ESET Endpoint Security

User guide

Click here to display the online version of this document

Copyright ©2023 by ESET, spol. s r.o.

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

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

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

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

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

REV. 3/19/2023

1 ESET Endpoint Security 7 ... 1
1.1 What's new in version 7 ... 2
1.2 System requirements ... 3
1.2 Supported languages ... 4
1.3 Prevention ... 5
1.4 Help pages ... 6
2 Documentation for endpoints managed remotely ... 7
2.1 Introduction to ESET Security Management Center ... 8
2.2 Introduction to ESET PROTECT Cloud ... 9
2.3 Password protected settings ... 9
2.4 What are policies ... 10
2.4 Merging policies ... 11
2.5 How flags work ... 11
3 Using ESET Endpoint Security by itself ... 12
3.1 Installation methods ... 12
3.1 Installation with ESET AV Remover ... 13
3.1 ESET AV Remover ... 13
3.1 Uninstallation using ESET AV Remover ended with error ... 16
3.1 Installation (.exe) ... 16
3.1 Change installation folder (.exe) ... 18
3.1 Installation (.msi) ... 19
3.1 Advanced installation (.msi) ... 21
3.1 Command-line installation ... 23
3.1 Deployment using GPO or SCCM ... 28
3.1 Upgrading to a more recent version ... 30
3.1 Common installation problems ... 31
3.1 Activation failed ... 31
3.2 Product activation ... 31
3.3 Computer scan ... 32
3.4 Beginner's guide ... 32
3.4 The user interface ... 32
3.4 Update setup ... 36
3.4 Zones setup ... 38
3.4 Web control tools ... 39
4 Work with ESET Endpoint Security ... 39
4.1 Computer ... 42
4.1 Detection engine (7.2 and later) ... 43
4.1 Detection engine advanced options ... 48
4.1 Detection engine (7.1 and below) ... 48
4.1 An infiltration is detected ... 49
4.1 Shared local cache ... 51
4.1 Real-time file system protection ... 51
4.1 Checking real-time protection ... 53
4.1 When to modify real-time protection configuration ... 53
4.1 What to do if real-time protection does not work ... 53
4.1 Computer scan ... 54
4.1 Custom scan launcher ... 56
4.1 Scan progress ... 57
4.1 Computer scan log ... 59
4.1 Malware scans ... 59

4.1 Idle-state scan 60
4.1 Scan profiles 60
4.1 Scan targets 61
4.1 Advanced scan options 61
4.1 Device control 62
4.1 Device control rules editor 63
4.1 Detected devices 64
4.1 Device groups 64
4.1 Adding Device control rules 65
4.1 Host-based Intrusion Prevention System (HIPS) 67
4.1 HIPS interactive window 69
4.1 Potential ransomware behavior detected 70
4.1 HIPS rule management 71
4.1 HIPS rule settings 72
4.1 HIPS advanced setup 75
4.1 Drivers always allowed to load 75
4.1 Presentation mode 76
4.1 Startup scan 76
4.1 Automatic startup file check 77
4.1 Document protection 77
4.1 Exclusions 78
4.1 Performance exclusions 78
4.1 Add or Edit performance exclusion 79
4.1 Path exclusion format 81
4.1 Detection exclusions 82
4.1 Add or Edit detection exclusion 84
4.1 Create detection exclusion wizard 86
4.1 Exclusions (7.1 and below) 86
4.1 Processes exclusions 87
4.1 Add or Edit processes exclusions 88
4.1 HIPS exclusions 88
4.1 ThreatSense parameters 89
4.1 Cleaning levels 92
4.1 File extensions excluded from scanning 94
4.1 Additional ThreatSense parameters 94
4.2 Network 95
4.2 Firewall 96
4.2 Learning mode 98
4.2 Network attack protection 99
4.2 Advanced filtering options 100
4.2 IDS exceptions 103
4.2 Suspected threat blocked 105
4.2 Network protection troubleshooting 106
4.2 Connected networks 106
4.2 Known networks 107
4.2 Known networks editor 107
4.2 Network authentication - Server configuration 110
4.2 Firewall profiles 111
4.2 Profiles assigned to network adapters 111
4.2 Application modification detection 112
4.2 Applications excluded from modification detection 112

4.2 Configuring and using rules 112
4.2 Firewall rules list 113
4.2 Adding or editing Firewall rules 114
4.2 Firewall rule - Local 116
4.2 Firewall rule - Remote 117
4.2 Temporary IP address blacklist 118
4.2 Trusted zone 118
4.2 Configuring zones 119
4.2 Firewall zones 119
4.2 Firewall log 120
4.2 Establishing connection - detection 120
4.2 Solving problems with ESET Firewall 121
4.2 Troubleshooting wizard 122
4.2 Logging and creating rules or exceptions from log 122
4.2 Create rule from log 122
4.2 Creating exceptions from firewall notifications 122
4.2 Advanced PCAP logging 123
4.2 Solving problems with protocol filtering 123
4.3 Web and email 124
4.3 Protocol filtering 126
4.3 Excluded applications 126
4.3 Excluded IP addresses 127
4.3 SSL/TLS 128
4.3 Certificates 129
4.3 Encrypted network traffic 130
4.3 List of known certificates 130
4.3 List of SSL/TLS filtered applications 131
4.3 Email client protection 131
4.3 Email protocols 133
4.3 Email alerts and notifications 134
4.3 Integration with email clients 135
4.3 Microsoft Outlook toolbar 135
4.3 Outlook Express and Windows Mail toolbar 135
4.3 Confirmation dialog 136
4.3 Rescan messages 136
4.3 Antispam protection 137
4.3 Antispam address books 138
4.3 Blacklist/Whitelist/Exceptions list 139
4.3 Add/Edit Blacklist/Whitelist/Exceptions address 140
4.3 Web access protection 140
4.3 Web access protection advanced setup 143
4.3 Web protocols 143
4.3 URL address management 144
4.3 URL addresses list 145
4.3 Create new URL address list 146
4.3 How to add URL mask 147
4.3 Anti-Phishing protection 147
4.4 Web control 149
4.4 Web control rules 150
4.4 Adding Web control rules 150
4.4 Category groups 152

4.4 URL groups ... 153
4.4 Blocked webpage message customization ... 155
4.5 Updating the program ... 157
4.5 Update setup ... 161
4.5 Update rollback ... 164
4.5 Program component update ... 165
4.5 Connection options ... 166
4.5 Update mirror ... 167
4.5 HTTP Server and SSL for the Mirror ... 169
4.5 Updating from the Mirror ... 169
4.5 Troubleshooting Mirror update problems ... 171
4.5 How to create update tasks ... 172
4.6 Tools ... 172
4.6 Log files ... 173
4.6 Log filtering ... 176
4.6 Logging configuration ... 177
4.6 Audit logs ... 178
4.6 Scheduler ... 179
4.6 Protection statistics ... 182
4.6 Watch activity ... 182
4.6 ESET SysInspector ... 183
4.6 Cloud-based protection ... 184
4.6 Exclusion filter for Cloud-based protection ... 187
4.6 Running processes ... 188
4.6 Security report ... 189
4.6 Network connections ... 191
4.6 ESET SysRescue Live ... 193
4.6 Submission of samples for analysis ... 193
4.6 Select sample for analysis - Suspicious file ... 194
4.6 Select sample for analysis - Suspicious site ... 194
4.6 Select sample for analysis - False positive file ... 195
4.6 Select sample for analysis - False positive site ... 195
4.6 Select sample for analysis - Other ... 195
4.6 Notifications ... 196
4.6 Application notifications ... 197
4.6 Desktop notifications ... 198
4.6 Email notifications ... 199
4.6 Customization of notifications ... 201
4.6 Quarantine ... 201
4.6 Proxy server setup ... 203
4.6 Time slots ... 204
4.6 Microsoft Windows update ... 205
4.6 License interval check ... 206
4.7 User interface ... 206
4.7 User interface elements ... 206
4.7 Application statuses ... 208
4.7 Access setup ... 209
4.7 Password for Advanced setup ... 210
4.7 Alerts and message boxes ... 210
4.7 Interactive alerts ... 212
4.7 Confirmation messages ... 214

4.7 Advanced settings conflict error 214
4.7 Restart required 214
4.7 Restart recommended 216
4.7 Removable media 218
4.7 System tray icon 219
4.7 Context menu 220
4.7 Help and support 220
4.7 About ESET Endpoint Security 221
4.7 Submit system configuration data 222
4.7 Profile manager 222
4.7 Keyboard shortcuts 223
4.7 Diagnostics 224
4.7 Command line scanner 225
4.7 ESET CMD 227
4.7 Idle-state detection 230
4.7 Import and export settings 230
4.7 Revert all settings to default 231
4.7 Revert all settings in current section 231
4.7 Error while saving the configuration 231
4.7 Remote monitoring and management 232
4.7 ERMM Command Line 233
4.7 List of ERMM JSON commands 234
4.7 get protection-status 235
4.7 get application-info 236
4.7 get license-info 238
4.7 get logs 238
4.7 get activation-status 240
4.7 get scan-info 240
4.7 get configuration 241
4.7 get update-status 242
4.7 start scan 243
4.7 start activation 244
4.7 start deactivation 245
4.7 start update 246
4.7 set configuration 247
5 Common Questions 247
5.1 How to update ESET Endpoint Security 248
5.2 How to activate ESET Endpoint Security 249
5.2 Entering your License Key during activation 249
5.2 Login to ESET Business Account 250
5.2 How to use legacy license credentials to activate a newer ESET endpoint product 250
5.3 How to remove a virus from my PC 250
5.4 How to allow communication for a certain application 251
5.5 How to create a new task in Scheduler 251
5.5 How to schedule a weekly computer scan 252
5.6 How to connect ESET Endpoint Security to ESET Security Management Center 253
5.6 How to use Override mode 253
5.6 How to apply a recommended policy for ESET Endpoint Security 255
5.7 How to configure a mirror 257
5.8 How do I upgrade to Windows 10 with ESET Endpoint Security 257
5.9 How to activate Remote monitoring and management 258

5.10 How to block the download of specific file types from the Internet 260
5.11 How to minimize the ESET Endpoint Security user interface 261
6 End User License Agreement 262
7 Privacy Policy 268

ESET Endpoint Security 7

ESET Endpoint Security 7 represents a new approach to truly integrated computer security. The most recent version of the ThreatSense® scanning engine, combined with our custom Firewall and 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 7 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 7 is primarily designed for use on workstations in a small business environment.

In the Using ESET Endpoint Security by itself 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 Security Management Center in an enterprise environment allows 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.
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 works by monitoring 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 Security Management Center allows you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location. Using the ESET Security Management Center Web Console (ESMC 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 lets you block webpages 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 in version 7

ESET Endpoint Security 7 has been released and is available to download.

What's new in ESET Endpoint Security 7.0

- New design of graphical user interface.
- Drag and drop files scan – You can scan a file or folder manually just by moving the file or folder to the marked area.
- Network attack protection is now available in ESET Endpoint Antivirus. For more information, see Network attack protection.
- In Protection status, quick action link can be disabled by ESET Security Management Center policy.
- Device control rules and Web control rules can be applied now for a certain time period. For more information, see Time slots.

What's new in ESET Endpoint Security 7.1

- New type of logging – Advanced type of logging is now available. For more information, see Audit logs.

What's new in ESET Endpoint Security 7.2

- Advanced machine learning is an advanced layer of protection that improves detection based on machine learning. Read more about this type of protection in the Glossary. The Detection engine setup no longer provides ON/OFF switches as for version 7.1 and below. ON/OFF buttons are replaced with four thresholds - "Aggressive", "Balanced", "Cautious" and "Off".
- Latvian localization added.
- Changes to exclusions. Performance exclusions allow you to exclude files and folders from scanning. Detection exclusions allow you to exclude objects from cleaning using the detection name, path or its hash.
- New HIPS program module includes Deep Behavioral Inspection, which analyzes the behavior of all programs running on the computer and warns you if the behavior of the process is malicious. Find more about HIPS in our help pages.
- Configurable interactive alerts allows you to adjust behavior for configurable interactive alerts (for example, hide the "Restart recommended" alert on endpoint machines).

What's new in ESET Endpoint Security 7.3

- This minor release comes with various bug fixes and performance improvements.

For additional information and screenshots about the new features in ESET Endpoint Security please read the following ESET Knowledgebase article:

- What's new in ESET Endpoint Security 7?

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 64bit (x64), 1 GHz or higher

Operating Systems

Microsoft® Windows® 10

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

Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 with latest Windows updates (at least KB4474419 and KB4490628)

Windows XP and Windows Vista is no longer supported for version 7.

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 1024x768
- Internet connection or a local area network connection to a source (see Note 3) of product updates

Although it might be possible to install and run the product on systems that do not meet these requirements, we recommend prior usability testing to be done based on performance requirements.

> **Note**
> **(1):** The product might use more memory if the memory would be otherwise unused on a heavily infected computer or when huge lists of data are being imported into the product (e.g. URL white lists).
> **(2):** The disk space needed to download the installer, install the product and to keep a copy of the installation package in program data as well as backups of product updates to support the rollback feature. The product might use more disk space under different settings (e.g. when more product update backup versions are stored, memory dumps or huge amounts of log records are kept) or on an infected computer (e.g. due to the quarantine feature). We recommend to keep enough free disk space to support the updates of the operating system and for ESET product updates.
> **(3):** Although not recommended, the product might be updated manually from a 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
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	nn-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
*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).

Prevention

When you work with your computer, and especially when you browse the Internet, please keep in mind that no antivirus system in the world can completely eliminate the risk of detections and remote attacks. To provide maximum protection and convenience, it is essential that you 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 in order to bypass existing security measures and bring profit to their authors – all at the expense of other users. The specialists at the ESET Virus Lab analyze these threats on a daily basis and prepare and release updates in order to continually improve the level of protection for our users. To ensure the maximum effectiveness of these updates it is important that updates are configured properly on your system. For more information on how to configure updates, see the Update setup chapter.

Download security patches

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

Back up important data

Malware writers usually do not care about user’s needs, and the activity of malicious programs often leads to

total malfunction of an operating system and the loss of of important data. It is important to regularly back up your important and sensitive 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 system failure.

Regularly scan your computer for viruses

Detection of more known and unknown viruses, worms, trojans and rootkits are handled by the Real-time file system protection module. This means that every time you access or open a file, it is scanned for a 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 each day.

Follow basic security rules

This is the most useful and most effective rule of all – always be cautious. Today, many infiltrations require user intervention in order to be executed and distributed. If you are cautious when opening new files, you will save considerable time and effort that would otherwise 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, particularly those from mass-mailed messages and messages from unknown senders.
- Don't use an Administrator account for everyday work on your computer.

Help pages

Welcome to the ESET Endpoint Security help files. The information provided here will familiarize you with your product and help you make your computer more secure.

Getting started

Before you start using ESET Endpoint Security please note that our product can be used by users connected via ESET Security Management Center or by itself. 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 particular 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 particular interest or significance.

Note
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.

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

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

Example
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 Security Management Center or ESET PROTECT Cloud.

- Introduction to ESET Security Management Center
- Introduction to ESET PROTECT Cloud

Third-party remote management tools

- Remote monitoring and management (RMM)

Best practices

- Connect all endpoints with ESET Endpoint Security to ESET Security Management Center
- 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 Security Management Center

ESET Security Management Center allows you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location.

ESET Security Management Center (ESMC) is a new generation of remote management system that differs significantly from previous versions of ESET Remote Administrator (ERA). Since the architecture is completely different, ESET Security Management Center 7 is only partially compatible with ERA 6 and there is no backward compatibility with ERA 5. However, compatibility with previous versions of ESET Security products remains.

To perform a complete deployment of the ESET security solutions portfolio, the following components must be installed (Windows and Linux platforms):

- ESMC Server
- ESMC Web Console
- ESET Management Agent

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

- RD Sensor
- Apache HTTP Proxy
- Mobile Device Connector

Using the ESET Security Management Center Web Console (ESMC 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.

> **More information**
> For more information please see the ESET Security Management Center Online user guide.

Introduction to ESET PROTECT Cloud

ESET PROTECT Cloud allows 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 ESMC. Using the ESET PROTECT Cloud, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

- Read more about this in the ESET PROTECT Cloud Online user guide

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 ESMC 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**.

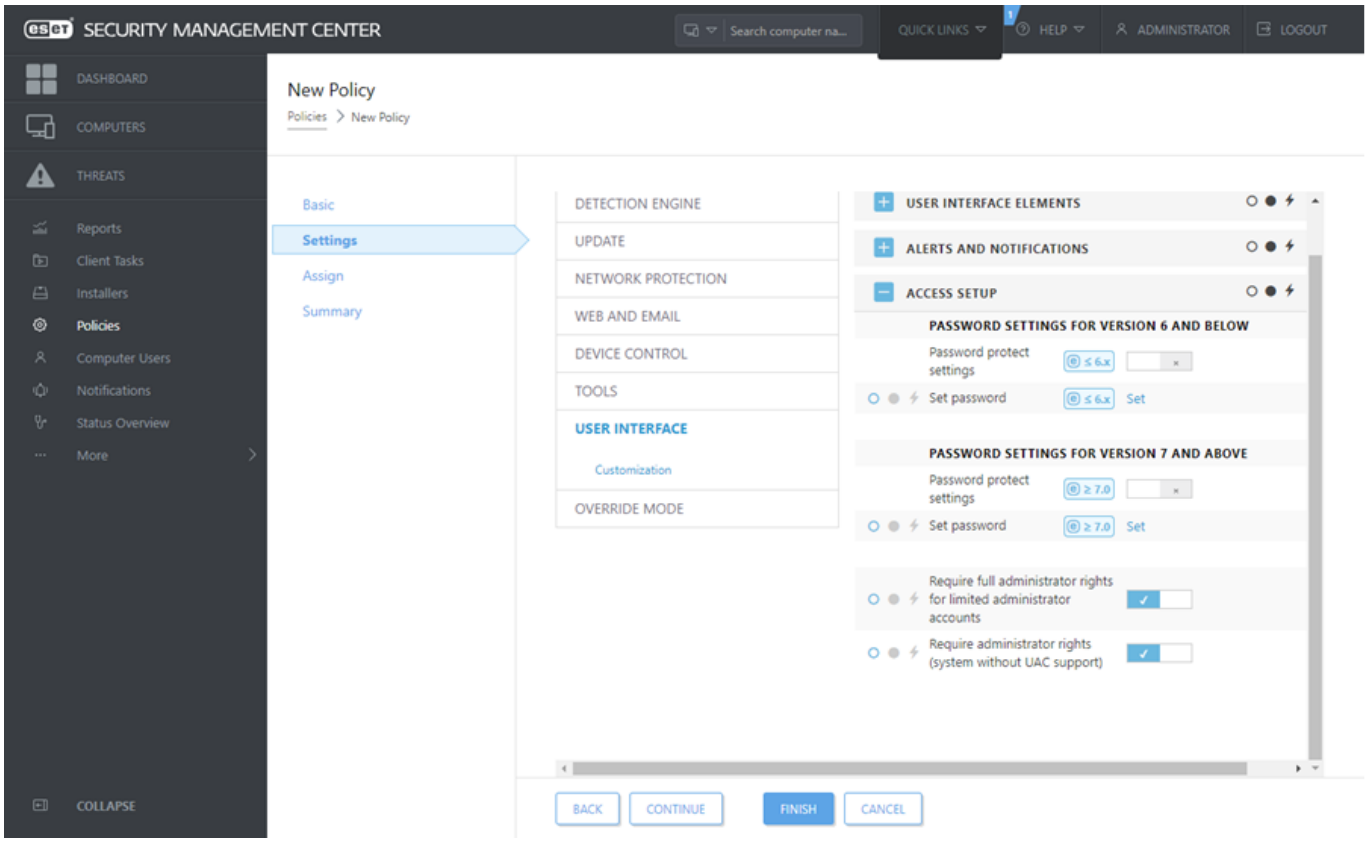
6. According to a version of ESET Endpoint Security, click the slider bar to enable **Password to protect settings**. Note that ESET Endpoint products version 7 offers enhanced protection. If you have both version 7 and version 6 of Endpoint products in the network, set a different password for each. We recommend that you do not set the password only in the filed for version 6 as it will lower the security on Endpoint products with version 7.

7. In the pop-up 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 ESMC Web Console. A policy can be applied directly to individual computers as well as to groups of computers. You can also assign multiple policies to a computer or to 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 that Static Groups are arranged. This is not true for Dynamic Groups, where policies are applied to child Dynamic Groups first. This allows you to apply policies with greater impact to the top of the Group tree and apply 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 ESMC Online user guide.

> **Assign more generic policies**
> We recommend that you assign more generic policies (for example, the update server policy) to groups that are higher 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 ESMC 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 won't 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.

EXAMPLE: Allow users to see all policies

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**.

Using ESET Endpoint Security by itself

This section and the Work with ESET Endpoint Security section of this User Guide is intended for users who are using ESET Endpoint Security without ESET Security Management Center or ESET PROTECT Cloud. All features and functionalities of ESET Endpoint Security are fully accessible depending on a user's account rights.

Installation methods

There are several ESET Endpoint Security version 7.x installation methods on a client workstation, unless you deploy ESET Endpoint Security remotely to client workstations via ESET Security Management Center or ESET PROTECT Cloud.

- Click here if you want to install or upgrade ESET Endpoint Security to version 6.6.x

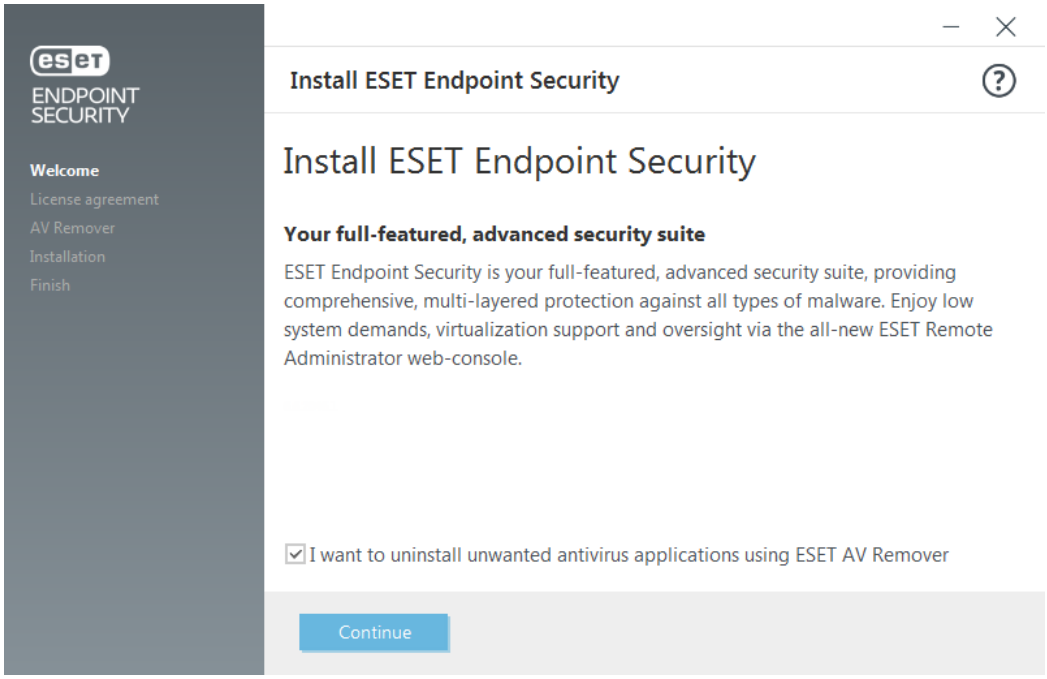
Method	Purpose	Download link
Installation with ESET AV Remover	The ESET AV Remover tool will help you to remove almost any antivirus software previously installed on your system before proceeding with installation.	Download 64-bit Download 32-bit
Installation (.exe)	Installation process without ESET AV Remover.	N/A

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 Security Management Center.	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 Security Management Center.	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 allows 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.

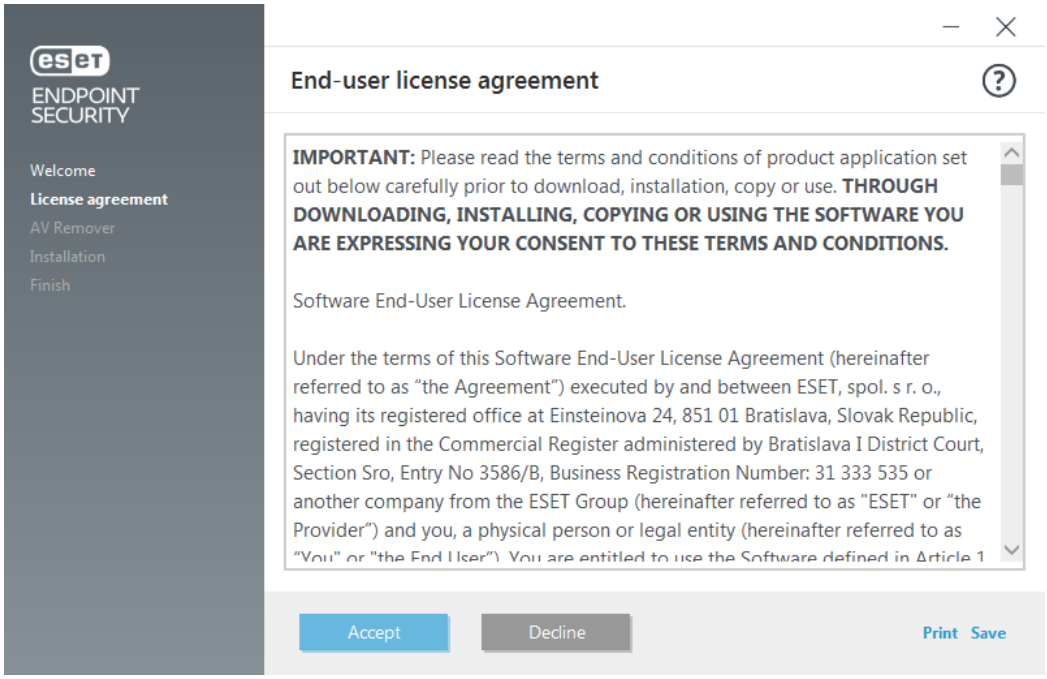


ESET AV Remover

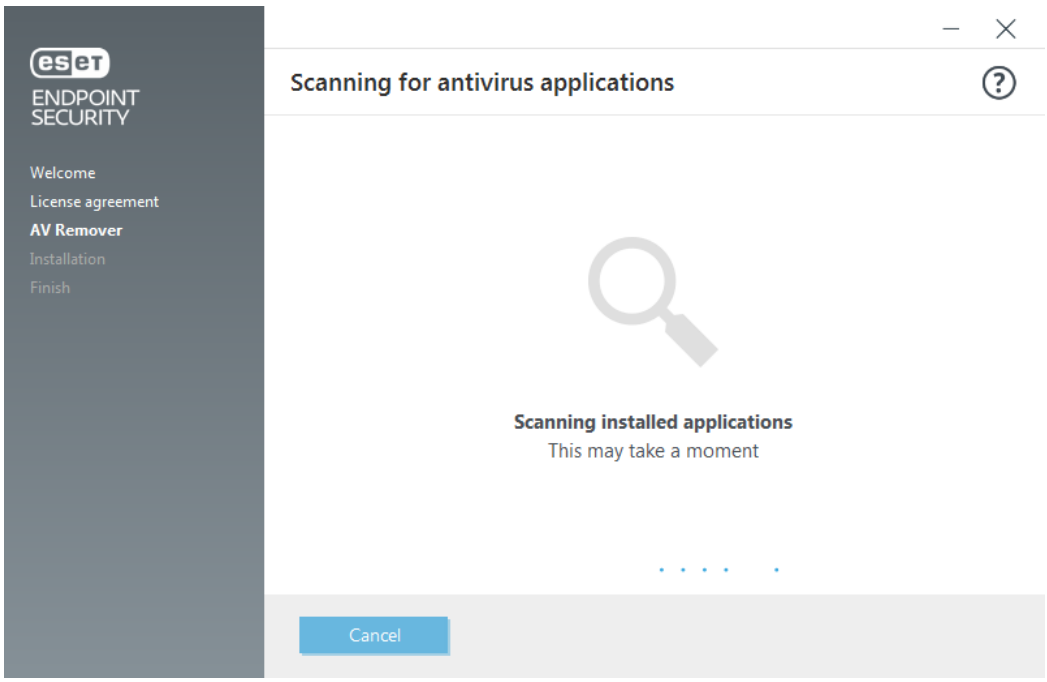
The ESET AV Remover tool will help you to remove almost any antivirus software previously installed on your system. Follow the instructions below to remove an existing antivirus program using ESET AV Remover:

1. To view a list of antivirus software that ESET AV Remover can remove, visit this ESET Knowledgebase article.

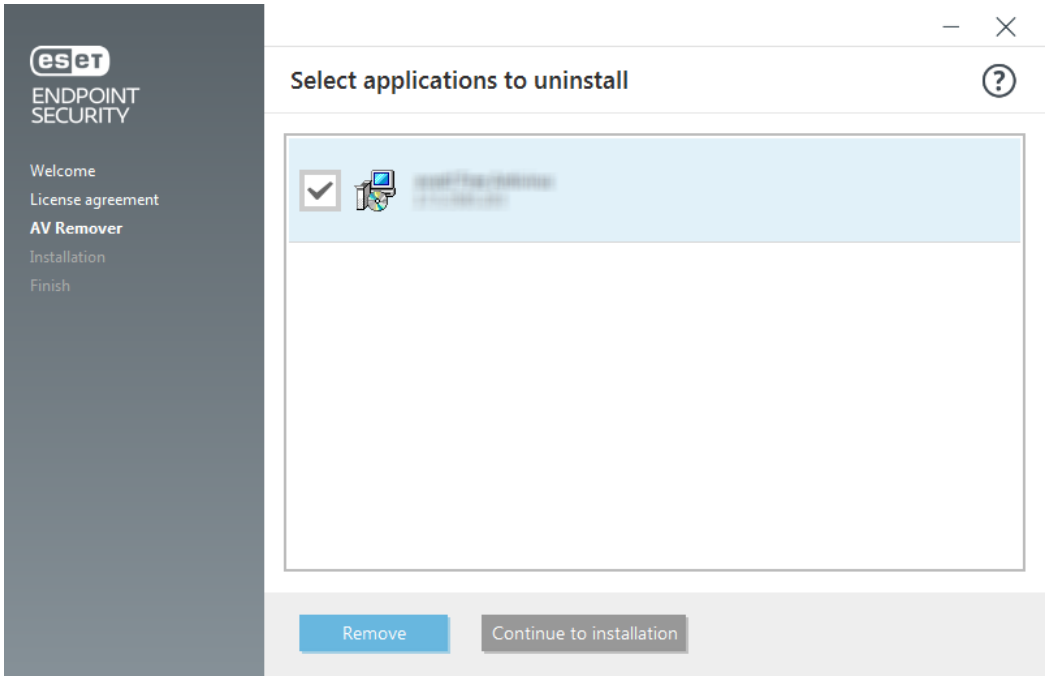
2. Read the End-User License Agreement and click **Accept** to acknowledge your acceptance. Clicking **Decline** will continue to installation of ESET Endpoint Security without removal of existing security application on the computer.



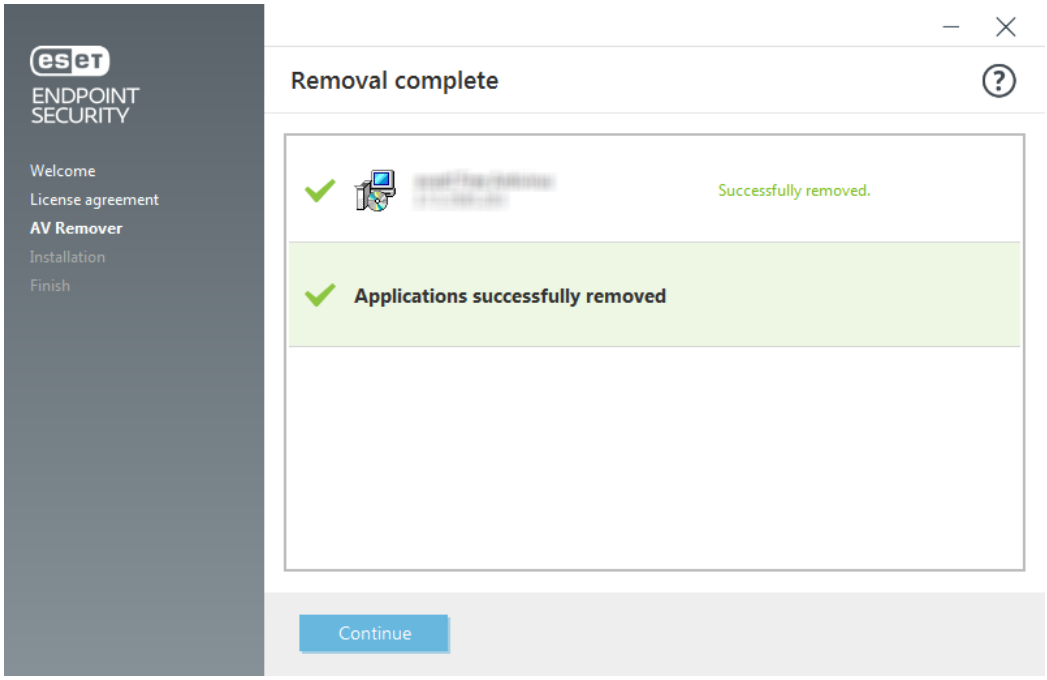
3. ESET AV Remover will begin searching your system for antivirus software.



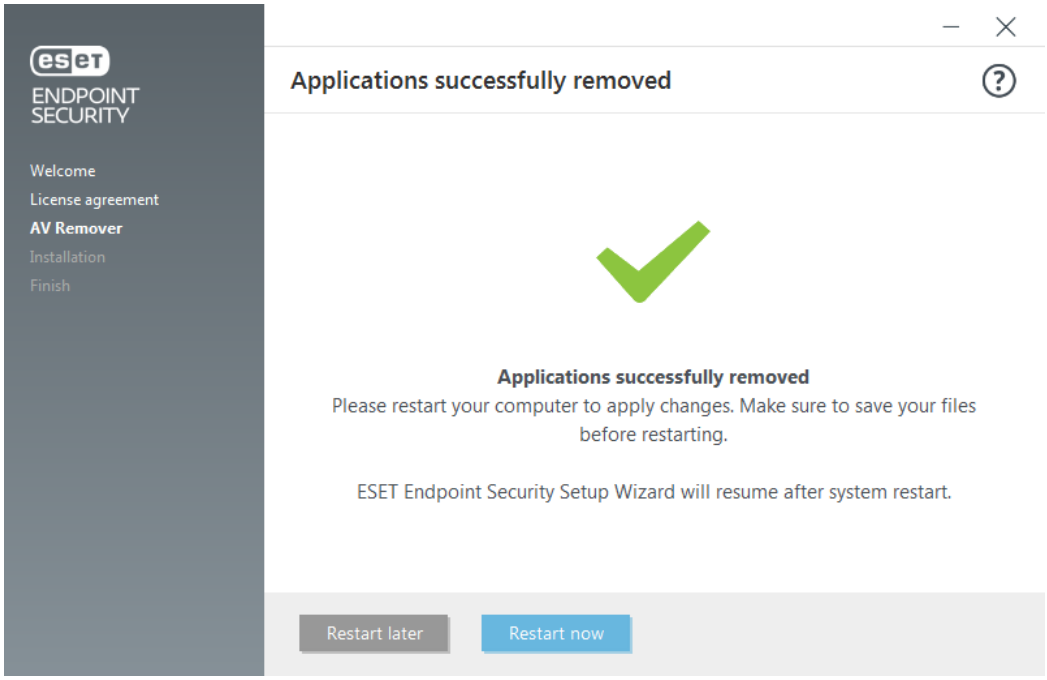
4. Select any listed antivirus applications and click **Remove**. Removal may take a moment.



5. 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.

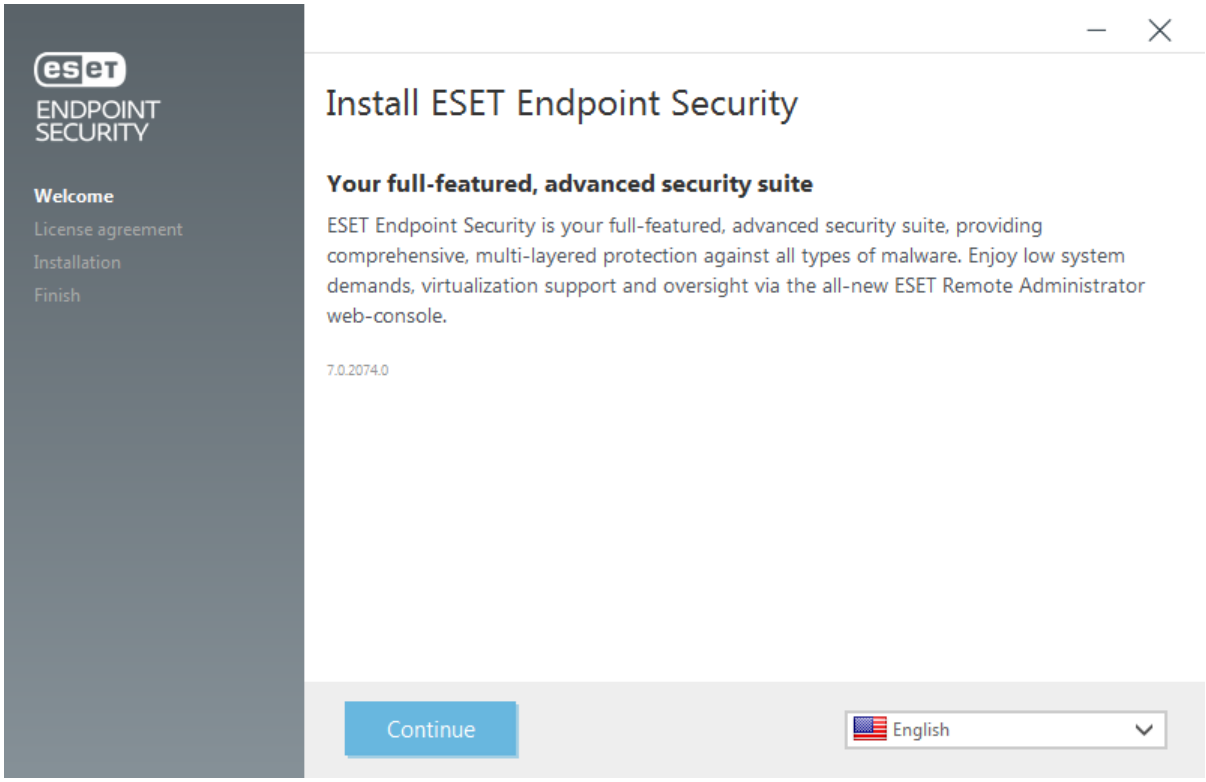
When the uninstallation of the security product was unsuccessful or some of its component was uninstalled partially, you are prompted to **Restart and rescan**. Confirm UAC after startup and continue with the scanning and uninstallation process.

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.

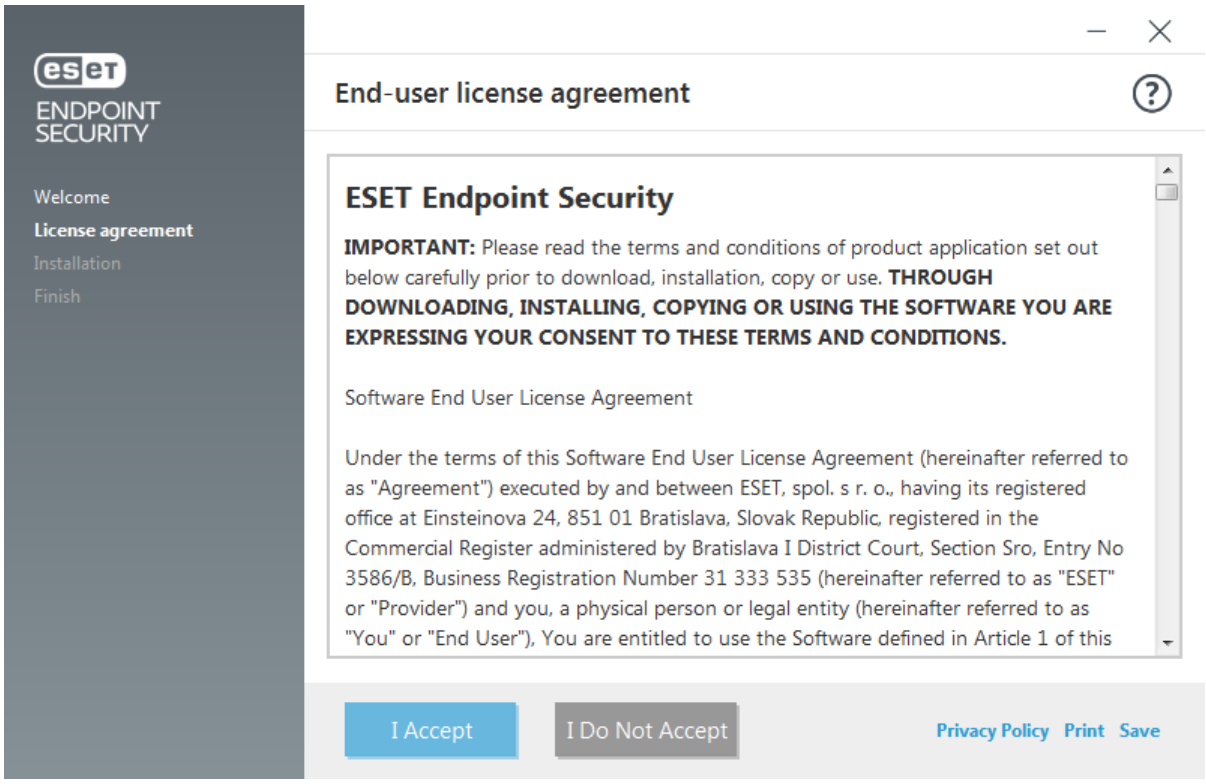
Installation (.exe)

Once you launch the .exe installer, the installation wizard will guide you through the installation process.

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

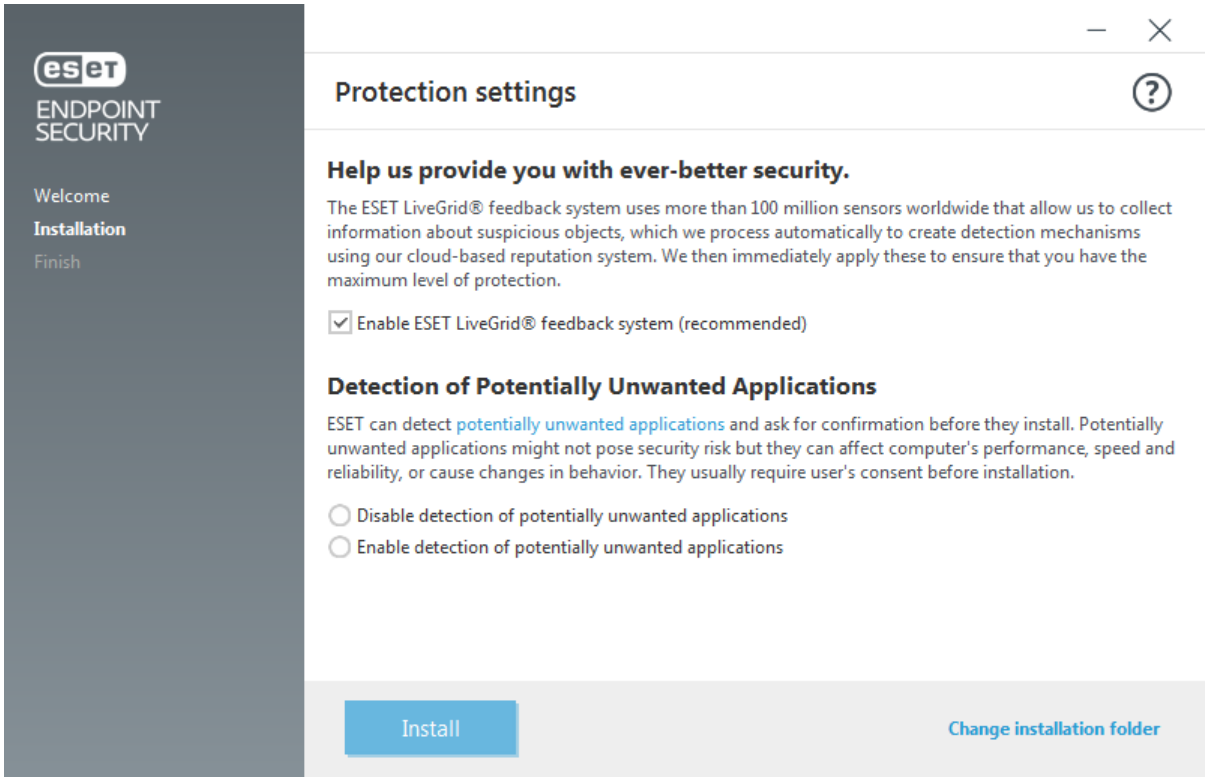


2. Choose whether enable ESET LiveGrid® feedback system. ESET LiveGrid® helps ensure that ESET is immediately and continuously informed about new infiltrations, which allows us to better protect our customers. The system allows you to submit new threats to the ESET Virus Lab, where they are analyzed, processed and added to the detection engine.

3. The next step in the installation process is to configure detection of Potentially unwanted applications. See the Potentially unwanted applications chapter for more details.

You can install ESET Endpoint Security to a specific folder by clicking **Change installation folder**.

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



Change installation folder (.exe)

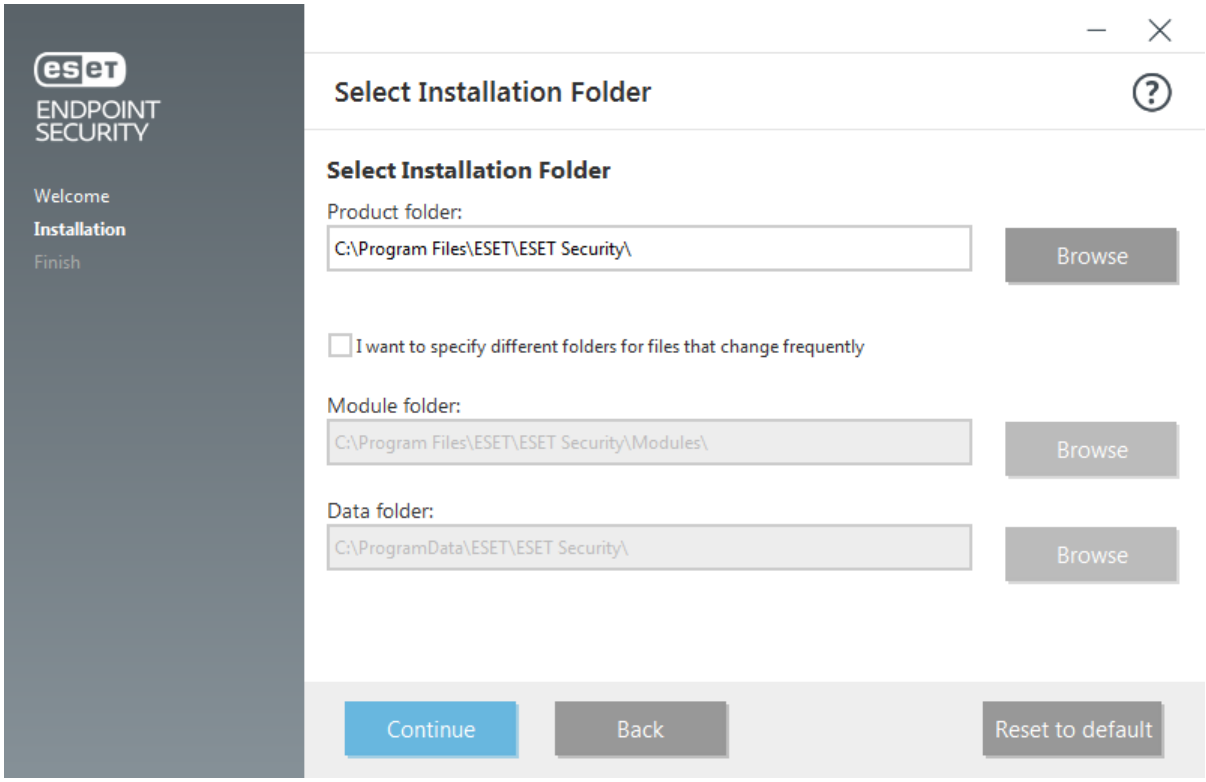
After selecting your preference for detection of potentially unwanted applications and clicking **Change installation folder**, you will be prompted to select a location for the installation ESET Endpoint Security folder. By default, the program installs to the following directory:

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, respectfully:

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

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



Click **Continue** and then **Install** to start installation.

Installation (.msi)

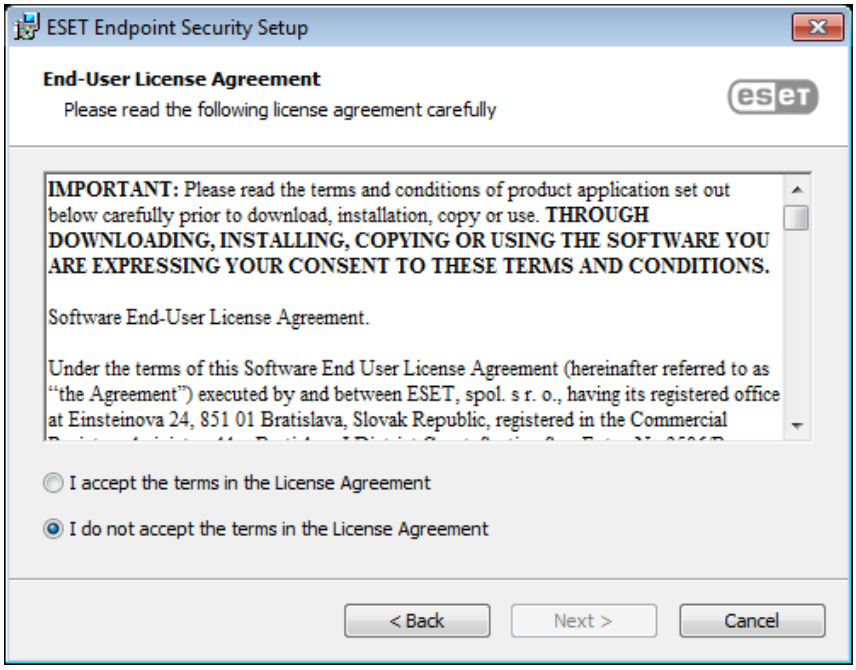
Once you launch the .msi installer, the installation wizard will guide you through the installation process.

> **Purpose of the .msi installer**
> 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 Security Management Center.

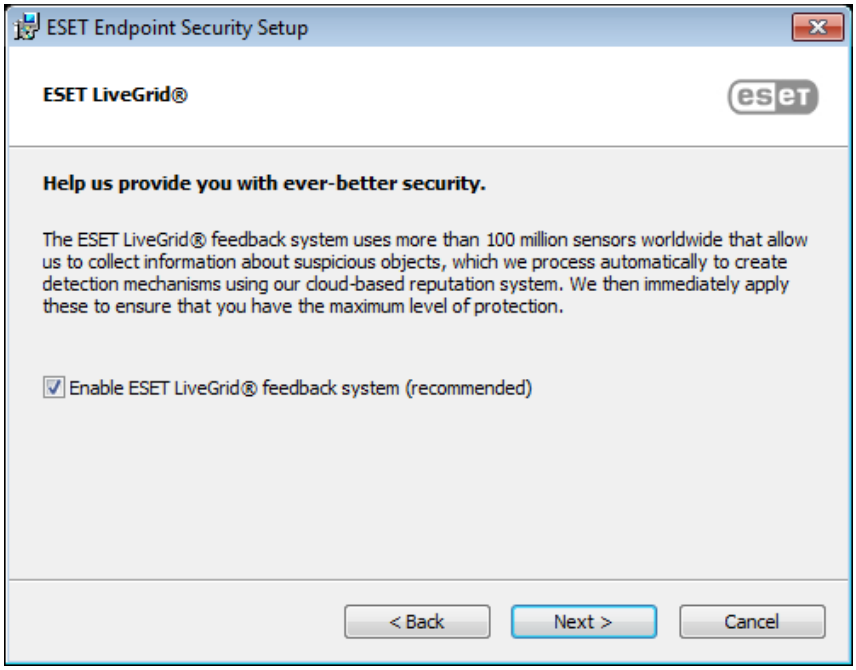
> **Important**
> Make sure that no other antivirus programs are installed on your computer. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system. See our knowledgebase article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

1. Select 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.

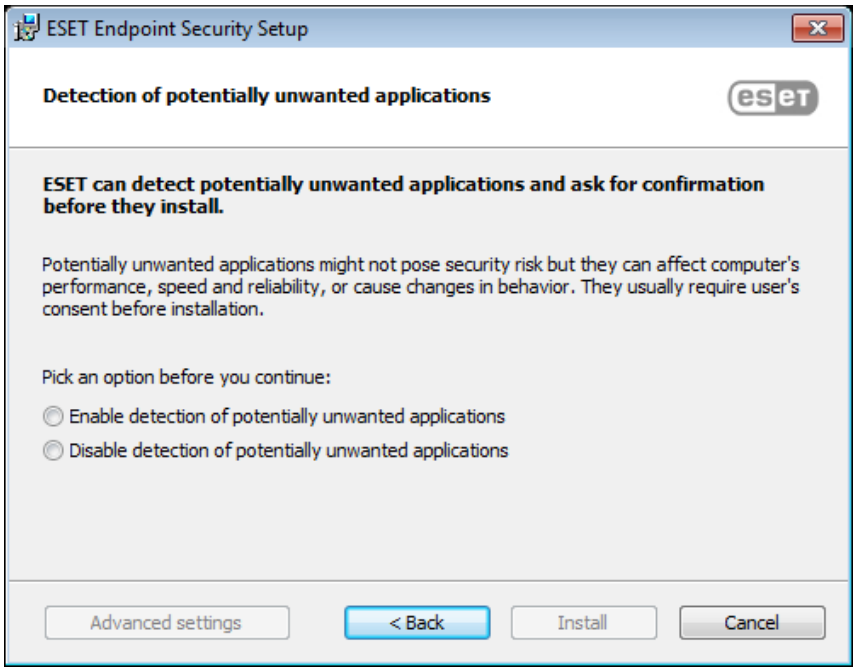


3. Select your preference for ESET LiveGrid® feedback system. ESET LiveGrid® helps ensure that ESET is immediately and continuously informed about new infiltrations, which allows us to better protect our customers. The system allows you to submit new threats to the ESET Virus Lab, where they are analyzed, processed and added to the detection engine.



4. The next step in the installation process is to configure the detection of Potentially unwanted applications. See the Potentially unwanted applications chapter for more details.

Click **Advanced settings** if you wish to proceed with Advanced installation (.msi).



5. 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 allow you to customize a number of installation parameters not available when performing a typical installation.

5. After selecting your preference for detection of Potentially unwanted applications and clicking **Advanced**

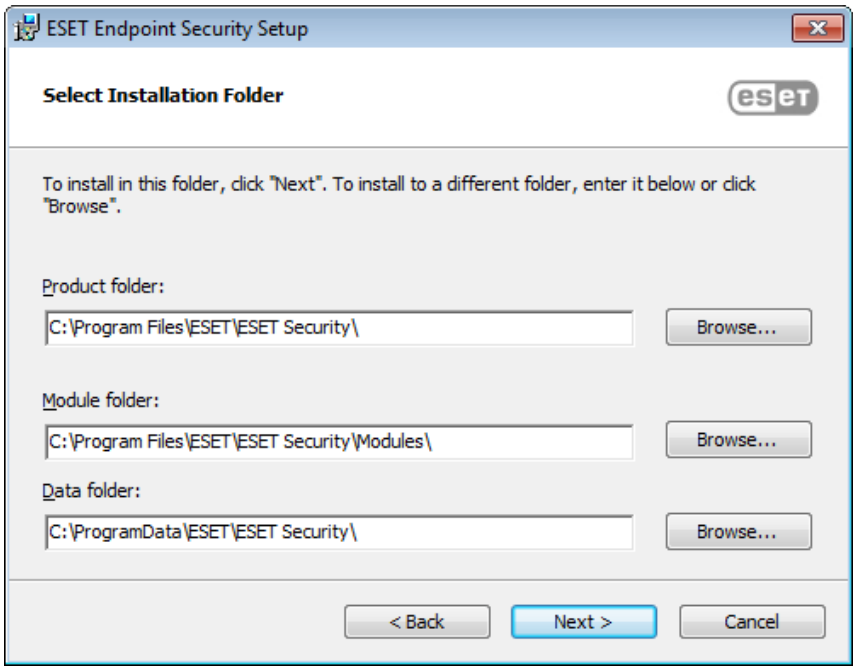
settings, you will be prompted to select a location for the installation ESET Endpoint Security folder. By default, the program installs to the following directory:

C:\Program Files\ESET\ESET Security

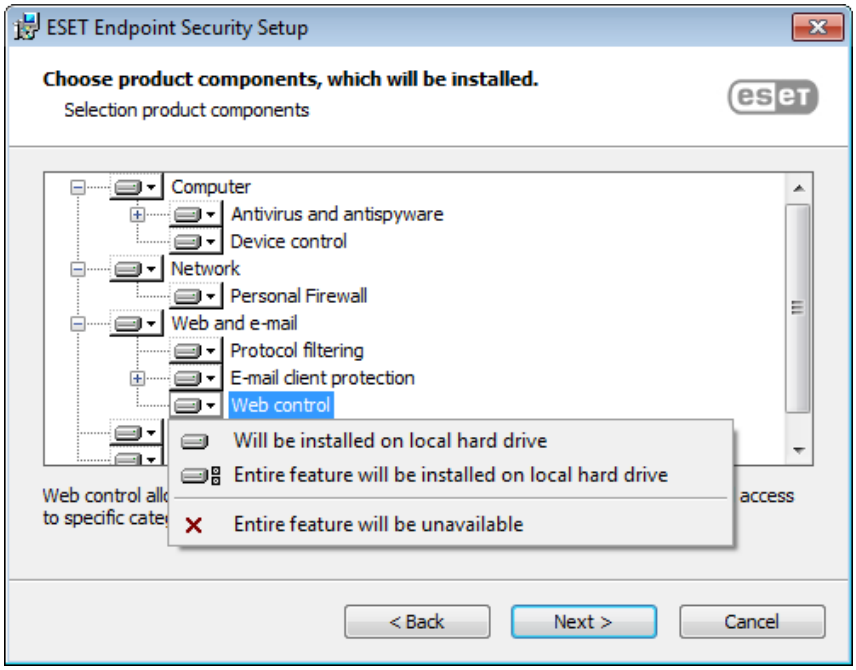
You can specify a location for program modules and data. By default, they are installed to the following directories, respectfully:

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

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



6. Choose which product components will be installed. Product components in the Computer section include Real-time file system protection, Computer scan, Document protection and Device control. Please note that the first two components are mandatory for your security solution to work. The Network section offers the option to install ESET firewall, which monitors all incoming and outgoing network traffic and applies rules for individual network connections. Firewall also provides protection against attacks from remote computers. Network attack protection (IDS) analyses the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked. Components in the Web and email section are responsible for your protection while you are browsing the Internet and communicating via email. 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.



7. The final step is to confirm installation by clicking **Install**.

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 Security Management Center.

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`

> **Note**
> **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

> **Note**
> 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
Network protection	Network		Placeholder
Network protection / Firewall	Firewall	Network	Optional
Network protection / Network attack protection / ...	IdsAndBotnetProtection	Network	Optional
Web and e-mail	WebAndEmail		Placeholder
Web and e-mail / Protocol filtering	ProtocolFiltering	WebAndEmail	Invisible
Web and e-mail / Web access protection	WebAccessProtection	WebAndEmail	Optional
Web and e-mail / E-mail client protection	EmailClientProtection	WebAndEmail	Optional
Web and e-mail / E-mail client protection / Email clients	MailPlugins	EmailClientProtection	Invisible
Web and e-mail / E-mail client protection / Antispam protection	Antispam	EmailClientProtection	Optional
Web and e-mail / Web control	WebControl	WebAndEmail	Optional
Tools / ESET RMM	Rmm		Optional
Update / Profiles / Update mirror	UpdateMirror		Optional
ESET Enterprise Inspector 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
CFG_PROXY_USERNAME=	<username>	User name 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.

Command line installation examples

Important
Make sure that you read the End User License Agreement and have administrative privileges prior to running the installation.

