ESET PROTECT

Installation, Upgrade and Migration Guide

Click here to display the Online help version of this document

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

REV. 1/21/2022

About help

This Installation guide was written to help with the installation and upgrade of ESET PROTECT and provides instructions for the process.

For consistency and to help prevent confusion, the terminology used throughout this guide is based on the ESET PROTECT parameter names. We also use a set of symbols to highlight topics of particular interest or significance.

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

This requires your attention and it should not be skipped. Usually, it provides non-critical but significant information.

Critical information you should treat with increased caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Please read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.

Example scenario that describes a user case relevant for the topic where it is included. Examples are used to explain more complicated topics.

Bold type	Names of interface items such as boxes and option buttons.
Italic type	Placeholders for information you provide. For example, filename or path means you type the actual path or a name of file.
`Courier New`	Code samples or commands.
Hyperlink	Provides quick and easy access to cross-referenced topics or external web location. Hyperlinks are highlighted in blue and may be underlined.
%ProgramFiles%	The Windows system directory which stores installed programs of Windows and others.

- Online Help is the primary source of help content. The latest version of Online Help will automatically be displayed when you have a working internet connection. The ESET PROTECT online help pages include four active tabs at the top navigation header: Installation/Upgrade, Administration, VA Deployment and SMB guide.
- Topics in this guide are divided into several chapters and sub-chapters. You can find relevant information by using the search field at the top.

Once you open a User Guide from the navigation bar at the top of the page, search will be limited to the contents of that guide. For example, if you open the Administrator guide, topics from the Installation/Upgrade and VA Deployment guides will not be included in search results.

- The ESET Knowledgebase contains answers to the most frequently asked questions, as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various types of problems.
- The 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 products.
- You can post your rating and/or provide a feedback on a particular topic in help: Click the **Was**

this information helpful? link underneath the help page.

Installation/Upgrade

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

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

ESET PROTECT 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 is designed to accommodate the growth of your infrastructure.

ESET PROTECT supports the new generation of ESET security products and is also compatible with the previous generation of products.

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

- Architecture of ESET PROTECT
- Installation processes
- Upgrade process
- License management
- Deployment processes and Agent deployment using GPO or SCCM
- First steps after installing ESET PROTECT
- Administration guide

New features in ESET PROTECT 9.0

One-click away from details

It's never been easier to quickly look at computer details or detection details and go over them. You just need to click the computer name in the **Computers** section, and a side panel with details will appear. Learn More We've also used the same approach for the **Detections** section when you click a detection type. Learn More

New overview Dashboard for EDTD

We've introduced a new Dashboard where you can find useful information and statistics related to ESET Dynamic Threat Defense. Learn More

Automatic Product Updates

To make your life easier, we're introducing auto-updates for our security products (Windows endpoint products for the time being) with out-of-the-box enablement in the upcoming ESET Endpoint Security/Antivirus v9, rolling out in November. With auto-updates, you can effortlessly keep ESET products in your network always up to date. Learn More

Management for brute-force attack protection

In Windows endpoint products v9, we bring a new security feature that protects devices against potential guessing of credentials and establishing a remote connection. You can easily configure this feature through a policy directly from the console and create exclusions from the **Detections** section when something is blocked but shouldn't be.

ESET Full Disk Encryption improvements

You can now save precious time by easily automating the updates of ESET Full Disk Encryption modules. We've also added the option to deploy an installer with a pre-defined password and keyboard map to start the encryption. Last but not least, we've improved the user interface to show currently installed ESET Full Disk Encryption modules.

Other improvements and usability changes

You can find more details in the changelog.

Architecture

ESET PROTECT is a new generation of a remote management system.

To perform a complete deployment of ESET security products, 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:

- Proxy

- RD Sensor
- Apache HTTP Proxy
- Mobile Device Connector

ESET PROTECT components use certificates to communicate with the ESET PROTECT Server. Read more about certificates in ESET PROTECT in our Knowledgebase article.

Infrastructure elements overview

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

Remote management of ESET security products (creation of policies, tasks, reports, etc.)	✔	X	X	X	X	X
Communication with the ESET PROTECT Server and managing ESET security product on the client device	X	✔	X	X	X	✔
Providing updates, license validation	X	X	X	X	✔	X
Caching and forwarding updates (detection engine, installers, modules)	X	X	✔	✔	X	X
Forwarding of network traffic between ESET Management Agent and ESET PROTECT Server	X	X	X	✔	X	X
Securing the client device	X	X	✔	X	X	X
Remote management of mobile devices	X	X	X	X	X	✔

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.

Web Console

The ESET PROTECT Web Console is a web-based user interface that allows you to manage ESET security solutions in your environment. It displays an overview of the status of clients

on your network and can be used to deploy ESET solutions 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 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.

HTTP Proxy

What is HTTP Proxy and how can it be useful?

HTTP Proxy is forwarding communication from Agents to ESET PROTECT Server in environments where Agent machines cannot reach the Server.

How does the Proxy work in ESET PROTECT?

ESET PROTECT 9 uses a customized version of Apache HTTP Proxy as the Proxy component. After a proper configuration, Apache HTTP Proxy can act as a Proxy for ESET Management Agents. The Proxy does not cache or open the communication; it only forwards it.

Can I use a Proxy other than the Apache HTTP Proxy?

Any proxy solution which fulfills the following conditions can be used with ESET Management Agent:

- can forward SSL communication
- supports HTTP CONNECT
- does not use a username and password

How is the new communication protocol different?

The ESET PROTECT Server communicates with ESET Management Agents via gRPC protocol. The communication uses TLS and HTTP2 so it can go through Proxy servers. There are also new self-recovery features and a persistent connection which improves overall communication performance.

What is the effect on performance?

Using HTTP Proxy has no significant impact on performance.

When should I use the Proxy?

We recommend that you use a Proxy if your infrastructure meets one or more of the following conditions:

- If your Agent machines cannot directly connect to the ESET PROTECT Server.
- If you have a remote location or branch office and want to use Proxy to handle communication:

  obetween ESET PROTECT Server and Proxy

  obetween Proxy and client computers in a remote location

How to set up the HTTP Proxy

To use the proxy, HTTP Proxy hostname must be set up in the Agent policy (**Advanced settings** □ **HTTP Proxy**). You can use different proxies for caching and forwarding; see the policy settings below:

- **Global Proxy** - you will use a single proxy solution for both caching downloads and for forwarding Agent communication.
- **Different Proxy Per Service** - you will use separate proxy solutions for caching and for forwarding communication.

What are other functions of Apache HTTP Proxy?

Apache HTTP Proxy

Apache HTTP Proxy is a proxy service that can be used to distribute updates to client computers.

To install Apache HTTP Proxy, read the instructions for Windows, Linux, or Virtual Appliance.

Apache HTTP Proxy functions

Caching of downloads and updates	Apache HTTP Proxy or other proxy solution
Caching of ESET Dynamic Threat Defense results	Only configured Apache HTTP Proxy
Replication ESET Management Agents' communication with ESET PROTECT Server	Apache HTTP Proxy or other proxy solution

Caching function

Apache HTTP Proxy downloads and caches:

- ESET module updates

- Installation packages from repository servers
- Product component updates

Cached data is distributed to endpoint clients on your network. Caching can significantly decrease internet traffic on your network.

In contrast to the Mirror Tool, which downloads all available data on the ESET update servers, Apache HTTP Proxy reduces the network load by only downloading the data requested by ESET PROTECT components or ESET endpoint products. If an endpoint client requests an update, Apache HTTP Proxy downloads it from the ESET update servers, saves the update to its cache directory and then serves it to the individual endpoint client. If another endpoint client requests the same update, Apache HTTP Proxy serves the download to the client directly from its cache, so there is no additional download from ESET update servers.

Caching for ESET Endpoint product

Caching settings of ESET Management Agent and Endpoint are not identical. ESET Management Agent can manage settings for ESET security products at client devices. You can set up proxy for ESET Endpoint Security:

- locally from GUI
- from ESET PROTECT Web Console, using a policy (the recommended way to manage client devices settings).

Caching results from ESET Dynamic Threat Defense

Apache HTTP Proxy can also cache results provided by ESET Dynamic Threat Defense. Caching requires specific configuration which is included in the Apache HTTP Proxy distributed by ESET. It is recommended to use caching with ESET Dynamic Threat Defense if possible. See the service's documentation for more details.

Using Apache as HTTP Proxy for Agent - Server communication

When correctly configured, Apache HTTP Proxy can be used to collect and forward data from ESET PROTECT components in a remote location. One proxy solution can be used for caching updates (Apache HTTP Proxy is recommended) and another proxy for Agent - Server communication. It is possible to use Apache HTTP Proxy for both functions at the same time, but it is not recommended for networks with more than 10,000 client machines per proxy machine. In enterprise environments (more than 1,000 managed computers), we recommend that you use a dedicated Apache HTTP Proxy server.

Read more about the Proxy function.

How to set up the HTTP Proxy

To use the proxy, HTTP Proxy hostname must be set up in the Agent policy (**Advanced settings** → **HTTP Proxy**). You can use different proxies for caching and forwarding; see the policy settings below:

- **Global Proxy** - you will use a single proxy solution for both caching downloads and for forwarding Agent communication.
- **Different Proxy Per Service** - you will use separate proxy solutions for caching and for forwarding communication.

Apache HTTP Proxy in the infrastructure

The following diagram illustrates a proxy server (Apache HTTP Proxy) that is being used to distribute ESET cloud traffic to all ESET PROTECT components and ESET endpoint products.

> You can use a proxy chain to add another proxy service to a remote location. Note that ESET PROTECT does not support proxy chaining when the proxies require authentication. You can use your own transparent web proxy solution, however that may require additional configuration beyond what is mentioned here.

> For offline detection engine updates, use the Mirror Tool (available for Windows and Linux) instead of Apache HTTP Proxy.

Agent

The ESET Management Agent is an essential part of ESET PROTECT. 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 stand-alone ESET Management Agent is included in the ESET PROTECT suite. It is simple, highly modular and lightweight service covering all communication between ESET PROTECT Server and any ESET product or operating system. Rather than communicate with the ESET PROTECT Server directly, ESET products 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 – it is possible to deploy Agent as a part of standard corporate installation.
- On-place security management – since 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.

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 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.

RD Sensor actively 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.

Mobile Device Connector

ESET PROTECT Mobile Device Connector is a component that allows for Mobile Device Management with ESET PROTECT, permitting you to manage mobile devices (Android and

iOS) and administer ESET Endpoint Security for Android.

View the image larger

We recommend that you deploy your MDM component on a host device separate from the one ESET PROTECT Server is hosted on.

The recommended hardware preconditions for approximately 80 managed mobile devices are:

Processor	4 cores, 2.5 GHz
RAM	4 GB (recommended)
HDD	100 GB

For more than 80 managed mobile devices, the hardware requirements are not much higher. The latency between sending the task from the ESET PROTECT and the execution of the task on the mobile device will increase proportionally to number of devices in your environment.

Follow the MDM installation instructions for Windows (All-in-one installer or component installation) or Linux.

The differences between Apache HTTP Proxy, Mirror Tool, and direct connectivity

ESET product communication involves detection engine and program module updates as well as the exchange of ESET LiveGrid® data (see the table below) and license information.

ESET PROTECT downloads the latest products for distribution to client computers from the repository. Once distributed, the product is ready to be deployed on the target machine.

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

ESET LiveGrid® Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order 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 product module updates. In general, an ESET security product downloads approximately 23.9 MB of 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, Apache HTTP Proxy or Mirror Tool (available for Windows and Linux).

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

ESET communication types

				1	2	
Agent Deployment (Push / Live Installers from repository)	One time	Approximately 50 MB per client	YES	YES3	NO	YES (GPO / SCCM, edited live installers)4
Endpoint Installation (Software Install from repository)	One time	Approximately 100 MB per client	YES	YES3	NO	YES (GPO / SCCM, installation by package URL)4
Detection engine module / Program Module Update	6+ times a day	23.9 MB per month5	YES	YES	YES	YES (Offline Mirror Tool & Custom HTTP Server)6
Update version file update.ver	~8 times a day	2.6 MB per month7	YES	NO	-	-
Activation / Licensing check	4 times a day	negligible	YES	NO	NO	YES (Offline files generated on ESET Business Account)8
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 Apache 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 newer detection engine updates and module updates will be downloaded. We recommended to install one client initially, and let it update, so the needed detection engine and program 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 product's 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 license files as a License Owner or Security Admin.

You cannot cache updates for version 4 and 5 products using Apache HTTP Proxy. To distribute updates for these products, use the Mirror Tool.

When to start using Apache HTTP Proxy

Based on our practical tests, we recommend that you deploy Apache 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 Apache HTTP Proxy is used)
- using Apache 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 Apache HTTP Proxy in a network of computers:

Direct connection to internet (MB/month)	375	900	1,250	2,500	12,500	25,000
Apache 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 product module updates, because it downloads all available Level and Nano updates upon 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 Apache HTTP Proxy and Mirror Tool is that Apache 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 particular product module is missing.

> Streamed updates are not available with Mirror Tool. We recommend to prefer update via 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 HTTP Proxy to cache update files, select this option.

In the same network of 1,000 computers we tested the Mirror Tool instead of Apache 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.

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

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

System requirements and sizing

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

Supported Operating Systems

The following sections describe ESET PROTECT component support for Windows, Linux, macOS and mobile operating system versions.

Windows

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

Windows Server 2008 R2 x64 SP1 with KB4474419 or KB4490628 installed		✔	✔	
Windows Server 2008 R2 CORE x64 with KB4474419 or KB4490628 installed		✔	✔	
Windows Storage Server 2008 R2 x64 with KB4474419 or KB4490628 installed		✔	✔	
Microsoft SBS 2011 Standard x64		✔	✔	
Microsoft SBS 2011 Essentials x64		✔	✔	
Windows Server 2012 x64	✔	✔	✔	✔
Windows Server 2012 CORE x64	✔	✔	✔	✔
Windows Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2012 R2 CORE x64	✔	✔	✔	✔
Windows Storage Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2016 x64	✔	✔	✔	✔

Windows Storage Server 2016 x64	✔	✔	✔	✔	
Windows Server 2019 x64	✔	✔	✔	✔	
Windows Server 2022 x64	✔	✔	✔	✔	

Windows 7 x86 SP1 with latest Windows updates (at least KB4474419 and KB4490628)		✔	✔	
Windows 7 x64 SP1 with latest Windows updates (at least KB4474419 and KB4490628)		✔	✔	
Windows 8 x86		✔	✔	
Windows 8 x64	✔*	✔	✔	✔*
Windows 8.1 x86		✔	✔	
Windows 8.1 x64	✔*	✔	✔	✔*
Windows 10 x86		✔	✔	
Windows 10 x64 (all official releases)	✔*	✔	✔	✔*
Windows 10 on ARM		✔		
Windows 11 x64	✔*	✔	✔	✔*

* Installing ESET PROTECT components on a desktop OS 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 installation or virtual appliance where applicable.

Older MS Windows systems:
• Always have the latest service pack installed, especially on older systems, such as Server 2008 and Windows 7.
• ESET PROTECT does not support the management of computers running Windows 7 (with no SP), Widows Vista, and Windows XP.
• Beginning March 24, 2020, ESET will no longer officially support or provide technical support for ESET PROTECT (Server and MDM) installed on the following Microsoft Windows operating systems: Windows 7, Windows Server 2008 (all versions).
We do not support illegal or pirated operating systems.

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.

You can run ESET PROTECT on a non-server OS without the need for ESXi. Install VMware Player on a desktop Operating System and deploy the ESET PROTECT Virtual Appliance.

Linux

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

Ubuntu 16.04.1 LTS x86 Desktop		✔	✔	
Ubuntu 16.04.1 LTS x86 Server		✔	✔	
Ubuntu 16.04.1 LTS x64 Desktop	✔	✔	✔	✔
Ubuntu 16.04.1 LTS x64 Server	✔	✔	✔	✔
Ubuntu 18.04.1 LTS x64 Desktop	✔	✔	✔	✔
Ubuntu 18.04.1 LTS x64 Server	✔	✔	✔	✔
Ubuntu 20.04 LTS x64	✔	✔	✔	✔
RHEL Server 7 x86		✔	✔	
RHEL Server 7 x64	✔	✔	✔	✔
RHEL Server 8 x64	✔*	✔		✔
CentOS 7 x64	✔	✔	✔	✔
SLED 15 x64	✔	✔	✔	✔
SLES 12 x64	✔	✔	✔	✔
SLES 15 x64	✔	✔	✔	✔
OpenSUSE Leap 15.2 x64	✔	✔	✔	✔
Debian 9 x64	✔	✔	✔	✔
Debian 10 x64	✔	✔	✔	✔
Debian 11 x64		✔	✔	
Oracle Linux 8		✔	✔	
Amazon Linux 2		✔	✔	

* Red Hat Entreprise Linux Server 8.x does not support generating of *.pdf* reports - see more details in ESET PROTECT known issues.

macOS

macOS 10.12 Sierra	✔
macOS 10.13 High Sierra	✔
macOS 10.14 Mojave	✔

macOS 10.15 Catalina	✔
macOS 11.0 Big Sur	✔
macOS 12.0 Monterey	✔

macOS is supported as a client only. The ESET Management Agent and ESET products for macOS can be installed on macOS. However, ESET PROTECT Server cannot be installed on macOS.

Mobile

Android 5.x+	✔			
Android 6.x+	✔			
Android 7.x+	✔	✔		
Android 8.x+	✔	✔		
Android 9.0	✔	✔		
Android 10.0	✔	✔		
Android 11	✔	✔		
Android 12	✔			

iOS 9.x+			✔	✔*
iOS 10.x+			✔	✔*
iOS 11.x+			✔	✔*
iOS 12.0.x			✔	✔*
iOS 13.x+			✔	✔
iOS 14.x+			✔	✔
iOS 15			✔	✔

iPadOS 13.x+			✔	✔
iPadOS 14.x+			✔	✔
iPadOS 15			✔	✔

* iOS DEP is only available in selected countries.

We recommend that you update the OS of your mobile device to the latest version to keep receiving important security patches.

Requirements for iOS 10.3 and later:

Since the release of iOS 10.3, a CA that is installed as part of the enrollment profile might not be trusted automatically. To resolve this issue, follow the steps below:
a)Use a certificate issued by certificate issuer trusted by Apple.
b)Install certificate trust manually prior to enrollment. This means that you will need to install the root CA manually on the mobile device prior to enrollment and enable full trust for the installed certificate.

Requirements for iOS 12:

Please review the requirements for iOS 10.3 and later.
- The connection must use **TLS 1.2 or greater**.
- The connection must use **AES-128** or **AES-256 symmetric cipher**. The negotiated TLS connection cipher suite must support **perfect forward secrecy (PFS)** through **Elliptic Curved Diffie-Hellman Ephemeral (ECDHE) key e✓change**, and must be one of the following:

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

- Be signed with **RSA key** with a length of **at least 2048 bits**. The certificate's hashing algorithm must be **SHA-2 with a digest length**, (sometimes called a "fingerprint") of at least 256 (that is, **SHA-256 or greater**). You can generate a certificate with these requirements in ESET PROTECT with Advanced Security turned on.
- Certificates must contain the **entire certificate chain including the root CA**. The Root CA included in the certificate is used to establish trust with devices and is installed as part of the MDM enrollment profile.

Requirements for iOS 13:

- Management of iOS 13 mobile devices require to meet new Apple communication certificate (MDM HTTPS) requirements. Certificates issued before July 1, 2019, must meet those criteria too.
- HTTPS certificate signed by ESMC CA does not meet these requirements.

> It is highly recommended not to upgrade your mobile devices to iOS 13 before you meet the Apple communication certificate requirements. Such action will lead to your devices stop connecting to ESET PROTECT MDM.

- If you've already upgraded without the proper certificate and your devices stopped connecting to ESET PROTECT MDM, you need to first, change your current HTTPS certificate used for communication with iOS devices to the certificate that meets the Apple communication certificate (MDM HTTPS) requirements and after that, re-enroll your iOS devices.
- If you've not upgraded to iOS 13, ensure that your current MDM HTTPS certificate used for communication with iOS devices meets the Apple communication certificate (MDM HTTPS) requirements. If yes, you can continue to upgrade your iOS devices to iOS 13. If it does not meet the requirements, change the current MDM HTTPS certificate to the HTTPS certificate that meets the Apple communication certificate (MDM HTTPS) requirements and then proceeds to upgrade your iOS devices to iOS 13.

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 OS (Citrix provisioning services), see the list of supported hypervisors.

ESET PROTECT supports:

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

Supported hypervisors

- Citrix XenServer
- Microsoft Hyper-V
- VMware vSphere
- VMware ESXi
- VMware Workstation
- VMware View
- Oracle VirtualBox

Supported hypervisor extensions

- Citrix VDI-in-a-box
- Citrix XenDesktop

Tools

(applies to both virtual and physical machines)

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

Hardware and infrastructure sizing

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

					1	2
Up to 1,000	4	2.1	4	Single		500
5,000	8	2.1	8			1,000
10,000 3	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

1 Single / Separate disk drive - We recommend installing the database on a separate drive for systems with over 10,000 clients.

2 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:

Up to 5,000 clients	diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat
Over 5,000 clients	diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat

3 See the example scenario for 10,000 clients environment.

Disk drive recommendations

The disk drive is the critical factor influencing the ESET PROTECT 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 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: 10x 1.2TB 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 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 performance. If you notice read/write latency goes over 20ms, 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 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.

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

8	2.1	64	High	High	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Normal	Low
2	2.1	16	Low	Low	Insufficient
2	2.1	8	Very low (not recommended)	Very low (not recommended)	Insufficient

Deployment recommendations

Best practices for deployment of ESET PROTECT

ESET PROTECT Server & Database Server on the same machine	✔	✔	✔	X	X	X
Use of MS SQL Express	✔	✔*	X	X	X	X
Use of MS 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
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 Enterprise Inspector.

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. Make sure to set the appropriate client connection interval. Make sure 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 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 products 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.

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. Make sure 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.


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 / CentOS: `/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

VMware	ESXi 6.7 Update 2 and later (VM version 15)
Hypervisor	VMware ESXi, 6.7.0
Logical Processors	112
Processor Type	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

> The test ran on dedicated machines
>
> The database and ESET PROTECT are running on separate virtual machines with identical hardware configurations.

Software used on virtual machines

ESET PROTECT:

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

Database:

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

ESET PROTECT 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

8	64	High
4	32	Normal
2	16	Low
2	8	Very low (not recommended)

Database

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.

The ESET PROTECT 9.0 All-in-one installer installs Microsoft SQL Server Express 2019 by default.

- If you use an older Windows edition (Server 2012 or SBS 2011), Microsoft SQL Server Express 2014 will be installed by default.
- The installer automatically generates a random password for database authentication (stored in *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Microsoft SQL Server Express has a 10 GB size limit for each relational database. We do not recommend using Microsoft SQL Server Express:
- In enterprise environments or large networks.
- If you want to use ESET PROTECT with ESET Enterprise Inspector.

Supported database servers and database connectors

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

ESET PROTECT does not support MariaDB. MariaDB is a default database in most current Linux environments and gets installed when you select to install MySQL.

Microsoft SQL Server	• Express and non-Express editions • 2014, 2016, 2017, 2019	• SQL Server • SQL Server Native Client 10.0 • ODBC Driver for SQL Server 11, 13, 17
MySQL	• 5.6* • 5.7 • 8.0	MySQL ODBC driver versions: • 5.1, 5.2 • 5.3.0-5.3.10 • 8.0.16, 8.0.17 • 8.0.27 (Windows only)

* MySQL 5.6 reached the End of Life in February 2021. We recommend that you upgrade your MySQL database server to version 5.7 and later.

The following MySQL ODBC driver versions are not supported:
- 5.3.11 and later 5.3.x
- 8.0.0-8.0.15
- 8.0.18 and later

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 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 a significantly higher number of 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 wish to manage more than 10,000 clients.

MS SQL Express	✔	(optional)	5,000	✔	
MS SQL Server	✔	✔	None	✔	
MySQL	✔	✔	10,000	✔	✔

Additional information

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 (for example, Windows SBS / Essentials). We recommend that you install ESET PROTECT on a different server or do not select the SQL Server Express component during installation (this requires you to 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.

• See the instructions to install and configure MySQL for Windows and MySQL for Linux to work properly with ESET PROTECT.

• MS SQL Server on Linux is not supported. However, you can connect the ESET PROTECT Server on Linux to MS SQL Server on Windows.

• If you install the ESET PROTECT Server and MS 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 MS SQL Server, not for MySQL.

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

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

Java

Apache Tomcat requires 64-bit Java/OpenJDK.

If you have multiple Java versions installed on your system, we recommend that you uninstall older 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.

Supported Web browsers, ESET security products and languages

The following Operating Systems are supported by ESET PROTECT:

- Windows, Linux and macOS

The ESET PROTECT Web Console can be run in the following web browsers:

Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

- For the best experience with the ESET PROTECT Web Console we recommend that you keep your web browsers updated.
- If you use Internet Explorer, ESET PROTECT Web Console will notify you that you are using an unsupported web browser.

Latest versions of ESET products manageable via ESET PROTECT 9.0

ESET Endpoint Security for Windows	7.x, 8.x, 9.x
ESET Endpoint Antivirus for Windows	7.x, 8.x, 9.x
ESET Endpoint Security for macOS	6.8+
ESET Endpoint Antivirus for macOS	6.8+
ESET Endpoint Security for Android	2.x
ESET Server Security for Windows	8.x
ESET File Security for Microsoft Windows Server	7.x

ESET File Security for Microsoft Azure	7.x
ESET Mail Security for Microsoft Exchange Server	7.x, 8.x
ESET Security for Microsoft SharePoint Server	7.x, 8.x
ESET Mail Security for IBM Domino Server	7.x, 8.x
ESET File Security for Linux	7.x, 8.x
ESET Server Security for Linux	8.1+
ESET Endpoint Antivirus for Linux	7.x, 8.x
ESET Dynamic Threat Defense	
ESET Enterprise Inspector Agent	1.5
ESET Full Disk Encryption for Windows	
ESET Full Disk Encryption for macOS	

Older versions of ESET products manageable via ESET PROTECT 9.0

ESET Endpoint Security for Windows	6.5+
ESET Endpoint Antivirus for Windows	6.5+
ESET File Security for Microsoft Windows Server	6.5
ESET File Security for Microsoft Azure	6.5
ESET Mail Security for Microsoft Exchange Server	6.5
ESET Mail Security for IBM Lotus Domino	6.5
ESET Security for Microsoft SharePoint Server	6.5
ESET Mail Security for Linux/FreeBSD*	4.5.x
ESET File Security for Linux/FreeBSD*	4.5.x
ESET Gateway Security for Linux/FreeBSD*	4.5.x

* You cannot manage this products using the ESET Management Agent 9. To manage the product, use ESET Management Agent 8.1 or older.

ESET security product versions earlier than those shown in the table above are not manageable using ESET PROTECT 9.
For more information about compatibility, visit the End of Life policy for ESET business products.

Products supporting activation via Subscription license

ESET Endpoint Antivirus/Security for Windows	7.0
ESET Endpoint Antivirus/Security for macOS	6.8.x
ESET Endpoint Security for Android	2.0.158
ESET Mobile Device Management for Apple iOS	7.0
ESET File Security for Microsoft Windows Server	7.0
ESET Mail Security for Microsoft Exchange	7.0

ESET File Security for Windows Server	7.0
ESET Mail Security for IBM Domino	7.0
ESET Security for Microsoft SharePoint Server	7.0
ESET File Security for Linux	7.0
ESET Endpoint Antivirus for Linux	7.0
ESET Server Security for Windows	8.0
ESET Server Security for Linux	8.1
ESET Dynamic Threat Defense	
ESET Enterprise Inspector (with ESET Endpoint for Windows 7.3 and later)	1.5

Supported languages

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 product is available in this language; Online Help is not available.

Network

It is essential that both ESET PROTECT Server and client computers managed by ESET PROTECT 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 Apache HTTP Proxy) to facilitate communication with your network and the Internet.

Computers managed by ESET PROTECT should be connected to the same LAN and should be in the same *Active Directory* domain as your ESET PROTECT Server. The ESET PROTECT Server must be visible by client computers. Additionally, client computers must be able to communicate with your ESET PROTECT Server to use remote deployment and the wake-up call feature.

ESET PROTECT 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 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 in each connection interval. Each connection generates traffic. See the table below for examples of traffic:

Client Task: Scan without cleaning	4 kB
Client Task: Modules update	4 kB
Client Task: SysInspector Log Request	300 kB
Policy: Antivirus - Maximum security	26 kB

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 Enterprise Inspector, the ESET Enterprise Inspector Agent 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 Apache HTTP Proxy. The diagram below shows the separated installation and the used ports:

The tables below list all possible network communication ports used when ESET PROTECT 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, other applications should not use any of the ports below.
Make sure to configure any firewall(s) within your network to allow communication via the ports listed below.

Client (ESET Management Agent) or Apache HTTP Proxy machine

TCP	2222	Communication between ESET Management Agents and ESET PROTECT Server
TCP	80	Connection to the ESET repository
MQTT	8883, 443	ESET Push Notification Service - Wake-Up calls between ESET PROTECT Server and ESET Management Agent, 443 is failover port.
TCP	3128	Communication with Apache HTTP Proxy
TCP	443	Communication with ESET Dynamic Threat Defense (Proxy only)

ESET Management Agent - ports used for remote deployment to a target computer with Windows OS

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)

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: • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

ESET PROTECT Server machine

TCP	2222	Communication between ESET Management Agent and ESET PROTECT Server
TCP	80	Connection to the ESET repository
MQTT	8883	ESET Push Notification Service - Wake-Up calls between ESET PROTECT Server and ESET Management Agent
TCP	2223	DNS resolving and MQTT fallback
TCP	3128	Communication with Apache HTTP Proxy
TCP	1433 (MS 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	Kerberos tickets (applies only to ESET PROTECT Virtual Appliance)

Rogue Detection (RD) Sensor

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

ESET PROTECT MDC machine

TCP	9977 9978	Internal communication between Mobile Device Connector and ESET Management Agent
TCP	9980	Mobile device enrollment
TCP	9981	Mobile device communication
TCP	2195	Sending notifications to Apple Push Notification service. (*gateway.push.apple.com*) up to ESMC version 7.2.11.1
TCP	2196	Apple Feedback service (*feedback.push.apple.com*) up to ESMC version 7.2.11.1
HTTPS	2197	• Apple push notification and feedback (*api.push.apple.com*) ESMC version 7.2.11.3 and later
TCP	2222	Communication (replication) between ESET Management Agent, MDC and ESET PROTECT Server
TCP	1433 (MS SQL) 3306 (MySQL)	Connection to an external database (only if the database is on another machine)

MDM managed device

TCP	9980	Mobile device enrollment
TCP	9981	Mobile device communication
TCP	5223	External communication with Apple Push Notification service (iOS)
TCP	443	• Fallback on Wi-Fi only, when devices can't reach APNs on port 5223. (iOS) • Android Device connection to GCM server. • Connection to the ESET licensing portal. • ESET LiveGrid® (Android) (Inbound: *https://i1.c.eset.com* ; Outbound: *https://i3.c.eset.com*) • Anonymous statistical information to ESET Research Lab (Android) (*https://ts.eset.com*) • Apps categorization installed on the device. Used for Application Control when blocking of some app categories was defined. (Android) (*https://play.eset.com*) • To send a support request using the Support Request function (Android) (*https://suppreq.eset.eu*)
TCP	5228 5229 5230	Sending notifications to Google Cloud Messaging (Android)* Sending notifications to Firebase Cloud Messaging (Android)*
TCP	80	• Modules update (Android) (*http://update.eset.com*) • Used only in the Web version. Info about the latest app version update and download of a new version. (Android) (*http://go.eset.eu*)

* The GCM (Google Cloud Messaging) service is deprecated and was removed as of April 11, 2019. It was replaced by FCM (Firebase Cloud Messaging). MDM v7 replaced the GCM service with the FCM service by this date, at which point you only need to allow communication for the FCM service.

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

Installation process

> The Installation guide covers many ways to install ESET PROTECT and is generally intended for enterprise customers. Please refer to the guide for small and medium-sized businesses if you want to install ESET PROTECT on a Windows platform to manage up to 250 Windows ESET endpoint products.
> For instructions to upgrade your existing ESET PROTECT 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 All-in-one installer package for Windows in zip format.

• 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 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.

Additional methods of installation:

• Installation on Microsoft Azure

• Step-by-step installation instructions for Linux

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

To decide what kind of ESET PROTECT 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 in cloud.

• Select an All-in-one installer if you are an SMB customer.

See also Hardware and infrastructure sizing.

All-in-One on Windows Server	✔	✔	✔			✔	✔		✔	✔	✔	✔
All-in-One on Windows Desktop	✔		✔		✔					✔	✔	✔
Virtual Appliance	✔		✔					✔		✔	✔	✔
Microsoft Azure VM	✔			✔					✔		✔	
Component Linux		✔	✔			✔	✔		✔	✔	✔	✔
Component Windows		✔	✔			✔	✔		✔	✔	✔	✔

All-in-one installation on Windows

You can install ESET PROTECT in a few different ways. Select the type of installation that best suits your needs and environment. The simplest method is to use the ESET PROTECT All-in-one installer. This method allows you to install ESET PROTECT and its components on a single machine.

The component installation allows you to customize the installation and install each ESET PROTECT component on a separate computer, provided that it meets system requirements.

You can install ESET PROTECT using:

• All-in-one package installation of ESET PROTECT Server, Apache HTTP Proxy or Mobile Device

Connector

- Stand-alone installers for ESET PROTECT components (component installation)

Custom installation scenarios include:

- Installation with Custom certificates
- Installation on a Failover Cluster

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 components:

Core components

- ESET PROTECT Server
- ESET PROTECT Web Console - You can install the ESET PROTECT Web Console on a different computer than the computer running the ESET PROTECT Server.
- ESET Management Agent (must be installed on client computers, optional on ESET PROTECT Server)

Optional components

- RD Sensor
- Mobile Device Connector
- Apache HTTP Proxy
- Mirror Tool

For instructions to upgrade ESMC to the latest ESET PROTECT 9.0, see our upgrade procedures.

Install the ESET PROTECT Server

The ESET PROTECT All-in-one installer is available for Windows operating systems only. The All-in-one installer allows you to install all ESET PROTECT components using the ESET PROTECT installation Wizard.

1. Open the installation package. On the Welcome screen, use the **Language** drop-down menu to adjust the language settings. Click **Next** to proceed.

2. Select **Install** and click **Next**.

3. Deselect the check box next to **Participate in product improvement program** if you do not agree to send crash reports and anonymous telemetry data to ESET (OS version and type, ESET product version and other product-specific information). If the check box is left selected, telemetry data and crash reports will be sent to ESET. After accepting the EULA, click **Next**.

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

Microsoft SQL Server Express

- The ESET PROTECT 9.0 All-in-one installer installs Microsoft SQL Server Express 2019 by default.
  - If you use an older Windows edition (Server 2012 or SBS 2011), Microsoft SQL Server Express 2014 will be installed by default.
  - The installer automatically generates a random password for database authentication (stored in *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> Microsoft SQL Server Express has a 10 GB size limit for each relational database. We do not recommend using Microsoft SQL Server Express:
> - In enterprise environments or large networks.
> - If you want to use ESET PROTECT with ESET Enterprise Inspector.

- If you already have another 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 (for example, Windows SBS / Essentials). We recommend that you install ESET PROTECT on a different server or do not select the SQL Server Express component during installation (this requires you to 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).

Apache HTTP Proxy

> The **Apache HTTP 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.

- Using HTTP Proxy can save much bandwidth on data downloaded from the Internet and improve download speeds for product updates. We recommend selecting the check box next to **Apache HTTP Proxy** if you manage more than 37 computers from ESET PROTECT. You can also choose to install Apache HTTP Proxy later.
- For more information, see What is Apache HTTP Proxy? and The differences between Apache HTTP Proxy, Mirror Tool, and direct connectivity.
- Select **Apache HTTP Proxy** to install Apache HTTP Proxy, create and apply policies (named **HTTP Proxy Usage**, applied on the group **All**) for the following products:
  - ESET Endpoint for Windows
  - ESET Endpoint for macOS (OS X) and Linux
  - ESET Management Agent
  - ESET File Security for Windows Server (6+)
  - ESET Server Security for Windows (8+)
  - ESET Shared Local Cache

  The policy enables HTTP Proxy for affected products. 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 products.

5. If you have selected **Add custom HTTPS certificate for Webconsole**, click **Browse** and select a valid Certificate (*.pfx* or .p12 file) and type its **Passphrase** (or 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.

6. If errors are found during the prerequisites check, address them accordingly. Make sure your system meets all prerequisites.

.NET v4 is not installed

Install .NET Framework

No Java found / Java (64-bit) detected

If you have multiple Java versions installed on your system, we recommend that you uninstall older 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.

There is only 32 MB free on a system disk

- The installer may display this notification if your system does not have enough disk space for ESET PROTECT to install.
- You must have at least 4,400 MB of free disk space to install ESET PROTECT and all its components.

ESET Remote Administrator 5.x or older is installed on the machine

The direct upgrade is not supported - see Migration from ERA 5.x or Upgrade from ERA 6.x.

7. When the prerequisites check is complete and your environment meets all requirements, the installation will begin. Be aware that installation can take over an hour, depending on your system and network configuration.

> When the installation is in progress, the ESET PROTECT installation Wizard is unresponsive.

8. If you chose to install **Microsoft SQL Server Express** in step 4, the installer will perform a database connection check. If you have an existing database server, the installer will prompt you

to enter your database connection details:

Configure the connection to SQL/MySQL Server

Enter your **Database name**, **Hostname**, **Port** number (you can find this information in Microsoft SQL Server Configuration Manager), and **Database account** details (**Username** and **Password**) into the appropriate fields and then click **Next**. The installer will verify the database connection. If you have an existing database from a previous ESMC/ESET PROTECT installation on your database server, it will be detected. You can choose to **Use the existing database and apply upgrade** or **Remove existing database and install a new version**.

Use Named Instance - If you are using an MS 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\ESMC7SQL*). For 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 MS SQL database installed in a Failover Cluster, enter the cluster name in the **Hostname** field.

> There are two options when entering **Database account** information. You can use a **dedicated database user account** with access to the ESET PROTECT database only, or you can use an **SA account** (MS SQL) or **root account** (MySQL). If you decide to use a dedicated user account, you need to create an account with specific privileges. For details, see the Dedicated database user account. If you do not intend to use a dedicated user account, enter your administrator account (SA or root).

If you entered 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**, you must select **Create new user** (if you have not already created one) or **Use existing user** (if you have a dedicated database user account).

9. The installer will prompt you to enter a password for the Web Console Administrator account. This password is important – you will use it to log into the ESET PROTECT Web Console. Click **Next**.

10. Leave the fields as they are or type in your corporate information to appear in the details of the ESET Management Agent and the ESET PROTECT Server certificates. If you choose to enter a password in the **Authority password** field, be sure to remember it. Click **Next**.

11. Enter the valid **License Key** (included in the new purchase email you received from ESET) and click **Next**. If you use legacy license credentials (Username and Password), convert the credentials to a License Key. Alternatively, you can choose to **Activate later** (see the Activation chapter for additional instructions).

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. Make sure to select the check box **Automatically start the WinPcap driver at boot time**.

14. When the installation is complete, "ESET PROTECT components were installed successfully" will be displayed in addition to your ESET PROTECT Web Console URL address. Click the URL 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.

Install ESET PROTECT Mobile Device Connector (Standalone)

To install Mobile Device Connector as a standalone tool, on a different computer than ESET PROTECT Server, complete following steps.

Mobile Device Connector must be accessible from the Internet so that mobile devices can be managed at all times regardless of their location.

Take into account that a mobile device communicates with Mobile Device Connector which inevitably affects usage of mobile data. This applies especially to roaming.

Follow the steps below to install Mobile Device Connector on Windows:

1. Please read the prerequisites first and make sure all are met.

2. Double-click the installation package to open it, select **Install** and click **Next**.

3. Deselect the check box next to **Participate in product improvement program** if you do not agree to send crash reports and anonymous telemetry data to ESET (OS version and type, ESET product version and other product-specific information). If the check box is left selected, telemetry data and crash reports will be sent to ESET.

4. After accepting the EULA, click **Next**.

5. Select only the check box next to **Mobile Device Connector (Standalone)**. ESET PROTECT Mobile Device Connector requires a **database** for operation. Select **Microsoft SQL Server Express** if you want to install the database, or leave the check box empty. If you would like to connect to an existing database, you will have the option to do so during installation. Click **Install** to proceed with the installation.

6. If you installed the database as part of this installation in step 5, the database will now be

installed automatically and you can skip to step 8. If chose not to install a database in step 5, you will now be prompted to connect the MDM component to your existing database.

> You can use the same database server you are using for the ESET PROTECT database, but we recommend that you use a different DB server if you are planning to enroll more than 80 mobile devices.

7. The installer must connect to an existing database that will be used by Mobile Device Connector. Specify the following connection details:

- **Database**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication
- **ODBC Driver**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/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
- **Database name**: We recommend that you use the pre-defined name or change it if required.
- **Hostname**: hostname or the IP address of your database server
- **Port**: used for connection to the database server
- Database admin account **Username/Password**
- **Use Named Instance** - If you are using an MS 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\ESMC7SQL*). For 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 MS SQL database installed in a Failover Cluster, enter the cluster name in the **Hostname** field.

8. If the connection was successful, you will be prompted to verify that you want to use the provided user as a database user for ESET PROTECT MDM.

9. After the new database is successfully installed, or the installer successfully connected to the existing database, you can proceed with the MDM Installation. Specify your **MDM hostname**: this is the public domain or public IP address of your MDM server as it is reachable by mobile devices from the Internet.

MDM hostname must be entered in the same form it appears in your **HTTPS Server certificate**, otherwise the iOS mobile device will refuse to install the MDM Profile. For example, if there is an IP address specified in the HTTPS certificate, type in this IP address into the **MDM hostname** field. If an FQDN is specified (for example, `mdm.mycompany.com`) in the HTTPS certificate, enter this FQDN in the **MDM hostname** field. Also, if a wildcard * is used (for example, `*.mycompany.com`) in the HTTPS certificate, you can use `mdm.mycompany.com` in the **MDM hostname** field.

> Be very careful what you fill in the **MDM Hostname** filed in this step of installation. If the information is incorrect, or in a wrong form, the MDM Connector will not work properly and the only way to fix it will be re-installation of the component.

10. In the next step, verify the connection to the database by clicking **Next**.

11. Connect the MDM Connector to the ESET PROTECT Server. Fill in the **Server host** and **Server port** required for connection to the ESET PROTECT Server and select either **Server Assisted installation** or **Offline Installation** to proceed:

- **Server assisted installation** - Provide ESET PROTECT Web Console administrator credentials and the installer will download the required certificates automatically. Also check the permissions required for server-assisted installation.

  1.Enter your **Server host** - name or IP address of your ESET PROTECT Server and **Web Console port** (leave default port 2223 if you are not using custom port). Also, provide Web Console administrator account credentials - **Username/Password**.

  2.When asked to Accept the Certificate, click **Yes**. Continue to step 11.

- **Offline installation** - Provide a Proxy certificate and Certification Authority which can be exported from ESET PROTECT. Alternatively, you can use your custom certificate and appropriate Certification Authority.

  1.Click **Browse** next to the Peer certificate and navigate to the location of your **Peer certificate** location (this is the Proxy certificate you have exported from ESET PROTECT). Leave the **Certificate password** text field blank as this certificate does not require a password.

  2.Repeat the procedure for Certificate Authority and continue to step 11.

> If you are using custom certificates with ESET PROTECT (instead of the default ones that were automatically generated during ESET PROTECT installation), these should be used when you are prompted to supply a Proxy certificate.

12. Specify the destination folder for Mobile Device Connector (we recommend using the default), click **Next** → **Install**.

After the MDM installation is finished, you will be prompted for an Agent installation. Click **Next** to start the installation and accept the EULA if you agree with it and follow these steps:

1. Enter 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).

> Make sure the **Server host** matches at least one of the values (ideally be FQDN) defined in **Host** field of the **Server certificate**. Otherwise you will get an error saying "Received server certificate is not valid". The only exception is when there is a wildcard (*) in Server certificate Host field, which means it will work with any **Server host**.

2. If you are using proxy, select the check box **Use Proxy**. When selected, the installer will continue with **offline installation**.

This proxy setting is only 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**: enter 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.

3. Select one of the following installation options and follow the steps from the appropriate section below:

Server assisted installation - You will need to provide ESET PROTECT Web Console administrator credentials (installer will download the required certificates automatically).

Offline installation - You will need to provide an Agent certificate and a Certification Authority which can be both exported from ESET PROTECT. Alternatively, you can use your custom certificate.

- To continue **server-assisted Agent installation** follow these steps:

1. Enter the hostname or IP address of your ESET PROTECT Web Console (same as ESET PROTECT Server) in the **Server host** field. Leave **Web Console port** set to the default port 2223 if you are not using custom port. Also, enter your Web Console account credentials in the **Username and Password fields**. To log in as a domain user, select the check box next to **Log into domain**.

• Make sure the **Server host** matches at least one the values (ideally be FQDN) defined in **Host** field of the **Server certificate**. Otherwise you will get an error saying "Received server certificate is not valid". The only exception is if there is a wildcard (*) in Server certificate Host field, which means it will work with any **Server host**.
• You cannot use a user with two-factor authentication for server-assisted installations.

2. Click **Yes** when asked if you want to accept the certificate.

3. Select **Do not create computer (computer will be created automatically during the first connection)** or **Choose custom static group**. If you click **Choose custom static group** you will be able to select from a list of existing Static groups in ESET PROTECT. The computer will be added to the group you have selected.

4. Specify a destination folder for the ESET Management Agent (we recommend that you use the default location), click **Next** and then click **Install**.

- To continue **offline Agent installation** follow these steps:

1. If you selected **Use Proxy** in the previous step, provide the **Proxy hostname**, **Proxy port** (the default port is 3128),**Username** and **Password** and click **Next**.

2. Click **Browse** and navigate to the location of your Peer certificate (this is the Agent certificate you exported from ESET PROTECT). 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.

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

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

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

After the installation is complete, check to see if Mobile Device Connector is running correctly by opening *https://your-mdm-hostname:enrollment-port* (for example *https://mdm.company.com:9980*) in your web browser or from a mobile device. If the installation was successful, you will see following message:

You can now activate MDM from ESET PROTECT.

Installation on Microsoft Azure

For users who prefer to use a managed solution, instead of maintaining ESET PROTECT on-premise, ESET offers ESET PROTECT on Microsoft Azure cloud platform.

See our Knowledgebase content for more information:

- Getting started with ESET PROTECT - Azure
- ESET PROTECT VM for Microsoft Azure—FAQ
- You can install ESET PROTECT 9.0 in Azure by following the steps in this Knowledgebase article and using ESET PROTECT 9.0 All-in-one installer. Alternatively, you can install ESMC 7.x in Azure and then upgrade it to ESET PROTECT.

Component 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 components:

Core components

- ESET PROTECT Server

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

• ESET Management Agent (must be installed on client computers, optional on ESET PROTECT Server)

Optional components

• RD Sensor

• Mobile Device Connector

• Apache HTTP Proxy

• Mirror Tool

For instructions to upgrade ESMC to the latest ESET PROTECT 9.0, see our upgrade procedures.

If you want to run the installation in your local language, you need to start the MSI installer of a particular 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:

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 product is available in this language; Online Help is not available.

Server installation

To install the ESET PROTECT Server component on Windows:

1. Visit the ESET PROTECT download section to download a standalone installer for this ESET PROTECT component (*server_x64.msi*).

2. Make sure all prerequisites are met.

3. Run the ESET PROTECT Server installer and accept the EULA if you agree.

4. Deselect the check box next to **Participate in product improvement program** if you do not agree to send crash reports and anonymous telemetry data to ESET (OS version and type, ESET product version and other product-specific information). If the check box is left selected, telemetry data and crash reports will be sent to ESET.

5. 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.

6. 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** - Provide domain user credentials: `DOMAIN\USERNAME` and password.

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

- **Database**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication
- **ODBC Driver**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/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
- **Database name**: We recommend that you use the pre-defined name or change it if required.

• **Hostname**: hostname or the IP address of your database server

• **Port**: used for connection to the database server

• Database admin account **Username/Password**

• **Use Named Instance** - If you are using an MS 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\ESMC7SQL*). For 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 MS SQL database installed in a Failover Cluster, enter the cluster name in the **Hostname** field.

ESET PROTECT Server stores large data blobs in the database, therefore it is necessary to configure MySQL to accept large packets for ESET PROTECT to run properly.

This step will verify your connection to the database. If the connection is good, proceed to the next step.

8. Select a user for ESET PROTECT that has access to the database. You can use an existing user, or setup can create a user for you.

9. Enter a password for **Web Console** access.

10. ESET PROTECT 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.

11. 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.

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`.

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

12. 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**.

13. Enter a valid License Key or choose **Activate later**.

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

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

When you have completed the installation of the ESET PROTECT Server, you can also install ESET Management Agent on the same machine (optional). This way you will be able to manage the server itself the same way you would mange a client computer.

Server prerequisites - Windows

You must meet the following prerequisites to install the ESET PROTECT Server on Windows:

- You must have a valid license key.
- 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. Read our Knowledgebase article to set up your database and database user for both MS SQL and MySQL.
- ESET PROTECT Web Console installed to manage the ESET PROTECT Server.
- MS SQL Server Express installation requires Microsoft .NET Framework 4. You can install it using the **Add Roles and Features Wizard**:

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**.

• 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 (for example, Windows SBS / Essentials). We recommend that you install ESET PROTECT on a different server or do not select the SQL Server Express component during installation (this requires you to use your existing SQL or MySQL Server to run the ESET PROTECT database).

MySQL Server installation and configuration

Installation

Make sure 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. Make sure 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.

5. Click **Next**. In **High Availability**, select **Standalone MySQL Server / Classic MySQL Replication** and click **Next**.

6. In **Type and Networking**, select **Server Computer** from the **Config Type** drop-down menu and click **Next**.

7. In the **Authentication Method**, select the recommended option **Use Strong Password Encryption for Authentication** and click **Next**.

8. In **Accounts and Roles**, type your **MySQL Root Password** twice. We recommend that you also create a dedicated database user account.

9. In **Windows Service**, keep the pre-selected values and click **Next**.

10. Click **Execute** and wait until MySQL Server installation completes. Click **Finish**, **Next** and **Finish** to close the installation window.

Configuration

1. Open the following file in a text editor:

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

2. Find and edit or append the following configuration into the `[mysqld]` section of the *my.ini* file:

```
max_allowed_packet=33M
```

To determine your MySQL version, run the command: `mysql --version`

- For the supported versions MySQL 8.x, you must set the following variable:
  - `log_bin_trust_function_creators=1`
  - Alternatively, you can disable binary logging: `log_bin=0`
- For the supported versions of MySQL 8.x, 5.7 and 5.6.22 (and later 5.6.x):
  - `innodb_log_file_size*innodb_log_files_in_group` needs to be set to at least **200 MB** (* denotes multiplication, the product of the two parameters must be > 200 MB. The minimum value for `innodb_log_files_in_group` is 2 and maximum value is 100, the value also has to be integer).
    For example:
    `innodb_log_file_size=100M`
    `innodb_log_files_in_group=2`
- For MySQL 5.6.20 and 5.6.21:
  - `innodb_log_file_size` needs to be set to at least **200 MB** (for example, `innodb_log_file_size=200M`), but not more than **3000 MB**.

3. Save and close the *my.ini* file.

4. Open the Command Prompt and enter 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
```

5. Enter the following command in Command Prompt to check whether the MySQL server is running:

```
sc query mysql80
```

Dedicated database user account

If you do not wish to use an **SA account** (MS 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 installation. Also, you will need to create an empty database that will be accessed by ESET PROTECT 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 http://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

You can find detailed guide how to set up your database and user account for both MS SQL and MySQL in our Knowledgebase article.

Agent installation

Available methods

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

GUI based installation from the *.msi* installer	• This chapter • KB	• The **standard** installation method. • This method can be executed as server-assisted or offline installation. • Use this method when installing Agent on ESET PROTECT Server machine.
ESET Remote Deployment Tool	• Online Help	• Recommended for mass-deployment over local network. • Can be used to deploy All-in-one installer (Agent + ESET security product)
All-in-one Agent installer	• Create an All-in-one Agent installer • KB	• The installer can include also a security product and embedded policy. • The size of the installer is several hundreds of MBs.
Agent live installer	• Create a Agent live installer • KB	• The installer is an executable script. It has a small size but it needs access to location of *.msi* installer. • The script can be edited to use local installer and HTTP Proxy.
SCCM and GPO deployment	• SCCM • GPO • KB	• Advanced method of remote mass-deployment. • Using a small *.ini* file.
Server task - Agent Deployment	• Online Help • KB	• An alternative to SCCM and GPO. • It is not viable through HTTP Proxy. • Executed by ESET PROTECT Server from the ESET PROTECT Web Console.

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

To install the ESET Management Agent component locally on Windows, follow these steps:

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 accept the EULA if you agree with it.

3. Deselect the check box next to **Participate in product improvement program** if you do not agree to send crash reports and anonymous telemetry data to ESET (OS version and type, ESET product version and other product-specific information). If the check box is left selected, telemetry data and crash reports will be sent to ESET.

4. Enter 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).

Make sure 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**. When selected, the installer will continue with offline installation.

This proxy setting is only 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**: enter 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. Select one of the following installation options and follow the steps from the appropriate section below:

- Server assisted installation - You will need to provide ESET PROTECT Web Console administrator credentials. The installer will download the required certificates automatically.

You cannot use a user with two-factor authentication for server-assisted installations.

• Offline installation - You will need to provide an Agent certificate and a Certification Authority. Both can be exported from ESET PROTECT. Alternatively, you can use your custom certificate.

Command line installation

MSI installer can be run locally or remotely. Download the ESET Management Agent from the ESET website.

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 (exported from ESET PROTECT Web Console).
P_CERT_AUTH_PATH=	Path to the Certification Authority in Base64 format in *.txt* file (exported from ESET PROTECT Web Console).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	**YES**; 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 (exported from ESET PROTECT Web Console).
P_CERT_AUTH_CONTENT=	Certification Authority string in Base64 format (exported from ESET PROTECT Web Console).
P_ENABLE_TELEMETRY=	**0** - disabled (default option); **1** - enabled. Sending of crash reports and telemetry data to ESET (optional parameter).
P_INSTALL_MODE_EULA_ONLY=	**1**; Use this parameter for semi-silent ESET Management Agent installation. You can see Agent installation window and you are prompted to accept the EULA 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=	**1**; 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=CJfXtf1kZqlZKAl9P48HymBHa3CkW 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
```

Server-assisted Agent installation

To continue **server-assisted Agent installation** follow these steps:

1. Enter the hostname or IP address of your ESET PROTECT Web Console (same as ESET PROTECT Server) in the **Server host** field. Leave **Web Console port** set to the default port 2223 if you are not using custom port. Also, enter your Web Console account credentials in the **Username and Password fields**. To log in as a domain user, select the check box next to **Log into domain**.

- Make sure the **Server host** matches at least one the values (ideally be FQDN) defined in **Host** field of the **Server certificate**. Otherwise you will get an error saying "Received server certificate is not valid". The only exception is if there is a wildcard (*) in Server certificate Host field, which means it will work with any **Server host**.
- You cannot use a user with two-factor authentication for server-assisted installations.

2. Click **Yes** when asked if you want to accept the certificate.

3. Select **Do not create computer (computer will be created automatically during the first connection)** or **Choose custom static group**. If you click **Choose custom static group** you will be able to select from a list of existing Static groups in ESET PROTECT. The computer will be added to the group you have selected.

4. Specify a destination folder for the ESET Management Agent (we recommend that you use the default location), click **Next** and then click **Install**.

Offline Agent installation

To continue **offline Agent installation** follow these steps:

1. If you selected **Use Proxy** in the previous step, provide the **Proxy hostname**, **Proxy port** (the default port is 3128),**Username** and **Password** and click **Next**.

2. Click **Browse** and navigate to the location of your Peer certificate (this is the Agent certificate you exported from ESET PROTECT). 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.

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

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

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

ESET Remote Deployment Tool

The ESET Remote Deployment Tool is a convenient way to distribute the installer package created by ESET PROTECT to deploy ESET Management Agent and ESET security products remotely on computers over a network.

The ESET Remote Deployment Tool is available for free on the ESET website as a standalone ESET PROTECT Component. The deployment tool is meant mainly for deployment on small to medium networks and is executed under admin privileges.

> 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

You can install ESET PROTECT Web Console on Windows in two ways:

- Using the All-in-one installer is recommended
- Advanced users can perform a manual installation

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

Install Web Console using the All-in-one installer

To install the ESET PROTECT Web Console component on Windows using the All-in-one installer:

1. Verify the following prerequisites are met:

- 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 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 you have multiple Java versions installed on your system, we recommend that you uninstall older 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.

2. Download the ESET PROTECT All-in-one installer from the ESET website and unzip the downloaded file.

3. If you want to install the latest version of Apache Tomcat and the All-in-one installer contains an older 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.

4. To launch the All-in-one installer, double-click the *Setup.exe* file and click **Next** in the **Welcome** screen.

5. Select **Install** and click **Next**.

6. After accepting the EULA, click **Next**.

7. 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** and select a valid Certificate (*.pfx* or .p12 file) and type its **Passphrase** (or 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.

8. 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.

9. 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**.

10. 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*

See also the additional Web Console configuration for enterprise solutions or low-performance systems.

Install Web Console manually

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

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

1. Make sure the following prerequisites are met:

• 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 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 you have multiple Java versions installed on your system, we recommend that you uninstall older 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)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.

a)Run the installer.

b)During the installation, select the path to Java (parent folder of Java *bin* and *lib* folders) and select the **Run Apache Tomcat** check box.

c)After the installation, make sure that the Apache Tomcat service is running and its startup type is set to **Automatic** (in **services.msc**).

2. Visit the ESET PROTECT download section to download a standalone installer for this ESET PROTECT component (Web Console file *era.war*).

3. Copy *era.war* to the Apache Tomcat web applications folder:

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

4. 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.

5. 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:
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**.

6. 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*

7. 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 also the additional Web Console configuration for enterprise solutions or low-performance systems.

HTTP Proxy installation

About HTTP Proxy

The HTTP Proxy forwards encrypted communication between ESET Management Agent and ESET PROTECT Server. By default, ESET PROTECT uses Apache HTTP Proxy as the HTTP Proxy.

Use the HTTP Proxy only if your ESET Management Agents does not have network visibility to ESET PROTECT Server. HTTP Proxy does not aggregate the communication or lower the network traffic.

It is recommended to have the ESET Management Agent on the machine with HTTP Proxy, but it is not necessary. ESET Management Agent cannot manage (configure) HTTP Proxy

application.

- HTTP Proxy architecture
- Apache HTTP Proxy architecture
- Advanced scenarios for HTTP Proxy

Before the installation

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.

Installation and configuration

You can install Apache HTTP Proxy from the separate installer or from the All-in-one ESET PROTECT installer.

- Installing from All-in-one installer requires download of the whole package, but it is more simple. Run the downloaded installer and select only the **Apache HTTP Proxy** from the installer selector. After the Apache is installed, it needs to be configured.

- Installing from the standalone installer is more advanced, however the download size is only a few MBs. See the installation and configuration instructions.

Configure the HTTP Proxy for a high number of clients

If you use 64-bit Apache HTTP Proxy, you can increase the thread limit for your Apache HTTP Proxy. Edit the configuration file *httpd.conf*, inside your Apache HTTP Proxy folder. Find the following settings in the file and update the values to match your number of clients.

Substitute the example value of `5000` with your number. The maximum value is `32000`.

```
ThreadLimit 5000

ThreadsPerChild 5000
```

Do not change the rest of the file.

RD Sensor installation

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.

To install the RD Sensor component on Windows, follow these steps:

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. Make sure all prerequisites are met.

3. Double-click the RD Sensor installer file to begin installation.

4. After accepting the EULA, click **Next**.

5. Deselect the check box next to **Participate in product improvement program** if you do not agree to send crash reports and anonymous telemetry data to ESET (OS version and type, ESET product version and other product-specific information). If the check box is left selected, telemetry data and crash reports will be sent to ESET.

6. Select the location where RD Sensor will be installed and click **Next** → **Install**.

RD Sensor prerequisites

The following prerequisites must be met in order to install the RD Sensor component on Windows:

• WinPcap - use the latest WinPcap version (at least 4.1.0)

• Network should be properly configured (appropriate ports open, incoming communication not being blocked by a firewall, etc.)

• ESET PROTECT Server must be reachable

• ESET Management Agent must be installed on the local computer to fully support all program features

• Rogue Detection Sensor log file can be found here: *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 downloads detection engine updates and other program modules only, it does not download PCUs (Program Component Updates) and ESET LiveGrid® data. It can also create a full offline repository. Alternatively, you can upgrade products individually.

Prerequisites

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 products for Windows - You can update them remotely using HTTP or a shared folder.

oESET security products 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 product.

• You must have a valid Offline license file that includes the Username and Password. When generating a license file, be sure to select the check box next to **Include Username and Password**. Also, you must enter a license **Name**. An offline license file is needed for the activation of the Mirror Tool and generation of the update mirror.

• Before running the Mirror Tool, you need to have the following packages installed:

• Visual C++ Redistributable for Visual Studio 2010

• Visual C++ 2015 Redistributable x86

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
```

All filters are case sensitive.

--updateServer	When you use it, you must specify the full URL of the update server.
--offlineLicenseFilename	You must specify a path to your offline license 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 Knowledgebase article.

--mirrorFileFormat	Before using the `--mirrorFileFormat` parameter, ensure that you environment does not contain both older (6.5 and older) and newer (6.6. and later) ESET security product versions. The incorrect usage of this parameter may result in incorrect updates of your ESET security products. You can specify which type of update files will be downloaded. Possible values (case sensitive): • dat - Use this value if you have environment only with ESET security product versions 6.5 and older. • dll - Use this value if you have environment only with ESET security product versions 6.6 and later. The parameter is ignored when creating a mirror for legacy products (ep4, ep5).
--compatibilityVersion	This optional parameter applies to the Mirror Tool distributed with ESET PROTECT 8.1 and later. The Mirror Tool will download update files compatible with ESET PROTECT repository version you specify in the parameter argument in format `x.x` or `x.x.x.x`, for example: `--compatibilityVersion 9.0` or `--compatibilityVersion 8.1.13.0`.

To reduce the amount of data dowloaded from the ESET repository, we recommend that you use the new parameters in Mirror Tool distributed with ESET PROTECT 9: `--filterFilePath` and `--dryRun`:
1.Create a filter in a *JSON* format (see `--filterFilePath` below).
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.

--filterFilePath

Use this optional parameter to filter ESET security products based on a text file in *JSON* format placed in the same folder as Mirror Tool, for example: `--filterFilePath filter.txt`).

Filter configuration description:

The configuration file format for product filtering is *JSON* with the following structure:

- root *JSON* object:

o`use_legacy` (boolean, optional) - if true, legacy products will be included.

o`defaults` (*JSON* object, optional) - defines filter properties that will be applied to all products.

■`languages` (string) - Specify ISO language codes of languages to include, for example for French type "fr_FR". Other languages codes are in the table below. To select more languages, separate them by a comma and a space, for example: "en_US", "zh_TW", "de_DE"

■`platforms` (string) - platfoms to include (`x64`, `x86`, `arm64`).

> Use the `platforms` 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 products will fail to install on 32-bit computers.

■`os_types` (string) - OS types to include.

o`products` (list of JSON objects, optional) - filters to apply to specific products - override `defaults` for specified products. The objects have the following properties:

■`app_id` (string) - required if `name` is not specified.

■`name` (string), required if `app_id` is not specified.

■`version` (string) - specifies version or range of versions to include.

■`languages` (string) - ISO language codes of languages to include (see the table below).

■`platforms` (string) - platforms to include (`x64`, `x86`).

■`os_types` (string) - OS types to include.

> To determine appropriate values for the fields, run Mirror Tool in dry run mode and find the relevant product in the created CSV file.

Version string format descriptions

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`).

Version string can have one of the two following formats:

- [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))

oSelects versions greater/smaller or equal/less or equal/equal than the version specified.

- <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))

oSelects versions that are greater than or equal to the lower bound and less than or equal to the higher bound.

Comparisons are done numerically on each part of the version number, left to right.

JSON example

```
{
"use_legacy": true,
"defaults": {
"languages": [ "en_US" ],
"platforms": [ "x64", "x86" ]
},
"products": [
{
"app_id": "com.eset.apps.business.ees.windows",
"version": "7.1.0.0 - 8.0.0.0"
},
{
"app_id": "com.eset.apps.business.eea.windows",
"version": ">7.1.0.0"
}
]
}
```

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

--dryRun	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. You can use this parameter without mandatory parameters `--intermediateRepositoryDirectory` and `--outputRepositoryDirectory`, for example: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. 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`. If you use the `--dryRun` parameter and also `--intermediateRepositoryDirectory` and `--outputRepositoryDirectory` parameters, the Mirror Tool does not clear the *outputRepositoryDirectory*.
--listUpdatableProducts	List all ESET products for which the Mirror Tool can download module updates (unless `--excludedProducts` is used). The parameter is available from Mirror Tool versions: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

The Mirror Tool creates a structure of folders different from what Endpoint mirror does. Each folder holds update files for a group of products. You have to specify the full path to the correct folder in the update settings of the product using the mirror.
For example, to update the ESET PROTECT 9 from the mirror set the Update server to (according to your HTTP server root location):
`http://your_server_address/mirror/eset_upd/era6`
Note: The `era6` mirror folder is common for these ESET remote management solutions: ERA 6, ESMC 7, ESET PROTECT.

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 products, 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 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).

Mobile Device Connector installation

To install the Mobile Device Connector component for ESET PROTECT Server, please complete following steps.

Mobile Device Connector must be accessible from the Internet so that mobile devices can be managed at all times regardless of their location.

We recommend that you deploy your MDM component on a host device separate from the one ESET PROTECT Server is hosted on.

1. Visit the ESET PROTECT download section to download a standalone installer for this ESET PROTECT component (*mdmcore_x64.msi*).

2. Please read the prerequisites first and make sure all are met.

3. Run the Mobile Device Connector installer and accept the EULA if you agree with it.

4. Click **Browse**, navigate to the location of your SSL certificate for communication via HTTPS, type in the password for this certificate.

5. Specify **MDM hostname**: this is the public domain or public IP address of your MDM server as it is reachable by mobile devices from the Internet.

MDM hostname must be entered in the same form as specified in your **HTTPS Server certificate**, otherwise the iOS mobile device will refuse to install MDM Profile. For example, if there is an IP address specified in the HTTPS certificate, type in this IP address into the **MDM hostname** field. If FQDN is specified (e.g. `mdm.mycompany.com`) in the HTTPS certificate, enter this FQDN in **MDM hostname** field. Also, if there is a wildcard * used (e.g. `*.mycompany.com`) in HTTPS certificate, you can use `mdm.mycompany.com` in the **MDM hostname** field.

6. The installer now needs to connect to an existing database that which will be used by Mobile Device Connector. Specify the following connection details:

• **Database**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication

• **ODBC Driver**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/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

- **Database name**: We recommend that you use the pre-defined name or change it if required.
- **Hostname**: hostname or the IP address of your database server
- **Port**: used for connection to the database server
- Database admin account **Username/Password**
- **Use Named Instance** - If you are using an MS 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\ESMC7SQL*). For 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 MS SQL database installed in a Failover Cluster, enter the cluster name in the **Hostname** field.

You can use the same database server you are using for ESET PROTECT database, but it is recommended to use a different DB server if you are planning to enroll more than 80 mobile devices.

7. Specify user for newly created Mobile Device Connector database. You can **Create new user** or **Use existing database user**. Type in the password for the database user.

8. Enter **Server host** (name or IP address of your ESET PROTECT Server) and **Server port** (default port is 2222, if you are using different port, then replace the default port with your custom port number).

9. Connect the MDM Connector to the ESET PROTECT Server. Fill in the **Server host** and **Server port** required for connection to the ESET PROTECT Server and select either **Server Assisted installation** or **Offline Installation** to proceed:

- **Server assisted installation** - Provide ESET PROTECT Web Console administrator credentials and the installer will download the required certificates automatically. Also check the permissions required for server-assisted installation.

    1.Enter your **Server host** - name or IP address of your ESET PROTECT Server and **Web Console port** (leave default port 2223 if you are not using custom port). Also, provide Web Console administrator account credentials - **Username/Password**.

    2.When asked to Accept the Certificate, click **Yes**. Continue to step 11.

- **Offline installation** - Provide a **Proxy certificate** and **Certification Authority** which can be exported from ESET PROTECT. Alternatively, you can use your custom certificate and appropriate Certification Authority.

    1.Click **Browse** next to the Peer certificate and navigate to the location of your **Peer certificate** location (this is the Proxy certificate you have exported from ESET PROTECT). Leave the **Certificate password** text field blank as this certificate does not require a password.

    2.Repeat the procedure for Certificate Authority and continue to step 11.

If you are using custom certificates with ESET PROTECT (instead of the default ones that were automatically generated during ESET PROTECT installation), these should be used when you are prompted to supply a Proxy certificate.

10. Specify destination folder for Mobile Device Connector (we recommend using default), click **Next**, then **Install**.

11. After the installation is complete, check if the Mobile Device Connector is running correctly by opening *https://your-mdm-hostname:enrollment-port* (for example *https://mdm.company.com:9980*) in your web browser or from mobile device. If the installation was successful, you will see following message: MDM Server up and running!

12. You can now activate MDM from ESET PROTECT.

Mobile Device Connector prerequisites

If the port or the hostname for the MDM server is changed, all mobile devices must be re-enrolled.
For this reason, it is recommended that you set up a dedicated hostname for the MDM server so that if you ever need to change the host device of the MDM server, you can do so by reassigning the new host device's IP address to the MDM hostname in your DNS settings.

The following prerequisites must be met in order to install Mobile Device Connector on Windows:

- Public IP address/hostname or public domain accessible from the Internet.

If you need to change the hostname of your MDM Server, you will need to run a repair installation of your MDC component. If you change the hostname of your MDM Server, you will need to import a new **HTTPS Server certificate** that includes this new hostname for MDM to continue working correctly.

- Ports open and available - see the complete list of ports. We recommend using default port numbers 9981 and 9980, but these can also be changed in configuration file of your MDM Server if needed. Make sure that mobile devices are able to connect via specified ports. Change your firewall and/or network settings (if applicable) to make this possible. Read more about MDM architecture.

- Firewall settings - when installing Mobile Device Connector on non-server OS such as Windows 7 (for evaluation purpose only), make sure to allow communication ports by creating firewall rules for:

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

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

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

Actual paths to *.exe* files may vary depending on where each of the ESET PROTECT components is installed on your client OS system.

• A database server already installed and configured. Make sure you meet Microsoft SQL or MySQL requirements.

• RAM usage of MDM connector is optimized so there can be maximum of 48 "ESET PROTECT MDMCore Module" processes running concurrently, and if the user connects more devices, the processes will then periodically change for each device that currently needs to use the resources.

• MS SQL Server Express installation requires Microsoft .NET Framework 4. You can install it using the **Add Roles and Features Wizard**:

Certificate requirements

• You will need an **SSL certificate** in *.pfx* format for secure communication over HTTPS. We recommend that you use a certificate provided by a third-party Certification Authority. Self-signed certificates (including certificates signed by the ESET PROTECT CA) are not recommended because not all mobile devices let users accept self-signed certificates.

• You need to have a certificate signed by CA and the corresponding private key, and utilize standard procedures (traditionally using OpenSSL), to merge those into one *.pfx* file:
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
This is the standard procedure for most servers which use SSL certificates.

• For Offline installation, you will also need a Peer certificate (the **Agent certificate** exported from ESET PROTECT). Alternatively, you can use your custom certificate with ESET PROTECT.

Mobile Device Connector activation

After you have installed Mobile Device Connector, you need to activate it with an ESET endpoint, business or office license:

1.Add the ESET Endpoint, Business or Office license to ESET PROTECT License Management.

2.Activate Mobile Device Connector using a Product Activation Client Tasks. This procedure is the same as when activating any ESET product on a client computer—in this case Mobile Device Connector is client computer.

MDM iOS licensing functionality

Since ESET does not offer an application on the Apple App Store, ESET Mobile Device Connector stores all licensing details for iOS devices.

Licenses are per-device and can be activated using a Product Activation Task (same as Android).

iOS licenses can be deactivated in the following ways:

• Removal of the device from the management via a Stop managing task

- Uninstallation of MDC via the **Remove database** option
- Deactivation by other means (ESET PROTECT or EBA deactivation)

Because MDC communicates with ESET licensing servers on behalf of iOS devices, EBA portal reflects the state of MDC and not the state of individual devices. Current device information is always available in ESET PROTECT Web Console.

Devices that are not activated or devices with expired licenses will display a red protection status and the "Product is not activated" message. These devices will refuse to handle tasks, set policies and deliver non-critical logs.

During uninstallation of MDM, if **Do not remove the database** is selected, licenses used will not be deactivated. These licenses can be reused if MDM is reinstalled on this database, removed via ESET PROTECT or by EBA deactivation. When moving to another MDM server, you will need to perform the Product Activation Task again.

HTTPS certificate requirements

To enroll a mobile device in ESET Mobile Device Connector, ensure that the HTTPS server returns the full certificate chain.

For the certificate to work properly, these requirements must be met:

- The HTTPS certificate (pkcs#12/pfx container) must contain the full certificate chain, including the root CA.
- The certificate must be valid during the required time (valid from / valid to).
- The **CommonName** or **subjectAltName**s must match the MDM hostname.

If the **MDM hostname** is hostname.mdm.domain.com, for example, your certificate can contain names like:
• hostname.mdm.domain.com
• *.mdm.domain.com
But not names like:
• *
• *.com
• *.domain.com
Basically, the " * " cannot be used to replace the "dot". This behavior is confirmed for the way the iOS accepts the certificates for MDM.

Note that some devices take their current time zone into consideration when checking the certificate validity, and other devices don’t. Avoid potential problems by giving the certificate validity a day or two before the current date.

Apache HTTP Proxy installation and cache

About Apache HTTP Proxy

Apache HTTP Proxy can serve various purposes:

Caching of downloads and updates	Apache HTTP Proxy or other proxy solution
Caching of ESET Dynamic Threat Defense results	Only configured Apache HTTP Proxy
Replication ESET Management Agents' communication with ESET PROTECT Server	Apache HTTP Proxy or other proxy solution

If you already have Apache HTTP Proxy installed on Windows and want to upgrade it to the most recent version, proceed to Upgrading Apache HTTP Proxy.

Caching function of Apache HTTP Proxy

Apache HTTP Proxy downloads and caches:

- ESET module updates
- Installation packages from repository servers
- Product component updates

Cached data is distributed to endpoint clients on your network. Caching can significantly decrease internet traffic on your network.

You can choose to install Squid as an alternative to Apache HTTP Proxy.

You can install Apache HTTP Proxy on Windows in two ways:

- Installation from the All-in-one installer
- Installation from the standalone installer

Installation from the standalone installer

1. Visit the ESET PROTECT download section to download a standalone installer for this ESET PROTECT component (*apachehttp.zip*).

2. Open *ApacheHttp.zip* and extract the files to *C:\Program Files\Apache HTTP Proxy*

If you want to install Apache HTTP Proxy on a different hard drive, *C:\Program Files* must be replaced with the corresponding path in the instructions below and in the *httpd.conf* file located in the *Apache HTTP Proxy\conf* directory. For example, if you extract the content of *ApacheHttp.zip* to *D:\Apache Http Proxy*, then *C:\Program Files* must be replaced with *D:\Apache Http Proxy*.

3. Open an administrative command prompt and change the directory to *C:\Program Files\Apache HTTP Proxy\bin*

4. Execute the following command:

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

5. Start the **ApacheHttpProxy** service using the following command:

```
sc start ApacheHttpProxy
```

6. You can verify that the Apache HTTP Proxy service is running in the `services.msc` snap-in (look for **ApacheHttpProxy**). By default, the service is configured to start automatically.

After the installation, configure the Apache HTTP Proxy for desired functionality.

Configuration of Apache HTTP Proxy

The Apache HTTP Proxy installer provided by ESET is pre-configured. However, additional custom configuration is needed for the service to work correctly.

Configuration of Apache HTTP Proxy for replication (Agent - Server)

1. Modify the *Apache HTTP Proxy* configuration file *httpd.conf* located in *C:\Program Files\Apache HTTP Proxy\conf*.

   a.By default, port 2222 is used for communication with the ESET Management Agent. If you changed the port during installation, use the changed port number. Change 2222 in the line: `AllowCONNECT 443 563 2222 8883 53535` to your port number.

   b.Add a separate `ProxyMatch` segment:

      I.The address which your Agents use to connect to the ESET PROTECT Server.

      II.All other possible addresses of your ESET PROTECT Server (IP, FQDN)
      (add the whole below code; IP address 10.1.1.10 and hostname `hostname.example` are only examples to be substituted by your addresses. You can also generate the `ProxyMatch` expression in this Knowledgebase article.)

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

   c.Restart the *Apache HTTP Proxy* service.

2. Set up a proper Agent policy to make sure your agents use the proxy for replication.

Configuration of Apache HTTP Proxy for caching

1. Stop the **ApacheHttpProxy** service using the following command:

```
sc stop ApacheHttpProxy
```

2. Open the file *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf* in a simple text editor. Add the following lines to the bottom of the file:

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

3. Save the file and start the Apache service.

```
sc start ApacheHttpProxy
```

If you prefer to have the cache directory located somewhere else, for example, on another disk drive such as `D:\Apache HTTP Proxy\cache`, then in the last line of the code above, change `"C:\Program Files\Apache HTTP Proxy\cache"` to `"D:\Apache HTTP Proxy\cache"`.

Configuration of Apache HTTP Proxy for username and password

The username and password setting can only be used for caching. Authentication is not supported in the replication protocol used in Agent - Server communication.

1. Stop the **ApacheHttpProxy** service by opening an elevated command prompt and executing the following command:

```
sc stop ApacheHttpProxy
```

2. Verify the presence of the following modules in *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*:

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

3. Add the following lines to *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf* under `<Proxy *>`:

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

4. Use the `htpasswd` command to create a file named `password.file` in the folder *Apache HTTP Proxy\bin* (you will be prompted for password):

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

5. Manually create the file `group.file` in the folder *Apache HTTP Proxy* with the following content:

```
usergroup:username
```

6. Start the **ApacheHttpProxy** service by executing the following command in an elevated command prompt:

```
sc start ApacheHttpProxy
```

7. Test the connection to HTTP Proxy by accessing the following URL in your browser:

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

> Once you have successfully completed installation of Apache HTTP Proxy, you have the option to only allow ESET communication (blocking all other traffic - by default) or to allow all traffic. Perform the necessary configuration changes described here:
> • Forwarding for ESET communication only
> • Proxy chaining (all traffic)

Display a list of content which is currently cached

"*C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe*" *-a -p "C:\ProgramData\Apache HTTP Proxy\cache*"

Use the htcacheclean tool to clean up the disk cache. See the recommended command below (setting cache size to 20 GB and cached files limit to ~128000):

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

To schedule cache clean up every hour run:

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

If you choose to allow all traffic, the recommended commands are:

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

> The ^ character right after the end of line in the commands above is essential and if it is not included the command will not execute correctly.

For more information, visit our Knowledgebase article or the Apache Authentication and Authorization documentation.

Squid installation on Windows and HTTP proxy cache

Squid is an alternative to Apache HTTP Proxy. To install Squid on Windows, follow these

steps:

1. Download the Squid MSI installer and install Squid.

2. Click the **Squid for Windows** icon in the tray menu and select **Stop Squid Service**.

3. Navigate to the Squid installation folder, for example C:\Squid\bin, and run the following command from command line:

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

This creates the swap directories for cache.

4. Click the **Squid for Windows** icon in the tray menu and select **Open Squid Configuration**.

5. Replace `http_access deny all` with `http_access allow all`.

6. Enable disk caching by adding this line:

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

- You can change the location of the cache directory based on your preferences. In the example, the cache directory is located in `C:\Squid\var\cache` (note the path format in the command).
- You can change the total cache size (3000 MB in the example) and the number of first-level sub-directories (16 in the example) and second-level sub-directories (256 in the example) in the cache directory.

7. Save and close the Squid configuration file *squid.conf*.

8. Click the **Squid for Windows** icon in the tray menu and select **Start Squid Service**.

9. You can verify that the Squid service is running in the `services.msc` snap-in (look for **Squid for Windows**).

Offline Repository

You can use the Mirror Tool to create an offline repository (on Windows). Usually this is needed for closed computer networks or networks with limited internet access. The Mirror Tool can be used to create a clone of the ESET repository in a local folder. This cloned repository can be afterward 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 HTTP server.

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. Make sure you have at least **600 GB** of free space before starting this procedure.

Best practices

See also the ESET Knowledgebase article Best practices for using the ESET PROTECT 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 HTTP server

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

   - Apache HTTP Proxy from the ESET download site (this scenario)
   - a different HTTP server

8. Open *apachehttp.zip* and extract the files to *C:\Program Files\Apache HTTP Proxy*

9. Open an administrative command prompt and change the directory to *C:\Program Files\Apache HTTP Proxy\bin* (`cd` command).

10. Execute the following command:

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

11. Using a simple text editor, open the *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf* file

and add the following lines at the bottom of the file:

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

12. Start the **ApacheHttpProxy** service using the following command:

```
sc start ApacheHttpProxy
```

13. Test if the service is running by opening *http://YourIPaddress:80/index.html* in your web browser (replace *YourIPaddress* with IP address of your computer).

III. Run the offline repository

14. Create a new folder for the offline repository, for example, *C:\Repository.*

15. In the *httpd.conf* file, replace the following lines

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

with the address of the repository folder, as follows:

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

16. Copy the downloaded repository into *C:\Repository* .

17. Restart the **ApacheHttpProxy** service using the following command:

```
sc restart ApacheHttpProxy
```

18. Now your offline repository is running on the address *http://YourIPaddress* (for example, *http://10.1.1.10*).

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

    a.ESET PROTECT Server - Click **More** → **Server Settings** → **Advanced Settings** → **Repository** and enter the offline repository address to the **Server** field.

    b.ESET Management Agents - Click **Policies**, click the Agent policy → **Edit** → **Settings** → **Advanced Settings** → **Repository** → enter the offline repository address to the **Server** field.

    c.ESET endpoint products (for Windows) - Click **Policies**, click the **ESET Endpoint for Windows** policy → **Edit** → **Settings** → **Update** → **Profiles** → **Updates** → **Modules Updates** → Deselect **Choose automatically** and enter the offline repository address to the **Custom server** field.

Failover Cluster

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

See also this Knowledgebase article about cluster installation of ESET PROTECT Server.

1. Create a Failover Cluster with a shared disk:

   - Instructions to create a failover cluster in Windows Server 2016 and 2019
   - Instructions to create a failover cluster in Windows Server 2012 and 2012 R2

2. In the **Create Cluster Wizard** enter 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. Make sure that **This is a cluster installation** is selected during installation and select the shared disk as application data storage. Make up a hostname and enter 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. Make sure 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

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.

For step-by-step ESET PROTECT Server installation, follow the instructions included in this section.

To upgrade ESET PROTECT for Linux to the latest version, see the Components Upgrade task chapter or our Knowledgebase article.

Core components

- ESET PROTECT Server
- ESET PROTECT Web Console - You can install the ESET PROTECT Web Console on a different computer than the computer running the ESET PROTECT Server.
- ESET Management Agent
- a Database server

Optional components

- RD Sensor
- Mobile Device Connector
- Apache HTTP Proxy
- Mirror Tool

MySQL installation and configuration

Installation

Make sure to install a supported version of MySQL Server and ODBC Connector.

If you have already installed and configured MySQL, proceed to Configuration.

1. Before installing the database on Linux, add MySQL repository:

Debian, Ubuntu	Run the following commands in the Terminal: a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb See also: Adding the MySQL APT Repository

CentOS, Red Hat	Adding the MySQL Yum Repository
OpenSuse, SUSE Linux Enterprise Server	Adding the MySQL SLES Repository

2. After adding the MySQL repository update your local repository cache (e.g. on Debian run `sudo apt-get update`), and you can proceed with MySQL installation.

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

Debian, Ubuntu	sudo apt-get install mysql-server	https://dev.mysql.com/doc/refman/5.7/en/linux-installation-apt-repo.html
CentOS, Red Hat	sudo yum install mysql-server	https://dev.mysql.com/doc/refman/5.7/en/linux-installation-yum-repo.html
OpenSuse, SUSE Linux Enterprise Server	sudo zypper install mysql-community-server	https://dev.mysql.com/doc/refman/5.7/en/linux-installation-sles-repo.html

- Manual installation – download and install MySQL Community Server edition from: https://dev.mysql.com/downloads/mysql/

Configuration

1. Run the following command to open the *my.cnf* (*my.ini* for Windows installation) file in a text editor:

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

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

2. Find the following configuration in the `[mysqld]` section of the *my.cnf* file and modify the values. If the parameters are not present in the file, add them to the `[mysqld]` section:

```
max_allowed_packet=33M
```

To determine your MySQL version, run the command: `mysql --version`

- For the supported versions MySQL 8.x, you must set the following variable:
  - `log_bin_trust_function_creators=1`
  - Alternatively, you can disable binary logging: `log_bin=0`
- For the supported versions of MySQL 8.x, 5.7 and 5.6.22 (and later 5.6.x):
  - `innodb_log_file_size*innodb_log_files_in_group` needs to be set to at least **200 MB** (* denotes multiplication, the product of the two parameters must be > 200 MB. The minimum value for `innodb_log_files_in_group` is 2 and maximum value is 100, the value also has to be integer).
    For example:

```
innodb_log_file_size=100M
innodb_log_files_in_group=2
```

- For MySQL 5.6.20 and 5.6.21:

  o`innodb_log_file_size` needs to be set to at least **200 MB** (for example, `innodb_log_file_size=200M`), but not more than **3000 MB**.

3. Save and close the file and enter the following command to restart the MySQL server and apply the configuration (in some cases, the service name is `mysqld`):

```
sudo service mysql restart
```

4. Run the following command to set up MySQL including privileges and password (this is optional and may not work for some Linux distributions):

```
/usr/bin/mysql_secure_installation
```

5. Enter the following command to check whether the MySQL server is running:

```
sudo service mysql status
```

ODBC installation and configuration

Make sure to install a supported version of MySQL Server and ODBC Connector.

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

Debian, Ubuntu

Run the following commands in the Terminal:

1. `sudo apt-get install unixodbc`

2. Download the ODBC connector:

   - Ubuntu 16: `wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz`

   - Ubuntu 18: `wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz`

   - Ubuntu 19 and 20: `wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`

3. `gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz` (Package name changes depending on link used.)

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

name changes depending on link used.)

5. `cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit` (Package name changes depending on link used.)

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

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

8. Register the driver for ODBC. For new Linux versions like Ubuntu 20.x we recommend using the Unicode driver, step a). For other systems, or when Unicode driver is not working use step b).

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

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

9. `myodbc-installer -d -l`

For more information, see: https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html.

Other supported Linux distributions

1. Download the ODBC connector for MySQL from the official MySQL site. Make sure to select and download the version compatible with your Linux distribution and version.

2. Follow these instructions to install the ODBC driver:

   • **CentOS, Red Hat**: https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-yum.html

   • **OpenSuse, SUSE Linux Enterprise Server**: https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html

3. Run the following command to open the *odbcinst.ini* file in a text editor:

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

4. Copy the following configuration into the **odbcinst.ini** file (make sure 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*"
```

5. 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
```

Server installation - Linux

Installation of the ESET PROTECT Server component on Linux is performed using a command in the Terminal. You can prepare an installation script and then execute it using `sudo`. Make sure all prerequisites are met before you begin installation.

> ### Installation instructions for selected Linux distributions
> You can follow our Knowledgebase articles with distribution-specific instructions:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

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. 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=127.0.0.1 \
--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"
```

You can modify the following attributes:

--uninstall	Uninstalls the product.	-
--keep-database	Database will not be removed during uninstallation.	-

--locale	The locale identifier (LCID) of the installed server (default value is `en_US`). See supported languages for possible options. If you do not specify the `--locale`, ESET PROTECT Server will be installed in the English language. After ESET PROTECT 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 installation and their language cannot be changed.	Yes
--skip-license	Installation will not ask the user for license agreement confirmation.	-
--skip-cert	Skip generation of certificates (use with the `--server-cert-path` parameter).	-
--license-key	ESET license key. This can be set later.	-
--server-port	ESET PROTECT server port (default value is `2222`)	-
--console-port	ESET PROTECT console port (default value is `2223`)	-
--server-root-password	Password for Web Console login of the user "Administrator", must be at least 8 characters long.	Yes
--db-type	The type of database that will be used (possible values: `"MySQL Server"`, `"MS SQL Server"`). MS SQL Server on Linux is not supported. However, you can connect the ESET PROTECT Server on Linux to MS SQL Server on Windows.	-
--db-driver	ODBC driver used for connecting to database specified in the *odbcinst.ini* file (command `odbcinst -q -d` gives a list of available drivers, use one of these drivers for example: `--db-driver="MySQL ODBC 8.0 Driver"`).	Yes
--db-hostname	Computer name or IP address of the database server. 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 `era_db`).	-
--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 `--db-user-username` and `--db-user-password`	Yes
--db-admin-password	Database administrator password. You can omit this parameter if there is a previously created database user defined by `--db-user-username` and `--db-user-password`	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 computer that ESET PROTECT Server will be installed on. This will need to match with the server name specified in the Agent certificate that tries to connect to the server.	Yes
--server-cert-path	Path to server peer certificate (use this option if you specified `--skip-cert` as well)	-
--server-cert-password	Password of server peer certificate	-
--agent-cert-password	Password of Agent peer certificate	-
--cert-auth-password	Certificate Authority password	-
--cert-auth-path	Path to the Server's Certificate Authority file	-
--cert-auth-common-name	Certification Authority common name (use `""`)	-
--cert-organizational-unit	-	-
--cert-organization	-	-
--cert-locality	-	-
--cert-state	-	-
--cert-country	-	-
--cert-validity	Certificate validity in days or years (specify in argument `--cert-validity-unit`)	-
--cert-validity-unit	Unit for certificate validity, possible values are 'Years' or 'Days' (default value is `Years`)	-
--ad-server	Active Directory server	-
--ad-user-name	Name of the user who has rights to search the AD network	-
--ad-user-password	Active Directory user password	-
--ad-cdn-include	Active Directory tree path, which will be synchronized for; use empty brackets "" to synchronize a whole tree	-
--enable-imp-program	Turn on the Product improvement program.	-
--disable-imp-program	Turn off the Product improvement program.	-

ESET recommends 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. 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

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

```
service eraserver status
```

Installer log

The installer log may be useful for troubleshooting and can be found in Log files.

Server prerequisites - Linux

The following prerequisites must be met to install the ESET PROTECT Server on Linux:

- You must have a valid license.
- 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 prior to the installation. The installer can create the account. MS SQL Server on Linux is not supported. However, you can connect the ESET PROTECT Server on Linux to MS 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 to run properly.

- **ODBC Driver** - The ODBC Driver is used to establish connection with the database server (MySQL).
- Configure the server installation file set as an executable. To do so, use the following terminal command:

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

- **We recommend that you use the latest OpenSSL version (1.1.1)**. The minimum supported version of OpenSSL is openssl-1.0.1e-30. There can be more versions of OpenSSL installed on one system in the same time. At least one supported version must be present on you system.
    - oYou can use the command `openssl version` to show current default version.
    - oYou can list all versions of OpenSSL present on your system. See the filename endings listed using the command `sudo find / -iname *libcrypto.so*`
- **Xvfb** - Required for proper report printing (Generate Report) on Linux Server systems without a graphical interface.
- **Xauth** - The package gets installed together with **xvfb**. You need to install **xauth** if you do not install **xvfb**.
- **cifs-utils** - Required for proper Agent deployment to a Windows OS.
- **Qt4 WebKit libraries** - Used for printing reports to PDF and PS format (must be version 4.8, not 5). All other Qt4 dependencies will be installed automatically. If the package is not available in your operating system repository, you can compile it yourself on a target machine or install it from a third-party repository (for example, EPEL repositories): CentOS 7 instructions, Ubuntu 20.04

instructions.

- **kinit + klist** - Kerberos is used for authentication of a domain user when logging in and Active Directory synchronization task. Make sure your Kerberos configured properly (*/etc/krb5.conf*). ESET PROTECT 9.0 supports synchronization with multiple domains.

- **ldapsearch** - Used in AD synchronization task and for authorization.

- **snmptrap** - Used to send SNMP traps. If the functionality will not be used, this is optional. SNMP also requires configuration.

- **SELinux devel package** - Used during product installation to build SELinux policy modules. This is only required on systems with SELinux enabled (CentOS, 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`):

ODBC Driver	See the chapter ODBC installation and configuration.		
xvfb	apt-get install xvfb	yum install xorg-x11-server-Xvfb	zypper install xorg-x11-server-extra
cifs-utils	apt-get install cifs-utils	yum install cifs-utils	zypper install cifs-utils
Qt4 WebKit libraries	apt-get install libqtwebkit4 See instructions for Ubuntu 20.04.	See our Knowledgebase article.	zypper install libqtwebkit4
kinit + klist - optional (necessary for Active Directory service)	apt-get install krb5-user	yum install krb5-workstation	zypper install krb5
ldapsearch	apt-get install ldap-utils libsasl2-modules-gssapi-mit	yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap	zypper install openldap2-client cyrus-sasl-gssapi cyrus-sasl-ldap-auxprop
snmptrap	apt-get install snmp	yum install net-snmp-utils net-snmp	zypper install net-snmp
SELinux devel package (optional - not necessary for ESET PROTECT Server; SELinux may cause problems with other applications.)	apt-get install selinux-policy-dev	yum install policycoreutils-devel	zypper install selinux-policy-devel
samba (optional, necessary only for remote deployment)	apt-get install samba	yum install samba samba-winbind-clients	zypper install samba samba-client
lshw	apt-get install -y lshw	yum install -y lshw	zypper install lshw

Agent installation - Linux

Installation of the ESET Management Agent component on Linux is performed using a command in the Terminal. Make sure all prerequisites are met.

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):

Server-assisted installation

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.179.36 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

Offline installation

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

ESET recommends 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.

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").

--hostname	Hostname or IP address of ESET PROTECT Server to connect.	Yes
--port	ESET PROTECT Server port (default value is `2222`).	Yes
--cert-path	Local path to the Agent certificate file (more about certificate).	Yes (Offline)
--cert-auth-path	Path to the server's Certificate Authority file (more about authority).	Yes (Offline)
--cert-password	Agent Certificate password.	Yes (Offline)
--cert-auth-password	Certificate Authority password.	Yes (if it is used)
--skip-license	Installation will not ask user for license agreement confirmation.	No
--cert-content	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 `--cert-path` or `--cert-content` options.	No
--cert-auth-content	Base64 encoded content of DER encoded Certificate Authority private key certificate used to verify remote peers (Proxy or Server). Use only one of the `--cert-auth-path` or `--cert-auth-content` options.	No
--webconsole-hostname	Hostname or IP address used by Web Console to connect to the server (if left empty, value will be copied from 'hostname').	No
--webconsole-port	Port used by Web Console to connect to the server (default value is `2223`).	No
--webconsole-user	Username used by Web Console to connect to the server (default value is `Administrator`). You cannot use a user with two-factor authentication for server-assisted installations.	No
--webconsole-password	Password used by Web Console to connect to the server.	Yes (Server-assisted)
--proxy-hostname	HTTP Proxy hostname. 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).	If proxy is used
--proxy-port	HTTP Proxy port for connecting to the server.	If proxy is used
--enable-imp-program	Turn on Product improvement program.	No
--disable-imp-program	Turn off 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 this connection information for **Server-assisted installation**: `--webconsole-port, --webconsole-user, --webconsole-password`
- 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 provided as plain text. That is:

`--password=env:SECRET_PASSWORD` where `SECRET_PASSWORD` is an environment variable with 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 the initialization of the Agent.

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.

Installer log

The installer log may be useful for troubleshooting and can be found in Log files.

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

```
sudo service eraagent status
```

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** - higher version of installer is run.
  - Server-assisted installation - application is upgraded, but it will keep using previous certificates.
  - Offline installation - application is upgraded, new certificates are used.
- **Repair** - same version of installer is run. This can be used for migration of the Agent to a different ESET PROTECT Server.
  - Server assisted installation - application is reinstalled and it will get current certificates from the ESET PROTECT Server (defined by `hostname` parameter).
  - Offline installation - application is reinstalled, new certificates are used.

If you are migrating agent from older Server to a different newer ESET PROTECT Server manually, and you are using Server-assisted installation, run the installation command twice. The first will upgrade the Agent and second one will get the new certificates, so the Agent can connect the ESET PROTECT Server.

Agent prerequisites - Linux

The following prerequisites must be met in order to install the ESET Management Agent component on Linux:

- **We recommend that you use the latest OpenSSL version (1.1.1)**. The minimum supported version of OpenSSL is openssl-1.0.1e-30. There can be more versions of OpenSSL installed on one system in the same time. At least one supported version must be present on you system.
  - You can use the command `openssl version` to show current default version.

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

• Install the `lshw` package on the client/server Linux machine for the ESET Management Agent to report the hardware inventory correctly.

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

• For Linux CentOS it is recommended to install the `policycoreutils-devel` package. Run the command to install the package:

```
yum install policycoreutils-devel
```

Server-assisted Agent installation:

• The server computer must be reachable from the network and have ESET PROTECT Server and ESET PROTECT Web Console installed

Offline Agent installation:

• 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

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 requires additional steps.

1. Install the Apache Tomcat and Java packages. Example package names below may differ from packages available in your Linux distribution repository.

Debian and Ubuntu distributions	sudo apt-get update sudo apt-get install openjdk-11-jdk tomcat9
CentOS and Red Hat distributions	yum update yum install java-1.8.0-openjdk tomcat
OpenSUSE	zypper refresh zypper install java-1_8_0-openjdk tomcat

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

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

3. Copy the `era.war` file to the Tomcat folder:

Debian and Ubuntu distributions	sudo cp era.war /var/lib/tomcat9/webapps/
CentOS and Red Hat distributions	sudo cp era.war /var/lib/tomcat/webapps/
OpenSUSE distribution	sudo cp era.war /usr/share/tomcat/webapps/

Alternatively, you can extract the contents of *era.war* to */var/lib/tomcat/webapps/era/*.

4. Restart the Tomcat service to deploy the *.war* file:

Debian and Ubuntu distributions	sudo service tomcat9 restart
CentOS and Red Hat distributions	sudo service tomcat restart
OpenSUSE distribution	sudo service tomcat restart

5. 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 service tomcat stop`

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 located 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 service tomcat restart`

6. 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*

7. 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 also the additional Web Console configuration for enterprise solutions or low-performance systems.

Rogue Detection Sensor installation and prerequisites - Linux

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.

To install the RD Sensor component on Linux, follow these steps:

1. Make sure the following prerequisites are met:

- The Network can be searched (ports are open, the firewall is not blocking incoming communication, etc.).
- The Server computer can be reached.
- ESET Management Agent must be installed on the local computer to fully support all program features.
- The Terminal is open.
- RD Sensor installation file set as an executable:

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

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

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

3. Read the End User License Agreement. Use **Space bar** to proceed to the next page of the EULA. You will be prompted to specify whether you accept the agreement. Press **Y** on your keyboard if you agree, otherwise press **N**.

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

5. ESET Rogue Detection Sensor will start after installation is completed.

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

```
sudo service rdsensor status
```

7. The Rogue Detection Sensor log file can be found in Log files:

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

Mobile Device Connector installation - Linux

You can install Mobile Device Connector on a different server than the one on which your ESET PROTECT Server is running. For example, you can use this installation scenario to make Mobile Device Connector accessible from the internet to manage user's mobile devices at all times.

Perform the MDC component installation on Linux using a command in the Terminal. Make sure to meet all prerequisites. You can prepare an installation script and then execute it using `sudo`.

Required installation command parameters

There are many optional installation parameters, but some of them are required:

- Peer Certificate - There are two methods to get the ESET PROTECT Peer Certificate:

  • **Server assisted installation** - You need to provide ESET PROTECT Web Console administrator credentials (the installer will automatically download required certificates).

  • **Offline installation** - You need to provide a Peer Certificate (the Proxy certificate exported from ESET PROTECT). Alternatively, you can use your custom certificate.

  oFor a **Server assisted installation**, at least include:

```
--webconsole-password=
```

  oFor an **Offline installation**, include:

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

(The default Agent Certificate created during ESET PROTECT Server installation does not need a password.)

- HTTPS (Proxy) certificate:

  oIf you already have an HTTPS certificate:

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

  oTo generate a new HTTPS certificate:

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

- Connection to ESET PROTECT Server (name or IP address):

```
--hostname=
```

- Database connection:

  oFor a MySQL database include:

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

oFor a MS SQL database include:

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

Example of an installation script

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

```
sudo ./mdmcore-linux-x86_64-0.0.0.0.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

For a complete list of available parameters (print help message), use:

```
--help
```

ESET recommends 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.

Installer log

The installer log may be helpful for troubleshooting and you can find it in Log files.

After installation is complete, check to see if the Mobile Device Connector is running correctly by opening *https://your-mdm-hostname:enrollment-port* (for example, *https://eramdm:9980*) in your web browser. If the installation was successful, you will see the following message:

You can also use this URL to check the availability of the Mobile Device Connector server

from the internet (if configured in such a way) by visiting it from a mobile device. If you cannot reach the page, check your firewall and the configuration of your network infrastructure.

Mobile Device Connector prerequisites - Linux

The following prerequisites must be met in order to install Mobile Device Connector on Linux:

- A Database Server already installed and configured with a root account (a user account does not have to be created prior to installation, the installer can create the account).
- An ODBC Driver for the connection to the database server (MySQL / MS SQL) installed on the computer. See the chapter ODBC installation and configuration.

You should use `unixODBC_23` package (not the default `unixODBC`) in order for the MDC to connect to the MySQL database without any issues. This is especially true for SUSE Linux.

We recommend that you deploy your MDM component on a host device separate from the one ESET PROTECT Server is hosted on.

- MDMCore installation file set as an executable.

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

- After installation, verify that MDMCore service is running.

```
service eramdmcore status
```

- **We recommend that you use the latest OpenSSL version (1.1.1)**. The minimum supported version of OpenSSL is openssl-1.0.1e-30. There can be more versions of OpenSSL installed on one system in the same time. At least one supported version must be present on you system.

  oYou can use the command `openssl version` to show current default version.

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

If your MDM database on MySQL is too large (thousands of devices) the default `innodb_buffer_pool_size` value is too small. For more information on database optimizing see: https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html

Certificate requirements

- You will need an **SSL certificate** in *.pfx* format for secure communication over HTTPS. We recommend that you use a certificate provided by a third-party Certification Authority. Self-signed certificates (including certificates signed by the ESET PROTECT CA) are not recommended because not all mobile devices let users accept self-signed certificates.

- You need to have a certificate signed by CA and the corresponding private key, and utilize standard procedures (traditionally using OpenSSL), to merge those into one *.pfx* file:
  `openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`

This is the standard procedure for most servers which use SSL certificates.

• For Offline installation, you will also need a Peer certificate (the **Agent certificate** exported from ESET PROTECT). Alternatively, you can use your custom certificate with ESET PROTECT.

Apache HTTP Proxy installation - Linux

ESET Management Agents can connect to the the ESET PROTECT Server via Apache HTTP Proxy. Read more about how the proxy for ESET Management Agents works.

The Apache HTTP Proxy is commonly distributed as a `apache2` or `httpd` package.

Choose the installation steps for Apache HTTP Proxy according to the Linux distribution you use on your server. If you want to use the Apache to cache also results from ESET Dynamic Threat Defense, see also the related documentation.

Linux installation (distribution generic) for Apache HTTP Proxy

1. Install Apache HTTP Server (at least version 2.4.10).

2. Verify that the following modules are loaded:

```
access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile,
authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk
```

3. Add the caching configuration:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. If the directory */var/cache/apache2/mod_cache_disk* does not exist, create it and assign Apache privileges (r,w,x).

5. Add Proxy configuration:

```
AllowCONNECT 443 563 2222 8883 53535

ProxyRequests On
ProxyVia On

CacheLock on
CacheLockMaxAge 10
ProxyTimeOut 900

SetEnv proxy-initial-not-pooled 1

<VirtualHost *:3128>
ProxyRequests On
</VirtualHost>

<VirtualHost *:3128>
ServerName r.edtd.eset.com

<If "%{REQUEST_METHOD} == 'CONNECT'">
Require all denied
</If>

ProxyRequests Off
CacheEnable disk /
SSLProxyEngine On

RequestHeader set Front-End-Https "On"
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=10
ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On
</VirtualHost>

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. By default, port 2222 is used for communication with the ESET Management Agent. If you changed the port during installation, use the changed port number. Change 2222 in the line: `AllowCONNECT 443 563 2222 8883 53535` to your port number.

7. Enable the added caching proxy and configuration (if configuration is in the main Apache configuration file, you can skip this step).

8. If necessary, change listening to your desired port (port 3128 is set by default).

9. Optional basic authentication:

oAdd authentication configuration to the proxy directive:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

oCreate a password file using `/etc/httpd/.htpasswd -c`

oManually create a file named group.file with `usergroup:username`

10. Restart the Apache HTTP Server.

Ubuntu Server and other Debian-based Linux distributions installation of Apache HTTP Proxy

1. Install the latest version of Apache HTTP Server from apt repository:

```
sudo apt-get install apache2
```

2. Execute the following command to load the required Apache modules:

```
sudo a2enmod access_compat auth_basic authn_core authn_file authz_core\

authz_groupfile authz_host proxy proxy_http proxy_connect cache cache_disk
```

3. Edit the Apache caching configuration file:

```
sudo vim /etc/apache2/conf-available/cache_disk.conf
```

and copy/paste the following configuration:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. This step should not be required, but if the caching directory is missing, run following commands:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. Edit the Apache proxy configuration file:

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

and copy/paste the following configuration:

```
AllowCONNECT 443 563 2222 8883 53535

ProxyRequests On
ProxyVia On

CacheLock on
CacheLockMaxAge 10
ProxyTimeOut 900

SetEnv proxy-initial-not-pooled 1

<VirtualHost *:3128>
ProxyRequests On
</VirtualHost>

<VirtualHost *:3128>
        ServerName r.edtd.eset.com

<If "%{REQUEST_METHOD} == 'CONNECT'">
Require all denied
</If>

ProxyRequests Off
CacheEnable disk /
SSLProxyEngine On

RequestHeader set Front-End-Https "On"
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=10
ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On
</VirtualHost>

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. By default, port 2222 is used for communication with the ESET Management Agent. If you changed the port during installation, use the changed port number. Change 2222 in the line: `AllowCONNECT 443 563 2222 8883 53535` to your port number.

7. Enable the configuration files you edited in earlier steps:

```
sudo a2enconf cache_disk.conf proxy.conf
```

8. Switch the listening port of Apache HTTP Server to 3128. Edit the file */etc/apache2/ports.conf* and replace `Listen 80` with `Listen 3128`.

9. Optional basic authentication:

```
sudo vim /etc/apache2/mods-enabled/proxy.conf
```

oCopy/paste authentication configuration before `</Proxy>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

```
oInstall apache2-
utils and create a new password file (for example username: user, group: usergroup):

sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user

oCreate a file called group:

sudo vim /etc/apache2/group.file

and copy/paste the following line:

usergroup:user
```

10. Restart the Apache HTTP Server using the following command:

```
sudo service apache2 restart
```

Forwarding for ESET communication onlyTo allow forwarding of ESET communication only, remove the following:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

And add the following:

```
<Proxy *>
Deny from all
</Proxy>

#*.eset.com:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#*.eset.eu:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#*.eset.systems:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#Antispam module (ESET Mail Security only):
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#Services (activation)
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(edf-pcs.cloudapp.net|edf-pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#ESET servers accessed directly via IP address:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(91.228.165.|91.228.166.|91.228.167.|38.90.226.)([0-9]+)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#AV Cloud over port 53535
<ProxyMatch ^.*e5.sk.*$>
Allow from all
</ProxyMatch>
```

Forwarding for all communication

To allow forwarding of all communication, add the following:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

and remove the following:

```
<Proxy *>
Deny from all
</Proxy>

#*.eset.com:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#*.eset.eu:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#*.eset.systems:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#Antispam module (ESET Mail Security only):
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#Services (activation)
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(edf-pcs.cloudapp.net|edf-pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#ESET servers accessed directly via IP address:
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(91.228.165.|91.228.166.|91.228.167.|38.90.226.)([0-9]+)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>

#AV Cloud over port 53535
<ProxyMatch ^.*e5.sk.*$>
Allow from all
</ProxyMatch>
```

Proxy chaining (all traffic)

ESET PROTECT does not support proxy chaining when proxies require authentication. You can use your own transparent web proxy solution, however there may be additional configuration required beyond what is mentioned here. Add the following to the proxy configuration (password is working only on child proxy):

```
<VirtualHost *:3128>
ProxyRequests On
ProxyRemote * http://IP_ADDRESS:3128
</VirtualHost>
```

When using Proxy chaining on the ESET PROTECT Virtual Appliance, the SELinux policy must be modified. Open the terminal on the ESET PROTECT VA and run the following command:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
```

Configure the HTTP Proxy for a high number of clients

If you use 64-bit Apache HTTP Proxy, you can increase the thread limit for your Apache HTTP Proxy. Edit the configuration file *httpd.conf*, inside your Apache HTTP Proxy folder. Find the following settings in the file and update the values to match your number of clients.

Substitute the example value of `5000` with your number. The maximum value is `32000`.

```
ThreadLimit 5000

ThreadsPerChild 5000
```

Do not change the rest of the file.

Configure the Apache HTTP Proxy to forward Agent-Server connections

1.On the proxy machine open the file

i.Debian distributions
`/etc/apache2/mods-available/proxy.conf`

ii.Red Hat distributions
`/etc/httpd/conf/httpd.conf`

2.Add the following line to the end of the file:
`AllowCONNECT 443 563 2222 8883 53535`

3.On the proxy machine open the file

i.Debian distributions
`/etc/apache2/apache2.conf`

ii.Red Hat distributions
`/etc/httpd/conf/httpd.conf`

4.Find the line:
`Listen 80`
and change it to
`Listen 3128`

5.If you have added restrictions for IP addresses in your proxy configuration (step 1), you have to allow access to your ESET PROTECT Server:

Add a separate `ProxyMatch` segment:
I.The address which your Agents use to connect to the ESET PROTECT Server.

II.All other possible addresses of your ESET PROTECT Server (IP, FQDN)
(add the whole below code; IP address 10.1.1.10 and hostname `hostname.example` are only examples to be substituted by your addresses. You can also generate the `ProxyMatch` expression in this Knowledgebase article.)

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

6.Restart the *Apache HTTP Proxy* service.

SELinux setting

When using Proxy on the ESET PROTECT Virtual Appliance, the SELinux policy must be modified (some other Linux distributions may have the same requirement). Open the terminal on the ESET PROTECT VA and run the following commands:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1

sudo semanage port -a -t http_port_t -p tcp 2222
```

Squid HTTP Proxy installation on Ubuntu Server

You can use the Squid proxy instead of Apache on the Ubuntu Server. To install and configure Squid on the Ubuntu Server (and similar Debian-based Linux distributions), follow the steps below:

1. Install the Squid3 package:

```
sudo apt-get install squid3
```

2. Edit the Squid configuration file */etc/squid3/squid.conf* and replace:

```
#cache_dir ufs /var/spool/squid3 100 16 256
```

with:

```
cache_dir ufs /var/spool/squid3 3000 16 256 max-size=200000000
```

- You can change the total cache size (3000 MB in the example) and the number of first-level sub-directories (16 in the example) and second-level sub-directories (256 in the example) in the cache directory.
- Parameter `max-size` defines the maximum cached file size in bytes.

3. Stop the squid3 service.

```
sudo service squid3 stop
sudo squid3 –z
```

4. Edit the Squid configuration file again and add `http_access allow all` before `http_access deny all` to allow all clients to access the proxy.

5. Restart the squid3 service:

```
sudo service squid3 restart
```

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 downloads detection engine updates and other program modules only, it does not download PCUs (Program Component Updates) and ESET LiveGrid® data. It can also create a full offline repository. Alternatively, you can upgrade products individually.

Prerequisites

• 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 products for Windows - You can update them remotely using HTTP or a shared folder.

oESET security products 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 product.

• You must have a valid Offline license file that includes the Username and Password. When generating a license file, be sure to select the check box next to **Include Username and Password**. Also, you must enter a license **Name**. An offline license file is needed for the activation of the Mirror Tool and generation of the update mirror.

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
```

All filters are case sensitive.

--updateServer	When you use it, you must specify the full URL of the update server.
--offlineLicenseFilename	You must specify a path to your offline license 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 Knowledgebase article.
--mirrorFileFormat	Before using the `--mirrorFileFormat` parameter, ensure that you environment does not contain both older (6.5 and older) and newer (6.6. and later) ESET security product versions. The incorrect usage of this parameter may result in incorrect updates of your ESET security products. You can specify which type of update files will be downloaded. Possible values (case sensitive): • dat - Use this value if you have environment only with ESET security product versions 6.5 and older. • dll - Use this value if you have environment only with ESET security product versions 6.6 and later. The parameter is ignored when creating a mirror for legacy products (ep4, ep5).

--compatibilityVersion	This optional parameter applies to the Mirror Tool distributed with ESET PROTECT 8.1 and later. The Mirror Tool will download update files compatible with ESET PROTECT repository version you specify in the parameter argument in format `x.x` or `x.x.x.x`, for example: `--compatibilityVersion 9.0` or `--compatibilityVersion 8.1.13.0`.

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

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

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.

--filterFilePath

Use this optional parameter to filter ESET security products based on a text file in *JSON* format placed in the same folder as Mirror Tool, for example: `--filterFilePath filter.txt`).

Filter configuration description:

The configuration file format for product filtering is *JSON* with the following structure:

- root *JSON* object:

o`use_legacy` (boolean, optional) - if true, legacy products will be included.

o`defaults` (*JSON* object, optional) - defines filter properties that will be applied to all products.

■`languages` (string) - Specify ISO language codes of languages to include, for example for French type "fr_FR". Other languages codes are in the table below. To select more languages, separate them by a comma and a space, for example: "en_US", "zh_TW", "de_DE"

■`platforms` (string) - platfoms to include (`x64`, `x86`, `arm64`).

> Use the `platforms` 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 products will fail to install on 32-bit computers.

■`os_types` (string) - OS types to include.

o`products` (list of JSON objects, optional) - filters to apply to specific products - override `defaults` for specified products. The objects have the following properties:

■`app_id` (string) - required if `name` is not specified.

■`name` (string), required if `app_id` is not specified.

■`version` (string) - specifies version or range of versions to include.

■`languages` (string) - ISO language codes of languages to include (see the table below).

■`platforms` (string) - platforms to include (`x64`, `x86`).

■`os_types` (string) - OS types to include.

> To determine appropriate values for the fields, run Mirror Tool in dry run mode and find the relevant product in the created CSV file.

Version string format descriptions

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`).

Version string can have one of the two following formats:

- [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))

oSelects versions greater/smaller or equal/less or equal/equal than the version specified.

- <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))

oSelects versions that are greater than or equal to the lower bound and less than or equal to the higher bound.

Comparisons are done numerically on each part of the version number, left to right.

JSON example

```
{
"use_legacy": true,
"defaults": {
"languages": [ "en_US" ],
"platforms": [ "x64", "x86" ]
},
"products": [
{
"app_id": "com.eset.apps.business.ees.windows",
"version": "7.1.0.0 - 8.0.0.0"
},
{
"app_id": "com.eset.apps.business.eea.windows",
"version": ">7.1.0.0"
}
]
}
```

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

--dryRun	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. You can use this parameter without mandatory parameters `--intermediateRepositoryDirectory` and `--outputRepositoryDirectory`, for example: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. 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`. If you use the `--dryRun` parameter and also `--intermediateRepositoryDirectory` and `--outputRepositoryDirectory` parameters, the Mirror Tool does not clear the *outputRepositoryDirectory*.
--listUpdatableProducts	List all ESET products for which the Mirror Tool can download module updates (unless `--excludedProducts` is used). The parameter is available from Mirror Tool versions: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

The Mirror Tool creates a structure of folders different from what Endpoint mirror does. Each folder holds update files for a group of products. You have to specify the full path to the correct folder in the update settings of the product using the mirror.
For example, to update the ESET PROTECT 9 from the mirror set the Update server to (according to your HTTP server root location):
`http://your_server_address/mirror/eset_upd/era6`
Note: The `era6` mirror folder is common for these ESET remote management solutions: ERA 6, ESMC 7, ESET PROTECT.

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 products, 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
```

ESET recommends 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 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.

Failover Cluster - Linux

The following refers to ESET PROTECT installation and configuration on a Red Hat high-availability cluster.

Linux Cluster Support

ESET PROTECT Server components can be installed on Red Hat Linux 7 cluster and later. Failover Cluster is only supported in active/passive mode with the cluster manager `rgmanager`.

Prerequisites

• Active/passive cluster must be installed and configured. Only one node can be active at a time, other nodes must be on standby. Load balancing is not supported.

• Shared storage - iSCSI SAN, NFS and other solutions are supported (any technology or protocol which provides block based or file based access to shared storage, and makes the shared devices appear like locally attached devices to the operating system). Shared storage must be accessible from each active node in the cluster, and the shared file system must be properly initialized (for example, using the EXT3 or EXT4 file system).

• The following HA add-ons are required for system management:

  ■`rgmanager`

  ■`Conga`

• `rgmanager` is the traditional Red Hat HA cluster stack. It is a mandatory component.

• The **Conga** GUI is optional. The Failover Cluster can be managed without it, however we recommend that you install it for best performance. In this guide we assume that it is installed.

• **Fencing** must be properly configured in order to prevent data corruption. The cluster administrator must configure fencing if it is not already configured.

If you do not already have a cluster running, you can use the following guide to set up a high-availability Failover Cluster (active/passive) on Red Hat: Red Hat Enterprise Linux 7 Cluster Administration.

Scope

ESET PROTECT components that can be installed on a **Red Hat Linux** HA cluster:

- ESET PROTECT Server with ESET Management Agent - ESET Management Agent must be installed, otherwise the ESET PROTECT cluster service will not run.

Installation of the ESET PROTECT Database on a cluster is supported only when the cluster is provided by the SQL service and ESET PROTECT is connecting to a single database host address.

The following installation example is for a 2-node cluster. However, you can install ESET PROTECT on a multi-node cluster using this example as a reference only. The cluster nodes in this example are named **node1** and **node2**.

Installation steps

1. Install ESET PROTECT Server on node1.

   - Please note that the hostname in the Server certificate must contain the external IP (or hostname) of the cluster's interface (not local IP or hostname of the node).

2. Stop and disable the ESET PROTECT Server Linux services using the following commands:

```
service eraserver stop
chkconfig eraserver off
```

3. Mount shared storage to node1. In this example, the shared storage is mounted to */usr/share/erag2cluster*.

4. In */usr/share/erag2cluster*, create the following directories:

/usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server

5. Move recursively the following directories to the destinations shown below (source > destination):

/etc/opt/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator*
/opt/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/opt/eset/RemoteAdministrator*
/var/log/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/var/log/eset/RemoteAdministrator*
/var/opt/eset/RemoteAdministrator/Server	*/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator*

6. Create symbolic links (this may require to create new folders manually):

```
ln -s /usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator/Server /etc/opt/eset/RemoteAdministrator/Server
ln -s /usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server /opt/eset/RemoteAdministrator/Server
ln -s /usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server /var/log/eset/RemoteAdministrator/Server
ln -s /usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server /var/opt/eset/RemoteAdministrator/Server
```

7. Copy the `eracluster_server` script found in the setup directory of ESET PROTECT Server to */usr/share/cluster*. The scripts do not use the*.sh* extension in the setup directory.

```
cp /opt/eset/RemoteAdministrator/Server/setup/eracluster_server /usr/share/cluster/eracluster_server.sh
```

8. Unmount the shared storage from node1.

9. Mount the shared storage to the same directory on node2 as you mounted to on node1 (*/usr/share/erag2cluster*).

10. On node2, create the following symbolic links:

```
ln -s /usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator/Server /etc/opt/eset/RemoteAdministrator/Server
ln -s /usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server /opt/eset/RemoteAdministrator/Server
ln -s /usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server /var/log/eset/RemoteAdministrator/Server
ln -s /usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server /var/opt/eset/RemoteAdministrator/Server
```

11. Copy the `eracluster_server` script found in the setup director of ESET PROTECT Server to */usr/share/cluster*. The scripts do not use the *.sh* extension in the setup directory.

```
cp /opt/eset/RemoteAdministrator/Server/setup/eracluster_server /usr/share/cluster/eracluster_server.sh
```

The next steps are performed in Conga Cluster Administration GUI:

12. Create a **Service Group**, for example PROTECTService.

The ESET PROTECT cluster service requires three resources: IP address, file system and script.

13. Create the necessary service resources.

    Add an IP address (external cluster address where Agents will connect), file system and Script resources.
    The file system resource should point to the shared storage.
    The mount point of the file system resource should be set to */usr/share/erag2cluster*.
    The "Full Path to Script File" parameter of the Script resource should be set to */usr/share/cluster/eracluster_server* .

14. Add the above resources to the PROTECTService group.

After the Server cluster is successfully set up, install ESET Management Agent on both nodes on the local disk (not on the shared cluster disk). When using the `--hostname=` command, you must specify the external IP address or hostname of the cluster's interface (not localhost!).

Step-by-step ESET PROTECT Server 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.

> ### Installation instructions for selected Linux distributions
> You can follow our Knowledgebase articles with distribution-specific instructions:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

Before installation

1. Verify that the database server is present in your network and make sure 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.

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 as shown in the ESET PROTECT Web Console installation topic. If you experience problems with the HTTPS connection to the ESET PROTECT Web Console, see our article on HTTPS/SSL connection set up.

6. Install ESET Management Agent on the server machine.

ESET recommends 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.

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.

macOS is supported as a client only. The ESET Management Agent and ESET products for macOS can be installed on macOS. However, ESET PROTECT Server cannot be installed on macOS.

Agent installation - macOS

These steps apply when performing a local installation of the Agent.

1. Make sure all **prerequisites** are met:

   • 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).

Should you experience problems when deploying ESET Management Agent remotely (the Server task **Agent deployment** ends with a failed status) please refer to Agent deployment troubleshooting.

2. Get the installation file (standalone agent installer *.dmg*) from the ESET download site or your system administrator.

3. Double-click the *Agent-MacOSX-x86_64.dmg* file and then double click the *.pkg* file to start the installation.

4. Proceed with the installation. When asked, enter 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 use HTTP Proxy for Agent - Server connection.

This proxy setting is only 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**: enter 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.

5. 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 the initialization of the Agent.

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

7. 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 Installers 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 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.Enter 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.Enter the tcp protocol in the **Protocol** field in the following format: _tcp.

6.Enter the port 2222 in the **Port number** field.

7.Enter 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.

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

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

On 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 product installers (for example, ESET Endpoint Security)

On 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.

2. Install the JDK package.

3. Install ESET PROTECT on Windows using the All-in-one installer. Choose **Activate later** during installation.

4. Activate ESET PROTECT with an offline license.

5. Deploy ESET Management Agent to computers in your offline environment via agent live installer. Modify the installation script to use the new URL to access the agent installation package from the shared network folder.

6. Deploy ESET security products 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 license.

8. Disable ESET LiveGrid®.

We highly recommend that you keep the offline ESET infrastructure updated by using a local update repository. Update ESET security product modules regularly. If 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, see Upgrade ESET PROTECT components in an offline environment.

Upgrade, migration and reinstallation procedures

There are different ways to upgrade, migrate and reinstall your ESET PROTECT Server and other ESET PROTECT components.

Make sure that you have a supported operating system before upgrading to ESET PROTECT 9.0. ESET PROTECT Server component version 9.0 is not compatible with 32-bit machines (x86 architecture). Upgrading a 32-bit Server machine from version 7.0 to 9.0 will fail.
• If you have already run the upgrade and your system is not working, reinstall manually all ESET PROTECT components to the original version.
• Before the upgrade, migrate your current ESET PROTECT to a 64-bit machine, and after successful migration, you can run the upgrade task.
If you have an older unsupported database installed (MySQL 5.5 or MS SQL 2008/2012), upgrade your database to a compatible database version before upgrading the ESET PROTECT Server.
ESET PROTECT 9.0 uses LDAPS as the default protocol for Active Directory synchronization. If you upgraded from versions 7.0-7.1 on a Windows machine to ESET PROTECT 9.0 and used the Active Directory synchronization, synchronization tasks will fail in ESET PROTECT 9.0.

Upgrade from ERA 5 or 6.5

The direct upgrade is not supported - see Migration from ERA 5.x or Upgrade from ERA 6.x.

Upgrade from ESMC 7.x to the ESET PROTECT version 9.0

Select one of the upgrade procedures:

Components Upgrade task in the Web Console	Windows/Linux	
ESET PROTECT 9.0 All-in-one installer	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 MS SQL database and Apache Tomcat).
Manual component-based upgrade	Linux	Linux instructions for advanced users.

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.

Migrate or reinstall ESET PROTECT 9 from one server to another

Migrate from one server to another or reinstall ESET PROTECT Server.

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.

Other procedures

Change an IP address or hostname on an ESET PROTECT Server.

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. Carefully review the directions here before upgrading.

If the components upgrade fails on a machine running the ESET PROTECT Server or Web Console, you may not be able to log into the Web Console remotely. We recommend that you configure physical access to the server machine before performing this upgrade. If you cannot arrange for physical access to the machine, make sure you can log onto it with administrative privileges using a remote desktop. We recommend that you back up your ESET PROTECT Server and Mobile Device Connector databases before performing this operation. To back up your Virtual Appliance, create a snapshot or clone your virtual machine.

Are you upgrading from ESMC Virtual Appliance?

The ESET PROTECT Server instance is installed on a failover cluster?

If your ESET PROTECT Server instance 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).

Important instructions before upgrading Apache HTTP Proxy on Microsoft Windows

If you are using Apache HTTP Proxy and have custom settings in your *httpd.conf* file (such as your username and password), back up your original *httpd.conf* file (located in *C:\Program Files\Apache HTTP Proxy\conf*). If you are not using custom settings, you do not need to back up the *httpd.conf* file. Upgrade to the latest version of Apache HTTP Proxy by any of the methods referenced in Upgrading Apache HTTP Proxy.

After you have successfully upgraded Apache HTTP Proxy on Windows and you have had custom settings in your original *httpd.conf* file (such as username and password), copy the settings from the backup *httpd.conf* file and apply your custom settings only in your new *httpd.conf* file. Do not use your original *httpd.conf* file with the upgraded version of Apache HTTP Proxy, it will not work correctly. Copy only your custom settings from it and use the new *httpd.conf* file. Alternatively, you can customize your new *httpd.conf* file manually, as described in Apache HTTP Proxy installation - Windows.

Important instructions before upgrading Apache HTTP Proxy on Virtual Appliance

If you are using **Apache HTTP Proxy** and have custom settings in your *httpd.conf* file (such as your username and password), back up your original *httpd.conf* file (located in */opt/apache/conf/*) and then run the **ESET PROTECT Components Upgrade** task to upgrade **Apache HTTP Proxy**. If you are not using custom settings, it is not necessary to create a backup of *httpd.conf*.
After the Components Upgrade task has completed successfully, run the following command. Assign it to the machine with Apache HTTP Proxy installed. Use the Run Command Client task; it updates the *httpd.conf* file (this is required for the upgraded version of Apache HTTP Proxy to run correctly):

```
wget https://help.eset.com/protect_install/90/apache/httpd.conf -O\
 /tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\
 /opt/apache/conf/httpd.conf
```

If Apache HTTP Proxy runs on your VA machine, you can run the same command directly from within the ESET PROTECT Virtual Appliance's console. Another option is to replace the Apache HTTP Proxy configuration file *httpd.conf* manually.

If you have custom settings in your original *httpd.conf* file (such as your username and password), copy the settings from the backup *httpd.conf* file and add only the custom settings to the new *httpd.conf* file. Do not use your original *httpd.conf* file with the upgraded version of Apache HTTP Proxy, it will not work correctly. Copy only your custom settings from it and use the new *httpd.conf* file. Alternatively, you can customize your new *httpd.conf* file manually. See the detailed settings in Apache HTTP Proxy installation - Linux.

You can upgrade to ESET PROTECT 9.0 only from ESMC version 7.0 and later.
ESET PROTECT 9 automatically notifies you when a new version of the ESET PROTECT Server is available.
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 ESMC/ESET PROTECT database. If you have an older unsupported database installed (MySQL 5.5 or MS SQL 2008/2012), upgrade your database to a compatible database version before upgrading the ESET PROTECT Server.

Make sure that you have a supported operating system before upgrading to ESET PROTECT 9.0.
ESET PROTECT Server component version 9.0 is not compatible with 32-bit machines (x86 architecture). Upgrading a 32-bit Server machine from version 7.0 to 9.0 will fail.
• If you have already run the upgrade and your system is not working, reinstall manually all ESET PROTECT components to the original version.
• Before the upgrade, migrate your current ESET PROTECT to a 64-bit machine, and after successful migration, you can run the upgrade task.
ESET PROTECT 9.0 uses LDAPS as the default protocol for Active Directory synchronization. If you upgraded from versions 7.0-7.1 on a Windows machine to ESET PROTECT 9.0 and used the Active Directory synchronization, synchronization tasks will fail in ESET PROTECT 9.0.
To upgrade ESET security products, run the Software Install task using the latest installer package to install the latest version over your existing product.

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 Apache 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 directly from the cache.

3. After the computers with upgraded ESET Management Agent are successfully connecting 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 9.0 supports the automatic upgrade of ESET Management Agent 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

oApache Tomcat is not upgraded during the ESET PROTECT Web Console upgrade via the Components Upgrade task.
oESET PROTECT Web Console upgrade does not work if Apache Tomcat was installed in a custom location.
oIf 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.

- ESET PROTECT Mobile Device Connector.

Components that require manual upgrade:

- Apache Tomcat (we strongly recommend that you keep Apache Tomcat up-to-date, see Upgrading Apache Tomcat)
- Database Server
- Apache HTTP Proxy (can be achieved using All-in-one installer, see Upgrading Apache HTTP Proxy)
- ESET Rogue Detection Sensor - Use the Software Install task for the upgrade. Alternatively, install a newer version over the older version (follow the installation instructions for Windows or Linux). If you installed RD Sensor with ESMC 7.2 and later, you do not need to upgrade it, as there are no new RD Sensor releases.

Troubleshooting

- Verify whether you can access the ESET PROTECT repository from an upgraded computer.
- Re-running the ESET PROTECT Components Upgrade task will not work if there is at least one component already upgraded to the newer version.
- If there is no clear reason for the failure, you can 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 9.0 All-in-one installer to upgrade

Use the ESET PROTECT 9.0 All-in-one installer to upgrade ESMC 7.x or an older ESET PROTECT version to the latest ESET PROTECT 9.0.

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 MS SQL database and Apache Tomcat).

The ESET PROTECT 9.0 All-in-one installer installs Microsoft SQL Server Express 2019 by default.

- If you use an older Windows edition (Server 2012 or SBS 2011), Microsoft SQL Server Express 2014 will be installed by default.
- The installer automatically generates a random password for database authentication (stored in *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Microsoft SQL Server Express has a 10 GB size limit for each relational database. We do not recommend using Microsoft SQL Server Express:
- In enterprise environments or large networks.
- If you want to use ESET PROTECT with ESET Enterprise Inspector.

You can upgrade to ESET PROTECT 9.0 only from ESMC version 7.0 and later.
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 ESMC/ESET PROTECT database. If you have an older unsupported database installed (MySQL 5.5 or MS SQL 2008/2012), upgrade your database to a compatible database version before upgrading the ESET PROTECT Server.

Make sure that you have a supported operating system before upgrading to ESET PROTECT 9.0.
ESET PROTECT Server component version 9.0 is not compatible with 32-bit machines (x86 architecture). Upgrading a 32-bit Server machine from version 7.0 to 9.0 will fail.
- If you have already run the upgrade and your system is not working, reinstall manually all ESET PROTECT components to the original version.
- Before the upgrade, migrate your current ESET PROTECT to a 64-bit machine, and after successful migration, you can run the upgrade task.

ESET PROTECT 9.0 uses LDAPS as the default protocol for Active Directory synchronization. If you upgraded from versions 7.0-7.1 on a Windows machine to ESET PROTECT 9.0 and used the Active Directory synchronization, synchronization tasks will fail in ESET PROTECT 9.0.

1. Run *Setup.exe*.
2. Select the language and click **Next**.
3. Select **Upgrade all components** and click **Next**.

4. Read the **End-user license agreement**, accept it 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, make sure 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 ESMC or an older ESET PROTECT version, re-create it for ESET PROTECT 9.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT version.

Apache HTTP Proxy upgrade limitations

The All-in-one installer overwrites *httpd.conf* and saves the original configuration to *httpd.conf.old*. To keep the custom Apache HTTP Proxy configuration, back up the configuration and reuse it.

6.Follow the **Pre-installation checkup** to make sure your system meets all prerequisites.

7.Click **Upgrade** to start the ESET PROTECT upgrade. The upgrade may take some time, depending on your system and network configuration.

8.When the upgrade completes, click **Finish**.

9.After upgrading ESET PROTECT, upgrade ESET Management Agent on managed computers using the Components Upgrade task. ESET PROTECT 9.0 supports the automatic upgrade of ESET Management Agent on managed computers.

Migration from ERA 5.x

You cannot directly upgrade or migrate ERA 5.x to ESET PROTECT 9.0.

If you have ERA 5.x installed, perform these actions:

1.Migrate from ERA 5.x to ESMC 7.2

2.Upgrade ESMC 7.2 to ESET PROTECT 9.0

Upgrade from ERA 6.5

You cannot directly upgrade to ESET PROTECT 9.0.

If you have ERA 6.5 installed, perform these actions:

1.Upgrade ERA 6.5 to ESET PROTECT 8.1.

2. Upgrade ESET PROTECT 8.1 to ESET PROTECT 9.0.

Migration from one server to another

There are several ways to migrate ESET PROTECT 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 - Database migration can only be performed between two similar database types (from MySQL to MySQL or from MS SQL to MS SQL) and two similar versions of ESET PROTECT.

Clean Installation - same IP address

The objective of this procedure is to install an entirely new instance of 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/MDM 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.

View the image larger

❑ **On your current (old) ESET PROTECT Server:**

If the client computers are encrypted with ESET Full Disk Encryption, decrypt them before migrating to another ESET PROTECT Server to avoid the loss of recovery data. After the migration, you can encrypt the client computers again using the new ESET PROTECT Server.

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.

❑ **On your new ESET PROTECT Server:**

To use a new ESET PROTECT Server with the same IP address, make sure 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.

1. Install ESET PROTECT Server/MDM 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 your Server settings to use the Server certificate from your old ESET PROTECT Server.

5. Import all required ESET licenses to ESET PROTECT.

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.

❑ **Old ESET PROTECT Server/MDM uninstallation:**

Once you have everything running correctly on your new ESET PROTECT Server, carefully decommission your old ESET PROTECT Server/MDM using our step-by-step instructions.

Migrated Database - same/different IP address

The objective of this procedure is to install an entirely new instance of 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 prior to installation.

• Migrating databases is only supported between identical database types (from MySQL to MySQL or from MS SQL to MS SQL).
• When migrating a database, you must migrate between instances of the same ESET PROTECT 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 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/Backup 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.

❑ **On your new ESET PROTECT Server:**

To use a new ESET PROTECT Server with the same IP address, make sure 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.

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/MDM 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** ▯ **Server 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.

❑ **Old ESET PROTECT Server/MDM uninstallation:**

Once you have everything running correctly on your new ESET PROTECT Server, carefully decommission your old ESET PROTECT Server/MDM using our step-by-step instructions.

Database Server Backup/Upgrade and ESET PROTECT Database Migration

ESET PROTECT uses a database to store client data. The following sections detail the backup, upgrade and migration of the ESET PROTECT Server (or ESMC Server) database or MDM 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 9.0 All-in-one installer installs Microsoft SQL Server Express 2019 by default.

oIf you use an older Windows edition (Server 2012 or SBS 2011), Microsoft SQL Server Express 2014 will be installed by default.

oThe installer automatically generates a random password for database authentication (stored in *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Microsoft SQL Server Express has a 10 GB size limit for each relational database. We do not recommend using Microsoft SQL Server Express:
• In enterprise environments or large networks.
• If you want to use ESET PROTECT with ESET Enterprise Inspector.

• If you have an older unsupported database installed (MySQL 5.5 or MS SQL 2008/2012), upgrade your database to a compatible database version before upgrading the ESET PROTECT Server.

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 (for example, Windows SBS / Essentials). We recommend that you install ESET PROTECT on a different server or do not select the SQL Server Express component during installation (this requires you to use your existing SQL or MySQL Server to run the ESET PROTECT database).

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 MS SQL Server
- Migration process for MySQL Server

Database Server Backup and Restore

All ESET PROTECT 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 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 product name from ESET Security Management Center to ESET PROTECT.
- If you use ESET PROTECT Virtual Appliance, follow the VA database backup instructions.

MS SQL Backup examples

To backup an MS 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 MS SQL server instance. You can install ESET PROTECT Server on a custom named SQL instance (when using MS 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:

```
1.@ECHO OFF
2.SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'
  WITH NOFORMAT,INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHECKSUM, STATS=10"
3.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:

```
1. @ECHO OFF
2. SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'
   WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHECKSUM, STATS=10"
```

MS SQL restore

To restore a MS SQL database from a file, follow the example shown below:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -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
```

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
```

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 Microsoft SQL Server instance to a newer version for use with ESET PROTECT Server database:

1. Stop all running ESMC/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 Microsoft SQL Server instance.

2. Back up all relevant databases safely before proceeding.

3. Perform the database server upgrade:

Upgrade SQL Server:

Follow the Knowledgebase article for upgrading MS SQL Express database to the latest version. Alternatively, following the database vendor's instructions: https://msdn.microsoft.com/en-us/library/bb677622.aspx.

Upgrade MySQL Server:

- Upgrade from MySQL 5.5 to version 5.6
- Upgrade from MySQL 5.6 to version 5.7
- Upgrade from MySQL 5.7 to version 8

4. Start ESET PROTECT Server service and check trace logs to verify the database connection is working correctly.

Migration process for MS SQL Server

This migration process is the same for **Microsof 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 (or ESMC Server Service) or ESET PROTECT MDM Service.

Do not start ESET PROTECT Server or ESET PROTECT MDM 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 your 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. Right-click the **era_db** database, select **New Query** and run the query below to delete the contents of **tbl_authentication_certificate** table (otherwise, Agents may fail to connect to the new Server):

```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. 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.

16. Create a new SQL Server login (for ESET PROTECT Server/ESET PROTECT MDM) in the target

SQL Server with **SQL Server authentication** and map the login to a user in the restored database.

- oDo not enforce password expiration!
- oRecommended characters for usernames:
  - ■Lower-case ASCII letters, numbers and character underscore "_"
- oRecommended characters for passwords:
  - ■ASCII characters ONLY, including upper-case and lower-case ASCII letters, numbers, spaces, special characters
- oDo not use non-ASCII characters, curly braces {} or @
- oPlease 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.

17. 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**.

18. To enable the latest database server features, change the restored database **Compatibility level** to the newest one. Right-click the new database and open the database **Properties**.

> 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.

19. Make sure 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.

20. Connect the ESET PROTECT Server or MDM 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/5.6/en/copying-databases.html
- https://dev.mysql.com/doc/refman/5.6/en/mysqldump.html
- https://dev.mysql.com/doc/refman/5.6/en/mysql.html

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/MDM services.

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 */;"
```

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;"
```

Use the apostrophe character ' instead of " quotation marks on Linux systems.

7. Delete the contents of **tbl_authentication_certificate** table (otherwise, Agents may fail to connect to the new Server):

```
mysql --host TARGETHOST -u root -p "--execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. Connect the ESET PROTECT Server or MDM to the database.

Connect ESET PROTECT Server or MDM to a database

Follow the steps below on the machine where ESET PROTECT Server or ESET PROTECT MDM is installed to connect it to a database.

1. Stop the ESET PROTECT Server/MDM service.
2. Find *startupconfiguration.ini*
   - Windows:

Server:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration\startupconfiguration.ini
```

   - Linux:

Server:

/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

MDMCore:

/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini

3. Change the database connection string in ESET PROTECT Server/MDM *startupconfiguration.ini*

oSet the address and port of the new database server.

oSet new ESET PROTECT user name and password in the connection string.

The final result should look like:

- MS SQL:

```
DatabaseType=MSSQLOdbc
DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pwd={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

In the configuration above, please always 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 or ESET PROTECT MDM and verify that the service is running correctly.

Migration of MDM

This procedure aims to migrate your existing instance of ESET PROTECT MDM and **keep your existing ESET PROTECT MDM database**, including enrolled mobile devices. The migrated ESET PROTECT MDM will have **the same IP address/hostname** as the old ESET PROTECT MDM, and the database of the old ESET PROTECT MDM will be imported to the new MDM host before installation.

• Migrating databases is only supported between identical database types (from MySQL to MySQL or from MS SQL to MS SQL).
• When migrating a database, you must migrate between instances of the same ESET PROTECT 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 your current (old) ESET PROTECT MDM server:**

1. Create a backup of MDM configuration.

a)In **Computers**, click the MDM Server and select **Show Details**.

b)Click **Configuration** → **Request configuration**. You may need to wait some time (depending on your Agent connection interval) until the requested configuration is created.

c)Click the **ESET PROTECT Mobile Device Connector** and select **Open Configuration**.

d)Export the following items from the configuration to external storage:

- The exact Hostname of your MDM Server.
- Peer Certificates - The exported *.pfx* file will have the private key included.

If you are running ESET PROTECT MDM server on Linux, you need to export the HTTPS certificate from the MDM configuration policy:
I.Click **View** next to **HTTPS Certificate**.
II.Click **Download** and download the HTTPS certificate in PFX format.

e)Export the following certificates and tokens as well if present:

- The enrollment profile signing certificate.
- An APNS Certificate (export both APNS Certificate and APNS Private Key).
- Apple Device Enrollment Program (DEP) authorization token.

2. Stop the ESET PROTECT MDM service.

3. Export/Back up the ESET PROTECT MDM Database.

4. Turn off the current ESET PROTECT MDM machine.

Do not uninstall/decommission your old ESET PROTECT MDM yet.

❑ **On your new ESET PROTECT MDM Server:**

Make sure the network configuration on your new ESET PROTECT MDM server (the hostname you exported from the configuration of your "old" MDM server) matches that of your old ESET PROTECT MDM.

1. Install/Launch a supported ESET PROTECT MDM database.

2. Import/Restore the ESET PROTECT MDM database from your old ESET PROTECT MDM.

3. Install ESET PROTECT Server/MDM 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 MDM.

When installing ESET PROTECT MDM on Linux, use the HTTPS certificate from your backup.

4. Connect to the ESET PROTECT Web Console.

5. Restart the ESET PROTECT MDM service.

Managed mobile devices should now connect to your new ESET PROTECT MDM server using their original certificate.

❑ **Old ESET PROTECT Server/MDM uninstallation:**

Once you have everything running correctly on your new ESET PROTECT Server, carefully decommission your old ESET PROTECT Server/MDM using our step-by-step instructions.

Upgrade ESMC/ESET PROTECT installed in Failover Cluster on Windows

If you have ESMC/ESET PROTECT Server installed in a Failover Cluster environment on Windows, follow the steps below to upgrade to the latest ESET PROTECT:

Make sure you have a supported operating system.

1. Stop the ESMC/ESET PROTECT Server cluster Role in the Cluster Manager. Make sure the service (**ESET Security Management Center Server** or **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, make sure 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. Once 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 HTTP Proxy

Apache HTTP Proxy is a service that can be used in combination with ESET PROTECT to distribute updates to client computers and installation packages to the ESET Management Agents.

If you installed Apache HTTP Proxy earlier on Windows and wish to upgrade it to the most recent version, then you have two ways to accomplish the upgrade, either manually or via the All-in-one installer.

Upgrade Apache HTTP Proxy using the All-in-one installer (Windows)

If you downloaded the latest ESET PROTECT All-in-one installer, you can use this method to quickly upgrade Apache HTTP Proxy to the latest version. If you do not have the latest installer downloaded, use the manual Apache HTTP Proxy upgrade method.

1. Back up the following files:
   - *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*
   - *C:\Program Files\Apache HTTP Proxy\bin\password.file*
   - *C:\Program Files\Apache HTTP Proxy\bin\group.file*
2. Launch the All-in-one installer by double-clicking the *setup.exe* file and in the Welcome screen, click **Next**.
3. Select **Upgrade all components** and click **Next**.

4. Read the **End-user license agreement**, accept it and click **Next**.
5. In **Components**, review ESET PROTECT components that can be upgraded and click **Next**.

6. Follow the **Pre-installation checkup** to make sure your system meets all prerequisites.
7. Click **Upgrade** to start the ESET PROTECT upgrade. The upgrade may take some time, depending on your system and network configuration.
8. When the upgrade completes, click **Finish**.

> The All-in-one installer overwrites *httpd.conf* and saves the original configuration to *httpd.conf.old*. To keep the custom Apache HTTP Proxy configuration, back up the configuration and reuse it.

9. Test the connection to the Apache HTTP Proxy by accessing the following URL in your browser:

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

Troubleshooting

To troubleshoot an issue, check the Apache HTTP Proxy log files.

If there was custom configuration made to *httpd.conf* file in the previous installation of Apache HTTP Proxy, follow these steps:

1.Stop the **ApacheHttpProxy** service by opening an administrative command prompt and executing the following command:

```
sc stop ApacheHttpProxy
```

2.If you use a username/password to access your Apache HTTP Proxy (Apache HTTP Proxy installation topic), replace the following block of code:

```
<Proxy *>
 Deny from all
</Proxy>
```

with the following block of code (found in the backup of *httpd.conf*):

```
<Proxy *>
 AuthType Basic
 AuthName "Password Required"
 AuthUserFile password.file
 AuthGroupFile group.file
 Require group usergroup
 Order deny,allow
 Deny from all
 Allow from all
</Proxy>
```

3.If you had other customizations made to your *httpd.conf* file in place in your previous installation of Apache HTTP Proxy, manually copy those modifications from *httpd.conf.old* (or from the *httpd.conf* backup from step 1) to the new (upgraded) *httpd.conf* file.

4.Save your changes and start the **ApacheHttpProxy** service by executing the following command in an elevated command prompt:

```
sc start ApacheHttpProxy
```

Upgrade Apache HTTP Proxy manually (Windows)

To upgrade Apache HTTP Proxy to the most recent version, follow the steps below.

1. Back up the following files:
   - *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*
   - *C:\Program Files\Apache HTTP Proxy\bin\password.file*
   - *C:\Program Files\Apache HTTP Proxy\bin\group.file*

2. Stop the **ApacheHttpProxy** service by opening an admnistrative command prompt and executing the following command:

```
sc stop ApacheHttpProxy
```

3. Download the Apache HTTP Proxy installer file from ESET download site and extract its contents to *C:\Program Files\Apache HTTP Proxy*. During the extraction overwrite the existing files.

4. Navigate to *C:\Program Files\Apache HTTP Proxy\conf*, right-click *httpd.conf*, from the context menu and select **Open with** ▯ **Notepad**.

5. Add the following code at the bottom of *httpd.conf*:

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

6. If you set a username/password to access your Apache HTTP Proxy (Apache HTTP Proxy installation topic), replace the following block of code:

```
<Proxy *>
 Deny from all
</Proxy>
```

with this one (found in your backed-up *httpd.conf* file you backed up in step 1):

```
<Proxy *>
 AuthType Basic
 AuthName "Password Required"
 AuthUserFile password.file
 AuthGroupFile group.file
 Require group usergroup
 Order deny,allow
 Deny from all
 Allow from all
</Proxy>
```

If there were other customizations made to *httpd.conf* file in the previous installation of Apache HTTP Proxy, copy the configuration modifications from the backed-up *httpd.conf* file to the new (upgraded) *httpd.conf* file.

7. Save your changes and start the **ApacheHttpProxy** service by executing the following command in an administrative command prompt:

```
sc start ApacheHttpProxy
```

8. Update the version in the service description.

```
sc description ApacheHttpProxy "Apache/2.4.43"
```

9. Test the connection to Apache HTTP Proxy by accessing the following URL in your browser:

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

See the Apache HTTP Proxy log files if you need to troubleshoot an issue.

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, 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.

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 9.0 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.

1. 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, make sure 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 ESMC or an older ESET PROTECT version, re-create it for ESET PROTECT 9.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT version.

2. Download the ESET PROTECT All-in-one installer from the ESET website and unzip the downloaded file.

3. If you want to install the latest version of Apache Tomcat and the All-in-one installer contains an older 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.

4. To launch the All-in-one installer, double-click the *Setup.exe* file and click **Next** in the **Welcome** screen.

5. Select **Upgrade all components** and click **Next**.

6. After accepting the EULA, click **Next**.

7. 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**.

8. Select a Java installation on the computer. Apache Tomcat requires 64-bit Java/OpenJDK. If you have multiple Java versions installed on your system, we recommend that you uninstall older 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.

9. Click **Upgrade** to complete the upgrade and then click **Finish**.

10. 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**.

11. Connect to the ESET PROTECT Web Console and verify that the Web console loads correctly.

See also the additional Web Console configuration for enterprise solutions or low-performance systems.

Troubleshooting

If the Apache Tomcat upgrade fails, install your previous version 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.

Before upgrading

- Apache Tomcat requires 64-bit Java/OpenJDK. If you have multiple Java versions installed on your system, we recommend that you uninstall older 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.

How to upgrade

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 system tray.

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 newer 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 make sure the *keystoreFile* path is correct (update the path if you upgraded to a higher major version of Apache Tomcat):

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat folder]\.keystore"

9. Make sure 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 make sure **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.

See also 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 ESMC or an older ESET PROTECT version, re-create it for ESET PROTECT 9.0 after

upgrading to ensure that you have the latest Offline help matching your ESET PROTECT version.

Upgrade Apache Tomcat (Linux)

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

Before upgrading Apache Tomcat

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 newer version is available:

   a.Ensure that the newer version is supported.

   b.Back up the Tomcat configuration file */etc/tomcat7/server.xml*.

How to upgrade

1. Run the following command to stop the Apache Tomcat service (in some cases, the service name is `tomcat7`):

```
service tomcat stop
```

2. Upgrade Apache Tomcat and Java. Example package names below may differ from packages available in your Linux distribution repository.

Debian and Ubuntu distributions	sudo apt-get update sudo apt-get install openjdk-11-jdk tomcat9
CentOS and Red Hat distributions	yum update yum install java-1.8.0-openjdk tomcat
OpenSUSE	zypper refresh zypper install java-1_8_0-openjdk tomcat

3. Replace the */etc/tomcat9/server.xml* file with the *server.xml* file from your backup.

4. Open the *server.xml* file and make sure the *keystoreFile* path is correct.

5. Make sure the HTTPS connection for Apache Tomcat is configured correctly.

See also the additional Web Console configuration for enterprise solutions or low-performance systems.

After upgrading Apache Tomcat to a later major version (for example Apache Tomcat version 7.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 ESMC or an older ESET PROTECT version, re-create it for ESET PROTECT 9.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT version.

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 Server 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.

Upgrade ESMC/ESET PROTECT installed in Failover Cluster on Linux

If you have ESET PROTECT Server installed in a Failover Cluster environment on Linux and want to upgrade the installation to the latest ESET PROTECT, proceed with the steps below.

1. Disable *EraService* in Conga (Cluster Administration GUI) under **Service groups** and ensure that Agent and Server are stopped on both nodes.

2. Upgrade ESMC/ESET PROTECT Server on node1 by performing the following steps:

a)Mount the shared storage to this node.

b)Upgrade the Server component manually to latest version by executing the server installation script *server-linux-x86_64.sh* as `root` or `sudo`.

c)Replace the old cluster script located at `/usr/share/cluster/eracluster_server.sh` with the new one found in `/opt/eset/RemoteAdministrator/Server/setup/eracluster_server`. Do not change the filename of `eracluster_server.sh`.

d)Stop the ESET PROTECT Server service (`stop eraserver`) after the upgrade.

e)Disable ESET PROTECT Server autostart by renaming the following files:

i. `mv /etc/init/eraserver.conf /etc/init/eraserver.conf.disabled`

ii. `mv /etc/init/eraserver-xvfb.conf /etc/init/eraserver-xvfb.conf.disabled`

f)Unmount the shared storage from this node.

3. Repeat these steps to upgrade ESMC/ESET PROTECT Server on node2.

4. Start *EraService* in Conga (Cluster Administration GUI) under Service groups.

5. Upgrade Agent on all cluster nodes.

6. Check ESET PROTECT Web Console to see if all nodes are connecting and show as the latest version.

Uninstall ESET PROTECT Server and its components

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 product
- Decommission the old ESMC/ESET PROTECT/MDM 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 click **New Task**.

Alternatively, select multiple computers by selecting the corresponding check boxes and then click **Actions** → **New Task**.

3. Type a **Name** for the task.

4. From the **Task category** drop-down menu select **ESET PROTECT**.

5. From the **Task** drop-down menu select Stop Managing (Uninstall ESET Management Agent).

Once you uninstall the ESET Management Agent from the client computer, the device is no longer managed by ESET PROTECT:
• ESET security product may retain some settings after the ESET Management Agent has been uninstalled.
• If the Agent is password protected, you will not be able to uninstall it. 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 be abandoned. The **Running**, **Finished** or **Failed** execution status of this task may not be displayed accurately in ESET PROTECT Web Console depending on replication.
• After the Agent is uninstalled, you can manage your security product via the integrated 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, uninstall Agents on managed computers.
Before uninstalling Mobile Device Connector, read MDM iOS licensing functionality.

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. Accept the EULA 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 particular components.

See also Decommission the old ESMC/ESET PROTECT/MDM 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.

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 product

Uninstall the ESET Management Agent and ESET endpoint product locally or remotely via ESET PROTECT.

You can find the more detailed instructions for local uninstallation of ESET Management Agent and ESET Endpoint product in our Knowledgebase article.

If you want to remotely uninstall the ESET Endpoint product, make sure 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 enter 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\ Administrator\ Agent.app/Contents/Scripts/Uninstall.command ; exit;
```

3. Type your administrator password and press **Enter** if you are prompted to enter 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

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 product 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 enter 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 product 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 enter a password.

4. You will see the **Process completed** message when ESET Endpoint product has been uninstalled.

Uninstall ESET Endpoint product remotely via ESET PROTECT

To uninstall the ESET Management Agent remotely via ESET PROTECT, you can use one of these options:

- In **Computers**, click the client macOS computer, select **Show Details** → **Installed Applications** → select **ESET Endpoint Security** or **ESET Endpoint Antivirus** and click the **Uninstall** button.

- Use the **Software Uninstall** task.

Decommission the old ESMC/ESET PROTECT/MDM Server after migration to another server

Make sure your new ESET PROTECT Server/MDM is running and client computers and mobile devices are connecting to your new ESET PROTECT correctly.

There are two options when decommissioning your old ESMC/ESET PROTECT Server/MDM after migration to another server:

I. **Keep the server machine OS and reuse it**

1. Stop the old ESMC/ESET PROTECT Server service.

2. Delete (`DROP DATABASE`) the old ESMC/ESET PROTECT Server database instance (MS SQL or MySQL).

If you migrated the database to the new ESET PROTECT Server, make sure to delete the database on the old ESMC/ESET PROTECT Server before uninstallation to prevent licenses from being dissociated (removed) from the new ESET PROTECT Server database.

3. Uninstall the old ESMC/ESET PROTECT/MDM Server and all its components (including ESET Management Agent, Rogue Detection Sensor, MDM etc.):

- Uninstall ESMC 7.x - Windows
- Uninstall ESET PROTECT 8.x - Windows
- Uninstall ESET PROTECT 9.x - Windows
- Uninstall ESET PROTECT - 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 ESMC/ESET PROTECT/MDM is to format the disk where it is installed.

This will erase everything on the disk, including the operating system.

Troubleshooting

Since ESET PROTECT is a complex product that uses several third-party tools and supports many OS platforms, there is the potential that you will encounter issues that require troubleshooting.

ESET documentation includes several methods to troubleshoot ESET PROTECT. See Answers

to common installation issues to resolve some common issues with ESET PROTECT. See also the known issues for ESET business products.

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 → **Advanced Settings** → **Logging** → **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).

  - ESET Management Agent policy - The policy must be applied to the device to take effect. 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).

  - ESET PROTECT Server Settings

  - ESET Mobile Device Connector policy - The policy must be applied to the device to take effect. See also MDM troubleshooting.

- 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 products 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

The Web Console and Apache Tomcat upgrade clears the Offline help files. If you used Offline help with ESMC or an older ESET PROTECT version, re-create it for ESET PROTECT 9.0 after upgrading to ensure that you have the latest Offline help matching your ESET PROTECT version.

Continue with the offline upgrade of ESET endpoint products

1. See which ESET products are installed on clients: Open ESET PROTECT Web Console and navigate to **Dashboard** → **ESET applications**.

2. Make sure you have the latest versions of ESET endpoint products.

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 OS:

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
netstat | grep 2223
```

Database not running / not reachable

- MS 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`).

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.

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 healh)

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.
```

Verify that the configuration of your database driver matches that shown as in the ODBC configuration section.

ESET Management Agent

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 product 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 remote deployment from Linux to Windows 8.1 (32bit) failed

This is an authentication problem caused by Microsoft's KB3161949. This can be solved only by removing that update from hosts where the deployment fails.

The ESET Management Agent cannot connect to the ESET PROTECT Server

See Troubleshooting Agent connection and our Knowledgebase article.

The Agent Live installer exited with the code 30

You use the live installer script with a custom installer location and you failed to edit the script correctly. Review the help page and try again.

Web Console

Apache HTTP Proxy

Apache HTTP Proxy cache size is several GB and is still growing

If you have installed Apache HTTP Proxy using the All-in-one installer, clean-ups are automatically enabled. If clean-ups are not working correctly, perform a manual clean-up or schedule a clean-up task.

Detection engine updates are not working after Apache HTTP Proxy is installed

If client workstations are not able to update, see our Knowledgebase instructions to disable Apache HTTP Proxy on endpoint workstations for a temporary period. After connection issues are resolved, consider enabling Apache HTTP Proxy again.

Remote update of ESET Management Agent fails with error code 20008

If remote update of ESET Management Agent fails with the following message:
GetFile: Failed to process the HTTP request (error code 20008, url: 'http://repository.eset.com/v1//info.meta')

Follow steps I - III in this article to troubleshoot the connection issue. If the machine on which ESET Management Agent is supposed to be updated is outside your corporate network, configure a policy for ESET Management Agent not to use a proxy to connect to the repository when outside the corporate network.

 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} throwed 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.

 Linux

Missing libQtWebKit dependecy on CentOS Linux

If the following error is displayed:

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

Follow the instructions in our Knowledgebase article.

ESET PROTECT Server installation on CentOS 7 has failed

If the following error is displayed:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

The issue is probably caused by environment/locale settings. Running the following command before the server installer script should help:

```
export LC_ALL="en_US.UTF-8"
```

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 products, 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.

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".

MS 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.

Make sure that all previous steps have been finished successfully. This error is caused by misconfigured system files. Restart you 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 Server	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

ESET Management Agent	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* See also Agent connection troubleshooting.
ESET PROTECT Web Console and Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* See also https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Mobile Device Connector	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* See also MDM troubleshooting.
Rogue Detection Sensor	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*
Apache HTTP Proxy	*C:\Program Files\Apache HTTP Proxy\logs* *C:\Program Files\Apache HTTP Proxy\logs\errorlog*

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 Server	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Management Agent	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
Mobile Device Connector	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* See also MDM troubleshooting.
Apache HTTP Proxy	*/var/log/httpd/*
ESET PROTECT Web Console and Apache Tomcat	*/var/log/tomcat/* See also https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

ESET PROTECT Virtual Appliance

ESET PROTECT VA configuration	*/root/appliance-configuration-log.txt*
ESET PROTECT Server	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Apache HTTP Proxy	*/var/log/httpd*

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 product components.

Diagnostic Tool location

Windows

Folder *C:\Program Files\ESET\RemoteAdministrator\<product>*__Diagnostic.exe__.

Linux

In the following directory on the server: */opt/eset/RemoteAdministrator/<product>/*, there is a __Diagnostic<product>__ 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.

Usage (Windows)

1. Run the tool using a Command Prompt.

2. Enter the location of log files to be stored (in our example "logs") and press **Enter**.

3. Enter the information you want to gather (in our example `1 trace status 3`). See **Actions** below for more information.

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.

 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 product name and product version of the currently installed product.

- **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. Activate the ESET PROTECT Server with a valid license key or select **Activate Later** (see License management for additional instructions) and click **Next**.

7. Click **Repair**.

8. 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 Security Management 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 Security Management 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 Security Management Server.

2. Repair ESET Management Agents using one of the following methods:

   - Agent live 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 API

The ESET PROTECT 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, generating and receiving reports, etc.

For more information and examples in C language and list of available JSON messages, please refer to the following Online Help:

ESET PROTECT 9 API

FAQ

Why are we installing Java on a server? Doesn’t this create a security risk? The majority of all security companies and security frameworks recommend that you uninstall Java from computers and 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 are using Java and a Web Server (Apache Tomcat) for their operation. Java is necessary to support a multi-platform web server. It is possible to 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 package) on Windows Server 2012 it does not appear to be listening on a standard SQL port. It is most likely listening 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?

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 Installer create a new database for me in an existing MS SQL Server installation, if I give it the proper MS SQL Server connection details and credentials? It would be convenient if the installer supported different versions of SQL Server (2014, 2019, etc.).

The database is created by *Server.msi*. So, yes, it can create an ESET PROTECT database for you on individually installed SQL Server instances. The supported versions of MS SQL Server are 2014 and later.

The ESET PROTECT 9.0 All-in-one installer installs Microsoft SQL Server Express 2019 by default.

- If you use an older Windows edition (Server 2012 or SBS 2011), Microsoft SQL Server Express 2014 will be installed by default.
- The installer automatically generates a random password for database authentication (stored in *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Microsoft SQL Server Express has a 10 GB size limit for each relational database. We do not recommend using Microsoft SQL Server Express:

- In enterprise environments or large networks.
- If you want to use ESET PROTECT with ESET Enterprise Inspector.

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 admin) 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 the installation of the ESET PROTECT Server.

Can I use MariaDB instead of MySQL?

No, MariaDB is not supported. Make sure to install a supported version of MySQL Server and ODBC Connector. See MySQL installation and configuration.

I had to install Microsoft .NET Framework 4 as the ESET PROTECT Installer pointed me to (http://www.microsoft.com/en-us/download/details.aspx?id=17851), but that did not work on a fresh installation of Windows Server 2012 R2 with SP1.

This installer cannot be used on Windows Server 2012 because of the Windows Server 2012 security policy. Microsoft .NET Framework must be installed via the **Add Roles and Features Wizard**.

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?

The SQL Server installation can, in rare cases, take up to 1 hour. Install times depend on system performance.

How do I reset the Administrator password for my Web Console (entered during set up)?

It is possible to reset the password by running the server installer and choosing **Repair**. Be aware the password may be required to gain access to the ESET PROTECT database if you did not use Windows Authentication during creation of the database.

- Please be careful since some of the repair options can potentially remove stored data.
- Password reset disables the 2FA.

When importing a file containing a list of computers to add to ESET PROTECT, what is the format required for the file?

The format is the following lines:

All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX
All is the required name of root group.

Can you use IIS instead of Apache? What about another HTTP server?

IIS is an HTTP server. The web console needs a Java servlet container (like Tomcat) to run, and the HTTP server is not sufficient. There have been solutions about how to change IIS into a Java servlet container, but in general, this is not supported.

We do not use Apache HTTP Server, we use Apache Tomcat, which is a different product.

Does ESET PROTECT have a command-line interface?

Yes, we have the ESET PROTECT ServerApi.

Can you install ESET PROTECT on a domain controller?

Do not install SQL Server on a Domain Controller (for example, Windows SBS / Essentials). We recommend that you install ESET PROTECT on a different server or do not select the SQL Server Express component during installation (this requires you to 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 on the system? What happens if it does? What about MySQL?

ESET PROTECT will check for SQL running on a system if you are using the installation wizard and you have selected SQL express to install. In the event 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 without SQL Express. See database requirements for ESET PROTECT.

Where can I find an ESET PROTECT component mapped by its release version?

See our Knowledgebase article.

How do I perform an upgrade of ESET PROTECT to the latest version?

See upgrade procedures.

How can I update a system without an Internet connection?

Using 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 product 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 install?

If you are installing the new instance of the 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 entered in all capital letters (`administrator@TEST.LOCAL` instead of `administrator@test.local`).

Is there a way to use my own network resource (like SMB share) instead of the repository?

You can choose to provide the direct URL where a package is located. If you are using a file share, specify it in a 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 admins. Once admin 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 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 enter 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?

It is necessary to change the port in your webserver configuration to allow webserver connections to the new port. To do so, follow the steps below:

1.Shut down your webserver.
2.Modify the port in your webserver 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 webserver again.

Can I upgrade from ERA 5 or 6 to ESET PROTECT 9 directly via All-in-one installer?

The direct upgrade is not supported - see Migration from ERA 5.x or Upgrade from ERA 6.x.

I am receiving error messages or have problems with ESET PROTECT, what should I do?

See Troubleshooting FAQs.

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept..." while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software

("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for functioning of the Software and for updating and upgrading the Software. The Provider shall be entitled to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol_business. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and

authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well

as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement.** This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR

INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software.** The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate

issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from

acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET´s right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes, Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

ADDENDUM TO THE AGREEMENT

Forwarding of Information to the Provider. Additional provisions apply to the Forwarding of Information to the Provider as follows:

The Software contains functions which collect data about the installation process, the Computer and/or the platform on which the Software is installed, information about the operations and functionality of the Software and information about managed devices (hereinafter referred to as "Information") and then send them to the Provider. The Information may contain data (including randomly or accidentally obtained personal data) concerning managed devices. By activating this function of the Software, Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations.

The Software requires a component installed on managed computer, which enables transfer of information between managed computer and remote management software. Information, which are subject to transfer contains management data such as hardware and software information of managed computer and managing instructions from the remote management software. Other content of data transferred from managed computer shall be determined by the settings of software installed on managed computer. The content of instructions from management software shall be determined by settings of remote management software.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Privacy policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Management of ESET security products requires and locally stores information such as seat ID and name, product name, license information, activation and expiration information, hardware and software information concerning managed computer with ESET security product installed. Logs concerning activities of managed ESET security products and devices are collected and available in order to facilitate managing and supervising features and services without automated submission to

ESET.

• Information concerning installation process, including platform on which our product is installed and information about the operations and functionality of our products such as hardware fingerprint, installation IDs, crash dumps, license IDs, IP address, MAC address, configuration settings of product which may also include managed devices.

• Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.

• Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support such as generated log files.

• Data concerning usage of our service are completely anonymous by the end of session. No personally identifiable information is stored after the session ends.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject’s Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

- right to request access to your personal data from ESET,
- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),
- right to request erasure of your personal data,
- right to request restriction of processing your personal data,
- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk