manuell aktualisieren (Windows)	172
5.7 Apache Tomcat aktualisieren (Linux)	174
6 Prozeduren für Migration und erneute Installation	175
6.1 Migration von Server zu Server	176
6.1 Erstinstallation - gleiche IP-Adresse	176
6.1 Migrierte Datenbank - gleiche/andere IP-Adresse	178
6.2 migration der ESET PROTECT-Datenbank	179
6.2 Migrationsprozess für MS SQL Server	179
6.2 Migrationsprozess für MySQL Server	188
6.2 Verbindungsaufbau zwischen ESET PROTECT Server oder MD und einer Datenbank	190

6.3 Migration von MDM	192
6.4 Neue IP-Adresse oder neuer Hostname für ESET PROTECT Server nach der Migration	193
6.5 Migration von ERA 5.x	194
7 ESET PROTECT Server und Komponenten deinstallieren	194
7.1 ESET Management Agent deinstallieren	194
7.2 Windows - ESET PROTECT Server und Komponenten deinstallieren	196
7.3 Linux - ESET PROTECT-Komponenten aktualisieren, erneut installieren oder deinstallieren	197
7.4 macOS - ESET Management Agent und ESET Endpoint-Produkt deinstallieren	198
7.5 Alten ESMC/ESET PROTECT/MDM-Server nach der Migration auf einen anderen Server außer Betrieb nehmen	200
8 Fehlerbehebung	201
8.1 Upgrade von ESET PROTECT-Komponenten in Offlineumgebungen	202
8.2 Antworten auf gängige Probleme bei der Installation	202
8.3 Log-Dateien	207
8.4 Diagnose-Tool	209
8.5 Probleme nach Upgrade oder Migration von ESET PROTECT Server	211
8.6 MSI-Logging	212
9 ESET PROTECT API	212
10 Häufig gestellte Fragen (FAQ)	212
11 Endbenutzer-Lizenzvereinbarung	220
12 Datenschutzerklärung	227

Über die Hilfe

Diese Installationsanleitung wurde geschrieben, um Sie bei Installation und Upgrade von ESET PROTECT zu unterstützen und enthält Anweisungen für den Prozess.

Aus Konsistenzgründen und um Verwirrungen zu vermeiden, richtet sich die Terminologie in dieser gesamten Anleitung nach den ESET PROTECT-Parameternamen. Wir verwenden außerdem bestimmte Symbole, um besonders interessante oder wichtige Themen hervorzuheben.

 Hinweise können wichtige Informationen wie bestimmte Features oder einen Link zu einem verwandten Thema enthalten.

 Auf diese Weise gekennzeichnete Informationen sind wichtig und sollten nicht übersprungen werden. Normalerweise handelt es sich um nicht-kritische, jedoch wichtige Informationen.

 Kritische Informationen, die besondere Vorsicht erfordern. Warnungen haben den Zweck, Sie vor potenziell schädlichen Fehlern zu schützen. Der Text in Warnhinweisen weist auf besonders empfindliche Systemeinstellungen oder riskante Vorgänge hin und muss daher unbedingt gelesen und verstanden werden.

 Beispielszenario mit einem relevanten Anwendungsfall für das jeweilige Thema. Beispiele werden eingesetzt, um komplexere Themen zu erklären.

Konvention	Bedeutung
Fettdruck	Namen von Elementen der Benutzeroberfläche, z. B. Schaltflächen und Optionsfelder.
<i>Kursivdruck</i>	Platzhalter für Informationen, die Sie eingeben. Dateiname oder Pfad bedeutet z. B., dass Sie den tatsächlichen Pfad oder den Namen einer Datei angeben.
Courier New	Codebeispiele oder Befehle.
Hyperlink	Schnellzugriff auf verwandte Themen oder externe Webadressen. Hyperlinks sind in blau hervorgehoben und können unterstrichen sein.
<code>%ProgramFiles%</code>	Das Windows-Systemverzeichnis, in dem installierte Windows-Programme und andere Anwendungen gespeichert werden.

- Die [Onlinehilfe](#) ist die primäre Quelle für Hilfeinhalte. Bei funktionierender Internetverbindung wird automatisch die neueste Version der Onlinehilfe angezeigt. Die ESET PROTECT-Onlinehilfe enthält vier aktive Registerkarten im oberen Navigationsbereich: [Installation/Upgrade](#), [Administration](#), [VA-Bereitstellung](#) und [SMB-Anleitung](#).
- Die Themen in diesem Handbuch sind in Kapitel und Unterkapitel eingeteilt. Verwenden Sie das Suchfeld im oberen Bereich, um nach relevanten Informationen zu suchen.

 Nachdem Sie ein Benutzerhandbuch über die Navigationsleiste am oberen Seitenrand geöffnet haben, bezieht sich die Suche nur noch auf den Inhalt dieses Handbuchs. Wenn Sie z. B. das Administratorhandbuch geöffnet haben, werden keine Themen aus den Handbüchern für Installation/Upgrade und VA-Bereitstellung in den Suchergebnissen angezeigt.

- Die [ESET-Knowledgebase](#) enthält Antworten auf häufig gestellte Fragen sowie Lösungsvorschläge für zahlreiche Probleme. Die Knowledgebase wird regelmäßig von den ESET-Supportmitarbeitern aktualisiert und eignet sich daher hervorragend für die Lösung verschiedenster Probleme.

- Im [ESET-Forum](#) erhalten ESET-Benutzer schnell und einfach Hilfe und können anderen Benutzern helfen. Dort können Sie Themen zu beliebigen Fragen oder Problemen mit Ihren ESET-Produkten erstellen.

Installation/Upgrade/Migration

ESET PROTECT ist eine Anwendung, mit der Sie ESET-Produkte auf Arbeitsstationen, Servern und Mobilgeräten in einer Netzwerkumgebung von einem zentralen Standort aus verwalten können. Mit dem integrierten Taskverwaltungssystem von ESET PROTECT können Sie ESET-Sicherheitslösungen auf Remotecomputern installieren und schnell auf neue Probleme und Ereignisse reagieren.

ESET PROTECT selbst bietet keinen Schutz vor Schadcode. Der Schutz Ihrer Umgebung hängt von einer ESET-Sicherheitslösung auf den Arbeitsstationen, Servern und Mobilgeräten ab, beispielsweise ESET Endpoint Security oder ESET Server Security für Windows.

ESET PROTECT basiert auf zwei grundlegenden Konzepten:

- **Zentrale Verwaltung** – Das gesamte Netzwerk kann von einem zentralen Punkt aus konfiguriert, verwaltet und überwacht werden.
- **Skalierbarkeit** – Das System eignet sich gleichermaßen zur Bereitstellung in kleinen Netzwerken und in großen Unternehmensumgebungen. ESET PROTECT passt sich an das Wachstum Ihrer Infrastruktur an.

ESET PROTECT [unterstützt die neueste Generation von ESET-Sicherheitsprodukten](#) und ist mit der vorherigen Produktgeneration kompatibel.

Auf den ESET PROTECT-Hilfeseiten finden Sie eine vollständige Installations- und Upgradanleitung:

- [Architektur von ESET PROTECT](#)
- [Installationsprozedur](#)
- [Upgradeprozeduren](#)
- [Migrationsprozeduren](#)
- [Deinstallationsprozeduren](#)
- [Lizenzverwaltung](#)
- [Bereitstellungsprozesse](#) und [Agenten-Bereitstellung mithilfe von GPO und SCCM](#)
- [Erste Schritte nach der Installation von ESET PROTECT](#)
- [Administrationshandbuch](#)

Neue Funktionen in ESET PROTECT 9.1

Produktrundgang

Wir haben einen neuen Produktrundgang implementiert, um Ihnen den Einstieg in unsere Lösung zu erleichtern und das Onboarding zu beschleunigen. [Weitere Informationen](#)

Änderungen an Produktnamen

ESET Enterprise Inspector wurde in ESET Inspect und ESET Dynamic Threat Defense in ESET LiveGuard Advanced umbenannt. Weitere Informationen finden Sie in [diesem Artikel](#).

Verbesserte Neustarts

Mit der neuesten Version von ESET Endpoint Security für Windows (9.1) haben wir die Neustarts überarbeitet und neue Optionen eingeführt. Sie können Neustarts jetzt so einrichten, dass die Endbenutzer diese verschieben können. [Weitere Informationen](#)

Einfachere Bereitstellung

Wir haben den Erstellungsassistenten für Installationsprogramme überarbeitet und intuitiver gestaltet. Im Task „Software-Installation“ können Sie jetzt den speziellen Parameter „latest“ verwenden, um zu gewährleisten, dass das erstellte Installationsprogramm beim Start immer die neueste Produktversion installiert. [Weitere Informationen](#)

Systemeigene ARM-Unterstützung für macOS

Mit der neuesten Version von ESET Management Agent und ESET Endpoint Antivirus für macOS (v7) erhalten Sie systemeigene ARM-Unterstützung. [Weitere Informationen](#)

Unterstützung für 2FA-Apps von Drittanbietern

Wir haben Unterstützung für 2FA-Apps von Drittanbietern hinzugefügt, die das erforderliche TOTP-Protokoll unterstützen, darunter Google Authenticator, Microsoft Authenticator und Authy. [Weitere Informationen](#)

Erweiterte Filter

Wir haben ein neues Konzept für die Datenfilterung eingeführt, mit dem Sie wichtige Geräte zum Beispiel in größeren Umgebungen mühelos filtern können. Sie haben jederzeit einen statistischen Überblick darüber, wie viele Geräte mit bestimmten Attributen in Ihrem Netzwerk vorhanden sind, und wissen stets, wie viele Ergebnisse Sie erhalten, bevor Sie auf den Filter klicken. Sie können ab sofort die neuen Filteroptionen im Bereich „Computer“ ausprobieren. [Weitere Informationen](#)

Bessere Kommunikation bei automatischen Updates

Wir haben beim Status der Komponentenversion im Dashboard der Statusübersicht einen neuen blauen Bereich hinzugefügt, damit Sie Endpoints mit aktivierten automatischen Updates, die auf Updates warten, aber auch im Voraus manuell aktualisiert werden können, einfacher identifizieren können. [Weitere Informationen](#)

Liste veralteter Komponenten

ESET PROTECT erkennt jetzt veraltete Komponenten, zeigt eine Liste der veralteten Komponenten für den Konsolenadministrator an und enthält Anweisungen zum Upgrade dieser Komponenten. [Weitere Informationen](#)

Web-Kontrolle für MDM

Die Web-Kontrolle von Cloud MDM wird in die lokale Variante zurückportiert. Administratoren können den Zugriff der Mitarbeiter auf bestimmte Inhaltskategorien oder bestimmte Internetlinks einschränken.

Weitere Fehlerkorrekturen und verbesserte Benutzerfreundlichkeit

Weitere Details finden Sie im [Änderungslog](#).

Architektur

ESET PROTECT ist eine neue Generation von Remoteverwaltungssystem.

Installieren Sie die folgenden Komponenten (Windows- und Linux-Plattformen), um die [ESET-Sicherheitsprodukte](#) vollständig bereitzustellen:

- [ESET PROTECT Server](#)
- [ESET PROTECT-Web-Konsole](#)
- [ESET Management Agent](#)

Die folgenden zusätzlichen Komponenten sind optional. Wir empfehlen jedoch ihre Installation, um die Leistung der Anwendung in Ihrem Netzwerk zu optimieren:

- [Proxy](#)
- [RD Sensor](#)
- [Apache HTTP Proxy](#)
- [Mobile Device Connector](#)

ESET PROTECT-Komponenten verwenden Zertifikate, um mit dem ESET PROTECT Server zu kommunizieren. Weitere Informationen zu Zertifikaten in ESET PROTECT finden Sie in unserem [Knowledgebase-Artikel](#).

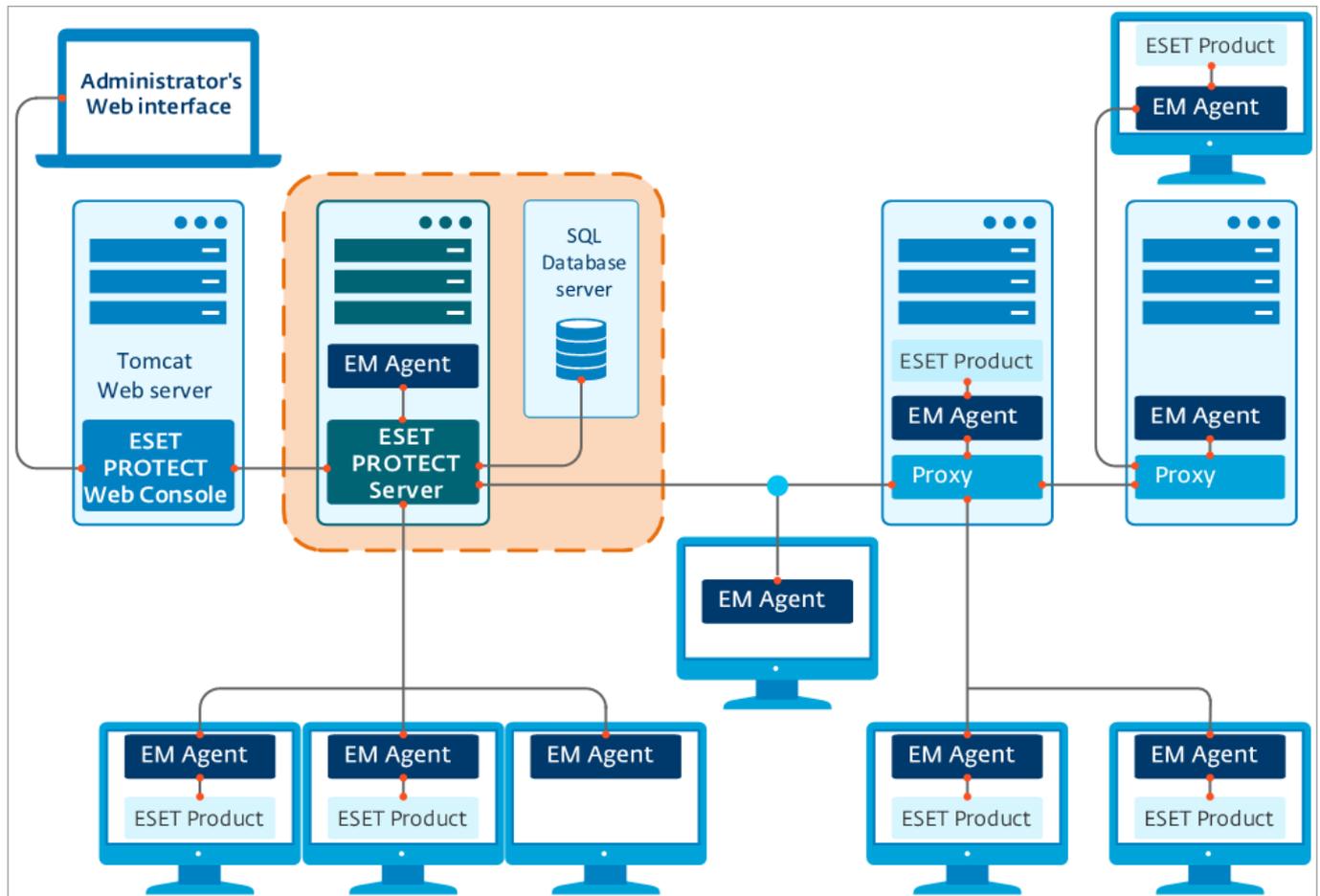
Übersicht über Infrastrukturelemente

Die folgende Tabelle enthält eine Übersicht über die Elemente der ESET PROTECT-Infrastruktur und deren wichtigste Funktionen:

Funktion	ESET PROTECT Server	ESET Management Agent	ESET-Sicherheitsprodukt	HTTP-Proxy	ESET-Server	Mobile Device Connector
Remoteverwaltung von ESET-Sicherheitsprodukten (Erstellung von Policies, Tasks, Berichten usw.)	✓	X	X	X	X	X
Kommunikation mit dem ESET PROTECT Server und Verwaltung des ESET-Sicherheitsprodukts auf dem Clientgerät	X	✓	X	X	X	✓
Bereitstellung von Updates, Lizenzüberprüfung	X	X	X	X	✓	X
Zwischenspeicherung und Weiterleitung von Updates (Erkennungsroutine, Installationsprogramme, Module)	X	X	✓	✓	X	X
Weiterleitung des Netzwerkverkehrs zwischen ESET Management Agent und ESET PROTECT Server	X	X	X	✓	X	X
Schutz des Clientgeräts	X	X	✓	X	X	X
Remoteverwaltung von Mobilgeräten	X	X	X	X	X	✓

Server

Der ESET PROTECT Server verarbeitet alle Daten von den Clients, die über den ESET Management Agenten oder den [HTTP Proxy](#) mit dem Server kommunizieren. Für die ordnungsgemäße Datenverarbeitung benötigt der Server eine stabile Verbindung zu dem Datenbankserver, auf dem sich die Netzwerkdaten befinden. Wir empfehlen, den Datenbankserver auf einem anderen Computer zu installieren, um eine höhere Leistung zu erreichen.

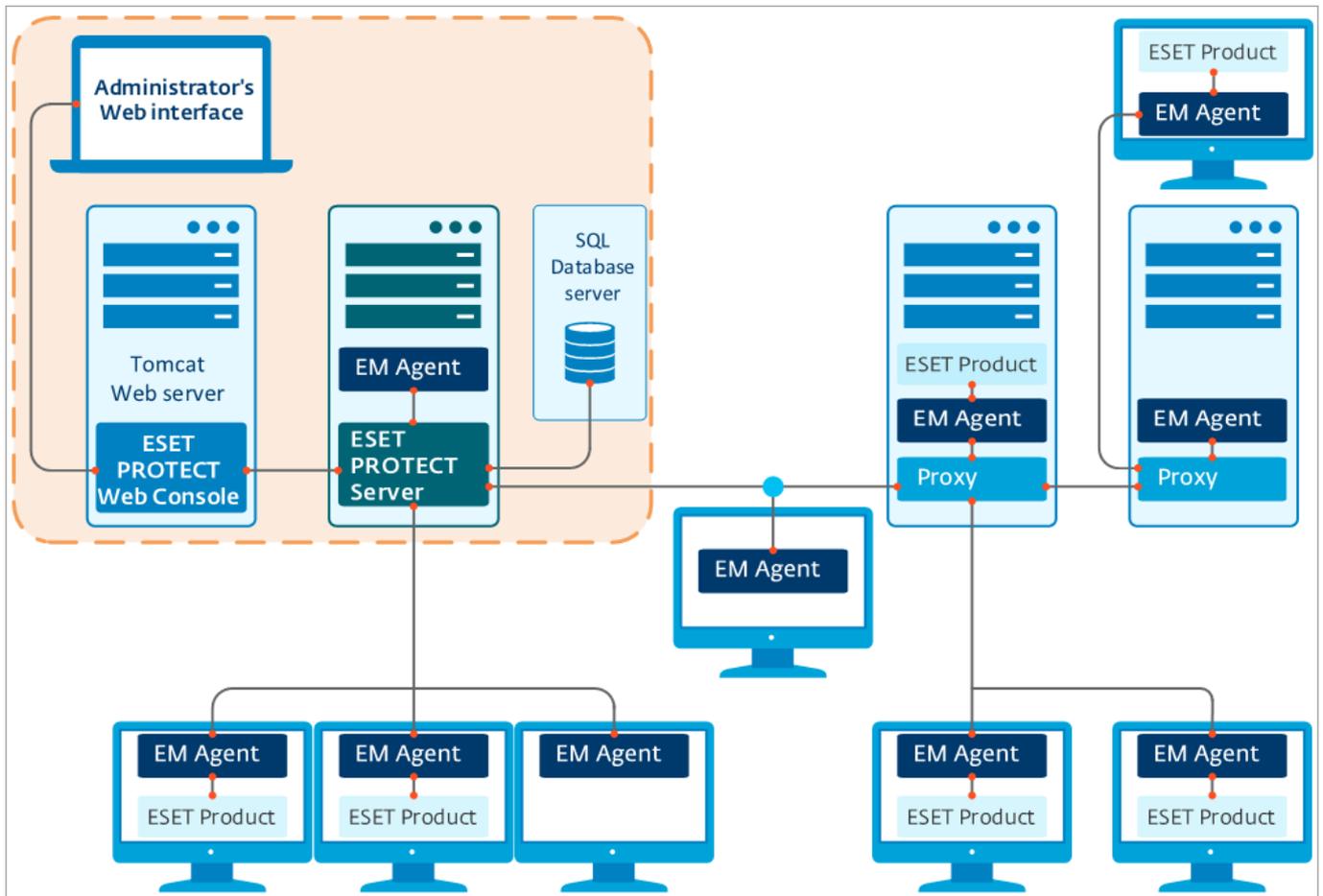


Web-Konsole

Die ESET PROTECT-Web-Konsole ist eine webbasierte Benutzeroberfläche, mit der Sie die ESET-Sicherheitslösungen in Ihrer Umgebung verwalten können. Sie bietet eine Übersicht über den Status der Clients im Netzwerk und kann zur Remote-Bereitstellung von ESET-Lösungen auf unverwalteten Computern verwendet werden. Der Zugriff auf die Web-Konsole erfolgt über einen Browser (siehe [Unterstützte Webbrowser](#)). Wenn Sie den Zugriff über das Internet auf den Webserver zulassen, können Sie ESET PROTECT von nahezu jedem beliebigen Standort und Gerät aus verwenden.

Die Web-Konsole verwendet Apache Tomcat als HTTP-Webserver. Wenn Sie den im ESET-Installationsprogramm oder in der virtuellen Appliance enthaltenen Tomcat verwenden, erlaubt die Web-Konsole nur Verbindungen mit TLS 1.2 und 1.3.

i Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server.



HTTP-Proxy

Was ist ein HTTP-Proxy, und welchen Zweck erfüllt er?

Der HTTP-Proxy leitet die Kommunikation von den Agenten zum ESET PROTECT Server in Umgebungen weiter, in denen die Agentencomputer den Server nicht erreichen können.

Wie funktioniert der Proxy in ESET PROTECT?

ESET PROTECT9 verwendet eine speziell konfigurierte Version von [Apache HTTP Proxy](#) als Proxykomponente. Mit der entsprechenden Konfiguration kann Apache HTTP Proxy als Proxy für ESET Management Agenten eingesetzt werden. Der Proxy führt kein Caching der Kommunikation durch und öffnet diese nicht, er leitet sie lediglich weiter.

Kann ich einen anderen Proxy verwenden als [Apache HTTP Proxy](#)?

Eine Proxy-Lösung muss die folgenden Bedingungen erfüllen, um mit dem ESET Management Agent kompatibel zu sein:

- Weiterleitung von SSL-Kommunikation
- unterstützt HTTP CONNECT
- Verwendet keinen Benutzernamen und kein Passwort

Wodurch unterscheidet sich das neue Kommunikationsprotokoll?

Der ESET PROTECT Server kommuniziert mit ESET Management Agenten über das gRPC-Protokoll. Die Kommunikation verwendet TLS und HTTP2 und kann daher über Proxyserver geleitet werden. Außerdem werden neue Selbstreparaturfunktionen und eine persistente Verbindung eingesetzt, um die Gesamtleistung der Kommunikation zu verbessern.

Wie wirkt sich dies auf die Leistung aus?

Der Einsatz eines HTTP-Proxy hat keine spürbaren Auswirkungen auf die Leistung.

Wann sollte ich den Proxy verwenden?

Sie sollten einen Proxy verwenden, wenn Ihre Infrastruktur mindestens eine der folgenden Bedingungen erfüllt:

- Wenn sich Ihre Agentencomputer nicht direkt mit dem ESET PROTECT Server verbinden können.
- Falls Sie Remote-Standorte oder Zweigstellen verwalten und den Proxy für die folgenden Kommunikationsarten einsetzen möchten:

○ Zwischen ESET PROTECT Server und Proxy

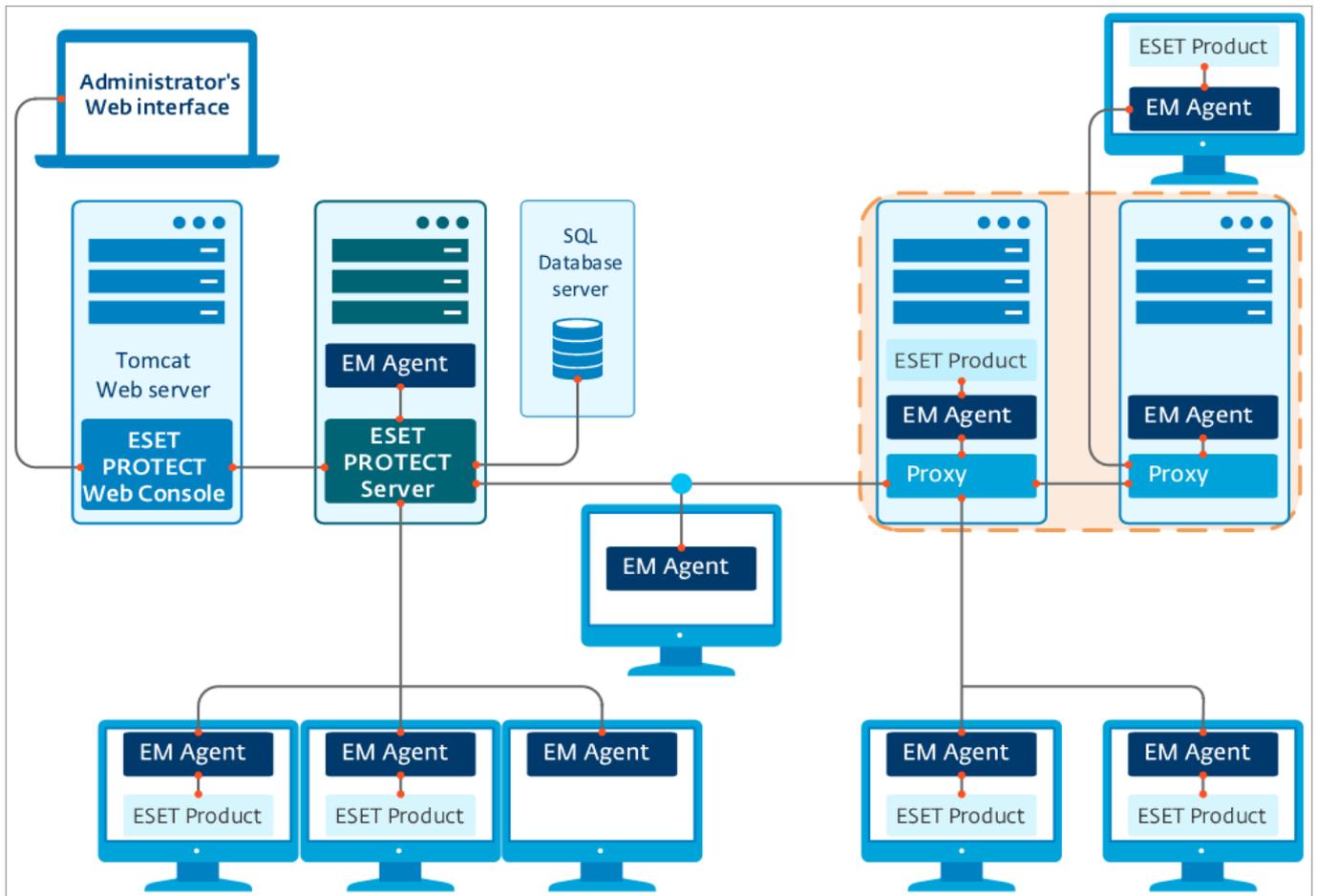
○ Zwischen Proxy und Clientcomputern an einem Remote-Standort

Einrichten des HTTP-Proxy

Um den Proxy verwenden zu können, müssen Sie den Hostnamen des HTTP-Proxy in der [Agenten-Policy \(Erweiterte Einstellungen > HTTP-Proxy\)](#) festlegen. Mit den folgenden Policy-Einstellungen können Sie unterschiedliche Proxys für Caching und Weiterleitung verwenden:

- **Globaler Proxy** – Sie verwenden eine einzige Proxylösung, um Downloads zwischenspeichern und die Agenten-Kommunikation weiterzuleiten.
- **Separater Proxy pro Dienst** – Sie verwenden jeweils separate Proxylösungen, um Downloads zwischenspeichern und die Agenten-Kommunikation weiterzuleiten.

i Welche weiteren Funktionen erfüllt der [Apache HTTP Proxy](#)?



Apache HTTP-Proxy

Apache HTTP Proxy ist ein Proxydienst, der verwendet werden kann, um Updates an Clientcomputer zu verteilen.

Um Apache HTTP Proxy zu installieren, lesen Sie die Anweisungen für [Windows](#), [Linux](#) oder die [virtuelle Appliance](#).

Apache HTTP Proxy: Funktionen

Funktion:	Proxylösung, die diese Funktion bereitstellt
Caching von Downloads und Updates	Apache HTTP Proxy oder eine andere Proxylösung
Caching von Ergebnissen aus ESET LiveGuard Advanced	Nur mit konfiguriertem Apache HTTP Proxy
Replikation der Kommunikation zwischen ESET Management Agenten und ESET PROTECT Server	Apache HTTP Proxy oder eine andere Proxylösung

Caching-Funktion

Apache HTTP Proxydownloads und Cache:

- ESET-Modulupdates
- Installationspakete von Repository-Servern
- Updates für Produktkomponenten

Die zwischengespeicherten Daten werden an die Endpunktclients in Ihrem Netzwerk verteilt. Mit Caching können Sie den Internet-Datenverkehr in Ihrem Netzwerk drastisch reduzieren.

Im Gegensatz zum Mirror-Tool, das alle verfügbaren Daten auf die ESET Update-Server herunterlädt, reduziert der Apache HTTP Proxy die Netzwerklast, indem er nur Daten herunterlädt, die von ESET PROTECT-Komponenten oder ESET-Endpunktprodukten angefordert werden. Wenn ein Endpunkt-Client ein Update anfordert, lädt der Apache HTTP Proxy dieses Update von den ESET Update-Servern herunter, speichert es in seinem Cache-Verzeichnis und liefert es dann an den entsprechenden Endpunkt-Client aus. Wenn ein weiterer Client dasselbe Update anfordert, liefert der Apache HTTP Proxy diesen Download direkt aus seinem Cache aus, ohne weitere Daten von den ESET Update-Servern herunterzuladen.

Caching für ESET-Endpunktprodukt

Die Caching-Einstellungen für ESET Management Agent und Endpoint sind nicht identisch. Der ESET Management Agent kann die Einstellungen für ESET-Sicherheitsprodukte auf Clientgeräten verwalten. Der Proxy für ESET Endpoint Security kann auf die folgenden Arten eingerichtet werden:

- [lokal](#) in der Benutzeroberfläche
- in der ESET PROTECT Web-Konsole mit einer Policy (die empfohlene Methode zur [Verwaltung](#) von Einstellungen auf Clientgeräten).

Caching von Ergebnissen aus ESET LiveGuard Advanced

Der Apache HTTP Proxy kann auch die von [ESET LiveGuard Advanced](#) gelieferten Ergebnisse im Cache speichern. Für das Caching ist eine spezielle Konfiguration erforderlich, die in dem von ESET verteilten Apache HTTP Proxy enthalten ist. Verwenden Sie das Caching nach Möglichkeit zusammen mit ESET LiveGuard Advanced. Weitere Details finden Sie in der [Dokumentation](#) des Diensts.

Apache als HTTP-Proxy für die Kommunikation zwischen Agent und Server

Bei korrekter Konfiguration kann der Apache HTTP Proxy verwendet werden, um Daten von ESET PROTECT-Komponenten an einem Remote-Standort zu sammeln und weiterzuleiten. Sie können unterschiedliche Proxylösungen für das Caching von Updates (wir empfehlen Apache HTTP Proxy) und für die Kommunikation zwischen Agent und Server verwenden. Apache HTTP Proxy kann zwar gleichzeitig für beide Funktionen verwendet werden, dies wird jedoch für Netzwerke mit mehr als 10.000 Clientcomputern pro Proxycomputer nicht empfohlen. In Unternehmensumgebungen (mehr als 1.000 verwaltete Computer) empfehlen wir, einen dedizierten Apache HTTP Proxy-Server zu verwenden.

Erfahren Sie mehr über die [Proxyfunktion](#).

Einrichten des HTTP-Proxy

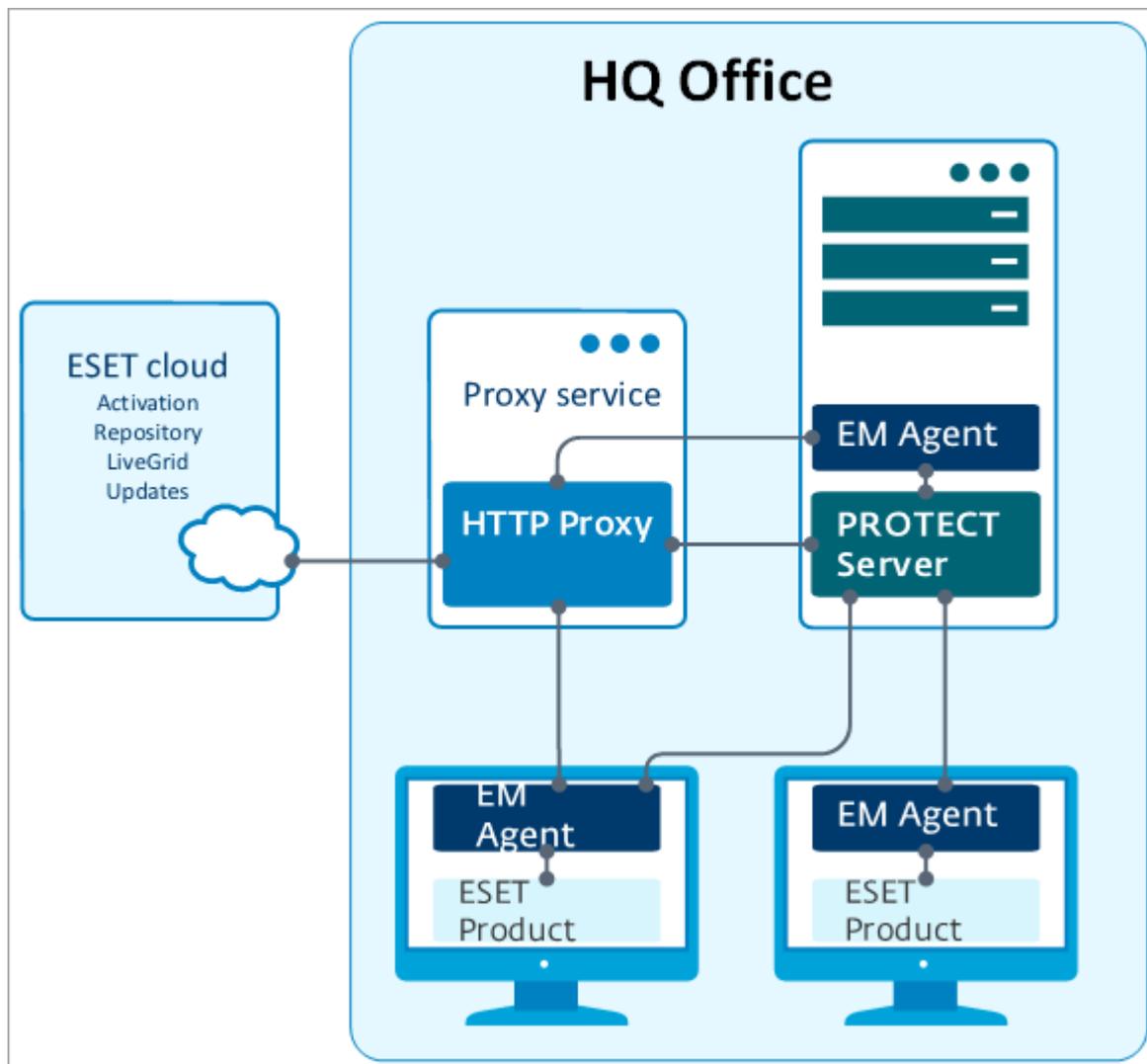
Um den Proxy verwenden zu können, müssen Sie den Hostnamen des HTTP-Proxy in der [Agenten-Policy](#) (**Erweiterte Einstellungen > HTTP-Proxy**) festlegen. Mit den folgenden Policy-Einstellungen können Sie unterschiedliche Proxys für Caching und Weiterleitung verwenden:

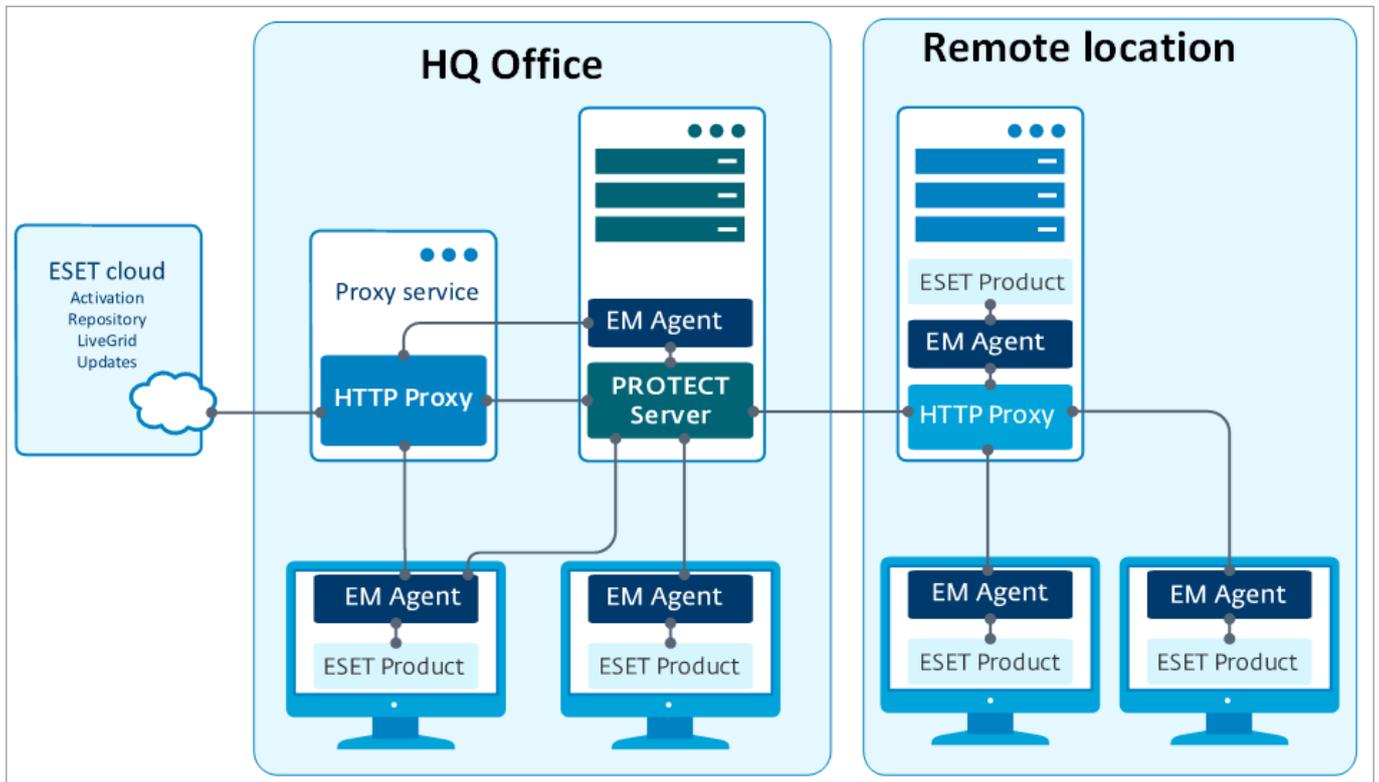
- **Globaler Proxy** – Sie verwenden eine einzige Proxylösung, um Downloads zwischenspeichern und die Agenten-Kommunikation weiterzuleiten.
- **Separater Proxy pro Dienst** – Sie verwenden jeweils separate Proxylösungen, um Downloads

zwischenzuspeichern und die Agenten-Kommunikation weiterzuleiten.

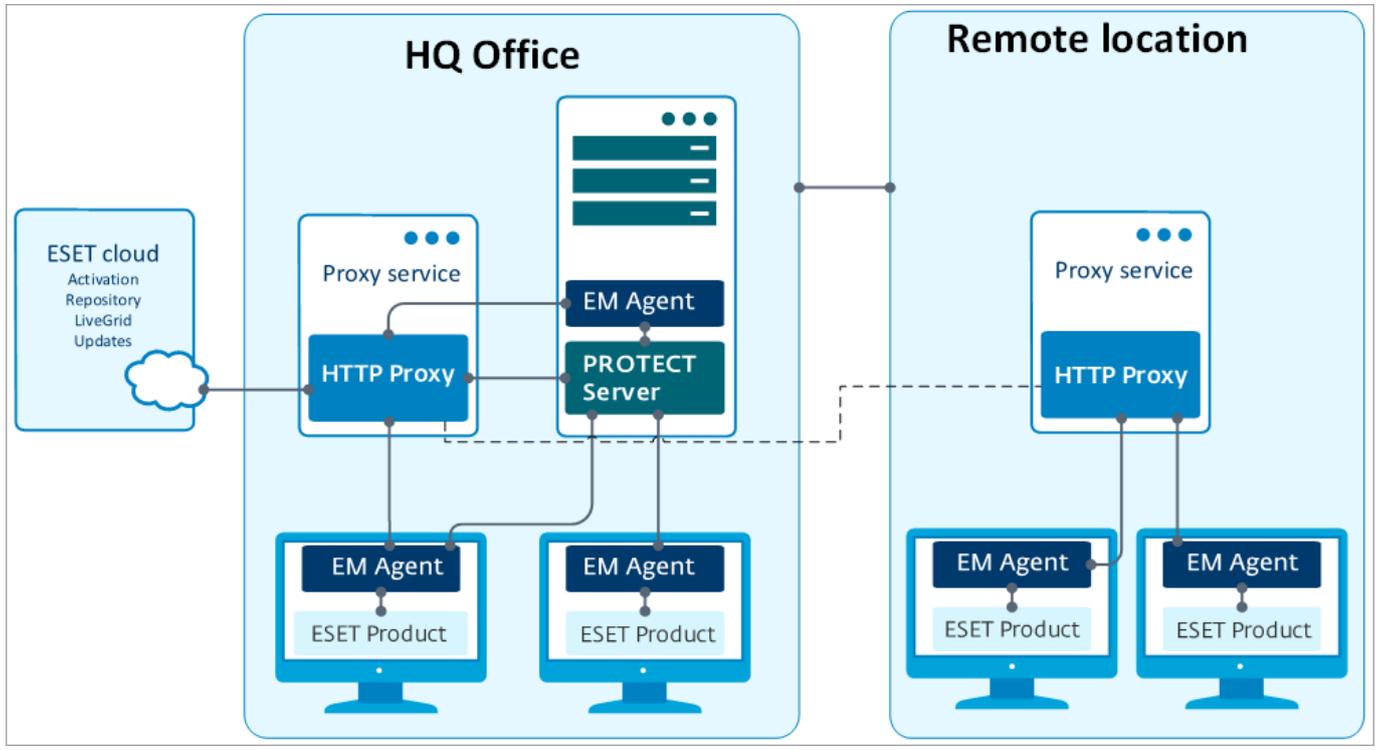
Apache HTTP Proxy in der Infrastruktur

Das folgende Diagramm zeigt einen Proxyserver (Apache HTTP Proxy), der den ESET-Cloud-Datenverkehr an alle ESET PROTECT-Komponenten und ESET-Endpunktprodukte verteilt.





! Sie können eine [Proxy-Kette](#) verwenden, um einen weiteren Proxy-Dienst an einem entfernten Standort einzurichten. ESET PROTECT unterstützt keine Verkettung von Proxies, wenn die Proxies Authentifizierung erfordern. Sie können eine eigene transparente Webproxy-Lösung verwenden, müssen jedoch ggf. weitere Konfigurationsschritte vornehmen, die hier nicht aufgeführt sind.



i Verwenden Sie für Offline-Updates der Erkennungsroutine das Mirror-Tool (verfügbar für [Windows](#) und [Linux](#)) anstelle des Apache HTTP Proxy.

Agent

Der ESET Management Agent ist ein wichtiger Bestandteil von ESET PROTECT. Die Clients kommunizieren nicht direkt mit dem ESET PROTECT Server, sondern über den Agenten. Der Agent erfasst Informationen vom Client und sendet sie an den ESET PROTECT Server. Wenn der ESET PROTECT Server dem Client einen Task übermittelt, wird dieser Task an den Agenten gesendet, der ihn an den Client weitergibt. Der ESET Management Agent verwendet ein neues, verbessertes [Kommunikationsprotokoll](#).

Zur einfacheren Implementierung des Endpunktschutzes ist der eigenständige ESET Management Agent in der ESET PROTECT Suite enthalten. Der Agent ist ein einfacher, hochmodularer und leichter Dienst, der die gesamte Kommunikation zwischen dem ESET PROTECT Server und beliebigen ESET-Produkten bzw. Betriebssystemen übernimmt. ESET-Produkte kommunizieren nicht direkt mit dem ESET PROTECT Server, sondern über den Agenten. Clientcomputer, auf denen der ESET Management Agent installiert ist und die mit dem ESET PROTECT Server kommunizieren können, werden als „verwaltet“ bezeichnet. Sie können den Agenten auf einem beliebigen Computer installieren, unabhängig davon, ob auf dem Computer eine ESET-Software installiert ist.

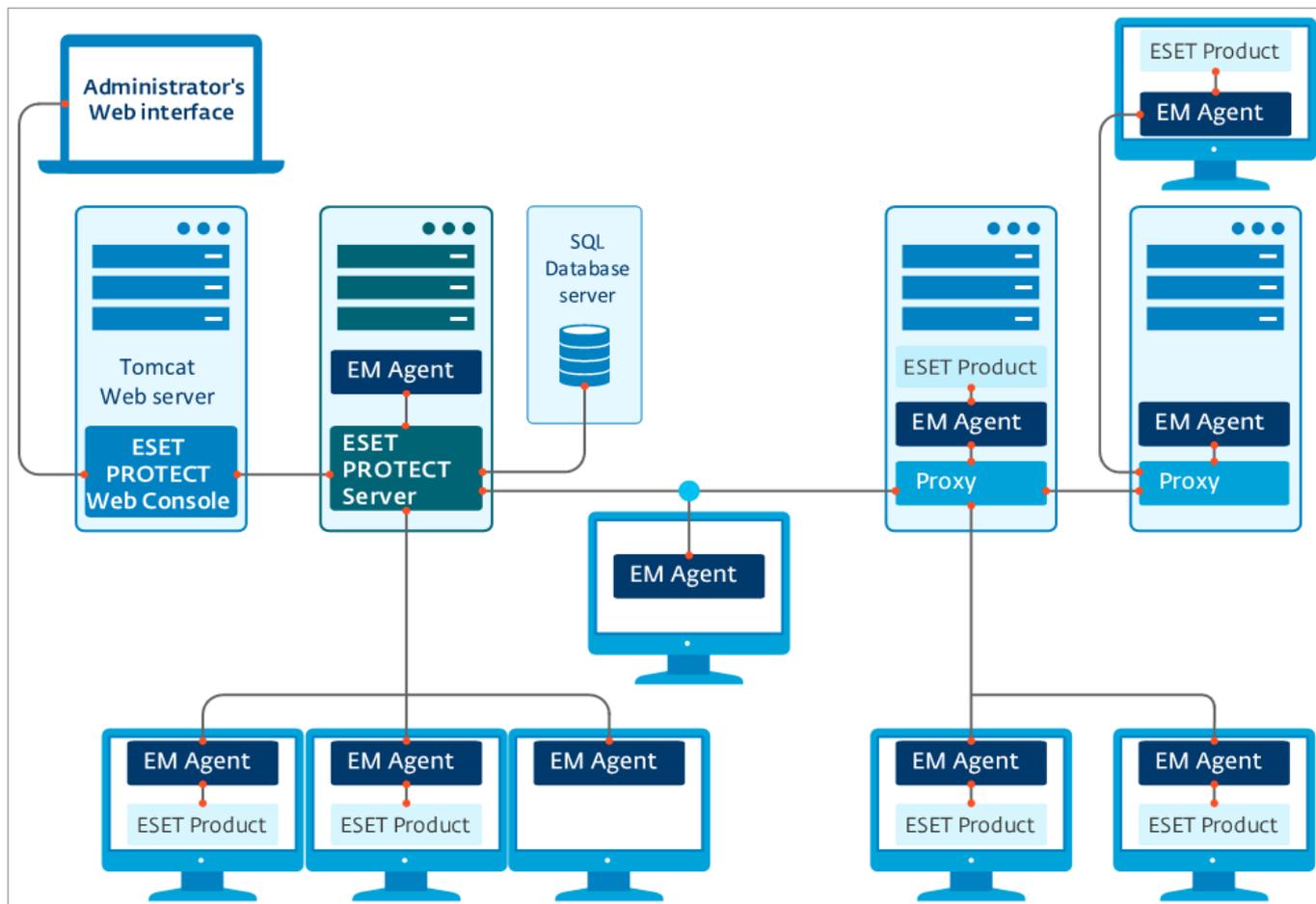
Vorteile des Agenten:

- **Einfache Einrichtung:** Der Agent kann als Bestandteil einer standardmäßigen Unternehmensinstallation bereitgestellt werden.
- **Sicherheitsverwaltung vor Ort:** Der Agent kann mit mehreren gespeicherten Sicherheitsszenarien konfiguriert werden, was die Reaktionszeit bei Ereignissen deutlich reduziert.
- **Offline-Sicherheitsverwaltung:** Der Agent kann auch ohne bestehende Verbindung zum ESET PROTECT Server auf Ereignisse reagieren.



Das Kommunikationsprotokoll zwischen Agent und ESET PROTECT Server unterstützt keine Authentifizierung. Daher können für die Weiterleitung der Agenten-Kommunikation zum ESET PROTECT Server keine Proxylösungen mit Authentifizierung verwendet werden.

Wenn Sie einen vom Standard abweichenden Port für Web-Konsole oder Agent verwenden, müssen Sie möglicherweise die Firewall anpassen. Andernfalls können bei der Installation Fehler auftreten.



Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) ist ein Erkennungstool, das Ihr Netzwerk auf unerwünschte Computer durchsucht. Der Sensor ist besonders hilfreich, weil er neue Computer aus ESET PROTECT erkennen kann, ohne dass diese gesucht und manuell hinzugefügt werden müssen. Die gefundenen Computer werden sofort erkannt und in einem vordefinierten Bericht gemeldet, sodass Sie diese in bestimmte statische Gruppen verschieben und mit Ihren Verwaltungsaufgaben fortfahren können.

RD Sensor wartet aktiv auf ARP-Broadcasts. Wenn eine neue aktive Netzwerkkomponente erkannt wird, sendet RD Sensor ARP-Unicasts, generiert den Fingerabdruck des Hosts (mit [mehreren Ports](#)) und sendet Informationen über die erkannten Computer an den ESET PROTECT Server. Der ESET PROTECT Server bewertet anschließend, ob die im Netzwerk gefundenen PCs dem ESET PROTECT Server unbekannt sind oder bereits verwaltet werden.

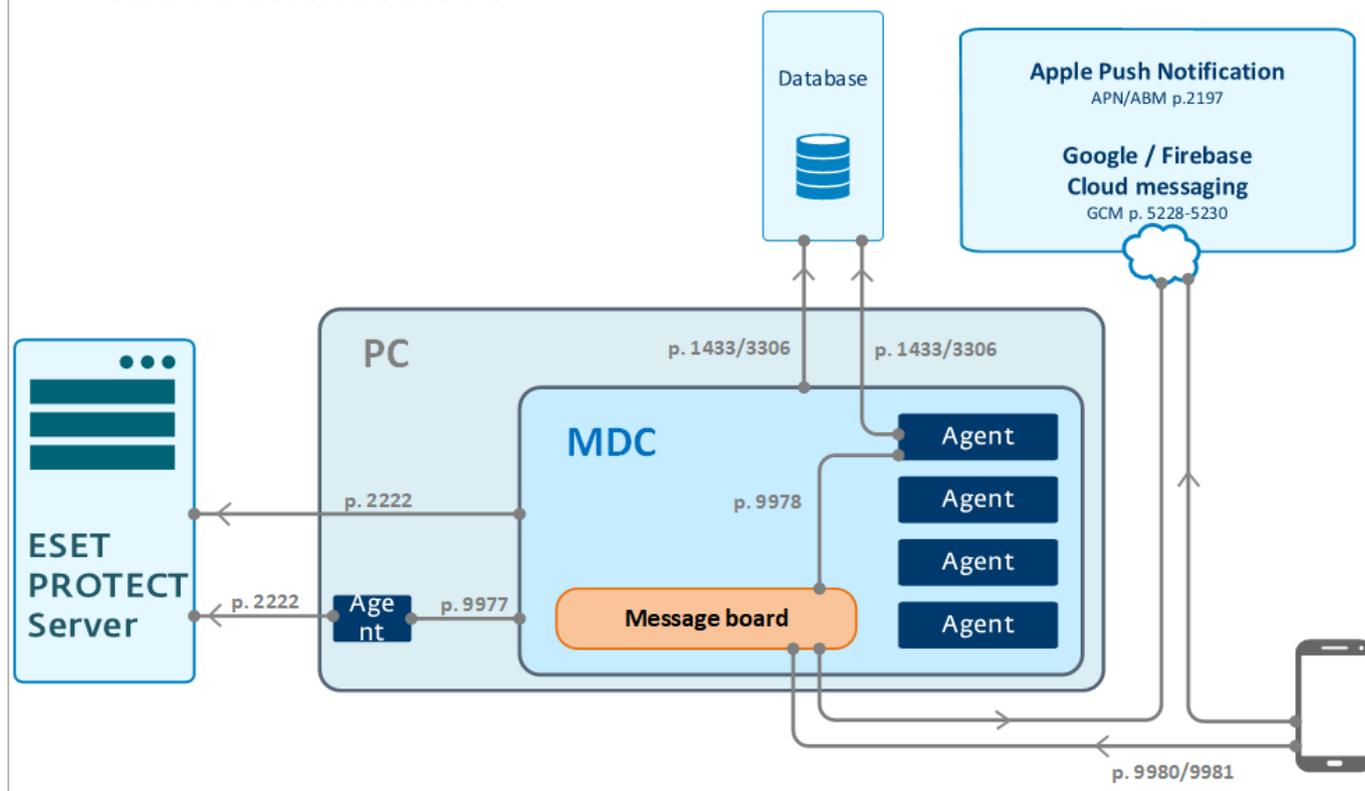
Das Generieren des Host-Fingerabdrucks kann nicht deaktiviert werden, da dies die Hauptfunktion von RD Sensor ist.



Falls Sie mehrere Netzwerksegmenten verwenden, müssen Sie den Rogue Detection Sensor in jedem Netzwerksegment separat installieren, um eine umfassende Liste aller Geräte im gesamten Netzwerk zu erstellen.

Jeder Computer innerhalb der Netzwerkstruktur (Domäne, LDAP, Windows-Netzwerk) wird über einen Serversynchronisierungstask automatisch zur Computerliste auf dem ESET PROTECT Server hinzugefügt. Mit dem RD Sensor können auf einfache Weise alle Computer erkannt werden, die nicht in der Domäne oder der Netzwerkstruktur vorhanden sind, und zum ESET PROTECT-Server hinzugefügt werden. RD Sensor merkt sich Computer, die bereits erkannt wurden, und sendet nicht zweimal die gleichen Informationen.

ESET PROTECT – MDC – Device Communication scheme



[Bild vergrößern](#)

i Stellen Sie Ihre MDM-Komponente nach Möglichkeit nicht auf demselben Hostgerät wie den ESET PROTECT Server bereit.

Für etwa 80 verwaltete Mobilgeräte gelten die folgenden Hardwareempfehlungen:

Hardware	Empfohlene Konfiguration
Prozessor	4 Prozessorkerne, 2,5 GHz
ARBEITSSPEICHER	4 GB (empfohlen)
HDD	100 GB

Für mehr als 80 verwaltete Mobilgeräte gelten unwesentlich höhere Hardwareanforderungen. Die Latenz zwischen der Übertragung des Tasks von ESET PROTECT und der Ausführung des Tasks auf dem Mobilgerät steigt proportional zur Anzahl der Geräte in Ihrer Umgebung.

Führen Sie die MDM-Installationsanweisungen für Windows ([All-in-One-Installationsprogramm](#) oder [Komponenteninstallation](#)) oder [Linux](#) aus.

Unterschiede zwischen Apache HTTP Proxy, Mirror-Tool und Direktverbindung

Bei der Kommunikation zwischen ESET-Produkten werden Updates für Erkennungsroutine und Programm-Module sowie [ESET LiveGrid®](#)-Daten (siehe [Tabelle](#) unten) und Lizenzinformationen übertragen.

ESET PROTECT lädt die neuesten Produkte für die Verteilung auf Clientcomputer aus dem Repository herunter. Nach der Verteilung kann das Produkt auf dem Zielcomputer bereitgestellt werden.

ESET-Sicherheitsprodukte müssen nach der Installation aktiviert werden, d. h. das Produkt muss Ihre Lizenzinformationen mit dem Lizenzserver abgleichen. Nach der Aktivierung werden Erkennungsroutine und Programmmodule regelmäßig aktualisiert.

Durch das [ESET LiveGrid®-Frühwarnsystem](#) ist ESET gegenüber neuen Infiltrationen immer auf dem neuesten Stand und kann seine Kunden schneller schützen. Das System überträgt neue Ereignisse zur Analyse und Verarbeitung an das ESET Research Lab.

Modulupdates sind für den Großteil des Netzwerkdatenverkehrs verantwortlich. ESET-Sicherheitsprodukte laden normalerweise ca. 23,9 MB an Modulupdates pro Monat herunter.

[ESET LiveGrid®](#)-Daten (ca. 22,3 MB) und die Update-Versionsdatei (bis zu 11 KB) sind die einzigen verteilten Dateien, die nicht im Cache gespeichert werden können.

Wir unterscheiden zwischen zwei Arten von Updates: Level- und Nano-Updates. [Weitere Informationen zu den Update-Typen finden Sie in unserem Knowledgebase-Artikel.](#)

Sie können die Netzwerklast bei der Verteilung von Updates in einem Netzwerk von Computern auf zwei Arten reduzieren: mit dem [Apache HTTP Proxy](#) oder dem Mirror-Tool (verfügbar für [Windows](#) und [Linux](#)).

i Lesen Sie [diesen Knowledgebase-Artikel](#) zum Einrichten der Verkettung für das Mirror-Tool (Mirror-Tool für den Download von Updates von einem anderen Mirror-Tool konfigurieren).

ESET-Kommunikationsarten

Kommunikationsart	Häufigkeit	Auswirkung auf den Netzwerkdatenverkehr	Per Proxy weitergeleitete Kommunikation	Proxy-Caching-Option ¹	Mirror-Option ²	Offline-Umgebung
Agenten-Bereitstellung (Push / Live-Installationsprogramme aus Repository)	Einmalig	Ca. 50 MB pro Client	JA	JA3	NEIN	JA (GPO / SCCM, angepasste Live-Installationsprogramme) ⁴
Endpunkt-Installation (Software-Installation aus Repository)	Einmalig	Ca. 100 MB pro Client	JA	JA3	NEIN	Ja (GPO / SCCM, Installation mit Paket-URL) ⁴
Updates für Erkennungsroutine / Programmmodule	6 mal pro Tag oder häufiger	23,9 MB pro Monat ⁵	JA	JA	JA	Ja (Offline Mirror Tool & eigener HTTP-Server) ⁶
Update-Versionsdatei update.ver	Ca. 8 mal pro Tag	2,6 MB pro Monat ⁷	JA	NEIN	-	-
Aktivierung / Lizenzprüfung	4 mal pro Tag	Unerheblich	JA	NEIN	NEIN	Ja (In ESET Business Account generierte Offlinedateien) ⁸
ESET LiveGrid® Cloudbasierte Reputation	Bei Bedarf	11 MB pro Monat	JA	NEIN	NEIN	NEIN

1. Informationen zu den Auswirkungen und Vorteilen von Proxy-Caching finden Sie unter [Wann sollte ich Apache HTTP Proxy verwenden?](#)

2. Informationen zu den Auswirkungen einer Mirroring-Lösung finden Sie unter [Wann sollte ich das Mirror-Tool verwenden?](#)

3. Stellen Sie nach Möglichkeit pro Installation/Upgrade einen Agenten (pro Version) bzw. einen Endpunkt

bereit, um sicherzustellen, dass das Installationsprogramm im Cache gespeichert ist.

4. Informationen zur Bereitstellung des ESET Management Agenten in einem großen Netzwerk finden Sie unter [Agenten-Bereitstellung mithilfe von GPO und SCCM](#).

5. Ihr erstes Update der Erkennungsroutine kann je nach Alter des Installationspakets größer als normal ausfallen, da alle neueren Updates für Erkennungsroutine und Module heruntergeladen werden. Installieren und aktualisieren Sie zunächst einen Client, um sicherzustellen, dass die Updates für Erkennungsroutine und Programmmodule im Cache gespeichert sind.

6. Ohne Internetverbindung kann das Mirror Tool keine Updates für die Erkennungsroutine herunterladen. Sie können Apache Tomcat als HTTP-Server einsetzen, um Updates in ein für das Mirror-Tool (verfügbar für [Windows](#) und [Linux](#)) erreichbares Verzeichnis herunterzuladen.

7. Bei der Suche nach Updates für die Erkennungsroutine wird die Datei *update.ver* immer heruntergeladen und analysiert. Der Taskplaner für ESET-Produkte sucht standardmäßig einmal pro Stunde nach neuen Updates. Wir gehen davon aus, dass Client-Arbeitsstationen 8 Stunden pro Tag eingeschaltet sind. Die Datei *update.ver* ist ca. 11 KB groß.

8. [Laden Sie Offline-Lizenzdateien aus ESET Business Administrator](#) herunter.

i Updates für die Produktversionen 4 und 5 können nicht mit dem Apache HTTP Proxy zwischengespeichert werden. Verwenden Sie das [Mirror Tool](#), um Updates für diese Produkte zu verteilen.

Wann sollte ich den Apache HTTP Proxy verwenden

Aufgrund der Ergebnisse unserer praktischen Tests sollten Sie den Apache HTTP Proxy ab einer Netzwerkgröße von 37 Computern einsetzen.

! Für eine effektive Zwischenspeicherung müssen Datum und Uhrzeit auf dem HTTP-Proxyserver korrekt festgelegt sein. Unterschiede von mehreren Minuten können dazu führen, dass der Cache-Mechanismus nicht funktioniert und dass mehr Dateien als erforderlich heruntergeladen werden.

Eine Analyse der Netzwerkbandbreite für Updates in einem Testnetzwerk mit 1.000 Computern und mehreren Installationen und Deinstallationen hat die folgenden Ergebnisse geliefert:

- Ein einzelner Computer lädt im Durchschnitt 23,9 MB pro Monat für [Updates](#) herunter, wenn er sich direkt mit dem Internet verbindet (ohne Apache HTTP Proxy).
- Mit Apache HTTP Proxy betrug die Gesamtmenge der Downloads für das Netzwerk 900 MB pro Monat

Vergleich der heruntergeladenen Updatedaten pro Monat mit Direktverbindung oder Apache HTTP Proxy in einem Computernetzwerk:

Anzahl der PCs in Ihrem Firmennetzwerk	25	36	50	100	500	1.000
Direktverbindung zum Internet (MB pro Monat)	375	900	1.250	2.500	12.500	25.000
Apache HTTP Proxy (MB pro Monat)	30	50	60	150	600	900

Wann sollte ich das Mirror Tool

In Offline-Umgebungen, in denen sich die Computer über längere Zeiträume (Monate, ein Jahr) nicht mit dem Internet verbinden, ist das Mirror-Tool (verfügbar für [Windows](#) und [Linux](#)) die einzige Möglichkeit, um Updates für Produktmodule zu verteilen. Dieses Tool lädt alle verfügbaren Level- und Nano-Updates bei jeder neuen Update-Anforderung herunter, wenn ein neues Update verfügbar ist.

i Lesen Sie [diesen Knowledgebase-Artikel](#) zum Einrichten der Verkettung für das Mirror-Tool (Mirror-Tool für den Download von Updates von einem anderen Mirror-Tool konfigurieren).

Apache HTTP Proxy und das Mirror-Tool unterscheiden sich hauptsächlich darin, dass Apache HTTP Proxy nur fehlende Updates herunterlädt (z. B. Nano-Update 3), während das Mirror Tool alle verfügbaren [Level- und Nano-Updates](#) (oder je nach Konfiguration auch nur Level-Updates) herunterlädt, egal welches Update dem entsprechenden Produktmodul fehlt.

i Streaming-Updates sind mit dem Mirror-Tool nicht verfügbar. Wir empfehlen, die Updates soweit möglich über den HTTP-Proxy anstelle des Mirrors durchzuführen. Aktivieren Sie diese Option, wenn ein Computer offline ist, aber Zugriff auf einen anderen Computer hat, der mit dem Internet verbunden ist und den HTTP-Proxy für die Zwischenspeicherung von Update-Dateien verwenden kann.

Wir haben Mirror-Tool und [Apache HTTP Proxy](#) in einem identischen Netzwerk mit 1.000 Computern getestet. Laut unserer Analyse wurden in einem Monat insgesamt 5.500 MB an Updates heruntergeladen. Die Menge der heruntergeladenen Updates ist nicht angestiegen, als mehr Computer zum Netzwerk hinzugefügt wurden. Dies ist eine drastische Senkung der Last im Vergleich zu einer Konfiguration, in der sich die Clients direkt mit dem Internet verbinden, allerdings ist die Leistungssteigerung nicht so deutlich wie beim Einsatz des HTTP Proxys.

Anzahl der PCs in Ihrem Firmennetzwerk	25	36	50	100	500	1.000
Direktverbindung zum Internet (MB pro Monat)	375	900	1.250	2.500	12.500	25.000
Mirror-Tool (MB pro Monat)	5.500	5.500	5.500	5.500	5.500	5.500

i Selbst mit mehr als 1.000 Computern im Netzwerk steigt die verwendete Bandbreite für Updates nicht spürbar an, wenn Sie Apache HTTP Proxy oder das Mirror-Tool einsetzen.

Systemanforderungen und Größenbemessung

Für die Installation und den Betrieb von ESET PROTECT muss Ihr System bestimmte [Hardware-](#), [Datenbank-](#), [Netzwerk-](#) und [Software-](#)Anforderungen erfüllen.

Unterstützte Betriebssysteme

Die folgenden Abschnitte enthalten Informationen zu den Betriebssystemversionen von [Windows](#), [Linux](#) und [macOS](#) und [mobilen Betriebssystemen](#), die von den einzelnen ESET PROTECT-Komponenten unterstützt werden.

Windows

Die folgende Tabelle enthält die unterstützten Windows-Betriebssysteme für die einzelnen ESET PROTECT-Komponenten:

Betriebssystem	Server	Agent	RD Sensor	MDM
Windows Server 2008 R2 x64 SP1 mit KB4474419 und KB4490628 installiert		✓	✓	
Windows Server 2008 R2 CORE x64 mit KB4474419 und KB4490628 installiert		✓	✓	
Windows Storage Server 2008 R2 x64 mit KB4474419 und KB4490628 installiert		✓	✓	
Microsoft SBS 2011 Standard x64		✓	✓	
Microsoft SBS 2011 Essentials x64		✓	✓	
Windows Server 2012 x64	✓	✓	✓	✓
Windows Server 2012 CORE x64	✓	✓	✓	✓
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	✓	✓	✓	✓

Betriebssystem	Server	Agent	RD Sensor	MDM
Windows 7 x86 SP1 mit den neuesten Windows-Updates (mindestens KB4474419 und KB4490628)		✓	✓	
Windows 7 x64 SP1 mit den neuesten Windows-Updates (mindestens KB4474419 und KB4490628)		✓	✓	
Windows 8 x86		✓	✓	
Windows 8 x64	ⓘ*	✓	✓	ⓘ*
Windows 8.1 x86		✓	✓	
Windows 8.1 x64	ⓘ*	✓	✓	ⓘ*

Betriebssystem	Server	Agent	RD Sensor	MDM
Windows 10 x86		✓	✓	
Windows 10 x64 (alle offiziellen Versionen)	?	✓	✓	?
Windows 10 auf ARM		✓		
Windows 11 x64	?	✓	✓	?

* Die Installation von ESET PROTECT-Komponenten auf einem Client-BS ist unter Umständen nicht mit der Microsoft-Lizenzierungsrichtlinie kompatibel. Überprüfen Sie die Microsoft-Lizenzierungsrichtlinie oder wenden Sie sich an Ihren Softwarelieferanten. Für kleine und mittelgroße Netzwerkumgebungen empfehlen wir Ihnen, ESET PROTECT nach Möglichkeit unter Linux oder als [virtuelle Appliance](#) zu installieren.

Ältere MS Windows-Systeme:

- Installieren Sie immer das neueste Service Pack, insbesondere auf älteren Systemen wie Server 2008 und Windows 7.
 - ESET PROTECT unterstützt keine Verwaltung von Computern mit Windows 7 (ohne SP), Windows Vista oder Windows XP.
 - Ab dem 24. März 2020 bietet ESET keinen offiziellen oder technischen Support mehr für ESET PROTECT (Server und MDM) unter den folgenden Microsoft Windows-Betriebssystemen mehr an: Windows 7, Windows Server 2008 (alle Versionen).
- Illegale oder Raubkopien von Betriebssystemen werden nicht unterstützt.



Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).



Sie können ESET PROTECT auf Nicht-Server-Betriebssystemen ohne ESXi ausführen. Sie können den [VMware Player](#) auch auf Desktop-Betriebssystemen installieren und die virtuelle [ESET PROTECT-Appliance](#) bereitstellen.

Linux

Die folgende Tabelle enthält die unterstützten Linux-Betriebssysteme für die einzelnen ESET PROTECT-Komponenten:

Betriebssystem	Server	Agent	RD Sensor	MDM
Ubuntu 16.04.1 LTS x86 Desktop		✓	✓	
Ubuntu 16.04.1 LTS x86 Server		✓	✓	
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	✓	✓	✓	✓
RHEL Server 7 x86		✓	✓	
RHEL Server 7 x64	✓	✓	✓	✓

Betriebssystem	Server	Agent	RD Sensor	MDM
RHEL Server 8 x64	?	✓		✓
CentOS 7 x64	✓	✓	✓	✓
SLED 15 x64	✓	✓	✓	✓
SLES 12 x64	✓	✓	✓	✓
SLES 15 x64	✓	✓	✓	✓
OpenSUSE Leap 15.2 x64	✓	✓	✓	✓
Debian 9 x64	✓	✓	✓	✓
Debian 10 x64	✓	✓	✓	✓
Debian 11 x64		✓	✓	
Oracle Linux 8		✓	✓	
Amazon Linux 2		✓	✓	

* Red Hat Enterprise Linux Server 8.x kann keine Berichte im *.pdf*-Format generieren. Weitere Details finden Sie unter [Bekanntes Problem mit ESET PROTECT](#).

macOS

Betriebssystem	Agent
macOS 10.12 Sierra	✓
macOS 10.13 High Sierra	✓
macOS 10.14 Mojave	✓
macOS 10.15 Catalina	✓
macOS 11.0 Big Sur	✓
macOS 12.0 Monterey	✓
macOS 13.0 Ventura	✓

i macOS wird nur als Client unterstützt. Der [ESET Management Agent](#) und die [ESET-Produkte für macOS](#) können unter macOS installiert werden. Der ESET PROTECT Server kann jedoch nicht unter macOS installiert werden.

Mobilgerät

Betriebssystem	EESA	EESA-Gerätebesitzer	MDM iOS	MDM iOS ABM
Android 5.x+	✓			

Betriebssystem	EESA	EESA-Gerätebesitzer	MDM iOS	MDM iOS ABM
Android 6.x+	✓			
Android 7.x+	✓	✓		
Android 8.x+	✓	✓		
Android 9.0	✓	✓		
Android 10.0	✓	✓		
Android 11	✓	✓		
Android 12	✓			
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			✓	✓

* iOS DEP ist nur in [ausgewählten Ländern](#) verfügbar.



Aktualisieren Sie das BS auf Ihrem Mobilgerät immer auf die neueste Version, um auch weiterhin wichtige Sicherheitspatches zu erhalten.

[Voraussetzungen für iOS 10.3 und neuer:](#)

Seit der Veröffentlichung von iOS 10.3 wird den im Registrierungsprofil installierten Zertifizierungsstellen nicht mehr automatisch vertraut. Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- a) Verwenden Sie ein Zertifikat von einem [Zertifikataussteller, dem Apple vertraut](#).
- b) Installieren Sie das Zertifikat vor der Registrierung manuell. In diesem Fall müssen Sie die Stamm-ZS vor der Registrierung manuell auf dem Mobilgerät installieren und das installierte Zertifikat als [vollständig vertrauenswürdig](#) festlegen.

[Voraussetzungen für iOS 12:](#)

Lesen Sie die Voraussetzungen für iOS 10.3 und neuer.

- Die Verbindung muss **TLS 1.2 oder höher verwenden**.

- Die Verbindung muss eine **symmetrische Verschlüsselung mit AES-128** oder **AES-256** verwenden. Die vereinbarte Verschlüsselungssuite für TLS-Verbindungen muss **Perfect Forward Secrecy (PFS)** mit **Elliptic Curved Diffie-Hellman Ephemeral-Schlüsselaustausch (ECDHE)** unterstützen, und es muss eine der folgenden Varianten verwendet werden:

```
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
```

- Signierung mit **RSA-Schlüssel** mit einer Länge von **mindestens 2048 Bit**. Der Hashingalgorithmus des Zertifikats muss **SHA-2 mit Digest-Länge** (manchmal auch als „Fingerabdruck“ bezeichnet) sein oder eine Mindestlänge von 256 Bit haben (also **SHA-256** oder höher). Sie können ein Zertifikat mit diesen Anforderungen in ESET PROTECT mit aktivierter [erweiterter Sicherheit](#) generieren.
- Die Zertifikate müssen die **gesamte Zertifikatkette enthalten, inklusive der Stamm-ZS**. Die im Zertifikat enthaltene Stamm-ZS wird verwendet, um ein Vertrauensverhältnis mit Geräten herzustellen, und wird als Teil des MDM-Registrierungsprofils installiert.

[Voraussetzungen für iOS 13:](#)

- Um Mobilgeräte mit iOS 13 verwalten zu können, müssen Sie die neuen [Anforderungen](#) für Apple-Kommunikationszertifikate (MDM HTTPS) erfüllen. Zertifikate, die vor dem 1. Juli 2019 ausgestellt wurden, müssen diese Kriterien ebenfalls erfüllen.
- Das von der ESMC-ZS signierte HTTPS-Zertifikat erfüllt diese Anforderungen nicht.

 Wir empfehlen dringend, Ihre Mobilgeräte nicht auf iOS 13 zu aktualisieren, bevor Sie die [Anforderungen](#) für das Apple-Kommunikationszertifikat erfüllt haben. Andernfalls können sich Ihre Geräte nicht mehr mit ESET PROTECT MDM verbinden.

- Falls Sie bereits ein Upgrade ohne korrektes Zertifikat durchgeführt haben und sich Ihre Geräte nicht mehr mit ESET PROTECT MDM verbinden, müssen Sie zunächst Ihr aktuell für die Kommunikation mit iOS-Geräten verwendetes HTTPS-Zertifikat durch das Zertifikat ersetzen, das die [Anforderungen](#) für das Apple-Kommunikationszertifikat (MDM HTTPS) erfüllt. Anschließend können Sie Ihre iOS-Geräte neu registrieren.
- Falls Sie noch kein Upgrade auf iOS 13 durchgeführt haben, stellen Sie sicher, dass Ihr aktuell für die Kommunikation mit iOS-Geräten verwendetes MDM-HTTPS-Zertifikat die [Anforderungen](#) für das Apple-Kommunikationszertifikat (MDM HTTPS) erfüllt. Wenn dies der Fall ist, können Sie Ihre iOS-Geräte auf iOS 13 aktualisieren. Wenn das Zertifikat die Anforderungen nicht erfüllt, tauschen Sie das aktuelle MDM-HTTPS-Zertifikat durch ein HTTPS-Zertifikat aus, das die [Anforderungen](#) für das Apple-Kommunikationszertifikat (MDM HTTPS) erfüllt. Anschließend können Sie Ihre iOS-Geräte auf iOS 13 aktualisieren.

Unterstützte Umgebungen für die Desktopbereitstellung

Die Desktopbereitstellung vereinfacht die Geräteverwaltung und ermöglicht eine schnellere Übergabe von Desktopcomputern an Endbenutzer.

Desktops können entweder physisch oder virtuell bereitgestellt werden. Für virtualisierte Umgebungen und Streamed OS (Citrix-Bereitstellungsdienste) finden Sie eine Liste der [unterstützten Hypervisoren](#).

ESET PROTECT [unterstützt](#) :

- Systeme mit nicht-persistenten Laufwerken
- VDI-Umgebungen
- Identifikation von geklonten Computern

Unterstützte Hypervisoren und Hypervisor-Erweiterungen

Hypervisor	ESET PROTECT	ESET Full Disk Encryption
Citrix XenServer	✓	X
Microsoft Hyper-V	✓	✓ (Sicherer Start wird nicht unterstützt)
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	✓

Hypervisor-Erweiterung	ESET PROTECT	ESET Full Disk Encryption
Citrix VDI-in-a-box	✓	X
Citrix XenDesktop	✓	X

Tools

(gilt für physische und virtuelle Computer)

- Microsoft SCCM
- Windows Server 2012/2016/2019/2022 Server Manager
- Windows Admin Center

Größenbemessung für Hardware und Infrastruktur

Der ESET PROTECT Server-Computer sollte die Hardwareempfehlungen in der folgenden Tabelle erfüllen.

Anzahl Clients	ESET PROTECT Server + SQL-Datenbankserver				
	Prozessorkerne	CPU-Taktfrequenz (GHz)	RAM (GB)	Datenträger ¹	Datenträger-IOPS ²
Bis zu 1.000	4	2.1	4	Einfach	500
5.000	8	2.1	8		1.000
10.000 ³	4	2.1	16	Separat	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 Einfacher / separater Datenträger – Wir empfehlen, die [Datenbank](#) für Systeme mit mehr als 10.000 Clients auf einem separaten Datenträger zu installieren.

2 IOPS (E/A-Operationen pro Sekunde) - Mindestanforderung.

- Wir empfehlen einen Wert von etwa 0,2 IOPS pro verbundenem Client, aber nicht weniger als 500.
- Sie können den IOPS-Wert Ihres Datenträgers mit dem Tool [diskspd](#) und dem folgenden Befehl überprüfen:

Anzahl Clients	Befehl
Bis zu 5.000 Clients	<code>diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat</code>
Mehr als 5.000 Clients	<code>diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat</code>

3 siehe [Beispielszenario](#) für die Umgebung mit 10.000 Clients.

Datenträgerempfehlungen

Der Datenträger ist der wichtigste Faktor für die Leistung von ESET PROTECT.

- Die SQL Server-Instanz kann Ressourcen mit dem ESET PROTECT Server teilen, um die Nutzung zu optimieren und die Latenz zu minimieren. Führen Sie den ESET PROTECT Server und den Datenbankserver auf einem einzigen Computer aus, um die Leistung von ESET PROTECT zu verbessern.
- Sie können die Leistung des SQL-Servers verbessern, indem Sie Datenbank und Transaktions-Log-Dateien auf separaten Datenträgern ablegen, vorzugsweise auf separaten physischen SSD-Laufwerken.
- In Systemen mit einem einzelnen Laufwerk sollten Sie ein SSD-Laufwerk verwenden.
- Wir empfehlen, eine All-Flash-Architektur zu verwenden. Solid-State-Datenträger (SSD) sind wesentlich schneller als herkömmliche HDD-Laufwerke.
- Für Konfigurationen mit großem Arbeitsspeicher reicht eine SAS-Einrichtung mit R5 aus. Getestete Konfiguration: 10x 1,2 TB SAS-Laufwerke in R5 – zwei Paritätsgruppen in RAID 4+1 ohne zusätzliches Caching.

- Die Leistung verbessert sich nicht, wenn Sie ein für Unternehmen ausgelegtes SSD-Laufwerk mit hohem IOPS-Wert verwenden.
- Eine Kapazität von 100 GB ist ausreichend für beliebig viele Clients. Falls Sie die Datenbank häufig sichern, brauchen Sie unter Umständen eine höhere Kapazität.
- Verwenden Sie kein Netzlaufwerk, um die Leistung von ESET PROTECT nicht zu beeinträchtigen.
- Falls Sie eine mehrschichtige Speicherinfrastruktur mit Unterstützung für Online-Speichermigration verwenden, sollten Sie zunächst langsamere gemeinsam genutzte Speicherstufen verwenden und die Leistung von ESET PROTECT überwachen. Wenn die Lese-/Schreiblatenz 20 ms überschreitet, können Sie Ihre Speicherebene unterbrechungsfrei auf eine schnellere Ebene migrieren, um das kostengünstige Backend zu nutzen. Dieser Vorgang kann auch in einem Hypervisor ausgeführt werden, wenn Sie ESET PROTECT als virtuelle Maschine verwenden.

Größenempfehlungen für unterschiedliche Clientanzahlen

Hier finden Sie die Leistungsergebnisse für virtuelle Umgebungen mit einer bestimmten Anzahl an Clients über ein Jahr hinweg.

i Die Datenbank und ESET PROTECT wurden auf separaten virtuellen Maschinen mit identischen Hardwarekonfigurationen ausgeführt.

Prozessorkerne	CPU-Taktfrequenz (GHz)	RAM (GB)	Leistung		
			10.000 Clients	20.000 Clients	40.000 Clients
8	2.1	64	Hoch	Hoch	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Normal	Niedrig
2	2.1	16	Niedrig	Niedrig	Ungenügend
2	2.1	8	Sehr niedrig (nicht empfohlen)	Sehr niedrig (nicht empfohlen)	Ungenügend

Bereitstellungsempfehlungen

Bewährte Methoden für die Bereitstellung von ESET PROTECT

Anzahl Clients	Bis zu 1.000	1.000 - 5.000	5.000 - 10.000	10.000 - 50.000	50.000 - 100.000	100.000+
ESET PROTECT Server & Datenbankserver auf dem gleichen Computer	✓	✓	✓	X	X	X
Einsatz von MS SQL Express	✓	?	X	X	X	X
Einsatz von MS SQL	✓	✓	✓	✓	✓	✓
Einsatz von MySQL	✓	✓	✓	X	X	X
Einsatz der virtuellen ESET PROTECT-Appliance	✓	✓	Nicht empfohlen	X	X	X
VM-Server verwenden	✓	✓	✓	Optional	X	X

Anzahl Clients	Bis zu 1.000	1.000 - 5.000	5.000 - 10.000	10.000 - 50.000	50.000 - 100.000	100.000+
Empfohlenes Verbindungsintervall (während der Bereitstellungsphase)	60 Sekunden	5 Minuten	10 Minuten	15 Minuten	20 Minuten	25 Minuten
Empfohlenes Verbindungsintervall (nach der Bereitstellungsphase, im normalen Einsatz)	10 Minuten	10 Minuten	20 Minuten	30 Minuten	40 Minuten	60 Minuten

* Um zu vermeiden, dass die ESET PROTECT-Datenbank vollgeschrieben wird, sollten Sie dieses Szenario nicht verwenden, wenn Sie auch ESET Inspect einsetzen.

Verbindungsintervall

ESET PROTECT Server verwendet permanente Verbindungen zu den ESET Management Agenten. Die Datenübertragung erfolgt trotz permanenter Verbindung nur einmal pro Verbindungsintervall. Wenn das Replikationsintervall für 5.000 Clients beispielsweise auf acht Minuten festgelegt ist, erfolgen 5.000 Übertragungen alle 480 Sekunden, also 10,4 Übertragungen pro Sekunde. Achten Sie darauf, ein passendes [Client-Verbindungsintervall](#) festzulegen. Achten Sie darauf, dass die Gesamtzahl der Verbindungen zwischen Agenten und Server auch für leistungsstarke Konfigurationen einen Wert von 1.000 pro Sekunde nicht überschreitet.

