

ESET Inspect On-Prem

Installation, Upgrade and Migration Guide

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

Copyright ©2024 by ESET, spol. s r.o.

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

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

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

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

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

REV. 4/18/2024

1 ESET Inspect On-Prem	1
2 Changelog	2
3 System Requirements	2
3.1 Hardware Requirements	2
3.1 Reduction of the database size	4
3.2 Software Requirements	5
3.2 Operating Systems	5
3.2 Windows	5
3.2 macOS	5
3.2 Linux	6
3.2 Database	6
3.2 MySQL Installation on Windows	7
3.2 MySQL Dedicated Partition	9
3.2 MySQL 5 on Linux System	9
3.2 MySQL 8 on Linux System	12
3.2 Microsoft SQL Server Installation	15
3.2 Supported Web Browsers and ESET Products	17
3.3 The ESET PROTECT On-Prem Permission Settings	19
4 ESET Inspect Server Installation	22
4.1 GUI - Mode Installation	23
4.1 Get the certificate from ESET PROTECT On-Prem	25
4.1 Import the server certificate from file	27
4.1 Get the ESET Inspect Web Console certificate from ESET PROTECT On-Prem	29
4.1 Import ESET Inspect Web Console certificate from file	29
4.1 Get the ESET Inspect Connector-side certificate from ESET PROTECT On-Prem	30
4.1 Import ESET Inspect Connector-side certificate from file	31
4.1 Web browser HTTPS/SSL certificate list	31
4.1 The type of PRODUCECTNAME user	32
4.1 Rules Sets	32
4.1 Data Collection	33
4.2 ESET PROTECT On-Prem Deployment	35
4.3 Troubleshooting the installation	37
4.4 ESET Inspect Server Migration	38
4.4 Clean installation with the same IP address	38
4.4 Clean installation with a different IP address	38
4.5 ESET Inspect Database Migration	39
4.5 The migration process for MySQL Server	39
4.5 The migration process for Microsoft SQL Server	40
4.6 Server upgrade through ESET PROTECT On-Prem	41
5 ESET Inspect Connector Installation	41
5.1 Windows	42
5.1 ESET Inspect All-in-one Installer	43
5.1 Windows GUI - Mode Installation	43
5.1 Installation from a windows command line	45
5.1 Troubleshooting the installation	46
5.1 GUI Repair/Change	46
5.1 Upgrade through ESET PROTECT On-Prem	47
5.1 GUI Upgrade from earlier version	47
5.2 macOS	48
5.2 macOS GUI - Mode Installation	48

5.2 Installation from a macOS terminal	50
5.3 Linux	51
5.3 Linux Terminal Installation	52
5.4 ESET PROTECT On-Prem Windows/macOS/Linux Deployment	53
5.5 ESET Inspect Connector uninstallation	55
6 Telemetry	56
7 End User License Agreement	57
8 Privacy Policy	63

ESET Inspect On-Prem

ESET Inspect On-Prem is an essential component to help ensure the highest level of enterprise security. While standard ESET Endpoint Security provides strong protection, ESET Inspect On-Prem takes your environment's security to a new dimension.

A security tool is needed to help security professionals protect their sensitive data and detect and investigate security incidents, advanced threats, and targeted attacks or breaches on endpoint devices.

ESET Inspect On-Prem is a tool that offers the peace of mind of continuous protection and security monitoring in a powerful and easy-to-use solution.

ESET Inspect On-Prem collects data in real time on endpoint devices. The data is matched against a set of rules to detect suspicious activities automatically. Then the aggregated data is processed, and the information is prioritized and correlated in a searchable form.

Aggregated data allows a security professional to search for unusual and suspicious activities more efficiently and enables an accurate incident response, management, and reporting.

ESET Inspect On-Prem is a solution that includes the following three components:

- **ESET Inspect Connector** is installed on endpoint devices that are monitored by ESET Inspect On-Prem and collects the data for the ESET Inspect On-Prem, removes malicious components, and blocks the execution of these components
- **ESET Inspect Server** continually aggregates and stores the collected data and displays it in the ESET Inspect Web Console
- **ESET Inspect Web Console** is the user interface for ESET Inspect On-Prem built as an HTML5 web application

The following ESET business security solutions have been renamed:		
Old name:	New name:	Renamed in version:
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	2.0

Key features

ESET Inspect On-Prem is an essential component to help ensure the highest level of enterprise security. As a critical tool for risk assessment and detection, ESET Inspect On-Prem is a comprehensive Endpoint Detection and Response (EDR) system that includes the following features:

- **Incident detection**—Monitor the [Detections](#) section to reveal security incidents, Advanced Persistent Threats (APT), and targeted attacks.
- **Incident management and response**—Use a built-in set of rules or create your own rules to respond to detected incidents. The rules guide is available in the help section of the ESET Inspect Web Console.
- **Data collection**—Determine when an executable was launched for the first time and by whom, and check the dwell time and attacked devices.
- **Indicators of Compromise (IOC) detection.**
- **Anomaly detection**—See what is being executed in your company network and reveal unexpected actions.
- **Behavior detection**—See what actions were carried out by an [Executable](#): modified files, changing registry entries, connections made. Assess whether the executed processes are safe or suspicious by

looking at LiveGrid® reputation markers.

- **Policy violations**—Block malicious executables from being executed on any computer in your company network.
- **Email notifications**—Cooperation of ESET Inspect On-Prem with ESET PROTECT On-Prem results in beneficial security email notifications.

Changelog

System Requirements

The system requirements for ESET Inspect On-Prem are specified for [Hardware](#) and [Software Requirements](#).

Hardware Requirements



Hardware requirements depend on the number of events. The event from the ESET Inspect On-Prem side of view includes File system events (read file, write file, etc.), TCP events, Registry events, HTTP events, DNS events, etc.

There are two ways to get the number of events.

Before installing the ESET Inspect Server:

1. Install the [ESET Inspect Connector](#) on at least three endpoints (ESET Inspect Connector is operable without ESET Inspect Server).
2. Activate the product with a valid ESET Inspect On-Prem license. The activation is done via ESET PROTECT On-Prem by creating a "Product activation" task. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.
3. Wait for at least a day.
4. Navigate to the folder where ESET Inspect Connector is installed (by default *C:\Program Files\ESET\Inspect Connector*) and run the command `EIConnector.exe --stats`.
5. From the output, use **Average Events Per Day**.

After the ESET Inspect Server is already installed and working:

1. Go to [Dashboard](#) > **Events load** tab and check the highest values of events received per 24h in the **Events processed and stored per computer** chart.

To calculate the estimated CPU, RAM, and disk space requirements for ESET Inspect Server and database on the same machine, use the following calculator:

☐ MySQL ☐ Microsoft SQL Server

Endpoints:

Events per 24h per endpoint:

Estimate

This environment requires ESET Inspect Server to be able to write at least events per second (EPS)

Minimum hardware configurations:

Estimated events written per second are shown in the brackets

The estimated number of CPU cores is based on tests using an Intel Xenon 2.7GHz but other server specific x64 CPUs, such as Intel Xeon and AMD Epyc, can be used after scaling the number of cores to compensate for potentially lower clock rates.

Estimated database sizes:

The values in the table below are based on the assumption that the endpoint does not have more than a hundred thousand events generated per day, and the default data retention is 31 days. If the number of events in your environment exceeds a hundred thousand, you should proportionally scale the number from the table.

	Minimum requirements					
	Microsoft SQL Server			MySQL		
Number of Endpoints	500	1000	5000	500	1000	5000
Memory	4 GB	4 GB	12 GB	4 GB	4 GB	12 GB
Disk space	566 GB	1.24 TB	6.2 TB	566 GB	1.1 TB	5.6 TB
Disk IOPS	1500	1500	3000	1000	2000	3000
Number of CPU cores	2	2	10	2	2	8



The current scalability limit is approximately 30 000 endpoints per ESET Inspect Server when considering the average event rate from global telemetry. The limit can vary based on the exact conditions and environment specifics; therefore, use the configuration calculator for accurate hardware/resource specifications.



The estimated database size does not consider various logs (MySQL general query log, MySQL binary log, or SQL Server transaction log). If you do not need to store them for your purposes, consider disabling them or clearing the logs regularly to reduce their disk space.

Disk Space Consumption Reduction

We recommend these [steps](#) for disk space consumption reduction.

This can significantly save the disk space used by stored events.



If the Windows Server OS's space goes under 10 percent of the partition capacity (C:\), ESET Inspect On-Prem stops accepting data from endpoints.

The disk IOPS

To get the information regarding the IOPS that your disk can provide, use the tool described below:

66% of IOPS triggered by ESET Inspect On-Prem are write-related operations, and the block size is 32KB.

IOPS achieved by the customer's hardware can be measured using the following command line: `diskspd -b32K`

```
-d60 -o4 -t8 -h -r -w65 -L -Z1G -c20G C:\iotest.dat > C:\DiskSpeedResults.txt.
```

diskspd is a Microsoft tool that can be downloaded from:

<https://learn.microsoft.com/azure-stack/hci/manage/diskspd-overview>

The CPU and RAM impact reduction

To reduce the impact on CPU and RAM, you can use two approaches:

1. Navigate to **Dashboard > Server Status > Event Packet Queue Length**. If the chart shows that most of the time, 500, then consider upgrading your hardware or lowering the server load by using the steps described in the [Disk Space Consumption Reduction](#).
2. You can change the interval of sending the events from connectors to the server. By default, the interval is every 7 minutes. You can change this in ESET PROTECT On-Prem by going into **Policies > New Policy > click Settings** and select **ESET Inspect Connector** from drop-down menu > **Interval of sending events to the server (minutes)**. The available interval is 5–1440 minutes.

To support a specific number of endpoints, ensure that the [ephemeral port pool](#) size is twice as big as the endpoint's count.

Command to check the current size of the ephemeral port pool:

```
netsh int ipv4 show dynamicport tcp
```



Command to set ephemeral port pool size:

```
netsh int ipv4 set dynamicport tcp start=<number> num=<size>
```

For example: To set the ephemeral port pool to 60k, type the following:

```
netsh int ipv4 set dynamicport tcp start=5536 num=60000
```

NOTE: Maximal port number can be 65536. It is recommended to set starting port at 1500.

Reduction of the database size

The ways to reduce disk space usage are:

1. Store the low-level data for the shortest possible time. The database size is proportional to the amount of low-level data stored in the database, so lower the amount by keeping the low-level data as briefly as possible. This can be configured in the **More > Settings > Database Retention** pane.



A low-level event is something a process does. So, write a file, do a DNS lookup, create a registry entry, etc. These can be seen in the Events view.

2. Store less low-level data. Instead of storing all data, keep only the most important data or data related directly to detections. This will not lower the protection because everything is still being analyzed to detect suspicious activity, even if not everything is stored. The amount of stored data can be changed in the **More > Settings > Data collection** pane. But some ESET Inspect On-Prem features don't work or are limited when not everything is stored. For more information about these limitations, [follow](#).

3. Use [Event Filters](#) to selectively not store low-level events from some executables or computers. **Dashboard > Events Load** helps to find executables and computers that report most low-level events and where filters should be applied.

4. Check database settings that can cause increased disk usage:

a. For MySQL, check binary log usage. For more information, [follow](#).

b. For Microsoft SQL Server, check recovery models. For more information, [follow](#).

These settings are commonly used for backups, so if needed, ensure they are configured and used correctly.

Software Requirements

The following sections describe ESET Inspect On-Prem software requirements like the support of [Operating Systems](#), [Database](#) or [Supported Web Browsers and ESET Products](#).

ESET PROTECT On-Prem 10.0 or later is required for ESET Inspect On-Prem to monitor computers. See [ESET PROTECT On-Prem Account Settings](#) for Administrator and User account settings. For instructions to install ESET PROTECT On-Prem, see [ESET PROTECT On-Prem Installation Guide](#).

The ESET Inspect Server requires a 64-bit version of Visual C++ redistributable to be installed before the server is installed. The redistributable file can be downloaded from this [link](#).

Operating Systems

The following sections describe ESET Inspect On-Prem support for [Windows](#), [macOS](#) and [Linux](#) operating system versions.

Windows

The following table displays the supported Windows operating systems for each ESET Inspect On-Prem component:

Operating System	ESET Inspect Server	ESET Inspect Connector
Windows 10, version 21H1 32-bit / 64-bit		✓
Windows 10, version 21H2 32-bit / 64-bit		✓
Windows 10, version 22H2 32-bit / 64-bit		✓
Windows 11, version 21H2 32-bit / 64-bit		✓
Windows 11, version 22H2 32-bit / 64-bit		✓
Windows 11, version 23H2 32-bit / 64-bit		✓
Windows Server 2012 64-bit	✓	✓
Windows Server 2012 R2 64-bit	✓	✓
Windows Server 2016 64-bit	✓	✓
Windows Server 2019 64-bit	✓	✓
Windows Server 2022 64-bit	✓	✓

i We are supporting Azure Virtual Desktop / Microsoft Windows 10 [multi-session](#) mode.

macOS

The following table displays the supported macOS operating systems for ESET Inspect Connector component:

Operating system	Connector
macOS 10.15 (Catalina)	✓

Operating system	Connector
macOS 11 (Big Sur)	✓
macOS 12 (Monterey)	✓
macOS 13 (Ventura)	✓
macOS 14 (Sonoma)	✓

Linux

The following table displays the supported Linux operating systems for ESET Inspect Connector component:

Operating system	Endpoint Antivirus for Linux	Server Security for Linux
RedHat Enterprise Linux (RHEL) 7		✓
RedHat Enterprise Linux (RHEL) 8	✓	✓
RedHat Enterprise Linux (RHEL) 9	✓	✓
Centos 7		✓
Ubuntu 18.04	✓	✓
Ubuntu 20.04	✓	✓
Ubuntu 22.04	✓	✓
Debian 10		✓
Debian 11		✓
Debian 12		✓
SUSE Linux Enterprise Server (SLES) 15		✓
Oracle Linux 8		✓
Amazon Linux 2		✓
Alma Linux 8		✓
Alma Linux 9		✓
Rocky Linux 8		✓
Rocky Linux 9		✓
Linux Mint 20	✓	
Linux Mint 21	✓	

i For Ubuntu 22.04 libfuse2 library must be installed first.

Database

ESET Inspect On-Prem supports two database servers: Microsoft SQL Server and MySQL.

Supported database server	Supported database versions	Supported database connectors
Microsoft SQL Server	2017, 2019, 2022	ODBC Driver for SQL Server 11, 13, 17
MySQL	5.7.44 or later, 8.0.35 or later, 8.1 or later	-

For installation instructions of MySQL Server, see [MySQL Installation on Windows](#) or [MySQL 5 on Linux System](#) or [MySQL 8 on Linux System](#).

For installation instructions of Microsoft SQL Server, [follow](#).

! Microsoft SQL Server database mirroring is not supported. Its use may cause further upgrades of ESET Inspect Server to fail.

i Clusters are not supported.

MySQL Installation on Windows

Prerequisites

- Download the MySQL server installer for Windows: <https://dev.mysql.com/downloads/windows/installer/>.
- Install Microsoft .NET Framework version 4 if required. Depending on the OS version.

Installation and configuration

1. Run the downloaded installer file to start the installation. Select the **Server-only** version in the **Choosing a Setup Type** screen and click **Next**.
2. In the **Type and Networking** screen, select **Config Type** (we recommend using a **Dedicated Computer** type for the SQL server), type in your preferred **Port Number** (or use port 3306 by default), and click **Next**.
3. We recommend using the **Authentication Method** screen's default (RECOMMENDED) option.
4. In the **Accounts and Roles** screen, set the **MySQL Root Password** and click **Add User** to create another MySQL user account secured with a password and with a DBA role assigned.



Remember the username and password you configured for a new user with the DB admin role, as it is used during the [ESET Inspect Server installation](#).

5. We recommend selecting **Configure MySQL Server as Windows Service** in the **Windows Service** screen and **Starting the MySQL Server at System Startup**. Otherwise, you will have to start the server manually each time (for example, using the `net start mysql` command from an administrative command prompt).
6. We recommend to using the default option **Yes, grant full access** in the **Server File Permissions** screen.
7. In the **Apply Configuration** screen, click **Execute**. If the configuration steps are completed successfully, click **Finish**.
8. In the subsequent screen, click **Next** and then **Finish**.



For editing the **my.ini** file, ensure it is saved in ANSI, not in UTF-8 format. We recommend using Notepad++, which will not change the file format after saving.

You must modify the **my.ini** file in *C:\ProgramData\MySQL\MySQL Server X.X.* for further ESET Inspect Server. Before editing, backup the ini file.

Find the following variables and change their values. If a variable does not exist, add it at the end of **my.ini** file:

Increase the value of `open_files_limit` to at least 30000.

Change the value of `innodb_flush_log_at_trx_commit` to 0.

Set `innodb_buffer_pool_size` to 80% percent of the RAM. For instance, if the server has 16GB of RAM, it should be set in the following way: `innodb_buffer_pool_size=12G`. The minimum value is 1G.

Set `innodb_log_file_size` to 50% of the value of setting `innodb_buffer_pool_size`. Valid for version 5.

Set `innodb_redo_log_capacity` to the value of setting `innodb_buffer_pool_size`. Valid for version 8.

Set `event_scheduler=ON`. Valid for version 5.

Set `local_infile=1`.

Add `disable-log-bin`.

Set `wait_timeout=900`.

Set `max_connections=300`.

Set `slow-query-log=0`.

After saving these changes, restart the MySQL service.

Because ESET Inspect On-Prem executes many SQL statements, [MySQL's general](#) and [binary](#) log can be huge. Consider disabling the general and binary logs if they are not used. Consider also limiting their size or time of logging using MySQL configuration parameters.

Moving the database to separate partition/machine

MySQL is the most crucial ESET Inspect Server part and can consume whole disk space. Due to operating system stability, we recommend moving the MySQL data and a temporary folder to the [dedicated partition](#) or a [separate server machine](#).

When calculating the required disk space, we are tracking three folders:

- Database folder—The folder where MySQL or SQL Server stores ESET Inspect Database
- Temporary database—The folder where MySQL or SQL Server stores temporary tables
- The ESET Inspect Server data folder—*C:\ProgramData\ESET\Inspect Server\Server* folder

If the database is installed on the same machine as the ESET Inspect Server, then ESET Inspect On-Prem stops accepting new events when:

- There is less than 3% of free space on the disk with the database folder
- There is less than 3% of free space on the disk with the temporary database folder
- There is less than 5% of free space on the disk with the ESET Inspect Server data folder

If the `<%EIS%>` data folder and temporary database folder are on the same disk, ESET Inspect On-Prem stops accepting new events if there is less than 10% free space on this disk.

If the database is located on the same machine as ESET Inspect On-Prem, there must be at least 10% free disk space where the temporary folder is for the [Purge](#) to work. Any problems with the database purge are displayed as red markers on the [Events processed](#) chart on the [Events Load](#) Dashboard's tab.

MySQL Dedicated Partition

1. Stop MySQL Service.

2. Move or copy the Data folder onto the dedicated partition, for instance, *D:*.



For editing the **my.ini** file, ensure it is saved in ANSI, not in UTF-8 format. We recommend using Notepad++, which will not change the file format after saving.

3. Edit **my.ini** file located by default in *C:\ProgramData\MySQL\MySQL Server X.X.* and search for the '# Path to the database root' string and change the path to the location of the new Data folder, for example, *D:\Data*. The folder has to be created before altering the my.ini file.

4. The Data folder has to be accessible by the Network Service. To add required permissions, follow these steps:

a. Go to **Start > Administrative Tools > Computer Management > System Tools > Local Users and Groups > Groups**.

b. Double-click **Users**.

c. Click **Add**.

d. Click **Locations**, select your computer node and click **OK**.

e. Type 'Network Service' into the 'Enter the object names' or click **Advanced**, then **Find Now** and select it from the **Search Results**.

5. Edit **my.ini** file located by default in *C:\ProgramData\MySQL\MySQL Server X.X.* Under [mysqld] search for "tmpdir". If missing, add the following line `tmpdir = D:/mysqltemp` where the "mysqltemp" is a custom folder. The folder has to be created before altering the my.ini file.

6. Start MySQL Service.

MySQL 5 on Linux System

Open the Terminal and run the following commands:

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

```
sudo apt-get install mysql-server-5.7
```

To install MySQL Workbench (optional), which is the GUI for the database:

```
sudo apt install mysql-workbench
```

Database setup

You need to set the database user for localhost and external connections and push the following SQL commands or via the cmd line.

Cmd line (not Workbench):

```
sudo mysql -u root -p
create user 'root'@'%' IDENTIFIED BY 'root';
ALTER USER 'root'@'%' IDENTIFIED WITH mysql_native_password BY 'admin.1';
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'admin.1';
grant all privileges on *.* to 'root'@'%' with grant option;
```

From the **mysql.user** menu, select host %, and user root.

After the user is added and defined, you can set up the MySQL database.

```
mysql_secure_installation
Validate password component [Y/n] n
Change the root password? [Y/n] n
Remove anonymous users? [Y/n] y
Disallow root login remotely? [Y/n] n
Remove test database and access to it? [Y/n] y
Reload privilege tables now? [Y/n] y
```

We recommend changing the password, as "admin.1" is the default. This password is required during ESET Inspect Server Installation. Through the terminal, follow the [tutorial](#).

Through the Workbench, click:

- **Database > Connect to Database...** select database > **OK**
- Then **Server > Users and Privileges** > Select **root%**—set the password and confirm it

Open the Terminal and execute the following command to copy *mysql.service* file:

```
sudo cp /lib/systemd/system/mysql.service /etc/systemd/system/
```

Open the */etc/systemd/system/mysql.service* in texteditor (or nano, pico, vi ...) and add following lines:

```
sudo nano /etc/systemd/system/mysql.service
```

```
LimitNOFILE=30000
```

```
LimitMEMLOCK=30000
```

Save the file and reload the system configuration by the following command:

```
sudo systemctl daemon-reload
```

Now you need to modify */etc/mysql/mysql.conf.d/mysqld.cnf* file (where are the db params).

Open the file in texteditor or nano, pico, vi ... and add the following lines under section [mysqld]:

```
sudo /etc/mysql/mysql.conf.d/mysqld.cnf
```

```
bind-address = IP_OF_THIS_MACHINE, BUT NO 127.0.0.1
```

```
thread_stack = 256K
```

**bind-address* – default value is 127.0.0.1. You must set this address to the machine's IP where MySQL is running. ESET Inspect On-Prem Installation cannot connect to MySQL in case of incorrect IP.

Insert the following parameters to the part InnoDB

```
innodb_buffer_pool_size=4G
```

```
innodb_flush_log_at_trx_commit=0
```

```
innodb_log_file_size=2G
```

**innodb_buffer_pool_size*—set to 80% of the RAM size of MySQL machine

**innodb_log_file_size* —set to 40% - 60% of the *innodb_buffer_pool_size* value

Add to the end these lines

```
event_scheduler = ON
```

```
wait_timeout=900
```

```
max_connections=300
```

Restart MySQL to load the new parameters:

```
sudo service mysql restart
```

Verify the status of the MySQL Service

Open the terminal, and type in the command.

```
systemctl status mysql.service
```

MySQL Service runs when the reported state is: active (running).

Sources

MySQL Installation	https://www.cyberciti.biz/faq/howto-install-mysql-on-ubuntu-linux-16-04/
Warning: World-writable config file '/etc/mysql/my.cnf' is ignored	https://stackoverflow.com/questions/32133353/unable-to-connect-to-mysql-database-in-ubuntu
Open_files_limit	https://support.plesk.com/hc/en-us/articles/213393029-MySQL-values-open-files-limit-and-max-connections-are-not-applied
MySQL command line commands	https://dev.mysql.com/doc/refman/5.5/en/getting-information.html

MySQL 8 on Linux System

Open the Terminal and run the following commands:

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

```
sudo apt-get install mysql-server
```

To install MySQL Workbench (optional), which is the GUI for the database:

```
sudo apt install mysql-workbench
```

Database setup

You need to set the database user for localhost and external connections and push the following SQL commands or via the cmd line.

Cmd line (not Workbench):

```
sudo mysql -u root -p
```

```
create user 'root'@'%' IDENTIFIED BY 'root';
```

```
ALTER USER 'root'@'%' IDENTIFIED WITH mysql_native_password BY 'admin.1';
```



```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'admin.1';  
grant all privileges on *.* to 'root'@'%' with grant option;
```

From the **mysql.user** menu, select host %, and user root.

After the user is added and defined, you can set up the MySQL database.

```
mysql_secure_installation  
Validate password component [Y/n] n  
Change the root password? [Y/n] n  
Remove anonymous users? [Y/n] y  
Disallow root login remotely? [Y/n] n  
Remove test database and access to it? [Y/n] y  
Reload privilege tables now? [Y/n] y
```

We recommend changing the password, as "admin.1" is the default. This password is required during ESET Inspect Server Installation. Through the terminal, follow the [tutorial](#).

Through the Workbench, click:

- **Database > Connect to Database...** select database > **OK**
- Then **Server > Users and Privileges > Select root%**—set the password and confirm it

Open the Terminal and execute the following command to copy *mysql.service* file:

```
sudo cp /lib/systemd/system/mysql.service /etc/systemd/system/
```

Open the */etc/systemd/system/mysql.service* in texteditor (or nano, pico, vi ...) and add following lines:

```
sudo nano /etc/systemd/system/mysql.service  
LimitNOFILE=30000  
LimitMEMLOCK=30000
```

Save the file and reload the system configuration by the following command:

```
sudo systemctl daemon-reload
```

Now you need to modify */etc/mysql/mysql.conf.d/mysqld.cnf* file (where are the db params).

Open the *mysqld.cnf* file in texteditor or nano, pico, vi ... and add the following lines under section [mysqld]:

```
sudo nano /etc/mysql/mysql.conf.d/mysqld.cnf
```

```
bind-address = xxx.xxx.xxx.xxx
```

```
innodb_flush_log_at_trx_commit=0
```

```
innodb_buffer_pool_size=2G
```

```
innodb_redo_log_capacity=2G
```

```
thread_stack=256K
```

```
disable-log-bin
```

```
local_infile = 1
```

```
wait_timeout=900
```

```
max_connections=300
```

***bind-address**—default value is 127.0.0.1. Set this address to the machine's IP where MySQL is running. If the incorrect IP address is used, ESET Inspect On-Prem Installation cannot connect to MySQL.

***innodb_buffer_pool_size**—set to 80% of the RAM size of MySQL machine

***innodb_log_file_size**—set to 40% - 60% of the **innodb_buffer_pool_size** value

Restart MySQL to load the new parameters:

```
sudo service mysql restart
```

Verify the status of the MySQL Service

Open the terminal, and type in the command.

```
systemctl status mysql.service
```

MySQL Service is running when the reported state is: active (running).

Sources

MySQL Installation	https://www.cyberciti.biz/faq/howto-install-mysql-on-ubuntu-linux-16-04/
Warning: World-writable config file '/etc/mysql/my.cnf' is ignored	https://stackoverflow.com/questions/32133353/unable-to-connect-to-mysql-database-in-ubuntu
Open_files_limit	https://support.plesk.com/hc/en-us/articles/213393029-MySQL-values-open-files-limit-and-max-connections-are-not-applied
MySQL command line commands	https://dev.mysql.com/doc/refman/5.5/en/getting-information.html

Microsoft SQL Server Installation



We recommend using the Microsoft SQL Server Enterprise/Standard edition but remember that it requires a license. Microsoft SQL Server Express version is not supported by ESET Inspect On-Prem.

Follow these steps (MSSQL 2017):

1. After starting the MSSQL installer choose the **Custom** installation process.
2. You can keep the default installation path or choose a different one. Click **Install**.
3. After downloading the installation files, the **SQL Server Installation Center** appears. If not, start it up.
4. Choose the **Installation** menu from the left-side panel.
5. Choose a **New SQL Server stand-alone installation or add features to an existing installation** to start the installation process.
6. Accept the **License terms** and click **Next**.
7. Select the check box to **Use Microsoft Update to check for updates**. Open <https://localhost> in a web browser to log into ESET Inspect On-Prem. If you want to access ESET Inspect On-Prem from a different device, write the IP Address or hostname of the ESET Inspect Server in a browser..
8. In the **Install Rules** window, click **Next**.
9. Select the **Database engine Services** and **SQL Client connectivity SDK**(not valid for 2022) check box in the **Feature Selection** window. Click **Next**.
10. You can keep the default value in the **Instance Configuration** window and click **Next**.
11. In the **Server Configuration** window, change the **Startup Type** for **SQL Server Agent** to **Automatic** and click **Next**.
12. In the **Database Engine Configuration** window, select the **Mixed Mode** option.
13. Type in and confirm the password for the default "sa" user (SQL Server system administrator). You can use this user during the ESET Inspect Server installation process or create a [custom user](#) with sufficient privileges.
14. Click **Add Current User** button.
15. Click **Next**.
16. Click **Install**.

Turn off/create firewall exception and allow TCP/IP communication for MSSQL to function ESET Inspect On-Prem with MSSQL fully. Otherwise, the ESET Inspect Server installation ends up with an error.

1. Open **SQL Server Configuration Manager**.
2. Click **SQL Server Network Configuration** in the left-side menu.

3. Click **Protocols for MSSQLSERVER**.

4. Ensure that the **TCP/IP** protocol is in status **Enabled** (it should be by default).

5. Click **SQL Server Services** from the left-side menu.

6. In the right-side menu, right-click the **SQL Server (MSSQLSERVER)** service, and from the context menu, select **Restart**.

7. In the right-side menu, right-click the **SQL Server Agent (MSSQLSERVER)** service, and from the context menu, select **Restart**.

8. Check the Windows Services that the SQL Server service is running. Otherwise, the ESET Inspect Server will not work.

Now is, the MSSQL Server ready for the ESET Inspect Server to be installed.

For safety purposes, we recommend using a different user with the necessary privileges:

1. Download [MSSQL Server Management Studio](#) and install it on the MSSQL Server machine.

2. Log into the server.

3. Server type: **Database Engine**. Select the server name used on that server, Authentication: **Windows Authentication**.