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

Example
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
```

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

Example
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
```

Example
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
```

Example
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 or remotely deploying using a Server task in ESMC, 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 Security Management Center (ESMC). ESMC 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 ESMC.
5. Deploy and activate ESET Endpoint Security to your client computers.

> **Illustrated instructions**
> The following ESET Knowledgebase article may only be available in English:
> - Deploy the ESET Management Agent via SCCM or GPO (7.x)
> - 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

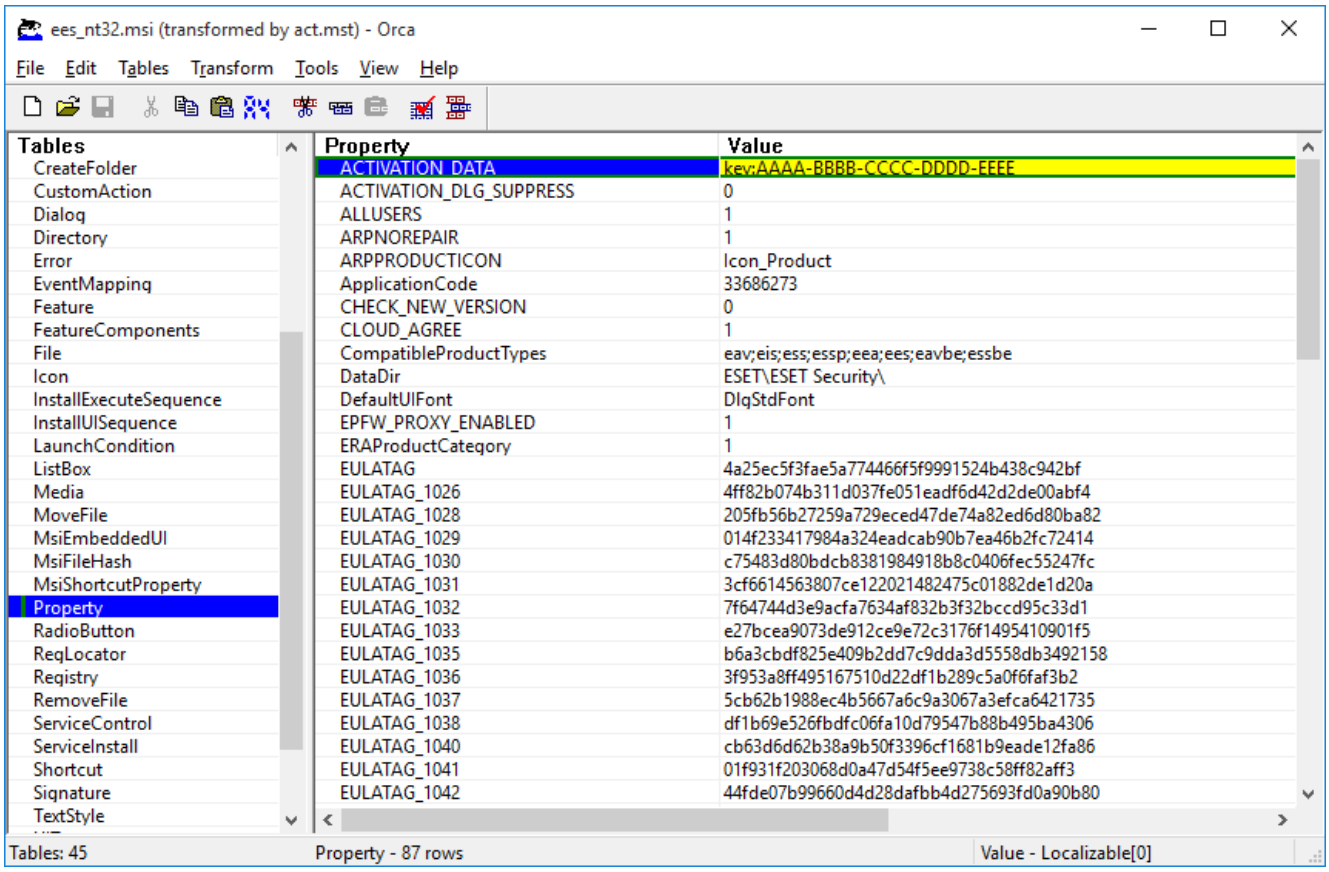
1. Open Orca.

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.

3. 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.

4. Deploy the .msi installer with the .mst file remotely using one of the method - 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

> **Remote monitoring and management**
> If you do not want to use ESMC or ESET PROTECT Cloud to remotely manage your ESET endpoint products, ESET Endpoint Security contains the ESET plugin for RMM which allows 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 Security Management Center (ESMC) or ESET PROTECT Cloud. ESET Endpoint Security version 7 cannot be managed by ESET Remote Administrator.

2.Automatically, using GPO or SCCM.

3.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 ESMC or ESET PROTECT

Cloud.

Please refer to the following documentation:

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

Upgrading manually on a client workstation

Do not install version 7 over a version 4.x, similarly, if you have an older/non-functional ESET Endpoint Security version 5.x or 6.x.

If you plan to handle upgrades on individual client workstations manually:

1. Verify that your operating system is supported (Windows Vista and Windows XP is not supported for version 7).

2. Download and install a more recent version over the previous one.

Common installation problems

If problems occur during installation, see our list of common installation errors and resolutions to find a solution to your problem.

Activation failed

In the case activation of ESET Endpoint Security was not successful, the most-common possible scenarios are:

- License key already in use

- Invalid License key. Product activation form error

- Additional information necessary for activation is missing or invalid

- Communication with the activation database failed. Please try to activate again in 15 minutes

- No or disabled connection to ESET activation servers

Make sure 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

Product activation

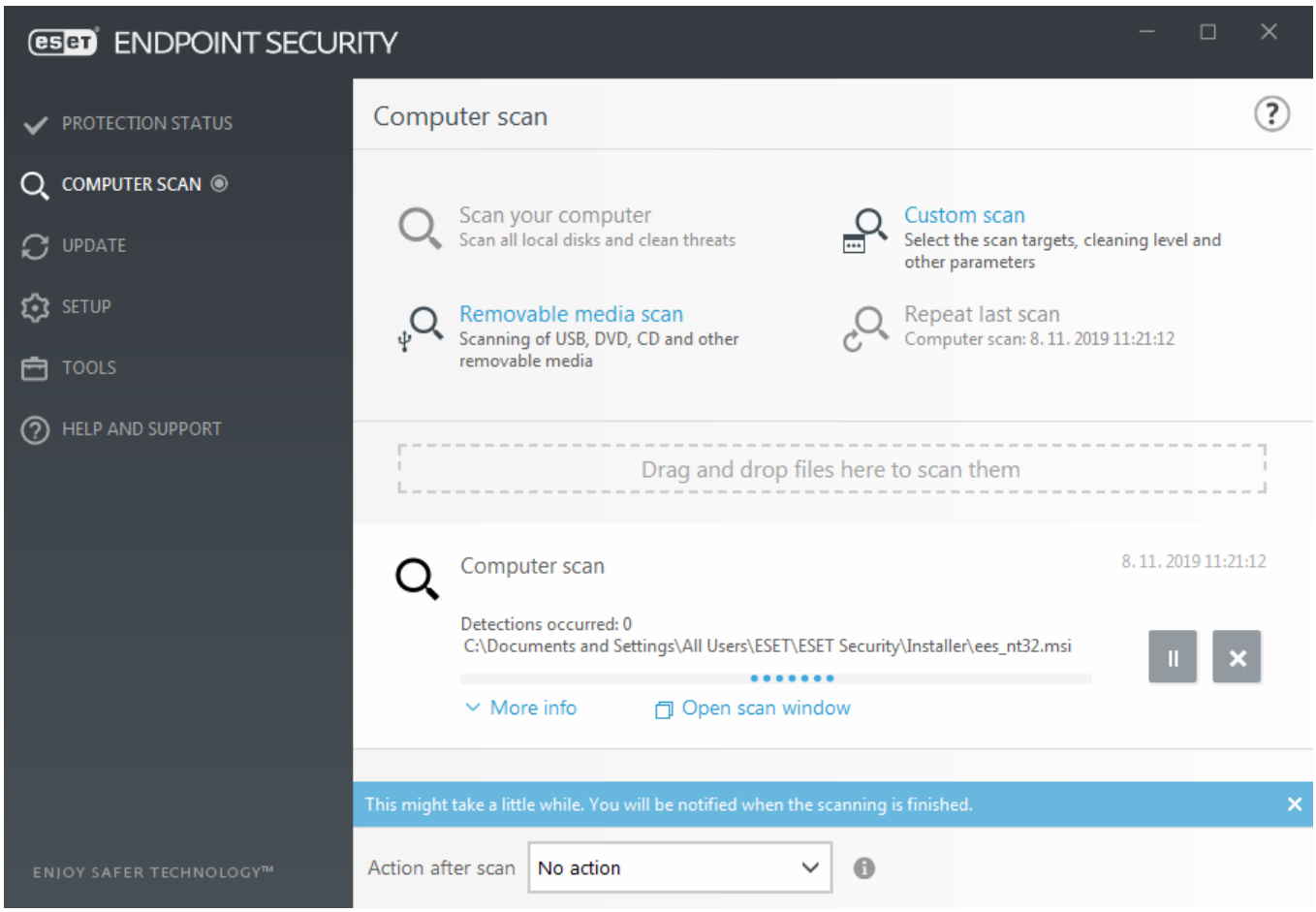
After installation is complete, you will be prompted to activate your product.

Select one of the available methods to activate ESET Endpoint Security. See How to activate ESET Endpoint

Security for more information.

Computer scan

We recommend that you perform regular computer scans, or schedule a regular scan, to check for threats. In the main program window, click **Computer scan** and then click **Smart scan**. For more information about computer scans, see Computer scan.



Beginner's guide

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

The user interface

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

The following is a description of options within the main menu:

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

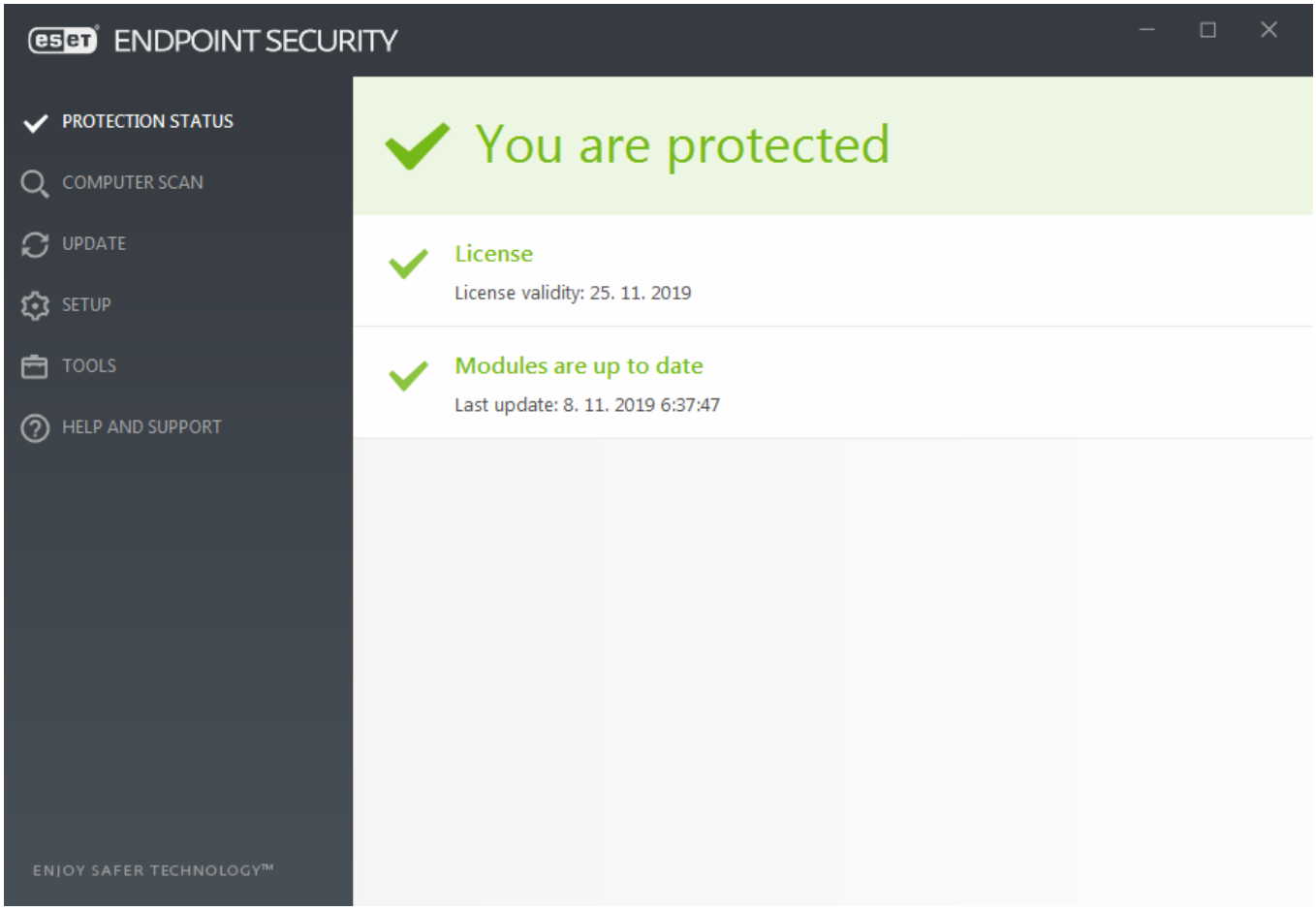
Computer scan – This option allows you to configure and launch of Smart scan, Custom scan, or Removable media scan. You can also repeat the last scan that was run.

Update – Displays information about the detection engine and allows to check for updates manually.

Setup – Select this option to adjust your Computer, Network or Web and Email security settings.

Tools – Provides access to Log files, Protection statistics, Watch activity, Running processes, Scheduler, Quarantine, Network connections, ESET SysInspector and ESET SysRescue to create a rescue CD. You can also submit a sample for analysis.

Help and support – Provides access to help files, ESET Knowledgebase and the ESET company website. Also available are links to open a Technical Support support request, support tools, and information about product activation.

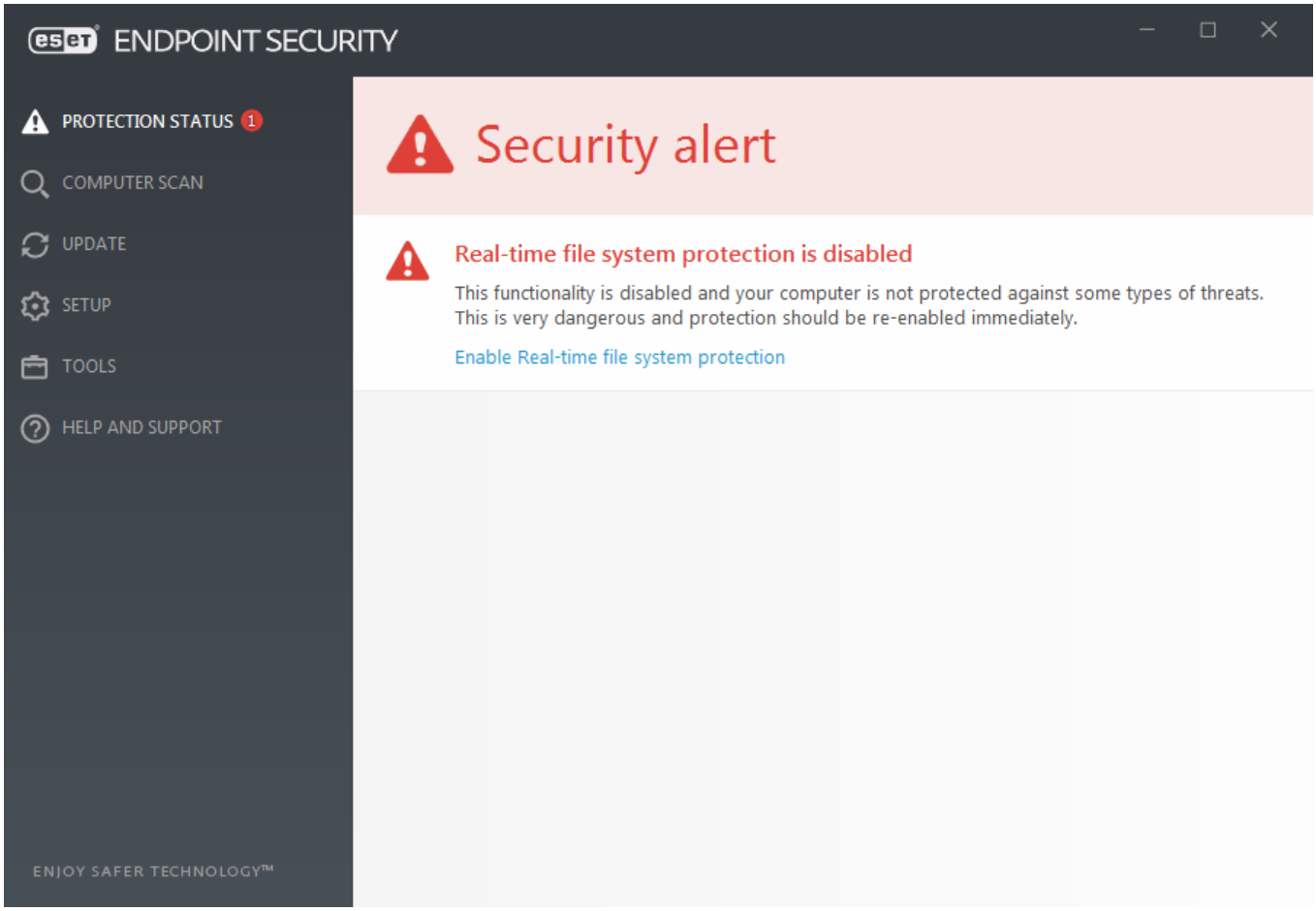


The **Protection status** screen informs you about the security and current protection level of your computer. The green **Maximum protection** status indicates that maximum protection is ensured.

The status window also displays quick links to frequently used features in ESET Endpoint Security and information about the last update.

What to do if the program doesn't 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.

- **The ESET 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 entered authentication data or incorrectly configured connection settings.

- **Product is not activated** or **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 disabled from

Advanced setup. Your computer is not protected against some types of threats and protection should be re-enabled immediately by clicking **Enable HIPS**.

- **ESET LiveGrid® is disabled** – This problem is indicated when ESET LiveGrid® disabled in Advanced setup.

- **No regular updates scheduled** – ESET Endpoint Security will not check for or receive important updates unless you schedule update task.

- **Anti-Stealth is disabled** – Click **Enable Anti-Stealth** to re-enable this functionality.

- **Network access blocked** – Displayed when the **Isolate computer from network** client task of this workstation from ESMC 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 on the security notification to re-enable Web access protection and then click **Enable Web access protection**.

- **Your license will expire soon** – 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**.

- **Antispam protection is paused** – Click **Enable Antispam protection 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.

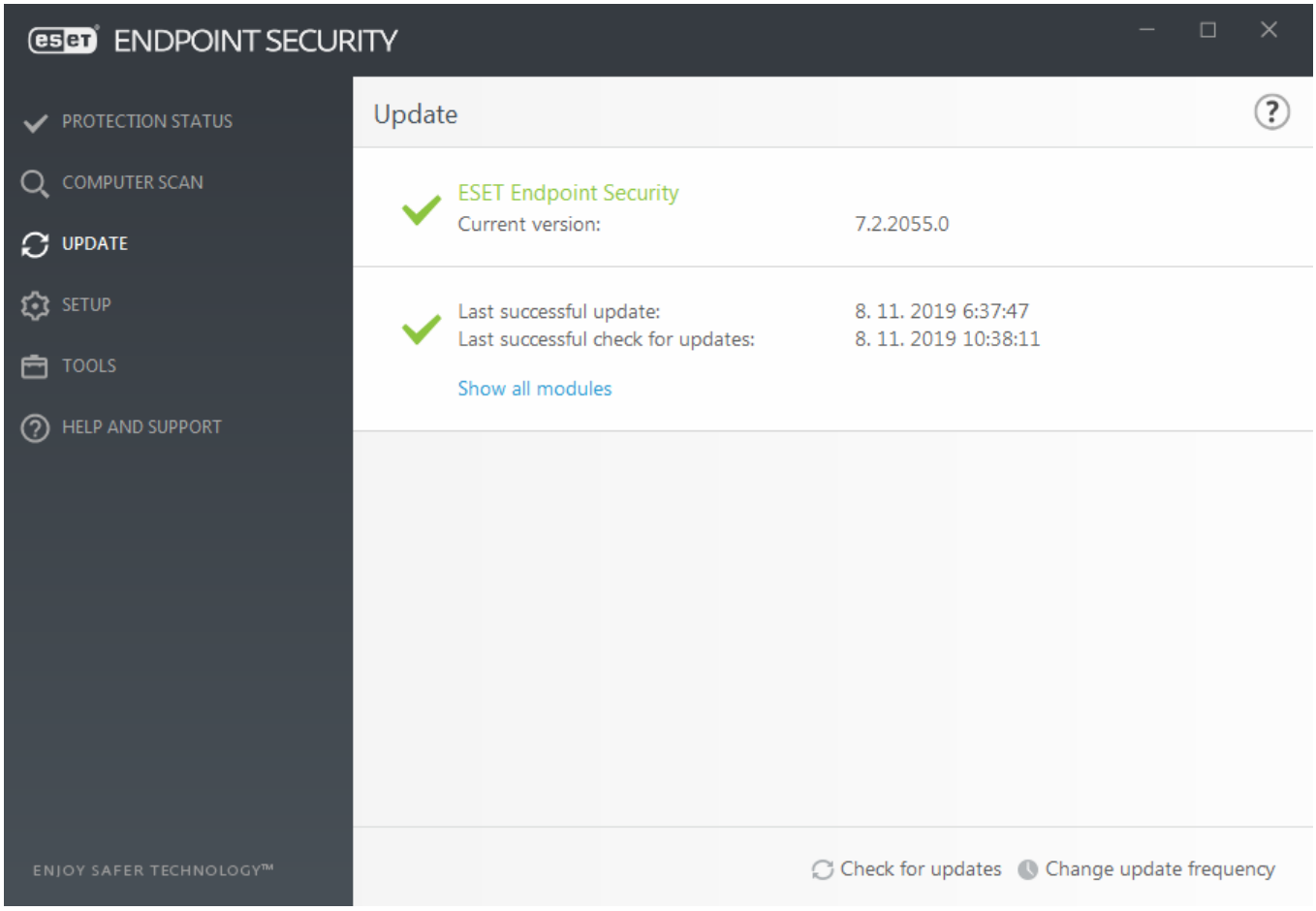
If you are unable to solve a problem by using the suggested solutions, click **Help and support** to access the help files or search the ESET Knowledgebase. If you still need assistance, you can submit an ESET Technical Support request. ESET Technical Support will respond quickly to your questions and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

> **Note**
> If a status belongs to a feature that is blocked by ESMC policy, the link will not be clickable.

Update setup

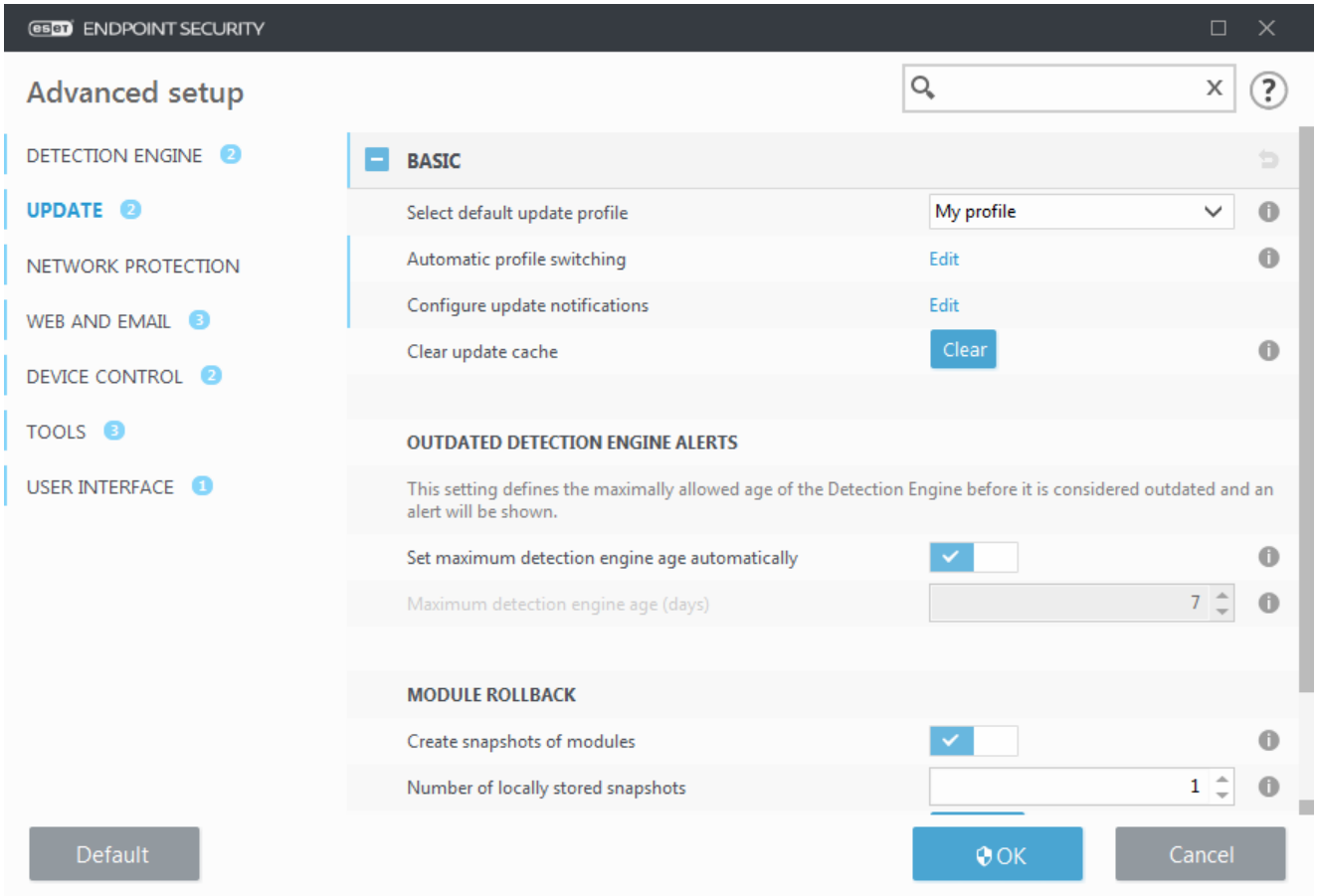
Updating modules is an important part of maintaining complete protection against malicious code. Please pay careful attention to update configuration and operation. From the main menu, select **Update** > **Check for updates** to check for a newer module update.

If your **License Key** is not entered yet, you will be unable to receive new updates and will be prompted to activate your product.



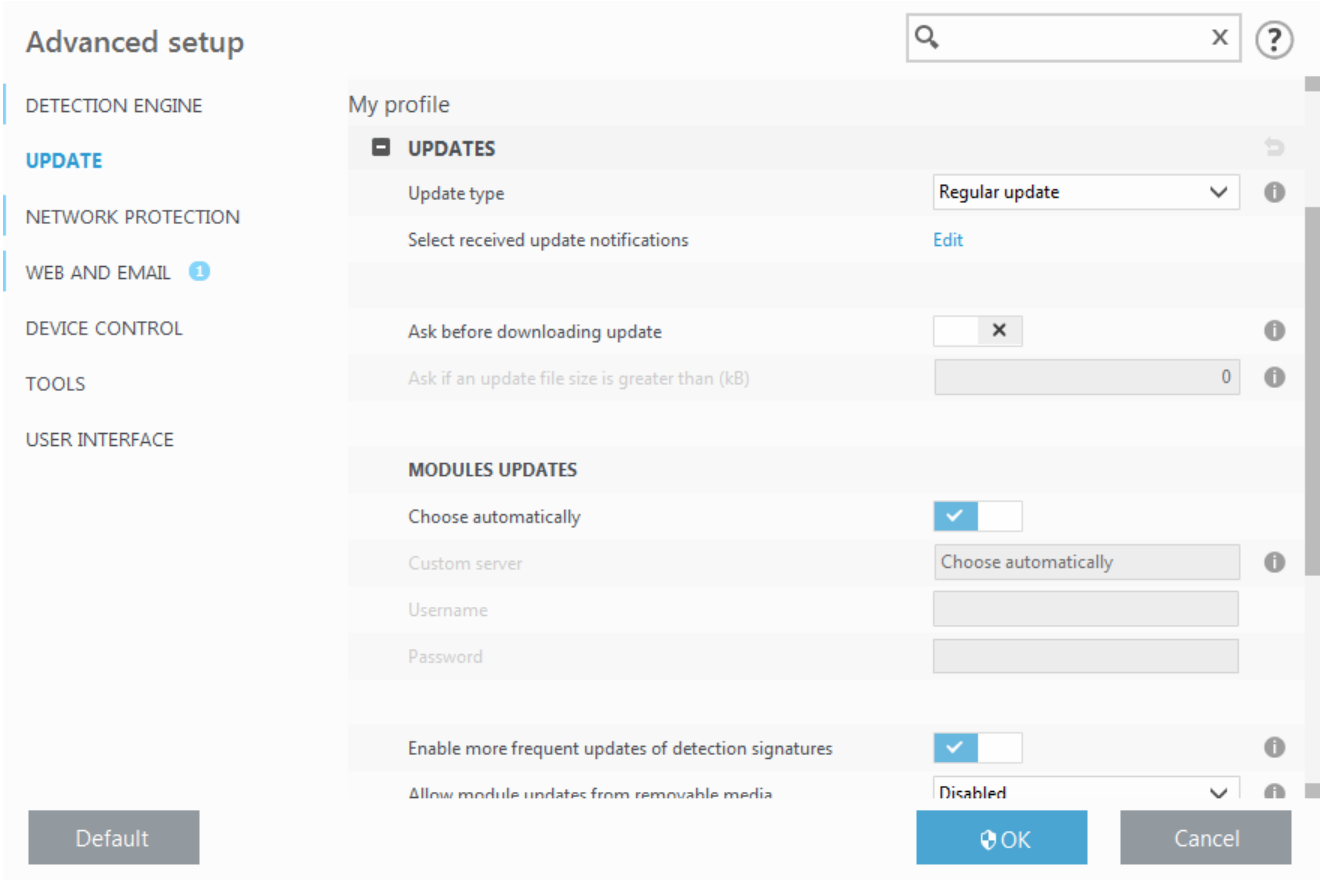
The Advanced setup window (click **Setup** > **Advanced setup from the main menu**, or press **F5** on your keyboard) contains additional update options. To configure advanced update options such as update mode, proxy server access, LAN connections and detection engine copy creation settings, click **Update** in the Advanced setup tree.

- If you experience problems with an update, click **Clear** to clear the temporary update cache.



- The **Choose automatically** option in **Profiles** > **Updates** > **Modules Updates** is enabled default. When using an ESET update server for receiving updates, we recommend that you leave this as is.

- If you do not want the successful update system tray notification at the bottom right corner of the screen to appear, expand **Profiles** > **Updates**, click **Edit** next to **Select received update notifications** and then adjust check boxes for the **Detection Engine was successfuly updated** notification.



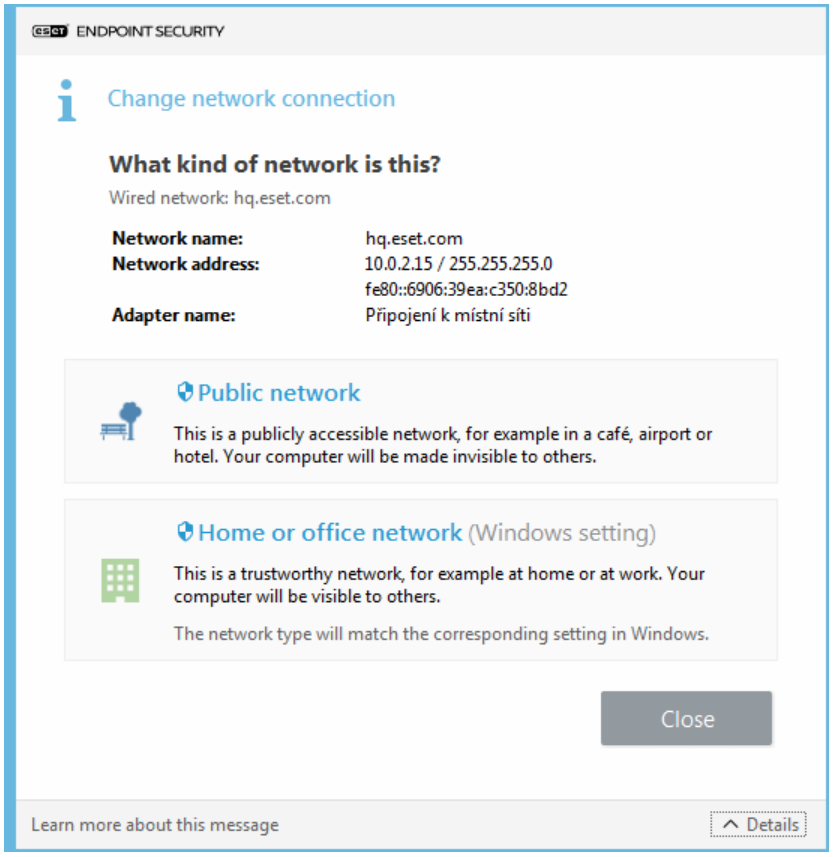
For optimal functionality, it is important that the program is automatically updated. This is only possible if the correct **License key** is entered in **Help and support** > **Activate Product**.

If you did not enter 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 and enter the credentials you received with your ESET Security product in **License details** window.

Zones setup

It is necessary to configure Trusted zones to protect your computer in a network environment. You can allow other users to access your computer by configuring a Trusted zone to allow sharing. Click **Advanced Setup** (F5) > **Network protection** > **Firewall** > **Advanced** > **Zones** to access settings for Trusted zones.

Trusted zone detection occurs after ESET Endpoint Security installation and whenever your computer connects to a new network. Therefore, there is usually no need to define the Trusted zone. By default, a dialog window is displayed upon detection of a new zone which allows you to set the protection level for that zone.



Important
An incorrect trusted zone configuration may pose a security risk to your computer.

Note
By default, workstations from a Trusted zone are granted access to shared files and printers, have incoming RPC communication enabled and have remote desktop sharing available.

For more details about this feature, read the following ESET Knowledgebase article:

- New network connection detected in ESET Endpoint Security

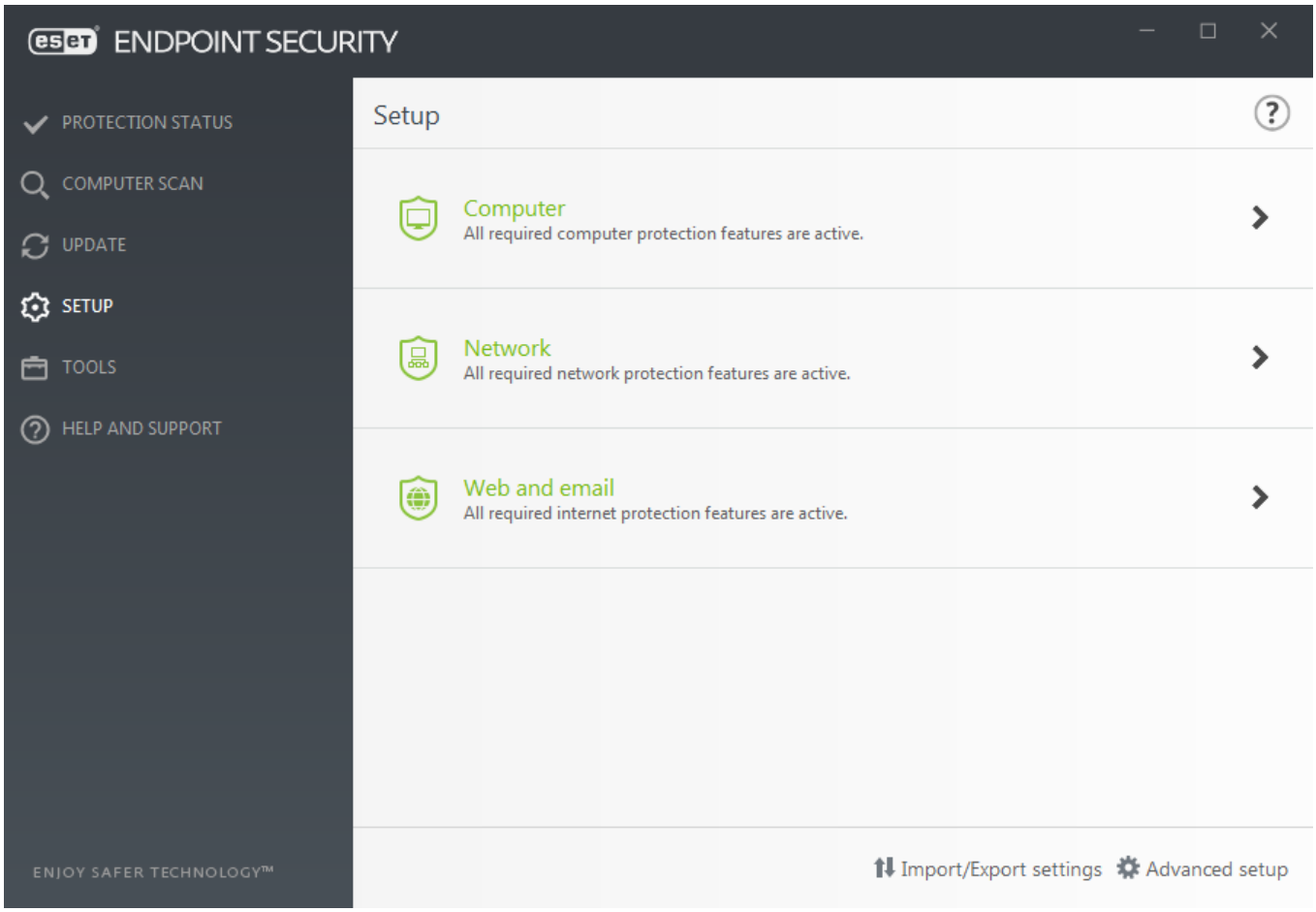
Web control tools

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. Please refer to the Web control chapter for instructions on how to create specific restrictions for your client workstations to protect them from potentially offensive material.

Work with ESET Endpoint Security

The ESET Endpoint Security setup options allow you to adjust the level of protection for your computer, web, email and network.

> **Note**
> When creating a policy from ESET Security Management Center 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 ESMC Online Help.



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

- **Computer**
- **Network**
- **Web and Email**

Computer section allows you to 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.
- **Device control** – Provides automatic device (CD/DVD/USB/...) control. This module allows 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 MS 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 pop-up windows, 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.

The **Network protection** section allows you to configure the Firewall, Network attack protection (IDS) and Botnet protection.

Web and email protection setup allows you to enable or disable the following components:

- **Web control** – Blocks web pages that may contain potentially offensive material. In addition, system administrators can specify access preferences for 27 pre-defined website categories.
- **Web access protection** – If enabled, all traffic through HTTP or HTTPS is scanned for malicious software.
- **Email client protection** – Monitors communication received through the POP3 and IMAP protocol.
- **Antispam protection** – Scans unsolicited email or spam.
- **Anti-Phishing protection** – Protects you from attempts to acquire passwords, banking data and other sensitive information by illegitimate websites disguised as legitimate ones.

To temporarily disable individual modules, click the **green switch** next to the desired module. Note that this may decrease the protection level of your computer.

To re-enable the protection of a disabled security component, click the red switch to return a component to its enabled state.

When ESMC/ERA policy is applied, you will see the lock icon next to a specific component. The policy applied by ESET Security Management Center can be overridden locally after authentication by logged user (e.g. administrator). For more information see the ESMC Online Help.

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

To access detailed settings for a particular security component, click the gear wheel next to any component**.**

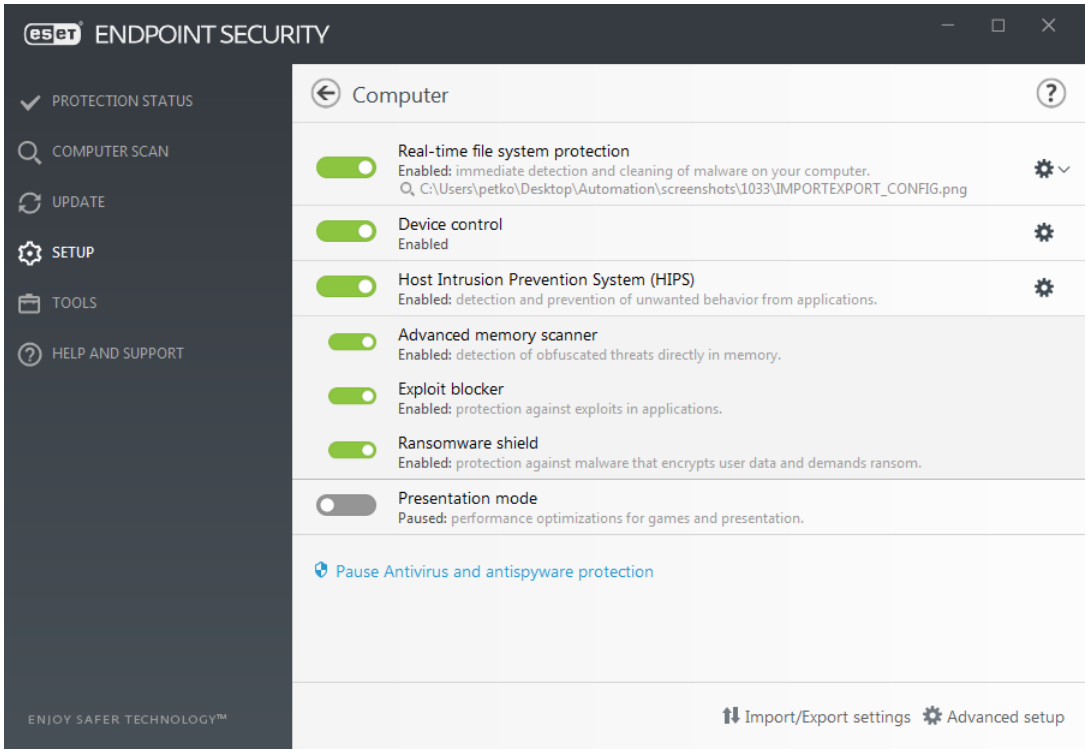
There are additional options at the bottom of the setup window. To load setup parameters using an *.xml* configuration file, or to save the current setup parameters to a configuration file, use **Import/Export settings**. Please see Import/Export settings for more detailed information.

For more detailed options, click **Advanced Setup** or press **F5**.

Computer

The **Computer** module can be found under **Setup** > **Computer**. It displays an overview of the protection modules described in the previous chapter. In this section, the following settings are available:

Click the gear wheel ⚙ next to **Real-time file system protection** and click **Edit exclusions** to open the Exclusion setup window, which allows you to exclude files and folders from scanning. To open **Real-time file system protection** advanced setup, click **Configure...**.



Computer section allows you to 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.

- **Device control** – Provides automatic device (CD/DVD/USB/...) control. This module allows 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 MS 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 pop-up windows, 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**.

Detection engine (7.2 and later)

Detection engine guards against malicious system attacks by controlling file, email and internet communication. For example, if an object classified as malware is detected, remediation will start. The detection engine can eliminate it by first blocking it and then cleaning, deleting or moving it to quarantine.

To configure the detection engine settings in detail, click **Advanced Setup** or press **F5**.

In this section:

- Real-time & Machine learning protection categories
- Malware scans
- Reporting setup
- Protection setup
- Best practices

> **Changes to the detection engine scanner configuration**
> Starting in version 7.2, the Detection engine section no longer provides ON/OFF switches as for version 7.1 and below. ON/OFF buttons are replaced with four thresholds - Aggressive, Balanced, Cautious and Off.

Real-time & Machine learning protection categories

Real-time & Machine learning protection for all protection modules (for example, Real-time file system protection, Web access protection, ...) allows you to configure reporting and protection levels of the following categories:

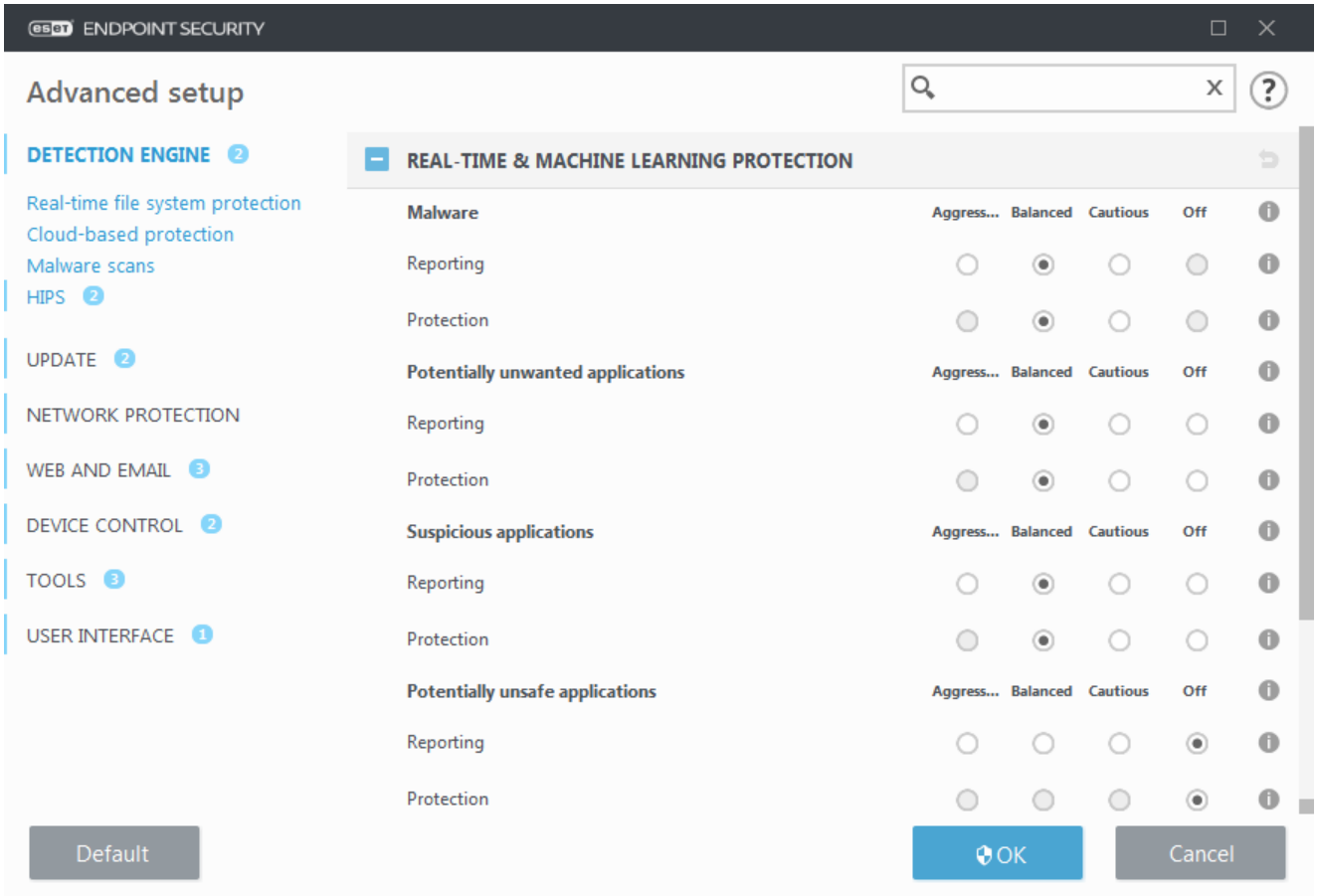
- **Malware** – A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term “virus” is often misused. "Malware” (malicious software) is a more accurate term. Malware detection is performed by the detection engine module combined with 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 with 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.

- **Potentially unsafe applications** – **R**efers 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.

- **Suspicious applications** include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.



Improved protection

Advanced machine learning is now a part of detection engine as an advanced layer of protection which improves detection based on machine learning. Read more about this type of protection in the Glossary.

Malware scans

Scanner settings can be configured separately for the real-time scanner and the on-demand scanner. By default, **Use real-time protection settings** is enabled. When enabled, relevant On-demand scan settings are inherited from the **Real-time & Machine Learning protection** section.

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.

Reporting threshold is configured for each category (referred to as "CATEGORY"):

1. Malware
2. Potentially unwanted applications
3. Potentially unsafe
4. Suspicious applications

Reporting performed with the detection engine, including the machine learning component. It is possible to 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 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

* Available in ESET Endpoint Security version 7.2 and later.
** 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 represents a comparable level of protection from previous versions of ESET Endpoint Security (7.1 and below). This 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 default value for potentially unsafe applications.

ESMC policy conversion table for ESET Endpoint Security 7.1 and below

As of the ESMC policy editor for the scanner settings no longer contains ON/OFF switches for each CATEGORY. The following table outlines a conversion between protection threshold and final state of the switch in ESET Endpoint Security 7.1 and below.

CATEGORY threshold state	Aggressive	Balanced	Cautious	Off
Applied CATEGORY switch	✓	✓	✓	✗

When upgrading from versions 7.1 and below to version 7.2 and later, the new threshold state will be as follows:

Category switch before upgrade	✓	✗
New CATEGORY threshold after upgrade	Balanced	Off

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 ESMC reports for possible missing detections.

Detection engine advanced options

Anti-Stealth technology is a sophisticated system that provides the detection of dangerous programs such as rootkits, which are able to hide themselves from the operating system. This means it is not possible to detect them using ordinary testing techniques.

Enable advanced scanning via AMSI – Microsoft Antimalware Scan Interface tool that allows application developers new malware defenses (Windows 10 only).

Detection engine (7.1 and below)

Detection engine guards against malicious system attacks by controlling file, email and internet communication. For example, if an object classified as malware is detected, remediation will start. The detection engine can eliminate it by first blocking it and then cleaning, deleting or moving it to quarantine.

To configure the detection engine settings in detail, click **Advanced Setup** or press **F5**.

> **Changes to detection engine scanner configuration**
> Starting from version 7.2, the Detection engine section looks different.

Scanner options for all protection modules (for example Real-time file system protection, Web access protection, ...) allows you to enable or disable detection of the following:

- **Potentially unwanted applications** – Grayware or Potentially Unwanted Application (PUA) is a broad category of software, whose intent is not as unequivocally malicious as with other types of malware, such as viruses or trojan horses. It may however 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.

- **Potentially unsafe applications** refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications include remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). This option is disabled by default.
  Read more about these types of applications in the glossary.

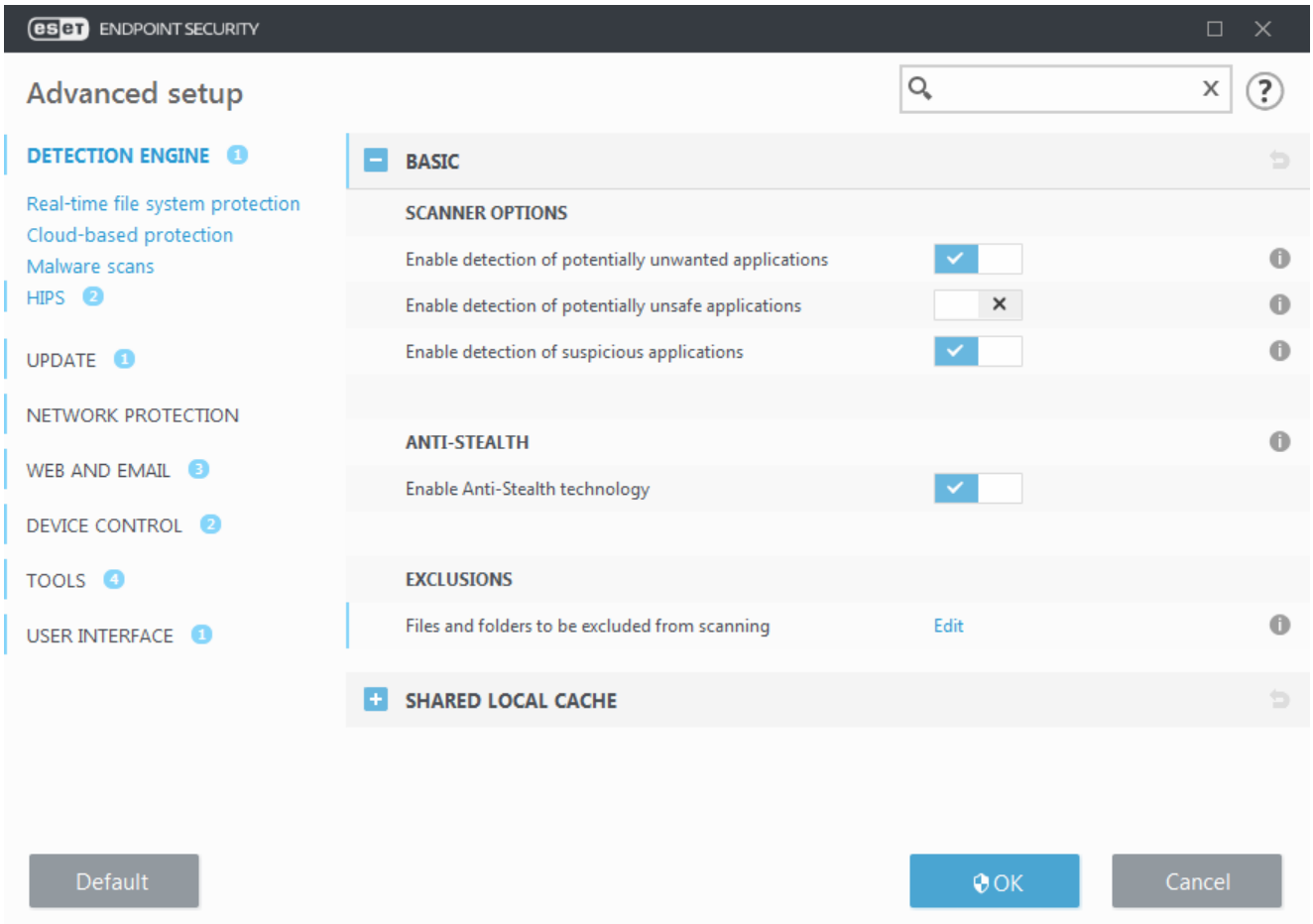
- **Suspicious applications** include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.

Anti-Stealth technology is a sophisticated system that provides the detection of dangerous programs such as

rootkits, which are able to hide themselves from the operating system. This means it is not possible to detect them using ordinary testing techniques.

Exclusions enable you to exclude objects from scanning. See Exclusions for more information.

Enable advanced scanning via AMSI – Microsoft Antimalware Scan Interface tool that allows application developers new malware defenses (Windows 10 only).



An infiltration is detected

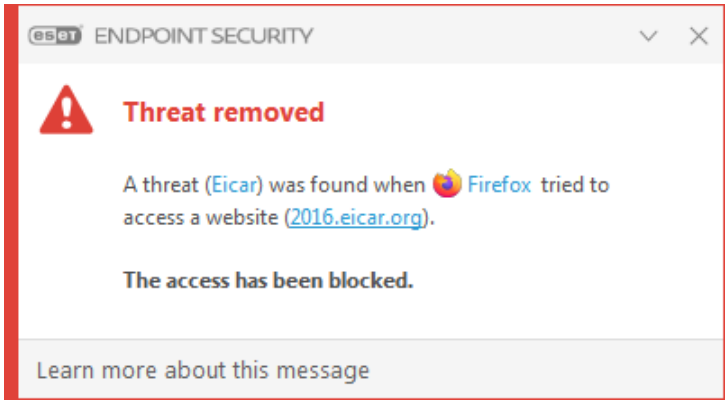
Infiltrations can reach the system from various entry points such as webpages, shared folders, via email or from removable devices (USB, external disks, CDs, DVDs, etc.).

Standard behavior

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

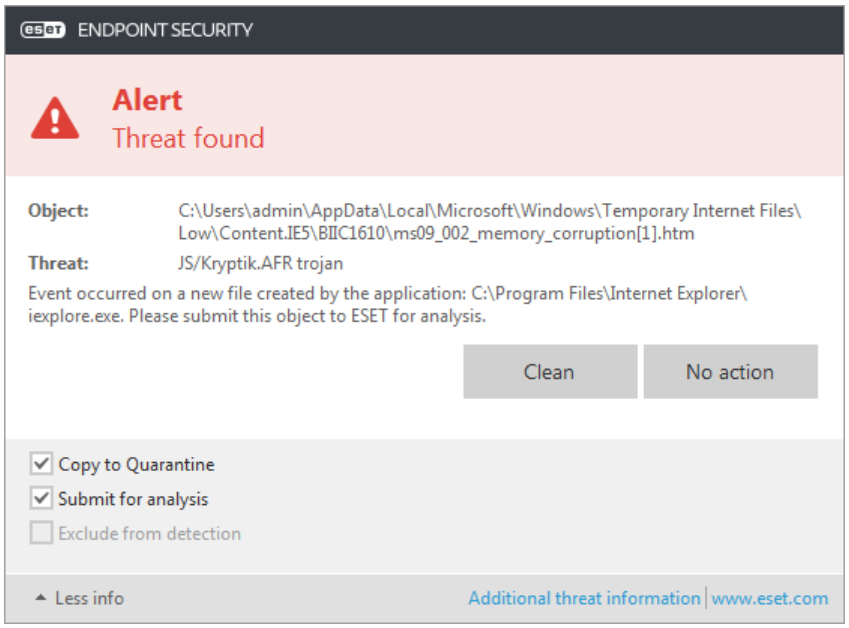
- Real-time file system protection
- Web access protection
- Email client protection
- On-demand computer scan

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 more information about cleaning levels and behavior, see Cleaning.



Cleaning and deleting

If there is no predefined 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 in order 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).

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.

Shared local cache

Shared local cache can boost performance in isolated environments (for example, virtual machines) by eliminating duplicate scanning in the network. This ensures that each file will be scanned only once and stored in the shared cache.

ESET Shared Local Cache must be installed and configured first.

- Download ESET Shared Local Cache.
- For more information, see ESET Shared Local Cache online help.

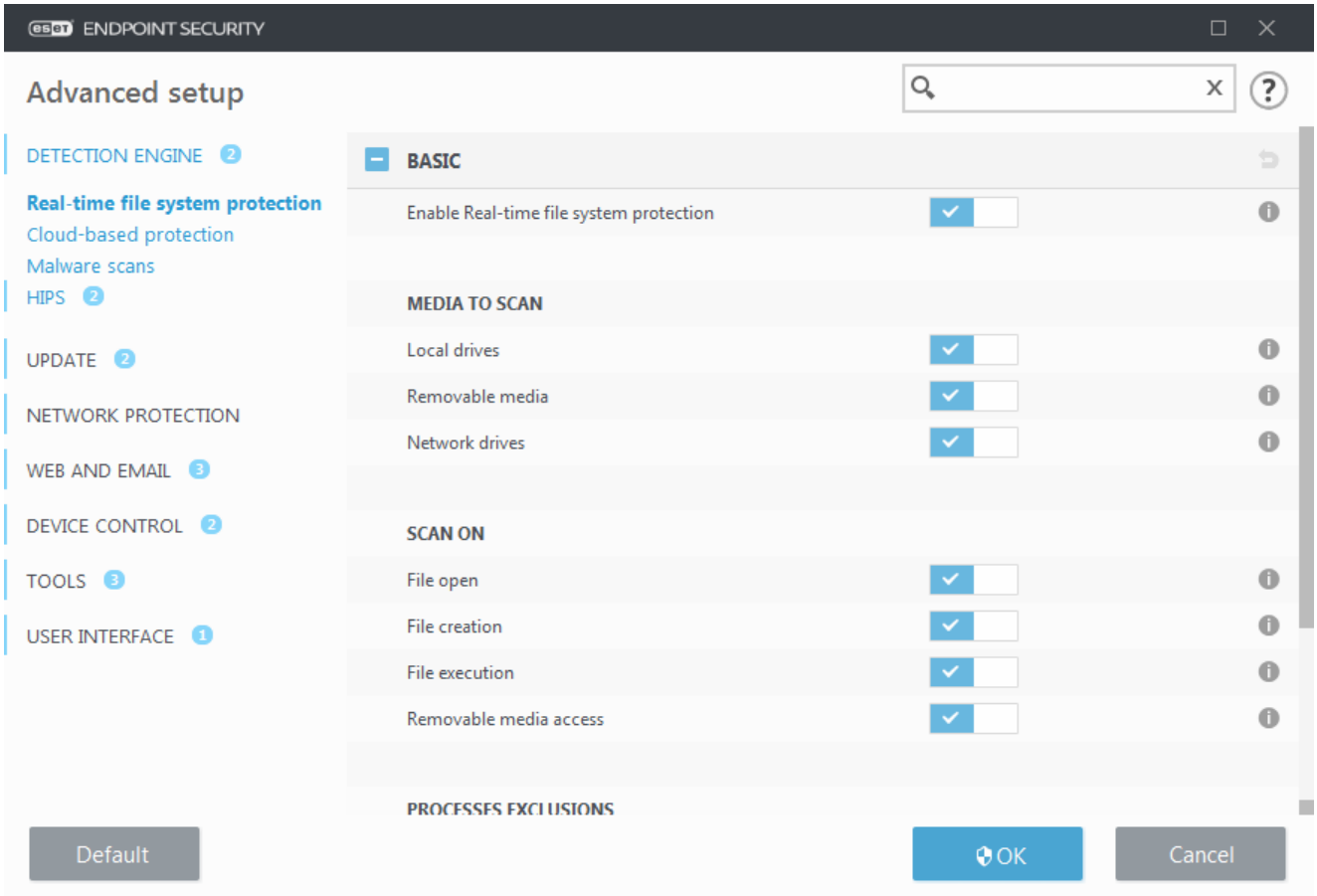
Turn on the **Caching option** switch to save information about scans of files and folders on your network to ESET Shared Local Cache. If you perform a new scan, ESET Endpoint Security will search for scanned files in ESET Shared Local Cache. If files match, they will be excluded from scanning.

The setup of **Cache server** contains the following:

- **Hostname** – Hostname or IP address of the computer where ESET Shared Local Cache is located.
- **Port** – Port number used for communication (same as was set in ESET Shared Local Cache).
- **Password** – Specify the password for ESET Shared Local Cache if required.

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** under **Detection engine** > **Real-time file system protection** > **Basic**.

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 upon opening, creation, or execution. 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 in 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 parameters.

Processes to be excluded from scanning – Read more about this type of exclusion in the Processes exclusions chapter.

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 the ThreatSense engine parameter setup section), 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 more closely monitor newly created files.

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 update of the detection engine. 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, press **F5** to open Advanced setup and expand **Detection engine** > **Real-time file system protection**. Click **ThreatSense parameters** > **Other** and select or deselect **Enable Smart optimization**.

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 enter this URL into your browser, you should see a message that the threat has been removed.

When to modify real-time protection configuration

Real-time file system protection is the most essential component for 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 each tab in the window (**Advanced setup** > **Detection engine** > **Real-time file system protection**).

What to do if real-time protection does not work

In this chapter, we describe problems that may arise when using real-time protection and how to troubleshoot them.

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup** in the main program window and click **Real-time file system protection**.

If real-time protection is not initiated at system startup, it is usually because **Start Real-time file system protection automatically** is deselected. To enable this option, navigate to **Advanced setup** (**F5**) and click **Detection engine** > **Real-time file system protection** > **Basic**. Make sure that the **Start Real-time file system protection automatically** switch is turned on.

If Real-time protection does not detect and clean infiltrations

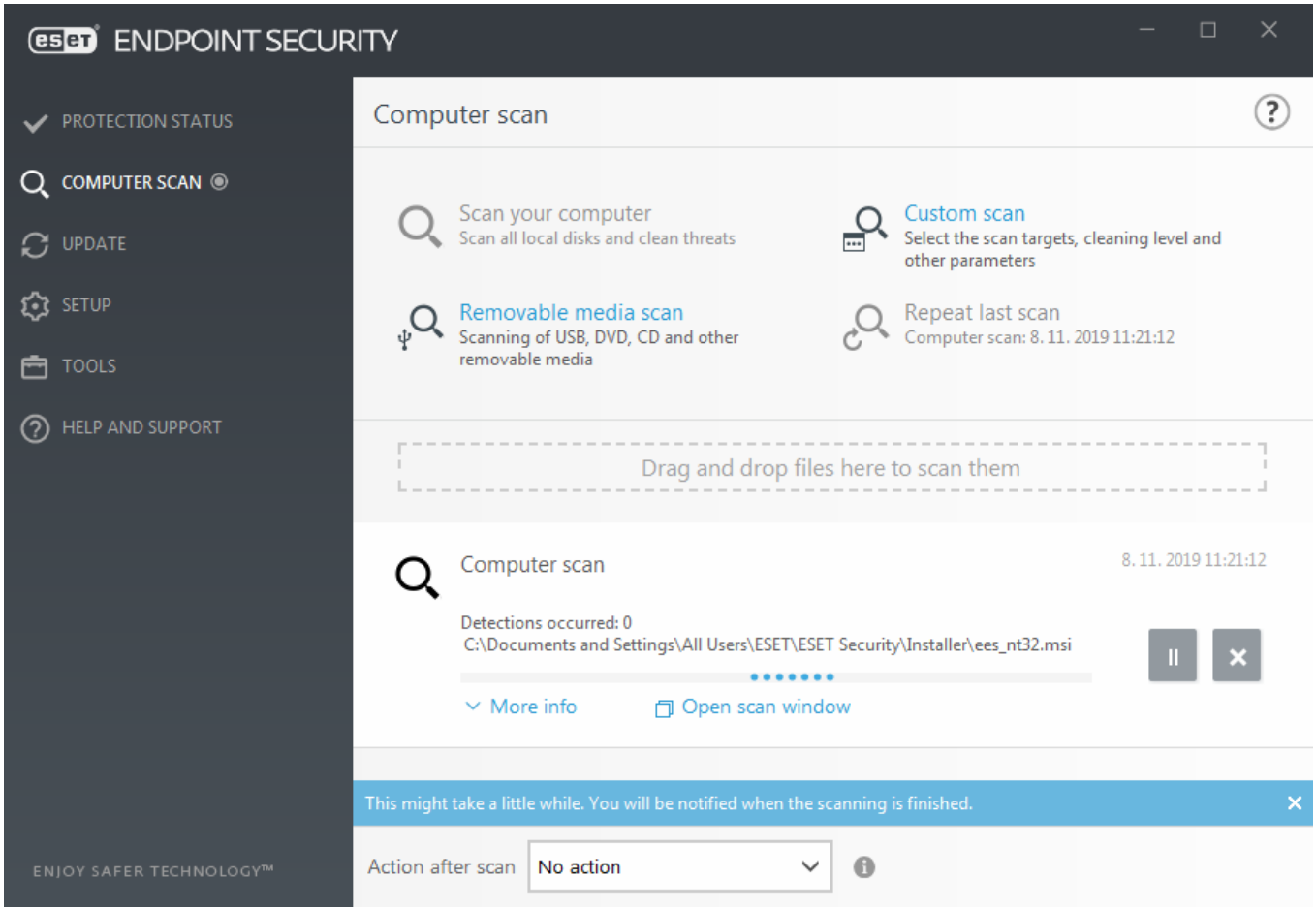
Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system before installing ESET.

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. For assistance resolving this issue, please contact ESET Technical Support.

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** allows you to select any of the predefined scan profiles and define specific scan targets.

See Scan progress for more information about the scanning process.

Scan your computer

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Smart scan is that it is easy to operate and does not require detailed scanning configuration. Smart 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 on types of cleaning, see Cleaning.

Custom scan

Custom scan is an optimal solution if you want to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed using the same parameters.

To select scan targets, select **Computer scan** > **Custom scan** and select an option from the **Scan targets** drop-down menu, or select specific targets from the tree structure. A scan target can also be specified by entering the path of the folder or file(s) you want to include. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. When performing a scan, you can choose from three cleaning levels by clicking **Setup...** > **ThreatSense parameters** > **Cleaning**.

Performing computer scans with Custom scan is suitable for advanced users with previous experience using antivirus programs.

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.

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 content for malware and other potential threats.

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

Repeat last scan

Allows you to quickly launch the previously performed scan using the same settings it was run with.

You can select **No action**, **Shutdown** or **Reboot** from **Action after scan** drop-down menu. The actions **Sleep** or **Hibernate** are available based on your computer Power & sleep operating system settings or your computer/laptop capabilities. The selected action will start after all of the running scans are finished. When **Shutdown** is selected, a shutdown confirmation dialog window will display a 30-second countdown (click **Cancel** to deactivate the requested shutdown). See Advanced scan options for more details.

> **Note**
> 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

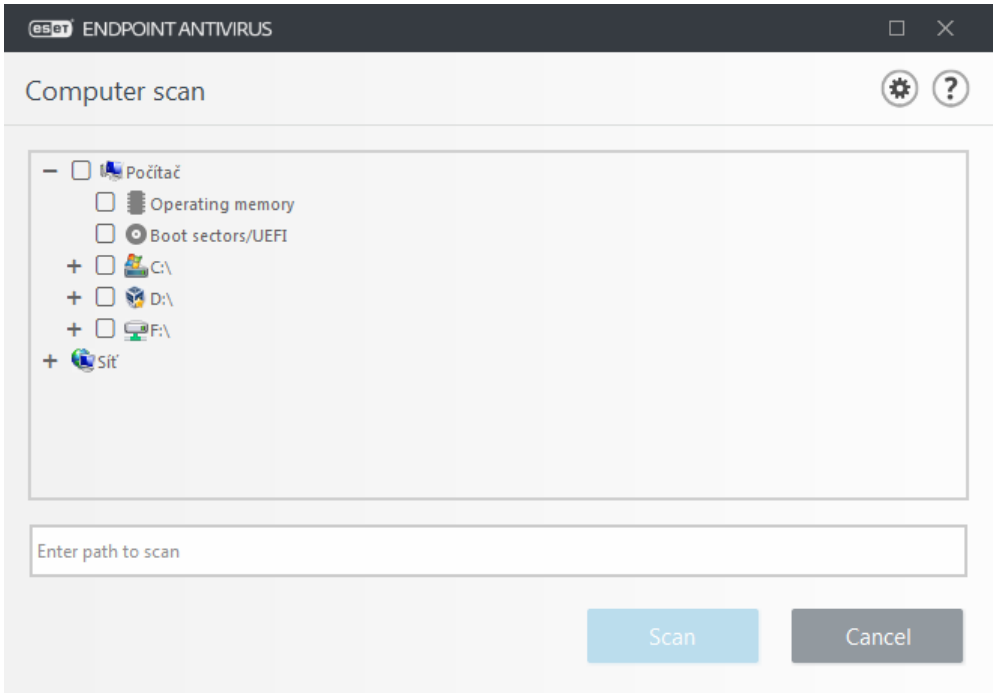
If only want to scan a specific target, you can use the Custom scan tool by clicking **Computer scan** > **Custom scan** and selecting an option from the **Scan targets** drop-down menu or selecting specific targets from the folder (tree) structure.

The scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** – Selects targets set in 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** – Allows user to create a custom selection of targets.

To quickly navigate to a scan target or add a target folder or file(s), enter the target directory in the blank field below the folder list.



Infected items are not cleaned automatically. Scanning without cleaning can be used to obtain an overview of the current protection status. Furthermore, you can choose from three cleaning levels by clicking **Advanced setup** > **Detection engine** > **On-demand scan** > **ThreatSense parameters** > **Cleaning**. If you are only interested in scanning the system without additional cleaning actions, 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 choose a profile from the **Scan profile** drop-down menu to be used for scanning chosen targets. The default profile is **Smart scan**. There are two more pre-defined scan profiles called **In-depth scan** and **Context menu scan**. These scan profiles use different ThreatSense parameters. The available options are described in **Advanced setup** > **Detection engine** > **Malware scans** > **On-demand scan** > ThreatSense parameters.

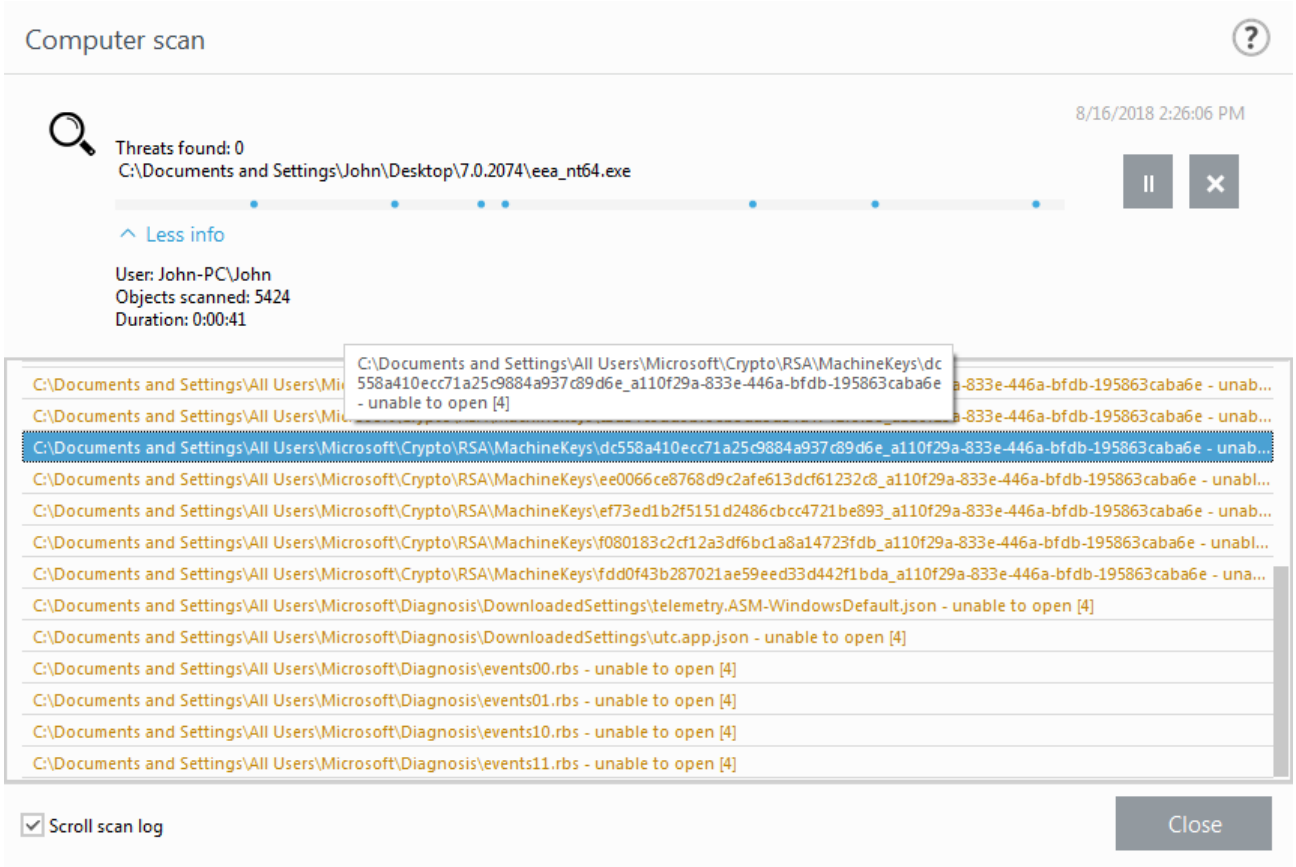
Click **Scan** to execute the scan using the custom parameters that you have set.

Scan as Administrator allows you to execute the scan under the Administrator account. Click this if the current user doesn't have privileges to access the appropriate files to be scanned. Note that this button is not available if the current user cannot call UAC operations as Administrator.

> **Note**
> 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.



> **Note**
> It is normal that some files, such as password protected files or files exclusively being used by the system (typically *pagefile.sys* and certain log files), cannot be scanned.

Scan progress – The progress bar shows the status of already-scanned objects compared to objects still waiting be scanned. The scan progress status is derived from the total number of objects included in scanning.

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

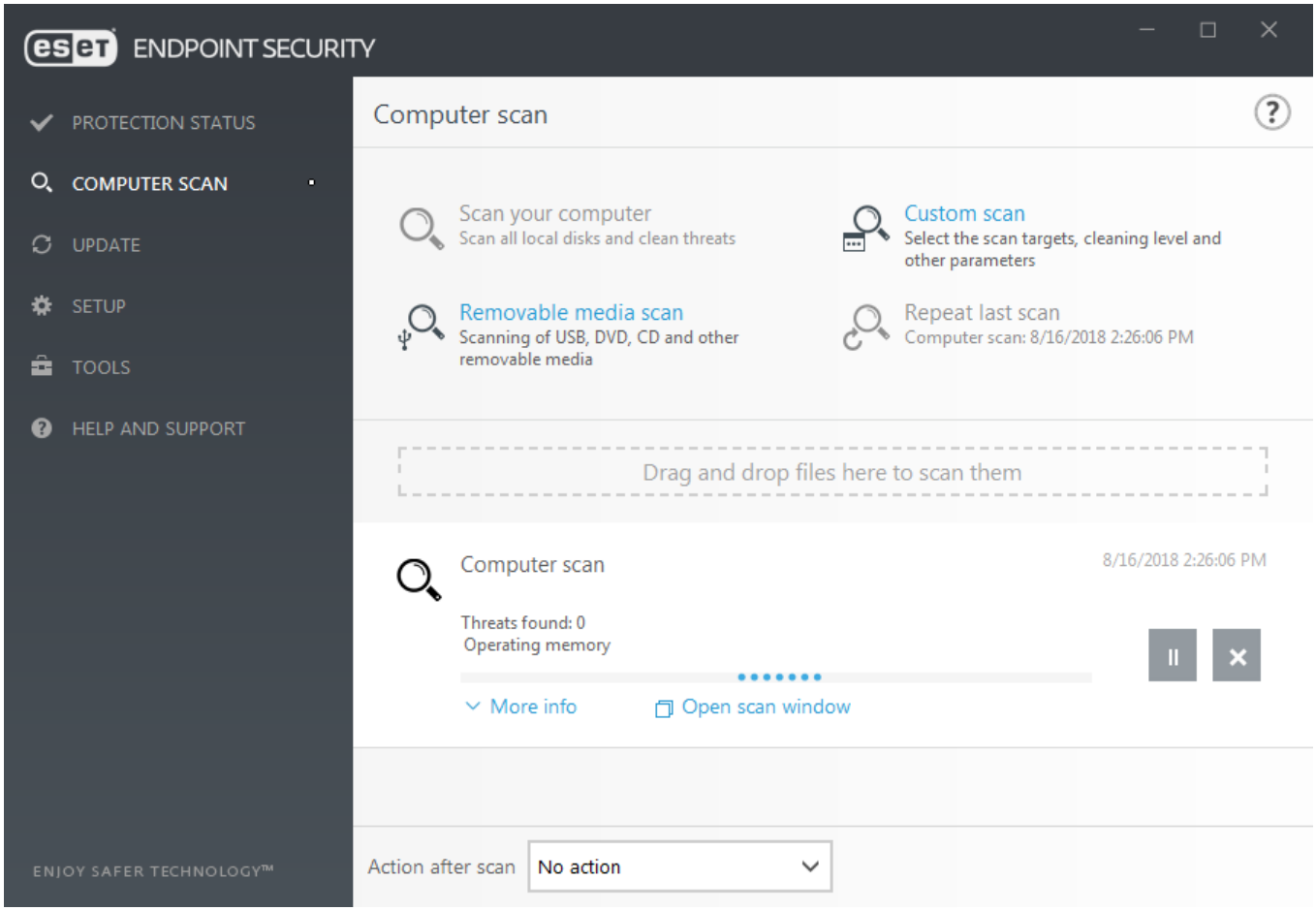
Threats found – Shows the total number of threats found during a scan.

Pause – Pauses a scan.

Resume – This option is visible when scan progress is paused. Click **Resume** to continue scanning.

Stop – Terminates 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.



Computer scan log

The Computer scan log gives you general information about the scan such as:

- Date and time of scan
- Scanned disks, folders and files
- Number of scanned objects
- Number of threats found
- Time of completion
- Total scanning time

Malware scans

The **Malware scans** section is accessible in the Advanced setup menu. Press the **F5** key, click **Detection engine** > **Malware scans** and provides options to select scanning parameters. This section includes the following options:

- **Selected profile** – A specific set of parameters used by the on-demand scanner.
  To create a new profile, click **Edit** next to **List of profiles**. See Scan profiles for more details.
- **On-demand & Machine learning protection** – see Detection engine (7.2 and later).

- **Scan targets** – If you only want to scan a specific target, you can click **Edit** next to **Scan targets** and select an option from the drop-down menu or select specific targets from the folder (tree) structure. See Scan targets for more details.
- **ThreatSense parameters** – Advanced setup options, such as file extensions you want to control, detection methods used, etc. can be found in this section. Click to open a tab with advanced scanner options.

Idle-state scan

You can enable the idle-state scanner in **Advanced setup** under **Detection engine** > **Malware scans** > **Idle-state scan.**

Idle-state scan

Set the switch next to Enable Idle-state scanning to **On** 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 activating the switch next to **Run even if computer is powered from battery** in Advanced setup.

Turn on the **Enable logging** switch in Advanced setup to record a computer scan output in the Log files section (from the main program window click **Tools** > **Log files**, and then 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 in order to trigger the idle-state scanner.

Click ThreatSense engine parameter setup to modify scan parameters (for example, detection methods) for the Idle-state scanner.

Scan profiles

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 the Advanced setup window (F5) and click **Detection engine** > **Malware scans** > **On-demand scan** > **List of profiles**. 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 the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

> **Note**
> 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 **Strict cleaning**. Enter 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 window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** – Selects targets set in 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** – Allows user to create a custom selection of targets.

To quickly navigate to a scan target or add a target folder or file(s), enter the target directory in the blank field below the folder list.

Advanced scan options

In this window, you can specify advanced options for a scheduled computer scan task. You can set an action to be performed automatically after a scan finishes using the drop-down menu:

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

> **Note**
> Please keep in mind that a sleeping computer is still a working computer. It is still running basic functions and using electricity when your computer is operating on battery power. To preserve battery life, for example when traveling outside of your office, we recommend using the Hibernate option.

Select **Action cannot be canceled by user** 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 the Scan progress chapter.

Device control

ESET Endpoint Security provides automatic device (CD/DVD/USB/...) control. This module allows you to block or adjust extended filters/permissions and define a users ability to access and work with a given device. This may be useful if the computer administrator wants to prevent the use of 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
- All device types

Device control setup options can be modified in **Advanced setup** (F5) > **Device control**.

Turning the switch on next to **Enable Device control** (formerly Integrate into system) activates the Device control feature in ESET Endpoint Security; you will need to restart your computer for this change to take effect. Once Device control is enabled, the **Rules** will become active, allowing you to open the Rules editor window.

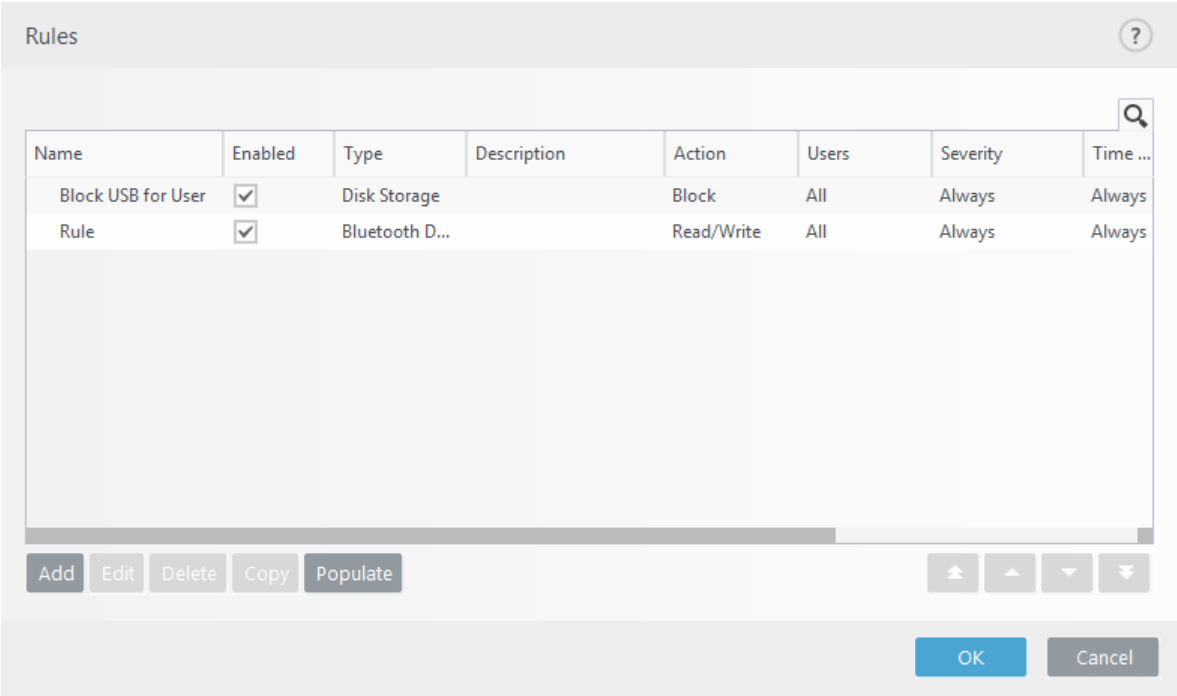
If a device blocked by an existing rule is inserted, a notification window will be displayed and access to the device

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.

> **Illustrated instructions**
> 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 predefined 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, about device vendor, model and serial number (if available).

If a device is selected (from the list of Detected devices) and **OK** is clicked, a rule editor window appears with predefined information (all settings can be adjusted).

Device groups

> Warning
> 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 respective group and the left part of the window contains created groups. Select a group with a list of devices you want to display 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 a devices from the populated list to add it to the group by clicking **OK**.

Control elements

Add – You can add a group by entering its name, or a device to existing group (optionally, you can specify details such as vendor name, model and serial number) depending on which part of the window you clicked the button.

Edit – Lets you modify the name of selected group or device's parameters (vendor, model, serial number).

Delete – Deletes selected group or device depending on which part of the window you clicked on the button.

Import – Imports a list of devices from a file.

The **Populate** button provides an overview of all currently connected devices with information about: device type, about device vendor, model and serial number (if available).

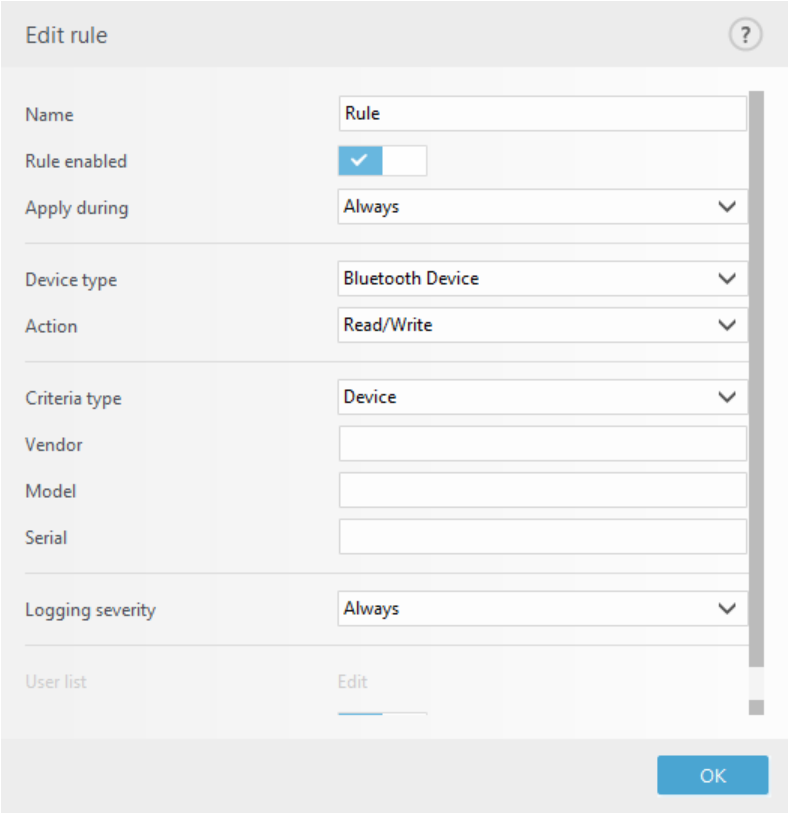
When you are done with customization click **OK**. Click **Cancel** if you want to leave the **Device groups** window without saving changes.

> Example
> You can create different groups of devices for which different rules will be applied. You can also create only one group of devices for which the rule with action **Read/Write** or **Read only** will be applied. This ensures blocking unrecognized devices by Device control when connected to your computer.

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 **Read Only** is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).

Adding Device control rules

A Device control rule defines the action that will be taken when a device meeting the rule criteria is connected to the computer.



Enter a description of the rule into the **Name** field for better identification. Click the switch next to **Rule enabled** to disable or enable this rule; this can be useful if you don't want to delete the rule permanently.

Apply during – Allows you to apply created rule during the certain time. From the drop-down menu, select created time slot. For more information click here.

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.

> **Note**
> 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 allow you to select one of the following rights settings:

- **Read/Write** – Full access to the device will be allowed.
- **Block** – Access to the device will be blocked.
- **Read Only** – 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 upon 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 **Read Only** 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 and tailor them to devices. All parameters are case-sensitive:

- **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.

> **Note**
> If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-sensitive, and no wildcards (*, ?) are supported.

> **Note**
> 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 allows you to select desired users.
- **Delete** – Removes the selected user from the filter.

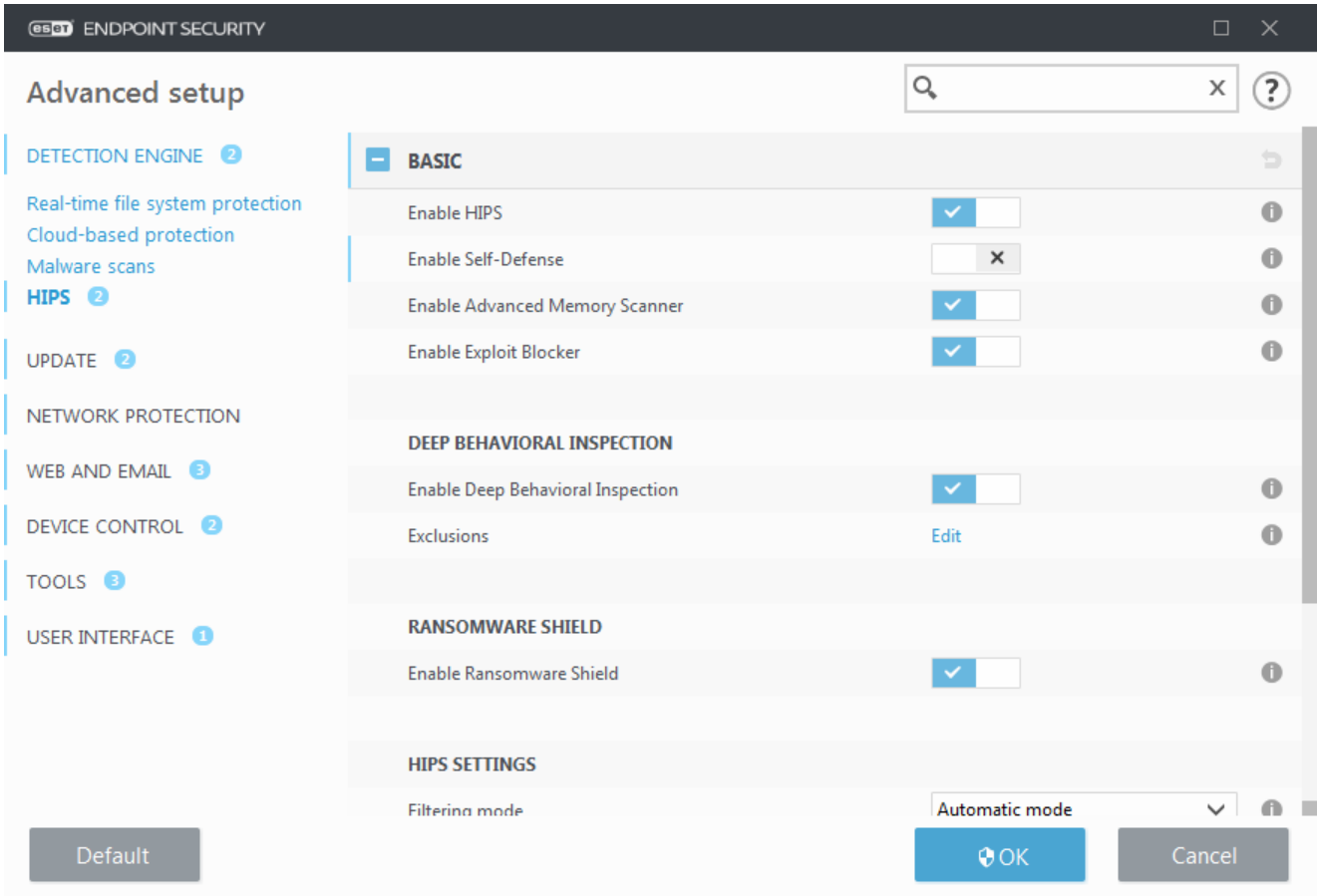
> **Note**
> Not all devices can be filtered by user rules, (for example imaging devices do not provide information about users, only about actions).

Host-based Intrusion Prevention System (HIPS)

> **Warning**
> 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.

HIPS settings can be found in **Advanced setup** (F5) > **Detection engine** > **HIPS** > **Basic**. The HIPS state (enabled/disabled) is shown in the ESET Endpoint Security main program window, in the **Setup** > **Computer**.



Basic

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 MS 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 enable 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 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 ESMC or ESET PROTECT Cloud 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 interactive window

The HIPS notification window allows you to create a rule based on new actions that HIPS detects and then define the conditions under which to allow or deny that 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).

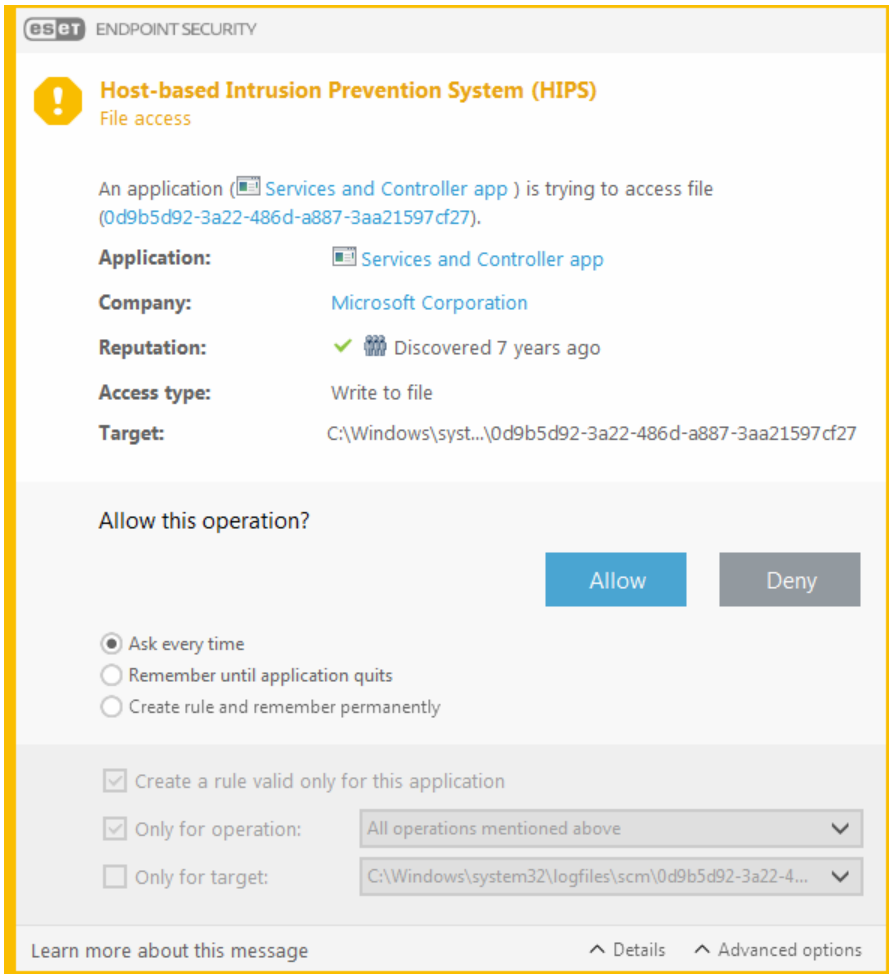
Click **Details** on the bottom to see what application triggers the operation, what is the reputation of the file or what kind of operation you are asked to allow or deny.

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.

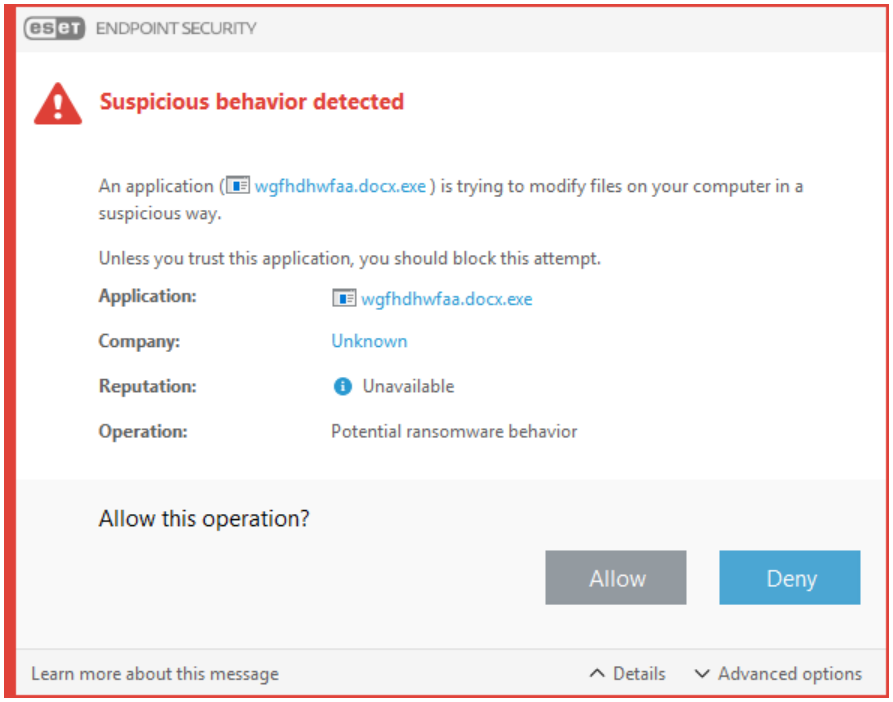
- **Only for target** –Select the rule file/application/registry target(s).

> **Endless HIPS notifications?**
> To stop the notifications from appearing, change the filtering mode to **Automatic mode** in **Advanced setup** (F5) > **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 allows you **Submit for analysis** or **Exclude from detection**.

> **Important**
> 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 small pop-up 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 this switch 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 small pop-up window 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.

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.

> **Note**
> Some operations of specific rules predefined 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.

Descriptions of important operations:

File operations

- **Delete file** – Application is asking for permission to delete the target file.
- **Write to file** – Application is asking for permission to write to the target file.
- **Direct access to disk** – Application is trying to read from or write to the disk in a non-standard way that will circumvent common Windows procedures. This may result in files being modified without the application of corresponding rules. This operation may be caused by malware trying to evade detection, backup software trying to make an exact copy of a disk, or a partition manager trying to reorganize disk volumes.
- **Install global hook** – Refers to calling the SetWindowsHookEx function from the MSDN library.
- **Load driver** – Installation and loading of drivers onto the system.

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.

> **Note**
> It is not possible to intercept process operations on the 64-bit version of Windows XP.

Registry operations

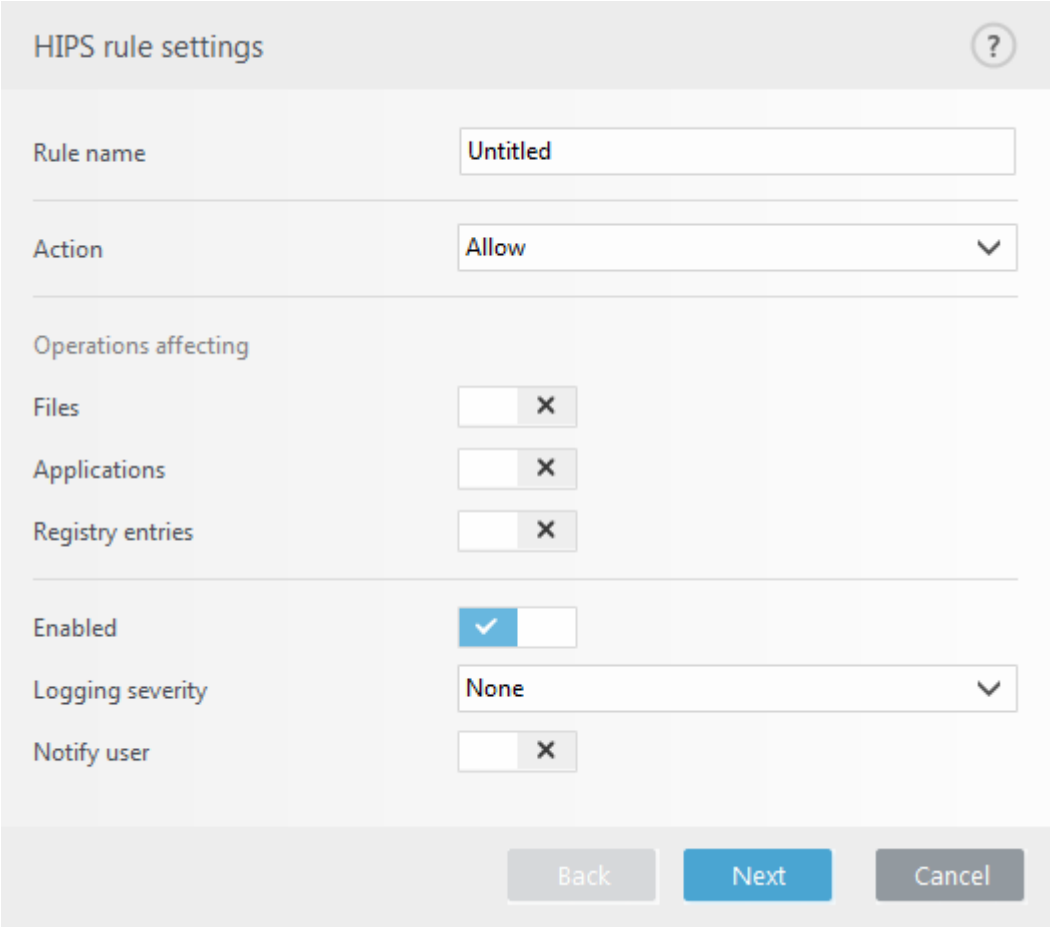
- **Modify startup settings** – Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for the Run key in the Windows Registry.
- **Delete from registry** – Deleting a registry key or its value.
- **Rename registry key** – 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.

> **Note**
> **Using wildcards in rules**
> An asterisk in rules can only be used to substitute a particular 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). In order 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.

> **Warning**
> 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.



HIPS advanced setup

The following options are useful for debugging and analyzing an application's behavior:

Drivers always allowed to load – Selected 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.

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.

> **Note**
> 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.

Presentation mode

Presentation mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. Presentation mode can also be used during presentations that cannot be interrupted by antivirus activity. When enabled, all pop-up windows are disabled and scheduled tasks are not run. System protection still runs in the background, but does not require any user interaction.

Click **Setup** > **Computer** and then click the switch next to **Presentation mode to enable presentation mode manually. I**n **Advanced setup** (F5), click **Tools** > **Presentation mode**, and then click the switch next to **Enable Presentation mode when running applications in full-screen mode automatically to have ESET Endpoint Security engage Presentation mode automatically when full-screen applications are run**. 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 enabled** in orange.

When **Enable Presentation mode when running applications in full-screen automatically is engaged,** Presentation mode will start whenever you initiate a full-screen application and will automatically stop after you exit the application. This is especially useful for starting Presentation mode immediately after starting a game, opening a full screen application or starting a presentation.

You can also select **Disable Presentation mode automatically after** to define the amount of time in minutes after which Presentation mode will automatically be disabled.

> **Note**
> 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 webpage 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.

Startup scan

By default, the automatic startup file check will be performed on system startup and during modules updates. This scan is dependent upon the Scheduler configuration and tasks.

Startup scan options are a part of the **System startup file check** scheduler task. To modify Startup scan settings, navigate to **Tools** > **Scheduler**, click on **Automatic startup file check** and then click **Edit**. In the last step, the Automatic startup file check window will appear (see the following chapter for more details).

For detailed instructions about Scheduler task creation and management, see Creating new tasks.

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 secret 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 that are 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 aforementioned group.

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 the **Advanced setup** window (press **F5**) > **Detection engine** > **Malware scans** > **Document protection** and click the **Enable Document protection** (formerly Integrate into system) switch.

> **Note**
> This feature is activated by applications that use the Microsoft Antivirus API (for example, Microsoft Office 2000 and higher, or Microsoft Internet Explorer 5.0 and higher).

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 allow you to 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 allow you to 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.

The exclusions in version 7.1 and below have both Performance exclusions and Detection exclusions merged into one.

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

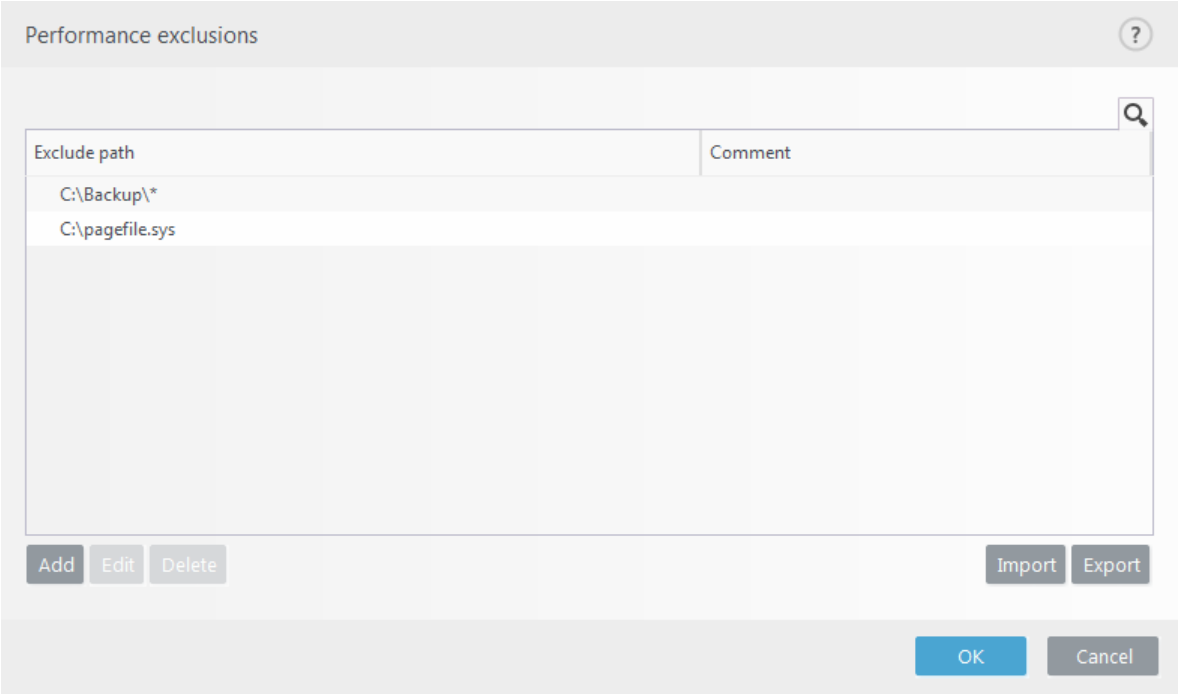
Performance exclusions

Performance exclusions allow 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 folder to be excluded from scanning into the list of exclusions via **Advanced setup** (**F5**) > **Detection engine** > **Exclusions** > **Performance exclusions** > **Edit**.

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



> **Note**
> 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

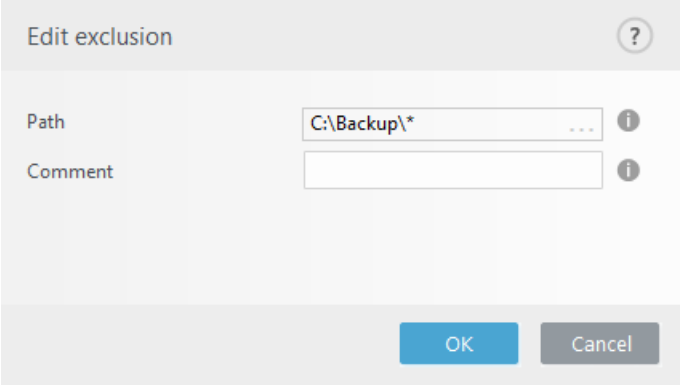
```
# {"product":"endpoint","version":"7.2.2055","path":"plugins.01000600.settings.Perfo
rmanceExclusions","columns":["Path","Description"]}