Wenn ein Server überlastet ist oder eine Malware-Infektion auftritt (Beispiel: 20.000 Clients verbinden sich alle zehn Minuten mit einem Server, der nur 10.000 Clients bedienen kann), wird ein Teil der verbundenen Clients übersprungen. Nicht verbundene Clients versuchen später erneut, sich mit dem ESET PROTECT Server zu verbinden.

Einzelner Server (kleines Unternehmen)

Für die Verwaltung kleiner Netzwerke (bis zu 1.000 Clients) empfehlen wir einen einzigen Computer, auf dem der ESET PROTECT Server und alle zugehörigen ESET PROTECT-Komponenten installiert sind. Für kleine und mittelgroße Netzwerkumgebungen empfehlen wir Ihnen, ESET PROTECT nach Möglichkeit unter Linux oder als [virtuelle Appliance](#) zu installieren.

Remotezweigstellen mit Proxyservern

Verwenden Sie einen [Proxy](#) zum Weiterleiten der Kommunikation der ESET-Produkte, falls die Clientcomputer den ESET PROTECT Server nicht direkt sehen können. Der HTTP-Proxy führt keine Aggregation der Kommunikation durch und reduziert den Replikationsdatenverkehr nicht.

Hochverfügbarkeit (Unternehmen)

In Unternehmensumgebungen (über 10.000 Clients) sollten Sie Folgendes beachten:

- Der [RD Sensor](#) durchsucht das Netzwerk nach neuen Computern.
- Sie können den ESET PROTECT Server in einem Failover-Cluster installieren.
- Konfigurieren Sie Ihren [HTTP-Proxy](#) für eine große Anzahl an Clients.

Konfiguration der Web-Konsole für Unternehmenslösungen oder Systeme mit eingeschränkter Leistung

Die mit dem All-in-One-Installationsprogramm für Windows installierte ESET PROTECT-Web-Konsole reserviert standardmäßig 1024 MB Arbeitsspeicher für Apache Tomcat.

Sie können die Standardkonfiguration der Web-Konsole ändern und an Ihre Infrastruktur anpassen:

- In Unternehmensumgebungen können mit der Standardkonfiguration der Web-Konsole bei einer großen Anzahl von Objekten Stabilitätsprobleme auftreten. Ändern Sie die Tomcat-Einstellungen, um Speicherprobleme zu vermeiden. Stellen Sie sicher, dass Ihr System über ausreichend Arbeitsspeicher (mindestens 16 GB) verfügt, bevor Sie diese Änderungen vornehmen.
- Auf Systemen mit geringer Leistung und eingeschränkten Hardwareressourcen können Sie die Speichernutzung von Tomcat verringern.

i Die folgenden Speicherwerte sind Empfehlungen. Sie können die Speichereinstellungen für Tomcat an Ihre Hardwareressourcen anpassen.

Windows

1. Öffnen Sie die Datei *tomcat9w.exe* oder führen Sie die Anwendung **Configure Tomcat** aus.
2. Wechseln Sie zur Registerkarte **Java**.
3. Ändern Sie die Speichernutzung:
 - a. Erhöhen (Unternehmen): Ändern Sie die Werte unter **Initial memory pool** (ursprünglicher Speicherpool) auf 2048 MB und **Maximum memory pool** (maximaler Speicherpool) auf 16384 MB.
 - b. Reduzieren (leistungsschwache Systeme): Ändern Sie die Werte unter **Initial memory pool** (ursprünglicher Speicherpool) auf 256 MB und **Maximum memory pool** (maximaler Speicherpool) auf 2048 MB.
4. Starten Sie den Tomcat-Dienst neu.

LINUX und die virtuelle ESET PROTECT-Appliance

1. Öffnen Sie das Terminal als root oder verwenden Sie `sudo`.
2. Öffnen Sie die Datei
 - a. Virtuelle ESET PROTECT-Appliance / CentOS: `/etc/sysconfig/tomcat`
 - b. Debian: `/etc/default/tomcat9`
3. Fügen Sie die folgende Zeile zur Datei hinzu:

a.Speichernutzung erhöhen (Unternehmen): `JAVA_OPTS="-Xms2048m -Xmx16384m"`

b.Speichernutzung reduzieren (niedrige Systemleistung): `JAVA_OPTS="-Xms256m -Xmx2048m"`

4.Speichern Sie die Datei und starten Sie den Tomcat-Dienst neu.

```
service tomcat restart
```

Bereitstellung für 10.000 Clients

Hier finden Sie die Leistungsergebnisse für eine virtuelle Umgebung mit 10.000 Clients, die ein Jahr lang ausgeführt werden.

Konfiguration des Hypervisor-Servers

Komponente	Wert
VMware	ESXi 6.7 Update 2 und höher (VM Version 15)
Hypervisor	VMware ESXi, 6.7.0
Logische Prozessoren	112
Prozessortyp	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

Der Test wurde auf dedizierten Rechnern ausgeführt



Die Datenbank und ESET PROTECT wurden auf separaten virtuellen Maschinen mit identischen Hardwarekonfigurationen ausgeführt.

Auf virtuellen Maschinen verwendete Software

ESET PROTECT:

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

Datenbank:

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

Beschreibung der ESET PROTECT-Umgebung

- 10.000 Clientverbindungen
- Etwa 2.000 dynamische Gruppen und 2.000 Templates für dynamische Gruppen
- Etwa 255 statische Gruppen
- 20 Benutzer
- 15-minütiges Verbindungsintervall für ESET Management Agenten
- Nachdem die Umgebung ein Jahr lang ausgeführt wurde, beträgt die Datenbankgröße 15 GB.

CPU-Anzahl	RAM (GB)	Leistung
8	64	Hoch
4	32	Normal
2	16	Niedrig
2	8	Sehr niedrig (nicht empfohlen)

Datenbank

Geben Sie den Datenbankserver und den Connector bei der Installation des ESET PROTECT Servers an. Sie können einen vorhandenen Datenbankserver in Ihrer Umgebung verwenden. Dieser muss jedoch die folgenden Anforderungen erfüllen.

ESET PROTECT 9.1 [All-in-One-Installationsprogramm](#) installiert standardmäßig Microsoft SQL Server Express 2019.

o Falls Sie eine ältere Windows Edition verwenden (Server 2012 oder SBS 2011), wird standardmäßig Microsoft SQL Server Express 2014 installiert.

o Das Installationsprogramm generiert automatisch ein zufälliges Passwort für die Datenbankauthentifizierung (gespeichert in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`).

 Microsoft SQL Server Express hat eine Obergrenze von je 10 GB für relationale Datenbanken. Microsoft SQL Server Express sollte nicht verwendet werden:

- In Unternehmensumgebungen oder großen Netzwerken.
- Falls Sie ESET PROTECT mit [ESET Inspect](#) verwenden möchten.

Unterstützte Datenbankserver und Datenbank-Connectoren

ESET PROTECT unterstützt zwei Arten Datenbankserver: Microsoft SQL Server und MySQL.

 MariaDB wird von ESET PROTECT nicht unterstützt. MariaDB ist eine Standarddatenbank in den meisten Linux-Umgebungen und wird installiert, wenn Sie die Installation von MySQL auswählen.

Unterstützte Datenbankserver	Unterstützte Datenbankversionen	Unterstützte Datenbank-Connectoren
Microsoft SQL Server	<ul style="list-style-type: none"> • Express- und nicht-Express-Editionen • 2014, 2016, 2017, 2019 	<ul style="list-style-type: none"> • SQL Server • SQL Server Native Client 10.0 • ODBC-Treiber für SQL Server 11, 13, 17, 18
MySQL	<ul style="list-style-type: none"> • 5.6* • 5.7 • 8.0 	MySQL ODBC-Treiberversionen: <ul style="list-style-type: none"> • 5.1, 5.2 • 5.3.0-5.3.10 • 8.0.16, 8.0.17 • 8.0.27 (Nur Windows)

* MySQL 5.6 wird seit Februar 2021 nicht mehr unterstützt. Wir empfehlen, Ihren MySQL-Datenbankserver auf 5.7 oder eine neuere Version zu [aktualisieren](#).

Die folgenden MySQL ODBC-Treiberversionen werden nicht unterstützt:



- 5.3.11 und höhere 5.3.x
- 8.0.0-8.0.15
- 8.0.18 und höher

Hardwareanforderungen für den Datenbankserver

Beachten Sie die Anweisungen bezüglich [Hardware](#) und Größenbemessung.

Leistungsempfehlungen

Aus Leistungsgründen empfehlen wir, die neueste unterstützte Version von Microsoft SQL Server als ESET PROTECT-Datenbank zu verwenden. ESET PROTECT ist zwar auch mit MySQL kompatibel, aber die Verwendung von MySQL kann die Systemleistung beeinträchtigen, wenn Sie mit großen Datenmengen arbeiten, beispielsweise mit großen Dashboards, vielen Ereignissen oder vielen Clients. Microsoft SQL Server kann mit derselben Hardware eine deutlich höhere Anzahl an Clients verarbeiten als MySQL.

Für den SQL-Datenbankserver haben Sie die folgenden Auswahlmöglichkeiten:

- Installation auf demselben Computer wie der ESET PROTECT Server.
- Installation auf demselben Computer, aber auf einem anderen Datenträger.
- Installation auf einem dedizierten SQL-Datenbankserver

Sie sollten einen dedizierten Computer mit reservierten Ressourcen verwenden, wenn Sie vorhaben, mehr als 10.000 Clients zu verwalten.

Datenbank	SMB-Kunde	Enterprise-Kunde	Clients-Limit	Windows	Linux
MS SQL Express	✓	(optional)	5.000	✓	
MS SQL Server	✓	✓	Keine	✓	
MySQL	✓	✓	10.000	✓	✓

Weitere Informationen



ESET PROTECT Server verwendet keine integrierte Sicherungslösung. Wir empfehlen dringend, den Datenbankserver regelmäßig zu [sichern](#), um Datenverluste zu vermeiden.

- [Installieren Sie SQL Server sollte nicht auf einem Domänencontroller](#) (z. B. Windows SBS oder Essentials). Sollten Sie ESET PROTECT auf einem anderen Server installieren oder während der Installation nicht die SQL Server Express-Komponente auswählen (in diesem Fall müssen Sie SQL Server oder MySQL als ESET PROTECT-Datenbank verwenden).
- Falls Sie vorhaben, ein speziell eingerichtetes Datenbankkonto zu verwenden, das nur Zugriff auf die ESET PROTECT-Datenbank hat, müssen Sie vor der Installation ein Benutzerkonto mit speziellen Berechtigungen

erstellen. Weitere Informationen finden Sie unter [Speziell eingerichtetes Datenbankkonto](#). Außerdem müssen Sie eine leere Datenbank erstellen, die von ESET PROTECT verwendet werden kann.

- Lesen Sie die Anweisungen zur Installation und Konfiguration von [MySQL für Windows](#) und [MySQL für Linux](#) für die Arbeit mit ESET PROTECT.
- [MS SQL Server unter Linux](#) wird nicht unterstützt. Sie können jedoch [den ESET PROTECT Server unter Linux mit MS SQL Server unter Windows verbinden](#).
- Falls Sie ESET PROTECT Server und MS SQL Server [auf separaten Computern](#) installieren, können Sie [eine verschlüsselte Verbindung zur Datenbank aktivieren](#).
- Clustereinrichtungen der Datenbank in Windows-Umgebungen werden nur für MS SQL Server unterstützt, nicht für MySQL.

Unterstützte Versionen von Apache Tomcat und Java

Apache Tomcat

Apache Tomcat wird für die Ausführung der ESET PROTECT-Web-Konsole benötigt.

ESET PROTECT unterstützt nur Apache Tomcat 9.x (64-Bit). Verwenden Sie unbedingt die neueste Version von Apache Tomcat 9.x.

ESET PROTECT unterstützt keine Alpha-/Beta-/RC-Versionen von Apache Tomcat.

Java

Apache Tomcat benötigt Java/OpenJDK (64-Bit).

Falls Sie mehrere Java-Versionen auf Ihrem System installiert haben, empfehlen wir, die älteren Java-Versionen zu deinstallieren und nur die neueste [unterstützte Java](#)-Version zu behalten.



Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).

Unterstützte Webbrowser, ESET-Sicherheitsprodukte und Sprachen

ESET PROTECT unterstützt die folgenden Betriebssysteme:

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

Die ESET PROTECT-Web-Konsole unterstützt die folgenden Webbrowser:

Webbrowser
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

Für ein optimales Erlebnis mit der ESET PROTECT-Web-Konsole sollten Sie immer die aktuelle Version Ihres Webbrowsers verwenden.

Falls Sie Internet Explorer verwenden, erhalten Sie in der ESET PROTECT-Web-Konsole eine Meldung, dass Sie einen nicht unterstützten Webbrowser verwenden.

Letzte Versionen der ESET-Produkte, die mit ESET PROTECT9.1 verwaltet werden können

Produkt	Produktversion
ESET Endpoint Security für Windows	7.x, 8.x, 9.x
ESET Endpoint Antivirus für Windows	7.x, 8.x, 9.x
ESET Endpoint Security für MacOS	6.8+
ESET Endpoint Antivirus für MacOS	6.8+
ESET Endpoint Security für Android	2.x
ESET Server Security für Microsoft Windows Server	8.x, 9.x
ESET File Security für Microsoft Windows Server	7.x
ESET File Security für Microsoft Azure	7.x
ESET Mail Security für Microsoft Exchange Server	7.x, 8.x, 9.x
ESET Security for Microsoft SharePoint Server	7.x, 8.x, 9x
ESET Mail Security für IBM Domino Server	7.x, 8.x, 9.x
ESET File Security für Linux	7.x, 8.x
ESET Server Security für Linux	8.1+
ESET Endpoint Antivirus für Linux	7.x, 8.x, 9.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.6+
ESET Full Disk Encryption für Windows	
ESET Full Disk Encryption für MacOS	

Ältere Versionen der ESET-Produkte, die mit ESET PROTECT 9.1 verwaltet werden können:

Produkt	Produktversion
ESET Endpoint Security für Windows	6.5+
ESET Endpoint Antivirus für Windows	6.5+

Produkt	Produktversion
ESET File Security für Microsoft Windows Server	6.5
ESET File Security für Microsoft Azure	6.5
ESET Mail Security für Microsoft Exchange Server	6.5
ESET Mail Security für IBM Lotus Domino	6.5
ESET Security for Microsoft SharePoint Server	6.5
ESET Mail Security für Linux/FreeBSD*	4.5.x
ESET File Security für Linux/FreeBSD*	4.5.x
ESET Gateway Security für Linux/FreeBSD*	4.5.x

* Sie können diese Produkte nicht mit dem ESET Management Agent 9 verwalten. Verwenden Sie den ESET Management Agent 8.1 oder älter, um das Produkt zu verwalten.

i Ältere Versionen der ESET-Sicherheitsprodukte für Windows Server als die in der obigen Tabelle angegebenen können momentan nicht mit ESET PROTECT 9 verwaltet werden. Weitere Informationen zur Kompatibilität finden Sie unter [End-of-Life-Policy für ESET-Unternehmensprodukte](#).

Produkte, die mit einer Abonnementlizenz aktiviert werden können

ESET-Produkt	Verfügbar ab Version
ESET Endpoint Antivirus/Security für Windows	7.0
ESET Endpoint Antivirus/Security für macOS	6.8.x
ESET Endpoint Security für Android	2.0.158
ESET Mobile Device Management für Apple iOS	7.0
ESET File Security für Microsoft Windows Server	7.0
ESET Mail Security für Microsoft Exchange	7.0
ESET File Security für Windows Server	7.0
ESET Mail Security für IBM Domino	7.0
ESET Security for Microsoft SharePoint Server	7.0
ESET File Security für Linux	7.0
ESET Endpoint Antivirus für Linux	7.0
ESET Server Security für Windows	8.0
ESET Server Security für Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect (mit ESET Endpoint für Windows 7.3 und neuere Versionen)	1.5

Unterstützte Sprachen

Sprache	Code
English (United States)	en-US
Arabisch (Ägypten)	ar-EG
Chinesisch vereinfacht	zh-CN

Sprache	Code
Chinesisch traditionell	zh-TW
Kroatisch (Kroatien)	hr-HR
Tschechisch (Tschechische Republik)	cs-CZ
Französisch (Frankreich)	fr-FR
Französisch (Kanada)	fr-CA
Deutsch (Deutschland)	de-DE
Griechisch (Griechenland)	el-GR
Ungarisch (Ungarn)*	hu-HU
Indonesisch (Indonesien)*	id-ID
Italienisch (Italien)	it-IT
Japanisch (Japan)	ja-JP
Koreanisch (Korea)	ko-KR
Polnisch (Polen)	pl-PL
Portugiesisch (Brasilien)	pt-BR
Russisch (Russland)	ru-RU
Spanisch (Chile)	es-CL
Spanisch (Spanien)	es-ES
Slowakisch (Slowakei)	sk-SK
Türkisch (Türkei)	tr-TR
Ukrainisch (Ukraine)	uk-UA

* Nur das Produkt ist in dieser Sprache verfügbar, die Onlinehilfe dagegen nicht.

Netzwerk

Sowohl ESET PROTECT Server als auch die von ESET PROTECT verwalteten Clientcomputer benötigen eine funktionierende Internetverbindung, um mit dem ESET-Repository und den Aktivierungsservern kommunizieren zu können. Falls sich Ihre Clients nicht direkt mit dem Internet verbinden, können sie einen Proxyserver verwenden (nicht zu verwechseln mit dem Apache HTTP Proxy), um die Kommunikation mit Ihrem Netzwerk und dem Internet zu erleichtern.

Die von ESET PROTECT verwalteten Computer müssen mit demselben LAN verbunden sein und sich in derselben *Active Directory*-Domäne befinden wie Ihr ESET PROTECT Server. Der ESET PROTECT Server muss für die Clientcomputer sichtbar sein. Außerdem müssen Ihre Clientcomputer in der Lage sein, mit Ihrem ESET PROTECT Server zu kommunizieren, um Remote-Bereitstellungen und das Aktivierungsaufruf-Feature nutzen zu können.

ESET PROTECT für Windows/Linux ist mit den Internetprotokollen IPv4 und IPv6 kompatibel. Die virtuelle ESET PROTECT-Appliance ist nur mit IPv4 kompatibel.

Verwendete Ports

Falls Ihr Netzwerk eine Firewall verwendet, finden Sie hier eine Liste der [möglichen Netzwerkkommunikationsports](#), die verwendet werden, wenn ESET PROTECT mit den Komponenten in Ihrer Infrastruktur installiert ist.

Auswirkungen der Kommunikation zwischen ESET PROTECT Server und ESET Management Agenten auf den Netzwerkdatenverkehr

Die Anwendungen auf den Clientcomputern kommunizieren nicht direkt mit dem ESET PROTECT Server, sondern über die ESET Management Agenten. Diese Lösung ist einfacher zu verwalten und reduziert die über das Netzwerk übertragenen Daten. Der Netzwerkdatenverkehr hängt vom Client-Verbindungsintervall und den Tasks ab, die auf den Clients ausgeführt werden. Selbst wenn auf einem Client kein Task ausgeführt wird oder geplant ist, kommuniziert der ESET Management Agent einmal pro Verbindungsintervall mit dem ESET PROTECT Server. Jede Verbindung generiert Datenverkehr. Die folgende Tabelle enthält einige Beispiele für den Datenverkehr:

Aktionstyp	Datenverkehr in einem einzigen Verbindungsintervall
Client-Task: Nur Prüfen, keine Aktion	4 KB
Client-Task: Modul-Update	4 KB
Client-Task: SysInspector-Loganfrage	300 KB
Policy Virenschutz - Maximale Sicherheit	26 KB

ESET Management Agent-Replikationsintervall	Täglicher Datenverkehr eines ESET Management Agenten im Leerlauf
1 Minute	16 MB
15 Minuten	1 MB
30 Minuten	0,5 MB
1 Stunde	144 KB
1 Tag	12 KB

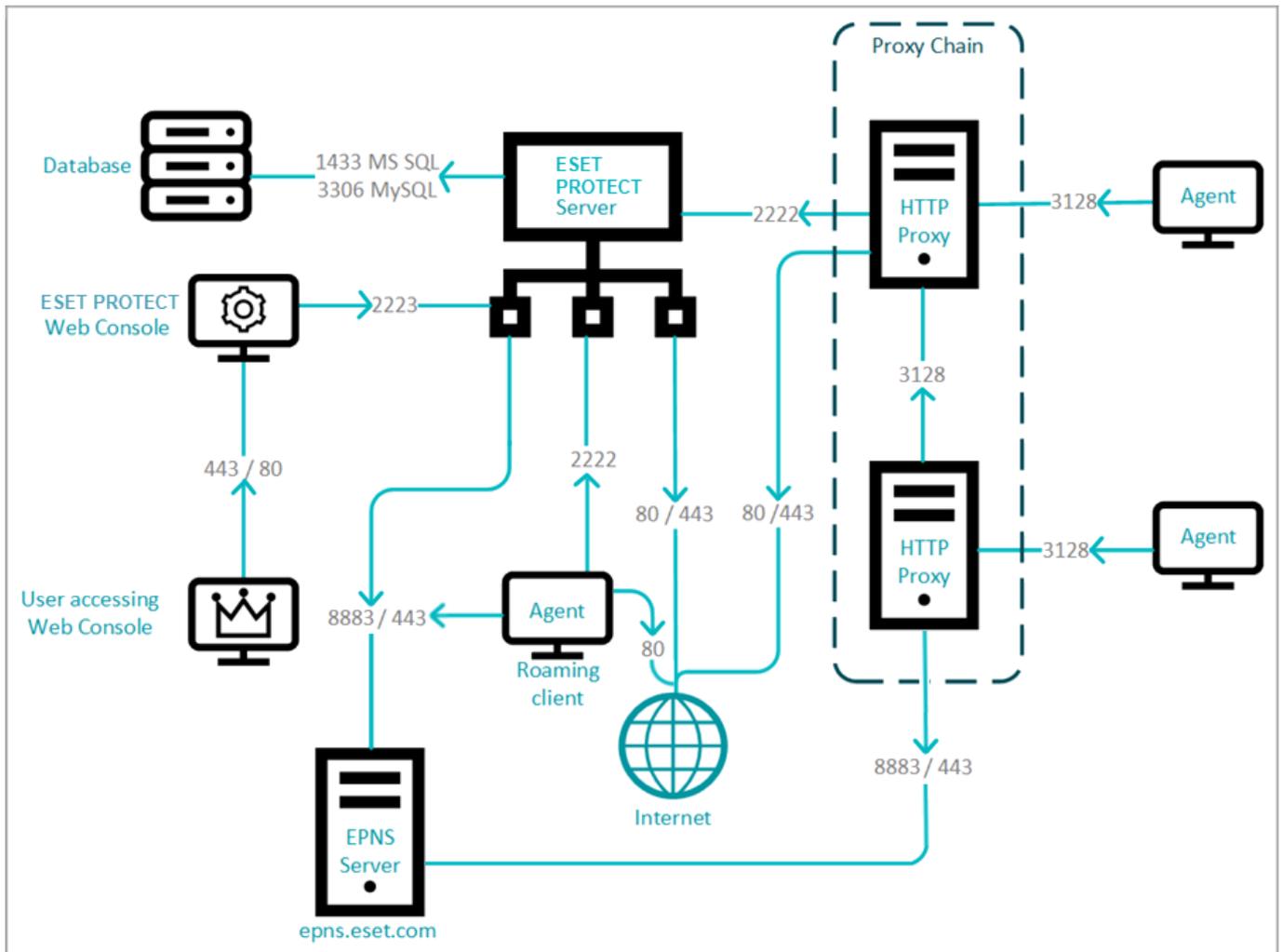
Mit der folgenden Formel können Sie den von den ESET Management Agenten verursachten Datenverkehr abschätzen:

*Anzahl der Clients * (Täglicher Datenverkehr eines ERA Agenten im Leerlauf + (Datenverkehr für einen bestimmten Task * Tägliche Ausführungen des Tasks))*

Wenn Sie ESET Inspect verwenden, generiert der ESET Inspect Connector einen täglichen Datenverkehr von 2-5 MB (je nach Anzahl der Ereignisse).

Verwendete Ports

Der ESET PROTECT Server kann auf demselben Computer wie Datenbank, ESET PROTECT-Web-Konsole und Apache HTTP Proxy installiert werden. Das folgende Diagramm zeigt die separate Installationen und die verwendeten Ports (Pfeile symbolisieren den Netzwerkverkehr):



Die folgenden Tabellen enthalten eine Liste aller verwendeten Netzwerkkommunikationsports, wenn Sie ESET PROTECT und die Komponenten in Ihrer Infrastruktur installieren. Die sonstige Kommunikation erfolgt über die nativen Prozesse des Betriebssystems (zum Beispiel NetBIOS über TCP/IP).

! Für eine ordnungsgemäße Funktionsweise von ESET PROTECT darf keiner der oben genannten Ports von anderen Anwendungen verwendet werden. Vergewissern Sie sich, dass die Firewalls in Ihrem Netzwerk die Kommunikation über die unten genannten Ports zulassen.

Client (ESET Management Agent) oder Apache HTTP Proxy-Computer

Protokoll	Port	Beschreibung
TCP	2222	Kommunikation zwischen ESET Management Agenten und ESET PROTECT Server
TCP	80	Verbindung zum ESET-Repository
MQTT	8883, 443	ESET Push Notification Service – Aktivierungsaufrufe zwischen ESET PROTECT Server und ESET Management Agent, 443 wird als Failover-Port verwendet.
TCP	3128	Kommunikation mit Apache HTTP Proxy
TCP	443	Kommunikation mit ESET LiveGuard Advanced (nur Proxy)

ESET Management Agent – Ports für die Remote-Bereitstellung auf einem Zielcomputer mit

Windows-Betriebssystem

Protokoll	Port	Beschreibung
TCP	139	Verwenden der Freigabe ADMIN\$
TCP	445	Direktzugriff auf freigegebene Ressourcen mit TCP/IP während der Remote-Installation (Alternative zu TCP 139)
UDP	137	Namensauflösung während der Remote-Installation
UDP	138	Durchsuchen während der Remote-Installation

Computer mit ESET PROTECT-Web-Konsole (falls nicht identisch mit dem ESET PROTECT Server-Computer)

Protokoll	Port	Beschreibung
TCP	2223	Kommunikation zwischen ESET PROTECT-Web-Konsole und ESET PROTECT Server für die unterstützte Installation.
TCP	443/80	Tomcat, der die Web-Konsole bereitstellt.
TCP	443	RSS-Feed für Support-News: <ul style="list-style-type: none">• https://era.welivesecurity.com:443• https://support.eset.com:443/rss/news.xml

ESET PROTECT Server-Computer

Protokoll	Port	Beschreibung
TCP	2222	Kommunikation zwischen ESET Management Agent und ESET PROTECT Server
TCP	80	Verbindung zum ESET-Repository
MQTT	8883	ESET Push Notification Service – Aktivierungsaufrufe zwischen ESET PROTECT Server und ESET Management Agent
TCP	2223	DNS-Auflösung und MQTT-Fallback
TCP	3128	Kommunikation mit Apache HTTP Proxy
TCP	1433 (MS SQL) 3306 (MySQL)	Verbindung mit einer externen Datenbank (nur falls sich die Datenbank auf einem anderen Computer befindet).
TCP	389	LDAP-Synchronisierung. Öffnen Sie diesen Port ebenfalls auf Ihrem AD-Controller.
UDP	88	Kerberos-Tickets (gilt nur für die virtuelle ESET PROTECT-Appliance)

Rogue Detection-Sensor (RD)

Protokoll	Port	Beschreibung
TCP	22, 139	Betriebssystemerkennung mit den Protokollen SMB (TCP 139) und SSH (TCP 22).
UDP	137	Auflösung von Computer-Hostnamen mit NetBIOS.

ESET PROTECT MDC-Computer

Protokoll	Port	Beschreibung
TCP	9977 9978	Interne Kommunikation zwischen Mobile Device Connector und ESET Management Agent
TCP	9980	Mobilgeräteregistrierung
TCP	9981	Kommunikation mit Mobilgeräten
TCP	2195	Versand von Benachrichtigungen an den Apple Push Notification Service. (<i>gateway.push.apple.com</i>) Bis zu ESMC Version 7.2.11.1
TCP	2196	Apple Feedback Service (<i>feedback.push.apple.com</i>) Bis zu ESMC Version 7.2.11.1
HTTPS	2197	• Apple Push Notification und Feedback (<i>api.push.apple.com</i>) ESMCVersion 7.2.11.3 und höher.
TCP	2222	Kommunikation (Replikation) zwischen ESET Management Agent, MDC und ESET PROTECT Server
TCP	1433 (MS SQL) 3306 (MySQL)	Verbindung mit einer externen Datenbank (nur falls sich die Datenbank auf einem anderen Computer befindet)

Mit MDM verwaltetes Gerät

Protokoll	Port	Beschreibung
TCP	9980	Mobilgeräteregistrierung
TCP	9981	Kommunikation mit Mobilgeräten
TCP	5223	Externe Kommunikation mit Apple Push Notification Service (iOS)
TCP	443	<ul style="list-style-type: none"> • WLAN-Fallback, falls die Geräte keinen APN auf Port 5223 erreichen können. • Verbindung zwischen Android-Gerät und GCM Server. • Verbindung zum ESET-Lizenzierungsportal. • ESET LiveGrid® (Android) (eingehend: https://i1.c.eset.com; ausgehend: https://i3.c.eset.com) • Anonyme statistische Daten für das ESET Research Lab (Android) (https://ts.eset.com) • App-Kategorisierung auf dem Gerät installiert. Wird für die Anwendungskontrolle verwendet, wenn bestimmte App-Kategorien gesperrt sind. (Android) (https://play.eset.com) • Senden von Supportanfragen mit der Funktion „Supportanfrage“ (Android) (https://suppreq.eset.eu)
TCP	5228 5229 5230	Versenden von Benachrichtigungen an Google Cloud Messaging (Android)* Versenden von Benachrichtigungen an Firebase Cloud Messaging (Android)*
TCP	80	<ul style="list-style-type: none"> • Modul-Update (Android) (http://update.eset.com) • Wird nur in der Web-Version verwendet. Update-Info für die neueste App-Version und Download neuer Versionen. (Android) (http://go.eset.eu)

* Der GCM-Dienst (Google Cloud Messaging) ist veraltet und wurde am 11. April 2019 entfernt. Er wurde durch FCM (Firebase Cloud Messaging) ersetzt. MDM v7 hat den GCM-Dienst durch den FCM-Dienst ersetzt, und Sie müssen nur noch die Kommunikation für den FCM-Dienst zulassen.

Die vordefinierten Ports 2222 und 2223 können bei Bedarf geändert werden.

Installationsprozess

Die Installationsanleitung beschreibt verschiedene Methoden für die Installation von ESET PROTECT und richtet sich hauptsächlich an Unternehmenskunden. Lesen Sie die [Anleitung für kleine und mittelgroße Unternehmen](#), falls Sie ESET PROTECT auf einer Windows-Plattform für bis zu 250 Windows ESET-Endpunktprodukte installieren möchten. Hinweise zum Upgrade Ihrer vorhandenen ESET PROTECT-Installation finden Sie unter [Upgradeprozeduren](#).

Die ESET PROTECT-Installationsprogramme stehen im Bereich [ESET PROTECT herunterladen](#) auf der ESET-Webseite zur Verfügung. Es stehen verschiedene Formate für verschiedene Installationsverfahren zur Verfügung. Standardmäßig ist die Registerkarte **All-in-One-Installationsprogramm** ausgewählt. Klicken Sie auf die entsprechende Registerkarte, um ein VA- oder ein Standalone-Installationsprogramm herunterzuladen. Folgende Downloads stehen zur Verfügung:

- Das ESET PROTECT [All-in-One-Installationsprogramm](#) für Windows liegt im ZIP-Format vor.
- Ein ISO-Abbild mit allen ESET PROTECT-Installationsprogrammen (mit Ausnahme der virtuellen ESET PROTECT-Appliances).
- Virtuelle Appliances (OVA-Dateien). Die virtuelle ESET PROTECT-Appliance eignet sich für Benutzer, die ESET PROTECT in einer virtualisierten Umgebung ausführen möchten oder eine einfachere Installation bevorzugen. Unsere [Bereitstellungsanleitung für die virtuelle ESET PROTECT-Appliance](#) enthält eine ausführliche Beschreibung.
- Separate Installationsprogramme für jede Komponente - für [Windows](#)- und [Linux](#)-Plattformen.

Weitere Installationsmethoden:

- [Installation in Microsoft Azure](#)
- Schritt-für-Schritt-[Installation unter Linux](#)

Nach der Installation dürfen Sie den Computernamen Ihres ESET PROTECT Servers nicht mehr ändern. Weitere Informationen finden Sie unter [Neue IP-Adresse oder neuer Hostname für den ESET PROTECT Server](#).

Die folgende Tabelle hilft Ihnen bei der Auswahl einer optimalen ESET PROTECT-Installation für Ihre Umgebung. Beispiel:

- Verwenden Sie ESET PROTECT in der Cloud nicht mit einer langsamen Internetverbindung.
- SMB-Kunden sollten das All-in-One-Installationsprogramm auswählen.

Siehe auch [Größenbemessung für Hardware und Infrastruktur](#).

Installationsmethoden	Kundentyp		Migration		Umgebung für ESET PROTECT-Installation					Internetverbindung		
	SMB	Unternehmen	Ja	Nein	Kein Server	Dedizierter Server	Gemeinsam genutzter Server	Virtualisierte Plattform	Cloudserver	Keine	Gut	Schlecht
All-in-One für Windows Server	✓	✓	✓			✓	✓		✓	✓	✓	✓
All-in-One für Windows (Desktops)	✓		✓		✓					✓	✓	✓
Virtuelle Appliance	✓		✓					✓		✓	✓	✓
Microsoft Azure-VM	✓			✓					✓		✓	
Komponente Linux		✓	✓			✓	✓		✓	✓	✓	✓
Komponente Windows		✓	✓			✓	✓		✓	✓	✓	✓

All-in-One-Installation unter Windows

Sie können ESET PROTECT auf verschiedene Arten installieren. Wählen Sie die Installationsart aus, die sich am besten für Ihre Anforderungen und Ihre Umgebung eignet. Die einfachste Methode ist die Verwendung des ESET PROTECT-Installationspakets (All-in-One-Installation). Mit dieser Methode können Sie ESET PROTECT und alle Komponenten auf einem einzigen Computer installieren.

Bei der Komponenteninstallation können Sie die Installation anpassen und jede ESET PROTECT-Komponente auf einem separaten Computer installieren, sofern die Systemanforderungen erfüllt sind.

Sie können ESET PROTECT auf die folgenden Arten installieren:

- All-in-One-Paketinstallation für [ESET PROTECT Server](#), [Apache HTTP Proxy](#) oder [Mobile Device Connector](#)
- [Standalone-Installationsprogramme](#) für ESET PROTECT Komponenten (Komponenteninstallation)

Die folgenden benutzerdefinierten Installationsszenarien sind möglich:

- Installation mit [benutzerdefinierten Zertifikaten](#)
- Installation auf einem [Failover-Cluster](#)

In vielen Installationsszenarien müssen Sie verschiedene ESET PROTECT-Komponenten auf verschiedenen Computern installieren, z. B. um Unterschiede in der Netzwerkarchitektur zu berücksichtigen oder Leistungsanforderungen zu erfüllen. Für einzelne ESET PROTECT-Komponenten sind die folgenden Installationspakete verfügbar:

Kernkomponenteninstallation

- [ESET PROTECT Server](#)
- [ESET PROTECT-Web-Konsole](#) – Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server.
- [ESET Management Agent](#) (muss auf Clientcomputern installiert sein, optional auf dem ESET PROTECT Server)

Installation optionaler Komponenten

- [RD Sensor](#)
- [Mobile Device Connector](#)

- [Apache HTTP Proxy](#)
- [Mirror-Tool](#)

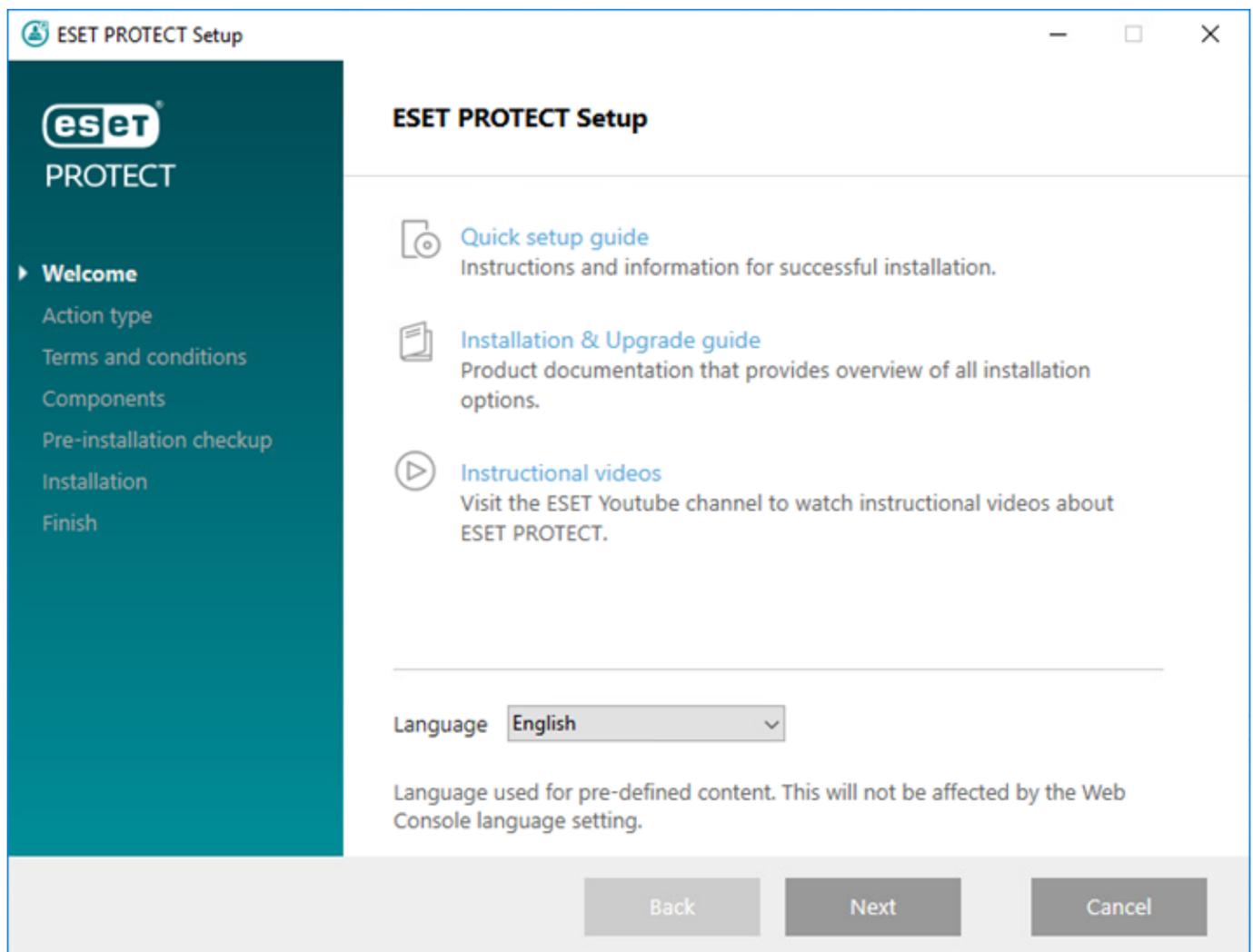
Siehe auch [ESET PROTECT All-in-One-Installation](#).

Hinweise zum Upgrade von ESMC auf die neueste Version ESET PROTECT 9.1 finden Sie in unseren [Upgradeprozeduren](#).

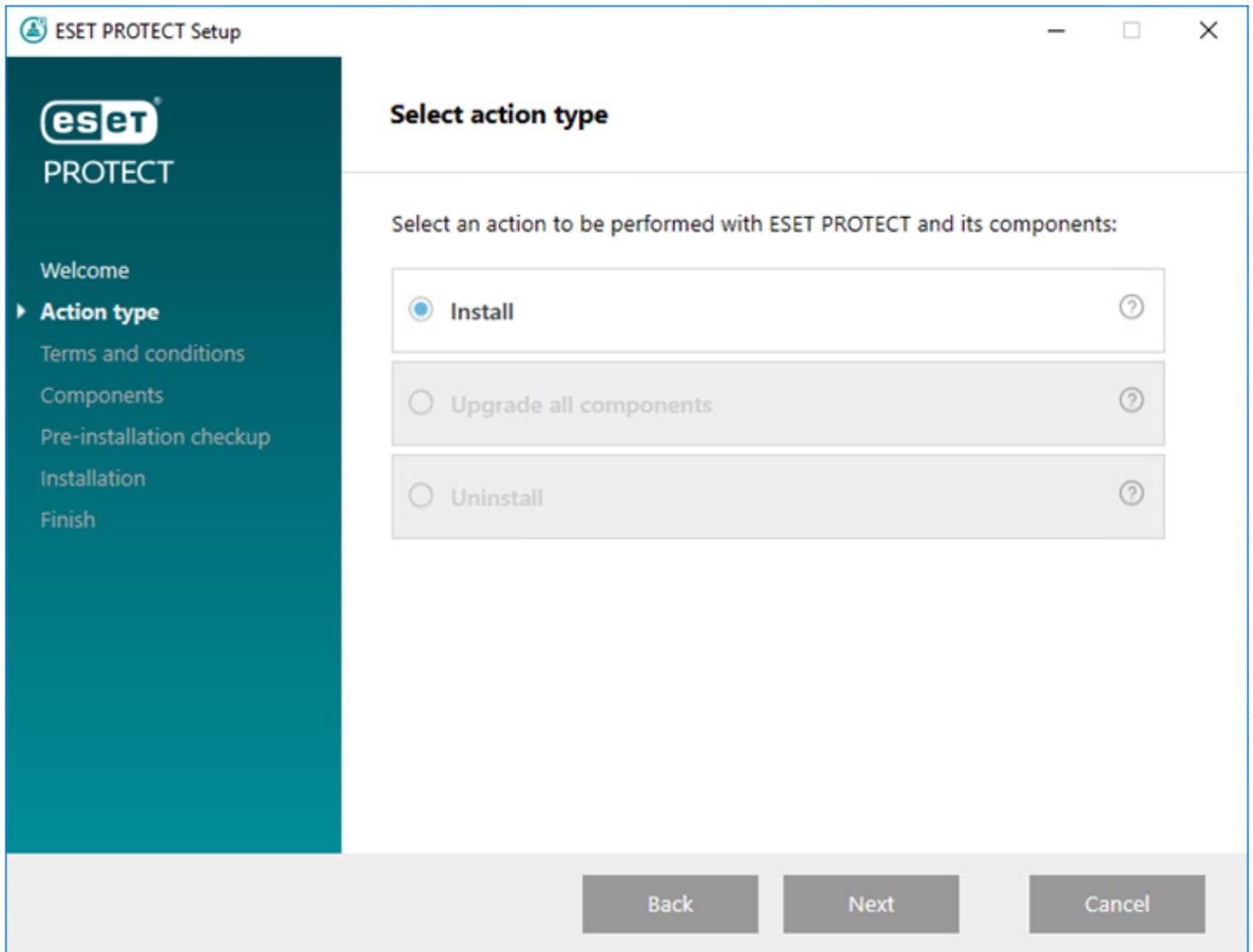
Installieren des ESET PROTECT Servers

Das [ESET PROTECT-All-in-One-Installationsprogramm](#) ist nur für Windows-Betriebssysteme verfügbar. Mit dem All-in-One-Installationsprogramm können Sie sämtliche ESET PROTECT-Komponenten mit dem ESET PROTECT-Installationsassistenten installieren.

1. Öffnen Sie das Installationspaket. Im Willkommensbildschirm können Sie die Spracheinstellungen im Dropdownmenü **Sprache** anpassen. Klicken Sie auf **Weiter**, um fortzufahren.



2. Wählen Sie **Installieren** aus und klicken Sie auf **Weiter**.



3. Deaktivieren Sie das Kontrollkästchen neben **Am Produktverbesserungsprogramm teilnehmen**, falls Sie der Übertragung von Absturzberichten und anonymen Telemetriedaten (Betriebssystemversion und -Typ, ESET-Produktversion und andere produktspezifische Daten) an ESET nicht zustimmen. Wenn Sie dieses Kontrollkästchen aktiviert lassen, werden Telemetriedaten und Absturzberichte an ESET übertragen. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.

4. Wählen Sie die gewünschten Komponenten für die Installation aus und klicken Sie auf **Weiter**.

[Microsoft SQL Server Express](#)

- ESET PROTECT 9.1 [All-in-One-Installationsprogramm](#) installiert standardmäßig Microsoft SQL Server Express 2019.

o Falls Sie eine ältere Windows Edition verwenden (Server 2012 oder SBS 2011), wird standardmäßig Microsoft SQL Server Express 2014 installiert.

o Das Installationsprogramm generiert automatisch ein zufälliges Passwort für die Datenbankauthentifizierung (gespeichert in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`).

Microsoft SQL Server Express Hat eine Obergrenze von je 10 GB für relationale Datenbanken. Microsoft SQL Server Express sollte nicht verwendet werden:



- In Unternehmensumgebungen oder großen Netzwerken.
- Falls Sie ESET PROTECT mit [ESET Inspect](#) verwenden möchten.

• Falls Sie bereits eine andere [unterstützte Version](#) von Microsoft SQL Server oder MySQL installiert haben oder vorhaben, sich mit einem anderen SQL Server zu verbinden, deaktivieren Sie das Kontrollkästchen neben **Microsoft SQL Server Express**.

• [Installieren Sie SQL Server sollte nicht auf einem Domänencontroller](#) (z. B. Windows SBS oder Essentials). Sollten Sie ESET PROTECT auf einem anderen Server installieren oder während der Installation nicht die SQL Server Express-Komponente auswählen (in diesem Fall müssen Sie SQL Server oder MySQL als ESET PROTECT-Datenbank verwenden).

[Benutzerdefiniertes HTTPS-Zertifikat für Web-Konsole hinzufügen](#)

- Wählen Sie diese Option aus, wenn Sie ein benutzerdefiniertes HTTPS-Zertifikat für die ESET PROTECT-Web-Konsole verwenden möchten.
- Wenn Sie diese Option nicht auswählen, generiert das Installationsprogramm automatisch einen neuen Tomcat-Schlüsselspeicher (ein selbstsigniertes HTTPS-Zertifikat).

[Apache HTTP-Proxy](#)

Die Option **Apache HTTP Proxy** eignet sich nur für kleinere oder zentralisierte Netzwerke ohne Roaming-Clients. Wenn Sie diese Option auswählen, konfiguriert das Installationsprogramm einen Tunnel für die Kommunikation zwischen Clients und ESET über einen Proxy, der auf demselben Computer installiert ist wie der ESET PROTECT Server. Diese Verbindung funktioniert nur, wenn der ESET PROTECT Server für die Clients im Netzwerk direkt sichtbar ist.

- Mit einem HTTP-Proxy können Sie die Bandbreitennutzung für Downloads aus dem Internet und die Downloadgeschwindigkeiten für Produktupdates drastisch verbessern. Daher sollten Sie das Kontrollkästchen neben **Apache HTTP Proxy** aktivieren, wenn Sie mehr als 37 Computer mit ESET PROTECT verwalten. Optional können Sie den [Apache HTTP Proxy auch später installieren](#).
- Weitere Informationen finden Sie unter [Apache HTTP Proxy: Beschreibung](#) und [Unterschiede zwischen Apache HTTP Proxy, Mirror-Tool und Direktverbindung](#).
- Wählen Sie **Apache HTTP Proxy** aus, um den Apache HTTP Proxy zu installieren und Policies (mit dem Namen **HTTP Proxy-Nutzung**, angewendet auf die Gruppe **Alle**) für die folgenden Produkte zu erstellen und anzuwenden:

OESET Endpoint für Windows

OESET Endpoint für macOS (OS X) und Linux

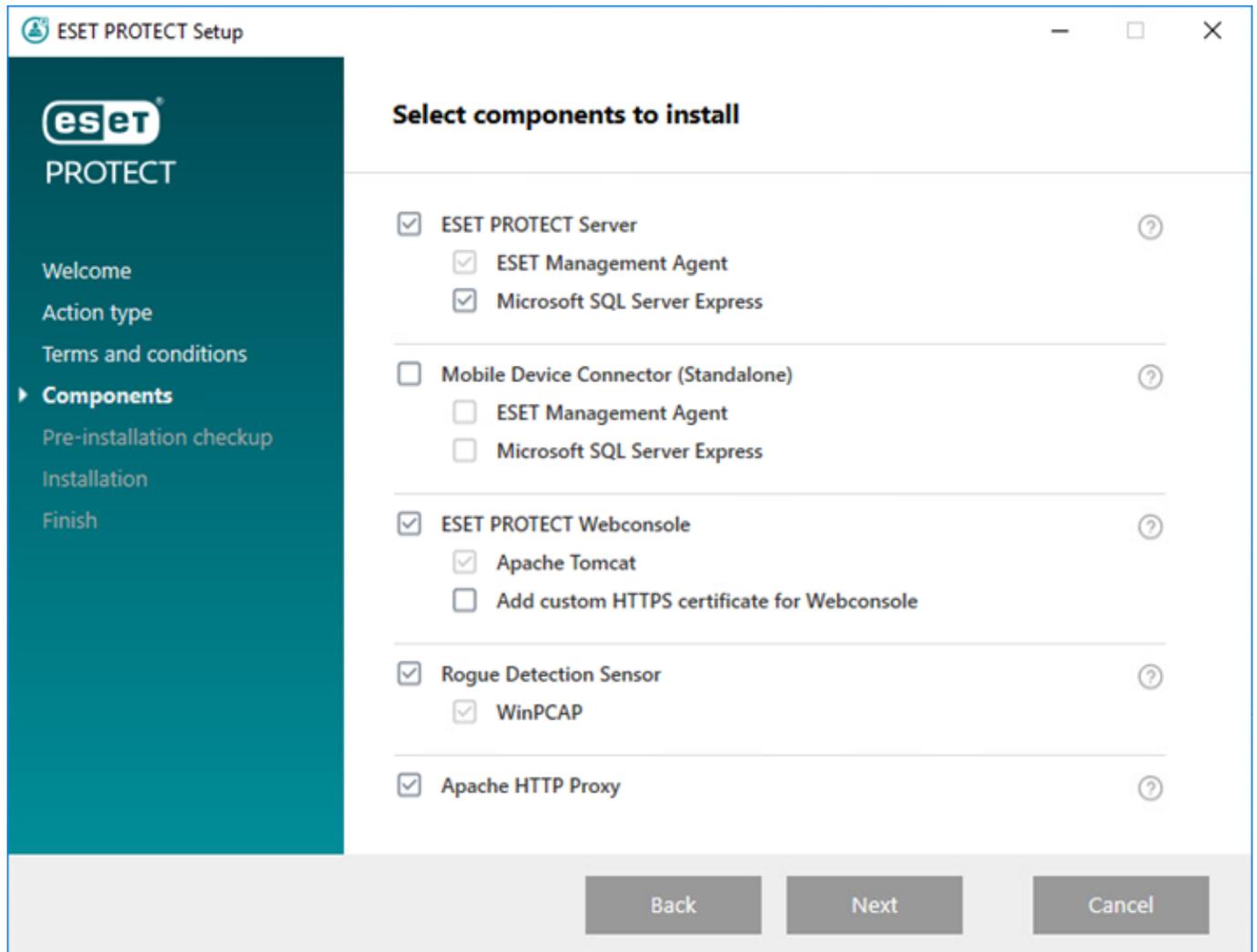
OESET Management Agent

OESET File Security für Windows Server (6+)

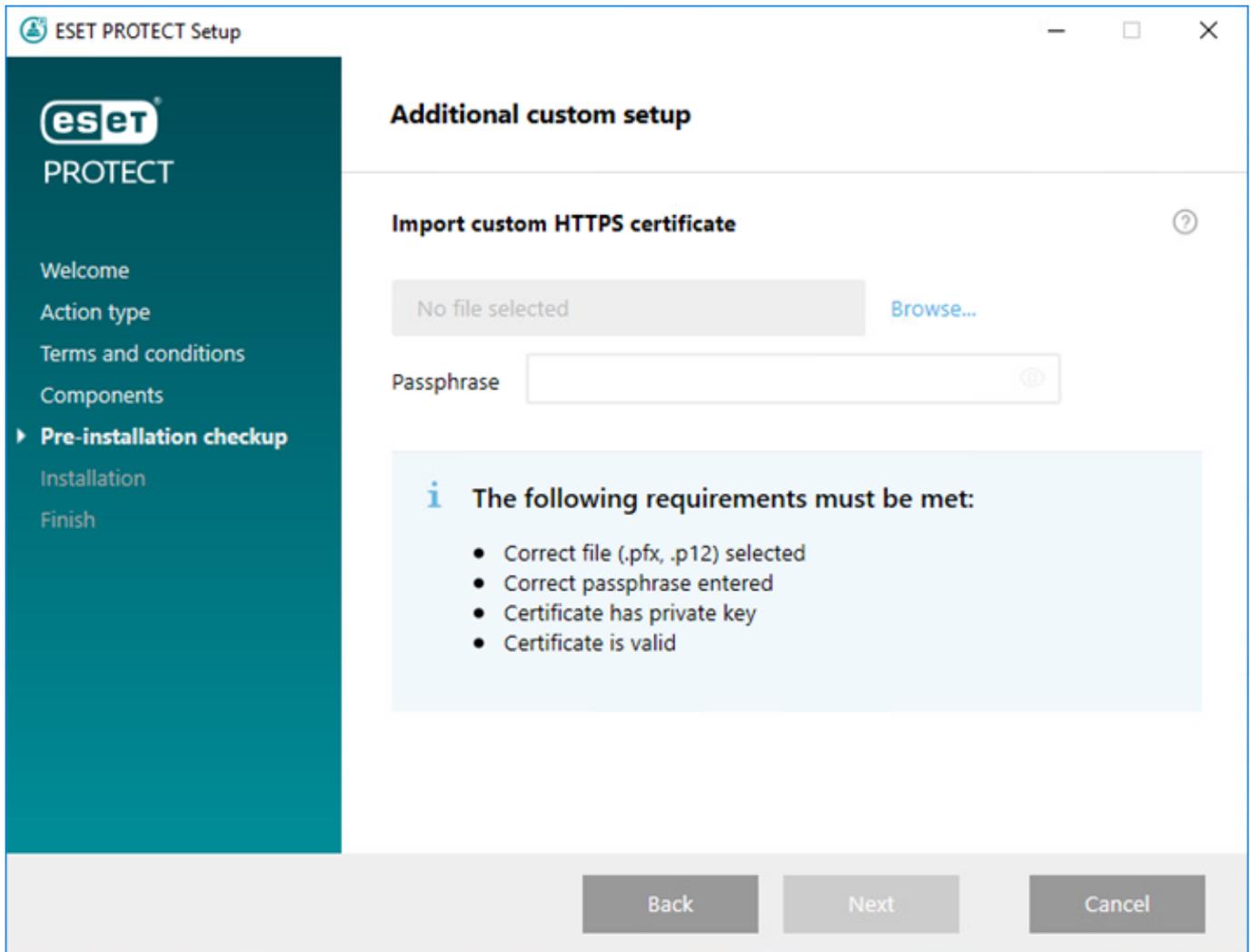
oESET Server Security für Windows (8+)

oESET Shared Local Cache

Die Policy aktiviert den HTTP-Proxy für die jeweiligen Produkte. Als HTTP-Proxyhost wird die lokale IP-Adresse des ESET PROTECT Servers und der Port 3128 konfiguriert. Authentifizierung ist deaktiviert. Sie können diese Einstellungen in andere Policies kopieren, falls Sie weitere Produkte einrichten möchten.



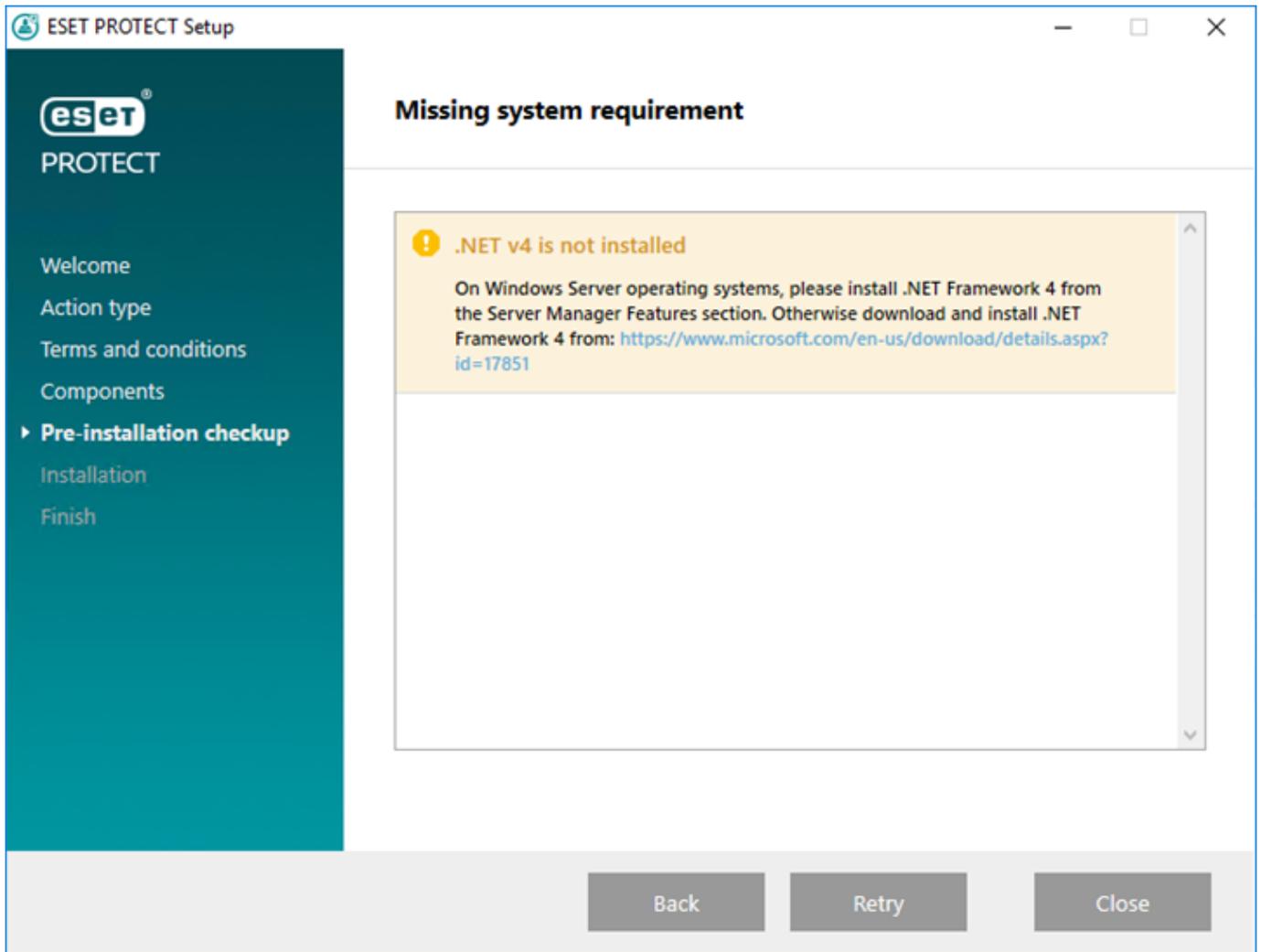
5. Falls Sie **Benutzerdefiniertes HTTPS-Zertifikat für Web-Konsole hinzufügen** ausgewählt haben, klicken Sie auf **Durchsuchen** und wählen Sie ein gültiges Zertifikat aus (.pfx- oder .p12-Datei) und geben Sie die **Passphrase** für das Zertifikat ein (bzw. lassen Sie das Feld leer, falls keine Passphrase festgelegt ist). Das Installationsprogramm installiert das Zertifikat für den Zugriff auf die Web-Konsole auf Ihrem Tomcat-Server. Klicken Sie auf **Weiter**, um fortzufahren.



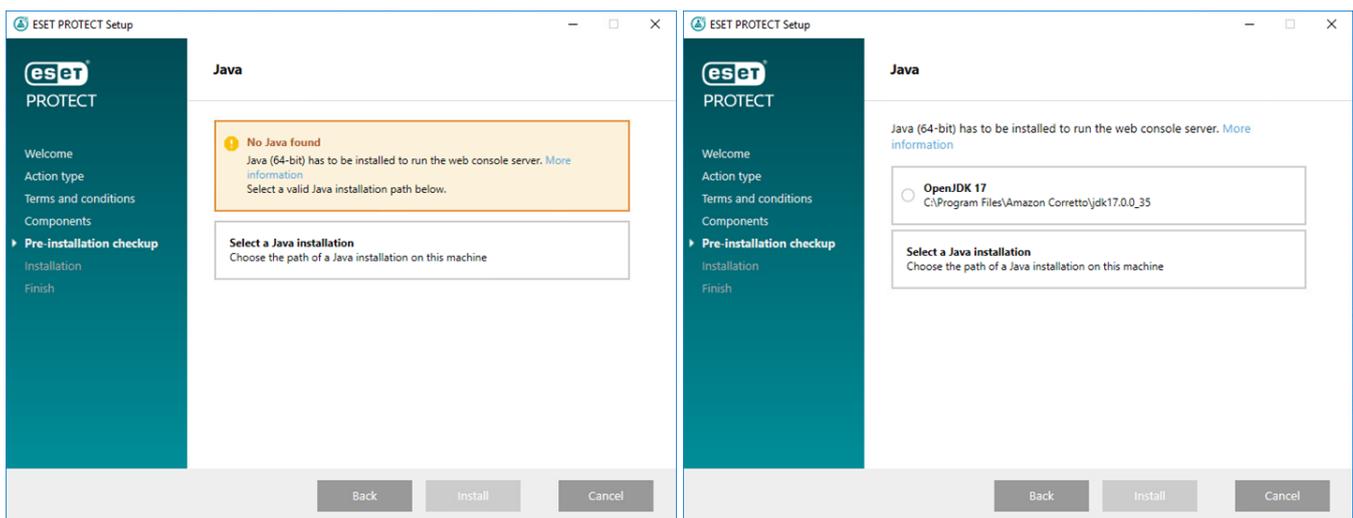
6. Wenn bei der Prüfung der Voraussetzungen Fehler gefunden werden, beheben Sie diese entsprechend. Vergewissern Sie sich, dass Ihr System alle [Voraussetzungen](#) erfüllt.

[^ .NET v4 ist nicht installiert](#)

[.NET Framework installieren](#)



Kein Java gefunden / Java (64-Bit) gefunden



Falls Sie mehrere Java-Versionen auf Ihrem System installiert haben, empfehlen wir, die älteren Java-Versionen zu deinstallieren und nur die neueste [unterstützte Java](#)-Version zu behalten.



Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).

a) Um die bereits installierte Java-Version auszuwählen, klicken Sie auf **Java-Installation auswählen**, wählen Sie den Java-Installationsordner aus (mit *bin*-Unterordner, zum Beispiel *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) und klicken Sie auf **OK**. Falls Sie einen ungültigen Pfad ausgewählt haben, wird ein Hinweis angezeigt.

b) Klicken Sie auf **Installieren**, um fortzufahren, oder auf **Ändern**, um den Java-Installationspfad zu ändern.

 [Es ist nur 32 MB freier Speicher auf dem Systemdatenträger verfügbar.](#)

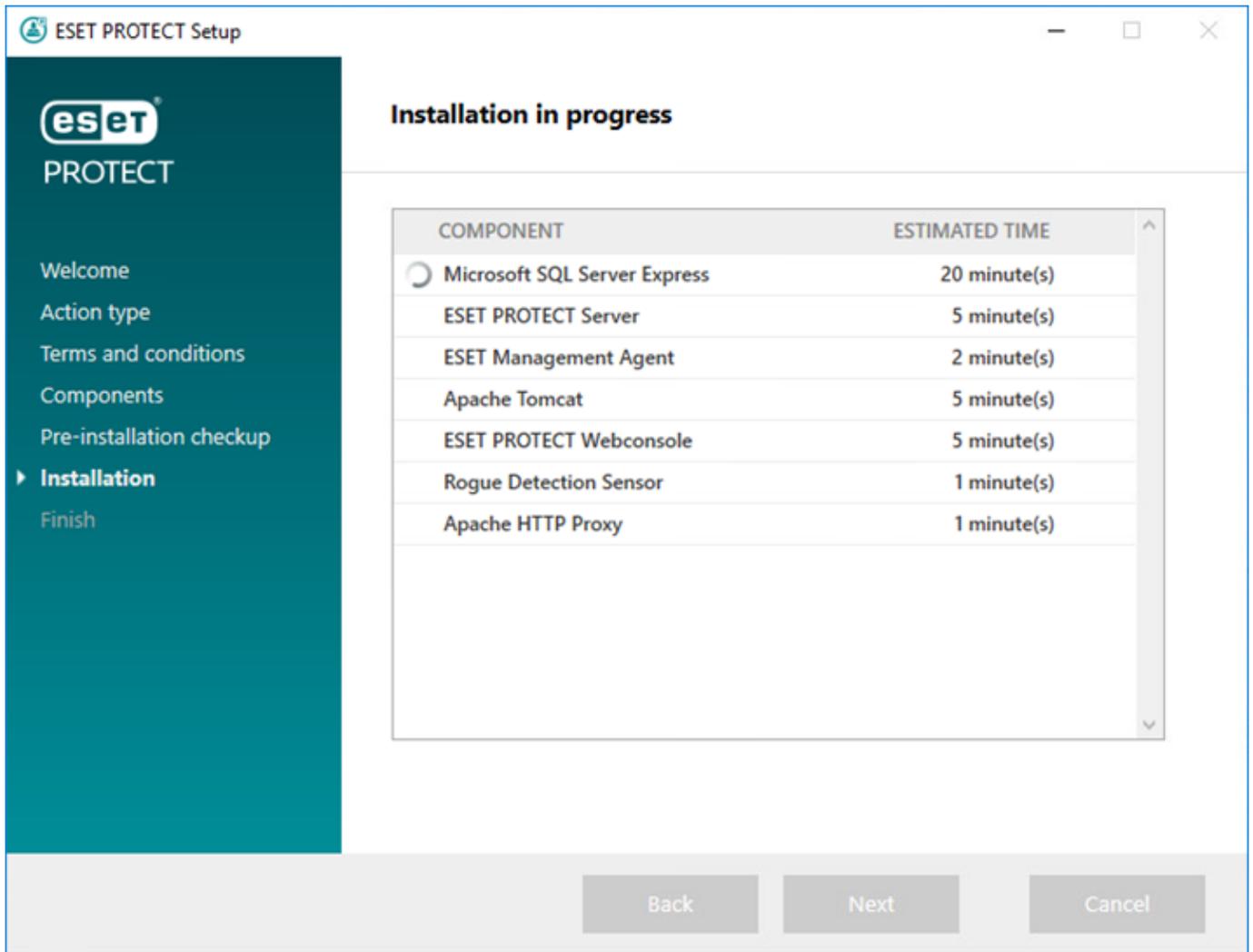
- Das Installationsprogramm kann diese Benachrichtigung anzeigen, wenn auf Ihrem System nicht genügend Speicherplatz für die Installation von ESET PROTECT vorhanden ist.
- Sie benötigen mindestens 4.400 MB freien Platz auf Ihrem Laufwerk, um ESET PROTECT mit sämtlichen Komponenten zu installieren.

 [ESET Remote Administrator 5.x oder eine frühere Version ist auf dem Computer installiert.](#)

Direkt-Upgrades werden nicht unterstützt, siehe [Migration von ERA 5.x](#) oder [Upgrade von ERA 6.x](#).

7. Wenn die Prüfung der Voraussetzungen abgeschlossen ist und Ihre Umgebung alle [Anforderungen](#) erfüllt, beginnt die Installation. Beachten Sie, dass die Installation je nach System und Netzwerkkonfiguration über eine Stunde dauern kann.

 Der ESET PROTECT-Installationsassistent reagiert nicht, während die Installation ausgeführt wird.



8. Falls Sie **Microsoft SQL Server Express** in Schritt 4 installiert haben, führt das Installationsprogramm eine Datenbankverbindungsprüfung durch. Falls Sie einen vorhandenen Datenbankserver verwenden, werden Sie vom Installationsprogramm aufgefordert, Ihre Datenbankverbindungsdetails einzugeben:

[Konfigurieren der Verbindung zum SQL/MySQL Server](#)

ESET PROTECT Server Setup

Database server connection
Please enter database server connection.

Database: MS SQL Server

ODBC driver: MySQL Server
MS SQL Server
MS SQL Server via Windows Authentication

Database name: era_db

Hostname: localhost

Use Named Instance:

Port: 1433

Database account

Username:

Password:

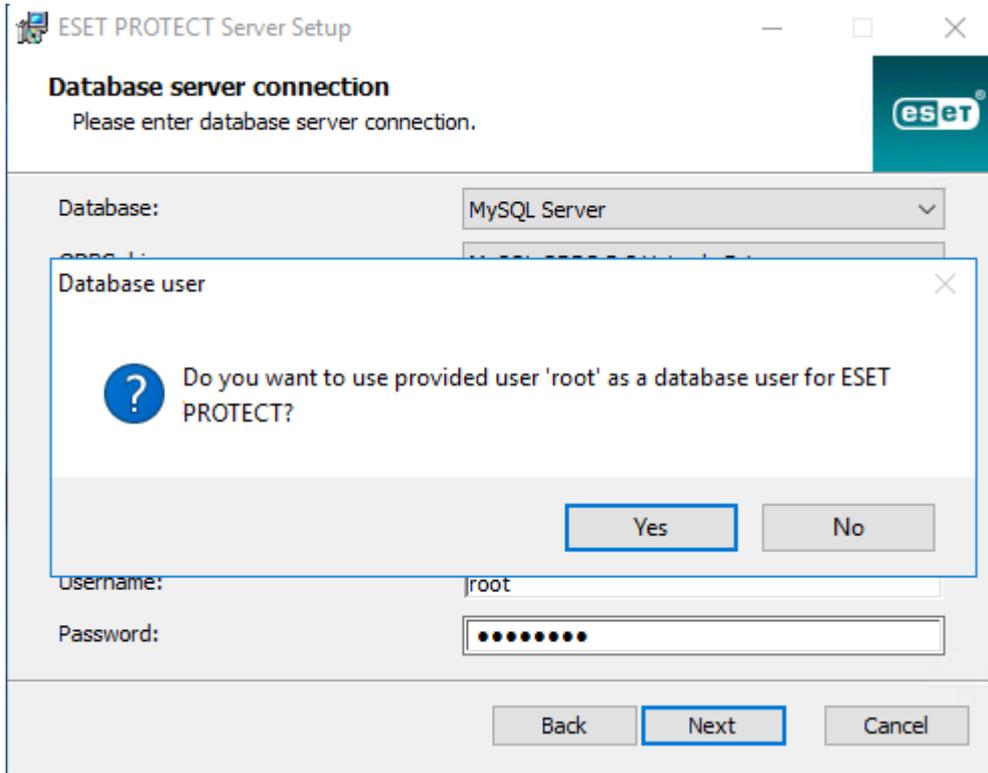
Back Next Cancel

Geben Sie **Datenbankname**, **Hostname**, **Portnummer** (Sie finden diese Informationen im Microsoft SQL Server Konfigurations-Manager) und das **Datenbankkonto (Benutzername und Passwort)** in die entsprechenden Felder ein und klicken Sie auf **Weiter**. Das Installationsprogramm überprüft die Datenbankverbindung. Falls Ihr Datenbankserver eine vorhandene -Datenbank (von einer früheren ESMC/ESET PROTECT-Installation) enthält, wird diese automatisch erkannt. Sie haben zwei Optionen: **Bestehende Datenbank verwenden und Upgrade ausführen** oder **Bestehende Datenbank entfernen und neue Version installieren**.

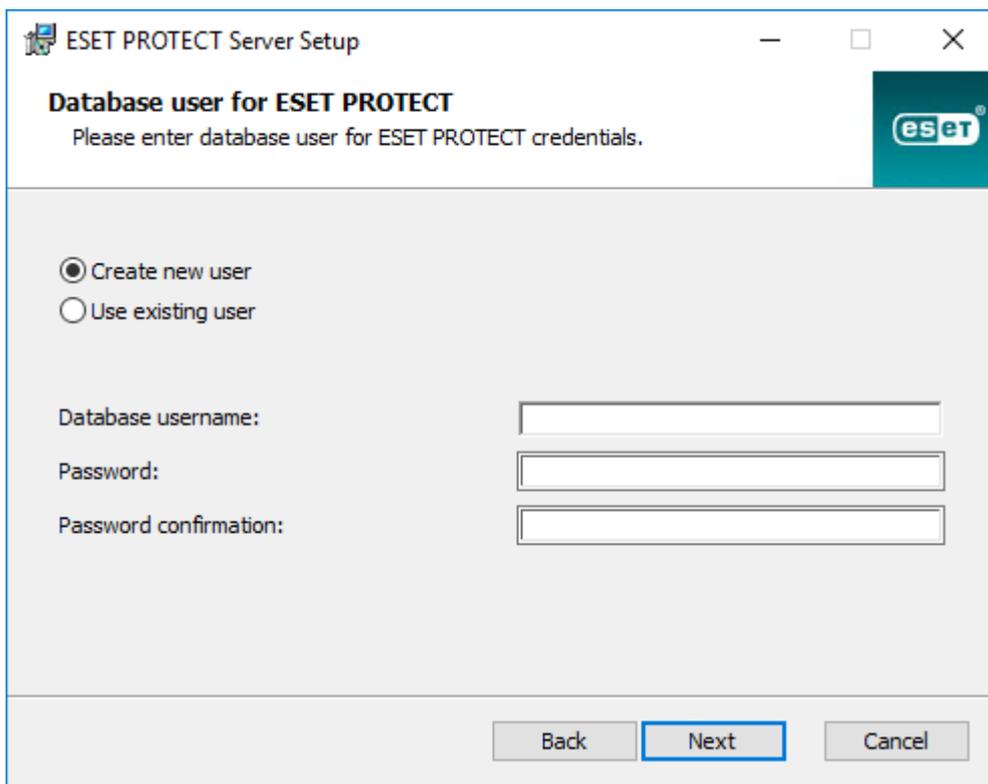
Benannte Instanz verwenden – Falls Sie eine MS SQL-Datenbank verwenden, können Sie auch das Kontrollkästchen **Benannte Instanz verwenden** auswählen, um eine benutzerdefinierte benannte Instanz zu verwenden. Sie können die Instanz im Feld **Hostname** im Format *HOSTNAME\DB_INSTANZ* angeben (zum Beispiel *192.168.0.10\ESMC7SQL*). Geben Sie für geclusterte Datenbanken nur den Clusternamen an. Wenn Sie diese Option auswählen, können Sie den Port für die Datenbankverbindung nicht ändern, und das System verwendet die von Microsoft festgelegten Standardports. Um den ESET PROTECT Server mit einer MS SQL-Datenbank in einem Failover-Cluster zu verbinden, geben Sie den Clusternamen in das Feld **Hostname** ein.

i Sie haben zwei Optionen für die Angabe eines **Datenbankkontos**. Sie können ein **speziell eingerichtetes Datenbankkonto** verwenden, das nur Zugriff auf die ESET PROTECT-Datenbank hat, oder das **SA-Konto** (MS SQL) bzw. das **root-Konto** (MySQL). Falls Sie ein speziell eingerichtetes Benutzerkonto verwenden, müssen Sie dieses Konto mit speziellen Berechtigungen erstellen. Weitere Details finden Sie unter [Speziell eingerichtetes Datenbankkonto](#). Falls Sie kein eigenes Benutzerkonto verwenden, geben Sie das Administratorkonto ein (SA bzw. root).

Falls Sie im vorherigen Fenster das **SA-Konto** bzw. das **root-Konto** eingegeben haben, klicken Sie auf **Ja**, um mit dem SA-/root-Benutzer als Datenbankbenutzer für ESET PROTECT fortzufahren.



Wenn Sie auf **Nein** klicken, wählen Sie **Neuen Benutzer erstellen** (falls Sie noch keinen Benutzer erstellt haben) oder **Vorhandenen Benutzer verwenden** (falls Sie bereits ein [Datenbankkonto erstellt haben](#)) aus.



9. Das Installationsprogramm fordert Sie auf, ein Passwort für das Administratorkonto der Web-Konsole einzugeben. Dieses Passwort ist wichtig, da Sie es für die Anmeldung bei der [ESET PROTECT-Web-Konsole](#) benötigen. Klicken Sie auf **Weiter**.

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 confirmation: [Masked]

Agent port: 2222

Console port: 2223

Buttons: Back, Next, Cancel

10. Lassen Sie die Felder unverändert oder geben Sie Ihre Firmeninformationen ein, falls diese in den Details der ESET Management Agent- und ESET PROTECT Server-Zertifikate eingetragen werden sollen. Falls Sie ein Passwort im Feld **Passwort der Zertifizierungsstelle** eingeben, bewahren Sie dieses Passwort unbedingt gut auf. Klicken Sie auf **Weiter**.

ESET PROTECT Server Setup

Certificate information
Please enter common certificate information below.

Organizational unit: [Empty]

Organization: [Empty]

Locality: [Empty]

State / Country: [Empty] [Dropdown]

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

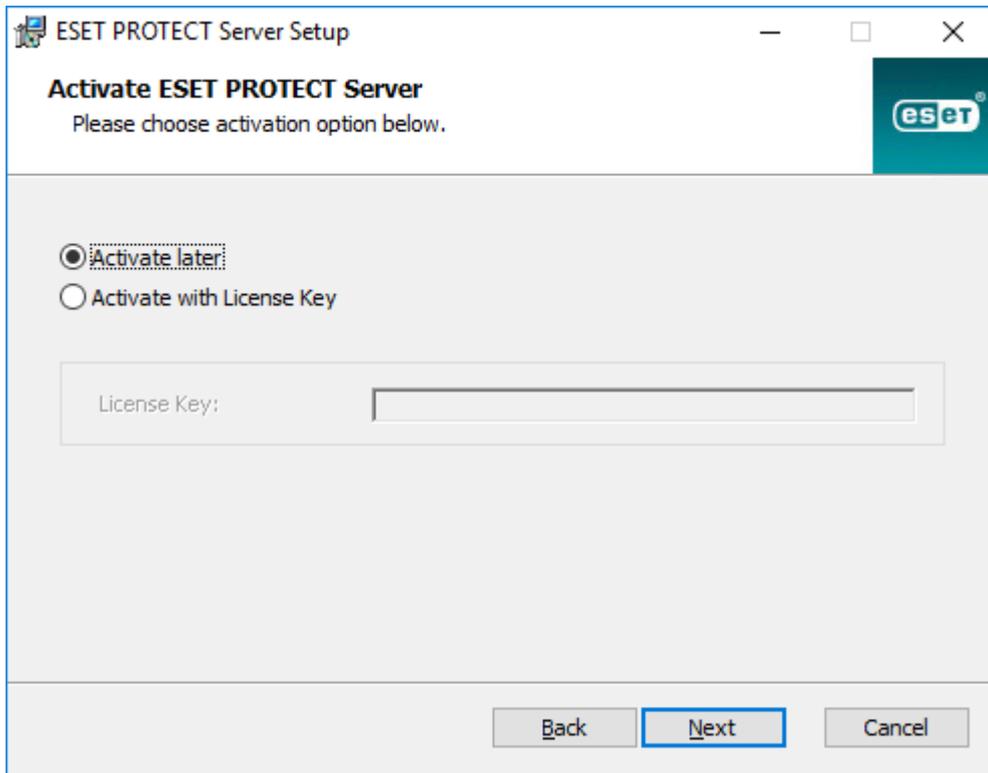
Authority common name: * Server Certification Authority

Authority password: [Empty]

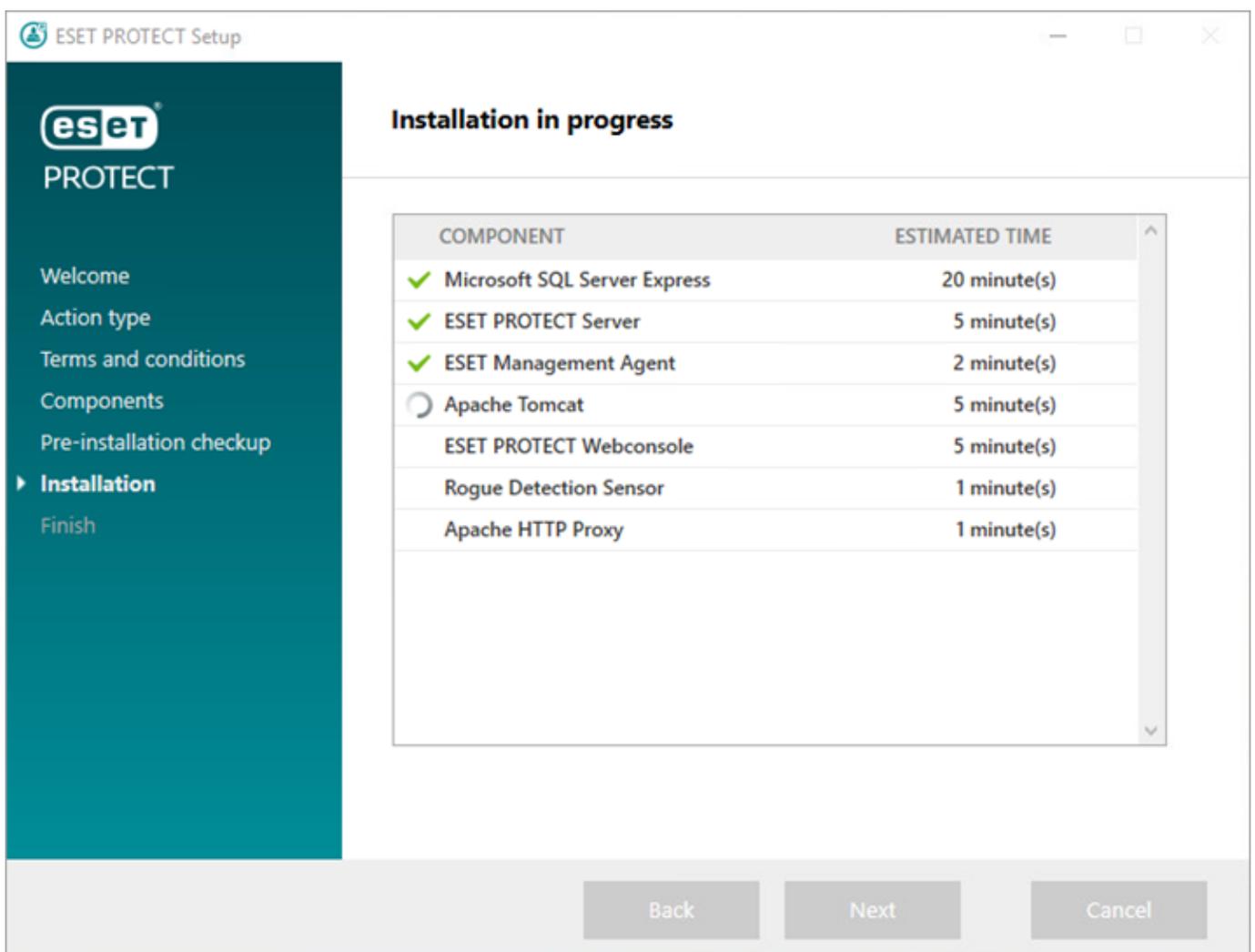
* required fields

Buttons: Back, Next, Cancel

11. Geben Sie einen gültigen **Lizenzschlüssel** (aus der Kaufbestätigungs-E-Mail von ESET) ein und klicken Sie auf **Weiter**. Wenn Sie einen alten Lizenznachweis (Benutzername und Passwort) haben, müssen Sie diese Anmeldedaten in einen Lizenzschlüssel [konvertieren](#). Alternativ können Sie die Option **Später aktivieren** auswählen (weitere Anweisungen finden Sie im Kapitel [Aktivierung](#)).



