

## **ESET PROTECT On-Prem 13.0**

### Installation, Upgrade and Migration Guide

[Click here to display the online version of this document](#)

Copyright ©2026 by ESET, spol. s r.o.

ESET PROTECT On-Prem 13.0 was developed by ESET, spol. s r.o.

For more information visit <https://www.eset.com>.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

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

REV. 4/1/2026

<b>1 Introduction</b>	<b>1</b>
<b>1.1 New features in ESET PROTECT On-Prem 13.0</b>	<b>1</b>
<b>1.2 About help</b>	<b>3</b>
<b>1.3 Architecture</b>	<b>4</b>
1.3 Server	5
1.3 Web Console	6
1.3 Agent	7
1.3 ESET Bridge (HTTP Proxy)	8
1.3 Rogue Detection Sensor	9
<b>1.4 The differences between ESET Bridge (HTTP Proxy), Mirror Tool, and direct connectivity</b>	<b>10</b>
1.4 When to start using ESET Bridge (HTTP Proxy)	12
1.4 When to start using Mirror Tool	12
<b>2 Specifications</b>	<b>13</b>
<b>2.1 Network</b>	<b>13</b>
2.1 Ports used	14
<b>2.2 Supported Operating Systems</b>	<b>16</b>
2.2 Windows	16
2.2 Linux	18
2.2 macOS	19
<b>2.3 Supported Web browsers, ESET security applications and languages</b>	<b>19</b>
<b>2.4 Supported database servers and database connectors</b>	<b>21</b>
<b>2.5 Supported versions of Apache Tomcat and Java</b>	<b>23</b>
<b>2.6 Hardware and infrastructure sizing</b>	<b>24</b>
2.6 Deployment recommendations	25
2.6 Deployment for 10,000 clients	27
<b>2.7 Supported Desktop Provisioning Environments</b>	<b>28</b>
<b>3 Install</b>	<b>29</b>
<b>3.1 All-in-one installation on Windows (recommended)</b>	<b>30</b>
<b>3.2 Component installation on Windows</b>	<b>42</b>
3.2 Server installation—Windows	44
3.2 Microsoft SQL Server requirements	52
3.2 MySQL Server installation and configuration—Windows	53
3.2 Dedicated database user account	55
3.2 Agent installation—Windows	55
3.2 ESET Remote Deployment Tool	58
3.2 Web Console installation—Windows	58
3.2 Install Web Console using the All-in-one installer—Windows (recommended)	58
3.2 Install Web Console manually—Windows (advanced users)	63
3.2 RD Sensor installation—Windows	64
3.2 Mirror Tool—Windows	65
3.2 Offline Repository—Windows	75
3.2 Failover Cluster—Windows	77
<b>3.3 Component installation on Linux</b>	<b>77</b>
3.3 Step-by-step ESET PROTECT On-Prem installation on Linux	78
3.3 MySQL installation and configuration—Linux	79
3.3 ODBC installation and configuration—Linux	81
3.3 Server installation—Linux	83
3.3 Server prerequisites—Linux	87
3.3 Agent installation—Linux	89
3.3 Web Console installation—Linux	92
3.3 Rogue Detection Sensor installation—Linux	94

3.3 Mirror Tool—Linux .....	95
3.3 Offline Repository—Linux .....	106
<b>3.4 Component installation on macOS</b> .....	108
3.4 Agent installation—macOS .....	108
<b>3.5 ISO image</b> .....	110
<b>3.6 DNS Service Record</b> .....	110
<b>3.7 Offline installation scenario for ESET PROTECT On-Prem</b> .....	111
<b>4 Upgrade</b> .....	112
<b>4.1 ESET PROTECT Components Upgrade task</b> .....	113
<b>4.2 Use the ESET PROTECT On-Prem 13.0 All-in-one installer to upgrade</b> .....	116
<b>4.3 Database Server Backup/Upgrade</b> .....	119
4.3 Database Server Backup and Restore .....	120
4.3 Database Server Upgrade .....	122
<b>4.4 Upgrade ESET PROTECT On-Prem installed in Failover Cluster on Windows</b> .....	123
<b>4.5 Upgrade Apache Tomcat</b> .....	123
4.5 Upgrade Apache Tomcat using the All-in-one installer (Windows) .....	124
4.5 Upgrade Apache Tomcat manually (Windows) .....	128
4.5 Upgrade Apache Tomcat and Java (Linux) .....	130
<b>5 Migrate and reinstall</b> .....	131
<b>5.1 Migration from one server to another</b> .....	131
5.1 Clean Installation—same IP address .....	131
5.1 Migrated Database—same/different IP address .....	133
<b>5.2 ESET PROTECT database migration</b> .....	135
5.2 Migration process for MS SQL Server .....	135
5.2 Migration process for MySQL Server .....	143
5.2 Connect ESET PROTECT Server to a database .....	145
<b>5.3 Change of ESET PROTECT Server IP address or hostname after migration</b> .....	146
<b>6 Uninstall</b> .....	147
<b>6.1 Uninstall ESET Management Agent</b> .....	147
<b>6.2 Windows—Uninstall ESET PROTECT Server and its components</b> .....	148
<b>6.3 Linux—Upgrade, reinstall or uninstall ESET PROTECT components</b> .....	150
<b>6.4 macOS—Uninstall ESET Management Agent and ESET endpoint application</b> .....	151
<b>6.5 Decommission the old ESET PROTECT Server after migration to another server</b> .....	153
<b>7 FAQ</b> .....	153
<b>8 Troubleshooting</b> .....	159
<b>8.1 Upgrade ESET PROTECT components in offline environment</b> .....	160
<b>8.2 Answers to common installation issues</b> .....	161
<b>8.3 Log files</b> .....	164
<b>8.4 Diagnostic Tool</b> .....	166
<b>8.5 Problems after upgrade/migration of ESET PROTECT Server</b> .....	168
<b>8.6 MSI Logging</b> .....	169
<b>9 ESET PROTECT On-Prem API</b> .....	169
<b>10 Legal documents</b> .....	169

# Introduction

ESET PROTECT On-Prem is an application that allows you to manage ESET applications on client workstations and servers in a networked environment from one central location. With ESET PROTECT On-Prem's built-in task management system, you can enable ESET security modules on remote computers and quickly respond to new problems and detections.

ESET PROTECT On-Prem does not provide protection against malicious code by itself. Protection of your environment depends on the presence of an ESET security application such as ESET Endpoint Security on workstations, or ESET Server Security for Windows on server machines.

ESET PROTECT On-Prem is built around two primary principles:

- Centralized management—The entire network can be configured, managed and monitored from one place.
- Scalability—The system can be deployed in a small network as well as in large enterprise environments. ESET PROTECT On-Prem is designed to accommodate the growth of your infrastructure.

ESET PROTECT On-Prem [supports ESET security applications for business](#).

The ESET PROTECT On-Prem help pages include a complete installation and upgrade guide:

- [Architecture of ESET PROTECT On-Prem](#)
- [Installation procedures](#)
- [Upgrade procedures](#)
- [Migration procedures](#)
- [Uninstallation procedures](#)

After you have installed ESET PROTECT On-Prem, we recommend that you read the following parts of the [Administration guide](#):

- [First steps after installing ESET PROTECT On-Prem](#)
- [Subscription management](#)
- ESET Management Agent [deployment methods](#) to start managing the computers in your network

## New features in ESET PROTECT On-Prem 13.0

### Transition to subscription-based licensing

To support the transition to a modern subscription-based licensing model, ESET PROTECT On-Prem now guides customers without an ESET account through account creation and adding an activation key. This version also includes terminology updates and changes to the Terms of Use. [Learn more](#)

See also [License vs. Subscription: New terminology explained](#).

## Get started with your ESET PROTECT Hub account

For a more streamlined and secure experience, subscriptions previously added to ESET PROTECT On-Prem via an activation key can now be linked to an ESET account through one of our subscription management platforms: ESET PROTECT Hub or <%EBA%>. If you have not done so already, create an ESET PROTECT Hub account or log in to your existing one to get started.

Going forward, all new subscriptions must be added through a subscription management platform. Existing subscriptions will continue to appear in ESET PROTECT On-Prem, but you will need to link them to an account to manage them.

### Why link your subscription?

Linking your subscriptions to an ESET account unlocks powerful benefits:

- Centralized identity, subscription, and user management across all ESET platforms.
- A clear overview of your subscriptions with status and usage insights.
- Granular access control for individual ESET platforms.
- Single sign-in for all linked platforms.

[Learn more about linking your subscription](#)

### Check if your subscriptions are synchronized

Follow these steps to ensure your subscriptions in ESET PROTECT On-Prem are synchronized with a subscription management platform:

1. Go to the **Subscription Management** section to check if any subscriptions are missing a linked account.
2. If you find a subscription without a linked account, log in to or create an account on the appropriate subscription management platform for the subscription owner. Then, add the subscription to the platform.
3. The subscription will synchronize automatically with your ESET PROTECT On-Prem once linked to your account.

## REST API for device and policy management

We are introducing the first set of REST APIs designed for device and policy management. These APIs streamline automation, accelerate integration with external systems, and enhance the efficiency of administrative workflows. [Learn more](#)

## Quarantined file upload for advanced analysis

It is now possible to securely upload quarantined files from endpoints to the ESET PROTECT Server, enabling deeper threat analysis and supporting advanced investigation workflows. [Learn more](#)

## Run Command access restricted to users with 2FA

To enhance security, access to the Run Command feature is now limited to users with Two-Factor Authentication (2FA), reducing the risk of unauthorized remote actions. [Learn more](#)

## Rebootless updates to minimize Windows Server downtime

A new option in the Software Install task allows updating server security applications without full system reboot. This enhancement streamlines updates, ensuring protection with minimal disruption. Rebootless updates are supported starting from version 12.1 for ESET Server Security, ESET Mail Security for Microsoft Exchange Server, and ESET Security for Microsoft SharePoint Server. [Learn more](#)

## Added support for RHEL 10 and Debian 13

ESET PROTECT Server installation is now officially supported on Red Hat Enterprise Linux 10 and Debian 13, ensuring compatibility with the latest enterprise-grade operating systems. [Learn more](#)

## Other improvements and bug fixes

Find out what else has been improved in the [changelog](#).

## About help


This installation guide was written to help with the installation, upgrade and migration of ESET PROTECT On-Prem.


The guide is divided into several chapters and subchapters to provide better orientation and context. You can find relevant information by using the search field at the top. We use a uniform set of symbols to highlight topics of specific interest or significance.


The ESET PROTECT On-Prem Online Help pages include three active tabs at the top navigation header: [Installation/Upgrade/Migration](#), [Administration](#) and [VA Deployment](#).


Help us improve the ESET PROTECT On-Prem user guide. You can post your rating and provide a feedback on a specific chapter in this guide. Click the **Was this information helpful?** at the bottom of the help page to rate and add your comments.

## Information boxes used in this guide

 Notes can provide valuable information, such as specific features or a link to some related topic.

 Information that requires your attention and should not be ignored. These boxes usually provide non-critical but significant information.

 Critical information that requires increased caution. Warnings are placed specifically to prevent potentially harmful mistakes. Read the warnings carefully, as they reference highly sensitive system settings or something risky.

 Examples illustrate use cases to help you understand how to utilize specific features and also explain more complex topics.

## Used text styles

Convention	Meaning
<b>Bold type</b>	Names of interface items such as boxes and option buttons.
Code	Code samples or commands.
<a href="#">Hyperlink</a>	Quick and easy access to cross-referenced topics or external web locations. Hyperlinks are highlighted in blue and may be underlined.
<code>%ProgramFiles%</code>	The Windows system directory where programs installed on Windows are stored.

## Sources of help content

- [ESET Online Help](#) is the primary source of help content. The latest version of Online Help is displayed automatically when you have a working internet connection.
- [ESET Knowledgebase](#) provides answers to the most frequently asked questions and recommends solutions to various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving issues.
- [ESET Forum](#) provides ESET users with an easy way to get help and to help others. You can post any problem or question related to your ESET applications.

## Architecture

ESET PROTECT On-Prem is a new generation of a remote management system.

To perform a complete deployment of [ESET security applications](#), install the following components (Windows and Linux platforms):

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

The following supporting components are optional, but we recommend that you install them to ensure the best performance of the application on the network:

- [ESET Bridge \(HTTP Proxy\)](#)
- [Rogue Detection Sensor](#)

ESET PROTECT components use certificates to communicate with the ESET PROTECT Server. Read more about ESET PROTECT certificates in our [Knowledgebase article](#).



ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

## Infrastructure elements overview

The table below contains an overview of the ESET PROTECT infrastructure elements and their main functions:

Functionality	ESET PROTECT Server	ESET Management Agent	ESET security application	ESET Bridge (HTTP Proxy)	ESET servers
Remote management of ESET security applications (creation of policies, tasks, reports, etc.)	✓	X	X	X	X
Communication with the ESET PROTECT Server and managing ESET security application on the client device	X	✓	X	X	X
Providing updates, subscription validation	X	X	X	☒*	✓
Caching and forwarding updates (detection engine, installers, application modules)	X	X	☒**	✓	X
Forwarding of network traffic between ESET Management Agent and ESET PROTECT Server	X	X	X	✓	X
Securing the client device	X	X	✓	X	X

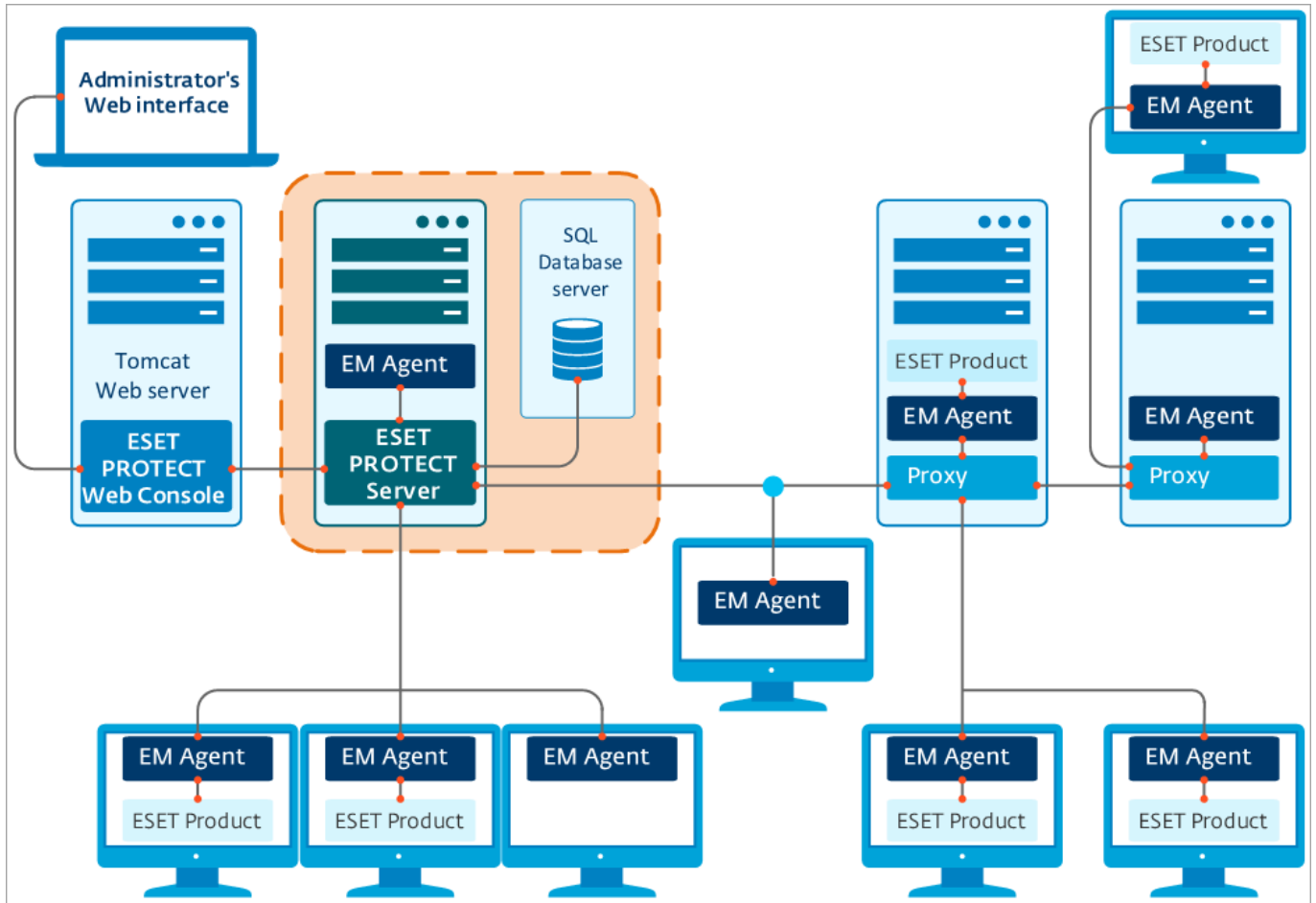
\* Only with an offline repository.

\*\* ESET security applications do not cache installers.

## Server

ESET PROTECT Server is the executive application that processes all data received from clients that connect to the Server (through the ESET Management Agent or [HTTP Proxy](#)). To correctly process data, the Server requires a stable connection to a database server where network data is stored. We recommend that you install the database server on a different computer to achieve better performance.

See also a detailed scheme of the [ESET PROTECT On-Prem network infrastructure](#) with individual components and used ports.



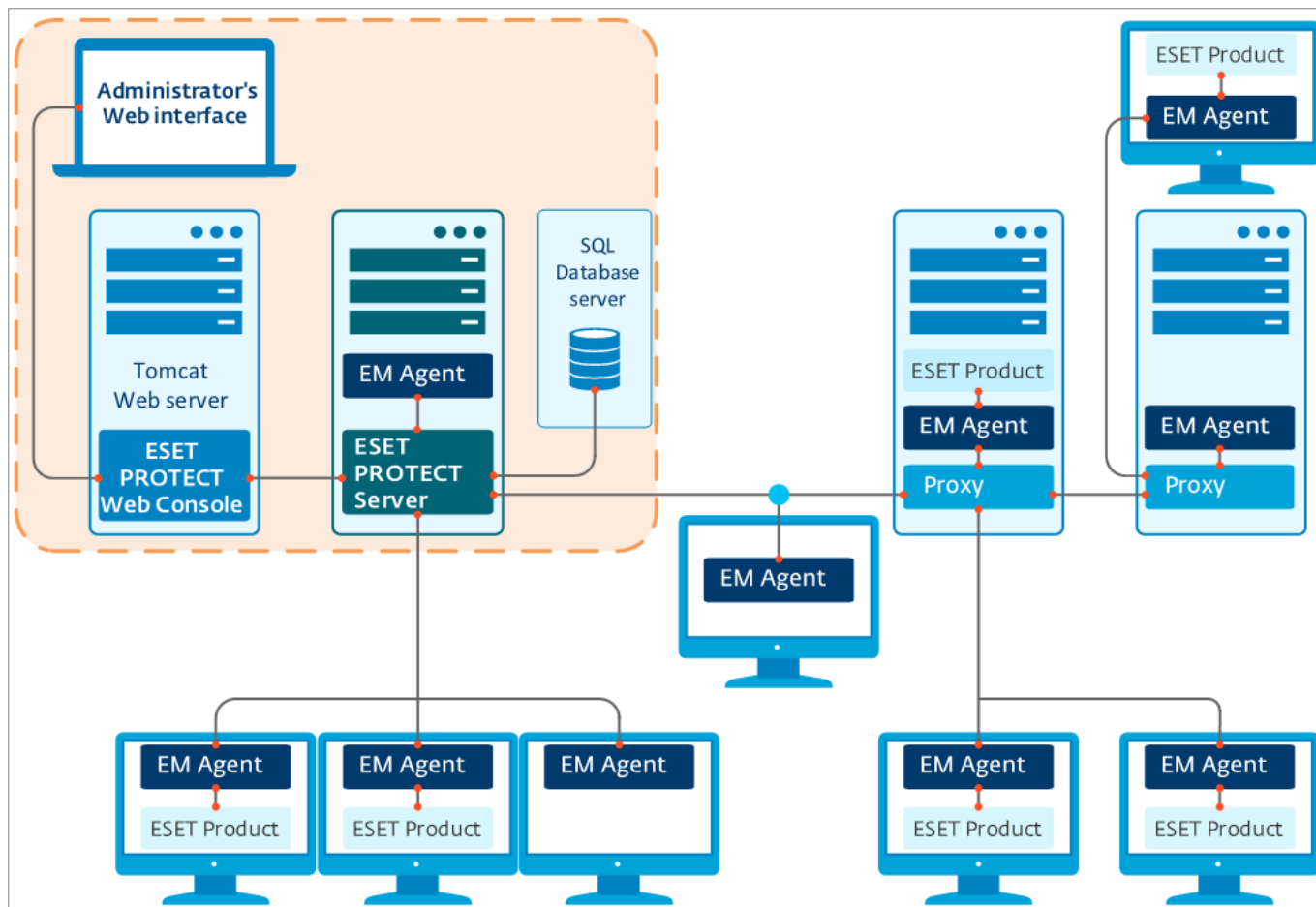
## Web Console

The ESET PROTECT Web Console is a web-based user interface that allows you to manage ESET security modules in your environment. It displays an overview of the status of clients on your network and can be used to deploy ESET modules to unmanaged computers remotely. The Web Console is accessed using your browser (see [Supported Web browsers](#)). If you choose to make the web server accessible from the internet, you can use ESET PROTECT On-Prem from virtually any place and device.

The Web Console uses Apache Tomcat as the HTTP web server. When using the Tomcat bundled in the ESET installer or Virtual Appliance, it only allows TLS 1.2 and 1.3 connections to the Web Console.



You can install the ESET PROTECT Web Console on a different computer than the computer running the ESET PROTECT Server.



## Agent

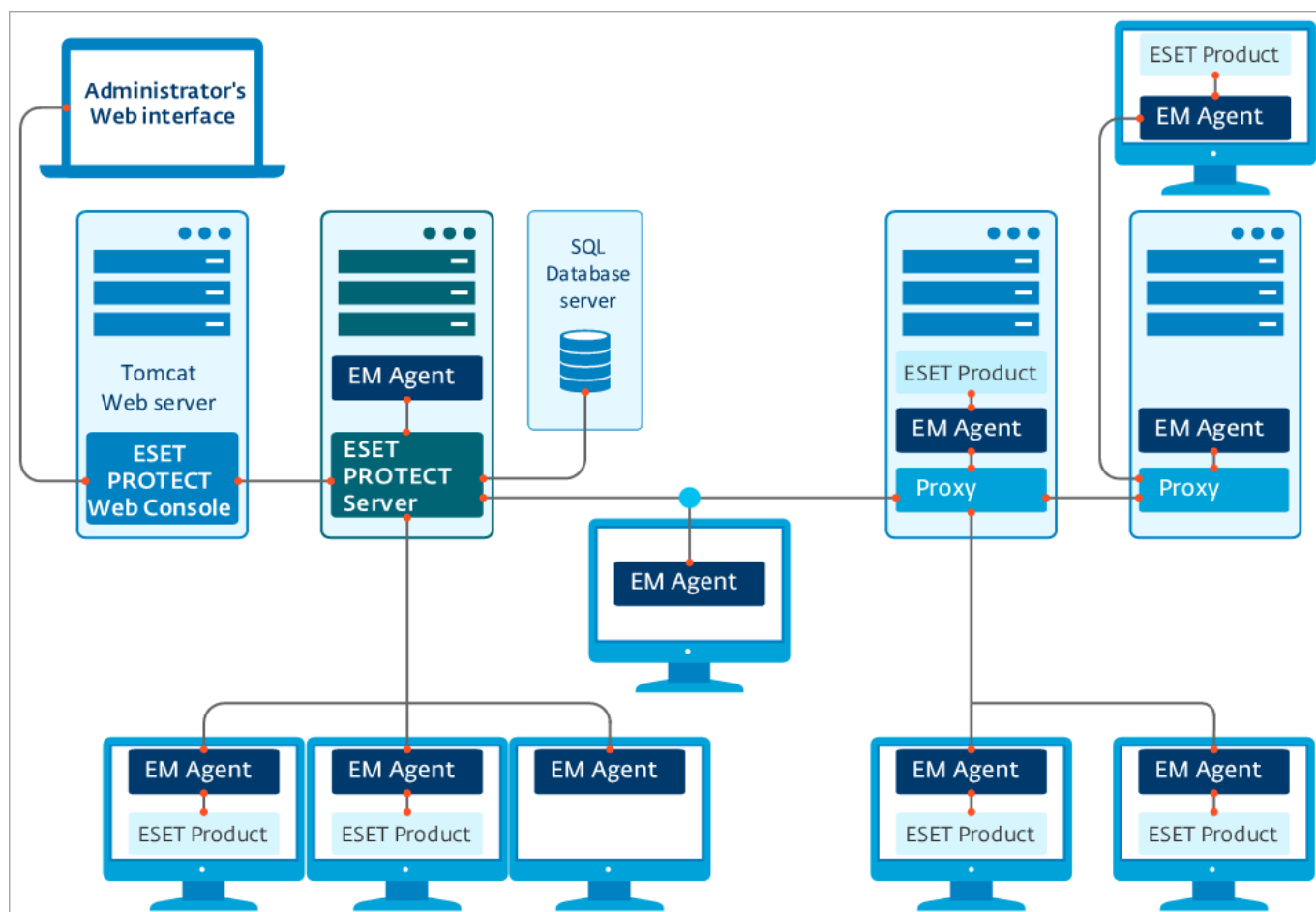
**The ESET Management Agent** is an essential part of ESET PROTECT On-Prem. Clients do not communicate with the ESET PROTECT Server directly, rather the Agent facilitates this communication. The Agent collects information from the client and sends it to the ESET PROTECT Server. If the ESET PROTECT Server sends a task for the client—it is sent to the Agent which then sends this task to the client. The ESET Management Agent is using a new, improved [communication protocol](#).

To simplify implementation of the endpoint protection the standalone ESET Management Agent is included in the ESET PROTECT On-Prem suite. It is simple, highly modular and lightweight service covering all communication between ESET PROTECT Server and any ESET module or operating system. Rather than communicate with the ESET PROTECT Server directly, ESET applications communicate through the Agent. Client computers that have ESET Management Agent installed and can communicate with the ESET PROTECT Server are referred to as 'managed'. You can install the Agent on any computer regardless of whether or not other ESET software has been installed.

The benefits are:

- Easy setup—you can deploy Agent as a part of standard corporate installation.
- On-place security management—because the Agent can be configured to store several security scenarios, reaction time to detection is significantly lowered.
- Off-line security management—the Agent can respond to an event if it is not connected to the ESET PROTECT Server.

The communication protocol between Agent and ESET PROTECT Server does not support authentication. Any proxy solution used for forwarding Agent communication to ESET PROTECT Server that requires authentication will not work. If you choose to use a non-default port for the Web Console or Agent, it may require a firewall adjustment. Otherwise, the installation may fail.



## ESET Bridge (HTTP Proxy)

[ESET Bridge](#) works with ESET PROTECT On-Prem as an HTTP proxy service to:

o [Cache and distribute updates](#) to client computers and installation packages to ESET Management Agent (for example, ESET Endpoint Security MSI installer), ESET security application updates (component and application module updates), ESET LiveGuard results.

o [Forward communication](#) from ESET Management Agents to ESET PROTECT Server in environments where Agent machines cannot reach the Server directly.

o [Cache HTTPS traffic](#)—ESET Bridge can decrypt and cache HTTPS traffic.

o [Proxy chaining](#)—ESET Bridge can forward the traffic to a remote proxy and cache data.

o [Run the offline repository](#)—You can use ESET Bridge as an HTTP server for offline repository.

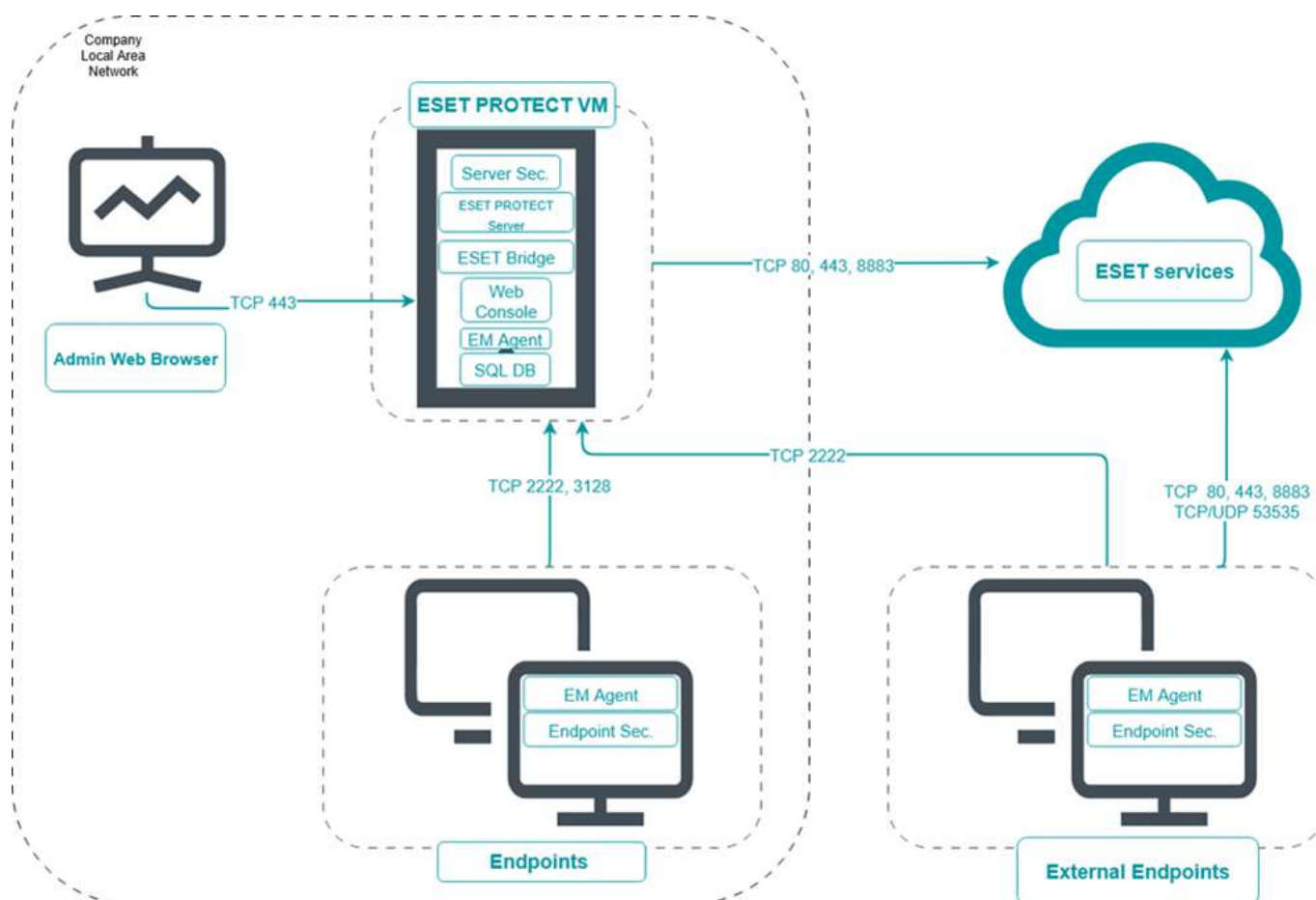
Read the [ESET Bridge Online Help](#) for more details about the ESET Bridge installation and configuration.

Read also about [the differences](#) between ESET Bridge (HTTP Proxy), Mirror Tool, and direct connectivity.

## Apache HTTP Proxy users

- ⚠ ESET distributes ESET Bridge as a Proxy component (replacing the Apache HTTP Proxy). We recommend [migrating to ESET Bridge](#) if you use Apache HTTP Proxy.

ESET Bridge in the network infrastructure with ESET PROTECT On-Prem:



## Rogue Detection Sensor

**Rogue Detection Sensor (RD Sensor)** is a rogue system detector tool that searches your network for computers. The Sensor is convenient because it can locate new computers from ESET PROTECT On-Prem without the need to search and add them manually. Discovered machines are immediately located and reported in a pre-defined report, allowing you to move them to specific static groups and proceed with management tasks.

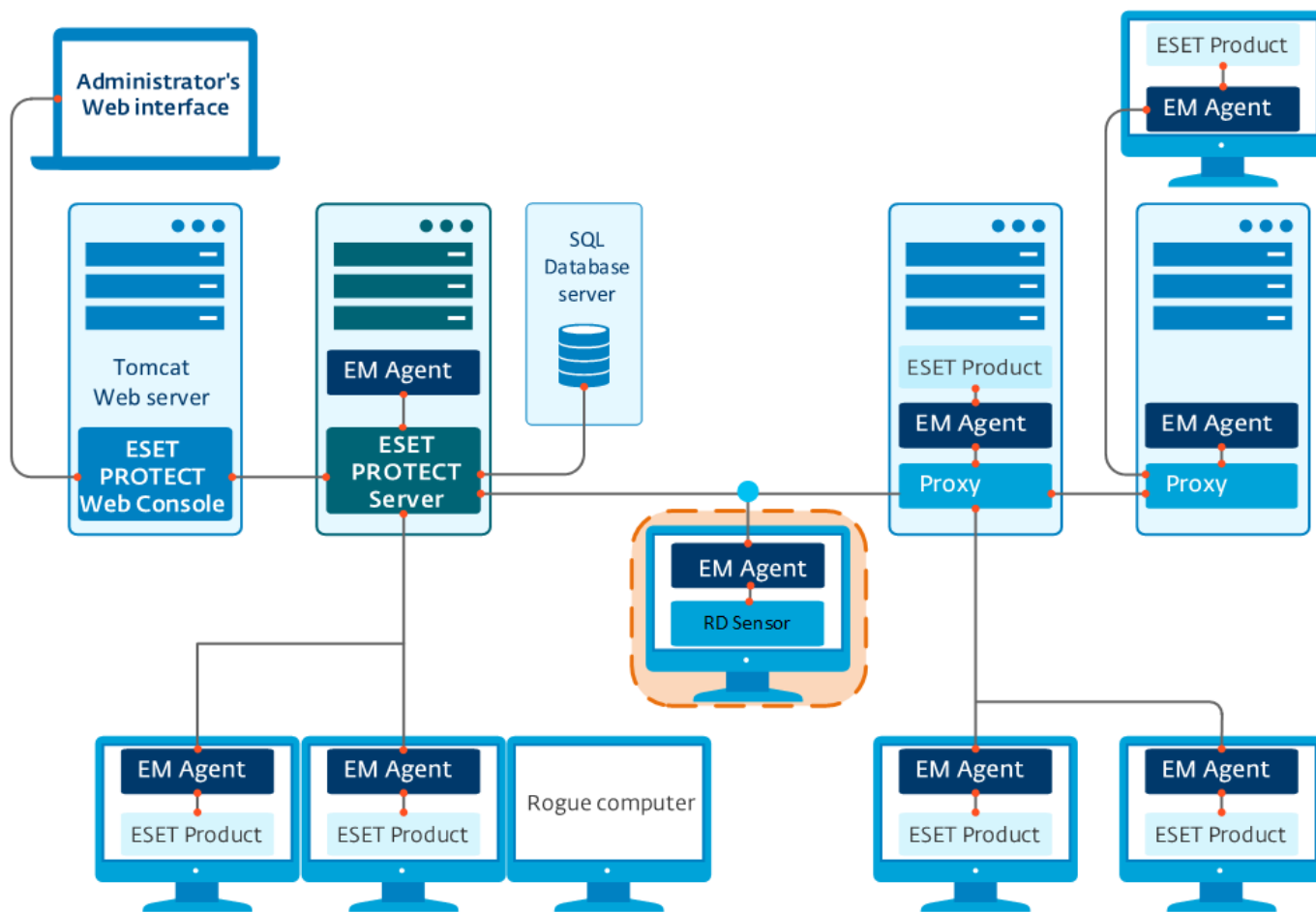
- ⚠ ESET Rogue Detection (RD) Sensor will be deprecated (there will be no future updates). Some of its features may not work properly. You can no longer manage RD Sensor configuration via a policy.

RD Sensor listens to ARP broadcasts. When RD Sensor detects a new active network component, RD Sensor sends ARP unicasts, performs the host fingerprinting (using [several ports](#)) and sends information about the detected computers to the ESET PROTECT Server. ESET PROTECT Server then evaluates whether the PCs found on the network are unknown to ESET PROTECT Server or already managed.

You cannot disable the host fingerprinting because it is the main functionality of RD Sensor.

- ⚠ If there are multiple network segments, Rogue Detection Sensor must be installed separately on each network segment to produce a comprehensive list of all devices on the whole network.

Every computer within the network structure (domain, LDAP, Windows network) is added to ESET PROTECT Server's computers list automatically via a server synchronization task. Using RD sensor is a convenient way to find computers that are not in the domain or other network structure and add them to ESET PROTECT Server. RD Sensor remembers computers that are already discovered and will not send the same information twice.



## The differences between ESET Bridge (HTTP Proxy), Mirror Tool, and direct connectivity

ESET module communication involves detection engine and application module updates as well as the exchange of [ESET LiveGrid®](#) data (see the [table](#) below) and subscription information.

ESET PROTECT On-Prem downloads the latest applications for distribution to client computers from the repository. When distributed, the application is ready to be deployed on the target machine.

After an ESET security application is installed, it must be activated, meaning the application needs to verify your subscription information against the activation server. After activation, detection engine and application modules are updated on a regular basis.

[ESET LiveGrid® Early Warning System](#) helps ensure that ESET is immediately and continuously informed of new infiltrations to quickly protect our customers. The system allows new detections to be submitted to the ESET Research Lab, where they are analyzed and processed.

Most network traffic is generated by application module updates. In general, an ESET security application downloads approximately 23.9 MB of application module updates in a month.

ESET LiveGrid® data (approximately 22.3 MB) and the update version file (up to 11 kB) are the only distributed files that cannot be cached.

There are two types of updates—level and nano updates. [See our Knowledgebase article for more information about update types.](#)

There are 2 ways to decrease network load when distributing updates to a network of computers, [ESET Bridge \(HTTP Proxy\)](#) or Mirror Tool (available for [Windows](#) and [Linux](#)).

**i** Read [this Knowledgebase article](#) to set up Mirror Tool chaining (configure Mirror Tool to download updates from another Mirror Tool).

## ESET communication types

Communication Type	Communication Frequency	Network traffic impact	Proxy-forwarded communication	Proxy Caching Option <sup>1</sup>	Mirroring Option <sup>2</sup>	Offline Environment Option
Agent Deployment (Push / Live Installers from repository)	One time	Approximately 50 MB per client	YES	YES <sup>3</sup>	NO	YES (GPO / SCCM, edited live installers) <sup>4</sup>
Endpoint Installation (Software Install from repository)	One time	Approximately 100 MB per client	YES	YES <sup>3</sup>	NO	YES (GPO / SCCM, installation by package URL) <sup>4</sup>
Detection engine module / Application Module Update	6+ times a day	23.9 MB per month <sup>5</sup>	YES	YES	YES	YES (Offline Mirror Tool & Custom HTTP Server) <sup>6</sup>
Update version file update.ver	~8 times a day	2.6 MB per month <sup>7</sup>	YES	NO	-	-
Activation check	4 times a day	negligible	YES	NO	NO	YES (Offline activation files generated in ESET Business Account or ESET PROTECT Hub) <sup>8</sup>
ESET LiveGrid® Cloud Based Reputation	On-the-fly	11 MB per month	YES	NO	NO	NO

1 For proxy caching impact / benefits see [When to start using ESET Bridge \(HTTP Proxy\)?](#)

2 For mirroring impact see [When to start using Mirror Tool?](#)

3 Once per installation / upgrade we recommend that you deploy one agent (one per specific version) / endpoint initially so that the installer is cached.

4 To deploy the ESET Management Agent across a large network, see [Agent deployment using GPO and SCCM.](#)

5 Your Initial detection engine update may be larger than normal depending on the age of the installation package, because all later detection engine updates and application module updates will be downloaded. We recommended to install one client initially, and let it update, so the needed detection engine and application module updates are cached.

6 Without an internet connection, Mirror Tool cannot download detection engine updates. You can use Apache Tomcat as an HTTP server to download updates to a directory available to the Mirror Tool (available for [Windows](#) and [Linux](#)).

7 When checking for detection engine updates, the *update.ver* file is always downloaded and parsed. By default, ESET endpoint application scheduler is querying for a new update each hour. We assume a client workstation is turned on 8 hours a day. The *update.ver* file contains approximately 11 kB.

8 Download offline activation files from [ESET Business Account](#) or [ESET PROTECT Hub](#).

# When to start using ESET Bridge (HTTP Proxy)

Based on our practical tests, we recommend that you deploy [ESET Bridge \(HTTP Proxy\)](#) if you have a network of 37 or more computers.



It is crucial for effective caching that the date and time on the HTTP Proxy server is set correctly. Differences of several minutes would cause the caching mechanism not to work effectively and more files would be downloaded than necessary.

Analysis of network bandwidth used solely by updates in a test network of 1,000 computers where several installations and uninstallations took place showed the following:

- a single computer downloads 23.9 MB/month in [updates](#) on average if directly connected to the internet (no HTTP Proxy is used)
- using HTTP Proxy, downloads for the entire network totaled 900 MB/month

A simple comparison of downloaded update data in a month using direct internet connection or HTTP Proxy in a network of computers:

Number of PCs in your corporate network	25	36	50	100	500	1,000
Direct connection to internet (MB/month)	375	900	1,250	2,500	12,500	25,000
ESET Bridge HTTP Proxy (MB/month)	30	50	60	150	600	900

# When to start using Mirror Tool

If you have an offline environment, meaning the computers in your network do not connect to the internet for a prolonged period of time (months, a year) the Mirror Tool (available for [Windows](#) and [Linux](#)) is the only way to distribute application module updates, because it downloads all available Level and Nano updates during each new update request if there is a new update available.



Read [this Knowledgebase article](#) to set up Mirror Tool chaining (configure Mirror Tool to download updates from another Mirror Tool).

The major difference between ESET Bridge (HTTP Proxy) and Mirror Tool is that ESET Bridge (HTTP Proxy) downloads only missing updates (for example, Nano update 3), while Mirror Tool downloads all available [Level and Nano updates](#) (or only Level updates, if specified), regardless of which update the specific application module is missing.



Streamed updates are not available with Mirror Tool. We recommend to prefer update via ESET Bridge (HTTP Proxy) to update from a mirror wherever possible. Even if a computer is offline but has access to another machine that is connected to the internet and can run ESET Bridge (HTTP Proxy) to cache update files, select this option.

In the same network of 1,000 computers we tested the Mirror Tool instead of [ESET Bridge \(HTTP Proxy\)](#). The analysis showed there were 5,500 MB of updates downloaded for the month. The size of downloaded updates did not increase by adding more computers to the network. This is still a huge decrease in load compared to a configuration where clients connect directly to the internet, but the improvement in performance is not as substantial as when HTTP Proxy is used.

Number of PCs in your corporate network	25	36	50	100	500	1,000
Direct connection to internet (MB/month)	375	900	1,250	2,500	12,500	25,000
Mirror Tool (MB/month)	5,500	5,500	5,500	5,500	5,500	5,500

**i** Even if there were more than 1,000 computers in a network, the bandwidth usage concerning updates would not increase significantly using either ESET Bridge (HTTP Proxy) or Mirror Tool.

## Specifications

Your system must meet a set of hardware, database, network, and software prerequisites to install and operate ESET PROTECT On-Prem.

- [Network](#)
  - o [Ports used](#)
- [Supported Operating Systems](#)
  - o [Windows](#)
  - o [Linux](#)
  - o [macOS](#)
- [Supported Web browsers, ESET security applications and languages](#)
- [Supported database servers and database connectors](#)
- [Supported versions of Apache Tomcat and Java](#)
- [Hardware and infrastructure sizing](#)
  - o [Deployment recommendations](#)
  - o [Deployment for 10,000 clients](#)
- [Supported Desktop Provisioning Environments](#)

## Network

It is essential that both ESET PROTECT Server and client computers managed by ESET PROTECT On-Prem have a working internet connection so that they can reach the ESET repository and activation servers. If you prefer not to have clients connect directly to the internet, you can use a proxy server (not the same as [ESET Bridge HTTP Proxy](#)) to facilitate communication with your network and the internet.

The ESET PROTECT Server must be visible by client computers—client computers must be able to communicate with your ESET PROTECT Server to use remote deployment and the wake-up call feature.

ESET PROTECT On-Prem for Windows/Linux is compatible with both IPv4 and IPv6 internet protocols. ESET PROTECT Virtual Appliance is compatible only with IPv4.

## Ports used

If your network uses a firewall, see our list of possible [network communication ports](#) used when ESET PROTECT On-Prem and its components are installed in your infrastructure.

## Network traffic impact by ESET PROTECT Server and ESET Management Agent communication

Applications on client machines do not communicate with ESET PROTECT Server directly, ESET Management Agent facilitates this communication. This solution is easier to manage and less demanding on data transferred over network. Network traffic depends on the client connection interval and types of tasks performed by clients. Even if no task is executed or scheduled on a client, ESET Management Agent communicates with ESET PROTECT Server once per each connection interval. Each connection generates traffic. See the table below for examples of traffic:

Action type	Traffic in a single connection interval
Client Task: Scan without cleaning	4 kB
Client Task: Application modules update	4 kB
Client Task: SysInspector Log Request	300 kB
Policy: Antivirus—Maximum security	26 kB

ESET Management Agent replication interval	Daily traffic generated by idle ESET Management Agent
1 minute	16 MB
15 minutes	1 MB
30 minutes	0.5 MB
1 hour	144 kB
1 day	12 kB

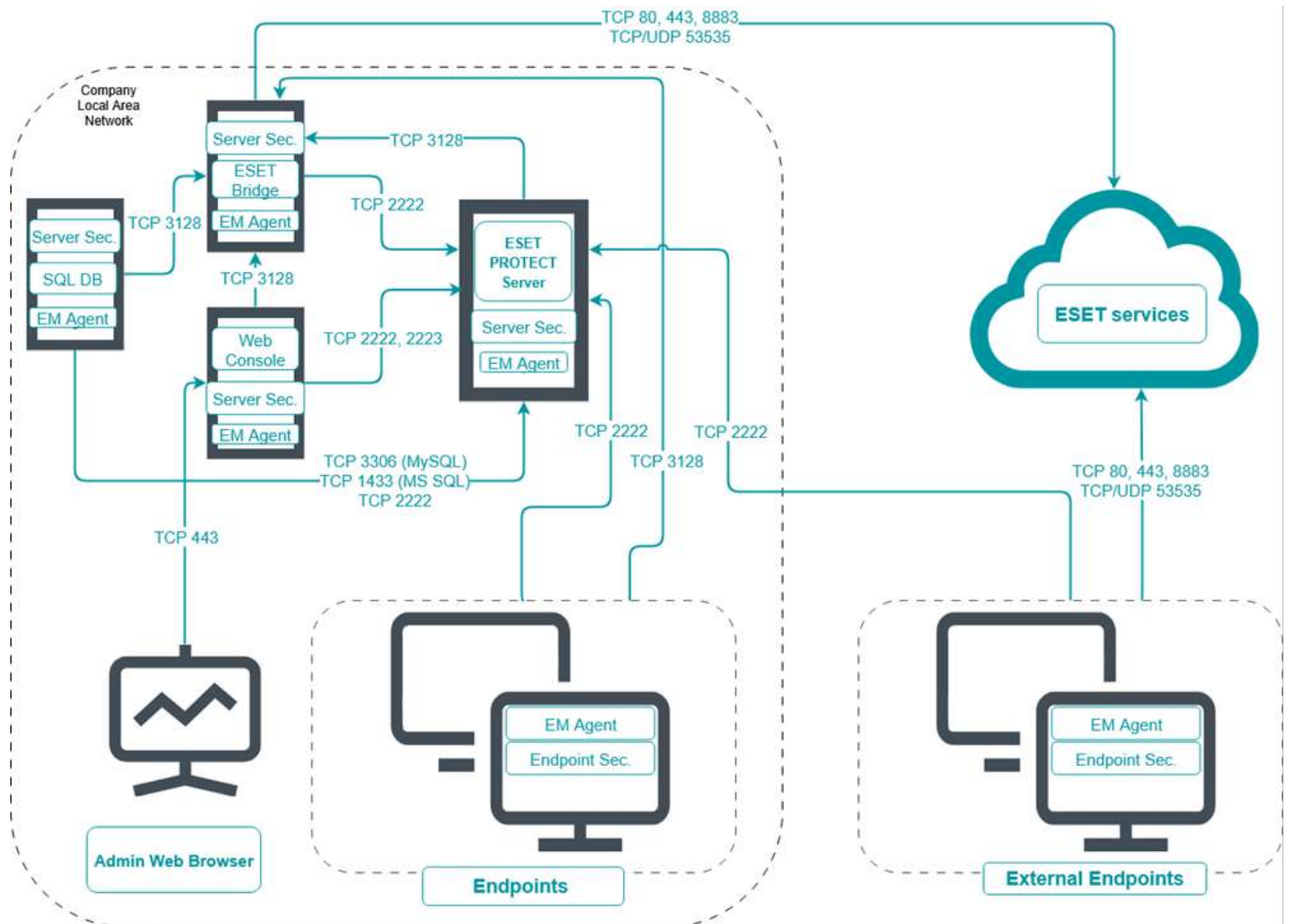
To estimate the overall traffic generated by ESET Management Agents, use the following formula:

*Number of clients \* (Daily traffic of idle agent + (Traffic for certain task \* daily occurrence of the task))*

If you use the ESET Inspect On-Prem, the ESET Inspect Connector generates daily traffic of 2–5 MB (it varies based on the number of events).

## Ports used

ESET PROTECT Server can be installed on the same computer as the database, ESET PROTECT Web Console and HTTP Proxy. The diagram below shows the separated installation and the used ports (arrows indicate the network traffic):



The tables below list all possible network communication ports used when ESET PROTECT On-Prem and its components are installed in your infrastructure. Additional communication occurs via the native operating system processes (for example, NetBIOS over TCP/IP).

**!** For the proper function of the ESET PROTECT On-Prem, other applications should not use any of the ports below. Ensure to configure any firewall(s) within your network to allow communication via the ports listed below.

### Client (ESET Management Agent) or ESET Bridge (HTTP Proxy) machine

Protocol	Port	Descriptions
TCP	2222	Communication between ESET Management Agents and ESET PROTECT Server
TCP	80	Connection to the ESET repository
MQTT	8883, 443	<a href="#">ESET Push Notification Service</a> —Wake-Up calls between ESET PROTECT Server and ESET Management Agent, 443 is failover port.
TCP	3128	Communication with ESET Bridge (HTTP Proxy)
TCP	443	Communication with ESET LiveGuard Advanced (Proxy only)

ESET Management Agent—ports used for remote deployment to a target computer with Windows operating system:

Protocol	Port	Descriptions
TCP	139	Using the share ADMIN\$
TCP	445	Direct access to shared resources using TCP/IP during remote installation (an alternative to TCP 139)
UDP	137	Name resolution during remote install
UDP	138	Browse during remote install

### ESET PROTECT Web Console machine (if not the same as ESET PROTECT Server machine)

Protocol	Port	Descriptions
TCP	2223	Communication between ESET PROTECT Web Console and ESET PROTECT Server; used for Assisted installation.
TCP	443/80	Tomcat broadcasting the Web Console.
TCP	443	RSS Feed for Support News: <ul style="list-style-type: none"> <li><a href="https://era.welivesecurity.com:443">https://era.welivesecurity.com:443</a></li> <li><a href="https://support.eset.com:443/rss/news.xml">https://support.eset.com:443/rss/news.xml</a></li> </ul>

## [ESET PROTECT Server machine](#)

Protocol	Port	Descriptions
TCP	2222	Communication between ESET Management Agent and ESET PROTECT Server
TCP	80	Connection to the ESET repository
MQTT	8883	<a href="#">ESET Push Notification Service</a> —Wake-Up calls between ESET PROTECT Server and ESET Management Agent
TCP	2223	DNS resolving and MQTT fallback
TCP	3128	Communication with ESET Bridge (HTTP Proxy)
TCP	1433 (Microsoft SQL) 3306 (MySQL)	Connection to an external database (only if the database is on another machine).
TCP	389	LDAP synchronization. Open this port also on your AD controller.
UDP	88	<a href="#">Kerberos tickets</a> (applies only to ESET PROTECT Virtual Appliance)

## [Rogue Detection \(RD\) Sensor](#)

Protocol	Port	Descriptions
TCP	22, 139	Detection of operating system via SMB (TCP 139) and SSH (TCP 22) protocols.
UDP	137	Computer hostname resolution via NetBIOS.

The pre-defined ports 2222, 2223 can be changed if necessary.

# Supported Operating Systems

The following sections describe ESET PROTECT component support for [Windows](#), [Linux](#) and [macOS](#) operating system versions.

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

## Windows

The following table displays the supported Windows operating systems for each ESET PROTECT component:

Operating System	Server	Agent	RD Sensor
Windows Server 2012 x64		10.1, 11.0–12.5, 13.0	✓
Windows Server 2012 CORE x64		10.1, 11.0–12.5, 13.0	✓
Windows Server 2012 R2 x64		10.1, 11.0–12.5, 13.0	✓
Windows Server 2012 R2 CORE x64		10.1, 11.0–12.5, 13.0	✓
Windows Storage Server 2012 R2 x64		10.1, 11.0–12.5, 13.0	✓
Windows Server 2016 x64	✓	10.1, 11.0–12.5, 13.0	✓
Windows Storage Server 2016 x64	✓	10.1, 11.0–12.5, 13.0	✓
Windows Server 2019 x64	✓	10.1, 11.0–12.5, 13.0	✓


Operating System	Server	Agent	RD Sensor
Windows Server 2022 x64	✓	10.1, 11.0–12.5, 13.0	✓
Windows Server 2022 CORE x64	✓	11.0–12.5, 13.0	
Windows Server 2025 x64	✓	12.0, 12.3, 12.5, 13.0	


Operating System	Server	Agent	RD Sensor
Windows 10 x86**		10.1, 11.0–12.0, 12.5, 13.0	✓
Windows 10 x64**	☒*	10.1, 11.0–12.5, 13.0	✓
Windows 10 on ARM**		10.1, 11.0–12.5, 13.0	
Windows 11 x64	☒*	10.1, 11.0–12.5, 13.0 (21H2 and 22H2) 10.1, 11.0–12.5, 13.0 (23H2) 11.2–12.5, 13.0 (24H2) 12.5, 13.0 (25H2)	✓
Windows 11 on ARM		10.1, 11.0–12.5, 13.0	

\* Installing ESET PROTECT components on a desktop operating system might not be in alignment with Microsoft licensing policy. Check the Microsoft licensing policy or consult your software supplier for details. In SMB / small network environments, we encourage you to consider a Linux ESET PROTECT On-Prem installation or [virtual appliance](#) where applicable.

\*\* Windows 10 reached its [end of support](#).

The [Support Policy Category B](#) in the ESET End of Life Policy determines the support level (Full Support/Limited Support/End of Life) and the support end dates for the ESET Management Agent. The latest ESET Management Agent version compatible with ESET PROTECT On-Prem 13.0 is Agent 13.0.


 ESET Rogue Detection (RD) Sensor will be deprecated (there will be no future updates). Some of its features may not work properly. You can no longer manage RD Sensor configuration via a policy.

 ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

We do not support illegal or pirated operating systems.

You can run ESET PROTECT On-Prem on a non-server operating system without the need for ESXi. Install [VMware Player](#) on a desktop Operating System and deploy the [ESET PROTECT Virtual Appliance](#).

**Earlier Microsoft Windows systems**

- ESET Management Agent 10.x is the last version that supports [Windows 7/8.x](#) and [Windows Server 2008 R2/Microsoft SBS 2011](#).
-  • Always have the latest service pack installed, especially on earlier systems, such as Windows Server 2012.
- ESET PROTECT On-Prem does not support the management of computers running Windows XP/Vista/7/8.

# Linux

The following table displays supported Linux operating systems for each ESET PROTECT component:

Operating System	Server	Agent	RD Sensor
Ubuntu 18.04.1 LTS x64 Desktop		10.1, 11.0–12.5, 13.0	✓
Ubuntu 18.04.1 LTS x64 Server		10.1, 11.0–12.5, 13.0	✓
Ubuntu 20.04 LTS x64	✓	10.1, 11.0–12.5, 13.0	✓
Ubuntu 22.04 LTS x64	✓	10.1, 11.0–12.5, 13.0	✓
Ubuntu 24.04 LTS x64	✓	11.0–12.5, 13.0	
Linux Mint 20		10.1, 11.0–12.5, 13.0	✓
Linux Mint 21		10.1, 11.0–12.5, 13.0	✓
Linux Mint 22		11.2–12.5, 13.0	✓
RHEL Server 7 x64		10.1, 11.0–12.5, 13.0	✓
RHEL Server 8 x64	✓	10.1, 11.0–12.5, 13.0	
RHEL Server 9 x64	✓	10.1, 11.0–12.5, 13.0	✓
RHEL Server 10 x64	🔗*	12.5, 13.0	
CentOS 7 x64		10.1, 11.0–12.5, 13.0	✓
SLED 15 x64		10.1, 11.0–12.5, 13.0	✓
SLES 12 x64		10.1, 11.0–12.5, 13.0	✓
SLES 15 x64		10.1, 11.0–12.5, 13.0	✓
Debian 10 x64		10.1, 11.0–12.5, 13.0	✓
Debian 11 x64	✓	10.1, 11.0–12.5, 13.0	✓
Debian 12 x64	✓	10.1, 11.0–12.5, 13.0	✓
Debian 13 x64	✓	12.3, 12.5, 13.0	✓
Oracle Linux 8		10.1, 11.0–12.5, 13.0	✓
Oracle Linux 9		12.5, 13.0	
Oracle Linux 10		12.5, 13.0	
Amazon Linux 2		10.1, 11.0–12.5, 13.0	✓
Amazon Linux 2023		11.2–12.5, 13.0	
Alma Linux 9		10.1, 11.0–12.5, 13.0	✓
Alma Linux 10		12.5, 13.0	
Rocky Linux 8		10.1, 11.0–12.5, 13.0	
Rocky Linux 9	✓	10.1, 11.0–12.5, 13.0	✓
Rocky Linux 10		12.5, 13.0	

\* Generating PDF reports does not work for ESET PROTECT On-Prem 13.0 installed on Red Hat 10.

ESET Management Agent has been tested and runs on the latest minor releases of the listed Linux distributions.

The [Support Policy Category B](#) in the ESET End of Life Policy determines the support level (Full Support/Limited Support/End of Life) and the support end dates for the ESET Management Agent. The latest ESET Management

Agent version compatible with ESET PROTECT On-Prem 13.0 is Agent 13.0.



ESET Rogue Detection (RD) Sensor will be deprecated (there will be no future updates). Some of its features may not work properly. You can no longer manage RD Sensor configuration via a policy.



ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

## macOS



macOS is supported as a client only. The [ESET Management Agent](#) and [ESET applications for macOS](#) can be installed on macOS. However, ESET PROTECT Server cannot be installed on macOS.

Operating System	Agent
macOS Catalina (10.15)	10.1, 11.0–12.5, 13.0
macOS Big Sur (11.0–11.1)	10.1, 11.0–12.5, 13.0
macOS Monterey (12.0)	10.1, 11.0–12.5, 13.0
macOS Ventura (13.0)	10.1, 11.0–12.5, 13.0
macOS Sonoma (14.0)	10.1, 11.0–12.5, 13.0
macOS Sequoia (15.0)	11.2–12.5, 13.0
macOS Tahoe (26.0)	12.3, 12.5, 13.0

The [Support Policy Category B](#) in the ESET End of Life Policy determines the support level (Full Support/Limited Support/End of Life) and the support end dates for the ESET Management Agent. The latest ESET Management Agent version compatible with ESET PROTECT On-Prem 13.0 is Agent 13.0.

## Supported Web browsers, ESET security applications and languages

### Supported operating systems

[Windows](#)

[Linux](#)

[macOS](#)

### Supported web browsers for the ESET PROTECT Web Console

For the best experience with the ESET PROTECT Web Console we recommend that you keep your web browsers updated.

Google Chrome

Microsoft Edge

Mozilla Firefox

Opera

Safari

## ESET Management Agent versioning and support

The [Support Policy Category B](#) in the ESET End of Life Policy determines the support level (Full Support/Limited Support/End of Life) and the support end dates for the ESET Management Agent. The latest ESET Management Agent version compatible with ESET PROTECT On-Prem 13.0 is Agent 13.0.

We recommend using the latest ESET Management Agent to fully manage the latest version of ESET security applications and their features. If you use an earlier ESET Management Agent version than the ESET PROTECT Server version, some of the latest management features might not be available.

## ESET security applications manageable via ESET PROTECT On-Prem 13.0

### Earlier ESET security applications

ESET security application versions earlier than those shown in the table below are not manageable using ESET PROTECT On-Prem 13.0.



When the ESET security application version reaches the End of Life:

- The application may stop functioning.
- Remote management via the ESET Management Agent may no longer work.
- An application upgrade to a later version may not be possible.

For more information about compatibility, visit the [End of Life policy for ESET business applications](#).

The ESET security application and service versions listed below are manageable with ESET Management Agent version 13.0.

Application or service	Version
ESET Endpoint Security for Windows	10.1+
ESET Endpoint Antivirus for Windows	10.1+
ESET Endpoint Security for macOS	8.0+
ESET Endpoint Antivirus for macOS	7.4+
ESET Server Security for Microsoft Windows Server (formerly ESET File Security for Microsoft Windows Server)	9.0+
ESET Mail Security for Microsoft Exchange Server	9.0+
ESET Security for Microsoft SharePoint Server	9.0+
ESET Mail Security for IBM Domino	9.0+
ESET Server Security for Linux (formerly ESET File Security for Linux)	9.1+
ESET Endpoint Antivirus for Linux	9.1+
ESET LiveGuard Advanced	
ESET Inspect Connector	2.3+
ESET Full Disk Encryption for Windows	2.0+
ESET Full Disk Encryption for macOS	1.3+

## Supported languages

Language	Code
English (United States)	en-US
Arabic (Egypt)	ar-EG

Language	Code
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Croatian (Croatia)	hr-HR
Czech (Czech Republic)	cs-CZ
French (France)	fr-FR
French (Canada)	fr-CA
German (Germany)	de-DE
Greek (Greece)	el-GR
Hungarian (Hungary)*	hu-HU
Indonesian (Indonesia)*	id-ID
Italian (Italy)	it-IT
Japanese (Japan)	ja-JP
Korean (Korea)	ko-KR
Polish (Poland)	pl-PL
Portuguese (Brazil)	pt-BR
Russian (Russia)	ru-RU
Spanish (Chile)	es-CL
Spanish (Spain)	es-ES
Slovak (Slovakia)	sk-SK
Turkish (Turkey)	tr-TR
Ukrainian (Ukraine)	uk-UA



\* Only the application is available in this language; Online Help is not available.

## Supported database servers and database connectors

Specify the database server and connector you want to use when installing the ESET PROTECT Server. You can use an existing database server running in your environment; however, it must meet the requirements below.

ESET PROTECT On-Prem supports two types of database servers: Microsoft SQL Server and MySQL.


Database server	Supported?	Supported database versions	Supported database connectors
Microsoft SQL Server	Yes	<ul style="list-style-type: none"> <li>Express and non-Express editions</li> <li>2016, 2017, 2019, 2022*</li> </ul>	<ul style="list-style-type: none"> <li>SQL Server</li> <li>SQL Server Native Client 10.0</li> <li>ODBC Driver for SQL Server 11, 13, 17, 18</li> </ul>

Database server	Supported?	Supported database versions	Supported database connectors
MySQL	Yes	<ul style="list-style-type: none"> <li>• 8.0</li> <li>• 8.1</li> <li>• 8.4</li> <li>• 9.0–9.4</li> </ul> The later 9.x versions are supported as long as they maintain backward compatibility with the listed versions.	MySQL ODBC driver versions: <ul style="list-style-type: none"> <li>• 8.x (8.0.x, 8.1.x)</li> <li>• 9.2</li> <li>• 9.3</li> </ul>
MariaDB	No	 ESET PROTECT On-Prem does not support MariaDB. MariaDB is a default database in most current Linux environments and gets installed when you select to install MySQL.	MariaDB ODBC 3.1 driver (Windows, Rocky Linux)  The ESET PROTECT Server Rocky Linux installation with <a href="#">mariadb-connector-odbc</a> driver fails with specific locales—Chinese, Korean, Japanese.

\* The ESET PROTECT On-Prem 13.0 [All-in-one installer](#) installs Microsoft SQL Server Express 2022 by default.


oUpgrading checks for previous SQL installations and offers an upgrade to SQL 2022 or 2016 (based on the operating system).

oThe installer generates a random password for database authentication and stores it in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`.


 Microsoft SQL Server Express (the free edition) has a 10 GB size limit for each relational database. We recommend using other Microsoft SQL Server editions than Microsoft SQL Server Express:
 

- In enterprise environments or large networks.
- If you want to use ESET PROTECT On-Prem with [ESET Inspect On-Prem](#).

## Database installation recommendations


 ESET PROTECT Server does not use an integrated backup. We strongly recommend that you [back up](#) your database server to prevent data loss.

- [Do not install SQL Server on a Domain Controller](#). Install ESET PROTECT On-Prem on a different server or deselect the SQL Server Express component during installation. Use your existing SQL or MySQL Server to run the ESET PROTECT database.
- If you intend to use a dedicated database user account that will only have access to the ESET PROTECT database, you must create a user account with specific privileges before installation. For more information, see the [dedicated database user account](#). Additionally, you will need to create an empty database that will be used by ESET PROTECT On-Prem.
- See the instructions to install and configure [MySQL for Windows](#) and [MySQL for Linux](#) to work properly with ESET PROTECT On-Prem.
- [Microsoft SQL Server on Linux](#) is not supported. However, you can [connect](#) the ESET PROTECT Server on Linux to Microsoft SQL Server on Windows.

- If you install the ESET PROTECT Server and Microsoft SQL Server [on separate computers](#), you can [enable encrypted connection](#) to the database.
- The cluster setup of the database on Windows environments is supported only for the Microsoft SQL Server, not for MySQL.

## Database server hardware requirements

See the [hardware](#) and sizing instructions.

## Performance recommendations

We recommend using the latest supported Microsoft SQL Server as your ESET PROTECT database for the best performance. While ESET PROTECT On-Prem is compatible with MySQL, using MySQL can negatively impact system performance when working with large amounts of data, including dashboards, detections, and clients. The same hardware with Microsoft SQL Server can handle significantly more clients than with MySQL.

You can decide whether to install an SQL database server on:

- The same machine as the ESET PROTECT Server.
- The same machine, but on a separate disk.
- A dedicated server for the installation of an SQL database server.

We recommend that you use a dedicated machine(s) with reserved resources if you want to manage more than 10,000 clients.

Database	SMB customer	Enterprise customer	Clients limit	Windows	Linux
Microsoft SQL Express	✓	(optional)	5,000	✓	
Microsoft SQL Server	✓	✓	None	✓	
MySQL	✓	✓	10,000	✓	✓

## Supported versions of Apache Tomcat and Java

### Apache Tomcat

Apache Tomcat is a mandatory component required to run the ESET PROTECT Web Console.


ESET PROTECT On-Prem supports only Apache Tomcat 9.x (64-bit). We recommend that you use the latest Apache Tomcat 9.x.

ESET PROTECT On-Prem does not support alpha/beta/RC versions of Apache Tomcat.

### Java

Apache Tomcat requires 64-bit Java/OpenJDK.

If your system has multiple Java versions installed, uninstall earlier Java versions and keep only the latest [supported Java](#) version.

 Starting January 2019, Oracle JAVA SE 8 public updates for business, commercial or production use require a commercial license. If you do not purchase a JAVA SE subscription, you can transition to a no-cost alternative. See the [supported versions of JDK](#).

## Hardware and infrastructure sizing

ESET PROTECT Server machine should meet the following hardware recommendations in the table below.

Number of clients	ESET PROTECT Server + SQL database server				
	CPU cores	CPU clock speed (GHz)	RAM (GB)	Disk drive <sup>1</sup>	Disk IOPS <sup>2</sup>
Up to 1,000	4	2.1	4	Single	500
5,000	8	2.1	8		1,000
10,000 <sup>3</sup>	4	2.1	16	Separate	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

<sup>1</sup> Single / Separate disk drive—We recommend installing the [database](#) on a separate drive for systems with over 10,000 clients.

<sup>2</sup> IOPS (total I/O operations per second)

- We recommend having approximately 0.2 IOPS per connected client, but no less than 500.
- You can check your drive's IOPS using the tool [diskspd](#), use the following command:

Clients number	Command
Up to 5,000 clients	<code>diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat</code>
Over 5,000 clients	<code>diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat</code>

<sup>3</sup> See the [example scenario](#) for 10,000 clients environment.

### Disk drive recommendations

The disk drive is the critical factor influencing the ESET PROTECT On-Prem performance.

- The SQL Server instance can share resources with the ESET PROTECT Server to maximize utilization and minimize latency. Run the ESET PROTECT Server and the database server on a single machine to increase the ESET PROTECT On-Prem performance.
- The performance of a SQL server is enhanced if you place database and transaction log files on separate drives, preferably separate physical SSD drives.
- If you have a single disk drive, we recommend that you use an SSD drive.

- We recommend that you use all-flash architecture. Solid-state disks (SSD) are much faster than the standard HDD.
- If you have a high RAM configuration, SAS setup with R5 is sufficient. The tested configuration: 10 x 1.2 TB SAS disks in R5—two parity group in 4+1 with no extra caching.
- The performance does not improve when using an enterprise-grade SSD with high IOPS.
- 100 GB capacity is enough for any number of clients. You may need a higher capacity if you backup the database often.
- Do not use a network drive, as its performance would slow the ESET PROTECT On-Prem down.
- If you have a working multi-tier storage infrastructure that allows online storage migration, we recommend to start with shared slower tiers, and monitor your ESET PROTECT On-Prem performance. If you notice read/write latency goes over 20 ms, you can perform non-disruptive move on your storage layer to a faster tier to use the most cost-effective backend. You can do the same in a hypervisor (if you use the ESET PROTECT On-Prem as virtual machine).

## Sizing recommendations for different client counts

Below you can find the performance results for a virtual environment with a set number of clients running for one year.

**i** The database and ESET PROTECT On-Prem are running on separate virtual machines with identical hardware configurations.

CPU cores	CPU clock speed (GHz)	RAM (GB)	Performance		
			10,000 clients	20,000 clients	40,000 clients
8	2.1	64	High	High	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Normal	Low

## Deployment recommendations

### Best practices for deployment of ESET PROTECT On-Prem

Number of clients	Up to 1,000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100,000+
ESET PROTECT Server & Database Server on the same machine	✓	✓	✓	X	X	X
Use of Microsoft SQL Express	✓	✗*	X	X	X	X
Use of Microsoft SQL	✓	✓	✓	✓	✓	✓
Use of MySQL	✓	✓	✓	X	X	X
Use of ESET PROTECT Virtual Appliance	✓	✓	Not Recommended	X	X	X
Use of VM server	✓	✓	✓	Optional	X	X
Recommended connection interval (during deployment phase)	60 seconds	5 minutes	10 minutes	15 minutes	20 minutes	25 minutes

Number of clients	Up to 1,000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100,000+
Recommended connection interval (after deployment, during standard usage)	10 minutes	10 minutes	20 minutes	30 minutes	40 minutes	60 minutes

\* To avoid filling ESET PROTECT database, we do not recommend this scenario if you also use ESET Inspect On-Prem.

## Connection interval

ESET PROTECT Server is connected to the ESET Management Agents using permanent connections. Despite the permanent connection, data transmission occurs only once during the connection interval. For example, if the replication interval on 5,000 clients is eight minutes, there are 5,000 transmissions in 480 seconds, 10.4 per second. Ensure to set the appropriate [client connection interval](#). Ensure to keep the total number of Agent—Server connections below 1,000 per second, even for high-performance hardware configurations.

If a server is overloaded or there is a malware outbreak (for example, we connect 20,000 clients to a server only able to service 10,000 clients at an interval of every 10 minutes), it will skip some connected clients. Not connected clients will try to connect to the ESET PROTECT Server later.

## Single Server (Small Business)

To manage small networks (1,000 clients or less), use a single machine with ESET PROTECT Server and all ESET PROTECT components installed on it. In SMB / small network environments, we encourage you to consider a Linux ESET PROTECT On-Prem installation or [virtual appliance](#) where applicable.

## Remote Branches with Proxies

If client machines do not directly see the ESET PROTECT Server, use a [proxy](#) to forward the ESET applications communication. HTTP Proxy is not aggregating the communication or lowering the traffic of replication.

## High Availability (Enterprise)

For enterprise environments (over 10,000 clients), consider the following:

- [RD Sensor](#) helps to search your network and discover new computers.
- You can install ESET PROTECT Server on a Failover Cluster.
- Configure your HTTP Proxy for a high number of clients or use more Proxies.

## Web Console configuration for enterprise solutions or low-performance systems

By default, the ESET PROTECT Web Console installed via All-in-one installer for Windows reserves a memory limit of 1024 MB for Apache Tomcat.

You can change the default Web Console configuration based on your infrastructure:

- In the enterprise environment, the default Web Console configuration can suffer from instability when working with a high number of objects. Change the Tomcat settings to prevent memory shortages. Ensure

your system has enough RAM (16 GB or more) before making these changes.

- If you have a low-performance system with limited hardware resources, you can decrease the Tomcat memory usage.

**i** Memory values provided below are recommendations. You can adjust the Tomcat memory settings based on your hardware resources.

## Windows

1. Open the *tomcat9w.exe* or run the **Configure Tomcat** application.
2. Switch to the **Java** tab.
3. Change the memory usage:
  - a. Increase (enterprise): Change the values **Initial memory pool** to 2048 MB and **Maximum memory pool** to 16384 MB.
  - b. Decrease (low-performance systems): Change the values **Initial memory pool** to 256 MB and **Maximum memory pool** to 2048 MB.
4. Restart the Tomcat service.

## Linux and ESET PROTECT Virtual Appliance

1. Open the Terminal as root or use `sudo`.
2. Open the file:
  - a. ESET PROTECT Virtual Appliance: `/etc/sysconfig/tomcat`
  - b. Debian: `/etc/default/tomcat9`
3. Add the following line to the file:
  - a. Increase memory usage (enterprise): `JAVA_OPTS="-Xms2048m -Xmx16384m"`
  - b. Decrease memory usage (low performance systems): `JAVA_OPTS="-Xms256m -Xmx2048m"`
4. Save the file and restart the Tomcat service.  
`service tomcat restart`

## Deployment for 10,000 clients

Below you can find the performance results for a virtual environment with 10,000 clients running for one year.

### Hypervisor server configuration

Component	Value
VMware	ESXi 6.7 Update 2 and later (VM version 15)

Component	Value
<b>Hypervisor</b>	VMware ESXi, 6.7.0
<b>Logical Processors</b>	112
<b>Processor Type</b>	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

### The test ran on dedicated machines

- ! The database and ESET PROTECT On-Prem are running on separate virtual machines with identical hardware configurations.

## Software used on virtual machines

ESET PROTECT On-Prem:

- Operating system: Microsoft Windows Server 2016 Standard (64-bit)

Database:

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

## ESET PROTECT On-Prem environment description

- 10,000 connecting clients
- Approximately 2,000 dynamic groups and 2,000 templates for dynamic groups
- Approximately 255 static groups
- 20 users
- 15 minute connection interval for ESET Management Agents
- After the environment is running for one year, the database size is 15 GB

CPU count	RAM (GB)	Performance
8	64	High
4	32	Normal

## Supported Desktop Provisioning Environments

Desktop Provisioning makes device management easier and provides for faster hand-off of desktop computers to end users.

Provisioned desktops are typically physical or virtual. For virtualized environments that use a streamed operating system (Citrix provisioning services), see the list of [supported hypervisors](#).

ESET PROTECT On-Prem [supports](#):

- systems with non-persistent disks
- VDI environments
- identification of cloned computers

## Supported hypervisors and hypervisor extensions

Hypervisor	ESET PROTECT On-Prem	ESET Full Disk Encryption
Citrix XenServer	✓	X
Microsoft Hyper-V	✓	✓ (secure boot not supported)
VMware vSphere	✓	✓ (7.0.3.00300)
VMware ESXi	✓	✓ (7.0)
VMware Workstation	✓	✓ (16.2.3)
VMware View	✓	X
Oracle VirtualBox	✓	X
VMware Fusion	☑ x64 X ARM	✓ (12.2.3)
Parallels	X	✓

Hypervisor extension	ESET PROTECT On-Prem	ESET Full Disk Encryption
Citrix VDI-in-a-box	✓	X
Citrix XenDesktop	✓	X

## Tools

(applies to both virtual and physical machines)

- Microsoft SCCM
- Windows Server 2016/2019/2022/2025 Server Manager
- Windows Admin Center

## Install



The Installation guide covers many ways to install ESET PROTECT On-Prem and is generally intended for enterprise customers. Please refer to the [All-in-one installation](#) if you want to install ESET PROTECT On-Prem on a Windows platform.

For instructions to upgrade your existing ESET PROTECT On-Prem installation, see [Upgrade procedures](#).

ESET PROTECT installers are available in the [Download ESET PROTECT](#) section of the ESET website. Different formats are available to support different install methods. By default, the **All-in-one installer** tab is selected. Click the appropriate tab to download a VA or a standalone installer. The following downloads are available:

- The ESET PROTECT On-Prem [All-in-one installer](#) package for Windows in zip format (recommended installer on Windows).

- An ISO image that contains all ESET PROTECT installers (except ESET PROTECT Virtual Appliances).
- Virtual appliances (OVA files). We recommend deploying of the ESET PROTECT Virtual Appliance for users who want to run ESET PROTECT On-Prem in a virtualized environment or prefer a more simple installation. See our complete [ESET PROTECT Virtual Appliance deployment guide](#) for step-by-step instructions.
- Individual installers for each component for [Windows](#) and [Linux](#) platforms.

**i** Since November 2022, we do not provide ESET PROTECT Virtual Appliance in the Azure Marketplace. Alternatively, you can use [ESET PROTECT in cloud](#) and let ESET manage all required infrastructure components.

To decide what kind of ESET PROTECT On-Prem installation is suitable for your environment, see the following table that will guide you to the best choice. For example:

- Do not use a slow internet connection for ESET PROTECT On-Prem in cloud.
- Select an All-in-one installer if you are an SMB customer.

See also [Hardware and infrastructure sizing](#). You can install ESET PROTECT On-Prem on physical or virtual machines.

Many installation scenarios require you to install different ESET PROTECT components on different machines to accommodate network architectures, meet performance requirements, or for other reasons.

Installation method	Customer type		Migration		Environment for ESET PROTECT On-Prem installation				Internet connection	
	SMB	Enterprise	Yes	No	No server	Dedicated server	Shared server	Virtualization platform	Available	None
<a href="#">All-in-One on Windows Server</a> (recommended)	✓	✓	✓			✓	✓		✓	✓
<a href="#">All-in-One on Windows Desktop</a>	✓		✓		✓				✓	✓
<a href="#">Virtual Appliance</a> (recommended)	✓		✓					✓	✓	✓
<a href="#">Component Linux</a>		✓	✓			✓	✓		✓	✓
<a href="#">Component Windows</a>		✓	✓			✓	✓		✓	✓

**!** Do not change the computer name of your ESET PROTECT Server machine after the installation. See [Change of IP address or hostname on ESET PROTECT Server](#) for more information.

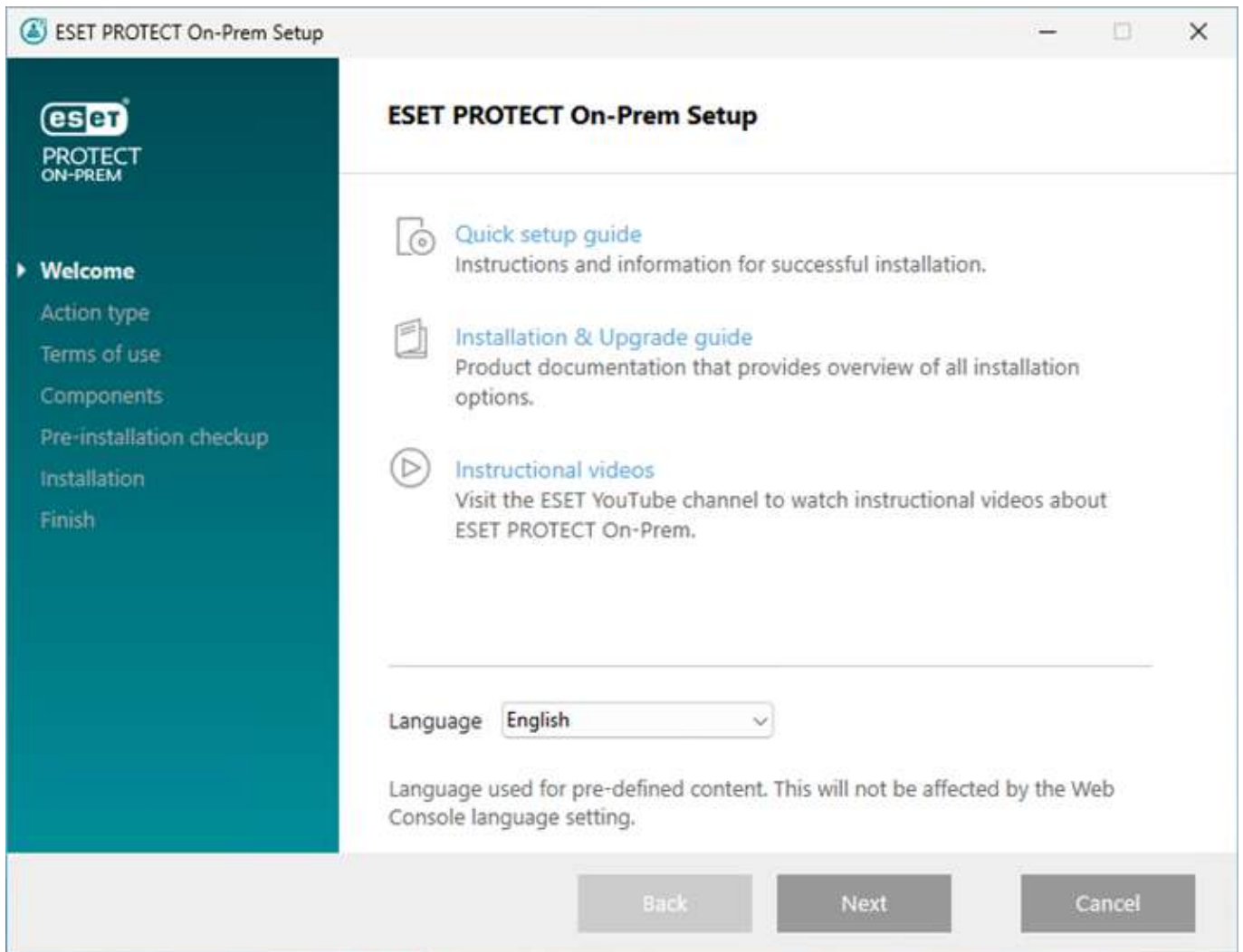
## All-in-one installation on Windows (recommended)

The All-in-one installer enables the installation of all ESET PROTECT components via the ESET PROTECT On-Prem installation Wizard.

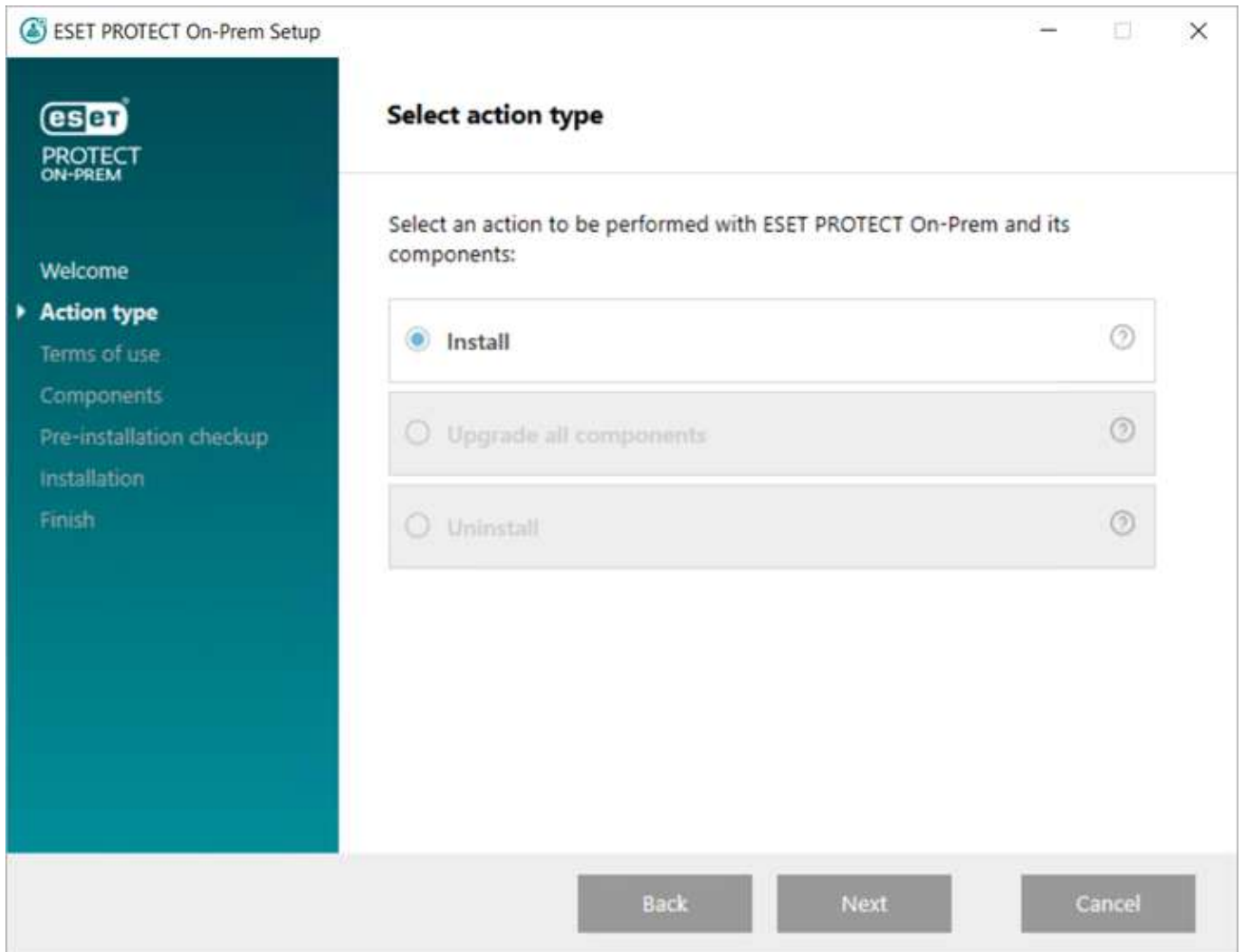
The ESET PROTECT All-in-one installer is available for Windows operating systems only. [Are you a Linux user?](#)

1. Visit the ESET PROTECT [download section](#) to download the ESET PROTECT All-in-one installer.

2. Open the installation package. On the **Welcome** screen, use the **Language** drop-down menu to set the language. Click **Next**.



3. Select **Install** and click **Next**.



4. Select the **Participate in product improvement program** check box to send anonymous telemetry data and crash report to ESET (operating system version and type, ESET application version and other application-specific information). Select **I accept the Terms of Use** and click **Next**.

5. Select the components to install and click **Next**.

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

- The ESET PROTECT On-Prem 13.0 [All-in-one installer](#) installs Microsoft SQL Server Express 2022 by default. OUpgrading checks for previous SQL installations and offers an upgrade to SQL 2022 or 2016 (based on the operating system).
- The installer generates a random password for database authentication and stores it in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`.

 Microsoft SQL Server Express (the free edition) has a 10 GB size limit for each relational database. We recommend using other Microsoft SQL Server editions than Microsoft SQL Server Express:


- In enterprise environments or large networks.
- If you want to use ESET PROTECT On-Prem with [ESET Inspect On-Prem](#).

- If you already have a [supported version](#) of Microsoft SQL Server or MySQL installed, or you plan to connect to a different SQL Server, deselect the check box next to **Microsoft SQL Server Express**.
- [Do not install SQL Server on a Domain Controller](#). Install ESET PROTECT On-Prem on a different server or deselect the SQL Server Express component during installation. Use your existing SQL or MySQL Server to run the ESET PROTECT database.


### [Add custom HTTPS certificate for Webconsole](#)

- Select this option if you want to use a custom HTTPS certificate for the ESET PROTECT Web Console.
- If you do not select this option, the installer automatically generates a new Tomcat keystore (a self-signed HTTPS certificate).


## [Rogue Detection Sensor](#)

 ESET Rogue Detection (RD) Sensor will be deprecated (there will be no future updates). Some of its features may not work properly. You can no longer manage RD Sensor configuration via a policy.

## [ESET Bridge Proxy](#)

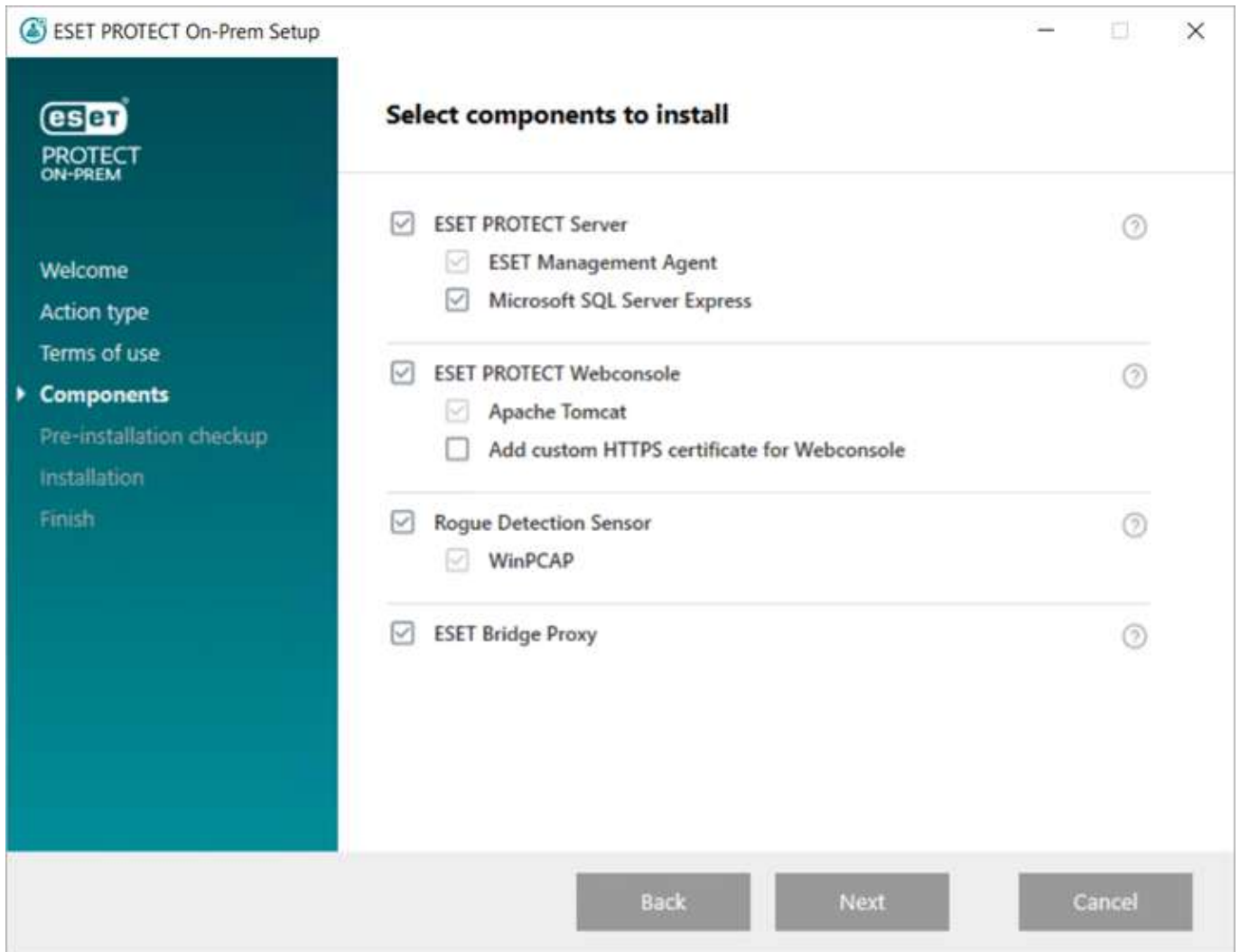
 The **ESET Bridge Proxy** option is intended only for smaller or centralized networks without roaming clients. If you select this option, the installer configures clients to tunnel communication with ESET via a proxy installed on the same machine as the ESET PROTECT Server. This connection will not work if there is no direct network visibility between clients and the ESET PROTECT Server.

- HTTP Proxy can considerably reduce bandwidth usage on data downloaded from the internet and improve download speeds for application updates. We recommend selecting the check box next to **ESET Bridge Proxy** if you manage more than 37 computers from ESET PROTECT On-Prem. You can also choose to [install ESET Bridge later](#).
- For more information, see [ESET Bridge \(HTTP Proxy\)](#) and [The differences between ESET Bridge \(HTTP Proxy\), Mirror Tool, and direct connectivity](#).

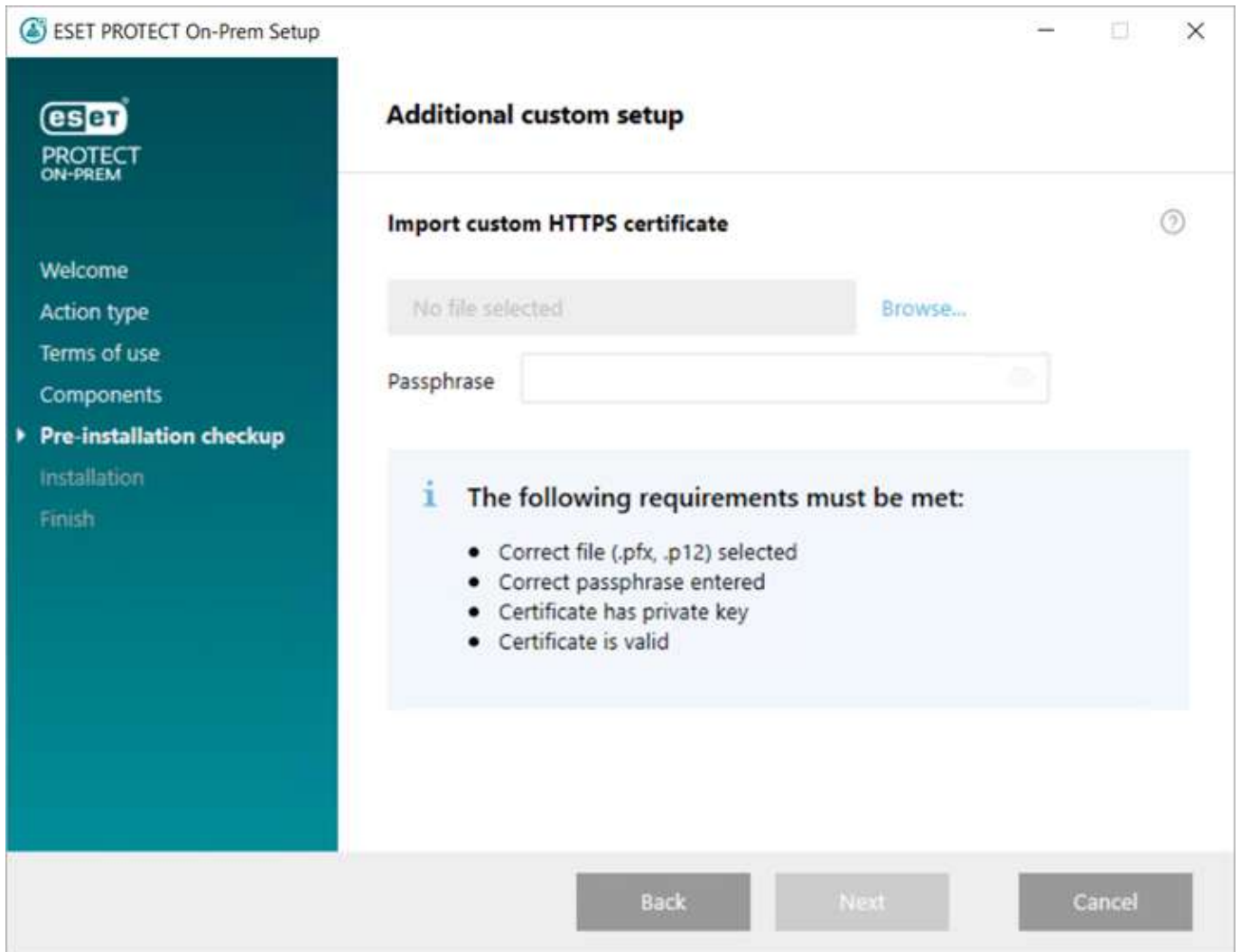
 The All-in-one installer creates default **HTTP Proxy Usage** policies for ESET Management Agent and ESET security applications applied to the **All Static Group**. The policies automatically configure ESET Management Agents and ESET security applications on managed computers to use ESET Bridge as a Proxy for caching update packages. The [HTTPS traffic caching](#) is enabled by default:

- The ESET Bridge policy contains the HTTPS certificate and the **Cache HTTPS Traffic** toggle is enabled.
- The **HTTP Proxy usage** policy for ESET Endpoint for Windows contains the Certificate Authority for the HTTPS traffic caching.

HTTP Proxy host is the ESET PROTECT Server's local IP address and port 3128. Authentication is disabled. You can copy these settings to another policy if you need to set up additional applications.



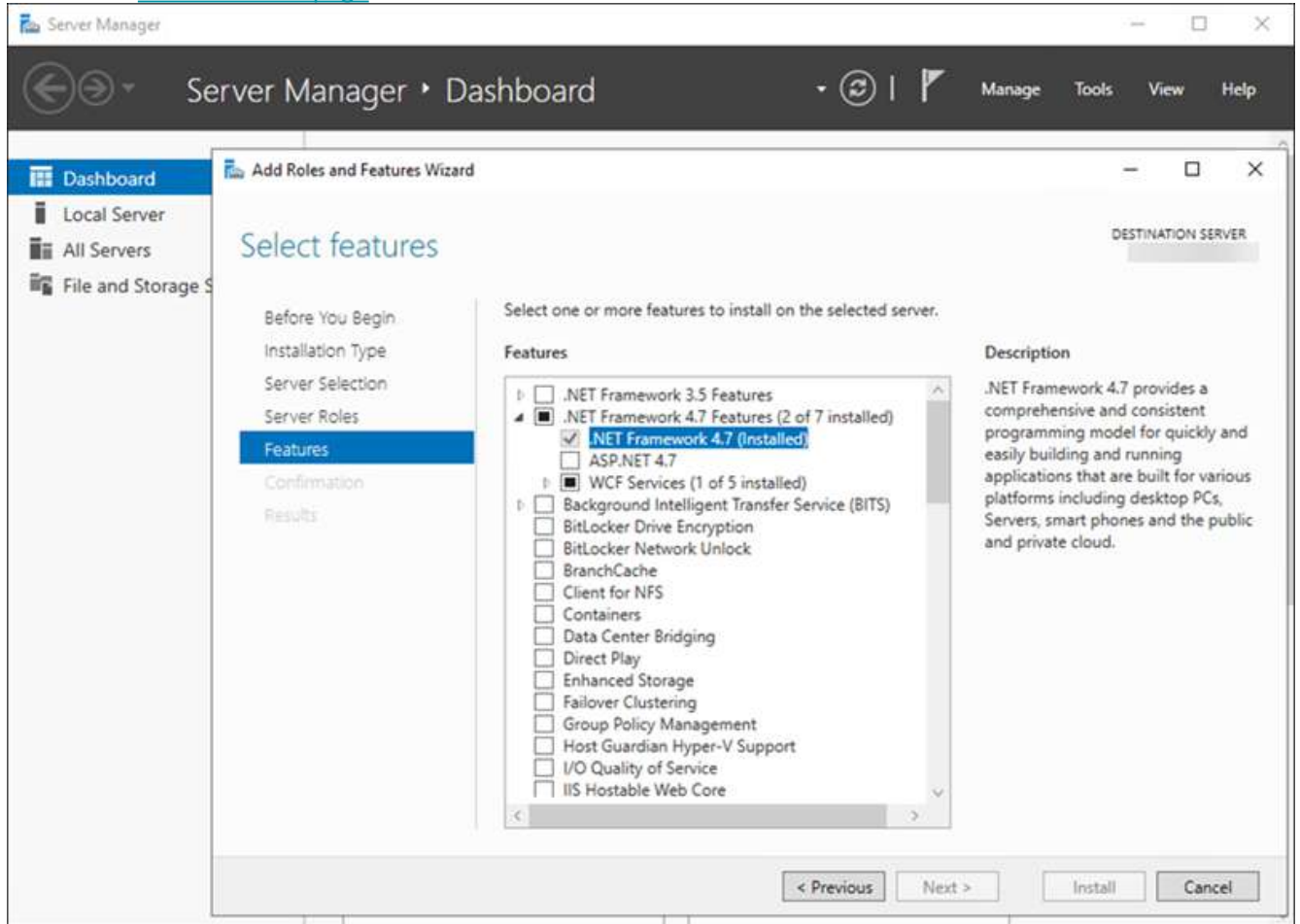
6. If you have selected **Add custom HTTPS certificate for Webconsole**, click **Browse**. Select a valid Certificate (.pfx or .p12 file) and type its **Passphrase**. Leave the field blank if there is no passphrase. The installer will install the certificate for Web Console access on your Tomcat server. Click **Next** to continue.



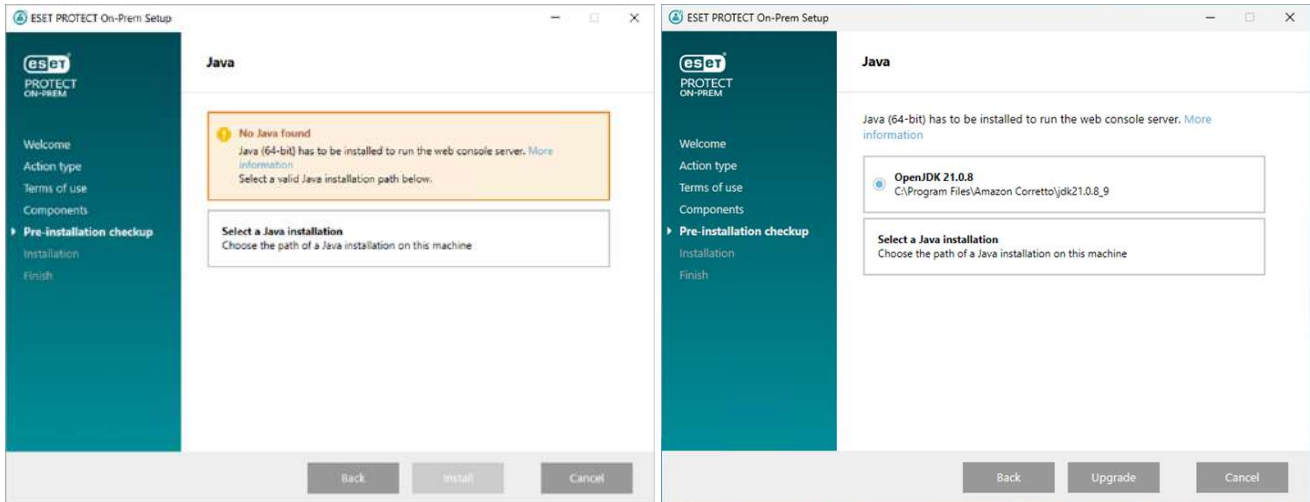
7. If errors appear during the prerequisites check, fix them. Ensure your system meets all [prerequisites](#).

^ [Required version of .NET is not installed](#)

Microsoft SQL Server Express 2022 installation requires Microsoft .NET Framework 4.7.2 or later (SQL 2016 requires .NET 4.6 or later). You can install it using the **Add Roles and Features Wizard** or download and install it from the [Microsoft web page](#).



^ [No Java found / Java \(64-bit\) detected](#)



If your system has multiple Java versions installed, uninstall earlier Java versions and keep only the latest [supported Java](#) version.

 Starting January 2019, Oracle JAVA SE 8 public updates for business, commercial or production use require a commercial license. If you do not purchase a JAVA SE subscription, you can transition to a no-cost alternative. See the [supported versions of JDK](#).

- a) To select the already installed Java, click **Select a Java installation**, select the folder where Java is installed (with a subfolder *bin*, for example, *C:\Program Files\Amazon Corretto\jdk1.8.0\_212*) and click **OK**. The installer prompts you if you have selected an invalid path.
- b) Click **Install** to continue or **change** to change the Java installation path.

#### [Setup is not in valid state/Microsoft SQL Server Express](#)

The installer displays this message for several reasons:

- The installer is corrupted. For example, some installer files are missing. [Download](#) and run the All-in-one installer again.
- The path to the All-in-one installer contains special characters—for example, letters with diacritics. Run the ESET PROTECT All-in-one installer from a path with no special characters.

#### [There is only 32 MB free on a system disk](#)

The installer displays this message if your system does not have enough disk space for ESET PROTECT On-Prem installation.

You need at least 4,400 MB of free disk space to install ESET PROTECT On-Prem.

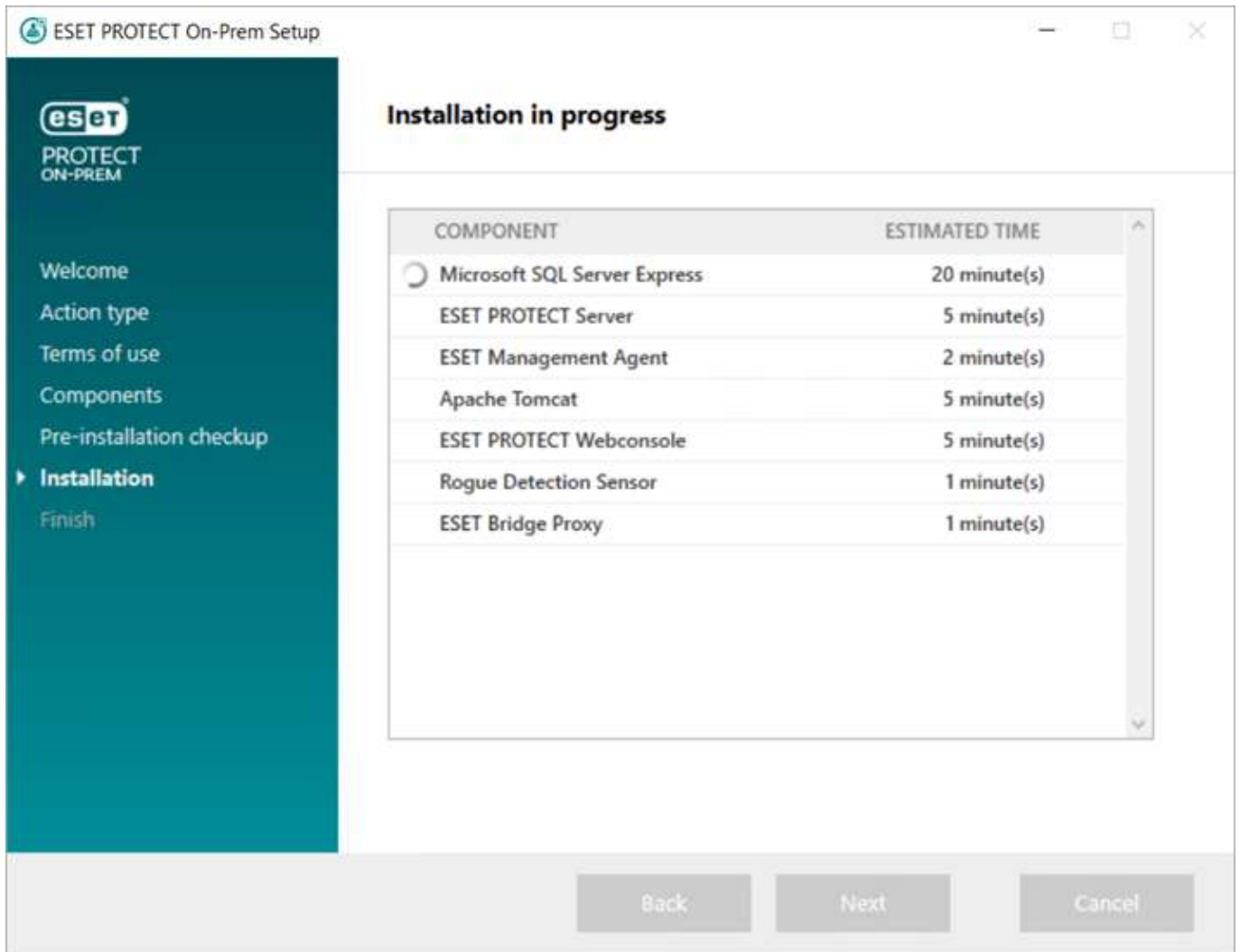
#### [ESET Remote Administrator 5.x or older is installed on the machine](#)

If you have ERA 5.x/6.x or ESMC 7.x, the direct upgrade to ESET PROTECT On-Prem 13.0 is not supported—Perform a clean installation of ESET PROTECT On-Prem 13.0.

You can upgrade to ESET PROTECT On-Prem 13.0 from ESET PROTECT On-Prem 10.1 and later. A direct upgrade from the End of Life versions 8.x–10.0 has not been tested and is not supported.

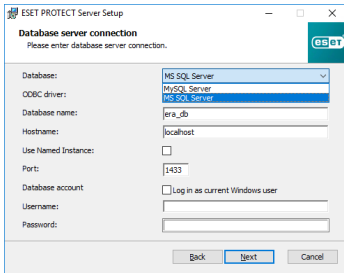
8. When the prerequisites check completes and your environment meets all [requirements](#), the installation begins. Note that installation can take more than an hour, depending on your system and network configuration.

 During installation, the ESET PROTECT On-Prem installation Wizard may not respond.



9. If you chose to install **Microsoft SQL Server Express** in step 5, the installer will perform a database connection check. If you have an existing database server, the installer will prompt you to type your database connection details:

[Configure the connection to SQL/MySQL Server](#)

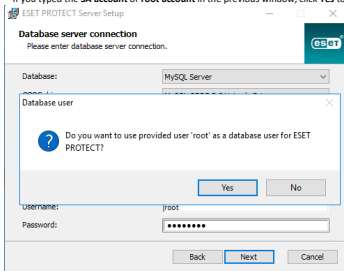


The database stores all data (ESET PROTECT Web Console password, client computer logs, etc.). Configure the **Database server connection**:

- **Database**—MySQL Server/MS SQL Server:
  - Microsoft SQL Server—You can find the **Database name**, **Hostname** and **Port** number in [SQL Server Configuration Manager](#).
  - MySQL Server—You must [configure MySQL to accept large packets](#) for ESET PROTECT On-Prem to run properly because ESET PROTECT Server stores large data blobs in the database.
- **ODBC Driver**
  - Microsoft SQL Server—SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server.
  - MySQL Server—MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/MySQL ODBC 9.2 Unicode Driver/MySQL ODBC 9.3 Unicode Driver/MariaDB ODBC 3.1 Driver.
- **Database name**—We recommend using the pre-defined name or changing it if required.
- **Hostname**—Hostname or the IP address of your database server.
- **Use Named Instance**—If you use a Microsoft SQL database, you can select the **Use Named Instance** check box to use a custom database instance. You can set it in the **Hostname** field in the form `HOSTNAME\DB_INSTANCE` (for example, `192.168.0.10\ESMCSQL`). For a clustered database, use only the cluster name. If this option is selected, you cannot change the database connection port—the system will use default ports determined by Microsoft. To connect the ESET PROTECT Server to the Microsoft SQL database installed in a Failover Cluster, type the cluster name in the **Hostname** field.
- **Port**—The port used for connection to the database server.
- **Database account**—**Username** and **Password**. You can use:
  - OA SA account (Microsoft SQL) or root account (MySQL).
  - OA [dedicated database user account](#) with access to the ESET PROTECT database only.
  - OA domain user (type `domain\username`) with access to the ESET PROTECT database.
- When you select the **Log in as current Windows user** check box, the Microsoft SQL database user (administrator or a [dedicated database user](#)) can use Windows authentication. As a result, the username and password will not be visible in the [StartupConfiguration.ini](#) file.

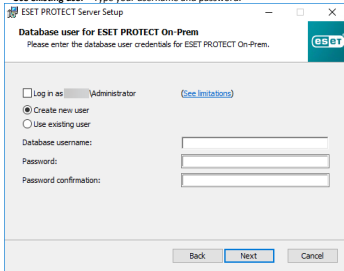
Click **Next**. The installer will verify the database connection:

- If you have an existing database from a previous ESET PROTECT On-Prem installation on your database server, the installer will detect it. You can choose to **Use the existing database and apply upgrade** or **Remove existing database and install a new version**.
- If you typed the **SA account** or **root account** in the previous window, click **Yes** to continue using the SA/root account as the ESET PROTECT database user. If you click **No**, proceed to the next installer window.



Select a database user for ESET PROTECT On-Prem—You have the following options:

- If you have selected **Custom account**, you can select the **Log in as hostname\username** check box.
- **Create new user**—The installer will create a new database user.
- **Use existing user**—Type your username and password.



10. The installer prompts you to type a password for the Web Console Administrator account. This password is important—use the password to log into the [ESET PROTECT Web Console](#).

The password must contain at least 14 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 17 characters.

Click **Next**.

**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

11. Leave the fields unchanged or type your corporate information that will appear in the details of the ESET Management Agent and the ESET PROTECT Server certificates. If you choose to type a password in the **Authority password** field, be sure to remember it.

**!** The password must contain at least 10 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 12 characters.

Click **Next**.

**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]

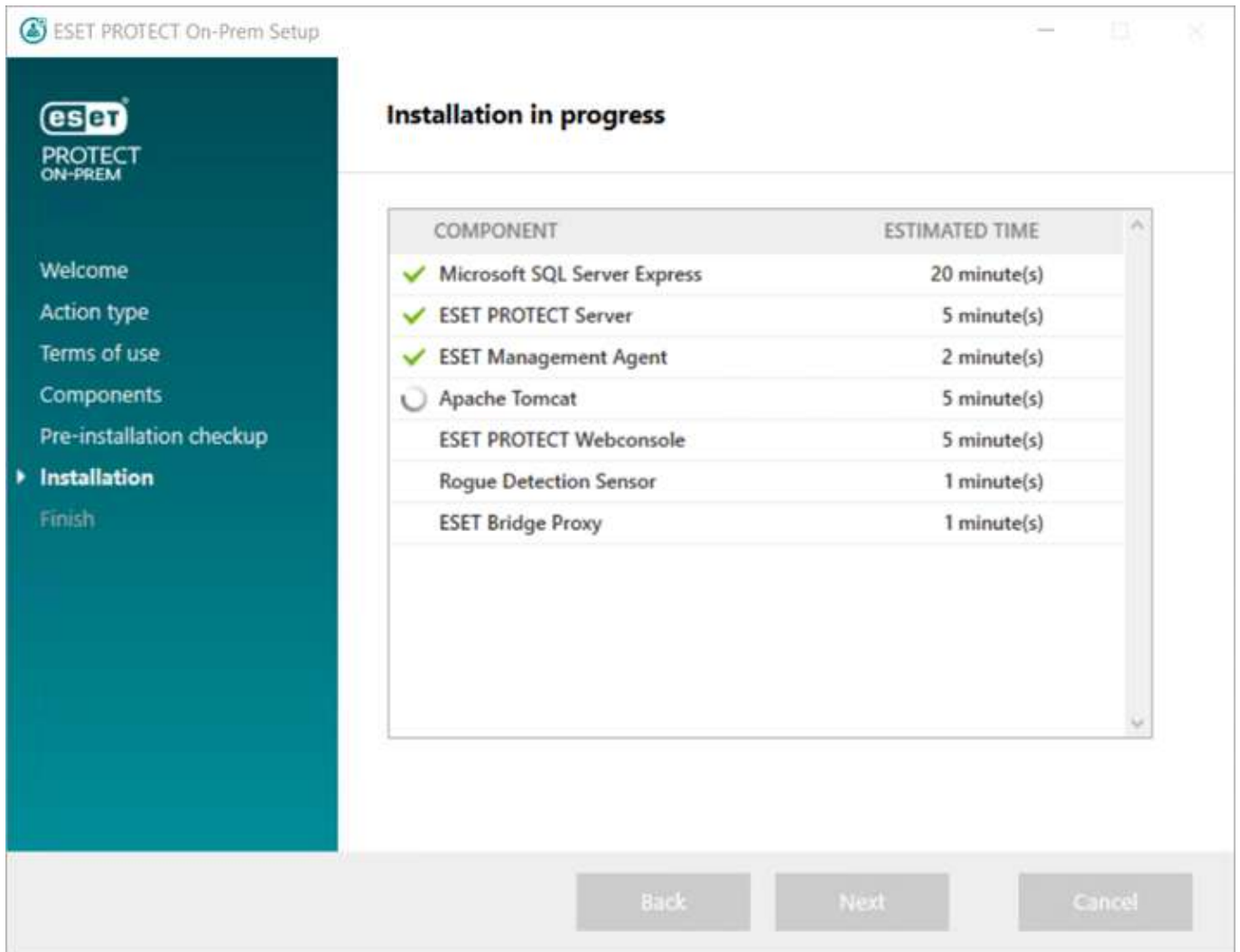
Authority common name: \* Server Certification Authority

Authority password: [Empty]

\* required fields

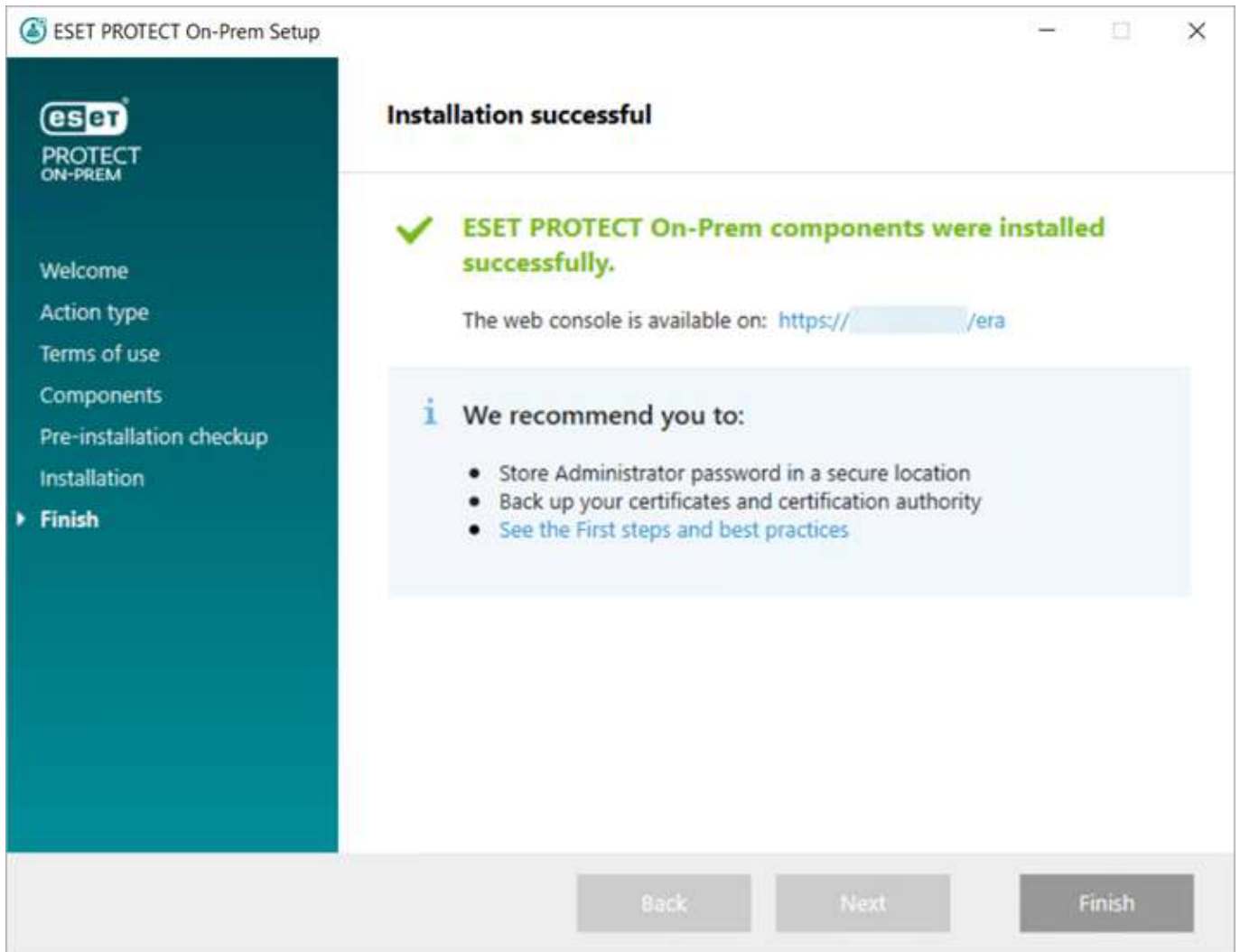
Buttons: Back, Next, Cancel

12. You will see the installation progress.




13. If you selected to install the [Rogue Detection Sensor](#), you will see the installation windows for the WinPcap driver. Ensure to select the check box **Automatically start the WinPcap driver at boot time**.

14. When the installation completes, the message "ESET PROTECT On-Prem components were installed successfully" appears along with your ESET PROTECT Web Console link. Click the link to open the [Web Console](#), or click **Finish**.



If the installation is not successful:

- Review the installation log files in the All-in-one installation package. The logs directory is the same as the directory for the All-in-one installer, for example:  
C:\Users\Administrator\Downloads\x64\logs\
- See [Troubleshooting](#) for additional steps to resolve your issue.

 Do not change the computer name of your ESET PROTECT Server machine after the installation. See [Change of IP address or hostname on ESET PROTECT Server](#) for more information.

## Component installation on Windows

 We recommend using the [ESET PROTECT All-in-one installation](#) on Windows.

Many installation scenarios require you to install different ESET PROTECT components on different machines to accommodate network architectures, meet performance requirements, or for other reasons. The following installation packages are available for individual ESET PROTECT Windows components:

Core components	Download links	Installation instructions
ESET PROTECT Server	<a href="#">server_x64.msi</a>	<a href="#">Server installation—Windows</a>


Core components	Download links	Installation instructions
ESET PROTECT Web Console	<a href="#">era_x64.war</a>	<a href="#">Install Web Console using the All-in-one installer—Windows (recommended)</a> <a href="#">Install Web Console manually—Windows (advanced users)</a>
ESET Management Agent	<a href="#">agent_x64.msi</a> (64-bit) <a href="#">agent_x86.msi</a> (32-bit) <a href="#">agent_arm64.msi</a> (ARM)	<a href="#">Agent installation—Windows</a>
Database server	<a href="#">Microsoft SQL Server</a> <a href="#">MySQL Server</a>	<a href="#">Microsoft SQL Server requirements</a> <a href="#">MySQL Server installation and configuration—Windows</a>

Optional components	Download links	Installation instructions
ESET Bridge (HTTP proxy)	<a href="#">esetbridge_nt64.msi</a>	<a href="#">Deploy ESET Bridge</a>
Mirror Tool	<a href="#">mirrortool_win_x64.zip</a>	<a href="#">Mirror Tool—Windows</a>
ESET Rogue Detection Sensor	<a href="#">rdsensor_x64.msi</a> (64-bit) <a href="#">rdsensor_x86.msi</a> (32-bit)	<a href="#">RD Sensor installation—Windows</a>

Custom installation scenarios include:

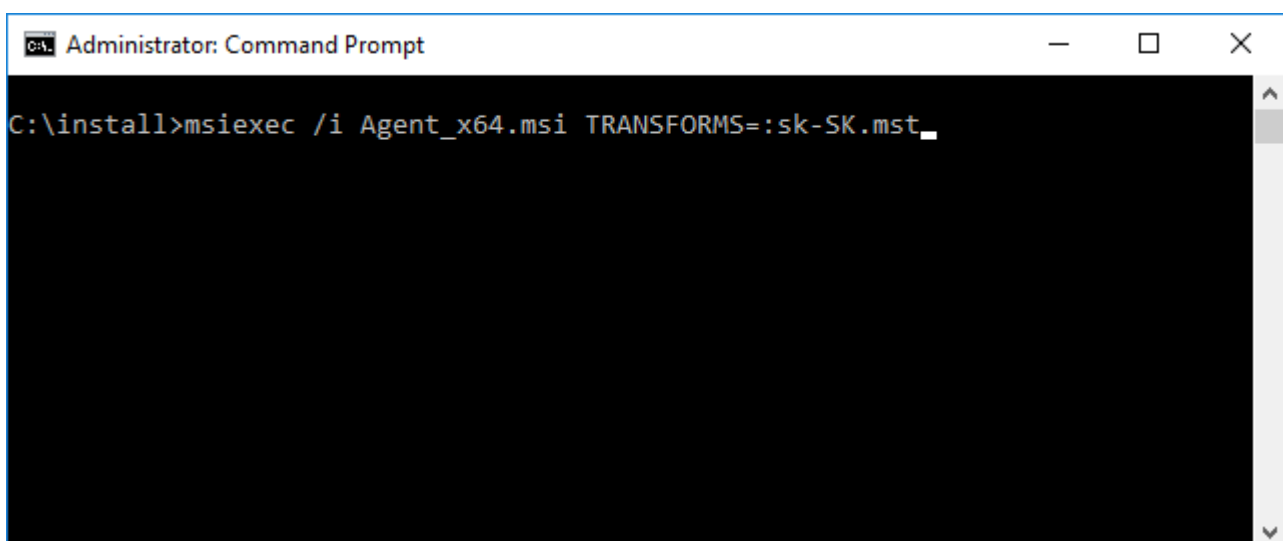
- Installation with [Custom certificates](#)
- Installation on a [Failover Cluster](#)

For instructions to upgrade earlier ESET PROTECT On-Prem to the latest ESET PROTECT On-Prem 13.0, see the [upgrade procedures](#).

 ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

If you want to run the installation in your local language, you need to start the MSI installer of a specific ESET PROTECT component via the command line.

Below is an example of how to run the installation in the Slovak language:



To select the language you want to run the installer in, specify the corresponding TRANSFORMS parameter

according to this table:

Language	Code
English (United States)	en-US
Arabic (Egypt)	ar-EG
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Croatian (Croatia)	hr-HR
Czech (Czech Republic)	cs-CZ
French (France)	fr-FR
French (Canada)	fr-CA
German (Germany)	de-DE
Greek (Greece)	el-GR
Hungarian (Hungary)*	hu-HU
Indonesian (Indonesia)*	id-ID
Italian (Italy)	it-IT
Japanese (Japan)	ja-JP
Korean (Korea)	ko-KR
Polish (Poland)	pl-PL
Portuguese (Brazil)	pt-BR
Russian (Russia)	ru-RU
Spanish (Chile)	es-CL
Spanish (Spain)	es-ES
Slovak (Slovakia)	sk-SK
Turkish (Turkey)	tr-TR
Ukrainian (Ukraine)	uk-UA

\* Only the application is available in this language; Online Help is not available.

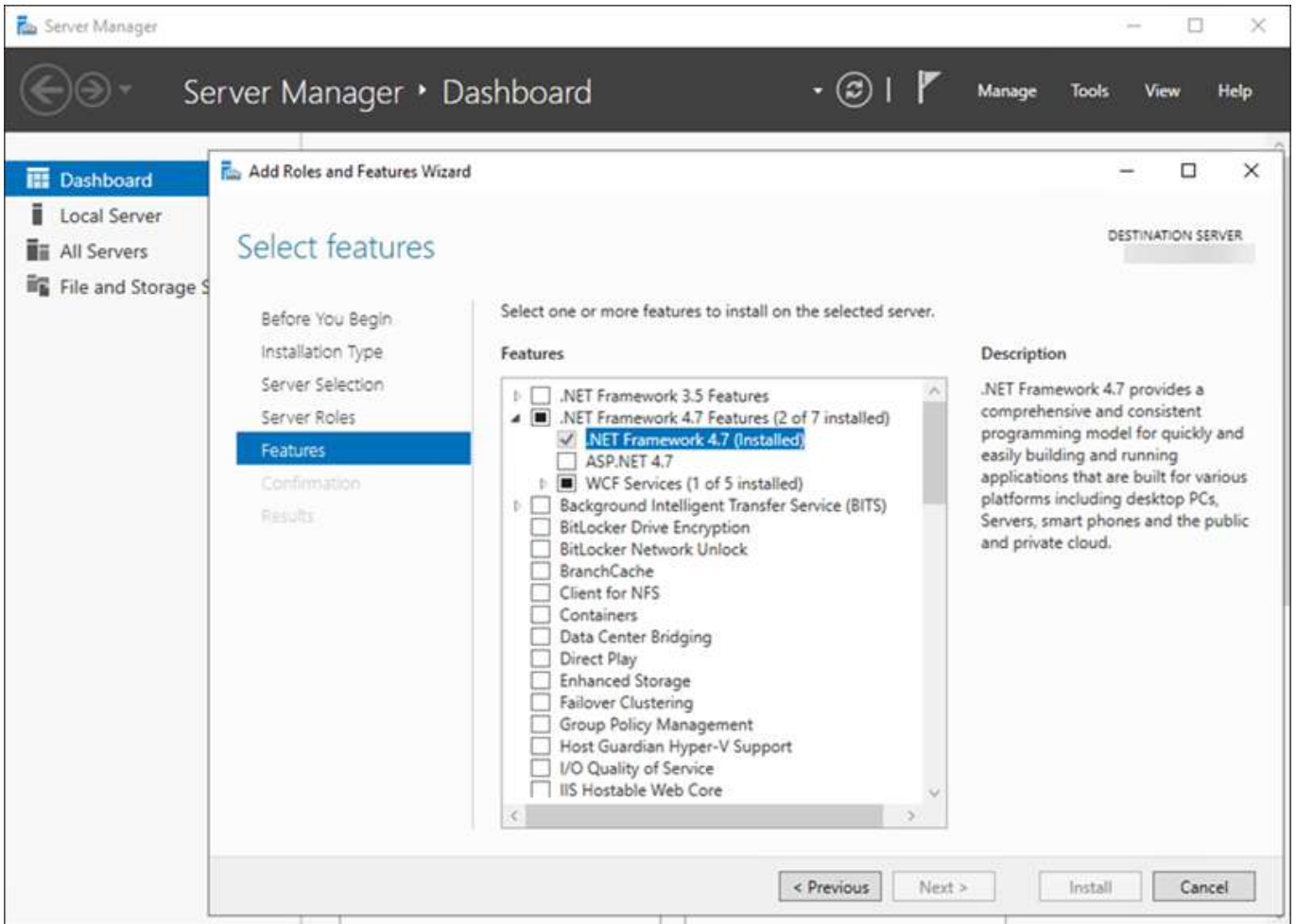
## Server installation—Windows

**i** We recommend using the [ESET PROTECT All-in-one installation](#) on Windows.

### Prerequisites

- You must have a [supported Windows operating system](#).
- The required ports must be open and available—see the complete [list of ports](#).
- The [supported database server and connector](#) ([Microsoft SQL Server](#) or [MySQL](#)) are installed and running. We recommend that you review the database server configuration details ([Microsoft SQL Server](#) or [MySQL](#)) to have the database properly configured for use with ESET PROTECT On-Prem. Read our [Knowledgebase article](#) to set up your database and database user for Microsoft SQL or MySQL.

- [ESET PROTECT Web Console installed](#) to manage the ESET PROTECT Server.
- Microsoft SQL Server Express 2022 installation requires Microsoft .NET Framework 4.7.2 or later (SQL 2016 requires .NET 4.6 or later). You can install it using the **Add Roles and Features Wizard** or download and install it from the [Microsoft web page](#).



## Installation

Follow the steps below to install the ESET PROTECT Server component on Windows:

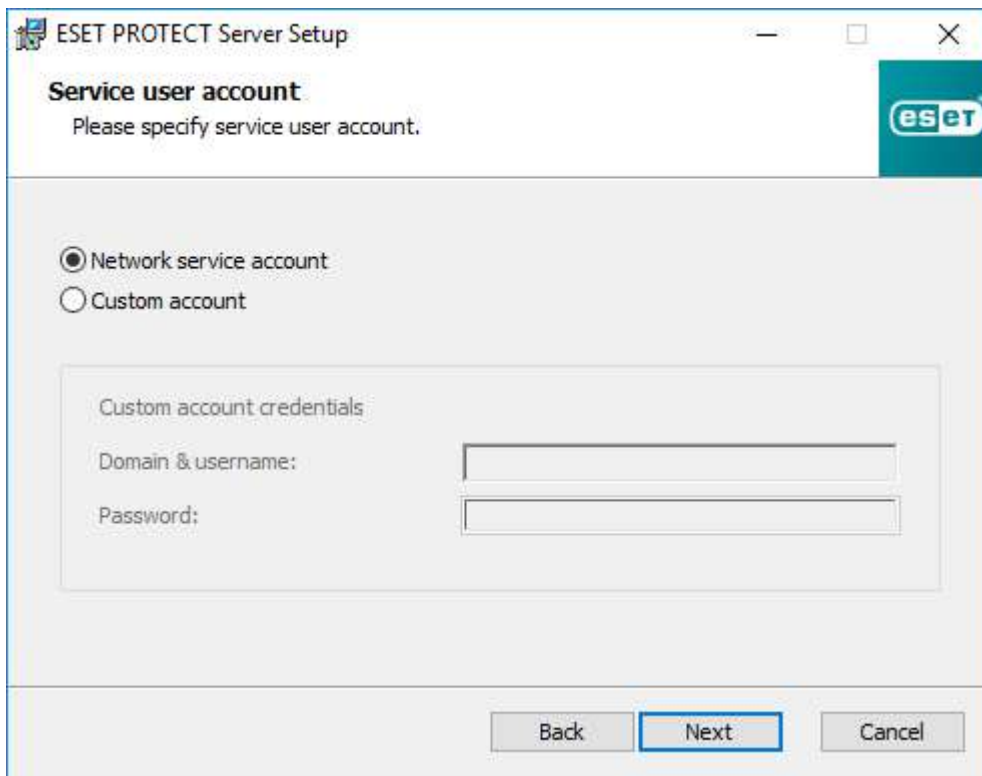
**!** Ensure to meet all the installation prerequisites listed above.

1. Visit the ESET PROTECT [download section](#) to download a standalone installer for this ESET PROTECT component (*server\_x64.msi*).
2. Run the ESET PROTECT Server installer and select **I accept the Terms of Use**.
3. Select the **Participate in product improvement program** check box to send anonymous telemetry data and crash report to ESET (operating system version and type, ESET application version and other application-specific information).
4. Leave the check box next to **This is cluster installation** empty and click **Next**. [Is this a cluster installation?](#)

**!** If you are installing ESET PROTECT Server on a Failover Cluster, select the check box next to **This is cluster installation**. Specify the **Custom application data path** to point to the shared storage for the cluster. The data must be stored at one location that is accessible by all nodes within the cluster.

5. Select a **Service user account**. This account will be used to run the ESET PROTECT Server service. The following options are available:

- **Network service account**—Select this option if you do not use a domain.
- **Custom account**—Select this option if you use a domain—Provide domain user credentials: DOMAIN\USERNAME and password. You can create and use a [dedicated Microsoft SQL database user](#).

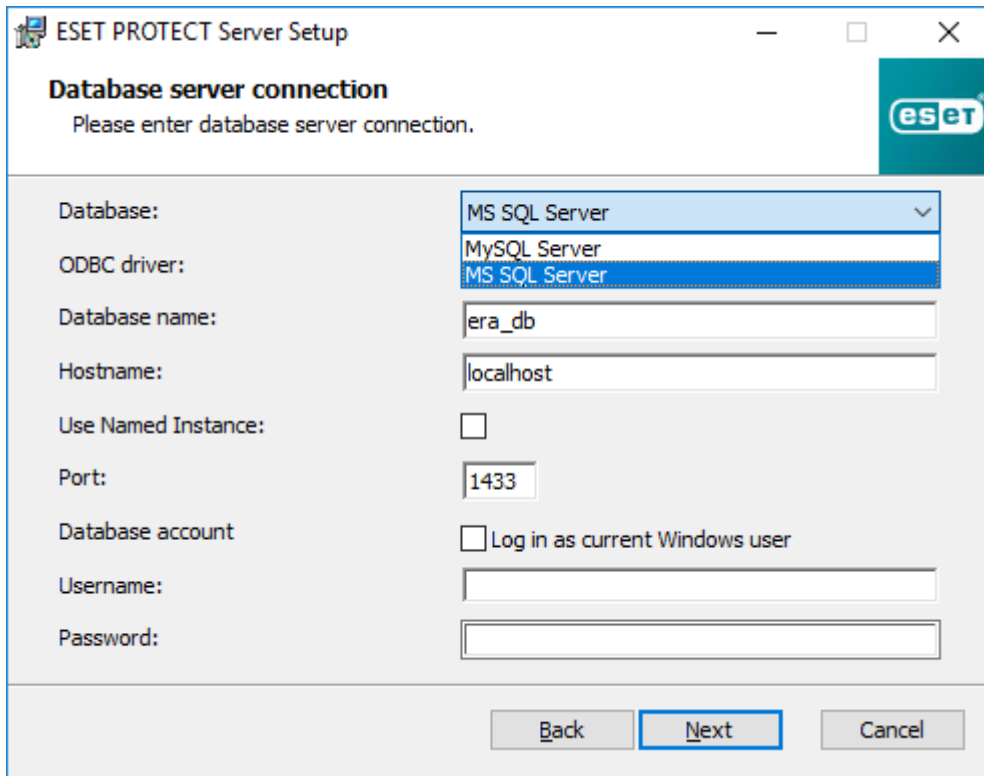


The screenshot shows the 'ESET PROTECT Server Setup' window. The title bar includes the ESET logo and standard window controls. The main heading is 'Service user account' with the instruction 'Please specify service user account.' Below this, there are two radio button options: 'Network service account' (which is selected) and 'Custom account'. Under the 'Custom account' option, there is a section titled 'Custom account credentials' containing two text input fields: 'Domain & username:' and 'Password:'. At the bottom of the window, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'.

6. Connect to a Database. All data is stored here (ESET PROTECT Web Console password, client computer logs, etc.).

### Server upgrade using the standalone Server installer

**!** If you copy the database password from the [StartupConfiguration.ini](#) file and the password contains the @ character, delete the escape character \ before it.



The database stores all data (ESET PROTECT Web Console password, client computer logs, etc.). Configure the **Database server connection**:

- **Database**—MySQL Server/MS SQL Server:

○Microsoft SQL Server—You can find the **Database name**, **Hostname** and **Port** number in [SQL Server Configuration Manager](#).

○MySQL Server—You must [configure MySQL to accept large packets](#) for ESET PROTECT On-Prem to run properly because ESET PROTECT Server stores large data blobs in the database.


- **ODBC Driver**

○Microsoft SQL Server—SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server.

○MySQL Server—MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/MySQL ODBC 9.2 Unicode Driver/MySQL ODBC 9.3 Unicode Driver/MariaDB ODBC 3.1 Driver.

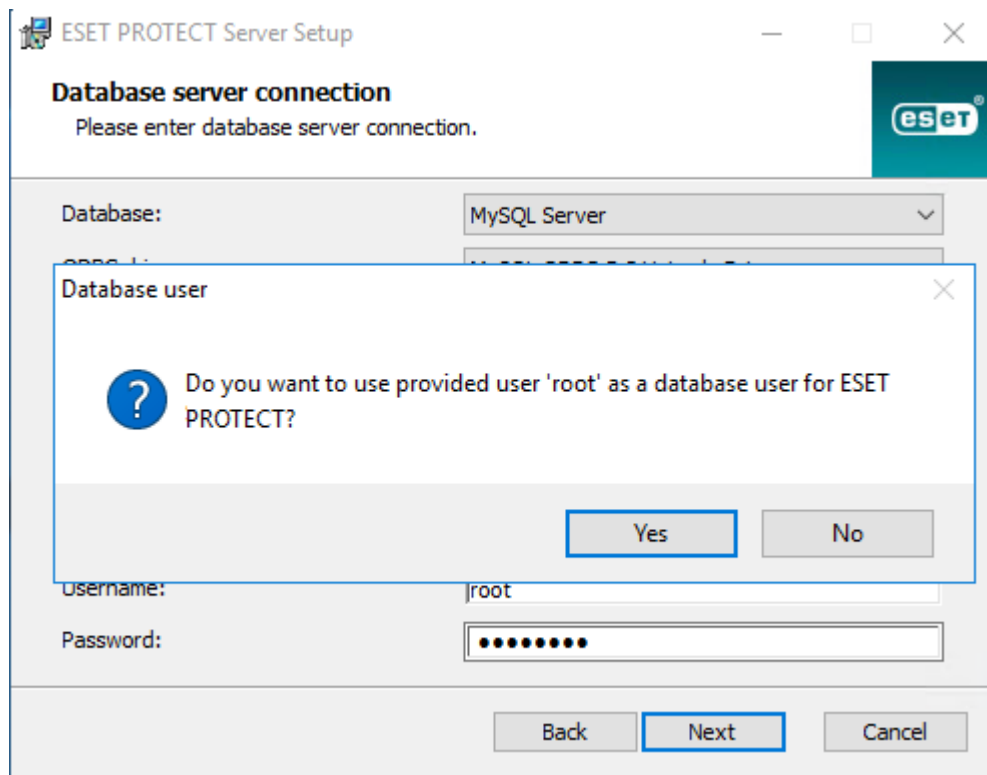
- **Database name**—We recommend using the pre-defined name or changing it if required.
- **Hostname**—Hostname or the IP address of your database server.
- **Use Named Instance**—If you use a Microsoft SQL database, you can select the **Use Named Instance** check box to use a custom database instance. You can set it in the **Hostname** field in the form *HOSTNAME\DB\_INSTANCE* (for example, *192.168.0.10\ESMCTSQL*). For a clustered database, use only the cluster name. If this option is selected, you cannot change the database connection port—the system will use default ports determined by Microsoft. To connect the ESET PROTECT Server to the Microsoft SQL database installed in a Failover Cluster, type the cluster name in the **Hostname** field.
- **Port**—The port used for connection to the database server.

- **Database account—Username and Password.** You can use:
  - o An **SA account** (Microsoft SQL) or **root account** (MySQL).
  - o A [dedicated database user account](#) with access to the ESET PROTECT database only.
  - o A domain user (type `domain\username`) with access to the ESET PROTECT database.
- When you select the **Log in as current Windows user** check box, the Microsoft SQL database user (administrator or a [dedicated database user](#)) can use Windows authentication. As a result, the username and password will not be visible in the [StartupConfiguration.ini](#) file.

 If you select **Log in as current Windows user** and use a dedicated Microsoft SQL database user (not the database administrator), the [ESET PROTECT Components Upgrade](#) task will be unable to upgrade the ESET PROTECT Server in the future. The ESET PROTECT Server upgrade, repair and removal will require entering the password of the custom domain user.

Click **Next**. The installer will verify the database connection:

- If you have an existing database from a previous ESET PROTECT On-Prem installation on your database server, the installer will detect it. You can choose to **Use the existing database and apply upgrade** or **Remove existing database and install a new version**.
- If you typed the **SA account** or **root account** in the previous window, click **Yes** to continue using the SA/root account as the ESET PROTECT database user. If you click **No**, proceed to the next installer window.




7. Select a database user for ESET PROTECT On-Prem—You have the following options:

- If you have selected **Custom account**, you can select the **Log in as hostname\username** check box.

- **Create new user**—The installer will create a new database user.
- **Use existing user**—Type your username and password.

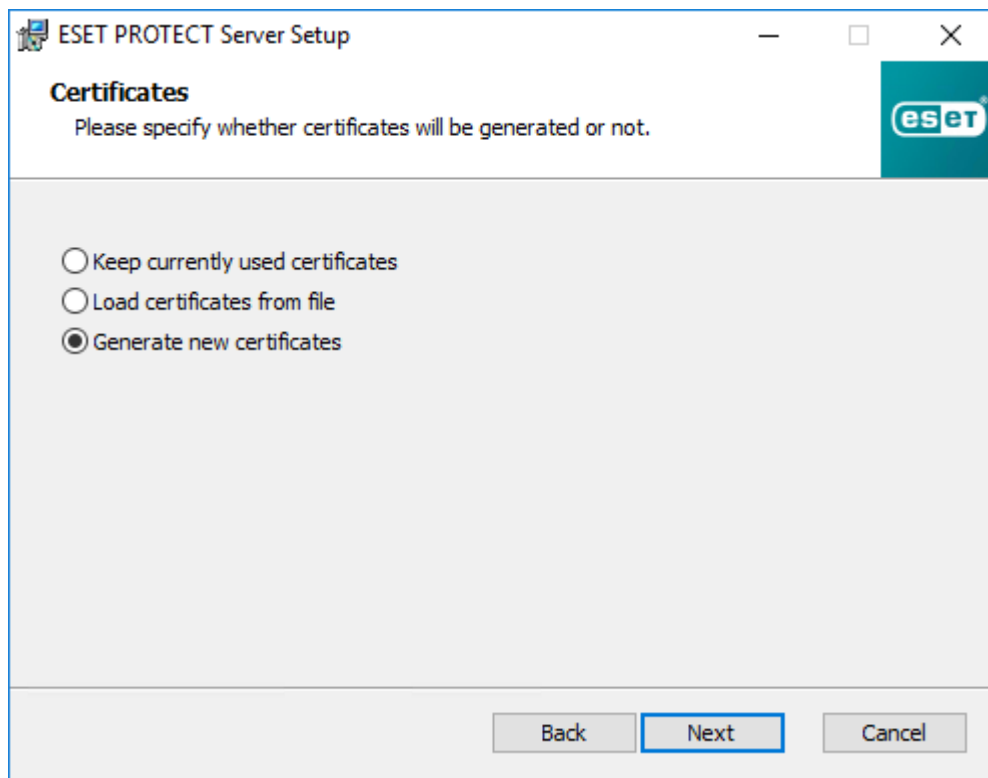
8. Type a password for **Web Console** access.

 The password must contain at least 14 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 17 characters.

9. ESET PROTECT On-Prem uses certificates for client-server communication. Select one of the following

options:

- **Keep currently used certificates**—This option is available only if the database was already used with another ESET PROTECT Server before.
- **Load certificates from file**—Select your existing Server certificate and Certification Authority.
- **Generate new certificates**—The installer generates new certificates.



10. Follow this step if you have selected the **Generate new certificates** option in the previous step.

a) Specify additional information about the certificates (optional). If you type the **Authority password**, be sure to remember it.



The password must contain at least 10 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 12 characters.

**ESET PROTECT Server Setup**

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

Organizational unit:

Organization:

Locality:

State / Country:  ▼

Certificate validity: \*  Years ▼

Authority common name: \*

Authority password:

\* required fields

Back Next Cancel

b) In the **Server Certificate** field, type the **Server hostname** and a **Certificate password** (optional).

**Server hostname** in the Server certificate must not contain any of the following keywords: `server`, `proxy`, `agent`.  
 To be able to use the [REST API](#) in the ESET PROTECT Server, **Server hostname** must contain `localhost` as one of its entries.

The password must contain at least 10 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 12 characters.

**ESET PROTECT Server Setup**

**Server certificate**  
Please enter server certificate information below.

Server hostname:

Certificate password:

Password confirmation:

Back Next Cancel

c) In the **Peer certificate password** field, type the password for Agent and Proxy Peer certificates.



The password must contain at least 10 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 12 characters.

The screenshot shows a window titled "ESET PROTECT Server Setup" with a sub-header "Peer certificate password". Below the sub-header is the instruction: "Please enter password for peer certificates which will be generated." There are two text input fields: "Password:" and "Password confirmation:". At the bottom of the window are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel". The ESET logo is visible in the top right corner of the window.

11. Setup can perform an initial [Static Group Synchronization](#) task. Select the method (**Do not synchronize, Sync with Windows Network, Sync with Active Directory**) and click **Next**.

12. Confirm or change the installation folder for the server and click **Next**.

13. Click **Install** to install the ESET PROTECT Server.



When you have completed the ESET PROTECT Server installation, you can install [ESET Management Agent](#) on the same machine (optional) to enable managing the Server the same way you manage a client computer.



Do not change the computer name of your ESET PROTECT Server machine after the installation. See [Change of IP address or hostname on ESET PROTECT Server](#) for more information.

## Microsoft SQL Server requirements

The following requirements for Microsoft SQL Server must be met:

- Install a [supported version of Microsoft SQL Server](#). Choose **Mixed mode** authentication during installation.
- If you have Microsoft SQL Server already installed, set authentication to **Mixed mode (SQL Server authentication and Windows authentication)**. To do so, follow the instructions in this [Knowledgebase article](#). If you want to use **Windows Authentication** to log in to Microsoft SQL Server, follow the steps in this [Knowledgebase article](#).

- Allow TCP/IP connections to the SQL Server. To do so, follow the steps in this [Knowledgebase article](#) from part II. **Allow TCP/IP connections to the SQL database.**

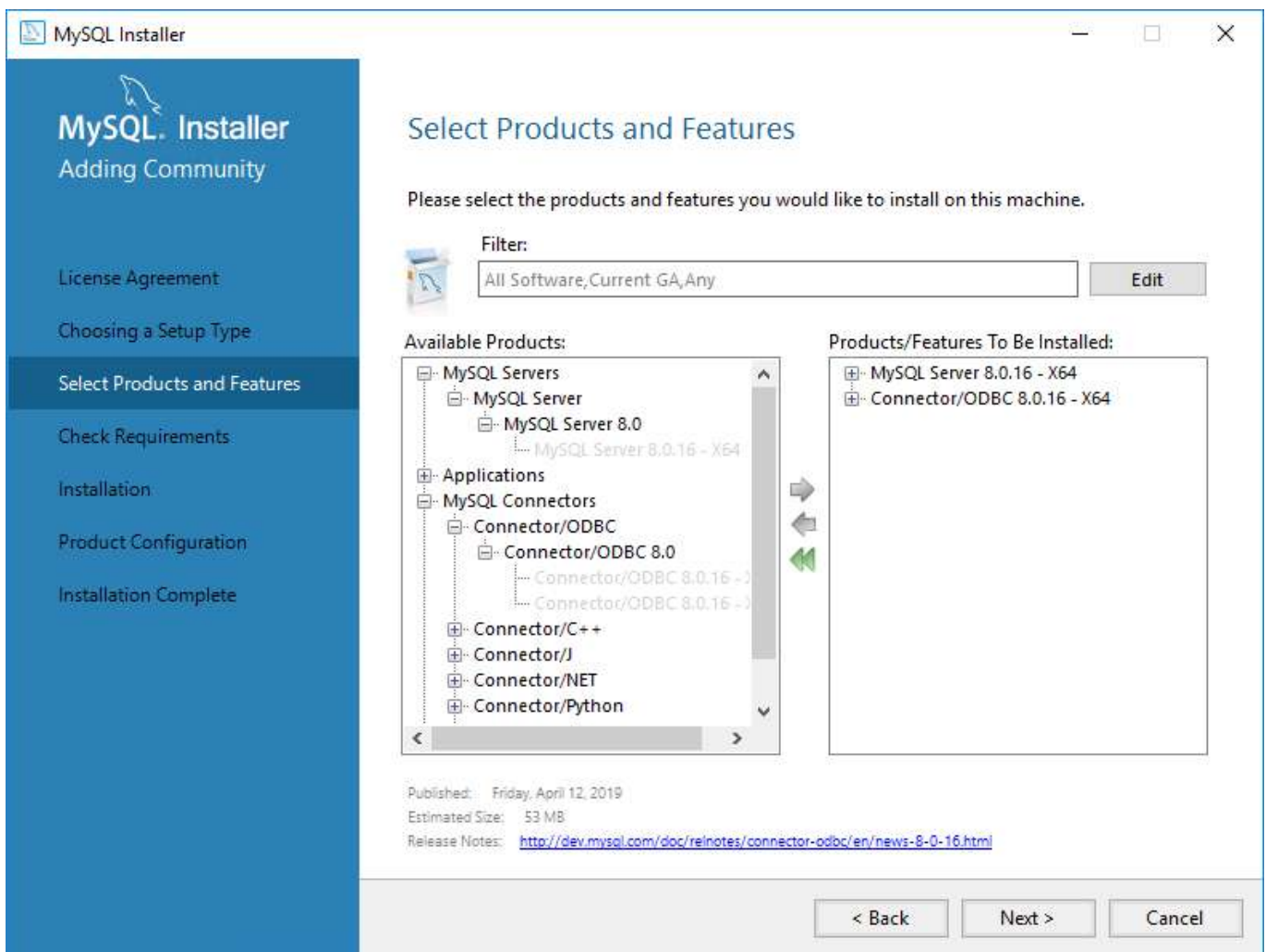
**i** • To configure, manage and administer Microsoft SQL Server (databases and users), [download SQL Server Management Studio \(SSMS\)](#).  
• [Do not install SQL Server on a Domain Controller](#). Install ESET PROTECT On-Prem on a different server or deselect the SQL Server Express component during installation. Use your existing SQL or MySQL Server to run the ESET PROTECT database.

# MySQL Server installation and configuration—Windows

## Installation

Ensure to install a [supported version of MySQL Server and ODBC Connector](#).

1. Download the MySQL 8 Windows installer from <https://dev.mysql.com/downloads/installer/> and execute it.
2. Select the check box **I accept the license terms** and click **Next**.
3. During the installation setup, select **Custom** and select **MySQL Server** and **Connector/ODBC** to install. Ensure that ODBC Connector matches the bitness of the installed MySQL Server (x86 or x64).



4. Click **Next** and **Execute** to install the MySQL Server and ODBC Connector.

- Click **Next**. In **High Availability**, select **Standalone MySQL Server / Classic MySQL Replication** and click **Next**.
- In **Type and Networking**, select **Server Computer** from the **Config Type** drop-down menu and click **Next**.
- In the **Authentication Method**, select the recommended option **Use Strong Password Encryption for Authentication** and click **Next**.

**i** The ESET PROTECT Server supports only the default MySQL database authentication method: `caching_sha2_password`.

- In **Accounts and Roles**, type your **MySQL Root Password** twice. We recommend that you also create a [dedicated database user account](#).
- In **Windows Service**, keep the pre-selected values and click **Next**.
- Click **Execute** and wait until MySQL Server installation completes. Click **Finish**, **Next** and **Finish** to close the installation window.

## Configuration

- Open the following file in a text editor:

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

- Find and edit or append the following configuration in the `[mysqld]` section of the `my.ini` file:

- Create the `[mysqld]` section if it is not present in the file.
- If the parameters are not present in the file, add them to the `[mysqld]` section.
- To determine your MySQL version, run the command: `mysql --version`

Parameter	Comments and recommended values	MySQL version
<code>max_allowed_packet=33M</code>		All the <a href="#">supported versions</a> .
<code>log_bin_trust_function_creators=1</code>	Alternatively, you can disable the binary logging: <code>log_bin=0</code>	8.x
<code>innodb_log_file_size=100M</code> <code>innodb_log_files_in_group=2</code>	The multiplication of values of these two parameters must be at least <b>200</b> . The minimum value for <code>innodb_log_files_in_group</code> is <b>2</b> and maximum value is <b>100</b> ; the value also must be integer.	8.x

- Save and close the `my.ini` file.
- Open the Command Prompt and type the following commands to restart the MySQL server and apply the configuration (the process name depends on the MySQL version: 8.0 = `mysql80` etc.):

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

- Type the following command in Command Prompt to check whether the MySQL server is running:

## Dedicated database user account

If you do not want to use an **SA account** (Microsoft SQL) or **root account** (MySQL), you can create a **dedicated database user account**. This dedicated user account will be used to access the ESET PROTECT database only. We recommend that you create a dedicated database user account within your database server before starting ESET PROTECT On-Prem installation. Also, you will need to create an empty database that will be accessed by ESET PROTECT On-Prem using this dedicated user account.

There is a minimum set of privileges that must to be granted to a dedicated database user account:

- MySQL user privileges: ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, SELECT, UPDATE, TRIGGER. For more information about MySQL privileges, see <https://dev.mysql.com/doc/refman/8.0/en/grant.html>.
- Microsoft SQL Server database-level roles: An ESET PROTECT database user must be a member of the db\_owner database role. For more information about Microsoft SQL Server database-level roles, see <https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspx>

### A dedicated Microsoft SQL database user with Windows authentication

You can set up a Windows user as a dedicated Microsoft SQL database user with Windows authentication:


- During the database installation—Select **Mixed Mode (SQL Server authentication and Windows authentication)**
- When the database is installed—Use the SQL Server Management Studio > in the **Object Explorer**, expand **Security** > right-click **Logins** > **New Login** > type the Login name in the format `HOSTNAME\username` > select **Windows Authentication** > click **Server Roles** > select **public** and **sysadmin**. If you select **Log in as current Windows user** during the ESET PROTECT Server installation ([all-in-one](#) or [standalone](#) installation), the username and password are not visible in the `startupconfiguration.ini` file. You see `Trusted_Connection=yes` instead. See also [Connect ESET PROTECT Server to a database](#).

You can find detailed guide how to set up your database and user account for both Microsoft SQL and MySQL in our [Knowledgebase article](#).

## Agent installation—Windows

### Available methods

There are various installation and deployment methods available for ESET Management Agent installation on Windows workstations:

Method	Documentation	Description
GUI based installation from the <code>.msi</code> installer	<ul style="list-style-type: none"> <li>• <a href="#">This chapter</a></li> <li>• <a href="#">KB</a></li> </ul>	<ul style="list-style-type: none"> <li>• The standard (offline) installation method.</li> <li>• Use this method when installing Agent on ESET PROTECT Server machine.</li> <li>•  ESET Management Agent 12.0 and later no longer supports the server-assisted installation.</li> </ul>
ESET Remote Deployment Tool	<ul style="list-style-type: none"> <li>• <a href="#">Online Help</a></li> </ul>	<ul style="list-style-type: none"> <li>• Recommended for mass-deployment over local network.</li> <li>• Can be used to deploy All-in-one installer (Agent + ESET security application)</li> </ul>
All-in-one Agent installer	<ul style="list-style-type: none"> <li>• <a href="#">Create an All-in-one Agent installer</a></li> <li>• <a href="#">KB</a></li> </ul>	<ul style="list-style-type: none"> <li>• The installer can include also a security application and embedded policy.</li> <li>• The size of the installer is several hundreds of MBs.</li> </ul>
Agent script installer	<ul style="list-style-type: none"> <li>• <a href="#">Create Agent script installer</a></li> <li>• <a href="#">KB</a></li> </ul>	<ul style="list-style-type: none"> <li>• The installer is an executable script. It has a small size but it needs access to location of <code>.msi</code> installer.</li> <li>• The script can be edited to use local installer and HTTP Proxy.</li> </ul>
SCCM and GPO deployment	<ul style="list-style-type: none"> <li>• <a href="#">SCCM</a></li> <li>• <a href="#">GPO</a></li> <li>• <a href="#">KB</a></li> </ul>	<ul style="list-style-type: none"> <li>• Advanced method of remote mass-deployment.</li> <li>• Using a small <code>.ini</code> file.</li> </ul>

Method	Documentation	Description
Server task—Agent Deployment	<ul style="list-style-type: none"> <li>• <a href="#">Online Help</a></li> <li>• <a href="#">KB</a></li> </ul>	<ul style="list-style-type: none"> <li>• An alternative to SCCM and GPO.</li> <li>• It is not viable through HTTP Proxy.</li> <li>• Executed by ESET PROTECT Server from the ESET PROTECT Web Console.</li> <li>• Use this method to deploy the ESET Management Agent to the <a href="#">computers synchronized from the Active Directory</a>.</li> </ul>



The communication protocol between Agent and ESET PROTECT Server does not support authentication. Any proxy solution used for forwarding Agent communication to ESET PROTECT Server that requires authentication will not work. If you choose to use a non-default port for the Web Console or Agent, it may require a firewall adjustment. Otherwise, the installation may fail.

## GUI based installation



ESET Management Agent 12.0 and later no longer supports the server-assisted installation.

Follow the steps below to install the ESET Management Agent component locally on Windows:

1. Visit the ESET PROTECT [download section](#) to download a standalone installer for this ESET PROTECT component (*agent\_x86.msi* or *agent\_x64.msi* or *agent\_arm64.msi*).
2. Run the ESET Management Agent installer and select **I accept the terms in the License Agreement**.
3. Select the **Participate in product improvement program** check box to send anonymous telemetry data and crash report to ESET (operating system version and type, ESET application version and other application-specific information).
4. Type the **Server host** (hostname or IP address of your ESET PROTECT Server) and **Server port** (the default port is 2222, if you are using a different port, replace the default port with your custom port number).



Ensure the **Server host** matches at least one of the values (ideally be FQDN) defined in the **Host** field of the **Server certificate**. Otherwise you will get an error saying "Received server certificate is not valid". Using the wildcard (\*) in the Server certificate Host field, will allow the certificate to work with any **Server host**.

5. If you use proxy for Agent—Server connection, select the check box next to **Use Proxy**. Provide the **Proxy hostname**, **Proxy port** (the default port is 3128), **Username** and **Password** and click **Next**.



This proxy setting is used only for (replication) between ESET Management Agent and ESET PROTECT Server, not for the caching of updates.

- **Proxy hostname:** hostname or IP address of the HTTP Proxy machine.
- **Proxy port:** default value is 3128.
- **Username, Password:** type the credentials used by your proxy if it uses authentication.

You can change proxy settings later in your [policy](#). [Proxy](#) must be installed before you can configure an Agent—Server connection via Proxy.

6. Click **Browse** and navigate to the location of your Peer certificate (this is the Agent certificate you exported from ESET PROTECT On-Prem). Leave the **Certificate password** text field blank as this certificate does not require a password. You do not need to browse for a **Certification Authority**—leave this field empty. The Agent certificate and a Certification Authority can be [exported](#) from ESET PROTECT On-Prem.



If you are using a [custom certificate](#) with ESET PROTECT On-Prem (instead of the default ones that was automatically generated during ESET PROTECT On-Prem installation), use your custom certificates accordingly.



- The certificate passphrase must not contain the following characters: " \ These characters cause a critical error during Agent initialization.
- The password must contain at least 14 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 17 characters.

7. Click **Next** to install to the default folder or click **Change** to choose another folder (we recommend that you use the default location).

8. Click **Next** and **Install** to finish the Agent installation.

## Command line installation

MSI installer can be run locally or remotely. Download the ESET Management Agent from the ESET [website](#).

Parameter	Description and allowed values
P_HOSTNAME=	Hostname or IP address of ESET PROTECT Server.
P_PORT=	Server port for Agent connection (optional; if not specified the default port 2222 is used).
P_CERT_PATH=	Path to the Agent Certificate in Base64 format in .txt file ( <a href="#">exported from ESET PROTECT Web Console</a> ).
P_CERT_AUTH_PATH=	Path to the Certification Authority in Base64 format in .txt file ( <a href="#">exported from ESET PROTECT Web Console</a> ).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	<b>YES</b> ; Use this parameter when you refer to Agent certificate and Certification Authority stored in .txt files.
P_CERT_PASSWORD=	Use this parameter to provide a password for Agent certificate.
P_CERT_CONTENT=	Agent certificate string in Base64 format ( <a href="#">exported from ESET PROTECT Web Console</a> ).
P_CERT_AUTH_CONTENT=	Certification Authority string in Base64 format ( <a href="#">exported from ESET PROTECT Web Console</a> ).
PASSWORD=	Password for the uninstallation of a <a href="#">password-protected Agent</a> .
P_ENABLE_TELEMETRY=	<b>0</b> —disabled (default option); <b>1</b> —enabled. Sending of crash reports and telemetry data to ESET (optional parameter).
P_INSTALL_MODE_EULA_ONLY=	<b>1</b> ; Use this parameter for semi-silent ESET Management Agent installation. You can see Agent installation window and you are prompted to accept the Terms of Use and enable/disable the telemetry (P_ENABLE_TELEMETRY is ignored when specified). Other Agent installation settings are taken from the command line parameters. You can see the completion of Agent installation process.
P_USE_PROXY=	<b>1</b> ; Use this parameter to enable using of HTTP Proxy (which is already installed in your network) for replication between ESET Management Agent and ESET PROTECT Server (not for caching of updates).
P_PROXY_HTTP_HOSTNAME=	Hostname or IP address of HTTP Proxy.
P_PROXY_HTTP_PORT=	HTTP Proxy port for Agent connection.

## Examples of command line installation

Replace the orange code below as necessary.

- Silent installation (/q parameter) with default port connection, enabled telemetry and Agent certificate and Certification Authority stored in files:

```
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
```

- Silent installation with provided strings for Agent certificate and for Certification Authority and Agent certificate password and HTTP Proxy parameters:

```
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
```

- Semi-silent 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
```

## ESET Remote Deployment Tool

The ESET Remote Deployment Tool is a convenient way to distribute the [installer package](#) created by ESET PROTECT On-Prem to deploy ESET Management Agent and ESET security applications remotely on computers over a network.

The ESET Remote Deployment Tool is available for free on the ESET [website](#) as a standalone ESET PROTECT On-Prem Component. The deployment tool is meant mainly for deployment on small to medium networks and is executed under administrator privileges.

**i** The ESET Remote Deployment Tool is dedicated to deploy ESET Management Agent to client computers with [supported](#) Microsoft Windows operating systems only.

For more details on prerequisites and usage of the tool, see the [ESET Remote Deployment Tool](#) chapter.

## Web Console installation—Windows

- [Install Web Console using the All-in-one installer—Windows \(recommended\)](#)
- [Install Web Console manually—Windows \(advanced users\)](#)

## Install Web Console using the All-in-one installer—Windows (recommended)

### Prerequisites

- ESET PROTECT Server is installed.

**i** You can install the ESET PROTECT Web Console on a different computer than the computer running the ESET PROTECT Server. This procedure requires [additional steps](#).

- Apache Tomcat is a mandatory component required to run the ESET PROTECT Web Console.
- Apache Tomcat requires 64-bit Java/OpenJDK. If your system has multiple Java versions installed, uninstall earlier Java versions and keep only the latest [supported Java](#) version.



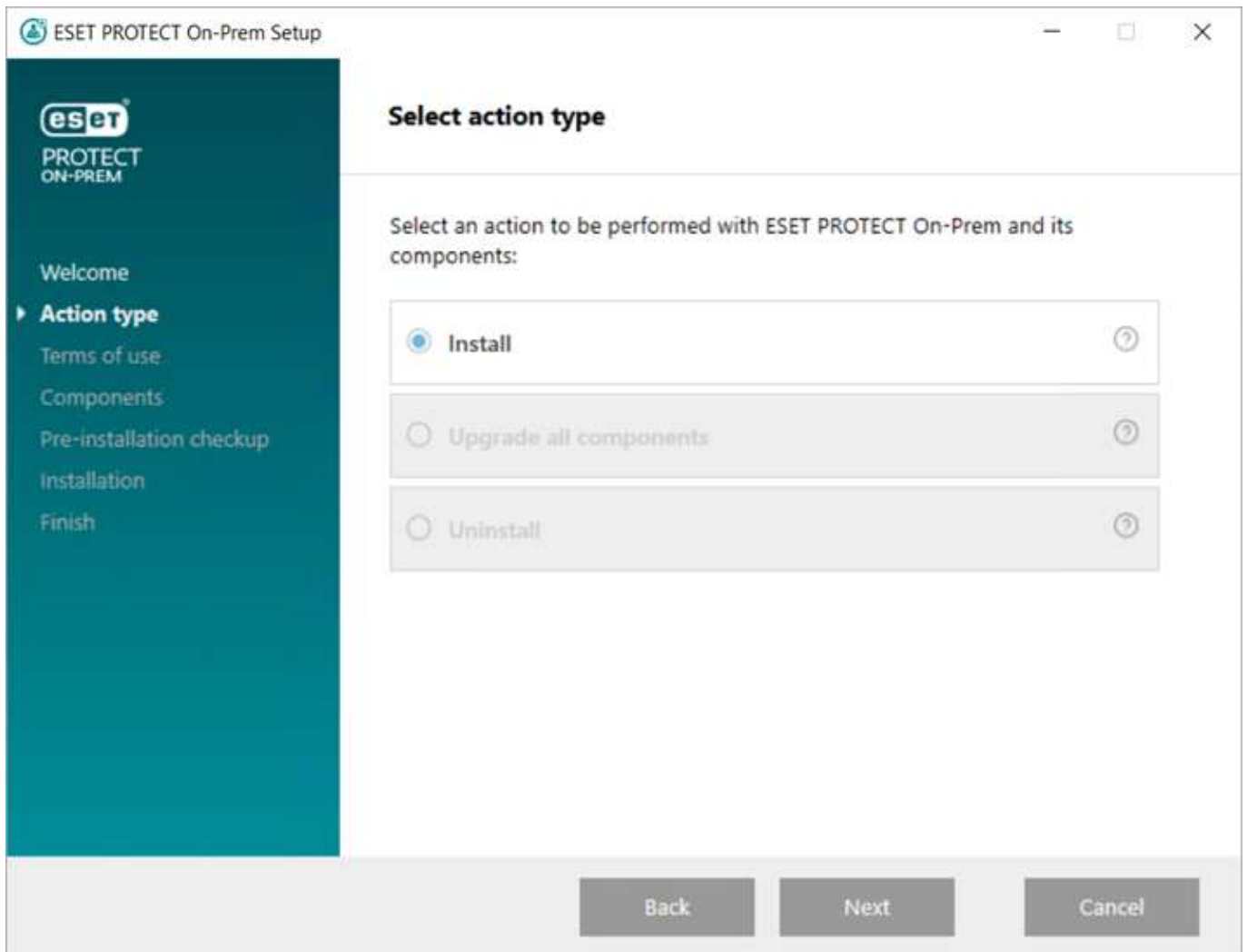
Starting January 2019, Oracle JAVA SE 8 public updates for business, commercial or production use require a commercial license. If you do not purchase a JAVA SE subscription, you can transition to a no-cost alternative. See the [supported versions of JDK](#).

# Installation

Follow the steps below to install the ESET PROTECT Web Console component on Windows using the All-in-one installer:

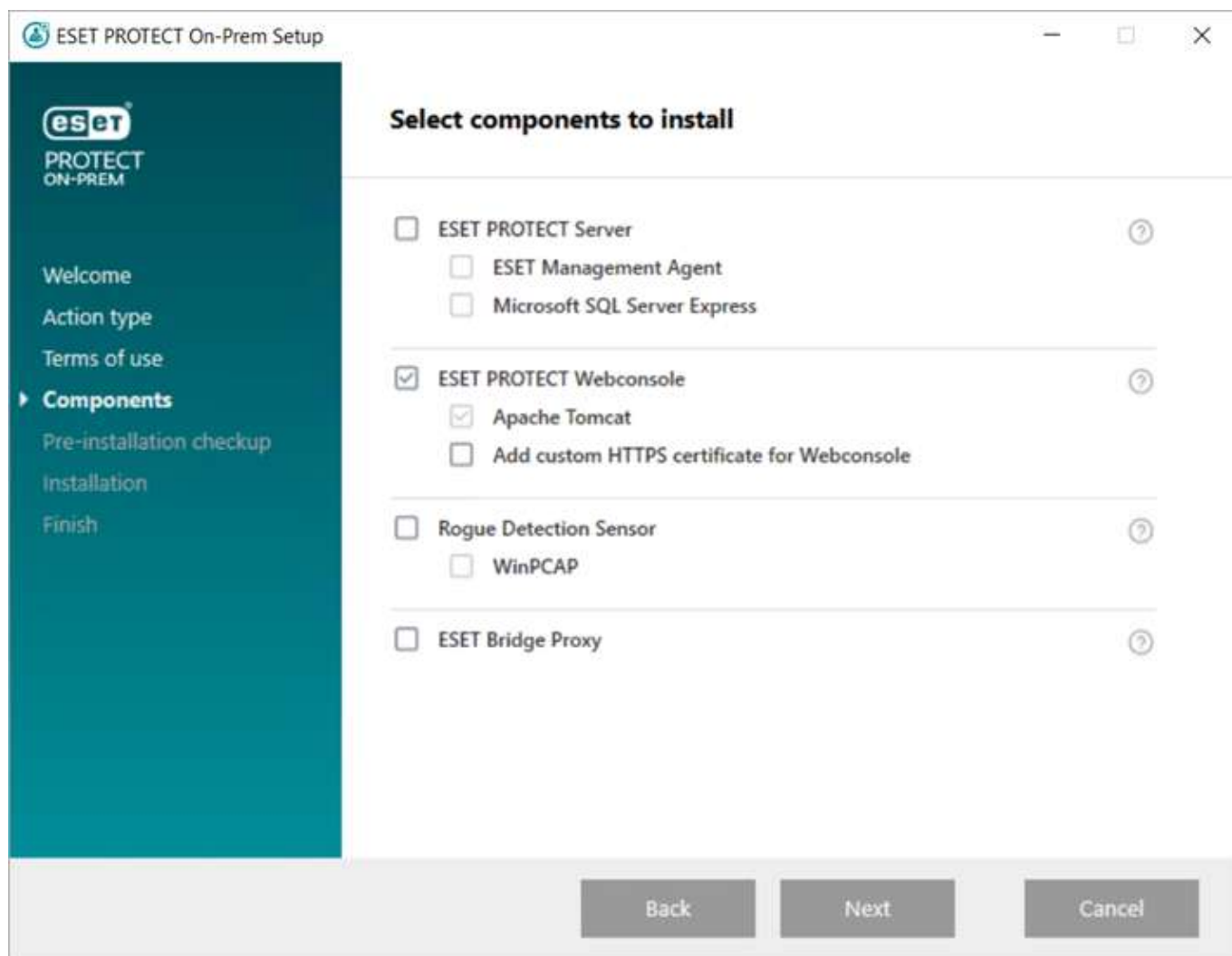
**!** Ensure to meet all the installation prerequisites listed above.

1. Download the [ESET PROTECT All-in-one installer](#) from the ESET website and unzip the downloaded file.
2. If you want to install the latest version of Apache Tomcat and the All-in-one installer contains an earlier version of Apache Tomcat (this step is optional—skip to step 4 if you do not need the latest version of Apache Tomcat):
  - a. Open the *x64* folder and navigate to the *installers* folder.
  - b. Remove the *apache-tomcat-9.0.x-windows-x64.zip* file located in the *installers* folder.
  - c. Download the Apache Tomcat 9 [64-bit Windows zip](#) package.
  - d. Move the downloaded zip package to the *installers* folder.
3. To launch the All-in-one installer, double-click the *Setup.exe* file and click **Next** on the **Welcome** screen.
4. Select **Install** and click **Next**.



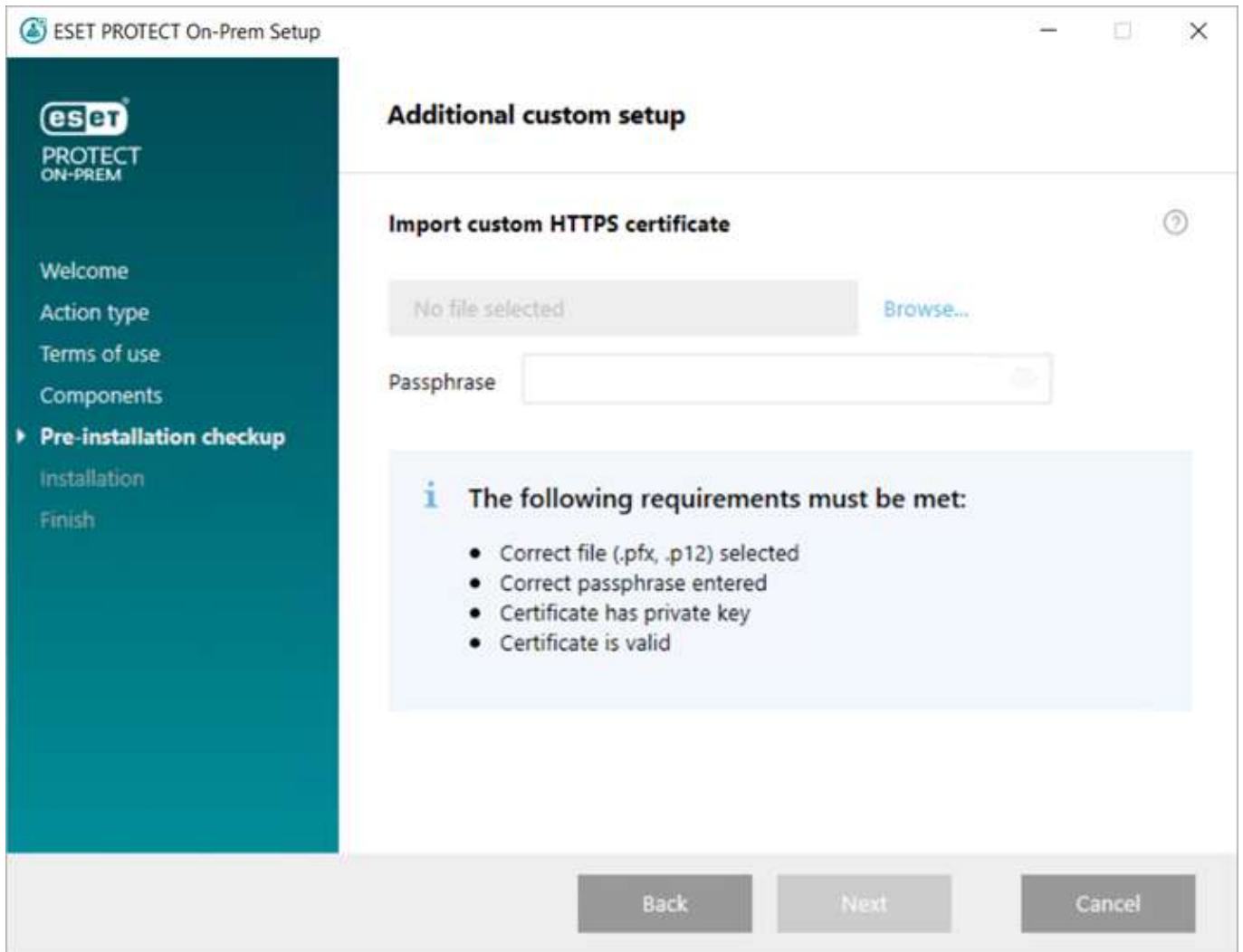
5. After accepting the Terms of Use, click **Next**.

6. In **Select Components to install**, only select the **ESET PROTECT Webconsole** check box and click **Next**.



Optionally, select the **Add custom HTTPS certificate for Webconsole** check box.

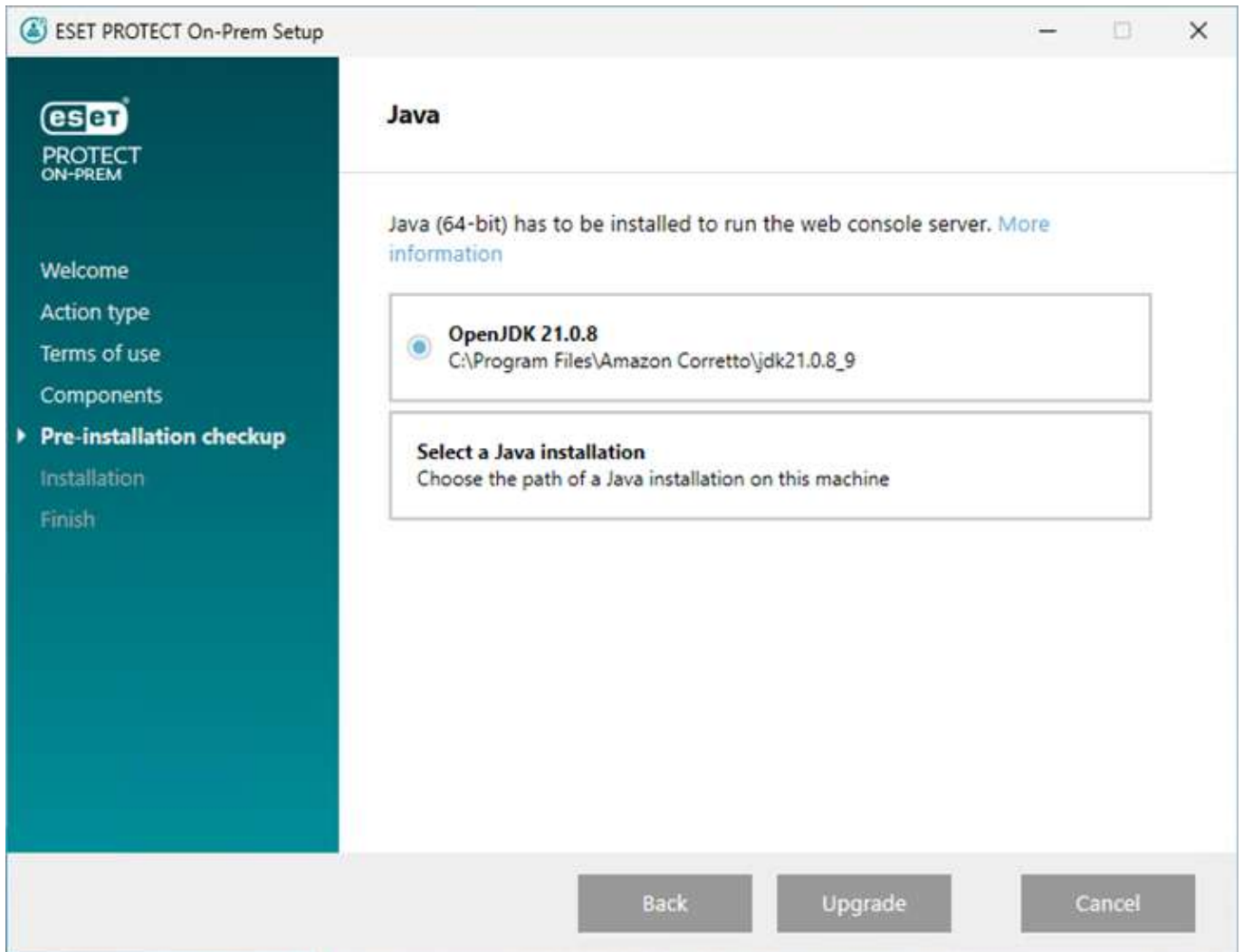
- Select this option if you want to use a custom HTTPS certificate for the ESET PROTECT Web Console.
- If you do not select this option, the installer automatically generates a new Tomcat keystore (a self-signed HTTPS certificate).
- If you have selected **Add custom HTTPS certificate for Webconsole**, click **Browse**. Select a valid Certificate (.pfx or .p12 file) and type its **Passphrase**. Leave the field blank if there is no passphrase. The installer will install the certificate for Web Console access on your Tomcat server. Click **Next** to continue.



7. Select a Java installation on the computer. Verify you are using the latest version of Java/OpenJDK.

a) To select the already installed Java, click **Select a Java installation**, select the folder where Java is installed (with a subfolder *bin*, for example, *C:\Program Files\Amazon Corretto\jdk1.8.0\_212*) and click **OK**. The installer prompts you if you have selected an invalid path.

b) Click **Install** to continue or **change** to change the Java installation path.



8. When the installation is complete, click **Finish**.

If you installed the ESET PROTECT Web Console on a different computer than the ESET PROTECT Server, perform these additional steps to enable communication between ESET PROTECT Web Console and ESET PROTECT Server:

- a) Stop the Apache Tomcat service: Navigate to **Start > Services** > right-click the Apache Tomcat service and select **Stop**.
- b) Run Notepad as an Administrator and edit the `C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.
- c) Find the `server_address=localhost`.
- d) Replace `localhost` with the IP address of your ESET PROTECT Server and save the file.
- e) Start the Apache Tomcat service: Navigate to **Start > Services** > right-click the Apache Tomcat service and select **Start**.

9. Open the ESET PROTECT Web Console in a [supported web browser](#); a login screen will be displayed:

- From the computer hosting the ESET PROTECT Web Console: `https://localhost/era`
- From any computer with internet access to the ESET PROTECT Web Console (substitute `IP_ADDRESS_OR_HOSTNAME` with the IP address or hostname of your ESET PROTECT Web Console): `https://IP_ADDRESS_OR_HOSTNAME/era`

**i** See the additional [Web Console configuration for enterprise solutions or low-performance systems](#).

# Install Web Console manually—Windows (advanced users)



Manual installation of ESET PROTECT Web Console is an advanced procedure. We recommend that you install ESET PROTECT Web Console using the [All-in-one installer](#).

## Prerequisites

- ESET PROTECT Server is installed.



You can install the ESET PROTECT Web Console on a different computer than the computer running the ESET PROTECT Server. This procedure requires [additional steps](#).

- Apache Tomcat is a mandatory component required to run the ESET PROTECT Web Console. Install Apache Tomcat:
  - a)Download the latest [supported version](#) of the Apache Tomcat installer file (32-bit/64-bit Windows Service Installer) *apache-tomcat-[version].exe* from <https://tomcat.apache.org>.
  - b)Run the installer.
  - c)During the installation, select the path to Java (parent folder of Java *bin* and *lib* folders) and select the **Run Apache Tomcat** check box.
  - d)After the installation, ensure that the Apache Tomcat service is running and its startup type is set to **Automatic** (in **services.msc**).
- Apache Tomcat requires 64-bit Java/OpenJDK. If your system has multiple Java versions installed, uninstall earlier Java versions and keep only the latest [supported Java](#) version.



Starting January 2019, Oracle JAVA SE 8 public updates for business, commercial or production use require a commercial license. If you do not purchase a JAVA SE subscription, you can transition to a no-cost alternative. See the [supported versions of JDK](#).

## Installation

Follow the steps below to install the ESET PROTECT Web Console component on Windows manually:



Ensure to meet all the installation prerequisites listed above.

1. Visit the ESET PROTECT [download section](#) to download a standalone installer for this ESET PROTECT component (Web Console file *era\_x64.war*).
2. Rename *era\_x64.war* to *era.war* and copy *era.war* to the Apache Tomcat web applications folder:

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

3. Apache Tomcat automatically extracts the *era.war* file into the *era* folder and installs ESET PROTECT Web Console. Wait a few minutes until the extraction completes. If the extraction does not occur, follow the

[troubleshooting steps](#).

4. If you installed the ESET PROTECT Web Console on the same computer as the ESET PROTECT Server, restart the Apache Tomcat service. Navigate to **Start > Services** > right-click the Apache Tomcat service and select **Stop**. Wait for 30 seconds and then click **Start**.

If you installed the ESET PROTECT Web Console on a different computer than the ESET PROTECT Server, perform these additional steps to enable communication between ESET PROTECT Web Console and ESET PROTECT Server:

- Stop the Apache Tomcat service: Navigate to **Start > Services** > right-click the Apache Tomcat service and select **Stop**.
- Run Notepad as an Administrator and edit the `C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.
- Find the `server_address=localhost`.
- Replace `localhost` with the IP address of your ESET PROTECT Server and save the file.
- Start the Apache Tomcat service: Navigate to **Start > Services** > right-click the Apache Tomcat service and select **Start**.


5. Open the ESET PROTECT Web Console in a [supported web browser](#) to see a login screen:

- From the computer hosting the ESET PROTECT Web Console: `http://localhost:8080/era`
- From any computer with internet access to the ESET PROTECT Web Console (substitute `IP_ADDRESS_OR_HOSTNAME` with the IP address or hostname of your ESET PROTECT Web Console): `http://IP_ADDRESS_OR_HOSTNAME:8080/era`

6. Configure the Web Console after the installation:


- The default HTTP port is set to 8080 during the manual installation of Apache Tomcat. We recommend that you set up an [HTTPS connection for Apache Tomcat](#).
- See the additional [Web Console configuration for enterprise solutions or low-performance systems](#).

## RD Sensor installation—Windows

 ESET Rogue Detection (RD) Sensor will be deprecated (there will be no future updates). Some of its features may not work properly. You can no longer manage RD Sensor configuration via a policy.


### Prerequisites

- [WinPcap](#)—use the latest WinPcap version (4.1.0 and later)
- Network should be properly configured (appropriate [ports](#) open, incoming communication not being blocked by a firewall, etc.)
- ESET PROTECT Server is reachable
- ESET Management Agent must be installed on the local computer to support all program features fully

 If there are multiple network segments, Rogue Detection Sensor must be installed separately on each network segment to produce a comprehensive list of all devices on the whole network.

## Installation

Follow the steps below to install the RD Sensor component on Windows:

 Ensure to meet all the installation prerequisites listed above.

1. Visit the ESET PROTECT [download section](#) to download a standalone installer for this ESET PROTECT component (*rdsensor\_x86.msi* or *rdsensor\_x64.msi*).
2. Double-click the RD Sensor installer file to begin the installation.
3. Accept the EULA and click **Next**.
4. Select the **Participate in product improvement program** check box to send anonymous telemetry data and crash report to ESET (operating system version and type, ESET application version and other application-specific information).
5. Select the installation location for RD Sensor and click **Next > Install**.
6. ESET Rogue Detection Sensor will start after installation completes.

You can find the Rogue Detection Sensor log file in [Log files](#): *C:\ProgramData\ESET\Rogue Detection Sensor\Logs\*

## Mirror Tool—Windows

[Are you a Linux user?](#)

The Mirror Tool is necessary for offline detection engine updates. If your client computers do not have an internet connection and need detection engine updates, you can use the Mirror Tool to download update files from ESET update servers and store them locally.

The Mirror Tool has these functions:

- Application module updates—It downloads detection engine updates and other application modules, but not [auto-updates](#) (uPCU).
  - Repository creation—It can create a full [offline repository](#), including [auto-updates](#) (uPCU).
- The Mirror Tool does not download ESET LiveGrid® data.

## Changelog

The following content is dynamic and can only be accessed online. [Visit the website to view the content.](#)

## Prerequisites

- The Mirror Tool for Windows supports these 64-bit operating systems:
  - o Windows Server 2012 R2 and later
  - o Windows 10/11
- The Mirror Tool does not support Windows XP and Windows Server 2003.

- The target folder must be available for sharing, Samba/Windows or HTTP/FTP service, depending on how you want to have the updates accessible.

oESET security applications for Windows—You can update them remotely using HTTP or a shared folder.

oESET security applications for Linux/macOS—You can update them remotely only using HTTP. If you use a shared folder, it must be on the same computer as the ESET security application.

- You must have a valid offline activation file needed for the activation of the Mirror Tool and generation of the update mirror. You can generate the offline activation file in ESET Business Account or ESET PROTECT Hub:

oIn [ESET Business Account](#), select the **Include Username and Password** check box.

oIn [ESET PROTECT Hub](#), select the **Allow online activation** check box.

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

Create offline license file

• Required field

**Solution**

ESET Endpoint Antivirus + ESET Server Security

• Offline license name

Offline

**Quantity**

0

**ESET PROTECT on-prem**

Allow management with ESET PROTECT

**ESET PROTECT token** ⓘ

Insert an ESET PROTECT token

**Online activation** ⓘ

Allow online activation

CREATE CLOSE

- Before running the Mirror Tool, you need to have the following package installed: [Microsoft Visual C++ 2022 Redistributable x64](#)

## How to use the Mirror Tool

1. Download the Mirror Tool from the [ESET download page](#) (**Standalone installers** section).
2. Unzip the downloaded archive.
3. Open the Command Prompt and navigate to the folder with the *MirrorTool.exe* file.
4. Run the command below to view all available parameters for the Mirror Tool and its version:

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

```

C:\Users\user\Desktop\MirrorTool_Win_x64>MirrorTool.exe --help
[info] Mirror Tool v1.2.143.0, Copyright (c) ESET, spol. s r.o. 1992-2024. All rights reserved.
[info] 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/ezet_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). Windows only
--networkDrivePassword arg [optional]
Password used, when output directory is accessed using smb(e.g:\\hostname). Windows only
--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(=AUTOSELECT)] [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, dylib. Parameter is ignored when creating mirror for legacy products (ep4, ep5) - only dat format is supported.
--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.
--logLevel arg [optional]
Specifies logging level - options can be: error, warning, info, debug.
--logFilename arg [optional]
Specifies where to store log file.
--logIntoStandardPath [optional]
Stores log file into standard path - 'ProgramData' on Windows, '/var/log' on Linux
--help [optional]
Display this help and exit

```

### Parameters limitations

The Mirror Tool parameters support only ASCII characters.



Case sensitivity:

- Mirror Tool 1.0.x—All the parameters are case-sensitive.
- Mirror Tool 1.2.x and later—All the parameters are case-insensitive.

You can use the parameters to create the repository mirror or application modules mirror:

### [Parameters for both repository and application modules mirror](#)



--proxyHost	
--proxyPort	
--proxyUsername	
--proxyPassword	
--help	
--logLevel	Set log level. The following values are available: error, warning, info (default), debug. Example: --logLevel debug The parameter is available since Mirror Tool 1.2.x.
--logFilename	Set the log filename and its location. Example: <ul style="list-style-type: none"><li>• Windows: --logFilename C:\MT_log.txt</li><li>• Linux: --logFilename ~/Downloads/MT_log.txt</li></ul> The parameter is available since Mirror Tool 1.2.x.
--logIntoStandardPath	Enable logging into the standard path: <ul style="list-style-type: none"><li>• Windows: C:\ProgramData\ESET\RemoteAdministrator\MirrorTool\Logs</li><li>• Linux: /var/log/eset/RemoteAdministrator/MirrorTool/Logs</li></ul> You cannot combine --logIntoStandardPath with --logFilename. The parameter is available since Mirror Tool 1.2.x.
--useSecureConnection	Uses HTTPS connections to update servers. The parameter is available since Mirror Tool 1.2.202.

### [Repository-specific parameters](#)

--repositoryServer	See the <a href="#">repository details in ESET PROTECT Settings</a> . If you do not provide the value, AUTOSELECT is used by default.
--intermediateRepositoryDirectory	
--outputRepositoryDirectory	
--compatibilityVersion	
--dryRun	
--filterFilePath	
--trustDownloadedFilesInRepositoryTemp	

### [Modules-specific parameters](#)

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

Parameter	Description
--updateServer	<p>The Mirror Tool creates <a href="#">a folder structure</a> different from what Endpoint mirror does. Each folder holds update files for a group of applications.</p> <div style="border: 1px solid red; padding: 5px;"> <p> You must specify the <a href="#">update server full link</a> (full path to the correct folder) in the update settings of the application using the mirror.</p> </div>
--offlineLicenseFilename	You must specify a path to your offline activation file (as mentioned above).
--mirrorOnlyLevelUpdates	No argument needed. If set, only level updates will be downloaded (nano updates will not be downloaded). Read more about update types in our <a href="#">Knowledgebase article</a> .
--mirrorFileFormat	<div style="border: 1px solid red; padding: 5px;"> <p> Before using the <code>--mirrorFileFormat</code> parameter, ensure that you environment does not contain both earlier (6.5 and earlier) and later (6.6. and later) ESET security application versions. The incorrect usage of this parameter may result in incorrect updates of your ESET security applications.</p> </div> <p>You can specify which type of update files will be downloaded. Possible values (case sensitive):</p> <ul style="list-style-type: none"> <li>• <code>dat</code>—Use this value if you have environment only with ESET security application versions 6.5 and earlier.</li> <li>• <code>dll</code>—Use this value if you have environment only with ESET security application versions 6.6 and later.</li> <li>• <code>dylib</code>—Use this value if you have environment only with ESET security application for macOS version 8 and later.</li> </ul> <p>This optional parameter applies to the Mirror Tool distributed with ESET PROTECT On-Prem 8.1 and later.</p> <p>The Mirror Tool will download update files compatible with ESET PROTECT On-Prem repository version you specify in the parameter argument in format <code>x.x</code> or <code>x.x.x.x</code>, for example: <code>--compatibilityVersion 13.0</code> or <code>--compatibilityVersion 8.1.13.0</code>.</p> <p>The <code>--compatibilityVersion</code> parameter excludes the <a href="#">auto-updates</a> (uPCU) from the mirror. If you need the auto-updates (uPCU) in your environment and want to decrease the mirror size, use the <code>--filterFilePath</code> parameter.</p>
--compatibilityVersion	<p>This optional parameter applies to the Mirror Tool distributed with ESET PROTECT On-Prem 8.1 and later.</p> <p>The Mirror Tool will download update files compatible with ESET PROTECT On-Prem repository version you specify in the parameter argument in format <code>x.x</code> or <code>x.x.x.x</code>, for example: <code>--compatibilityVersion 13.0</code> or <code>--compatibilityVersion 8.1.13.0</code>.</p> <p>The <code>--compatibilityVersion</code> parameter excludes the <a href="#">auto-updates</a> (uPCU) from the mirror. If you need the auto-updates (uPCU) in your environment and want to decrease the mirror size, use the <code>--filterFilePath</code> parameter.</p>



To reduce the amount of data downloaded from the ESET repository, we recommend that you use the new parameters in Mirror Tool distributed with ESET PROTECT On-Prem 9: `--filterFilePath` and `--dryRun`:

1. Create a filter in a *JSON* format (see `--filterFilePath` below).

**i** 2. Perform a test Mirror Tool run with the `--dryRun` parameter (see below) and adjust the filter as necessary.

3. Run the Mirror Tool with the `--filterFilePath` parameter and the defined download filter, together with `--intermediateRepositoryDirectory` and `--outputRepositoryDirectory` parameters.

4. Run the Mirror Tool regularly to always use the latest installers.

Parameter	Description
<p><code>--filterFilePath</code></p>	<p>Use this optional parameter to filter ESET security applications based on a text file in <i>JSON</i> format placed in the same folder as Mirror Tool, for example: <code>--filterFilePath filter.txt</code>.</p> <p><a href="#">Filter configuration description:</a></p> <p>The configuration file format for application filtering is <i>JSON</i> with the following structure:</p> <ul style="list-style-type: none"> <li>• root <i>JSON</i> object: <ul style="list-style-type: none"> <li>• <code>use_legacy</code> (boolean, optional)—if true, legacy applications will be included.</li> <li>• <code>defaults</code> (<i>JSON</i> object, optional)—defines filter properties that will be applied to all applications. <ul style="list-style-type: none"> <li>■ <code>languages</code> (list)—Specify ISO language codes of languages to include, for example for French type "fr_FR". Other languages codes are in the <a href="#">table below</a>. To select more languages, separate them by a comma and a space, for example: (["en_US", "zh_TW", "de_DE"])</li> <li>■ <code>platforms</code> (list)—platforms to include (["x64", "x86", "arm64"]).</li> </ul> <div data-bbox="531 600 1473 705" style="border: 1px solid red; padding: 5px;"> <p> Use the <code>platforms</code> filter carefully. For example, if the Mirror Tool downloads only 64-bit installers and there are 32-bit computers in your infrastructure, 64-bit ESET security applications will fail to install on 32-bit computers.</p> </div> </li></ul> </li> <li>• <code>os_types</code> (list)—operating system types to include (["windows"], ["linux"], ["mac"]).</li> <li>• <code>products</code> (list of <i>JSON</i> objects, optional)—filters to apply to specific applications—override <code>defaults</code> for specified applications. The objects have the following properties: <ul style="list-style-type: none"> <li>■ <code>app_id</code> (string)—required if <code>name</code> is not specified.</li> <li>■ <code>name</code> (string), required if <code>app_id</code> is not specified.</li> <li>■ <code>version</code> (string)—specifies version or range of versions to include.</li> <li>■ <code>languages</code> (list)—ISO language codes of languages to include (see the <a href="#">table below</a>).</li> <li>■ <code>platforms</code> (list)—platforms to include (["x64", "x86", "arm64"]).</li> <li>■ <code>os_types</code> (list)—operating system types to include (["windows"], ["linux"], ["mac"]).</li> </ul> <div data-bbox="531 1137 1473 1211" style="border: 1px solid blue; padding: 5px;"> <p> To determine appropriate values for the fields, run Mirror Tool in dry run mode and find the relevant application in the created CSV file.</p> </div> </li> </ul> <p><b>Version string format descriptions</b></p> <p>All version numbers—consist of four numbers separated by dots (for example, 7.1.0.0). You can specify less numbers when writing version filters (for example, 7.1) and the rest of the numbers will be zero (7.1 is equal to 7.1.0.0).</p> <p>Version string can have one of the two following formats:</p> <ul style="list-style-type: none"> <li>• <code>[&gt; &lt; &gt;= &lt;= &lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))]</code></li> </ul> <p><code>O</code>Selects versions higher/smaller or equal/less or equal/equal than the version specified.</p> <ul style="list-style-type: none"> <li>• <code>&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))-&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))]</code></li> </ul> <p><code>O</code>Selects versions that are higher than or equal to the lower bound and less than or equal to the higher bound.</p> <p>Comparisons are done numerically on each part of the version number, left to right.</p> <div data-bbox="531 1585 1236 2101" style="border: 1px solid green; padding: 10px;"> <p><b>JSON example</b></p> <pre> {   "use_legacy": true,   "defaults": {     "languages": [ "en_US" ],     "platforms": [ "x64", "x86" ]   },   "products": [     ✓ {       "app_id": "com.eset.apps.business.ees.windows",       "version": "7.1.0.0 - 8.0.0.0"     },     {       "app_id": "com.eset.apps.business.eea.windows",       "version": "&gt;7.1.0.0"     }   ] } </pre> </div>

The `--filterFilePath` parameter replaces the `--languageFilterForRepository`, `--productFilterForRepository` and `--downloadLegacyForRepository` parameters used in earlier Mirror Tool versions (released with ESET PROTECT On-Prem 8.x).

Parameter	Description
--dryRun	<p>When you use this optional parameter, Mirror Tool will not download any files, but it will generate a .csv file listing all packages that will be downloaded.</p> <p>You can use this parameter without mandatory parameters --intermediateRepositoryDirectory and --outputRepositoryDirectory, for example:</p> <ul style="list-style-type: none"> <li>Windows: <code>MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv</code></li> <li>Linux: <code>sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv</code></li> </ul> <div style="border: 1px solid blue; padding: 5px;"> <p><b>i</b> Some ESET installers are language-generic (with the <code>multilang</code> language code) and the Mirror Tool will list them in the .csv file even if you specify languages in --filterFilePath.</p> </div> <p>If you use the --dryRun parameter and also --intermediateRepositoryDirectory and --outputRepositoryDirectory parameters, the Mirror Tool does not clear the <i>outputRepositoryDirectory</i>.</p>
--listUpdatableProducts	<p>List all ESET applications for which the Mirror Tool can download application module updates (unless --excludedProducts is used).</p> <p>The parameter is available from Mirror Tool versions: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).</p>
--networkDriveUsername	<p>Username used to access the output directory via SMB (for example, \\hostname). The parameter works only on Mirror Tool for Windows.</p>
--networkDrivePassword	<p>Password used to access the output directory via SMB. The parameter works only on Mirror Tool for Windows.</p>

## Mirror Tool folder structure

By default, if you do not specify the --updateServer parameter, the Mirror Tool creates this folder structure on your HTTP server:

### Do not use an HTTP-only mirror server

**!** Ensure the local mirror server uses HTTP and HTTPS protocols or only HTTPS. If the mirror server uses only HTTP, you cannot use the Software Install client task because the ESET security application EULA or Terms of Use cannot be retrieved from an HTTP server.

Mirror Tool default folders	ESET security application	Update server (according to your HTTP server root location)
<i>mirror/eset_upd/era6</i>	ESET PROTECT On-Prem (all versions)	To update the ESET PROTECT On-Prem 13.0 from the mirror, set the <a href="#">Update server</a> to <code>http://your_server_address/mirror/eset_upd/era6</code>
<i>mirror/eset_upd/ep[version]</i>	ESET Endpoint Antivirus/Security version 6.x (and later) for Windows. Each major version has its folder, for example, <i>ep10</i> for version 10.x.	<code>http://your_server_address/mirror/eset_upd/ep10</code> (an example for version 10.x)
<i>mirror/eset_upd/v5</i>	ESET Endpoint Antivirus/Security version 5.x for Windows	<code>http://your_server_address/mirror/eset_upd/v5</code>

## ESET security applications for Linux/macOS



You must specify the `--updateServer` parameter and create additional folders to update ESET security applications for Linux/macOS from the HTTP mirror (see below).

<code>--updateServer</code>	Additional Mirror Tool folder	ESET security application	Update server (according to your HTTP server root location)
<code>http://update.eset.com/eset_upd/businesslinux</code>	<code>mirror/eset_upd/BusinessLinux</code>	ESET Endpoint Antivirus for Linux	<code>http://your_server_address/mirror/eset_upd/BusinessLinux</code>
<code>http://update.eset.com/eset_upd/serverlinux</code>	<code>mirror/eset_upd/LinuxServer</code>	ESET Server Security for Linux	<code>http://your_server_address/mirror/eset_upd/LinuxServer</code>
<code>http://update.eset.com/eset_upd/businessmac</code>	<code>mirror/eset_upd/BusinessMac</code>	ESET Endpoint Security version 7.x+ for macOS	<code>http://your_server_address/mirror/eset_upd/BusinessMac</code>
<code>http://update.eset.com/eset_mobile/eesa</code>	<code>mirror/eset_upd/EndpointAndroid</code>	ESET Endpoint Security for Android	<code>http://your_server_address/mirror/eset_upd/EndpointAndroid</code>

### [Language codes table](#)

To create a mirror, run the Mirror Tool with at least the minimum required parameters. Here is an example:

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

Here is an example of more advanced configuration for an offline repository with selected applications, languages and enabled download of legacy files defined in the `filter.txt` file (see the file contents example in `--filterFilePath` details above):


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

## Mirror Tool and Update settings

- To automate downloads for application modules updates, you can create a schedule to run the Mirror Tool. To do so, open your Web Console and click **Client Tasks > Operating System > Run Command. Select Command line to run** (including a path to the `MirrorTool.exe`) and a reasonable trigger (such as CRON for every hour `0 0 * * * ? *`). Alternatively, you can use the Windows Task Scheduler or Cron in Linux.

- To configure updates on a client computer(s), create a new policy and configure **Update server** to point to your mirror address or shared folder.


 If you are using an HTTPS mirror server, you need to import its certificate to the trusted root store on the client machine. See [Installing the trusted root certificate](#) in Windows.

 Read [this Knowledgebase article](#) to set up Mirror Tool chaining (configure Mirror Tool to download updates from another Mirror Tool).

## Offline Repository—Windows

You can use the Mirror Tool to create an offline repository on Windows ([Are you a Linux user?](#)) when using closed computer networks or networks with limited internet access. You can use the Mirror Tool to create a clone of the ESET repository in a local folder. This cloned repository can be moved (for example, onto an external disk) to a location in the closed network. You can copy the repository to a secure location in the local network and make it available via an HTTP server (for example, ESET Bridge).

To update the offline repository, run the same command with the same parameters as used for offline repository creation. Previous data in the intermediary folder will be used, and only outdated files will be downloaded.

 Be aware that the size of the repository is growing, and the intermediary directory will be the same size. Ensure you have at least **1.2 TB** of free space before starting this procedure.

### Best practices

See also the ESET Knowledgebase article [Best practices for using the ESET PROTECT On-Prem in an offline environment](#).

## Example scenario for Windows

### I. Create repository clone

1. [Download](#) the Mirror Tool.
2. Extract the Mirror Tool from the downloaded *.zip* file.
3. Prepare (create) folders for:
  - intermediary files
  - final repository
4. Open command prompt and change the directory to the folder where the Mirror Tool is extracted (`cd` command).
5. Run the following command (change the intermediary and output repository directories to the folders from step 3):

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

--outputRepositoryDirectory C:\Repository

6. After the repository is copied to the `outputRepositoryDirectory` folder, move the folder and its contents to another machine where your closed network is accessible.

## II. Set up the HTTP server

1. You need an HTTP server running on the machine in the closed network. You can use:

- ESET Bridge proxy from the ESET [download site](#) (this scenario)
- a different HTTP server

2. [Install ESET Bridge](#) proxy.

## III. Run the offline repository

1. Navigate to `C:\Program Files\ESET\Bridge` and open the `pkgid` file using a simple text editor. Change the `http_proxy_settings_static_content_enabled` setting to `true` to activate the offline repository server. Save the changes and close the `pkgid` file.

2. Copy the downloaded repository from step 6 (section I. above) to the offline repository server directory:

- The default offline repository server directory is `C:\ProgramData\ESET\Bridge\OfflineRepository` with proper access rights.
- To use a custom directory, create a new folder for the offline repository (for example, `C:\Repository`). In the `pkgid` file, replace the line `"http_proxy_settings_offline_repository_dirPath": "%DATADIR%\OfflineRepository"` with `"http_proxy_settings_offline_repository_dirPath": "C:\\Repository"`. The NETWORK SERVICE user needs full access rights to the directory.

3. Restart the ESET Bridge service using the command line commands: `net stop "EsetBridge"` and `net start "EsetBridge"`. You must restart the service only after changing the `pkgid` file—the service restart is unnecessary when the repository data is changed, deleted, or added.

4. The offline repository runs on the address `http://YourIPaddress:4449` (for example, `http://10.1.1.10:4449`).

5. Set the new repository address using the ESET PROTECT Web Console:

- a. [ESET PROTECT Server](#)—Click **More > Settings > Advanced Settings > Repository** and type the offline repository address into the **Server** field.
- b. [ESET Management Agents](#)—Click **Policies**, click the Agent policy > **Edit > Settings > Advanced Settings > Repository** > type the offline repository address into the **Server** field.
- c. ESET endpoint applications (for Windows)—Click **Policies**, click the **ESET Endpoint for Windows** policy > **Edit > Settings > Updates > Profiles > Updates > Application Updates** > type the offline repository address into the **Custom server** field.

# Failover Cluster—Windows

Below are the high-level steps required to install ESET PROTECT On-Prem in a Failover Cluster environment.

**i** See also this [Knowledgebase article](#) about cluster installation of ESET PROTECT Server.

1. [Create a Failover Cluster](#) with a shared disk.
2. In the **Create Cluster Wizard** type the desired hostname (make up one) and IP address.
3. Get the shared disk of the cluster online on node1 and [install ESET PROTECT Server using the standalone installer](#) on it. Ensure that **This is a cluster installation** is selected during installation and select the shared disk as application data storage. Make up a hostname and type it for the Server certificate of ESET PROTECT Server next to the pre-filled hostnames. Remember this hostname and use it in step no. 6 when creating the ESET PROTECT Server Role in the Cluster Manager.
4. Stop ESET PROTECT Server on node1, bring the shared disk of the cluster online on node2 and [install ESET PROTECT Server using the standalone installer](#) on it. Ensure that **This is a cluster installation** is selected during installation. Choose the shared disk as application data storage. Keep database connection and certificate information intact, they were configured during installation of ESET PROTECT Server on node1.
5. Configure your firewall to allow incoming connections on all [ports](#) used by ESET PROTECT Server.
6. In the cluster configuration manager create and start a Role (**Configure Role > Select Role > Generic service**) for the ESET PROTECT Server service. Select the **ESET PROTECT Server** service from the list of available services. It is very important to use the same hostname for the Role as was used in step 3 concerning the Server certificate.
7. Install ESET Management Agent on all cluster nodes using the standalone installer. In the **Agent configuration** and **Connection to ESET PROTECT Server** screens use the hostname you used in step no. 6. Store Agent data on the local node (not on the cluster disk).
8. Web server (Apache Tomcat) is not supported on a cluster, therefore you need to install it on a non-clustered disk or a different machine:
  - a. [Install the Web Console](#) on a separate computer and configure it properly to connect to ESET PROTECT Server cluster Role.
  - b. After Web Console is installed, locate its configuration file at: `C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`
  - c. Open the file in Notepad or any other simple text editor. In the line `server_address=localhost` replace localhost with the IP address or hostname of the ESET PROTECT Server cluster Role.

## Component installation on Linux

Many installation scenarios require you to install different ESET PROTECT components on different machines to accommodate network architectures, meet performance requirements, or for other reasons. The following installation packages are available for individual ESET PROTECT Linux components:

Follow the [step-by-step ESET PROTECT On-Prem Linux installation](#) instructions.

Core components	Download links	Installation instructions
ESET PROTECT Server	<a href="#">server_linux_x86_64.sh</a>	<a href="#">Server installation—Linux</a>
ESET PROTECT Web Console	<a href="#">era_x64.war</a>	<a href="#">Web Console installation—Linux</a>
ESET Management Agent	<a href="#">agent_linux_x86_64.sh</a> (64-bit) <a href="#">agent_linux_i386.sh</a> (32-bit)	<a href="#">Agent installation—Linux</a>
Database server	<a href="#">MySQL Server</a>	<a href="#">MySQL installation and configuration—Linux</a>

Optional components	Download links	Installation instructions
ESET Bridge (HTTP proxy)	<a href="#">eset-bridge.x86_64.bin</a>	<a href="#">Deploy ESET Bridge</a>
Mirror Tool	<a href="#">mirrortool_linux_x86_64.zip</a>	<a href="#">Mirror Tool—Linux</a>
ESET Rogue Detection Sensor	<a href="#">rdsensor_linux_x86_64.sh</a> (64-bit) <a href="#">rdsensor_linux_i386.sh</a> (32-bit)	<a href="#">Rogue Detection Sensor installation—Linux</a>

To upgrade ESET PROTECT On-Prem for Linux to the latest version, see the [Components Upgrade task](#) chapter or our [Knowledgebase article](#).

## Step-by-step ESET PROTECT On-Prem installation on Linux

In this installation scenario we will simulate the step-by-step installation of ESET PROTECT Server and ESET PROTECT Web Console. We will simulate installation using MySQL.

### Before installation

1. Verify that the [database server](#) is present in your network and ensure you have access to it on your local/remote server. If a database server is not installed, [install and configure](#) a new one.
2. Download ESET PROTECT Linux standalone components (Agent, Server, Web Console). You can find these installation files in the [ESET PROTECT Standalone Installers](#) category available on the ESET website.

### Installation process

You must be able to use the `sudo` command or install under `root` privileges to complete the installation.

**i** Your installation experience may vary according to the [supported Linux distribution](#) running on your server.

1. Install [required packages](#) for ESET PROTECT Server.
2. Configure the connection to MySQL server, as shown in the [MySQL configuration](#) topic.
3. Verify the configuration of the MySQL ODBC driver. See [ODBC installation and configuration](#) for more information.
4. Customize the installation parameters and execute the ESET PROTECT Server installation. See [Server installation—Linux](#) for more information.

5. Install the required Java and Tomcat packages and [install the ESET PROTECT Web Console](#). If you experience problems with the HTTPS connection to the ESET PROTECT Web Console, see [HTTPS/SSL connection setup](#).
6. [Install ESET Management Agent](#) on the server machine.

We recommend that you delete commands containing sensitive data (for example, a password) from the command line history:

1. Run `history` to see the list of all commands in the history.
2. Run `history -d line_number` (specify the line number of the command). Alternatively, run `history -c` to delete the entire command line history.

## MySQL installation and configuration—Linux

### Installation

**⚠** Ensure to install a [supported version of MySQL Server and ODBC Connector](#).

If you have already installed and configured MySQL, proceed to [Configuration](#).

1. Add the MySQL repository:

**i** Your installation experience may vary according to the [supported Linux distribution](#) running on your server.

<b>Debian, Ubuntu</b>	Run the following commands in the Terminal: 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> You can select the versions of components that you want to install during the package installation. We recommend that you select the default options. See also <a href="#">Adding the MySQL APT Repository</a> .
<b>Red Hat</b>	<a href="#">Adding the MySQL Yum Repository</a>
<b>SUSE Linux Enterprise Server</b>	<a href="#">Adding the MySQL SLES Repository</a>

2. Update your local repository cache:

<b>Debian, Ubuntu</b>	<code>sudo apt update</code>
<b>Red Hat</b>	<code>sudo dnf update</code>
<b>SUSE Linux Enterprise Server</b>	<code>sudo zypper update</code>

3. MySQL installation differs depending on the Linux distribution and version used:

Linux distribution:	MySQL Server installation command:	MySQL Server advanced installation:
<b>Debian, Ubuntu</b>	<code>sudo apt install mysql-server</code>	<a href="#">Installing MySQL from Source with the MySQL APT Repository</a>
<b>Red Hat</b>	<code>sudo dnf install mysql-community-server</code>	<a href="#">Installing MySQL on Linux Using the MySQL Yum Repository</a>

Linux distribution:	MySQL Server installation command:	MySQL Server advanced installation:
<b>SUSE Linux Enterprise Server</b>	<code>sudo zypper install mysql-community-server</code>	<a href="#">Steps for a Fresh Installation of MySQL</a>

[Download MySQL Community Server](#) for a manual installation.

## Configuration

1. Open the `my.cnf` configuration file in a text editor:

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

If the file is not present, try `/etc/mysql/my.cnf` or `/etc/my.cnf.d/community-mysql-server.cnf` or `/etc/mysql/mysql.conf.d/mysqld.cnf`.

2. Find the following configuration in the `[mysqld]` section of the `my.cnf` configuration file and modify the values:



- Create the `[mysqld]` section if it is not present in the file.
- If the parameters are not present in the file, add them to the `[mysqld]` section.
- To determine your MySQL version, run the command: `mysql --version`

Parameter	Comments and recommended values	MySQL version
<code>max_allowed_packet=33M</code>		All the <a href="#">supported versions</a> .
<code>log_bin_trust_function_creators=1</code>	Alternatively, you can disable the binary logging: <code>log_bin=0</code>	8.x
<code>innodb_log_file_size=100M</code> <code>innodb_log_files_in_group=2</code>	The multiplication of values of these two parameters must be at least <b>200</b> . The minimum value for <code>innodb_log_files_in_group</code> is <b>2</b> and maximum value is <b>100</b> ; the value also must be integer.	8.x

3. Press **CTRL + X** and type **Y** to save changes and close the file.

4. Restart the MySQL server and apply the configuration (in some cases, the service name is `mysqld`):

```
sudo systemctl restart mysql
```

5. Set up MySQL privileges and password (this step is optional and may not work for some Linux distributions):

a)Reveal the temporary MySQL password: `sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b)Copy and save the password.

c)Set a new password by following one of these options:

- Run `/usr/bin/mysql_secure_installation` and type the temporary password. Then you will be prompted to create a new password.

- Run `mysql -u root -p` and type the temporary password. Run `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';` to change the root password (replace `strong_new_password` with your password) and type `Quit`.

See also [Improve MySQL Installation Security](#) in the MySQL Reference Manual.

6. Verify that the MySQL server service is running:

```
sudo systemctl status mysql
```

## ODBC installation and configuration—Linux

**!** Ensure to install a [supported version of MySQL Server and ODBC Connector](#).

**i** You can install the Microsoft ODBC driver (version 13 and later) to connect the ESET PROTECT Server on Linux to Microsoft SQL Server on Windows. For more information, visit [this Knowledgebase article](#).

Install the MySQL ODBC driver using the Terminal. Follow the steps for your Linux distribution:

- [Debian, Ubuntu](#)
- [Red Hat](#)
- [Other supported Linux distributions](#)

**i** Your installation experience may vary according to the [supported Linux distribution](#) running on your server.

### Debian, Ubuntu

1. Install unixODBC drivers:

```
sudo apt install unixodbc
```

2. Download the ODBC connector:

```
wget <mysql-connector-package>
```

Replace `<mysql-connector-package>` with the download link to the package.

**i** You can download the MySQL ODBC connector from the [official MySQL site](#). Select and download the version [compatible](#) with your Linux distribution and version ([earlier versions](#) are also available).

3. Install the ODBC driver:

- Ubuntu 22.04/24.04, Debian 11/12—See [Installing Connector/ODBC from a DEB Distribution](#). Run the following command to install a `.deb` package on Ubuntu: `sudo dpkg -i package_file.deb`
- Debian 10 and Ubuntu 20.04—See [Installing Connector/ODBC from a Binary Tarball Distribution](#).

## Example of tar.gz driver installation steps:

1. Unzip the ODBC driver archive (package name may vary depending on link used):  
`gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`
2. Extract the ODBC driver (package name may vary depending on link used):  
`tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar`
3. Navigate to the ODBC driver folder (package name may vary depending on link used):  
`cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit`
4. Copy ODBC driver files:  
`sudo cp bin/* /usr/local/bin`  
`sudo cp lib/* /usr/local/lib`
5. Register the driver for ODBC.
  - For new Linux versions like Ubuntu 20.x, we recommend using the Unicode driver:  
`sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t "Driver=/usr/local/lib/libmyodbc8w.so"`
  - For other systems, or when Unicode driver is not working, use this command:  
`sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t "Driver=/usr/local/lib/libmyodbc8a.so"`

Run the following command to list the installed drivers:

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

## Red Hat

1. Install unixODBC drivers:

```
sudo dnf install unixODBC -y
```

2. Download the ODBC connector:

```
wget <mysql-connector-package>
```

Replace `<mysql-connector-package>` with the download link to the package.

**i** You can download the MySQL ODBC connector from the [official MySQL site](#). Select and download the version [compatible](#) with your Linux distribution and version ([earlier versions](#) are also available).

3. Install the ODBC driver:

**!** Do not install the ODBC connector using YUM/DNF—it would install the latest, not compatible version.

```
sudo rpm -ivh mysql-connector-odbc-9.3.0-1.el10.x86_64.rpm --nodeps
```

4. Set up the ODBC driver:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 9.3.0" -t "Driver=/usr/lib64/libmyodbc9w.so"
```

5. List the installed drivers:

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

## Other supported Linux distributions

1. Follow these instructions to install the ODBC driver:

- **SUSE Linux Enterprise Server:** `sudo zypper install unixODBC`.
- [Installing Connector/ODBC from an RPM Distribution](#)
- [Installing Connector/ODBC from a DEB Distribution](#)
- [Installing Connector/ODBC from a Binary Tarball Distribution](#)



The ESET PROTECT Server Rocky Linux installation with [mariadb-connector-odbc](#) driver fails with specific locales—Chinese, Korean, Japanese.

2. Run the following command to open the `odbcinst.ini` file in a text editor:

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

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

3. Copy the following configuration into the `odbcinst.ini` file (ensure the paths to **Driver** and **Setup** are correct), then save and close the file:

```
[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
```

The Driver may be in a different location for some distributions. You can find the file using the following command:

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

4. Update the configuration files that control ODBC access to database servers on the current host by running the following command:

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

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

## Server installation—Linux

### Installation

Follow the steps below to install the ESET PROTECT Server component on Linux using a Terminal command:



Ensure to meet all the installation [prerequisites](#).

1. Download the ESET PROTECT Server component:

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server_linux_x86_64.sh
```

2. Make the downloaded file executable:

```
chmod +x server_linux_x86_64.sh
```




3. You can prepare an installation script and then execute it using `sudo`.

Run the installation script based on the example below (New lines are split by "\ " for copying the whole command to Terminal):

```
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"
```

Run `sudo ./server_linux_x86_64.sh -h` to see the list all available parameters:

Attribute	Description	Required
<code>-h, --help</code>	Show the list of all available parameters.	-
<code>-v, --version</code>	Show the ESET PROTECT Server version.	-
<code>--uninstall</code>	<a href="#">Uninstalls</a> the application.	-
<code>--keep-database</code>	<a href="#">Uninstallation</a> will not remove the database.	-
<code>--locale</code>	The locale identifier (LCID) of the installed server (default value is <code>en_US</code> ). See <a href="#">supported languages</a> for available options. <div style="border: 1px solid blue; padding: 5px;"><p><b>i</b> If you do not specify the <code>--locale</code>, ESET PROTECT Server will be installed in English. After ESET PROTECT On-Prem installation, you can set a language for each ESET PROTECT Web Console session. Not all elements of the Web Console will change after the language change. Some of the elements (default dashboards, policies, tasks, etc.) are created during the ESET PROTECT On-Prem installation and their language cannot be changed.</p></div>	Yes
<code>--skip-os-check</code>	Do not check the operating system for minimum requirements.	-
<code>--skip-license</code>	The installation will not ask the user for Terms of Use confirmation.	-
<code>--server-port</code>	ESET PROTECT Server port (default value is 2222)	-

Attribute	Description	Required
--console-port	ESET PROTECT Web Console port (default value is 2223)	-
--server-root-password	Password for Web Console login of the Administrator user. <div style="border: 1px solid orange; padding: 5px; margin-top: 5px;">  The password must contain at least 14 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 17 characters. </div>	Yes
--db-type	The type of database that will be used (possible values: "MySQL Server", "MS SQL Server"). <a href="#">Microsoft SQL Server on Linux</a> is not supported. However, you can <a href="#">connect</a> the ESET PROTECT Server on Linux to Microsoft SQL Server on Windows.	-
--db-driver	ODBC driver used for connecting to database specified in the <i>odbcinst.ini</i> file (command <code>odbcinst -q -d</code> gives a list of available drivers, use one of these drivers for example: <code>--db-driver="MySQL ODBC 8.0 Driver"</code> , <code>--db-driver="MySQL ODBC 8.0 Unicode Driver"</code> or <code>--db-driver="MySQL ODBC 8.0.17"</code> ). <div style="border: 1px solid blue; padding: 5px; margin-top: 5px;">  The ESET PROTECT Server supports only the default MySQL database authentication method: <code> caching_sha2_password </code>. </div>	Yes
--db-hostname	Computer name or IP address of the database server. The named database instance is not supported.	Yes
--db-port	Port of the database server (default value is 3306).	Yes
--db-name	Name of ESET PROTECT Server database (default value is <code>era_db</code> ).	-
--db-admin-username	Database administrator username (used by installation for creating and modifying database). You can omit this parameter if there is a previously created database user-defined in <code>--db-user-username</code> and <code>--db-user-password</code>	Yes
--db-admin-password	Database administrator password. You can omit this parameter if there is a previously created database user-defined by <code>--db-user-username</code> and <code>--db-user-password</code>	Yes
--db-user-username	Database ESET PROTECT Server user username (used by ESET PROTECT Server for connecting to database); should be no longer than 16 characters.	Yes
--db-user-password	Database ESET PROTECT Server user password	Yes
--cert-hostname	Contains all the possible names and/or the IP of the ESET PROTECT Server computer. The value must match the server name specified in the Agent certificate that tries to connect to the server. <div style="border: 1px solid orange; padding: 5px; margin-top: 5px;">  To be able to use the <a href="#">REST API</a> in the ESET PROTECT Server, this list must contain <code>localhost</code> as one of its entries. </div>	Yes
--skip-cert	Skip generation of certificates (use with the <code>--server-cert-path</code> parameter).	-

Attribute	Description	Required
--server-cert-path	Path to server peer certificate (use this option if you specified --skip-cert as well)	-
--cert-auth-path	Path to the Server's Certificate Authority file	-
--server-cert-password	Password of server peer certificate	-
--peer-cert-password	Password of peer certificates which will be generated during installation.	-
--cert-auth-password	Certificate Authority password	-
--cert-auth-common-name	Certification Authority common name. Default is "Server Certification Authority". Use "" for no common name.	-
--cert-organizational-unit	Certificate organizational unit	-
--cert-organization	Certificate organization	-
--cert-locality	Certificate locality	-
--cert-state	Certificate state	-
--cert-country	Certificate country (default is US)	-
--cert-validity	Certificate validity in days or years (specify in argument --cert-validity-unit). Default is 10.	-
--cert-validity-unit	Unit for certificate validity, possible values are 'Years' or 'Days' (default value is Years)	-
--enable-imp-program	Turn on the Product improvement program.	-
--disable-imp-program	Turn off the Product improvement program.	-
--ad-server	Active Directory server	-
--ad-user-name	Name of the user who has rights to search the Active Directory network	-
--ad-user-password	Active Directory user password	-
--ad-cdn-include	Active Directory tree path (Container Distinguished Name) that will be synchronized; use empty brackets "" to synchronize a whole tree	-

We recommend that you delete commands containing sensitive data (for example, a password) from the command line history:

- i** 1. Run `history` to see the list of all commands in the history.
2. Run `history -d line_number` (specify the line number of the command). Alternatively, run `history -c` to delete the entire command line history.

## [Password type parameters](#)

Password type parameters can be provided as environment variables, files, read from `stdin`, or as plain text. That is:

- password=env:SECRET\_PASSWORD where SECRET\_PASSWORD is an environment variable with a password
- password=file:/opt/secret where first line of regular file /opt/secret contains your password
- password=stdin instructs the installer to read the password from standard input
- password="pass:PASSWORD" is equal to --password="PASSWORD" and is mandatory if the actual password is "stdin" (standard input) or a string starting with "env:", "file:" or "pass:"

4. The installation prompts if you want to participate in the Product improvement program. Press **Y** if you

agree to send crash reports and telemetry data to ESET or press **N** not to send any data.

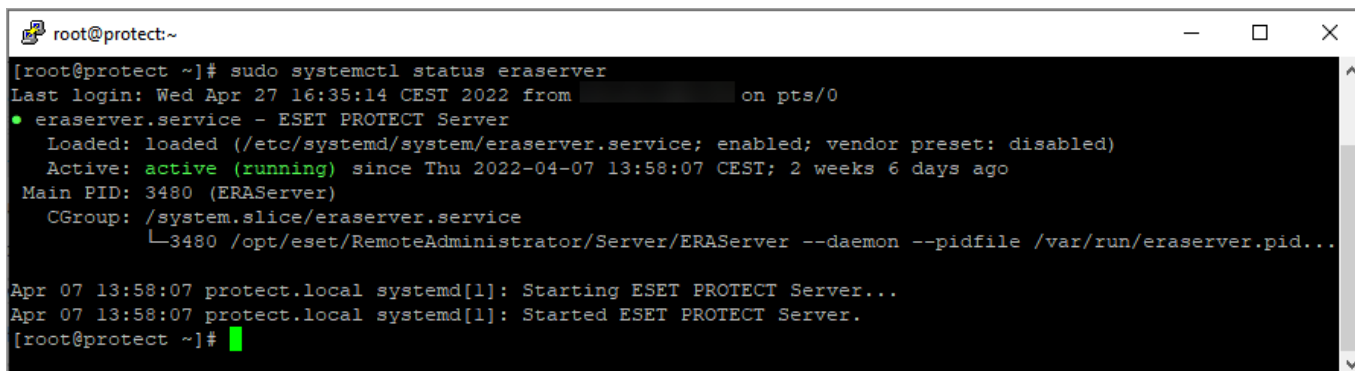
5. The ESET PROTECT Server and the `eraserver` service will be installed in the following location:

```
/opt/eset/RemoteAdministrator/Server
```

The installation may end with **SELinux policy... failure**. You can ignore it if you do not use SELinux.

6. After the installation, verify that the ESET PROTECT Server service is running using the command shown below:


```
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 ~]#
```

## Installer log


The installer log may be useful for troubleshooting and you can find it in [Log files](#).

 Do not change the computer name of your ESET PROTECT Server machine after the installation. See [Change of IP address or hostname on ESET PROTECT Server](#) for more information.

## Server prerequisites—Linux

Ensure to meet the following prerequisites to install the ESET PROTECT Server on Linux:

- You must have a [supported Linux operating system](#).
- The required ports must be open and available—see the complete [list of ports](#).
- [A database server must be installed and configured](#) with a root account. A user account does not have to be created before the installation. The installer can create the account. [Microsoft SQL Server on Linux](#) is not supported. However, you can [connect](#) the ESET PROTECT Server on Linux to Microsoft SQL Server on Windows.

 The ESET PROTECT Server stores large data blobs in the database. Configure MySQL to [accept large packet size](#) for ESET PROTECT On-Prem to run properly.  
The ESET PROTECT Server supports only the default MySQL database authentication method: `caching_sha2_password`.

- **ODBC Driver**—The ODBC Driver is used to establish a connection with the [database server](#) (MySQL).
- Set the server installation file as an executable using the Terminal command:

```
chmod +x server_linux_x86_64.sh
```

• We recommend that you **use the latest version of OpenSSL 1.1.1**. ESET Management Agent also supports OpenSSL 3.x. The minimum supported version of OpenSSL for Linux is openssl-1.0.1e-30. There can be more versions of OpenSSL installed on one system simultaneously. At least one supported version must be present on your system.

o Use the command `openssl version` to show the current default version.

o You can list all versions of OpenSSL present on your system. See the filename endings listed using the command `sudo find / -iname *libcrypto.so*`

o Verify if your Linux client is compatible using the following command: `openssl s_client -connect google.com:443 -tls1_2`

### OpenSSL 3.x support



- ESET Management Agent supports OpenSSL 3.x.
- ESET PROTECT Server does not natively support OpenSSL 3.x, but you can [enable the OpenSSL 3.x support for ESET PROTECT On-Prem](#).

- **Xvfb**—Required for proper report printing ([Generate Report](#)) on all Linux Server systems. On Rocky Linux, **gtk3** is also required for report printing.
- **Xauth**—The package gets installed together with **xvfb**.
- **cifs-utils**—Required for proper Agent deployment to a Windows operating system.
- **kinit + klist**—Kerberos is used to authenticate a domain user when logging in and the Active Directory synchronization task. Ensure to configure Kerberos properly (`/etc/krb5.conf`). ESET PROTECT On-Prem supports synchronization with multiple domains.
- **ldapsearch**—Used in AD synchronization task and for authorization.
- **snmptrap**—Optional; used to send SNMP traps. SNMP also requires configuration.
- **SELinux devel package**—Used during application installation to build SELinux policy modules. The package is only required on systems with SELinux enabled (RHEL). SELinux may cause problems with other applications. For ESET PROTECT Server, it is not necessary.
- **lshw**—Install the `lshw` package on the client/server Linux machine for the ESET Management Agent to report the [hardware inventory](#) correctly.

The table below contains the appropriate terminal commands for each package described above for various Linux distributions (run the commands as `sudo` or `root`):

Package	Debian and Ubuntu distributions	Red Hat distributions and Rocky Linux
ODBC Driver	See <a href="#">ODBC installation and configuration</a> .	See <a href="#">ODBC installation and configuration</a> .
OpenSSL	<code>apt install openssl -y</code>	<code>dnf install openssl -y</code>
xvfb gtk3 (Rocky Linux only)	<code>apt install xvfb -y</code>	<code>dnf install xorg-x11-server-Xvfb -y</code> <code>dnf install gtk3 -y</code>
cifs-utils	<code>apt install cifs-utils -y</code>	<code>dnf install cifs-utils -y</code>
kinit + klist (optional)	<code>apt install krb5-user -y</code>	<code>dnf install krb5-workstation -y</code>
ldapsearch	<code>apt install ldap-utils libsasl2-modules-gssapi-mit -y</code>	<code>dnf install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y</code>
snmptrap (optional)	<code>apt install snmp -y</code>	<code>dnf install net-snmp-utils net-snmp -y</code>

Package	Debian and Ubuntu distributions	Red Hat distributions and Rocky Linux
SELinux devel package (optional)	<code>apt install selinux-policy-dev -y</code>	<code>dnf install policycoreutils-devel -y</code>
samba (optional; necessary only for remote deployment)	<code>apt install samba -y</code>	<code>dnf install samba samba-winbind-clients -y</code>
lshw	<code>apt install lshw -y</code>	<code>dnf install lshw -y</code>

# Agent installation—Linux

## Prerequisites

- We recommend that you **use the latest version of OpenSSL 1.1.1**. ESET Management Agent also supports OpenSSL 3.x. The minimum supported version of OpenSSL for Linux is openssl-1.0.1e-30. There can be more versions of OpenSSL installed on one system simultaneously. At least one supported version must be present on your system.

o Use the command `openssl version` to show the current default version.

o You can list all versions of OpenSSL present on your system. See the filename endings listed using the command `sudo find / -iname *libcrypto.so*`

o Verify if your Linux client is compatible using the following command: `openssl s_client -connect google.com:443 -tls1_2`

### OpenSSL 3.x support



- ESET Management Agent supports OpenSSL 3.x.
- ESET PROTECT Server does not natively support OpenSSL 3.x, but you can [enable the OpenSSL 3.x support for ESET PROTECT On-Prem](#).

- Install the `lshw` package on the client/server Linux machine for the ESET Management Agent to report the [hardware inventory](#) correctly.

Linux distribution	Terminal command
Debian, Ubuntu	<code>sudo apt install lshw -y</code>
Red Hat	<code>sudo yum install lshw -y</code>
SUSE Linux Enterprise Server	<code>sudo zypper install lshw</code>


- For Linux CentOS, we recommend installing the `policycoreutils-devel` package. Run the command to install the package:

```
yum install policycoreutils-devel
```

- The server computer must be reachable from the network and have [ESET PROTECT Server](#) installed.
- A [Certificate](#) for the Agent must be present.
- A server [Certification Authority](#) public key file must be present.

# Installation

Follow the steps below to install the ESET Management Agent component on Linux using a Terminal command:

 Ensure to meet all the installation prerequisites listed above.


1. Download the Agent installation script:


```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent_linux_x86_64.sh
```

2. Make the file executable:

```
chmod +x agent_linux_x86_64.sh
```

3. Run the installation script based on the example below (New lines are split by "\" for copying the whole command to Terminal):


 For more details, see [Parameters](#) below.

 ESET Management Agent 12.0 and later no longer supports the server-assisted installation.

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
```

We recommend that you delete commands containing sensitive data (for example, a password) from the command line history:


-  1.Run `history` to see the list of all commands in the history.
- 2.Run `history -d line_number` (specify the line number of the command). Alternatively, run `history -c` to delete the entire command line history.

4. When prompted, press **y** to accept the certificate. You can ignore any errors about SELinux returned by the installer.

5. After the installation, verify that the ESET Management Agent service is running:

```
sudo systemctl status eraagent
```

6. Set the **eraagent** service to start at boot: `sudo systemctl enable eraagent`

 **Installer log**  
The installer log may be useful for troubleshooting. You can find it in [Log files](#).

## Parameters

Connection to the ESET PROTECT Server is resolved using the parameters `--hostname` and `--port` (port is not used when an SRV record is provided). [Possible connection formats.](#)

- **Hostname and port**
- **IPv4 address and port**
- **IPv6 address and port**
- **Service record (SRV record)**—To configure the DNS resource record in Linux, the computer must be in a domain with a working DNS server. See [DNS resource record](#). The SRV record must start with the prefix "`_NAME._tcp`" where 'NAME' represents custom naming (for example, "era").

Attribute	Description	Required
<code>-h, --help</code>	Show the list of all available parameters.	No
<code>-v, --version</code>	Show the Agent version.	No
<code>--uninstall</code>	Uninstall the Agent.	No
<code>--skip-license</code>	The installation will not ask the user for Terms of Use confirmation.	No
<code>--hostname</code>	Hostname or IP address of ESET PROTECT Server to connect.	Yes
<code>--port</code>	ESET PROTECT Server port (default value is 2222).	Yes
<code>--cert-path</code>	Local path to the Agent certificate file (more about <a href="#">certificate</a> ).	Yes
<code>--cert-password</code>	Agent Certificate password.	Yes
<code>--cert-auth-path</code>	Path to the Server Certificate Authority file (more about <a href="#">authority</a> ).	Yes
<code>--cert-auth-password</code>	Certificate Authority password.	Yes (if used)
<code>--cert-content</code>	Base64 encoded content of PKCS12 encoded public key certificate plus private key used to set up secure communication channels with Server and Agents. Use only one of the <code>--cert-path</code> or <code>--cert-content</code> options.	No
<code>--cert-auth-content</code>	Base64 encoded content of DER-encoded Certificate Authority private key certificate used to verify remote peers (Proxy or Server). Use only one of the <code>--cert-auth-path</code> or <code>--cert-auth-content</code> options.	No
<code>--proxy-hostname</code>	HTTP Proxy hostname. Use this parameter to enable using HTTP Proxy (already installed in your network) for replication between ESET Management Agent and ESET PROTECT Server (not for caching of updates).	If a proxy is used
<code>--proxy-port</code>	HTTP Proxy port for connecting to the server.	If a proxy is used
<code>--proxy-user</code>	Username for HTTP Proxy.	No
<code>--proxy-password</code>	Password for HTTP Proxy.	No
<code>--enable-imp-program</code>	Turn on the Product improvement program.	No
<code>--disable-imp-program</code>	Turn off the Product improvement program.	No

## Connection and certificates

- **Connection to the ESET PROTECT Server** must be provided: `--hostname`, `--port` (port is not needed if service record is provided, the default port value is 2222)
- Provide certificate information for offline installation: `--cert-path`, `--cert-password`. Installation parameters `--cert-path` and `--cert-auth-path` require certification files (`.pfx` and `.der`) which can be exported from ESET PROTECT Web Console. (Read how to [export the .pfx file](#) and the [.der file](#).)

### [Password type parameters](#)

Password type parameters can be provided as environment variables, files, read from `stdin`, or as plain text. That is:

- `--password=env:SECRET_PASSWORD` where `SECRET_PASSWORD` is an environment variable with a password
- `--password=file:/opt/secret` where first line of regular file `/opt/secret` contains your password
- `--password=stdin` instructs the installer to read the password from standard input
- `--password="pass:PASSWORD"` is equal to `--password="PASSWORD"` and is mandatory if the actual password is `"stdin"` (standard input) or a string starting with `"env:"`, `"file:"` or `"pass:"`

- The certificate passphrase must not contain the following characters: " \ These characters cause a critical error during Agent initialization.
- The password must contain at least 14 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 17 characters.

## HTTP Proxy connection

If you are using HTTP Proxy for replication between ESET Management Agent and ESET PROTECT Server (not for caching of updates), you can specify the connection parameters in `--proxy-hostname` and `--proxy-port`.

EXAMPLE—Offline Agent installation with HTTP Proxy Connection:

```
./agent_linux_x86_64.sh \  
--skip-license \  
--cert-path=/home/admin/Desktop/agent.pfx \  
--cert-auth-path=/home/admin/Desktop/CA.der \  
--cert-password=N3lluI4#2aCC \  
--hostname=10.1.179.36 \  
--port=2222 \  
--proxy-hostname=10.1.180.3 \  
--proxy-port=3333 \  

```

- The communication protocol between Agent and ESET PROTECT Server does not support authentication. Any proxy solution used for forwarding Agent communication to ESET PROTECT Server that requires authentication will not work. If you choose to use a non-default port for the Web Console or Agent, it may require a firewall adjustment. Otherwise, the installation may fail.

## Upgrade and repair installation of Agent on Linux

If you run the Agent installation manually on a system where the Agent is already installed, the following scenarios can occur:

- **Upgrade**—Run a later version of the installer. The Agent is upgraded and new certificates are used.
- **Repair**—Run the same version of the installer. You can use this option to migrate the Agent to a different ESET PROTECT Server. The Agent is reinstalled and new certificates are used.

## Web Console installation—Linux

Follow these steps to install the ESET PROTECT Web Console:

- You can install the ESET PROTECT Web Console on a different computer than the computer running the ESET PROTECT Server. This procedure requires [additional steps](#).

1. Install the Apache Tomcat and Java packages.

## Packages may have different names and may not be available in the default repository



- Example package names below may differ from your Linux distribution repository packages.
- Your Linux distribution's default repository may not contain the latest [supported version of Apache Tomcat and Java](#). For example, you must manually install Tomcat 9 on Ubuntu 24.04 and Debian 12 because their default repositories contain the unsupported Tomcat 10.
- For installation and configuration of Apache Tomcat, see the [Apache Tomcat documentation](#).

Linux distribution	Terminal commands
Debian and Ubuntu distributions	<pre>sudo apt update sudo apt install openjdk-17-jdk tomcat9</pre>
Red Hat distributions and Rocky Linux	<pre>dnf update dnf install java-17-openjdk tomcat</pre>
SUSE Linux Enterprise Server	<pre>zypper refresh sudo zypper install java-17-openjdk tomcat9</pre>

2. Download the Web Console file (*era\_x64.war*):

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era_x64.war
```

3. Rename the *era\_x64.war* file to *era.war*:

```
mv era_x64.war era.war
```

4. Copy the *era.war* file to the Tomcat folder:

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

5. Restart the Tomcat service to deploy the *era.war* file:

```
sudo systemctl restart tomcat (or tomcat9 based on the service name)
```

6. Verify the *era* folder is present in the Tomcat folder (replace *Path\_to\_Tomcat* with the Tomcat folder):

```
ls Path_to_Tomcat
```

The output should look like this: *era era.war*

7. Set the Tomcat service to start at boot: `sudo systemctl enable tomcat` (or `tomcat9` based on the service name)

8. If you installed the ESET PROTECT Web Console on a different computer than the ESET PROTECT Server, perform these additional steps to enable communication between ESET PROTECT Web Console and ESET PROTECT Server:

a) Stop the Tomcat service: `sudo systemctl stop tomcat`

b) Edit the *EraWebServerConfig.properties* file:

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

If the *EraWebServerConfig.properties* file is not present in the above path, you can use the following command to find the file on your system:

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

c) Find the `server_address=localhost`

d) Replace `localhost` with the IP address of your ESET PROTECT Server and save the file.

e) Restart the Tomcat service: `sudo systemctl restart tomcat` (or `tomcat9` based on the service name)

f) Set the Tomcat service to start at boot: `sudo systemctl enable tomcat` (or `tomcat9` based on the service name)


9. Open the ESET PROTECT Web Console in a [supported web browser](#) to see a login screen:

- From the computer hosting the ESET PROTECT Web Console: `http://localhost:8080/era`
- From any computer with internet access to the ESET PROTECT Web Console (substitute `IP_ADDRESS_OR_HOSTNAME` with the IP address or hostname of your ESET PROTECT Web Console): `http://IP_ADDRESS_OR_HOSTNAME:8080/era`

10. Configure the Web Console after the installation:


- The default HTTP port is set to 8080 during the manual installation of Apache Tomcat. We recommend that you set up an [HTTPS connection for Apache Tomcat](#).
- See the additional [Web Console configuration for enterprise solutions or low-performance systems](#).

## Rogue Detection Sensor installation—Linux

 ESET Rogue Detection (RD) Sensor will be deprecated (there will be no future updates). Some of its features may not work properly. You can no longer manage RD Sensor configuration via a policy.


### Prerequisites

- The Network can be searched (ports are open, the firewall is not blocking incoming communication, etc.).
- The ESET PROTECT Server computer is reachable.
- [ESET Management Agent](#) must be installed on the local computer to support all program features fully.

 If there are multiple network segments, Rogue Detection Sensor must be installed separately on each network segment to produce a comprehensive list of all devices on the whole network.

## Installation

Follow the steps below to install the RD Sensor component on Linux using a Terminal command:

 Ensure to meet all the installation prerequisites listed above.

1. Visit the ESET PROTECT [download section](#) to download a standalone installer for this ESET PROTECT component (*rdsensor-linux-i386.sh* or *rdsensor\_linux\_x86\_64.sh*).

2. Open the Terminal and set RD Sensor installation file as an executable: `chmod +x rdsensor_linux_x86_64.sh`

3. Use the following command to run the installation file as sudo:

```
sudo ./rdsensor_linux_x86_64.sh
```

4. Read the End User License Agreement. Use the **Space bar** to proceed to the next page. The installer will prompt you to specify whether you accept the agreement. Press **Y** on your keyboard if you agree. Otherwise, press **N**.

5. Press **Y** if you agree to participate in the Product improvement program. Otherwise, press **N**.

6. ESET Rogue Detection Sensor will start after installation completes.

7. To see if the installation was successful, verify that the service is running by executing the following command:

```
sudo systemctl status rdsensor
```

You can find the Rogue Detection Sensor log file in [Log files](#): `/var/log/eset/RogueDetectionSensor/trace.log`

## Mirror Tool—Linux

[Are you a Windows user?](#)

The Mirror Tool is necessary for offline detection engine updates. If your client computers do not have an internet connection and need detection engine updates, you can use the Mirror Tool to download update files from ESET update servers and store them locally.

The Mirror Tool has these functions:

- Application module updates—It downloads detection engine updates and other application modules, but not [auto-updates](#) (uPCU).
- Repository creation—It can create a full [offline repository](#), including [auto-updates](#) (uPCU).

The Mirror Tool does not download ESET LiveGrid® data.

## Changelog

The following content is dynamic and can only be accessed online. [Visit the website to view the content.](#)

## Prerequisites

- The Mirror Tool for Linux supports these 64-bit operating systems:

- oUbuntu 20.04 LTS/22.04 LTS/24.04 LTS

- oRHEL Server 8

- oDebian 10/11

- oRocky Linux 9

- The repository where the mirror is created must have read and execute permissions for all users. Run this command as a privileged user to grant the permission: `chmod 755 mirror/folder/path` (replace `mirror/folder/path` with the mirror folder path).
- The target folder must be available for sharing, Samba/Windows or HTTP/FTP service, depending on how you want to have the updates accessible.

- oESET security applications for Windows—You can update them remotely using HTTP or a shared folder.

- oESET security applications for Linux/macOS—You can update them remotely only using HTTP. If you use a shared folder, it must be on the same computer as the ESET security application.

- You must have a valid offline activation file needed for the activation of the Mirror Tool and generation of the update mirror. You can generate the offline activation file in ESET Business Account or ESET PROTECT Hub:

- oIn [ESET Business Account](#), select the **Include Username and Password** check box.

- oIn [ESET PROTECT Hub](#), select the **Allow online activation** check box.

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

Create offline license file

• *Required field*

**Solution**

ESET Endpoint Antivirus + ESET Server Security

• **Offline license name**

Offline

**Quantity**

0

**ESET PROTECT on-prem**

Allow management with ESET PROTECT

**ESET PROTECT token** ⓘ

Insert an ESET PROTECT token

**Online activation** ⓘ

Allow online activation

CREATE CLOSE

## How to use the Mirror Tool

1. Download the Mirror Tool from the [ESET download page](#) (**Standalone installers** section).
2. Unzip the downloaded archive.
3. Open the Terminal in the folder with the *MirrorTool* file and make the file executable:

```
chmod +x MirrorTool
```

4. Run the command below to view all available parameters for the Mirror Tool and its version:

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

```

user@ubuntu: ~/Desktop/MirrorTool_Linux_x86_64$ ./MirrorTool --help
[Info] Mirror Tool v1.2.143.0, Copyright (c) ESET, spol. s r.o. 1992-2024. All rights reserved.
[Info] 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).
Windows only
--networkDrivePassword arg [optional]
Password used, when output directory is accessed using smb(e.g:\\hostname).
Windows only
--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(=AUTOSELECT)] [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, dyltb.
Parameter is ignored when creating mirror for legacy products (ep4, ep5) - only dat format is supported.
--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.
--logLevel arg [optional]
Specifies logging level - options can be: error, warning, info, debug.
--logFilename arg [optional]
Specifies where to store log file.
--logIntoStandardPath [optional]
Stores log file into standard path - 'ProgramData' on Windows, '/var/log' on Linux
--help [optional]
Display this help and exit

```

## Parameters limitations

The Mirror Tool parameters support only ASCII characters.



Case sensitivity:

- Mirror Tool 1.0.x—All the parameters are case-sensitive.
- Mirror Tool 1.2.x and later—All the parameters are case-insensitive.

You can use the parameters to create the repository mirror or application modules mirror:

### [Parameters for both repository and application modules mirror](#)



--proxyHost	
--proxyPort	
--proxyUsername	
--proxyPassword	
--help	
--logLevel	Set log level. The following values are available: error, warning, info (default), debug. Example: <code>--logLevel debug</code> The parameter is available since Mirror Tool 1.2.x.
--logFilename	Set the log filename and its location. Example: <ul style="list-style-type: none"><li>• Windows: <code>--logFilename C:\MT_log.txt</code></li><li>• Linux: <code>--logFilename ~/Downloads/MT_log.txt</code></li></ul> The parameter is available since Mirror Tool 1.2.x.
--logIntoStandardPath	Enable logging into the standard path: <ul style="list-style-type: none"><li>• Windows: C:\ProgramData\ESET\RemoteAdministrator\MirrorTool\Logs</li><li>• Linux: /var/log/eset/RemoteAdministrator/MirrorTool/Logs</li></ul> You cannot combine <code>--logIntoStandardPath</code> with <code>--logFilename</code> . The parameter is available since Mirror Tool 1.2.x.
--useSecureConnection	Uses HTTPS connections to update servers. The parameter is available since Mirror Tool 1.2.202.

### [Repository-specific parameters](#)

--repositoryServer	See the <a href="#">repository details in ESET PROTECT Settings</a> . If you do not provide the value, AUTOSELECT is used by default.
--intermediateRepositoryDirectory	
--outputRepositoryDirectory	
--compatibilityVersion	
--dryRun	
--filterFilePath	
--trustDownloadedFilesInRepositoryTemp	

### [Modules-specific parameters](#)

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

Parameter	Description
--updateServer	<p>The Mirror Tool creates <a href="#">a folder structure</a> different from what Endpoint mirror does. Each folder holds update files for a group of applications.</p> <div style="border: 1px solid red; padding: 5px;"> <p> You must specify the <a href="#">update server full link</a> (full path to the correct folder) in the update settings of the application using the mirror.</p> </div>
--offlineLicenseFilename	You must specify a path to your offline activation file (as mentioned above).
--mirrorOnlyLevelUpdates	No argument needed. If set, only level updates will be downloaded (nano updates will not be downloaded). Read more about update types in our <a href="#">Knowledgebase article</a> .
--mirrorFileFormat	<div style="border: 1px solid red; padding: 5px;"> <p> Before using the <code>--mirrorFileFormat</code> parameter, ensure that you environment does not contain both earlier (6.5 and earlier) and later (6.6. and later) ESET security application versions. The incorrect usage of this parameter may result in incorrect updates of your ESET security applications.</p> </div> <p>You can specify which type of update files will be downloaded. Possible values (case sensitive):</p> <ul style="list-style-type: none"> <li>• <code>dat</code>—Use this value if you have environment only with ESET security application versions 6.5 and earlier.</li> <li>• <code>dll</code>—Use this value if you have environment only with ESET security application versions 6.6 and later.</li> <li>• <code>dylib</code>—Use this value if you have environment only with ESET security application for macOS version 8 and later.</li> </ul> <p>This optional parameter applies to the Mirror Tool distributed with ESET PROTECT On-Prem 8.1 and later.</p> <p>The Mirror Tool will download update files compatible with ESET PROTECT On-Prem repository version you specify in the parameter argument in format <code>x.x</code> or <code>x.x.x.x</code>, for example: <code>--compatibilityVersion 13.0</code> or <code>--compatibilityVersion 8.1.13.0</code>.</p> <p>The <code>--compatibilityVersion</code> parameter excludes the <a href="#">auto-updates</a> (uPCU) from the mirror. If you need the auto-updates (uPCU) in your environment and want to decrease the mirror size, use the <code>--filterFilePath</code> parameter.</p>
--compatibilityVersion	<p>This optional parameter applies to the Mirror Tool distributed with ESET PROTECT On-Prem 8.1 and later.</p> <p>The Mirror Tool will download update files compatible with ESET PROTECT On-Prem repository version you specify in the parameter argument in format <code>x.x</code> or <code>x.x.x.x</code>, for example: <code>--compatibilityVersion 13.0</code> or <code>--compatibilityVersion 8.1.13.0</code>.</p> <p>The <code>--compatibilityVersion</code> parameter excludes the <a href="#">auto-updates</a> (uPCU) from the mirror. If you need the auto-updates (uPCU) in your environment and want to decrease the mirror size, use the <code>--filterFilePath</code> parameter.</p>



To reduce the amount of data downloaded from the ESET repository, we recommend that you use the new parameters in Mirror Tool distributed with ESET PROTECT On-Prem 9: `--filterFilePath` and `--dryRun`:

1. Create a filter in a *JSON* format (see `--filterFilePath` below).

**i** 2. Perform a test Mirror Tool run with the `--dryRun` parameter (see below) and adjust the filter as necessary.

3. Run the Mirror Tool with the `--filterFilePath` parameter and the defined download filter, together with `--intermediateRepositoryDirectory` and `--outputRepositoryDirectory` parameters.

4. Run the Mirror Tool regularly to always use the latest installers.

Parameter	Description
<pre>--filterFilePath</pre>	<p>Use this optional parameter to filter ESET security applications based on a text file in <i>JSON</i> format placed in the same folder as Mirror Tool, for example: <code>--filterFilePath filter.txt</code>.</p> <p><a href="#">Filter configuration description:</a></p> <p>The configuration file format for application filtering is <i>JSON</i> with the following structure:</p> <ul style="list-style-type: none"> <li>• root <i>JSON</i> object: <ul style="list-style-type: none"> <li>• <code>use_legacy</code> (boolean, optional)—if true, legacy applications will be included.</li> <li>• <code>defaults</code> (<i>JSON</i> object, optional)—defines filter properties that will be applied to all applications. <ul style="list-style-type: none"> <li>■ <code>languages</code> (list)—Specify ISO language codes of languages to include, for example for French type "fr_FR". Other languages codes are in the <a href="#">table below</a>. To select more languages, separate them by a comma and a space, for example: (["en_US", "zh_TW", "de_DE"])</li> <li>■ <code>platforms</code> (list)—platforms to include (["x64", "x86", "arm64"]).</li> </ul> <div data-bbox="531 600 1473 705" style="border: 1px solid red; padding: 5px;"> <p> Use the <code>platforms</code> filter carefully. For example, if the Mirror Tool downloads only 64-bit installers and there are 32-bit computers in your infrastructure, 64-bit ESET security applications will fail to install on 32-bit computers.</p> </div> </li> <li>■ <code>os_types</code> (list)—operating system types to include (["windows"], ["linux"], ["mac"]).</li> <li>• <code>products</code> (list of <i>JSON</i> objects, optional)—filters to apply to specific applications—override <code>defaults</code> for specified applications. The objects have the following properties: <ul style="list-style-type: none"> <li>■ <code>app_id</code> (string)—required if <code>name</code> is not specified.</li> <li>■ <code>name</code> (string), required if <code>app_id</code> is not specified.</li> <li>■ <code>version</code> (string)—specifies version or range of versions to include.</li> <li>■ <code>languages</code> (list)—ISO language codes of languages to include (see the <a href="#">table below</a>).</li> <li>■ <code>platforms</code> (list)—platforms to include (["x64", "x86", "arm64"]).</li> <li>■ <code>os_types</code> (list)—operating system types to include (["windows"], ["linux"], ["mac"]).</li> </ul> <div data-bbox="531 1137 1473 1211" style="border: 1px solid blue; padding: 5px;"> <p> To determine appropriate values for the fields, run Mirror Tool in dry run mode and find the relevant application in the created CSV file.</p> </div> </li> </ul> </li> </ul> <p><b>Version string format descriptions</b></p> <p>All version numbers—consist of four numbers separated by dots (for example, 7.1.0.0). You can specify less numbers when writing version filters (for example, 7.1) and the rest of the numbers will be zero (7.1 is equal to 7.1.0.0).</p> <p>Version string can have one of the two following formats:</p> <ul style="list-style-type: none"> <li>• <code>[&gt; &lt; &gt;= &lt;= &lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))]</code></li> </ul> <p><code>O</code>Selects versions higher/smaller or equal/less or equal/equal than the version specified.</p> <ul style="list-style-type: none"> <li>• <code>&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))-&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;.(&lt;n&gt;)))]</code></li> </ul> <p><code>O</code>Selects versions that are higher than or equal to the lower bound and less than or equal to the higher bound.</p> <p>Comparisons are done numerically on each part of the version number, left to right.</p> <div data-bbox="531 1585 1236 2096" style="border: 1px solid green; padding: 10px;"> <p><b>JSON example</b></p> <pre>{   "use_legacy": true,   "defaults": {     "languages": [ "en_US" ],     "platforms": [ "x64", "x86" ]   },   "products": [     ✓ {       "app_id": "com.eset.apps.business.ees.windows",       "version": "7.1.0.0 - 8.0.0.0"     },     {       "app_id": "com.eset.apps.business.eea.windows",       "version": "&gt;7.1.0.0"     }   ] }</pre> </div>

The `--filterFilePath` parameter replaces the `--languageFilterForRepository`, `--productFilterForRepository` and `--downloadLegacyForRepository` parameters used in earlier Mirror Tool versions (released with ESET PROTECT On-Prem 8.x).

Parameter	Description
--dryRun	<p>When you use this optional parameter, Mirror Tool will not download any files, but it will generate a .csv file listing all packages that will be downloaded.</p> <p>You can use this parameter without mandatory parameters --intermediateRepositoryDirectory and --outputRepositoryDirectory, for example:</p> <ul style="list-style-type: none"> <li>• Windows: MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv</li> <li>• Linux: sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv</li> </ul> <div style="border: 1px solid blue; padding: 5px;"> <p><b>i</b> Some ESET installers are language-generic (with the multilang language code) and the Mirror Tool will list them in the .csv file even if you specify languages in --filterFilePath.</p> </div> <p>If you use the --dryRun parameter and also --intermediateRepositoryDirectory and --outputRepositoryDirectory parameters, the Mirror Tool does not clear the outputRepositoryDirectory.</p>
--listUpdatableProducts	<p>List all ESET applications for which the Mirror Tool can download application module updates (unless --excludedProducts is used).</p> <p>The parameter is available from Mirror Tool versions: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).</p>
--networkDriveUsername	<p>Username used to access the output directory via SMB (for example, \\hostname). The parameter works only on Mirror Tool for Windows.</p>
--networkDrivePassword	<p>Password used to access the output directory via SMB. The parameter works only on Mirror Tool for Windows.</p>

## Mirror Tool folder structure

By default, if you do not specify the --updateServer parameter, the Mirror Tool creates this folder structure on your HTTP server:

### Do not use an HTTP-only mirror server



Ensure the local mirror server uses HTTP and HTTPS protocols or only HTTPS. If the mirror server uses only HTTP, you cannot use the Software Install client task because the ESET security application EULA or Terms of Use cannot be retrieved from an HTTP server.

Mirror Tool default folders	ESET security application	Update server (according to your HTTP server root location)
mirror/eset_upd/era6	ESET PROTECT On-Prem (all versions)	To update the ESET PROTECT On-Prem 13.0 from the mirror, set the <a href="#">Update server</a> to <code>http://your_server_address/mirror/eset_upd/era6</code>
mirror/eset_upd/ep[version]	ESET Endpoint Antivirus/Security version 6.x (and later) for Windows. Each major version has its folder, for example, ep10 for version 10.x.	<code>http://your_server_address/mirror/eset_upd/ep10</code> (an example for version 10.x)
mirror/eset_upd/v5	ESET Endpoint Antivirus/Security version 5.x for Windows	<code>http://your_server_address/mirror/eset_upd/v5</code>

## ESET security applications for Linux/macOS

**!** You must specify the `--updateServer` parameter and create additional folders to update ESET security applications for Linux/macOS from the HTTP mirror (see below).

<code>--updateServer</code>	Additional Mirror Tool folder	ESET security application	Update server (according to your HTTP server root location)
<code>http://update.eset.com/eset_upd/businesslinux</code>	<code>mirror/eset_upd/BusinessLinux</code>	ESET Endpoint Antivirus for Linux	<code>http://your_server_address/mirror/eset_upd/BusinessLinux</code>
<code>http://update.eset.com/eset_upd/serverlinux</code>	<code>mirror/eset_upd/LinuxServer</code>	ESET Server Security for Linux	<code>http://your_server_address/mirror/eset_upd/LinuxServer</code>
<code>http://update.eset.com/eset_upd/businessmac</code>	<code>mirror/eset_upd/BusinessMac</code>	ESET Endpoint Security version 7.x+ for macOS	<code>http://your_server_address/mirror/eset_upd/BusinessMac</code>
<code>http://update.eset.com/eset_mobile/eesa</code>	<code>mirror/eset_upd/EndpointAndroid</code>	ESET Endpoint Security for Android	<code>http://your_server_address/mirror/eset_upd/EndpointAndroid</code>

### [Language codes table](#)

To create a mirror, run the Mirror Tool with at least the minimum required parameters. Here is an example:

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

Here is an example of more advanced configuration for an offline repository with selected applications, languages and enabled download of legacy files defined in the `filter.txt` file (see the file contents example in `--filterFilePath` details above):

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

We recommend that you delete commands containing sensitive data (for example, a password) from the command line history:

1. Run `history` to see the list of all commands in the history.
2. Run `history -d line_number` (specify the line number of the command). Alternatively, run `history -c` to delete the entire command line history.

## Mirror Tool and Update settings

- To automate downloads for application modules updates, you can create a schedule to run the Mirror Tool. To do so, open your Web Console and click **Client Tasks > Operating System > Run Command. Select Command line to run** (including a path to the *MirrorTool.exe*) and a reasonable trigger (such as CRON for every hour 0 0 \* \* \* ? \*). Alternatively, you can use the Windows Task Scheduler or Cron in Linux.
- To configure updates on a client computer(s), create a new policy and configure **Update server** to point to your mirror address or shared folder.

## Offline Repository—Linux

You can use the Mirror Tool to create an offline repository on Linux ([Are you a Windows user?](#)) when using closed computer networks or networks with limited internet access. You can use the Mirror Tool to create a clone of the ESET repository in a local folder. This cloned repository can be moved (for example, onto an external disk) to a location in the closed network. You can copy the repository to a secure location in the local network and make it available via an HTTP server (for example, ESET Bridge).

To update the offline repository, run the same command with the same parameters as used for offline repository creation. Previous data in the intermediary folder will be used, and only outdated files will be downloaded.



Be aware that the size of the repository is growing, and the intermediary directory will be the same size. Ensure you have at least **1.2 TB** of free space before starting this procedure.

## Best practices

See also the ESET Knowledgebase article [Best practices for using the ESET PROTECT On-Prem in an offline environment](#).

## Example scenario for Linux

### I. Create repository clone

1. [Download](#) the Mirror Tool.
2. Extract the Mirror Tool from the downloaded *.zip* file.
3. Prepare (create) folders for:
  - intermediary files
  - final repository
4. Open the Terminal in the folder with the *MirrorTool* file and make the file executable:

```
chmod +x MirrorTool
```

5. Run the following command (change the intermediary and output repository directories to the folders from step 3):

```
./MirrorTool --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory ~/Documents/Intermediary ^
--outputRepositoryDirectory ~/Documents/Repository
```

6. After the repository is copied to the `outputRepositoryDirectory` folder, move the folder and its contents to another machine where your closed network is accessible.

## II. Set up the HTTP server

1. You need an HTTP server running on the machine in the closed network. You can use:

- ESET Bridge proxy from the ESET [download site](#) (this scenario)
- a different HTTP server

2. [Install ESET Bridge](#) proxy.

## III. Run the offline repository

1. Navigate to `/opt/eset/bridge/etc` and open the `pkgid` file using a simple text editor. Change the `http_proxy_settings_static_content_enabled` setting to `true` to activate the offline repository server. Save the changes and close the `pkgid` file.

2. Copy the downloaded repository from step 6 (section I. above) to the offline repository server directory:

- The default offline repository server directory is `/var/opt/eset/bridge/OfflineRepository` with proper access rights.
- To use a custom directory, create a new folder for the offline repository (for example, `/var/opt/CustomOfflineRepository`). In the `pkgid` file, replace the line `"http_proxy_settings_offline_repository_dirPath": "%DATADIR%\OfflineRepository"` with `"http_proxy_settings_offline_repository_dirPath": "/var/opt/CustomOfflineRepository"`.

oThe `eset-bridge` user needs full access rights to the directory. Use this Terminal command to grant the access rights: `sudo chown -R eset-bridge:eset-bridge /var/opt/CustomOfflineRepository`

oCopy the downloaded repository into `/var/opt/CustomOfflineRepository`.

3. Restart the ESET Bridge service using the Terminal command: `sudo systemctl restart EsetBridge.service`. You must restart the service only after changing the `pkgid` file—the service restart is unnecessary when the repository data is changed, deleted, or added.

4. The offline repository runs on the address `http://YourIPAddress:4449` (for example, `http://10.1.1.10:4449`).

5. Set the new repository address using the ESET PROTECT Web Console:

a. [ESET PROTECT Server](#)—Click **More > Settings > Advanced Settings > Repository** and type the offline repository address into the **Server** field.

b. [ESET Management Agents](#)—Click **Policies**, click the Agent policy > **Edit > Settings > Advanced Settings > Repository** > type the offline repository address into the **Server** field.

c. ESET endpoint applications (for Windows)—Click **Policies**, click the **ESET Endpoint for Windows** policy > **Edit** > **Settings** > **Updates** > **Profiles** > **Updates** > **Application Updates** > type the offline repository address into the **Custom server** field.

## Component installation on macOS

In most installation scenarios, you need to install different ESET PROTECT components on different machines to accommodate different network architectures, meet performance requirements, or for other reasons.

**i** macOS is supported as a client only. The [ESET Management Agent](#) and [ESET applications for macOS](#) can be installed on macOS. However, ESET PROTECT Server cannot be installed on macOS.

## Agent installation—macOS

You can install ESET Management Agent on macOS in two ways:

- Remotely—Using the Server task **Agent deployment**. If you experience problems deploying ESET Management Agent remotely (the Server task **Agent deployment** ends with a failed status), refer to [Agent deployment troubleshooting](#).
- Locally—See the instructions below.

### Prerequisites

- ESET PROTECT Server and the ESET PROTECT Web Console are installed (on a Server computer).
- An Agent [certificate](#) is created and prepared on your local drive.
- A [Certification Authority](#) is prepared on your local drive (only needed for unsigned certificates).

## Installation

Follow the steps below to install the ESET Management Agent component locally on macOS:

**i** Ensure to meet all the installation prerequisites listed above.

1. Get the installation file (standalone agent installer *.dmg*) from the [ESET download site](#) or your system administrator.
2. Double-click the *Agent\_macosx\_x86\_64.dmg* file and then double-click the *.pkg* file to start the installation.
3. Proceed with the installation. When asked, type the **Server connection** data:
  - **Server hostname:** hostname or IP address of the ESET PROTECT Server
  - **Server port:** port for Agent—Server communication, default is 2222.
  - **Use Proxy:** click if you want to use HTTP Proxy for Agent—Server connection.

This proxy setting is used only for (replication) between ESET Management Agent and ESET PROTECT Server, not for the caching of updates.

- **Proxy hostname:** hostname or IP address of the HTTP Proxy machine.

- **Proxy port:** default value is 3128.

- **Username, Password:** type the credentials used by your proxy if it uses authentication.

You can change proxy settings later in your [policy](#). [Proxy](#) must be installed before you can configure an Agent—Server connection via Proxy.

4. Select a Peer [certificate](#) and a password for this certificate. Optionally, you can add a [Certification Authority](#).

- The certificate passphrase must not contain the following characters: " \ These characters cause a critical error during Agent initialization.

- The password must contain at least 14 characters in three categories: lowercase letters, uppercase letters, digits or special characters. We recommend using a password with no less than 17 characters.

5. Review the install location and click **Install**. The Agent will be installed on your computer.

6. Enable Full disk access for ESET Management Agent:

Locally:

a)Open **System Preferences > Security & Privacy > Privacy**.

b)Unlock the settings in the lower corner.

c)Click **Full Disk Access**.

d)Click + > **Application > ESET > Open** and add the ESET Management Agent to the application list in the **Full Disk Access** folder.

e)Lock the settings in the lower corner.

Remotely:

a)Download the [.plist](#) configuration file.

b)Generate two UUIDs with a UUID generator of your choice and use a text editor to replace strings with the text. Insert your UUID 1 and UUID 2 in the downloaded configuration profile instead of the `<string>` values under `<key>PayloadUUID</key>`.

c)Deploy the `.plist` configuration profile file [using the MDM server](#). Your computer needs to be enrolled in the MDM server to deploy configuration profiles to computers.

7. The computer with the installed Agent will appear in your ESET PROTECT Web Console, and you can manage it using ESET PROTECT On-Prem.

## Agent installation troubleshooting

Verify that the Agent is running: Click **Go > Utilities** and then double-click **Activity Monitor**. Click the **Energy** tab or the **CPU** tab and locate the process called **ERAAgent**.

The ESET Management Agent log file can be found here:

*/Library/Application Support/com.eset.remoteadministrator.agent/Logs/  
/Users/%user%/Library/Logs/EraAgentInstaller.log*



The communication protocol between Agent and ESET PROTECT Server does not support authentication. Any proxy solution used for forwarding Agent communication to ESET PROTECT Server that requires authentication will not work. If you choose to use a non-default port for the Web Console or Agent, it may require a firewall adjustment. Otherwise, the installation may fail.

## ISO image

An ISO image file is one of the formats you can [download](#) (**All-in-one Installer** category) ESET PROTECT installers in. The ISO image contains the following:

- ESET PROTECT Installer package
- Separate installers for each component

The ISO image is useful when you want to keep all ESET PROTECT installers in one place. It also eliminates the need to download the installers from the ESET website every time you need to run the installation. The ISO image is also useful to have when you want to install ESET PROTECT On-Prem on a virtual machine.

## DNS Service Record

### To set up a DNS Resource Record:

1. On your DNS Server (DNS server on your Domain controller), navigate to **Control Panel > Administrative Tools**.
2. Select the DNS value.
3. In the DNS Manager, select `_tcp` from the tree and create a new **Service location (SRV)** record.
4. Type the service name in the **Service** field according to DNS standard rules, type an underscore (`_`) in front of the service name (use your own service name, for example `_era`).
5. Type the `tcp` protocol in the **Protocol** field in the following format: `_tcp`.
6. Type the port `2222` in the **Port number** field.
7. Type the ESET PROTECT Server fully qualified domain name (FQDN) in the **Host offering this service** field.
8. Click **OK > Done** to save the record. The record will be displayed in the list.

### To verify the DNS record:

1. Log into any computer in your domain and open a command prompt (`cmd.exe`).
2. Type `nslookup` into the command prompt and press **Enter**.

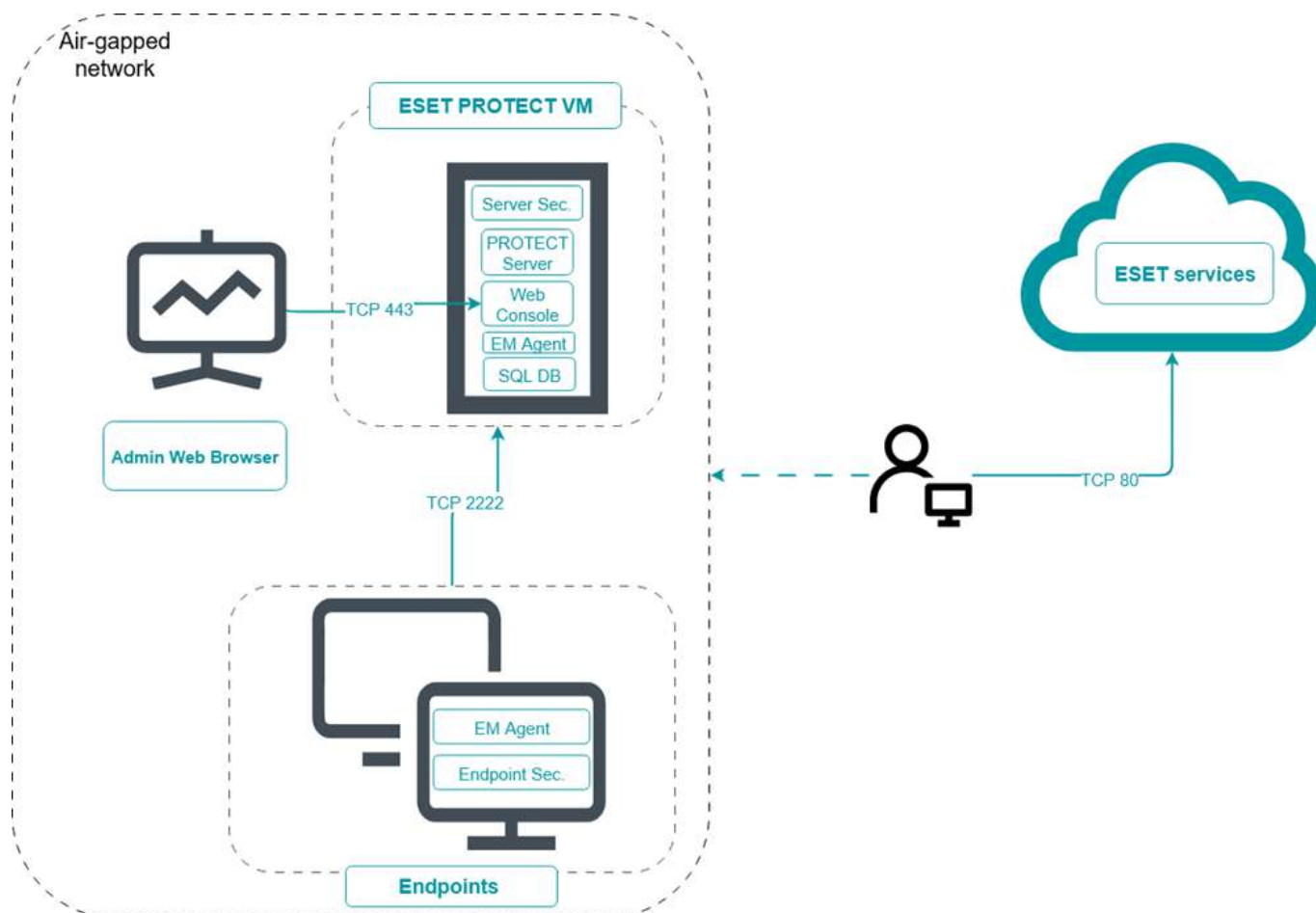
3.Type `set querytype=srv` and press **Enter**.

4.Type `_era._tcp.domain.name` and press **Enter**. The service location is displayed correctly.

**i** Do not forget to change the "Host offering this service:" value to the FQDN of your new server when you install ESET PROTECT Server on a different machine.

## Offline installation scenario for ESET PROTECT On-Prem

To install ESET PROTECT On-Prem and its components in environments without access to the internet, follow the high-level installation instructions (with ESET PROTECT On-Prem installed on Windows).



### A computer with an internet connection

1. Create a shared network folder.
2. Download the following installers to the shared folder:
  - [ESET PROTECT All-in-one installer](#)
  - A [supported JDK package](#) (required for the Web Console).
  - ESET Management Agent installer
  - ESET security application installers (for example, ESET Endpoint Security)

## An offline Windows computer in the same local network

1. Copy the installers from the network shared folder to an offline Windows computer where you want to install ESET PROTECT On-Prem.
2. Install the JDK package.
3. [Install ESET PROTECT On-Prem](#) on Windows using the All-in-one installer. Choose **Activate later** during installation.
4. Activate ESET PROTECT On-Prem with an [offline activation file](#).
5. Deploy ESET Management Agent to computers in your offline environment via [Agent script installer](#). Modify the installation script to use the new link to access the agent installation package from the shared network folder.
6. Deploy ESET security applications to workstations using a [Software Install task](#). Select **<Choose package>** and provide a custom URL for the installation package from the local repository.
7. [Activate managed endpoints with an offline activation file](#).
8. [Disable ESET LiveGrid®](#).



We highly recommend that you [keep the offline ESET infrastructure updated](#) by using a local update repository. Update ESET application modules regularly. If application modules are not updated, the ESET PROTECT Web Console flags computers as **Not updated**. To mute this Web Console warning, click the computer in the list and select **Mute** from the context menu.

For instructions to upgrade ESET PROTECT On-Prem, see [Upgrade ESET PROTECT components in an offline environment](#).

## Upgrade

There are different ways to upgrade your ESET PROTECT Server and other ESET PROTECT components. See also [migration and reinstallation procedures](#).



Ensure you have a [supported operating system](#) before upgrading to ESET PROTECT On-Prem 13.0. We recommend that you [back up the ESET PROTECT database](#) before upgrading. If you have an earlier unsupported database installed (MySQL 5.7 and earlier or Microsoft SQL Server 2014 and earlier), [upgrade your database](#) to a [compatible database version](#) before upgrading the ESET PROTECT Server.


To look up what version of each ESET PROTECT component you are running, verify your ESET PROTECT Server version. Navigate to the [About](#) page in the ESET PROTECT Web Console, and see the [list of all ESET PROTECT component versions](#).

## Upgrade from an earlier ESET PROTECT On-Prem version to version 13.0




You can upgrade to ESET PROTECT On-Prem 13.0 from ESET PROTECT On-Prem 10.1 and later. A direct upgrade from the End of Life versions 8.x–10.0 has not been tested and is not supported.


If you have ERA 5.x/6.x or ESMC 7.x, the direct upgrade to ESET PROTECT On-Prem 13.0 is not supported—Perform a clean installation of ESET PROTECT On-Prem 13.0.

 ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

Select one of the upgrade procedures:

Upgrade procedure	Operating system	Comment
<a href="#">Components Upgrade</a> task in the Web Console	Windows/Linux	
<a href="#">ESET PROTECT On-Prem 13.0 All-in-one installer</a>	Windows	All-in-one installer is the recommended upgrade option if the existing installation was performed via the All-in-one installer (you have default installations of the Microsoft SQL database and Apache Tomcat).  Upgrade Apache Tomcat to fix the <a href="#">failed file import</a> in the ESET PROTECT Web Console.
<a href="#">Manual component-based upgrade</a>	Linux	Linux instructions for advanced users.
<a href="#">Upgrade ESET PROTECT Virtual Appliance</a>	Linux (Virtual Appliance)	


### Server upgrade using the standalone Server installer

 If you copy the database password from the [StartupConfiguration.ini](#) file and the password contains the @ character, delete the escape character \ before it.

## ESET PROTECT Components Upgrade task

### Recommendations before upgrading

We recommend using the [ESET PROTECT Components Upgrade](#) task in the ESET PROTECT Web Console to upgrade your ESET PROTECT infrastructure. Ensure you review the directions in detail before upgrading.

-  If the components upgrade fails on a machine running the ESET PROTECT Server or Web Console, you might not be able to log in to the Web Console remotely. We recommend that you ensure physical access to the server machine before performing this upgrade. If physical access to the machine is not possible, ensure you can access it with administrative privileges using a remote desktop.
- If you have installed ESET PROTECT database with a dedicated database user with Windows authentication, the ESET PROTECT Components Upgrade task cannot upgrade the ESET PROTECT Server in the future.

### [Are you upgrading from an earlier ESET PROTECT Virtual Appliance?](#)

#### [The ESET PROTECT Server is installed on a failover cluster?](#)

If your ESET PROTECT Server is installed on a failover cluster, you must upgrade the ESET PROTECT Server component on each cluster node manually. After upgrading the ESET PROTECT Server, run the [Components Upgrade](#) task to upgrade the rest of your infrastructure (for example, ESET Management Agents on client computers).

You can upgrade to ESET PROTECT On-Prem 13.0 from ESET PROTECT On-Prem 10.1 and later. A direct upgrade from the End of Life versions 8.x–10.0 has not been tested and is not supported. ESET PROTECT On-Prem automatically notifies you when [a new version of the ESET PROTECT Server is available](#).

Back up the following data before the upgrade:

- Your [ESET PROTECT database](#).

If you have an earlier unsupported database installed (MySQL 5.7 and earlier or Microsoft SQL Server 2014 and earlier), [upgrade your database](#) to a [compatible database version](#) before upgrading the ESET PROTECT Server.



To back up your Virtual Appliance, create a snapshot or clone the virtual machine.

- All certificates (Certification Authority, Server Certificate and Agent Certificate):

Export your [Certification Authority Certificates](#) from an old ESET PROTECT Server to a *.der* file and save them to external storage.

Export your [Peer Certificates](#) (for ESET Management Agent, ESET PROTECT Server) and private key *.pfx* file from an old ESET PROTECT Server and save them to external storage.

Ensure you have a [supported operating system](#) before upgrading to ESET PROTECT On-Prem 13.0.

Upgrade ESET security applications by running the [Software Install task](#) using the latest installer package to install the latest version over your existing application.



ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

## Recommended upgrade procedure

1. Upgrade the ESET PROTECT Server—Select only the machine with the ESET PROTECT Server as the target for the **ESET PROTECT Components Upgrade** task.
2. Select some client computers (as a test sample—at least one client from each operating system and bitness) and run the **ESET PROTECT Components Upgrade** task on them.

We recommend that you use [ESET Bridge HTTP Proxy](#) (or any other transparent web proxy with caching enabled) to limit the network load. The test client machines will trigger the download/caching of the installers. When the task runs again, the installers will be distributed to client computers from the cache.

3. After the computers with upgraded ESET Management Agent successfully connect to the ESET PROTECT Server, proceed with upgrading the rest of the clients.



To upgrade ESET Management Agents on all managed computers in the network, select the Static Group **All** as the target for the **ESET PROTECT Components Upgrade** task. The task will skip computers that already run the latest ESET Management Agent.

ESET PROTECT On-Prem supports the [automatic upgrade of ESET Management Agents](#) on managed computers.

### Components upgraded automatically:

- ESET PROTECT Server
- ESET Management Agent
- ESET PROTECT Web Console—Only applies when Apache Tomcat was installed to its default installation folder in both Windows and Linux distributions, including ESET PROTECT Virtual Appliance (for example: */var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*).

## Web Console upgrade limitations

Apache Tomcat is not upgraded during the ESET PROTECT Web Console upgrade via the Components Upgrade task.

- ⚠ ESET PROTECT Web Console upgrade does not work if Apache Tomcat is installed in a custom location. If a custom version of Apache Tomcat is installed (manual installation of the Tomcat service), the future ESET PROTECT Web Console upgrade via the All-in-one installer or Components Upgrade Task is not supported.

Upgrade Apache Tomcat to fix the [failed file import](#) in the ESET PROTECT Web Console.

## Components that require a manual upgrade:

- [ESET Rogue Detection Sensor](#)—Use the [Software Install task](#) for the upgrade. Alternatively, install the latest version over an earlier version (follow the installation instructions for [Windows](#) or [Linux](#)). If you installed RD Sensor with an earlier ESET PROTECT On-Prem version, you do not need to upgrade it, as there are no new RD Sensor releases.

ⓘ ESET Rogue Detection (RD) Sensor will be deprecated (there will be no future updates). Some of its features may not work properly. You can no longer manage RD Sensor configuration via a policy.


In addition to ESET components, ESET PROTECT On-Prem uses third-party components that require a manual upgrade.

- We recommend installing the latest supported version of third-party components. The latest available version may vary based on the operating system running the ESET PROTECT Server.
- ESET PROTECT Virtual Appliance does not report available upgrades for third-party components.

In **Quick Links > Server Components**, the ESET PROTECT Web Console recommends an upgrade for third-party component versions earlier than those listed below:

Third-party component:	Version:	Notes:	Upgrade instructions
Microsoft SQL Server	2022 (build 16.0.4215.2)	Determine your <a href="#">version and edition of SQL Server Database Engine</a> and install the latest <a href="#">cumulative update</a> .	<a href="#">SQL Server upgrade</a>
MySQL	8.0.0.0	Click <b>Help &gt; About</b> in the ESET PROTECT Web Console to see the installed database version.	<a href="#">MySQL Server upgrade</a>
Operating system	Windows Server 2016	ESET PROTECT On-Prem does not report available updates for Linux.	<a href="#">Operating system update</a>
Apache Tomcat	9.0.112	Determine the installed Apache Tomcat version: <ul style="list-style-type: none"><li>• Windows—Navigate to <i>C:\Program Files\Apache Software Foundation\[ Tomcat folder ]</i> and open the <i>RELEASE-NOTES</i> file in a text editor to check the version number.</li><li>• Linux—Run the Terminal command: <code>tomcat version</code></li></ul>	<a href="#">Apache Tomcat upgrade</a>

Third-party component:	Version:	Notes:	Upgrade instructions
Java	17.0	Determine the installed Java version: <ul style="list-style-type: none"> <li>• Windows—Open the Command Prompt and run: <code>java -version</code></li> <li>• Linux—Run the Terminal command: <code>java -version</code></li> </ul>	<a href="#">Java Runtime Environment upgrade</a>
Apache HTTP Proxy	-	<div style="border: 1px solid orange; padding: 5px;"> <p><b>Apache HTTP Proxy users</b></p> <p>ESET distributes ESET Bridge as a Proxy component (replacing the Apache HTTP Proxy). We recommend <a href="#">migrating to ESET Bridge</a> if you use Apache HTTP Proxy.</p> </div>	<a href="#">Migrate to ESET Bridge</a>

 ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

## Troubleshooting

- Verify if you can [access the ESET PROTECT On-Prem repository](#) from an upgraded computer.
- Re-running the ESET PROTECT Components Upgrade task will not work if at least one component is already upgraded to the later version.
- If the ESET PROTECT Web Console does not load or you see an error during the login, see the [Web Console troubleshooting](#).
- If there is no clear reason for the upgrade failure, upgrade components manually. See our instructions for [Windows](#) or [Linux](#).
- For more suggestions to resolve upgrade issues, see [general troubleshooting information](#).

## Use the ESET PROTECT On-Prem 13.0 All-in-one installer to upgrade

Use the ESET PROTECT On-Prem 13.0 All-in-one installer to upgrade an earlier ESET PROTECT On-Prem version to the latest ESET PROTECT On-Prem 13.0.

All-in-one installer is the recommended upgrade option if the existing installation was performed via the All-in-one installer (you have default installations of the Microsoft SQL database and Apache Tomcat).

The ESET PROTECT On-Prem 13.0 [All-in-one installer](#) installs Microsoft SQL Server Express 2022 by default.

oUpgrading checks for previous SQL installations and offers an upgrade to SQL 2022 or 2016 (based on the operating system).

oThe installer generates a random password for database authentication and stores it in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`.

Microsoft SQL Server Express (the free edition) has a 10 GB size limit for each relational database. We recommend using other Microsoft SQL Server editions than Microsoft SQL Server Express:



- In enterprise environments or large networks.
- If you want to use ESET PROTECT On-Prem with [ESET Inspect On-Prem](#).

You can upgrade to ESET PROTECT On-Prem 13.0 from ESET PROTECT On-Prem 10.1 and later. A direct upgrade from the End of Life versions 8.x–10.0 has not been tested and is not supported.

Back up the following data before running the upgrade:



- All certificates (Certificate Authority, Server Certificate and Agent Certificate)
- Export your [Certification Authority Certificates](#) from an old ESET PROTECT Server to a *.der* file and save them to external storage.
- Export your [Peer Certificates](#) (for ESET Management Agent, ESET PROTECT Server) and private key *.pfx* file from an old ESET PROTECT Server and save them to external storage.
- Your [ESET PROTECT database](#). If you have an earlier unsupported database installed (MySQL 5.7 and earlier or Microsoft SQL Server 2014 and earlier), [upgrade your database](#) to a [compatible database version](#) before upgrading the ESET PROTECT Server.

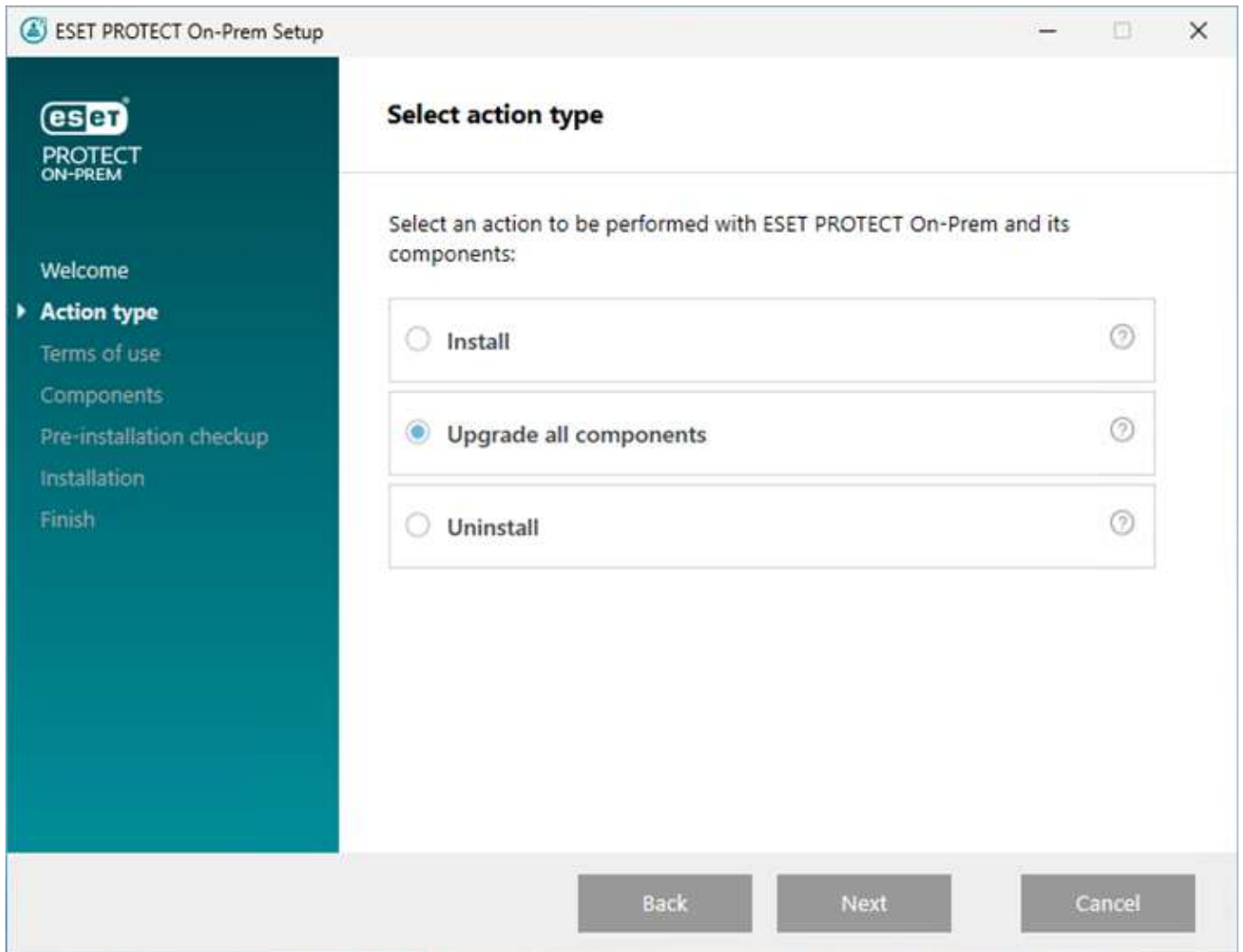
Ensure you have a [supported operating system](#) before upgrading to ESET PROTECT On-Prem 13.0.

ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only)



reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

- 1.Run *Setup.exe*.
- 2.Select the language and click **Next**.
- 3.Select **Upgrade all components** and click **Next**.



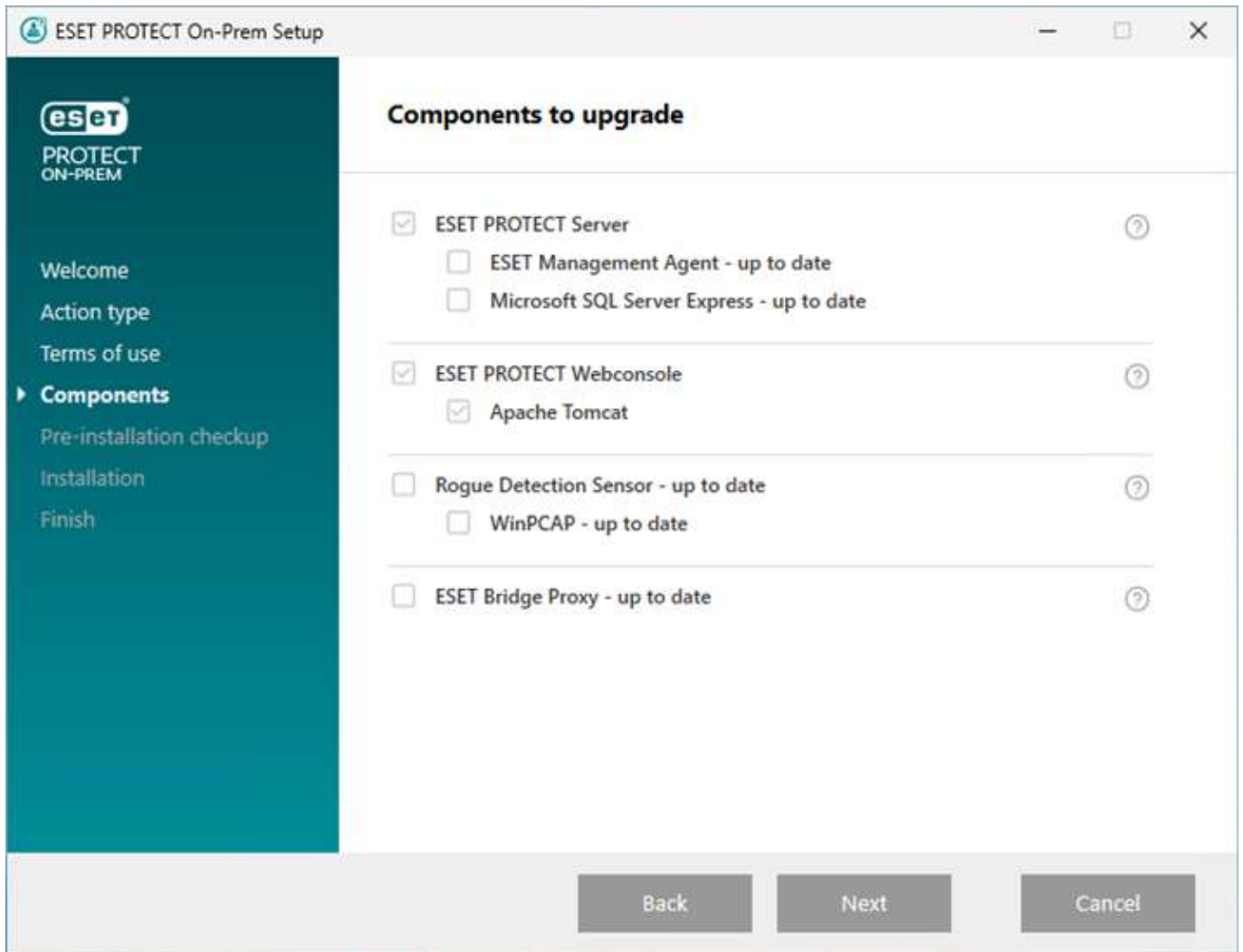
4. Select **I accept the Terms of Use** and click **Next**.

5. In **Components**, review ESET PROTECT components that can be upgraded and click **Next**.

### Apache Tomcat and Web Console upgrade limitations

- If a custom version of Apache Tomcat is installed (manual installation of the Tomcat service), the future ESET PROTECT Web Console upgrade via the All-in-one installer or Components Upgrade Task is not supported.
- Apache Tomcat upgrade will delete the *era* folder located in *C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\*. If you use the *era* folder to store additional data, ensure to back up the data before upgrading.
- If *C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\* contains additional data (other than the *era* and *ROOT* folders), the Apache Tomcat upgrade will not take place and only the Web Console will be upgraded.
- The Web Console and Apache Tomcat upgrade clears the [Offline help](#) files. If you used Offline help with an earlier ESET PROTECT On-Prem version, re-create it for ESET PROTECT On-Prem 13.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT On-Prem version.
- Upgrade Apache Tomcat to fix the [failed file import](#) in the ESET PROTECT Web Console.

⚠ If you run the All-in-one installer on a Windows machine that has Apache HTTP Proxy installed, the installer will automatically uninstall Apache HTTP Proxy and install [ESET Bridge](#) instead.



6. Follow the **Pre-installation checkup** to ensure your system meets all prerequisites.

7. Click **Upgrade** to start the ESET PROTECT On-Prem upgrade. The upgrade may take some time, depending on your system and network configuration.

8. When the upgrade completes, click **Finish**.

If the ESET PROTECT Web Console does not load or you see an error during the login, see the [Web Console troubleshooting](#).

After upgrading ESET PROTECT On-Prem, upgrade ESET Management Agent on managed computers using the Components Upgrade task. ESET PROTECT On-Prem supports the [automatic upgrade of ESET Management Agents](#) on managed computers.

## Database Server Backup/Upgrade

ESET PROTECT On-Prem uses a database to store client data. The following sections detail the [backup](#) and [upgrade](#) of the ESET PROTECT Server database:

- If you do not have a database configured for use with ESET PROTECT Server, **Microsoft SQL Server Express** is included with the installer. The ESET PROTECT On-Prem 13.0 [All-in-one installer](#) installs Microsoft SQL Server Express 2022 by default.

Upgrading checks for previous SQL installations and offers an upgrade to SQL 2022 or 2016 (based on the operating system).

The installer generates a random password for database authentication and stores it in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`.

Microsoft SQL Server Express (the free edition) has a 10 GB size limit for each relational database. We recommend using other Microsoft SQL Server editions than Microsoft SQL Server Express:

- In enterprise environments or large networks.
- If you want to use ESET PROTECT On-Prem with [ESET Inspect On-Prem](#).

- If you have an earlier unsupported database installed (MySQL 5.7 and earlier or Microsoft SQL Server 2014 and earlier), [upgrade your database](#) to a [compatible database version](#) before upgrading the ESET PROTECT Server.

See also [ESET PROTECT database migration](#).

The following requirements for Microsoft SQL Server must be met:

- Install a [supported version of Microsoft SQL Server](#). Choose **Mixed mode** authentication during installation.
- If you have Microsoft SQL Server already installed, set authentication to **Mixed mode (SQL Server authentication and Windows authentication)**. To do so, follow the instructions in this [Knowledgebase article](#). If you want to use **Windows Authentication** to log in to Microsoft SQL Server, follow the steps in this [Knowledgebase article](#).
- Allow TCP/IP connections to the SQL Server. To do so, follow the steps in this [Knowledgebase article](#) from part II. **Allow TCP/IP connections to the SQL database**.

- To configure, manage and administer Microsoft SQL Server (databases and users), [download SQL Server Management Studio \(SSMS\)](#).

- [Do not install SQL Server on a Domain Controller](#). Install ESET PROTECT On-Prem on a different server or deselect the SQL Server Express component during installation. Use your existing SQL or MySQL Server to run the ESET PROTECT database.

## Database Server Backup and Restore

All ESET PROTECT On-Prem information and settings are stored in the database. We recommend that you back up your database regularly to prevent loss of data. You can use the backup later when migrating ESET PROTECT On-Prem to a new server. Refer to the appropriate section below for your database:

- The names of databases and log files are staying same even after the change of the application name from ESET Security Management Center to ESET PROTECT On-Prem.
- If you use ESET PROTECT Virtual Appliance, follow [the VA database backup instructions](#).

## Microsoft SQL Backup examples

To backup a Microsoft SQL database to a file, follow the examples shown below:

These examples are intended for use with default settings (for example, default database name and database connection settings). Your backup script will need to be customized to accommodate any changes you have made to default settings.



You need to have sufficient rights to run the commands below. If you do not use a local administrator user account, you need to change the backup path, for example to 'C:\USERS\PUBLIC\BACKUPFILE'.

## One time database backup

Execute this command in a Windows command prompt to create a backup into file named **BACKUPFILE**:

```
SQLCMD -S HOST\ERASQL -  
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE' "
```



In this example, **HOST** stands for the IP address or hostname and **ERASQL** for the name of the Microsoft SQL server instance. You can install ESET PROTECT Server on a custom named SQL instance (when using Microsoft SQL database). Modify backup scripts accordingly in this scenario.

## Regular database backup with SQL script

Choose one of the following SQL scripts:

a) Create regular backups and store them based on date of creation:

```
@ECHO OFF
```

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -  
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'  
  WITH NOFORMAT, INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHE  
CKSUM, STATS=10"
```

```
REN BACKUPFILE BACKUPFILE-  
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b) Append your backup to one file:

```
@ECHO OFF
```

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -  
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'  
  WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR,  
  CHECKSUM, STATS=10"
```

## Microsoft SQL restore

To restore a Microsoft SQL database from a file, follow the example shown below based your environment:

- With an existing ERA\_DB database:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -  
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE' "
```

- Without an existing ERA\_DB database:

```
SQLCMD.EXE -S HOST\ERASQL -E -  
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE' "
```

## MySQL backup

To backup a MySQL database to a file, follow the example shown below:

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -  
p DBNAME -r BACKUPFILE
```

**i** In this example, **HOST** stands for the IP address or hostname of the MySQL server, **ROOTLOGIN** for the root account of the MySQL Server, and **DBNAME** stands for ESET PROTECT database name.

## MySQL restore

To restore a MySQL database from a file, follow the example shown below:

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

**i** For more information on Microsoft SQL Server backup, please visit [Microsoft technet website](#). For more information on MySQL Server backup, please visit [MySQL documentation website](#).

## Database Server Upgrade

Follow the instructions below to upgrade an existing database server to a later version for use with ESET PROTECT Server database:

1. [Stop](#) all running ESET PROTECT Server services connecting to the database server that you will be upgrading. Additionally, stop any other applications that might be connecting to your database server instance.
2. [Back up](#) all relevant databases safely before proceeding.
3. Perform the database server upgrade:

 [SQL Server \(Windows\)](#):

- Follow the [Knowledgebase article for upgrading Microsoft SQL Express database to the latest version](#).
- Alternatively, follow the database vendor's instructions: <https://msdn.microsoft.com/en-us/library/bb677622.aspx>.
- [Microsoft SQL Server on Linux](#) is not supported. However, you can [connect](#) the ESET PROTECT Server on Linux to Microsoft SQL Server on Windows.

### [MySQL Server \(Windows and Linux\):](#)

- [Upgrade from MySQL 5.7 to version 8.0](#)
- [Upgrade from MySQL 8.x to version 8.4](#)
- [Upgrade from MySQL 8.4 to version 9.x](#)

4. Start ESET PROTECT Server service and check [trace logs](#) to verify the database connection is working correctly.

## Upgrade ESET PROTECT On-Prem installed in Failover Cluster on Windows

If you have ESET PROTECT Server [installed in a Failover Cluster](#) environment on Windows, follow the steps below to upgrade to the latest ESET PROTECT On-Prem:

 Ensure you have a [supported operating system](#).

1. Stop the ESET PROTECT Server cluster Role in the Cluster Manager. Ensure the service (**ESET PROTECT Server**) is stopped on all cluster nodes.
2. Get the cluster shared disk online on node1 and upgrade the Server component manually by executing the latest `.msi` installer as in case of a [component installation](#).
3. After the installation (upgrade) is finished, ensure the **ESET PROTECT Server** service is stopped.
4. Get the cluster shared disk online on node2 and upgrade the Server component the same way as in step 2.
5. When ESET PROTECT Server is updated on all cluster nodes, start the **ESET PROTECT Server Role** in the Cluster Manager.
6. Upgrade ESET Management Agent manually by executing the latest `.msi` installer on all cluster nodes.
7. In ESET PROTECT Web Console check if Agent and Server versions for all nodes report the latest version to which you upgraded to.

## Upgrade Apache Tomcat

Apache Tomcat is a mandatory component required to run the ESET PROTECT Web Console.

If you are upgrading to a most recent version of ESET PROTECT On-Prem, or if you have not upgraded Apache Tomcat for a prolonged period of time, you should consider upgrading Apache Tomcat to the latest version. Keeping public-facing services including Apache Tomcat and its dependencies up-to-date will decrease security risks to your environment.

## File import fails in the Web Console on All-in-one installations with Apache Tomcat 9.0.105 and earlier



File import fails in the Web Console on All-in-one installations with Apache Tomcat 9.0.105 and earlier. The issue affects the import of computers, notifications, policies, certificates, etc.

The issue is due to code changes in the latest ESET PROTECT On-Prem [hotfix](#), which was released for compatibility with Apache Tomcat 9.0.106, which fixed a critical vulnerability in the Apache Tomcat. To resolve the issue, upgrade Apache Tomcat to version 9.0.106 and later.

To upgrade Apache Tomcat, follow the instructions:

- [Windows instructions \(the latest ESET PROTECT All-in-one installer\)](#)—This is the recommended upgrade option if the existing Apache Tomcat installation was performed via the All-in-one installer.
- [Windows instructions \(manual installation\)](#)—Upgrade Apache Tomcat manually if you performed the existing Apache Tomcat installation manually or you do not have the latest ESET PROTECT All-in-one installer.
- [Linux instructions](#)

## Upgrade Apache Tomcat using the All-in-one installer (Windows)

Apache Tomcat is a mandatory component required to run the ESET PROTECT Web Console. Use this method to upgrade Apache Tomcat using the latest [ESET PROTECT On-Prem 13.0 All-in-one installer](#). This is the recommended upgrade option if the existing Apache Tomcat installation was performed via the All-in-one installer. Alternatively, you can [upgrade Apache Tomcat manually](#).



Upgrade Apache Tomcat to fix the [failed file import](#) in the ESET PROTECT Web Console.

### Before upgrading

Back up the following files:

```
C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\.keystore  
C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\conf\server.xml  
C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties
```

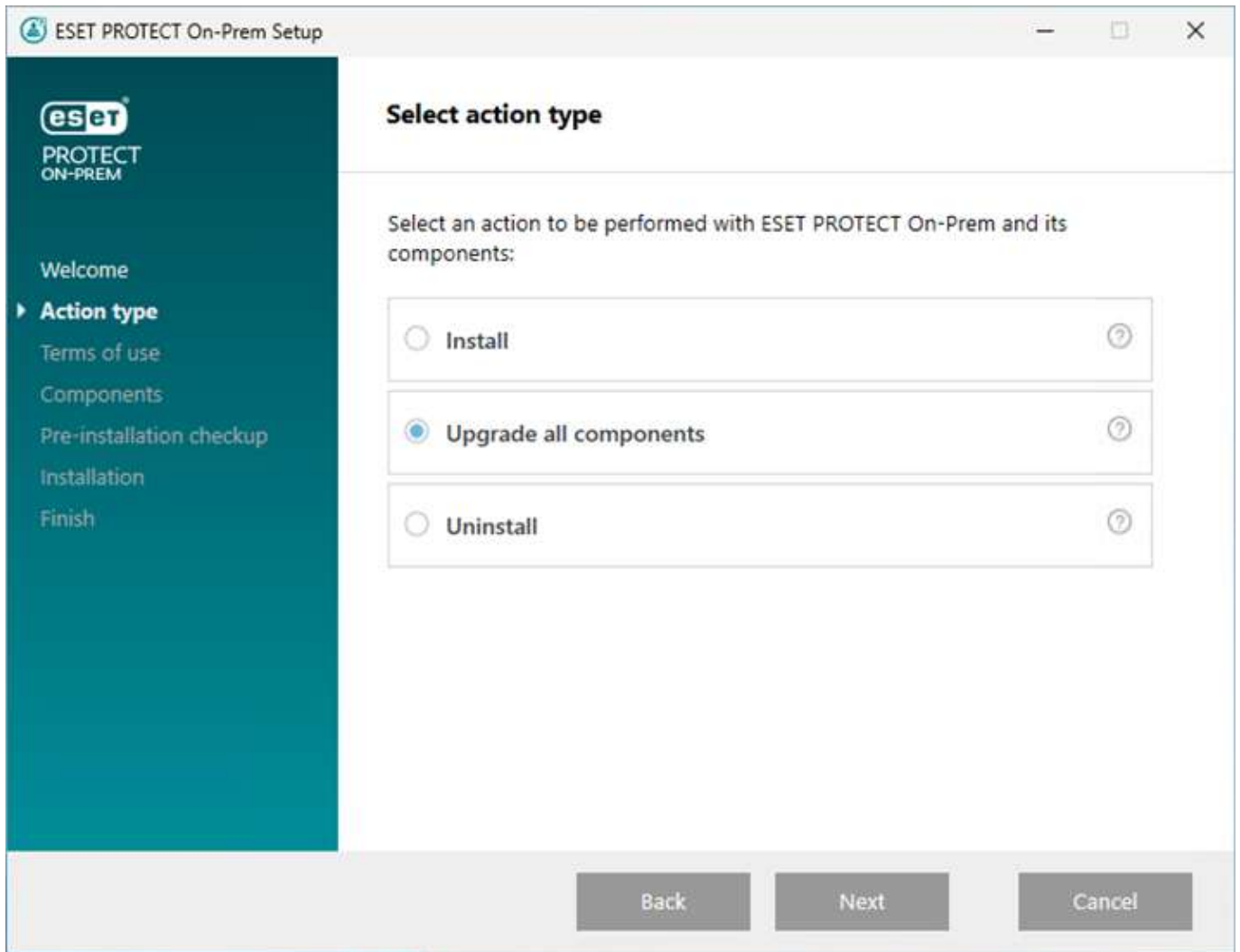
If you are using a custom SSL certificate store in the *Tomcat* folder, also back up that certificate.

### Apache Tomcat and Web Console upgrade limitations

- If a custom version of Apache Tomcat is installed (manual installation of the Tomcat service), the future ESET PROTECT Web Console upgrade via the All-in-one installer or Components Upgrade Task is not supported.
- Apache Tomcat upgrade will delete the *era* folder located in *C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\*. If you use the *era* folder to store additional data, ensure to back up the data before upgrading.
- If *C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\* contains additional data (other than the *era* and *ROOT* folders), the Apache Tomcat upgrade will not take place and only the Web Console will be upgraded.
- The Web Console and Apache Tomcat upgrade clears the [Offline help](#) files. If you used Offline help with an earlier ESET PROTECT On-Prem version, re-create it for ESET PROTECT On-Prem 13.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT On-Prem version.
- Upgrade Apache Tomcat to fix the [failed file import](#) in the ESET PROTECT Web Console.

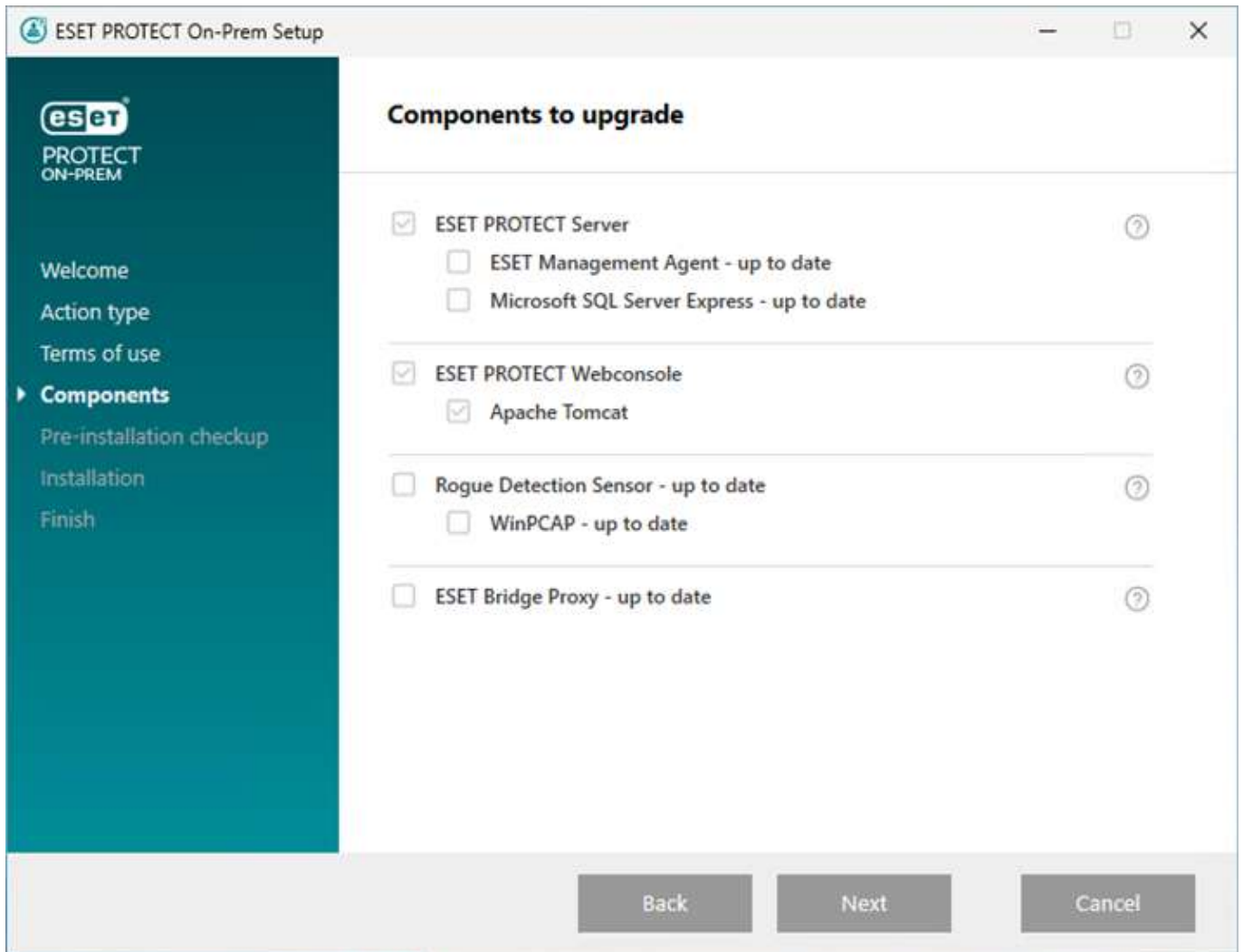
## Upgrade procedure

1. Download the [ESET PROTECT All-in-one installer](#) from the ESET website and unzip the downloaded file.
2. If you want to install the latest version of Apache Tomcat and the All-in-one installer contains an earlier version of Apache Tomcat (this step is optional—skip to step 4 if you do not need the latest version of Apache Tomcat):
  - a. Open the *x64* folder and navigate to the *installers* folder.
  - b. Remove the *apache-tomcat-9.0.x-windows-x64.zip* file located in the *installers* folder.
  - c. Download the Apache Tomcat 9 [64-bit Windows zip](#) package.
  - d. Move the downloaded zip package to the *installers* folder.
3. To launch the All-in-one installer, double-click the *Setup.exe* file and click **Next** on the **Welcome** screen.
4. Select **Upgrade all components** and click **Next**.



5. After accepting the Terms of Use, click **Next**.

6. The All-in-one installer automatically detects if the upgrade is available: there are check boxes next to the upgradable ESET PROTECT components. Click **Next**.



7. Select a Java installation on the computer. Apache Tomcat requires 64-bit Java/OpenJDK. If your system has multiple Java versions installed, uninstall earlier Java versions and keep only the latest [supported Java](#) version.

**!** Starting January 2019, Oracle JAVA SE 8 public updates for business, commercial or production use require a commercial license. If you do not purchase a JAVA SE subscription, you can transition to a no-cost alternative. See the [supported versions of JDK](#).

8. Click **Upgrade** to complete the upgrade and then click **Finish**.

9. If you installed the Web Console on a different computer than the ESET PROTECT Server:

a. Stop the Apache Tomcat service: Navigate to **Start > Services** > right-click the Apache Tomcat service and select **Stop**.

b. Restore the *EraWebServerConfig.properties* file from step 1 to its original location.

c. Start the Apache Tomcat service: Navigate to **Start > Services** > right-click the Apache Tomcat service and select **Start**.

10. [Connect to the ESET PROTECT Web Console](#) and verify that the Web console loads correctly.

**i** See the additional [Web Console configuration for enterprise solutions or low-performance systems](#).

## Troubleshooting

If the Apache Tomcat upgrade fails, uninstall Apache Tomcat and then install it again and apply the configuration from step 1.

## Upgrade Apache Tomcat manually (Windows)

Apache Tomcat is a mandatory component required to run the ESET PROTECT Web Console. Upgrade Apache Tomcat manually if you performed the existing Apache Tomcat installation manually or you do not have the latest ESET PROTECT All-in-one installer.



If a custom version of Apache Tomcat is installed (manual installation of the Tomcat service), the future ESET PROTECT Web Console upgrade via the All-in-one installer or Components Upgrade Task is not supported.



Upgrade Apache Tomcat to fix the [failed file import](#) in the ESET PROTECT Web Console.

### Before upgrading

- Apache Tomcat requires 64-bit Java/OpenJDK. If your system has multiple Java versions installed, uninstall earlier Java versions and keep only the latest [supported Java](#) version.



Starting January 2019, Oracle JAVA SE 8 public updates for business, commercial or production use require a commercial license. If you do not purchase a JAVA SE subscription, you can transition to a no-cost alternative. See the [supported versions of JDK](#).

- Check to see which version of Apache Tomcat is currently available.
  - a. Navigate to the Apache Tomcat installation folder:  
`C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\`
  - b. Open the RELEASE-NOTES file in a text editor and check the version number (for example, 9.0.34).
  - c. If a more recent [supported version](#) is available, perform an upgrade.

### Upgrade procedure

1. Stop the Apache Tomcat service: Navigate to **Start > Services >** right-click the Apache Tomcat service and select **Stop**.

Close *Tomcat7w.exe* if it is running in your Windows notification area.

2. Back up the following files:

```
C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\.keystore  
C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\conf\server.xml  
C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties
```

If you are using a custom SSL certificate store in the *Tomcat* folder, also back up that certificate.

3. Uninstall the current version of Apache Tomcat.
4. Delete the following folder if it is still present on your system:

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

5. Download the latest supported version of the Apache Tomcat installer file (32-bit/64-bit Windows Service Installer) `apache-tomcat-[version].exe` from <https://tomcat.apache.org>.
6. Install the later version of Apache Tomcat that you downloaded:
  - If you have more Java versions installed, select the path to the latest Java during the installation.
  - When the installation completes, deselect the check box next to **Run Apache Tomcat**.
7. Restore `.keystore`, `server.xml`, and custom certificates to their original location.
8. Open the `server.xml` file and ensure the `keystoreFile` path is correct (update the path if you upgraded to a later major version of Apache Tomcat):

`keystoreFile="C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\.keystore"`

9. Ensure that the [HTTPS connection for Apache Tomcat](#) for ESET PROTECT Web Console is configured correctly.
10. Deploy the ESET PROTECT Web Console ([Web Console installation—Windows](#)).
11. Restore `EraWebServerConfig.properties` to its original location.
12. Run Apache Tomcat and set a correct Java VM:
  - a. Navigate to the folder `C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\bin` and run `Tomcat9w.exe`.
  - b. In the **General** tab, set **Startup Type** to **Automatic** and press **Start**.
  - c. Click the **Java** tab, deselect **Use default**, and ensure **Java Virtual Machine** includes the path to `jvm.dll` file ([see illustrated Knowledgebase instructions](#)), and then click **OK**.
13. [Connect to the ESET PROTECT Web Console](#) and verify that the Web Console loads correctly.

**i** See the additional [Web Console configuration for enterprise solutions or low-performance systems](#).

## Troubleshooting

- If you are unsuccessful in setting up an HTTPS connection for Apache Tomcat, you can skip this step and use an HTTP connection temporarily.
- If the upgrade of Apache Tomcat fails, install your original version and apply the configuration from step 2.
- The Web Console and Apache Tomcat upgrade clears the [Offline help](#) files. If you used Offline help with an

earlier ESET PROTECT On-Prem version, re-create it for ESET PROTECT On-Prem 13.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT On-Prem version.

## Upgrade Apache Tomcat and Java (Linux)

Apache Tomcat is a mandatory component required to run the ESET PROTECT Web Console.

### Before upgrading

1. Execute the following command to see the installed version of Apache Tomcat (in some cases, the folder name is `tomcat7` or `tomcat8`):

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. If a later version is available:
  - a. Ensure that the later version is [supported](#).
  - b. Back up the `server.xml` Tomcat configuration file. (File location may vary based on the Linux distribution, for example `/etc/tomcat9/server.xml`).

### Upgrade procedure

1. Run the following command to stop the Apache Tomcat service (in some cases, the service name is `tomcat9`):

```
sudo systemctl stop tomcat
```

2. Upgrade Apache Tomcat and Java.

#### Packages may have different names and may not be available in the default repository

- Example package names below may differ from your Linux distribution repository packages.
- Your Linux distribution's default repository may not contain the latest [supported version of Apache Tomcat and Java](#). For example, you must manually install Tomcat 9 on Ubuntu 24.04 and Debian 12 because their default repositories contain the unsupported Tomcat 10.
- For installation and configuration of Apache Tomcat, see the [Apache Tomcat documentation](#).

Linux distribution	Terminal commands
Debian and Ubuntu distributions	<pre>sudo apt update sudo apt install openjdk-17-jdk tomcat9</pre>
Red Hat distributions and Rocky Linux	<pre>dnf update dnf install java-17-openjdk tomcat</pre>
SUSE Linux Enterprise Server	<pre>zypper refresh sudo zypper install java-17-openjdk tomcat9</pre>

3. Replace the `server.xml` file with the `server.xml` file from your backup.
4. Ensure the [HTTPS connection for Apache Tomcat](#) is configured correctly.

See the additional [Web Console configuration for enterprise solutions or low-performance systems](#).

**i** If you have upgraded Java, ensure to configure Apache Tomcat to use the latest Java package installed on your system.

After upgrading Apache Tomcat to a later major version (for example, 8.x to 9.x):

1. Deploy ESET PROTECT Web Console again (see [ESET PROTECT Web Console installation—Linux](#))

2. Reuse `%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties` to preserve any custom settings in ESET PROTECT Web Console.

**!** The Web Console and Apache Tomcat upgrade clears the [Offline help](#) files. If you used Offline help with an earlier ESET PROTECT On-Prem version, re-create it for ESET PROTECT On-Prem 13.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT On-Prem version.

## Migrate and reinstall

There are different ways to migrate and reinstall your ESET PROTECT Server and other ESET PROTECT components:

- [Migrate](#) or reinstall ESET PROTECT On-Prem 13.0 from one server to another.

**!** To migrate from one ESET PROTECT Server to a new server machine, export/back up all Certificate Authorities and the ESET PROTECT Server Certificate. Otherwise, none of the ESET PROTECT components will be able to communicate with your new ESET PROTECT Server.

- [ESET PROTECT database migration](#)
- [Change an IP address or hostname](#) on an ESET PROTECT Server
- [Migrate to the cloud ESET PROTECT](#)

See also [upgrade procedures](#).

## Migration from one server to another

There are several ways to migrate ESET PROTECT On-Prem from one server to another (these scenarios can be used when reinstalling your ESET PROTECT Server):

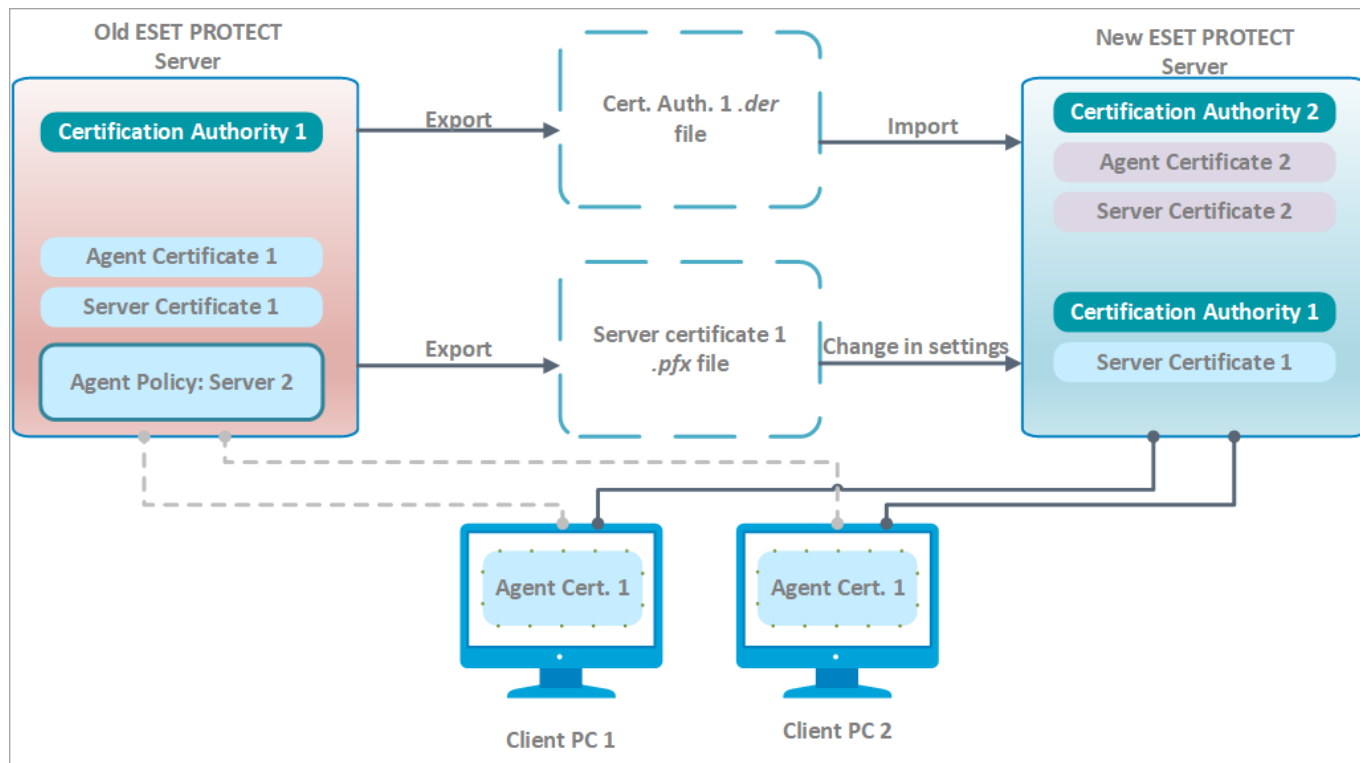
- [Clean Installation—same IP address](#)—The new installation does not use the previous database from the old ESET PROTECT Server and keeps the original IP address.
- [Clean Installation—different IP addresses](#) (Knowledgebase article)—The new installation does not use the previous database from the old ESET PROTECT Server and has a different IP address.
- [Migrated Database—same/different IP address](#)—[ESET PROTECT database migration](#) is only supported between identical database types (from MySQL to MySQL or from Microsoft SQL to Microsoft SQL) and identical ESET PROTECT On-Prem version.

## Clean Installation—same IP address

The objective of this procedure is to install an entirely new ESET PROTECT Server that does not use the previous database. This new ESET PROTECT Server will have the **the same IP address** as your previous server, but will not use the database from the old ESET PROTECT Server.

The instructions below require that your old ESET PROTECT Server is running with an accessible Web Console. If your old ESET PROTECT Server is inaccessible:

1. Install ESET PROTECT Server using the [All-in-one package installer](#) (Windows) or choose [another installation method](#) (Windows manual installation, Linux or Virtual Appliance).
2. [Connect](#) to ESET PROTECT Web Console.
3. [Add client computers](#) to ESET PROTECT infrastructure and [deploy the ESET Management Agent locally or remotely](#).



## I. On your current (old) ESET PROTECT Server:


If you manage devices encrypted with [ESET Full Disk Encryption](#), follow these steps to avoid the loss of [recovery data](#).

1. Before the migration—Navigate to **Status Overview > Encryption**. Here you can **Export** your current **ESET Full Disk Encryption Recovery Data**.


2. After the migration—**Import** the **ESET Full Disk Encryption Recovery Data** on your new management console.


If you are unable to perform these steps, you need to [decrypt the managed devices](#) before the migration. After the migration, you can [encrypt the managed devices](#) from the ESET PROTECT Web Console.

1. Export a server certificate from your current ESET PROTECT Server and save it to external storage.
  - Export all [Certification Authority Certificates](#) from your ESET PROTECT Server and save each CA certificate as a *.der* file.
  - Export [Server Certificate](#) from your ESET PROTECT Server to a *.pfx* file. The exported *.pfx* will include a private key as well.
2. Stop the ESET PROTECT Server service.
3. Turn off your ESET PROTECT Server machine.

 Do not uninstall/decommission your old ESET PROTECT Server yet.


## II. On your new ESET PROTECT Server:

 To use a new ESET PROTECT Server with the same IP address, ensure the network configuration on your new ESET PROTECT Server (**IP address, FQDN, Computer name, DNS SRV record**) matches that of your old ESET PROTECT Server.

 ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

1. Install ESET PROTECT Server using the [All-in-one package installer](#) (Windows) or choose [another installation method](#) (Windows manual installation, Linux or Virtual Appliance).
2. [Connect](#) to ESET PROTECT Web Console.
3. Import all CAs that you have exported from your old ESET PROTECT Server. To do so, follow the instructions for [importing a public key](#).
4. Change the ESET PROTECT Server certificate in **More** > [Settings](#) to use the Server certificate from your old ESET PROTECT Server.
5. [Import all required ESET subscriptions](#) to ESET PROTECT On-Prem.
6. Restart the ESET PROTECT Server service, see our [Knowledgebase article](#) for details.

After one or two [Agent connection intervals](#), client computers should connect to your new ESET PROTECT Server using their original ESET Management Agent certificate, which is being authenticated by the imported CA from the old ESET PROTECT Server. If clients are not connecting, see [Problems after upgrade/migration of ESET PROTECT Server](#).

 When adding new client computers, use a new Certification Authority to sign the Agent certificates. This is done because an imported CA cannot be used to sign new peer certificates, it can only authenticate ESET Management Agents of client computers that were migrated.

## III. Old ESET PROTECT Server uninstallation:

When you have everything running correctly on your new ESET PROTECT Server, carefully decommission your old ESET PROTECT Server using our [step-by-step instructions](#).

## Migrated Database—same/different IP address

The objective of this procedure is to install an entirely new ESET PROTECT Server and **keep your existing ESET PROTECT database**, including existing client computers. The new ESET PROTECT Server will have **the same or different IP address**, and the database of the old ESET PROTECT Server will be imported to the new server machine before installation.

- [ESET PROTECT database migration](#) is only supported between identical database types (from MySQL to MySQL or from Microsoft SQL to Microsoft SQL) and identical ESET PROTECT On-Prem version.
- When migrating a database, we recommend migrating between instances of the same ESET PROTECT On-Prem version. See our [Knowledgebase article](#) for instructions to determine the versions of your ESET PROTECT components. After completing database migration, you can perform an upgrade, if necessary, to get the latest version of ESET PROTECT On-Prem.

## I. On your current (old) ESET PROTECT Server:

We recommend the migration to a different IP address for advanced users only. If your new ESET PROTECT Server has a **different IP address**, perform these additional steps on your current (old) ESET PROTECT Server:

- a) Generate a [new ESET PROTECT Server certificate](#) with connection information for the new ESET PROTECT Server. Leave the default value (an asterisk) in the **Host** field to allow for distribution of this certificate with no association to a specific DNS name or IP address.
- b) Create a policy to define a [new ESET PROTECT Server IP address](#) and assign it to all computers. Wait for the policy to be distributed to all client computers (computers will stop reporting in as they receive the new server information).

1. Stop the ESET PROTECT Server service.
2. [Export/Back up the ESET PROTECT database](#).
3. Turn off the current ESET PROTECT Server machine (optional if the new server has a different IP address).

! Do not uninstall/decommission your old ESET PROTECT Server yet.

## II. On your new ESET PROTECT Server:

! To use a new ESET PROTECT Server with the same IP address, ensure the network configuration on your new ESET PROTECT Server (**IP address, FQDN, Computer name, DNS SRV record**) matches that of your old ESET PROTECT Server.

! ESET PROTECT Mobile Device Management/Connector (MDM/MDC) component (on-premises only) reached End of Life in January 2024. ESET PROTECT On-Prem versions 11.1 and later do not support [mobile device management](#).

1. Install/Launch a [supported](#) ESET PROTECT database.
2. Import/Restore the [ESET PROTECT database](#) from your old ESET PROTECT Server.
3. Install ESET PROTECT Server using the [All-in-one package installer](#) (Windows) or choose [another installation method](#) (Windows manual installation, Linux or Virtual Appliance). Specify your database connection settings during installation of ESET PROTECT Server.
4. [Connect](#) to ESET PROTECT Web Console.
5. Navigate to **More > Settings > Connection**. Click **Change certificate > Open certificate list** and select the **Server certificate** of the old ESET PROTECT Server and click **OK** twice.
6. [Restart the ESET PROTECT Server service](#).

7. [Log in](#) to ESET PROTECT Web Console and click **Computers**.

After one or two [Agent connection intervals](#), client computers should connect to your new ESET PROTECT Server using their original ESET Management Agent certificate. If clients are not connecting, see [Problems after upgrade/migration of ESET PROTECT Server](#).

### III. Old ESET PROTECT Server uninstallation:

When you have everything running correctly on your new ESET PROTECT Server, carefully decommission your old ESET PROTECT Server using our [step-by-step instructions](#).

## ESET PROTECT database migration

These instructions apply to ESET PROTECT database migration between different SQL Server instances (this also applies when migrating to a different SQL Server version or when migrating to a SQL Server hosted on a different machine):

- [Migration process for Microsoft SQL Server](#)
- [Migration process for MySQL Server](#)

## Migration process for Microsoft SQL Server

This migration process is the same for Microsoft SQL Server and Microsoft SQL Server Express.

For additional information, see the following Microsoft Knowledge Base article:


<https://msdn.microsoft.com/en-us/library/ms189624.aspx>.

### Prerequisites

- Source and target SQL Server instances must be installed. They may be hosted on different machines.
- The target SQL Server instance must have at least the same version as the source instance. Downgrade is not supported!
- SQL Server Management Studio must be installed. If the SQL Server instances are on different machines, it must be present on both.

### Migration using SQL Server Management Studio

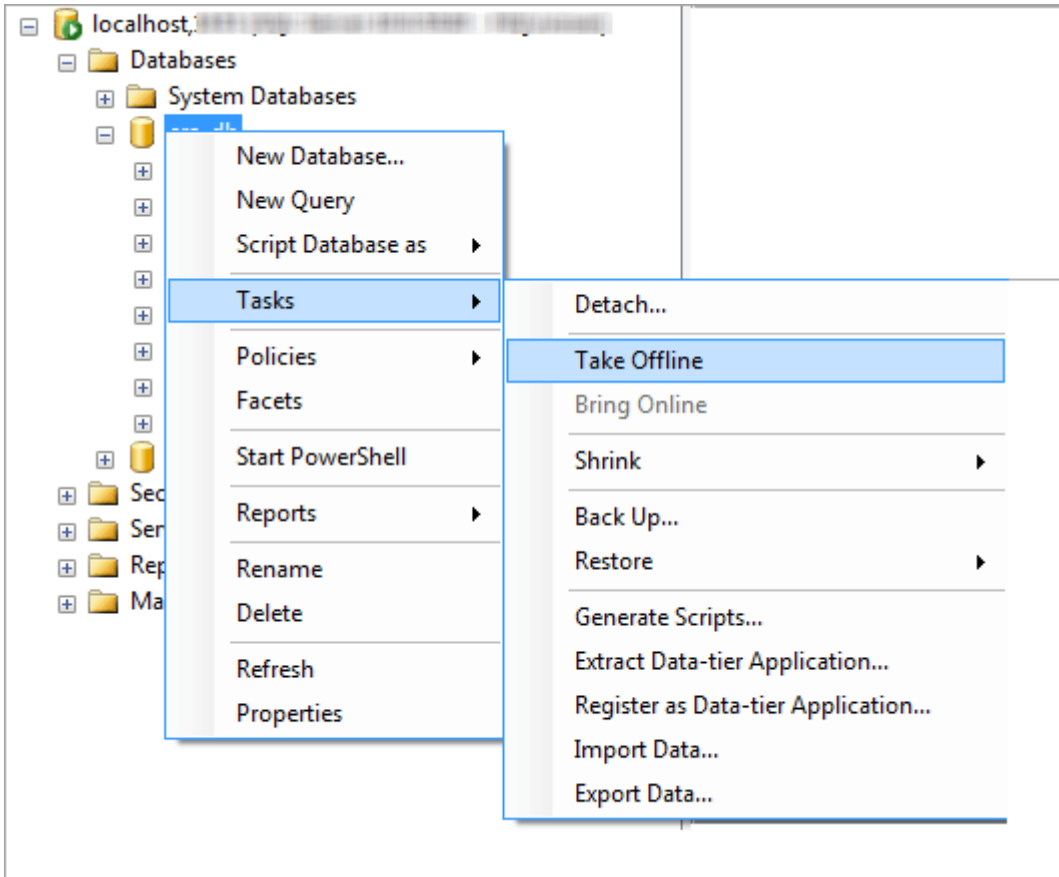
1. Stop the ESET PROTECT Server Service.

 Do not start ESET PROTECT Server before you complete all the steps below.

2. Log into the source SQL Server instance via SQL Server Management Studio.

3. Create a [full database backup](#) of the database to be migrated. We recommend that you specify a new backup set name. Otherwise if the backup set has already been used, the new backup will be appended to it, which will result in an unnecessarily large backup file.

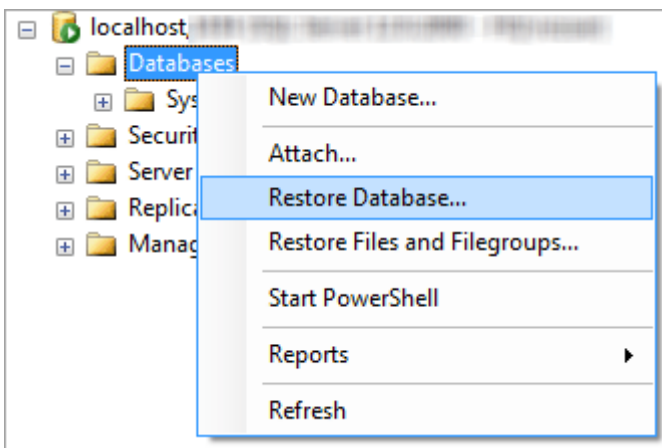
4. Take the source database offline, select **Tasks > Take Offline**.



5. Copy the backup (.bak) file that you created in step 3 to a location that is accessible from the target SQL Server instance. You may need to edit access rights for the database backup file.

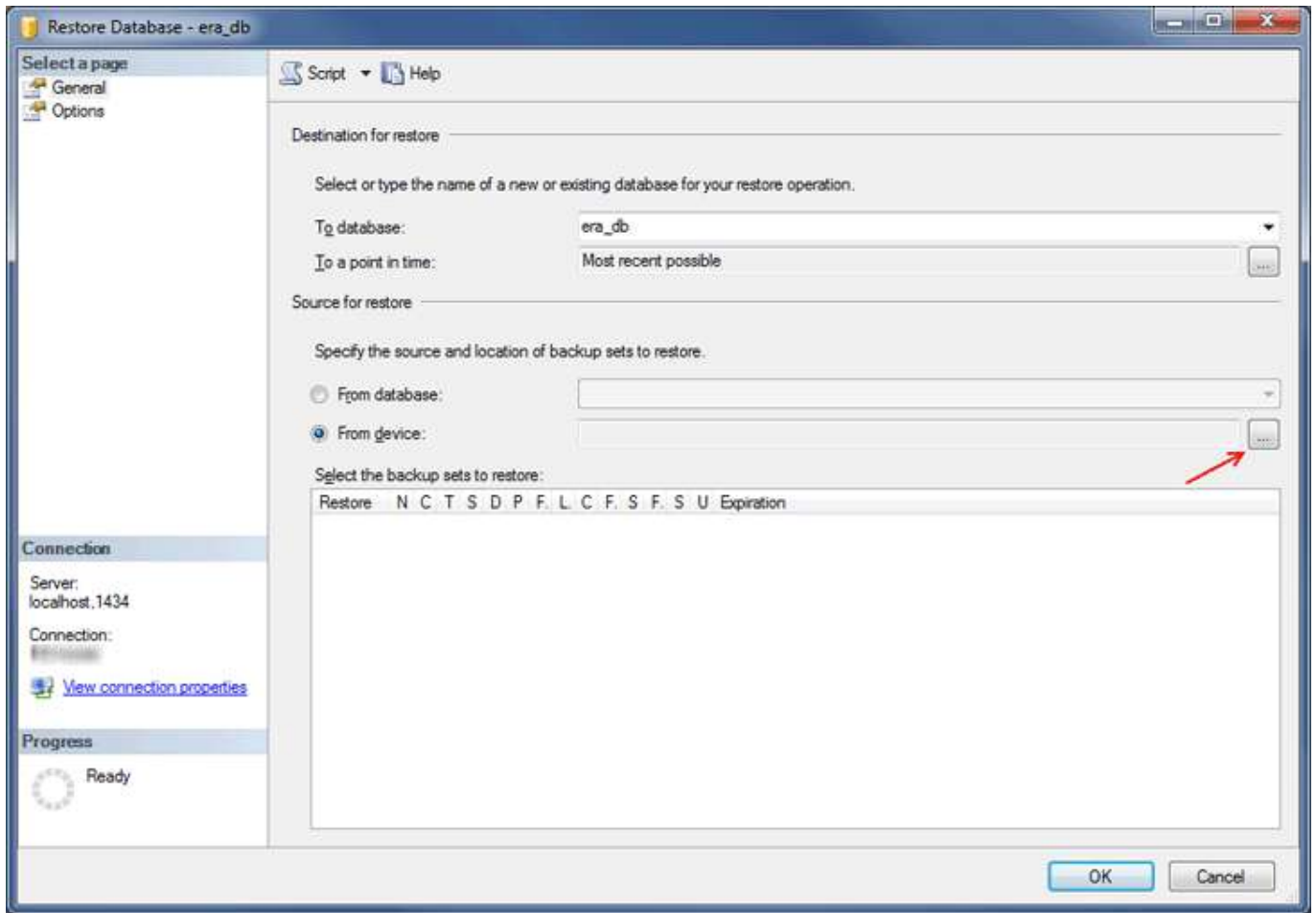
6. Log into the target SQL Server instance with SQL Server Management Studio.

7. [Restore your database](#) on the target SQL Server instance.



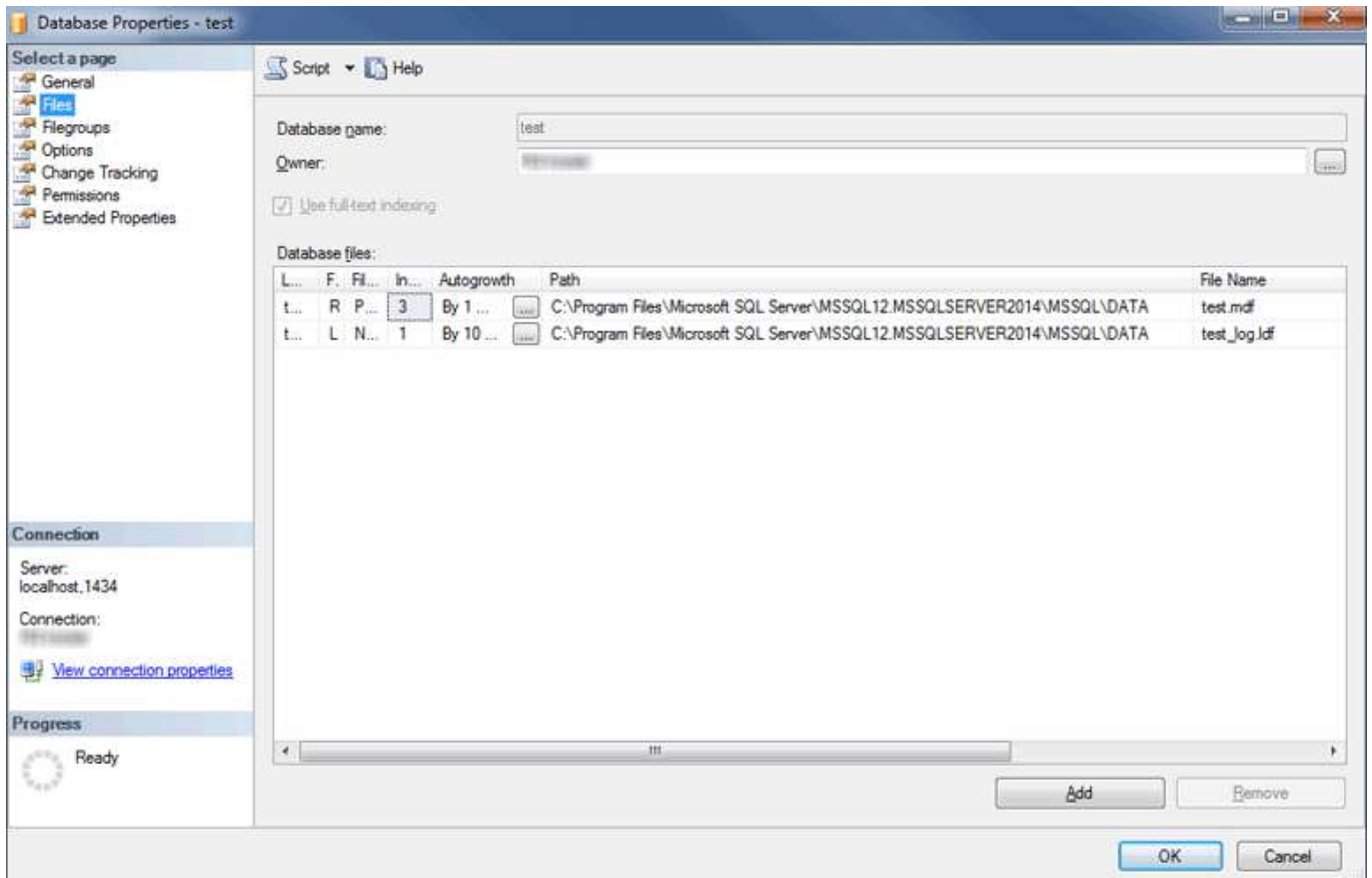
8. Type a name for your new database into the **To database** field. You can use the same name as your old database if you prefer.

9. Select **From device** under **Specify the source and location of backup sets to restore** and then click ... .



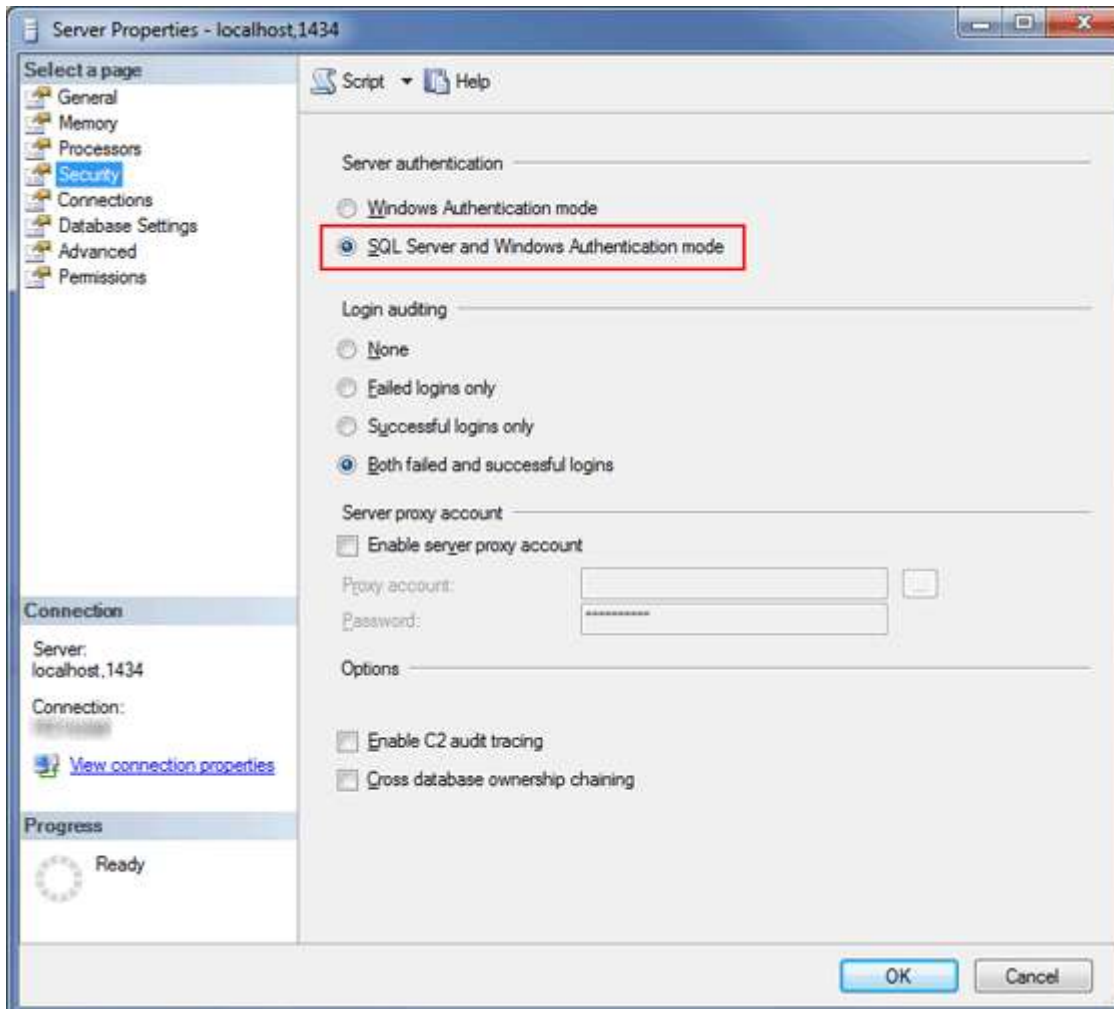
10. Click **Add**, navigate to your backup file and then open it.
11. Select the most recent possible backup to restore (the backup set may contain multiple backups).
12. Click the **Options** page of the restore wizard. Optionally, select **Overwrite existing database** and ensure that the restore locations for the database (*.mdf*) and for the log (*.ldf*) are correct. Leaving the default values unchanged will use the paths from your source SQL server, so please check these values.

If you are unsure where the DB files are stored on the target SQL Server instance, right-click an existing database, select **properties** and click the **Files** tab. The directory where the database is stored is displayed in the **Path** column of the table shown below.



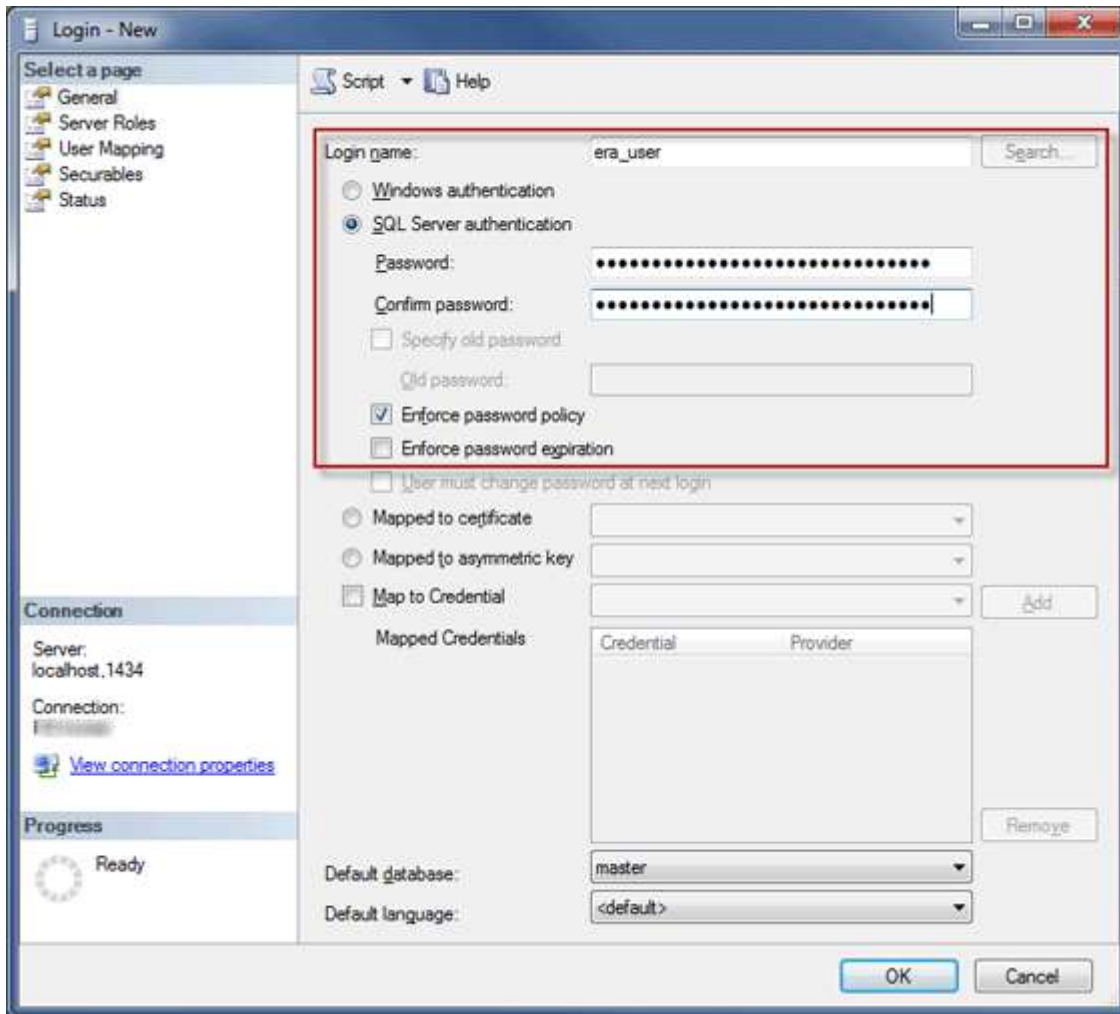
13. Click **OK** in the restore wizard window.

14. Ensure that the new database server has **SQL Server Authentication enabled**. Right-click the server and click **Properties**. Navigate to **Security** and verify that **SQL Server and Windows Authentication mode** is selected.

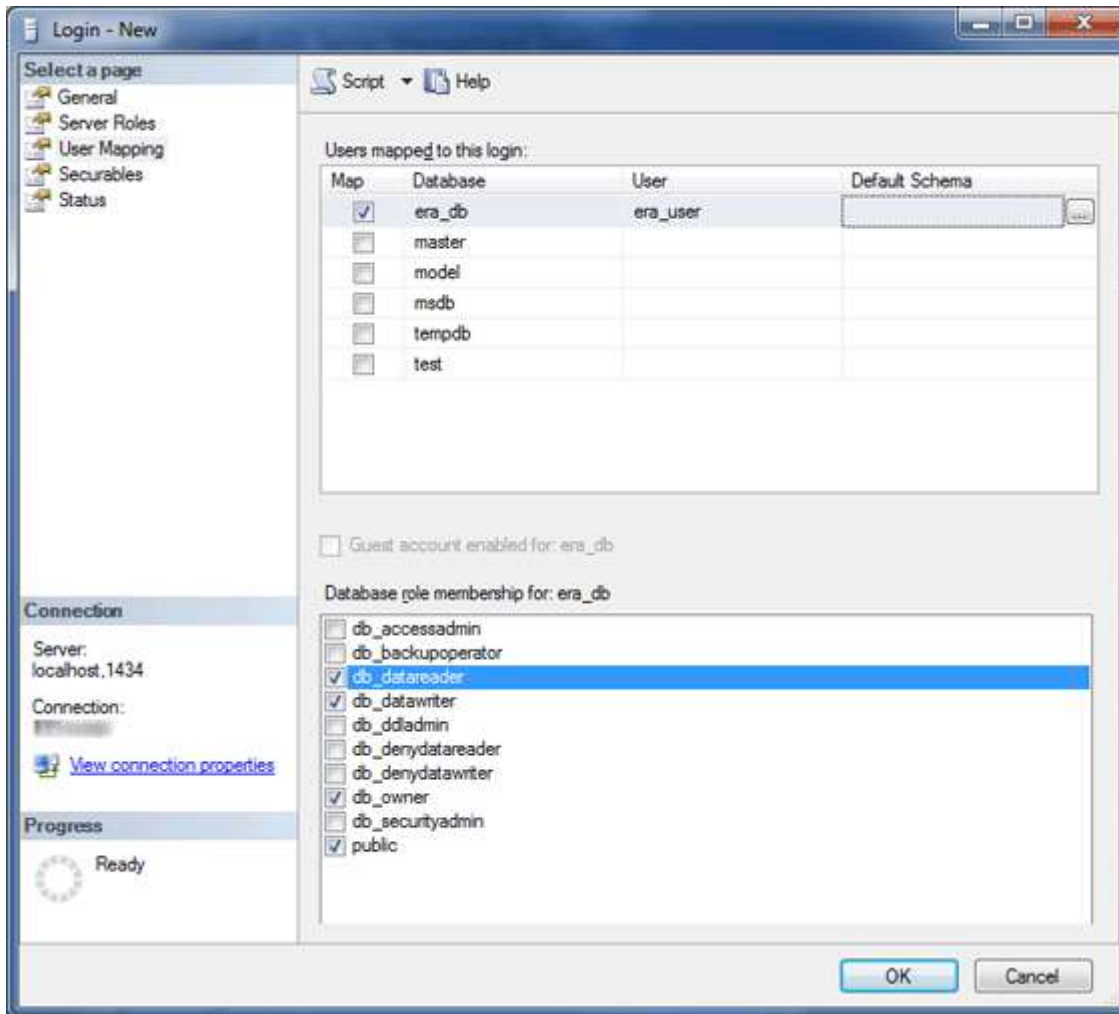


15. Create a new SQL Server login (for ESET PROTECT Server) in the target SQL Server with **SQL Server authentication** and map the login to a user in the restored database.

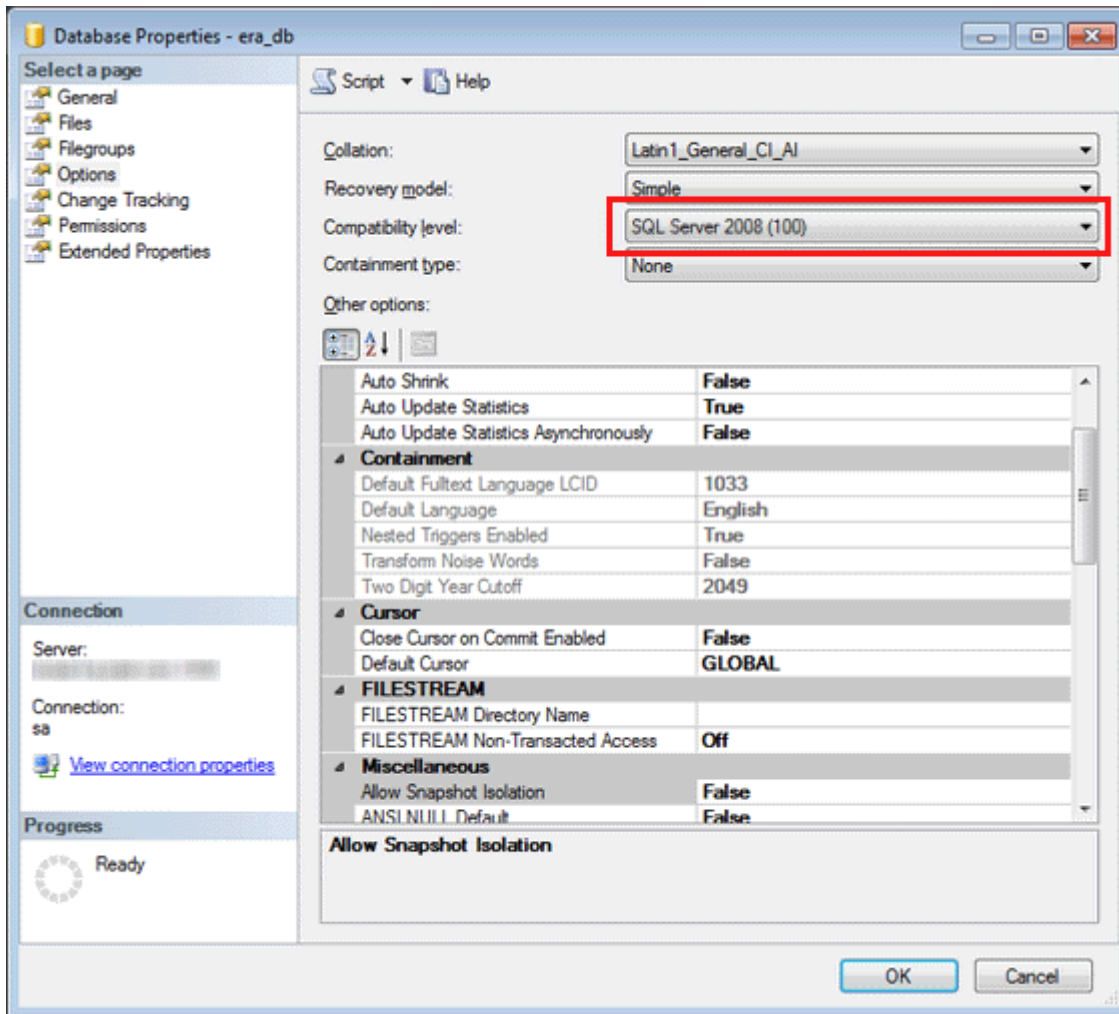
- Do not enforce password expiration!
- Recommended characters for usernames: Lower case ASCII letters, numbers and character underscore "\_"
- Recommended characters for passwords: ASCII characters ONLY, including upper case and lower case ASCII letters, numbers, spaces, special characters
- Do not use non-ASCII characters, curly braces {} or @
- Please note that if you do not follow the character recommendations above, you may have database connectivity problems or you will need to escape the special characters in the later steps during database connection string modification. Character escaping rules are not included in this document.



16. Map the login to a user in the target database. In the **user mappings** tab, ensure that the database user has the roles: **db\_datareader**, **db\_datawriter**, **db\_owner**.

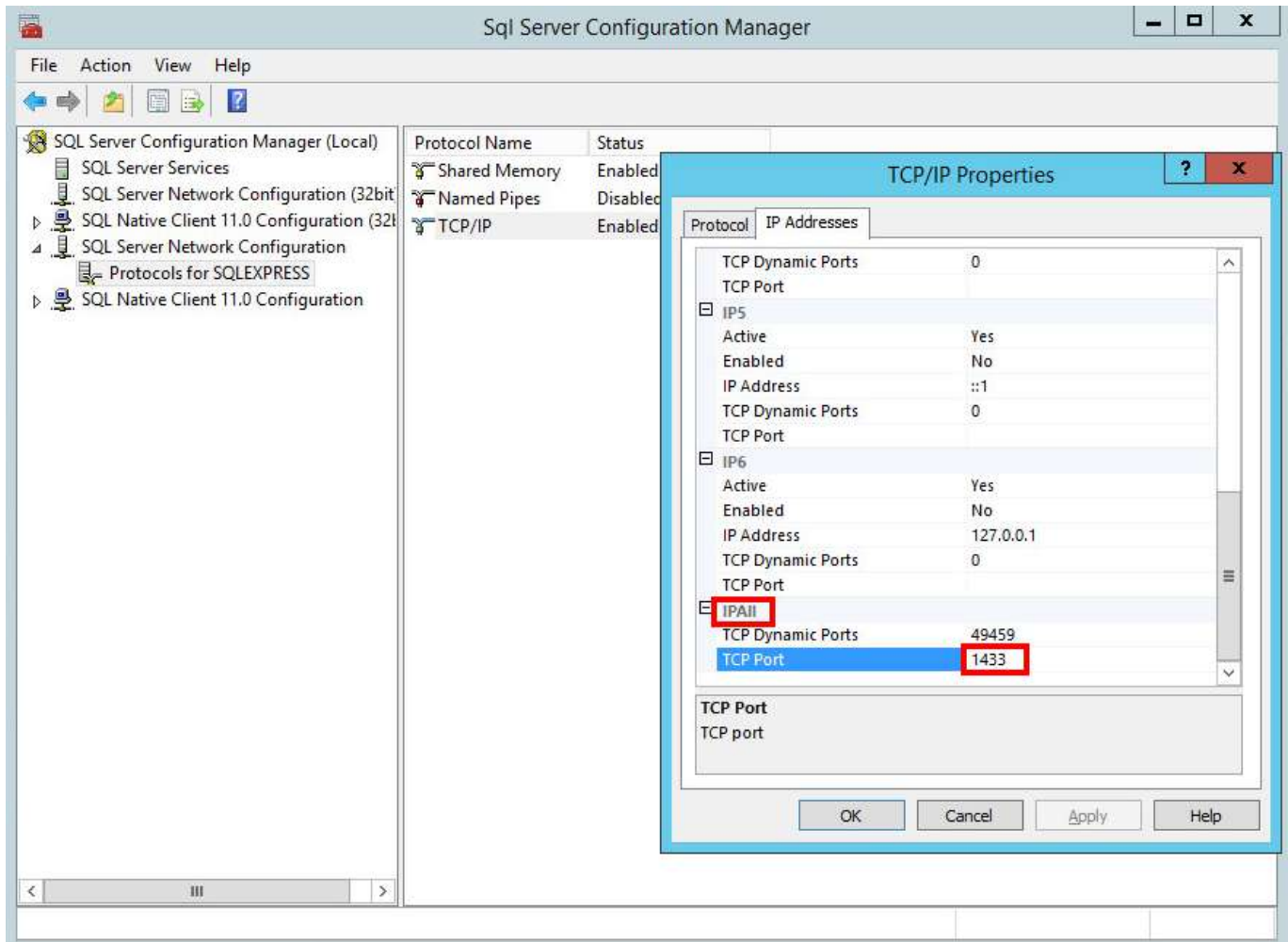


17. To enable the latest database server features, change the restored database **Compatibility level** to the latest one. Right-click the new database and open the database **Properties**.



**i** SQL Server Management Studio is unable to define compatibility levels later than that of the version in use. For example SQL Server Management Studio 2014 is unable to set compatibility level for SQL Server 2019.

18. Ensure the **TCP/IP** connection protocol is **enabled** for "db\_instance\_name"(e.g SQLEXPRESS or MSSQLSERVER) and the TCP/IP **port** is set to **1433**. To do so, open **Sql Server Configuration Manager**, navigate to **SQL Server Network Configuration > Protocols for db\_instance\_name**, right-click **TCP/IP** and select **Enabled**. Double-click **TCP/IP**, switch to the **Protocols** tab, scroll down to **IPAll** and in the **TCP Port** field, type 1433. Click **OK** and restart the **SQL Server** service.



19. [Connect the ESET PROTECT Server to the database.](#)

## Migration process for MySQL Server

### Prerequisites

- Source and target SQL Server instances must be installed. They may be hosted on different machines.
- MySQL tools must be available on at least one of the computers (`mysqldump` and `mysql` client).

### Useful links

- <https://dev.mysql.com/doc/refman/8.0/en/copying-databases.html>
- <https://dev.mysql.com/doc/refman/8.0/en/mysqldump.html>
- <https://dev.mysql.com/doc/refman/8.0/en/mysql.html>

### Migration process

In the commands, configuration files or SQL statements below, please always replace:

- **SRCHOST** with the address of the source database server
- **SRCROOTLOGIN** with the source MySQL server root user login
- **SRCDBNAME** with the name of the source ESET PROTECT database to back up
- **BACKUPFILE** with the path to the file where the backup will be stored
- **TARGETROOTLOGIN** with the target MySQL server root user login
- **TARGETHOST** with the address of the target database server
- **TARGETDBNAME** with the name of the target ESET PROTECT database (after migration)
- **TARGETLOGIN** with the login name for the new ESET PROTECT database user on the target database server
- **TARGETPASSWD** with the password of the new ESET PROTECT database user on the target database server

It is not necessary to execute the SQL statements below via the command line. If there is GUI tool available, you can use an application you already know.

1. Stop the ESET PROTECT Server service.
2. Create a full database backup of the source ESET PROTECT database (the database you plan to migrate):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -  
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. Prepare an empty database on the target MySQL server:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

**i** Use the apostrophe character ' instead of " quotation marks on Linux systems.

4. Restore the database on the target MySQL server to the previously prepared empty database:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. Create an ESET PROTECT database user on the target MySQL server:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

Recommended characters for **TARGETLOGIN**:

- Lower case ASCII letters, numbers and underscore "\_"

Recommended characters for **TARGETPASSWD**:

- ASCII characters only, including upper case and lower case ASCII letters, numbers, spaces and special characters

- Do not use non-ASCII characters, curly braces {} or @

Please note that if you do not follow the character recommendations above, you may have database connectivity problems or you will need to escape the special characters in the later steps during database connection string modification. Character escaping rules are not included in this document.

6. Grant proper access rights for the ESET PROTECT database user on the target MySQL server:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--  
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

**i** Use the apostrophe character ' instead of " quotation marks on Linux systems.

7. [Connect the ESET PROTECT Server to the database.](#)

## Connect ESET PROTECT Server to a database

Follow the steps below on the machine where ESET PROTECT Server is installed to connect it to a database.

1. Stop the ESET PROTECT Server service.
2. Find *startupconfiguration.ini*

Windows:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration  
\startupconfiguration.ini
```

Linux:

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

### Server upgrade using the standalone Server installer

**i** If you copy the database password from the *StartupConfiguration.ini* file and the password contains the @ character, delete the escape character \ before it.

3. Change the database connection string in ESET PROTECT Server *startupconfiguration.ini*

oSet the address and port of the new database server.

oSet new ESET PROTECT username and password in the connection string.

**i** If you select **Log in as current Windows user** during the ESET PROTECT Server installation ([all-in-one](#) or [standalone](#) installation), the username and password are not visible in the *startupconfiguration.ini* file. You see `Trusted_Connection=yes` instead.

The final result should look like:

Microsoft SQL:

```
DatabaseType=MSSQL0dbc  
DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pwd={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

MySQL:

```
DatabaseType=MySql0dbc  
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETLOGIN;  
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

In the configuration above, replace:

- **TARGETHOST** with the address of the target database server
- **TARGETDBNAME** with the name of the target ESET PROTECT database (after migration)
- **TARGETLOGIN** with the login name for the new ESET PROTECT database user on the target database server
- **TARGETPASSWD** with the password of the new ESET PROTECT database user on the target database server

4. Start the ESET PROTECT Server and verify that the service is running correctly.

## Change of ESET PROTECT Server IP address or hostname after migration

To change an IP address or hostname on your ESET PROTECT Server, follow these steps:

1. If your ESET PROTECT Server certificate contains a specific IP address and/or hostname, [create a new Server certificate](#) and include the new IP address or hostname you are switching to. However, if you have a wildcard \* in the host field of the Server certificate, skip to step 2. If not, create new Server certificate adding the new IP address and host name separated by a comma and include the previous IP address and hostname as well.
2. Sign the new Server certificate using your ESET PROTECT Server Certification Authority.
3. Create a policy changing the client connections to the new IP address or hostname (preferably the IP address), but include a second (alternative) connection to the old IP address or hostname to give the ESET Management Agent a chance to connect to both servers. For more details, see [Create policy for ESET Management Agents to connect to the new ESET PROTECT Server](#).
4. Apply this policy to your client computers and allow the ESET Management Agents to replicate. Even though the policy will redirect clients to your new server (which is not running), the ESET Management Agents will use the alternative Server information to connect to the original IP address.
5. Set your [new Server certificate in More > Settings](#).
6. Restart the ESET PROTECT Server service and change the IP address or hostname.

See our [Knowledgebase article](#) for illustrated instructions to change the ESET PROTECT Server address.

# Uninstall

Select one of the below chapters to uninstall ESET PROTECT Server and its components:

- [Uninstall ESET Management Agent](#)
- [Windows—Uninstall ESET PROTECT Server and its components](#)
- [Linux—Upgrade, reinstall or uninstall ESET PROTECT components](#)
- [macOS—Uninstall ESET Management Agent and ESET endpoint application](#)
- [Decommission the old ESET PROTECT Server after migration to another server](#)

## Uninstall ESET Management Agent

The ESET Management Agent can be uninstalled in several ways.

### Remote uninstallation using ESET PROTECT Web Console

1. [Log in to ESET PROTECT Web Console](#).
2. From the **Computers** pane, select a computer from which you want to remove the ESET Management Agent and select **Tasks > New Task**.  
  
Alternatively, select multiple computers by selecting the corresponding check boxes and then click **Computer > Tasks > New Task**.
3. Type a **Name** for the task.
4. From the **Task category** drop-down menu select **ESET PROTECT On-Prem**.
5. From the **Task** drop-down menu select [Stop Managing \(Uninstall ESET Management Agent\)](#).

Uninstalling the ESET Management Agent removes the device from ESET PROTECT On-Prem management:

- ESET security application may keep some settings after uninstalling the ESET Management Agent.
- If the ESET Management Agent is password-protected, you must provide the password to uninstall, repair or upgrade (with changes) the Agent. We recommend that you reset some settings that you do not want to keep (for example, password protection) to default settings using a [policy](#) before the device is removed from management.
- All tasks running on the Agent will stop. The Web Console may not show accurate task statuses (**Running, Finished, Failed**) due to replication.
- After uninstalling the Agent, you can manage your security application with EGUI or [eShell](#).


6. Review the task **Summary** and click **Finish**.
7. Click [Create Trigger](#) to specify when this Client Task should be executed and on what **Targets**.

## Local uninstallation—Windows

 See also the instructions for local uninstallation of ESET Management Agent on [Linux](#) or [macOS](#). For Agent uninstallation troubleshooting, see [ESET Management Agent uninstallation troubleshooting](#).

1. Connect to the endpoint computer where you want to remove the ESET Management Agent (for example via RDP).
2. Navigate to **Control Panel > Programs and Features** and double-click **ESET Management Agent**.
3. Click **Next > Remove** and follow the uninstallation instructions.

If you have set up a password using a policy for your ESET Management Agents, you have these options:

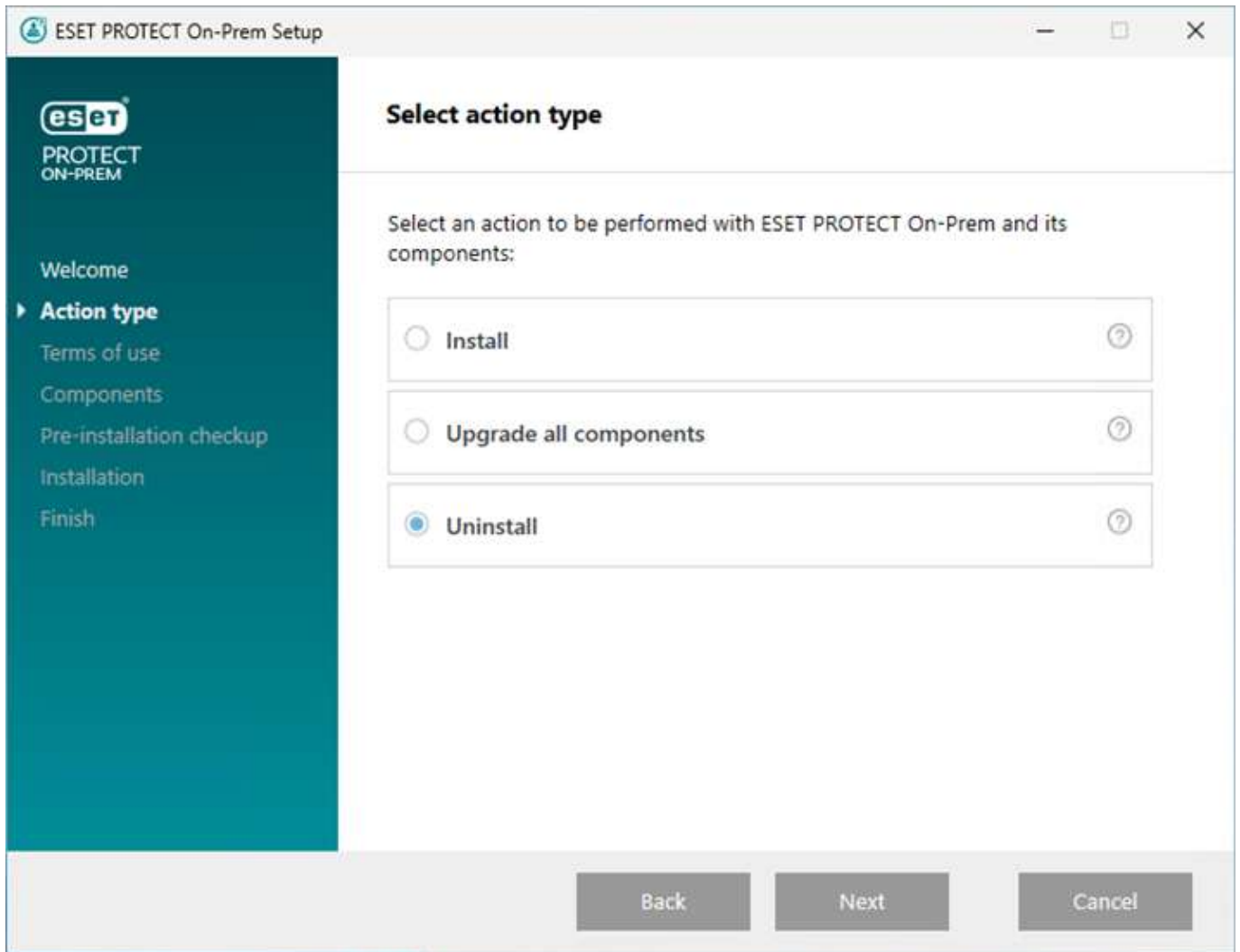
-  • You will need to type the password during uninstallation.
- Unassign the policy first before uninstalling ESET Management Agent.
- [Redeploy ESET Management Agent over an existing password protected Agent](#) (a Knowledgebase article).

## Windows—Uninstall ESET PROTECT Server and its components

 Before uninstalling ESET PROTECT On-Prem, [uninstall Agents on managed computers](#).

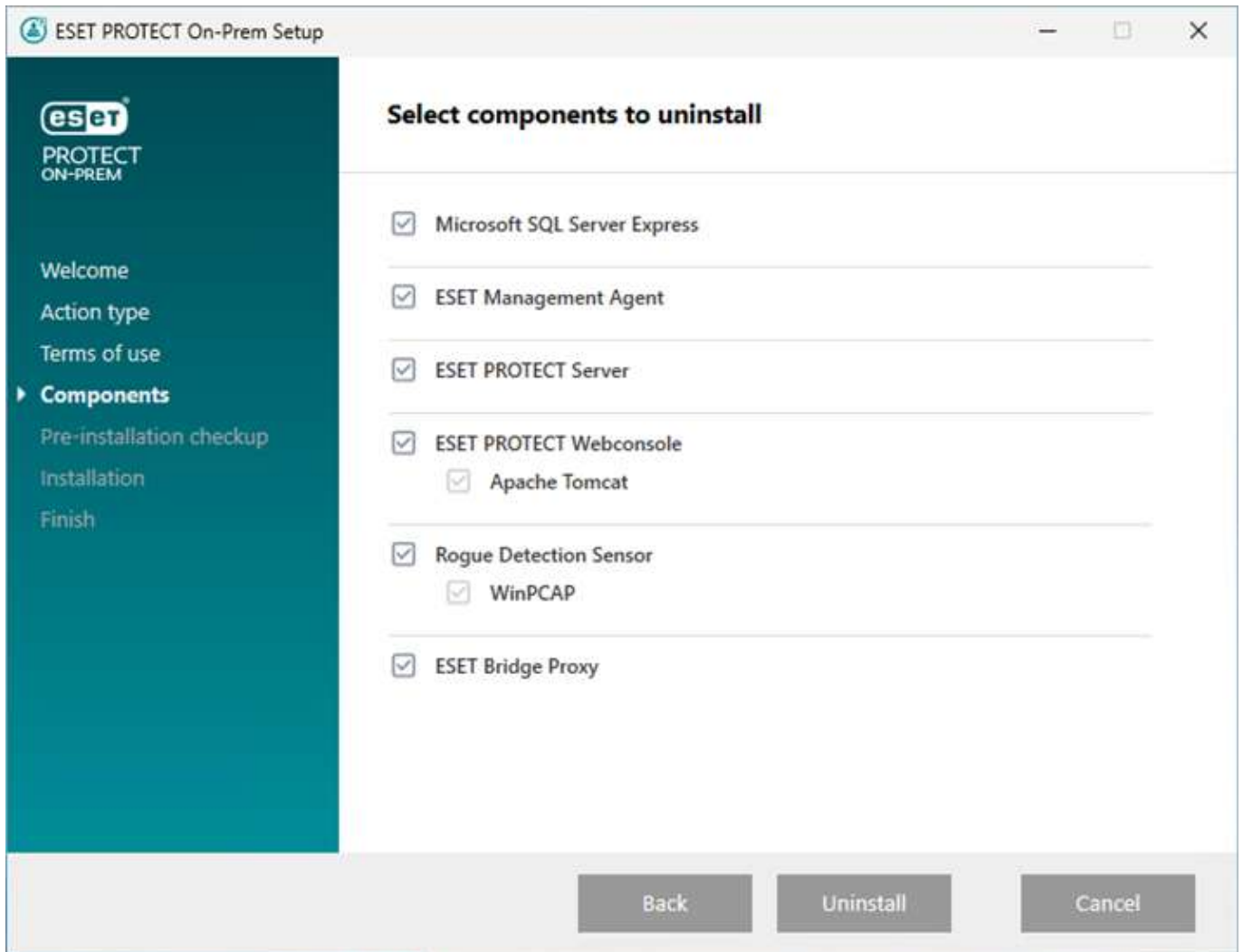
Follow these steps to uninstall ESET PROTECT Server and its components on Windows:

1. Download the [ESET PROTECT All-in-one installer](#) and unzip the package.
2. Run the *Setup.exe*. You can select **Language** from the drop-down menu. Click **Next**.
3. Select **Uninstall** and click **Next**.



4. Select **I accept the Terms of Use** and click **Next**.

5. Select the component(s) you want to uninstall and click **Uninstall**.



6. A computer restart may be required to complete the removal of specific components.

**i** See also [Decommission the old ESET PROTECT On-Prem Server after migration to another server.](#)

## Linux—Upgrade, reinstall or uninstall ESET PROTECT components

If you want to reinstall or upgrade to a more recent version, run the installation script again.

To uninstall a component (in this case ESET PROTECT Server), run the installer with the `--uninstall` parameter, as shown below:

```
sudo ./server_linux_x86_64.sh --uninstall --keep-database
```

If you want to uninstall other component, use appropriate package name in the command. For example ESET Management Agent:

```
sudo ./agent_linux_x86_64.sh --uninstall
```

**!** Configuration and database files will be removed during uninstallation. To preserve database files, create a SQL dump of the database or use the `--keep-database` parameter.

After uninstalling, verify whether

- the service `eraserver` is deleted.
- the folder `/etc/opt/eset/RemoteAdministrator/Server/` is deleted.

**i** We recommend that you create a database dump backup before performing uninstallation if you need to restore your data.  
For more information on reinstalling the Agent, see the related [chapter](#).  
For Agent uninstallation troubleshooting, see [ESET Management Agent uninstallation troubleshooting](#).

## macOS—Uninstall ESET Management Agent and ESET Endpoint application

Uninstall the ESET Management Agent and ESET endpoint application locally or remotely via ESET PROTECT On-Prem.

You can find the more detailed instructions for local uninstallation of ESET Management Agent and ESET Endpoint application in our [Knowledgebase article](#).

**!** If you want to remotely uninstall the ESET Endpoint application, ensure to do so before uninstalling the ESET Management Agent.

### Uninstall the ESET Management Agent locally

1. Click **Finder** to open a new **Finder** window.
2. Click **Applications** > hold **CTRL** > click **ESET Management Agent** > select **Show Package Contents** from the context menu.
3. Navigate to **Contents** > **Scripts** and double-click **Uninstaller.command** to run the uninstaller.
4. Type your administrator password and press **Enter** if you are prompted to type a password.
5. You will see the **Process completed** message when ESET Management Agent has been uninstalled.

### Uninstall the ESET Management Agent locally via Terminal

1. Open **Finder** > **Applications** > **Utilities** > **Terminal**.
2. Type the following code and press **Enter**:

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;  
exit;
```

3. Type your administrator password and press **Enter** if you are prompted to type a password.
4. You will see the **Process completed** message when ESET Management Agent has been uninstalled.

## Uninstall the ESET Management Agent remotely via ESET PROTECT On-Prem

In **Computers**, click the client macOS computer and select [Remove](#) to uninstall the ESET Management Agent and remove the computer from management.

For Agent uninstallation troubleshooting, see [ESET Management Agent uninstallation troubleshooting](#).

## Uninstall ESET Endpoint application locally

1. Click **Finder** to open a new **Finder** window.
2. Click **Applications** > hold **CTRL** > click **ESET Endpoint Security** or **ESET Endpoint Antivirus** > select **Show Package Contents** from the context menu.
3. Navigate to **Contents** > **Helpers** and double-click **Uninstaller.app** to run the uninstaller.
4. Click **Uninstall**.
5. Type your administrator password and click **OK** if you are prompted to type a password.
6. You will see the **Uninstall Succeeded** message when ESET Endpoint Security or ESET Endpoint Antivirus has been successfully uninstalled. Click **Close**.

## Uninstall ESET Endpoint application locally via Terminal

1. Open **Finder** > **Applications** > **Utilities** > **Terminal**.
2. Type the following code and press **Enter**:

- Uninstall ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
```

- Uninstall ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/Contents/Scripts/uninstall.sh
```


3. Type your administrator password and press **Enter** if you are prompted to type a password.
4. You will see the **Process completed** message when ESET Endpoint application has been uninstalled.

## Uninstall ESET Endpoint application remotely via ESET PROTECT On-Prem

To uninstall the ESET Management Agent remotely via ESET PROTECT On-Prem, you can use one of these options:

- In **Computers**, click the client macOS computer, select **Details > Installed Applications** > select **ESET Endpoint Security** or **ESET Endpoint Antivirus** and click the **Uninstall** button.
- Use the [Software Uninstall task](#).


## Decommission the old ESET PROTECT Server after migration to another server

 Ensure your new ESET PROTECT Server is running and client computers are connecting to your new ESET PROTECT On-Prem correctly.

There are two options when decommissioning your old ESET PROTECT Server after migration to another server:

### I. Keep the server machine operating system and reuse it


1. [Stop the old ESET PROTECT Server service](#).
2. Delete (DROP DATABASE) the old ESET PROTECT Server database instance (Microsoft SQL or MySQL).

 If you migrated the database to the new ESET PROTECT Server, ensure to delete the database on the old ESET PROTECT Server before uninstallation to prevent subscriptions from being dissociated (removed) from the new ESET PROTECT Server database.

3. Uninstall the old ESET PROTECT On-Prem Server and all its components (including ESET Management Agent, Rogue Detection Sensor, etc.):

o [Uninstall ESET PROTECT On-Prem—Windows](#)


o [Uninstall ESET PROTECT On-Prem—Linux](#)

 Do not uninstall your database if there is other software dependent on your database.

4. Plan an operating system restart of your server after uninstallation.

### II. Keep the server machine

The easiest way to remove ESET PROTECT On-Prem is to format the disk where it is installed.

 This will erase everything on the disk, including the operating system.

## FAQ

- [Why are we installing Java on a server? Doesn't this create a security risk? Most security companies and frameworks recommend that you uninstall Java from computers, especially from servers.](#)
- [How do I determine which port the SQL Server is using?](#)
- [How do I configure MySQL to accept large packet size?](#)

- [If I install SQL myself, how should I create a database for ESET PROTECT On-Prem?](#)
- [Can the ESET PROTECT On-Prem Installer create a new database for me in an existing Microsoft SQL Server installation if I give it the proper Microsoft SQL Server connection details and credentials? It would be convenient if the installer supported different versions of SQL Server.](#)
- [If installing on an existing SQL Server, should the SQL Server use built-in Windows Authentication mode by default?](#)
- [Can I use MariaDB instead of MySQL?](#)
- [It is very difficult to tell whether the SQL Server installation is running. How can I tell what is happening if the installation takes more than 10 minutes?](#)
- [How do I reset the Administrator password for Web Console \(typed during the setup\)?](#)
- [Can you use IIS instead of Apache Tomcat? What about another HTTP server?](#)
- [Does ESET PROTECT On-Prem have a command line interface?](#)
- [Can you install ESET PROTECT On-Prem on a domain controller?](#)
- [Will the ESET PROTECT Server installation detect if SQL is already installed? What happens if it does? What about MySQL?](#)
- [Where can I find an ESET PROTECT component mapped by its release version?](#)
- [How do I upgrade ESET PROTECT On-Prem to the latest version?](#)
- [How can I update a system without an internet connection?](#)
- [How do I reinstall my ESET PROTECT Server and connect it to an existing SQL server if the SQL server was set up automatically by the initial ESET PROTECT On-Prem install?](#)
- [How do I fix issues with Active Directory sync on Linux?](#)
- [Can I use my network resource \(like SMB share\) instead of the repository?](#)
- [How do I reset or change my password?](#)
- [How do I change ESET PROTECT Server and ESET PROTECT Web Console ports?](#)
- [Can I upgrade from ERA 5.x/6.x or ESMC 7.x directly to ESET PROTECT On-Prem 13.0?](#)
- [I am receiving error messages or have problems with ESET PROTECT On-Prem. What should I do?](#)

**Why are we installing Java on a server? Doesn't this create a security risk? Most security companies and frameworks recommend that you uninstall Java from computers, especially from servers.**

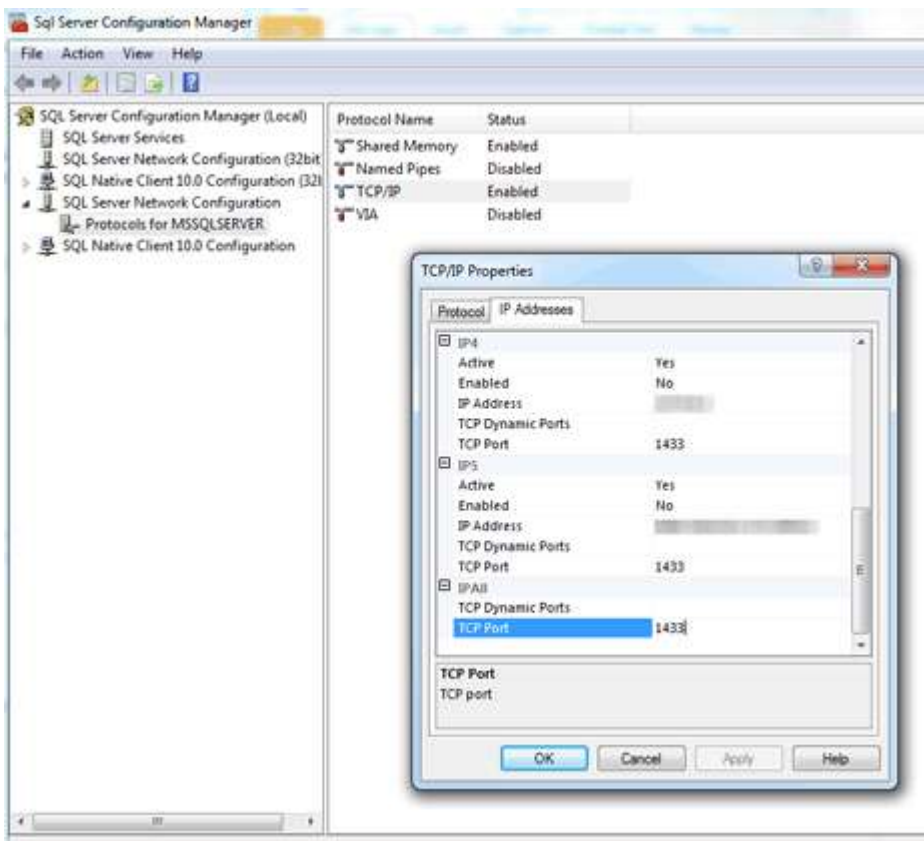
The ESET PROTECT Web Console requires Java/OpenJDK to function. Java is an industry standard for web-based consoles, and all major web consoles use Java and a Web Server (Apache Tomcat) for their operation. Java is

necessary to support a multi-platform web server. You can install a Web Server on a dedicated machine for security reasons.

**!** Starting January 2019, Oracle JAVA SE 8 public updates for business, commercial or production use require a commercial license. If you do not purchase a JAVA SE subscription, you can transition to a no-cost alternative. See the [supported versions of JDK](#).

## How do I determine which port the SQL Server is using?

There are multiple ways to determine the port used by the SQL Server. You can get the most accurate result via the SQL Server Configuration Manager. See the figure below for an example of where to locate this information in SQL Configuration Manager:



After installing SQL Server Express (included in ESET PROTECT On-Prem package) on Windows Server 2012, it does not appear to listen on a standard SQL port. It most likely listens to a port other than the default port 1433.

## How do I configure MySQL to accept large packet size?

See MySQL installation and configuration for [Windows](#) or [Linux](#).

## If I install SQL myself, how should I create a database for ESET PROTECT On-Prem?

You do not have to. A database is created by the *Server.msi* installer, not by the ESET PROTECT Installer. The ESET PROTECT Installer is included to simplify steps for you. It installs the SQL Server, and then the database is created by the *Server.msi* installer.

## Can the ESET PROTECT On-Prem Installer create a new database for me in an existing Microsoft SQL Server installation if I give it the proper Microsoft SQL Server connection details and credentials? It would be convenient if the installer supported different versions of SQL Server.

The database is created by *Server.msi*. So, yes, it can create an ESET PROTECT database for you on individually installed SQL Server instances. See the list of [supported versions of Microsoft SQL Server](#).

The ESET PROTECT On-Prem 13.0 [All-in-one installer](#) installs Microsoft SQL Server Express 2022 by default.

oUpgrading checks for previous SQL installations and offers an upgrade to SQL 2022 or 2016 (based on the operating system).

oThe installer generates a random password for database authentication and stores it in `%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini`.

Microsoft SQL Server Express (the free edition) has a 10 GB size limit for each relational database. We recommend using other Microsoft SQL Server editions than Microsoft SQL Server Express:



- In enterprise environments or large networks.
- If you want to use ESET PROTECT On-Prem with [ESET Inspect On-Prem](#).

## If installing on an existing SQL Server, should the SQL Server use built-in Windows Authentication mode by default?

No, because Windows Authentication mode can be disabled on the SQL Server, and the only way to log in is to use SQL Server Authentication (entering a Username and Password). During the installation of the ESET PROTECT Server, the Mixed mode authentication (SQL Server Authentication and Windows Authentication) is required. When manually installing the SQL Server, we recommend you create a root password (root user is named "sa", which stands for security administrator) and store it for later in a safe place. The root password may be needed when upgrading the ESET PROTECT Server. You can set the [Windows Authentication](#) after installing the ESET PROTECT Server.

## Can I use MariaDB instead of MySQL?

No, MariaDB is not supported. Ensure to install a [supported version of MySQL Server and ODBC Connector](#). See [MySQL installation and configuration](#).

## It is very difficult to tell whether the SQL Server installation is running. How can I tell what is happening if the installation takes more than 10 minutes?

In rare cases, the SQL Server installation can take up to 1 hour. Install times depend on system performance.

## How do I reset the Administrator password for Web Console (typed during the setup)?

Read the instructions on how to [reset the Administrator password](#).

## Can you use IIS instead of Apache Tomcat? What about another HTTP server?

IIS is an HTTP server. The Web Console needs a Java servlet container (like Apache Tomcat) to run, and the HTTP server is not sufficient. There have been solutions for changing IIS into a Java servlet container, but in general, this is not supported.

**i** We do not use Apache HTTP Server. We use Apache Tomcat, which is a different application.

## Does ESET PROTECT On-Prem have a command line interface?

Yes, we have the ESET PROTECT On-Prem [ServerApi](#).

## Can you install ESET PROTECT On-Prem on a domain controller?

[Do not install SQL Server on a Domain Controller](#). Install ESET PROTECT On-Prem on a different server or deselect the SQL Server Express component during installation. Use your existing SQL or MySQL Server to run the ESET PROTECT database.

## Will the ESET PROTECT Server installation detect if SQL is already installed? What happens if it does? What about MySQL?

ESET PROTECT On-Prem will check for SQL running on a system if you are using the Installation Wizard and you have selected SQL Express to install. If there is already an SQL running on a system, the wizard will display a notification to uninstall the existing SQL, and then run the installation again, or install ESET PROTECT On-Prem without SQL Express. See [database requirements](#) for ESET PROTECT On-Prem.

## Where can I find an ESET PROTECT component mapped by its release version?

See the [Knowledgebase article](#).

## How do I upgrade ESET PROTECT On-Prem to the latest version?

See [upgrade procedures](#).

## How can I update a system without an internet connection?

Using [ESET Bridge HTTP Proxy](#) installed on a machine that can connect to the ESET update servers (where update files are cached) and pointing endpoints to that HTTP Proxy on a local network. If your server does not have an internet connection, you can enable the mirror feature of the endpoint application on one machine, use a USB

drive to deliver update files to this computer and configure all other offline computers to use it as an update server.

For details on how to perform an offline installation, [follow these instructions](#).

## How do I reinstall my ESET PROTECT Server and connect it to an existing SQL server if the SQL server was set up automatically by the initial ESET PROTECT On-Prem install?

If you are installing the new ESET PROTECT Server using the same user account (for example, a domain administrator's account) under which you have installed the original ESET PROTECT Server, you can use **MS SQL Server via Windows Authentication**.

## How do I fix issues with Active Directory sync on Linux?

Verify your domain name is typed in all capital letters (`administrator@TEST.LOCAL` instead of `administrator@test.local`).

## Can I use my network resource (like SMB share) instead of the repository?

You can choose to provide the direct link where a package is located. If you are using a file share, specify it in the following format: `file://` followed by the full network path to the file, for example:

```
file://\eraserver\install\ees_nt64_ENU.msi
```

## How do I reset or change my password?

Ideally, the administrator account should only be used to create accounts for individual administrators. When [administrator accounts](#) are created, the administrator password should be saved and the administrator account should not be used. This practice allows for the administrator account to be used for password reset/account details only.

How to reset the password of a built-in ESET PROTECT On-Prem Administrator account:

1. Open **Programs and Features** (run `appwiz.cpl`), locate the ESET PROTECT Server and right-click.
2. Select **Change** from the context menu.
3. Choose **Repair**.
4. Specify database connection details.
5. Select **Use existing database and apply upgrade**.
6. Deselect **Use password already Stored in database** and type a new password.
7. Log into the ESET PROTECT Web Console with your new password.



We strongly recommend that you create additional accounts with specific access rights based on your desired account competencies.

## How do I change ESET PROTECT Server and ESET PROTECT Web Console ports?

You must change the port in your web server configuration to allow web server connections to the new port. To do so, follow the steps below:

1. Shut down your web server.
2. Modify the port in your web server configuration.
  - a) Open the file `webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties`
  - b) Set the new port number (for example, `server_port=44591`)
3. Start the web server again.

## Can I upgrade from ERA 5.x/6.x or ESMC 7.x directly to ESET PROTECT On-Prem 13.0?

If you have ERA 5.x/6.x or ESMC 7.x, the direct upgrade to ESET PROTECT On-Prem 13.0 is not supported—Perform a clean installation of ESET PROTECT On-Prem 13.0.

You can upgrade to ESET PROTECT On-Prem 13.0 from ESET PROTECT On-Prem 10.1 and later. A direct upgrade from the End of Life versions 8.x–10.0 has not been tested and is not supported.

## I am receiving error messages or have problems with ESET PROTECT On-Prem. What should I do?

See [Troubleshooting FAQs](#).

## Troubleshooting

Since ESET PROTECT On-Prem is a complex application that uses several third-party tools and supports many operating system platforms, there is the potential that you will encounter issues that require troubleshooting.

ESET documentation includes several methods to troubleshoot ESET PROTECT On-Prem. See [Answers to common installation issues](#) to resolve some common issues with ESET PROTECT On-Prem. See also the [known issues for ESET business applications](#).

## Unable to resolve your issue?

- Each ESET PROTECT component has a [log file](#) that you can configure to be more or less verbose. Review logs to identify errors that might explain the issue you are having.
- Logging verbosity of each component is set in its [policy](#) > **Trace log verbosity**—Set the log verbosity to determine the level of information that will be collected and logged, from **Trace** (informational) to **Fatal** (most important critical information). The policy must be applied to the device to take effect.

o [ESET Management Agent policy](#)—To enable full ESET Management Agent logging in the *trace.log* file, create a dummy file named *traceAll* without an extension in the same folder as a *trace.log* and then restart the computer (to restart the ESET Management Agent service).

o [ESET Bridge policy](#)

o The logging verbosity for ESET PROTECT Server is in [Settings](#).

- If you cannot resolve your issue, you can visit the [ESET Security Forum](#) and consult the ESET community for information about issues you may encounter.
- When contacting [ESET Technical Support](#), you may be asked to collect log files using [ESET Log Collector](#) or [Diagnostic Tool](#). We strongly recommend that you include logs when contacting support to speed up your customer care service request.

## Upgrade ESET PROTECT components in offline environment

Follow these steps to upgrade your ESET PROTECT components and ESET Endpoint applications without access to the internet:

Use of the [Components Upgrade task](#) for an offline environment is possible when:

- There is an [offline repository](#) available.
- Location of the repository for ESET Management Agent is configured using a [policy](#) to an accessible location.

### Perform an upgrade of ESET PROTECT Server and Web Console

1. [Check which version of ESET management console](#) is running on the server.
2. Download the latest [All-in-one installer for Windows](#) or the latest [standalone ESET PROTECT component installers for Linux](#) from the ESET Download site.
3. Perform an upgrade of ESET PROTECT Server and ESET PROTECT Web Console:
  - Windows—[Upgrade using the All-in-one installer](#)
  - Linux—[Manual component-based upgrade](#)

**i** The Web Console and Apache Tomcat upgrade clears the [Offline help](#) files. If you used Offline help with an earlier ESET PROTECT On-Prem version, re-create it for ESET PROTECT On-Prem 13.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT On-Prem version.

### Continue with the offline upgrade of ESET endpoint applications

1. See which ESET applications are installed on clients: Open ESET PROTECT Web Console and navigate to **Dashboard > ESET applications**.
2. Ensure you have the [latest versions of ESET endpoint applications](#).

3. Download installers from the [ESET Download site](#) to the local repository configured during [offline installation](#).
4. Run a [Software Install task](#) from ESET PROTECT Web Console.

## Answers to common installation issues

Expand the section for the error message you want to resolve:

 [ESET PROTECT Server](#)

The ESET PROTECT Server service does not start:

## Broken installation

- This might be the result of missing registry keys, missing files or invalid file permissions.
- The ESET All-in-one installer has its [own log file](#). When installing a component manually, use the [MSI Logging](#) method.

## Listening port already used (mostly 2222 and 2223)

Use the appropriate Command for your operating system:

- Windows:

```
netstat -an | find "2222"
```

```
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
```

```
netstat | grep 2223
```

## Database not running / not reachable

- Microsoft SQL Server: Verify that port 1433 is available on/to the database server or try to log in to SQL Server Management Studio.
- MySQL: Verify that port 3306 is available on/to the database server or try to log in to your database interface (for example, using the MySQL command line interface or `phpmyadmin`).

## Changed IP of the ESET PROTECT Server



Do not change the computer name of your ESET PROTECT Server machine after the installation. See [Change of IP address or hostname on ESET PROTECT Server](#) for more information.

## Corrupted database

Multiple SQL errors will be shown in the ESET PROTECT Server log file. We recommend that you restore your database from a backup. If a backup is not present, reinstall ESET PROTECT On-Prem.

## Insufficient system resources (RAM, disk space)

Review running processes and system performance:

- Windows users: Run and review information in Task Manager or Event Viewer
- Linux users: Run one of the following commands:

```
df -h (to review disk space information)
```

```
cat /proc/meminfo (to review memory space information)
```

```
dmesg (to review your Linux system health)
```

## Error with ODBC connector during ESET PROTECT Server installation

Error: (Error 65533) ODBC connector compatibility check failed.

Please install ODBC driver with support for multi-threading.

Reinstall an ODBC driver version that supports multi-threading or reconfigure `odbcinst.ini` as shown in the [ODBC configuration section](#).

## Error with a database connection during ESET PROTECT Server installation

Installation of ESET PROTECT Server finishes with the generic error message:

The database server is not configured correctly.

Please check the documentation and reconfigure the database server as needed.

Error message from the install log:

```
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.
```

ESET Management Agent

Verify that the configuration of your database driver matches that shown as in the [ODBC configuration section](#).

## ESET Management Agent uninstallation troubleshooting

- See [log files](#) for ESET Management Agent.
- You can uninstall ESET Management Agent using [ESET Uninstaller](#) or using a non-standard way (such as removing files, removing the ESET Management Agent service and registry entries). If there is an ESET endpoint application on the same machine, it will not be possible because of an [enabled Self-Defense](#).
- The message "The database cannot be upgraded. Please remove the product first." is displayed during Agent uninstallation—Repair ESET Management Agent:
  1. Click **Control Panel > Programs and Features** and double-click **ESET Management Agent**.
  2. Click **Next > Repair** and follow the instructions.All possible ways of uninstalling ESET Management Agent are described in the [Uninstallation section](#).

## Error Code 1603 occurred during the Agent installation

This error can occur when the installer files are not located on the local disk. To fix this, copy the installer files to the local directory and run the installation again. If the files are already present, or the error persists, follow our [Knowledgebase instructions](#).

## Error message appears during the installation of Agent on Linux

Error message:

```
Checking certificate ... failed
```

```
Error checking peer certificate: NOT_REGULAR_FILE
```

The possible cause of this error is an incorrect filename in the installation command. The console is case sensitive. For example, `Agent.pfx` is not the same as `agent.pfx`.

## The ESET Management Agent cannot connect to the ESET PROTECT Server

See [Troubleshooting Agent connection](#) and our [Knowledgebase article](#).

## The Agent script installer exited with the code 30

You use the Agent script installer with a custom installer location and you failed to edit the script correctly. Review the [help page](#) and try again.

[Web Console](#)

[ESET Bridge \(HTTP Proxy\)](#)

 [ESET Rogue Detector Sensor](#)

## Why is the following error message continuously logged in the ESET Rogue Detector's trace.log?

```
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)
```

This is a problem with WinPcap. Stop the ESET Rogue Detector Sensor service, reinstall the latest version of WinPcap (at least 4.1.0) and restart the ESET Rogue Detector Sensor service.

 [Microsoft SQL Server](#)

## Error code -2068052081 during Microsoft SQL Server installation.

Restart your computer and run setup again. If the issue persists, uninstall the SQL Server Native Client and run installation again. If this does not resolve the issue, uninstall all Microsoft SQL Server applications, restart your computer, and then run installation again.

## Error code -2067922943 during Microsoft SQL Server installation.

Verify that your system meets the [database requirements](#) for ESET PROTECT On-Prem.

## Error code -2067922934 during Microsoft SQL Server installation.

Ensure that you have the correct [user account privileges](#).

## The Web Console shows "Failed to Load Data".

Microsoft SQL Server tries to use as much disk space as possible for transaction logs. If you want to clean up this, [visit official Microsoft website](#).

## Error code -2067919934 during Microsoft SQL Server installation.

Ensure that all previous steps have been finished successfully. This error is caused by misconfigured system files. Restart your computer and run installation again.

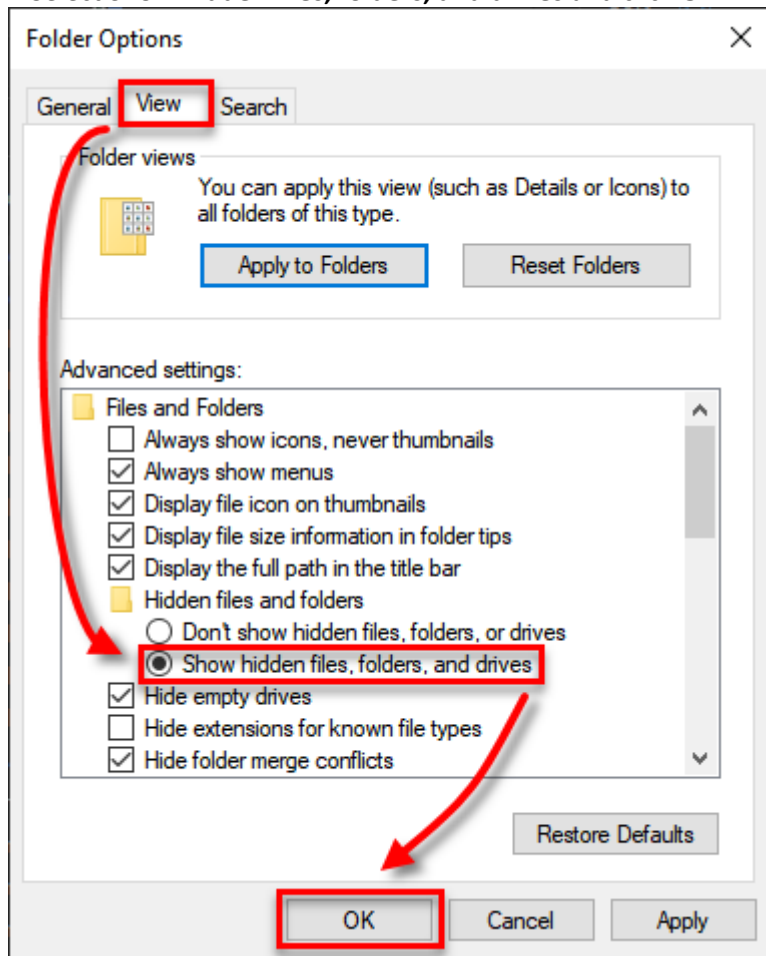
## Log files

Each ESET PROTECT component performs logging. ESET PROTECT components write information about specific events into log files. The location of log files varies depending on the component. The following is a list of log file locations:

## Windows

ESET PROTECT component	Log files location
ESET PROTECT Server	<i>C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\</i>
ESET Management Agent	<i>C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\</i> See also <a href="#">Agent connection troubleshooting</a> .
ESET PROTECT Web Console and Apache Tomcat	<i>C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs\</i> See also <a href="https://tomcat.apache.org/tomcat-9.0-doc/logging.html">https://tomcat.apache.org/tomcat-9.0-doc/logging.html</a>
Rogue Detection Sensor	<i>C:\ProgramData\ESET\Rogue Detection Sensor\Logs\</i>
ESET Bridge (HTTP Proxy)	See <a href="#">ESET Bridge Online Help</a> .

C:\ProgramData is hidden by default. To display the folder:  
 1.Navigate to **Start > Control Panel > Folder Options > View**.  
 2.Select **Show hidden files, folders, and drives** and click **OK**.



## Linux

ESET PROTECT component	Log files location
ESET PROTECT Server	<i>/var/log/eset/RemoteAdministrator/Server/ /var/log/eset/RemoteAdministrator/EraServerInstaller.log</i>
ESET Management Agent	<i>/var/log/eset/RemoteAdministrator/Agent/ /var/log/eset/RemoteAdministrator/EraAgentInstaller.log</i>
ESET Bridge (HTTP Proxy)	See <a href="#">ESET Bridge Online Help</a> .
ESET PROTECT Web Console and Apache Tomcat	<i>/var/log/tomcat/</i> See also <a href="https://tomcat.apache.org/tomcat-9.0-doc/logging.html">https://tomcat.apache.org/tomcat-9.0-doc/logging.html</a>
ESET RD Sensor	<i>/var/log/eset/RogueDetectionSensor/</i>

## ESET PROTECT Virtual Appliance

ESET PROTECT component	Log files location
ESET PROTECT VA configuration	<i>/opt/appliance/log/appliance-configuration-log.txt</i>
ESET PROTECT Server	<i>/var/log/eset/RemoteAdministrator/EraServerInstaller.log</i>
ESET Bridge (HTTP Proxy)	See <a href="#">ESET Bridge Online Help</a> .

## macOS

*/Library/Application Support/com.eset.remoteadministrator.agent/Logs/*

*/Users/%user%/Library/Logs/EraAgentInstaller.log*

## Diagnostic Tool

The diagnostic tool is a part of all ESET PROTECT components. It is used to collect and pack logs that can be used by technical support agents and developers to solve problems with application components.

### Diagnostic Tool location

#### Windows

Folder *C:\Program Files\ESET\RemoteAdministrator\[application]\Diagnostic.exe*.

#### Linux

In the following directory on the server: */opt/eset/RemoteAdministrator/[application]/*, there is a **Diagnostic[application]** executable (one word, for example, **DiagnosticServer**, **DiagnosticAgent**)

### Usage

#### Linux

Run the diagnostics executable in the terminal as root and follow the instructions displayed on your screen.

#### Windows

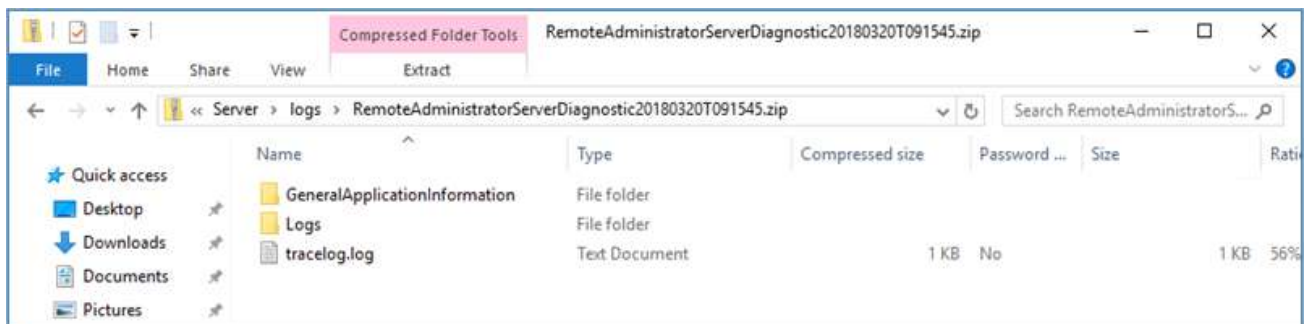
1. Run the tool using a Command Prompt.
2. Type the location of log files to be stored (in our example "logs") and press **Enter**.
3. Type the information you want to gather (in our example `1 trace status 3`). See **Actions** below for more information.

```

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. When you are finished, you can find the log files compressed in a .zip file in the "logs" directory in the Diagnostic Tool location.



## Actions

- **ActionEraLogs**—A logs folder is created where all logs are saved. To specify certain logs only, use a space to separate each log.
- **ActionGetDumps**—A new folder is created. A process dump file is generally created if a problem was detected. When a serious problem is detected, a dump file is created by system. To check it manually, go to the folder %temp% (in Windows) or folder /tmp/ (in Linux) and insert a dmp file.

**i** The component service (Agent, Server, RD Sensor) must be running.

- **ActionGeneralApplicationInformation**—The GeneralApplicationInformation folder is created and inside it the file *GeneralApplicationInformation.txt*. This file contains text information, including the application name and version of the currently installed application.
- **ActionConfiguration**—A configuration folder is created where file storage.lua is saved.

# Problems after upgrade/migration of ESET PROTECT Server

If you are unable to start the ESET PROTECT Server service because of a damaged installation and unknown log file error messages, perform a repair operation using the steps shown below:

 We recommend that you perform a [Database Server Backup](#) before you begin the repair operation.

1. Navigate to **Start > Control Panel > Programs and Features** and double-click **ESET PROTECT Server**.
2. Select **Repair** and click **Next**.
3. Reuse your existing database connection settings and click **Next**. Click **Yes** if you are prompted for **confirmation**. You can find the database connection information here:  
*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*
4. Select **Use Administrator password already stored in the database** and click **Next**.
5. Select **Keep currently existing certificates** and click **Next**.
6. Click **Repair**.
7. [Connect to Web Console](#) again and check if everything is OK.

## Other troubleshooting scenarios:

### ESET PROTECT Server is not running but there is a database backup

1. Restore your [database backup](#).
2. Verify the new machine uses the same IP address or hostname as your previous installation to ensure Agents will connect.
3. Repair ESET PROTECT Server and use the database you restored.

### ESET PROTECT Server is not running but you have the exported server certificate and Certification Authority from it

1. Verify the new machine uses the same IP address or hostname as your previous installation to ensure Agents will connect.
2. Repair ESET PROTECT Server using backup certificates (when repairing, select **Load certificates from file** and follow the instructions).

### ESET PROTECT Server is not running and you do not have a database backup or ESET PROTECT Server Certificate and Certification Authority:

1. Repair ESET PROTECT Server.

2. Repair ESET Management Agents using one of the following methods:

- Agent script installer
- Remote deployment (this will require you to disable the firewall on target machines)
- Manual Agent component installer

## MSI Logging

This is useful if you are not able to install an ESET PROTECT component on Windows properly, for example ESET Management Agent:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

## ESET PROTECT On-Prem API

ESET PROTECT On-Prem has two API types: REST API (since version 13.0) and ServerApi (legacy).

### ESET PROTECT On-Prem REST API

See [ESET PROTECT On-Prem REST API](#).

### ESET PROTECT On-Prem ServerApi

The ESET PROTECT On-Prem ServerApi (*ServerApi.dll*) is an application programming interface; a set of functions and tools for building custom software applications to meet your needs and specifics. Using the ServerApi, your application can provide a custom interface, functionality and operations you would normally perform via ESET PROTECT Web Console, such as managing ESET PROTECT On-Prem, generating and receiving reports, etc.

For more information and examples in C language and list of available JSON messages, please refer to [ESET PROTECT On-Prem 13.0 API](#).



This API is not an official document intended for general use. The API can help users in edge cases but should not be used as a standard way of using ESET PROTECT On-Prem. The declared set of API functions only covers part of the functionality. ESET does not provide support or guarantee backward compatibility for the ESET PROTECT On-Prem API.

## Legal documents

- [Terms of Use](#)
- [Privacy Policy](#)