ESET Endpoint Security

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

ESET Endpoint Security was developed by ESET, spol. s r.o.

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

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

REV. 4/12/2024

ESET Endpoint Security

ESET Endpoint Security represents a new approach to truly integrated computer security. The most recent version of the ESET LiveGrid® scanning engine, combined with our custom Firewall and Email client antispam module, utilizes speed and precision to keep your computer safe. The result is an intelligent system that is constantly on alert for attacks and malicious software endangering your computer.

ESET Endpoint Security is a complete security solution produced from our long-term effort to combine maximum protection and a minimal system footprint. The advanced technologies, based on artificial intelligence, are capable of proactively eliminating infiltration by viruses, spyware, trojan horses, worms, adware, rootkits, and other internet-borne attacks without hindering system performance or disrupting your computer.

ESET Endpoint Security is primarily designed for use on workstations in a business environment.

In the Installation section you can find help topics divided into several chapters and subchapters to provide orientation and context, including Download, Installation and Activation.

Using ESET Endpoint Security with ESET PROTECT On-Prem in an enterprise environment enables you to easily manage any number of client workstations, apply policies and rules, monitor detections and remotely configure clients from any networked computer.

The Common Questions chapter covers some of the most frequently asked questions and problems encountered.

Features and benefits

Redesigned user interface	The user interface in this version has been significantly redesigned and simplified based on the results of usability testing. All GUI wording and notifications have been carefully reviewed and the interface now provides support for right-to-left languages such as Hebrew and Arabic. Online Help is now integrated into ESET Endpoint Security and offers dynamically updated support content.
Dark mode	An extension that helps you quickly switch the screen to a dark color scheme. You can choose your preferred color scheme in User interface elements.
Antivirus and antispyware	Proactively detects and cleans more known and unknown viruses, worms, trojans and rootkits. Advanced heuristics flags even never-before-seen malware, protecting you from unknown threats and neutralizing them before they can do any harm. Web access protection and Anti-Phishing monitor communication between web browsers and remote servers (including SSL). Email client protection provides control of email communication received through the POP3(S) and IMAP(S) protocols.
Regular updates	Regularly updating the detection engine (previously known as "virus signature database") and program modules is the best way to ensure the maximum level of security on your computer.
ESET LiveGrid® (Cloud-powered Reputation)	You can check the reputation of running processes and files directly from ESET Endpoint Security.
Remote management	ESET PROTECT On-Prem enables you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location. Using the ESET PROTECT Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

Network attack protection	Analyses the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked.
Web control (ESET Endpoint Security only)	Web control enables you to block web pages that may contain potentially offensive material. In addition, employers or system administrators can prohibit access to more than 27 pre-defined website categories and over 140 subcategories.

What's new?

What's new in ESET Endpoint Security version 11

New Firewall rules editor

The Firewall rules editor has been redesigned to enable you to define Firewall rules more easily with more configuration options.

Vulnerability & Patch Management

Feature available in ESET PROTECT that regularly scans a workstation to detect any installed software vulnerable to security risks. Patch management checks if the available space matches before starting the download (default and minimal value is 2GB) and helps remediate these risks through automated software updates, keeping the devices more secure.

End of Life product statuses

ESET Endpoint Security in this version can display various Application support statuses. You can set up Application support status communication in Notifications.

Various bug fixes and performance improvements

System requirements

For seamless operation of ESET Endpoint Security, the system should meet the following hardware and software requirements (default product settings):

Processors Supported

Intel or AMD processor, 32-bit (x86) with SSE2 instruction set or 64-bit (x64), 1 GHz or higher
ARM64-based processor, 1 GHz or higher

Operating Systems

Microsoft® Windows® 11

Microsoft® Windows® 10

> For a detailed list of supported Microsoft® Windows® 10 and Microsoft® Windows® 11 versions, see the Windows Operating system support policy.

Always keep your operating system up to date.

Support for Azure Code Signing must be installed on all Windows operating systems to install or upgrade ESET products released after July 2023. More information.

ESET Endpoint Security features requirements

See the system requirements for specific ESET Endpoint Security features in the table below:

Feature	Requirements
Intel® Threat Detection Technology	See the supported processors.
Secure Browser	See the supported web browsers.
Specialized Cleaner	Non-ARM64-based processor.
Exploit Blocker	Non-ARM64-based processor.
Deep Behavioral Inspection	Non-ARM64-based processor.

The ESET Endpoint Security installer created in ESET PROTECT On-Prem supports Windows 10 Enterprise for Virtual Desktops and Windows 10 multi-session mode.

Other

- System requirements of the operating system and other software installed on the computer are fulfilled
- 0.3 GB of free system memory (see Note 1)
- 1 GB of free disk space (see Note 2)
- Minimum display resolution 1024 x 768
- Internet connection or a local area network connection to a source (see Note 3) for product updates
- Two antivirus programs running simultaneously on a single device causes inevitable system resource conflicts, such as slowing down the system to make it inoperable

Although installing and running the product on systems that do not meet these requirements might be possible, we recommend prior usability testing based on performance requirements.

(1) The product might use more memory if the memory would be otherwise unused on a heavily infected computer or when huge data lists are being imported into the product (for example, URL white lists).
(2) The disk space is needed to download the installer, install the product, keep a copy of the installation package in the program data and save product update backups to support the rollback feature. The product might use more disk space under different settings (for example, when more product update backup versions, memory dumps or large log records are stored) or on an infected computer (due to the quarantine feature). We recommend keeping enough free disk space to support operating system and ESET product updates.
(3) Although not recommended, you can update the product manually from removable media.

Supported languages

ESET Endpoint Security is available for installation and download in the following languages.

Language	Language code	LCID
English (United States)	en-US	1033

Language	Language code	LCID
Arabic (Egypt)	ar-EG	3073
Bulgarian	bg-BG	1026
Chinese Simplified	zh-CN	2052
Chinese Traditional	zh-TW	1028
Croatian	hr-HR	1050
Czech	cs-CZ	1029
Estonian	et-EE	1061
Finnish	fi-FI	1035
French (France)	fr-FR	1036
French (Canada)	fr-CA	3084
German (Germany)	de-DE	1031
Greek	el-GR	1032
*Hebrew	he-IL	1037
Hungarian	hu-HU	1038
*Indonesian	id-ID	1057
Italian	it-IT	1040
Japanese	ja-JP	1041
Kazakh	kk-KZ	1087
Korean	ko-KR	1042
*Latvian	lv-LV	1062
Lithnuanian	lt-LT	1063
Nederlands	nl-NL	1043
Norwenian	nb-NO	1044
Polish	pl-PL	1045
Portuguese (Brazil)	pt-BR	1046
Romanian	ro-RO	1048
Russian	ru-RU	1049
Spanish (Chile)	es-CL	13322
Spanish (Spain)	es-ES	3082
Swedish (Sweden)	sv-SE	1053
Slovak	sk-SK	1051
Slovenian	sl-SI	1060
Thai	th-TH	1054
Turkish	tr-TR	1055
Ukrainian (Ukraine)	uk-UA	1058
*Vietnamese	vi-VN	1066

* ESET Endpoint Security is available in this language, but Online user guide is not available (redirects to the English version).

To change the language of this Online user guide, see the language select box (in the upper-right corner).

Changelogs

Prevention

When using your computer, especially when you browse the internet, keep in mind that no antivirus system can completely eliminate the risk of detections and remote attacks. To provide maximum protection and convenience, you must use your antivirus solution correctly and adhere to several useful rules:

Update regularly

According to statistics from ESET LiveGrid®, thousands of new, unique infiltrations are created each day to bypass existing security measures and profit their authors—all at the expense of other users. The specialists at the ESET Virus Lab analyze these threats daily, and prepare and release updates to continually improve protection levels for our users. To ensure the maximum effectiveness, updates must be configured properly on your system. For more information on how to configure updates, see Update setup.

Download security patches

Malicious software authors often exploit system vulnerabilities to increase the effectiveness of spreading malicious code. With this in mind, software companies watch closely for any vulnerabilities in their applications and release security updates to eliminate potential threats regularly. It is essential to download these security updates as they are released. Microsoft Windows and web browsers, such as Microsoft Edge, are two examples for which security updates are released on a regular schedule.

Back up important data

Malware writers usually do not care about users' needs, and malicious program activity often leads to a total operating system malfunction and the loss of important data. It is essential to regularly back up your data to an external source, such as a DVD or external hard drive. This will make it far easier and faster to recover your data in the event of a system failure.

Regularly scan your computer for viruses

The detection of known and unknown viruses, worms, trojans and rootkits is handled by the real-time file system protection module. Every time you access or open a file, it is scanned for malware activity. We recommend that you run a full computer scan at least once a month because malware signatures may vary and the detection engine updates itself daily.

Follow basic security rules

The most useful and effective rule of all is always be cautious. Today, many infiltrations require user intervention to be executed and distributed. If you are mindful when opening new files, you will save considerable time and effort that could be spent cleaning infiltrations. Here are some useful guidelines:

- Do not visit suspicious websites with multiple pop-ups and flashing advertisements.
- Be careful when installing freeware programs, codec packs, etc. Only use safe programs and only visit safe internet websites.

- Be cautious when opening email attachments, specifically those from mass-mailed messages and messages from unknown senders.
- Do not use an Administrator account for everyday work on your computer.

Application support status

ESET Endpoint Security can show automated notifications or warnings to inform you about upcoming application support status changes or available application updates in several places in the main program window.

Read more about:
- End of Life policy (Business products)
- Product updates
- Security and Stability Hotfixes

The table below shows some of the examples of product statuses and notifications with actions based on categories:

Category	Notification or alert window	Update page	Help and support page
New feature or servicing update available	A new version is available An update containing important servicing fixes required by ESET Endpoint Security is available. Update now to ensure the most up-to-date protection. **Action**: Learn more	A new version of ESET Endpoint Security is available A new version of ESET Endpoint Security is available **Actions**: Update now/Enable auto-updates	A new version of ESET Endpoint Security is available. Update now to get the latest version with new features and improvements. Supported until: mm/dd/yyyy
	A servicing update is available A new version of ESET Endpoint Security is available. Update now to get the latest version with new features and improvements. **Action**: Learn more	A servicing update for ESET Endpoint Security is available Installed version number Supported until: mm/dd/yyyy **Action**: Learn more	An update containing important servicing fixes required by ESET Endpoint Security is available. Update now to ensure the most up-to-date protection. Supported until: mm/dd/yyyy
	Device restart recommended An update containing important servicing fixes required by ESET Endpoint Security is available. Update now to ensure the most up-to-date protection. **Action**: Learn more		Supported until: mm/dd/yyyy
	A critical servicing update is available An update containing critical servicing fixes required by ESET Endpoint Security is available. Update now to ensure the most up-to-date protection. **Action**: Learn more	A critical servicing update for ESET Endpoint Security is available Installed version number Supported until: mm/dd/yyyy **Action**: Learn more	An update containing critical servicing fixes required by ESET Endpoint Security is available. Update now to ensure the most up-to-date protection. Supported until: mm/dd/yyyy
	Device restart required An update to version number has been downloaded, containing important servicing and stability fixes required by your ESET Endpoint Security. Update now to ensure the most up-to-date protection. **Action**: Learn more		Supported until: mm/dd/yyyy

Category	Notification or alert window	Update page	Help and support page
Expiring support for application	Support for your installed application version ends on mm/dd/yyyy, and your device will soon lose protection. Update now to stay protected. **Action**: Update now	Installed version number/Supported until: mm/dd/yyyy **Actions**: Update now/Enable auto-updates	Support for the installed version of ESET Endpoint Security ends soon, and your computer will lose protection. Update now to stay protected. Supported until: mm/dd/yyyy
	ESET Extended Support for your installed application version ends on mm/dd/yyyy, and your device will soon lose protection. Update now to stay protected. **Action**: Update now	Installed version number/Supported until: mm/dd/yyyy **Actions**: Update now/Enable auto-updates	ESET Extended Support for the installed version of ESET Endpoint Security ends soon, and your device will lose protection. Update now to stay protected. Supported until: mm/dd/yyyy
	The installed operating system is outdated, and the support for your installed application version ends on mm/dd/yyyy. Upgrade your operating system to get the latest application update and stay protected. **Actions**: Learn more	Installed version number Supported until: mm/dd/yyyy **Action**: Learn more	Support for the installed version of ESET Endpoint Security ends soon, and your computer will lose protection. Update now to stay protected. Supported until: mm/dd/yyyy
	ESET Extended Support for the installed application version ends soon The installed operating system is outdated, and the support for your installed application version ends on mm/dd/yyyy. Upgrade your operating system to get the latest application update and stay protected. **Action**: Learn more	ESET Extended Support for the installed version of ESET Endpoint Security ends soon Installed version number Supported until: mm/dd/yyyy **Actions**: Learn more	ESET Extended Support for the installed version of ESET Endpoint Security ends soon, and your device will lose protection. Update now to stay protected. Supported until: mm/dd/yyyy

Category	Notification or alert window	Update page	Help and support page
Application version no longer supported	⚠ The installed application version is no longer supported Support for your installed application version has ended, and your device may not be protected. Update now to get protection. **Action**: Update now	⚠ The installed version of ESET Endpoint Security is no longer supported Installed version number/Supported until: mm/dd/yyyy **Actions**: Update now/Enable auto-updates	⚠ Supported until: mm/dd/yyyy
	⚠ The installed application version is no longer supported The installed operating system is outdated, and the support for your installed application version has ended. Your computer is not protected. Upgrade your operating system to receive the latest application update and get protection. **Action**: Learn more	⚠ The installed version of ESET Endpoint Security is no longer supported Installed version number Supported until: mm/dd/yyyy **Action**: Learn more	⚠ Support for the installed version of ESET Endpoint Security has ended, and your computer is not protected. Update now to get protection. Supported until: mm/dd/yyyy
Operating system update required	⚠ The installed operating system is outdated The installed operating system is outdated. Upgrade your operating system to get the latest application update and stay protected. **Action**: Learn more	✓ ESET Endpoint Security Installed version number	Supported until: mm/dd/yyyy

ℹ Customers who order ESET extended Support for the affected application version will see the regular yellow application status **Support for your installed application version ends soon** before the End of Life date. After this date, the product will display that it is supported (green application status), and later, when the Extended Support end is near, the yellow application status will reappear with the notification **ESET Extended Support for your installed application version ends soon**.

Help pages

Welcome to the ESET Endpoint Security user guide. The information provided here will introduce you to your product and help you make your computer more secure.

Getting started

Before you start using ESET Endpoint Security note that the product can be managed remotely using ESET PROTECT On-Prem. We also recommend that you familiarize yourself with the various types of detections and remote attacks you might encounter when using your computer.

See new features to learn about features introduced in this version of ESET Endpoint Security. We have also

prepared a guide to help you setup and customize the basic settings of ESET Endpoint Security.

How to use ESET Endpoint Security Help pages

Help topics are divided into several chapters and subchapters to provide orientation and context. You can find related information by browsing the help pages structure.

Press **F1** to learn more about any window in the program. The help page related to the window you are currently viewing will be displayed.

You can search the Help pages by keyword or by typing words or phrases. The difference between these two methods is that a keyword may be logically related to help pages that do not contain that specific keyword in the text. Searching by words and phrases will search the content of all pages and display only those containing the searched word or phrase.

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

A note is just a short observation. Although you can omit it, notes can provide valuable information, such as specific features or a link to some related topic.

This requires your attention that we encourage you not to skip over. Usually, it provides non-critical but significant information.

This is information that requires extra attention and caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.

This is a use case or a practical example that aims to help you understand how a certain function or feature can be used.

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

Online Help is the primary source of help content. The latest version of Online Help will automatically be displayed when you have a working internet connection.

Documentation for endpoints managed remotely

ESET business products as well as ESET Endpoint Security can be managed remotely on client workstations, servers and mobile devices in a networked environment from one central location. System administrators who manage more than 10 client workstations may consider deploying one of the ESET remote management tools to deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers from one central location.

ESET remote management tools

ESET Endpoint Security can be managed remotely by either ESET PROTECT On-Prem or ESET PROTECT.

- Introduction to ESET PROTECT On-Prem.
- Introduction to ESET PROTECT.

- ESET PROTECT HUB—Central gateway to the ESET PROTECT On-Prem unified security platform. It provides centralized identity, subscription and user management for all ESET platform modules. See ESET PROTECT On-Prem License Management for instructions to activate your product. ESET PROTECT HUB will replace ESET Business Account and ESET MSP Administrator completely.

- ESET Business Account—License management portal for ESET business products. See ESET PROTECT On-Prem License Management for instructions to activate your product, or see the ESET Business Account Online Help for more information about using ESET Business Account. If you already have an ESET-issued Username and Password that you want to convert to a license key, see Convert legacy license credentials.

Additional security products

- ESET Inspect—Is a comprehensive Endpoint Detection and Response system that includes features, such as incident detection, incident management and response, data collection, indicators of compromise detection, anomaly detection, behavior detection and policy violations.
- ESET Endpoint Encryption—Is a comprehensive security application designed to protect your data at rest and in transit. Using ESET Endpoint Encryption, you can encrypt files, folders and emails or create encrypted virtual disks, compress archives and include a desktop shredder for secure file deletion.

Third-party remote management tools

- Remote monitoring and management (RMM).

Best practices

- Connect all endpoints with ESET Endpoint Security to ESET PROTECT On-Prem.
- Protect the Advanced setup settings on connected client computers to avoid unauthorized modifications.
- Apply a recommended policy to enforce available security features.
- Minimize the user interface to reduce or limit user interaction with ESET Endpoint Security.

How to guides

- How to use Override mode.
- How to deploy ESET Endpoint Security using GPO or SCCM.

Introduction to ESET PROTECT On-Prem

ESET PROTECT On-Prem allows you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location.

Using the ESET PROTECT On-Prem Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers. See ESET PROTECT On-Prem architecture and infrastructure elements overview, Getting started with ESET PROTECT On-

Prem Web Console and Supported Desktop Provisioning Environments.

ESET PROTECT On-Prem is made up of the following components:

- ESET PROTECT On-Prem Server—Handles communication with Agents, and collects and stores application data in the database. ESET PROTECT On-Prem Server can be installed on Windows and Linux servers, and also comes as a Virtual Appliance.
- ESET PROTECT On-Prem Web Console—Is the primary interface that enables you to manage client computers in your environment. It displays a status overview of clients on your network and enables you to deploy ESET solutions to unmanaged computers remotely. After you install ESET PROTECT On-Prem Server, you can access the Web Console using your web browser. If you choose to make the web server available via the internet, you can use ESET PROTECT On-Prem from any place or device with an internet connection.
- ESET Management Agent—Facilitates communication between the ESET PROTECT On-Prem Server and client computers. The Agent must be installed on a client computer to establish communication between that computer and the ESET PROTECT On-Prem Server. Because it is located on a client computer and can store multiple security scenarios, the ESET Management Agent significantly lowers reaction time to new detections. Using ESET PROTECT On-Prem Web Console, you can deploy the ESET Management Agent to unmanaged computers identified by Active Directory or ESET RD Sensor. If necessary, you can also manually install the ESET Management Agent on client computers.
- ESET Rogue Detection Sensor—Detects unmanaged computers on your network and sends their information to the ESET PROTECT On-Prem Server. This enables you to manage new client computers in ESET PROTECT On-Prem without needing to manually search and add them. The Rogue Detection Sensor remembers computers that have been discovered and will not send the same information twice.
- ESET Bridge—Is a service that can be used in combination with ESET PROTECT On-Prem to:
    - Distribute updates to client computers and installation packages to the ESET Management Agent.
    - Forward communication from ESET Management Agents to the ESET PROTECT On-Prem Server.
- Mobile Device Connector—Is a component for Mobile Device Management with ESET PROTECT On-Prem, permitting you to manage mobile devices (Android and iOS) and administer ESET Endpoint Security for Android.
- ESET PROTECT On-Prem Virtual Appliance—Is intended for users who want to run ESET PROTECT On-Prem in a virtualized environment.
- ESET PROTECT On-Prem Virtual Agent Host—Is a component of ESET PROTECT On-Prem that virtualizes agent entities to manage agent-less virtual machines. This solution enables automation, dynamic group utilization and the same level of task management as ESET Management Agent on physical computers. The Virtual Agent collects information from virtual machines and sends it to the ESET PROTECT On-Prem Server.
- Mirror Tool—Is necessary for offline module updates. If your client computers do not have an internet connection, you can use the Mirror Tool to download update files from ESET update servers and store them locally.
- ESET Remote Deployment Tool—Deploys all-in-one packages created in the <%PRODUCT%> Web Console. It is a convenient way to distribute ESET Management Agent with an ESET product on computers over a network.

For more information, see the ESET PROTECT On-Prem Online Help.

Introduction to ESET PROTECT

ESET PROTECT enables you to manage ESET products on workstations and servers in a networked environment from one central location without the requirement to have a physical or virtual server like for ESET PROTECT On-Prem. Using the (ESET PROTECT Web Console), you can deploy ESET solutions, manage tasks, enforce security

policies, monitor system status and quickly respond to problems or threats on remote computers.

ESET PROTECT is made up of the following components:

- ESET PROTECT Instance—Handles communication with Agents, and collects and stores application data in the database.
- ESET PROTECT Web Console—Is the primary interface that enables you to manage client computers in your environment. It displays a status overview of clients on your network and enables you to deploy ESET solutions to unmanaged computers remotely. You can use ESET PROTECT from any place or device with an internet connection.
- ESET Management Agent—Facilitates communication between the ESET PROTECT and client computers. The Agent must be installed on a client computer to establish communication between that computer and the ESET PROTECT. Because it is located on a client computer and can store multiple security scenarios, the ESET Management Agent significantly lowers reaction time to new detections. Using ESET PROTECT Web Console, you can deploy the ESET Management Agent to unmanaged computers. If necessary, you can also manually install the ESET Management Agent on client computers.
- ESET Bridge—Is a service that can be used in combination with ESET PROTECT to:
    - Distribute updates to client computers and installation packages to the ESET Management Agent.
    - Forward communication from ESET Management Agents to ESET PROTECT.
- Mobile Device Management—Is a component for Mobile Device Management with ESET PROTECT, permitting you to manage mobile devices (Android and iOS) and administer ESET Endpoint Security for Android.
- Vulnerability & Patch Management—Feature available in ESET PROTECT that regularly scans a workstation to detect any installed software that could be vulnerable to security risks. Patch management helps remediate these risks through automated software updates, keeping the devices more secure.

For more information, see the ESET PROTECT Online Help.

Password protected settings

To provide maximum security for your system, ESET Endpoint Security needs to be configured correctly. Any unqualified change or setting may result in lowering the client security and level of protection. To limit user access to advanced settings, an administrator can password protect the settings.

The administrator can create a policy to password protect the Advanced setup settings for ESET Endpoint Security on connected client computers. To create a new policy:

1. In the ESET PROTECT On-Prem Web Console, click **Policies** in the left-hand main menu.
2. Click **New Policy**.
3. Name your new policy and optionally, give it a short description. Click the **Continue** button.
4. From the list of products, select **ESET Endpoint for Windows**.
5. Click **User interface** in the **Settings** list and expand **Access setup**.
6. According to a version of ESET Endpoint Security, click the toggle to enable **Password to protect settings**. Note that ESET Endpoint products version 7 and later offer enhanced protection. If you have both version 7 and later and version 6 of Endpoint products in the network, we recommend creating two separate policies with different passwords for each version.
7. In the notification window, create a new password, confirm it and click **OK**. Click **Continue**.
8. Assign the policy to clients. Click **Assign** and select the computers or groups of computers to password protect. Click **OK** to confirm.

9. Check that all desired client computers are in the target list and click **Continue**.
10. Review the policy settings in the summary and click **Finish** to save your new policy.

What are policies

The administrator can push specific configurations to ESET products running on client computers using policies from the ESET PROTECT On-Prem Web Console. A policy can be applied directly to individual computers and to groups of computers. You can also assign multiple policies to a computer or a group.

A user must have the following permissions to create a new policy: **Read** permission to read the list of policies, **Use** permission to assign policies to target computers and **Write** permission to create, modify or edit policies.

Policies are applied in the order of Static Groups. For Dynamic Groups, policies are applied to child Dynamic Groups first. This enables you to apply policies with higher impact to the top of the Group tree, and more specific policies to subgroups. Using flags, an ESET Endpoint Security user with access to groups located higher in the tree can override the policies of lower groups. The algorithm is explained in ESET PROTECT On-Prem Online user guide.

> We recommend to assign more generic policies (for example, the update server policy) to higher groups within the group tree. More specific policies (for example, device control settings) should be assigned deeper in the group tree. The lower policy usually overrides the settings of the upper policies when merged (unless defined otherwise using policy flags).

Merging policies

A policy applied to a client is usually the result of multiple policies being merged into one final policy. Policies are merged one by one. When merging policies, the general rule is that the later policy always replaces the settings set by the former one. To change this behavior, you can use policy flags (Available for each setting).

When creating policies, you will notice that some settings have an additional rule (replace/append/prepend) that you can configure.

- **Replace**—the whole list is replaced, adds new values and removes all previous one.
- **Append**—items are added to the bottom of the currently applied list (must be another policy, the local list is always overwritten).
- **Prepend**—items are added to the top of the list (the local list is overwritten).

ESET Endpoint Security supports merging of local settings with the remote policies in a new way. If the setting is a list (for example a list of blocked websites) and remote policy conflicts with an existing local setting, the remote policy overwrites it. You can choose how to combine local and remote lists by selecting the different merging rules for:

- Merging settings for remote policies.
- Merging of remote and local policies—local settings with the resulting remote policy.

To learn more about merging policies, follow the ESET PROTECT On-Prem Online user guide and see the example.

How flags work

The policy that is applied to a client computer is usually the result of multiple policies being merged into one final policy. When merging policies, you can adjust the expected behavior of the final policy, due to the order of applied policies, by using policy flags. Flags define how the policy will handle a specific setting.

For each setting, you can select one of the following flags:

Not apply	Any setting with this flag is not set by the policy. Since the setting is not set by the policy, it can be changed by other policies applied later.
Apply	Settings with the **Apply** flag will be applied to the client computer. However, when merging policies, it can be overwritten by other policies applied later. When a policy is sent to a client computer containing settings marked with this flag, those settings will change the local configuration of the client computer. Since the setting is not forced, it can still be changed by other policies applied later.
Force	Settings with the **Force** flag have priority and cannot be overwritten by any policy applied later (even if it also has a **Force** flag). This assures that other policies applied later will not be able to change this setting during merging. When a policy is sent to a client computer containing settings marked with this flag, those settings will change the local configuration of the client computer.

Scenario: The *Administrator* wants to allow user *John* to create or edit policies in his home group and see all policies created by the *Administrator* including Policies that have Force flags. The *Administrator* wants *John* to be able to see all policies, but not edit existing policies created by *Administrator*. *John* can only create or edit policies within his Home Group, San Diego.
Solution: *Administrator* has to follow these steps:
Create custom static groups and permission sets
1. Create a new Static Group called *San Diego*.
2. Create a new Permission set called *Policy – All John* with access to the Static Group *All* and with **Read** permission for **Policies**.
3. Create a new Permission set called *Policy John* with access to Static Group *San Diego*, with functionality access **Write** permission for **Group & Computers** and **Policies**. This permission set allows *John* to create or edit policies in his Home Group *San Diego*.
4. Create a new user *John* and in the **Permission Sets** section select *Policy – All John* and *Policy John*.

Create policies
5. Create a new policy *All- Enable Firewall*, expand the **Settings** section, select **ESET Endpoint for Windows**, navigate to **Personal Firewall** > **Basic** and apply all settings by **Force** flag. Expand the **Assign** section and select the Static Group *All*.
6. Create a new policy *John Group- Enable Firewall*, expand the **Setting** section, select **ESET Endpoint for Windows**, navigate to **Personal Firewall** > **Basic** and apply all settings by **Apply** flag. Expand the **Assign** section and select Static Group *San Diego*.

Result
The Policies created by *Administrator* will be applied first since **Force** flags were applied to the policy settings. Settings with the Force flag applied have priority and cannot be overwritten by another policy applied later. The policies that are created by user *John* will be applied after the policies created by the Administrator.
To see the final policy order, navigate to **More** > **Groups** > **San Diego**. Select the computer and select **Show details**. In the **Configuration** section, click **Applied policies**.

Installation

There are several ESET Endpoint Security installation methods on a client workstation, unless you deploy ESET Endpoint Security remotely to client workstations via ESET PROTECT On-Prem or ESET PROTECT.

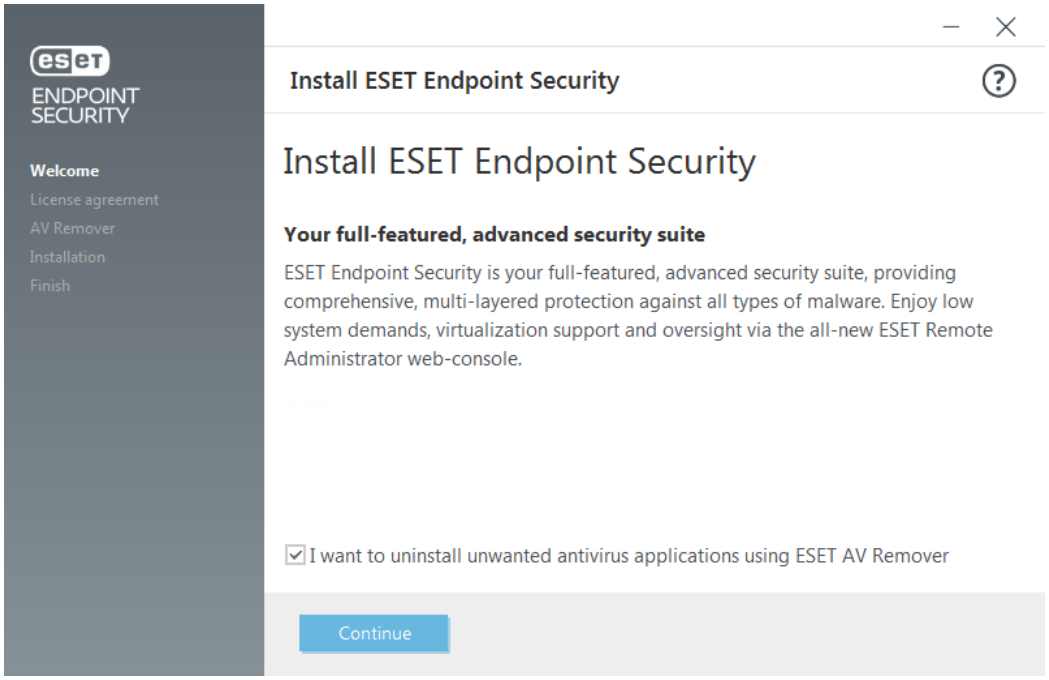
You can downgrade from ESET Endpoint Security to ESET Endpoint Antivirus by running the ESET Endpoint Antivirus installer with ESET Endpoint Security already installed. However, you must install the same or later version.

Method	Purpose	Download link
Installation with ESET AV Remover	The ESET AV Remover tool will help you to remove almost any antivirus software previously installed on your system before proceeding with installation.	Download 64-bit Download 32-bit
Installation (.exe)	Installation process without ESET AV Remover.	Download 64-bit Download 32-bit
Installation (.msi)	In business environments, the .msi installer is the preferred installation package. This is mainly due to offline and remote deployments that use various tools such as ESET PROTECT On-Prem.	Download 64-bit Download 32-bit
Command-line installation	ESET Endpoint Security can be installed locally using command-line or remotely using a client task from ESET PROTECT On-Prem.	N/A
Deployment using GPO or SCCM	Use management tools such as GPO or SCCM to deploy ESET Management Agent and ESET Endpoint Security to client workstations.	N/A
Deployment using RMM tools	ESET DEM plugins for the Remote Management and Monitoring (RMM) tool enables you to deploy ESET Endpoint Security to client workstations.	N/A

ESET Endpoint Security is available in more than 30 languages.

Installation with ESET AV Remover

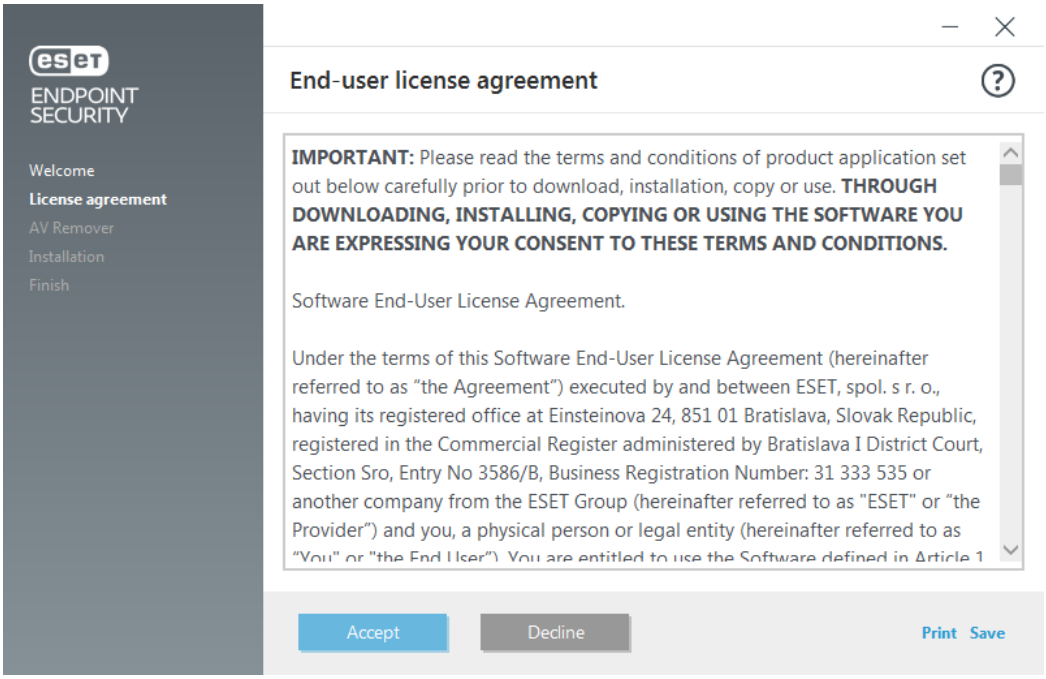
Before you continue with the installation process, it is important that you uninstall any existing security application on the computer. Select the check box next to **I want to uninstall unwanted antivirus applications using ESET AV Remover** to have ESET AV Remover scan your system and remove any supported security applications. Leave the check box deselected and click **Continue** to install ESET Endpoint Security without running ESET AV Remover.



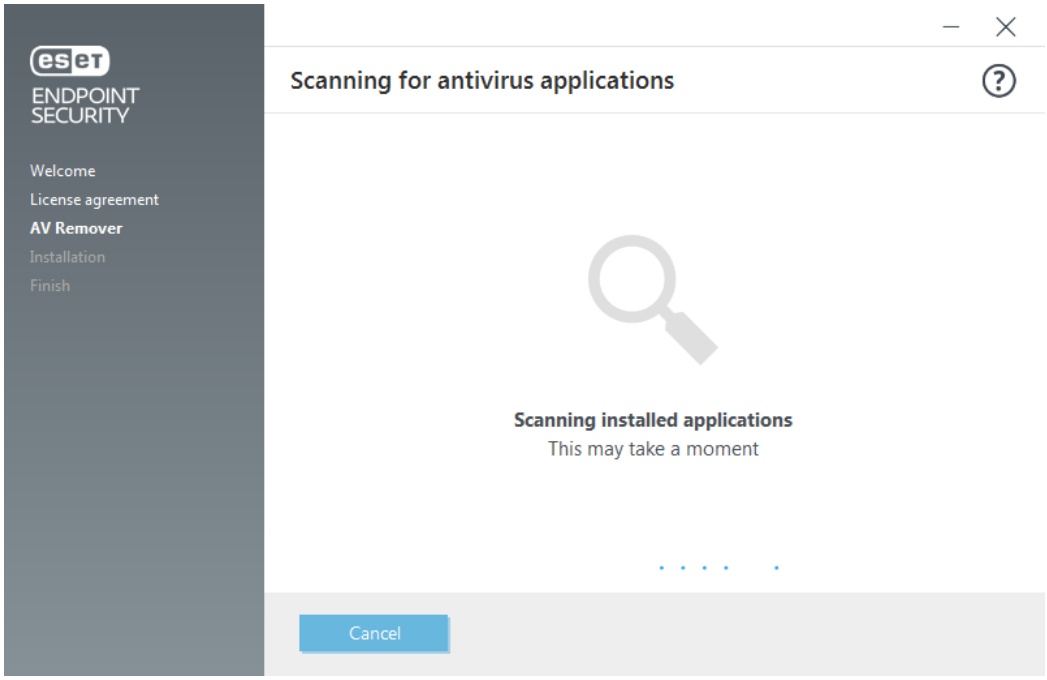
ESET AV Remover

The ESET AV Remover tool will help you to remove almost any antivirus software previously installed on your system. Follow the instructions below to remove an existing antivirus program using ESET AV Remover:

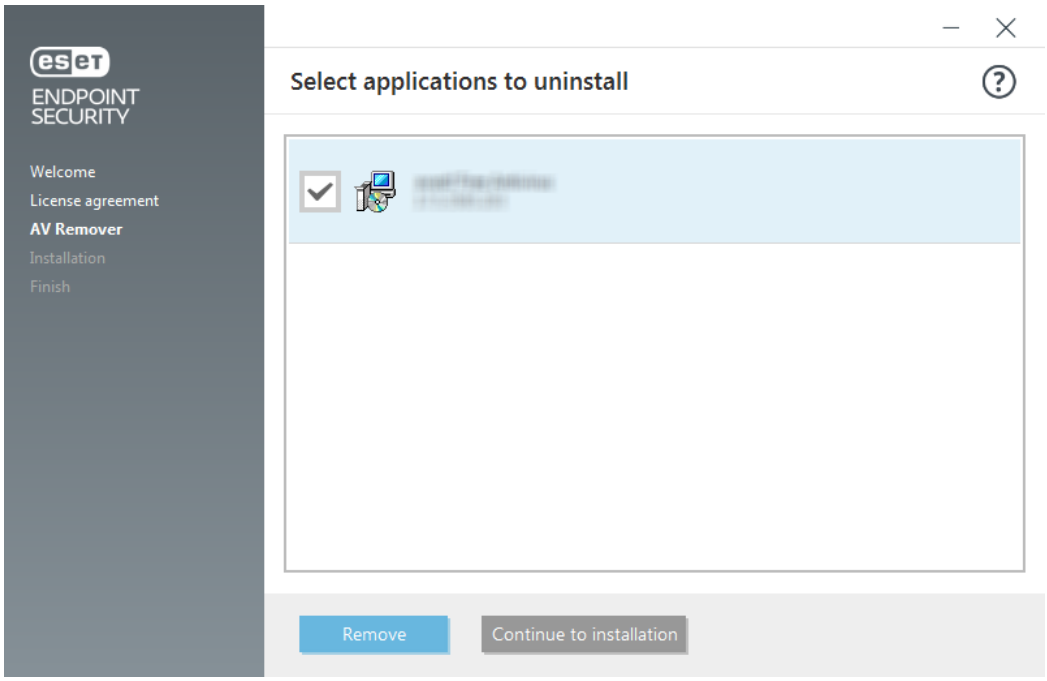
1. To view a list of antivirus software that ESET AV Remover can remove, visit this ESET Knowledgebase article.
2. Read the End-User License Agreement and click **Accept** to acknowledge your acceptance. Clicking **Decline** will continue to installation of ESET Endpoint Security without removal of existing security application on the computer.



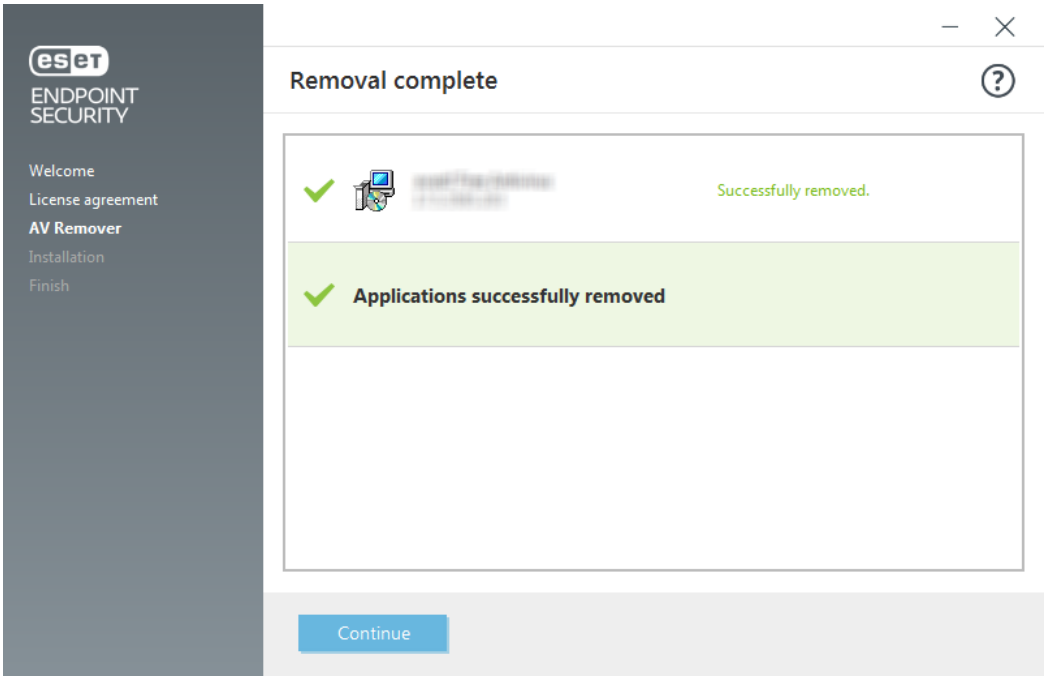
2. ESET AV Remover will begin searching your system for antivirus software.



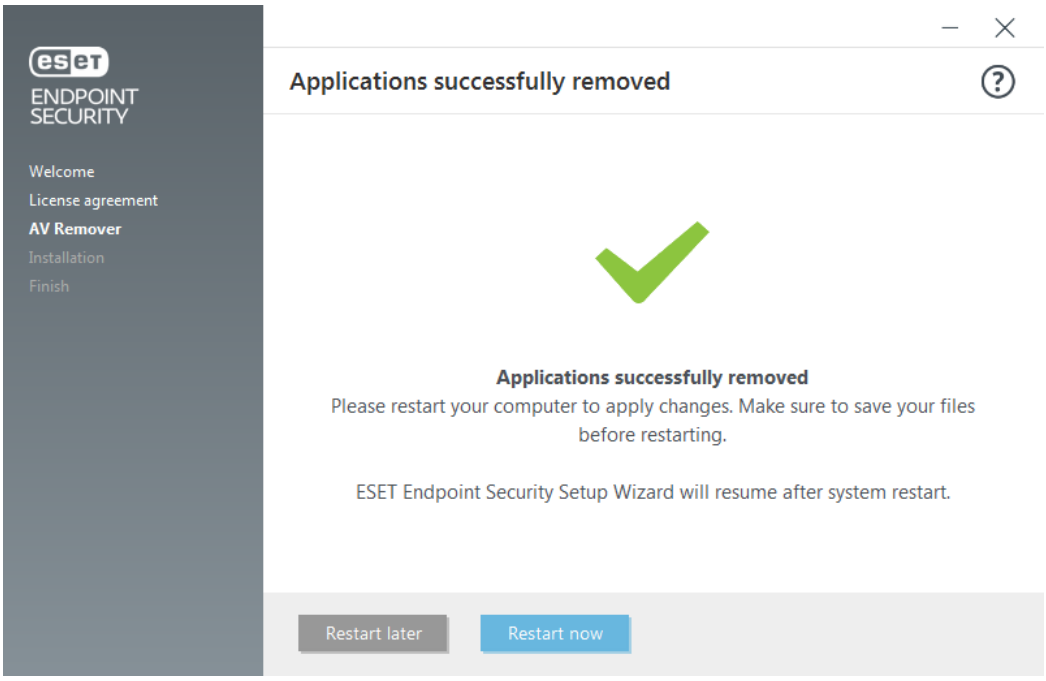
2. Select any listed antivirus applications and click **Remove**. Removal may take a moment.



2. When removal is successful, click **Continue**.



6. Restart your computer to apply changes and continue with installation of ESET Endpoint Security. If uninstallation is unsuccessful, see the Uninstallation with ESET AV Remover ended with an error section of this guide.



Uninstallation using ESET AV Remover ended with error

If you are not able to remove an antivirus program using ESET AV Remover, you will receive a notification that the application you are trying to remove might not be supported by ESET AV Remover. Visit the list of supported products or uninstallers for common Windows antivirus software on ESET Knowledgebase to see if this specific program can be removed.

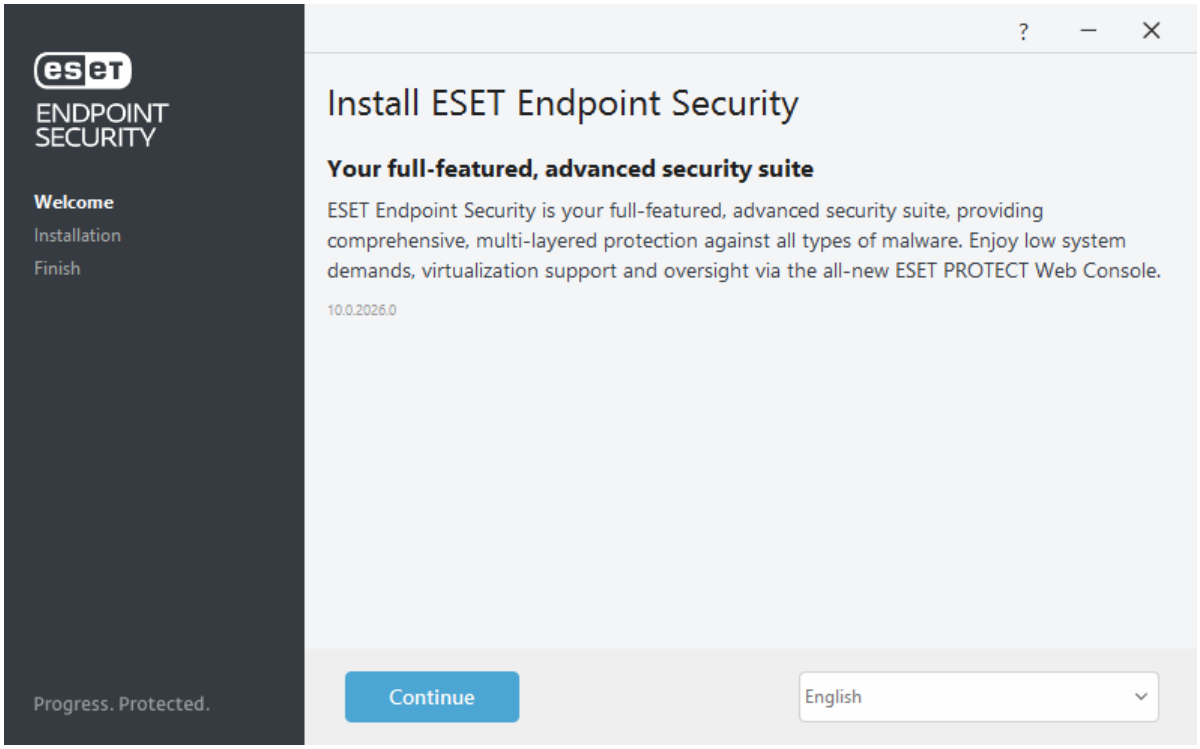
When the uninstallation of the security product was unsuccessful or some of its component was uninstalled partially, you are prompted to **Restart and rescan**. Confirm UAC after startup and continue with the scanning and uninstallation process.

If necessary, contact ESET Technical Support to open a support request and have the **AppRemover.log** file available to assist ESET Technicians. The **AppRemover.log** file is located in the **eset** folder. Browse to *%TEMP%* in Windows Explorer to access this folder. ESET Technical Support will respond as quickly as possible to help resolve your issue.

Installation (.exe)

When you launch the .exe installer, the Installation Wizard will guide you through the installation process.

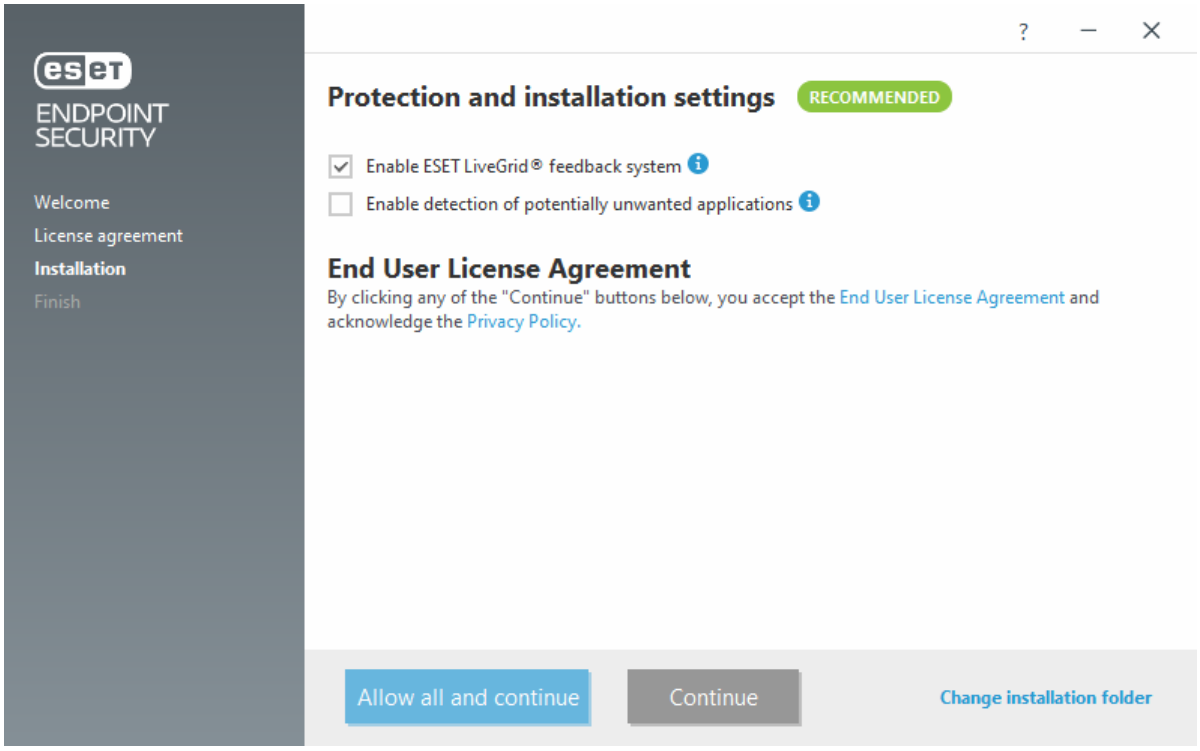
Ensure that no other antivirus programs are installed on your computer. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system. See our knowledgebase article for a list of uninstaller tools for common antivirus software (available in English and several other languages).



1. Select your preference for the following features, read the End User License Agreement and the Privacy Policy and click **Continue**, or click **Allow all and continue** to enable all features:

- ESET LiveGrid® feedback system
- Detection of potentially unwanted applications

By clicking **Continue** or **Allow all and continue**, you accept the End User License Agreement and acknowledge the Privacy Policy. You can install ESET Endpoint Security to a specific folder by clicking Change installation folder.



2. After installation is complete, you will be prompted to activate ESET Endpoint Security.

Change installation folder (.exe)

You can **Change installation folder** during the installation. Select a location for the ESET Endpoint Security installation. By default, the program installs to the following directory:

C:\Program Files\ESET\ESET Security

You can specify a location for program modules and data. By default, they are installed to the following directories:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Click **Browse** to change these locations (not recommended).

Click **Back** and then continue with the installation process.

Installation (.msi)

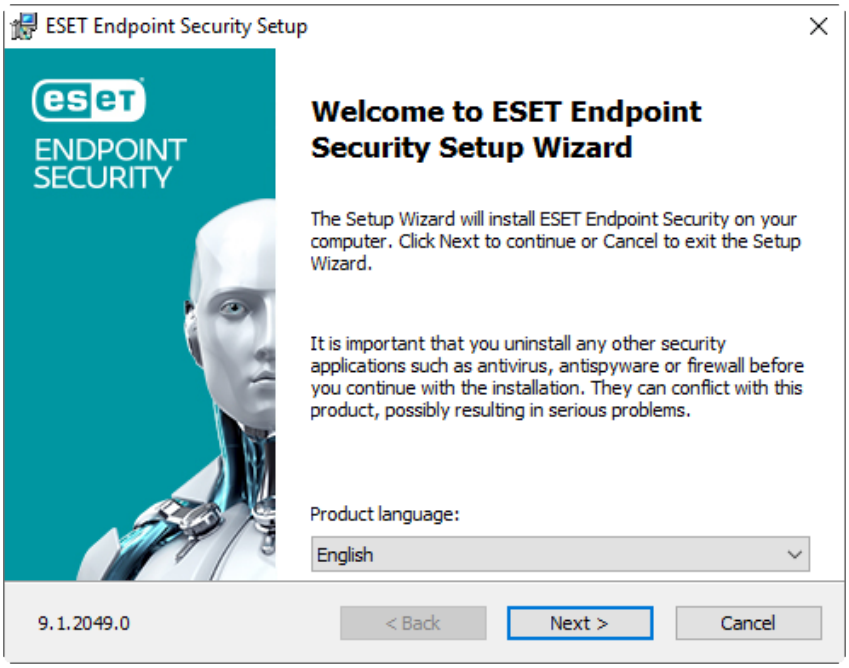
When you launch the .msi installer, the Installation Wizard will guide you through the installation process.

In business environments, the .msi installer is the preferred installation package. This is mainly due to offline and remote deployments that use various tools such as ESET PROTECT On-Prem.

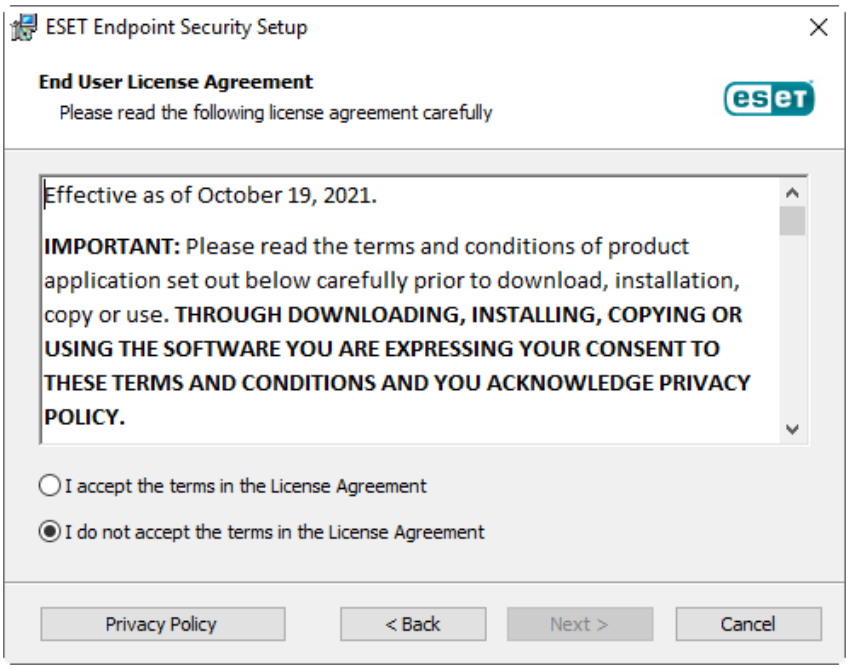
Ensure that no other antivirus programs are installed on your computer. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system. See our knowledgebase article for a list of uninstaller tools for common antivirus software (available in English and several other languages).

The ESET Endpoint Security installer created in ESET PROTECT On-Prem supports Windows 10 Enterprise for Virtual Desktops and Windows 10 multi-session mode.

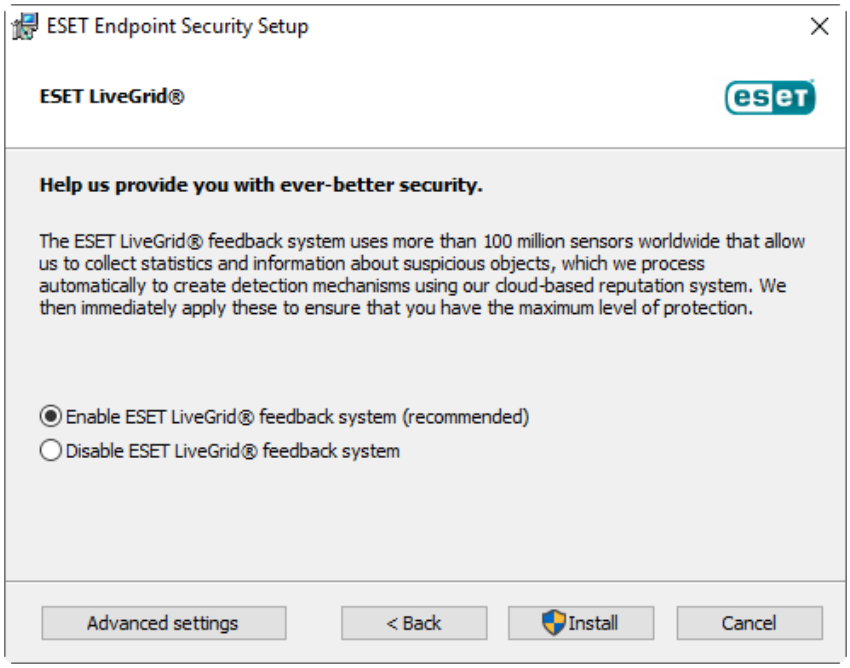
1. Select a desired language and click **Next**.



2. Read the End User License Agreement and click **I Accept the terms in the License Agreement** to acknowledge your acceptance of the End-User License Agreement. Click **Next** after you accept the terms to continue with installation.



3. Select your preference for the ESET LiveGrid® feedback system. ESET LiveGrid® helps ensure that ESET is immediately and continuously informed about new infiltrations, enabling us to protect our customers better. The system enables you to submit new threats to the ESET Virus Lab, where they are analyzed, processed and added to the detection engine. Click **Advanced settings** to configure additional installation parameters.



4. The final step is to confirm installation by clicking **Install**. After installation is complete, you will be prompted to activate ESET Endpoint Security.

Advanced installation (.msi)

Advanced installation enables you to customize installation parameters not available when performing a typical installation.

1. You can **Change installation folder** during the installation. Select a location for the ESET Endpoint Security installation. By default, the program installs to the following directories:

C:\Program Files\ESET\ESET Security

You can specify a location for program modules and data. By default, they are installed to the following directories:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Click **Browse** to change these locations (not recommended).

2. Select which product components will be installed. You can select your preference for the computer scan and all protections available. The Update mirror component can be used to update other computers on your network. Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems using a locally installed agent that can be accessed by a management service provider.
3. Click **Install** to start the installation process.

Minimal modules installation

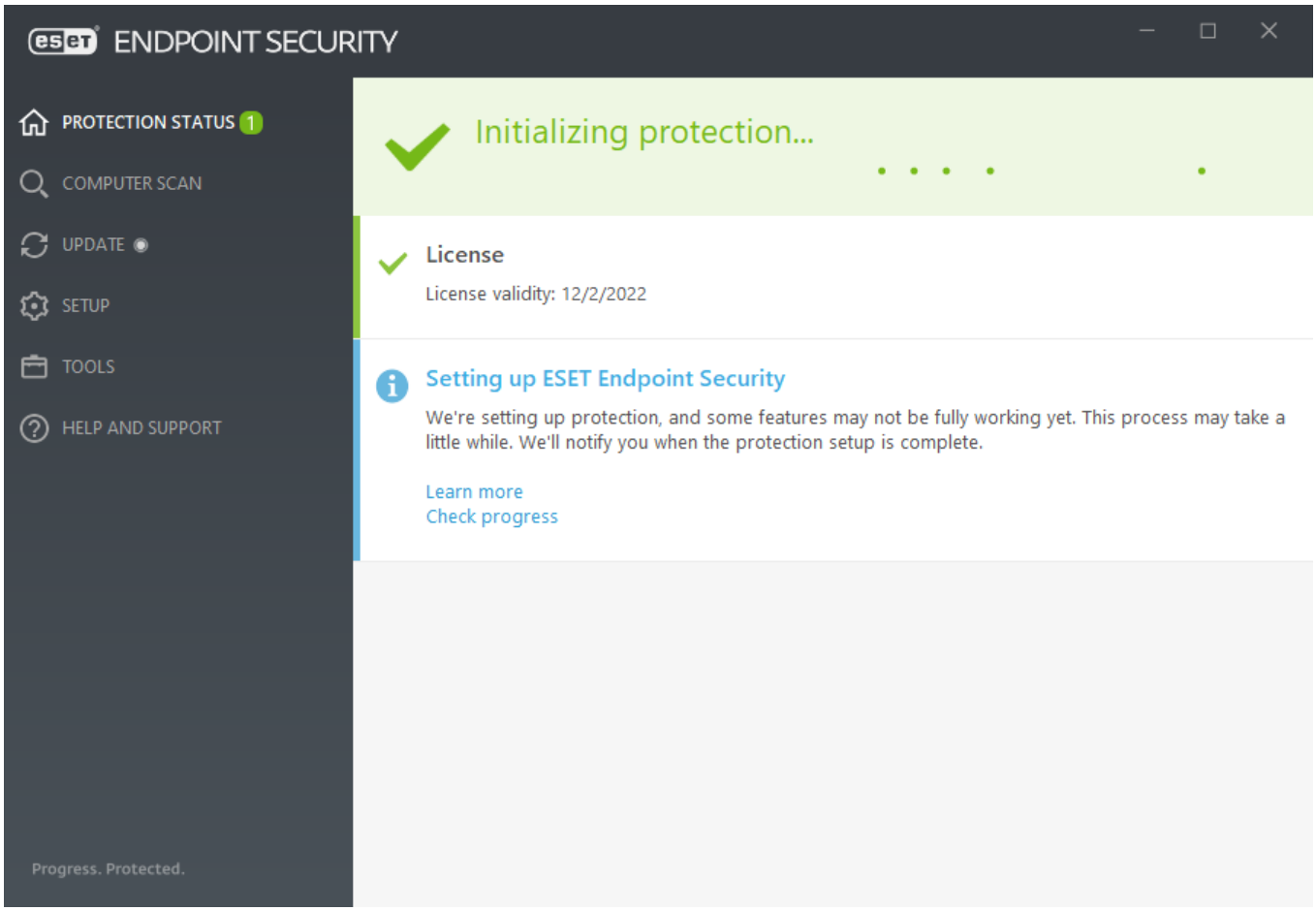
To reduce network traffic related to the size of the installer and save resources, ESET product comes with a minimal modules installer. The installer contains only essential modules, and all other modules will download during the initial module update after product activation. The main advantage is to have a significantly smaller

installer, and ESET Endpoint Security downloads only the latest application modules when you activate the product.

The minimal module installer still contains the following modules:

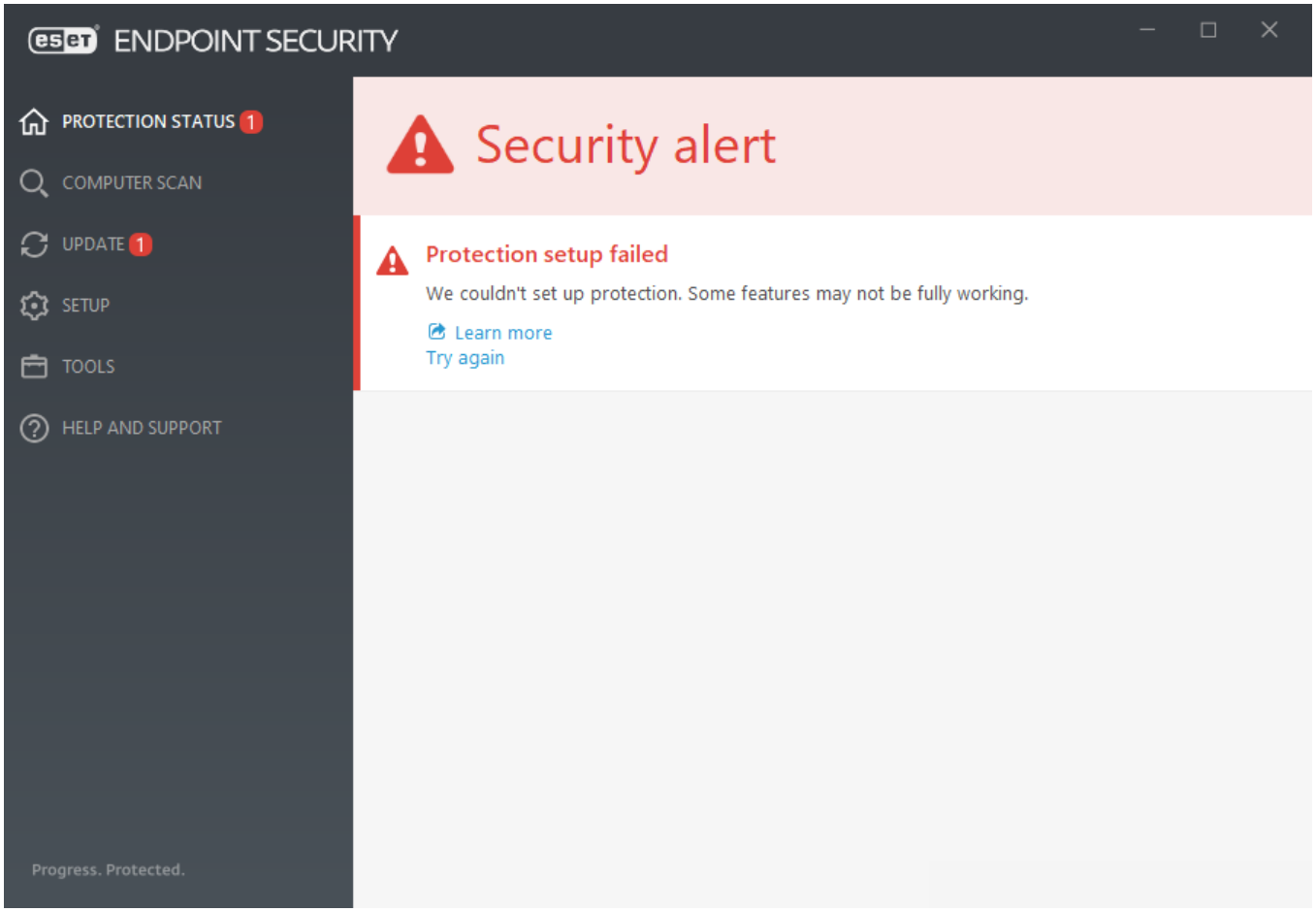
- Loaders
- Direct Cloud communication
- Translation support
- Configuration
- SSL

After the product activation, you will see the **Initializing protection** status that informs you about features initializing.



In case of a problem with module downloads (for example, proxy settings, no network, etc.), a warning application status **Attention required** is displayed. In the main program window, click **Update** > **Check for updates** to start the process again.

After several unsuccessful attempts, a red application status **Protection setup failed** is displayed. Click Try again to start the protection setup again. If the initialization process fails and you are still unable to download modules, download full MSI installers.



If your client computers do not have an internet connection or work offline and need updates, use the following methods to download update files from ESET update servers:

- Updating from the Mirror
- Using Mirror Tool

Command-line installation

You can install ESET Endpoint Security locally using the command-line or you can install remotely using a client task from ESET PROTECT On-Prem.

Supported parameters

APPDIR=<path>

- Path—Valid directory path.
- Application installation directory.

APPDATADIR=<path>

- Path—Valid directory path.
- Application Data installation directory.

MODULEDIR=<path>

- Path—Valid directory path.
- Module installation directory.

ADDLOCAL=<list>

- Component installation—list of non-mandatory features to be installed locally.
- Usage with ESET .msi packages: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- For more information about the **ADDLOCAL** property see http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<list>

- The ADDEXCLUDE list is a comma-separated list of all feature names not to be installed, as a replacement for the obsolete REMOVE.
- When selecting a feature not to install, then the whole path (i.e., all its sub-features) and related invisible features must be explicitly included in the list.
- Usage with ESET .msi packages: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> **ADDEXCLUDE** cannot be used together with **ADDLOCAL**.

See documentation for the **msiexec** version used for the appropriate command line switches.

Rules

- The **ADDLOCAL** list is a comma separated list of all feature names to be installed.
- When selecting a feature to install, the whole path (all parent features) must be explicitly included in the list.
- See additional rules for correct usage.

Components and features

> Component installation using ADDLOCAL/ADDEXCLUDE parameters will not work with ESET Endpoint Antivirus.

The features are divided into 4 categories:

- **Mandatory**—the feature will always be installed.
- **Optional**—the feature can be deselected so that it is not installed.
- **Invisible**—logical feature that is mandatory for other features to work properly.
- **Placeholder**—feature with no effect on the product, but must be listed with sub-features.

The feature set of ESET Endpoint Security is following:

Description	Feature Name	Feature Parent	Presence
Base program components	`Computer`		Placeholder
Detection engine	`Antivirus`	`Computer`	Mandatory
Detection engine / Malware scans	`Scan`	`Computer`	Mandatory
Detection engine / Real-time file system protection	`RealtimeProtection`	`Computer`	Mandatory
Detection engine / Malware scans / Document protection	`DocumentProtection`	`Antivirus`	Optional
Device control	`DeviceControl`	`Computer`	Optional

Description	Feature Name	Feature Parent	Presence
Network protection	Network		Placeholder
Network protection / Firewall	Firewall	Network	Optional
Network protection / Network attack protection / ...	IdsAndBotnetProtection	Network	Optional
Secure Browser	OnlinePaymentProtection	WebAndEmail	Optional
Web and email	WebAndEmail		Placeholder
Web and email / Protocol filtering	ProtocolFiltering	WebAndEmail	Invisible
Web and email / Web access protection	WebAccessProtection	WebAndEmail	Optional
Web and email / Email client protection	EmailClientProtection	WebAndEmail	Optional
Web and email / Email client protection / Email clients	MailPlugins	EmailClientProtection	Invisible
Web and email / Email client protection / Email client antispam	Antispam	EmailClientProtection	Optional
Web and email / Web control	WebControl	WebAndEmail	Optional
Tools / ESET RMM	Rmm		Optional
Update / Profiles / Update mirror	UpdateMirror		Optional
ESET Inspect plugin	EnterpriseInspector		Invisible

Group feature set:

Description	Feature Name	Feature Presence
All mandatory features	_Base	Invisible
All available features	ALL	Invisible

Additional rules

- If any of the **WebAndEmail** features are selected for installation, the invisible **ProtocolFiltering** feature must be included in the list.
- Names of all the features are case sensitive, for example UpdateMirror is not equal to UPDATEMIRROR.

List of configuration properties

Property	Value	Feature
CFG_POTENTIALLYUNWANTED_ENABLED=	0—Disabled 1—Enabled	PUA detection
CFG_LIVEGRID_ENABLED=	See below	See the LiveGrid property below
FIRSTSCAN_ENABLE=	0—Disabled 1—Enabled	Schedule and run a Computer scan after installation
CFG_PROXY_ENABLED=	0—Disabled 1—Enabled	Proxy server settings
CFG_PROXY_ADDRESS=	<ip>	Proxy server IP address
CFG_PROXY_PORT=	<port>	Proxy server port number

Property	Value	Feature
CFG_PROXY_USERNAME=	<username>	Username for authentication
CFG_PROXY_PASSWORD=	<password>	Password for authentication
ACTIVATION_DATA=	See below	Product activation, license key or offline license file
ACTIVATION_DLG_SUPPRESS=	0—Disabled 1—Enabled	When set to "1", do not show the product activation dialog after the first start
ADMINCFG=	<path>	Path to exported XML configuration (default value *cfg.xml*)

Configuration properties only in ESET Endpoint Security

CFG_EPFW_MODE=	0—Automatic (default) 1—Interactive 2—Policy-based 3—Learning	Firewall filtering mode
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	End date of the Learning Mode as Unix timestamp

LiveGrid® property

When installing ESET Endpoint Security with CFG_LIVEGRID_ENABLED, the behavior of the product after the installation will be:

Feature	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ESET LiveGrid® reputation system	On	On
ESET LiveGrid® feedback system	Off	On
Submit anonymous statistics	Off	On

ACTIVATION_DATA property

Format	Method
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Activation using ESET license key (internet connection should be active)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	Activation using an offline license file

Language properties

ESET Endpoint Security language (you must specify both properties).

Property	Value
PRODUCT_LANG=	LCID Decimal (Locale ID), for example, 1033 for English (United States). See the list of language codes.
PRODUCT_LANG_CODE=	LCID String (Language Culture Name) in lowercase, for example, en-us for English (United States). See the list of language codes.

Restart properties

Specify the following parameters to restart the computer after installation:

Property	Value	Feature
REBOOT_WHEN_NEEDED=	0—Disabled 1—Enabled	If enabled, after installation, the computer will restart.
REBOOT_CANCELABLE=	0—Disabled 1—Enabled	If enabled, the user can cancel the computer restart.
REBOOT_POSTPONE=	value in seconds	Maximum amount of time in seconds for the user to postpone the computer restart.

REBOOT_CANCELABLE and REBOOT_POSTPONE are available only if REBOOT_WHEN_NEEDED is enabled.

Command line installation examples

Ensure that you read the End User License Agreement and have administrative privileges before running the installation.

Exclude the **NetworkProtection** section from the installation (you must also specify all child features):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

If you want your ESET Endpoint Security to be automatically configured after the installation, you can specify basic configuration parameters within the installation command.
Install ESET Endpoint Security with ESET LiveGrid® enabled:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Install to a different application installation directory than the default.
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Install and activate ESET Endpoint Security using your ESET license key.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Silent installation with detailed logging (useful for troubleshooting), and RMM only with mandatory components:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Forced silent full installation with a specified language.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Post-installation command line options

- ESET CMD—Import an .xml configuration file or turn on/off a security feature.
- Command line scanner—Run a Computer scan from the command line.

Deployment using GPO or SCCM

Apart from installing ESET Endpoint Security directly on a client workstation, you can also install using management tools such as Group Policy Object (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris or Puppet.

Managed (recommended)

For managed computers, we first install ESET Management Agent, then deploy ESET Endpoint Security via ESET PROTECT On-Prem. ESET PROTECT On-Prem must be installed in your network.

1. Download the standalone installer for ESET Management Agent.
2. Prepare the GPO/SCCM remote deployment script.
3. Deploy ESET Management Agent using either GPO or SCCM.
4. Ensure that the client computers has been added to ESET PROTECT On-Prem.
5. Deploy and activate ESET Endpoint Security to your client computers.

> The following ESET Knowledgebase article may only be available in English:
> • Deploy the ESET Management Agent via SCCM or GPO
> • Deploy the ESET Management Agent using a Group Policy Object (GPO)

Unmanaged

For unmanaged computers, you can deploy ESET Endpoint Security directly to client workstations. This is not recommended because you will not be able to monitor and enforce policies for all your ESET endpoint products on workstations.

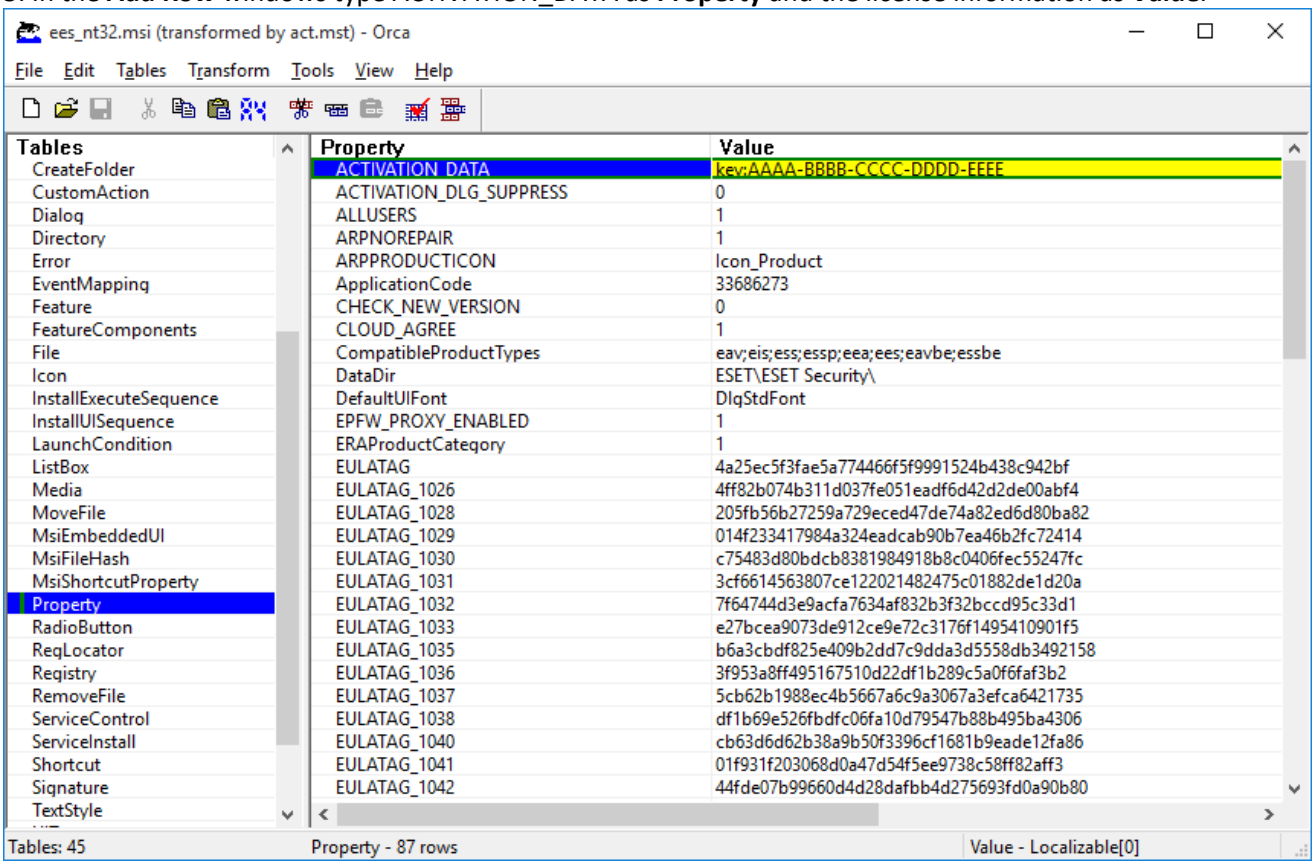
By default, ESET Endpoint Security is not activated after installation and therefore not functional.

Option 1 (Software installation)

1. Download the .msi installer for ESET Endpoint Security.
2. Create an .mst transform package from the .msi file (for example by using the Orca .msi editor) to include the product activation property (see `ACTIVATION_DATA` in Command-line installation).

Show steps for creating .mst in Orca

1. Open Orca.
2. Load the .msi installer by clicking **File** > **Open**.
3. Click **Transform** > **New Transform**.
4. Click **Property** in the **Tables** section and then in the menu **Tables** > **Add row**.
5. In the **Add Row** windows type ACTIVATION_DATA as **Property** and the license information as **Value**.



6. Click **Transform** > **Generate Transform** to save the .mst file.

1. Optional: To import your customized ESET Endpoint Security .xml configuration file (for example, to enable RMM or configure proxy server settings), put the cfg.xml file in the same location as the .msi installer.
2. Deploy the .msi installer with the .mst file remotely using GPO (via Software installation) or SCCM.

Option 2 (using a scheduled task)

1. Download the .msi installer for ESET Endpoint Security.
2. Prepare a Command-line installation script to include the product activation property (see `ACTIVATION_DATA`).
3. Make the .msi installer and the .cmd script accessible in the network for all workstations.
4. Optional: To import your customized ESET Endpoint Security .xml configuration file (for example, to enable RMM or configure proxy server settings), put the cfg.xml file in the same location as the .msi installer.
5. Apply a prepared command-line installation script using either GPO or SCCM.
    - For GPO, use Group Policy Preferences > Group Policy Schedule Tasks > Immediate task

> If you do not want to use ESET PROTECT On-Prem to remotely manage your ESET endpoint products, ESET Endpoint Security contains the ESET plugin for RMM which enables you to supervise and control software systems using a locally installed agent that can be accessed by a management service provider. Find more information.

Upgrading to a more recent version

New versions of ESET Endpoint Security are issued to implement improvements or fix issues that cannot be resolved by automatic updates to program modules.

Upgrading to a more recent version can be accomplished in several ways:

1. Automatically, using ESET PROTECT On-Prem, or ESET PROTECT.
2. Automatically, using GPO or SCCM.
3. Automatically, using a program update.
   Because the program upgrade is distributed to all users and may impact certain system configurations, it is issued after a long testing period to ensure functionality with all possible system configurations. If you need to upgrade to a later version immediately after its release, use one of the methods below.
   Ensure that you have enabled **Update mode** in Advanced setup > **Update** > **Profiles** > **Product updates**.
4. Manually, by downloading and installing a more recent version over the previous one.

Recommended upgrade scenarios

I manage or I want to manage my ESET products remotely

If you manage more than 10 ESET Endpoint products, consider handling upgrades using ESET PROTECT On-Prem or ESET PROTECT. See the following documentation:

- ESET PROTECT On-Prem | Upgrade ESET software via a client task
- ESET PROTECT On-Prem | Guide for small to medium-sized businesses that manage up to 250 Windows ESET endpoint products
- Introduction to ESET PROTECT

Upgrading manually on a client workstation

To upgrade ESET Endpoint Security on individual client workstations manually:

1. Verify the version you have currently installed is supported.
2. Verify that your operating system is supported.

2. Download and install the latest version over the previous one.

> Successful installation of the latest version over the previous one is not guaranteed for versions with "End of Life" support level. See the End of life policy to review your ESET Endpoint Security support level.
> To upgrade from unsupported versions, uninstall your ESET Endpoint Security first. Read the following ESET Knowledgebase article for additional information about upgrading ESET Endpoint Security on a client workstation.

Legacy product automatic upgrade

Your ESET product version is no longer supported, and your product has been upgraded to the latest version.

Common installation problems

Each new version of ESET products feature many bugfixes and improvements. Existing customers with a valid license for an ESET product may upgrade to the latest version of the same product for free.

To finish the installation:

1. Click **Accept and continue** to accept the End User License Agreement and acknowledge the Privacy Policy. If you do not agree with the End User License Agreement, click **Uninstall**. You cannot revert to the previous version.
2. Click **Allow all and continue** to allow ESET LiveGrid® feedback system or click **Continue** if you do not want to participate.
3. After activating the new ESET product with your license key, the Home page will be displayed. If your license information is not found, continue with a new trial license. If your license used in the previous product is not valid, activate your ESET product.
4. A device restart is required to complete the installation.

Security and stability hotfixes

Updating ESET Endpoint Security is an essential part of maintaining complete protection against malicious code. Each new version of ESET Endpoint Security features many improvements and bugfixes. We highly recommend periodic updating of ESET Endpoint Security to prevent you from security vulnerabilities and threats. ESET Endpoint Security fits into a specific stage of the product lifecycle as any other of ESET products.

Read more about:
End of Life policy (Business products)
Product updates
Security and Stability Hotfixes

Automatic updates ensure the maximum security and stability of your product. You cannot disable security and stability updates.

Product activation

After installation is complete, you will be prompted to activate your product.

There are several methods for activating your product. Availability of a specific activation scenario in the activation window may vary depending on the country and the means of distribution (ESET web page, installer type .msi or .exe, etc.).

You can activate ESET Endpoint Security in the main program window > **Help and support** > **Activate product** or **Protection status** > **Activate product**.

You can use any of the following methods to activate ESET Endpoint Security:

- **Use a purchased License Key**—Unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the license owner and for activation of the license.
- **Use your account**—An ESET PROTECT HUB account which you have to create. ESET PROTECT HUB is a central gateway to the ESET PROTECT On-Prem unified security platform. It provides centralized identity, subscription and user management for all ESET platform modules. You can use this option to activate ESET Endpoint Security also with older license management tools: ESET Business Account or ESET MSP

Administrator.

- **Offline License**—Automatically generated file that will be transferred to the ESET product to provide license information. If a license allows you to download an offline license file (.lf), that file can be used to perform offline activation. The number of offline licenses will be subtracted from the total number of available licenses. For more details about the generation of an offline file see the ESET Business Account Online user guide.

Click **Activate later** if your computer is a member of managed network and your administrator will perform remote activation via ESET PROTECT On-Prem. You can also use this option if you would like to activate this client at a later time.

If you have a Username and Password used for activation of earlier ESET products, convert your legacy credentials to a license key.

You can change your product license at any time in the main program window > **Help and support** > **Change license**. You will see the public license ID used to identify your license to ESET Support.

ESET PROTECT On-Prem can activate client computers silently using licenses made available by the administrator. For instructions, see the ESET PROTECT On-Prem Online help.

Failed product activation?

Entering your license key during activation

Automatic updates are important for your security. ESET Endpoint Security will only receive updates when activated using your **License Key**.

If you did not enter your license key after installation, your product will not be activated. You can change your license in the main program window. To do so, click **Help and support** > **Activate License** and enter the license data you received with your ESET Security product into the Product activation window.

When entering your **License Key**, it is important to type it exactly as it is written:

- Your License Key is a unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the the license owner and activation of the license.

We recommend that you copy and past your License Key from your registration email to ensure accuracy.

ESET PROTECT HUB account

ESET PROTECT HUB is a central gateway to the ESET PROTECT On-Prem unified security platform. It provides centralized identity, subscription and user management for all ESET platform modules. Using ESET PROTECT HUB you can:

- Get a security subscriptions overview
- Check subscribed services usage and statuses
- Allocate and control granular access to individual ESET platforms
- Use a single sign-in for all linked and accessible ESET platforms

You can use this activation option to activate ESET Endpoint Security also with older license management tools:

ESET Business Account or ESET MSP Administrator.

You can create an ESET PROTECT HUB account and log in with your **Email address** and **Password**.

If you have forgotten your password click **I forgot my password**, and you will be redirected to the ESET PROTECT HUB. Type your email address and click **Sign in** to confirm. Next, you will obtain a message with instructions on how to reset your password.

How to use legacy license credentials to activate ESET endpoint product

If you already have your Username and Password and would like to receive a license key, visit the ESET Business Account portal, where you can convert your credentials to a new license key.

Activation failed

If the activation of ESET Endpoint Security is not successful, the most common scenarios are:

- License key is already in use.
- You have entered an invalid license key.
- Information in the activation form is missing or invalid.
- Communication with the activation server failed.
- No connection or disabled connection to ESET activation servers.

Verify that you have entered the proper license key or attached an Offline license and attempt to activate again.

If you are unable to activate, our welcome package will walk you through to common questions, errors, problems about activation and licensing (available in English and several other languages).

- Start ESET product activation troubleshooting

Registration

Register your license by completing the fields contained in the registration form and clicking **Continue**. The fields marked as required in brackets are mandatory. This information will only be used for matters involving your ESET License.

Activation progress

ESET Endpoint Security is now activating, this may take a few moments.

Activation successful

Activation was successful and ESET Endpoint Security is now activated. From now on, ESET Endpoint Security will receive regular updates to identify the latest threats and keep your computer safe. Click **Done** to finish product

activation.

Common installation problems

If problems occur during installation, the Installation Wizard provides a troubleshooter that resolves the issue, if possible.

Click **Run troubleshooter** to start the troubleshooter. When the troubleshooter finishes, follow the recommended solution.

If the problem persists, see the list of common installation errors and resolutions.

Beginner's guide

This chapter provides an initial overview of ESET Endpoint Security and its basic settings.

System tray icon

Some of the most important setup options and features are available by right-clicking the system tray (Windows notification area) icon.

To access the system tray (Windows notification area) icon menu, make sure the start mode of User Interface elements is set to Full.

If ESET Endpoint Security has an enabled protection layer assigned from a policy, the pause protection functionality will not be operational for the specific layer.
If all protection layers are enabled and the administrator pushes this setting by the policy, the pause protection functionality will not pause any protection. All toggles for protection layers in the product will appear grey if the administrator pushes their state by the policy.
You can use the Override mode if you have ESET Endpoint Security 6.5 and later installed on your machine. Override mode enables users on the client-computer level to change settings in the installed ESET product, even if a policy is applied over these settings.

Pause protection—Displays the confirmation dialog box that disables Detection engine, which guards against attacks by controlling file, web and email communication. The **Time interval** drop-down menu enables you to specify how long the protection will be disabled.

Pause firewall (allow all traffic)—Switches the firewall to an inactive state. See Network for more information.

Block all network traffic—Blocks all network traffic. You can re-enable it by clicking **Stop blocking all network traffic**.

Advanced setup—Opens the ESET Endpoint Security Advanced setup. To open Advanced setup from the main program window, press F5 on your keyboard or click **Setup** > **Advanced setup**.

Log files—Contains information about important program events that have occurred and provides an overview of detections.

Open ESET Endpoint Security—Opens the ESET Endpoint Security main program window from the tray (Windows

notification area) icon.

Reset window layout—Resets the ESET Endpoint Security's window to its default size and position on the screen.

Color mode—Opens User Interface settings where you can change the color of the graphical user interface.

Check for updates—Starts a module or product update to ensure you are protected. ESET Endpoint Security checks for updates automatically several times a day.

About—Provides system information, details about the installed version of ESET Endpoint Security, installed program modules, and information about the operating system and system resources.

Keyboard shortcuts

For better navigation in ESET Endpoint Security, you can use the following keyboard shortcuts:

Keyboard shortcut	Action
F1	open help pages
F5	open Advanced setup
Up Arrow / Down Arrow	navigation in drop-down menu items
TAB	move to the next GUI element in a window
Shift+TAB	move to the previous GUI element in a window
ESC	close the active dialog window
Ctrl+U	show information about your ESET license and your computer (Details for Technical Support)
Ctrl+R	reset the product window to its default size and position on the screen
ALT + Left Arrow	navigate back
ALT + Right Arrow	navigate forward
ALT+Home	navigate home

You can also use mouse buttons back or forward for navigation.

Profiles

Profile manager is used in two places within ESET Endpoint Security—In the **On-demand scan** section and in the **Update** section.

Computer scan

There are 4 pre-defined scan profiles in ESET Endpoint Security:

- **Smart scan**—This is the default advanced scanning profile. The Smart scan profile uses Smart Optimization technology, which excludes files that were found to be clean in a previous scan and have not been modified since that scan. This allows for lower scan times with a minimal impact to system security.
- **Context menu scan**—You can start an on-demand scan of any file from the context menu. The Context menu scan profile enables you to define a scan configuration that will be used when you trigger the scan

this way.

- **In-depth scan**—The In-depth scan profile does not use Smart optimization by default, so no files are excluded from scanning using this profile.
- **Computer scan**—This is the default profile used in the standard computer scan.

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open Advanced setup > **Detection engine** > **Malware scans** > **On-demand scan** > **List of profiles** > **Edit**. The **Profile manager** window includes the **Selected profile** drop-down menu that lists existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see ThreatSense for a description of each parameter of the scan setup.

> Suppose that you want to create your own scan profile and the **Scan your computer** configuration is partially suitable, but you do not want to scan runtime packers or potentially unsafe applications and you also want to apply **Always remedy detection**. Type the name of your new profile in the **Profile manager** window and click **Add**. Select your new profile from the **Selected profile** drop-down menu and adjust the remaining parameters to meet your requirements, and then click **OK** to save your new profile.

Update

The profile editor in the Update setup enables you to create new update profiles. Create and use your own custom profiles (other than the default **My profile**) only if your computer uses multiple means to connect to update servers.

For example, a laptop that normally connects to a local server (Mirror) in the local network but downloads updates directly from ESET update servers when disconnected from the local network (business trip) might use two profiles: the first one for connecting to the local server; the other one for connecting to ESET servers. When these profiles are configured, navigate to **Tools** > **Scheduler** and edit the update task parameters. Designate one profile as primary and the other as secondary.

Update profile—The currently used update profile. To change it, choose a profile from the drop-down menu.

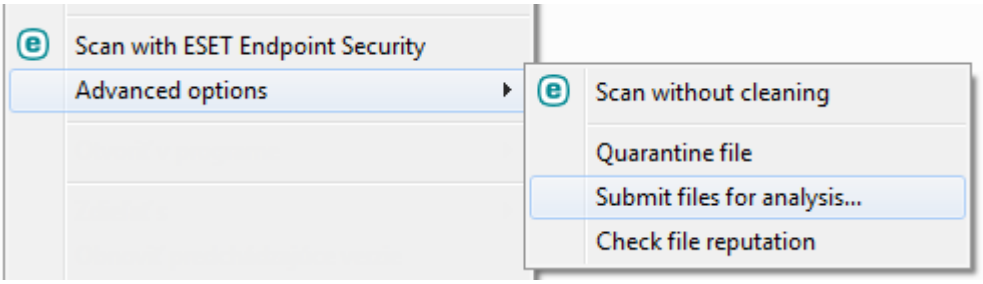
List of profiles—Create new or remove existing update profiles.

Context menu

The context menu is displayed after right-clicking an object (file). The menu lists all of the actions that you can perform on an object.

You can integrate ESET Endpoint Security control elements into the context menu. Setup option for this functionality are available in Advanced setup > **User Interface** > **User interface elements**.

Integrate into the context menu—Integrate the ESET Endpoint Security control elements into the context menu.

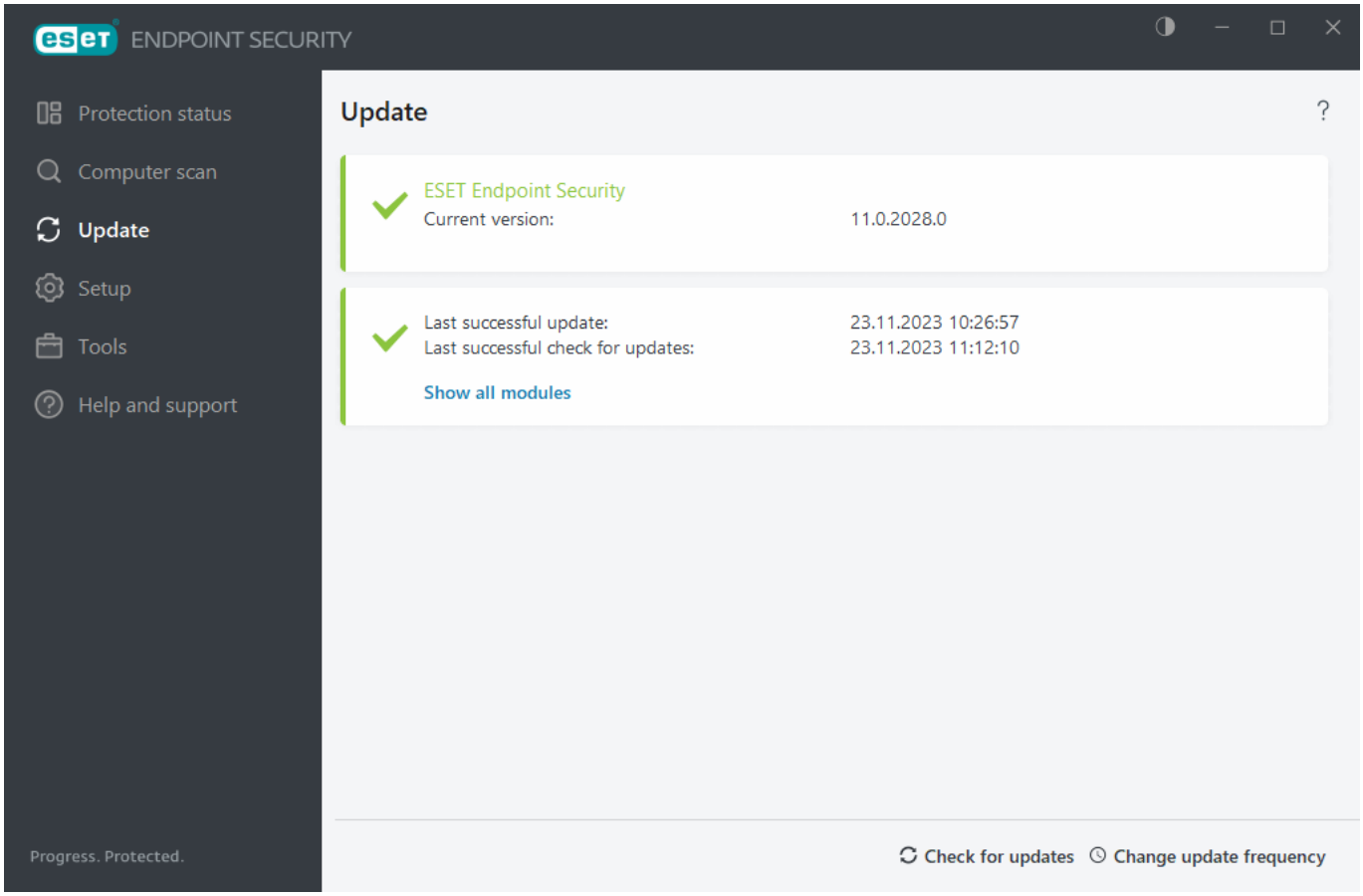


Update setup

Regularly updating ESET Endpoint Security is the best method to provide maximum security on your computer. The Update module ensures that the program modules and the system components are always up to date.

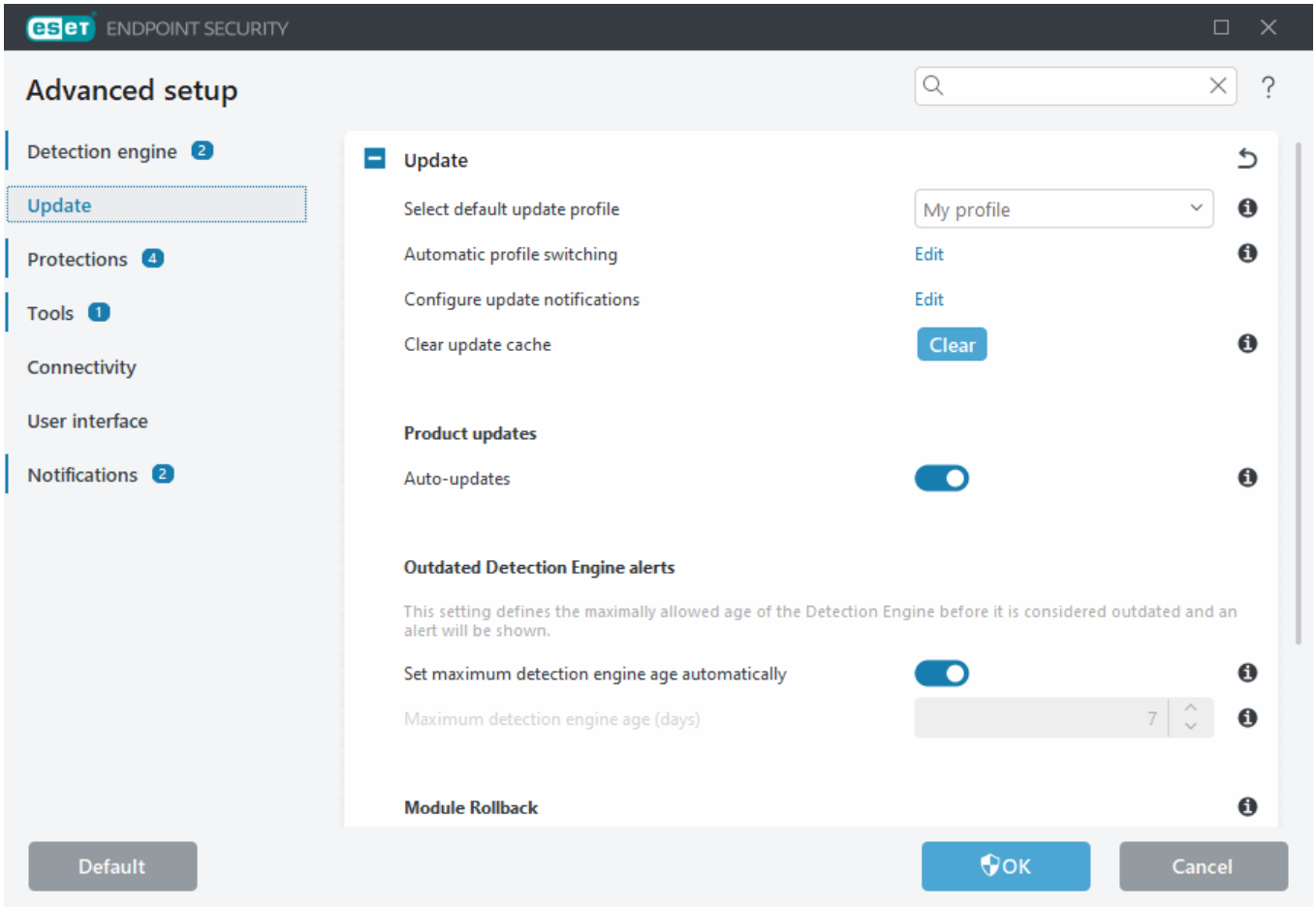
By clicking **Update** in the main program window, you can view the current update status, including the date and time of the last successful update and if an update is needed.

In addition to automatic updates, you can click **Check for updates** to trigger a manual update.



Advanced setup > **Update** contains additional update options such as update mode, proxy server access and LAN connections.

If you experience problems with an update, click **Clear** to clear the update cache. If you still cannot update program modules, see the Troubleshooting for "Modules update failed" message section.

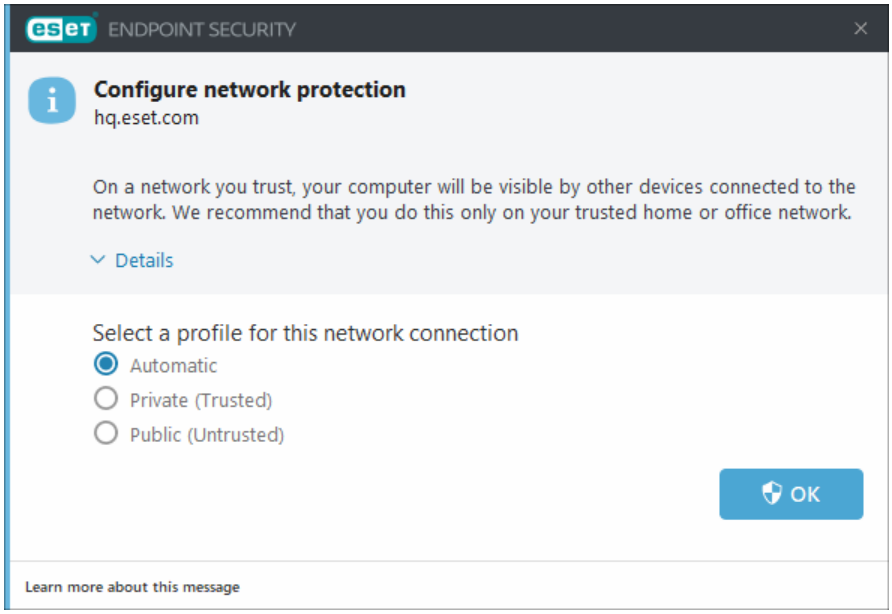


The **Choose automatically** option in Advanced setup > **Update** > **Profiles** > **Updates** > **Module Updates** is enabled by default. When using an ESET update server for receiving updates, we recommend that you leave this as it is.

For optimal functionality, the program must be automatically updated. Automatic updates can only occur if the correct license key is entered in **Help and support** > **Activate Product**. If you did not type in your license key after installation, you can do so at any time. For more detailed information about activation, see How to activate ESET Endpoint Security.

Configure network protection

By default, ESET Endpoint Security uses Windows settings when a new network connection is detected. To display a dialog window when a new network is detected, change the Network protection profile assignment to **Ask**. Network protection configuration will be displayed whenever your computer connects to a new network.



You can select from the following Network connection profiles:

Automatic—ESET Endpoint Security will select the profile automatically, based on the Activators configured for each profile.

Private—For trusted networks (home or office network). Your computer and shared files stored on your computer are visible to other network users, and system resources are accessible to other users on the network (access to shared files and printers is enabled, incoming RPC communication is enabled and remote desktop sharing is available). We recommend using this setting when accessing a secure local network. This profile is automatically assigned to a network connection if it is configured as Domain or Private network in Windows.

Public—For untrusted networks (public network). Files and folders on your system are not shared with or visible to other users on the network, and system resource sharing is deactivated. We recommend using this setting when accessing wireless networks. This profile is automatically assigned to any network connection that is not configured as Domain or Private network in Windows.

User-defined profile—You can select a profile you created from the drop-down menu. This option is only available if you have created at least one custom profile.

⚠ An incorrect network configuration may pose a security risk to your computer.

Web control tools

If you have already enabled Web control in ESET Endpoint Security, you must also configure Web control for your desired user accounts in order for Web control to function properly. See Web control for instructions on how to create specific restrictions for your client workstations to protect them from potentially offensive content.

Blocked hashes

Using ESET Inspect in your environment enables administrators to block access to specified executables based on their hash. If the administrator blocks access to an executable and you try to access it, ESET Endpoint Security displays this notification:

File access blocked—The application (name of the application is displayed) tried to access a file that is not permitted by your administrator.

If you are the administrator and want to allow access to the application specified in the notification, see Blocked Hashes in ESET Inspect Online Help. If you are a user and want to change the application's behavior, contact your administrator.

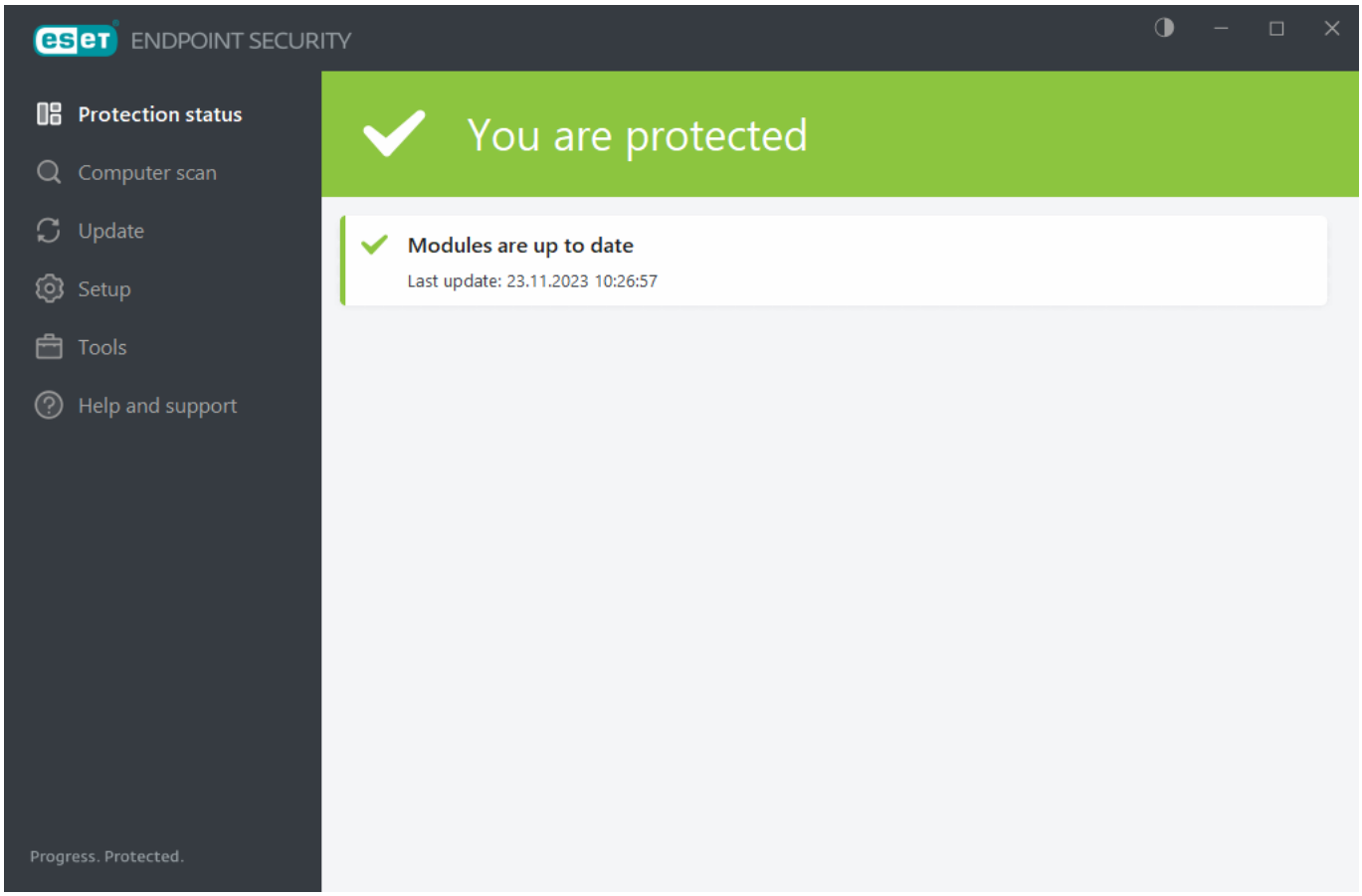
Working with ESET Endpoint Security

The ESET Endpoint Security main program window is split into two sections. The primary window on the right displays information corresponding to the option selected from the main menu on the left.

> **Illustrated instructions**
> See Open the main program window of ESET Windows products for illustrated instructions available in English and several other languages.

You can select the color scheme of ESET Endpoint Security GUI in the top right corner of the main program window. Click the **Color scheme** icon (the icon changes based on the currently selected color scheme) next to **Minimize** icon and select the color scheme from the drop-down menu:

- **Same as the system color**—Sets the color scheme of ESET Endpoint Security based on your operating system settings.
- **Dark**—ESET Endpoint Security will have a dark color scheme (dark mode).
- **Light**—ESET Endpoint Security will have a standard, light color scheme.



Main menu options:

Protection status—Provides information about the protection status of ESET Endpoint Security.

Computer scan—Enables you to configure and launch a scan of your computer or create a custom scan.

Update—Displays information about the module and detection engine updates.

Tools—Provides access to features that help simplify program administration and offer additional options for advanced users.

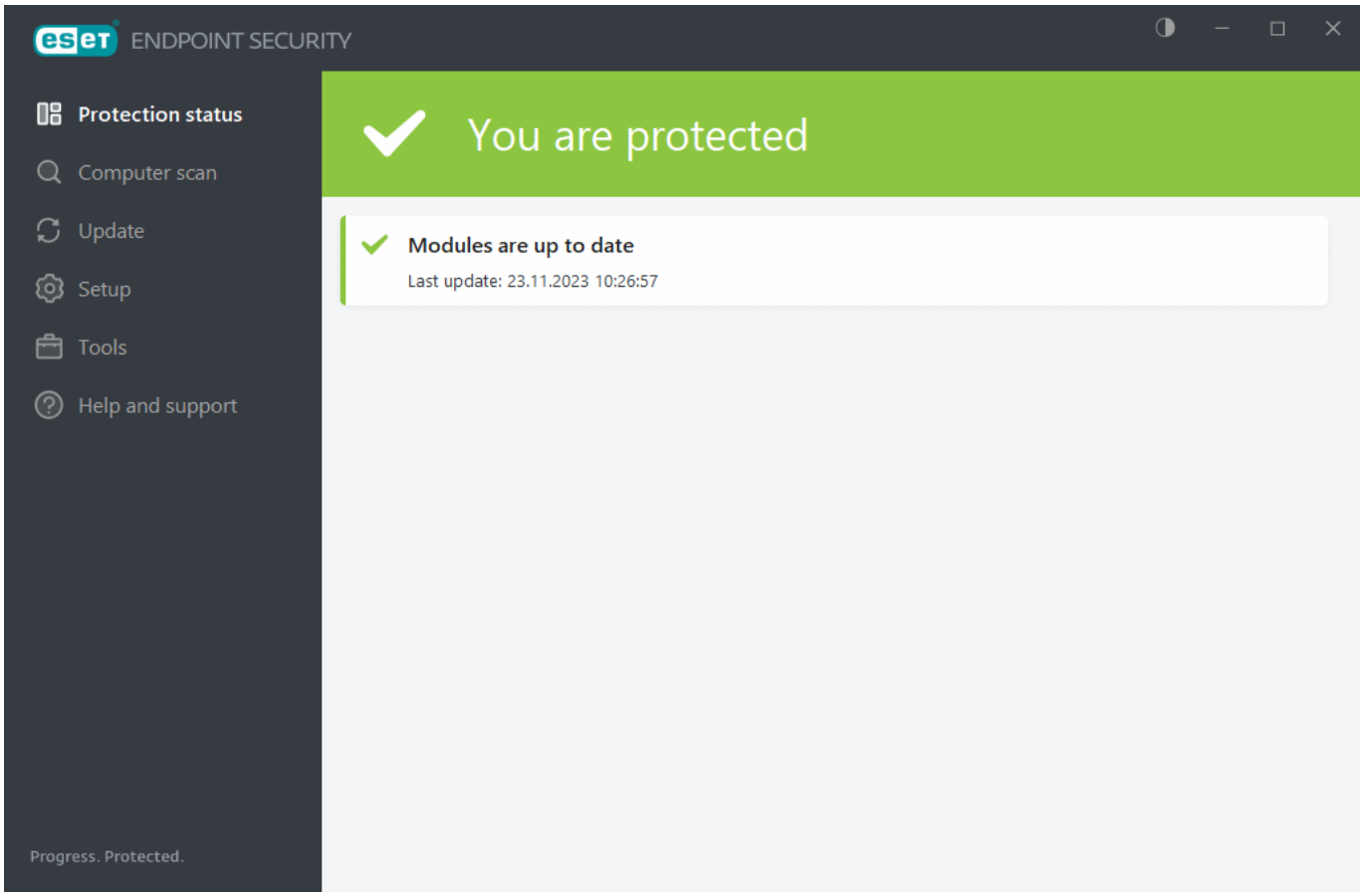
Setup—Provides configuration options for the ESET Endpoint Security protection features and access to Advanced setup.

Help and support—Displays information about your license, the installed ESET product, and links to Online Help, ESET Knowledgebase, and Technical Support.

Protection status

The **Protection status** window displays information about your computer's current protection and the last update. The green **Maximum protection** status indicates that maximum protection is ensured.

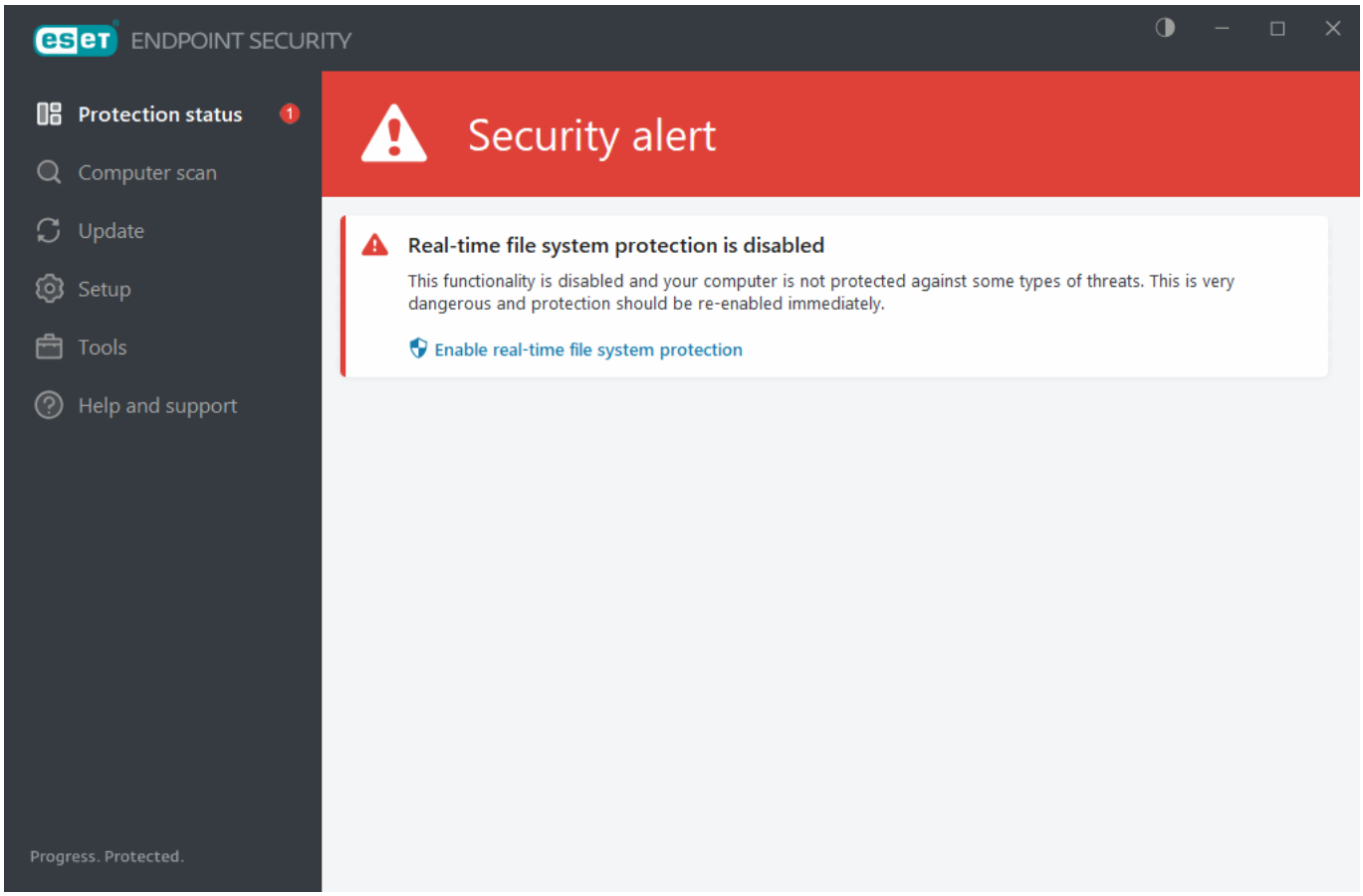
The **Protection status** window displays notifications with detailed information and recommended solutions to improve the security of ESET Endpoint Security, turn on additional features or ensure maximum protection.



The green icon and green **You are protected** status indicate that maximum protection is ensured.

What to do if the program does not work properly?

A green check mark will be displayed next to all program modules that are fully functional. A red exclamation point or orange notification icon is displayed if a module needs attention. Additional information about the module, including our recommendation about how to restore full functionality is shown in the upper part of the window. To change a module's status, click **Setup** in the main menu and then click the desired module.



The red exclamation point (!) icon indicates that maximum protection of your computer is not ensured. You may encounter this type of notification in the following scenarios:

- **Antivirus and antispyware protection is paused**—Click **Start all antivirus and antispyware protection modules** to re-enable antivirus and antispyware protection in **Protection status** pane or **Enable Antivirus and antispyware protection** in **Setup** pane in the main program window.
- Antivirus protection is non-functional—Virus scanner initialization failed. Most ESET Endpoint Security modules will not function properly.
- **Anti-Phishing protection is non-functional**—This feature is not functional because other required program modules are not active.
- **Firewall is disabled**—This problem is indicated by a red icon and a security notification next to the **Network** item. Click **Enable filtering mode** to re-enable network protection.
- **Firewall initialization failed**—The firewall is disabled due to system integration issues. Restart your computer as soon as possible.
- **Detection engine is out of date**—This error will appear after several unsuccessful attempts to update the detection engine (formerly virus signature database). We recommend that you check the update settings. The most common reason for this error is incorrectly typed authentication data or incorrectly configured connection settings.
- **Product is not activated** or **Your license expired**—This is indicated by a red protection status icon. The

program is not able to update after your license expires. Follow the instructions in the alert window to renew your license.

- **Host Intrusion Prevention System (HIPS) is disabled**—This problem is indicated when HIPS is disabled. Your computer is not protected against some types of threats and protection should be re-enabled immediately by clicking **Enable HIPS**.
- **No regular updates scheduled**—ESET Endpoint Security will not check for or receive important updates unless you schedule update task.
- **Network access blocked**—Displayed when the **Isolate computer from network** client task of this workstation from ESET PROTECT On-Prem is triggered. Contact your system administrator for more information.
- **Real-time file system protection is paused**—Real-time protection was disabled by the user. Your computer is not protected against threats. Click Enable Real-time protection re-enable this functionality.


The orange "i" indicates that your ESET product requires attention for a non-critical problem. Possible reasons include:

- **Web access protection is disabled**—Click the security notification to re-enable Web access protection and then click **Enable Web access protection**.
- **Your license expires soon / Your license expires today**—This is indicated by the protection status icon displaying an exclamation point. After your license expires, the program will not be able to update and the Protection status icon will turn red.
- **Botnet protection is paused**— Click **Enable Botnet protection** to re-enable this feature.
- **Network attack protection (IDS) is paused**—Click **Enable Network attack protection (IDS)** to re-enable this feature.
- **Email client antispam is paused**—Click **Enable Email client antispam** to re-enable this feature.
- **Web control is paused**—Click **Enable Web control to re-enable this feature**.
- **Policy override active**—The configuration set by the policy is temporarily overridden, possibly until troubleshooting is complete. Only authorized user can override the policy settings. For more information see How to use Override mode.
- **Device control is paused**—Click **Enable Device control** to re-enable this feature.

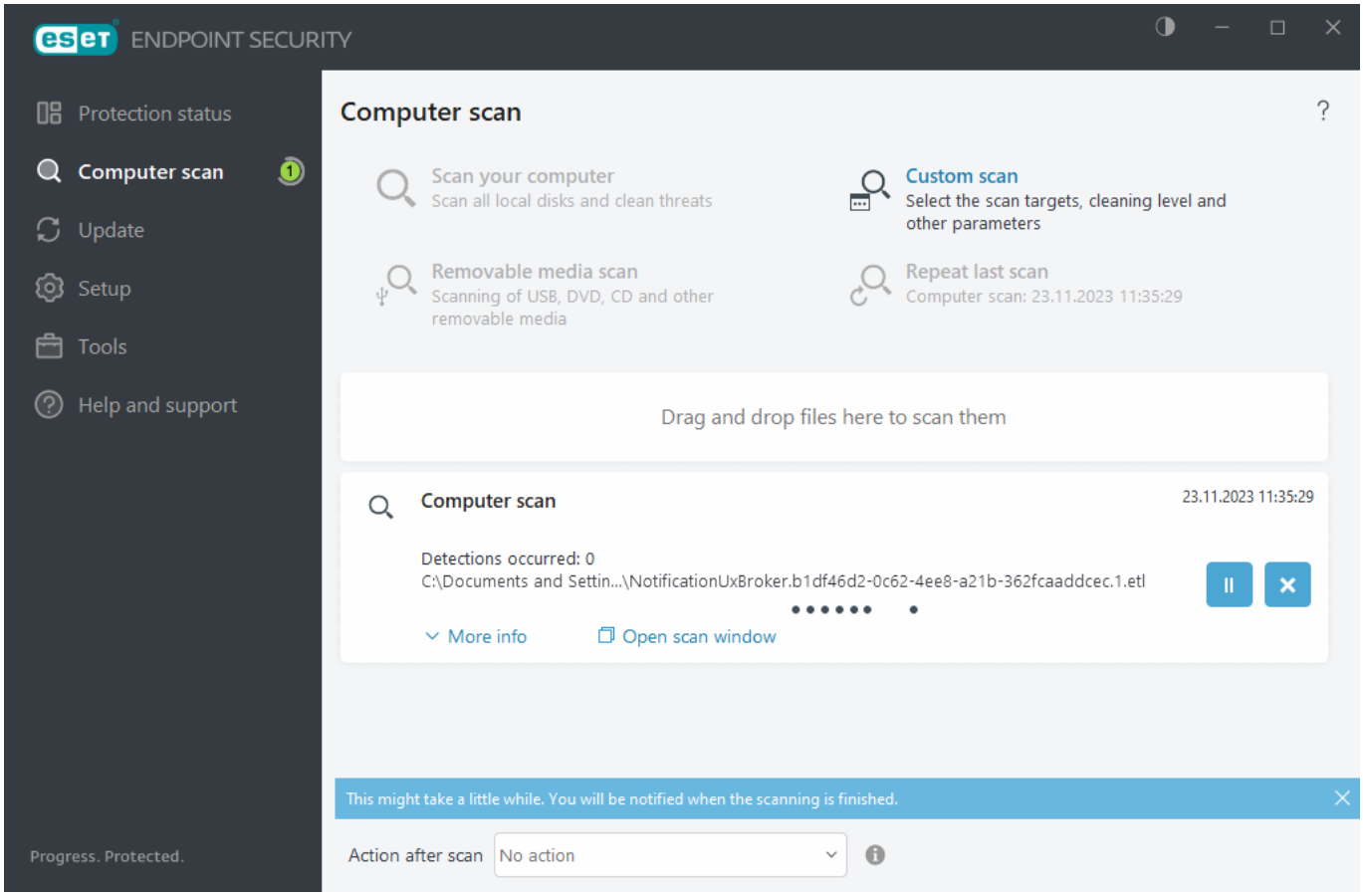
To adjust visibility in-product statuses in the first pane of ESET Endpoint Security, see Application statuses.

If you are unable to solve a problem by using the suggested solutions, click **Help and support** to access the help files or search the ESET Knowledgebase. If you still need assistance, you can submit an ESET Technical Support request. ESET Technical Support will respond quickly to your questions and help find a resolution.

> If a status belongs to a feature that is blocked by ESET PROTECT On-Prem policy, the link will not be clickable.

Computer scan

The on-demand scanner is an important part of ESET Endpoint Security. It is used to perform scans of files and folders on your computer. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. We recommend that you perform regular (for example once a month) in-depth scans of your system to detect viruses not detected by Real-time file system protection. This can happen if Real-time file system protection was disabled at the time, if the detection engine was obsolete or if the file was not detected as a virus when it was saved to the disk.



Two types of **Computer scan** are available. **Scan your computer** quickly scans the system with no need for further configuration of the scan parameters. **Custom scan** enables you to select any of the pre-defined scan profiles and define specific scan targets.

See Scan progress for more information about the scanning process.

Scan your computer

Scan your computer enables you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of **Scan your computer** is it is easy to operate and does not require detailed scanning configuration. This scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information about cleaning modes, see Cleaning.

You can also use the **Drag and drop scan** feature to scan a file or folder manually by clicking the file or folder, moving the mouse pointer to the marked area while keeping the mouse button pressed and then releasing it. After that, the application is moved to the foreground.

The following scanning options are available under **Advanced scans**:

Custom scan

Custom scan enables you to specify scanning parameters such as scan targets and methods. The advantage of **Custom scan** is that you can configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with the same parameters.

Removable media scan

Similar to **Scan your computer**—quickly launch a scan of removable media (such as CD/DVD/USB) that are currently connected to the computer. This may be useful when you connect a USB flash drive to a computer and want to scan its contents for malware and other potential threats.

This type of scan can also be initiated by clicking **Custom scan**, selecting **Removable media** from the **Scan targets** drop-down menu and clicking **Scan**.

Repeat last scan

Enables you to quickly launch the previously performed scan using the same settings as before.

Action after scan drop-down menu enables you to set an action to be performed automatically after a scan finishes:

- **No action**—After a scan finishes, no action will be performed.
- **Shut down**—The computer turns off after a scan finishes.
- **Restart if needed**—The computer restarts if only needed to complete cleaning of detected threats.
- **Restart**—Closes all open programs and restarts the computer after a scan finishes.
- **Force restart if needed**—The computer forces restart if only needed to complete cleaning of detected threats.
- **Force restart**— Forces closing of all open programs without waiting for user interaction and restarts the computer after a scan finishes.
- **Sleep**—Saves your session and puts the computer in a low-power state so that you can quickly resume working.
- **Hibernate**—Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down but will resume its previous state the next time you start it.

> **Sleep** or **Hibernate** actions are available based on your computer Power & sleep operating system settings or your computer/laptop capabilities. Remember that a sleeping computer is still a working computer. It is still running basic functions and using electricity when your computer runs on battery power. To preserve battery life, for example, when traveling outside of your office, we recommend using the Hibernate option.

The selected action will start after all of the running scans are finished. When you select **Shutdown** or **Restart**, a confirmation dialog window will display a 30-second countdown (click **Cancel** to deactivate the requested action).

> We recommend that you run a computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**. How do I schedule a weekly computer scan?

Custom scan launcher

You can use the Custom Scan to scan operating memory, network, or specific parts of a disk rather than the entire disk. To do so, click **Advanced scans** > **Custom scan** and select specific targets from the folder (tree) structure.

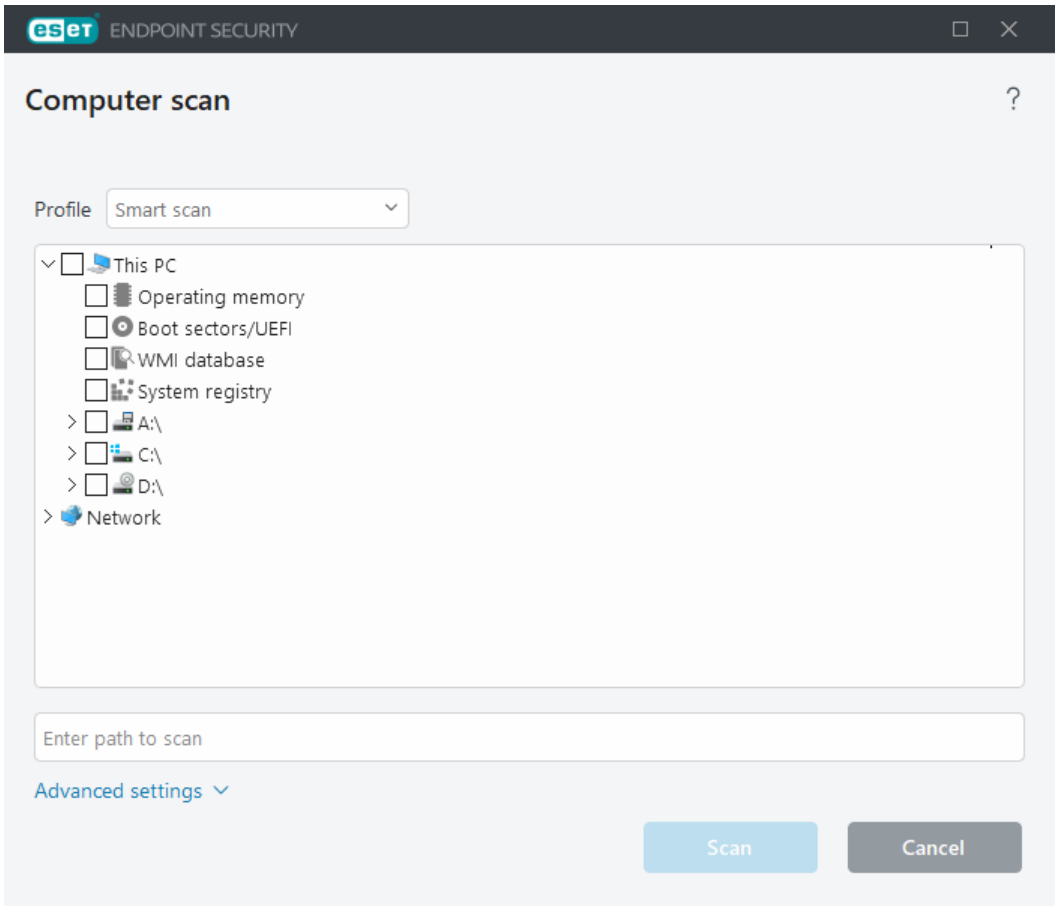
You can choose a profile from the **Profile** drop-down menu when scanning specific targets. The default profile is **Smart scan**. There are three more pre-defined scan profiles called **In-depth scan**, **Context menu scan** and **Computer scan**. These scan profiles use different ThreatSense parameters. The available options are described in Advanced setup > **Detection engine** > **Malware scans** > **On-demand scan** > ThreatSense.

The folder (tree) structure also contains specific scan targets.

- **Operating memory**—Scans all processes and data currently used by operating memory.
- **Boot sectors/UEFI**—Scans Boot sectors and UEFI for the presence of malware. Read more about the UEFI scanner in the glossary.
- **WMI database**—Scans the whole Windows Management Instrumentation (WMI) database, all namespaces, class instances, and properties. Searches for references to infected files or malware embedded as data.
- **System registry**—Scans the whole system registry, all keys, and subkeys. Searches for references to infected files or malware embedded as data. When cleaning the detections, the reference remains in the registry to ensure important data is not lost.

To quickly navigate to a scan target (file or folder), type its path into the text field below the tree structure. The path is case-sensitive. To include the target in the scan, select its check box in the tree structure.

> **How to schedule a weekly computer scan**
> To schedule a regular task, see How to schedule a weekly computer scan.



You can configure cleaning parameters for the scan in Advanced setup > **Detection engine** > **Malware scans** > **On-demand scan** > **ThreatSense** > **Cleaning**. To run a scan with no cleaning action, click **Advanced settings** and select **Scan without cleaning**. Scan history is saved to the scan log.

When **Ignore exclusions** is selected, files with previously excluded extensions will be scanned with no exception.

Click **Scan** to execute the scan using the custom parameters you have set.

Scan as Administrator enables you to execute the scan under the Administrator account. Use this if the current

user does not have privileges to access the files you want to scan. This button is not available if the current user cannot call UAC operations as an Administrator.

> You can view the computer scan log when a scan completes by clicking Show log.

Scan progress

The scan progress window shows the current status of the scan and information about the number of files found that contain malicious code.

> It is normal that some files, such as password-protected files or files being exclusively used by the system (typically *pagefile.sys* and certain log files), cannot be scanned. You can find more details in our Knowledgebase article.

> **How to schedule a weekly computer scan**
> To schedule a regular task, see How to schedule a weekly computer scan.

Scan progress—The progress bar shows the status of the running scan.

Target—The name of the currently scanned object and its location.

Detections occurred—Shows the total number of scanned files, threats found and threats cleaned during a scan.

Click More info to show the following information:

- **User**—Name of the user account which started the scan.
- **Objects scanned**—Number of already scanned objects.
- **Duration**—Time elapsed.

Pause icon—Pauses a scan.

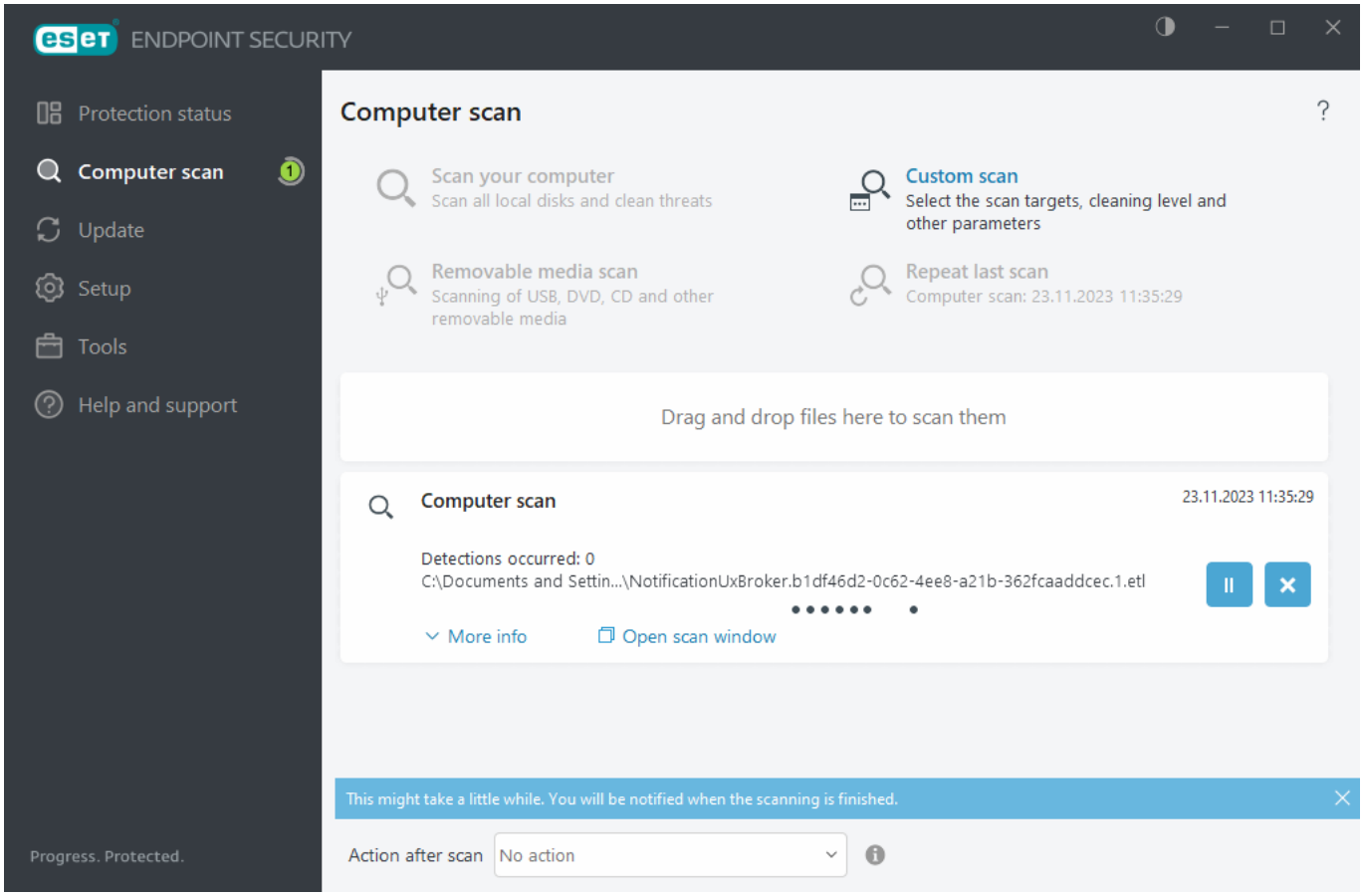
Resume icon—This option is visible when scan progress is paused. Click the icon to continue scanning.

Stop icon—Terminates the scan.

Click **Open Scan window** to open the Computer scan log with more details about the scan.

Scroll scan log—If enabled, the scan log will scroll down automatically as new entries are added so that the most recent entries are visible.

> Click the magnifier or arrow to show details about the scan that is currently running. You can run another parallel scan by clicking **Scan your computer** or **Advanced scans** > **Custom scan**.



Action after scan drop-down menu enables you to set an action to be performed automatically after a scan finishes:

- **No action**—After a scan finishes, no action will be performed.
- **Shut down**—The computer turns off after a scan finishes.
- **Restart if needed**—The computer restarts if only needed to complete cleaning of detected threats.
- **Restart**—Closes all open programs and restarts the computer after a scan finishes.
- **Force restart if needed**—The computer forces restart if only needed to complete cleaning of detected threats.
- **Force restart**— Forces closing of all open programs without waiting for user interaction and restarts the computer after a scan finishes.
- **Sleep**—Saves your session and puts the computer in a low-power state so that you can quickly resume working.
- **Hibernate**—Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down but will resume its previous state the next time you start it.

Sleep or **Hibernate** actions are available based on your computer Power & sleep operating system settings or your computer/laptop capabilities. Remember that a sleeping computer is still a working computer. It is still running basic functions and using electricity when your computer runs on battery power. To preserve battery life, for example, when traveling outside of your office, we recommend using the Hibernate option.

The selected action will start after all of the running scans are finished. When you select **Shutdown** or **Restart**, a confirmation dialog window will display a 30-second countdown (click **Cancel** to deactivate the requested action).

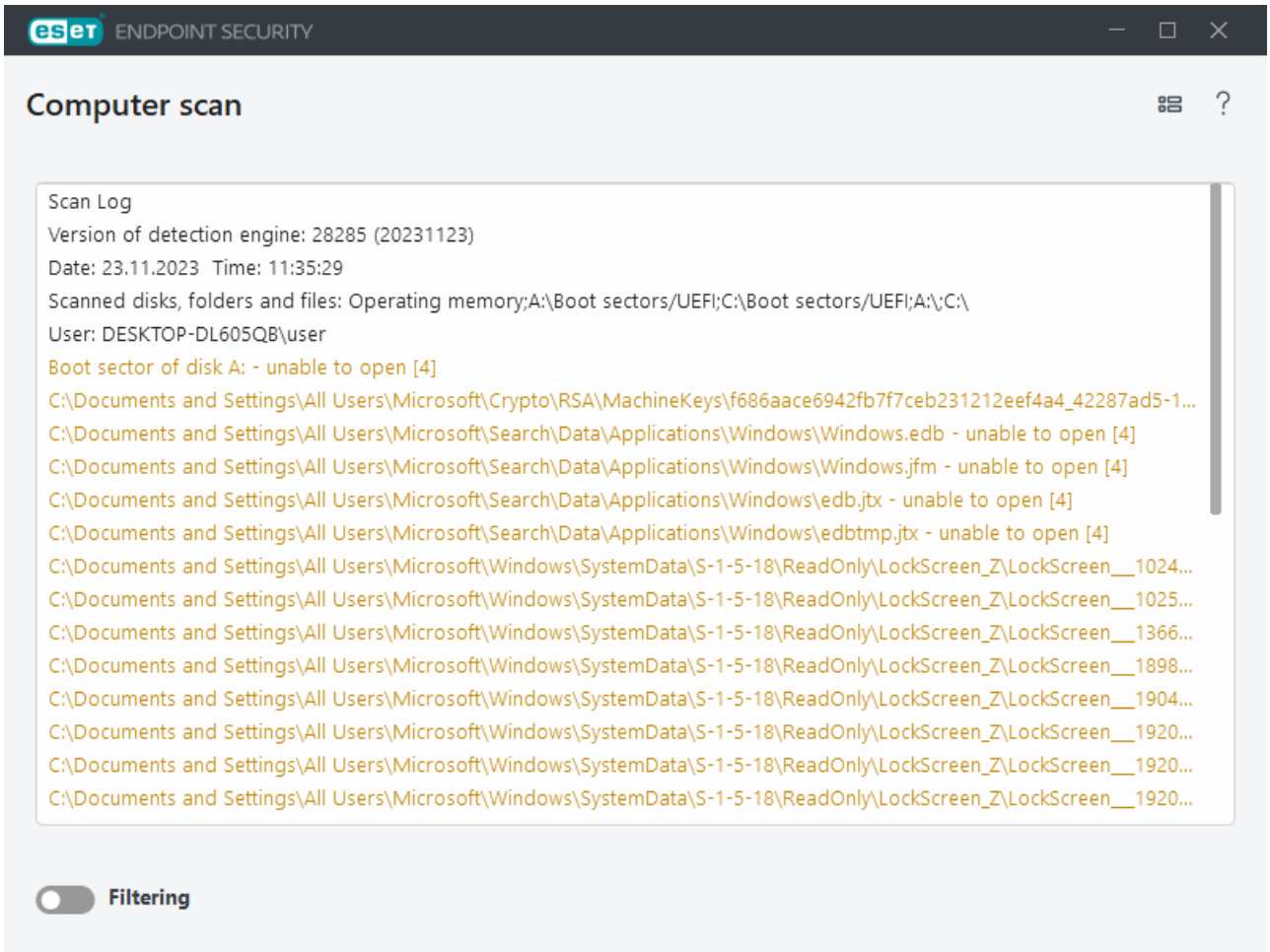
Computer scan log

You can view detailed information related to a specific scan in Log files. Scan log contains the following information:

- Version of detection engine
- Starting date and time
- List of scanned disks, folders, and files
- Scheduled scan name (scheduled scan only)
- User who started the scan.
- Scan status
- Number of scanned objects
- Number of detections found
- Time of completion
- Total scanning time

> A new start of a scheduled computer scan task is skipped if the same scheduled task that was executed earlier is still running. The skipped scheduled scan task will create a Computer scan log with 0 scanned objects and **Scan did not start because the previous scan was still running** status.

To find previous scan logs, in the main program window, select **Tools** > **Log files**. In the drop-down menu, select **Computer scan** and double-click the desired record.



> To learn more about "unable to open", "error opening" and/or "archive damaged" records, see our ESET Knowledgebase article.

Click the toggle icon **Filtering** to open the Log filtering window where you can define custom criteria to narrow your search. To view the context menu, right-click a specific log entry:

Action	Usage
Filter same records	Activates the log filtering. The log will show only records of the same type as the selected one.
Filter	This option opens the Log filtering window and enables you to define criteria for specific log entries. Shortcut: `Ctrl+Shift+F`
Enable filter	Activates the filter settings. If you activate the filter for the first time, you must define settings, and the Log filtering window opens.
Disable filter	Turns the filter off (same as clicking the toggle at the bottom).
Copy	Copies highlighted record(s) into clipboard. Shortcut: `Ctrl+C`
Copy all	Copies all records in the window.
Export	Exports highlighted record(s) into clipboard to an XML file.
Export all	This option exports all records in the window to an XML file.
Detection description	Opens the ESET Threat Encyclopedia, which contains detailed information about the dangers and symptoms of the highlighted infiltration.

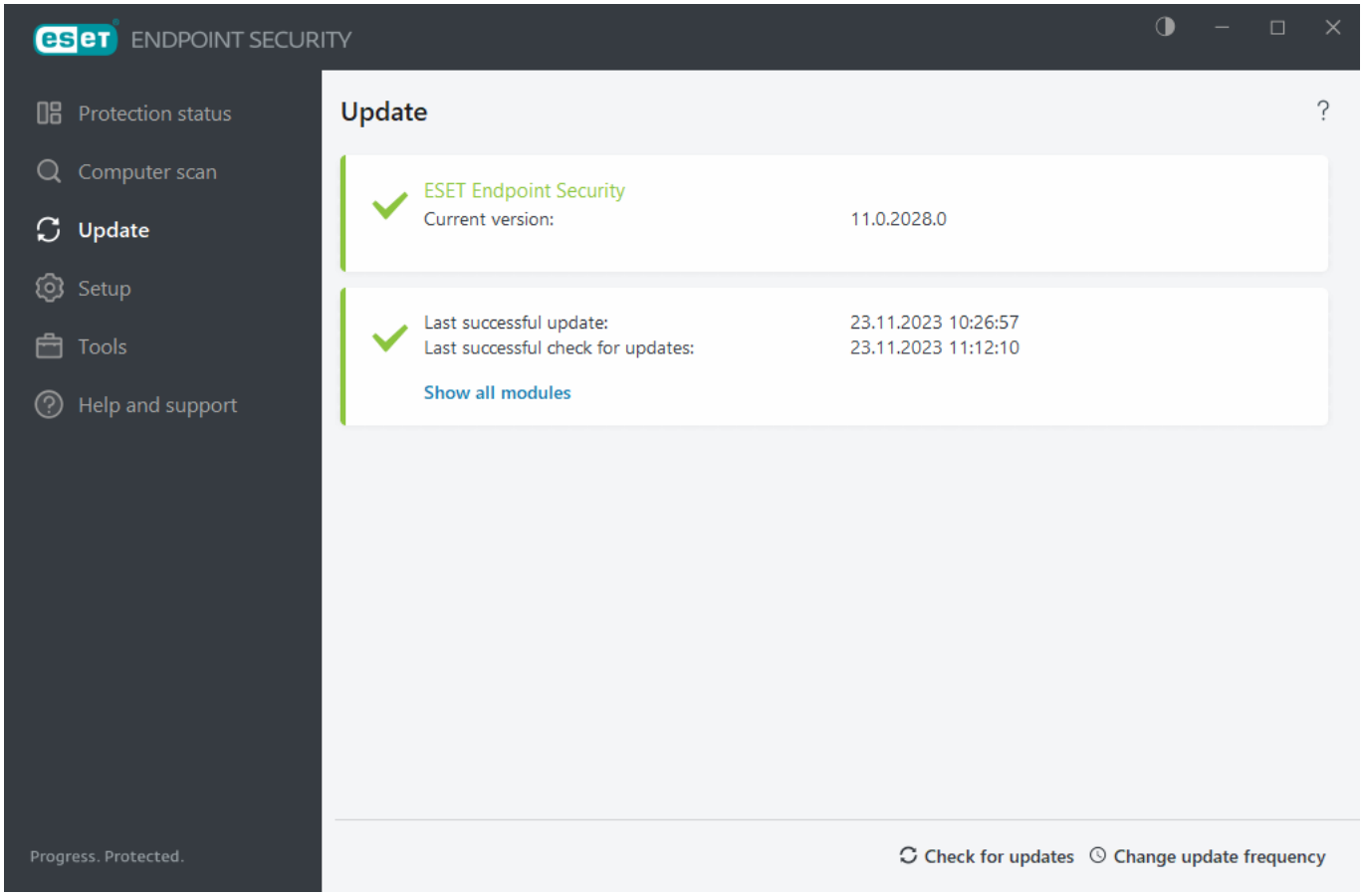
Update

Regularly updating ESET Endpoint Security is the best method to ensure the maximum level of security on your computer. The Update module ensures that both the program modules and the system components are always up-to-date.

By clicking **Update** in the main program window, you can view the current update status including the date and time of the last successful update and if an update is needed.

In addition to automatic updates, you can click **Check for updates** to trigger a manual update. Regularly updating the program modules and components is an important aspect of maintaining complete protection against malicious code. Please pay attention to the product modules configuration and operation. You must activate your product by using your License key to receive updates. If you did not do so during installation, you will need to activate ESET Endpoint Security to access ESET update servers. Your License key was sent to you in an email from ESET after purchasing ESET Endpoint Security.

If you activate ESET Endpoint Security with Offline license file without Username and Password and try to update, the red information **Modules update failed** signals you can download updates from the mirror only.



Current version—The ESET Endpoint Security build number.

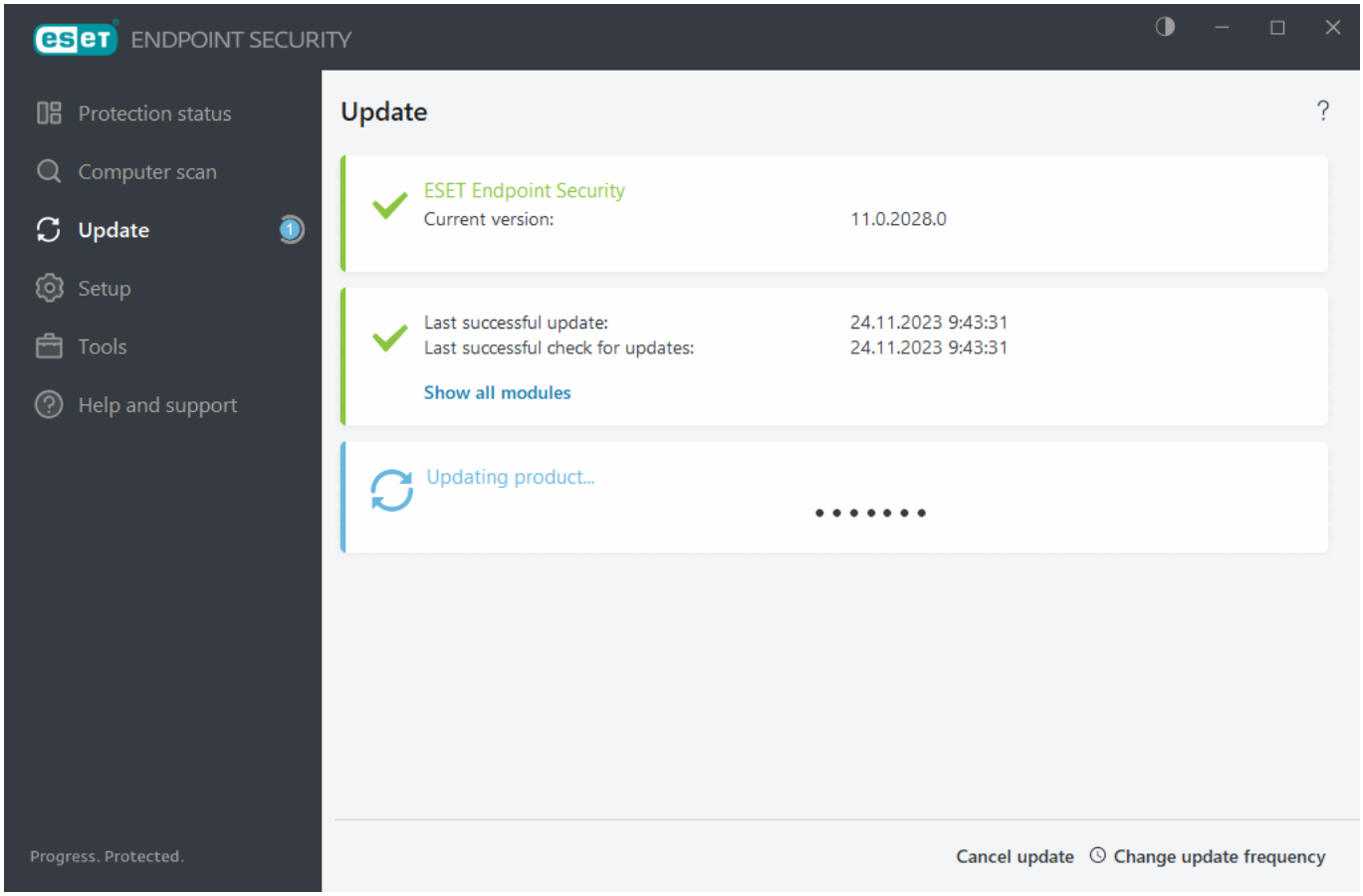
Last successful update—The date and time of the last successful update. Ensure it refers to a recent date, which means that the detection engine is current.

Last successful check for updates—The date and time of the last successful attempt to update modules.

Show all modules—Click the link to open the list of installed modules and check the version and the last update of a module.

Update process

After clicking **Check for updates**, the download process begins. A download progress bar and remaining time to download will be displayed. To interrupt the update, click **Cancel update**.



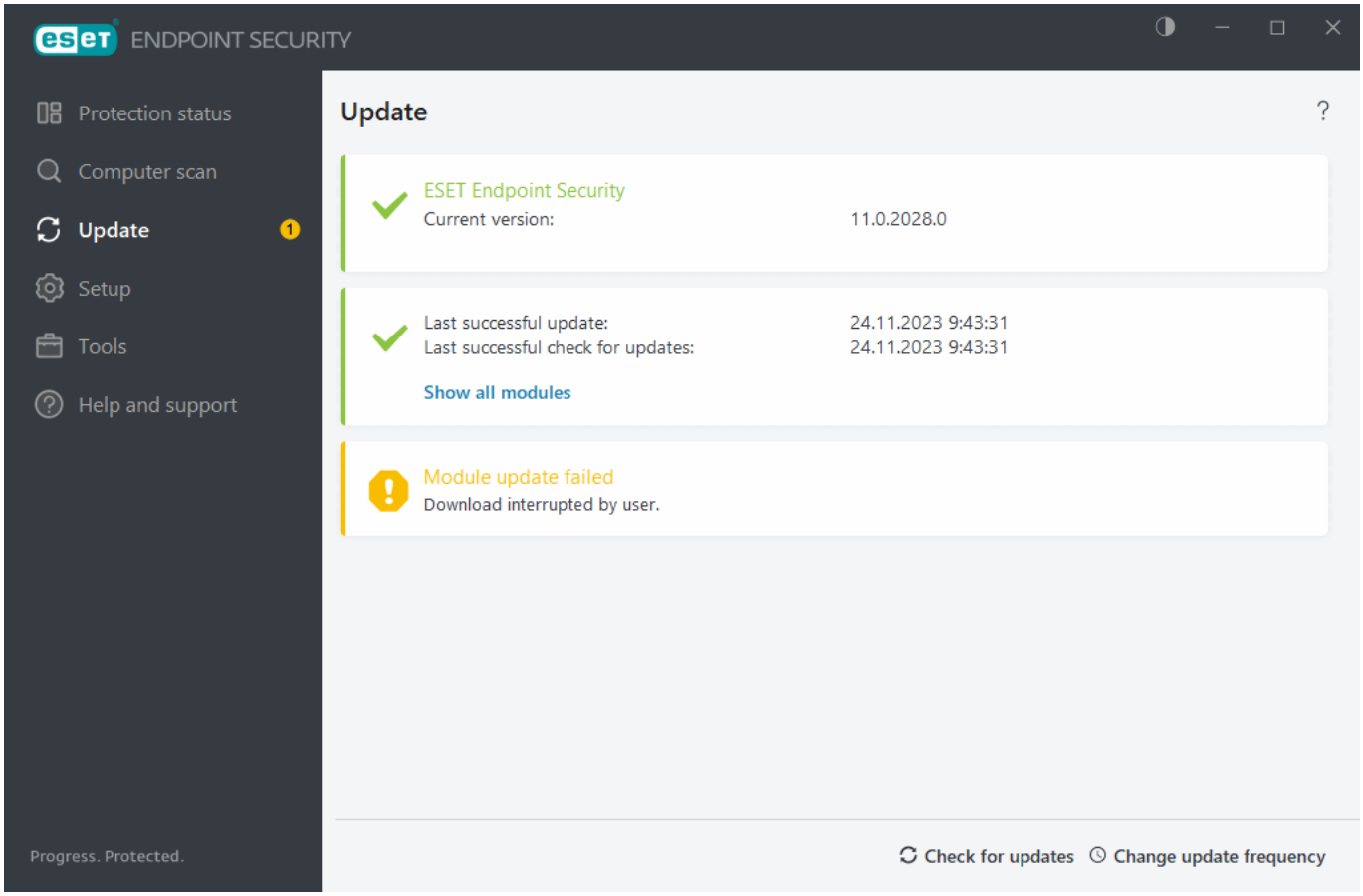
Under normal circumstances, you will see the green check mark in the **Update** window, indicating that the program is up-to-date. If you do not see a green check mark, the program is out-of-date and is more vulnerable to infection. Please update the program modules as soon as possible.

Unsuccessful update

Detection engine out of date—This error will appear after several unsuccessful attempts to update modules. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured connection settings.

The previous notification is related to the following two **Modules update failed** messages about unsuccessful updates:

1. **Invalid license**—Your license is not active. We recommend that you check your authentication data. Click **Help and support** > **Change license** from the main menu to enter a new license key.
2. **An error occurred while downloading update files**—A possible cause of the error is incorrect Internet connection settings. We recommend that you check your internet connectivity (by opening any website in your web browser). If the website does not open, it is likely that an internet connection is not established or there are connectivity problems with your computer. Ensure you have an active internet connection from your Internet Service Provider (ISP).



For more information, see the ESET Knowledgebase article.

How to create update tasks

Updates can be triggered manually by clicking **Check for updates** in the primary window displayed after clicking **Update** from the main menu.

Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following update tasks are activated in ESET Endpoint Security:

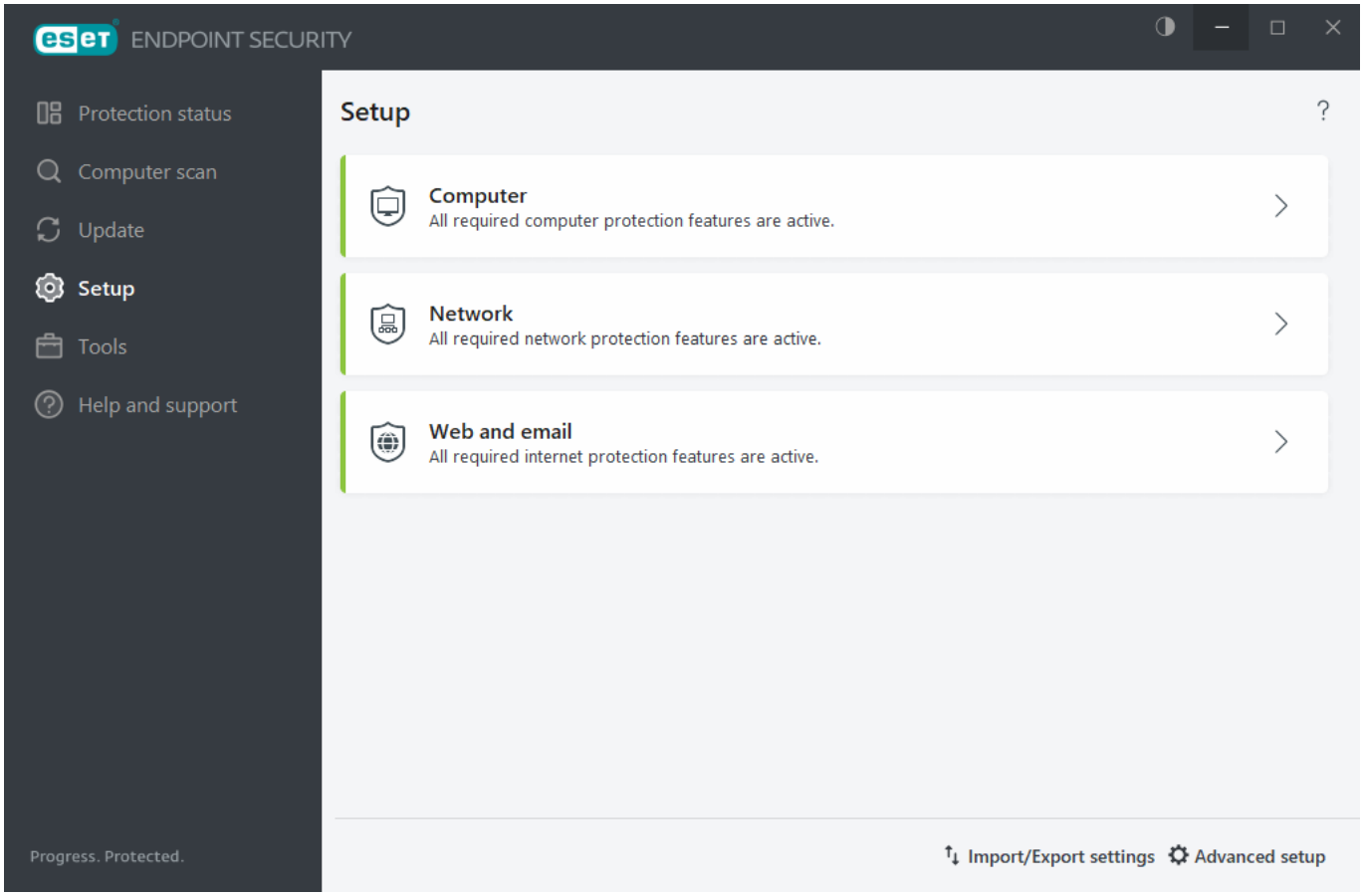
- **Regular automatic update**
- **Automatic update after user logon**

Each update task can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see section Scheduler.

Setup

You can find groups of available protection features in the main program window > **Setup**.

When creating a policy from ESET PROTECT On-Prem Web Console you can select the flag for each setting. Settings with the Force flag have priority and cannot be overwritten by a later policy (even if the later policy has a Force flag). This assures that this setting will not be changed (e.g. by user or by later policies during merging). For more information see Flags in ESET PROTECT On-Prem Online Help.



The **Setup** menu contains the following sections:

Computer

Network

Web and Email

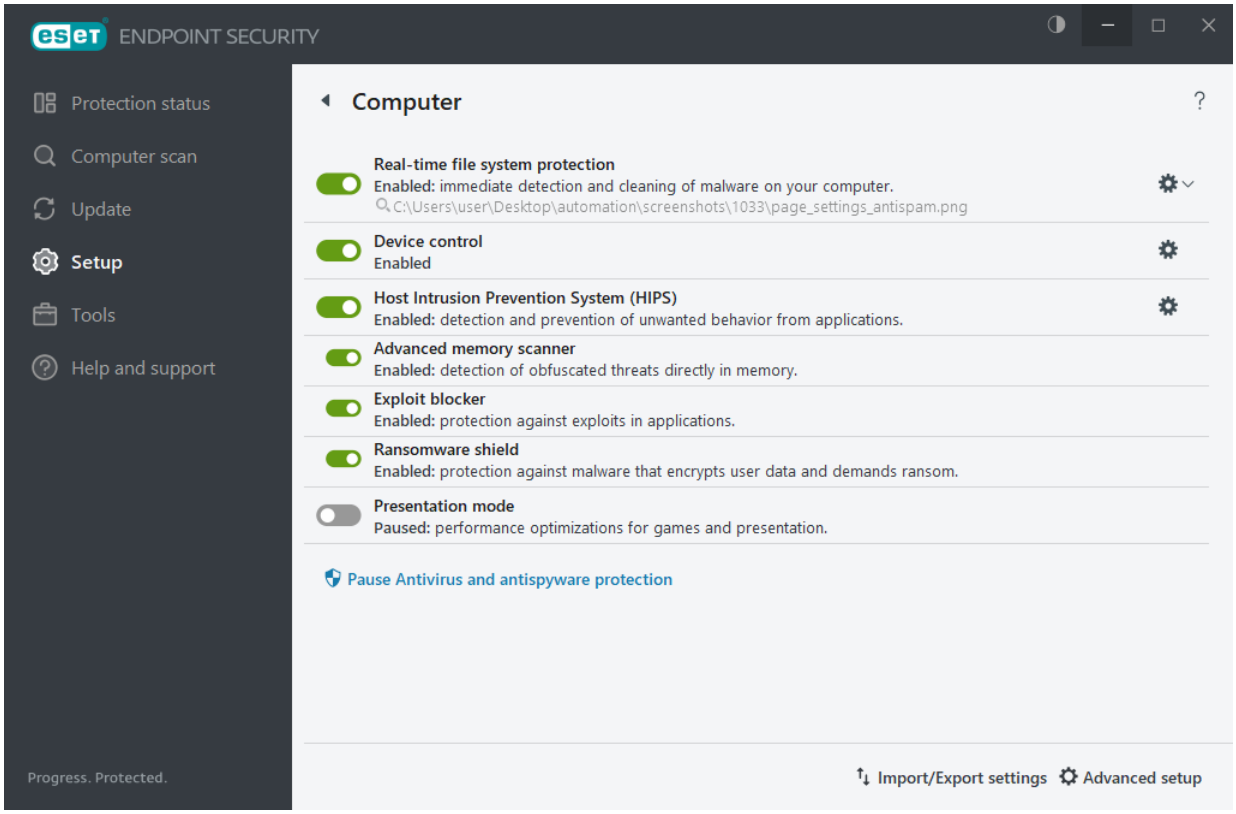
When ESET PROTECT On-Prem policy is applied, you will see the lock icon next to a specific component. The policy applied by ESET PROTECT On-Prem can be overridden locally after authentication by logged user (e.g. administrator). For more information see the ESET PROTECT On-Prem Online Help.

All protective measures disabled this way will be re-enabled after a computer restart.

Additional options are available at the bottom of the setup window. Click Advanced setup to configure more detailed parameters for each module. Use Import/Export settings to load setup parameters using an .xml configuration file, or to save your current setup parameters to a configuration file.

Computer

Click **Computer** in the main program window > **Setup** to see an overview of all protection modules:



In the **Computer** section you can enable or disable the following components:

- Real-time file system protection—All files are scanned for malicious code when they are opened, created or run on your computer. Click the gear icon next to Real-time file system protection and click Edit exclusions to open the Exclusion setup window and exclude files and folders from scanning. To open Real-time file system protection advanced setup, click Configure.
- Device control—Provides automatic device (CD/DVD/USB/...) control. This module enables you to block or adjust extended filters/permissions and define a users ability to access and work with a given device.
- Host Intrusion Prevention System (HIPS)—The HIPS system monitors events that occur within the operating system and reacts to them according to a customized set of rules.
- **Advanced memory scanner**—Works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced memory scanner is enabled by default. Read more about this type of protection in the glossary.
- **Exploit blocker**—Designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and Microsoft Office components. Exploit blocker is enabled by default. Read more about this type of protection in the glossary.
- **Ransomware shield**—It is another layer of protection that works as a part of HIPS feature. You must have the ESET LiveGrid® reputation system enabled for Ransomware shield to work. Read more about this type of protection.
- Presentation mode—A feature for users that demand uninterrupted usage of their software, do not want to be disturbed by notifications, and want to minimize CPU usage. You will receive a warning message (potential security risk) and the main program window will turn orange after enabling Presentation mode.

Pause Antivirus and antispyware protection—Any time that you temporarily disable Antivirus and antispyware protection, you can select the period of time for which you want the selected component to be disabled using the drop-down menu and then click **Apply** to disable the security component. To re-enable protection, click **Enable Antivirus and antispyware protection**.

To pause or disable individual protection modules, click the toggle icon .

Turning off protection modules may decrease the protection level of your computer.

A Threat is detected

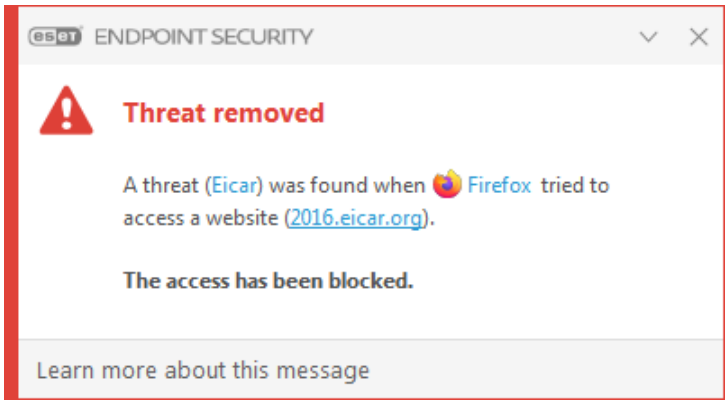
Infiltrations can reach the system from various entry points such as web pages, shared folders, via email or from removable devices (USB, external disks, CDs, DVDs, etc.).

Standard behavior

As a general example of how infiltrations are handled by ESET Endpoint Security, infiltrations can be detected using:

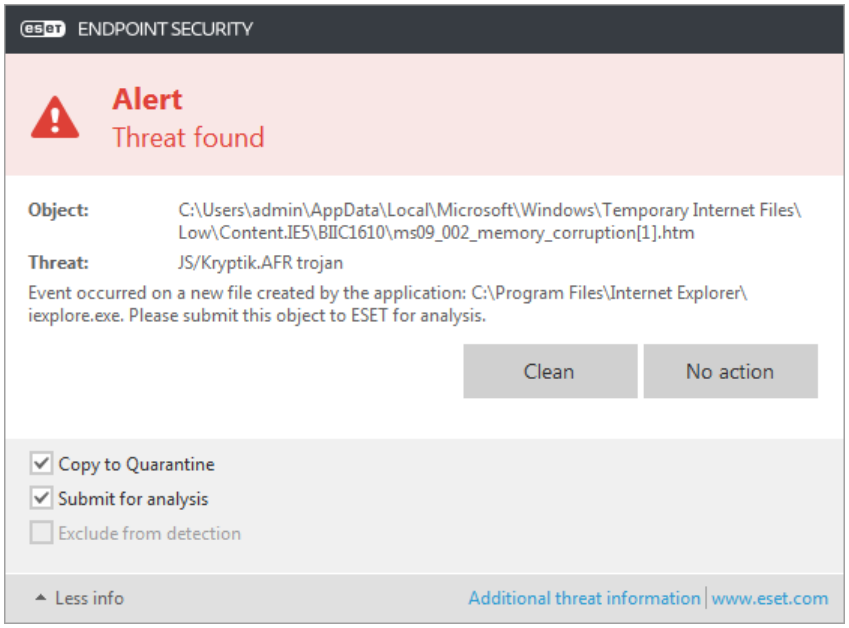
- Real-time file system protection
- Web access protection
- Email client protection
- On-demand computer scan

Each uses the standard cleaning level and will attempt to clean the file and move it to Quarantine or terminate the connection. A notification window is displayed in the notification area at the bottom right corner of the screen. For detailed information about the detected/cleaned objects, see Log files. For more information about cleaning levels and behavior, see Cleaning.



Cleaning and deleting

If there is no pre-defined action to take for Real-time file system protection, you will be prompted to select an option in the alert window. Usually the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, as this will leave infected files uncleaned. The exception to this is when you are sure that a file is harmless and has been detected by mistake.



Apply cleaning if a file has been attacked by a virus that has attached malicious code to the file. If this is the case, first attempt to clean the infected file to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.

If an infected file is “locked“ or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

Restoring from the Quarantine

The Quarantine can be accessed from the ESET Endpoint Security main program window by clicking **Tools** > **Quarantine**.

Quarantined files can also be restored to their original location:

- Use the **Restore** feature for this purpose, which is available from the context menu by right-clicking a given file in the Quarantine.
- If a file is marked as a potentially unwanted application, the **Restore and exclude from scanning** option is enabled. See also Exclusions.
- The context menu also offers the **Restore to** option, to restore a file to a location other than the one from which it was deleted.
- The restore functionality is not available in some cases, for example, for files located on a read-only network share.

Multiple threats

If any infected files were not cleaned during Computer scan (or the Cleaning level was set to **No Cleaning**), an alert window prompting you to select action for those files is displayed.

Deleting files in archives

In Default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. Use caution when performing a Strict cleaning scan, with Strict cleaning enabled an archive will be deleted if it contains at least one infected file regardless of the status of other files in the archive.

If your computer is showing signs of a malware infection, for example, it is slower, often freezes, etc., we recommend that you do the following:

- Open ESET Endpoint Security and click Computer scan
- Click **Smart scan** (for more information, see Computer scan)
- After the scan has finished, review the log for the number of scanned, infected and cleaned files

If you only want to scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.

Network

Open the main program window > **Setup** > **Network** to configure basic Network protection settings or troubleshoot network communication.

To pause or disable individual protection modules, click the toggle icon  .

⚠ Turning off protection modules may decrease the protection level of your computer.

Click the gear icon ⚙ next to a protection module to access advanced settings.

Firewall—Filters all network communication based on the ESET Endpoint Security configuration.

Configure—Opens the Firewall Advanced setup, where you can define how the firewall handles network communication.

Pause firewall (allow all traffic)—The opposite of blocking all network traffic. If selected, all firewall filtering options are turned off, and all incoming and outgoing connections are permitted. Click **Enable firewall** to re-enable the firewall while network traffic filtering is in this mode.

Block all traffic—All inbound and outbound communication is blocked by the firewall. Only use this option if you suspect a critical security risk that requires the system to be disconnected from the network. While Network traffic filtering is in **Block all traffic** mode, click **Stop blocking all traffic** to restore normal firewall operation.

Automatic mode (when another filtering mode is enabled)—Click to change the filtering mode to automatic (with user-defined rules).

Interactive mode (when another filtering mode is enabled)—Click to change the filtering mode to interactive.

Network attack protection (IDS)—Analyzes the content of network traffic and protects from network attacks. Any traffic considered harmful is blocked. ESET Endpoint Security informs you when you connect to an unprotected wireless network or a network with weak protection.

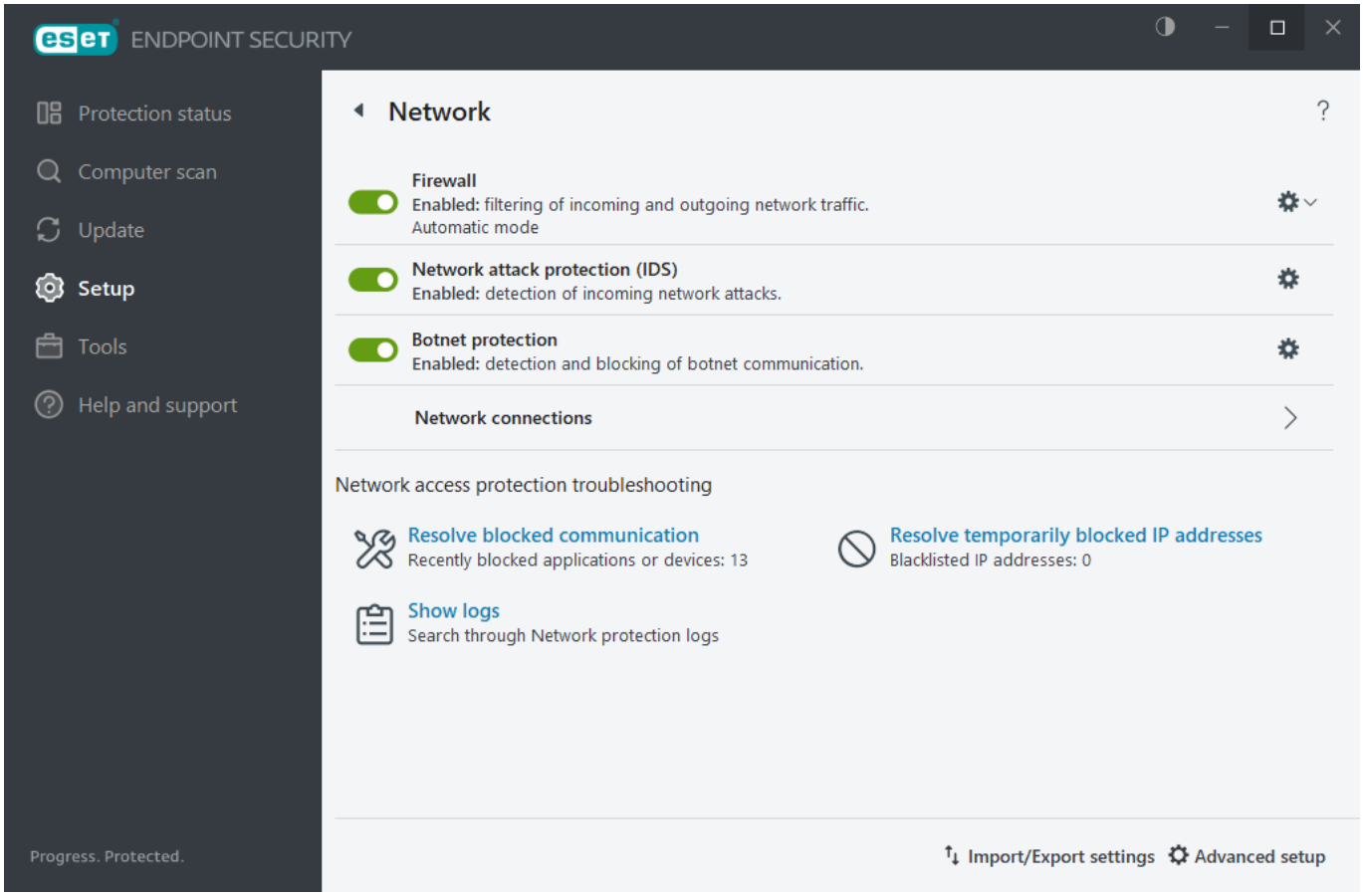
Botnet protection—Identifies malware in the system quickly and accurately.

Network connections—Shows the networks where network adapters are connected with detailed information.

Resolve blocked communication—Helps you solve connectivity problems caused by ESET Firewall. For more detailed information, refer to the Troubleshooting wizard.

Resolve temporarily blocked IP addresses—Shows a list of IP addresses detected as the source of attacks and added to the blacklist to block connections for a certain period.

Show logs— Opens the network protection Log file.



Network connections

Shows the networks to which network adapters are connected. To see network connections, open the main program window > **Setup** > **Network** > **Network connections**.

Double-click a connection in the list to show its details and Network adapter details.

Hover over a specific network connection and click the menu icon ⋮ in the **Trusted** column to choose one of the following options:

- **Edit**—Opens the Configure network protection window where you can assign a Network protection profile to the specific network.
- **Forget**—Resets the network connection configuration to default.

Network connection details

Double-click a connection in the list of Network connections to show its details together with network adapter details. Network connection and adapter details can help you identify the network you are trying to configure in Network access protection.

Network connection details:

- Status of the network connection

- Date and time of the first network detection
- Last time the network was active
- Total time spent connected to this network
- Network connection profile
- Network connection profile defined in Windows
- Network protection configuration (whether the network is trusted)

Network adapter details:

- Type of the connection (wired, virtual, etc.)
- Network adapter name
- Adapter description
- IP address with MAC address
- The IPv4 and IPv6 address of the network with subnet
- DNS suffix
- DNS server IP
- DHCP server IP
- Default gateway IP and MAC address
- Adapter MAC address

Network access troubleshooting

Troubleshooting wizard helps you resolve connectivity problems caused by the Firewall. **Network access troubleshooting** can be found in the main program window > **Setup** > **Network** > **Resolve blocked communication**.

Select if you want to show communication blocked for **Local applications** or blocked communication from **Remote devices**.

From the drop-down menu, select a period of time during which communication has been blocked. A list of recently blocked communications gives you an overview of the type of application or device, its reputation, and the total number of applications and devices blocked during that time period. For more details about blocked communication, click **Details**. The next step is to unblock the application or device on which you are experiencing connectivity problems.

When you click **Unblock**, the previously blocked communication will be allowed. If you continue to experience problems with an application or your device does not work as expected, click **creating another rule**, and all communications previously blocked for that device will now be allowed. If the issue persists, restart the computer.

Click **Open Firewall rules** to see rules created by the wizard. Additionally, you can see rules created by the wizard in Advanced setup > **Protections** > **Network access protection** > **Firewall** > **Rules** > **Edit**.

The following ESET Knowledgebase article may only be available in English:
- Add a firewall exception using the Troubleshooting wizard

If the rule cannot be created, you will receive an error message. Click **Try again** and repeat the process to unblock communication, or create another rule from the list of blocked communication.

Temporary IP address blacklist

To view IP addresses that have been detected as sources of attacks and have been added to the blacklist to block connection for a certain period of time, open the main program window > **Setup** > **Network protection** > **Resolve temporarily blocked IP addresses**. Temporarily blocked IP addresses are blocked for 1 hour.

Columns

IP address— shows an IP address that has been blocked.

Block reason—shows type of attack that has been prevented from the address (for example TCP Port Scanning attack).

Timeout—shows time and date when the address will expire from the black list.

Control elements

Remove—click to remove an address from the blacklist before it will expire.

Remove all—click to remove all addresses from the blacklist immediately.

Add exception—click to add an firewall exception into IDS filtering.

Network protection logs

The ESET Endpoint Security Network protection saves all important events in a log file. To view the log file, open the main program window > **Setup** > **Network** > **Show logs**.

The log files can be used to detect errors and reveal intrusions into your system. Network protection logs contain the following data:

- Date and time of the event
- Name of event
- Source
- Target network address
- Network communication protocol
- The rule applied, or name of a worm, if identified
- Application path and name
- Hash
- User
- Signer of the application (publisher)
- Package name
- Name of the service

A thorough analysis of this data can help detect attempts to compromise system security. Many other factors indicate potential security risks and enable you to minimize their impact: frequent connections from unknown locations, multiple attempts to establish connections, unknown applications communicating or unusual port numbers used.

> **Security vulnerability exploitation**
> The message of security vulnerability exploitation is logged even if the specific vulnerability is already patched since the exploitation attempt is detected and blocked on the network level before actual exploitation can happen.

Solving problems with ESET Network Protection

If you experience connectivity problems with ESET Endpoint Security installed, there are several ways to tell if the ESET Network Protection is causing the issue. Moreover, ESET Network Protection can help you create new rules or exceptions to resolve connectivity problems.

See the following topics for help resolving problems with the ESET Network Protection:

- Network access troubleshooting
- Logging and creating rules or exceptions from log
- Creating exceptions from firewall notifications
- Network protection advanced logging
- Solving problems with Network traffic scanner

Logging and creating rules or exceptions from log

By default, the ESET Firewall does not log all blocked connections. If you want to see what was blocked by the Network protection, Open Advanced setup > **Tools** > **Diagnostics** > **Advanced logging** and enable **Enable Network protection advanced logging**. If you see something in the log that you do not want the Firewall to block, you can create a rule or an IDS rule for it by right-clicking on that item and selecting **Don't block similar events in the future**. Please note that the log of all blocked connections can contain thousands of items and it might be difficult to find a specific connection in this log. You can turn logging off after you have resolved your issue.

For more information about the log see Log files.

> Use logging to see the order in which the Network protection blocked specific connections. Moreover, creating rules from the log enables you to create rules that do exactly what you want.

Create rule from log

The new version of ESET Endpoint Security enables you to create a rule from the log. From the main menu click **Tools** > **Log files**. Choose **Network protection** from drop-down menu, right-click your desired log entry and select **Don't block similar events in the future** from the context menu. A notification window will display your new rule.

To allow for the creation of new rules from the log, ESET Endpoint Security must be configured with the following settings:

1. Set the minimum logging verbosity to **Diagnostic** in Advanced setup > **Tools** > **Log files**.
2. Enable **Notify about incoming attacks against security holes** in Advanced setup > **Protections** > **Network access protection** > **Network attack protection** > **Advanced options** > **Intrusion detection**.

Creating exceptions from firewall notifications

When ESET Firewall detects malicious network activity, a notification window describing the event will be displayed. This notification contains a link to learn more about the event and set up an exception for this event if you want.

> If a network application or device does not implement network standards correctly it can trigger repetitive firewall IDS notifications. You can create an exception directly from the notification to keep the ESET Firewall from detecting this application or device.

Network protection advanced logging

This feature is intended to provide more complex log files for ESET Technical support. Use this feature only when requested to by ESET Technical support, as it might generate a huge log file and slow down your computer.

1. Open Advanced setup > **Tools** > **Diagnostics** and enable **Enable Network protection advanced logging**.
2. Attempt to reproduce the problem you are experiencing.
3. Disable Network protection advanced logging.
4. The PCAP log file created by Network protection advanced logging can be found in the same directory where diagnostic memory dumps are generated: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Solving problems with Network traffic scanner

If you experience problems with your browser or email client, the first step is determining if Network traffic scanner is responsible. To do that, try temporarily disabling Network traffic scanner in Advanced setup > **Detection engine** > **Network traffic scanner** (remember to turn it back on after you are finished, otherwise, your browser and email client will remain unprotected). If your problem disappears after turning it off, here is a list of common problems and a way to solve them:

Update or secure communication problems

If your application complains about the inability to update or that a communication channel is not secure:

- If you have SSL/TLS enabled, try temporarily turning it off. If that helps, you can keep using SSL/TLS and make the update work by excluding the problematic communication:
  Disable SSL/TLS. Rerun the update. There should be a dialog informing you about encrypted network traffic. Ensure the application matches the one you are troubleshooting, and the certificate looks like coming from the server it is updating from. Then choose to remember the action for this certificate and click ignore. If no more relevant dialogs are shown, you can switch the filtering mode back to automatic, and the problem should be solved.
- If the application in question is not a browser or email client, you can completely exclude it from Web access protection (doing this for the browser or email client would leave you exposed). Any application that had its communication filtered in the past should already be in the list provided to you when adding an exception, so manually adding one should not be necessary.

Problem accessing a device on your network

If you cannot use any device's functionality on your network (this could mean opening a web page of your webcam or playing video on a home media player), try adding its IPv4 and IPv6 addresses to the list of excluded addresses.

Problems with a specific website

You can exclude specific websites from Web access protection using URL address management. For example, if you cannot access https://www.gmail.com/intl/en/mail/help/about.html, try adding *gmail.com* to the list of excluded addresses.

Error "Some of the applications capable of importing the root certificate are still running"

When you enable SSL/TLS, ESET Endpoint Security ensures that installed applications trust the way it filters SSL protocol by importing a certificate to their certificate store. Some applications may require a restart to import a certificate. This includes Firefox and Opera. Verify that none of them are running (the best way to do this is to open Task Manager and ensure there is no firefox.exe or opera.exe under the Processes tab), then hit retry.

Error about an untrusted issuer or invalid signature

This most likely means that the import described above failed. First, ensure that none of the mentioned applications are running. Then disable SSL/TLS and enable it back on. This reruns the import.

Network threat blocked

This situation can occur when a port scanning attempt on your system is detected or when an application on your computer tries to transmit malicious traffic to another device on the network or exploit a security hole.

You can find the type of threat and the related device IP address in the notification. Click **Change handling of this threat** to show the following options:

Continue blocking—Blocks detected threat. If you want to stop receiving notifications about this type of threat from the specific remote address, select the radio button next to **Do not notify** before you click **Continue blocking**. This will create an Intrusion Detection Service (IDS) rule with the following configuration: **Block** - default, **Notify** - no, **Log** - no.

Allow—Creates an Intrusion Detection Service (IDS) rule to allow the detected threat. Select one from the following options before you click **Allow** to specify the rule settings:

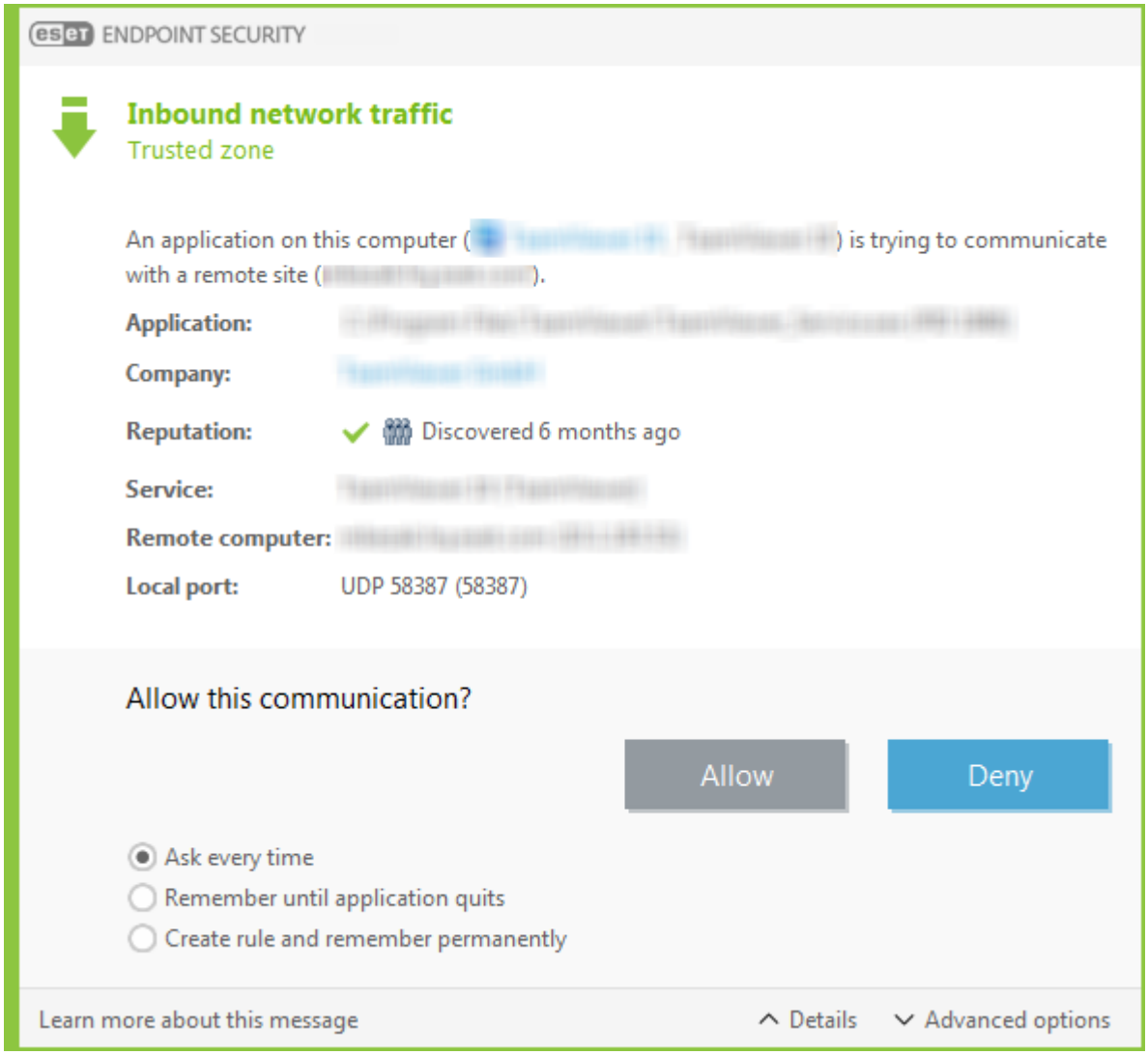
- **Notify only when this threat is blocked**—Rule configuration: **Block** - no, **Notify** - no, **Log** - no.
- **Notify whenever this threat occurs**—Rule configuration: **Block** - no, **Notify** - default, **Log** - default.
- **Do not notify**—Rule configuration: **Block** - no, **Notify** - no, **Log** - no.

> The information shown in this notification window may vary depending on the type of threat detected. For more information about threats and other related terms, see Types of remote attacks or Types of detections.
> To resolve the **Duplicate IP addresses on network** event, see our ESET Knowledgebase article.

Establishing connection – detection

The Firewall detects each newly-created network connection. The active firewall mode determines which actions are performed for the new rule. If **Automatic mode** or **Policy-based mode** is activated, the Firewall will perform pre-defined actions with no user interaction.

The **Interactive mode** displays an informational window that reports the detection of a new network connection with detailed information about the connection. You can choose to **Allow** or **Deny** (block) the connection. If you repeatedly allow the same connection in the dialog window, we recommend that you create a new rule for the connection. Select **Create rule and remember permanently** to save the action as a new rule for the Firewall. If the Firewall recognizes the same connection in the future, it will apply the existing rule without requiring user interaction.



When creating new rules, only allow connections that you know are secure. If all connections are allowed, the Firewall fails to accomplish its purpose. These are the important parameters for connections:

Application—Executable file location and process ID. Do not allow connections for unknown applications and processes.

Signer—Application's publisher name. Click the text to show a security certificate for the company.

Reputation—Risk level of the connection. Connections are assigned a risk level: Fine (green), Unknown (orange)

or Risky (red), by using a series of heuristic rules that examine the characteristics of each connection, the number of users, and discovery time. This information is gathered by ESET LiveGrid® technology.

Service—Name of the service, if the application is a windows service.

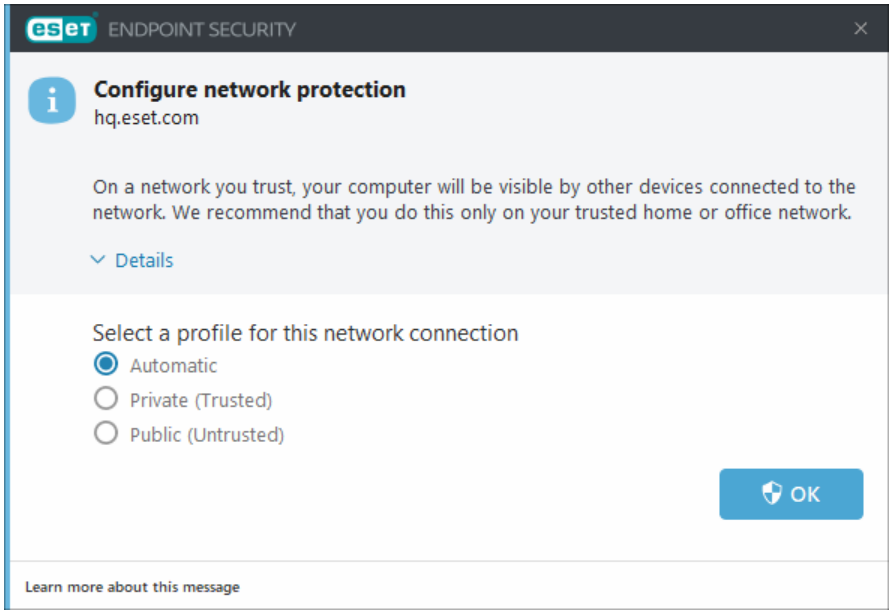
Remote computer—Address of the remote device. Only allow connections to trusted and known addresses.

Remote port—Communication port. Communication on common ports (e.g., web traffic – port number 80,443) can be allowed under normal circumstances.

Computer infiltrations often use the internet and hidden connections to help them infect remote systems. If rules are configured correctly, a Firewall becomes a useful tool for protection against a variety of malicious code attacks.

New network detected

By default, ESET Endpoint Security uses Windows settings when a new network connection is detected. To display a dialog window when a new network is detected, change the Network protection profile assignment to **Ask**. Network protection configuration will be displayed whenever your computer connects to a new network.



You can select from the following Network connection profiles:

Automatic—ESET Endpoint Security will select the profile automatically, based on the Activators configured for each profile.

Private—For trusted networks (home or office network). Your computer and shared files stored on your computer are visible to other network users, and system resources are accessible to other users on the network (access to shared files and printers is enabled, incoming RPC communication is enabled and remote desktop sharing is available). We recommend using this setting when accessing a secure local network. This profile is automatically assigned to a network connection if it is configured as Domain or Private network in Windows.

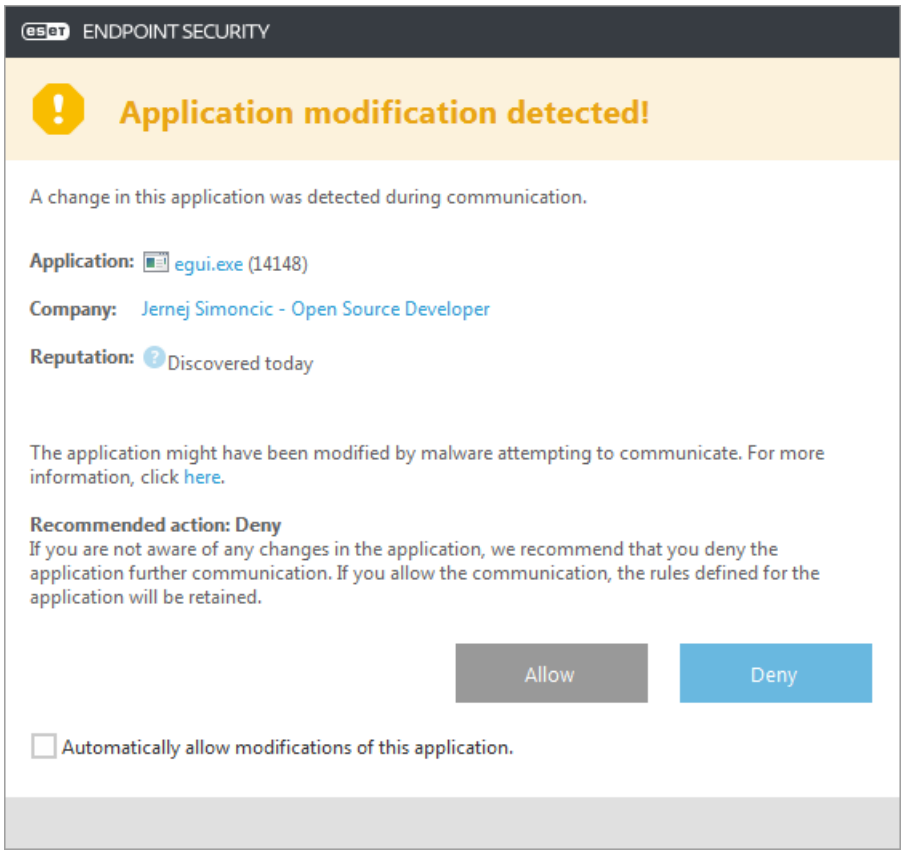
Public—For untrusted networks (public network). Files and folders on your system are not shared with or visible to other users on the network, and system resource sharing is deactivated. We recommend using this setting when accessing wireless networks. This profile is automatically assigned to any network connection that is not configured as Domain or Private network in Windows.

User-defined profile—You can select one of the profiles you have created from the drop-down menu. This option is available only if you have created at least one custom profile.

⚠ An incorrect network configuration may pose a security risk to your computer.

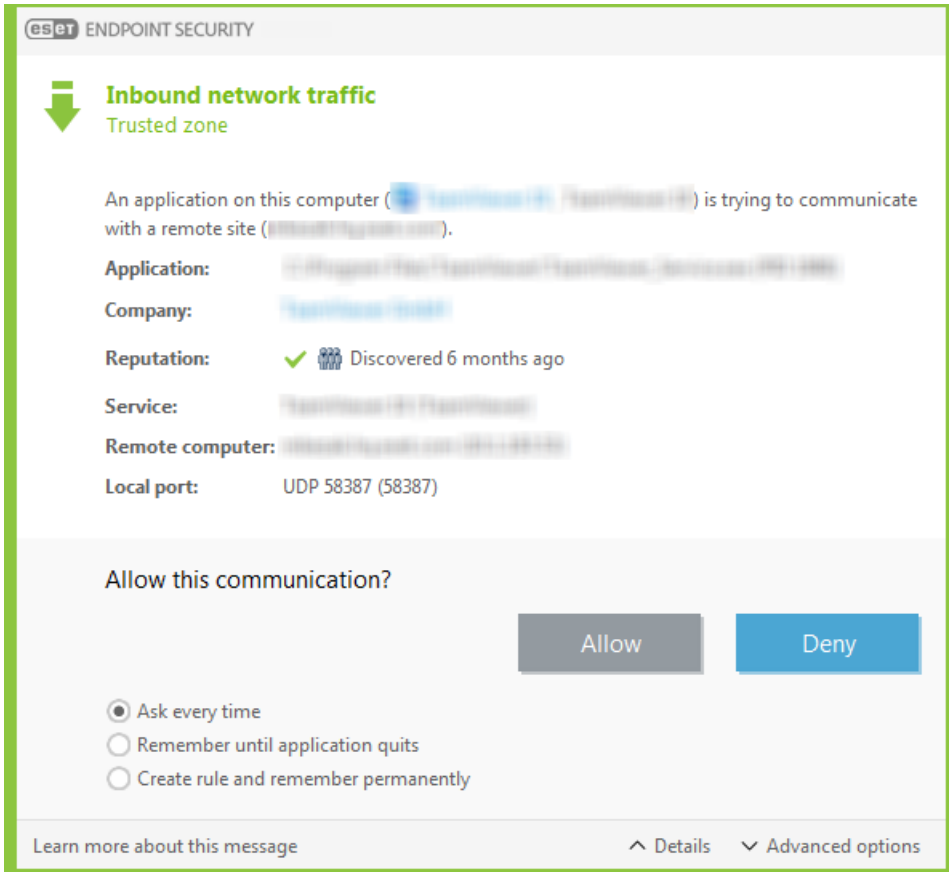
Application change

The firewall has detected a modification in an application which is used to establish outgoing connections from your computer. It is possible that the application has simply been updated to a new version. On the other hand, a modification can be caused by a malicious application. If you are not aware of any legitimate modification, we recommend that you deny the connection and scan your computer using the most recent version of detection engine. If you are sure of any modification and allow the communication with selected **Automatically allow modifications of this application** check box, the rule applied for this application will be retained.



Incoming trusted communication

Example of an incoming connection within the trusted zone:
A remote computer from within the trusted zone attempting to establish communication with a local application running on your computer.



Application—Application contacted by a remote device.

Application path—Location of the application.

Microsoft store application—Name of the application in Microsoft store.

Signer—Application's publisher name. Click the text to show a security certificate for the company.

Reputation—Reputation of the application as obtained by ESET LiveGrid® technology.

Service—Name of the service that is currently running on your computer.

Remote computer—Remote computer trying to establish communication with the application on your computer.

Remote port—Port used for the communication.

Ask every time—If the default action for a rule is set to **Ask**, a dialog window will be displayed each time that the rule is triggered.

Remember until application quits—ESET Endpoint Security will remember the chosen action until the next restart.

Create rule and remember permanently—If you select this option before allowing or denying a communication, ESET Endpoint Security will remember the action and use it if the application is contacted by the remote computer again.

Allow—Allows the incoming communication.

Deny—Denies the incoming communication.

Edit rule—Enables you to customize rule properties using the Firewall rule editor.

Outgoing trusted communication

Example of an outgoing connection within the trusted zone:
A local application attempting to establish a connection to another computer within the local network, or within a network in the trusted zone.

Application—Application contacted by a remote device.

Application path—Location of the application.

Microsoft store application—Name of the application in Microsoft store.

Signer—Application's publisher name. Click the text to show a security certificate for the company.

Reputation—Reputation of the application as obtained by ESET LiveGrid® technology.

Service—Name of the service that is currently running on your computer.

Remote computer—Remote computer trying to establish communication with the application on your computer.

Remote port—Port used for the communication.

Ask every time—If the default action for a rule is set to **Ask**, a dialog window will be displayed each time that the rule is triggered.

Remember until application quits—ESET Endpoint Security will remember the chosen action until the next restart.

Create rule and remember permanently—If you select this option before allowing or denying a communication, ESET Endpoint Security will remember the action and use it if the application is contacted by the remote computer again.

Allow—Allows the incoming communication.

Deny—Denies the incoming communication.

Edit rule—Enables you to customize rule properties using the Firewall rule editor.

Incoming communication

Example of an incoming internet connection:
A remote computer attempting to communicate with an application running on the computer.

Application—Application contacted by a remote device.

Application path—Location of the application.

Microsoft store application—Name of the application in Microsoft store.

Signer—Application's publisher name. Click the text to show a security certificate for the company.

Reputation—Reputation of the application as obtained by ESET LiveGrid® technology.

Service—Name of the service that is currently running on your computer.

Remote computer—Remote computer trying to establish communication with the application on your computer.

Remote port—Port used for the communication.

Ask every time—If the default action for a rule is set to **Ask**, a dialog window will be displayed each time that the rule is triggered.

Remember until application quits—ESET Endpoint Security will remember the chosen action until the next restart.

Create rule and remember permanently—If you select this option before allowing or denying a communication, ESET Endpoint Security will remember the action and use it if the application is contacted by the remote computer again.

Allow—Allows the incoming communication.

Deny—Denies the incoming communication.

Edit rule—Enables you to customize rule properties using the Firewall rule editor.

Outgoing communication

Example of an outgoing internet connection:
A local application trying to establish an internet connection.

Application—Application contacted by a remote device.

Application path—Location of the application.

Microsoft store application—Name of the application in Microsoft store.

Signer—Application's publisher name. Click the text to show a security certificate for the company.

Reputation—Reputation of the application as obtained by ESET LiveGrid® technology.

Service—Name of the service that is currently running on your computer.

Remote computer—Remote computer trying to establish communication with the application on your computer.

Remote port—Port used for the communication.

Ask every time—If the default action for a rule is set to **Ask**, a dialog window will be displayed each time that the rule is triggered.

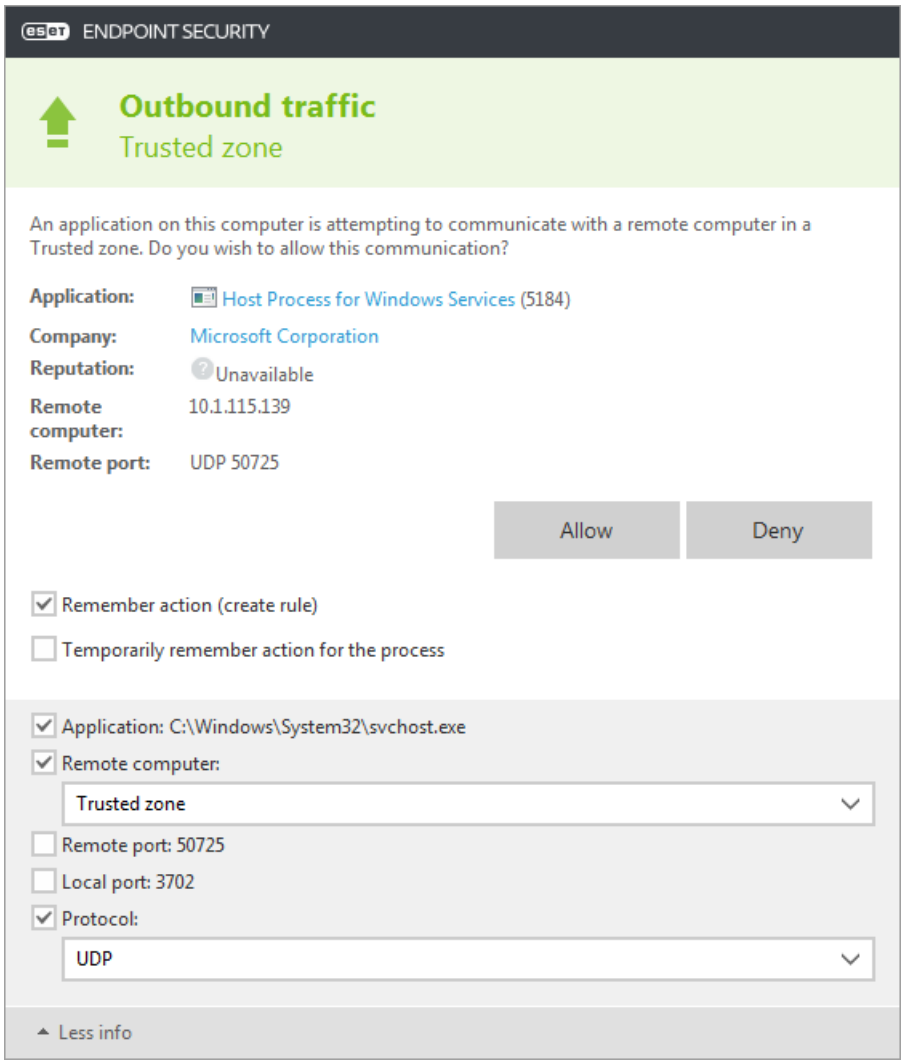
Remember until application quits—ESET Endpoint Security will remember the chosen action until the next restart.

Create rule and remember permanently—If you select this option before allowing or denying a communication, ESET Endpoint Security will remember the action and use it if the application is contacted by the remote computer again.

Allow—Allows the incoming communication.

Deny—Denies the incoming communication.

Edit rule—Enables you to customize rule properties using the Firewall rule editor.



Connection view setup

Right-click a connection to see additional options that include:

Resolve host names—If possible, all network addresses are displayed in DNS format, not in the numeral IP address format.

Show only TCP connections—The list only displays connections that belong to the TCP protocol suite.

Show listening connections—Select this option to only display connections where no communication is currently established, but the system has opened a port and is waiting for a connection.

Show connections within the computer—Select this option to only show connections, where the remote side is a

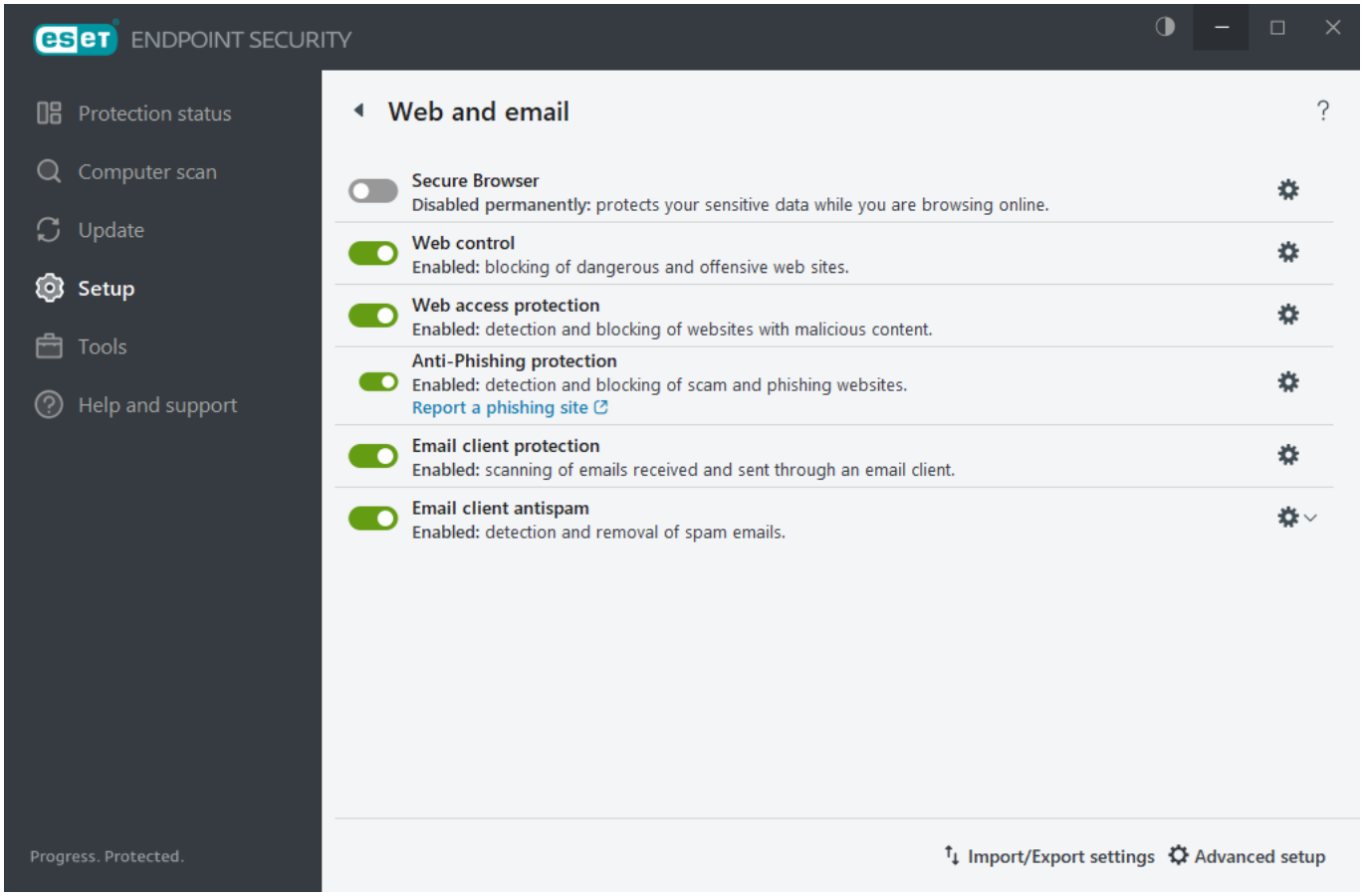
local system – so-called localhost connections.

Web and email

Internet connectivity is a standard feature in a personal computer but also the main medium for transferring malicious code. Open the main program window > **Setup** > **Web and email** to configure ESET Endpoint Security features that increase internet protection.

To pause or disable individual protection modules, click the toggle icon .

⚠ Turning off protection modules may decrease the protection level of your computer.



Click the gear icon next to a protection module to access advanced settings for that module.

Secure Browser protects your sensitive data while you are browsing online.

Web control module enables you to configure settings that provide administrators with automated tools to help protect their workstations and set restrictions for internet browsing. The Web control functionality prevents access to pages with inappropriate or harmful content. Refer to Web control for more information.

Web access protection scans HTTP/HTTPS communication for malware and phishing. Web access protection should only be turned off for troubleshooting.

Anti-Phishing protection enables you to block web pages known to distribute phishing content. We strongly recommend that you leave Anti-Phishing enabled.

Report a phishing site—Report a phishing/malicious website to ESET for analysis.

Before submitting a website to ESET, verify it meets one or more of the following criteria:
• The website is not detected at all
• The website is incorrectly detected as a threat; in this case, you can report an incorrectly blocked page

Email client protection provides control of email communications received through the POP3(S) and IMAP(S) protocols. Using the plugin program for your email client, ESET Endpoint Security provides control of all communications from/to the email client.

Email client antispam filters unsolicited email messages.

For **Email client antispam**, click the gear icon and choose from the following options:

- **Configure**—Opens advanced settings for Email client antispam
- **User's address list** (if enabled)—Opens a dialog window where you can add, edit or delete addresses to define the antispam rules; rules in this list will be applied to the current user
- **Global address list** (if enabled)—Opens a dialog window where you can add, edit or delete addresses to define the antispam rules; rules in this list will be applied to all users

Anti-Phishing protection

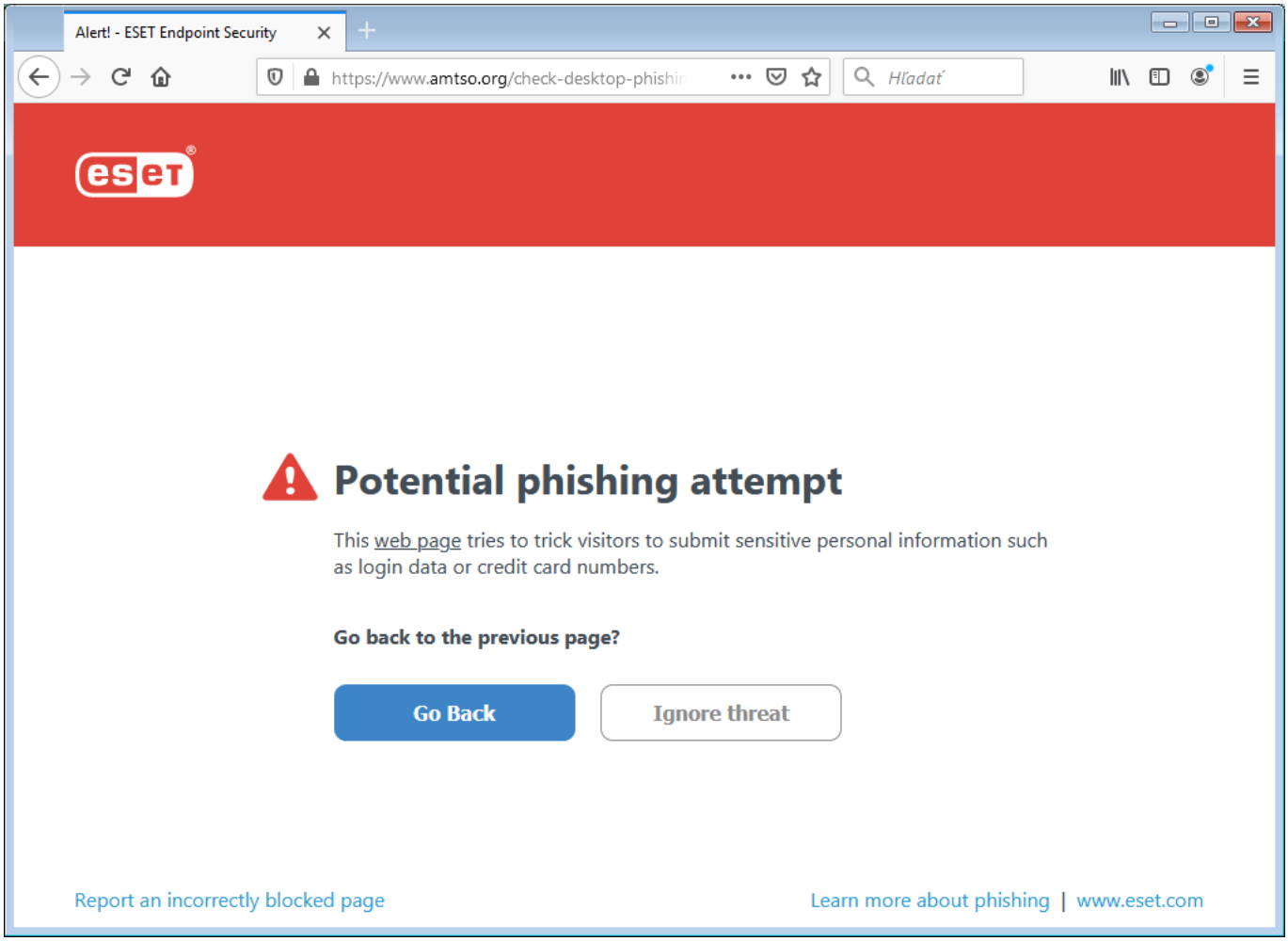
Phishing is a criminal activity that uses social engineering (manipulating users to obtain confidential information). Phishing is used to access sensitive data such as bank account numbers, PINs, etc. For more information, see the glossary. ESET Endpoint Security includes anti-phishing protection, which blocks web pages known to distribute this type of content.

Anti-Phishing protection is enabled by default. This setting can be configured in Advanced setup > **Protections** > **Web access protection**.

Visit our Knowledgebase article for more information on Anti-Phishing protection in ESET Endpoint Security.

Accessing a phishing website

When you access a recognized phishing website, your web browser will display the following dialog. If you still want to access the website, click **Ignore threat** (not recommended).



Potential phishing websites that have been whitelisted will expire after several hours by default. To allow a website permanently, use the URL address management tool. In Advanced setup > **Protections** > **Web access protection** > **URL address management** > **Address list** > **Edit** add the website that you want to edit to the list.

Report a phishing site

The **Report an incorrectly blocked page** link enables you to report a website that is incorrectly detected as a threat.

Alternatively, you can submit the website by email. Send your email to samples@eset.com. Remember to use a descriptive subject and enclose as much information about the website as possible (for example, the website that referred you there, how you learned of this website, etc.).

Import and export settings

You can import or export your customized ESET Endpoint Security .xml configuration file from the **Setup** menu.

Illustrated instructions

See Import or export ESET configuration settings using an .xml file for illustrated instructions available in English and several other languages.

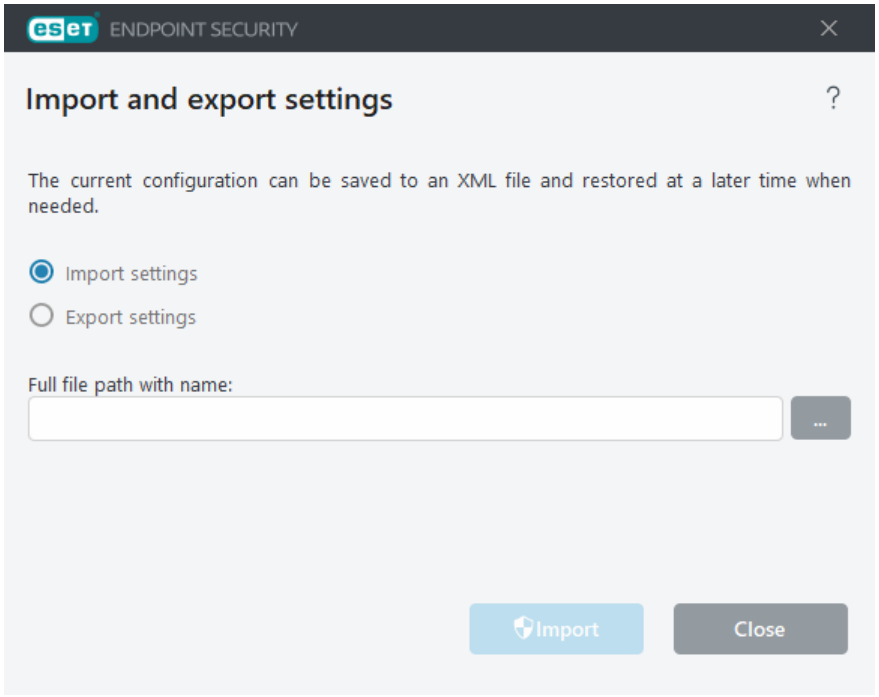
Importing and exporting configuration files is useful if you need to backup your current configuration of ESET

Endpoint Security for use at a later time. The export settings option is also convenient when you want to use your preferred configuration on multiple systems. You can import a .xml file to transfer these settings.

To import a configuration, in the main program window, click **Setup** > **Import/Export settings** and select **Import settings**. Type the configuration filename or click the **...** button to navigate to the configuration file you want to import.

To export a configuration, in the main program window, click **Setup** > **Import/Export settings**. Select **Export settings** and type the full file path with the name. Click **...** to navigate to a location on your computer to save the configuration file.

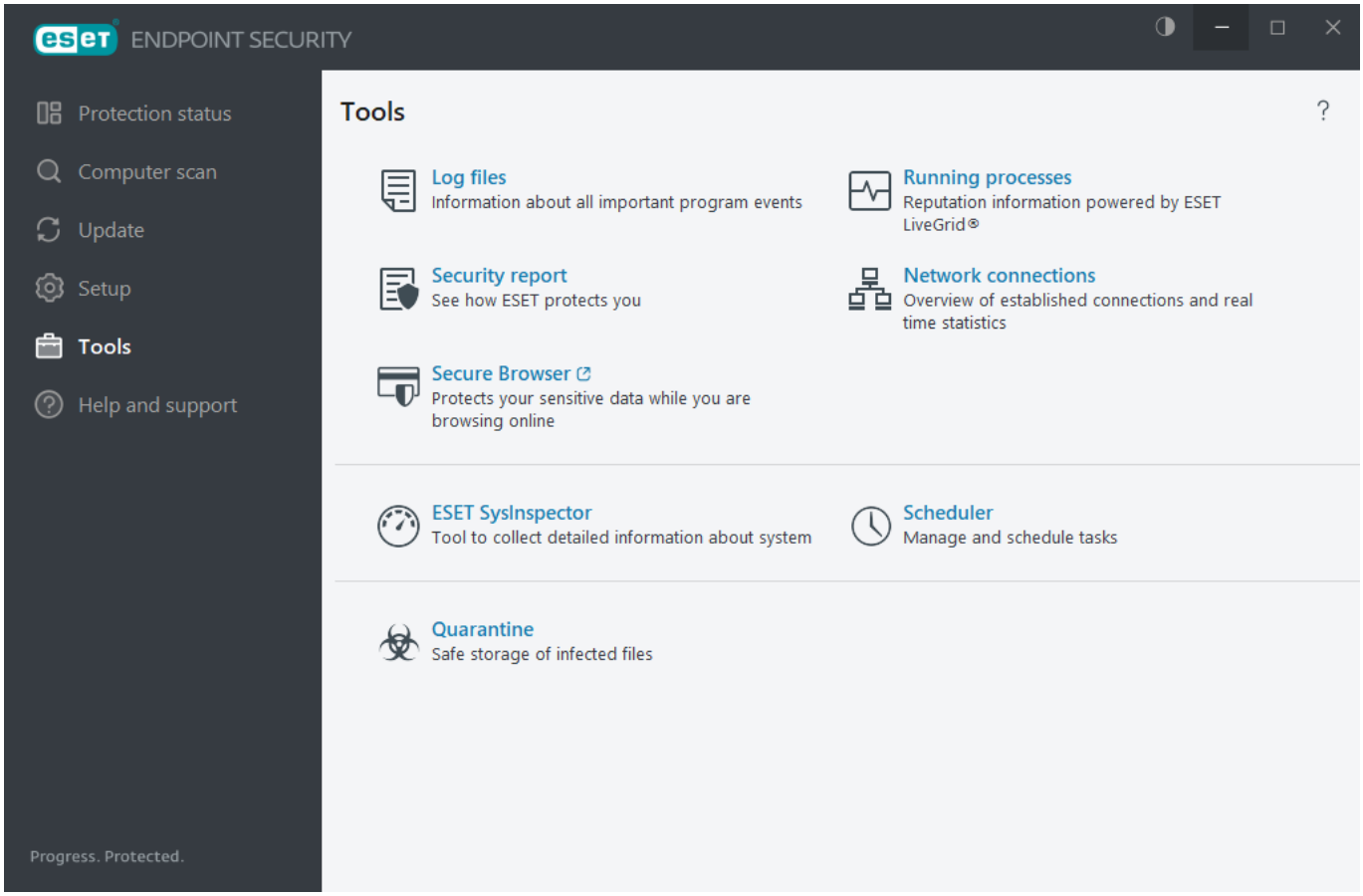
> You may encounter an error while exporting settings if you do not have enough rights to write the exported file to the specified directory.



Tools

The **Tools** menu includes modules that help simplify program administration and offers additional options for advanced users:

- Log files
- Running processes (if ESET LiveGrid® is enabled in ESET Endpoint Security)
- Security report (for non-managed endpoints)
- Network connections (if Firewall is enabled in ESET Endpoint Security)
- ESET SysInspector
- Scheduler
- Submit sample for analysis—Submits a suspicious file to the ESET Research Lab for analysis (may not be available based on your ESET LiveGrid® configuration)
- Quarantine



Log files

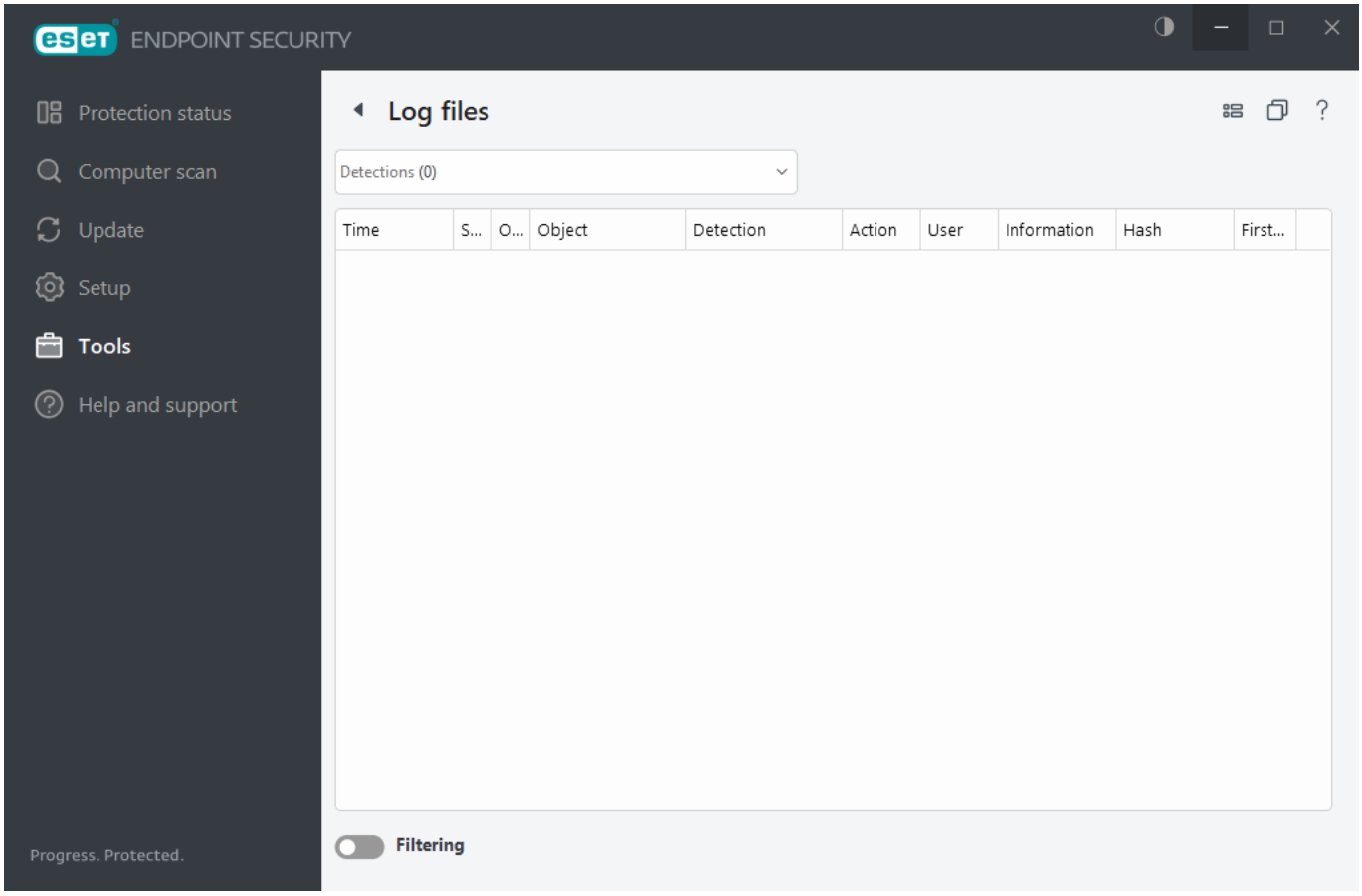
Log files contain information about all important program events that have occurred and provide an overview of detected threats. Logs are an essential tool in system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. You can view text messages and logs directly from the ESET Endpoint Security environment. It is also possible to archive log files.

Log files are accessible from the main program window by clicking **Tools** > **Log files**. Select the desired log type from the **Log** drop-down menu. The following logs are available:

- **Detections**—This log offers detailed information about detections and infiltrations detected by ESET Endpoint Security modules. The information includes the time of detection, name of detection, location, the performed action and the name of the user logged in at the time the infiltration was detected. Double-click any log entry to display its details in a separate window. Not-cleaned infiltrations are always marked with red text on light red background, cleaned infiltrations are marked with yellow text on white background. Not-cleaned PUAs or Potentially unsafe applications are marked with yellow text on white background.
- **Events**—All important actions performed by ESET Endpoint Security are recorded in the event log. The event log contains information about events and errors that have occurred in the program. It is designed to help system administrators and users resolve problems. Often the information found here can help you find a solution for a problem occurring in the program.
- **Computer scan**—All scan results are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view the details of the respective scan.
- **Blocked files**—Contains records of blocked files that could not be accessible when connected to ESET Enterprise Inspector. The protocol shows the reason and the source module that blocked the file, as well as

the application and user that executed the file. For more information, see the ESET Enterprise Inspector Online user guide.

- **Sent files**—Contains records of files that were sent to ESET LiveGrid® or ESET LiveGuard for analysis.
- **Audit logs**—Each log contains information about the date and time when the change was performed, type of change, description, source and user. See Audit logs for more details.
- **HIPS**—Contains records of specific rules that are marked for recording. The protocol shows the application that called the operation, the result (whether the rule was permitted or prohibited) and the name of the rule created.
- **Secure browser**—Contains records of not-verified/untrusted files loaded in the browser.
- **Network protection**—The firewall log displays all remote attacks detected by Network attack protection or Firewall. Here you will find information about any attacks on your computer. The Event column lists the detected attacks. The Source column informs you more about the attacker. The Protocol column reveals the communication protocol used for the attack. Analysis of the network protection log may help you to detect system infiltration attempts in time to prevent unauthorized access to your system. For more details on specific network attacks, see IDS and advanced options.
- **Filtered websites**—This list is useful if you want to view a list of websites that were blocked by Web access protection or Web control. In these logs you can see the time, URL, user and application that opened a connection to the specific website.
- **Email client antispam**—Contains records related to email messages that were marked as spam.
- **Web control**—Shows blocked or allowed URL addresses and details about how they are categorized. The Action performed column tells you how filtering rules were applied.
- **Device control**—Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device type, serial number, vendor name and media size (if available).



Select the contents of any log and press `Ctrl + C` **to copy it to the clipboard**. Hold `Ctrl + Shift` to select multiple entries.

Click **Filtering** to open the Log filtering window where you can define the filtering criteria.

Right-click a specific record to open the context menu. The following options are available in the context menu:

- **Show**—Shows more detailed information about the selected log in a new window.
- **Filter same records**—After activating this filter, you will only see records of the same type (diagnostics, warnings, ...).
- **Filter**—After clicking this option, you can define filtering criteria for specific log entries in the Log filtering window.
- **Enable filter**—Activates filter settings.
- **Disable filter**—Clears all filter settings (as described above).
- **Copy/Copy all**—Copies information about all the records in the window.
- **Copy cell**—Copies the content of the right-clicked cell.
- **Delete/Delete all**—Deletes the selected record(s) or all the records displayed—this action requires administrator privileges.
- **Export**—Exports information about the record(s) in XML format.
- **Export all**—Export information about all records in XML format.
- **Find/Find next/Find previous**—After clicking this option, you can define filtering criteria to highlight the specific entry in the Log filtering window.
- **Create exclusion**—Create a new Detection exclusion using a wizard (Not available for malware detections).

Log filtering

Click **Filtering** in **Tools** > **Log files** to define filtering criteria.

The log filtering feature will help you find the information you are looking for, especially when there are many records. You can narrow down log records, for example, if you are looking for a specific type of event, status or time period. You can filter log records by specifying certain search options, only records that are relevant (according to those search options) will be displayed in the Log files window.

Type the keyword you are searching for into the **Find text** field. Use the **Search in columns** drop-down menu to refine your search. Choose one or more record from the **Record log types** drop-down menu. Define the **Time period** from which you want the results to be displayed. You can also use further search options, such as **Match whole words only** or **Case sensitive**.

Find text

Type a string (word, or part of a word). Only records that contain this string will be shown. Other records will be omitted.

Search in columns

Select what columns will be taken into account when searching. You can check one or more columns to be used for searching.

Record types

Choose one or more log record types from the drop-down menu:

- **Diagnostic**—Logs information needed to fine-tune the program and all records above.
- **Informative**—Records informative messages, including successful update messages, plus all records above.
- **Warnings**—Records critical errors and warning messages.
- **Errors**—Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical**—Logs only critical errors (error starting antivirus protection).

Time period

Define the time period from which you want the results to be displayed:

- **Not specified** (default)—Does not search within time period, searches the whole log.
- **Last day**
- **Last week**
- **Last month**
- **Time period**—You can specify the exact time period (From: and To:) to filter only the records of the specified time period.

Match whole words only

Use the check box if you want to search whole words for more precise results.

Case sensitive

Enable this option if it is important for you to use capital or lower case letters while filtering. After you configured your filtering/search options, click **OK** to show filtered log records or Find to start searching. The log files are searched from top to bottom, starting from your current position (the record that is highlighted). The search stops when it finds the first corresponding record. Press **F3** to search for the next record or right-click and select **Find** to refine your search options.

Audit logs

In an enterprise environment there are usually multiple users with access rights defined for configuring endpoints. Since the modification of the product configuration might dramatically affect how the product operates it is essential that administrators would like to trace the changes done by users to help administrators quickly identify, resolve, and also to prevent occurring of the same or similar problems in the future.

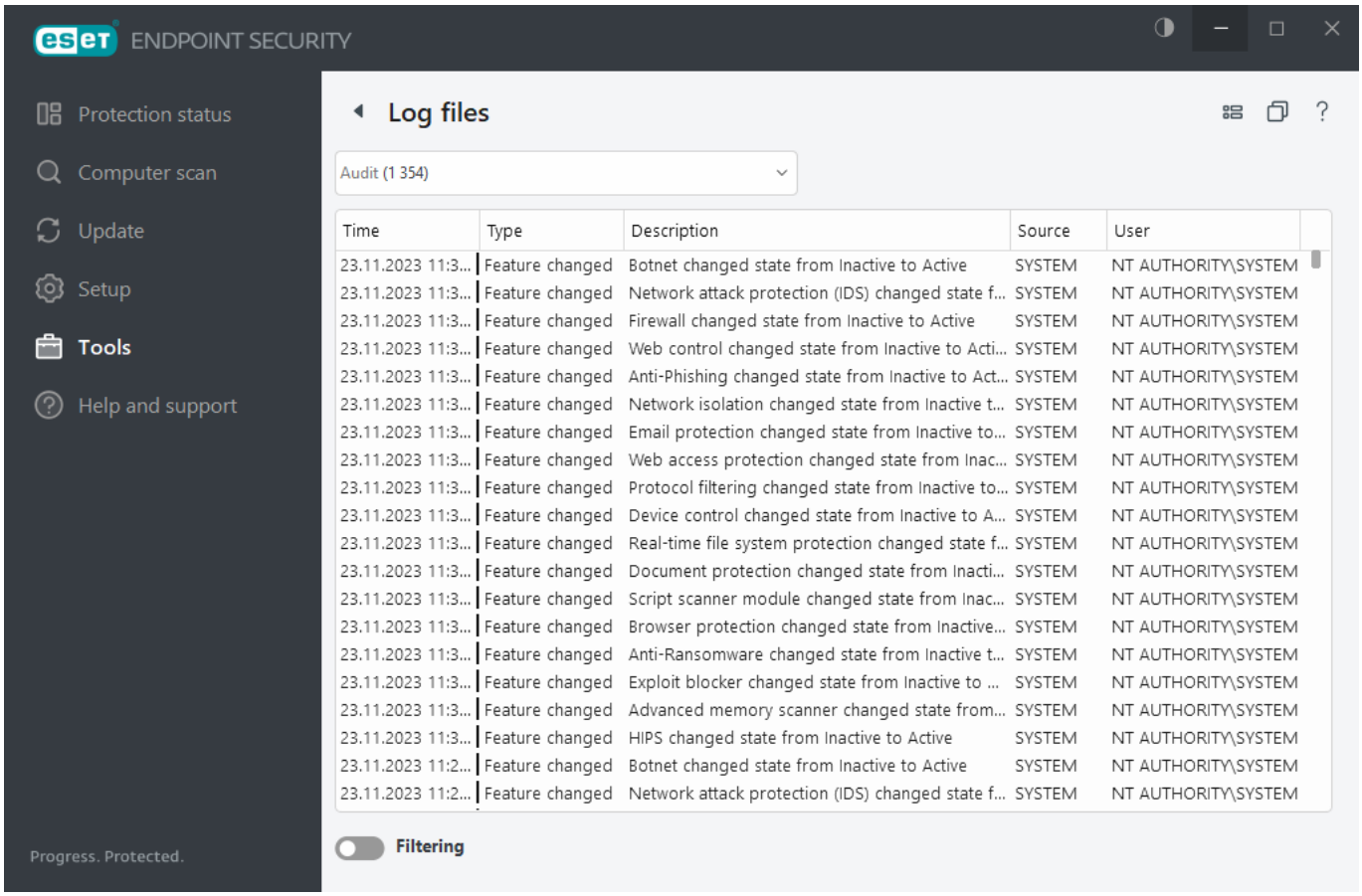
The Audit log is a new type of logging for the identification of the origin of the problem. Audit log tracks changes in configuration or protection state and records snapshots for later reference.

To see the **Audit log**, click **Tools** in the main menu and then click **Log files** and select **Audit logs** from the drop-down menu.

The Audit log contains information about:

- **Time**—when the change was performed

- **Type**—what type of setting or feature was changed
- **Description**—what exactly was changed and which part of setting has been changed together with number of changed settings
- **Source**—where is the source of the change
- **User**—who made the change



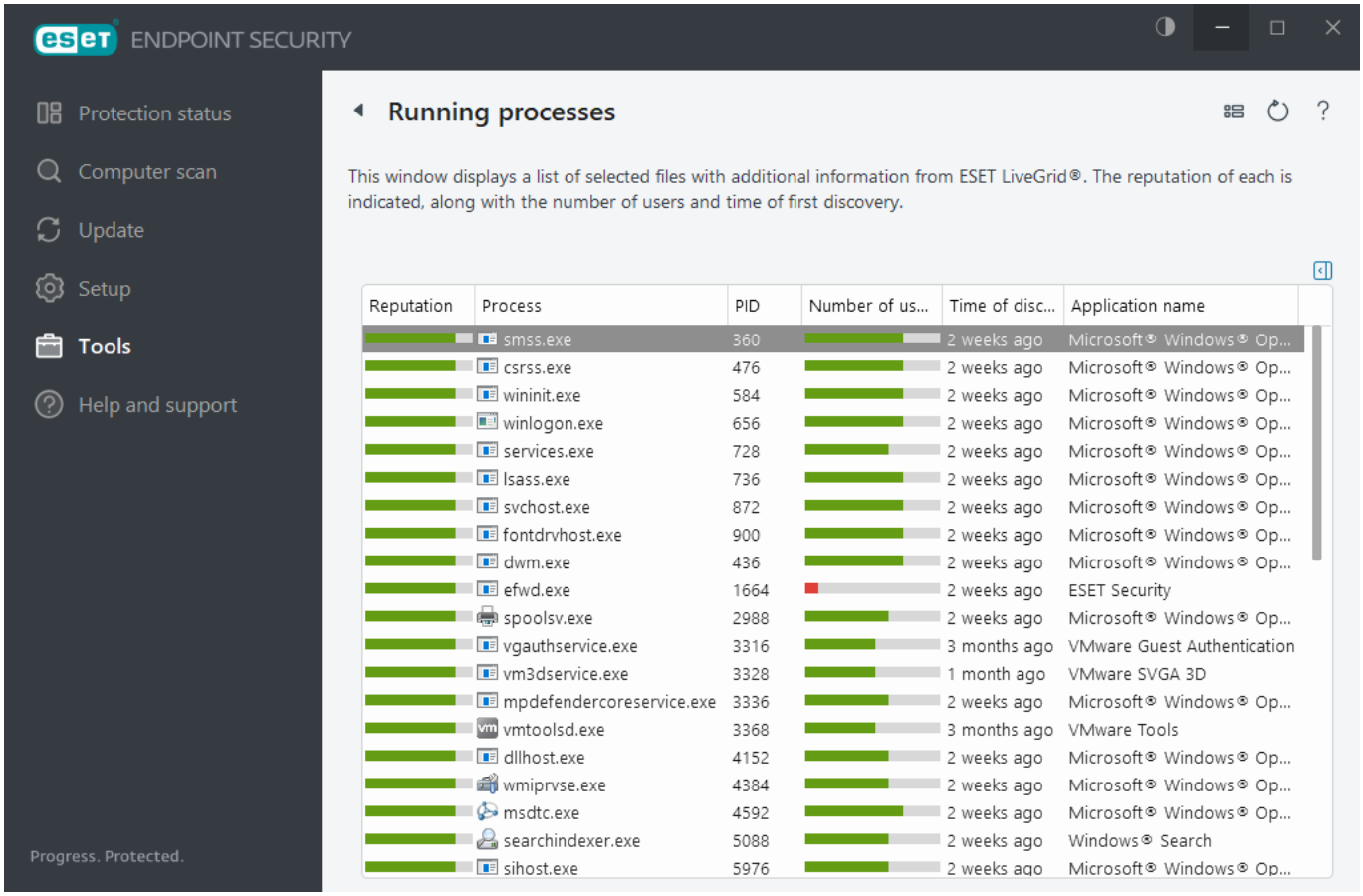
Right-click any **Settings changed** type of audit log in the Log files window and select **Show changes** from the context menu to display detailed information about the performed change. Besides, you can restore setting change by clicking **Restore** from the context menu (not available for product managed by ESET PROTECT On-Prem). If you select **Delete all** from the context menu, the log with information about this action will be created.

If **Optimize log files automatically** enabled in Advanced setup > **Tools** > **Log files**, the Audit logs will automatically be defragmented as other logs.

if **Automatically delete records older than (days)** enabled in Advanced setup > **Tools** > **Log files**, log entries older than the specified number of days will automatically be deleted.

Running processes

Running processes displays the running programs or processes on your computer and keeps ESET immediately and continuously informed about new infiltrations. ESET Endpoint Security provides detailed information on running processes to protect users with ESET LiveGrid® technology enabled.



Reputation—In most cases, ESET Endpoint Security and ESET LiveGrid® technology assign risk levels to objects (files, processes, registry keys, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a reputation level from 9 – Best reputation (green) to 0 – Worst reputation (red).

Process—Image name of the program or process that is currently running on your computer. You can also use the Windows Task Manager to see all running processes on your computer. You can open Task Manager by right-clicking an empty area on the taskbar and then clicking Task Manager, or by pressing **Ctrl**+**Shift**+**Esc** on your keyboard.

PID—Is an ID of processes running in Windows operating systems.

> Known applications marked green are definitely clean (white-listed) and will be excluded from scanning, as this will improve the scanning speed of on-demand computer scan or Real-time file system protection on your computer.

Number of users—The number of users that use a given application. This information is gathered by ESET LiveGrid® technology.

Time of discovery—Period of time since the application was discovered by ESET LiveGrid® technology.

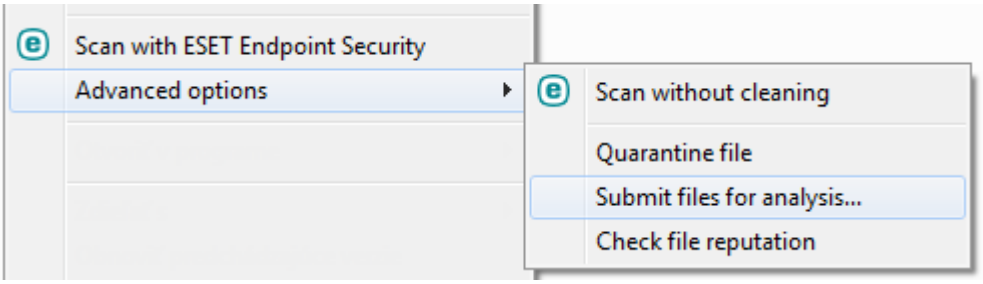
> When an application is marked as Unknown (orange) security level, it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, use the submit file for analysis feature to send the file to the ESET Virus Lab. If the file turns out to be a malicious application, its detection will be added to one of the upcoming detection engine updates.

Application name—The given name of a program or process.

By clicking a given application at the bottom, the following information will appear at the bottom of the window:

- **Path**—Location of an application on your computer.
- **Description**—File characteristics based on the description from the operating system.
- **Version**—Information from the application publisher.
- **Company**—Name of the vendor or application process.
- **Product**—Application name and/or business name.
- **Size**—File size either in kB (kilobytes) or MB (megabytes).
- **Created on**—Date and time when an application was created.
- **Modified on**—Last date and time when an application was modified.

Reputation can also be checked on files that do not act as running programs/processes - mark files you want to check, right-click them and from the context menu select **Advanced options** > **Check file reputation**.



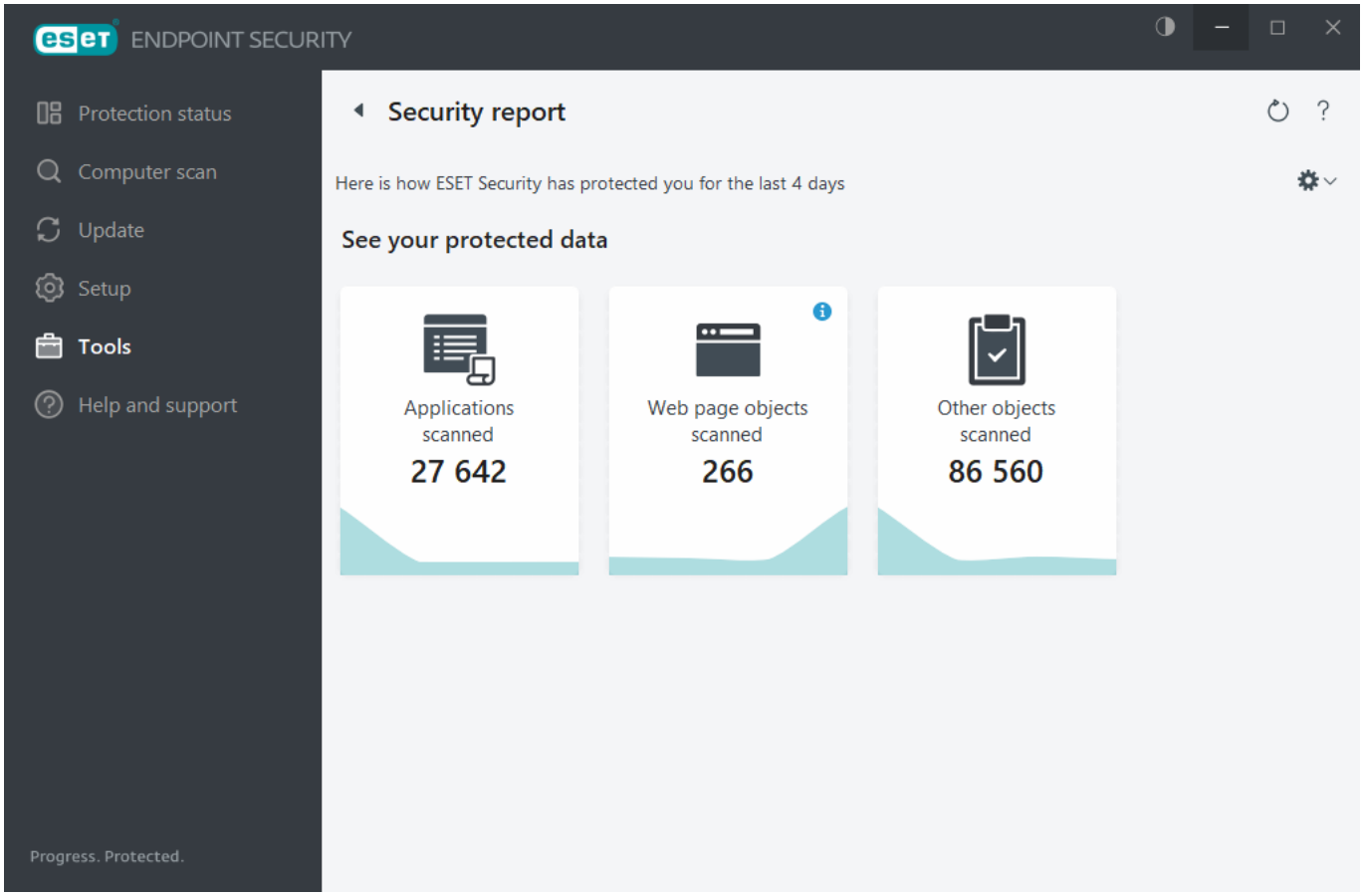
Security report

This feature gives an overview of the statistics for the following categories:

- **Blocked Web pages**—Displays the number of blocked web pages (blacklisted URL for PUA, phishing, hacked router, IP or certificate).
- **Infected email objects detected**—Displays the number of infected email objects that have been detected.
- **Blocked Web pages in Web control**—Displays the number of blocked web pages in Web control.
- **PUA detected**—Displays the number of Potentially unwanted applications (PUA).
- **Spam emails detected**—Displays the number of detected spam emails.
- **Documents scanned**—Displays the number of scanned document objects.
- **Applications scanned**—Displays the number of scanned executable objects.
- **Other objects scanned**—Displays the number of other scanned objects.
- **Web page objects scanned**—Displays the number of scanned web page objects.
- **Email objects scanned**—Displays the number of scanned email objects.

The order of these categories is based on the numeric value from the highest to the lowest. The categories with zero values are not displayed. Click **Show more** to expand and display hidden categories.

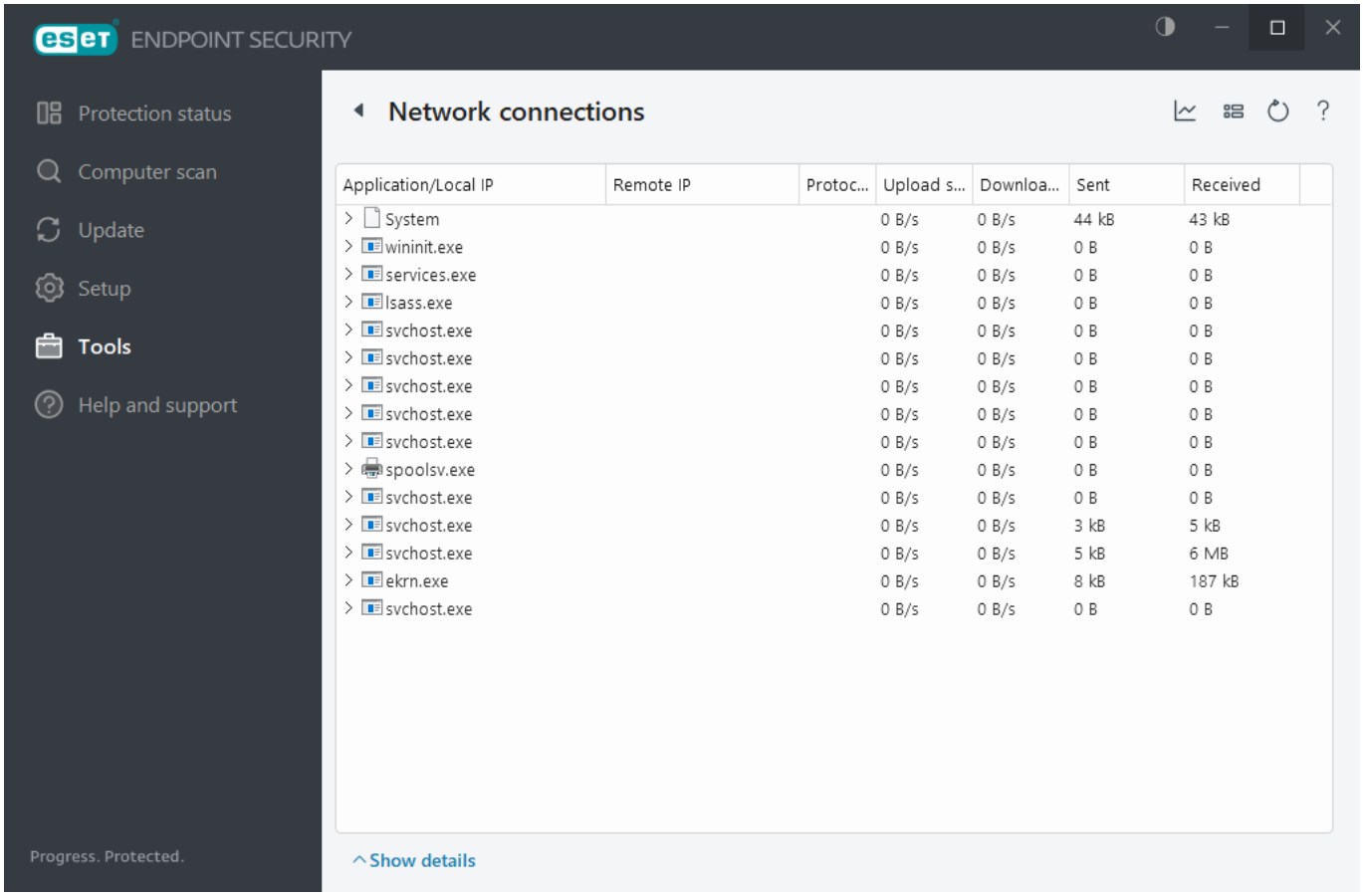
Click the gear wheel in the upper right corner you can **Enable/Disable Security report notifications** or select whether the data will be displayed for the last 30 days or since the product was activated. If ESET Endpoint Security is installed less than 30 days, then only the number of days from installation can be selected. The period of 30 days is set by default.



Reset data will clear all statistics and remove the existing data for Security report. This action has to be confirmed except the case that you deselect the **Ask before resetting statistics** option in Advanced setup > **Notifications** > **Interactive alerts** > **Confirmation messages**.

Network connections

In the Network connections section, you can see a list of active and pending connections. This helps you control all applications establishing outgoing connections.



Click the graph icon to open Network activity.

The first line displays the name of the application and its data transfer speed. To see the list of connections made by the application (and also more detailed information), click **>**.

Columns

Application/Local IP—Name of application, local IP addresses and communication ports.

Remote IP—IP address and port number of the specific remote computer.

Protocol—Transfer protocol used.

Up-Speed/Down-Speed—The current speed of outgoing and incoming data.

Sent/Received—Amount of data exchanged within the connection.

Show details—Choose this option to display detailed information about the selected connection.

Selecting an application or IP address in the Network connections screen and right-clicking it will show a context menu with following structure:

Resolve host names—If possible, all network addresses are displayed in DNS format, not in the numeral IP address format.

Show only TCP connections—The list only displays connections which belong to the TCP protocol suite.

Show listening connections—Select this option to only display connections, where no communication is currently

established, but the system has opened a port and is waiting for a connection.

Show connections within the computer—Select this option to only show connections, where the remote side is a local system—so-called localhost connections.

Right-click a connection to see additional options that include:

Deny communication for the connection—Terminates the established communication. This option is available only after clicking on an active connection.

Refresh speed—Choose the frequency to refresh the active connections.

Refresh now—Reloads the Network connections window.

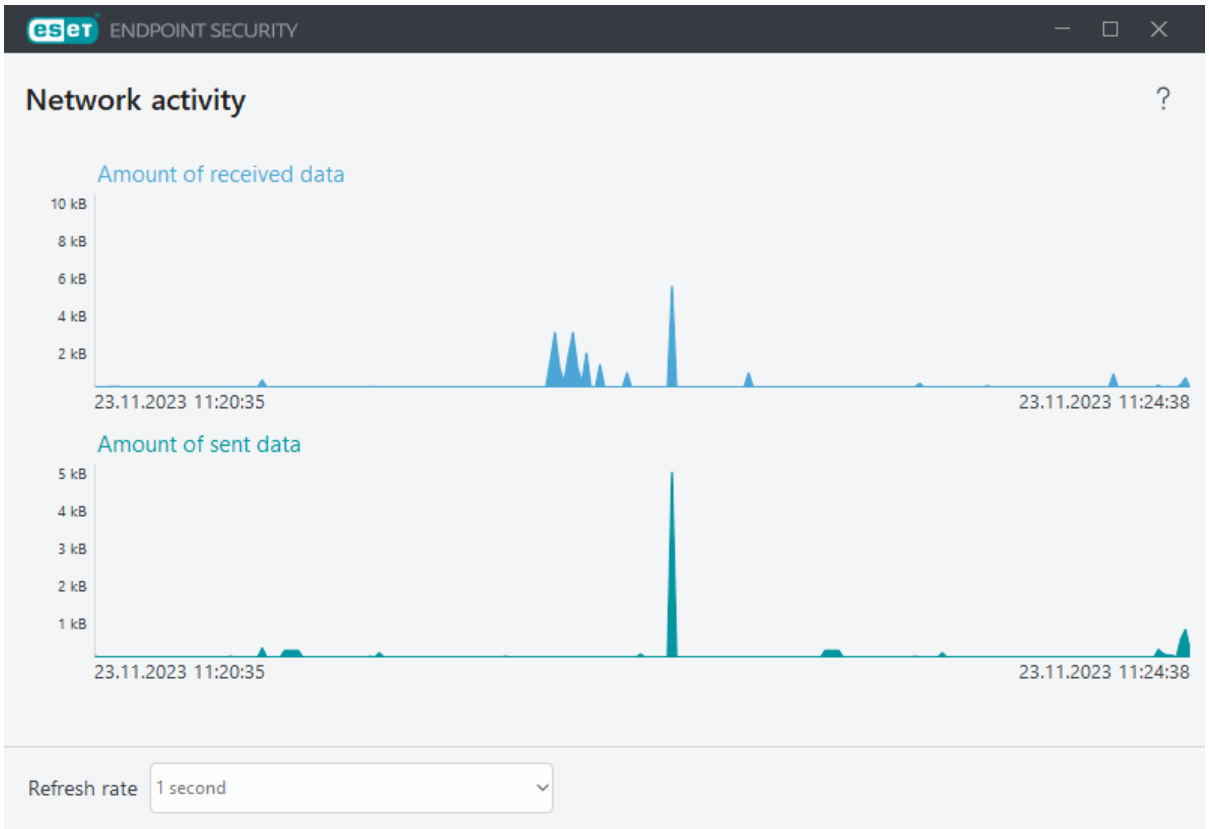
The following options are available only after clicking on an application or process, not an active connection:

Temporarily deny communication for the process—Rejects current connections for the given application. If a new connection is established, the firewall uses a pre-defined rule. A description of the settings can be found in the Firewall rules section.

Temporarily allow communication for the process—Permits current connections for the given application. If a new connection is established, the firewall uses a pre-defined rule. A description of the settings can be found in the Firewall rules section.

Network activity

To see the current **Network activity** in graph form, click **Tools** > **Network connections** and click the graph icon . At the bottom of the graph is a timeline that records network activity in real-time based on the selected time span. To change the time span, select the applicable value from the **Refresh rate** drop-down menu.



The following options are available:

- **1 second**—The graph refreshes every second, and the timeline covers the last 4 minutes.
- **1 minute (last 24 hours)**—The graph refreshes every minute, and the timeline covers the last 24 hours.
- **1 hour (last month)**—The graph refreshes every hour, and the timeline covers the last month.

The graph's vertical axis represents the amount of received or sent data. Hover your mouse over the graph to see the exact amount of received/sent data at a specific time.

ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and gathers detailed information about system components such as drivers and applications, network connections, or important registry entries and evaluates the risk level of each component. This information can help determine the cause of suspicious system behavior, software or hardware incompatibility, or malware infection. To learn how to use ESET SysInspector, see the ESET SysInspector Online Help.

The ESET SysInspector window displays the following information about logs:

- **Time**—The time of log creation.
- **Comment**—A short comment.
- **User**—The name of the user who created the log.
- **Status**—The status of log creation.

The following actions are available:

- **Show**—Opens the selected log in ESET SysInspector. You can also right-click a given log file and select **Show** from the context menu.
- **Create**—Creates a new log. Wait until ESET SysInspector is generated (**Created** status) before attempting to access the log. The log is saved in C:\ProgramData\ESET\ESET Security\SysInspector.
- **Delete**—Removes the selected log(s) from the list.

The following items are available from the context menu when one or more log files are selected:

- **Show**—Opens the selected log in ESET SysInspector (same function as double-clicking a log).
- **Create**—Creates a new log. Wait until ESET SysInspector is generated (**Created** status) before attempting to access the log.
- **Delete**—Removes the selected log(s) from the list.
- **Delete all**—Deletes all logs.
- **Export**—Exports the log to a .xml file or zipped .xml.

Scheduler

the Scheduler manages and launches scheduled tasks with pre-defined configuration and properties.

The Scheduler can be accessed from the ESET Endpoint Security main program window by clicking **Tools** > **Scheduler**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the pre-defined date, time, and scanning profile used.

The Scheduler serves to schedule the following tasks: detection engine update, scanning task, system startup file

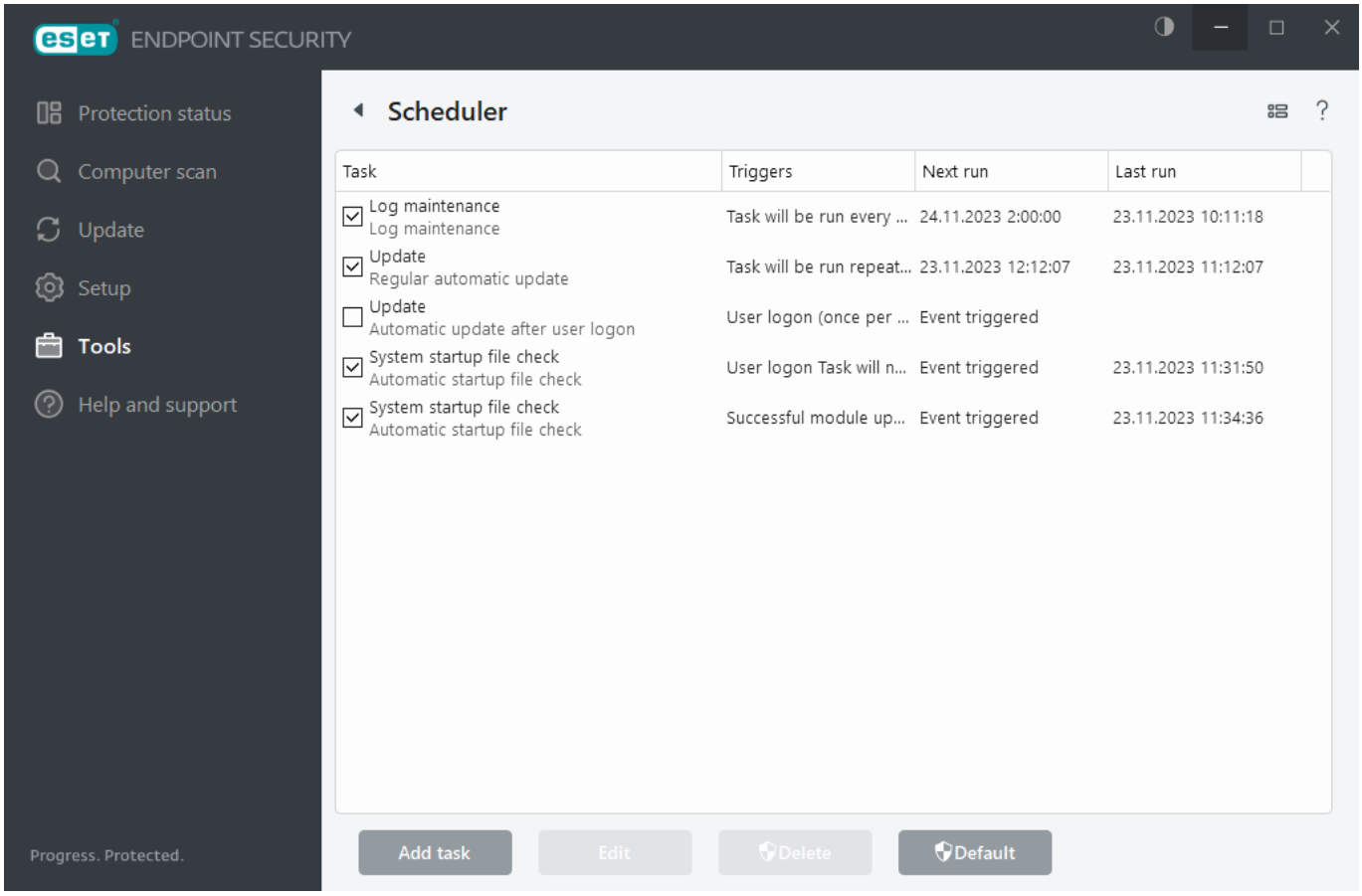
check and log maintenance. You can add or delete tasks directly from the main Scheduler window (click **Add task** or **Delete** at the bottom). Right-click anywhere in the Scheduler window to perform the following actions: display detailed information, perform the task immediately, add a new task, and delete an existing task. Use the check boxes at the beginning of each entry to activate/deactivate the tasks.

By default, the following scheduled tasks are displayed in **Scheduler**:

- **Log maintenance**
- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Automatic startup file check** (after user logon)
- **Automatic startup file check** (after successful module update)

> In ESET PROTECT On-Prem, random task execution delays can be used to reduce server load when executing tasks, especially on larger networks. This option enables you to define a time scope during which a task is to be run on the whole network, as opposed to running a task on all workstations on the whole network at the same time. When a task is run, the set time value is randomly segmented, to allocate a unique task execution time to each workstation on the network. This helps to prevent server overloads and related issues (e.g. some servers may report a DoS attack when performing a simultaneous mass update on workstations throughout the whole network).

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit** or select the task you want to modify and click the **Edit** button.



Add a new task

1. Click **Add task** at the bottom of the window.
2. Type the name of the task.
3. Select the desired task from the drop-down menu:

- **Run external application**—Schedules the execution of an external application.
- **Log maintenance**—Log files also contain leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check**—Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot**—Creates an ESET SysInspector computer snapshot—gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan**—Performs a computer scan of files and folders on your computer.
- **Update**—Schedules an Update task by updating the detection engine and program modules.

4. Enable the **Enabled** toggle if you want to activate the task (you can do this later by selecting/deselecting the check box in the list of scheduled tasks), click **Next** and select one of the timing options:

- **Once**—The task will be performed at the pre-defined date and time.
- **Repeatedly**—The task will be performed at the specified time interval.
- **Daily**—The task will run repeatedly each day at the specified time.
- **Weekly**—The task will be run on the selected day and time.
- **Event triggered**—The task will be performed on a specified event.

5. **Select Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. If the task could not be run at the pre-defined time, you can specify when it will be performed again:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if the time since the last run exceeds a specified value** (the interval can be defined using the **Time since last run** scroll box)

To review a scheduled task, right-click a task and click **Show task details**.

Scheduled scan options

In this window, you can specify advanced options for a scheduled computer scan task.

To run a scan with no cleaning action, click **Advanced settings** and select **Scan without cleaning**. Scan history is saved to the scan log.

When **Ignore exclusions** is selected, files with extensions that were previously excluded from scanning will be scanned with no exception.

You can set an action to be performed automatically after a scan finishes using the drop-down menu:

- **No action**—After a scan finishes, no action will be performed.
- **Shut down**—The computer turns off after a scan finishes.
- **Reboot**—Closes all open programs and restarts the computer after a scan finishes.

- **Reboot if needed**—The computer reboots if only needed to complete cleaning of detected threats.
- **Force reboot**— Forces closing of all open programs without waiting for user interaction and restarts the computer after a scan finishes.
- **Force reboot if needed**—The computer forces reboot if only needed to complete cleaning of detected threats.
- **Sleep**—Saves your session and puts the computer in a low-power state so that you can quickly resume working.
- **Hibernate**—Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down but will resume its previous state the next time you start it.

> **Sleep** or **Hibernate** actions are available based on your computer Power & sleep operating system settings or your computer/laptop capabilities. Remember that a sleeping computer is still a working computer. It is still running basic functions and using electricity when your computer runs on battery power. To preserve battery life, for example, when traveling outside of your office, we recommend using the Hibernate option.

Select **Scan cannot be interrupted** to deny non-privileged users the ability to stop actions taken after scanning.

Select **The scan may be paused by user for (min)** option if you want to allow the limited user to pause the computer scan for a specified time period.

See also Scan progress.

Scheduled task overview

This dialog window displays detailed information about the selected scheduled task when you double-click a custom task or right-click a custom scheduler task and click **Show task details**.

Task details

Type in the **Task name**, select one of the **Task type** options, and then click **Next**:

- **Run external application**—Schedules the execution of an external application.
- **Log maintenance**—Log files also contain leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check**—Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot**—Creates an ESET SysInspector computer snapshot—gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan**—Performs a computer scan of files and folders on your computer.
- **Update**—Schedules an Update task by updating the modules.

Task timing

The task will be performed repeatedly at the specified time interval. Select one of the timing options:

- **Once**—The task will be performed only once at the pre-defined date and time.
- **Repeatedly**—The task will be performed at the specified interval (in hours).
- **Daily**—The task will run each day at the specified time.

- **Weekly**—The task will run one or more times a week, on the selected day(s) and time.
- **Event triggered**—The task will be performed after a specified event.

Skip task when running on battery power—A task will not start if your computer is running on battery when the task should launch. This also applies to computers running on UPS.

Task timing - Once

Task execution—The specified task will be run only once at the specified date and time.

Task timing - Daily

The task will repeatedly run each day at the specified time.

Task timing - Weekly

The task will repeatedly run every week on the selected day(s) and time.

Task timing - Event triggered

The task will be triggered by one of the following events:

- **Every time the computer starts**
- **The first time the computer starts each day**
- **Dial-up connection on the Internet/VPN**
- **Successful module update**
- **Successful product update**
- **User logon**
- **Threat detection**

When scheduling a task triggered by an event, you can specify the minimum interval between two task completions. For example, if you log on to your computer several times a day, choose 24 hours to perform the task only at the first logon of the day and then the next day.

Skipped task

A task can be skipped when the computer is running on battery power or is powered off. Select when the skipped task should run from one of these options and click **Next**:

- **At the next scheduled time**—The task will run if the computer is turned on at the next scheduled time.
- **As soon as possible**—The task will run when the computer is turned on.
- **Immediately, if time since last scheduled run exceeds (hours)**—Represents the time elapsed since the first skipped run of the task. If this time is exceeded, the task will run immediately.

Immediately, if time since last scheduled run exceeds (hours) – examples

An example task is set to run repeatedly every hour. The option **Immediately, if time since last scheduled run exceeds (hours)** is selected and the exceeded time is set to two hours. The task runs at 13:00, and when finished, the computer goes to sleep:

• The computer wakes up at 15:30. The first skipped run of the task was at 14:00. Only 1.5 hours have passed since 14:00, so the task will run at 16:00.

• The computer wakes up at 16:30. The first skipped run of the task was at 14:00. Two and a half hours have passed since 14:00, so the task will run immediately.

Task details - Update

If you want to update the program from two update servers, then it is necessary to create two different update profiles. If the first one fails to download the update files, the program automatically switches to the alternative one. This is suitable, for example, for notebooks that normally update from a local LAN update server, but their owners often connect to the internet using other networks. So, if the first profile fails, the second one will automatically download update files from ESET's update servers.

Task details - Run application

This task schedules the execution of an external application.

Executable file—Choose an executable file from the directory tree, click the **...** option or type the path manually.

Work folder—Define the external application's working directory. All temporary files of the selected **Executable file** will be created within this directory.

Parameters—Command line parameters for the application (optional).

Click **Finish** to apply the task.

Submission of samples for analysis

If you find a suspiciously behaving file on your computer or suspicious site on the internet, you can submit it to the ESET Research Lab for analysis (may not be available based on your configuration of ESET LiveGrid®).

Do not submit a sample unless it meets at least one of the following criteria:

• The sample is not detected by your ESET product at all

• The sample is incorrectly detected as a threat

• We do not accept your personal files (that you would like to scan for malware by ESET) as samples (ESET Research Lab does not perform on-demand scans for users)

• Use a descriptive subject line and enclose as much information about the file as possible (for example, a screenshot or the website you downloaded it from)

Sample submission enables you to send a file or a site to ESET for analysis using one of these methods:

1. Using the sample submission dialog can be found in **Tools** > **Submit sample for analysis**.
2. Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using WinRAR/ZIP, protect the archive with the password "infected", and send it to samples@eset.com.
3. To report spam, spam false positives or miscategorized websites by the Web control module, see our ESET

Knowledgebase article.

With **Select sample for analysis** opened, select the description from the **Reason for submitting the sample** drop-down menu that best fits your message:

- Suspicious file
- Suspicious site (a website that is infected by any malware)
- False positive file (file that is detected as an infection but are not infected)
- False positive site
- Other

File/Site—The path to the file or website you intend to submit.

Contact email—This contact email is sent along with suspicious files to ESET and may be used to contact you if further information is required for analysis. Entering a contact email is optional, select **Submit anonymously** to leave it empty.

> You will not get a response from ESET unless more information is required from you. Each day our servers receive tens of thousands of files, making it impossible to reply to all submissions.
> If the sample turns out to be a malicious application or website, its detection will be added to an upcoming ESET update.

Select sample for analysis - Suspicious file

Observed signs and symptoms of malware infection—Type a description of the suspicious file behavior observed on your computer.

File origin (URL address or vendor)—Type the file origin (source) and how you encountered this file.

Notes and additional information—Here you can type additional info or a description that will help with the process of identifying the suspicious file.

> The first parameter—**Observed signs and symptoms of malware infection**—is required, but providing additional information will help our laboratories with the identification process of samples significantly.

Select sample for analysis - Suspicious site

Choose one of the following from the **What's wrong with the site** drop-down menu:

- **Infected**—A website that contains viruses or other malware distributed by various methods.
- **Phishing**—Often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this type of attack in the glossary.
- **Scam**—A swindle or a fraudulent website, especially for making a quick profit.
- Select **Other** if the aforementioned options do not refer the site you are going to submit.

Notes and additional information—Here you can type additional info or a description that will help while analyzing the suspicious website.

Select sample for analysis - False positive file

We request that you submit files that are detected as an infection but are not infected to improve our antivirus and antispyware engine and help others to be protected. False positives (FP) may occur when a pattern of a file matches the same pattern contained in a detection engine.

Application name and version—Program title and its version (for example number, alias or code name).

File origin (URL address or vendor)—Type a file origin (source) and note how you encountered this file.

Application's purpose—The general application description, type of an application (e.g. browser, media player, ...) and its functionality.

Notes and additional information—Here you can add additional information or descriptions that will help while processing the suspicious file.

> The first three parameters are required to identify legitimate applications and distinguish them from malicious code. By providing additional information, you will help our laboratories significantly in the identification process and in the processing of samples.

Select sample for analysis - False positive site

We request that you submit sites that are detected as an infected, scam or phishing but are not. False positives (FP) may occur when a pattern of a file matches the same pattern contained in a detection engine. Provide this website to improve our antivirus and anti-phishing engine and help others to be protected.

Notes and additional information—Here you can add additional information or descriptions that will help while processing the suspicious website.

Select sample for analysis - Other

Use this form if the file cannot be categorized as a **Suspicious file** or as a **False positive**.

Reason for submitting the file—Type a detailed description and the reason for sending the file.

Quarantine

The main function of the quarantine is to safely store reported objects (such as malware, infected files or potentially unwanted applications).

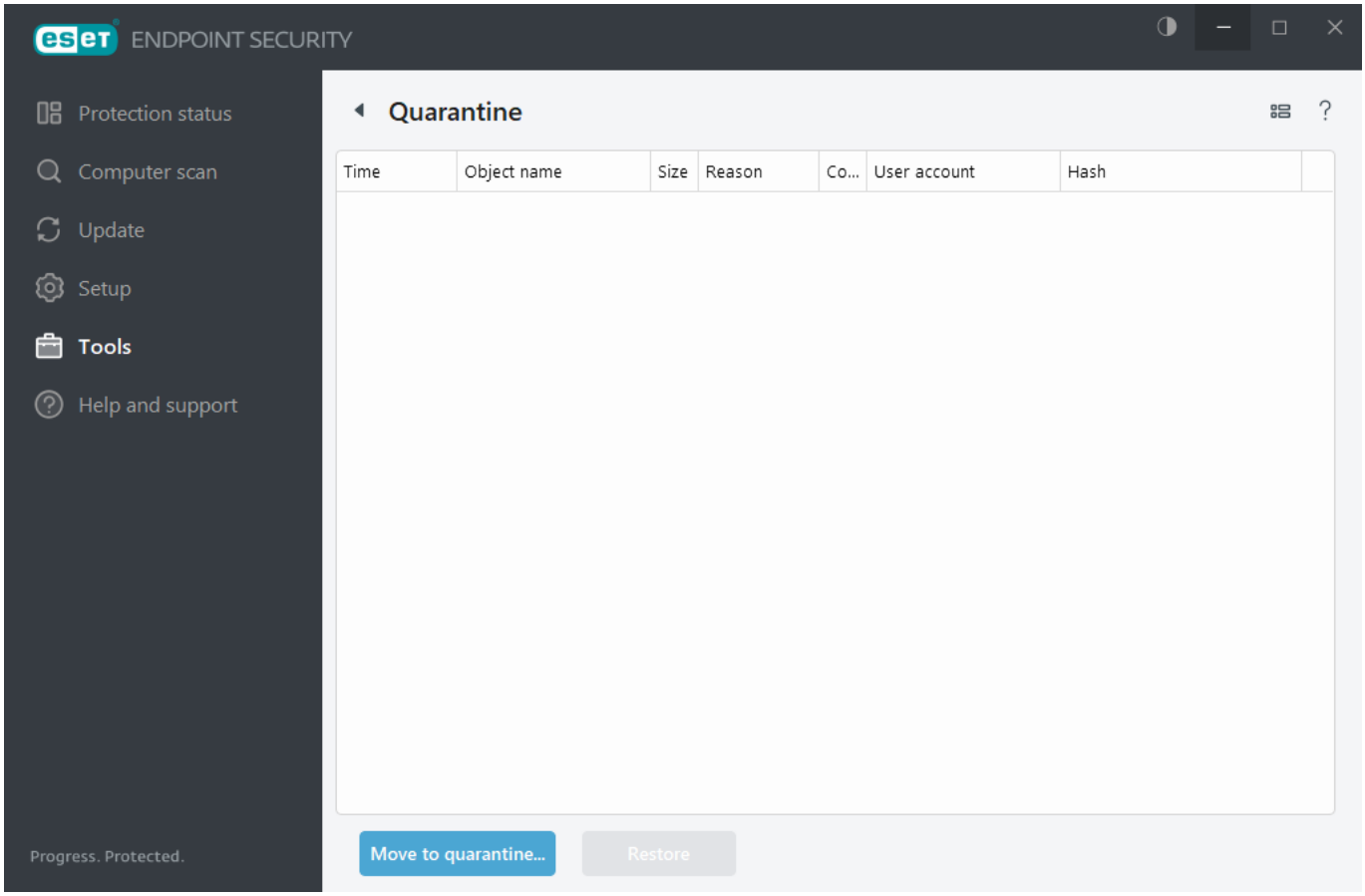
The Quarantine can be accessed from the ESET Endpoint Security main program window by clicking **Tools** > **Quarantine**.

Files stored in the quarantine folder can be viewed in a table that displays:

- the date and time of quarantine,
- the path to the original location of the file,
- its size in bytes,

- reason (for example, object added by user),
- and a number of detections (for example, duplicated detections of the same file or if it is an archive containing multiple infiltrations).

I manage the Quarantine on client workstations remotely



Quarantining files

ESET Endpoint Security automatically quarantines deleted files (if you have not canceled this option in the alert window).

Additional files should be quarantined if they:

- cannot be cleaned,
- if it is not safe or advisable to delete them,
- if they are falsely detected by ESET Endpoint Security,
- or if a file behaves suspiciously but is not detected by the scanner.

To quarantine a file, you have multiple options:

- use the drag and drop feature to quarantine a file manually by clicking the file, moving the mouse pointer to the marked area while keeping the mouse button pressed and then releasing it. After that, the application is moved to the foreground.
- Click **Move to quarantine** from the main program window.
- The context menu can also be used for this purpose; right-click in the **Quarantine** window and select **Quarantine**.

Restoring from the Quarantine

Quarantined files can also be restored to their original location:

- Use the **Restore** feature for this purpose, which is available from the context menu by right-clicking a given file in the Quarantine.
- If a file is marked as a potentially unwanted application, the **Restore and exclude from scanning** option is enabled. See also Exclusions.
- The context menu also offers the **Restore to** option, to restore a file to a location other than the one from which it was deleted.
- The restore functionality is not available in some cases, for example, for files located on a read-only network share.

Deleting from the Quarantine

Right-click a given item and select **Delete from Quarantine**, or select the item you want to delete and press **Delete** on your keyboard. You can also select multiple items and delete them together. Deleted items will be permanently removed from your device and quarantine.

Submitting a file from the Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was determined to be infected incorrectly (for example, by heuristic analysis of the code) and subsequently quarantined, you can send the sample for analysis ESET Research Lab. To submit a file, right-click the file and select **Submit for analysis** from the context menu.

The following ESET Knowledgebase article may only be available in English:
- Manage the Quarantine in ESET PROTECT On-Prem
- My ESET product notified me of a detection—what should I do?

Help and support

Click **Help and support** in the main program window to display support information and troubleshooting tools which help you solve issues you may encounter.

Installed product

- About ESET Endpoint Security—Displays information about your copy of ESET Endpoint Security.
- Product troubleshooting—Click this link to find solutions to the most frequently encountered problems.
- License troubleshooting—Click this link to find solutions for problems with activation or license change.
- Change license—Click to launch the activation window and activate your product.

Help page—Click this link to launch the ESET Endpoint Security help pages.

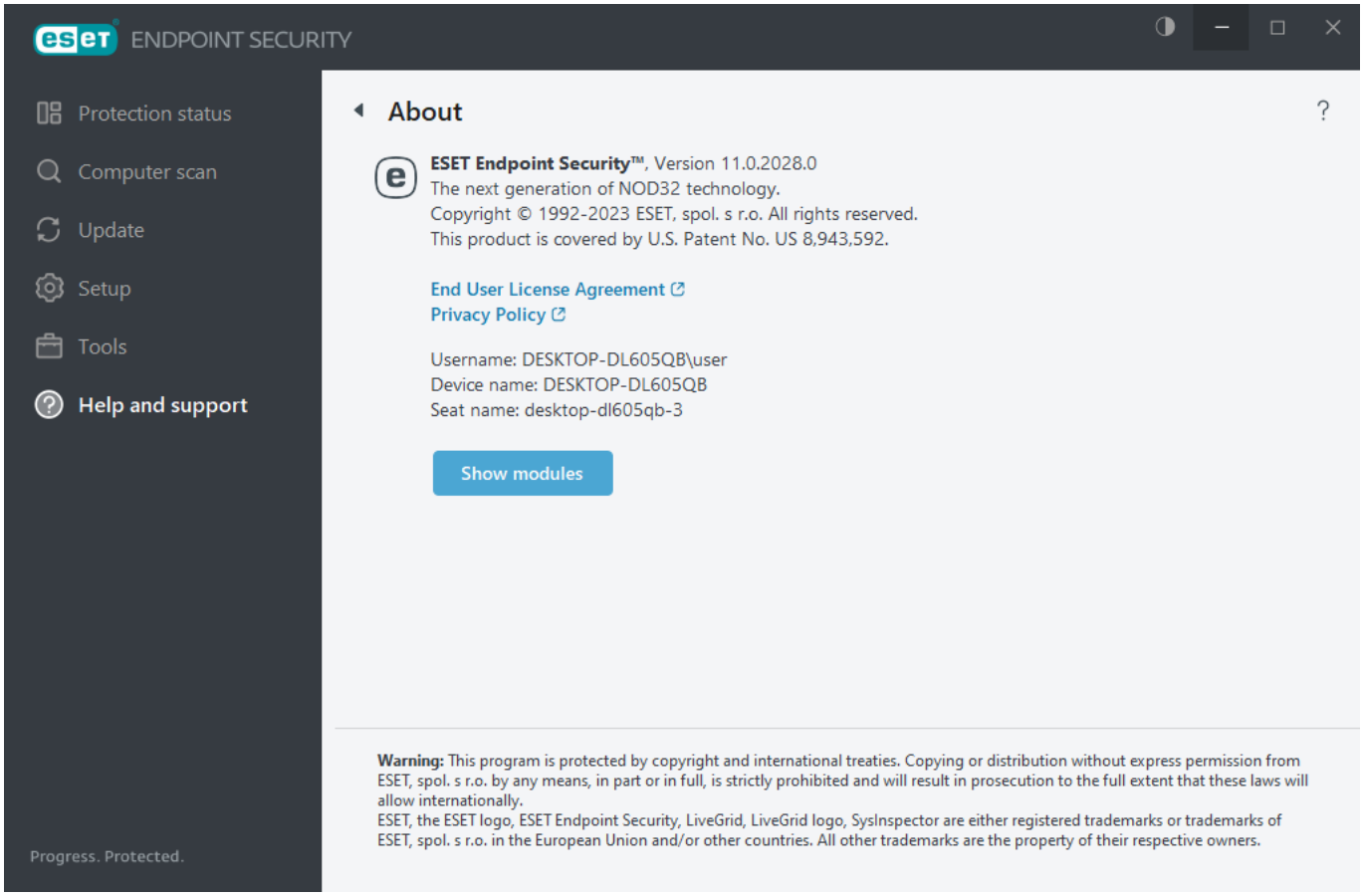
Technical Support

Knowledgebase—The ESET Knowledgebase contains answers to the most frequently asked questions and recommended solutions for various issues. Regularly updated by ESET technical specialists, the ESET

Knowledgebase is the most powerful tool for resolving various problems.

About ESET Endpoint Security

This window provides details about the installed version of ESET Endpoint Security and your computer.



Click **Show modules** to see information about the list of loaded program modules.

- You can copy information about modules to the clipboard by clicking **Copy**. This may be useful during troubleshooting or when contacting Technical Support.
- Click **Detection Engine** in the Modules window to open the ESET Virus radar, which contains information about each version of the ESET Detection Engine.

Submit system configuration data

To provide assistance as quickly and accurately as possible, ESET requires information about ESET Endpoint Security configuration, detailed system information and running processes (ESET SysInspector log file) and registry data. ESET will use this data only to provide technical assistance to the customer.

After you submit the web form, your system configuration data will be sent to ESET. Select **Always submit this information** if you want to remember this action for this process. To submit the web form without sending any data, click **Don't submit data** and continue.

You can configure the submission of system configuration data in Advanced setup > **Tools** > **Diagnostics** > Technical Support.

If you have decided to submit system configuration data, it is necessary to fill out and submit the web form. Otherwise, your ticket will not be created, and your system configuration data will be lost. If the system configuration data cannot be submitted, fill in the web form and wait for instructions from Technical Support.

Technical support

In the main program window, click **Help and Support** > **Technical Support**.

Contact Technical Support

Request support—If you cannot find an answer to your problem, you can use this form located on the ESET website to contact the ESET Technical Support department quickly. Based on your settings, the submit your system configuration data window is displayed before filling the web form.

Get information for Technical Support

Details for Technical Support—When prompted, you can copy and send information to ESET Technical Support (such as license details, product name, product version, operating system and computer information).

ESET Log Collector—Links to the ESET Knowledgebase article, where you can download ESET Log Collector, an application that automatically collects information and logs from a computer to help resolve issues more quickly. For more information, see the ESET Log Collector online user guide.

Enable **Advanced logging** to create advanced logs for all available features to help developers diagnose and solve issues. Minimum logging verbosity is set to **Diagnostic** level. Advanced logging will be automatically disabled after two hours, unless you stop it earlier by clicking **Stop advanced logging**. When all logs are created, the notification window is displayed providing direct access to the Diagnostic folder with the created logs.

Advanced setup

Advanced setup enables you to configure detailed ESET Endpoint Security settings to fit your needs.

To open Advanced setup, open the main program window and press the **F5** key on your keyboard or click **Setup** > **Advanced setup**.

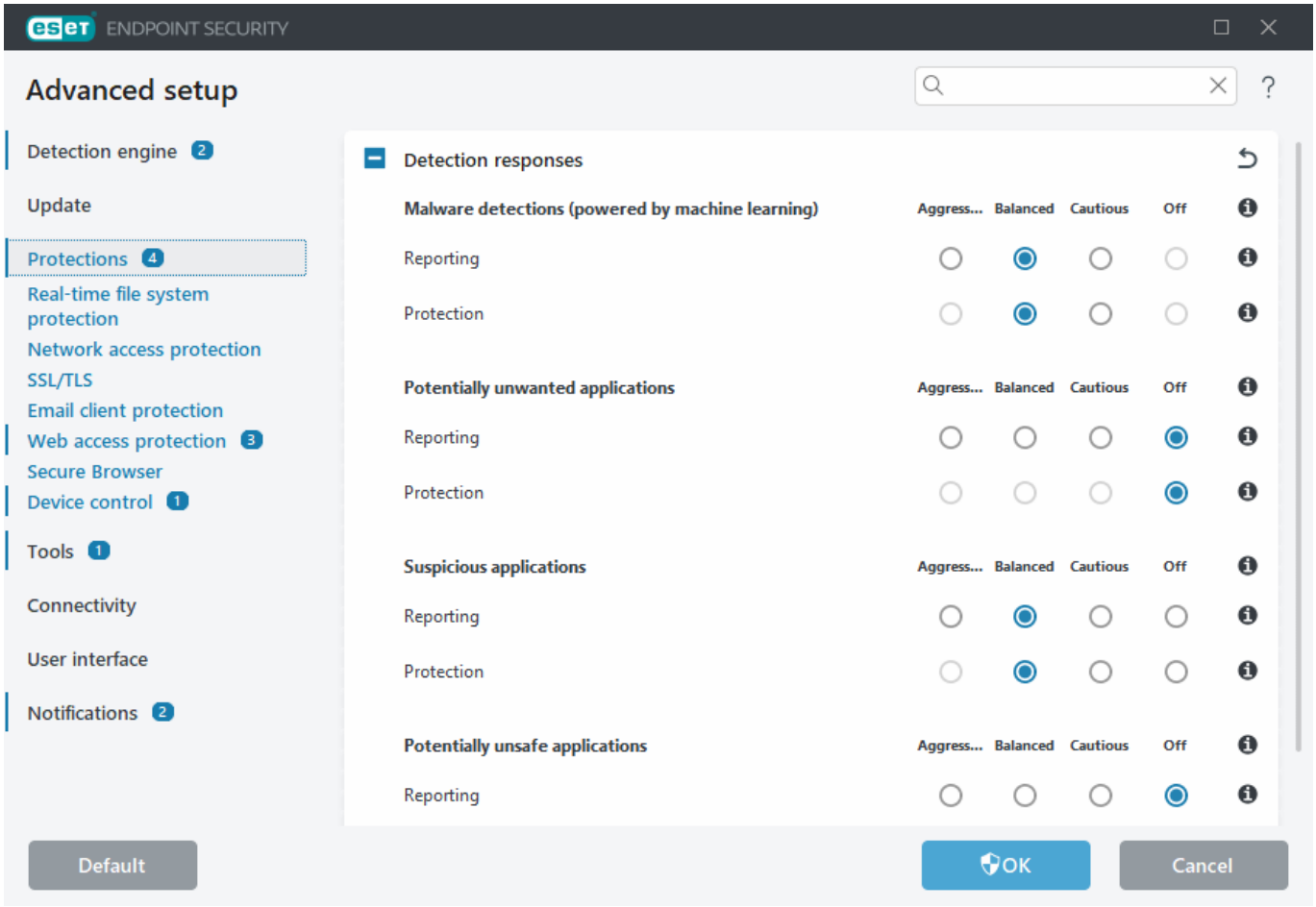
When creating a policy from ESET PROTECT On-Prem Web Console you can select the flag for each setting. Settings with the Force flag have priority and cannot be overwritten by a later policy (even if the later policy has a Force flag). This assures that this setting will not be changed (e.g. by user or by later policies during merging). For more information see Flags in ESET PROTECT On-Prem Online Help.

Based on your Access setup, you may be prompted to type a password to open Advanced setup.

In the advanced setup, you can configure the following settings:

- Detection engine
- Update
- Protections
- Tools

- Connectivity
- User interface
- Notifications



Detection engine

Advanced setup > **Detection engine** enables you to configure the following options:

- Exclusions
- Advanced options
- Network traffic scanner

Exclusions

Exclusions enable you to exclude objects from the detection engine. To ensure that all objects are scanned, we recommend only creating exclusions when it is absolutely necessary. Situations where you may need to exclude an object might include scanning large database entries that would slow your computer during a scan or software that conflicts with the scan.

Performance exclusions—Exclude files and folders from scanning. Performance exclusions are useful to exclude file-level scanning of gaming applications or when causing abnormal system behavior or increased performance.

Detection exclusions—Exclude objects from cleaning using the detection name, path or its hash. Detection exclusions do not exclude files and folders from scanning as performance exclusions do. Detection exclusions

exclude objects only when they are detected by the detection engine and an appropriate rule is present in the exclusion list.

Not to be confused with other types of exclusions:

- Process exclusions—All file operations attributed to excluded application processes are excluded from scanning (may be required to improve backup speed and service availability).
- Excluded file extensions
- HIPS exclusions
- Exclusion filter for Cloud-based protection

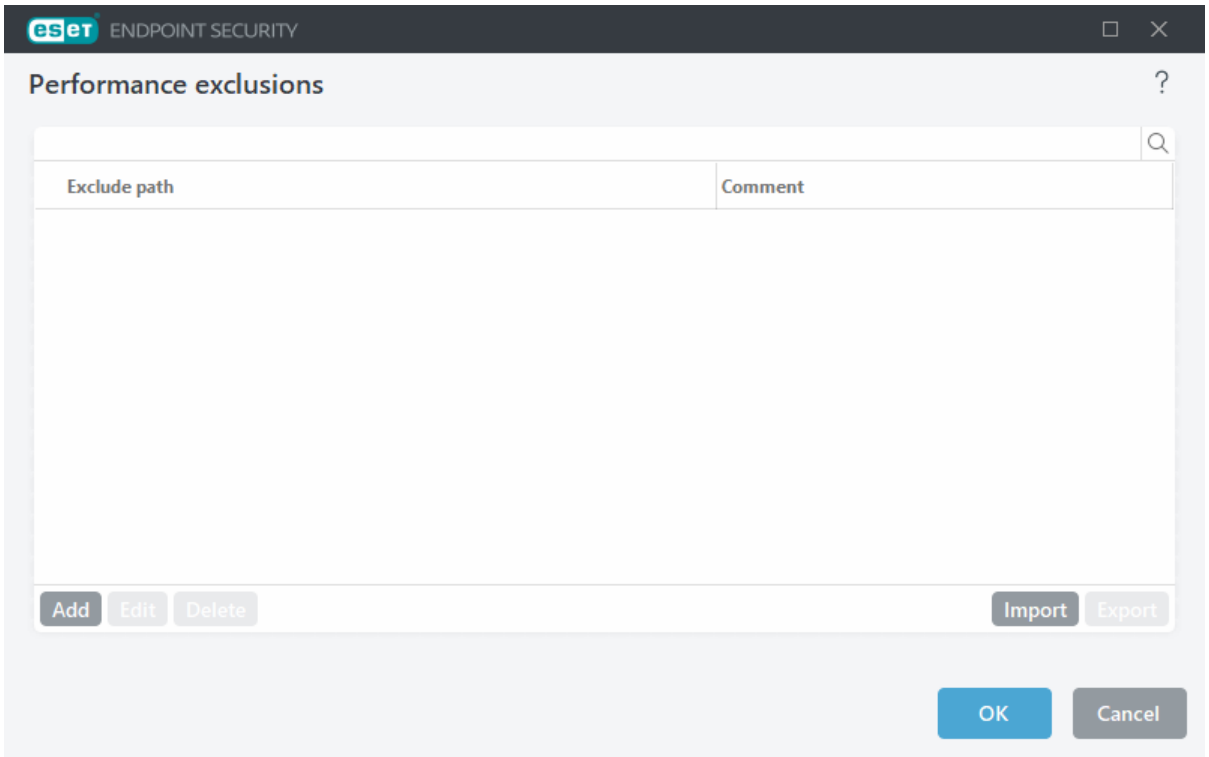
Performance exclusions

Performance exclusions enable you to exclude files and folders from scanning.

To ensure that all objects are scanned for threats, we recommend creating performance exclusions only when it is absolutely necessary. However, there are situations when you may need to exclude an object, for example, large database entries that would slow your computer during a scan or software that conflicts with the scan.

You can add files and folders to be excluded from scanning into the list of exclusions in Advanced setup > **Detection engine** > **Exclusions** > **Performance exclusions** > **Edit**.

To exclude an object (path: file or folder) from scanning, click **Add** and type the applicable path or select it in the tree structure.



A threat within a file will not be detected by the **Real-time file system protection** module or **Computer scan** module if a file meets the criteria for exclusion from scanning.

Control elements

- **Add**—Add a new entry to exclude objects from scanning.
- **Edit**—Enables you to edit selected entries.
- **Delete**—Removes selected entries (CTRL + click to select multiple entries).
- **Import/Export**—Importing and exporting of performance exclusions is useful if you need to backup your current exclusions for use at a later time. The export settings option is also convenient for users in unmanaged environments who want to use their preferred configuration on multiple systems, they can easily import a .txt file to transfer these settings.

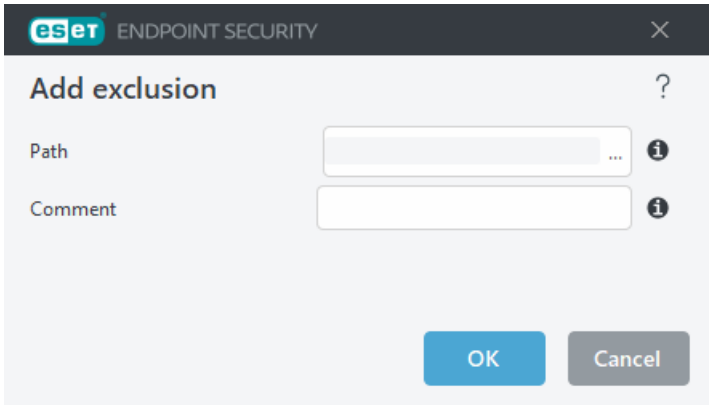
  Display example of the import/export file format

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagem
ent.PerformanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

Add or Edit performance exclusion

This dialog window excludes a specific path (file or directory) for this computer.

> To choose an appropriate path, click **...** in the **Path** field.
> When entering manually, see more exclusion format examples below.



You can use wildcards to exclude a group of files. A question mark (*?*) represents a single character, whereas an asterisk (***) represents a string of zero or more characters.

• If you want to exclude all files and subfolders in a folder, type the path to the folder and use the mask *
• If you want to exclude doc files only, use the mask **.doc*
• If the name of an executable file has a certain number of characters (with varying characters) and you only know the first one (for example, "D"), use the following format:
D????.exe (question marks replace the missing/unknown characters)
Examples:
• *C:\Tools**—The path must end with the backslash (\) and asterisk (*) to indicate that it is a folder and all folder content (files and subfolders) will be excluded.
• *C:\Tools*.**—Same behavior as *C:\Tools**
• *C:\Tools*— *Tools* folder will not be excluded. From the scanner perspective, *Tools* can also be a file name.
• *C:\Tools*.dat*—This will exclude .dat files in the *Tools* folder.
• *C:\Tools\sg.dat*—This will exclude this specific file located in the exact path.

You can use system variables like *%PROGRAMFILES%* to define scan exclusions.
• To exclude the Program Files folder using this system variable, use the path *%PROGRAMFILES%** (remember to add backslash and asterisk at the end of path) when adding to exclusions.
• To exclude all files and folders in a *%PROGRAMFILES%* subdirectory, use the path *%PROGRAMFILES%\Excluded_Directory**

Expand list of supported system variables

The following variables can be used in the path exclusion format:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
User-specific system variables (like *%TEMP%* or *%USERPROFILE%*) or environment variables (like *%PATH%*) are not supported.

Using wildcards in the middle of a path (for example *C:\Tools*\Data\file.dat*) may work but is not officially supported for the performance exclusions. See the following Knowledgebase article for more information. There are no restrictions to using wildcards in the middle of a path when using detection exclusions.

Order of exclusions:
• There are no options to adjust the priority level of exclusions using the top/bottom buttons (as for Firewall rules where rules are executed from top to bottom).
• When the first applicable rule is matched by the scanner, the second applicable rule will not be evaluated.
• The fewer the rules, the better the scanning performance.
• Avoid creating concurrent rules.

Path exclusion format

You can use wildcards to exclude a group of files. A question mark (*?*) represents a single character, whereas an asterisk (***) represents a string of zero or more characters.

• If you want to exclude all files and subfolders in a folder, type the path to the folder and use the mask *
• If you want to exclude doc files only, use the mask **.doc*
• If the name of an executable file has a certain number of characters (with varying characters) and you only know the first one (for example, "D"), use the following format:
D????.exe (question marks replace the missing/unknown characters)
Examples:
• *C:\Tools**—The path must end with the backslash (\) and asterisk (*) to indicate that it is a folder and all folder content (files and subfolders) will be excluded.
• *C:\Tools*.**—Same behavior as *C:\Tools**
• *C:\Tools*— *Tools* folder will not be excluded. From the scanner perspective, *Tools* can also be a file name.
• *C:\Tools*.dat*—This will exclude .dat files in the *Tools* folder.
• *C:\Tools\sg.dat*—This will exclude this specific file located in the exact path.

You can use system variables like *%PROGRAMFILES%* to define scan exclusions.
• To exclude the Program Files folder using this system variable, use the path *%PROGRAMFILES%** (remember to add backslash and asterisk at the end of path) when adding to exclusions.
• To exclude all files and folders in a *%PROGRAMFILES%* subdirectory, use the path *%PROGRAMFILES%\Excluded_Directory**

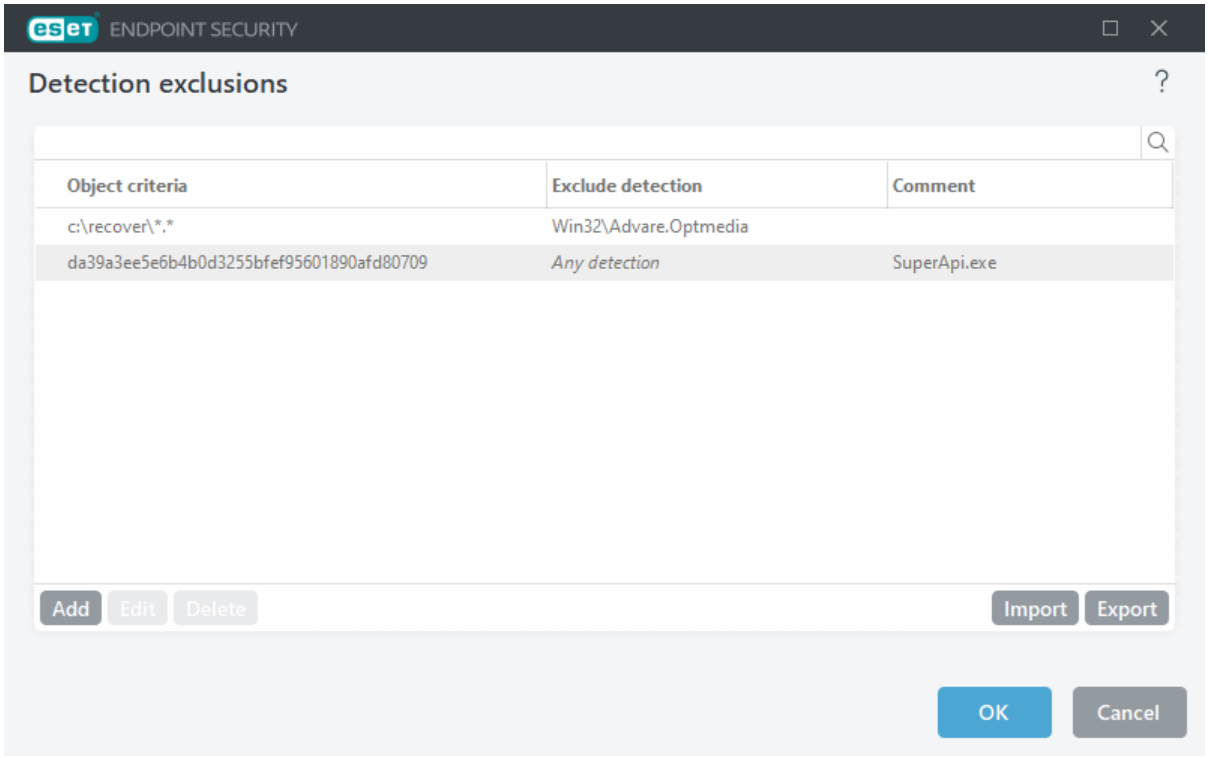
Expand list of supported system variables

The following variables can be used in the path exclusion format:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
User-specific system variables (like *%TEMP%* or *%USERPROFILE%*) or environment variables (like *%PATH%*) are not supported.

Detection exclusions

Detection exclusions enable you to exclude objects from cleaning by filtering the detection name, object path or its hash.

Detection exclusions do not exclude files and folders from scanning as Performance exclusions do.
Detection exclusions exclude objects only when they are detected by the detection engine and an appropriate rule is present in the exclusion list.
For example (see the first row on the image below), when an object is detected as Win32/Adware.Optmedia and the detected file is *C:\Recovery\file.exe*. On the second row, each file, which has the appropriate SHA-1 hash, will always be excluded despite the detection name.



To ensure that all threats are detected, we recommend creating detection exclusions only when it is absolutely necessary.

To add files and folders to the exclusions list, open Advanced setup > **Detection engine** > **Exclusions** > **Detection exclusions** > **Edit**.

To exclude an object (by its detection name or hash) from cleaning, click **Add**.

For Potentially unwanted applications and Potentially unsafe applications, the exclusion by its detection name can also be created:

- In the alert window reporting the detection (click **Show advanced options** and then select **Exclude from detection**).
- From the Log Files context menu using Create detection exclusion wizard.
- By clicking **Tools** > **Quarantine** and then right-clicking the quarantined file and selecting **Restore and exclude from scanning** from the context menu.

Detection exclusions object criteria

- **Path**—Limit a detection exclusion for a specified path (or any).
- **Detection name**—If there is a name of a detection next to an excluded file, it means that the file is only excluded for the given detection, not completely. If that file becomes infected later with other malware, it will be detected.
- **Hash**—Excludes a file based on a specified SHA-1 hash, regardless of the file type, location, name, or extension.

Control elements

- **Add**—Add a new entry to exclude objects from cleaning.
- **Edit**—Enables you to edit selected entries.
- **Delete**—Removes selected entries (CTRL + click to select multiple entries).
- **Import/Export**—Importing and exporting of detection exclusions is useful if you need to backup your current exclusions for use at a later time. The export settings option is also convenient for users in unmanaged environments who want to use their preferred configuration on multiple systems, they can easily import a .txt file to transfer these settings.

  Display example of the import/export file format

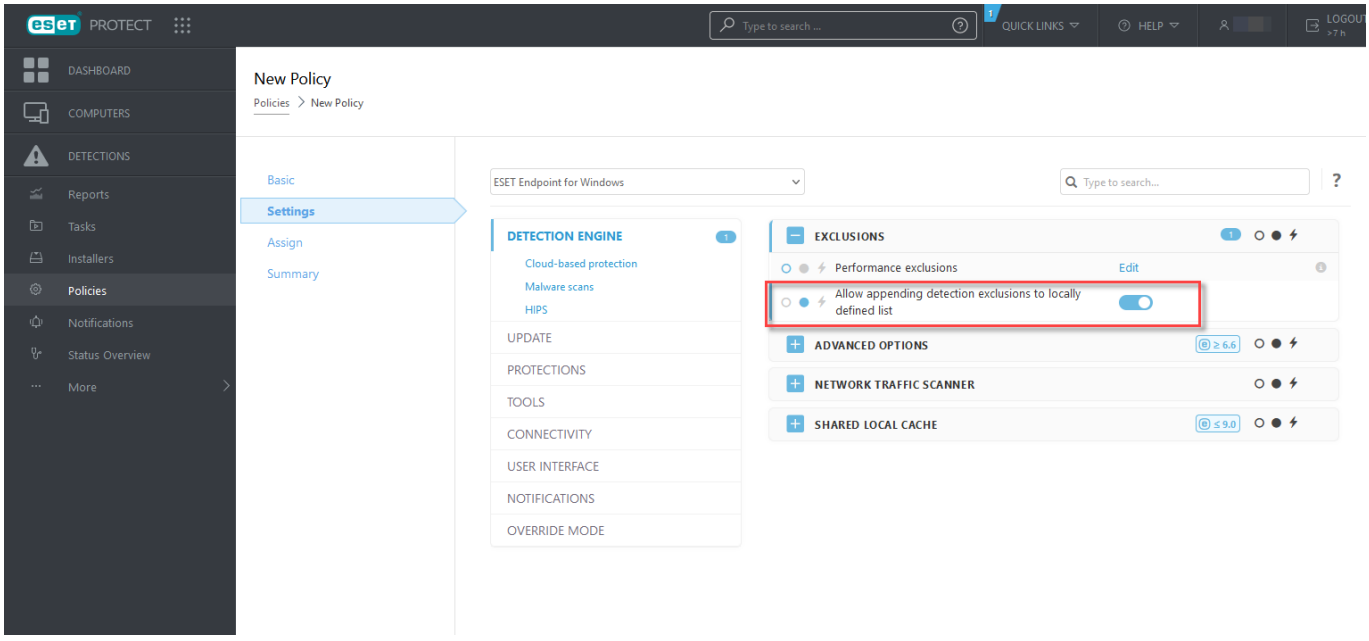
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Detection exclusions setup in ESET PROTECT On-Prem

ESET PROTECT On-Prem detection exclusions management wizard—Create a detection exclusion and apply it to more computers/group(s).

Possible detection exclusions override from ESET PROTECT On-Prem

When there is an existing presence of a detection exclusions local list, the admin has to apply a policy with **Allow appending detection exclusions to locally defined list**. After that, appending detection exclusions from ESET PROTECT On-Prem will work as expected.

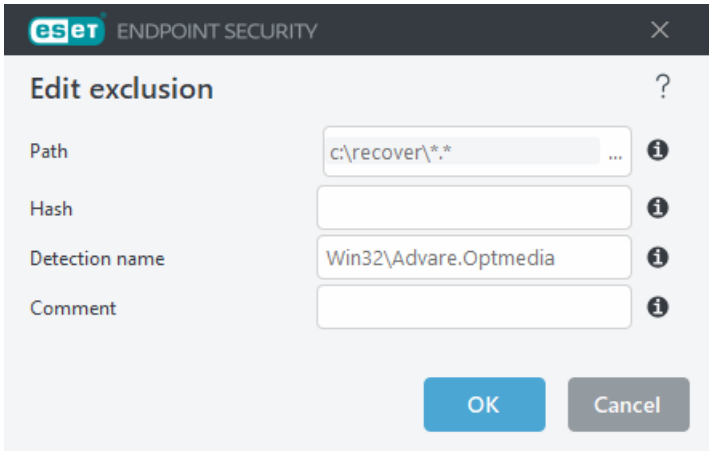


Add or Edit detection exclusion

Exclude detection

A valid ESET detection name should be provided. For a valid detection name, see Log files and then select **Detections** from the Log files drop-down menu. This is useful when a false positive sample is being detected in ESET Endpoint Security. Exclusions for real infiltrations are very dangerous, consider excluding only affected files / directories by clicking **...** in the **Path** field and/or only for a temporary period of time. Exclusions apply also to Potentially unwanted applications, potentially unsafe applications and suspicious applications.

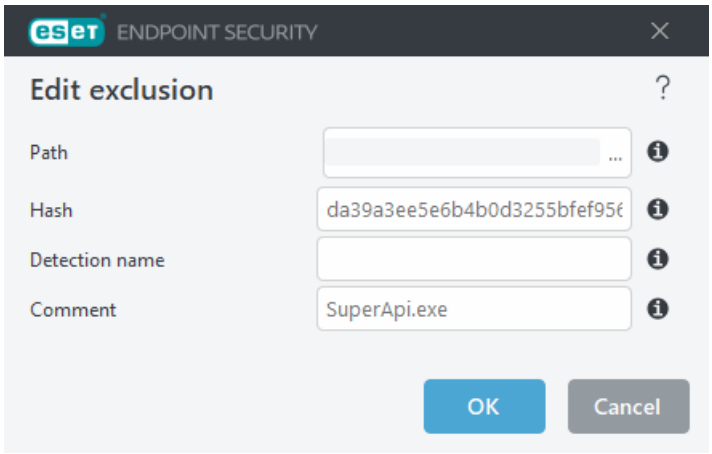
See also Path exclusion format.



See the Detection exclusions example below.

Exclude hash

Excludes a file based on a specified SHA-1 hash, regardless of the file type, location, name, or extension.



To exclude a specific detection by its name, type the valid detection name:
Win32/Adware.Optmedia
You can also use the following format when you exclude a detection from the ESET Endpoint Security alert window:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Control elements

- **Add**—Excludes objects from detection.
- **Edit**—Enables you to edit selected entries.
- **Delete**—Removes selected entries (CTRL + click to select multiple entries).

Create detection exclusion wizard

A detection exclusion can also be created from the Log files context menu (not available for malware detections):

1. In the main program window, click **Tools** > **Log files**.
2. Right-click a detection in the **Detections log**.
3. Click **Create exclusion**.

To exclude one or more detections based on the **Exclusion criteria**, click **Change criteria**:

- **Exact files**—Exclude each file by its SHA-1 hash.
- **Detection**—Exclude each file by its detection name.
- **Path + Detection**—Exclude each file by its detection name and path, including file name (e.g., *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

The recommended option is pre-selected based on the detection type.

Optionally, you can add a **Comment** before clicking **Create exclusion**.

Detection engine advanced options

Enable advanced scanning via AMSI—Microsoft Antimalware Scan Interface tool that allows scanning of PowerShell scripts, scripts executed by Windows Script Host and data scanned using AMSI SDK.

Network traffic scanner

The Network traffic scanner provides malware protection for application protocols, which integrates multiple advanced malware scanning techniques. Network traffic scanner scans HTTP(S), POP3(S) and IMAP(S) protocols automatically, regardless of the internet browser or email client. You can enable/disable the Network traffic scanner in Advanced setup > **Detection engine** > **Network traffic scanner**.

Enable Network traffic scanner—If you disable this option, HTTP(S), POP3(S) and IMAP(S) protocols will not be scanned. Note that the following ESET Endpoint Security features require Network traffic scanner enabled:

- Web access protection
- Web control
- Secure Browser
- SSL/TLS

- Anti-phishing protection
- Email client protection

Cloud-based protection

ESET LiveGrid® (built on the ESET ThreatSense.Net advanced early warning system) utilizes data that ESET users have submitted worldwide and sends it to the ESET Research Lab. By providing suspicious samples and metadata, ESET LiveGrid® enables us to react immediately to needs of our customers and keep ESET responsive to the latest threats.

The following options are available:

Option 1: Enable the ESET LiveGrid® reputation system

The ESET LiveGrid® reputation system provides cloud-based whitelisting and blacklisting.

Check the reputation of Running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid®.

Option 2: Enable the ESET LiveGrid® feedback system

In addition to the ESET LiveGrid® reputation system, the ESET LiveGrid® feedback system collects information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer‘s operating system.

By default, ESET Endpoint Security is configured to submit suspicious files for detailed analysis to the ESET Virus Lab. Files with certain extensions such as *.doc* or *.xls* are always excluded. You can also add other extensions if there are specific files that you or your organization want to avoid sending.

Option 3: Choose not to enable ESET LiveGrid®

You will not lose any software functionality, but in some cases, ESET Endpoint Security may respond faster to new threats than the detection engine update when ESET LiveGrid® is enabled.

> Read more about ESET LiveGrid® in the glossary.
> See our illustrated instructions available in English and several other languages on how to enable or disable ESET LiveGrid® in ESET Endpoint Security.

Cloud-based protection configuration in Advanced setup

To access ESET LiveGrid® settings, open Advanced setup > **Detection Engine** > **Cloud-based Protection**.

Enable ESET LiveGrid® reputation system (recommended)—The ESET LiveGrid® reputation system improves the efficiency of ESET anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.

Enable ESET LiveGrid® feedback system—Sends relevant submission data (described in the **Submission of**

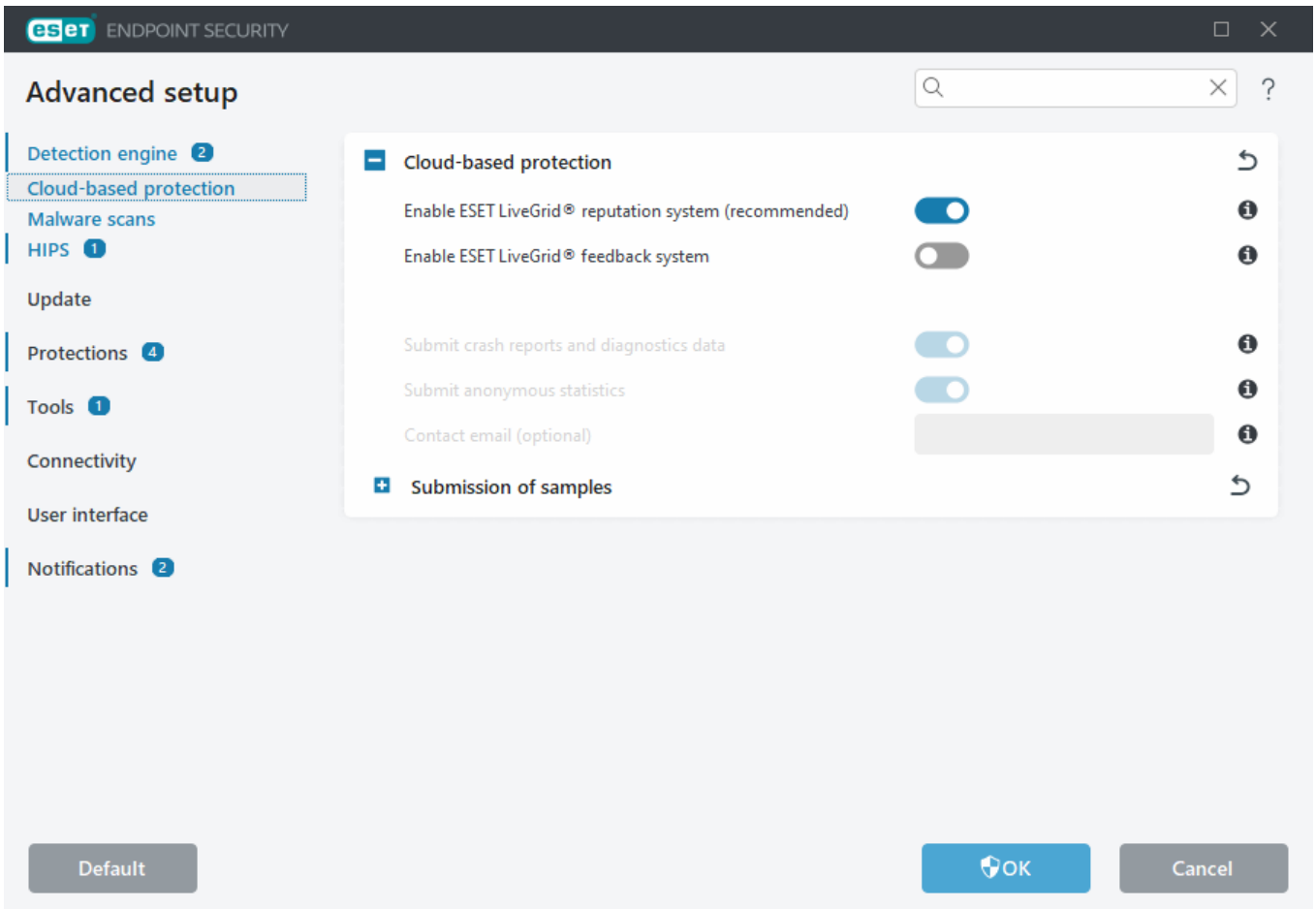
samples section below) along with crash reports and statistics to the ESET Research lab for further analysis.

Enable ESET LiveGuard (ESET LiveGuard is an additional functionality sold by ESET and is not available by default)—ESET LiveGuard is a paid service provided by ESET. Its purpose is to add a layer of protection specifically designed to mitigate never-before-seen threats. Suspicious files are automatically submitted to ESET cloud. In the cloud they are analyzed by our advanced malware detection engines. The user who provided the sample will receive a behavior report that provides a summary of the observed sample's behavior.

Submit crash reports and diagnostics data—Submit ESET LiveGrid® related diagnostics data such as crash reports and modules memory dumps. We recommend keeping it enabled to help ESET diagnose problems, improve the products, and ensure better end-user protection.

Submit anonymous statistics—Allow ESET to collect information about newly detected threats such as the threat name, date and time of detection, detection method and associated metadata, product version, and configuration including information about your system.

Contact email (optional)—Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. You will not receive a response from ESET unless more information is needed.



Submission of samples

Manual submission of samples—Enables you to manually submit samples to ESET from the context menu, Quarantine or Tools.

Automatic submission of detected samples

Select what kind of samples are submitted to ESET for analysis and to help improve future detection. The following options are available:

- **All detected samples**—All detected objects by Detection engine (including potentially unwanted applications when enabled in the scanner settings).
- **All samples except documents**—All detected objects except **Documents** (see below).
- **Do not submit**—Detected objects will not be sent to ESET.

Automatic submission of suspicious samples

These samples will also be sent to ESET if the detection engine did not detect them. For example, samples which nearly missed the detection, or one of the ESET Endpoint Security protection modules consider these samples as suspicious or have an unclear behavior.

- **Executables**—Includes files like .exe, .dll, .sys.
- **Archives**—Includes filetypes like .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripts**—Includes filetypes like .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Other**—Includes filetypes like .jar, .reg, .msi, .sfw, .lnk.
- **Possible Spam emails**—This will allow sending possible spam parts or whole possible spam emails with attachment to ESET for further analysis. Enabling this option improve global detection of spam including improvements to future spam detection for you.
- **Documents**—Include Microsoft Office or PDF documents with or without active content.

  Expand list of all included document file types

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Exclusions

The Exclusion filter enables you to exclude certain files/folders from submission (for example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets). The files listed will never be sent to ESET labs for analysis, even if they contain suspicious code. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

To exclude files downloaded from download.domain.com, open Advanced setup > **Cloud-based protection** > **Submission of samples** > **Exclusions** and add the exclusion *download.domain.com*.

Maximum size of samples (MB)—Defines the maximum size of automatically submitted samples (1-64 MB).

ESET LiveGuard

To enable ESET LiveGuard service on a client machine using ESET PROTECT On-Prem Web Console, see ESET LiveGuard configuration for ESET Endpoint Security.

If you have used ESET LiveGrid® before and have disabled it, there may still be data packages to send. Even after deactivating, such packages will be sent to ESET. When all current information is sent, no further packages will be created.

Exclusion filter for Cloud-based protection

The Exclusion filter enables you to exclude certain files or folders from samples submission. The files listed will never be sent to ESET labs for analysis, even if they contain suspicious code. Common file types (such as .doc, etc.) are excluded by default.

This feature is useful to exclude files that may carry confidential information, such as documents or spreadsheets.

To exclude files downloaded from download.domain.com, open Advanced setup > **Detection Engine** > **Cloud-based protection** > **Submission of samples** > **Exclusions** and add the exclusion *download.domain.com*.

Malware scans

The **Malware scans** section is accessible from Advanced setup > **Detection engine** > **Malware scans** and allows you to configure scanning parameters for scan profiles.

On-demand scan

Selected profile—A specific set of parameters used by the on-demand scanner. To create a new one, click **Edit** next to **List of profiles**. Refer to Scan profiles for more details.

After you select the scan profile, you can configure the following options:

Scan targets—If you want to scan a specific target or a group of targets, click **Edit** next to **Scan targets** and select an option from the folder (tree) structure. Refer to Scan targets for more details.

On-demand & detection responses—You can configure reporting and protection levels for each scan profile. By default, scan profiles use the same setup as defined in the Real-time file system protection. Disable the toggle next to **Use real-time protection settings** to configure custom reporting and protection levels. Refer to Protections for a detailed explanation of reporting and protection levels.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. Refer to ThreatSense for more information.

Scan profiles

There are 4 pre-defined scan profiles in ESET Endpoint Security:

- **Smart scan**—This is the default advanced scanning profile. The Smart scan profile uses Smart Optimization technology, which excludes files that were found to be clean in a previous scan and have not been modified since that scan. This allows for lower scan times with a minimal impact to system security.
- **Context menu scan**—You can start an on-demand scan of any file from the context menu. The Context menu scan profile enables you to define a scan configuration that will be used when you trigger the scan this way.
- **In-depth scan**—The In-depth scan profile does not use Smart optimization by default, so no files are excluded from scanning using this profile.

- **Computer scan**—This is the default profile used in the standard computer scan.

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open Advanced setup > **Detection engine** > **Malware scans** > **On-demand scan** > **List of profiles** > **Edit**. The **Profile manager** window includes the **Selected profile** drop-down menu that lists existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see ThreatSense for a description of each parameter of the scan setup.

> Suppose that you want to create your own scan profile and the **Scan your computer** configuration is partially suitable, but you do not want to scan runtime packers or potentially unsafe applications and you also want to apply **Always remedy detection**. Type the name of your new profile in the **Profile manager** window and click **Add**. Select your new profile from the **Selected profile** drop-down menu and adjust the remaining parameters to meet your requirements, and then click **OK** to save your new profile.

Scan targets

The **Scan targets** drop-down menu enables you to select pre-defined scan targets.

- **By profile settings**—Selects targets specified by the selected scan profile.
- **Removable media**—Selects diskettes, USB storage devices, CD/DVD.
- **Local drives**—Selects all system hard drives.
- **Network drives**—Selects all mapped network drives.
- **Custom selection**—Cancels all previous selections.

The folder (tree) structure also contains specific scan targets.

- **Operating memory**—Scans all processes and data currently used by operating memory.
- **Boot sectors/UEFI**—Scans Boot sectors and UEFI for the presence of malware. Read more about the UEFI scanner in the glossary.
- **WMI database**—Scans the whole Windows Management Instrumentation (WMI) database, all namespaces, all class instances, and all properties. Searches for references to infected files or malware embedded as data.
- **System registry**—Scans the whole system registry, all keys, and subkeys. Searches for references to infected files or malware embedded as data. When cleaning the detections, the reference remains in the registry to ensure no important data will be lost.

To quickly navigate to a scan target (file or folder), type its path into the text field below the tree structure. The path is case-sensitive. To include the target in the scan, select its check box in the tree structure.

Idle-state scan

You can enable the idle-state scanner in Advanced setup > **Detection engine** > **Malware scans** > **Idle-state scan**.

Idle-state scan

Enable the toggle next to **Enable Idle-state scanning** to enable this feature. When the computer is in idle state, a

silent computer scan is performed on all local drives.

By default, the idle-state scanner will not run when the computer (notebook) is operating on battery power. You can override this setting by enabling the toggle next to **Run even if computer is powered from battery** in Advanced setup.

Enable the toggle next to **Enable logging** in Advanced setup to record a computer scan output in the Log files section (from the main program window click **Tools** > **Log files** and select **Computer scan** from the **Log** drop-down menu).

Idle-state detection

See Idle state detection triggers for a full list of conditions that must be met to trigger the idle-state scanner.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. See ThreatSense for more information.

Idle-state detection

Idle state detection settings can be configured in Advanced setup > **Detection engine** > **Malware scans** > **Idle-state scanning** > **Idle state detection**. These settings specify a trigger for Idle-state scanning:

- **Turned off screen or screen saver**
- **Computer lock**
- **User logoff**

Use the toggle for each respective state to enable or disable the different idle state detection triggers.

Startup scan

By default, the automatic startup file check will be performed on system startup and during detection engine updates. This scan is dependent on the Scheduler configuration and tasks.

The startup scan options are part of a **System startup file check** scheduler task. To modify its settings, navigate to **Tools** > **Scheduler**, click **Automatic startup file check** and then **Edit**. In the last step, the Automatic startup file check window will appear. For detailed instructions about Scheduler task creation and management, see Creating new tasks.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. See ThreatSense for more information.

Automatic startup file check

When creating a System startup file check scheduled task, you have several options to adjust the following parameters:

The **Scan target** drop-down menu specifies the scan depth for files run at system startup based on a sophisticated algorithm. Files are arranged in descending order according to the following criteria:

- **All registered files** (most files scanned)
- **Rarely used files**
- **Commonly used files**
- **Frequently used files**
- **Only the most frequently used files** (least files scanned)

Two specific groups are also included:

- **Files run before user logon**—Contains files from locations that may be accessed without the user being logged in (includes almost all startup locations such as services, browser helper objects, winlogon notify, Windows scheduler entries, known dll's, etc.).
- **Files run after user logon**—Contains files from locations that may only be accessed after a user has logged in (includes files only run by a specific user, typically files in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Lists of files to be scanned are fixed for each group above. If you choose a lower scan depth for files run at system startup, the not scanned files will be scanned after opening or execution.

Scan priority—The level of priority used to determine when a scan will start:

- **When idle**—the task will be performed only when the system is idle,
- **Lowest**—when the system load is the lowest possible,
- **Lower**—at a low system load,
- **Normal**—at an average system load.

Document protection

The Document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements. Document protection provides a layer of protection in addition to Real-time file system protection, and can be disabled to enhance performance on systems that do not handle a high number of Microsoft Office documents.

To activate Document protection, open Advanced setup > **Detection engine** > **Malware scans** > **Document protection** and click the toggle next to **Enable Document protection**.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. See ThreatSense for more information.

> This feature is activated by applications that use the Microsoft Antivirus API (for example, Microsoft Office 2000 and later, or Microsoft Internet Explorer 5.0 and later).

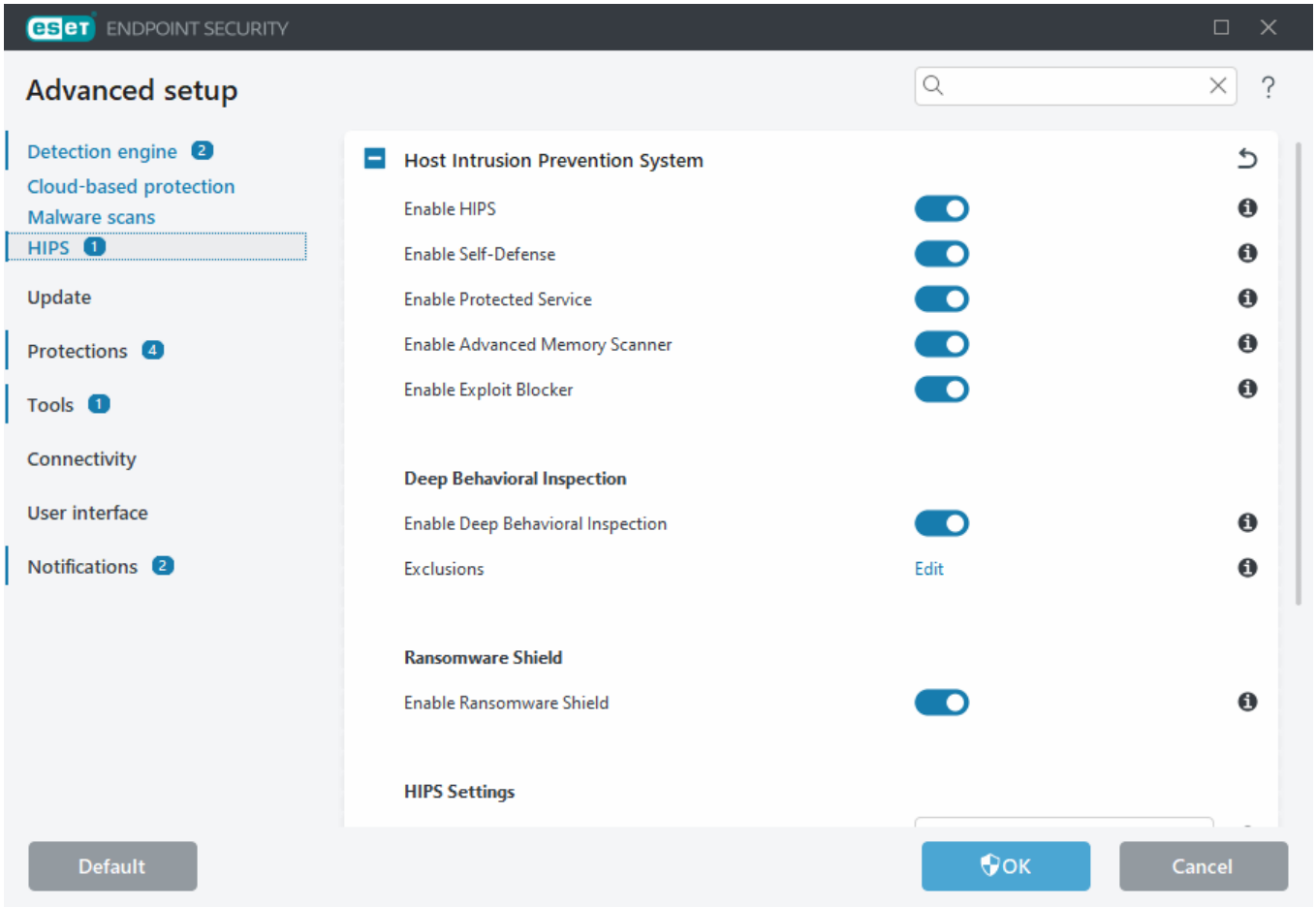
HIPS - Host-based Intrusion Prevention System)

> Changes to HIPS settings should only be made by an experienced user. Incorrect configuration of HIPS settings can lead to system instability.

The Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate

from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

You can configure HIPS settings in Advanced setup > **Detection engine** > **HIPS** > **Host Intrusion Prevention System**. The HIPS state (enabled/disabled) is shown in the ESET Endpoint Security main program window > **Setup** > **Computer**.



Host Intrusion Prevention System

Enable HIPS—HIPS is enabled by default in ESET Endpoint Security. Turning off HIPS will disable rest of the HIPS features like Exploit Blocker.

Enable Self-Defense—ESET Endpoint Security uses the built-in **Self-defense** technology as a part of HIPS to prevent malicious software from corrupting or disabling your antivirus and antispyware protection. Self-defense protects crucial system and ESET's processes, registry keys and files from being tampered with. ESET Management Agent is protected as well when installed.

Enable Protected Service—Enables protection for ESET Service (ekrn.exe). When enabled, the service is started as a protected Windows process to defend attacks by malware. This option is available in Windows 8.1 and Windows 10.

Enable Advanced memory scanner—Works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced memory scanner is enabled by default. Read more about this type of protection in the glossary.

Enable Exploit Blocker—Designed to fortify commonly exploited application types such as web browsers, PDF

readers, email clients and Microsoft Office components. Exploit blocker is enabled by default. Read more about this type of protection in the glossary.

Deep Behavioral Inspection

Enable Deep Behavioral Inspection—Another layer of protection that works as a part of the HIPS feature. This extension of HIPS analyzes the behavior of all programs running on the computer and warns you if the behavior of the process is malicious.

HIPS exclusions from Deep Behavioral Inspection—Enables you to exclude processes from analysis. To ensure that all processes are scanned for possible threats, we recommend only creating exclusions when it is absolutely necessary.

Ransomware shield

Enable Ransomware shield—Another layer of protection that works as a part of HIPS feature. You must have the ESET LiveGrid® reputation system enabled for Ransomware shield to work. Read more about this type of protection.

Enable Intel® Threat Detection Technology—Helps to detect ransomware attacks by utilizing unique Intel CPU telemetry to increase detection efficacy, lower false positive alerts, and expand visibility to catch advanced evasion techniques. See the supported processors.

Enable Audit mode—Everything detected by the Ransomware shield is not automatically blocked, but logged with a warning severity and sent to the management console with the "AUDIT MODE" flag. Administrator can either decide to exclude such detection to prevent further detection, or keep it active, which means that after Audit mode ends, it will be blocked and removed. Enabling/disabling the Audit mode will also be logged in ESET Endpoint Security. This option is available only in the ESET PROTECT On-Prem policy configuration editor.

HIPS settings

Filtering mode can be performed in one of the following modes:

Filtering mode	Description
Automatic mode	Operations are enabled with the exception of those blocked by pre-defined rules that protect your system.
Smart mode	The user will only be notified about very suspicious events.
Interactive mode	User will be prompted to confirm operations.
Policy-based mode	Blocks all operations that are not defined by a specific rule that allows them.
Learning mode	Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the **HIPS rules** editor, but their priority is lower than the priority of rules created manually or rules created in automatic mode. When you select **Learning mode** from the **Filtering mode** drop down menu, the **Learning mode will end at** setting will become available. Select the time span that you want to engage learning mode for, the maximum duration is 14 days. When the specified duration has passed, you will be prompted to edit the rules created by HIPS while it was in learning mode. You can also choose a different filtering mode, or postpone the decision and continue using learning mode.

Mode set after learning mode expiration—Select the filtering mode that will be used after learning mode

expires. After expiration, the **Ask user** option requires administrative privileges to perform a change to the HIPS filtering mode.

The HIPS system monitors events inside the operating system and reacts accordingly based on rules similar to those used by the Firewall. Click **Edit** next to **Rules** to open the **HIPS rules** editor. In the HIPS rules window you can select, add, edit or remove rules. More details on rule creation and HIPS operations can be found in Edit a HIPS rule.

HIPS exclusions

Exclusions enable you to exclude processes from HIPS Deep Behavioral Inspection.

To Edit HIPS exclusions, open Advanced setup > **Detection engine** > **HIPS** > **Host Intrusion Prevention System** > **Exclusions** > **Edit**.

> Not to be confused with Excluded file extensions, Detection exclusions, Performance exclusions or Processes exclusions.

To exclude an object, click **Add** and type the path to an object or select it in the tree structure. You can also Edit or Delete selected entries.

HIPS advanced setup

The following options are useful for debugging and analyzing an application's behavior:

Drivers always allowed to load—Listed drivers are always allowed to load regardless of configured filtering mode unless explicitly blocked by user rule.

Log all blocked operations—All blocked operations will be written to the HIPS log. Use this feature only when troubleshooting or requested by ESET Technical Support, as it might generate a huge log file and slow down your computer.

Notify when changes occur in Startup applications—Displays a desktop notification each time an application is added to or removed from system startup.

Drivers always allowed to load

Drivers shown in this list will always be allowed to load regardless of HIPS filtering mode, unless explicitly blocked by user rule.

Add—Adds a new driver.

Edit—Edits a selected driver.

Remove—Removes a driver from the list.

Reset—Reloads a set of system drivers.

Click **Reset** if you do not want drivers that you have added manually to be included. This can be useful if you have added several drivers and you cannot delete them from the list manually.

After installation, the list of drivers is empty. ESET Endpoint Security fills the list automatically over time.

Drivers always allowed to load are specific for each device and cannot be edited using ESET PROTECT On-Prem policy. After installation, the list of drivers is empty. ESET Endpoint Security fills the list automatically over time.

HIPS interactive window

The HIPS notification window enables you to create a rule based on new actions that HIPS detects and then define the conditions under which to allow or deny an action.

Rules created from the notification window are considered to be equivalent to rules created manually. A rule created from a notification window can be less specific than the rule that triggered that dialog window. This means that after creating a rule in the dialog box, the same operation can trigger the same window. For more information see Priority for HIPS rules.

If the default action for a rule is set to **Ask every time**, a dialog window will be displayed each time that the rule is triggered. You can choose to **Deny** or **Allow** the operation. If you do not choose an action in the given time, a new action is selected based on the rules.

Remember until application quits causes the action (**Allow/Deny**) to be used until a change of rules or filtering mode, a HIPS module update or a system restart. After any of these three actions, temporary rules will be deleted.

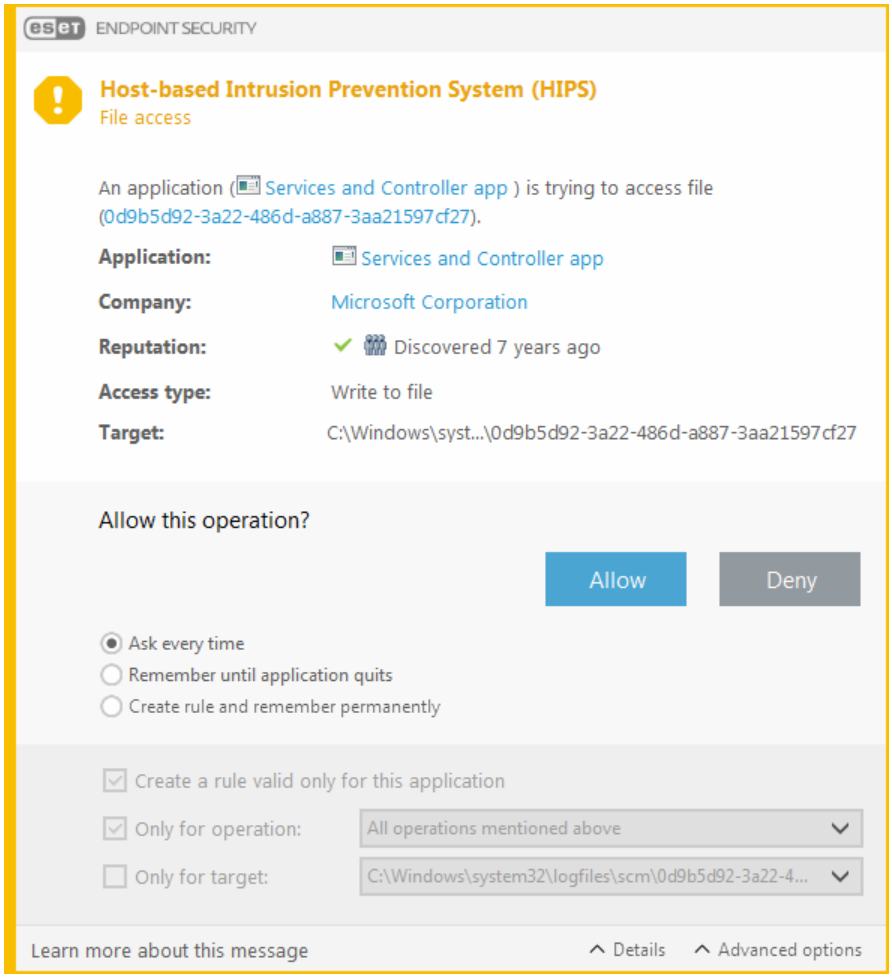
The **Create rule and remember permanently** option will create a new HIPS rule which can be later altered in the HIPS rule management section (requires administration privileges).

Click **Details** on the bottom to see what application triggers the operation, what is the reputation of the file or what kind of operation you are asked to allow or deny.

Settings for the more detailed rule parameters can be accessed by clicking **Advanced options**. The options below are available if you select **Create rule and remember permanently**:

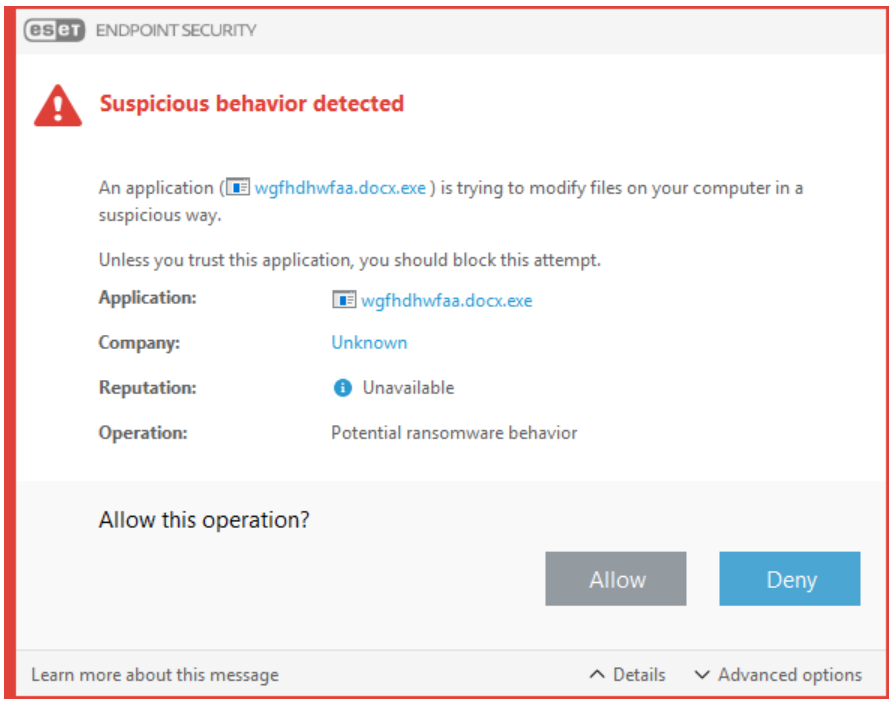
- **Create a rule valid only for this application**—If you deselect this check box, the rule will be created for all source applications.
- **Only for operation**—Select the rule file/application/registry operation(s). See descriptions for all HIPS operations.
- **Only for target** –Select the rule file/application/registry target(s).

To stop the notifications from appearing, change the filtering mode to **Automatic mode** in Advanced setup > **Detection engine** > **HIPS** > **Basic**.



Potential ransomware behavior detected

This interactive window will appear when potential ransomware behavior is detected. You can choose to **Deny** or **Allow** the operation.



Click **Details** to view specific detection parameters. The dialog window enables you to **Submit for analysis** or **Exclude from detection**.

ESET LiveGrid® must be enabled for Ransomware protection to function properly.

HIPS rule management

This is a list of user-defined and automatically-added rules in the HIPS system. More details about rule creation and HIPS operations can be found in the HIPS rules settings chapter. See also General principle of HIPS.

Columns

Rule—User-defined or automatically chosen rule name.

Enabled—Deactivate this option if you want to keep the rule in the list but do not want to use it.

Action—The rule specifies an action – **Allow**, **Block** or **Ask** – that should be performed when the conditions are met.

Sources—The rule will be used only if the event is triggered by an application(s).

Targets—The rule will be used only if the operation is related to a specific file, application or registry entry.

Logging severity—If you activate this option, information about this rule will be written to the HIPS log.

Notify—A notification appears in the lower-right corner if an event is triggered.

Control elements

Add—Creates a new rule.

Edit—Enables you to edit selected entries.

Delete—Removes selected entries.

Priority for HIPS rules

There are no options to adjust the priority level of HIPS rules using the top/bottom buttons (as for Firewall rules where rules are executed from top to bottom).

- All rules that you create have the same priority
- The more specific the rule, the higher the priority (for example, the rule for a specific application has higher priority than the rule for all applications)
- Internally, HIPS contains higher-priority rules that are not accessible to you (for example, you cannot override Self-defense defined rules)
- A rule you create that might freeze your operating system will not be applied (will have the lowest priority)

HIPS rule settings

See HIPS rule management as first.

Rule name—User-defined or automatically chosen rule name.

Action—Specifies an action – **Allow**, **Block** or **Ask** – that should be performed if conditions are met.

Operations affecting—You must select the type of operation for which the rule will be applied. The rule will be used only for this type of operation and for the selected target.

Enabled—Disable the toggle if you want to keep the rule in the list but not apply it.

Logging severity—If you activate this option, information about this rule will be written to the HIPS log.

Notify user—A notification appears in the lower-right corner if an event is triggered.

The rule consists of parts that describe the conditions triggering this rule:

Source applications—The rule will be used only if the event is triggered by this application(s). Select **Specific applications** from drop-down menu and click **Add** to add new files or you can select **All applications** from the drop-down menu to add all applications.

Target files—The rule will be used only if the operation is related to this target. Select **Specific files** from drop-down menu and click **Add** to add new files or folders or you can select **All files** from the drop-down menu to add all files.

Applications—The rule will be used only if the operation is related to this target. Select **Specific applications** from the drop-down menu and click **Add** to add new files or folders or you can select **All applications** from the drop-down menu to add all applications.

Registry entries—The rule will be used only if the operation is related to this target. Select **Specific entries** from the drop-down menu and click **Add** to add new files or folders, or you can select **All entries** from the drop-down menu to add all applications.

> Some operations of specific rules pre-defined by HIPS cannot be blocked and are allowed by default. In addition, not all system operations are monitored by HIPS. HIPS monitors operations that may be considered unsafe.

> When specifying a path, C:\example affects actions with the folder itself, and C:\example*.* affects the files in the folder.

Application operations

- **Debug another application**—Attaching a debugger to the process. While debugging an application, many details of its behavior can be viewed and modified and its data can be accessed.
- **Intercept events from another application**—The source application is attempting to catch events targeted at a specific application (for example a keylogger trying to capture browser events).
- **Terminate/suspend another application**—Suspending, resuming or terminating a process (can be accessed directly from Process Explorer or the Processes pane).
- **Start new application**—Starting of new applications or processes.

- **Modify state of another application**—The source application is attempting to write into the target applications' memory or run code on its behalf. This functionality may be useful to protect an essential application by configuring it as a target application in a rule blocking the use of this operation.

Registry operations

- **Modify startup settings**—Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for the Run key in the Windows Registry.
- **Delete from registry**—Deleting a registry key or its value.
- **Rename registry key**—Renaming registry keys.
- **Modify registry**—Creating new values of registry keys, changing existing values, moving data in the database tree or setting user or group rights for registry keys.

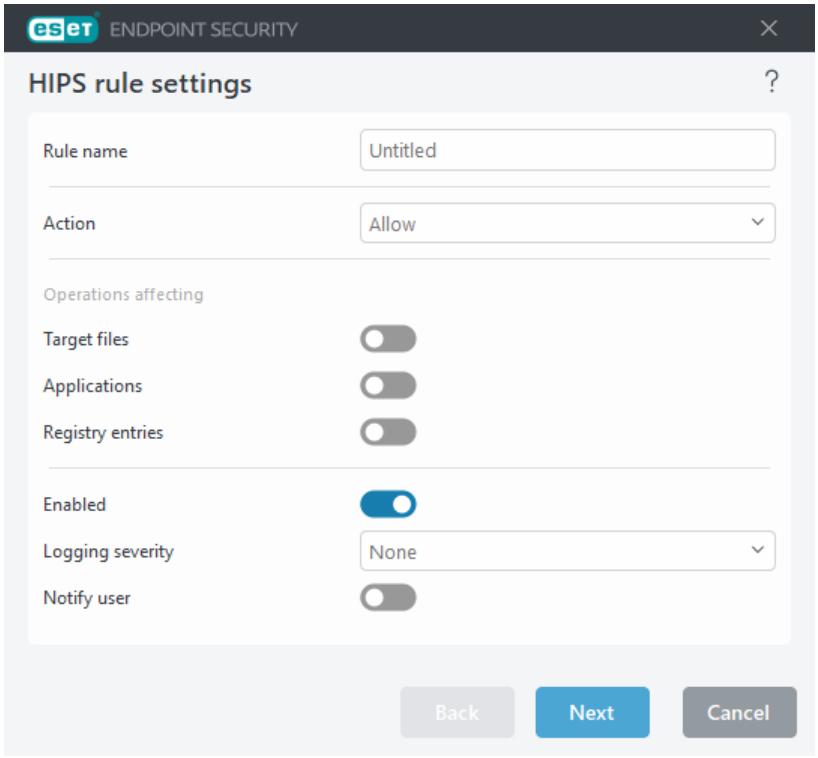
Using wildcards in rules
An asterisk in rules can only be used to substitute a specific key, e.g. “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start”. Other ways of using wildcards are not supported.

Creating rules targeting HKEY_CURRENT_USER key
This key is just a link to the appropriate subkey of HKEY_USERS specific to the user identified by SID (secure identifier). To create a rule only for the current user, instead of using a path to HKEY_CURRENT_USER, use a path pointing to HKEY_USERS\%SID%. As SID you can use an asterisk to make the rule applicable for all users.

If you create a very generic rule, the warning about this type of rule will be shown.

In the following example, we will demonstrate how to restrict unwanted behavior of a specific application:

1. Name the rule and select **Block** (or **Ask** if you prefer to choose later) from the **Action** drop-down menu.
2. Enable the **Notify user** switch to display a notification any time that a rule is applied.
3. Select at least one operation in the **Operations affecting** section for which the rule will be applied.
4. Click **Next**.
5. In the **Source applications** window, select **Specific applications** from the drop-down menu to apply your new rule to all applications attempting to perform any of the selected application operations on the applications you specified.
6. Click **Add** and then **...** to choose a path to a specific application and then press **OK**. Add more applications if you prefer.
   For example: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Select the **Write to file** operation.
8. Select **All files** from the drop-down menu. This will block any attempts to write to any files by the selected application(s) from the previous step.
9. Click **Finish** to save your new rule.



Add applicaton/registry path for HIPS

Select a file application path by clicking the **...** option. While selecting a folder, all applications located at this location will be included.

The **Open Registry Editor** option will start the Windows registry editor (regedit). While adding a registry path, type the correct location to the **Value** field.

Examples of the file or registry path:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Update

Update setup options are available in Advanced setup > **Update**. This section specifies update source information like the update servers being used and authentication data for these servers.

For updates to be downloaded properly, it is essential that you fill in all update parameters correctly. If you use a firewall, ensure that your ESET program is allowed to communicate with the internet (for example, HTTPS communication).

Update

The update profile currently in use is displayed in the **Select default update profile** drop-down menu.

To create a new profile, see the Update profiles section.

Automatic profile switching—Enables you to set an update profile for a specific network connection profile.

Configure update notifications—Click Edit to select what application notifications are displayed. You can choose if the notifications Show on a desktop and/or are Send by email.

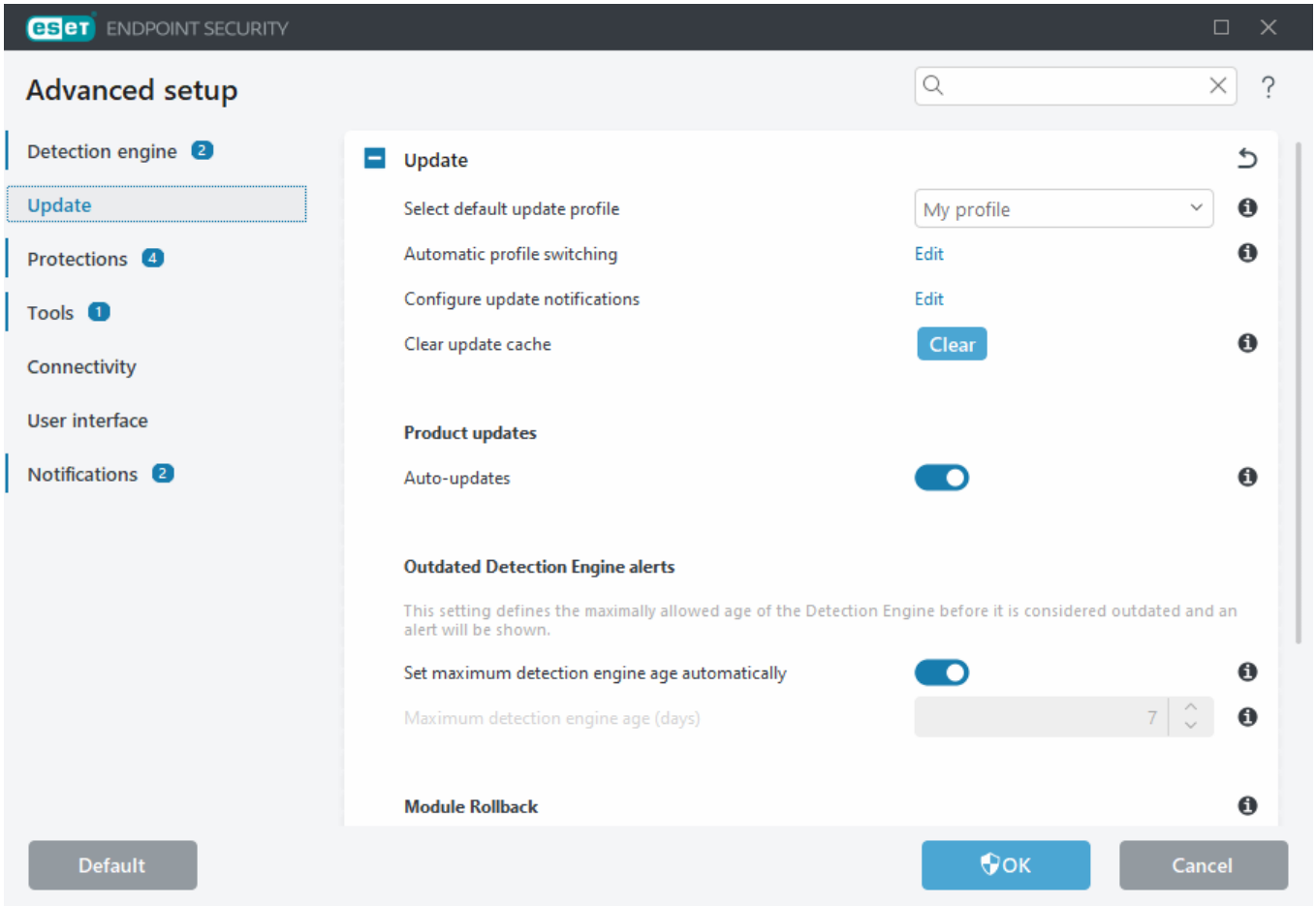
If you are experiencing difficulty when attempting to download modules updates, click **Clear** next to **Clear update cache** to clear the temporary update files/cache.

Outdated Detection Engine alerts

Set maximum detection engine age automatically—Allows to set maximum time (in days) after which the detection engine will be reported as out of date. Default value of **Maximum detection engine age (days)** is 7.

Module Rollback

If you suspect that a new update of the detection engine and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time.



Profiles

Update profiles can be created for various update configurations and tasks. Creating update profiles is especially useful for mobile users who need an alternative profile for internet connection properties that regularly change.

The **Select profile to edit** drop-down menu displays the currently selected profile and is set to **My profile** by default.

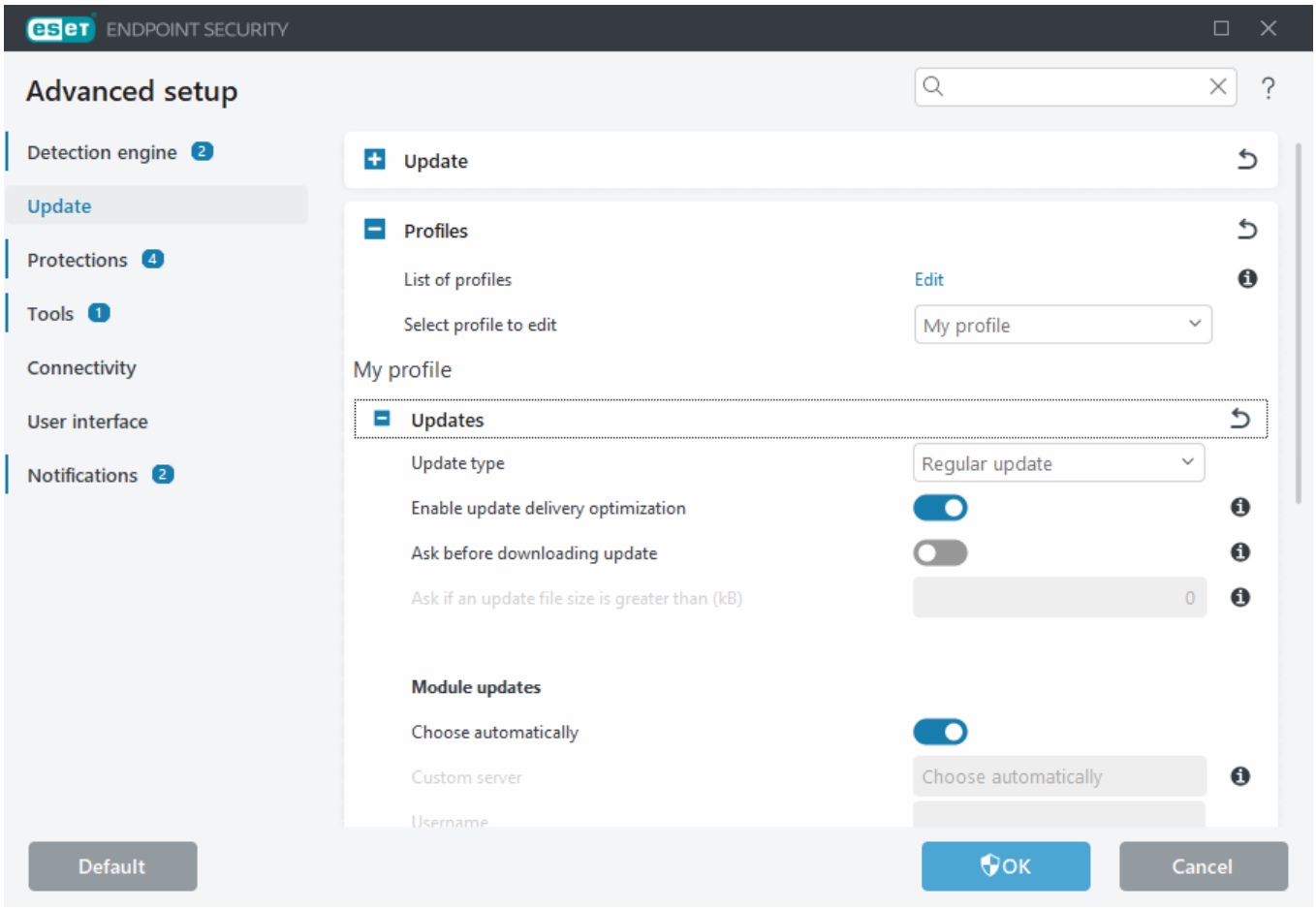
To create a new profile, click **Edit** next to **List of profiles**, type your own **Profile name** and then click **Add**.

Updates

By default, the **Update type** is set to **Regular update** to ensure that update files will automatically be download from the ESET server with the least network traffic. Pre-release updates (the **Pre-release update** option) are updates that have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times and SHOULD NOT be used on production servers and workstations where maximum availability and stability is required. Delayed update allows updating from special update servers providing new versions of virus databases with a delay of at least X hours (i.e. databases tested in a real environment and therefore considered as stable).

Enable update delivery optimization—When enabled, update files may be downloaded from CDN (content delivery network). Disabling this setting may cause download interruptions and slowdowns when dedicated ESET update servers are overloaded. Disabling is useful when a firewall is limited to access ESET update server IP addresses only or a connection to CDN services are not working.

Ask before downloading update—The program will display a notification where you can choose to confirm or decline update file downloads. If the update file size is greater than the value specified in the Ask if an update file size is greater than (kB) field, the program will display a confirmation dialog. If the update file size is set to 0 kB, the program will always display a confirmation dialog.



Modules updates

The **Choose automatically** option is enabled by default. The **Custom server** option is the location where updates are stored. If you use an ESET update server, we recommend that you leave the default option selected.

Enable more frequent updates of detection signatures—Detection signatures will be updated in shorter interval. Disabling this setting may negatively impact detection rate.

Allow module updates from removable media—Enables you to update from removable media if it contains created mirror. When Automatic selected, update will run on background. If you want to show update dialogs select Always ask.

When using a local HTTP server – also known as a Mirror—the update server should be set as follows: *http://computer_name_or_its_IP_address:2221*

When using a local HTTP server with SSL—the update server should be set as follows: *https://computer_name_or_its_IP_address:2221*

When using a local shared folder—the update server should be set as follows: *\\computer_name_or_its_IP_address\shared_folder*

> HTTP server port number specified in the examples above depends on what port your HTTP/HTTPS server listens.

Product updates

See Product updates.

Connection options

See Connection options.

Update mirror

See Update mirror.

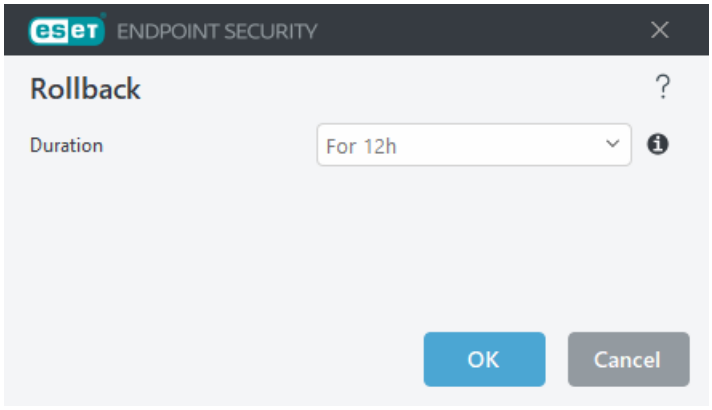
Update rollback

If you suspect that a new detection engine update or program modules may be unstable or corrupt, you can roll back to the previous version and temporarily disable updates. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.

ESET Endpoint Security records snapshots of the detection engine and program modules for use with the rollback feature. To create virus database snapshots, keep **Create snapshots of modules** enabled. When **Create snapshots of modules** enabled, the first snapshot is created during the first update. The next one is created after 48 hours. The **Number of locally stored snapshots** field defines the number of stored detection engine snapshots.

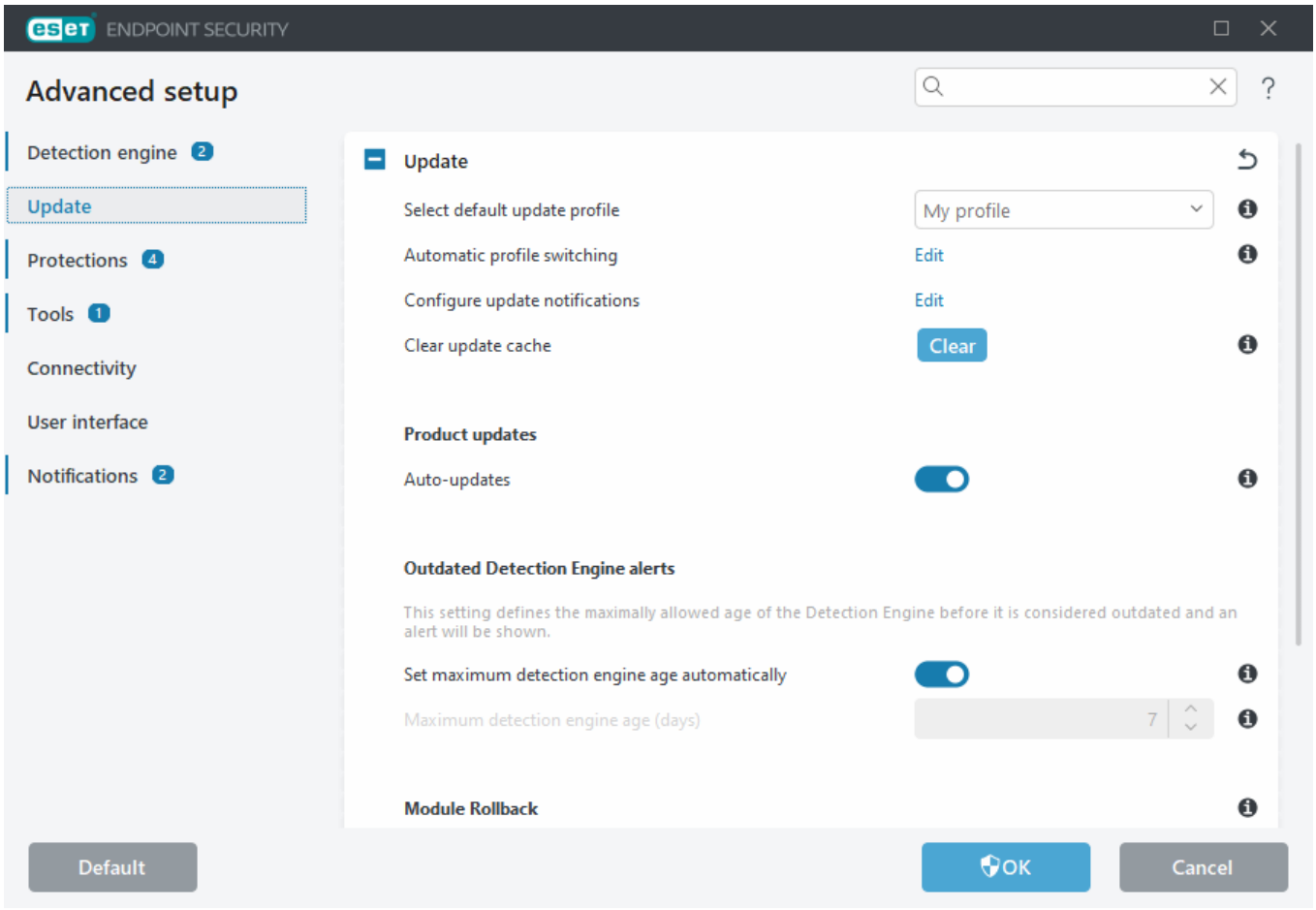
> When the maximum amount of snapshots is reached (for example, three), the oldest snapshot is replaced with a new snapshot every 48 hours. ESET Endpoint Security rolls back detection engine and program module update versions to the oldest snapshot.

Open Advanced setup > **Update** > **Update** > **Module rollback** > **Rollback** to select a time interval from the **Duration** drop-down menu.



Select **Until revoked** to postpone regular updates indefinitely until you restore update functionality manually. We do not recommend selecting this option because it represents a potential security risk.

If a rollback is performed, the **Rollback** button changes to **Allow updates**. Updates are not allowed for the time interval selected from the **Suspend updates** drop-down menu. The detection engine version is downgraded to the oldest available version and stored as a snapshot in the local computer file system.



Assume 22700 is the most recent detection engine version number, and 22698 and 22696 are stored as detection engine snapshots. Note that 22697 is unavailable. In this example, the computer was turned off during the 22697 update, and a more recent update was made available before 22697 was downloaded. If the **Number of locally stored snapshots** field is two and you click **Rollback**, the detection engine (including program modules) is restored to version number 22696. This process may take some time. Verify the detection engine version has downgraded on the Update screen.

Product updates

The **Product updates** section contains options related to the product updates. The program enables you to predefine its behavior when a new product updates are available.

Product updates bring new features or makes changes to those that already exist from previous versions. It can be performed automatically without user intervention, or you can choose to be notified. After a product updates have been installed, a computer restart may be required.

Auto-updates—Pausing auto-updates for specific update profiles temporarily disables automatic product updates while connected to the internet using other networks or metered connections. Keep this setting enabled to have constant access to the latest features and the highest possible protection. For more information on Auto-updates, see Auto-updates FAQ.

By default, product updates are downloaded from ESET repository servers. In large or offline environments, the traffic can be distributed to allow internal caching of the product files.

Define custom server for program component updates

1. Define the path to the product updates in the **Custom server** field.
It can be an HTTP(S) link, SMB network share path, a local disk drive or a removable media path. For network drives, use the UNC path instead of a mapped drive letter.
2. Leave **Username** and **Password** blank if not required.
If required, define the appropriate credentials here for HTTP authentication on the custom web server.
3. Confirm the changes and test the presence of a product updates using a standard ESET Endpoint Security update.

Selecting the most appropriate option depends on the workstation where the settings will be applied. There are differences between workstations and servers – for example, restarting the server automatically after a product update can cause significant damage to your company.

Connection options

To access the proxy server setup options for a given update profile, open Advanced setup > **Update** > **Profiles** > **Updates** > **Connection options**.

Proxy server

Click the **Proxy mode** drop-down menu and select one of the three following options:

- Do not use proxy server
- Connection through a proxy server
- Use global proxy server settings

Select **Use global proxy server settings** to use the proxy server configuration options already specified in Advanced setup > **Connectivity** > **Proxy server**.

Select **Do not use proxy server** to specify that no proxy server will be used to update ESET Endpoint Security.

Connection through a proxy server option should be selected if:

- A different proxy server than the one defined in **Tools** > **Proxy server** is used to update ESET Endpoint Security. In this configuration, information for the new proxy should be specified under **Proxy server** address, communication **Port** (3128 by default), and **Username** and **Password** for the proxy server if required.
- Proxy server settings are not set globally, but ESET Endpoint Security will connect to a proxy server for updates.
- Your computer is connected to the internet via a proxy server. Settings are taken from the browser during program installation, but if they are changed (for example, if you change your ISP), ensure the proxy settings listed in this window are correct. Otherwise the program will not be able to connect to update servers.

The default setting for the proxy server is **Use global proxy server settings**.

Use direct connection if proxy is not available—Proxy will be bypassed during update if it is unreachable.

Windows shares

When updating from a local server with a version of the Windows NT operating system, authentication for each network connection is required by default.

To configure such an account, select from the **Connect to LAN as** drop-down menu:

- **System account (default)**,
- **Current user**,
- **Specified user**.

Select **System account (default)** to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authenticates using a currently logged-in user account, select **Current user**. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

Select **Specified user** if you want the program to use a specific user account for authentication. Use this method when the default system account connection fails. The specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

Username and **Password** settings are optional.

When either **Current user** or **Specified user** is selected, an error may occur when changing the identity of the program to the desired user. We recommend entering the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be typed as follows: *domain_name**user* (if it is a workgroup, type *workgroup_name**name*) and password. When updating from the HTTP version of the local server, no authentication is required.

Select **Disconnect** from server after update to force a disconnection if a connection to the server remains active even after updates have been downloaded.

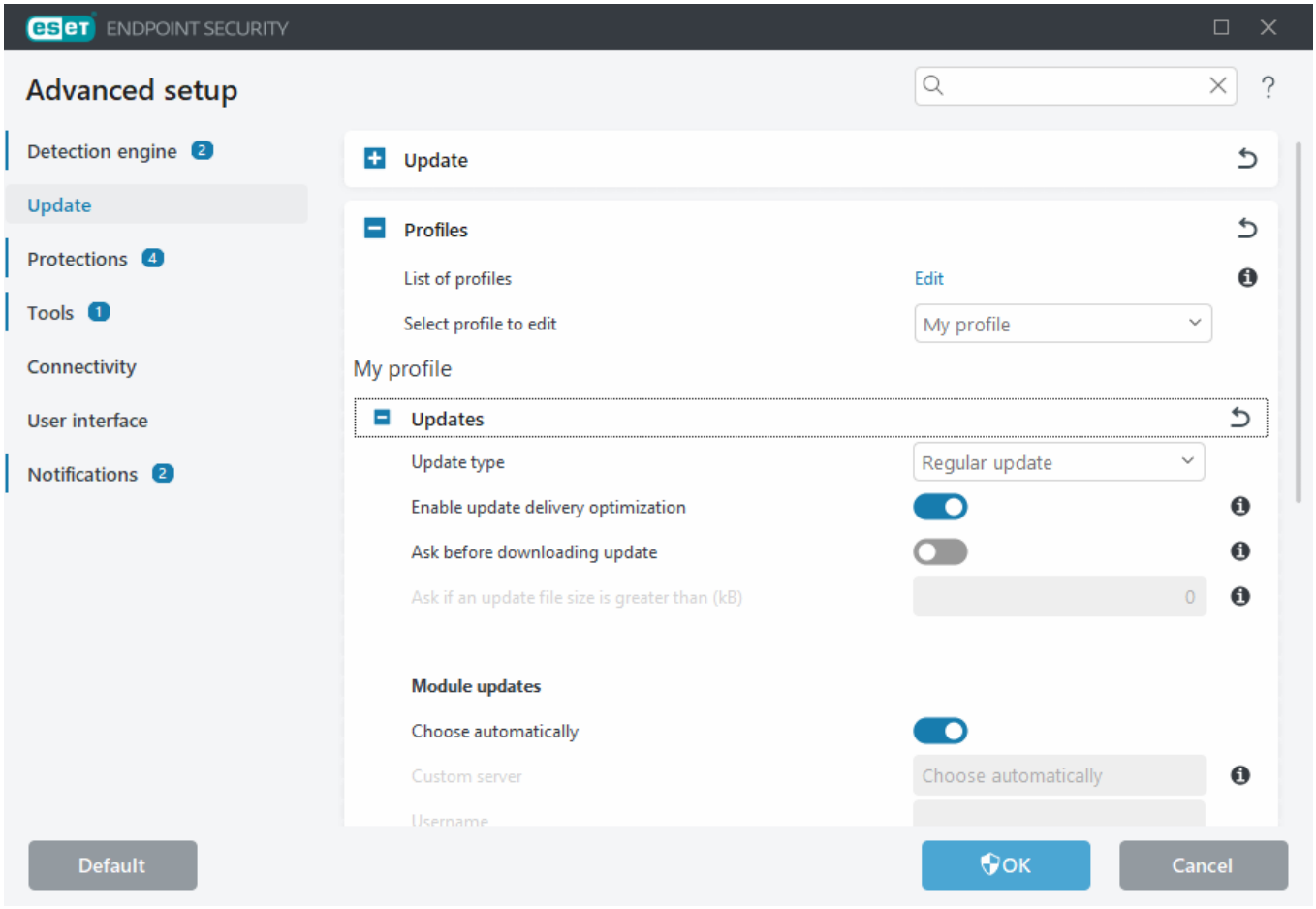
Update mirror

ESET Endpoint Security enables you to create copies of update files that can be used to update other workstations on the network. The use of a "mirror" – a copy of the update files in the LAN environment is convenient because the update files do not need to be downloaded from the vendor update server repeatedly by each workstation. Updates are downloaded to the local mirror server and then distributed to all workstations to avoid the risk of network traffic overload. Updating client workstations from a Mirror optimizes network load balance and saves internet connection bandwidth.

Update mirror creates copies of update files that can be used to update workstations that are running the same generation of the ESET Endpoint Security for Windows (for example, ESET Endpoint Security for Windows version 10.x creates update files only for version 10.x ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows).

To minimize internet traffic on networks where ESET PROTECT On-Prem or ESET PROTECT is used to manage a large number of clients, we recommend that you use ESET Bridge rather than configure a client as a mirror. ESET Bridge can be installed with ESET PROTECT On-Prem or ESET PROTECT using the all-in-one installer or as a standalone component. For more information and differences between ESET Bridge, Apache HTTP Proxy, Mirror Tool, and direct connectivity, see our <%ESET PROTECT%> Online Help page.

Configuration options for the local Mirror server are located in Advanced setup > **Update** > **Profiles** > **Update Mirror**.



To create a mirror on a client workstation, enable **Create update mirror**. Enabling this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

Access to update files

Enable HTTP server—If enabled, update files can be accessed through HTTP, no credentials are required.

Methods to access the Mirror server are described in detail in Updating from the Mirror. There are two basic methods for accessing the Mirror – the folder with update files can be presented as a shared network folder, or clients can access the mirror located on an HTTP server.

The folder dedicated to storing update files for the Mirror is defined under **Folder to store mirrored files**. To choose a different folder click **Clear** to delete pre-defined folder *C:\ProgramData\ESET\ESET Endpoint Security\mirror* and click **Edit** to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be typed in the **Username** and **Password** fields. If the selected destination folder is located on a network disk running the Windows NT/2000/XP operating system, the username and password specified must have write privileges for the selected folder. The username should be typed in the format *Domain/User* or *Workgroup/User*. Remember to supply the corresponding passwords.

HTTP Server and SSL for the Mirror

In the **HTTP Server** section of the **Mirror** tab you can specify the **Server port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to **2221**.

The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **None**, **Basic**, and **NTLM**. Select **Basic** to use base64 encoding with basic username and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **None**, which grants access to the update files with no need for authentication.

Authentication data such as **Username** and **Password** is intended only for accessing the mirror HTTP server. Complete these fields only if a username and password are required.

Append your **Certificate chain file**, or generate a self-signed certificate if you want to run HTTP server with HTTPS (SSL) support. The following **certificate types** are available: ASN, PEM and PFX. For additional security, you can use HTTPS protocol to provide update files for download. It is almost impossible to track data transfers and login credentials using this protocol. The **Private key type** option is set to **Integrated** by default (and therefore the **Private key file** option is disabled by default). This means that the private key is a part of the selected certificate chain file.

Self-signed certificates for HTTPS mirror
If you are using an HTTPS mirror server, you need to import its certificate to the trusted root store on all client machines. See Installing the trusted root certificate in Windows.

Updating from the Mirror

There are two basic methods to configure a Mirror, which is essentially a repository where clients can download update files. The folder with update files can be presented as a shared network folder or as an HTTP server.

Update mirror creates copies of update files that can be used to update workstations that are running the same generation of the ESET Endpoint Security for Windows (for example, ESET Endpoint Security for Windows version 10.x creates update files only for version 10.x ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows).

Accessing the Mirror using an internal HTTP server

This is the default configuration specified in the pre-defined program configuration. To allow access to the Mirror using the HTTP server, open Advanced setup > **Update** > **Profiles** > **Update mirror** and select **Create update mirror**.

In the **HTTP Server** section of the **Mirror** tab you can specify the **Server port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to **2221**.

The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **None**, **Basic**, and **NTLM**. Select **Basic** to use base64 encoding with basic username and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **None**, which grants access to the update files with no need for authentication.

If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Endpoint Security instance creating it.

An error **Invalid Username and/or Password** will appear in the Update pane from the main menu after several unsuccessful attempts to update from the Mirror. We recommend that you open Advanced setup > **Update** > **Profiles** > **Update mirror** and check the Username and Password. The most common reason for this error is incorrectly entered authentication data.

After your Mirror server is configured, you must add the new update server on client workstations. To do this, follow the steps below:

- Open Advanced setup and click **Update** > **Profiles** > **Updates** > **Module updates**.
- Disable **Choose automatically** and add a new server to the **Update server** field using one of the following formats:
  http://IP_address_of_your_server:2221
  https://IP_address_of_your_server:2221 (if SSL is used)

Accessing the Mirror via system shares

First, a shared folder should be created on a local or network device. When creating the folder for the Mirror, you must provide “write” access for the user who will save update files to the folder and “read” access for all users who will update ESET Endpoint Security from the Mirror folder.

Next, configure access to the Mirror in Advanced setup > **Update** > **Profiles** > **Update mirror** tab by disabling **Enable HTTP server**. This option is enabled by default in the program install package.

If the shared folder is located on another computer in the network, you must type authentication data to access the other computer. To type authentication data, open Advanced setup and click **Update** > **Profiles** > **Updates** > **Connection options** > **Windows shares** > **Connect to LAN as**. This is the same setting used for updating, as described in the Connect to LAN as section.

To access the mirror folder, this needs to be done under the same account as the one used for logging into the computer the mirror is created on. If the computer is in a domain, "domain\user" username should be used. If the computer is not in a domain, "IP_address_of_your_server\user" or "hostname\user" should be used.

After the Mirror configuration is complete, on client workstations set *\\UNC\PATH* as the update server using the steps below:

1. Open Advanced setup and click **Update** > **Profiles** > **Updates**.
2. Disable **Choose automatically** next to **Module updates** and a new server to the **Update server** field using the *\\UNC\PATH* format.

For updates to function properly, the path to the Mirror folder must be specified as a UNC path. Updates from mapped drives may not work.

Creating the Mirror using Mirror Tool
The Mirror tool creates a structure of folders different from what Endpoint mirror does. Each folder holds update files for a group of products. You have to specify the full path to the correct folder in the update settings of the product using the mirror.
For example, to update the ESET PROTECT On-Prem from the mirror, set the Update server to (according to your HTTP server root location):
`http://your_server_address/mirror/eset_upd/ep10`

The last section controls program components (PCUs). By default, downloaded program components are prepared to copy to the local mirror. If **Product updates** is activated, there is no need to click **Update**, because files are copied to the local mirror automatically when they are available. See Update mode for more information about product updates.

Troubleshooting Mirror update problems

In most cases, problems during an update from a Mirror server are caused by one or more of the following: incorrect specification of the Mirror folder options, incorrect authentication data to the Mirror folder, incorrect configuration on local workstations attempting to download update files from the Mirror, or by a combination of the reasons above. Below is an overview of the most frequent problems which may occur during an update from the Mirror:

ESET Endpoint Security reports an error connecting to Mirror server—Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates. To verify the folder, click the Windows **Start** menu, click **Run**, type the folder name and click **OK**. The contents of the folder should be displayed.

ESET Endpoint Security requires a username and password—Likely caused by incorrect authentication data (username and password) in the update section. The username and password are used to grant access to the update server, from which the program will update itself. Ensure that the authentication data is correct and entered in the correct format. For example, Domain/Username, or Workgroup/Username, plus the corresponding Passwords. If the Mirror server is accessible to “Everyone”, this does not mean that any user is granted access. “Everyone” does not mean any unauthorized user, it just means that the folder is accessible for all domain users. As a result, if the folder is accessible to “Everyone”, a domain username and password will still need to be entered in the update setup section.

ESET Endpoint Security reports an error connecting to the Mirror server—Communication on the port defined for accessing the HTTP version of the Mirror is blocked.

ESET Endpoint Security reports an error while downloading update files—Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates.

Protections

Protections guard against malicious system attacks by controlling file, email and internet communications. For example, remediation will start if an object classified as malware is detected. Protections can eliminate it by blocking it and then cleaning, deleting or moving it to quarantine.

To configure protections in detail, open Advanced setup > **Protections**.

Changes to Protections should only be made by an experienced user. Incorrect configuration of settings can lead to a decreased level of protection.

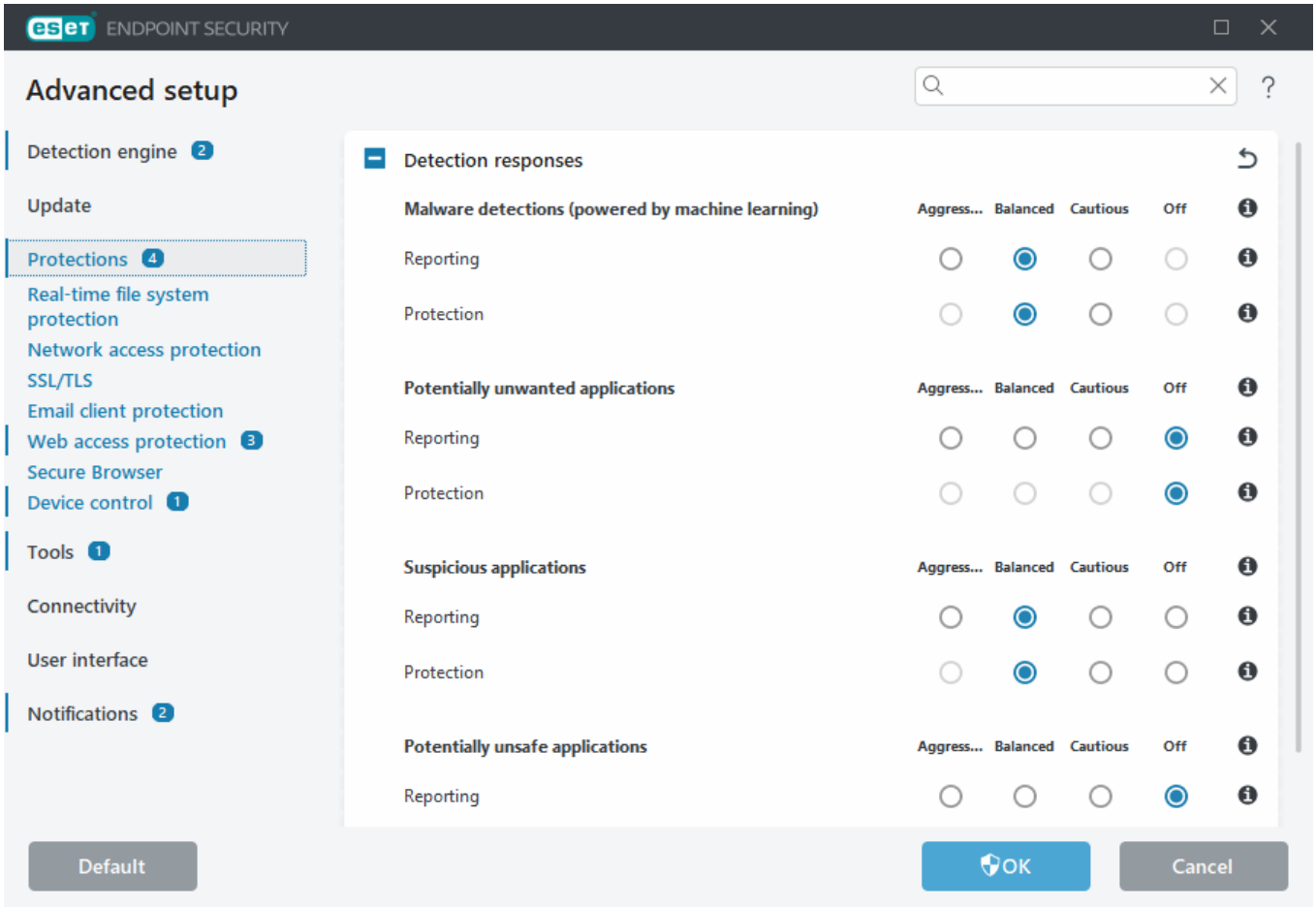
In this section:

- Detection responses
- Reporting setup
- Protection setup

Detection responses

Detection responses enable you to configure reporting and protection levels for the following categories:

- **Malware detections (powered by machine learning)**—A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term “virus” is often misused. "Malware” (malicious software) is a more accurate term. Malware detection is performed by the detection engine module combined with the machine learning component. Read more about these types of applications in the Glossary.
- **Potentially unwanted applications**—Grayware or potentially unwanted applications (PUAs) is a broad category of software, whose intent is not as unequivocally malicious as other types of malware, such as viruses or trojan horses. However, it could install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user. Read more about these types of applications in the Glossary.
- **Suspicious applications**—Includes programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.
- **Potentially unsafe applications**—Refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications (PUAs) include remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). Read more about these types of applications in the Glossary.



Improved protection

Advanced machine learning is now a part of the protections as an advanced layer of protection which improves detection based on machine learning. Read more about this type of protection in the Glossary.

Reporting setup

When a detection occurs (e.g., a threat is found and classified as malware), information is recorded to the Detections log, and Desktop notifications occur if configured in ESET Endpoint Security.

A reporting threshold is configured for each category (referred to as "CATEGORY"):

1. Malware detections
2. Potentially unwanted applications
3. Potentially unsafe
4. Suspicious applications

Reporting is performed with the detection engine, including the machine learning component. You can set a higher reporting threshold than the current protection threshold. These reporting settings do not influence blocking, cleaning or deleting objects.

Read the following before modifying a threshold (or level) for CATEGORY reporting:

Threshold	Explanation
Aggressive	CATEGORY reporting configured to maximum sensitivity. More detections are reported. The **Aggressive** setting can falsely identify objects as CATEGORY.
Balanced	CATEGORY reporting configured as balanced. This setting is optimized to balance the performance and accuracy of detection rates and the number of falsely reported objects.
Cautious	CATEGORY reporting configured to minimize falsely identified objects while maintaining a sufficient level of protection. Objects are reported only when the probability is evident and matches CATEGORY behavior.
Off	Reporting for CATEGORY is not active, and detections of this type are not found, reported or cleaned. As a result, this setting disables protection from this detection type. Off is not available for malware reporting and it is the default value for potentially unsafe applications.

Availability of ESET Endpoint Security protection modules

Availability (enabled or disabled) of a protection module for a selected CATEGORY threshold is as follows:

	Aggressive	Balanced	Cautious	Off*
Advanced machine learning module	✓ (aggressive mode)	✓ (conservative mode)	X	X
Detection engine module	✓	✓	✓	X
Other protection modules	✓	✓	✓	X

*Not recommended.

Determine product version, program module versions and build dates

1. Click **Help and support** > **About ESET Endpoint Security**.
2. In the **About** screen, the first line of text displays the version number of your ESET product.
3. Click **Installed components** to access information about specific modules.

Keynotes

Several keynotes when setting up an appropriate threshold for your environment:

- The **Balanced** threshold is recommended for most of the setups.
- The **Cautious** threshold is recommended for environments where the priority focuses on minimizing false identified objects by security software.
- The higher reporting threshold, the higher detection rate but a higher chance of falsely identified objects.
- From the real-world perspective, there is no guaranty of a 100% detection rate as well as a 0% chance to avoid incorrect categorization of clean objects as malware.
- Keep ESET Endpoint Security and its modules up-to-date to maximize the balance between performance and accuracy of detection rates and the number of falsely reported objects.

Protection setup

If an object classified as CATEGORY is reported, the program blocks the object and then cleans, deletes or moves it to Quarantine.

Read the following before modifying a threshold (or level) for CATEGORY protection:

Threshold	Explanation
Aggressive	Reported aggressive (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started. This setting is recommended when all endpoints have been scanned with aggressive settings and falsely reported objects have been added to detection exclusions.
Balanced	Reported balanced (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Cautious	Reported cautious level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Off	Useful to identify and exclude falsely reported objects. Off is not available for malware protection and it is the default value for potentially unsafe applications.

Best practices

UNMANAGED (Individual client workstation)

Keep the default recommended values as is.

MANAGED ENVIRONMENT

These settings are usually applied to workstations via a policy.

1. Initial phase

This phase might take up to a week.

- Set up all **Reporting** thresholds to **Balanced**.
  NOTE: If needed, set up to **Aggressive**.
- Set up or keep **Protection** for malware as **Balanced**.
- Set up **Protection** for other CATEGORIES to **Cautious**.
  NOTE: It is not recommended to set up the **Protection** threshold to **Aggressive** in this phase because all found detections would be remediated, including the falsely identified ones.
- Identify falsely identified objects from Detections log and add them to Detection exclusions first.

2. Transition phase

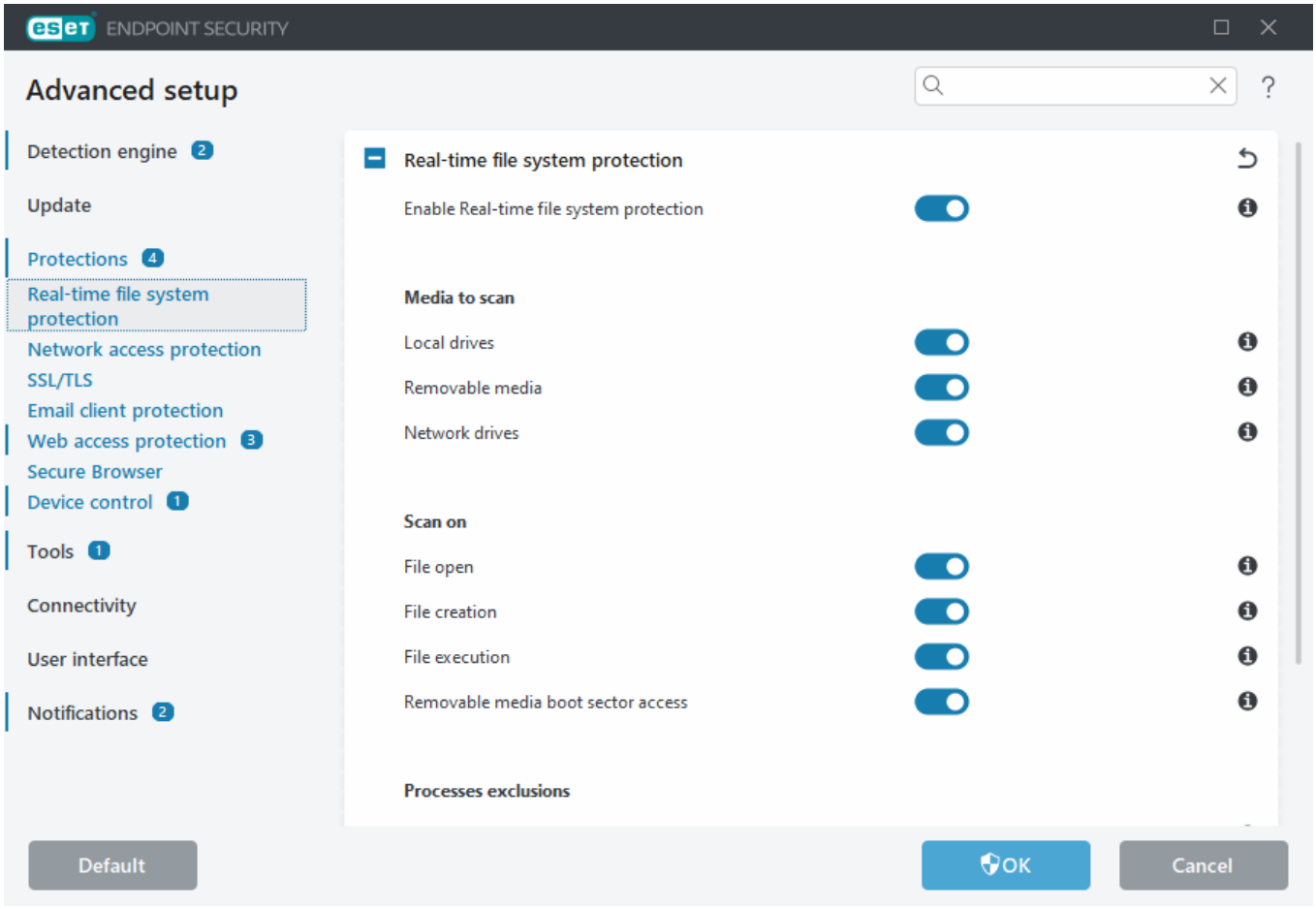
- Implement the "Production phase" to some of the workstations as a test (not for all workstations on the network).

3. Production phase

- Set up all **Protection** thresholds to **Balanced**.
- When managed remotely, use an appropriate antivirus pre-defined policy for ESET Endpoint Security.
- **Aggressive** protection threshold can be set if the highest detection rates are required and falsely identified objects are accepted.
- Check Detection log or ESET PROTECT On-Prem reports for possible missing detections.

Real-time file system protection

Real-time file system protection controls all files in the system for malicious code when opened, created, or run.



By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. We do not recommend disabling **Enable Real-time file system protection** in Advanced setup > **Protections** > **Real-time file system protection** > **Real-time file system protection**.

Media to scan

By default, all types of media are scanned for potential threats:

- **Local drives**—Scans all system and fixed hard drives (example: *C:*\, *D:*\).
- **Removable media**—Scans CD/DVDs, USB storage, memory cards, etc.
- **Network drives**—Scans all mapped network drives (example: *H:*\ as *store04*) or direct access network drives (example: *store08*).

We recommend that you use default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

Scan on

By default, all files are scanned when opened, created, or executed. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:

- **File open**—Scans when a file is opened.
- **File creation**—Scans a created or modified file.
- **File execution**—Scans when a file is executed or run.
- **Removable media boot sector access**—When removable media that contains a boot sector is inserted into the device, the boot sector is immediately scanned. This option does not enable removable media file scanning. Removable media file scanning is located **Media to scan** > **Removable media**. For **Removable media boot sector access** to work correctly, keep **Boot sectors/UEFI** enabled in ThreatSense.

Processes exclusions

See Processes exclusions.

ThreatSense

Real-time file system protection checks all types of media and is triggered by various system events, such as accessing a file. Using **ThreatSense** technology detection methods (as described in ThreatSense), Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to monitor newly created files more closely.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each detection engine update. This behavior is controlled using **Smart optimization**. If this **Smart optimization** is disabled, all files are scanned each time they are accessed. To modify this setting, open Advanced setup > **Protections** > **Real-time file system protection**. Click **ThreatSense** > **Other** and select or deselect **Enable Smart optimization**.

Real-time file system protection also enables you to configure Additional ThreatSense parameters.

Processes exclusions

The Processes exclusions feature enables you to exclude application processes from Real-time file system protection. To improve backup speed, process integrity and service availability, some techniques that are known to conflict with file-level malware protection are used during backup. The only effective way to avoid both situations is to deactivate Anti-Malware software. By excluding specific process (for example those of the backup solution) all file operations attributed to such excluded process are ignored and considered safe, thus minimizing interference with the backup process. We recommend that you use caution when creating exclusions – a backup tool that has been excluded can access infected files without triggering an alert which is why extended permissions are only allowed in the real-time protection module.

> Not to be confused with Excluded file extensions, HIPS exclusions, Detection exclusions or Performance exclusions.

Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (*.exe*).

You can add executable files into the list of excluded processes in Advanced setup > **Protections** > **Real-time file system protection** > **Real-time file system protection** > **Processes exclusions**.

This feature was designed to exclude backup tools. Excluding the backup tool's process from scanning not only

ensures system stability, but it also does not affect backup performance as the backup is not slowed down while it is running.

Click **Edit** to open the **Processes exclusions** management window, where you can add exclusions and browse for executable file (for example *Backup-tool.exe*), which will be excluded from scanning.
As soon as the *.exe* file is added to the exclusions, activity of this process is not monitored by ESET Endpoint Security and no scanning is run on any file operations performed by this process.

If you do not use browse function when selecting process executable, you need to manually type a full path to the executable. Otherwise, the exclusion will not work correctly and HIPS may report errors.

You can also **Edit** existing processes or **Delete** them from exclusions.

Web access protection does not take into account this exclusion, so if you exclude the executable file of your web browser, downloaded files are still scanned. This way an infiltration can still be detected. This scenario is an example only, and we do not recommend that you create exclusions for web browsers.

Add or Edit processes exclusions

This dialog window enables you to **add** processes excluded from detection engine. Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (*.exe*).

Select the file path of an excepted application by clicking ... (for example *C:\Program Files\Firefox\Firefox.exe*). Do NOT type the name of the application.
As soon as the *.exe* file is added to the exclusions, activity of this process is not monitored by ESET Endpoint Security and no scanning is run on any file operations performed by this process.

If you do not use browse function when selecting process executable, you need to manually type a full path to the executable. Otherwise, the exclusion will not work correctly and HIPS may report errors.

You can also **Edit** existing processes or **Delete** them from exclusions.

When to modify real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Always be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases.

After installing ESET Endpoint Security, all settings are optimized to provide the maximum level of system security for users. To restore default settings, click ↩ next to Advanced setup > **Protections** > **Detection responses**.

Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs.

The file is available for download at http://www.eicar.org/download/eicar.com

After you type this URL into your browser, you should see a message that the threat has been removed.

What to do if real-time protection does not work

This topic describes problems that may arise when using real-time protection and how to troubleshoot them.

Real-time protection is disabled

If a user inadvertently disables real-time protection, you should reactivate the feature. To reactivate real-time protection, go to **Setup** in the main program window and click **Computer** > **Real-time file system protection**.

If real-time protection is not initiated at system startup, it is usually because **Enable Real-time file system protection** is disabled. To ensure that this option is enabled, open Advanced setup > **Protections** > **Real-time file system protection**.

If real-time protection does not detect and clean infiltrations

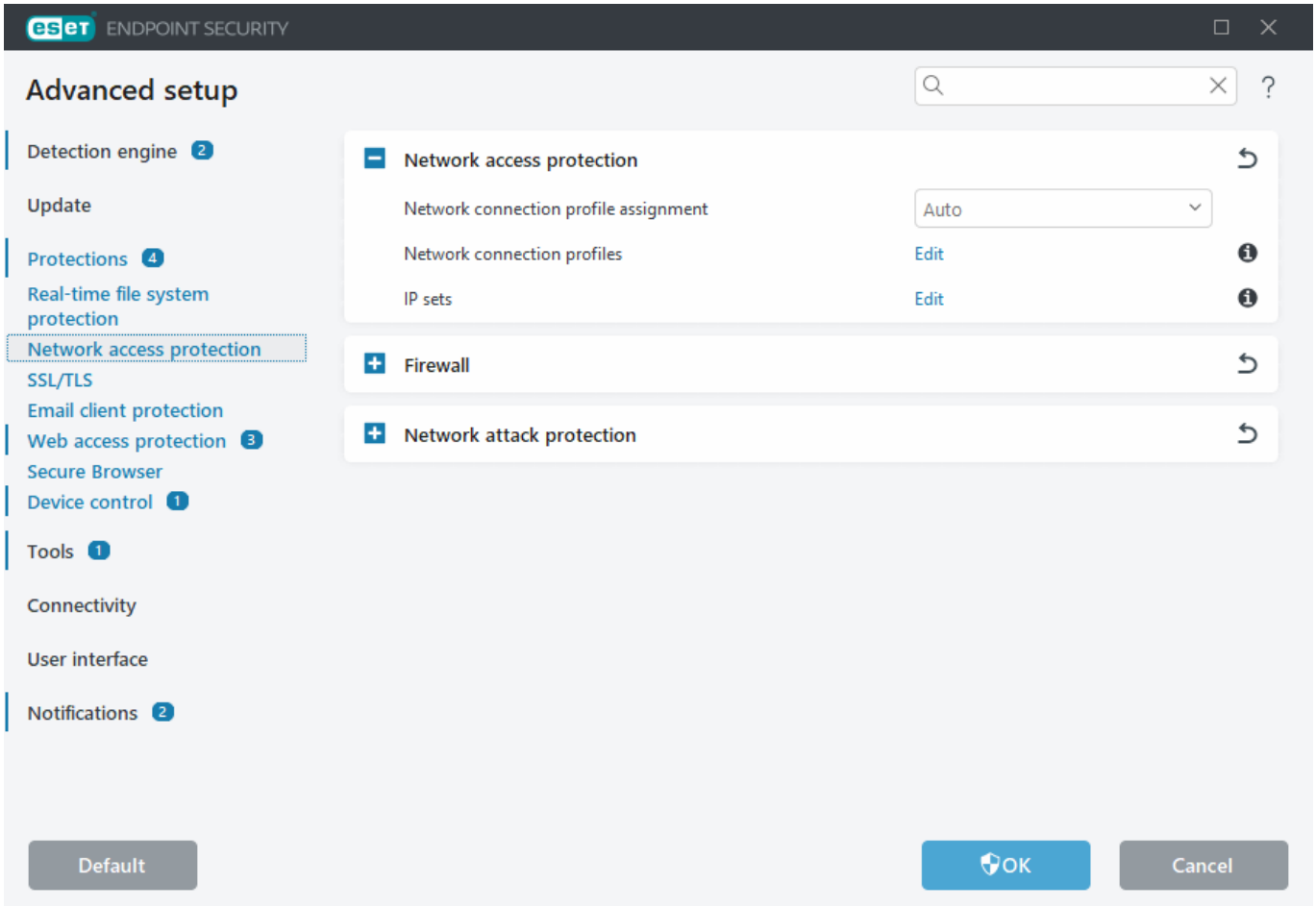
Verify that no other antivirus programs are installed on your computer. If two antivirus programs are installed at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system before installing ESET.

Real-time protection does not start

If real-time protection is not initiated at system startup (and **Enable Real-time file system protection** is enabled), it may be due to conflicts with other programs. To resolve the issue, create an ESET SysInspector log and submit it to ESET Technical Support for analysis.

Network access protection

Network access protection enables you to configure all your network connections. You can allow/deny access to your computer on specific networks, allow/deny access to network devices from your computer and more based on the configuration. By default, ESET Endpoint Security has pre-configured firewall rules and network access protection for maximum security. However, specific environments may need custom configuration. Changing the default settings should only be done by an experienced user.



You can configure the following settings in Advanced setup > **Protections** > **Network access protection** (click the links below for a detailed description of each Network access protection option):

Network access protection

Network connection profiles—Profiles can be used to control the Network access protection and Firewall for specific network connections.

IP sets—You can define IP address collections that create one logical IP address group, which you can use for Firewall and Brute-force attack protection rules.

Firewall

Network attack protection

Network connection profiles

Profiles can be used to control the behavior of the ESET Endpoint Security Network access protection for specific Network connection. When creating or editing Firewall rules, IDS rules or Brute-force attack protection rules , you can assign it to a specific profile or apply it to all profiles. When a profile is active on a network connection, only the global rules (rules with no profile specified) and the rules that have been assigned to that profile are applied to it. You can create multiple profiles with different rules assigned to network connections to alter Firewall behavior easily.

You can configure Network connection profiles and assignments in Advanced setup > **Protections** > **Network**

access protection > **Network access protection**.

Network connection profile assignment—Enables you to choose if newly discovered network connections are automatically (select **Auto** from the drop-down menu) assigned a pre-defined or custom profile based on Activators configured in network connection profiles or if you want to be asked (select **Ask** from the drop-down menu) to Configure network protection and assign a profile manually every time a new network connection is detected.

You can also manually assign a specific network connection profile in the main program window > **Setup** > **Network** > **Network connections**. Hover over a specific network connection and click the menu icon > **Edit** to open the Configure network protection window and select a profile.

Network connection profiles—Click **Edit** to Add or edit Network connection profiles.

The following profiles are pre-defined and cannot be edited/deleted:

Private—For trusted networks (home or office network). Your computer and shared files stored on your computer are visible to other network users, and system resources are accessible to other users on the network (access to shared files and printers is enabled, incoming RPC communication is enabled and remote desktop sharing is available). We recommend using this setting when accessing a secure local network. This profile is automatically assigned to a network connection if it is configured as Domain or Private network in Windows.

Public—For untrusted networks (public network). Files and folders on your system are not shared with or visible to other users on the network, and system resource sharing is deactivated. We recommend using this setting when accessing wireless networks. This profile is automatically assigned to any network connection that is not configured as Domain or Private network in Windows.

When the network connection switches to another profile, a notification will appear in the bottom right corner of your screen.

Add or edit Network connection profiles

You can add or edit Network connection profiles in Advanced setup > **Protections** > **Network access protection** > **Network access protection** > **Network connection profiles** > **Edit**. To Edit a profile, it must be selected from the list of **Network connection profiles** window.

The following profiles are pre-defined and cannot be edited/deleted:

Private—For trusted networks (home or office network). Your computer and shared files stored on your computer are visible to other network users, and system resources are accessible to other users on the network (access to shared files and printers is enabled, incoming RPC communication is enabled and remote desktop sharing is available). We recommend using this setting when accessing a secure local network. This profile is automatically assigned to a network connection if it is configured as Domain or Private network in Windows.

Public—For untrusted networks (public network). Files and folders on your system are not shared with or visible to other users on the network, and system resource sharing is deactivated. We recommend using this setting when accessing wireless networks. This profile is automatically assigned to any network connection that is not configured as Domain or Private network in Windows.

Top/Up/Down/Bottom —Enables you to adjust the priority level of network connection profiles (Network connection profiles are evaluated and applied by their priority. The first matching profile is

always applied).

Add or Edit a profile

Custom network connection profile enables you to apply Firewall rules, Brute-force attack protection rules and define additional settings for specific network connections. You will specify to which network connections the custom profile will be assigned in the Activators section.

To open the profile editor, in the **Network connection profiles** window:

- Click **Add**.
- Select one of the existing profiles and click **Edit**.
- Select one of the existing profiles and click **Copy**.

Name—Custom name for your profile.

Description—Description of the profile to help identify the profile.

Additional trusted addresses—Addresses defined here are added to the trusted zone of the network connection to which this profile is applied (regardless of the network's protection type).

Trusted connection—Your computer and shared files stored on your computer are visible to other network users, and system resources are accessible to other users on the network (access to shared files and printers is enabled, incoming RPC communication is enabled and remote desktop sharing is available). We recommend using this setting when creating a profile for a secure local network connection. All directly connected network subnets are also considered trusted. For example, if a network adapter is connected to this network with the IP address 192.168.1.5 and the subnet mask is 255.255.255.0, the subnet 192.168.1.0/24 is added to that network connection trusted zone. If the adapter has more addresses/subnets, all of them will be trusted.

Report weak WiFi encryption—ESET Endpoint Security will display a desktop notification when you connect to an unprotected wireless network or network with weak protection.

Activators—Custom conditions that must be met to assign this network connection profile to a network connection. See Activators for detailed explanation.

Activators

Activators are custom conditions that must be met to assign a Network connection profile to a Network connection. If the connected network has the same attributes as defined in activators for a connected network profile, the profile will be applied to the network. A network connection profile can have one or multiple activators. If there are multiple activators, the OR logic applies (at least one condition must be met). You can define activators in the Network connection profile editor. Creating custom network connection profiles should be done by an experienced user.

The following Activators are available (If you want to know details for the network you are currently connected to, see Network connections):

Adapter

Adapter type—Apply profile if the network connection is established on the selected adapter type.
Adapter name—Apply profile if the network adapter name matches.
Adapter IP—Apply profile if the IP address of your network adapter matches.

DNS

DNS suffix—Apply profile if the domain name matches.
DNS IP—Apply the profile if the DNS server IP address matches.

WINS

Apply the profile if the Windows Internet Name Service (WINS) mapped IP address matches.

DHCP

DHCP IP—Match the DHCP server IP address.

Default gateway

IP—Apply profile if the Default gateway IP address matches.
MAC address—Apply profile if the Default gateway MAC address matches.

Wi-Fi

SSID—Apply profile if the SSID (name of the Wi-Fi) matches.
Profile name—Apply profile if the Wi-Fi profile name matches.
Security type—Apply profile if the security type matches the one selected from the drop-down menu. If you want to match more than one, create another activator.
Encryption type—Apply profile if the encryption type matches the one selected from the drop-down menu. If you want to match more than one, create another activator.
Network security—Apply profile if the network is **Open**/**Secured**.

Windows profile

Apply profile if the network is configured in Windows as **Domain**/**Private**/**Public**.

Authentication

Network authentication searches for a specific server in the network and uses asymmetric encryption (RSA) to authenticate that server. The network's name being authenticated must match the name set in the authentication server settings. The name is case-sensitive. The server name can be typed as an IP address, DNS or NetBios name.
Download the ESET Authentication Server.
The public key can be imported using any of the following file types:
• PEM encrypted public key (.pem); you can generate this key using the ESET Authentication Server
• Encrypted public key
• Public key certificate (.crt)
Click **Test** to test your settings. If authentication is successful, Server authentication was successful is displayed. If authentication is not configured properly, one of the following error messages will display:
Server authentication failed. Invalid or mismatched signature.
Server signature does not match the public key entered.
Server authentication failed. Network name doesn't match.
The configured network name does not correspond with the authentication server network name. Review both names and ensure they are identical.
Server authentication failed. Invalid or no response from server.
No response is received if the server is not running or is inaccessible. An invalid response may be received if another HTTP server is running on the specified address.
Invalid public key entered.
Verify that the public key file you have entered is not corrupted.

IP sets

An IP set is a collection of IP addresses that create one logical group of IP addresses, useful when reusing the same set of addresses in multiple Firewall rules or Brute-force attack protection rules. ESET Endpoint Security also contains pre-defined IP sets for which internal rules are applied. One example of such a group is a **Trusted zone**. Trusted zone represents a group of network addresses where your computer and shared files stored on your computer are visible to other network users, and system resources are accessible to other users on the network.

To add an IP set:

1. Open Advanced setup > **Protections** > **Network access protection** > **IP sets** > **Edit**.
2. Click **Add**, type in a **Name** and **Description** for the zone, and type a remote IP address in **Remote computer address (IPv4/IPv6, range, mask)**.
3. Click **OK**.

For more information, see Edit IP sets.

Edit IP sets

For more information about IP sets, see IP sets.

Columns

Name—Name of a group of remote computers.

Description—A general description of the group.

IP addresses—Remote IP addresses that belong to an IP set.

Control elements

When you **add** or **edit** an IP set, the following fields are available:

Name—Name of a group of remote computers.

Description—A general description of the group.

Remote computer address (IPv4, IPv6, range, mask)—Enables you to add a remote address, address range, or subnet.

Delete—Removes a zone from the list.

Pre-defined IP sets cannot be removed.

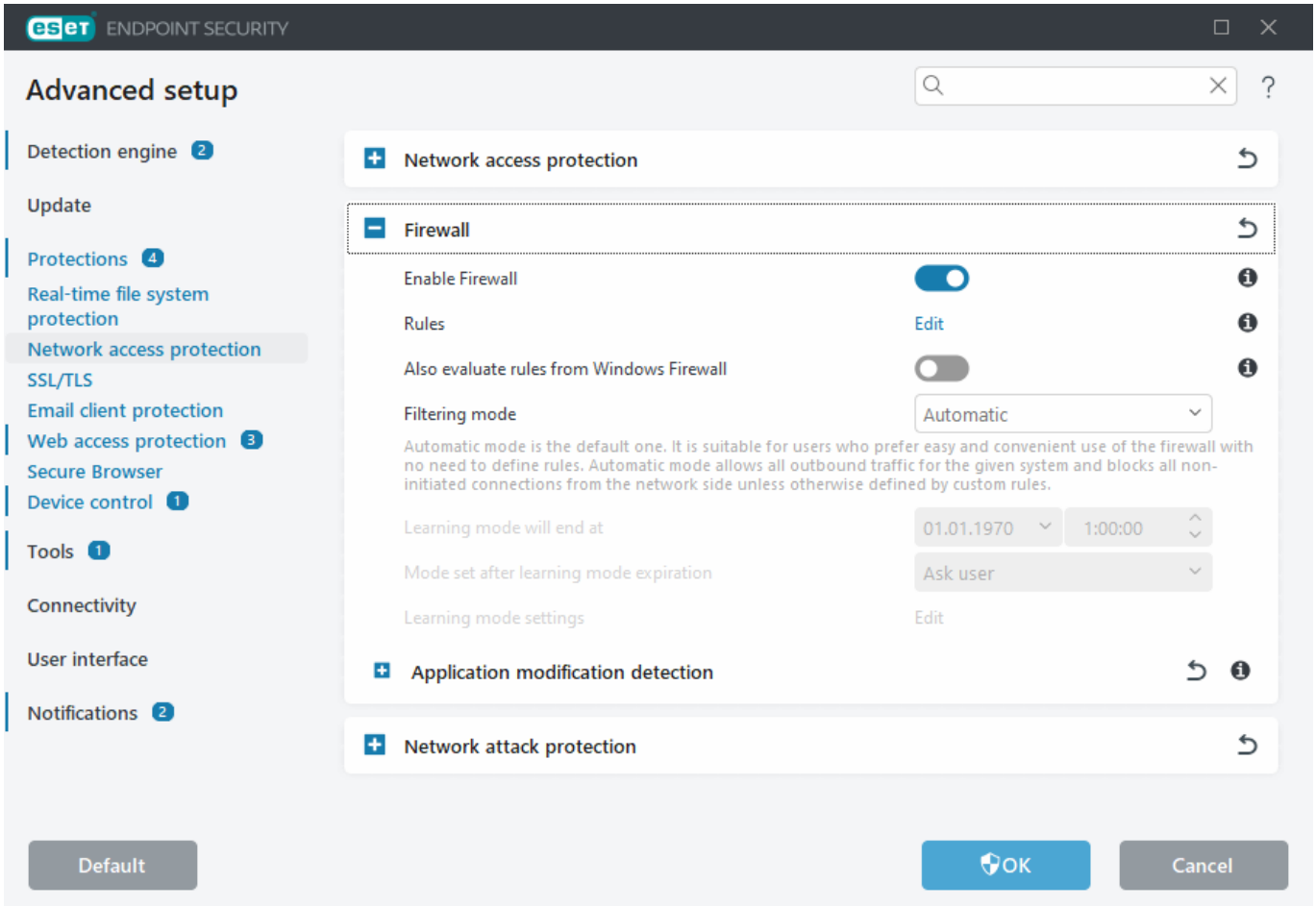
IP addresses examples

Add IPv4 address:
Single address—Adds an IP address of an individual computer (for example, *192.168.0.10*).
Address range—Type the starting and ending IP addresses to specify the IP range of several computers (for example, *192.168.0.1-192.168.0.99*).
Subnet—Subnet (a group of computers) defined by an IP address and mask. For example, 255.255.255.0 is the network mask for the 192.168.1.0 subnet. To exclude the whole subnet type in *192.168.1.0/24*.
Add IPv6 address:
Single address—Adds the IP address of an individual computer (for example, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Subnet—Subnet (a group of computers) is defined by an IP address and mask (for example, *2002:c0a8:6301:1::1/64*).

Firewall

Firewall controls all inbound and outbound network traffic on your computer based on internal rules and rules defined by you. This is accomplished by allowing or denying individual network connections. Firewall provides protection against attacks from remote devices and can block potentially threatening services.

To configure the Firewall, open Advanced setup > **Protections** > **Network access protection** > **Firewall**.



Firewall

Enable Firewall

We recommend that you leave this feature enabled to ensure the security of your system. With Firewall enabled, network traffic is scanned in both directions.

Rules

Rules setup enables you to view and edit all Firewall rules applied to traffic generated by individual applications within trusted connections and the internet.

Rules from Windows firewall configured using Group Policy (GPO) are not evaluated.

You can create an IDS rule when a Botnet attacks your computer. A rule can be modified in Advanced setup > **Protections** > **Network access protection** > **Network attack protection** > **IDS rules** by clicking **Edit**.

Also evaluate rules from Windows Firewall

In automatic filtering mode, incoming traffic allowed by rules from Windows Firewall is evaluated and processed, unless explicitly blocked by ESET rules.

Filtering mode

The behavior of the firewall changes based on the filtering mode. Filtering modes also influence the level of user interaction required.

The following filtering modes are available for the ESET Endpoint Security Firewall:

Filtering mode	Description
Automatic mode	The default mode. This mode is suitable for users who prefer easy and convenient use of the firewall without the need to define rules. Custom, user-defined rules can be created but are not required in **Automatic mode**. Automatic mode allows all outbound traffic for a given system and blocks most inbound traffic with the exception of some traffic from the Trusted Zone (as specified in IDS and advanced options/Allowed services) and responses to recent outbound communications.
Interactive mode	Enables you to build a custom configuration for your Firewall. When a communication is detected and no existing rules apply to that communication, a dialog window reporting an unknown connection will be displayed. The dialog window gives the option to allow or deny the communication, and the decision to allow or deny can be saved as a new rule for the Firewall. If you choose to create a new rule, all future connections of this type will be allowed or blocked according to that rule.
Policy-based mode	Blocks all connections that are not defined by a specific rule that allows them. This mode enables advanced users to define rules that permit only desired and secure connections. All other unspecified connections will be blocked by the Firewall.
Learning mode	Automatically creates and saves rules; this mode is best used for the initial configuration of the Firewall, but should not be left on for prolonged periods of time. No user interaction is required because ESET Endpoint Security saves rules according to pre-defined parameters. Learning mode should only be used until all rules for required communications have been created to avoid security risks.

Learning mode will end at—Set date and time when the learning mode ends automatically. You can also turn off the learning mode manually whenever you want.

Mode set after learning mode expiration—Define which filtering mode the Firewall will revert to after the time period for learning mode ends. Read more about filtering modes in the table above. When finished, the **Ask user** option requires administrative privileges to perform a change to the Firewall filtering mode.

Learning mode settings—Click **Edit** to configure parameters for saving rules created in Learning mode.

Application modification detection

The application modification detection feature displays notifications if modified applications, for which a Firewall rule exists, attempt to establish connections.

Learning mode settings

Learning mode automatically creates and saves a rule for each communication that has been established in the system. No user interaction is required because ESET Endpoint Security saves rules according to the pre-defined parameters.

This mode can expose your system to risk and is only recommended for initial configuration of the Firewall.

Select **Learning** from the drop-down menu in Advanced setup > **Protections** > **Network access protection** > **Firewall** > **Firewall** > **Filtering mode** to activate Learning mode options. Click **Edit** next to **Learning mode settings** to configure the following options:

While in Learning mode, the Firewall does not filter communication. All outgoing and incoming communications are allowed. In this mode, your computer is not fully protected by the Firewall.

Inbound traffic from the Trusted zone—An example of an incoming connection within the trusted zone would be a remote device from within the trusted zone attempting to establish communication with a local application running on your computer.

Outbound traffic to the Trusted zone—A local application attempting to establish a connection to another device within the local network or within a network in the trusted zone.

Inbound Internet traffic—A remote device attempting to communicate with an application running on the computer.

Outbound Internet traffic—A local application attempting to establish a connection to another device.

Each section enables you to define parameters to be added to newly created rules:

Add local port—Includes the local port number of the network communication. For outgoing communications, random numbers are usually generated. For this reason, we recommend enabling this option only for incoming communications.

Add application—Includes the name of the local application. This option is suitable for future application-level rules (rules that define communication for an entire application). For example, you can enable communication only for a web browser or email client.

Add remote port—Includes the remote port number of the network communication. For example, you can allow or deny a specific service associated with a standard port number (HTTP – 80, POP3 – 110, etc.).

Add remote IP address/Trusted zone—A remote IP address or zone can be used as a parameter for new rules defining all network connections between the local system and that remote address/zone. This option is suitable if you want to define actions for a certain device or a group of networked devices.

Maximum number of different rules for an application—If an application communicates through different ports to various IP addresses, etc., the Firewall in learning mode creates an appropriate count of rules for this application. This option enables you to limit the number of rules that can be created for one application.

Dialog window - End learning mode

When the usage period for Learning mode has elapsed, you will be prompted to switch to **Interactive** or **Policy-based** filtering mode. When the firewall is in Learning mode, new rules are created without user's interaction.

See Filtering modes to find out more information about each filtering mode.

We recommend that you review the rules created in learning mode by clicking **Open rule editor**.

Firewall rules

Firewall Rules represent a set of conditions used to meaningfully test all network connections and all actions assigned to these conditions. Using Firewall rules, you can define the action that is taken when different types of

network connections are established.

Rules are evaluated from top to bottom and you can see their priority in the first column. The action of the first matching rule is used for each network connection being evaluated.

Connections can be divided into incoming and outgoing connections. Incoming connections are initiated by a remote device attempting to establish a connection with the local system. Outgoing connections work in the opposite way – the local system contacts a remote device.

If a new unknown communication is detected, you must carefully consider whether to allow or deny it. Unsolicited, unsecured or unknown connections pose a security risk to the system. If such a connection is established, we recommend that you pay attention to the remote device and the application attempting to connect to your computer. Many infiltrations try to obtain and send private data or download other malicious applications to host workstations. The Firewall enables you to detect and terminate such connections.

You can view and edit Firewall rules in Advanced setup > **Protections** > **Network access protection** > **Firewall** > **Rules** > **Edit**.

If you have many Firewall rules, you can use a filter to show only specific rules. To filter Firewall rules, click **More filters** above the Firewall rules list. You can filter the rules based on the following criteria:

- Origin
- Direction
- Action
- Availability

By default, the pre-defined Firewall rules are hidden. To display all pre-defined rules, disable the toggle next to **Hide built-in (pre-defined) rules**. You can disable these rules, but you cannot delete a pre-defined rule.

Click the search icon at the top right to search for rule(s).

Columns

Priority—Rules are evaluated from top to bottom and you can see their priority in the first column.

Enabled—Shows if a rule is enabled or disabled; the corresponding check box must be selected to enable a rule.

Application—The application to which the rule applies.

Direction—Direction of communication (incoming/outgoing/both).

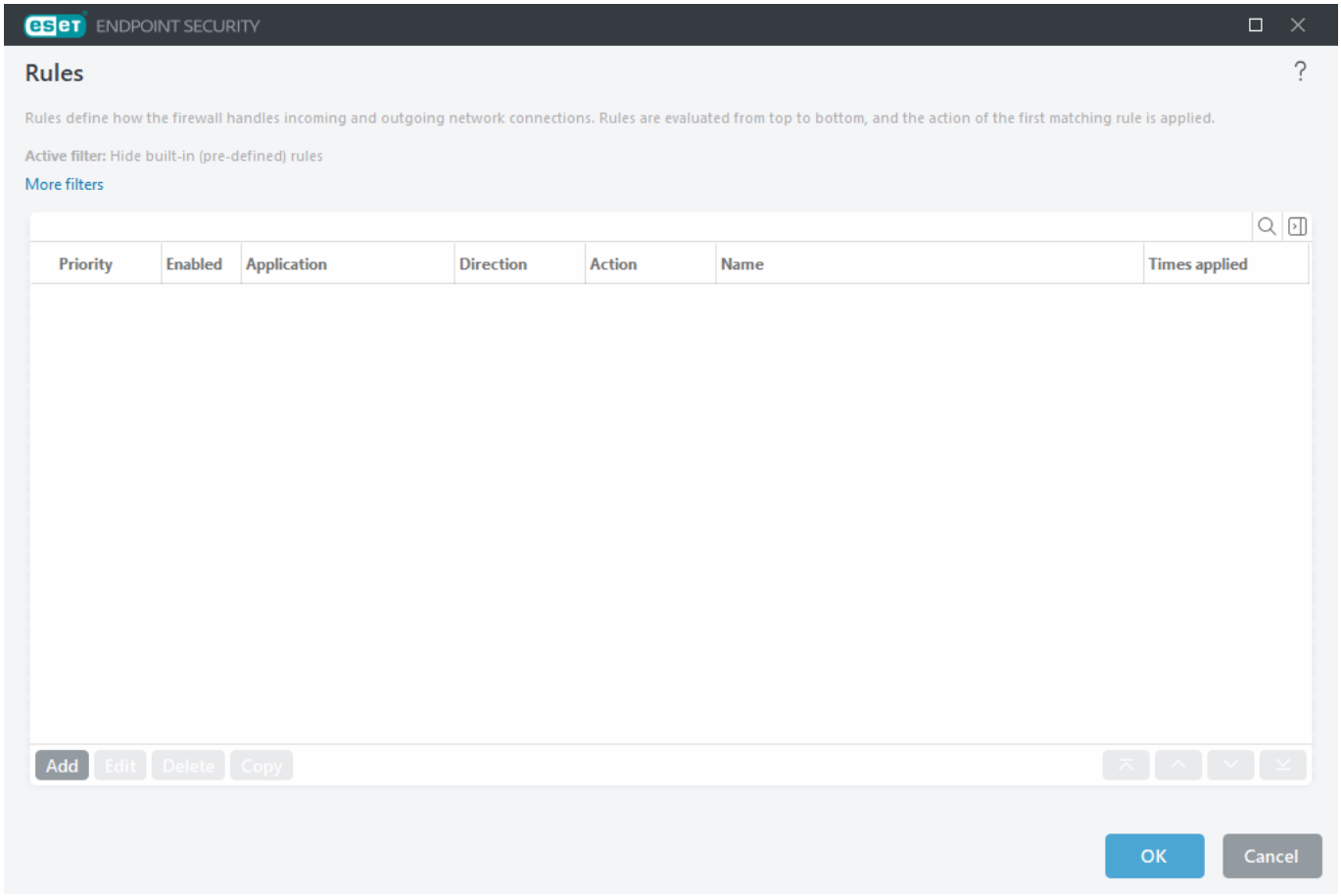
Action—Shows the status of communication (block/allow/ask).

Name—Name of the rule. The ESET Icon represents a pre-defined rule.

Times applied—Total number of times the rule has been applied.

Click the expand icon to display the rule details.

You can choose which columns are displayed by right-clicking on the table header.



Control elements

Add—Create a new rule.

Edit—Edit an existing rule.

Delete—Remove an existing rule.

Copy—Create a copy of a selected rule.

Top/Up/Down/Bottom—Enables you to adjust the priority level of rules (rules are executed from top to bottom).

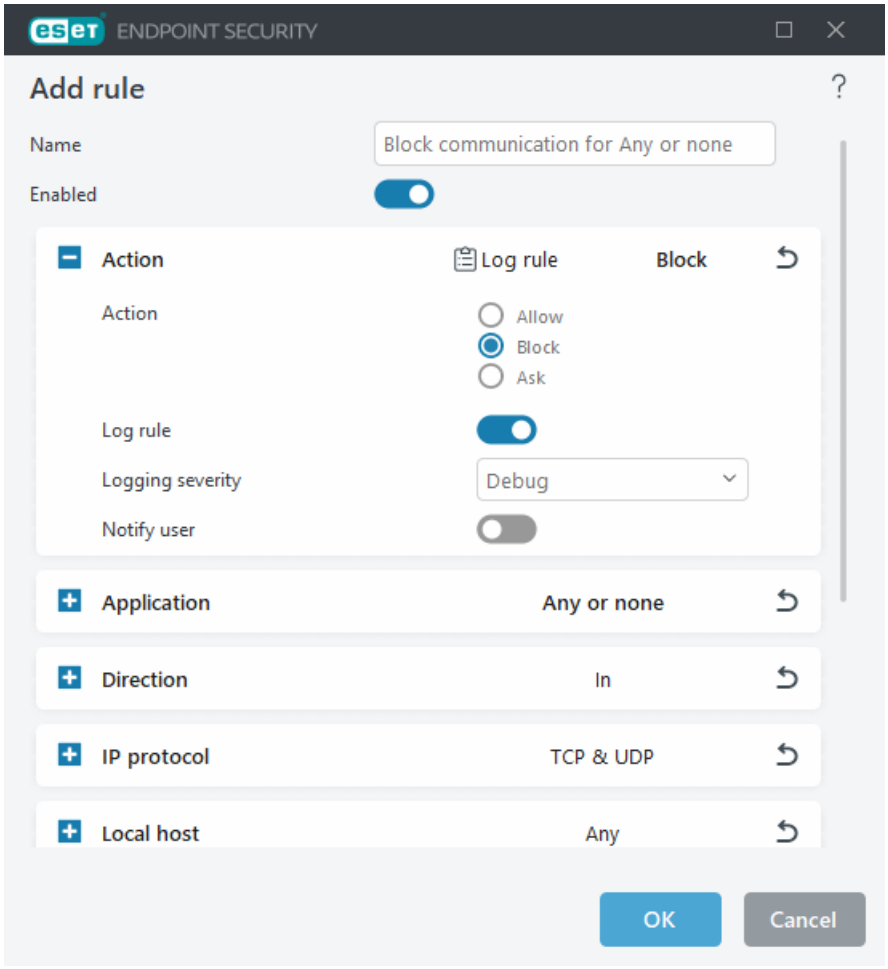
Adding or editing Firewall rules

Firewall Rules represent conditions used to meaningfully test all network connections and actions assigned to these conditions. Editing or adding Firewall rules may be required when the network settings change (for example, the network address or port number for the remote side changes) to ensure the correct operation of an application affected by a rule. An experienced user should create custom Firewall rules.

The following ESET Knowledgebase articles may only be available in English:
- Create or edit firewall rules in ESET Endpoint Security
- Create or edit firewall rules for client workstations in ESET PROTECT On-Prem

To add or edit a Firewall rule, open Advanced setup > **Protections** > **Network access protection** > **Firewall** > **Rules**

> **Edit**. In the Firewall rules window, click **Add** or **Edit**.



Name—Type a name for the rule.

Enabled—Enable the toggle to make the rule active.

Add actions and conditions for the Firewall rule:

Action

Action—Select if you want to **Allow**/**Block** the communication which matches the conditions defined in this rule or if you want ESET Endpoint Security to **Ask** every time the communication establishes.
Log rule—If the rule is applied, it will be recorded in Log files.
Logging severity—Select the severity of the log record for this rule.
Notify user—Displays a notification when the rule is applied.

Application

Specify an application for which this rule will be applied.
Application path—Click **...** and navigate to an application or enter the full path to the application (for example C:\Program Files\Firefox\Firefox.exe). Do NOT enter the name of the application alone.
Application signature—You can apply the rule to applications based on their signatures (publisher name). Select from the drop-down menu if you want to apply the rule to applications with **Any valid signature** or to applications **Signed by a specific signer**. If you select applications **Signed by a specific signer**, you need to define the signer in the **Name of signer** field.
Microsoft Store application—Select an application installed from Microsoft Store from the drop-down menu.
Service—You can select a system service instead of application. Open the drop-down menu to select a service.
Apply to child processes—Some applications may run more processes while you see only one application window. Enable this toggle to ensure that the rule will apply to every process for the specified application.

Direction

Select the **Direction** of communication to which this rule will apply:
- **Both**—Inbound and outbound communication.
- **In**—Inbound communication only.
- **Out**—Outbound communication only.

IP protocol

Select a **Protocol** from the drop-down menu if you want this rule to apply only to a specific protocol.

Local host

Local addresses, address range or subnet for which this rule is applied. If there is no address specified, the rule will apply to the whole communication with local hosts. You can add IP addresses, address ranges or subnets directly into the **IP** text field or select from already existing IP sets by clicking **Edit** next to **IP sets**.

Local port

Local **Port** number(s). If there are no numbers supplied, the rule will apply to any port. You can add a single communication port or a range of communication ports.

Remote host

Remote address, address range or subnet for which this rule is applied. If there is no address specified, the rule will apply to the whole communication with remote hosts. You can add IP addresses, address ranges or subnets directly into the **IP** text field or select from already existing IP sets by clicking **Edit** next to **IP sets**.

Remote port

Remote **Port** number(s). If there are no numbers supplied, the rule will apply to any port. You can add a single communication port or a range of communication ports.

Profile

A Firewall rule can be applied to specific Network connection profiles.
Any—The rule will be applied to any network connection despite the used profile.
Selected—The rule will be applied to a specific network connection based on the selected profile. Select the check box next to the profiles you want to select.

In this example, we create a new rule to allow the Firefox web browser application to access the internet / local network websites:
1. In the **Action** section, select **Action** > **Allow**.
2. In the **Application** section, specify the **Application path** of the web browser (for example C:\Program Files\Firefox\Firefox.exe). Do NOT enter the name of the application alone.
3. In the **Direction** section, select **Direction** > **Out**.
4. In the **IP protocol** section, select **TCP & UDP** from the **Protocol** drop-down menu.
5. In the **Remote port** section, add **Port** numbers: *80,443* to allow standard browsing.

Pre-defined rules can be modified in a limited way.

Application modification detection

The application modification detection feature displays notifications if modified applications, for which a firewall rule exists, attempt to establish connections. Application modification is a mechanism of temporarily or permanently replacing an original application by another application by a different executable (protects against abusing firewall rules).

This feature is not meant to detect modifications to any application in general. The goal is to avoid abusing existing firewall rules, and only applications for which specific firewall rules exist are monitored.

To edit **Application modification detection**, open Advanced setup > **Protections** > **Network access protection** > **Firewall** > **Application modification detection**.

Enable detection of application modifications—If selected, the program will monitor applications for changes (updates, infections, other modifications). When a modified application attempts to establish a connection, you will be notified by the Firewall.

Allow modification of signed (trusted) applications—Do not notify if the application has the same valid digital signature before and after the modification.

List of applications excluded from detection—Add or remove individual applications for which modifications are allowed without notification.

List of applications excluded from detection

The firewall in ESET Endpoint Security detects changes to applications for which rules exist (see Application modification detection).

In certain cases you may not want to use this functionality for some applications if you want to exclude them from checking by the firewall.

Add—Opens a window where you can select an application to add to the list of applications excluded from modification detection. You can choose from a list of running applications with open network communication, for which firewall rule exists or add a specific application.

Edit—Opens a window where you can change the location of an application that is on the list of applications excluded from modification detection. You can choose from a list of running applications with open network communication, for which firewall rule exists or change the location manually.

Delete—Removes entries from the list of applications excluded from modification detection.

Network attack protection (IDS)

Network attack protection (IDS) improves the detection of exploits for known vulnerabilities. Read more about Network attack protection in the Glossary. To configure Network attack protection, open Advanced setup > **Protections** > **Network access protection** > **Network attack protection**.

Enable Network attack protection (IDS)—Analyses network traffic content and protects from network attacks. Any traffic considered harmful will be blocked.

Enable Botnet protection—Detects and blocks communication with malicious command and control servers based on typical patterns when the computer is infected and a bot is attempting to communicate. Read more about Botnet protection in the Glossary.

IDS rules—This option enables you to configure advanced filtering options to detect several attack and exploit types that might be used to harm your computer.

All important events detected by network protection are saved in a log file. See network protection log for more information.

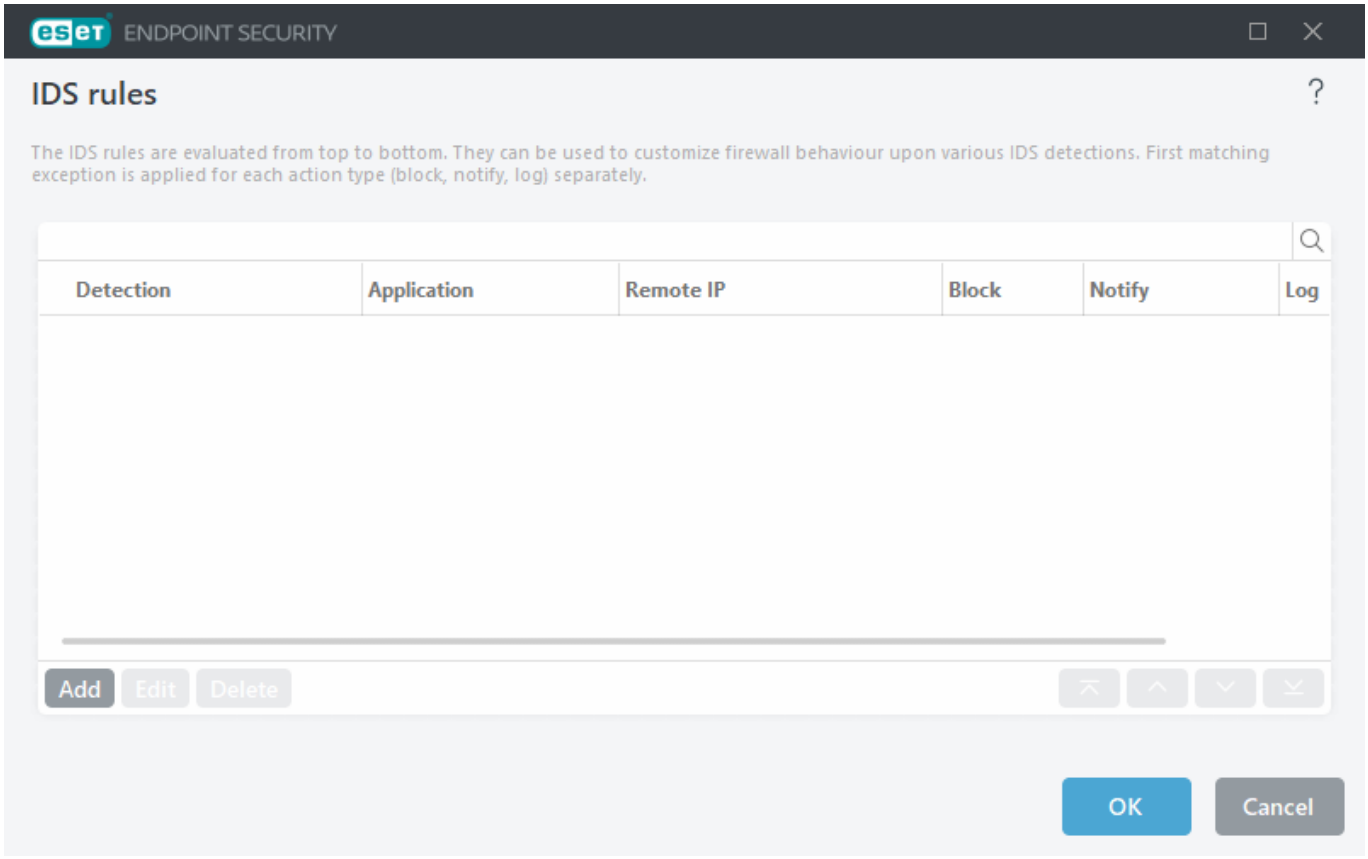
IDS rules

In some situations the Intrusion Detection Service (IDS) may detect communication between routers or other internal networking devices as a potential attack. For example, you can add the known safe address to the Addresses excluded from IDS zone to bypass the IDS.

The following ESET Knowledgebase articles may only be available in English:
- Create IDS rules on client workstations in ESET Endpoint Security
- Create IDS rules for client workstations in ESET PROTECT On-Prem

Managing IDS rules

- **Add**—Click to create a new IDS rule.
- **Edit**—Click to edit an existing IDS rule.
- **Delete**—Select and click if you want to remove an existing rule from the list of IDS rules.
-  **Top/Up/Down/Bottom**—Adjust the priority level of rules (exceptions are evaluated from top to bottom).



Tab **Exclusions** will be displayed if an administrator creates IDS exclusions in ESET PROTECT On-Prem Web Console. IDS exclusions can contain allowing rules only and are evaluated before IDS rules.

Rule editor

Detection—Type of detection.

Threat name—You can specify a threat name for some of the detections available.

Application—Select the file path of an excepted application by clicking ... (for example *C:\Program Files\Firefox\Firefox.exe*). Do NOT type the name of the application.

Remote IP address—A list of remote IPv4 or IPv6 addresses/ranges/subnets. Multiple addresses must be separated by a comma.

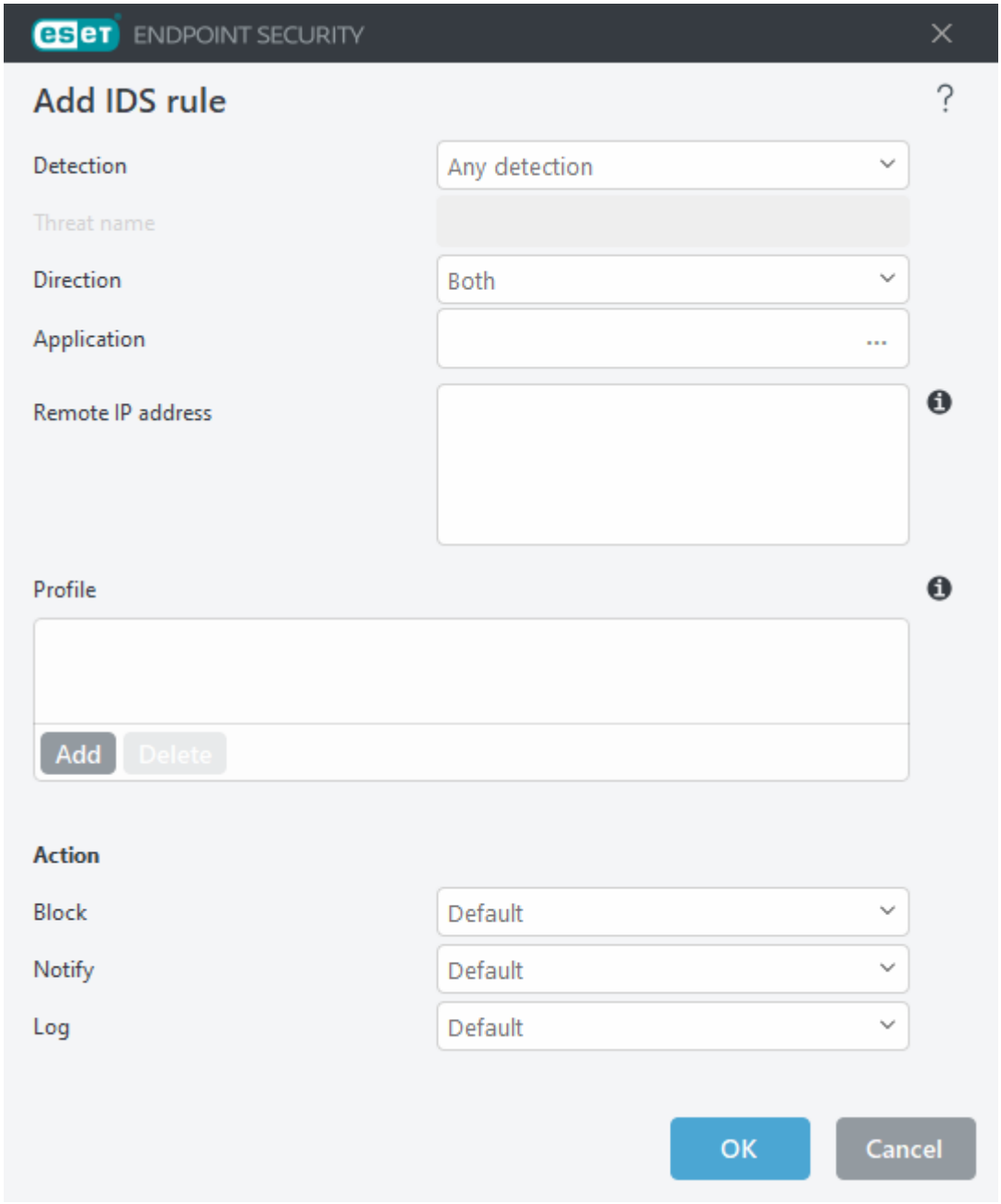
Profile—You can choose a network connection profile to which this rule will apply.

Action

Block—Each system process has its own default behavior and assigned action (block or allow). To override the default behavior for ESET Endpoint Security you can choose to block or allow it using the drop-down menu.

Notify—Select Yes to display Desktop notifications on your computer. Select No if you do not want desktop notifications. The available values are Default/Yes/No.

Log—Select **Yes** to log events to ESET Endpoint Security log files. Select **No** if you do not want to log events. The available values are **Default**/**Yes**/**No**.



You want to display a notification and collect a log each time the event occurs:
1. Click **Add** to add a new IDS rule.
2. Select specific alert from the **Detection** drop-down menu.
3. Click **...** and select the file path of the application to which you want to apply the notification.
4. Leave **Default** in the **Block** drop-down menu. This will inherit the default action applied by ESET Endpoint Security.
5. Set both the **Notify** and **Log** drop-down menus to **Yes**.
6. Click **OK** to save this notification.

You want to remove recurring notifications for a type of detection you do not consider to be a threat:
1. Click **Add** to add a new IDS exception.
2. Select specific alert from the **Detection** drop-down menu, for example **SMB session without security extensions** or **TCP Port Scanning attack**.
3. Select **In** from the direction drop-down menu if it is from an inbound communication.
4. Set the **Notify** drop-down menu to **No**.
5. Set the **Log** drop-down menu to **Yes**.
6. Leave **Application** blank.
7. If the communication is not coming from a specific IP address, leave **Remote IP addresses** blank.
8. Click **OK** to save this notification.

Brute-force attack protection

Brute-force attack protection blocks password-guessing attacks for RDP and SMB services. A brute-force attack is a method of discovering a targeted password by systematically trying all combinations of letters, numbers, and symbols. To configure the Brute-force attack protection, open Advanced setup > **Protections** > **Network access protection** > **Network attack protection** > **Brute-force attack protection**.

Enable Brute-force attack protection—ESET Endpoint Security inspects network traffic content and blocks the attempts of password-guessing attacks.

Rules—Enables you to create, edit and view rules for incoming and outgoing network connections. For more information, see Rules.

Exclusions—List of excluded detections defined by an IP address or application path. You can create and edit exclusions in ESET PROTECT On-Prem. For more information, see Exclusions.

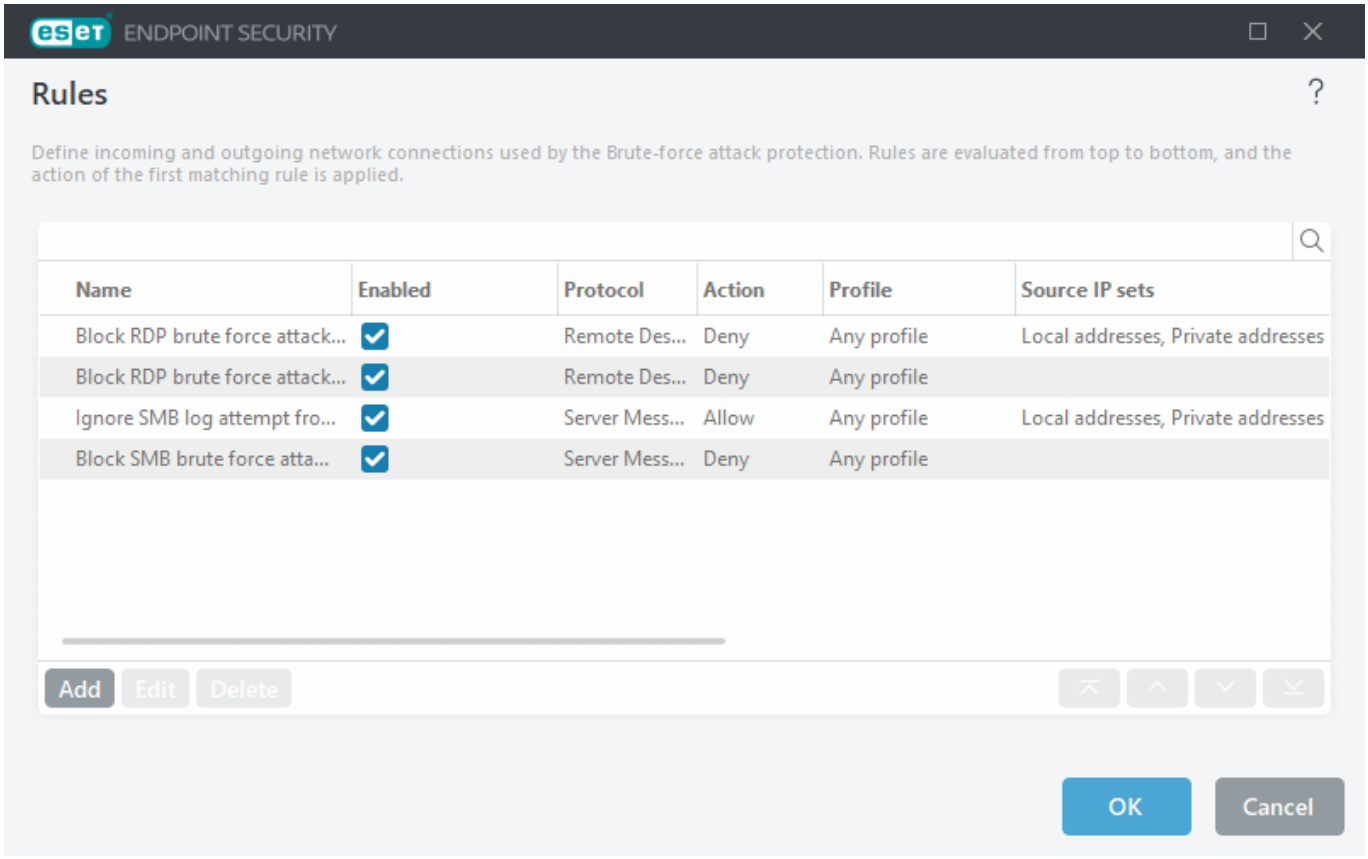
For more information about Brute-force attack protection, see the ESET Digital Security Guide article.

Rules

Brute-force attack protection rules enable you to create, edit and view rules for incoming and outgoing network connections. The pre-defined rules cannot be edited or deleted.

Managing Brute-force attack protection rules

- **Add**—Click to create a new Brute-force attack protection rule.
- **Edit**—Click to edit an existing Brute-force attack protection rule.
- **Delete**—Select and click if you want to remove an existing exception from the list of IDS rules.
- **Top/Up/Down/Bottom**—Adjust the priority level of rules.



> To ensure the highest possible protection, the blocking rule with the lowest **Max attempts** value is applied even if the rule is positioned lower in the Rules list when multiple blocking rules match the detection conditions.

Rule editor

Name—Name of the rule.

Enabled—Disable the toggle if you want to keep the rule in the list but not apply it.

Action—Choose whether to **Deny** or **Allow** the connection if the rule settings are fulfilled.

Protocol—The communication protocol this rule will inspect.

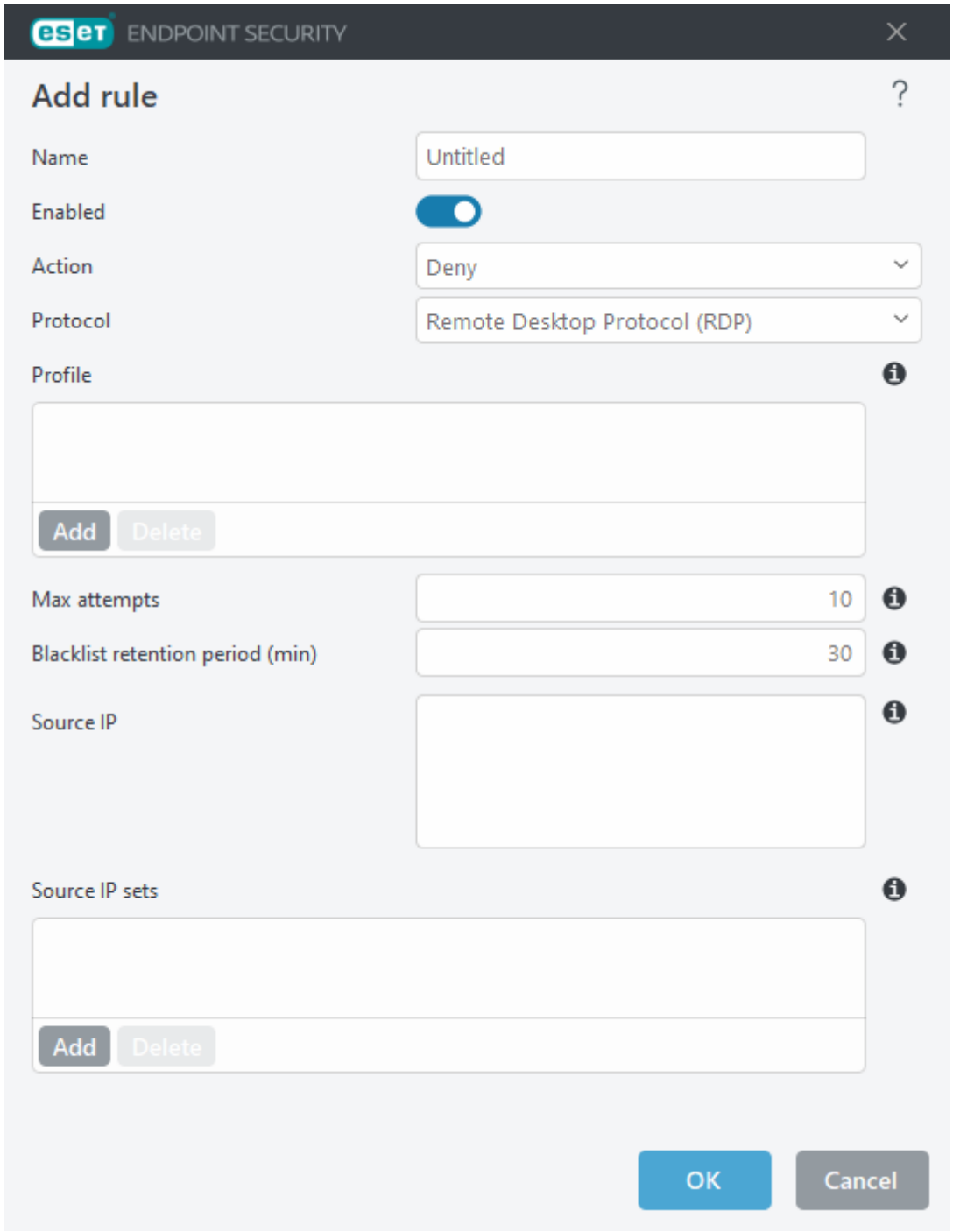
Profile—You can choose a network connection profile to which this rule will apply.

Max attempts—The maximum number of allowed attempts of attack repetition until the IP address is blocked and added to the blacklist.

Blacklist retention period (min)—Sets the time for the address expiration from the blacklist.

Source IP—A list of IP addresses/ranges/subnets. Multiple addresses must be separated by a comma.

Source IP sets—Set of IP addresses you have already defined in IP sets.



Exclusions

Brute-force exclusions can be used to suppress Brute-force detection for specific criteria. These exclusions are created from ESET PROTECT On-Prem based on Brute-force detection.

Columns

- **Detection**—Type of detection.
- **Application**—Select the file path of an excepted application by clicking ... (for example *C:\Program Files\Firefox\Firefox.exe*). Do NOT type the name of the application.
- **Remote IP**—A list of remote IPv4 or IPv6 address/ranges/subnets. Multiple addresses must be separated by a comma.

Managing Exclusions

The exclusions will be displayed if an administrator creates Brute-force exclusions in ESET PROTECT On-Prem Web Console. Exclusions can contain allowing rules only and are evaluated before IDS rules.

Advanced options

In Advanced setup > **Protections** > **Network access protection** > **Network attack protection** > **Advanced options**, you can enable or disable detection of several types of attacks and exploits that may harm your computer.

> In some cases, you will not receive a threat notification about blocked communications. See the Logging and creating rules or exceptions from log section for instructions to view all blocked communications in the firewall log.

> The availability of specific options in this window may vary depending on the type or version of your ESET product and firewall module, as well as the version of your operating system.

Intrusion detection

- **Protocol SMB**—Detects and blocks various security problems in SMB protocol, namely:
- **Rogue server challenge attack authentication detection**—Protects against an attack that uses a rogue challenge during authentication to obtain user credentials.
- **IDS evasion during named pipe opening detection**—Detection of known evasion techniques used for opening MSRPCS named pipes in SMB protocol.
- **CVE detections** (Common Vulnerabilities and Exposures)—Implemented detection methods of various attacks, forms, security holes and exploits over SMB protocol. See the CVE website at cve.mitre.org to search and obtain more detailed info about CVE identifiers (CVEs).
- **Protocol RPC**—Detects and blocks various CVEs in the remote procedure call system developed for the Distributed Computing Environment (DCE).
- **Protocol RDP**—Detects and blocks various CVEs in the RDP protocol (see above).
- **ARP Poisoning attack detection**—Detection of ARP poisoning attacks triggered by man in the middle attacks or detection of sniffing at network switch. ARP (Address Resolution Protocol) is used by the network application or device to determine the Ethernet address.
- **TCP/UDP Port Scanning attack detection**—Detects attacks of port scanning software—application designed to probe a host for open ports by sending client requests to a range of port addresses with the goal of finding active ports and exploiting the vulnerability of the service. Read more about this type of attack in the glossary.
- **Block unsafe address after attack detection**—IP addresses detected as sources of attacks are added to the Blacklist to prevent connection for a certain time. You can define **Blacklist retention period**, which sets the time for how long the address will be blocked after attack detection.
- **Notify about attack detection**—Turns on the Windows notification area notification at the bottom right corner of the screen.
- **Notify about incoming attacks against security holes**—Alerts you if attacks against security holes are detected or if an attempt is made by a threat to enter the system this way.

Packet inspection

- **Allow incoming connection to admin shares in SMB protocol**—The administrative shares (admin shares) are the default network shares that share hard drive partitions (*C$*, *D$*, ...) in the system together with the system folder (*ADMIN$*). Disabling connection to admin shares should mitigate many security risks. For example, the Conficker worm performs dictionary attacks to connect to admin shares.

- **Deny old (unsupported) SMB dialects**—Deny SMB sessions that use an old SMB dialect unsupported by IDS. Modern Windows operating systems support old SMB dialects due to backward compatibility with old operating systems such as Windows 95. The attacker can use an old dialect in an SMB session to evade traffic inspection. Deny old SMB dialects if your computer does not need to share files (or use SMB communication in general) with a computer with an old version of Windows.
- **Deny SMB sessions without extended security**—Extended security can be used during the SMB session negotiation to provide a more secure authentication mechanism than LAN Manager Challenge/Response (LM) authentication. The LM scheme is considered weak and is not recommended for use.
- **Deny opening of executable files on a server outside the Trusted zone in SMB protocol**—Drops connection when you are trying to open an executable file (.exe, .dll, ...) from a shared folder on the server that does not belong to the Trusted zone in firewall. Note that copying executable files from trusted sources can be legitimate, however this detection should mitigate risks from the unwanted opening of a file on a malicious server (for example, a file opened by clicking a hyperlink to a shared malicious executable file).
- **Deny NTLM authentication in SMB protocol for connecting a server in/outside the Trusted zone**—Protocols that use NTLM (both versions) authentication schemes are subject to a credentials forwarding attack (known as an SMB Relay attack in the case of SMB protocol). Denying NTLM authentication with a server outside the Trusted zone should mitigate risks from forwarding credentials by a malicious server outside the Trusted zone. Similarly, you can deny NTLM authentication with servers in the Trusted zone.

- **Allow communication with the Security Account Manager service**—For more information about this service see [MS-SAMR].

- **Allow communication with the Local Security Authority service**—For more information about this service see [MS-LSAD] and [MS-LSAT].

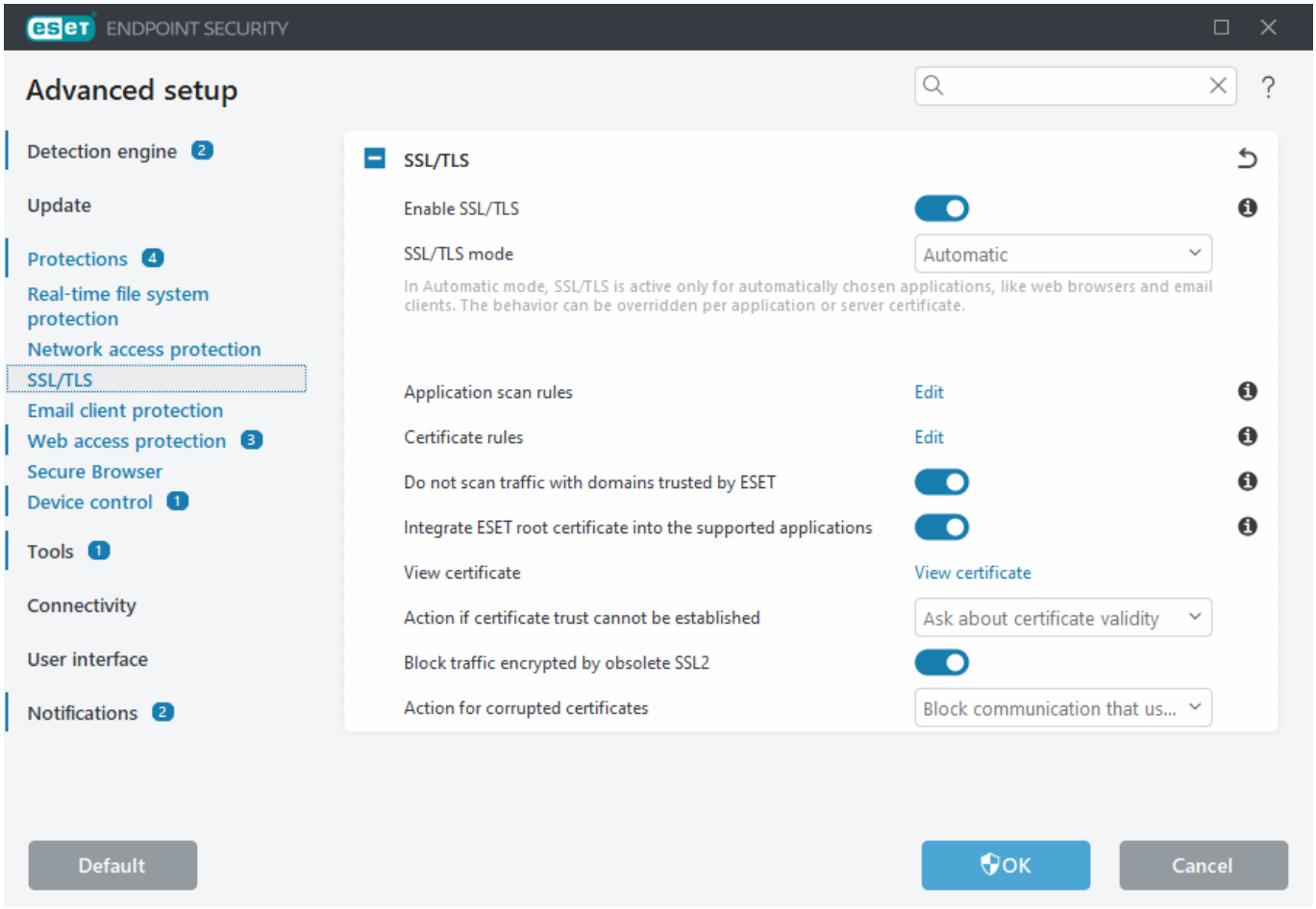
- **Allow communication with the Remote Registry service**—For more information about this service see [MS-RRP].

- **Allow communication with the Service Control Manager service**—For more information about this service see [MS-SCMR].

- **Allow communication with the Server service**—For information about this service see [MS-SRVS].
- **Allow communication with the other services**—Other MSRPC services. MSRPC is the Microsoft implementation of the DCE RPC mechanism. Moreover, MSRPC can use named pipes carried into the SMB (network file sharing) protocol for transport (ncacn_np transport). MSRPC services provide interfaces for accessing and managing windows systems remotely. Several security vulnerabilities have been discovered and exploited in the wild in the Windows MSRPC system (for example, Conficker worm, Sasser worm,...). Disable communication with MSRPC services that you do not need to provide to mitigate many security risks (such as remote code execution or service failure attacks).

SSL/TLS

ESET Endpoint Security can check for communication threats that use the SSL protocol. You can use various filtering modes to examine SSL-protected communication with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking. To edit SSL/TLS settings, open Advanced setup > **Protections** > **SSL/TLS**.



Enable SSL/TLS—If disabled, ESET Endpoint Security will not scan communication over SSL/TLS.

SSL/TLS mode is available in the following options:

Filtering mode	Description
Automatic	The default mode will only scan appropriate applications, such as web browsers and email clients. You can override it by selecting the applications where communication is scanned.
Interactive	If you access a new SSL-protected site (with an unknown certificate), an action selection dialog is displayed. This mode allows you to create a list of SSL certificates/applications that will be excluded from scanning.
Policy-based	Select this option to scan all SSL-protected communication, except communication protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate marked as trusted (it is on the trusted certificates list), communication to the server is allowed, and the communication channel content is filtered.

Application scan rules—Allows you to customize ESET Endpoint Security behavior for specific applications.

Certificate rules—Allows you to customize ESET Endpoint Security behavior for specific SSL certificates.

Do not scan traffic with domains trusted by ESET—When enabled, communication with trusted domains will be excluded from scanning. An ESET-managed, built-in whitelist determines a domain's trustworthiness.

Integrate ESET root certificate into the supported applications—For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root certificates (publishers). When enabled, ESET Endpoint Security will automatically add the ESET SSL Filter CA certificate to known browsers (for example, Opera). For browsers using the system certification store, the certificate is added automatically. For example, Firefox is automatically configured to trust Root authorities in the system certification store.

To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File** and manually import it into the browser.

Action if certificate trust cannot be established—In some cases, a website certificate cannot be verified using the Trusted Root Certification Authorities (TRCA) store (for example, expired certificate, untrusted certificate, certificate not valid for the specific domain or signature that can be parsed but does not sign the certificate correctly). Legitimate websites will always use trusted certificates. If they are not providing one, it could mean that an attacker is decrypting your communication or the website is experiencing technical difficulties.

If **Ask about certificate validity** is selected (selected by default), you will be prompted to choose an action when encrypted communication is established. An action selection dialog will be displayed where you can mark the certificate as trusted or excluded. If the certificate is not present in the TRCA list, the window is red. If the certificate is on the TRCA list, the window will be green.

You can select **Block communication that uses the certificate** to always terminate an encrypted connection to a site that uses an untrusted certificate.

Block traffic encrypted by obsolete SSL2—Communication using the earlier version of the SSL protocol will automatically be blocked.

Action for corrupted certificates—A corrupted certificate means that the certificate uses a format not recognized by ESET Endpoint Security or has been received damaged (for example, overwritten by random data). In this case, we recommend leaving **Block communication that uses the certificate** selected. If **Ask about certificate validity** is selected, the user is prompted to choose an action when the encrypted communication is established.

The following ESET Knowledgebase article may only be available in English:
- Certificate notifications in ESET products
- "Encrypted network traffic: Untrusted certificate" is displayed when visiting web pages

Application scan rules

The **Application scan rules** can be used to customize ESET Endpoint Security behavior for specific applications and remember actions chosen when **SSL/TLS mode** is in **Interactive mode**. The list can be viewed and edited in Advanced setup > **Protections** > **SSL/TLS** > **Application scan rules** > **Edit**.

The **Application scan rules** window consists of:

Columns

Application—Choose an executable file from the directory tree, click the **...** option or type the path manually.

Scan action—Select **Scan** or **Ignore** to scan or ignore communication. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** to always ask the user what to do.

Control elements

Add—Add filtered application.

Edit—Select the application you want to configure and click **Edit**.

Delete—Select the application you want to delete and click **Delete**.

Import/Export—Import applications from a file or save your current list of applications to a file.

OK/Cancel—Click **OK** if you want to save changes or click **Cancel** if you want to exit without saving.

Certificate rules

Certificate rules can be used to customize ESET Endpoint Security behavior for specific SSL certificates and to remember actions chosen when **SSL/TLS mode** is in **Interactive mode**. The list can be viewed and edited in Advanced setup > **Protections** > **SSL/TLS** > **Certificate rules** > **Edit**.

The **Certificate rules** window consists of:

Columns

Name—Name of the certificate.

Certificate issuer—Name of the certificate creator.

Certificate subject—The subject field identifies the entity associated with the public key stored in the subject public key field.

Access—Select **Allow** or **Block** as the **Access action** to allow/block communication secured by this certificate regardless of its trustworthiness. Select **Auto** to allow trusted certificates and ask for untrusted ones. Select **Ask** to always ask user what to do.

Scan—Select **Scan** or **Ignore** as the **Scan action** to scan or ignore communication secured by this certificate. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** to always ask the user what to do.

Control elements

Add—Add a new certificate and adjust its settings regarding access and scan options.

Edit—Select the certificate that you want to configure and click **Edit**.

Delete—Select the certificate that you want to delete and click **Remove**.

OK/Cancel—Click **OK** if you want to save changes or click **Cancel** if you want to exit without saving.

Encrypted network traffic

If your system is configured to use SSL/TLS scanning, a dialog window prompting you to choose an action will be displayed in two situations:

First, if a website uses an unverifiable or invalid certificate, and ESET Endpoint Security is configured to ask the user in such cases (by default yes for unverifiable certificates, no for invalid ones), a dialog box will ask you whether to **Allow** or **Block** the connection. If the certificate is not located in the Trusted Root Certification Authorities store (TRCA), it is considered untrusted.

Second, if **SSL/TLS mode** is set to **Interactive mode**, a dialog box for each website will ask whether to **Scan** or **Ignore** the traffic. Some applications verify that their SSL traffic is not modified nor inspected by anyone, in such cases ESET Endpoint Security must **Ignore** that traffic to keep the application working.

> **Illustrated examples**
> The following ESET Knowledgebase article may only be available in English:
> - Certificate notifications in ESET Windows products
> - "Encrypted network traffic: Untrusted certificate" is displayed when visiting web pages

In both cases, the user can choose to remember the selected action. Saved actions are stored in the Certificate rules.

Email client protection

To configure the Email client protection, open Advanced setup > **Protections** > **Email client protection**, and choose from the following configuration options:

- Mail transport protection
- Mailbox protection
- Address lists management
- ThreatSense

Mail transport protection

IMAP(S) and POP3(S) protocols are the most widespread protocols used to receive email communication in an email client application. The Internet Message Access Protocol (IMAP) is another internet protocol for email retrieval. IMAP has some advantages over POP3, for example, multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. The protection module providing this control is automatically initiated at system startup and is then active in memory.

ESET Endpoint Security provides protection for these protocols regardless of the email client used, and without requiring re-configuration of the email client. By default, all communication over POP3 and IMAP protocols is scanned, regardless of the default POP3/IMAP port numbers.

MAPI protocol is not scanned. However the communication with the Microsoft Exchange server can be scanned by the integration module in email clients such as Microsoft Outlook.

> ESET Endpoint Security also supports the scanning of IMAPS (585, 993) and POP3S (995) protocols, which use an encrypted channel to transfer information between server and client. ESET Endpoint Security checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. Encrypted communication will be scanned by default. To view the scanner setup, open Advanced setup > **Protections** > SSL/TLS.

To configure Mail transport protection, open Advanced setup > **Protections** > **Email client protection** > **Mail transport protection**.

Enable Mail transport protection—When enabled, mail transport communication will be scanned by ESET Endpoint Security.

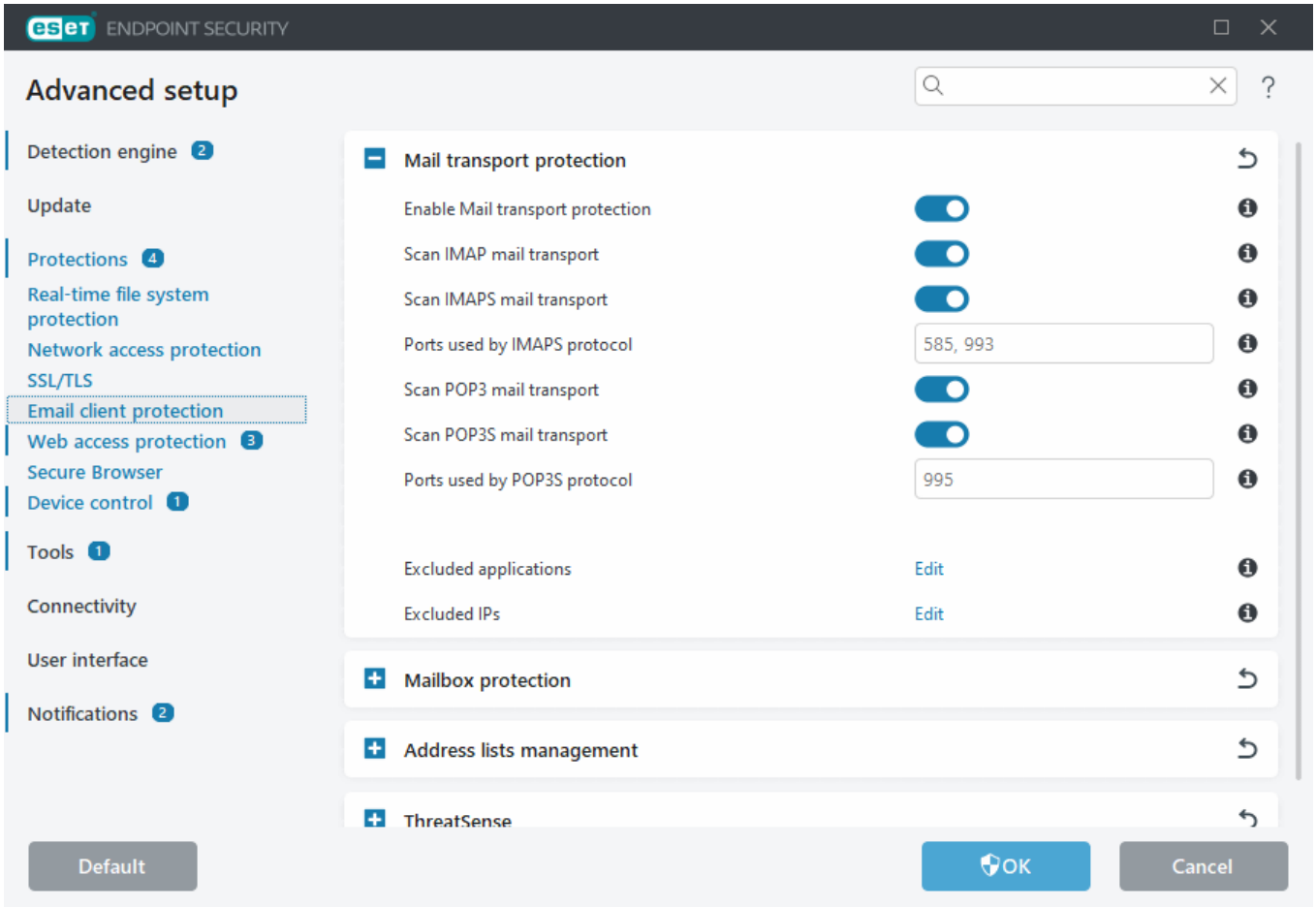
You can choose which mail transport protocols will be scanned by clicking the toggle next to the following options (by default, scanning of all protocols is enabled):

- **Scan IMAP mail transport**
- **Scan IMAPS mail transport**
- **Scan POP3 mail transport**
- **Scan POP3S mail transport**

By default, ESET Endpoint Security will scan IMAPS and POP3S communication on the standard ports. To add custom ports for IMAPS and POP3S protocols, add them to the text field next to **Ports used by IMAPS protocol** or **Ports used by POP3S protocol**. Multiple port numbers must be delimited by a comma.

Excluded applications—Enables you to exclude specific applications from being scanned by Mail transport protection. Useful when Web access protection causes compatibility issues.

Excluded IPs—Enables you to exclude specific remote addresses from being scanned by Mail transport protection. Useful when Web access protection causes compatibility issues.



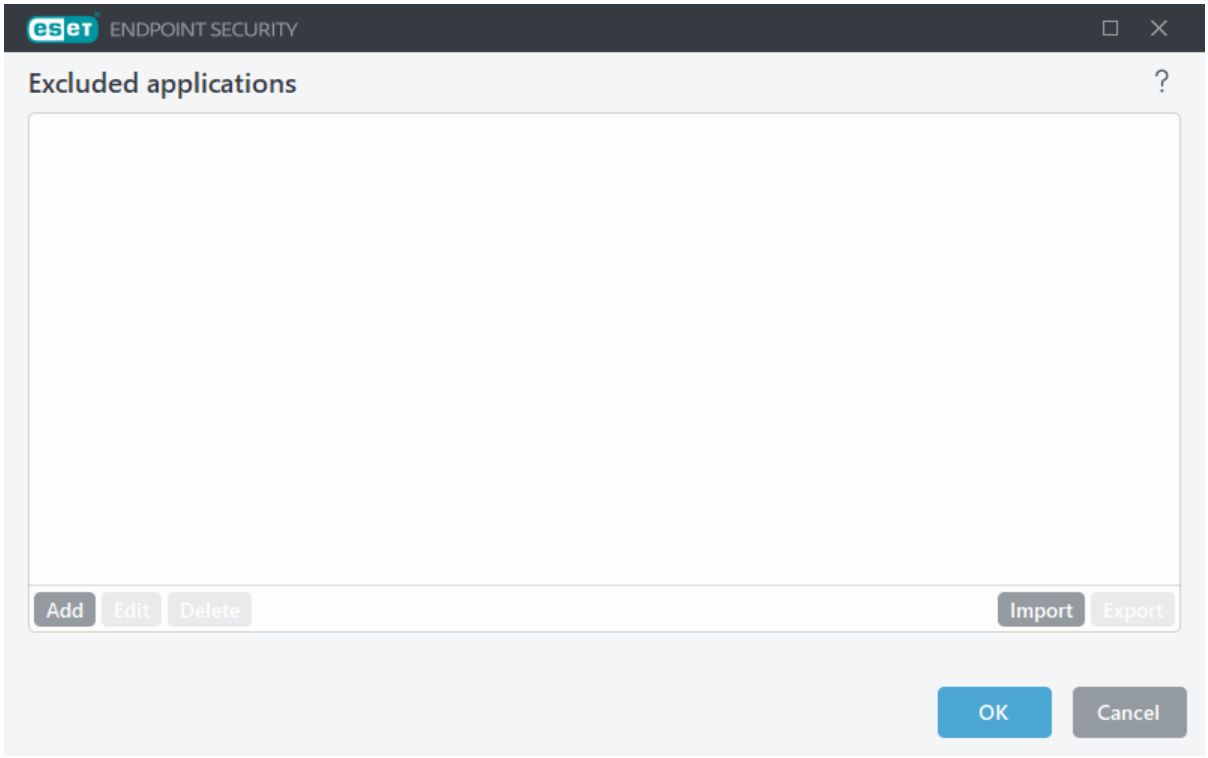
Excluded applications

To exclude scanning of communication for specific applications, add them to the list. HTTP(S)/POP3(S)/IMAP(S) communication of the selected applications will not be checked for threats. We recommend only using this for applications that do not work properly with their communication being scanned.

Running applications and services will be available here automatically when you click **Add**. Click **...** and navigate to an application to add exclusion manually.

Edit—Edit selected entries from the list.

Delete—Remove selected entries from the list.



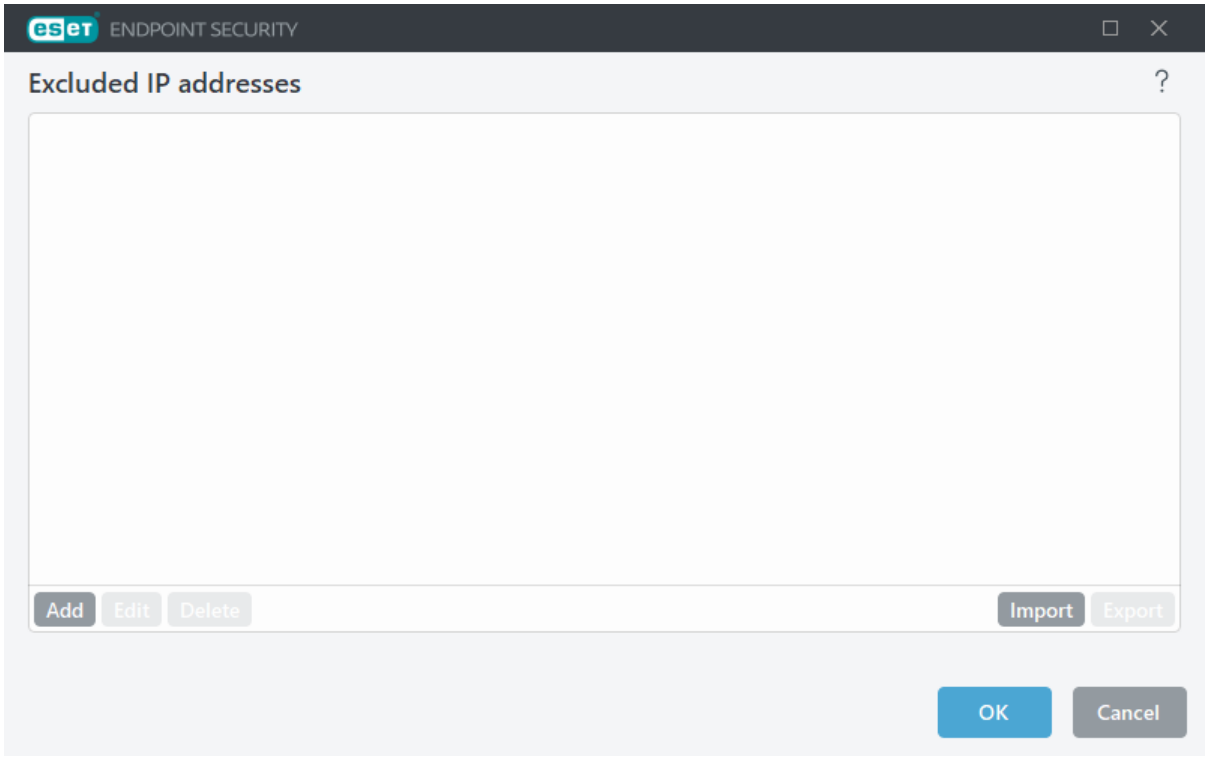
Excluded IPs

The entries in the list will be excluded from scanning. HTTP(S)/POP3(S)/IMAP(S) communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Add—Click to add an IP address/address range/subnet of a remote point to which a rule is applied.

Edit—Edit selected entries from the list.

Delete—Remove selected entries from the list.



IP addresses examples

Add IPv4 address:

Single address—Adds an IP address of an individual computer (for example, *192.168.0.10*).

Address range—Type the starting and ending IP addresses to specify the IP range of several computers (for example, *192.168.0.1-192.168.0.99*).

Subnet—Subnet (a group of computers) defined by an IP address and mask. For example, 255.255.255.0 is the network mask for the 192.168.1.0 subnet. To exclude the whole subnet type in *192.168.1.0/24*.

Add IPv6 address:

Single address—Adds the IP address of an individual computer (for example, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnet—Subnet (a group of computers) is defined by an IP address and mask (for example, *2002:c0a8:6301:1::1/64*).

Mailbox protection

Integration of ESET Endpoint Security with your Mailbox increases the level of active protection against malicious code in email messages.

To configure Mailbox protection, open Advanced setup > **Protections** > **Email client protection** > **Mailbox protection**.

Enable email protection by client plugins—When disabled, protection by email client plugins is turned off.

Select emails to scan:

- **Received email**
- **Sent email**
- **Read email**
- **Modified email**

We recommend that you keep **Enable email protection by client plugins** enabled. Even if integration is not enabled or functional, email communication is still protected by Mail transport protection (IMAP/IMAPS and POP3/POP3S).

Scan for spam

Unsolicited email, called spam, ranks among the greatest electronic communication problems. Spam represents up to 30 percent of all email communication. Email client antispam serves to protect against this problem. Combining several email security principles, Email client antispam provides superior filtering to keep your inbox clean. For spam detection, one important principle is recognizing unsolicited emails based on pre-defined trusted addresses (allowed) and spam addresses (blocked).

The primary method used to detect spam is scanning email message properties. Received messages are scanned for basic antispam criteria (message definitions, statistical heuristics, recognizing algorithms and other unique methods), and the resulting index value determines whether a message is a spam or not.

Enable Email client antispam—When enabled, received messages will be scanned for spam.

Use advanced spam scanner—Additional antispam data will be downloaded periodically, increasing antispam capabilities producing better results.

Spam score logging—The ESET Endpoint Security Antispam engine assigns a spam score to every scanned message. The message will be recorded in the Antispam protection log (main program window > **Tools** > **Log files** > **Email client antispam**).

- **None**—The score from antispam scanning will not be logged.
- **Reclassified and marked as spam**—Select this if you want to record a spam score for messages marked as SPAM.
- **All**—All messages will be recorded to the log with a spam score.

When you click a message in the junk email folder, you can choose **Reclassify selected messages as NOT spam**, and the message will be moved to the inbox. When you click a message you consider spam in the inbox, select **Reclassify messages as spam** and the message will be moved to the junk email folder. You can select multiple messages and act on all of them simultaneously.

Integrations—Enables you to integrate Mailbox protection into your Email client. See Integrations for more information.

Response—Enables you to customize handling of spam messages. See Response for more information.

Integrations

Integration of ESET Endpoint Security with your email client increases the level of active protection against malicious code in email messages. If your email client is supported, you can enable integration in ESET Endpoint Security. When integrated into your email client, the ESET Endpoint Security toolbar is inserted directly into the email client for more efficient email protection. To edit Integration settings, open Advanced setup > **Protections** > **Email client protection** > **Mailbox protection** > **Integration**.

Integrate into Microsoft Outlook—Microsoft Outlook is currently the only supported email client. Email protection works as a plugin. The main advantage of the plugin is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. See this ESET Knowledgebase article for a complete list of supported Microsoft Outlook versions.

Advanced email client processing—Processes extra Outlook Messaging API (MAPI) events: Object modified (`fnevObjectModified`) and Object created (`fnevObjectCreated`). If you are experiencing a system slowdown when working with your email client, disable this option.

Microsoft Outlook toolbar

Microsoft Outlook protection works as a plugin module. After ESET Endpoint Security is installed, this toolbar containing the antivirus protection and Email client antispam options is added to Microsoft Outlook:

Spam—Marks chosen messages as spam. After marking, a "fingerprint" of the message is sent to a central server storing spam signatures. If the server receives more similar "fingerprints" from several users, the message will be classified as spam in the future.

Not spam—Marks chosen messages as not spam.

Spam address (Blocked, a list of spam addresses)—Adds a new sender address to the Address list as Blocked. All messages received from the list will be automatically classified as spam.

Beware of spoofing—forging a sender's address on email messages to mislead email recipients into reading and responding.

Trusted address (Allowed, a list of trusted addresses)—Adds a new sender address to the Address list as Allowed. All messages received from allowed addresses will never be automatically classified as spam.

ESET Endpoint Security—Double-click the icon to open the main window of ESET Endpoint Security.

Rescan messages—Enables you to launch email checking manually. You can specify messages that will be checked, and you can activate rescanning of the received emails. For more information, see Mailbox protection.

Scanner setup—Displays Mailbox protection setup options.

Antispam setup—Displays Mailbox protection setup options.

Antispam address list—Opens the Address lists management window, where you can access lists of excluded, trusted and spam addresses.

Confirmation dialog

This notification serves to verify that user really wants to perform the selected action, which should eliminate possible mistakes.

On the other hand, the dialog also offers the option to disable confirmations.

Rescan messages

The ESET Endpoint Security toolbar integrated in email clients enables users to specify several options for email checking. The option **Rescan messages** offers two scanning modes:

All messages in the current folder—Scans messages in the currently displayed folder.

Selected messages only—Scans only messages marked by the user.

The **Rescan already scanned messages** checkbox provides the user with the option to run another scan on messages that have been scanned before.

Response

Based on the message scan results, ESET Endpoint Security can move scanned messages or add custom text to subject. You can configure these settings in Advanced setup > **Protections** > **Email client protection** > **Mailbox protection** > **Response**.

Email client antispam in ESET Endpoint Security enables you to configure the following parameters for messages:

Add text to email subject—Enables you to add a custom prefix string to the subject line of messages that have been classified as spam. The default **Text** is "[SPAM]".

Move to spam folder—When enabled, spam messages will be moved to the default junk email folder, and messages reclassified as not spam will be moved to the inbox. When you right-click an email message and select ESET Endpoint Security from the context menu, you can choose from applicable options.

Move to custom folder—When enabled, spam messages will be moved to a folder specified below.

Folder—Specify the custom folder where you want to move infected emails when detected.

If there is a message containing detection, by default, ESET Endpoint Security attempts to clean the message. If the message cannot be cleaned, you can choose an **Action to take if cleaning not possible**:

- **No action**—If enabled, the program will identify infected attachments but will leave emails without taking any action.
- **Delete email**—The program will notify the user about infiltration(s) and delete the message.
- **Move email to the Deleted items folder**—Infected emails will be moved automatically to the Deleted items folder.
- **Move email to folder** (default action)—Infected emails will be moved automatically to the specified folder.

Folder—Specify the custom folder where you want to move infected emails when detected.

Mark spam messages as read—Enable this to mark spam as read automatically. It will help you to focus your attention on "clean" messages.

Mark reclassified messages as unread—Messages originally classified as spam but later marked as "clean" will be displayed as unread.

After an email has been checked, a notification with the scan result can be appended to the message. You can

elect to **Append tag messages to received and read email** or **Append tag messages to sent email**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The following options are available:

- **Never**—No tag messages will be added.
- **When a detection occurs**—Only messages containing malicious software will be marked as checked (default).
- **To all email when scanned**—The program will append messages to all scanned email.

Update subject of received and read email / Update subject of sent email—Enable this option to add custom text specified below to the message.

Text to add to subject of detected email—Edit this template if you want to modify the subject prefix format of an infected email. This function will replace the message subject "Hello" to the following format: "[detection %DETECTIONNAME%] Hello". The variable %DETECTIONNAME% represents the detection.

Address lists management

The Email client antispam feature in ESET Endpoint Security enables you to configure various parameters for address lists. To configure address lists, open Advanced setup > **Protections** > **Email client protection** > **Address lists management**.

Enable user's address list—Enable this option to activate the user's address list.

User's address list—List of email addresses where you can add, edit or delete addresses to define the antispam rules. Rules in this list will be applied to the current user.

Enable global address list—Enable this option to activate the global address list shared by all users on this device.

Global address list—List of email addresses where you can add, edit or delete addresses to define the antispam rules. Rules in this list will be applied to all users.

Automatically allow and add into user's address list

Treat addresses from address book as trusted—Addresses from your contact list will be treated as trusted without adding to user's address list.

Add recipient addresses from outgoing messages—Add recipient addresses from sent messages to the user's address list as allowed.

Add addresses from messages reclassified as NOT spam—Add sender addresses from messages reclassified as NOT spam to the user's address list as allowed.

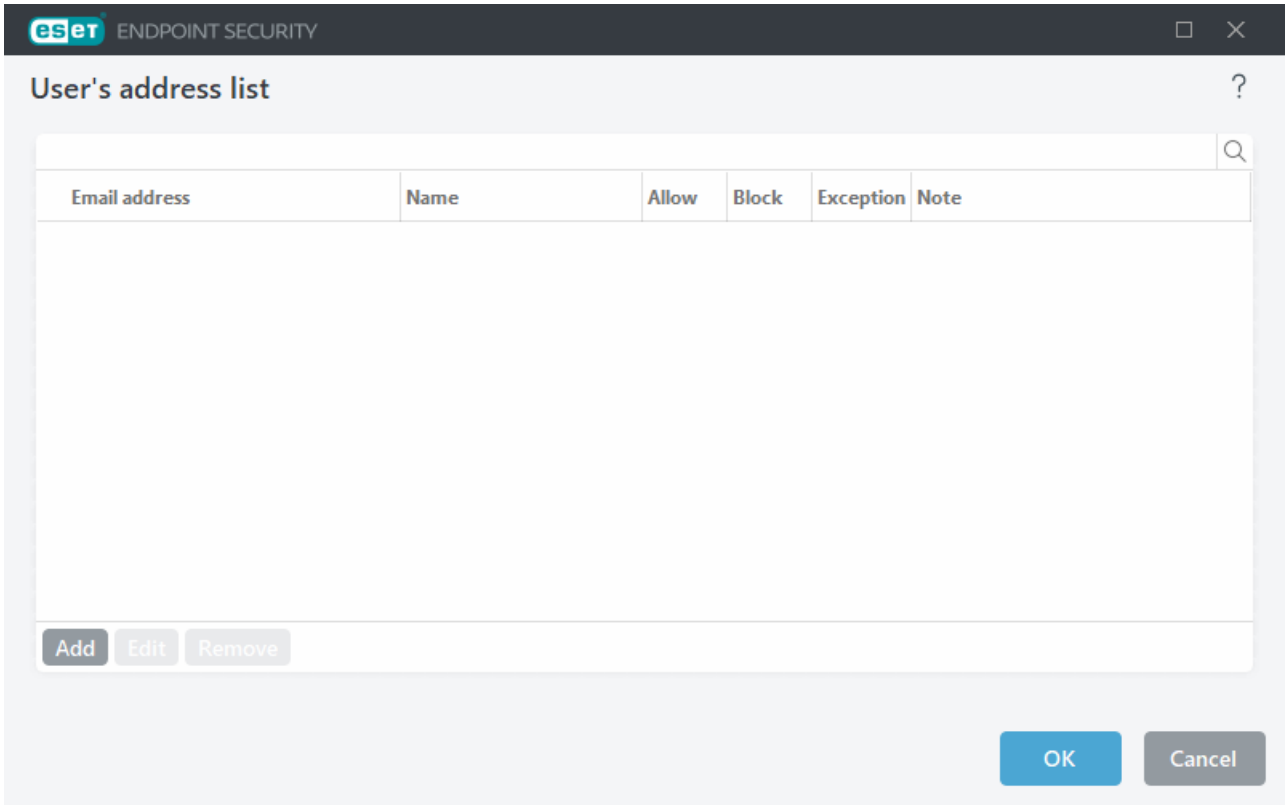
Automatically add into user's address list as an exception

Add addresses from own accounts—Add your addresses from existing email client accounts to the user's address list as an exception.

Address lists

To protect against unsolicited emails, ESET Endpoint Security enables you to classify email addresses in address lists.

To edit address lists, open Advanced setup > **Protections** > **Email client protection** > **Address lists management**, and click **Edit** next to **User's address list** or **Global address list**.



Columns

Email address—Address to which the rule will apply.

Name—Custom rule name.

Allow/Block/Exception—Radio buttons used to determine which action to take for the email address (click the radio button in the preferred column to quickly change the action):

- **Allow**—Addresses that are considered safe and from whom you want to receive messages.
- **Block**—Addresses that are considered unsafe/spam and from whom you do not want to receive messages.
- **Exception**—Addresses that are always checked for spam and that may be spoofed and used for sending spam.

Note—Information on how the rule was created and whether it applies to the whole domain / lower-level domains.

Managing the addresses

- **Add**—Click to add a rule for a new address.

- **Edit**—Select and click to edit an existing rule.
- **Remove**—Select and click if you want to delete a rule from the address list.

Add/Edit address

This window enables you to add or edit an address in the Address lists management and configure the action taken:

Email address—Address to which the rule will apply. Wildcards are not supported.

Name—Custom rule name.

Action—Action to take if the email address of the contact matches the address specified in the **Email address** field:

- **Allow**—Addresses that are considered safe and from whom you want to receive messages.
- **Block**—Addresses that are considered unsafe/spam and from whom you do not want to receive messages.
- **Exception**—Addresses that are always checked for spam and that may be spoofed and used for sending spam.

Whole domain—Select this option for the rule to be applied to the whole domain of the contact (not only to the address specified in the **Email address** field but all email addresses at the *address.info* domain).

Lower level domains—Select this option for the rule to be applied to the lower level domains of the contact (The *address.info* represents the domain, while *my.address.info* represents a subdomain).

Address processing result

When adding new addresses or changing the action taken for email address, ESET Endpoint Security displays notification messages. The content of notification messages varies based on the action you attempt to perform.

Select the **Do not ask again** check box to act automatically without displaying the message the next time.

ThreatSense

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options enable you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense** in the Advanced setup for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind,

ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section enables you to define which computer components and files will be scanned for infiltrations.

Operating memory—Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI—Scans boot sectors for the presence of malware in the master boot record. Read more about UEFI in the glossary.

Email files—The program supports the following extensions: DBX (Outlook Express) and EML.

Archives—The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives—Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers—After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics—A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist or was not covered by the previous versions of the detection engine module. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures—Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of ESET Endpoint Security while cleaning objects.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine setup for a On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS)—Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority—Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects—The Scan log will show all the scanned files in self-extracting archives, even those not infected (may generate a lot of scan log data and increase the scan log file size).

Enable Smart optimization—With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the specific modules are applied when performing a scan.

Preserve last access timestamp—Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

Limits

The Limits section enables you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size—Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited.

Maximum scan time for object (sec.)—Defines the maximum time value for the scan of files in a container object (such as a RAR/ZIP archive or an email with multiple attachments). This setting does not apply for standalone files. If a user-defined value has been typed and that time has elapsed, a scan will stop as soon as possible, regardless of whether the scan of each file in a container object has finished. In the case of an archive with large files, the scan will stop no sooner than a file from the archive is extracted (for example, when a user-defined variable is 3

seconds, but the extraction of a file takes 5 seconds). The rest of the files in the archive will not be scanned when that time has elapsed. To limit scanning time, including bigger archives, use **Maximum object size** and **Maximum size of file in archive** (not recommended due to possible security risks). Default value: unlimited.

Archive scan setup

Archive nesting level—Specifies the maximum depth of archive scanning. Default value: 10.

Maximum size of file in archive—This option enables you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. The maximum value is 3 GB.

> We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

Web access protection

Web access protection allows you to configure advanced Internet protection module settings. The following options are available in Advanced setup > **Protections** > **Web access protection** > **Web access protection**:

Enable Web access protection—When disabled, Web access protection and Anti-Phishing protection does not run.

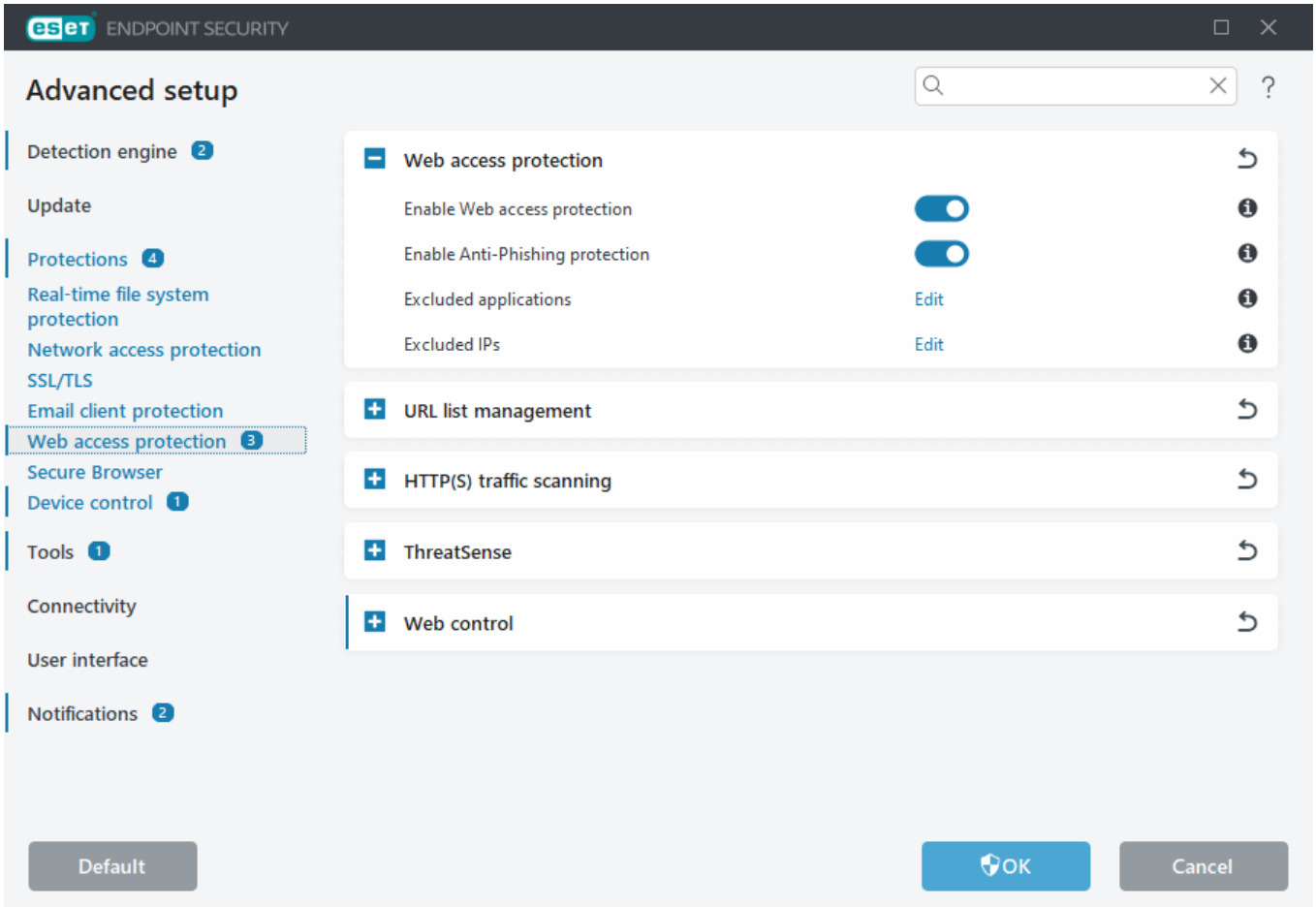
> We strongly recommend you leave Web access protection enabled and not exclude any applications or IP addresses by default.

Scan browser scripts—When enabled, the detection engine checks all JavaScript programs executed by web browsers.

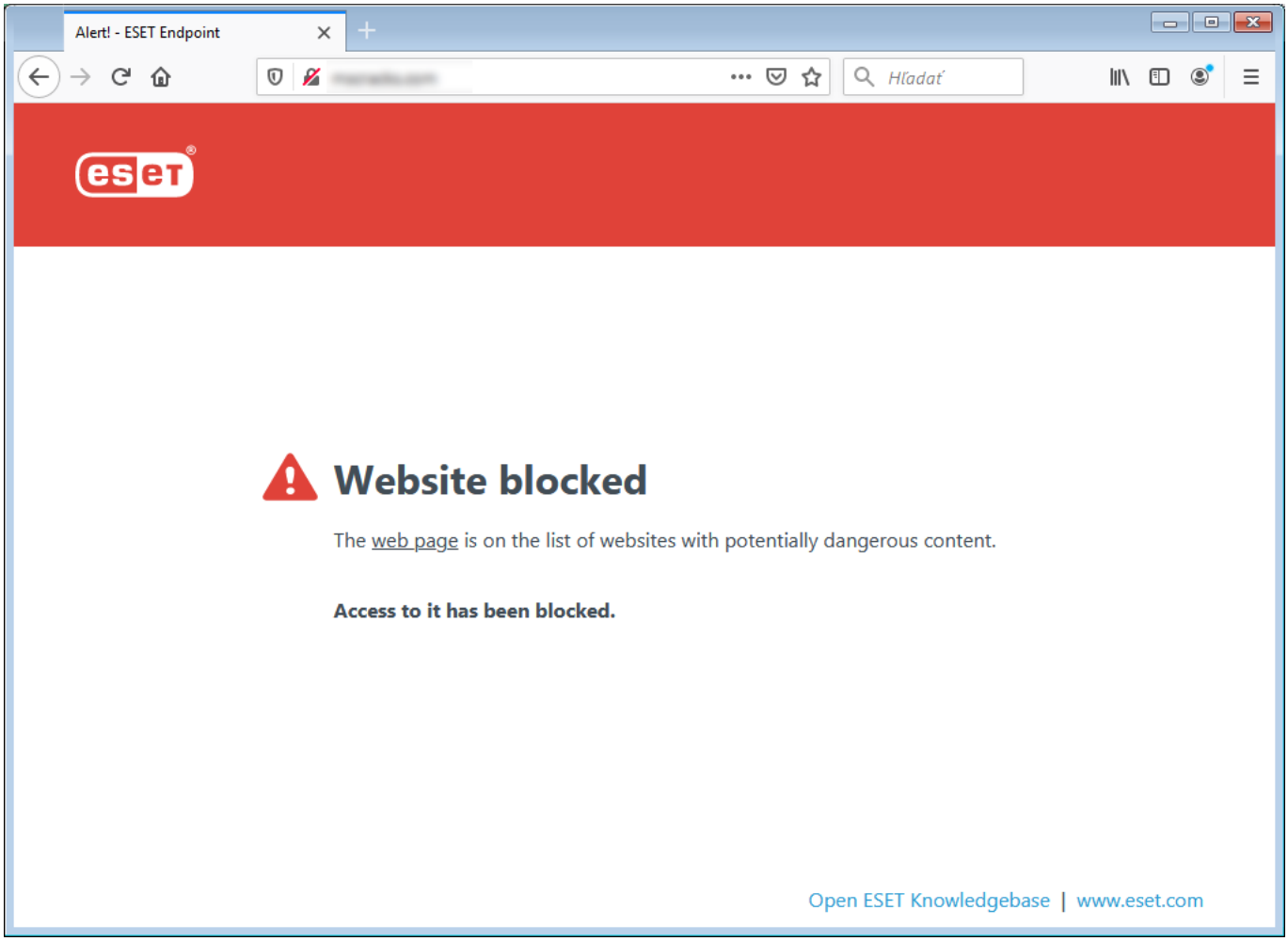
Enable Anti-Phishing protection—When enabled, phishing web pages are blocked. See Anti-Phishing protection for more information.

Excluded applications—Enables you to exclude specific applications from being scanned by Web access protection. Useful when Web access protection causes compatibility issues.

Excluded IPs—Enables you to exclude specific remote addresses from being scanned by Web access protection. Useful when Web access protection causes compatibility issues.



Web access protection will display the following message in your browser when the website is blocked:



The following ESET Knowledgebase article may only be available in English:
- Unblock a safe website on an individual workstation in ESET Endpoint Security

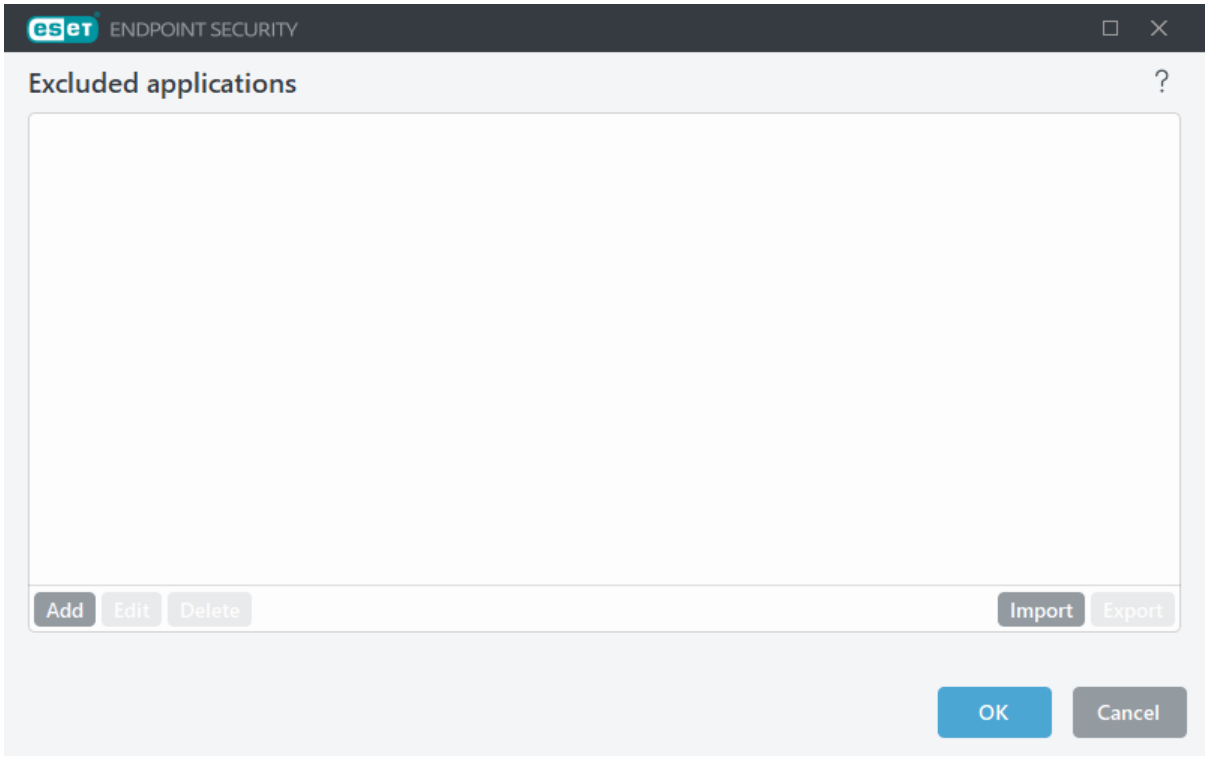
Excluded applications

To exclude scanning of communication for specific applications, add them to the list. HTTP(S)/POP3(S)/IMAP(S) communication of the selected applications will not be checked for threats. We recommend only using this for applications that do not work properly with their communication being scanned.

Running applications and services will be available here automatically when you click **Add**. Click **...** and navigate to an application to add exclusion manually.

Edit—Edit selected entries from the list.

Delete—Remove selected entries from the list.



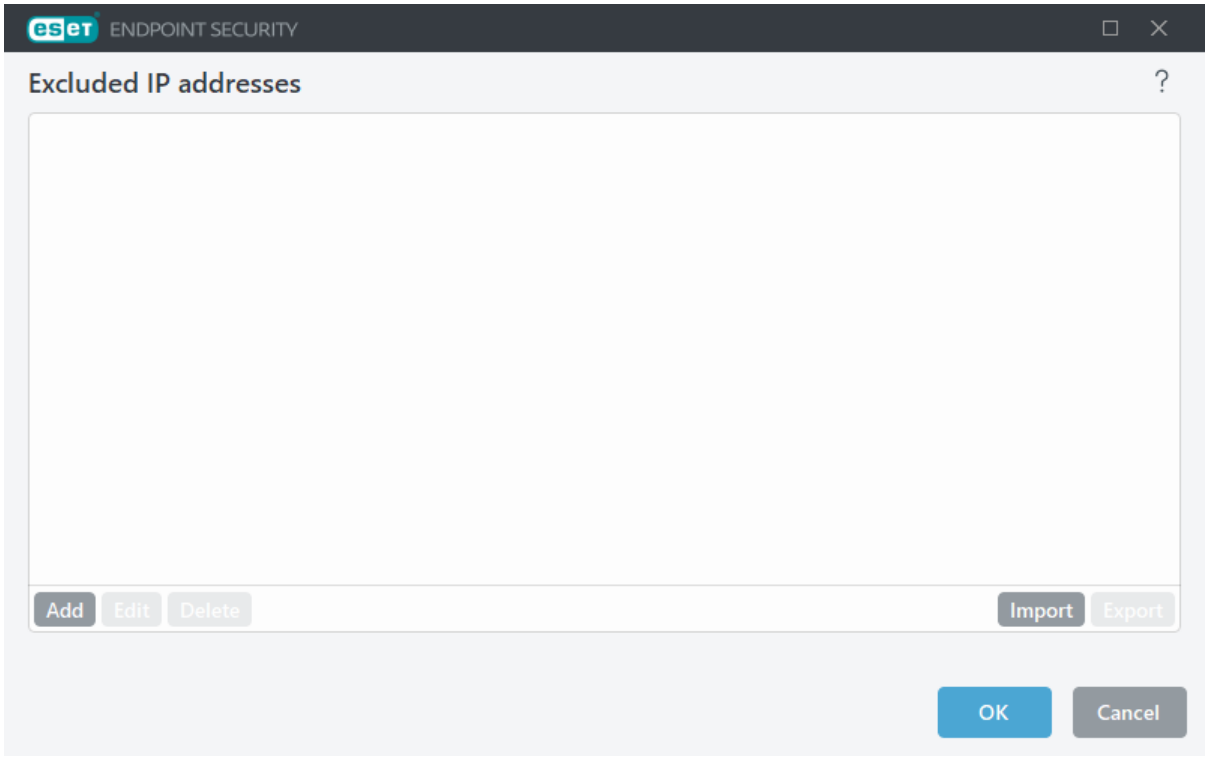
Excluded IPs

The entries in the list will be excluded from scanning. HTTP(S)/POP3(S)/IMAP(S) communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Add—Click to add an IP address/address range/subnet of a remote point to which a rule is applied.

Edit—Edit selected entries from the list.

Delete—Remove selected entries from the list.



IP addresses examples

Add IPv4 address:

Single address—Adds an IP address of an individual computer (for example, *192.168.0.10*).

Address range—Type the starting and ending IP addresses to specify the IP range of several computers (for example, *192.168.0.1-192.168.0.99*).

Subnet—Subnet (a group of computers) defined by an IP address and mask. For example, 255.255.255.0 is the network mask for the 192.168.1.0 subnet. To exclude the whole subnet type in *192.168.1.0/24*.

Add IPv6 address:

Single address—Adds the IP address of an individual computer (for example, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnet—Subnet (a group of computers) is defined by an IP address and mask (for example, *2002:c0a8:6301:1::1/64*).

URL list management

The **URL list management** in Advanced setup > **Protections** > **Web access protection** enables you to specify HTTP addresses to block, allow or exclude from content scan.

SSL/TLS must be enabled if you want to filter HTTPS addresses in addition to HTTP. Otherwise only the domains of HTTPS sites that you have visited will be added, the full URL will not be.

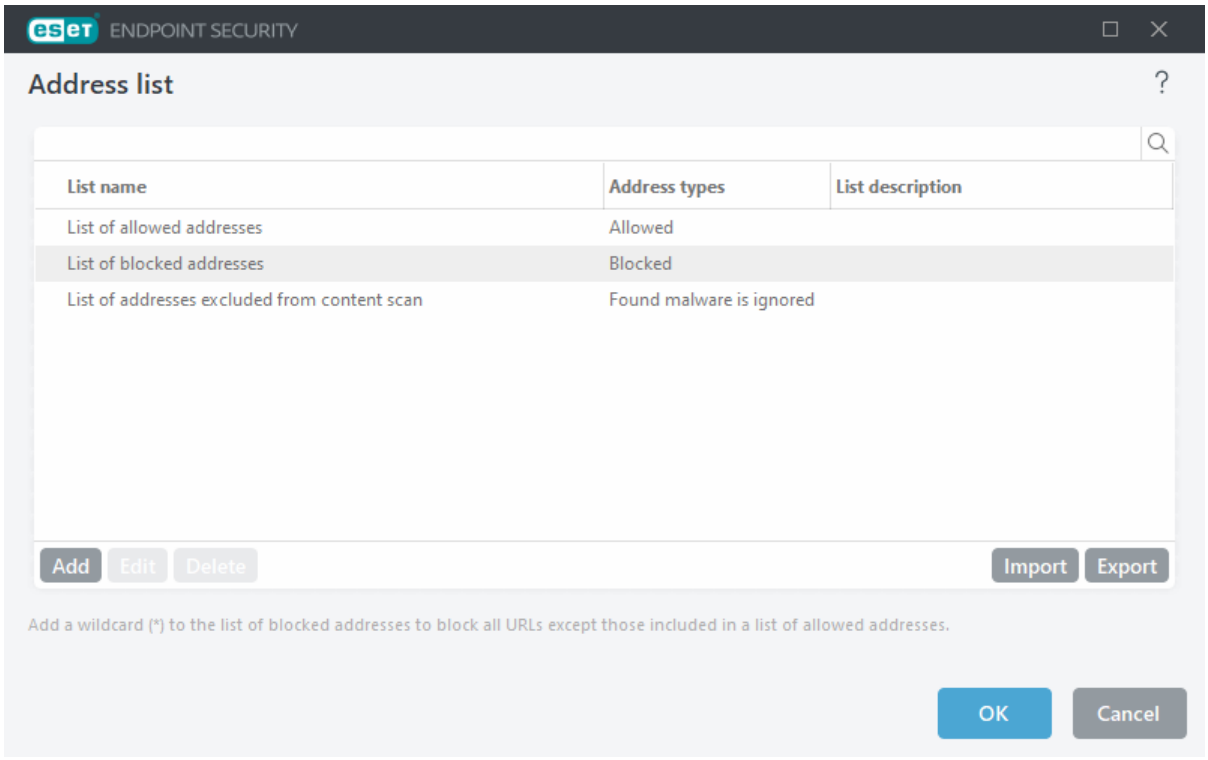
Websites in the **List of blocked addresses** will not be accessible unless they are also included in the **List of allowed addresses**. Websites in the **List of addresses excluded from content scan** are not scanned for malicious code when accessed.

If you want to block all HTTP addresses except addresses present in the active **List of allowed addresses**, add * to the active **List of blocked addresses**.

The special symbols * (asterisk) and ? (question mark) can be used in lists. The asterisk substitutes any character string, and the question mark substitutes any symbol. Pay attention when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and

? are used correctly in this list. See Add HTTP address / domain mask for how a whole domain including all subdomains can be matched safely. To activate a list, select **List active**. If you want to be notified when entering an address from the current list, select **Notify when applying**.

> **Addresses Trusted by ESET**
> If **Do not scan traffic with domains trusted by ESET** is enabled in SSL/TLS, domains on whitelist managed by ESET will not be affected by URL list management configuration.



Control elements

Add—Creates a new list in addition to the pre-defined ones. This can be useful if you want to logically split different groups of addresses. For example, one list of blocked addresses may contain addresses from an external public blacklist, and a second one may contain your own blacklist, making it easier to update the external list while keeping yours intact.

Edit—Modifies existing lists. Use this to add or remove addresses.

Delete—Deletes existing lists. Only available for lists created with **Add**, not for default lists.

Address list

In this section you can specify lists of HTTP(S) addresses that will be blocked, allowed or excluded from checking.

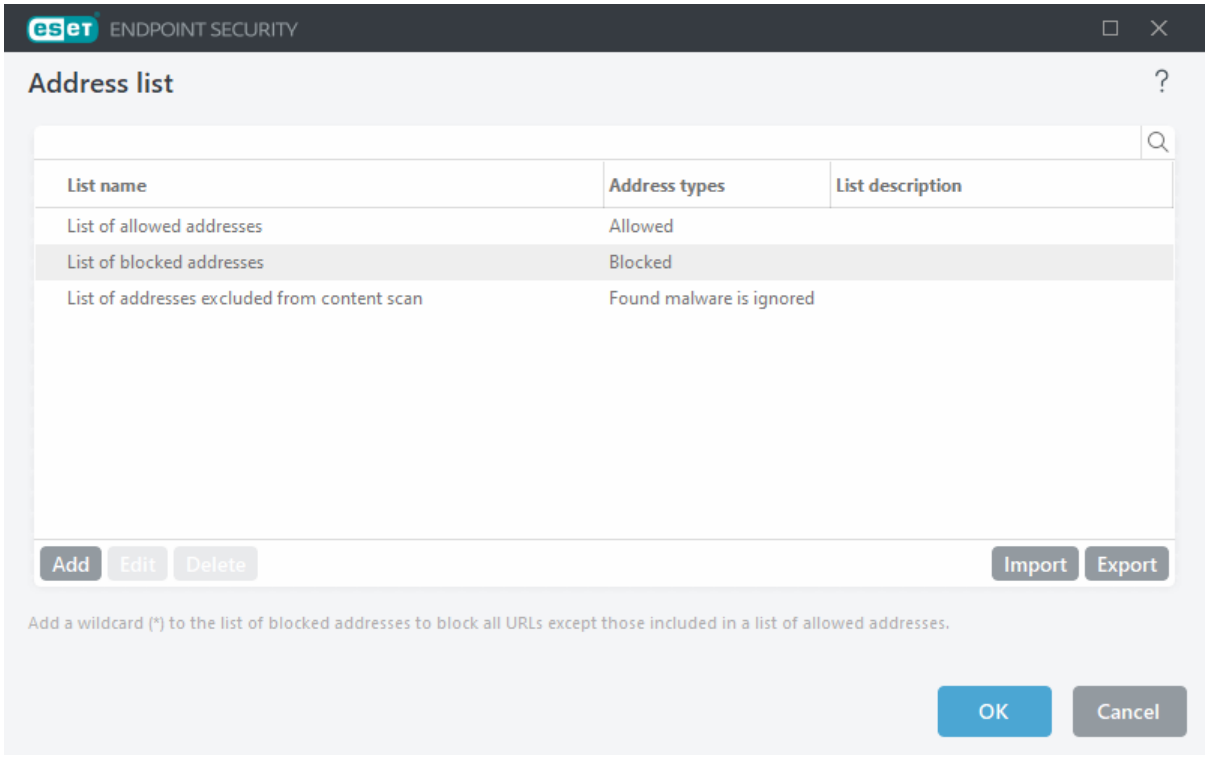
By default, the following three lists are available:

- **List of addresses excluded from content scan**—No checking for malicious code will be performed for any address added to this list.
- **List of allowed addresses**—If allow access only to HTTP addresses in the list of allowed addresses is enabled and the list of blocked addresses contains * (match everything), the user will be allowed to access addresses specified in this list only. The addresses in this list are allowed even if they are included in the list

of blocked addresses.

- **List of blocked addresses**—The user will not be allowed to access addresses specified in this list unless they also occur in the list of allowed addresses.

Click **Add** to create a new list. To delete selected lists, click **Delete**.



The following ESET Knowledgebase article may only be available in English:

- Unblock a safe website on an individual workstation in ESET Endpoint Security

For more information see URL address management.

Create new Address list

This dialog window enables you to configure a new list of URL addresses/masks that will be blocked, allowed or excluded from checking.

You can configure the following options:

Address list type—Three list types are available:

- **Found malware is ignored**—No checking for malicious code will be performed for any address added to this list.
- **Blocked**—Access to addresses specified in this list will be blocked.
- **Allowed**—Access to addresses specified in this list will be allowed. Addresses in this list are allowed even if they match the list of blocked addresses.

List name—Specify the name of the list. This field will be unavailable when editing one of the pre-defined lists.

List description—Type a short description for the list (optional). Unavailable when editing one of the pre-defined list.

To activate a list, select **List active** next to that list. If you want to be notified when a specific list is used when accessing websites, select **Notify when applying**. For example, you will receive a notification when a website is blocked or allowed because it is included in list of blocked or allowed addresses. The notification will contain the name of the list.

Logging severity—Select the Logging severity from the drop-down menu. Records with Warning verbosity can be collected by ESET PROTECT On-Prem.

Information and Warning logging verbosity is available only for rules which contain at least two components without wildcards within the domain. For example:
- *.domain.com/*
- *www.domain.com/*

Control elements

Add—Add a new URL address to the list (type multiple values with separator).

Edit—Modifies existing address in the list. Only available for addresses created with **Add**.

Delete—Deletes existing addresses in the list. Only available for addresses created with **Add**.

Import—Import a file with URL addresses (separate values with a line break, for example, *.txt using encoding UTF-8).

For information, see the How to add URL mask chapter.

How to add URL mask

See the instructions in this dialog before you type the desired address/domain mask.

ESET Endpoint Security enables you to block access to specified websites and prevent the internet browser from displaying their content. You can also specify addresses, which should be excluded from checking. If the complete name of the remote server is unknown, or the user wants to specify a whole group of remote servers, so called masks can be used to identify such a group. The masks include the symbols “?” and “*”:

- use ? to substitute a symbol
- use * to substitute a text string.

For example *.c?m applies to all addresses, where the last part begins with the letter c, ends with the letter m and contains an unknown symbol in between them (.com, .cam, etc.).

For instance, the mask *x? denotes any address with x as the last but one character. To match the whole domain, type it in the form **.domain.com/**. Specifying protocol prefix *http://*, *https://* in the mask is optional. If omitted, the mask will match any protocol. A leading "*." sequence is treated specially if used at the beginning of domain name. First, the * wildcard does not match the slash character ('/') in this case. This is to avoid circumventing the mask, for example the mask **.domain.com* will not match *http://anydomain.com/anypath#.domain.com* (such suffix can be appended to any URL without affecting the download). And second, the "*." also matches an empty string in this special case. This is to allow matching whole domain including any subdomains using a single mask. For example the mask **.domain.com* also matches *http://domain.com*. Using **domain.com* would be incorrect, as that would also match *http://anotherdomain.com*.

Information and Warning logging verbosity is available only for rules which contain at least two components without wildcards within the domain. For example:
- *.domain.com/*
- *www.domain.com/*

HTTP(S) traffic scanning

By default, ESET Endpoint Security is configured to scan the HTTP and HTTPS traffic which is used by internet browsers and other applications. You should disable the traffic scanning only if you are experiencing problems with a 3rd party software and want to know if the issue is caused by ESET Endpoint Security.

Enable HTTP traffic scanning—HTTP traffic is always monitored on all ports for all applications.

Enable HTTPS traffic scanning—HTTPS traffic uses an encrypted channel to transfer information between server and client. ESET Endpoint Security checks communication utilizing the SSL (Secure Socket Layer) and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by HTTPS protocol**, regardless of operating system version (you can add ports to the pre-defined 443 and 0-65535).

ThreatSense

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options enable you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense** in the Advanced setup for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section enables you to define which computer components and files will be scanned for infiltrations.

Operating memory—Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI—Scans boot sectors for the presence of malware in the master boot record. Read more about UEFI in the glossary.

Email files—The program supports the following extensions: DBX (Outlook Express) and EML.

Archives—The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives—Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers—After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics—A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist or was not covered by the previous versions of the detection engine module. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures—Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of ESET Endpoint Security while cleaning objects.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine setup for a On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS)—Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by

disguising themselves as alternate data streams.

Run background scans with low priority—Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects—The Scan log will show all the scanned files in self-extracting archives, even those not infected (may generate a lot of scan log data and increase the scan log file size).

Enable Smart optimization—With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the specific modules are applied when performing a scan.

Preserve last access timestamp—Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

Limits

The Limits section enables you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size—Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited.

Maximum scan time for object (sec.)—Defines the maximum time value for the scan of files in a container object (such as a RAR/ZIP archive or an email with multiple attachments). This setting does not apply for standalone files. If a user-defined value has been typed and that time has elapsed, a scan will stop as soon as possible, regardless of whether the scan of each file in a container object has finished. In the case of an archive with large files, the scan will stop no sooner than a file from the archive is extracted (for example, when a user-defined variable is 3 seconds, but the extraction of a file takes 5 seconds). The rest of the files in the archive will not be scanned when that time has elapsed. To limit scanning time, including bigger archives, use **Maximum object size** and **Maximum size of file in archive** (not recommended due to possible security risks). Default value: unlimited.

Archive scan setup

Archive nesting level—Specifies the maximum depth of archive scanning. Default value: 10.

Maximum size of file in archive—This option enables you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. The maximum value is 3 GB.

> We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

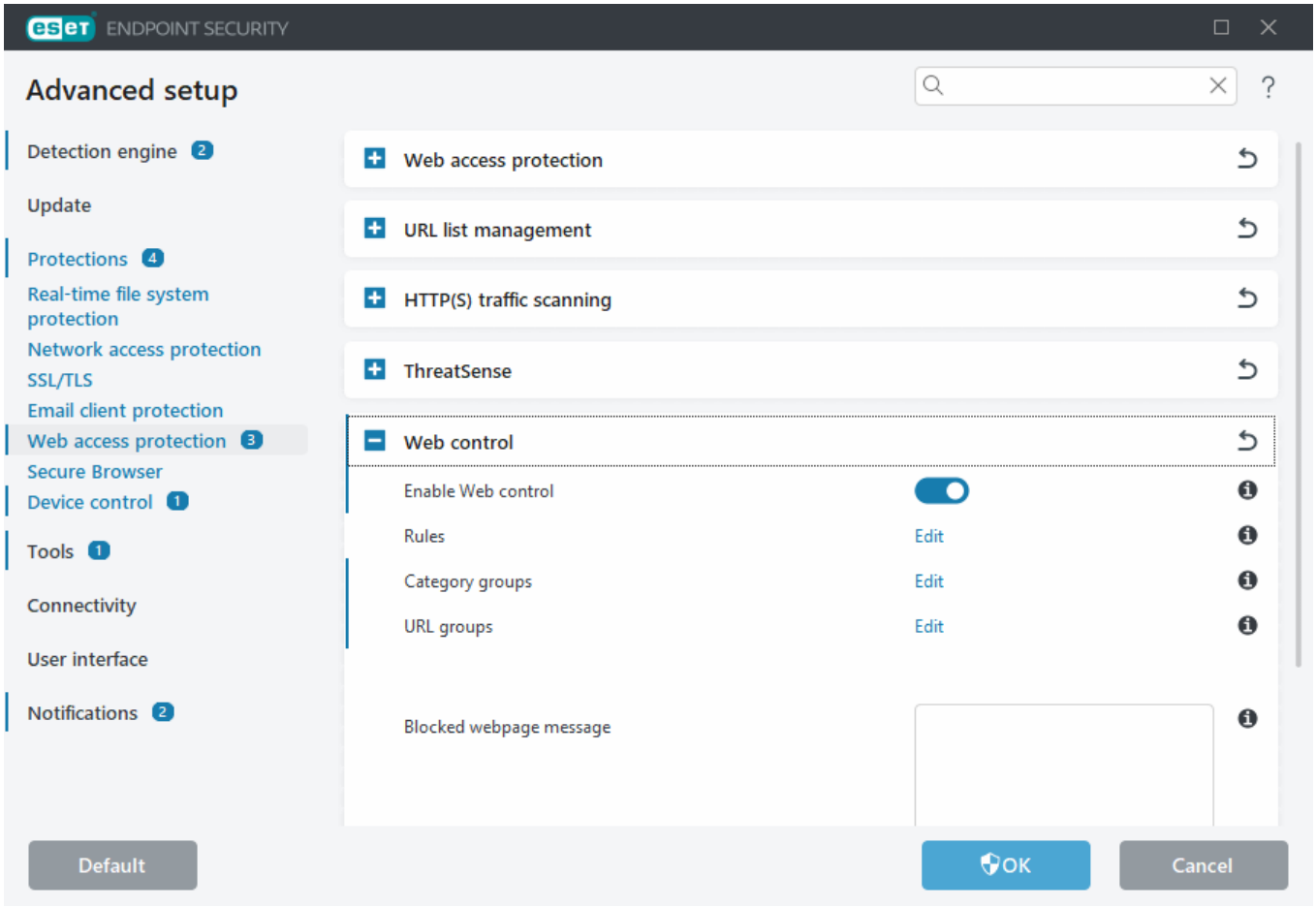
Web control

The Web control section enables you to configure settings that protect your company from risk of legal liability. Web control can regulate access to websites that violate intellectual property rights. The goal is to prevent employees from accessing pages with inappropriate or harmful content, or pages that may have a negative impact on productivity.

Web control enables you to block web pages that may contain potentially offensive material. In addition, employers or system administrators can prohibit access to more than 27 pre-defined website categories and over 140 subcategories.

By default, Web control is disabled. To activate Web control:

1. Open Advanced setup > **Protections** > **Web access protection** > **Web control**.
2. Enable the **Enable Web control** toggle to activate Web control in ESET Endpoint Security.
3. Configure access to specific web pages. Click **Edit** next to **Rules** to access the Web control rules editor window.

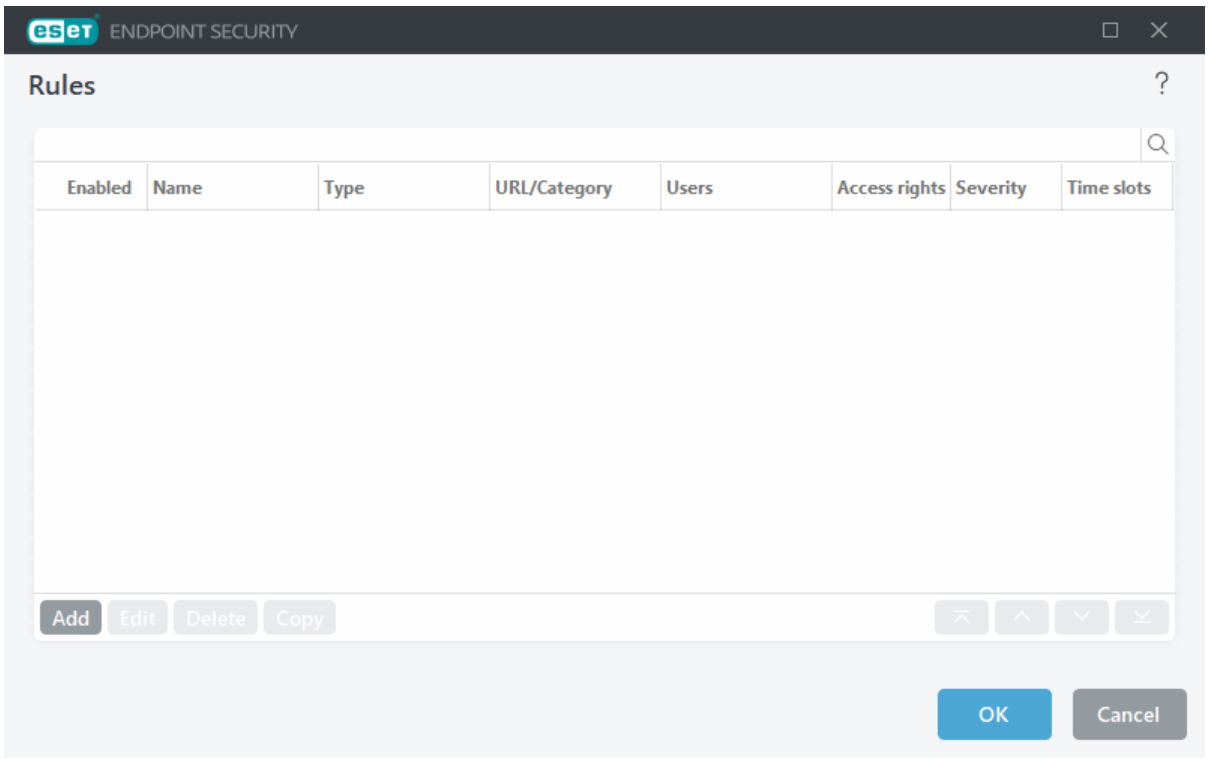


Blocked webpage message and **Blocked webpage graphic** fields enable you to customize the displayed message when a website is blocked.

If you want to block all web pages and leave only certain available, use URL address management.

Web control rules

The **Rules** editor window displays existing URL-based or Category-based rules.



The list of rules contains several descriptions of rules such as name, type of blocking, action to perform after matching a Web control rule and log severity.

Click **Add** or **Edit** to manage a rule. Click **Copy** to create a new rule with pre-defined options used for another selected rule. By pressing **Ctrl** and clicking, you can select multiple rules and delete all selected rules. The **Enabled** check box disables or enables a rule; this can be useful if you do not want to delete a rule permanently because it might be used in the future.

Rules are sorted in the order determining their priority, with higher priority rules on top. To change the priority of a rule, select the rule and click the arrow button to increase or decrease the rule priority. Click the double arrow to move the rule to the top or bottom of the list.

See also creating rules.

Adding Web control rules

The Web control rules window enables you to create or modify an existing Web control filtering rule manually.

Name

Type a description of the rule into the **Name** field for better identification.

Enabled

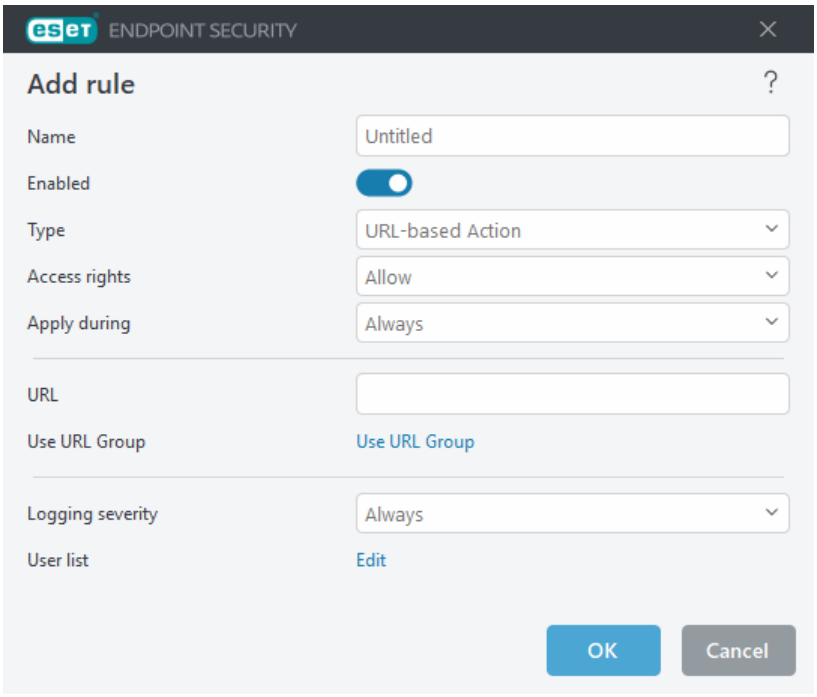
Click the **Enabled** switch to disable or enable the rule; this can be useful if you do not want to delete the rule permanently.

Action

Choose between **URL-based Action** or **Category-based Action**:

URL-based Action

For rules that control access to a given website, type the URL in the **URL** field.
The special symbols * (asterisk) and ? (question mark) cannot be used in the URL address list. When creating a URL group that contains a website with multiple top-level domains (TLDs), each TLD must be added separately. If you add a domain to the group, all content located on this domain and all subdomains (for example, *sub.examplepage.com*) will be blocked or allowed based on your choice of URL-based action.
URL or **Use URL Group**—Define the URL link or URL group of links to allow, block or warn the user when one of these URLs is accessed.



Category-based Action

The rule will be applied based on a website category.
URL Category or **Use Group**—Select the website category or a Group of categories to allow, block or warn the user when one of the categories is detected.

Access rights

- **Allow**—Access to the URL address/category is allowed.
- **Warn**—Blocks access to the URL address/category. You can click **Go Back** to return to the previous website or click **Continue** to access the website. If you click **Continue**, the blocking page will not be displayed the next time you visit the website.
- **Warn always**—Blocks access to the URL address/category. You can click **Go Back** to return to the previous website or click **Continue** to access the website. The blocking page will be displayed each time you visit the

website.

- **Block**—Blocks access to the URL address/category. You can click **Go Back** to return to the previous website.

Apply during

Enables you to apply the created rule during a certain time. Select created time slot from the **Apply during** drop-down menu. More information about Time slots.

Logging severity

- **Always** —Logs all online communications.
- **Diagnostic**—Logs information needed to fine-tune the program.
- **Information**—Records informative messages, including successful update messages, plus all records above.
- **Warning**—Records critical errors and warning messages.
- **None**—No logs will be created.

> The Logging severity can be configured separately for each list. Logs with **Warning** status can be collected by ESET PROTECT On-Prem.

User list

- **Add**—Opens the **Select Users or Groups** dialog window to select desired users. When no user is selected, the rule is applied to all users.
- **Delete**—Removes the selected user from the filter.

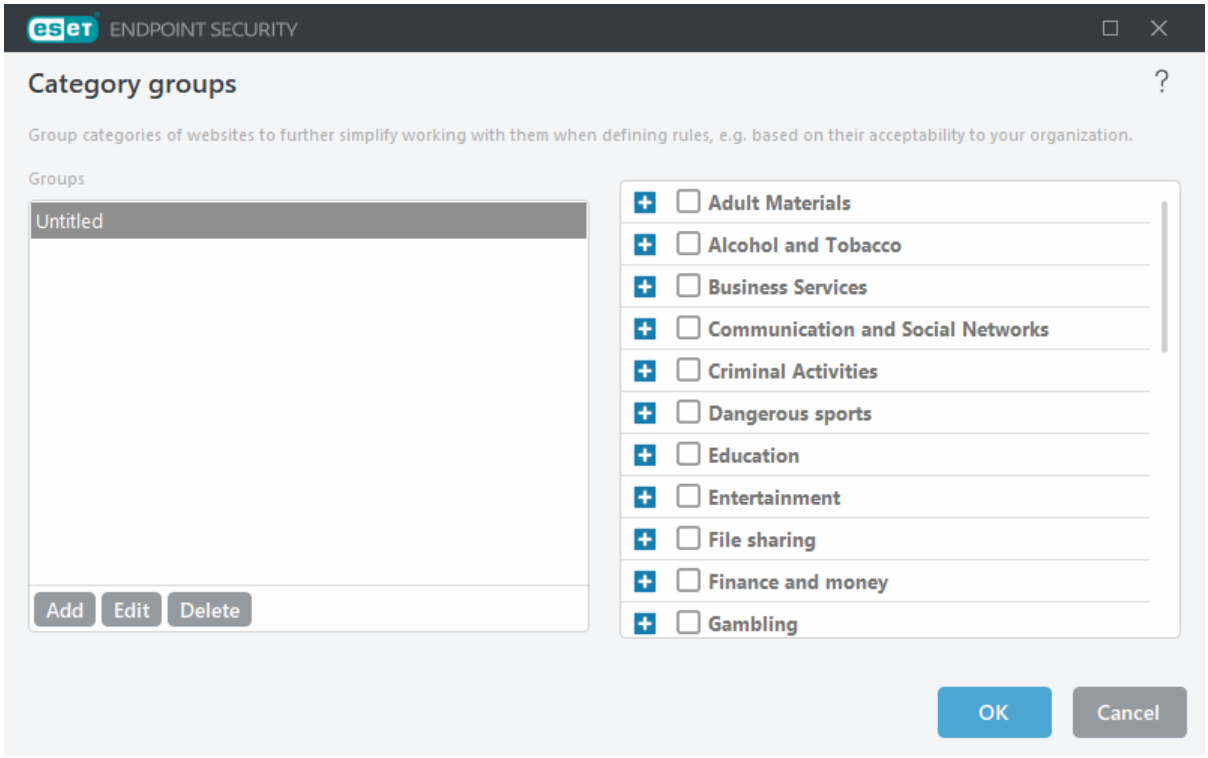
Category groups

The Category groups window is divided into two parts. The left part of the window contains a list of Category groups.

- **Add**—Click to create a new Category group.
- **Edit**—Click to edit an existing Category group.
- **Remove**—Select and click if you want to remove an existing Category group from the list of Category groups.

The right part of the window contains a list of categories and subcategories. Select a category in the Category list to display its subcategories. Each group contains adult and/or generally inappropriate subcategories as well as categories considered generally acceptable. When you open the Category groups window and click the first group, you can add or remove categories/subcategories from the list of appropriate groups (for example Violence or Weapons). Web pages with inappropriate content can be blocked and users can be informed when accessing a blocked web page.

Select the check box to add or remove a subcategory to a specific group.



Here are some examples of categories that users might not be familiar with:

- **Miscellaneous**—Usually private (local) IP addresses such as intranet, 192.168.0.0/16, etc. When you get a 403 or 404 error code, the website will also match this category.
- **Not resolved**—This category includes web pages that are not resolved because of an error when connecting to the Web control database engine.
- **Not categorized**—Unknown web pages that are not yet in the Web control database.
- **Proxies**—Web pages such as anonymizers, redirectors or public proxy servers can be used to obtain (anonymous) access to web pages that are usually prohibited by the Web control filter.
- **File sharing**—These web pages contain large amounts of data such as photos, videos or e-books. There is a risk that these sites contain potentially offensive material or adult content.

You can report a wrong categorization of an URL.

A subcategory can belong to any group. There are some subcategories that are not included in pre-defined groups (for example, Games). To match a desired subcategory using Web control filter, add it to your desired group.

URL groups

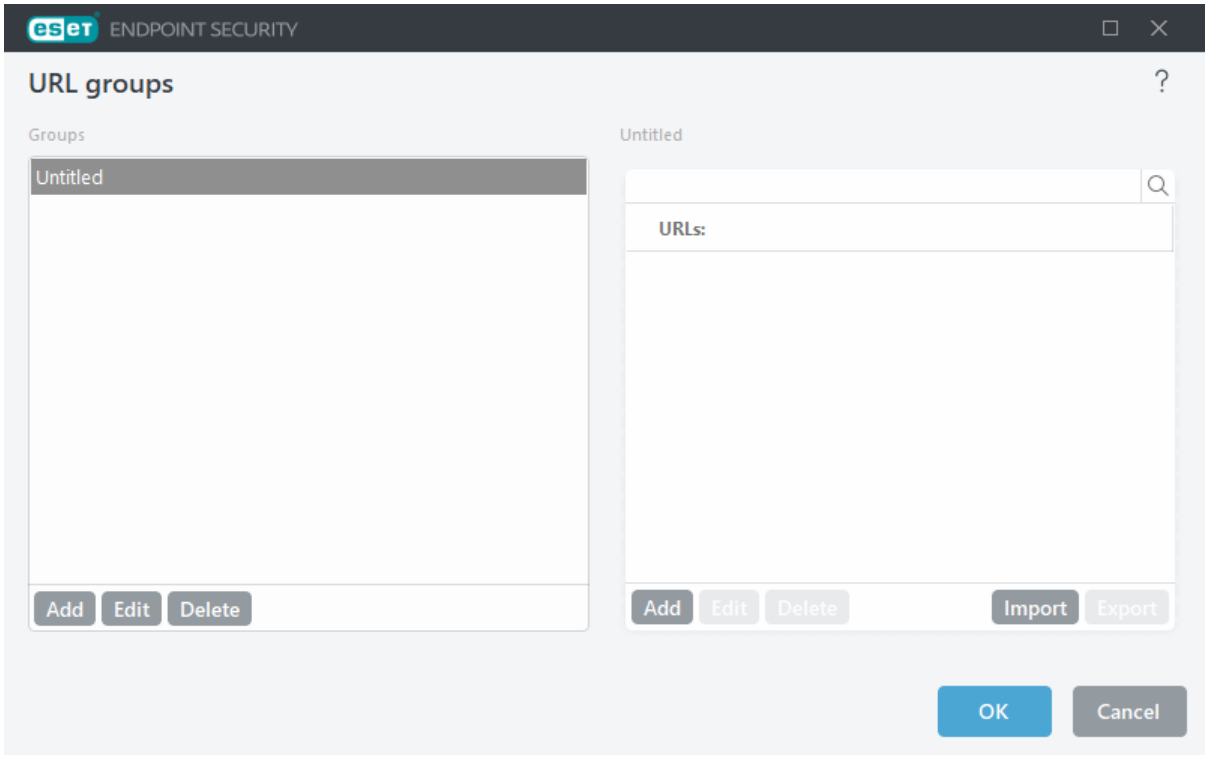
URL groups enable you to create a group that contains several URL links for which you want to create a rule (allow/block a specific website).

Create a new URL group

To create a new URL group click **Add** and type the name of new URL group.

Using a URL group can be useful when the administrator wants to create a rule for more web pages (blocked or allowed based on your choice).

Add URL addresses to the URL group list - manually



To add a new URL address to the list select a URL group and click **Add** in the bottom right of the window.

The special symbols * (asterisk) and ? (question mark) cannot be used in the URL address list.

It is not necessary to type the full name of domain with http:// or https://.

If you add a domain to the group, all content located on this domain and all subdomains (for example, *sub.examplepage.com*) will be blocked or allowed based on your choice of URL-based action.

If there is a conflict between two rules in the meaning of the first rule blocks the domain, and the second rule allows the same domain, the specific domain or IP address will be blocked anyway. For more information on creating rules see URL-based Action.

Add URL addresses to the URL group list - import using a .txt file

Click **Import** to import a file with a list of URL addresses (separate values with a line break, for example .txt file using encoding UTF-8). The special symbols * (asterisk) and ? (question mark) cannot be used in the URL address list.

Using URL groups in Web control

If you want to set an action to be performed for a specific URL group, open the Web control rules editor, select your URL group using the drop-down menu, adjust other parameters and then click **OK**.

Blocking or allowing a specific web page can be more accurate than blocking or allowing a whole category of web pages. Be careful when changing these settings and adding a category/web page to the list.

Blocked webpage message customization

Blocked webpage message and **Blocked webpage graphic** fields enable you to easily customize the displayed message when a website is blocked.

Usage

Let's block the "Weapons" website category.

An example of a blocked web page message would be:

```
The webpage %URL_OR_CATEGORY% was blocked because it is considered inappropriate or
 with harmful content.
Please contact your administrator for details.
```

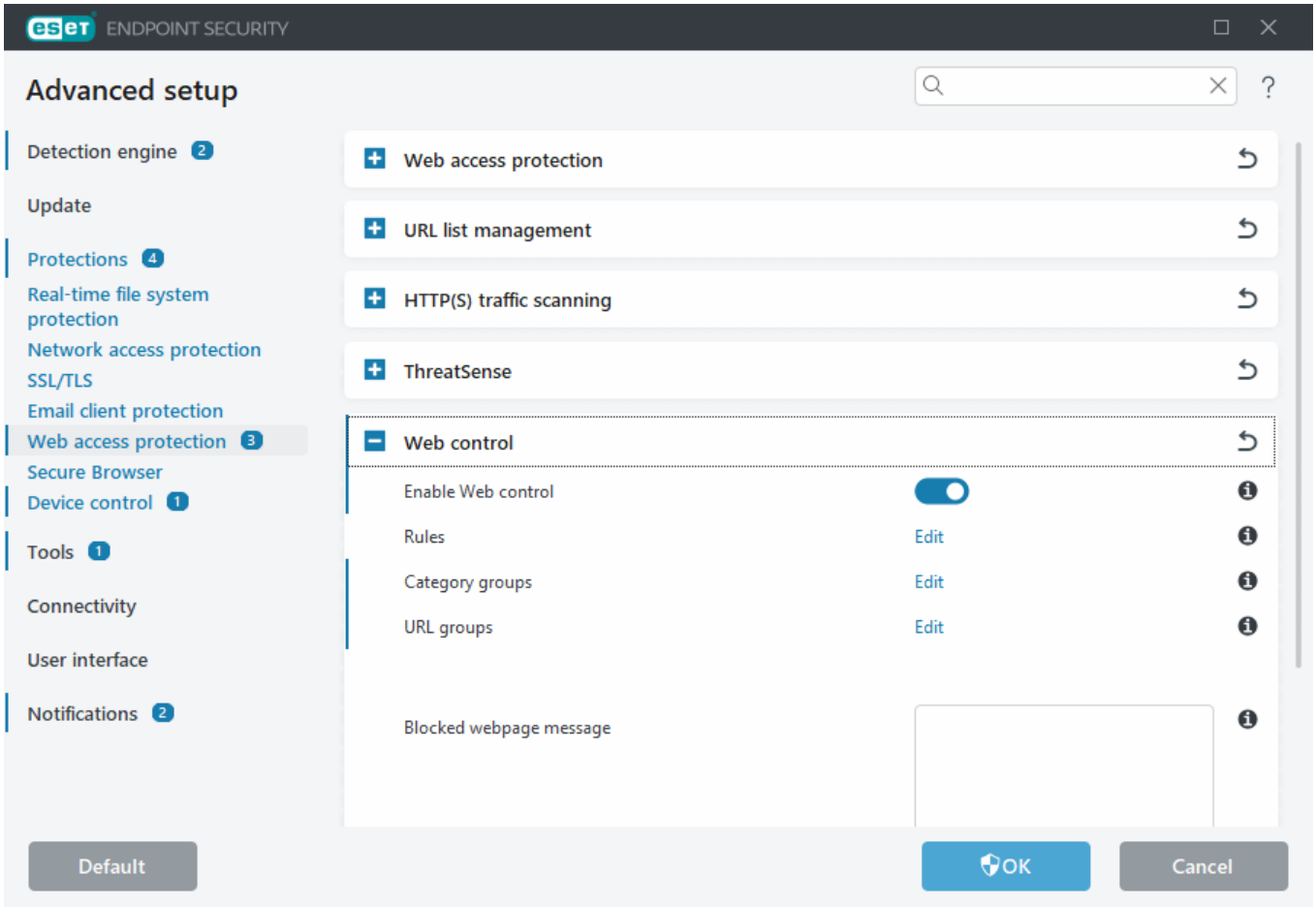
Variable	Description
%CATEGORY%	Blocked Web control category.
%URL_OR_CATEGORY%	Blocked Web control website or category (depends on the Web control blocking rule).
%STR_GOBACK%	"Go Back" button value.
%product_name%	Name of the ESET product (ESET Endpoint Security)
%product_version%	Version of the ESET product.

An example of a blocked web page graphics URL will be:

```
https://www.example.com/blocked_web_graphics.png
```

The image size (width/height) will scale automatically if the size is too high.

The configuration in ESET Endpoint Security will look like:



Dialog window - Web control

The main functionality of Web control is to control the websites accessed for each user in the company network. The network administrator must be able to define the categories of websites that users will be able to access, either by user or by user group. Integration with directory services will allow the use of Active Directory groups for web control configuration. By default, this functionality is disabled. If you want to enable this feature, set **Enable Web control** to on. Click **Edit** to access the Rules editor. Click **Edit** next to Category groups to modify pre-defined groups or click **Edit** next to URL groups editor to add new URL group.

Secure Browser

Secure Browser is an additional layer of protection designed to protect your financial data during online transactions.

ESET LiveGrid® reputation system must be enabled (enabled by default) to ensure that Secure Browser protection works properly.

To configure the Secure Browser behavior, open Advanced setup > **Protections** > **Secure Browser**.

You can use the following Secure Browser configuration option:

- **Secure all browsers**—All supported web browsers start in a secure mode. This enables you to browse the internet, access internet banking, and make online purchases and transactions in one secured browser window without redirection.

Basic

Browser protection

Secure all browsers—Start all supported web browsers in a secure mode. This enables you to browse the internet, access internet banking, and make online purchases and transactions in one secure browser window without redirection.

Extension installation mode—From the drop-down menu, you can select which extensions will be allowed to be installed on a browser secured by ESET. Changing the Extension installation mode does not affect previously installed browser extensions:

- **Essential extensions**—Only the most essential extensions, developed by a specific browser manufacturer.
- **All extensions**—All extensions supported by a specific browser.

Secured browser

Enhanced memory protection—If enabled, the secure browser memory will be protected from inspection by other processes.

Keyboard protection—If enabled, information typed via the keyboard into a secure browser will be hidden from other applications. This increases protection against keyloggers.

Browser's green frame—If disabled, the informative in-browser notification and the green frame around the browser will be hidden.

Configure Secure Browser interactive alerts—Enables you to open the Interactive alerts window.

> In some situations, a specific interactive alert shows only when there is an error in starting Secure Browser properly. For more information, see Interactive alerts.

In-browser notification

Secured browser informs you about its current status through in-browser notifications and the color of the browser frame.

In-browser notifications are shown in the tab on the right side.

To expand the in-browser notification, click the ESET icon. To minimize the notification, click the notification text. To dismiss the notification and the green browser frame, click the close icon.

> Only the Informative notification and green browser frame can be dismissed.

In-browser notifications

Notification type	Status
Informative notification and green browser frame	Maximum protection is ensured and the in-browser notification is minimized by default.
Warning and orange browser frame	Secured browser requires your attention for a non-critical issue. For more information about the issue or a solution, follow the instructions in the in-browser notification.
Security alert and red browser frame	The browser is not protected. Restart the browser to ensure the protection is active. To resolve a conflict with files loaded in the browser, open Log files > **Secure browser** and ensure the logged files are not loaded the next time you start the browser. If the issue persists, contact ESET Technical Support by following the instructions in our Knowledgebase article.

Device control

ESET Endpoint Security provides automatic device (CD/DVD/USB/etc.) control. You can block or adjust extended filters/permissions and define a user's ability to access and work with a given device. This may be useful if the computer administrator wants to prevent using devices containing unsolicited content.

Supported external devices:

- Disk Storage (HDD, USB removable disk)
- CD/DVD
- USB Printer
- FireWire Storage
- Bluetooth Device
- Smart card reader
- Imaging Device
- Modem
- LPT/COM port
- Portable Device (battery-powered devices such as media players, smartphones, plug-and-play devices, etc.)
- All device types

Device control setup options can be modified in Advanced setup > **Protections** > **Device control**.

Click the **Enable Device control** toggle to enable the Device control feature in ESET Endpoint Security; you must restart your computer for this change to take effect. After enabling Device control, you can define the **Rules** in the Rules editor window.

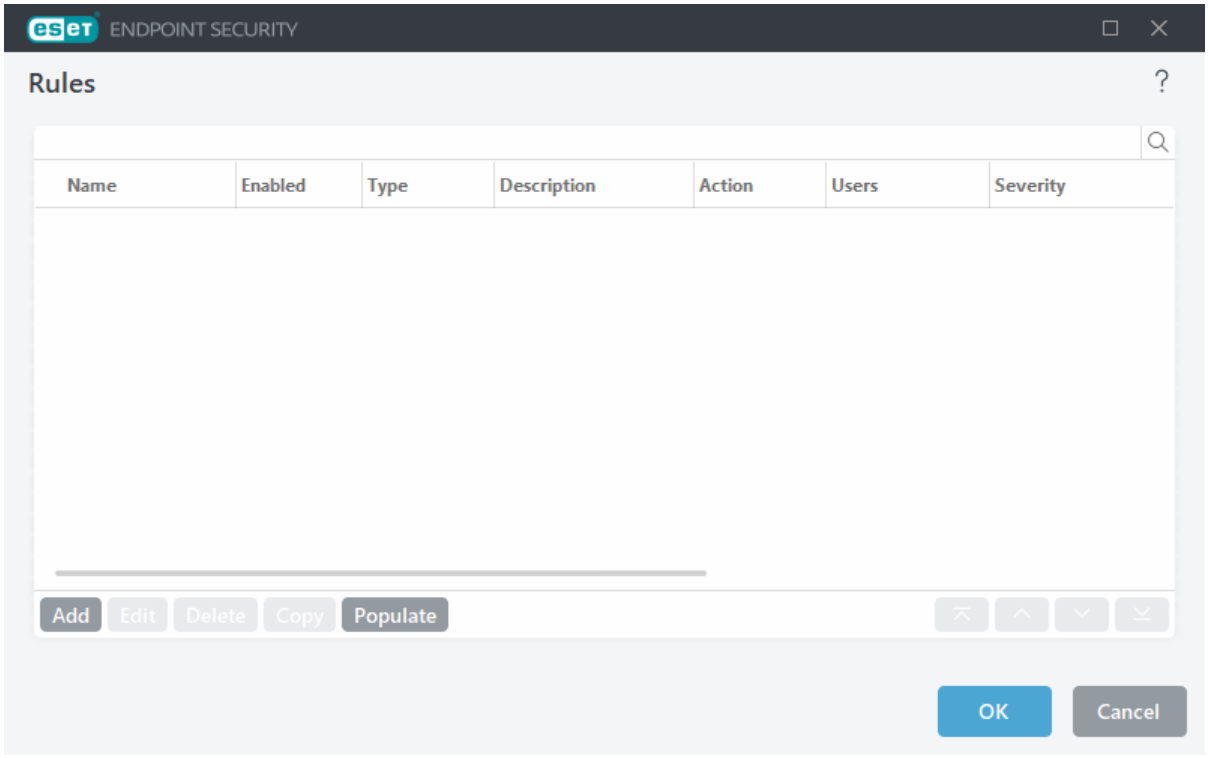
> You can import a Device control group with rules from an xml file using the scheduler. For more information and a step-by-step guide, see our ESET Knowledgebase article.

If a device blocked by an existing rule is inserted, a notification window will be displayed and access to the device will not be granted.

Device control rules editor

The **Device control rules editor** window displays existing rules and allows for precise control of external devices that users connect to the computer. See also Adding Device control rules.

> The following ESET Knowledgebase article may only be available in English:
> Add and modify Device control rules using ESET endpoint products



Specific devices can be allowed or blocked according to their user, user group, or any of several additional parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as name, type of external device, action to perform after connecting an external device to your computer and log severity.

Click **Add** or **Edit** to manage a rule. Deselect the **Enabled** check box next to a rule to disable it until you want to use it in the future. Select one or more rules and click **Delete** to delete the rule(s) permanently.

Copy—Creates a new rule with pre-defined options used for another selected rule.

Click **Populate** to auto-populate removable media device parameters for devices connected to your computer.

Rules are listed in order of priority with higher-priority rules closer to the top. Rules can be moved by clicking  **Top/Up/Down/Bottom** and can be moved individually or in groups.

The Device control log records all occurrences where Device control is triggered. Log entries can be viewed from the main program window of ESET Endpoint Security in **Tools** > **Log files**.

Detected devices

The **Populate** button provides an overview of all currently connected devices with information about device type, vendor, model and serial number (if available).

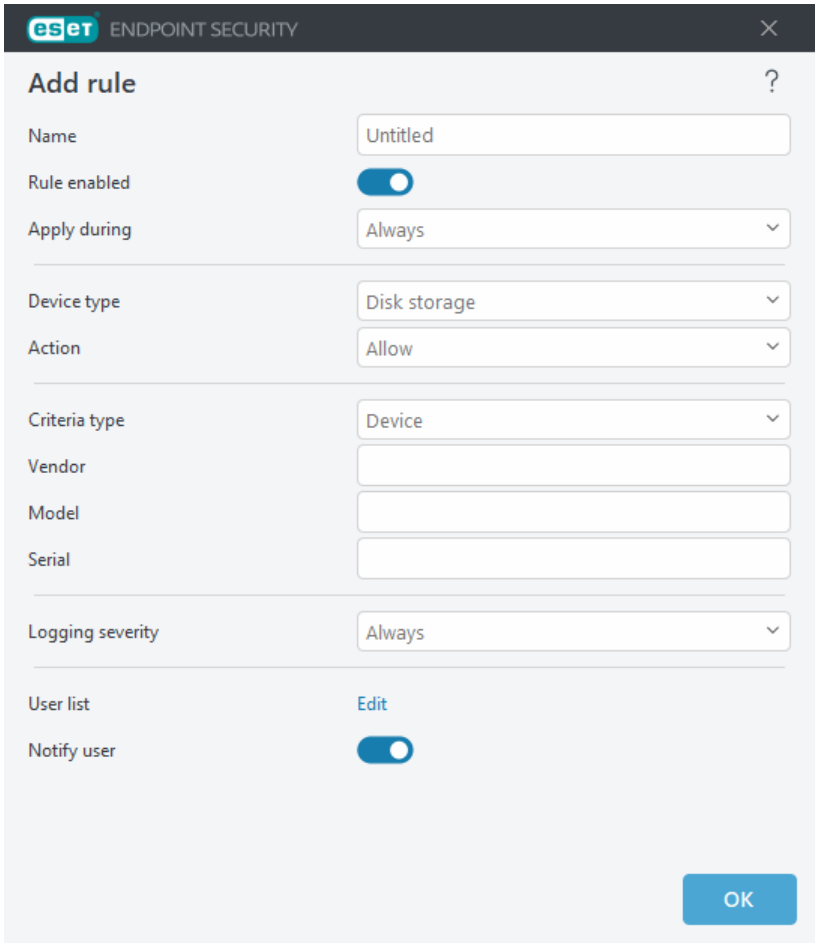
Select a device from the list of Detected devices and click **OK** to add a device control rule with pre-defined information (all settings can be adjusted).

Devices in low power (sleep) mode are marked with a warning icon. To enable the **OK** button and add a rule for this device:

- Reconnect the device.
- Use the device (for example, start the Camera app in Windows to wake up a webcam).

Adding Device control rules

A Device control rule defines an action to take when a device meeting the rule criteria is connected to the computer.



Type a description of the rule into the **Name** field for better identification. Click the toggle next to **Rule enabled** to disable or enable this rule; this can be useful if you do not want to delete the rule permanently.

Apply during—Enables you to apply created rule during the certain time. From the drop-down menu, select created time slot. See more information about Timeslots.

Device type

Choose the external device type from the drop-down menu (Disk storage/Portable device/Bluetooth/FireWire/...). Device type information is collected from the operating system and can be seen in the system Device manager if a device is connected to the computer. Storage devices include external disks or conventional memory card readers connected via USB or FireWire. Smart card readers include all readers of smart cards with an embedded integrated circuit, such as SIM cards or authentication cards. Examples of imaging devices are scanners or cameras. Because these devices only provide information about their actions and do not provide information about users, they can only be blocked globally.

> The user list functionality is not available for the modem device type. The rule will be applied for all users and the current user list will be deleted.

Action

Access to non-storage devices can either be allowed or blocked. In contrast, rules for storage devices enable you to select one of the following rights settings:

- **Allow**—Full access to the device will be allowed.
- **Block**—Access to the device will be blocked.
- **Write Block**—Only read access to the device will be allowed.
- **Warn**—Each time that a device is connected, the user will be notified if it is allowed/blocked, and a log entry will be made. Devices are not remembered, a notification will still be displayed for subsequent connections of the same device.

Note that not all Actions (permissions) are available for all device types. If it is a device of storage type, all four Actions are available. For non-storage devices, there are only three Actions available (for example **Write Block** is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).

Criteria type

Select **Device group** or **Device**.

Additional parameters shown below can be used to fine-tune rules for different devices. All parameters are case-sensitive and support wildcards (*, ?):

- **Vendor**—Filter by vendor name or ID.
- **Model**—The given name of the device.
- **Serial**—External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

> If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-sensitive and support wildcards (a question mark (?) represents a single character, whereas an asterisk (*) represents a string of zero or more characters).

> To view information about a device, create a rule for that type of device, connect the device to your computer and then check the device details in the Device control log.

Logging Severity

- **Always**—Logs all events.
- **Diagnostic**—Logs information needed to fine-tune the program.
- **Information**—Records informative messages, including successful update messages, plus all records above.
- **Warning**—Records critical errors and warning messages and sends them to ERA Server.
- **None**—No logs will be recorded.

Rules can be limited to certain users or user groups by adding them to the **User list**:

- **Add**—Opens the **Object types: Users or Groups** dialog window that enables you to select desired users.
- **Delete**—Removes the selected user from the filter.

> **User list limitations**
> The User list cannot be defined for rules with specific Device types:
> • USB Printer
> • Bluetooth device
> • Smart card reader
> • Imaging device
> • Modem
> • LPT/COM port

Notify user—If a device blocked by an existing rule is inserted, a notification window will be displayed.

Device groups

> A device connected to your computer may pose a security risk.

The Device groups window is divided into two parts. The right part of the window contains a list of devices belonging to the respective group, and the left part contains created groups. Select a group to display devices in the right pane.

When you open the Device groups window and select a group, you can add or remove devices from the list. Another way to add devices to the group is to import them from a file. Alternatively, you can click **Populate** button, and all devices connected to your computer will be listed in the **Detected devices** window. Select devices from the populated list to add them to the group by clicking **OK**.

Control elements

Add—You can add a group by entering its name or a device to an existing group, depending on which part of the window you clicked the button.

Edit—You can modify the name of the selected group or device's parameters (vendor, model, serial number).

Delete—Deletes the selected group or device depending on which part of the window you clicked on the button.

Import—Imports a list of devices from a text file. Importing devices from a text file requires correct formatting:

- Each device starts at a new line.
- **Vendor**, **Model**, and **Serial** must be present for each device and separated with a comma.

Here is an example of the text file content:
```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Export—Exports a list of devices to a file.

The **Populate** button provides an overview of all currently connected devices with information about device type, vendor, model and serial number (if available).

You can import a Device control group with rules from an xml file using the scheduler. For more information and a step-by-step guide, see our ESET Knowledgebase article.

Add device

Click Add in the right window to add a device to an existing group. Additional parameters shown below can be used to fine-tune rules for different devices. All parameters are case-sensitive and support wildcards (*, ?):

- **Vendor**—Filter by vendor name or ID.
- **Model**—The given name of the device.
- **Serial**—External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.
- **Description**—Your description of the device for better organization.

If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-sensitive and support wildcards (a question mark (?) represents a single character, whereas an asterisk (*) represents a string of zero or more characters).

Click **OK** to save the changes. Click **Cancel** if you want to leave the **Device groups** window without saving changes.

After creating a device group, you have to add a new device control rule for the created device group and choose the action to take.

Note that not all Actions (permissions) are available for all device types. If it is a device of storage type, all four Actions are available. For non-storage devices, there are only three Actions available (for example, **Write Block** is not available for Bluetooth; therefore, Bluetooth devices can only be allowed, blocked or warned).

ThreatSense

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options enable you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense** in the Advanced setup for any module that uses ThreatSense

technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section enables you to define which computer components and files will be scanned for infiltrations.

Operating memory—Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI—Scans boot sectors for the presence of malware in the master boot record. Read more about UEFI in the glossary.

Email files—The program supports the following extensions: DBX (Outlook Express) and EML.

Archives—The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives—Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers—After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics—A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist or was not covered by the previous versions of the detection engine module. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures—Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of ESET Endpoint Security while cleaning objects.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine setup for a On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS)—Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority—Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects—The Scan log will show all the scanned files in self-extracting archives, even those not infected (may generate a lot of scan log data and increase the scan log file size).

Enable Smart optimization—With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the specific modules are applied when performing a scan.

Preserve last access timestamp—Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

Limits

The Limits section enables you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size—Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited.

Maximum scan time for object (sec.)—Defines the maximum time value for the scan of files in a container object (such as a RAR/ZIP archive or an email with multiple attachments). This setting does not apply for standalone files. If a user-defined value has been typed and that time has elapsed, a scan will stop as soon as possible, regardless of whether the scan of each file in a container object has finished. In the case of an archive with large files, the scan will stop no sooner than a file from the archive is extracted (for example, when a user-defined variable is 3

seconds, but the extraction of a file takes 5 seconds). The rest of the files in the archive will not be scanned when that time has elapsed. To limit scanning time, including bigger archives, use **Maximum object size** and **Maximum size of file in archive** (not recommended due to possible security risks). Default value: unlimited.

Archive scan setup

Archive nesting level—Specifies the maximum depth of archive scanning. Default value: 10.

Maximum size of file in archive—This option enables you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. The maximum value is 3 GB.

> We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

Cleaning levels

To change cleaning level settings for a desired protection module, expand **ThreatSense** (for example, **Real-time file system protection**) and then choose a **Cleaning level** from the drop-down menu.

ThreatSense has the following remediation (i.e. cleaning) levels.

Remediation in ESET Endpoint Security

Cleaning level	Description
Always remedy detection	Attempt to remediate the detection while cleaning objects without any end-user intervention. In some rare cases (for example, system files), if the detection cannot be remediated, the reported object is left in its original location. **Always remedy detection** is the recommended default setting in a managed environment.
Remedy detection if safe, keep otherwise	Attempt to remediate the detection while cleaning objects without any end-user intervention. In some cases (for example, system files or archives with both clean and infected files), if a detection cannot be remediated, the reported object is left in its original location.
Remedy detection if safe, ask otherwise	Attempt to remediate the detection while cleaning objects. In some cases, if no action can be performed, the end-user receives an interactive alert and must select a remediation action (for example, delete or ignore). This setting is recommended in most cases.
Always ask the end-user	The end-user receives an interactive window while cleaning objects and must select a remediation action (for example, delete or ignore). This level is designed for more advanced users who know which steps to take in the event of a detection.

File extensions excluded from scanning

Excluded file extensions are a part of ThreatSense. To configure excluded file extensions, click **ThreatSense** in the Advanced setup for any module that uses ThreatSense technology.

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense setup lets you define the types of files to scan.

Not to be confused with Processes exclusions, HIPS exclusions or File/folder exclusions.

By default, all files are scanned. Any extension can be added to the list of files excluded from scanning.

Excluding files is sometimes necessary if scanning certain file types prevents the program that is using certain extensions from running properly. For example, it may be advisable to exclude the `.edb`, `.eml` and `.tmp` extensions when using Microsoft Exchange servers.

To add a new extension to the list, click **Add**. Type the extension into the blank field (for example tmp) and click **OK**. When you select **Enter multiple values**, you can add multiple file extensions delimited by lines, commas or semicolons (for example, choose **Semicolon** from drop-down menu as a separator, and type `edb;eml;tmp`).
You can use a special symbol ? (question mark). The question mark represents any symbol (for example `?db`).

To see the exact extension (if any) of a file in a Windows operating system you have to select the **File name extensions** check box in **Windows Explorer** > **View** (tab).

Additional ThreatSense parameters

To edit these settings open Advanced setup > **Protections** > **Real-time file system protection** > **Additional ThreatSense parameters**.

Additional ThreatSense parameters for newly created and modified files

The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. ESET Endpoint Security uses advanced heuristics, which can detect new threats before the detection engine update is released in combination with signature-based scanning methods.

In addition to newly-created files, scanning is also performed on **Self-extracting archives** (.sfx) and **Runtime packers** (internally compressed executable files). By default, archives are scanned up to the 10th nesting level, and are checked regardless of their actual size. To modify archive scan settings, deselect **Default archive scan settings**.

Additional ThreatSense parameters for executed files

Advanced heuristics on file execution—By default, Advanced heuristics is used when files are executed. When enabled, we strongly recommend keeping Smart optimization and ESET LiveGrid® enabled to mitigate impact on system performance.

Advanced heuristics on executing files from removable media—Advanced heuristics emulates code in a virtual environment and evaluates its behavior before the code is allowed to run from removable media.

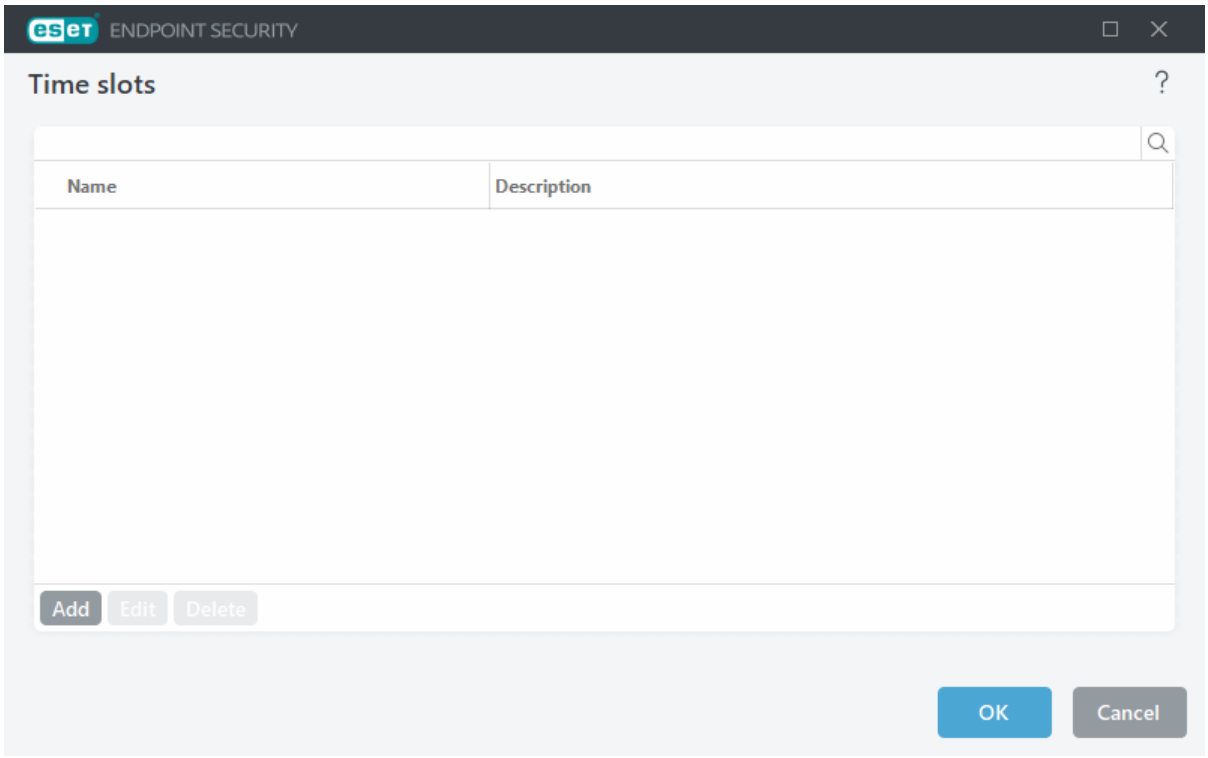
Tools

You can configure advanced settings for features that offer additional security and help simplify ESET Endpoint Security administration in Advanced setup > **Tools**.

- Time slots
- Microsoft Windows update
- ESET CMD
- Remote monitoring and management
- License interval check
- Log files
- Presentation mode
- Diagnostics

Time slots

Time slots can be created and then assigned to rules for **Device control** and **Web control**. The **Time slots** setting can be found in Advanced setup > **Tools**. This enables you to define commonly used time slots (e.g. work time, weekend, etc.) and reuse them easily without redefining the time ranges for every rule. Time slot is applicable to any relevant type of rule that supports time-based control.



To create a time slot, complete the following:

1. Click **Edit** > **Add**.
2. Type the name and **description** of the time slot and click **Add**.
3. Specify the day and start/end time for the time slot or select **All day**.
4. Click **OK** to confirm.

A single time slot can be defined with one or more time ranges based on days and times. When the time slot is created, it will show in the **Apply during** drop-down menu in the Device control rules editor window or Web control rules editor window.

Microsoft Windows update

The Windows update feature is an important component of protecting users from malicious software. For this reason, it is vital that you install Microsoft Windows updates as soon as they become available. ESET Endpoint Security notifies you about missing updates according to the level you specify. The following levels are available:

- **No updates**—No system updates will be offered for download.
- **Optional updates**—Updates marked as low priority and higher will be offered for download.
- **Recommended updates**—Updates marked as common and higher will be offered for download.
- **Important updates**—Updates marked as important and higher will be offered for download.
- **Critical updates**—Only critical updates will be offered for download.

Click **OK** to save changes. The System updates window will be displayed after status verification with the update server. Accordingly, the system update information may not be immediately available after saving changes.

Dialog window - Operating system updates

If there are some updates for your operating system, the ESET Endpoint Security Home window shows the notification. Click **More information** to open the System updates window.

The System updates window shows the available updates ready to be downloaded and installed. The update type is shown next to the name of the update.

Double-click any update row to display the Update information window with additional information.

Click **Run system update** to download and install all listed operating system updates.

Update information

The System updates window shows the list of available updates ready to be downloaded and installed. The update priority level is shown next to the name of the update.

Click **Run system update** to start downloading and installing operating system updates.

Right-click any update row and click **Show information** to display a new window with additional info.

ESET CMD

This is a feature that enables advanced ecmd commands. You can export and import settings using the command line (ecmd.exe). Until now, it was possible to export and import settings using GUI only. ESET Endpoint Security configuration can be exported to an *.xml* file.

When you have enabled ESET CMD, there are two authorization methods available:

- **None**—no authorization. We do not recommend you this method because it allows importation of any unsigned configuration, which is a potential risk.
- **Advanced setup password**—a password is required to import a configuration from an *.xml* file, this file must be signed (see signing *.xml* configuration file further down). The password specified in Access Setup

must be provided before a new configuration can be imported. If you do not have access setup enabled, your password does not match or the *.xml* configuration file is not signed, the configuration will not be imported.

When ESET CMD is enabled, you can use the command line to import or export ESET Endpoint Security configurations. You can do it manually or create a script for the purpose of automation.

To use advanced ecmd commands, you need to run them with administrator privileges, or open Windows Command Prompt (cmd) using **Run as administrator**. Otherwise, you will get **Error executing command** message. Also, when exporting configuration, destination folder must exist. The export command still works when the ESET CMD setting is switched off.

Advanced ecmd commands can only be run locally. Pausing ecmd commands can only be ran via client task **Run command** using ESET PROTECT On-Prem.

Export settings command:
`ecmd /getcfg c:\config\settings.xml`
Import settings command:
`ecmd /setcfg c:\config\settings.xml`

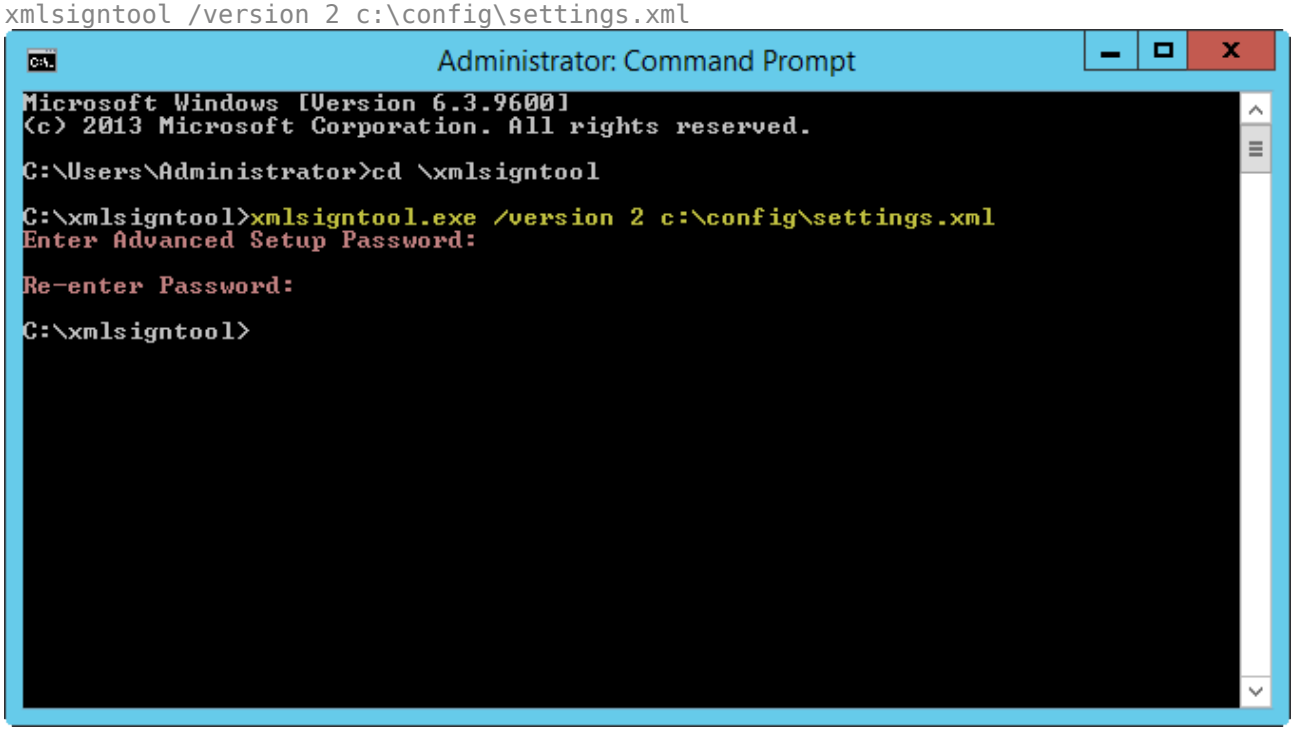
Signing an *.xml* configuration file:

1. Download the XmlSignTool executable.
2. Open a Windows Command Prompt (cmd) using **Run as administrator**.
3. Navigate to the save location of `xmlsigntool.exe`
4. Execute a command to sign the *.xml* configuration file, usage: `xmlsigntool /version 1|2 <xml_file_path>`

The value of the `/version` parameter depends on your version of ESET Endpoint Security. Use `/version 2` for version 7 and later.

5. Enter and Re-enter your Advanced setup Password when prompted by the XmlSignTool. Your *.xml* configuration file is now signed and can be used to import another instance of ESET Endpoint Security with ESET CMD using the password authorization method.

Sign exported configuration file command:
`xmlsigntool /version 2 c:\config\settings.xml`



If your Access Setup password changes and you want to import a configuration that was signed earlier with an old password, you need to sign the *.xml* configuration file again using your current password. This enables you to use an older configuration file without exporting it to another machine running ESET Endpoint Security before the import.

Enabling ESET CMD without an authorization is not recommended, since this will allow the import of any unsigned configuration. Set the password in Advanced setup > **User interface** > **Access setup** to prevent from unauthorized modification by users.

List of ecmd commands

Individual security features can be enabled and temporarily disabled with the ESET PROTECT On-Prem Client Task Run command. The commands do not override policy settings and any paused settings will revert back to its original state after the command has executed or after a device reboot. To utilize this feature, specify the command line to run in the field of the same name.

Review the list of commands for each security feature below:

Security Feature	Temporary Pause command	Enable Command
Real-time file system protection	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Document protection	ecmd /setfeature document pause	ecmd /setfeature document enable
Device control	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Presentation mode	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Personal firewall	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Network attack protection (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Botnet protection	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Web Control	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Web access protection	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable

Security Feature	Temporary Pause command	Enable Command
Email client protection	ecmd /setfeature email pause	ecmd /setfeature email enable
Email client antispam	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Anti-Phishing protection	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Remote monitoring and management

Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems using a locally installed agent that can be accessed by a management service provider.

ERMM - ESET plugin for RMM

- The default ESET Endpoint Security installation contains the file `ermm.exe` located in the Endpoint application within the directory:
  C:\Program Files\ESET\ESET Security\ermm.exe
- `ermm.exe` is a command line utility designed to facilitate the management of endpoint products and communications with any RMM plugin.
- `ermm.exe` exchanges data with the RMM Plugin, which communicates with the RMM Agent linked to an RMM Server. By default, the ESET RMM tool is disabled.

Additional resources

- ERMM Command Line
- List of ERMM JSON commands

- How to activate Remote monitoring and management in ESET Endpoint Security

ESET Direct Endpoint Management plugins for third-party RMM solutions

RMM Server is running as a service on a third-party server. For more information see the following ESET Direct Endpoint Management online user guides:

- ESET Direct Endpoint Management plugin for ConnectWise Automate
- ESET Direct Endpoint Management plugin for N-able N-central
- ESET Direct Endpoint Management plugin for N-able RMM
- ESET Direct Endpoint Management plugin for NinjaOne
- ESET Direct Endpoint Management plugin for Datto RMM
- ESET Direct Endpoint Management plugin for Kaseya VSA

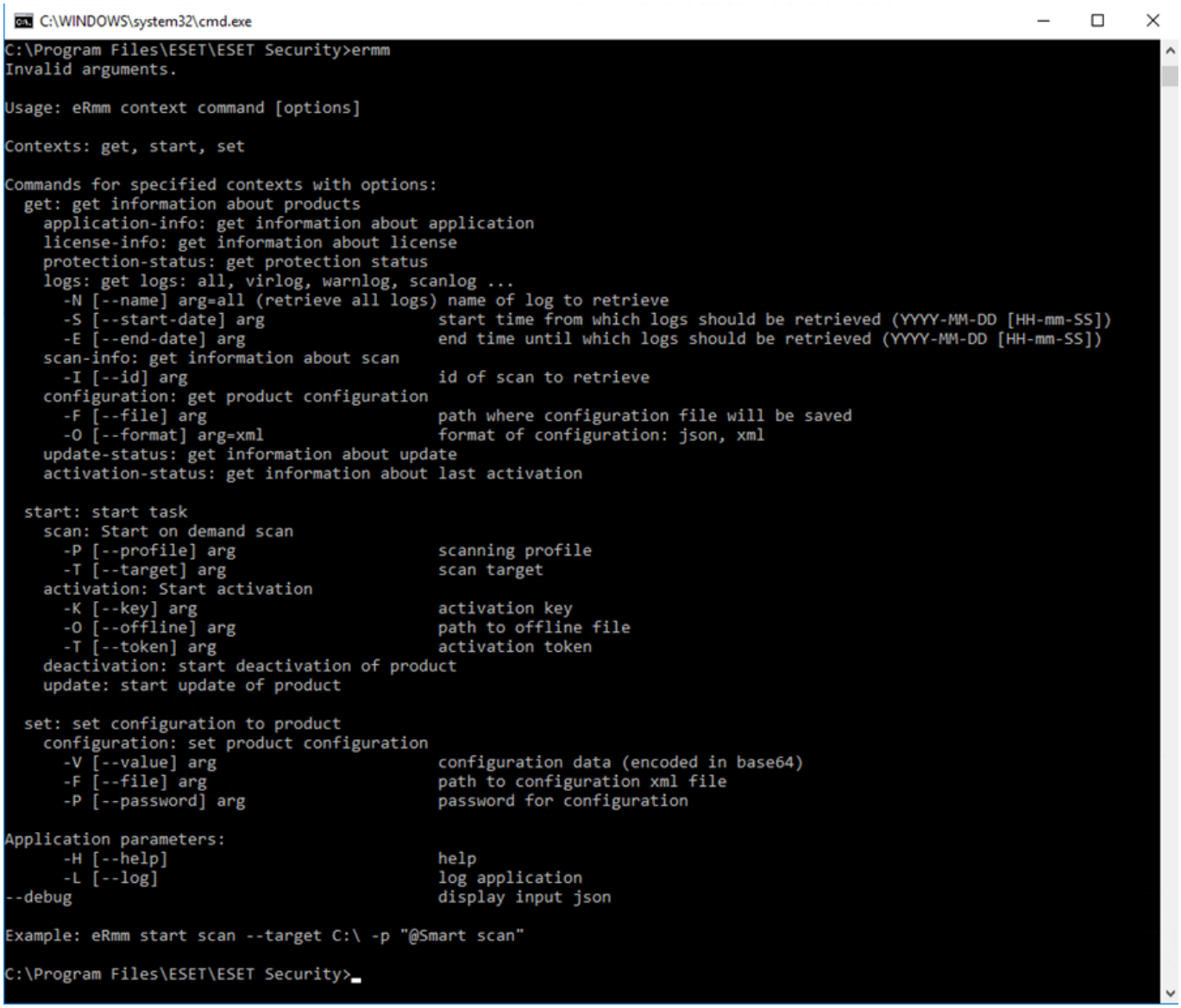
ERMM Command Line

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path (to open Command Prompt, press Windows button + R on your keyboard, type cmd into the Run window and press Enter).

The command syntax is: `ermm context command [options]`

The log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	application-info	Get information about product
	license-info	Get information about license
	protection-status	Get protection status
	logs	Get logs
	scan-info	Get information about running scan
	configuration	Get product configuration
	update-status	Get information about update
	activation-status	Get information about last activation
start		**Start task**

Context	Command	Description
	scan	Start on demand scan
	activation	Start activation of product
	deactivation	Start deactivation of product
	update	Start update of product
set		**Set options for product**
	configuration	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Specific command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM is not enabled in advanced settings or started as an administrator

List of ERMM JSON commands

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value
key	Activation key

offline	Path to offline file

Example

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

License interval check

ESET Endpoint Security needs to connect to the ESET License servers automatically. You can limit the number of connections to ESET License server in Advanced setup > **Tools** > **License**. By default, **Interval check** is set to **Automatic** and the connection is established a few times every hour. In case of an increased network traffic change the **Interval check** to **Limited** to decrease overload. When **Limited** is selected, ESET Endpoint Security connects to the license server only once a day, or when the computer restarts.

If **Interval check** is set to **Limited**, all license-related changes done via ESET PROTECT HUB / ESET MSP Administrator may take up to one day to apply to the ESET Endpoint Security settings.

Log files

The Logging configuration of ESET Endpoint Security is accessible in Advanced setup > **Tools** > **Log files**. The logs section is used to define how the logs will be managed. The program automatically deletes older logs to save hard disk space. You can specify the following options for log files:

Minimum logging verbosity—Specifies the minimum verbosity level of events to be logged:

- **Diagnostic**—Logs information needed to fine-tune the program and all records above.
- **Informative**—Records informative messages, including successful update messages, plus all records above.
- **Warnings**—Records critical errors and warning messages.
- **Errors**—Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical**—Logs only critical errors (error starting antivirus protection, built-in firewall, etc.).

All blocked connections will be recorded when you select the **Diagnostic** verbosity level.

Log entries older than the specified number of days in the **Automatically delete records older than (days)** field

will automatically be deleted.

Optimize log files automatically—When engaged, ESET Endpoint Security will automatically defragment log files if the fragmentation percentage is higher than the value specified in the field **If the number of unused records exceeds (%)**. Optimization is a process of defragmentation files, which means <%PRODUCTNAME %> will delete all unused records.

Click **Optimize** to begin defragmenting the log files. All empty log entries are removed to improve performance and log processing speed. This improvement can be observed specifically when the logs contain a large number of entries.

Enable text protocol enables the storage of logs in another file format separate from Log files:

- **Target directory**—Select the directory where log files will be stored (only applies to Text/CSV). You can copy the path or select another directory by clicking **Clear**. Each log section has its own file with a pre-defined file name (for example, *virlog.txt* for the **Detected threats** section of log files, if you use a plain text file format to store logs).
- **Type**—If you select the **Text** file format, logs will be stored in a text file and data will be separated into tabs. The same applies to the comma-separated **CSV** file format. If you choose **Event**, logs will be stored in the Windows Event log (can be viewed using Event Viewer in Control panel) as opposed to the file.
- **Delete all logs files**—Erases all stored logs currently selected in the **Type** drop-down menu. A notification about successful deletion of the logs will be shown.

Enable tracking of configuration changes in Audit log—Informs you about each configuration change. See Audit logs for more information.

> To help resolve issues more quickly, ESET may ask you to provide logs from your computer. ESET Log Collector makes it easy for you to collect the information needed. For more information about ESET Log Collector see our ESET Knowledgebase article.

Presentation mode

Presentation mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by notification/alert windows, and want to minimize CPU usage. Presentation mode can also be used during presentations that cannot be interrupted by antivirus activity. By enabling this feature, all pop-up windows are disabled and the activity of the scheduler will be stopped completely. System protection still runs in the background but does not demand any user interaction.

You can enable or disable Presentation mode in the main program window under **Setup** > **Computer** by clicking  or  next to **Presentation mode**. Enabling Presentation mode is a potential security risk, so the protection status icon in the taskbar will turn orange and display a warning. You will also see this warning in the main program window where you will see **Presentation mode active** in orange.

Activate **Enable Presentation mode when running applications in full-screen mode automatically** in Advanced setup > **Tools** > **Presentation mode** to have Presentation mode start whenever you initiate a full-screen application and stop after you exit the application.

Activate **Disable Presentation mode automatically after** to define the amount of time after which Presentation mode will automatically be disabled.

If the firewall is in Interactive mode and Presentation mode is enabled, you might have trouble connecting to the internet. This can be problematic if you start a game that connects to the internet. Normally, you would be asked to confirm such an action (if no communication rules or exceptions have been defined), but user interaction is disabled in Presentation mode. The solution is to define a communication rule for every application that might be in conflict with this behavior or to use a different Filtering mode in the firewall. Keep in mind that if Presentation mode is enabled and you go to a web page or an application that might be a security risk, it may be blocked but you will not see any explanation or warning because user interaction is disabled.

Diagnostics

Diagnostics provides application crash dumps of ESET processes (for example, ekrn). If an application crashes, a dump will be generated. This can help developers debug and fix various ESET Endpoint Security problems.

Click the drop-down menu next to **Dump type** and select one of three available options:

- Select **Disable** to disable this feature.
- **Mini** (default)—Records the smallest set of useful information that may help identify why the application crashed unexpectedly. This kind of dump file can be useful when space is limited, however because of the limited information included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.
- **Full**—Records all the contents of system memory when the application stops unexpectedly. A complete memory dump may contain data from processes that were running when the memory dump was collected.

Target directory—Directory where the dump during the crash will be generated.

Open diagnostics folder—Click **Open** to open this directory in a new *Windows explorer* window.

Create diagnostic dump—Click **Create** to create diagnostic dump files in the **Target directory**.

Advanced logging

Enable Antispam engine advanced logging—Record all events that occur during antispam scanning. This can help developers to diagnose and fix problems related to ESET Antispam engine.

Enable Browser protection advanced logging—Record all events that occur in Secure Browser to allow diagnosing and solving problems.

Enable Computer Scanner advanced logging—Record all events that occur while scanning files and folders by Computer scan or Real-time file system protection.

Enable Device control advanced logging—Record all events that occur in Device control. This can help developers diagnose and fix problems related to Device control.

Enable Direct Cloud advanced logging—Record all product communication between the product and Direct Cloud servers.

Enable Document protection advanced logging—Record all events that occur in Document protection to allow diagnosing and solving problems.

Enable Email client protection advanced logging—Record all events that occur in Email client protection and email client plug-in to allow diagnosing and solving problems.

Enable Kernel advanced logging—Record all events that occur in ESET kernel service (ekrn) to allow diagnosing and solving problems.

Enable Licensing advanced logging—Record all product communication with ESET activation and licensing servers.

Enable Memory tracing—Record all events which will help developers diagnose memory leaks.

Enable Network protection advanced logging—Record all network data passing through Firewall in the PCAP format to help developers diagnose and fix problems related to Firewall.

Enable Network traffic scanner advanced logging—Record all data passing through the Network traffic scanner in the PCAP format to help the developers diagnose and fix problems related to Network traffic scanner.

Enable Operating System advanced logging—Additional information about Operating system such as running processes, CPU activity, disc operations will be gathered. This can help developers to diagnose and fix problems related to ESET product running on your operating system.

Enable push messaging advanced logging—Record all events that occur during push messaging to allow diagnostics and problem solving.

Enable Real-time file system protection advanced logging—Record all events that occur in Real-time file system protection to allow diagnosing and solving problems.

Enable Update engine advanced logging—Record all events that occur during update process. This can help developers diagnose and fix problems related to the Update engine.

Enable Vulnerability & Patch management advanced logging—Record all events in Vulnerability & Patch management. This setting is shown only if the Vulnerability & Patch management is enabled in your environment (enabled in ESET PROTECT).

Enable Web control advanced logging—Record all events that occur in Web control. This can help developers diagnose and fix problems related to Web control.

Log files are located in *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Technical support

When contacting ESET Technical Support from the ESET Endpoint Security, you can submit system configuration data. Select **Always submit** from the **Submit system configuration data** drop-down menu to submit the data automatically, or select **Ask before submission** to be prompted before submitting data.

Connectivity

In specific networks, a proxy server can mediate communication between your computer and the internet. If you are using a proxy server, you need to define the following settings. Otherwise, ESET Endpoint Security and its modules cannot update automatically. In ESET Endpoint Security, proxy server setup is available in two different

sections of Advanced setup.

Global proxy server settings can be configured in Advanced setup > **Connectivity** > **Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET Endpoint Security. Parameters here will be used by all modules that require a connection to the internet.

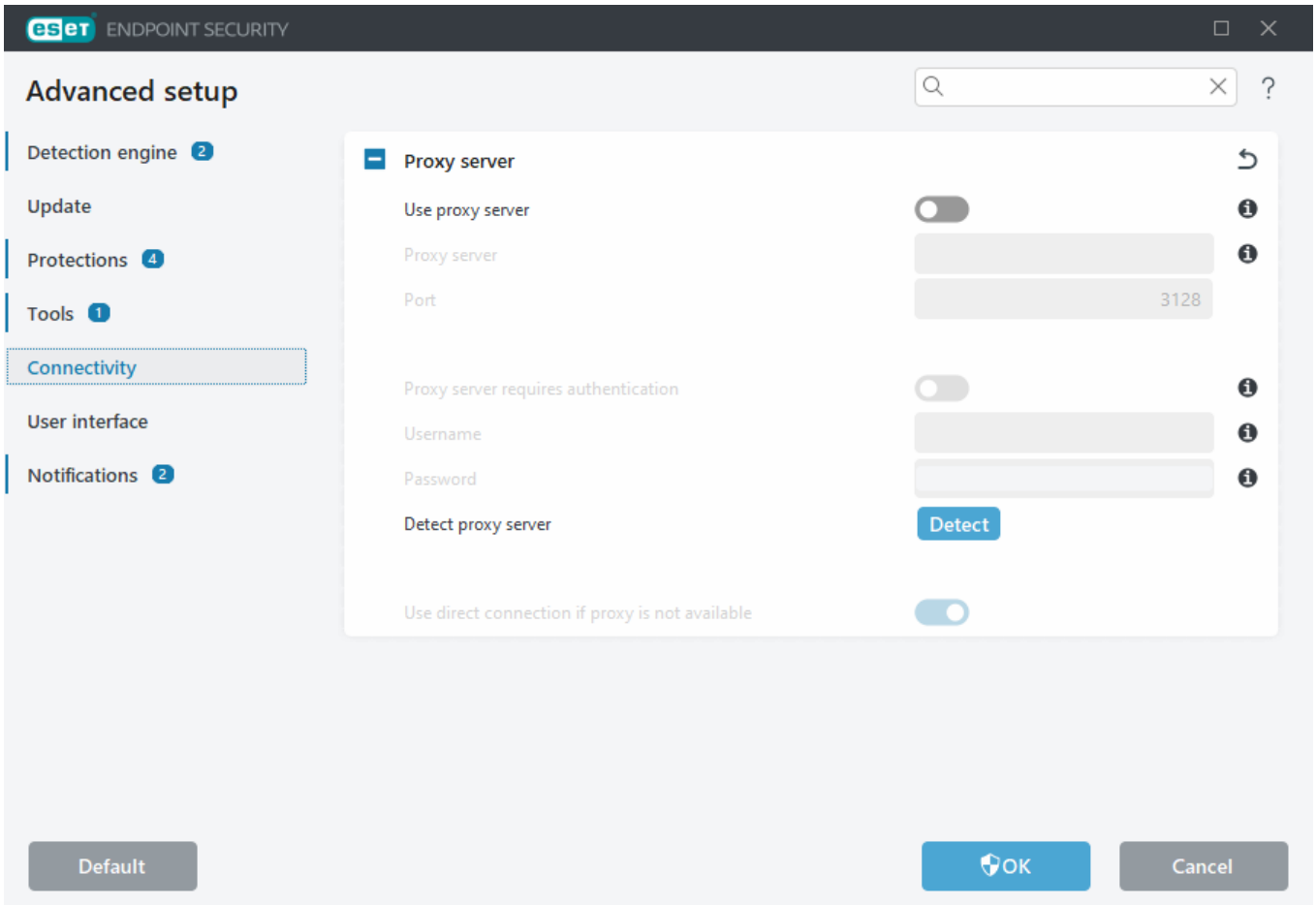
To specify global proxy server settings, enable **Use proxy server** and type the **Proxy server** address together with the proxy server's **Port** number.

If communication with the proxy server requires authentication, select **Proxy server requires authentication** and type a valid **Username** and **Password** into the corresponding fields. Click **Detect proxy server** to detect and populate proxy server settings automatically. To find proxy settings in your operating system, press **Windows + I** shortcut keys and click **Network & Internet** > **Proxy**. ESET Endpoint Security will copy the parameters specified in internet options for Internet Explorer or Google Chrome.

You must manually type your Username and Password in the **Proxy server** settings.

Use direct connection if proxy is not available—If ESET Endpoint Security is configured to connect via proxy and the proxy is unreachable, ESET Endpoint Security will bypass the proxy and communicate directly with ESET servers.

Proxy server settings can also be configured in Advanced setup > **Update** > **Profiles** > **Updates** > **Connection options** by selecting **Connection through a proxy server** from the **Proxy mode** drop-down menu. This configuration applies only for updates and is recommended for laptops receiving module updates from remote locations. For more information, refer to Advanced update setup.



User interface

To configure the program's graphical user interface (GUI) behavior, open Advanced setup > **User interface**.

You can adjust the program's visual appearance and effects in the User interface elements Advanced setup screen.

To provide maximum security of your security software, you can prevent uninstallation or any unauthorized changes by protecting the settings by a password using the Access setup tool.

> To configure the behavior of system notifications, detection alerts and application statuses, see the Notifications section.

Presentation mode is useful for users, who want to work with an application and not be interrupted by notifications, scheduled tasks and any components that could load the processor and RAM.

See also How to minimize the ESET Endpoint Security user interface (useful for managed environments).

User interface elements

User interface configuration options in ESET Endpoint Security enable you to adjust the working environment to fit your needs. These configuration options are accessible in **Advanced setup** (F5) > **User interface** > **User interface elements**.

In the **User interface elements** section, you can adjust the working environment. Use the **Start mode** drop-down menu to select from the following Graphical user interface (GUI) start modes:

Full—The complete GUI will be displayed.

Minimal—The GUI is running, but only notifications are displayed to the user.

Manual—The GUI is not started automatically on logon. Any user may start it manually.

Silent—No notifications or alerts will be displayed. The GUI can only be started by the Administrator. This mode can be useful in managed environments or in situations where you need to preserve system resources.

> When the Minimal GUI start mode is selected and your computer is restarted, notifications will be displayed but the graphical interface will not. To revert to full graphical user interface mode, run the GUI from the Start menu under **All Programs** > **ESET** > ESET Endpoint Security as an administrator, or you can do this via ESET PROTECT On-Prem using a policy.

Color mode—Select the color scheme of the ESET Endpoint Security graphical user interface (GUI) from the drop-down menu:

- **Same as the system color**—The ESET Endpoint Security color scheme will be set based on your operating system settings
- **Dark**—ESET Endpoint Security will have a dark color scheme (dark mode)
- **Light**—ESET Endpoint Security will have a standard, light color scheme

You can also select the color scheme of ESET Endpoint Security GUI in the top right corner of the main program window.

If you want to deactivate the ESET Endpoint Security splash-screen, deselect **Show splash-screen at startup**.

To have ESET Endpoint Security play a sound when important events occur during a scan, for example when a threat is discovered or when the scan has finished, select **Use sound signal**.

Integrate into the context menu—Integrate the ESET Endpoint Security control elements into the context menu.

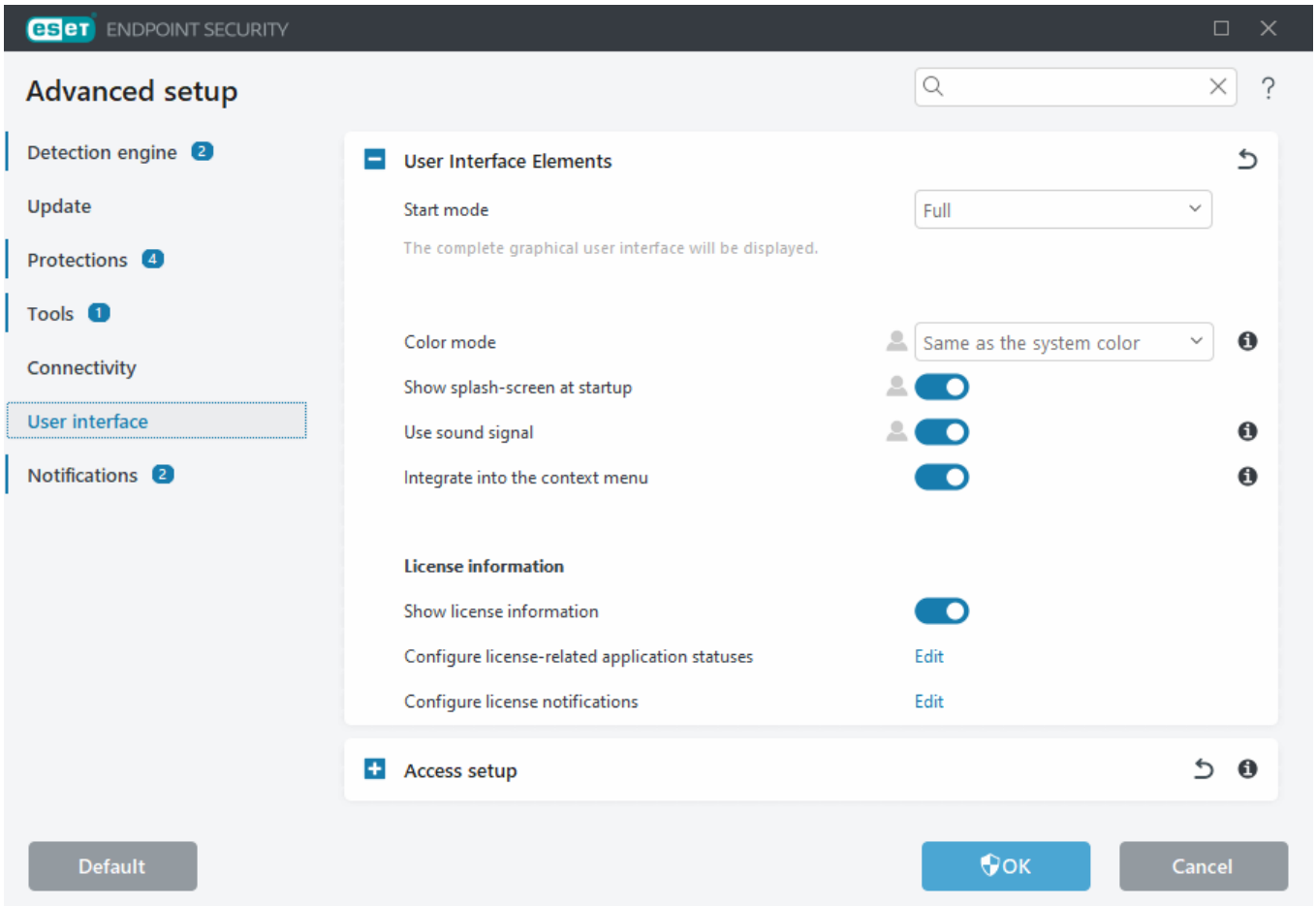
License information

Show license information—When disabled, the license expiration date on **Protection status** and **Help and support** screen will not be displayed.

Configure license-related application statuses—Opens the list of license-related application statuses.

Configure license notifications—Opens the list of license-related notifications.

License information settings are applied but not accessible for ESET Endpoint Security activated with an MSP license.



Access setup

ESET Endpoint Security settings are a crucial part of your security policy. Unauthorized modifications can potentially endanger the stability and protection of your system. To avoid unauthorized modifications, the setup parameters and uninstallation of ESET Endpoint Security can be password protected. Access setup can be configured in Advanced setup > **User interface** > **Access setup**.

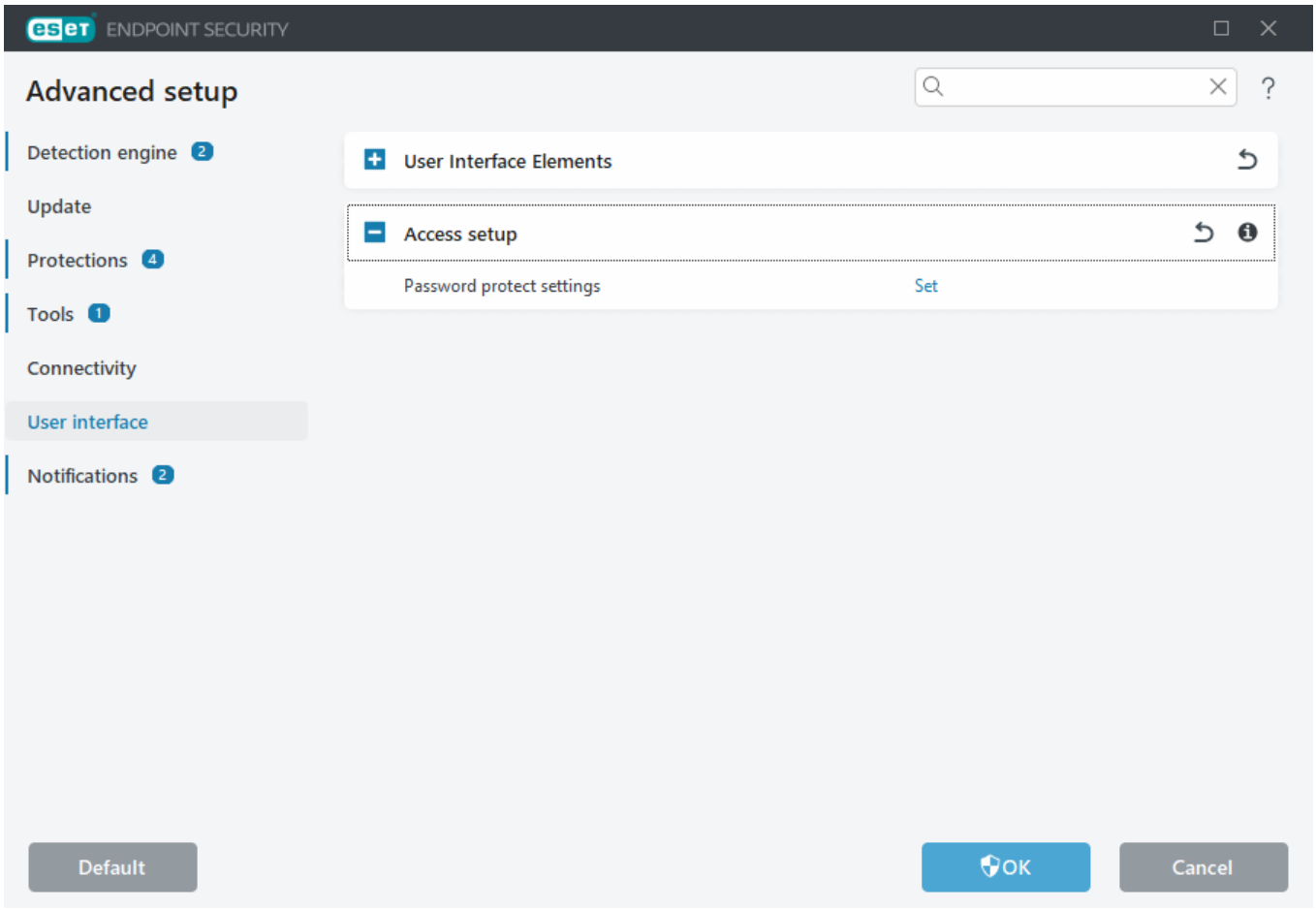
To set a password to protect setup parameters and uninstallation of ESET Endpoint Security, click **Set** next to **Password protect settings**.

To change your password, click **Change password** next to **Password protect settings**.

To remove your password, click **Remove** next to **Password protect settings**.

Managed environments

The administrator can create a policy to password protect the settings for ESET Endpoint Security on connected client computers. To create a new policy see Password protected settings.



Password for Advanced setup

To protect the ESET Endpoint Security Advanced setup and to avoid unauthorized modification, type your new password in the **New password** and **Confirm password** fields. Click **OK**.

Managed environments

The administrator can create a policy to password protect the settings for ESET Endpoint Security on connected client computers. To create a new policy see Password protected settings.

Unmanaged

When you want to change an existing password:

1. Type your old password in the **Old password** field.
2. Type your new password in the **New password** and **Confirm password** fields.
3. Click **OK**.

This password will be required for any future modifications to ESET Endpoint Security.

If you forgot your password, see Unlock your settings password in ESET Endpoint products.

To recover your lost ESET license key, the expiration date of your license, or other license information for ESET Endpoint Security, see I lost my Username and Password/license key.

Password

To avoid unauthorized modification, the setup parameters of ESET Endpoint Security can be password protected.

Safe mode

If the graphical interface of ESET Endpoint Security is launched in safe mode, a dialog window reporting that the application is to be run in safe mode is displayed. Since in safe mode the operation of all programs is limited, you cannot open the graphical interface of ESET Endpoint Security as in the standard mode.

The displayed window will enable you to run a computer scan. If you want to check your computer for malicious code, select the option **Yes**.

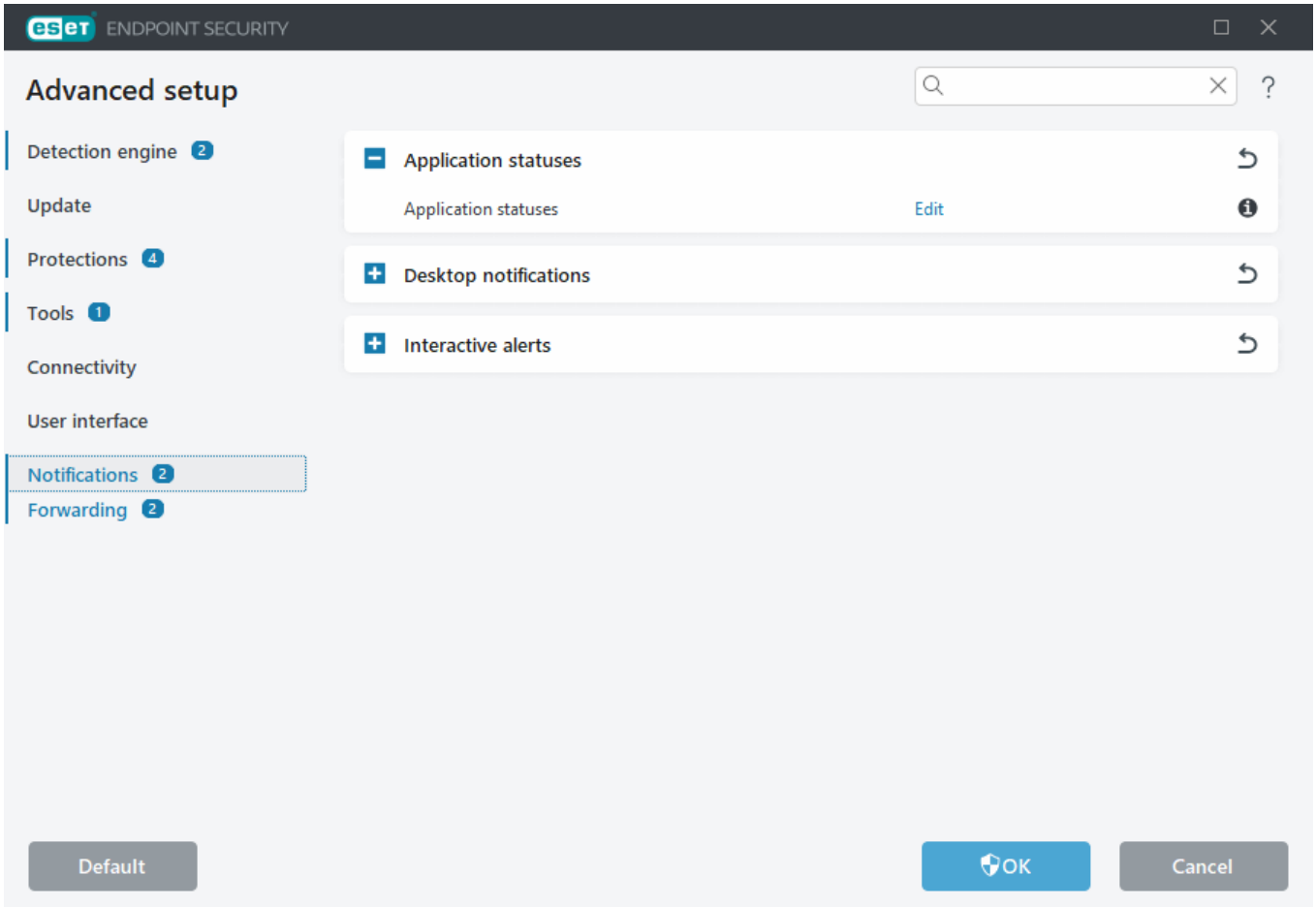
Doing so will launch scanning in a separate window using the same parameters as the default computer scan profile after the installation of ESET Endpoint Security.

Select the option **No** to close the dialog window; ESET Endpoint Security will perform no action.

Notifications

To manage ESET Endpoint Security notifications, open Advanced setup > **Notifications**. You can configure the following types of notifications:

- Application statuses—Notifications displayed in the home section of the main program window.
- Desktop notifications—Small notification windows next to the system taskbar.
- Interactive alerts—Alert windows and message boxes that require user interaction.
- Forwarding (email notifications)—Notifications are sent to a specified email address.
- Customization of notifications—Add custom message to e.g. a desktop notification.



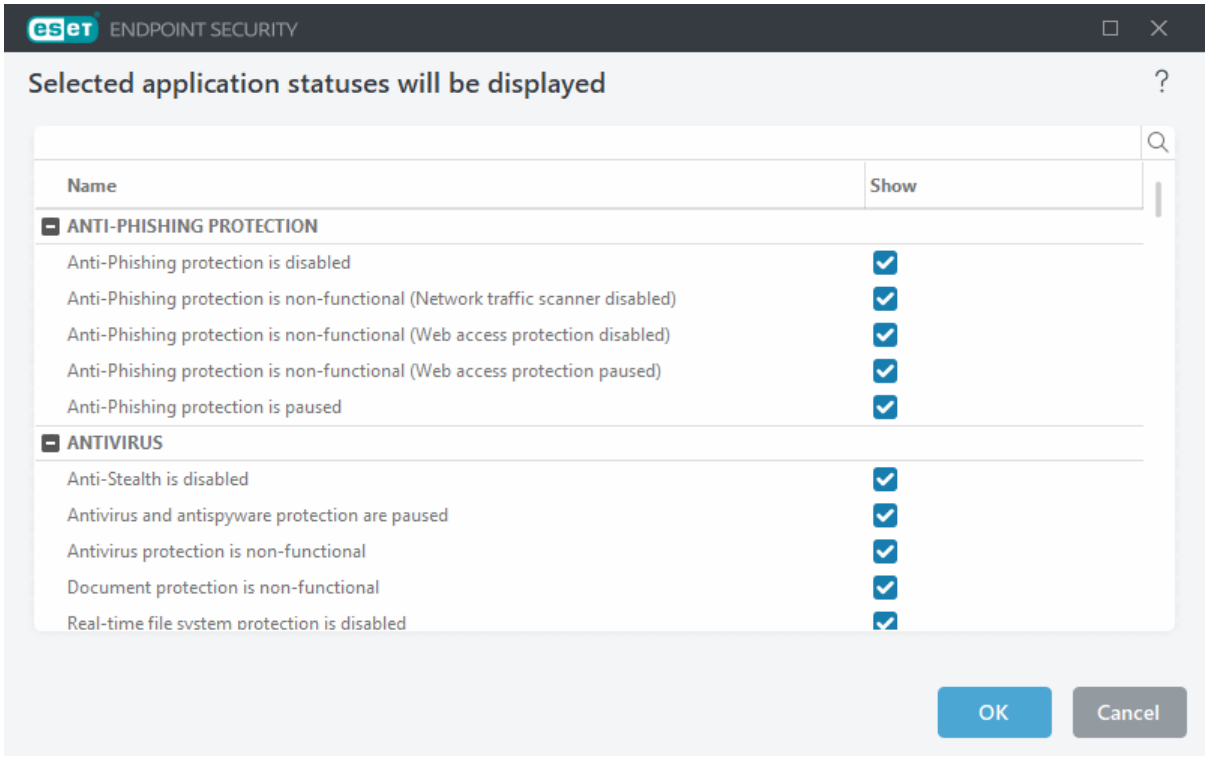
Application statuses

Application statuses—Click **Edit** to select which application statuses will be displayed in the home section of the main program window.

Application statuses

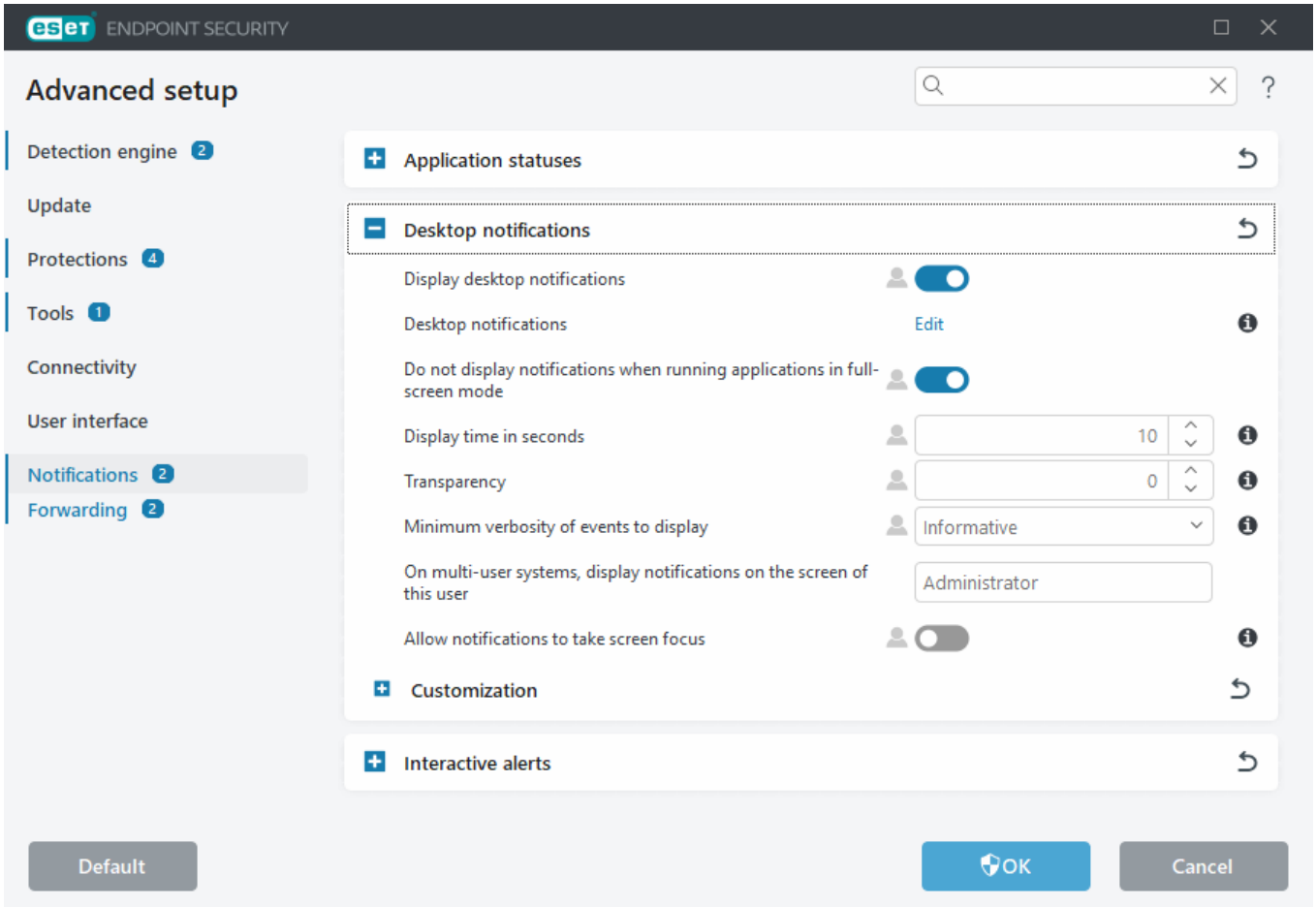
To configure which application statuses will be displayed (for example, when you pause Antivirus and antispyware protection or enable Presentation mode), open Advanced setup > **Notifications** and click **Edit** next to **Application statuses**.

Application status will also be displayed if your product is not activated or your license has expired. This setting can be changed via ESET PROTECT On-Prem policies.



Desktop notifications

Desktop notification is represented by small notification window next to system taskbar. By default, it is set to show for 10 seconds, then it slowly disappears. This is the main way how ESET Endpoint Security communicates with user, notifying about successful product updates, new devices connected, virus scans tasks completion or new threat found.



Display desktop notifications—We recommend keeping this option enabled so the product can inform you when a new event occurs.

Desktop notifications—Click **Edit** to enable or disable specific Desktop notifications.

Do not display notifications when running applications in full-screen mode—Suppress all non-interactive notifications when running applications in full screen mode.

Timeout in seconds—Set the notification visibility duration. The value must be between 3-30 seconds.

Transparency—Set the notification transparency percentage. The supported range is 0 (no transparency) to 80 (very high transparency).

Minimum verbosity of events to display—Set the starting notification severity level displayed. From the drop-down menu, select one of the following options:

- **Diagnostic**—Logs information needed to fine-tune the program and all records above.
- **Informative**—Records informative messages such as non-standard network events, including successful update messages, plus all records above.
- **Warnings**—Records critical errors and warning messages (for example, update failed).
- **Errors**—Errors (document protection not started) and critical errors will be recorded.
- **Critical**—Logs only critical errors error starting antivirus protection or infected system.

On multi-user systems, display notifications on the screen of this user—Allows selected account to receive desktop notifications. For example, if you do not use the Administrator account, type the full account name and the desktop notifications will be displayed for the specified account. Only one user account can receive the desktop notifications.

Allow notifications to take screen focus—Notifications will take screen focus and will be accessible by Alt+Tab.

Customization of notifications

In this window you can customize the messaging used in notifications.

Default notification message—A default message to be shown in the footer of notification.

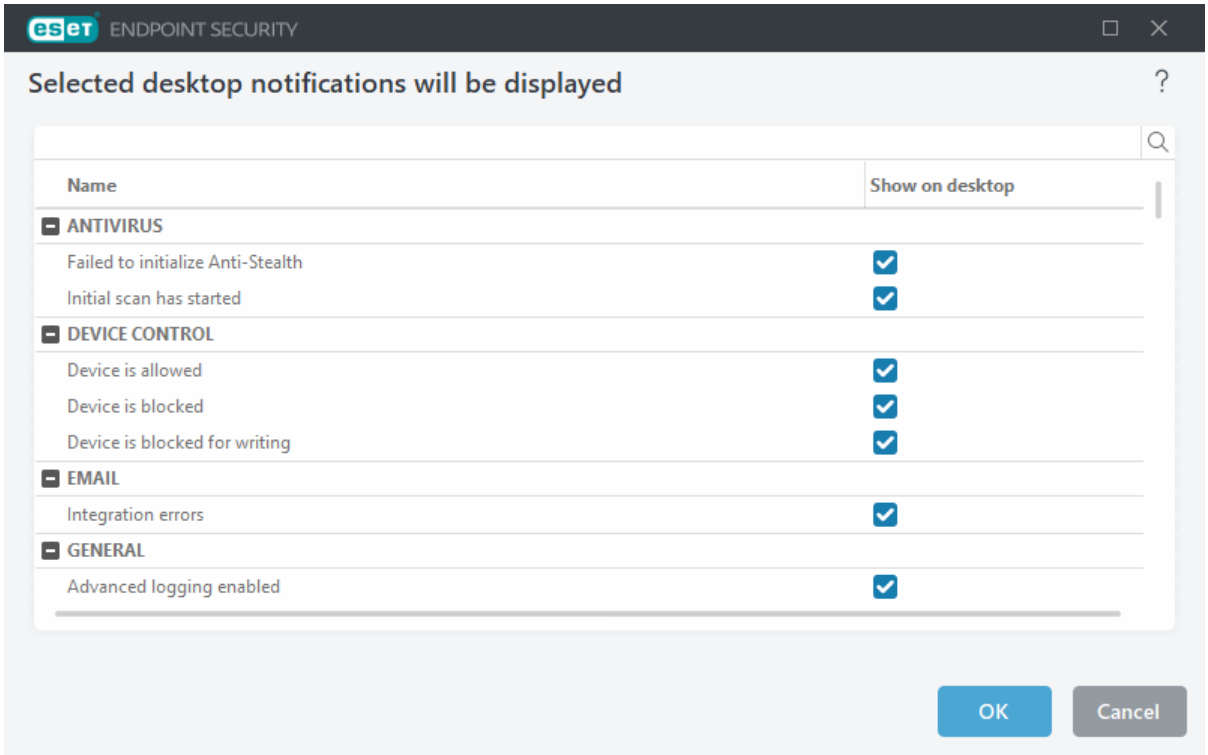
Detections

Enable **Do not close malware notifications automatically** to have malware notifications stay on screen until they are closed manually.

Disable **Use default message** and type your own message in the **Detection notification message** field to use customized notification messaging.

Dialog window - Desktop notifications

To adjust the visibility of desktop notifications (displayed at the bottom right of the screen), open Advanced setup > **Notifications** > **Desktop notifications**. Click **Edit** next to **Desktop notifications** and select the appropriate **Show on desktop** check box.



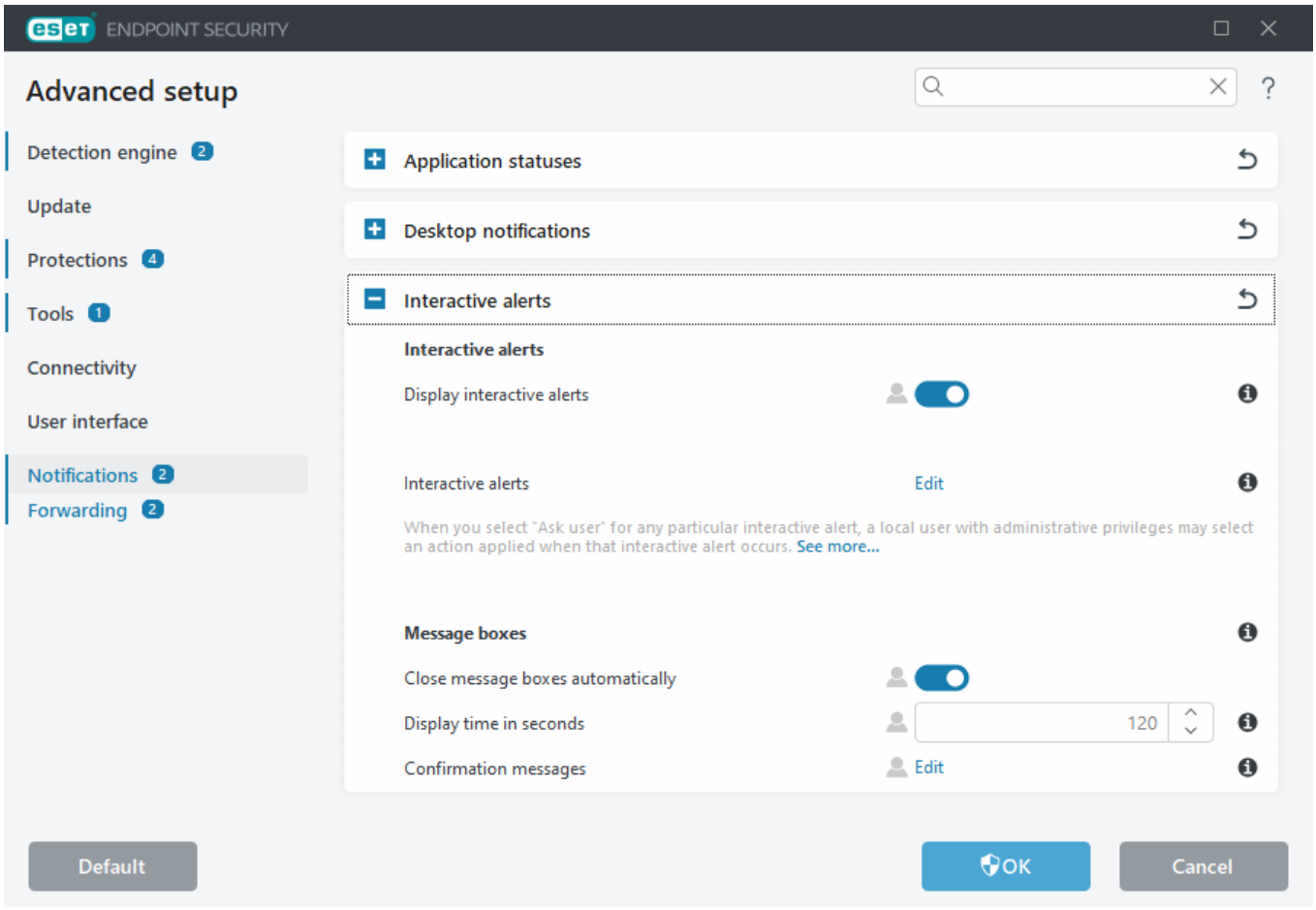
If you want to set-up notifications **File analyzed** and **File not analyzed** while using ESET LiveGuard, Proactive protection must be set to **Block execution until receiving the analysis result**.

Interactive alerts

Looking for information about common alerts and notifications?

- Threat found
- Address has been blocked
- Product not activated
- Update is available
- Update information is not consistent
- Troubleshooting for "Modules update failed" message
- 'File corrupt' or 'Failed to rename file'
- Website certificate revoked
- Network threat blocked
- File blocked due to analysis

The **Interactive alerts** section in Advanced setup > **Notifications** enables you to configure how message boxes and interactive alerts for detections, where a decision is needed to be made by a user (for example, potential phishing website) are handled by ESET Endpoint Security.



Interactive alerts

Disabling **Display interactive alerts** will hide all alert windows and in-browser dialogs and is only suitable for a limited amount of specific situations.

- For unmanaged users, we recommend this option is left in its default setting (enabled).
- For managed users, keep this setting enabled and select a pre-defined action for users in the List of interactive alerts.

Interactive alerts—Click **Edit** to select which Interactive alerts will be displayed.

Message boxes

To close the message boxes automatically after a certain time, select **Close message boxes automatically**. If they are not closed manually, alert windows are automatically closed after the specified time elapses.

Timeout in seconds—Sets the alert visibility duration. The value must be between 10-999 seconds.

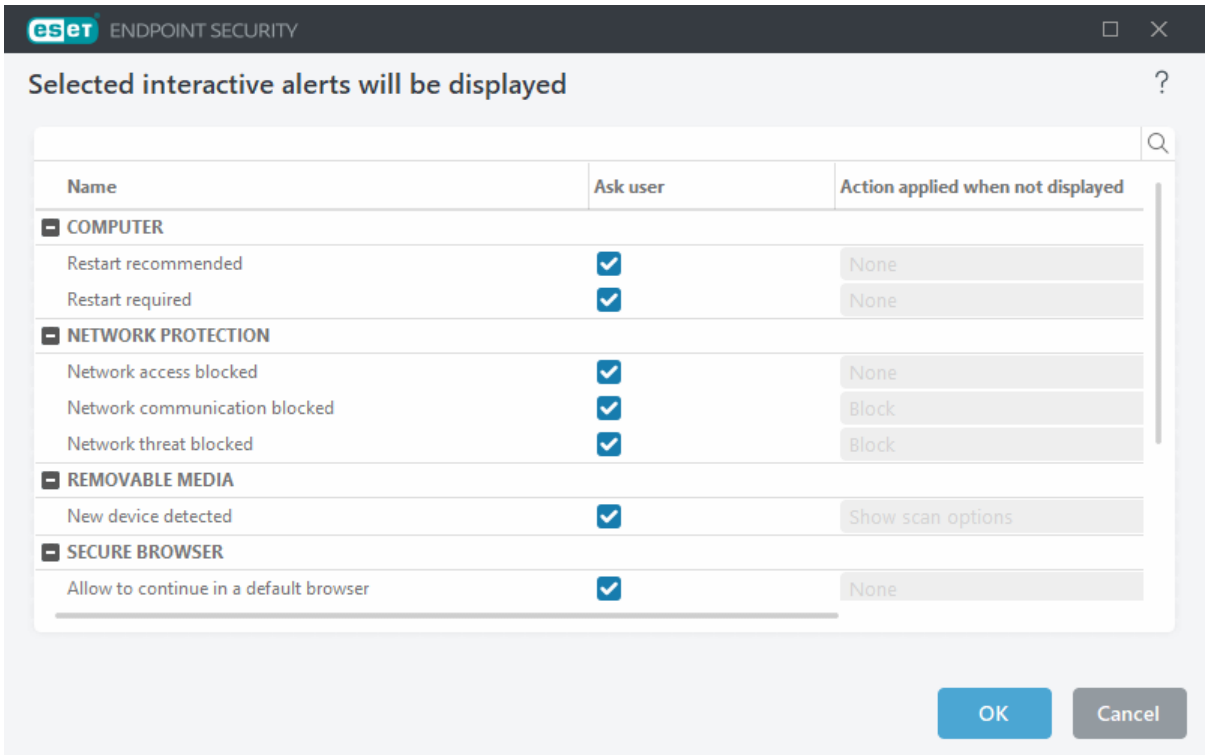
Confirmation messages—Click **Edit** to show a list of confirmation messages you can select to display or not to display.

List of interactive alerts

This section outlines several interactive alert windows that ESET Endpoint Security will display before any action is performed.

To adjust the behavior for configurable interactive alerts, open Advanced setup > **Notifications** > **Interactive alerts**, and click **Edit** next to **Interactive alerts**.

> Useful for managed environments where the administrator can deselect **Ask user** everywhere and select a pre-defined action applied when interactive alert windows are displayed.



Check other help sections for reference to a specific interactive alert window:

Removable media

- New device detected

Secure Browser

- Allow to continue in a default browser

Network protection

- Network access blocked is displayed when the **Isolate computer from network** client task of this workstation from ESET PROTECT On-Prem is triggered.
- Network communication blocked
- Network threat blocked

Web browser alerts

- Potentially unwanted content found
- Website blocked because of phishing

Computer

The presence of these alerts will change the user interface color:

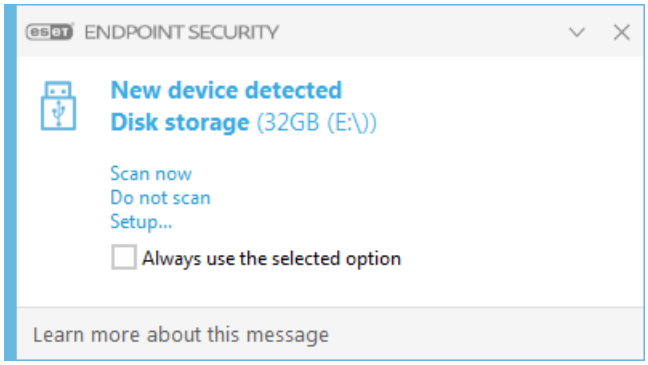
- Restart computer (required)
- Restart computer (recommended)

> Interactive alerts do not contain Detection engine, HIPS or Firewall interactive windows as their behavior can be configured individually in the specific feature.

Removable media

ESET Endpoint Security provides automatic removable media (CD/DVD/USB/...) scanning when inserted to a computer. This may be useful if the computer administrator wishes to prevent the users from using removable media with unsolicited content.

When a removable media is inserted, and **Show scan options** is set in Advanced setup > **Notifications** > **Interactive alerts > Edit** > **Removable media**, the following dialog will be shown:



Options for this dialog:

- **Scan now**—This will trigger a scan of removable media.
- **Do not scan**—Removable media will not be scanned.

- **Setup**—Opens the Advanced setup.
- **Always use the selected option**—When selected, the same action will be performed when a removable media is inserted another time.

In addition, ESET Endpoint Security features the Device control functionality, which enables you to define rules for the use of external devices on a given computer. More details on Device control can be found in the Device control section.

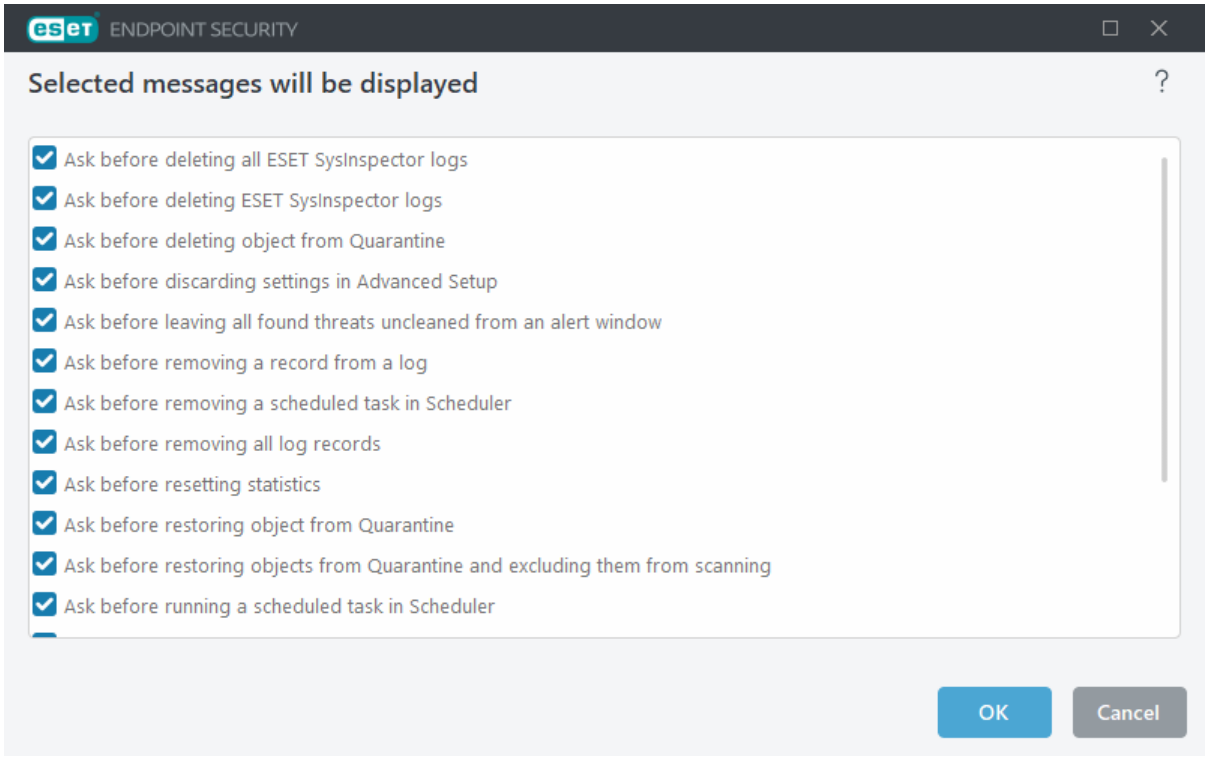
To access settings for removable media scan, open Advanced setup > **Notifications** > **Interactive alerts > Edit** > **Removable media**.

Action to take after inserting removable media—Select the default action that will be performed when a removable media device is inserted into the computer (CD/DVD/USB). Choose the desired action when inserting a removable media to a computer:

- **Do not scan**—No action will be performed, and the **New device detected** window will not open.
- **Automatic device scan**—A computer scan of the inserted removable media device will be performed.
- **Forced device scan**—A computer scan of the inserted removable media device will be performed and cannot be canceled.
- **Show scan options**—Opens the **Removable media** setup section.

Confirmation messages

To adjust confirmation messages, navigate to Advanced setup > **Notifications** > **Interactive alerts** and click **Edit** next to **Confirmation messages**.



This dialog window displays confirmation messages that ESET Endpoint Security will display before any action is performed. Select or deselect the check box next to each confirmation message to allow or disable it.

Learn more about specific feature related to confirmation messages:

- Ask before deleting ESET SysInspector logs
- Ask before deleting all ESET SysInspector logs
- Ask before deleting object from Quarantine
- Ask before discarding settings in Advanced Setup
- Ask before leaving all found threats uncleaned from an alert window
- Ask before removing a record from a log
- Ask before removing a scheduled task in Scheduler
- Ask before removing all log records
- Ask before resetting statistics
- Ask before restoring object from Quarantine
- Ask before restoring objects from Quarantine and excluding them from scanning
- Ask before running a scheduled task in Scheduler
- Show Antispam processing result notifications
- Show Antispam processing result notifications for email clients
- Show product confirmation dialogs for Outlook Express and Windows Mail email clients
- Show product confirmation dialogs for Windows Live Mail
- Show product confirmation dialogs for the Outlook email client

Advanced settings conflict error

This error may occur if some component (e.g. HIPS or Firewall) and user create the rules in interactive or learning mode at the same time.

We recommend to change the filtering mode into the default **Automatic mode** if you want to create your own rules. Read more about ESET Firewall Learning mode. Read more about HIPS and HIPS filtering modes.

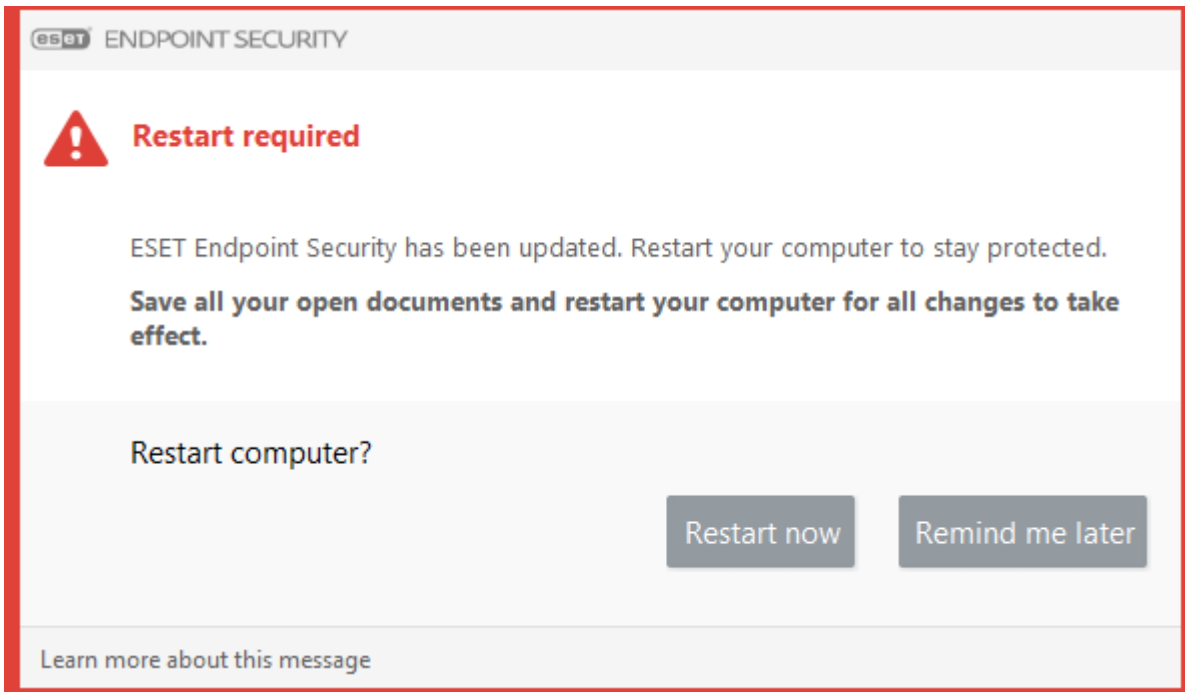
Allow to continue in a default browser

A specific interactive alert shows only when there is an error in starting Secure Browser properly.

Restart required

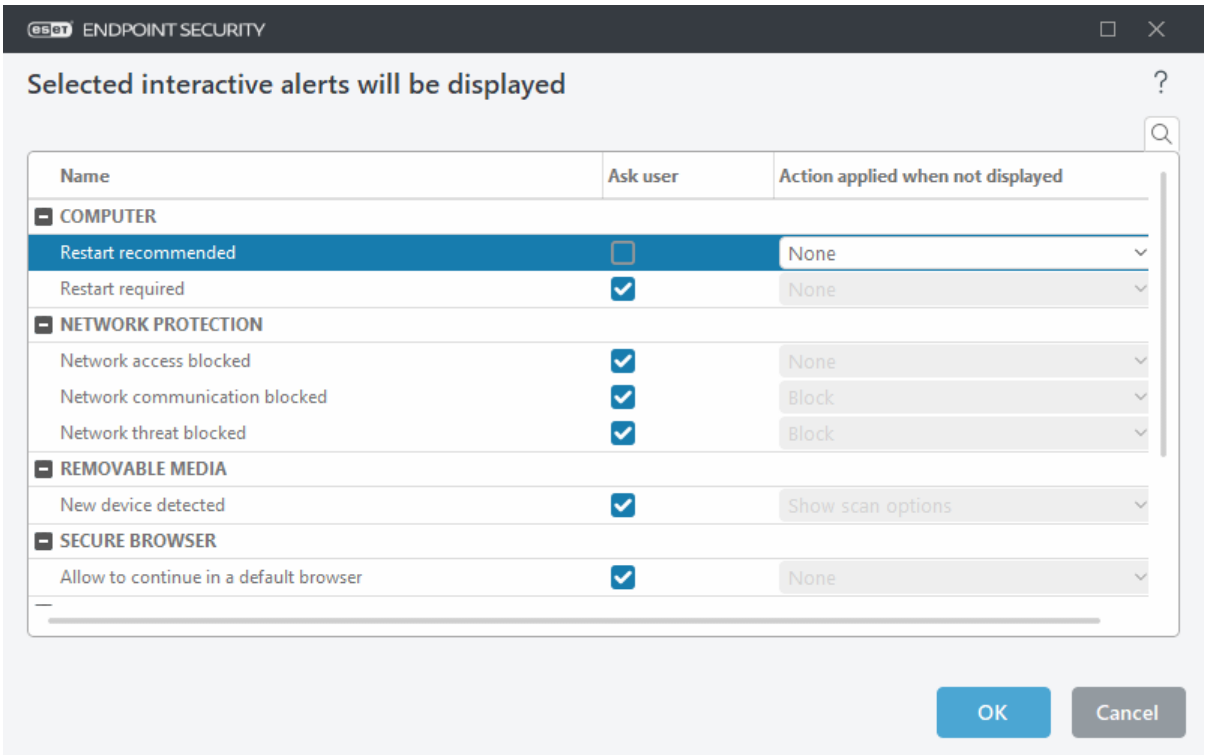
A computer restart is required after upgrading the ESET Endpoint Security to a new version or applying patches to applications via Vulnerability & Patch management. New versions of ESET Endpoint Security are issued to implement improvements or fix issues that automatic updates of program modules cannot resolve.

Click **Restart now** to restart your computer. If you plan to restart your computer later, click **Remind me later**. Later, you can restart your computer manually from the **Protection status** screen in the main program window.

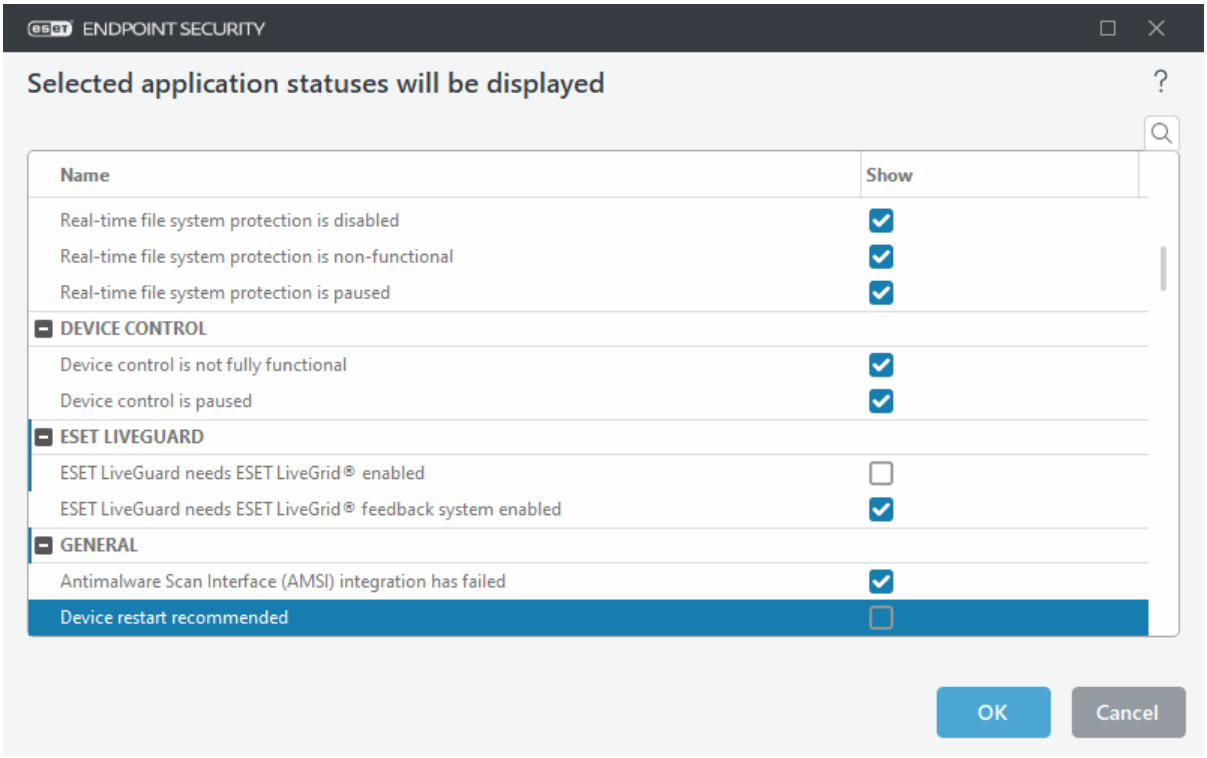


To disable the "Restart required" or "Restart recommended" alert, follow the steps below:

1. Open **Advanced setup** (F5) > **Notifications** > **Interactive alerts**.
2. Click **Edit** next to **Interactive alerts**. In the **Computer** section, deselect the check boxes next to **Restart computer (required)** and **Restart computer (recommended)**.



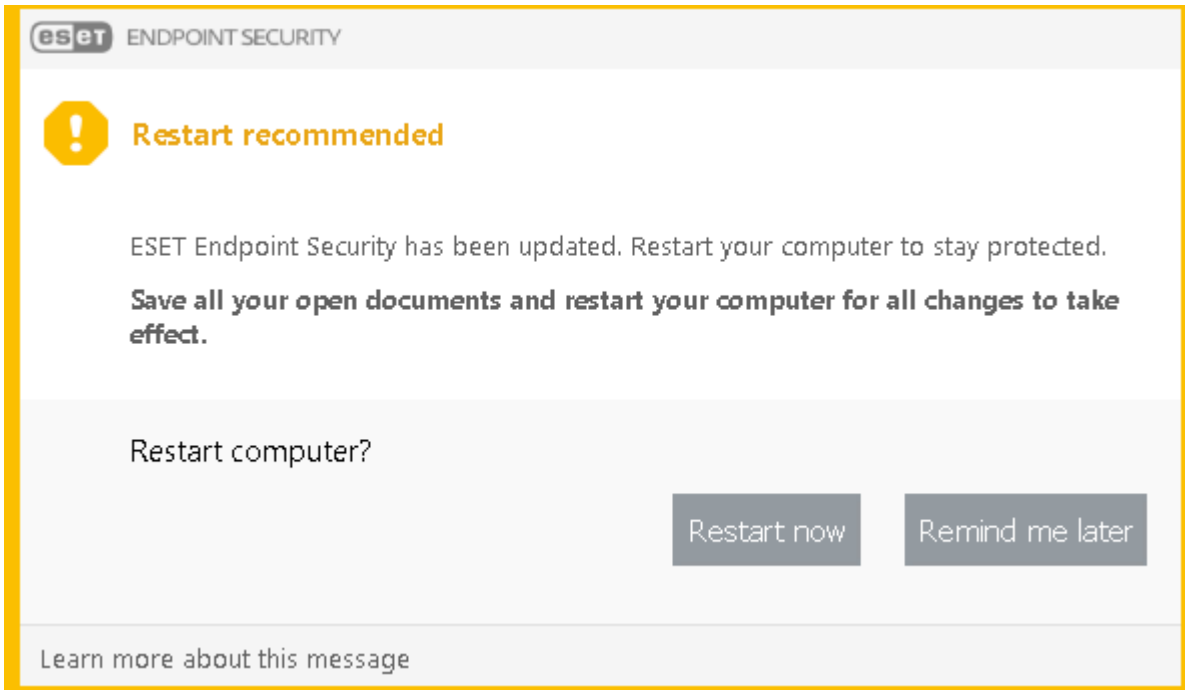
3. Click **OK** to save your changes in both open windows.
4. The alerts will no longer appear on the endpoint machine.
5. (optional) To disable the application status in the main program window of ESET Endpoint Security, from the Application statuses window deselect the check boxes next to **Computer restart required** and **Computer restart recommended**.



Restart recommended

A computer restart is required after updating the ESET Endpoint Security to a new version. New versions of ESET Endpoint Security are issued to implement improvements or fix issues that automatic updates of program modules cannot resolve.

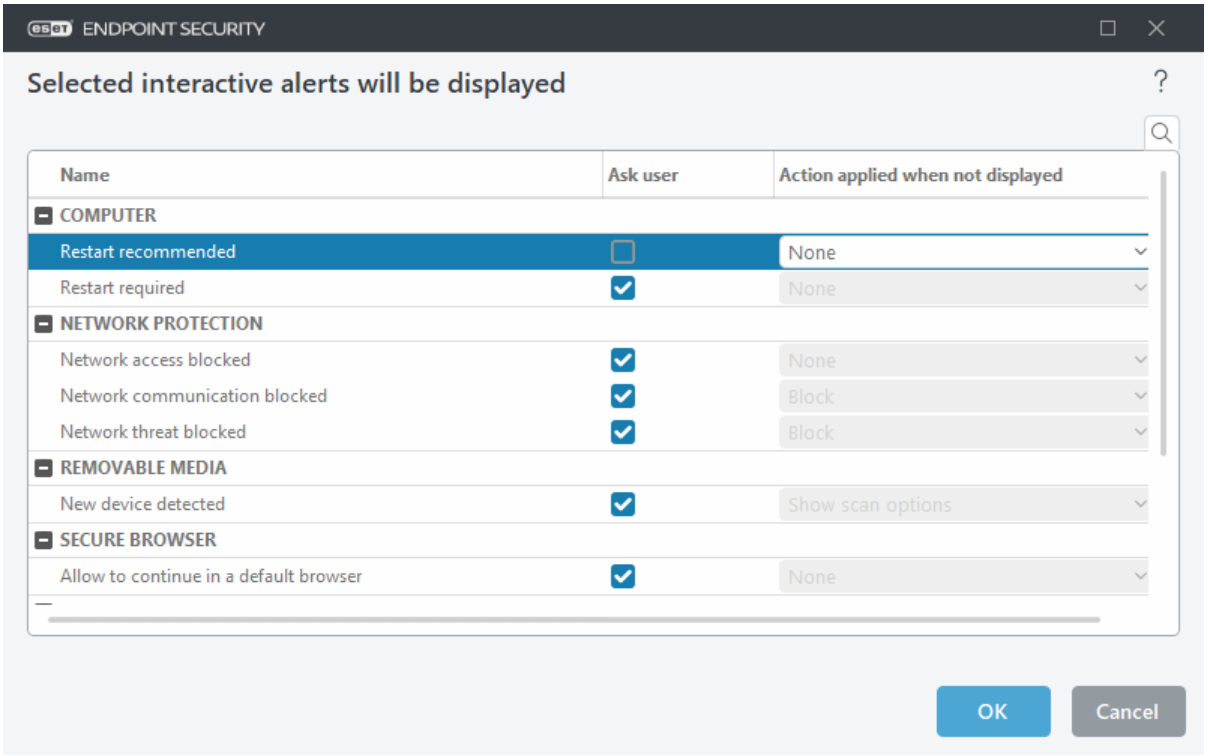
Click **Restart now** to restart your computer. If you plan to restart your computer later, click **Remind me later**. Later, you can restart your computer manually from the **Protection status** screen in the main program window.



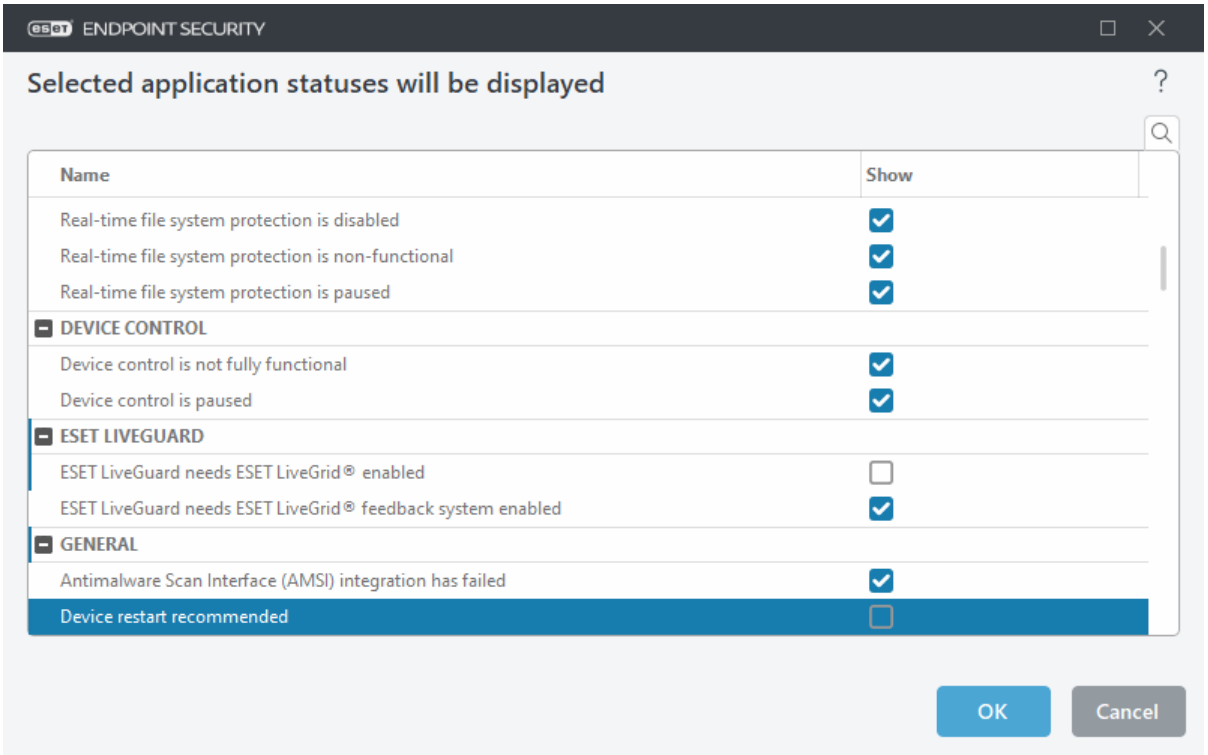
To disable the "Restart required" or "Restart recommended" alert, follow the steps below:

1. Open **Advanced setup** (F5) > **Notifications** > **Interactive alerts**.

2. Click **Edit** next to **Interactive alerts**. In the **Computer** section, deselect the check boxes next to **Restart computer (required)** and **Restart computer (recommended)**.



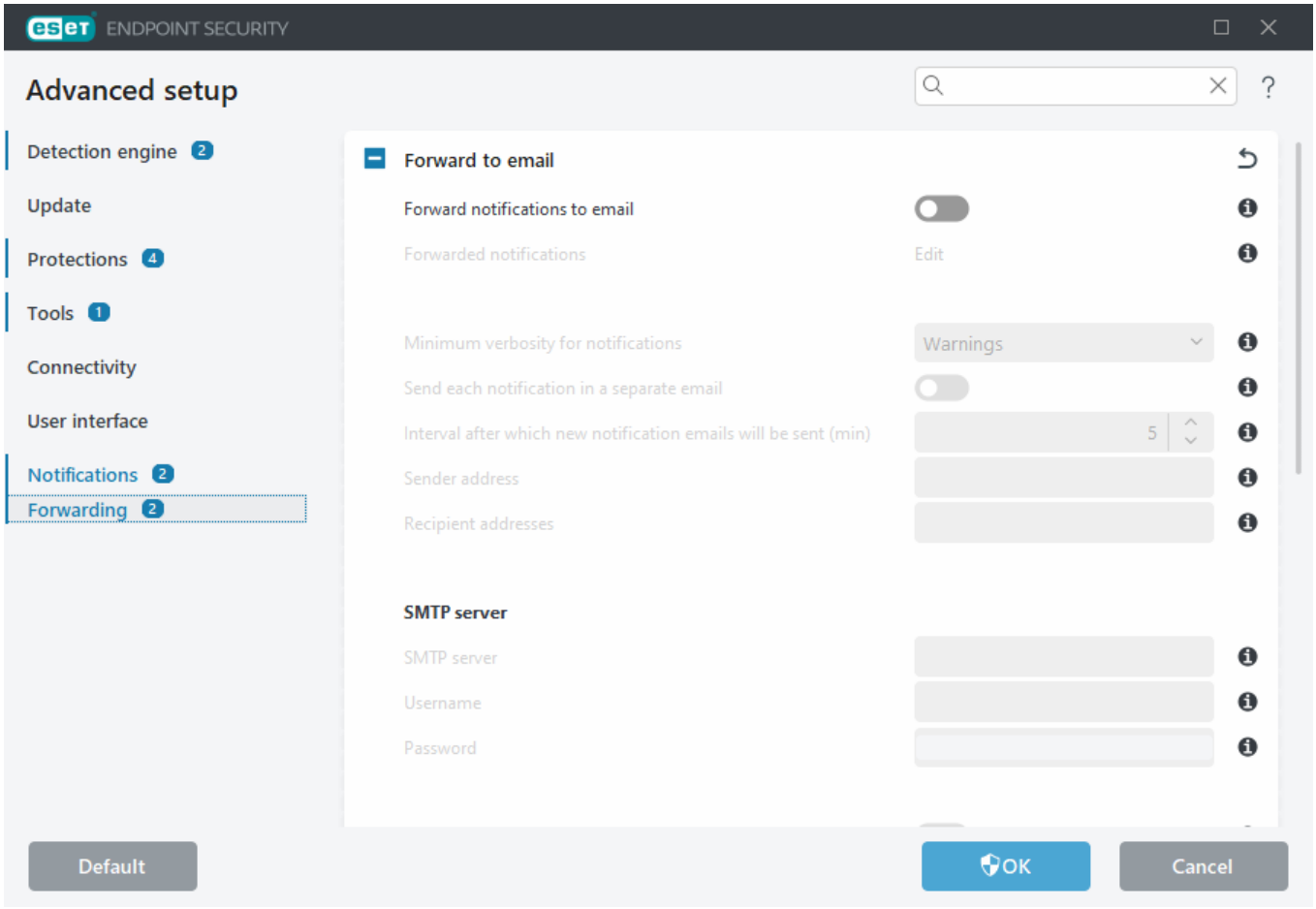
3. Click **OK** to save your changes in both open windows.
4. The alerts will no longer appear on the endpoint machine.
5. (optional) To disable the application status in the main program window of ESET Endpoint Security, from the Application statuses window deselect the check boxes next to **Computer restart required** and **Computer restart recommended**.



Forwarding

ESET Endpoint Security can automatically send notification emails if an event with the selected verbosity level occurs. In Advanced setup > **Notifications** > **Forwarding** > **Forward to email** section, enable **Forward notifications to email** to activate email notifications.

Forwarded notifications—Select which desktop notifications are forwarded to email.



From the **Minimum verbosity for notifications** drop-down menu, you can select the starting severity level of notifications to be sent.

- **Diagnostic**—Logs information needed to fine-tune the program and all records above.
- **Informative**—Records informative messages such as non-standard network events, including successful update messages, plus all records above.
- **Warnings**—Records critical errors and warning messages (for example, update failed).
- **Errors**—Errors (for example, Document protection not started) and critical errors will be recorded.
- **Critical**—Logs only critical errors (for example, Error starting antivirus protection, or Threat found).

Send each notification in a separate email—When enabled, the recipient will receive a new email for each notification. This may result in many emails received in a short period.

Interval after which new notification emails will be sent (min)—Interval in minutes after which new notifications will be sent to email. If you set this value to 0, the notifications will be sent immediately.

Sender address—Define the sender address displayed in the header of notification emails.

Recipient addresses—Define the recipient addresses displayed in the header of notification emails. Multiple values are supported. Use semi-colon as the separator.

SMTP server

SMTP server—The SMTP server used for sending notifications (e.g. *smtp.provider.com:587*, pre-defined port is 25).

SMTP servers with TLS encryption are supported by ESET Endpoint Security.

Username and password—If the SMTP server requires authentication, these fields should be filled in with a valid username and password to access the SMTP server.

Sender address—This field specifies the sender address that will be displayed in the header of notification emails.

Recipient addresses—This field specifies the recipient addresses that will be displayed in the header of notification emails. Use a semi-collon ";" to separate multiple email addresses.

Enable TLS—Enable sending alert and notification messages supported by TLS encryption.

Message format

Communications between the program and a remote user or system administrator are done via emails or LAN messages (using the Windows messaging service). The default format of the alert messages and notifications will be optimal for most situations. In some circumstances, you may need to change the message format of event messages.

Format of event messages—Format of event messages that are displayed on remote computers.

Format of threat warning messages—Threat alert and notification messages have a pre-defined default format. We advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format.

Charset—Converts an email message to the ANSI character encoding based on Windows Regional settings (for example, windows-1250, Unicode (UTF-8), ACSII 7-bit, or Japanese (ISO-2022-JP)). As the result, "á" will be changed to "a" and an unknown symbol to "?".

Use Quoted-printable encoding—The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

Keywords (strings separated by % signs) are replaced in the message by the actual information as specified. The following keywords are available:

- **%TimeStamp%**—Date and time of the event
- **%Scanner%**—Module concerned
- **%ComputerName%**—Name of the computer where the alert occurred
- **%ProgramName%**—Program that generated the alert
- **%InfectedObject%**—Name of infected file, message, etc
- **%VirusName%**—Identification of the infection
- **%Action%**—Action taken over infiltration
- **%ErrorDescription%**—Description of a non-virus event

The keywords **%InfectedObject%** and **%VirusName%** are only used in threat warning messages, and **%ErrorDescription%** is only used in event messages.

Revert all settings to default

Click **Default** in Advanced setup to revert all program settings, for all modules. This will be reset to the status they would have had after a new installation.

See also Import and export settings.

Revert all settings in current section

Click the curving arrow ⍰ to revert all settings in the current section to the default settings defined by ESET.

Any changes that have been made will be lost after you click **Revert to default**.

Revert contents of tables—When enabled, the rules, tasks or profiles that have been added manually or automatically will be lost.

See also Import and export settings.

Error while saving the configuration

This error message indicates that the settings were not saved correctly due to an error.

This usually means that the user who attempted to modify program parameters:

- has insufficient access rights or does not have the necessary operating system privileges required to modify configuration files and the system registry.
  > To perform desired modifications, the system administrator must log in.
- has recently enabled Learning mode in HIPS or Firewall and attempted to make changes to Advanced setup.
  > To save the configuration and avoid the configuration conflict, close Advanced setup without saving and attempt to make desired changes again.

The second most common cause may be that the program no longer works properly, is corrupted and therefore needs to be reinstalled.

Command line scanner

ESET Endpoint Security's antivirus module can be launched via the command line – manually (with the "ecls" command) or with a batch ("bat") file.

ESET Command-line scanner usage:

```
ecls [OPTIONS...] FILES...
```

The following parameters and switches can be used while running the on-demand scanner from the command

line:

Options

/base-dir=FOLDER	load modules from FOLDER
/quar-dir=FOLDER	quarantine FOLDER
/exclude=MASK	exclude files matching MASK from scanning
/subdir	scan subfolders (default)
/no-subdir	do not scan subfolders
/max-subdir-level=LEVEL	maximum sub-level of folders within folders to scan
/symlink	follow symbolic links (default)
/no-symlink	skip symbolic links
/ads	scan ADS (default)
/no-ads	do not scan ADS
/log-file=FILE	log output to FILE
/log-rewrite	overwrite output file (default – append)
/log-console	log output to console (default)
/no-log-console	do not log output to console
/log-all	also log clean files
/no-log-all	do not log clean files (default)
/aind	show activity indicator
/auto	scan and automatically clean all local disks

Scanner options

/files	scan files (default)
/no-files	do not scan files
/memory	scan memory
/boots	scan boot sectors
/no-boots	do not scan boot sectors (default)
/arch	scan archives (default)
/no-arch	do not scan archives
/max-obj-size=SIZE	only scan files smaller than SIZE megabytes (default 0 = unlimited)
/max-arch-level=LEVEL	maximum sub-level of archives within archives (nested archives) to scan
/scan-timeout=LIMIT	scan archives for LIMIT seconds at maximum
/max-arch-size=SIZE	only scan the files in an archive if they are smaller than SIZE (default 0 = unlimited)
/max-sfx-size=SIZE	only scan the files in a self-extracting archive if they are smaller than SIZE megabytes (default 0 = unlimited)
/mail	scan email files (default)
/no-mail	do not scan email files
/mailbox	scan mailboxes (default)

/no-mailbox	do not scan mailboxes
/sfx	scan self-extracting archives (default)
/no-sfx	do not scan self-extracting archives
/rtp	scan runtime packers (default)
/no-rtp	do not scan runtime packers
/unsafe	scan for potentially unsafe applications
/no-unsafe	do not scan for potentially unsafe applications (default)
/unwanted	scan for potentially unwanted applications
/no-unwanted	do not scan for potentially unwanted applications (default)
/suspicious	scan for suspicious applications (default)
/no-suspicious	do not scan for suspicious applications
/pattern	use signatures (default)
/no-pattern	do not use signatures
/heur	enable heuristics (default)
/no-heur	disable heuristics
/adv-heur	enable Advanced heuristics (default)
/no-adv-heur	disable Advanced heuristics
/ext-exclude=EXTENSIONS	exclude file EXTENSIONS delimited by colon from scanning
/clean-mode=MODE	use cleaning MODE for infected objects The following options are available: • `none` (default)—No automatic cleaning will occur. • `standard`—ecls.exe will attempt to clean or delete infected files automatically. • `strict`—ecls.exe will attempt to automatically clean or delete infected files without user intervention (you will not be prompted before files are deleted). • `rigorous`—ecls.exe will delete files without attempting to clean regardless of the file. • `delete`—ecls.exe will delete files without attempting to clean but will refrain from deleting sensitive files such as Windows system files.
/quarantine	copy infected files (if cleaned) to Quarantine (supplements the action carried out while cleaning)
/no-quarantine	do not copy infected files to Quarantine

General options

/help	show help and quit
/version	show version information and quit
/preserve-time	preserve the last access timestamp

Exit codes

0	no threat found
1	threat found and cleaned
10	some files could not be scanned (can be threats)

50	threat found
100	error

Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

Common Questions

This chapter covers some of the most frequently asked questions and problems encountered. Click a topic title to find out how to solve your problem:

- How to update ESET Endpoint Security
- How to activate ESET Endpoint Security
- ESET Endpoint Security has detected a threat
- How to remove a virus from my PC
- How to allow communication for a certain application
- How to create a new task in Scheduler
- How to schedule a weekly computer scan
- How to manage notifications and interactive alerts
- How to connect my product to ESET PROTECT On-Prem
  - How to use Override mode
  - How to apply a recommended policy for ESET Endpoint Security
- How to configure a mirror
- How do I upgrade to Windows 10 with ESET Endpoint Security
- How to activate Remote monitoring and management
- How to block the download of specific file types from the internet
- How to minimize the ESET Endpoint Security user interface

If your problem is not included in the help pages listed above, try searching by keyword or phrase describing your problem in the ESET Endpoint Security Help pages.

If you cannot find the solution to your problem/question in the Help pages, visit the ESET Knowledgebase where answers to common questions and issues are available.

- How to uninstall ESET Endpoint Security
- Best practices to protect against Filecoder (ransomware) malware
- ESET Endpoint Security and ESET Endpoint Antivirus FAQ
- What addresses and ports on my third-party firewall should I open to allow full functionality for my ESET product?

If necessary, you can contact our online technical support center with your questions or problems. The link to our online contact form can be found in the **Help and Support** pane in the main program window.

Auto-updates FAQ

For additional information about product updates in ESET Endpoint Security, read the following ESET Knowledgebase article:
- What are the different ESET product update and release types?

Will the computers be updated automatically? Is the update downloaded before or after the restart?

The download happens before the restart, and the updated files are also prepared in this stage. After the restart, the updated files are still only prepared for use, and the currently installed version provides uninterrupted protection. The changes are applied after the next start of ESET Endpoint Security.

I have approximately 3000 computers. Will all of the computers download the updates at the same time? Can I use a proxy for auto-updates with so many computers?

ESET offers the ESET Bridge, Mirror Tool and proxy solutions for larger networks, so updates are downloaded only one time from the internet and then distributed locally. Updates are smaller, typically 5–10 MB, and ESET will throttle updates during the first few weeks of availability. Therefore, not all clients will start the download simultaneously when connected directly to ESET servers.

Can I decide how many or which computers will be updated automatically? I do not want to download more than ten computers per hour, or I only would like to update ten computers for now and another computer after a couple of days.

Managed environments have an auto-update policy where you can specify the latest desired version. Wild cards (for example, 9.0.2032.*) are also supported. For more information, see the Automatic updates chapter in Online Help for ESET PROTECT On-Prem or ESET PROTECT. Unfortunately, there are no other available options to limit auto-updates at this time. You can assign multiple policies for multiple groups.

Are auto-updates configured only by policy? Can I disable the policy if I do not want an ESET product to be updated?

If there is a Security and Stability hotfix for an ESET Endpoint product, the product will be updated even when auto-updates are disabled, as per the terms set in the applicable EULA. ESET uses Security and Stability Hotfixes to address critical issues and ensure maximum security and stability for your ESET product.

You can assign an auto-update policy to any group of endpoints, regardless of their current auto-update configuration. In non-managed environments, the user can locally configure auto-updates in the Advanced setup screen of an ESET Endpoint product.

What if I configure a policy to use the earliest available version? Even then, will ESET update my products?

Hotfixes and critical hotfixes (Security and Stability updates) are slightly different update categories. Regular hotfixes are assigned to auto-update with a standard priority when user settings are accepted. Critical hotfixes are applied top priority, regardless of user settings.

How will updates work in offline scenarios? When are users using the offline repository?

The offline repository also contains .dup and .fup files. The repository section has to be downloaded by the Mirror Tool, not the module update. For additional information, see Offline repository topic in Online Help for ESET PROTECT On-Prem.

How do ESET products know that the update is required? From the repository? Is there data sent to the servers? If ESET plans to make an update one month after a version release, can ESET servers handle a worldwide release?

ESET products download auto-updates from the repository. Servers are ready for that, as critical updates are only a few kilobytes in size. ESET will not throttle critical updates on repository servers. However, there is an option to throttle server updates if the auto-updates are larger. The table below gives examples of hotfix sizes in the event of a differential auto-update.

Previous version	New version	Size
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

If a differential auto-update fails, your ESET product may start a full update. It is still an auto-update with a functionality guarantee, but instead of a .dup file, a larger .fup file will be downloaded. For version 9.0.2032.2, it is 27MB. However, such a scenario is rare.

Will the ESET Endpoint Security update release with throttling? If so, how long is the update throttled after release?

ESET throttles updates for the first few weeks after a new version is released to reduce the load on our servers and distribute the new version evenly.

Auto-updates will become one of the primary methods to upgrade. How does it work in detail?

ESET aims to have as many customers using auto-updates as are able. Having many earlier product versions available is difficult to support. The auto-updates feature works simply—.dup files are downloaded during the first module update check. The product is fully functional during the update procedure and protects the computer. The new version is activated after a restart. In ESET PROTECT On-Prem (server-side), you can use a policy to specify the latest version you want to update to, or use wildcards. For more information, see the Automatic updates chapter in Online Help for ESET PROTECT On-Prem or ESET PROTECT.

Is it correct that auto-updates work on 1/10? I am using ESET Endpoint

Security 8.0.2028.1 now. What version will it update to if auto-updates run?

Updating products using auto-updates may be delayed due to throttling on repository servers. If a product update is released with throttling, automatic update checks may not receive it immediately. If the update is considered safe and stable, throttling may be reduced or removed completely so that all remaining clients receive the update.

The throttling procedure could take a different amount of time for each update. It varies depending on how many clients request the update, the traffic on our servers and other factors. This procedure is always evolving, and changes are happening all the time.

When will the auto-updates begin if I start a computer at 8:45 a.m. and shut it down at 5:00 p.m.?

Auto-updates will start with the next successful scheduled module update, at most one time every 24 hours.

When will the update run next if the computer shuts down while the auto-updates are running?

The update will run at the next scheduled update window. There is a robust fail-safe mechanism for the auto-update (formerly uPCU) procedure. After downloading the update and restarting the computer, the updated files are still prepared for use, and the currently installed version provides uninterrupted protection. The changes are applied after the next start of the ESET Endpoint product.

How can I run auto-updates immediately without waiting for a regular connection every 24 hours? Is there any other way to click Check for updates?

You can manually start the auto-update procedure only when you open the main program window and click **Update** > **Check for updates**. All other ways of starting module updates reflect the 24-hours Auto-update scheduler policy. You cannot remotely start an auto-update download at the moment. We will add this feature in the future.

How to update ESET Endpoint Security

Updating module updates of ESET Endpoint Security can be performed either manually or automatically. To trigger the update, click **Update** in the main program window and then click **Check for updates**.

The default installation settings create an automatic update task which is performed on an hourly basis. To change the interval, navigate to **Tools** > Scheduler.

For more information on product upgrades, see Upgrading to a more recent version.

How to remove a virus from my PC

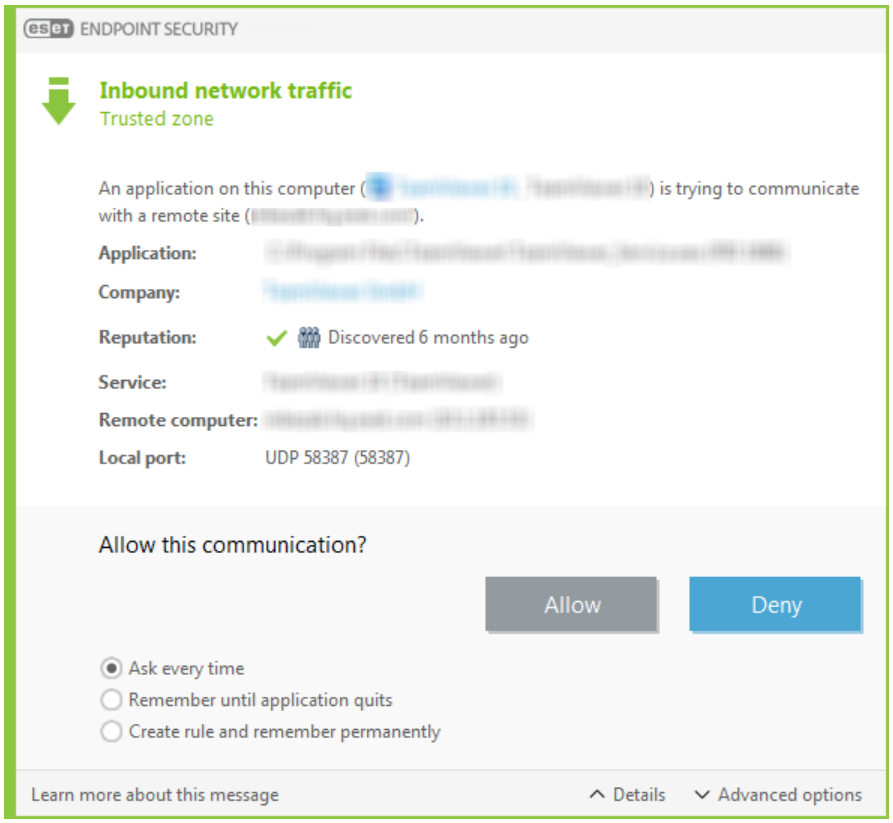
If your computer is showing symptoms of malware infection, for example it is slower, often freezes, we recommend that you do the following:

1. In the main program window, click **Computer scan**.
2. Click **Smart scan** to begin scanning your system.
3. After the scan has finished, review the log with the number of scanned, infected and cleaned files.
4. If you want to only scan a certain part of your disk click **Custom scan** and select targets to be scanned for viruses.

For additional information, see our regularly updated ESET Knowledgebase article.

How to allow communication for a certain application

If a new connection is detected in interactive mode and if there is no matching rule, you will be prompted to allow or deny the connection. If you want ESET Endpoint Security to perform the same action every time the application attempts to establish a connection, select the **Remember action (create rule)** check box.



You can create new firewall rules for applications before they are detected by ESET Endpoint Security in the firewall setup window, open the main program window > **Setup** > **Network** > **Firewall** > click the cogwheel > **Configure** > **Advanced** > **Rules** by clicking **Edit**.

Click **Add** to add the rule. In the **General** tab, type the name, direction and communication protocol for the rule. This window enables you to define the action to be taken when the rule is applied.

Type the path to the application's executable and the local communication port in the **Local** tab. Click the **Remote** tab to type the remote address and port (if applicable). The newly-created rule will be applied as soon as the

application tries to communicate again.

How to create a new task in Scheduler

To create a new task in **Tools** > **Scheduler**, click **Add task** or right-click and select **Add** from the context menu. Five types of scheduled tasks are available:

- **Run external application**—Schedules the execution of an external application.
- **Log maintenance**—Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check**—Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot**—Creates an ESET SysInspector computer snapshot—gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan**—Performs a computer scan of files and folders on your computer.
- **Update**—Schedules an Update task by updating modules.

Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task below:

From the **Scheduled task** drop-down menu, select **Update**. Type the name of the task into the **Task name** field and click **Next**. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered. Select Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. Next, define the action to take if the task cannot be performed or completed at the scheduled time. The following options are available:

- **At the next scheduled time**
- **As soon as possible**
- **Immediately, if time since last exceeds a specified value** (the interval can be defined using the **Time since last run** scroll box)

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

A dialog window will appear, enabling you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of currently scheduled tasks.

How to schedule a weekly computer scan

To schedule a regular task, open the main program window > **Tools** > **Scheduler**. Below is a short guide on how to schedule a task that will scan your local drives every week. See our Knowledgebase article for more detailed instructions.

To schedule a scan task:

1. Click **Add task** in the main Scheduler screen.

2. Select **On-demand computer scan** from the drop-down menu.
3. Type a name for the task and select **Weekly for the task frequency**.
4. Set the day and time the task will execute.
5. Select **Run the task as soon as possible** to perform the task later if the scheduled task does not run for any reason (for example, if the computer was turned off).
6. Review the summary of the scheduled task and click **Finish**.
7. From the **Targets** drop-down menu, select **Local drives**.
8. Click **Finish** to apply the task.

How to connect ESET Endpoint Security to ESET PROTECT On-Prem

When you have installed ESET Endpoint Security on your computer and you want to connect via ESET PROTECT On-Prem, ensure that you have also installed ESET Management Agent on your client workstation. It is an essential part of every client solution that communicates with ESET PROTECT On-Prem Server.

- Install or deploy ESET Management Agent on client workstations

See also:

- Documentation for endpoints managed remotely
- How to use Override mode
- How to apply a recommended policy for ESET Endpoint Security

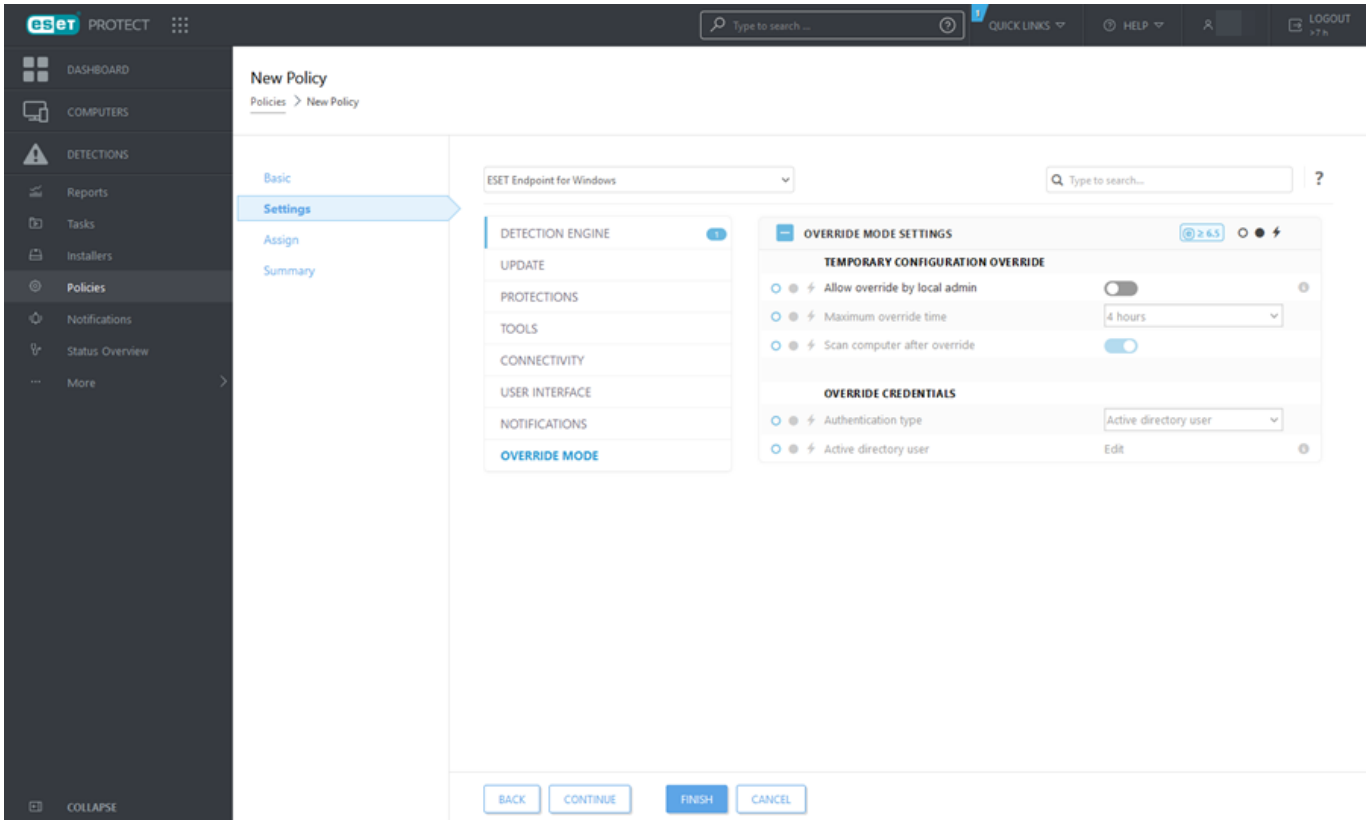
How to use Override mode

Users with ESET Endpoint products (version 6.5 and above) for Windows installed on their machine can use the Override feature. Override mode enables users on the client-computer level to change settings in the installed ESET product, even if there is a policy applied over these settings. Override mode can be enabled for certain AD users, or it can be password-protected. The function can not be enabled for more than four hours at once.

Override mode cannot be stopped from the ESET PROTECT On-Prem Web Console when enabled. Override mode will be disabled automatically when the override time period expires. It can also be turned off on the client machine.
The user who is using the Override mode needs to have Windows admin rights too. Otherwise, the user can not save the changes in settings of ESET Endpoint Security.
Active Directory group authentication is supported.

To set the **Override mode**:

1. Navigate to **Polices** > **New Policy**.
2. In the **Basic** section, type in a **Name** and **Description** for this policy.
3. In the **Settings** section, select **ESET Endpoint for Windows**.
4. Click **Override mode** and configure rules for override mode.
5. In the **Assign** section, select the computer or group of computers on which this policy will be applied.
6. Review the settings in the **Summary** section and click **Finish** to apply the policy.



If *John* has a problem with his endpoint settings blocking some important functionality or web access on his machine, the Administrator can allow *John* to override his existing endpoint policy and tweak the settings manually on his machine. Afterward, these new settings can be requested by ESET PROTECT On-Prem so the Administrator can create a new policy out of them.

To do so, follow the steps below:

1. Navigate to **Polices** > **New Policy**.
2. Complete the **Name** and **Description** fields. In the **Settings** section, select **ESET Endpoint for Windows**.
3. Click **Override mode**, enable the override mode for one hour and select *John* as the AD user.
4. Assign the policy to *John's computer* and click **Finish** to save the policy.
5. *John* has to enable the **Override mode** on his ESET endpoint and change the settings manually on his machine.
6. On the ESET PROTECT On-Prem Web Console, navigate to **Computers**, select *John's computer* and click **Show Details**.
7. In the **Configuration** section, click **Request configuration** to schedule a client task to get the configuration from the client ASAP.
8. After short time, the new configuration will appear. Click the product which settings you want to save and then click **Open Configuration**.
9. You can review settings and then click **Convert to policy**.
10. Complete the **Name** and **Description** fields.
11. In the **Settings** section, you can modify the settings if needed.
12. In the **Assign** section, you can assign this policy to *John's computer* (or others).
13. Click **Finish** to save the settings.
14. Do not forget to remove the override policy when no longer needed.

How to apply a recommended policy for ESET Endpoint

Security

The best practice after connecting ESET Endpoint Security to ESET PROTECT On-Prem is to apply a recommended policy or apply a custom one.

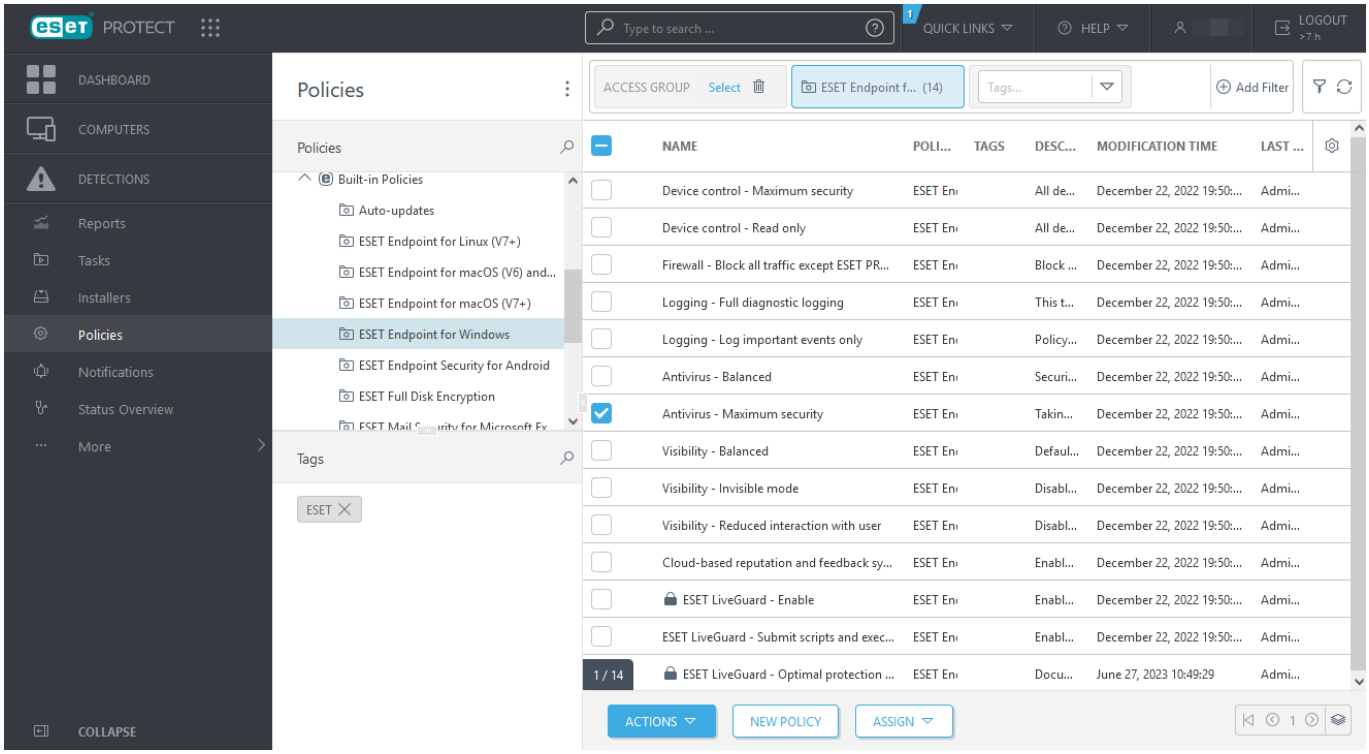
There are several built-in policies for ESET Endpoint Security:

Policy	Description
Antivirus—Balanced	Security configuration recommended for most of the setups.
Antivirus—Maximum security	Taking advantage of machine learning, deep behavioral inspection and SSL filtering. Detection of potentially unsafe, unwanted and suspicious applications are affected.
Cloud-based reputation and feedback system	Enables ESET LiveGrid® cloud-based reputation as well as feedback system to improve detection of latest threats and help sharing malicious or unknown potential threats for further analysis.
Device control—Maximum security	All devices are blocked. When any device wants to be connected, it needs to be allowed by an admin.
Device Control—Read-only	All devices can only be read. No write is allowed.
Firewall—Block all traffic except ESET PROTECT On-Prem & ESET Inspect connection	Block all traffic except connection to ESET PROTECT On-Prem and ESET Inspect Server (ESET Endpoint Security only).
Logging—Full diagnostic logging	This template will ensure that the administrator will have all logs available, when needed. Everything will be logged from minimum verbosity including HIPS and ThreatSense, Firewall. Logs are automatically deleted after 90 days.
Logging—Log important events only	Policy ensures that warnings, errors and critical events will be logged. Logs are automatically deleted after 90 days.
Visibility—Balanced	Default setting for visibility. Statuses and notifications are enabled.
Visibility—Invisible mode	Disabled notifications, alerts, GUI, integration to context menu. No egui.exe will run. Suitable for management solely from ESET PROTECT.
Visibility—Reduced interaction with user	Disabled statuses, disabled notifications, GUI presented.

To set the policy named as **Antivirus - Maximum security** which enforces more than 50 recommended settings for ESET Endpoint Security installed on your workstations, follow these steps:

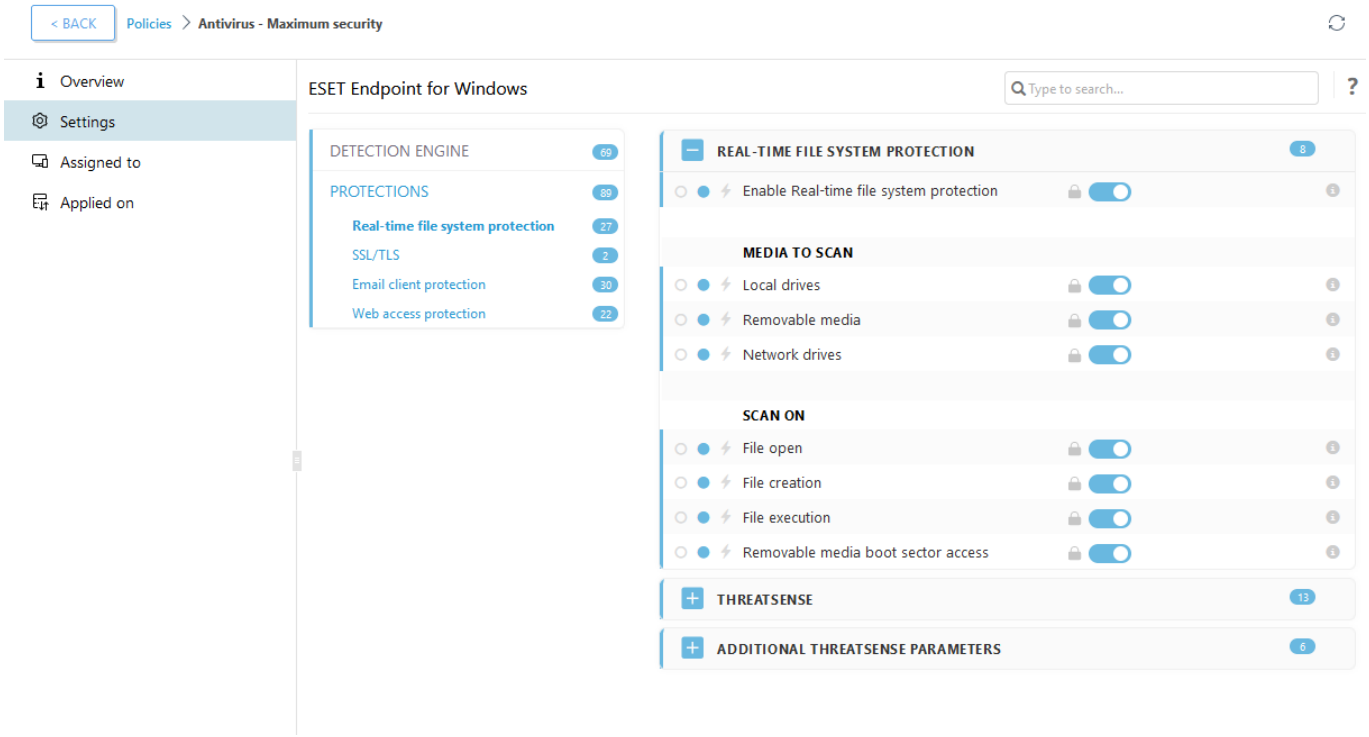
> The following ESET Knowledgebase article may only be available in English:
> Apply a recommended or pre-defined policy for ESET Endpoint Security using ESET PROTECT On-Prem

1. Open the ESET PROTECT On-Prem Web Console.
2. Navigate to **Polices** and expand **Built-in Policies** > **ESET Endpoint for Windows**.
3. Click **Antivirus - Maximum security - recommended**.
4. In the **Assigned to** tab click **Assign client(s)** or **Assign groups(s)** and select the appropriate computers for which you want to apply this policy.



To see which settings are applied for this policy, click the **Settings** tab and expand the Advanced setup tree.

- The blue dot represents an altered setting for this policy
- The number in the blue frame represents a number of altered settings by this policy
- Read more about ESET PROTECT On-Prem policies



How to configure a mirror

ESET Endpoint Security can be configured to store copies of detection engine update files and distribute updates to other workstations running ESET Endpoint Antivirus or ESET Endpoint Security.

Update mirror creates copies of update files that can be used to update workstations that are running the same generation of the ESET Endpoint Security for Windows (for example, ESET Endpoint Security for Windows version 10.x creates update files only for version 10.x ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows).

Configuring ESET Endpoint Security as a Mirror server to provide updates via an internal HTTP server

1. Press **F5** to access Advanced setup and expand **Update** > **Profiles** > **Update Mirror**.
2. Expand **Updates** and ensure the **Choose automatically** option under **Modules updates** is enabled.
3. Expand **Update mirror** and enable **Create update mirror** and **Enable HTTP server**.

For more information, see:
- Update mirror
- Updating from the Mirror

Configuring a Mirror server to provide updates via a shared network folder

1. Create a shared folder on a local or network device. This folder must be readable by all users running ESET security solutions and writable from the local SYSTEM account.
2. Activate **Create update mirror** under **Advanced setup** > **Update** > **Profiles** > **Update Mirror**.
3. Choose an appropriate **Storage folder** by clicking **Clear** and then **Edit**. Browse and select the created shared folder.

If you do not want to provide module updates via the internal HTTP server, disable **Enable HTTP server**.

How do I upgrade to Windows 10 with ESET Endpoint Security

We highly recommend that you upgrade to the latest version of your ESET product, then download the latest module updates, before upgrading to Windows 10. This will ensure maximum protection and preserve your program settings and license information during the upgrade to Windows 10.

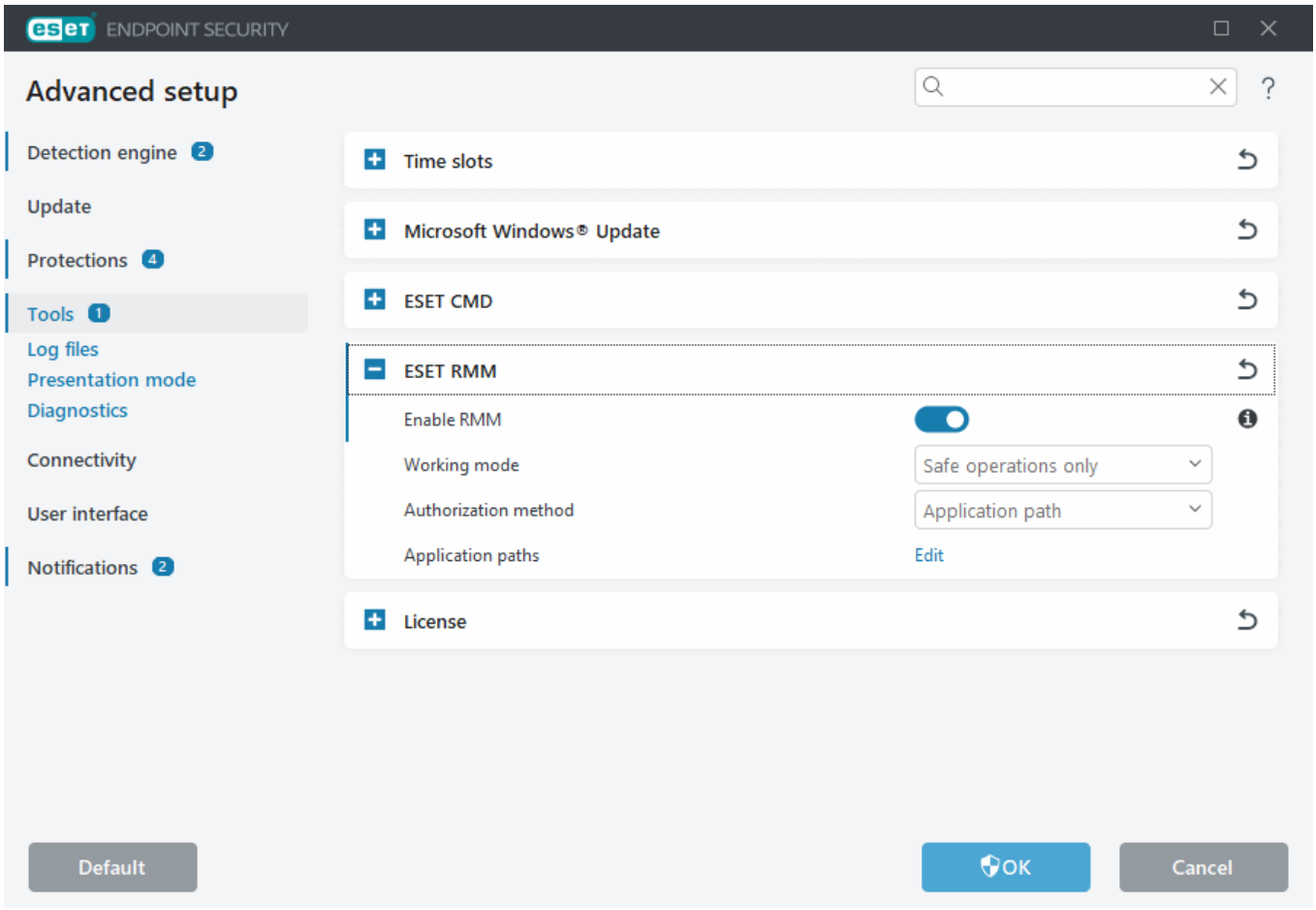
Other language versions:

If you are looking for another language version of your ESET endpoint product, visit our download page.

More information about compatibility of ESET business products with Windows 10.

How to activate Remote monitoring and management

Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems (such as those on desktops, servers and mobile devices) using a locally installed agent that can be accessed by a management service provider. ESET Endpoint Security can be managed by RMM from the version 6.6.2028.0.



By default, ESET RMM is disabled. To enable ESET RMM, open Advanced setup > **Tools** > **ESET RMM** and enable the toggle next to **Enable RMM**.

Working mode—Select **Safe operations only** if you want to enable RMM interface for safe and read-only operations. Select **All operations** if you want to enable RMM interface for all operations.

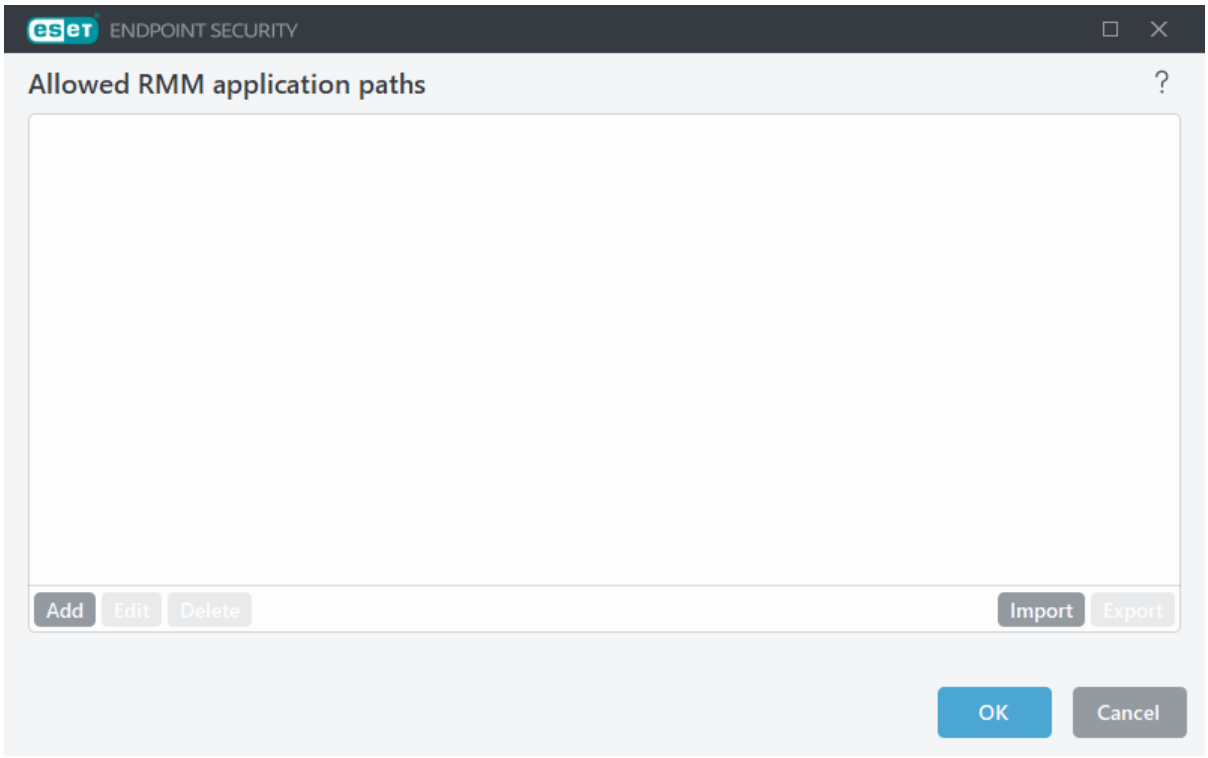
Operation	Mode Safe operations only	Mode All operations
Get application info	✔	✔
Get configuration	✔	✔
Get license info	✔	✔
Get logs	✔	✔
Get protection status	✔	✔
Get update status	✔	✔
Set configuration		✔
Start activation		✔
Start scan	✔	✔

Operation	Mode Safe operations only	Mode All operations
Start update	✔	✔

Authorization method—Set the RMM authorization method. To use authorization, select **Application path** from the drop-down menu, otherwise select **None**.

RMM should always use authorization to prevent malicious software from disabling or circumventing ESET Endpoint protection.

Application paths—Specific application which is allowed to run RMM. If you have selected **Application path** as an authorization method, click **Edit** to open the **Allowed RMM application paths** configuration window.



Add—Create a new allowed RMM application path. Type the path or click the **…** button to select an executable.

Edit—Modify an existing allowed path. Use **Edit** if the location of the executable has changed to another folder.

Delete—Delete an existing allowed path.

Default ESET Endpoint Security installation contains file ermm.exe located in Endpoint application directory (default path C*:\Program Files\ESET\ESET Security*). The file ermm.exe exchange data with RMM Plugin, which communicates with RMM Agent, linked to a RMM Server.

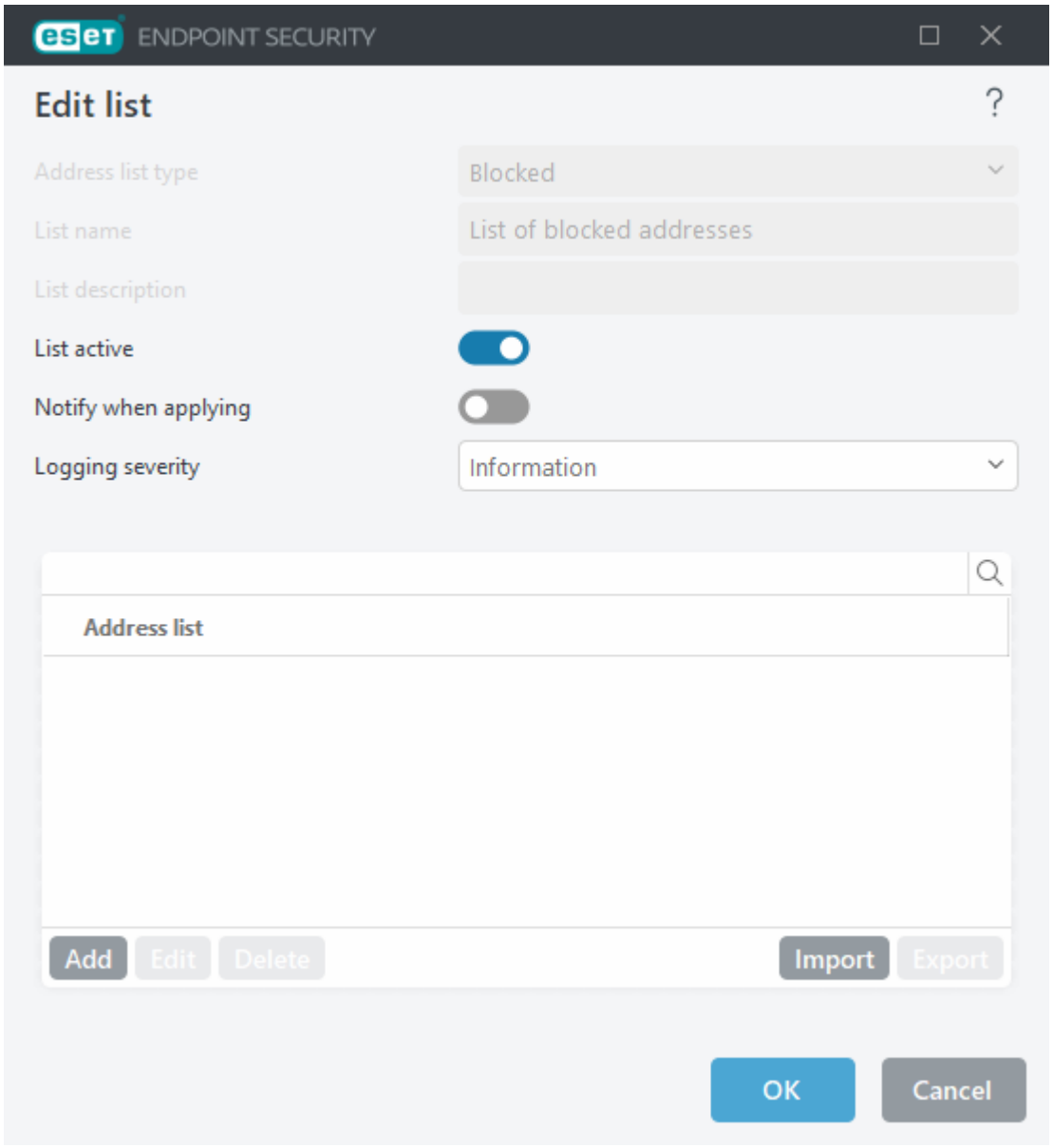
- ermm.exe—command line utility developed by ESET that allows managing of Endpoint products and communication with any RMM Plugin.
- RMM Plugin is a third party application running locally on Endpoint Windows system. The plugin was designed to communicate with specific RMM Agent (e.g. Kaseya only) and with ermm.exe.
- RMM Agent is a third party application (e.g. from Kaseya) running locally on Endpoint Windows system. Agent communicates with RMM Plugin and with RMM Server.

How to block the download of specific file types from the internet

If you do not want to allow downloading of specific file types (f.e. exe, pdf or zip) from the internet, use URL Address management with a combination of wildcards. Press the F5 key to access **Advanced setup**. Click **Web and Email** > **Web access protection** and expand **URL Address Management**. Click **Edit** next to **Address list**.

In the **Address list** window, select **List of blocked addresses** and click **Edit** or **Add** to create/edit a list. A new window opens. If you are creating a new list, select **Blocked** from the **Address list type** drop-down menu and name the list. If you want to be notified when accessing a file type from the current list, enable the **Notify when applying** toggle. Select the **Logging severity** from the drop-down menu. ESET PROTECT On-Prem can collect records with **Warning** verbosity.

Information and Warning logging verbosity is available only for rules which contain at least two components without wildcards within the domain. For example:
- *.domain.com/*
- *www.domain.com/*



Click **Add** to type a mask that specifies file types you want to block from downloading. Type the full URL if you want to block the download of a specific file from a specific website, for example, *http://example.com/file.exe*. You can use wildcards to cover a group of files. A question mark (?) represents a single variable character, whereas an asterisk (*) represents a variable string of zero or more characters. For example, the mask **/*.zip* blocks all compressed zip files from being downloaded.

Note that you can only block the download of specific file types using this method when the file extension is the part of the file URL. If the web page uses file download URLs, for example, *www.example.com/download.php?fileid=42*, any file located at this link would be downloaded even if it has an extension that you blocked.

How to minimize the ESET Endpoint Security user interface

When managed remotely, you can apply a "Visibility" pre-defined policy.

If not, perform the steps manually:

1. Press **F5** to access Advanced setup and expand **User interface** > **User interface elements**.
2. Set **Start mode** to the desired value. More information about start modes.
3. Disable **Show splash-screen at startup** and **Use sound signal**.
4. Configure Notifications.
5. Configure Application statuses.
6. Configure Confirmation messages.
7. Configure Alerts and message boxes.

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of

Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software.** The Provider shall be entitled from time 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.

b) **Forwarding of infiltrations and information to the Provider.** 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 ("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, information about the operations and functionality of the Software ("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 following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations

to Provider. This function is enabled under the Software's standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of 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, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

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; 3537.0

Privacy Policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Update and other statistics covering information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, IP address, MAC address, configuration settings of product.
- One-way hashes related to infiltrations as part of ESET LiveGrid® Reputation System which improves the efficiency of our anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.
- Suspicious samples and metadata from the wild as part of ESET LiveGrid® Feedback System which enables ESET to react immediately to needs of our end users and keep us responsive to the latest threats providing. We are dependent on You sending us
  - infiltrations such as potential samples of viruses and other malicious programs and suspicious; problematic, potentially unwanted or potentially unsafe objects such as executable files, email messages reported by You as spam or flagged by our product;
  - information about devices in local network such as type, vendor, model and/or name of device;

- information concerning the use of internet such as IP address and geographic information, IP packets, URLs and ethernet frames;
- crash dump files and information contained.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it. Accidentally collected data may be included in malware itself (collected without your knowledge or approval) or as part of filenames or URLs and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

- Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.
- Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject’s Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

- right to request access to your personal data from ESET,
- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),
- right to request erasure of your personal data,
- right to request restriction of processing your personal data,

- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

We believe that every information we process is valuable and necessary for the purpose of our legitimate interest which is provision of services and products to our customers.

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