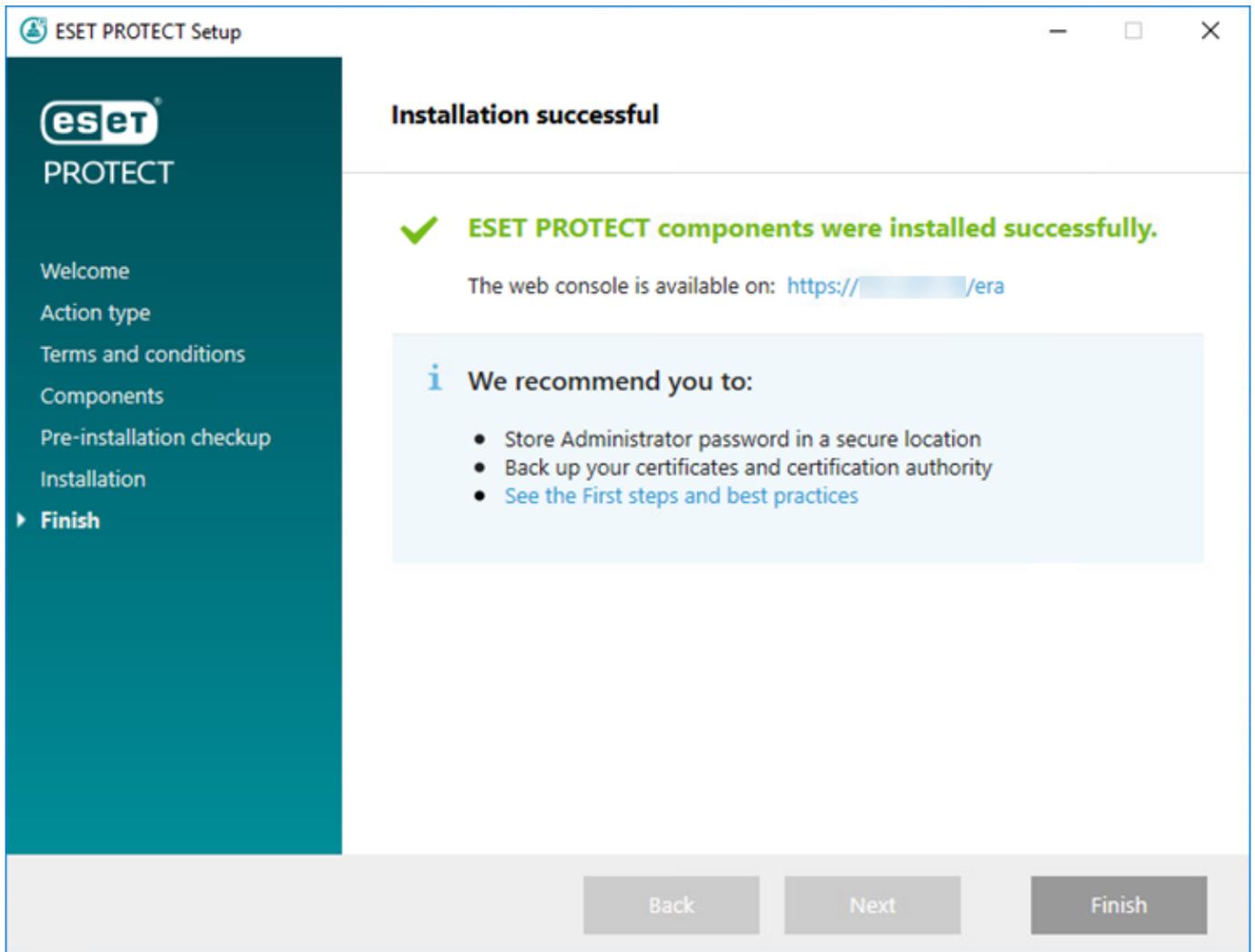
12. Der Installationsfortschritt wird angezeigt.



13. Wenn Sie den **Rogue Detection Sensor** für die Installation ausgewählt haben, wird das Installationsfenster

für den WinPcap-Treiber geöffnet. Aktivieren Sie das Kontrollkästchen **Automatically start the WinPcap driver at boot time** (WinPcap-Treiber beim Systemstart automatisch starten).

14. Nach Abschluss der Installation wird die Meldung „ESET PROTECT-Komponenten wurden erfolgreich installiert“ und die URL-Adresse der ESET PROTECT-Web-Konsole angezeigt. Klicken Sie auf die URL, um die [Web-Konsole](#) zu öffnen, oder klicken Sie auf **Fertig stellen**.



Falls die Installation nicht erfolgreich war:

- Überprüfen Sie die Installationslogs des All-in-One-Installationspakets. Sie finden die Logs im gleichen Verzeichnis wie die Logs des All-in-One-Installationsprogramms, z. B.:
C:\Users\Administrator\Downloads\x64\logs\
- Unter [Fehlerbehebung](#) finden Sie weitere Hinweise zur Behebung Ihres Problems.

Installation des ESET PROTECT Mobile Device Connector (Standalone)

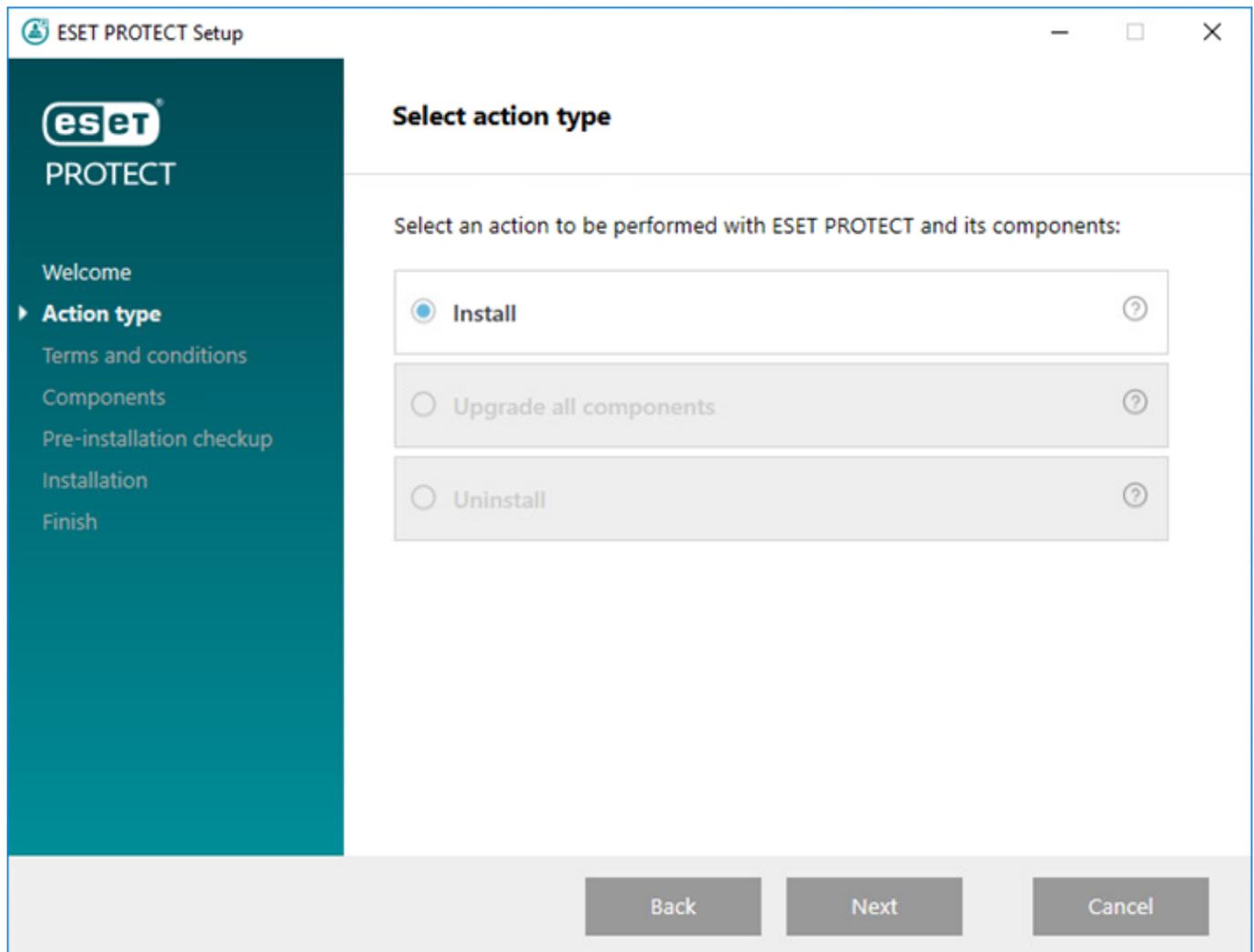
Gehen Sie wie folgt vor, um den Mobile Device Connector als Standalone-Tool auf einem anderen Server als den ESET PROTECT Server zu installieren.

 Der Mobile Device Connector muss jederzeit über das Internet verfügbar sein, um die Mobilgeräte jederzeit und unabhängig von ihrem Standort verwalten zu können.

 Bei der Kommunikation zwischen den Mobilgeräten und dem Mobile Device Connector werden unweigerlich Mobildaten verbraucht. Dies gilt insbesondere im Fall von Datenroaming.

Führen Sie die nachfolgenden Schritte aus, um den Mobile Device Connector unter Windows zu installieren:

1. Lesen Sie die [Voraussetzungen](#) und stellen Sie sicher, dass diese erfüllt sind.
2. Doppelklicken Sie auf das Installationspaket, um es auszuführen, wählen Sie **Installieren** aus und klicken Sie auf **Weiter**.

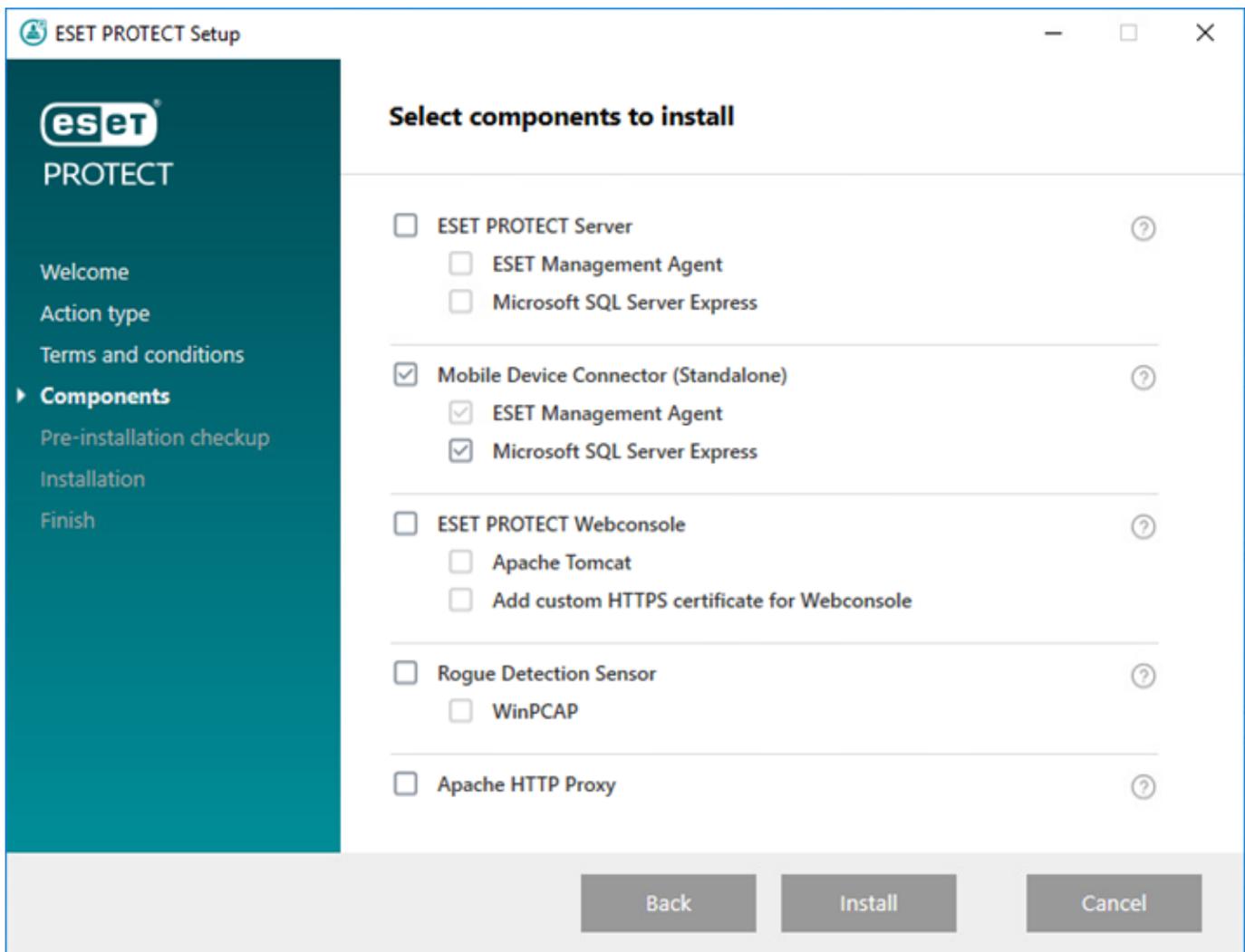


3. Deaktivieren Sie das Kontrollkästchen neben **Am Produktverbesserungsprogramm teilnehmen**, falls Sie der Übertragung von Absturzberichten und anonymen Telemetriedaten (Betriebssystemversion und -Typ, ESET-Produktversion und andere produktspezifische Daten) an ESET nicht zustimmen. Wenn Sie dieses Kontrollkästchen aktiviert lassen, werden Telemetriedaten und Absturzberichte an ESET übertragen.

4. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.

5. Wählen Sie nur das Kontrollkästchen neben **Mobile Device Connector (eigenständig)** aus. Der ESET PROTECT Mobile Device Connector benötigt eine **Datenbank**. Wählen Sie **Microsoft SQL Server Express** aus, falls Sie diese Datenbank installieren möchten, oder lassen Sie das Kontrollkästchen leer. Falls Sie sich mit einer vorhandenen Datenbank verbinden möchten, können Sie dies während der Installation angeben. Klicken

Sie auf **Installieren**, um die Installation fortzusetzen.



6. Wenn Sie die Installation der Datenbank in Schritt 5 installiert haben, wird die Datenbank jetzt automatisch installiert, und Sie können mit Schritt 8 fortfahren. Wenn Sie in Schritt 5 keine Installation der Datenbank ausgewählt haben, werden Sie jetzt aufgefordert, die MDM-Komponente mit Ihrer vorhandenen Datenbank zu verbinden.

i Sie können den gleichen Datenbankserver wie für die ESET PROTECT-Datenbank verwenden. Falls Sie jedoch vorhaben, mehr als 80 Mobilgeräte zu registrieren, sollten Sie nach Möglichkeit einen anderen DB-Server verwenden.

7. Das Installationsprogramm muss sich mit einer vorhandenen Datenbank verbinden, die vom Mobile Device Connector verwendet wird. Geben Sie die folgenden Verbindungsdetails ein:

- **Datenbank:** MySQL Server/MS SQL Server/MS SQL Server mit Windows-Authentifizierung
- **ODBC-Treiber:** MySQL ODBC 5.1-Treiber/MySQL ODBC 5.2 Unicode-Treiber/MySQL ODBC 5.3 Unicode-Treiber/MySQL ODBC 8.0 Unicode-Treiber/SQL Server/SQL Server Native Client 10.0/ODBC-Treiber 11 für SQL Server/ODBC-Treiber 13 für SQL Server/ODBC-Treiber 17 für SQL Server/ODBC-Treiber 18 für SQL Server
- **Datenbankname:** Sie können den vordefinierten Namen beibehalten oder den Namen bei Bedarf ändern.
- **Hostname:** Hostname oder IP-Adresse des Datenbankservers

- **Port:** für die Verbindung zum Datenbankserver
- Benutzername/Passwort **des Datenbankadministratorkontos**
- **Benannte Instanz verwenden** – Falls Sie eine MS SQL-Datenbank verwenden, können Sie auch das Kontrollkästchen **Benannte Instanz verwenden** auswählen, um eine benutzerdefinierte benannte Instanz zu verwenden. Sie können die Instanz im Feld **Hostname** im Format *HOSTNAME\DB_INSTANZ* angeben (zum Beispiel *192.168.0.10\ESMC7SQL*). Geben Sie für geclusterte Datenbanken nur den Clusternamen an. Wenn Sie diese Option auswählen, können Sie den Port für die Datenbankverbindung nicht ändern, und das System verwendet die von Microsoft festgelegten Standardports. Um den ESET PROTECT Server mit einer MS SQL-Datenbank in einem Failover-Cluster zu verbinden, geben Sie den Clusternamen in das Feld **Hostname** ein.

The screenshot shows the 'Database server connection' window of the ESET PROTECT Mobile Device Connector Setup. The window title is 'ESET PROTECT Mobile Device Connector Setup'. Below the title bar, it says 'Database server connection' and 'Please enter database server connection.' The ESET logo is in the top right corner. The main area contains several fields:

- Database:** A dropdown menu with 'MS SQL Server' selected.
- ODBC driver:** A dropdown menu with 'MS SQL Server' selected.
- Database name:** A text box containing 'era_mdm_db'.
- Hostname:** A text box containing 'localhost'.
- Use Named Instance:** An unchecked checkbox.
- Port:** A text box containing '1433'.
- Database account:** A label above two empty text boxes for 'Username:' and 'Password:'.

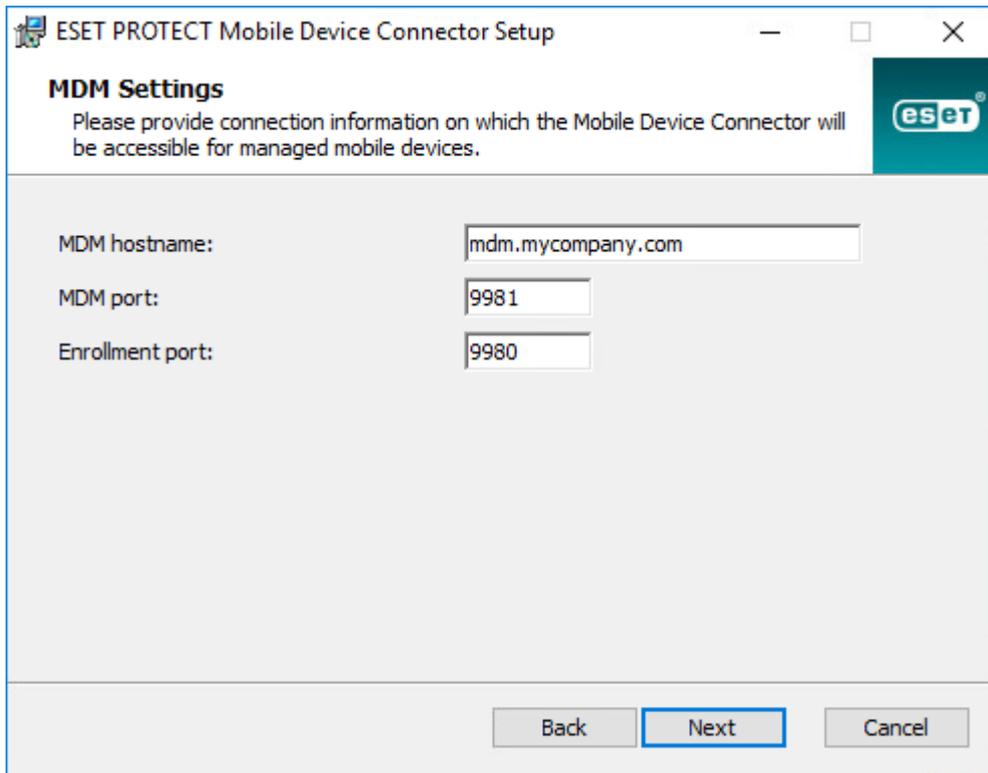
 At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

8. Nach dem Verbindungsaufbau werden Sie aufgefordert, zu bestätigen, dass Sie den angegebenen Benutzer als Datenbankbenutzer für ESET PROTECT MDM verwenden möchten.

9. Nachdem die neue Datenbank erfolgreich installiert bzw. sich das Installationsprogramm erfolgreich mit der vorhandenen Datenbank verbunden hat, können Sie mit der MDM-Installation fortfahren. Geben Sie Ihren **MDM-Hostnamen** an: Dies ist der öffentliche Domänenname bzw. die öffentliche IP-Adresse, unter der Ihr MDM-Server für mobile Geräte aus dem Internet erreichbar ist.

Der MDM-Hostname muss auf dieselbe Weise wie in Ihrem **HTTPS-Serverzertifikat** angegeben werden, um das [MDM-Profil](#) auf iOS-Geräten installieren zu können. Wenn im HTTPS-Zertifikat eine IP-Adresse angegeben ist, müssen Sie diese IP-Adresse in das Feld **MDM-Hostname** eingeben. Wenn das HTTPS-Zertifikat einen FQDN enthält (z. B. *mdm.mycompany.com*), müssen Sie diesen FQDN in das Feld **MDM-Hostname** eingeben. Wenn das HTTPS-Zertifikat einen Platzhalter „*“ enthält (z. B. **.mycompany.com*), dann können Sie *mdm.mycompany.com* in das Feld **MDM-Hostname** eingeben.

 Überlegen Sie sich sorgfältig, welchen Wert Sie in diesem Installationsschritt in das Feld **MDM-Hostname** eingeben. Wenn Sie einen ungültigen oder einen falsch formatierten Wert eingeben, funktioniert der MDM Connector nicht ordnungsgemäß, und Sie müssen die Komponente erneut installieren.



10. Klicken Sie im nächsten Schritt auf **Weiter**, um die Datenbankverbindung zu überprüfen.

11. Verbinden Sie den MDM Connector mit dem ESET PROTECT Server. Füllen Sie die Pflichtfelder **Serverhost** und **Serverport** für die Verbindung zum ESET PROTECT Server aus und wählen Sie entweder **Servergestützte Installation** oder **Offline-Installation** aus, um fortzufahren:

- **Servergestützte Installation** - Geben Sie die Anmeldedaten des Administrators der ESET PROTECT-Web-Konsole ein (das Installationsprogramm lädt die erforderlichen Zertifikate automatisch herunter). Überprüfen Sie außerdem die benötigten [Berechtigungen](#) für die servergestützte Installation.

1. Geben Sie **Serverhost** (Name oder IP-Adresse des ESET PROTECT Servers) und **Web-Konsolen-Port** ein (lassen Sie den standardmäßigen Port 2223 unverändert, sofern Sie keinen benutzerdefinierten Port verwenden). Geben Sie außerdem die Anmeldedaten des Administrators der Web-Konsole ein: **Benutzername/Passwort**.

2. Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob Sie das Zertifikat akzeptieren möchten. Fahren Sie mit Schritt 11 fort.

- **Offline-Installation** - Geben Sie ein Proxy-Zertifikat und eine Zertifizierungsstelle an, die Sie aus ESET PROTECT [exportieren](#) können. Alternativ können Sie Ihr [benutzerdefiniertes Zertifikat](#) mit einer passenden Zertifizierungsstelle verwenden.

1. Klicken Sie neben dem Peerzertifikat auf **Durchsuchen** und navigieren Sie zum Speicherort des **Peerzertifikats** (das Proxy-Zertifikat, das Sie aus ESET PROTECT exportiert haben). Lassen Sie das Textfeld **Zertifikatspasswort** leer, da für dieses Zertifikat kein Passwort erforderlich ist.

2. Wiederholen Sie den Vorgang für die Zertifizierungsstelle und fahren Sie mit Schritt 11 fort.



Wenn Sie benutzerdefinierte Zertifikate mit ESET PROTECT verwenden (anstelle der bei der Installation von ESET PROTECT generierten Standardzertifikate), geben Sie diese entsprechend an, wenn Sie nach einem Proxy-Zertifikat gefragt werden.

12. Geben Sie einen Zielordner für den Mobile Device Connector an (wir empfehlen, den standardmäßigen Speicherort beizubehalten), klicken Sie auf **Weiter > Installieren**.

Nach Abschluss der MDM-Installation werden Sie zur Installation des Agenten aufgefordert. Klicken Sie auf **Weiter**, um die Installation zu starten, akzeptieren Sie die EULA, falls Sie ihr zustimmen, und führen Sie die folgenden Schritte aus:

1. Geben Sie **Serverhost** (Name oder IP-Adresse Ihres ESET PROTECT Servers) und **Serverport** (standardmäßig 2222, ersetzen Sie diesen Wert ggf. durch einen benutzerdefinierten Port) ein.



Achten Sie darauf, dass der **Serverhost** mit mindestens einem der Werte (idealerweise dem FQDN) übereinstimmt, die im Feld **Host** des **Serverzertifikats** definiert sind. Andernfalls erhalten Sie die Fehlermeldung "Das empfangene Serverzertifikat ist nicht gültig". Die einzige Ausnahme ist die Angabe von Platzhaltern (*) im Host-Feld des Serverzertifikats. In diesem Fall werden alle **Serverhosts** akzeptiert.

2. Falls Sie einen Proxy verwenden, aktivieren Sie das Kontrollkästchen **Proxy verwenden**. Wenn dieses Feld ausgewählt ist, fährt das Installationsprogramm mit der **Offline-Installation** fort.



Diese Proxyeinstellung wird nur für die Replikation zwischen dem ESET Management Agenten und dem ESET PROTECT Server verwendet, nicht für die Zwischenspeicherung von Updates.

- **Proxy-Hostname:** Hostname oder IP-Adresse des HTTP-Proxycomputers.

- **Proxyport:** Standardmäßig 3128.

- **Benutzername, Passwort:** geben Sie die Anmeldeinformationen für Ihren Proxy ein, falls dieser Authentifizierung verwendet.

Sie können die Proxyeinstellungen später in Ihrer [Policy](#) ändern. Sie müssen den [Proxy](#) installieren, bevor Sie eine Verbindung zwischen Agent und Server über einen Proxy konfigurieren können.

3. Wählen Sie eine der folgenden Installationsoptionen und führen Sie die Schritte aus, die in den entsprechenden Abschnitten beschrieben sind:

Servergestützte Installation – Bei dieser Installationsart müssen Sie die Administrator-Anmeldeinformationen für die ESET PROTECT-Web-Konsole eingeben (das Installationsprogramm lädt die erforderlichen Zertifikate automatisch herunter).

Offline-Installation – Geben Sie ein Agentenzertifikat und eine Zertifizierungsstelle an, die Sie aus ESET PROTECT [exportieren](#) können. Alternativ können Sie Ihr [benutzerdefiniertes Zertifikat](#) verwenden.

- Gehen Sie wie folgt vor, um die **servergestützte Installation des Agenten** fortzusetzen:

1. Geben Sie Hostname oder IP-Adresse Ihrer ESET PROTECT-Web-Konsole (gleiche Werte wie ESET PROTECT Server) in das Feld **Serverhost** ein. Lassen Sie im Feld **Web-Konsolen-Port** den Standardport 2223 unverändert, falls Sie keinen benutzerdefinierten Port verwenden. Geben Sie außerdem die Anmeldedaten für das Web-Konsolen-Konto in die Felder **Benutzername und Passwort** ein. Um sich als Domänenbenutzer anzumelden, aktivieren Sie das Kontrollkästchen neben **An Domäne anmelden**.



- Achten Sie darauf, dass **Serverhost** mit mindestens einem der Werte (idealerweise der FQDN) übereinstimmt, die im Feld **Host** des **Serverzertifikats** definiert sind. Andernfalls erhalten Sie die Fehlermeldung "Das empfangene Serverzertifikat ist nicht gültig". Die einzige Ausnahme ist die Angabe von Platzhaltern (*) im Host-Feld des Serverzertifikats. In diesem Fall werden alle **Serverhosts** akzeptiert.
- Sie können keinen Benutzer mit [Zwei-Faktor-Authentifizierung](#) für servergestützte Installationen verwenden.

2. Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob Sie das Zertifikat akzeptieren möchten.

3. Wählen Sie **Computer nicht erstellen (Computer wird bei der ersten Verbindung automatisch erstellt)** oder **Benutzerdefinierte statische Gruppe auswählen** aus. Wenn Sie auf **Benutzerdefinierte statische Gruppe auswählen** klicken, können Sie aus einer Liste vorhandener statischer Gruppen in ESET PROTECT eine Auswahl treffen. Der Computer wird zur ausgewählten Gruppe hinzugefügt.

4. Geben Sie einen Zielordner für den ESET Management Agenten an (nach Möglichkeit der standardmäßige Speicherort), klicken Sie auf **Weiter** und dann auf **Installieren**.

- Gehen Sie wie folgt vor, um die **Offline-Installation des Agenten** fortzusetzen:

1. Falls Sie im vorherigen Schritt die Option **Proxy verwenden** ausgewählt haben, geben Sie den **Proxy-Hostnamen**, den **Proxy-Port** (der Standardport ist 3128), den **Benutzernamen** und das **Passwort** ein, und klicken Sie auf **Weiter**.

2. Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort Ihres Peerzertifikats (das Agentenzertifikat, das Sie aus ESET PROTECT exportiert haben). Lassen Sie das Textfeld **Zertifikatspasswort** leer, da für dieses Zertifikat kein Passwort erforderlich ist. Sie müssen keine **Zertifizierungsstelle** suchen. Lassen Sie dieses Feld leer.



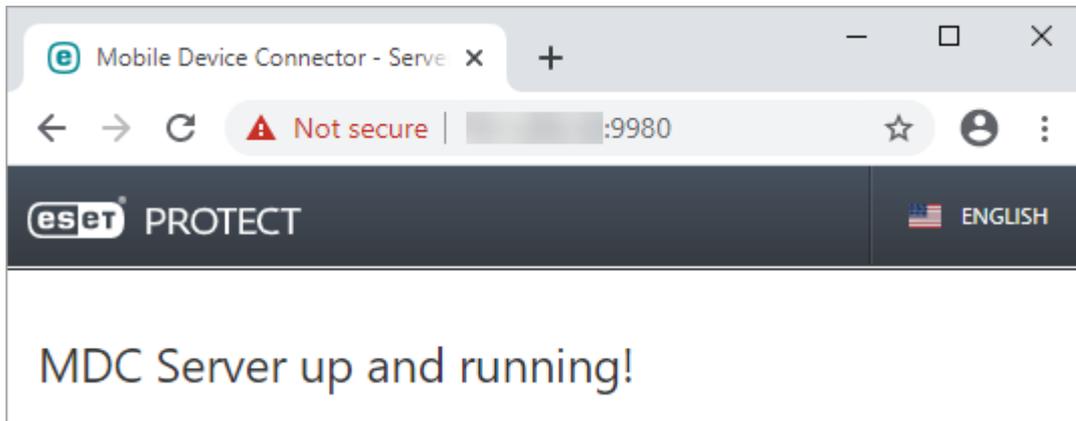
Wenn Sie ein benutzerdefiniertes Zertifikat mit ESET PROTECT verwenden (anstelle des standardmäßigen Zertifikats, das bei der Installation von ESET PROTECT automatisch generiert wurde), geben Sie dies entsprechend an.



Die Zertifikat-Passphrase darf die folgenden Zeichen nicht enthalten: " \ Diese Zeichen verursachen kritische Fehler bei der Initialisierung des Agenten.

3. Klicken Sie auf **Weiter**, um die Installation im standardmäßigen Ordner auszuführen, oder auf **Ändern**, um einen anderen Ordner auszuwählen. Wir empfehlen, den standardmäßigen Speicherort beizubehalten.

Überprüfen Sie nach dem Abschluss der Installation, ob der Mobile Device Connector richtig ausgeführt wird. Öffnen Sie dazu die Adresse <https://ihr-mdm-hostname:registrierungs-port> (z. B. <https://mdm.company.com:9980>) in einem Webbrowser oder auf einem Mobilgerät. Wenn die Installation erfolgreich war, wird die folgende Meldung angezeigt:



Sie können [MDM jetzt in ESET PROTECT](#) aktivieren.

Installation in Microsoft Azure

Für Benutzer, die eine verwaltete Lösung gegenüber einer selbstverwalteten lokalen ESET PROTECT-Installation bevorzugen, bietet ESET ESET PROTECT für die [Microsoft Azure](#)-Cloud-Plattform an.

Weitere Informationen finden Sie in unserer Knowledgebase:

- [Erste Schritte mit ESET PROTECT - Azure](#)
- [ESET PROTECT VM für Microsoft Azure—FAQ](#)
- Sie können ESET PROTECT 9.1 in Azure installieren, indem Sie die Schritte in [diesem Knowledgebase-Artikel](#) ausführen und das [All-in-One-Installationsprogramm für ESET PROTECT 9.1](#). Alternativ können Sie ESMC 7.2 in Azure installieren und anschließend ein [Upgrade auf ESET PROTECT](#) durchführen.

Komponenteninstallation unter Windows

In vielen Installationsszenarien müssen Sie verschiedene ESET PROTECT-Komponenten auf verschiedenen Computern installieren, z. B. um Unterschiede in der Netzwerkarchitektur zu berücksichtigen oder Leistungsanforderungen zu erfüllen. Für einzelne ESET PROTECT-Komponenten sind die folgenden Installationspakete verfügbar:

Kernkomponenteninstallation

- [ESET PROTECT Server](#)
- [ESET PROTECT-Web-Konsole](#) – Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server.
- [ESET Management Agent](#) (muss auf Clientcomputern installiert sein, optional auf dem ESET PROTECT Server)

Installation optionaler Komponenten

- [RD Sensor](#)

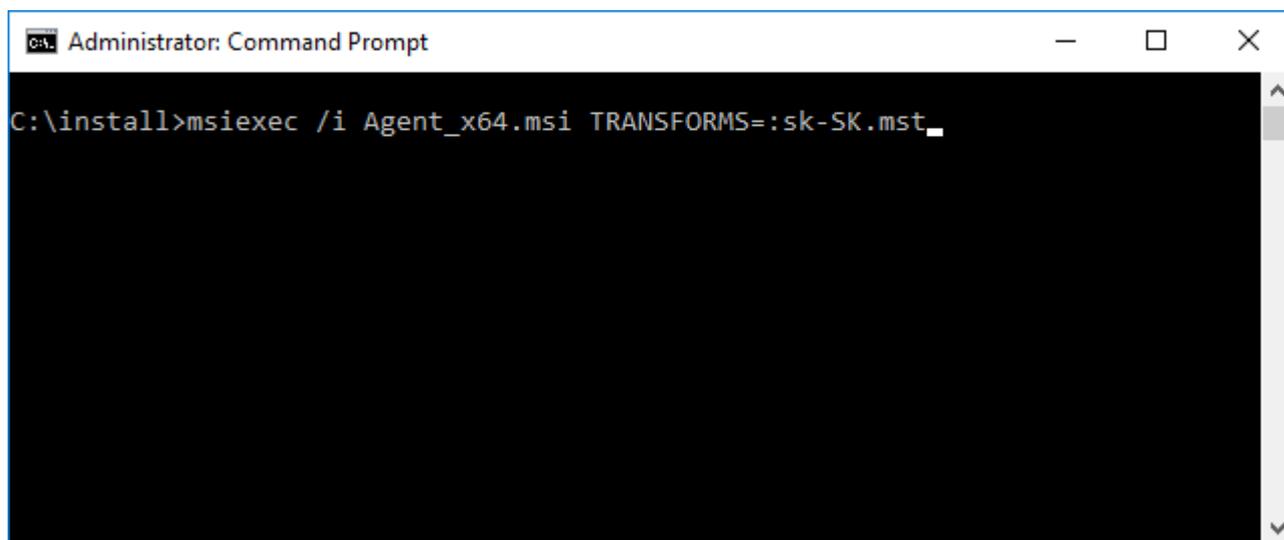
- [Mobile Device Connector](#)
- [Apache HTTP Proxy](#)
- [Mirror-Tool](#)

Siehe auch [ESET PROTECT All-in-One-Installation](#).

Hinweise zum Upgrade von ESMC auf die neueste Version ESET PROTECT 9.1 finden Sie in unseren [Upgradeprozeduren](#).

Wenn Sie die Installation in Ihrer lokalen Sprache ausführen möchten, müssen Sie das MSI-Installationsprogramm der entsprechenden ESET PROTECT-Komponente über die Befehlszeile ausführen.

Nachstehend finden Sie ein Beispiel zur Ausführung der Installation auf Slowakisch:



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

Um die Sprache festzulegen, in der das Installationsprogramm ausgeführt werden soll, geben Sie gemäß folgender Tabelle den entsprechenden TRANSFORMS-Parameter an:

Sprache	Code
English (United States)	en-US
Arabisch (Ägypten)	ar-EG
Chinesisch vereinfacht	zh-CN
Chinesisch traditionell	zh-TW
Kroatisch (Kroatien)	hr-HR
Tschechisch (Tschechische Republik)	cs-CZ
Französisch (Frankreich)	fr-FR
Französisch (Kanada)	fr-CA
Deutsch (Deutschland)	de-DE
Griechisch (Griechenland)	el-GR
Ungarisch (Ungarn)*	hu-HU
Indonesisch (Indonesien)*	id-ID
Italienisch (Italien)	it-IT
Japanisch (Japan)	ja-JP

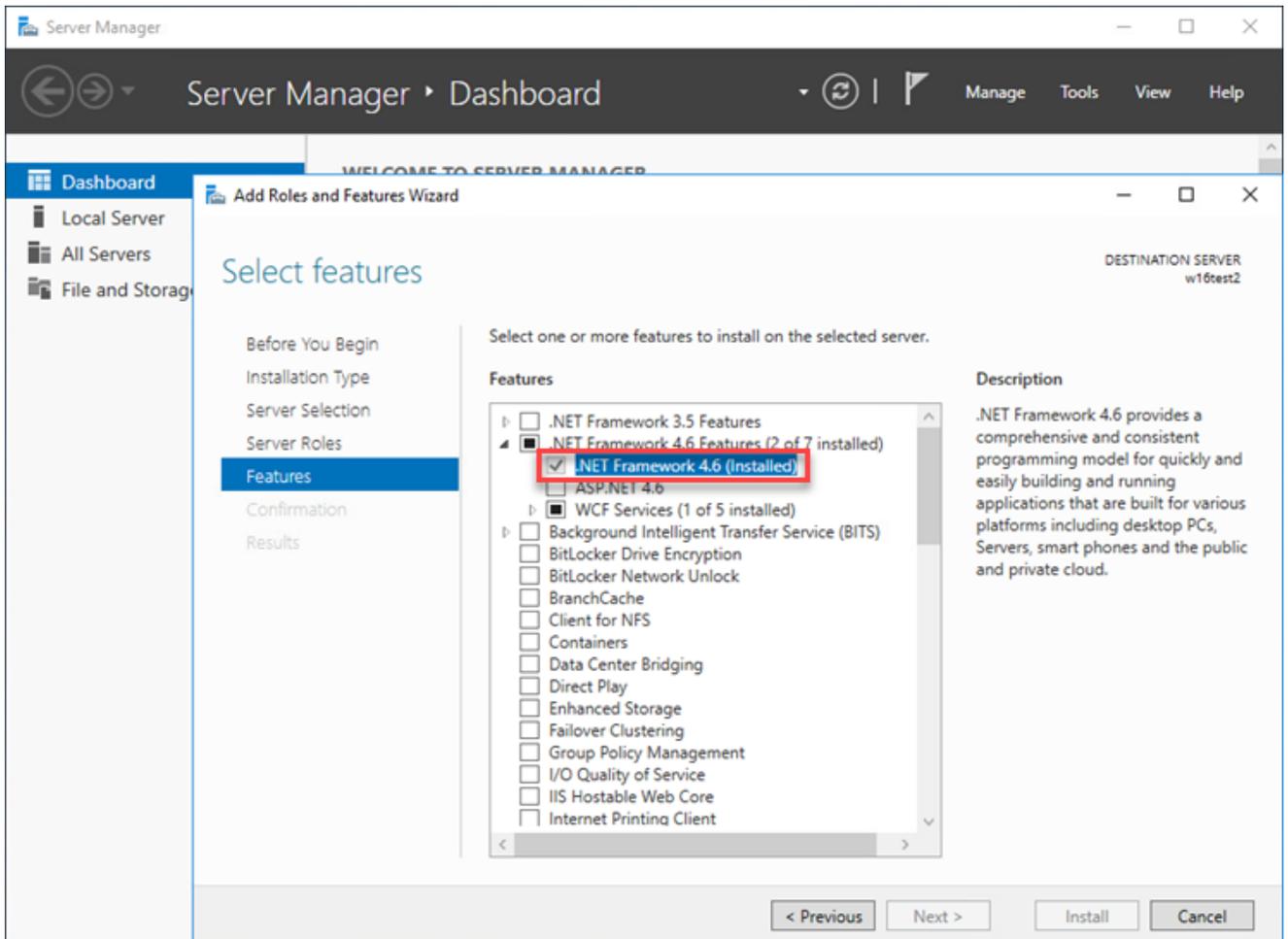
Sprache	Code
Koreanisch (Korea)	ko-KR
Polnisch (Polen)	pl-PL
Portugiesisch (Brasilien)	pt-BR
Russisch (Russland)	ru-RU
Spanisch (Chile)	es-CL
Spanisch (Spanien)	es-ES
Slowakisch (Slowakei)	sk-SK
Türkisch (Türkei)	tr-TR
Ukrainisch (Ukraine)	uk-UA

* Nur das Produkt ist in dieser Sprache verfügbar, die Onlinehilfe dagegen nicht.

Serverinstallation – Windows

Voraussetzungen

- Sie benötigen einen gültigen [Lizenzschlüssel](#).
- Sie benötigen ein [unterstütztes Windows-Betriebssystem](#).
- Die erforderlichen Ports müssen geöffnet und verfügbar sein. Eine vollständige [Liste der Ports finden Sie hier](#).
- Ein [unterstützter Datenbankserver und der entsprechende Connector](#) ([Microsoft SQL Server](#) oder [MySQL](#)) sind installiert und werden ausgeführt. Überprüfen Sie die Konfigurationsdetails des Datenbankservers ([Microsoft SQL Server](#) oder [MySQL](#)), um sicherzustellen, dass die Datenbank korrekt für die Verwendung mit ESET PROTECT konfiguriert ist. Lesen Sie unseren [Knowledgebase-Artikel](#) zur Einrichtung von Datenbank und Datenbankbenutzer für MS SQL und MySQL.
- Die [ESET PROTECT-Web-Konsole](#) muss installiert sein, um den ESET PROTECT Server verwalten zu können.
- Für die Installation von MS SQL Server Express ist Microsoft .NET Framework 4 erforderlich. Sie können die Software mit dem **Assistenten zum Hinzufügen von Rollen und Features** installieren:



Installation

Führen Sie die folgenden Schritte aus, um die ESET PROTECT Server-Komponente unter Windows zu installieren:

! Vergewissern Sie sich, dass alle oben genannten Installationsvoraussetzungen erfüllt sind.

1. Besuchen Sie den [ESET PROTECT-Downloadbereich](#), um ein eigenständiges Installationsprogramm für diese ESET PROTECT-Komponente herunterzuladen (*server_x64.ms*).
2. Führen Sie das Installationsprogramm für den ESET PROTECT Server aus und akzeptieren Sie die EULA, falls Sie ihr zustimmen.
3. Deaktivieren Sie das Kontrollkästchen neben **Am Produktverbesserungsprogramm teilnehmen**, falls Sie der Übertragung von Absturzberichten und anonymen Telemetriedaten (Betriebssystemversion und -Typ, ESET-Produktversion und andere produktspezifische Daten) an ESET nicht zustimmen. Wenn Sie dieses Kontrollkästchen aktiviert lassen, werden Telemetriedaten und Absturzberichte an ESET übertragen.
4. Lassen Sie das Kontrollkästchen neben **Dies ist eine Clusterinstallation** leer und klicken Sie auf **Weiter**. [Führen Sie eine Clusterinstallation durch?](#)
5. Wählen Sie ein **Dienstbenutzerkonto** aus. Mit diesem Konto wird der ESET PROTECT-Serverdienst ausgeführt. Folgende Optionen stehen zur Verfügung:

- **Netzwerkdienstkonto** - Wählen Sie diese Option aus, wenn Sie keine Domäne verwenden.
- **Benutzerdefiniertes Konto:** Anmeldeinformationen für Domänenbenutzer angeben: DOMÄNE\BENUTZERNAME und Passwort.

6. Stellen Sie eine Verbindung zu einer Datenbank her. Hier werden alle Daten gespeichert (Passwort für die ESET PROTECT-Web-Konsole, Logs der Clientcomputer usw.):

- **Datenbank:** MySQL Server/MS SQL Server/MS SQL Server mit Windows-Authentifizierung
- **ODBC-Treiber:** MySQL ODBC 5.1-Treiber/MySQL ODBC 5.2 Unicode-Treiber/MySQL ODBC 5.3 Unicode-Treiber/MySQL ODBC 8.0 Unicode-Treiber/SQL Server/SQL Server Native Client 10.0/ODBC-Treiber 11 für SQL Server/ODBC-Treiber 13 für SQL Server/ODBC-Treiber 17 für SQL Server/ODBC-Treiber 18 für SQL Server
- **Datenbankname:** Sie können den vordefinierten Namen beibehalten oder den Namen bei Bedarf ändern.
- **Hostname:** Hostname oder IP-Adresse des Datenbankservers
- **Port:** für die Verbindung zum Datenbankserver
- **Benutzername/Passwort des Datenbankadministratorkontos**
- **Benannte Instanz verwenden** – Falls Sie eine MS SQL-Datenbank verwenden, können Sie auch das Kontrollkästchen **Benannte Instanz verwenden** auswählen, um eine benutzerdefinierte benannte Instanz zu verwenden. Sie können die Instanz im Feld **Hostname** im Format *HOSTNAME\DB_INSTANZ* angeben (zum Beispiel *192.168.0.10\ESMC7SQL*). Geben Sie für geclusterte Datenbanken nur den Clusternamen an. Wenn Sie diese Option auswählen, können Sie den Port für die Datenbankverbindung nicht ändern, und das System verwendet die von Microsoft festgelegten Standardports. Um den ESET PROTECT Server mit einer MS SQL-Datenbank in einem Failover-Cluster zu verbinden, geben Sie den Clusternamen in das Feld **Hostname** ein.

ESET PROTECT Server Setup

Database server connection
Please enter database server connection.

Database: MS SQL Server

ODBC driver: MS SQL Server

Database name: era_db

Hostname: localhost

Use Named Instance:

Port: 1433

Database account

Username:

Password:

Back Next Cancel

i Der ESET PROTECT Server speichert große Datenblöcke in der Datenbank. Daher muss [MySQL große Pakete annehmen](#), um ESET PROTECT ordnungsgemäß zu unterstützen.

In diesem Schritt wird die Verbindung zur Datenbank überprüft. Wenn die Verbindung erfolgreich hergestellt wird, können Sie mit dem nächsten Schritt fortfahren.

7. Wählen Sie einen Benutzer für ESET PROTECT aus, der zum Zugriff auf die Datenbank berechtigt ist. Sie können einen vorhandenen Benutzer angeben oder einen neuen Benutzer erstellen lassen.

ESET PROTECT Server Setup

Database user for ESET PROTECT
Please enter database user for ESET PROTECT credentials.

Create new user

Use existing user

Database username:

Password:

Password confirmation:

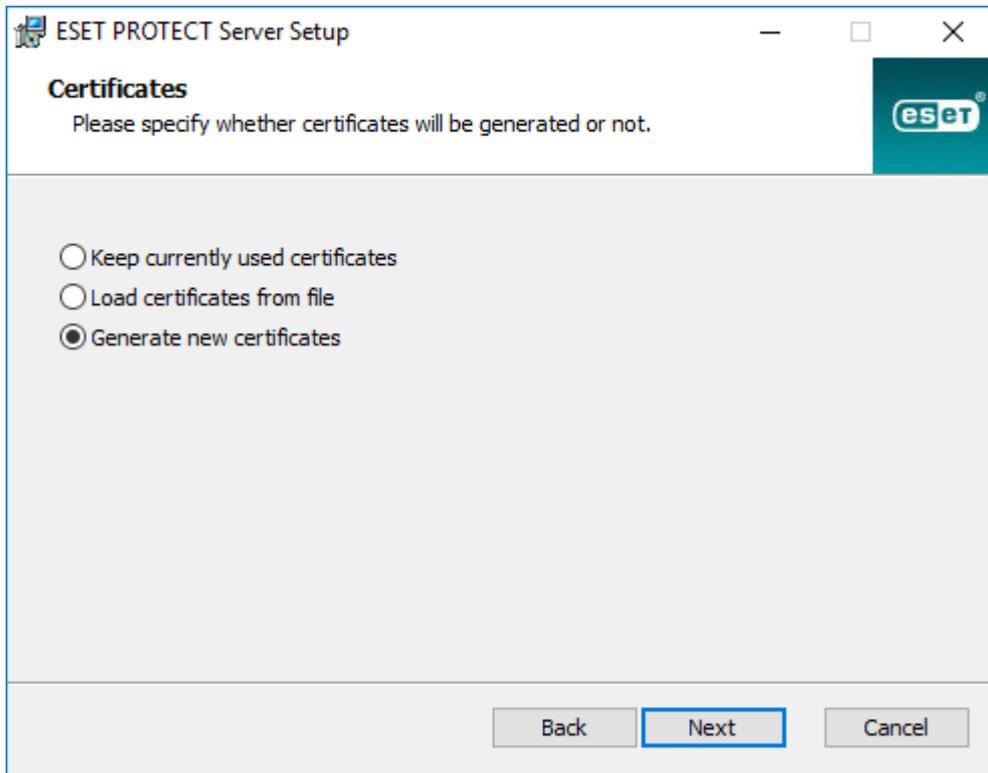
Back Next Cancel

8. Geben Sie ein Passwort für den Zugriff auf die **Web-Konsole** ein.

The screenshot shows the 'ESET PROTECT Server Setup' window. The title bar includes the ESET logo and window controls. The main heading is 'Web Console user & server connection' with the instruction 'Please enter Web Console user password and server connection.' Below this, there are several input fields: 'Web Console user:' with the value 'Administrator'; 'Password:' and 'Password confirmation:' fields, both containing ten black dots; 'Agent port:' with the value '2222'; and 'Console port:' with the value '2223'. At the bottom, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'.

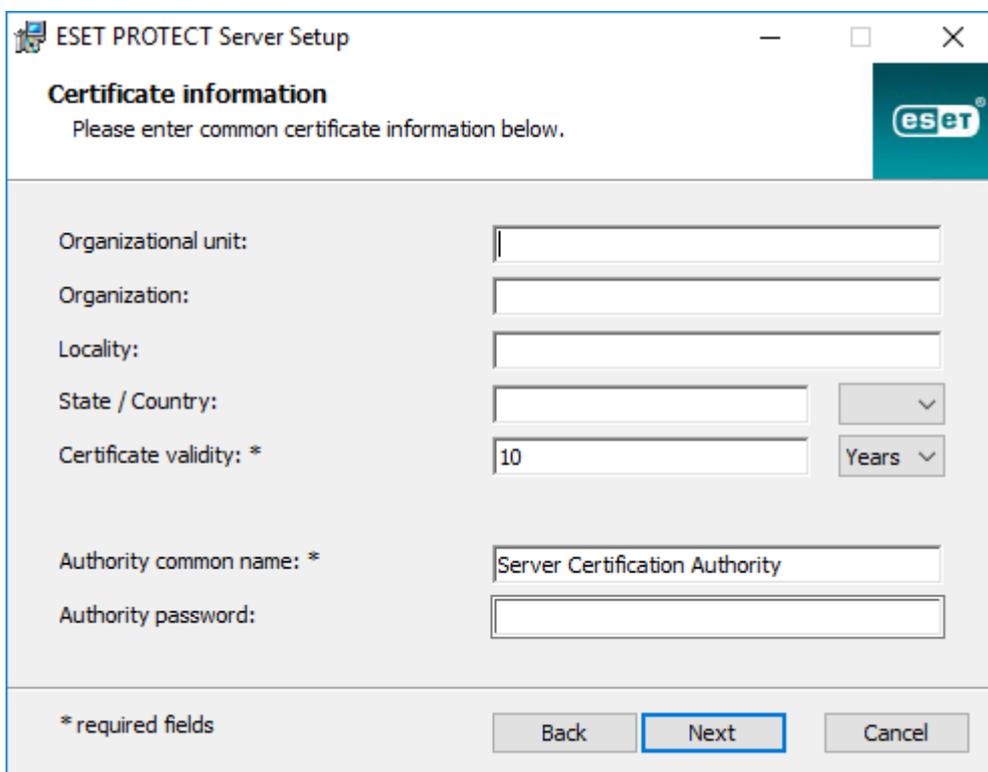
9. ESET PROTECT verwendet Zertifikate für die Client-Server-Kommunikation. Wählen Sie eine der folgenden Optionen aus:

- **Aktuell verwendete Zertifikate behalten** - Diese Option ist nur verfügbar, wenn die Datenbank bereits zuvor mit einem anderen ESET PROTECT Server verwendet wurde.
- **Zertifikate aus Datei laden** - Wählen Sie das vorhandene Serverzertifikat und die Zertifizierungsstelle aus.
- **Neue Zertifikate generieren** - Das Installationsprogramm generiert neue Zertifikate.



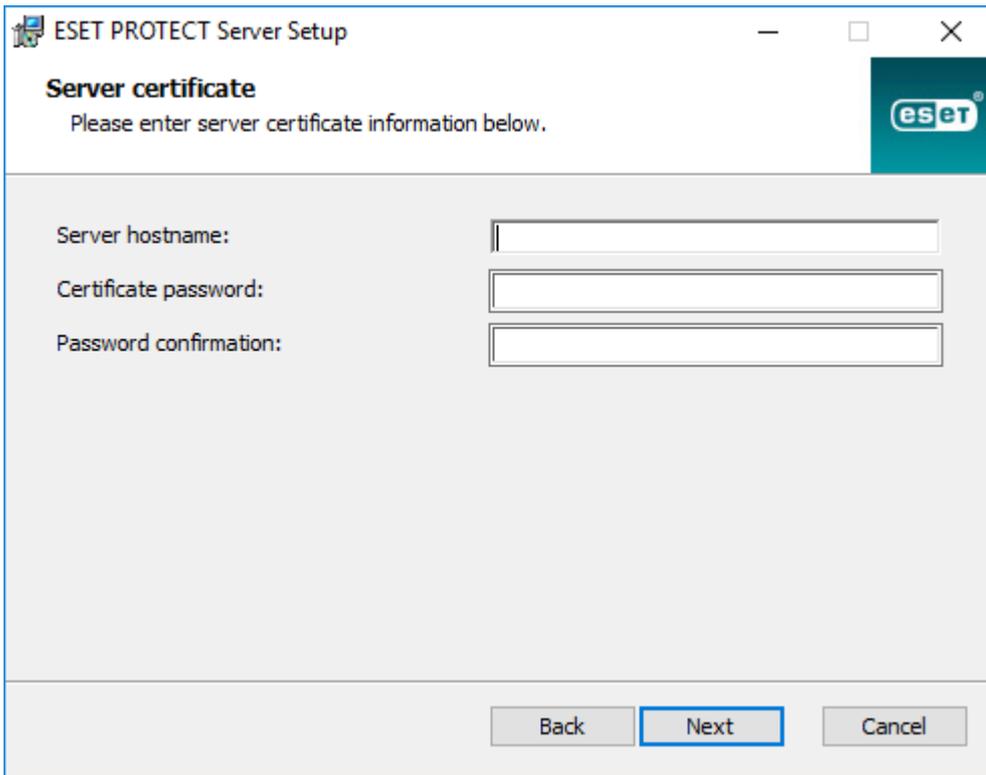
10. Führen Sie diesen Schritt aus, wenn Sie im vorherigen Schritt die Option **Neue Zertifikate generieren** ausgewählt haben.

a) Geben Sie zusätzliche Informationen zu den Zertifikaten ein (optional). Wenn Sie das **Passwort für die Zertifizierungsstelle** eingeben, sollten Sie es sich unbedingt merken.



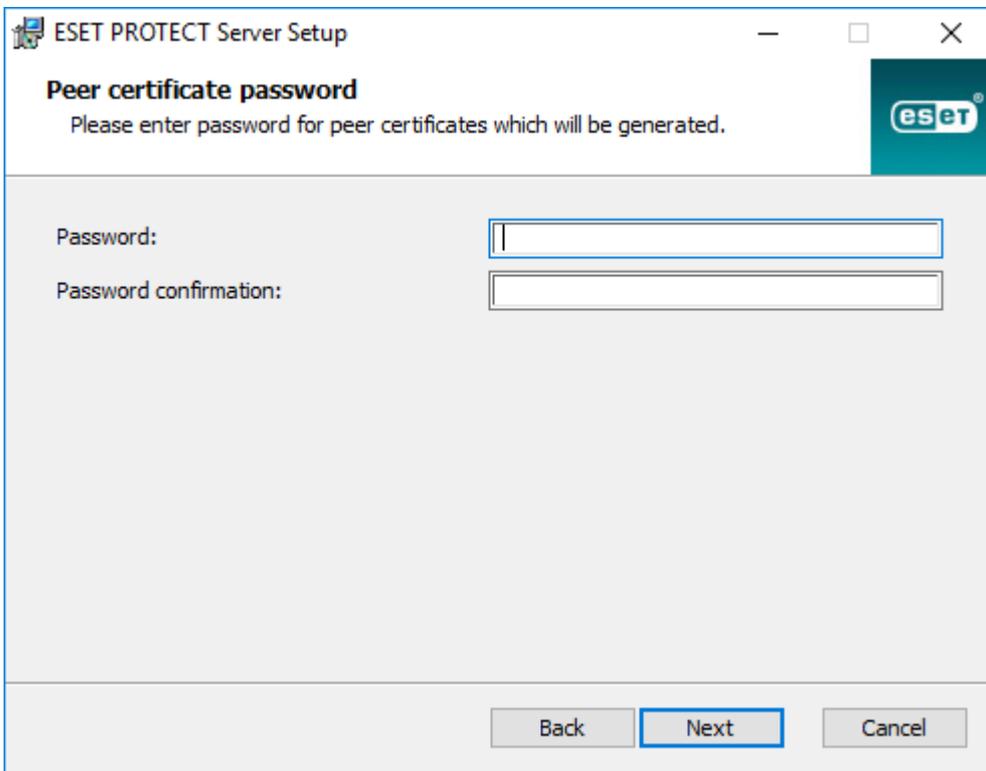
b) Geben Sie im Feld des **Serverzertifikat** den **Hostnamen des Servers** und optional ein **Zertifikatpasswort** ein.

 Der **Serverhostname** im Serverzertifikat darf keine der folgenden Schlüsselwörter enthalten: server, proxy, agent.



The screenshot shows the 'Server certificate' step of the ESET PROTECT Server Setup. The window title is 'ESET PROTECT Server Setup'. The main heading is 'Server certificate' with the instruction 'Please enter server certificate information below.' Below this, there are three input fields: 'Server hostname:', 'Certificate password:', and 'Password confirmation:'. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

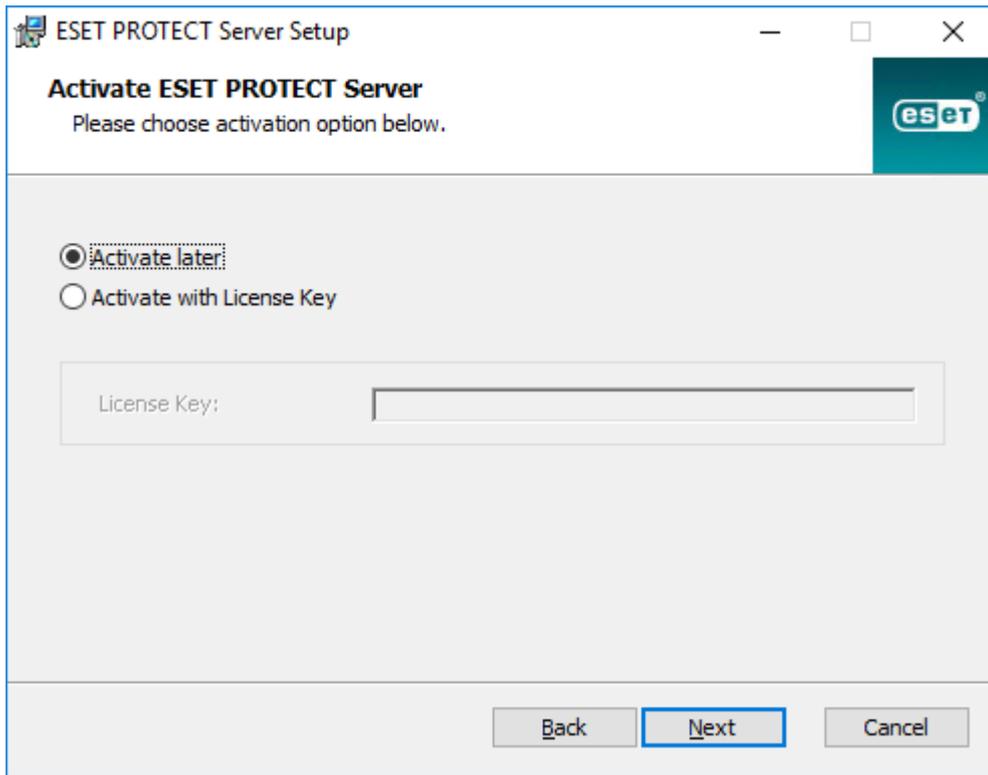
c) Geben Sie das Passwort für die Agenten- und Proxy-Peerzertifikate in das Feld **Passwort für das Peerzertifikat** ein.



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

11. Während der Einrichtung kann ein erster [Task zur Synchronisierung statischer Gruppen](#) ausgeführt werden. Wählen Sie die Methode aus (**Nicht synchronisieren, Mit Windows-Netzwerk synchronisieren, Mit Active Directory synchronisieren**) und klicken Sie auf **Weiter**.

12. Geben Sie einen gültigen [Lizenzschlüssel](#) ein oder wählen Sie **Später aktivieren** aus.



13. Bestätigen oder ändern Sie den Installationsordner für den Server und klicken Sie auf **Weiter**.

14. Klicken Sie auf **Installieren**, um den ESET PROTECT Server zu installieren.



Nach Abschluss der Installation von ESET PROTECT Server können Sie den [ESET Management Agenten](#) auf dem gleichen Computer installieren (optional), um den Server auf dieselbe Weise zu verwalten wie einen Clientcomputer.

Microsoft SQL Server – Anforderungen

Die folgenden Voraussetzungen für Microsoft SQL Server müssen erfüllt sein:

- Installieren Sie eine [unterstützte Version von Microsoft SQL Server](#). Wählen Sie bei der Installation den **Gemischten Modus** für die Authentifizierung aus.
- Falls Sie Microsoft SQL Server bereits installiert haben, legen Sie die Authentifizierung auf **Gemischter Modus (SQL Server-Authentifizierung und Windows-Authentifizierung)** fest. Führen Sie dazu die Anweisungen in diesem [KnowledgeBase-Artikel](#) aus. Falls Sie die **Windows-Authentifizierung** verwenden möchten, um sich beim Microsoft SQL Server anzumelden, führen Sie die Schritte in diesem [Knowledgebase-Artikel](#) aus.
- Erlauben Sie TCP/IP-Verbindungen zum SQL Server. Führen Sie dazu die Anweisungen in diesem [KnowledgeBase-Artikel](#) ab Teil II **aus. Erlauben Sie TCP/IP-Verbindungen zum SQL Server** aus.

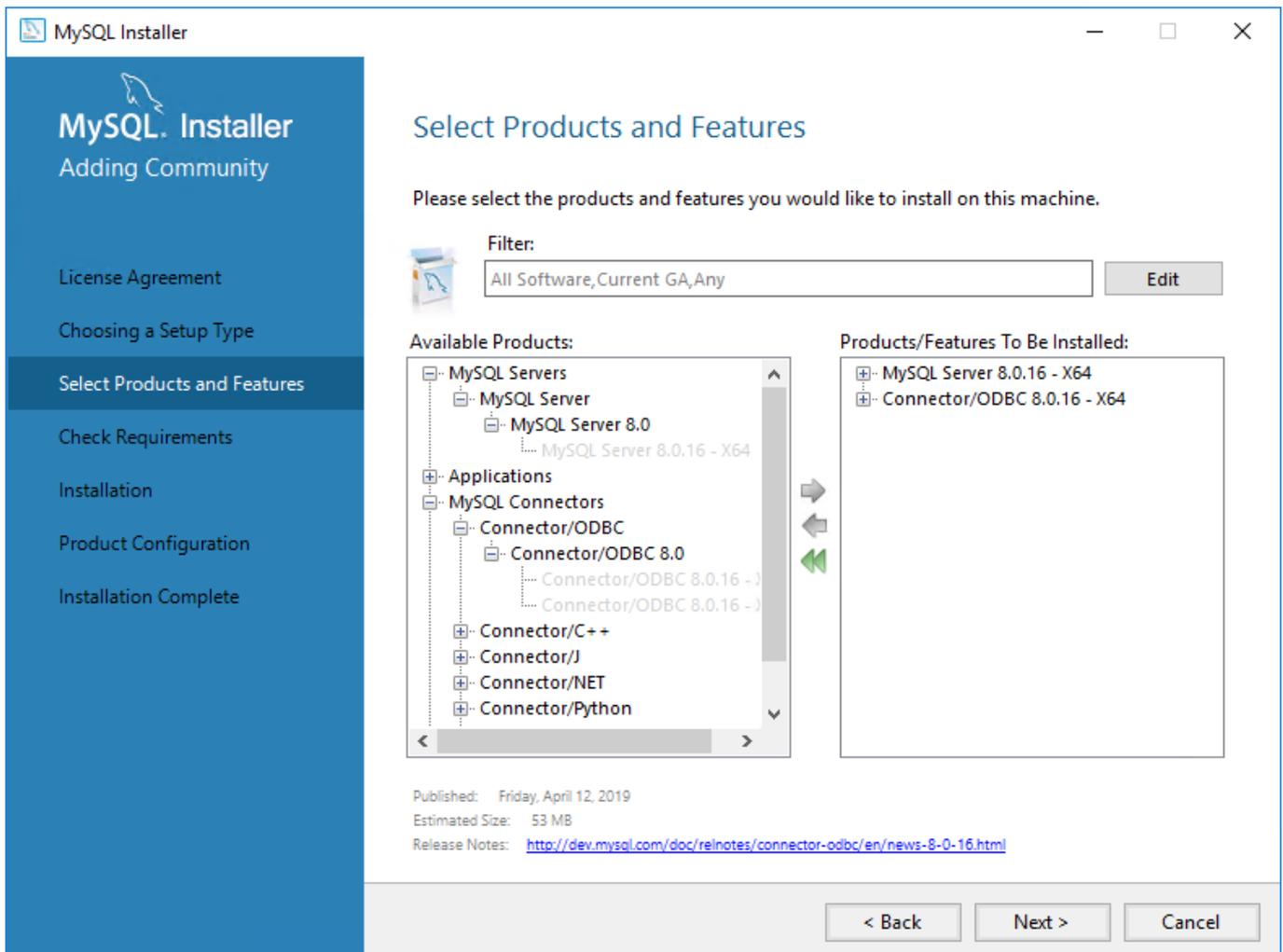
- Für die Konfiguration, Verwaltung und Administration von Microsoft SQL Server (Datenbanken und Benutzer) empfehlen wir Ihnen, [SQL Server Management Studio \(SSMS\) herunterzuladen](#).
- [Installieren Sie SQL Server sollte nicht auf einem Domänencontroller](#) (z. B. Windows SBS oder Essentials). Sollten Sie ESET PROTECT auf einem anderen Server installieren oder während der Installation nicht die SQL Server Express-Komponente auswählen (in diesem Fall müssen Sie SQL Server oder MySQL als ESET PROTECT-Datenbank verwenden).

MySQL Server – Installation und Konfiguration

Installation

Achten Sie darauf, [unterstützte Versionen von MySQL Server und ODBC Connector](#) zu installieren.

1. Laden Sie das Windows-Installationsprogramm für MySQL 8 unter <https://dev.mysql.com/downloads/installer/> herunter und führen Sie es aus.
2. Aktivieren Sie das Kontrollkästchen **Ich stimme den Lizenzbedingungen zu** und klicken Sie auf **Weiter**.
3. Wählen Sie im Installations-Setup **Benutzerdefiniert > MySQL Server** und **Connector/ODBC** für die Installation aus. Überprüfen Sie, ob die Plattform des ODBC-Connectors mit dem installierten MySQL-Server übereinstimmt (x86 oder x64).



4. Klicken Sie auf **Weiter** und **Ausführen**, um MySQL Server und den ODBC Connector zu installieren.

5. Klicken Sie auf **Weiter**. Wählen Sie unter **Hochverfügbarkeit** die Option **Eigenständige MySQL-Server- / klassische MySQL-Replikation** aus und klicken Sie auf **Weiter**.
6. Wählen Sie unter **Art und Netzwerk** die Option **Servercomputer** im Dropdownmenü **Konfigurationstyp** aus und klicken Sie auf **Weiter**.
7. Wählen Sie unter **Authentifizierungsmethode** die empfohlene Option **Starke Passwortverschlüsselung für die Authentifizierung verwenden** aus und klicken Sie auf **Weiter**.
8. Geben Sie unter **Konten und Rollen** zweimal Ihr **MySQL-Root-Passwort** ein. Außerdem empfehlen wir, ein [speziell eingerichtetes Datenbankkonto zu erstellen](#).
9. Behalten Sie im **Windows-Dienst** die vorausgewählten Werte bei und klicken Sie auf **Weiter**.
10. Klicken Sie auf **Ausführen** und warten Sie, bis die Installation von MySQL Server abgeschlossen wurde. Klicken Sie auf **Fertig, Weiter** und **Fertig stellen**, um das Installationsfenster zu schließen.

Konfiguration

1. Öffnen Sie die folgende Datei in einem Text-Editor:

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

2. Bearbeiten Sie die folgende Konfiguration im Abschnitt `[mysqld]` der Datei `my.ini` bzw. hängen Sie sie an:



- Erstellen Sie den Abschnitt `[mysqld]`, falls er in der Datei noch nicht vorhanden ist.
- Wenn die Parameter nicht in der Datei vorhanden sind, fügen Sie sie zum Abschnitt `[mysqld]` hinzu.
- Führen Sie den folgenden Befehl aus, um Ihre MySQL-Version zu ermitteln: `mysql --version`.

Parameter	Anmerkungen und empfohlene Werte	MySQL version
<code>max_allowed_packet=33M</code>		Alle unterstützten Versionen .
<code>log_bin_trust_function_creators=1</code>	Alternativ können Sie das binäre Logging deaktivieren: <code>log_bin=0</code> .	Unterstützte 8.x-Versionen
<code>innodb_log_file_size=100M</code>	Die Multiplikation der Werte dieser beiden Parameter muss mindestens 200 ergeben. Der Mindestwert für <code>innodb_log_files_in_group</code> ist 2 und der Höchstwert ist 100 . Außerdem muss der Wert eine Ganzzahl sein).	Unterstützte 8x-Versionen 5.7 5.6.22 (und höher 5.6.x)
<code>innodb_log_files_in_group=2</code>		
<code>innodb_log_file_size=200M</code>	Legen Sie den Wert mindestens auf 200M und höchstens auf 3000M fest.	5.6.20 und 5.6.21

3. Speichern und schließen Sie die Datei `my.ini`.
4. Öffnen Sie die Eingabeaufforderung und geben Sie die folgenden Befehle ein, um den MySQL-Server neu zu starten und die Konfiguration zu übernehmen (der Prozessname hängt von der MySQL-Version ab: 8.0 = `mysql80` usw.):

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

5. Geben Sie den folgenden Befehl ein in der Eingabeaufforderung, um zu überprüfen, ob der MySQL-Server gestartet wurde:

```
sc query mysql80
```

Speziell eingerichtetes Datenbankkonto

Falls Sie nicht das **SA-Konto** (MS SQL) bzw. das **root-Konto** (MySQL) verwenden möchten, können Sie ein **speziell eingerichtetes Datenbankkonto** erstellen. Dieses Benutzerkonto wird ausschließlich für den Zugriff auf die ESET PROTECT-Datenbank verwendet. Erstellen Sie nach Möglichkeit ein Datenbankbenutzerkonto auf Ihrem Datenbankserver, bevor Sie mit der Installation von ESET PROTECT beginnen. Außerdem benötigen Sie eine leere Datenbank, die von ESET PROTECT mit diesem Benutzerkonto verwendet werden kann.

Dieses speziell eingerichtete Datenbankbenutzerkonto benötigt einen Mindestsatz an Berechtigungen:

- **MySQL-Benutzerrechte:** ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, SELECT, UPDATE, TRIGGER. - Weitere Informationen zu den MySQL-Berechtigungen finden Sie unter <http://dev.mysql.com/doc/refman/8.0/en/grant.html>.
- **Microsoft SQL Server-Datenbankrollen:** Der ESET PROTECT-Datenbankbenutzer muss Mitglied der Datenbankrolle db_owner sein. Weitere Informationen zu den Microsoft SQL Server-Datenbankrollen finden Sie unter <https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspx>.

Unser [Knowledgebase-Artikel](#) enthält eine ausführliche Anleitung für die Einrichtung von Datenbank und Benutzerkonto für MS SQL und MySQL.

Installation des Agenten – Windows

Verfügbare Methoden

Für die Installation des ESET Management Agenten auf Windows-Arbeitsstationen sind verschiedene Installations- und Bereitstellungsmethoden verfügbar:

Methode	Dokumentation	Beschreibung
GUI-basierte Installation mit dem .msi-Installationsprogramm	<ul style="list-style-type: none"> • Dieses Kapitel • KB 	<ul style="list-style-type: none"> • Die normale Installationsmethode. • Diese Methode kann entweder servergestützt oder offline ausgeführt werden. • Verwenden Sie diese Methode, um den Agenten auf einem ESET PROTECT Server-Computer zu installieren.
ESET Remote Deployment Tool	<ul style="list-style-type: none"> • Onlinehilfe 	<ul style="list-style-type: none"> • Empfohlen für die massenhafte Bereitstellung in einem lokalen Netzwerk. • Kann verwendet werden, um das All-in-One-Installationsprogramm (Agent + ESET-Sicherheitsprodukt) bereitzustellen
All-in-One-Agent-Installationsprogramm	<ul style="list-style-type: none"> • All-in-One-Agent-Installationsprogramm erstellen • KB 	<ul style="list-style-type: none"> • Das Installationsprogramm kann außerdem ein Sicherheitsprodukt und eine eingebettete Policy enthalten. • Das Installationsprogramm ist mehrere Hundert MB groß.
Installations-Skript für Agenten	<ul style="list-style-type: none"> • Installationskript für Agenten erstellen • KB 	<ul style="list-style-type: none"> • Das Installationsprogramm ist ein ausführbares Skript. Das Skript ist klein, benötigt jedoch Zugang zum Speicherort des .msi-Installationsprogramms. • Das Skript kann angepasst werden, um ein lokales Installationsprogramm und einen HTTP-Proxy zu verwenden.
Bereitstellung mit SCCM und GPO	<ul style="list-style-type: none"> • SCCM • GPO • KB 	<ul style="list-style-type: none"> • Erweiterte Methode für die Remote-Massenbereitstellung. • Verwendet eine kleine .ini-Datei.
Server-Task - Agenten-Bereitstellung	<ul style="list-style-type: none"> • Onlinehilfe • KB 	<ul style="list-style-type: none"> • Eine Alternative zu SCCM und GPO. • Ist nicht mit HTTP-Proxy kompatibel. • Ausgeführt vom ESET PROTECT Server über die ESET PROTECT-Web-Konsole.

Das Kommunikationsprotokoll zwischen Agent und ESET PROTECT Server unterstützt keine Authentifizierung. Daher können für die Weiterleitung der Agenten-Kommunikation zum ESET PROTECT Server keine Proxylösungen mit Authentifizierung verwendet werden.

Wenn Sie einen vom Standard abweichenden Port für Web-Konsole oder Agent verwenden, müssen Sie möglicherweise die Firewall anpassen. Andernfalls können bei der Installation Fehler auftreten.

GUI-basierte Installation

Führen Sie die folgenden Schritte aus, um den ESET Management Agenten unter Windows lokal zu installieren:

1. Besuchen Sie den ESET PROTECT-[Downloadbereich](#), um ein eigenständiges Installationsprogramm für diese ESET PROTECT-Komponente herunterzuladen (*agent_x86.msi* oder *agent_x64.msi* oder *agent_arm64.msi*).
2. Führen Sie das Installationsprogramm für den ESET Management Agenten aus und akzeptieren Sie die EULA, falls Sie ihr zustimmen.
3. Deaktivieren Sie das Kontrollkästchen neben **Am Produktverbesserungsprogramm teilnehmen**, falls Sie der Übertragung von Absturzberichten und anonymen Telemetriedaten (Betriebssystemversion und -Typ, ESET-Produktversion und andere produktspezifische Daten) an ESET nicht zustimmen. Wenn Sie dieses Kontrollkästchen aktiviert lassen, werden Telemetriedaten und Absturzberichte an ESET übertragen.
4. Geben Sie **Serverhost** (Name oder IP-Adresse Ihres ESET PROTECT Servers) und **Serverport** (standardmäßig 2222, ersetzen Sie diesen Wert ggf. durch einen benutzerdefinierten Port) ein.

Achten Sie darauf, dass der **Serverhost** mit mindestens einem der Werte (idealerweise dem FQDN) übereinstimmt, die im Feld **Host** des **Serverzertifikats** definiert sind. Andernfalls erhalten Sie die Fehlermeldung "Das empfangene Serverzertifikat ist nicht gültig". Wenn Sie einen Platzhalter (*) im Host-Feld des Serverzertifikats verwenden, funktioniert das Zertifikat für jeden beliebigen **Serverhost**.

5. Aktivieren Sie das Kontrollkästchen neben **Proxy verwenden**, falls Sie einen Proxy für die Verbindung zwischen Agent und Server verwenden. Wenn dieses Feld ausgewählt ist, fährt das Installationsprogramm mit der [Offline-Installation](#) fort.

Diese Proxyeinstellung wird nur für die Replikation zwischen dem ESET Management Agenten und dem ESET PROTECT Server verwendet, nicht für die Zwischenspeicherung von Updates.

- **Proxy-Hostname:** Hostname oder IP-Adresse des HTTP-Proxycomputers.

- **Proxyport:** Standardmäßig 3128.

- **Benutzername, Passwort:** geben Sie die Anmeldeinformationen für Ihren Proxy ein, falls dieser Authentifizierung verwendet.

Sie können die Proxyeinstellungen später in Ihrer [Policy](#) ändern. Sie müssen den [Proxy](#) installieren, bevor Sie eine Verbindung zwischen Agent und Server über einen Proxy konfigurieren können.

6. Wählen Sie eine der folgenden Installationsoptionen und führen Sie die Schritte aus, die in den entsprechenden Abschnitten beschrieben sind:

- [Servergestützte Installation](#) - Für diese Installationsart müssen Sie die Anmeldedaten des Administrators der ESET PROTECT-Web-Konsole eingeben. Das Installationsprogramm lädt die erforderlichen Zertifikate automatisch herunter.



Sie können keinen Benutzer mit [Zwei-Faktor-Authentifizierung](#) für servergestützte Installationen verwenden.

- [Offline-Installation](#) – Geben Sie ein Agentenzertifikat und eine Zertifizierungsstelle an. Beide Werte können aus ESET PROTECT [exportiert](#) werden. Alternativ können Sie Ihr [benutzerdefiniertes Zertifikat](#) verwenden.

Installation über die Befehlszeile

Sie können das *MSI*-Installationsprogramm lokal oder remote ausführen. Laden Sie die den ESET Management Agenten von der ESET-[Website](#) herunter.

Parameter	Beschreibung und zulässige Werte
P_HOSTNAME=	Hostname oder IP-Adresse des ESET PROTECT Servers.
P_PORT=	Serverport für die Agentenverbindung (optional, standardmäßig wird Port 2222 verwendet).
P_CERT_PATH=	Pfad zum Agentenzertifikat im Base64-Format als <i>.txt</i> -Datei (exportiert aus der ESET PROTECT-Web-Konsole).
P_CERT_AUTH_PATH=	Pfad zur Zertifizierungsstelle im Base64-Format als <i>.txt</i> -Datei (exportiert aus der ESET PROTECT-Web-Konsole).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	YES ; Verwenden sie diesen Parameter, falls das Agentenzertifikat und die Zertifizierungsstelle, auf die Sie verwenden, in <i>.txt</i> -Dateien gespeichert sind.
P_CERT_PASSWORD=	Verwenden Sie diesen Parameter, um ein Passwort für das Agentenzertifikat anzugeben.
P_CERT_CONTENT=	Zeichenfolge des Agentenzertifikats im Base64-Format (exportiert aus der ESET PROTECT-Web-Konsole).
P_CERT_AUTH_CONTENT=	Zeichenfolge der Zertifizierungsstelle im Base64-Format (exportiert aus der ESET PROTECT-Web-Konsole).
PASSWORD=	Passwort für die Deinstallation eines passwortgeschützten Agenten .
P_ENABLE_TELEMETRY=	0 - deaktiviert (Standardoption); 1 - aktiviert. Absturzberichte und Telemetriedaten an ESET senden (optionaler Parameter).
P_INSTALL_MODE_EULA_ONLY=	1 ; Verwenden Sie diesen Parameter für eine teilweise unbeaufsichtigte Installation des ESET Management Agenten. Das Fenster für die Agenten-Installation wird geöffnet, und Sie werden aufgefordert, die Endbenutzer-Lizenzvereinbarung zu akzeptieren und die Telemetrie zu aktivieren oder zu deaktivieren (P_ENABLE_TELEMETRY wird ignoriert, falls angegeben). Sonstige Installationseinstellungen für den Agenten werden aus den Befehlszeilenparametern übernommen. Der Fortschritt der Agenten-Installation wird angezeigt.
P_USE_PROXY=	1 ; Verwenden Sie diesen Parameter, um den (bereits in Ihrem Netzwerk installierten) HTTP-Proxy für die Replikation zwischen ESET Management Agent und ESET PROTECT Server zu verwenden (nicht für die Zwischenspeicherung von Updates).
P_PROXY_HTTP_HOSTNAME=	Hostname oder IP-Adresse des HTTP-Proxys.

Parameter	Beschreibung und zulässige Werte
P_PROXY_HTTP_PORT=	Port des HTTP-Proxy für die Agenten-Verbindung.

Beispiele für die Installation über die Befehlszeile

Ersetzen Sie den orangefarbenen Code unten durch Ihre Werte.