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.

Choose path or enter manually

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.

Exclusion format

- If you want to exclude all files 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)

System variables in exclusions

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.

Path exclusions using an asterisk

A few more exclusion examples using an asterisk:
*C:\Tools** – The path must ends with the backslash and asterisk to indicate that it is a folder and all its subfolders that are being excluded.
C:\Tools.dat* – This will exclude .dat files in the *Tools* folder.
C:\Tools\sg.dat – This will exclude this particular file located in the exact path.
An exception for performance exclusions:
C:\Tools.** – Same behavior as *C:\Tools** (not to be confused that the mask *.* will exclude only files with extensions in the *Tools* folder).
A wrong manually entered exclusion example:
C:\Tools – *Tools* folder will not be excluded. From the scanner perspective, *Tools* can also be a file name.
C:\Tools – Do not forget to add the asterisk at the end of the path: *C:\Tools**

Wildcards in the middle of a path

We highly recommend that you do not use wildcards in the middle of a path (for example *C:\Tools*\Data\file.dat*) unless your system infrastructure requires it. 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.

Exclusion format

- If you want to exclude all files 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)

System variables in exclusions

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.

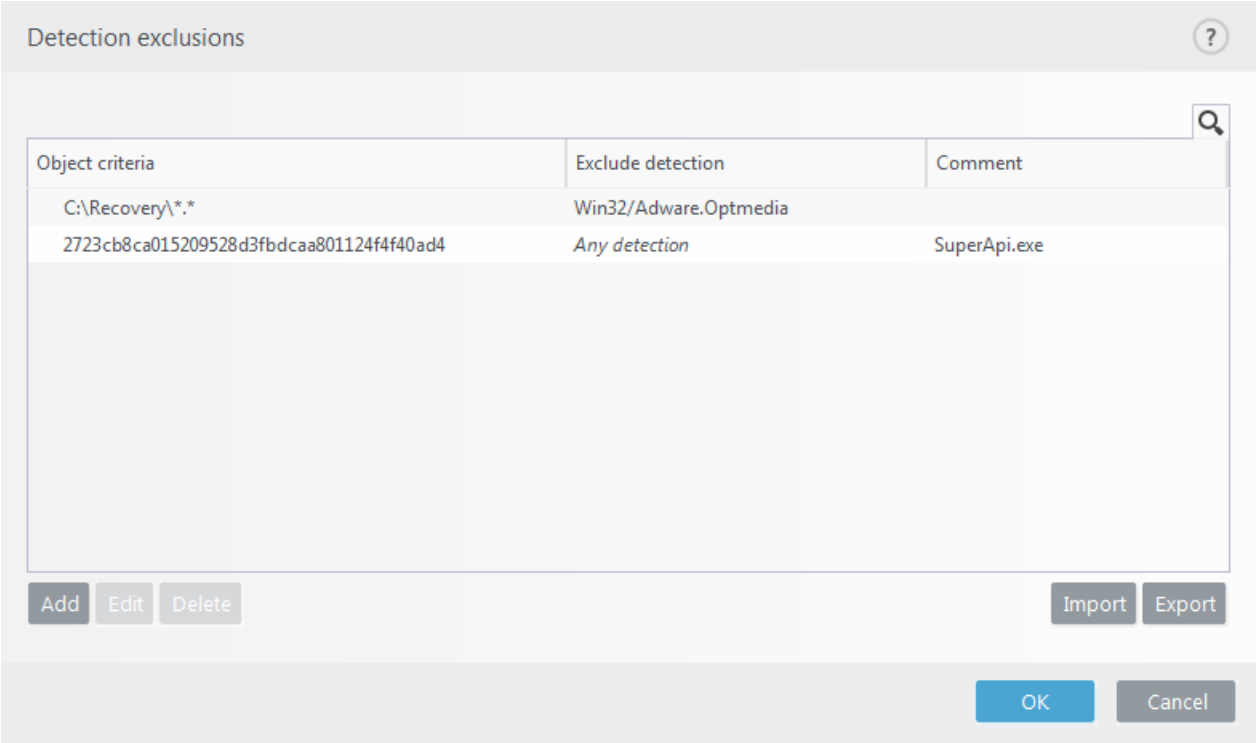
Detection exclusions

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

How detection exclusions work

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, **Advanced setup** (**F5**) > **Detection engine** > **Exclusions** > **Detection exclusions** > **Edit**.

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

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. This type of exclusion can only be used for certain types of infiltrations and it can be created either in the alert window reporting the infiltration (click **Show advanced options** and then select **Exclude from detection**), or by clicking **Tools** > **Quarantine** and then right-clicking the quarantined file and selecting **Restore and exclude from scanning** from the context menu.
- **Hash** – Excludes a file based on a specified hash (SHA1), regardless of the file type, location, name or its 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

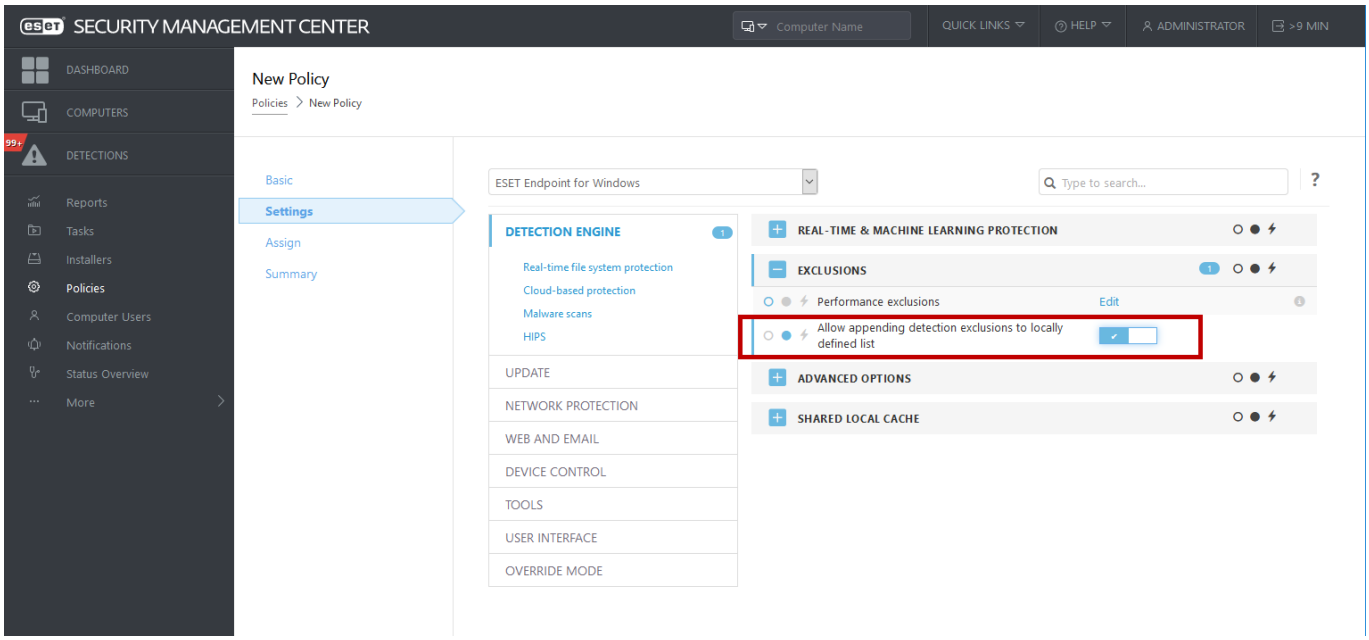
```
# {"product":"endpoint","version":"7.2.2055","path":"Settings.ExclusionsManagement.D
etectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}

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

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

Detection exclusions setup in ESMC

ESMC 7.1 includes a new wizard for detection exclusions management—create a detection exclusion and apply it to more computers/group(s).

Possible detection exclusions override from ESMC

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 ESMC will work as expected.

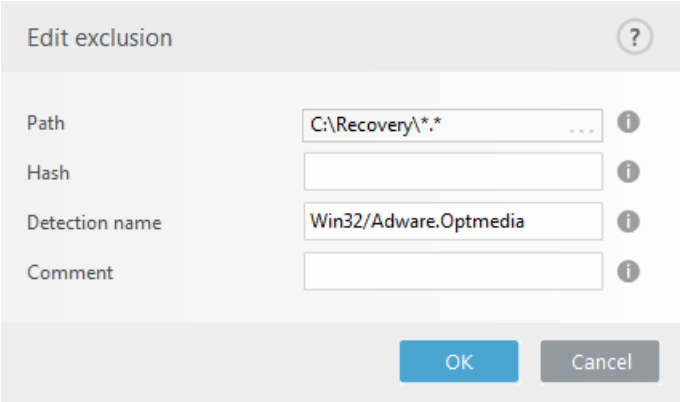


Add or Edit detection exclusion

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.

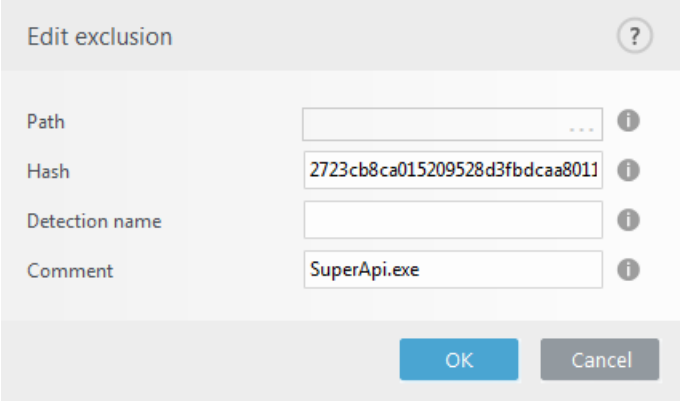
See also Path exclusion format.



See the Detection exclusions example below.

Exclude hash

Excludes a file based on a specified hash (SHA1), regardless of the file type, location, name or its extension.



Exclusions by detection name

To exclude a specific detection by its name, enter 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):

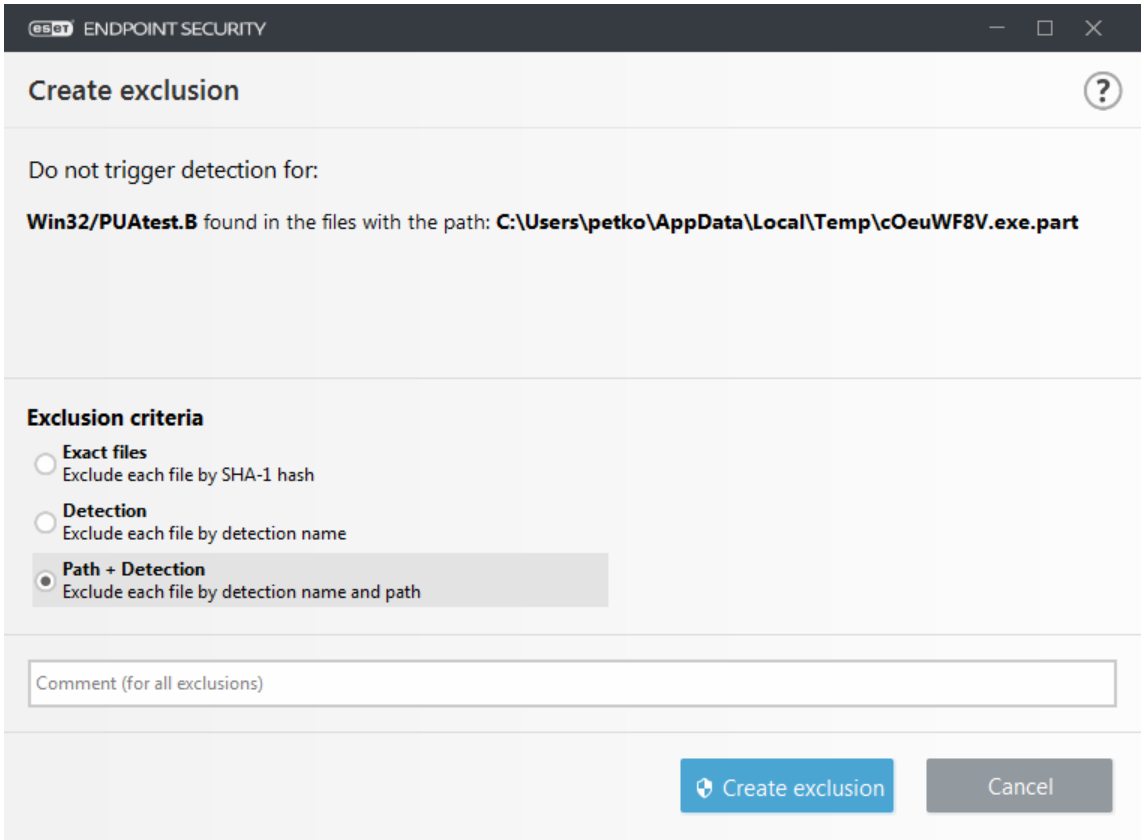
1. In the main program window, click **Tools** > **Log files**.
2. Right-click a detection in the **Detections log**.
3. Click **Create exclusion**.

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*).

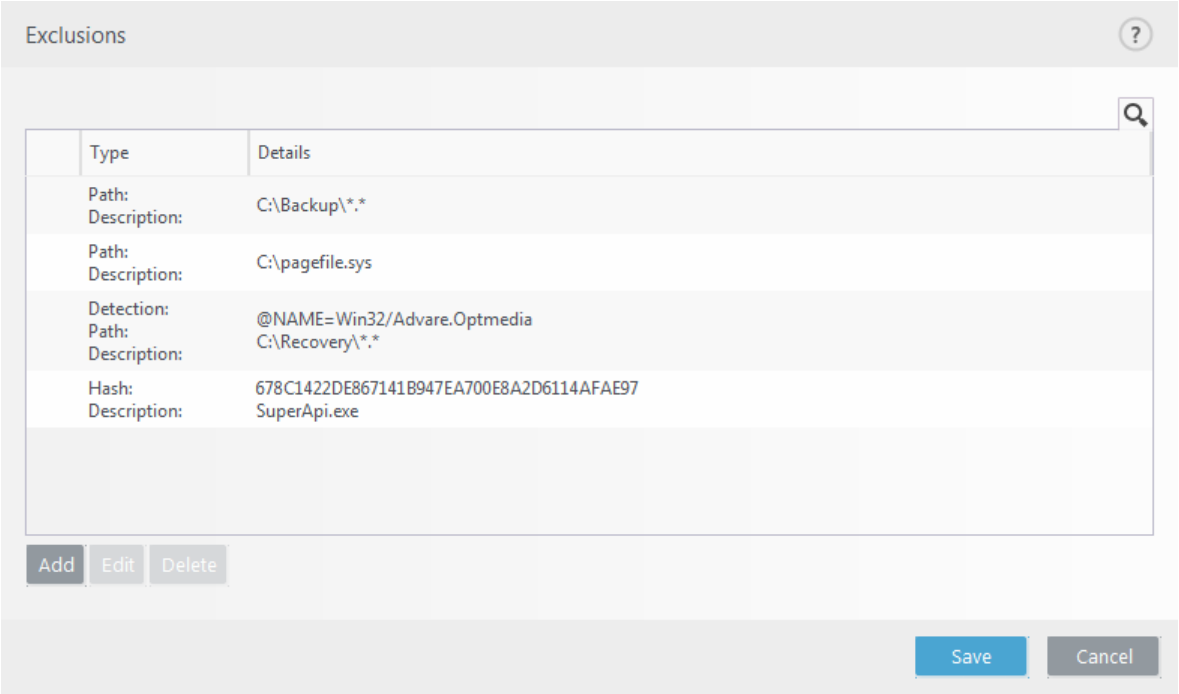
The recommended option is pre-selected based on the detection type.

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



Exclusions (7.1 and below)

The exclusions in version 7.1 and below have both Performance exclusions and Detection exclusions merged into one.



Processes exclusions

The Processes exclusions feature allows 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. Similar problems can occur when attempting live migrations of virtual machines. 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.

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 via **Advanced setup** (**F5**) > **Detection engine** > **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.

Example

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.

> **Important**
> If you do not use browse function when selecting process executable, you need to manually enter 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.

> **Note**
> 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 you to 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*).

> **Example**
> Select the file path of an excepted application by clicking ... (for example *C:\Program Files\Firefox\Firefox.exe*). Do NOT enter 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.

> **Important**
> If you do not use browse function when selecting process executable, you need to manually enter 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.

HIPS exclusions

Exclusions enable you to exclude processes from HIPS Deep Behavioral Inspection.

To exclude an object, click **Add** and enter the path to an object or select it in the tree structure. You can also **Edit** or **Delete** selected entries.

> **Learn more about exclusions**
> Refer to the Exclusions chapter.

ThreatSense parameters

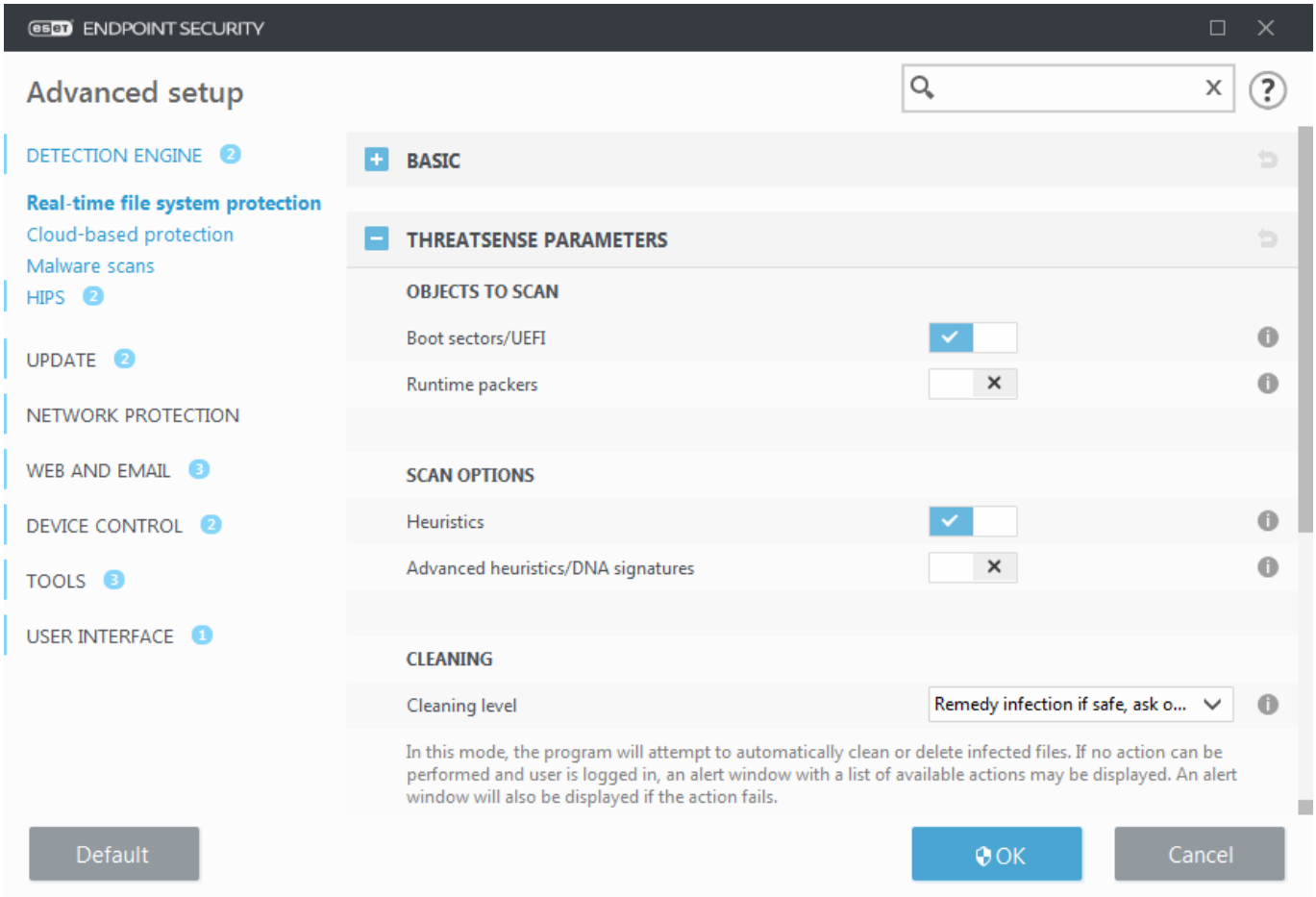
ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly 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 allow 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 parameters** in the Advanced setup window 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 allows 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 parameter setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters 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 particular 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 allows 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 entered 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 allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: unlimited.

> **Note**
> We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

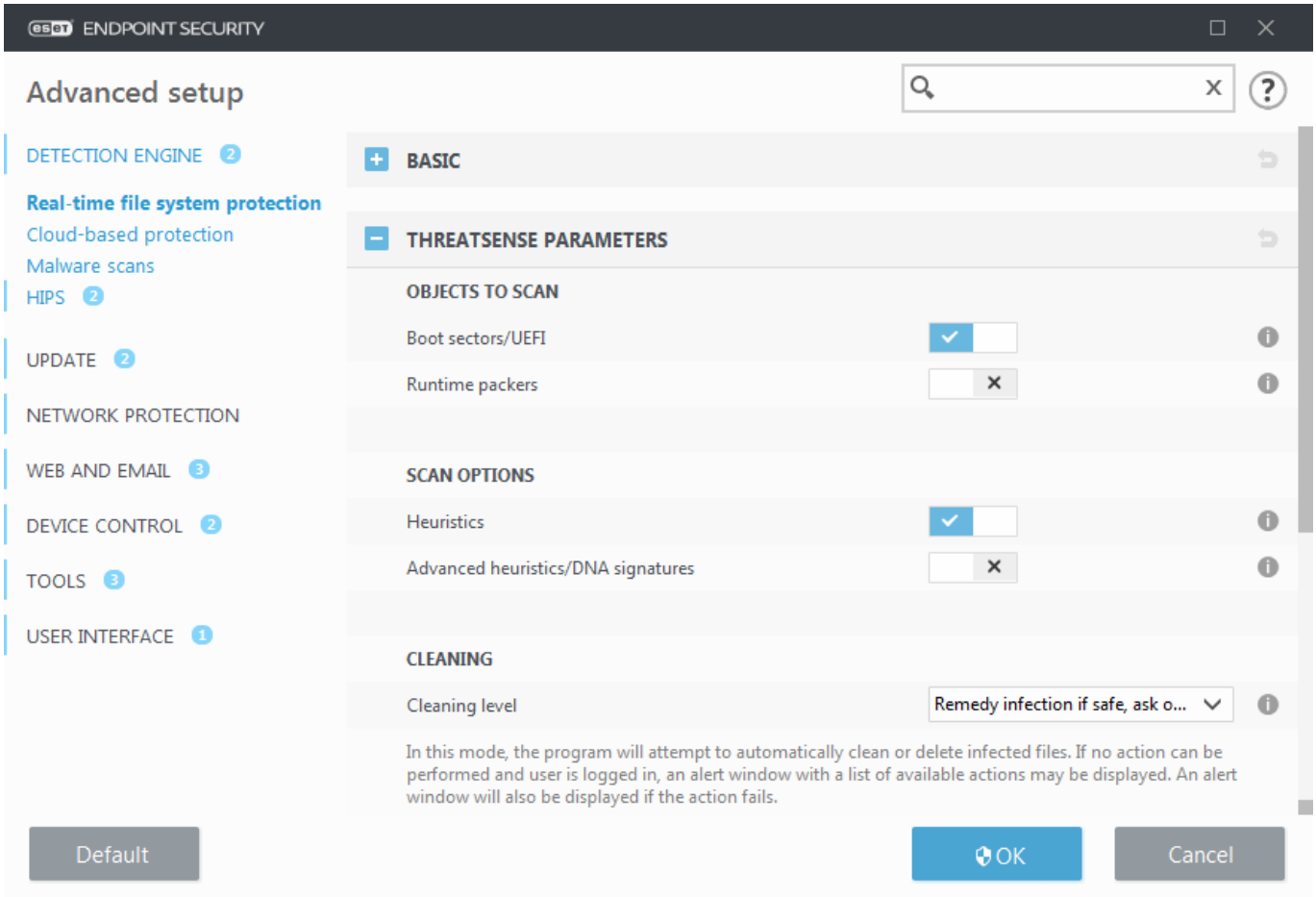
Cleaning levels

To access cleaning level settings for a desired protection module, expand **ThreatSense parameters** (for example, **Real-time file system protection**) and then click **Cleaning**.

Real-time protection and other protection modules have the following remediation (i.e. cleaning) levels.

Remediation in ESET Endpoint Security 7.2 and later

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.



Cleaning levels in ESET Endpoint Security 7.1 and below

Cleaning level	Description
No cleaning	Detections will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of a detection.
Normal cleaning	The program will attempt to automatically clean or delete detections based on a predefined action (depending on the type of infiltration). Detection and deletion of an object is signaled by a notification the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.
Strict cleaning	The program will clean or delete all detections. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

The mentioned cleaning level is applied when setting up an ESMC policy for older versions of ESET Endpoint Security:

Cleaning level in the ESMC policy	Applied cleaning level
Always remedy detection	Strict cleaning
Remedy detection if safe, keep otherwise	Normal cleaning
Remedy detection if safe, ask otherwise*	Normal cleaning
Always ask the end-user	No cleaning

* Default value when upgrading to version 7.2 and later with **Normal cleaning** set in ESET Endpoint Security.

File extensions excluded from scanning

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 parameter setup lets you define the types of files to scan.

> **Note**
> Not to be confused with other types of 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.

> **Example**
> 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`).

> **Note**
> In order to see the exact extension (if any) of a file in a Windows operating system you have to uncheck the **Hide extensions for known file types** option at **Control Panel** > **Folder Options** > **View** (tab) and apply this change.

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. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before the detection engine update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (.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, disable **Default archive scan settings**.

To learn more about **Runtime packers**, **Self-extracting archives** and **Advanced heuristics** see ThreatSense engine parameters setup.

Additional ThreatSense parameters for executed files – 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.

Network

The **Network** section allows you to have quick access to the following components or settings in Advanced setup:

- **Firewall** – Here you can adjust the filtering mode for the ESET Firewall. To access more detailed settings, click the gear wheel > **Configure** next to **Firewall**, or press **F5** to access **Advanced setup**.

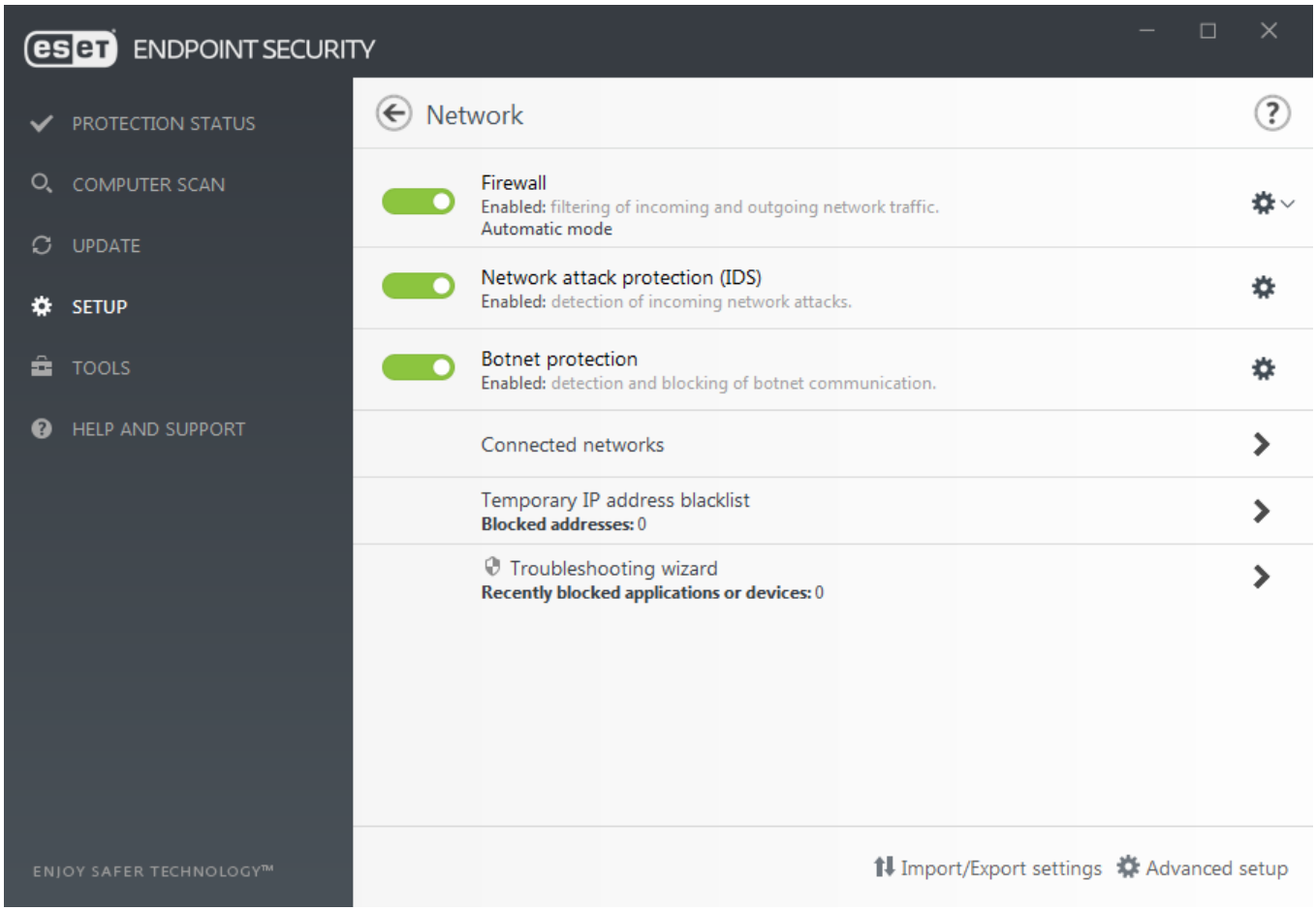
- Network attack protection (IDS) – Analyzes the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked. ESET Endpoint Security will inform you when you connect to an unprotected wireless network or a network with weak protection.

- **Botnet protection** – Quickly and accurately identifies malware in the system. To disable Botnet protection for a specific period of time, click (not recommended).

- **Connected networks** – Displays the networks to which network adapters are connected. After clicking the gear wheel, you will be prompted to select a protection type for the network you are connected to via your network adapter. In this window you can also see **Network adapters** in lower right corner. You can view each network adapter and its assigned firewall profile and trusted zone. For more detailed information, see Network adapters.

- **Temporary IP address blacklist** – View a list of IP addresses that have been detected as the source of attacks and added to the blacklist to block connections for a certain period of time. For more information, click this option and press F1.

- **Troubleshooting wizard** – Helps you solve connectivity problems caused by ESET Firewall. For more detailed information see Troubleshooting wizard.



Click the gear wheel ⚙ next to **Firewall** to access the following settings:

- **Configure...** – Opens the firewall window in Advanced setup, where you can define how the firewall will handle network communication.

- **Block all traffic** – All inbound and outbound communication will be 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. To restore the firewall to normal operation while Network traffic filtering is in the **Block all traffic** mode, click **Stop blocking all traffic**.

- **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. To re-enable the firewall while Network traffic filtering is in this mode, click **Enable firewall**.

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

- **Interactive mode** – (when another filtering mode is enabled) – Click to change the filtering mode to interactive filtering mode.

Firewall

The Firewall controls all network traffic to and from the system. This is accomplished by allowing or denying individual network connections based on specified filtering rules. It provides protection against attacks from remote computers and can block potentially threatening services.

Basic

Enable Firewall

We recommend that you leave this feature enabled to ensure the security of your system. With the firewall engaged, network traffic is scanned in both directions.

Also evaluate rules from Windows firewall

In automatic mode, allow also incoming traffic allowed by rules from Windows Firewall, unless explicitly blocked by ESET rules.

> **Important**
> Rules from Windows firewall configured using Group Policy (GPO) are not evaluated.

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	Allows 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 allows 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 predefined parameters. Learning mode should only be used until all rules for required communications have been created to avoid security risks.

Profiles can be used to customize the behavior of the ESET Endpoint Security Firewall by specifying different sets of rules in different situations.

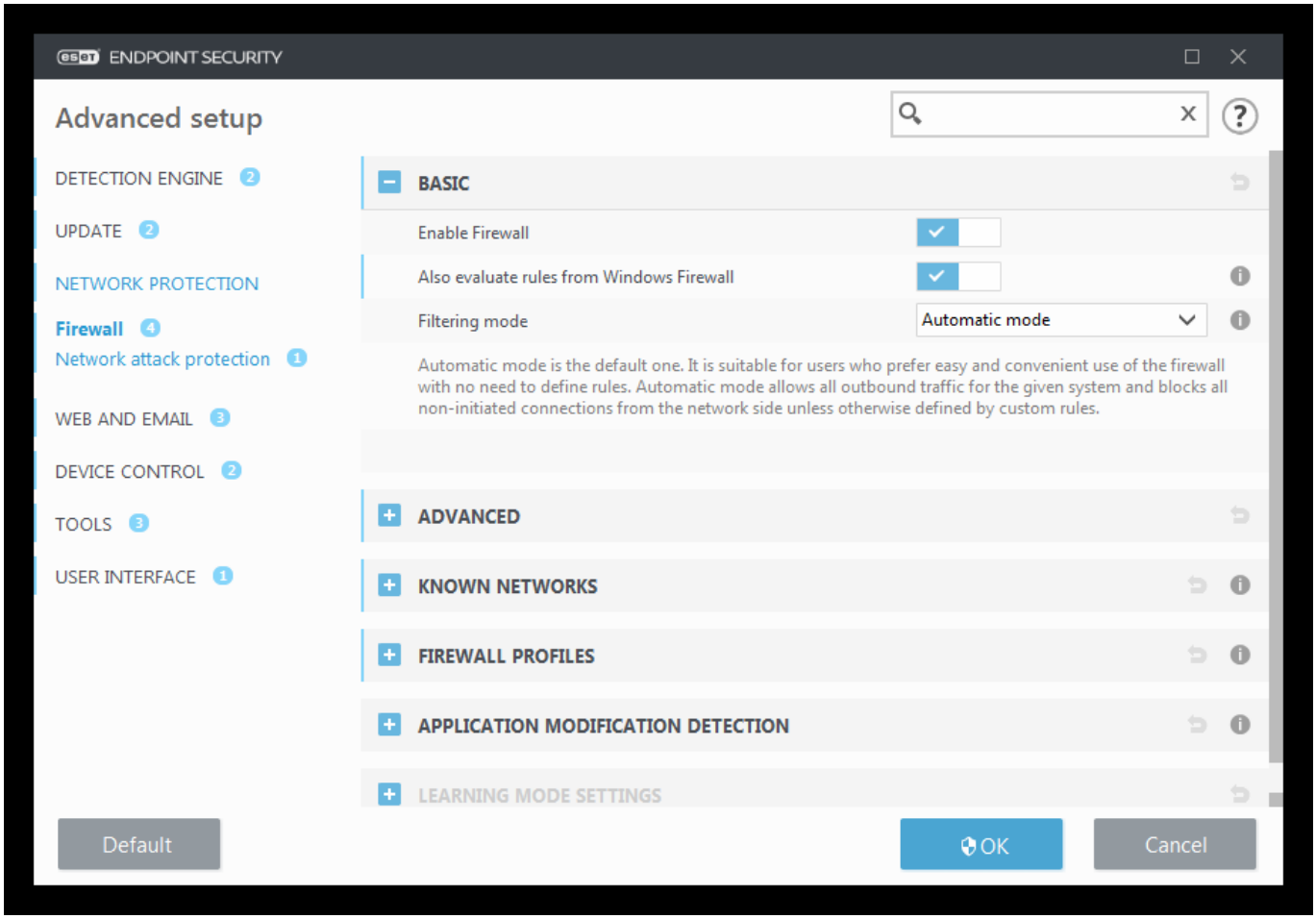
Advanced

Rules

Rules setup allows you to view all rules applied to traffic generated by individual applications within trusted zones and the Internet.

Zones

A zone represents a collection of network addresses that create one logical group.



> **Note**
> You can create an IDS exception when a Botnet attacks your computer. An exception can be modified in **Advanced setup** (F5) > **Network protection** > **Network attack protection** > **IDS exceptions** by clicking **Edit**.

Learning mode

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 predefined parameters.

This mode can expose your system to risk, and is only recommended for initial configuration of the firewall.

Select **Learning mode** from drop-down menu in **Advanced setup** (F5) > **Firewall** > **Basic** > **Filtering mode** to activate **Learning mode options**. This section includes the following items:

> **Warning**
> 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.

Mode set after learning mode expiration – Define which filtering mode the ESET Endpoint Security Firewall will revert to after the time period for learning mode ends. Read more about filtering modes. After expiration, the **Ask user** option requires administrative privileges to perform a change to the firewall filtering mode.

Communication type – Select specific rule creation parameters for each type of communication. There are four types of communication:

- **Inbound traffic from the Trusted zone** – An example of an incoming connection within the trusted zone would be a remote computer 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 computer within the local network, or within a network in the trusted zone.

- **Inbound Internet traffic** – A remote computer attempting to communicate with an application running on the computer.

- **Outbound Internet traffic** – A local application attempting to establish a connection to another computer.

Each section allows 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 computer or a group of networked computers.

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 appropriate count of rules for this application. This option allows you to limit the number of rules that can be created for one application.

Network attack protection

Enable Network attack protection (IDS) – Analyses the content of network traffic and protects from network attacks. Any traffic which is 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 exceptions – This option allows you to configure advanced filtering options to detect several types of attacks and exploits that might be used to harm your computer.

Advanced filtering options

The Firewall and Network attack protection sections allow you to configure advanced filtering options to detect several types of attacks and vulnerabilities that can be carried out against your computer.

> **Notifications and logging**
> In some cases you will not receive a threat notification about blocked communications. Please consult the Logging and creating rules or exceptions from log section for instructions to view all blocked communications in the firewall log.

> **Availability of particular options in this help page**
> The availability of particular options in Advanced setup (**F5**) > **Network Protection** > **Firewall** and Advanced setup (**F5**) > **Network Protection** > **Network attack protection** may vary depending on the type or version of your firewall module, as well as the version of your operating system.

Allowed services

Settings in this group are meant to simplify the configuration of access to this computer´s services from the trusted zone. Many of them enable/disable predefined firewall rules.

- **Allow file and printer sharing in the Trusted zone** – Allows remote computers in the Trusted zone to access your shared files and printers.

- **Allow UPNP for system services in the Trusted zone** – Allows incoming and outgoing requests of UPnP protocols for system services. UPnP (Universal Plug and Play also known as Microsoft Network Discovery) is used in Windows Vista and later operating systems.

- **Allow incoming RPC communication in the Trusted zone** – Enables TCP connections from the Trusted zone allowing access to the MS RPC Portmapper and RPC/DCOM services.

- **Allow remote desktop in the Trusted zone** – Enables connections via Microsoft Remote Desktop Protocol (RDP) and allows computers in the Trusted zone to access your computer using a program that uses RDP (for example, "Remote Desktop Connection"). See also how to allow RDP connections outside Trusted zone.

- **Enable logging into multicast groups through IGMP** – Allows incoming/outgoing IGMP and incoming UDP multicast streams, for example video streams generated by applications using the IGMP protocol (Internet Group Management Protocol).

- **Allow communication for bridged connections** – Select this option to avoid terminating bridged connections. Bridged networking connects a virtual machine to a network using the host computer's Ethernet adapter. If you use bridged networking, the virtual machine can access other devices on the network, and vice versa as if it were a physical computer on the network.

- **Allow Metro applications** – Communication of Windows Store applications that are running in the Metro environment is allowed according to the Metro application manifest. This option will override all rules and exceptions for Metro applications regardless of whether you have selected Interactive mode or Policy-based

mode in ESET Firewall settings.

- **Allow automatic Web Services Discovery (WSD) for system services in the Trusted zone** – Allows incoming Web Services Discovery requests from Trusted zones through the firewall. WSD is the protocol used to locate services on a local network.

- **Allow multicast addresses resolution in the Trusted zone (LLMNR)** – The LLMNR (Link-local Multicast Name Resolution) is a DNS packet based protocol that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link without requiring a DNS server or DNS client configuration. This option allows incoming multicast DNS requests from the Trusted zone through the firewall.

- **Windows HomeGroup support** – Enables HomeGroup support for Windows 7 and later operating systems. A HomeGroup is able to share files and printers on a home network. To configure a Homegroup, navigate to **Start** > **Control Panel** > **Network and Internet** > **HomeGroup**.

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 in order 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. Please 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.

- **Allow response to ARP requests from outside the Trusted zone** – Select this option if you want the system to respond to ARP requests with IP addresses that are not from the Trusted zone. ARP (Address Resolution Protocol) is used by the network application to determine the Ethernet address.

- **DNS Poisoning attack detection** – Detection of DNS poisoning – relieving a fake answer to a DNS request (sent by an attacker) which can point you to fake and malicious websites. DNS (Domain name systems) are distributed database systems that translate between human-friendly domain names and numeric IP addresses and allow users to refer to a website simply by using its domain name. Read more about this type of attack in the glossary.

- **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 that have been detected as sources of attacks are

added to the Blacklist to prevent connection for a certain period of time.

- **Display notification after attack detection** – Turns on the system tray notification at the bottom right corner of the screen.

- **Display notifications also for 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 in order 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 in order 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 in order 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).

- **Check TCP connection status** – Checks to see if all TCP packets belong to an existing connection. If a packet does not exist in a connection, it will be dropped.

- **Maintain inactive TCP connections** – In order to function, some applications require that the TCP connection that they establish is maintained even though the TCP connection may be inactive. Select this option to avoid terminating inactive TCP connections.

- **TCP protocol overload detection** – The principle of this method involves exposing the computer/server to multiple requests – also see DoS (Denial of service attacks).

- **ICMP protocol message checking** – Prevents attacks that exploit the weaknesses of the ICMP protocol, which could lead to computer unresponsiveness - also see DoS (Denial of service attacks).

- **Covert data in ICMP protocol detection** – Checks to see if the ICMP protocol is used for data transfer. Many malicious techniques use the ICMP protocol to bypass the firewall.

Please see this ESET Knowledgebase article for an updated version of this help page.

IDS exceptions

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.

> **Illustrated instructions**
> The following ESET Knowledgebase articles may only be available in English:
> - Create IDS exclusions on client workstations in ESET Endpoint Security
> - Create IDS exclusions for client workstations in ESET Security Management Center

Columns

- **Alert** – Type of alert.

- **Application** – Select the file path of an excepted application by clicking **...** (for example *C:\Program Files\Firefox\Firefox.exe*). Do NOT enter the name of the application.

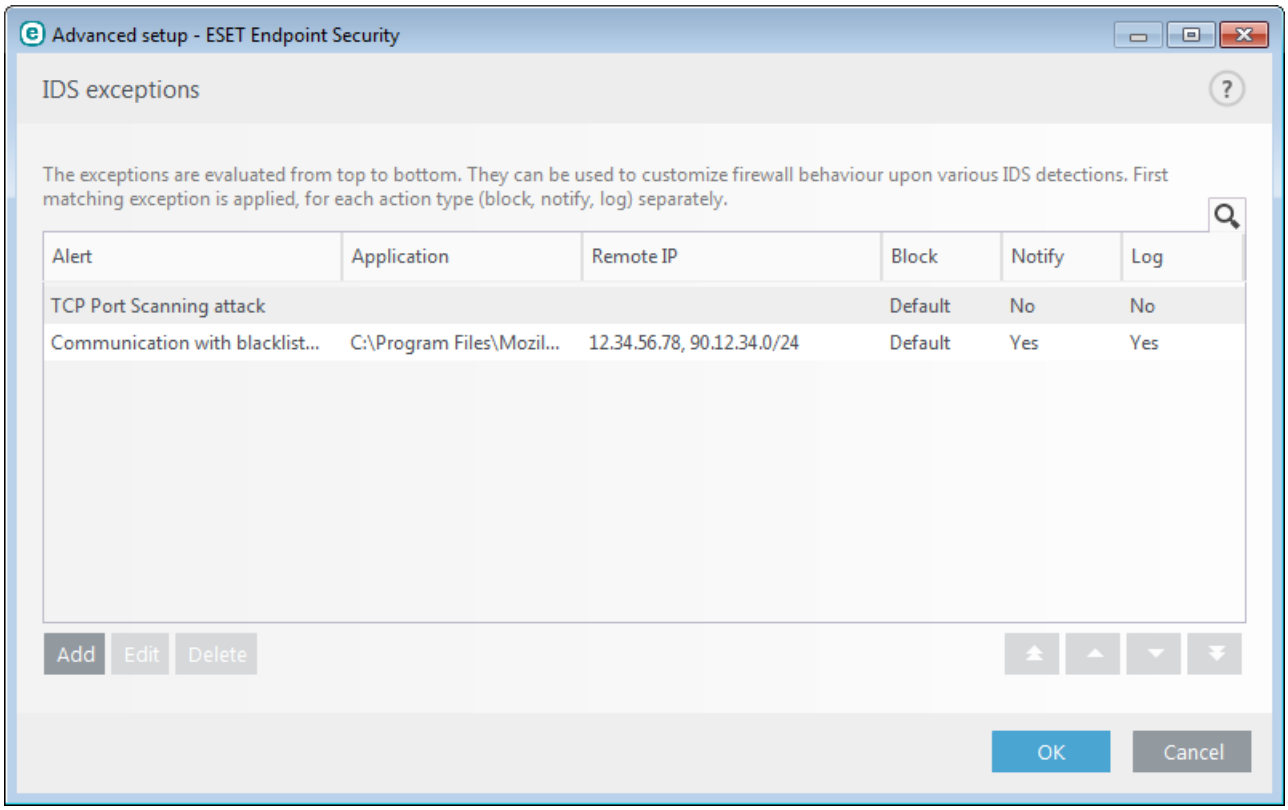
- **Remote IP** – A list of remote IPv4 or IPv6 address / ranges / subnets. Multiple addresses must be separated by a comma.

- **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

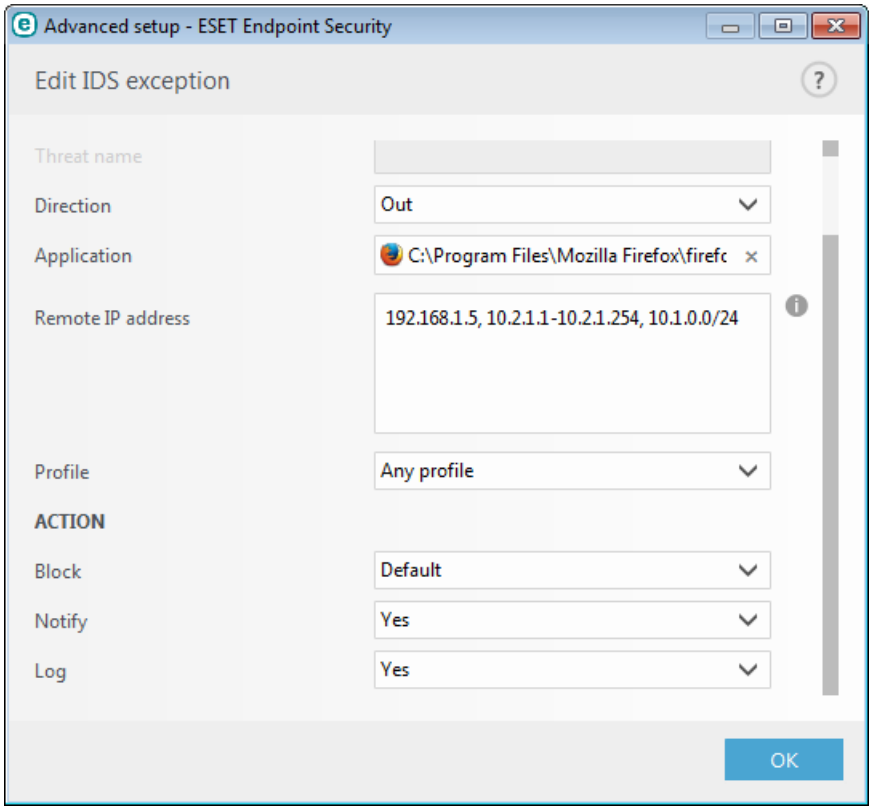
desktop notifications. The available values are **Default**/**Yes**/**No**.

- **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**.



Managing IDS exceptions

- **Add** – Click to create a new IDS exception.
- **Edit** – Click to edit an existing IDS exception.
- **Delete** – Select and click if you want to remove an existing exception from the list of IDS exceptions.
- **Top/Up/Down/Bottom** – Allows you to adjust the priority level of exceptions (exceptions are evaluated from top to bottom).



Example

You want to display a notification and collect a log each time the event occurs:

1.Click **Add** to add a new IDS exception.
2.Select particular alert from the **Alert** 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.

Example

You want to remove recurring notifications for a type of alert you do not consider to be a threat:

1.Click **Add** to add a new IDS exception.
2.Select particular alert from the **Alert** drop-down menu, for example **SMB session without security extensions** or **TCP Port Scanning attack**.
3.Select **In** from the direction drop-down menu in case 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 particular IP address, leave **Remote IP addresses** blank.
8.Click **OK** to save this notification.

Suspected threat blocked

This situation can occur when an application on your computer is trying to transmit malicious traffic to another computer on the network, exploiting a security hole or if someone is trying to scan ports on your network.

Threat – Name of the threat.

Source – Source network address.

Target – Target network address.

Stop blocking – Creates an IDS exception for the suspected threat with settings to allow communication.

Keep blocking – Blocks the detected threat. To create an IDS exception with settings to block communication for this threat, select **Do not notify me again**.

> **Note**
> 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.

Network protection troubleshooting

The Troubleshooting wizard helps you resolve connectivity problems caused by the ESET Firewall. 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 about the type of application or device, reputation and total number of application 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 **The application still doesn't work** and all communications previously blocked for that device will now be allowed. If the issue persist, restart the computer.

Click **Show changes** to see rules created by the wizard. Additionally, you can see rules created by the wizard **Advanced setup** > **Network protection** > **Firewall** > **Advanced** > **Rules**.

Click **Unblock another to troubleshoot communications issues with a different device or application.**

Connected networks

The Connected network section is accessible from the main program window of ESET Endpoint Security by clicking **Setup** > **Network** > **Connected networks**.

It shows the networks to which network adapters are connected. After clicking the link below the network name, you will be prompted to select a protection type (strict or allowed) for the network you are connected to via your network adapter, or you can click the gear wheel to change this selection in Advanced setup. This setting defines how accessible your computer is to other computers on the network.

Clicking the **Network adapters** in lower right corner of the window allows you to view each network adapter and its assigned firewall profile and trusted zone. For more detailed information, see Network adapters.

Known networks

When using a computer that frequently connects to public networks or networks outside of your normal work network, we recommend that you verify the network credibility of new networks that you are connecting to. Once networks are defined, ESET Endpoint Security can recognize trusted (Home/office) networks using various network parameters configured in **Network Identification**. Computers often enter networks with IP addresses that are similar to the trusted network. In such cases, ESET Endpoint Security may consider an unknown network to be trusted (Home/office). We recommend that you use **Network authentication** to avoid this type of situation.

When a network adapter is connected to a network or its network settings are reconfigured, ESET Endpoint Security will search the known network list for a record that matches the new network. If **Network identification** and **Network authentication** (optional) match, the network will be marked connected in this interface. When no known network is found, network identification configuration will create a new network connection to identify the network the next time that you connect to it. By default, the new network connection uses the **Public network** protection type. The **New Network Connection Detected** dialog window will prompt you to choose between the **Public network**, **Home or office network** or **Use Windows setting** protection type. If a network adapter is connected to a known network and that network is marked as **Home or office network**, local subnets of the adapter will be added to the Trusted zone.

Protection type of new networks – Select which of the following options: **Use Windows setting**, **Ask user** or **Mark as public** is used by default for new networks.

> **Note**
> When you select **Use Windows setting a** dialog will not appear and the network you are connected to will automatically be marked according to your Windows settings. This will cause certain features (for example file sharing and remote desktop) to become accessible from new networks.

Known networks can be configured manually in the Known networks editor window.

Known networks editor

Known networks can be configured manually in **Advanced setup** > **Network protection** > **Firewall** > **Known Networks** by clicking **Edit** next to **Known networks**.

Columns

Name – Name of known network.

Protection type – Shows if the network is set to **Home or office network**, **Public** or **Use Windows setting**.

Firewall profile – Select a profile from the **Display rules used in the profile** drop-down menu to display the profiles rules filter.

Update profile – Allows you to apply created update profile when connected to this network.

Control elements

Add – Creates a new known network.

Edit – Click to edit an existing known network.

Delete – Select a network and click **Delete** to remove it from the list of known networks.

Top/Up/Down/Bottom – Allows you to adjust the priority level of known networks (networks are evaluated from top to bottom).

Network configuration settings are arranged in the following tabs:

Network

Here you can define the **Network name** and select the **Protection type** (Public network, Home or office network or Use Windows setting) for the network. Use the **Firewall profile** drop-down menu to select the profile for this network. If the network uses the **Home or office network** protection type, all directly connected network subnets are 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 255.255.255.0, the subnet 192.168.1.0/24 is added to that adapter's trusted zone. If the adapter has more addresses/subnets, all of them will be trusted, regardless of the **Network Identification** configuration of the known network.

Additionally, addresses added under **Additional trusted addresses** are always added to the trusted zone of adapters connected to this network (regardless of the network's protection type)**.**

Warn about weak WiFi encryption – ESET Endpoint Security will inform you when you connect to an unprotected wireless network or network with weak protection.

Firewall profile – Select firewall profile that will be used when connected to this network.

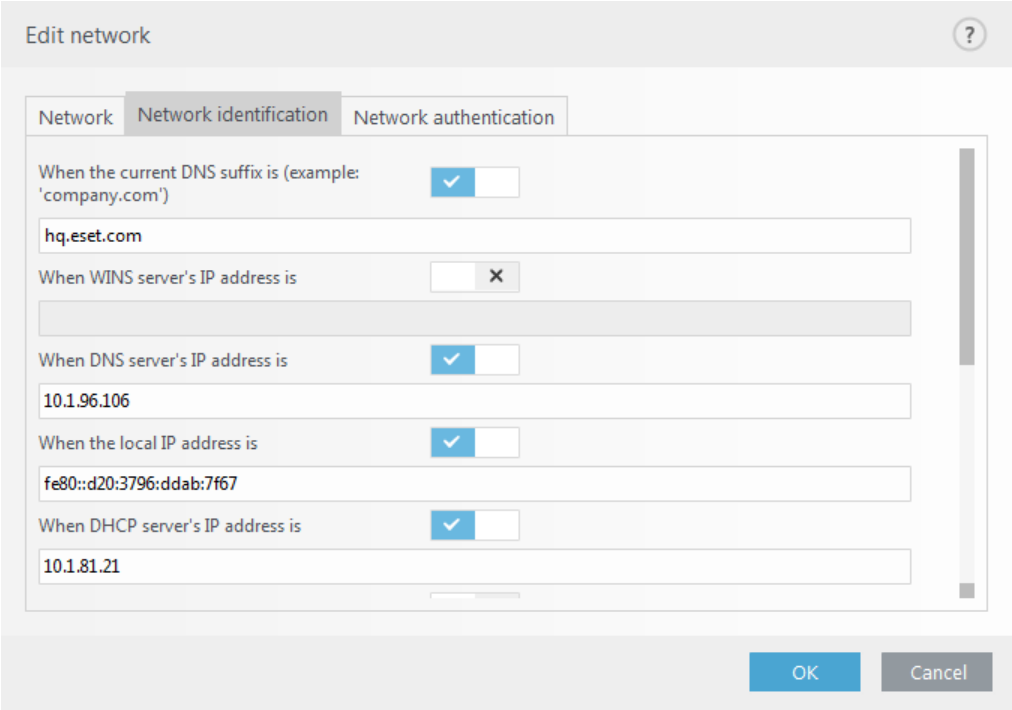
Update profile – Select update profile that will be used when connected to this network.

The following conditions must be met for a network to be marked as connected in the list of connected networks:

- Network identification – All filled in parameters must match active connection parameters.
- Network authentication – if authentication server is selected, successful authentication with the ESET Authentication Server must take place.

Network identification

Network identification is performed based on the local network adapter's parameters. All selected parameters are compared against the actual parameters of active network connections. IPv4 and IPv6 addresses are allowed.



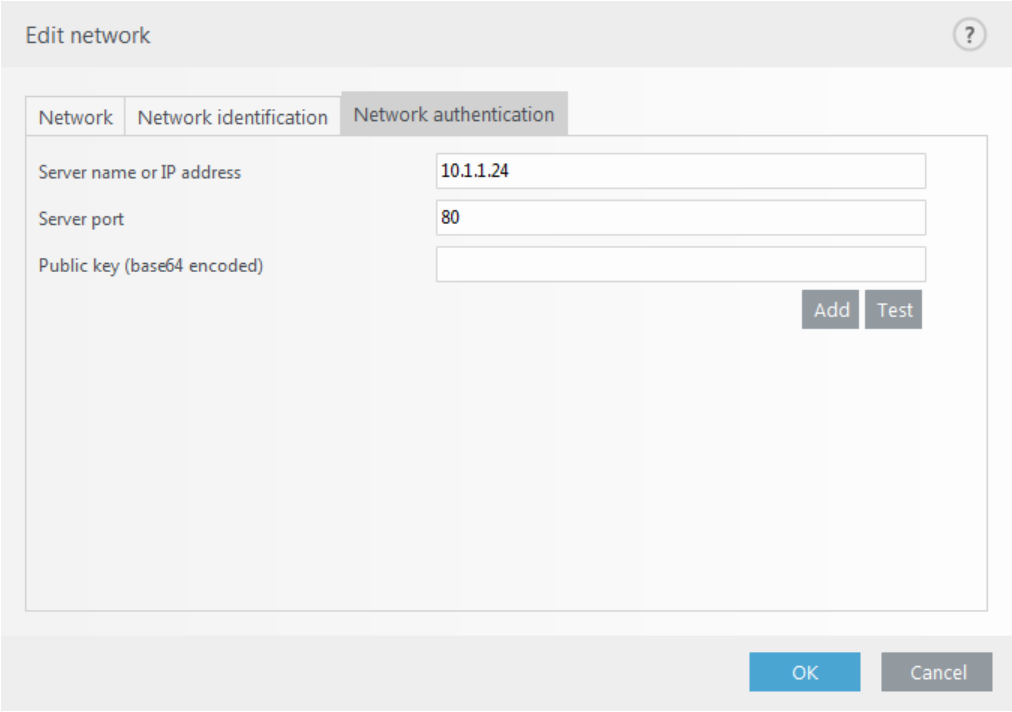
Network authentication

Network authentication searches for a specific server in the network and uses asymmetric encryption (RSA) to authenticate that server. The name of the network being authenticated must match the zone name set in authentication server settings. The name is case sensitive. Specify a server name, server listening port and a public key that corresponds to the private server key (see Network authentication – Server configuration). The server name can be entered in the form of an IP address, DNS or NetBios name and can be followed by a path specifying the location of the key on the server (for example, server_name_/directory1/directory2/authentication). You can specify alternate servers to use by appending them to the path, separated by semicolons.

Download the ESET Authentication Server.

The public key can be imported using any of the following file types:

- PEM encrypted public key (.pem), this key can be generated using the ESET Authentication Server (see Network authentication – Server configuration).
- Encrypted public key
- Public key certificate (.crt)



Click **Test** to test your settings. If authentication is successful, Server authentication was successful will be displayed. If authentication is not configured properly, one of the following error messages will be displayed:

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 zone 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.

Network authentication - Server configuration

The authentication process can be executed by any computer/server connected to the network that is to be authenticated. The ESET Authentication Server application needs to be installed on a computer/server that is always accessible for authentication whenever a client attempts to connect to the network. The installation file for the ESET Authentication Server application is available for download on ESET's website.

After you install the ESET Authentication Server application, a dialog window will appear (you can access the application by clicking **Start** > **Programs** > **ESET** > **ESET Authentication Server**).

To configure the authentication server, enter the authentication network name, the server listening port (default is 80) as well as the location to store the public and private key pair. Next, generate the public and private key that will be used in the authentication process. The private key will remain on the server while the public key needs to be imported on the client side in the Network authentication section when setting up a network in the firewall setup.

Firewall profiles

Global default profile – If there is no profile from network nor from network adapter configuration, the global default profile is used.

List of profiles – Profiles can be used to control the behavior of the ESET Endpoint Security Firewall. When creating or editing a firewall rule, you can assign it to a specific profile, or have it apply to every profile. When a profile is active on a network interface, 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 adapters or assigned to networks to easily alter firewall behavior.

Profiles assigned to network adapters – A network adapter can be set up to use a profile configured for a specific network when it is connected to that network.

You can also assign a specific profile to use when on a given network in **Advanced setup** (F5) > **Firewall** > **Known networks**. Select a network from the list of **Known networks** and click **Edit to** assign a firewall profile to the specific network from the **Firewall profile** drop-down menu. If that network has no assigned profile, then the adapter's default profile will be used. If the adapter is set up not to use the network's profile, its default profile will be used regardless of which network it is connected to. If there is no profile for a network or for adapter configuration, the global default profile is used. To assign a profile to a network adapter, select the network adapter, click **Edit** next to **Profiles assigned to network adapters**, select the profile from **Default firewall profile** drop-down menu and then click **OK**.

When the firewall switches to another profile, a notification will appear in the lower right corner by the system clock.

Profiles assigned to network adapters

By switching profiles you can quickly make multiple changes to firewall behavior. Custom rules can be set and applied for particular profiles. Network adapter entries for all adapters present on the machine are added to the list of **Network adapters** automatically.

Columns

Name – Name of the network adapter.

Default firewall profile – The default profile is used when the network you are connected to has no configured profile, or your network adapter is set not to use a network profile.

Prefer network's profile – Network adapter can use firewall profile configured for the connected known network. If that network has no configured profile, or network adapter is set up not to use the network's profile, then adapter's default profile is used.

Control elements

Add – Adds a new network adapter.

Edit – Allows you to edit an existing network adapter.

Delete – Select a network adapter and click **Delete** if you want to remove a network adapter from the list.

OK/Cancel – Click **OK** if you want to save changes or click **Cancel** to leave without any changes.

Application modification detection

The application modification detection feature displays notifications if modified applications, for which a firewall rule exists, attempt to establish connections. This is useful to avoid abusing rules configured for some application by another application by temporarily or permanently replacing the original application's executable file with the other applications executable file, or by maliciously modifying the original application's executable file.

Please be aware that 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.

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 – Don't notify if the application has the same valid digital signature before and after the modification.

List of applications excluded from checking – You can add or remove individual applications for which modifications are allowed without notification.

Applications excluded from modification 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.

Edit – Opens a window where you can change the location of an application that is on the list of applications excluded from modification detection.

Delete – Removes entries from the list of applications excluded from modification detection.

Configuring and using rules

Rules represent a set of conditions used to test all network connections and all actions assigned to these conditions. Using a firewall rules, you can define the action that is taken when different types of network connections are established. To access rule filtering setup, navigate to **Advanced setup** (F5) > **Network protection** > **Firewall** > **Advanced**. Some of predefined rules are bound to the check boxes from **allowed services** (Allowed services and advanced options) and they can not be turned off directly, instead you can use those related check boxes to do it.

Unlike the previous version of ESET Endpoint Security, rules are evaluated from top to bottom. The action of the first matching rule is used for each network connection being evaluated. This is an important behavioral change

from the previous version, in which the priority of rules was automatic and more specific rules had higher priority then more general ones.

Connections can be divided into incoming and outgoing connections. Incoming connections are initiated by a remote computer attempting to establish a connection with the local system. Outgoing connections work the opposite way – the local system contacts a remote computer.

If a new unknown communication is detected, consider carefully 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 particular attention to the remote computer 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 allows you to detect and terminate such connections.

Firewall rules list

The Firewal rules list can be found in **Advanced setup** (F5) > **Network protection** > **Firewall** > **Basic** by clicking **Edit** next to **Rules**.

Columns

Name – Name of rule.

Enabled – Shows if rule is enabled or disabled; the corresponding check box must be selected to activate a rule.

Protocol – The Internet protocol this rule is valid for.

Profile – Shows the firewall profile this rule is valid for.

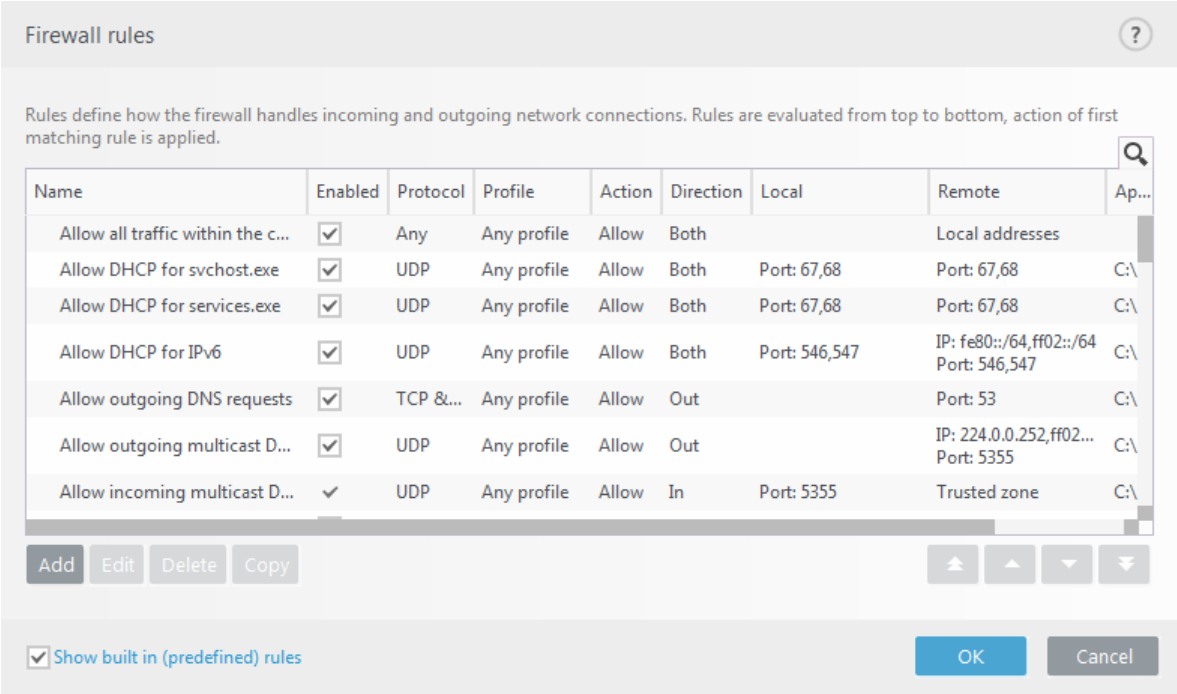
Action – Shows the status of communication (block/allow/ask).

Direction – Direction of communication (incoming/outgoing/both).

Local – Remote IPv4 or IPv6 address / range / subnet and port of local computer.

Remote – Remote IPv4 or IPv6 address / range / subnet and port of remote computer.

Applications – The application to which the rule applies.



Control elements

Add – Creates a new rule.

Edit – Edit an existing rule.

Delete – Remove an existing rule.

Copy – Create a copy of a selected rule.

Show built in (predefined) rules – Rules predefined by ESET Endpoint Security which allow or deny specific communications. You can disable these rules, but you cannot delete a predefined rule.

Top/Up/Down/Bottom – Allows you to adjust the priority level of rules (rules are executed from top to bottom).

> **Note**
> Click the search icon at the top right to search for rule(s) by name, protocol or port.

Adding or editing Firewall rules

Modification is required each time that monitored parameters are changed. If changes are made such that a rule cannot fulfill the conditions and the specified action cannot be applied, the given connection may be refused. This can lead to problems with the operation of the application affected by a rule. An example is a change of network address or port number for the remote side.

> **Illustrated instructions**
> 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 Security Management Center

The upper part of the window contains three tabs:

- **General** – Specify a rule name, the direction of the connection, the action (**Allow**, **Deny**, **Ask**), the protocol and the profile to which the rule will apply.

- **Local** – Displays information about the local side of the connection, including the number of the local port or port range and the name of the communicating application. Also allows you to add a predefined or created zone with a range of IP addresses here by clicking **Add**.

- **Remote** – This tab contains information about the remote port (port range). It allows you to define a list of remote IP addresses or zones for a given rule. You can also add a predefined or created zone with range of IP addresses here by clicking **Add**.

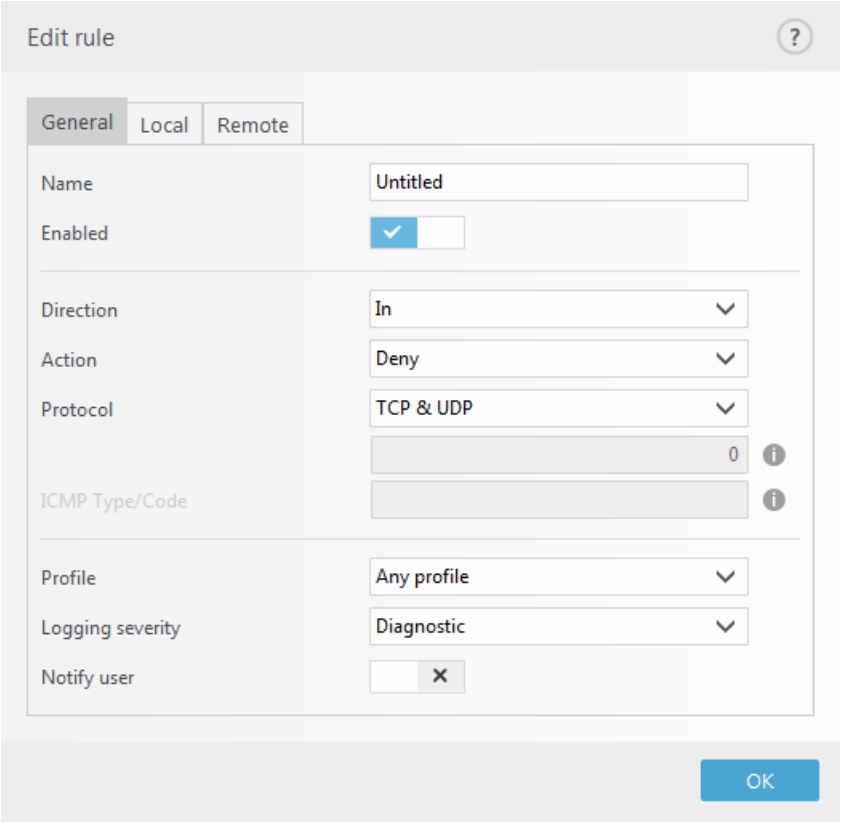
When creating a new rule, you must enter a name for the rule in the **Name** field. Select the direction to which the rule applies from the **Direction** drop-down menu and the action to be executed when a communication meets the rule from the **Action** drop-down menu.

Protocol represents the transfer protocol used for the rule. Select which protocol to use for a given rule from the drop-down menu.

ICMP Type/Code represents an ICMP message identified by a number (for example; 0 represents "Echo Reply").

All rules are enabled for **Any profile** by default. Alternatively, select a custom firewall profile using the **Profiles** drop-down menu.

If you enable **Logging severity**, the activity connected with the rule will be recorded in a log. **Notify user** displays a notification when the rule is applied.



Note
Firewall logs with **Warning** status can be collected by ESET Security Management Center.

Example
We create a new rule to allow the Firefox web browser application to access the Internet / local network websites. In this example, the following must be configured:
1.In the **General** tab, enable outgoing communication via the TCP and UDP protocol.
2.Click the **Local** tab.
3.Select the file path of the web browser you use by clicking **...** (for example *C:\Program Files\Firefox\Firefox.exe*). Do NOT enter the name of the application.
4.In the **Remote** tab, enable port numbers 80 and 443 if you want to allow standard Internet browsing.

Note
Please be aware that predefined rules can be modified in a limited way.

Firewall rule - Local

Specify the name of the local application and the local port/ports that a rule applies to.

Port – Remote port number(s). If there are no numbers supplied, the rule will apply for all ports. Add a single communication port or a range of communication ports.

IP – Allows you to add a remote address/addresses, address range, or subnet on which the rule is applied. If there is no value supplied, the rule will apply for all communication.

Zones – List of added zones.

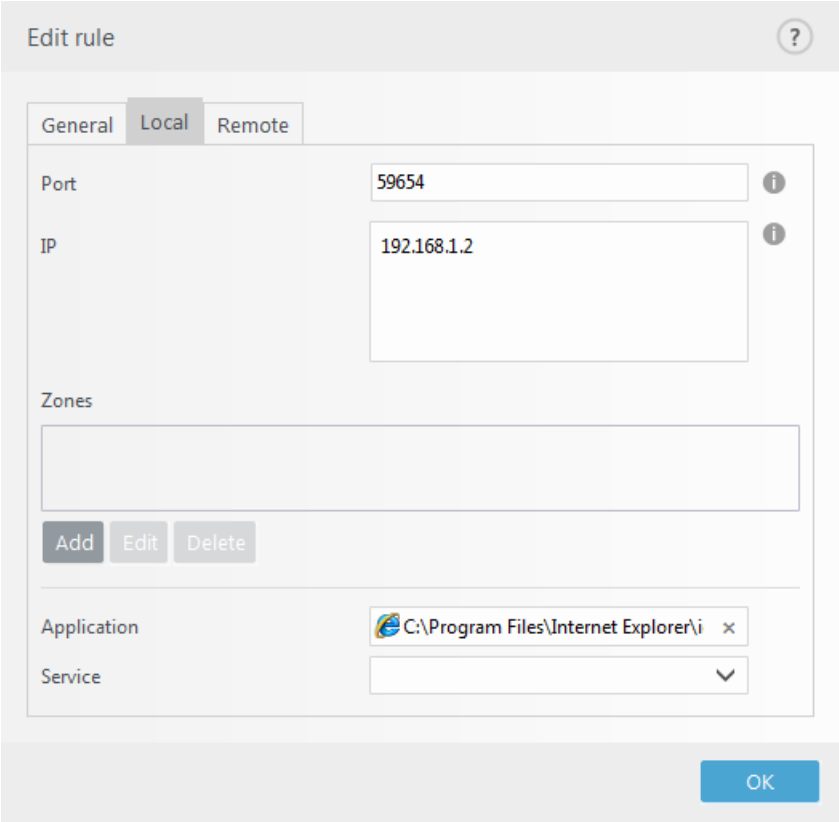
Add – Add a created zone from the drop-down menu. To create a zone, use the Zone setup tab.

Delete – Removes zones from the list.

Application – The name of the application to which the rule applies. Add the location of the application for which the rule will apply.

Service – The drop-down menu shows system services.

Example
You might want to create a rule for your Mirror which provides updates via port 2221 using the EHttpSrv *service* for communication in the drop-down menu.



Firewall rule - Remote

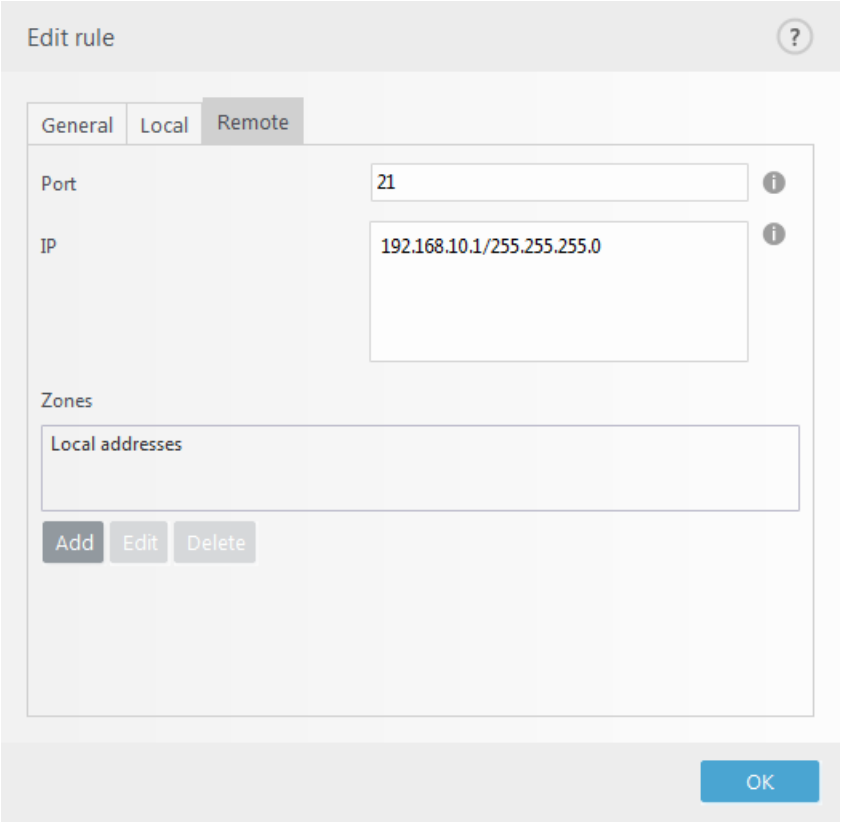
Port – Remote port number(s). If there are no numbers supplied, the rule will apply for all ports. Add a single communication port or a range of communication ports.

IP – Allows you to add a remote address, address range, or subnet. The address, range/subnet or remote zone for which the rule is applied. If there is no value supplied, the rule will apply for the whole communication.

Zones – List of added zones.

Add – Add a zone by selecting it from drop-down menu. To create a zone, use the Zone setup tab.

Delete – Removes zones from the list.



Temporary IP address blacklist

To view IP addresses that have been detected as sources of attacks are added to the blacklist to block connection for a certain period of time, from ESET Endpoint Security navigate to **Setup** > **Network protection** > **Temporary IP address blacklist**.

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.

Trusted zone

The trusted zone represents a group of network addresses from which the firewall allows some inbound traffic using default settings. Settings for features like file sharing and remote desktop inside of the trusted zone are determined in Allowed services and advanced options.

The actual trusted zone is computed dynamically and separately for each network adapter based on what network the computer is currently connected to. Addresses defined as inside of the trusted zone in the Zones editor are always trusted. If a network adapter is connected to a known network, then the **Additional trusted addresses** configured for that network are added to the adapter's trusted zone. If a network has the Home/office protection type, all directly connected subnets are included in the trusted zone. The actual trusted zone for each network adapter can be viewed from the **Setup** window under **Network** > **Network adapters**.

> **Note**
> Per-interface trusted zone is not supported on Windows XP operating systems. For these operating systems, all adapters have the same trusted zone, and this is also visible in the Network adapters page.

Configuring zones

A zone represents a collection of network addresses that create one logical group of IP addresses, useful when you need to reuse the same set of addresses in multiple rules. Each address in a given group is assigned similar rules defined centrally for the whole group. One example of such a group is a **Trusted zone**. A Trusted zone represents a group of network addresses that are not blocked by the Firewall in any way. These zones can be configured in **Advanced setup** > **Network protection**> **Firewall** > **Advanced**, by clicking **Edit** next to **Zones**. To add a new zone click **Add,** enter a **Name** for the zone, a **Description** and add a remote IP address into the **Remote computer address (IPv4/IPv6, range, mask)** field. See also Firewall zones.

Firewall zones

For more information about zones, see the section Configuring zones.

Columns

Name – Name of a group of remote computers.

IP addresses – Remote IP addresses that belong to a zone.

Control elements

When you **add** or **edit** a zone, 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) – Allows you to add a remote address, address range or subnet.

Delete – Removes a zone from the list.

> **Note**
> Please be aware that predefined zones cannot be removed.

Firewall log

The ESET Endpoint Security Firewall saves all important events in a log file, which can be viewed directly from the main menu. Click **Tools** > **Log files**, and then select **Firewall** from the **Log** drop-down menu. To enable firewall logging, navigate to **Advanced setup** > **Tools** > **Log files and** set the minimum logging verbosity to **Diagnosic.** All denied connections will be recorded.

Log files can be used to detect errors and reveal intrusions on your system. The ESET Firewall logs contain the following data:

- **Time** – Date and time of event.
- **Event** – Name of event.
- **Source** – Source network address.
- **Target** – Target network address.
- **Protocol** – Network communication protocol.
- **Rule/worm name** – Rule applied, or name of worm, if identified.
- **Application** – Application involved.

- **User** – Name of the user logged in at the time the infiltration was detected.

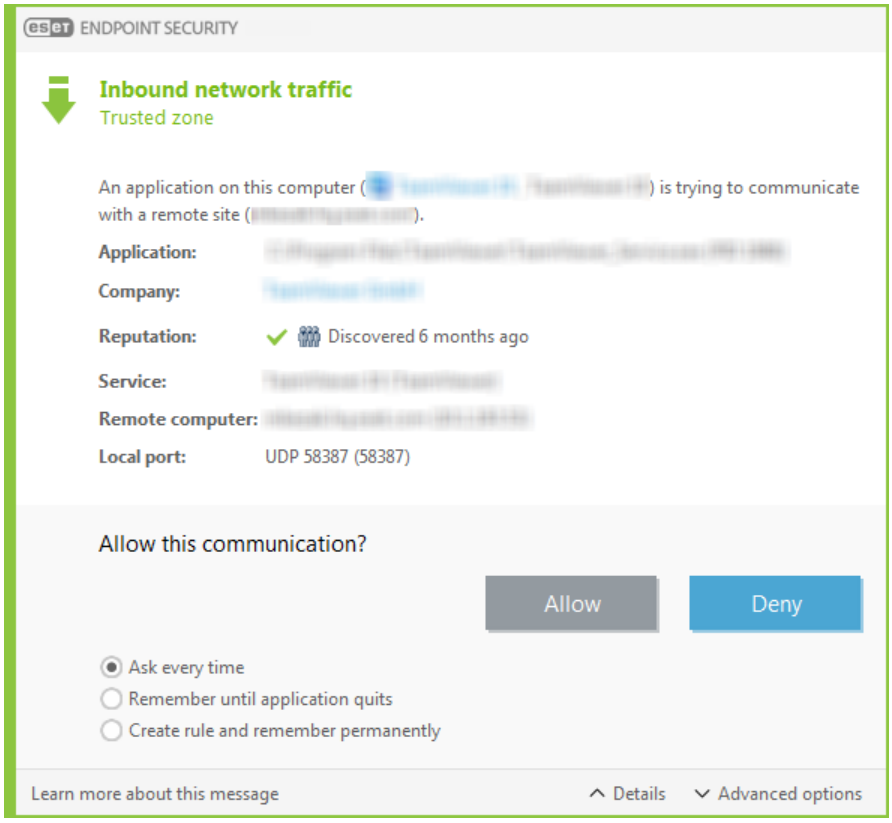
A thorough analysis of this data can help detect attempts to compromise system security. Many other factors indicate potential security risks and allow you to minimize their impact. Some examples of potential threat indicators include frequent connections from unknown locations, multiple attempts to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

Establishing connection – detection

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

Interactive mode displays an informational window that reports detection of a new network connection, supplemented with detailed information about the connection. You can opt to allow the connection or refuse (block) it. If you repeatedly allow the same connection in the dialog window, we recommend that you create a new rule for the connection. To do this, select **Remember action (create rule)** and 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.

Temporarily remember action for the process causes an action (**Allow**/**Deny**) to be used until application restart, a change of rules or filtering modes, a Firewall module update or a system restart. After any of these actions, temporary rules will be deleted.



Please be careful when creating new rules and only allow connections that you know are secure. If all connections are allowed, then the firewall fails to accomplish its purpose. These are the important parameters for connections:

- **Remote side** – Only allow connections to trusted and known addresses.
- **Local application** – It is not advisable to allow connections for unknown applications and processes.
- **Port number** – Communication on common ports (for example, web traffic – port number 80) should be allowed under normal circumstances.

In order to proliferate, 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.

Solving problems with ESET Firewall

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

See the following topics for help resolving problems with the ESET Firewall:

- Troubleshooting wizard
- Logging and creating rules or exceptions from log
- Creating exceptions from firewall notifications

- Advanced PCAP logging
- Solving problems with protocol filtering

Troubleshooting wizard

The troubleshooting wizard silently monitors all blocked connections, and will guide you through the troubleshooting process to correct firewall issues with specific applications or devices. Next, the wizard will suggest a new set of rules to be applied if you approve them. **Troubleshooting wizard** can be found in the main menu under **Setup** > **Network**.

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 firewall, enable Network protection advanced logging in the **Diagnostics** section of **Advanced setup** under **Tools** > **Diagnostics**. If you see something in the log that you do not want the firewall to block, you can create a rule or an IDS exception 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.

> **Note**
> Use logging to see the order in which the firewall blocked specific connections. Moreover, creating rules from the log allows you to create rules that do exactly what you want.

Create rule from log

The new version of ESET Endpoint Security allows 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:

- set the minimum logging verbosity to **Diagnostic** in **Advanced setup** (F5) > **Tools** > **Log files**,
- enable **Display notifications also for incoming attacks against security holes** in **Advanced setup** (F5) > **Network 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 that will allow you to learn more about the event and set up an exception for this event if you want.

> **Note**
> 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.

Advanced PCAP logging

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

1. Navigate to **Advanced setup** > **Tools** > **Diagnostics** and enable **Enable Protocol filtering advanced logging**.
2. Attempt to reproduce the problem you are experiencing.
3. Disable advanced PCAP logging.
4. The PCAP log file can be found in the same directory where diagnostic memory dumps are generated:

- Microsoft Windows Vista or newer

C:\ProgramData\ESET\ESET Security\Diagnostics

- Microsoft Windows XP

C:\Documents and Settings\All Users\...

Solving problems with protocol filtering

If you experience problems with your browser or email client, the first step is to determine if protocol filtering is responsible. To do that, try temporarily disabling application protocol filtering in the advanced setup (remember to turn it back on after you're 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 protocol filtering enabled, try temporarily turning it off. If that helps, you can keep using SSL filtering and make the update work by excluding the problematic communication:
  Switch SSL protocol filtering mode to interactive. Rerun the update. There should be a dialog informing you about encrypted network traffic. Make sure the application matches the one you're troubleshooting and the certificate looks like coming from the server it is updating from. Then choose to remember action for this certificate and click ignore. If no more relevant dialogs are show, 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 protocol filtering (doing this for 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 exception, so manually adding one shouldn't be necessary.

Problem accessing a device on your network

If you are unable to use any functionality of a device on your network (this could mean opening a webpage 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 particular website

You can exclude specific websites from protocol filtering using URL address management. For example if you can't 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“

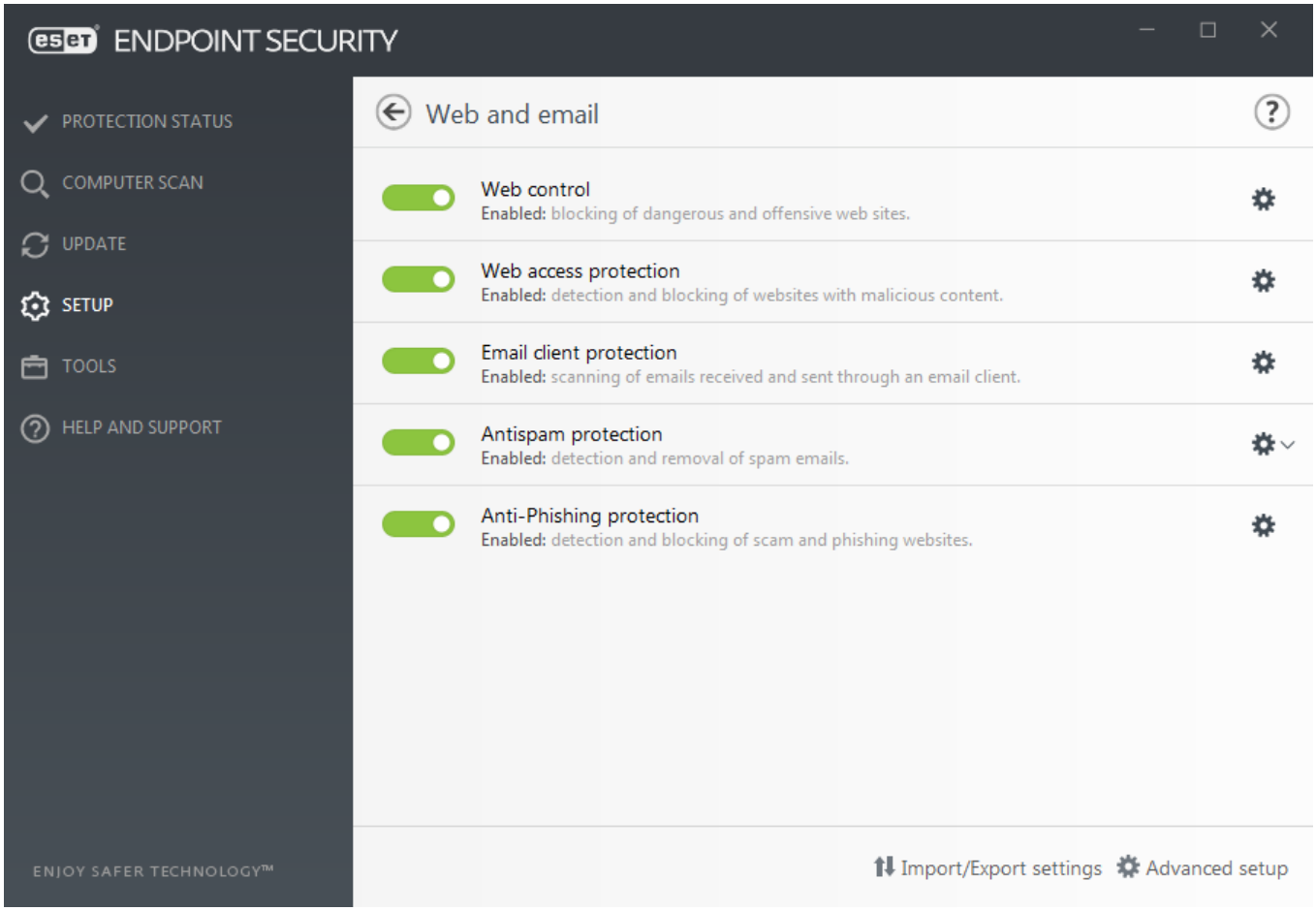
When you enable SSL protocol filtering, ESET Endpoint Security makes sure that installed applications trust the way it filters SSL protocol by importing a certificate to their certificate store. For some applications this is not possible while they are running. This includes Firefox and Opera. Make sure none of them are running (the best way to do this is to open Task Manager and make sure there is no firefox.exe or opera.exe under Processes tab), then hit retry.

Error about untrusted issuer or invalid signature

This most likely means that the import described above failed. First make sure that none of the mentioned applications are running. Then disable SSL protocol filtering and enable it back on. This reruns the import.

Web and email

Web and email configuration can be found under **Setup** > **Web and email**. From here you can access more detailed program settings.



Secure Browser.....

The Web control module allows you to configure settings that provide administrators with automated tools to help protect their workstations and set restrictions for internet browsing. The aim of the Web control functionality is to prevent access to pages with inappropriate or harmful content. See Web control for more information.

Internet connectivity is a standard feature for personal computers. Unfortunately, the Internet has become the primary medium for distributing malicious code. For this reason it is essential that you carefully consider your **Web access protection** settings.

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

Antispam protection filters unsolicited email messages.

When you click the gear wheel ⚙ next to **Antispam protection** the following options are available:

Configure... – Opens advanced settings for Email client antispam protection.

User's Whitelist/Blacklist/Exceptions list – Opens a dialog window where you can add, edit or delete email addresses that are considered safe or unsafe. According to rules defined here, email from these addresses will not be scanned or will be treated as spam. Click **User´s Exceptions list** to open a dialog where you can add, edit or delete email addresses that may be spoofed and used for sending spam. Email messages received from addresses listed in the Exception list will always be scanned for spam.

Anti-Phishing protection is another layer of protection that provides increased defense from illegitimate websites that attempt to acquire passwords and other sensitive information. Anti-Phishing protection can be found in the **Setup** pane **under Web and email**. See Anti-Phishing protection for more information.

You can disable the web/email/anti-phishing/antispam protection module temporarily by clicking .

Protocol filtering

Antivirus protection for application protocols is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. Protocol filtering works automatically, regardless of the Internet browser or email client used. To edit encrypted (SSL) settings, go to **Advanced Setup** (F5) > **Web and email** > **SSL/TLS**.

Enable application protocol content filtering – Can be used to disable protocol filtering. Note that many ESET Endpoint Security components (Web access protection, Email protocols protection, Anti-Phishing, Web control) depend on this and will be non-functional without it.

Excluded applications – Allows you to exclude specific applications from protocol filtering. Useful when protocol filtering causes compatibility issues.

Excluded IP addresses – Allows you to exclude specific remote addresses from protocol filtering. Useful when protocol filtering causes compatibility issues.

Example of excluded IP addresses

IPv4 addresses and mask:

- *192.168.0.10* – IP address of an individual computer for which the rule is to be applied.
- *192.168.0.1* to *192.168.0.99* – the starting and ending address IP address to specify the IP range (of several computers) for which the rule is to be applied.
- Subnet (a group of computers) defined by an IP address and mask. For example, *255.255.255.0* is the network mask for the *192.168.1.0/24* prefix, that means *192.168.1.1* to 192.168.1.254 address range.

IPv6 address and mask:

- *2001:718:1c01:16:214:22ff:fec9:ca5* – the IPv6 address of an individual computer for which the rule is to be applied
- *2002:c0a8:6301:1::1/64* – IPv6 address with the prefix length of 64 bits, that means *2002:c0a8:6301:0001:0000:0000:0000:0000 to 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

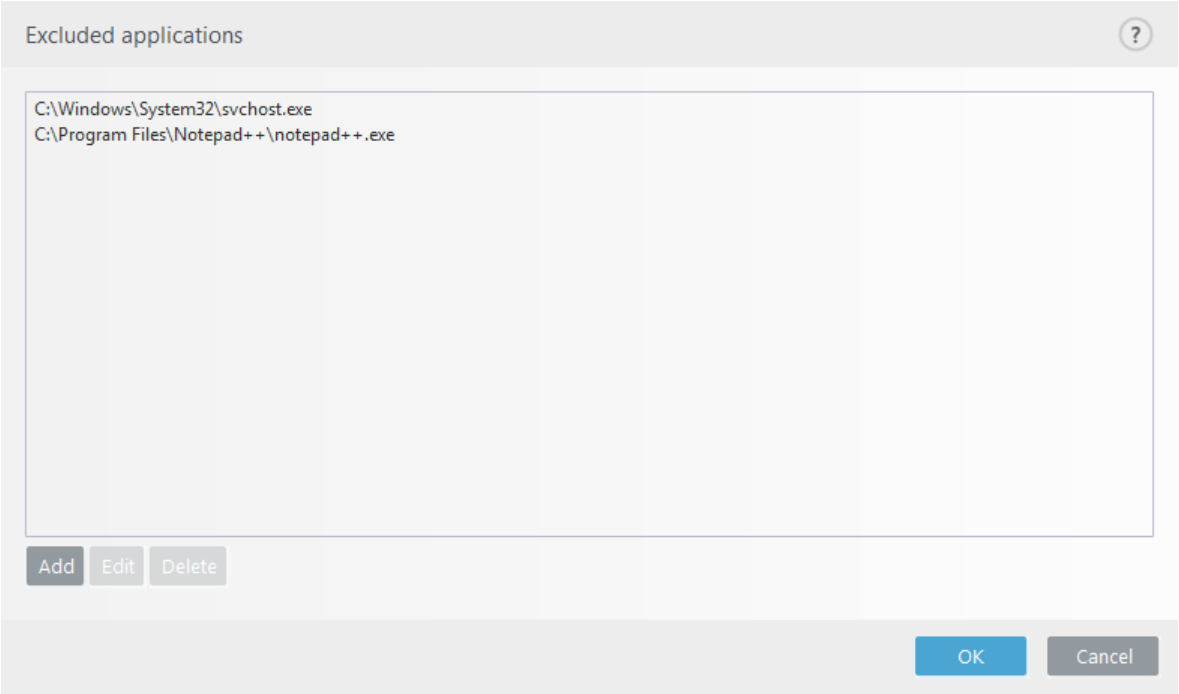
Excluded applications

To exclude communications for specific network-aware applications from protocol filtering, add them to this list. HTTP/POP3/IMAP communication for the selected applications will not be checked for threats. We recommend that you only use this technique in cases where applications do not function properly with protocol filtering enabled.

Applications and services that were already affected by protocol filtering will be automatically displayed after clicking **Add**.

Edit – Edit selected entries from the list.

Delete – Remove selected entries from the list.



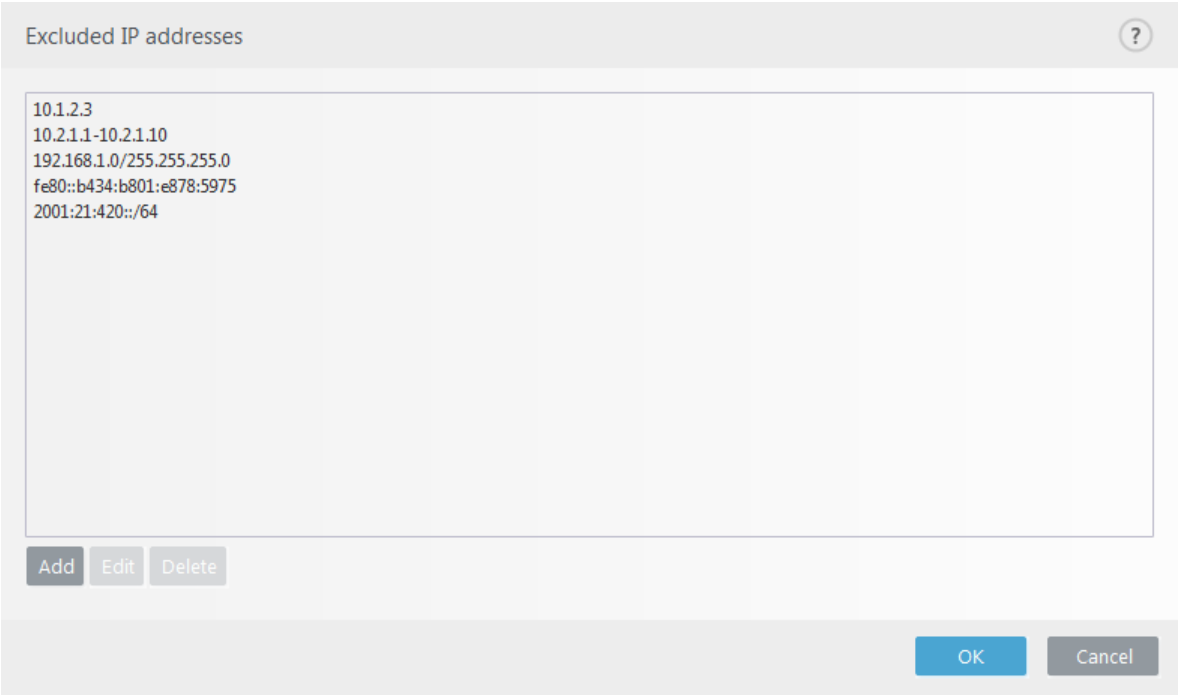
Excluded IP addresses

IP addresses in this list will be excluded from protocol content filtering. HTTP/POP3/IMAP 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.



SSL/TLS

ESET Endpoint Security is capable of checking for threats in communication that use the SSL protocol. You can use various scanning modes to examine SSL-protected communication with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Enable SSL/TLS protocol filtering – Protocol filtering is enabled by default. You can disable SSL/TLS protocol filtering in **Advanced setup** > **Web and email** > **SSL/TLS** or via policy. If protocol filtering is disabled, the program will not scan communication over SSL.

SSL/TLS protocol filtering mode is available in the following options:

Filtering mode	Description
Automatic mode	Default mode will only scan appropriate applications such as web browsers and email clients. You can override it by selecting applications for which their communication will be scanned.
Interactive mode	If you enter 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 mode	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 that is marked as trusted (it is on the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.

The **List of SSL/TLS filtered applications** can be used to customize ESET Endpoint Security behavior for specific applications.

List of known certificates allows you to customize ESET Endpoint Security behavior for specific SSL certificates.

Exclude communication with trusted domains – When enabled, communication with trusted domains will be excluded from checking. The trustworthiness of a domain is determined by a built-in whitelist.

Block encrypted communication utilizing the obsolete protocol SSL v2 – Communication using the earlier version of the SSL protocol will automatically be blocked.

> **Note**
> Addresses will not be filtered if the setting **Exclude communication with trusted domains** is enabled and the domain is considered trusted.

Root certificate

Root certificate – 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). **Add the root certificate to known browsers** should be enabled. Select this option to automatically add the ESET root certificate to known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (for example, in Internet Explorer).

To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File...** and

manually import it into the browser.

Certificate validity

If the certificate trust cannot be established – In some cases, a website certificate cannot be verified using the Trusted Root Certification Authorities (TRCA) store. This means that the certificate is signed by someone (for example, the administrator of a web server or a small business) and considering this certificate as trusted is not always a risk. Most large businesses (for example banks) use a certificate signed by the TRCA. If **Ask about certificate validity** is selected (selected by default), the user will be prompted to select an action to take when encrypted communication is established. You can select **Block communication that uses the certificate** to always terminate encrypted connections to sites with unverified certificates.

If the certificate is corrupt – This means that the certificate was incorrectly signed or is damaged. In this case, we recommend that you leave **Block communication that uses the certificate** selected. If **Ask about certificate validity** is selected, the user will be prompted to select an action to take when the encrypted communication is established.

> **Illustrated examples**
> 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

Certificates

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). **Add the root certificate to known browsers** should be enabled. Select this option to automatically add the ESET root certificate to the known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (e.g. Internet Explorer). To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File...** and then manually import it into the browser.

In some cases, the certificate cannot be verified using the Trusted Root Certification Authorities store (e.g. VeriSign). This means that the certificate is self-signed by someone (e.g. administrator of a web server or a small business company) and considering this certificate as trusted is not always a risk. Most large businesses (for example banks) use a certificate signed by TRCA. If **Ask about certificate validity** is selected (selected by default), the user will be prompted to select an action to take when encrypted communication is established. An action selection dialog will be displayed where you can decide to 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 the site that uses the unverified certificate.

If the certificate is invalid or corrupt, it means that the certificate expired or was incorrectly self-signed. In this case, we recommend that you block the communication that uses the certificate.

Encrypted network traffic

If your system is configured to use SSL protocol 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 protocol filtering 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 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 List of known certificates.

List of known certificates

The **List of known certificates** can be used to customize ESET Endpoint Security behavior for specific SSL certificates, and to remember actions chosen if **Interactive mode** is selected in **SSL/TLS protocol filtering mode**. The list can be viewed and edited in **Advanced setup** (F5) > **Web and email** > **SSL/TLS** > **List of known certificates**.

The **List of known certificates** 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 – A certificate can be loaded manually as a file with the extension *.cer*, *.crt* or *.pem*. Click **File** to upload a local certificate or click **URL** to specify the location of a certificate online.

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** to exit without saving.

List of SSL/TLS filtered applications

The **List of SSL/TLS filtered applications** can be used to customize ESET Endpoint Security behavior for specific applications, and to remember actions chosen if **Interactive mode** is selected in **SSL/TLS protocol filtering mode**. The list can be viewed and edited in **Advanced setup** (F5) > **Web and email** > **SSL/TLS** > **List of SSL/TLS filtered applications**.

The **List of SSL/TLS filtered applications** window consists of:

Columns

Application – Name of the application.

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.

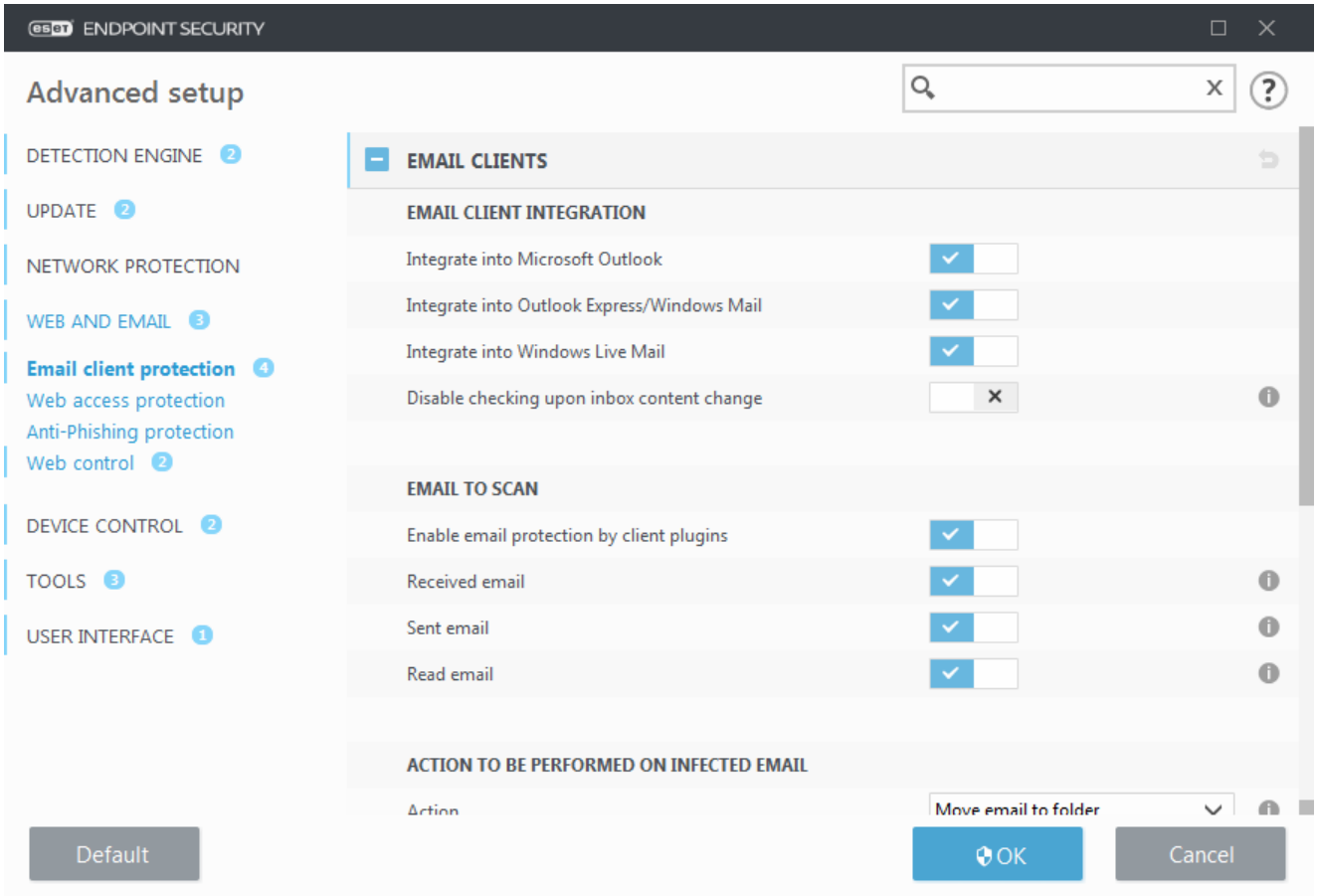
Edit – Select the certificate that you want to configure and click **Edit**.

Delete – Select the certificate that you want to delete and click **Delete**.

OK/Cancel – Click **OK** if you want to save changes or click **Cancel** if you want to exit without saving.

Email client protection

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, integration can be enabled 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. Integration settings are located under **Advanced setup** (F5) > **Web and email** > **Email client protection** > **Email clients**.



Email client integration

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in 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. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.

Turn on **Disable checking upon inbox content change** if you experience a system slowdown when retrieving emails.

Email to scan

Enable email protection by client plugins – When disabled, protection by email client plugins is turned off.

Received email – Checks email messages that are received when enabled.

Sent email – Checks email messages that are sent when enabled.

Read email – Checks email messages that are read when enabled.

> **Note**
> 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 Protocol filtering (IMAP/IMAPS and POP3/POP3S).

Action to be performed on infected email

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.

Repeat scan after update – Rescans the infected emails after a detection engine update when enabled.

Accept scan results from other modules – Allows the email protection module to use the scan results received from the other protection modules instead of scanning again.

Email protocols

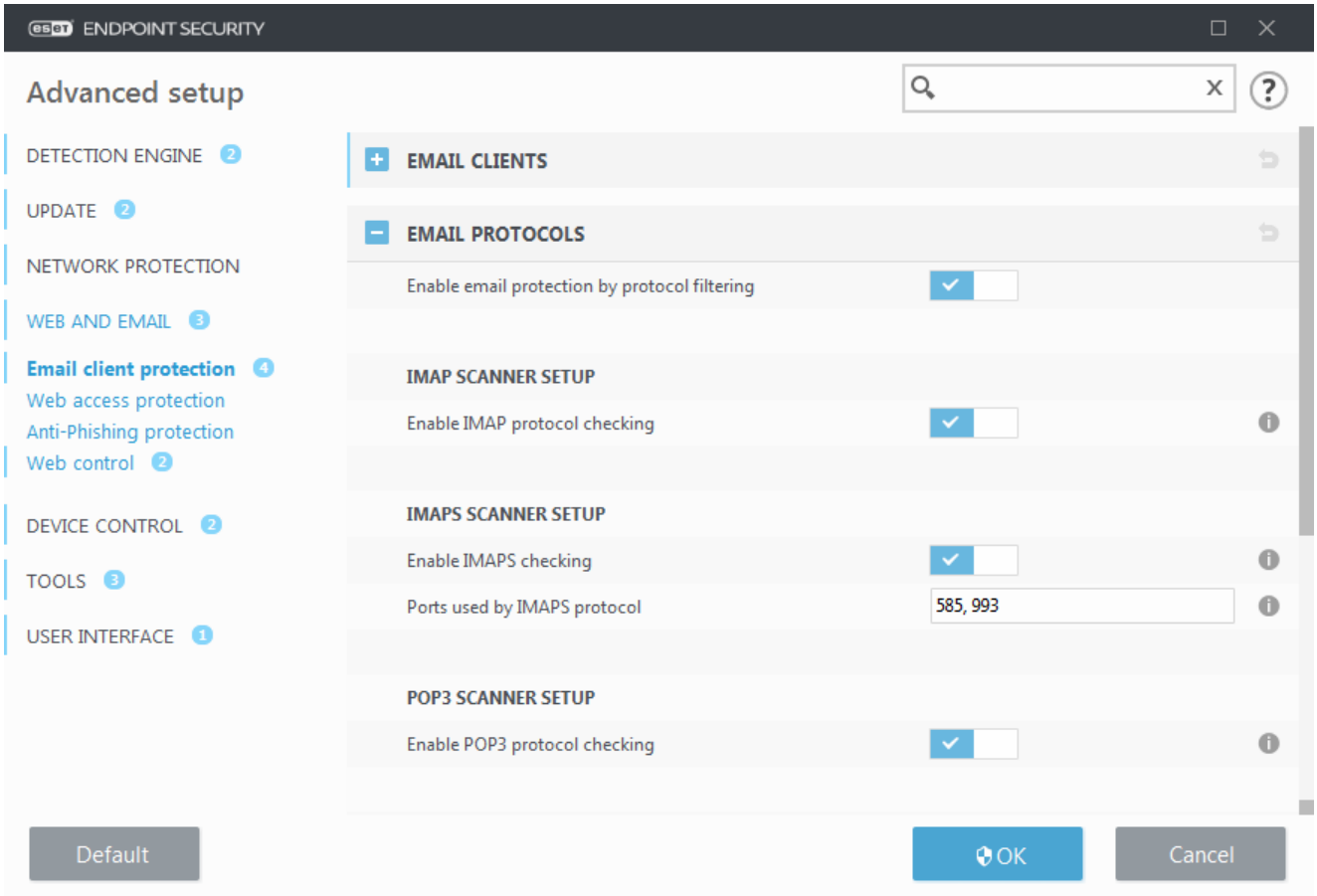
The IMAP and POP3 protocols are the most widespread protocols used to receive email communication in an email client application. The Internet Message Access Protocol (IMAP) is another Internet protocol for email retrieval. IMAP has some advantages over POP3, for example, multiple clients can simultaneously 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.

We recommend that you keep **Enable email protection by protocol filtering** enabled**.** To configure IMAP/IMAPS and POP3/POP3S protocol checking, navigate to Advanced setup > **Web and email** > **Email client protection** > **Email protocols**.

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. The program will only scan traffic on ports defined in **Ports used by IMAPS/POP3S protocol**, regardless of operating system version. Other communication ports can be added if necessary. Multiple port numbers must be delimited by a comma.

Encrypted communication will be scanned by default. To view the scanner setup, navigate to SSL/TLS in the Advanced setup section, click **Web and email** > **SSL/TLS**, and enable the **Enable SSL/TLS protocol filtering** option.



Email alerts and notifications

The options for this functionality are available in **Advanced setup under Web and email** > **Email client protection** > **Alerts and notifications**.

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 available options are:

- **Never** – No tag messages will be added at all.
- **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 sent email – Disable this if you do not want email protection to include a virus warning in the subject of an infected email. This feature allows for simple, subject-based filtering of infected emails (if supported by your email program). It also increases the level of credibility for the recipient and if an infiltration is detected, provides valuable information about the threat level of a given email or sender.

Text to add to subject of detected email – Edit this template if you wish 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.

Integration with email clients

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in 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. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.

Microsoft Outlook toolbar

Microsoft Outlook protection works as a plug-in module. After ESET Endpoint Security is installed, this toolbar containing the antivirus/antispam protection 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 (blacklist, a list of spam addresses) – Adds a new sender address to the Blacklist. All messages received from the list will be automatically classified as spam.

> **Warning**
> Beware of spoofing – forging a sender's address on email messages to mislead email recipients into reading and responding.

Trusted address (whitelist, a list of trusted addresses) – Adds a new sender address to the Whitelist. All messages received from addresses in the Whitelist will never be automatically classified as spam.

ESET Endpoint Security – Click on icon opens the main program 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 received email. For more information see Email client protection.

Scanner setup – Displays the Email client protection setup options.

Antispam setup – Displays the Antispam protection setup options.

Address books – Opens the antispam protection window, where you can access lists of excluded, trusted and spam addresses.

Outlook Express and Windows Mail toolbar

Outlook Express and Windows Mail protection works as a plug-in module. After ESET Endpoint Security is installed, this toolbar containing the antivirus/antispam protection options is added to Outlook Express or Windows Mail:

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 – Adds a new sender address to the Blacklist. All messages received from the list will be automatically classified as spam.

> **Warning**
> Beware of spoofing – forging a sender's address on email messages to mislead email recipients into reading and responding.

Trusted address – Adds a new sender address to the Whitelist. All messages received from addresses in the Whitelist will never be automatically classified as spam.

ESET Endpoint Security – Click on icon opens the main program 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 received email. For more information see Email client protection.

Scanner setup – Displays the Email client protection setup options.

Antispam setup – Displays the Antispam protection setup options.

User interface

Customize appearance – The appearance of the toolbar can be modified for your email client. Deselect the option to customize appearance independent of email program parameters.

Show text – Displays descriptions for icons.

Text to the right – Option descriptions are moved from the bottom to the right side of icons.

Large icons – Displays large icons for menu options.

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:

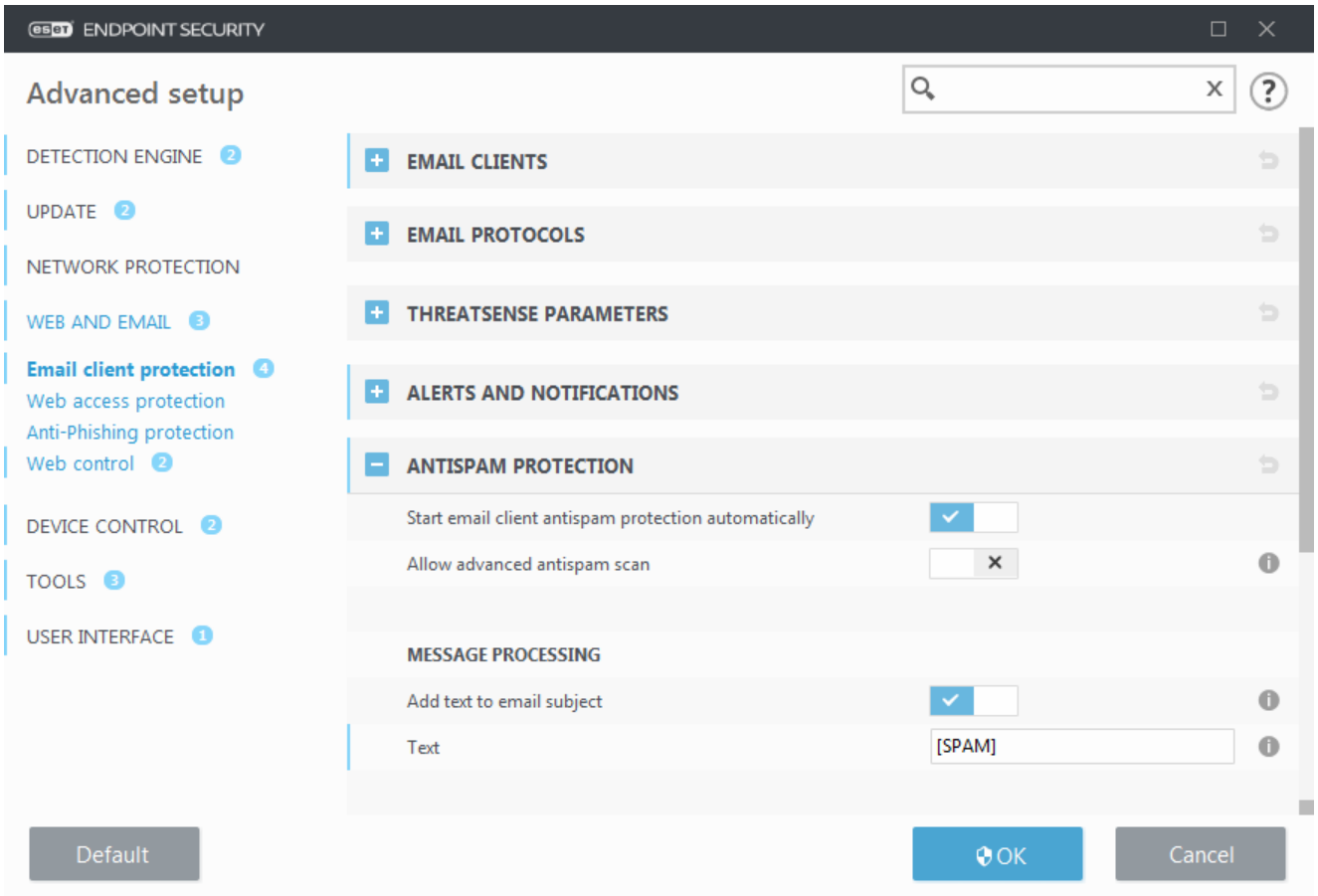
All messages in the current folder – Scans messages in the currently displayed folder.

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.

Antispam protection

Unsolicited email, called spam, ranks among the greatest problems of electronic communication. Spam represents up to 50 percent of all email communication. Antispam protection serves to protect against this problem. Combining several email security principles, the Antispam module provides superior filtering to keep your inbox clean.



One important principle for spam detection is the ability to recognize unsolicited email based on predefined trusted addresses (whitelist) and spam addresses (blacklist). All addresses from your contact list are automatically added to the whitelist, as well as all other addresses you mark as safe.

The primary method used to detect spam is the scanning of 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 spam or not.

Start email client antispam protection automatically – When enabled, antispam protection will be activated automatically on system startup.

Allow advanced antispam scan – Additional antispam data will be downloaded periodically, increasing antispam capabilities and producing better results.

Antispam protection in ESET Endpoint Security allows you to set different parameters to work with mailing lists. Options are as follows:

Message processing

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 is "[SPAM]".

Move messages to spam folder – When enabled, spam messages will be moved to the default junk email folder and also messages reclassified as not spam will be moved to inbox. When you right-click an email message and select ESET Endpoint Security from the context menu, you can choose from applicable options.

Use the folder – Specify the custom folder where you want to move infected emails when detected.

Mark spam messages as read – Enable this to automatically mark spam as read. 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.

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 log (ESET Endpoint Security > Tools > Log files > Antispam protection).

- **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.

> **Note**
> When you click a message in junk email folder, you can choose **Reclassify selected messages as NOT spam** and the message will be moved to inbox. When you click a message you consider spam in inbox, select **Reclassify messages as spam** and the message will be moved to junk email folder. You can select multiple messages and perform the action on all of them at the same time.

> **Note**
> ESET Endpoint Security supports Antispam protection for Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail.

Antispam address books

The Antispam feature in ESET Endpoint Security allows you to configure various parameters for address lists.

Address books

Allow user address list – Enable this option to activate the address book created by a user within their own email client.

Allow global address lists – Enable this option to activate the global address book shared by all users on this workstation, the directory service within the email system. The GAL (Global Address List) contains information for all email users, distribution groups and resources.

User's Whitelist – List of contacts where you can add, edit or delete addresses that are considered safe and from whom the user wants to receive messages.

User's Blacklist – List of contacts where you can add, edit or delete addresses that are considered unsafe and from whom the user does not want to receive messages.

User's Exception list – This list of contacts contains email addresses that may be spoofed and used for sending spam. See also Exception list.

Global Whitelist/Blacklist/Exception list – These lists are used for applying antispam policies to all users who use ESET Endpoint Security on this workstation. When ESET Endpoint Security is remotely managed, the ESMC/ESET PROTECT Cloud policy will apply to all assigned workstations.

Add to user's Whitelist automatically

Add addresses from address book – Add addresses from your contact list to the Whitelist.

Add recipient addresses from outgoing messages – Add recipient addresses from sent messages to the Whitelist.

Add addresses from messages reclassified as NOT spam – Add sender addresses from messages reclassified as NOT spam to the Whitelist.

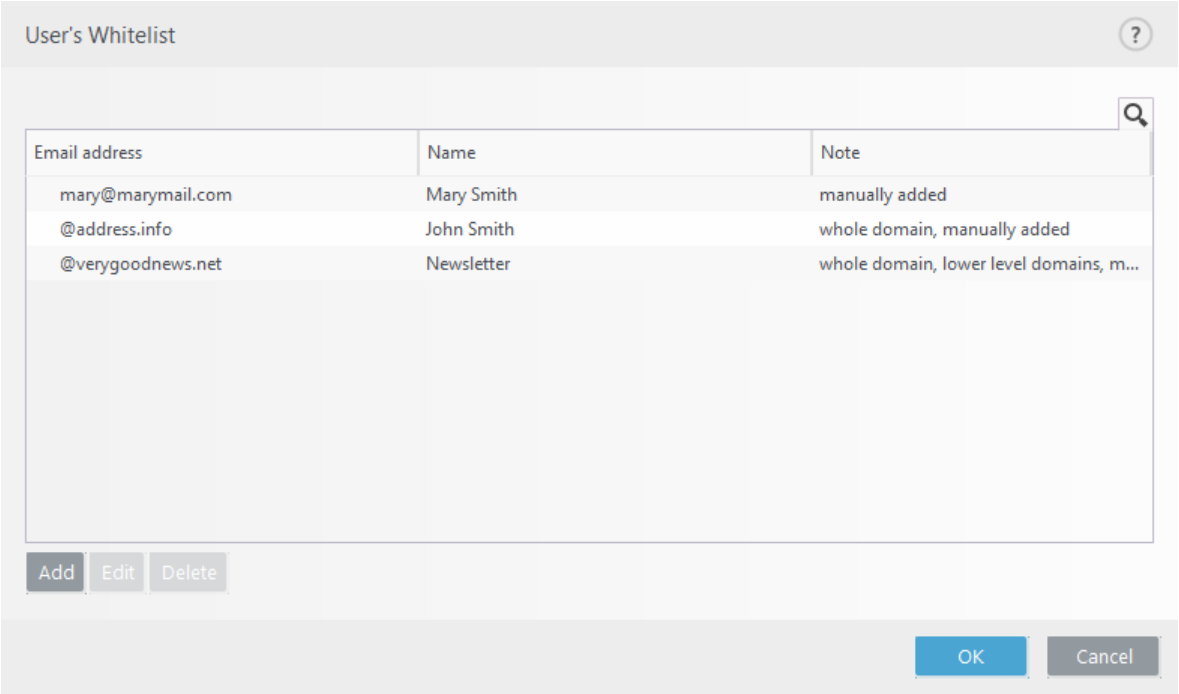
Add to user's Exception list automatically

Add addresses from own accounts – Add your addresses from existing email client accounts to the Exception list.

Blacklist/Whitelist/Exceptions list

To provide protection against unsolicited emails, ESET Endpoint Security allows you to classify email addresses using specialized lists. The Whitelist contains email addresses you consider to be safe. Messages from users on the Whitelist are always available in the incoming mail folder. The Blacklist contains email addresses classified as spam, and all messages from senders on the Blacklist are marked accordingly. The exception list contains email addresses that are always checked for spam but may also contain addresses from unsolicited email messages that might not be recognized as spam initially.

All lists can be edited from main program window of ESET Endpoint Security in **Advanced Setup** > **Web and email** > **Email client protection** > **Antispam address books** using the **Add**, **Edit** and **Delete** buttons in each list's dialog window, or from **Setup** > **Web and email** after you click the gear wheel ⚙ next to **Antispam protection**.



By default, ESET Endpoint Security adds all addresses from the address book of supported email clients to the Whitelist. The Blacklist is empty by default. The Exception list only contains user's own email addresses by default.

Add/Edit Blacklist/Whitelist/Exceptions address

This window allows you to add or edit entries in the Whitelist or Blacklist.

Email address – The email address to add/edit.

Name – The name of the entry.

Whole domain – Select this option for the entry 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).

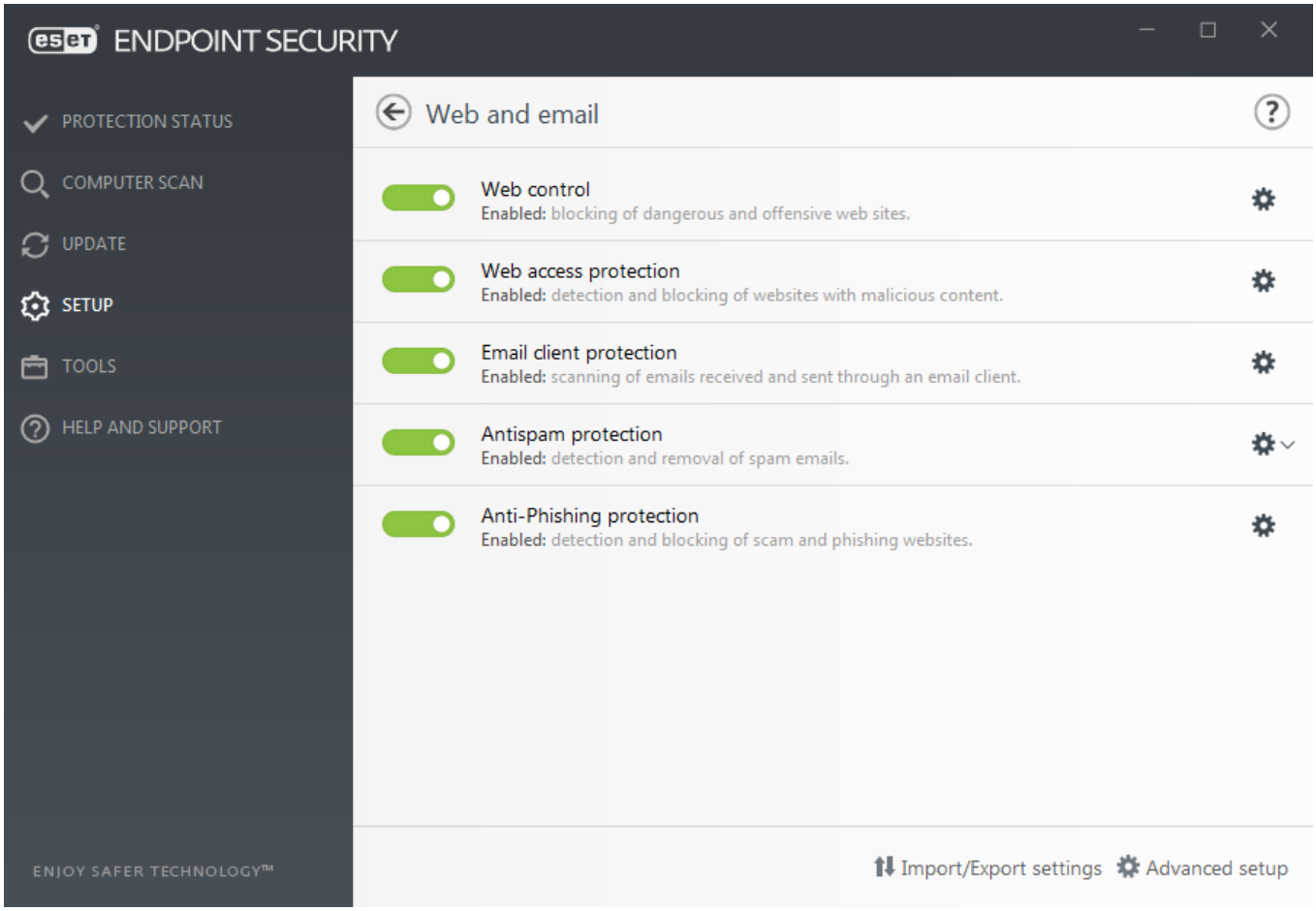
Lower level domains – Select this option for the entry to be applied to the lower level domains of the contact (The *address.info* represents domain, while *my.address.info* represents a subdomain).

Web access protection

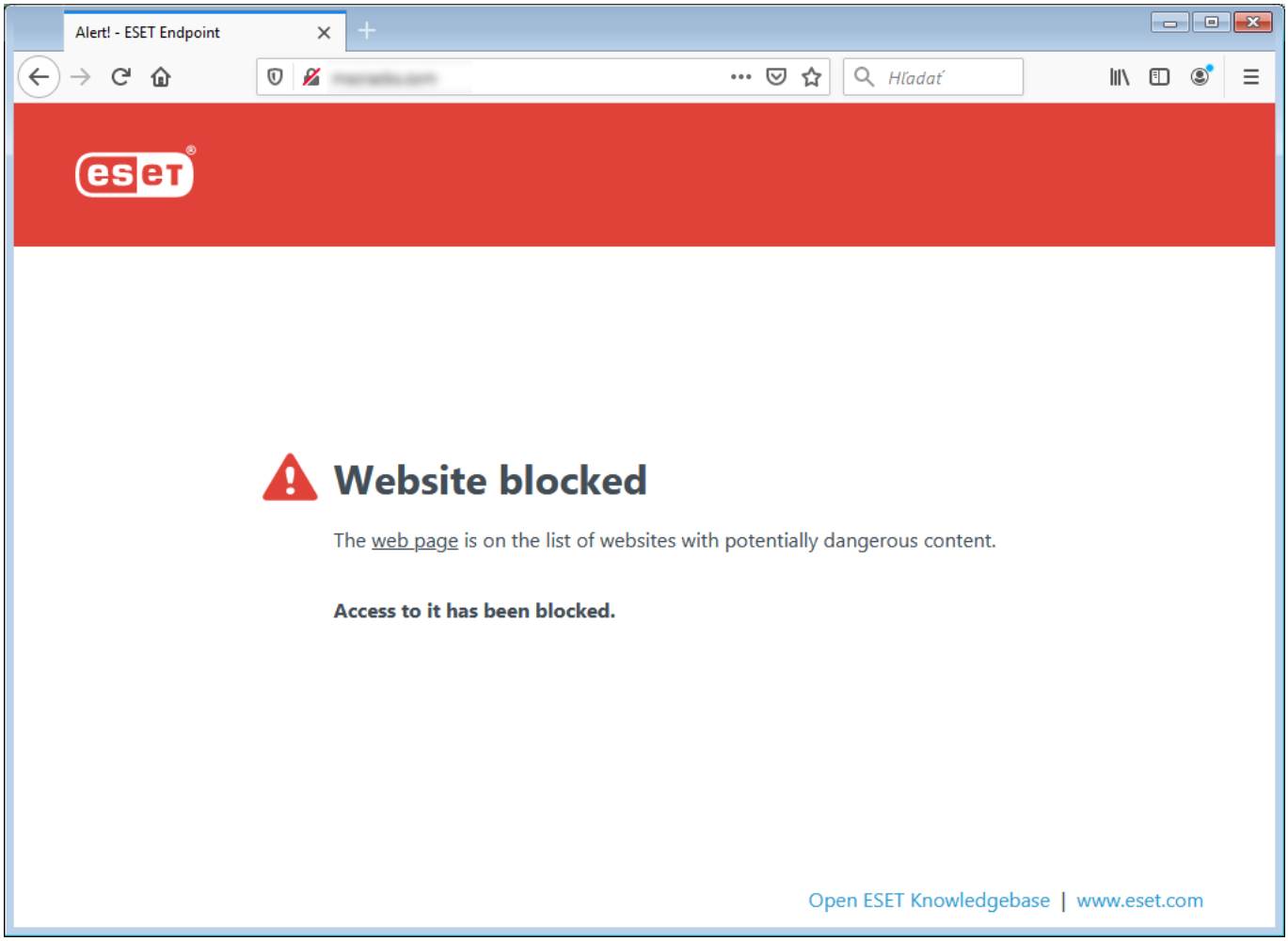
Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Web access protection works by monitoring communication between web browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPS (encrypted communication) rules.

Access to web pages known to contain malicious content is blocked before content is downloaded. All other webpages are scanned by the ThreatSense scanning engine when they are loaded and blocked if malicious content is detected. Web access protection offers two level of protection, blocking by blacklist and blocking by content.

We strongly recommend that Web access protection is enabled. This option can be accessed from the main window of ESET Endpoint Security by navigating to **Setup** > **Internet protection** > **Web access protection**.



Web access protection will display the following message in your browser when the website is blocked:



Illustrated instructions

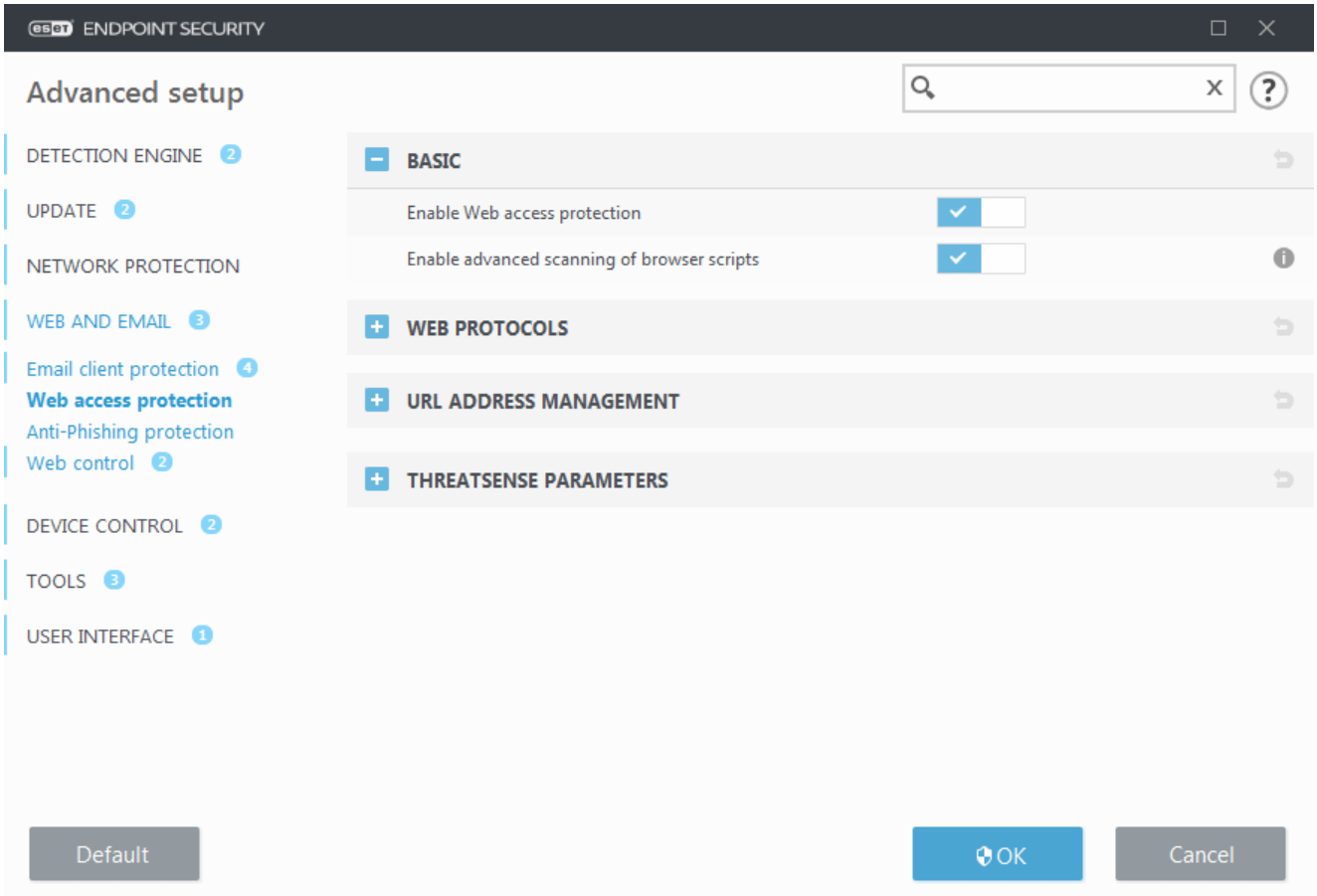
The following ESET Knowledgebase articles may only be available in English:

- Unblock a safe website on an individual workstation in ESET Endpoint Security
- Unblock a safe website on an endpoint using ESET Security Management Center

---

The following options are available in **Advanced setup** (F5) > **Web and email** > **Web access protection**:

- **Basic** – To enable or disable this feature from Advanced setup.
- **Web protocols** – Enables you to configure monitoring for these standard protocols which are used by most Internet browsers.
- **URL address management** – Enables you to specify URL addresses to block, allow or exclude from checking.
- **ThreatSense parameters** – Advanced virus scanner setup – enables you to configure settings such as types of objects to scan (emails, archives, etc.), detection methods for Web access protection etc.



Web access protection advanced setup

The following options are available in **Advanced setup** (F5) > **Web and email** > **Web access protection** > **Basic**:

Enable Web access protection – When disabled, Web access protection and Anti-Phishing protection will not run.

Enable advanced scanning of browser scripts – When enabled, all JavaScript programs executed by web browsers will be checked by the detection engine.

> **Note**
> We strongly recommend you leave Web access protection enabled.

Web protocols

By default, ESET Endpoint Security is configured to monitor the HTTP protocol used by most Internet browsers.

HTTP Scanner setup

HTTP traffic is always monitored on all ports for all applications.

HTTPS Scanner setup

ESET Endpoint Security also supports HTTPS protocol checking. HTTPS communication 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 (443, 0-65535) defined in **Ports used by HTTPS protocol**, regardless of operating system version.

Encrypted communication will be scanned by default. To view the scanner setup, navigate to SSL/TLS in the Advanced setup section, click **Web and email** > **SSL/TLS**, and enable the **Enable SSL/TLS protocol filtering** option.

URL address management

The URL address management section enables you to specify HTTP addresses to block, allow or exclude from content scan.

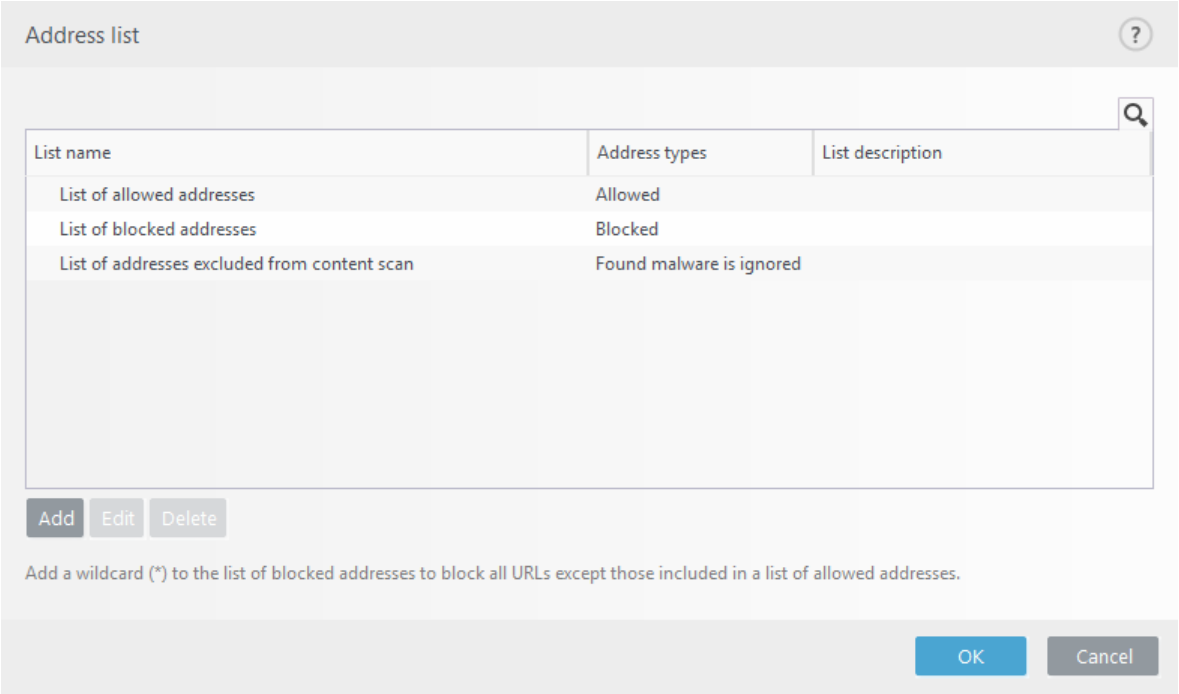
Enable SSL/TLS protocol filtering must be selected if you want to filter HTTPS addresses in addition to HTTP web pages. Otherwise only the domains of HTTPS sites that you have visited will be added, the full URL will not be.

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. Particular care should be taken 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**.

> **Trussted domains**
> Addresses will not be filtered if the setting **Web and email** > **SSL/TLS** > **Exclude communication with trusted domains** is enabled and the domain is considered trusted.



Control elements

Add – Creates a new list in addition to the predefined 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.

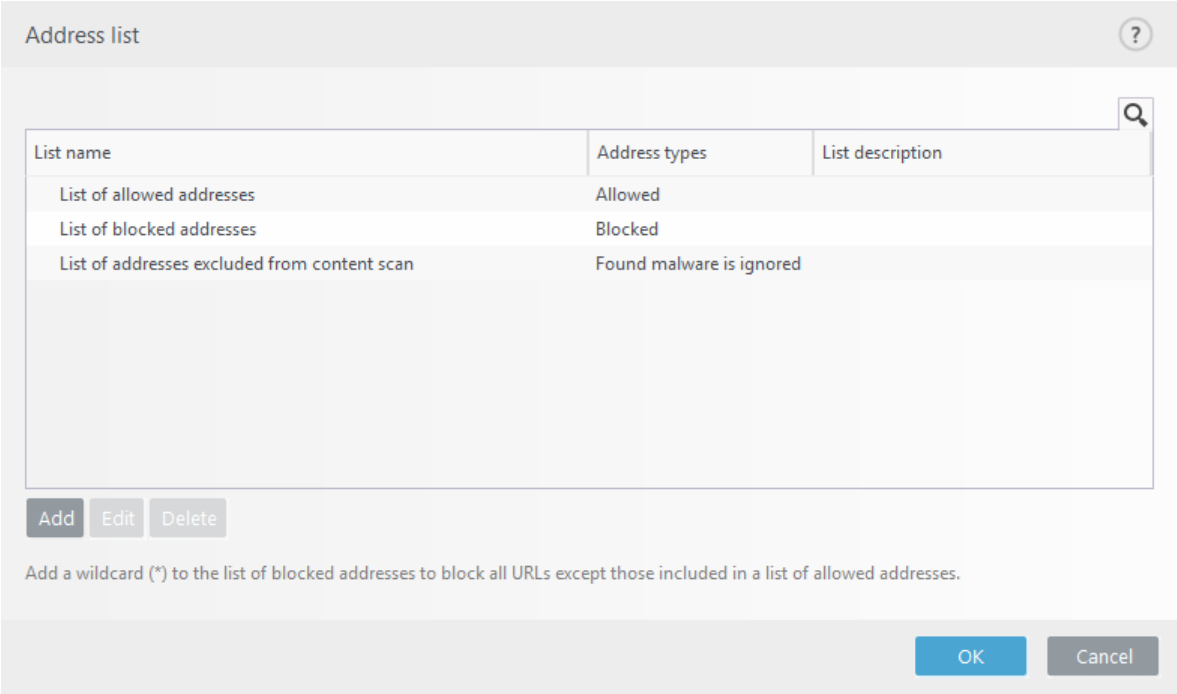
URL addresses list

In this section you can specify lists of HTTP 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**.



> **Illustrated instructions**
> The following ESET Knowledgebase articles may only be available in English:
> - Unblock a safe website on an individual workstation in ESET Endpoint Security
> - Unblock a safe website on an endpoint using ESET Security Management Center

For more information see URL address management.

Create new URL address list

This section allows you to specify lists of URL addresses/masks that will be blocked, allowed or excluded from checking.

When creating a new list, the following options are available to configure:

Address list type – Three predefined list types are available:

- **Excluded from checking** – No checking for malicious code will be performed for any address added to this list.
- **Blocked** - The user will not be allowed to access addresses specified in this list.
- **Allowed** – If your policy is configured to use this feature and the wildcard (*) value is added to this list, you will be allowed to access addresses in this list even if those addresses are also present in the blocked list.

List name – Specify the name of the list. This field will be unavailable if you are editing one of the three predefined lists.

List description – Type a short description for the list (optional).This field will be unavailable if you are editing one of the three predefined lists.

List active – select the slider bar to activate the list.

Notify when applying – select the slider bar if you want to be notified when this list is used to evaluate an HTTP

site that you visited. For example, a notification will be issued when a website is either blocked or allowed because the website is included in the list of blocked or allowed addresses. The notification will display the list name for the list that specifies the website.

Logging severity – Select the Logging severity from the drop-down menu. Records with Warning verbosity can be collected by Remote Administrator.

Control elements

Add – Add a new URL address to the list (enter multiple values with separator).

Edit – Modifies existing address in the list. Only possible for addresses created with **Add**.

Delete – Deletes existing addresses in the list. Only possible 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).

How to add URL mask

Please refer to the instructions in this dialog before you enter the desired address/domain mask.

ESET Endpoint Security enables user to block access to specified websites and prevent the Internet browser from displaying their content. Furthermore, it allows user to specify addresses, which should be excluded from checking. If the complete name of the remote server is unknown, or the user wishes 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.).

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*.

Anti-Phishing protection

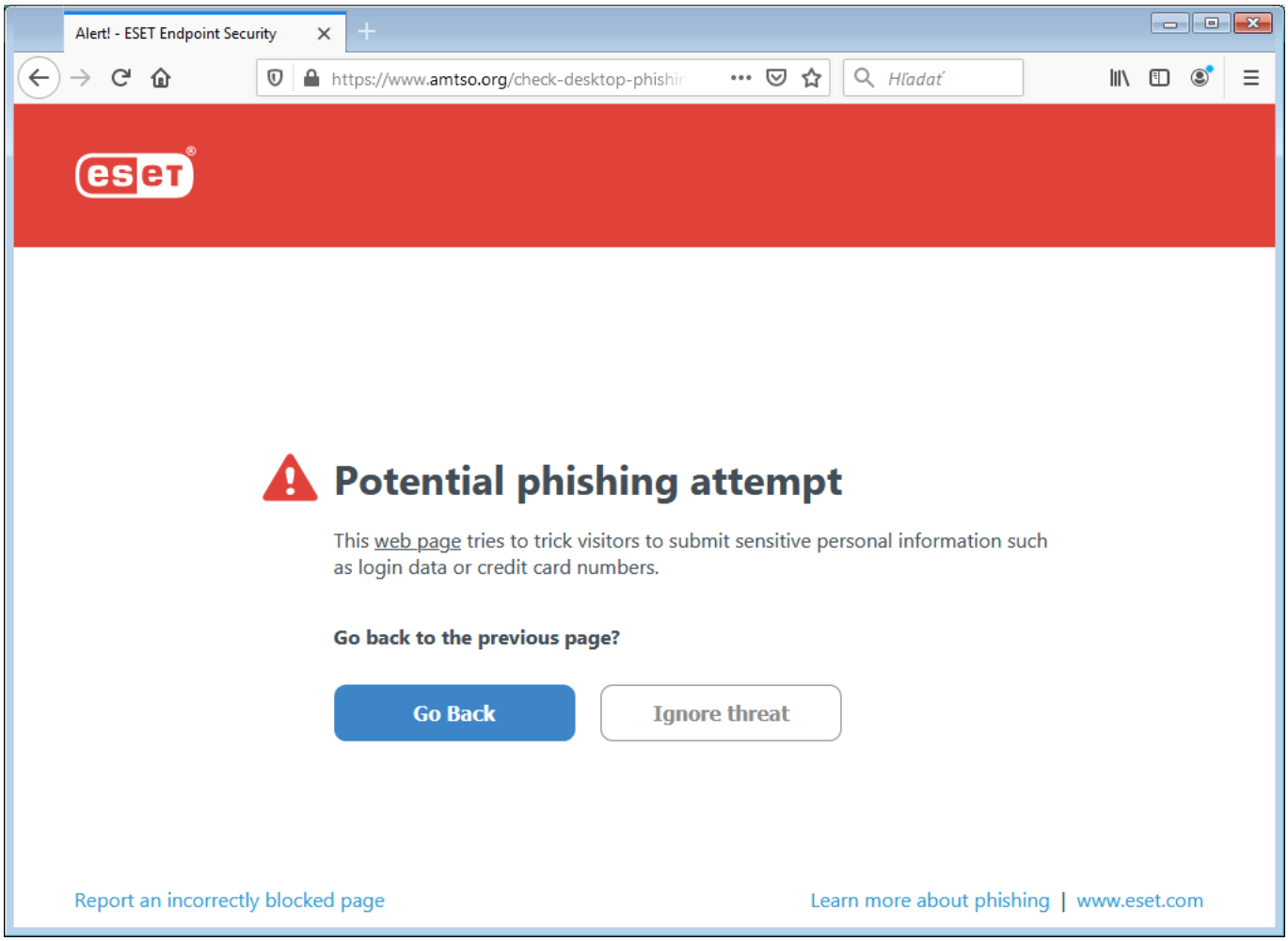
The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this activity in the glossary. ESET Endpoint Security includes anti-phishing protection, which blocks web pages known to distribute this type of content.

We strongly recommend that you enable Anti-Phishing in ESET Endpoint Security. To do so, open **Advanced setup** (F5) and navigate to **Web and email** > **Anti-Phishing 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, the following dialog will be displayed in your web browser. If you still want to access the website, click **Proceed to the site** (not recommended).



> **Note**
> 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. From **Advanced setup** (F5) expand **Web and email** > **Web access protection** > **URL address management** > **Address list**, click **Edit** and then add the website that you want to edit to the list.

Phishing site reporting

The Report link enables you to report a phishing/malicious website to ESET for analysis.

> **Note**
> Before submitting a website to ESET, make sure 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 a false-positive phishing site.

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.).

Web control

The Web control section allows 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.

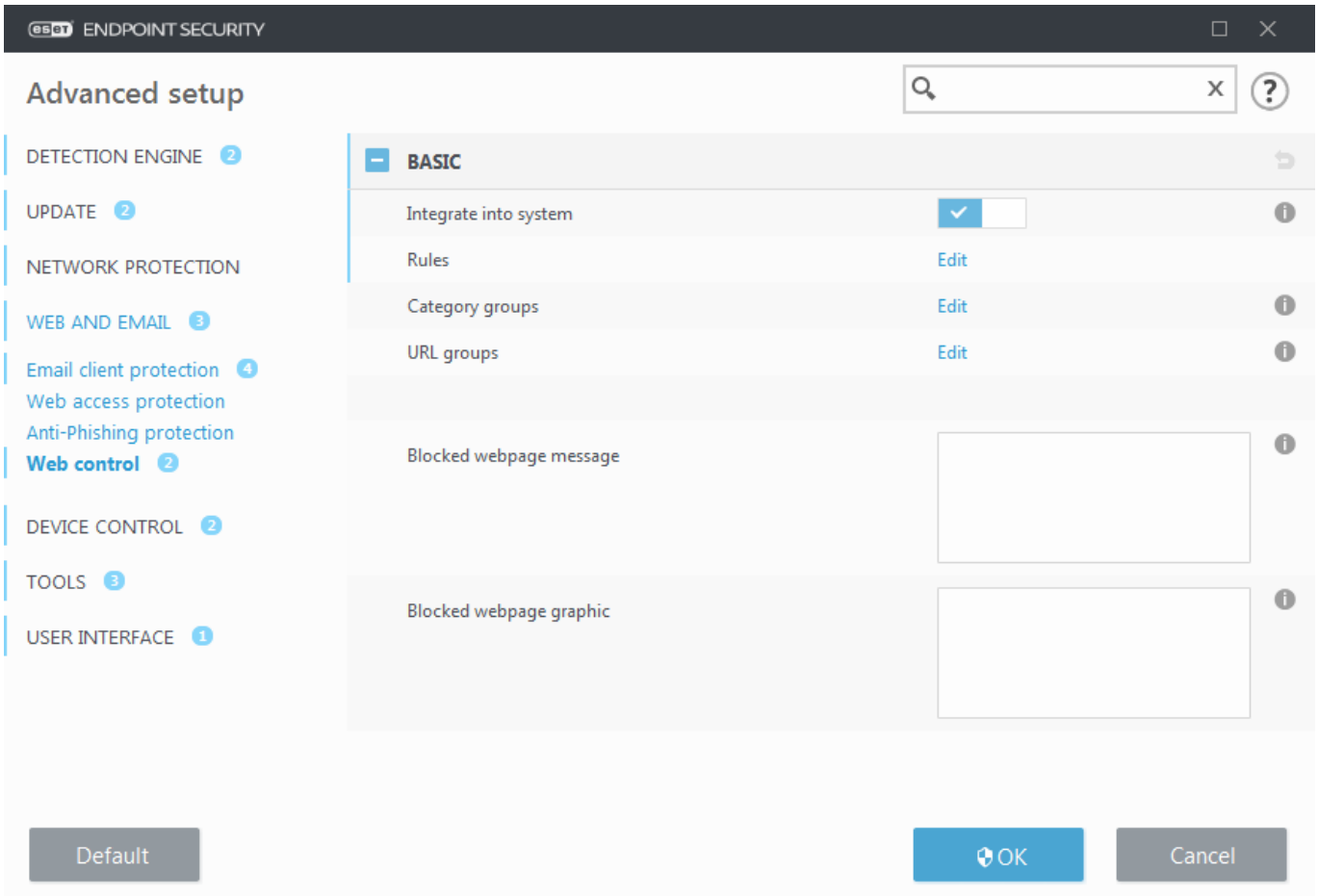
Web control lets you block webpages that may contain potentially offensive material. In addition, employers or system administrators can prohibit access to more than 27 pre-defined website categories and over 140 subcategories.

By default, Web control is disabled. To activate Web control:

1.Press **F5** to enter **Advanced setup** and expand **Web and email** > **Web control**.

2.Select **Enable Web control** (formerly Integrate into system) to activate Web control in ESET Endpoint Security.

3.To configure access to specific webpages, click **Edit** next to **Rules** to access the Web control rules editor window.

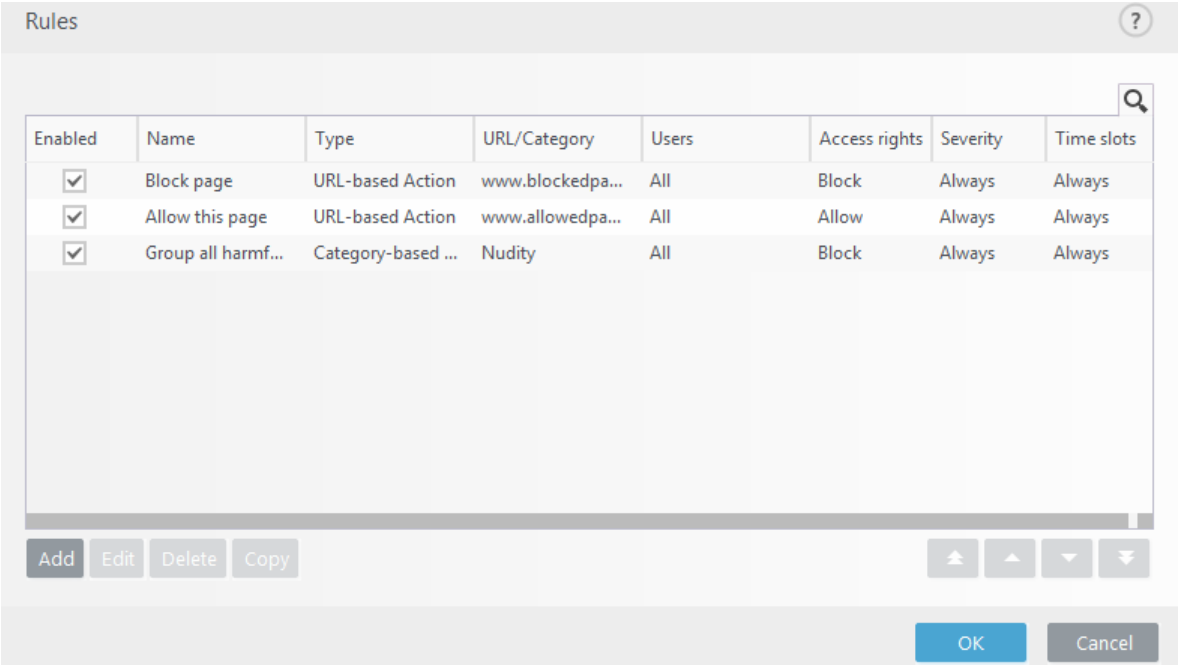


Blocked webpage message and **Block webpage graphic** fields allow you to easily customize the displayed message when a website is blocked.

> **Note**
> In case you want to block all webpages 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 predefined 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.

For more information on creating rules click here.

Adding Web control rules

The Web control rules window allows you to manually create or modify an existing Web control filtering rule.

Name

Enter 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

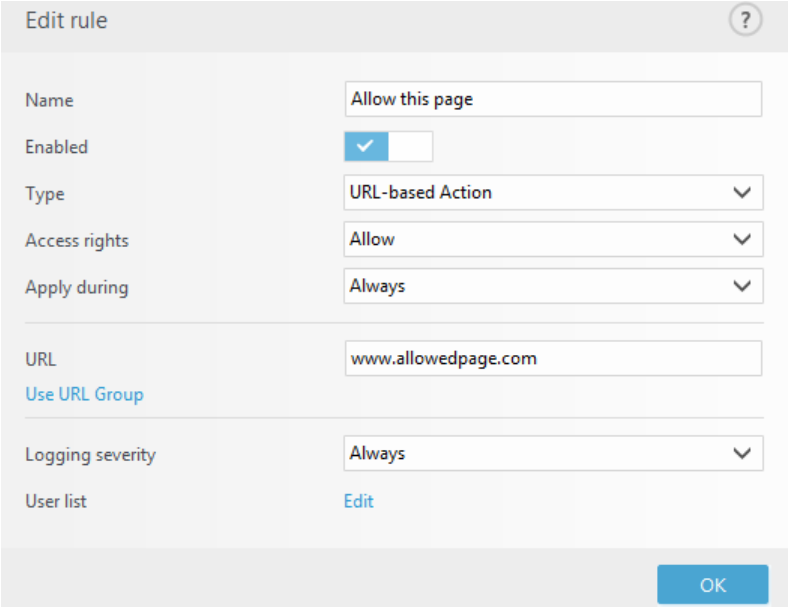
Choose between **URL-based Action** or **Category-based Action**:

URL-based Action

For rules that control access to a given website, enter 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** – Uses the URL link or URL group of links to allow, block or warn the user when one of these URLs are detected.



Category-based Action

When this is selected, set the website category for your action using the drop-down menu.

URL Category or **Use Group** – Uses the website category or Category groups of categories to allow, block or warn the user when one of these groups are detected.

Access rights

- **Allow** – Access to the URL address/category will be granted.
- **Warn** – Warns the user about the URL address/category.
- **Block** – Blocks the URL address/category.

Apply during

Allows you to apply created rule during the certain time. From the drop-down menu, select created time slot.

- 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.

> **Note**
> The Logging severity can be configured separately for each list. Logs with **Warning** status can be collected by ESET Security Management Center.

User list

- **Add** – Opens the **Select Users or Groups** dialog window, which allows you to select desired users. When no user is entered the rule is applied for all users.
- **Delete** – Removes the selected user from the filter.

Category groups

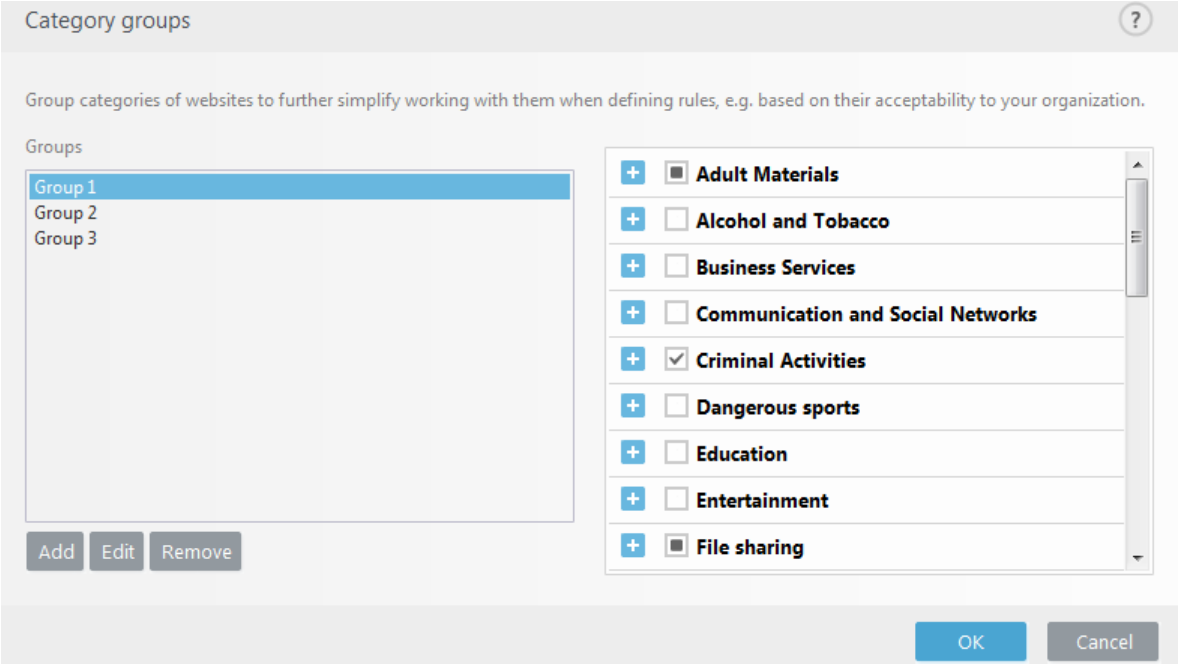
The Category groups window is divided into two parts. The left part of the window contains a list of Category groups.

- **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 on 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, or users can be informed after a rule with

predefined actions is created.

Select the check box to add or remove a subcategory to a particular 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.

> **Note**
> A subcategory can belong to any group. There are some subcategories that are not included in predefined groups (for example, Games). In order to match a desired subcategory using Web control filter, add it to your desired group.

URL groups

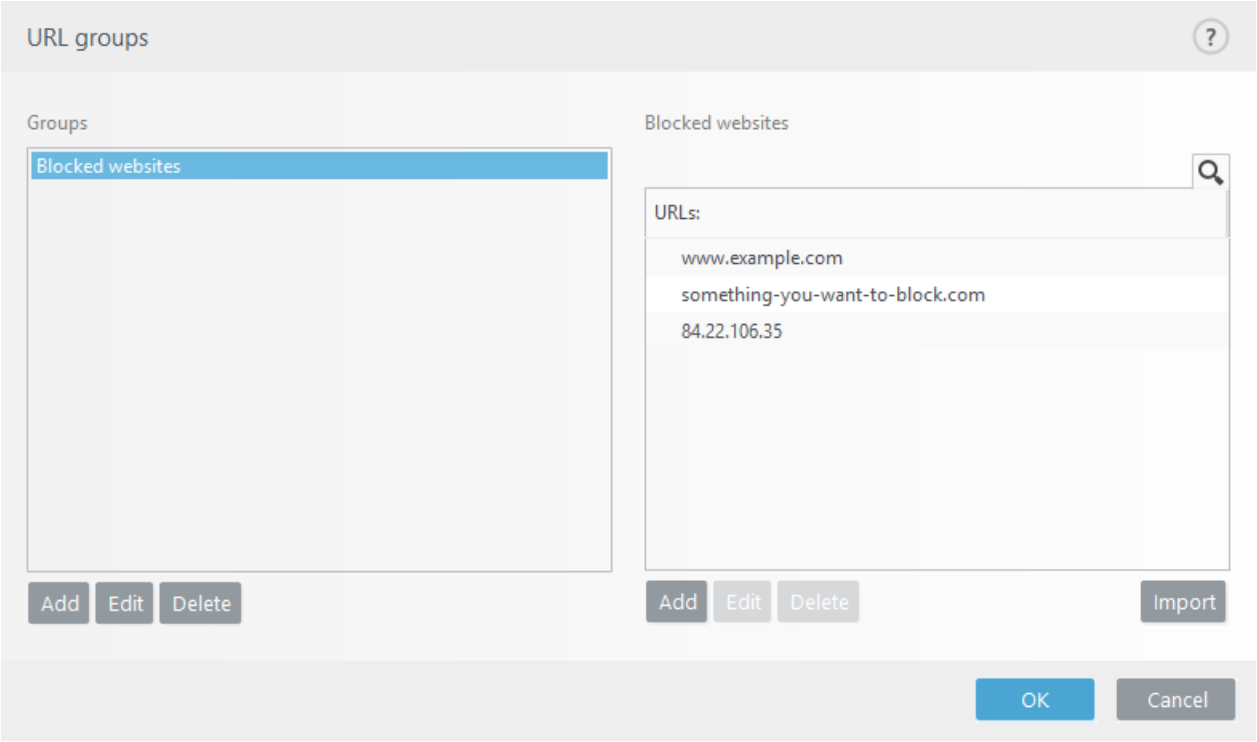
URL groups allow you to create a group that contains several URL links for which you want to create a rule (allow/disallow a particular website).

Create a new URL group

To create a new URL group click **Add** and enter 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 enter 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

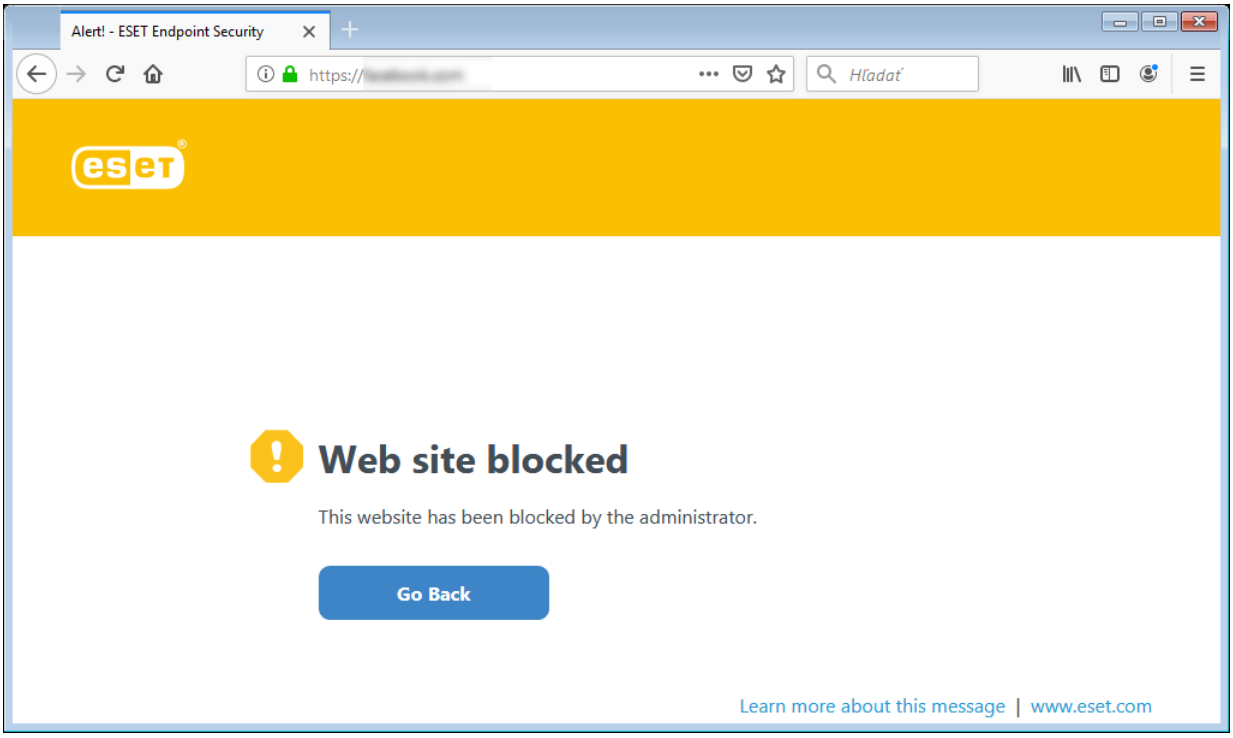
If you want to set an action to be performed for a specific URL group, open the Web control rules editor, **select your URL group using the** drop-down menu, adjust other parameters and then click **OK**.

> **Note**
> 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 **Block webpage graphic** fields allow you to easily customize the displayed message when a website is blocked.

This is the default message and design of the in-browser notification when a user tries to access a blocked website:



Usage

Let's block the "Weapons" website category.

An example of a blocked webpage 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.
```

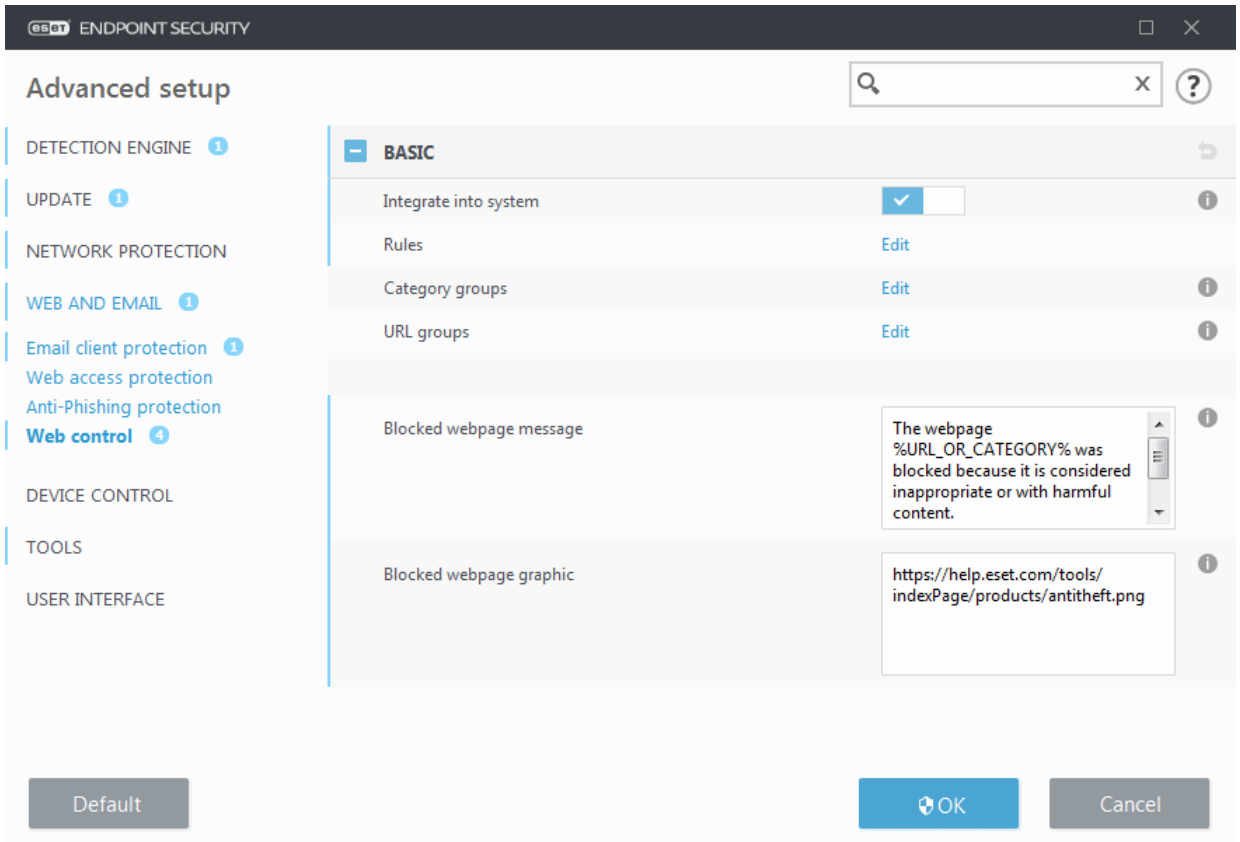
Variable	Description
%CATEGORY%	Blocked Web control category.
%URL_OR_CATEGORY%	Blocked Web control website or category (depends on the Web control blocking rule).
%STR_GOBACK%	"Go Back" button value.
%product_name%	Name of the ESET product (ESET Endpoint Security)
%product_version%	Version of the ESET product.

An example of a blocked webpage graphics will be:

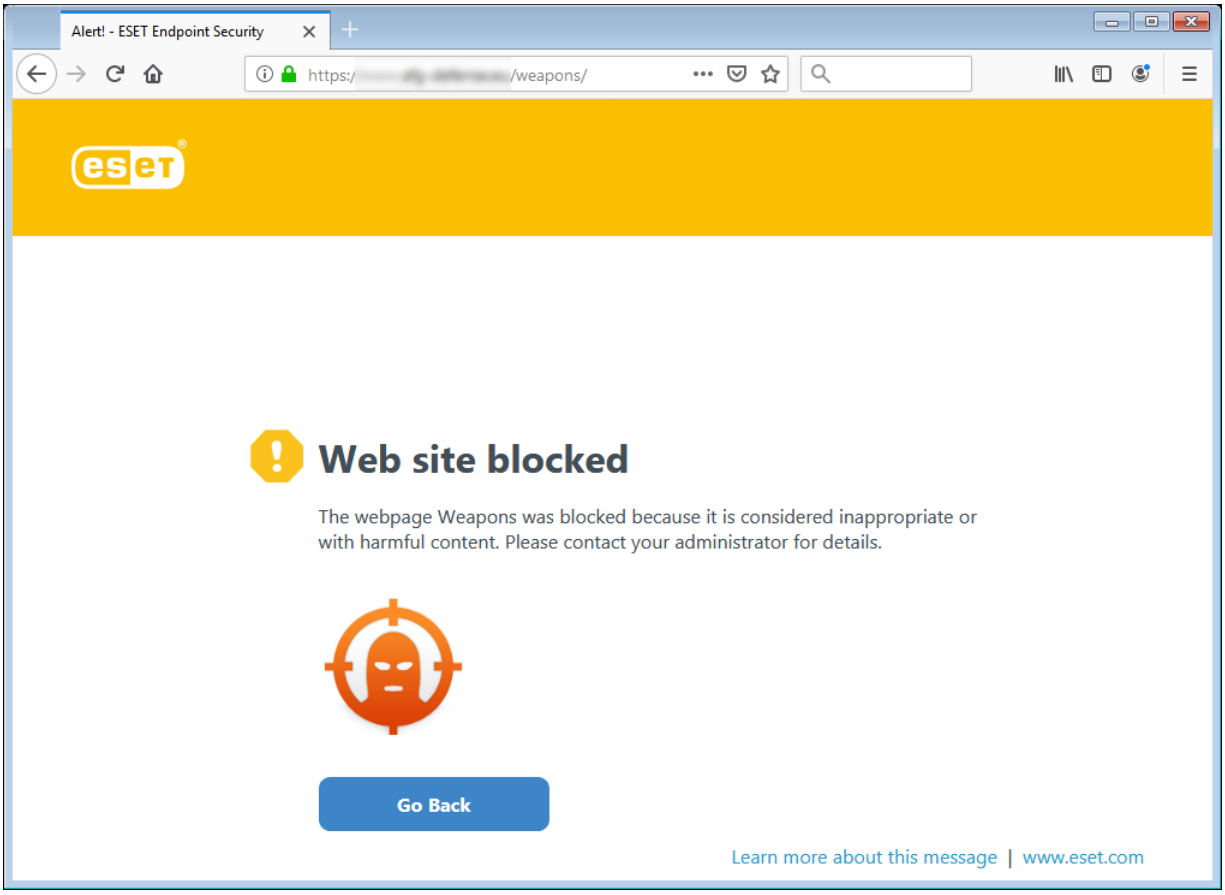
```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

The image size (width/height) will scale automatically if the size is too high.

The configuration in ESET Endpoint Security will look like:



The custom in-browser notification when a user tries to access a blocked website will look like:



Updating the program

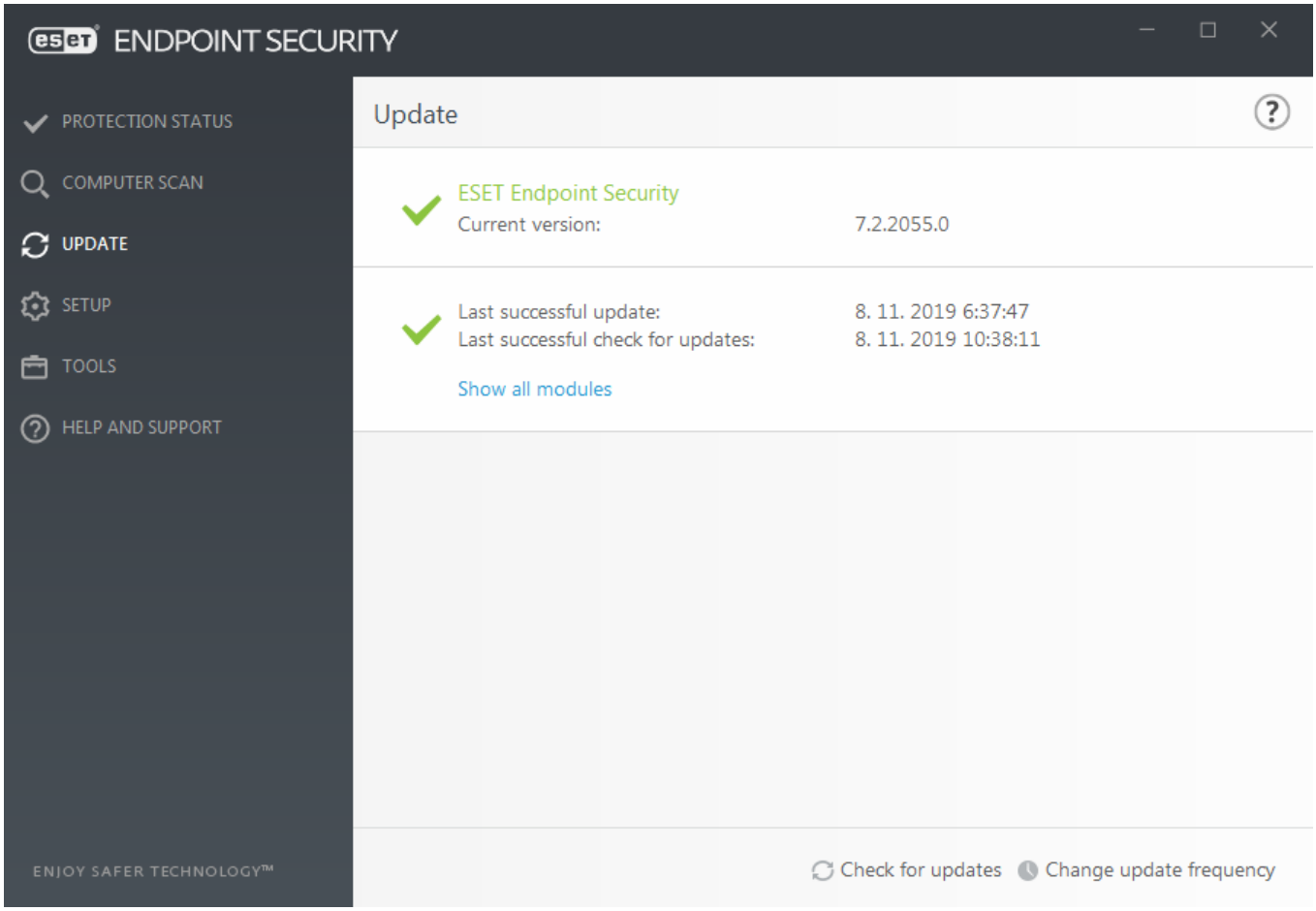
Regularly updating ESET Endpoint Security is the best method to obtain the maximum level of security on your computer. The Update module ensures that the program is always up to date in two ways, by updating the detection engine and by updating system components. Updates are automatic by default when the program is activated.

By clicking **Update** in the main program window, you can find the current update status including the date and time of the last successful update and if an update is needed. You can also click the **Show all modules** link to open the list of installed modules and check the version and the last update of a module.

In addition, the option to manually begin the update process, **Check for updates** is available. Updating the detection engine and updating program components are important parts of maintaining complete protection against malicious code. Please pay attention to their configuration and operation. If you did not enter your License details during installation, you can enter your license key by clicking **Activate product** when updating to access ESET's update servers.

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.

> **Note**
> Your license key is provided by ESET after purchasing ESET Endpoint Security.



Current version – The ESET Endpoint Security build number.

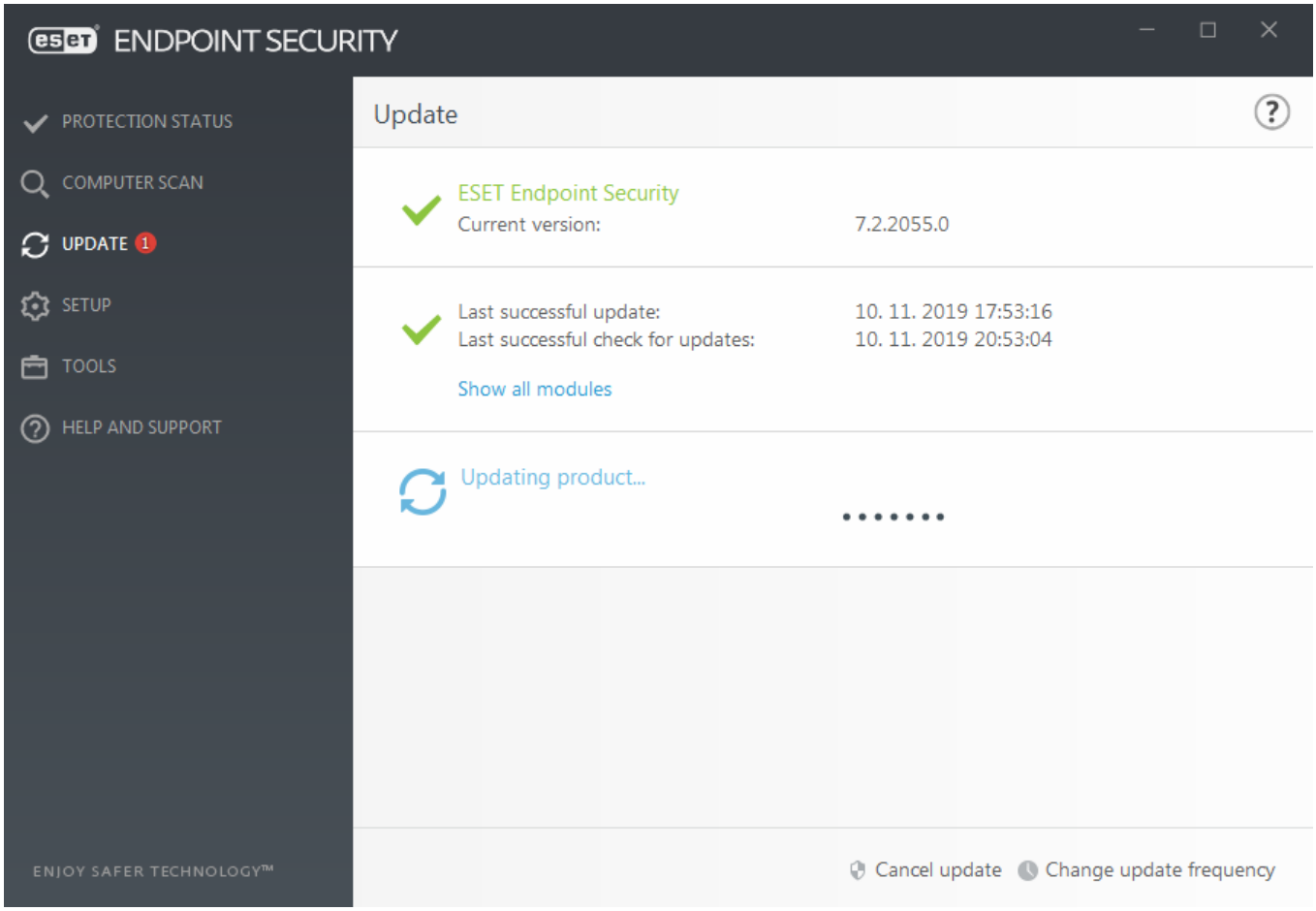
Last successful update – The date and time of the last successful update. Make sure it refers to a recent date, which means that the detection engine is current.

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**.

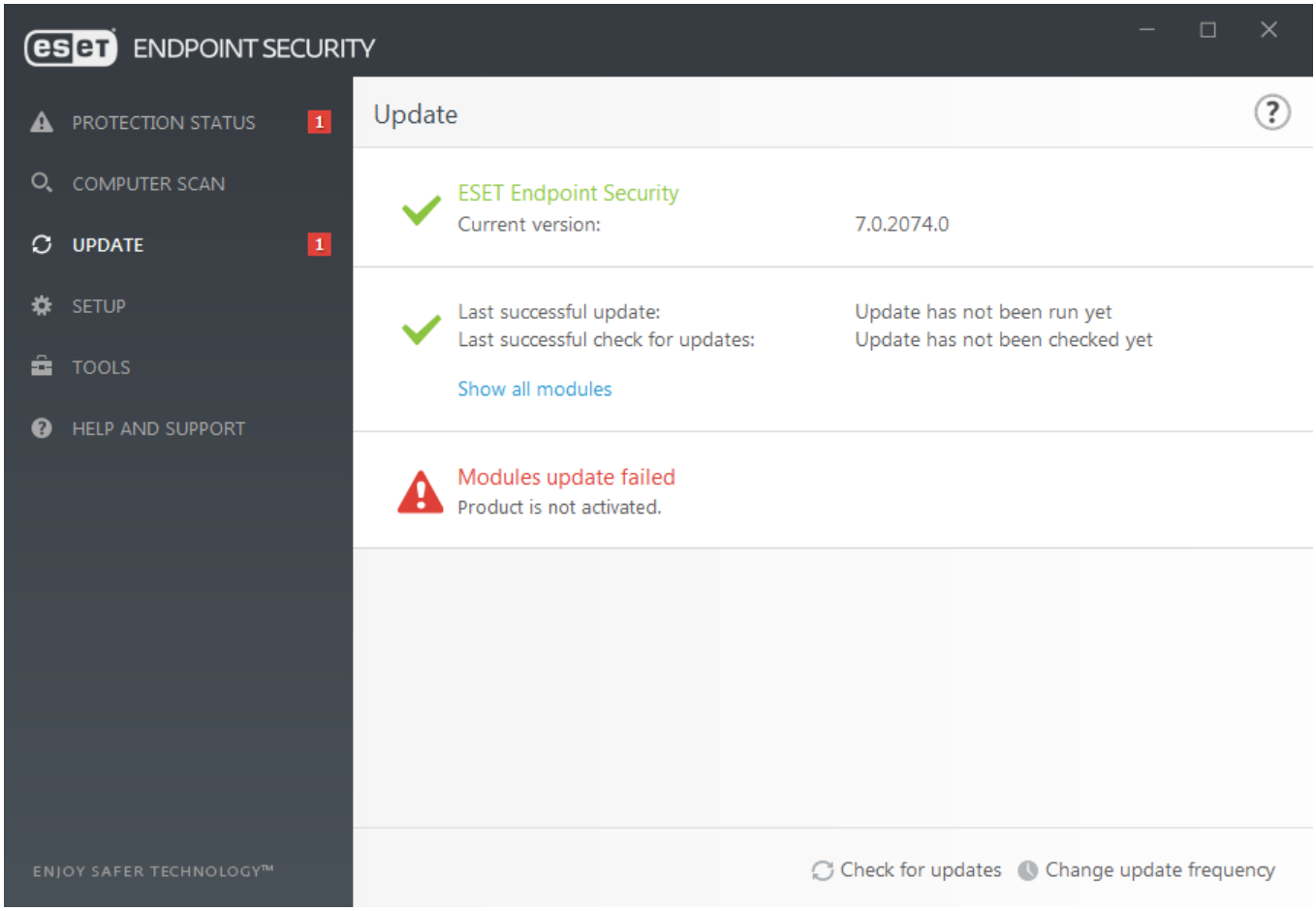


> **Important**
> Under normal circumstances the modules updates several times a day. If this is not the case, the program is out of date and more vulnerable to infection. Please update the modules as soon as possible.

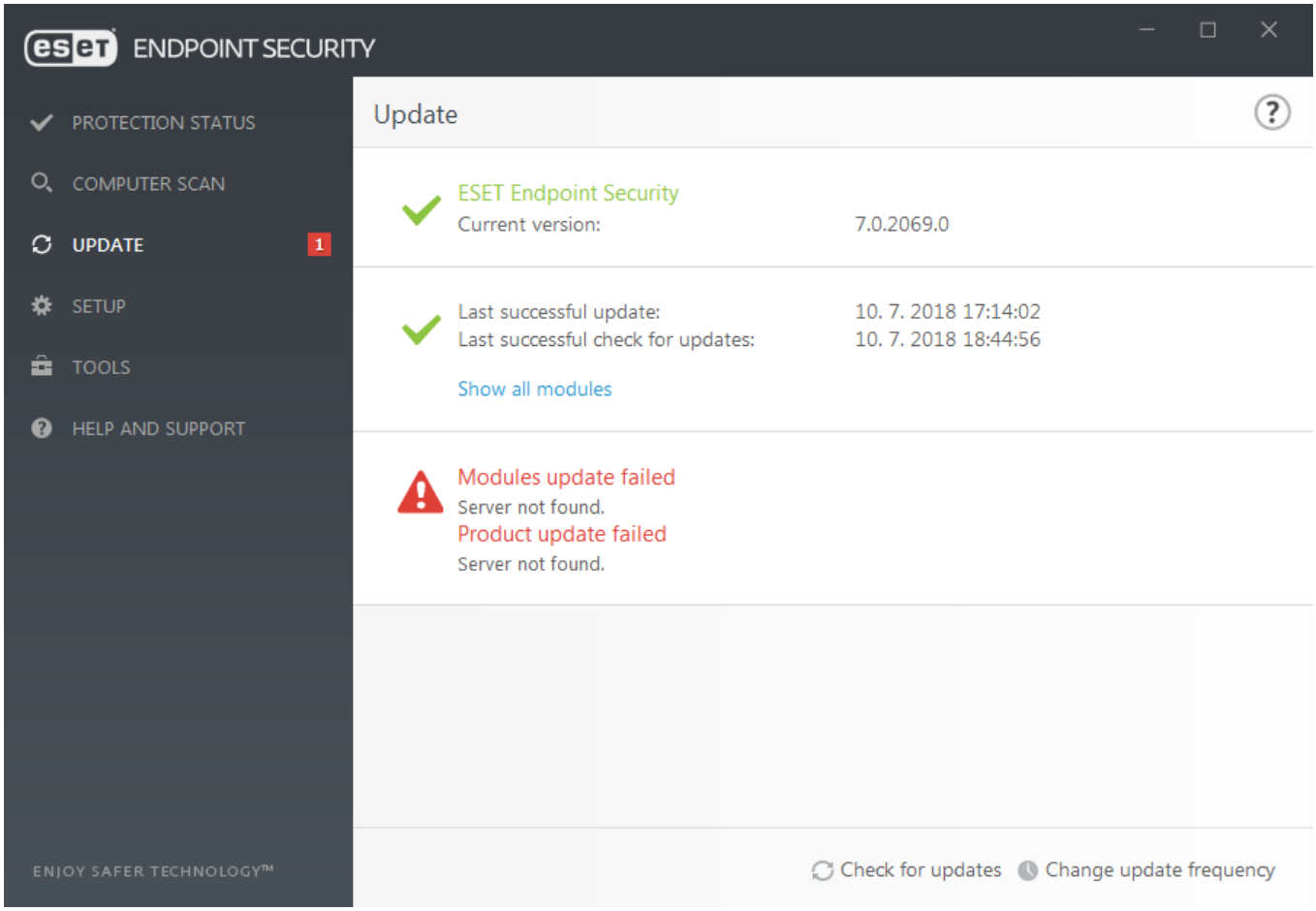
Detection engine out of date – This error will appear after several unsuccessful attempts to update modules. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured connection settings.

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

1. **Invalid license** – The license key has been incorrectly entered in update setup. We recommend that you check your authentication data. The Advanced setup window (click **Setup** from the main menu and then click **Advanced setup**, or press F5 on your keyboard) contains additional update options. 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. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.



> **Note**
> For more information please visit this ESET Knowledgebase article.

Update setup

Update setup options are available in the **Advanced setup** tree (F5) under **Update**. This section specifies update source information like the update servers being used and authentication data for these servers.

> **Adjust update settings correctly**
> For updates to be downloaded properly, it is essential that you fill in all update parameters correctly. If you use a firewall, please make sure that your ESET program is allowed to communicate with the Internet (for example, HTTPS communication).

Basic

The update profile that is 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 – Assign an update profile according to Known networks in Firewall. Automatic profile switching allows to change the profile for specific network depending on the setting in Scheduler. Check help pages for more information

Configure update notifications (formerly **Select received 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**.

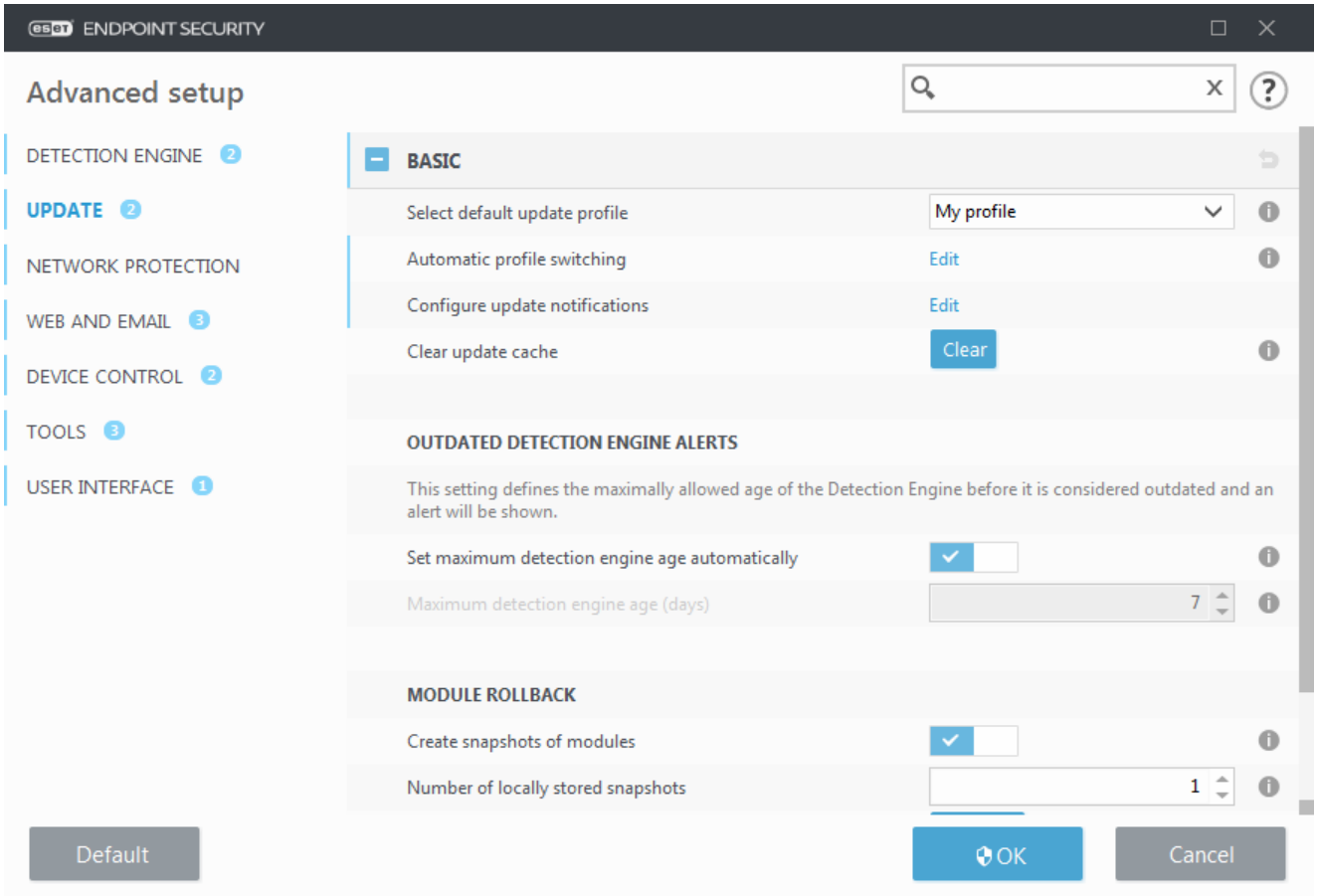
If you are experiencing difficulty when attempting to download modules updates, click **Clear** next to **Clear update cache** to clear the temporary update files/cache.

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.

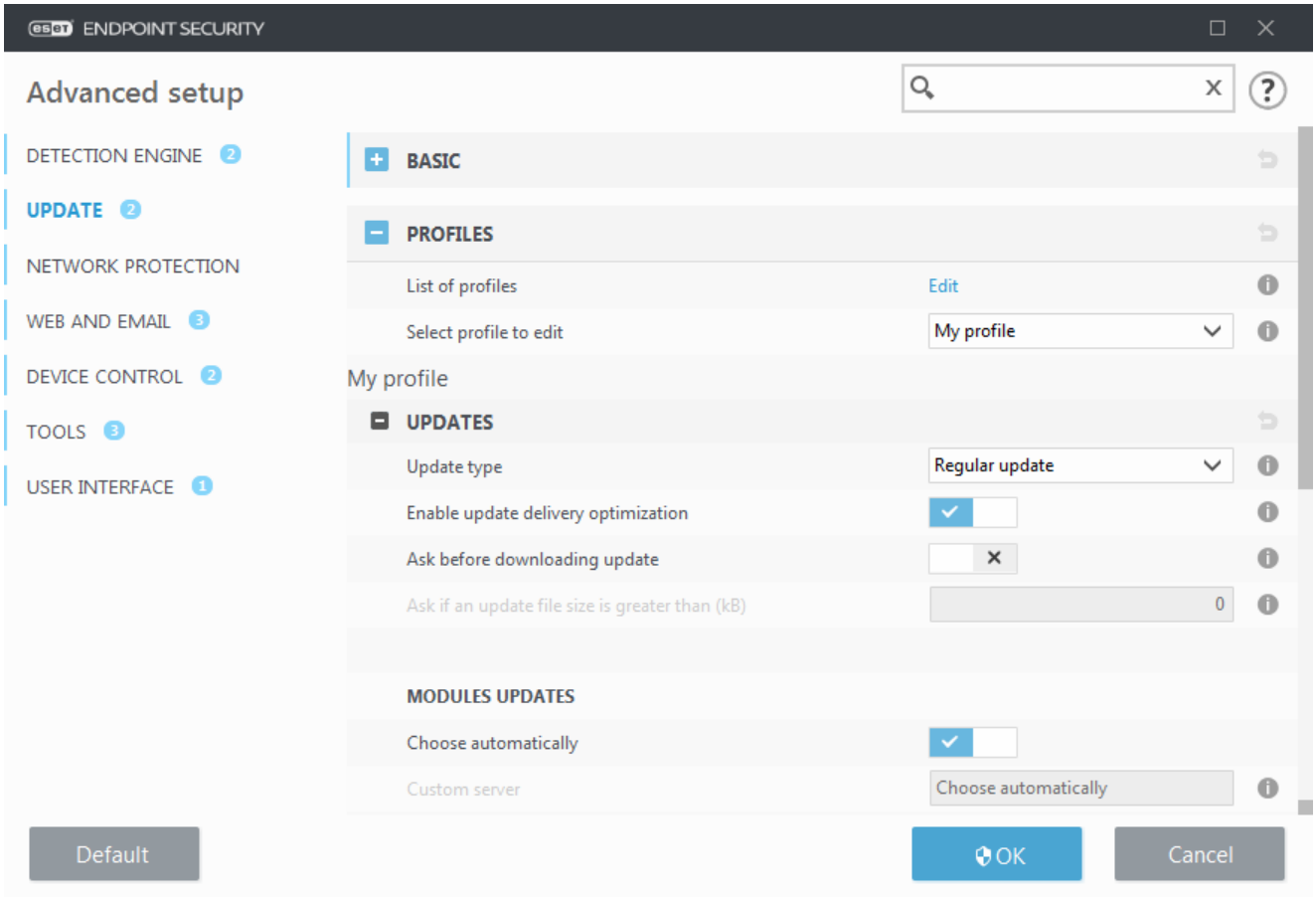
To create a new profile, click **Edit** next to **List of profiles**, enter your own **Profile name** and then click **Add**.

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 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 – Allows you to update from removable media if 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**
> HTTP server port number specified in the examples above depends on what port your HTTP/HTTPS server listens.

Program component update

See Program component update.

Connection options

See Connection options.

Update mirror

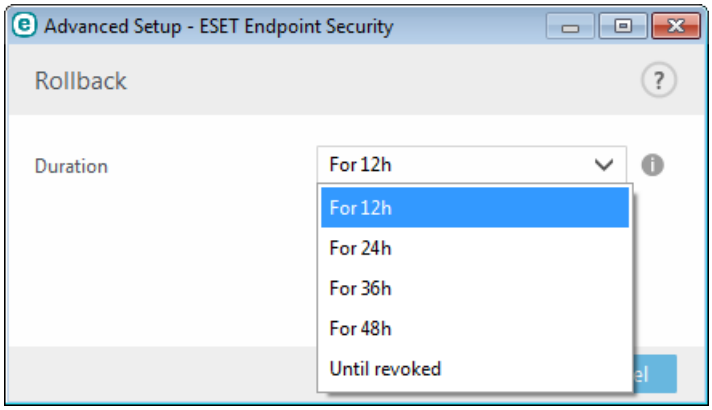
See Update mirror.

Update 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. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.

ESET Endpoint Security records snapshots of detection engine and program modules for use with the rollback feature. In order to create virus database snapshots, leave the **Create snapshots of modules** switch enabled. The **Number of locally stored snapshots** field defines the number of previous detection engine snapshots stored.

If you click **Rollback** (**Advanced setup** (F5) > **Update** > **Basic** > **Module rollback**), you have to select a time interval from the drop-down menu that represents the period of time that the detection engine and program module updates will be paused.



Select **Until revoked** to postpone regular updates indefinitely until you restore update functionality manually. Because it represents a potential security risk, we do not recommend selecting this option.

The detection engine version is downgraded to the oldest available and stored as a snapshot in the local computer file system.

> **Note**
> Let the number 19959 be the most recent version of detection engine. 19958 and 19956 are stored as a detection engine snapshots. Note that 19957 is not available because, for example, the computer was turned off and a more recent update was made available before 19957 was downloaded. If the **Number of locally stored snapshots** field is set to 2 and you click **Roll back**, the detection engine (including program modules) will be restored to version number 19956. This process may take some time. Check whether the version of detection engine has downgraded from the main program window of ESET Endpoint Security in the Update section.

Program component update

The **Program component update** section contains options related to the program component update. The program enables you to predefine its behavior when a new program component upgrade is available.

Program component updates brings 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 program component update has been installed, a computer restart may be required.

In the **Update mode** drop-down menu, three options are available:

- **Ask before update** – The default option. You will be prompted to confirm or refuse program component updates when they are available.
- **Auto-update** – A program component update will be downloaded and installed automatically. Please remember that a computer restart may be required.
- **Never update** – Program component updates will not be performed at all. This option is suitable for server installations, since servers can usually be restarted only when they are undergoing maintenance.

By default, program component updates are downloaded from ESET repository servers. In large or offline environments, the traffic can be distributed to allow internal caching of the program component files.

⊟ Define custom server for program component updates

1.Define the path to the program component update 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 program component update using a standard ESET Endpoint Security update.

> **Note**
> Selecting the most appropriate option depends on the workstation where the settings will be applied. Please be aware that there are differences between workstations and servers – for example, restarting the server automatically after a program update could cause serious damage.

Connection options

To access the proxy server setup options for a given update profile, click **Update** in the **Advanced setup** tree (F5) and then click **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 the **Tools** > **Proxy server** branch of the Advanced setup tree.

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 Internet Explorer during program installation, but if they are changed (for example, if you change your ISP), please make sure 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. Please be aware that 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.

> **Warning**
> 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 entered as follows: *domain_name\user* (if it is a workgroup, enter *workgroup_name\name*) and password. When updating from the HTTP version of the local server, no authentication is required.

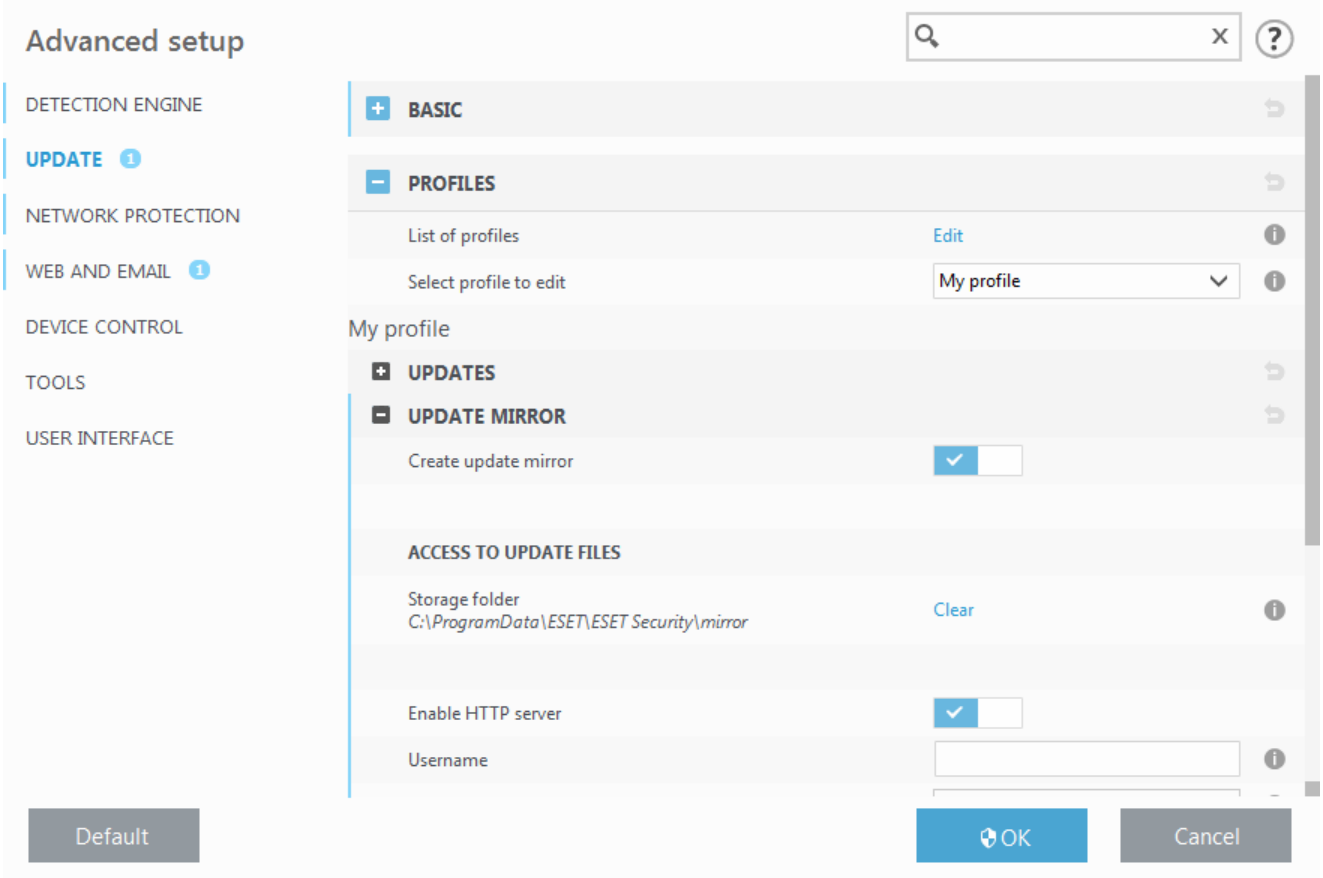
Select **Disconnect from server after update to force a disconnection if a** connection to the server remains active even after updates have been downloaded.

Update mirror

ESET Endpoint Security allows 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.

> **Use Apache HTTP Proxy to configure a mirror on large networks**
> To minimize Internet traffic on networks where ESET Security Management Center 7 is used to manage a large number of clients, we recommend that you use Apache HTTP Proxy rather than configure a client as a mirror. Apache HTTP Proxy can be installed with ESET Security Management Center Server (ESMC Server) using the all-in-one installer or as a standalone component if you have already installed the ERA Server. For more information and differences between Apache HTTP Proxy, Mirror Tool, and direct connectivity, see our ESMC Online Help page.

Configuration options for the local Mirror server are located in Advanced setup under **Update.** To access this section press **F5** to access Advanced setup, click **Update** > **Profiles and expand 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 predefined 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 entered 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 and password should be entered in the format *Domain/User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

Program component update

Files – When configuring the Mirror you can specify the language versions of updates you want to download. Languages selected must be supported by the mirror server configured by the user.

Update components automatically – Allows for the installation of new features and updates to existing features. An update can be performed automatically without user intervention, or you can choose to be notified. After a program component update has been installed, a computer restart may be required.

Update components now – Updates your program components to the latest version.

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.

> **Note**
> 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.

Accessing the Mirror using an internal HTTP server

This is the default configuration specified in the predefined program configuration. To allow access to the Mirror using the HTTP server, navigate to **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.

> **Warning**
> 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.

> **Note**
> An error **Invalid Username and/or Password** will appear in the Update pane from the main menu after several unsuccessful attempts to update the detection engine from the Mirror. We recommend that you navigate to **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:

- **Access Advanced setup** (F5) 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 enter authentication data to access the other computer. To enter authentication data, open ESET Endpoint Security **Advanced setup** (F5) 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. In case the computer is in a domain, "domain\user" username should be used. In case 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 ESET Endpoint Security **Advanced setup** and click **Update** > **Profiles** > **Updates**.

2. Disengage **Choose automatically** next to **Module updates** and a new server to the **Update server field** using the *\\UNC\PATH* format.

> **Note**
> 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 ESMC 7 from the mirrorm set the Update server to (according to your HTTP server root location):
> `http://your_server_address/mirror/eset_upd/era6`

The last section controls program components (PCUs). By default, downloaded program components are prepared to copy to the local mirror. If **Program component update** 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 program component 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**, enter 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. Make sure 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”, please be aware that 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.

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 tasks are activated in ESET Endpoint Security:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **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 Scheduler.

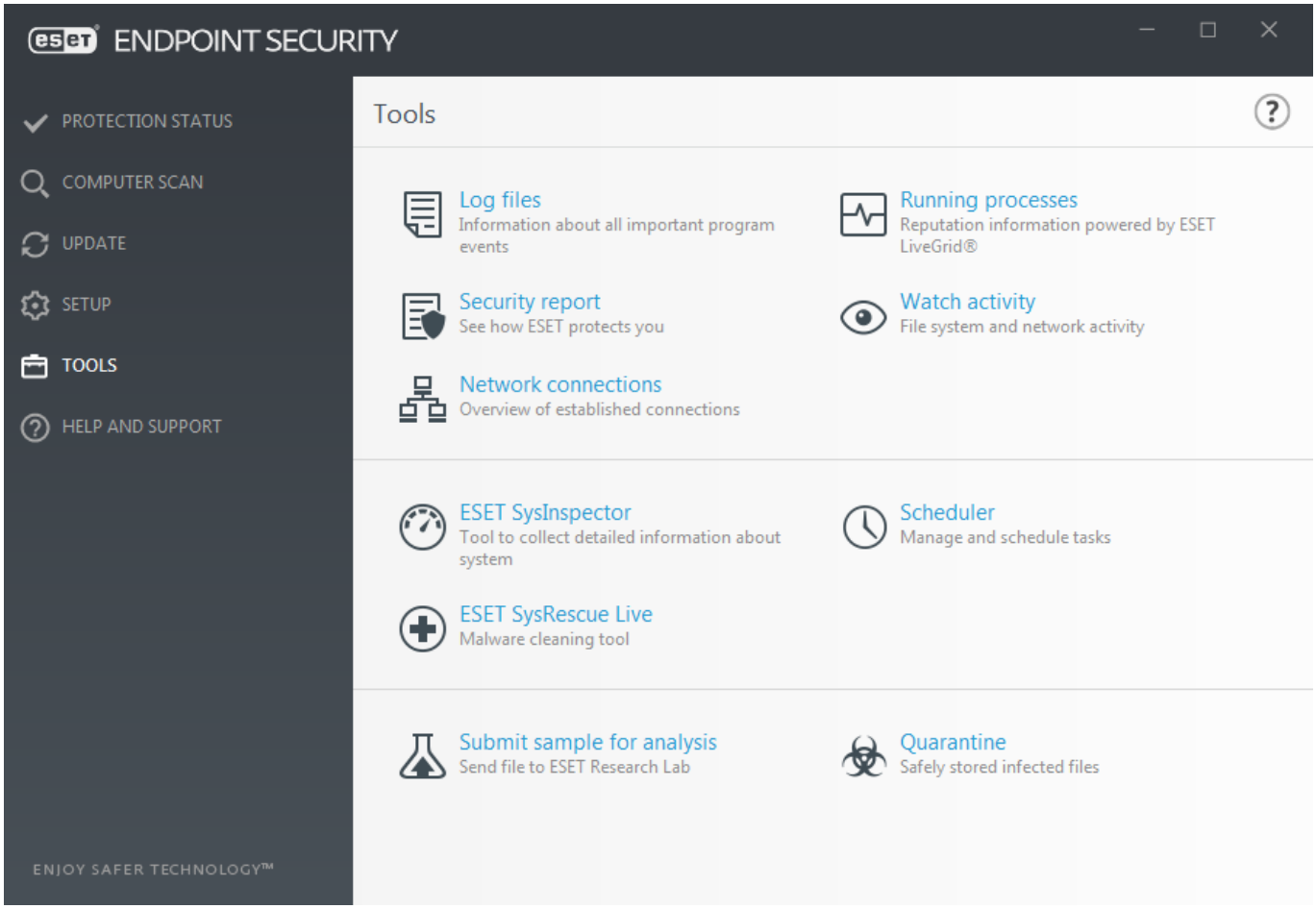
Tools

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

This menu includes the following tools:

- Log files
- Security report (for non-managed endpoints)
- Running processes (if ESET LiveGrid® is enabled in ESET Endpoint Security)
- Watch activity
- Scheduler
- Network connections (if Firewall is enabled in ESET Endpoint Security)
- ESET SysInspector
- ESET SysRescue Live – Redirects you to the ESET SysRescue Live website, where you can download the ESET SysRescue Live .iso CD/DVD image.
- Quarantine
- Submit sample for analysis – Allows you to submit a suspicious file for analysis to the ESET Research Lab

(may not be available based on your configuration of ESET LiveGrid®).



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. It is possible to 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 files that were blocked and could not be accessible. The protocol shows the reason and the source module that blocked the file, as well as the application and user that executed the file.

- **Sent files** – Contains records of files that were sent to ESET LiveGrid® or ESET Dynamic Threat Defense 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.

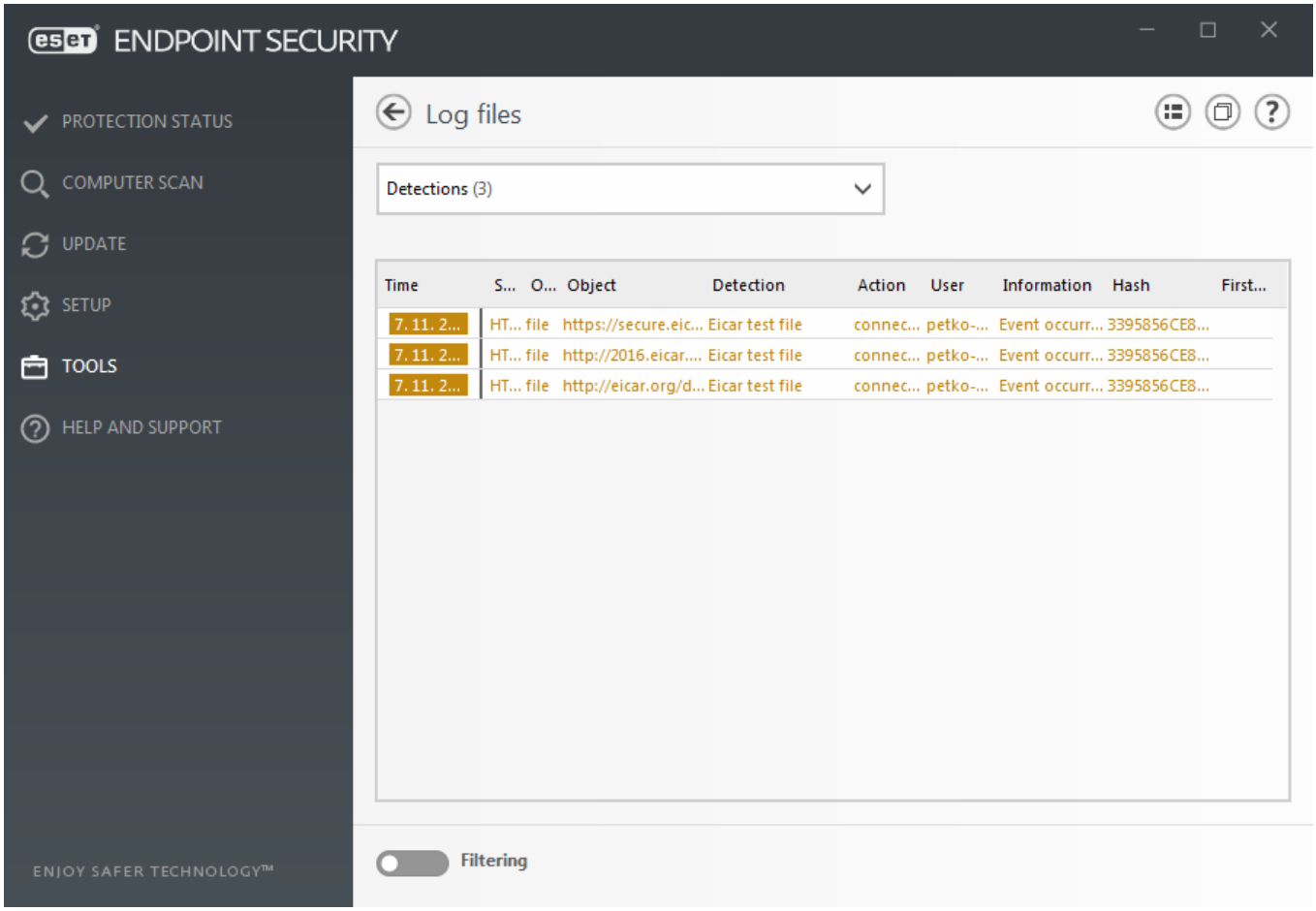
- **Network protection** – The firewall log displays all remote attacks detected by Network attack protection or Firewall. Here you will find information about any attacks on your computer. The Event column lists the detected attacks. The Source column informs you more about the attacker. The Protocol 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 particular 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 particular website.

- **Antispam protection** – 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, the Log filtering window will allow you to define filtering criteria for specific log entries.
- **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.
- **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, the Log filtering window will allow you to define filtering criteria to highlight the specific entry.

- **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. It lets you 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. Once you have 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.

Logging configuration

The Logging configuration of ESET Endpoint Security is accessible from the main program window. Click **Setup** > **Advanced Setup** > **Tools** > **Log files**. The logs section is used to define how the logs will be managed. The program automatically deletes older logs in order 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...).

> **Note**
> 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, log files will automatically be defragmented if fragmentation percentage is higher than value specified in the **If the number of unused records exceeds (%)** field.

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 particularly 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 predefined 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.

> **ESET Log Collector**
> In order 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 please visit our ESET Knowledgebase article.

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 from ESET Endpoint Security version 7.1 and solution 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:

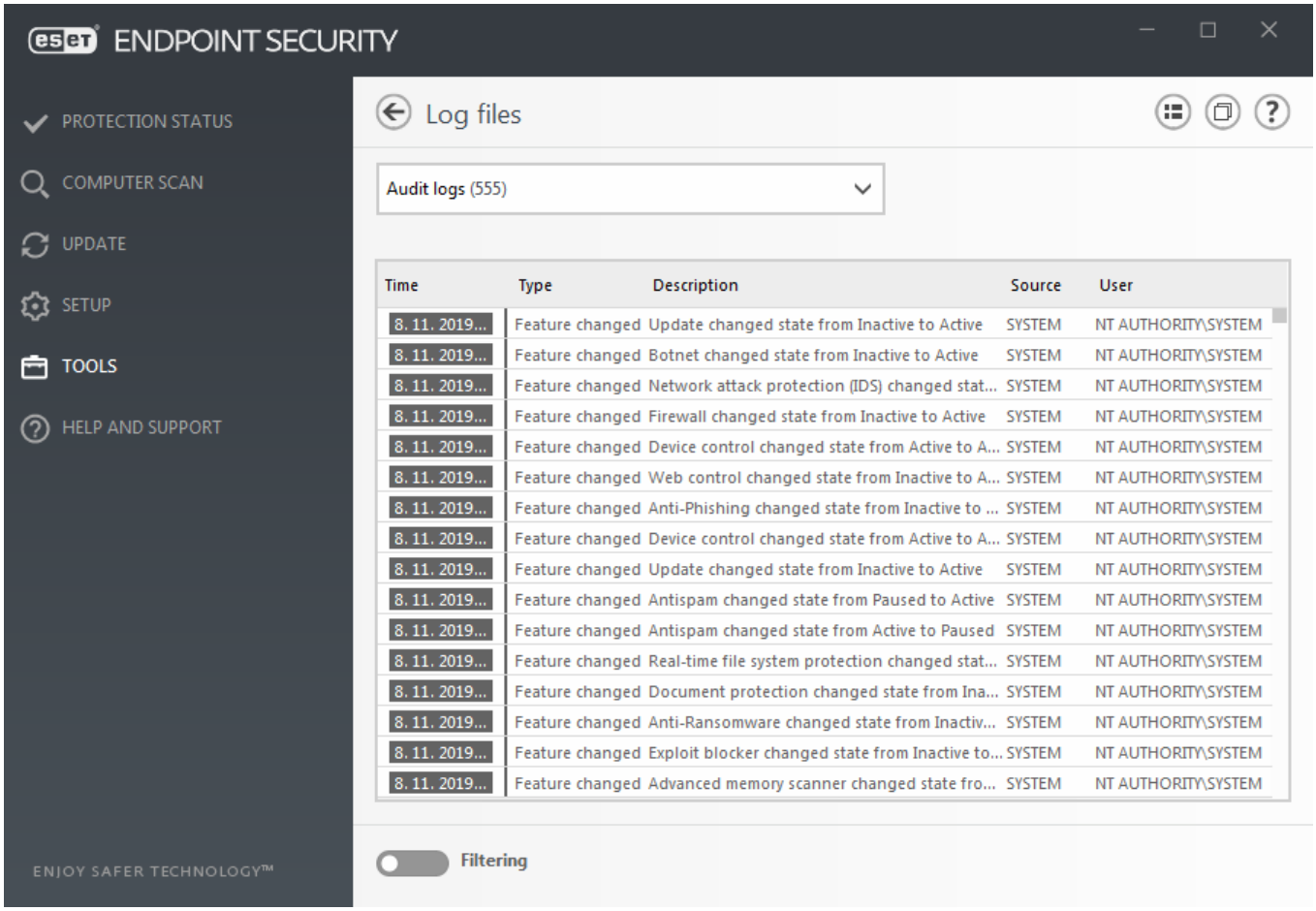
- Time - when the change was performed

- 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 ESMC). 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.

Scheduler

The Scheduler manages and launches scheduled tasks with predefined configuration and properties.

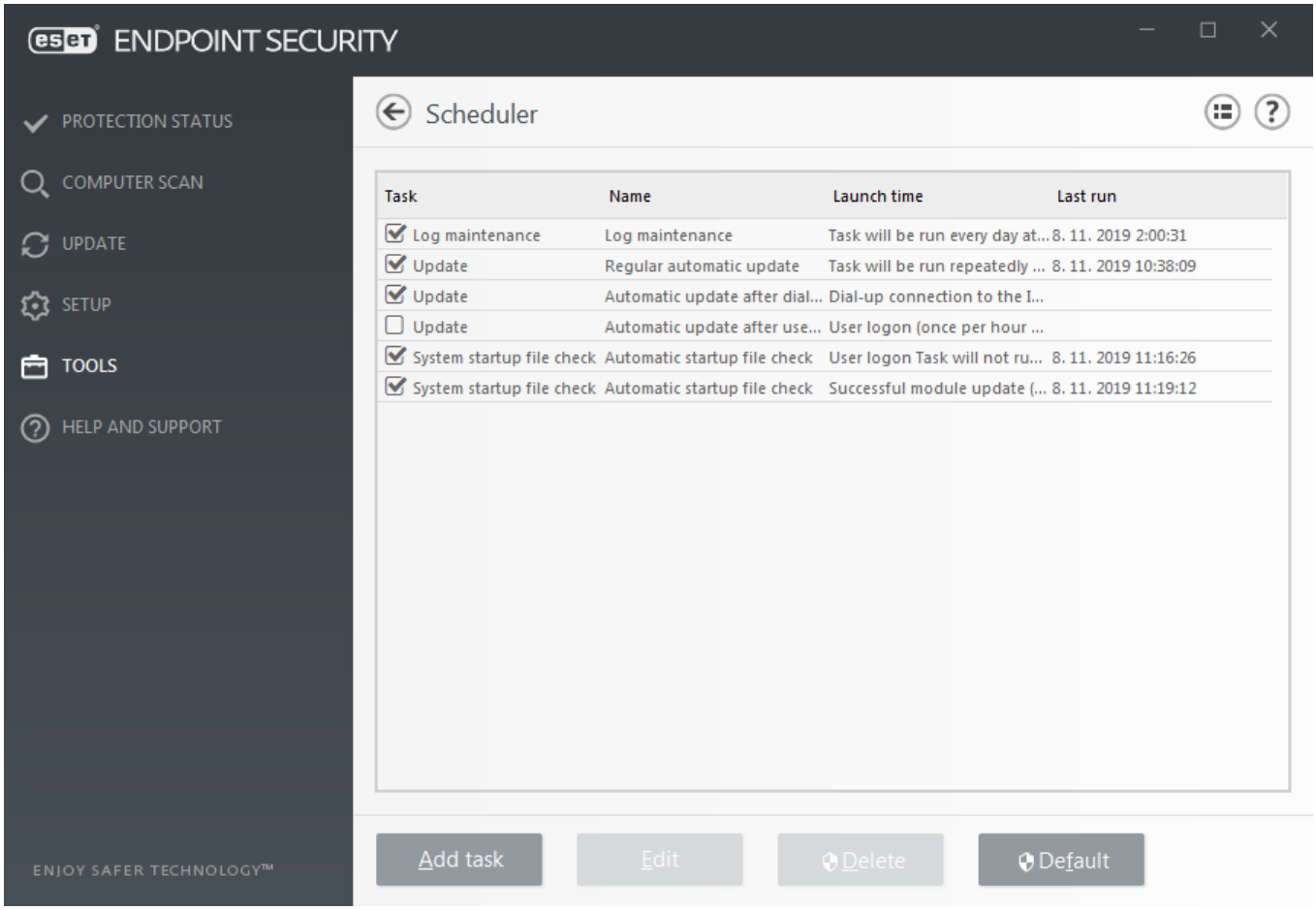
The Scheduler can be accessed from the ESET Endpoint Security main program window by clicking **Tools** > **Scheduler**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time and scanning profile used.

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)

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 wish to modify and click the **Edit** button.



Add a new task

1. Click **Add task** at the bottom of the window.
2. Enter a 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 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 the detection engine and program modules.

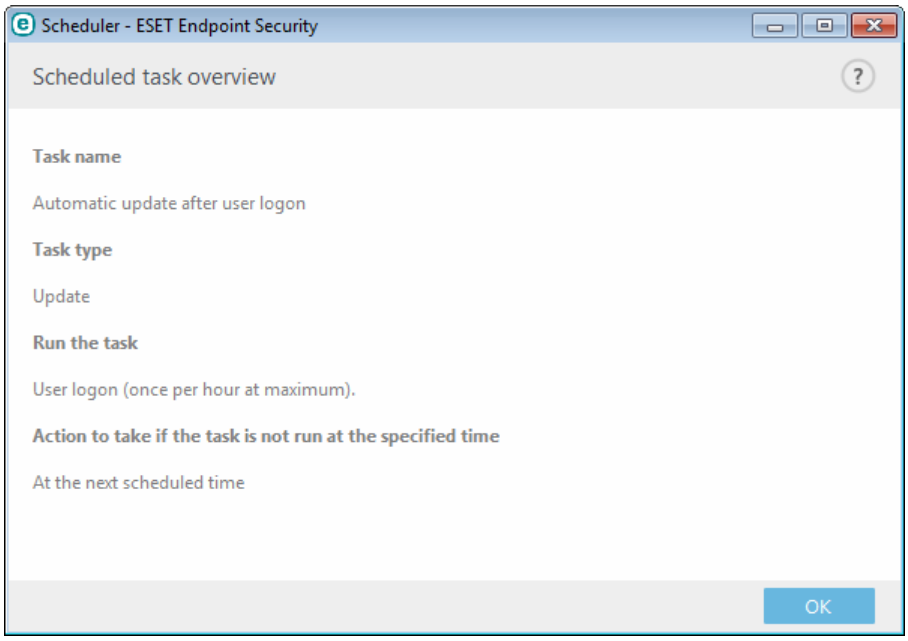
4. Turn on the **Enabled** switch if you want to activate the task (you can do this later by selecting/deselecting check box in the list of scheduled tasks), click **Next** and select one of the timing options:

- **Once** – The task will be performed at the predefined 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 predefined 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)

You can review scheduled task when right click and click **Show task details**.



Protection statistics

To view a graph of statistical data related to ESET Endpoint Security's protection modules, click **Tools** > **Protection statistics**. Select the applicable protection module from the **Statistics** drop-down menu to see the corresponding graph and legend. If you mouse over an item in the legend, only the data for that item will display in the graph.

A new type of reporting has been introduced from ESET Endpoint Security version 7.1 - Security report. The Protection statistics section will no longer be available.

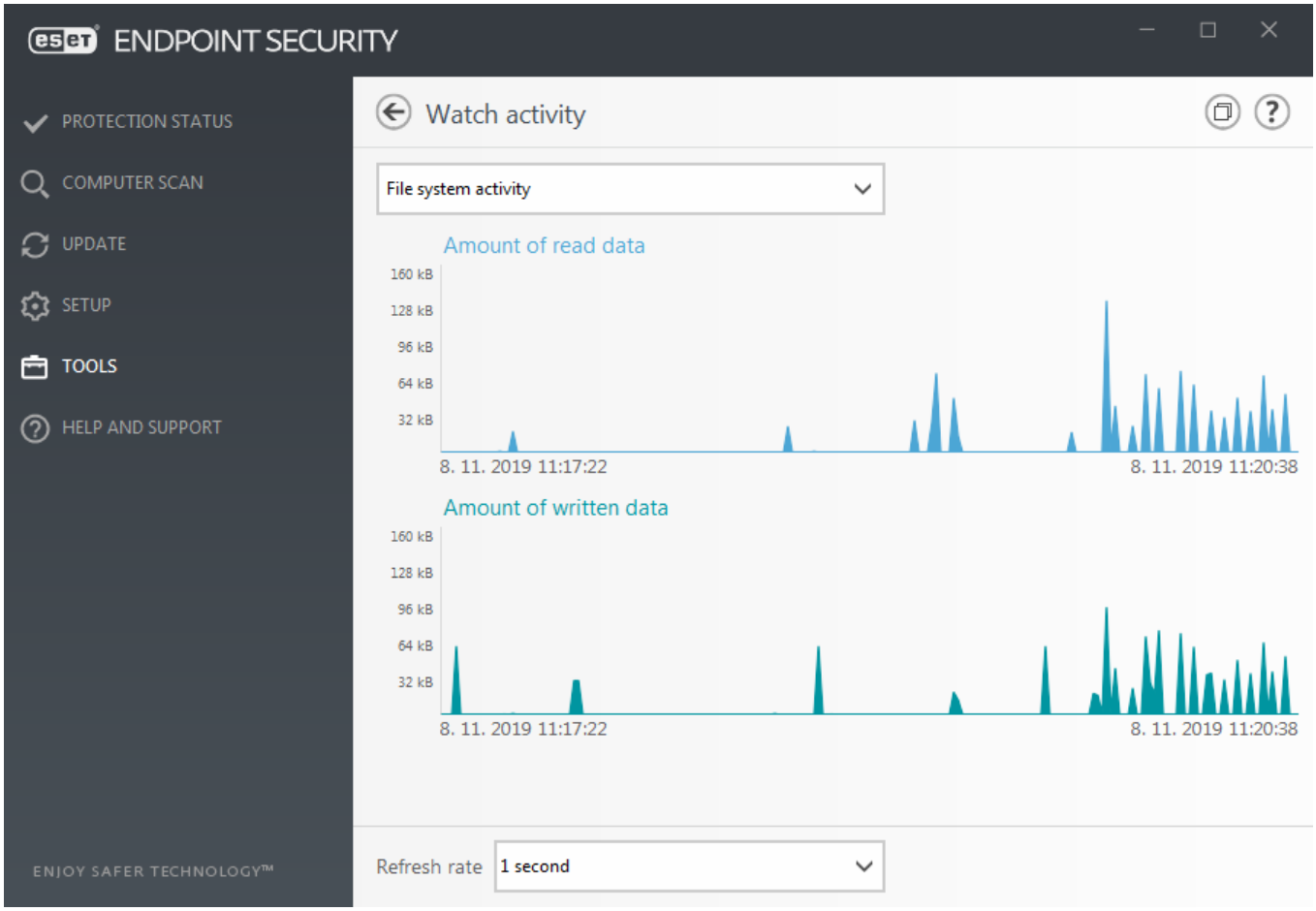
The following statistic graphs are available:

- **Antivirus and Antispyware protection** – Displays the number of infected and cleaned objects.
- **File system protection** – Only displays objects that were read or written to the file system.
- **Email client protection** – Only displays objects that were sent or received by email clients.
- **Web access and Anti-Phishing protection** – Only displays objects downloaded by web browsers.
- **Email client antispam protection** – Displays the history of antispam statistics since the last startup.

Next to the statistics graphs, you can see the number of all scanned objects, number of infected objects, number of cleaned objects and the number of clean objects. Click **Reset** to clear statistics information or click **Reset all** to clear and remove all the existing data.

Watch activity

To see the current **File system activity** in graph form, click **Tools** > **Watch activity**. At the bottom of the graph is a timeline that records file system activity in real-time based on the selected time span. To change the time span, select from **Refresh rate** drop-down menu.



The following options are available:

- **Step: 1 second** – The graph refreshes every second and the timeline covers the last 10 minutes.
- **Step: 1 minute (last 24 hours)** – The graph is refreshed every minute and the timeline covers the last 24 hours.
- **Step: 1 hour (last month)** – The graph is refreshed every hour and the timeline covers the last month.
- **Step: 1 hour (selected month)** – The graph is refreshed every hour and the timeline covers the last X selected months.

The vertical axis of the **File system activity graph** represents the amount of read data (blue color) and the amount of written data (turquoise color). Both values are given in kB (kilobytes)/MB/GB. If you mouse over either read data or written data in the legend below the graph, the graph will only display data for that activity type.

You can also select **Network activity** from the drop-down menu. The graph display and options for **File system activity** and **Network activity** are the same except that the latter displays the amount of received data (blue color) and amount of sent data (turquoise color).

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 assesses the risk level of each component. This information can help determine the cause of suspicious system behavior that may be due to software or hardware incompatibility or malware infection. See also Online

user guide for ESET SysInspector.

The SysInspector window displays the following information about created 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 created log. You can also right-click a given log file and select **Show** from the context menu.
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as **Created**) before attempting to access the log.
- **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).
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as **Created**) before attempting to access the log.
- **Delete** – Deletes selected log.
- **Delete all** – Deletes all logs.
- **Export...** – Exports the log to an .xml file or zipped .xml.

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 from the wild, ESET LiveGrid® enables us to react immediately to needs of our customers and keep ESET responsive to the latest threats.

There are three options:

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 particular 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.

> **Related information**
> 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, press **F5** to enter Advanced setup and expand **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.

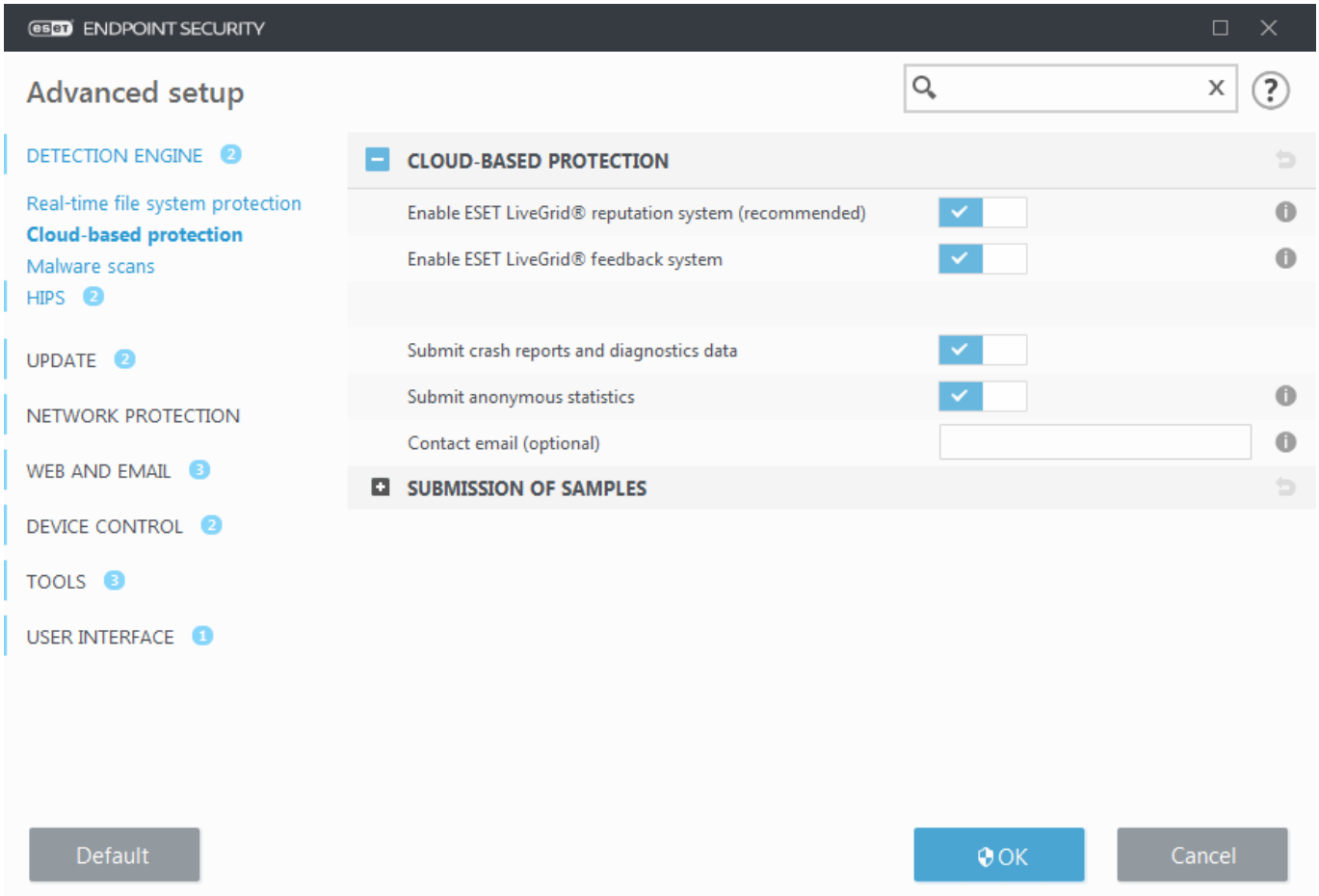
Enable ESET LiveGrid® feedback system – Sends relevant submission data (described in the **Submission of samples section** below) along with crash reports and statistics to the ESET Research lab for further analysis.

Enable ESET Dynamic Threat Defense (not visible in ESET Endpoint Security) – ESET Dynamic Threat Defense is a paid service provided by ESET. Its purpose is to add a layer of protection specifically designed to mitigate threats that are new in the wild. 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. Please note that you will not receive a response from ESET unless more information is needed.



Submission of samples

Manual submission of samples – Enables the option to manually submit samples to ESET from the context menu, Quarantine or Tools > Submit sample for analysis.

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 in case 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 allows 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.

ESET Dynamic Threat Defense

To enable ESET Dynamic Threat Defense service on a client machine using ESMC Web Console, see EDTD 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.

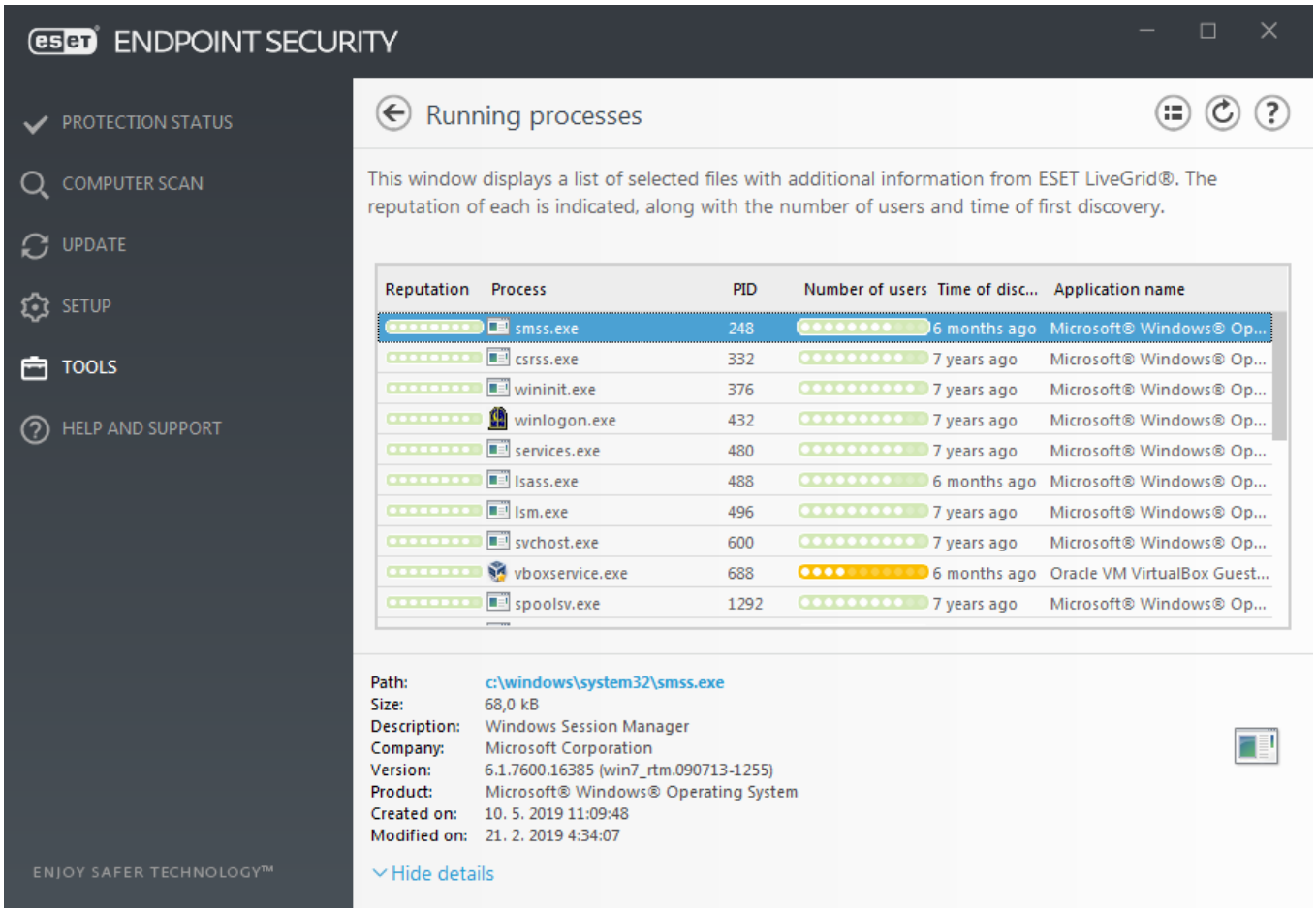
Exclusion filter for Cloud-based protection

The Exclusion filter allows 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.

> **Note**
> This feature is useful to exclude files that may carry confidential information, such as documents or spreadsheets.

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.

> **Note**
> 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.

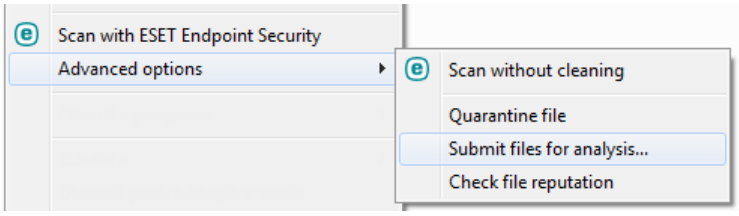
> **Note**
> When an application is marked as Unknown (orange) security level, it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, use the submit file for analysis feature to send the file to the ESET Virus Lab. If the file turns out to 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.
- **Size** – File size either in kB (kilobytes) or MB (megabytes).
- **Description** – File characteristics based on the description from the operating system.
- **Company** – Name of the vendor or application process.
- **Version** – Information from the application publisher.
- **Product** – Application name and/or business name.
- **Created on** – Date and time when an application was created.
- **Modified on** – Last date and time when an application was modified.

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



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.

Web pages in Web control blocked – 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 checked – 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.

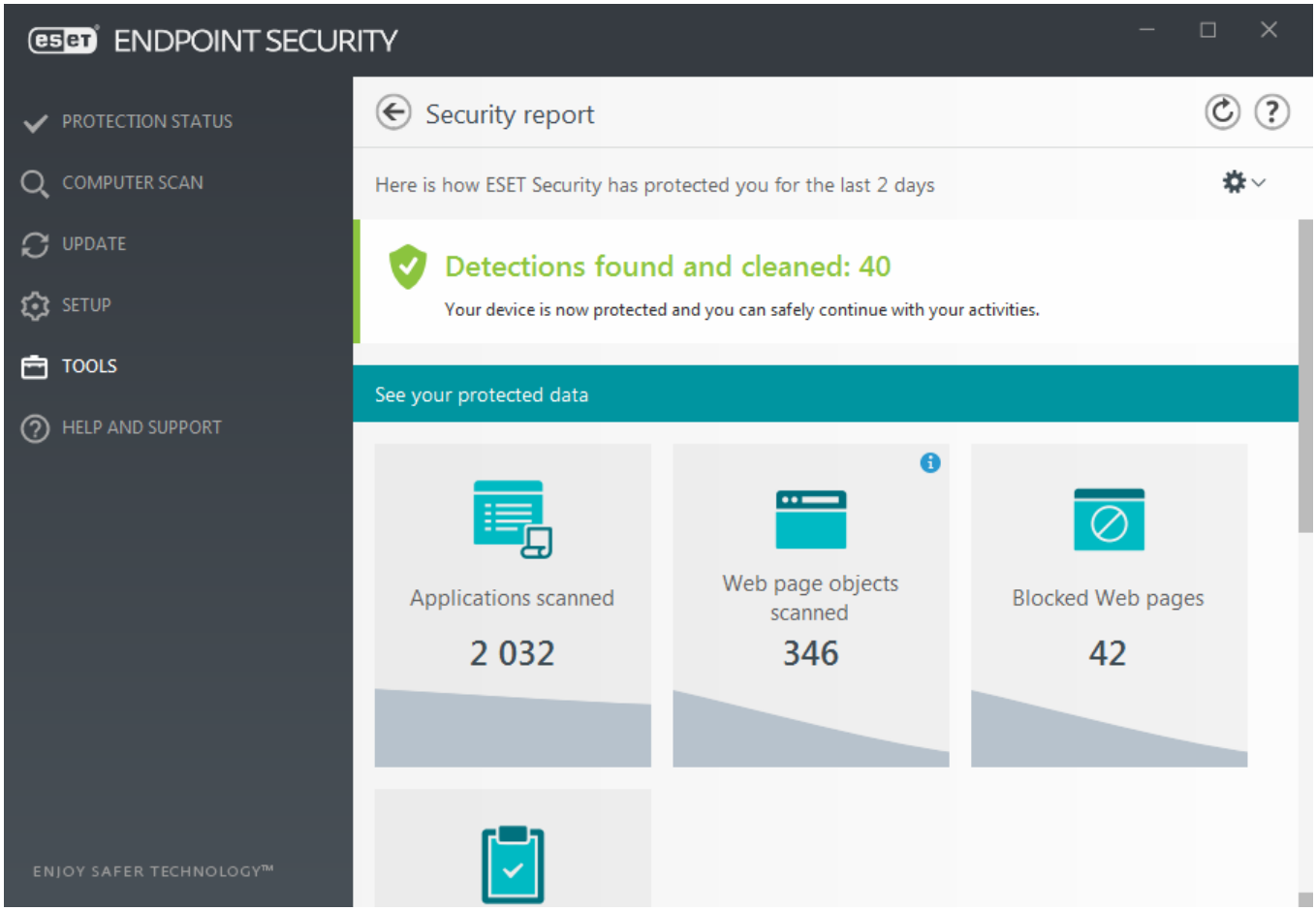
Web page objects scanned – Displays the number of scanned web page objects.

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.

Below the categories, you can see the actual virus situation with the map of the world. The presence of virus in each country is indicated with color (the darker the color, the higher the number). Countries without data are grayed. Hover mouse over the country displays data for the selected country. You can select the specific continent and it will be automatically zoomed.

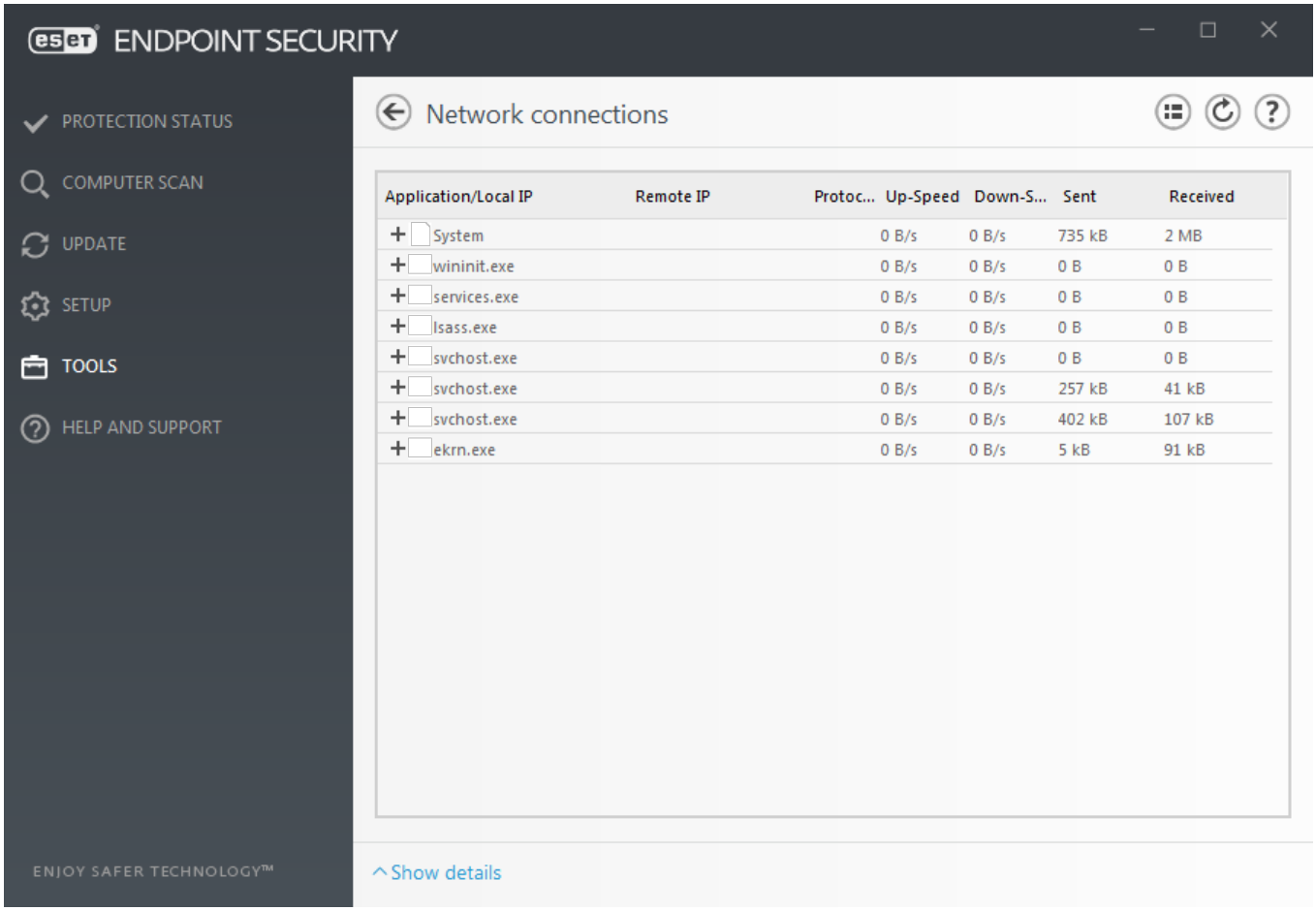
Click the gear wheel in the upper right corner you can **Enable/Disable Security report notifications** or select whether the data will be displayed for the last 30 days or since the product was activated. If ESET Endpoint Security is installed less than 30 days, then only the number of days from installation 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** > **User interface** > **Alerts and message boxes** > **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.



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 particular 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.

Select an application or IP address in the Network connections screen and right-click on it will show 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 on 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 predefined rule. A description of the settings can be found in the Rules and zones section.

Temporarily allow communication for the process – Permits current connections for the given application. If a new connection is established, the firewall uses a predefined rule. A description of the settings can be found in the Rules and zones section.

ESET SysRescue Live

ESET SysRescue Live is a free utility that allows you to create a bootable rescue CD/DVD or USB drive. You can boot an infected computer from your rescue media, and then scan for malware and clean infected files.

The main advantage of ESET SysRescue Live is the fact that it runs independent of the host operating system, but has direct access to the disk and file system. This makes it possible to remove threats that under normal operating conditions might be impossible to delete (for example, when the operating system is running, etc.).

- Online Help for ESET SysRescue Live

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®).

Before submitting samples to ESET

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, please refer to 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 may not get a response from ESET**
> 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 – Enter a description of the suspicious file behavior observed on your computer.

File origin (URL address or vendor) – Please enter the file origin (source) and how you encountered this file.

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

> **Note**
> 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

Please select 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 enter 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) – Please enter 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.

> **Note**
> 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. Please 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 file.

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 – Please enter a detailed description and the reason for sending the file.

Notifications

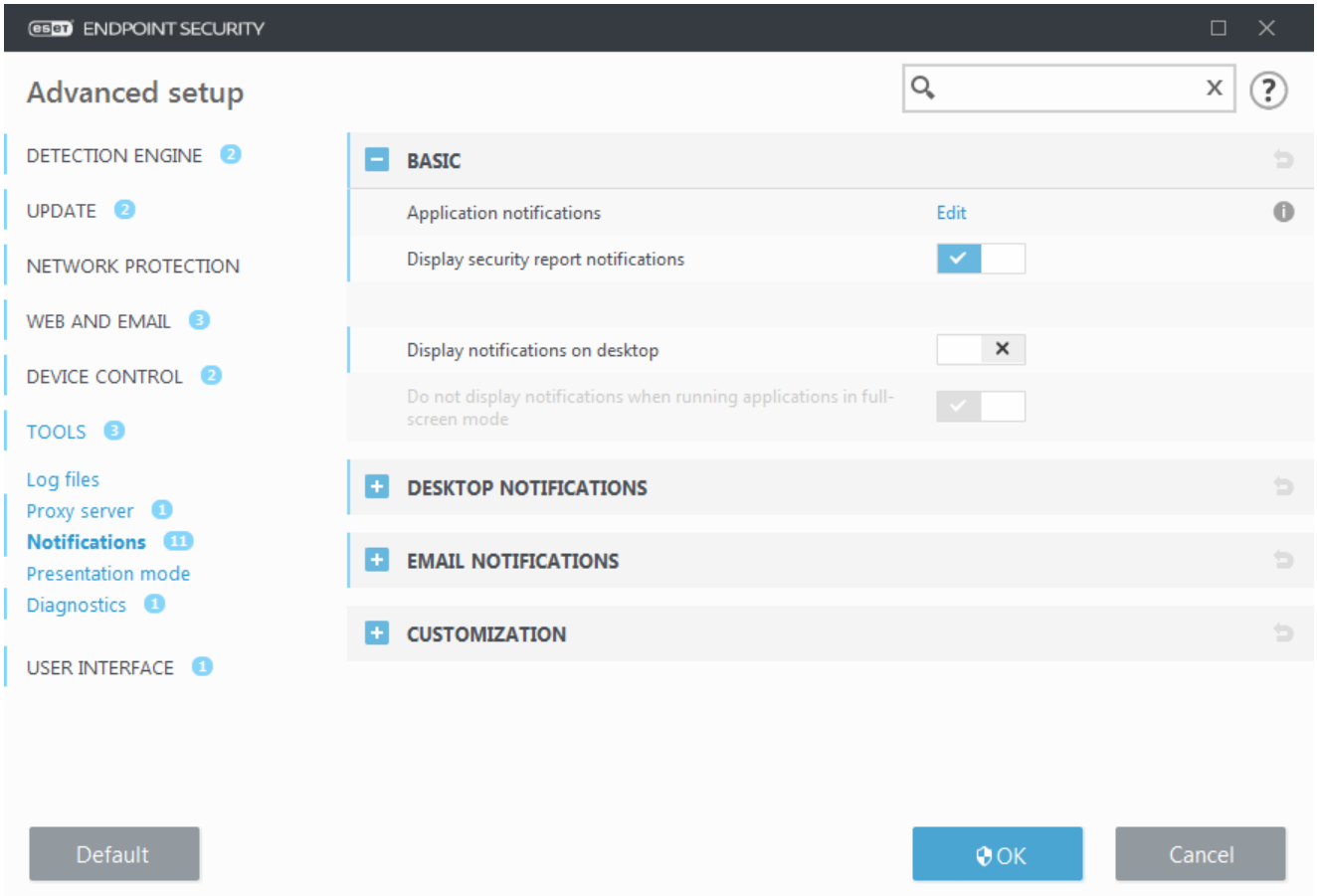
To manage the way how ESET Endpoint Security communicates events with the user, navigate to **Advanced setup (F5)** > **Tools** > **Notifications**. This configuration window allows you to set the following types of notifications:

- Application notifications – Shows directly in the main program window.
- Desktop notifications – A desktop notification shown as a small pop-up window next to system taskbar.
- Email notifications – Email notifications are sent to the specified email address.
- Customization of notifications – Add custom message to e.g. a desktop notification.

In the **Basic** section, use the corresponding switches to adjust the following:

Switch	Default	Description
Display notifications on desktop	✓	Disable to hide pop-up notifications next to system taskbar. We recommend keeping this option enabled so the product could inform you when a new event occurs.
Do not display notifications when...	✓	Keep **Do not display notifications when running applications in full-screen mode** enabled to suppress all non-interactive notifications.
Display Security report notifications	×	Enable to receive a notification when a new version of Security report is generated (available only if not managed by ESET Security Management Center).
Display notification about successful update	×	Enable to receive a notification when product updates its components and Detection engine modules.
Send event notification by email	×	Enable to activate Email notifications.

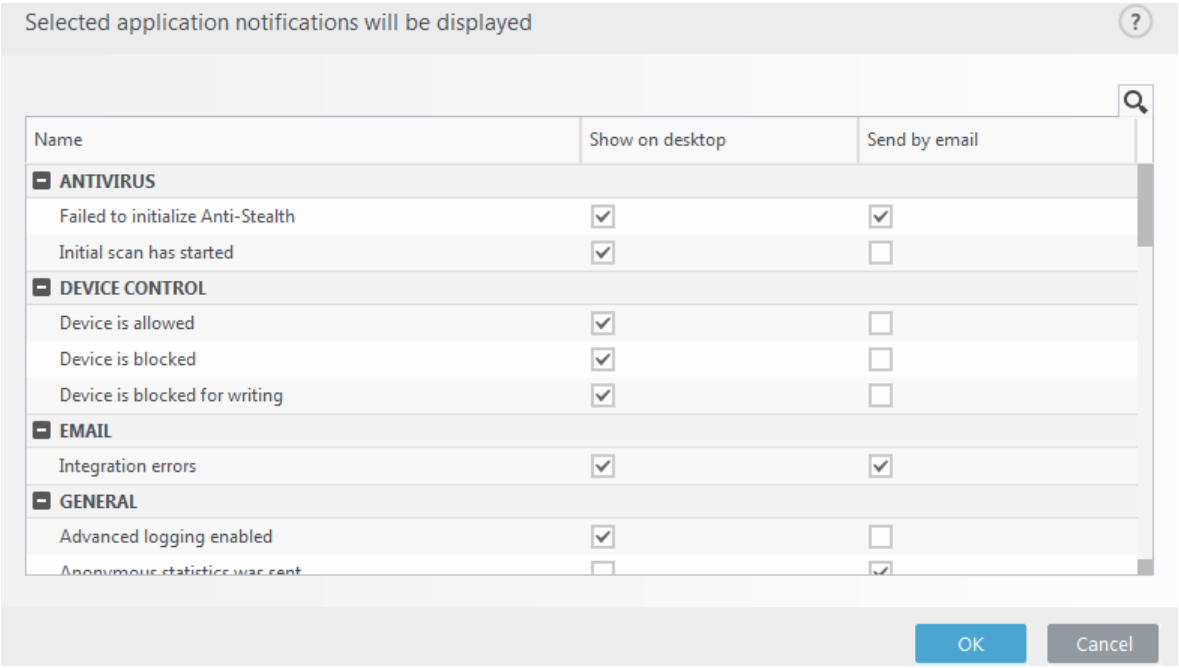
To enable or disable specific Application notifications, click **Edit** next to **Application notifications**.



Application notifications

To adjust the visibility of application notifications (displayed at the bottom right of the screen) navigate to **Tools** > **Notifications** > **Basic** > **Application notifications** of the ESET Endpoint Security Advanced setup tree.

List of notifications is divided into three columns. Notifications names are sorted by categories in the first column. To change the way, how the product notifies about new application events, select the checkboxes in corresponding columns **Show on desktop** and **Send by email**.



To set general settings for Desktop notifications, for example, how long will be a message displayed or minimum verbosity of events to display, see Desktop notifications in **Advanced setup** > **Tools** > **Notifications**.

To set email message format and to configure SMTP server settings, see Email notifications in **Advanced setup** > **Tools** > **Notifications**.

> **Notifications after submitting files for analysis**
> If you want to set-up notifications **File analyzed** and **File not analyzed** while using ESET Dynamic Threat Defense, Proactive protection must be set to **Block execution until receiving the analysis result**.

Desktop notifications

Desktop notification is represented by small pop-up 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.

Desktop notifications section allows to customize the behavior of pop-up notifications. The following attributes can be set:

Duration – Sets the duration of how long the notification message is visible. The value must be in the range of 3 to 30 seconds.

Transparency – Sets the transparency of notification message in percents. The supported range is 0 (no transparency) to 80 (very high transparency).

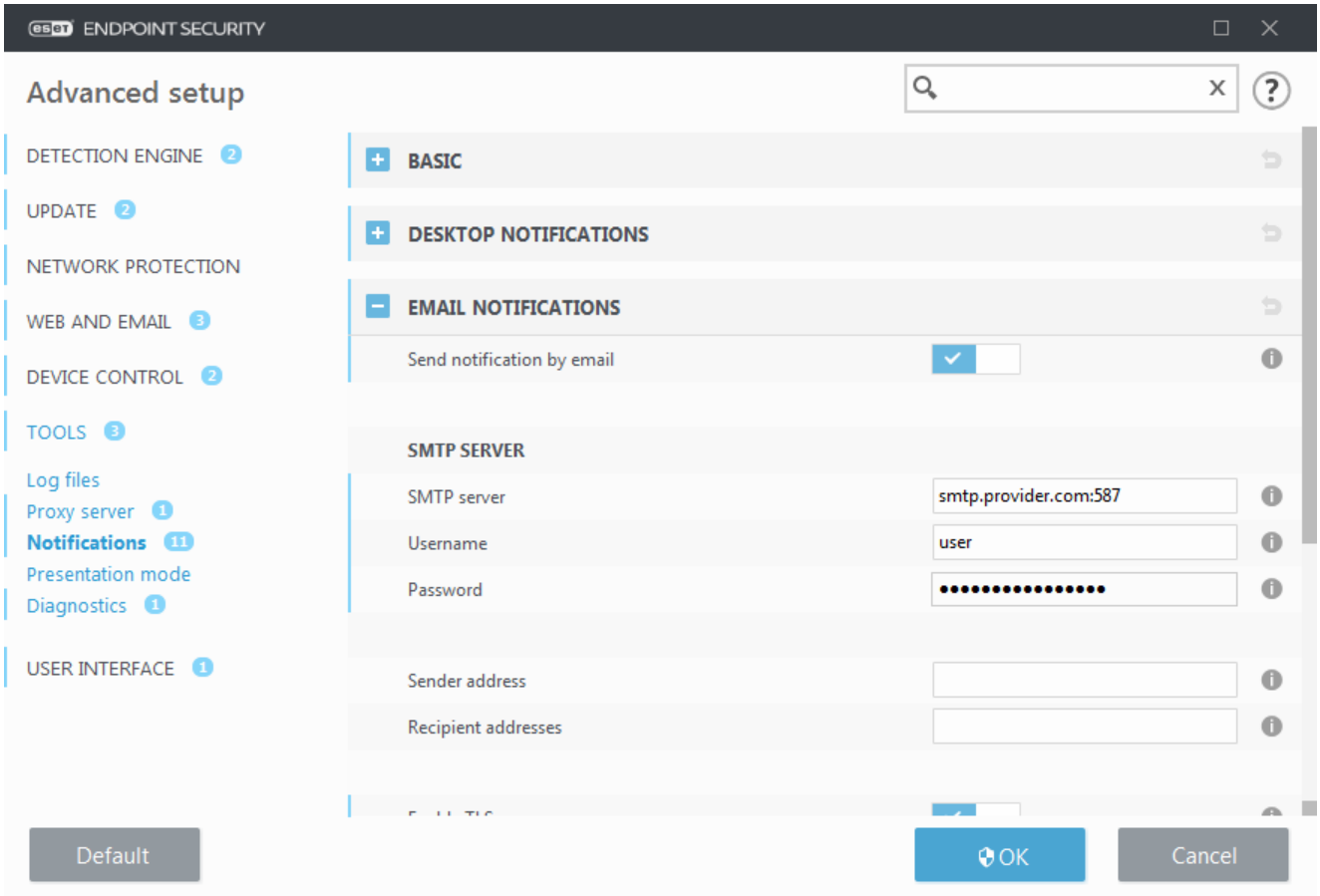
Minimum verbosity of events to display – From the drop-down menu, you can select the starting severity level of notifications to be displayed:

- **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 (Antistealth is not running properly or 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 – Type in the full account names of users that should be allowed to receive desktop notifications. For example, if you use your computer using other than Administrator account and you want to keep being informed about new product events.

Email notifications

ESET Endpoint Security can automatically send notification emails if an event with the selected verbosity level occurs. In the Basic section, enable **Send event notifications by email** to activate email notifications.



SMTP server

SMTP server – The SMTP server used for sending notifications (e.g. *smtp.provider.com:587*, predefined port is 25).

> **Note**
> 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.

Email settings

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 (Antistealth is not running properly or 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.

Send each notification in a separate email – When enabled, the recipient will receive a new email for each individual notification. This may result in large number of emails being received in a short period of time.

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.

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 predefined 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 upon 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.

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.

Threats

Enable **Do not close malware notifications automatically** to have malware notifications stay on screen until they are closed manually.

Disable **Use default message** and enter your own message in the **Threat notification message** field to use customized notification messaging.

Quarantine

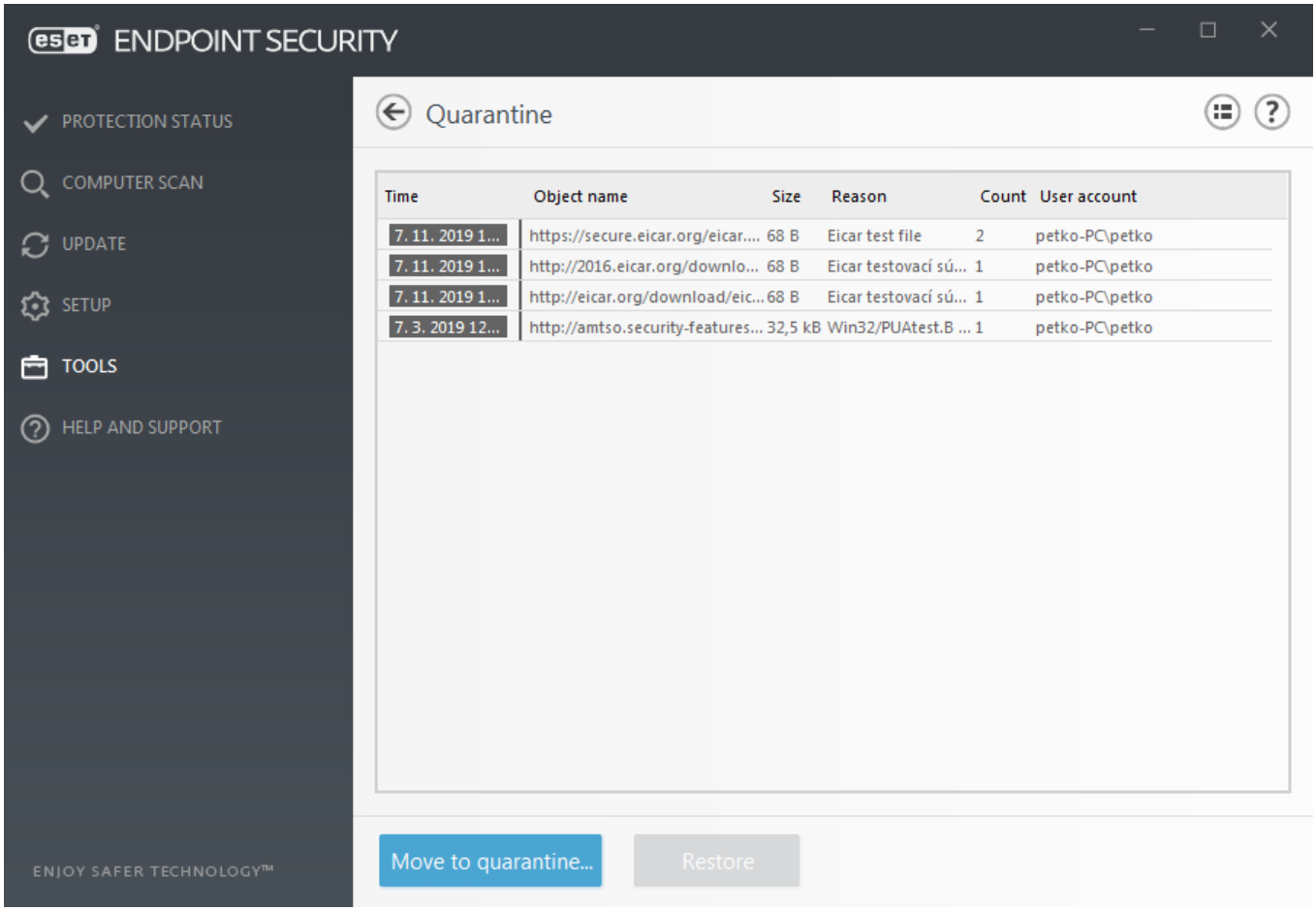
The main function of the quarantine is to safely store reported objects (such as malware, infected files or potentially unwanted applications).

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:

a.cannot be cleaned,

b.if it is not safe or advisable to delete them,

c.if they are falsely detected by ESET Endpoint Security,

d.or if a file behaves suspiciously but is not detected by the scanner.

To quarantine a file, you have multiple options:

a.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.

b.Click **Move to quarantine...** from the main program window.

c.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, which allows you 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 on 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.

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, please 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.

> **Illustrated instructions**
> The following ESET Knowledgebase article may only be available in English:
> - Manage the Quarantine in ESMC (7.x)
> - My ESET product notified me of a detection—what should I do?

Proxy server setup

In large LAN networks, communication between your computer and the internet can be mediated by a proxy server. Using this configuration, the following settings need to be defined. Otherwise the program will not be able to update itself automatically. In ESET Endpoint Security, proxy server setup is available from two different sections of the Advanced setup tree.

First, proxy server settings can be configured in **Advanced setup** under **Tools** > **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 proxy server settings for this level, select **Use proxy server** and enter the address of the proxy server into the **Proxy server** field along with the **Port** number of the proxy server.

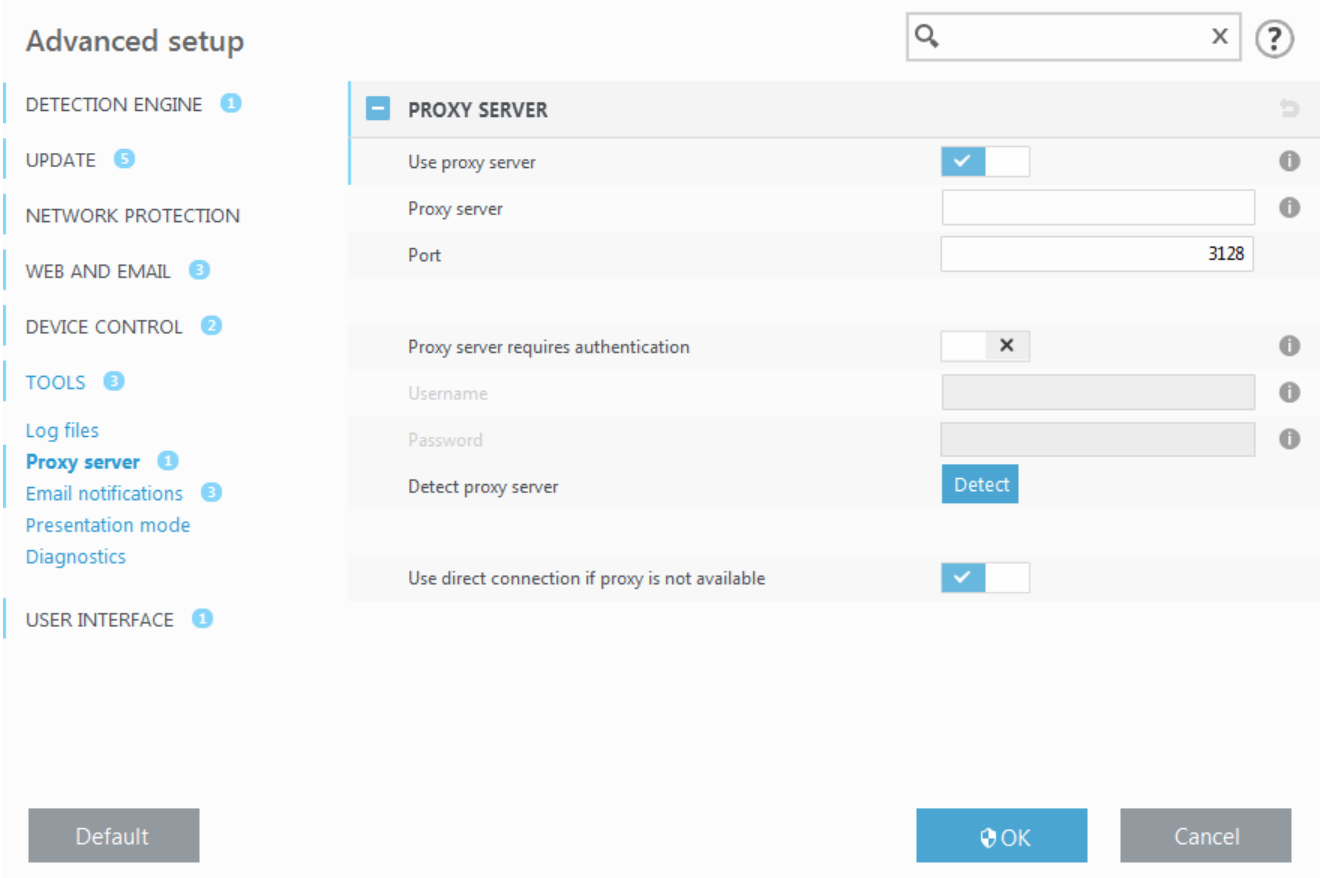
If communication with the proxy server requires authentication, select **Proxy server requires authentication** and enter a valid **Username** and **Password** into the respective fields. Click **Detect proxy server** to automatically detect

and populate proxy server settings. The parameters specified in Internet options for Internet Explorer or Google Chrome will be copied.

> **Note**
> You must manually enter your Username and Password in **Proxy server** settings.

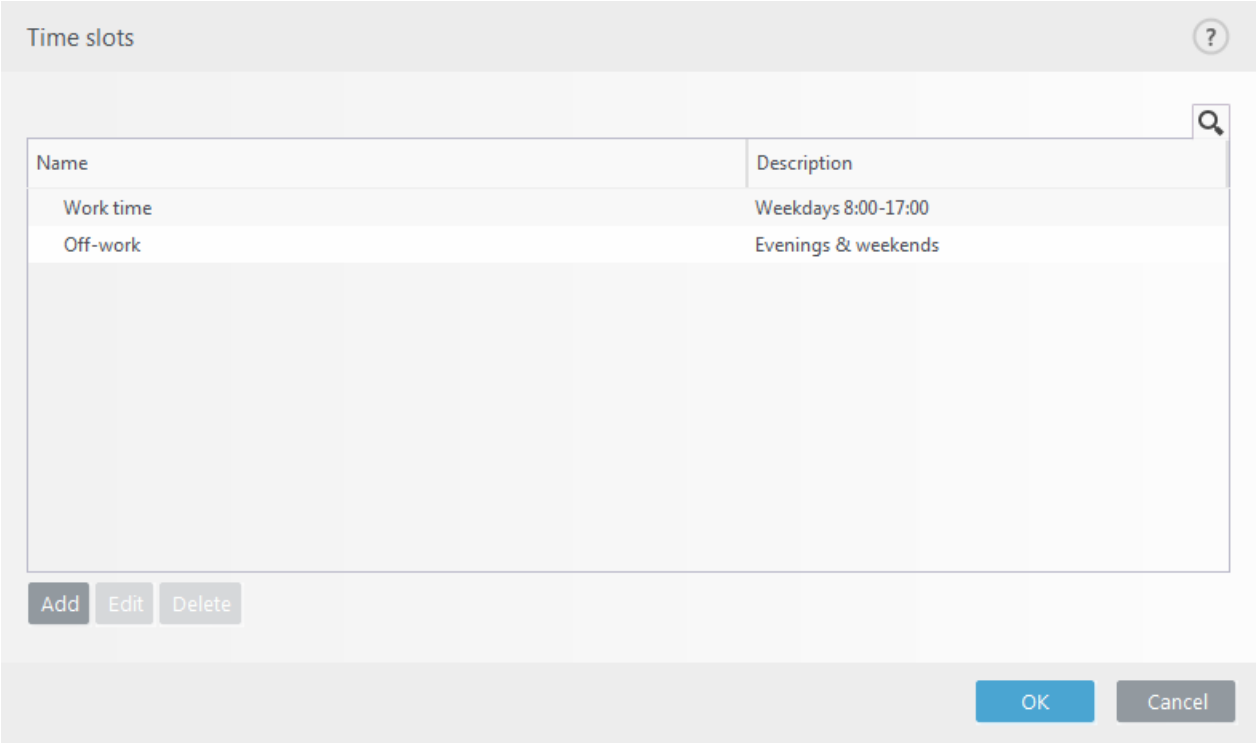
Use direct connection if proxy is not available – If ESET Endpoint Security is configured to connect via proxy and the proxy is unreachable, ESET Endpoint Security will bypass the proxy and communicate directly with ESET servers.

Proxy server settings can also be established from Advanced update setup (**Advanced setup** > **Update** > **Profiles** > **Updates** > **Connection options** by selecting **Connection through a proxy server** from the **Proxy mode** drop-down menu). This setting applies for the given update profile and is recommended for laptops that often receive detection engine updates from remote locations. For more information about this setting, see Advanced update setup.



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 lets you 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.

License interval check

ESET Endpoint Security needs to connect to the ESET servers automatically. To change this setting, navigate to **Advanced setup (F5)** > **Tools** > **License**. By default, **Interval check** is set to **Automatic**, and ESET License server checks the product a few times every hour. In case of an increased network traffic change settings to **Limited** to decrease overload. When **Limited** is selected, ESET Endpoint Security checks the license server only once a day, or when the computer restarts.

> **Important**
> If **Interval check** setting is set to **Limited**, all license-related changes done via ESET Business Account /ESET MSP Administrator may take up to one day to apply to the ESET Endpoint Security settings.

User interface

The **User interface** section allows you to configure the behavior of the program's Graphical user interface (GUI).

Using the User Interface elements tool, you can adjust the program's visual appearance and effects used.

To provide maximum security of your security software, you can prevent any unauthorized changes using the Access setup tool.

By configuring Alerts and message boxes and Notifications, you can change the behavior of detection alerts and system notifications. These can be customized to fit your needs.

If you choose not to display some notifications, they will be displayed in **User interface elements** > **Application statuses**. Here you can check their status or alternatively prevent to display these notifications.

The Context menu integration is displayed after right-clicking on the selected object. Use this tool to integrate the ESET Endpoint Security control elements into the context menu.

Presentation mode is useful for users, who want to work with an application and not be interrupted by pop-up windows, 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 allow you to adjust the working environment to fit your needs. These configuration options are accessible in the **User interface** > **User interface elements** branch of the ESET Endpoint Security Advanced setup tree.

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.

> **Note**
> Once 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 Security Management Center using a policy.

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.

Statuses

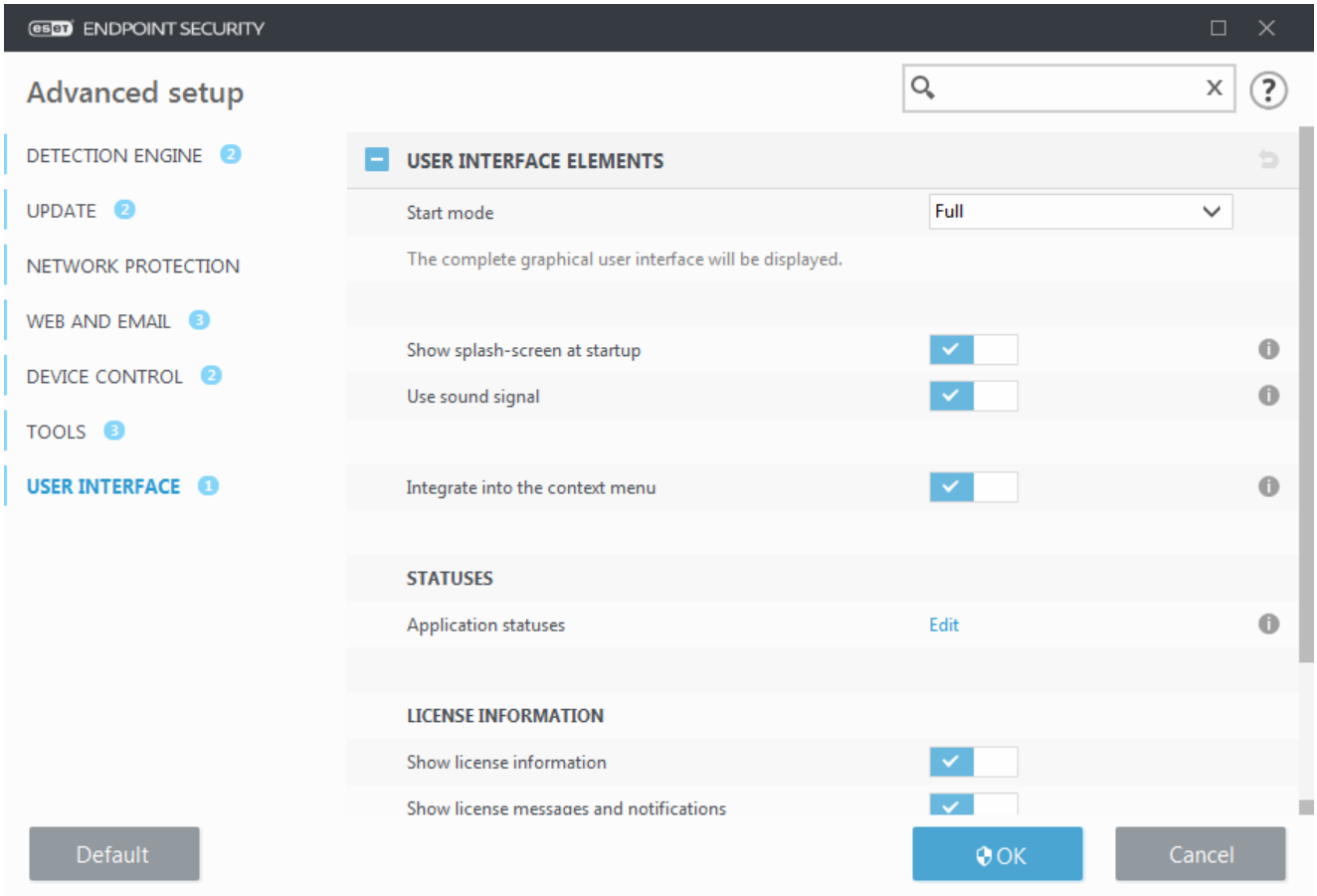
Application statuses – Click **Edit** button to manage (disable) statuses that are displayed in the **Protection status** pane in main menu.

License information

Show license information – When disabled, the license expiration date on **Protection status** and **Help and support** screen will not be displayed.

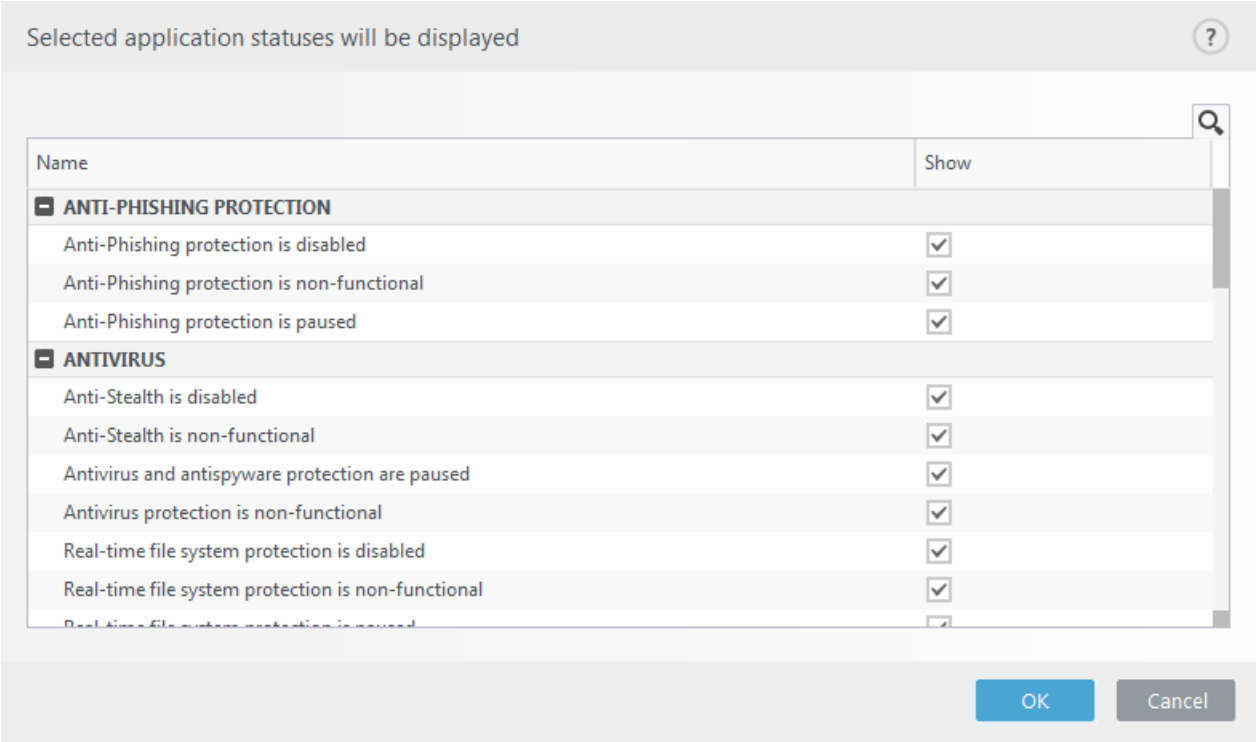
Show license messages and notifications – When disabled, the notifications and messages will only be displayed when the license expired.

> **MSP licenses**
> License information settings are applied but not accessible for ESET Endpoint Security activated with an MSP license.



Application statuses

To adjust in-product statuses in the first pane of ESET Endpoint Security navigate to **User interface** > **User interface elements** > **Application statuses** of the ESET Endpoint Security Advanced setup tree.



Enable or disable which application statuses will be or will not be displayed. For example, when you pause

antivirus and antispyware protection or when you enable presentation mode. An application status will also be displayed if your product is not activated or if you license has expired. This setting can be changed via ESET Security Management Center policies.

Access setup

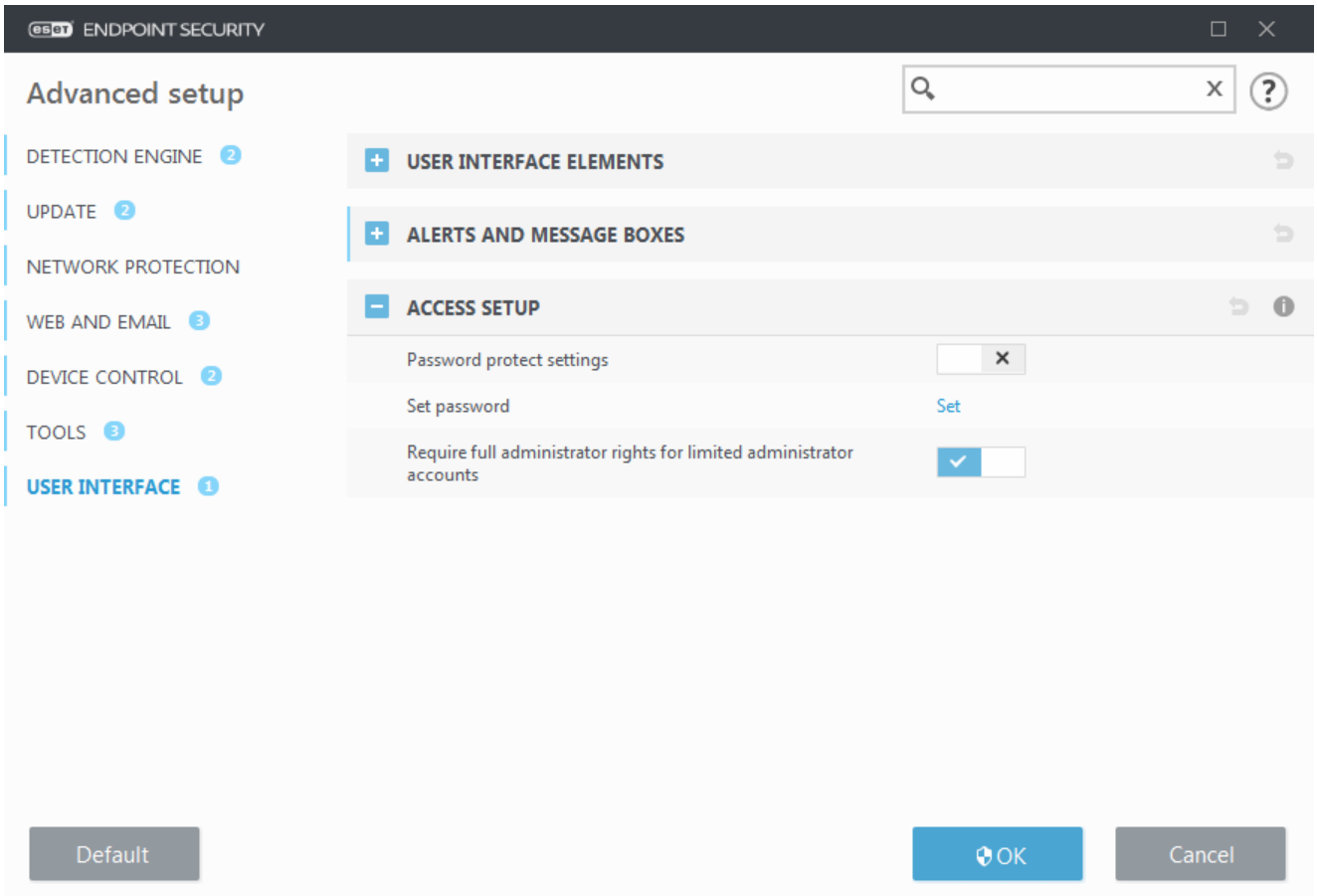
In order to provide maximum security for your system, it is essential that ESET Endpoint Security is correctly configured. Any unqualified change may result in a loss of important data. To avoid unauthorized modifications, the setup parameters of ESET Endpoint Security can be password protected.

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

Configuration settings for password protection are located in **Advanced setup** (F5) under **User interface** > **Access setup**.



Password protect settings – Indicate password settings. Click to open the Password setup window.

To set or change a password to protect setup parameters, click **Set**.

Require full administrator rights for limited administrator accounts – Leave this option active to prompt the current user (if he or she does not have administrator rights) to enter the administrator username and password

when modifying certain system parameters (similar to the UAC in Windows Vista). The modifications include disabling protection modules or turning off the firewall.

For Windows XP only:

Require administrator rights (system without UAC support) – Enable this option to have ESET Endpoint Security prompt for administrator credentials.

Password for Advanced setup

To protect the setup paramaters of ESET Endpoint Security in order to avoid unauthorized modification, a new password must be set.

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. Enter 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 forget your password, access to advanced settings can be restored.

- Restore by using the "Restore password" method (version 7.1 and above)
- Restore by using the ESET Unlock Tool (version 7.0 and below)

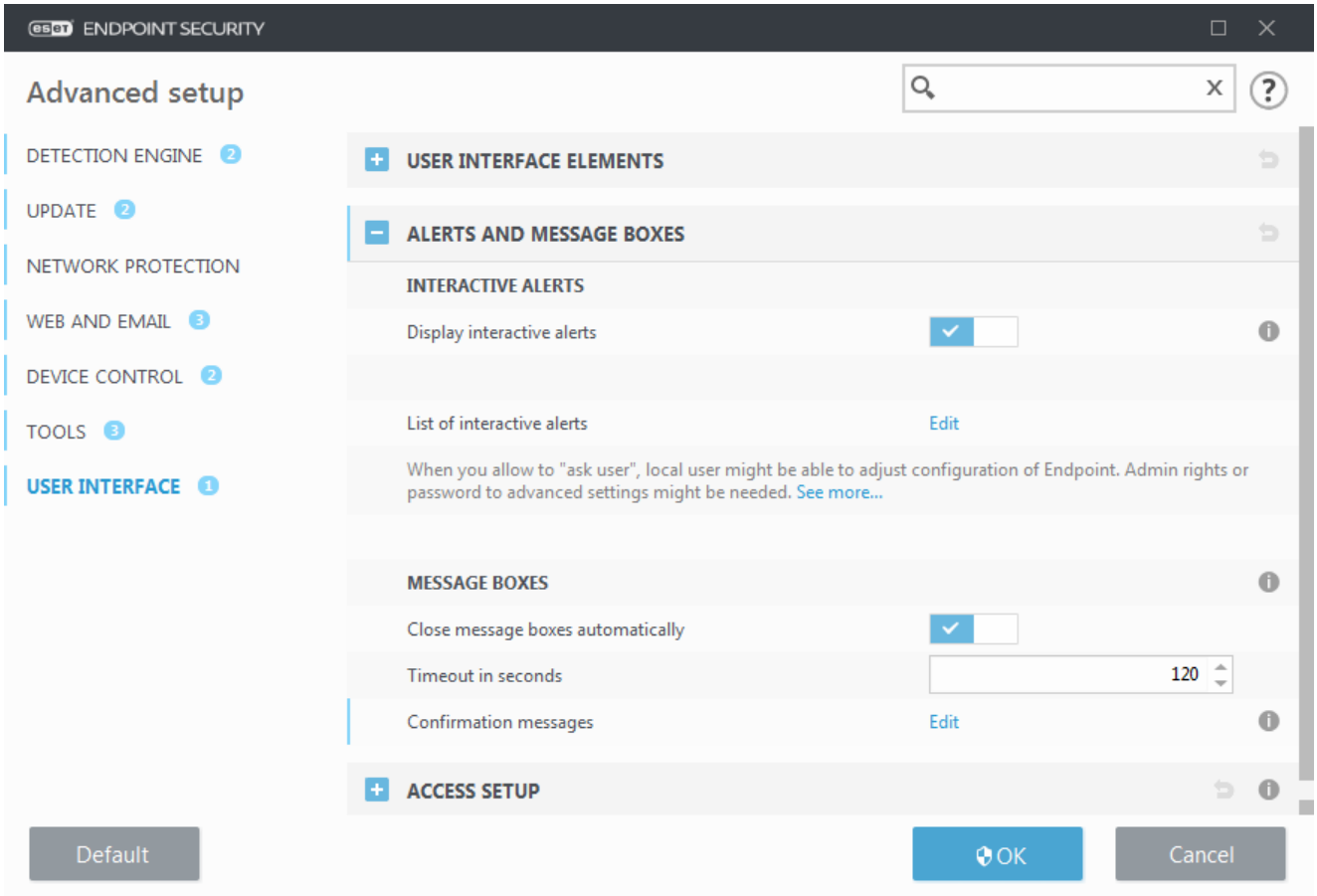
Click here if you forgot your ESET-issued License Key, expiration date of your license, or other license information for ESET Endpoint Security.

Alerts and message boxes

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

The **Alerts and message boxes** (formerly **Alerts and notifications**) section under **User interface** allows you to configure how detections, where a decision is needed to be made by a user (for example, potential phishing websites) are handled by ESET Endpoint Security.



Interactive alerts

Interactive alert windows are displayed if a detection is found, or if user intervention is required.

Display interactive alerts

ESET Endpoint Security version 7.2 and later:

- For unmanaged users, we recommend that this option be 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.

Disabling **Display interactive alerts** will hide all alert windows and in-browser dialogs. A pre-defined default action will be automatically selected (for example, "potential phishing website" will be blocked).

ESET Endpoint Security version 7.1 and below:

The name of this setting is **Display alerts**, and it is not possible to customize pre-defined actions for specific interactive alert windows.

Desktop notifications

Notifications on the Desktop and balloon tips are informative only, and do not require user interaction. The **Desktop notifications** section was moved under **Tools** > **Notifications** in Advanced setup (version 7.1 and later).

Message boxes

To close pop-up windows automatically after a certain period of time, select **Close message boxes automatically**. If they are not closed manually, alert windows are automatically closed after the specified time period elapses.

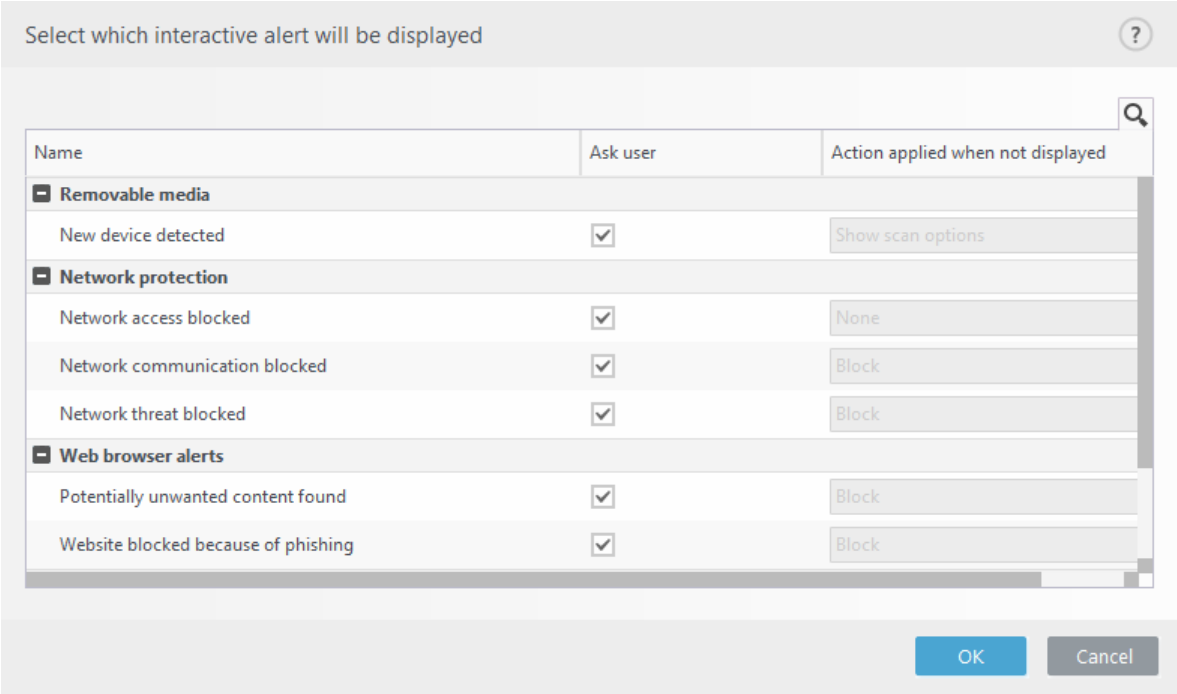
Confirmation messages – Shows you a list of confirmation messages that you can select to display or not to display.

Interactive alerts

This section outlines several interactive alert windows that ESET Endpoint Security will display before any action is performed.

To adjust behavior for configurable interactive alerts, navigate to **User interface** > **Alerts and message boxes** > **List of interactive alerts** of the ESET Endpoint Security Advanced setup tree and click **Edit**.

> **Purpose**
> 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.
> Also see in-product application statuses.



Check other help sections for reference to a specific interactive alert window:

Removable media

- New device detected

Network protection

- Network access blocked is displayed when the **Isolate computer from network** client task of this workstation from ESMC is triggered.
- Network communication blocked
- Network threat blocked

Web browser alerts

- Potentially unwanted content found
- Website blocked because of phishing

Computer

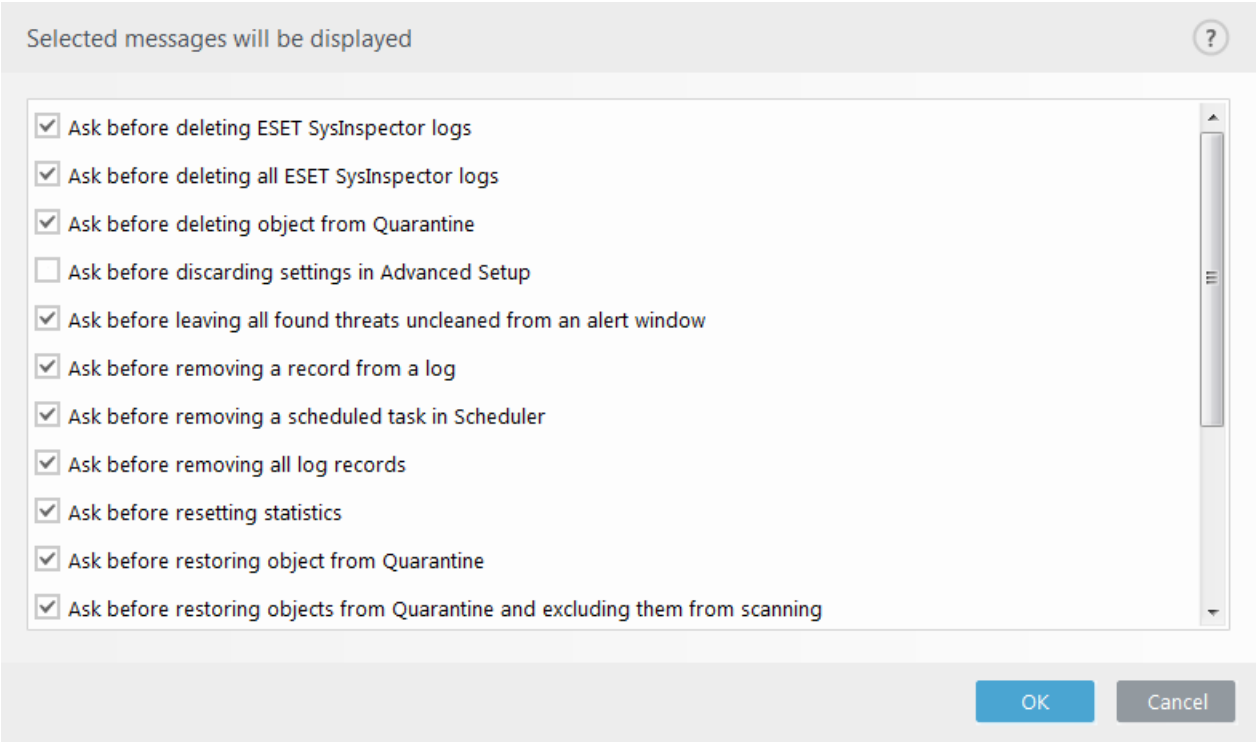
Presence of these alerts will change the user interface to orange:

- Restart computer (required)
- Restart computer (recommended)

> **Limitations**
> Interactive alerts do not contain Detection engine, HIPS or Firewall interactive windows - as their behavior can be configured individually in the specific feature.

Confirmation messages

To adjust confirmation messages, navigate to **User interface** > **Alerts and message boxes** > **Confirmation messages** of the ESET Endpoint Security Advanced setup tree and click **Edit**.



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.

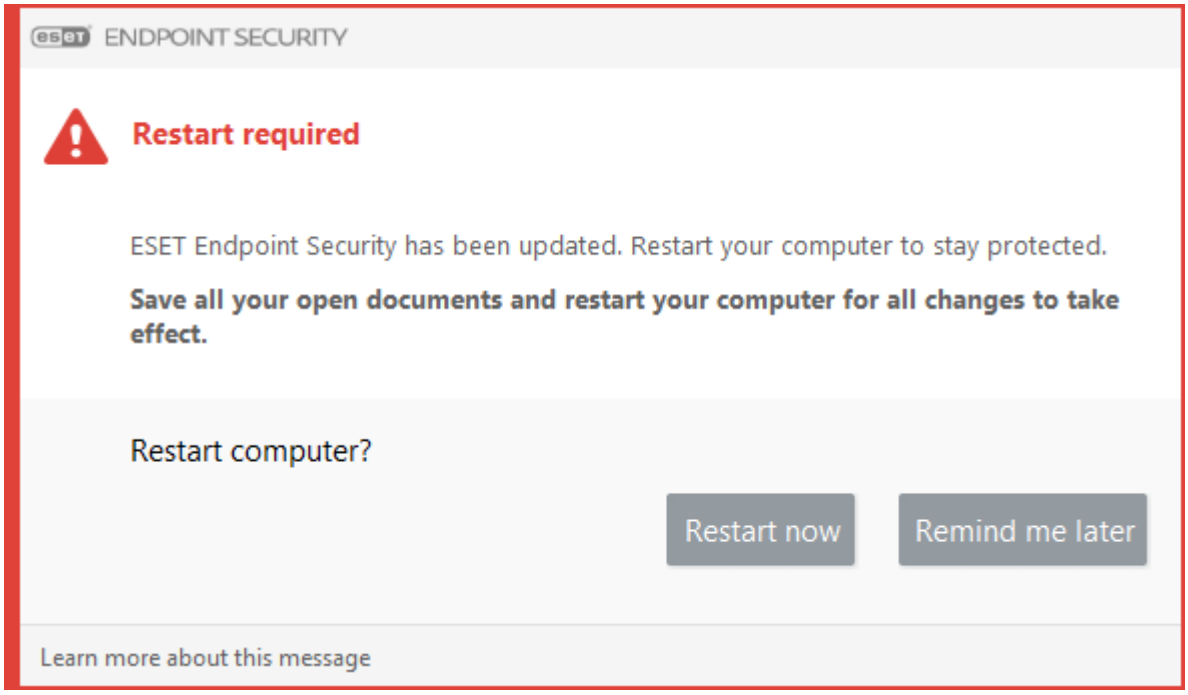
Advanced settings conflict error

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.

> **Important**
> 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.

Restart required

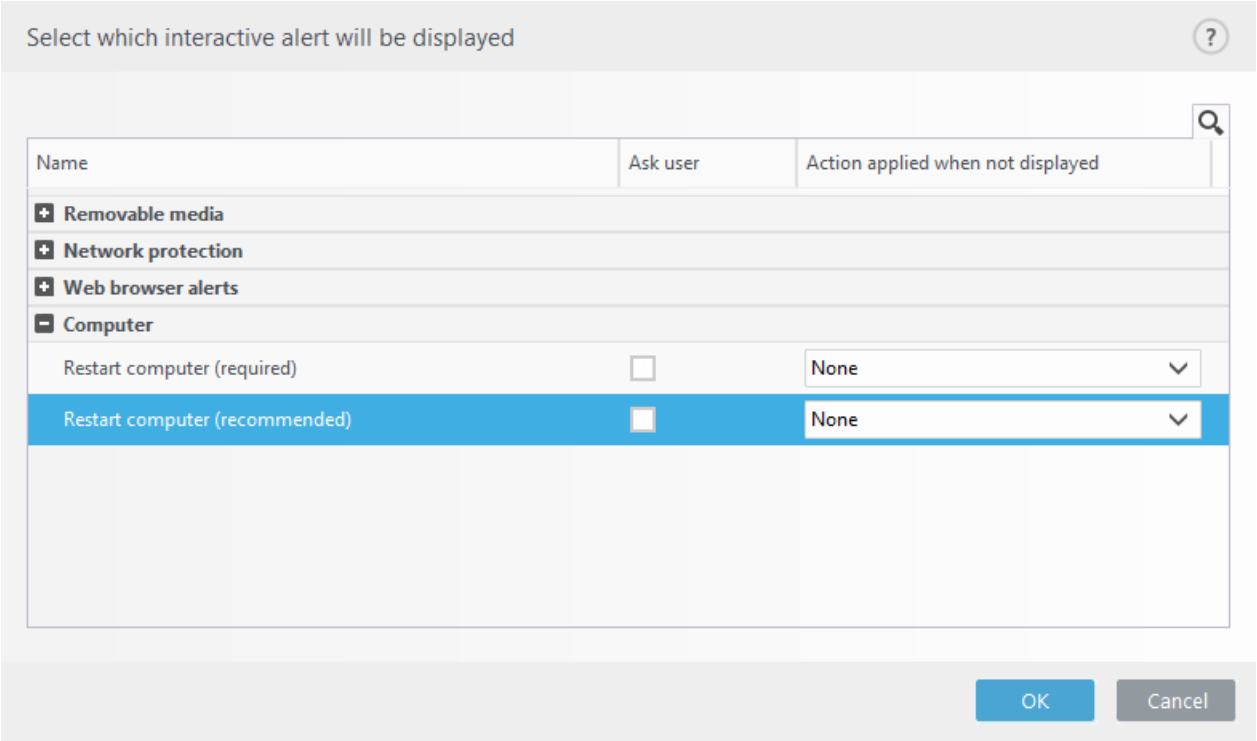
If endpoint machines are receiving the "Restart required" red alert, you can disable the alerts from displaying.



To disable the "Restart required" or "Restart recommended" alert, follow the steps below:

1.Press the **F5** key to access Advanced setup and expand the **Alerts and Message Boxes** section.

2.Click **Edit** next to **List of interactive alerts**. In the **Computer** section, deselect the check boxes next to **Restart computer (required)** and **Restart computer (recommended)**.

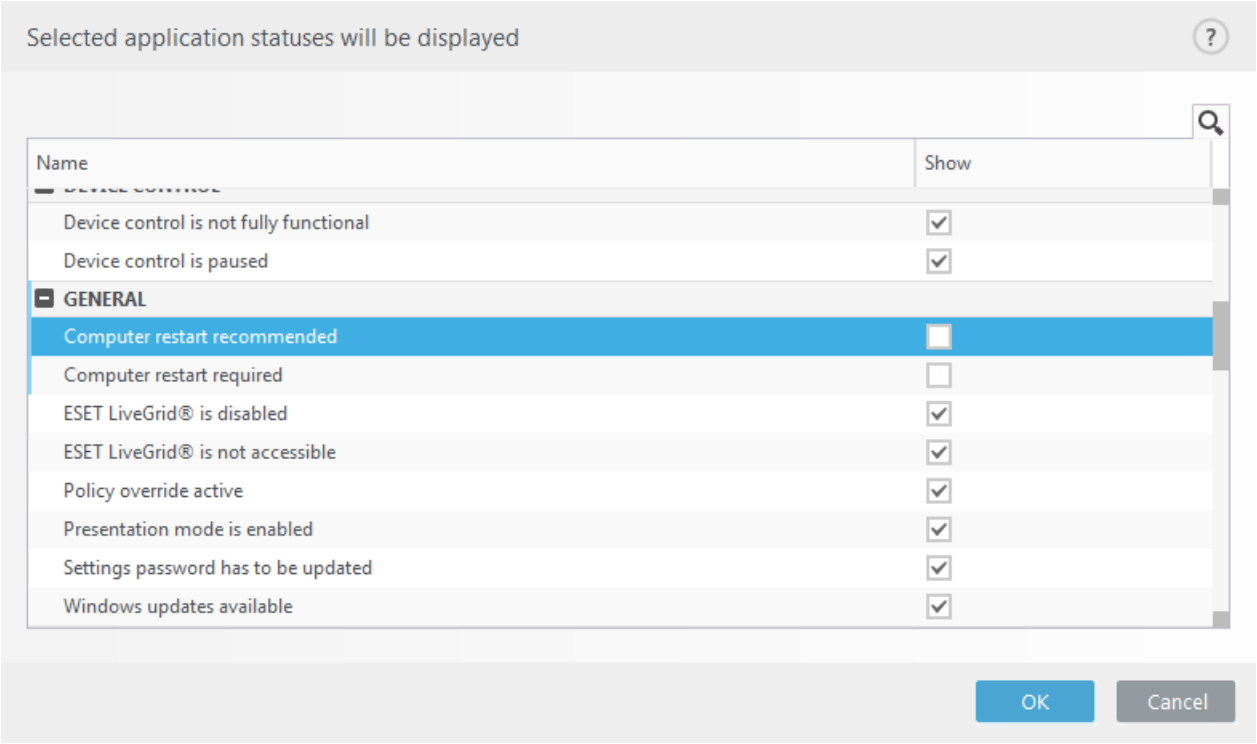


3.Click **OK** to save your changes in both open windows.

4.The alerts will no longer appear on the endpoint machine.

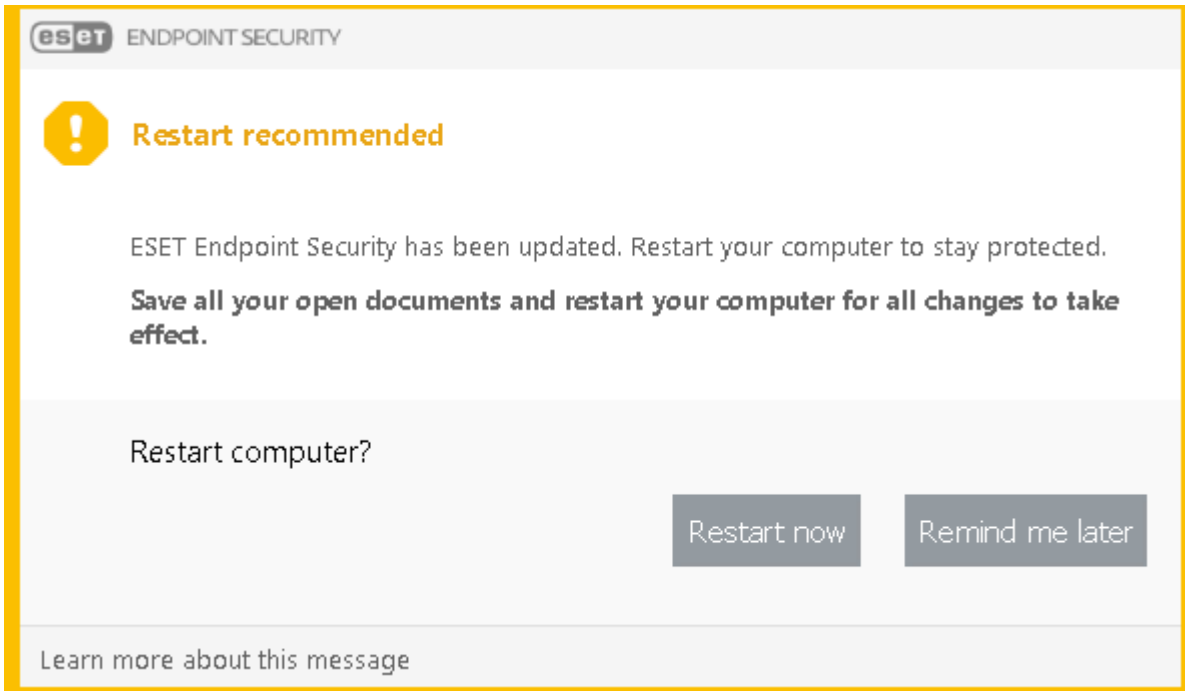
5.(optional) To disable the application status in the main program window of ESET Endpoint Security, from the Application statuses window deselect the check boxes next to **Computer restart required** and **Computer**

restart recommended.



Restart recommended

If endpoint machines are receiving the "Restart recommended" yellow alert, you can disable the alerts from displaying.

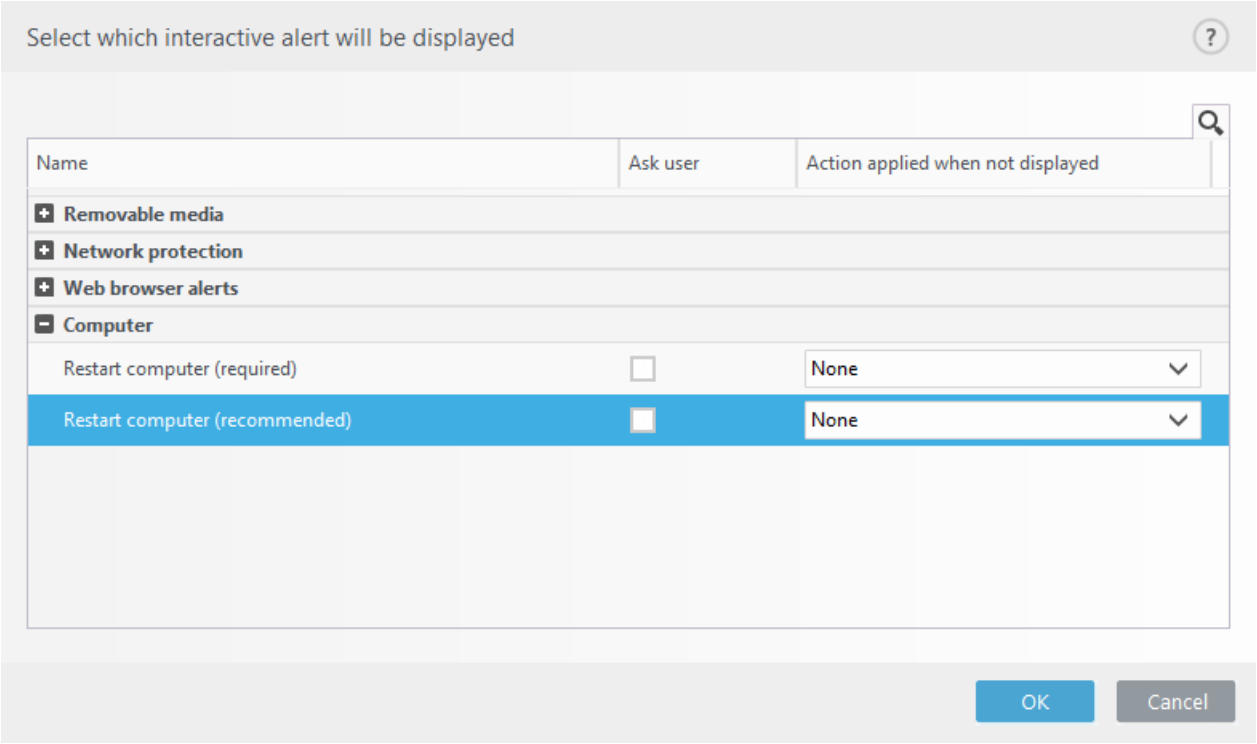


To disable the "Restart required" or "Restart recommended" alert, follow the steps below:

1.Press the **F5** key to access Advanced setup and expand the **Alerts and Message Boxes** section.

2.Click **Edit** next to **List of interactive alerts**. In the **Computer** section, deselect the check boxes next to **Restart**

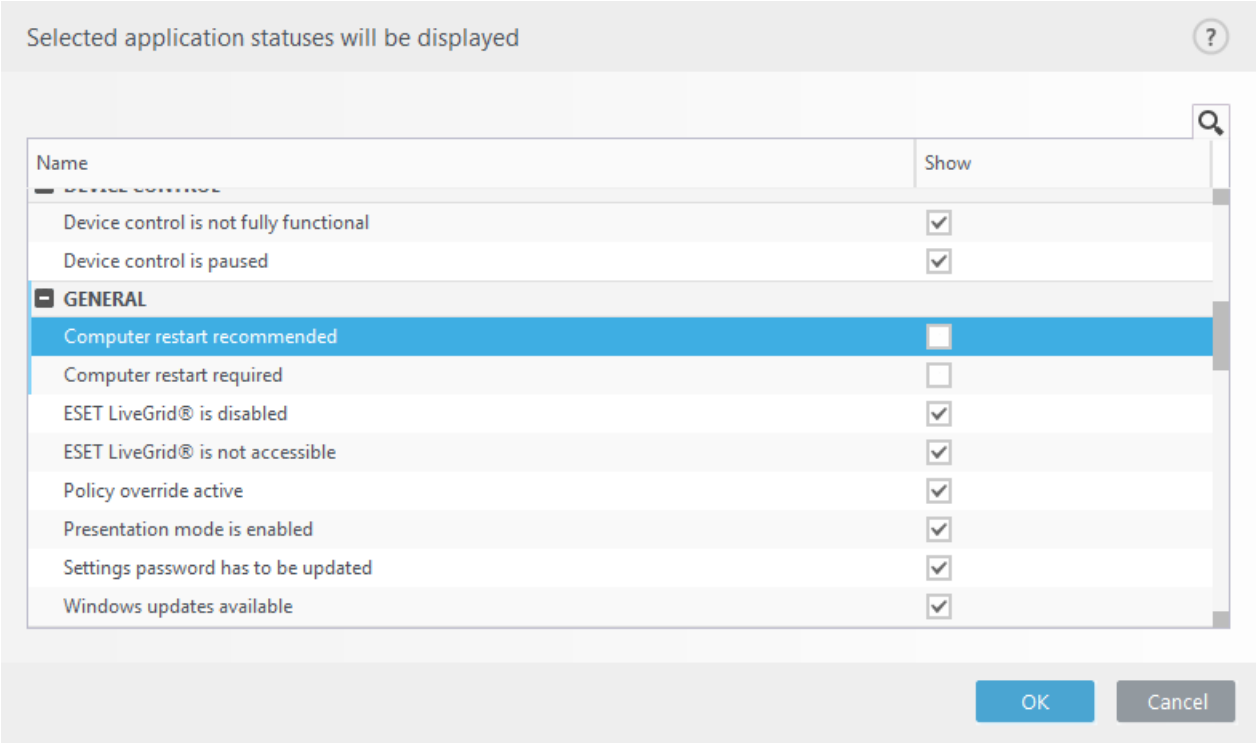
computer (required) and **Restart computer (recommended)**.



3.Click **OK** to save your changes in both open windows.

4.The alerts will no longer appear on the endpoint machine.

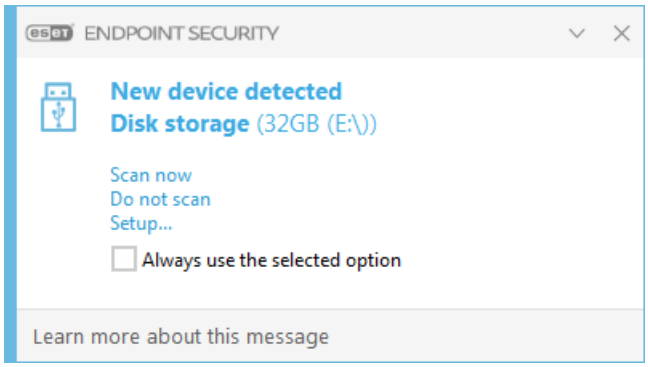
5.(optional) To disable the application status in the main program window of ESET Endpoint Security, from the Application statuses window deselect the check boxes next to **Computer restart required** and **Computer restart recommended**.



Removable media

ESET Endpoint Security provides automatic removable media (CD/DVD/USB/...) scanning upon inserting 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 ESET Endpoint Security, the following dialog will be shown:



Options for this dialog:

- **Scan now** – This will trigger a scan of removable media.
- **Scan later** – Scan of removable media will be postponed.
- **Setup** – Opens the **Advanced setup** section.
- **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 allows 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.

ESET Endpoint Security 7.2 and later

To access settings for removable media scan, open Advanced setup (**F5**) > **User interface** > **Alerts and message boxes** > **Interactive alerts** > **List of interactive alerts** > **Edit** > **New device detected**.

If **Ask user** is not selected, choose the desired action upon 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.
- **Show scan options** – Opens the **Interactive alerts** setup section.

ESET Endpoint Security 7.1 and below

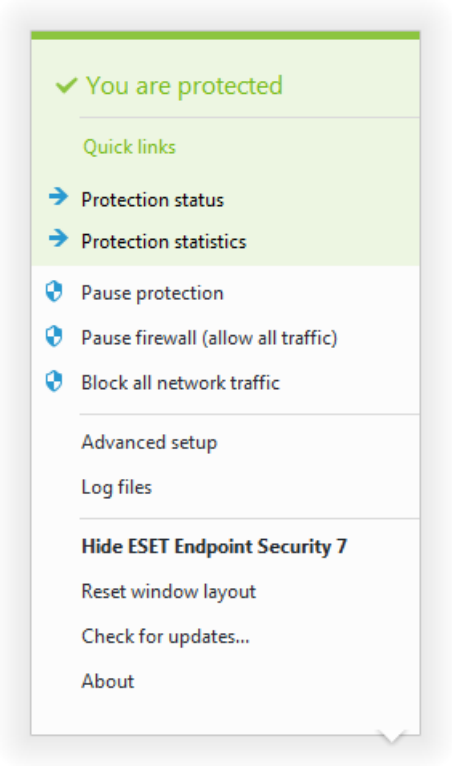
To access settings for removable media scan, open Advanced setup (**F5**) > **Detection engine** > **Malware scans** > **Removable media**.

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 upon 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.
- **Show scan options** – Opens the **Removable media** setup section.

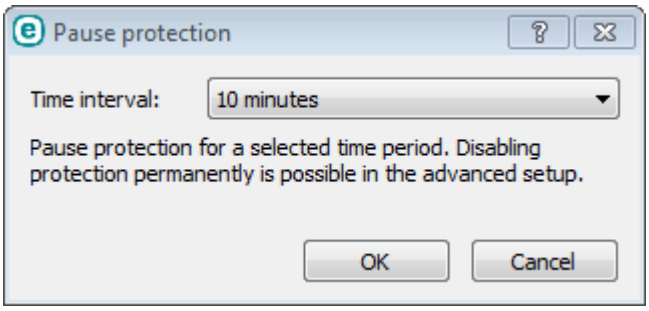
System tray icon

Some of the most important setup options and features are available by right-clicking the system tray icon .



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 represents the period of time that the protection will be disabled for.



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

Block all network traffic – Firewall will block all outgoing / incoming network and internet traffic. You can re-enable it by clicking **Stop blocking all network traffic**.

Advanced setup – Select this option to enter the **Advanced setup** tree. You can also access Advanced setup by pressing the F5 key or navigating to **Setup** > **Advanced setup**.

Log files – Log files contain information about all important program events that have occurred and provide an overview of detections.

Open ESET Endpoint Security – Opens the ESET Endpoint Security main program window from the tray icon.

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

Check for updates... – Starts updating the program modules to ensure your level of protection against malicious code.

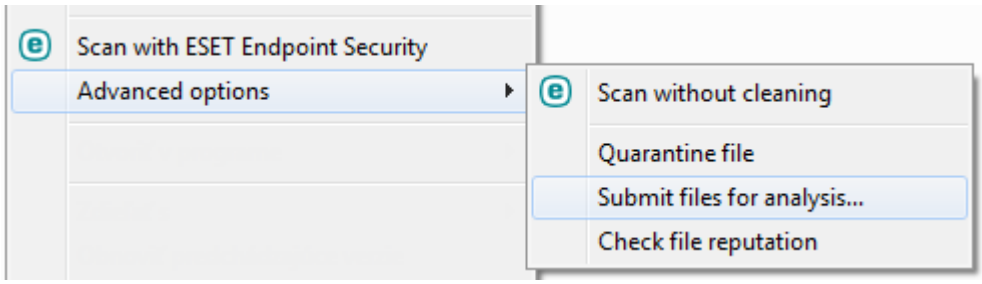
About – Provides system information, details about the installed version of ESET Endpoint Security and the installed program modules as well as your license expiration date. Information about your operating system and system resources can be found at the bottom of the page.

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.

It is possible to integrate ESET Endpoint Security control elements into the context menu. Setup option for this functionality are available in the Advanced setup tree under **User Interface** > **User interface elements**.

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



Help and support

ESET Endpoint Security contains troubleshooting tools and support information that will help you solve issues that you may encounter.

Help

Search ESET Knowledgebase – The ESET Knowledgebase contains answers to the most frequently asked questions as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various problems.

Open help – Click this link to launch the ESET Endpoint Security help pages.

Find quick solution – Click this link to find solutions to the most frequently encountered problems. We recommend that you read this section before contacting Technical Support.

Technical Support

Submit support request – If you could not find an answer to your problem, you can use this form located on the ESET website to quickly contact our Technical Support department.

Details for Technical Support – When prompted, you can copy and send information to ESET Technical Support (such as product name, product version, operating system and processor type).

Support Tools

Threat encyclopedia – Links to the ESET Threat Encyclopedia, which contains information about the dangers and symptoms of different types of infiltration.

Detection Engine history – Links to ESET Virus radar, which contains information about each version of the ESET detection database (previously known as "virus signature database").

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

ESET Specialized Cleaner – Removal tools for common malware infections, for more information please visit this ESET Knowledgebase article.

Product and License Information

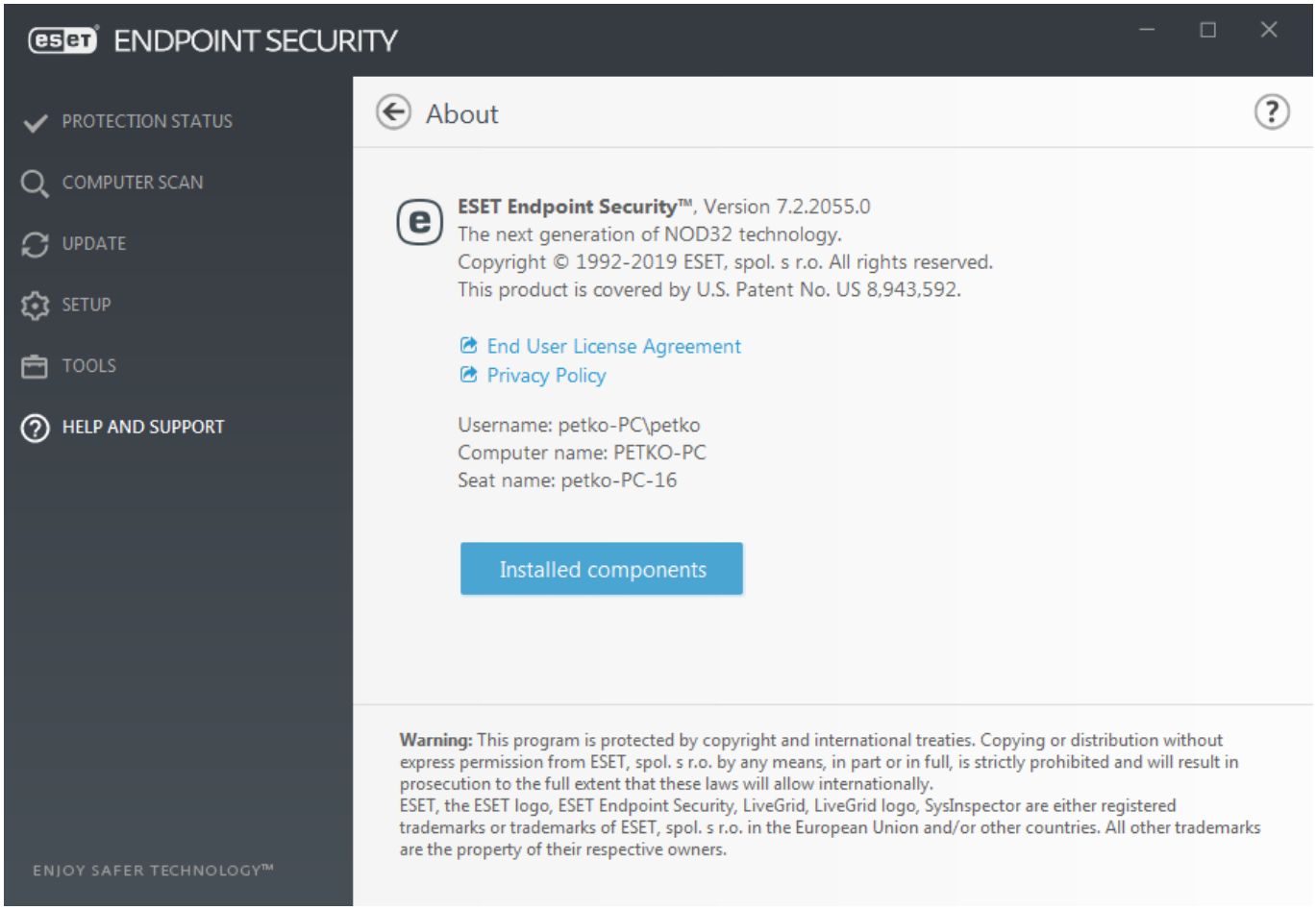
About ESET Endpoint Security – Displays information about your copy of ESET Endpoint Security.

Activate Product/Change License – Click to launch the activation window and activate your product.

About ESET Endpoint Security

This window provides details about installed version of ESET Endpoint Security, your operating system and system resources.

Click **Installed components** to see information about the list of installed program modules and their versions. You can copy information about modules to the clipboard by clicking **Copy**. This may be useful during troubleshooting or when contacting Technical Support.



Submit system configuration data

In order to provide assistance as quickly and accurate 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 for providing technical assistance to the customer.

When submit the web form, your system configuration data will be submitted to ESET. Select **Always submit this information** if you want to remember this action for this process. To submit the form without sending any data click **Don't submit data** and you can contact ESET Technical Support using the online support form.

This setting can also be configured in **Advanced setup** > **Tools** > **Diagnostics** > **Technical Support**.

> **Note**
> If you have decided to submit system data it is needed to fill and submit the web form, otherwise your ticket will not be created and your system data will be lost.

Profile manager

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

On-demand 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 the Advanced setup window (F5) and click **Antivirus** > **On-demand computer scan** and then **Edit** next to **List of profiles**. The **Update profile** drop-down menu that lists existing scan profiles. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

> **Note**
> 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 **Strict cleaning**. Enter 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 section allows users 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. Once 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.

Keyboard shortcuts

For better navigation in ESET Endpoint Security, the following keyboard shortcuts can be used:

Keyboard shortcut	Action taken
F1	opens help pages
F5	opens Advanced setup
Up/Down	navigation in product through items
TAB	moves the cursor in a window
Esc	closes the active dialog window
Ctrl+U	shows information about ESET license and your computer (Details for Technical Support)
Ctrl+R	resets product window to its default size and position on the screen

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 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 Kernel advanced logging – Record all events that occur in ESET kernel service (ekrn) to allow diagnosing and solving problems (available in version 7.2 and later).

Enable Licensing advanced logging – Record all product communication with ESET activation and ESET Business Account 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 in order to help developers diagnose and fix problems related to Firewall.

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 Protocol filtering advanced logging – Record all data passing through the Protocol filtering engine in the PCAP format in order to help the developers diagnose and fix the problems related to Protocol filtering.

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 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 location

Operating system	Log files directory
Windows Vista and later	C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics\
Earlier versions of Windows	C:\Documents and Settings\All Users\...

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 automatically clean or delete infected files. • `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 what the file is. • `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 last access timestamp

Exit codes

0	no threat found
1	threat found and cleaned
10	some files could not be scanned (may be threats)
50	threat found
100	error

> **Note**
> Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

ESET CMD

This is a feature that enables advanced ecmd commands. It allows you to 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.

Once 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.

> **Important**
> 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.

> **Note**
> Advanced ecmd commands can only be run locally. Executing a client task **Run command** using ESMC will not work.

> **Example**
> 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>`

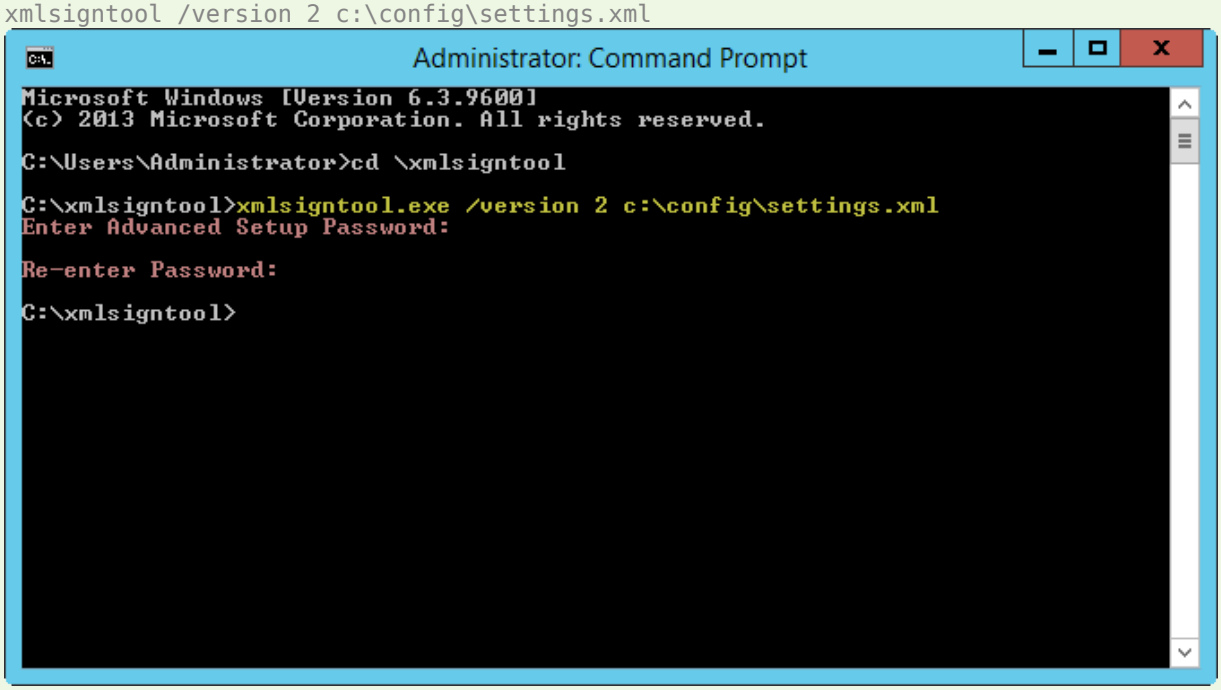
> **Important**
> The value of the `/version` parameter depends on your version of ESET Endpoint Security. Use `/version 2` for version 7 and newer.

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.

Example

Sign exported configuration file command:

```
xmlsigntool /version 2 c:\config\settings.xml
```



Note

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 allows you to use an older configuration file without exporting it to another machine running ESET Endpoint Security before the import.

Warning

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 ESMC 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
Anti-Stealth technology	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth 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
Email client protection	ecmd /setfeature email pause	ecmd /setfeature email enable
Antispam protection	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Anti-Phishing protection	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Idle-state detection

Idle state detection settings can be configured in **Advanced setup** under **Detection engine** > **Malware scans** > **Idle-state scanning** > **Idle state detection**. These settings specify a trigger for Idle-state scanning, when:

- the screen saver is running,
- the computer is locked,
- a user logs off.

Use the switches for each respective state to enable or disable the different idle state detection triggers.

Import and export settings

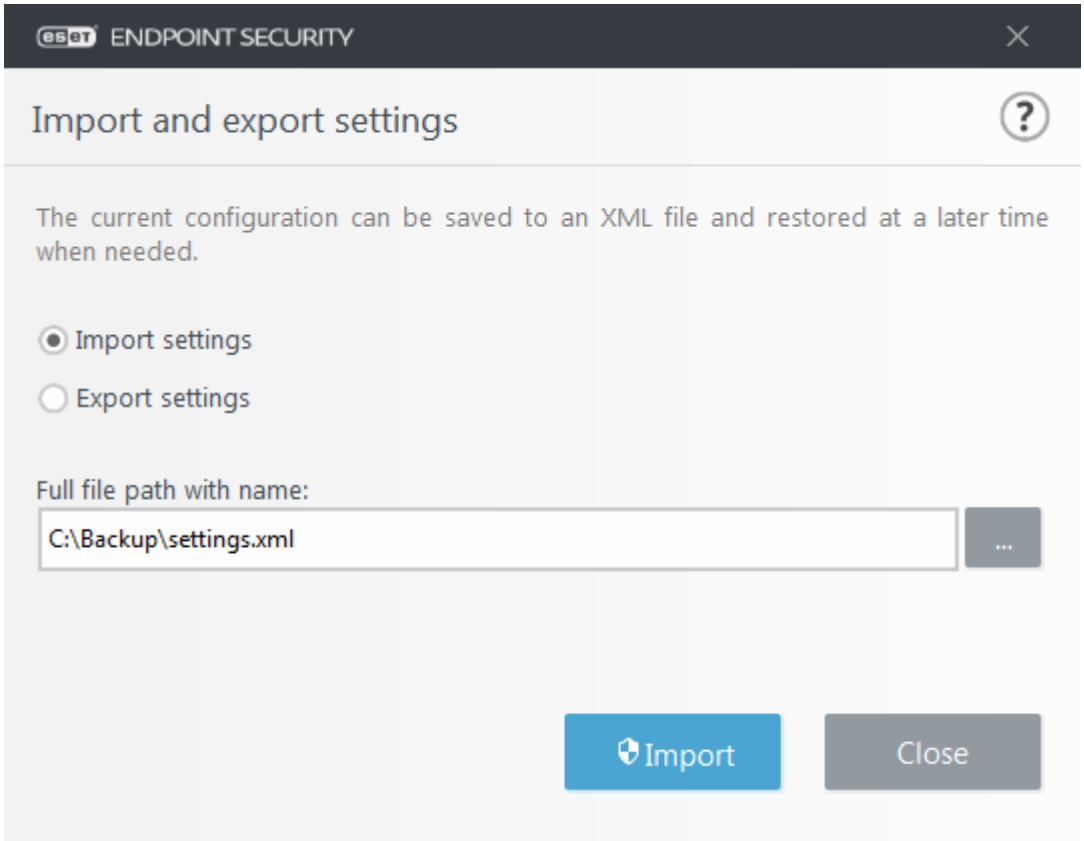
You can import or export your customized ESET Endpoint Security .xml configuration file from the **Setup** menu.

Importing and exporting of 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 for users who want to use their preferred configuration on multiple systems, they can easily import an .xml file to transfer these settings.

Importing a configuration is very easy. In the main program window click **Setup** > **Import/Export settings**, and then select **Import settings**. Enter the file name of the configuration file or click the **...** button to browse for the configuration file you want to import.

The steps to export a configuration are very similar. In the main program window, click **Setup** > **Import/Export settings**. Select **Export settings** and enter the file name of the configuration file (i.e. *export.xml*). Use the browser to select a location on your computer to save the configuration file.

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



Revert all settings to default

Click **Default** in Advanced setup (F5) 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.

Please note, 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.

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 Plug-in for ConnectWise Automate
- ESET Direct Endpoint Management Plugin for DattoRMM
- ESET Direct Endpoint Management for Solarwinds N-Central
- ESET Direct Endpoint Management for NinjaRMM

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 a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.

```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:
  get: get information about products
    application-info: get information about application
    license-info: get information about license
    protection-status: get protection status
    logs: get logs: all, virlog, warnlog, scanlog ...
      -N [--name] arg=all (retrieve all logs) name of log to retrieve
      -S [--start-date] arg                   start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
      -E [--end-date] arg                     end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    scan-info: get information about scan
      -I [--id] arg                           id of scan to retrieve
    configuration: get product configuration
      -F [--file] arg                         path where configuration file will be saved
      -O [--format] arg=xml                   format of configuration: json, xml
    update-status: get information about update
    activation-status: get information about last activation

  start: start task
    scan: Start on demand scan
      -P [--profile] arg                      scanning profile
      -T [--target] arg                       scan target
    activation: Start activation
      -K [--key] arg                          activation key
      -O [--offline] arg                      path to offline file
      -T [--token] arg                        activation token
    deactivation: start deactivation of product
    update: start update of product

  set: set configuration to product
    configuration: set product configuration
      -V [--value] arg                        configuration data (encoded in base64)
      -F [--file] arg                         path to configuration xml file
      -P [--password] arg                     password for configuration

Application parameters:
      -H [--help]                             help
      -L [--log]                              log application
--debug                                       display input json

Example: eRmm start scan --target C:\ -p "@Smart scan"

C:\Program Files\ESET\ESET Security>_
```

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**
	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	Particular 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 isn't enabled in advanced settings or isn't 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":"ANTISTEALTH32",
    "description":"Anti-Stealth support module",
    "version":"1106",
    "date":"2016-10-17"
   },{
    "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, error }

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" | --token "activation token"
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file
token	Activation token

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
}
```

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
- How to use current credentials to activate a new product
- 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 connect my product to ESET Security Management Center
- 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.

- Best practices to protect against Filecoder (ransomware) malware
- ESET Endpoint Security and ESET Endpoint Antivirus 7 FAQ
- Create or edit a firewall rule to allow RDP connections in ESMC
- 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.

How to update ESET Endpoint Security

Updating 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 Scheduler, click here).

How to activate ESET Endpoint Security

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

There are several methods for activating your product. Availability of a particular 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.).

To activate your copy of ESET Endpoint Security directly from the program, open the ESET Endpoint Security main program window and in the main menu, click **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** – A 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.

- **ESET Business Account** – An account created on the ESET Business Account portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.

- **Offline License** – An 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 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 Security Management Center. 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 older ESET products and do not know how to activate ESET Endpoint Security, convert your legacy credentials to a License key.

Failed product activation?

You can change your product license at any time. To do so, click **Help and support** > **Change license** in the main program window. You will see the public license ID used to identify your license to ESET Support. The Username under which your computer is registered is stored in the **About** section, which you can view by right-clicking the system tray icon.

> **Note**
> ESET Security Management Center can activate client computers silently using licenses made available by the administrator. For instructions to do so, see the ESET Security Management Center Online help.

Entering your License Key during activation

Automatic updates are important for your security. ESET Endpoint Security will only receive updates once 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.poslem

Login to ESET Business Account

The Security Admin account is an account created on the ESET Business Account portal with your **Email address** and **Password**, which is able to see all seat authorizations. A Security Admin account allows you to manage multiple licenses. If you do not have a Security Admin account click **Create account** and you will be redirected to the ESET Business Account portal where you can register with your credentials.

If you have forgotten your password click **I forgot my password** and you will be redirected to the ESET Business Account portal. Enter your email address and click **Sign in** to confirm. After that you will obtain a message with instructions how to reset your password.

How to use legacy license credentials to activate a newer 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.

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.

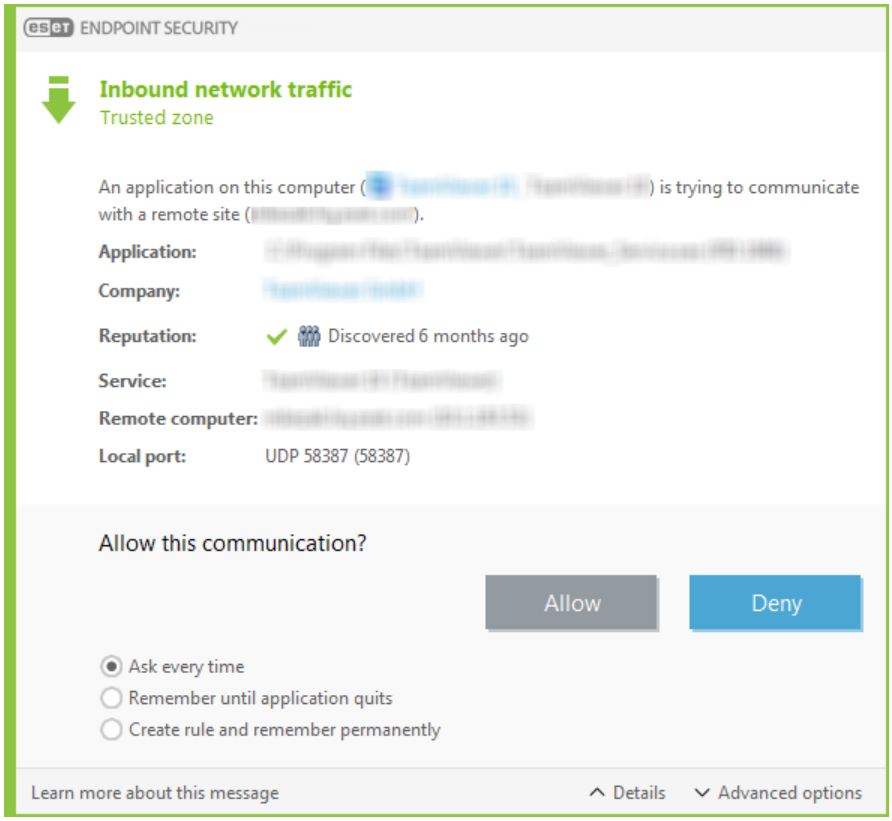
3. After the scan has finished, review the log with the number of scanned, infected and cleaned files.

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 please 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, located under **Advanced setup** > **Firewall** > **Basic** > **Rules** by clicking **Edit**.

Click **Add** to add the rule. In the **General** tab, enter the name, direction and communication protocol for the rule. This window allows you to define the action to be taken when the rule is applied.

Enter the path to the application's executable and the local communication port in the **Local** tab. Click the **Remote** tab to enter 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**. Enter 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, allowing 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 and click **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** in the main Scheduler screen.

2. Select **On-demand computer scan** from the drop-down menu.

3. Enter 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 Security Management Center

When you have installed ESET Endpoint Security on your computer and you want to connect via ESET Security Management Center, make sure that you have also installed ESET Management Agent on your client workstation. It is an essential part of every client solution that communicates with ESMC 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 allows 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.

Warning

- Override mode cannot be stopped from the ESMC Web Console once it is 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 for ESET Endpoint Security version 7.0.2100.4 and later.

To set the **Override mode**:

1. Navigate to **Polices** > **New Policy**.

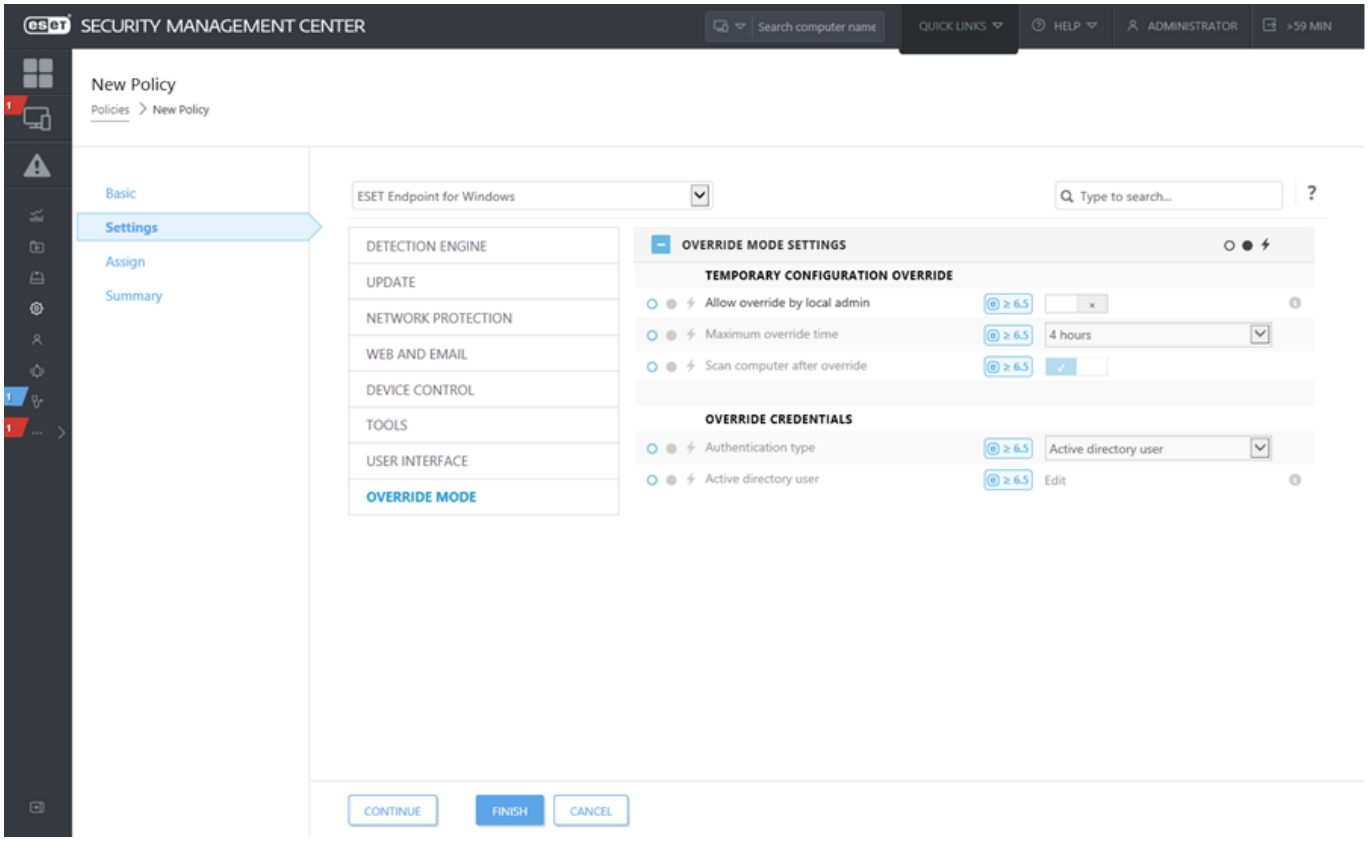
2. In the **Basic** section, type in a **Name** and **Description** for this policy.

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.



Example

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 ESMC 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 ESMC 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 on 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 once it is no longer needed.

How to apply a recommended policy for ESET Endpoint Security

The best practice after connecting ESET Endpoint Security to ESET Security Management Center 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 ESMC & EEI connection	Block all traffic except connection to ESET Security Management Center and ESET Enterprise Inspector 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 parameters, 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 Cloud.
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:

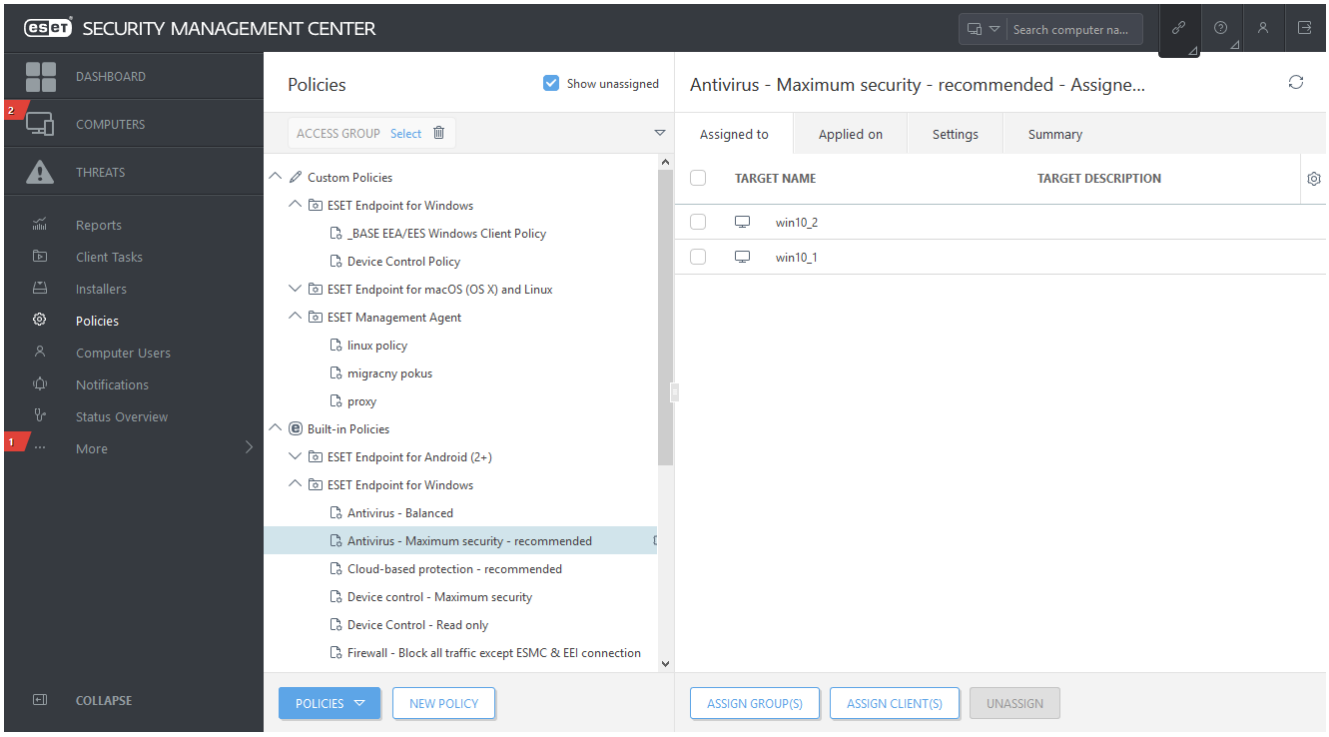
> **Illustrated instructions**
> The following ESET Knowledgebase article may only be available in English:
> - Apply a recommended or predefined policy for ESET Endpoint Security using ESMC

1. Open the ESMC Web Console.

2. Navigate to **Polices** and expand **Built-in Policies** > **ESET Endpoint for Windows**.

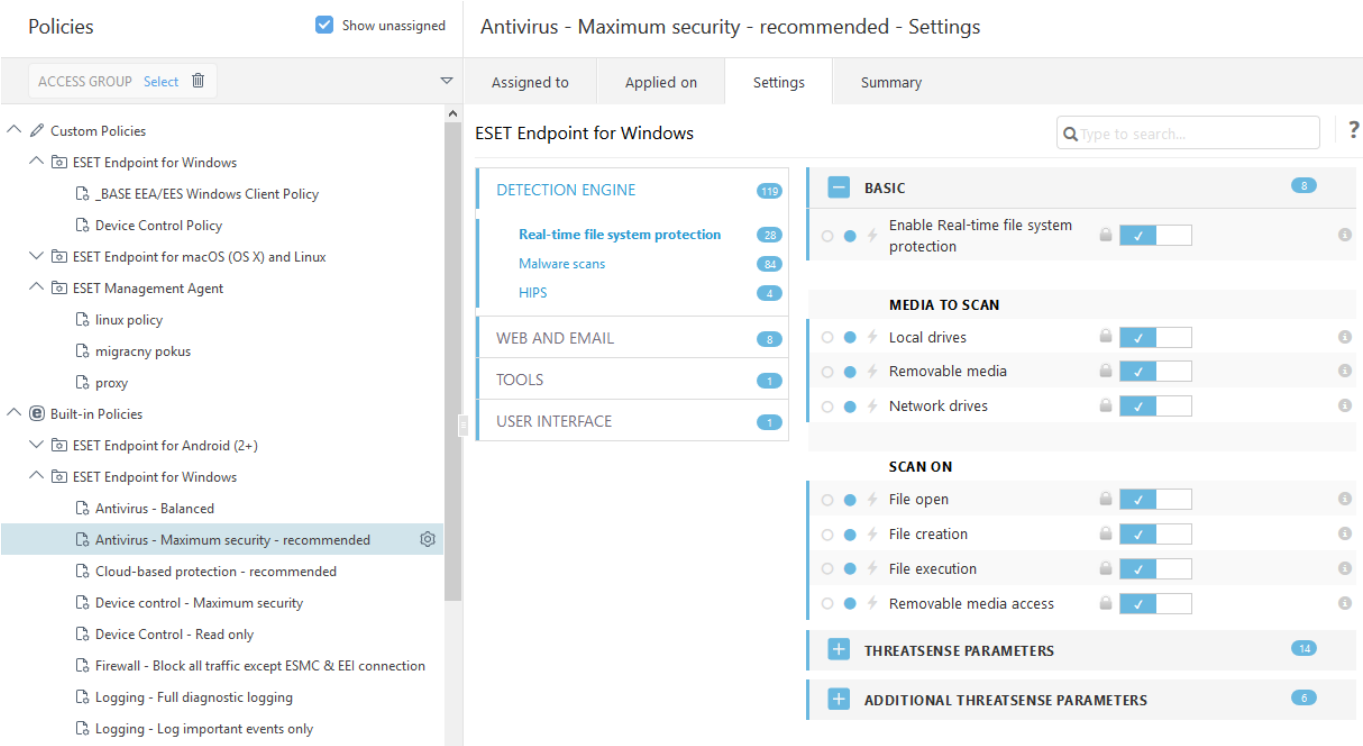
3. Click **Antivirus - Maximum security - recommended**.

4. In the **Assigned to** tab click **Assign client(s)** or **Assign groups(s)** and select the appropriate computers for which you wish 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 ESMC policies here]



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 that are running ESET Endpoint Security or ESET Endpoint Antivirus.

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 make sure 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.

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.

> **Note**
> If you do not want to provide module updates via internal HTTP server disengage **Create update mirror**.

How do I upgrade to Windows 10 with ESET Endpoint Security

> **Warning**
> 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.

Version 7.x:

Click the appropriate link below to download and install the latest version to prepare for your upgrade to Microsoft Windows 10:

Download ESET Endpoint Security 7 32-bit Download ESET Endpoint Antivirus 7 32-bit

Download ESET Endpoint Security 7 64-bit Download ESET Endpoint Antivirus 7 64-bit

Version 5.x:

> **Important**
> ESET Endpoint products in version 5 are currently in Basic Support. This means builds are no longer publicly available for download. We strongly recommend upgrading to the latest version of ESET Endpoint products. If you need to access the MSI installers, contact ESET Technical Support for further assistance.

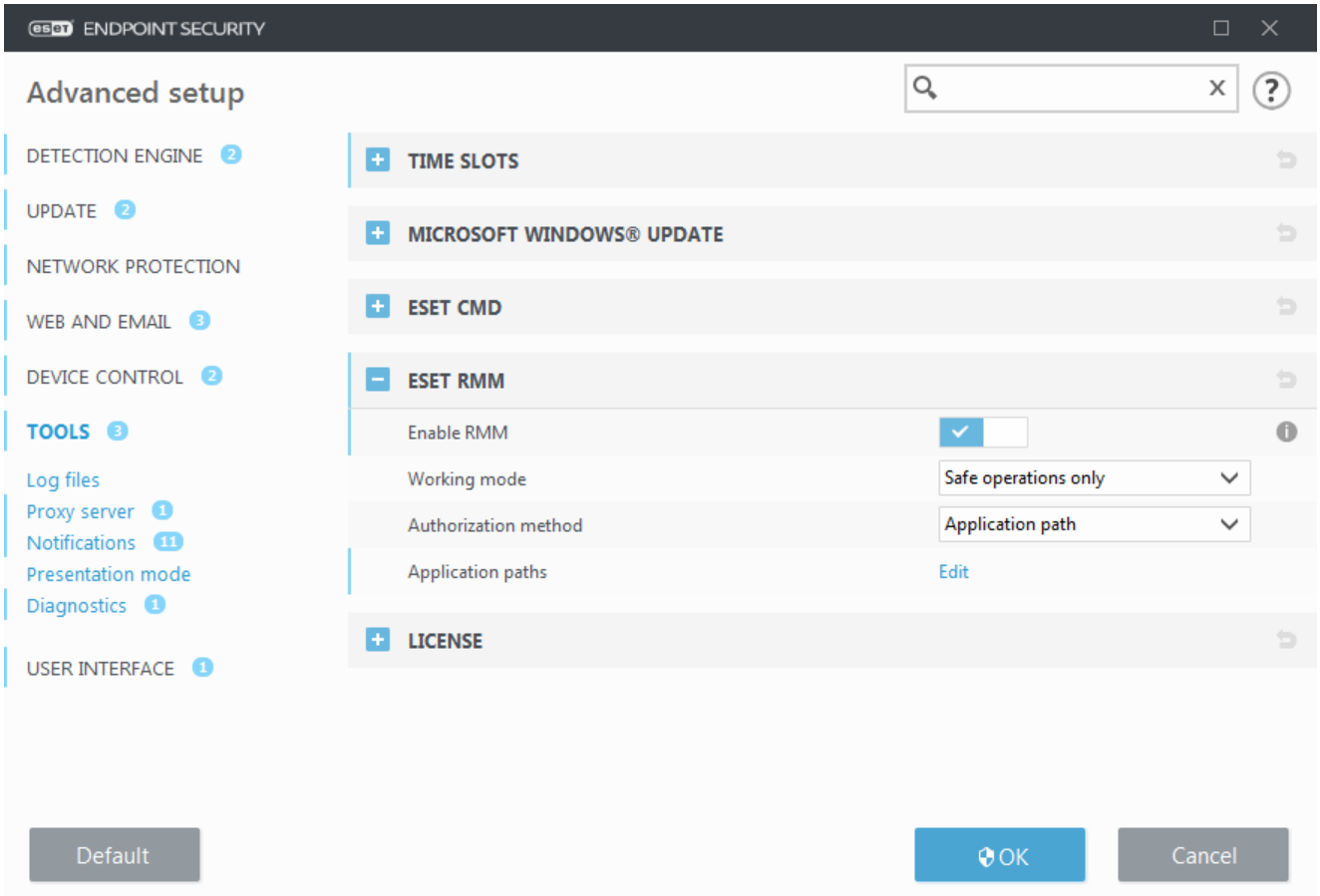
Other language versions:

If you are looking for another language version of your ESET endpoint product, please visit our download page.

> **Note**
> 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, press **F5** to access Advanced setup, click **Tools**, expand **ESET RMM** and turn on the switch next to **Enable RMM**.

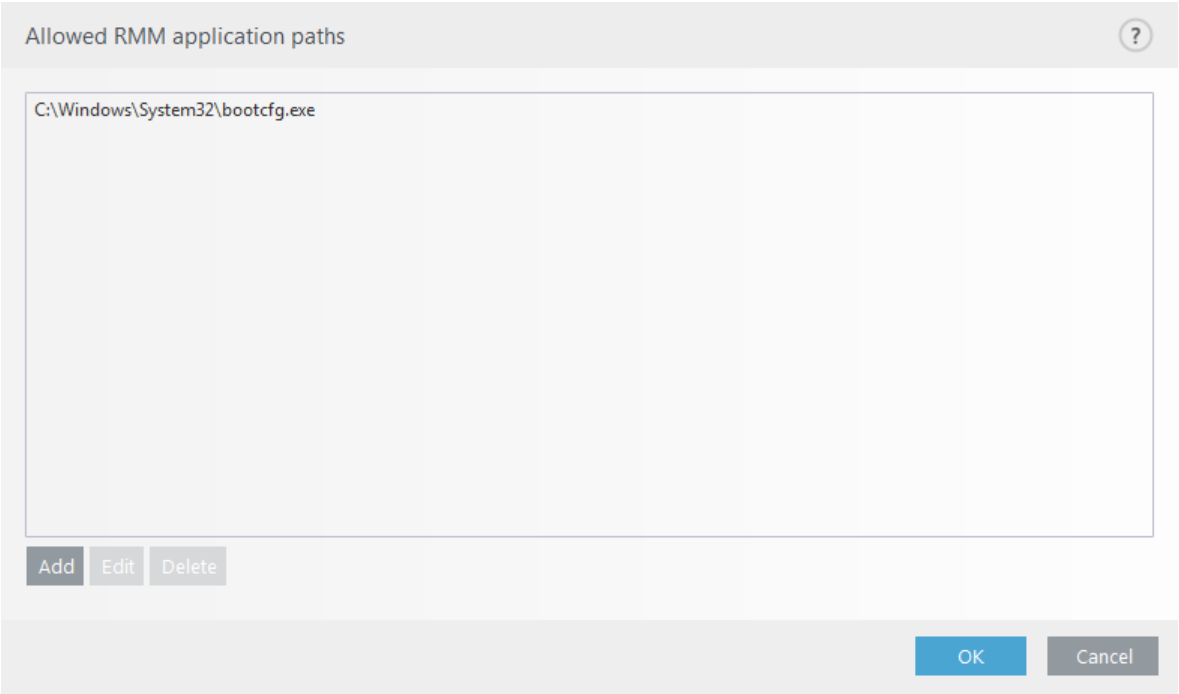
Working mode – Select **Safe operations only** if you want to enable RMM interface for safe and read only operations. Select **All operations** if you want to enable RMM interface for all operations.

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	✔	✔
Start update	✔	✔

Authorization method – Set the RMM authorization method. To use authorization, select **Application path** from the drop-down menu, otherwise select **None**.

> **Warning**
> 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. Enter 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.

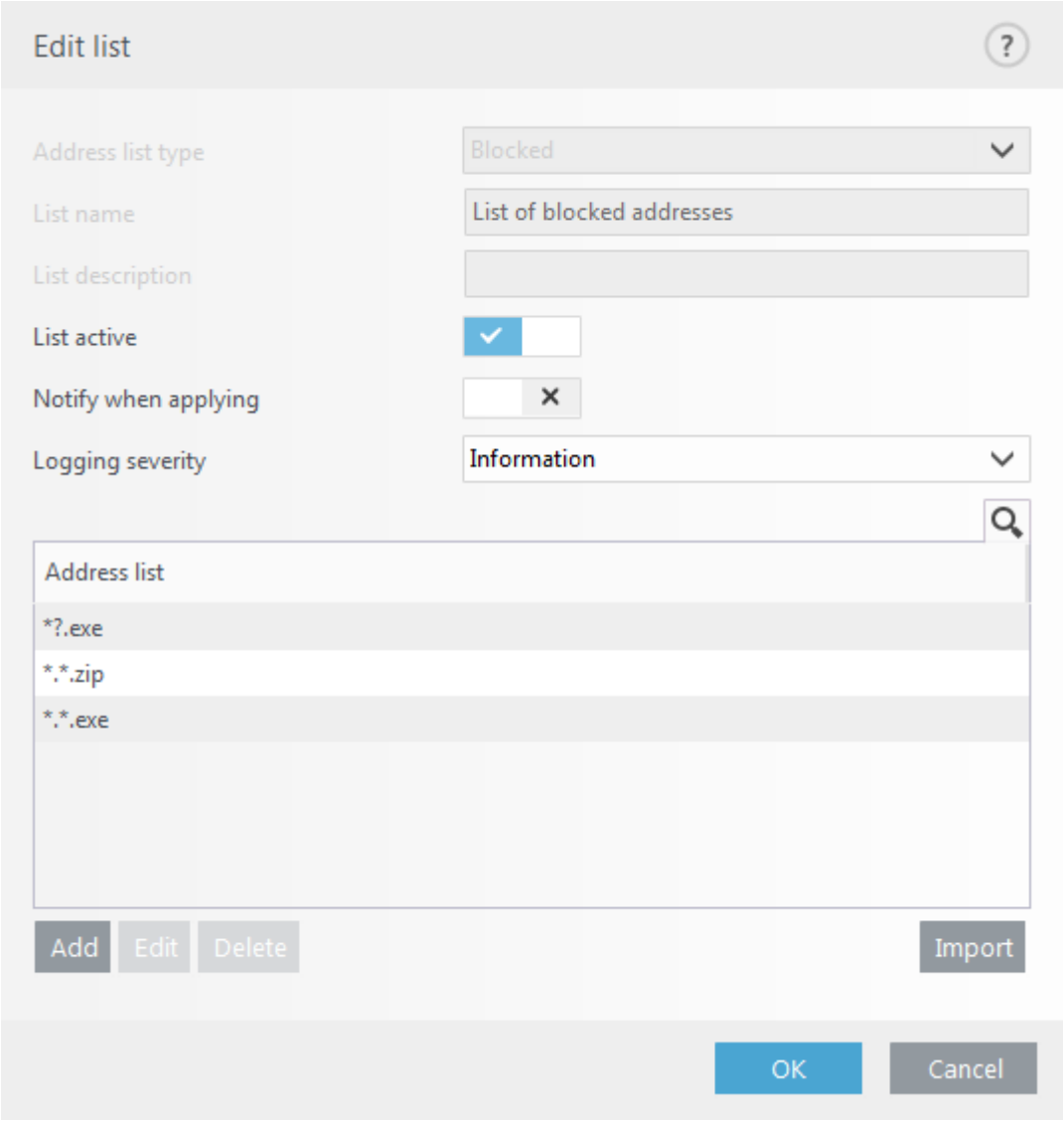
Default ESET Endpoint Security installation contains file ermm.exe located in Endpoint application directory (default path C*:\Program Files\ESET\ESET Security*). The file ermm.exe exchange data with RMM Plugin, which communicates with RMM Agent, linked to a RMM Server.

- 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 click **Add** to create a new 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** slider bar. Select the **Logging severity** from the drop-down menu. Remote Administrator can collect records with **Warning** verbosity.



Click **Add** to enter a mask that specifies file types you want to block from downloading. Enter 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 zip compressed files to be 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 webpage 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 have 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

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 (hereinafter referred to as "the Agreement") executed by and between 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 (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the 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. If You do not agree to all of the terms and conditions of this Agreement, 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 (hereinafter referred to as " 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, smart phones, 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 (hereinafter referred to as "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 system; or (ii) if the extent of a license is bound to the number of mail boxes, then one End User shall be taken to refer to a computer user who accepts electronic mail via a Mail User Agent (hereinafter referred to as "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 in which has the right to use the Software in accordance 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) **Business Edition.** A Business Edition version of the Software must be obtained 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.** OEM Software 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 be also 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 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 automatic installation of Updates. For the purpose of 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.

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 (hereinafter referred to as "Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed, information about the operations and functionality of the Software and information about devices in local network such as type, vendor, model and/or name of device (hereinafter referred to as "Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by 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. You hereby agree to receive notification and messages including but not limited to marketing information.

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 back-up 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 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 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 back-up copies and all related materials provided by the Provider or its business partners. 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 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. 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 act, 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 (hereinafter referred to as "Affiliates") being in violation of, or being subject to negative consequences under, Trade Control Laws which includes

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 (hereinafter referred to as "Export Control Laws") 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 (hereinafter referred to as "Sanction 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 return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

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. In case of a discrepancy between language versions of this Agreement, the English version shall prevail. This Agreement may only be modified in written form, signed by an authorized representative of the Provider, or a person expressly authorized to act in this capacity under the terms of a power of attorney.

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.

EULA ID: BUS-STANDARD-20-01

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