4. Click **Connect**.

5. Right-click the **Security** folder on the left-side menu. Choose **New** from the context menu > **Login**.

6. Type in the **Login name**. Choose **SQL Server Authentication**. Fill in the **Password** and confirm it.

7. Deselect **Enforce password expiration**.

8. In the left-side menu of the same window, click **User Mapping**. From the list of users mapped to this login, choose a **master**, and in the **Database role membership** list keep checked **public** role.

9. In the left-side menu of the same window, click the **Securables**. Click the **Search** button and select the third option, **The server**. Scroll down the **Permission for** list and check the **Grant** box for **View Server State**.

10. In the left-side menu, click **Server Roles**. From the server roles list, choose the **dbcreator** and leave the **public** checked.

11. Click **OK**.

Now you can proceed with the ESET Inspect Server installation with this new custom SQL user.



Required user privileges have changed since the 1.7 version. In case of upgrading ESET Inspect On-Prem to version 1.8 or later, set the user rights as described above and then upgrade ESET Inspect Server.

Moving the database to separate partition/machine

MySQL is the most crucial ESET Inspect Server part and can consume whole disk space. Due to operating system stability, we recommend moving the MySQL data and a temporary folder to the [dedicated partition](#) or a [separate server machine](#).

Follow these steps:

- 1.Run SQL Server Management Center.
- 2.In Object Explorer, right-click the name of the server.
- 3.In the context menu, click **properties**.
- 4.Select **Database Settings** from the left side menu.
- 5.In the **Database Default Location**, change the **Data** path.

When calculating the required disk space, we are tracking three folders:

- Database folder—The folder where MySQL or SQL Server stores ESET Inspect Database
- Temporary database—The folder where MySQL or SQL Server stores temporary tables
- The ESET Inspect Server data folder—*C:\ProgramData\ESET\Inspect Server\Server* folder

If the database is installed on the same machine as the ESET Inspect Server, then ESET Inspect On-Prem stops accepting new events when:

- There is less than 3% of free space on the disk with the database folder
- There is less than 3% of free space on the disk with the temporary database folder
- There is less than 5% of free space on the disk with the ESET Inspect Server data folder

If the <%EIS%> data folder and temporary database folder are on the same disk, ESET Inspect On-Prem stops accepting new events if there is less than 10% free space on this disk.

If the database is located on the same machine as ESET Inspect On-Prem, there must be at least 10% free disk space where the temporary folder is for the [Purge](#) to work. Any problems with the database purge are displayed as red markers on the [Events processed](#) chart on the [Events Load](#) Dashboard's tab.

Supported Web Browsers and ESET Products

- Google Chrome
- Mozilla Firefox
- Safari
- Edge (based on Chromium)




Use the latest version of browsers.

ESET Inspect Web Console

ESET Inspect Web Console is a [single-page application](#) that communicates with the ESET Inspect Server via REST calls.

 The minimum screen resolution supported by the Web Console is 1280x768.

Supported ESET Products



 ESET Inspect On-Prem is at the moment compatible with ESET PROTECT On-Prem, not ESET PROTECT.

- ESET Endpoint Security 11.0.2032 or later.
- ESET Endpoint Antivirus 11.0.2032 or later.
- ESET Endpoint Security for macOS 6.11.616.0 or later
- ESET Endpoint Antivirus for macOS 7.3.3600.0 or later
- ESET Endpoint Antivirus for Linux 10.2.2.0 or later
- ESET Mail Security for Microsoft Exchange Server 10.1.10012.0 or later
- ESET Mail Security for IBM Lotus Domino 10.0.14006.0 or later
- ESET Server Security for Microsoft Windows Server 10.0.12014 or later
- ESET Server Security for Linux 10.2.41.0 or later
- ESET Security for Microsoft Sharepoint Server 10.0.15004.0 or later
- ESET PROTECT On-Prem 10.1.28.0 or later

Because the ESET Inspect On-Prem can show some malware/scripts, ESET Endpoint Security / ESET Endpoint Antivirus can sometimes show ESET Inspect On-Prem as a threat. Follow these steps to prevent ESET Endpoint Security / ESET Endpoint Antivirus from blocking ESET Inspect On-Prem:

- In ESET Endpoint Security and ESET Endpoint Antivirus settings go to **Web and Email > Web access protection > Url address management > Address List > List of addresses excluded from content scan > Edit**
- If not present, add the Hostname/IP Address of the ESET Inspect Server and add /* at the end of the string. You can use the [ESET PROTECT On-Prem policy](#) to deploy such a setting to multiple ESET Endpoint Security / ESET Endpoint Antivirus.

When the ESET product version reaches the End of Life:

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

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

ESET Bridge

ESET Bridge is a new ESET software based on the open-source nginx software adjusted for the needs of ESET security solutions. You can use ESET Bridge as HTTP Proxy solution with ESET Inspect Server. The ESET Bridge default configuration supports the cloud ESET Inspect. You can [configure ESET Bridge](#) to support ESET Inspect On-Prem.

LiveGrid®

i Enable LiveGrid® in ESET Endpoint Security to evaluate detection rules in ESET Inspect Connector since version 1.8 (mandatory for the Cloud environment. If rules evaluation is on the ESET Inspect Server side, then this needs to have communication to LiveGrid® allowed). Some rules depend on information from LiveGrid®, and without the information, these rules are not functional.

HIPS

i HIPS monitors events inside the operating system and provides information needed for ESET Inspect On-Prem and following rules evaluation.

The ESET PROTECT On-Prem Permission Settings

In the ESET PROTECT On-Prem, it is necessary to create a [Static Group](#), where security engineers have access and full permission rights.

We recommend using pre-defined permission sets in the ESET PROTECT On-Prem.

Refer to the [ESET PROTECT On-Prem documentation](#) for more details on creating an ESET PROTECT On-Prem Native User.

For the **EI_SERVER_INSTALLER** Web Console access user, the permission set should be:

ESET Inspect server permission set

i The user with this permission set should be used during the ESET Inspect Server installation process. If there is an error, logs with diagnostics data is created too, which will help solve the problem better.

For the **EI_ADMIN** Web Console access user, the permission set should be:

ESET Inspect user permission set

For the **EI_READ_ONLY** Web Console access user, the permission set should be:

ESET Inspect reviewer permission set

Custom permission sets

You can create custom permission sets (see the [Permission Sets](#) Online Help topic).

A given permissions set enables **Read**, **Use** or **Write** access. In general:

- **Read** permissions are good for auditing users. They can view data but cannot make changes.
- **Use** permissions allow users to use objects and run tasks but not modify or delete them.
- **Write** permissions allow users to either modify respective objects and/or duplicate them.

Certain permissions (listed below) control a process, not an object. That is why they work globally, so it does not matter which static group the permission is applied to. It will work regardless. If the process is allowed to a user, it can use it only over objects with sufficient permissions.

Functionality types:

Access to ESET Inspect On-Prem

- **Read**—Allows logging into ESET Inspect Web Console.

Change Server Settings

- **Write**—Allows changing ESET Inspect Server Settings in **More > Admin > [Settings](#)**.

Edit Notes/Comments

- **Write**—Allows editing notes and comments through whole ESET Inspect On-Prem.

Edit Tags

- **Write**—Allows creating and editing tags in the ESET Inspect On-Prem.

Create & Edit Incidents

- **Write**—Allows creating and editing [incidents](#) in the ESET Inspect On-Prem.

Add Objects to Incidents

- **Write**—Allows working with objects within ESET Inspect On-Prem [incidents](#).

Assign Incidents

- **Write**—Allows to assign incidents to specific user in the [Incidents](#) window.

Change Incident Status

- **Write**—Allows to change the progress status of the [incident](#) report.

Block Modules

- **Write**—Allows blocking executables based on the SHA-1 hash. The blocked executable will appear in the [blocked hashes](#) section. It also allows using the remediation option in [detection details](#).

Clean Modules

- **Write**—Allows to delete the executable file and add it to the [blocked hashes](#) section to prevent future occurrences. It also allows using the remediation option in [detection details](#).

Kill Process

- **Use**—Allows to kill the running process that triggered the [detection](#).

Remote Shell Access

- **Use**—Allows connecting to the Computer via [remote Terminal](#).

Resolve Detection

- **Write**—Allows changing the [detection](#) status.

Change Detection Priority

- **Write**—Allows changing the [detection](#) priority levels.

Mark as Safe/Unsafe

- **Write**—Allows marking [executables](#) as Safe/Unsafe.

Mark as Safe/Unsafe

- **Write**—Allows marking [scripts](#) as Safe/Unsafe.

Create and Manage Rules

- **Write**—Allows allows to create, save and manage [rules](#).

Enable/Disable Rules

- **Write**—Allows enabling or disabling [rules](#).

Import/Export Rules

- **Read**—Allows exporting the [rule](#) from ESET Inspect On-Prem.
- **Write**—Allows importing the [rule](#) into ESET Inspect On-Prem.

Create and Manage Exclusions

- **Write**—Allows creating, saving and managing [exclusions](#).

Enable/Disable Exclusions

- **Write**—Allows enabling or disabling [exclusions](#).

Import/Export Exclusions

- **Read**—Allows exporting the [exclusion](#) from ESET Inspect On-Prem.
- **Write**—Allows importing the [exclusion](#) into ESET Inspect On-Prem.

Resolve Questions

- **Write**—Allows resolving the [question](#).

Create and Manage Tasks

- **Write**—Allows to create and manage [tasks](#).

Pause/Resume Tasks

- **Write**—Allows to pause and resume [tasks](#).

Download Executables

- **Use**—Allows to download the executable file for further diagnostics.

Download Scripts

- **Use**—Allows to download the script file for further diagnostics.

Audit Log

- **Read**—Allows reading the audit log.

ESET Inspect Server Installation

There are several possible ways to install the ESET Inspect Server:

- Using [Graphical User Interface](#) provided by the installer. A recommended way of installation.
- Using [ESET PROTECT On-Prem Deployment](#)



Remember that upgrade will need additional free space depending on the number of endpoints. It will never need more space than the database size. The installer checks exact space requirements.



When the ESET Inspect Server service starts, the following process function executes:

Purge - Clean old data from the database. By default, it executes at midnight, checks all the data older than 30 days, and deletes them (events, processes, and computers that do not send any data for 30 days). You can change the interval of the purge in the [Server settings](#) tab.

When you lower the time frame set for purge, it takes several days to clean up old data before the new setting takes effect.

GUI - Mode Installation

Prerequisites:



Ensure you fulfilled the [requirements](#) before proceeding with the ESET Inspect Server installation. We recommend not installing the ESET PROTECT On-Prem Server and ESET Inspect Server on the same machine.



For installation purposes, use only the user with the Two Factor Authentication option disabled.



Applies to users upgrading from version 1.5 of ESET Enterprise Inspector.

Since version 1.6 of ESET Enterprise Inspector there is a feature, "Optional Rules". We have a separate group of rules that are not enabled by default, yet they are still installed by the installer but in a disabled state. Users can decide on these rules if they suit their environment and enable them manually.

Having this feature, we have decided to move some of the existing rules to the "Optional" category. It means some of the existing rules enabled in your environment may, after the installation, become disabled because they are updated with the new version of the rule, which is optional now. Check disabled rules after the upgrade from previous versions whether this mechanism did not disable some of the rules you want to have enabled.

- ESET Inspect Server has a built-in HTTP/S server and is listening to ports 80(HTTP) or 443(HTTPS). You can change the port settings during the installation process.
- The server needs to have a connection to [LiveGrid®](#).
- Ensure you have a proper host, port number, login, and password to the MySQL database. The user must be able to create a new database and tables.

ESET Inspect Server installation using GUI (only on the server machine)

Follow the steps below to configure and start your ESET Inspect Server:

1. Execute the downloaded installer [file ei_server_nt64_ENU.msi](#).
2. Read the End User License Agreement, select the check box to accept the License Agreement terms (without it, you cannot continue with the installation process), or read the Privacy Policy at the left lower corner of the window. Click **Next**.
3. Choose whether you want to participate in ESET Customer Improvement Program by selecting the check box and click **Next**. ([Telemetry information](#))
4. Choose the destination directory where you want ESET Inspect Server to be installed and click **Next**. You can change the path directly by typing the destination in the command path or by clicking the **Change** button and navigating to the desired folder.
5. Type in the **Web Console HTTPS port** number (by default, it is 443).
6. Type in the **Web Console HTTP port** number (by default, it is 80).
7. Type in the **Connectors port** number (by default, it is 8093, bear in mind that if a different port number is used, you have to change it also during the connector installation process or by [ESET PROTECT On-Prem policy](#))

8. Click **Next**.

9. Select the type of **Database** that you will use for the ESET Inspect Server:

a. In the case of **MySQL**, type in the **Database name** (by default enterpriseinspectordb), **Hostname** (by default localhost, or use the hostname or the IP Address if the database is seated on a different machine than the ESET Inspect Server), **Port** of the database (filled during the database installation process, by default 3306 for MySQL). Fill in the **Username** and **Password** of the database account with sufficient [access rights](#). Click **Next**.

b. If the database type you selected at the top is **MS SQL Server**, type in the **Database name** (by default eidb), **Hostname** (by default localhost, or use the hostname or the IP Address if the database is seated on a different machine than the ESET Inspect Server), **Port** of the database (filled during the database installation process, by default 1433 for MSSQL). Then choose whether you want to use **Use Named Instance** or not by checking the check-box or unchecking it. This will allow you to use a custom database instance, and you can set it in the **Hostname** field in the form HOSTNAME\DB_INSTANCE, for example, 192.168.0.10\EISQL. For the clustered database, use only the clustername. If this option is selected, you cannot change which port will be used, and the system will use default ports determined by Microsoft. Select the **ODBC driver** that is actually installed on the Server machine where the ESET Inspect Server will be installed (if not present, install it following the [ODBC installation process](#)). Fill in the **Username** and **Password** of the database account with sufficient [access rights](#). Click **Next**.

10. The installer will check the database parameters. If some parameters are missing, follow the instructions displayed on the screen. The installer will check the connection to the database. It may take a few seconds to complete. A dialog box explaining the error appears (it may appear behind other windows). If no problems occur, the next screen is displayed. If the database was already created, you are asked to check whether you want to **Keep the data and upgrade the database to the newest format** or **Delete the data and create new database from scratch**. Click **Next**.



For editing the **my.ini** file, ensure it is saved in ANSI, not in UTF-8 format. We recommend using Notepad++, which will not change the file format after saving.

11. If you selected the Delete option or installed the ESET Inspect Server on a fresh MySQL database, the window with requirements for *my.ini* file appears. Make changes as requested, click **Check**. Click **Next**.

12. Select [the type of ESET Inspect user](#). Click **Next**.

13. The default [Detection Rules Set](#) is selected based on [the type of ESET Inspect On-Prem](#). This can also be changed now or after the first log in to the Web Console in a notification screen that appears or by the filtering rules mentioned at the end of this [topic](#). Click **Next**.