- Unbeaufsichtigte Installation (Parameter /q) mit Verbindung zum Standardport, aktivierter Telemetrie und Agentenzertifikat und Zertifizierungsstelle in Dateien gespeichert:

```
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
```

- Unbeaufsichtigte Installation mit Angabe von Zeichenfolgen für Agentenzertifikat, Zertifizierungsstelle, Zertifikatspasswort für den Agenten und HTTP-Proxyparameter:

```
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=45hvkpqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_HTTP_PORT=3128
```

- Teilweise unbeaufsichtigte Installation:

```
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\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

Servergestützte Installation des Agenten

Gehen Sie wie folgt vor, um die **servergestützte Installation des Agenten** fortzusetzen:

1. Geben Sie Hostname oder IP-Adresse Ihrer ESET PROTECT-Web-Konsole (gleiche Werte wie ESET PROTECT Server) in das Feld **Serverhost** ein. Lassen Sie im Feld **Web-Konsolen-Port** den Standardport 2223 unverändert, falls Sie keinen benutzerdefinierten Port verwenden. Geben Sie außerdem die Anmeldedaten für das Web-Konsolen-Konto in die Felder **Benutzername** und **Passwort** ein. Um sich als Domänenbenutzer anzumelden, aktivieren Sie das Kontrollkästchen neben **An Domäne anmelden**.



- Achten Sie darauf, dass **Serverhost** mit mindestens einem der Werte (idealerweise der FQDN) übereinstimmt, die im Feld **Host** des **Serverzertifikats** definiert sind. Andernfalls erhalten Sie die Fehlermeldung "Das empfangene Serverzertifikat ist nicht gültig". Die einzige Ausnahme ist die Angabe von Platzhaltern (*) im Host-Feld des Serverzertifikats. In diesem Fall werden alle **Serverhosts** akzeptiert.
- Sie können keinen Benutzer mit [Zwei-Faktor-Authentifizierung](#) für servergestützte Installationen verwenden.

2. Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob Sie das Zertifikat akzeptieren möchten.

3. Wählen Sie **Computer nicht erstellen (Computer wird bei der ersten Verbindung automatisch erstellt)** oder **Benutzerdefinierte statische Gruppe auswählen** aus. Wenn Sie auf **Benutzerdefinierte statische Gruppe auswählen** klicken, können Sie aus einer Liste vorhandener statischer Gruppen in ESET PROTECT eine Auswahl treffen. Der Computer wird zur ausgewählten Gruppe hinzugefügt.

4. Geben Sie einen Zielordner für den ESET Management Agenten an (nach Möglichkeit der standardmäßige Speicherort), klicken Sie auf **Weiter** und dann auf **Installieren**.

Offline-Installation des Agenten

Gehen Sie wie folgt vor, um die **Offline-Installation des Agenten** fortzusetzen:

1. Falls Sie im vorherigen Schritt die Option **Proxy verwenden** ausgewählt haben, geben Sie den **Proxy-Hostnamen**, den **Proxy-Port** (der Standardport ist 3128), den **Benutzernamen** und das **Passwort** ein, und klicken Sie auf **Weiter**.

2. Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort Ihres Peerzertifikats (das Agentenzertifikat, das Sie aus ESET PROTECT exportiert haben). Lassen Sie das Textfeld **Zertifikatspasswort** leer, da für dieses Zertifikat kein Passwort erforderlich ist. Sie müssen keine **Zertifizierungsstelle** suchen. Lassen Sie dieses Feld leer.



Wenn Sie ein benutzerdefiniertes Zertifikat mit ESET PROTECT verwenden (anstelle des standardmäßigen Zertifikats, das bei der Installation von ESET PROTECT automatisch generiert wurde), geben Sie dies entsprechend an.



Die Zertifikat-Passphrase darf die folgenden Zeichen nicht enthalten: " \ Diese Zeichen verursachen kritische Fehler bei der Initialisierung des Agenten.

3. Klicken Sie auf **Weiter**, um die Installation im standardmäßigen Ordner auszuführen, oder auf **Ändern**, um einen anderen Ordner auszuwählen. Wir empfehlen, den standardmäßigen Speicherort beizubehalten.

ESET Remote Deployment Tool

Das ESET Remote Deployment Tool ist ein praktischer Weg, um das mit ESET PROTECT erstellte [Installationspaket](#) zu verteilen und den ESET Management Agenten und die ESET-Sicherheitsprodukte remote auf Computern im Netzwerk bereitzustellen.

Das ESET Remote Deployment Tool ist auf der ESET-[Webseite](#) kostenlos als eigenständige ESET PROTECT-Komponente verfügbar. Das Deployment Tool eignet sich hauptsächlich für die Bereitstellung in kleinen und mittelgroßen Netzwerken und wird mit Administratorberechtigungen ausgeführt.



Das ESET Remote Deployment Tool stellt ESET Management Agenten auf Clientcomputern mit [unterstützten](#) Microsoft Windows-Betriebssystemen bereit.

Weitere Informationen zu Voraussetzungen und zur Nutzung des Tools finden Sie im Kapitel [ESET Remote](#)

Installation der Web-Konsole – Windows

Sie können die ESET PROTECT-Web-Konsole unter Windows auf zwei Arten installieren:

- Wir empfehlen, das [All-in-One-Installationsprogramm zu verwenden](#).
- Fachkundige Benutzer können eine [manuelle Installation](#) ausführen.

i Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server.

Web-Konsole mit dem All-in-One-Installationsprogramm installieren

Voraussetzungen

- ESET PROTECT Server installiert.

i Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server. Für diese Prozedur sind [zusätzliche Schritte](#) erforderlich.

- Apache Tomcat wird für die Ausführung der ESET PROTECT-Web-Konsole benötigt.
- Apache Tomcat benötigt Java/OpenJDK (64-Bit). Falls Sie mehrere Java-Versionen auf Ihrem System installiert haben, empfehlen wir, die älteren Java-Versionen zu deinstallieren und nur die neueste [unterstützte Java](#)-Version zu behalten.



Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).

Installation

So installieren Sie die ESET PROTECT-Web-Konsole unter Windows mit dem All-in-One-Installationsprogramm:



Vergewissern Sie sich, dass alle oben genannten Installationsvoraussetzungen erfüllt sind.

1. Laden Sie das [All-in-One-Installationsprogramm für ESET PROTECT](#) von der ESET-Website herunter und entpacken Sie die heruntergeladene Datei.
2. Falls Sie die neueste Version von Apache Tomcat installieren möchten und das All-in-One-Installationsprogramm eine ältere Version von Apache Tomcat enthält (Dieser Schritt ist optional. Überspringen Sie Schritt 4, falls Sie nicht die neueste Version von Apache Tomcat benötigen):
 - a. Öffnen Sie den Ordner *x64* und navigieren Sie zum Ordner *installers*.

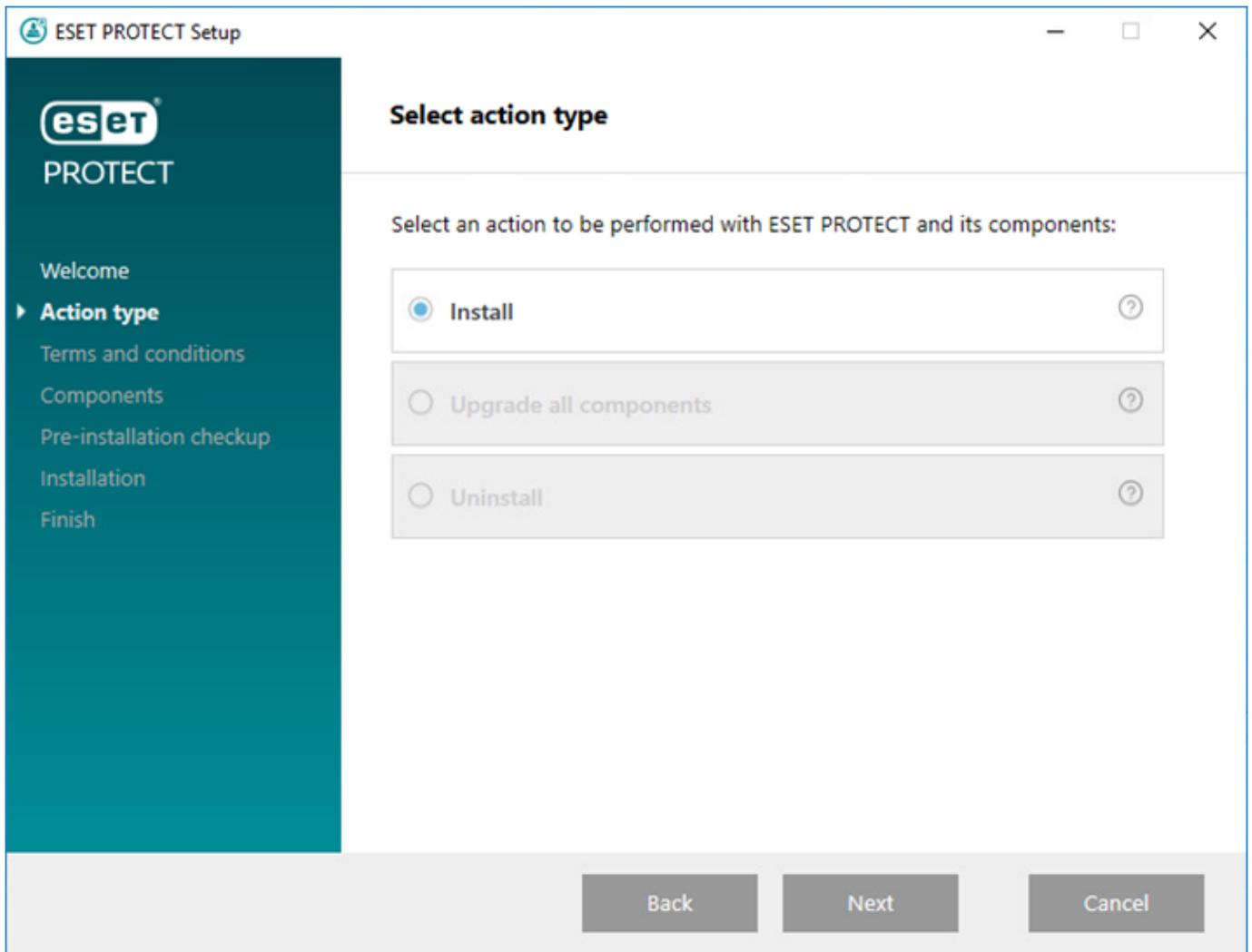
b. Entfernen Sie die Datei *apache-tomcat-9.0.x-windows-x64.zip* im Ordner *installers*.

c. Laden Sie das Paket Apache Tomcat 9 [64-bit Windows Zip](#) herunter.

d. Verschieben Sie das heruntergeladene Zip-Paket in den Ordner *installers*.

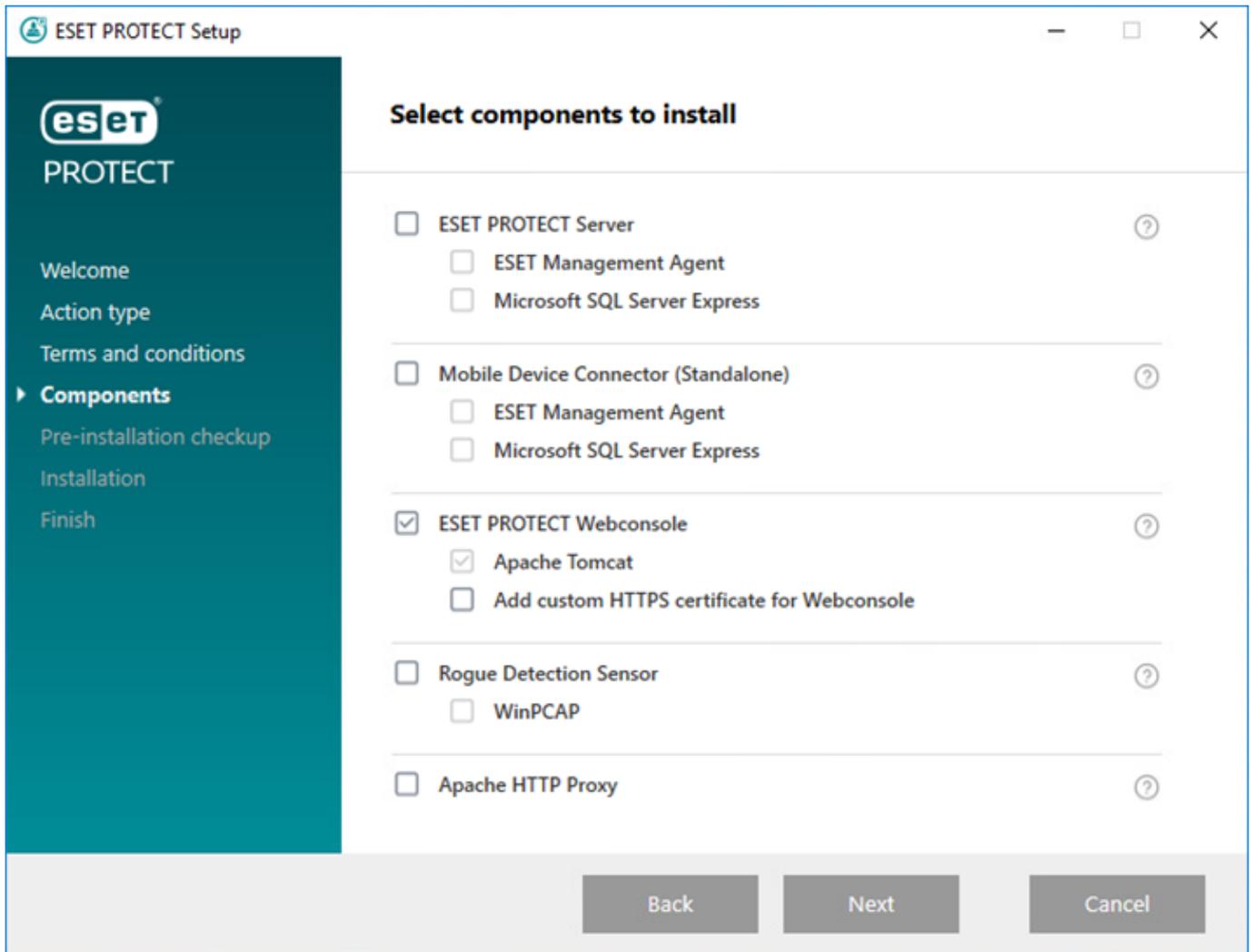
3. Um das All-in-One-Installationsprogramm zu starten, doppelklicken Sie auf die Daten *Setup.exe* und klicken Sie auf **Weiter** im **Willkommensbildschirm**.

4. Wählen Sie **Installieren** aus und klicken Sie auf **Weiter**.



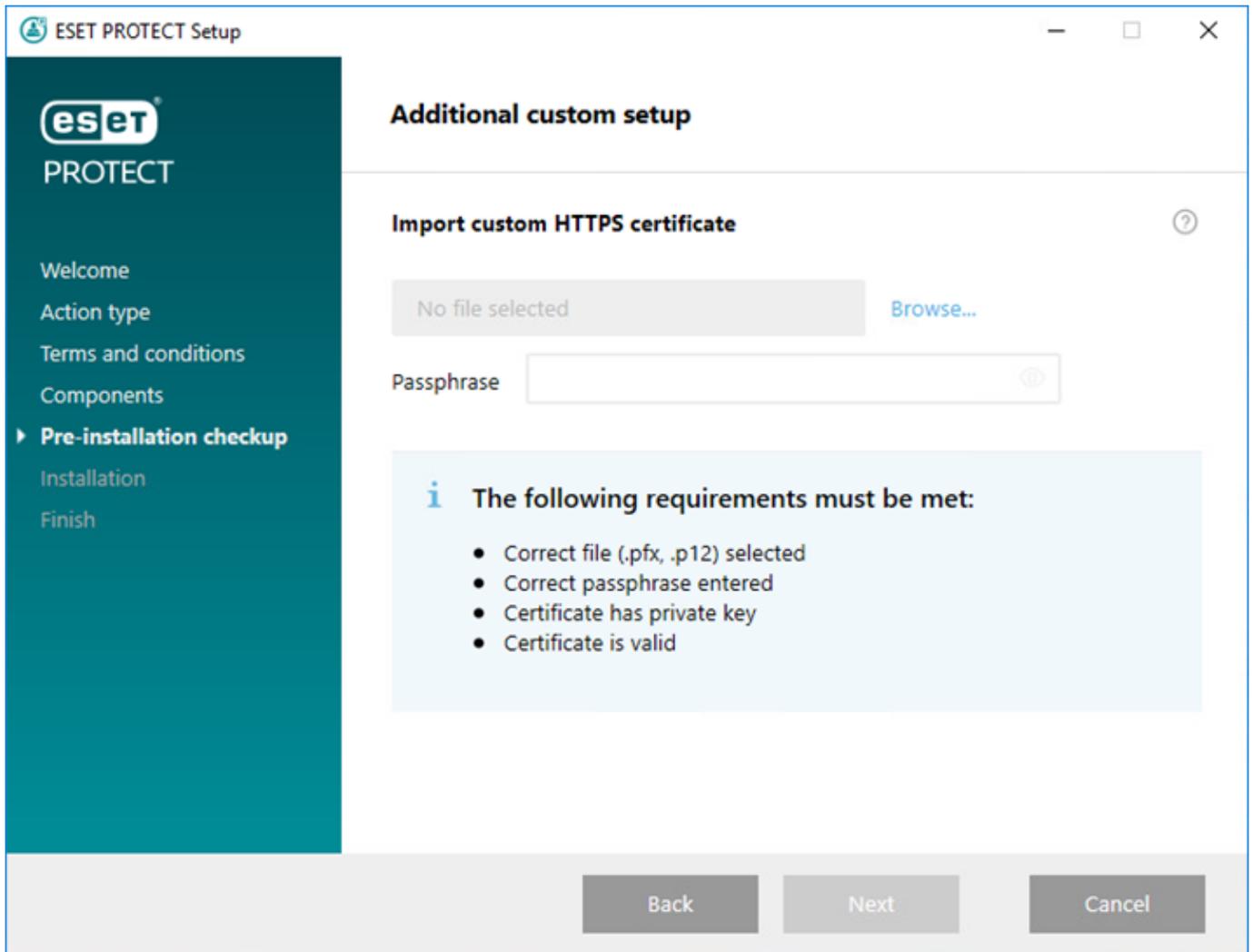
5. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.

6. Aktivieren Sie unter **Wählen Sie die zu installierenden Komponenten aus** nur das Kontrollkästchen für die **ESET PROTECT-Web-Konsole** und klicken Sie auf **Weiter**.



Aktivieren Sie optional das Kontrollkästchen **Benutzerdefiniertes HTTPS-Zertifikat für Web-Konsole hinzufügen**.

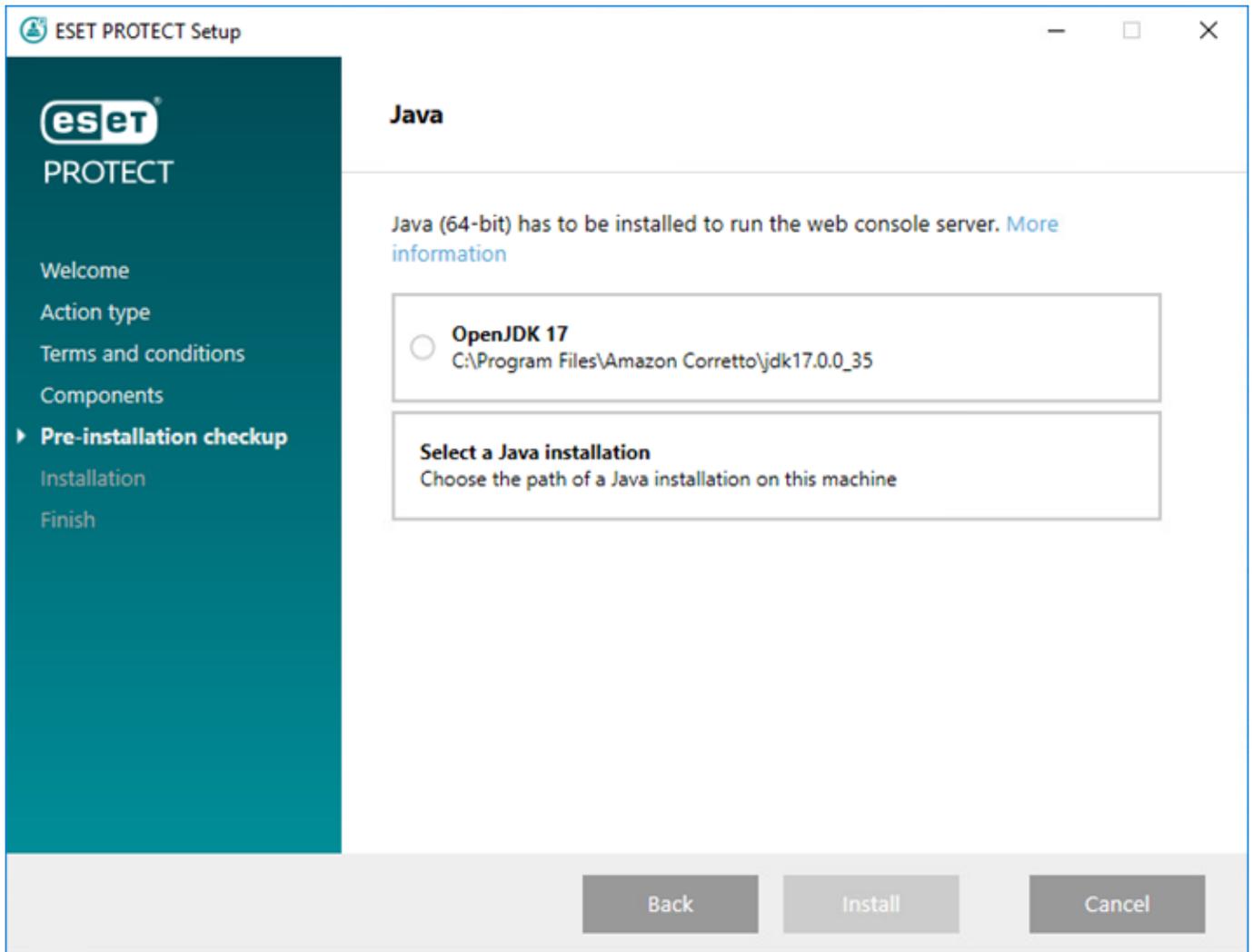
- Wählen Sie diese Option aus, wenn Sie ein benutzerdefiniertes HTTPS-Zertifikat für die ESET PROTECT-Web-Konsole verwenden möchten.
- Wenn Sie diese Option nicht auswählen, generiert das Installationsprogramm automatisch einen neuen Tomcat-Schlüsselspeicher (ein selbstsigniertes HTTPS-Zertifikat).
- Falls Sie **Benutzerdefiniertes HTTPS-Zertifikat für Web-Konsole hinzufügen** ausgewählt haben, klicken Sie auf **Durchsuchen** und wählen Sie ein gültiges Zertifikat aus (.pfx- oder .p12-Datei) und geben Sie die **Passphrase** für das Zertifikat ein (bzw. lassen Sie das Feld leer, falls keine Passphrase festgelegt ist). Das Installationsprogramm installiert das Zertifikat für den Zugriff auf die Web-Konsole auf Ihrem Tomcat-Server. Klicken Sie auf **Weiter**, um fortzufahren.



7. Wählen Sie eine Java-Installation auf dem Computer aus. Überprüfen Sie, ob Sie die neueste Version von Java/OpenJDK verwenden.

a) Um die bereits installierte Java-Version auszuwählen, klicken Sie auf **Java-Installation auswählen**, wählen Sie den Java-Installationsordner aus (mit *bin*-Unterordner, zum Beispiel *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) und klicken Sie auf **OK**. Falls Sie einen ungültigen Pfad ausgewählt haben, wird ein Hinweis angezeigt.

b) Klicken Sie auf **Installieren**, um fortzufahren, oder auf **Ändern**, um den Java-Installationspfad zu ändern.



8. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.

Wenn Sie die ESET PROTECT-Web-Konsole nicht auf demselben Computer wie den ESET PROTECT Server installiert haben, führen Sie diese zusätzlichen Schritte aus, um die Kommunikation zwischen der ESET PROTECT-Web-Konsole und dem ESET PROTECT Server zu ermöglichen:

a) Halten Sie den Apache Tomcat-Dienst an. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Beenden** aus.

 b) Führen Sie Notepad als Administrator aus und bearbeiten Sie die Datei `C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.

c) Suchen Sie nach dem Eintrag `server_address=localhost`.

d) Ersetzen Sie `localhost` durch die IP-Adresse Ihres ESET PROTECT Servers und speichern Sie die Datei.

e) Neu starten Sie den Apache Tomcat-Dienst neu. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Starten** aus.

9. Öffnen Sie die ESET PROTECT-Web-Konsole in einem [unterstützten Webbrowser](#): Ein Anmeldebildschirm wird angezeigt.

- Auf dem Computer, auf dem die ESET PROTECT-Web-Konsole gehostet wird: `https://localhost/era`

- Auf einem beliebigen Computer mit Internetzugriff auf die ESET PROTECT-Web-Konsole (ersetzen Sie `IP_ADDRESS_OR_HOSTNAME` durch die IP-Adresse oder den Hostnamen Ihrer ESET PROTECT-Web-Konsole): `https://IP_ADDRESS_OR_HOSTNAME/era`

 Siehe auch die zusätzliche [Konfiguration der Web-Konsole für Enterprise-Lösungen oder leistungsschwache Systeme](#).

Web-Konsole manuell installieren

 Die manuelle Installation der ESET PROTECT-Web-Konsole wird nur für fachkundige Benutzer empfohlen. Wir empfehlen, die ESET PROTECT-Web-Konsole mit dem [All-in-One-Installationsprogramm](#) zu installieren.

Voraussetzungen

- ESET PROTECT Server installiert.

 Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server. Für diese Prozedur sind [zusätzliche Schritte](#) erforderlich.

- Apache Tomcat wird für die Ausführung der ESET PROTECT-Web-Konsole benötigt. Apache Tomcat installieren:
 - a) Laden Sie die [aktuelle Version](#) der Apache Tomcat-Installationsdatei (32-Bit- bzw. 64-Bit-Windows Service-Installationsprogramm) *apache-tomcat-[Version].exe* von <https://tomcat.apache.org> herunter.
 - a) Führen Sie das Installationsprogramm aus.
 - b) Wählen Sie während der Installation den Pfad zu Java (übergeordneter Ordner von Java *bin* und *lib*) aus und aktivieren Sie das Kontrollkästchen **Run Apache Tomcat**.
 - c) Vergewissern Sie sich nach der Installation, dass der Apache Tomcat-Dienst ausgeführt wird und dass der Starttyp des Diensts in **services.msc** auf **Automatisch** festgelegt ist.
- Apache Tomcat benötigt Java/OpenJDK (64-Bit). Falls Sie mehrere Java-Versionen auf Ihrem System installiert haben, empfehlen wir, die älteren Java-Versionen zu deinstallieren und nur die neueste [unterstützte Java](#)-Version zu behalten.

 Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).

Installation

Führen Sie diese Schritte aus, um die ESET PROTECT-Web-Konsole unter Windows zu installieren:

 Vergewissern Sie sich, dass alle oben genannten Installationsvoraussetzungen erfüllt sind.

1. Besuchen Sie den ESET PROTECT-[Downloadbereich](#), um ein eigenständiges Installationsprogramm für diese ESET PROTECT-Komponente herunterzuladen (Web-Konsole *era.war*).
2. Kopieren Sie die Datei *era.war* in den Tomcat-Ordner für Webanwendungen:

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

3. Apache Tomcat extrahiert die Datei *era.war* automatisch in den Ordner *era* und installiert die ESET PROTECT-Web-Konsole. Warten Sie einige Minuten, bis die Extraktion abgeschlossen wurde. Führen Sie die [Fehlerbehebungsschritte](#) aus, falls die Extraktion nicht ausgeführt wird.

4. Falls Sie die ESET PROTECT-Web-Konsole auf demselben Computer wie den ESET PROTECT Server installiert haben, starten Sie den Apache Tomcat-Dienst neu. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Beenden** aus. Klicken Sie auf Anhalten, warten Sie 30 Sekunden lang und klicken Sie auf **Start**.

Wenn Sie die ESET PROTECT-Web-Konsole nicht auf demselben Computer wie den ESET PROTECT Server installiert haben, führen Sie diese zusätzlichen Schritte aus, um die Kommunikation zwischen der ESET PROTECT-Web-Konsole und dem ESET PROTECT Server zu ermöglichen:

a) Halten Sie den Apache Tomcat-Dienst an. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Beenden** aus.

! b) Führen Sie Notepad als Administrator aus und bearbeiten Sie die Datei *C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.

c) Suchen Sie nach dem Eintrag `server_address=localhost`.

d) Ersetzen Sie `localhost` durch die IP-Adresse Ihres ESET PROTECT Servers und speichern Sie die Datei.

e) Neu starten Sie den Apache Tomcat-Dienst neu. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Starten** aus.

5. Wenn Sie die ESET PROTECT-Web-Konsole in einem [unterstützten Webbrowser](#) öffnen, wird ein Anmeldebildschirm angezeigt:

- Auf dem Computer, auf dem die ESET PROTECT-Web-Konsole gehostet wird: *http://localhost:8080/era*
- Auf einem beliebigen Computer mit Internetzugriff auf die ESET PROTECT-Web-Konsole (ersetzen Sie *IP_ADDRESS_OR_HOSTNAME* durch die IP-Adresse oder den Hostnamen Ihrer ESET PROTECT-Web-Konsole): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

6. Konfigurieren Sie die Web-Konsole nach der Installation:

- Der HTTP-Port wird bei der manuellen Installation von Apache Tomcat standardmäßig auf 8080 festgelegt. Wir empfehlen, eine [HTTPS-Verbindung für Apache Tomcat](#) einzurichten.
- Siehe auch die zusätzliche [Konfiguration der Web-Konsole für Enterprise-Lösungen oder leistungsschwache Systeme](#).

Installation des HTTP-Proxy

Über den HTTP-Proxy

Der HTTP-Proxy weiterleitet die verschlüsselte Kommunikation zwischen ESET Management Agent und ESET PROTECT Server weiter. Standardmäßig verwendet ESET PROTECT Apache HTTP Proxy als HTTP-Proxy.

Verwenden Sie den HTTP-Proxy nur, wenn sich Ihre ESET Management Agenten nicht über das Netzwerk mit ESET PROTECT verbinden können. Der HTTP-Proxy ist nicht dafür zuständig, die Kommunikation zu aggregieren oder den Netzwerkverkehr zu reduzieren.

Es ist zwar empfehlenswert, den ESET Management Agent auf dem HTTP-Proxycomputer zu installieren, jedoch nicht zwingend erforderlich. Der ESET Management Agent kann die HTTP-Proxyanwendung nicht verwalten (konfigurieren).

- [Architektur mit HTTP-Proxy](#)
- [Architektur mit Apache HTTP Proxy](#)
- [Komplexere Szenarien mit HTTP-Proxy](#)

Vor der Installation



Das Kommunikationsprotokoll zwischen Agent und ESET PROTECT Server unterstützt keine Authentifizierung. Daher können für die Weiterleitung der Agenten-Kommunikation zum ESET PROTECT Server keine Proxylösungen mit Authentifizierung verwendet werden. Wenn Sie einen vom Standard abweichenden Port für Web-Konsole oder Agent verwenden, müssen Sie möglicherweise die Firewall anpassen. Andernfalls können bei der Installation Fehler auftreten.

Installation und Konfiguration

Sie können den Apache HTTP Proxy mit einem separaten Installationsprogramm oder mit dem ESET PROTECT All-in-One-Installationsprogramm installieren.

- Wenn Sie das All-in-One-Installationsprogramm verwenden, müssen Sie zwar das ganze Paket [herunterladen](#), aber der eigentliche Vorgang ist einfacher. Führen Sie das heruntergeladene Installationsprogramm aus und wählen Sie im Auswahlménü nur die Option **Apache HTTP Proxy** aus. Apache muss nach der Installation [konfiguriert](#) werden.
- Die Installation mit dem [eigenständigen](#) Installationsprogramm ist etwas komplizierter, aber der Download ist nur wenige MB groß. Weitere Informationen finden Sie in den [Installations-](#) und [Konfigurationsanleitungen](#).

Konfigurieren Sie den HTTP-Proxy für eine große Anzahl von Clients

Wenn Sie die 64-Bit-Version des Apache HTTP-Proxy verwenden, können Sie das Thread-Limit für Ihren Apache HTTP Proxy erhöhen. Bearbeiten Sie die Konfigurationsdatei *httpd.conf* in Ihrem Apache HTTP Proxy-Ordner. Suchen Sie die folgenden Einstellungen in der Datei und passen Sie die Werte an die Anzahl Ihrer Clients an.

Ersetzen Sie den Beispielwert 5000 durch den gewünschten Wert. Der Höchstwert ist 32000.

```
ThreadLimit 5000
```

```
ThreadsPerChild 5000
```

Ändern Sie den Rest der Datei nicht.

RD Sensor-Installation – Windows

Voraussetzungen

- [WinPcap](#) - verwenden Sie die neueste WinPcap-Version (mindestens 4.1.0)

- Das Netzwerk muss korrekt konfiguriert sein (entsprechende [Ports](#) geöffnet, eingehende Kommunikation nicht durch Firewall blockiert usw.)
- ESET PROTECT Server ist erreichbar
- Der ESET Management Agent muss auf dem lokalen Computer installiert sein, um alle Programmfunktionen vollständig zu unterstützen
- Die Log-Datei des Rogue Detection Sensor befindet sich unter Log-Dateien: `C:\ProgramData\ESET\Rogue Detection Sensor\Logs\`

Installation

Führen Sie die folgenden Schritte aus, um die RD Sensor-Komponente unter Windows zu installieren:

 Vergewissern Sie sich, dass alle oben genannten Installationsvoraussetzungen erfüllt sind.

1. Besuchen Sie den ESET PROTECT-[Downloadbereich](#), um ein eigenständiges Installationsprogramm für diese ESET PROTECT-Komponente herunterzuladen (`rdsensor_x86.msi` oder `rdsensor_x64.msi`).
2. Doppelklicken Sie auf die RD Sensor-Installationsdatei, um die Installation zu beginnen.
3. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.
4. Deaktivieren Sie das Kontrollkästchen neben **Am Produktverbesserungsprogramm teilnehmen**, falls Sie der Übertragung von Absturzberichten und anonymen Telemetriedaten (Betriebssystemversion und -Typ, ESET-Produktversion und andere produktspezifische Daten) an ESET nicht zustimmen. Wenn Sie dieses Kontrollkästchen aktiviert lassen, werden Telemetriedaten und Absturzberichte an ESET übertragen.
5. Wählen Sie den Installationsort für RD Sensor aus und klicken Sie auf **Weiter > Installieren**.

 Falls Sie mehrere Netzwerksegmenten verwenden, müssen Sie den Rogue Detection Sensor in jedem Netzwerksegment separat installieren, um eine umfassende Liste aller Geräte im gesamten Netzwerk zu erstellen.

Mirror-Tool - Windows

[Sind Sie Linux-Benutzer?](#)

Das Mirror-Tool wird für Updates der Erkennungsroutine im Offlinemodus benötigt. Falls Ihre Clientcomputer nicht mit dem Internet verbunden sind und Updates die Erkennungsroutine brauchen, können Sie die Update-Dateien mit dem Mirror-Tool von den ESET-Updateservern herunterladen und lokal speichern.

 Das Mirror-Tool lädt nur Updates für die Erkennungsroutine und andere Programm-Module herunter, keine PCUs (Updates für Programmkomponenten) oder ESET LiveGrid®-Daten. Das Tool kann außerdem ein vollständiges [Offline-Repository](#) erstellen. Alternativ können Sie die Produkte einzeln aktualisieren.

Voraussetzungen

 Windows XP und Windows Server 2003 werden vom Mirror-Tool nicht unterstützt.

- Der Zielordner muss für die Freigabe, den Samba/Windows- oder den HTTP/FTP-Dienst verfügbar sein, je nachdem, wie Sie die Updates bereitstellen möchten.

OESET Sicherheitsprodukte für Windows – Updates können remote per HTTP oder mit einem freigegebenen Ordner ausgeführt werden.

OESET Sicherheitsprodukte für Linux/macOS – Updates können remote nur per HTTP ausgeführt werden. Wenn Sie einen freigegebenen Ordner verwenden, muss dieser sich auf demselben Computer befinden wie das ESET Sicherheitsprodukt.

- Sie benötigen eine gültige [Offline-Lizenzdatei](#) inklusive Benutzername und Passwort. Achten Sie beim Generieren der Lizenzdatei darauf, das Kontrollkästchen neben der Option **Benutzername und Passwort einschließen** zu markieren. Geben Sie außerdem einen **Lizenznamen** an. Sie benötigen eine Offline-Lizenzdatei, um das Mirror-Tool zu aktivieren und den Update-Mirror zu generieren.

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

- Um das Mirror-Tool ausführen zu können, müssen Sie die folgenden Pakete installieren:
- [Visual C++ Redistributable für Visual Studio 2010](#)
- [Visual C++ 2015 Redistributable x86](#)

Verwenden des Mirror-Tools

1. Laden Sie das Mirror-Tool auf der [ESET-Downloadseite](#) (Bereich **Standalone-Installationsprogramme**) herunter.
2. Extrahieren Sie den heruntergeladenen Archiv.
3. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Ordner mit der Datei *MirrorTool.exe*.
4. Führen Sie den folgenden Befehl aus, um alle verfügbaren Parameter für das Mirror-Tool und dessen Version anzuzeigen:

```
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 Sämtliche Filter unterscheiden zwischen Groß- und Kleinschreibung.

Parameter	Beschreibung
--updateServer	Wenn Sie diesen Parameter verwenden, müssen Sie die komplette URL des Updateservers angeben.
--offlineLicenseFilename	Geben Sie einen Pfad zu Ihrer Offline-Lizenzdatei an (siehe oben).
--mirrorOnlyLevelUpdates	Kein Argument erforderlich. Wenn diese Option festgelegt ist, werden nur Level-Updates heruntergeladen (Nano-Updates werden nicht heruntergeladen). Weitere Informationen zu Updatetypen finden Sie in unserem Knowledgebase-Artikel .
--mirrorFileFormat	<div style="border: 1px solid red; padding: 5px;"> <p>⚠ Stellen Sie vor der Verwendung des --mirrorFileFormat Parameters sicher, dass Ihre Umgebung keine Mischung aus älteren (6.5 und älter) und neueren Versionen (6.6 und neuer) des ESET-Sicherheitsprodukts enthält. Fehler bei der Verwendung dieses Parameters können dazu führen, dass Ihre ESET-Sicherheitsprodukte falsch aktualisiert werden.</p> </div> <p>Sie können festlegen, welche Art von Updatedateien heruntergeladen werden sollen. Mögliche Werte (Groß-/Kleinschreibung beachten):</p> <ul style="list-style-type: none"> • dat - Verwenden Sie diesen Wert, falls Sie in Ihrer Version nur Version 6.5 und älter des ESET-Sicherheitsprodukts verwenden. • dll - Verwenden Sie diesen Wert, falls Sie in Ihrer Version nur Version 6.6 und neuer des ESET-Sicherheitsprodukts verwenden.
--compatibilityVersion	<p>Der Parameter wird beim Erstellen eines Mirrors für veraltete Produkte (<i>ep4, ep5</i>) ignoriert. Dieser optionale Parameter gilt für das Mirror-Tool, das zusammen mit ESET PROTECT 8.1 und neueren Versionen verteilt wird.</p> <p>Das Mirror-Tool lädt Updatedateien herunter, die mit der ESET PROTECT Repository-Version kompatibel sind, die Sie im Parameterargument im Format <i>x.x</i> oder <i>x.x.x.x</i> angeben, z. B. <code>--compatibilityVersion 9.1</code> oder <code>--compatibilityVersion 8.1.13.0</code>.</p>

Um weniger Daten aus dem ESET-Repository herunterzuladen, können Sie die neuen Parameter im Mirror-Tool verwenden, das mit ESET PROTECT 9 ausgeliefert wird: `--filterFilePath` und `--dryRun`:

1. Erstellen Sie einen Filter im *JSON*-Format (siehe `--filterFilePath` unten).
- i** 2. Testen Sie das Mirror-Test-Tool mit dem Parameter `--dryRun` (siehe unten) und passen Sie den Filter bei Bedarf an.
3. Führen Sie das Mirror-Tool mit dem Parameter `--filterFilePath` und dem definierten Downloadfilter zusammen mit den Parametern `--intermediateRepositoryDirectory` und `--outputRepositoryDirectory` aus.
4. Führen Sie das Mirror-Tool regelmäßig aus, um immer die neuesten Installationsprogramme zu verwenden.

Parameter	Beschreibung
<p><code>--filterFilePath</code></p>	<p>Verwenden Sie diesen optionalen Parameter, um ESET Sicherheitsprodukte anhand einer Textdatei im <i>JSON</i>-Format zu filtern, die sich im gleichen Ordner wie das Mirror-Tool befindet, z. B.: <code>--filterFilePath filter.txt</code></p> <p>Beschreibung der Filterkonfiguration:</p> <p>Die Konfigurationsdatei für die Produktfilterung hat die folgende <i>JSON</i>-Struktur:</p> <ul style="list-style-type: none"> • <i>JSON</i>-Stammobjekt: <ul style="list-style-type: none"> • <code>use_legacy</code> (boolescher Wert, optional) – Wenn dieser Wert gleich „Wahr“ ist, werden veraltete Produkte einbezogen. • <code>defaults</code> (<i>JSON</i>-Objekt, optional) – Definiert die Filtereigenschaften, die auf alle Produkte angewendet werden. <ul style="list-style-type: none"> ■ <code>languages</code> (Liste) – Geben Sie ISO-Sprachcodes für die Sprachen an, die einbezogen werden sollen, z. B. "fr_FR" für Französisch. In der folgenden Tabelle finden Sie weitere Sprachcodes. Geben Sie weitere Sprachen mit Komma und Leerzeichen getrennt ein, zum Beispiel: (["en_US", "zh_TW", "de_DE"]) ■ <code>platforms</code> (Liste) – Plattformen, die einbezogen werden sollen (["x64", "x86", "arm64"]). <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p> Verwenden Sie den <code>platforms</code>-Filter mit Bedacht. Wenn das Mirror-Tool beispielsweise nur 64-Bit-Installationsprogramme herunterlädt und Ihre Infrastruktur 32-Bit-Computer enthält, können die 64-Bit ESET Sicherheitsprodukte nicht auf den 32-Bit-Computern installiert werden.</p> </div> <ul style="list-style-type: none"> ■ <code>os_types</code> (Liste) – Betriebssystemtypen, die einbezogen werden sollen (["windows"], ["linux"], ["mac"]). • <code>products</code> (Liste der <i>JSON</i>-Objekte, optional) – Filter, die auf bestimmte Produkte angewendet werden, überschreibt <code>defaults</code> für bestimmte Produkte. Die Objekte haben die folgenden Eigenschaften: <ul style="list-style-type: none"> ■ <code>app_id</code> (Zeichenfolge) – Erforderlich, wenn <code>name</code> nicht angegeben wird. ■ <code>name</code> (Zeichenfolge) – Erforderlich, wenn <code>app_id</code> nicht angegeben wird. ■ <code>version</code> (Zeichenfolge) – Gibt an, welche Version oder welcher Versionsbereich einbezogen werden soll. ■ <code>languages</code> (Zeichenfolge) – ISO-Sprachcodes der Sprachen, die einbezogen werden sollen (siehe Tabelle unten). ■ <code>platforms</code> (Liste) – Plattformen, die einbezogen werden sollen (["x64", "x86", "arm64"]). ■ <code>os_types</code> (Liste) – Betriebssystemtypen, die einbezogen werden sollen (["windows"], ["linux"], ["mac"]). <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p> Um angemessene Werte für die Felder zu ermitteln, führen Sie das Mirror-Tool im Dry-Run-Modus aus und suchen Sie in der erstellten CSV-Datei nach dem entsprechenden Produkt.</p> </div> <p>Format für Versionszeichenfolgen</p> <p>Alle Versionsnummern bestehen aus vier Ziffern, die durch Punkte getrennt sind (z. B. 7.1.0.0). Wenn Sie in Versionsfiltern weniger Zahlen angeben (z. B. 7.1), werden Nullen für die restlichen Zahlen angenommen (7.1 entspricht 7.1.0.0).</p> <p>Versionszeichenfolgen können eines der beiden folgenden Formate haben:</p> <ul style="list-style-type: none"> • <code>[> < >= <= <=>]<n>.<n>.<n>.<n></code> <p>OWählt Versionen größer/kleiner oder gleich/kleiner oder gleich/gleich der angegebenen Version aus.</p> <ul style="list-style-type: none"> • <code><n>.<n>.<n>.<n> - <n>.<n>.<n>.<n></code> <p>OWählt Versionen aus, die größer oder gleich der unteren Grenze und kleiner oder gleich der oberen Grenze sind.</p> <p>Vergleiche werden numerisch für alle Teile der Versionsnummer von links nach rechts durchgeführt.</p> <div style="border: 1px solid green; padding: 10px; margin: 10px 0;"> <p>JSON-Beispiel</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": ">7.1.0.0" }] } </pre> </div>

Parameter	Beschreibung
--dryRun	<p>Wenn Sie diesen optionalen Parameter verwenden, lädt das Mirror-Tool keine Dateien herunter, generiert jedoch eine .csv-Datei mit allen Paketen, die heruntergeladen werden.</p> <p>Sie können diesen Parameter ohne die Pflichtparameter --intermediateRepositoryDirectory und --outputRepositoryDirectory verwenden, z. B.: <code>MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv</code>.</p> <div style="border: 1px solid #00aaff; padding: 5px;"> <p>i Manche ESET Installationsprogramme sind sprachunabhängig (Sprachcode <code>multilang</code>). Das Mirror-Tool listet diese Versionen in der .csv-Datei auf, auch wenn Sie Sprachen in --filterFilePath angegeben haben.</p> </div> <p>Wenn Sie den Parameter --dryRun und die Parameter --intermediateRepositoryDirectory und --outputRepositoryDirectory verwenden, löscht das Mirror-Tool das <code>outputRepositoryDirectory</code> nicht.</p>
--listUpdatableProducts	<p>Listet alle ESET Produkte auf, für die das Mirror Tool Modul-Updates herunterladen kann (sofern --excludedProducts nicht verwendet wird).</p> <p>Der Parameter ist ab den folgenden Mirror Tool Versionen verfügbar: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).</p>

Das Mirror-Tool erstellt eine andere Ordnerstruktur als der Endpoint-Mirror. Jeder Ordner enthält die Updatedateien für eine Gruppe von Produkten. Sie müssen den vollständigen Pfad zum korrekten Ordner in den Update-Einstellungen des Produkts angeben, das den Mirror verwendet.



Beispiel: Um ESET PROTECT 9 über den Mirror zu aktualisieren, legen Sie den [Update-Server](#) wie folgt fest (abhängig vom Stamm Ihres HTTP-Servers):

`http://your_server_address/mirror/ eset_upd/era6`

Hinweis: Die folgenden ESET Remote Management-Lösungen verwenden denselben era6 Mirror-Ordner: ERA 6, ESMC 7, ESET PROTECT.

[Tabelle mit Sprachcodes](#)

--	--	--	--	--	--

```
MirrorTool.exe --mirrorType regular ^
--intermediateUpdateDirectory c:\temp\mirrorTemp ^
--offlineLicenseFilename c:\temp\offline.lf ^
--outputDirectory c:\temp\mirror
```

Im folgende Beispiel sehen Sie eine komplexere Konfiguration für ein Offline-Repository mit ausgewählten Produkten und Sprachen und aktiviertem Download von veralteten Dateien in der Datei `filter.txt` (siehe Details zu --filterFilePath weiter oben für Beispiele zum Dateiinhalt):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory c:\temp\repoTemp ^
--outputRepositoryDirectory c:\temp\repository ^
--filterFilePath filter.txt
```

Mirror-Tool und Updateeinstellungen

- Sie können die Ausführung des Mirror-Tools planen, um die Downloads von Modulupdates zu

automatisieren. Navigieren Sie dazu in der Web-Konsole zu **Client-Tasks > Betriebssystem > Befehl ausführen**. Wählen Sie **Auszuführende Befehlszeile** (inklusive Pfad zum *MirrorTool.exe*) und einen passenden Auslöser aus (z. B. CRON für jede Stunde um 0 0 * * * ? *). Alternativ können Sie den Windows-Taskplaner oder Cron in Linux verwenden.

- Erstellen Sie eine neue Policy und verweisen Sie im Feld **Updateserver** auf Ihren Mirror-Server bzw. Ihren freigegebenen Ordner, um Updates auf Clientcomputern zu konfigurieren.

 Falls Sie einen HTTPS-Mirror-Server verwenden, müssen Sie das Zertifikat des Servers in den vertrauenswürdigen Stammspeicher auf dem Clientcomputer importieren. Siehe [Installieren des vertrauenswürdigen Stammzertifikats](#) in Windows.

 Lesen Sie [diesen Knowledgebase-Artikel](#) zum Einrichten der Verkettung für das Mirror-Tool (Mirror-Tool für den Download von Updates von einem anderen Mirror-Tool konfigurieren).

Mobile Device Connector-Installation – Windows

 Der Mobile Device Connector muss jederzeit über das Internet verfügbar sein, um die Mobilgeräte jederzeit und unabhängig von ihrem Standort verwalten zu können.

 Stellen Sie Ihre MDM-Komponente nach Möglichkeit nicht auf demselben Hostgerät wie den ESET PROTECT Server bereit.

Führen Sie die folgenden Schritte aus, um die Mobile Device Connector-Komponente für ESET PROTECT Server unter Windows zu installieren:

 Vergewissern Sie sich, dass alle [Installationsvoraussetzungen](#) erfüllt sind.

1. Besuchen Sie den ESET PROTECT-[Downloadbereich](#), um ein eigenständiges Installationsprogramm für diese ESET PROTECT-Komponente herunterzuladen (*mdmcore_x64.msi*).
2. Führen Sie das Installationsprogramm für den Mobile Device Connector aus und akzeptieren Sie die EULA, sofern Sie mit ihr zustimmen.
3. Klicken Sie auf **Durchsuchen**, navigieren Sie zum Speicherort des [SSL-Zertifikats](#) für die Kommunikation über HTTPS und geben Sie das Passwort für dieses Zertifikat ein:
4. Geben Sie Ihren **MDM-Hostnamen** an: Dies ist der öffentliche Domänenname bzw. die öffentliche IP-Adresse, unter der Ihr MDM-Server für mobile Geräte aus dem Internet erreichbar ist.

 Der MDM-Hostname muss auf dieselbe Weise wie in Ihrem **HTTPS-Serverzertifikat** angegeben werden, um das [MDM-Profil](#) auf iOS-Geräten installieren zu können. Wenn im HTTPS-Zertifikat eine IP-Adresse angegeben ist, müssen Sie diese IP-Adresse in das Feld **MDM-Hostname** eingeben. Wenn das HTTPS-Zertifikat einen FQDN enthält (z. B. *mdm.mycompany.com*), müssen Sie diesen FQDN in das Feld **MDM-Hostname** eingeben. Wenn das HTTPS-Zertifikat einen Platzhalter enthält (z. B. **.mycompany.com*), dann können Sie *mdm.mycompany.com* in das Feld **MDM-Hostname** eingeben.

5. Das Installationsprogramm muss sich mit einer vorhandenen Datenbank verbinden, die vom Mobile Device Connector verwendet wird. Geben Sie die folgenden Verbindungsdetails ein:

- **Datenbank:** MySQL Server/MS SQL Server/MS SQL Server mit Windows-Authentifizierung

- **ODBC-Treiber:** MySQL ODBC 5.1-Treiber/MySQL ODBC 5.2 Unicode-Treiber/MySQL ODBC 5.3 Unicode-Treiber/MySQL ODBC 8.0 Unicode-Treiber/SQL Server/SQL Server Native Client 10.0/ODBC-Treiber 11 für SQL Server/ODBC-Treiber 13 für SQL Server/ODBC-Treiber 17 für SQL Server/ODBC-Treiber 18 für SQL Server
- **Datenbankname:** Sie können den vordefinierten Namen beibehalten oder den Namen bei Bedarf ändern.
- **Hostname:** Hostname oder IP-Adresse des Datenbankservers
- **Port:** für die Verbindung zum Datenbankserver
- Benutzername/Passwort **des Datenbankadministratorkontos**
- **Benannte Instanz verwenden** – Falls Sie eine MS SQL-Datenbank verwenden, können Sie auch das Kontrollkästchen **Benannte Instanz verwenden** auswählen, um eine benutzerdefinierte benannte Instanz zu verwenden. Sie können die Instanz im Feld **Hostname** im Format *HOSTNAME\DB_INSTANZ* angeben (zum Beispiel *192.168.0.10\ESMC7SQL*). Geben Sie für geclusterte Datenbanken nur den Clusternamen an. Wenn Sie diese Option auswählen, können Sie den Port für die Datenbankverbindung nicht ändern, und das System verwendet die von Microsoft festgelegten Standardports. Um den ESET PROTECT Server mit einer MS SQL-Datenbank in einem Failover-Cluster zu verbinden, geben Sie den Clusternamen in das Feld **Hostname** ein.

i Sie können den gleichen Datenbankserver wie für die ESET PROTECT-Datenbank verwenden. Falls Sie jedoch vorhaben, mehr als 80 Mobilgeräte zu registrieren, sollten Sie nach Möglichkeit einen anderen DB-Server verwenden.

6. Geben Sie den Benutzer für die neu erstellte Datenbank des Connectors für Mobilgeräte an. Sie können einen **Neuen Benutzer erstellen** oder den **Bestehenden Benutzer verwenden**. Geben Sie das Passwort für den Datenbankbenutzer ein.

7. Geben Sie den **Server-Host** (Name oder IP-Adresse Ihres ESET PROTECT Servers) und den **Serverport** (standardmäßig 2222; ersetzen Sie diesen Wert durch einen benutzerdefinierten Port, falls Sie einen anderen Port verwenden) ein.

8. Verbinden Sie den MDM Connector mit dem ESET PROTECT Server. Füllen Sie die Pflichtfelder **Serverhost** und **Serverport** für die Verbindung zum ESET PROTECT Server aus und wählen Sie entweder **Servergestützte Installation** oder **Offline-Installation** aus, um fortzufahren:

- **Servergestützte Installation** - Geben Sie die Anmeldedaten des Administrators der ESET PROTECT-Web-Konsole ein (das Installationsprogramm lädt die erforderlichen Zertifikate automatisch herunter). Überprüfen Sie außerdem die benötigten [Berechtigungen](#) für die servergestützte Installation.

1. Geben Sie **Serverhost** (Name oder IP-Adresse des ESET PROTECT Servers) und **Web-Konsolen-Port** ein (lassen Sie den standardmäßigen Port 2223 unverändert, sofern Sie keinen benutzerdefinierten Port verwenden). Geben Sie außerdem die Anmeldedaten des Administrators der Web-Konsole ein: **Benutzername/Passwort**.

2. Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob Sie das Zertifikat akzeptieren möchten. Fahren Sie mit Schritt 10 fort.

- **Offline-Installation** - Geben Sie ein **Proxy-Zertifikat** und eine **Zertifizierungsstelle** an, die Sie aus ESET PROTECT [exportieren](#) können. Alternativ können Sie Ihr [benutzerdefiniertes Zertifikat](#) mit einer passenden Zertifizierungsstelle verwenden.

1. Klicken Sie neben dem Peerzertifikat auf **Durchsuchen** und navigieren Sie zum Speicherort des **Peerzertifikats** (das Proxy-Zertifikat, das Sie aus ESET PROTECT exportiert haben). Lassen Sie das Textfeld **Zertifikatspasswort** leer, da für dieses Zertifikat kein Passwort erforderlich ist.

2. Wiederholen Sie den Vorgang für die Zertifizierungsstelle und fahren Sie mit Schritt 10 fort.

i Wenn Sie benutzerdefinierte Zertifikate mit ESET PROTECT verwenden (anstelle der bei der Installation von ESET PROTECT generierten Standardzertifikate), geben Sie diese entsprechend an, wenn Sie nach einem Proxy-Zertifikat gefragt werden.

9. Geben Sie einen Zielordner für den Mobile Device Connector an (wir empfehlen, den standardmäßigen Speicherort beizubehalten), klicken Sie auf **Weiter** und dann auf **Installieren**.

10. Überprüfen Sie nach dem Abschluss der Installation, ob der Mobile Device Connector richtig ausgeführt wird. Öffnen Sie dazu <https://your-mdm-hostname:enrollment-port> (z. B. <https://mdm.company.com:9980>) in Ihrem Webbrowser oder auf einem Mobilgerät. Wenn die Installation erfolgreich war, wird die folgende Meldung angezeigt: MDM-Server ist hochgefahren und wird ausgeführt!

11. Sie können [MDM jetzt in ESET PROTECT](#) aktivieren.

Mobile Device Connector-Voraussetzungen

Wenn der Port oder der Hostname des MDM-Servers geändert wird, müssen alle Mobilgeräte neu registriert werden.

! Daher sollten Sie einen dedizierten Hostnamen für den MDM-Server einrichten. In diesem Fall können Sie die IP-Adresse des neuen Hostgeräts auf den MDM-Hostnamen in Ihren DNS-Einstellungen verweisen, falls Sie je das Hostgerät austauschen, auf dem der MDM-Server ausgeführt wird.

Zur Installation des Mobile Device Connector unter Windows müssen folgende Voraussetzungen erfüllt sein:

- Öffentliche IP-Adresse/Hostname oder öffentliche Domäne, über das Internet erreichbar.

i Um den Hostnamen Ihres MDM Servers zu ändern, müssen Sie eine Reparaturinstallation Ihrer MDC-Komponente durchführen. Wenn Sie den Hostnamen Ihres MDM Servers ändern, müssen Sie unter Umständen ein neues **HTTPS-Serverzertifikat** mit dem neuen Hostnamen importieren, um MDM weiterhin verwenden zu können.

- Die erforderlichen Ports sind geöffnet und verfügbar. Eine vollständige [Liste der Ports finden Sie hier](#). Verwenden Sie nach Möglichkeit die Standardports 9981 und 9980. Sie können diese Ports bei Bedarf auch in der Konfigurationsdatei Ihres MDM Servers ändern. Stellen Sie sicher, dass sich Mobilgeräte mit den angegebenen Ports verbinden können. Ändern Sie gegebenenfalls die Firewall- und Netzwerkeinstellungen, um dies zu ermöglichen. Weitere Infos zur [MDM-Architektur](#).
- Firewall-Einstellungen - falls Sie den Mobile Device Connector auf einem nicht-Server-BS wie Windows 7 installieren (nur zu Testzwecken), müssen Sie die Kommunikations-Ports öffnen. Erstellen Sie dazu [Firewallregeln](#) für:

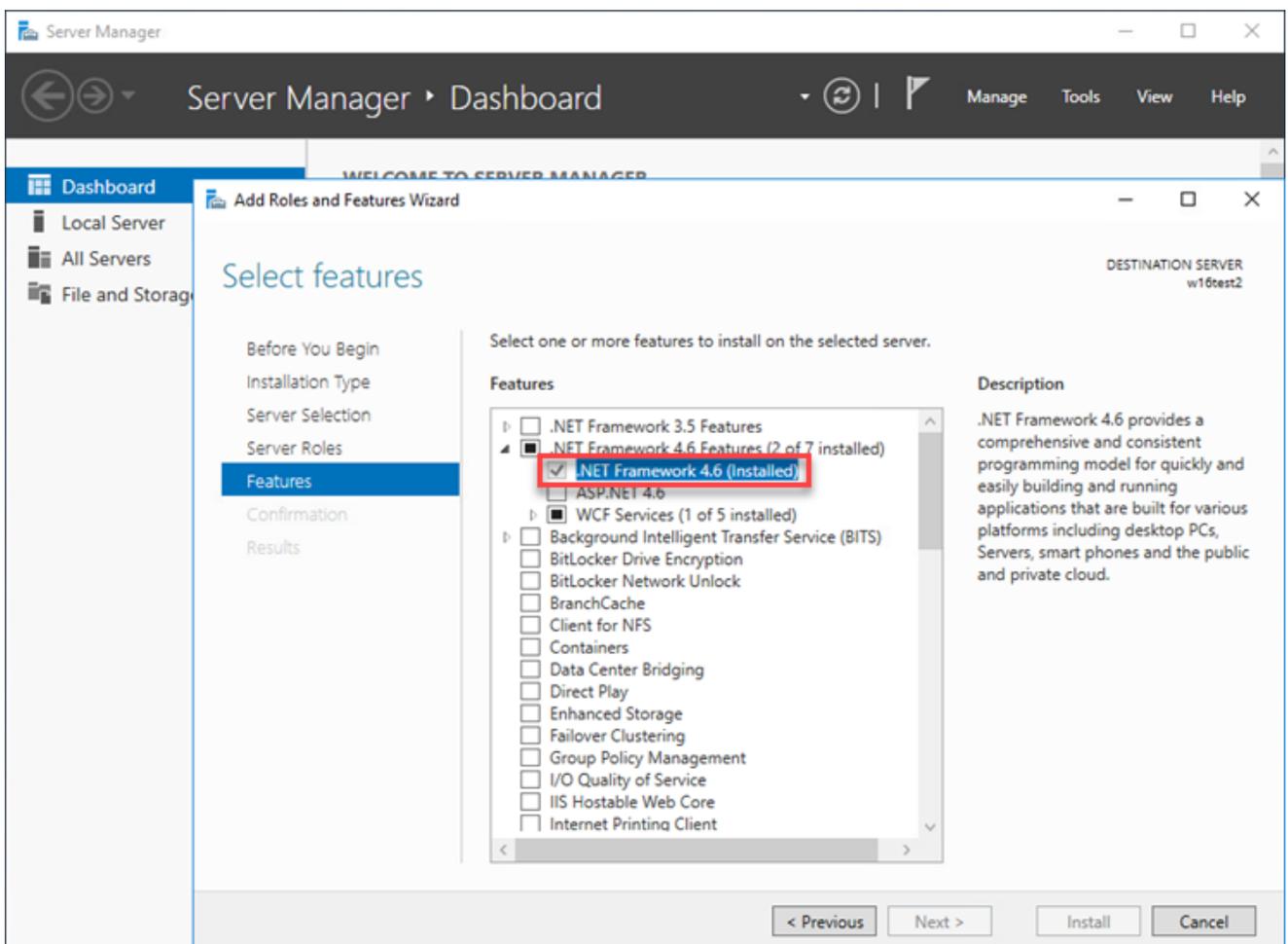
C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP-Port 9980

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

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

i Die tatsächlichen Pfade zu den .exe-Dateien können je nach Installationsort der ESET PROTECT-Komponenten auf Ihrem Client-Betriebssystem abweichen.

- Ein Datenbankserver ist bereits installiert und konfiguriert. Vergewissern Sie sich, dass die [Microsoft SQL](#)- bzw. [MySQL](#)-Anforderungen erfüllt sind.
- Die RAM-Nutzung des MDM-Connectors ist optimiert, und Sie können bis zu 48 „ESET PROTECT MDMCore Module“-Prozesse parallel ausführen. Wenn ein Benutzer mehr Geräte verbindet, werden die Prozesse regelmäßig ausgetauscht und den jeweiligen Geräten zugewiesen, die die Ressourcen aktuell benötigen.
- Für die Installation von MS SQL Server Express ist Microsoft .NET Framework 4 erforderlich. Sie können die Software mit dem **Assistenten zum Hinzufügen von Rollen und Features** installieren:



Zertifikatanforderungen

- Sie brauchen ein **SSL-Zertifikat** im .pfx-Format, um sicher per HTTPS zu kommunizieren. Verwenden Sie nach Möglichkeit ein von einer externen Zertifizierungsstelle ausgestelltes Zertifikat. Selbstsignierte Zertifikate (inklusive von der ESET PROTECT-ZS signierte Zertifikate) werden nicht empfohlen, da manche Mobilgeräte keine selbstsignierten Zertifikate akzeptieren.
- Ihr Zertifikat muss von einer ZS signiert sein, Sie benötigen einen privaten Schlüssel und müssen das Standardverfahren verwenden (normalerweise per OpenSSL), um diese Komponenten in eine .pfx-Datei zusammenzuführen:

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

Dies ist das Standardverfahren für die meisten Server, die SSL-Zertifikate verwenden.

- Für die [Offline-Installation](#) benötigen Sie außerdem ein Peerzertifikat (das **Agentenzertifikat**, das Sie aus ESET PROTECT [exportiert](#) haben). Alternativ können Sie in ein [benutzerdefiniertes Zertifikat](#) mit ESET PROTECT verwenden.

Mobile Device Connector-Aktivierung

Nachdem Sie den Mobile Device Connector installiert haben, müssen Sie ihn mit einer Unternehmenslizenz für ESET-Endpunkte aktivieren:

1. [Fügen Sie die ESET Endpoint, Business oder Office Lizenz](#) zur ESET PROTECT-Lizenzverwaltung hinzu.

2. Aktivieren Sie den Mobile Device Connector mit dem Clienttask [Produktaktivierung](#). Diese Prozedur entspricht der Aktivierung anderer ESET-Produkte. In diesem Fall ist der Mobile Device Connector der Clientcomputer.

MDM iOS-Lizenzierungsfunktion

ESET bietet keine Applikation im Apple App Store an. Daher werden sämtliche Lizenzierungsdetails für iOS-Geräte im ESET Mobile Device Connector verwaltet.

Die Lizenzierung erfolgt pro Gerät und kann mit einem [Produktaktivierungs-Task](#) (gleich wie unter Android) aktiviert werden.

iOS-Lizenzen können auf folgende Weise deaktiviert werden:

- Entfernen des Geräts aus der Verwaltung über den Task „Verwaltung beenden“
- Deinstallation von MDC über die Option **Datenbank entfernen**
- Deaktivierung auf andere Arten (ESET PROTECT- oder [ELA-Deaktivierung](#))

Da MDC im Namen der iOS-Geräte mit den ESET-Lizenzservern kommuniziert, wird im EBA-Portal der MDC-Status angezeigt, und nicht der Status der einzelnen Geräte. Die aktuellen Geräteinformationen sind immer in der ESET PROTECT Web-Konsole verfügbar.

Nicht aktivierte Geräte und Geräte mit abgelaufener Lizenz werden mit einem roten Schutzstatus und der Nachricht „Produkt ist nicht aktiviert“ angezeigt. Für diese Geräte können keine Tasks verarbeitet, Policies eingerichtet und nichtkritische Logs ausgeliefert werden.

Wenn Sie bei der Deinstallation von MDM die Option **Datenbank nicht entfernen** auswählen, werden die verwendeten Lizenzen nicht deaktiviert. Diese Lizenzen können wiederverwendet werden, wenn MDM erneut auf dieser Datenbank installiert wird, oder mit ESET PROTECT oder der [EBA-Deaktivierung](#) entfernt wird. Beim Wechsel zu einem anderen MDM Server müssen Sie den [Produktaktivierungs-Task](#) erneut ausführen.

HTTPS-Zertifikatanforderungen

Stellen Sie zur Registrierung eines Mobilgeräts im ESET Mobile Device Connector sicher, dass der HTTPS-Server die vollständige Zertifikatkette zurückgibt.

Zur ordnungsgemäßen Funktion des Zertifikats müssen die folgenden Anforderungen erfüllt sein:

- Das HTTPS-Zertifikat (pkcs#12/pfx-Container) muss die vollständige Zertifikatkette enthalten, inklusive der Stamm-ZS.
- Das Zertifikat muss in der gesamten erforderlichen Zeit (gültig von/bis) gültig sein.
- Entweder **CommonName** oder **subjectAltName** muss mit dem MDM-Hostnamen übereinstimmen.

Wenn der **MDM-Hostname** beispielsweise hostname.mdm.domain.com lautet, darf das Zertifikat Namen der folgenden Art enthalten:

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

i Nicht zulässig sind jedoch folgende Namen:

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

Das Sternchen („*“) darf also den Punkt nicht ersetzen. Dieses Verhalten ist bestätigt für die Art und Weise, wie iOS Zertifikate für MDM akzeptiert.

i Beachten Sie, dass nicht alle Geräte die aktuelle Zeitzone berücksichtigen, um die Gültigkeit des Zertifikats zu überprüfen. Vermeiden Sie potenzielle Probleme, indem Sie die Gültigkeit des Zertifikats einen oder zwei Tage vor dem aktuellen Datum festlegen.

Apache HTTP Proxy – Installation und Cache

Über Apache HTTP Proxy

[Apache HTTP Proxy](#) kann zu verschiedenen Zwecken eingesetzt werden:

Funktion:	Proxylösung, die diese Funktion bereitstellt
Caching von Downloads und Updates	Apache HTTP Proxy oder eine andere Proxylösung
Caching von Ergebnissen aus ESET LiveGuard Advanced	Nur mit konfiguriertem Apache HTTP Proxy
Replikation der Kommunikation zwischen ESET Management Agenten und ESET PROTECT Server	Apache HTTP Proxy oder eine andere Proxylösung



Falls Sie Apache HTTP Proxy bereits unter Windows installiert haben und auf die neueste Version aktualisieren möchten, lesen Sie weiter unter [Apache HTTP Proxy aktualisieren](#).

Zwischenspeicherung mit Apache HTTP Proxy

Apache HTTP Proxydownloads und Cache:

- ESET-Modulupdates
- Installationspakete von Repository-Servern
- Updates für Produktkomponenten

Die zwischengespeicherten Daten werden an die Endpunktclients in Ihrem Netzwerk verteilt. Mit Caching können Sie den Internet-Datenverkehr in Ihrem Netzwerk drastisch reduzieren.

i Sie können [Squid](#) als Alternative zum Apache HTTP Proxy installieren.

Sie können den Apache HTTP Proxy unter Windows auf zwei Arten installieren:

- [Installation mit dem All-in-One-Installationsprogramm](#)
- [Installation mit dem eigenständigen Installationsprogramm](#)

Installation mit dem eigenständigen Installationsprogramm

1. Besuchen Sie den ESET PROTECT-[Downloadbereich](#), um ein eigenständiges Installationsprogramm für diese ESET PROTECT-Komponente herunterzuladen (*apachehttp.zip*).
2. Öffnen Sie *ApacheHttp.zip* und extrahieren Sie die Dateien nach *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*

i Falls Sie Apache HTTP Proxy auf einem anderen Laufwerk installieren möchten, müssen Sie *C:\Program Files* in den folgenden Anweisungen und in der Datei *httpd.conf* im Verzeichnis *Apache HTTP Proxy\conf* durch den entsprechenden Pfad ersetzen. Wenn Sie den Inhalt von *ApacheHttp.zip* zum Beispiel nach *D:\Apache Http Proxy* extrahiert haben, dann müssen Sie *C:\Program Files* durch *D:\Apache Http Proxy* ersetzen.

3. Öffnen Sie eine Eingabeaufforderung als Administrator und wechseln Sie in das Verzeichnis *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin*
4. Führen Sie den folgenden Befehl aus:

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

5. Starten Sie den **ApacheHttpProxy**-Dienst mit dem folgenden Befehl:

```
sc start ApacheHttpProxy
```

6. Im Snap-In *services.msc* können Sie überprüfen, ob der Apache HTTP Proxy-Dienst ausgeführt wird (suchen Sie nach **ApacheHttpProxy**). Standardmäßig ist der Dienst so konfiguriert, dass er automatisch gestartet wird.

Nach der Installation müssen Sie Apache HTTP Proxy für die gewünschte Funktion [konfigurieren](#).

Konfiguration von Apache HTTP Proxy

Das von ESET bereitgestellte Installationsprogramm für den Apache HTTP Proxy ist bereits vorkonfiguriert. Sie müssen jedoch einige zusätzliche Änderungen vornehmen, um den Dienst verwenden zu können.

Konfiguration von Apache HTTP Proxy für die Replikation (Agent - Server)

1. Bearbeiten Sie die *Apache HTTP Proxy*-Konfigurationsdatei *httpd.conf* im Verzeichnis *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*.

a. Standardmäßig wird Port 2222 für die Kommunikation mit dem ESET Management Agenten verwendet. Falls Sie den Port bei der Installation geändert haben, verwenden Sie die geänderte Portnummer. Ersetzen Sie den Wert 2222 in der Zeile `AllowCONNECT 443 563 2222 8883 53535` durch Ihre Portnummer.

b. Fügen Sie in einem separaten `ProxyMatch`-Segment Folgendes hinzu:

I. Die Adresse, die Ihre Agenten verwenden, um sich mit dem ESET PROTECT Server zu verbinden.

II. Alle weiteren möglichen Adressen Ihres ESET PROTECT Servers (IP, FQDN)

(Fügen Sie den gesamten untenstehenden Code hinzu. Die IP-Adresse 10.1.1.10 und der Hostname `hostname.example` sind nur Beispiele und müssen durch Ihre tatsächlichen Adressen ersetzt werden. Außerdem können Sie den `ProxyMatch`-Ausdruck in [diesem Knowledgebase-Artikel](#) generieren).

```
<ProxyMatch ^(hostname\.example(?:[0-9]+)?(\/*\.*)?|10\.1\.1\.10(?:[0-9]+)?(\/*\.*)?)$>
Allow from all
</ProxyMatch>
```

c. Starten Sie den *Apache HTTP Proxy*-Dienst neu.

2. Richten Sie eine [Agent-Policy](#) ein, um sicherzustellen, dass Ihre Agenten den Proxy für die Replikation verwenden.

Konfiguration von Apache HTTP Proxy für Caching

1. Stopp Sie den **ApacheHttpProxy**-Dienst mit dem folgenden Befehl:

```
sc stop ApacheHttpProxy
```

2. Öffnen Sie die Datei *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* in einem einfachen Text-Editor. Fügen Sie die folgenden Zeilen am Ende der Datei hinzu:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
```

```
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

3. Speichern Sie die Datei und starten Sie den Apache-Dienst.

```
sc start ApacheHttpProxy
```

i Falls das Cacheverzeichnis an einem anderen Ort eingerichtet werden soll, z. B. auf einem anderen Laufwerk wie `D:\Apache HTTP Proxy\cache`, dann ersetzen Sie in der letzten Zeile des obigen Codes `"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"` durch `"D:\Apache HTTP Proxy\cache"`.

Konfiguration von Apache HTTP Proxy für die Verwendung von Benutzernamen und Passwort

Die Option zur Verwendung von Benutzernamen und Passwort kann nur für das Caching verwendet werden. Das bei der Kommunikation zwischen Agent und Server verwendete [Replikationsprotokoll](#) unterstützt keine Authentifizierung.

1. Halten Sie den **ApacheHttpProxy**-Dienst an, indem Sie eine [Eingabeaufforderung als Administrator](#) öffnen und den folgenden Befehl ausführen:

```
sc stop ApacheHttpProxy
```

2. Prüfen Sie, ob die folgenden Module in `C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf` vorhanden sind:

```
LoadModule authn_core_module modules\mod_authn_core.dll
LoadModule authn_file_module modules\mod_authn_file.dll
LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll
LoadModule auth_basic_module modules\mod_auth_basic.dll
```

3. Fügen Sie die folgenden Zeilen zu `C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf` unter `<Proxy *>` hinzu:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
```

4. Erstellen Sie mit dem Befehl `htpasswd` eine Datei mit dem Namen `password.file` im Ordner `Apache HTTP Proxy\bin` (Sie werden zur Eingabe des Passworts aufgefordert):

```
htpasswd.exe -c ..\password.file username
```

5. Erstellen Sie die Datei `group . file` im Ordner `Apache HTTP Proxy\` manuell mit dem folgenden Inhalt:

```
usergroup:username
```

6. Starten Sie den **ApacheHttpProxy**-Dienst, indem Sie den folgenden Befehl in einer Eingabeaufforderung mit erhöhten Rechten ausführen:

```
sc start ApacheHttpProxy
```

7. Testen Sie die Verbindung zum HTTP Proxy, indem Sie die folgende URL in Ihrem Browser öffnen:

```
http://[IP address]:3128/index.html
```

Nachdem Sie Apache HTTP Proxy installiert haben, können Sie auswählen, ob Sie nur ESET-Kommunikation zulassen (und den restlichen Datenverkehr sperren, Standardverhalten) oder sämtlichen Datenverkehr zulassen möchten. Führen Sie die hier beschriebenen Konfigurationsänderungen aus:

- [Weiterleitung nur für ESET-Kommunikation](#)
- [Proxy-Verkettung \(sämtlicher Datenverkehr\)](#)

Anzeigen der aktuellen Inhalte im Cache

```
"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -a -p "C:\ProgramData\Apache HTTP Proxy\cache"
```

Verwenden Sie [htcacheclean](#), um den Datenträgercache zu leeren. Unten sehen Sie den empfohlenen Befehl (Cachegröße wird auf 20 GB und Anzahl der Cachedateien auf ~128.800 festgelegt):

```
"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -n -t^  
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M -L128000
```

Um die Cachebereinigung stündlich auszuführen:

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask^  
/TR "\"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe\" "^  
-n -t -p "\"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M -L128000"
```

Führen Sie die folgenden Befehle aus, um sämtlichen Datenverkehr zuzulassen:

```
"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -n -t^  
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M
```

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask^  
/TR "\"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe\" "^  
-n -t -p "\"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M"
```

i Das ^-Zeichen direkt nach dem Zeilenende in den gezeigten Befehlen ist wichtig. Ohne dieses Zeichen wird der Befehl nicht korrekt ausgeführt.

Weitere Informationen finden Sie in unserem [Knowledgebase-Artikel](#) oder in der [Apache-Dokumentation für Authentifizierung und Autorisierung](#).

Squid Installation unter Windows und HTTP Proxy Cache

Squid ist eine Alternative zum [Apache HTTP Proxy](#). Führen Sie die folgenden Schritte aus, um Squid unter Windows zu installieren:

1. [Laden Sie](#) das MSI-Installationsprogramm für Squid herunter und installieren Sie Squid.
2. Klicken Sie auf das Symbol **Squid for Windows** in der Taskleiste und wählen Sie **Stop Squid Service** aus.
3. Navigieren Sie zum Installationsordner von Squid, z. B. C:\Squid\bin, und führen Sie den folgenden Befehl in der Befehlszeile aus:

```
squid.exe -z -F
```

Dieser Befehl erstellt die Austauschverzeichnisse für den Cache.

4. Klicken Sie auf das Symbol **Squid for Windows** in der Taskleiste und wählen Sie **Open Squid Configuration** aus.
5. Ersetzen Sie `http_access deny all` durch `http_access allow all`.
6. Fügen Sie die folgende Zeile hinzu, um den Datenträgercache zu aktivieren:

```
cache_dir aufs /cygdrive/c/Squid/var/cache 3000 16 256
```

- Sie können den Ort des Cacheverzeichnisses nach Ihren Wünschen anpassen. Im obigen Beispiel befindet sich das Cacheverzeichnis unter `C:\Squid\var\cache` (beachten Sie das Pfadformat im Befehl).
- i** • Außerdem können Sie die Gesamtgröße des Cache (3000 MB im Beispiel) und die Anzahl der Unterverzeichnisse auf der ersten Ebene (16 im Beispiel) und der zweiten Ebene (256 im Beispiel) im Cacheverzeichnis anpassen.

7. Speichern und schließen Sie die Squid-Konfigurationsdatei `squid.conf`.
8. Klicken Sie auf das Symbol **Squid for Windows** in der Taskleiste und wählen Sie **Start Squid Service** aus.
9. Im Snap-In `services.msc` können Sie überprüfen, ob der Squid-Dienst ausgeführt wird (suchen Sie nach **Squid for Windows**).

Offline-Repository – Windows

Mit dem Mirror-Tool können Sie ein Offline-Repository unter Windows erstellen. Diese Option eignet sich für geschlossene Computernetzwerke oder Netzwerke mit eingeschränktem Internetzugang. Mit dem Mirror-Tool können Sie einen Klon des ESET-Repositorys in einem lokalen Ordner erstellen. Das geklonte Repository kann anschließend beispielsweise auf ein externes Laufwerk oder einen anderen Ort im geschlossenen Netzwerk verschoben werden. Sie können das Repository an einen sicheren Ort im lokalen Netzwerk kopieren und über einen HTTP-Server bereitstellen.

Um das Offline-Repository zu aktualisieren, führen Sie denselben Befehl mit denselben Parametern aus, die Sie bei der Erstellung des Offline-Repositorys verwendet haben. Die vorherigen Daten im Zwischenverzeichnis werden wiederverwendet, nur die veralteten Dateien werden heruntergeladen.

 Das Repository wächst ständig, und das Zwischenverzeichnis benötigt denselben Speicherplatz. Stellen Sie sicher, dass Sie mindestens **1,2 TB** freien Speicherplatz haben, bevor Sie diesen Vorgang starten.

Best Practices

Weitere Informationen finden Sie im Artikel [Bewährte Methoden für die Nutzung von ESET PROTECT in einer Offline-Umgebung](#) in der ESET-Knowledgebase.

Beispielszenario für Windows

I. Erstellen des Repository-Klons

1. [Laden Sie](#) das Mirror-Tool herunter.
2. Extrahieren Sie das Mirror-Tool aus der heruntergeladenen *.zip*-Datei.
3. Erstellen Sie Ordner für:
 - Temporäre Dateien
 - Repository-Klon
4. Öffnen Sie eine Eingabeaufforderung und wechseln Sie zum Ordner, in den Sie das Mirror-Tool extrahiert haben (Befehl `cd`).
5. Führen Sie den folgenden Befehl aus (ändern Sie das Zwischenverzeichnis und das Ausgabeverzeichnis für das Repository zu den in Schritt 3 erstellten Ordnern):

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

6. Nachdem das Repository in den Ordner `outputRepositoryDirectory` kopiert wurde, können Sie den Ordner und seinen Inhalt auf einen anderen Computer verschieben, der für Ihr geschlossenes Netzwerk erreichbar ist.

II. Einrichten des HTTP-Servers

7. Sie benötigen einen HTTP-Server auf dem Computer im geschlossenen Netzwerk. Sie haben mehrere Möglichkeiten:
 - Apache HTTP Proxy von der ESET-[Downloadseite](#) (dieses Szenario)
 - Sie können auch andere HTTP-Server verwenden
8. Öffnen Sie *apachehttp.zip* und extrahieren Sie die Dateien nach *C:\Program Files\Apache HTTP Proxy*

2.[x.xx]

9. Öffnen Sie eine Eingabeaufforderung als Administrator und wechseln Sie in das Verzeichnis *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin* (Befehl *cd*).

