ESET PROTECT

Guide for Small and Medium-sized Businesses

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

Digital Security
Progress. Protected.

ESET PROTECT was developed by ESET, spol. s r.o.

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

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

REV. 3/19/2023

About help

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.

Convention	Meaning
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.

Introduction

This guide is intended for a small to medium-sized businesses that manage up to 250 Windows ESET endpoint products using ESET PROTECT 9.
It will explain basic concepts important for deploying and using ESET security products.

ESET PROTECT 9

ESET PROTECT 9 (formerly ESMC) 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.

The built-in task management system in ESET PROTECT allows you to 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.

Manageable ESET endpoint products

ESET endpoint products are primarily designed for use on workstations in a small business/enterprise environment and can be used with ESET PROTECT.

ESET PROTECT 9 is able to deploy, activate or manage the following ESET endpoint products:

Manageable via ESET PROTECT 9	Product version
ESET Endpoint Security for Windows	6.5+, 7.x, 8.x, 9.x
ESET Endpoint Antivirus for Windows	6.5+, 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

See also the full list of manageable ESET security products.

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.

ESET PROTECT components and architecture

To perform a complete deployment of the ESET security solutions portfolio, the following components must be installed:

- ESET PROTECT Server (controls the communication with client computers)
- ESET PROTECT Web Console (browser-based user interface for the ESET PROTECT Server)
- ESET Management Agent (deployed on client computers, communicates with ESET PROTECT Server)

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

- Apache HTTP Proxy
- RD Sensor (can detect unmanaged computers on the network)

See also Certificates and ESET PROTECT component structure.

Server

The ESET PROTECT Server is the application that processes all data received from clients that connect to the Server (through the ESET Management Agent).

Agent

The ESET Management Agent is an essential part of ESET PROTECT. Client computers do not communicate with the 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 to the client, it is sent to the Agent which then sends this task to the ESET endpoint product running on the client.

Web Console

ESET PROTECT Web Console is a browser-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. If you choose to make the web server accessible from the internet, you can use ESET PROTECT from virtually any place and device.

Apache HTTP Proxy

Apache HTTP Proxy is a service that can be used in combination with ESET PROTECT 9 to distribute installation packages and updates to client computers. It acts as a transparent proxy, meaning it caches files that have already been downloaded to minimize Internet traffic on your network.

Using Apache HTTP Proxy offers the following benefits:

- Downloads and caches the following:
  - Detection engine updates
  - Activation tasks, including communication with activation servers and caching of license requests
  - ESET PROTECT repository data
  - Product component updates—Apache proxy caches and distributes updates to endpoint clients on your network.
- Minimized internet traffic on your network.

Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) searches your network for computers not registered in ESET PROTECT. This component can locate new computers and add them in ESET PROTECT automatically.

> Rogue Detection Sensor can take up to 24 hours to locate new computers on your network.

Newly discovered machines are listed in a pre-defined report, making it easy to deploy ESET Management Agent to them, assign them to specific static groups and manage them via tasks and policies.

System requirements

Before you install ESET PROTECT, verify that all hardware, operating system, network and software prerequisites are met.

Hardware

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

Number of clients	ESET PROTECT Server + SQL database server				
	CPU cores	CPU clock speed (GHz)	RAM (GB)	Disk drive[1]	Disk IOPS[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:

Clients number	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.

CPU cores	CPU clock speed (GHz)	RAM (GB)	Performance		
			10,000 clients	20,000 clients	40,000 clients
8	2.1	64	High	High	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Normal	Low
2	2.1	16	Low	Low	Insufficient
2	2.1	8	Very low (not recommended)	Very low (not recommended)	Insufficient

Operating system

The table below displays the supported Windows operating systems for each ESET PROTECT component. See also the full list of supported operating systems.

Operating System	Server	Agent	RD Sensor	MDM
Windows Server 2008 R2 x64 SP1 with KB4474419 and KB4490628 installed		✔	✔	
Windows Server 2008 R2 CORE x64 with KB4474419 and KB4490628 installed		✔	✔	
Windows Storage Server 2008 R2 x64 with KB4474419 and KB4490628 installed		✔	✔	

Operating System	Server	Agent	RD Sensor	MDM
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	✔	✔	✔	✔

Operating System	Server	Agent	RD Sensor	MDM
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.

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/or 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.

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.

Software

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

- You must have a valid license.

- Microsoft .NET Framework 4 must be installed; you can install it using the **Add Roles and Features Wizard**.

- The ESET PROTECT Web Console requires Java/OpenJDK (64-bit).

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.

- ESET PROTECT supports two types of database servers: MS SQL and MySQL. We recommend that you use Microsoft SQL Server Express 2019 included with ESET PROTECT All-in-one installer for Windows. If you already have a database server and you want to use it for ESET PROTECT, make sure it meets database requirements.

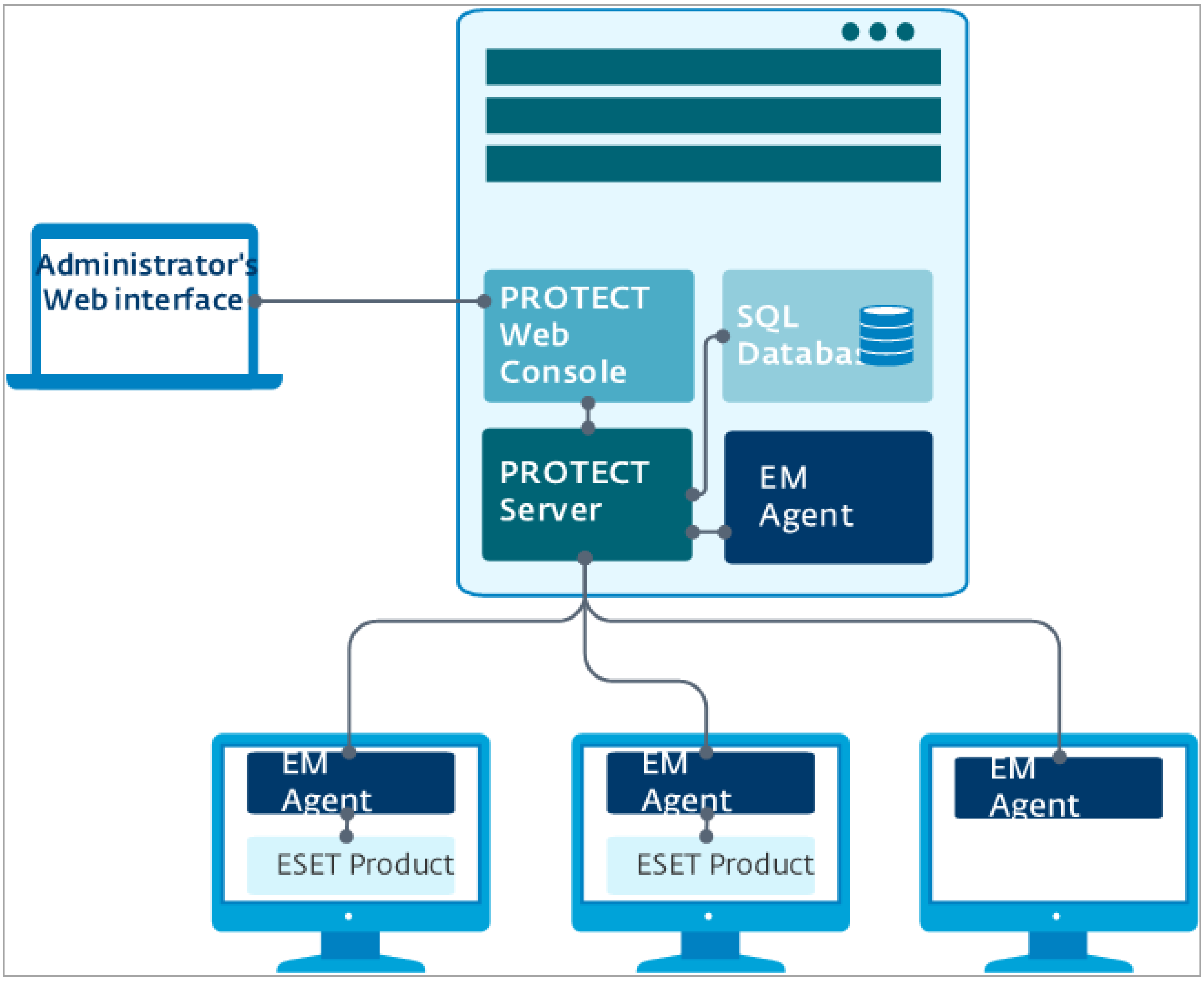
- The ESET PROTECT Web Console can be run in the following web browsers:
  - Mozilla Firefox
  - Microsoft Edge
  - Google Chrome
  - Safari
  - Opera

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.

Install the ESET PROTECT Server

ESET PROTECT component structure

To manage small to medium-sized networks (1,000 clients or fewer), a single machine with the ESET PROTECT server and all its components (supplied web server, database, and so on) installed on it is usually sufficient. You can think of it as a single server or stand-alone installation. All managed clients are connected directly to the ESET PROTECT server via the ESET Management Agent. The administrator can connect to the ESET PROTECT Web Console via a web browser from any computer on the network or run the Web Console directly from the ESET PROTECT server.



Installation

ESET PROTECT installers are available in different formats to support various installation methods:

- ESET recommends the All-in-one installer for small deployments on Windows.
- ESET recommends deploying a pre-configured ESET PROTECT Virtual Appliance (running on CentOS Linux) if you use a hypervisor. Its deployment is quick and more straightforward than installation on Windows.

If you are upgrading from a previous version of ESET PROTECT or ESMC 7.x, follow these instructions.

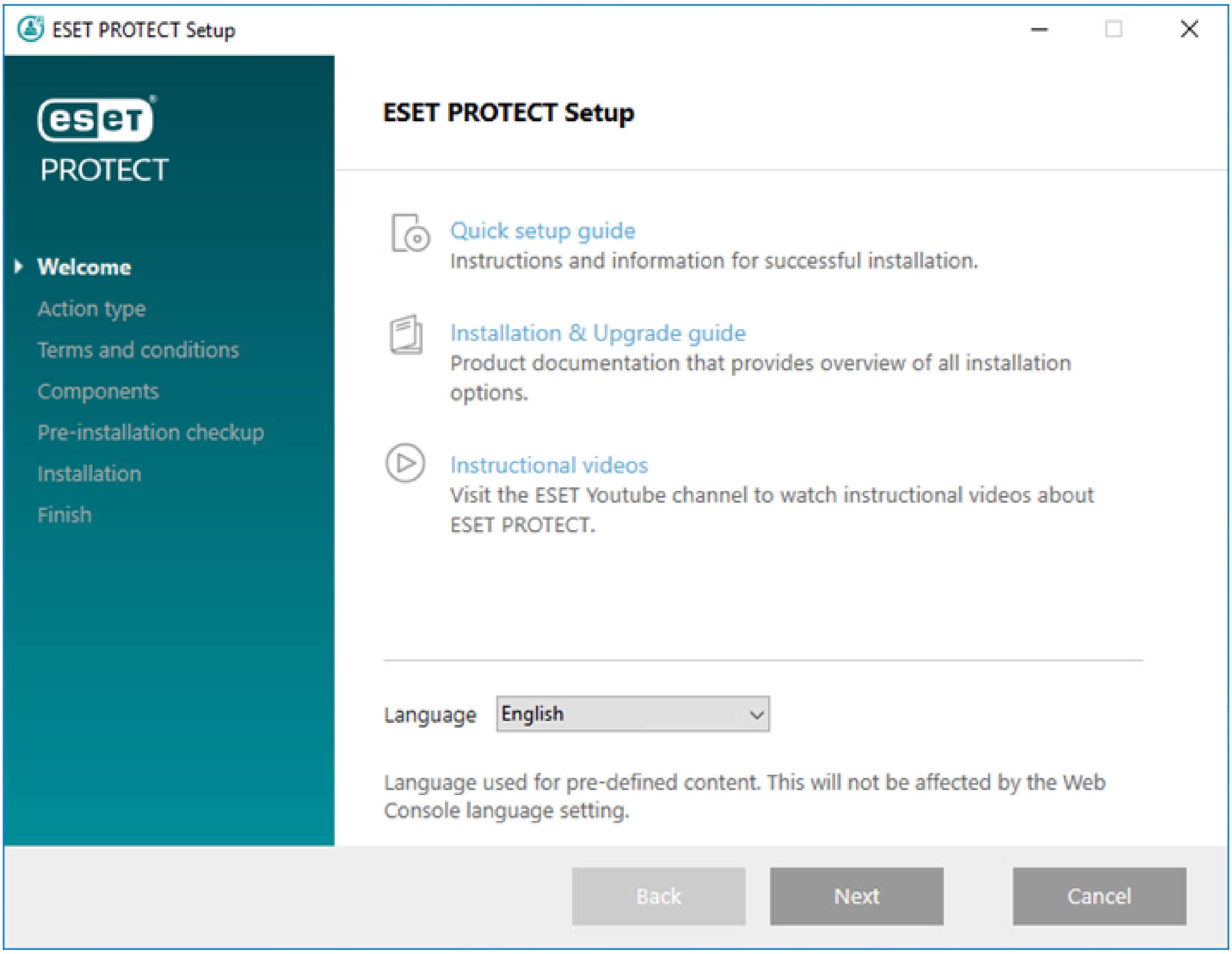
All-in-one installation of ESET PROTECT Server

- Another alternative is to deploy a pre-configured ESET PROTECT Virtual Appliance (if you use a hypervisor).
- If you are upgrading from a previous version of ESET PROTECT or ESMC 7.x, follow these instructions.

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.



ESET PROTECT Setup

Quick setup guide
Instructions and information for successful installation.

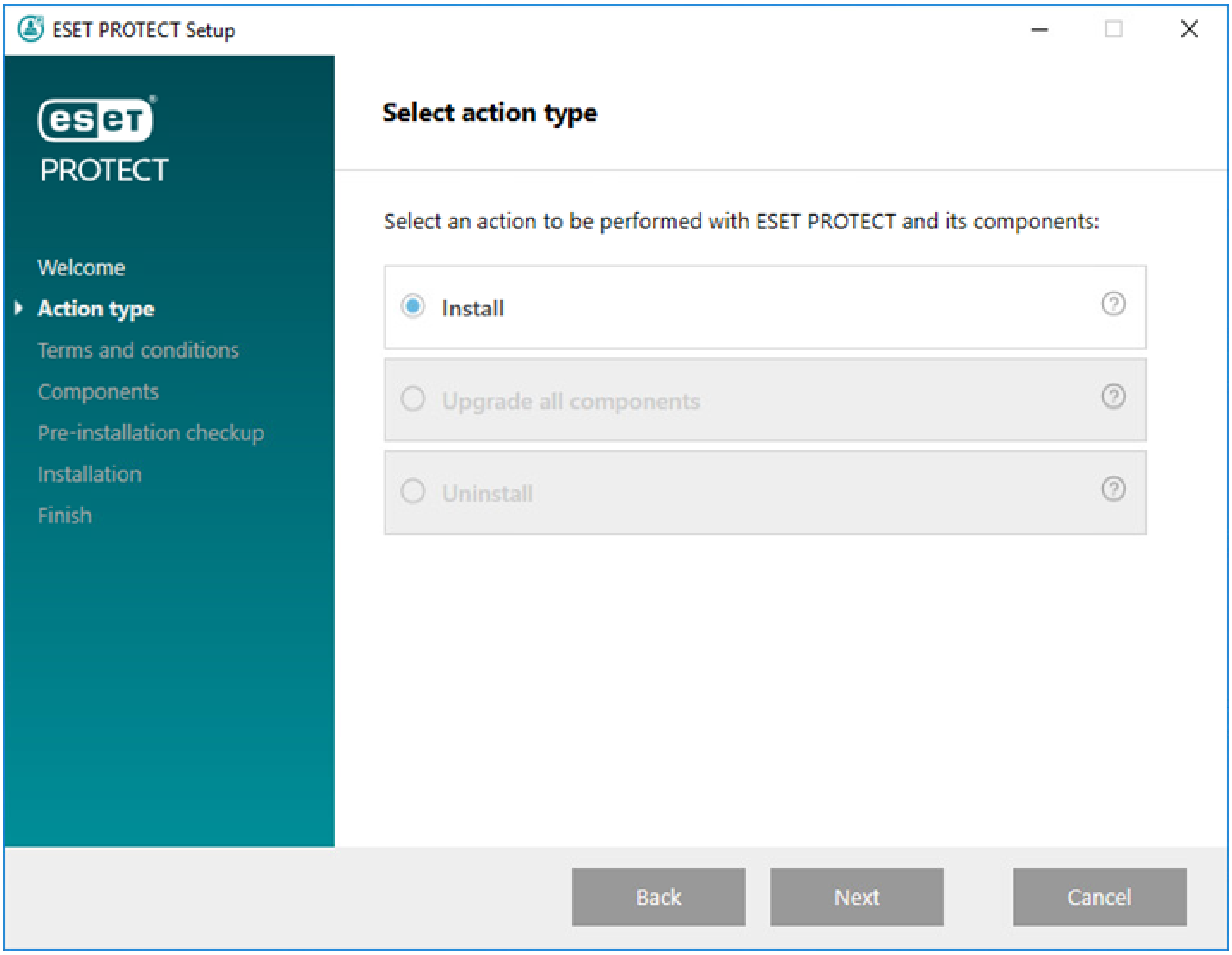
Installation & Upgrade guide
Product documentation that provides overview of all installation options.

Instructional videos
Visit the ESET Youtube channel to watch instructional videos about ESET PROTECT.

Language: English

Language used for pre-defined content. This will not be affected by the Web Console language setting.

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



Select action type

Select an action to be performed with ESET PROTECT and its components:

● Install

○ Upgrade all components

○ Uninstall

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

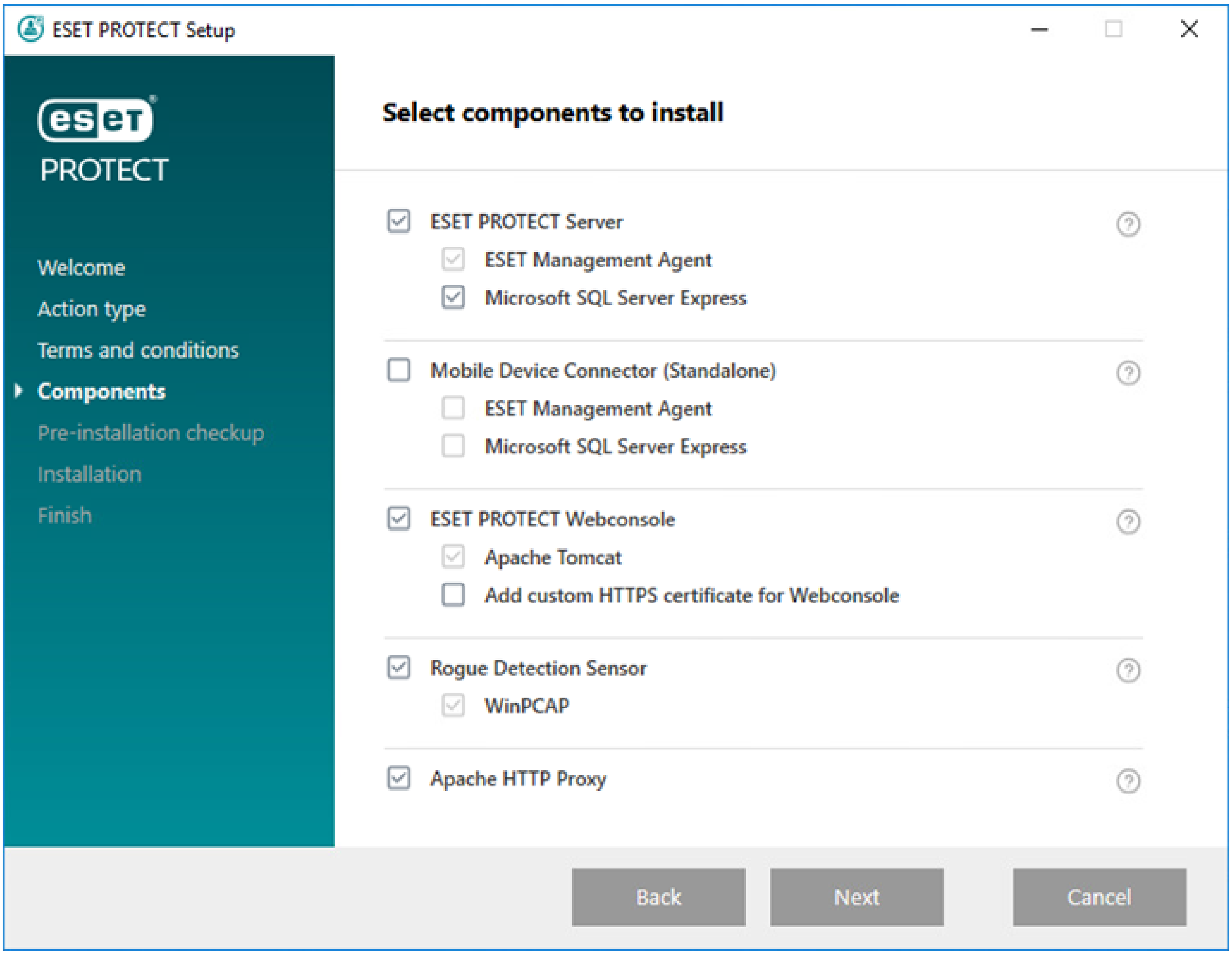
> The **Apache HTTP Proxy** option is intended only for smaller or centralized networks without roaming clients. If you select this option, the installer configures clients to tunnel communication with ESET via a proxy installed on the same machine as the ESET PROTECT Server. This connection will not 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

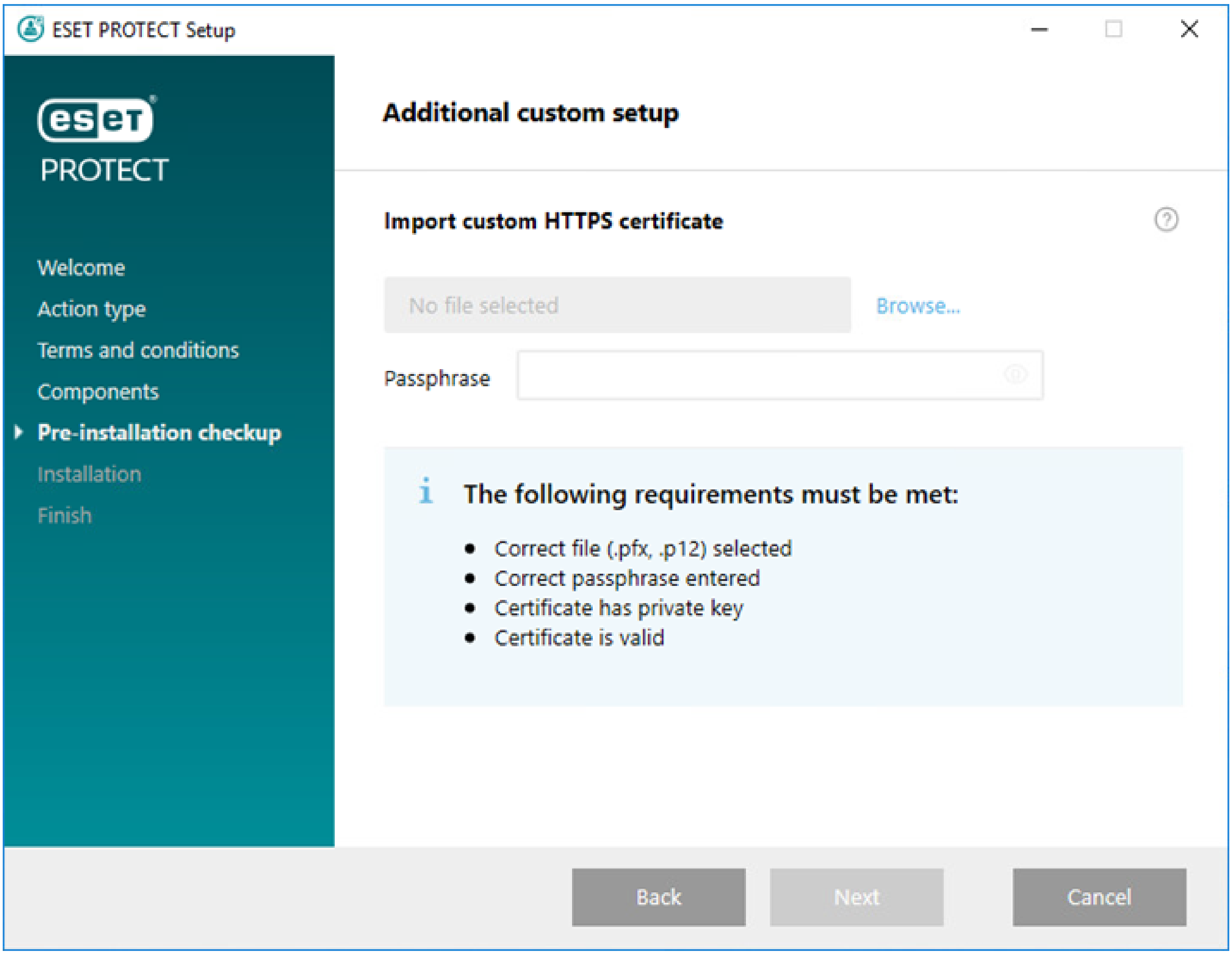
The policy enables HTTP Proxy for affected products. HTTP Proxy host is the ESET PROTECT Server's local IP address and port 3128. Authentication is disabled. You can copy these settings to another policy if you need to set up additional products.



Select components to install

- ☑ ESET PROTECT Server
  - ☑ ESET Management Agent
  - ☑ Microsoft SQL Server Express
- ☐ Mobile Device Connector (Standalone)
  - ☐ ESET Management Agent
  - ☐ Microsoft SQL Server Express
- ☑ ESET PROTECT Webconsole
  - ☑ Apache Tomcat
  - ☐ Add custom HTTPS certificate for Webconsole
- ☑ Rogue Detection Sensor
  - ☑ WinPCAP
- ☑ Apache HTTP Proxy

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.



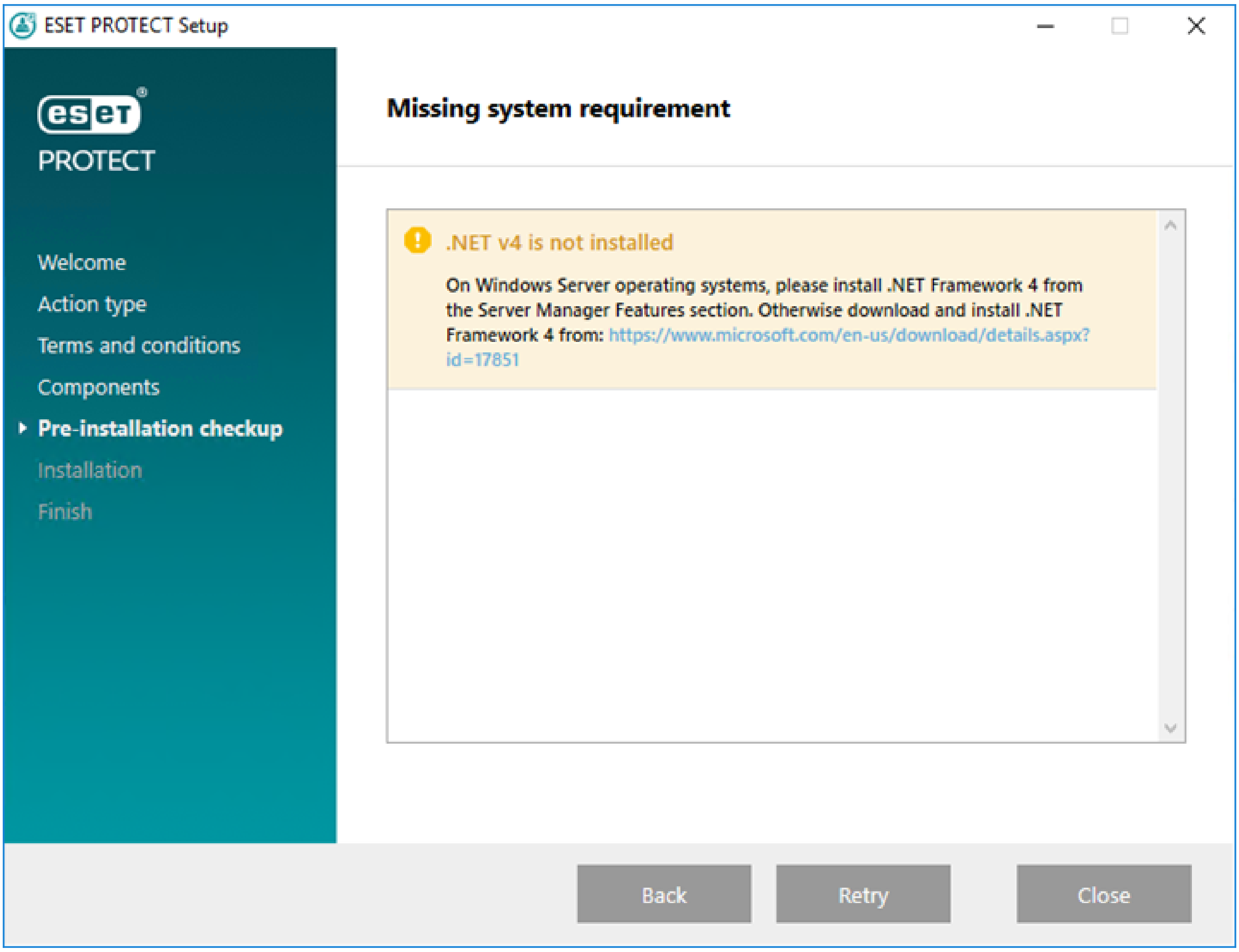
The following requirements must be met:

- Correct file (.pfx, .p12) selected
- Correct passphrase entered
- Certificate has private key
- Certificate is valid

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

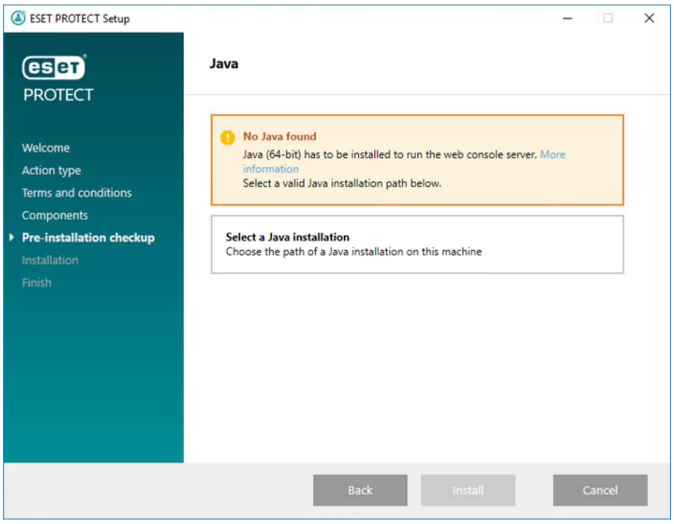


Missing system requirement

.NET v4 is not installed

On Windows Server operating systems, please install .NET Framework 4 from the Server Manager Features section. Otherwise download and install .NET Framework 4 from: https://www.microsoft.com/en-us/download/details.aspx?id=17851

No Java found / Java (64-bit) detected



Java

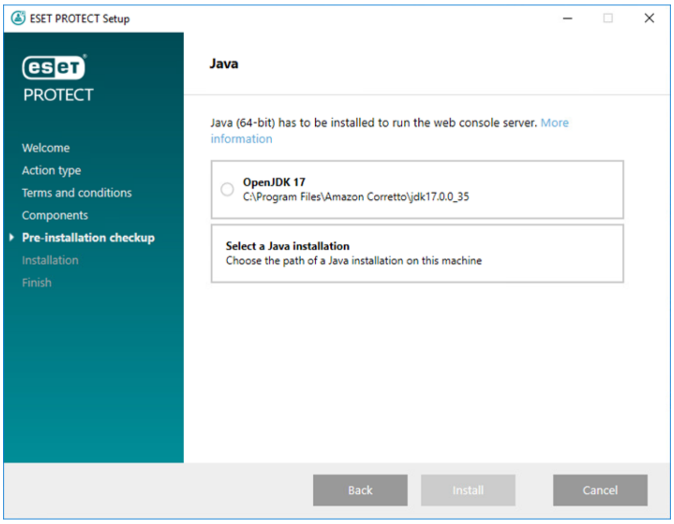
No Java found

Java (64-bit) has to be installed to run the web console server. More information

Select a valid Java installation path below.

Select a Java installation

Choose the path of a Java installation on this machine



Java

Java (64-bit) has to be installed to run the web console server. More information

○ **OpenJDK 17**
C:\Program Files\Amazon Corretto\jdk17.0.0_35

Select a Java installation

Choose the path of a Java installation on this machine

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

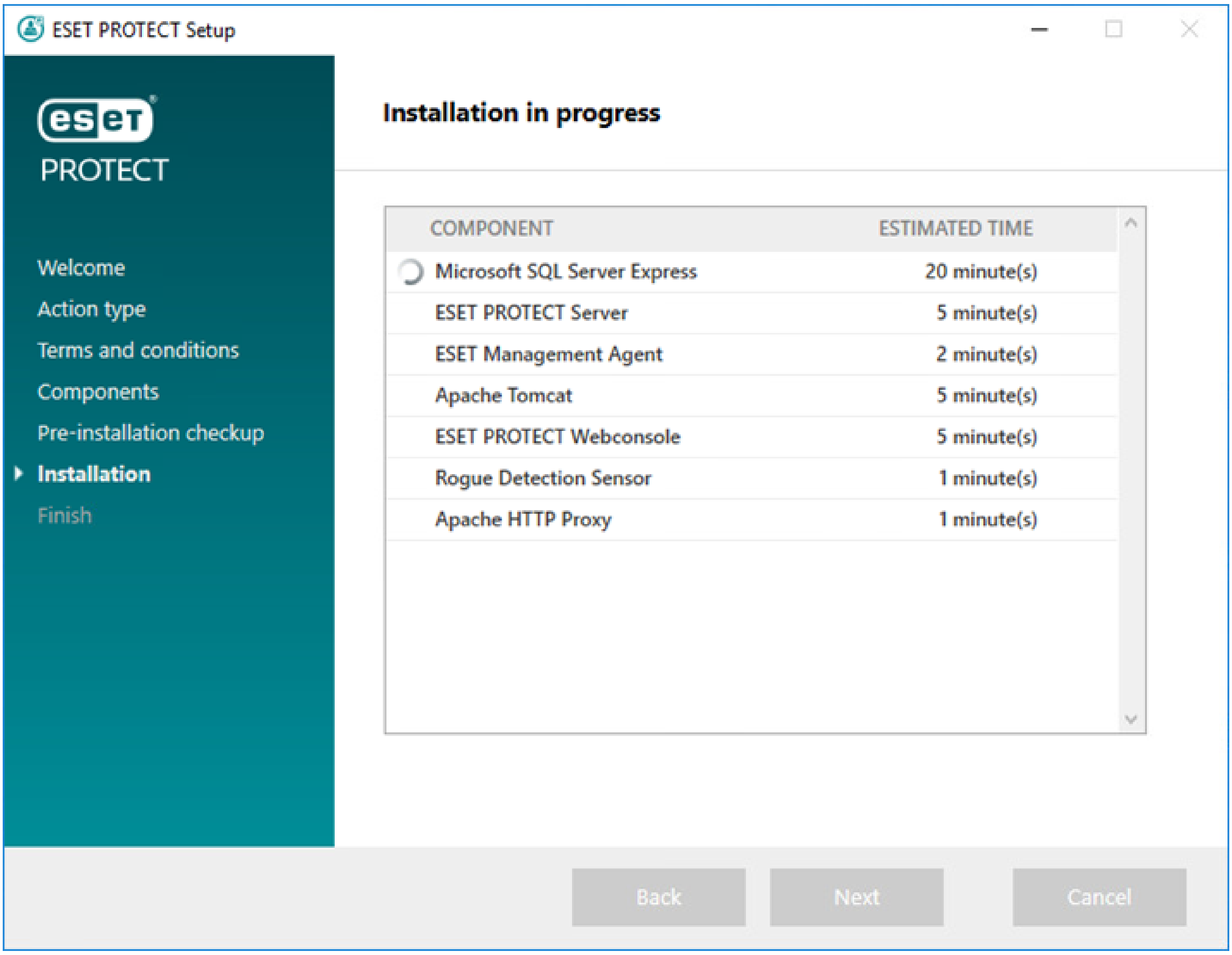
- The installer may display this notification if your system does not have enough disk space for ESET PROTECT to install.
- You must have at least 4,400 MB of free disk space to install ESET PROTECT and all its components.

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.

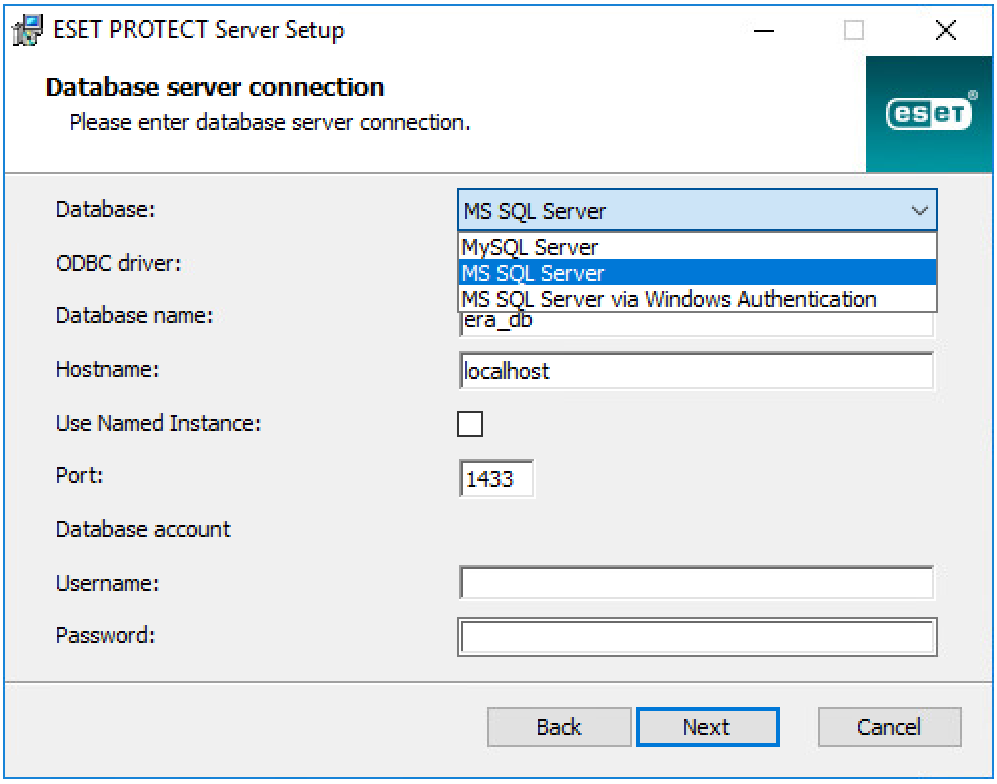


Installation in progress

COMPONENT	ESTIMATED TIME
Microsoft SQL Server Express	20 minute(s)
ESET PROTECT Server	5 minute(s)
ESET Management Agent	2 minute(s)
Apache Tomcat	5 minute(s)
ESET PROTECT Webconsole	5 minute(s)
Rogue Detection Sensor	1 minute(s)
Apache HTTP Proxy	1 minute(s)

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



ESET PROTECT Server Setup

Database server connection

Please enter database server connection.

Database: MS SQL Server

ODBC driver:

Database name: era_db

Hostname: localhost

Use Named Instance: ☐

Port: 1433

Database account

Username:

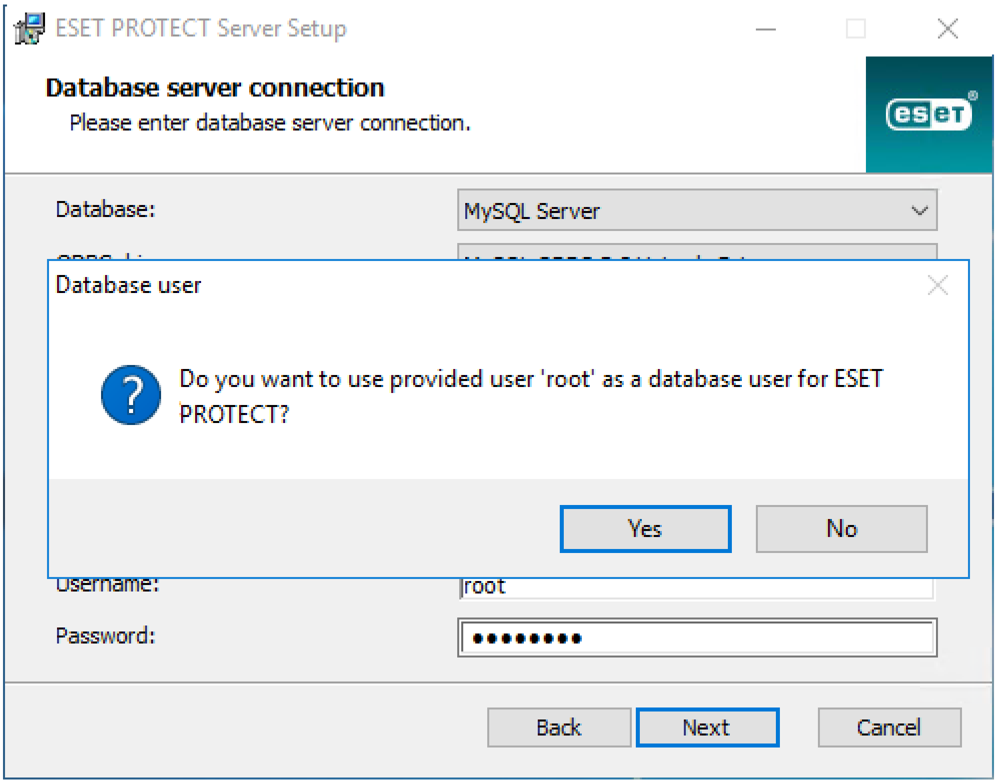
Password:

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.



ESET PROTECT Server Setup

Database server connection

Please enter database server connection.