14. The default [Data Collection](#) option is selected based on the ESET Inspect On-Prem user selected type. Click **Next**.

15. Select the period for detection storage and low-level data storage ([Data Retention](#)). Click **Next**.



A low-level event is something a process does. So, write a file, do a DNS lookup, create a registry entry, etc. These can be seen in the Events view.



For installation purposes, use only the user with the Two Factor Authentication option disabled.

16. In the next window, fill in the **ESET PROTECT On-Prem hostname** or IP address, ESET PROTECT On-

Prem port for the data connection (by default 2223), ESET PROTECT On-Prem user, and ESET PROTECT On-Prem password (we recommend using EI_SERVER user, which permission settings you will find in [ESET PROTECT On-Prem Permission Settings](#)). Choose the protocol you want to use for communication (we recommend **HTTPS** as a secure option) and **ESET PROTECT On-Prem port of web console** communication (by default 443). Click **Next**. The error message window appears if you typed in the wrong credentials or IP address. Repair invalid data entry and continue.

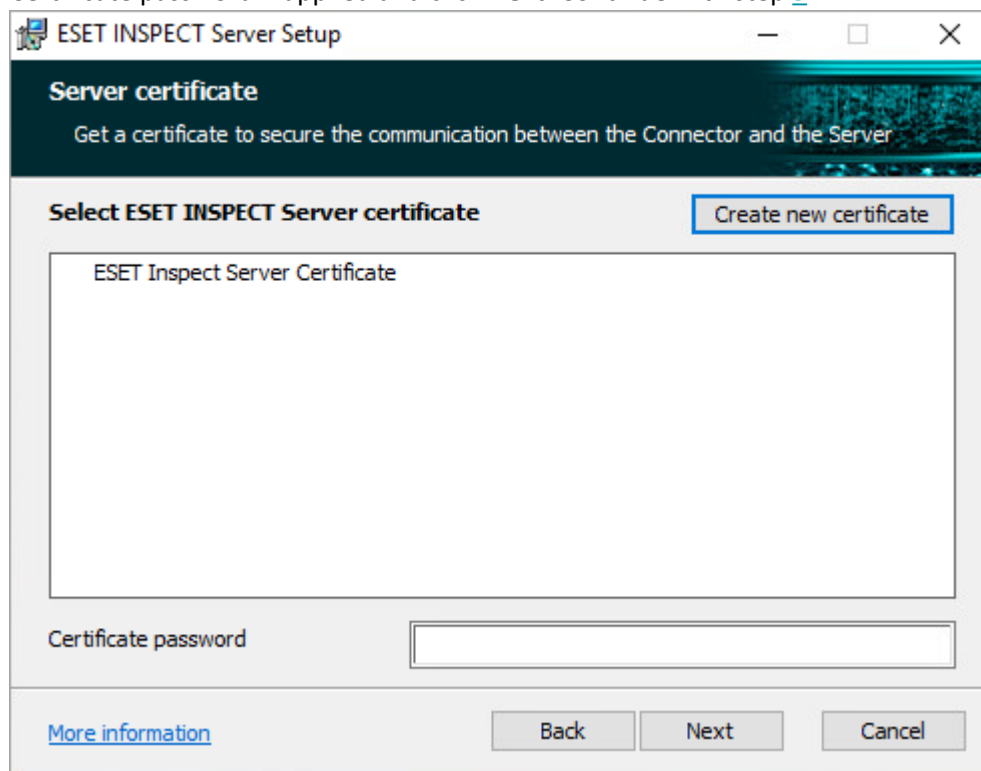
17. Accept the Certification Authority file.

18. Continue with one of the available options:

- a. [Get the certificate from ESET PROTECT On-Prem](#)
- b. [Import the certificate from a file](#)

Get the certificate from ESET PROTECT On-Prem

1. The ESET Inspect Server certificate list displays, where you can select the one desired, type in the Certificate password if applied and click **Next**. Continue with step [5](#).



2. No certificates are displayed here if no ESET Inspect Server certificate is available in ESET PROTECT On-Prem. Generate a new certificate by clicking **Create new certificate**.

3. Select a Certificate authority, type in the corresponding password if required, and click **Next**.

ESET INSPECT Server Setup

Create certificate

Create a certificate to secure the communication between the Connector and the Server

Create new certificate

Select the Certification Authority to create the certificate:

- ESET Bridge Certification Authority
- ESET PROTECT Certification authority
- MSP Synchronization CA

Certification Authority password

[More information](#) Back Next Cancel

4. Fill in the required details. **Description** is used when displaying the list of available server certificates. Parameters like **Host**, **Valid from**, and **Valid to** are pre-filled automatically. Click **Next**, and **Next**. You can also create the certificates in the ESET PROTECT On-Prem itself. [Learn how to create a Certificate Authority](#). [Learn how to create a Peer Certificate](#).

ESET INSPECT Server Setup

Create certificate

Create a certificate to secure the communication between the Connector and the Server

Create new certificate

Description: EI Server certificate

Password

Confirm password

Host

Valid from

Valid to

[More information](#) Back Next Cancel

5. Continue with one of the available options for implementing the essential certificate for HTTPS/SSL connection between the ESET Inspect Web Console and web browser:

- a. [Get the ESET Inspect Web Console certificate from ESET PROTECT On-Prem](#)
- b. [Import the certificate from a file](#)
- c. **Use the same certificate as for Connector/Server communication.**

The HTTPS/SSL certificate has to be signed using the SHA-2 algorithm, or if created in ESET PROTECT On-Prem, the Advanced security has to be enabled (In ESET PROTECT On-Prem navigate **More > Settings > Connection**).

! The Certification Authority used to sign the certificate must be present in the [Web Browser HTTPS/SSL certification list](#).

A web browser will display a warning when connecting to the ESET Inspect Web Console if these requirements are unmet.

Import the server certificate from file

Fill in the path to the ESET Inspect Server Certificate (.PFX file) that was created in ESET PROTECT Server or use the **Change** button to navigate to the file location manually. Fill in the certificate password if applicable. Fill in the path to Certification Authority or use the **Change** button to manually navigate to the file location. Click **Next**.

ESET INSPECT Server Setup

Server certificate
Select a certificate to secure the communication between the Connector and the Server

Import the server certificate from a file:

Server certificate [Change...](#)

Certificate password

Certification Authority [Change...](#)

Select all required Certification Authority files. Leave this field empty if the Certification Authority is already in the system's certificate store on the computers that connect to the ESET INSPECT Server

[More information](#) [Back](#) [Next](#) [Cancel](#)

Continue with one of the available options for implementing the essential certificate for HTTPS/SSL connection between the ESET Inspect Web Console and web browser:

1. [Get the ESET Inspect Web Console certificate from ESET PROTECT On-Prem](#)
2. [Import the certificate from a file](#)
3. **Use the same certificate as for Connector/Server communication.**

By default, certificates created by the ESET PROTECT On-Prem use * (an asterisk) as a hostname (wildcard certificate). ESET Inspect On-Prem does not support such certificates. The user has to use the real hostname of the ESET Inspect Server.

The certificates have to be provided in **PKCS #12** format.

PKCS #12 is a file format, used for storing many cryptography objects as a single file - like certificates or certification authorities. Usually, files that use **PKCS #12** have extension ".pfx" or ".p12".

Certificates cannot have only "*" (one asterisk, nothing more) in place for a host in the following places:

- CN (common name)
- alternative names (from extension {{Subject Alternative Name from }}RFC5280)
- CN in additional certificates (PKCS #12 can hold additional certificates)
- alternative names in additional certificates, for example:



"*" is not allowed.

"*.yourcompany.com" is allowed

"yourcompany.*.hq.com" is allowed.

Another file format frequently used in cryptography is X509. Files using those formats usually have extension ".der" or ".pem".

In ESET Inspect On-Prem, certificates are kept in ".pfx" files, and certification authorities are kept in ".der" files.

Mandatory parameters for creating a Peer Certificate are:

- Product: **"ESET Inspect Server"**
 - Host: Use a real IP Address of the ESET Inspect Server
- If you want to connect ESET Inspect Connector from another network, add another IP or hostname by separating it with a space, comma, or semicolon. For example, HOST 192.168.20.22;10.1.183.88



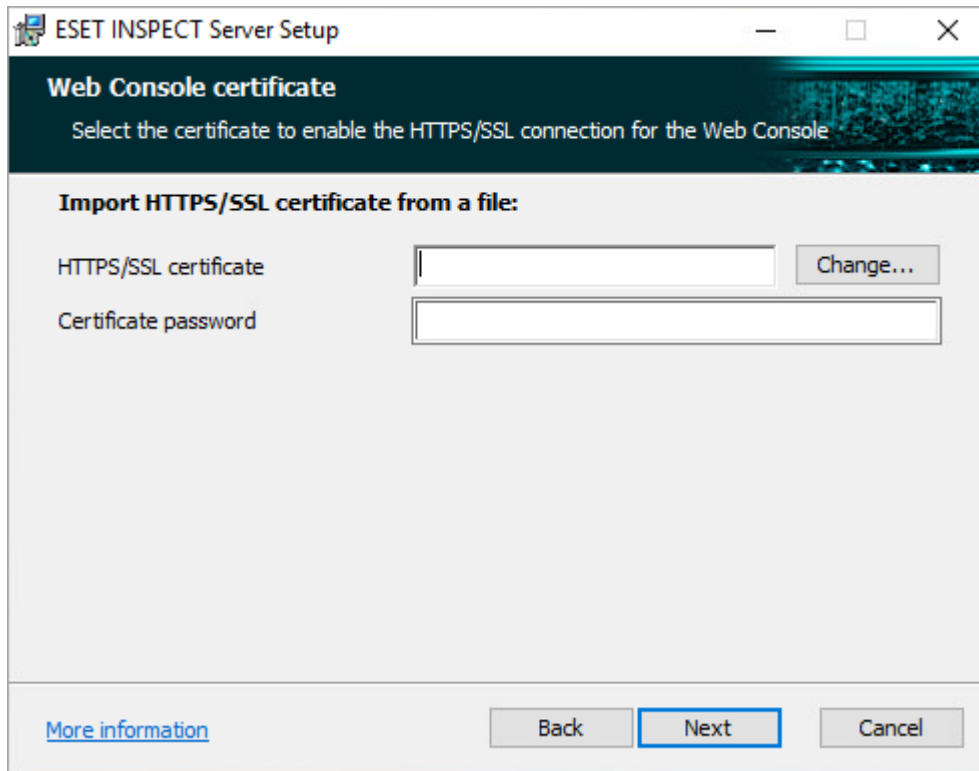
Do not use the semicolon symbol ";" in the filename or the folder name in the path of the certificate. It is used to separate multiple certificates if applicable.

Get the ESET Inspect Web Console certificate from ESET PROTECT On-Prem

1. The list of ESET Inspect Web Console certificates displays, where you can select the one desired, type in the Certificate password if applied and click **Next**.
2. If you do not have the ESET Inspect Web Console certificate created yet in ESET PROTECT On-Prem, you can generate the certificate by clicking the **Create new certificate** button in the upper right corner through the installer.
3. Here you see the Certificate Authorities on the ESET PROTECT On-Prem Server.
4. Select desired Certificate authority, fill in the password if applied, and click **Next**.
5. Fill in the **Description** (you will see this string in the list of ESET Inspect Web Console certificates shown in the previous step) and password if desired. Other parameters can be changed if needed but are pre-defined and filled with, for example, the server's IP address where you are installing the <%EIS%>. Click **Next**, and **Next**. You can also create the certificates in the ESET PROTECT On-Prem itself. [Learn how to create a Certificate Authority](#). [Learn how to create a Peer Certificate](#).
6. Continue with one of the available options for implementing the essential certificate for ESET Inspect Connector-side:
 - a. [Get the certificate from ESET PROTECT On-Prem](#)
 - b. [Import the certificate from a file](#)
 - c. **Do not use connector-side certificate.**

Import ESET Inspect Web Console certificate from file

1. Fill in the path to the ESET Inspect Web Console certificate (.PFX file) that was created in ESET PROTECT On-Prem Server or use the **Change** button to navigate to the file location manually. Fill in the password (if applicable). Click **Next**.



2. Continue with one of the available options for implementing the essential certificate for ESET Inspect Connector-side:

- a. [Get the certificate from ESET PROTECT On-Prem](#)
- b. [Import the certificate from a file](#)
- c. **Do not use connector-side certificate.**

Get the ESET Inspect Connector-side certificate from ESET PROTECT On-Prem

1. The list of ESET Inspect Connector-side certificates displays, where you can select the one desired, type in the Certificate password if applied and click **Next**.

2. If you do not have the ESET Inspect Connector-side certificate created yet in ESET PROTECT On-Prem, you can generate the certificate by clicking the **Create new certificate** button in the upper right corner through the installer.

3. Here you see the Certificate Authorities on the ESET PROTECT Server.

4. Select desired Certificate authority, fill in the password if applied, and click **Next**.

5. Fill in the **Description** (you will see this string in the list of ESET Inspect Web Console certificates shown in the previous step) and password if desired. Other parameters can be changed if needed but are pre-defined and filled with, for example, the server's IP address where you are installing the <%EIS%>. Click **Next**, and **Next**. After choosing this option, click the **Install** button to start the installation process. You can also create the certificates in the ESET PROTECT On-Prem itself. [Learn how to create a Certificate Authority](#). [Learn how to create a Peer Certificate](#).

6. If there is a problem with the installation, follow the instructions in the dialog box. Click **Finish** to finish

the installation.

7. Open **https://localhost** in a web browser to log into ESET Inspect On-Prem. If you want to access ESET Inspect On-Prem from a different device, write the IP Address or hostname of the ESET Inspect Server in a browser.

8. Type in the username and password of the ESET PROTECT On-Prem user with the correct [ESET PROTECT On-Prem Permission Settings](#). An Administrator and User account with the following [ESET PROTECT On-Prem Account Settings](#) is needed. See the [Admin Access Rights](#) topic for ESET PROTECT On-Prem account creation instructions.

Import ESET Inspect Connector-side certificate from file

1. Fill in the path to the ESET Inspect Connector-side Certificate (.PFX file) that was created in ESET PROTECT Server or use the **Change** button to navigate to the file location manually. Fill in the certificate password if applicable. Fill in the path to Certification Authority or use the **Change** button to manually navigate to the file location. Click **Next**.
2. After choosing this option, click the **Install** button to start the installation process.
3. If there is a problem with the installation, follow the instructions in the dialog box that appears. Click **Finish** to complete the installation.
4. Open **https://localhost** in a web browser to log into ESET Inspect On-Prem. If you want to access ESET Inspect On-Prem from a different device, write the IP Address or hostname of the ESET Inspect Server in a browser.
5. Type in the username and password of the ESET PROTECT On-Prem user with the correct [ESET PROTECT On-Prem Permission Settings](#). An Administrator and User account with the following [ESET PROTECT On-Prem Account Settings](#) is needed. See the [Admin Access Rights](#) topic for ESET PROTECT On-Prem account creation instructions.

Web browser HTTPS/SSL certificate list

Download the Authority Public key (.DER file) to the PC/Server from which you will access the ESET Inspect Web Console.

The following procedure will suit the most used web browsers. For Mozilla Firefox, use the second one below:


1. Double-click the DER file.
2. Click **Install Certificate > Local Machine > Place all certificates in the following store > Trusted Root Certification Authorities**.
3. To verify that the certificate was installed successfully, open **Microsoft Management Console** by pressing **Win + R** and type in "MMC".
4. In MMC go to **File > Add/Remove Snap-in... > Certificates > Add > My user account > Finish**, do the same for the **Computer Account** and click **OK**.
5. The certificate installed in the first step should be visible in the following sections:

a. Certificates - Current User > Trusted Root Certificates > Certificates

b. Certificates (Local computer) > Trusted Root Certificates > Certificates

Procedure for Mozilla Firefox

This procedure should work for the most recent Mozilla Firefox version:

1. Click  icon.

2. Go **Options > Privacy & Security > Certificates > View Certificates > Authorities > Import**. Select desired **Authority Public key > Open > Trust this CA to identify websites > OK**.

The type of ESET Inspect On-Prem user

There are three types of ESET Inspect On-Prem users that we think of:

- **Security Operations Center (SOC)**—is recommended to the center with its staff, usually at least five to ten people, consisting of Security Engineers or Analysts. They can work with large amounts of data and analyze it continuously daily. They want to have maximum visibility and do not mind spending additional effort. They also have the skills to effectively and efficiently analyze detections and other data on the network. We're configuring the product to provide as much information as possible.
- **Security-focused IT**—usually has several IT Administrators, some of whom can focus on IT Security. Typically found in Enterprises before the organization establishes its own SOC. They can dedicate time or even people to security but less than an entire SOC. We're limiting information not directly related to threats to prevent an overload of information.
- **IT Administrators**—work alone or with only a few others and have generalist roles without time to dedicate to security. They deal with IT Security as one of many topics and may not have time for it during the week. We limit the amount of information to the most severe issues to prevent an overload of information.

Rules Sets

This dialog controls which new detection rules are enabled after the installation.

New means added with the new install pack and in the **Web Console** in the **Admin > Detection Rules** tab can be found after filtering by **Tag New**.

When updating the ESET Inspect Server, if ESET updated the default rule, it is marked with a tag **Updated**.

- **Enable detection rules with Threat, Warning, and Information severity**—ideal for advanced users who want complete visibility and are already familiar with ESET Inspect On-Prem, which prefer to customize everything manually.
- **Enable detection rules with Threat and Warning severity**—ideal for skilled users who want to do Threat Hunting and evaluate malicious and potentially malicious events.
- **Enable only detection rules with Threat severity**—ideal for new users who know cyber attacks but want to evaluate only confirmed threats.
- **Disable all detection rules**—ideal for new users with no experience with EDR solutions and start with an analysis of confirmed malware and attacks detected and blocked by the ESET Endpoint product.

The more severities are enabled, the more sensitive the product reacts to threats and generates more detections.

Rules can be enabled or disabled at any time in the **Admin > Detection rules** tab of the product:

- The first option can be achieved by filtering the view by severity, enabling all three Threat, Warning, and Info.
- The second option can be achieved by filtering the view by severity, enabling Warning, Info.
- The third option can be achieved by filtering the view by severity and enabling Info.

After selecting the filter of your choice, choose all rules by clicking the check box on the left side of the first row (Rule Name (count)). Click the **Enable/Disable** button.

Data Collection

Data collection settings impact how data is stored in the database.

Regardless of the user's option, all low-level raw events are collected on the endpoints, sent to the server and processed by the rule engine, which generates detections when appropriate.

When detection is generated for a specific event, this specific event is also stored in the database regardless of the selected data collection option. For the events processed by the rule-engine without triggering detection, data collection settings apply as follows:

Store all available data

All collected low-level raw events are stored in the database. This option creates a vast database but allows detailed investigation of possible incidents because the analyst can see everything that happened on the system, regardless of whether it was previously flagged as suspicious by the product or not.

This option allows using all the product's features, such as retroactive search, execution of Threat Hunting queries or a re-run of existing or custom rules on the data.

Store most important data

Stores all the data related to the processes (for instance, you will see all processes executed on the endpoints along with their properties, such as command line, etc.). It also limits the storage of low-level events generated by the processes only to those generating the detection. It means the analyst will see a complete process tree during the investigation (be aware that the data retention setting applies here). Still, for the actions of the processes (such as writing to the disk, writing to the registry, network connection etc.), the analyst will see only those explicitly caught by the rule.

This may turn into a situation where you will see a network connection (detected by the rule) but will not see that the downloaded file was written to the disk (unless another rule does not detect a specific file write). Similarly, you will not be able to retroactively search for IOCs that are not connected to the process/file and were not detected by the rule previously. For example, you will find a file hash or command line fragment but not the registry write anymore.

Suppose you are missing some important events using this option. In that case, you can still customize this setting by creating custom rules (typically with low severity, which you will ignore during the monitoring) that will solely detect events of your interest to save these low-level events to the database.

Store only data directly related to detections

This option stores only those low-level event data explicitly caught by the rule, creating the smallest database in this mode. It applies to the actions (such as writing to the disk, writing to the registry, network connection etc.) and to the processes themselves (process execution, command line, etc.). However, when detection is triggered for the process, process-related data for the process itself, and with the process-related data about all the processes upwards, the process tree and direct child processes will be stored. (Storing process-related data for these additional processes will not store other data, such as "action-related" events.) The database will not store information about all the other processes.

That means that similarly to the option "Store most important data" you may not see some actions and, in this case, also processes that were not explicitly caught by the rule (and are not in that stored part of the process tree mentioned above) with the corresponding consequences. The process tree will not show processes for stored data.

The ability to retroactively search for IOCs would be minimal since you will see neither IOCs related to actions nor IOCs related to process properties (command line, etc.) unless they were detected by the rule previously.

As mentioned in the previous option, you can customize this setting by creating custom rules (typically with low severity, which you will ignore during the monitoring) that will detect events of your interest (including process execution) to save these low-level events to the database.



As mentioned, the storage of low-level event data is significantly affected by which events are detected. It means that lowering the number of enabled rules will, in turn, also decrease the amount of stored data (available for investigation and retroactive search). This should be considered when lowering the Data Collection settings and disabling some rules simultaneously.

For example, selecting "Store only data directly related to detections" and disabling all the rules will lead to storing no data at all and thus causing the product to be dysfunctional.

Store most important data/Store only data directly related to detections

Some features are limited:

- Events view
- Aggregated events view
- Background tasks
- Scripts view
- Search

The goal is to control the database size. The user is making a trade-off between database size and some advanced options.

Store only data directly related to detections option is recommended for IT Administrators.

To change what data is stored in the database, go to **Admin** > [Server Settings](#) in the Database Collection section.

Data Retention

Select how long the data should be in the database stored. The longer the period, the more extensive database will become before old data is [purged](#).

Choose how long you want the data in the database to be stored. By default, it is three months.

Choose how long you want the low-level data in the database to be stored. By default, it is one month. Low-level data accounts for most of the database size and should be kept as brief as possible. It only limits detailed investigations of data not identified as suspicious by the product when removed.

This setting can be changed in **Admin** > [Server Settings](#) in the Database cleanup section.

ESET Inspect Connector collects information about

- the start and termination of a process running on a workstation (including metadata of such executables)
- dynamically loading libraries and dynamically loading drivers (including metadata of such libraries and drivers)
- events when executable files are being saved to the disk
- file modification (including all files present on the disk)
- events when a file (that is important from a security point of view) is being opened or accessed by a user or process (for example, files containing password information used by popular web browsers)
- a modification to registry entries
- network connections
- any code injections to any running processes
- the creation of named pipes
- the creation of users and groups
- users' logins
- WMI executions and queries

ESET PROTECT On-Prem Deployment



Ensure you fulfilled the [requirements](#) before proceeding with the ESET Inspect Server installation. We recommend not installing the ESET PROTECT Server and ESET Inspect Server on the same machine. We do not recommend using this process. Instead, use the [GUI installation](#) process.



For installation purposes, use only the user with the Two Factor Authentication option disabled.

1. Log in to the ESET PROTECT On-Prem with proper rights (ESET PROTECT On-Prem Admin rights or ask ESET PROTECT On-Prem Admin to create and deploy connectors for you if you do not have sufficient

rights).

2. Ensure the computer for installing ESET Inspect Server has an [ESET Management Agent installed](#).

3. Click the desired computer and choose **New Task**.

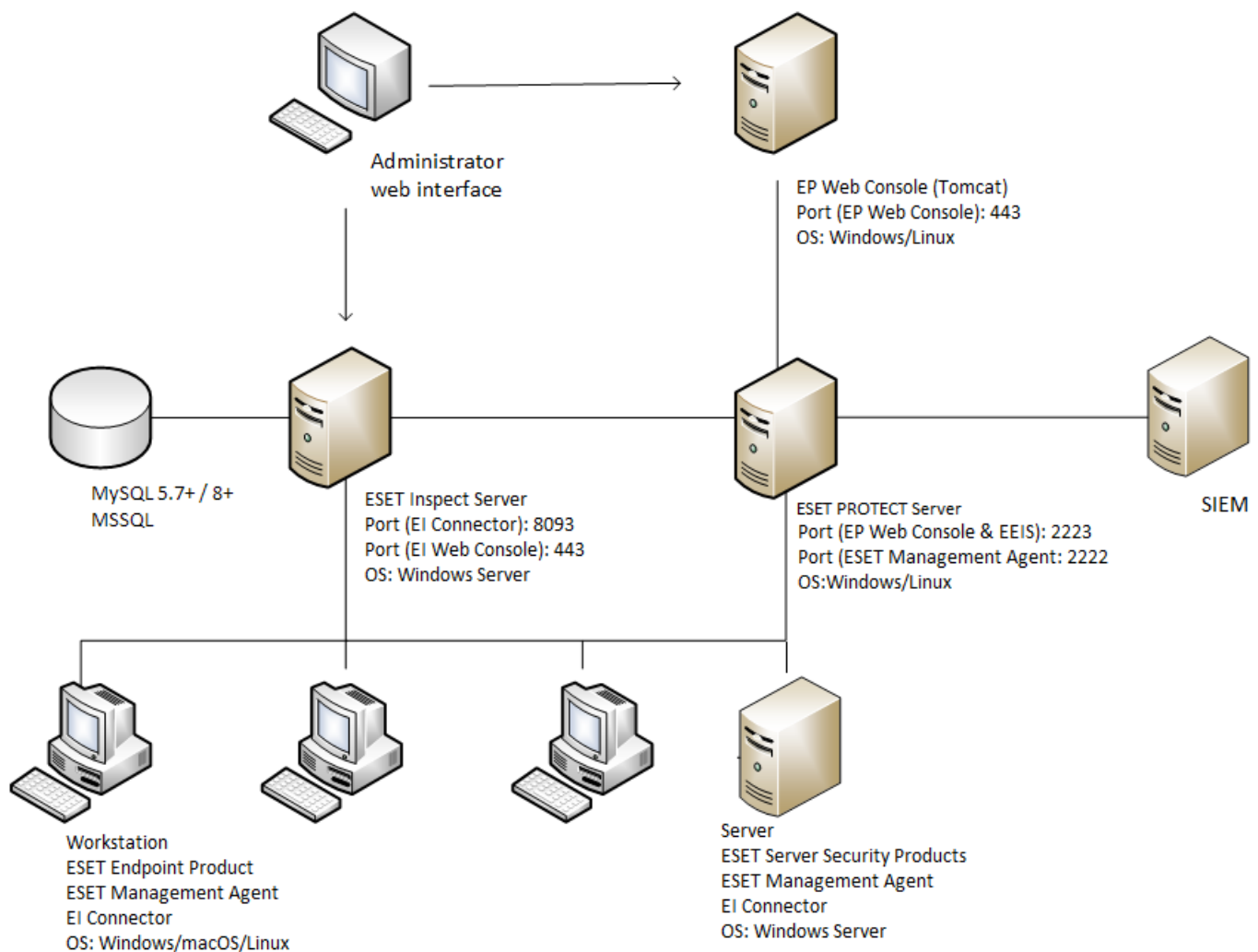
4. Fill in the desired **Name**, **Description**, in **Task Category**, you can keep **All Tasks**, in **Task** select **Software Install**. Click **Settings** in the left menu or the **Continue** button at the bottom of the window.

5. Choose whether you want to install ESET Inspect Server from the repository or specify the URL path to the installer.

6. Fill in the **Installation parameters** field. Use the parameters from the [table](#), or you can leave them blank (if it is an upgrade from the existing installation). Click **Finish**.

7. If the task is already created, you can rerun it on another computer or group of computers. See [Client Tasks executions](#).

ESET Inspect On-Prem Communication Scheme



i SIEM is an acronym for Security Information and Event Management.

Attribute	Description	Required	Default value
APPDIR	Used to set the directory under which application should be installed.	-	By default, the path is "C:\Program Files (x86)\ESET\ESET Inspect Server\" for 32-bit OS and "C:\Program Files\ESET\ESET Inspect Server\" for 64-bit
P_DATABASEHOST	Set the hostname of the Database Server.	-	"localhost"
P_DATABASEPORT	Set the port number the Database Server operates on.	-	"3306"
P_DATABASEUSER	The user that should be used to modify the database.	-	"root"
P_DATABASEPASSWORD	Password to be used to connect to the database. Even if the database allows users not to use a password, the ESET Inspect On-Prem installer does not allow users without passwords for security reasons.	yes	-
P_PORTFORSECUREWEB	The port is used for a secure connection to the ESET Inspect Server frontend.	-	"443"
P_PORTFORWEB	The port is used for standard connection to the ESET Inspect Server frontend.	-	"80"
P_PORTFORAGENTS	The port on which the ESET Inspect Server is supposed to listen for events reported by Agents.	-	"8093"
P_DATABASENAME	Name of the database which is created for the ESET Inspect Server by the installer.	-	"enterpriseinspectordb"
P_ERAHOST	Hostname of ESET PROTECT On-Prem.	-	"localhost"
P_ERAPORT	The port on which ESET PROTECT On-Prem is configured to listen.	-	"2223"
P_ERAUSER	Name of the user used to connect to ESET PROTECT On-Prem.	-	"Administrator"
P_ERAPASSWORD	The password of the user used to connect to ESET PROTECT On-Prem.	yes	-
P_PATH_OF_CERT_FOR_AGENT	An absolute path, on target PC, as for now, we do not support URLs. Mounted remote drives works.	yes	-
P_PATH_OF_CERT_FOR_WEB	An absolute path, on target PC, as for now, we do not support URLs. Mounted remote drives works.	yes	-
P_PATH_OF_CERT_AUTH	An absolute path, on target PC, as for now, we do not support URLs. Mounted remote drives works. It is required to install a Connector with Server assisted certification installation.	-	-
P_PASSWORD_OF_CERT_FOR_AGENT	The certificate's password, if it was typed during the creation process.	-	-
P_PASSWORD_OF_CERT_FOR_WEB	The certificate's password, if it was typed during the creation process.	-	-
P_DELETE_EXISTING_DB	In the case of installation: If set to "1", and the database of a provided name already exists, then this database is deleted and recreated. In the case of uninstalling: If set to "1", deletes existing application database after removing all files. It does not require providing the database name. Do not use with reinstall and update.	-	"0"
P_ISTEMETRYACCEPTED	It enables ESET Inspect On-Prem to send systems telemetry to ESET. It is enabled if different than 0.	-	"1"
P_IS_SERVER_ASSISTED_ERA_CERT_AUTH	It causes the installer to download the ESET PROTECT On-Prem certificate from ERA Server. It is enabled if different than 0.	-	-
P_PATH_OF_ERA_CERT_AUTH	An absolute path, on target PC, as for now, we do not support URLs. Mounted remote drives works. The server-assisted option can be used when ESET PROTECT On-Prem certificate authority cannot be downloaded from ESET PROTECT On-Prem	-	-
P_DATABASETYPE	Choose what type of SQL database you want to use. MySQL or MSSQL	-	MySQL
P_ENABLE_RULES_WITH_SEVERITY_ABOVE	Built-in rules will be marked as disabled if their severity score is not at least the given value.	-	39
P_DETECTIONS_STORAGE_DAYS	Number of days after which detections will be removed from a database	-	93
P_EVENT_STORAGE_DAYS	Number of days after which events will be removed from a database	-	7
P_DATA_COLLECTION_LEVEL	The level of data collection allows to set a type of data to be stored in a database. 0(Detections only): This mode saves only detections. events and processes not related to detection are discard 1(Most data): This mode saves detections and all processes. 2(All data): This mode saves detections, events, and processes.	-	0

Troubleshooting the installation

ESET Inspect Server and ESET Inspect Connector write error logs to *C:\ProgramData\ESET\Inspect Server\Logs* respectively *C:\ProgramData\ESET\Inspect Connector\Logs*.



If you use Windows Firewall as your default firewall, the installation creates necessary Windows Firewall rules for communication between ESET Inspect On-Prem components. If the Firewall is disabled or you use a third-party firewall, ensure that ports "80,443,8093,2223" are allowed.

To gather the data on the installation process (both successful or failed installation), it is required to execute the installer package from an administrative command line along with some additional parameters: `/L*Vx temp_log.txt`

Below is a sample command to install the ESET Inspect Server in silent mode and save logs to *temp_log.txt*:

To run GUI - Mode installation and collect logs, use:

```
msiexec /i "ei_server_nt32_ENU.msi" /L*Vx temp_log.txt"
```

```
msiexec /i "ei_server_nt32_ENU.msi" /q /L*Vx temp_log.txt P.DATABASEPASSWORD="yourDatabasePasswordHere"
```

The following is a sample command to install ESET Inspect Connector along with GUI mode and providing one

optional parameter:

```
✓ msixexec /i "ei_connector_nt32_ENU.msi" /L*Vx temp_log.txt /q P_HOSTNAME="localhost"
```

ESET Inspect Server Migration

There are two ways to migrate ESET Inspect Server from one server to another:

- [Clean installation with the same IP address](#)—the new installation uses the original IP address.
- [Clean installation with a different IP address](#)—the new installation uses the new IP address.

Clean installation with the same IP address

This procedure aims to install an entirely new instance of ESET Inspect Server that will have the same IP address as your previous server but will not use the database from the old ESET Inspect Server.

- 1.**Stop** ESET Inspect On-Prem Service on an old ESET Inspect Server machine.
- 2.**Turn** off the old ESET Inspect Server machine.

⚠ Ensure that the new ESET Inspect Server machine has the same IP address as the old one.

- 3.**Run** the ESET Inspect Server installer on a new server machine and proceed like a typical [installation](#) process.
- 4.**Connect** to ESET Inspect Server's Web Console.
- 5.If the connection works, you can dismantle/disband/uninstall the old ESET Inspect Server.

Clean installation with a different IP address

This procedure aims to install an entirely new ESET Inspect Server instance that does not use the same IP address as your previous server of the old ESET Inspect Server.

- 1.**Stop** ESET Inspect On-Prem Service on an old ESET Inspect Server machine.
- 2.**Turn** off the old ESET Inspect Server machine.
- 3.**Run** the ESET Inspect Server installer on a new server machine and proceed like a typical [installation](#) process.
- 4.To make ESET Inspect Connectors connect to the new ESET Inspect Server, create a new [policy](#) in ESET PROTECT On-Prem for ESET Inspect Connectors.
- 5.**Connect** to ESET Inspect Server's Web Console.
- 6.If the connection works, you can dismantle/disband/uninstall the old ESET Inspect Server.

ESET Inspect Database Migration

Click the appropriate link below for instructions to migrate the ESET Inspect Server database between different SQL Server instances (this also applies when relocating to a different SQL Server version or when migrating to a SQL Server hosted on a different machine):

- [The migration process for Microsoft SQL Server](#)
- [The migration process for MySQL Server](#)

The migration process for MySQL Server

Prerequisites

- Source and target SQL Server instances must be installed.
- The target SQL Server instance must have at least the same version as the source instance. A downgrade is not supported!

Using command prompt

In the commands, configuration files, or SQL statements below, always replace the following:

- **SRCHOST** with the address of the source database server
- **SRCROOTLOGIN** with the source MySQL server root user login
- **SRCEEIDBNAME** with the name of the source ESET Inspect Server database to back up
- **TARGETHOST** with the address of the target database server
- **TARGETROOTLOGIN** with the target MySQL server root user login

It is unnecessary to execute the SQL statements below via the command line. You can use an application you already know if a graphical user interface tool is available.

You can run the commands from the Source or Target machine if those machines are in the same network and the ping between those machines is working. You must manually move the backup file to the target machine if they are not in the same network.

1.**Stop** the ESET Inspect Server service.

2.**Navigate** to *C:\Program Files\MySQL\MySQL Server 5.7\bin* or *C:\Program Files\MySQL\MySQL Server 8\bin* based on the MySQL version you have installed.

3.**Create** a full database backup of the source ESET Inspect Server database (the database you plan to migrate):

```
mysqldump --host SRCHOST --user=SRCROOTLOGIN --password --events --opt --routines --triggers --databases SRCEEIDBNAME --default-character-set=utf8mb4 --result-file="C:\USERS\public\BACKUPFILE.sql"
```

4.**Enter** the root login password. You can also add it directly after the **--password** parameter (**--password=ABCD**).

5.**Adjust** the my.ini file on the target machine based on the version of MySQL you are using. [Version 5.7 or](#)

8.

6. **Restore** the database on the target MySQL server.

```
✓ mysql --host TARGETHOST --user=TARGETROOTLOGIN --password < "C:\USERS\public\BACKUPFILE.sql"
```

7. **Enter** the root login password. You can do it as well by adding it directly after the -p parameter (-pABCD).

8. **Run** the ESET Inspect Server service if the target MySQL Server machine keeps the same IP address and name of the database as the Source one.

9. When you migrate the database to another server (MySQL IP or port are changed) or change the database name (MySQL IP and port are the same, but database name changed), you have to re-setup the ESET Inspect Server by using the "Repair/Change" option in the Installer. Leave all the settings as they are, but change the database settings like MySQL IP, port, or database name.

The migration process for Microsoft SQL Server

Prerequisites

- Source and target SQL Server instances must be installed.
- The target SQL Server instance must have at least the same version as the source instance. A downgrade is not supported!

Using command prompt

1. **Stop** the **ESET Inspect Server** service.

2. **Run** the **Command Prompt** application and use this command:

```
✓ SQLCMD -U sa -S localhost -Q "BACKUP DATABASE enterpriseinspectordb TO DISK = N'C:\USERS\public\BACKUPFILE.bak'"
```

3. **Copy** created backup file to the designated MSSQL machine and run this command to restore the backup of the database on the designated machine:

```
✓ SQLCMD -U sa -S localhost -Q "RESTORE DATABASE enterpriseinspectordb FROM DISK = N'C:\USERS\public\BACKUPFILE.bak'"
```

4. **Enable** TCP/IP on the target machine.

5. Ensure the Firewall on the source machine is set up to allow incoming and outgoing communication at port (by default 1433, or changed by the user during [installation process](#))

6. **Run** the ESET Inspect Server service if the target MSSQL Server machine keeps the same IP address as the Source one.

7. When you migrate the database to another server (Microsoft SQL IP or port will be changed), you have to re-setup the ESET Inspect Server by using the "Repair/Change" option in the Installer. Leave all the settings, but change the database settings like Microsoft SQL IP port.

For attribute meaning, visit <https://learn.microsoft.com/sql/tools/sqlcmd/sqlcmd-utility>.

The **enterpriseinspectordb** in the example is the default DB name created during the ESET Inspect Server [installation](#) process. If you used a different name for the DB, replace the one used in the example above.

Server upgrade through ESET PROTECT On-Prem



We do not recommend upgrading the ESET Inspect Server via the ESET PROTECT On-Prem task because the server upgrade can take a long time due to the database upgrade, and the user cannot check the progress of the upgrade operation. We recommend [manually installing/upgrading the ESET Inspect Server](#) where a progress bar is visible, displaying the current status.

Update ESET Products button in ESET PROTECT On-Prem

1. In the ESET PROTECT On-Prem, navigate to the ESET Inspect Server computer overview.
2. In the **Products & Licenses** tile, you see if the version of ESET Products needs to be updated.
3. Click the tile, and you are redirected to the sub-tab Products & Licenses.
4. Click the **UPDATE ESET PRODUCTS** button, and the window with available latest versions for ESET Products will appear.
5. Check the check box on the line with ESET Inspect Server and click the **OK** button.

ESET Inspect Connector Installation

ESET Inspect Connector is installed on endpoint devices that are monitored by ESET Inspect On-Prem / ESET Inspect and collects the data for the ESET Inspect On-Prem, removes malicious components, and blocks execution of these components.

ESET Inspect Connector can be installed/deployed on [Windows](#), [macOS](#) or [Linux](#) systems using their GUI, from the command line or by deploying through ESET PROTECT On-Prem.

For the uninstallation process of ESET Inspect Connector, [follow](#).



Before installing the ESET Inspect Connector, use the latest ESET Endpoint Product update.



Remember that if the ESET Inspect Connector loses the connection with the ESET Inspect Server, it caches the data locally, and the limit is 1GB. The value is in Bytes, so the actual set value is 1073741824. This can be changed in *ESET Inspect Connector.policy.ini* file by adding MaxOfflineStorageSize under the [Offline] section.

If you have *ESET Inspect Connector.ini* file, add to the end of the file:

[Offline]

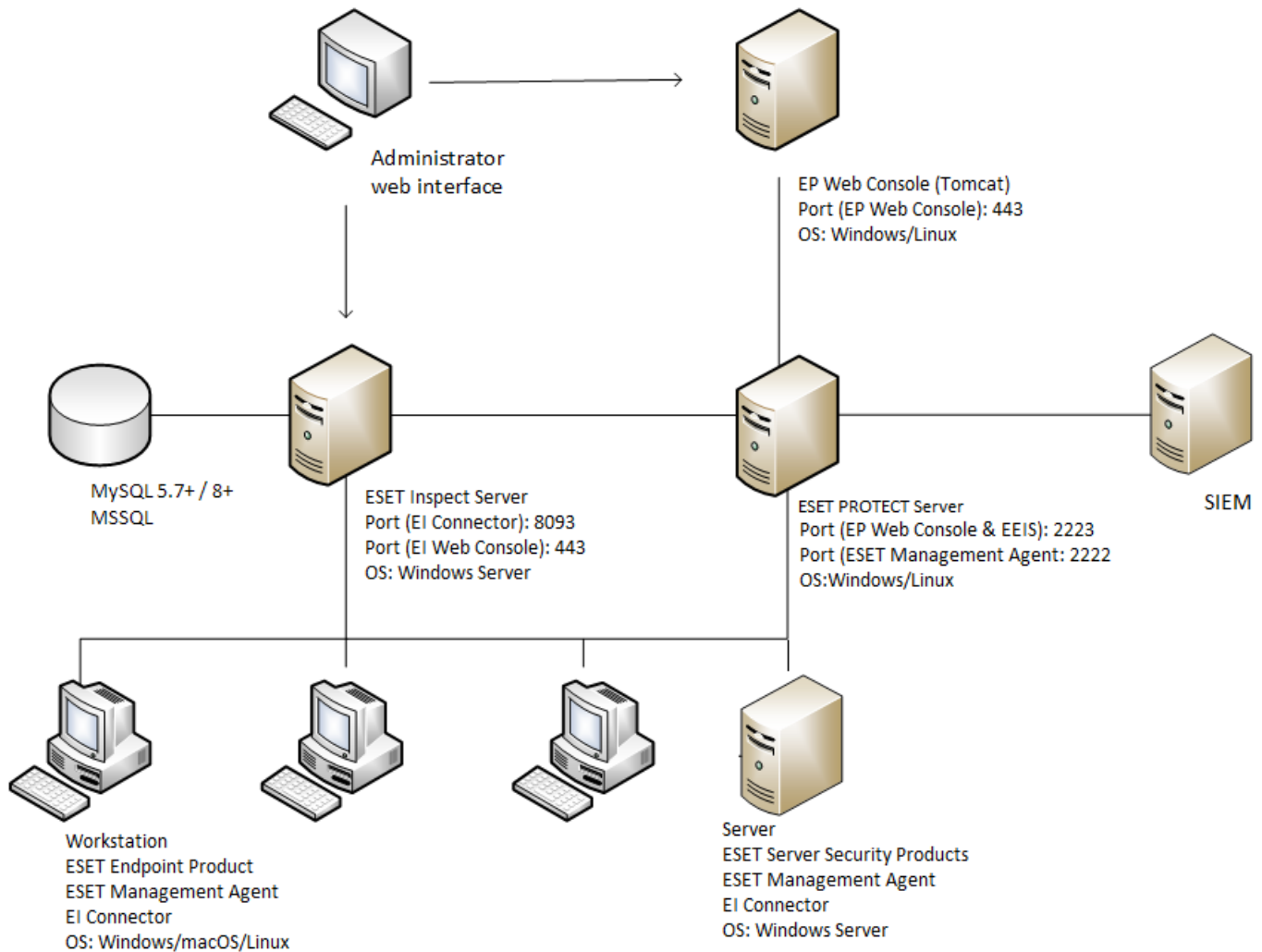
MaxOfflineStorageSize=value_in_bytes

But *ESET Inspect Connector.ini* can be changed only in Safe Mode.



After installing or upgrading ESET Inspect Connector, there is approximately a 7-minute delay until the connector starts communicating with ESET Inspect Server. Because of that, you see the warning message in ESET PROTECT On-Prem that the computer cannot connect to ESET Inspect Server. If connected correctly, the ESET Inspect Connector will be immediately visible as active at ESET Inspect Web Console.

ESET Inspect On-Prem Communication Scheme



i SIEM is an acronym for Security Information and Event Management.

Windows

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

The recommended way to install ESET Inspect Connector for ESET Inspect is to use an [All-in-one installer](#). The installer with all needed components is created and ready to deploy at the endpoint.

A [canary file](#) is deployed during the installation process. You can prevent the deployment of it by using [command](#)

[line parameter](#) P_INSTALL_CANARY_FILES.

[Installation of the ESET Inspect Connector for ESET Inspect](#)

There are several possible ways to install the ESET Inspect Connector for ESET Inspect On-Prem version:

- Using [Graphical User Interface](#) provided by the installer
- Using [Command line](#)
- Using [ESET PROTECT On-Prem Deployment](#)
- Using an [All-in-one installer](#) from ESET PROTECT On-Prem. A recommended way as the installer with all needed components is created and ready to deploy at the endpoint

ESET Inspect All-in-one Installer

A recommended way to install ESET Inspect Connector for ESET Inspect endpoints is to use an [All-in-one installer](#).



You need to activate ESET Inspect Connector with an "ESET Inspect" license. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.



The ESET Inspect Connector will be visible in ESET Inspect Web Console immediately after activation and correct policy setting. In a few minutes, you should be able to view the first events sent by connectors.

ESET Inspect Connector is writing error logs into the folder:

- Windows *C:\ProgramData\ESET\Inspect Connector\logs*
- macOS */Library/Application Support/ESET/eset_eia/logs*
- Linux */var/log/eset/eei/*

If you experience any other issues, follow the instructions on gathering debug data as detailed in [Troubleshooting the installation](#) topic.

Windows GUI - Mode Installation

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

Installation process

1. Execute the downloaded [installer](#) file **ei_connector_nt32_ENU.msi** or **ei_connector_nt64_ENU.msi**, depending on the system.
2. Accept the license agreement and click **Next**.
3. Choose the destination directory where you want ESET Inspect Connector installed and click **Next**.

4.If you need to change the default connection settings to ESET Inspect Connector:

- a.Type the proper values into the following fields: ESET Inspect Server host, ESET Inspect Server port.
- b.Choose whether you want to use Server assisted installation or Offline installation.

5.Click **Next**.

The ESET Inspect Connector needs the same Certificate authority used to sign a certificate for ESET Inspect Server. You can provide it in one of the methods below:

- Server assisted installation
- Certificate authority on local disk
- Certificate authority installed in Windows Certificate Store

6.In the case of Server assisted installation, the dialog box with certification details appears. Click **Yes** to accept the Certification Authority for ESET Inspect Connector.

7.In the Offline installation, fill the path to the [Certification Authority](#) or click the **Change** button and navigate to it. Click **Next**.

8.Click **Install**. A progress bar appears, displaying the current status.

9.Click **Finish**.

10.If there is a problem with the installation, follow the instructions in the dialog box that appears.

You need to activate ESET Inspect Connector with an "ESET Inspect" license. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.

Assign policy

It is necessary to create a [Policy](#) to make ESET Inspect Connector communicate with ESET Inspect Server (this is not necessary for ESET Inspect):

- 1.In the **Settings** window, select the product "ESET Inspect Connector"
- 2.Fill in the **Server Address** with the ESET Inspect Server IP address.
- 3.Edit the **Certificate Authority** by clicking **Edit** > **Add** > **Open Certificate Authority**. Chose the certificate that was used during ESET Inspect Server installation. Click **Save**.
- 4.Click **Continue**.
- 5.Select the **Assign** button and select the computer/computers you want the policy to be applied on in the **Assign** window. Click **Finish**.

The ESET Inspect Connector will be visible in ESET Inspect Web Console immediately after activation and correct policy setting. In a few minutes, you should be able to view the first events sent by connectors. ESET Inspect Connector is writing error logs into the folder:

- Windows *C:\ProgramData\ESET\Inspect Connector\logs*
- macOS */Library/Application Support/ESET/eset_eia/logs*
- Linux */var/log/eset/eei/*

If you experience any other issues, follow the instructions on gathering debug data as detailed in [Troubleshooting the installation](#) topic.

Installation from a windows command line

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

For the command line installation, follow these steps:

1. Download the [installer](#) file `ei_connector_nt32_ENU.msi` or `ei_connector_nt64_ENU.msi`, depending on the system.
2. Open the command line and navigate to the downloaded file.
3. You can use the example from below with altered attributes or run with specified in the table of attributes.

You may use several attributes with the installer using the silent mode during installation. The hostname is required:

Attribute	Description	Required	Default value
APPDIR	Used to set directory under which application will be installed	-	C:\Program Files(x86)\ESET\ESET Inspect Connector\ for 32-bit OS and C:\Program Files\ESET\ESET Inspect Connector\ for 64-bit
P_HOSTNAME	Used to set host, on which ESET Inspect Server is installed	yes	"localhost"
P_PORT	Used to set the number of the port on which ESET Inspect Server is listening for data from ESET Inspect Connectors	-	8093
APPDATADIR	The directory used to store logs and additional output files	-	"C:\ProgramData\ESET\Inspect Server"
P_PATH_TO_CERT_AUTH	The absolute path to the Certificate Authority file on the target PC. Currently, URLs are not supported. Mounted remote drives like \\store03 should work. Multiple files can be separated by char ";"	-	-
P_IS_SERVER_ASSISTED	If you do not have the Certificate Authority present, set this parameter to 1 (P_IS_SERVER_ASSISTED=1) for server-assisted installation. If this parameter is used user does not need to use P_PATH_TO_CERT_AUTH	-	-
P_INSTALL_CANARY_FILES	If enabled, the installer will generate a canary file and place it in a hidden directory. Setting this value to "0" skips file generation.	-	1

✓ `msiexec /i ei_connector_nt32_ENU.msi P_HOSTNAME="192.168.5.21" P_PORT="8093" P_PATH_TO_CERT_AUTH="C:\repo\Component\Products\Inspect Server\Src\test\http_server\certs\ca_store\ca.cert.der"`



You need to activate ESET Inspect Connector with an "ESET Inspect" license. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.

Assign policy

It is necessary to create a [Policy](#) to make ESET Inspect Connector communicate with ESET Inspect Server (this is not necessary for ESET Inspect):

1. In the **Settings** window, select the product "ESET Inspect Connector"
2. Fill in the **Server Address** with the ESET Inspect Server IP address.
3. Edit the **Certificate Authority** by clicking **Edit** > **Add** > **Open Certificate Authority**. Chose the certificate that was used during ESET Inspect Server installation. Click **Save**.
4. Click **Continue**.

5. Select the **Assign** button and select the computer/computers you want the policy to be applied on in the **Assign** window. Click **Finish**.

The ESET Inspect Connector will be visible in ESET Inspect Web Console immediately after activation and correct policy setting. In a few minutes, you should be able to view the first events sent by connectors. ESET Inspect Connector is writing error logs into the folder:

- Windows *C:\ProgramData\ESET\Inspect Connector\logs*
- macOS */Library/Application Support/ESET/eset_eia/logs*
- Linux */var/log/eset/eei/*

If you experience any other issues, follow the instructions on gathering debug data as detailed in [Troubleshooting the installation](#) topic.

Troubleshooting the installation

ESET Inspect Server and ESET Inspect Connector write error logs to *C:\ProgramData\ESET\Inspect Server\Logs* respectively *C:\ProgramData\ESET\Inspect Connector\Logs*.

- ! If you use Windows Firewall as your default firewall, the installation creates necessary Windows Firewall rules for communication between ESET Inspect On-Prem components. If the Firewall is disabled or you use a third-party firewall, ensure that ports "80,443,8093,2223" are allowed.

To gather data on the installation process (both successful or failed installation), it is required to execute the installer package from an administrative command line along with some additional parameters: */L*Vx temp_log.txt*

Below is a sample command to install ESET Inspect Server in silent mode and save logs to *temp_log.txt*:

To run GUI - Mode installation and collect logs, use:

```
✓ msixexec /i "ei_server_nt32_ENU.msi" /L*Vx temp_log.txt"
```

```
✓ msixexec /i "ei_server_nt32_ENU.msi" /q /L*Vx temp_log.txt P.DATABASEPASSWORD="yourDatabasePasswordHere"
```

The following is a sample command to install ESET Inspect Connector along with GUI mode and providing one optional parameter:

```
✓ msixexec /i "ei_connector_nt32_ENU.msi" /L*Vx temp_log.txt /q P_HOSTNAME="localhost"
```

GUI Repair/Change

ESET Inspect Connector reinstallation using GUI

1. Use the "Modify" option from Apps & Features (or Programs and Features at Control Panel for earlier systems) or execute the downloaded installer file **ei_connector_nt32_ENU.msi** or **ei_connector_nt64_ENU.msi**, depending on the system.

2. Click **Repair/Change**.

3. Change the ESET Inspect Server host address and port or keep those from the previous installation.

4. Choose one of the following options:

a. Do not change current CA settings—This will keep the certification authority from the previous installation.

b. Server assisted installation—If certificates on the server side change and you do not want to add them manually.

c. Offline installation—You can install certificates manually if you have exported them from the server.

5. In the case of a Server assisted installation, the dialog box with certification details appears. Click **Yes** to accept the Certification Authority for ESET Inspect Connector.

6. In the Offline installation, fill the path to the **Certification Authority** or click the **Change** button and navigate to it. Click **Next**.

7. Click **Repair**. A progress bar appears, displaying the current status.

8. If no problems occur, the next screen shows up. Click **Finish**, and your application is ready to use.

9. If there is a problem with the installation, follow the instructions in the dialog box that appears.

The ESET Inspect Connector will be visible in ESET Inspect Web Console immediately after activation and correct policy setting. In a few minutes, you should be able to view the first events sent by connectors.

ESET Inspect Connector is writing error logs into the folder:



- Windows *C:\ProgramData\ESET\Inspect Connector\logs*
- macOS */Library/Application Support/ESET/eset_eia/logs*
- Linux */var/log/eset/eei/*

If you experience any other issues, follow the instructions on gathering debug data as detailed in [Troubleshooting the installation](#) topic.

Upgrade through ESET PROTECT On-Prem

For upgrade through the ESET PROTECT On-Prem, you can follow the same procedure described in the [ESET PROTECT On-Prem Deployment](#) topic.

GUI Upgrade from earlier version

In the second installation screen:

Fill in the proper ESET Inspect Server IP address (if unchanged, no action is needed)

Fill in the proper ESET Inspect Server port (if unchanged, no action is necessary)

Choose how you want to work with the Certification Authority:

- **Do not change current CA settings**—use this option if you use the same CA.
- **Server assisted installation**—if the ESET Inspect Server IP address changed or you want to use a different CA currently used by your ESET Inspect Server, you can use this option to help you with the proper setting. Click **Next**. The dialog box with certification details appears. Click **Yes** to accept the Certification Authority for ESET Inspect Connector.
- **Offline installation**—in the next screen, fill the path to the **Certification Authority** or click the **Change** button and navigate to it. Click **Next**.

Click **Install**. A progress bar will appear, displaying the current status.

If no problems occur, the next screen displays. Click **Finish**, and your application is ready to use.

If there is a problem with the installation, follow the instructions in the dialog box that appears.

macOS

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

Due to the deprecation of Auditpipe/OpenBSM, the HIPS component on macOS Sonoma (14.0) requires additional installation steps provided below:



1. Rename or copy `/etc/security/audit_control.example` to `/etc/security/audit_control`.
2. Re-enable the `system/com.apple.auditd` service, execute the following command as a privileged user:
`launchctl enable system/com.apple.auditd`
3. Reboot the computer.

ESET Inspect Connector installation on macOS

There are several possible ways to install the ESET Inspect Connector for ESET Inspect On-Prem / ESET Inspect version:

- Using [Graphical User Interface](#) provided by the installer
- Using [Terminal](#)
- Using [ESET PROTECT On-Prem Deployment](#)

macOS GUI - Mode Installation

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

ESET Inspect Connector installation on macOS

1. Download the ESET Inspect Connector installation [file](#).
2. Copy the installation file to the desired computer.
3. Run *ei_connector_macos.pkg* file.
4. On the introduction screen, click the **Continue** button.
5. On the read me screen, you can **Print** or **Save** the System requirements or **Go Back**. Click **Continue**.
6. You can change the installation folder on the installation type screen by clicking the **Change Installation Location** button. Click **Install**.
7. Type your administrator credential to allow the installer to continue. Click **Install Software**.
8. In the summary window, click the **System preferences/Security & Privacy/Privacy/Full disk access** to grant ESET Inspect Connector full disk access.
9. Click **Close**.



You need to activate ESET Inspect Connector with an "ESET Inspect" license. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.

Assign policy

It is necessary to create a [Policy](#) to make ESET Inspect Connector communicate with ESET Inspect Server (this is not necessary for ESET Inspect):

1. In the **Settings** window, select the product "ESET Inspect Connector"
2. Fill in the **Server Address** with the ESET Inspect Server IP address.
3. Edit the **Certificate Authority** by clicking **Edit > Add > Open Certificate Authority**. Chose the certificate that was used during ESET Inspect Server installation. Click **Save**.
4. Click **Continue**.
5. Select the **Assign** button and select the computer/computers you want the policy to be applied on in the **Assign** window. Click **Finish**.

From version macOS 10.14 onwards, you will receive the notification, "**Your computer is partially protected from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow Full disk access to ESET Endpoint Security for macOS**".

For a fully functional ESET Inspect Connector, grant full disk access:

1. Open **Preferences > Security & Privacy > Privacy**.
2. Unlock settings in the lower-left corner.
3. Scroll the left side menu and click **full disk access**.
4. In the right side menu mark the ESET Endpoint Security/ESET Endpoint Antivirus, ESET Management

Agent, ESET Inspect Connector and also ESET Real-time system protection.

5.Lock your settings.

Using MDM

To allow Full disk access remotely:

- 1.Download the [.plist](#) configuration file.
- 2.Deploy the .plist configuration profile file using the MDM server.

Your computer needs to be enrolled in the MDM server to deploy configuration profiles to those computers.

Installation from a macOS terminal

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

ESET Inspect Connector installation on macOS

1. Download the ESET Inspect Connector installation [file](#).
2. Copy the installation file to the desired computer.
3. Open the Terminal.
4. Execute the command `"sudo installer -pkg "/PATH_TO_INSTALLER/ESET_Inspect_Connector.pkg" -target LocalSystem"`.



You need to activate ESET Inspect Connector with an "ESET Inspect" license. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.

Assign policy

It is necessary to create a [Policy](#) to make ESET Inspect Connector communicate with ESET Inspect Server (this is not necessary for ESET Inspect):

- 1.In the **Settings** window, select the product "ESET Inspect Connector"
- 2.Fill in the **Server Address** with the ESET Inspect Server IP address.
- 3.Edit the **Certificate Authority** by clicking **Edit** > **Add** > **Open Certificate Authority**. Chose the certificate that was used during ESET Inspect Server installation. Click **Save**.

4. Click **Continue**.

5. Select the **Assign** button and select the computer/computers you want the policy to be applied on in the **Assign** window. Click **Finish**.

From version macOS 10.14 onwards, you will receive the notification, "**Your computer is partially protected from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow Full disk access to ESET Endpoint Security for macOS**".

For a fully functional ESET Inspect Connector, grant full disk access:

1. Open **Preferences > Security & Privacy > Privacy**.

2. Unlock settings in the lower-left corner.

3. Scroll the left side menu and click **full disk access**.

4. In the right side menu mark the ESET Endpoint Security/ESET Endpoint Antivirus, ESET Management Agent, ESET Inspect Connector and also ESET Real-time system protection.

5. Lock your settings.

Using MDM

To allow Full disk access remotely:

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

2. Deploy the .plist configuration profile file using the MDM server.

Your computer needs to be enrolled in the MDM server to deploy configuration profiles to those computers.

Linux

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

ESET Inspect Connector installation on Linux

There are several possible ways to install the ESET Inspect Connector for ESET Inspect On-Prem / ESET Inspect version:

- Using [Terminal](#)

- Using [ESET PROTECT On-Prem Deployment](#)

Linux Terminal Installation

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

ESET Inspect Connector installation on Linux

1. Download the ESET Inspect Connector installation [file](#).
2. Copy the installation file to the desired computer.
3. Open the Terminal in the folder where the file was copied to.
4. Execute the command "`sudo chmod 777 *`" to get full access to the installation file.
5. Execute the command "`sudo ./ei_connector_linux.sh`".



You need to activate ESET Inspect Connector with an "ESET Inspect" license. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.

Assign policy

It is necessary to create a [Policy](#) to make ESET Inspect Connector communicate with ESET Inspect Server (this is not necessary for ESET Inspect):

1. In the **Settings** window, select the product "ESET Inspect Connector"
2. Fill in the **Server Address** with the ESET Inspect Server IP address.
3. Edit the **Certificate Authority** by clicking **Edit > Add > Open Certificate Authority**. Chose the certificate that was used during ESET Inspect Server installation. Click **Save**.
4. Click **Continue**.
5. Select the **Assign** button and select the computer/computers you want the policy to be applied on in the **Assign** window. Click **Finish**.

The ESET Inspect Connector will be visible in ESET Inspect Web Console immediately after activation and correct policy setting. In a few minutes, you should be able to view the first events sent by connectors. ESET Inspect Connector is writing error logs into the folder:

- Windows *C:\ProgramData\ESET\Inspect Connector\logs*
- macOS */Library/Application Support/ESET/eset_eia/logs*
- Linux */var/log/eset/eei/*

If you experience any other issues, follow the instructions on gathering debug data as detailed in [Troubleshooting the installation](#) topic.

ESET PROTECT On-Prem Windows/macOS/Linux Deployment

Prerequisites

Ensure you have met the [System Requirements](#) needed to install the ESET Inspect Connector successfully.

To install ESET Inspect Connector for ESET Inspect, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#). For the ESET Inspect Connector installation for ESET Inspect On-Prem on-premises version, you need first deploy the [ESET Management Agent](#) and install [ESET Endpoint Product](#).

Otherwise, the ESET Inspect Connector will display information that ESET Endpoint Product is required, and your installation will fail if they are not installed.

ESET PROTECT On-Prem Windows/macOS/Linux deployment

1. Log in to the ESET PROTECT On-Prem with proper rights (ESET PROTECT On-Prem Admin rights or ask ESET PROTECT On-Prem Admin to create and deploy connectors for you if you do not have sufficient privileges).
2. Click **COMPUTERS** in the left side menu.
3. You can deploy the connector in two ways:
 - On one computer.
 - On a group of computers.
4. Click the desired computer and choose **New Task**.
5. Fill in the desired **Name** and **Description**.
6. In **Task Category**, you can keep **All Tasks**.
7. In **Task**, select **Software Install**.
8. Click **Settings** in the left menu or the **Continue** button at the bottom of the window.
9. Choose a proper license. You need to activate ESET Inspect Connector with an "ESET PROTECT Enterprise" license. To learn how to manage the license for ESET Inspect On-Prem, [follow](#).
10. Choose whether you want to install ESET Inspect Connector from the repository or specify the URL

path to the installer (32-bits or 64-bits, depending on the operating system).

11. In case of Linux or macOS, skip to step 12. Fill in the **Installation parameters** field. You can use the same parameters as in [Installation from a command line](#), or you can leave it blank (it will install without Certificate Authority, and ESET Inspect Server address will be "localhost". You can change this by creating a Policy with ESET Inspect Server address and Certificate Authority. To learn how to create a policy in the ESET PROTECT On-Prem, [follow](#) or ask ESET PROTECT On-Prem Administrator to create a policy for you). Click **Finish**.

12. For Linux and macOS (if you left parameters blank for the Windows part, then for it as well), it is necessary to create a [Policy](#) to make ESET Inspect Connector communicate with ESET Inspect Server (this is not necessary for ESET Inspect):

a. In the **Settings** window, select the product "ESET Inspect Connector"

b. Fill in the **Server Address** with the ESET Inspect Server IP address.

c. Edit the **Certificate Authority** by clicking **Edit > Add > Open Certificate Authority**. Choose the certificate that was used during ESET Inspect Server installation. Click **Save**.

d. Click **Continue**.

e. Select the **Assign** button and select the computer/computers you want the policy to be applied on in the **Assign** window. Click **Finish**.

13. If the task is already created, you can rerun it on another computer or group of computers. See [Client Tasks executions](#).

Example:

The easiest way to install the connector (Windows only) through a deployment is to use these parameters:

```
✓ P_HOSTNAME="IP_OR_HOSTNAME_OF_EI_SERVER" P_IS_SERVER_ASSISTED=1
```

ESET PROTECT On-Prem macOS Deployment

From version macOS 10.14 onwards, you will receive the notification, "**Your computer is partially protected from ESET Endpoint Security for macOS. To access all ESET Endpoint Security for macOS functions, you need to allow Full disk access to ESET Endpoint Security for macOS**".

For a fully functional ESET Inspect Connector, grant full disk access:

1. Open **Preferences > Security & Privacy > Privacy**.

2. Unlock settings in the lower-left corner.

3. Scroll the left side menu and click **full disk access**.

4. In the right side menu mark the ESET Endpoint Security/ESET Endpoint Antivirus, ESET Management Agent, ESET Inspect Connector and also ESET Real-time system protection.

5. Lock your settings.

Using MDM

To allow Full disk access remotely:

- 1.Download the [.plist](#) configuration file.
- 2.Deploy the .plist configuration profile file using the MDM server.

Your computer needs to be enrolled in the MDM server to deploy configuration profiles to those computers.



You need to activate ESET Inspect Connector with an "ESET Inspect" license. To do this, contact your ESET PROTECT On-Prem Administrator or create a [Product Activation](#) task.



The ESET Inspect Connector will be visible in ESET Inspect Web Console immediately after activation and correct policy setting. In a few minutes, you should be able to view the first events sent by connectors. ESET Inspect Connector is writing error logs into the folder:

- Windows *C:\ProgramData\ESET\Inspect Connector\logs*
- macOS */Library/Application Support/ESET/eset_eia/logs*
- Linux */var/log/eset/eei/*

If you experience any other issues, follow the instructions on gathering debug data as detailed in [Troubleshooting the installation](#) topic.

ESET Inspect Connector uninstallation

Through ESET PROTECT On-Prem / ESET PROTECT

To uninstall ESET Inspect Connector for ESET Inspect, use the [Software Uninstall](#) Task in the ESET PROTECT instance.

To uninstall ESET Inspect Connector for ESET Inspect On-Prem, use the [Software Uninstall](#) Task in the ESET PROTECT On-Prem instance.

- 1.Navigate to **Tasks > New**.
- 2.In the Task creation wizard in the **Basic** section, fill in the Name and Description and select **Software uninstall** from the **Task** drop-down menu.
- 3.Select the application to uninstall from the **Uninstall** drop-down menu in the **Settings** section. Under **Package name**, click **Select package to uninstall**, select the ESET Inspect Connector you want to uninstall and click **OK**.
- 4.Under **Package version**, click **Uninstall all versions of package** to prevent problems when uninstalling different versions of ESET Inspect Connector on client computers in your network.
- 5.Select the check box next to **Automatic reboot when needed** to ensure that the uninstallation process is finished.
- 6.Click **Finish** to create the task.
- 7.Click **Create trigger** to select a Target for the task.
- 8.Click **Add Groups** and select the **All** group as the target.

9. Select the appropriate trigger and click **Finish** to execute.

Manual uninstallation

Windows

Standard windows application uninstallation processes can be used.

macOS

In the Terminal, run the command: `sudo "/Library/Application Support/ESET/ESET Inspect Connector.app/Contents/Scripts/Uninstall.command"`

Linux

In the Terminal, run the command: `sudo "/opt/eset/eei/uninstall.sh"`

Telemetry

ESET Inspect On-Prem Telemetry services collect usage information based on user behavior within the ESET Inspect Web Console to improve user experience and overall system performance.

Data collected

- Number of computers with the ESET Inspect Connector installed
- Information about the machine where the ESET Inspect Server is installed:
 - OS name and version
 - CPU model and speed
 - RAM size
 - MySQL database version and size
- Information about the machine where the ESET Inspect Connector is installed:
 - Agent version
 - OS name and version
 - RAM size
 - CPU model and speed
- Number of computers managed by ESET PROTECT
- Number of events received by the ESET Inspect Server, the processing time
- Web browser name and version in which the ESET Inspect Web Console is viewed
- Commands executed by the user in the ESET Inspect Web Console
- Report how long it takes to run purge for one partition
- Report if the purge was completed successfully or failed
- How many detections were generated from which rule
- How many detections were generated each day (week)

Due to the nature of telemetry, the IP address of the ESET Inspect Server from which the information is sent is also collected.

End User License Agreement

Effective as of January 31, 2024.

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, 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.

EULAID: EULA-PRODUCT-LG-EI; 3537.0

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 samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames (hereinafter referred to as "Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the computer and/or the platform on which the Software is installed and/or information about the operations and functionality of the Software (hereinafter referred to as "Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by LiveGrid Reputation System function which includes collection and sending of one-way hashes related to Infiltrations to Provider. This function is enabled under the Software's standard settings.

The Provider shall only use Information and Infiltrations received for analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software You are agreeing to Infiltrations and Information being sent to the Provider and You are also granting the Provider the necessary approval, as specified under the relevant legal regulations, for processing Infiltrations and Information obtained. You can deactivate these functions at any time.

EULAID: EULA-PRODUCT-LG-EI; 3537.0

Privacy Policy

The protection of personal data is of particular importance to ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We"). We want to comply with the transparency requirement as legally standardized under the EU General Data Protection Regulation ("GDPR"). To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") as a data subject about following personal data protection topics:

- Legal Basis of Personal Data Processing,
- Data Sharing and Confidentiality,

- Data Security,
- Your Rights as a Data Subject,
- Processing of Your Personal Data,
- Contact Information.

Processing of Your Personal Data

Services provided by ESET implemented in our product are provided under the terms of [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 the product [documentation](#). To make it all work, We need to collect the following information:

Server and web console

- Information concerning installation process, including platform on which our product is installed and information about the operations and functionality of our product such as hardware fingerprint, installation IDs, crash dumps, license IDs, IP address, MAC address, configuration settings of ESET product installed on server (not including data from monitored endpoint devices).
- Licensing information such as license ID and personal data such as company name, name and 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.
- Telemetry data concerning usage.

Monitored endpoint devices

- ESET product collects and locally stores information from monitoring of endpoint devices and network exclusively based on preferences, requirements and setting managed by You.
- Data from monitored endpoint devices and from network are not transferred to ESET.

We encourage You to check and review the legislation and legal requirements for data collection and processing in Your country while setting up ESET product. You might be required to notify users of monitored endpoint devices or ask for specific permission under the certain jurisdiction when You monitor and collect.

Data Sharing and Confidentiality

We do not share your data with third parties. However, ESET is a company that operates globally through affiliated companies or partners as part of our sales, service and support network. Licensing, billing and technical support information processed by ESET may be transferred to and from affiliates or partners for the purpose of fulfilling the EULA, such as providing services or support.

ESET prefers to process its data in the European Union (EU). However, depending on your location (use of our products and/or services outside the EU) and/or the service you choose, it may be necessary to transfer your data to a country outside the EU. For example, we use third-party services in connection with cloud computing. In these cases, we carefully select our service providers and ensure an appropriate level of data protection through contractual as well as technical and organizational measures. As a rule, we agree on the EU standard contractual clauses, if necessary, with supplementary contractual regulations.

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a

comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these countries does not require any special authorization or agreement.

Data Subject's Rights

The rights of every End User matter and We would like to inform you that all End Users (from any EU or any non-EU country) have the following rights guaranteed at ESET. To exercise your data subject's rights, you can contact us via support form or by e-mail at dpo@eset.sk. For identification purposes, we ask you for the following information: Name, e-mail address and - if available - license key or customer number and company affiliation. Please refrain from sending us any other personal data, such as the date of birth. We would like to point out that to be able to process your request, as well as for identification purposes, we will process your personal data.

Right to Withdraw the Consent. Right to withdraw the consent is applicable in case of processing based on consent only. If We process your personal data on the basis of your consent, you have the right to withdraw the consent at any time without giving reasons. The withdrawal of your consent is only effective for the future and does not affect the legality of the data processed before the withdrawal.

Right to Object. Right to object the processing is applicable in case of processing based on the legitimate interest of ESET or third party. If We process your personal data to protect a legitimate interest, You as the data subject have the right to object to the legitimate interest named by us and the processing of your personal data at any time. Your objection is only effective for the future and does not affect the lawfulness of the data processed before the objection. If we process your personal data for direct marketing purposes, it is not necessary to give reasons for your objection. This also applies to profiling, insofar as it is connected with such direct marketing. In all other cases, we ask you to briefly inform us about your complaints against the legitimate interest of ESET to process your personal data.

Please note that in some cases, despite your consent withdrawal or your objection processing, we are entitled to further process your personal data on the basis of another legal basis, for example, for the performance of a contract.

Right of Access. As a data subject, you have the right to obtain information about your data stored by ESET free of charge at any time.

Right to Rectification. If we inadvertently process incorrect personal data about you, you have the right to have this corrected.

Right to Erasure. As a data subject, you have the right to request the deletion or restriction of the processing of your personal data. If we process your personal data, for example, with your consent, you withdraw it and there is no other legal basis, for example, a contract, We delete your personal data immediately. Your personal data will also be deleted as soon as they are no longer required for the purposes stated for them at the end of our retention period.

Right to Restriction of Processing. If we use your personal data for the sole purpose of direct marketing and you have revoked your consent or objected to the underlying legitimate interest of ESET, We will restrict the processing of your personal data to the extent that we include your contact data in our internal black list in order to avoid unsolicited contact. Otherwise, your personal data will be deleted.

Please note that We may be required to store your data until the expiry of the retention obligations and periods issued by the legislator or supervisory authorities. Retention obligations and periods may also result from the Slovak legislation. Thereafter, the corresponding data will be routinely deleted.

Right to Data Portability. We are happy to provide You, as a data subject, with the personal data processed by

ESET in the xls format.

Right to Lodge a Complaint. As a data subject, You have a right to lodge a complaint with a supervisory authority at any time. ESET is subject to the regulation of Slovak laws and We are bound by data protection legislation as part of the European Union. The relevant data supervisory authority is The Office for Personal Data Protection of the Slovak Republic, located at Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Contact Information

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