10. Führen Sie den folgenden Befehl aus:

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

11. Öffnen Sie die Datei *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* mit einem Texteditor und fügen Sie am Ende der Datei die folgenden Zeilen hinzu:

```
Listen 80
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

12. Starten Sie den **ApacheHttpProxy**-Dienst mit dem folgenden Befehl:

```
sc start ApacheHttpProxy
```

13. Testen Sie, ob der Dienst ausgeführt wird, indem Sie *http://YourIPAddress:80/index.html* in Ihrem Browser öffnen (ersetzen Sie *YourIPAddress* durch die IP-Adresse Ihres Computers).

III. Ausführen des Offline-Repositorys

14. Erstellen Sie einen neuen Ordner für das Offline-Repository, z. B. *C:\Repository*.

15. Ersetzen Sie in der Datei *httpd.conf* die Zeilen

```
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
```

durch die Adresse des Repository-Ordners:

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

16. Kopieren Sie das heruntergeladene Repository nach *C:\Repository*.

17. Neu starten Sie den **ApacheHttpProxy**-Dienst mit dem folgenden Befehl:

```
sc restart ApacheHttpProxy
```

18. Ihr Offline-Repository ist jetzt unter der Adresse *http://YourIPAddress* verfügbar (zum Beispiel *http://10.1.1.10*).

19. Legen Sie die neue Repository-Adresse in der ESET PROTECT-Web-Konsole fest:

a. [ESET PROTECT Server](#) – Klicken Sie auf **Mehr > Einstellungen > Erweiterte Einstellungen > Repository** und geben Sie die Adresse des Offline-Repositorys in das Feld **Server** ein.

b. [ESET Management Agenten](#) – Klicken Sie auf **Policies**, dann auf die Agenten-Policy > **Bearbeiten > Einstellungen > Erweiterte Einstellungen > Repository** und geben Sie die Adresse des Offline-Repositorys in das Feld **Server** ein.

c. ESET Endpoint-Produkte (für Windows) – Klicken Sie auf **Policies**, klicken Sie auf die Policy **ESET Endpoint für Windows > Bearbeiten > Einstellungen > Update > Profile > Updates > Modulupdates**, deaktivieren Sie die Option **Automatisch auswählen** und geben Sie die Adresse des Offline-Repositorys in das Feld **Benutzerdefinierter Server** ein.

Failover-Cluster – Windows

Zur Installation von ESET PROTECT in einer Failover-Cluster-Umgebung sind im Wesentlichen die folgenden Schritte erforderlich.

i Lesen Sie auch diesen [Knowledgebase-Artikel](#) zur Clusterinstallation von ESET PROTECT Server.

1. Erstellen Sie ein Failover-Cluster mit einem gemeinsam genutzten Laufwerk:

- [Anweisungen zum Erstellen eines Failover-Clusters unter Windows Server 2016 und 2019](#)
- [Anweisungen zum Erstellen eines Failover-Clusters unter Windows Server 2012 und 2012 R2](#)

2. Geben Sie im **Assistenten für die Clustererstellung** den gewünschten Hostnamen (frei wählbar) und die IP-Adresse ein.

3. Verbinden Sie das gemeinsam genutzte Clusterlaufwerk mit dem ersten Knoten und [installieren Sie ESET PROTECT Server mit dem Standalone-Installationsprogramm](#) auf diesem Knoten. Aktivieren Sie bei der Installation die Option **Dies ist eine Clusterinstallation** und wählen Sie das gemeinsam genutzte Laufwerk für die Speicherung der Anwendungsdaten aus. Wählen Sie einen Hostnamen aus und geben Sie ihn für das Serverzertifikat von ESET PROTECT Server neben den vorausgefüllten Hostnamen ein. Notieren Sie sich diesen Hostnamen und verwenden Sie ihn in Schritt 6 bei der Erstellung der ESET PROTECT Server-Rolle im Cluster-Manager.

4. Halten Sie den ESET PROTECT Server auf dem ersten Knoten an, verbinden Sie das gemeinsam genutzte Clusterlaufwerk mit dem zweiten Knoten, und [installieren Sie ESET PROTECT Server mit dem Standalone-Installationsprogramm](#) auf diesem Knoten. Aktivieren Sie bei der Installation die Option **Dies ist eine Clusterinstallation**. Wählen Sie den freigegebenen Datenträger als Datenspeicher für die Anwendung. Ändern Sie die Informationen zu Datenbankverbindung und Zertifikaten nicht, da diese bei der Installation von ESET PROTECT Server auf dem ersten Knoten konfiguriert wurden.

5. Konfigurieren Sie Ihre Firewall, sodass diese eingehende Verbindungen auf allen [Ports](#) akzeptiert, die von ESET PROTECT Server verwendet werden.

6. Erstellen und starten Sie eine Rolle im Cluster-Konfigurations-Manager (**Rolle konfigurieren > Rolle**

auswählen > Allgemeiner Dienst) für den ESET PROTECT Server-Dienst. Wählen Sie den **ESET PROTECT Server-**Dienst in der Liste der verfügbaren Dienste aus. Verwenden Sie unbedingt denselben Hostnamen für die Rolle, den Sie in Schritt 3 für das Serverzertifikat eingegeben haben.

7. Installieren Sie den ESET Management Agenten mit dem Standalone-Installationsprogramm auf allen Clusterknoten. Geben Sie in den Bildschirmen **Agent-Konfiguration** und **Verbindung mit ESET PROTECT Server** den Hostnamen ein, den Sie in Schritt 6 verwendet haben. Speichern Sie die Agenten-Daten auf dem lokalen Knoten, und nicht auf dem Cluster-Laufwerk.

8. Der Webserver (Apache Tomcat) wird für Cluster nicht unterstützt und muss daher auf einem nicht-Clusterlaufwerk oder einem separaten Computer installiert werden:

a. [Installieren Sie die Web-Konsole](#) auf einem separaten Computer und konfigurieren Sie sie ordnungsgemäß für die Verbindung mit der ESET PROTECT Server-Clusterrolle.

b. Installieren Sie die Web-Konsole und lokalisieren Sie anschließend die Konfigurationsdatei unter:
C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

c. Öffnen Sie die Datei in Notepad oder einem anderen Text-Editor. Ersetzen Sie in der Zeile `server_address=localhost` den Eintrag „localhost“ durch die IP-Adresse bzw. den Hostnamen der ESET PROTECT Server-Clusterrolle.

Komponenteninstallation unter Linux

In den meisten Installationsszenarien müssen Sie verschiedene ESET PROTECT-Komponenten auf verschiedenen Computern installieren, beispielsweise um Unterschiede in der Netzwerkarchitektur zu berücksichtigen oder Leistungsanforderungen zu erfüllen.

Folgen Sie der [Schritt-für-Schritt-Installationsanleitung für ESET PROTECT](#).

Kernkomponenteninstallation

- [ESET PROTECT Server](#)
- [ESET PROTECT-Web-Konsole](#) – Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server.
- [ESET Management Agent](#)
- [Datenbankserver](#)

Installation optionaler Komponenten

- [RD Sensor](#)
- [Mobile Device Connector](#)
- [Apache HTTP Proxy](#)
- [Mirror-Tool](#)

Informationen zum Upgrade von ESET PROTECT für Linux auf die aktuelle Version finden Sie im Kapitel [Task „Komponenten-Upgrade“](#) oder in unserem [Knowledgebase-Artikel](#).

ESET PROTECT Schritt-für-Schritt-Installation unter Windows

In diesem Installationsszenario wird eine Schritt-für-Schritt-Installation des ESET PROTECT Servers und der ESET PROTECT-Web-Konsole simuliert. Wir simulieren hier eine Installation mit MySQL.

Installationsanweisungen für ausgewählte Linux-Distributionen

Folgen Sie unseren Knowledgebase-Artikeln mit distributionsspezifischen Anweisungen:



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

Vor der Installation

1. Stellen Sie sicher, dass der [Datenbankserver](#) in Ihrem Netzwerk vorhanden ist und dass Sie von Ihrem lokalen Server bzw. Ihrem Remoteserver auf die Datenbank zugreifen können. Wenn kein Datenbankserver installiert ist, müssen Sie einen neuen Datenbankserver [installieren und konfigurieren](#).
2. Laden Sie die eigenständigen ESET PROTECT Linux-Komponenten herunter (Agent, Server, Web-Konsole). Sie finden diese Installationsdateien in der Kategorie [ESET PROTECT Standalone-Installationsprogramme](#) auf der ESET-Website.

Installationsprozess

Für die Installation müssen Sie den Befehl `sudo` bzw. eine Installation mit `root`-Berechtigungen ausführen können.

1. Installieren Sie die [erforderlichen Pakte](#) für den ESET PROTECT Server.
2. Konfigurieren Sie die Verbindung zum MySQL-Server wie im Abschnitt [MySQL-Konfiguration](#) beschrieben.
3. Überprüfen der Konfiguration des MySQL ODBC-Treibers. Weitere Informationen finden Sie unter [ODBC – Installation und Konfiguration](#).
4. Passen Sie die Installationsparameter an und führen Sie die ESET PROTECT Server-Installation aus. Weitere Informationen finden Sie unter [Serverinstallation – Linux](#).
5. Installieren Sie die erforderlichen Java- und Tomcat-Pakete sowie die [ESET PROTECT Web-Konsole](#). Falls bei der HTTPS-Verbindung zur ESET PROTECT Web-Konsole Probleme auftreten, finden Sie weitere Hinweise unter [HTTPS-/SSL-Verbindung einrichten](#).
6. [Installieren Sie den ESET Management Agenten](#) auf dem Server.

ESET empfiehlt, Befehle mit vertraulichen Daten (z. B. Passwörter) aus dem Verlauf der Befehlszeile zu löschen:

- i** 1. Führen Sie `history` aus, um die Liste aller Befehle im Verlauf anzuzeigen.
- 2. Führen Sie `history -d line_number` aus (geben Sie die Zeilennummer des Befehls an). Alternativ können Sie mit `history -c` den gesamten Verlauf der Befehlszeile löschen.

MySQL – Installation und Konfiguration

Installation

! Achten Sie darauf, [unterstützte Versionen von MySQL Server und ODBC Connector](#) zu installieren.

Falls Sie MySQL bereits installiert und konfiguriert haben, fahren Sie mit der [Konfiguration](#) fort.

1. Fügen Sie das MySQL-Repository hinzu:

Debian, Ubuntu	Führen Sie die folgenden Befehle im Terminal aus: 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> Sie können die Versionen der Komponenten auswählen, die Sie während der Paketinstallation installieren möchten. Wir empfehlen, die Standardoptionen zu verwenden. Siehe auch Hinzufügen des MySQL APT-Repositorys
CentOS, Red Hat	Hinzufügen des MySQL Yum-Repositorys
OpenSuse, SUSE Linux Enterprise Server	Hinzufügen des MySQL SLES-Repositorys

2. Aktualisieren Sie Ihren lokalen Repository-Cache:

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

3. Die Installationsprozedur für MySQL hängt von der verwendeten Linux-Distribution und -Version ab:

Linux Distribution:	MySQL Serverinstallationsbefehl:	MySQL Erweiterte Serverinstallation:
Debian, Ubuntu	<code>sudo apt-get install mysql-server</code>	MySQL von der Quelle mit dem MySQL APT-Repository installieren
CentOS, Red Hat	<code>sudo yum install mysql-community-server</code>	MySQL unter Linux mit dem MySQL Yum-Repository installieren
OpenSuse, SUSE Linux Enterprise Server	<code>sudo zypper install mysql-community-server</code>	Schritte für eine frische Installation von MySQL

Für eine manuelle Installation [laden Sie den MySQL Community Server herunter](#).

Konfiguration

1. Öffnen Sie die Konfigurationsdatei `my.cnf` in einem Text-Editor:

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

Versuchen Sie `/etc/mysql/my.cnf` oder `/etc/my.cnf.d/community-mysql-server.cnf` oder `/etc/mysql/mysql.conf.d/mysqld.cnf`, falls die Datei nicht vorhanden ist.

2. Suchen Sie im Abschnitt `[mysqld]` der Datei `my.cnf` die folgende Konfiguration und ändern Sie die Werte.



- Erstellen Sie den Abschnitt `[mysqld]`, falls er in der Datei noch nicht vorhanden ist.
- Wenn die Parameter nicht in der Datei vorhanden sind, fügen Sie sie zum Abschnitt `[mysqld]` hinzu.
- Führen Sie den folgenden Befehl aus, um Ihre MySQL-Version zu ermitteln: `mysql --version`.

Parameter	Anmerkungen und empfohlene Werte	MySQL version
<code>max_allowed_packet=33M</code>		Alle unterstützten Versionen .
<code>log_bin_trust_function_creators=1</code>	Alternativ können Sie das binäre Logging deaktivieren: <code>log_bin=0</code> .	Unterstützte 8.x-Versionen
<code>innodb_log_file_size=100M</code>	Die Multiplikation der Werte dieser beiden Parameter muss mindestens 200 ergeben. Der Mindestwert für <code>innodb_log_files_in_group</code> ist 2 und der Höchstwert ist 100 . Außerdem muss der Wert eine Ganzzahl sein).	Unterstützte 8x-Versionen 5.7 5.6.22 (und höher 5.6.x)
<code>innodb_log_files_in_group=2</code>		
<code>innodb_log_file_size=200M</code>	Legen Sie den Wert mindestens auf 200M und höchstens auf 3000M fest.	5.6.20 und 5.6.21

3. Drücken Sie **CTRL + X** und dann **Y**, um die Änderungen zu speichern und die Datei zu schließen.

4. Starten Sie den MySQL Server neu und übernehmen Sie die Konfiguration (in manchen Fällen lautet der Dienstname `mysqld`):

```
sudo systemctl restart mysql
```

5. Richten Sie MySQL inklusive Berechtigungen und Passwort ein (optionaler Schritt, funktioniert unter Umständen nicht auf allen Linux-Distributionen):

a) Zeigen Sie das temporäre MySQL-Passwort an: `sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b) Kopieren und speichern Sie das Passwort.

c) Erstellen ein neues Passwort mit einer der folgenden Optionen:

- Führen Sie `/usr/bin/mysql_secure_installation` aus und geben Sie das temporäre Passwort ein. Daraufhin werden Sie aufgefordert, ein neues Passwort zu erstellen.
- Führen Sie `mysql -u root -p` aus und geben Sie das temporäre Passwort ein. Führen Sie `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';` aus, um das root-Passwort zu ändern (ersetzen Sie `strong_new_password` durch Ihr Passwort), und geben Sie `Quit` ein.

Siehe auch [Improve MySQL Installation Security](#) (Sicherheit der MySQL-Installation verbessern, in Englischer Sprache) im MySQL-Referenzhandbuch.

6. Überprüfen Sie, ob der MySQL-Serverdienst ausgeführt wird:

```
sudo systemctl status mysql
```

ODBC – Installation und Konfiguration

! Achten Sie darauf, [unterstützte Versionen von MySQL Server und ODBC Connector](#) zu installieren.



Sie können den MS ODBC-Treiber (Version 13 und neuer) installieren, um eine Verbindung zwischen ESET PROTECT Server unter Linux und MS SQL Server unter Windows herzustellen. Weitere Informationen finden Sie in [diesem Knowledgebase-Artikel](#).

Installieren Sie den MySQL ODBC-Treiber mit dem Terminal. Führen Sie die Schritte für Ihre Linux-Distribution aus:

- [Debian, Ubuntu](#)
- [CentOS 7](#)
- [Sonstige unterstützte Linux-Distributionen](#)

Debian, Ubuntu

1. unixODBC Treiber werden installiert:

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

2. Laden Sie den ODBC-Connector herunter:

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

- !**
- Achten Sie darauf, die korrekte Version für Ihre Version und Distribution von Linux auszuwählen.
 - Sie können den ODBC-Connector für MySQL von der [offiziellen MySQL-Website](#) herunterladen.

3. Entzippen Sie das Archiv des ODBC-Treibers (Der Paketname hängt vom verwendeten Link ab):

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

4. Extrahieren Sie den ODBC-Treiber (Der Paketname hängt vom verwendeten Link ab):

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

5. Navigieren Sie zum Ordner des ODBC-Treibers (Der Paketname hängt vom verwendeten Link ab):

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

6. Kopieren Sie die ODBC-Treiberdateien:

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

7. Registrieren Sie den Treiber für ODBC.

- Für neue Linux-Versionen wie Ubuntu 20.x empfehlen wir die Verwendung des Unicode-Treibers:

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

- Für andere Systeme oder falls der Unicode-Treiber nicht funktioniert:

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

8. Listen Sie die installierten Treiber auf:

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

Weitere Informationen finden Sie unter:

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

CentOS 7

1. unixODBC Treiber werden installiert:

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

2. Laden Sie den ODBC-Connector herunter:

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

- Installieren Sie den ODBC Connector nicht mit YUM. Ansonsten wird die neueste, inkompatible Version installiert.
 - Achten Sie darauf, die korrekte Version für Ihre Version und Distribution von Linux auszuwählen.
 - Sie können den ODBC-Connector für MySQL von der [offiziellen MySQL-Website](https://dev.mysql.com) herunterladen.

3. Installieren des ODBC Driver:

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

4. Richten Sie den ODBC-Treiber ein:

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

5. Listen Sie die installierten Treiber auf:

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

Sonstige unterstützte Linux-Distributionen

- Achten Sie darauf, die korrekte Version für Ihre Version und Distribution von Linux auszuwählen.
- Sie können den ODBC-Connector für MySQL von der [offiziellen MySQL-Website](#) herunterladen.

1. Folgen Sie diesen Anweisungen, um den ODBC-Treiber zu installieren:

- **OpenSuse, SUSE Linux Enterprise Server:** `sudo zypper install unixODBC`. Siehe auch <https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html>
- [Connector/ODBC mit einer Tarball-Binärdistribution installieren](#)

2. Führen Sie den folgenden Befehl aus, um die Datei `odbcinst.ini` in einem Text-Editor zu öffnen:

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

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

3. Kopieren Sie die folgende Konfiguration in die Datei `odbcinst.ini` (überprüfen Sie die Pfade unter **Driver** und **Setup**) und speichern und schließen Sie die Datei:

```
[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
```

In manchen Distributionen befindet sich der Treiber an einem anderen Ort. Sie können die Datei mit dem folgenden Befehl lokalisieren:

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

4. Aktualisieren Sie die Konfigurationsdateien für den ODBC-Zugriff auf die Datenbankserver auf dem aktuellen Host mit dem folgenden Befehl:

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

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

Serverinstallation – Linux

Installationsanweisungen für ausgewählte Linux-Distributionen

Folgen Sie unseren Knowledgebase-Artikeln mit distributionsspezifischen Anweisungen:



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

Installation

Führen Sie die folgenden Schritte aus, um die ESET PROTECT Server-Komponente unter Linux mit einem Terminalbefehl zu installieren:

 Vergewissern Sie sich, dass alle [Installationsvoraussetzungen](#) erfüllt sind.

1. Laden Sie die ESET PROTECT Server-Komponente herunter:

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

2. Legen Sie die heruntergeladene Datei als ausführbar fest:

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

3. Sie können ein Installationskript vorbereiten und mit `sudo` ausführen.

Führen Sie das im folgenden Beispiel gezeigte Installationskript aus (Neue Zeilen werden mit „\
um den gesamten Befehl ins Terminal zu kopieren):

```
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"
```

Sie können folgende Attribute ändern:

Attribut	Beschreibung	Erforderlich
<code>--uninstall</code>	Deinstalliert das Produkt.	-
<code>--keep-database</code>	Die Datenbank wird bei der Deinstallation nicht entfernt.	-
<code>--locale</code>	Die Gebietsschema-ID (LCID) des installierten Servers (Standardwert: <code>en_US</code>). Unter Unterstützte Sprachen finden Sie Hinweise zu den verfügbaren Optionen. <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"><p>i Wenn Sie den Parameter <code>--locale</code> nicht angeben, wird der ESET PROTECT Server auf Englisch installiert. ESET PROTECT sie können für jede Sitzung der ESET PROTECT-Web-Konsole eine Sprache festlegen. Nicht alle Elemente der Web-Konsole ändern sich, wenn Sie die Sprache wechseln. Einige Elemente (Standard-Dashboards, Policies, Tasks usw.) werden bei der Installation von ESET PROTECT erstellt, und ihre Sprache kann nicht geändert werden.</p></div>	Ja
<code>--skip-license</code>	Der Benutzer wird während der Installation nicht zur Bestätigung der Lizenzvereinbarung aufgefordert.	-
<code>--skip-cert</code>	Die Zertifikaterzeugung wird übersprungen (zusammen mit dem Parameter <code>--server-cert-path</code> verwenden).	-
<code>--license-key</code>	ESET-Lizenzschlüssel. Sie können den Lizenzschlüssel später angeben.	-

Attribut	Beschreibung	Erforderlich
--server-port	port des ESET PROTECT Servers (Standardwert: 2222).	-
--console-port	Port der ESET PROTECT-Konsole (Standardwert: 2223)	-
--server-root-password	Passwort für die Anmeldung bei der Web-Konsole mit dem Benutzer „Administrator“; mindestens 8 Zeichen lang.	Ja
--db-type	Art der Datenbank, die verwendet wird (mögliche Werte: "MySQL Server", "MS SQL Server"). MS SQL Server unter Linux wird nicht unterstützt. Sie können jedoch den ESET PROTECT Server unter Linux mit MS SQL Server unter Windows verbinden .	-
--db-driver	ODBC-Treiber für die Datenbankverbindung in der Datei <i>odbcinst.ini</i> (der Befehl <code>odbcinst -q -d</code> zeigt eine Liste der verfügbaren Treiber an. Verwenden Sie einen dieser Treiber, z. B. <code>--db-driver="MySQL ODBC 8.0 Driver"</code> , <code>--db-driver="MySQL ODBC 8.0 Unicode Driver"</code> oder <code>--db-driver="MySQL ODBC 8.0.17"</code>).	Ja
--db-hostname	Computernamen oder IP-Adresse des Datenbankservers. Benannte Datenbankinstanzen werden nicht unterstützt.	Ja
--db-port	Port für den Datenbankserver (Standardwert: 3306).	Ja
--db-name	Name der Datenbank des ESET PROTECT Servers (Standardwert: <code>era_db</code>)	-
--db-admin-username	Benutzername des Datenbankadministrators (wird während der Installation zum Erstellen und Ändern der Datenbank verwendet). Dieser Parameter kann ausgelassen werden, wenn bereits ein Datenbankbenutzer in <code>--db-user-username</code> und <code>--db-user-password</code> definiert wurde.	Ja
--db-admin-password	Passwort des Datenbankadministrators. Dieser Parameter kann ausgelassen werden, wenn bereits ein Datenbankbenutzer in <code>--db-user-username</code> und <code>--db-user-password</code> definiert wurde.	Ja
--db-user-username	Benutzername des ESET PROTECT Server-Datenbankbenutzers (wird vom ESET PROTECT Server für die Verbindung zur Datenbank verwendet); maximal 16 Zeichen.	Ja
--db-user-password	Passwort des ESET PROTECT Server-Datenbankbenutzers	Ja
--cert-hostname	Enthält alle möglichen Namen und/oder die IP-Adresse des ESET PROTECT Server-Computers. Der Wert muss mit dem Servernamen im Zertifikat des Agenten übereinstimmen, der sich mit dem Server verbinden soll.	Ja
--server-cert-path	Pfad zum Server-Peerzertifikat (verwenden Sie diese Option auch, wenn Sie <code>--skip-cert</code> angegeben haben)	-
--server-cert-password	Passwort für das Server-Peerzertifikat	-
--agent-cert-password	Passwort für das Agenten-Peerzertifikat	-
--cert-auth-password	Passwort der Zertifizierungsstelle	-
--cert-auth-path	Pfad zur Zertifizierungsstellendatei des Servers	-
--cert-auth-common-name	Allgemeiner Name der Zertifizierungsstelle (Anführungszeichen "" verwenden)	-
--cert-organizational-unit	-	-

Attribut	Beschreibung	Erforderlich
--cert-organization	-	-
--cert-locality	-	-
--cert-state	-	-
--cert-country	-	-
--cert-validity	Gültigkeit des Zertifikats in Tagen oder Jahren (im Argument -cert-validity-unit angeben)	-
--cert-validity-unit	Einheit für die Zertifikatgültigkeit; mögliche Werte sind „Years“ (Jahre) und „Days“ (Tage) (Standardwert: Years)	-
--ad-server	Active Directory-Server	-
--ad-user-name	Name des Benutzers, der zum Durchsuchen des AD-Netzwerks berechtigt ist	-
--ad-user-password	Active Directory-Benutzerpasswort	-
--ad-cdn-include	Active Directory-Strukturpfad für die Synchronisierung; mit leeren Anführungszeichen "" wird die gesamte Struktur synchronisiert	-
--enable-imp-program	Aktivieren Sie das Produktverbesserungsprogramm.	-
--disable-imp-program	Deaktivieren Sie das Produktverbesserungsprogramm.	-

ESET empfiehlt, Befehle mit vertraulichen Daten (z. B. Passwörter) aus dem Verlauf der Befehlszeile zu löschen:

- i** 1. Führen Sie `history` aus, um die Liste aller Befehle im Verlauf anzuzeigen.
- 2. Führen Sie `history -d line_number` aus (geben Sie die Zeilennummer des Befehls an). Alternativ können Sie mit `history -c` den gesamten Verlauf der Befehlszeile löschen.

4. Bei der Installation werden Sie gefragt, ob Sie am Produktverbesserungsprogramm teilnehmen möchten. Drücken Sie **Y**, falls Sie der Übermittlung von Absturzberichten und Telemetriedaten an ESET zustimmen, oder **N**, um keine Daten zu senden.

5. Der ESET PROTECT Server und der `eraserver`-Dienst werden am folgenden Speicherort installiert:

```
/opt/eset/RemoteAdministrator/Server
```

Die Installation wird unter Umständen mit **SELinux policy... failure** beendet. Sie können diese Meldung ignorieren, wenn Sie SELinux nicht verwenden.

6. Überprüfen Sie nach der Installation mit dem folgenden Befehl, ob der ESET PROTECT Server-Dienst ausgeführt wird:

```
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 ~]#
```

Installationsprogramm-Log

Das Log des Installationsprogramms ist hilfreich für die Fehlersuche und befindet sich unter [Logdateien](#).

Servervoraussetzungen – Linux

Für die Installation von ESET PROTECT Server unter Linux müssen folgende Voraussetzungen erfüllt sein:

- Sie benötigen eine gültige [Lizenz](#).
- Sie benötigen ein [unterstütztes Linux-Betriebssystem](#).
- Die erforderlichen Ports müssen geöffnet und verfügbar sein. Eine vollständige [Liste der Ports finden Sie hier](#).
- [Ein Datenbankserver muss installiert und](#) mit einem Root-Konto konfiguriert sein. Vor der Installation muss kein Benutzerkonto erstellt werden. Dieses Konto kann vom Installationsprogramm erstellt werden. [MS SQL Server unter Linux](#) wird nicht unterstützt. Sie können jedoch [den ESET PROTECT Server unter Linux mit MS SQL Server unter Windows verbinden](#).

i Der ESET PROTECT Server speichert große Datenblöcke in der Datenbank. Daher muss MySQL [große Pakete akzeptieren](#), um ESET PROTECT verwenden zu können.

- **ODBC-Treiber** - Der ODBC-Treiber wird für den Verbindungsaufbau zum [Datenbankserver](#) (MySQL) benötigt.
- Legen Sie die Serverinstallationsdatei mit dem folgenden Terminalbefehl als ausführbar fest:

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

- Wir empfehlen, **die neueste Version von OpenSSL 1.1.1** zu verwenden. OpenSSL 3.x wird nicht unterstützt. Die niedrigste unterstützte Version von OpenSSL für Linux ist openssl-1.0.1e-30. Sie können mehrere Versionen von OpenSSL parallel auf einem System installieren. Mindestens eine unterstützte Version muss auf Ihrem System vorhanden sein.

oMit dem Befehl `openssl version` können Sie die aktuelle Standardversion abrufen.

oSie können alle auf Ihrem System vorhandenen OpenSSL-Versionen auflisten. Sie können die Dateinamenendungen mit dem Befehl `sudo find / -iname *libcrypto.so*` anzeigen.

oMit dem folgenden Befehl können Sie überprüfen, ob Ihr Linux-Client kompatibel ist: `openssl s_client -connect google.com:443 -tls1_2`

- **Xvfb** - Wird auf Linux-Serversystemen ohne grafische Benutzeroberfläche zum Drucken von Berichten ([Bericht generieren](#)) benötigt.
- **Xauth** – Das Paket wird zusammen mit **xvfb** installiert. Sie müssen **xauth** installieren, falls Sie **xvfb** nicht installieren.
- **cifs-utils** - Wird für die ordnungsgemäße Agenten-Bereitstellung auf Windows-Betriebssystemen benötigt.
- **Qt4 WebKit-Bibliotheken** – Werden zum Drucken von Berichten im PDF- und PS-Format benötigt (Version 4.8, nicht 5). Alle anderen Qt4-Abhängigkeiten werden automatisch installiert. Wenn das Paket nicht im Betriebssystem-Repository verfügbar ist, können Sie es selbst auf einem Zielcomputer kompilieren oder aus einem Repository eines Drittanbieters installieren (z. B. den [EPEL-Repositories](#)): [CentOS 7-Anweisungen](#), [Ubuntu 20.04-Anweisungen](#).
- **kinit + klist** – Kerberos wird verwendet, um Domänenbenutzer bei der Anmeldung zu authentifizieren und um Active Directory zu synchronisieren. Achten Sie darauf, Kerberos korrekt zu konfigurieren (`/etc/krb5.conf`). ESET PROTECT 9.1 kann mit mehreren Domänen synchronisiert werden.
- **Idapsearch** - Wird für den AD-Synchronisierungstask und für die Autorisierung benötigt.
- **snmptrap** – Optional, wird zum Senden von SNMP-Traps verwendet. SNMP muss ebenfalls konfiguriert werden.
- **SELinux devel-Paket** - Dieses Paket wird bei der Produktinstallation zur Erstellung von SELinux-Policy-Modulen verwendet. Wird nur auf Systemen mit aktiviertem SELinux benötigt (CentOS, RHEL). SELinux kann Probleme mit anderen Anwendungen verursachen. Diese Komponente wird für den ESET PROTECT Server nicht benötigt.
- **lshw** - Installieren Sie das `lshw`-Paket auf dem Linux-Client/-Server, damit der ESET Management Agent den [Hardwarebestand](#) korrekt melden kann.

Die folgende Tabelle enthält die einzelnen Konsolenbefehle für die oben beschriebenen Pakete unter verschiedenen Linux-Distributionen (Führen Sie die Befehle als `sudo` oder `root` aus):

Paket	Debian- und Ubuntu-Distributionen	CentOS- und Red Hat-Distributionen	OpenSUSE-Distribution
ODBC-Treiber	Siehe Kapitel ODBC – Installation und Konfiguration .		
OpenSSL	<code>apt-get install openssl</code>	<code>yum install openssl -y</code>	<code>zypper install openssl</code>
xvfb	<code>apt-get install xvfb</code>	<code>yum install xorg-x11-server-Xvfb -y</code>	<code>zypper install xorg-x11-server-extra</code>
cifs-utils	<code>apt-get install cifs-utils</code>	<code>yum install cifs-utils</code>	<code>zypper install cifs-utils</code>
Qt4 WebKit-Bibliotheken	<code>apt-get install libqtwebkit4</code> Lesen Sie die Anweisungen für Ubuntu 20.04 .	Das Qt4 WebKit ist nicht im CentOS-Standardrepository enthalten. Installieren Sie die folgenden Pakete: <code>yum install -y epel-release</code> <code>yum install qtwebkit-devel</code> Alternativ können Sie das Paket aus den Fedora-Repositories installieren.	<code>zypper install libqtwebkit4</code>

Paket	Debian- und Ubuntu-Distributionen	CentOS- und Red Hat-Distributionen	OpenSUSE-Distribution
kinit+klist - optional (wird für den Active Directory-Dienst benötigt)	apt-get install krb5-user	yum install krb5-workstation	zypper install krb5-client
ldapsearch	apt-get install ldap-utils libsasl2-modules-gssapi-mit	yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y	zypper install openldap2-client cyrus-sasl-gssapi cyrus-sasl-ldap-auxprop
snmptrap	apt-get install snmp	yum install net-snmp-utils net-snmp	zypper install net-snmp
SELinux devel-Paket (optional, nicht benötigt für ESET PROTECT Server; SELinux kann Probleme mit anderen Anwendungen verursachen.)	apt-get install selinux-policy-dev	yum install policycoreutils-devel	zypper install selinux-policy-devel
samba (optional, nur für Remotebereitstellung erforderlich)	apt-get install samba	yum install samba samba-winbind-clients	zypper install samba samba-client
lshw	apt-get install -y lshw	yum install -y lshw	zypper install lshw

Agenten-Installation – Linux

Voraussetzungen

- Wir empfehlen, **die neueste Version von OpenSSL 1.1.1** zu verwenden. OpenSSL 3.x wird nicht unterstützt. Die niedrigste unterstützte Version von OpenSSL für Linux ist openssl-1.0.1e-30. Sie können mehrere Versionen von OpenSSL parallel auf einem System installieren. Mindestens eine unterstützte Version muss auf Ihrem System vorhanden sein.

OMit dem Befehl `openssl version` können Sie die aktuelle Standardversion abrufen.

OSie können alle auf Ihrem System vorhandenen OpenSSL-Versionen auflisten. Sie können die Dateinamenendungen mit dem Befehl `sudo find / -iname *libcrypto.so*` anzeigen.

OMit dem folgenden Befehl können Sie überprüfen, ob Ihr Linux-Client kompatibel ist: `openssl s_client -connect google.com:443 -tls1_2`

- Installieren Sie das `lshw`-Paket auf dem Linux-Client/-Server, damit der ESET Management Agent den [Hardwarebestand](#) korrekt melden kann.

Linux-Distribution	Terminalbefehl
Debian, Ubuntu	<code>sudo apt-get install -y lshw</code>
Red Hat, CentOS, RHEL	<code>sudo yum install -y lshw</code>

Linux-Distribution	Terminalbefehl
OpenSUSE	sudo zypper install lshw

- Für Linux CentOS empfehlen wir, das Paket `policycoreutils-devel` zu installieren. Führen Sie den folgenden Befehl aus, um das Paket zu installieren:

```
yum install policycoreutils-devel
```

- Servergestützte Installation des Agenten:

oDer Server muss über das Netzwerk erreichbar sein, und die Komponenten [ESET PROTECT Server](#) und [ESET PROTECT-Web-Konsole](#) müssen installiert sein.

- Offline-Installation des Agenten:

oDer Server muss über das Netzwerk erreichbar sein, und die Komponente [ESET PROTECT Server](#) muss installiert sein.

oDer Agent benötigt ein [Zertifikat](#).

oEin Datei mit dem öffentlichen Schlüssel der [Zertifizierungsstelle](#) des Servers muss vorhanden sein.

Installation

Führen Sie die folgenden Schritte aus, um den ESET Management Agenten unter Linux mit einem Terminalbefehl zu installieren:

 Vergewissern Sie sich, dass alle oben genannten Installationsvoraussetzungen erfüllt sind.

1. Laden Sie das Installationskript für Agenten herunter:

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

2. Legen Sie die Datei als ausführbar fest:

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

3. Führen Sie das im folgenden Beispiel gezeigte Installationskript aus (Neue Zeilen werden mit „\
umgebrochen, um den gesamten Befehl ins Terminal zu kopieren):

 Weitere Details finden Sie weiter unten im Abschnitt [Parameter](#).

Servergestützte Installation

```
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
```

Offline-Installation

```
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
```

ESET empfiehlt, Befehle mit vertraulichen Daten (z. B. Passwörter) aus dem Verlauf der Befehlszeile zu löschen:

1. Führen Sie `history` aus, um die Liste aller Befehle im Verlauf anzuzeigen.
2. Führen Sie `history -d line_number` aus (geben Sie die Zeilennummer des Befehls an). Alternativ können Sie mit `history -c` den gesamten Verlauf der Befehlszeile löschen.

4. Wenn Sie dazu aufgefordert werden, drücken Sie auf **y**, um das Zertifikat zu akzeptieren. Sie können alle vom Installationsprogramm zurückgegebenen SELinux-Fehler ignorieren.

5. Überprüfen Sie nach der Installation, ob der ESET Management Agenten-Dienst ausgeführt wird:

```
sudo systemctl status eraagent
```

6. Legen Sie fest, dass der **eraagent** Dienst beim Systemstart gestartet werden soll: `sudo systemctl enable eraagent`

Installationsprogramm-Log

1. Das Log des Installationsprogramms ist hilfreich für die Fehlerbehebung. Sie finden diese Datei in den [Log-Dateien](#).

Parameter

Für die Verbindung zum ESET PROTECT Server werden die Parameter `--hostname` und `--port` verwendet („port“ wird nur verwendet, wenn kein SRV-Eintrag angegeben wird). [Mögliche Verbindungsformate](#).

- **Hostname und Port**

- **IPv4-Adresse und Port**

- **IPv6-Adresse und Port**

- **Diensteintrag (SRV-Eintrag)** – Um den DNS-Ressourceneintrag unter Linux zu konfigurieren, benötigt der Computer einen funktionierenden DNS-Server in derselben Domäne. Siehe [DNS-Ressourceneintrag](#). Der SRV-Eintrag muss mit dem Präfix „_NAME._tcp“ beginnen. „NAME“ ist ein benutzerdefinierter Name (zum Beispiel „era“).

Attribut	Beschreibung	Erforderlich
--hostname	Hostname oder IP-Adresse des ESET PROTECT Servers für die Verbindung.	Ja
--port	Port des ESET PROTECT Servers (Standardwert: 2222).	Ja
--cert-path	Lokaler Pfad zur Agenten-Zertifikatsdatei (weitere Infos zu Zertifikaten).	Ja (Offline)
--cert-auth-path	Pfad zur Zertifizierungsstellendatei des Servers (weitere Infos zu Zertifizierungsstellen).	Ja (Offline)
--cert-password	Passwort für das Agentenzertifikat.	Ja (Offline)
--cert-auth-password	Passwort der Zertifizierungsstelle.	Ja (falls verwendet)
--skip-license	Der Benutzer wird während der Installation nicht zur Bestätigung der Lizenzvereinbarung aufgefordert.	Nein
--cert-content	Base64-codierter Inhalt des PKCS12-codierten Zertifikats für den öffentlichen Schlüssel plus der private Schlüssel, der für die Einrichtung sicherer Kommunikationskanäle mit Servern und Agenten verwendet wird. Verwenden Sie nur eine der Optionen --cert-path oder --cert-content.	Nein
--cert-auth-content	Base64-codierter Inhalt des DER-codierten privaten Zertifikats der Zertifizierungsstelle zur Verifizierung von Remote-Rechnern (Proxy oder Server). Verwenden Sie nur eine der Optionen --cert-auth-path oder --cert-auth-content.	Nein
--webconsole-hostname	Hostname oder IP-Adresse für die Verbindung von der Web-Konsole zum Server (Das Installationsprogramm kopiert den Wert aus „hostname“, falls er leer ist).	Nein
--webconsole-port	Port für die Verbindung von der Web-Konsole zum Server (Standardwert: 2223).	Nein
--webconsole-user	Benutzername für die Verbindung von der Web-Konsole zum Server (Standardwert: Administrator). <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;">  Sie können keinen Benutzer mit Zwei-Faktor-Authentifizierung für servergestützte Installationen verwenden. </div>	Nein
--webconsole-password	Benutzername für die Verbindung von der Web-Konsole zum Server.	Ja (servergestützt)
--proxy-hostname	HTTP-Proxy-Hostname. Verwenden Sie diesen Parameter, um den (bereits in Ihrem Netzwerk installierten) HTTP-Proxy für die Replikation zwischen ESET Management Agent und ESET PROTECT Server zu verwenden (nicht für die Zwischenspeicherung von Updates).	Falls ein Proxy verwendet wird
--proxy-port	Port des HTTP-Proxy für die Verbindung zum Datenbankserver.	Falls ein Proxy verwendet wird
--enable-imp-program	Aktivieren Sie das Produktverbesserungsprogramm.	Nein
--disable-imp-program	Deaktivieren Sie das Produktverbesserungsprogramm.	Nein

Verbindung und Zertifikate

- Die **Verbindung zum ESET PROTECT Server** muss angegeben werden: `--hostname`, `--port` (Port ist nicht erforderlich, wenn ein Servicedatensatz angegeben wird; der Standardwert für den Port ist 2222)
- Geben Sie diese Verbindungsdaten für die **servergestützte Installation** an: `--webconsole-port`, `--webconsole-user`, `--webconsole-password`
- Geben Sie Zertifikatsinformationen für die **Offline-Installation** an: `--cert-path`, `--cert-password` Für die Installationsparameter `--cert-path` und `--cert-auth-path` sind Zertifikatdateien erforderlich (`.pfx` und `.der`), die Sie aus der ESET PROTECT-Web-Konsole exportieren können. (Lesen Sie nach, wie Sie die [.pfx-Datei](#) und die [.der-Datei exportieren](#) können)

Passwort-Typ-Parameter

Passwort-Typ-Parameter können als Umgebungsvariablen oder in einer Datei angegeben, aus `stdin` gelesen oder als Nur-Text angegeben werden. Folgende Parameter sind möglich:

`--password=env:SECRET_PASSWORD`, wobei `SECRET_PASSWORD` eine Umgebungsvariable mit einem Passwort ist

`--password=file:/opt/secret`, wobei die erste Zeile der regulären Datei `/opt/secret` das Passwort enthält

`--password=stdin` weist das Installationsprogramm an, das Passwort aus der Standardeingabe zu lesen

`--password="pass:PASSWORD"` entspricht `--password="PASSWORD"` und muss angegeben werden, falls das Passwort gleich `"stdin"` (Standardeingabe) ist oder mit `"env:"`, `"file:"` oder `"pass:"` beginnt.



Die Zertifikat-Passphrase darf die folgenden Zeichen nicht enthalten: " \ Diese Zeichen verursachen kritische Fehler bei der Initialisierung des Agenten.

HTTP-Proxy-Verbindung

Falls Sie einen HTTP-Proxy für die Replikation zwischen ESET Management Agent und ESET PROTECT Server verwenden (nicht zum Zwischenspeichern von Updates), können Sie die Verbindungsparameter in `--proxy-hostname` und `--proxy-port` angeben.

BEISPIEL – Offline-Installation des Agenten mit HTTP-Proxy-Verbindung

```
./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 \  
123
```

--proxy-hostname=10.1.180.3 \

--proxy-port=3333 \



Das Kommunikationsprotokoll zwischen Agent und ESET PROTECT Server unterstützt keine Authentifizierung. Daher können für die Weiterleitung der Agenten-Kommunikation zum ESET PROTECT Server keine Proxylösungen mit Authentifizierung verwendet werden.

Wenn Sie einen vom Standard abweichenden Port für Web-Konsole oder Agent verwenden, müssen Sie möglicherweise die Firewall anpassen. Andernfalls können bei der Installation Fehler auftreten.

Upgrade und Reparatur der Agenten-Installation unter Linux

Falls Sie den Agenten auf einem System mit bereits installiertem Agenten manuell installieren, tritt eines der folgenden Szenarien auf:

- **Upgrade** – Eine neuere Version des Installationsprogramms wird ausgeführt.

OServergestützte Installation – Die Anwendung wird aktualisiert, verwendet jedoch weiterhin die bisherigen Zertifikate.

OOffline-Installation – Die Anwendung wird aktualisiert und neue Zertifikate werden verwendet.

- **Reparieren** – Dieselbe Version des Installationsprogramms wird ausgeführt. Mit dieser Option können Sie den Agenten auf einen anderen ESET PROTECT Server migrieren.

OServergestützte Installation – Die Anwendung wird neu installiert und erhält aktuelle Zertifikate vom ESET PROTECT Server (definiert im Parameter `hostname`).

OOffline-Installation – Die Anwendung wird neu installiert und neue Zertifikate werden verwendet.

Falls Sie eine manuelle Migration von einem älteren Server auf einen anderen neuen ESET PROTECT durchführen und die servergestützte Installation verwenden, müssen Sie den Installationsbefehl zwei Mal ausführen. Bei der ersten Ausführung wird der Agent aktualisiert, und beim zweiten Mal werden die neuen Zertifikate für die Verbindung vom Agenten zum ESET PROTECT Server abgerufen.

Installation der Web-Konsole – Linux

Führen Sie diese Schritte aus, um die ESET PROTECT-Web-Konsole zu installieren:



Die ESET PROTECT-Web-Konsole kann auf einem anderen Computer installiert werden als der ESET PROTECT Server. Für diese Prozedur sind [zusätzliche Schritte](#) erforderlich.

1. Installieren Sie die Apache Tomcat- und Java-Pakete. Die genauen Namen der folgenden Pakete hängen vom verwendeten Repository für Ihre Linux-Distribution ab.

Linux-Distribution	Terminalbefehle
Debian und Ubuntu-Distributionen	<pre>sudo apt-get update sudo apt-get install openjdk-17-jdk tomcat9</pre>

Linux-Distribution	Terminalbefehle
CentOS und Red Hat-Distributionen	yum update yum install java-17-openjdk tomcat
OpenSUSE	zypper refresh sudo zypper install java-17-openjdk tomcat9

2. Laden Sie die Datei für die Web-Konsole herunter (*era.war*):

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

3. Kopieren Sie die Datei *era.war* in den Tomcat-Ordner.

Debian, Ubuntu	sudo cp era.war /var/lib/tomcat9/webapps/
CentOS, Red Hat	sudo cp era.war /var/lib/tomcat/webapps/
OpenSUSE	sudo cp era.war /usr/share/tomcat/webapps/

4. Starten Sie den Tomcat-Dienst neu, um die *era.war*-Datei bereitzustellen:

Debian, Ubuntu	sudo systemctl restart tomcat9
CentOS, Red Hat	sudo systemctl restart tomcat
OpenSUSE	sudo systemctl restart tomcat

5. Vergewissern Sie sich, dass der Ordner *era* im Tomcat-Ordner existiert:

Debian, Ubuntu	ls /var/lib/tomcat9/webapps
CentOS, Red Hat	ls /var/lib/tomcat/webapps
OpenSUSE	ls /usr/share/tomcat/webapps

Die Ausgabe sollte wie folgt aussehen: era era.war

6. Legen Sie fest, dass der Tomcat-Dienst beim Systemstart gestartet werden soll: `sudo systemctl enable tomcat` (oder `tomcat9`, je nachdem, wie der Dienst heißt).

7. Wenn Sie die ESET PROTECT-Web-Konsole nicht auf demselben Computer wie den ESET PROTECT Server installiert haben, führen Sie diese zusätzlichen Schritte aus, um die Kommunikation zwischen der ESET PROTECT-Web-Konsole und dem ESET PROTECT Server zu ermöglichen:

a) Halten Sie den Tomcat-Dienst an: `sudo systemctl stop tomcat`

b) Bearbeiten Sie die Datei *EraWebServerConfig.properties*:

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

Falls sich die Datei *EraWebServerConfig.properties* nicht unter dem obigen Pfad befindet, können Sie den folgenden Befehl ausführen, um die Datei auf Ihrem System zu finden:

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

c) Suchen Sie nach dem Eintrag `server_address=localhost`

d) Ersetzen Sie `localhost` durch die IP-Adresse Ihres ESET PROTECT Servers und speichern Sie die Datei.

e) Starten Sie den Tomcat-Dienst neu: `sudo systemctl restart tomcat` (oder `tomcat9`, je nachdem, wie der Dienst heißt).

f) Legen Sie fest, dass der Tomcat-Dienst beim Systemstart gestartet werden soll: `sudo systemctl enable tomcat` (oder `tomcat9`, je nachdem, wie der Dienst heißt).

8. Wenn Sie die ESET PROTECT-Web-Konsole in einem [unterstützten Webbrowser](#) öffnen, wird ein Anmeldebildschirm angezeigt:

- Auf dem Computer, auf dem die ESET PROTECT-Web-Konsole gehostet wird: `http://localhost:8080/era`
- Auf einem beliebigen Computer mit Internetzugriff auf die ESET PROTECT-Web-Konsole (ersetzen Sie `IP_ADDRESS_OR_HOSTNAME` durch die IP-Adresse oder den Hostnamen Ihrer ESET PROTECT-Web-Konsole): `http://IP_ADDRESS_OR_HOSTNAME:8080/era`

9. Konfigurieren Sie die Web-Konsole nach der Installation:

- Der HTTP-Port wird bei der manuellen Installation von Apache Tomcat standardmäßig auf 8080 festgelegt. Wir empfehlen, eine [HTTPS-Verbindung für Apache Tomcat](#) einzurichten.
- Siehe auch die zusätzliche [Konfiguration der Web-Konsole für Enterprise-Lösungen oder leistungsschwache Systeme](#).

Rogue Detection Sensor-Installation – Linux



Falls Sie mehrere Netzwerksegmenten verwenden, müssen Sie den Rogue Detection Sensor in jedem Netzwerksegment separat installieren, um eine umfassende Liste aller Geräte im gesamten Netzwerk zu erstellen.

Voraussetzungen

- Das Netzwerk muss durchsucht werden können (Ports sind geöffnet, die Firewall blockiert die eingehende Kommunikation nicht usw.).
- Der Servercomputer ist erreichbar.
- Der [ESET Management Agent](#) muss auf dem lokalen Computer installiert sein, um alle Programmfunktionen vollständig zu unterstützen
- Das Terminal ist offen.
- Legen Sie die Installationsdatei für RD Sensor als ausführbar fest:

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

Installation

Führen Sie die folgenden Schritte aus, um die RD Sensor-Komponente unter Linux mit einem Terminalbefehl zu installieren:

! Vergewissern Sie sich, dass alle oben genannten Installationsvoraussetzungen erfüllt sind.

1. Mit folgendem Befehl können Sie die Installationsdatei als sudo ausführen:

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

2. Lesen Sie die Endbenutzer-Lizenzvereinbarung. Mit der **Leertaste** wechseln Sie zur nächsten Seite der EULA. Das Installationsprogramm fordert Sie auf, auszuwählen, ob Sie die Vereinbarung akzeptieren. Drücken Sie auf die Taste **Y**, wenn Sie zustimmen. Drücken Sie andernfalls **N**.

3. Drücken Sie **Y**, falls Sie am Produktverbesserungsprogramm teilnehmen möchten. Drücken Sie andernfalls **N**.

4. ESET Rogue Detection Sensor wird gestartet, nachdem die Installation abgeschlossen ist.

5. Um zu überprüfen, ob die Installation erfolgreich war, überprüfen Sie, ob der Dienst ausgeführt wird. Führen Sie dazu folgenden Befehl aus:

```
sudo systemctl status rdsensor
```

6. Die Log-Datei des Rogue Detection Sensor befindet sich unter [Log-Dateien](#):

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

Mobile Device Connector-Installation - Linux

Sie können den Mobile Device Connector auf einem anderen Server installieren als demjenigen, auf dem der ESET PROTECT Server ausgeführt wird. Dieses Installationsszenario kann beispielsweise verwendet werden, um den Mobile Device Connector über das Internet erreichbar zu machen und die Mobilgeräte der Benutzer jederzeit verwalten zu können.

Führen Sie die folgenden Schritte aus, um die Mobile Device Connector-Komponente unter Linux mit einem Terminalbefehl zu installieren:

! Vergewissern Sie sich, dass alle [Installationsvoraussetzungen](#) erfüllt sind.

1. Laden Sie das Installationskript für den Mobile Device Connector herunter:

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

2. Führen Sie das im folgenden Beispiel gezeigte Installationskript aus (Neue Zeilen werden mit „\
umgebrochen, um den gesamten Befehl ins Terminal zu kopieren):

```
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
```

Mit folgendem Befehl erhalten Sie die vollständige Liste aller verfügbaren Parameter (Hilfemeldung drucken):

```
--help
```

ESET empfiehlt, Befehle mit vertraulichen Daten (z. B. Passwörter) aus dem Verlauf der Befehlszeile zu löschen:

1. Führen Sie `history` aus, um die Liste aller Befehle im Verlauf anzuzeigen.
2. Führen Sie `history -d line_number` aus (geben Sie die Zeilennummer des Befehls an). Alternativ können Sie mit `history -c` den gesamten Verlauf der Befehlszeile löschen.

Erforderliche Parameter für den Installationsbefehl

Es stehen viele optionale Installationsparameter zur Verfügung, einige sind jedoch erforderlich:

- Peerzertifikat – Das ESET PROTECT-[Peerzertifikat](#) kann auf zwei verschiedene Weisen abgerufen werden:
 - **Servergestützte Installation** – Hierzu müssen Sie die Anmeldedaten des Administrators der ESET PROTECT-Web-Konsole eingeben (das Installationsprogramm lädt die erforderlichen Zertifikate automatisch herunter).
 - **Offline-Installation** - Hierzu müssen Sie ein Peerzertifikat angeben (das Proxy-Zertifikat, das Sie aus ESET PROTECT [exportiert](#) haben). Alternativ können Sie Ihr [benutzerdefiniertes Zertifikat](#) verwenden.

• Bei einer **servergestützten Installation** muss mindestens Folgendes enthalten sein:

```
--webconsole-password=
```

• Bei einer **Offline-Installation** Folgendes angeben:

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

(Für das standardmäßige Agentenzertifikat, das bei der Installation von ESET PROTECT Server erstellt wird, ist kein Passwort erforderlich.)

- HTTPS (Proxy)-Zertifikat:

o Falls Sie bereits ein HTTPS-Zertifikat haben:

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

o So generieren Sie ein neues HTTPS-Zertifikat:

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

- Verbindung zum ESET PROTECT Server (Name oder IP-Adresse):

```
--hostname=
```

- Datenbankverbindung:

o Für eine MySQL-Datenbank Folgendes angeben:

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

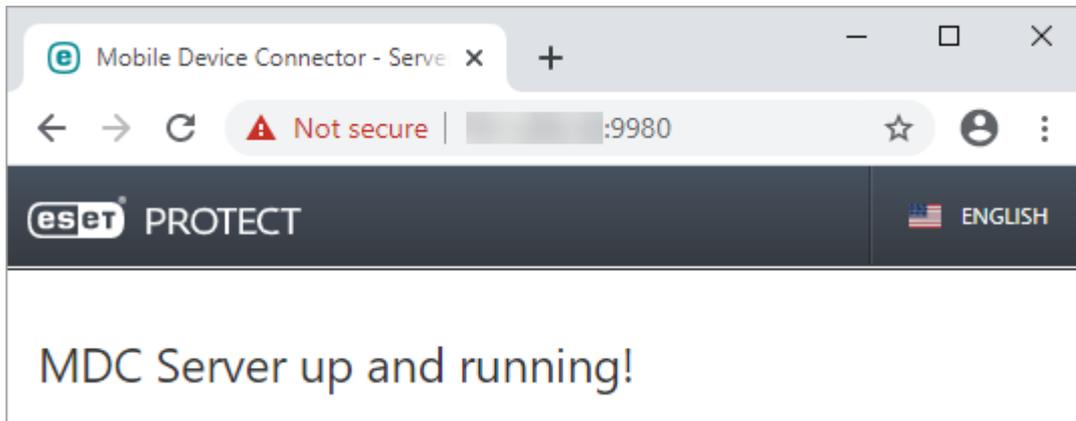
o Geben Sie für eine MS SQL-Datenbank Folgendes an:

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

Installationsprogramm-Log

Das Log des Installationsprogramms ist hilfreich für die Fehlersuche und befindet sich unter [Logdateien](#).

Überprüfen Sie nach dem Abschluss der Installation, ob der Mobile Device Connector richtig ausgeführt wird. Öffnen Sie dazu in einem Webbrowser die Adresse *https://ihr-mdm-hostname:registrierungs-port* (zum Beispiel *https://eramdm:9980*). Wenn die Installation erfolgreich war, wird die folgende Meldung angezeigt:



Sie können diese URL außerdem dazu verwenden, um die Verfügbarkeit des Connectors für Mobilgeräte aus dem Internet zu überprüfen (sofern so konfiguriert), indem Sie mit einem Mobilgeräte auf die URL zugreifen. Wenn Sie die Seite nicht erreichen können, überprüfen Sie die Firewall und die Konfiguration der Netzwerkinfrastruktur.

Voraussetzungen für den Mobile Device Connector - Linux

Zur Installation des Mobile Device Connector unter Linux müssen folgende Voraussetzungen erfüllt sein:

- Ein Datenbankserver muss installiert und mit einem Root-Konto konfiguriert sein (vor der Installation muss kein Benutzerkonto erstellt werden, dieses kann vom Installationsprogramm erstellt werden).
- Ein ODBC-Treiber zur Verbindung mit dem [Datenbankserver](#) (MySQL / MS SQL) ist auf dem Computer installiert. Siehe Kapitel [ODBC – Installation und Konfiguration](#).

i Verwenden Sie das Paket `unixODBC_23` (anstelle des standardmäßigen `unixODBC`), um eine problemlose Verbindung zwischen dem MDC und der MySQL-Datenbank zu gewährleisten. Dies gilt besonders für Installationen unter SUSE Linux.

i Stellen Sie Ihre MDM-Komponente nach Möglichkeit nicht auf demselben Hostgerät wie den ESET PROTECT Server bereit.

- Die MDMCore-Installationsdatei muss als ausführbares Programm festgelegt sein.

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

- Überprüfen Sie nach der Installation, ob der Dienst MDMCore ausgeführt wird.

```
sudo systemctl status eramdmcore
```

- Wir empfehlen, **die neueste Version von OpenSSL 1.1.1** zu verwenden. OpenSSL 3.x wird nicht unterstützt. Die niedrigste unterstützte Version von OpenSSL für Linux ist `openssl-1.0.1e-30`. Sie können mehrere Versionen von OpenSSL parallel auf einem System installieren. Mindestens eine unterstützte Version muss auf Ihrem System vorhanden sein.

o Mit dem Befehl `openssl version` können Sie die aktuelle Standardversion abrufen.

o Sie können alle auf Ihrem System vorhandenen OpenSSL-Versionen auflisten. Sie können die Dateinamenendungen mit dem Befehl `sudo find / -iname *libcrypto.so*` anzeigen.

OMit dem folgenden Befehl können Sie überprüfen, ob Ihr Linux-Client kompatibel ist: `openssl s_client -connect google.com:443 -tls1_2`

i Falls Ihre MDM-Datenbank in MySQL zu groß ist (Tausende von Geräten), reicht der Standardwert für `innodb_buffer_pool_size` nicht aus. Weitere Informationen zur Datenbankoptimierung finden Sie unter: <https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html>

Zertifikatanforderungen

- Sie brauchen ein **SSL-Zertifikat** im `.pfx`-Format, um sicher per HTTPS zu kommunizieren. Verwenden Sie nach Möglichkeit ein von einer externen Zertifizierungsstelle ausgestelltes Zertifikat. Selbstsignierte Zertifikate (inklusive von der ESET PROTECT-ZS signierte Zertifikate) werden nicht empfohlen, da manche Mobilgeräte keine selbstsignierten Zertifikate akzeptieren.
- Ihr Zertifikat muss von einer ZS signiert sein, Sie benötigen einen privaten Schlüssel und müssen das Standardverfahren verwenden (normalerweise per OpenSSL), um diese Komponenten in eine `.pfx`-Datei zusammenzuführen:

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

Dies ist das Standardverfahren für die meisten Server, die SSL-Zertifikate verwenden.
- Für die [Offline-Installation](#) benötigen Sie außerdem ein Peerzertifikat (das **Agentenzertifikat**, das Sie aus ESET PROTECT [exportiert](#) haben). Alternativ können Sie in ein [benutzerdefiniertes Zertifikat](#) mit ESET PROTECT verwenden.

Apache HTTP Proxy-Installation – Linux

ESET Management Agenten können sich über den Apache HTTP Proxy mit dem ESET PROTECT Server verbinden. Siehe auch [Funktionsweise des Proxy für ESET Management Agenten](#).

Der Apache HTTP Proxy wird normalerweise als `apache2`- oder `httpd`-Paket verteilt.

Wählen Sie die Installationsschritte für [Apache HTTP Proxy](#) entsprechend der auf dem Server verwendeten Linux-Distribution aus: Falls Sie Apache verwenden möchten, um die Ergebnisse aus ESET LiveGuard Advanced zwischenzuspeichern, lesen Sie die entsprechende [Dokumentation](#).

Linux-Installation (allgemeine Distribution) für Apache HTTP Proxy

1. Installieren Sie den Apache HTTP-Server (mindestens Version 2.4.10).
2. Stellen Sie sicher, dass die folgenden Module geladen sind:

```
access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile, authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk
```

3. Fügen Sie die Caching-Konfiguration hinzu:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
```

```
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Falls das Verzeichnis `/var/cache/apache2/mod_cache_disk` nicht existiert, erstellen Sie es und erteilen Sie Apache die Berechtigungen (r,w,x).

5. Fügen Sie die Proxy-Konfiguration hinzu:

```
AllowCONNECT 443 563 2222 8883 53535
```

```
ProxyRequests On
ProxyVia On
```

```
CacheLock on
CacheLockMaxAge 10
ProxyTimeOut 900
```

```
SetEnv proxy-initial-not-pooled 1
```

```
<VirtualHost *:3128>
ProxyRequests On
</VirtualHost>
```

```
<VirtualHost *:3128>
ServerName r.edtd.eset.com
```

```
<If "%{REQUEST_METHOD} == 'CONNECT'">
Require all denied
</If>
```

```
ProxyRequests Off
CacheEnable disk /
SSLProxyEngine On
```

```
RequestHeader set Front-End-Https "0n"
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=0n ttl=100 max=100 smax=1
0
ProxyPassReverse / http://r.edtd.eset.com/ keepalive=0n
```

```
</VirtualHost>
```

```
<Proxy *>  
Order deny,allow  
Deny from all  
Allow from all  
</Proxy>
```

6. Standardmäßig wird Port 2222 für die Kommunikation mit dem ESET Management Agenten verwendet. Falls Sie den Port bei der Installation geändert haben, verwenden Sie die geänderte Portnummer. Ersetzen Sie den Wert 2222 in der Zeile `AllowCONNECT 443 563 2222 8883 53535` durch Ihre Portnummer.

7. Aktivieren Sie den hinzugefügten Caching-Proxy und die Konfiguration hinzu. (Sie können diesen Schritt überspringen, wenn die Konfiguration in der Apache-Hauptkonfigurationsdatei enthalten ist).

8. Ändern Sie bei Bedarf die Überwachung auf den gewünschten Port (standardmäßig ist Port 3128 eingestellt).

9. Optionale Standardauthentifizierung:

o Fügen Sie die Authentifizierungskonfiguration zur Proxy-Anweisung hinzu:

```
AuthType Basic  
AuthName "Password Required"  
AuthUserFile /etc/apache2/password.file  
AuthGroupFile /etc/apache2/group.file  
Require group usergroup
```

o Erstellen Sie eine Passwortdatei mit dem Befehl `/etc/htpasswd/.htpasswd -c`.

o Erstellen Sie manuell eine Datei mit dem Namen „group.file“ mit dem Befehl `usergroup:username`.

10. Starten Sie den Apache HTTP-Server neu.

Installationen des Apache HTTP Proxy in Ubuntu Server und anderen Debian-basierten Linux-Distributionen

1. Installieren Sie die neueste Version des Apache HTTP-Servers aus dem Repository „apt“:

```
sudo apt-get install apache2
```

2. Führen Sie den folgenden Befehl aus, um die erforderlichen Apache-Module zu laden:

```
sudo a2enmod access_compat auth_basic authn_core authn_file authz_core\  
authz_groupfile authz_host proxy proxy_http proxy_connect cache cache_disk
```

3. Bearbeiten Sie die Apache-Caching-Konfigurationsdatei:

```
sudo vim /etc/apache2/conf-available/cache_disk.conf
```

Kopieren und fügen Sie die folgenden Konfigurationsangaben ein:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Dieser Schritt wird normalerweise nicht benötigt. Falls jedoch das Caching-Verzeichnis fehlt, führen Sie die folgenden Befehle aus:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. Bearbeiten Sie die Apache-Proxy-Konfigurationsdatei:

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

Kopieren und fügen Sie die folgenden Konfigurationsangaben ein:

```
AllowCONNECT 443 563 2222 8883 53535
```

```
ProxyRequests On
ProxyVia On
```

```
CacheLock on
CacheLockMaxAge 10
ProxyTimeOut 900
```

```
SetEnv proxy-initial-not-pooled 1
```

```
<VirtualHost *:3128>
```

```
ProxyRequests On
```

```
</VirtualHost>
```

```
<VirtualHost *:3128>
```

```
    ServerName r.edtd.eset.com
```

```
<If "%{REQUEST_METHOD} == 'CONNECT'">
```

```
Require all denied
```

```
</If>
```

```
ProxyRequests Off
```

```
CacheEnable disk /
```

```
SSLProxyEngine On
```

```
RequestHeader set Front-End-Https "On"
```

```
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=100
```

```
ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On
```

```
</VirtualHost>
```

```
<Proxy *>  
Order deny,allow  
Deny from all  
Allow from all  
</Proxy>
```

6. Standardmäßig wird Port 2222 für die Kommunikation mit dem ESET Management Agenten verwendet. Falls Sie den Port bei der Installation geändert haben, verwenden Sie die geänderte Portnummer. Ersetzen Sie den Wert 2222 in der Zeile `AllowCONNECT 443 563 2222 8883 53535` durch Ihre Portnummer.

7. Aktivieren Sie die in früheren Schritten bearbeiteten Konfigurationsdateien:

```
sudo a2enconf cache_disk.conf proxy.conf
```

8. Setzen Sie den überwachten Port des Apache HTTP-Servers auf 3128. Bearbeiten Sie die Datei `/etc/apache2/ports.conf` und ersetzen Sie `Listen 80` durch `Listen 3128`.

9. Optionale Standardauthentifizierung:

```
sudo vim /etc/apache2/mods-enabled/proxy.conf
```

o Fügen Sie die Authentifizierungs-Konfiguration vor dem folgenden `</Proxy>` Block ein:

```
AuthType Basic  
AuthName "Password Required"  
AuthUserFile /etc/apache2/password.file  
AuthGroupFile /etc/apache2/group.file  
Require group usergroup
```

o Installieren Sie `apache2-utils` und erstellen Sie eine neue Passwortdatei (zum Beispiel Benutzername: `user`, Gruppe: `usergroup`):

```
sudo apt-get install apache2-utils  
sudo htpasswd -c /etc/apache2/password.file user
```

o Erstellen Sie eine Datei mit dem Namen „group“:

```
sudo vim /etc/apache2/group.file
```

Kopieren und fügen Sie die folgende Zeile ein:

```
usergroup:user
```

10. Starten Sie den Apache HTTP-Server mit dem folgenden Befehl neu:

```
sudo systemctl restart apache2
```

Weiterleitung nur für ESET-Kommunikation Entfernen Sie Folgendes, um nur die ESET-Kommunikation weiterzuleiten:

```
<Proxy *>  
Order deny,allow  
Deny from all  
Allow from all  
</Proxy>
```

Fügen Sie außerdem den folgenden Code hinzu:

```
<Proxy *>  
Deny from all  
</Proxy>
```

```
##.eset.com:
```

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>  
Allow from all  
</ProxyMatch>
```

```
##.eset.eu:
```

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>  
Allow from all  
</ProxyMatch>
```

```
##.eset.systems:
```

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?$>  
Allow from all  
</ProxyMatch>
```

```
#Antispam module (ESET Mail Security only):
```

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(ds1-uk-
rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-
uk11.mailshell.net)(:[0-9]+)?(/.)*?>
```

Allow from all

```
</ProxyMatch>
```

#Services (activation)

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(edf-pcs.cloudapp.net|edf-
pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.)*?>
```

Allow from all

```
</ProxyMatch>
```

#ESET servers accessed directly via IP address:

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(91.228.165.|91.228.166.|91.2
28.167.|38.90.226.)(:[0-9]+)(:[0-9]+)?(/.)*?>
```

Allow from all

```
</ProxyMatch>
```

#AV Cloud over port 53535

```
<ProxyMatch ^.*e5.sk.*>
```

Allow from all

```
</ProxyMatch>
```

Sämtliche Kommunikation weiterleiten

Fügen Sie den folgenden Code hinzu, um sämtliche Kommunikation weiterzuleiten:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

Entfernen Sie außerdem den folgenden Code:

```
<Proxy *>
Deny from all
</Proxy>
```

#*.eset.com:

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?([a-zA-Z0-9-]{0,63}\.)*?([a-zA-
Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M])(:[0-9]+)?(/.)*?>
```

Allow from all

</ProxyMatch>

#*.eset.eu:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?>

Allow from all

</ProxyMatch>

#*.eset.systems:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?>

Allow from all

</ProxyMatch>

#Antispam module (ESET Mail Security only):

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net)(:[0-9]+)?(/.*)?>

Allow from all

</ProxyMatch>

#Services (activation)

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(edf-pcs.cloudapp.net|edf-pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?>

Allow from all

</ProxyMatch>

#ESET servers accessed directly via IP address:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(91.228.165.|91.228.166.|91.228.167.|38.90.226.)(:[0-9]+)(:[0-9]+)?(/.*)?>

Allow from all

</ProxyMatch>

#AV Cloud over port 53535

<ProxyMatch ^.*e5.sk.*>

Allow from all

</ProxyMatch>

Proxy-Verkettung (sämtlicher Datenverkehr)

ESET PROTECT unterstützt keine Verkettung von Proxies, wenn die Proxies Authentifizierung erfordern. Wenn Sie eine eigene transparente Webproxy-Lösung verwenden, müssen Sie ggf. weitere Konfigurationsschritte vornehmen, die hier nicht aufgeführt sind. Fügen Sie die folgende Zeile zur Proxy-Konfiguration hinzu (Passwort funktioniert nur für untergeordneten Proxy):

```
<VirtualHost *:3128>
ProxyRequests On
ProxyRemote * http://IP_ADDRESS:3128
</VirtualHost>
```

Wenn Sie die Proxy-Verkettung auf der virtuellen ESET PROTECT-Appliance verwenden, müssen Sie die SELinux-Policy anpassen. Öffnen Sie das Terminal auf der ESET PROTECT-VA und führen Sie den folgenden Befehl aus:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
```

Konfigurieren Sie den HTTP-Proxy für eine große Anzahl von Clients

Wenn Sie die 64-Bit-Version des Apache HTTP-Proxy verwenden, können Sie das Thread-Limit für Ihren Apache HTTP Proxy erhöhen. Bearbeiten Sie die Konfigurationsdatei *httpd.conf* in Ihrem Apache HTTP Proxy-Ordner. Suchen Sie die folgenden Einstellungen in der Datei und passen Sie die Werte an die Anzahl Ihrer Clients an.

Ersetzen Sie den Beispielwert 5000 durch den gewünschten Wert. Der Höchstwert ist 32000.

```
ThreadLimit 5000
ThreadsPerChild 5000
```

Ändern Sie den Rest der Datei nicht.

Konfigurieren von Apache HTTP Proxy für die Weiterleitung der Verbindungen zwischen Agenten und Server

1. Öffnen Sie auf dem Proxy-Computer die Datei

i. Debian-Distributionen
`/etc/apache2/mods-available/proxy.conf`

ii. Red Hat-Distributionen
`/etc/httpd/conf/httpd.conf`

2. Fügen Sie die folgenden Zeilen zum Ende der Datei hinzu:

```
AllowCONNECT 443 563 2222 8883 53535
```

3. Öffnen Sie auf dem Proxy-Computer die Datei

i. Debian-Distributionen
`/etc/apache2/apache2.conf`

ii.Red Hat-Distributionen
/etc/httpd/conf/httpd.conf

4.Suchen Sie die folgende Zeile:

Listen 80

und ändern Sie sie zu

Listen 3128

5.Falls Sie bei Ihrer Proxy-Konfiguration in Schritt 1 Einschränkungen für IP-Adressen hinzugefügt haben, müssen Sie den Zugriff auf Ihren ESET PROTECT Server erlauben:

Fügen Sie in einem separaten `ProxyMatch`-Segment Folgendes hinzu:

I.Die Adresse, die Ihre Agenten verwenden, um sich mit dem ESET PROTECT Server zu verbinden.

II.Alle weiteren möglichen Adressen Ihres ESET PROTECT Servers (IP, FQDN)
(Fügen Sie den gesamten untenstehenden Code hinzu. Die IP-Adresse 10.1.1.10 und der Hostname `hostname.example` sind nur Beispiele und müssen durch Ihre tatsächlichen Adressen ersetzt werden. Außerdem können Sie den `ProxyMatch`-Ausdruck in [diesem Knowledgebase-Artikel](#) generieren).

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\/.*)?|10\.1\.1\.10(:[0-9]+)?(\/.*)?)$>
Allow from all
</ProxyMatch>
```

6.Starten Sie den *Apache HTTP Proxy*-Dienst neu.

Caching konfigurieren

Mit [htcacheclean](#) können Sie die Cachegröße und die Cache-Bereinigung für Apache HTTP Proxy konfigurieren. Siehe auch [Cache-Konfigurationsanweisungen für die ESET PROTECT VA](#).

SELinux-Einstellung

Wenn Sie den Proxy auf der virtuellen ESET PROTECT-Appliance verwenden, müssen Sie die SELinux-Policy anpassen (gilt möglicherweise auch für andere Linux-Distributionen). Öffnen Sie das Terminal auf der ESET PROTECT-VA und führen Sie den folgenden Befehl aus:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
sudo semanage port -a -t http_port_t -p tcp 2222
```

Squid HTTP Proxy-Installation auf Ubuntu Server

Auf Ubuntu Server können Sie den Squid-Proxy anstelle von Apache verwenden. Führen Sie die folgenden Schritte aus, um Squid auf Ubuntu Server (und ähnlichen Debian-basierten Linux-Distributionen) zu installieren und konfigurieren:

1. Installieren Sie das Squid3-Paket:

```
sudo apt-get install squid3
```

2. Bearbeiten Sie die Squid-Konfigurationsdatei `/etc/squid3/squid.conf` und ersetzen Sie:

```
#cache_dir ufs /var/spool/squid3 100 16 256
```

durch:

```
cache_dir ufs /var/spool/squid3 3000 16 256 max-size=2000000000
```



- Außerdem können Sie die Gesamtgröße des Cache (3000 MB im Beispiel) und die Anzahl der Unterverzeichnisse auf der ersten Ebene (16 im Beispiel) und der zweiten Ebene (256 im Beispiel) im Cacheverzeichnis anpassen.
- Der Parameter `max-size` definiert die maximale Größe für zwischengespeicherte Dateien in Byte.

3. Stoppen Sie den Dienst „squid3“.

```
sudo systemctl stop squid3  
sudo squid3 -z
```

4. Bearbeiten Sie die Squid-Konfigurationsdatei erneut und fügen Sie `http_access allow all` vor `http_access deny all` hinzu, um allen Clients den Proxyzugriff zu erlauben.

5. Starten Sie den Dienst „squid3“ neu:

```
sudo systemctl restart squid3
```

Mirror-Tool - Linux

[Sind Sie Windows-Benutzer?](#)

Das Mirror-Tool wird für Updates der Erkennungsroutine im Offlinemodus benötigt. Falls Ihre Clientcomputer nicht mit dem Internet verbunden sind und Updates die Erkennungsroutine brauchen, können Sie die Update-Dateien mit dem Mirror-Tool von den ESET-Updateservern herunterladen und lokal speichern.



Das Mirror-Tool lädt nur Updates für die Erkennungsroutine und andere Programm-Module herunter, keine PCUs (Updates für Programmkomponenten) oder ESET LiveGrid®-Daten. Das Tool kann außerdem ein vollständiges [Offline-Repository](#) erstellen. Alternativ können Sie die Produkte einzeln aktualisieren.

Voraussetzungen

- Der Zielordner muss für die Freigabe, den Samba/Windows- oder den HTTP/FTP-Dienst verfügbar sein, je nachdem, wie Sie die Updates bereitstellen möchten.

OESET Sicherheitsprodukte für Windows – Updates können remote per HTTP oder mit einem freigegebenen Ordner ausgeführt werden.

OESET Sicherheitsprodukte für Linux/macOS – Updates können remote nur per HTTP ausgeführt werden. Wenn Sie einen freigegebenen Ordner verwenden, muss dieser sich auf demselben Computer befinden wie das ESET Sicherheitsprodukt.

- Sie benötigen eine gültige [Offline-Lizenzdatei](#) inklusive Benutzername und Passwort. Achten Sie beim Generieren der Lizenzdatei darauf, das Kontrollkästchen neben der Option **Benutzername und Passwort einschließen** zu markieren. Geben Sie außerdem einen **Lizenznamen** an. Sie benötigen eine Offline-Lizenzdatei, um das Mirror-Tool zu aktivieren und den Update-Mirror zu generieren.

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

Verwenden des Mirror-Tools

1. Laden Sie das Mirror-Tool auf der [ESET-Downloadseite](#) (Bereich **Standalone-Installationsprogramme**) herunter.
2. Extrahieren Sie den heruntergeladenen Archiv.
3. Öffnen Sie das Terminal im Ordner mit der *MirrorTool*-Datei und legen Sie die Datei als ausführbar fest:

```
chmod +x MirrorTool
```

4. Führen Sie den folgenden Befehl aus, um alle verfügbaren Parameter für das Mirror-Tool und dessen Version anzuzeigen:

```
./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 Sämtliche Filter unterscheiden zwischen Groß- und Kleinschreibung.

Parameter	Beschreibung
<code>--updateServer</code>	Wenn Sie diesen Parameter verwenden, müssen Sie die komplette URL des Updateservers angeben.
<code>--offlineLicenseFilename</code>	Geben Sie einen Pfad zu Ihrer Offline-Lizenzdatei an (siehe oben).
<code>--mirrorOnlyLevelUpdates</code>	Kein Argument erforderlich. Wenn diese Option festgelegt ist, werden nur Level-Updates heruntergeladen (Nano-Updates werden nicht heruntergeladen). Weitere Informationen zu Updatetypen finden Sie in unserem Knowledgebase-Artikel .
<code>--mirrorFileFormat</code>	<p> Stellen Sie vor der Verwendung des <code>--mirrorFileFormat</code> Parameters sicher, dass Ihre Umgebung keine Mischung aus älteren (6.5 und älter) und neueren Versionen (6.6 und neuer) des ESET-Sicherheitsprodukts enthält. Fehler bei der Verwendung dieses Parameters können dazu führen, dass Ihre ESET-Sicherheitsprodukte falsch aktualisiert werden.</p> <p>Sie können festlegen, welche Art von Updatedateien heruntergeladen werden sollen. Mögliche Werte (Groß-/Kleinschreibung beachten):</p> <ul style="list-style-type: none"> • <code>dat</code> - Verwenden Sie diesen Wert, falls Sie in Ihrer Version nur Version 6.5 und älter des ESET-Sicherheitsprodukts verwenden. • <code>dll</code> - Verwenden Sie diesen Wert, falls Sie in Ihrer Version nur Version 6.6 und neuer des ESET-Sicherheitsprodukts verwenden.
<code>--compatibilityVersion</code>	<p>Der Parameter wird beim Erstellen eines Mirrors für veraltete Produkte (<code>ep4</code>, <code>ep5</code>) ignoriert. Dieser optionale Parameter gilt für das Mirror-Tool, das zusammen mit ESET PROTECT 8.1 und neueren Versionen verteilt wird.</p> <p>Das Mirror-Tool lädt Updatedateien herunter, die mit der ESET PROTECT Repository-Version kompatibel sind, die Sie im Parameterargument im Format <code>x.x</code> oder <code>x.x.x.x</code> angeben, z. B. <code>--compatibilityVersion 9.1</code> oder <code>--compatibilityVersion 8.1.13.0</code>.</p>

Um weniger Daten aus dem ESET-Repository herunterzuladen, können Sie die neuen Parameter im Mirror-Tool verwenden, das mit ESET PROTECT 9 ausgeliefert wird: `--filterFilePath` und `--dryRun`:

1. Erstellen Sie einen Filter im *JSON*-Format (siehe `--filterFilePath` unten).



2. Testen Sie das Mirror-Test-Tool mit dem Parameter `--dryRun` (siehe unten) und passen Sie den Filter bei Bedarf an.

3. Führen Sie das Mirror-Tool mit dem Parameter `--filterFilePath` und dem definierten Downloadfilter zusammen mit den Parametern `--intermediateRepositoryDirectory` und `--outputRepositoryDirectory` aus.

4. Führen Sie das Mirror-Tool regelmäßig aus, um immer die neuesten Installationsprogramme zu verwenden.

Parameter	Beschreibung
<p><code>--filterFilePath</code></p>	<p>Verwenden Sie diesen optionalen Parameter, um ESET Sicherheitsprodukte anhand einer Textdatei im <i>JSON</i>-Format zu filtern, die sich im gleichen Ordner wie das Mirror-Tool befindet, z. B.: <code>--filterFilePath filter.txt</code></p> <p>Beschreibung der Filterkonfiguration:</p> <p>Die Konfigurationsdatei für die Produktfilterung hat die folgende <i>JSON</i>-Struktur:</p> <ul style="list-style-type: none"> • <i>JSON</i>-Stammobjekt: <ul style="list-style-type: none"> • <code>use_legacy</code> (boolescher Wert, optional) – Wenn dieser Wert gleich „Wahr“ ist, werden veraltete Produkte einbezogen. • <code>defaults</code> (<i>JSON</i>-Objekt, optional) – Definiert die Filtereigenschaften, die auf alle Produkte angewendet werden. <ul style="list-style-type: none"> ■ <code>languages</code> (Liste) – Geben Sie ISO-Sprachcodes für die Sprachen an, die einbezogen werden sollen, z. B. "fr_FR" für Französisch. In der folgenden Tabelle finden Sie weitere Sprachcodes. Geben Sie weitere Sprachen mit Komma und Leerzeichen getrennt ein, zum Beispiel: (["en_US", "zh_TW", "de_DE"]) ■ <code>platforms</code> (Liste) – Plattformen, die einbezogen werden sollen (["x64", "x86", "arm64"]). <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p> Verwenden Sie den <code>platforms</code>-Filter mit Bedacht. Wenn das Mirror-Tool beispielsweise nur 64-Bit-Installationsprogramme herunterlädt und Ihre Infrastruktur 32-Bit-Computer enthält, können die 64-Bit ESET Sicherheitsprodukte nicht auf den 32-Bit-Computern installiert werden.</p> </div> <ul style="list-style-type: none"> ■ <code>os_types</code> (Liste) – Betriebssystemtypen, die einbezogen werden sollen (["windows"], ["linux"], ["mac"]). • <code>products</code> (Liste der <i>JSON</i>-Objekte, optional) – Filter, die auf bestimmte Produkte angewendet werden, überschreibt <code>defaults</code> für bestimmte Produkte. Die Objekte haben die folgenden Eigenschaften: <ul style="list-style-type: none"> ■ <code>app_id</code> (Zeichenfolge) – Erforderlich, wenn <code>name</code> nicht angegeben wird. ■ <code>name</code> (Zeichenfolge) – Erforderlich, wenn <code>app_id</code> nicht angegeben wird. ■ <code>version</code> (Zeichenfolge) – Gibt an, welche Version oder welcher Versionsbereich einbezogen werden soll. ■ <code>languages</code> (Zeichenfolge) – ISO-Sprachcodes der Sprachen, die einbezogen werden sollen (siehe Tabelle unten). ■ <code>platforms</code> (Liste) – Plattformen, die einbezogen werden sollen (["x64", "x86", "arm64"]). ■ <code>os_types</code> (Liste) – Betriebssystemtypen, die einbezogen werden sollen (["windows"], ["linux"], ["mac"]). <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p> Um angemessene Werte für die Felder zu ermitteln, führen Sie das Mirror-Tool im Dry-Run-Modus aus und suchen Sie in der erstellten CSV-Datei nach dem entsprechenden Produkt.</p> </div> <p>Format für Versionszeichenfolgen</p> <p>Alle Versionsnummern bestehen aus vier Ziffern, die durch Punkte getrennt sind (z. B. 7.1.0.0). Wenn Sie in Versionsfiltern weniger Zahlen angeben (z. B. 7.1), werden Nullen für die restlichen Zahlen angenommen (7.1 entspricht 7.1.0.0).</p> <p>Versionszeichenfolgen können eines der beiden folgenden Formate haben:</p> <ul style="list-style-type: none"> • <code>[> < >= <= <=>]<n>.<n>.<n>.<n>]]</code> <p>OWählt Versionen größer/kleiner oder gleich/kleiner oder gleich/gleich der angegebenen Version aus.</p> <ul style="list-style-type: none"> • <code><n>.<n>.<n>.<n>]] - <n>.<n>.<n>.<n>]]</code> <p>OWählt Versionen aus, die größer oder gleich der unteren Grenze und kleiner oder gleich der oberen Grenze sind.</p> <p>Vergleiche werden numerisch für alle Teile der Versionsnummer von links nach rechts durchgeführt.</p> <div style="border: 1px solid green; padding: 10px; margin: 10px 0;"> <p>JSON-Beispiel</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": ">7.1.0.0" }] } </pre> </div>

Parameter	Beschreibung
--dryRun	<p>Wenn Sie diesen optionalen Parameter verwenden, lädt das Mirror-Tool keine Dateien herunter, generiert jedoch eine .csv-Datei mit allen Paketen, die heruntergeladen werden.</p> <p>Sie können diesen Parameter ohne die Pflichtparameter --intermediateRepositoryDirectory und --outputRepositoryDirectory verwenden, z. B.: MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv.</p> <div style="border: 1px solid blue; padding: 5px;"> <p>i Manche ESET Installationsprogramme sind sprachunabhängig (Sprachcode multilang). Das Mirror-Tool listet diese Versionen in der .csv-Datei auf, auch wenn Sie Sprachen in --filterFilePath angegeben haben.</p> </div> <p>Wenn Sie den Parameter --dryRun und die Parameter --intermediateRepositoryDirectory und --outputRepositoryDirectory verwenden, löscht das Mirror-Tool das <i>outputRepositoryDirectory</i> nicht.</p>
--listUpdatableProducts	<p>Listet alle ESET Produkte auf, für die das Mirror Tool Modul-Updates herunterladen kann (sofern --excludedProducts nicht verwendet wird).</p> <p>Der Parameter ist ab den folgenden Mirror Tool Versionen verfügbar: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).</p>

Das Mirror-Tool erstellt eine andere Ordnerstruktur als der Endpoint-Mirror. Jeder Ordner enthält die Updatedateien für eine Gruppe von Produkten. Sie müssen den vollständigen Pfad zum korrekten Ordner in den Update-Einstellungen des Produkts angeben, das den Mirror verwendet.



Beispiel: Um ESET PROTECT 9 über den Mirror zu aktualisieren, legen Sie den [Update-Server](#) wie folgt fest (abhängig vom Stamm Ihres HTTP-Servers):

`http://your_server_address/mirror/ eset_upd/era6`

Hinweis: Die folgenden ESET Remote Management-Lösungen verwenden denselben era6 Mirror-Ordner: ERA 6, ESMC 7, ESET PROTECT.

[Tabelle mit Sprachcodes](#)

--	--	--	--	--	--

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

Im folgende Beispiel sehen Sie eine komplexere Konfiguration für ein Offline-Repository mit ausgewählten Produkten und Sprachen und aktiviertem Download von veralteten Dateien in der Datei *filter.txt* (siehe Details zu --filterFilePath weiter oben für Beispiele zum Dateiinhalt):

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

ESET empfiehlt, Befehle mit vertraulichen Daten (z. B. Passwörter) aus dem Verlauf der Befehlszeile zu löschen:

- i** 1. Führen Sie `history` aus, um die Liste aller Befehle im Verlauf anzuzeigen.
- 2. Führen Sie `history -d line_number` aus (geben Sie die Zeilennummer des Befehls an). Alternativ können Sie mit `history -c` den gesamten Verlauf der Befehlszeile löschen.

Mirror-Tool und Updateeinstellungen

- Sie können die Ausführung des Mirror-Tools planen, um die Downloads von Modulupdates zu automatisieren. Navigieren Sie dazu in der Web-Konsole zu **Client-Tasks > Betriebssystem > Befehl ausführen**. **Wählen Sie Auszuführende Befehlszeile** (inklusive Pfad zum `MirrorTool.exe`) und einen passenden Auslöser aus (z. B. CRON für jede Stunde um `0 0 * * * ? *`). Alternativ können Sie den Windows-Taskplaner oder Cron in Linux verwenden.
- Erstellen Sie eine neue Policy und verweisen Sie im Feld **Updateserver** auf Ihren Mirror-Server bzw. Ihren freigegebenen Ordner, um Updates auf Clientcomputern zu konfigurieren.

Komponenteninstallation unter macOS

In den meisten Installationsszenarien müssen Sie verschiedene ESET PROTECT-Komponenten auf verschiedenen Computern installieren, beispielsweise um Unterschiede in der Netzwerkarchitektur zu berücksichtigen oder Leistungsanforderungen zu erfüllen.

- i** macOS wird nur als Client unterstützt. Der [ESET Management Agent](#) und die [ESET-Produkte für macOS](#) können unter macOS installiert werden. Der ESET PROTECT Server kann jedoch nicht unter macOS installiert werden.

Agenten-Installation – macOS

Sie können den ESET Management Agenten unter macOS auf zwei Arten installieren:

- Remote – Mit dem Server-Task **Agenten-Bereitstellung**. Wenn bei der Remote-Bereitstellung des ESET Management Agenten Probleme auftreten (Servertask **Agenten-Bereitstellung** wird mit Fehlerstatus beendet), beachten Sie die Hinweise unter [Behebung von Fehlern bei der Agenten-Bereitstellung](#).
- Lokal – Mit den folgenden Anweisungen.

Voraussetzungen

- ESET PROTECT Server und die ESET PROTECT-Web-Konsole werden auf einem Servercomputer installiert.
- Ein Agenten-[Zertifikat](#) wurde erstellt und auf dem lokalen Laufwerk vorbereitet.
- Eine [Zertifizierungsstelle](#) ist auf dem lokalen Laufwerk vorbereitet (nur für nicht signierte Zertifikate erforderlich).

Installation

Führen Sie die folgenden Schritte aus, um den ESET Management Agenten unter macOS lokal zu installieren:

 Vergewissern Sie sich, dass alle oben genannten Installationsvoraussetzungen erfüllt sind.

1. Laden Sie die Installationsdatei (Standalone-Installationsdatei *.dmg*) von der [ESET-Downloadseite](#) oder von Ihrem Systemadministrator herunter.
2. Doppelklicken Sie auf die Datei *Agent-MacOSX-x86_64.dmg* und doppelklicken Sie anschließend auf die *.pkg*-Datei, um die Installation zu starten.
3. Fahren Sie mit der Installation fort. Geben Sie die **Serververbindungsdaten** ein, wenn Sie dazu aufgefordert werden:
 - **Server-Hostname:** Hostname oder IP-Adresse des ESET PROTECT Servers
 - **Server-Port:** Port für die Kommunikation zwischen Agent und Server (standardmäßig 2222).
 - **Proxy verwenden:** Klicken Sie hier, wenn Sie einen HTTP-Proxy für die Verbindung zwischen Agent und Server verwenden möchten.

Diese Proxyeinstellung wird nur für die Replikation zwischen dem ESET Management Agenten und dem ESET PROTECT Server verwendet, nicht für die Zwischenspeicherung von Updates.

- **Proxy-Hostname:** Hostname oder IP-Adresse des HTTP-Proxycomputers.
 - **Proxyport:** Standardmäßig 3128.
 - **Benutzername, Passwort:** geben Sie die Anmeldeinformationen für Ihren Proxy ein, falls dieser Authentifizierung verwendet.
- Sie können die Proxyeinstellungen später in Ihrer [Policy](#) ändern. Sie müssen den [Proxy](#) installieren, bevor Sie eine Verbindung zwischen Agent und Server über einen Proxy konfigurieren können.

4. Wählen Sie ein [Peerzertifikat](#) und ein Passwort für das Zertifikat aus. Optional können Sie eine [Zertifizierungsstelle](#) hinzufügen.

 Die Zertifikat-Passphrase darf die folgenden Zeichen nicht enthalten: " \ Diese Zeichen verursachen kritische Fehler bei der Initialisierung des Agenten.

5. Überprüfen Sie das Installationsverzeichnis und klicken Sie auf **Installieren**. Der Agent wird auf dem Computer installiert.
6. Die Log-Datei des ESET Management Agenten befindet sich unter folgendem Pfad:

```
/Library/Application Support/com.eset.remoteadministrator.agent/Logs/  
/Users/%user%/Library/Logs/EraAgentInstaller.log
```

 Das Kommunikationsprotokoll zwischen Agent und ESET PROTECT Server unterstützt keine Authentifizierung. Daher können für die Weiterleitung der Agenten-Kommunikation zum ESET PROTECT Server keine Proxylösungen mit Authentifizierung verwendet werden. Wenn Sie einen vom Standard abweichenden Port für Web-Konsole oder Agent verwenden, müssen Sie möglicherweise die Firewall anpassen. Andernfalls können bei der Installation Fehler auftreten.

ISO-Abbild

Das ESET PROTECT-Installationsprogramm kann unter anderem als ISO-Abbilddatei (Kategorie All-in-One-Installationspakete) [heruntergeladen](#) werden. Das ISO-Abbild enthält Folgendes:

- ESET PROTECT-Installationspaket
- Getrennte Installationsprogramme für jede Komponente

Das ISO-Abbild ist besonders nützlich, wenn sie alle ESET PROTECT-Installationsprogramme an einem Ort aufbewahren möchten. Wenn Sie über ein ISO-Abbild verfügen, müssen Sie die Installationsprogramme nicht für jede Installation von der ESET-Website herunterladen. Das ISO-Abbild ist auch hilfreich, wenn Sie ESET PROTECT auf einer virtuellen Maschine installieren möchten.

DNS-Diensteintrag

So richten Sie einen DNS-Ressourceneintrag ein:

1. Navigieren Sie auf dem DNS-Server (DNS-Server im Domänencontroller) zu **Systemsteuerung > Verwaltung**.
2. Wählen Sie den DNS-Wert aus.
3. Wählen Sie in der Baumstruktur des DNS Managers `_tcp` aus und erstellen Sie einen neuen **Eintrag für Dienstidentifizierung (SRV)**.
4. Geben Sie den Dienstnamen im Feld **Dienst** ein. Beachten Sie dabei die DNS-Standardregeln und geben Sie vor dem Dienstnamen einen Unterstrich ein (`_`). Verwenden Sie einen eigenen Dienstnamen, z. B. `_era`.
5. Geben Sie das TCP-Protokoll im Feld **Protokoll** im folgenden Format ein: `_tcp`.
6. Geben Sie im Feld **Portnummer** den Port 2222 ein.
7. Geben Sie den vollständig qualifizierten Domännennamen (FQDN) des ESET PROTECT Servers im Feld **Host, der diesen Dienst anbietet** ein.
8. Klicken Sie auf **OK > Fertig**, um den Eintrag zu speichern. Der Eintrag wird in der Liste angezeigt.

So überprüfen Sie einen DNS-Eintrag:

1. Melden Sie sich bei einem beliebigen Computer in Ihrer Domäne an und öffnen Sie die Eingabeaufforderung (`cmd.exe`).
2. Geben Sie `nslookup` in der Befehlszeile ein und drücken Sie die **Eingabetaste**.
3. Geben Sie `set querytype=svr` ein und drücken Sie die **Eingabetaste**.
4. Geben Sie `_era._tcp.domain.name` ein und drücken Sie die **Eingabetaste**. Die Dienstidentifizierung wird korrekt angezeigt.

i Denken Sie daran, den Wert unter „Host, der diesen Dienst anbietet“ in den FQDN des neuen Servers zu ändern, wenn Sie den ESET PROTECT-Server auf einem anderen Computer installieren.

Offline-Installation von ESET PROTECT

Um ESET PROTECT und die Komponenten in Umgebungen ohne Internetzugang zu installieren, führen Sie die Installationsanweisungen aus (mit unter Windows installiertem ESET PROTECT).

Auf Computern mit Internetverbindung

1. Erstellen Sie einen freigegebenen Netzwerkordner.
2. Laden Sie die folgenden Installationsprogramme in den freigegebenen Ordner herunter:
 - [ESET PROTECT All-in-One-Installationsprogramm](#)
 - Ein [unterstütztes JDK-Paket](#) (wird für die Web-Konsole benötigt).
 - ESET Management Agenten-Installationsprogramm
 - Installationsprogramme für ESET Sicherheitsprodukt (z. B. ESET Endpoint Security)

Auf Offline-Windows-Computern im gleichen lokalen Netzwerk

1. Kopieren Sie die Installationsprogramme aus dem freigegebenen Netzwerkordner auf einen Offline-Windows-Computer, auf dem Sie ESET PROTECT installieren möchten.
2. Installieren Sie das JDK-Paket.
3. [Installieren Sie ESET PROTECT](#) unter Windows mit dem All-in-One-Installationsprogramm. Wählen Sie während der Installation **Später aktivieren** aus.
4. Aktivieren Sie ESET PROTECT mit einer [Offline-Lizenz](#).
5. Stellen Sie den ESET Management Agenten mit dem [Installations-Skript für Agenten](#) auf den Computern in Ihrer Offlineumgebung bereit. Bearbeiten Sie das Installationsskript, um die neue URL für den Zugriff auf das Agenten-Installationspaket aus dem freigegebenen Netzwerkordner zu verwenden.
6. Verwenden Sie einen [Task „Software-Installation“](#), um die ESET Sicherheitsprodukte auf den Arbeitsstationen bereitzustellen. Wählen Sie **<Choose package>** aus und geben Sie eine benutzerdefinierte URL für das Installationspaket aus dem lokalen Repository an.
7. [Aktivieren Sie die verwalteten Endpunkte mit einer Offlinelizenz](#).
8. [Deaktivieren Sie ESET LiveGrid®](#).

Wir empfehlen dringend, die [ESET Offline-Infrastruktur](#) mit einem lokalen Update-Repository regelmäßig zu aktualisieren. Aktualisieren Sie die Module des ESET Sicherheitsprodukts regelmäßig. Wenn die Module nicht aktualisiert werden, werden die Computer in der ESET PROTECT-Web-Konsole als **Nicht aktualisiert** markiert. Um diese Warnung in der Web-Konsole stummzuschalten, klicken Sie auf den Computer in der Liste und wählen Sie **Stummschalten** im Kontextmenü aus.

Anweisungen zur Aktualisierung von ESET PROTECT finden Sie unter [Upgrade von ESET PROTECT-Komponenten in Offlineumgebungen](#).

Upgradeprozeduren

Upgrades von ESET PROTECT Server und anderen ESET PROTECT Komponenten können auf verschiedene Arten ausgeführt werden. Siehe auch [Prozeduren für Migration und erneute Installation](#).

Stellen Sie vor dem Upgrade auf ESET PROTECT 9.1 sicher, dass Sie ein [unterstütztes Betriebssystem](#) verwenden.

! Falls Sie eine ältere, nicht unterstützte Datenbank installiert haben (MySQL 5.5 oder MS SQL 2008/2012), [aktualisieren Sie Ihre Datenbank](#) auf eine [kompatible Datenbankversion](#), bevor Sie den ESET PROTECT Server aktualisieren.

Upgrade von ERA 5 oder 6.5

Direkt-Upgrades werden nicht unterstützt, siehe [Migration von ERA 5.x](#) oder [Upgrade von ERA 6.x](#).

Upgrade von ESMC 7.2 auf ESET PROTECT Version 9.1

Wählen Sie eine der Upgrade-Prozeduren aus:

Upgradeprozeduren	Betriebssystem	Kommentar
Task Komponenten-Upgrade in der Web-Konsole	Windows/Linux	
ESET PROTECT 9.1 All-in-One-Installationsprogramm	Windows	Das All-in-One-Installationsprogramm ist die empfohlene Upgradeoption, wenn die vorhandene Installation mit dem All-in-One-Installationsprogramm durchgeführt wurde und Sie Standardinstallationen der MS SQL-Datenbank und von Apache Tomcat verwenden.
Manuelles komponentenbasiertes Upgrade	Linux	Linux-Anleitung für fortgeschrittene Benutzer.
Virtuelle ESET PROTECT Appliance aktualisieren	Virtuelle Linux-Appliance	

i Um herauszufinden, welche Versionen der einzelnen ESET PROTECT-Komponenten Sie installiert haben, müssen Sie die Version Ihres ESET PROTECT Servers überprüfen. Öffnen Sie die Seite [Info](#) in der ESET PROTECT-Web-Konsole und machen Sie sich mit der [Liste der ESET PROTECT-Komponentenversionen](#) vertraut.

Task „ESET PROTECT Komponenten-Upgrade“

Empfehlungen vor dem Upgrade

Verwenden Sie nach Möglichkeit den Task [ESET PROTECT Komponenten-Upgrade](#) in der ESET PROTECT-Web-Konsole, um Upgrades für Ihre ESET PROTECT-Infrastruktur zu installieren. Lesen Sie die hier beschriebenen Anweisungen vor dem Upgrade sorgfältig.



Wenn das Komponenten-Upgrade auf einem Computer fehlschlägt, auf dem der ESET PROTECT Server oder die Web-Konsole ausgeführt wird, ist unter Umständen keine Remote-Anmeldung mehr bei der Web-Konsole möglich. Konfigurieren Sie nach Möglichkeit vor dem Upgrade einen physischen Zugriff auf den Servercomputer. Wenn Sie keinen physikalischen Zugriff auf dem Computer einrichten können, stellen Sie sicher, dass Sie sich mit Administratorberechtigungen per Remotedesktop anmelden können. [Sichern](#) Sie außerdem die Datenbanken von ESET PROTECT Server und Mobile Device Connector, bevor Sie diesen Vorgang ausführen. Erstellen Sie einen Snapshot oder klonen Sie Ihre virtuelle Maschine, um die virtuelle Appliance zu sichern.

[Führen Sie ein Upgrade von der virtuellen ESMC-Appliance durch?](#)

[Ist die ESET PROTECT Server-Instanz auf einem Failover-Cluster installiert?](#)

Wenn die ESET PROTECT Server-Instanz auf einem Failover-Cluster installiert ist, müssen Sie die ESET PROTECT Server-Komponente auf jedem Clusterknoten manuell aktualisieren. Nach dem Upgrade des ESET PROTECT Servers können Sie das [Komponenten-Upgrade](#) ausführen, um den Rest der Infrastruktur (zum Beispiel ESET Management Agenten auf Clientcomputern) zu aktualisieren.

[Wichtige Hinweise, bevor Sie Apache HTTP Proxy unter Microsoft Windows aktualisieren](#)

Falls Sie Apache HTTP Proxy einsetzen und benutzerdefinierte Einstellungen in Ihrer *httpd.conf*-Datei verwenden (z. B. Benutzername und Passwort), müssen Sie Ihre *httpd.conf*-Originaldatei (in *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*) sichern. Wenn Sie keine benutzerdefinierten Einstellungen verwenden, müssen Sie die Datei *httpd.conf* nicht sichern. Verwenden Sie eine der unter [Upgrade von Apache HTTP Proxy](#) beschriebenen Methoden, um Apache HTTP Proxy auf die neueste Version zu aktualisieren.



Wenn Ihre *httpd.conf*-Originaldatei benutzerdefinierte Einstellungen enthält (z. B. Benutzername und Passwort), müssen Sie die Einstellungen aus der Sicherung Ihrer *httpd.conf*-Datei nach dem erfolgreichen Upgrade von Apache HTTP Proxy unter Windows kopieren zur neuen *httpd.conf*-Datei kopieren. Verwenden Sie Ihre *httpd.conf*-Originaldatei nicht mit der aktualisierten Version von Apache HTTP Proxy, da ansonsten Fehler auftreten können. Kopieren Sie nur Ihre benutzerdefinierten Einstellungen aus der alten Datei und verwenden Sie die neue *httpd.conf*-Datei. Alternativ können Sie Ihre neue *httpd.conf*-Datei manuell anpassen, wie unter [Apache HTTP Proxy-Installation – Windows](#) beschrieben.

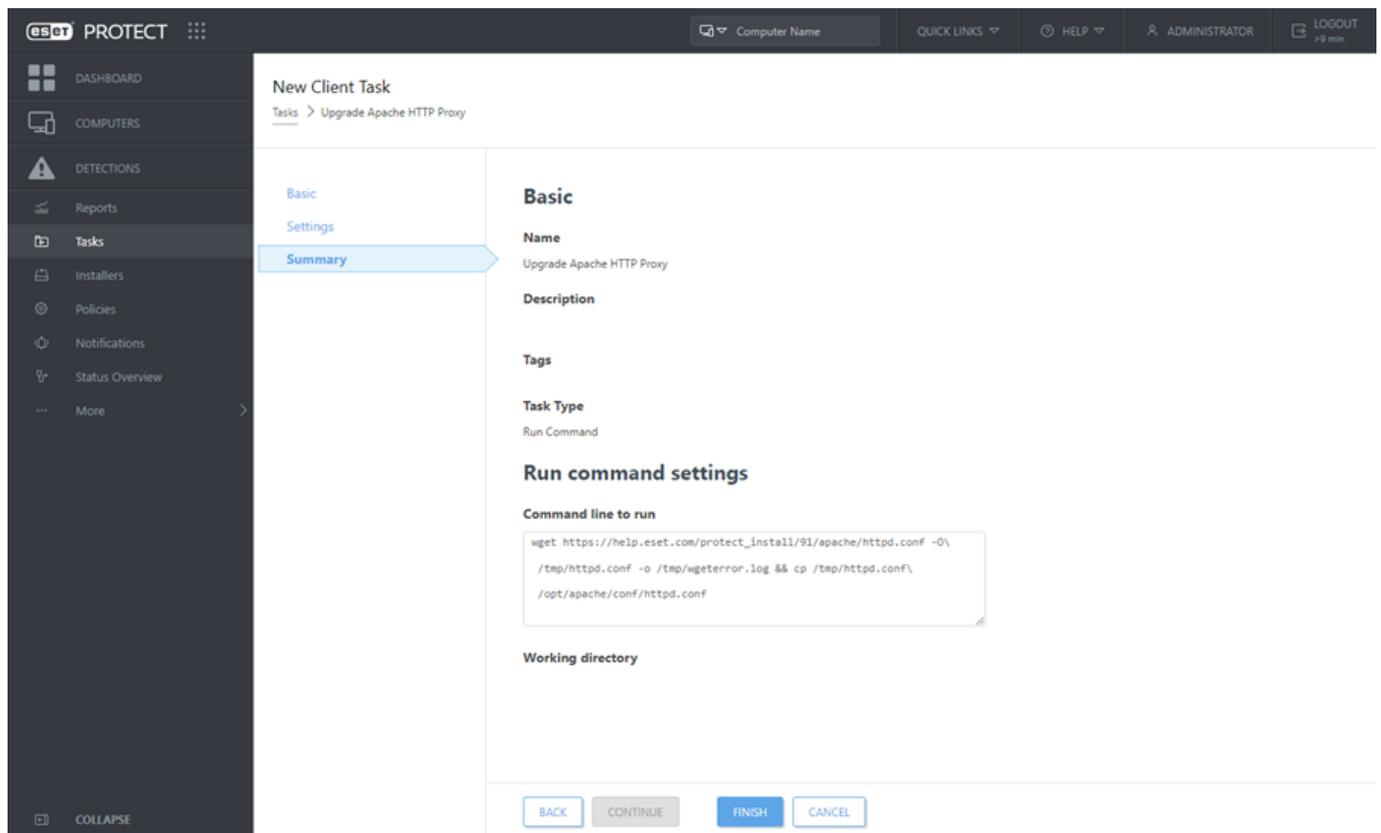
[Wichtige Hinweise, bevor Sie Apache HTTP Proxy auf einer virtuellen Appliance aktualisieren](#)

Falls Sie **Apache HTTP Proxy** einsetzen und benutzerdefinierte Einstellungen in Ihrer *httpd.conf*-Datei verwenden (z. B. Benutzername und Passwort), müssen Sie Ihre *httpd.conf*-Originaldatei (in */opt/apache/conf/*) sichern und anschließend den Task **Upgrade von ESET PROTECT-Komponenten** ausführen, um **Apache HTTP Proxy** zu

aktualisieren. Falls Sie keine benutzerdefinierten Einstellungen verwenden, brauchen Sie keine Sicherung von *httpd.conf* zu erstellen.

Nachdem der Task „Komponenten-Upgrade“ erfolgreich ausgeführt wurde, führen Sie den folgenden Befehl aus. Weisen Sie ihn zum Computer zu, auf dem Apache HTTP Proxy installiert ist. Führen Sie den Client-Task [Befehl ausführen](#) aus, um die Datei *httpd.conf* zu aktualisieren (wird für den korrekten Betrieb der aktualisierten Version von Apache HTTP Proxy benötigt):

```
wget https://help.eset.com/protect_install/91/apache/httpd.conf -O\
/tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\
/opt/apache/conf/httpd.conf
```



Falls Apache HTTP Proxy auf Ihrem VA-Computer ausgeführt wird, können Sie diesen Befehl auch direkt in der Konsole der virtuellen ESET PROTECT-Appliance ausführen. Bei Bedarf können Sie die Apache HTTP Proxy-Konfigurationsdatei [httpd.conf](#) auch manuell ersetzen.

⚠ Wenn Ihre *httpd.conf*-Originaldatei benutzerdefinierte Einstellungen enthält (z. B. Benutzername und Passwort), kopieren Sie die Einstellungen aus der Sicherung Ihrer *httpd.conf*-Datei und fügen Sie nur die benutzerdefinierten Einstellungen zur neuen *httpd.conf*-Datei hinzu. Verwenden Sie Ihre *httpd.conf*-Originaldatei nicht mit der aktualisierten Version von Apache HTTP Proxy, da ansonsten Fehler auftreten können. Kopieren Sie nur Ihre benutzerdefinierten Einstellungen aus der alten Datei und verwenden Sie die neue *httpd.conf*-Datei. Alternativ können Sie Ihre neue *httpd.conf*-Datei manuell anpassen. Beachten Sie die ausführlichen Einstellungen unter [Apache HTTP Proxy-Installation unter Linux](#).

Upgrades auf ESET PROTECT 9.1 sind nur von ESMC Version 7.2 und neuer aus möglich. ESET PROTECT 9 benachrichtigt Sie automatisch, wenn [eine neue Version von ESET PROTECT Server verfügbar ist](#).

Sichern Sie die folgenden Daten, bevor Sie das Upgrade ausführen:

- Alle Zertifikate (Zertifizierungsstelle, Serverzertifikat, Proxy- und Agent-Zertifikat)
- Exportieren Sie Ihre [Zertifizierungsstellenzertifikate](#) aus dem alten ESET PROTECT Server in eine *.der*-Datei auf einem externen Speichermedium.
- Exportieren Sie Ihre [Peerzertifikate](#) (für ESET Management Agent und ESET PROTECT Server) und den privaten Schlüssel als *.pfx*-Datei von einem alten ESET PROTECT Server auf ein externes Speichermedium.
- Ihre [ESMC-/ESET PROTECT-Datenbank](#). Falls Sie eine ältere, nicht unterstützte Datenbank installiert haben (MySQL 5.5 oder MS SQL 2008/2012), [aktualisieren Sie Ihre Datenbank](#) auf eine [kompatible Datenbankversion](#), bevor Sie den ESET PROTECT Server aktualisieren.

Stellen Sie vor dem Upgrade auf ESET PROTECT 9.1 sicher, dass Sie ein [unterstütztes Betriebssystem](#) verwenden.

Um Ihre ESET-Sicherheitsprodukte zu aktualisieren, führen Sie den [Task „Software-Installation“](#) mit dem neuesten Installationspaket aus, um die neueste Version über Ihr vorhandenes Produkt zu installieren.

Empfohlene Upgradeprozedur

1. ESET PROTECT Server aktualisieren - Wählen Sie nur den Computer mit dem ESET PROTECT Server als Ziel für den Task **Upgrade von ESET PROTECT-Komponenten** aus.
2. Wählen Sie einige Clientcomputer (als Testsample, mindestens ein Client pro Betriebssystem und Bitness-Plattform) aus und führen Sie den Task **Upgrade von ESET PROTECT-Komponenten** auf diesen Computern aus.

Verwenden Sie nach Möglichkeit [Apache HTTP Proxy](#) (oder einen anderen transparenten Webproxy mit Caching), um die Netzwerklast zu reduzieren. Die Testclientcomputer lösen den Download bzw. das Caching der Installationsprogramme aus. Bei der nächsten Ausführung des Tasks werden die Installationsprogramme direkt aus dem Cache an die Clientcomputer verteilt.

3. Nachdem sich die Computer mit aktualisierten ESET Management Agenten erfolgreich mit dem ESET PROTECT Server verbunden haben, können Sie die restlichen Clients aktualisieren.

i Um die ESET Management Agenten auf allen verwalteten Computern im Netzwerk zu aktualisieren, wählen Sie die statische Gruppe **Alle** als Ziel für den Task **Upgrade von ESET PROTECT-Komponenten** aus. Der Task überspringt Computer, auf denen bereits der neueste ESET Management Agent ausgeführt wird. ESET PROTECT 9.1 unterstützt [automatische Upgrades für ESET Management Agenten](#) auf verwalteten Computern.

Die folgenden Komponenten werden automatisch aktualisiert:

- ESET PROTECT Server
- ESET Management Agent
- ESET PROTECT-Web-Konsole - Gilt nur, wenn Apache Tomcat sowohl unter Windows als auch in Linux-Distributionen im Standardordner installiert wurde, inklusive der virtuellen ESET PROTECT-Appliance (Beispiel: */var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*).

Einschränkungen für Upgrades der Web-Konsole

o Apache Tomcat wird nicht aktualisiert, wenn Sie die ESET PROTECT-Web-Konsole mit dem Task „Komponenten-Upgrade“ aktualisieren.

! o Das Upgrade der ESET PROTECT-Web-Konsole funktioniert nicht, wenn Apache Tomcat an einem benutzerdefinierten Ort installiert wurde.

o Wenn eine benutzerdefinierte Version von Apache Tomcat installiert ist (manuelle Installation des Tomcat-Diensts), kann die ESET PROTECT-Web-Konsole anschließend nicht mit dem All-in-One-Installationsprogramm oder mit dem Task Komponenten-Upgrade aktualisiert werden.

- ESET PROTECT Mobile Device Connector

Komponenten, die manuell aktualisiert werden müssen:

ESET-Komponenten

- [ESET Rogue Detection Sensor](#) – Führen Sie den [Task „Software-Installation“](#) für das Upgrade aus. Installieren Sie alternativ die neueste Version über eine ältere Version (folgen Sie den Installationsanweisungen für [Windows](#) oder [Linux](#)). Falls Sie den RD Sensor mit einer Version von ESMC 7.2 und höher installiert haben, ist kein Upgrade erforderlich, da keine neue Version des RD Sensors veröffentlicht wurde.

Komponenten von Drittanbietern

Neben ESET Komponenten verwendet ESET PROTECT auch Komponenten von Drittanbietern, die möglicherweise veraltet sind und manuell aktualisiert werden müssen.

Klicken Sie in der ESET PROTECT Web-Konsole auf **Quicklinks > Veraltete Komponenten**, um die veralteten Komponenten von Drittanbietern anzuzeigen.

Die virtuelle ESET PROTECT Appliance enthält keine veralteten Komponenten von Drittanbietern.

ESET PROTECT meldet ältere als die folgenden Versionen als veraltet:

Komponente von Drittanbietern:	Version:
Microsoft SQL Server	2019 (Build 15.0.4223.0) ¹
MySQL	8.0.0.0
Betriebssystem ²	Windows Server 2016
Apache Tomcat	9.0.62
Java	17.0

1 Ermitteln Sie [Version und Edition Ihrer SQL Server Datenbankengine](#) und installieren Sie das neueste [kumulative Update](#).

2 ESET PROTECT meldet kein veraltetes Linux Betriebssystem.

Führen Sie die Update-Anweisungen für Komponenten von Drittanbietern aus:

- [Datenbankserver](#)
- [Betriebssystem](#)
- [Apache Tomcat](#)

- [Java Runtime Environment](#)
- [Apache HTTP Proxy](#)

Fehlerbehebung

- Überprüfen Sie, ob Sie von einem aktualisierten Computer [auf das ESET PROTECT-Repository zugreifen können](#).
- Wenn mindestens eine Komponente bereits auf eine neuere Version aktualisiert wurde, kann der Task „ESET PROTECT Komponenten-Upgrade“ nicht erneut ausgeführt werden.
- Wenn keine klare Ursache für den Fehler ermittelt werden kann, können Sie die Komponenten manuell aktualisieren. Lesen Sie unsere Anweisungen für [Windows](#) oder [Linux](#).
- In den [allgemeinen Hinweisen zur Fehlerbehebung](#) finden Sie weitere Vorschläge zur Behebung von Upgradeproblemen.

Verwenden Sie das ESET PROTECT 9.1 All-in-One-Installationsprogramm für Ihr Upgrade

Mit dem ESET PROTECT 9.1 All-in-One-Installationsprogramm können Sie ESMC 7.2 oder eine ältere Version von ESET PROTECT auf die neueste Version von ESET PROTECT 9.1 aktualisieren.

Das All-in-One-Installationsprogramm ist die empfohlene Upgradeoption, wenn die vorhandene Installation mit dem All-in-One-Installationsprogramm durchgeführt wurde und Sie Standardinstallationen der MS SQL-Datenbank und von Apache Tomcat verwenden.

ESET PROTECT 9.1 [All-in-One-Installationsprogramm](#) installiert standardmäßig Microsoft SQL Server Express 2019.

o Falls Sie eine ältere Windows Edition verwenden (Server 2012 oder SBS 2011), wird standardmäßig Microsoft SQL Server Express 2014 installiert.

o Das Installationsprogramm generiert automatisch ein zufälliges Passwort für die Datenbankauthentifizierung (gespeichert in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`).

- Microsoft SQL Server Express Hat eine Obergrenze von je 10 GB für relationale Datenbanken. Microsoft SQL Server Express sollte nicht verwendet werden:

 - In Unternehmensumgebungen oder großen Netzwerken.
 - Falls Sie ESET PROTECT mit [ESET Inspect](#) verwenden möchten.

Upgrades auf ESET PROTECT 9.1 sind nur von ESMC Version 7.2 und neuer aus möglich.

Sichern Sie die folgenden Daten, bevor Sie das Upgrade ausführen:

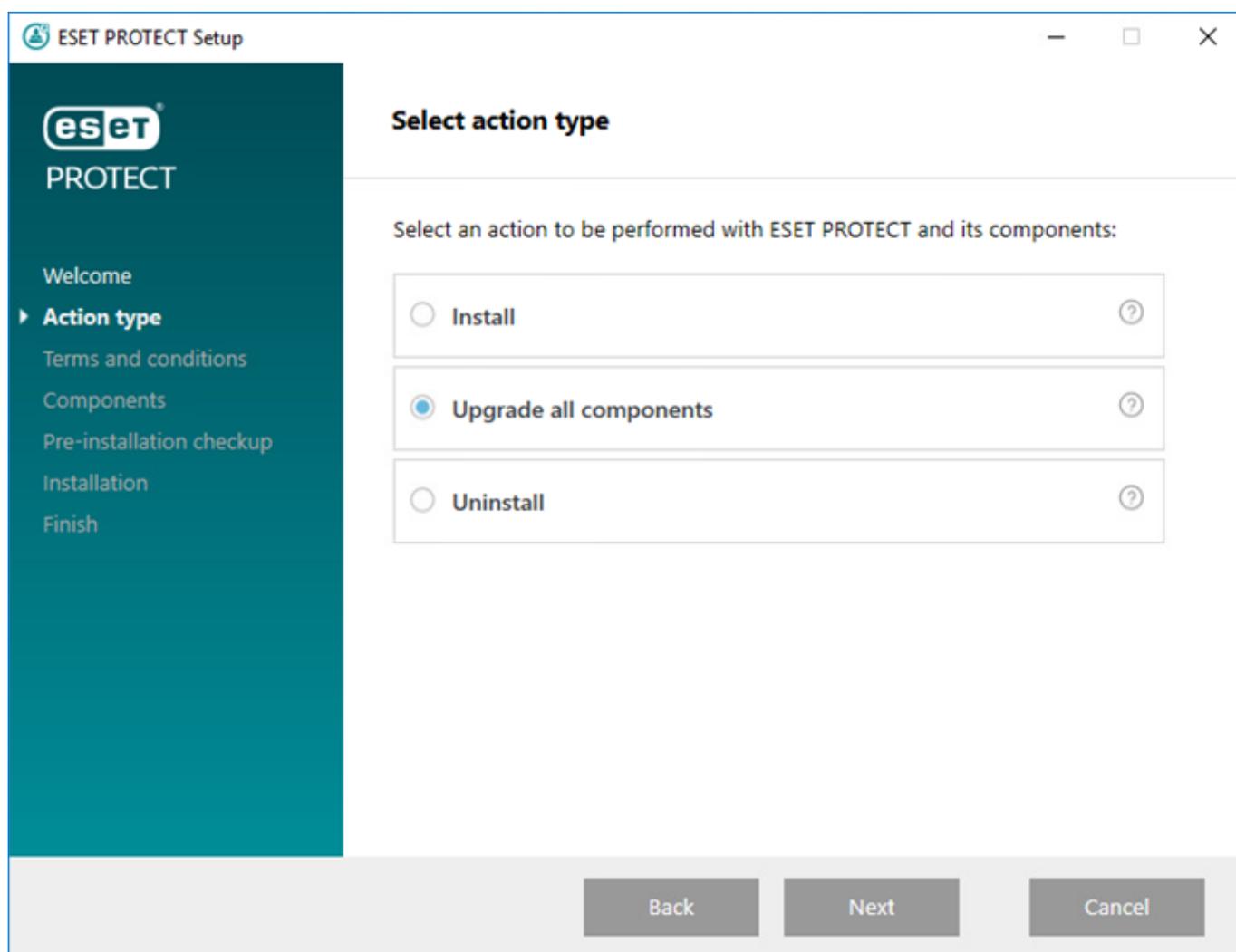
- Alle Zertifikate (Zertifizierungsstelle, Serverzertifikat, Proxy- und Agent-Zertifikat)
- Exportieren Sie Ihre [Zertifizierungsstellenzertifikate](#) aus dem alten ESET PROTECT Server in eine *.der*-Datei auf einem externen Speichermedium.
- Exportieren Sie Ihre [Peerzertifikate](#) (für ESET Management Agent und ESET PROTECT Server) und den privaten Schlüssel als *.pfx*-Datei von einem alten ESET PROTECT Server auf ein externes Speichermedium.
- Ihre [ESMC-/ESET PROTECT-Datenbank](#). Falls Sie eine ältere, nicht unterstützte Datenbank installiert haben (MySQL 5.5 oder MS SQL 2008/2012), [aktualisieren Sie Ihre Datenbank](#) auf eine [kompatible Datenbankversion](#), bevor Sie den ESET PROTECT Server aktualisieren.

Stellen Sie vor dem Upgrade auf ESET PROTECT 9.1 sicher, dass Sie ein [unterstütztes Betriebssystem](#) verwenden.

1.Führen Sie *Setup.exe* aus.

2.Wählen Sie eine Sprache aus und klicken Sie auf **Weiter**.

3.Wählen Sie **Upgrade für alle Komponenten** aus und klicken Sie auf **Weiter**.



4.Lesen Sie die **Endbenutzer-Lizenzvereinbarung**, akzeptieren Sie sie und klicken Sie auf **Weiter**.

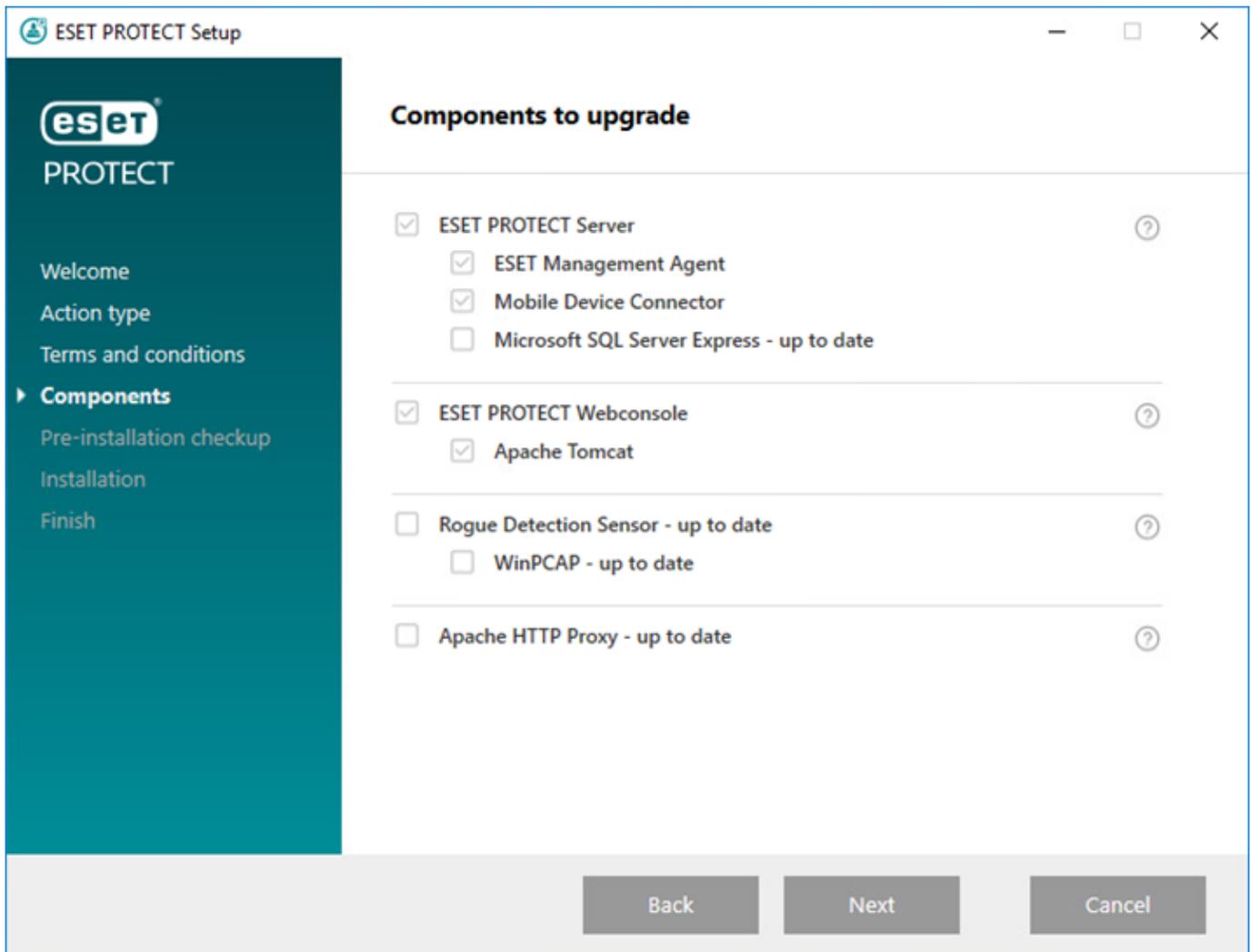
5.Überprüfen Sie unter **Komponenten**, für welche ESET PROTECT-Komponenten Upgrades verfügbar sind, und klicken Sie auf **Weiter**.

Einschränkungen für Upgrades von Apache Tomcat und der Web-Konsole

- Wenn eine benutzerdefinierte Version von Apache Tomcat installiert ist (manuelle Installation des Tomcat-Diensts), kann die ESET PROTECT-Web-Konsole anschließend nicht mit dem All-in-One-Installationsprogramm oder mit dem Task Komponenten-Upgrade aktualisiert werden.
- Das Apache Tomcat-Upgrade löscht den Ordner *era* in *C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps*. Wenn Sie zusätzliche Daten im Ordner *era* gespeichert haben, müssen Sie diese Daten vor dem Upgrade sichern.
- Wenn Sie den *C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps* enthält zusätzliche Daten (abgesehen von den Ordnern *era* und *ROOT*), das Apache Tomcat-Upgrade wird nicht ausgeführt und nur die Web-Konsole wird aktualisiert.
- Bei den Upgrades für die Web-Konsole und für Apache Tomcat wird die [Offlinehilfe](#) gelöscht. Falls Sie die Offlinehilfe mit ESMC oder einer älteren Version von ESET PROTECT verwendet haben, können Sie sie nach dem Upgrade für ESET PROTECT 9.1 erneut erstellen, um sicherzustellen, dass Sie die neueste Offline-Hilfe für Ihre Version von ESET PROTECT verwenden.

Upgrade-Einschränkungen für Apache HTTP Proxy

- Das All-in-One-Installationsprogramm überschreibt die Datei *httpd.conf* und speichert die ursprüngliche Konfiguration als *httpd.conf.old*. [Sichern Sie die Konfiguration und verwenden Sie sie erneut](#), um Ihre benutzerdefinierte Apache HTTP Proxy-Konfiguration zu behalten.



6. Führen Sie die **Prüfungen vor der Installation** durch, um sich zu vergewissern, dass Ihr System alle Voraussetzungen erfüllt.

7. Klicken Sie auf **Upgrade**, um das Upgrade von ESET PROTECT zu starten. Je nach System und

Netzwerkconfiguration kann das Upgrade einige Zeit dauern.

8. Klicken Sie nach Abschluss des Upgrades auf **Fertig stellen**.

9. Führen Sie nach dem Upgrade von ESET PROTECT ein Upgrade für den ESET Management Agenten auf den verwalteten Computern mit dem Task „Komponenten-Upgrade“ aus. ESET PROTECT 9.1 unterstützt [automatische Upgrades für ESET Management Agenten](#) auf verwalteten Computern.

Upgrade von ERA 6.5

Direkte Upgrades zu ESET PROTECT 9.1 werden nicht unterstützt.

Falls Sie ERA 6.5 installiert haben, führen Sie die folgenden Aktionen aus:

1. [Führen Sie ein Upgrade von ERA 6.5 zu ESET PROTECT 8.1 aus](#).
2. [Führen Sie ein Upgrade von ESET PROTECT 8.1 zu ESET PROTECT 9.1 aus](#).

Datenbankserver sichern/aktualisieren

ESET PROTECT verwendet eine Datenbank zur Speicherung von Clientdaten. In den folgenden Abschnitten werden [Sicherung](#) und [Upgrade](#) der Datenbank für den ESET PROTECT Server (oder ESMC Server) bzw. für MDM beschrieben:

- Für den Fall, dass Sie keine Datenbank für den ESET PROTECT Server konfiguriert haben, ist **Microsoft SQL Server Express** im Installationsprogramm enthalten. ESET PROTECT 9.1 [All-in-One-Installationsprogramm](#) installiert standardmäßig Microsoft SQL Server Express 2019.

o Falls Sie eine ältere Windows Edition verwenden (Server 2012 oder SBS 2011), wird standardmäßig Microsoft SQL Server Express 2014 installiert.

o Das Installationsprogramm generiert automatisch ein zufälliges Passwort für die Datenbankauthentifizierung (gespeichert in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`).

- Microsoft SQL Server Express Hat eine Obergrenze von je 10 GB für relationale Datenbanken. Microsoft SQL Server Express sollte nicht verwendet werden:

 - In Unternehmensumgebungen oder großen Netzwerken.
 - Falls Sie ESET PROTECT mit [ESET Inspect](#) verwenden möchten.

- Falls Sie eine ältere, nicht unterstützte Datenbank installiert haben (MySQL 5.5 oder MS SQL 2008/2012), [aktualisieren Sie Ihre Datenbank](#) auf eine [kompatible Datenbankversion](#), bevor Sie den ESET PROTECT Server aktualisieren.

Siehe auch [Migration der ESET PROTECT-Datenbank](#).

Die folgenden Voraussetzungen für Microsoft SQL Server müssen erfüllt sein:

- Installieren Sie eine [unterstützte Version von Microsoft SQL Server](#). Wählen Sie bei der Installation den **Gemischten Modus** für die Authentifizierung aus.
- Falls Sie Microsoft SQL Server bereits installiert haben, legen Sie die Authentifizierung auf **Gemischter Modus (SQL Server-Authentifizierung und Windows-Authentifizierung)** fest. Führen Sie dazu die Anweisungen in diesem [KnowledgeBase-Artikel](#) aus. Falls Sie die **Windows-Authentifizierung** verwenden möchten, um sich beim Microsoft SQL Server anzumelden, führen Sie die Schritte in diesem [Knowledgebase-Artikel](#) aus.
- Erlauben Sie TCP/IP-Verbindungen zum SQL Server. Führen Sie dazu die Anweisungen in diesem [KnowledgeBase-Artikel](#) ab Teil II aus. **Erlauben Sie TCP/IP-Verbindungen zum SQL Server** aus.

- i**
- Für die Konfiguration, Verwaltung und Administration von Microsoft SQL Server (Datenbanken und Benutzer) empfehlen wir Ihnen, [SQL Server Management Studio \(SSMS\) herunterzuladen](#).
 - [Installieren Sie SQL Server sollte nicht auf einem Domänencontroller](#) (z. B. Windows SBS oder Essentials). Sollten Sie ESET PROTECT auf einem anderen Server installieren oder während der Installation nicht die SQL Server Express-Komponente auswählen (in diesem Fall müssen Sie SQL Server oder MySQL als ESET PROTECT-Datenbank verwenden).

Datenbankserver-Sicherung und Wiederherstellung

Alle Informationen und Einstellungen von ESET PROTECT werden in einer Datenbank gespeichert. Wir empfehlen, die Datenbank regelmäßig zu sichern, um einen Datenverlust zu vermeiden. Sie können die Sicherung später verwenden, wenn Sie ESET PROTECT auf einen neuen Server migrieren. Weitere Informationen finden Sie im Abschnitt für den verwendeten Datenbanktyp:

- i**
- Die Namen von Datenbanken und Log-Dateien bleiben auch nach der Änderung des Produktnamens von ESET Security Management Center zu ESET PROTECT gleich.
 - Führen Sie die [Sicherungsanweisungen für die VA-Datenbank](#) aus, falls Sie die virtuelle ESET PROTECT-Appliance verwenden.

Sicherungsbeispiele für MS SQL

Führen Sie die folgenden Anweisungen aus, um eine Sicherungsdatei einer MS SQL-Datenbank zu erstellen:

- !**
- Diese Beispiele gelten für die Standardeinstellungen (z. B. Standard-Datenbankname und Verbindungseinstellungen). Passen Sie Ihr Sicherungsskript ggf. an die Änderungen an, die Sie an den Standardeinstellungen vorgenommen haben.
- Sie benötigen ausreichende Berechtigungen, um die folgenden Befehle auszuführen. Falls Sie kein lokales Administratorkonto verwenden, müssen Sie den Sicherungspfad ändern, zum Beispiel zu 'C:\USERS\PUBLIC\BACKUPFILE'.

Einmalige Datenbanksicherung

Führen Sie diesen Befehl in einer Windows-Eingabeaufforderung aus, um eine Sicherung in einer Datei mit dem Namen **BACKUPFILE** zu erstellen:

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE' "
```

i In diesem Beispiel steht **HOST** für die IP-Adresse bzw. den Hostnamen und **ERASQL** für den Namen der MS SQL Server-Instanz. Sie können ESET PROTECT Server in einer SQL-Instanz mit benutzerdefiniertem Namen installieren (falls Sie MS SQL verwenden). Passen Sie die Sicherungsskripts in diesem Szenario entsprechend an.

Regelmäßige Datenbanksicherung mit SQL-Skript

Wählen Sie eines der folgenden SQL-Skripts aus:

a)Regelmäßige Sicherungen und Speicherung anhand des Erstellungsdatums:

```
1.@ECHO OFF
2.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, CHE
CKSUM, STATS=10"
3.REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)Sicherung an eine einzige Datei anhängen:

```
1.@ECHO OFF
2. 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"
```

MS SQL-Wiederherstellung

Führen Sie die folgenden Anweisungen aus, um eine MS SQL-Datenbank aus einer Datei wiederherzustellen:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

MySQL-Sicherung

Führen Sie die folgenden Anweisungen aus, um eine Sicherungsdatei einer MySQL-Datenbank zu erstellen:

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

i In diesem Beispiel steht **HOST** für die IP-Adresse bzw. den Hostnamen des MySQL-Servers, **ROOTLOGIN** für das root-Konto des MySQL-Servers und **DBNAME** für den Namen der ESET PROTECT-Datenbank.

MySQL-Wiederherstellung

Führen Sie die folgenden Anweisungen aus, um eine MySQL-Datenbank aus einer Datei wiederherzustellen:

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

i Weitere Informationen zu Microsoft SQL Server-Sicherungen finden Sie auf der [Microsoft Technet-Webseite](#). Weitere Informationen zu MySQL Server-Sicherungen finden Sie in der [MySQL-Dokumentation](#).

Datenbankserver-Upgrade

Gehen Sie wie folgt vor, um eine vorhandene Microsoft SQL Server-Instanz auf eine neuere Version zu aktualisieren, die als Datenbank für den ESET PROTECT Server verwendet werden kann:

1. Beenden Sie alle laufenden ESMC/ESET PROTECT Serverdienste, die sich mit dem Datenbankserver verbinden, den Sie aktualisieren werden. Beenden Sie außerdem alle sonstigen Anwendungen, die sich mit Ihrer Microsoft SQL Server-Instanz verbinden.
2. [Sichern](#) Sie alle relevanten Datenbanken an einem sicheren Ort, bevor Sie fortfahren.
3. Führen Sie ein Datenbankserver-Upgrade durch:

SQL Server aktualisieren (Windows):

- Folgen Sie dem [Knowledgebase-Artikel, um die MS SQL Express-Datenbank auf die neueste Version zu aktualisieren](#).
- Alternativ können Sie den Anweisungen des Datenbankanbieters folgen: <https://msdn.microsoft.com/en-us/library/bb677622.aspx>.
- [MS SQL Server unter Linux](#) wird nicht unterstützt. Sie können jedoch [den ESET PROTECT Server unter Linux mit MS SQL Server unter Windows verbinden](#).

MySQL Server aktualisieren (Windows und Linux):

- [Upgrade von MySQL 5.6 auf Version 5.7](#)
- [Upgrade von MySQL 5.7 auf Version 8](#)

4. Starten Sie den ESET PROTECT Server-Dienst und überprüfen Sie in den Trace-Logs, ob die Datenbankverbindung korrekt hergestellt wird.

Upgrade einer ESMC/ESET PROTECT-Installation in einem Failover-Cluster unter Windows

Wenn Sie den ESMC/ESET PROTECT Server [in einer Failover-Cluster-Umgebung](#) unter Windows auf die neueste Version von ESET PROTECT aktualisieren möchten, gehen Sie wie folgt vor.

! Stellen Sie sicher, dass Sie ein [unterstütztes Betriebssystem](#) verwenden.

1. Halten Sie die ESET PROTECT/ESMC Server-Clusterrolle im Cluster-Manager an. Stellen Sie sicher, dass der Dienst (**ESET Security Management Center Server** oder **ESET PROTECT Server**) auf allen Clusterknoten beendet wurde.
2. Verbinden Sie das gemeinsam genutzte Clusterlaufwerk auf dem ersten Knoten und aktualisieren Sie die Serverkomponente manuell, indem Sie das neueste *.msi*-Installationsprogramm wie bei einer [Komponenteninstallation](#) ausführen.
3. Stellen Sie nach Abschluss der Installation (Upgrade) sicher, dass der **ESET PROTECT Server**-Dienst angehalten ist.
4. Verbinden Sie das gemeinsam genutzte Clusterlaufwerk auf dem zweiten Knoten und aktualisieren Sie die Serverkomponente auf dieselbe Weise wie in Schritt 2.
5. Aktualisieren Sie den ESET PROTECT Server auf allen Clusterknoten und starten Sie anschließend die **ESET PROTECT Server-Clusterrolle** im Cluster-Manager.
6. Aktualisieren Sie den ESET Management Agenten manuell, indem Sie das neueste *.msi*-Installationsprogramm auf allen Clusterknoten ausführen.
7. Überprüfen Sie in der ESET PROTECT-Web-Konsole, ob Agenten und Server auf allen Knoten auf die gewünschte Version aktualisiert wurden.

Apache HTTP-Proxy aktualisieren

[Apache HTTP Proxy](#) ist ein Dienst, der zusammen mit ESET PROTECT verwendet werden kann, um Updates an Clientcomputer und Installationspakete an die ESET Management Agenten zu verteilen.

Falls Sie Apache HTTP Proxy bereits unter Windows installiert haben und ein Upgrade auf die neueste Version durchführen möchten, können Sie dies entweder [manuell](#) oder mit dem [All-in-One-Installationsprogramm](#) tun.

Apache HTTP-Proxy mit dem All-in-One-Installationsprogramm aktualisieren (Windows)

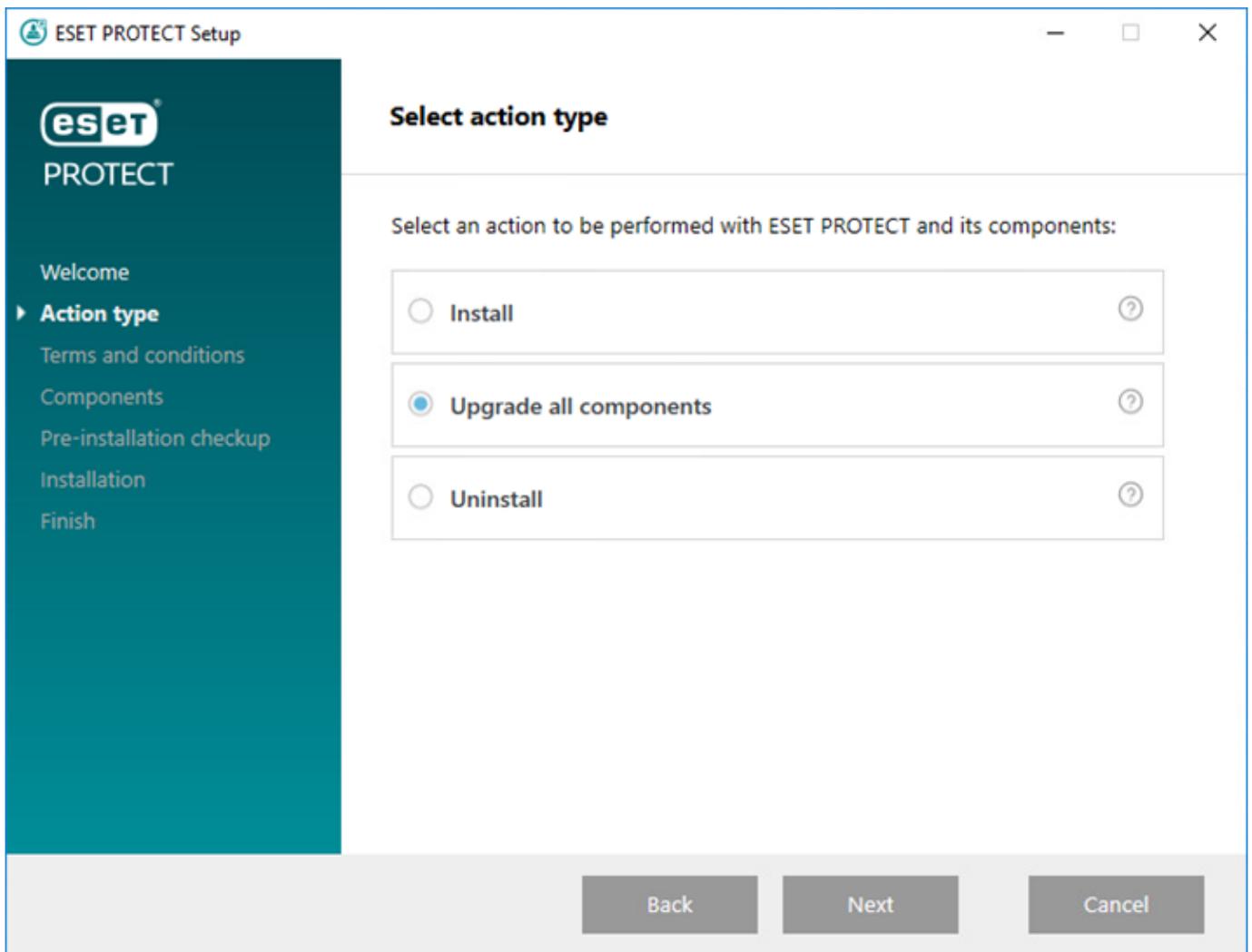
Falls Sie das neueste [ESET PROTECT All-in-One-Installationsprogramm](#) heruntergeladen haben, können Sie Apache HTTP Proxy mit dieser Methode schnell auf die neueste Version aktualisieren. Verwenden Sie die [manuelle Upgrademethode für den Apache HTTP Proxy](#), falls Sie nicht das neueste Installationsprogramm heruntergeladen haben.

1. Sichern Sie die folgenden Dateien:

- *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*
- *C:\Programme\Apache HTTP Proxy\bin\password.file*
- *C:\Programme\Apache HTTP Proxy\bin\group.file*

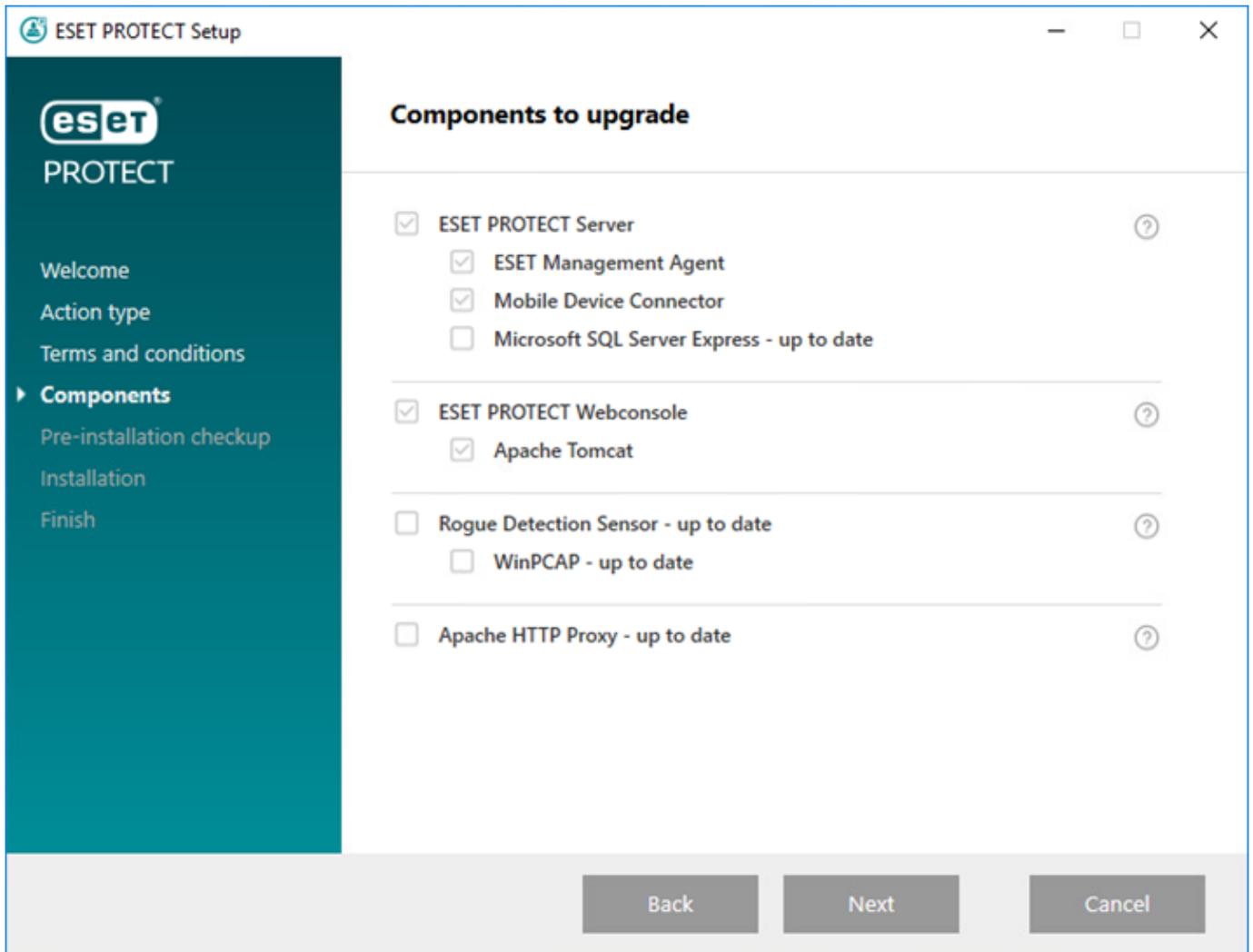
2. Starten Sie das All-in-One-Installationsprogramm, indem Sie auf die Datei *setup.exe* doppelklicken. Klicken Sie im Willkommensbildschirm auf **Weiter**.

3. Wählen Sie **Upgrade für alle Komponenten** aus und klicken Sie auf **Weiter**.



4. Lesen Sie die **Endbenutzer-Lizenzvereinbarung**, akzeptieren Sie sie und klicken Sie auf **Weiter**.

5. Überprüfen Sie unter **Komponenten**, für welche ESET PROTECT-Komponenten Upgrades verfügbar sind, und klicken Sie auf **Weiter**.



6. Führen Sie die **Prüfungen vor der Installation** durch, um sich zu vergewissern, dass Ihr System alle Voraussetzungen erfüllt.

7. Klicken Sie auf **Upgrade**, um das Upgrade von ESET PROTECT zu starten. Je nach System und Netzwerkkonfiguration kann das Upgrade einige Zeit dauern.

8. Klicken Sie nach Abschluss des Upgrades auf **Fertig stellen**.



Das All-in-One-Installationsprogramm überschreibt die Datei *httpd.conf* und speichert die ursprüngliche Konfiguration als *httpd.conf.old*. [Sichern Sie die Konfiguration und verwenden Sie sie erneut](#), um Ihre benutzerdefinierte Apache HTTP Proxy-Konfiguration zu behalten.

9. Testen Sie die Verbindung zum Apache HTTP Proxy, indem Sie die folgende URL in Ihrem Browser öffnen:

http://[IP address]:3128/index.html

Fehlerbehebung

Falls Probleme auftreten, überprüfen Sie die [Apache HTTP Proxy-Logdateien](#).

Falls Sie in der vorherigen Installation von Apache HTTP Proxy Änderungen an der Datei *httpd.conf* vorgenommen haben, führen Sie die folgenden Schritte aus:

1. Halten Sie den **ApacheHttpProxy**-Dienst an, indem Sie eine [Eingabeaufforderung als Administrator](#) öffnen

und den folgenden Befehl ausführen:

```
sc stop ApacheHttpProxy
```

2. Falls Sie Benutzernamen und Passwort für den Zugriff auf Ihren Apache HTTP Proxy verwenden (Thema [Apache HTTP Proxy-Installation](#)), ersetzen Sie den folgenden Codeblock:

```
<Proxy *>
  Deny from all
</Proxy>
```

durch den folgenden Codeblock (aus der Sicherung von *httpd.conf*):

```
<Proxy *>
  AuthType Basic
  AuthName "Password Required"
  AuthUserFile password.file
  AuthGroupFile group.file
  Require group usergroup
  Order deny,allow
  Deny from all
  Allow from all
</Proxy>
```

3. Wenn Sie in Ihrer vorherigen Installation von Apache HTTP Proxy weitere Anpassungen an der Datei *httpd.conf* vorgenommen haben, können Sie diese Änderungen manuell aus *httpd.conf.old* (oder aus der Sicherung von *httpd.conf* aus Schritt 1) in die neue (aktualisierte) Datei *httpd.conf* kopieren.

4. Speichern Sie Ihre Änderungen und starten Sie den **ApacheHttpProxy**-Dienst, indem Sie den folgenden Befehl in einer [Eingabeaufforderung mit erhöhten Rechten](#) ausführen:

```
sc start ApacheHttpProxy
```

Apache HTTP Proxy manuell aktualisieren (Windows)

Führen Sie die folgenden Schritte aus, um Apache HTTP Proxy auf die aktuelle Version zu aktualisieren.

1. Sichern Sie die folgenden Dateien:

- *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*
- *C:\Programme\Apache HTTP Proxy\bin\password.file*
- *C:\Programme\Apache HTTP Proxy\bin\group.file*

2. Halten Sie den **ApacheHttpProxy**-Dienst an, indem Sie eine [Eingabeaufforderung als Administrator](#) öffnen und den folgenden Befehl ausführen:

```
sc stop ApacheHttpProxy
```

3. Laden Sie die Apache HTTP Proxy-Installationsdatei von der ESET-[Downloadseite](#) herunter und extrahieren Sie den Inhalt nach *C:\Programme\Apache HTTP Proxy*. Überschreiben Sie die vorhandenen Dateien beim Extrahieren.

4. Navigieren Sie zu `C:\Programme\Apache HTTP Proxy\conf`, klicken Sie mit der rechten Maustaste auf `httpd.conf` und wählen Sie im Kontextmenü **Öffnen mit > Notepad** aus.

5. Fügen Sie den folgenden Code am Ende der Datei `httpd.conf`:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
  Options Indexes FollowSymLinks
  AllowOverride None
  Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

6. Falls Sie Benutzername und Passwort für den Zugriff auf Ihren Apache HTTP Proxy eingerichtet haben (Thema [Apache HTTP Proxy-Installation](#)), ersetzen Sie den folgenden Codeblock:

```
<Proxy *>
  Deny from all
</Proxy>
```

durch diesen Code (aus der Sicherung der Datei `httpd.conf`, die Sie in Schritt 1 angelegt haben):

```
<Proxy *>
  AuthType Basic
  AuthName "Password Required"
  AuthUserFile password.file
  AuthGroupFile group.file
  Require group usergroup
  Order deny,allow
  Deny from all
  Allow from all
</Proxy>
```

 Falls Sie in der vorherigen Installation von Apache HTTP Proxy weitere Anpassungen an der Datei `httpd.conf` vorgenommen wurden, kopieren Sie die Konfigurationsänderungen aus der Sicherung der Datei `httpd.conf` in die neue (aktualisierte) Datei `httpd.conf`.

7. Speichern Sie Ihre Änderungen und starten Sie den **ApacheHttpProxy**-Dienst, indem Sie den folgenden Befehl in einer [Eingabeaufforderung mit Administratorrechten](#) ausführen:

```
sc start ApacheHttpProxy
```

8. Aktualisieren Sie die Version in der Dienstbeschreibung.

```
sc description ApacheHttpProxy "Apache/2.4.43"
```

9. Testen Sie die Verbindung zum Apache HTTP Proxy, indem Sie die folgende URL in Ihrem Browser öffnen:

```
http://[IP address]:3128/index.html
```

Beachten Sie die [Apache HTTP Proxy-Logdateien](#), falls ein Problem auftritt.

Apache Tomcat aktualisieren

Apache Tomcat wird für die Ausführung der ESET PROTECT-Web-Konsole benötigt.

Falls Sie ein Upgrade auf die aktuelle Version von ESET PROTECT durchführen oder Apache Tomcat seit längerer Zeit nicht aktualisiert haben, sollten Sie ein Upgrade von Apache Tomcat auf die aktuelle Version in Betracht ziehen. Sie können die Sicherheit Ihrer Umgebung verbessern, indem Sie öffentlich erreichbare Dienste wie Apache Tomcat und dessen Abhängigkeiten fortlaufend aktualisieren.

Gehen Sie wie folgt vor, um Apache Tomcat zu aktualisieren:

- [Windows-Anleitung \(neuestes ESET PROTECT All-in-One-Installationsprogramm\)](#) – Wir empfehlen diese Upgradeoption, falls die vorhandene Apache Tomcat-Installation mit dem All-in-One-Installationsprogramm durchgeführt wurde.
- [Windows-Anleitung \(manuell Installation\)](#) – Aktualisieren Sie Apache Tomcat manuell, falls Sie die vorhandene Apache Tomcat-Installation manuell ausgeführt haben oder nicht über das neueste ESET PROTECT-All-in-One-Installationsprogramm verfügen.
- [Linux-Anleitung](#)

Apache Tomcat mit dem All-in-One-Installationsprogramm aktualisieren (Windows)

Apache Tomcat wird für die Ausführung der ESET PROTECT-Web-Konsole benötigt. Verwenden Sie diese Methode, um Apache Tomcat mit dem neuesten [ESET PROTECT 9.1 All-in-One-Installationsprogramm](#) zu aktualisieren. Wir empfehlen diese Upgradeoption, falls die vorhandene Apache Tomcat-Installation mit dem All-in-One-Installationsprogramm durchgeführt wurde. Alternativ können Sie [Apache Tomcat manuell aktualisieren](#).

Vor dem Upgrade

Sichern Sie die folgenden Dateien:

```
C:\Program Files\Apache Software Foundation\[ Tomcat ordner ]\.keystore  
C:\Program Files\Apache Software Foundation\[ Tomcat ordner ]\conf\server.xml  
C:\Program Files\Apache Software Foundation\[ Tomcat ordner ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties
```

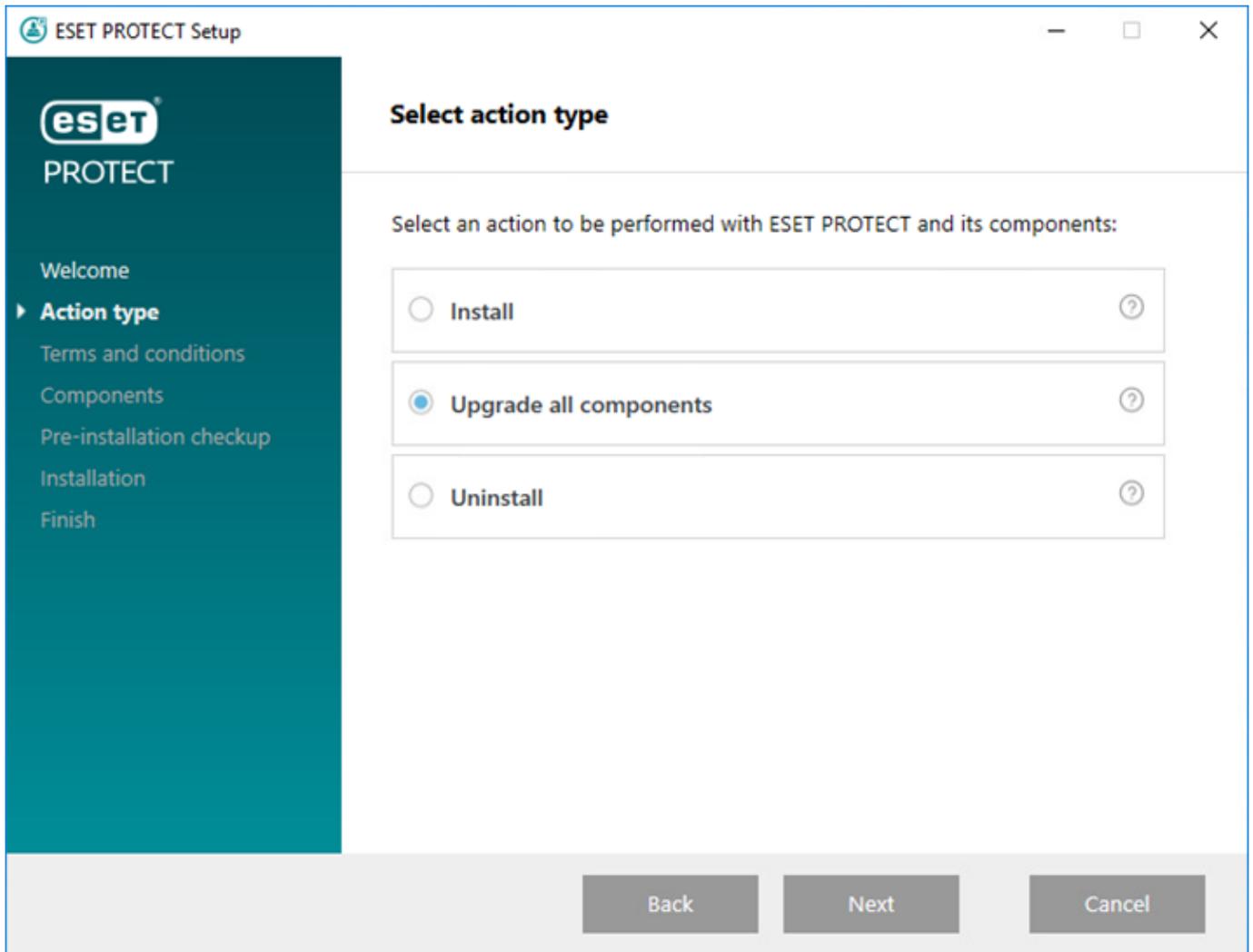
Falls Sie einen benutzerdefinierten SSL-Zertifikatspeicher im *Tomcat*-Ordner verwenden, sichern Sie das Zertifikat ebenfalls.

Einschränkungen für Upgrades von Apache Tomcat und der Web-Konsole

- Wenn eine benutzerdefinierte Version von Apache Tomcat installiert ist (manuelle Installation des Tomcat-Diensts), kann die ESET PROTECT-Web-Konsole anschließend nicht mit dem All-in-One-Installationsprogramm oder mit dem Task Komponenten-Upgrade aktualisiert werden.
- Das Apache Tomcat-Upgrade löscht den Ordner *era* in *C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps*. Wenn Sie zusätzliche Daten im Ordner *era* gespeichert haben, müssen Sie diese Daten vor dem Upgrade sichern.
- Wenn Sie den *C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps* enthält zusätzliche Daten (abgesehen von den Ordnern *era* und *ROOT*), das Apache Tomcat-Upgrade wird nicht ausgeführt und nur die Web-Konsole wird aktualisiert.
- Bei den Upgrades für die Web-Konsole und für Apache Tomcat wird die [Offlinehilfe](#) gelöscht. Falls Sie die Offlinehilfe mit ESMC oder einer älteren Version von ESET PROTECT verwendet haben, können Sie sie nach dem Upgrade für ESET PROTECT 9.1 erneut erstellen, um sicherzustellen, dass Sie die neueste Offline-Hilfe für Ihre Version von ESET PROTECT verwenden.

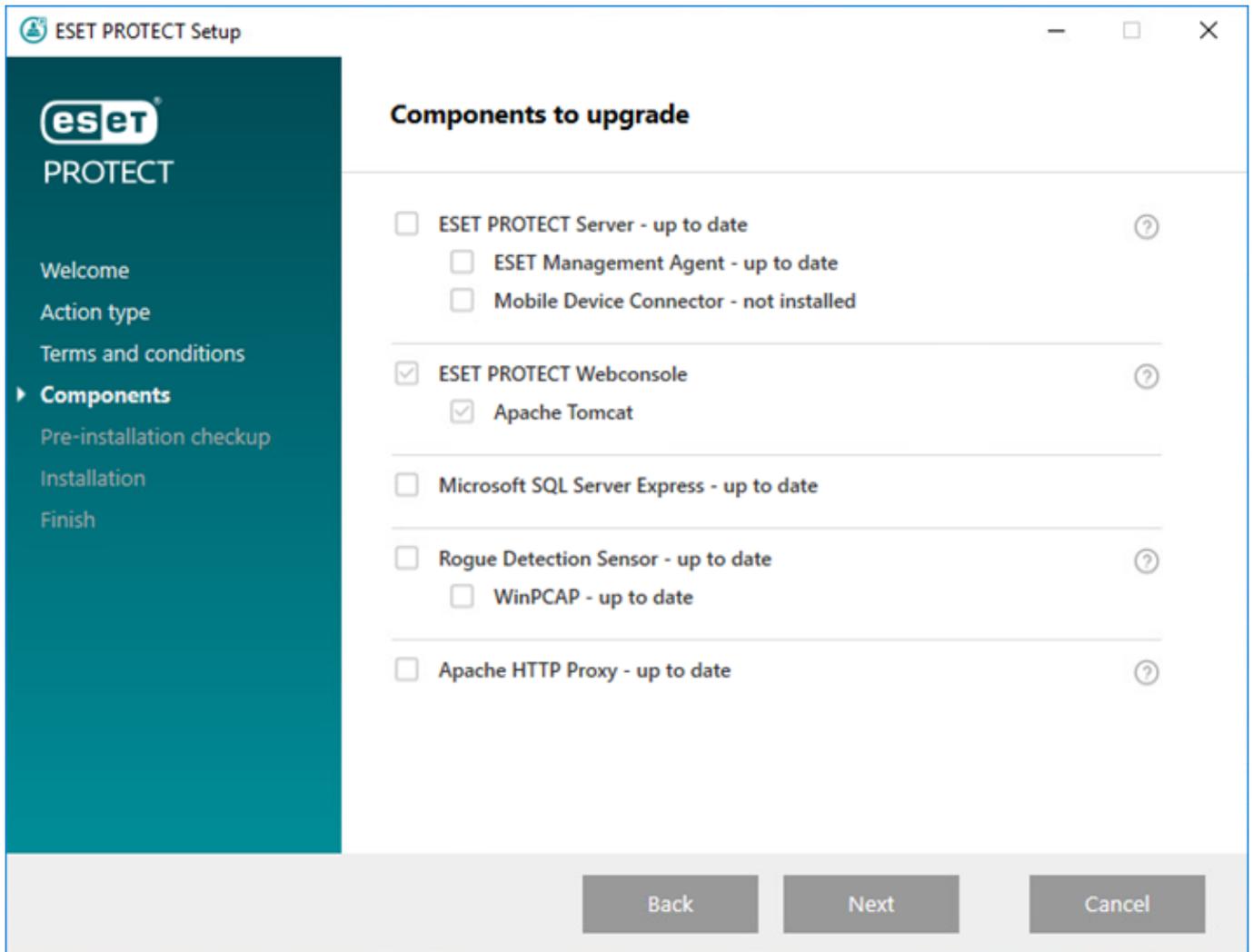
Upgradeprozeduren

1. Laden Sie das [All-in-One-Installationsprogramm für ESET PROTECT](#) von der ESET-Website herunter und entpacken Sie die heruntergeladene Datei.
2. Falls Sie die neueste Version von Apache Tomcat installieren möchten und das All-in-One-Installationsprogramm eine ältere Version von Apache Tomcat enthält (Dieser Schritt ist optional. Überspringen Sie Schritt 4, falls Sie nicht die neueste Version von Apache Tomcat benötigen):
 - a. Öffnen Sie den Ordner *x64* und navigieren Sie zum Ordner *installers*.
 - b. Entfernen Sie die Datei *apache-tomcat-9.0.x-windows-x64.zip* im Ordner *installers*.
 - c. Laden Sie das Paket Apache Tomcat 9 [64-bit Windows Zip](#) herunter.
 - d. Verschieben Sie das heruntergeladene Zip-Paket in den Ordner *installers*.
3. Um das All-in-One-Installationsprogramm zu starten, doppelklicken Sie auf die Daten *Setup.exe* und klicken Sie auf **Weiter** im **Willkommensbildschirm**.
5. Wählen Sie **Upgrade für alle Komponenten** aus und klicken Sie auf **Weiter**.



6. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.

7. Das All-in-One-Installationsprogramm erkennt automatisch, ob das Upgrade verfügbar ist: neben den entsprechenden ESET PROTECT-Komponenten wird ein Kontrollkästchen angezeigt. Klicken Sie auf **Weiter**.



8. Wählen Sie eine Java-Installation auf dem Computer aus. Apache Tomcat benötigt Java/OpenJDK (64-Bit). Falls Sie mehrere Java-Versionen auf Ihrem System installiert haben, empfehlen wir, die älteren Java-Versionen zu deinstallieren und nur die neueste [unterstützte Java](#)-Version zu behalten.

 Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).

9. Klicken Sie auf **Upgrade**, um das Upgrade abzuschließen, und dann auf **Fertig stellen**.

10. Falls Sie die Web-Konsole auf einem anderen Computer installiert haben als den ESET PROTECT Server:

a. Halten Sie den Apache Tomcat-Dienst an. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Beenden** aus.

b. Stellen Sie die Datei *EraWebServerConfig.properties* (aus Schritt 1) an ihrem ursprünglichen Speicherort wieder her.

c. Neu starten Sie den Apache Tomcat-Dienst neu. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Starten** aus.

11. [Verbinden Sie sich mit der ESET PROTECT-Web-Konsole](#) und überprüfen Sie, ob die Web-Konsole korrekt geladen wird.

 Siehe auch die zusätzliche [Konfiguration der Web-Konsole für Enterprise-Lösungen oder leistungsschwache Systeme](#).

Fehlerbehebung

Falls das Upgrade für Apache Tomcat fehlschlägt, installieren Sie Ihre vorherige Version und übernehmen Sie die Konfiguration aus Schritt 1.

Apache Tomcat manuell aktualisieren (Windows)

Apache Tomcat wird für die Ausführung der ESET PROTECT-Web-Konsole benötigt. Aktualisieren Sie Apache Tomcat manuell, falls Sie die vorhandene Apache Tomcat-Installation manuell ausgeführt haben oder nicht über das neueste ESET PROTECT-All-in-One-Installationsprogramm verfügen.



Wenn eine benutzerdefinierte Version von Apache Tomcat installiert ist (manuelle Installation des Tomcat-Diensts), kann die ESET PROTECT-Web-Konsole anschließend nicht mit dem All-in-One-Installationsprogramm oder mit dem Task Komponenten-Upgrade aktualisiert werden.

Vor dem Upgrade

- Apache Tomcat benötigt Java/OpenJDK (64-Bit). Falls Sie mehrere Java-Versionen auf Ihrem System installiert haben, empfehlen wir, die älteren Java-Versionen zu deinstallieren und nur die neueste [unterstützte Java](#)-Version zu behalten.



Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).

- Überprüfen Sie, welche Version von Apache Tomcat aktuell verfügbar ist.
 - a. Navigieren Sie zum Apache Tomcat-Installationsordner:
`C:\Program Files\Apache Software Foundation\[Tomcat ordner]\`
 - b. Öffnen Sie die Datei RELEASE-NOTES in einem Texteditor und überprüfen Sie die Versionsnummer (zum Beispiel 9.0.34).
 - c. Führen Sie ein Upgrade durch, falls eine neuere [unterstützte Version](#) verfügbar ist.

Upgradeprozeduren

1. Halten Sie den Apache Tomcat-Dienst an. Navigieren Sie zu **Start > Dienste** > klicken Sie mit der rechten Maustaste auf den Apache Tomcat-Dienst und wählen Sie **Beenden** aus.

Schließen Sie *Tomcat7w.exe*, falls die Anwendung in Ihrer Taskleiste ausgeführt wird.

2. Sichern Sie die folgenden Dateien:

```
C:\Program Files\Apache Software Foundation\[ Tomcat ordner ]\.keystore  
C:\Program Files\Apache Software Foundation\[ Tomcat ordner ]\conf\server.xml
```

C:\Program Files\Apache Software Foundation\[Tomcat ordner]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Falls Sie einen benutzerdefinierten SSL-Zertifikatspeicher im *Tomcat*-Ordner verwenden, sichern Sie das Zertifikat ebenfalls.

3. Deinstallieren Sie die aktuell installierte Version von Apache Tomcat.

4. Löschen Sie den folgenden Ordner, falls dieser immer noch auf Ihrem System vorhanden ist:

C:\Program Files\Apache Software Foundation\[Tomcat ordner]

5. Laden Sie die aktuelle Version der Apache Tomcat-Installationsdatei (32-Bit- bzw. 64-Bit-Windows Service-Installationsprogramm) *apache-tomcat-[Version].exe* von <https://tomcat.apache.org> herunter.

6. Installieren Sie die neuere Version von Apache Tomcat, die Sie heruntergeladen haben:

- Falls Sie mehrere Java-Versionen installiert haben, wählen Sie bei der Installation den Pfad zur neuesten Java-Version aus.
- Deaktivieren Sie nach Abschluss der Installation das Kontrollkästchen neben **Apache Tomcat ausführen**.

7. Stellen Sie die Dateien *.keystore* und *server.xml* sowie Ihre benutzerdefinierten Zertifikate an ihren ursprünglichen Speicherorten wieder her.