Database: MySQL Server

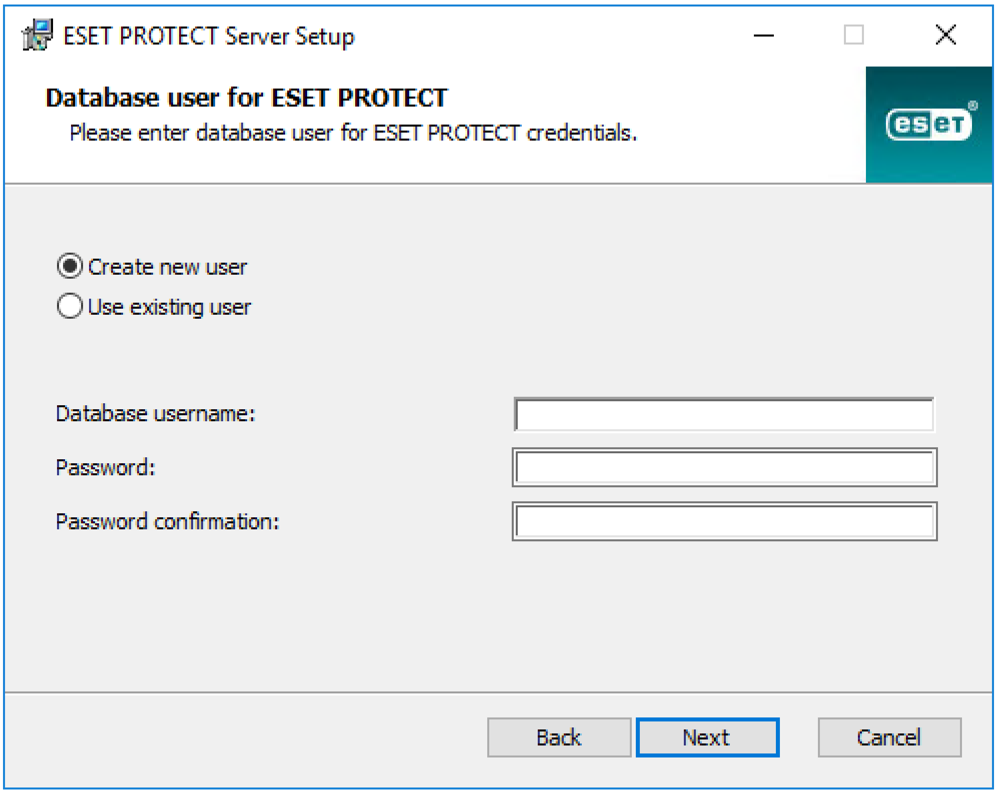
Database user

Do you want to use provided user 'root' as a database user for ESET PROTECT?

Username: root

Password: •••••••••

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).



ESET PROTECT Server Setup

Database user for ESET PROTECT

Please enter database user for ESET PROTECT credentials.

● Create new user

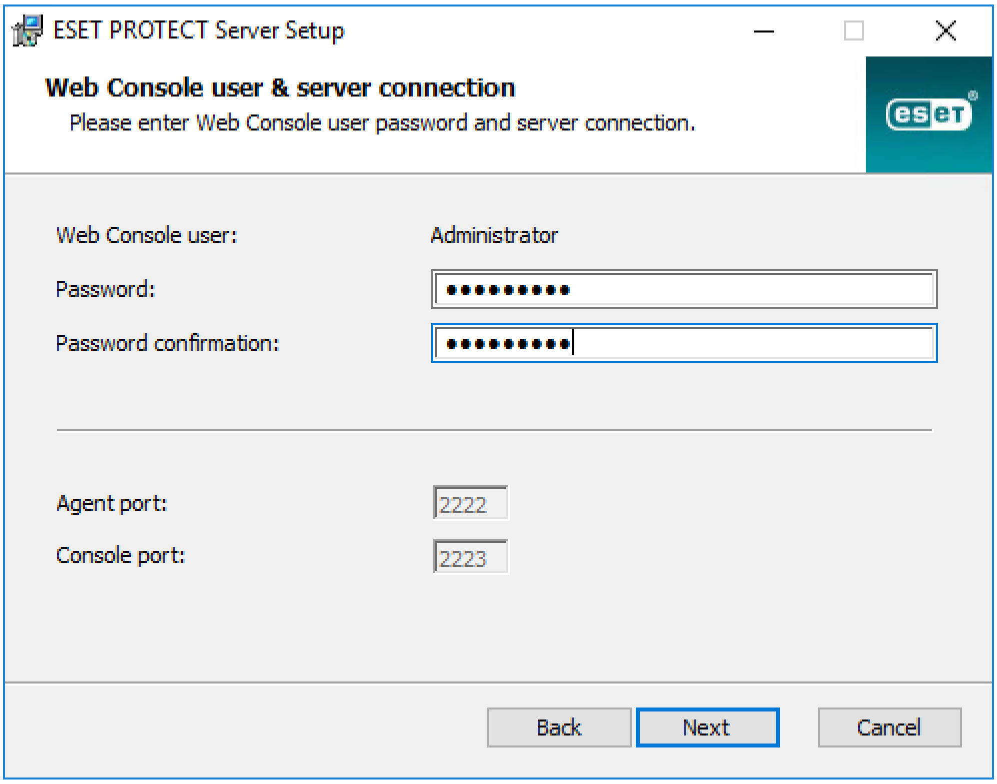
○ Use existing user

Database username:

Password:

Password confirmation:

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**.



ESET PROTECT Server Setup

Web Console user & server connection

Please enter Web Console user password and server connection.

Web Console user: Administrator

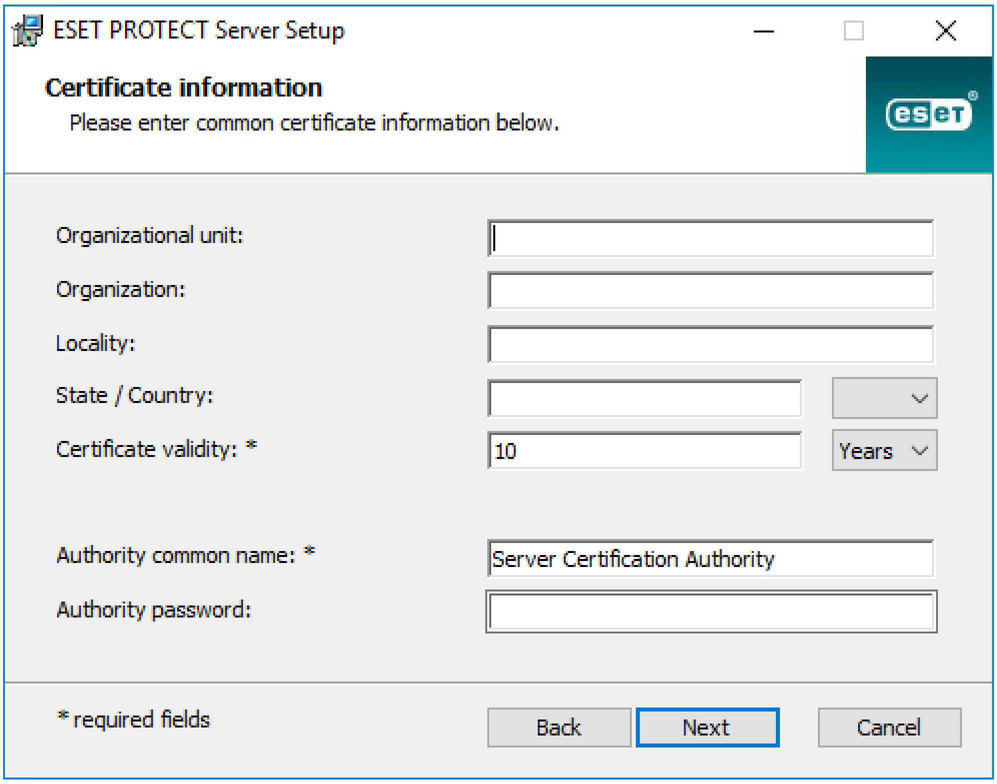
Password: ●●●●●●●●●

Password confirmation: ●●●●●●●●●

Agent port: 2222

Console port: 2223

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**.



ESET PROTECT Server Setup

Certificate information

Please enter common certificate information below.

Organizational unit:

Organization:

Locality:

State / Country:

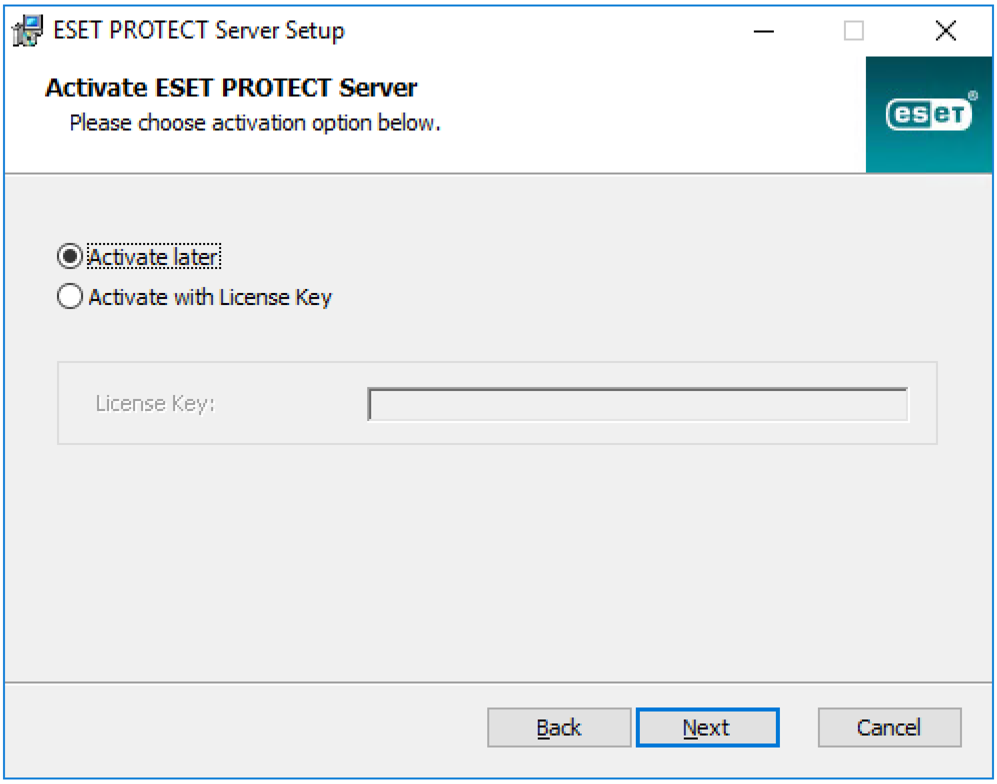
Certificate validity: * 10 Years

Authority common name: * Server Certification Authority

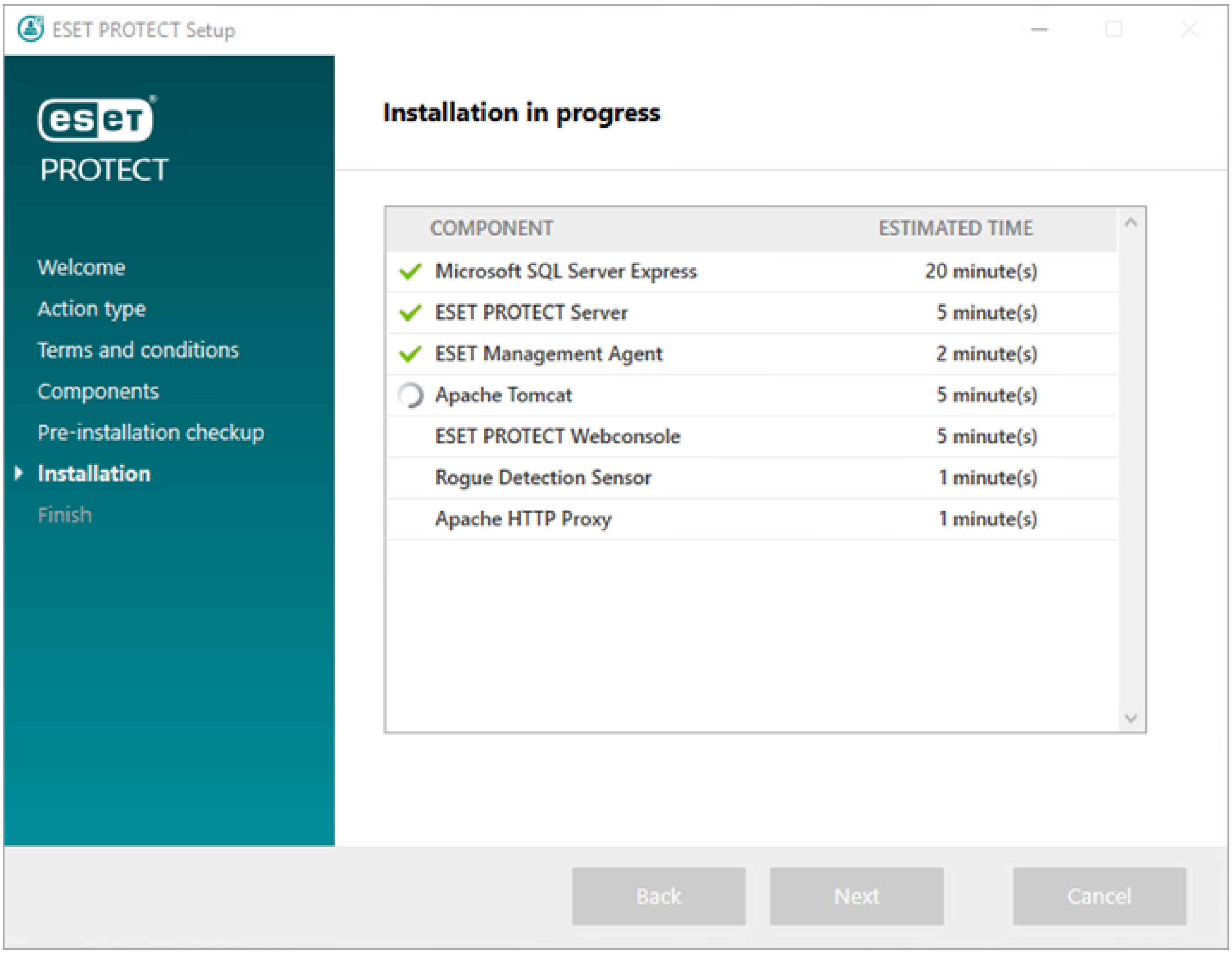
Authority password:

* required fields

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).


ESET PROTECT Server Setup
Activate ESET PROTECT Server
Please choose activation option below.
● Activate later
○ Activate with License Key
License Key:
Back
Next
Cancel

12. You will see the installation progress.

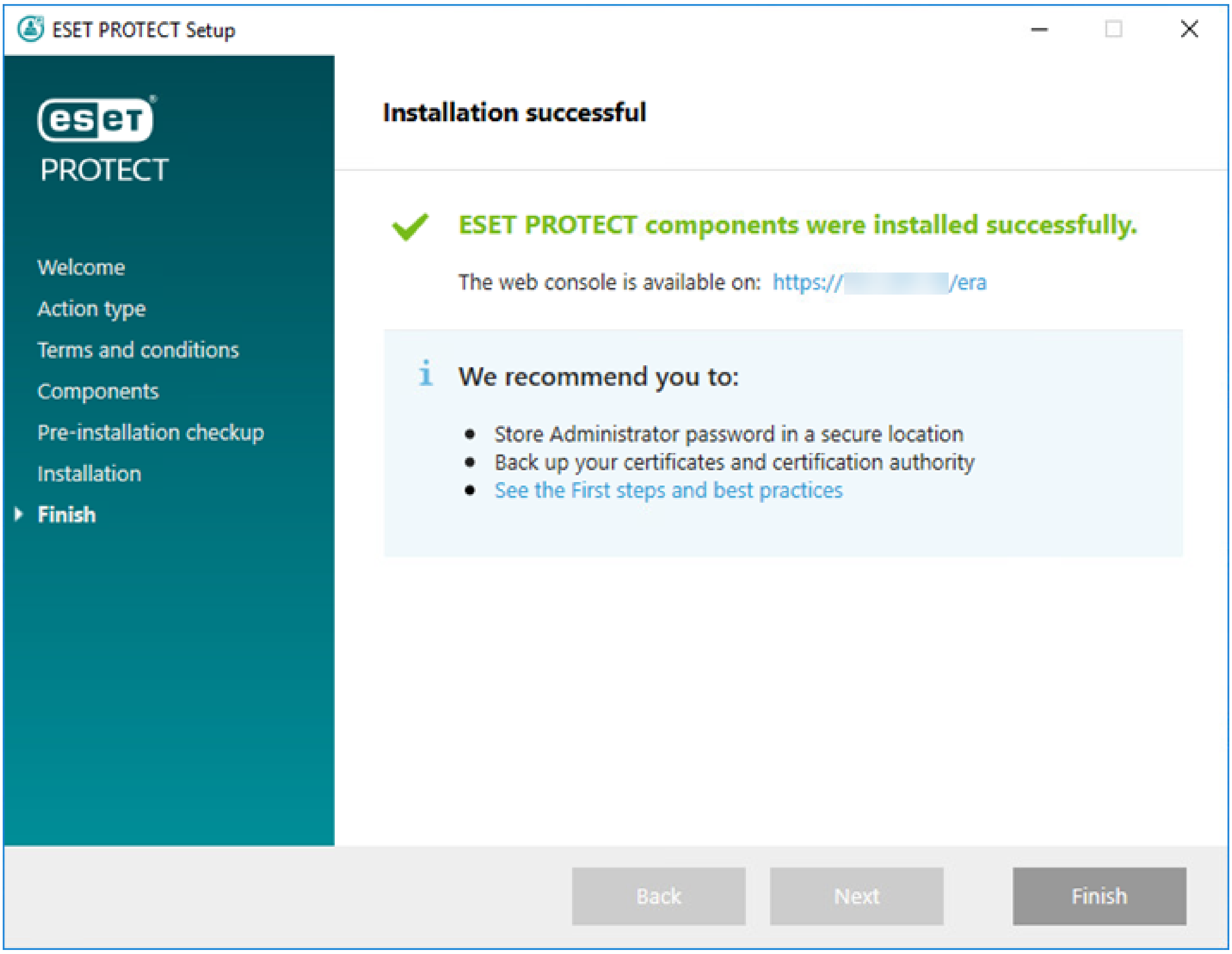


COMPONENT	ESTIMATED TIME
✓ Microsoft SQL Server Express	20 minute(s)
✓ ESET PROTECT Server	5 minute(s)
✓ ESET Management Agent	2 minute(s)
Apache Tomcat	5 minute(s)
ESET PROTECT Webconsole	5 minute(s)
Rogue Detection Sensor	1 minute(s)
Apache HTTP Proxy	1 minute(s)

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**.



Installation successful

ESET PROTECT components were installed successfully.

The web console is available on: https://[redacted]/era

We recommend you to:

- Store Administrator password in a secure location
- Back up your certificates and certification authority
- See the First steps and best practices

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.

Post-installation steps

After you install ESET PROTECT, you can start the configuration.

First steps after ESET PROTECT server deployment

1. Connect to the ESET PROTECT Web Console.

2.Read the Startup Wizard instructions.

3.Add your license(s).

4.Deploy the ESET Management Agent and ESET endpoint products to computers in your network.

The Status Overview can help you with the initial configuration of ESET PROTECT.

With the ESET PROTECT server installed on your server and ESET endpoint solutions installed on clients, you can start managing your network. Refer to the Administrator Guide for more information on how you can manage ESET Endpoint products.

Additional recommended steps

- Use notifications and reports to monitor the status of client computers in your environment, for example, if you want to receive a notification about certain events or view or download a report.

- Configure an SMTP server connection. This configuration is optional if you want to receive notifications or reports by email. You can configure ESET PROTECT Server to send notifications to your Syslog server.

- Create a new ESET PROTECT Web Console user.

Deploy ESET Management Agent and ESET endpoint products

After the successful installation of ESET PROTECT, it is necessary to deploy the ESET Management Agent and ESET endpoint products to computers in your network.

Deployment consists of the following steps:

1. Create the deployment package
2. Install the deployment package

See also other deployment options. For larger networks, we recommend that you use ESET Remote Deployment Tool.

Deployment package creation

The procedure of creating an All-in-one installer (including ESET Management Agent and an ESET security product) package is similar to a Startup Wizard.

Click **Other Deployment Options** in the **Quick Links** section of the menu bar. In the **Deploy Agent** window, click **Create installer** under **Create All-in-one installer (Windows only)**. The **Create All-in-one installer** window will open.

> ! The installer package is an *.exe* file and is valid for Microsoft Windows operating systems only.

Basic

Deselect the check box **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.

Package contents - Select the check box(es) from the following options:

- **Management Agent** - If you do not select other items in the **Package contents**, the installer will include only the ESET Management Agent. Select this option if you want to install the ESET security product on the client computer later, or if the client computer already has an ESET security product installed.
- **Security Product** - Include the ESET security product with the ESET Management Agent. Select this option if the client computer does not have any ESET security product installed and you want to install it with the ESET Management Agent.
- **Full Disk Encryption** - Encryption option is visible only with active ESET Full Disk Encryption license.
- **Enterprise Inspector Agent** - Include ESET Enterprise Inspector Connector in the installer.

Security Product

1. **License** (Optional) - you can add a license using one of the methods described in License Management. If you already have existing licenses in License Management, simply choose the license that will be used to activate the ESET security product during the installation. If you do not choose a license, you can create an installer without it and activate the product later. Addition/removal of a license is only allowed to be done by the Administrator whose home group is set to **All** and who has **Write** permission on licenses in that group.

2. **Product** - Select an ESET security product that will be installed together with ESET Management Agent.

> i If you do not see any product installation files, make sure you have the repository set to **AUTOSELECT**. For more information, see the **Advanced settings** section of Server settings.

3. **Language** - Select the language version of the ESET security product installer.

4. Optionally, you can select a **Policy** that will be applied on the ESET security product during its installation.

5. **Protection settings** - select the check box next to the setting to enable it for the installer:

oEnable The ESET LiveGrid® feedback system (recommended)

oEnable detection of potentially unwanted applications - Read more in our Knowledgebase article.

Select the check box next to **Do not define Protection settings right now (not recommended)** if you do not want to define the protection settings for the installer and you want to set them via policy later.

6. Select the check box **I accept the terms of the application End User License Agreement and acknowledge the Privacy Policy**. See End User License Agreement (EULA), Terms of Use and Privacy Policy for ESET products for more information.

Enterprise Inspector Agent

ESET Enterprise Inspector Agent requirements:

- You must have a ESET Enterprise Inspector license to activate ESET Enterprise Inspector Connector.
- A compatible ESET security product installed on the managed computer.

1. **License** (optional) - ESET recommends that you select the ESET Enterprise Inspector license to activate ESET Enterprise Inspector Connector during the installation. If you create the installer without the license, you can activate ESET Enterprise Inspector Agent later.

2. **Product/Version** - Select the version of ESET Enterprise Inspector Connector. The latest available version is preselected.

3. **Configuration Policy** (optional) - Select an existing ESET Enterprise Inspector Connector policy to apply policy settings during the ESET Enterprise Inspector Connector installation.

4. Select the check box **I accept the terms of the application End User License Agreement and acknowledge the Privacy Policy**. See End User License Agreement (EULA), Terms of Use and Privacy Policy for ESET products for more information.

5. Type the ESET Enterprise Inspector **Server hostname** and the connection **port** specified during the ESET Enterprise Inspector server installation (the default port is 8093).

6. Select the **Certification Authority** for connection to the ESET Enterprise Inspector server.

Certificate

A Peer Certificate and ESET PROTECT Certification Authority are chosen automatically based on the available certificates. To use a different certificate than the one automatically selected, click **ESET PROTECT Certificate** to see a list of available certificates and then select the one you want to use. To use your own Custom certificate, click the radio button and upload a *.pfx* certificate file.

Enter your **Certificate passphrase** if needed. For example, if you have specified the passphrase during the installation of ESET PROTECT, or if you are using a Custom certificate with a passphrase. Otherwise, leave the **Certificate passphrase** field blank.

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

Be aware that it is possible to extract the **Certificate passphrase** because it is embedded in the *.exe* file.

Advanced

In this section, you can customize the All-in-one installer package:

1. Optionally, you can change the **Name** and enter a **Description** for the package installer.

2. Click **Select tags** to assign tags.

3. **Parent group (optional)** - Select the Parent group where the computer will be placed after installation. You can select an existing static group or create a new static group to which the device will be assigned after the installer is deployed.

4. **ESET AV Remover** - Select the check box to uninstall or completely remove other antivirus programs on the target device.

5. **Initial installer configuration (Optional)** - Use this option to apply configuration policy to ESET Management Agent. Click **Select** under **Agent configuration (optional)** and choose from the list of available policies. If none of the pre-defined policies are suitable, you can create a new policy or customize the existing ones.

6. **Server hostname (optional)** - Type the ESET PROTECT Server hostname or IP address. If necessary, you can specify the **Port** number (default is 2222).

7. If you use an HTTP Proxy, select the check box **Enable HTTP Proxy settings** and specify the Proxy settings (**Host**, **Port**, **Username** and **Password**) to set ESET Management Agent connection to Proxy to enable communication forwarding between ESET Management Agent and ESET PROTECT Server. The **Host** field is the address of the machine where the HTTP Proxy is running. HTTP Proxy uses the port 3128 by default. You can set a different port if needed. Make sure to set the same port also in the HTTP Proxy configuration.

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.

Enable **Use direct connection if HTTP proxy is not available** if you want to allow this fallback option.

8. Click **Finish**.

9. Download the generated All-in-one installation package. Select the version you want to deploy:

   - **Download 32-bit version** (for example, *PROTECT_Installer_x86_en_US.exe*)

   - **Download 64-bit version** (for example, *PROTECT_Installer_x64_en_US.exe*)

   - **Download ARM64 version** (for example, *PROTECT_Installer_arm64.exe*) - You cannot install the x86 or x64 version of ESET Management Agent or ESET security product on Windows ARM64.

All data downloaded from the repository (ESET repository or a custom repository mirror) is digitally signed by ESET and ESET PROTECT Server verifies file hashes and PGP signatures. ESET PROTECT Server generates the All-in-one installer locally. Therefore, the All-in-one installer is not digitally signed, which might generate a web browser warning during the installer download or generate an operating system alert and prevent the installation on systems where unsigned installers are blocked.

The ESET Endpoint Antivirus/Security installer created in ESET PROTECT 8.1 and later supports Windows 10 Enterprise for Virtual Desktops and Windows 10 multi-session mode.

10. Run the installation package file on a client computer. It will install the ESET Management Agent and the ESET security product on the device and connect the device to ESET PROTECT. For step-by-step instructions, see the deployment package installation. You can run the installation package in silent mode to hide the setup wizard window.

Deployment package installation

You can create this installer package in ESET PROTECT.

The installer package installs the ESET Management Agent, and the package can also install these components (if selected during the installer package creation):

- ESET security product (for endpoint or server)
- ESET Full Disk Encryption
- ESET Inspect Connector

- The installer package comes via *.exe* file and is only valid for Windows operating system.
- If you run the installer on a client machine where ESET security product or ESET Management Agent is already installed, the installer will upgrade it to the version in the installer.
- You must execute the installer using the built-in Administrator account or a domain Administrator account (if the built-in Administrator account is disabled). Any other user, even a member of the Administrators group, will not have sufficient access rights. Therefore, you need to use the built-in Administrator account. You cannot complete the installation under any other user account than the local or domain Administrator.
- All data downloaded from the repository (ESET repository or a custom repository mirror) is digitally signed by ESET and ESET PROTECT Server verifies file hashes and PGP signatures. ESET PROTECT Server generates the All-in-one installer locally. Therefore, the All-in-one installer is not digitally signed, which might generate a web browser warning during the installer download or generate an operating system alert and prevent the installation on systems where unsigned installers are blocked.
- Be aware that it is possible to extract sensitive data (for example, the Certificate passphrase) because it is embedded in the installer.
- The ESET Endpoint Antivirus/Security installer created in ESET PROTECT 8.1 and later supports Windows 10 Enterprise for Virtual Desktops and Windows 10 multi-session mode.

Installation process

- If you want to run the installer without displaying a dialog, follow the silent installation instructions.
- If an error has occurred during installation, see the troubleshooting section for the most common installation errors.

1. Run the installer package.

Make sure to uninstall any third-party security product from your computer before installing the ESET security product.

- If you selected to include **ESET AV Remover** when creating the installation package, **ESET AV Remover** will help you uninstall or completely remove third-party security software:

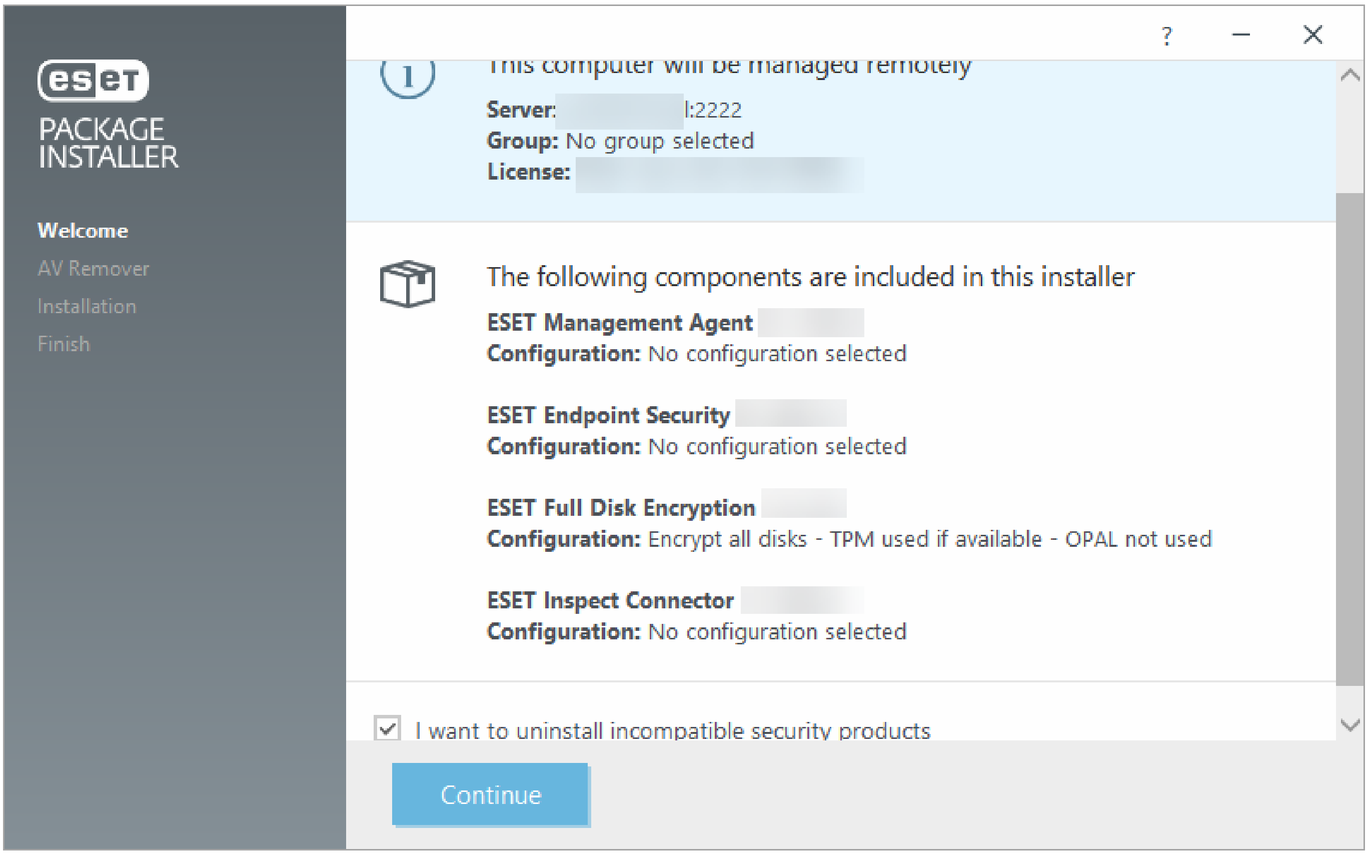
  a)Select the **I want to uninstall incompatible security products** check box to remove/uninstall third-party security software running or installed on your computer. Check the list of supported software.

  b)Click **Continue**.

  c)After scanning installed applications, select the check box next to the application(s) you want to remove and click **Remove**. See our Knowledgebase article about ESET AV Remover for details.

  d)Once ESET AV Remover uninstalls third-party security software, or if you have not removed any application, click **Continue to installation**.

- If you do not use any third-party security product on your local computer, click **Continue**.



This computer will be managed remotely

Server: [redacted]:2222
Group: No group selected
License: [redacted]

The following components are included in this installer

ESET Management Agent [redacted]
Configuration: No configuration selected

ESET Endpoint Security [redacted]
Configuration: No configuration selected

ESET Full Disk Encryption [redacted]
Configuration: Encrypt all disks - TPM used if available - OPAL not used

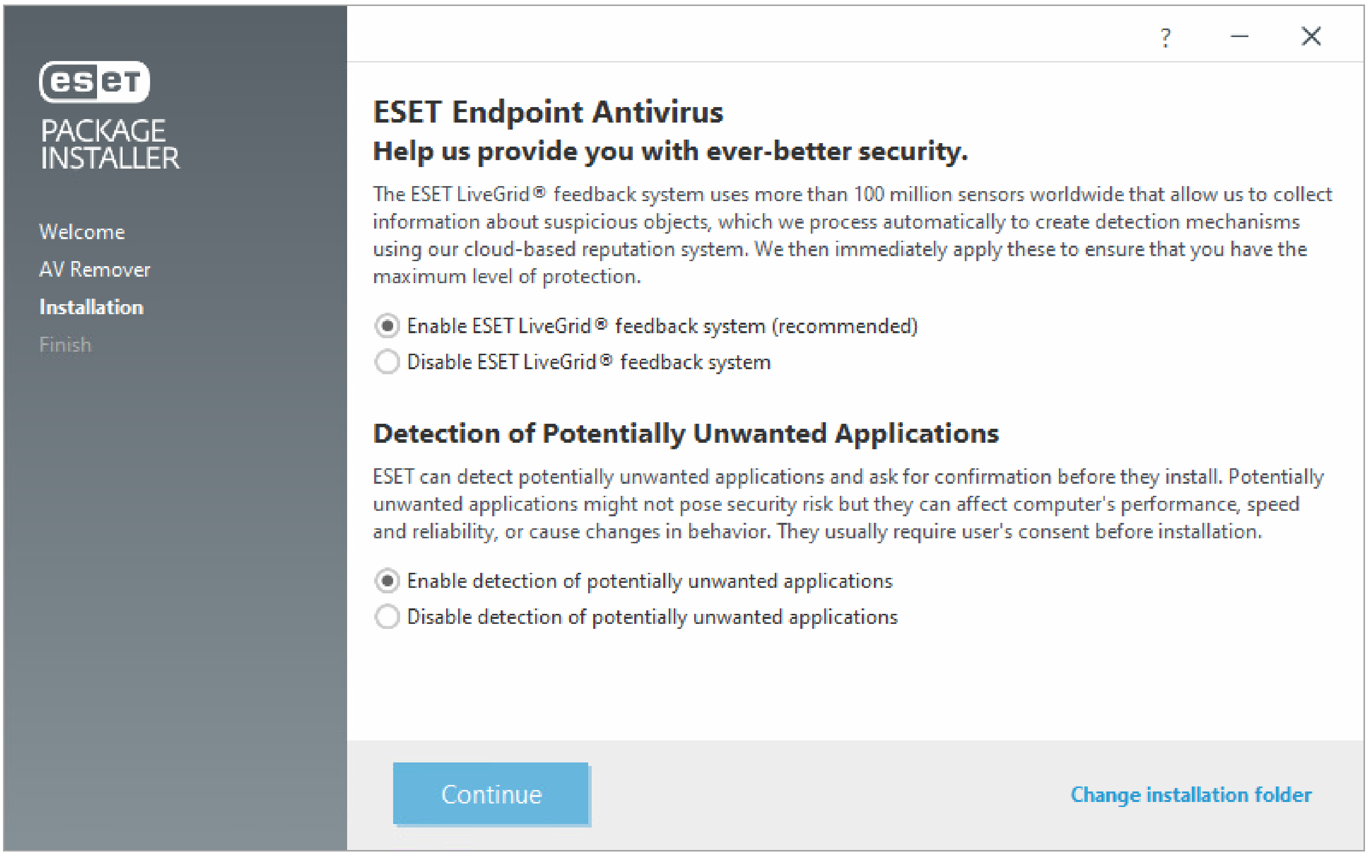
ESET Inspect Connector [redacted]
Configuration: No configuration selected

☑ I want to uninstall incompatible security products

2. **Protection settings** - select the check box next to the setting to enable it for the installer:

oEnable The ESET LiveGrid® feedback system (recommended)

oEnable detection of potentially unwanted applications - Read more in our Knowledgebase article.



ESET Endpoint Antivirus

Help us provide you with ever-better security.

The ESET LiveGrid® feedback system uses more than 100 million sensors worldwide that allow us to collect information about suspicious objects, which we process automatically to create detection mechanisms using our cloud-based reputation system. We then immediately apply these to ensure that you have the maximum level of protection.

● Enable ESET LiveGrid® feedback system (recommended)
○ Disable ESET LiveGrid® feedback system

Detection of Potentially Unwanted Applications

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

● Enable detection of potentially unwanted applications
○ Disable detection of potentially unwanted applications

3. After the installation is complete, click **Done**. The ESET security product will open automatically. You can check the status log (*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html* this location is hidden by default) on the client machine to make sure the ESET Management Agent is working properly. If there are problems with the installed ESET Management Agent (for example, it is not connecting to the ESET PROTECT Server), see Agent connection troubleshooting.

Troubleshooting

If an error has occurred during installation, see the troubleshooting section for the most common installation errors.

Other deployment methods

You can deploy the ESET Management Agent and ESET endpoint products separately and in multiple ways.

Deploy the ESET Management Agent

Local deployment:

- All-in-one installer - The package contains the ESET Management Agent and an ESET security product.

- Agent Live Installer
- Download the Agent from the ESET website and use server-assisted installation or offline installation.

Remote deployment (recommended for larger networks):

- ESET Remote Deployment Tool - Deploy the All-in-one installer remotely.
- Group Policy Object (GPO)
- Agent Deployment Server task

Deploy ESET endpoint products

After the ESET Management Agent is deployed, you can install an ESET endpoint product directly from ESET PROTECT in two ways:

- Using the Software install task
- Locally, using the standard ESET product installation

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.

ESET Remote Deployment Tool prerequisites

> For remote deployments, verify all client computers have an internet connection.

The following prerequisites must be met to use ESET Remote Deployment Tool on Windows:

- ESET PROTECT Server and the ESET PROTECT Web Console must be installed (on a Server computer).
- Appropriate ports must be opened. See ports used for remote deployment of ESET Management Agent to a target computer with Windows OS.
- The names of installation packages must include string "x86" or "x64". Otherwise the deployment will not work.
- A bundle (All-in-one) installer package must be created and downloaded to your local drive.
- It is necessary to have permissions to create All-in-one installer.

The deployment may fail due to a number of reasons. In case of any problems with deployment, read the Troubleshooting chapter or verified example scenarios of ESET Management Agent deployment.

To deploy ESET Management Agents on client computers follow these steps:

1. Download the ESET Remote Deployment Tool from the ESET website.

2. Make sure all prerequisites are met.

3. Run the ESET Remote Deployment Tool on the client computer.

4. Select **Add computers manually**. You will need to manually enter the list of hostnames or IP addresses.

5. Enter the hostnames or IP addresses and click **Next**. Each IP address or hostname must be on a new line.

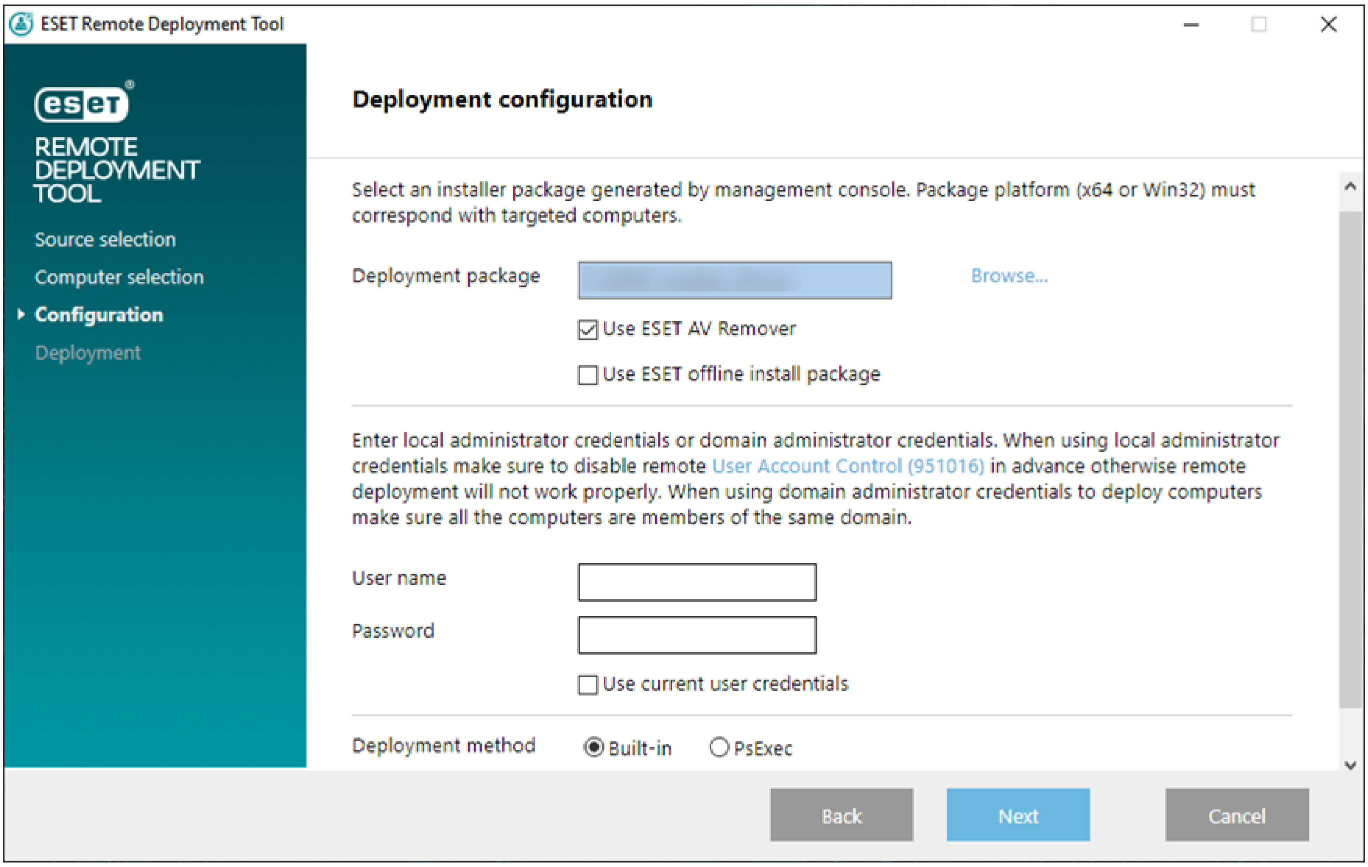
Make sure that all selected computers have the same platform (64-bit or 32-bit operating systems).

6. Selected computers for remote deployment will be displayed. Make sure all computers are added and then click **Next**.

7. Click **Browse** and select the bundle installer package you created in ESET PROTECT or ESET PROTECT Cloud Web Console. You can also select **Use ESET offline install package** (*.dat* file) created from the ESET PROTECT Live Installer. If you do not have any additional security applications installed on your local computer, deselect the check box next to **Use ESET AV Remover**. ESET AV Remover can remove certain applications.

8. Enter login credentials for the target computers. If computers are members of a domain, enter **domain administrator credentials**. If you log in with **local administration credentials**, it is necessary to disable remote UAC on the target computers. Optionally, you can select the check box next to **Use current user credentials** and login credentials will be automatically completed.

9. **Deployment method** is used to execute programs on remote machines. **Built-in** method is a default setting which supports Windows error messages. **PsExec** is a third-party tool and it is an alternative to the built-in method. Select one of these options and click **Next**.



Deployment configuration

Select an installer package generated by management console. Package platform (x64 or Win32) must correspond with targeted computers.

Deployment package

☑ Use ESET AV Remover

☐ Use ESET offline install package

Enter local administrator credentials or domain administrator credentials. When using local administrator credentials make sure to disable remote User Account Control (951016) in advance otherwise remote deployment will not work properly. When using domain administrator credentials to deploy computers make sure all the computers are members of the same domain.

User name

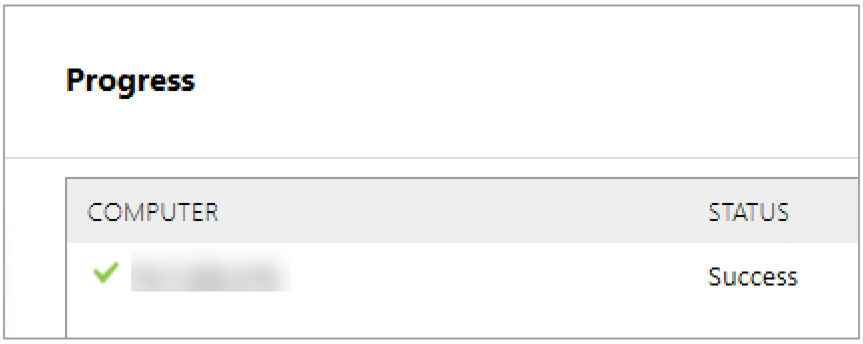
Password

☐ Use current user credentials

Deployment method ● Built-in ○ PsExec

If you have selected **PsExec**, the deployment will fail, because the tool is unable to accept the **PsExec** EULA. For a successful deployment, open the command line and run the **PsExec** command manually.

10. When the installation is started, "Success" will be displayed. Click **Finish** to complete the deployment. If deployment fails, you can export a list of failed computers. Click **Browse** next the **Export failed computers** field, select a *.txt* file to which you want to save the list and then click **Export failed computer**.



Progress

COMPUTER	STATUS
✓	Success

You can check the status log (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) on the client machine to make sure ESET Management Agent is working properly.

Other methods how to deploy ESET Management Agents by ESET Remote Deployment Tool

- Active Directory - Provide Active Directory credentials. This option includes an export of Active Directory structure for subsequent import to ESET PROTECT.
- Scan Network - Provide IP ranges to scan computers in the network.

- Import list - Provide list of hostnames or IP addresses.

Troubleshooting

> The deployment may fail due to a number of reasons. In case of any problems with deployment, read the Troubleshooting chapter or verified example scenarios of ESET Management Agent deployment.

ESET PROTECT Web Console

Log in to the ESET PROTECT Web Console

- On your local Windows server (the machine hosting your Web Console):

Click **Start** > **All Programs** > **ESET** > **ESET PROTECT Web Console**.

- From any place with internet access to your web server, type the URL in the following format (Replace "yourservername" with the actual name or IP address of your web server): https://yourservername/era/

A log-in screen opens in your default web browser. If an SSL certificate warning is displayed, add the certificate exception to your web browser.

> ! Use a supported web browser to connect to the ESET PROTECT Web Console.

When you log into the Web Console for the first time, a Startup Wizard for ESET PROTECT is displayed, and you can use the wizard to deploy ESET Management agents to computers in your network.

ESET PROTECT Web Console user interface

The ESET PROTECT Web Console user interface consists of several parts:

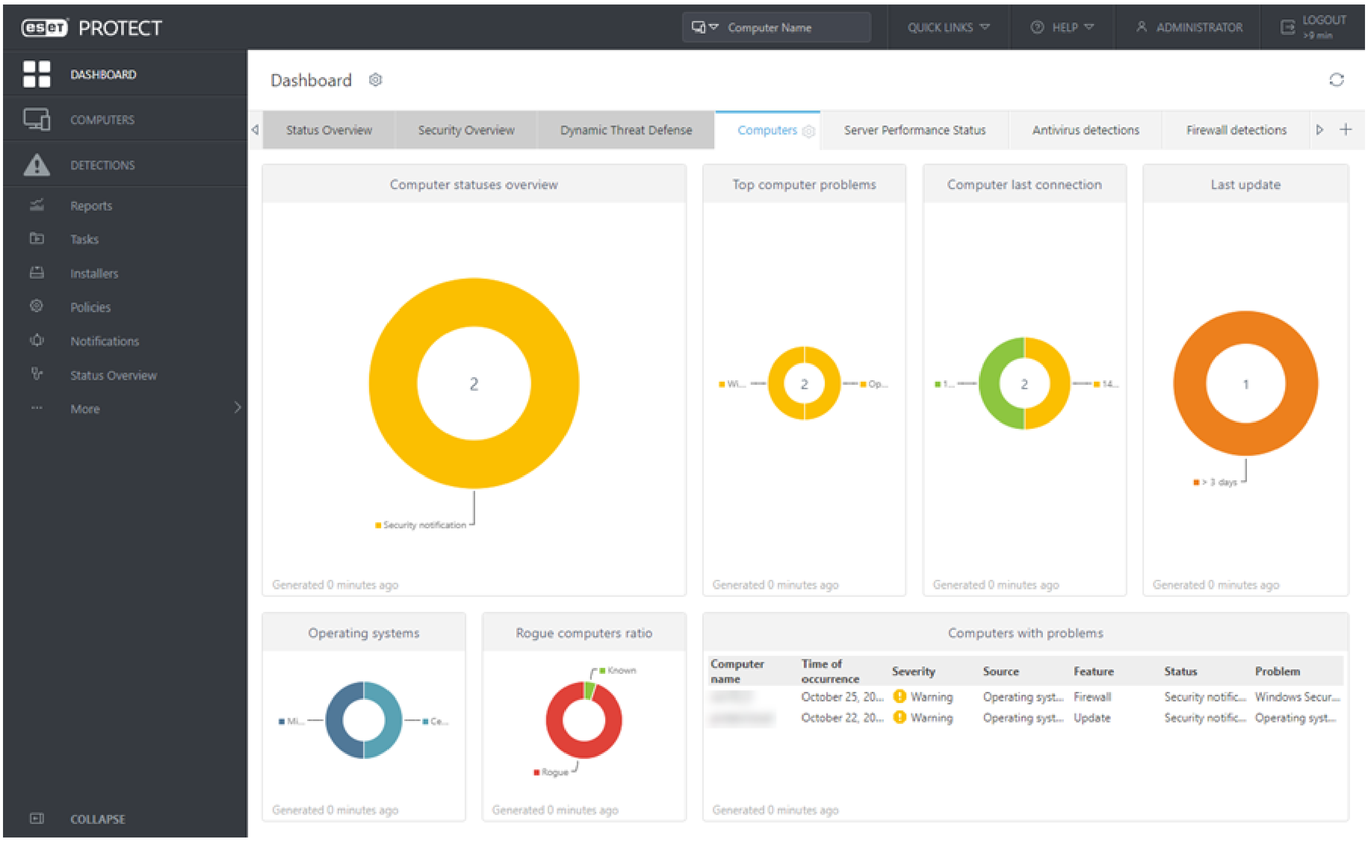
- You can use the **Search** tool at the top of the ESET PROTECT Web Console.

- Click **Quick Links** to perform some of the most commonly used Web Console actions.

- If you need help when working with ESET PROTECT, click the ? **Help** in the top right corner and click **<Current topic> - Help**. The respective help window for the current page is displayed.

- The upper right corner displays the current user with the user session timeout countdown. You can click **Logout** to log out at any time. When a session times out (because of user inactivity), you must log in again.

- The main menu on the left side of Web Console contains tools that administrators can use to manage client security solutions and ESET PROTECT server settings. You can use the tools under **More** to configure your network environment and minimize maintenance needs. You can also configure notifications and dashboards to stay aware of the network status.



Computer name	Time of occurrence	Severity	Source	Feature	Status	Problem
[redacted]	October 25, 20...	Warning	Operating syst...	Firewall	Security notific...	Windows Secur...
[redacted]	October 22, 20...	Warning	Operating syst...	Update	Security notific...	Operating syst...

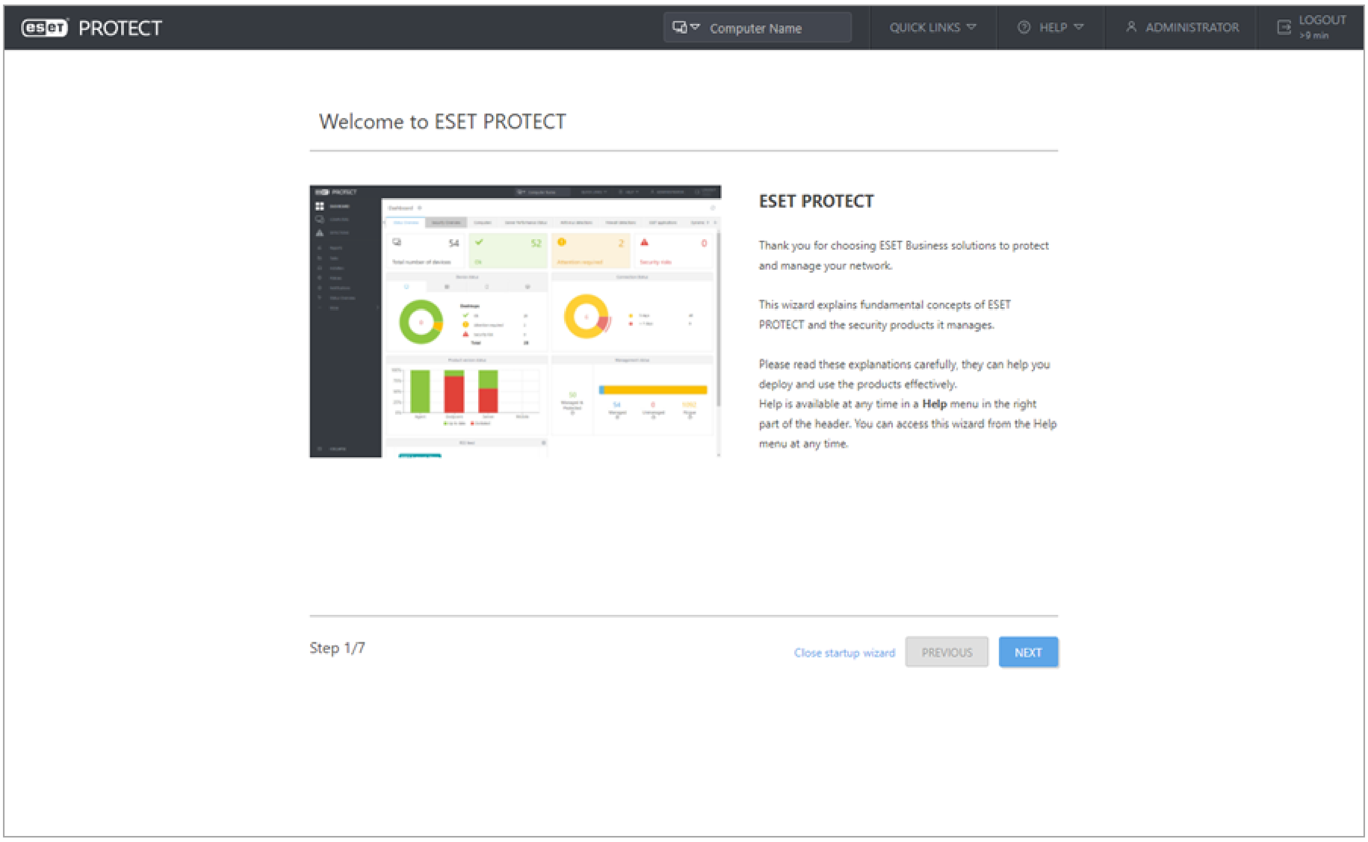
Generated 0 minutes ago

The topics below describe the main menu items:

Dashboard
Computers and Groups
Detections
Reports
Tasks
Policies
Notifications
Status Overview
More > Exclusions
More > Quarantine
More > Users and Permission Sets
More > License Management
More > Certificates

Startup Wizard

When you log into the Web Console for the first time, a **Startup Wizard** for ESET PROTECT will appear and you can use it to deploy ESET Management Agents to computers in your network. The wizard will give you a basic explanation of important ESET PROTECT Web Console sections.



Welcome to ESET PROTECT

ESET PROTECT

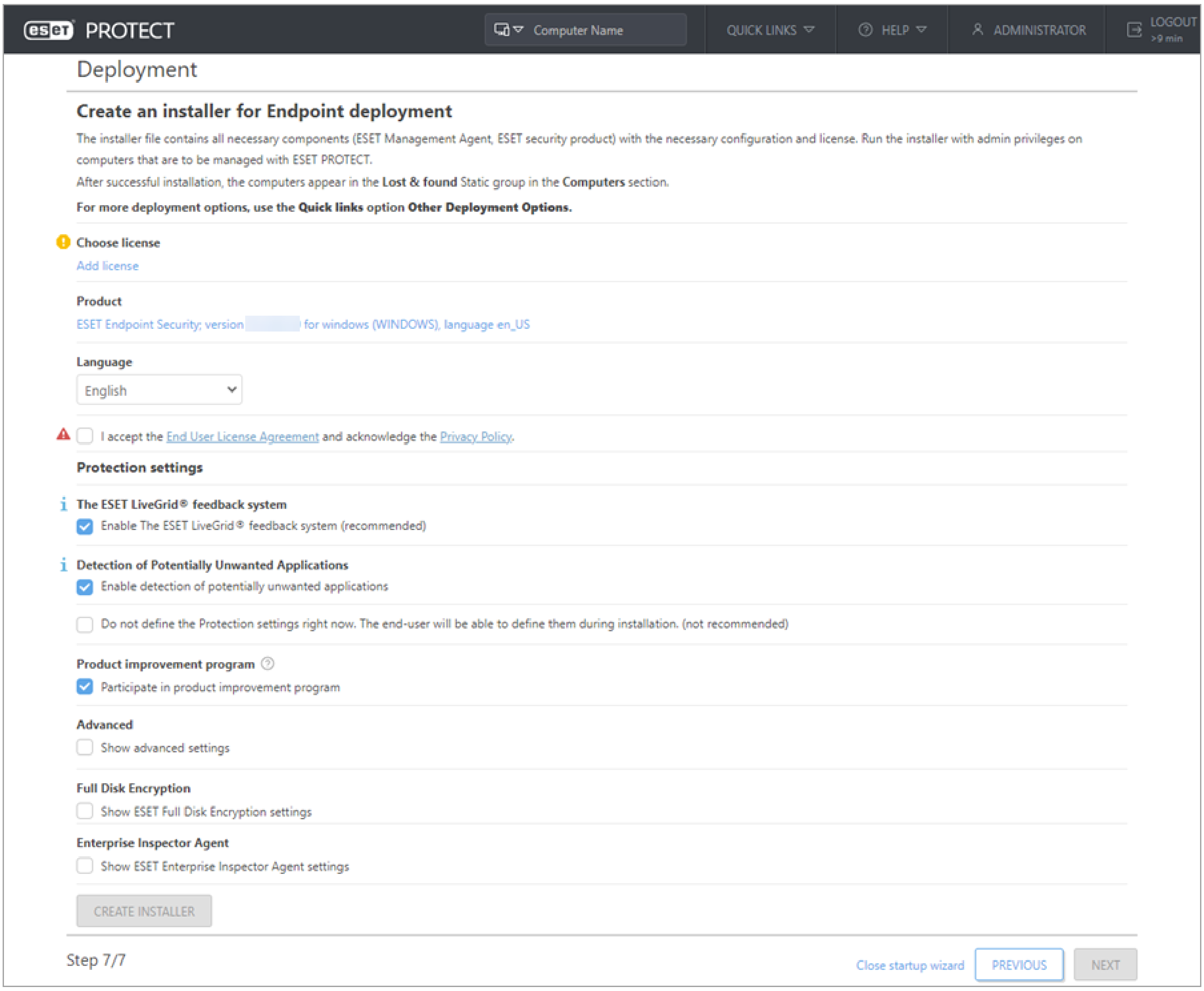
Thank you for choosing ESET Business solutions to protect and manage your network.

This wizard explains fundamental concepts of ESET PROTECT and the security products it manages.

Please read these explanations carefully, they can help you deploy and use the products effectively.
Help is available at any time in a **Help** menu in the right part of the header. You can access this wizard from the Help menu at any time.

Step 1/7

The last step of the Startup Wizard called **Deployment** helps you create an All-in-one installer package (containing the ESET Management Agent and ESET security product). You can also create an All-in-one Agent installer without using the wizard by clicking **Other Deployment Options** in the **Quick Links** section.



Deployment

Create an installer for Endpoint deployment

The installer file contains all necessary components (ESET Management Agent, ESET security product) with the necessary configuration and license. Run the installer with admin privileges on computers that are to be managed with ESET PROTECT.

After successful installation, the computers appear in the **Lost & found** Static group in the **Computers** section.

For more deployment options, use the Quick links option Other Deployment Options.

Choose license

Add license

Product

ESET Endpoint Security; version [redacted] for windows (WINDOWS), language en_US

Language

English

☐ I accept the End User License Agreement and acknowledge the Privacy Policy.

Protection settings

The ESET LiveGrid® feedback system

☑ Enable The ESET LiveGrid® feedback system (recommended)

Detection of Potentially Unwanted Applications

☑ Enable detection of potentially unwanted applications

☐ Do not define the Protection settings right now. The end-user will be able to define them during installation. (not recommended)

Product improvement program

☑ Participate in product improvement program

Advanced

☐ Show advanced settings

Full Disk Encryption

☐ Show ESET Full Disk Encryption settings

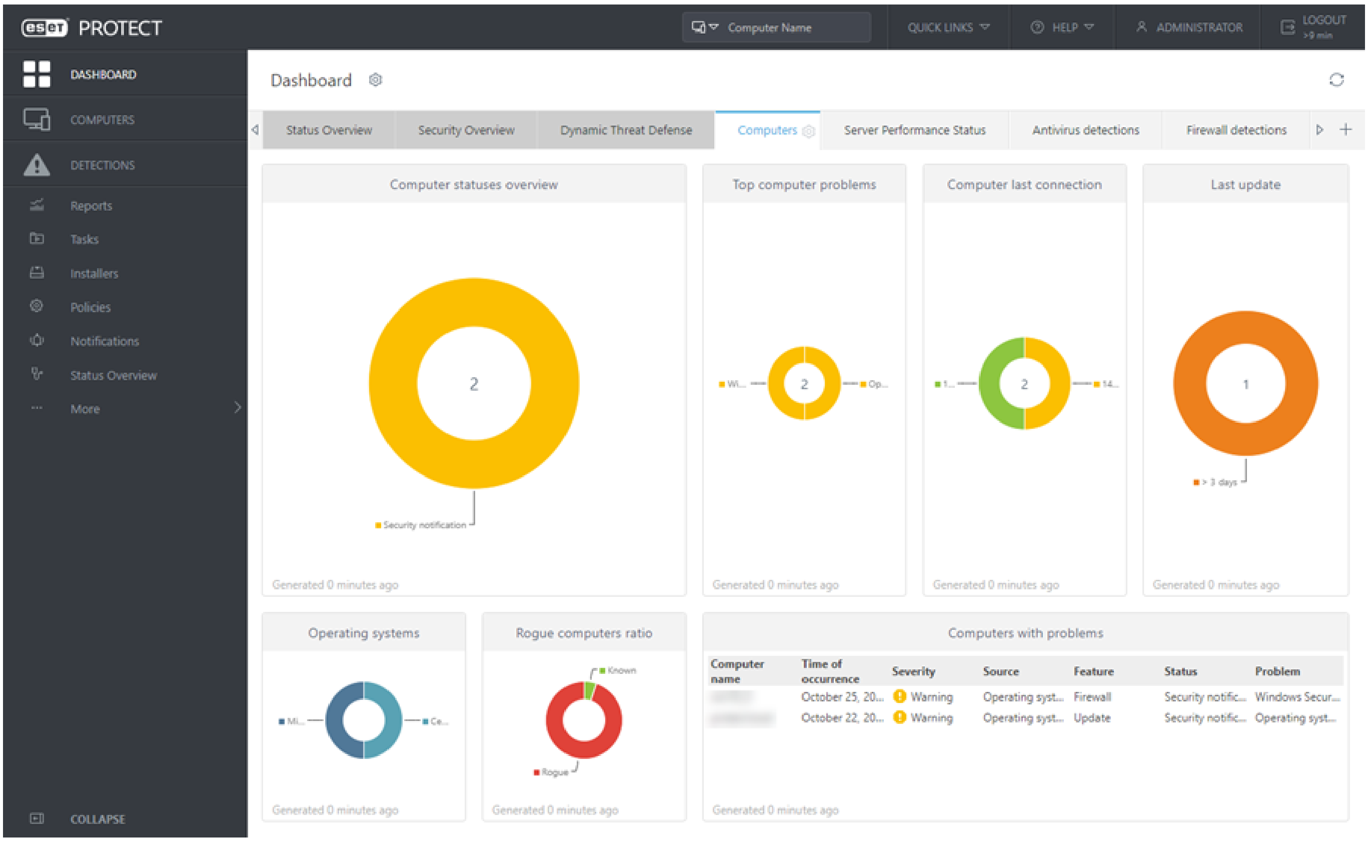
Enterprise Inspector Agent

☐ Show ESET Enterprise Inspector Agent settings

You can view the Startup Wizard again by clicking **Help** > **Startup Wizard**.

Dashboard

Dashboard is the default screen that displays after the user logs into the ESET PROTECT Web Console. It displays pre-defined reports about your network. You can switch between dashboards using the tabs on the top menu bar. Each dashboard consists of several reports.



Computer name	Time of occurrence	Severity	Source	Feature	Status	Problem
[redacted]	October 25, 20...	Warning	Operating syst...	Firewall	Security notific...	Windows Secur...
[redacted]	October 22, 20...	Warning	Operating syst...	Update	Security notific...	Operating syst...

You can customize your dashboards (except the **Status Overview**, **Security Overview** and **Dynamic Threat Defense**) by adding reports, modifying existing reports, resizing, moving and re-arranging reports. This flexibility allows you to create a comprehensive overview of ESET PROTECT and its objects (computers, groups, tasks, policies, users, etc.).

The following dashboards come pre-configured in ESET PROTECT:

- **Status Overview** - Basic dashboard window with the key information about your ESET PROTECT network. This dashboard cannot be modified.
- **Security Overview** - This dashboard provides an overview of unresolved detections reported in the last 7 days, including their severity, detection method, resolution status and top 10 computers/users with detections. This dashboard cannot be modified.
- **Dynamic Threat Defense** - If you are using the ESET Dynamic Threat Defense, you can find here an overview of useful ESET Dynamic Threat Defense reports.
- **Computers** - This dashboard gives you an overview of client machines - their protection status, operating systems, update status, etc.
- **Server Performance Status** - This dashboard lets you view information about the ESET PROTECT server itself - server load, clients with problems, CPU load, database connections, etc.
- **Antivirus detections** - Here you can see reports from the anti-virus module of the client security products - active detections, detections in the last 7/30 days and so on.
- **Firewall detections** - Firewall events of the connected clients - according to their severity, time of reporting, etc.
- **ESET applications** - This dashboard lets you view information about installed ESET applications.

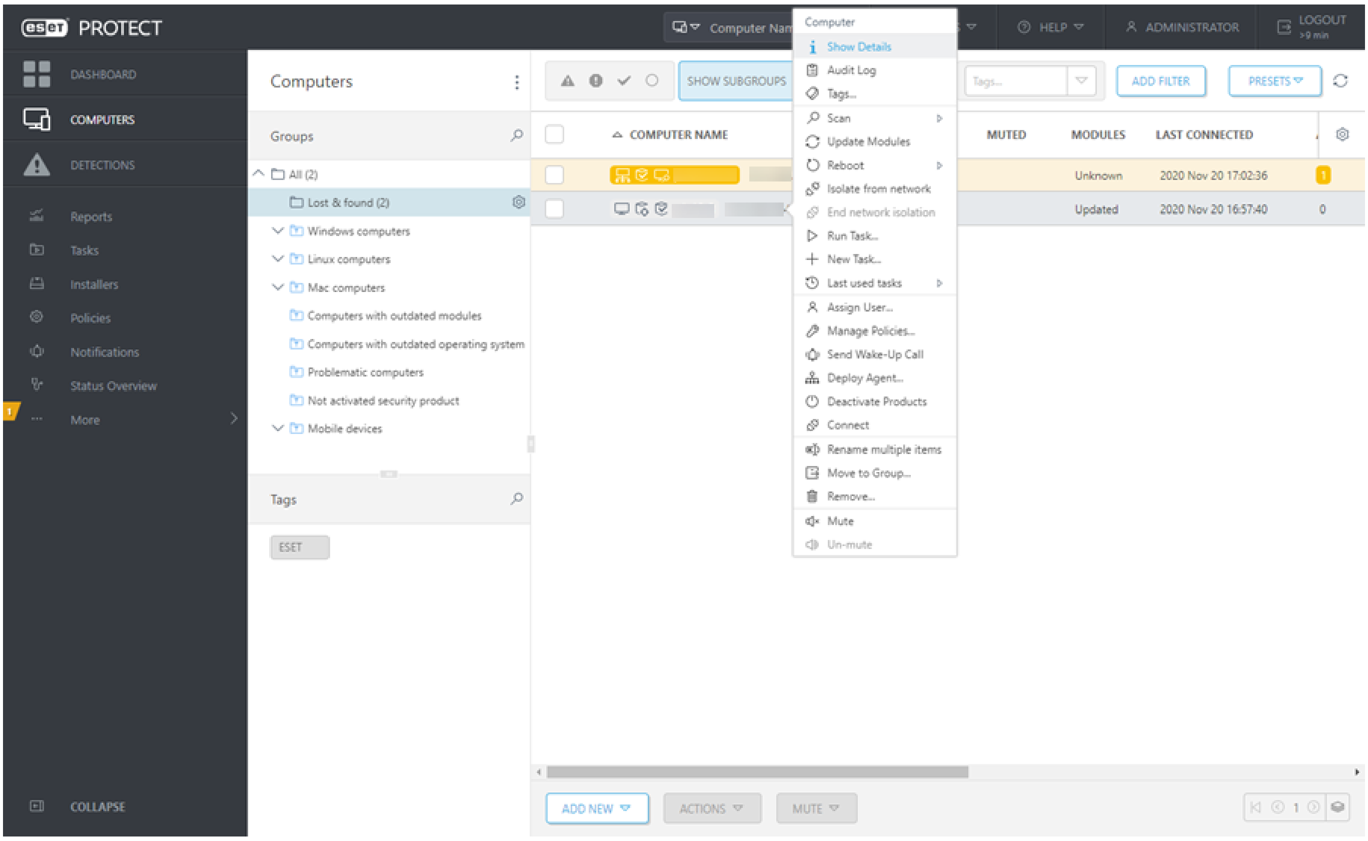
- **Cloud-based protection** - This dashboard gives you an overview of cloud-based protection reports (ESET LiveGrid® and if you have the eligible license, also ESET Dynamic Threat Defense).

Computers

All client computers that are reachable by ESET PROTECT are displayed in **Computers** and organized by groups. Clicking a group from the list (left pane) displays the members (clients) of this group in the right pane. You can drag-and-drop clients to move them between groups.

Manage computers

Click a device to open a new menu with actions available for that device. You can also select the check box next to a device and click **Actions** on the bottom bar. The **Actions** menu displays different options depending on the type of device.



Filter computers

If you cannot find a specific computer in the list and know it is in your ESET PROTECT infrastructure, make sure to disable all filters.

You can filter the clients (computers) using the filters at the top of the page:

- Select the **Show Subgroups** check box to show subgroups of the currently selected group.
- Clicking **Add Filter** shows the available filtering criteria. A few predefined filters are also available and quickly accessible.

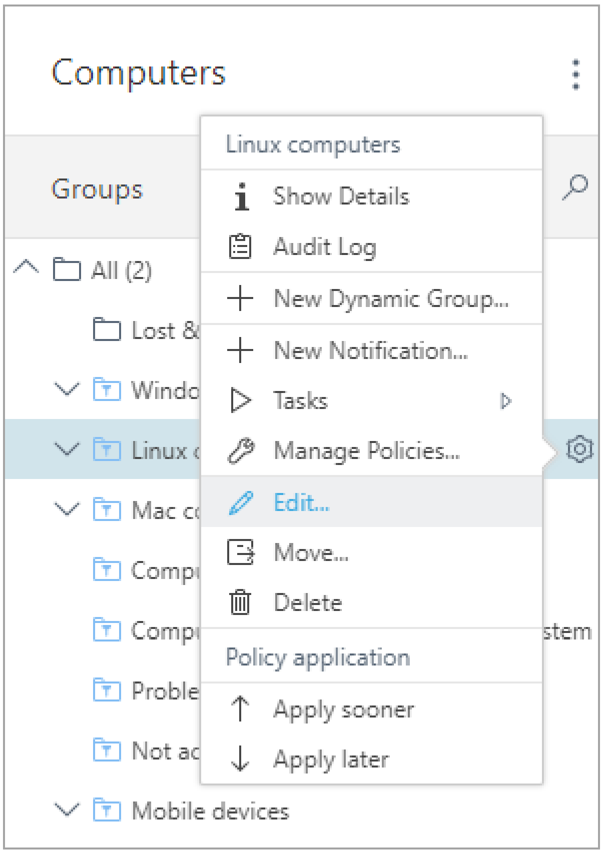
- You can click **Add Filter** > **Product Category** and select from the available categories:
    - **All Devices** - Display all client computers without filtering. You can use a combination of all the above filtering options when narrowing down the view.
    - **ESET Protected** - Display clients protected by an ESET product.
    - **ESET PROTECT -** Display individual ESET PROTECT components such as Agent, RD Sensor, and Proxy.
    - **Other** - Display only client computers running the selected product (Shared Local Cache, Virtual Security Appliance, or Enterprise Inspector).
- You can use the status icons to filter clients by the severity of issues detected (⚠ red for errors, ❗ yellow for warnings, ✓ green for notices, and ○ gray for unmanaged computers). The status icon represents the current status of a specific client computer and the ESET solution installed on it. You can hide or show the status icons of different severity to evaluate clients on your network by status. For example, to see only the computers with warnings, activate only the yellow icon (the rest of the icons must be inactive). To see both warnings and errors, activate the red and yellow status icons. Unmanaged computers ○ (clients on the network that do not have the ESET Management Agent or an ESET security product installed) usually appear in the **Lost & found** static group.
- You can also click the header of a column to sort computers by that attribute.

Last Connected displays the date and time of last connection of the managed device. A green dot indicates that the computer connected less than 10 minutes ago. The **Last Connected** information gets highlighted to indicate that the computer is not connecting:

- Yellow (error) - computer is not connecting for 2-14 days.
- Red (warning) - computer is not connecting for more than 14 days.

Groups

You can manage groups from 🖥 Computers. Groups enable you to organize endpoints on your network so that you can assign policies and tasks to them systematically. The setting applies to all the group members. Computers that are members of a group are listed on the right pane. Click the gear icon ⚙ next to a group name to see the available group actions and group details.



There are two types of groups: static groups and dynamic groups.

Static Groups

- Static groups are groups of selected client computers and other objects.
- All mobile and computer devices are located in a static group.
- You can manually select which endpoints belong to any static group.
- An object can only be present in one static group.
- Static groups play an important role in the ESET PROTECT security model.

Dynamic Groups

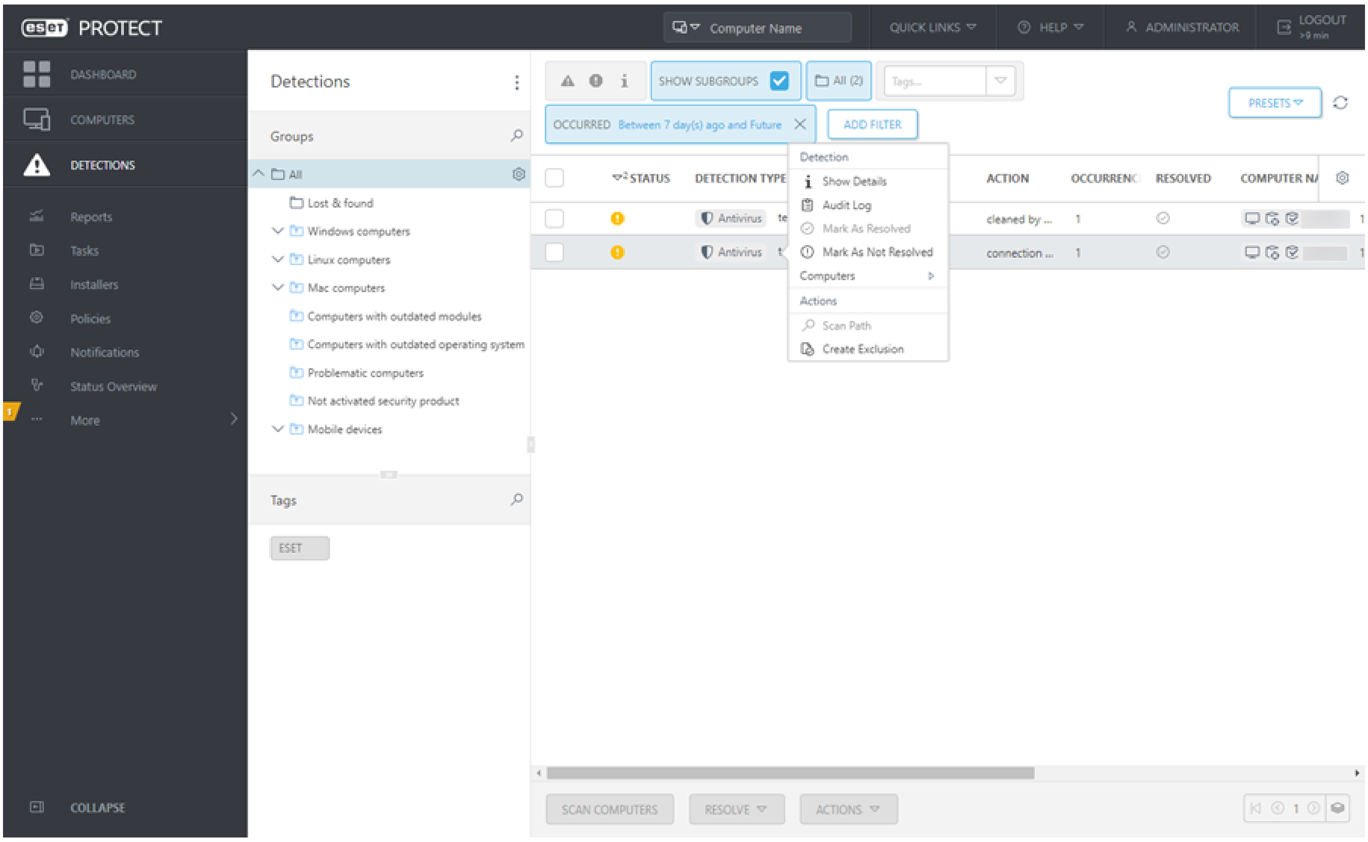
- You can understand dynamic groups as custom filters where one can set rules to filter computers accordingly.
- Dynamic groups are template-based and automatically include endpoints that meet the criteria established in your template.
- If a client device does not meet the criteria, it is automatically removed from the dynamic group.
- A computer can be in various dynamic groups at the same time or in none at all.

Knowledgebase articles are available to help you add computers to static groups, create new dynamic group templates, and assign a policy to a group.

You can find additional information on groups in Groups.

Detections

To access detection reports, click **Detections** in the Web Console menu on the left. The **Detections** panel gives you an overview of all detections found on computers in your network.



You can browse groups and view detections on members of a given group. You can filter the view; all detection types from the last seven days are visible by default. Detections can be **Marked as resolved** in the **Detections** section or under details for a specific client.

Detections are aggregated by time and other criteria to simplify their resolution. Detections older than 24 hours are aggregated automatically every midnight. You can identify aggregated detections by the X/Y (resolved items/total items) value in the **Resolved** column. You can see the list of aggregated detections in the **Occurrences** tab in detection details.

You can find the quarantined detections in ⋯ **More** > **Quarantine**.

Exclusions

You can exclude selected item(s) in **Detections** from being detected in the future. Click a detection and select **Create Exclusion**. You can exclude only **Antivirus** detections and **Firewall** detections - IDS rules. You can create an exclusion and apply it to more computers and groups.

⚠ Use exclusions with caution. They may result in an infected computer.

The ⋯ **More** > **Exclusions** section contains all created exclusions, increases their visibility, and simplifies their management.

Detections in archives

If one or more detections are found in an archive, the archive and each detection inside the archive are reported in **Detections**.

> ⚠ Excluding an archive file that contains a detection does not exclude the detection. You must exclude the individual detections inside the archive. The maximum file size for files contained in archives is 3 GB.

The excluded detections will not be detected anymore, even if they occur in another archive or are unarchived.

Ransomware Shield

ESET business products (version 7 and later) include **Ransomware Shield**. This new security feature is a part of HIPS and protects computers from ransomware. When ransomware is detected on a client computer, you can view the detection details in the ESET PROTECT Web Console under **Detections**. To filter only ransomware detections, click **Add Filter** > **Scanner** > **Anti-Ransomware scanner**. For more information about Ransomware Shield, see the ESET Glossary.

You can remotely configure **Ransomware Shield** from the ESET PROTECT Web Console using the **Policy** settings for your ESET business product:

- **Enable Ransomware Shield** - The ESET business product automatically blocks all the suspicious applications that behave like ransomware.

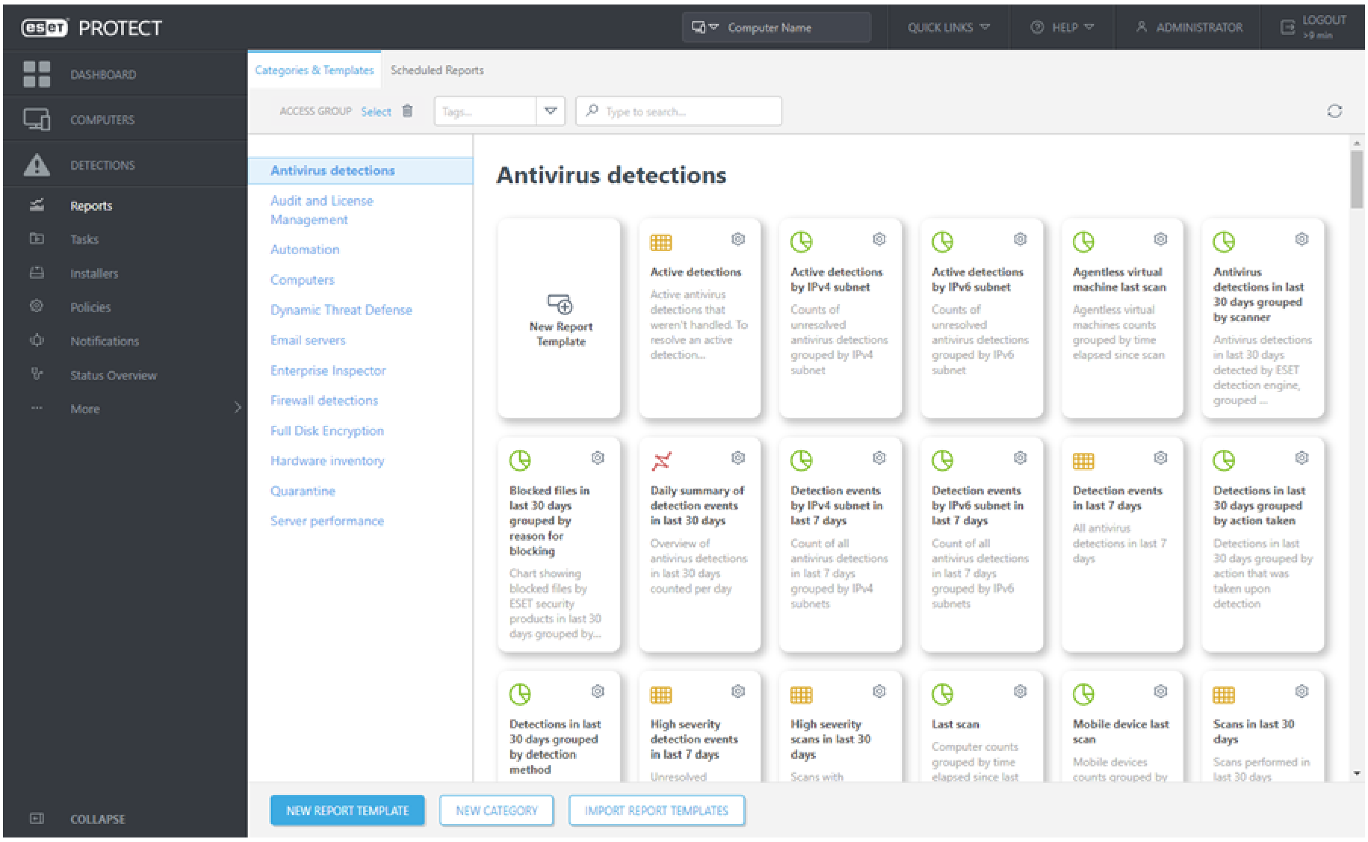
- **Enable Audit Mode** - When you enable the Audit Mode, detections identified by the Ransomware Shield are reported in the ESET PROTECT Web Console, but the ESET security product does not block them. The administrator can decide to block the reported detection or exclude it by selecting **Create Exclusion**. This Policy setting is available only via ESET PROTECT Web Console.

> ! By default, Ransomware Shield blocks all applications with potential ransomware behavior, including legitimate applications. We recommend that you **Enable Audit Mode** for a short period on a new managed computer, so that you can exclude legitimate applications that are detected as ransomware based on their behavior (false positives). We do not recommend that you use the Audit Mode permanently, because ransomware on the managed computers is not automatically blocked when Audit Mode is enabled.

Reports

Reports allow you to access and filter data from the database in a convenient way. Reports have categories, and each category includes a short description.

To access reports, click **Reports** in the Web Console menu on the left, select the desired report template (a tile with a description and action) for which you want to view the report, and click the ⚙ (gear icon) > **Generate Now**.


PROTECT
Computer Name
QUICK LINKS
HELP
ADMINISTRATOR
LOGOUT
>9 min
DASHBOARD
COMPUTERS
DETECTIONS
Reports
Tasks
Installers
Policies
Notifications
Status Overview
More
COLLAPSE
Categories & Templates
Scheduled Reports
ACCESS GROUP Select
Tags...
Type to search...
Antivirus detections
Audit and License Management
Automation
Computers
Dynamic Threat Defense
Email servers
Enterprise Inspector
Firewall detections
Full Disk Encryption
Hardware inventory
Quarantine
Server performance
Antivirus detections
New Report Template
Active detections
Active antivirus detections that weren't handled. To resolve an active detection...
Active detections by IPv4 subnet
Counts of unresolved antivirus detections grouped by IPv4 subnet
Active detections by IPv6 subnet
Counts of unresolved antivirus detections grouped by IPv6 subnet
Agentless virtual machine last scan
Agentless virtual machines counts grouped by time elapsed since scan
Antivirus detections in last 30 days grouped by scanner
Antivirus detections in last 30 days detected by ESET detection engine, grouped ...
Blocked files in last 30 days grouped by reason for blocking
Chart showing blocked files by ESET security products in last 30 days grouped by...
Daily summary of detection events in last 30 days
Overview of antivirus detections in last 30 days counted per day
Detection events by IPv4 subnet in last 7 days
Count of all antivirus detections in last 7 days grouped by IPv4 subnets
Detection events by IPv6 subnet in last 7 days
Count of all antivirus detections in last 7 days grouped by IPv6 subnets
Detection events in last 7 days
All antivirus detections in last 7 days
Detections in last 30 days grouped by action taken
Detections in last 30 days grouped by action that was taken upon detection
Detections in last 30 days grouped by detection method
High severity detection events in last 7 days
Unresolved
High severity scans in last 30 days
Scans with
Last scan
Computer counts grouped by time elapsed since last
Mobile device last scan
Mobile devices counts grouped by
Scans in last 30 days
Scans performed in last 30 days
NEW REPORT TEMPLATE
NEW CATEGORY
IMPORT REPORT TEMPLATES

> By default, all report templates are only accessible to the administrator. Other users cannot see or use these templates unless assigned sufficient permission (or unless templates are in another location).

To receive reports via email, you must configure an SMTP server connection properly.

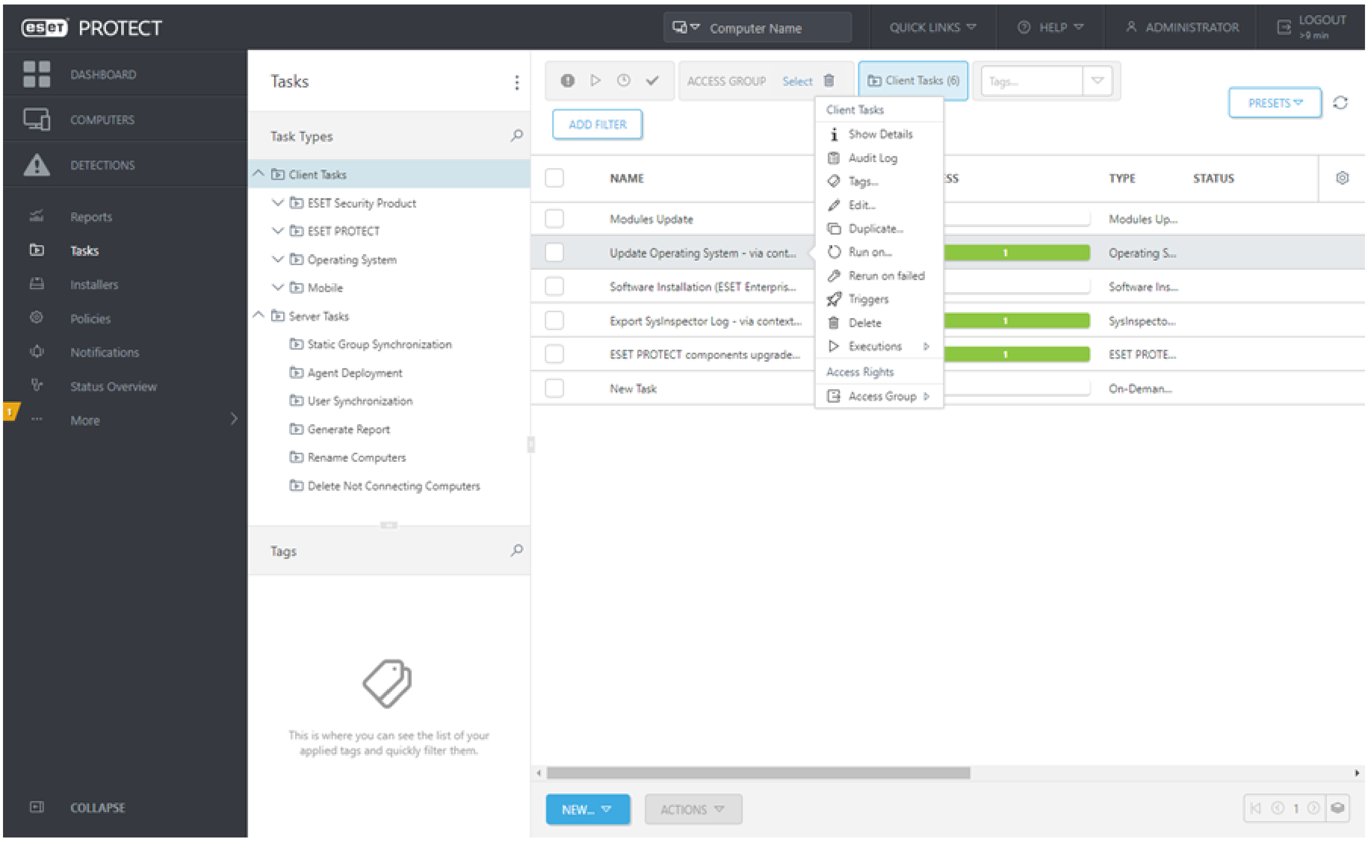
See the ESET Knowledgebase article for step-by-step instructions to configure automated reports in ESET PROTECT.

Tasks

You can use tasks to manage the ESET PROTECT server, client computers, and ESET products. Tasks can automate routine jobs. Task targets can be individual computers and groups.

Tasks enable you to assign specific procedures to individual clients or groups of clients.

In addition to the **Tasks** window, you can create tasks from context menus in Computers. To see the status of executed tasks, click **Tasks**, and observe whether tasks have finished successfully.



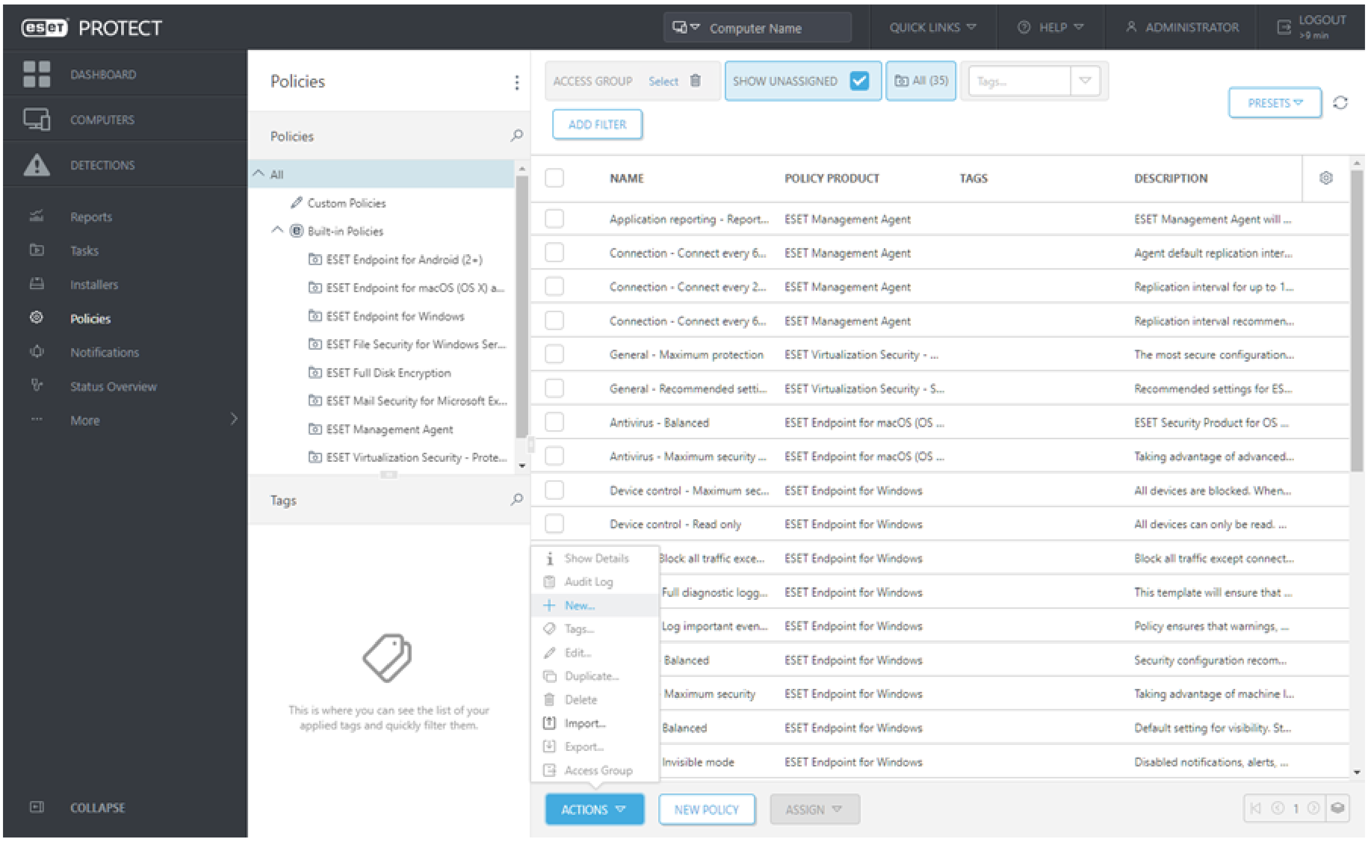
The Tasks section of the ESET PROTECT Administrator Guide contains information about how to create, assign, and schedule new tasks.

The ESET Knowledgebase has examples of procedures to configure specific tasks, such as:

- Send a wake-up call to client computers to execute a task immediately in ESET PROTECT.
- Change the agent connection interval for client computers in ESET PROTECT.
- Use a Software Install client task to deploy or upgrade ESET endpoint products.
- Synchronize ESET PROTECT with Active Directory.

Policies

You can use policies to manage client computers. Policies are sets of configuration rules you can apply to ESET products running on client computers so that you can avoid configuring each client's ESET product manually. You can apply a policy directly to individual computers and groups. You can also assign multiple policies to a computer or a group.



NAME	POLICY PRODUCT	TAGS	DESCRIPTION
Application reporting - Report...	ESET Management Agent		ESET Management Agent will ...
Connection - Connect every 6...	ESET Management Agent		Agent default replication inter...
Connection - Connect every 2...	ESET Management Agent		Replication interval for up to 1...
Connection - Connect every 6...	ESET Management Agent		Replication interval recommen...
General - Maximum protection	ESET Virtualization Security - ...		The most secure configuration...
General - Recommended setti...	ESET Virtualization Security - S...		Recommended settings for ES...
Antivirus - Balanced	ESET Endpoint for macOS (OS ...		ESET Security Product for OS ...
Antivirus - Maximum security ...	ESET Endpoint for macOS (OS ...		Taking advantage of advanced...
Device control - Maximum sec...	ESET Endpoint for Windows		All devices are blocked. When...
Device control - Read only	ESET Endpoint for Windows		All devices can only be read. ...
Block all traffic exce...	ESET Endpoint for Windows		Block all traffic except connect...
Full diagnostic logg...	ESET Endpoint for Windows		This template will ensure that ...
Log important even...	ESET Endpoint for Windows		Policy ensures that warnings, ...
Balanced	ESET Endpoint for Windows		Security configuration recom...
Maximum security	ESET Endpoint for Windows		Taking advantage of machine l...
Balanced	ESET Endpoint for Windows		Default setting for visibility. St...
Invisible mode	ESET Endpoint for Windows		Disabled notifications, alerts, ...

Follow the steps from the ESET Knowledgebase article to create a new policy and assign it to a group.

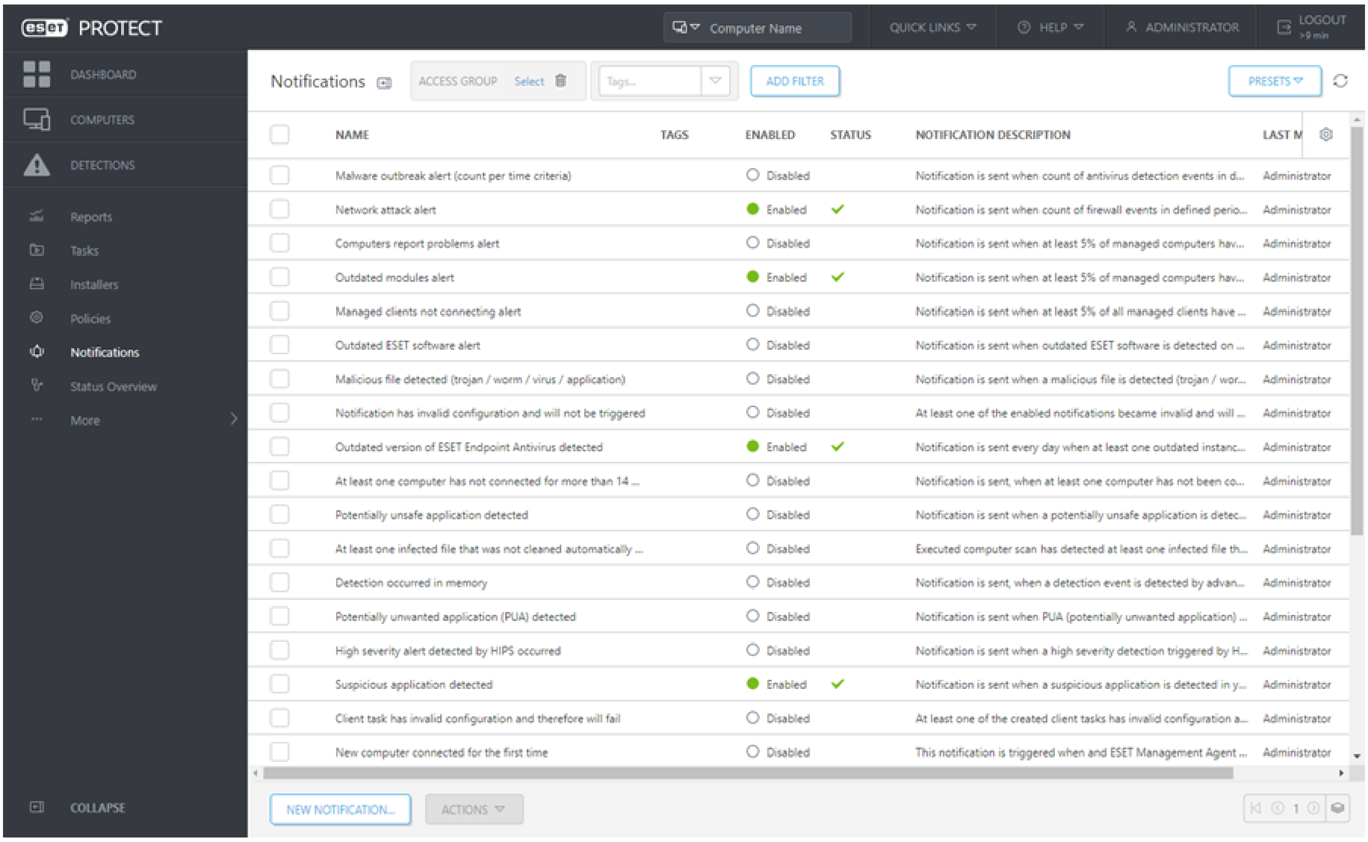
Policies are applied in the order that static groups are arranged. This rule is not valid for dynamic groups, where child dynamic groups are traversed first so that you can apply policies with greater impact at the top of the group tree and apply more specific policies for subgroups.

> ESET recommends that you assign more generic policies (for example, the update server) to groups that are higher within the group tree. You should assign more specific policies (for example, device control settings) farther down in the group tree.

Refer to the Policies section of the ESET PROTECT Administrator Guide to learn more about managing and applying policies and about policy removal rules.

Notifications

You can configure automatic notifications based on specific events such as reported detections, out-of-date endpoints, and more. See the Notifications section of the ESET PROTECT Administrator guide or our Knowledgebase article for more information about how to configure and manage notifications.



☐	NAME	TAGS	ENABLED	STATUS	NOTIFICATION DESCRIPTION	LAST M
☐	Malware outbreak alert (count per time criteria)		○ Disabled		Notification is sent when count of antivirus detection events in d...	Administrator
☐	Network attack alert		● Enabled	✓	Notification is sent when count of firewall events in defined perio...	Administrator
☐	Computers report problems alert		○ Disabled		Notification is sent when at least 5% of managed computers hav...	Administrator
☐	Outdated modules alert		● Enabled	✓	Notification is sent when at least 5% of managed computers hav...	Administrator
☐	Managed clients not connecting alert		○ Disabled		Notification is sent when at least 5% of all managed clients have ...	Administrator
☐	Outdated ESET software alert		○ Disabled		Notification is sent when outdated ESET software is detected on ...	Administrator
☐	Malicious file detected (trojan / worm / virus / application)		○ Disabled		Notification is sent when a malicious file is detected (trojan / wor...	Administrator
☐	Notification has invalid configuration and will not be triggered		○ Disabled		At least one of the enabled notifications became invalid and will ...	Administrator
☐	Outdated version of ESET Endpoint Antivirus detected		● Enabled	✓	Notification is sent every day when at least one outdated instanc...	Administrator
☐	At least one computer has not connected for more than 14 ...		○ Disabled		Notification is sent, when at least one computer has not been co...	Administrator
☐	Potentially unsafe application detected		○ Disabled		Notification is sent when a potentially unsafe application is detec...	Administrator
☐	At least one infected file that was not cleaned automatically ...		○ Disabled		Executed computer scan has detected at least one infected file th...	Administrator
☐	Detection occurred in memory		○ Disabled		Notification is sent, when a detection event is detected by advan...	Administrator
☐	Potentially unwanted application (PUA) detected		○ Disabled		Notification is sent when PUA (potentially unwanted application) ...	Administrator
☐	High severity alert detected by HIPS occurred		○ Disabled		Notification is sent when a high severity detection triggered by H...	Administrator
☐	Suspicious application detected		● Enabled	✓	Notification is sent when a suspicious application is detected in y...	Administrator
☐	Client task has invalid configuration and therefore will fail		○ Disabled		At least one of the created client tasks has invalid configuration a...	Administrator
☐	New computer connected for the first time		○ Disabled		This notification is triggered when and ESET Management Agent ...	Administrator

To receive notifications via email, you need to configure an SMTP server connection properly.

ESET PROTECT can automatically send email reports and notifications. Enable **Use SMTP server**, click **More** > **Server Settings** > **Advanced Settings** > **SMTP Server** and specify the following:

- **Host** - Hostname or an IP address of your SMTP server
- **Port** - SMTP uses port 25 by default, but you can change it if your SMTP server uses a different port.
- **Username** - If your SMTP server requires authentication, specify the SMTP user account name (do not include the domain as this will not work).
- **Password** - The password associated with the SMTP user account
- **Connection security type** - Specify the connection type, the default is **Not secured**, but if your SMTP server allows for secure connections, choose TLS or STARTTLS. If you want to make your connection more secure, use a STARTTLS or a SSL/TLS extension, because they use a separate port for encrypted communication.
- **Authentication type** - The default is set to **No authentication**. However, you can select the appropriate Authentication type from the drop-down list (for example, Login, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM, or Automatic)
- **Sender address** - Specify the sender address that will be displayed in the header of notification emails (From:)
- **Test SMTP server** - This is to make sure the SMTP settings are correct. Click **Send test email** to open a pop-up window. Type the recipient's email address, and the test email message will be sent via the SMTP server to this address. Check the recipient's mailbox to verify that the test email was delivered.

You can use Gmail as the SMTP server if you have a Gmail account. Use the settings below:

Setting	Value
Use SMTP server	*True*
Host	`smtp.gmail.com`
Port	**465** (**TLS**) or **587** (**STARTTLS**)
Username	*your Gmail address*
Password	*your Gmail password*
Connection security type	**TLS** or **STARTTLS**
Authentication type	**Automatic**
Sender address	*your Gmail address*

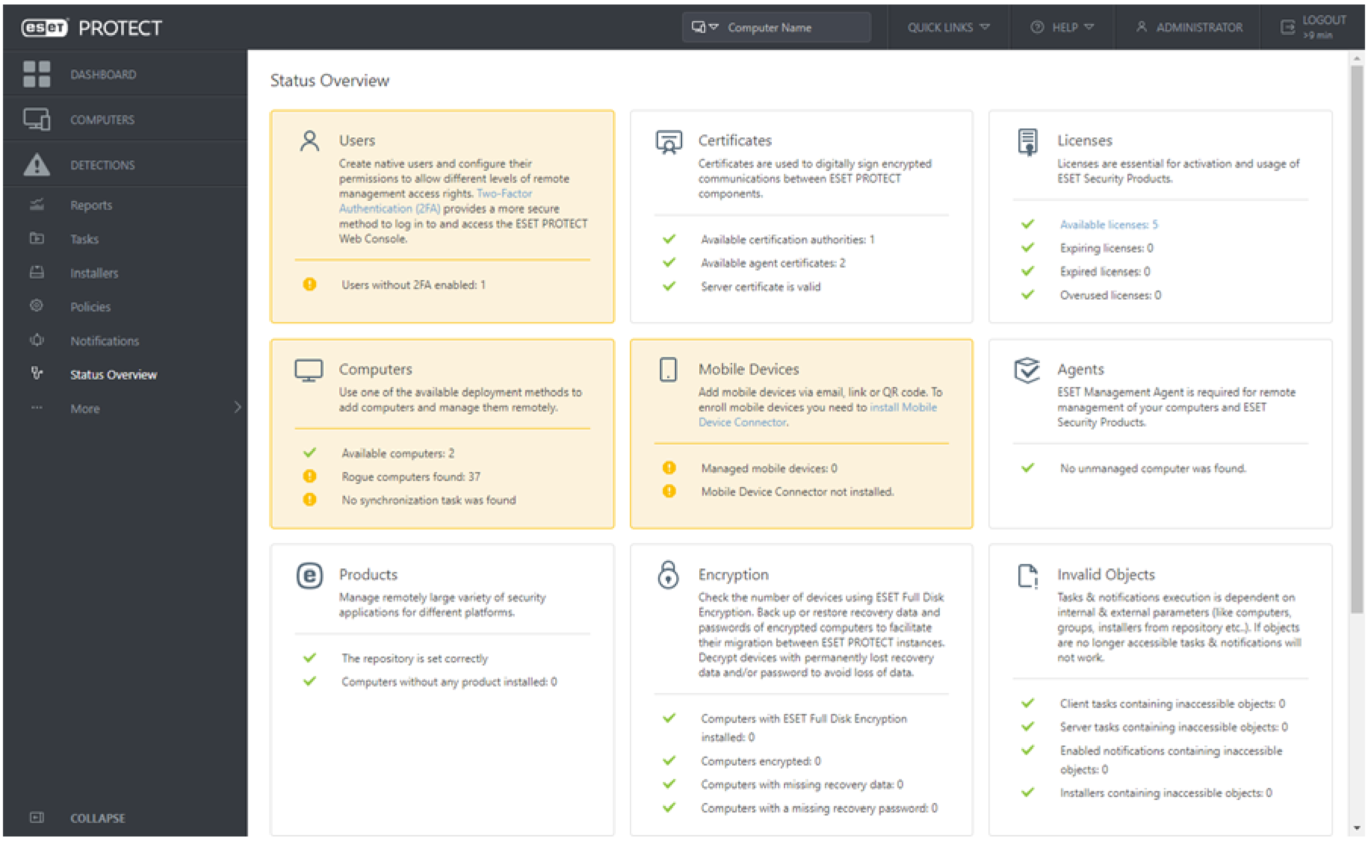
If sending of emails fails, you may need to allow less secure apps in your Gmail account or unlock your Gmail account.

Status overview

The ESET PROTECT server performs periodic diagnostics checkups.

1. Click **Status Overview** to see detailed status information about ESET PROTECT. Use the **Status Overview** to see usage statistics and the general status of your ESET PROTECT. It can also help you with the initial configuration of ESET PROTECT.

2. Click a section tile to display a taskbar on the right with actions.



Status Overview

Users
Create native users and configure their permissions to allow different levels of remote management access rights. Two-Factor Authentication (2FA) provides a more secure method to log in to and access the ESET PROTECT Web Console.
- ! Users without 2FA enabled: 1

Certificates
Certificates are used to digitally sign encrypted communications between ESET PROTECT components.
- ✓ Available certification authorities: 1
- ✓ Available agent certificates: 2
- ✓ Server certificate is valid

Licenses
Licenses are essential for activation and usage of ESET Security Products.
- ✓ Available licenses: 5
- ✓ Expiring licenses: 0
- ✓ Expired licenses: 0
- ✓ Overused licenses: 0

Computers
Use one of the available deployment methods to add computers and manage them remotely.
- ✓ Available computers: 2
- ! Rogue computers found: 37
- ! No synchronization task was found

Mobile Devices
Add mobile devices via email, link or QR code. To enroll mobile devices you need to install Mobile Device Connector.
- ! Managed mobile devices: 0
- ! Mobile Device Connector not installed.

Agents
ESET Management Agent is required for remote management of your computers and ESET Security Products.
- ✓ No unmanaged computer was found.

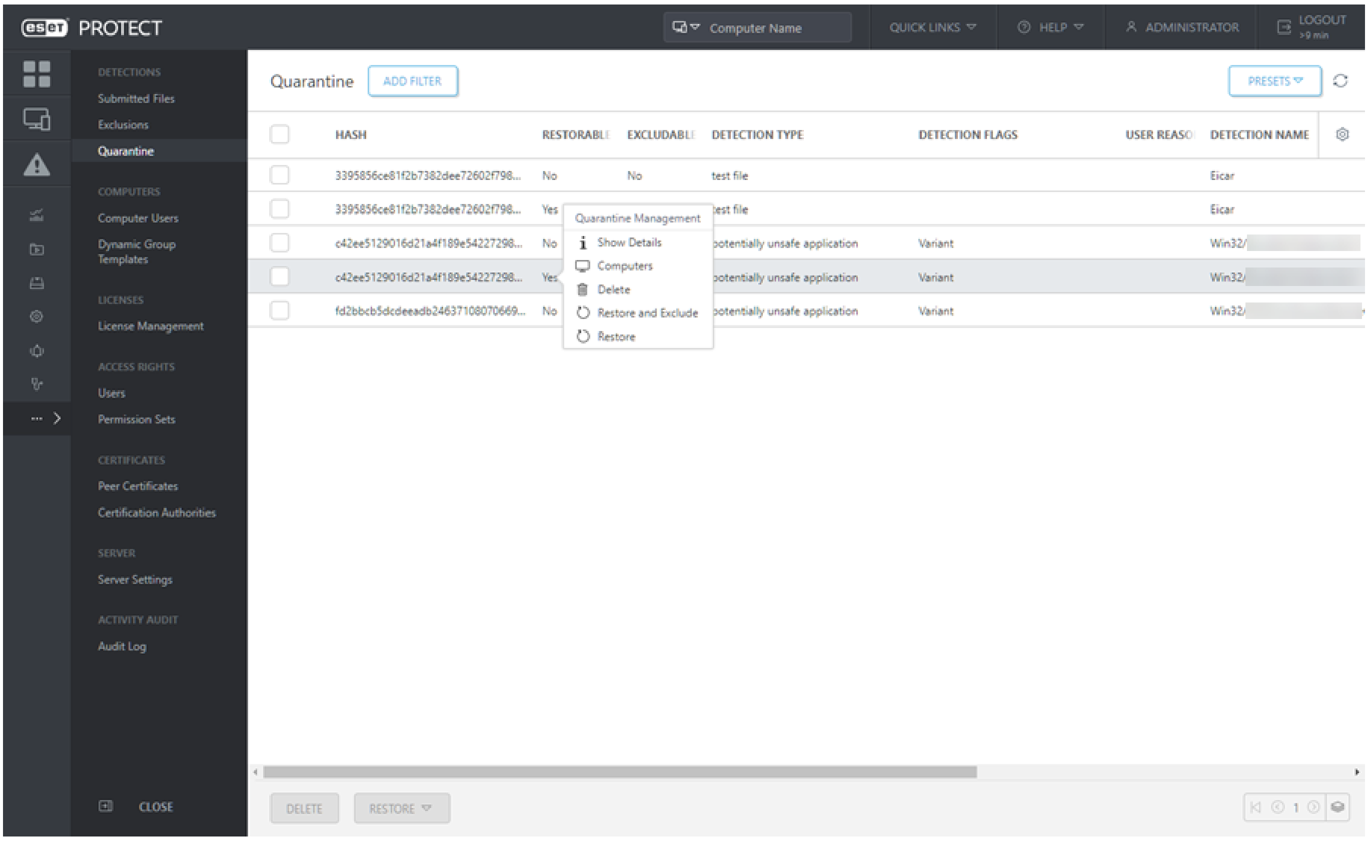
Products
Manage remotely large variety of security applications for different platforms.
- ✓ The repository is set correctly
- ✓ Computers without any product installed: 0

Encryption
Check the number of devices using ESET Full Disk Encryption. Back up or restore recovery data and passwords of encrypted computers to facilitate their migration between ESET PROTECT instances. Decrypt devices with permanently lost recovery data and/or password to avoid loss of data.
- ✓ Computers with ESET Full Disk Encryption installed: 0
- ✓ Computers encrypted: 0
- ✓ Computers with missing recovery data: 0
- ✓ Computers with a missing recovery password: 0

Invalid Objects
Tasks & notifications execution is dependent on internal & external parameters (like computers, groups, installers from repository etc.). If objects are no longer accessible tasks & notifications will not work.
- ✓ Client tasks containing inaccessible objects: 0
- ✓ Server tasks containing inaccessible objects: 0
- ✓ Enabled notifications containing inaccessible objects: 0
- ✓ Installers containing inaccessible objects: 0

Quarantine

The Quarantine section is in the Web Console under ⋯ **More** > **Quarantine**. This section shows all files quarantined on client devices.



	HASH	RESTORABLE	EXCLUDABLE	DETECTION TYPE	DETECTION FLAGS	USER REASO	DETECTION NAME
☐	3395856ce81f2b7382dee72602f798...	No	No	test file			Eicar
☐	3395856ce81f2b7382dee72602f798...	Yes		est file			Eicar
☐	c42ee5129016d21a4f189e54227298...	No		otentially unsafe application	Variant		Win32/[redacted]
☐	c42ee5129016d21a4f189e54227298...	Yes		otentially unsafe application	Variant		Win32/[redacted]
☐	fd2bbcb5dcdeeadb24637108070669...	No		otentially unsafe application	Variant		Win32/[redacted]

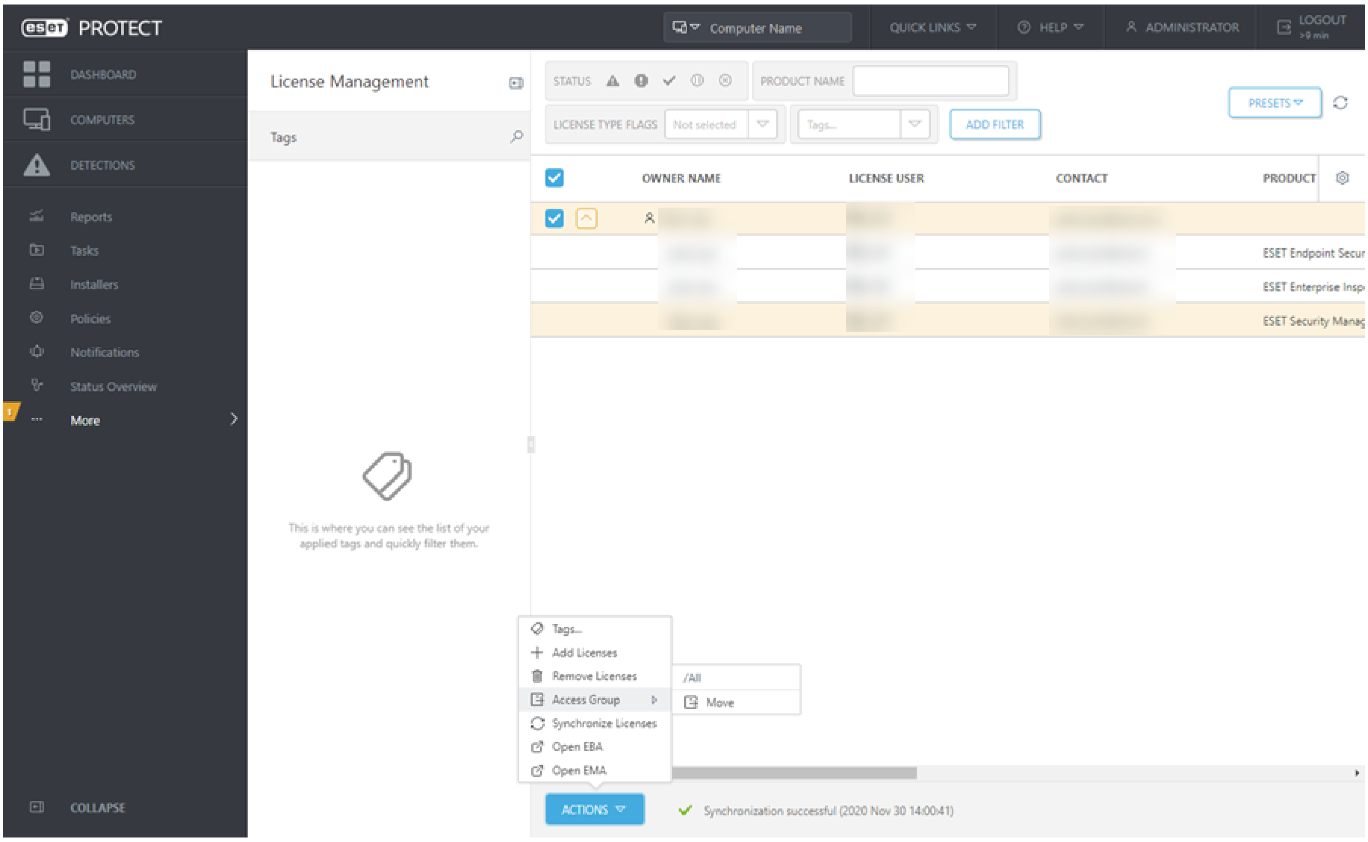
You should quarantine files if you cannot clean them, if it is not safe or advisable to delete them, or an ESET product falsely detects them.

> Not all detections found on client devices are moved to quarantine. Detections that are not quarantined include:
> - Detections that cannot be deleted
> - Detections that are suspicious based on their behavior, but are not identified as malware, for example, PUAs

See also the ESET Knowledgebase article about quarantine management.

License management

Select ⋯ **More** > **License Management** to manage your licenses.



This is where you can see the list of your applied tags and quickly filter them.

Synchronization successful (2020 Nov 30 14:00:41)

To add a new license to ESET PROTECT:

1.Click ··· **More** > **License Management** and click **Actions** > **Add Licenses**.

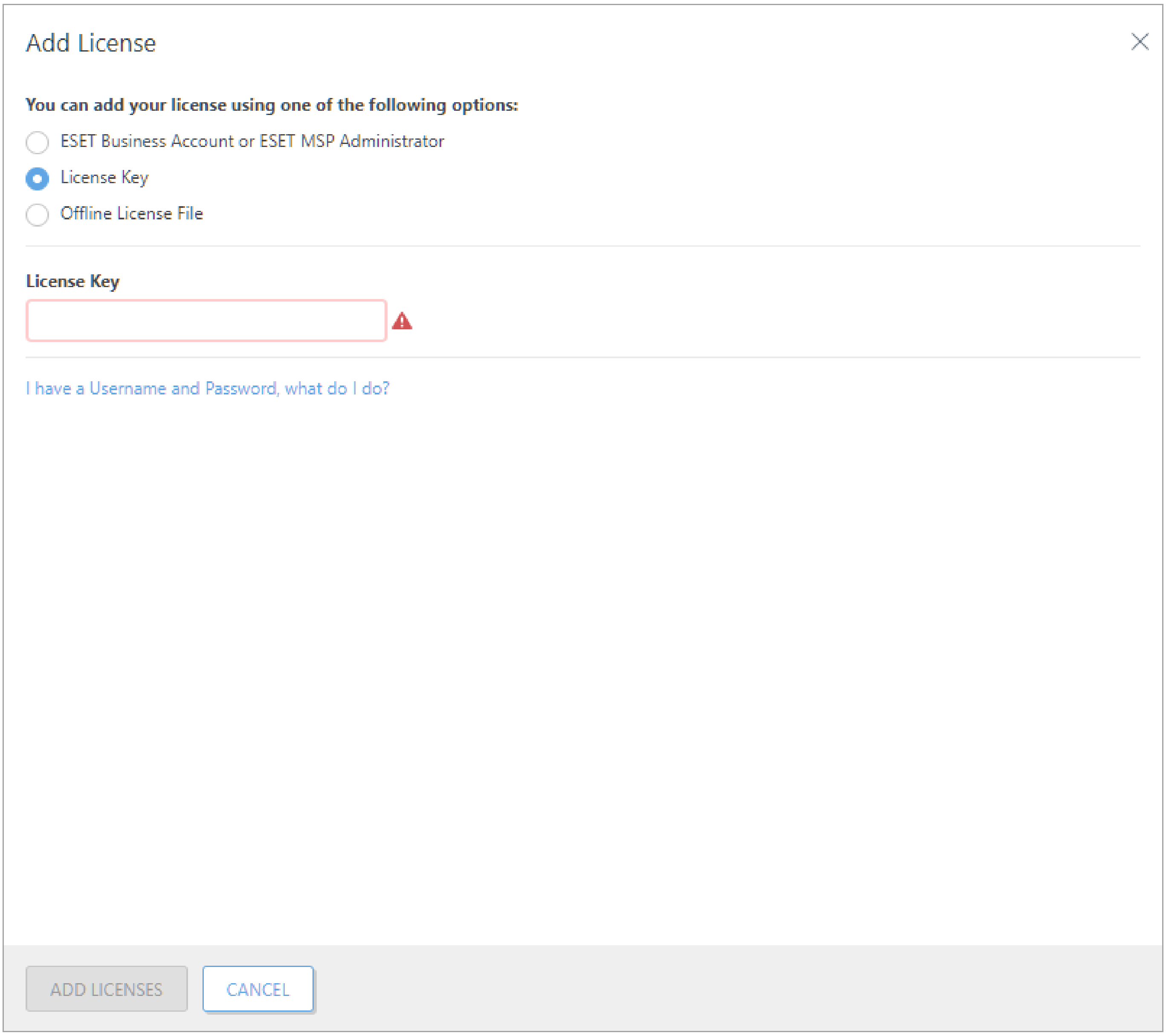
2.Select the method you want to use to add your new license(s):

a.**ESET Business Account or ESET MSP Administrator** - Synchronize the licenses from your ESET Business Account or ESET MSP Administrator account with the ESET PROTECT Web Console. You can import the complete structure of your ESET Business Account, including the distribution of license seats among the sites.

b.**License Key** - Type or copy/paste the license key you received when you purchased your ESET security solution in the **License Key** field.

c.**Offline License File**.

3.Click **Add licenses**.



Add License

You can add your license using one of the following options:

○ ESET Business Account or ESET MSP Administrator

● License Key

○ Offline License File

License Key

I have a Username and Password, what do I do?

ESET PROTECT supports the management of subscription licenses. You can add a license using ESET Business Account, ESET MSP Administrator, or a license key. You can verify your subscription's validity under **License Management** in the **Validity** column or by clicking **Computers** > Show Details.

Users and permission sets

ESET PROTECT security model

These are key terms used in the security model:

Term	Explanation
Home group	The home group is where all objects (devices, tasks, templates, and so on) a user creates are automatically stored. Each user must only have one home group.
Object	Each object (computer, task, policy, report, or notification) is in a static group. Access to objects is by groups, not users (providing access by group makes it easy to accommodate multiple users, for example, if one user is on holiday).

Term	Explanation
Access group	An access group is a static group that enables users to filter the object location based on access rights.
Administrator	An administrator is a user with the home group **All** and a full permission set over the group.
Access right	The right to access an object or to execute a task is assigned with a permission set.
Permission set	A permission set represents the permissions for users who access the ESET PROTECT Web Console. A permission set defines what a user can see or do in the ESET PROTECT Web Console. A user can be assigned multiple permission sets. Permission sets are applied only to objects in defined static groups.
Functionality	Functionality is one type of object or action. Typically, functionality gets these values: **Read**, **Write**, or **Use**. The combination of functionality applied to an access group is called a permission set.

For more detailed information, see Access Rights in the ESET PROTECT Administration Guide.

Create a new ESET PROTECT Web Console user

A fresh ESET PROTECT setup initially has a default **administrator** (a user with the home group **All** and access to everything) as the only user.

> ESET does not recommend using the default administrator user account. You should create another administrator account. You can also create additional users with narrower access rights based on your desired competencies.

Certificates

Certificates

Certificates are an essential part of ESET PROTECT. They serve for secure communication between ESET PROTECT components and the ESET PROTECT server and to establish a secure connection of the ESET PROTECT Web Console. You can manage ESET PROTECT certificates in ⋯ **More** > **Peer Certificates**.

> You can use certificates that are automatically generated during ESET PROTECT installation.

Certification authorities

A certification authority legitimizes certificates distributed from your network. In an enterprise setting, a public key serves for an automatic association of client software with the ESET PROTECT server to enable the remote installation of ESET products. You can manage ESET PROTECT certification authorities in ⋯ **More** > **Certification Authorities**.

> All peer certifications must be valid and signed by the same certification authority to ensure that all components can communicate correctly.

For more information about certificates and the certification authority, read the ESET Knowledgebase article or Online Help.

Help and support

ESET is constantly working to update and improve ESET PROTECT and ESET endpoint products.

- The ESET Knowledgebase is a searchable repository of support articles designed to help you resolve issues and answer questions.
- The ESET user Forum is monitored by ESET staff and allows ESET users to share issues they are having and find solutions.
- The ESET Knowledgebase video channel contains video walkthroughs of common procedures for ESET products.
- Visit ESET Support News and Customer Advisories for the latest announcements about ESET product features and upgrades.
- You can open a case with ESET Customer Care at any time if you are not able to resolve an issue or find the answer to your question.

You can also refer to the ESET PROTECT Installation guide (including upgrade, migration and troubleshooting), Administration guide (ESET PROTECT management with ESET PROTECT Web Console) and Virtual Appliance guide (ESET PROTECT in a hypervisor) for more detailed information.

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