8. Öffnen Sie die Datei *server.xml* und überprüfen Sie den Pfad unter *keystoreFile* (aktualisieren Sie den Pfad, falls Sie ein Upgrade auf eine höhere Hauptversion von Apache Tomcat durchgeführt haben):

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat ordner]\.keystore"

9. Vergewissern Sie sich, dass die [HTTPS-Verbindung für Apache Tomcat](#) für die ESET PROTECT-Web-Konsole korrekt konfiguriert ist.

10. Stellen Sie die ESET PROTECT-Web-Konsole bereit, siehe [Installation der Web-Konsole - Windows](#).

11. Stellen Sie die Datei *EraWebServerConfig.properties* an ihrem ursprünglichen Speicherort wieder her.

12. Starten Sie Apache Tomcat und wählen Sie eine korrekte Java VM aus:

a. Navigieren Sie zum Ordner *C:\Program Files\Apache Software Foundation\[Tomcat ordner]\bin* und führen Sie *Tomcat9w.exe* aus.

b. Legen Sie auf der Registerkarte **Allgemein** den **Starttyp** auf **Automatisch** fest und drücken Sie auf **Starten**.

c. Klicken Sie auf die Registerkarte **Java**, deaktivieren Sie die Option **Standard verwenden**, vergewissern Sie sich, dass unter **Java Virtual Machine** der Pfad zur Datei *jvm.dll* angegeben ist ([illustrierte Knowledgebase-Anleitung](#)), und klicken Sie auf **OK**.

13. [Verbinden Sie sich mit der ESET PROTECT-Web-Konsole](#) und überprüfen Sie, ob die Web-Konsole korrekt geladen wird.

Fehlerbehebung

- Falls Sie Probleme bei der Einrichtung einer HTTPS-Verbindung für Apache Tomcat haben, können Sie diesen Schritt überspringen und vorübergehend eine HTTP-Verbindung verwenden.
- Falls das Upgrade für Apache Tomcat fehlschlägt, installieren Sie Ihre ursprüngliche Version und übernehmen Sie die Konfiguration aus Schritt 2.
- Bei den Upgrades für die Web-Konsole und für Apache Tomcat wird die [Offlinehilfe](#) gelöscht. Falls Sie die Offlinehilfe mit ESMC oder einer älteren Version von ESET PROTECT verwendet haben, können Sie sie nach dem Upgrade für ESET PROTECT 9.1 erneut erstellen, um sicherzustellen, dass Sie die neueste Offline-Hilfe für Ihre Version von ESET PROTECT verwenden.

Apache Tomcat aktualisieren (Linux)

Apache Tomcat wird für die Ausführung der ESET PROTECT-Web-Konsole benötigt.

Vor dem Upgrade

1. Führen Sie den folgenden Befehl aus, um die installierte Version von Apache Tomcat anzuzeigen (in manchen Fällen lautet der Ordnername `tomcat7` oder `tomcat8`):

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. Falls eine neuere Version verfügbar ist:
 - a. Vergewissern Sie sich, dass die neuere Version [unterstützt](#) wird.
 - b. Sichern Sie die Tomcat-Konfigurationsdatei (`/etc/tomcat7/server.xml`).

Upgradeprozeduren

1. Führen Sie den folgenden Befehl aus, um den Apache Tomcat-Dienst zu beenden (in manchen Fällen lautet der Dienstname `tomcat7`):

```
sudo systemctl stop tomcat
```

2. Aktualisieren Sie Apache Tomcat und Java. Die genauen Namen der folgenden Pakete hängen vom verwendeten Repository für Ihre Linux-Distribution ab.

Linux-Distribution	Terminalbefehle
Debian und Ubuntu-Distributionen	<pre>sudo apt-get update sudo apt-get install openjdk-17-jdk tomcat9</pre>

Linux-Distribution	Terminalbefehle
CentOS und Red Hat-Distributionen	yum update yum install java-17-openjdk tomcat
OpenSUSE	zypper refresh sudo zypper install java-17-openjdk tomcat9

3. Ersetzen Sie die Datei `/etc/tomcat9/server.xml` durch die Datei `server.xml` aus Ihrer Sicherung.
4. Öffnen Sie die Datei `server.xml` und überprüfen Sie den Pfad unter `keystoreFile`.
5. Stellen Sie sicher, dass die [HTTPS-Verbindung für Apache Tomcat](#) korrekt konfiguriert ist.

Siehe auch die zusätzliche [Konfiguration der Web-Konsole für Enterprise-Lösungen oder leistungsschwache Systeme](#).

Nach der Aktualisierung von Apache Tomcat auf eine spätere Hauptversion (z. B. Apache Tomcat Version 7.x auf 9.x):

1. Stellen Sie die ESET PROTECT-Web-Konsole erneut bereit (siehe [Installation der ESET PROTECT-Web-Konsole - Linux](#)).
2. Behalten Sie die Datei `%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties` bei, um Ihre benutzerdefinierten Einstellungen in der ESET PROTECT-Web-Konsole zu erhalten.

Bei den Upgrades für die Web-Konsole und für Apache Tomcat wird die [Offlinehilfe](#) gelöscht. Falls Sie die Offlinehilfe mit ESMC oder einer älteren Version von ESET PROTECT verwendet haben, können Sie sie nach dem Upgrade für ESET PROTECT 9.1 erneut erstellen, um sicherzustellen, dass Sie die neueste Offline-Hilfe für Ihre Version von ESET PROTECT verwenden.

Prozeduren für Migration und erneute Installation

Upgrade, Migration und erneute Installation von ESET PROTECT Server und anderen ESET PROTECT-Komponenten können auf verschiedene Arten ausgeführt werden:

- [Migration](#) oder erneute Installation von ESET PROTECT 9 von einem Server auf einen anderen Server.

Falls Sie Ihren ESET PROTECT Server auf einen neuen Computer migrieren möchten, müssen Sie sämtliche Zertifizierungsstellen und das ESET PROTECT-Serverzertifikat exportieren oder sichern. Andernfalls kann keine der ESET PROTECT-Komponenten mit Ihrem neuen ESET PROTECT Server kommunizieren.

- [migration der ESET PROTECT-Datenbank](#)
- [Migration von MDM](#)
- [Ändern der IP-Adresse oder des Hostnamens](#) auf einem ESET PROTECT Server
- [Migration von ERA 5.x](#)

Siehe [Upgradeprozeduren](#).

Migration von Server zu Server

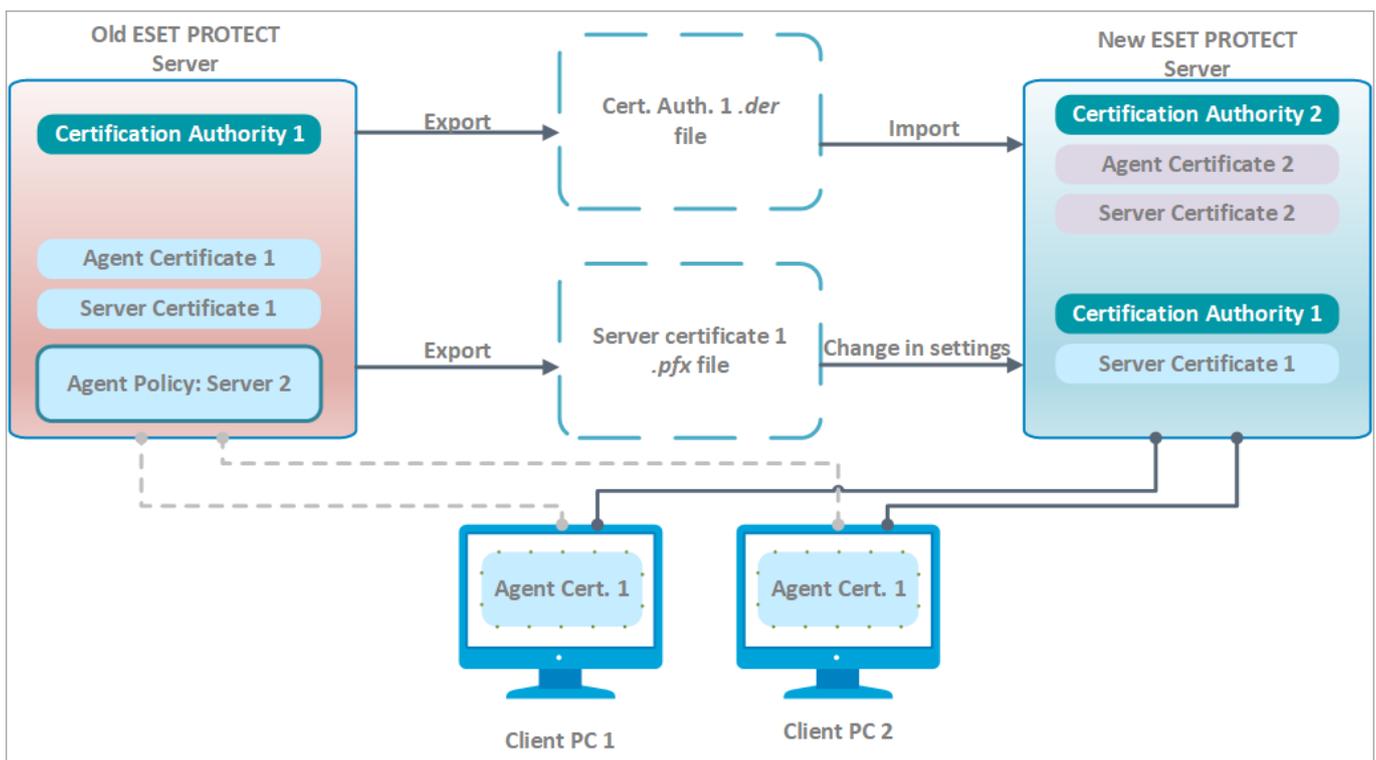
Sie können ESET PROTECT auf verschiedene Arten von einem Server auf einen anderen Server migrieren (diese Szenarien können auch für die erneute Installation des ESET PROTECT Servers eingesetzt werden):

- [Erstinstallation - gleiche IP-Adresse](#) – Die neue Installation verwendet nicht die vorherige Datenbank aus dem alten ESET PROTECT Server und behält die ursprüngliche IP-Adresse bei.
- [Erstinstallation - neue IP-Adressen](#) (Knowledgebase-Artikel) – Die neue Installation verwendet nicht die vorherige Datenbank aus dem alten ESET PROTECT Server und erhält eine neue IP-Adresse.
- [Migrierte Datenbank – gleiche/andere IP-Adresse](#) – Die Datenbankmigration kann nur zwischen zwei gleichen Datenbanktypen (von MySQL zu MySQL oder von MS SQL zu MS SQL) und ähnlichen Versionen von ESET PROTECT durchgeführt werden.

Erstinstallation - gleiche IP-Adresse

Mit dem hier beschriebenen Verfahren können Sie eine völlig neue ESET PROTECT Server-Instanz installieren, die eine neue Datenbank verwendet. Dieser neue ESET PROTECT Server erhält **dieselbe IP-Adresse** wie Ihr alter Server, verwendet jedoch nicht die Datenbank aus dem alten ESET PROTECT Server.

- Die folgenden Anweisungen setzen voraus, dass Ihr alter ESET PROTECT Server ausgeführt wird und die Web-Konsole erreichbar ist. Falls Ihr alter ESET PROTECT Server nicht erreichbar ist:
1. Installieren Sie den ESET PROTECT Server/MDM mit dem [All-in-One-Installationsprogramm](#) (Windows) oder wählen Sie [eine andere Installationsart aus](#) (manuelle Windows-Installation, Linux oder virtuelle Appliance).
 2. [Verbinden](#) Sie sich mit der ESET PROTECT-Web-Konsole.
 3. [Fügen Sie Clientcomputer](#) zur ESET PROTECT-Infrastruktur hinzu und [stellen Sie den ESET Management Agenten lokal oder remote bereit](#).



Führen Sie auf Ihrem aktuellen (alten) ESET PROTECT Server die folgenden Aktionen aus:

Wenn Sie mit [ESET Full Disk Encryption](#) verschlüsselte Geräte verwalten, führen Sie diese Schritte aus, um den Verlust von [Wiederherstellungsdaten](#) zu vermeiden.

1. Vor der Migration: Navigieren Sie zu **Statusübersicht > Verschlüsselung**. Dort können Sie Ihre aktuellen **Wiederherstellungsdaten für ESET Full Disk Encryption exportieren**.

 2. Nach der Migration: **Importieren** Sie die **ESET Full Disk Encryption Wiederherstellungsdaten** in Ihrer neuen Management-Konsole.

Wenn Sie diese Schritte nicht ausführen können, müssen Sie die [verwalteten Geräte vor der Migration entschlüsseln](#). Nach der Migration können Sie die [verwalteten Geräte](#) in der ESET PROTECT-Web-Konsole verschlüsseln.

1. Exportieren Sie ein Serverzertifikat aus Ihrem aktuellen ESET PROTECT Server und speichern Sie es auf einem externen Speichermedium.

- Exportieren Sie alle [Zertifizierungsstellenzertifikate](#) aus Ihrem ESET PROTECT Server und speichern Sie die ZS-Zertifikate in je einer *.der*-Datei.
- Exportieren Sie ein [Serverzertifikat](#) aus Ihrem ESET PROTECT Server in eine *.pfx*-Datei. Die exportierte *.pfx*-Datei enthält außerdem einen privaten Schlüssel.

2. Halten Sie den ESET PROTECT Server-Dienst an.

3. Fahren Sie den aktuellen ESET PROTECT Server-Computer herunter.

 Sie sollten Ihren alten ESET PROTECT Server noch nicht deinstallieren oder stilllegen.

Führen Sie auf Ihrem neuen ESET PROTECT Server die folgenden Aktionen aus:

 Um einen neuen ESET PROTECT Server mit derselben IP-Adresse zu verwenden, stellen Sie sicher, dass die Netzwerkkonfiguration auf Ihrem neuen ESET PROTECT Server (**IP-Adresse, FQDN, Computername, DNS SRV-Eintrag**) mit der Konfiguration Ihres alten ESET PROTECT Servers übereinstimmt.

1. Installieren Sie den ESET PROTECT Server/MDM mit dem [All-in-One-Installationsprogramm](#) (Windows) oder wählen Sie [eine andere Installationsart aus](#) (manuelle Windows-Installation, Linux oder virtuelle Appliance).

2. [Verbinden](#) Sie sich mit der ESET PROTECT-Web-Konsole.

3. Importieren Sie alle ZS, die Sie aus Ihrem alten ESET PROTECT Server exportiert haben. Führen Sie dazu die Anweisungen im Artikel [Öffentlichen Schlüssel importieren](#) aus.

4. Ändern Sie das ESET PROTECT Server-Zertifikat in Ihren **Mehr > Einstellungen** und verwenden Sie das Serverzertifikat aus Ihrem alten ESET PROTECT Server.

5. [Importieren Sie alle benötigten ESET-Lizenzen](#) nach ESET PROTECT.

6. Starten Sie den ESET PROTECT Server-Dienst neu. Weitere Informationen finden Sie in unseren [Knowledgebase-Artikel](#).

Nach einem oder zwei [Agenten-Verbindungsintervallen](#) sollten sich die Clientcomputer mit Ihrem neuen ESET PROTECT Server verbinden und dabei das ursprüngliche ESET Management Agent-Zertifikat verwenden, das von

der importierten ZS aus dem alten ESET PROTECT Server authentifiziert wird. Falls sich die Clients nicht verbinden, lesen Sie den Abschnitt [Probleme nach Upgrade oder Migration von ESET PROTECT Server](#).

 Wenn Sie neue Clientcomputer hinzufügen, müssen Sie eine neue Zertifizierungsstelle zum Signieren der Agenten-Zertifikate verwenden. Dies liegt daran, dass eine importierte ZS nicht zum Signieren neuer Peerzertifikate verwendet werden kann. Eine solche ZS kann nur ESET Management Agenten von migrierten Clientcomputern authentifizieren.

Deinstallation des alten ESET PROTECT Servers/MDM:

Sobald Ihr neuer ESET PROTECT Server reibungslos funktioniert, können Sie Ihren alten ESET PROTECT Server/MDM mit unserer [Schritt-für-Schritt-Anleitung](#) sorgfältig deinstallieren.

Migrierte Datenbank - gleiche/andere IP-Adresse

Mit dem hier beschriebenen Verfahren können Sie eine völlig neue ESET PROTECT Server-Instanz installieren und **Ihre vorhandene ESET PROTECT-Datenbank weiterverwenden**, inklusive vorhandener Clientcomputer. Der neue ESET PROTECT Server hat **dieselbe oder eine andere IP-Adresse** und die Datenbank des alten ESET PROTECT Servers wird vor der Installation auf den neuen Server importiert.

- Die [Datenbankmigration](#) wird nur zwischen gleichen Datenbanktypen unterstützt (von MySQL zu MySQL oder von MSSQL zu MSSQL).
-  • Bei der Migration einer Datenbank müssen Sie zwischen Instanzen derselben ESET PROTECT-Version migrieren. In unserem [Knowledgebase-Artikel](#) finden Sie Anweisungen zur Ermittlung der Versionen Ihrer ESET PROTECT-Komponenten. Nach Abschluss der Datenbankmigration können Sie bei Bedarf ein Upgrade auf die aktuelle Version von ESET PROTECT durchführen.

Führen Sie auf Ihrem aktuellen (alten) ESET PROTECT Server die folgenden Aktionen aus:

Die Migration auf eine andere IP-Adresse sollte nur von fortgeschrittenen Benutzern ausgeführt werden. Falls Ihr neuer ESET PROTECT Server eine **andere IP-Adresse** hat, führen Sie diese zusätzlichen Schritte auf Ihrem aktuellen (alten) ESET PROTECT Server aus:

-  a) Generieren Sie ein [neues ESET PROTECT Server-Zertifikat](#) (mit Verbindungsinformationen für den neuen ESET PROTECT Server). Lassen Sie den Standardwert (ein Sternchen) im Feld **Host** unverändert, wenn dieses Zertifikat ohne Zuordnung an bestimmte DNS-Namen oder IP-Adressen verteilt werden soll.
- b) Erstellen Sie eine Policy, um die [neue IP-Adresse des ESET PROTECT Servers](#) festzulegen, und wenden Sie die Policy auf allen Computern an. Warten Sie, bis die Policy auf alle Clientcomputer verteilt wurde (die Computer melden sich nicht mehr, nachdem sie die neuen Serverinformationen erhalten haben).

1. Halten Sie den ESET PROTECT Server-Dienst an.
2. [Exportieren/Sichern Sie die ESET PROTECT-Datenbank](#).
3. Deaktivieren Sie den aktuellen ESET PROTECT Servercomputer (optional, falls der neue Server eine andere IP-Adresse hat).

 Sie sollten Ihren alten ESET PROTECT Server noch nicht deinstallieren oder stilllegen.

Führen Sie auf Ihrem neuen ESET PROTECT Server die folgenden Aktionen aus:

! Um einen neuen ESET PROTECT Server mit derselben IP-Adresse zu verwenden, stellen sie sicher, dass die Netzwerkkonfiguration auf Ihrem neuen ESET PROTECT Server (**IP-Adresse, FQDN, Computername, DNS SRV-Eintrag**) mit der Konfiguration Ihres alten ESET PROTECT Servers übereinstimmt.

1. Installieren/Starten Sie eine von ESET PROTECT [unterstützte](#) Datenbank.
2. Importieren Sie die [ESET PROTECT-Datenbank](#) aus Ihrem alten ESET PROTECT Server bzw. stellen Sie sie wieder her.
3. Installieren Sie den ESET PROTECT Server/MDM mit dem [All-in-One-Installationsprogramm](#) (Windows) oder wählen Sie [eine andere Installationsart aus](#) (manuelle Windows-Installation, Linux oder virtuelle Appliance). Geben Sie die Einstellungen für Ihre Datenbankverbindung bei der Installation des ESET PROTECT Servers an.
4. [Verbinden](#) Sie sich mit der ESET PROTECT-Web-Konsole.
5. Navigieren Sie zu **Mehr > Einstellungen > Verbindung**. Klicken Sie auf **Zertifikat ändern > Zertifikatliste öffnen**, wählen Sie das **Serverzertifikat** des alten ESET PROTECT Servers aus und klicken Sie zweimal auf **OK**.
6. [Starten Sie den ESET PROTECT Server-Dienst neu](#).
7. [Melden Sie sich](#) bei der ESET PROTECT-Web-Konsole an und klicken Sie auf **Computer**.

Nach einem oder zwei [Agenten-Verbindungsintervallen](#) sollten sich die Clientcomputer mit Ihrem neuen ESET PROTECT Server verbinden und dabei das ursprüngliche ESET Management Agent-Zertifikat verwenden. Falls sich die Clients nicht verbinden, lesen Sie den Abschnitt [Probleme nach Upgrade oder Migration von ESET PROTECT Server](#).

Deinstallation des alten ESET PROTECT Servers/MDM:

Sobald Ihr neuer ESET PROTECT Server reibungslos funktioniert, können Sie Ihren alten ESET PROTECT Server/MDM mit unserer [Schritt-für-Schritt-Anleitung](#) sorgfältig deinstallieren.

migration der ESET PROTECT-Datenbank

Diese Anweisungen gelten für die Migration der ESET PROTECT-Datenbank zwischen unterschiedlichen SQL Server-Instanzen (bzw. für die Migration zwischen unterschiedlichen SQL Server-Versionen oder auf einen SQL Server auf einem anderen Computer):

- [Migrationsprozess für MS SQL Server](#)
- [Migrationsprozess für MySQL Server](#)

Migrationsprozess für MS SQL Server

Für **Microsoft SQL Server** und **Microsoft SQL Server Express** wird jeweils derselbe Migrationsprozess verwendet.

Weitere Informationen finden Sie im folgenden Artikel der Microsoft-Knowledgebase:
<https://msdn.microsoft.com/en-us/library/ms189624.aspx>.

Voraussetzungen

- SQL Server-Quell- und Zielinstanzen müssen installiert sein. Diese Instanzen können sich auf unterschiedlichen Computern befinden.
- Die SQL Server-Zielinstanz muss mindestens dieselbe Version wie die Quellinstanz haben. **Herabstufung wird nicht unterstützt!**
- **SQL Server Management Studio** muss installiert sein. Wenn sich die SQL Server-Instanzen auf unterschiedlichen Computern befinden, muss Management Studio auf beiden Computern vorhanden sein.

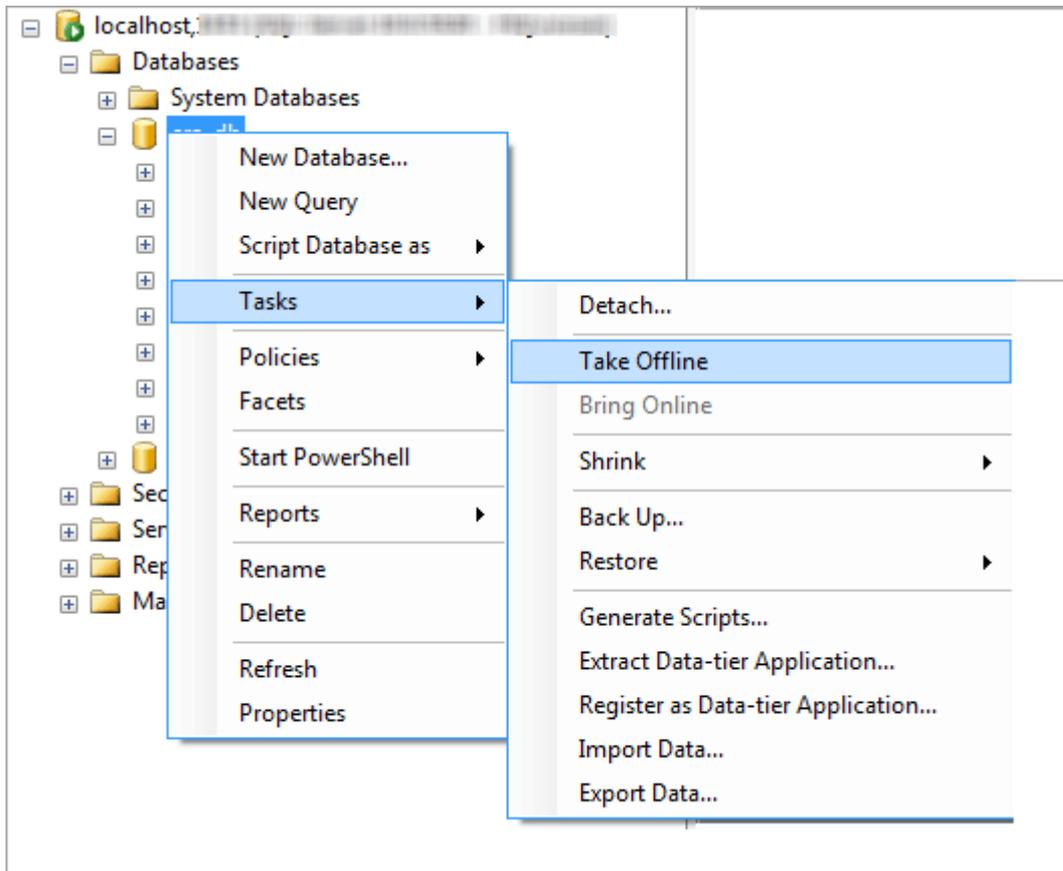
Migration mit SQL Server Management Studio

1. Beenden Sie den ESET PROTECT Server-Dienst (bzw. den ESMC Server-Dienst) oder den ESET PROTECT MDM-Dienst.



Starten Sie ESET PROTECT Server oder ESET PROTECT MDM nicht, bevor Sie alle unten genannten Schritte abgeschlossen haben.

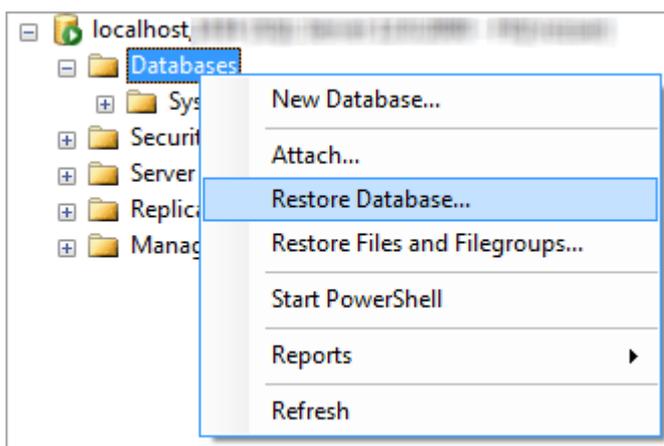
2. Melden Sie sich über SQL Server Management Studio bei der SQL Server-Quellinstanz an.
3. Erstellen Sie eine [vollständige Datenbanksicherung](#) der zu migrierenden Datenbank. Wir empfehlen die Angabe eines neuen Namens für den Sicherungssatz. Falls der Sicherungssatz bereits verwendet wurde, kann es ansonsten passieren, dass die neue Sicherung daran angehängt wird, was wiederum zu einer unnötig großen Sicherungsdatei führt.
4. Nehmen Sie die Quelldatenbank vom Netz. Wählen Sie dazu **Tasks > Offline nehmen** aus.



5. Kopieren Sie die in Schritt 3 erstellte Sicherungsdatei (.bak) an einen von der SQL Server-Zielinstanz aus erreichbaren Ort. Möglicherweise müssen Sie die Zugriffsrechte für die Datenbank-Sicherungsdatei bearbeiten.

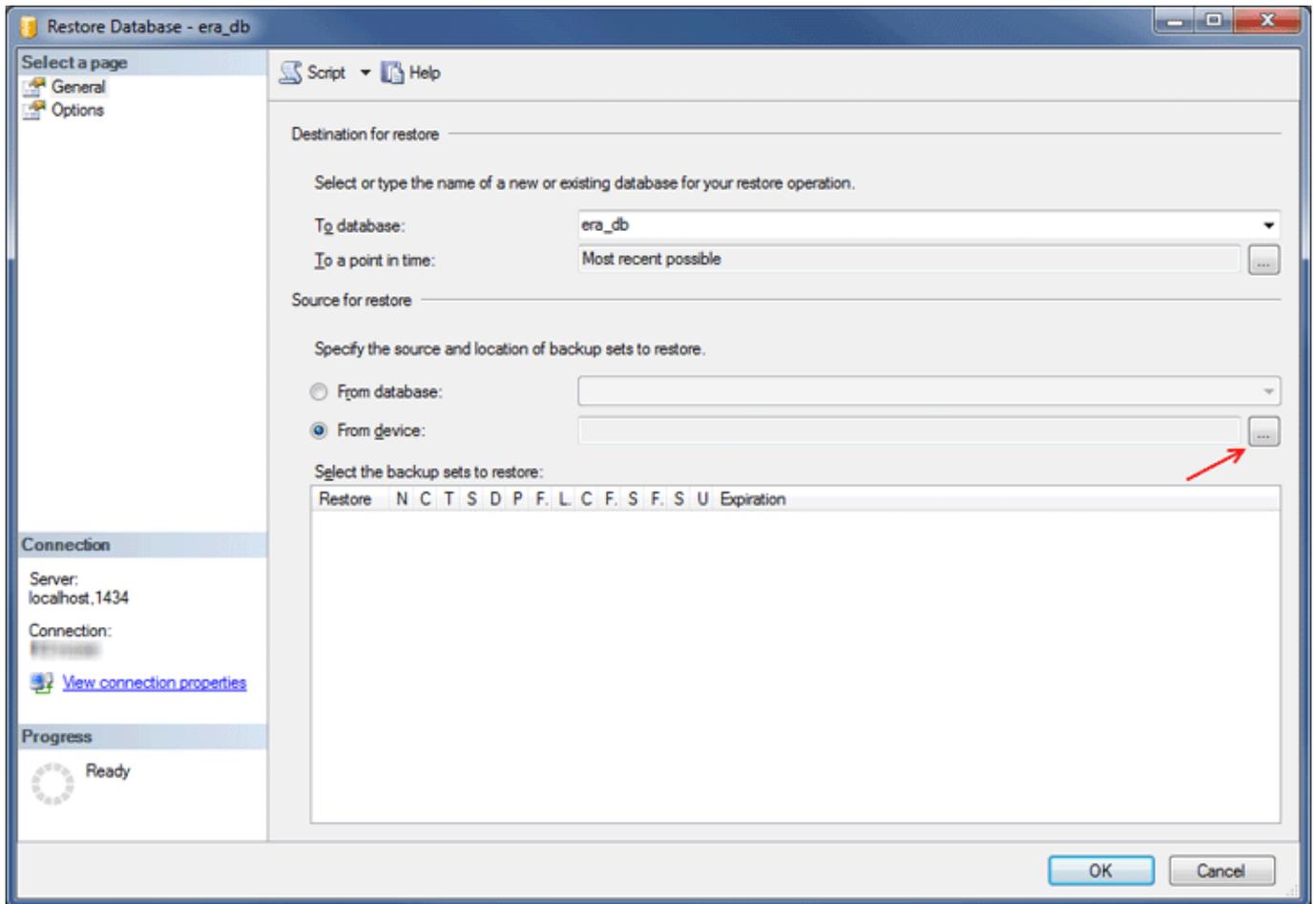
6. Melden Sie sich über SQL Server Management Studio bei der SQL Server-Zielinstanz an.

7. [Stellen Sie Ihre Datenbank](#) auf der SQL Server-Zielinstanz wieder her.



8. Geben Sie im Feld **Zieldatenbank** einen Namen für Ihre neue Datenbank ein. Sie können auch den Namen Ihrer alten Datenbank verwenden.

9. Wählen Sie „Von Gerät“ unter **Geben Sie die Quelle und den Speicherort der wiederherzustellenden Sicherungssätze an** aus und klicken Sie auf „...“.

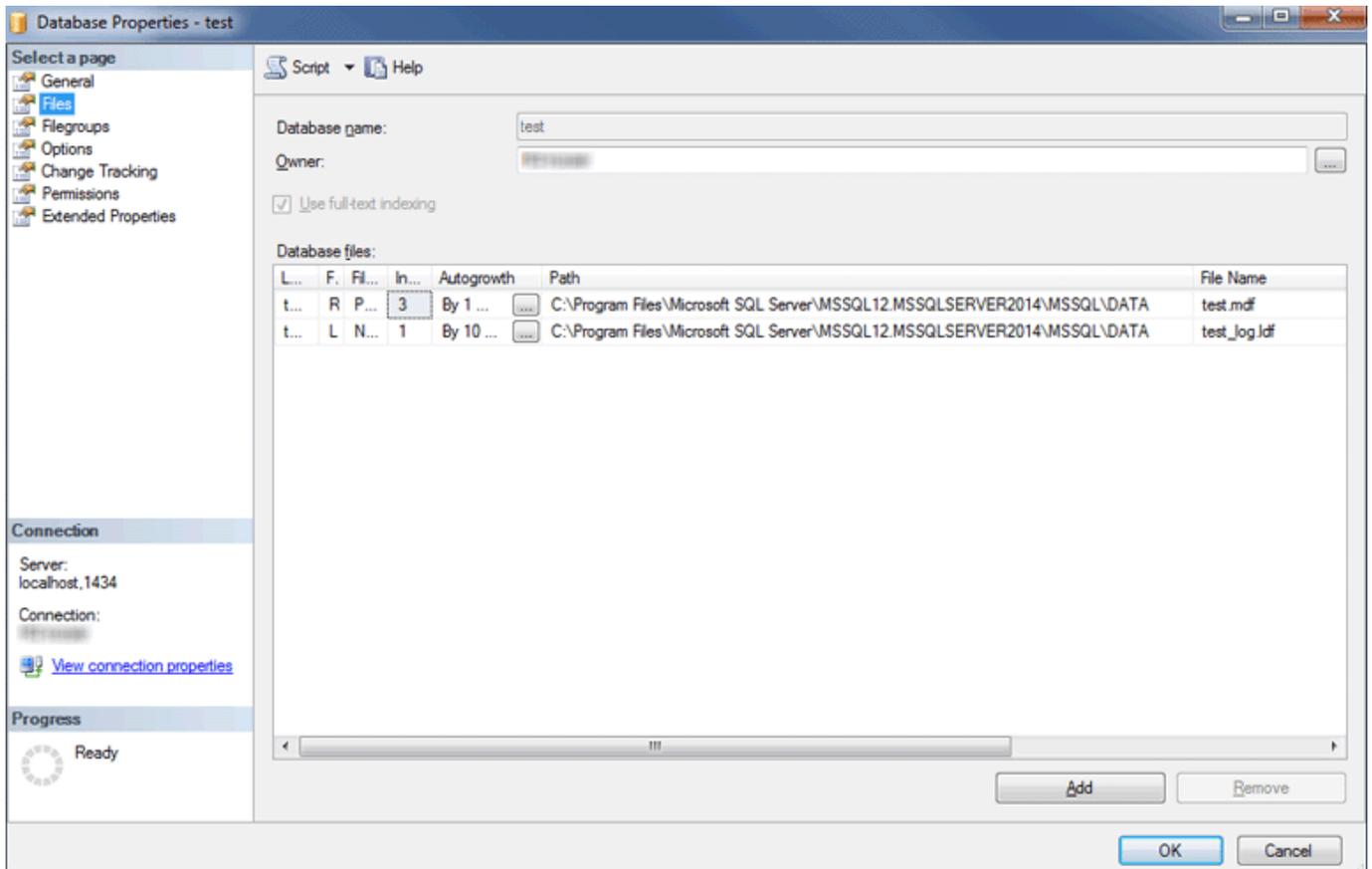


10. Klicken Sie auf **Hinzufügen**, navigieren Sie zu Ihrer Sicherungsdatei und öffnen Sie die Datei.

11. Wählen Sie die aktuellste Sicherung für die Wiederherstellung aus (der Sicherungssatz kann mehrere Sicherungen enthalten).

12. Klicken Sie im Wiederherstellungs-Assistenten auf die Seite **Optionen**. Wählen Sie bei Bedarf die Option **Vorhandene Datenbank überschreiben** aus und stellen Sie sicher, dass die Wiederherstellungsorte für die Datenbank (*.mdf*) und für das Log (*.ldf*) korrekt sind. Wenn Sie die Standardwerte unverändert übernehmen, werden die Pfade von Ihrer SQL Server-Quellinstanz verwendet. Sie sollten diese Werte daher überprüfen.

- Falls Sie nicht sicher sind, wo die DB-Dateien auf der SQL Server-Zielinstanz liegen, klicken Sie mit der rechten Maustaste auf eine vorhandene Datenbank, wählen Sie **Eigenschaften** aus und klicken Sie auf die Registerkarte **Dateien**. Sie finden den Speicherort der Datenbank in der Spalte **Pfad** der gezeigten Tabelle.

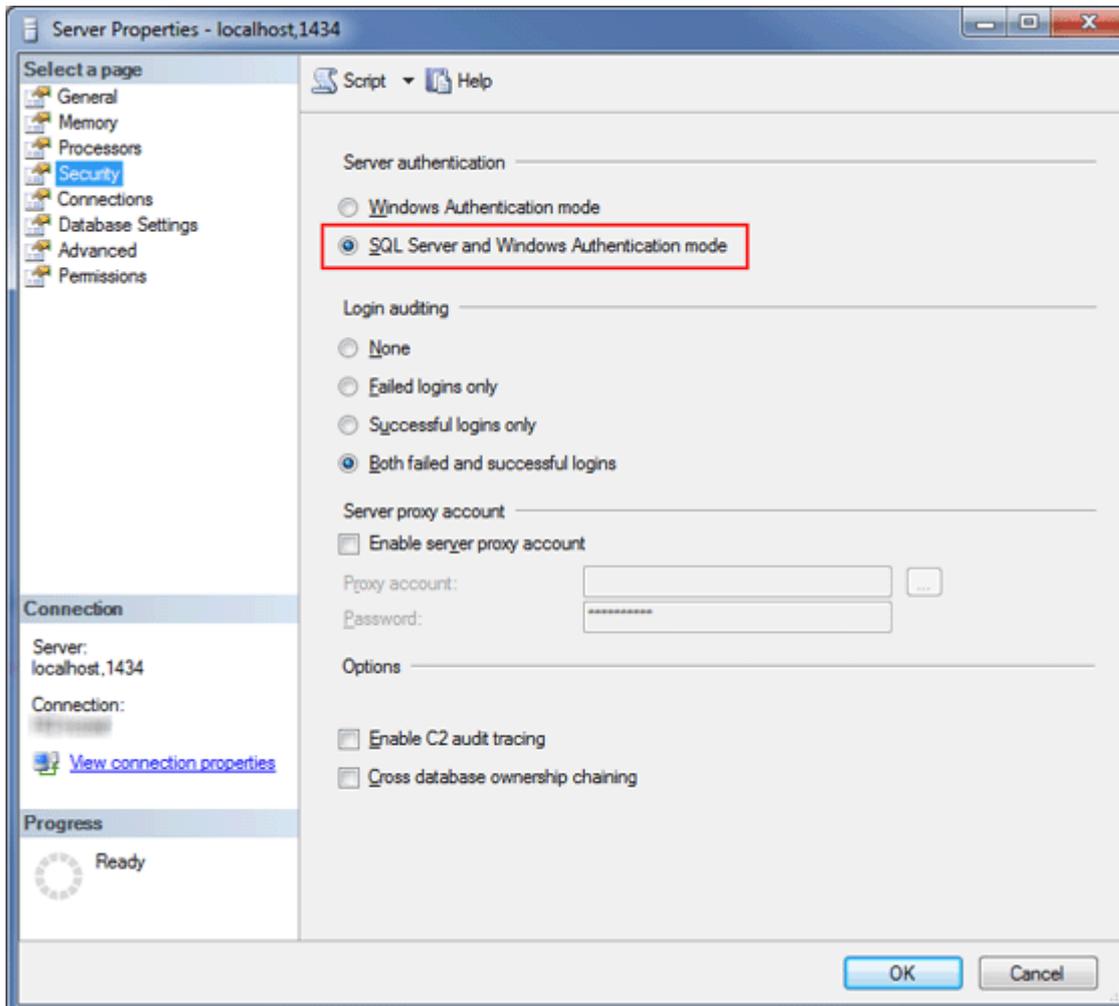


13. Klicken Sie im Wiederherstellungs-Assistenten auf **OK**.

14. Klicken Sie mit der rechten Maustaste auf die Datenbank **era_db**, wählen Sie **Neue Abfrage** aus und führen Sie die folgende Abfrage aus, um den Inhalt der Tabelle **tbl_authentication_certificate** zu löschen (andernfalls können sich die Agenten unter Umständen nicht mit dem neuen Server verbinden):

```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. Stellen Sie sicher, dass im neuen Datenbankserver die **SQL Server-Authentifizierung aktiviert** ist. Klicken Sie mit der rechten Maustaste auf den Server und klicken Sie anschließend auf **Eigenschaften**. Navigieren Sie zu **Sicherheit** und vergewissern Sie sich, dass der **SQL Server- und Windows-Authentifizierungsmodus** ausgewählt ist.



16. Erstellen Sie eine neue SQL Server-Anmeldung (für ESET PROTECT Server/ESET PROTECT MDM) auf der SQL Server-Zielinstanz mit **SQL Server-Authentifizierung** und ordnen Sie die Anmeldung zu einem Benutzer in der wiederhergestellten Datenbank zu.

o Deaktivieren Sie unbedingt die Option Kennwortablauf!

o Empfohlene Zeichen für Benutzernamen:

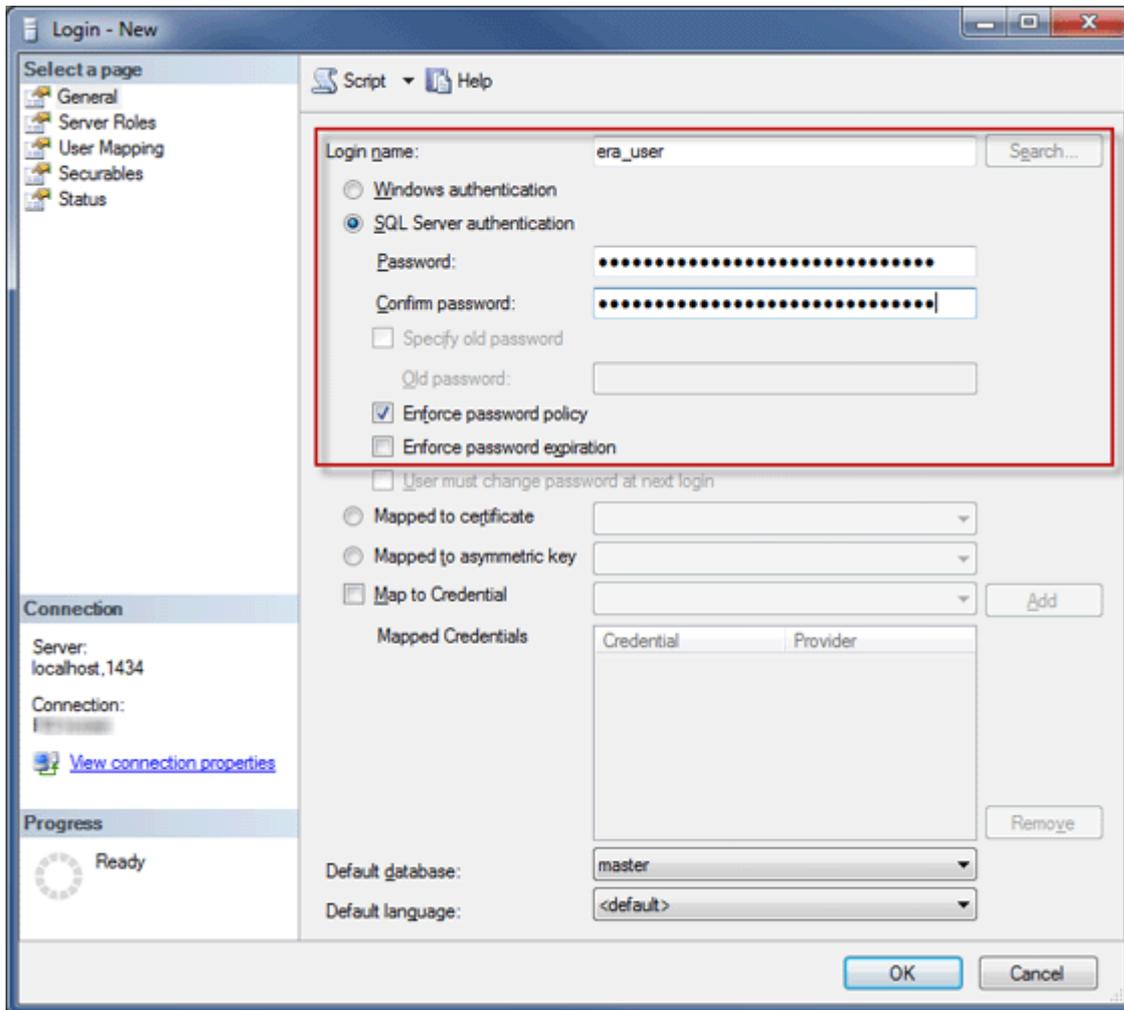
- ASCII-Kleinbuchstaben, Ziffern und Unterstrich "_"

o Empfohlene Zeichen für Passwörter:

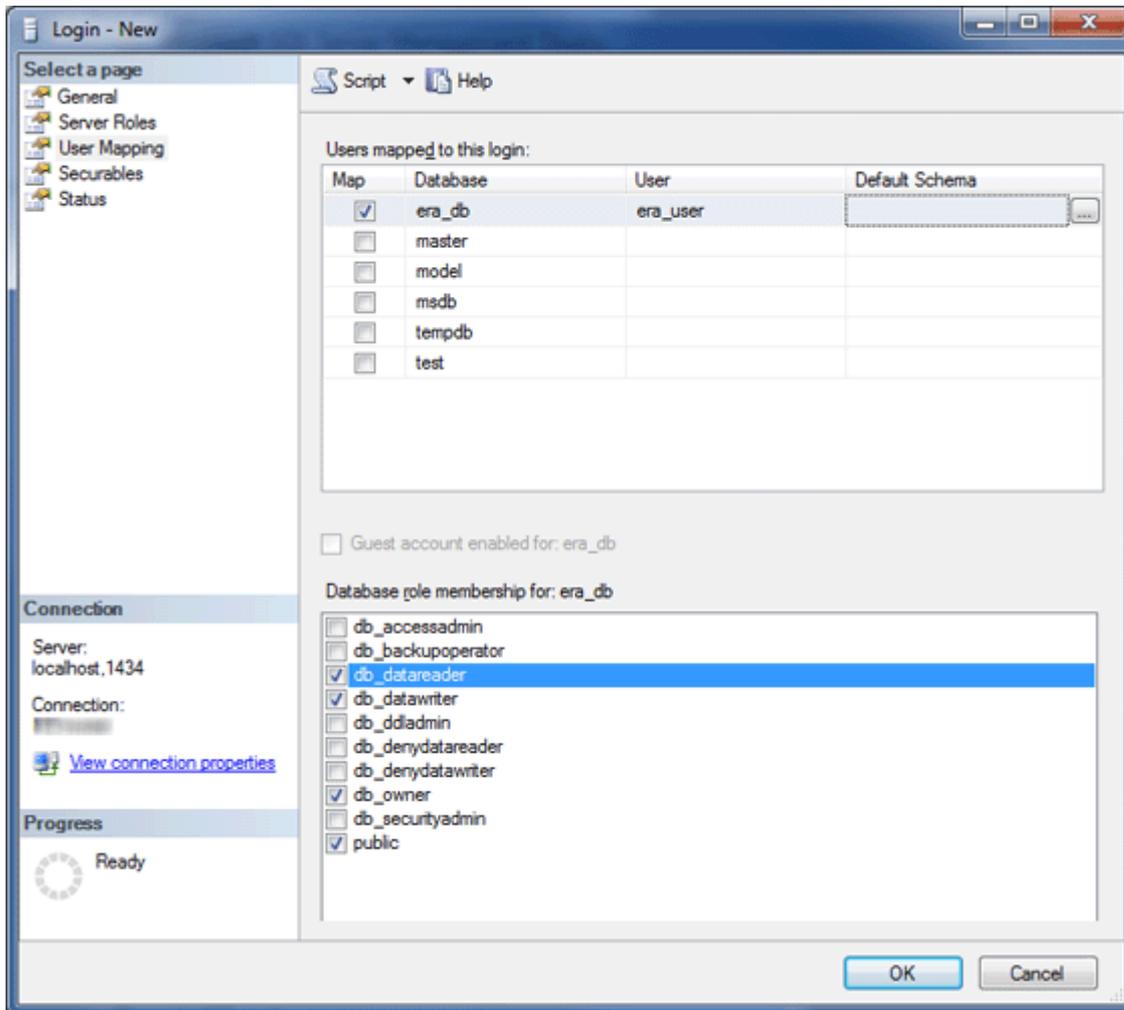
- AUSSCHLIESSLICH ASCII-Zeichen, inklusive ASCII-Groß- und Kleinbuchstaben, Ziffern, Leerzeichen, Sonderzeichen

o Verwenden Sie keine nicht-ASCII-Zeichen wie geschweifte Klammern {} oder @

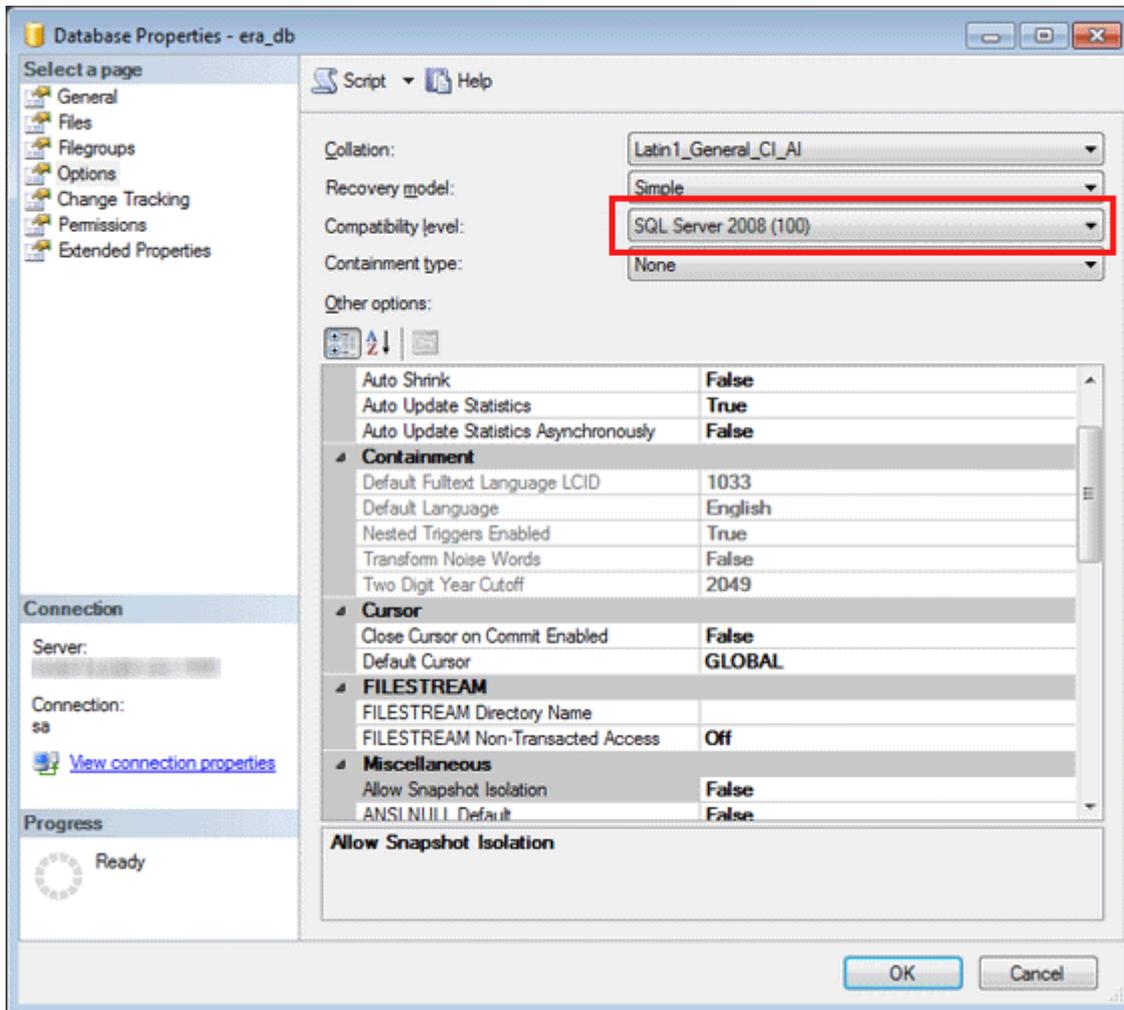
o Nichtbeachtung der obigen Zeichenempfehlungen kann zu Verbindungsproblemen in der Datenbank führen, falls Sie die Sonderzeichen in den späteren Schritten bei der Modifikation der Datenbankverbindungszeichenfolgen nicht maskieren. Dieses Dokument enthält keine Regeln für die Maskierung von Zeichen.



17. Ordnen Sie die Anmeldung zu einem Benutzer in der Zieldatenbank zu. Vergewissern Sie sich in der Registerkarte **Benutzerzuordnungen**, dass der Datenbankbenutzer die folgenden Rollen hat: **db_datareader**, **db_datawriter**, **db_owner**.

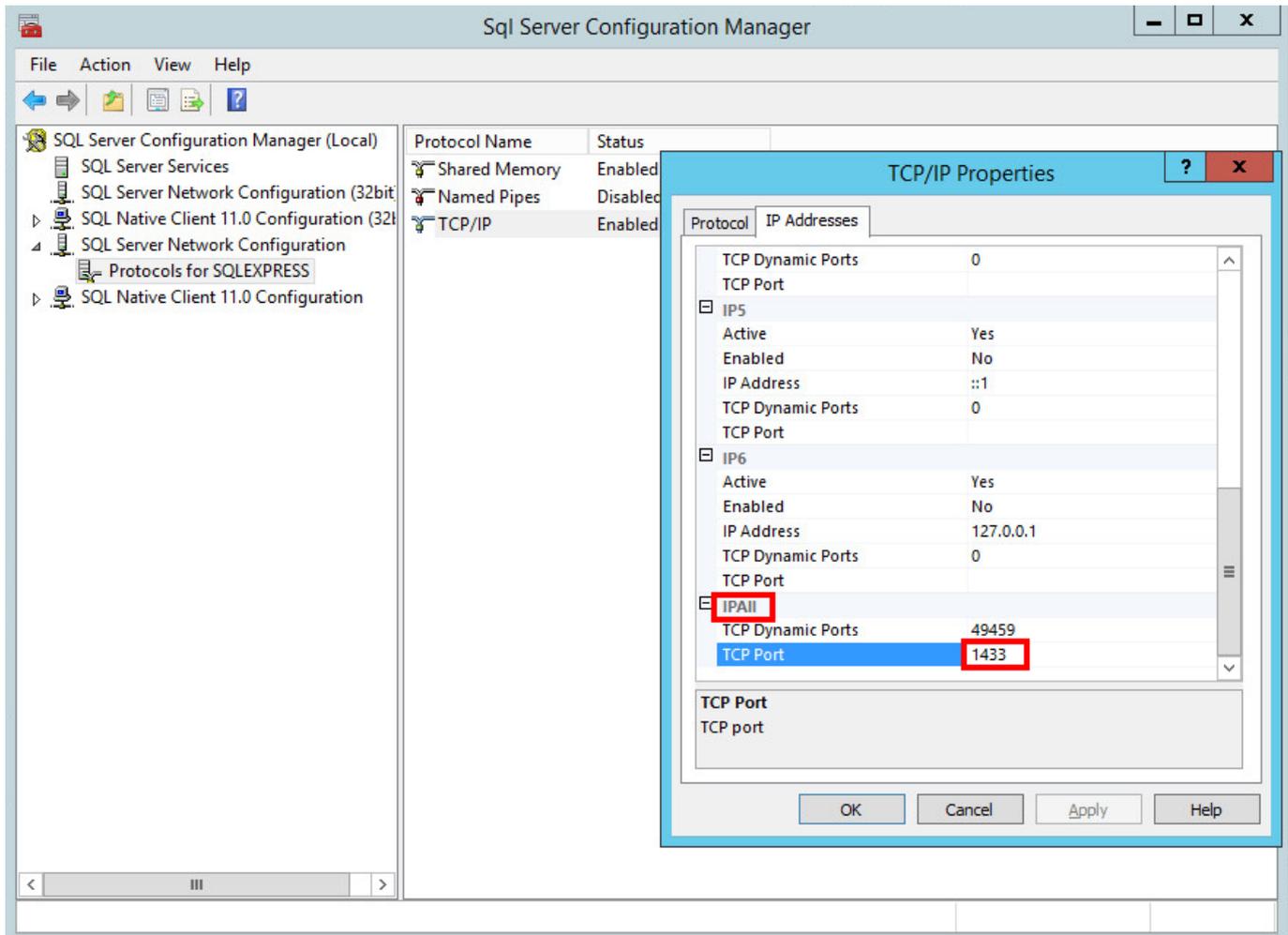


18. Ändern Sie den **Kompatibilitätsgrad** der wiederhergestellten Datenbank auf die neueste Version, um die aktuellsten Datenbankserver-Features nutzen zu können. Klicken Sie mit der rechten Maustaste auf die neue Datenbank und öffnen Sie deren **Eigenschaften**.



i SQL Server Management Studio kann keine neueren Kompatibilitätsgrade als die der verwendeten Version festlegen. Beispiel: In SQL Server Management Studio 2014 kann der Kompatibilitätsgrad SQL Server 2019 nicht festgelegt werden.

19. Stellen Sie sicher, dass das **TCP/IP**-Verbindungsprotokoll für „db_instance_name“ (z. B. SQLEXPRESS oder MSSQLSERVER) **aktiviert** ist, und dass der **TCP/IP-Port** auf **1433** festgelegt ist. Öffnen Sie dazu den **SQL Server-Konfigurations-Manager**, navigieren Sie zu **SQL Server-Netzwerkconfiguration > Protokolle für db_instance_name**, klicken Sie mit der rechten Maustaste auf **TCP/IP** und wählen Sie **Aktiviert** aus. Doppelklicken Sie auf **TCP/IP**, wechseln Sie zur Registerkarte **Protokolle**, blättern Sie nach unten zu **IPAll** und geben Sie 1433 in das Feld **TCP-Port** ein. Klicken Sie auf **OK** und starten Sie den **SQL Server**-Dienst neu.



20. [Verbinden Sie den ESET PROTECT Server oder MDM mit der Datenbank.](#)

Migrationsprozess für MySQL Server

Voraussetzungen

- SQL Server-Quell- und Zielinstanzen müssen installiert sein. Diese Instanzen können sich auf unterschiedlichen Computern befinden.
- Die MySQL-Tools (`mysqldump` und `mysql-Client`) müssen auf mindestens einem der Computer installiert sein.

Hilfreiche Links

- <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>

Migrationsprozess

Nehmen Sie in den folgenden Befehlen, Konfigurationsdateien und SQL-Anweisungen immer die folgenden Ersetzungen vor:

- **SRCHOST** mit der Adresse des Quelldatenbankservers
- **SRCROOTLOGIN** mit der root-Benutzeranmeldung für den MySQL-Quellserver
- **SRCDATABASE** mit dem Namen der zu sichernden ESET PROTECT-Quelldatenbank
- **BACKUPFILE** mit dem Pfad der Datei, in der die Sicherung gespeichert werden soll
- i** • **TARGETROOTLOGIN** mit der root-Benutzeranmeldung für den MySQL-Zielserver
- **TARGETHOST** mit der Adresse des Zieldatenbankservers
- **TARGETDATABASE** mit dem Namen der ESET PROTECT-Zieldatenbank (nach der Migration)
- **TARGETLOGIN** mit dem Anmeldenamen für den neuen ESET PROTECT-Datenbankbenutzer auf dem Datenbank-Zielserver
- **TARGETPASSWD** mit dem Passwort des neuen ESET PROTECT-Datenbankbenutzers auf dem Datenbank-Zielserver

Es ist nicht erforderlich, die folgenden SQL-Anweisungen in der Befehlszeile auszuführen. Falls kein GUI-Werkzeug verfügbar ist, können Sie eine Anwendung Ihrer Wahl verwenden.

1. Halten Sie die ESET PROTECT Server/MDM-Dienste an.
2. Erstellen Sie eine vollständige Datenbanksicherung der ESET PROTECT-Quelldatenbank (die zu migrierende Datenbank):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -  
u SRCROOTLOGIN -p SRCDATABASE > BACKUPFILE
```

3. Bereiten Sie eine leere Datenbank auf dem MySQL-Zielserver vor:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=CREATE DATABASE TARGETDATABASE /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

i Verwenden Sie Apostroph ' anstelle von Anführungszeichen " auf Linux-Systemen.

4. Stellen Sie die Datenbank auf dem MySQL-Zielserver in die zuvor vorbereitete leere Datenbank her:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDATABASE < BACKUPFILE
```

5. Erstellen Sie einen ESET PROTECT-Datenbankbenutzer auf dem MySQL-Zielserver:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

Empfohlene Zeichen für **TARGETLOGIN**:

- ASCII-Kleinbuchstaben, Ziffern und Unterstrich "_"

Empfohlene Zeichen für **TARGETPASSWD**:

- Ausschließlich ASCII-Zeichen, inklusive ASCII-Groß- und Kleinbuchstaben, Ziffern, Leerzeichen und Sonderzeichen
- Verwenden Sie keine nicht-ASCII-Zeichen wie geschweifte Klammern {} oder @

Nichtbeachtung der obigen Zeichenempfehlungen kann zu Verbindungsproblemen in der Datenbank führen, falls Sie die Sonderzeichen in den späteren Schritten bei der Modifikation der Datenbankverbindungszeichenfolgen nicht maskieren. Dieses Dokument enthält keine Regeln für die Maskierung von Zeichen.

6. Erteilen Sie dem ESET PROTECT-Datenbankbenutzer die benötigten Zugriffsrechte auf dem MySQL-Zielserver:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

i Verwenden Sie Apostroph ' anstelle von Anführungszeichen " auf Linux-Systemen.

7. Löschen Sie den Inhalt der Tabelle **tbl_authentication_certificate** (andernfalls können sich die Agenten unter Umständen nicht mit dem neuen Server verbinden):

```
mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. [Verbinden Sie den ESET PROTECT Server oder MDM mit der Datenbank.](#)

Verbindungsaufbau zwischen ESET PROTECT Server oder MD und einer Datenbank

Führen Sie die folgenden Schritte auf dem Computer mit ESET PROTECT Server oder ESET PROTECT MDM aus, um eine Datenbankverbindung herzustellen.

1. Beenden Sie den ESET PROTECT Server-/MDM-Dienst.
2. Suchen Sie die Datei *startupconfiguration.ini*.

- Windows:

Server:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration\startupconfiguration.ini
```

- Linux:

Server:

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore:

```
/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini
```

3. Ändern Sie die Datenbankverbindungszeichenfolge in der Datei *startupconfiguration.ini* für den ESET PROTECT Server/MDM.

o Tragen Sie Adresse und Port des neuen Datenbankservers ein.

o Tragen Sie den ESET PROTECT-Benutzernamen und das Passwort in die Verbindungszeichenfolge ein.

Das Endergebnis sollte wie folgt aussehen:

- MS 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;
```

Ersetzen Sie in der obigen Konfiguration immer Folgendes:

- **TARGETHOST** mit der Adresse des Zieldatenbankservers
- **TARGETDBNAME** mit dem Namen der ESET PROTECT-Zieldatenbank (nach der Migration)
- **TARGETLOGIN** mit dem Anmeldenamen für den neuen ESET PROTECT-Datenbankbenutzer auf dem Datenbank-Zielservers
- **TARGETPASSWD** mit dem Passwort des neuen ESET PROTECT-Datenbankbenutzers auf dem Datenbank-Zielservers

4. Starten Sie den ESET PROTECT Server bzw. ESET PROTECT MDM und vergewissern Sie sich, dass der Dienst korrekt ausgeführt wird.

Migration von MDM

Mit dem hier beschriebenen Verfahren können Sie Ihre vorhandene Instanz von ESET PROTECT MDM migrieren und **Ihre vorhandene ESET PROTECT MDM-Datenbank behalten**, inklusive der registrierten Mobilgeräte. Die migrierte ESET PROTECT MDM-Instanz hat **dieselbe IP-Adresse und denselben Hostnamen** wie die alte ESET PROTECT MDM-Instanz, und die Datenbank der alten ESET PROTECT MDM-Instanz wird vor der Installation auf den neuen MDM-Host importiert.

- Die [Datenbankmigration](#) wird nur zwischen gleichen Datenbanktypen unterstützt (von MySQL zu MySQL oder von MSSQL zu MSSQL).
- Bei der Migration einer Datenbank müssen Sie zwischen Instanzen derselben ESET PROTECT-Version migrieren. In unserem [Knowledgebase-Artikel](#) finden Sie Anweisungen zur Ermittlung der Versionen Ihrer ESET PROTECT-Komponenten. Nach Abschluss der Datenbankmigration können Sie bei Bedarf ein Upgrade auf die aktuelle Version von ESET PROTECT durchführen.

Gehen Sie auf Ihrem aktuellen (alten) ESET PROTECT MDM Server wie folgt vor:

1. Erstellen Sie eine Sicherung der MDM-Konfiguration.

a) Klicken Sie unter **Computer** auf den MDM-Server und wählen Sie **Details** aus.

b) Klicken Sie auf **Konfiguration > Konfiguration anfordern**. Je nach Verbindungsintervall des Agenten müssen Sie unter Umständen einige Zeit warten, bis die angeforderte Konfiguration erstellt wurde.

c) Klicken Sie auf den **ESET PROTECT Mobile Device Connector** und wählen Sie **Konfiguration öffnen** aus.

d) Exportieren Sie die folgenden Elemente aus der Konfiguration in einen externen Speicher:

o Der exakte Hostname Ihres MDM Servers.

o Peerzertifikate – Die exportierten `.pfx`-Dateien enthalten den privaten Schlüssel.

- Falls Sie einen ESET PROTECT MDM-Server unter Linux verwenden, müssen Sie das HTTPS-Zertifikat aus der MDM-Konfigurations-Policy exportieren:
- I. Klicken Sie auf **Ansicht** neben **HTTPS-Zertifikat**.
 - II. Klicken Sie auf  **Herunterladen** und laden Sie das HTTPS-Zertifikat im PFX-Format herunter.

e) Exportieren Sie ebenfalls die folgenden Zertifikate und Token, falls vorhanden:

o Das Signaturzertifikat für das Registrierungsprofil.

o Ein APNS-Zertifikat (exportieren Sie sowohl das APNS-Zertifikat als auch den privaten APNS-Schlüssel).

o Das Autorisierungstoken für das Apple Device Enrollment Program (DEP).

2. Halten Sie den ESET PROTECT MDM-Dienst an.

3. [Exportieren/Sichern Sie die ESET PROTECT MDM-Datenbank](#).

4. Fahren Sie den aktuellen ESET PROTECT MDM-Computer herunter.

 Sie sollten Ihren alten ESET PROTECT MDM noch nicht deinstallieren oder stilllegen.

Gehen Sie auf Ihrem neuen ESET PROTECT MDM Server wie folgt vor:

 Stellen Sie sicher, dass die Netzwerkkonfiguration auf Ihrem neuen ESET PROTECT MDM Server (der Hostname, den Sie aus der Konfiguration Ihres alten MDM Servers exportiert haben) mit der Konfiguration Ihres alten ESET PROTECT MDM Servers übereinstimmt.

1. Installieren/Starten Sie eine ESET PROTECT [unterstützte](#) MDM-Datenbank.
2. Importieren Sie die [ESET PROTECT-Datenbank](#) aus Ihrem alten ESET PROTECT MDM bzw. stellen Sie sie wieder her.
3. Installieren Sie den ESET PROTECT Server/MDM mit dem [All-in-One-Installationsprogramm](#) (Windows) oder wählen Sie [eine andere Installationsart aus](#) (manuelle Windows-Installation, Linux oder virtuelle Appliance). Geben Sie die Einstellungen für Ihre Datenbankverbindung bei der Installation des ESET PROTECT MDM an.

 Verwenden Sie bei der [Installation von ESET PROTECT MDM unter Linux](#) das HTTPS-Zertifikat aus Ihrer Sicherung.

4. [Verbinden](#) Sie sich mit der ESET PROTECT-Web-Konsole.
5. [Starten Sie den ESET PROTECT-Dienst neu](#).

Die verwalteten Mobilgeräte sollten sich jetzt mit dem ursprünglichen Zertifikat mit Ihrem neuen ESET PROTECT MDM Server verbinden können.

Deinstallation des alten ESET PROTECT Servers/MDM:

Sobald Ihr neuer ESET PROTECT Server reibungslos funktioniert, können Sie Ihren alten ESET PROTECT Server/MDM mit unserer [Schritt-für-Schritt-Anleitung](#) sorgfältig deinstallieren.

Neue IP-Adresse oder neuer Hostname für ESET PROTECT Server nach der Migration

Gehen Sie wie folgt vor, um die IP-Adresse oder den Hostnamen Ihres ESET PROTECT Servers zu ändern:

1. Falls Ihr ESET PROTECT Server-Zertifikat eine exakte IP-Adresse und/oder einen Hostnamen enthält, müssen Sie ein [neues Serverzertifikat erstellen](#) und dabei die neue IP-Adresse bzw. den neuen Hostnamen angeben. Wenn das Host-Feld in Ihrem Serverzertifikat ein Platzhalterzeichen (*) enthält, können Sie **mit Schritt 2 fortfahren**. Erstellen Sie andernfalls das neue Serverzertifikat mit der neuen IP-Adresse und dem neuen Hostnamen getrennt durch ein Komma, und geben Sie die alte IP-Adresse und den alten Hostnamen ebenfalls an.
2. Signieren Sie das neue Serverzertifikat mit Ihrer ESET PROTECT Server-Zertifizierungsstelle.
3. Erstellen Sie eine Policy, in der Sie die Clientverbindungen auf die neue IP-Adresse bzw. den neuen Hostnamen ändern (bevorzugt die IP-Adresse). Geben Sie eine zweite (alternative) Verbindung zur alten IP-

Adresse bzw. dem alten Hostnamen an, damit sich der ESET Management Agent mit beiden Servern verbinden kann. Weitere Informationen finden Sie unter [Erstellen einer Policy für die Verbindung zwischen ESET Management Agent und ESET PROTECT Server](#).

4. Wenden Sie diese Policy auf Ihren Clientcomputern an und warten Sie ab, bis die ESET Management Agenten repliziert wurden. Obwohl die Policy Ihre Clients auf den neuen Server verweist (der noch nicht online ist), verwenden die ESET Management Agenten die alternativen Serverinformationen, um sich mit der alten IP-Adresse zu verbinden.

5. Legen Sie Ihr [neues Serverzertifikat unter Mehr > Einstellungen](#) fest.

6. Starten Sie den ESET PROTECT Server-Dienst neu und ändern Sie die IP-Adresse bzw. den Hostnamen.

Unser [Knowledgebase-Artikel](#) enthält illustrierte Anweisungen zur Änderung der Adresse des ESET PROTECT Servers.

Migration von ERA 5.x

Direkte Upgrades oder Migrationen von ERA 5.x zu ESET PROTECT 9.1 werden nicht unterstützt.

Falls Sie ERA 5.x installiert haben, führen Sie die folgenden Aktionen aus:

1. [Migrieren Sie von ERA 5.x zu ESMC 7.2](#).
2. [Führen Sie ein Upgrade von ESMC 7.2 zu ESET PROTECT 9.1 aus](#)

ESET PROTECT Server und Komponenten deinstallieren

Wählen Sie eines der folgenden Kapitel aus, um ESET PROTECT Server und die Komponenten zu deinstallieren:

- [ESET Management Agent deinstallieren](#)
- [Windows - ESET PROTECT Server und Komponenten deinstallieren](#)
- [Linux - ESET PROTECT-Komponenten aktualisieren, erneut installieren oder deinstallieren](#)
- [macOS - ESET Management Agent und ESET Endpoint-Produkt deinstallieren](#)
- [Alten ESMC/ESET PROTECT/MDM-Server nach der Migration auf einen anderen Server außer Betrieb nehmen](#)

ESET Management Agent deinstallieren

Der ESET Management Agent kann auf verschiedene Arten deinstalliert werden.

Remote-Deinstallation mit der ESET PROTECT-Web-Konsole

1. [Melden Sie sich bei der ESET PROTECT-Web-Konsole an](#).
2. Wählen Sie im Bereich **Computer** einen Computer aus, von dem Sie den ESET Management Agenten

entfernen möchten, und klicken Sie auf **Neuer Task**.

Bei Bedarf können Sie mehrere Computer über die jeweiligen Kontrollkästchen auswählen und auf **Computer > Tasks > Neuer Task** klicken.

3. Geben Sie einen **Namen** für den Task ein.

4. Wählen Sie in der Dropdownliste **Taskkategorie** den Eintrag **ESET PROTECT** aus.

5. Wählen Sie in der Dropdownliste **Task** den Eintrag [Verwaltung beenden \(ESET Management Agent deinstallieren\)](#) aus.

Wenn Sie den ESET Management Agenten von einem Clientcomputer deinstallieren, wird das Gerät nicht mehr von ESET PROTECT verwaltet:

- Im ESET-Sicherheitsprodukt werden nach der Deinstallation des ESET Management Agenten möglicherweise einige Einstellungen beibehalten.
- Wenn der Agent mit einem Passwort geschützt ist, können Sie ihn nicht deinstallieren. Es ist sinnvoll, bestimmte Einstellungen, die Sie nicht beibehalten möchten (z. B. den Passwortschutz) mithilfe einer [Policy](#) auf den Standardwert zurückzusetzen, bevor Sie das Gerät von der Verwaltung ausschließen.
- Außerdem werden alle auf dem Agenten ausgeführten Tasks abgebrochen. Der Ausführungsstatus **Wird ausgeführt**, **Fertig** oder **Fehler des Tasks** wird je nach Replikation möglicherweise nicht richtig in der ESET PROTECT-Web-Konsole angezeigt.
- Nach der Deinstallation des Agenten können Sie Ihr Sicherheitsprodukt über die integrierte EGUI oder über die [eShell](#) verwalten.

6. Überprüfen Sie die **Zusammenfassung** des Tasks und klicken Sie auf **Fertig** stellen.

7. Klicken Sie auf [Trigger erstellen](#), um festzulegen, wann und auf welchen **Zielen** dieser Client-Task ausgeführt werden soll.

Lokale Deinstallation – Windows

Beachten Sie auch die Anweisungen zur lokalen Deinstallation des ESET Management Agenten unter [Linux](#) oder [macOS](#).

i Hinweise zur Fehlerbehebung bei der Deinstallation des Agenten finden Sie unter [ESET Management Agent – Deinstallation und Fehlerbehandlung](#).

1. Verbinden Sie sich mit dem Endpunkt-Computer, von dem Sie den ESET Management Agenten deinstallieren möchten (z. B. per RDP).

2. Navigieren Sie zu **Systemsteuerung > Programme und Features** und doppelklicken Sie auf **ESET Management Agent**.

3. Klicken Sie auf **Weiter > Entfernen** und folgen Sie den Anweisungen für die Deinstallation.

Falls Sie ein Passwort mit einer Policy für Ihre ESET Management Agenten eingerichtet haben, können Sie die folgenden Optionen verwenden:

- Sie müssen das Passwort bei der Deinstallation eingeben.
- Heben Sie die Zuweisung der Policy auf, bevor Sie den ESET Management Agent deinstallieren.
- [Stellen Sie den ESET Management Agent mit einem vorhandenen passwortgeschützten Agent erneut bereit](#) (Knowledgebase-Artikel).

Windows - ESET PROTECT Server und Komponenten deinstallieren

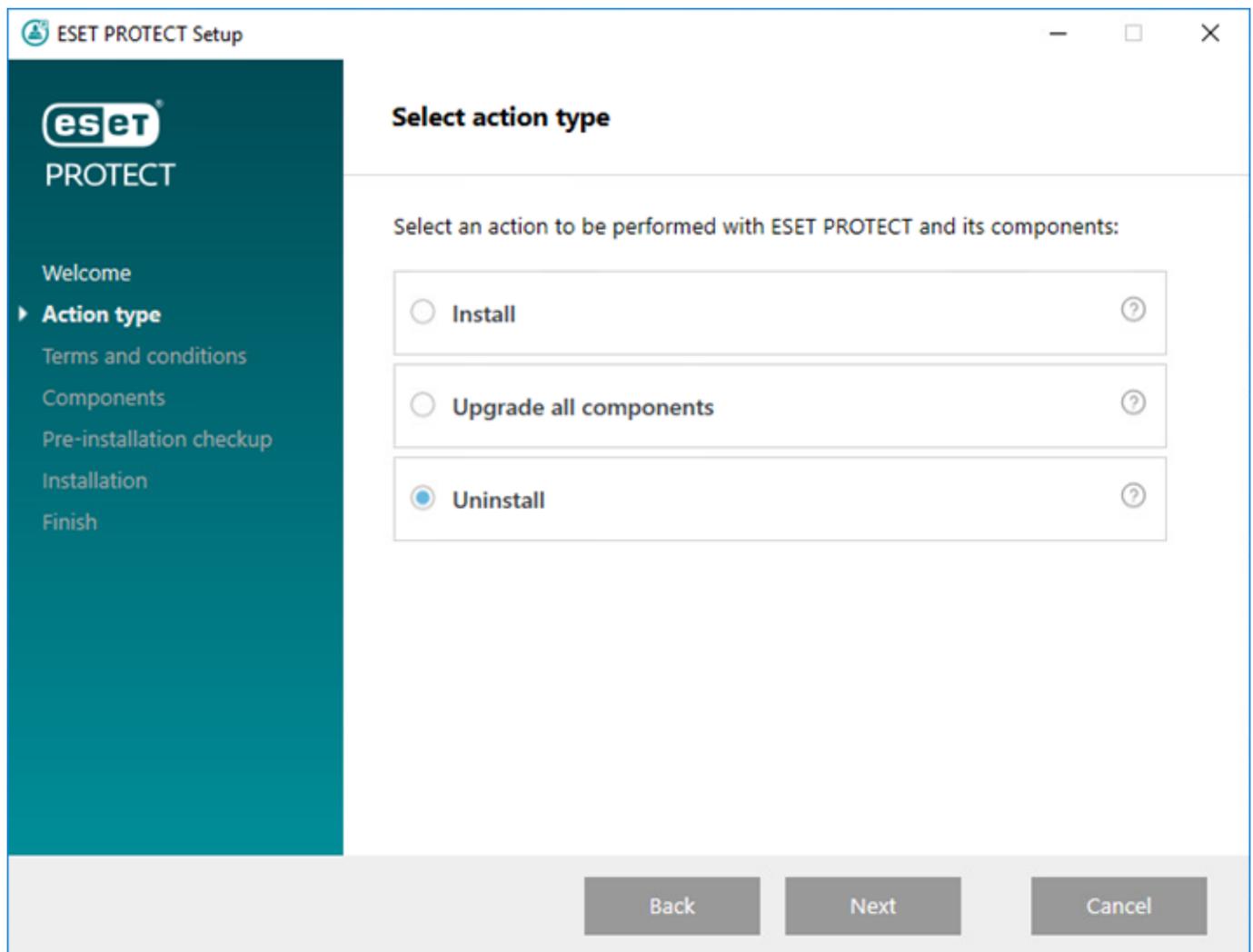
Vor der Deinstallation von ESET PROTECT müssen Sie [die Agenten auf den verwalteten Computern deinstallieren](#).



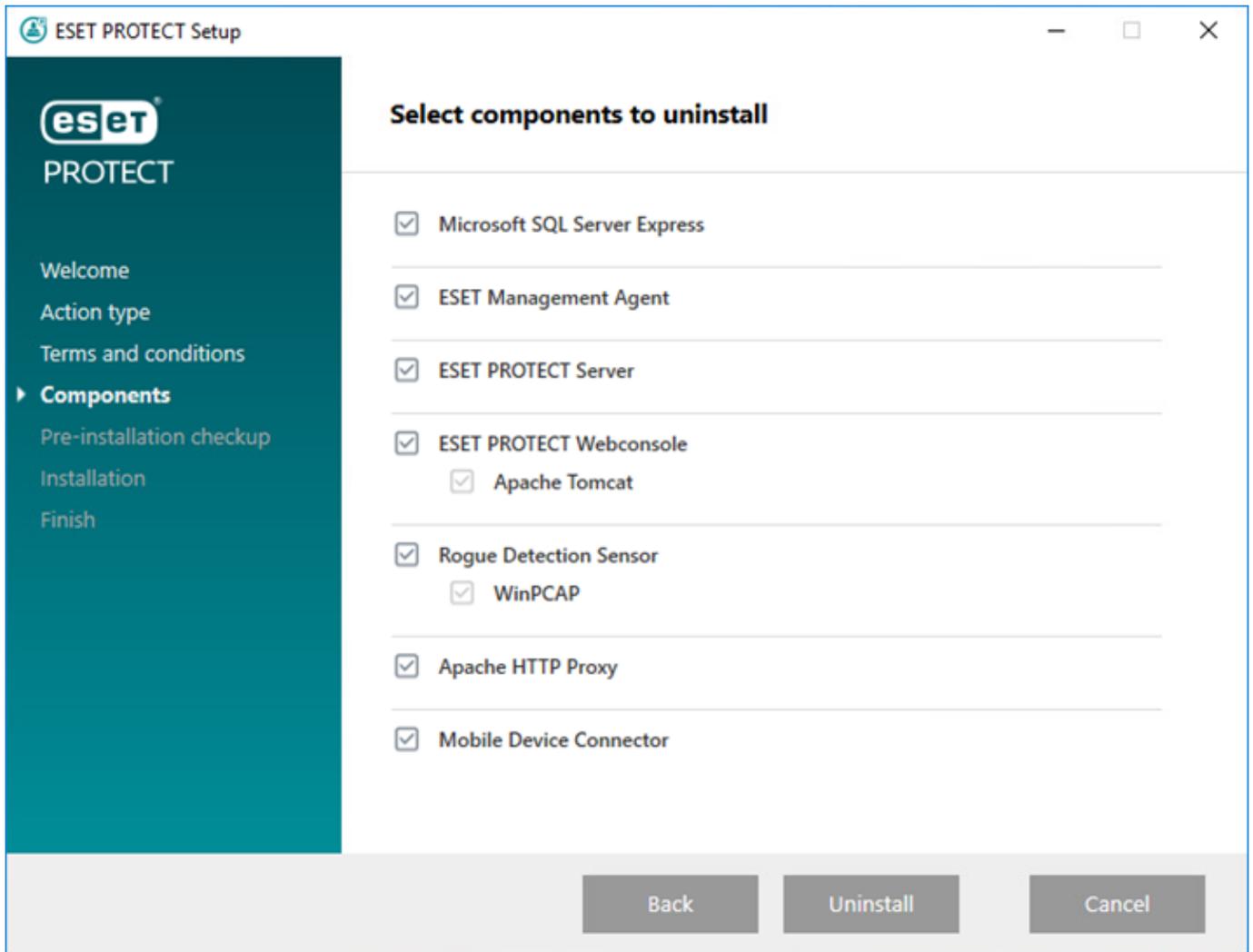
Lesen Sie den Artikel [MDM iOS-Lizenzierungsfunktion](#), bevor Sie den Mobile Device Connector deinstallieren.

Gehen Sie wie folgt vor, um ESET PROTECT Server und die Komponenten unter Windows zu deinstallieren:

1. Laden Sie das [ESET PROTECT All-in-One-Installationsprogramm](#) herunter und extrahieren Sie das Paket.
2. Führen Sie die Datei *Setup.exe* aus. Sie können die **Sprache** im Dropdownmenü auswählen. Klicken Sie auf **Weiter**.
3. Wählen Sie **Deinstallieren** aus und klicken Sie auf **Weiter**.



4. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.
5. Wählen Sie die Komponenten aus, die deinstalliert werden sollen und klicken Sie auf **Deinstallieren**.



6. Unter Umständen muss der Computer neu gestartet werden, um die Deinstallation der Komponenten abzuschließen.

i Siehe auch [Alten ESMC/ESET PROTECT/MDM-Server nach der Migration auf einen anderen Server außer Betrieb nehmen](#).

Linux - ESET PROTECT-Komponenten aktualisieren, erneut installieren oder deinstallieren

Zum Ausführen einer Neuinstallation oder einer Aufrüstung auf eine neuere Version führen Sie erneut das Installationskript aus.

Zur Deinstallation einer Komponente (in diesem Fall der ESET PROTECT Server) führen Sie das Installationsprogramm wie nachfolgend gezeigt mit dem Parameter `--uninstall` aus:

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

Falls Sie andere Komponenten deinstallieren möchten, verwenden Sie den entsprechenden Paketnamen im Befehl. Zum Beispiel für den ESET Management Agenten:

```
sudo ./agent-linux-x86_64.sh --uninstall
```



Bei der Deinstallation werden Konfigurations- und Datenbankdateien gelöscht. Um die Datenbankdateien beizubehalten, erstellen Sie eine SQL-Sicherung der Datenbank oder verwenden Sie den Parameter `--keep-database`.

Überprüfen Sie nach der Deinstallation, ob

- der Dienst `eraserver` gelöscht wurde.
- der Ordner `/etc/opt/eset/RemoteAdministrator/Server/` gelöscht wurde.



Es empfiehlt sich, vor der Deinstallation eine Datenbanksicherung auszuführen, falls Sie die Daten später wiederherstellen möchten.

Weitere Informationen zum erneuten Installieren des Agenten finden Sie im entsprechenden [Kapitel](#). Hinweise zur Fehlerbehebung bei der Deinstallation des Agenten finden Sie unter [ESET Management Agent – Deinstallation und Fehlerbehandlung](#).

macOS - ESET Management Agent und ESET Endpoint-Produkt deinstallieren

Deinstallieren Sie den ESET Management Agent und das ESET Endpoint-Produkt lokal oder Remote über ESET PROTECT.

In unserem [Knowledgebase-Artikel](#) finden Sie eine ausführliche Anleitung für die lokale Deinstallation von ESET Management Agent und ESET Endpoint-Produkt.



Falls Sie das ESET Endpoint-Produkt remote deinstallieren möchten, sollten Sie dies unbedingt tun, bevor Sie den ESET Management Agenten deinstallieren.

ESET Management Agent lokal deinstallieren

1. Klicken Sie auf **Finder**, um ein neues **Finder**-Fenster zu öffnen.
2. Klicken Sie auf **Anwendungen** > halten Sie **Strg** gedrückt > klicken Sie auf **ESET Management Agent** > wählen Sie **Paketinhalt anzeigen** im Kontextmenü aus.
3. Navigieren Sie zu **Inhalt** > **Skripts** und doppelklicken Sie auf **Uninstaller.command**, um das Installationsprogramm auszuführen.
4. Geben Sie Ihr Administratorpasswort ein und drücken Sie die **Eingabetaste**, wenn Sie zur Eingabe des Passworts aufgefordert werden.
5. Wenn der ESET Management Agent deinstalliert wurde, wird die Nachricht **Prozess abgeschlossen** angezeigt.

ESET Management Agent lokal im Terminal deinstallieren

1. Öffnen Sie **Finder** > **Anwendungen** > **Hilfsprogramme** > **Terminal**.

2. Geben Sie den folgenden Code ein und drücken Sie die **Eingabetaste**:

```
sudo /Applications/ESET\ Administrator\ Agent.app/Contents/Scripts/Uninstall.command ; exit;
```

3. Geben Sie Ihr Administratorpasswort ein und drücken Sie die **Eingabetaste**, wenn Sie zur Eingabe des Passworts aufgefordert werden.

4. Wenn der ESET Management Agent deinstalliert wurde, wird die Nachricht **Prozess abgeschlossen** angezeigt.

ESET Management Agent über ESET PROTECT remote deinstallieren

Klicken Sie unter **Computer** auf den macOS-Clientcomputer und wählen Sie [Entfernen](#) aus, um den ESET Management Agenten zu deinstallieren und den Computer aus der Verwaltung zu entfernen.

Hinweise zur Fehlerbehebung bei der Deinstallation des Agenten finden Sie unter [ESET Management Agent – Deinstallation und Fehlerbehandlung](#).

ESET Endpoint-Produkt lokal deinstallieren

1. Klicken Sie auf **Finder**, um ein neues **Finder**-Fenster zu öffnen.

2. Klicken Sie auf **Anwendungen** > halten Sie **Strg** gedrückt > klicken Sie auf **ESET Endpoint Security** oder **ESET Endpoint Antivirus** > wählen Sie **Paketinhalt anzeigen** im Kontextmenü aus.

3. Navigieren Sie zu **Inhalt** > **Hilfsprogramme** und doppelklicken Sie auf **Uninstaller.app**, um das Installationsprogramm auszuführen.

4. Klicken Sie auf **Deinstallieren**.

5. Geben Sie Ihr Administratorpasswort ein und klicken Sie auf **OK**, wenn Sie zur Eingabe des Passworts aufgefordert werden.

6. Wenn ESET Endpoint Security oder ESET Endpoint Antivirus erfolgreich deinstalliert wurde, wird die Meldung **Deinstallation erfolgreich** angezeigt. Klicken Sie auf **Schließen**.

ESET Endpoint-Produkt lokal im Terminal deinstallieren

1. Öffnen Sie **Finder** > **Anwendungen** > **Hilfsprogramme** > **Terminal**.

2. Geben Sie den folgenden Code ein und drücken Sie die **Eingabetaste**:

- Deinstallieren ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
```

- Deinstallieren ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/  
Contents/Scripts/uninstall.sh
```

3. Geben Sie Ihr Administratorpasswort ein und drücken Sie die **Eingabetaste**, wenn Sie zur Eingabe des Passworts aufgefordert werden.
4. Wenn das ESET Endpoint-Produkt deinstalliert wurde, wird die Nachricht **Prozess abgeschlossen** angezeigt.

ESET Endpoint-Produkt über ESET PROTECT remote deinstallieren

Um den ESET Management Agenten remote über ESET PROTECT zu deinstallieren, haben Sie die folgenden Optionen:

- Klicken Sie unter **Computer** auf den macOS-Clientcomputer, wählen Sie **Details > Installierte Anwendungen** aus > wählen Sie **ESET Endpoint Security** oder **ESET Endpoint Antivirus** aus und klicken Sie auf die Schaltfläche **Deinstallieren**.
- Führen Sie den [Task Software-Installation](#) aus.

Alten ESMC/ESET PROTECT/MDM-Server nach der Migration auf einen anderen Server außer Betrieb nehmen



Stellen Sie sicher, dass Ihr neuer ESET PROTECT Server/MDM funktioniert und dass sich die Clientcomputer und Mobilgeräte korrekt mit Ihrem neuen ESET PROTECT verbinden.

Bei der Außerbetriebnahme Ihres alten ESMC/ESET PROTECT/MDM Servers nach der Migration auf einen anderen Server haben Sie verschiedene Optionen zur Auswahl:

I. Betriebssystem des Servers beibehalten und wiederverwenden

1. [Beenden Sie den alten ESMC/ESET PROTECT Server-Dienst](#).
2. Löschen Sie (DROP DATABASE) die alte ESMC/ESET PROTECT Server-Datenbankinstanz (MS SQL oder MySQL).



Falls Sie die Datenbank auf den neuen ESET PROTECT Server migriert haben, sollten Sie die Datenbank auf dem alten ESMC/ESET PROTECT Server vor der Deinstallation löschen, um zu verhindern, dass Lizenzen aus der neuen ESET PROTECT Server-Datenbank getrennt (entfernt) werden.

3. Deinstallieren Sie den alten ESMC/ESET PROTECT/MDM-Server und alle zugehörigen Komponenten (inklusive ESET Management Agent, Rogue Detection Sensor, MDM usw.):

o [ESMC 7.2 deinstallieren - Linux](#)

o [ESET PROTECT 8.x deinstallieren - Windows](#)

o [ESET PROTECT 9.x deinstallieren – Windows](#)

⚠ Deinstallieren Sie Ihre Datenbank nicht, wenn diese für andere Programme benötigt wird.

4. Planen Sie einen Neustart Ihres Servers nach der Deinstallation

II. Servercomputer beibehalten

Der einfachste Weg, um ESMC/ESET PROTECT/MDM zu entfernen, ist das Formatieren des Datenträgers, auf dem die Software installiert ist.

⚠ Dabei werden alle Daten auf dem Datenträger gelöscht, inklusive des Betriebssystems.

Fehlerbehebung

ESET PROTECT ist ein komplexes Produkt, das verschiedene externe Tools verwendet und unterschiedliche BS-Plattformen unterstützt. Daher können Probleme auftreten, die behoben werden müssen.

In der ESET-Dokumentation finden Sie verschiedene Methoden zur Fehlerbehebung für ESET PROTECT. Lesen Sie die [Antworten auf gängige Probleme bei der Installation](#), um häufig auftretende Probleme mit ESET PROTECT zu beheben. Siehe auch [bekannte Probleme für ESET Unternehmensprodukte](#).

Konnten Sie Ihr Problem nicht beheben?

- Jede ESET PROTECT-Komponente hat eine [Logdatei](#), die für verschiedene Ausführlichkeitsstufen konfiguriert werden kann. Überprüfen Sie die Logs, um Fehler zu identifizieren, die bei der Behebung Ihres Problems hilfreich sein können.
- Der Informationsumfang für die einzelnen Komponenten wird in der jeweiligen [Policy festgelegt](#) > **Erweiterte Einstellungen** > **Logging** > **Informationsumfang für Trace-Log** – Legen Sie die Mindestinformationen fest, die erfasst und in Logs geschrieben werden. Die Abstufung reicht von **Trace** (umfangreiche Informationen) bis **Schwerwiegend** (wichtigste, kritische Informationen).

o [ESET Management Agenten-Policy](#) – Die Policy muss auf das Gerät angewendet werden, um in Kraft zu treten. Um das vollständige ESET Management Agenten-Logging in der Datei *trace.log* zu aktivieren, erstellen Sie im gleichen Ordner wie *trace.log* eine Dummy-Datei mit dem Namen *traceAll* und ohne Dateierweiterung, und starten Sie den Computer neu (um den ESET Management Agenten-Dienst neu zu starten).

o [ESET PROTECT Servereinstellungen](#)

o [ESET Mobile Device Connector-Policy](#) – Die Policy muss auf das Gerät angewendet werden, um in Kraft zu treten. Siehe auch [MDM-Fehlerbehebung](#).

- Falls Sie Ihr Problem nicht beheben können, besuchen Sie das [ESET Sicherheitsforum](#) und wenden Sie sich an die ESET-Community für Informationen zu möglichen Problemen.
- Wenn Sie sich an den technischen [ESET-Support](#) wenden, werden Sie unter Umständen aufgefordert, Log-Dateien mit dem [ESET Log Collector](#) oder dem [Diagnose-Tool](#) zu sammeln. Wir empfehlen dringend, Logs an Supportanfragen anzufügen, um die Bearbeitung Ihrer Supportanfrage zu beschleunigen.

Upgrade von ESET PROTECT-Komponenten in Offlineumgebungen

Führen Sie die folgenden Schritte aus, um Ihre ESET PROTECT-Komponenten und ESET-Endpunktprodukte ohne Internetzugang zu aktualisieren:

Der [Task Komponenten-Upgrade](#) kann für eine Offline-Umgebung verwendet werden, wenn die folgenden Bedingungen erfüllt sind:

- Ein [Offline-Repository](#) ist verfügbar.
- Der Speicherort des Repositories für den ESET Management Agenten ist mit einer [Policy](#) auf einen erreichbaren Ort konfiguriert.

Führen Sie ein Upgrade für ESET PROTECT Server und Web-Konsole durch:

1. [Überprüfen Sie, welche Version von der ESET Management-Konsole](#) auf dem Server ausgeführt wird.
2. Laden Sie das neueste [All-in-One-Installationsprogramm für Windows](#) bzw. die neuesten [eigenständigen Installationsprogramme für ESET PROTECT-Komponenten für Linux](#) von der ESET-Downloadseite herunter.
3. Führen Sie ein Upgrade für ESET PROTECT Server und ESET PROTECT Web-Konsole durch:
 - Windows – [Upgrade mit dem All-in-One-Installationsprogramm](#)
 - Linux – [Manuelles komponentenbasiertes Upgrade](#)

Bei den Upgrades für die Web-Konsole und für Apache Tomcat wird die [Offlinehilfe](#) gelöscht. Falls Sie die Offlinehilfe mit ESMC oder einer älteren Version von ESET PROTECT verwendet haben, können Sie sie nach dem Upgrade für ESET PROTECT 9.1 erneut erstellen, um sicherzustellen, dass Sie die neueste Offline-Hilfe für Ihre Version von ESET PROTECT verwenden.

Führen Sie anschließend ein Offline-Upgrade der folgenden ESET-Endpunktprodukte durch

1. Anzeigen, welche ESET-Produkte auf den Clients installiert sind: Öffnen Sie die ESET PROTECT-Web-Konsole und navigieren Sie zu **Dashboard** > **ESET-Anwendungen**.
2. Stellen Sie sicher, dass Sie [die neuesten Versionen der ESET Endpoint-Produkte verwenden](#).
3. Laden Sie die Installationsprogramme von der [ESET-Downloadseite](#) in das lokale Repository herunter, das Sie bei der [Offline-Installation](#) konfiguriert haben.
4. Führen Sie einen [Task Software-Installation](#) über die ESET PROTECT-Web-Konsole aus.

Antworten auf gängige Probleme bei der Installation

Erweitern Sie den Bereich für die Fehlermeldung, die Sie beheben möchten:

Der ESET PROTECT Server-Dienst wird nicht gestartet:

Beschädigte Installation

- Mögliche Gründe hierfür sind fehlende Registrierungsschlüssel, fehlende Dateien oder ungültige Dateiberechtigungen.
- Das All-in-One-Installationsprogramm hat eine [eigene Logdatei](#). Verwenden Sie die [MSI-Loggingmethode](#), wenn Sie Komponenten manuell installieren.

Listening-Port bereits in Verwendung (hauptsächlich 2222 und 2223)

Führen Sie den entsprechenden Befehl für Ihr BS aus:

- Windows:

```
netstat -an | find "2222"  
netstat -an | find "2223"
```
- Linux:

```
netstat | grep 2222  
netstat | grep 2223
```

Datenbank wird nicht ausgeführt oder ist nicht erreichbar

- MS SQL Server: Stellen Sie sicher, dass Port 1433 auf dem Datenbankserver erreichbar ist oder versuchen Sie, sich mit SQL Server Management Studio anzumelden
- MySQL: Stellen Sie sicher, dass Port 3306 auf dem Datenbankserver erreichbar ist oder versuchen Sie, sich mit Ihrer Datenbankschnittstelle anzumelden (z. B. mit der MySQL-Befehlszeile oder `phpmyadmin`)

Beschädigte Datenbank

In diesem Fall enthält die ESET PROTECT Server-Logdatei mehrere SQL-Fehler. Stellen Sie Ihre Datenbank aus einer Sicherungskopie wieder her. Falls keine Sicherung vorhanden ist, installieren Sie ESET PROTECT neu.

Unzureichende Systemressourcen (Arbeitsspeicher, Festplattenplatz)

Überprüfen Sie die laufenden Prozesse und die Systemleistung:

- Windows-Benutzer: Öffnen Sie den Task-Manager oder die Ereignisanzeige und überprüfen Sie die angezeigten Informationen
- Linux-Benutzer: Führen Sie einen der folgenden Befehle aus:

```
df -h
```

 (um den freien Festplattenplatz zu überprüfen)

```
cat /proc/meminfo
```

 (um den Arbeitsspeicher zu überprüfen)

```
dmesg
```

 (um die Linux-Systemintegrität zu überprüfen)

Fehler im ODBC Connector bei der ESET PROTECT Server-Installation

```
Error: (Error 65533) ODBC connector compatibility check failed.  
Please install ODBC driver with support for multi-threading.
```

Installieren Sie eine Version des ODBC-Treibers, die Multithreading unterstützt oder konfigurieren Sie `odbcinst.ini`,

wie im Abschnitt zur [ODBC-Konfiguration](#) angegeben.

Fehler bei einer Datenbankverbindung während der Installation des ESET PROTECT Servers

Nach Abschluss der ESET PROTECT Server-Installation wird die folgende allgemeine Fehlermeldung angezeigt:

```
The database server is not configured correctly.  
Please check the documentation and reconfigure the database server as needed.
```

Fehlermeldung aus dem Installationslog:

```
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.
```

Überprüfen Sie, ob die Konfiguration Ihres Datenbanktreibers mit den Informationen im Abschnitt zur [ODBC-Konfiguration](#) übereinstimmt.

 [ESET Management Agent](#)

ESET Management Agent – Deinstallation und Fehlerbehandlung

- Analysieren Sie die [Logdateien](#) des ESET Management Agenten.
- Sie können den ESET Management Agenten mit dem [ESET-Deinstallationsprogramm](#) oder auf andere Arten entfernen (z. B. indem Sie die Dateien entfernen und den ESET Management Agenten-Dienst sowie die Registrierungseinträge löschen). Wenn auf dem Computer ein weiteres ESET-Endpunktprodukt vorhanden ist, wird dies durch einen [integrierten Selbstschutzmechanismus](#) verhindert.
- Die Nachricht "Aktualisierung der Datenbank ist fehlgeschlagen. Entfernen Sie das Produkt zunächst." wird bei der Deinstallation des Agenten angezeigt – Reparieren Sie den ESET Management Agenten:
 1. Klicken Sie auf **Systemsteuerung > Programme und Features** und doppelklicken Sie auf **ESET Management Agent**.
 2. Klicken Sie auf **Weiter > Reparieren** und folgen Sie den Anweisungen.

Alle Möglichkeiten zur Deinstallation des ESET Management Agenten sind im Bereich [Deinstallation](#) beschrieben.

Fehlercode 1603 bei der Installation des Agenten

Dieser Fehlercode kann auftreten, wenn sich das Installationsprogramm nicht auf dem lokalen Laufwerk befindet. Kopieren Sie das Installationsprogramm in das lokale Verzeichnis und führen Sie die Installation erneut aus, um diesen Fehler zu beheben. Führen Sie unsere [Anweisungen in der Knowledgebase](#) aus, falls das Programm bereits lokal gespeichert ist und der Fehler weiterhin auftritt.

Fehlermeldung bei der Installation des Agenten auf Linux

Fehlermeldung:

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

Eine mögliche Ursache für diesen Fehler ist ein falscher Dateiname im Installationsbefehl. Die Groß-/Kleinschreibung der Konsole muss beachtet werden. `Agent . pfx` ist nicht dasselbe wie `agent . pfx`.

Fehler bei der Remote-Bereitstellung von Linux auf Windows 8.1 (32 Bit)

Dies ist ein Authentifizierungsproblem, das von Microsofts KB3161949 verursacht wurde. Sie können dieses Problem beheben, indem Sie dieses Update auf den Hosts entfernen, auf denen die Bereitstellung fehlgeschlagen ist.

Der ESET Management Agent kann sich nicht mit dem Server ESET PROTECT verbinden

Weitere Informationen finden Sie in unter [Fehlerbehebung – Agenten-Verbindung](#) und in unserem [Knowledgebase-Artikel](#).

Das Installationskript für Agenten wurde mit dem Code 30 beendet

Sie verwenden das Installationskript für Agenten mit einem benutzerdefinierten Speicherort und haben das Skript nicht korrekt bearbeitet. Lesen Sie die [Hilfeseite](#) und versuchen Sie es erneut.

[Web-Konsole](#)

 [Apache HTTP-Proxy](#)

Der Apache HTTP Proxy-Cache ist mehrere GB groß und wächst immer weiter

Falls Sie den Apache HTTP Proxy mit dem All-in-One-Installationsprogramm installiert haben, ist die Bereinigungsfunktion automatisch aktiviert. Falls die Bereinigung nicht korrekt funktioniert, [führen Sie eine manuelle Bereinigung durch oder planen Sie einen Bereinigungs-Task](#).

Nach der Installation von Apache HTTP Proxy wird die Erkennungsroutine nicht mehr aktualisiert

Falls die Client-Arbeitsplatzrechner keine Updates erhalten, finden Sie in unserer Knowledgebase Anweisungen dazu, wie Sie [Apache HTTP Proxy auf Endpunkt-Arbeitsplatzrechnern](#) vorübergehend deaktivieren können. Nachdem Sie die Verbindungsprobleme behoben haben, sollten Sie den Apache HTTP Proxy erneut aktivieren.

Fehlercode 20008 beim Remote-Update des ESET Management Agenten

Falls beim Remote-Update des ESET Management Agenten die folgende Fehlermeldung angezeigt wird:

GetFile: Failed to process the HTTP request (error code 20008, url: 'http://repository.eset.com/v1//info.meta')

[Führen Sie die Schritte I - III in diesem Artikel aus](#), um das Verbindungsproblem zu beheben. Falls sich der Computer, auf dem der ESET Management Agent aktualisiert werden soll, nicht in Ihrem Firmennetzwerk befindet, konfigurieren Sie eine Policy für den ESET Management Agenten, sodass dieser keinen Proxy für die Verbindung zum Repository verwendet, wenn er sich außerhalb des Firmennetzwerks befindet.

 [ESET Rogue Detector Sensor](#)

Warum taucht die folgende Fehlermeldung immer wieder in der trace.log-Datei von ESET Rogue Detection auf?

```
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)
```

Dabei handelt es sich um ein WinPcap-Problem. Halten Sie den ESET Rogue Detector Sensor-Dienst an, installieren Sie die neueste WinPcap-Version (mindestens 4.1.0) und starten Sie den ESET Rogue Detector Sensor-Dienst neu.

 [Linux](#)

Fehlende libQtWebKit-Abhängigkeit unter CentOS-Linux

Die folgende Fehlermeldung wird angezeigt:

```
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]
```

Führen Sie die Anweisungen in unserem [KnowledgeBase-Artikel](#) aus.

Fehler bei der Installation von ESET PROTECT unter CentOS 7

Die folgende Fehlermeldung wird angezeigt:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

Die Ursache liegt vermutlich in den Umgebungs- oder Gebietseinstellungen. Führen Sie den folgenden Befehl aus, bevor Sie das Installer-Skript ausführen:

export LC_ALL="en_US.UTF-8"



Fehlercode -2068052081 bei der Installation von Microsoft SQL Server.

Starten Sie Ihren Computer neu und führen Sie die Einrichtung erneut aus. Deinstallieren Sie bei Fortbestehen des Problems SQL Server Native Client und wiederholen Sie die Installation. Wenn das Problem damit nicht behoben wird, deinstallieren Sie alle Microsoft SQL Server-Produkte, starten Sie Ihren Computer neu und wiederholen Sie die Installation.

Fehlercode -2067922943 bei der Installation von Microsoft SQL Server.

Stellen Sie sicher, dass Ihr System die [Datenbankanforderungen](#) für ESET PROTECT erfüllt.

Fehlercode -2067922934 bei der Installation von Microsoft SQL Server.

Stellen Sie sicher, dass Ihr [Benutzerkonto die richtigen Berechtigungen](#) hat.

In der Web-Konsole wird „Fehler beim Laden der Daten“ angezeigt.

MS SQL Server versucht, möglichst viel Festplattenplatz für Transaktions-Logs zu nutzen. Auf der [offiziellen Microsoft-Webseite](#) finden Sie Hinweise zur Bereinigung dieser Logs.

Fehlercode -2067919934 bei der Installation von Microsoft SQL Server.

Vergewissern Sie sich, dass alle vorigen Schritte erfolgreich abgeschlossen wurden. Dieser Fehler wird durch falsch konfigurierte Systemdateien verursacht. Starten Sie den Computer neu und führen Sie die Installation erneut aus.

Log-Dateien

Jede ESET PROTECT-Komponente erstellt Logs. Die ESET PROTECT-Komponenten schreiben Informationen zu bestimmten Ereignissen in die Log-Dateien. Der Speicherort der Log-Dateien hängt von der jeweiligen Komponente ab. Hier finden Sie eine Liste der Speicherorte von Log-Dateien:

Windows

ESET PROTECT Komponente	Speicherort der Log-Dateien
ESET PROTECT Server	<i>C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\</i>
ESET Management Agent	<i>C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\</i> Siehe auch Fehlerbehebung bei der Agentenverbindung .

ESET PROTECT Komponente	Speicherort der Log-Dateien
ESET PROTECT-Web-Konsole und Apache Tomcat	<i>C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs\</i> Siehe auch https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Mobile Device Connector	<i>C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs\</i> Siehe auch MDM-Fehlerbehebung .
Rogue Detection Sensor	<i>C:\ProgramData\ESET\Rogue Detection Sensor\Logs\</i>
Apache HTTP-Proxy	<i>C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs\</i> <i>C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs\errorlog</i>

- i** *C:\ProgramData* ist standardmäßig ausgeblendet. Um den Ordner anzuzeigen:
1. Navigieren Sie zu **Start > Systemsteuerung > Ordneroptionen > Ansicht**.
 2. Wählen Sie **Ausgeblendete Dateien, Ordner und Laufwerke anzeigen** aus und klicken Sie auf **OK**.

Linux

ESET PROTECT Komponente	Speicherort der Log-Dateien
ESET PROTECT Server	<i>/var/log/eset/RemoteAdministrator/Server/</i> <i>/var/log/eset/RemoteAdministrator/EraServerInstaller.log</i>
ESET Management Agent	<i>/var/log/eset/RemoteAdministrator/Agent/</i> <i>/var/log/eset/RemoteAdministrator/EraAgentInstaller.log</i>
Mobile Device Connector	<i>/var/log/eset/RemoteAdministrator/MDMCore/</i> <i>/var/log/eset/RemoteAdministrator/MDMCore/Proxy/</i> Siehe auch MDM-Fehlerbehebung .
Apache HTTP-Proxy	<i>/var/log/httpd/</i>
ESET PROTECT-Web-Konsole und Apache Tomcat	<i>/var/log/tomcat/</i> Siehe auch https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	<i>/var/log/eset/RogueDetectionSensor/</i>

Virtuelle ESET PROTECT-Appliance

ESET PROTECT Komponente	Speicherort der Log-Dateien
Konfiguration der ESET PROTECT-VA	<i>/root/appliance-configuration-log.txt</i>
ESET PROTECT Server	<i>/var/log/eset/RemoteAdministrator/EraServerInstaller.log</i>
Apache HTTP-Proxy	<i>/var/log/httpd</i>

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

Diagnose-Tool

Das Diagnose-Tool ist in allen ESET PROTECT-Komponenten enthalten. Es dient zum Erfassen und Erstellen von Logs, die technischen Supportmitarbeitern und Entwicklern zur Behebung von Problemen mit den Produktkomponenten verwendet werden.

Diagnose-Tool – Speicherort

Windows

Ordner `C:\Program Files\ESET\RemoteAdministrator\<product>\Diagnostic.exe`.

Linux

Im Verzeichnis `/opt/eset/RemoteAdministrator/<product>/` auf dem Server befindet sich eine ausführbare Datei **Diagnostic<product>** (ein Wort, z. B. **DiagnosticServer**, **DiagnosticAgent**)

Verwendung (Linux)

Führen Sie das Diagnoseprogramm im Terminal als root aus und folgen Sie den Anweisungen auf dem Bildschirm.

Verwendung (Windows)

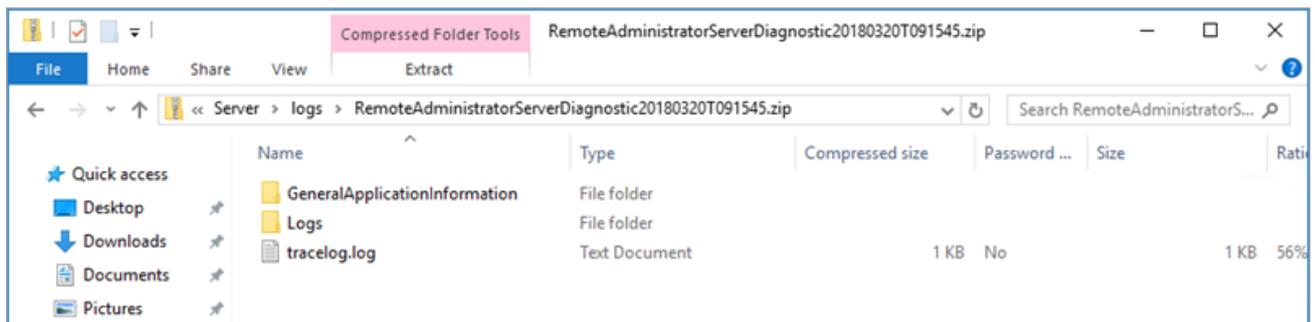
1. Starten Sie das Tool aus einer Eingabeaufforderung heraus.
2. Geben Sie den gewünschten Speicherort für die Logdateien ein ("logs" in unserem Beispiel) und drücken Sie die **Eingabetaste**.
3. Geben Sie die Informationen ein, die Sie sammeln möchten (`1 trace status 3` in unserem Beispiel). Weitere Informationen finden Sie in diesem Dokument unter **Aktionen**.

```

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. Anschließend finden Sie die Logdateien komprimiert in einer *.zip*-Datei im Verzeichnis „logs“ im Speicherort des Diagnose-Tools.



Aktionen

- **ActionEraLogs**– Ein Log-Ordner zum Speichern der Logs wird erstellt. Trennen Sie die einzelnen Logs mit einem Leerzeichen, um nur bestimmte Logs auszuwählen.
- **ActionGetDumps**– Ein neuer Ordner wird erstellt. Eine Prozesssicherungsdatei wird üblicherweise erstellt, wenn ein Problem erkannt wurde. Im Falle eines schwerwiegenden Problems erstellt das System eine Dumpdatei. Sie können dies manuell überprüfen, indem Sie im Ordner %temp% (Windows) bzw. /tmp/ (Linux) eine DMP-Datei einfügen.

i Der Komponentendienst (Agent, , Server, RD Sensor,) muss ausgeführt werden.

- **ActionGeneralApplicationInformation**– Der Ordner GeneralApplicationInformation und die enthaltene Datei *GeneralApplicationInformation.txt* werden erstellt. Diese Datei enthält Textinformationen wie den Produktnamen und die Produktversion des aktuell installierten Produkts.
- **ActionConfiguration** – Ein Konfigurationsordner wird erstellt, in dem die Datei storage.lua gespeichert wird.

Probleme nach Upgrade oder Migration von ESET PROTECT Server

Wenn Sie den ESET PROTECT Server-Dienst aufgrund einer beschädigten Installation nicht mehr starten können und in den Logs unbekannte Fehlermeldungen auftauchen, können Sie mit den folgenden Schritten einen Reparaturvorgang ausführen:

 Legen Sie unbedingt eine [Sicherung Ihres Datenbankservers](#) an, bevor Sie mit dem Reparaturvorgang beginnen.

1. Navigieren Sie zu **Start > Systemsteuerung > Programm und Features** und doppelklicken Sie auf **ESET PROTECT Server**.
2. Wählen Sie **Reparieren** aus und klicken Sie auf **Weiter**.
3. Verwenden Sie die vorhandenen Einstellungen für die Datenbankverbindung und klicken Sie auf **Weiter**. Klicken Sie auf **Ja, wenn Sie zu einer Bestätigung aufgefordert werden**. Sie finden die Datenbankverbindungsinformationen unter:
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
4. Wählen Sie **Benutzerpasswort ist bereits in der Datenbank gespeichert** aus und klicken Sie auf **Weiter**.
5. Wählen Sie **Aktuell verwendete Zertifikate behalten** aus und klicken Sie auf **Weiter**.
6. Aktivieren Sie den ESET PROTECT Server mit einem gültigen Lizenzschlüssel oder wählen Sie **Später aktivieren** aus (weitere Hinweise finden Sie unter [Lizenzverwaltung](#)) und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Reparieren**.
8. [Verbinden Sie sich erneut mit der Web-Konsole](#) und überprüfen Sie, ob das Problem behoben wurde.

Weitere Fehlerbehebungsszenarien:

ESET PROTECT Server lässt sich nicht starten, aber ich habe eine Datenbanksicherung:

1. Stellen Sie Ihre [Datenbanksicherung](#) wieder her.
2. Der neue Computer muss dieselbe IP-Adresse bzw. denselben Hostnamen wie Ihre vorherige Installation verwenden, um sicherzustellen, dass sich die Agenten verbinden können.
3. Reparieren Sie ESET PROTECT Server und verwenden Sie die wiederhergestellte Datenbank.

ESET PROTECT Server lässt sich nicht starten, aber Sie haben das

exportierte Serverzertifikat und die Zertifizierungsstelle von Ihrem Server:

1. Der neue Computer muss dieselbe IP-Adresse bzw. denselben Hostnamen wie Ihre vorherige Installation verwenden, um sicherzustellen, dass sich die Agenten verbinden können.
2. Reparieren Sie ESET PROTECT mit den gesicherten Zertifikaten (wählen Sie bei der Reparatur **Zertifikate aus Datei laden** aus und folgen Sie den Anweisungen).

ESET PROTECT Server lässt sich nicht starten, und Sie haben weder Datenbanksicherung noch ein ESET PROTECT Server-Zertifikat oder eine Zertifizierungsstelle:

1. Reparieren Sie den ESET PROTECT Server.
2. Reparieren Sie die ESET Management Agenten auf eine der folgenden Arten:
 - Installations-Skript für Agenten
 - Remote-Bereitstellung (in diesem Fall müssen Sie die Firewall auf den Zielcomputern deaktivieren)
 - Manuelles Installationsprogramm für die Agenten-Komponente

MSI-Logging

Dies ist hilfreich, wenn bei der Installation einer ESET PROTECT-Komponente unter Windows Fehler auftreten, z. B. ESET Management Agent:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT API

Die ServerApi von ESET PROTECT (*ServerApi.dll*) ist eine Programmierungsschnittstelle und enthält Funktionen und Tools, mit denen Sie eigene Anwendungen nach Ihren Anforderungen entwickeln können. Die ServerApi stellt Schnittstellen, Funktionen und Operationen für Ihre Anwendung bereit, die Sie normalerweise in der ESET PROTECT-Web-Konsole ausführen würden, z. B. die Verwaltung von ESET PROTECT, Erstellung und Versand von Berichten usw.

Weitere Informationen und Beispiele in der C-Programmiersprache sowie eine Liste der verfügbaren JSON-Nachrichten finden Sie in der Onlinehilfe:

[ESET PROTECT 9 API](#)

Häufig gestellte Fragen (FAQ)

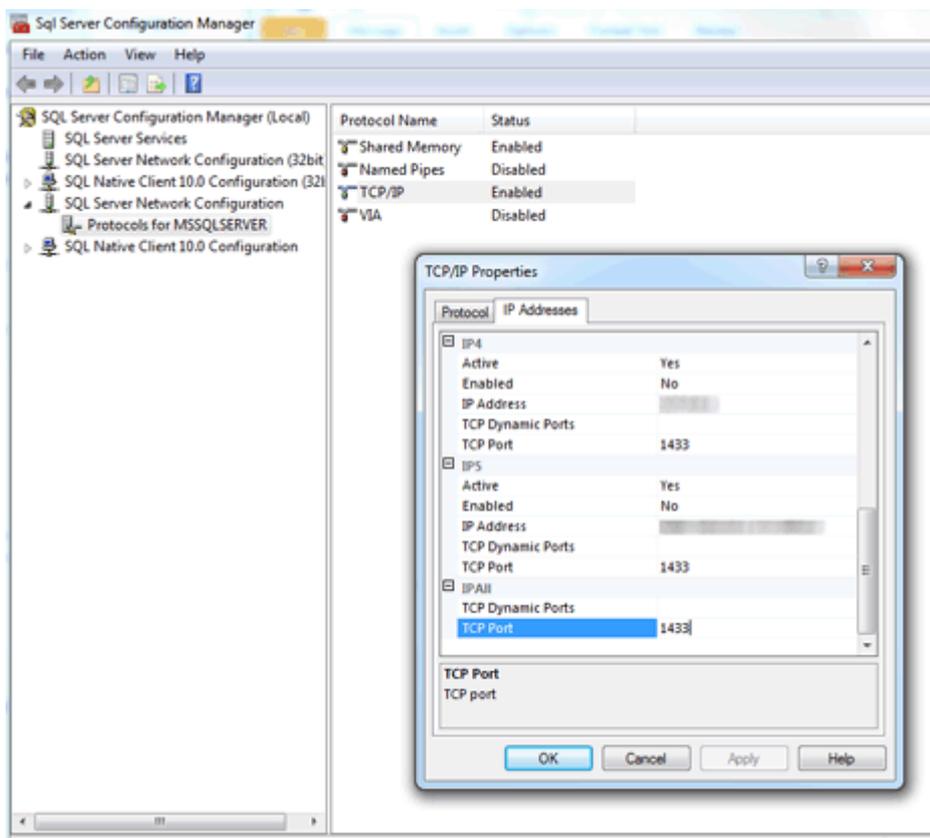
Warum wird Java auf einem Server installiert? Stellt das nicht ein Sicherheitsrisiko dar? Ein Großteil aller Sicherheitsunternehmen und Sicherheits-Frameworks warnen vor der Installation von Java auf Computern, insbesondere auf Servern.

Die ESET PROTECT-Web-Konsole benötigt Java/OpenJDK. Java ist ein Branchenstandard für webbasierte Konsolen, und alle wichtigen Web-Konsolen verwenden Java und einen Webserver (Apache Tomcat). Java wird für die Unterstützung unseres plattformübergreifenden Webserver benötigt. Falls Sie Sicherheitsbedenken haben, können Sie den Webserver auf einem separaten Computer installieren.

! Ab Januar 2019 ist für die öffentlichen Updates für Oracle JAVA SE 8 für kommerzielle, geschäftliche oder Produktionszwecke eine kommerzielle Lizenz erforderlich. Falls Sie kein JAVA SE-Abonnement gekauft haben, finden Sie Hinweise für den Wechsel zu einer kostenfreien Alternative in dieser Anleitung. Siehe [unterstützte Versionen von JDK](#).

Wie kann ich herausfinden, welchen Port SQL Server verwendet?

Es gibt mehrere Möglichkeiten, um den von SQL Server verwendeten Port zu ermitteln. Das exakteste Ergebnis erhalten Sie im SQL Server-Konfigurations-Manager. Im folgenden Beispiel sehen Sie, wo Sie diese Informationen im SQL-Konfigurationsmanager finden:



Nach der Installation von SQL Server Express (im ESET PROTECT-Paket enthalten) auf Windows Server 2012 scheint SQL Express einen nicht-standardmäßigen SQL-Port zu verwenden. Die Datenbank verwendet vermutlich einen anderen Port als den Standardport 1433.

Wie konfiguriere ich MySQL so, dass es große Pakete akzeptiert?

Siehe MySQL-Installation und -Konfiguration für [Windows](#) oder [Linux](#).

Wenn ich SQL selbst installiere: Wie erstelle ich eine Datenbank für ESET PROTECT?

Das ist nicht erforderlich. Die Datenbank wird vom *Server.msi* Installationsprogramm erstellt, nicht vom ESET PROTECT Installationsprogramm. Das ESET PROTECT-Installationsprogramm vereinfacht bestimmte Schritte für Sie und installiert den SQL Server. Die Datenbank wird anschließend vom Installationsprogramm *Server.msi* erstellt.

Kann das ESET PROTECT-Installationsprogramm eine neue Datenbank in einer vorhandenen MS SQL Server-Installation erstellen, wenn ich die richtigen Verbindungsinformationen und Anmeldedaten für MS SQL Server angebe? Es wäre hilfreich, wenn das Installationsprogramm verschiedene Versionen von SQL Server (2014, 2019 usw.) unterstützen würde.

Die Datenbank wird von *Server.msi* erstellt. Ja, das Installationsprogramm kann eine ESET PROTECT-Datenbank für Sie in einer individuell installierten SQL Server-Instanz erstellen. MS SQL Server wird ab Version 2014 unterstützt.

ESET PROTECT 9.1 [All-in-One-Installationsprogramm](#) installiert standardmäßig Microsoft SQL Server Express 2019.

o Falls Sie eine ältere Windows Edition verwenden (Server 2012 oder SBS 2011), wird standardmäßig Microsoft SQL Server Express 2014 installiert.

o Das Installationsprogramm generiert automatisch ein zufälliges Passwort für die Datenbankauthentifizierung (gespeichert in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`).

Microsoft SQL Server Express Hat eine Obergrenze von je 10 GB für relationale Datenbanken. Microsoft SQL Server Express sollte nicht verwendet werden:



- In Unternehmensumgebungen oder großen Netzwerken.
- Falls Sie ESET PROTECT mit [ESET Inspect](#) verwenden möchten.

Sollte bei der Installation in einem vorhandenen SQL Server standardmäßig der integrierte Windows-Authentifizierungsmodus verwendet werden?

Nein. Der Windows-Authentifizierungsmodus kann in SQL Server deaktiviert werden. Die einzige Möglichkeit zur Anmeldung ist die SQL Server-Authentifizierung (Eingabe von Benutzername und Passwort). Bei der Installation von ESET PROTECT Server ist die gemischte Authentifizierung (SQL Server-Authentifizierung und Windows-Authentifizierung) erforderlich. Wenn Sie SQL Server manuell installieren, sollten Sie ein Root-Passwort erstellen (der Root-Benutzer ist „sa“ für „Sicherheitsadministrator“) und zur späteren Verwendung an einem sicheren Ort aufbewahren. Das Root-Passwort wird evtl. für spätere Upgrades des ESET PROTECT Servers benötigt. Sie können die [Windows-Authentifizierung](#) auswählen, nachdem Sie den ESET PROTECT Server installiert haben.

Kann ich MariaDB anstelle von MySQL einsetzen?

Nein, MariaDB wird nicht unterstützt. Achten Sie darauf, [unterstützte Versionen von MySQL Server und ODBC Connector](#) zu installieren. Siehe [MySQL – Installation und Konfiguration](#).

Das ESET PROTECT Installationsprogramm hat mich dazu aufgefordert, Microsoft .NET Framework 4 zu installieren (<http://www.microsoft.com/de-de/download/details.aspx?id=17851>), aber dabei ist auf einer frischen Installation von Windows Server 2012 R2 mit SP1 ein Fehler aufgetreten.

Das Installationsprogramm kann aufgrund der Windows Server 2012-Sicherheitsrichtlinie nicht unter Windows Server 2012 verwendet werden. Microsoft .NET Framework muss mit dem **Assistenten zum Hinzufügen von Rollen und Features** installiert werden.

Es ist nicht erkennbar, ob die SQL Server-Installation tatsächlich ausgeführt wird. Liegt ein Problem vor, wenn die Installation länger als 10 Minuten dauert?

Die SQL Server-Installation kann in seltenen Fällen bis zu 1 Stunde dauern. Die Installationsdauer hängt von der Systemleistung ab.

Wie kann ich das bei der Einrichtung für die Web-Konsole eingegebene Administratorpasswort zurücksetzen?

Sie können das Passwort zurücksetzen, indem Sie das Serverinstallationsprogramm ausführen und die Option **Reparieren** auswählen. Sie benötigen dabei jedoch evtl. das Passwort für die ESET PROTECT-Datenbank, falls Sie bei der Erstellung der Datenbank keine Windows-Authentifizierung verwendet haben.



- Verwenden Sie diese Funktion mit Bedacht, da manche Reparaturoptionen gespeicherte Daten entfernen können.
- Beim Passwort-Reset wird [2FA](#) zurückgesetzt.

Welches Dateiformat wird für den Import einer Liste von Computern benötigt, die zu ESET PROTECT hinzugefügt werden sollen?

In den folgenden Zeilen sehen Sie das Format:

All\Group1\GroupN\Computer1

All\Group1\GroupM\ComputerX

„All“ ist der erforderliche Name der Stammgruppe.

Kann IIS anstelle von Apache verwendet werden? Können andere HTTP-Server eingesetzt werden?

IIS ist ein HTTP-Server. Die Web-Konsole benötigt einen Java-Servletcontainer (z. B. Tomcat), ein HTTP-Server reicht nicht aus. IIS kann zwar in einen Java-Servletcontainer konvertiert werden, dies wird jedoch im Allgemeinen nicht unterstützt.



Apache HTTP-Server und Apache Tomcat sind zwei unterschiedliche Produkte. Wir verwenden Apache Tomcat.

Gibt es in ESET PROTECT eine Befehlszeilenschnittstelle?

Ja, dafür haben wir unsere ESET PROTECT [ServerApi](#).

Kann ESET PROTECT auf einem Domänencontroller installiert werden?

[Installieren Sie SQL Server sollte nicht auf einem Domänencontroller](#) (z. B. Windows SBS oder Essentials). Sollten Sie ESET PROTECT auf einem anderen Server installieren oder während der Installation nicht die SQL Server Express-Komponente auswählen (in diesem Fall müssen Sie SQL Server oder MySQL als ESET PROTECT-Datenbank verwenden).

Erkennt der ESET PROTECT Server bei der Installation bereits vorhandene SQL-Instanzen? Was geschieht in diesem Fall? Was ist mit MySQL?

ESET PROTECT sucht nach vorhandenen SQL-Instanzen auf dem System, falls Sie den Installations-Assistenten verwenden und SQL Express für die Installation ausgewählt haben. Falls bereits eine SQL-Instanz auf dem System vorhanden ist, fragt der Assistent nach, ob die vorhandene SQL-Instanz deinstalliert und die Installation wiederholt oder ob ESET PROTECT ohne SQL Express installiert werden soll. Siehe [Datenbankanforderungen](#) für ESET PROTECT.

Wo finde ich eine ESET PROTECT-Komponentenübersicht für einzelne Versionen?

Lesen Sie unseren [Knowledgebase-Artikel](#).

Wie kann ich ein Upgrade von ESET PROTECT auf die aktuelle Version durchführen?

Siehe [Upgradeprozeduren](#).

Wie kann ich Systeme ohne Internetverbindung aktualisieren?

Sie können einen HTTP Proxy auf einem Computer installieren, der sich mit den ESET-Updateservern verbinden kann (auf denen die Update-dateien liegen) und die Endpunkte auf diesen HTTP Proxy im lokalen Netzwerk verweisen. Falls Ihr Server nicht mit dem Internet verbunden ist, können Sie die Mirror-Funktion im Endpoint-Produkt auf einem Computer aktivieren und Updates per USB-Laufwerk auf diesen Computer aufspielen. Alle weiteren Offlinecomputer können diesen Computer anschließend als Updateserver nutzen.

[Folgen Sie diesen Anweisungen](#) für weitere Details zur Offlineinstallation.

Wie kann ich meinen ESET PROTECT Server neu installieren und mit einem vorhandenen SQL Server verbinden, der bei der ersten ESET PROTECT Installation?

Wenn Sie die neue ESET PROTECT Server-Instanz unter demselben Benutzerkonto installieren (z. B. ein Domänenadministrator-Benutzerkonto), unter dem Sie die erste ESET PROTECT Server-Installation ausgeführt haben, können Sie die Option **MS SQL Server mit Windows-Authentifizierung** verwenden.

Was kann ich bei Problemen mit der Active Directory-Synchronisierung unter Linux tun?

Überprüfen Sie, ob Ihr Domänenname komplett in Großbuchstaben angegeben ist (administrator@TEST.LOCAL anstelle von administrator@test.local).

Kann ich meine eigene Netzwerkressource (z. B. eine SMB-Freigabe) anstelle des Repositorys verwenden?

Sie können die URL für den Direktzugriff eingeben, unter der sich ein Paket befindet. Verwenden Sie für Dateifreigaben das folgende Format: „file:///“ gefolgt vom vollständigen Netzwerkpfad der Datei, z. B.:

file://\eraserver\install\ees_nt64_ENU.msi

Wie kann ich mein Passwort zurücksetzen oder ändern?

Im Idealfall sollte das Administratorkonto nur zum Erstellen von Konten für einzelne Benutzer mit Administratorrechten verwendet werden. Nachdem diese [Administratorkonten](#) erstellt wurden, sollte das Administratorpasswort sicher aufbewahrt und das Administratorkonto nicht verwendet werden. Auf diese Weise kann das Administratorkonto dazu verwendet werden, bei Bedarf die Passwörter/Kontodetails zurückzusetzen.

So können Sie das Passwort eines integrierten ESET PROTECT-Administratorkontos zurücksetzen:

1. Öffnen Sie **Programme und Funktionen** (führen Sie appwiz.cpl aus), suchen Sie den ESET PROTECT Server und klicken Sie ihn mit der rechten Maustaste an.
2. Wählen Sie im Kontextmenü **Ändern** aus.
3. Klicken Sie auf **Reparieren**.
4. Geben Sie die Datenbankverbindungsdetails ein.
5. Wählen Sie **Bestehende Datenbank verwenden und Upgrade ausführen** aus.
6. Deaktivieren Sie die Option **Benutzerpasswort ist bereits in der Datenbank gespeichert** und geben Sie ein neues Passwort ein.
7. Melden Sie sich mit Ihrem neuen Passwort bei der ESET PROTECT-Web-Konsole an.



Wir empfehlen dringend, zusätzliche Konten mit eingeschränkten Zugriffsrechten zu erstellen, die den erforderlichen Berechtigungen entsprechen.

Wie kann ich die Ports für den ESET PROTECT Server und die ESET PROTECT-Web-Konsole ändern?

Sie müssen den Port in der Konfiguration Ihrer Webserver ändern, um Verbindungen zum neuen Port zu ermöglichen. Führen Sie dazu die folgenden Schritte aus:

1. Halten Sie Ihren Webserver an.
 2. Ändern Sie den Port in der Konfiguration Ihres Webserver.
 - a) Öffnen Sie die Datei `webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties`
 - b) Geben Sie die neue Portnummer ein (z. B. `server_port=44591`)
 3. Starten Sie den Webserver neu.
-

Kann ich mit dem All-in-One-Installationsprogramm ein Direkt-Upgrade von ERA 5 oder 6 auf ESET PROTECT 9 ausführen?

Direkt-Upgrades werden nicht unterstützt, siehe [Migration von ERA 5.x](#) oder [Upgrade von ERA 6.x](#).

Ich erhalte Fehlermeldungen oder habe Probleme mit ESET PROTECT, was kann ich tun?

Lesen Sie unsere [Fehlerbehebungs-FAQs](#).

Endbenutzer-Lizenzvereinbarung

Gültig ab dem 19. Oktober 2021.

WICHTIG: Vor dem Herunterladen, Installieren, Kopieren oder Verwenden des Produkts lesen Sie bitte die folgenden Nutzungsbedingungen. **DURCH DAS HERUNTERLADEN, INSTALLIEREN, KOPIEREN ODER VERWENDEN DER SOFTWARE ERKLÄREN SIE SICH MIT DEN NUTZUNGSBEDINGUNGEN EINVERSTANDEN UND ERKENNEN DIE [DATENSCHUTZERKLÄRUNG AN](#).**

Endbenutzer-Lizenzvereinbarung

Diese Endbenutzer-Lizenzvereinbarung (die "Vereinbarung") zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 85101 Bratislava, Slovak Republic, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31333532, ("ESET" oder "Anbieter") und Ihnen, einer natürlichen oder juristischen Person ("Sie" oder der "Endbenutzer"), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

DIESES DOKUMENT IST KEIN KAUFVERTRAG, SONDERN EINE VEREINBARUNG ÜBER DIE RECHTE DES ENDBENUTZERS. Der Anbieter bleibt Eigentümer des Exemplars der Software und, soweit vorhanden, des physischen Mediums, auf dem die Software für den Verkauf vorliegt, sowie aller Kopien der Software, zu deren Erstellung der Endbenutzer unter den Bedingungen dieser Vereinbarung berechtigt ist.

Durch Klicken auf die Schaltfläche „Ich stimme zu“ oder „Ich stimme zu...“ beim Installieren, Herunterladen, Kopieren oder Verwenden der Software erklären Sie sich mit den Bestimmungen und Bedingungen dieser Vereinbarung einverstanden und akzeptieren die Datenschutzerklärung. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung und/oder der Datenschutzerklärung nicht einverstanden sind, klicken Sie auf die Schaltfläche „Ablehnen“ oder „Ich stimme nicht zu“. Brechen Sie den Download oder die Installation der Software ab, vernichten oder geben Sie die Software, das Installationsmedium, die zugehörige Dokumentation und den Erwerbsnachweis an den Anbieter oder an dem Ort, an dem Sie die Software erworben haben, zurück.

MIT DER NUTZUNG DER SOFTWARE ZEIGEN SIE AN, DASS SIE DIESE VEREINBARUNG GELESEN UND VERSTANDEN HABEN UND DASS SIE DIESER VEREINBARUNG ZUGESTIMMT HABEN.

1. Software. Mit "Software" wird in dieser Vereinbarung bezeichnet: (i) das mit dieser Vereinbarung ausgelieferte Computerprogramm und all dessen Komponenten; (ii) alle Inhalte der Disks, CD-ROMs, DVDs, E-Mails und Anlagen oder sonstiger Medien, denen diese Vereinbarung beigelegt ist, einschließlich der Objektcodeform der Software, die auf einem Datenträger, in einer E-Mail oder durch Herunterladen im Internet bereitgestellt wurde; (iii) alle verwandten erklärenden Schriftdokumente und andere Dokumentationen in Bezug auf die Software, insbesondere Beschreibungen der Software und ihrer Spezifikationen, jede Beschreibung der Softwareeigenschaften oder -funktionen, Beschreibungen der Betriebsumgebung, in der die Software verwendet wird, Anweisungen zu Installation und zum Einsatz der Software ("Dokumentation"); (iv) Kopien der Software, Patches für mögliche Softwarefehler, Hinzufügungen zur Software, Erweiterungen der Software, geänderte Versionen und Aktualisierungen der Softwarebestandteile, sofern zutreffend, deren Nutzung der Anbieter gemäß Artikel 3 dieser Vereinbarung gewährt. Die Software wird ausschließlich in Form von ausführbarem Objektcode ausgeliefert.

2. Installation, Computer und ein Lizenzschlüssel. Die auf einem Datenträger bereitgestellte, per E-Mail verschickte, aus dem Internet oder von den Servern des Anbieters heruntergeladene oder auf anderem Weg beschaffte Software muss installiert werden. Sie müssen die Software auf einem korrekt konfigurierten Computer installieren, der die in der Dokumentation genannten Mindestvoraussetzungen erfüllt. Die Installationsmethode ist in der Dokumentation beschrieben. Auf dem Computer, auf dem Sie die Software installieren, darf kein Computerprogramm und keine Hardware vorhanden sein, die sich negativ auf die Software auswirken könnte. Die Bezeichnung "Computer" erstreckt sich auf Hardware inklusive, jedoch nicht ausschließlich, Personal Computer, Laptops, Arbeitsstationen, Palmtop-Computer, Smartphones, tragbare elektronische Geräte oder andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder eingesetzt wird. Der Begriff "Lizenzschlüssel" bezeichnet die eindeutige Abfolge von Symbolen, Buchstaben und Zahlen, die dem Endbenutzer bereitgestellt wird, um die legale Nutzung der Software in der jeweiligen Version bzw. die Verlängerung der Lizenz gemäß dieser Vereinbarung zu ermöglichen.

3. Lizenz. Unter der Voraussetzung, dass Sie sich mit dieser Vereinbarung einverstanden erklärt haben und sämtliche darin enthaltenen Bestimmungen einhalten, gewährt Ihnen der Anbieter die folgenden Rechte (die "Lizenz"):

a) **Installation und Nutzung.** Sie erhalten das nicht exklusive und nicht übertragbare Recht, die Software auf der Festplatte eines Computers oder einem ähnlichen Medium zur dauerhaften Datenspeicherung zu installieren, die Software im Arbeitsspeicher eines Computers zu speichern und die Software auf Computern zu implementieren, zu speichern und anzuzeigen.

b) **Anzahl der Lizenzen.** Das Nutzungsrecht für die Software ist durch die Anzahl der Endbenutzer beschränkt. Unter einem „Endbenutzer“ ist Folgendes zu verstehen: (i) die Installation der Software auf einem Computer; oder (ii) wenn sich der Umfang einer Lizenz nach der Anzahl von Postfächern richtet, ist ein Endbenutzer ein Computerbenutzer, der E-Mails über ein E-Mail-Programm empfängt. Wenn das E-Mail-Programm E-Mail empfängt und diese anschließend automatisch an mehrere Benutzer weiterleitet, richtet sich die Anzahl der Endbenutzer nach der tatsächlichen Anzahl von Benutzern, an die auf diesem Weg E-Mail-Nachrichten gesendet

werden. Wenn ein Mailserver die Funktion eines E-Mail-Gateways ausführt, entspricht die Zahl der Endbenutzer der Anzahl von Mailservern, für die dieses Gateway Dienste bereitstellt. Wenn mehrere E-Mail-Adressen (z. B. durch Aliasnamen) von einem Benutzer verwendet werden und nur ein Benutzer über diese Adressen E-Mail empfängt, während auf Clientseite keine E-Mail-Nachrichten automatisch an mehrere Benutzer verteilt werden, ist nur eine Lizenz für einen Computer erforderlich. Die gleichzeitige Nutzung derselben Lizenz auf mehreren Computern ist untersagt. Der Endbenutzer darf den Lizenzschlüssel für die Software nur in dem Umfang eingeben, für den er die entsprechende Anzahl von Lizenzen zur Nutzung der Software vom Anbieter erworben hat. Der Lizenzschlüssel ist vertraulich, und die Lizenz darf nicht mit Drittparteien geteilt oder von Drittparteien genutzt werden, sofern dies nicht in dieser Vereinbarung oder vom Anbieter erlaubt wurde. Benachrichtigen Sie den Anbieter unverzüglich, falls Ihr Lizenzschlüssel kompromittiert wurde.

c) **Home/Business Edition.** Die Home Edition der Software darf ausschließlich in privaten und/oder nichtkommerziellen Umgebungen für den Haus- und Familiengebrauch eingesetzt werden. Für die Verwendung der Software in kommerziellen Umgebungen sowie auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

d) **Laufzeit der Lizenz.** Ihr Nutzungsrecht für die Software ist zeitlich beschränkt.

e) **OEM-Software.** Als „OEM“ klassifizierte Software darf ausschließlich auf dem Computer genutzt werden, mit dem sie ausgeliefert wurde. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

f) **Nicht für den Wiederverkauf bestimmte Software und Testversionen.** Nicht für den Wiederverkauf („not for resale“, NFR) oder als Testversion bereitgestellte Software darf nicht veräußert, sondern ausschließlich zum Vorführen oder Testen der Softwarefunktionen verwendet werden.

g) **Ablauf und Kündigung der Lizenz.** Die Lizenz läuft automatisch zum Ende des jeweiligen Lizenzzeitraums aus. Sollten Sie eine Ihrer Pflichten aus dieser Vereinbarung verletzen, ist der Anbieter berechtigt, diese außerordentlich zu kündigen und, ggf. auf dem Rechtsweg, etwaige weitere Ansprüche geltend zu machen. Bei Ablauf oder Kündigung der Lizenz müssen Sie die Software und ggf. alle Sicherungskopien sofort löschen, zerstören oder auf eigene Kosten an ESET oder das Geschäft zurückgeben, in dem Sie die Software erworben haben. Nach Ablauf oder Kündigung der Lizenz ist der Anbieter berechtigt, das Recht des Endbenutzers zur Nutzung der Softwarefunktionen zurückzuziehen, für die eine Verbindung zu Servern des Anbieters oder zu Servern von Drittanbietern erforderlich ist.

4. **Funktionen mit Datenerfassung und Anforderungen an die Internetverbindung.** Für den korrekten Betrieb benötigt die Software eine Internetverbindung und muss in der Lage sein, sich in regelmäßigen Abständen mit den Servern des Anbieters, Servern einer Drittpartei und entsprechenden Datenerfassungen gemäß der Datenschutzrichtlinie zu verbinden. Eine Internetverbindung und die entsprechende Datenerfassung ist für den Betrieb der Software sowie für deren Updates und Upgrades erforderlich. Der Anbieter hat das Recht, Aktualisierungen für die Software („Updates“) oder Upgrades bereitzustellen, ist dazu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat. Zur Bereitstellung von Aktualisierungen muss die Echtheit der Lizenz überprüft werden. Dazu gehören Informationen über den Computer und/oder die Plattform, auf der die Software installiert wurde, in Übereinstimmung mit der Datenschutzerklärung.

Die Bereitstellung von Updates unterliegt möglicherweise der End-of-Life-Richtlinie („EOL-Richtlinie“), die auf https://go.eset.com/eol_business verfügbar ist. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, werden keine Aktualisierungen mehr bereitgestellt.

Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Für die in dieser Vereinbarung festgelegten Zwecke werden Daten gesammelt, verarbeitet und gespeichert, mit denen der Anbieter Sie gemäß der Datenschutzrichtlinie identifizieren kann. Sie stimmen zu, dass der Anbieter mit eigenen Mitteln überprüfen

darf, ob Sie die Software in Übereinstimmung mit den Bestimmungen dieser Vereinbarung nutzen. Sie erkennen an, dass es für die in dieser Vereinbarung festgelegten Zwecke erforderlich ist, dass Ihre Daten zwischen der Software und den Computersystemen des Anbieters bzw. denen seiner Geschäftspartner im Rahmen des Distributions- und Verteilungsnetzwerks des Anbieters übertragen werden, um die Funktionstüchtigkeit der Software und die Genehmigung zu deren Nutzung sowie die Rechte des Anbieters zu schützen.

Mit Abschluss dieser Vereinbarung willigen Sie zudem in die Übertragung, Verarbeitung und Speicherung Ihrer personenbezogenen Daten durch den Anbieter bzw. seine Geschäftspartner ein, soweit eine solche Nutzung zur Abrechnung und zur Erfüllung dieser Vereinbarung und zum Übertragen von Benachrichtigungen auf Ihren Computer erforderlich ist.

Details zur Privatsphäre, zum Schutz persönlicher Daten und zu Ihren Rechten als betroffene Person finden Sie in der Datenschutzrichtlinie auf der Webseite des Anbieters oder direkt beim Installationsprozess. Sie finden diese Informationen außerdem im Hilfebereich der Software.

5. Ausübung der Rechte des Endbenutzers. Sie müssen Ihre Rechte als Endbenutzer selbst oder gegebenenfalls über Ihre Angestellten ausüben. Sie dürfen die Software ausschließlich zur Gewährleistung der Arbeitsfähigkeit und zum Schutz der Computer verwenden, für die Sie eine Lizenz erworben haben.

6. Beschränkungen der Rechte. Es ist untersagt, die Software zu kopieren, zu verbreiten oder aufzuteilen. Außerdem dürfen keine abgeleiteten Versionen erstellt werden. Für die Nutzung der Software gelten die folgenden Einschränkungen:

a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.

b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.

c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.

d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiert oder disassembliert oder auf andere Weise beschafft werden, soweit eine solche Beschränkung nicht ausdrücklich gesetzlichen Bestimmungen widerspricht.

e) Sie verpflichten sich, die Software nur in Übereinstimmung mit allen am Verwendungsort geltenden gesetzlichen Bestimmungen zu verwenden, insbesondere gemäß den Beschränkungen, die sich aus dem Urheberrecht und anderen Rechten an geistigem Eigentum ergeben.

f) Sie verpflichten sich, die Software und ihre Funktionen nur so zu nutzen, dass der Zugriff anderer Endbenutzer auf die betreffenden Dienste nicht eingeschränkt wird. Der Anbieter behält sich das Recht vor, den Leistungsumfang gegenüber einzelnen Endbenutzern einzuschränken, damit die Dienste von möglichst vielen Endbenutzern verwendet werden können. Dies kann auch bedeuten, dass die Nutzung beliebiger Softwarefunktionen vollständig gesperrt wird und dass Daten sowie Informationen im Zusammenhang mit bestimmten Funktionen der Software von den Servern des Anbieters bzw. Dritter gelöscht werden.

g) Sie verpflichten sich hiermit, keine Aktivitäten im Zusammenhang mit dem Lizenzschlüssel auszuführen, die den Bestimmungen dieser Vereinbarung widersprechen oder die dazu führen, dass der Lizenzschlüssel an unbefugte Personen weitergegeben wird, z. B. durch die Übertragung von benutzten oder nicht benutzten Lizenzschlüsseln

in jeglicher Form oder die nicht autorisierte Verteilung von duplizierten oder generierten Lizenzschlüsseln oder die Nutzung der Software im Zusammenhang mit einem Lizenzschlüssel, der aus einer anderen Quelle als direkt vom Anbieter beschafft wurde.

7. Urheberrecht. Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompileieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

8. Rechteevorbehalt. Mit Ausnahme der Rechte, die Ihnen als Endbenutzer der Software in dieser Vereinbarung ausdrücklich gewährt werden, behält sich der Anbieter alle Rechte an der Software vor.

9. Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare. Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

10. Beginn und Gültigkeitsdauer der Vereinbarung. Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Ihr Recht zur Nutzung der Software und deren Funktionen unterliegt möglicherweise einer EOL-Richtlinie. Wenn die Software oder deren Funktionen das in der EOL-Richtlinie definierte Ende des Lebenszyklus erreichen, erlischt Ihr Nutzungsrecht für die Software. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 19 und 21 auf unbegrenzte Zeit ihre Gültigkeit.

11. AUSDRÜCKLICHE ERKLÄRUNGEN DES ENDBENUTZERS. ALS ENDBENUTZER ERKENNEN SIE AN, DASS DIE SOFTWARE IM JEWEILIGEN IST-ZUSTAND UND OHNE JEGLICHE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT WIRD, SOWEIT DIES IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG IST. WEDER DER ANBIETER NOCH SEINE LIZENZGEBER ODER DIE RECHTEINHABER GEWÄHREN AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, INSBESONDERE KEINE ZUSICHERUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON PATENTEN, URHEBER- UND MARKENRECHTEN ODER SONSTIGEN RECHTEN DRITTER. ES BESTEHT VON SEITEN DES ANBIETERS ODER DRITTER KEINERLEI GEWÄHRLEISTUNG, DASS DIE IN DER SOFTWARE ENTHALTENEN FUNKTIONEN IHREN ANFORDERUNGEN ENTSPRECHEN ODER DASS DIE SOFTWARE STÖRUNGS- UND FEHLERFREI AUSGEFÜHRT WIRD. SIE ÜBERNEHMEN DIE VOLLE VERANTWORTUNG UND DAS VOLLE RISIKO HINSICHTLICH DER AUSWAHL DER SOFTWARE ZUM ERREICHEN DER VON IHNEN BEABSICHTIGTEN ERGEBNISSE SOWIE FÜR INSTALLATION UND NUTZUNG DER SOFTWARE UND DEN MIT DIESER ERZIELTEN ERGEBNISSEN.

12. Keine weiteren Verpflichtungen. Aus dieser Vereinbarung ergeben sich für den Anbieter und seine Lizenzgeber keine weiteren Verpflichtungen außer den explizit aufgeführten.

13. HAFTUNGSAUSSCHLUSS. SOWEIT IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG, ÜBERNEHMEN DER ANBIETER, SEINE ANGESTELLTEN UND SEINE LIZENZGEBER KEINERLEI HAFTUNG FÜR ENTGANGENE GEWINNE, ERTRÄGE ODER VERKÄUFE. VON DER HAFTUNG AUSGESCHLOSSEN SIND AUSSERDEM DATENVERLUSTE, BESCHAFFUNGSKOSTEN FÜR ERSATZTEILE ODER DIENSTE, SACH- UND PERSONENSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, DER VERLUST VON GESCHÄFTSINFORMATIONEN SOWIE JEDWEGE ANDERE NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE INFOLGE DER INSTALLATION, NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGSAUSSCHLUSS NICHT ZULÄSSIG IST, EINE HAFTUNGSBESCHRÄNKUNG JEDOCH MÖGLICH, BESCHRÄNKT SICH DIE HAFTUNG DES ANBIETERS, SEINER ANGESTELLTEN UND LIZENZGEBER AUF DEN FÜR DIE LIZENZ ENTRICHTETEN PREIS.

14. Gesetzlich verankerte Verbraucherrechte haben im Konfliktfall Vorrang vor den Bestimmungen dieser Vereinbarung.

15. Technischer Support. ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Nachdem die Software oder eine ihrer Funktionen das in der EOL-Policy festgelegte End-of-Life-Datum erreicht hat, wird kein technischer Support mehr bereitgestellt. Endbenutzer sind verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen. Für die Bereitstellung des technischen Supports sind unter Umständen Lizenzinformationen, Informationen und andere Daten gemäß der Datenschutzrichtlinie erforderlich.

16. Übertragung der Lizenz. Die Software darf von einem Computersystem auf ein anderes übertragen werden, sofern dabei nicht gegen Bestimmungen dieser Vereinbarung verstoßen wird. Sofern in dieser Vereinbarung nicht anderweitig geregelt, ist es dem Endbenutzer gestattet, die Lizenz und alle Rechte aus dieser Vereinbarung an einen anderen Endbenutzer zu übertragen, sofern der Anbieter dem zustimmt und die folgenden Voraussetzungen beachtet werden: (i) Der ursprüngliche Endbenutzer darf keine Kopien der Software zurückbehalten. (ii) Die Übertragung der Rechte muss direkt erfolgen, d. h. vom ursprünglichen Endbenutzer an den neuen Endbenutzer. (iii) Der neue Endbenutzer muss sämtliche Rechte und Pflichten des ursprünglichen Endbenutzers aus dieser Vereinbarung übernehmen. (iv) Der ursprüngliche Endbenutzer muss dem neuen Endbenutzer einen der in Abschnitt 17 genannten Nachweise für die Gültigkeit des Softwarelizenz übereignen.

17. Gültigkeitsnachweis für die Softwarelizenz. Der Endbenutzer kann seine Nutzungsrechte an der Software auf eine der folgenden Arten nachweisen: (i) über ein Lizenzzertifikat, das vom Anbieter oder einem von diesem beauftragten Dritten ausgestellt wurde; (ii) über eine schriftliche Lizenzvereinbarung, falls abgeschlossen; (iii) durch Vorlage einer E-Mail des Anbieters mit den Lizenzdaten (Benutzername und Passwort). Zur Überprüfung der Echtheit der Software sind unter Umständen Lizenzinformationen und Identifikationsdaten des Endbenutzers gemäß der Datenschutzrichtlinie erforderlich.

18. Lizenzvergabe an Behörden und die US-Regierung. Für die Lizenzvergabe an Behörden, insbesondere an Stellen der US-Regierung, gelten ausschließlich die in dieser Vereinbarung beschriebenen Lizenzrechte und Einschränkungen.

19. Einhaltung von Handelskontrollen.

(a) Sie werden die Software nicht direkt oder indirekt an andere Personen exportieren, reexportieren, übertragen

oder auf andere Arten verfügbar machen, auf eine Art verwenden oder sich an Handlungen beteiligen, die zu einer Verletzung der Handelskontrollgesetze durch oder zu sonstigen negativen Folgen für ESET oder eines der übergeordneten Unternehmen, die Tochtergesellschaften von ESET oder die Tochtergesellschaften der übergeordneten Unternehmen sowie die Entitäten unter der Kontrolle der übergeordneten Unternehmen („angeschlossene Unternehmen“) führen könnten. Zu diesen Handelskontrollgesetzen zählen:

i. alle Gesetze, die Lizenzierungsanforderungen zum Export, Reexport oder zur Übertragung von Waren, Software, Technologie oder Dienstleistungen kontrollieren, einschränken oder auferlegen und die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist

ii. alle sonstigen wirtschaftlichen, finanziellen oder handelsbezogenen Sanktionen, Einschränkungen, Embargos, Import- oder Exportbeschränkungen, Verbote von Vermögens- oder Assetübertragungen oder von Dienstleistungen sowie alle gleichwertigen Maßnahmen, die von Regierungen, Bundesstaaten/Bundesländern oder Regulierungsbehörden in den USA, in Singapur, in Großbritannien, der Europäischen Union oder ihren Mitgliedsstaaten oder in anderen Ländern eingeführt oder übernommen wurden, in denen die Verpflichtungen der Vereinbarung gelten, oder in denen ESET oder eines der angeschlossenen Unternehmen sesshaft oder tätig ist.

(die in den Punkten i und ii genannten Gesetze zusammengefasst als „Handelskontrollgesetze“).

b) ESET behält sich das Recht vor, die eigenen Verpflichtungen im Rahmen dieser Bestimmungen fristlos aufzuheben oder die Bestimmungen fristlos aufzukündigen, falls Folgendes eintritt:

i. ESET hat nach eigenem Ermessen festgestellt, dass ein Benutzer die Bestimmungen in Artikel 19 a) dieser Vereinbarung verletzt hat oder vermutlich verletzen wird; oder

ii. ein Endbenutzer und/oder die Software fällt unter die Handelskontrollgesetze, und ESET ist nach eigenem Ermessen der Ansicht, dass die weitere Erfüllung der Verpflichtungen aus der Vereinbarung dazu führen könnte, dass ESET oder ein angeschlossenes Unternehmen die Handelskontrollgesetze verletzt oder dass sonstige negative Folgen zu erwarten sind.

c) Die Vereinbarung ist nicht darauf ausgelegt und darf nicht so interpretiert oder ausgelegt werden, dass eine der Parteien dazu aufgefordert oder verpflichtet wird, auf irgendeine Weise zu handeln oder Handlungen zu unterlassen (oder Handlungen bzw. deren Unterlassung zuzustimmen), die geltende Handelskontrollgesetze verletzt oder gemäß dieser Gesetze unter Strafe steht oder verboten ist.

20. Kündigungen. Alle Kündigungen sowie zurückgegebene Software und Dokumentation sind an folgende Adresse zu senden: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. ESET behält sich das Recht vor, Sie über alle Änderungen an dieser Vereinbarung, der Datenschutzerklärung, der EOL-Richtlinie und der Dokumentation gemäß Art. 22 der Vereinbarung zu informieren. ESET kann Ihnen E-Mails oder In-App-Benachrichtigungen über die Software schicken oder die Kommunikation auf unserer Website veröffentlichen. Sie stimmen zu, rechtliche Mitteilungen von ESET in elektronischer Form zu erhalten, inklusive Mitteilungen zu Änderungen an Bedingungen, Sonderbedingungen oder Datenschutzerklärungen, Benachrichtigungen oder Einladungen zu Vertragsverlängerungen, Kündigungen oder andere rechtliche Mitteilungen. Diese elektronische Kommunikation gilt als schriftlich empfangen, sofern nicht durch geltendes Recht eine andere Kommunikationsform vorgeschrieben ist.

21. Geltendes Recht, Gerichtsstand. Diese Vereinbarung unterliegt slowakischem Recht. Endbenutzer und Anbieter vereinbaren, dass gesetzliche Bestimmungen zur Konfliktlösung und UN-Kaufrecht nicht zur Anwendung kommen. Sie erklären sich ausdrücklich damit einverstanden, dass als Gerichtsstand für alle Streitfälle mit dem

Anbieter oder bezüglich Ihrer Verwendung der Software das Amtsgericht Bratislava I, Slowakische Republik vereinbart wird.

22. Allgemeine Bestimmungen. Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar ist, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Diese Vereinbarung wird auf Englisch getroffen. Falls eine Übersetzung der Vereinbarung aus Gründen der Annehmlichkeit bereitgestellt wird, sind die Bestimmungen der englischen Version maßgeblich, falls Abweichungen bestehen.

ESET behält sich das Recht vor, Änderungen an der Software vorzunehmen und die Bestimmungen dieser Vereinbarung, deren Anhänge und Ergänzungen, die Datenschutzerklärung, die EOL-Richtlinie und die Dokumentation ganz oder in Teilen jederzeit zu ändern, indem das entsprechende Dokument aktualisiert wird, (i) um Änderungen an der Software oder der Funktionsweise von ESET zu berücksichtigen, (ii) aus rechtlichen, regulatorischen oder Sicherheitsgründen oder (iii) um Missbrauch oder Schaden zu verhindern. Bei Änderungen an dieser Vereinbarung werden Sie per E-Mail, per In-App-Benachrichtigung oder über andere elektronische Kommunikationsformen informiert. Wenn Sie den Änderungen der Vereinbarung nicht zustimmen, können Sie diese gemäß Artikel 10 innerhalb von 30 Tagen nach Erhalt der Änderungsbenachrichtigung kündigen. Sofern Sie die Vereinbarung nicht innerhalb dieser Frist kündigen, gelten die Änderungen als von Ihnen akzeptiert und wirksam ab dem Tag, an dem Sie die Änderungsbenachrichtigung erhalten haben.

Dies ist die vollständige Vereinbarung zwischen dem Anbieter und Ihnen in Bezug auf die Software. Sie ersetzt alle vorigen Darstellungen, Diskussionen, Unternehmungen, Kommunikationen und Werbungen in Bezug auf die Software.

ANHANG ZUR VEREINBARUNG

Weiterleitung von Informationen an den Anbieter. Zur Weiterleitung von Informationen an den Anbieter gelten die folgenden zusätzlichen Bestimmungen:

Die Software enthält Funktionen zur Erfassung von Informationen über den Installationsprozess, den Computer und/oder die Plattform, auf der die Software installiert ist, anderen Informationen über Betrieb und Funktionsweise der Software sowie Informationen zu verwalteten Geräten (im Folgenden "Informationen"). Diese Daten werden anschließend an den Anbieter übertragen. Diese Informationen können Daten (inklusive zufällig oder versehentlich erfasster persönlicher Daten) zu den verwalteten Geräten enthalten. Wenn diese Softwarefunktion aktiviert wird, darf der Anbieter gemäß der Datenschutzerklärung und gemäß geltender Gesetze Informationen erfassen und verarbeiten.

Die Software setzt voraus, dass auf dem verwalteten Computer eine Komponente installiert wird, um die Informationen zwischen dem verwalteten Computer und der Remoteverwaltungssoftware übertragen zu können. Zu den übertragenen Informationen gehören Verwaltungsdaten wie Hardware- und Softwareinformationen der verwalteten Computer, sowie Verwaltungsanweisungen von der Remoteverwaltungssoftware. Alle sonstigen vom verwalteten Computer übertragenen Daten werden durch die Einstellungen der auf dem verwalteten Computer installierten Software bestimmt. Der Inhalt der Anweisungen von der Remoteverwaltungssoftware wird durch die Einstellungen der Remoteverwaltungssoftware bestimmt.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Datenschutzerklärung

ESET, spol. s r. o., mit eingetragenem Firmensitz in Einsteinova 24, 851 01 Bratislava, Slowakei, eingetragen im Handelsregister Bratislava I, Abschnitt Sro, Eintragsnummer 3586/B, Firmenregisternummer 31333532 als Datenverarbeiter („ESET“ oder „Wir“) hat das Ziel, die persönlichen Daten und die Privatsphäre seiner Kunden

transparent zu behandeln. Daher veröffentlichen wir diese Datenschutzerklärung mit dem ausschließlichen Ziel, unsere Kunden („Endkunde“ oder „Sie“) über die folgenden Themen zu informieren:

- Verarbeitung persönlicher Daten,
- Vertraulichkeit der Daten,
- Rechte betroffener Personen.

Verarbeitung persönlicher Daten

Die von ESET angebotenen und in unserem Produkt implementierten Dienste werden unter den Bestimmungen der Endbenutzer-Lizenzvereinbarung („EULA“) bereitgestellt. Einige dieser Dienste erfordern jedoch möglicherweise zusätzliche Aufmerksamkeit. Wir möchten Ihnen weitere Details zur Datensammlung im Zusammenhang mit der Bereitstellung unserer Dienste liefern. Wir bieten verschiedene in der EULA und der Produktdokumentation beschriebene Dienste an, darunter die Upgrade- und Updatedienste, ESET LiveGrid[®], den Schutz vor dem Missbrauch von Daten, Support usw. Für die Erbringung dieser Dienste erfassen wir die folgenden Informationen:

- Für die Verwaltung der ESET-Sicherheitsprodukte werden Informationen gesammelt und lokal gespeichert, wie etwa ID und Name des Lizenzplatzes, Produktname, Lizenzinformationen, Aktivierungs- und Ablaufinformationen, Hardware- und Softwareinformationen über den verwalteten Computer, auf dem das ESET-Sicherheitsprodukt installiert wurde. Logs zu den Aktivitäten der verwalteten ESET-Sicherheitsprodukte und Geräte werden erfasst und sind verfügbar für verschiedene Funktionen und Dienste zur Verwaltung und Überwachung. Diese Logs werden nicht automatisch an ESET übertragen.
- Informationen zum Installationsprozess, inklusive der Plattform, auf der unser Produkt installiert wird sowie Informationen zum Betrieb und zur Funktionsweise unserer Produkte, wie etwa Hardwarefingerabdrücke, Installations-IDs, Absturzabbilder, Lizenz-IDs, IP-Adressen, MAC-Adressen und Konfigurationseinstellungen des Produkts, wozu auch verwaltete Geräte gehören können.
- Lizenzinformationen wie die Lizenz-ID und persönliche Daten wie Vor- und Nachname, Adresse und E-Mail-Adresse werden zu Abrechnungszwecken, zur Überprüfung der Echtheit der Lizenz und zur Erbringung unserer Dienste benötigt.
- Kontaktinformationen und andere Daten in Ihren Supportanfragen werden für möglicherweise für die Erbringung von Supportdiensten benötigt. Auf Basis des von Ihnen gewählten Kontaktkanals erfassen wir unter Umständen Ihre E-Mail-Adresse, Telefonnummer, Lizenzinformationen, Produktdetails und eine Beschreibung Ihres Supportfalls. Möglicherweise werden Sie aufgefordert, uns weitere Informationen wie generierte Log-Dateien bereitzustellen, um die Bearbeitung der Supportanfrage zu erleichtern.
- Die Daten zur Nutzung unserer Dienste werden zum Ende der Sitzung vollständig anonymisiert. Nach dem Ende der Sitzung werden keinerlei personenbezogene Daten gespeichert.

Vertraulichkeit der Daten

ESET ist ein weltweit operierendes Unternehmen über angeschlossene Unternehmen oder Partner im Rahmen unseres Distributions-, Dienst- und Supportnetzwerks. Die von ESET verarbeiteten Informationen können zur Erbringung der EULA von und zu angeschlossenen Unternehmen übertragen werden, beispielsweise für die Bereitstellung von Diensten, Supportleistungen oder Abrechnungen. Je nach Ihrem Standort und den von Ihnen ausgewählten Diensten müssen wir Ihre Daten unter Umständen in Länder ohne Gleichstellungsbeschluss der Europäischen Kommission übertragen. Selbst in diesem Fall unterliegen alle Datenübertragungen den Datenschutzbestimmungen und finden nur bei Bedarf statt. Übliche Vertragsklauseln, bindende Unternehmensregeln oder andere geeignete Mechanismen müssen ausnahmslos umgesetzt werden.

Wir unternehmen größte Anstrengungen, um zu verhindern, dass Ihre Daten bei der Bereitstellung von Diensten im Rahmen der EULA länger als notwendig gespeichert werden. Unser Aufbewahrungszeitraum ist unter Umständen länger als die Gültigkeitsdauer Ihrer Lizenz, um Ihnen eine problemlose und komfortable Erneuerung zu ermöglichen. Minimierte und pseudonymisierte Statistiken und sonstige Daten aus ESET LiveGrid® können zu statistischen Zwecken weiterverarbeitet werden.

ESET implementiert angemessene technische und organisatorische Maßnahmen, um einen angemessenen Schutz vor potenziellen Risiken zu bieten. Wir bemühen uns nach Kräften, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Dienste zu gewährleisten. Falls jedoch Ihre Rechte und Freiheiten durch einen Datenangriff gefährdet sind, müssen wir die Aufsichtsbehörden sowie die betroffenen Personen informieren. Betroffene Personen haben das Recht, Beschwerde bei einer Aufsichtsbehörde einzulegen.

Rechte betroffener Personen

ESET unterliegt slowakischem Recht und ist als Teil der Europäischen Union an die Datenschutzgesetze gebunden. Im Rahmen der geltenden Datenschutzgesetze haben Sie als betroffene Person die folgenden Rechte:

- das Recht, Ihre persönlichen Daten von ESET anzufordern,
- das Recht, Ihre persönlichen Daten bei Bedarf zu berichtigen (Sie haben auch das Recht, unvollständige persönliche Daten zu vervollständigen),
- das Recht, die Löschung Ihrer persönlichen Daten anzufordern,
- das Recht, eine Einschränkung der Verarbeitung Ihrer persönlichen Daten anzufordern,
- Einlegen von Einspruch gegen die Verarbeitung
- Einlegen von Beschwerden sowie
- das Recht auf Übertragbarkeit der Daten.

Falls Sie Ihre Rechte als betroffene Person in Anspruch nehmen möchten oder Fragen oder Bedenken haben, schicken Sie uns eine Nachricht an:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk