ESET NOD32 Antivirus

User guide

ESET
®
Digital Security
Progress. Protected.

ESSENTIAL SECURITY

ESET NOD32 Antivirus

ESET NOD32 Antivirus represents a new approach to truly integrated computer security. The most recent version of the ESET LiveGrid® scanning engine 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 that might harm your computer.

ESET NOD32 Antivirus is a complete security solution that combines maximum protection and a minimal system footprint. Our advanced technologies use artificial intelligence to prevent infiltration by viruses, spyware, trojan horses, worms, adware, rootkits, and other threats without hindering system performance or disrupting your computer.

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 NOD32 Antivirus and offers dynamically updated support content.
Dark mode	An extension that helps you quickly switch the screen to a dark color scheme. You can choose your preferred color scheme in User interface elements.
Antivirus and antispyware	Proactively detects and cleans more known and unknown viruses, worms, trojans and rootkits. Advanced heuristics flags even never-before-seen malware, protecting you from unknown threats and neutralizing them before they can do any harm. Web access protection and Anti-Phishing protection monitors 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 NOD32 Antivirus.
Device control	Automatically scans all USB flash drives, memory cards and CDs/DVDs. Blocks removable media based on the type of media, manufacturer, size and other attributes.
HIPS functionality	You can customize the behavior of the system in greater detail; specify rules for the system registry, active processes and programs, and fine-tune your security posture.
Gamer mode	Postpones all pop-up windows, updates or other system-intensive activities to conserve system resources for gaming and other full-screen activities.

A license needs to be active in order for features of ESET NOD32 Antivirus to be operational. It is recommended that you renew your license several weeks before the license for ESET NOD32 Antivirus expires.

What's new?

What's new in ESET NOD32 Antivirus 16.2

Intel® Threat Detection Technology

This is a hardware-based technology that exposes ransomware as it attempts to avoid detection in memory. Its integration boosts ransomware protection while keeping overall system performance high. See the supported processors.

Dark Mode

This feature allows you to choose a light or dark color scheme for ESET NOD32 Antivirus Graphical user interface. You can now switch the color scheme in the top right corner of the main program window.

Removed Windows 7, 8 and 8.1 support.

ESET NOD32 Antivirus 16.2 is supported only on Windows 10 and 11. For more information, see Outdated versions of Microsoft Windows.

Redesigned Advanced setup

Advanced setup has been redesigned and settings are now grouped for a better user experience.

> **i** To disable **What's new notifications**, open Advanced setup > **Notifications** > **Desktop notifications**. Click **Edit** next to **Desktop notifications**, deselect the **Display What's new notifications** check box and click **OK**. For more information about notifications, see the Notifications section.

> **i** For a detailed list of changes in ESET NOD32 Antivirus, see ESET NOD32 Antivirus changelogs.

Which product do I have?

ESET offers multiple layers of security with new products from powerful and fast antivirus solution to all-in-one security solution with minimal system footprint:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

To determine which product you have installed open the main program window and you will see the name of the product at the top of the window (see the Knowledgebase article).

The table below details features available in each specific product.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detection engine	✔	✔	✔
Advanced Machine Learning	✔	✔	✔
Exploit Blocker	✔	✔	✔
Script-Based Attack Protection	✔	✔	✔
Anti-Phishing	✔	✔	✔
Web access protection	✔	✔	✔
HIPS (including Ransomware shield)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Network Inspector		✔	✔
Webcam Protection		✔	✔
Network Attack Protection		✔	✔
Botnet Protection		✔	✔
Banking & Payment Protection		✔	✔
Parental Control		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

> **i** Some of the products above may not be available for your language / region.

System requirements

Your system should meet the following hardware and software requirements for ESET NOD32 Antivirus to perform optimally:

Processors supported

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

Operating Systems supported

Microsoft® Windows® 11

Microsoft® Windows® 10

> ⚠ The latest version of ESET NOD32 Antivirus requires Windows 10 or Windows 11 operating systems. If you cannot upgrade Windows, install ESET NOD32 Antivirus version 16.0. See the ESET NOD32 Antivirus version 16.0 Online Help for more information.

> ⚠️ Always keep your operating system up to date.

ESET NOD32 Antivirus features requirements

See the system requirements for specific ESET NOD32 Antivirus features in the table below:

Feature	Requirements
Intel® Threat Detection Technology	See the supported processors.
Transparent background	Windows 10 version RS4 and later.
Specialized Cleaner	Non-ARM64-based processor.
System Cleaner	Non-ARM64-based processor.
Exploit Blocker	Non-ARM64-based processor.
Deep Behavioral Inspection	Non-ARM64-based processor.

Other

An internet connection is required for activation and ESET NOD32 Antivirus updates to function properly.

Two antivirus programs running simultaneously on a single device causes inevitable system resource conflicts, including slowing down the system to make it inoperable.

Outdated versions of Microsoft Windows

Issue

- You want to install the latest version of ESET NOD32 Antivirus on a computer with Windows 7, Windows 8 (8.1) or Windows Home Server 2011

- ESET NOD32 Antivirus displays an error **Outdated operating system** during the installation

Details

The latest version of ESET NOD32 Antivirus requires Windows 10 or Windows 11 operating systems.

Solution

The following solutions are available:

Upgrade to Windows 10 or Windows 11

The upgrade process is relatively easy, and in many cases, you can do it without losing your files. Before upgrading to Windows 10:

1. Back up important data.

2. Read Microsoft's Upgrade to Windows 10 FAQ or Upgrade to Windows 11 FAQ and update your Windows operating system.

Install ESET NOD32 Antivirus version 16.0

If you cannot upgrade Windows, install ESET NOD32 Antivirus version 16.0. See the ESET NOD32 Antivirus version 16.0 Online Help for more information.

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 to bypass existing security measures and bring profit to their authors – all at the expense of other users. The specialists at the ESET Research Lab analyze these threats on a daily basis and prepare and release updates 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 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 users' 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 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.

- Do not use an Administrator account for everyday work on your computer.

Help pages

Welcome to the ESET NOD32 Antivirus user guide. The information provided here will introduce you to your product and help you make your computer more secure.

Getting started

Before using ESET NOD32 Antivirus, you can read about various types of detections and remote attacks you might encounter when using your computer. We have also compiled a list of new features introduced in ESET NOD32 Antivirus.

Start by installing ESET NOD32 Antivirus. If you already have ESET NOD32 Antivirus installed, see Working with ESET NOD32 Antivirus.

How to use ESET NOD32 Antivirus Help pages

Online Help is divided into several chapters and sub-chapters. Press **F1** in ESET NOD32 Antivirus to view information about the currently opened window.

Online Help enables you to search for a help topic by keyword(s) or search content 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 the 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 in the actual text.

For consistency and to prevent confusion, the terminology used in this guide is based on the ESET NOD32 Antivirus user interface. We also use a uniform set of symbols to highlight topics of specific interest or significance.

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

> **!** This requires your attention, and we encourage you not to skip over. Usually, it provides non-critical but important information.

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

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

Convention	Meaning
Bold type	Names of interface items such as boxes and option buttons.
Italic type	Placeholders for the information you provide. For example, filename or path means you type the actual path or a name of a 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 Online Help version will automatically display when you have a working internet connection.

Installation

There are several methods for installing ESET NOD32 Antivirus on your computer. Installation methods may vary depending on country and means of distribution:

- Live installer—Downloaded from the ESET website or CD/DVD. The installation package is universal for all languages (choose the appropriate language). The Live installer is a small file; additional files required to install ESET NOD32 Antivirus are downloaded automatically.

- Offline installation—Uses an .exe file larger than the Live installer file and does not require an internet connection or additional files to complete the installation.

⚠️ Make sure that no other antivirus programs are installed on your computer before you install ESET NOD32 Antivirus. 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 ESET Knowledgebase article for a list of uninstaller tools for common antivirus software (available in English and several other languages).

Live installer

When you have downloaded the Live installer installation package, double-click the installation file and follow the step-by-step instructions in the Installation Wizard.

⚠️ For this type of installation, you must be connected to the internet.
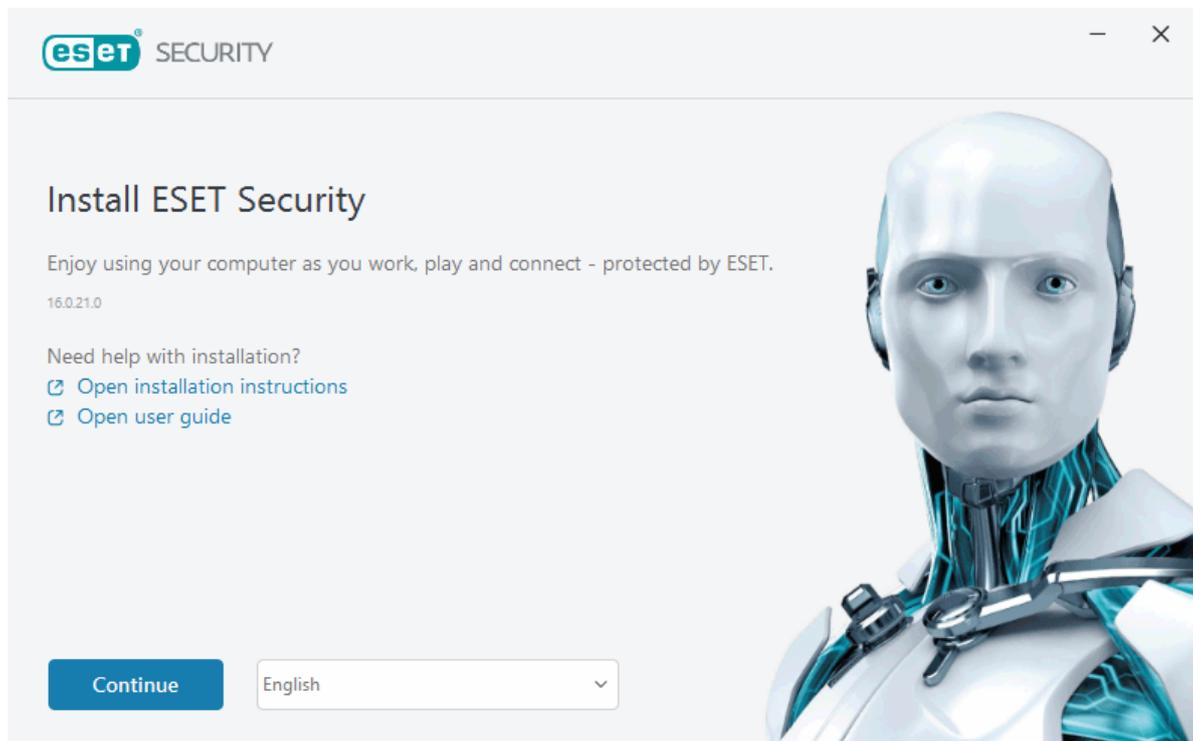
1. Select the appropriate language from the drop-down menu and click **Continue**.

> ℹ️ If you are installing a more recent version over the previous version with password-protected settings, type your password. You can configure the settings password in the Access setup.

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

- ESET LiveGrid® feedback system

- Potentially unwanted applications

- Customer Experience Improvement Program

> ℹ️ By clicking **Continue** or **Allow all and continue**, you accept the End User License Agreement and acknowledge the Privacy Policy.

3. To activate, manage and view the device's security using the ESET HOME, connect your device to the ESET HOME account. Click **Skip Login** to continue without connecting to ESET HOME. You can connect your device to your ESET HOME account later.

4. If you continue without connecting to ESET HOME, choose an activation option. When installing a more recent version over the previous version, your License Key is entered automatically.

5. The Installation Wizard determines which ESET product will be installed based on your license. The version with the most security features is always pre-selected. Click **Change product** if you want to install a different version of the ESET product. Click **Continue** to start the installation process. It may take a few moments.

> ℹ️ If there are any leftovers (files or folders) from ESET products uninstalled in the past, you will be prompted to allow their removal. Click **Install** to continue.

6. Click **Done** to exit the Installation Wizard.

⚠️ Installation troubleshooter.

> ℹ️ After the product is installed and activated, the modules start downloading. Protection is being initialized, and some features may not be fully functional unless the download is complete.

Offline installation

Download and install your ESET Windows home product using the offline installer (.exe) below. Choose which version of ESET home product to download (32-bit, 64-bit or ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
64-bit Download 32-bit Download ARM Download	64-bit Download 32-bit Download ARM Download	64-bit Download 32-bit Download ARM Download

> ⚠️ If you have an active internet connection, install your ESET product using a Live installer.

When you launch the offline installer (.exe), the Installation Wizard guides you through the setup process.

1. Select the appropriate language from the drop-down menu and click **Continue**.

> ℹ️ If you are installing a more recent version over the previous version with password-protected settings, type your password. You can configure the settings password in the Access setup.

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

- ESET LiveGrid® feedback system

- Potentially unwanted applications

9

- Customer Experience Improvement Program

> **i** By clicking **Continue** or **Allow all and continue**, you accept the End User License Agreement and acknowledge the Privacy Policy.

3. Click **Skip login**. When you have an internet connection, you can connect your device to your ESET HOME account.

4. Click **Skip activation**. ESET NOD32 Antivirus must be activated after the installation to be fully functional. Product activation requires an active internet connection.

5. The Installation Wizard shows which ESET product will be installed based on the downloaded offline installer. Click **Continue** to start the installation process. It may take a few moments.

> **i** If there are any leftovers (files or folders) from ESET products uninstalled in the past, you will be prompted to allow their removal. Click **Install** to continue.

6. Click **Done** to exit the Installation Wizard.

⚠ Installation troubleshooter.

Product activation

There are several methods available to activate your product. Availability of a specific activation scenario in the activation window may vary depending on the country and means of distribution (CD/DVD, ESET web page, etc.):

- If you purchased a retail boxed version of the product or received an email with license details, activate your product by clicking **Use a purchased License Key**. The License Key must be entered as supplied for activation to be successful. License Key is a unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX or XXXX-XXXXXXXX, which is used for identification of the license owner and for the activation. The License Key is usually located inside or on the backside of the product package.

- After selecting Use ESET HOME account you will be asked to log in to your ESET HOME account.

- To evaluate ESET NOD32 Antivirus before making a purchase, select Free trial. Type your email address and country to activate ESET NOD32 Antivirus for a limited time. Your trial license will be emailed to you. Trial licenses can only be activated once per customer.

- If you do not have a license and want to buy one, click **Purchase license**. This will redirect you to the website of your local ESET distributor. ESET Windows home product full licenses are not free.

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.

⚠ Failed product activation?

Entering your License Key during activation

Automatic updates are important for your security. ESET NOD32 Antivirus will only receive updates once activated.

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 license owner and activation of the license.

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

If you did not enter your License Key after installation, your product will not be activated. You can activate ESET NOD32 Antivirus in the main program window > **Help and support** > **Activate License**.

ESET Windows home product full licenses are not free.

Use ESET HOME account

Connect your device to ESET HOME to view and manage all your activated ESET licenses and devices. You can renew, upgrade or extend your license and view important license details. In the ESET HOME management portal or mobile app, you can add different licenses, download products to your devices, check the product security status, or share licenses through email. For more information, visit ESET HOME Online Help.
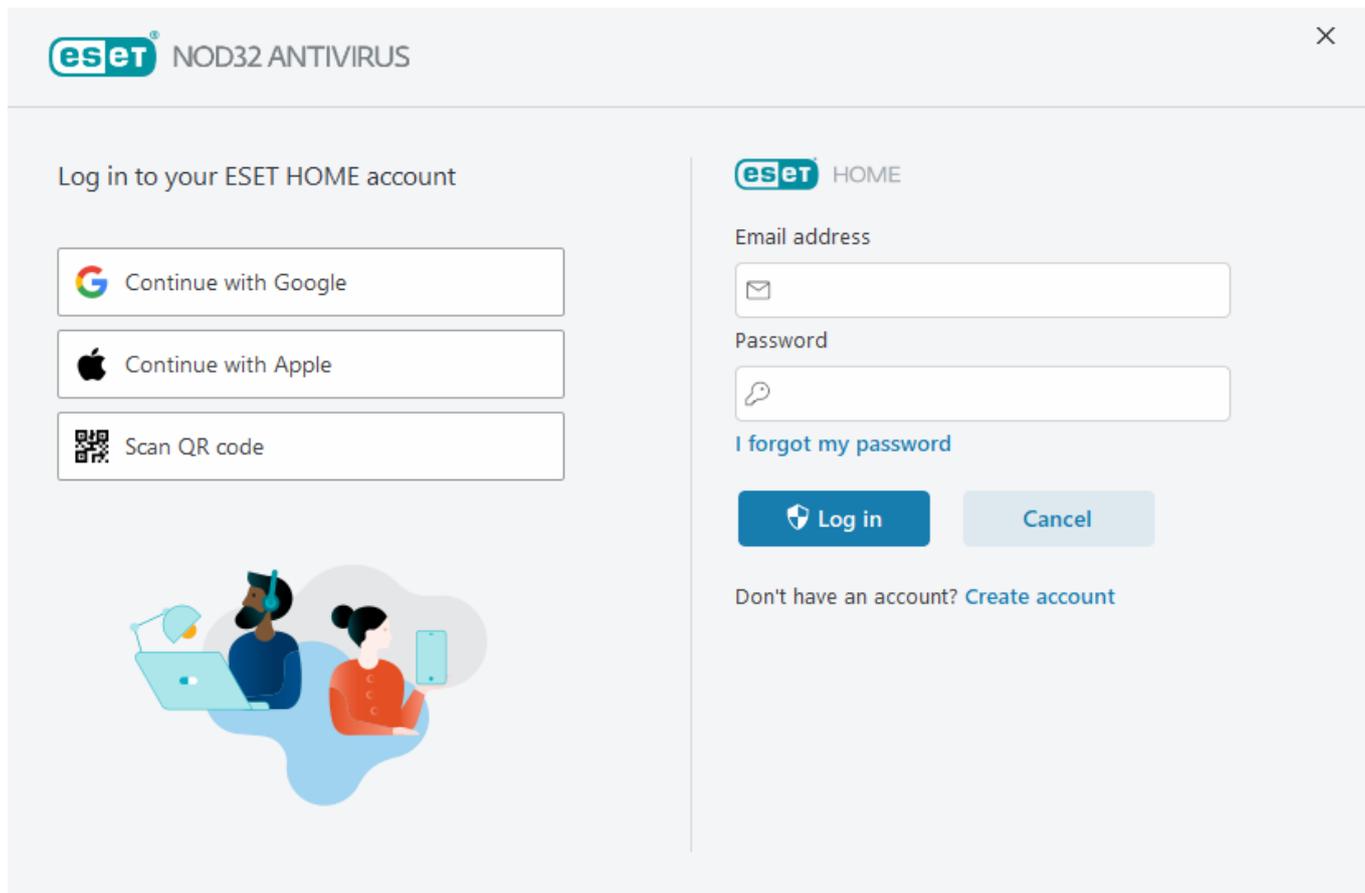
After selecting **Use ESET HOME account** as an activation method or when connecting to ESET HOME account during installation:

1. Log in to your ESET HOME account.

> ℹ️ If you do not have an ESET HOME account, click **Create account** to register or see instructions in the ESET HOME Online Help.
> If you forgot your password click **I forgot my password** and follow the on-screen steps or see instructions in the ESET HOME Online Help.

2. Set a **Device name** for your device that will be used in all ESET HOME services and click **Continue**.

3. Choose a license for activation or add a new license. Click **Continue** to activate ESET NOD32 Antivirus.

Activate Trial License

To activate your ESET NOD32 Antivirus trial version, type a valid email address into the **Email address** and **Confirm email address** fields. After activation, your ESET license will be generated and sent to your email. This email address will also be used for product expiration notifications and other communication with ESET. The trial can only be activated once.

Select your country from the **Country** drop-down menu to register ESET NOD32 Antivirus with your local distributor, who will provide technical support.

Free ESET License key

Full license for ESET NOD32 Antivirus is not free.

ESET license key is a unique sequence of letters and numbers separated by a dash, provided by ESET to allow the legal use of ESET NOD32 Antivirus in compliance with the End User License Agreement. Every End User is entitled to use the License key only to the extent in which has the right to use ESET NOD32 Antivirus based on the number of licenses granted by ESET. The License key is deemed confidential and cannot be shared; however, you can share the license seats using the ESET HOME.

There are sources on the internet that might provide you a "free" ESET license keys, but remember:

- Clicking on a "Free ESET license" ad can compromise your computer or device and can lead to becoming infected with malware. Malware can be hidden in unofficial web content (e.g., videos), websites that display ads to earn money based on your visits, etc. Usually, these are a trap.

- ESET can and does disable pirated licenses.

- Having a pirated license key is not aligned with the End User License Agreement that you must accept to install ESET NOD32 Antivirus.

- Buy ESET licenses only through official channels such as www.eset.com, ESET distributors or resellers (do not buy licenses from unofficial third-party websites like eBay or shared licenses from a third-party).

- Downloading the ESET NOD32 Antivirus is free, but activation during installation requires a valid ESET license key (you can download and install it, but without activation, it will not work).

- Do not share your license on the internet or social media (it might become widespread).

To identify and report a pirated ESET license, visit our Knowledgebase article for instructions.

If you are uncertain about buying an ESET Security product, you can use a trial version while you decide:

1. Activate ESET NOD32 Antivirus using a free trial license

2. Participate in ESET Beta Program

3. Install ESET Mobile Security if you are using Android mobile device, it is freemium.

To gain a discount / prolong your license, Renew your ESET.

Activation failed – common scenarios

If the activation of ESET NOD32 Antivirus is not successful, the most common scenarios are:

- License key is already in use.

- You have entered an invalid license key.

- Information in the activation form is missing or invalid.

- Communication with the activation server failed.

- No connection or disabled connection to ESET activation servers.

Verify that you entered the proper license key and your internet connection is active. Try to activate ESET NOD32 Antivirus again. If you use an ESET HOME account for activation, see the ESET HOME License Management - Online Help.

> ⓘ If you receive a specific error (for example, Suspended license or Overused license), follow the instructions in License status.

If you still cannot activate ESET NOD32 Antivirus, the ESET Activation Troubleshooter walks you through common questions, errors and problems about activation and licensing (available in English and several other languages).

License status

Your license can have different statuses. You can find your license status in ESET HOME. To add your license to your ESET HOME account, see Add a license.

> ⓘ If you do not have the ESET HOME account, you can Create a new ESET HOME account.

If the license status is other than **Active**, you will receive an error during activation or a notification in the main program window.

To disable license status notifications, open Advanced setup > **Notifications** > **Application statuses**. Click **Edit** next to **Application statuses**, expand **Licensing** and deselect the check box next to the notification you want to disable. Disabling the notification does not solve the issue.

See descriptions and recommended solutions for different license statuses in the table below:

License status	Description	Solution
Active	The license is valid, and there is no need for your interaction. ESET NOD32 Antivirus can be activated, and you can find the license details in the main program window > **Help and support**.	

License status	Description	Solution
Overused	More devices are using this license than allowed. You will receive an activation error.	See Activation failed due to overused license for more information.
Suspended	Your license was suspended due to payment issues. To use the license, ensure your payment details in ESET HOME are up to date or contact your license reseller. You can receive this error during activation or in the main program window.	Installed product—If you have the ESET HOME account, in the notification displayed in the main program window, click **Manage your license in ESET HOME** and review your payment details. Otherwise, contact your license reseller. Activation error—If you have the ESET HOME account, in the activation error window, click **Open ESET HOME** and review your payment details. Otherwise, contact your license reseller.
Expired	Your license has expired, and you are not able to use this license to activate ESET NOD32 Antivirus. You can receive this error during activation or in the main program window. If you have ESET NOD32 Antivirus already installed, your computer is not protected and updated.	Installed product—In the notification displayed in the main program window, click **Renew license** and follow the instructions in How do I renew my license?, or click **Activate product** and choose your activation method. Activation error—In the activation error window, click **Renew your license** and follow the instructions in How do I renew my license?, or type in a new or renewed license key and click **Renew license**.
Canceled	Your license has been canceled by ESET or by your license reseller.	If you receive an error: Canceled license in the main program window or during activation and your license should work properly, contact your license reseller.

Activation failed due to overused license

Issue

- Your license may be overused or abused

- Activation failed due to overused license

Solution

There are more devices using this license than it allows. You may be a victim of software piracy or counterfeiting. The license cannot be used to activate any other ESET product. You can solve this problem directly if you are allowed to manage the license in your ESET HOME account or purchased the license from a legitimate source. If you do not yet have an account, create one.

If you are a license owner and you were not prompted to type your email address:

1. To manage your ESET license, open a web browser and navigate to https://home.eset.com. Access ESET

License Manager and remove or deactivate seats. For more information, see [What to do in case of an overused license](#).

2. To identify and report a pirated ESET license, [visit our Identify and report pirated ESET licenses article](#) for instructions.

3. If you are unsure, click **Back** and [email ESET Technical Support](#).

If you are not a license owner, contact the owner of this license with information that you cannot activate the ESET product due to the license overuse. The owner can solve the problem in the [ESET HOME](#) portal.

If prompted to confirm your email address (several cases only), type the email address originally used to purchase or activate your ESET NOD32 Antivirus.

License upgrade

This notification window appears when the license used to activate your ESET product has changed. Your changed license enables you to activate a product with more security features. If no change has been performed, ESET NOD32 Antivirus will show an alert window once, called **Change to a product with more features**.

Yes (recommended)—will automatically install the product with more security features.

No, thanks—no changes will be made, and the notification will disappear permanently.

To change the product later, see our [ESET Knowledgebase article](#). For more information about ESET licenses, see [Licensing FAQ](#).

The table below details features available in each specific product.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detection engine	✔	✔	✔
Advanced Machine Learning	✔	✔	✔
Exploit Blocker	✔	✔	✔
Script-Based Attack Protection	✔	✔	✔
Anti-Phishing	✔	✔	✔
Web access protection	✔	✔	✔
HIPS (including Ransomware shield)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Network Inspector		✔	✔
Webcam Protection		✔	✔
Network Attack Protection		✔	✔
Botnet Protection		✔	✔
Banking & Payment Protection		✔	✔
Parental Control		✔	✔
Anti-Theft		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Product upgrade

You have downloaded a default installer and decided to change the product to be activated, or you want to change your installed product to one with more security features.

Change product during installation.

The table below details features available in each specific product.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detection engine	✔	✔	✔
Advanced Machine Learning	✔	✔	✔
Exploit Blocker	✔	✔	✔
Script-Based Attack Protection	✔	✔	✔
Anti-Phishing	✔	✔	✔
Web access protection	✔	✔	✔
HIPS (including Ransomware shield)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Network Inspector		✔	✔
Webcam Protection		✔	✔
Network Attack Protection		✔	✔
Botnet Protection		✔	✔
Banking & Payment Protection		✔	✔
Parental Control		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

License downgrade

This dialog window appears when the license used to activate your ESET product has changed. Your changed license can be used only with different ESET product with fewer security features. The product has been changed automatically to prevent protection loss.

For more information about ESET licenses, see Licensing FAQ.

The table below details features available in each specific product.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detection engine	✔	✔	✔
Advanced Machine Learning	✔	✔	✔
Exploit Blocker	✔	✔	✔
Script-Based Attack Protection	✔	✔	✔
Anti-Phishing	✔	✔	✔
Web access protection	✔	✔	✔
HIPS (including Ransomware shield)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Network Inspector		✔	✔
Webcam Protection		✔	✔
Network Attack Protection		✔	✔
Botnet Protection		✔	✔
Banking & Payment Protection		✔	✔
Parental Control		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Product downgrade

The product you have currently installed has more security features than the one you are about to activate.

The table below details features available in each specific product.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detection engine	✔	✔	✔
Advanced Machine Learning	✔	✔	✔
Exploit Blocker	✔	✔	✔
Script-Based Attack Protection	✔	✔	✔
Anti-Phishing	✔	✔	✔
Web access protection	✔	✔	✔
HIPS (including Ransomware shield)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Network Inspector		✔	✔
Webcam Protection		✔	✔
Network Attack Protection		✔	✔
Botnet Protection		✔	✔
Banking & Payment Protection		✔	✔
Parental Control		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Installation troubleshooter

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

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

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

First scan after installation

After installing ESET NOD32 Antivirus, a computer scan will start automatically after first successful update to check for malicious code.

You can also start a computer scan manually from the main program window > **Computer scan** > **Scan your computer**. For more information about computer scans, see Computer scan.
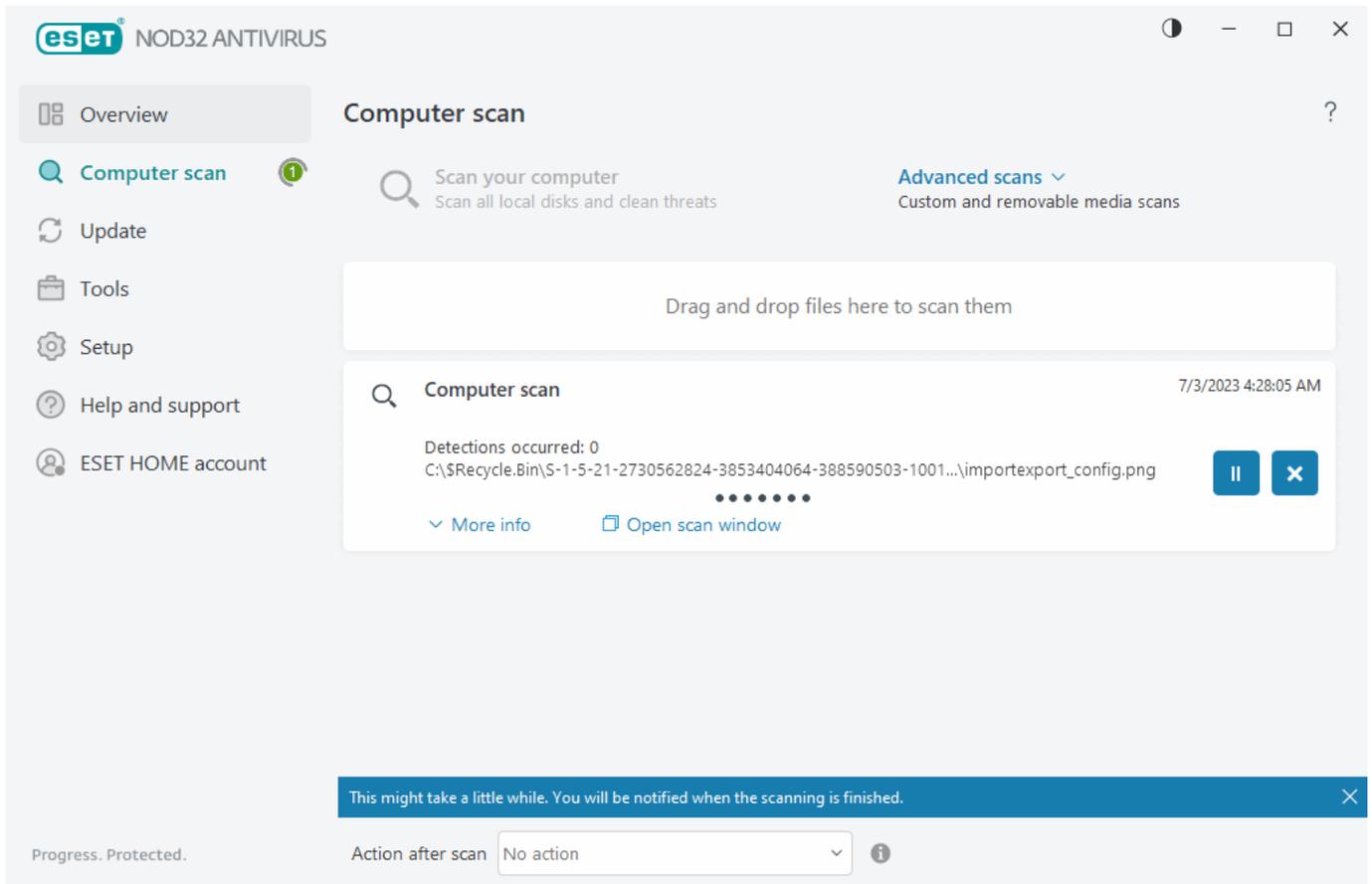
Upgrading to a more recent version

New versions of ESET NOD32 Antivirus are issued to implement improvements or fix issues that cannot be resolved by automatic updates to program modules. Upgrading to a later version can be accomplished in several ways:

1. Automatically, by means of a program update.
Since the program upgrade is distributed to all users and may have an impact on certain system configurations, it is issued after a long testing period to ensure functionality with all possible system configurations. If you need to upgrade to a later version immediately after its release, use one of the methods below.
Make sure that you have enabled **Application feature updates** in Advanced setup > **Update** > **Profiles** > **Updates**.

2. Manually, in the main program window by clicking **Check for updates** in the **Update** section.

3. Manually, by downloading and installing a more recent version over the previous one.

For additional information and illustrated instructions see:

- Update ESET Products—check for latest product modules

- What are the different ESET product update and release types?

Legacy product automatic upgrade

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

⚠ Common installation problems

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

To finish the installation:

1. Click **Accept and continue** to accept the End User License Agreement and acknowledge the Privacy Policy. If you do not agree with the End User License Agreement, click **Uninstall**. You cannot revert to the previous version.

2. Click **Allow all and continue** to allow both ESET LiveGrid® feedback system and Customer Experience Improvement Program or click **Continue** if you do not want to participate.

3. After activating the new ESET product with your License Key, the Overview page will be displayed. If your license information is not found, continue with a new trial license. If your license used in the previous product is not valid, activate your ESET product.

4. A device restart is required to complete the installation.

ESET NOD32 Antivirus will be installed

This dialog window can be displayed:

- During the installation process—Click **Continue** to install ESET NOD32 Antivirus.

- When changing a license in ESET NOD32 Antivirus—Click **Activate** to change the license and activate ESET NOD32 Antivirus.

According to your ESET license, the **Change product** option enables you to switch between ESET Windows home products. See Which product do I have? for more information.

Change to a different product line

According to your ESET license, you can switch between various ESET Windows home products. See Which product do I have? for more information.

Registration

Register your license by completing the fields contained in the registration form and clicking Activate. The fields marked as required are mandatory. The information you provide will only be used for matters involving your ESET license.

Activation progress

Allow a few seconds for the activation process to complete (required time may vary depending on your internet connection speed or computer).

Activation successful

The Activation process is complete.

A module update will start in a few seconds. Regular updates of ESET NOD32 Antivirus will begin immediately.

An initial scan will start automatically within 20 minutes after the module update.

Beginner's guide

This chapter provides an initial overview of ESET NOD32 Antivirus and its basic settings.

System tray icon

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

Pause protection—Displays the confirmation dialog box that disables the Detection engine, which guards against malicious system attacks by controlling file, web and email communication. The **Time interval** drop-down menu enables you to specify how long the protection will be disabled.
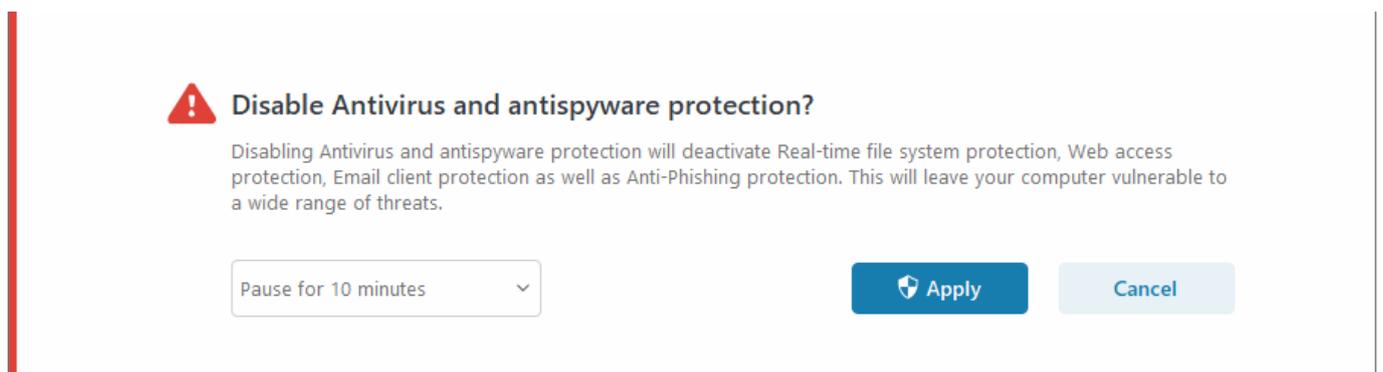
Advanced setup—Opens the ESET NOD32 Antivirus Advanced setup. To open Advanced setup from the main product window, press F5 on your keyboard or click **Setup** > **Advanced setup**.

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

Open ESET NOD32 Antivirus—Opens the ESET NOD32 Antivirus main program window.

Reset window layout—Resets the ESET NOD32 Antivirus's window to its default size and position on the screen.

Color mode—Opens User Interface settings where you can change the color of the GUI.

Check for updates—Starts a module or product update to ensure you are protected. ESET NOD32 Antivirus checks for updates automatically several times a day.

About—Provides system information, details about the installed version of ESET NOD32 Antivirus, installed program modules and information about the operating system and system resources.

Keyboard shortcuts

For better navigation in ESET NOD32 Antivirus, you can use the following keyboard shortcuts:

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

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

Profiles

Profile manager is used in two places within ESET NOD32 Antivirus—In the **On-demand scan** section and in the **Update** section.

Computer scan

There are 4 pre-defined scan profiles in ESET NOD32 Antivirus:

- **Smart scan**—This is the default advanced scanning profile. The Smart scan profile uses Smart Optimization technology, which excludes files that were found to be clean in a previous scan and have not been modified since that scan. This allows for lower scan times with a minimal impact to system security.

- **Context menu scan**—You can start an on-demand scan of any file from the context menu. The Context menu scan profile enables you to define a scan configuration that will be used when you trigger the scan this way.

- **In-depth scan**—The In-depth scan profile does not use Smart optimization by default, so no files are excluded from scanning using this profile.

- **Computer scan**—This is the default profile used in the standard computer scan.

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

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

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

Update

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

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

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

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

Updates

Regularly updating ESET NOD32 Antivirus is the best method to ensure the maximum level of security on your computer. The Update module ensures that both the program modules and the system components are always up to date.

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

In addition to automatic updates, you can click **Check for updates** to trigger a manual update.
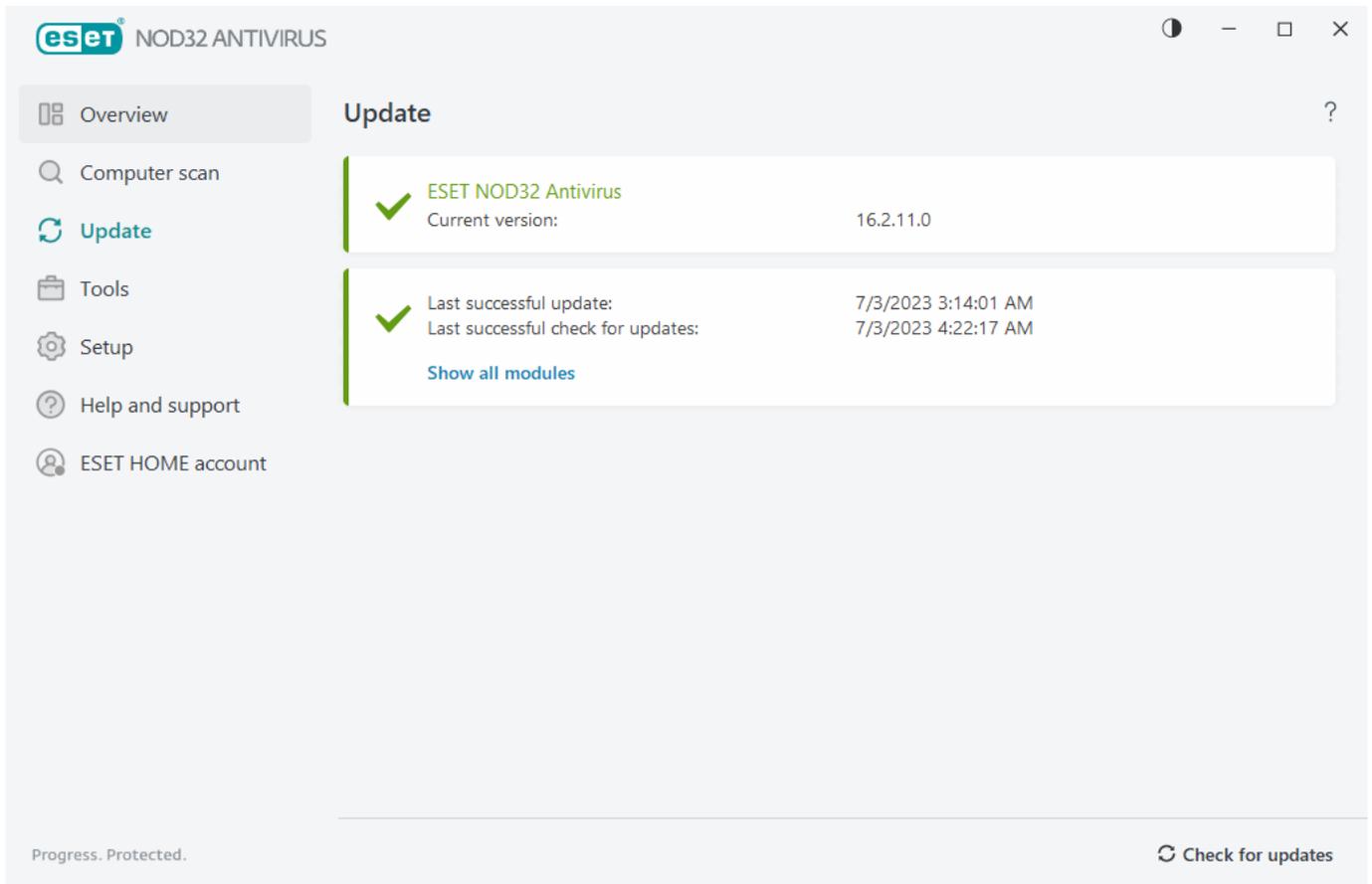
[Advanced setup](#) > **Update** contains additional update options such as update mode, proxy server access and LAN connections.

If you experience problems with an update, click **Clear** to clear the update cache. If you still cannot update program modules, see the [Troubleshooting for "Modules update failed" message](#) section.
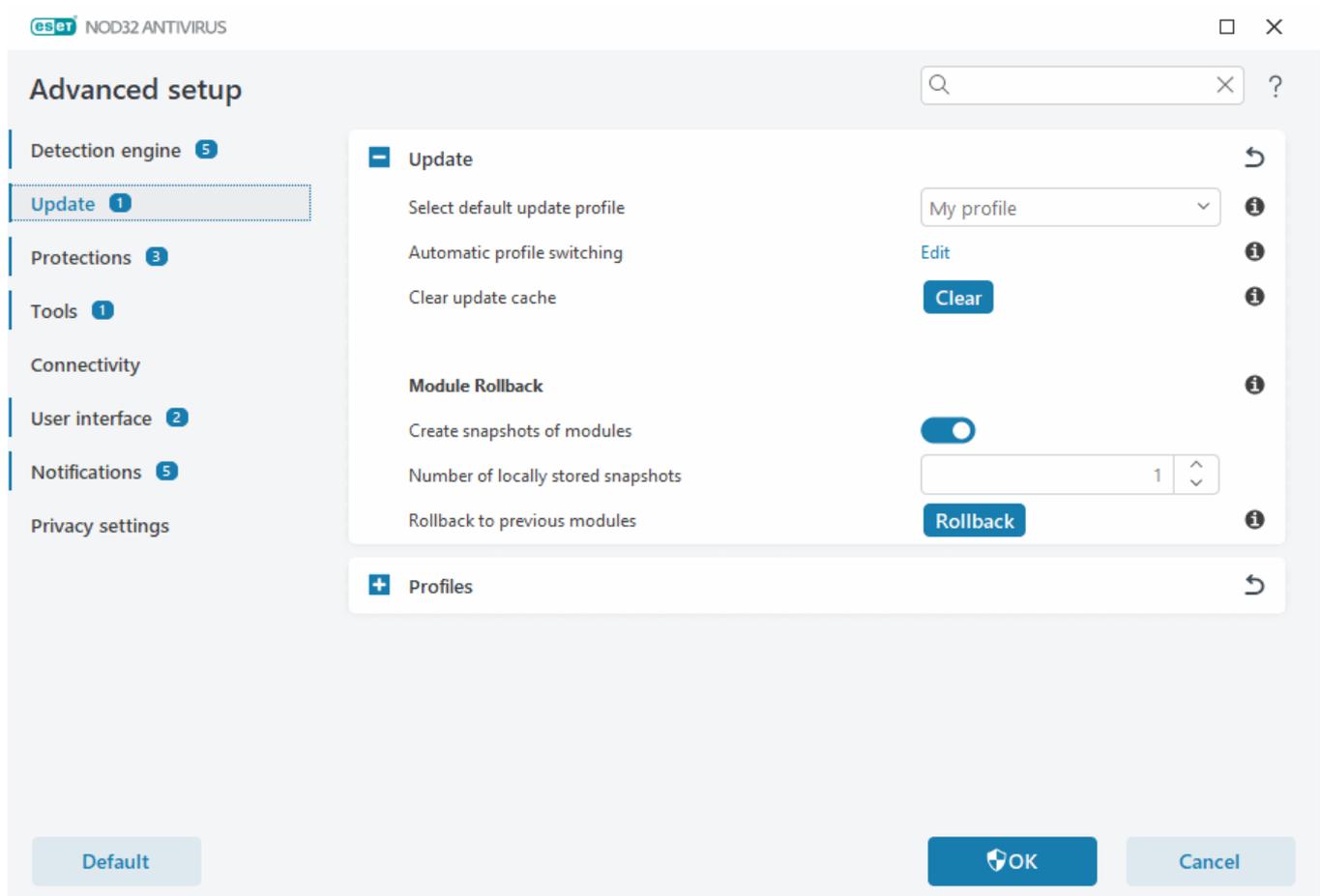
Working with ESET NOD32 Antivirus

The ESET NOD32 Antivirus main program window is split into two sections. The primary window on the right displays information corresponding to the option selected from the main menu on the left.

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

You can select the color scheme of ESET NOD32 Antivirus GUI in the top right corner of the main program window. Click the **Color scheme** icon (the icon changes based on the currently selected color scheme) next to **Minimize** icon and select the color scheme from the drop-down menu:

- **Same as the system color**—Sets the color scheme of ESET NOD32 Antivirus based on your operating system settings.

- **Dark**—ESET NOD32 Antivirus will have a dark color scheme (dark mode).

- **Light**—ESET NOD32 Antivirus will have a standard, light color scheme.
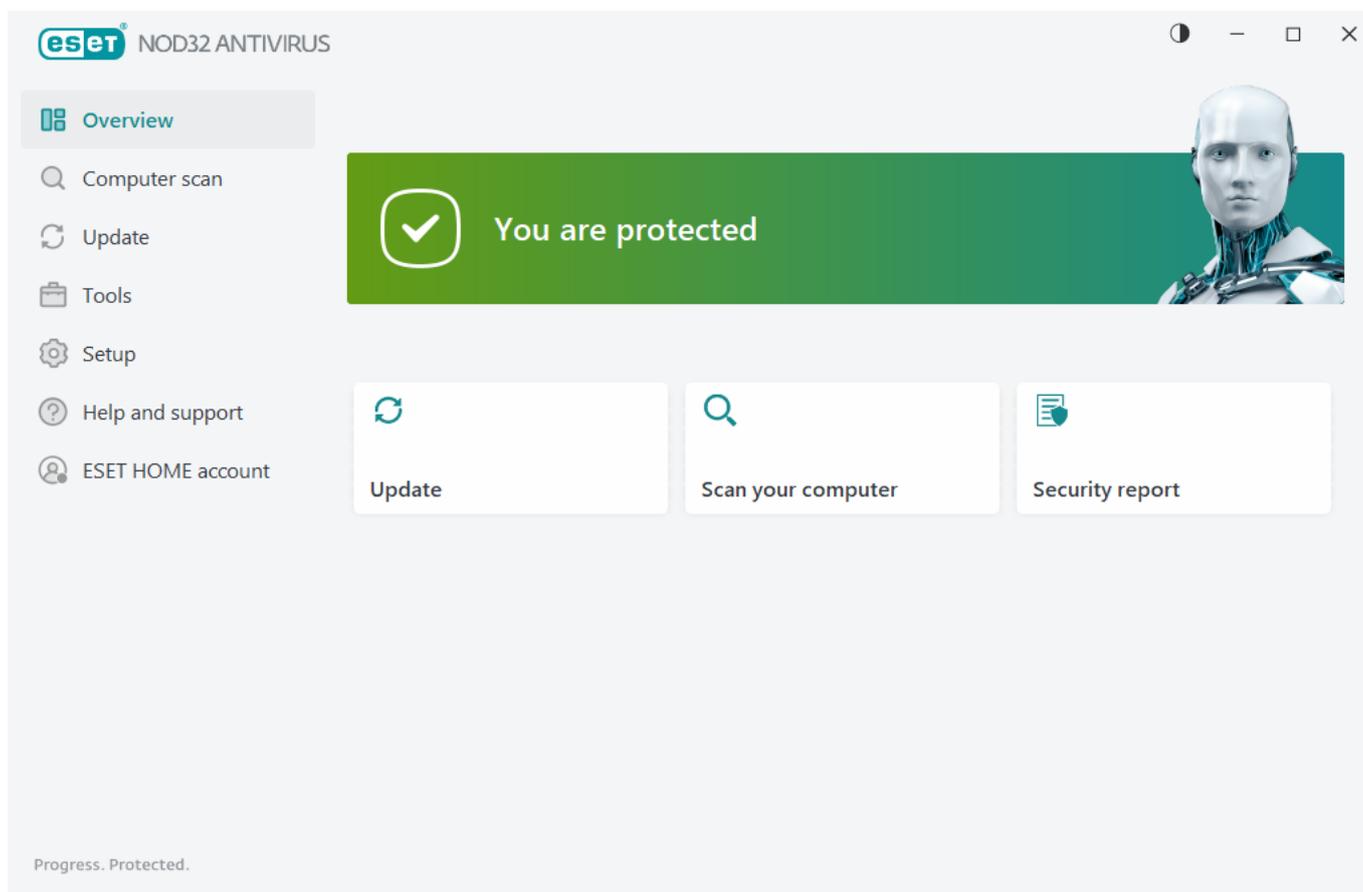
Main menu options:

Overview—Provides information about the protection status of ESET NOD32 Antivirus.

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

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

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

Setup—Provides configuration options for the ESET NOD32 Antivirus protection features (Computer protection and Internet protection) and access to Advanced setup.

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

ESET HOME account—Connect your device to ESET HOME or review the ESET HOME account connection status. Use ESET HOME to view and manage your activated ESET licenses and devices.

Overview

The **Overview** window displays information about your computer's current protection together with quick links to the security features in ESET NOD32 Antivirus.

The **Overview** window displays notifications with detailed information and recommended solutions to improve the security of ESET NOD32 Antivirus, turn on additional features, or ensure maximum protection. If there are

more notifications, click **X more notifications** to expand all.

Update—Opens the Update page and checks for updates.

Scan your computer—Opens the Computer scan page and starts a standard computer scan.

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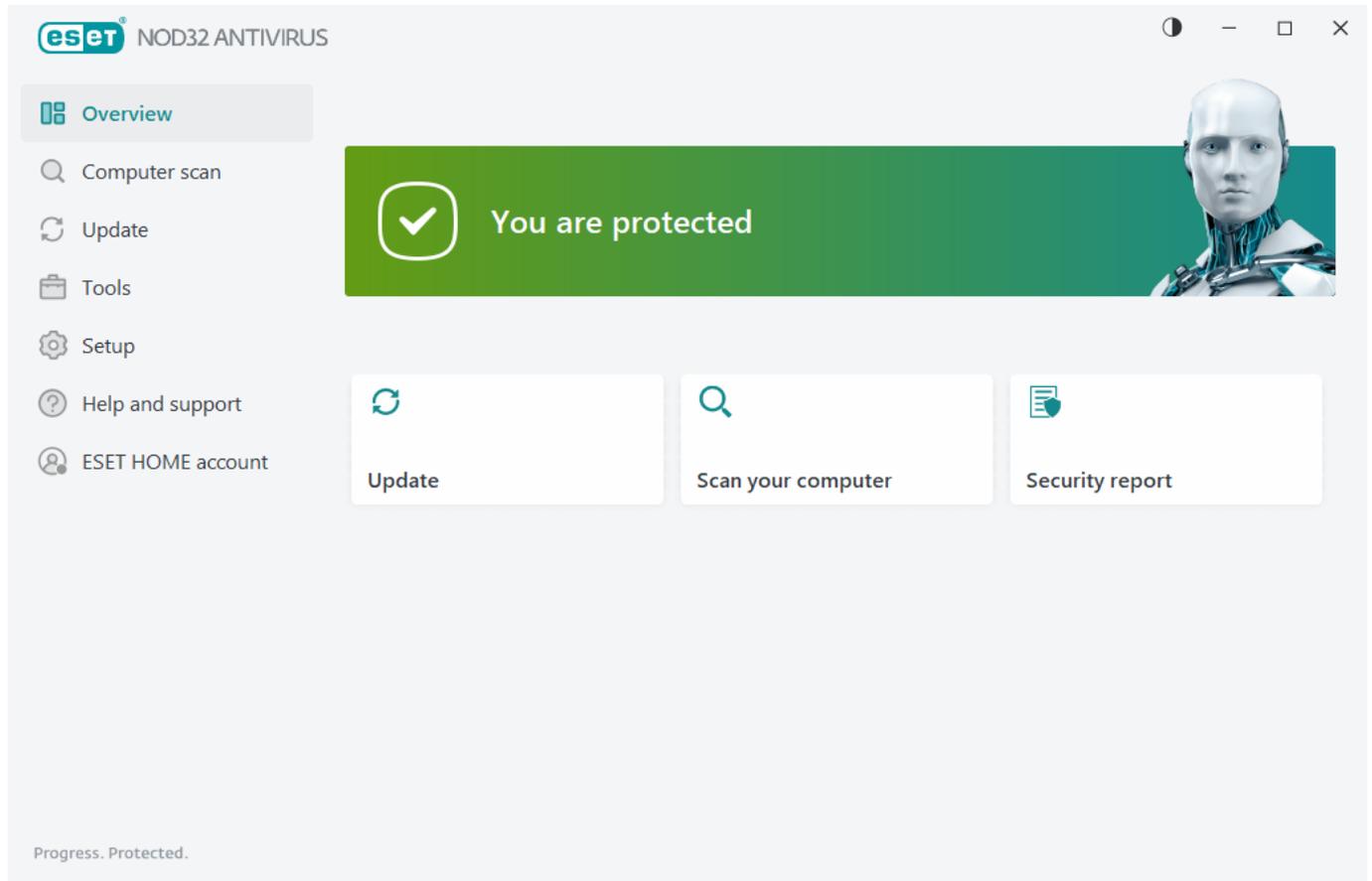
 The green icon and green **You are protected** status indicate that maximum protection is ensured.

What to do if the program doesn't work properly?

If an active protection module is working properly its protection status icon will be green. A red exclamation point or orange notification icon indicates that maximum protection is not ensured. Additional information about the protection status of each module, as well as suggested solutions for restoring full protection, are displayed as a notification in the **Overview** window. To change the status of individual modules, click **Setup** and select the desired module.

![Security alert screenshot]
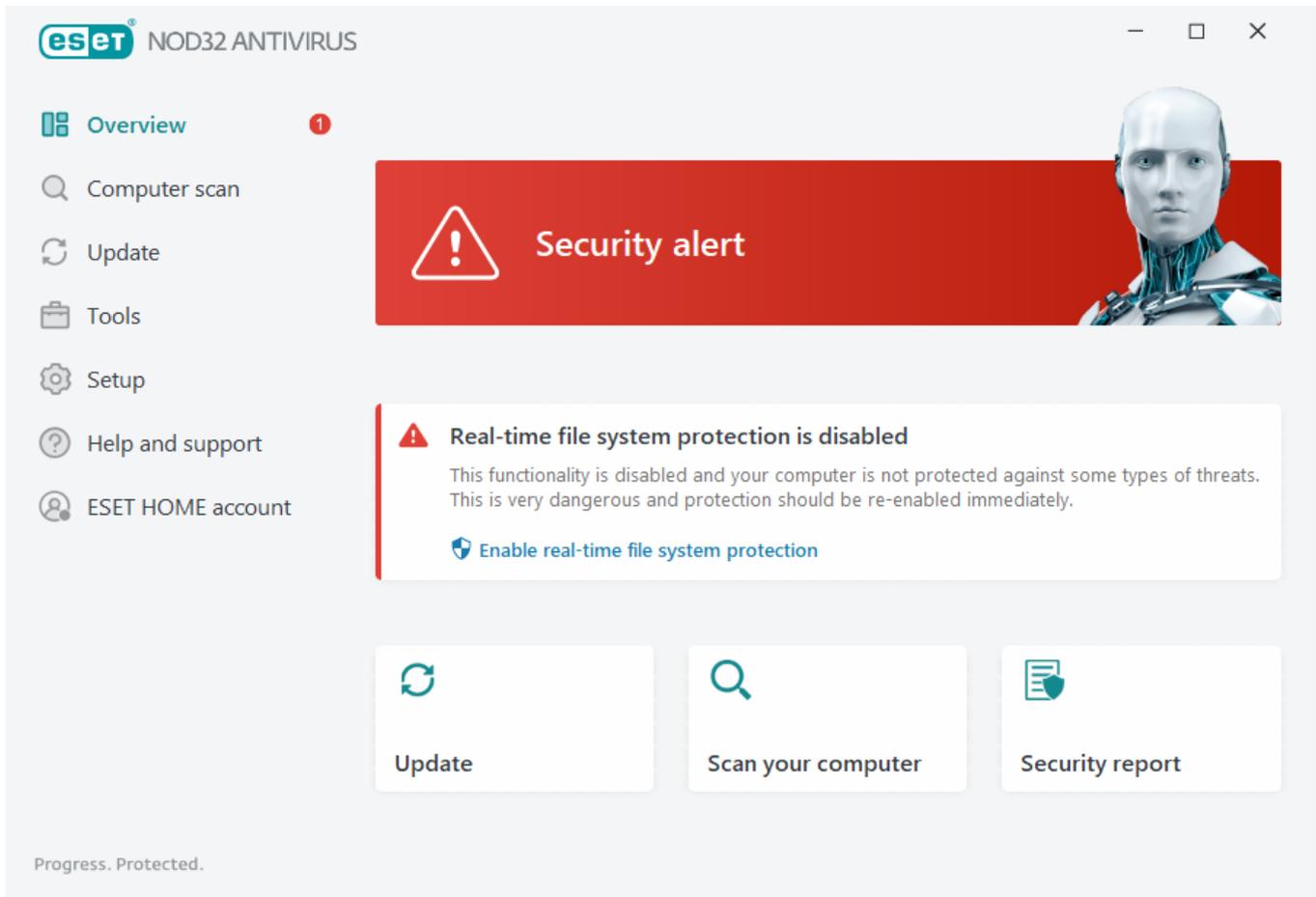
The red icon and red **Security alert** status indicate critical problems.
There are several reasons this status may be displayed, for example:

- **Product 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.

- **Detection engine is out of date**—This error will appear after several unsuccessful attempts to update the detection engine. 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.

- **Real-time file system protection is disabled**—Real-time protection was disabled by the user. Your computer is not protected against threats. Click **Enable Real-time file system protection** re-enable this functionality.

- **Antivirus and antispyware protection disabled**—You can re-enable antivirus and antispyware protection by clicking **Enable antivirus and antispyware protection**.

The orange icon indicates limited protection. For example, there might be a problem updating the program or your license may be nearing its expiration date.
There are several reasons this status may be displayed, for example:

- **Gamer mode active**—Enabling Gamer mode is a potential security risk. Enabling this feature disables all notification/alert windows and stops any scheduled tasks.

- **Your license expires soon/Your license expires today**—This is indicated by the protection status icon displaying an exclamation point next to the system clock. After your license expires, the program will

not be able to update and the Protection status icon will turn red.

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

Computer scan

The On-demand scanner is an important part of your antivirus solution. It is used to perform scans of files and folders on your computer. From a security standpoint, it is essential that computer scans are performed regularly as part of routine security measures, not just when an infection is suspected. We recommend that you perform regular in-depth scans of your system to detect viruses that are not captured by Real-time file system protection when they are written to the disk. This can happen if Real-time file system protection is disabled at the time, the detection engine is obsolete, or the file is not detected as a virus when it is saved to the disk.
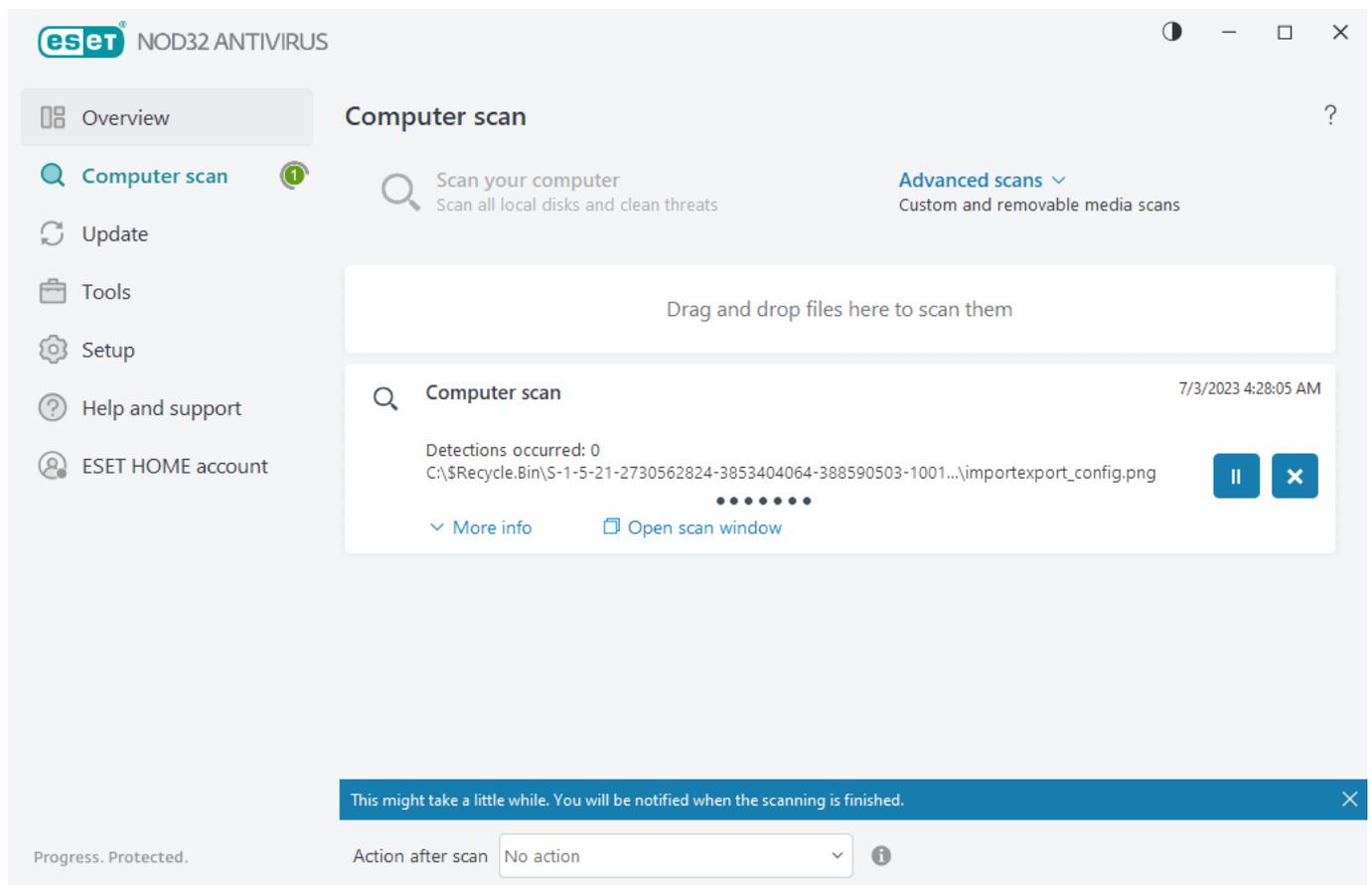
Two types of **Computer scan** are available. **Scan your computer** quickly scans the system without specifying scan parameters. **Custom scan** (under Advanced scans) enables you to select from pre-defined scan profiles designed to target specific locations and choose specific scan targets.

See Scan progress for more information about the scanning process.

> ℹ️ By default, ESET NOD32 Antivirus attempts to clean or delete detections found during the computer scan automatically. In some cases, if no action can be performed, you receive an interactive alert and must select a cleaning action (for example, delete or ignore). To change the cleaning level and for more detailed information, see Cleaning. To review previous scans, see Log files.

🔍 Scan your computer

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

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

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

🔍 Custom scan

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

🔍 Removable media scan

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

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

🔍 Repeat last scan

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

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

- **No action**—After a scan finishes, no action will be performed.

- **Shut down**—The computer turns off after a scan finishes.

- **Restart if needed**—The computer restarts if only needed to complete cleaning of detected threats.

- **Restart**—Closes all open programs and restarts the computer after a scan finishes.

- **Force restart if needed**—The computer forces restart if only needed to complete cleaning of detected threats.

- **Force restart**— Forces closing of all open programs without waiting for user interaction and restarts the computer after a scan finishes.

- **Sleep**—Saves your session and puts the computer in a low-power state so that you can quickly resume working.

- **Hibernate**—Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down but will resume its previous state the next time you start it.

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

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

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

Custom scan launcher

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

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

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

- **Operating memory**—Scans all processes and data currently used by operating memory.

- **Boot sectors/UEFI**—Scans Boot sectors and UEFI for the presence of malware. Read more about the UEFI scanner in the glossary.

- **WMI database**—Scans the whole Windows Management Instrumentation (WMI) database, all namespaces, class instances, and properties. Searches for references to infected files or malware embedded as data.

- **System registry**—Scans the whole system registry, all keys, and subkeys. Searches for references to infected files or malware embedded as data. When cleaning the detections, the reference remains in the registry to ensure important data is not lost.

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

> ℹ️ How to schedule a weekly computer scan
> To schedule a regular task, see How to schedule a weekly computer scan.
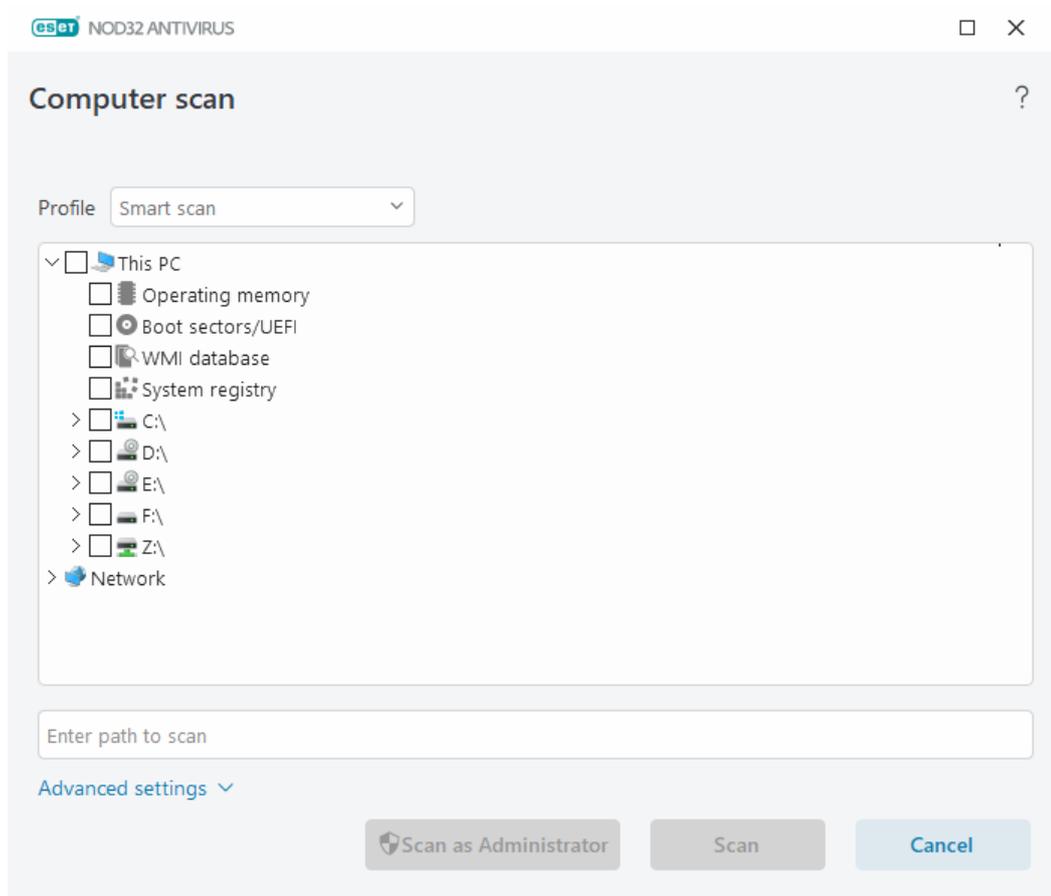
You can configure cleaning parameters for the scan in [Advanced setup](#) > **Detection engine** > **Malware scans** > **On-demand scan** > **ThreatSense** > **Cleaning**. To run a scan with no cleaning action, click **Advanced settings** and select **Scan without cleaning**. Scan history is saved to the scan log.

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

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

Scan as Administrator enables you to execute the scan under the Administrator account. Use this if the current user does not have privileges to access the files you want to scan. This button is not available if the current user cannot call UAC operations as an Administrator.

> ℹ️ 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.

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

> ℹ️ How to schedule a weekly computer scan
> To schedule a regular task, see [How to schedule a weekly computer scan](#).

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

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

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

Click More info to show the following information:

- **User**—Name of the user account which started the scan.

- **Objects scanned**—Number of already scanned objects.

- **Duration**—Time elapsed.

Pause icon—Pauses a scan.

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

Stop icon—Terminates the scan.

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

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

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

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

finishes:

- **No action**—After a scan finishes, no action will be performed.

- **Shut down**—The computer turns off after a scan finishes.

- **Restart if needed**—The computer restarts if only needed to complete cleaning of detected threats.

- **Restart**—Closes all open programs and restarts the computer after a scan finishes.

- **Force restart if needed**—The computer forces restart if only needed to complete cleaning of detected threats.

- **Force restart**— Forces closing of all open programs without waiting for user interaction and restarts the computer after a scan finishes.

- **Sleep**—Saves your session and puts the computer in a low-power state so that you can quickly resume working.

- **Hibernate**—Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down but will resume its previous state the next time you start it.

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

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

Computer scan log

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

- Version of detection engine

- Starting date and time

- List of scanned disks, folders, and files

- Scheduled scan name (scheduled scan only)

- User who started the scan.

- Scan status

- Number of scanned objects

- Number of detections found

- Time of completion

• Total scanning time

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

To find previous scan logs, in the [main program window](#), select **Tools** > **Log files**. In the drop-down menu, select **Computer scan** and double-click the desired record.
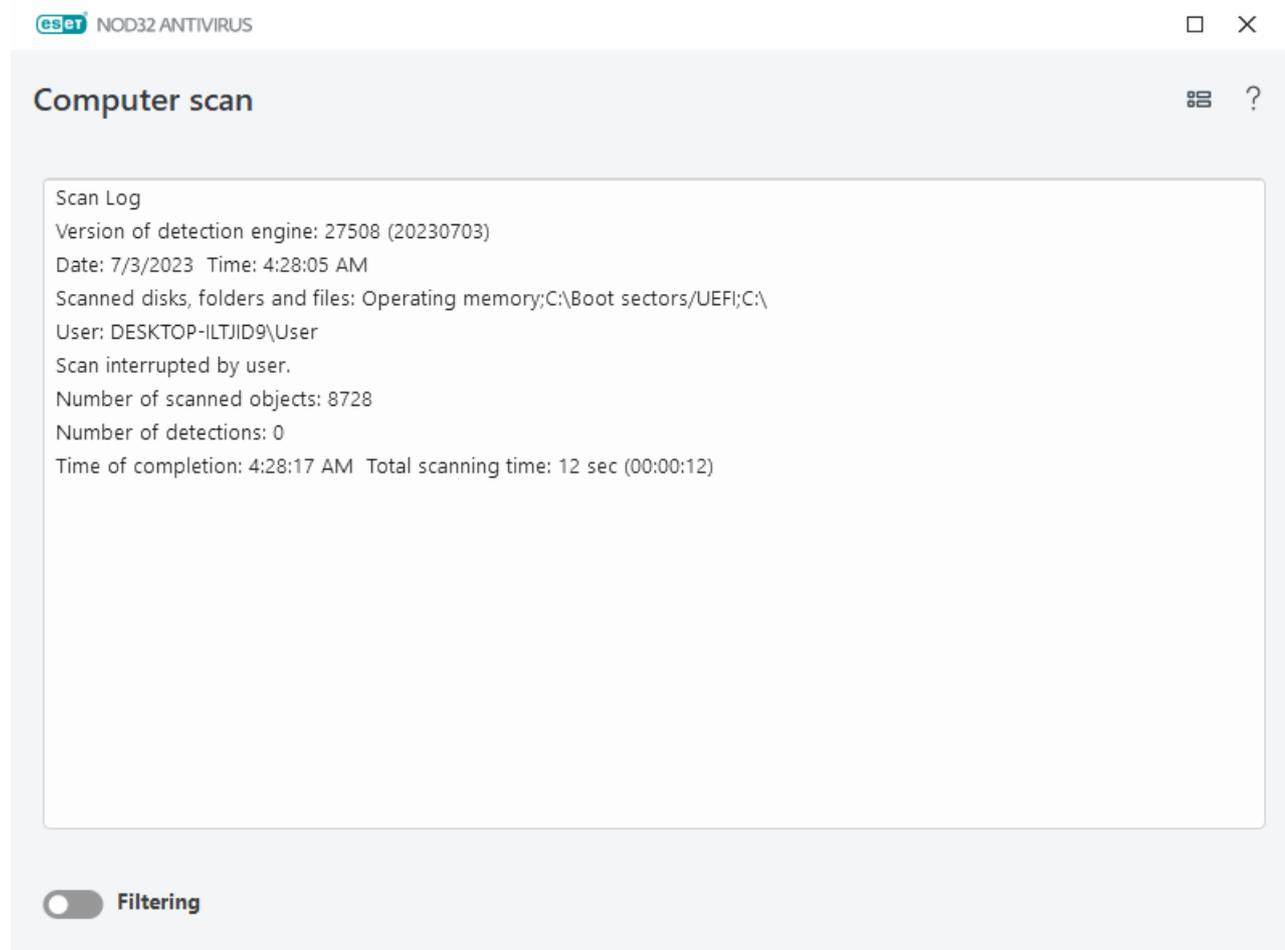
> ⓘ To learn more about "unable to open", "error opening" and/or "archive damaged" records, see our [ESET Knowledgebase article](#).

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

Action	Usage
Filter same records	Activates the log filtering. The log will show only records of the same type as the selected one.
Filter	This option opens the Log filtering window and enables you to define criteria for specific log entries. Shortcut: `Ctrl+Shift+F`
Enable filter	Activates the filter settings. If you activate the filter for the first time, you must define settings, and the Log filtering window opens.
Disable filter	Turns the filter off (same as clicking the switch at the bottom).
Copy	Copies highlighted record(s) into clipboard. Shortcut: `Ctrl+C`

Action	Usage
Copy all	Copies all records in the window.
Export	Exports highlighted record(s) into clipboard to an XML file.
Export all	This option exports all records in the window to an XML file.
Detection description	Opens the ESET Threat Encyclopedia, which contains detailed information about the dangers and symptoms of the highlighted infiltration.

Update

Regularly updating ESET NOD32 Antivirus is the best method to ensure the maximum level of security on your computer. The Update module ensures that both the program modules and the system components are always up-to-date.

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

In addition to automatic updates, you can click **Check for updates** to trigger a manual update. Regularly updating the program modules and components is an important aspect of maintaining complete protection against malicious code. Please pay attention to the product modules configuration and operation. You must activate your product by using your License key to receive updates. If you did not do so during installation, you will need to activate ESET NOD32 Antivirus to access ESET update servers. Your License key was sent to you in an email from ESET after purchasing ESET NOD32 Antivirus.
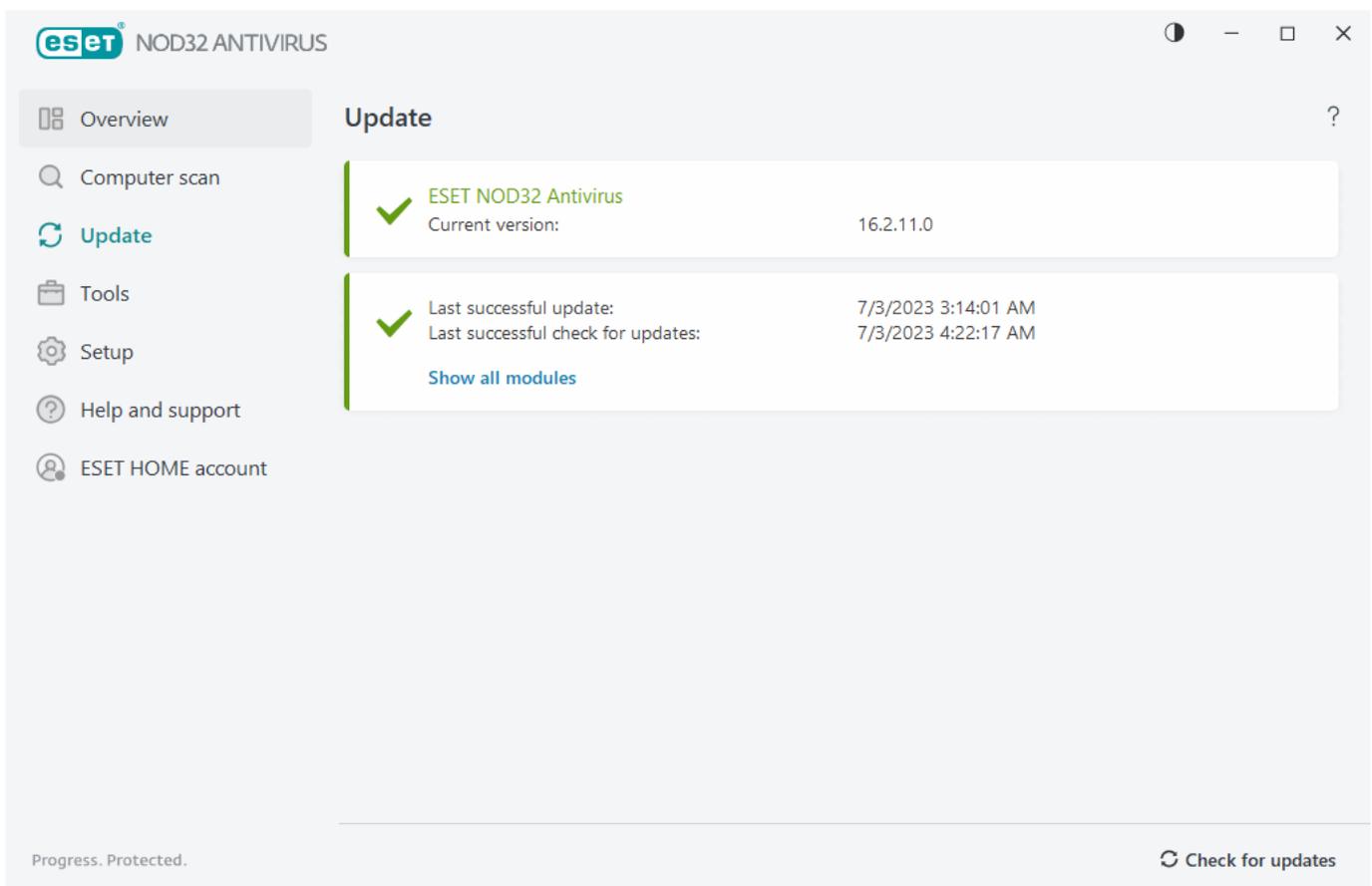
Current version—Shows the version number of the current product version you have installed.

Last successful update—Shows the date of the last successful update. If you do not see a recent date, your product modules may not be current.

Last successful check for updates—Shows the date of the last successful check for updates.

Show all modules—Shows the list of installed program modules.

Click **Check for updates** to check for the latest available version of ESET NOD32 Antivirus.

Update process

After clicking **Check for updates**, the download will begin. A download progress bar and remaining time to download will be displayed. To interrupt the update, click **Cancel update**.
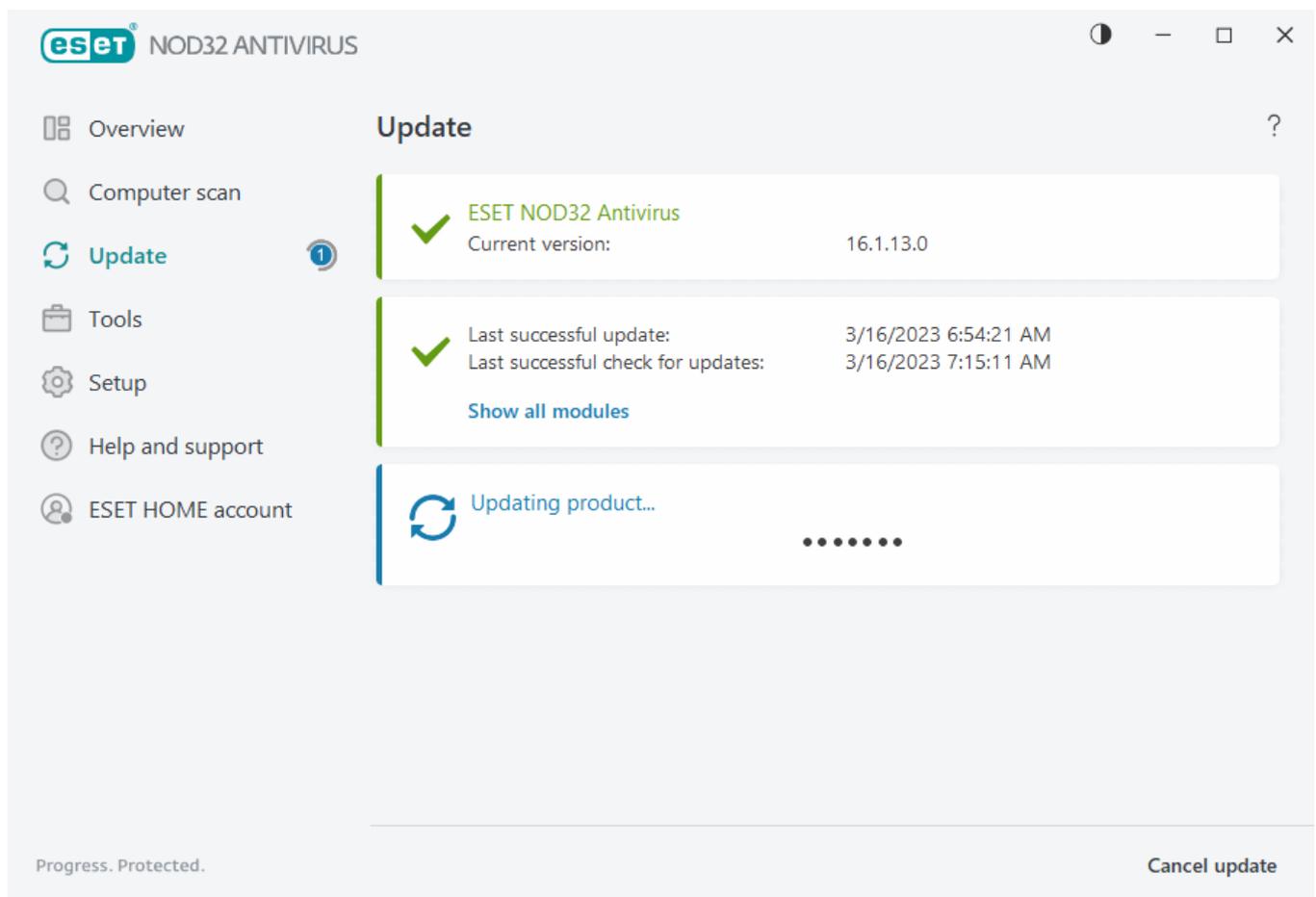
> Under normal circumstances, you will see the green check mark in the **Update** window, indicating that the program is up-to-date. If you do not see a green check mark, the program is out-of-date and is more vulnerable to infection. Please update the program modules as soon as possible.

Unsuccessful update

If you receive a modules update failed message, it may be caused by the following issues:

1. **Invalid license**—The license used for activation is invalid or has expired. In the main program window, click **Help and support** > **Change license** and activate your product.

2. **An error occurred while downloading update files**—This can be caused by 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, likely 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.
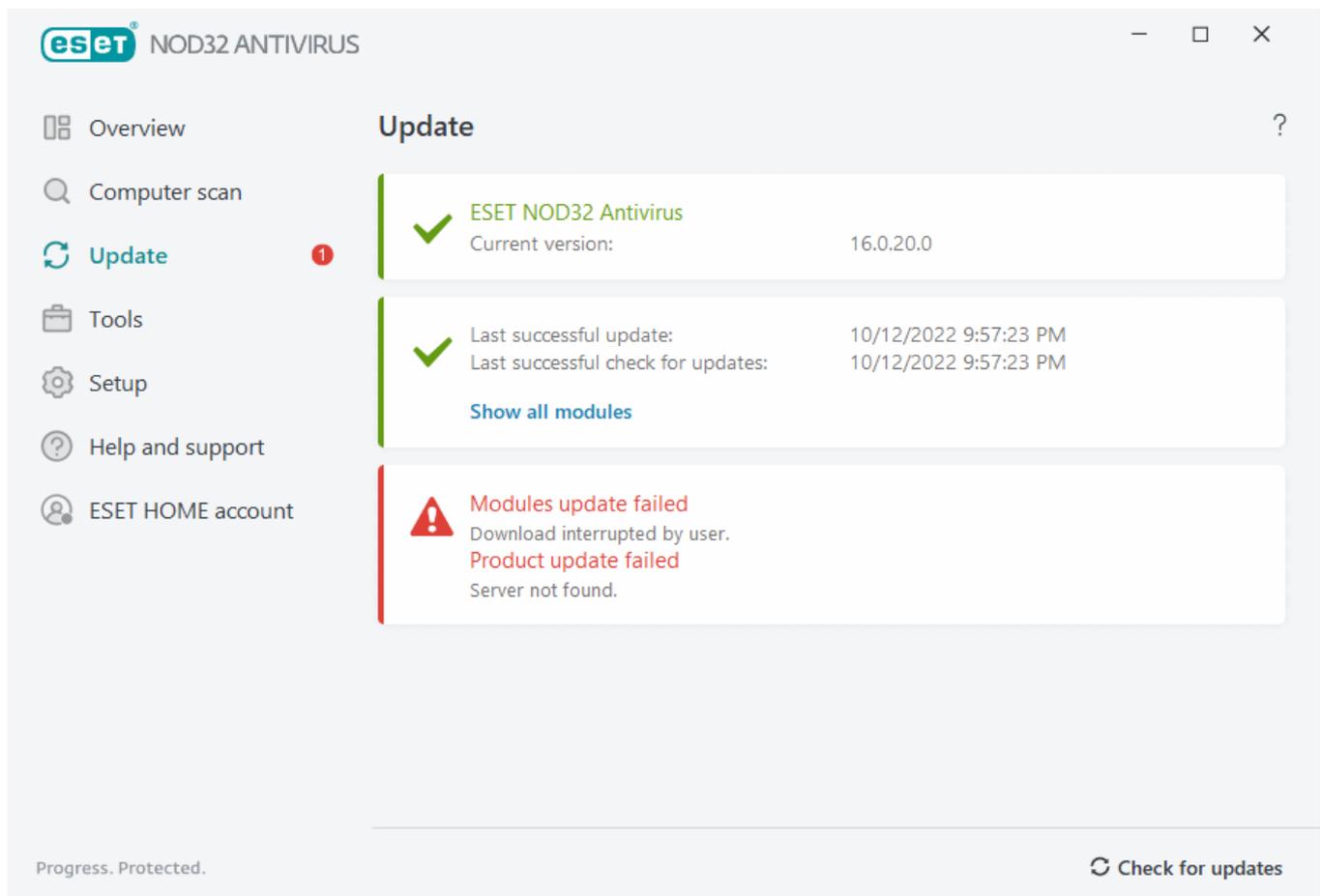
⚠️ You must restart your computer after a successful ESET NOD32 Antivirus update to a later product version to ensure that all program modules were updated correctly. It is not necessary to restart your computer after regular modules updates.

ℹ️ For more information, please visit Troubleshooting for "Modules update failed" message.

Dialog window - Restart required

A computer restart is required after updating the ESET NOD32 Antivirus to a new version. New versions of ESET NOD32 Antivirus are issued to implement improvements or fix issues that automatic updates of program modules cannot resolve.

The new version of ESET NOD32 Antivirus can be installed automatically, based on your program update settings, or manually by downloading and installing a newer version over the previous one.

Click **Restart now** to restart your computer. If you plan to restart your computer later, click **Remind me later**.

Later, you can restart your computer manually from the **Overview** screen in the [main program window](#).

How to create update tasks

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

Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following update tasks are activated in ESET NOD32 Antivirus:

- **Regular automatic update**

- **Automatic update after user logon**

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

Tools

The **Tools** menu includes features that offer additional security and help to simplify ESET NOD32 Antivirus administration. The following tools are available:

[Log files](#)

[Running processes](#) (if ESET LiveGrid® is enabled in ESET NOD32 Antivirus)

[Security report](#)

[ESET SysInspector](#)

[Scheduler](#)

[System cleaner](#)

[Submit sample for analysis](#) (may not be available based on your [ESET LiveGrid®](#) configuration).

[Quarantine](#)
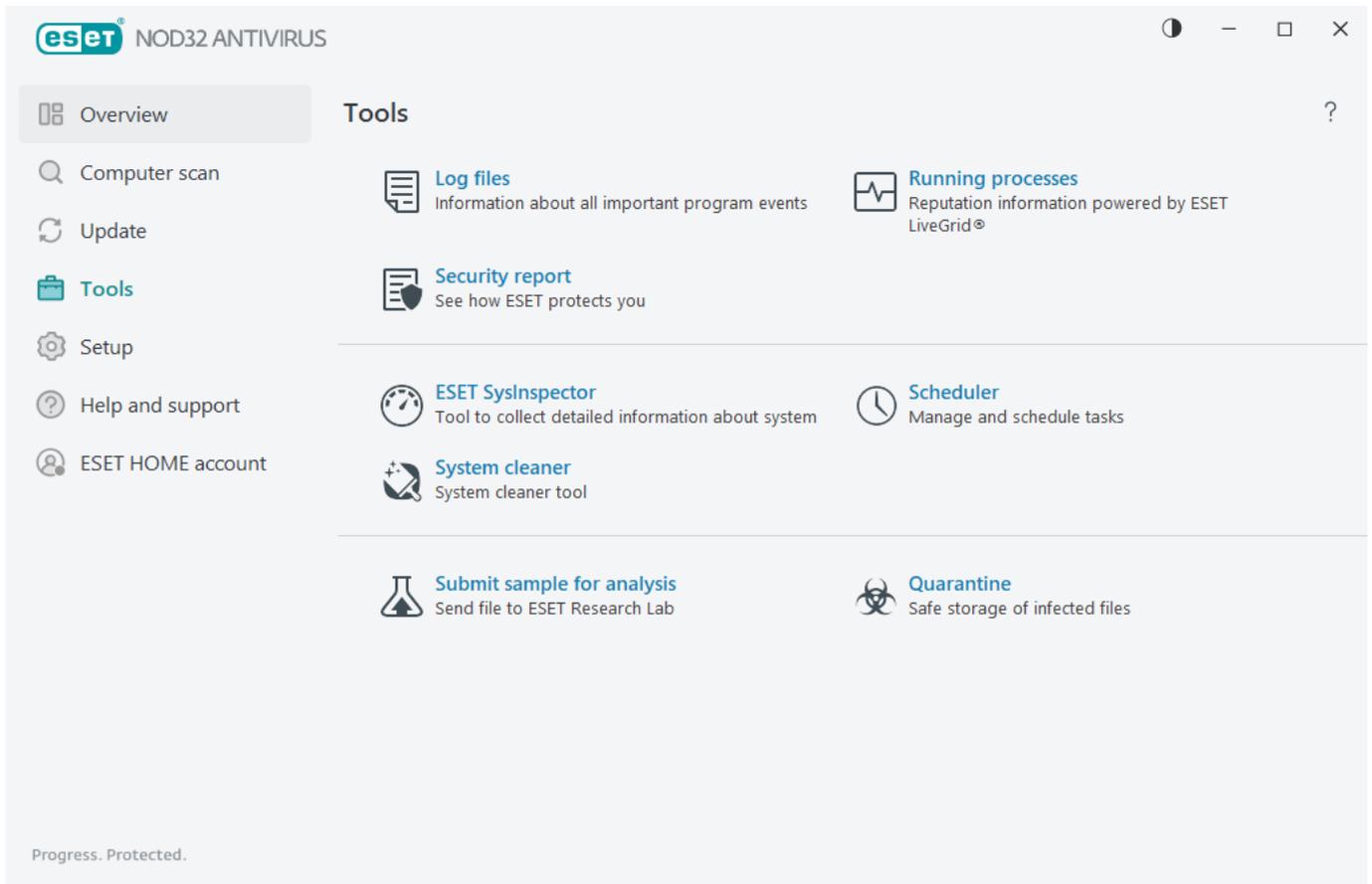
Log files

Log files contain information about important program events and provide an overview of detected threats. Logging is an essential part of system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. You can view text messages and logs directly from the ESET NOD32 Antivirus environment, as well as to archive logs.
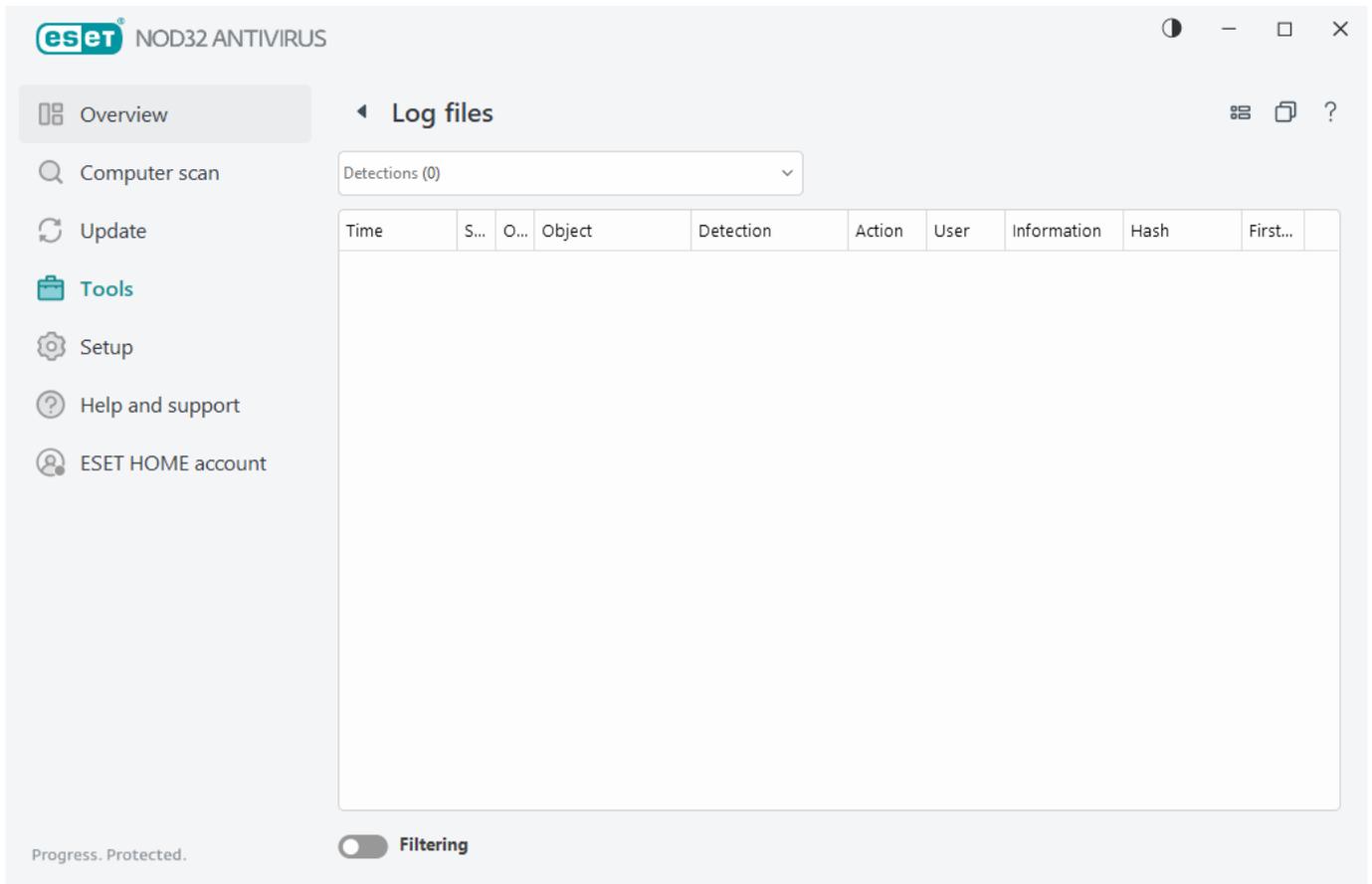
Log files are accessible from the main program window by clicking **Tools** > **Log files**. Select the desired log type from the drop-down menu:

- **Detections**—This log offers detailed information about detections and infiltrations detected by ESET NOD32 Antivirus. Log information includes the time of detection, scanner type, object type, object location, name of detection, the action taken, name of the user logged when the infiltration was detected, hash, and first occurrence. Not cleaned infiltrations are always marked with red text on a 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 NOD32 Antivirus are recorded in the event log. The event log contains information about events and errors in the program. It is designed for system administrators and users to solve problems. The information found here can often help you find a solution for a problem occurring in the program.

- **Computer scan**—Results of all previous scans are displayed in this window. Each line corresponds to a single computer scan. Double-click any entry to view the details of the selected scan.

- **HIPS**—Contains records of specific HIPS rules which are marked for recording. The protocol shows the application that triggered the operation, the result (whether the rule was permitted or prohibited) and the rule name.

- **Filtered websites**—This list is useful if you want to view a list of websites that were blocked by Web access protection. Each log includes time, URL address, user and application that created a connection to a specific website.

- **Device control**—Contains records of removable media or devices that were connected to the computer. Only devices with respective Device control rules 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. You can also view 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** or **SHIFT** to select multiple entries.

Click ⬤ **Filtering** to open the Log filtering window where you can define 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, etc.).

- **Filter**—After clicking this option, the Log filtering window will enable 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 the selected records.

- **Copy cell**—Copies the content of the right-clicked cell.

- **Delete/Delete all**—Deletes the selected records or all displayed records. This action requires administrator privileges.

- **Export/Export all**—Exports information about the selected records or all the records in XML format.

- **Find/Find next/Find previous**—After clicking this option, you can define filtering criteria to highlight the specific entry using the Log filtering window.

- **Detection description**—Opens the ESET Threat Encyclopedia, which contains detailed information about the dangers and symptoms of the recorded infiltration.

- **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. After 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.

Running processes

Running processes displays the running programs or processes on your computer and keeps ESET immediately and continuously informed about new infiltrations. ESET NOD32 Antivirus provides detailed information on running processes to protect users with ESET LiveGrid® technology.
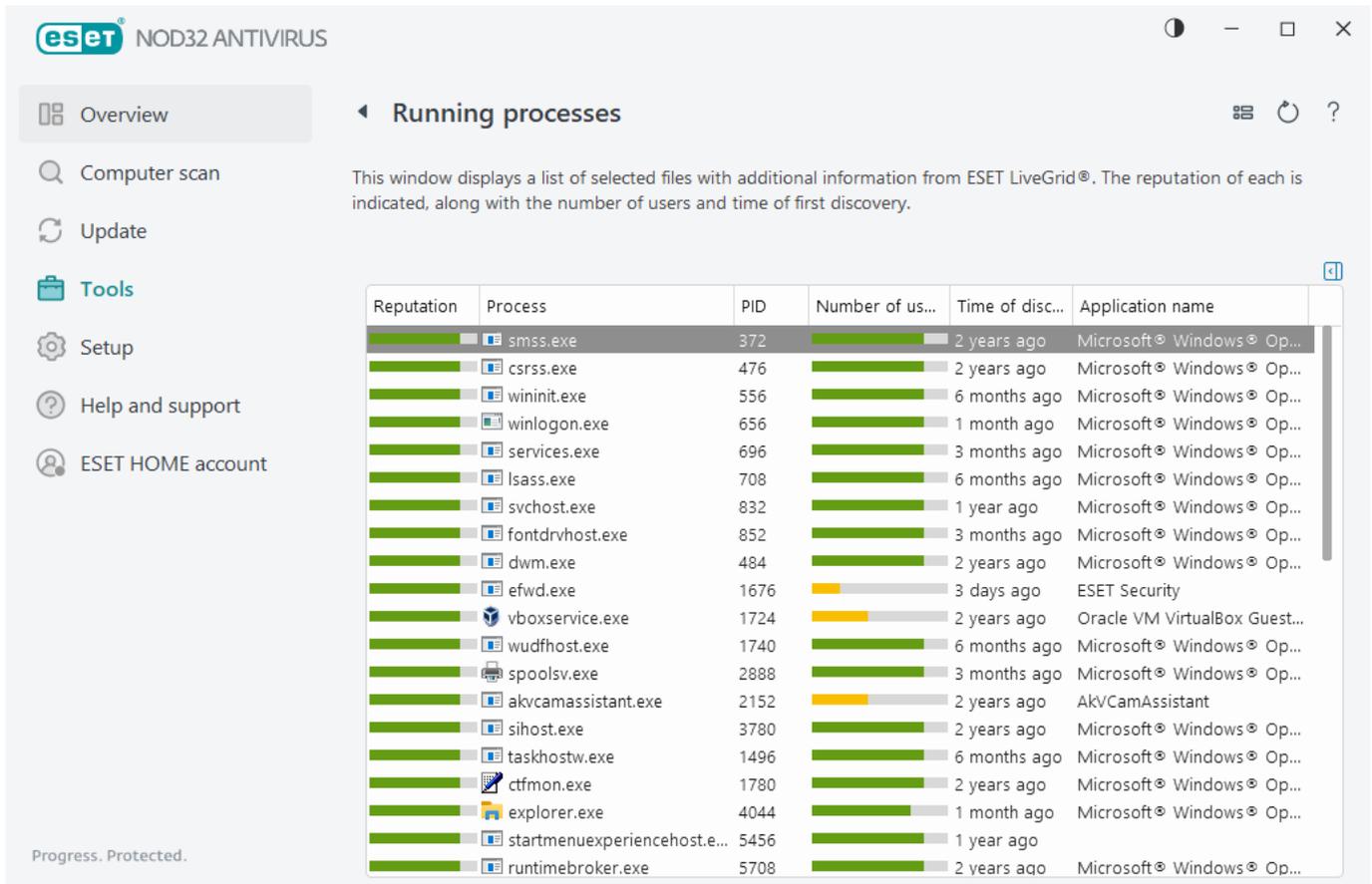
Reputation—In most cases, ESET NOD32 Antivirus and ESET LiveGrid® technology assign risk levels to objects (files, processes, registry keys, etc.) by using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 – Fine (green) to 9 – Risky (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. To open Task Manager, right-click an empty area on the taskbar and then click **Task Manager**, or press **Ctrl**+**Shift**+**Esc** on your keyboard.

> ℹ️ Known applications marked as Fine (green) are definitely clean (whitelisted) and will be excluded from scanning to improve performance.

PID—The process identifier number may be used as a parameter in various function calls such as adjusting the process's priority.

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.

> ℹ️ An application marked as Unknown (orange) is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, you can submit the file for analysis to the ESET Research Lab. If the file turns out to be a malicious application, its detection will be added to an upcoming update.

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

Click an application to display the following details of that application:

- **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/Modified on**—Date and time of creation (modification).

> ℹ️ You can also check the reputation of files that do not act as running programs/processes. To do so, right-click them in a file explorer and select **Advanced options** > **Check file reputation**.
>
>
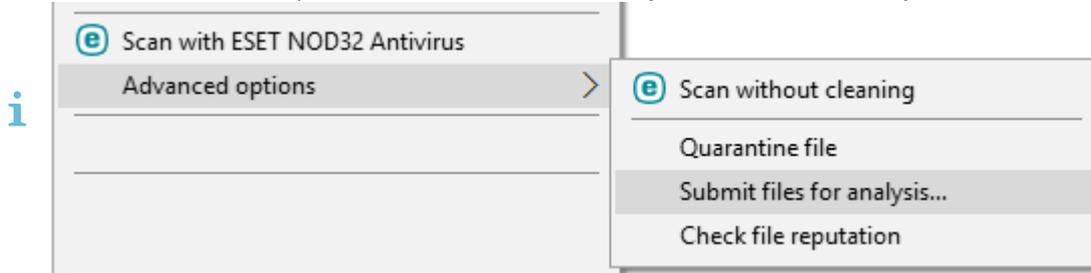
Security report

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

- **Blocked Web pages**—Displays the number of blocked web pages (blacklisted URL for PUA, phishing, hacked router, IP or certificate).

- **Infected email objects detected**—Displays the number of infected email objects that have been detected.

- **PUA detected**—Displays the number of Potentially unwanted applications (PUA).

- **Documents scanned**—Displays the number of scanned document objects.

- **Applications scanned**—Displays the number of scanned executable objects.

- **Other objects scanned**—Displays the number of other scanned objects.

- **Web page objects scanned**—Displays the number of scanned web page objects.

- **Email objects scanned**—Displays the number of scanned email objects.

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

When the feature is enabled, it is no more displayed as non-functional in the Security report.

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 NOD32 Antivirus is installed less than 30 days, then only the number of days from installation can be selected. The period of 30 days is set by default.
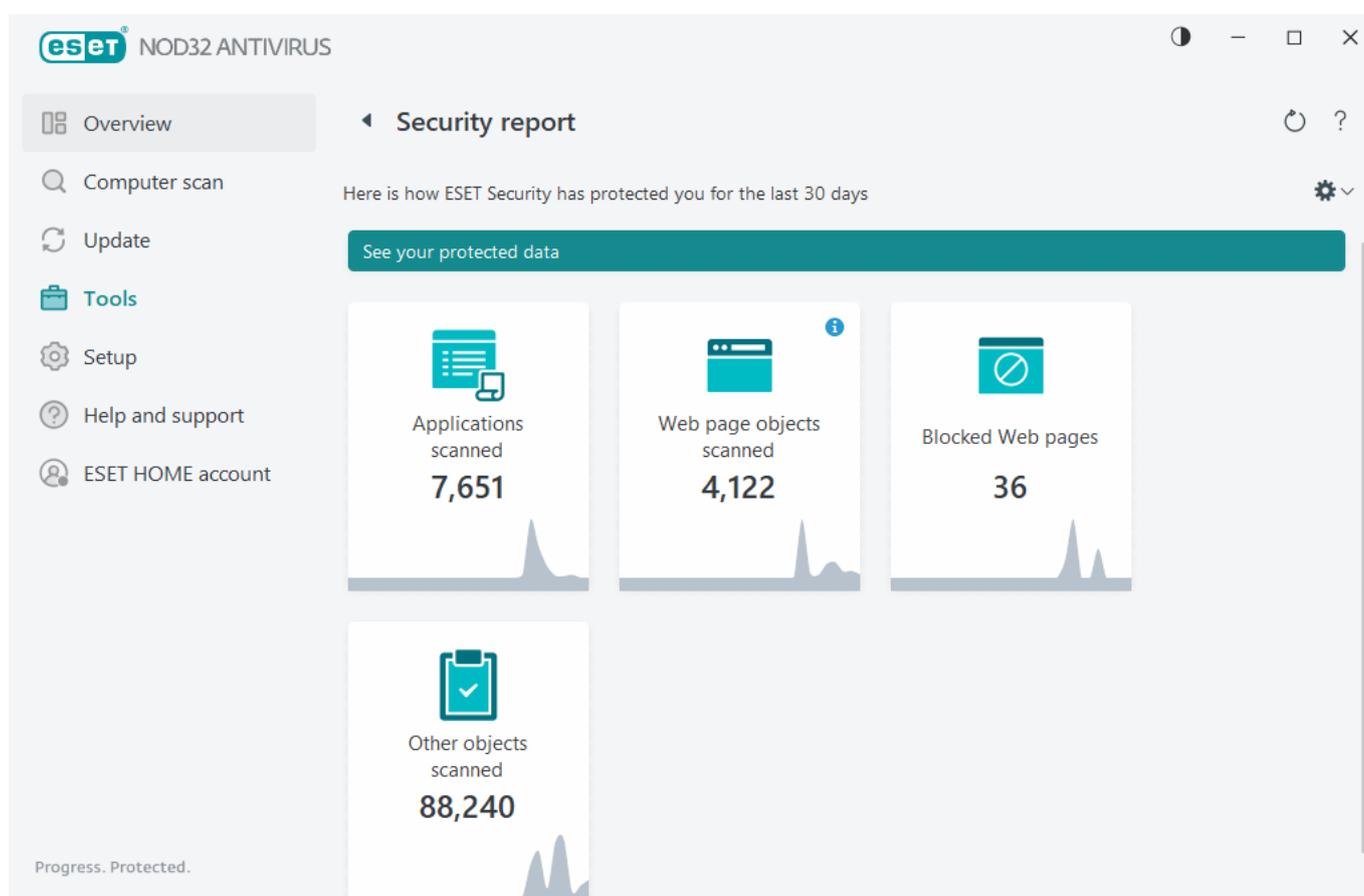
Reset data will clear all statistics and remove the existing data for Security report. This action has to be confirmed except the case that you deselect the **Ask before resetting statistics** option in Advanced setup > **Notifications** > **Interactive alerts** > **Confirmation messages** > **Edit**.

ESET SysInspector

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

The ESET SysInspector window displays the following information about logs:

- **Time**—The time of log creation.

- **Comment**—A short comment.

- **User**—The name of the user who created the log.

- **Status**—The status of log creation.

The following actions are available:

- **Show**—Opens the selected log in ESET SysInspector. You can also right-click a given log file and select **Show** from the context menu.

- **Create**—Creates a new log. Wait until ESET SysInspector is generated (**Created** status) before attempting to access the log. The log is saved in C:\ProgramData\ESET\ESET Security\SysInspector.

- **Delete**—Removes the selected log(s) from the list.

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

- **Show**—Opens the selected log in ESET SysInspector (same function as double-clicking a log).

- **Create**—Creates a new log. Wait until ESET SysInspector is generated (**Created** status) before attempting to access the log.

- **Delete**—Removes the selected log(s) from the list.

- **Delete all**—Deletes all logs.

- **Export**—Exports the log to a .xml file or zipped .xml.

Scheduler

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

The Scheduler can be accessed from the ESET NOD32 Antivirus main program window by clicking **Tools** > **Scheduler**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the pre-defined date, time and scanning profile used.

The Scheduler serves to schedule the following tasks: update modules, 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). You can revert the list of scheduled tasks to default and delete all changes by clicking **Default**. 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 checkboxes 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 user logon**

- **Automatic startup file check** (after user logon)

- **Automatic startup file check** (after successful update of the detection engine)

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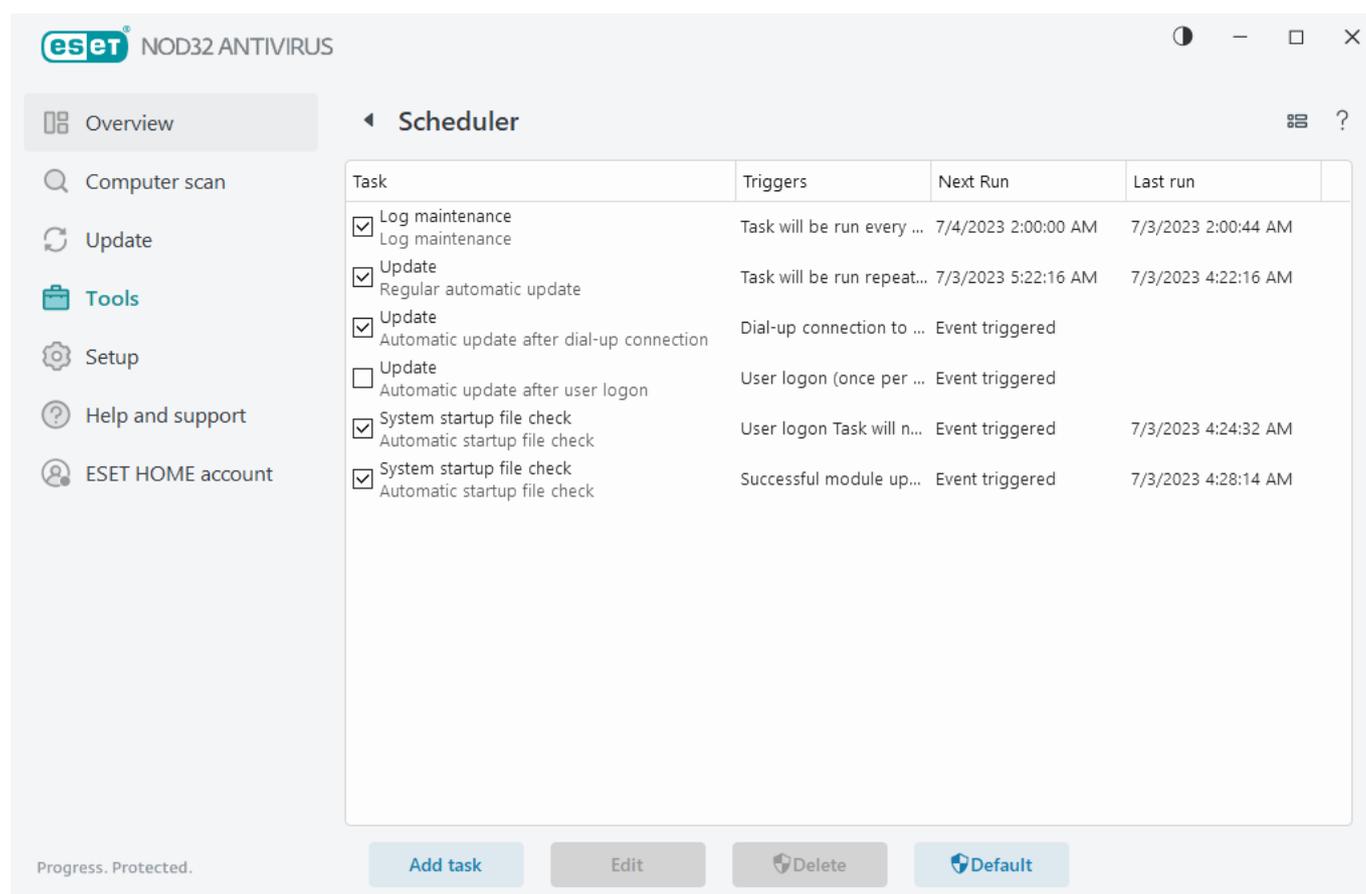
Add a new task

1. Click **Add task** at the bottom of the window.

2. Type a name of the task.

3. Select the desired task from the pull-down menu:

- **Run external application**—Schedules the execution of an external application.

- **Log maintenance**—Log files also contain leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.

- **System startup file check**—Checks files that are allowed to run at system startup or logon.

- **Create a computer status snapshot**—Creates an ESET SysInspector computer snapshot – gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each

49

component.

- **On-demand computer scan**—Performs a computer scan of files and folders on your computer.

- **Update**—Schedules an Update task by updating the modules.

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

- **Once**—The task will be performed at the pre-defined date and time.

- **Repeatedly**—The task will be performed at the specified time interval.

- **Daily**—The task will run repeatedly each day at the specified time.

- **Weekly**—The task will be run on the selected day and time.

- **Event triggered**—The task will be performed on a specified event.

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

- **At the next scheduled time**

- **As soon as possible**

- **Immediately, if time since the last run exceeds (hours)**—Represents the time elapsed since the first skipped run of the task. If this time is exceeded, the task will run immediately. Set the time using the spinner below.

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

Scheduled scan options

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

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

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

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

- **No action**—After a scan finishes, no action will be performed.

- **Shut down**—The computer turns off after a scan finishes.

- **Restart if needed**—The computer restarts if only needed to complete cleaning of detected threats.

- **Restart**—Closes all open programs and restarts the computer after a scan finishes.

- **Force restart if needed**—The computer forces restart if only needed to complete cleaning of detected threats.

- **Force restart**— Forces closing of all open programs without waiting for user interaction and restarts the computer after a scan finishes.

- **Sleep**—Saves your session and puts the computer in a low-power state so that you can quickly resume working.

- **Hibernate**—Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down but will resume its previous state the next time you start it.

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

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

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

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

See also Scan progress.

Scheduled task overview

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

Task details

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

- **Run external application**—Schedules the execution of an external application.

- **Log maintenance**—Log files also contain leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.

- **System startup file check**—Checks files that are allowed to run at system startup or logon.

- **Create a computer status snapshot**—Creates an ESET SysInspector computer snapshot – gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.

- **On-demand computer scan**—Performs a computer scan of files and folders on your computer.

- **Update**—Schedules an Update task by updating the modules.

Task timing

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

- **Once**—The task will be performed only once at the pre-defined date and time.

- **Repeatedly**—The task will be performed at the specified interval (in hours).

- **Daily**—The task will run each day at the specified time.

- **Weekly**—The task will run one or more times a week, on the selected day(s) and time.

- **Event triggered**—The task will be performed after a specified event.

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

Task timing - Once

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

Task timing - Daily

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

Task timing - Weekly

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

Task timing - Event triggered

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

- **Every time the computer starts**

- **The first time the computer starts each day**

- **Dial-up connection on the internet/VPN**

- **Successful module update**

- **Successful product update**

- **User logon**

• **Threat detection**

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

Skipped task

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

> • **At the next scheduled time**—The task will run if the computer is turned on at the next scheduled time.

> • **As soon as possible**—The task will run when the computer is turned on.

> • **Immediately, if time since last scheduled run exceeds (hours)**—Represents the time elapsed since the first skipped run of the task. If this time is exceeded, the task will run immediately.

> ✓ **Immediately, if time since last scheduled run exceeds (hours) – examples**
> An example task is set to run repeatedly every hour. The option **Immediately, if time since last scheduled run exceeds (hours)** is selected and the exceeded time is set to two hours. The task runs at 13:00, and when finished, the computer goes to sleep:
> • The computer wakes up at 15:30. The first skipped run of the task was at 14:00. Only 1.5 hours have passed since 14:00, so the task will run at 16:00.
> • The computer wakes up at 16:30. The first skipped run of the task was at 14:00. Two and a half hours have passed since 14:00, so the task will run immediately.

Task details - Update

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

Task details - Run application

This task schedules the execution of an external application.

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

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

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

Click **Finish** to apply the task.

System cleaner

System cleaner is a tool that helps you to restore the computer to usable state after cleaning the threat. Malware can disable system utilities such as Registry Editor, Task manager or Windows Updates. System cleaner restores the default values and settings for given system in a single click.

System cleaner reports issues from five settings categories:

- **Security settings**: changes in settings which can cause an increased vulnerability of your computer, such as Windows Update

- **System settings**: changes in system settings, that can change behavior of your computer, such as file associations

- **System appearance**: settings that affects how your system looks, such as your desktop wallpaper

- **Disabled features**: important features and applications that may be disabled

- **Windows System Restore**: settings for the Windows System Restore feature, that enables you to revert your system to a previous state

System cleaning can be requested:

- when a threat is found

- when a user clicks **Reset**

You can review the changes and reset settings if appropriate.
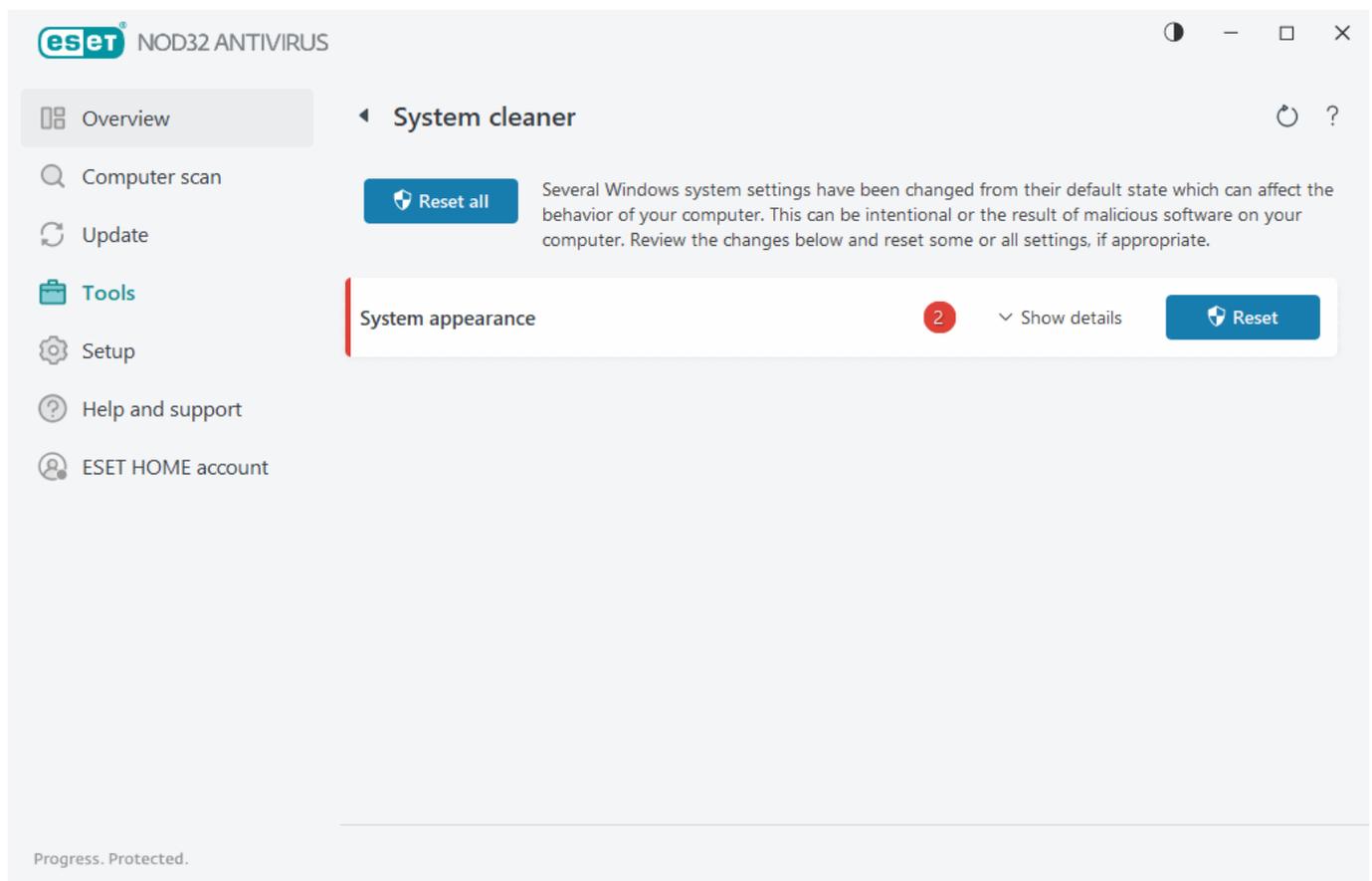
> ℹ Only a user with Administrator rights can perform actions in the System cleaner.

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 NOD32 Antivirus 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).
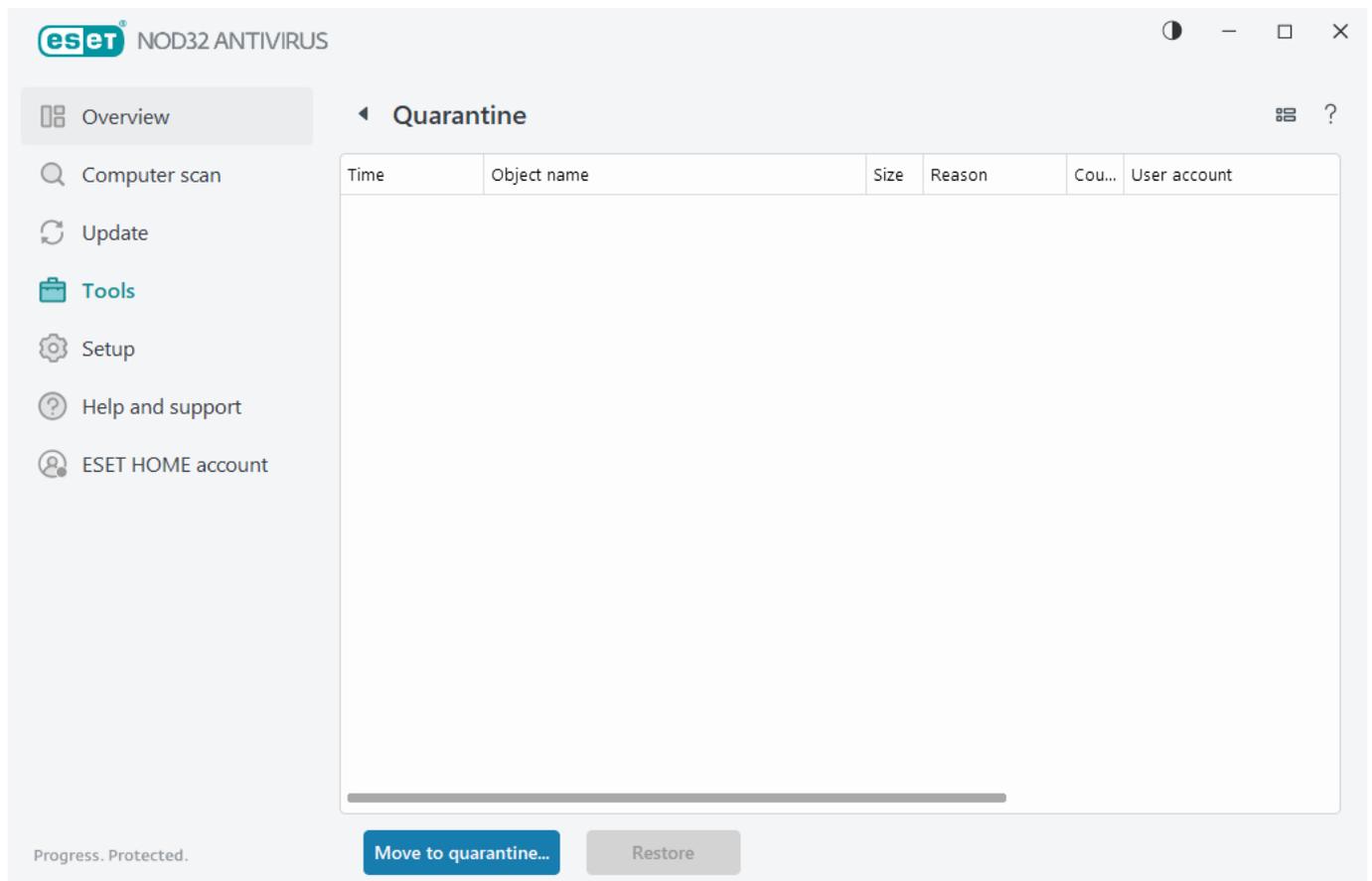
Quarantining files

ESET NOD32 Antivirus 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 NOD32 Antivirus,

    d.or if a file behaves suspiciously but is not detected by [Protections](#).

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.Right-click the file > click **Advanced options** > **Quarantine file**.

    c.Click **Move to quarantine** from the **Quarantine** window.

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

Submitting a file from the Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was determined to be infected incorrectly (for example, by heuristic analysis of the code) and subsequently quarantined, 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.

Detection description

Right-click an item and click **Detection description** to open the ESET Threat Encyclopedia, which contains detailed information about the dangers and symptoms of the recorded infiltration.

> **ℹ Illustrated instructions**
> The following ESET Knowledgebase article may only be available in English:
> • Restore a quarantined file in ESET NOD32 Antivirus
> • Delete a quarantined file in ESET NOD32 Antivirus
> • My ESET product notified me of a detection—what should I do?

Quarantine failed

Reasons why specific files cannot be moved to Quarantine are the following:

- **You do not have the read permissions**—means that you cannot view the content of a file.

- **You do not have the write permissions**—means that you cannot modify the contents of the file, i.e. either add new content or delete the existing content.

- **File, you are trying to quarantine, is too large**—You need to reduce file size.

When you receive error message "Quarantine failed", click **More info**. Quarantine error list window appears and you will see the name of file and reason, why the file cannot be quarantined.

Select sample for analysis

If you find a suspicious file on your computer or a 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, screenshot or the website you downloaded it from)

You can send a sample submission (a file or a website) to ESET for analysis by using one of these methods:

1. Use the sample submission form in your product. It is located in **Tools** > **Submit sample for analysis**. The maximum size of a submitted sample is 256MB.

2. Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using WinRAR/WinZIP, protect the archive with the password "infected" and send it to samples@eset.com.

3. To report spam or spam false positives, please refer to our ESET Knowledgebase article.

In the **Select sample for analysis** form, select the description from the **Reason for submitting the sample** drop-

down menu that best fits your message purpose:

- [Suspicious file](#)

- [Suspicious site](#) (a website that is infected by any malware)

- [False positive site](#)

- [False positive file](#) (file that is detected as an infection but are not infected)

- [Other](#)

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

Contact email—This contact email is sent along with the 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.

> **i** **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—Type a description of the suspicious file behavior observed on your computer.

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

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

> **i** The first parameter – **Observed signs and symptoms of malware infection** – is required, but providing additional information will help significantly to our laboratories in identification process and in processing of samples.

Select sample for analysis - Suspicious site

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, PINs and more. Read more about this type of attack in the [glossary](#).

- **Scam**—A hoax or a fraudulent website, especially for making a quick profit.

- Select **Other** if the options above do not refer to the site you will submit.

Notes and additional information—You can type additional information or a description that will help analyze the suspicious website.

Select sample for analysis - False positive file

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

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

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

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

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

> **i** 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 website.

Select sample for analysis - Other

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

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

Setup

You can find groups of available protection features in the main program window > **Setup**.
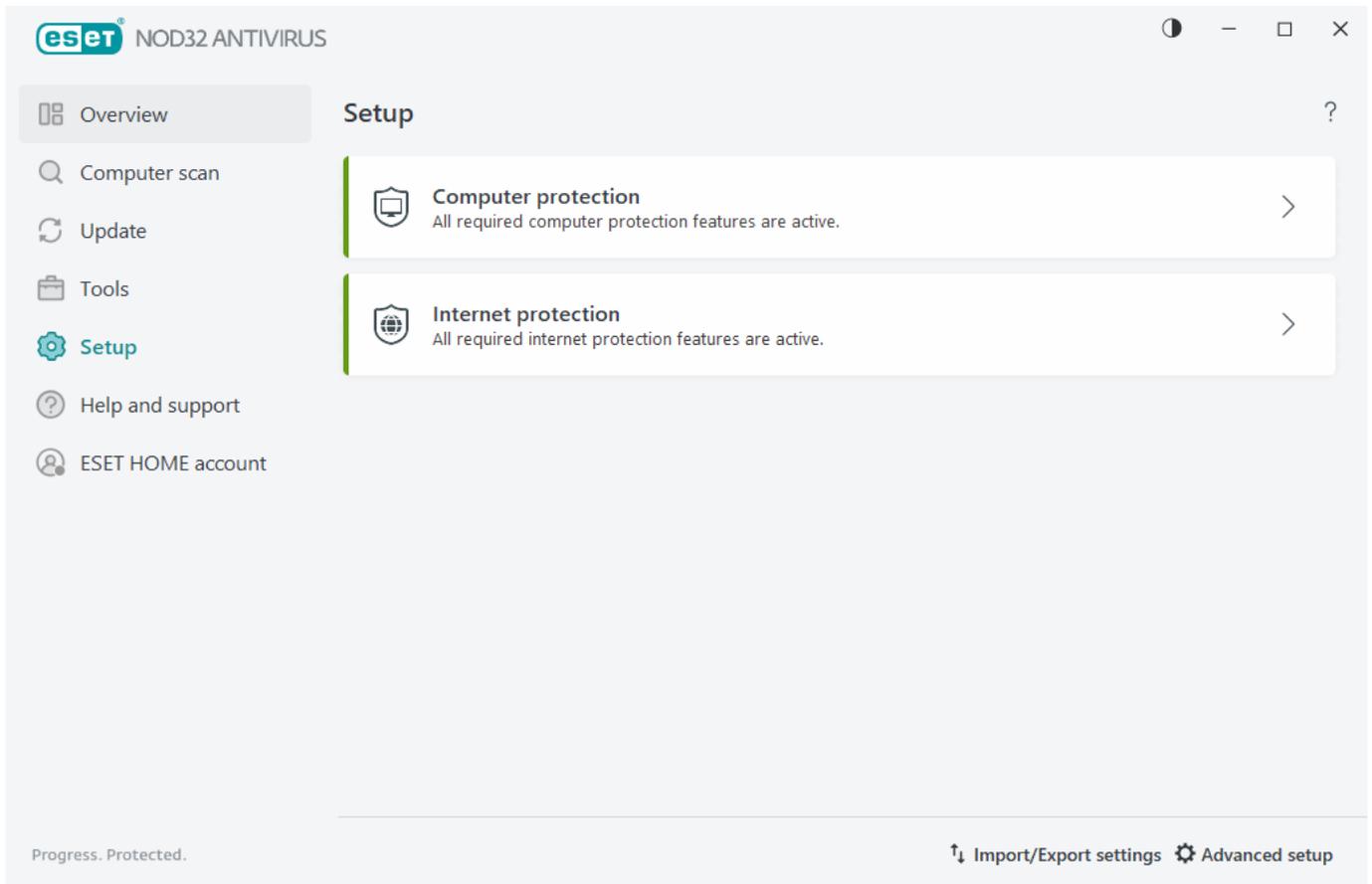
The **Setup** menu is divided into the following groups:

 Computer protection

 Internet protection

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

Computer protection

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

- Real-time file system protection—All files are scanned for malicious code when they are opened, created, or run.

- Device control—This module enables you to scan, block or adjust extended filters/permissions and select how the user can access and use a given device (CD/DVD/USB...).

- Host Intrusion Prevention System (HIPS)—The HIPS system monitors the events within the operating system and reacts to them according to a customized set of rules.

- Gamer mode—Enables or disables Gamer mode. You will receive a warning message (potential security risk) and the main window will turn orange after enabling Gamer mode.

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

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

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

For the **Real-time file system protection**, click the gear icon ⚙ and choose from the following options:

- **Configure**—Opens Real-time file system protection Advanced setup.

- **Edit exclusions**—Opens the Exclusion setup window so that you can exclude files and folders from scanning.
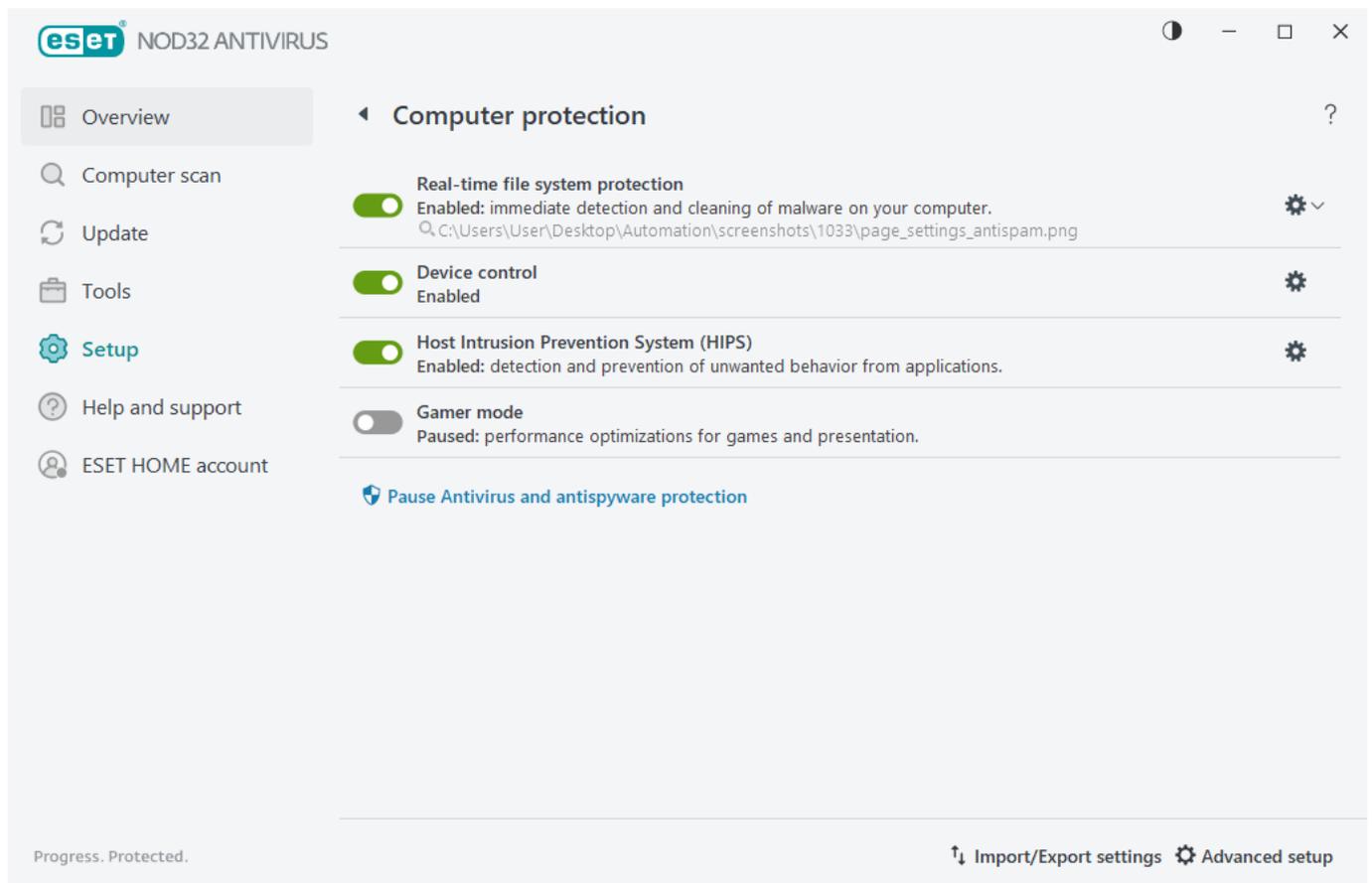
Pause Antivirus and antispyware protection—Disables all antivirus and antispyware protection modules. When you disable protection, a window will open to determine how long will the protection be disabled using the **Time interval** drop-down menu. Use only if you are an experienced user or instructed by ESET Technical Support.

An infiltration is detected

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

Standard behavior

As a general example of how infiltrations are handled by ESET NOD32 Antivirus, infiltrations can be detected using:

- Real-time file system protection

- Web access protection

- Email client protection

- On-demand computer scan

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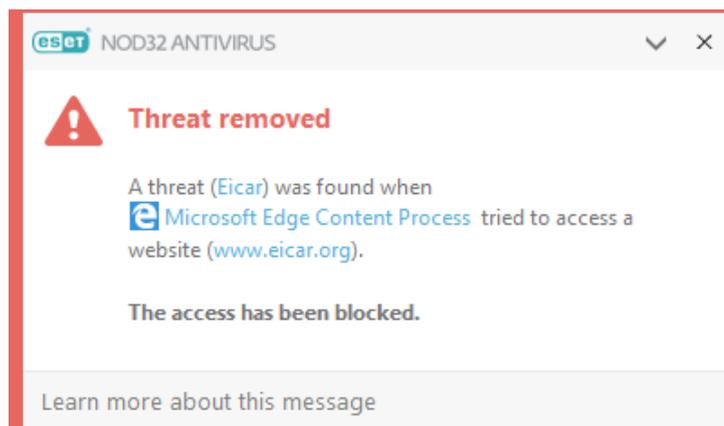
Scanning computer for infected files

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

1.Open ESET NOD32 Antivirus and click **Computer scan**.

2.Click **Scan your computer** (for more information, see Computer scan).

3.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.

Cleaning and deleting

If there is no pre-defined action to take for Real-time file system protection, you will be prompted to select an option in the alert window. Usually the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, as this will leave infected files uncleaned. The exception to this is when you are sure that a file is harmless and has been detected by mistake.
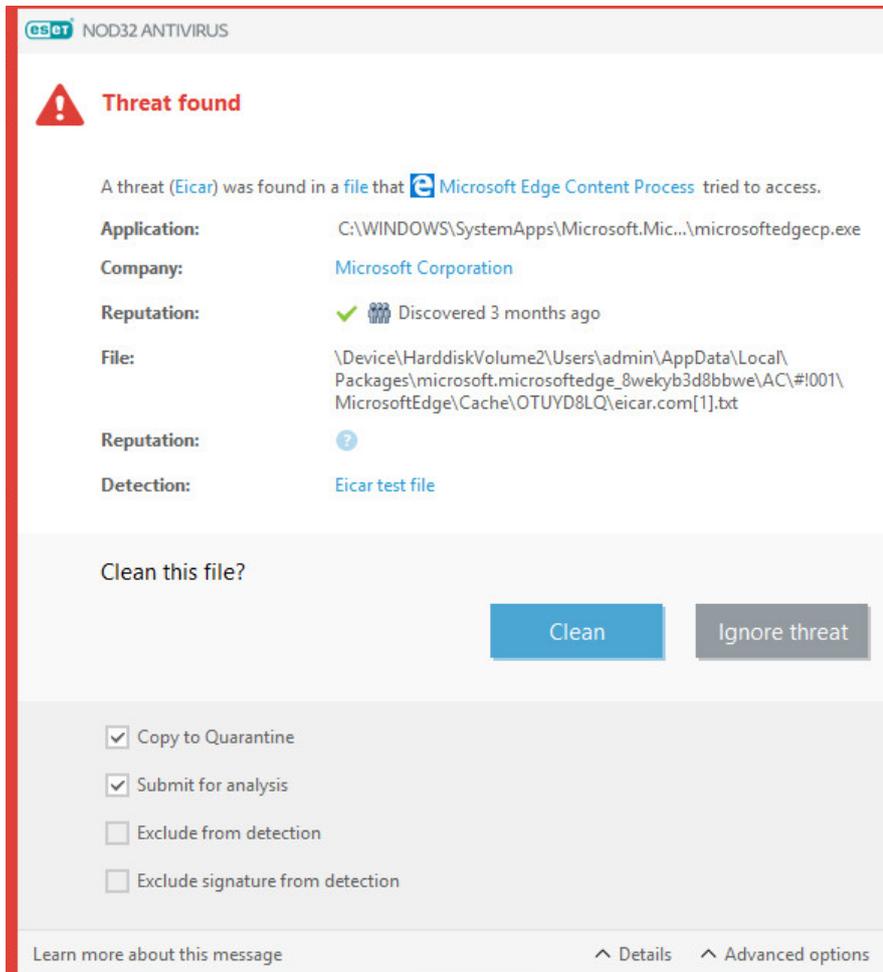
Apply cleaning if a file has been attacked by a virus that has attached malicious code to the file. If this is the case, first attempt to clean the infected file to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.

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

Restoring from the Quarantine

The Quarantine can be accessed from the ESET NOD32 Antivirus main program window by clicking **Tools** > **Quarantine**.

Quarantined files can also be restored to their original location:

• Use the **Restore** feature for this purpose, which is available from the context menu by right-clicking a given file in the Quarantine.

• If a file is marked as a potentially unwanted application, the **Restore and exclude from scanning** option is enabled. See also Exclusions.

• The context menu also offers the **Restore to** option, which enables 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.

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 actions for those files is displayed. Select actions for the files (actions are set individually for each file in the list) and then click **Finish**.

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.

Internet protection

Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Open the [main program window](#) > **Setup** > **Internet protection** to configure features in ESET NOD32 Antivirus that increase your internet protection.

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

> ⚠ Turning off protection modules may decrease the protection level of your computer.
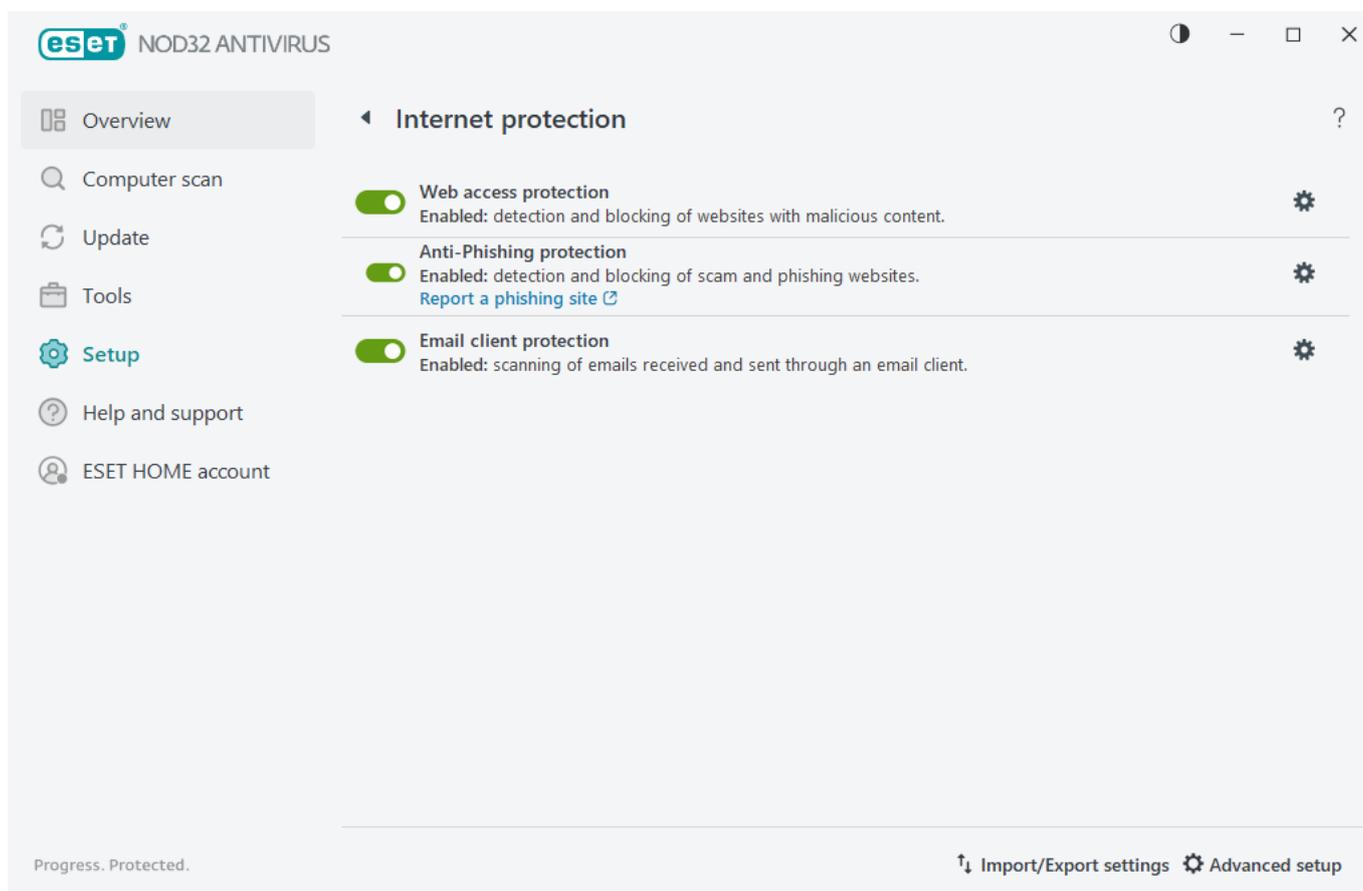
Click the gear icon next to a protection module to access advanced settings for that module.

[Web access protection](#) scans HTTP/HTTPS communication for malware and phishing. Web access protection should only be turned off for troubleshooting.

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

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

> **i** 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 an incorrectly blocked page](#).

[Email client protection](#) provides control of email communications received through the POP3(S) and IMAP(S) protocols. Using the plugin program for your email client, ESET NOD32 Antivirus provides control of all communications from/to the email client.

Anti-Phishing protection

Phishing is a criminal activity that uses social engineering (manipulating users to obtain confidential information). Phishing is used to access sensitive data such as bank account numbers, PINs, etc. For more information, see the [glossary](#). ESET NOD32 Antivirus includes anti-phishing protection, which blocks web pages known to distribute this type of content.

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

Visit our [Knowledgebase article](#) for more information on Anti-Phishing protection in ESET NOD32 Antivirus.

Accessing a phishing website

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

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

Report a phishing site

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

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

Import and export settings

You can import or export your customized ESET NOD32 Antivirus .xml configuration file from the **Setup** menu.

Importing and exporting configuration files is useful if you need to backup your current configuration of ESET NOD32 Antivirus for use at a later time. The export settings option is also convenient when you want to use your preferred configuration on multiple systems. You can import a .xml file to transfer these settings.

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

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

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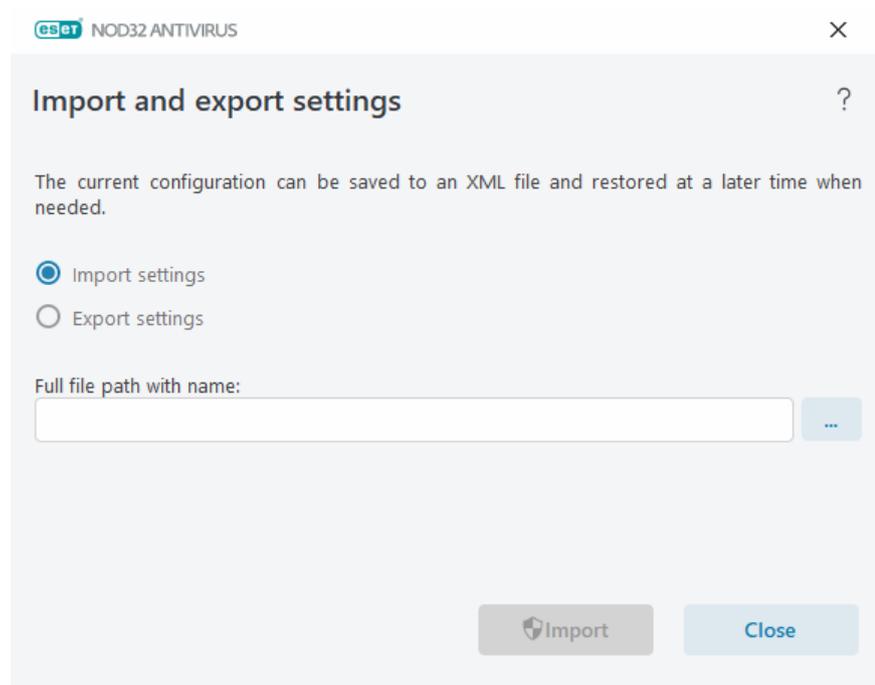
Help and support

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

License

- License troubleshooting—Click this link to find solutions for problems with activation or license change.

- Change license—Click to launch the activation window and activate your product. If your device is connected to ESET HOME, choose a license from your ESET HOME account or add a new one.

ⓔ Installed product

- **What's New**—Click this to open the information window about new and improved features.

- **About ESET NOD32 Antivirus**—Displays information about your copy of ESET NOD32 Antivirus.

- **Product troubleshooting**—Click this link to find solutions to the most frequently encountered problems.

- **Change product**—Click to see if ESET NOD32 Antivirus can be changed to a different product line with the current license.

Help page—Click this link to launch the ESET NOD32 Antivirus help pages.

Technical Support

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

About ESET NOD32 Antivirus

This window provides details about the installed version of ESET NOD32 Antivirus and your computer.

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

- You can copy information about modules to the clipboard by clicking **Copy**. This may be useful during troubleshooting or when contacting Technical Support.

- Click **Detection Engine** in the Modules window to open the ESET Virus radar, which contains information about each version of the ESET Detection Engine.

ESET News

In this window, ESET NOD32 Antivirus informs you of ESET news on a regular basis.

In-product messaging is designed to inform users of ESET news and other communications. Sending marketing messages requires the consent of a user. Marketing messages are not sent to a user by default (shown as a question mark). By enabling this option, you agree to receive ESET marketing messages. If you are not interested in receiving ESET marketing material, disable the **Display marketing messages** option.

To enable or disable receiving marketing messages via notification window, follow the instructions below.

1. Open Advanced setup.

2. Click **Notifications** > **Interactive Alerts**.

3. Modify **Display marketing messages** option.
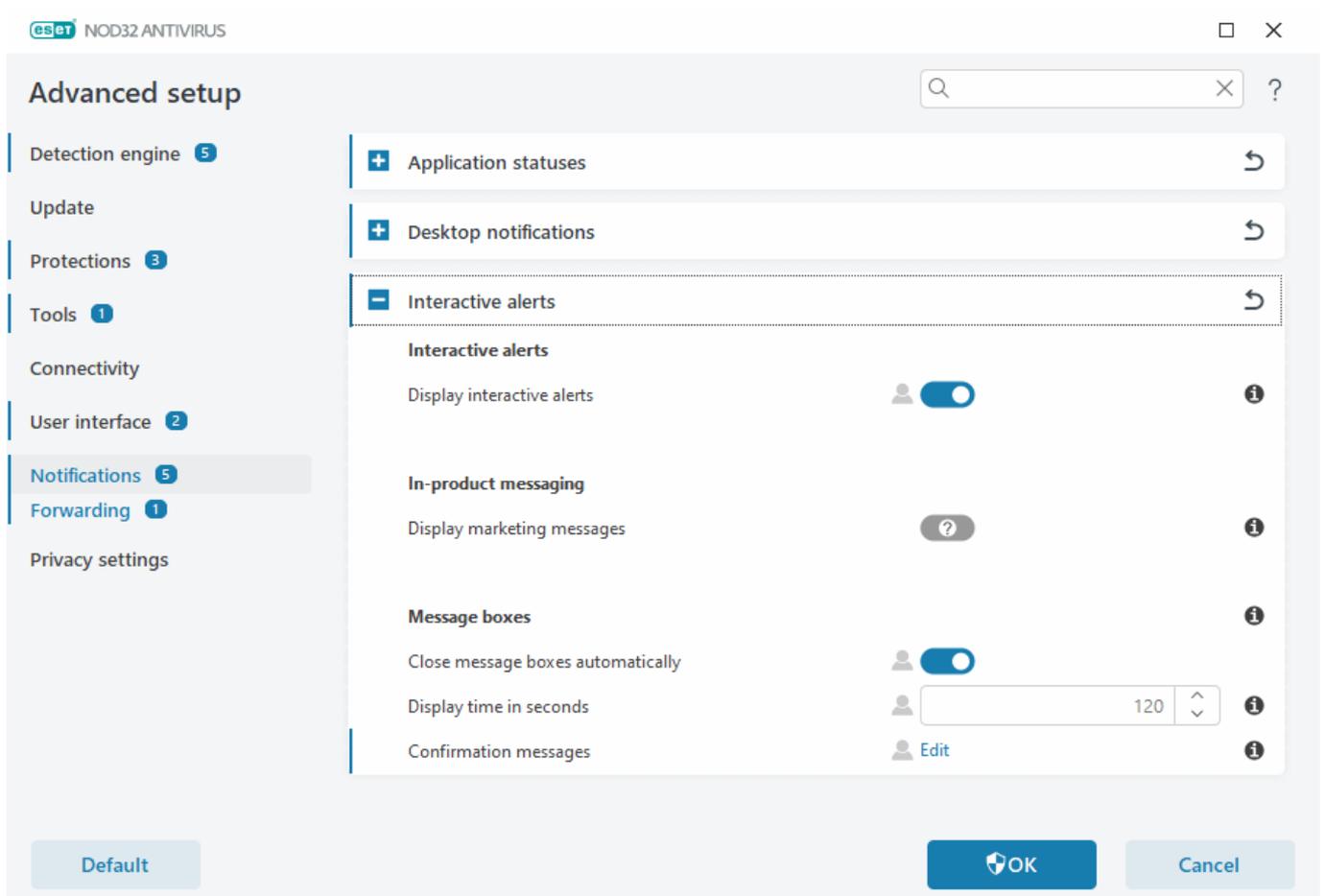
Submit system configuration data

To provide assistance as quickly and accurately as possible, ESET requires information about ESET NOD32 Antivirus configuration, detailed system information and running processes (ESET SysInspector log file) and registry data. ESET will use this data only to provide technical assistance to the customer.

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

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

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

Technical support

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

Contact Technical Support

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

Get information for Technical Support

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

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

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

ESET HOME account

You can review the ESET HOME account connection status in the main program window > **ESET HOME account**.
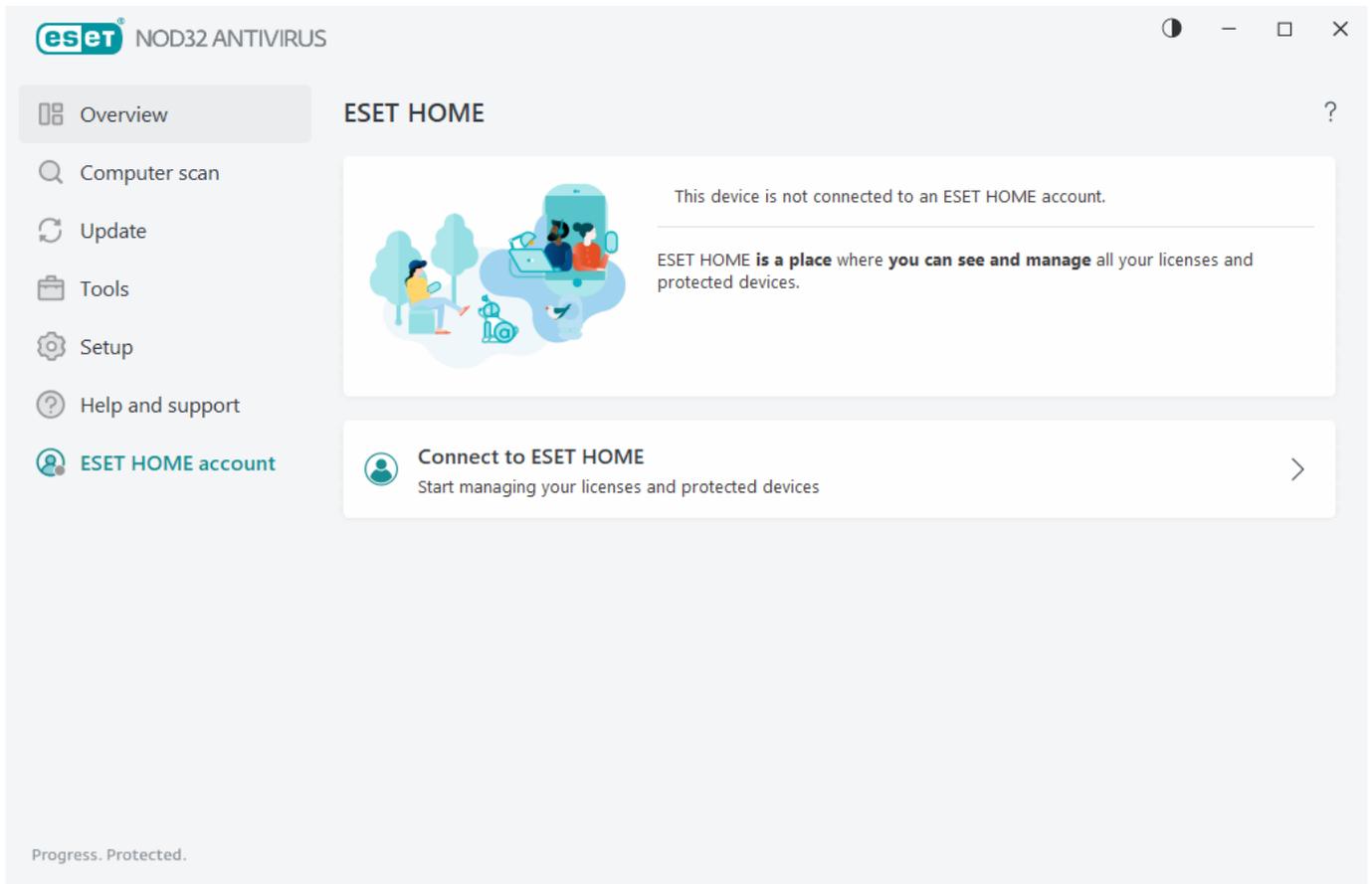
This device is not connected to an ESET HOME account

Click Connect to ESET HOME to connect your device to ESET HOME and manage your licenses and protected devices. You can renew, upgrade or extend your license and view important details. In the ESET HOME management portal or mobile app, you can add different licenses, download products to your devices, check the product security status or share licenses through email. For more information, visit ESET HOME Online Help.

This device is connected to an ESET HOME account

You can manage your device's security remotely using ESET HOME portal or mobile app. Click **App Store** or **Google Play** to display a QR code that you can scan with your mobile phone to download the ESET HOME mobile app from App Store or Google Play.

ESET HOME account—Your ESET HOME account name.

Device name—The name of this device displayed in the ESET HOME account.

Open ESET HOME—Opens the ESET HOME management portal.

To disconnect your device from your ESET HOME account, click **Disconnect from ESET HOME** > **Disconnect**. The license used for activation will remain active, and your device will be protected.

Connect to ESET HOME

Connect your device to ESET HOME to view and manage all your activated ESET licenses and devices. You can renew, upgrade or extend your license and view important license details. In the ESET HOME management portal

71

or mobile app, you can add different licenses, download products to your devices, check the product security status, or share licenses through email. For more information, visit ESET HOME Online Help.
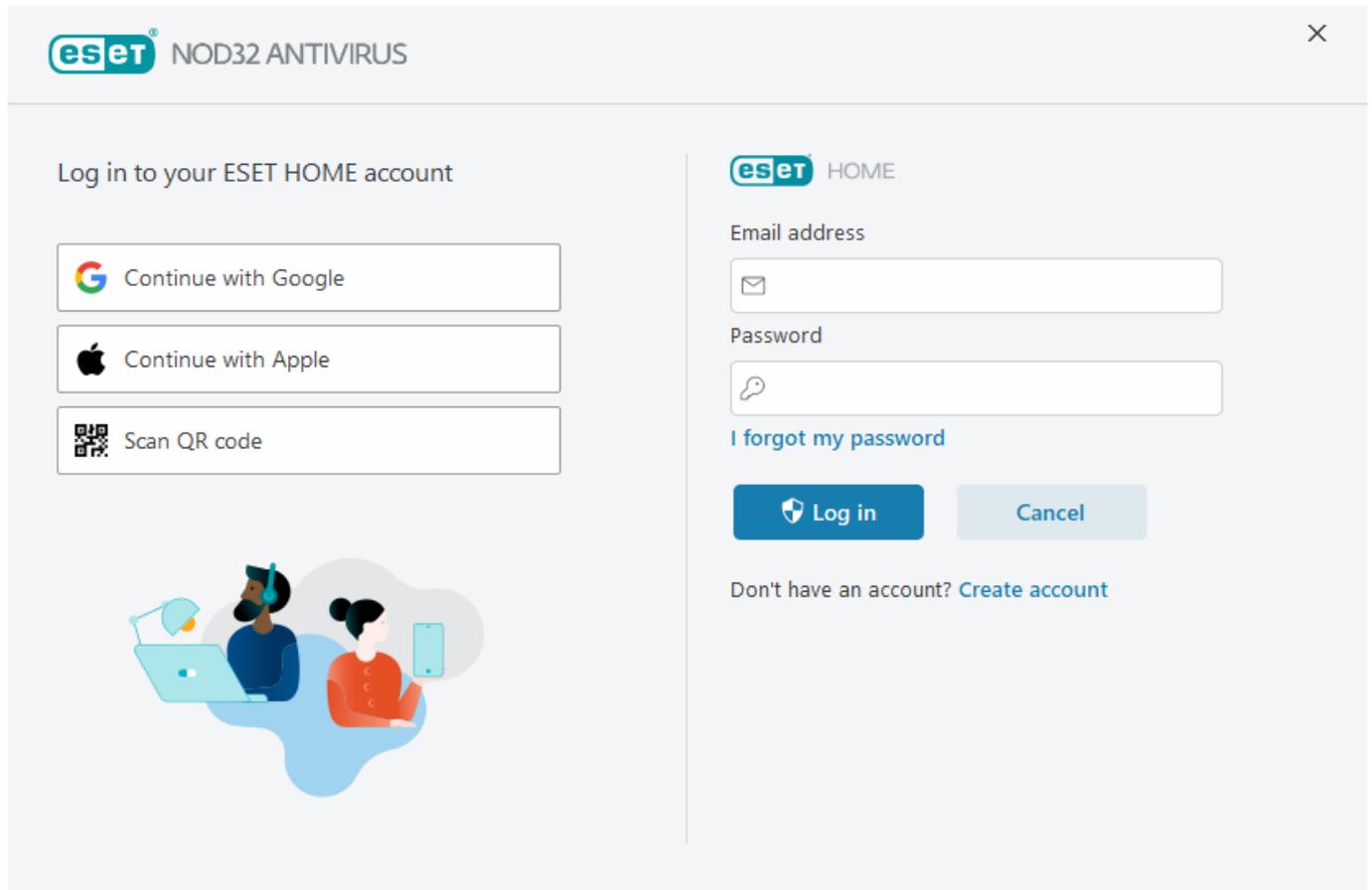
To connect your device to ESET HOME:

> ℹ️ If you are connecting to ESET HOME during installation or when selecting **Use ESET HOME account** as an activation method, follow the instructions in Use ESET HOME account topic.
> If you already have ESET NOD32 Antivirus installed and activated with a license added in your ESET HOME account, you can connect your device to ESET HOME using the ESET HOME portal. Follow the instructions in the ESET HOME Online Help guide and allow the connection in ESET NOD32 Antivirus.

1. In the main program window, click **ESET HOME account** > **Connect to ESET HOME** or click **Connect to ESET HOME** in **Connect this device to an ESET HOME account** notification.

2. Log in to your ESET HOME account.

> ℹ️ If you do not have an ESET HOME account, click **Create account** to register or see instructions in the ESET HOME Online Help.
> If you forgot your password click **I forgot my password** and follow the on-screen steps or see instructions in the ESET HOME Online Help.

3. Set a **Device name** and click **Continue**.

4. After a successful connection, a details window displays. Click **Done**.

Log in to ESET HOME

There are several methods available to log in to your ESET HOME account:

- **Use your ESET HOME email address and password**—Type the **Email address** and **Password** you used to create your ESET HOME account and click **Log in**.

- **Use your Google account/AppleID**—Click **Continue with Google** or **Continue with Apple** and log in to the appropriate account. After a successful login, you will be redirected to the ESET HOME confirmation web page. To continue, switch back to your ESET product window. For more information about the Google account/AppleID login, see instructions in the ESET HOME Online Help.

- **Scan QR code**—Click **Scan QR code** to display the QR code. Open your ESET HOME mobile app and scan the QR code or point your device camera to the QR code. For more information, see instructions in the ESET HOME Online Help.

> i
> If you do not have an ESET HOME account, click **Create account** to register or see instructions in the ESET HOME Online Help.
> If you forgot your password click **I forgot my password** and follow the on-screen steps or see instructions in the ESET HOME Online Help.

⚠ Login failed - common errors.
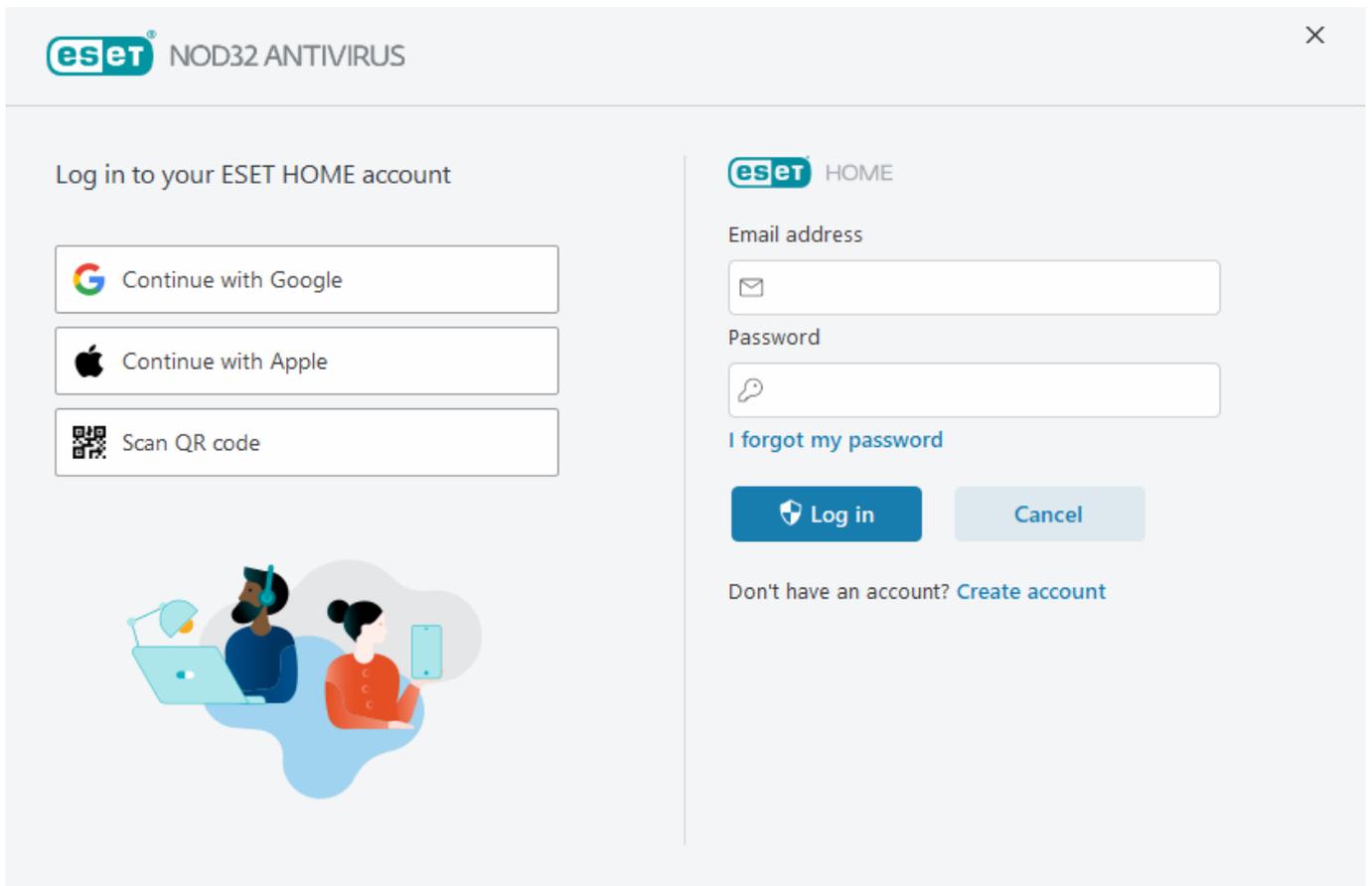
Login failed – common errors

We couldn't find an account that matches the entered email address

The email address you entered does not match any ESET HOME account. Click **Back** and type the correct email address and password.

To log in, you must create an ESET HOME account. If you do not have an ESET HOME account, click **Back** > **Create account** or see Create a new ESET HOME account.

Username and password don't match

The entered password does not match the entered email address. Click **Back**, type in the correct password and make sure the entered email address is correct. If you are still unable to log in, click **Back** > **I forgot my password** to reset your password and follow the on-screen steps or see I forgot my ESET HOME password.

The selected login option doesn't match your account

Your account is linked to your social media account. To log in to the ESET HOME click **Continue with Google** or **Continue with Apple** and log in to the appropriate account. After a successful login, you will be redirected to the ESET HOME confirmation web page. You can disconnect your social media account from your ESET HOME account on the ESET HOME portal.

Incorrect password

This error can occur if your ESET NOD32 Antivirus is already connected to ESET HOME and you are making changes that require you to log in (for example, disabling Anti-Theft) and the password you entered does not match your account. Click **Back** and type the correct password. If you are still unable to log in, click **Back** > **I forgot my password** to reset your password and follow the on-screen steps or see I forgot my ESET HOME password.

Add device in ESET HOME

If you already have ESET NOD32 Antivirus installed and activated with a license added in your ESET HOME account, you can connect your device to ESET HOME using the ESET HOME portal:

1. Send a connection request to your device.

2. ESET NOD32 Antivirus displays **Connect this device to an ESET HOME account** dialog window with an ESET HOME account name. Click **Allow** to connect the device to the mentioned ESET HOME account.

> ℹ️ If there is no interaction, the connection request will be canceled automatically after approximately 30 minutes.

Advanced setup

Advanced setup enables you to configure detailed ESET NOD32 Antivirus settings to fit your needs.

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

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

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

- Detection engine

- Update

- Protections

- Tools

- Connectivity

- User interface

- Notifications

- Privacy settings
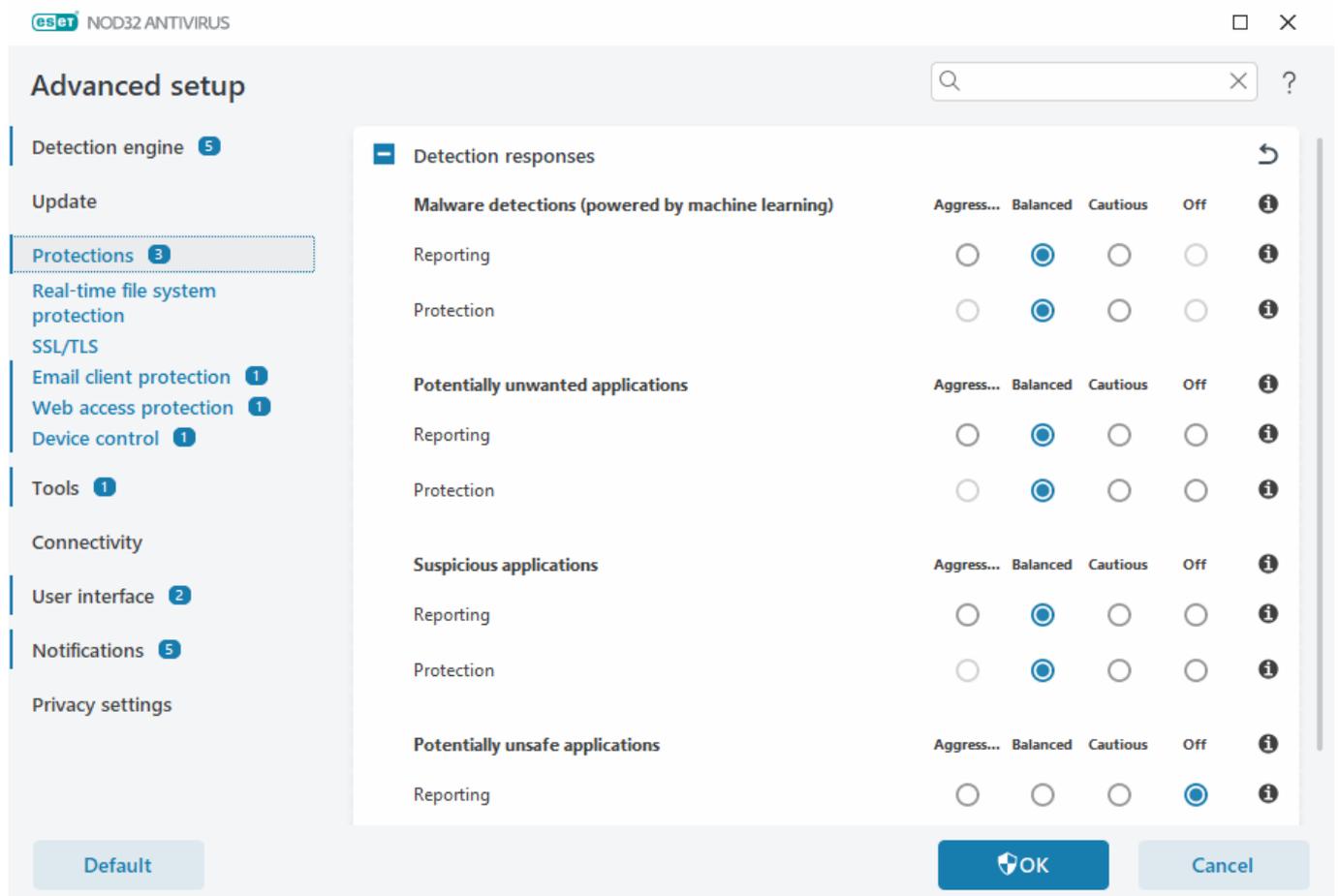
Detection engine

[Advanced setup]() > **Detection engine** enables you to configure the following options:

- [Exclusions]()

- [Advanced options]()

- [Network traffic scanner]()

Exclusions

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

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

[Detection exclusions]()—exclude objects from detection using the detection name, path, or its hash. Detection exclusions do not exclude files and folders from scanning as performance exclusions do. Detection exclusions exclude objects only when they are detected by the detection engine and an appropriate rule is present in the exclusion list.

Not to be confused with other types of exclusions:

- [Process exclusions]()—All file operations attributed to excluded application processes are excluded from scanning (may be required to improve backup speed and service availability),

- [Excluded file extensions](),

- [HIPS exclusions](),

- [Exclusion filter for Cloud-based protection]().

Performance exclusions

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

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

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

> **i** Not to be confused with [Detection exclusions](), [Excluded file extensions](), [HIPS exclusions]() or [Processes exclusions]().

To exclude an object (path: file or folder) from scanning, click **Add** and type the applicable path or select it in the tree structure.
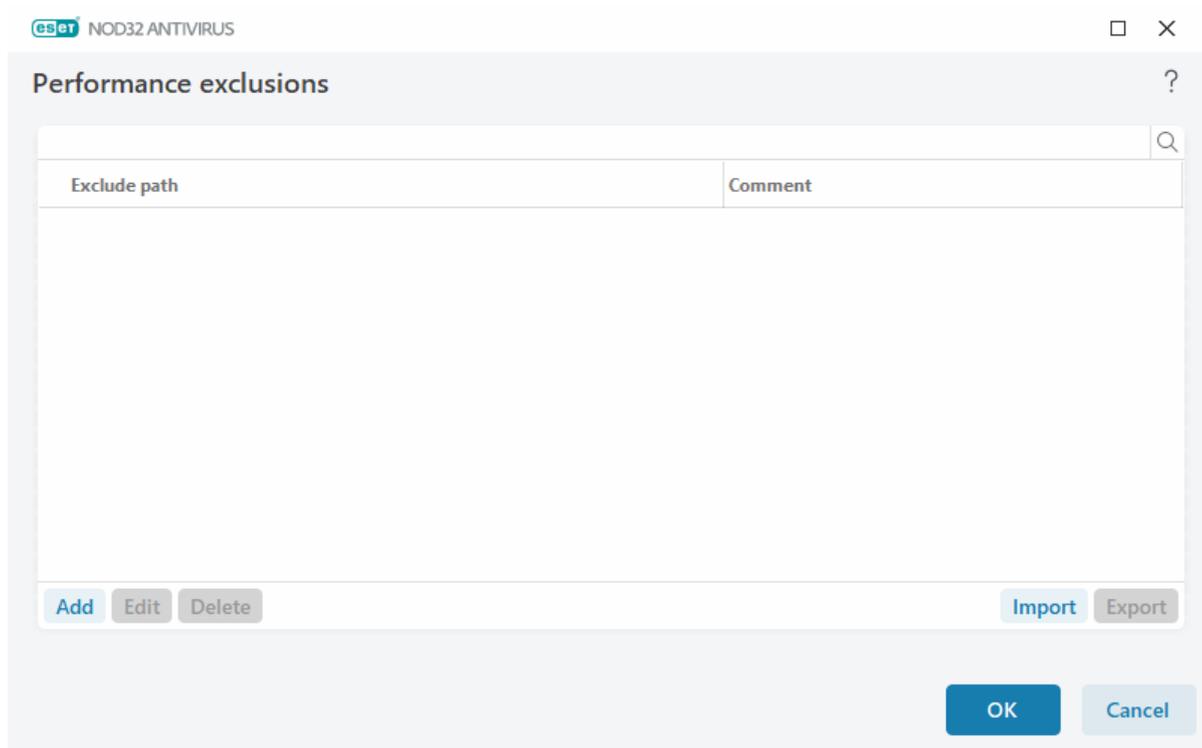
> ℹ️ A threat within a file will not be detected by the **Real-time file system protection** module or **Computer scan** module if a file meets the criteria for exclusion from scanning.

Control elements

- **Add**—Excludes objects from detection.

- **Edit**—Enables you to edit selected entries.

- **Delete**—Removes selected entries (CTRL + click to select multiple entries).

Add or Edit performance exclusion

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

> ℹ️ **Choose path or type manually**
> To choose an appropriate path, click **...** in the **Path** field.
> When typing 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 and subfolders in a folder, type the path to the folder and use the mask ***
- If you want to exclude doc files only, use the mask **.doc*
- If the name of an executable file has a certain number of characters (with varying characters) and you only know the first one (for example, "D"), use the following format:

D????.exe (question marks replace the missing/unknown characters)

✔ Examples:

- *C:\Tools**—The path must end with the backslash (\) and asterisk (*) to indicate that it is a folder and all folder content (files and subfolders) will be excluded.
- *C:\Tools*.**—Same behavior as *C:\Tools**
- *C:\Tools*—*Tools* folder will not be excluded. From the scanner perspective, *Tools* can also be a file name.
- *C:\Tools*.dat*—This will exclude .dat files in the *Tools* folder.
- *C:\Tools\sg.dat*—This will exclude this specific file located in the exact path.

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.

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

> ✔️ **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 enable you to exclude objects from detection 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.
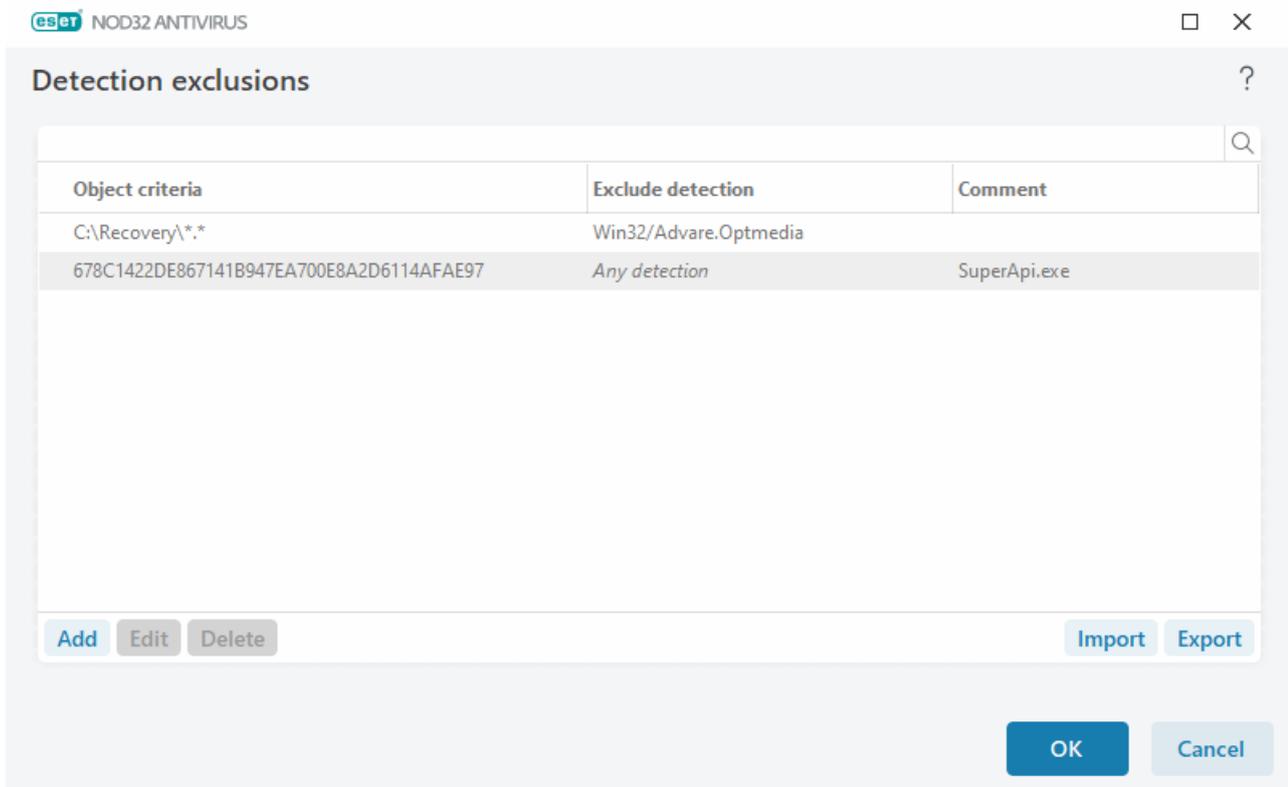
To ensure that all threats are detected, we recommend creating detection exclusions only when it is absolutely necessary.

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

> **i** Not to be confused with [Performance exclusions](#), [Excluded file extensions](#), [HIPS exclusions](#) or [Processes exclusions](#).

To [exclude an object (by its detection name or hash)](#) from detection engine, click **Add**.

For [Potentially unwanted applications](#) and [Potentially unsafe applications](#), the exclusion by its detection name can also be created:

- In the alert window reporting the detection (click **Show advanced options** and then select **Exclude from detection**).

- From the Log Files context menu using Create detection exclusion wizard.

- By clicking **Tools** > **Quarantine** and then right-clicking the quarantined file and selecting **Restore and exclude from scanning** from the context menu.

Detection exclusions object criteria

- **Path**—Limit a detection exclusion for a specified path (or any).

- **Detection name**—If there is a name of a detection next to an excluded file, it means that the file is only excluded for the given detection, not completely. If that file becomes infected later with other malware, it will be detected.

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

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 NOD32 Antivirus. Exclusions for real infiltrations are very dangerous, consider excluding only affected files / directories by clicking **...** in the **Path** field and/or only for a temporary period of time. Exclusions apply also to Potentially unwanted applications, potentially unsafe applications and suspicious applications.

See also Path exclusion format.

See the Detection exclusions example below.

Exclude hash

Excludes a file based on a specified SHA-1 hash, regardless of the file type, location, name, or extension.
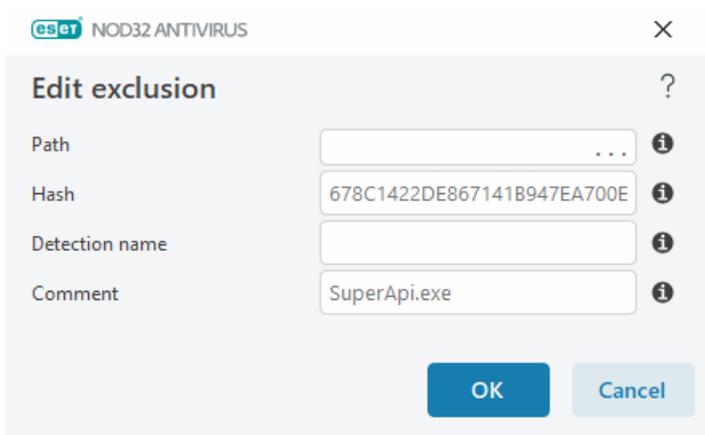
> **Exclusions by detection name**
> To exclude a specific detection by its name, type the valid detection name:
> Win32/Adware.Optmedia
> You can also use the following format when you exclude a detection from the ESET NOD32 Antivirus alert window:
> @NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
> @NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
> @NAME=Win32/Bagle.D@TYPE=worm

Control elements

- **Add**—Excludes objects from detection.

- **Edit**—Enables you to edit selected entries.

- **Delete**—Removes selected entries (CTRL + click to select multiple entries).

Create detection exclusion wizard

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

1. In the main program window, click **Tools** > **Log files**.

2. Right-click a detection in the **Detections log**.

3. Click **Create exclusion**.

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

- **Exact files**—Exclude each file by its SHA-1 hash.

- **Detection**—Exclude each file by its detection name.

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

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

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

Detection engine advanced options

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

Network traffic scanner

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

Enable Network traffic scanner—If you disable this option, HTTP(S), POP3(S) and IMAP(S) protocols will not be scanned. Note that the following ESET NOD32 Antivirus features require Network traffic scanner enabled:

- Web access protection

- SSL/TLS

- Anti-phishing protection

- Email client protection

Cloud-based protection

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

The following options are available:

Enable ESET LiveGrid® reputation system

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

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

Enable ESET LiveGrid® feedback system

In addition to the ESET LiveGrid® reputation system, ESET LiveGrid® feedback system will collect information about your computer related to newly detected threats. This information may include:

- Sample or copy of the file in which the threat appeared

- Path to the file

- Filename

- Date and time

- The process by which the threat appeared on your computer

- Information about your computer's operating system

By default, ESET NOD32 Antivirus is configured to submit suspicious files to the ESET Virus Lab for detailed analysis. Files with specific extensions such as *.doc* or *.xls* are always excluded. You can also add other extensions if there are specific files that you or your organization want to avoid sending.

> ℹ️ Read more about sending the relevant data in the [Privacy Policy](#).

You can choose not to enable ESET LiveGrid®

You will not lose any functionality in the software, but in some cases, ESET NOD32 Antivirus may respond faster to new threats when ESET LiveGrid® is enabled. 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.

> ℹ️ Read more about ESET LiveGrid® in the [Glossary](#).
> See our [illustrated instructions](#) available in English and several other languages for enabling or disabling ESET LiveGrid® in ESET NOD32 Antivirus.

Cloud-based protection configuration in Advanced setup

To access settings for ESET LiveGrid®, open [Advanced setup](#) > **Detection Engine** > **Cloud-based Protection**.

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

- **Enable ESET LiveGrid® feedback system**—Sends the 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.

- **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 products, and ensure better end-user protection.

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

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

Submission of samples

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

Automatic submission of detected samples

Select what kind of samples will be submitted to ESET for analysis and to improve future detection (the default maximum sample size is 64MB). The following options are available:

- **All detected samples**—All objects detected by the Detection engine (including potentially unwanted applications when enabled in the scanner settings).

- **All samples except documents**—All detected objects except **Documents** (see below).

- **Do not submit**—Detected objects will not be sent to ESET.

Automatic submission of suspicious samples

These samples will also be sent to ESET if the detection engine does not detect them. For example, samples that nearly missed the detection or one of the ESET NOD32 Antivirus protection modules consider these samples suspicious or behaving unclear (the default maximum sample size is 64MB).

- **Executables**—Includes executable files like .exe, .dll, .sys.

- **Archives**—Includes archive filetypes like .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

- **Scripts**—Includes script filetypes like .bat, .cmd, .hta, .js, .vbs, .ps1.

- **Other**—Includes filetypes like .jar, .reg, .msi, .sfw, .lnk.

- **Possible Spam emails**—enables sending possible spam parts or whole possible spam emails with attachments to ESET for further analysis. Enabling this option improves global spam detection, including improvements to future spam detection.

- **Documents**—Includes Microsoft Office or PDF documents with or without active content.

  ∨ Expand for a list of all included document file types

  > ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Exclusions

The Exclusion filter enables you to exclude 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.

Maximum size of samples (MB)—Defines the maximum size of automatically submitted samples (1-64 MB).

Exclusion filter for Cloud-based protection

The Exclusion filter enables you to exclude certain files or folders from samples submission. The files listed will never be sent to ESET labs for analysis, even if they contain suspicious code. Common file types (such as .doc, etc.) are excluded by default.

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

✔ To exclude files downloaded from download.domain.com, open <u>Advanced setup</u> > **Detection Engine** > **Cloud-based protection** > **Submission of samples** > **Exclusions** and add the exclusion *download.domain.com*.

Malware scans

The **Malware scans** section is accessible from <u>Advanced setup</u> > **Detection engine** > **Malware scans** and allows you to configure scanning parameters for scan profiles.

On-demand scan

Selected profile—A specific set of parameters used by the on-demand scanner. To create a new one, click **Edit** next to **List of profiles**. Refer to <u>Scan profiles</u> for more details.

After you select the scan profile, you can configure the following options:

Scan targets—If you want to scan a specific target or a group of targets, click **Edit** next to **Scan targets** and select an option from the folder (tree) structure. Refer to <u>Scan targets</u> for more details.

On-demand & Machine learning protection—You can configure reporting and protection levels for each scan profile. By default, scan profiles use the same setup as defined in the <u>Real-time file system protection</u>. Disable the toggle next to **Use real-time protection settings** to configure custom reporting and protection levels. Refer to <u>Protections</u> for a detailed explanation of reporting and protection levels.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. Refer to <u>ThreatSense</u> for more information.

Scan profiles

There are 4 pre-defined scan profiles in ESET NOD32 Antivirus:

• **Smart scan**—This is the default advanced scanning profile. The Smart scan profile uses Smart Optimization technology, which excludes files that were found to be clean in a previous scan and have not been modified

since that scan. This allows for lower scan times with a minimal impact to system security.

- **Context menu scan**—You can start an on-demand scan of any file from the context menu. The Context menu scan profile enables you to define a scan configuration that will be used when you trigger the scan this way.

- **In-depth scan**—The In-depth scan profile does not use Smart optimization by default, so no files are excluded from scanning using this profile.

- **Computer scan**—This is the default profile used in the standard computer scan.

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

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

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

Scan targets

The **Scan targets** drop-down menu enables you to select pre-defined scan targets.

- **By profile settings**—Selects targets specified by the selected scan profile.
- **Removable media**—Selects diskettes, USB storage devices, CD/DVD.

- **Local drives**—Selects all system hard drives.

- **Network drives**—Selects all mapped network drives.

- **Custom selection**—Cancels all previous selections.

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

- **Operating memory**—Scans all processes and data currently used by operating memory.

- **Boot sectors/UEFI**—Scans Boot sectors and UEFI for the presence of malware. Read more about the UEFI scanner in the glossary.

- **WMI database**—Scans the whole Windows Management Instrumentation (WMI) database, all namespaces, all class instances, and all properties. Searches for references to infected files or malware embedded as data.

- **System registry**—Scans the whole system registry, all keys, and subkeys. Searches for references to infected files or malware embedded as data. When cleaning the detections, the reference remains in the registry to make sure no important data will be lost.

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

Idle-state scan

You can enable the idle-state scanner in [Advanced setup](#) > **Detection engine** > **Malware scans** > **Idle-state scan**.

Idle-state scan

Enable the toggle next to **Enable Idle-state scanning** to enable this feature. When the computer is in idle state, a silent computer scan is performed on all local drives.

By default, the idle-state scanner will not run when the computer (notebook) is operating on battery power. You can override this setting by enabling the toggle next to **Run even if computer is powered from battery** in Advanced setup.

Enable the toggle next to **Enable logging** in Advanced setup to record a computer scan output in the [Log files](#) section (from the [main program window](#) click **Tools** > **Log files** and select **Computer scan** from the **Log** drop-down menu).

Idle-state detection

See [Idle state detection triggers](#) for a full list of conditions that must be met to trigger the idle-state scanner.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. See [ThreatSense](#) for more information.

Idle-state detection

Idle state detection settings can be configured in [Advanced setup](#) > **Detection engine** > **Malware scans** > **Idle-state scanning** > **Idle state detection**. These settings specify a trigger for [Idle-state scanning](#):

- **Turned off screen or screen saver**

- **Computer lock**

- **User logoff**

Use the toggle for each respective state to enable or disable the different idle state detection triggers.

Startup scan

By default, the automatic startup file check will be performed on system startup and during detection engine updates. This scan is dependent on the [Scheduler configuration and tasks](#).

The startup scan options are part of a **System startup file check** scheduler task. To modify its settings, navigate to **Tools** > **Scheduler**, click **Automatic startup file check** and then **Edit**. In the last step, the [Automatic startup file check](#) window will appear. For detailed instructions about Scheduler task creation and management, see [Creating](#)

new tasks.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. See ThreatSense for more information.

Automatic startup file check

When creating a System startup file check scheduled task, you have several options to adjust the following parameters:

The **Scan target** drop-down menu specifies the scan depth for files run at system startup based on a sophisticated algorithm. Files are arranged in descending order according to the following criteria:

- **All registered files** (most files scanned)

- **Rarely used files**

- **Commonly used files**

- **Frequently used files**

- **Only the most frequently used files** (least files scanned)

Two specific groups are also included:

- **Files run before user logon**—Contains files from locations that may be accessed without the user being logged in (includes almost all startup locations such as services, browser helper objects, winlogon notify, Windows scheduler entries, known dll's, etc.).

- **Files run after user logon**—Contains files from locations that may only be accessed after a user has logged in (includes files only run by a specific user, typically files in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Lists of files to be scanned are fixed for each group above. If you choose a lower scan depth for files run at system startup, the not scanned files will be scanned after opening or execution.

Scan priority—The level of priority used to determine when a scan will start:

- **When idle**—the task will be performed only when the system is idle,

- **Lowest**—when the system load is the lowest possible,

- **Lower**—at a low system load,

- **Normal**—at an average system load.

Removable media

ESET NOD32 Antivirus provides automatic removable media (CD/DVD/USB/...) scanning when inserted to a computer. This may be useful if the computer administrator wishes to prevent the users from using removable media with unsolicited content.

When a removable media is inserted, and **Show scan options** is set in Advanced setup > **Detection engine** > **Malware scans** > **Removable media**, the following dialog will be shown:
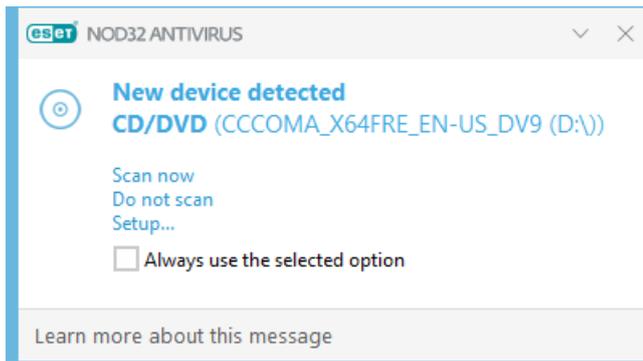
Options for this dialog:

- **Scan now**—This will trigger a scan of removable media.

- **Do not scan**—Removable media will not be scanned.

- **Setup**—Opens the Advanced setup.

- **Always use the selected option**—When selected, the same action will be performed when a removable media is inserted another time.

In addition, ESET NOD32 Antivirus features the Device control functionality, which enables you to define rules for the use of external devices on a given computer. More details on Device control can be found in the Device control section.

To access settings for removable media scan, open Advanced setup > **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 when inserting a removable media to a computer:

- **Do not scan**—No action will be performed, and the **New device detected** window will not open.

- **Automatic device scan**—A computer scan of the inserted removable media device will be performed.

- **Show scan options**—Opens the **Removable media** setup section.

Document protection

The Document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements. Document protection provides a layer of protection in addition to Real-time file system protection, and can be disabled to enhance performance on systems that do not handle a high number of Microsoft Office documents.

To activate Document protection, open Advanced setup > **Detection engine** > **Malware scans** > **Document**

protection and click the toggle next to **Enable Document protection**.

ThreatSense—Advanced setup options, such as file extensions you want to control and detection methods used. See ThreatSense for more information.

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

HIPS - Host Intrusion Prevention System

> ⚠ Changes to HIPS settings should only be made by an experienced user. Incorrect configuration of HIPS settings can lead to system instability.

The **Host Intrusion Prevention System (HIPS)** protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

You can configure HIPS settings in Advanced setup > **Detection engine** > **HIPS** > **Host Intrusion Prevention System**. The HIPS state (enabled/disabled) is shown in the ESET NOD32 Antivirus main program window > **Setup** > **Computer protection**.
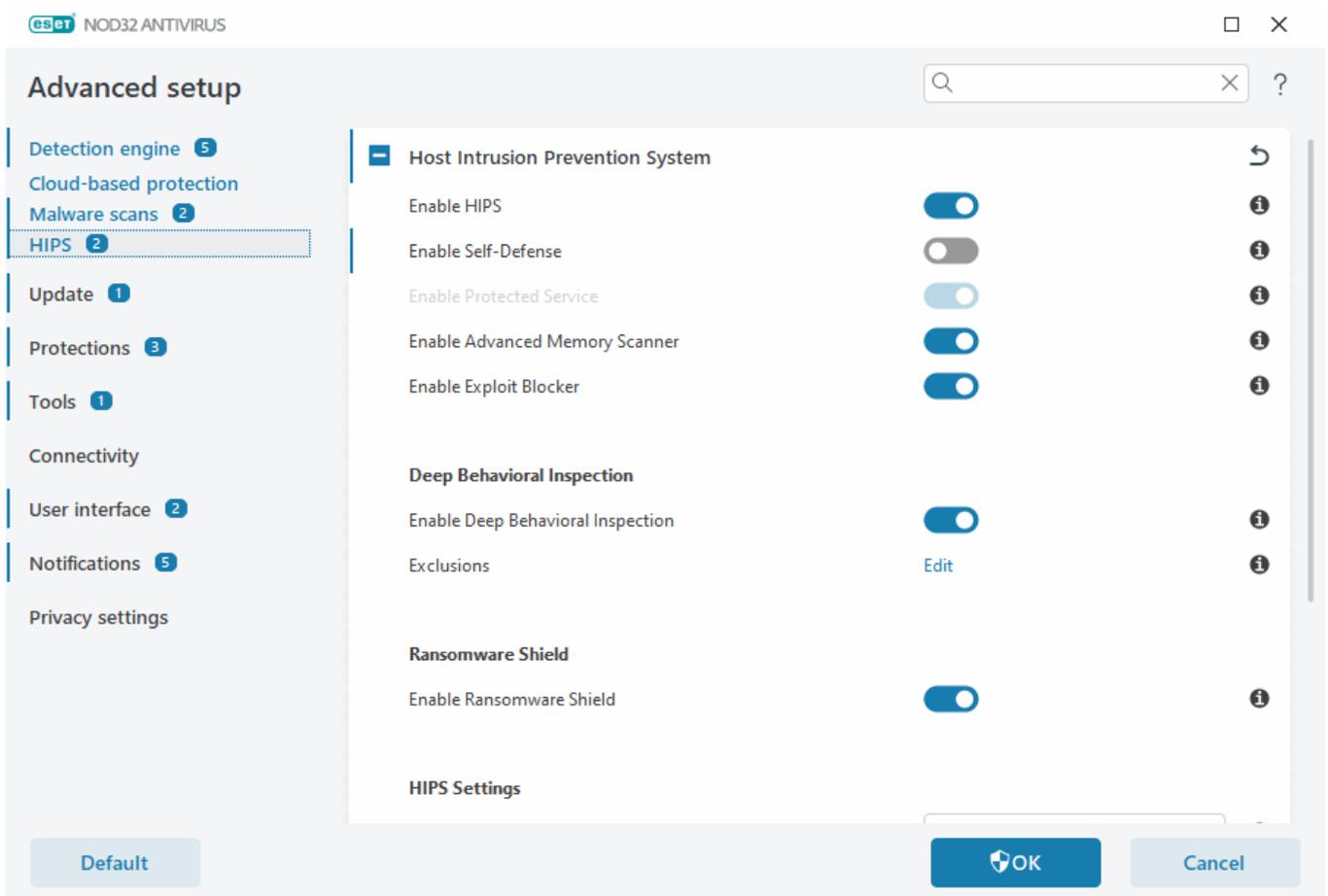
Host Intrusion Prevention System

Enable HIPS—HIPS is enabled by default in ESET NOD32 Antivirus. Turning off HIPS will disable rest of the HIPS features like Exploit Blocker.

Enable Self-Defense—ESET NOD32 Antivirus 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.

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.

Enable Advanced memory scanner—Works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation or encryption. Advanced memory scanner is enabled by default. Read more about this type of protection in the glossary.

Enable Exploit Blocker—Designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and Microsoft Office components. Exploit blocker is enabled by default. Read more about this type of protection in the glossary.

Deep Behavioral Inspection

Enable Deep Behavioral Inspection—Another layer of protection that works as a part of the HIPS feature. This extension of HIPS analyzes the behavior of all programs running on the computer and warns you if the behavior of the process is malicious.

HIPS exclusions from Deep Behavioral Inspection—Enables you to exclude processes from analysis. To ensure that all processes are scanned for possible threats, we recommend only creating exclusions when it is absolutely necessary.

Ransomware shield

Enable Ransomware shield—Another layer of protection that works as a part of HIPS feature. You must have the ESET LiveGrid® reputation system enabled for Ransomware shield to work. Read more about this type of protection.

Enable Intel® Threat Detection Technology—Helps to detect ransomware attacks by utilizing unique Intel CPU telemetry to increase detection efficacy, lower false positive alerts, and expand visibility to catch advanced evasion techniques. See the supported processors.

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.

Filtering mode	Description
Policy-based mode	Blocks all operations that are not defined by a specific rule that allows them.
Learning mode	Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the **HIPS rules** editor, but their priority is lower than the priority of rules created manually or rules created in automatic mode. When you select **Learning mode** from the **Filtering mode** drop-down menu, the **Learning mode will end at** setting will become available. Select the time span that you want to engage learning mode for, the maximum duration is 14 days. When the specified duration has passed, you will be prompted to edit the rules created by HIPS while it was in learning mode. You can also choose a different filtering mode, or postpone the decision and continue using learning mode.

Mode set after learning mode expiration—Select the filtering mode that will be used after learning mode expires. After expiration, the **Ask user** option requires administrative privileges to perform a change to the HIPS filtering mode.

The HIPS system monitors events inside the operating system and reacts accordingly based on rules similar to those used by the Firewall. Click **Edit** next to **Rules** to open the **HIPS rules** editor. In the HIPS rules window you can select, add, edit or remove rules. More details on rule creation and HIPS operations can be found in Edit a HIPS rule.

HIPS exclusions

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

To Edit HIPS exclusions, open Advanced setup > **Detection engine** > **HIPS** > **Host Intrusion Prevention System** > **Exclusions** > **Edit**.

> **i** Not to be confused with Excluded file extensions, Detection exclusions, Performance exclusions or Processes exclusions.

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

HIPS advanced setup

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

Drivers always allowed to load—Listed drivers are always allowed to load regardless of configured filtering mode unless explicitly blocked by user rule.

Log all blocked operations—All blocked operations will be written to the HIPS log. Use this feature only when troubleshooting or requested by ESET Technical Support, as it might generate a huge log file and slow down your computer.

Notify when changes occur in Startup applications—Displays a desktop notification each time an application is added to or removed from system startup.

Drivers always allowed to load

Drivers shown in this list will always be allowed to load regardless of HIPS filtering mode, unless explicitly blocked by user rule.

Add—Adds a new driver.

Edit—Edits a selected driver.

Delete—Removes a driver from the list.

> **Reset**—Reloads a set of system drivers.

> **i** 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.

> **i** After installation, the list of drivers is empty. ESET NOD32 Antivirus fills the list automatically over time.

HIPS interactive window

The HIPS notification window enables you to create a rule based on new actions that HIPS detects and then define the conditions under which to allow or deny 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 choose **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**—Choose rule file/application/registry operation(s). See descriptions for all HIPS operations.

- **Only for target**—Choose rule file/application/registry target(s).

> ### Endless HIPS notifications?
> ⚠️ To stop the notifications from appearing, change the filtering mode to **Automatic** in Advanced setup >
> **Detection engine** > **HIPS** > **Host Intrusion Prevention System**.
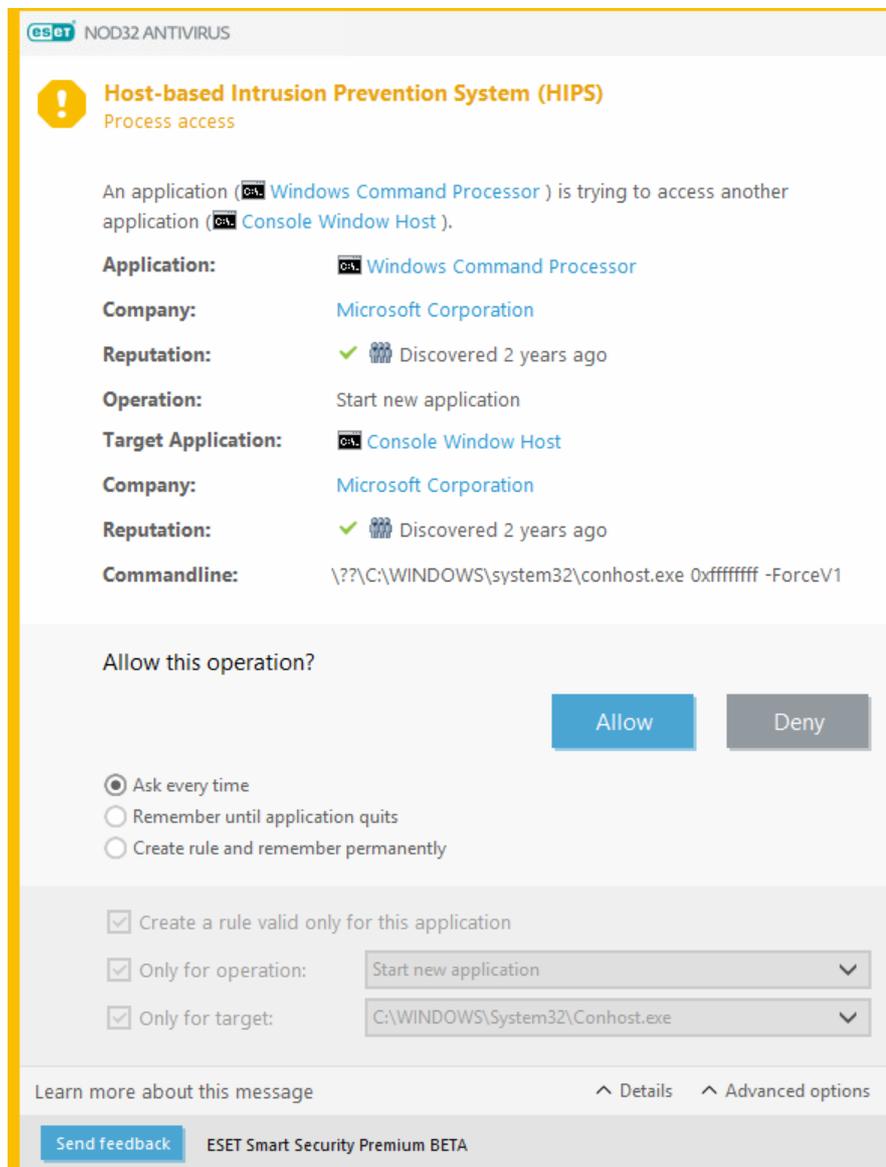
Potential ransomware behavior detected

This interactive window will appear when potential ransomware behavior is detected. You can choose to **Deny** or **Allow** the operation.
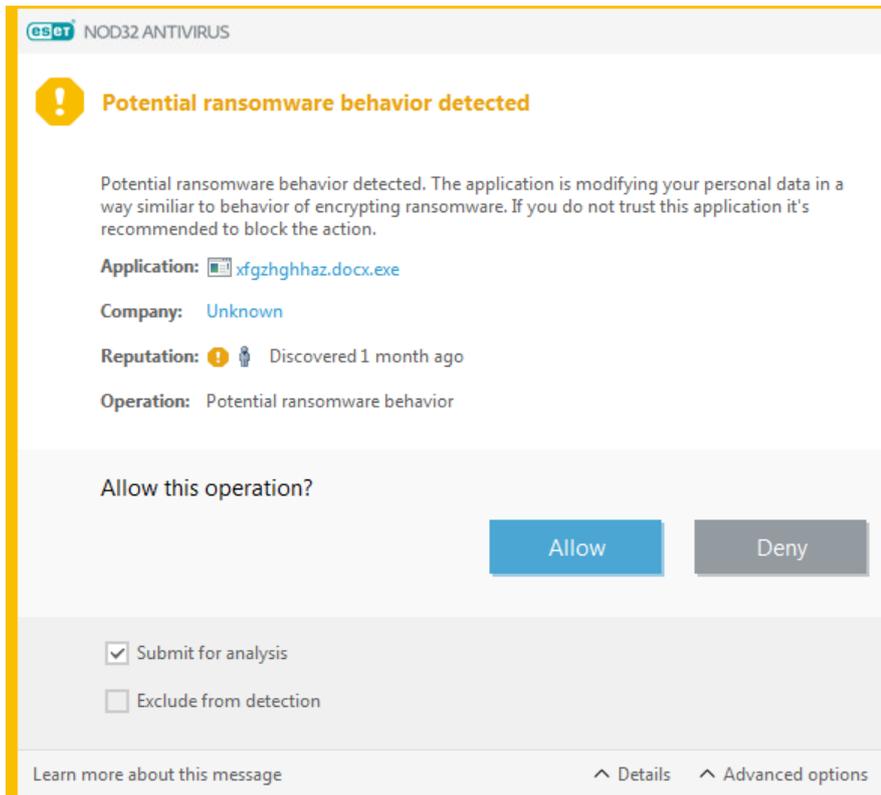
Click **Details** to view specific detection parameters. The dialog window enables you to **Submit for analysis** or **Exclude from detection**.

> 🔶 ESET LiveGrid® must be enabled for Ransomware protection to function properly.

HIPS rule management

A list of user-defined and automatically added rules from the HIPS system. More details on rule creation and HIPS operations can be found in the HIPS rule settings. See also General principle of HIPS.

Columns

Rule—User-defined or automatically chosen rule name.

Enabled—Disable the toggle 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 if the conditions are right.

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 notification window 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.

- • 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)

Edit a HIPS rule

See HIPS rule management first.

Rule name—User-defined or automatically chosen rule name.

Action—Specifies an action – **Allow**, **Block** or **Ask** – that should be performed if conditions are met.

Operations affecting—You must select the type of operation for which the rule will be applied. The rule will be used only for this type of operation and for the selected target.

Enabled—Disable the toggle if you want to keep the rule in the list but not to apply it.

Logging severity—If you activate this option, information about this rule will be written to the HIPS log.

Notify user—A small notification 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.

Target files—The rule will be used only if the operation is related to this target. Select **Specific files** from drop-down menu and click **Add** to add new files or folders or you can select **All files** from the drop-down menu to add all files.

Applications—The rule will be used only if the operation is related to this target. Select **Specific applications** from

the drop-down menu and click **Add** to add new files or folders or you can select **All applications** from the drop-down menu to add all applications.

Registry entries—The rule will be used only if the operation is related to this target. Select **Specific entries** from the drop-down menu and click **Add** to type it manually, or you can click **Open Registry Editor** to select a key from Registry. Also, you can select **All entries** from the drop-down menu to add all applications.

> ℹ️ Some operations of specific rules pre-defined by HIPS cannot be blocked and are allowed by default. In addition, not all system operations are monitored by HIPS. HIPS monitors operations that may be considered unsafe.

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.

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.

> ℹ️ You can use wildcards with certain restrictions when entering a target. Instead of a specific key the * (asterisk) symbol can be used in registry paths. For example *HKEY_USERS*\software* can mean *HKEY_USER\.default\software* but not *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** is not a valid registry key path. A registry key path containing * defines "this path, or any path on any level after that symbol". This is the only way of using wildcards for file targets. First, the specific part of a path will be evaluated, then the path following the wildcard symbol (*).

> ⚠️ 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 toggle next to **Notify user** to display a notification any time that a rule is applied.

3. Select at least one operation in the **Operations affecting** section for which the rule will be applied.

4. Click **Next**.

5. In the **Source applications** window, select **Specific applications** from the drop-down menu to apply your new rule to all applications attempting to perform any of the selected application operations on the applications you specified.

6. Click **Add** and then **...** to choose a path to a specific application and then press **OK**. Add more applications if you prefer.
For example: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Select the **Write to file** operation.

8. Select **All files** from the drop-down menu. This will block any attempts to write to any files by the selected application(s) from the previous step.

9. Click **Finish** to save your new rule.
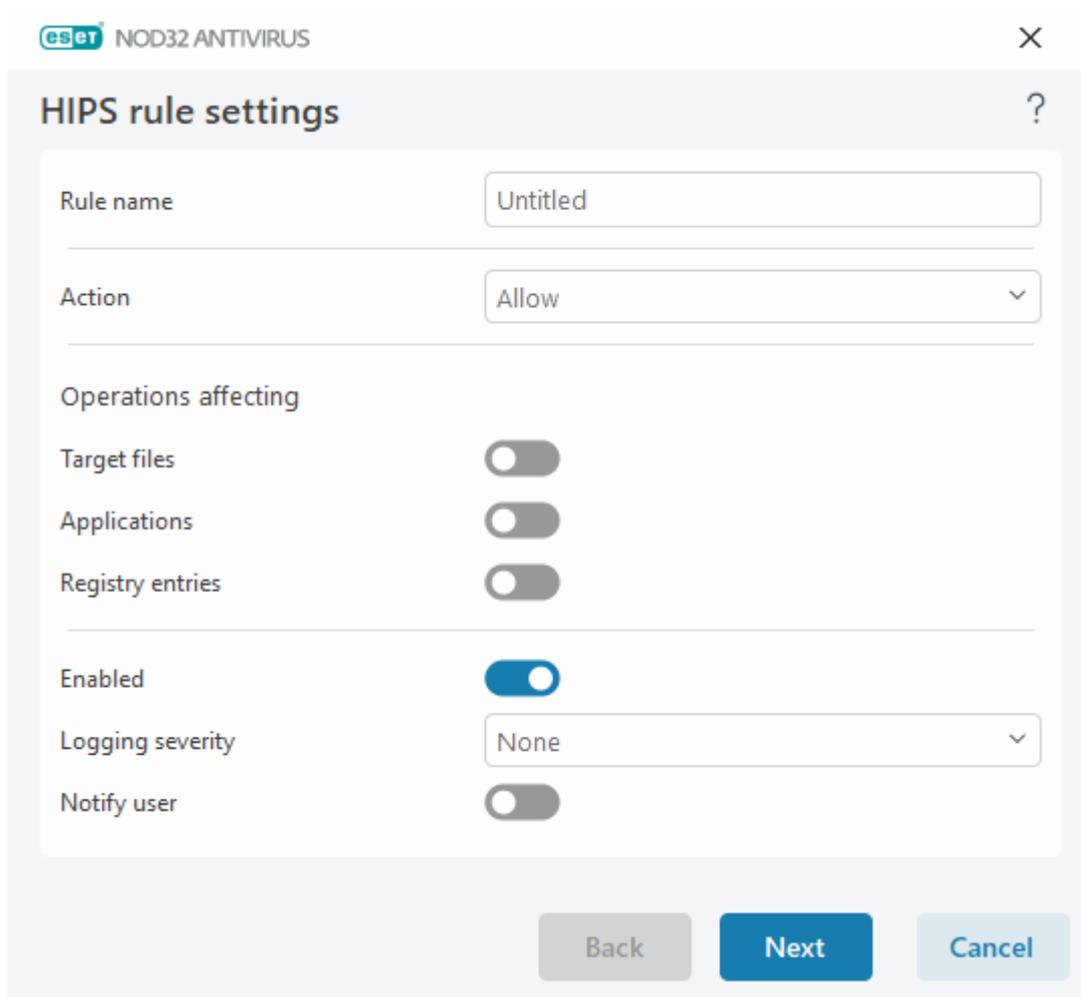
Add applicaton/registry path for HIPS

Select a file application path by clicking the **...** option. While selecting a folder, all applications located at this location will be included.

The **Open Registry Editor** option will start the Windows registry editor (regedit). While adding a registry path, type the correct location to the **Value** field.

Examples of the file or registry path:

- *C:\Program Files\Internet Explorer\iexplore.exe*

- *HKEY_LOCAL_MACHINE\system\ControlSet*

Update

Update setup options are available in [Advanced setup](#) > **Update**. This section specifies update source information like the update servers being used and authentication data for these servers.

⊟ **Update**

The update profile currently in use is displayed in the **Select default update profile** drop-down menu.

To create a new profile, see the [Update profiles](#) section.

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

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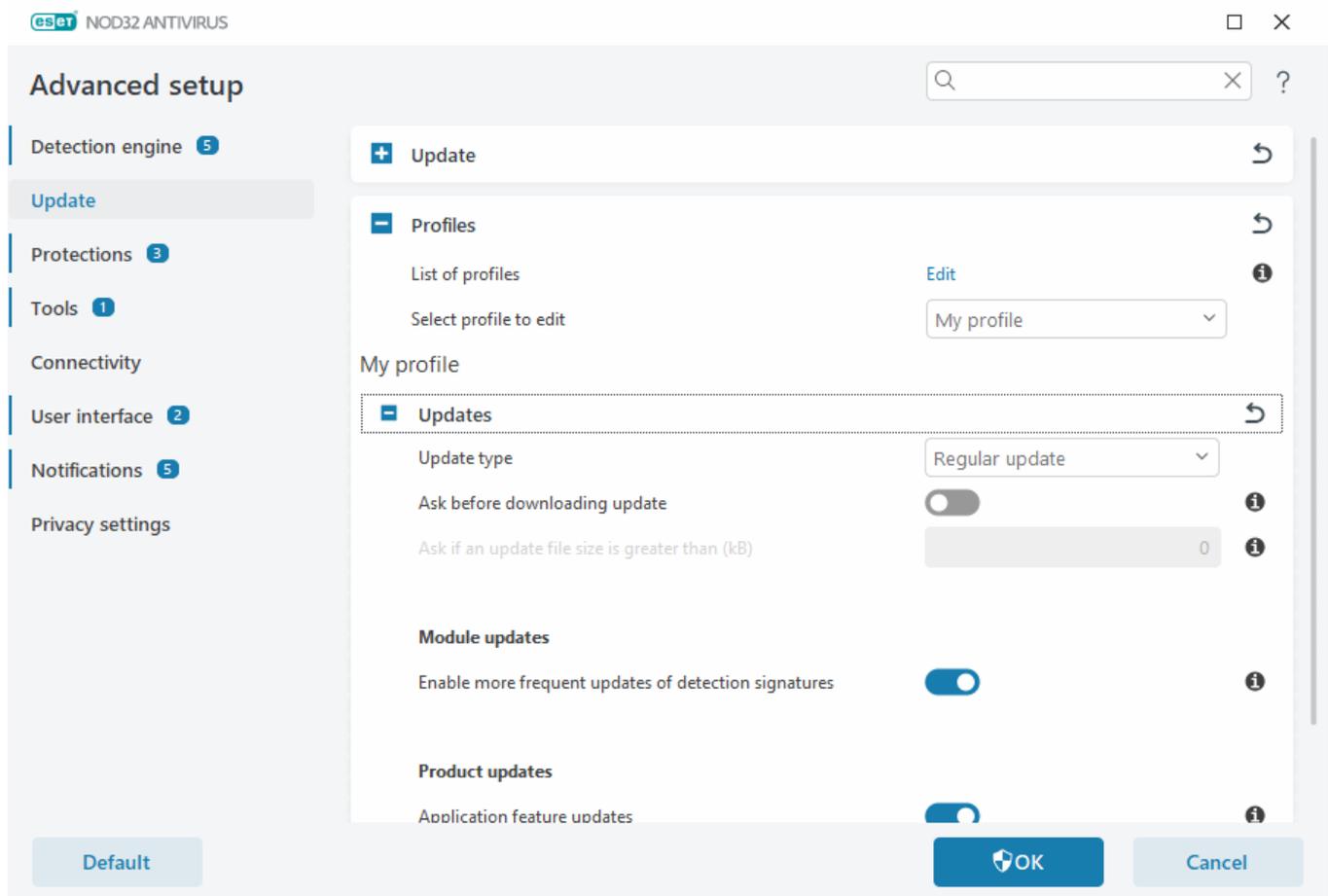
For updates to be downloaded properly, it is essential that you fill in all update parameters correctly. If you use a firewall, please make sure that your ESET program is allowed to communicate with the internet (for example, HTTP communication).

▬ Profiles

Update profiles can be created for various update configurations and tasks. Creating update profiles is especially useful for mobile users who need an alternative profile for internet connection properties that regularly change.

The **Select profile to edit** drop-down menu displays the currently selected profile and is set to **My profile** by default. To create a new profile, click **Edit** next to **List of profiles**, type your own **Profile name** and then click **Add**.

▬ Updates

By default, the **Update type** is set to **Regular update** to ensure that update files will automatically be download from the ESET server with the least network traffic. Pre-release updates (the **Pre-release update** option) are

updates that have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times and SHOULD NOT be used on production servers and workstations where maximum availability and stability is required.

Ask before downloading update—The program will display a notification where you can choose to confirm or decline update file downloads.

Ask if an update file size is greater than (kB)—The program will display a confirmation dialog if the update file size is greater than specified value. If the update file size is set to 0 kB, the program will always display a confirmation dialog.

Module updates

Enable more frequent updates of detection signatures—Detection signatures will be updated in shorter intervals. Disabling this setting may negatively impact the detection rate.

Product updates

Application feature updates—Automatically install new versions of ESET NOD32 Antivirus.

■ Connection options

To use a proxy server for downloading updates, see the Connection options section.

Update rollback

If you suspect that a new detection engine update or program modules may be unstable or corrupt, you can roll back to the previous version and temporarily disable updates. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.

ESET NOD32 Antivirus records snapshots of the detection engine and program modules for use with the rollback feature. To create virus database snapshots, keep **Create snapshots of modules** enabled. When **Create snapshots of modules** enabled, the first snapshot is created during the first update. The next one is created after 48 hours. The **Number of locally stored snapshots** field defines the number of stored detection engine snapshots.

> ℹ️ When the maximum amount of snapshots is reached (for example, three), the oldest snapshot is replaced with a new snapshot every 48 hours. ESET NOD32 Antivirus rolls back detection engine and program module update versions to the oldest snapshot.

If you click **Rollback** in Advanced setup > **Update** > **Update**, you have to select a time interval from the **Duration** drop-down menu that represents the period of time that the detection engine and program module updates will be paused.
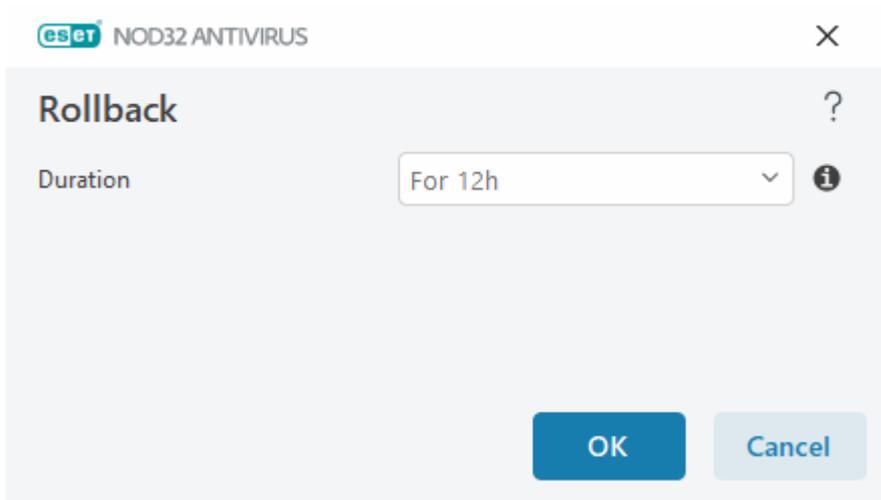
Select **Until revoked** to postpone regular updates indefinitely until you restore update functionality manually. ESET does not recommend selecting this option because it represents a potential security risk.

If a rollback is performed, the **Rollback** button changes to **Allow updates**. Updates are not allowed for the time interval selected from the **Suspend updates** drop-down menu. The detection engine version is downgraded to the oldest available version and stored as a snapshot in the local computer file system.
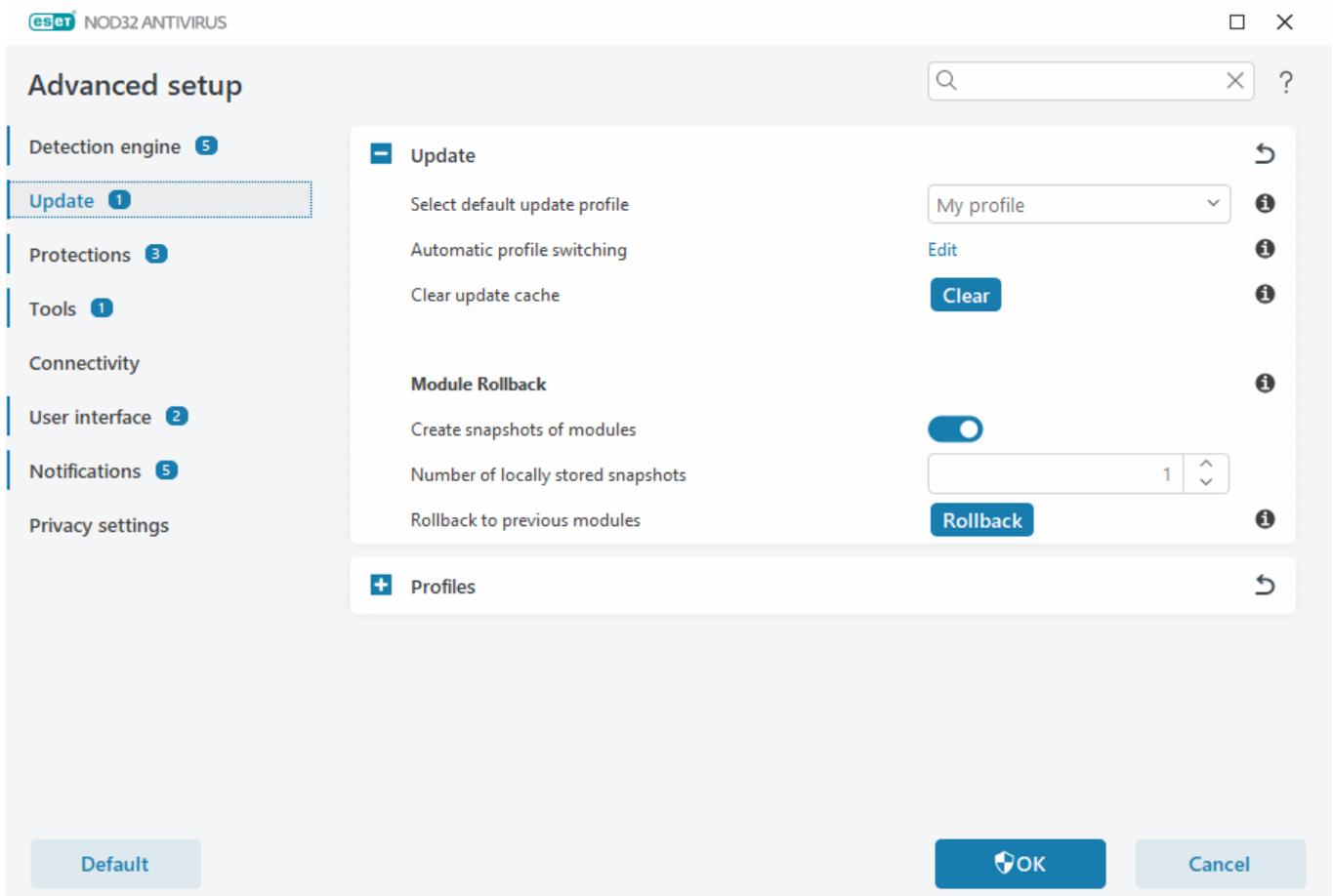
✓ Assume 22700 is the most recent detection engine version number, and 22698 and 22696 are stored as detection engine snapshots. Note that 22697 is unavailable. In this example, the computer was turned off during the 22697 update, and a more recent update was made available before 22697 was downloaded. If the **Number of locally stored snapshots** field is two and you click **Rollback**, the detection engine (including program modules) is restored to version number 22696. This process may take some time. Verify the detection engine version has downgraded on the Update screen.

Rollback time interval

If you click **Rollback** in [Advanced setup](#) > **Update** > **Update**, you have to select a time interval from the **Duration** drop-down menu that represents the period of time that the detection engine and program module updates will be paused.
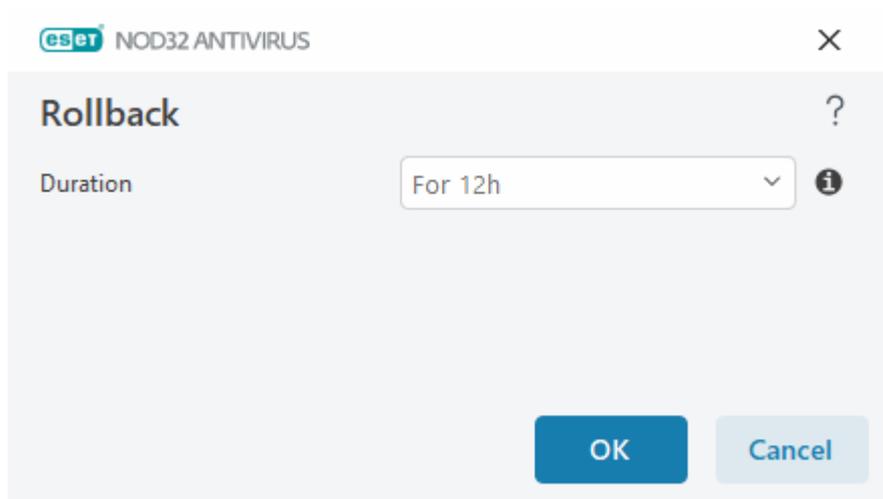
Select **Until revoked** to postpone regular updates indefinitely until you restore update functionality manually. ESET does not recommend selecting this option because it represents a potential security risk.

Product updates

The **Product updates** section enables you to install new feature updates when available automatically.

Application feature updates bring new features or change those that already exist from previous versions. It can be performed automatically without user intervention, or you can choose to be notified. After an application feature update has been installed, a computer restart may be required.

Application feature updates—When enabled, application feature updates will be performed automatically.

Connection options

To access the proxy server setup options for a specific update profile, open [Advanced setup](#) > **Update** > **Profiles** > **Updates** > **Connection options**. 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](#) already specified in [Advanced setup](#) > **Connectivity** > **Proxy server**.

Select **Do not use proxy server** to specify that no proxy server will be used to update ESET NOD32 Antivirus.

Connection through a proxy server option should be selected if:

- A different proxy server than the one defined in <u>Advanced setup</u> > **Connectivity** is used to update ESET NOD32 Antivirus. 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 NOD32 Antivirus 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.

> ℹ️ The **Username** and **Password** fields in this section are specific to the proxy server. Complete these fields only if a username and password are required to access the proxy server. These fields should only be completed if you know you need a password to access the internet via a proxy server.

Protections

Protections guard against malicious system attacks by controlling file, email and internet communications. For example, remediation will start if an object classified as malware is detected. Protections can eliminate it by blocking it and then cleaning, deleting or moving it to quarantine.

To configure protections in detail, open <u>Advanced setup</u> > **Protections**.

> ⚠️ Changes to Protections should only be made by an experienced user. Incorrect configuration of settings can lead to a decreased level of protection.

In this section:

- <u>Detection responses</u>

- <u>Reporting setup</u>

- <u>Protection setup</u>

Detection responses

Detection responses enable you to configure reporting and protection levels for the following categories:

- **Malware detections (powered by machine learning)**—A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term "virus" is often misused. "Malware" (malicious software) is a more accurate term. Malware detection is performed by the detection

engine module combined with the machine learning component. Read more about these types of applications in the Glossary.

- **Potentially unwanted applications**—Grayware or potentially unwanted applications (PUAs) is a broad category of software, whose intent is not as unequivocally malicious as other types of malware, such as viruses or trojan horses. However, it could install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user. Read more about these types of applications in the Glossary.

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

- **Potentially unsafe applications**—Refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications (PUAs) include remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). Read more about these types of applications in the Glossary.
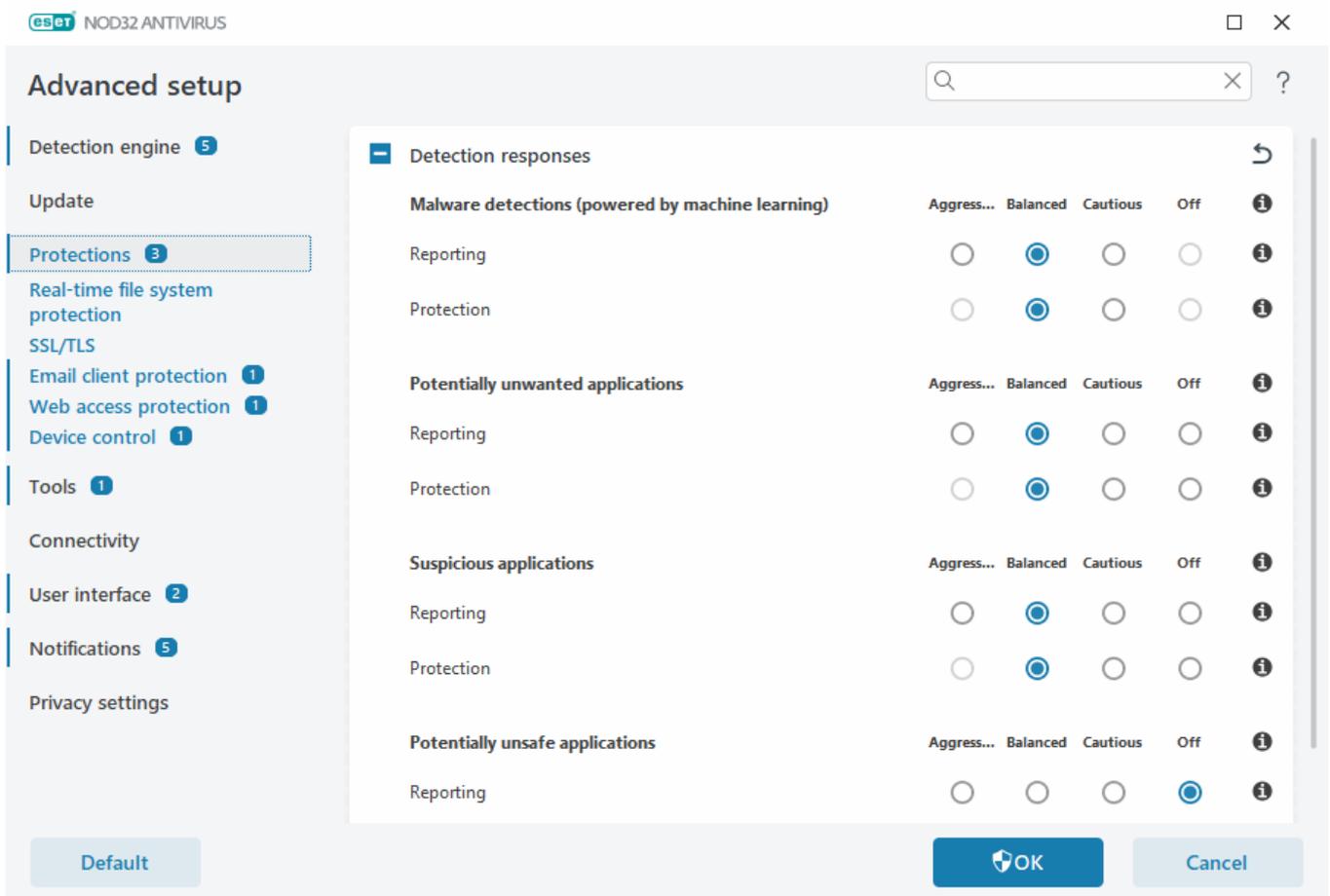
> **Improved protection**
> Advanced machine learning is now a part of the protections as an advanced layer of protection which improves detection based on machine learning. Read more about this type of protection in the Glossary.

Reporting setup

When a detection occurs (e.g., a threat is found and classified as malware), information is recorded to the

Detections log, and Desktop notifications occur if configured in ESET NOD32 Antivirus.

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

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

Reporting is performed with the detection engine, including the machine learning component. You can set a higher reporting threshold than the current protection threshold. These reporting settings do not influence blocking, cleaning or deleting objects.

Read the following before modifying a threshold (or level) for CATEGORY reporting:

Threshold	Explanation
Aggressive	CATEGORY reporting configured to maximum sensitivity. More detections are reported. The **Aggressive** setting can falsely identify objects as CATEGORY.
Balanced	CATEGORY reporting configured as balanced. This setting is optimized to balance the performance and accuracy of detection rates and the number of falsely reported objects.
Cautious	CATEGORY reporting configured to minimize falsely identified objects while maintaining a sufficient level of protection. Objects are reported only when the probability is evident and matches CATEGORY behavior.
Off	Reporting for CATEGORY is not active, and detections of this type are not found, reported or cleaned. As a result, this setting disables protection from this detection type. Off is not available for malware reporting and it is the default value for potentially unsafe applications.

∨ Availability of ESET NOD32 Antivirus protection modules

Availability (enabled or disabled) of a protection module for a selected CATEGORY threshold is as follows:

	Aggressive	Balanced	Cautious	Off*
Advanced machine learning module	✓ (aggressive mode)	✓ (conservative mode)	X	X
Detection engine module	✓	✓	✓	X
Other protection modules	✓	✓	✓	X

*Not recommended.

∨ Determine product version, program module versions and build dates

1. Click **Help and support** > **About ESET NOD32 Antivirus**.
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 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 NOD32 Antivirus and its modules up-to-date to maximize the balance between performance and accuracy of detection rates and the number of falsely reported objects.

Protection setup

If an object classified as CATEGORY is reported, the program blocks the object and then cleans, deletes or moves it to Quarantine.

Read the following before modifying a threshold (or level) for CATEGORY protection:

Threshold	Explanation
Aggressive	Reported aggressive (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started. This setting is recommended when all endpoints have been scanned with aggressive settings and falsely reported objects have been added to detection exclusions.
Balanced	Reported balanced (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Cautious	Reported cautious level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Off	Useful to identify and exclude falsely reported objects. Off is not available for malware protection and it is the default value for potentially unsafe applications.

Real-time file system protection

Real-time file system protection controls all files in the system for malicious code when opened, created, or run.
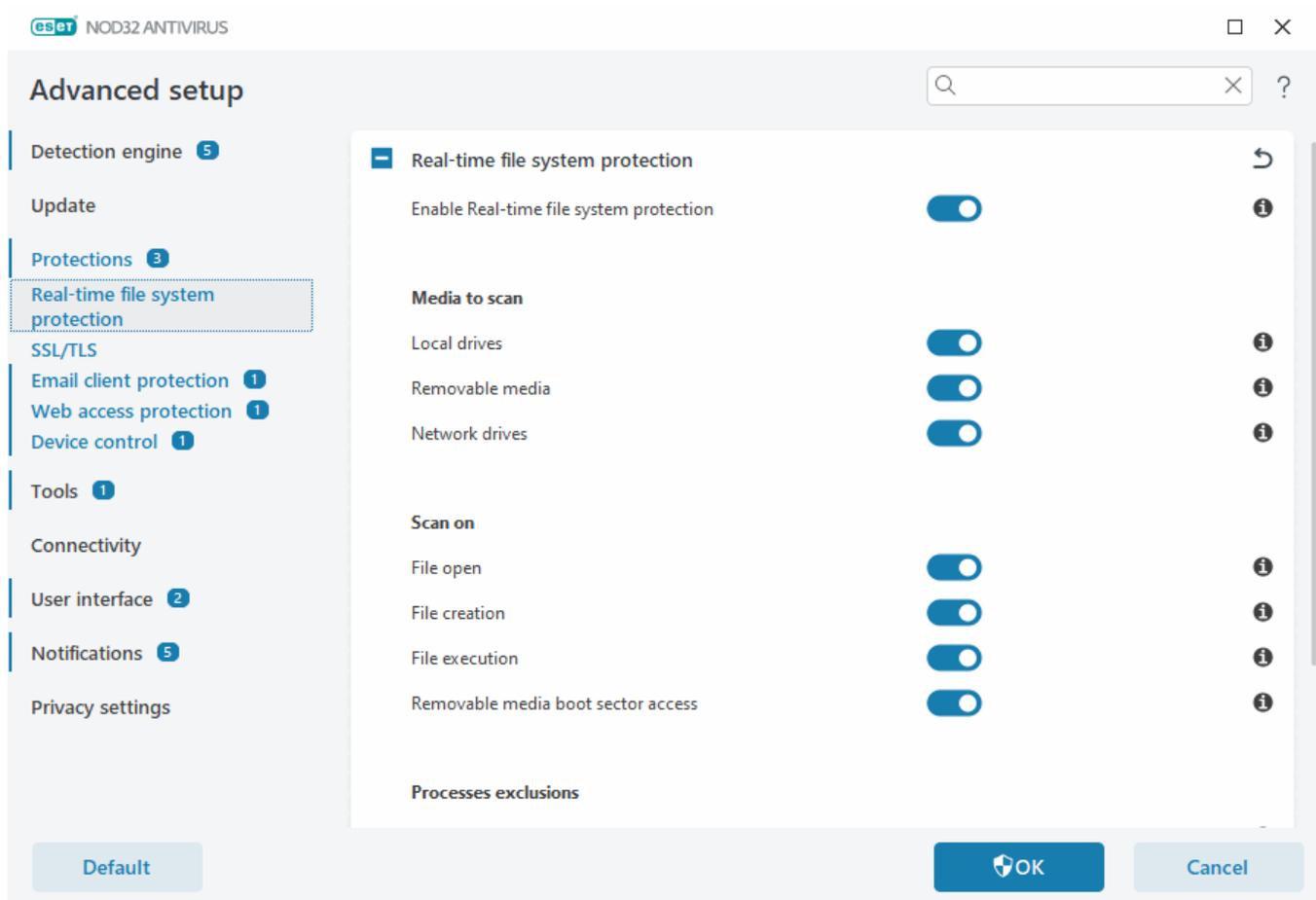
By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. We do not recommend disabling **Enable Real-time file system protection** in Advanced setup > **Protections** > **Real-time file system protection** > **Real-time file system protection**.

Media to scan

By default, all types of media are scanned for potential threats:

- **Local drives**—Scans all system and fixed hard drives (example: *C:*, *D:*).

- **Removable media**—Scans CD/DVDs, USB storage, memory cards, etc.

- **Network drives**—Scans all mapped network drives (example: *H:* as *\\store04*) or direct access network drives (example: *\\store08*).

We recommend that you use default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

Scan on

By default, all files are scanned when opened, created, or executed. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:

- **File open**—Scans when a file is opened.

- **File creation**—Scans a created or modified file.

109

- **File execution**—Scans when a file is executed or run.

- **Removable media boot sector access**—When removable media that contains a boot sector is inserted into the device, the boot sector is immediately scanned. This option does not enable removable media file scanning. Removable media file scanning is located **Media to scan** > **Removable media**. For **Removable media boot sector access** to work correctly, keep **Boot sectors/UEFI** enabled in ThreatSense.

Processes exclusions

See Processes exclusions.

ThreatSense

Real-time file system protection checks all types of media and is triggered by various system events, such as accessing a file. Using **ThreatSense** technology detection methods (as described in ThreatSense), Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to monitor newly created files more closely.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each detection engine update. This behavior is controlled using **Smart optimization**. If this **Smart optimization** is disabled, all files are scanned each time they are accessed. To modify this setting, open Advanced setup > **Protections** > **Real-time file system protection**. Click **ThreatSense** > **Other** and select or deselect **Enable Smart optimization**.

Real-time file system protection also enables you to configure Additional ThreatSense parameters.

Processes exclusions

The Processes exclusions feature enables you to exclude application processes from Real-time file system protection. To improve backup speed, process integrity and service availability, some techniques that are known to conflict with file-level malware protection are used during backup. The only effective way to avoid both situations is to deactivate Anti-Malware software. By excluding specific process (for example those of the backup solution) all file operations attributed to such excluded process are ignored and considered safe, thus minimizing interference with the backup process. We recommend that you use caution when creating exclusions – a backup tool that has been excluded can access infected files without triggering an alert which is why extended permissions are only allowed in the real-time protection module.

> **i** Not to be confused with Excluded file extensions, HIPS exclusions, Detection exclusions or Performance exclusions.

Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (*.exe*).

You can add executable files into the list of excluded processes in Advanced setup > **Protections** > **Real-time file system protection** > **Real-time file system protection** > **Processes exclusions**.

This feature was designed to exclude backup tools. Excluding the backup tool's process from scanning not only ensures system stability, but it also does not affect backup performance as the backup is not slowed down while it

is running.

> ✓ Click **Edit** to open the **Processes exclusions** management window, where you can add exclusions and browse for executable file (for example *Backup-tool.exe*), which will be excluded from scanning. As soon as the *.exe* file is added to the exclusions, activity of this process is not monitored by ESET NOD32 Antivirus and no scanning is run on any file operations performed by this process.

> ⚠ If you do not use browse function when selecting process executable, you need to manually type a full path to the executable. Otherwise, the exclusion will not work correctly and HIPS may report errors.

You can also **Edit** existing processes or **Delete** them from exclusions.

> ℹ Web access protection does not take into account this exclusion, so if you exclude the executable file of your web browser, downloaded files are still scanned. This way an infiltration can still be detected. This scenario is an example only, and we do not recommend that you create exclusions for web browsers.

Add or Edit processes exclusions

This dialog window enables you to **add** processes excluded from detection engine. Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (*.exe*).

> ✓ Select the file path of an excepted application by clicking ... (for example *C:\Program Files\Firefox\Firefox.exe*). Do NOT type the name of the application. As soon as the *.exe* file is added to the exclusions, activity of this process is not monitored by ESET NOD32 Antivirus and no scanning is run on any file operations performed by this process.

> ⚠ If you do not use browse function when selecting process executable, you need to manually type a full path to the executable. Otherwise, the exclusion will not work correctly and HIPS may report errors.

You can also **Edit** existing processes or **Delete** them from exclusions.

When to modify real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Always be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases.

After installing ESET NOD32 Antivirus, all settings are optimized to provide the maximum level of system security for users. To restore default settings, click ↺ next to Advanced setup > **Protections** > **Detection responses**.

Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from *www.eicar.com*. This test file is a harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs.

The file is available for download at http://www.eicar.org/download/eicar.com
After you type this URL into your browser, you should see a message that the threat has been removed.

What to do if real-time protection does not work

This topic describes problems that may arise when using real-time protection and how to troubleshoot them.

Real-time protection is disabled

If a user inadvertently disables real-time protection, you should reactivate the feature. To reactivate real-time protection, go to **Setup** in the main program window and click **Computer protection** > **Real-time file system protection**.

If real-time protection is not initiated at system startup, it is usually because **Enable Real-time file system protection** is disabled. To ensure that this option is enabled, open Advanced setup > **Protections** > **Real-time file system protection**.

If real-time protection does not detect and clean infiltrations

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

Real-time protection does not start

If real-time protection is not initiated at system startup (and **Enable Real-time file system protection** is enabled), it may be due to conflicts with other programs. To resolve the issue, create an ESET SysInspector log and submit it to ESET Technical Support for analysis.

SSL/TLS

ESET NOD32 Antivirus can check for communication threats that use the SSL protocol. You can use various filtering modes to examine SSL-protected communication with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking. To edit SSL/TLS settings, open Advanced setup > **Protections** > **SSL/TLS**.
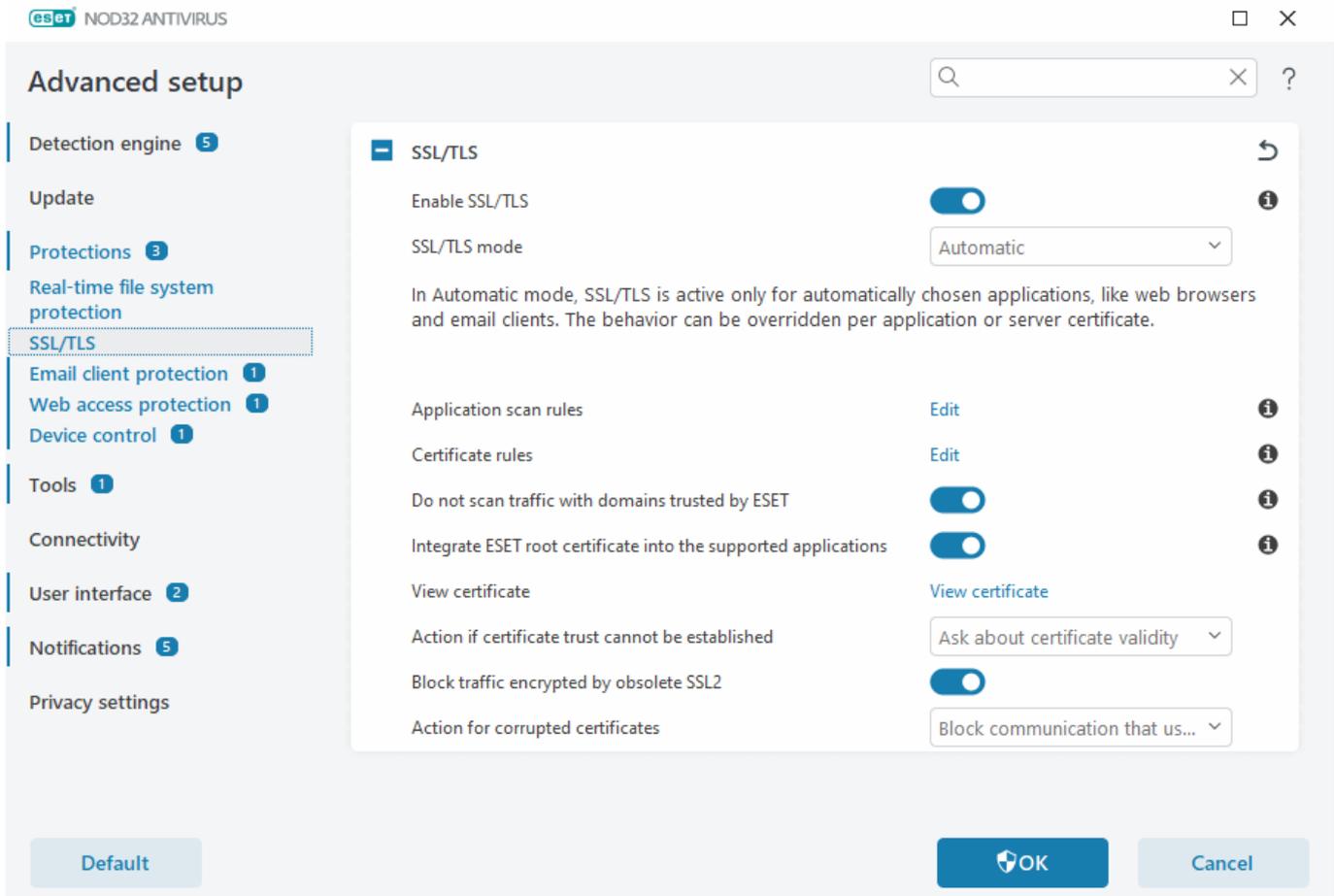
Enable SSL/TLS—If disabled, ESET NOD32 Antivirus will not scan communication over SSL/TLS.

SSL/TLS mode is available in the following options:

Filtering mode	Description
Automatic	The default mode will only scan appropriate applications, such as web browsers and email clients. You can override it by selecting the applications where communication is scanned.
Interactive	If you access a new SSL-protected site (with an unknown certificate), an action selection dialog is displayed. This mode allows you to create a list of SSL certificates/applications that will be excluded from scanning.
Policy-based	Select this option to scan all SSL-protected communication, except communication protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate marked as trusted (it is on the trusted certificates list), communication to the server is allowed, and the communication channel content is filtered.

Application scan rules—Allows you to customize ESET NOD32 Antivirus behavior for specific applications.

Certificate rules—Allows you to customize ESET NOD32 Antivirus behavior for specific SSL certificates.

Do not scan traffic with domains trusted by ESET—When enabled, communication with trusted domains will be excluded from scanning. An ESET-managed, built-in whitelist determines a domain's trustworthiness.

Integrate ESET root certificate into the supported applications—For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root

certificates (publishers). When enabled, ESET NOD32 Antivirus will automatically add the ESET SSL Filter CA certificate to known browsers (for example, Opera). For browsers using the system certification store, the certificate is added automatically. For example, Firefox is automatically configured to trust Root authorities in the system certification store.

To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File** and manually import it into the browser.

Action if certificate trust cannot be established—In some cases, a website certificate cannot be verified using the Trusted Root Certification Authorities (TRCA) store (for example, expired certificate, untrusted certificate, certificate not valid for the specific domain or signature that can be parsed but does not sign the certificate correctly). Legitimate websites will always use trusted certificates. If they are not providing one, it could mean that an attacker is decrypting your communication or the website is experiencing technical difficulties.

If **Ask about certificate validity** is selected (selected by default), you will be prompted to choose an action when encrypted communication is established. An action selection dialog will be displayed where you can mark the certificate as trusted or excluded. If the certificate is not present in the TRCA list, the window is red. If the certificate is on the TRCA list, the window will be green.

You can select **Block communication that uses the certificate** to always terminate an encrypted connection to a site that uses an untrusted certificate.

Block traffic encrypted by obsolete SSL2—Communication using the earlier version of the SSL protocol will automatically be blocked.

Action for corrupted certificates—A corrupted certificate means that the certificate uses a format not recognized by ESET NOD32 Antivirus or has been received damaged (for example, overwritten by random data). In this case, we recommend leaving **Block communication that uses the certificate** selected. If **Ask about certificate validity** is selected, the user is prompted to choose an action when the encrypted communication is established.

> **i** Illustrated examples
> The following ESET Knowledgebase article may only be available in English:
> • Certificate notifications in ESET Windows home products
> • "Encrypted network traffic: Untrusted certificate" is displayed when visiting web pages

Application scan rules

The **Application scan rules** can be used to customize ESET NOD32 Antivirus behavior for specific applications and remember actions chosen when **SSL/TLS mode** is in **Interactive mode**. The list can be viewed and edited in Advanced setup > **Protections** > **SSL/TLS** > **Application scan rules** > **Edit**.

The **Application scan rules** window consists of:

Columns

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

Scan action—Select **Scan** or **Ignore** to scan or ignore communication. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** to always ask the user what to do.

Control elements

Add—Add filtered application.

Edit—Select the application you want to configure and click **Edit**.

Delete—Select the application you want to delete and click **Delete**.

Import/**Export**—Import applications from a file or save your current list of applications to a file.

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

Certificate rules

Certificate rules can be used to customize ESET NOD32 Antivirus behavior for specific SSL certificates and to remember actions chosen when **SSL/TLS mode** is in **Interactive mode**. The list can be viewed and edited in [Advanced setup](#) > **Protections** > **SSL/TLS** > **Certificate rules** > **Edit**.

The **Certificate rules** window consists of:

Columns

Name—Name of the certificate.

Certificate issuer—Name of the certificate creator.

Certificate subject—The subject field identifies the entity associated with the public key stored in the subject public key field.

Access—Select **Allow** or **Block** as the **Access action** to allow/block communication secured by this certificate regardless of its trustworthiness. Select **Auto** to allow trusted certificates and ask for untrusted ones. Select **Ask** to always ask user what to do.

Scan—Select **Scan** or **Ignore** as the **Scan action** to scan or ignore communication secured by this certificate. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** to always ask the user what to do.

Control elements

Add—Add a new certificate and adjust its settings regarding access and scan options.

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

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

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

Encrypted network traffic

If your system is configured to use SSL/TLS scanning, a dialog window prompting you to choose an action will be displayed in two situations:

First, if a website uses an unverifiable or invalid certificate, and ESET NOD32 Antivirus is configured to ask the user in such cases (by default yes for unverifiable certificates, no for invalid ones), a dialog box will ask you whether to **Allow** or **Block** the connection. If the certificate is not located in the Trusted Root Certification Authorities store (TRCA), it is considered untrusted.

Second, if **SSL/TLS mode** is set to **Interactive mode**, a dialog box for each website will ask whether to **Scan** or **Ignore** the traffic. Some applications verify that their SSL traffic is not modified nor inspected by anyone, in such cases ESET NOD32 Antivirus must **Ignore** that traffic to keep the application working.

> **i** **Illustrated examples**
> The following ESET Knowledgebase article may only be available in English:
> - Certificate notifications in ESET Windows home products
> - "Encrypted network traffic: Untrusted certificate" is displayed when visiting web pages

In both cases, the user can choose to remember the selected action. Saved actions are stored in the Certificate rules.

Email client protection

To configure the Email client protection, open Advanced setup > **Protections** > **Email client protection**, and choose from the following configuration options:

- Mail transport protection

- Mailbox protection

- ThreatSense

Mail transport protection

IMAP(S) and POP3(S) protocols are the most widespread protocols used to receive email communication in an email client application. The Internet Message Access Protocol (IMAP) is another internet protocol for email retrieval. IMAP has some advantages over POP3, for example, multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. The protection module providing this control is automatically initiated at system startup and is then active in memory.

ESET NOD32 Antivirus provides protection for these protocols regardless of the email client used, and without requiring re-configuration of the email client. By default, all communication over POP3 and IMAP protocols is scanned, regardless of the default POP3/IMAP port numbers.
MAPI protocol is not scanned. However the communication with the Microsoft Exchange server can be scanned by the integration module in email clients such as Microsoft Outlook.

ESET NOD32 Antivirus 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 NOD32 Antivirus checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. Encrypted communication will be scanned by default. To view the scanner setup, open Advanced setup > **Protections** > SSL/TLS.

To configure Mail transport protection, open Advanced setup > **Protections** > **Email client protection** > **Mail transport protection**.

Enable Mail transport protection—When enabled, mail transport communication will be scanned by ESET NOD32 Antivirus.

You can choose which mail transport protocols will be scanned by clicking the toggle next to the following options (by default, scanning of all protocols is enabled):

- **Scan IMAP mail transport**

- **Scan IMAPS mail transport**

- **Scan POP3 mail transport**

- **Scan POP3S mail transport**

By default, ESET NOD32 Antivirus will scan IMAPS and POP3S communication on the standard ports. To add custom ports for IMAPS and POP3S protocols, add them to the text field next to **Ports used by IMAPS protocol** or **Ports used by POP3S protocol**. Multiple port numbers must be delimited by a comma.

Excluded applications—Enables you to exclude specific applications from being scanned by Mail transport protection. Useful when Web access protection causes compatibility issues.

Excluded IPs—Enables you to exclude specific remote addresses from being scanned by Mail transport protection. Useful when Web access protection causes compatibility issues.

Excluded applications

To exclude scanning of communication for specific applications, add them to the list. HTTP(S)/POP3(S)/IMAP(S) communication of the selected applications will not be checked for threats. We recommend only using this for applications that do not work properly with their communication being scanned.

Running applications and services will be available here automatically when you click **Add**. Click **...** and navigate to an application to add exclusion manually.

Edit—Edit selected entries from the list.

Delete—Remove selected entries from the list.

ⓔⓢⓔⓣ NOD32 ANTIVIRUS

Excluded applications

?

Add   Edit   Delete   Import   Export

OK   Cancel

Excluded IPs

The entries in the list will be excluded from scanning. HTTP(S)/POP3(S)/IMAP(S) communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Click **Add** to exclude an IP address/address range/subnet of a remote point.

Click **Edit** to change selected IP address.

Click **Delete** to remove the selected entries from the list.

> **IP addresses examples**
>
> Add IPv4 address:
> **Single address**—Adds an IP address of an individual computer (for example, *192.168.0.10*).
> **Address range**—Type the starting and ending IP addresses to specify the IP range of several computers (for example, *192.168.0.1-192.168.0.99*).
> **Subnet**—Subnet (a group of computers) defined by an IP address and mask. For example, 255.255.255.0 is the network mask for the 192.168.1.0 subnet. To exclude the whole subnet type in *192.168.1.0/24*.
> Add IPv6 address:
> **Single address**—Adds the IP address of an individual computer (for example, *2001:718:1c01:16:214:22ff:fec9:ca5*).
> **Subnet**—Subnet (a group of computers) is defined by an IP address and mask (for example, *2002:c0a8:6301:1::1/64*).

Mailbox protection

Integration of ESET NOD32 Antivirus with your Mailbox increases the level of active protection against malicious code in email messages.

To configure Mailbox protection, open Advanced setup > **Protections** > **Email client protection** > **Mailbox protection**.

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

Select emails to scan:

- **Received email**

- **Sent email**

- **Read email**

- **Modified email**

> ℹ️ We recommend that you keep **Enable email protection by client plugins** enabled. Even if integration is not enabled or functional, email communication is still protected by Mail transport protection (IMAP/IMAPS and POP3/POP3S).

Attachment handling optimization—If optimization is disabled, all attachments are scanned immediately. You may experience an email client performance slowdown.

Integrations—Enables you to integrate Mailbox protection into your Email client. See Integrations for more information.

Response—Enables you to customize handling of spam messages. See Response for more information.

Integrations

Integration of ESET NOD32 Antivirus with your email client increases the level of active protection against malicious code in email messages. If your email client is supported, you can enable integration in ESET NOD32 Antivirus. When integrated into your email client, the ESET NOD32 Antivirus toolbar is inserted directly into the email client for more efficient email protection. To edit Integration settings, open Advanced setup > **Protections** > **Email client protection** > **Mailbox protection** > **Integration**.

Integrate into Microsoft Outlook—Microsoft Outlook is currently the only supported email client. Email protection works as a plugin. The main advantage of the plugin is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. See this ESET Knowledgebase article for a complete list of supported Microsoft Outlook versions.

Advanced email client processing—Processes extra Outlook Messaging API (MAPI) events: Object modified (`fnevObjectModified`) and Object created (`fnevObjectCreated`). If you are experiencing a system slowdown when working with your email client, disable this option.

Microsoft Outlook toolbar

Microsoft Outlook protection works as a plugin module. After ESET NOD32 Antivirus is installed, this toolbar containing the antivirus protection options is added to Microsoft Outlook:

ESET NOD32 Antivirus—Double-click the icon to open the main window of ESET NOD32 Antivirus.

Rescan messages—Enables you to launch email checking manually. You can specify messages that will be checked, and you can activate rescanning of the received emails. For more information, see Mailbox protection.

Scanner setup—Displays Mailbox protection setup options.

Confirmation dialog

This notification serves to verify that the 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 NOD32 Antivirus toolbar integrated in email clients enables users to specify several options for email checking. The option **Rescan messages** offers two scanning modes:

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

Selected messages only—Scans only messages marked by the user.

The **Rescan already scanned messages** checkbox provides the user with the option to run another scan on messages that have been scanned before.

Response

Based on the message scan results, ESET NOD32 Antivirus can move scanned messages or add custom text to subject. You can configure these settings in [Advanced setup](#) > **Protections** > **Email client protection** > **Mailbox protection** > **Response**.

If there is a message containing detection, by default, ESET NOD32 Antivirus attempts to clean the message. If the message cannot be cleaned, you can choose an **Action to take if cleaning not possible**:

- **No action**—If enabled, the program will identify infected attachments but will leave emails without taking any action.

- **Delete email**—The program will notify the user about infiltration(s) and delete the message.

- **Move email to the Deleted items folder**—Infected emails will be moved automatically to the Deleted items folder.

- **Move email to folder** (default action)—Infected emails will be moved automatically to the specified folder.

Folder—Specify the custom folder where you want to move infected emails when detected.

After an email has been checked, a notification with the scan result can be appended to the message. You can elect to **Append tag messages to received and read email** or **Append tag messages to sent email**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The following options are available:

- **Never**—No tag messages will be added.

- **When a detection occurs**—Only messages containing malicious software will be marked as checked (default).

- **To all email when scanned**—The program will append messages to all scanned email.

Update subject of received and read email / Update subject of sent email—Enable this option to add custom text specified below to the message.

Text to add to subject of detected email—Edit this template if you want to modify the subject prefix format of an infected email. This function will replace the message subject "Hello" to the following format: "[detection %DETECTIONNAME%] Hello". The variable %DETECTIONNAME% represents the detection.

ThreatSense

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options enable you to specify several scan parameters:

- File types and extensions that are to be scanned

- The combination of various detection methods

- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense** in the [Advanced setup](#) for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection

- Idle-state scanning

- Startup scan

- Document protection

- Email client protection

- Web access protection

- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section enables you to define which computer components and files will be scanned for infiltrations.

Operating memory—Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI—Scans boot sectors for the presence of malware in the master boot record. [Read more about UEFI in the glossary](#).

Email files—The program supports the following extensions: DBX (Outlook Express) and EML.

Archives—The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives—Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers—After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics—A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist or was not covered by the previous versions of the detection engine module. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures—Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of ESET NOD32 Antivirus while cleaning objects. There are 4 levels of cleaning:

ThreatSense has the following remediation (i.e. cleaning) levels.

Remediation in ESET NOD32 Antivirus

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.
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 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.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters for an On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS)—Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority—Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects—The Scan log will show all the scanned files in self-extracting archives, even those not infected (may generate a lot of scan log data and increase the scan log file size).

Enable Smart optimization—With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the specific modules are applied when performing a scan.

Preserve last access timestamp—Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

▬ Limits

The Limits section enables you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size—Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited.

Maximum scan time for object (sec.)—Defines the maximum time value for the scan of files in a container object (such as a RAR/ZIP archive or an email with multiple attachments). This setting does not apply for standalone files. If a user-defined value has been 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 enables you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. The maximum value is **3 GB**.

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

Web access protection

Web access protection allows you to configure advanced Internet protection module settings. The following options are available in Advanced setup > **Protections** > **Web access protection** > **Web access protection**:

Enable Web access protection—When disabled, Web access protection and Anti-Phishing protection does not run.

> ℹ We strongly recommend you leave Web access protection enabled and not exclude any applications or IP addresses by default.

Scan browser scripts—When enabled, the detection engine checks all JavaScript programs executed by web browsers.

Enable Anti-Phishing protection—When enabled, phishing web pages are blocked. See Anti-Phishing protection for more information.

Excluded applications—Enables you to exclude specific applications from being scanned by Web access protection. Useful when Web access protection causes compatibility issues.

Excluded IPs—Enables you to exclude specific remote addresses from being scanned by Web access protection. Useful when Web access protection causes compatibility issues.
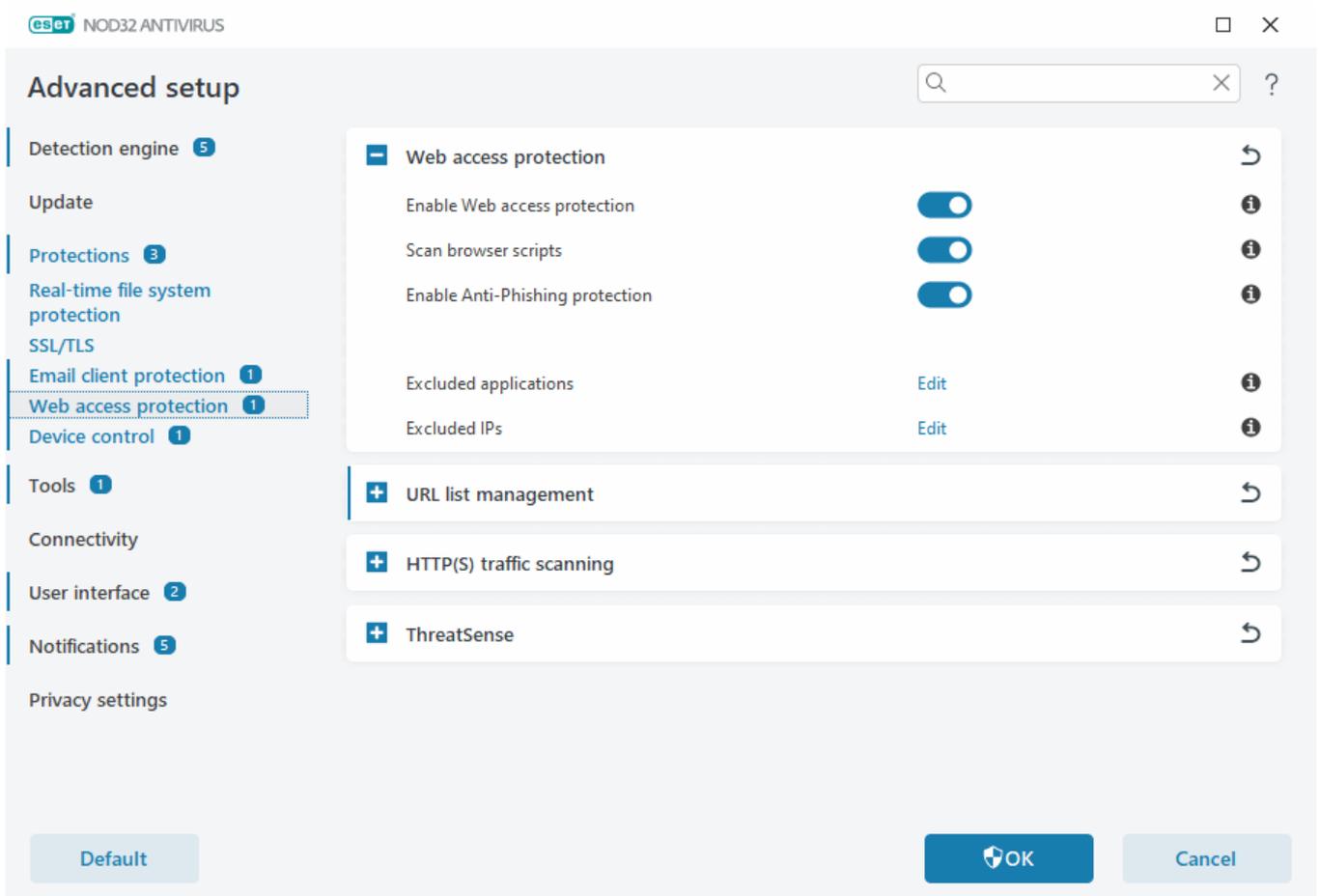
Web access protection will display the following message in your browser when the website is blocked:

Threat found

This web page contains potentially dangerous content.

Threat: HTML/ScrInject.B trojan

Access to it has been blocked. Your computer is safe.

Open ESET Knowledgebase | www.eset.com

> **Illustrated instructions**
> The following ESET Knowledgebase articles may only be available in English:
> • Exclude a safe website from being blocked by Web Access Protection
> • Block a website using ESET NOD32 Antivirus

Excluded applications

To exclude scanning of communication for specific applications, add them to the list. HTTP(S)/POP3(S)/IMAP(S) communication of the selected applications will not be checked for threats. We recommend only using this for applications that do not work properly with their communication being scanned.

Running applications and services will be available here automatically when you click **Add**. Click **...** and navigate to an application to add exclusion manually.

Edit—Edit selected entries from the list.

Delete—Remove selected entries from the list.

Excluded IPs

The entries in the list will be excluded from scanning. HTTP(S)/POP3(S)/IMAP(S) communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Click **Add** to exclude an IP address/address range/subnet of a remote point.

Click **Edit** to change selected IP address.

Click **Delete** to remove the selected entries from the list.

> **IP addresses examples**
> Add IPv4 address:
> **Single address**—Adds an IP address of an individual computer (for example, *192.168.0.10*).
> **Address range**—Type the starting and ending IP addresses to specify the IP range of several computers (for example, *192.168.0.1-192.168.0.99*).
> **Subnet**—Subnet (a group of computers) defined by an IP address and mask. For example, 255.255.255.0 is the network mask for the 192.168.1.0 subnet. To exclude the whole subnet type in *192.168.1.0/24*.
> Add IPv6 address:
> **Single address**—Adds the IP address of an individual computer (for example, *2001:718:1c01:16:214:22ff:fec9:ca5*).
> **Subnet**—Subnet (a group of computers) is defined by an IP address and mask (for example, *2002:c0a8:6301:1::1/64*).

URL list management

The **URL list management** in <u>Advanced setup</u> > **Protections** > **Web access protection** enables you to specify HTTP addresses to block, allow or exclude from content scan.

<u>SSL/TLS</u> must be enabled if you want to filter HTTPS addresses in addition to HTTP. Otherwise only the domains of HTTPS sites that you have visited will be added, the full URL will not be.

Websites in the **List of blocked addresses** will not be accessible unless they are also included in the **List of allowed addresses**. Websites in the **List of addresses excluded from content scan** are not scanned for malicious code when accessed.

If you want to block all HTTP addresses except addresses present in the active **List of allowed addresses**, add * to the active **List of blocked addresses**.

The special symbols * (asterisk) and ? (question mark) can be used in lists. The asterisk substitutes any character string, and the question mark substitutes any symbol. Pay attention when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and

? are used correctly in this list. See Add HTTP address / domain mask for how a whole domain including all subdomains can be matched safely. To activate a list, select **List active**. If you want to be notified when entering an address from the current list, select **Notify when applying**.

> ℹ **Addresses Trusted by ESET**
> If **Do not scan traffic with domains trusted by ESET** is enabled in SSL/TLS, domains on whitelist managed by ESET will not be affected by URL list management configuration.
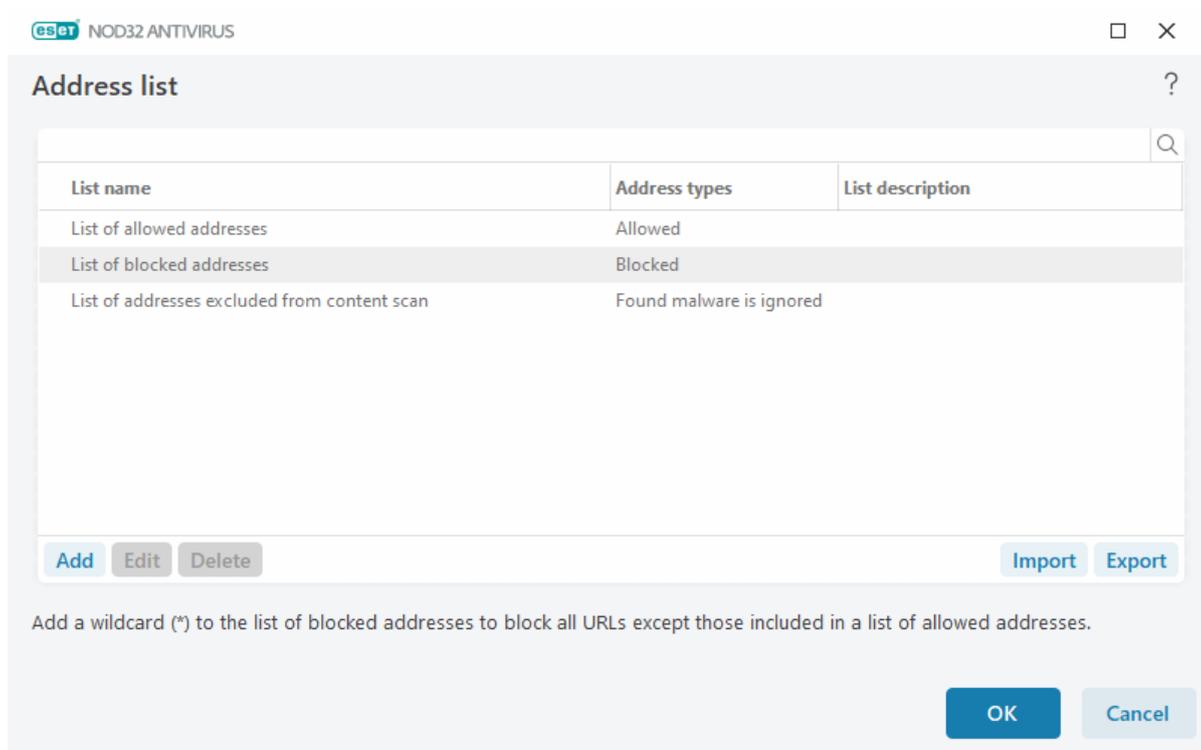
Control elements

Add—Creates a new list in addition to the pre-defined ones. This can be useful if you want to logically split different groups of addresses. For example, one list of blocked addresses may contain addresses from an external public blacklist, and a second one may contain your own blacklist, making it easier to update the external list while keeping yours intact.

Edit—Modifies existing lists. Use this to add or remove addresses.

Delete—Deletes existing lists. Only available for lists created with **Add**, not for default lists.

Address list

In this section you can specify lists of HTTP(S) addresses that will be blocked, allowed or excluded from checking.

By default, the following three lists are available:

- **List of addresses excluded from content scan**—No checking for malicious code will be performed for any address added to this list.

- **List of allowed addresses**—If allow access only to HTTP addresses in the list of allowed addresses is enabled and the list of blocked addresses contains * (match everything), the user will be allowed to access

addresses specified in this list only. The addresses in this list are allowed even if they are included in the list of blocked addresses.

- **List of blocked addresses**—The user will not be allowed to access addresses specified in this list unless they also occur in the list of allowed addresses.

Click **Add** to create a new list. To delete selected lists, click **Delete**.
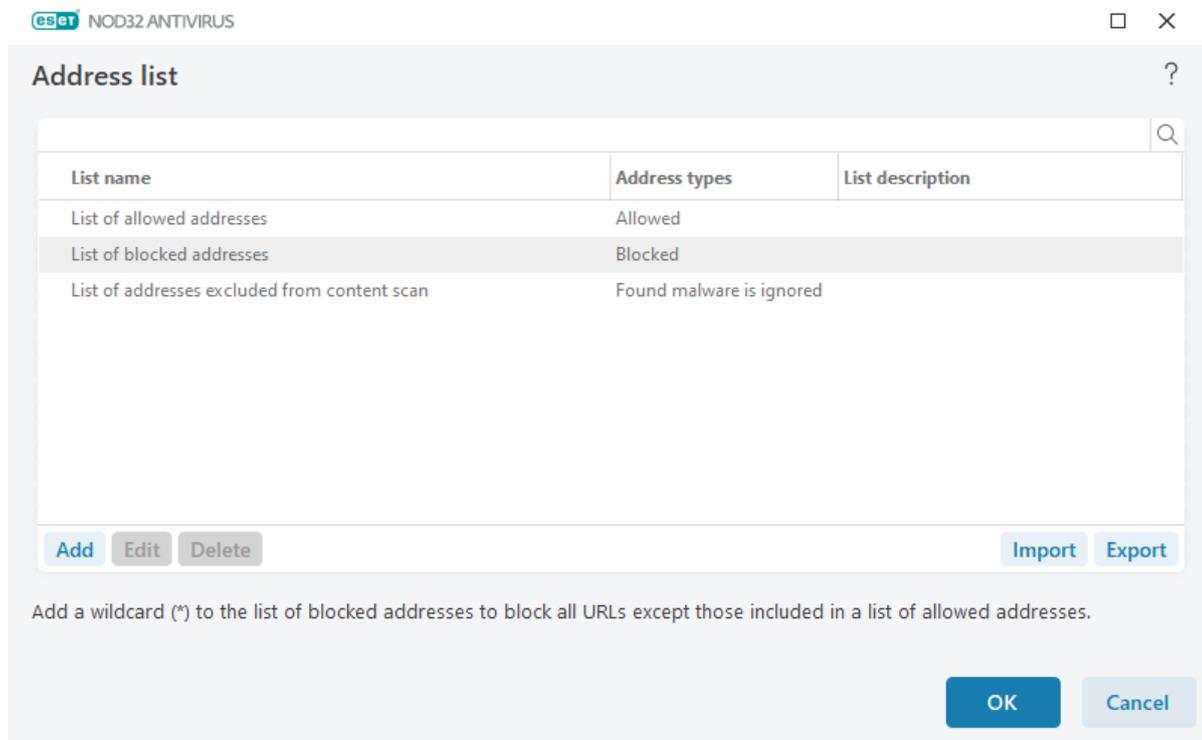
For more information see URL list management.

Create new Address list

This dialog window enables you to configure a new list of URL addresses/masks that will be blocked, allowed or excluded from checking.

You can configure the following options:

Address list type—Three list types are available:

- **Found malware is ignored**—No checking for malicious code will be performed for any address added to this list.

- **Blocked**—Access to addresses specified in this list will be blocked.

- **Allowed**—Access to addresses specified in this list will be allowed. Addresses in this list are allowed even if they match the list of blocked addresses.

List name—Specify the name of the list. This field will be unavailable when editing one of the pre-defined lists.

List description—Type a short description for the list (optional). Unavailable when editing one of the pre-defined list.

To activate a list, select **List active** next to that list. If you want to be notified when a specific list is used when accessing websites, select **Notify when applying**. For example, you will receive a notification when a website is blocked or allowed because it is included in list of blocked or allowed addresses. The notification will contain the name of the list.

Logging severity—information about the specific list being used when accessing websites can be written to the Log files.

Control elements

Add—Add a new URL address to the list (type multiple values with separator).

Edit—Modifies existing address in the list. Only available for addresses created with **Add**.

Delete—Deletes existing addresses in the list. Only available for addresses created with **Add**.

Import—Import a file with URL addresses (separate values with a line break, for example, *.txt using encoding UTF-8).

How to add URL mask

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

ESET NOD32 Antivirus enables user to block access to specified websites and prevent the internet browser from displaying their content. Furthermore, it enables 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.

HTTP(S) traffic scanning

By default, ESET NOD32 Antivirus is configured to scan the HTTP and HTTPS traffic which is used by internet browsers and other applications. You should disable the traffic scanning only if you are experiencing problems with a 3rd party software and want to know if the issue is caused by ESET NOD32 Antivirus.

Enable HTTP traffic scanning—HTTP traffic is always monitored on all ports for all applications.

Enable HTTPS traffic scanning—HTTPS traffic uses an encrypted channel to transfer information between server and client. ESET NOD32 Antivirus checks communication utilizing the SSL (Secure Socket Layer) and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by HTTPS protocol**, regardless of operating system version (you can add ports to the pre-defined 443 and 0-65535).

ThreatSense

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options enable you to specify several scan parameters:

- File types and extensions that are to be scanned

- The combination of various detection methods

- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense** in the Advanced setup for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection

- Idle-state scanning

- Startup scan

- Document protection

- Email client protection

- Web access protection

- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense

parameters unchanged for all modules except Computer scan.

Objects to scan

This section enables you to define which computer components and files will be scanned for infiltrations.

Operating memory—Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI—Scans boot sectors for the presence of malware in the master boot record. [Read more about UEFI in the glossary](#).

Email files—The program supports the following extensions: DBX (Outlook Express) and EML.

Archives—The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives—Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers—After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics—A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist or was not covered by the previous versions of the detection engine module. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures—Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of ESET NOD32 Antivirus while cleaning objects. There are 4 levels of cleaning:

ThreatSense has the following remediation (i.e. cleaning) levels.

Remediation in ESET NOD32 Antivirus

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.

Cleaning level	Description
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 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.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters for an On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS)—Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority—Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects—The Scan log will show all the scanned files in self-extracting archives, even those not infected (may generate a lot of scan log data and increase the scan log file size).

Enable Smart optimization—With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the specific modules are applied when performing a scan.

Preserve last access timestamp—Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

▬ Limits

The Limits section enables you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size—Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited.

Maximum scan time for object (sec.)—Defines the maximum time value for the scan of files in a container object (such as a RAR/ZIP archive or an email with multiple attachments). This setting does not apply for standalone files. If a user-defined value has been 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 enables you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. The maximum value is **3 GB**.

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

Device control

ESET NOD32 Antivirus provides automatic device (CD/DVD/USB/etc.) control. You can block or adjust extended filters/permissions and define a user's ability to access and work with a given device. This may be useful if the computer administrator wants to prevent using devices containing unsolicited content.

Supported external devices:

- Disk Storage (HDD, USB removable disk)

- CD/DVD

- USB Printer

- FireWire Storage

- Bluetooth Device

- Smart card reader

- Imaging Device

- Modem

- LPT/COM port

- Portable Device (battery-powered devices such as media players, smartphones, plug-and-play devices, etc.)

- All device types

Device control setup options can be modified in Advanced setup > **Protections** > **Device control**.

Click the **Enable Device control** toggle to enable the Device control feature in ESET NOD32 Antivirus; you must restart your computer for this change to take effect. After enabling Device control, you can define the **Rules** in the Rules editor window.

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

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.
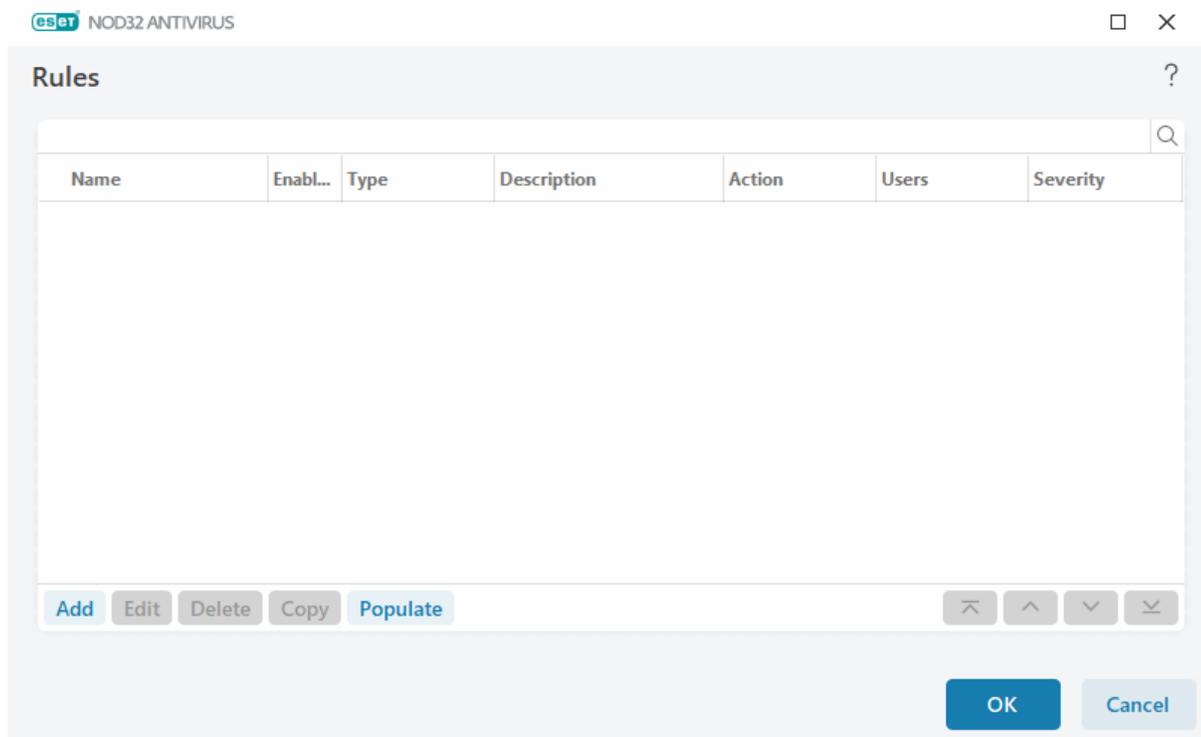
Specific devices can be allowed or blocked per user or user group and based on additional device parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as name, type of external device, action to perform after connecting an external device to your computer and logging severity. See also Adding Device control rules.

Click **Add** or **Edit** to manage a rule. Click **Copy** to create a new rule with pre-defined options used for another

selected rule. XML strings displayed when clicking a rule can be copied to the clipboard to help system administrators export/import these data and use them.

By pressing **CTRL** and clicking, you can select multiple rules and apply actions, such as deleting or moving them up or down the list, to all selected rules. The **Enabled** check box disables or enables a rule; this can be useful if you want to keep the 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.

Log entries can be viewed in the main program window > **Tools** > Log files.

The Device control log records all occurrences where Device control is triggered.

Detected devices

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

Select a device from the list of Detected devices and click **OK** to add a device control rule with pre-defined information (all settings can be adjusted).

Devices in low power (sleep) mode are marked with a warning icon ⚠. To enable the **OK** button and add a rule for this device:

- Reconnect the device

- Use the device (for example, start the Camera app in Windows to wake up a webcam)

Adding Device control rules

A Device control rule defines an action to take when a device meeting the rule criteria is connected to the computer.

Type a description of the rule into the **Name** field for better identification. Click the toggle next to **Rule enabled** to disable or enable this rule; this can be useful if you do not want to delete the rule permanently.

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.

Action

Access to non-storage devices can either be allowed or blocked. In contrast, rules for storage devices enable you to select one of the following rights settings:

- **Allow**—Full access to the device will be allowed.
- **Block**—Access to the device will be blocked.
- **Write Block**—Only read access to the device will be allowed.
- **Warn**—Each time a device is connected, the user will be notified if it is allowed/blocked, and a log entry will be recorded. Devices are not remembered and a notification will still be displayed in case of subsequent connections of the same device.

Not all actions (permissions) are available for all device types. If it is a device of storage type, all four actions are

available. For non-storage devices, there are only three actions available (for example, **Write Block** is not available for Bluetooth; therefore, Bluetooth devices can only be allowed, blocked or warned).

Criteria type

Select **Device group** or **Device**.

Additional parameters shown below can be used to fine-tune rules for different devices. All parameters are case-sensitive and support wildcards (*, ?):

- **Vendor**—Filter by vendor name or ID.

- **Model**—The given name of the device.

- **Serial**—External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

> ℹ If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-sensitive and support wildcards (a question mark (?) represents a single character, whereas an asterisk (*) represents a string of zero or more characters).

> ℹ 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

ESET NOD32 Antivirus saves all important events in a log file, which can be viewed directly from the main menu. Click **Tools** > **Log files** and then select **Device control** from the **Log** drop-down menu.

- **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.

- **None**—No logs will be recorded.

User list

Rules can be limited to certain users or user groups by adding them to the User list clicking **Edit** next to **User list**.

- **Add**—Opens the **Object types: Users or Groups** dialog window that enables you to select desired users.

- **Delete**—Removes the selected user from the filter.

Notify user—If a device blocked by an existing rule is inserted, a notification window will be displayed.

Device groups

> ⚠ A device connected to your computer may pose a security risk.

The Device groups window is divided into two parts. The right part of the window contains a list of devices belonging to the respective group, and the left part contains created groups. Select a group to display devices in the right pane.

When you open the Device groups window and select a group, you can add or remove devices from the list. Another way to add devices to the group is to import them from a file. Alternatively, you can click **Populate** button, and all devices connected to your computer will be listed in the **Detected devices** window. Select devices from the populated list to add them to the group by clicking **OK**.

Control elements

Add—You can add a group by typing its name or a device to an existing group, depending on which part of the window you clicked the button.

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

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

Import—Imports a list of devices from a text file. Importing devices from a text file requires correct formatting:

- Each device starts at a new line.

- **Vendor**, **Model**, and **Serial** must be present for each device and separated with a comma.

> ✔ Here is an example of the text file content:
> ```
> Kingston,DT 101 G2,001CCE0DGRFC0371
> 04081-0009432,USB2.0 HD WebCam,20090101
> ```

Export—Exports a list of devices to a file.

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

Add device

Click **Add** in the right window to add a device to an existing group. Additional parameters shown below can be used to fine-tune rules for different devices. All parameters are case-sensitive and support wildcards (*, ?):

- **Vendor**—Filter by vendor name or ID.

- **Model**—The given name of the device.

- **Serial**—External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

- **Description**—Your description of the device for better organization.

> ℹ️ The rule will ignore these fields while matching if these parameters are undefined. Filtering parameters in all text fields are case-sensitive and support wildcards (a question mark [?] represents a single character, whereas an asterisk [*] represents a string of zeros or more characters).

Click **OK** to save changes. Click **Cancel** to leave the **Device groups** window without saving changes.

> ℹ️ After creating a device group, you have to add a new device control rule for the created device group and choose the action to take.

Not all actions (permissions) are available for all device types. All four actions are available if it is a storage-type device. For non-storage devices, only three actions are available (for example, **Write Block** is not available for Bluetooth; therefore, Bluetooth devices can only be allowed, blocked or warned).

ThreatSense

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options enable you to specify several scan parameters:

- File types and extensions that are to be scanned

- The combination of various detection methods

- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense** in the Advanced setup for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection

- Idle-state scanning

- Startup scan

- Document protection

- Email client protection

- Web access protection

- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section enables you to define which computer components and files will be scanned for infiltrations.

Operating memory—Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI—Scans boot sectors for the presence of malware in the master boot record. Read more about UEFI in the glossary.

Email files—The program supports the following extensions: DBX (Outlook Express) and EML.

Archives—The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives—Self-extracting archives (SFX) are archives that can extract themselves.

Runtime packers—After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics—A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist or was not covered by the previous versions of the detection engine module. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA signatures—Advanced heuristics are a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of ESET NOD32 Antivirus while cleaning objects. There are 4 levels of cleaning:

ThreatSense has the following remediation (i.e. cleaning) levels.

Remediation in ESET NOD32 Antivirus

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.
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 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.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters for an On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS)—Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority—Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects—The Scan log will show all the scanned files in self-extracting archives, even those not infected (may generate a lot of scan log data and increase the scan log file size).

Enable Smart optimization—With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the specific

modules are applied when performing a scan.

Preserve last access timestamp—Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

▬ Limits

The Limits section enables you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size—Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: unlimited.

Maximum scan time for object (sec.)—Defines the maximum time value for the scan of files in a container object (such as a RAR/ZIP archive or an email with multiple attachments). This setting does not apply for standalone files. If a user-defined value has been 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 enables you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. The maximum value is **3 GB**.

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

Cleaning levels

To change cleaning level settings for a desired protection module, expand **ThreatSense** (for example, **Real-time file system protection**) and then choose a **Cleaning level** from the drop-down menu.

ThreatSense has the following remediation (i.e. cleaning) levels.

Remediation in ESET NOD32 Antivirus

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.
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 detection cannot be remediated, the reported object is left in its original location.
Remedy detection if safe, ask otherwise	Attempt to remediate the detection while cleaning objects. In some cases, if no action can be performed, the end-user receives an interactive alert and must select a remediation action (for example, delete or ignore). This setting is recommended in most cases.
Always ask the end-user	The end-user receives an interactive window while cleaning objects and must select a remediation action (for example, delete or ignore). This level is designed for more advanced users who know which steps to take in the event of a detection.

File extensions excluded from scanning

Excluded file extensions are a part of ThreatSense. To configure excluded file extensions, click **ThreatSense** in the Advanced setup for any module that uses ThreatSense technology.

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of ThreatSense setup lets you define the types of files to scan.

> **i** Not to be confused with Processes exclusions, HIPS exclusions or File/folder exclusions.

By default, all files are scanned. Any extension can be added to the list of files excluded from scanning.

Excluding files is sometimes necessary if scanning certain file types prevents the program that is using certain extensions from running properly. For example, it may be advisable to exclude the `.edb`, `.eml` and `.tmp` extensions when using Microsoft Exchange servers.

> ✓ To add a new extension to the list, click **Add**. Type the extension into the blank field (for example tmp) and click **OK**. When you select **Enter multiple values**, you can add multiple file extensions delimited by lines, commas or semicolons (for example, choose **Semicolon** from drop-down menu as a separator, and type `edb;eml;tmp`).
> You can use a special symbol ? (question mark). The question mark represents any symbol (for example `?db`).

> **i** To see the exact extension (if any) of a file in a Windows operating system you have to select the **File name extensions** check box in **Windows Explorer** > **View** (tab).

Additional ThreatSense parameters

To edit these settings open Advanced setup > **Protections** > **Real-time file system protection** > **Additional ThreatSense parameters**.

Additional ThreatSense parameters for newly created and modified files

The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. ESET NOD32 Antivirus uses advanced heuristics, which can detect new threats before the detection engine update is released in combination with signature-based scanning methods.

In addition to newly-created files, scanning is also performed on **Self-extracting archives** (.sfx) and **Runtime packers** (internally compressed executable files). By default, archives are scanned up to the 10th nesting level, and are checked regardless of their actual size. To modify archive scan settings, deselect **Default archive scan settings**.

Additional ThreatSense parameters for executed files

Advanced heuristics on file execution—By default, Advanced heuristics is used when files are executed. When enabled, we strongly recommend keeping Smart optimization and ESET LiveGrid® enabled to mitigate impact on system performance.

Advanced heuristics on executing files from removable media—Advanced heuristics emulates code in a virtual environment and evaluates its behavior before the code is allowed to run from removable media.

Tools

You can configure advanced settings for features that offer additional security and help simplify ESET NOD32 Antivirus administration in Advanced setup > **Tools**.

- Microsoft Windows® update

- ESET CMD

- Log files

- Gamer mode

- Diagnostics

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 NOD32 Antivirus notifies you about missing updates according to the level you specify in Advanced setup > **Tools**. 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.

Dialog window - System updates

If there are updates for your operating system, ESET NOD32 Antivirus displays a notification in the main program window > **Overview**. Click **More information** to open the System updates window.

The System updates window shows the available updates ready to be downloaded and installed. The update type is shown next to the name of the update.

Double-click any update row to display the Update information window with additional information.

Click **Run system update** to download and install all listed operating system updates.

Update information

The System updates window shows the list of available updates ready to be downloaded and installed. The update priority level is shown next to the name of the update.

Click **Run system update** to start downloading and installing operating system updates.

Right-click any update row and click **Show information** to display a new window with additional info.

ESET CMD

This is a feature that enables advanced ecmd commands. It enables 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 NOD32 Antivirus 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 the import of any unsigned configuration, which is a potential risk.

- **Advanced setup password**—A password is required to import a configuration from an .xml file, this file must be signed (see signing .xml configuration file further down). The password specified in Access Setup must be provided before a new configuration can be imported. If you do not have access setup enabled, your password does not match or the .xml configuration file is not signed, the configuration will not be imported.

When ESET CMD is enabled, you can use the command line to import or export ESET NOD32 Antivirus configurations. You can do it manually or create a script for the purpose of automation.

> To use advanced ecmd commands, you need to run them with administrator privileges, or open a Windows Command Prompt (cmd) using **Run as administrator**. Otherwise, you will get **Error executing command**. message. Also, when exporting a configuration, the destination folder must exist. The export command still works when the ESET CMD setting is switched off.

> ✓ Export settings command:
> `ecmd /getcfg c:\config\settings.xml`
>
> Import settings command:
> `ecmd /setcfg c:\config\settings.xml`

> **i** Advanced ecmd commands can only be run locally.

Signing an *.xml* configuration file:

1. Download the XmlSignTool executable.

2. Open a Windows Command Prompt (cmd) using **Run as administrator**.

3. Navigate to the save location of `xmlsigntool.exe`

4. Execute a command to sign the *.xml* configuration file, usage: `xmlsigntool /version 1|2 <xml_file_path>`

> ⚠ The value of the `/version` parameter depends on the version of your ESET NOD32 Antivirus. Use `/version 1` for earlier versions of ESET NOD32 Antivirus than 11.1. Use `/version 2` for the current version of ESET NOD32 Antivirus.

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 NOD32 Antivirus with ESET CMD using the password authorization method.

> ✓ Sign exported configuration file command:
> `xmlsigntool /version 2 c:\config\settings.xml`
>
>

> **i** If your Access Setup password changes and you want to import a configuration that was signed earlier with an old password, you need to sign the *.xml* configuration file again using your current password. This enables you to use an older configuration file without exporting it to another machine running ESET NOD32 Antivirus before the import.

> ⚠️ Enabling ESET CMD without an authorization is not recommended, since this will allow the import of any unsigned configuration. Set the password in <u>Advanced setup</u> > **User interface** > **Access setup** to prevent from unauthorized modification by users.

Log files

You can find the Logging configuration of ESET NOD32 Antivirus in <u>Advanced setup</u> > **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, etc...).

> ℹ️ 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—If checked, log files will be automatically be defragmented if the 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 during this process, which improves performance and log processing speed. This improvement can be observed especially if the logs contain a large number of entries.

Enable text protocol enables the storage of logs in another file format separate from <u>Log files</u>:

- **Target directory**—The directory where log files will be stored (only applies to Text/CSV). Each log section has its own file with a pre-defined file name (for example, virlog.txt for the **Detections** 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 log files**—Erases all stored logs currently selected in the **Type** drop-down menu. A notification about successful deletion of the logs will be shown.

> ℹ️ 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 <u>ESET Knowledgebase</u> article.

Gamer mode

Gamer mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by notification/alert windows, and want to minimize CPU usage. Gamer mode can also be used during presentations that cannot be interrupted by antivirus activity. By enabling this feature, all pop-up windows are disabled and the activity of the scheduler will be stopped completely. System protection still runs in the background but does not demand any user interaction.

You can enable or disable Gamer mode in the main program window under **Setup** > **Computer protection** by clicking or next to **Gamer mode**. Enabling Gamer 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 **Gamer mode active** in orange.

Activate **Enable Gamer mode when running applications in full-screen mode automatically** in Advanced setup > **Tools** > **Gamer mode** to have Gamer mode start whenever you initiate a full-screen application and stop after you exit the application.

Activate **Disable Gamer mode automatically after** to define the amount of time after which Gamer mode will automatically be disabled.

Diagnostics

Diagnostics provides application crash dumps of ESET processes (for example, ekrn). If an application crashes, a dump will be generated. This can help developers debug and fix various ESET NOD32 Antivirus 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 advanced logging in marketing messages—Record all events related to marketing messages within the product.

Enable Computer Scanner advanced logging—Record all events that occur while scanning files and folders by a computer scan.

Enable Device control advanced logging—Record all events that occur in Device control. This can help developers diagnose and fix problems related to device control.

Enable Direct Cloud advanced logging—Record all events that occur in ESET LiveGrid®. This can help developers diagnose and fix problems related to ESET LiveGrid®.

Enable Document protection advanced logging—Record all events in Document protection to allow diagnosing and solving problems.

Enable Email client protection advanced logging—Record all events that occur in Email client protection and email client plug-in to allow diagnosing and solving problems.

Enable Kernel advanced logging—Record all events that occur in the ESET kernel (ekrn).

Enable Licensing advanced logging—Record all product communication with ESET activation or ESET License Manager servers.

Enable Memory tracing—Record all events that help developers diagnose memory leaks.

Enable Network traffic scanner advanced logging—Record all data passing through the Network traffic scanner in the PCAP format to help the developers diagnose and fix problems related to Network traffic scanner.

Enable Operating System advanced logging—Record additional information about the operating system, such as running processes, CPU activity, and disc operations. This can help developers diagnose and fix problems related to the ESET product running on your operating system.

Enable push messaging advanced logging—Record all events that occur during push messaging.

Enable Real-time file system protection advanced logging—Record all events that occur while scanning files and folders by Real-time file system protection.

Enable Update engine advanced logging—Record all events that occur during the update process. This can help developers diagnose and fix problems related to the Update engine.

Log files are located in *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Technical support

When contacting ESET Technical Support from the ESET NOD32 Antivirus, you can submit system configuration data. Select **Always submit** from the **Submit system configuration data** drop-down menu to submit the data automatically, or select **Ask before submission** to be prompted before submitting data.

Connectivity

In specific networks, a proxy server can mediate communication between your computer and the internet. If you are using a proxy server, you need to define the following settings. Otherwise, ESET NOD32 Antivirus and its modules cannot update automatically. In ESET NOD32 Antivirus, proxy server setup is available in two different sections of Advanced setup.

Global proxy server settings can be configured in Advanced setup > **Connectivity** > **Proxy server**. Specifying the

proxy server at this level defines global proxy server settings for all of ESET NOD32 Antivirus. Parameters here will be used by all modules that require a connection to the internet.

To specify global proxy server settings, enable **Use proxy server** and type the **Proxy server** address together with the proxy server's **Port** number.

If communication with the proxy server requires authentication, select **Proxy server requires authentication** and type a valid **Username** and **Password** into the corresponding fields. Click **Detect proxy server** to detect and populate proxy server settings automatically. ESET NOD32 Antivirus will copy the parameters specified in internet options for Internet Explorer or Google Chrome.

> **i** You must manually type your Username and Password in the **Proxy server** settings.

Use direct connection if proxy is not available—If ESET NOD32 Antivirus is configured to connect via proxy and the proxy is unreachable, ESET NOD32 Antivirus will bypass the proxy and communicate directly with ESET servers.

Proxy server settings can also be configured in Advanced setup > **Update** > **Profiles** > **Updates** > **Connection options** by selecting **Connection through a proxy server** from the **Proxy mode** drop-down menu. This configuration applies only for updates and is recommended for laptops receiving module updates from remote locations. For more information, refer to Advanced update setup.
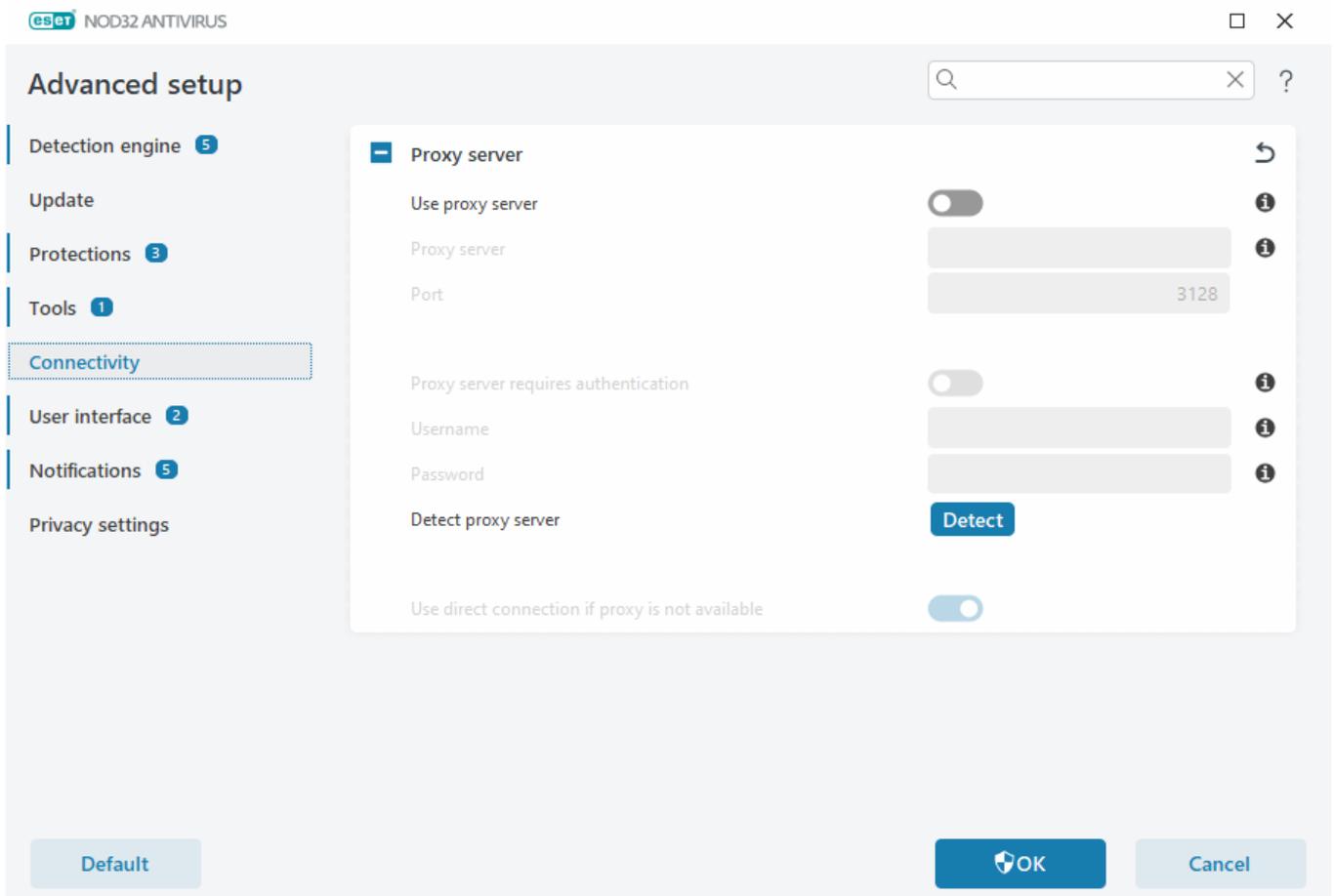
User interface

To configure the program's graphical user interface (GUI) behavior, open Advanced setup > **User interface**.

You can adjust the program's visual appearance and effects in the User interface elements Advanced setup screen.

To provide maximum security of your security software, you can prevent uninstallation or any unauthorized changes by protecting the settings by a password using the Access setup tool.

> **i** To configure the behavior of system notifications, detection alerts and application statuses, see the Notifications section.

User interface elements

You can adjust the ESET NOD32 Antivirus working environment (GUI) to fit your needs in Advanced setup > **User interface** > **User interface elements**.

Color mode—Select the color scheme of the ESET NOD32 Antivirus GUI from the drop-down menu:

- **Same as the system color**—Sets the color scheme of ESET NOD32 Antivirus based on your operating system settings.

- **Dark**—ESET NOD32 Antivirus will have a dark color scheme (dark mode).

- **Light**—ESET NOD32 Antivirus will have a standard, light color scheme.

> **i** You can also select the color scheme of ESET NOD32 Antivirus GUI in the top right corner of the main program window.

Show splash-screen at startup—Displays the ESET NOD32 Antivirus splash-screen during startup.

Use sound signal—Plays a sound when important events occur during a scan, for example, when a threat is discovered or when the scan has finished.

Transparent background—Enables a transparent background effect for the main program window. Transparent background is available only for the latest Windows versions (RS4 and later).

Integrate into the context menu—Integrates the ESET NOD32 Antivirus control elements into the context menu.
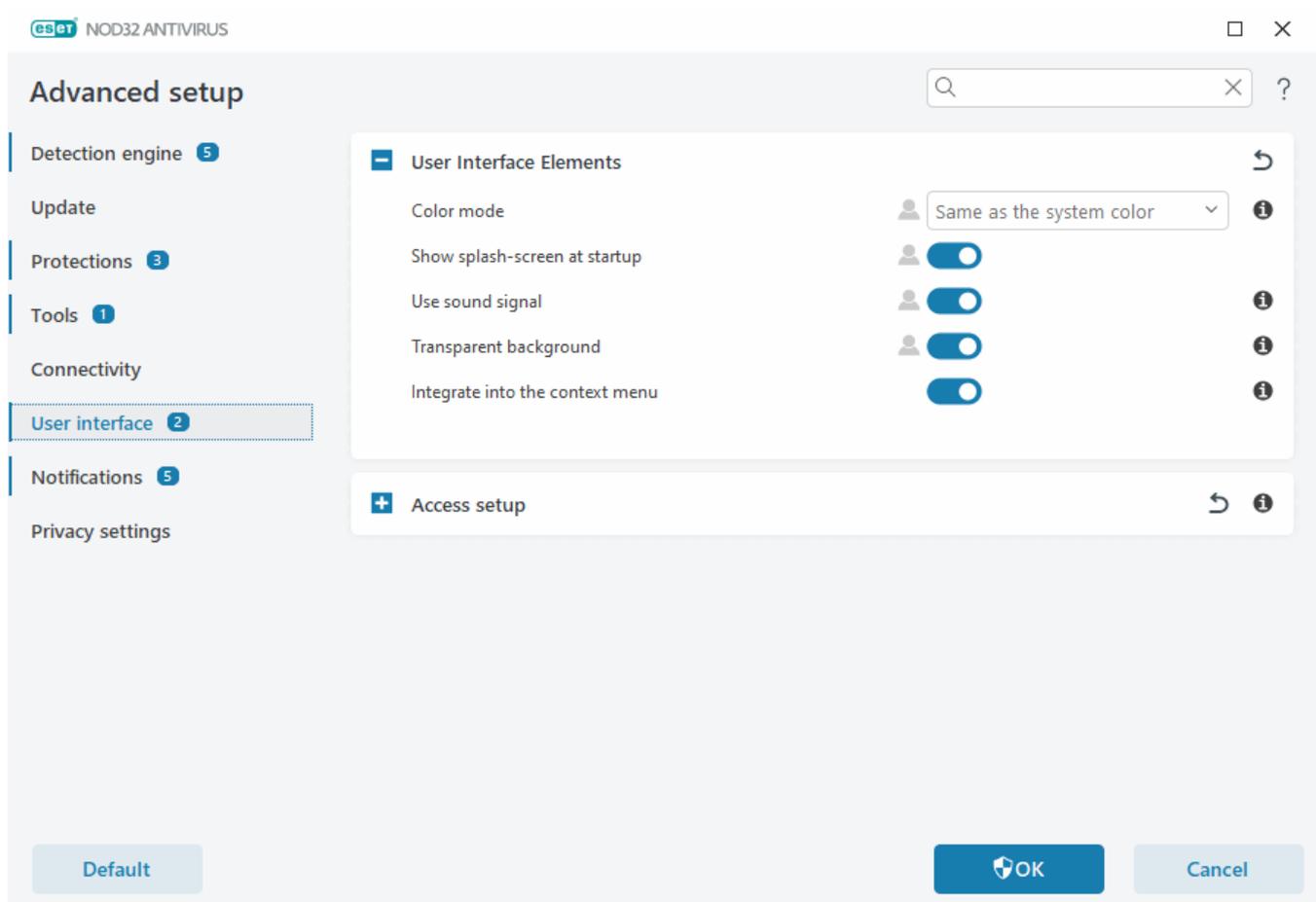
Access setup

ESET NOD32 Antivirus settings are a crucial part of your security policy. Unauthorized modifications can potentially endanger the stability and protection of your system. To avoid unauthorized modifications, the setup parameters and uninstallation of ESET NOD32 Antivirus can be password protected. Access setup can be configured in Advanced setup > **User interface** > **Access setup**.

To set a password to protect setup parameters and uninstallation of ESET NOD32 Antivirus, click **Set** next to **Password protect settings**.

> ℹ️ When you want to access protected Advanced setup, the window for entering the password is displayed. If you forget or lose your password, click the **Restore password** option below and type the email address you used for license registration. ESET will send you an email with the verification code and instruction on how to reset your password.
> - How to unlock Advanced setup

To change your password, click **Change password** next to **Password protect settings**.

To remove your password, click **Remove** next to **Password protect settings**.
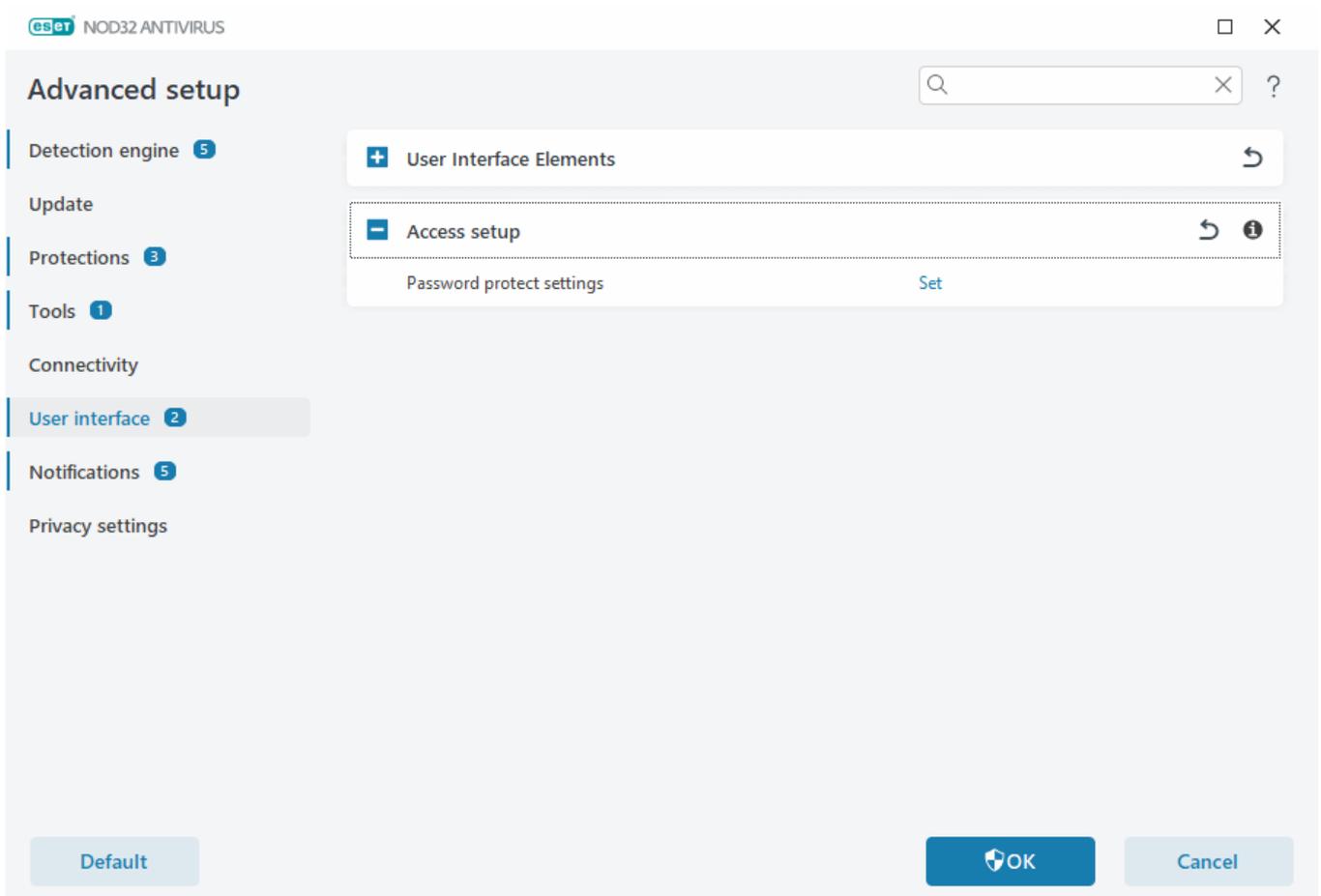
Password for Advanced setup

To protect the ESET NOD32 Antivirus Advanced setup and to avoid unauthorized modification, type your new password in the **New password** and **Confirm password** fields. Click **OK**.

When you want to change an existing password:

1. Type your old password in the **Old password** field.

2. Type your new password in the **New password** and **Confirm password** fields.

3. Click **OK**.

This password will be required for access to Advanced setup.

If you forget your password, see Unlock your settings password in ESET home products.

To recover your lost ESET license key, the expiration date of your license, or other license information for ESET NOD32 Antivirus, see I lost my License Key.

Screen reader support

ESET NOD32 Antivirus can be used together with screen readers to enable ESET users with impaired vision to navigate in the product or to configure the settings. The following screen readers are supported (JAWS, NVDA, Narrator).

To make sure the screen reader software can access ESET NOD32 Antivirus GUI correctly, follow the instructions in our Knowledgebase article.

Notifications

To manage ESET NOD32 Antivirus notifications, open Advanced setup > **Notifications**. You can configure the following types of notifications:

- Application statuses—Notifications displayed in the main program window > **Overview**.

- Desktop notifications—Small notification windows next to the system taskbar.

- Interactive alerts—Alert windows and message boxes that require user interaction.

- Forwarding (email notifications)—Notifications are sent to a specified email address.
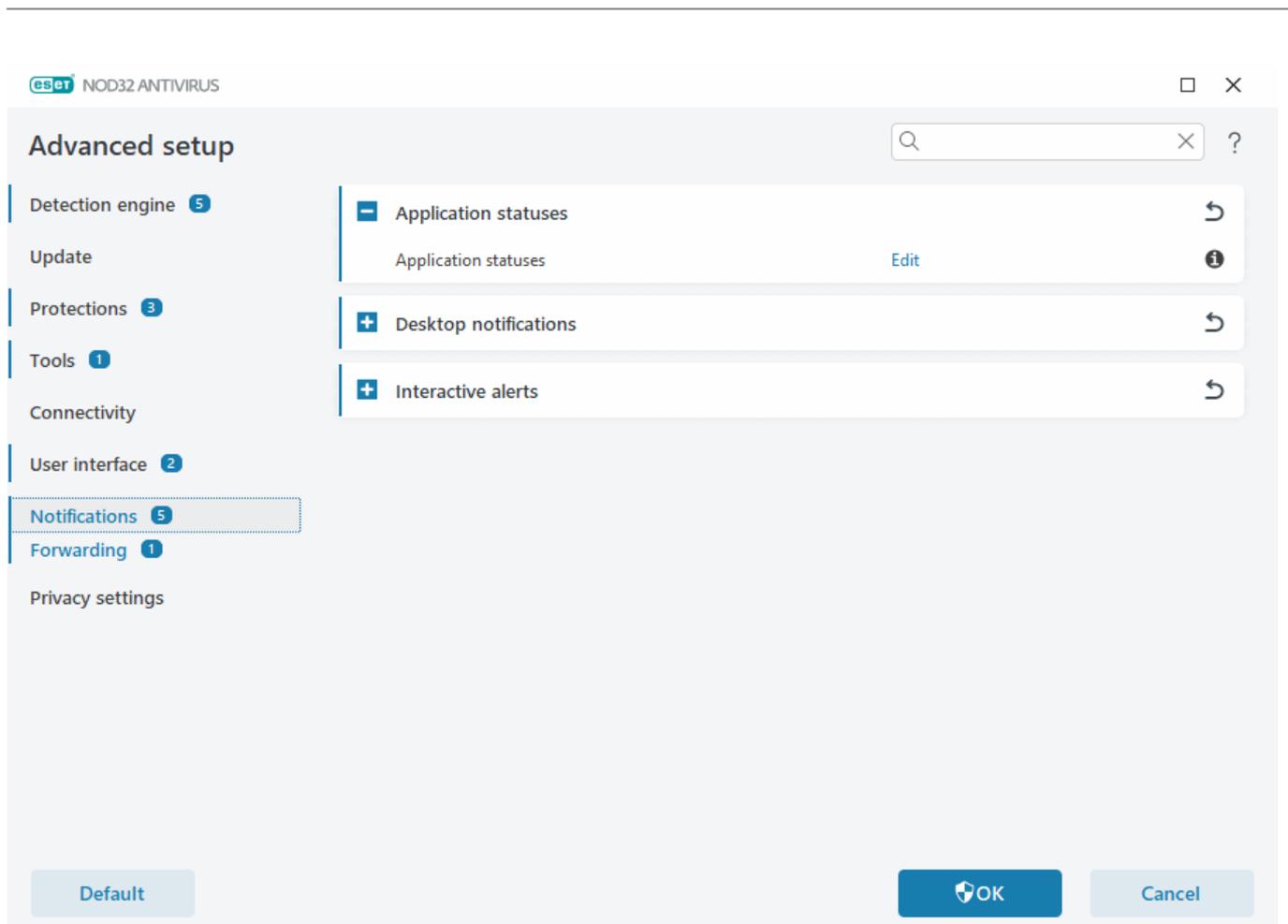
⊟ Application statuses

Application statuses—Click **Edit** to select which application statuses will be displayed in the main program window > **Overview**.

Dialog window - Application statuses

In this dialog window, you can select which application statuses will be displayed. For example, when you pause Antivirus and antispyware protection or enable Gamer mode.

Application status will also be displayed if your product is not activated or your license has expired.

Desktop notifications

Desktop notifications are represented by a small notification window next to the system taskbar. By default, it shows for 10 seconds, then it slowly disappears. Notifications include successful product updates, new devices connected, virus scans tasks completion, or new threats found.
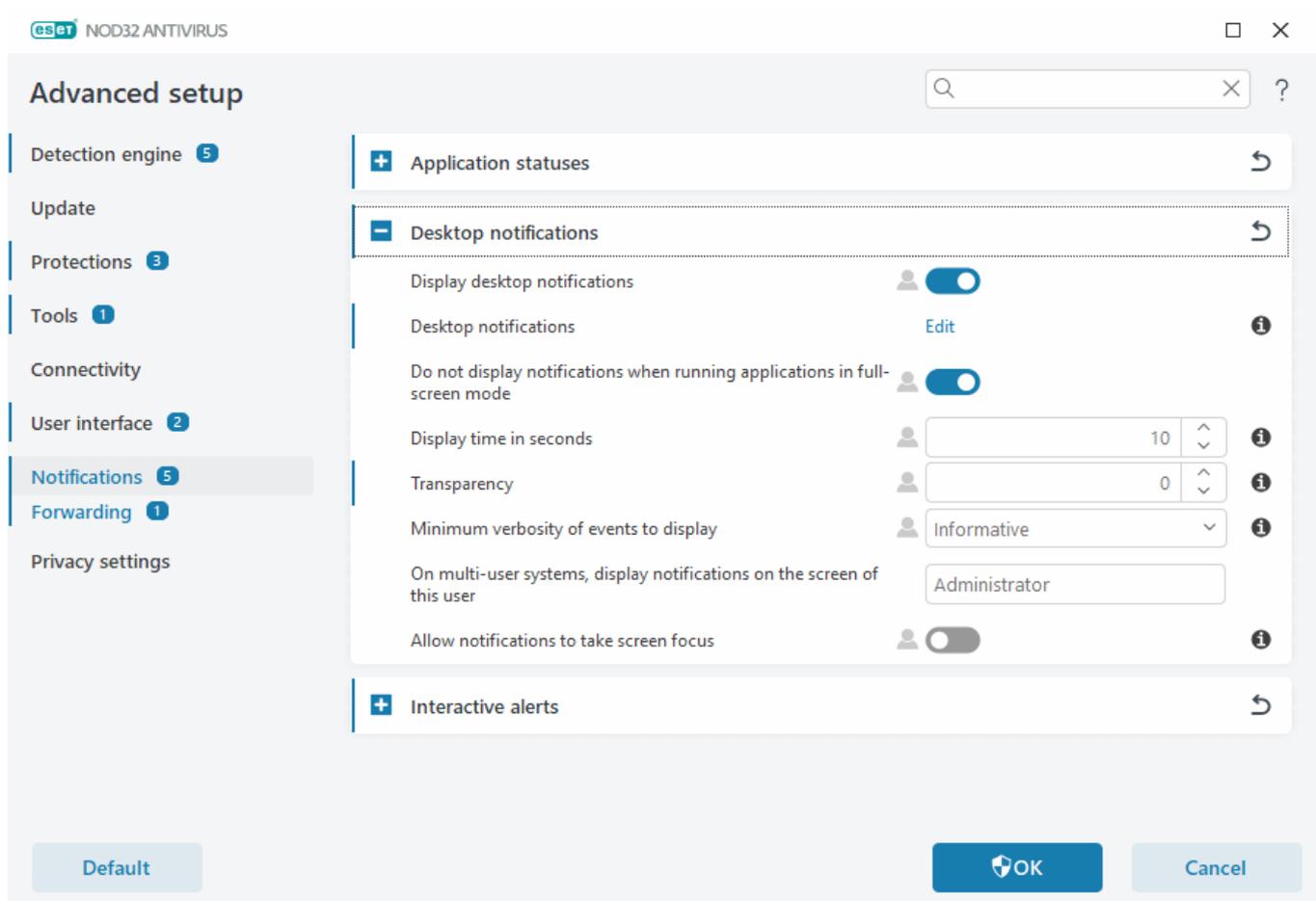
Display desktop notifications—We recommend keeping this option enabled so the product can inform you when a new event occurs.

Desktop notifications—Click **Edit** to enable or disable specific Desktop notifications.

Do not display notifications when running applications in full-screen mode—Suppress all non-interactive notifications when running applications in full screen mode.

Timeout in seconds—Set the notification visibility duration. The value must be between 3-30 seconds.

Transparency—Set the notification transparency percentage. The supported range is 0 (no transparency) to 80 (very high transparency).

Minimum verbosity of events to display—Set the starting notification severity level displayed. From the drop-down menu, select one of the following options:

o**Diagnostic**—Displays information needed to fine-tune the program and all records above.

o**Informative**—Displays informative messages such as non-standard network events, including successful update messages, plus all records above.

o**Warnings**—Displays warning messages, errors and critical errors (for example, update failed).

o**Errors**—Displays errors (for example, document protection not started) and critical errors.

o**Critical**—Displays only critical errors (for example, error starting antivirus protection or infected system).

On multi-user systems, display notifications on the screen of this user—Enables selected account to receive desktop notifications. For example, if you do not use the Administrator account, type the full account name and the desktop notifications will be displayed for the specified account. Only one user account can receive the desktop notifications.

Allow notifications to take screen focus—Allows notifications to take screen focus and are accessible in the **ALT + Tab** menu.

Desktop notifications list

To adjust the visibility of desktop notifications (displayed at the bottom right of the screen), open Advanced setup > **Notifications** > **Desktop notifications**. Click **Edit** next to **Desktop notifications** and select the appropriate **Show** check box.
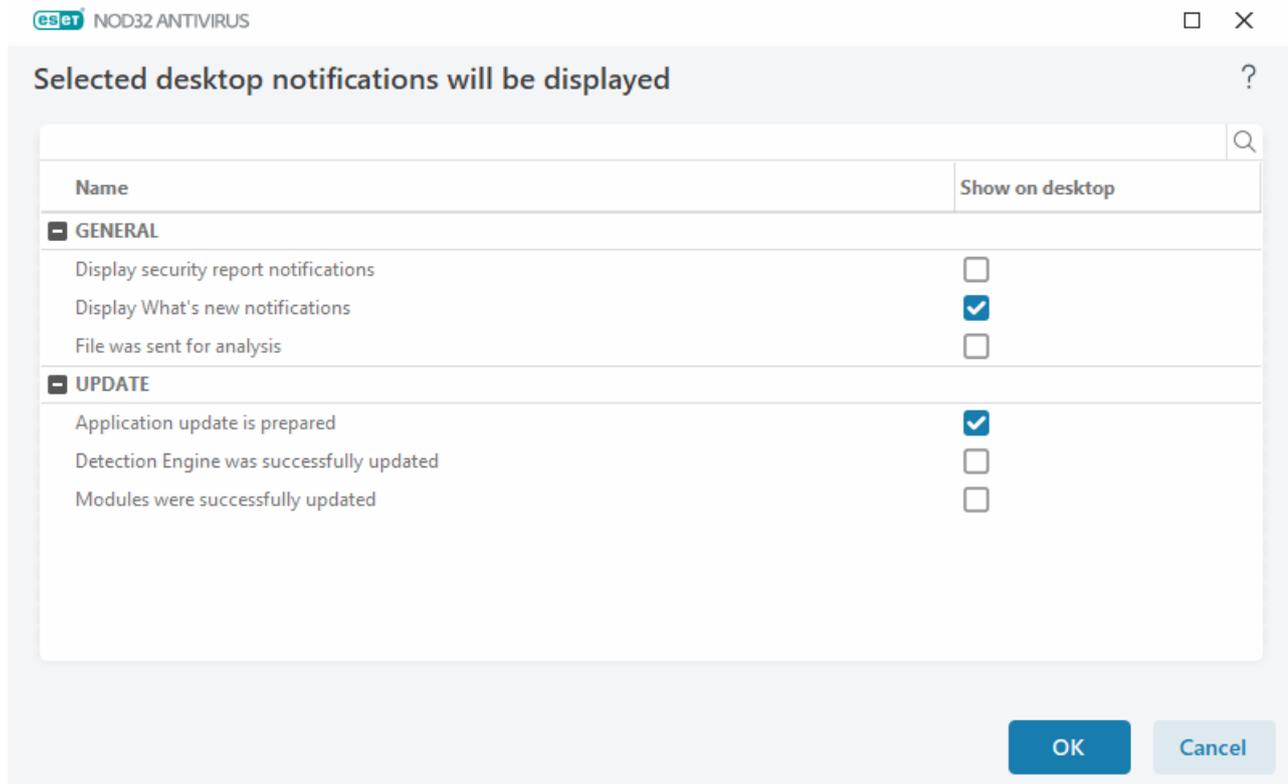
General

Display Security report notifications—Receive a notification when a new [Security report](#) is generated.

Display What's new notifications—Notifications about all new and enhanced features of the latest product version.

File was sent for analysis—Receive a notification every time the ESET NOD32 Antivirus sends a file for analysis.

Network Protection

Wifi protection warnings—Receive a notification when you attempt to connect to a Wi-Fi network with a weak or no password.

Update

Application update is prepared—Receive a notification when there is an update to a new version of the ESET NOD32 Antivirus prepared.

Detection Engine was successfully updated—Receive a notification when the product updates Detection Engine modules.

Modules were successfully updated—Receive a notification when the product updates program components.

To set general Desktop notifications settings (for example, how long a message displays or the minimum verbosity of events to display), see [Desktop notifications](#) in [Advanced setup](#) > **Notifications**.

Interactive alerts

> **Looking for information about common alerts and notifications?**
> - [Threat found](#)
> - [Address has been blocked](#)
> - [Product not activated](#)
> - [Change to a product with more features](#)
> - [Change to a product with less features](#)
> - [Update is available](#)
> - [Update information is not consistent](#)
> - [Troubleshooting for "Modules update failed" message](#)
> - [Resolve modules update errors](#)
> - [Website certificate revoked](#)

The **Interactive alerts** section in [Advanced setup](#) > **Notifications** enables you to configure how message boxes and interactive alerts for detections, where a decision is needed to be made by a user (for example, potential phishing website) are handled by ESET NOD32 Antivirus.
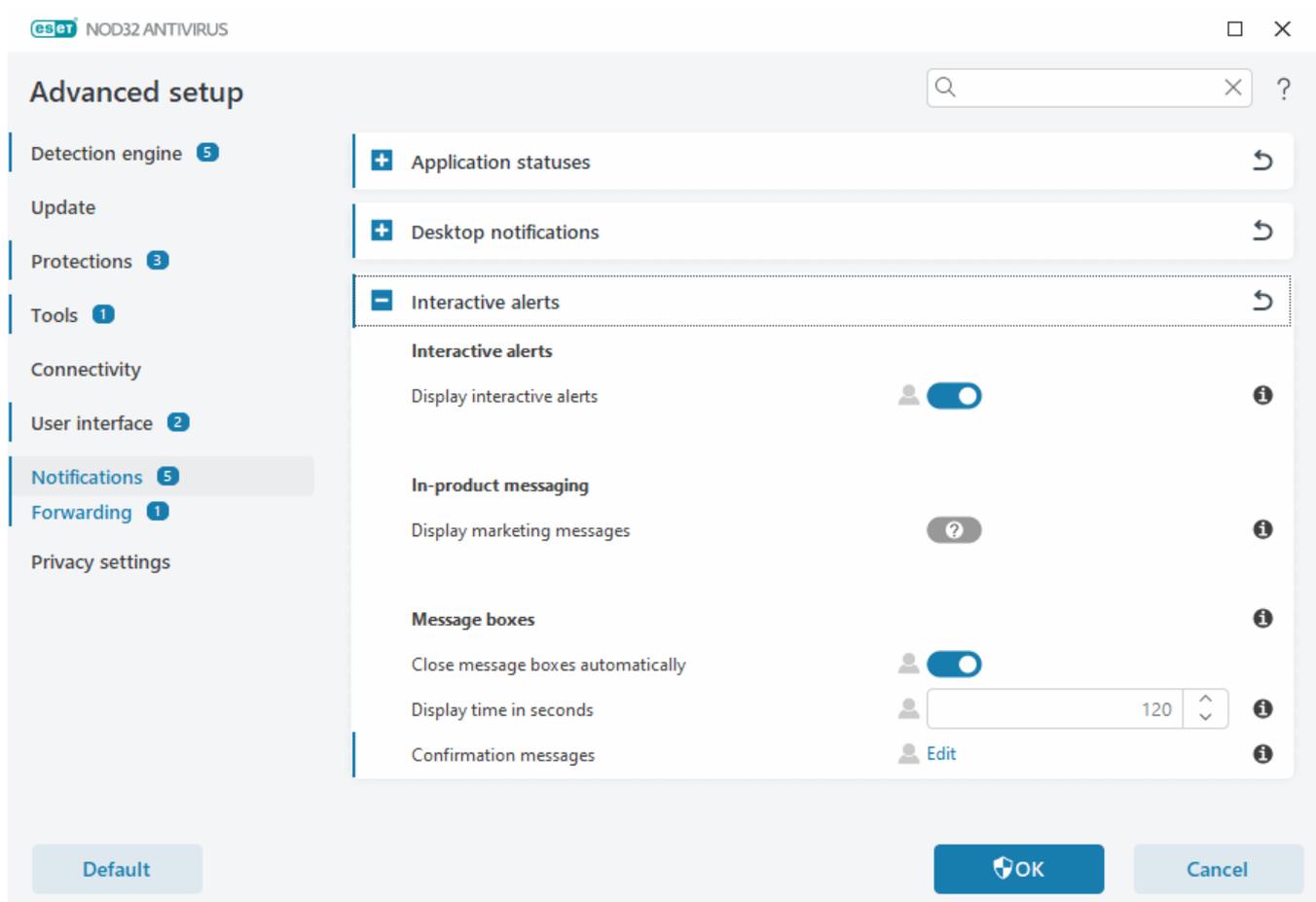
Interactive alerts

Disabling **Display interactive alerts** will hide all alert windows and in-browser dialogs and is only suitable for a limited amount of specific situations. We recommend keeping this option enabled.

In-product messaging

In-product messaging is designed to inform users of ESET news and other communications. Sending marketing messages requires the consent of a user. Marketing messages are not sent to a user by default (shown as a question mark). By enabling this option, you agree to receive ESET marketing messages. If you are not interested in receiving ESET marketing material, disable the **Display marketing messages** option.

Message boxes

To close the message boxes automatically after a certain time, select **Close message boxes automatically**. If they are not closed manually, alert windows are automatically closed after the specified time elapses.

Timeout in seconds—Sets the alert visibility duration. The value must be between 10-999 seconds.

Confirmation messages—Click **Edit** to show a list of confirmation messages you can select to display or not to display.

Confirmation messages

To adjust confirmation messages, open Advanced setup > **Notifications** > **Interactive alerts** and click **Edit** next to **Confirmation messages**.
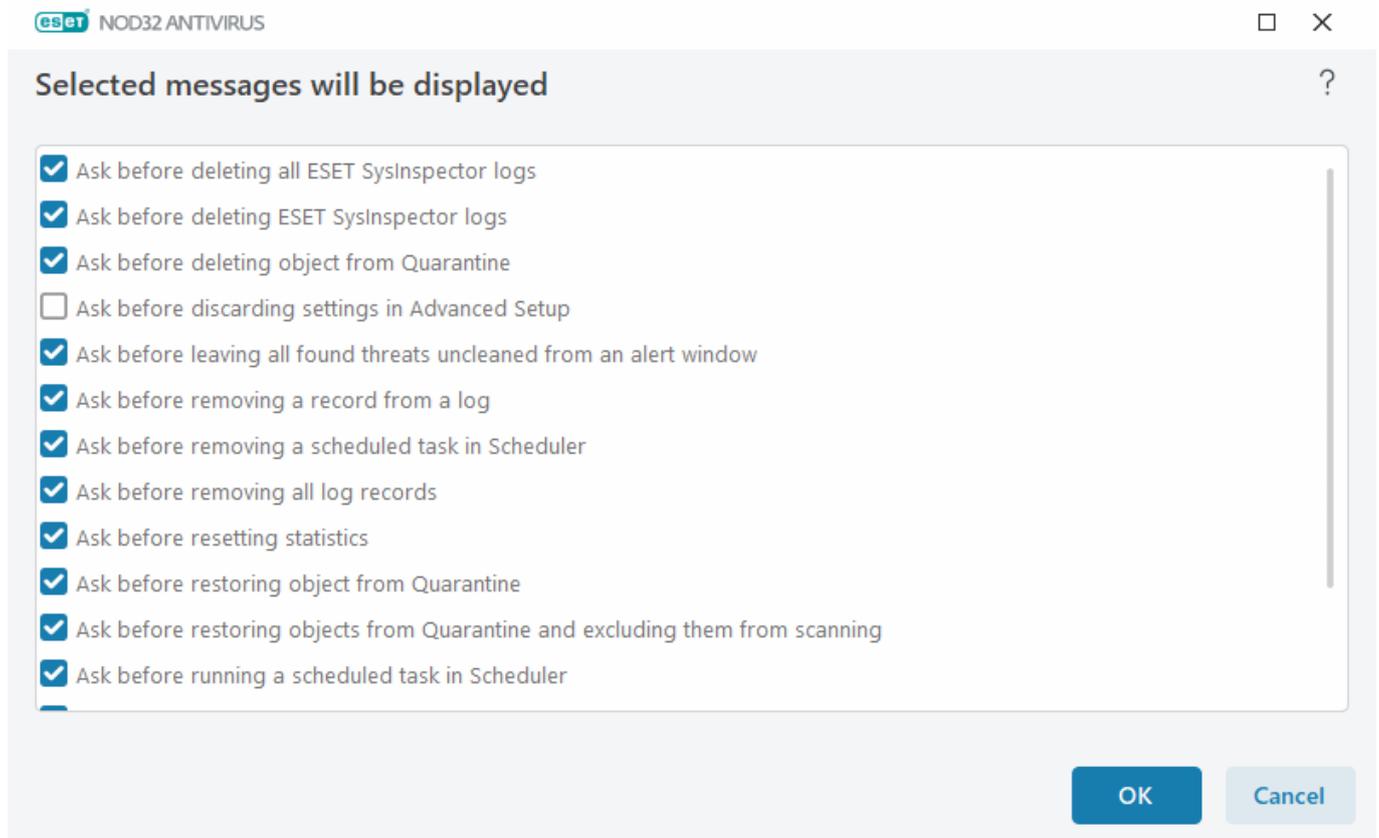
This dialog window displays confirmation messages that ESET NOD32 Antivirus will display before any performed action. Select or deselect the check box next to each confirmation message to allow or disable it.

Learn more about specific feature related to confirmation messages:

- Ask before deleting ESET SysInspector logs

- Ask before deleting all ESET SysInspector logs

- Ask before deleting object from Quarantine

- Ask before discarding settings in Advanced Setup

- Ask before leaving all found threats uncleaned from an alert window

- Ask before removing a record from a log

- Ask before removing a scheduled task in Scheduler

- Ask before removing all log records

- Ask before resetting statistics

- Ask before restoring object from Quarantine

- [Ask before restoring objects from Quarantine and excluding them from scanning](#)

- [Ask before running a scheduled task in Scheduler](#)

- [Show product confirmation dialogs for Outlook Express and Windows Mail email clients](#)

- [Show product confirmation dialogs for Windows Live Mail](#)

- [Show product confirmation dialogs for the Outlook email client](#)

Forwarding

ESET NOD32 Antivirus can automatically send notification emails if an event with the selected verbosity level occurs. Open [Advanced setup](#) > **Notifications** > **Forwarding** and enable **Forward notifications to email** to activate email notifications.
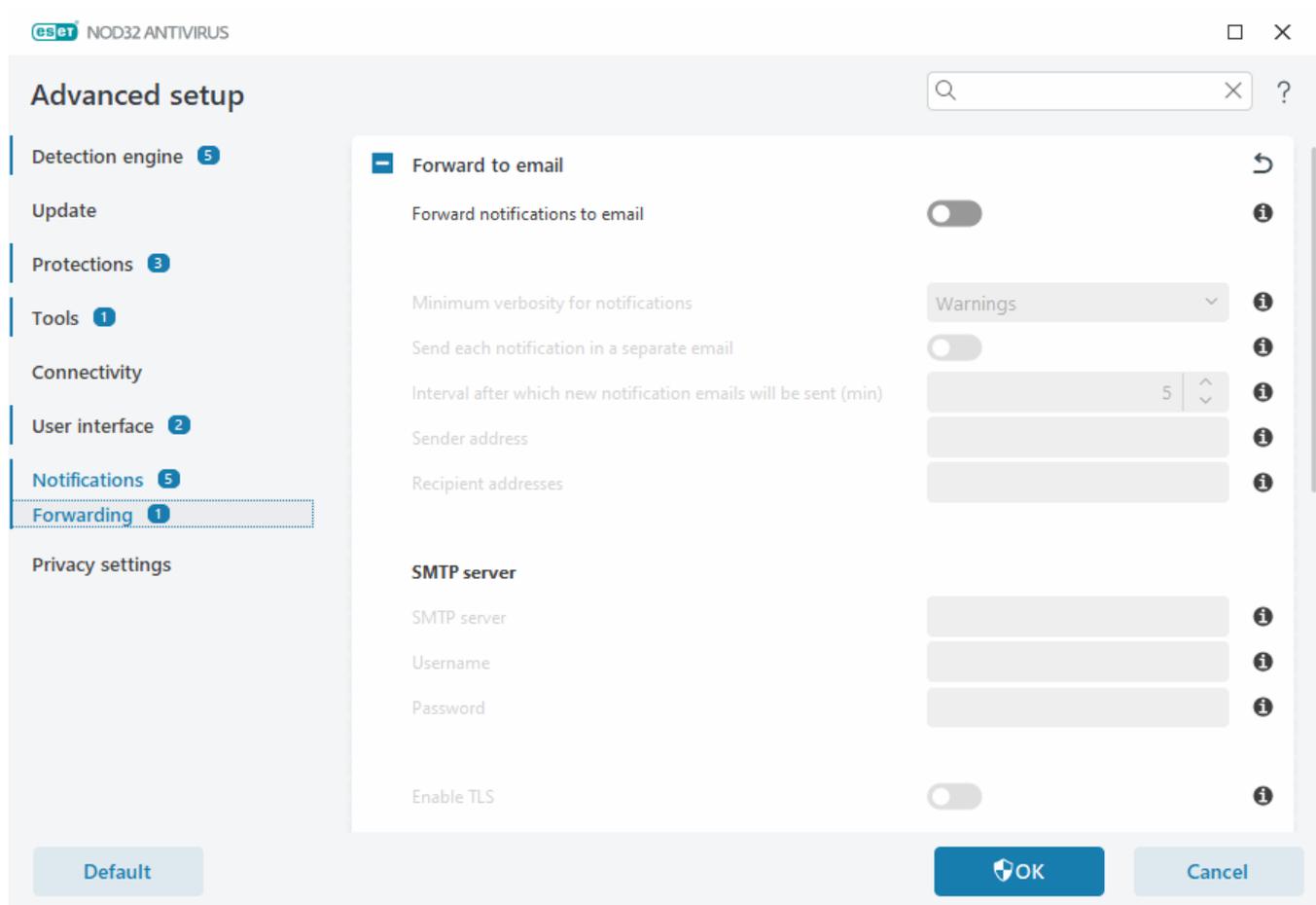
From the **Minimum verbosity for notifications** drop-down menu, you can select the starting severity level of notifications to be sent.

- **Diagnostic**—Logs information needed to fine-tune the program and all records above.

- **Informative**—Records informative messages such as non-standard network events, including successful update messages, plus all records above.

- **Warnings**—Records critical errors and warning messages (for example, update failed).

- **Errors**—Errors (for example, Document protection not started) and critical errors will be recorded.

- **Critical**—Logs only critical errors (for example, Error starting antivirus protection, or Threat found).

Send each notification in a separate email—When enabled, the recipient will receive a new email for each notification. This may result in many emails received in a short period.

Interval after which new notification emails will be sent (min)—Interval in minutes after which new notifications will be sent to email. If you set this value to 0, the notifications will be sent immediately.

Sender address—Define the sender address displayed in the header of notification emails.

Recipient addresses—Define the recipient addresses displayed in the header of notification emails. Multiple values are supported. Use semi-colon as the separator.

SMTP server

SMTP server—The SMTP server used for sending notifications (for example, smtp.provider.com:587, pre-defined port is 25).

> **i** SMTP servers with TLS encryption are supported by ESET NOD32 Antivirus.

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.

Enable TLS—Secure Alert and notifications using TLS encryption.

Test SMTP connection—A test email will be sent to the recipient's email address. SMTP server, Username, Password, Sender address, and Recipient addresses need to be filled in.

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 **Use default message format** for 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 displayed on remote computers.

Format of threat warning messages—Threat alert and notification messages have a pre-defined default format. We recommend keeping the pre-defined format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format.

Charset—Converts an email message to the ANSI character encoding based on Windows Regional settings (for example, windows-1250, Unicode (UTF-8), ACSII 7-bit, or Japanese (ISO-2022-JP)). As a 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).

- **%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 the 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.

Privacy settings

Open Advanced setup > **Privacy settings**.
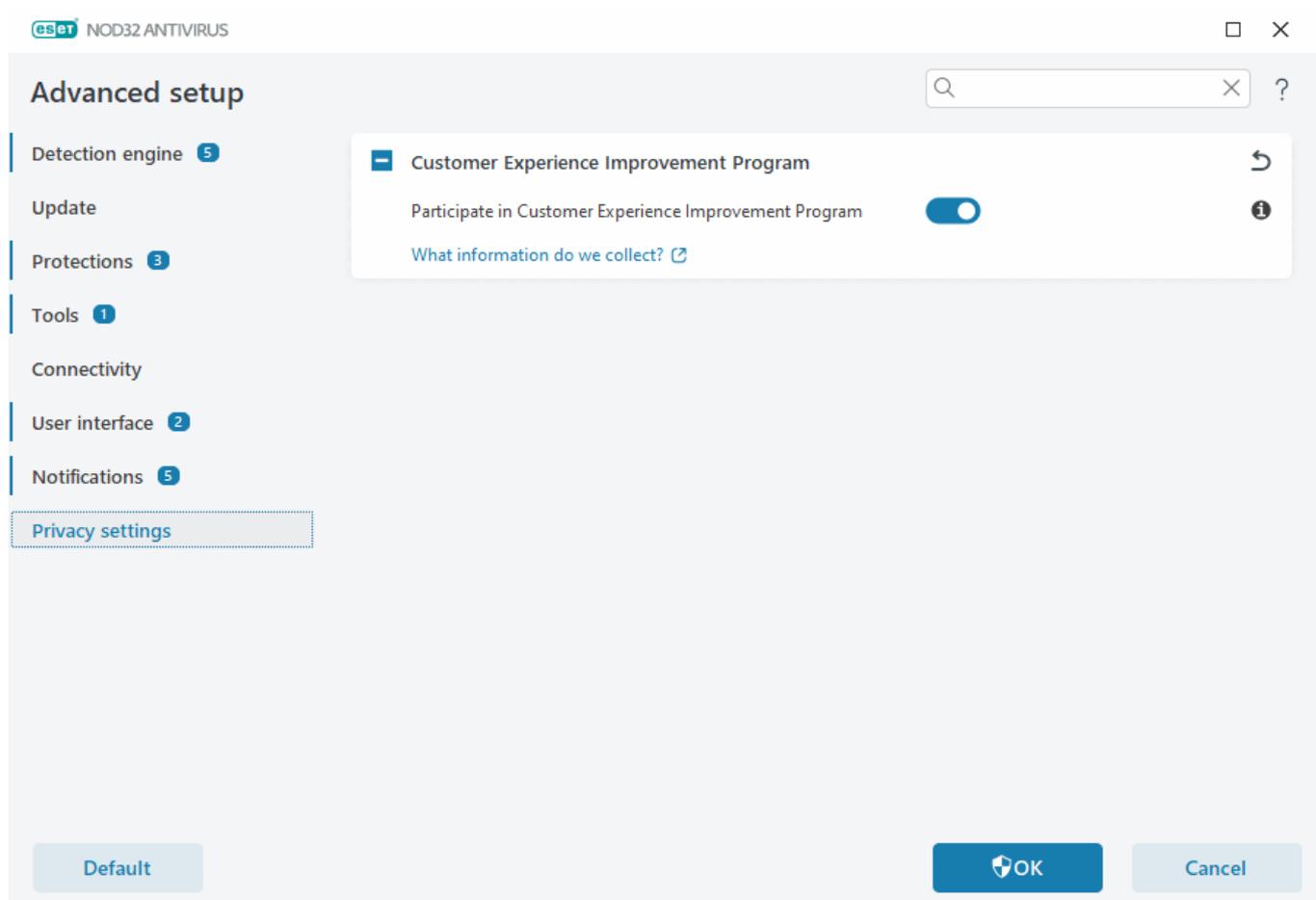
Customer Experience Improvement Program

Enable the toggle next to **Participate in the Customer Experience Improvement Program** to join the Customer Experience Improvement Program. By joining, you provide ESET with anonymous information relating to the use

of ESET products. The collected data will help us improve your experience will never be shared with third parties.
[What information do we collect?](#)

Revert to default settings

Click **Default** in [Advanced setup](#) to revert all program settings, for all modules. This will be reset to the status they would have had after a new installation.

See also [Import and export settings](#).

Revert all settings in current section

Click the curving arrow ⟳ to revert all settings in the current section to the default settings defined by ESET.

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.

Command line scanner

ESET NOD32 Antivirus'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

> **i**   Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

Common Questions

You can find some of the most frequently asked questions and problems encountered below. Click the topic title to find out how to solve your problem:

- How to update ESET NOD32 Antivirus

- ESET NOD32 Antivirus has detected a threat

- How to remove a virus from my PC

- How to create a new task in Scheduler

- How to schedule a scan task (weekly)

- How to unlock Advanced setup

- How to resolve product deactivation from ESET HOME

If your problem is not included in the list above, try searching the ESET NOD32 Antivirus Online Help.

If you cannot find a solution to your problem/question in the ESET NOD32 Antivirus Online Help, you can visit our regularly updated online ESET Knowledgebase. Links to our most popular Knowledgebase articles are included below:

- How to renew my license?

- I received an activation error while installing my ESET product. What does it mean?

- Activate my ESET Windows home product using the license Key

- Uninstall or reinstall my ESET home product

- I received the message that my ESET installation ended prematurely

- What do I need to do after renewing my license? (Home users)

- What if I change my email address?

- Transfer my ESET product to a new computer or device

- How to start Windows in Safe Mode or Safe Mode with networking

- Exclude a safe website from being blocked

- Allow access for screen readers software to ESET GUI

If necessary, you can contact our Technical Support with your questions or problems.

How to update the ESET NOD32 Antivirus

Updating ESET NOD32 Antivirus 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. If you need to change the interval, navigate to **Tools** > Scheduler.

How to remove a virus from my PC

If your computer is showing symptoms of malware infection, for example, is slower or often freezes, we recommend that you do the following:

1. In the main program window, click **Computer scan**.

2. Click **Scan your computer** 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 scan only a selected part of your disk, click **Custom scan** and select targets to be scanned for viruses.

For additional information, see our regularly updated ESET Knowledgebase article.

How to 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 the modules.

Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task below:

From the **Scheduled task** drop-down menu, select **Update**. Type the name of the task into the **Task name** field and click **Next**. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered**. Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. Next, define the action to take if the task cannot be performed or completed at the scheduled time. The following options are available:

- **At the next scheduled time**

- **As soon as possible**

- **Immediately, if time since last run exceeds a specified value** (the interval can be defined using the **Time since last run (hours)** scroll box)

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

A dialog window will appear, enabling you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of currently scheduled tasks.

How to schedule a weekly computer scan

To schedule a regular task, open the [main program window](#) 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. Type a name for the task and select **On-demand computer scan** from the **Task type** drop-down menu.

3. Select **Weekly** as 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 unlock password protected Advanced setup

When you want to access the protected Advanced setup, the window for entering the password is displayed. If you forget or lose your password, click **Restore password** and type the email address you used for license registration. ESET sends an email with the verification code. Type the verification code and then write and confirm the new password. The verification code is valid for seven days.

Restore password via your ESET HOME account—Use this option if the license used for activation is associated with your ESET HOME account. Type the email address you use to log in to your ESET HOME account.

If you cannot remember your email address or have difficulties restoring the password, click **Contact Technical Support**. You are redirected to the ESET website to contact our Technical Support department.

Generate code for Technical Support—This option generates a code for Technical Support. Copy the code provided by Technical Support and click **I have a verification code**. Type the verification code and then write and confirm the new password. The verification code is valid for seven days.

For more information, see Unlock your settings password in ESET Windows home products.

How to resolve product deactivation from ESET HOME

Product not activated

This error message appears when the license owner deactivates your ESET NOD32 Antivirus from ESET HOME portal or the license shared with your ESET HOME account is no longer shared. To resolve this issue:

- Click **Activate** and use one of the Activation methods to activate ESET NOD32 Antivirus.

- Contact the license owner with information that your ESET NOD32 Antivirus has been deactivated by the license owner or the license is no longer shared with you. The owner can solve the problem in the ESET HOME.

Product deactivated, device disconnected

This error message appears after removing a device from the ESET HOME account. To resolve this issue:

- Click **Activate** and use one of the Activation methods to activate ESET NOD32 Antivirus.

- Contact the license owner with information that your ESET NOD32 Antivirus has been deactivated and the device has been disconnected from ESET HOME.

- If you are the license owner and unaware of these changes, review your ESET HOME Activity feed. If you find any suspicious activity, change your ESET HOME account password and contact ESET Technical Support.

Product deactivated, device disconnected

This error message appears after removing a device from the ESET HOME account. To resolve this issue:

- Click **Activate** and use one of the [Activation methods](#) to activate ESET NOD32 Antivirus.

- Contact the license owner with information that your ESET NOD32 Antivirus has been deactivated and the device has been disconnected from ESET HOME.

- If you are the license owner and unaware of these changes, review your [ESET HOME Activity feed](#). If you find any suspicious activity, [change your ESET HOME account password](#) and [contact ESET Technical Support](#).

Product not activated

This error message appears when the license owner deactivates your ESET NOD32 Antivirus from ESET HOME portal or the license shared with your ESET HOME account is no longer shared. To resolve this issue:

- Click **Activate** and use one of the [Activation methods](#) to activate ESET NOD32 Antivirus.

- Contact the license owner with information that your ESET NOD32 Antivirus has been deactivated by the license owner or the license is no longer shared with you. The owner can solve the problem in the [ESET HOME](#).

Customer Experience Improvement Program

By joining the Customer Experience Improvement Program you provide ESET with anonymous information relating to the use of our products. More information on data processing is available in our Privacy Policy.

Your consent

Participation in the Program is voluntary and based on your consent. After joining in, the participation is passive, which means you don't need to take any further action. You may revoke your consent by changing the product settings at any time. Doing so will bar us from further processing of your anonymous data.

You may revoke your consent by changing the product settings at any time:

- [Change the Customer Experience Improvement Program settings in ESET Windows home products](#)

What types of information do we collect?

Data about interaction with the product

This information tells us more about how our products are used. Thanks to this we know, for example, which functionalities are used often, what settings users modify or how much time they spend using the product.

Data about devices

We collect this information to understand where and what devices our products are used on. Typical examples are device model, country, version and name of the operating system.

Error diagnostics data

Information about error and crash situations is also collected. For example, what error has occurred and which

actions led to it.

Why do we collect this information?

This anonymous information lets us improve our products for you, our user. It helps us to make them the most relevant, easy-to-use and faultless as possible.

Who controls this information?

ESET, spol. s r.o. is the sole controller of data collected in the Program. This information is not shared with third parties.

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE [PRIVACY POLICY](#).**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the

Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software.** The Provider shall be entitled from time to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol_home. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

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

Information and Infiltrations may be collected by following functions of Software:

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

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as

part of Provider's distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider's rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider's distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider's website and accessible directly from the installation process. You can also visit it from Software's help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are

permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement.** This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software.** The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in

the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET's right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes, Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

ADDENDUM TO THE AGREEMENT

Network Connected Devices Security Assessment. Additional provisions apply to the Network Connected Devices Security Assessment as follows:

The Software contains a function for checking the security of End User's local network and security of devices in

local network which requires local network name and information about devices in local network such as presence, type, name, IP address and MAC address of device in local network in connection with license information. The information also includes wireless security type and wireless encryption type for router devices. This function may also provide information concerning availability of security software solution to secure devices in local network.

Protection Against Misuse of Data. Additional provisions apply to the Protection Against Misuse of Data as follows:

The Software contains a function that prevents loss or misuse of critical data in direct connection with theft of a Computer. This function is switched off under the default settings of the Software. The ESET HOME Account needs to be created for it to be activated, through which the function activates data collection in the event of computer theft. If you chose to activate this function of the Software, data about the stolen Computer will be collected and sent to the Provider, which can include data about the Computer's network location, data about the content displayed on the Computer screen, data about the configuration of the Computer and/or data recorded by a camera connected to the Computer (hereinafter referred to as "Data"). The End User shall be entitled to use Data obtained by this function and provided via ESET HOME Account exclusively for rectifying an adverse situation caused by theft of a Computer. For the sole purpose of this function, Provider process Data as specified in Privacy Policy and in compliance with relevant legal regulations. The Provider shall allow End User to access the Data for the period required to achieve the purpose for which the data was obtained which shall not exceed retention period specified in Privacy Policy. Protection against misuse of data shall be used exclusively with Computers and accounts End User have legitimate access to. Any illegal use will be reported to competent authority. Provider will comply with relevant laws and assist law enforcement authorities in case of the misuse. You agree and acknowledge that You are responsible for safeguarding the password to access ESET HOME Account and you agree that You shall not disclose your password to any third party. End User is responsible for any activity using Protection Against Misuse of Data function and ESET HOME Account, authorized or not. If ESET HOME Account is compromised, notify Provider immediately. Additional provisions for the Protection Against Misuse of Data shall be applicable exclusively to ESET Internet Security and ESET Smart Security Premium End Users.

ESET Secure Data. Additional provisions apply to the ESET Secure Data as follows:

1. Definitions. In these additional provisions to the ESET Secure Data the following words have the corresponding meanings:

a) "Information" any information or data encrypted or decrypted using the software;

b) "Products" the ESET Secure Data software and the documentation;

c) "ESET Secure Data" the software(s) used for the encryption and decryption of electronic data;

All references to the plural shall include the singular and all references to the masculine shall include the feminine and neuter and vice versa. Words without specific definition shall be used in compliance with definitions stipulated by the Agreement.

2. Additional End User declaration. You acknowledge and accept that:

a) It is Your responsibility to protect, maintain and backup Information;

b) You should fully back-up all information and data (including without limit any critical information and data) on Your Computer before installation of the ESET Secure Data;

c) You must keep a safe record of any passwords or other information used for setting up and using ESET Secure Data, you must also make backup copies of all encryption keys, license codes, key-files and other data generated

182

to separate storage media;

d) You are responsible for the use of Products. The Provider shall not be liable for any loss, claim or damage suffered as a consequence of any unauthorized or mistaken encryption or decryption of Information or other data wherever and however that Information or other data is stored;

e) Whilst Provider has taken all reasonable steps to ensure the integrity and security of the ESET Secure Data, the Products (or any of them) must not be used in any area which is dependent on a fail-safe level of security or is potentially hazardous or dangerous, including but not limited to nuclear facilities, aircraft navigation, control or communication systems, weapon and defense systems and life support or life monitoring systems;

f) It is End User's responsibility to ensure that the level of security and encryption provided by the products is adequate for Your requirements;

g) You are responsible for Your use of the Products or any of them, including but not limited to ensure that such use complies with all applicable laws and regulations of the Slovak Republic or such other country, region or state where the Products are used. You must ensure that prior to any use of the Products you have ensured that it is not in contravention of any government (in the Slovak Republic or otherwise) embargo;

h) ESET Secure Data may contact the Provider servers from time to time in order to check for the license information, available patches, service packs and other updates that may improve, maintain, modify or enhance the operation of ESET Secure Data and may send general system information related to the its functioning in compliance with Privacy Policy.

i) Provider shall not be responsible for any loss, damage, expense or claim arising from the loss, theft, misuse, corruption, damage or destruction of passwords, set up information, encryption keys, license activation codes and other data generated or stored during use of the software.

Additional provisions for the ESET Secure Data shall be applicable exclusively to ESET Smart Security Premium End Users.

Password Manager Software. Additional provisions apply to the Password Manager Software as follows:

1. Additional End User declaration. You acknowledge and accept that You may not:

a) use Password Manager Software to operate any mission-critical application where human life or property may be at stake. You understand that the Password Manager Software is not designed for such purposes and that its failure in such cases could lead to death, personal injury, or severe property or environmental damage for which Provider is not responsible.

PASSWORD MANAGER SOFTWARE IS NOT DESIGNED, INTENDED OR LICENSED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE CONTROLS INCLUDING, WITHOUT LIMITATION, THE DESIGN, CONSTRUCTION, MAINTENANCE OR OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, AND LIFE SUPPORT OR WEAPONS SYSTEMS. PROVIDER SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH PURPOSES.

b) use Password Manager Software in a manner that breaches this agreement or the laws of the Slovak Republic or your jurisdiction. Specifically you may not use Password Manager Software to conduct or promote any illegal activities including uploading data of harmful content or content that might be used for any illegal activities or that in any way violates the law or the rights of any third party (including any intellectual property rights), including but not limited to any attempts to gain access to accounts in Storage (For the purposes of these additional terms to the Password Manager Software "Storage" refers to the data storage space managed by Provider or a third party other than Provider and the user for the purpose of enabling synchronization and backup

of user data) or any accounts and data of other Password Manager Software or Storage users. If you violate any of these provisions, Provider is entitled to immediately terminate this agreement and pass on to you the cost of any necessary remedy, as well as take any necessary steps to prevent you from further use of Password Manager Software without the possibility of refund.

2. LIMITATION OF LIABILITY. PASSWORD MANAGER SOFTWARE IS PROVIDED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE THE SOFTWARE AT YOUR OWN RISK. THE PRODUCER IS NOT LIABLE FOR DATA LOSS, DAMAGES, LIMITATION OF SERVICE AVAILABILITY INCLUDING ANY DATA SENT BY PASSWORD MANAGER SOFTWARE TO EXTERNAL STORAGE FOR THE PURPOSE OF DATA SYNCHRONIZATION AND BACKUP. ENCRYPTING THE DATA USING PASSWORD MANAGER SOFTWARE DOES NOT IMPLY ANY LIABILITY OF THE PROVIDER REGARD-ING THE SECURITY OF THAT DATA. YOU EXPRESSLY AGREE THAT THE DATA ACQUIRED, USED, ENCRYPTED, STORED, SYNCHRONIZED OR SENT USING PASSWORD MANAGER SOFTWARE CAN ALSO BE STORED ON THIRD-PARTY SERVERS (APPLIES ONLY TO THE USE OF PASSWORD MANAGER SOFTWARE WHERE SYNCHRONIZATION AND BACKUP SERVICES HAVE BEEN ENABLED). IF PROVIDER IN ITS SOLE DISCRETION SELECTS TO USE SUCH A THIRD-PARTY STORAGE, WEBSITE, WEB PORTAL, SERVER OR SERVICE, PROVIDER IS NOT LIABLE FOR THE QUALITY, SECURITY, OR AVAILABILITY OF SUCH A THIRD-PARTY SERVICE AND TO NO EXTENT IS PROVIDER LIABLE TO YOU FOR ANY BREACH OF CONTRACTUAL OR LEGAL OBLIGATIONS BY THE THIRD PARTY NOR FOR DAMAGES, LOSS OF PROFITS, FINANCIAL OR NON-FINANCIAL DAMAGES, OR ANY OTHER KIND OF LOSS WHILE USING THIS SOFTWARE. PROVIDER IS NOT LIABLE FOR THE CONTENT OF ANY DATA ACQUIRED, USED, ENCRYPTED, STORED, SYNCHRONIZED, OR SENT USING PASSWORD MANAGER SOFTWARE OR IN STORAGE. YOU ACKNOWLEDGE THAT PROVIDER DOES NOT HAVE ACCESS TO THE CONTENT OF THE STORED DATA AND IS NOT ABLE TO MONITOR IT OR REMOVE LEGALLY HARMFUL CONTENT.

Provider owns all rights to improvements, upgrades and fixes related to Password Manager Software ("Improvements") even in the event that any such Improvements have been created based on feedback, ideas or suggestions submitted by you in any form. You will not be entitled to any compensation, including any royalties related to such Improvements.

PROVIDER ENTITIES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR CLAIMS AND LIABILITIES OF ANY KIND ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF PASSWORD MANAGER SOFTWARE BY YOU OR BY THIRD PARTIES, TO THE USE OR NON-USE OF ANY BROKERAGE FIRM OR DEALER, OR TO THE SALE OR PURCHASE OF ANY SECURITY, WHETHER SUCH CLAIMS AND LIABILITIES ARE BASED ON ANY LEGAL OR EQUITABLE THEORY.

PROVIDER ENTITIES AND LICENSORS ARE NOT LIABLE TO YOU FOR ANY AND ALL DIRECT, INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO ANY THIRD-PARTY SOFTWARE, ANY DATA ACCESSED THROUGH PASSWORD MANAGER SOFTWARE, YOUR USE OR INABILITY TO USE OR ACCESS PASSWORD MANAGER SOFTWARE, OR ANY DATA PROVIDED THROUGH PASSWORD MANAGER SOFTWARE, WHETHER SUCH DAMAGE CLAIMS ARE BROUGHT UNDER ANY THEORY OF LAW OR EQUITY. DAMAGES EXCLUDED BY THIS CLAUSE INCLUDE, WITHOUT LIMITATION, THOSE FOR LOSS OF BUSINESS PROFITS, INJURY TO PERSON OR PROPERTY, BUSINESS INTERRUPTION, LOSS OF BUSINESS OR PERSONAL INFORMATION. SOME JURISDICTIONS DO NOT ALLOW LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS RESTRICTION MAY NOT APPLY TO YOU. IN SUCH CASE THE EXTENT OF PROVIDER LIABILITY WILL BE THE MINIMUM PERMITTED UNDER APPLICABLE LAW.

INFORMATION PROVIDED THROUGH PASSWORD MANAGER SOFTWARE, INCLUDING STOCK QUOTES, ANALYSIS, MARKET INFORMATION, NEWS, AND FINANCIAL DATA, MAY BE DELAYED, INACCURATE, OR CONTAIN ERRORS OR OMISSIONS, AND PROVIDER ENTITIES AND LICENSORS WILL HAVE NO LIABILITY WITH RESPECT THERETO. PROVIDER MAY CHANGE OR DISCONTINUE ANY ASPECT OR FEATURE OF PASSWORD MANAGER SOFTWARE OR THE USE OF ALL OR ANY FEATURES OR TECHNOLOGY IN PASSWORD MANAGER SOFTWARE AT ANY TIME WITHOUT PRIOR NOTICE TO YOU.

IF THE PROVISIONS IN THIS ARTICLE ARE VOID FOR ANY REASON OR PROVIDER IS DEEMED LIABLE FOR LOSSES, DAMAGES ETC UNDER APPLICABLE LAWS, THE PARTIES AGREE THAT PROVIDER'S LIABILITY TO YOU WILL BE

LIMITED TO THE TOTAL AMOUNT OF LICENSE FEES PAID BY YOU.

YOU AGREE TO INDEMNIFY, DEFEND AND HOLD HARMLESS PROVIDER AND ITS EMPLOYEES, SUBSIDIARIES, AFFILIATES, REBRANDING AND OTHER PARTNERS FROM AND AGAINST ANY AND ALL THIRD PARTY (INCLUDING OWNERS OF THE DEVICE OR PARTIES WHOSE RIGHTS WERE AFFECTED BY THE DATA USED IN PASSWORD MANAGER SOFTWARE OR IN STORAGE) CLAIMS, LIABILITIES, DAMAGES, LOSSES, COSTS, EXPENSES, FEES THAT SUCH PARTIES MAY INCUR AS A RESULT OF YOUR USE OF THE PASSWORD MANAGER SOFTWARE.

3. Data in Password Manager Software. Unless otherwise, and explicitly, selected by you, all data entered by you that is saved into a Password Manager Software database is stored in encrypted format on your computer, or other storage device as defined by you. You understand that in the case of deletion of, or damage to, any Password Manager Software database or other files, all the data contained therein will be irreversibly lost and you under-stand and accept the risk of such loss. The fact that your personal data is stored in encrypted format on the computer does not mean that the information cannot be stolen or misused by someone who discovers the Master Password or gains access to the customer-defined activation device for opening the database. You are responsible for maintaining the security of all access methods.

4. Transmission of Personal Data to Provider or Storage. If You select so and solely for the purpose of ensuring timely data synchronization and backup, Password Manager Software transmits or sends personal data from the Password Manager Software database - namely passwords, login information, Accounts and Identities to Storage over the Internet. Data is transmitted exclusively in encrypted form. The use of Password Manager Software for filling in online forms with passwords, logins or other data may require that information being sent over the Internet to the website identified by You. This transmission of data is not initiated by Password Manager Software and therefore Provider cannot be held responsible for the security of such interactions with any website operated by various providers. Any transactions over the Internet whether or not in conjunction with Password Manager Software is done at Your own discretion and risk, and You will be solely responsible for any damage to Your Computer or loss of data resulting from the download and/or use of any such material or service. To minimize the risk of losing valuable data, Provider recommends that End User perform periodic backup of the database and other sensitive files to external drives. Provider is not able to provide You with any assistance in recovering lost or damaged data. If Provider provides backup services for End User database files in case of damage or deletion of the files on End User's Computer, such backup service is without any warranty and does not imply any liability of Provider to you whatsoever.

By using Password Manager Software, you agree that the software may contact the Provider servers from time to time in order to check for the license information, available patches, service packs and other updates that may improve, maintain, modify or enhance the operation of Password Manager Software. The software may send general system information related to the functioning of Password Manager Software in compliance with Privacy Policy.

5. Uninstall information and instructions. Any information that you would like to retain from the database must be exported prior to uninstalling Password Manager Software.

Additional provisions for the Password Manager Software shall be applicable exclusively to ESET Smart Security Premium End Users.

ESET LiveGuard. Additional provisions apply to the ESET LiveGuard as follows:

The Software contains a function of additional analysis of files submitted by End User. The Provider shall only use the files submitted by End User and results of analysis in compliance with Privacy Policy and in compliance with relevant legal regulations.

Additional provisions for the ESET LiveGuard shall be applicable exclusively to ESET Smart Security Premium End Users.

185

Privacy Policy

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

- Legal Basis of Personal Data Processing,

- Data Sharing and Confidentiality,

- Data Security,

- Your Rights as a Data Subject,

- Processing of Your Personal Data

- Contact Information.

Legal Basis of Personal Data Processing

There are a few legal bases for data processing which We use according to the applicable legislative framework related to protection of personal data. The processing of personal data at ESET is mainly necessary for the performance of the End User License Agreement ("EULA") with End User (Art. 6 (1) (b) GDPR), which is applicable for the provision of ESET products or services, unless explicitly stated otherwise, e.g.:

- Legitimate interest legal basis (Art. 6 (1) (f) GDPR), that enables us to process data on how our customers use our Services and their satisfaction to provide our users with the best protection, support and experience We can offer. Even marketing is recognized by applicable legislation as a legitimate interest, therefore We usually rely on it for marketing communication with our customers.

- Consent (Art. 6 (1) (a) GDPR), which We may request from You in specific situations when we deem this legal basis as the most suitable one or if it is required by law.

- Compliance with a legal obligation (Art. 6 (1) (c) GDPR), e.g. stipulating requirements for electronic communication, retention for invoicing or billing documents.

Data Sharing and Confidentiality

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

ESET prefers to process its data in the European Union (EU). However, depending on your location (use of our products and/or services outside the EU) and/or the service you choose, it may be necessary to transfer your data

to a country outside the EU. For example, we use third-party services in connection with cloud computing. In these cases, we carefully select our service providers and ensure an appropriate level of data protection through contractual as well as technical and organizational measures. As a rule, we agree on the EU standard contractual clauses, if necessary, with supplementary contractual regulations.

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these countries does not require any special authorization or agreement.

Data Security

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 the relevant supervisory authority as well as affected End Users as data subjects.

Data Subject's Rights

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

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

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

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

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

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

Right to Erasure and Right to Restriction of Processing. As a data subject, you have the right to request the deletion or restriction of the processing of your personal data. If we process your personal data, for example, with your consent, you withdraw it and there is no other legal basis, for example, a contract, We delete your personal

data immediately. Your personal data will also be deleted as soon as they are no longer required for the purposes stated for them at the end of our retention period.

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

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

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

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

Processing of Your Personal Data

Services provided by ESET implemented in our product are provided under the terms of [EULA](#), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and the product [documentation](#). To make it all work, We need to collect the following information:

Licensing and Billing Data. The name, e-mail address, license key and (if applicable) address, company affiliation and payment data are collected and processed by ESET in order to facilitate the activation of license, license key delivery, reminders on expiration, support requests, license genuineness verification, provision of our service sand other notifications including marketing messages in line with applicable legislation or Your consent. ESET is legally obliged to keep the billing information for the period of 10 years, however the licensing information will be anonymized no later than 12 months after the expiration of license.

Update and Other Statistics. The processed information includes 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 are processed for the purpose of provision update and upgrade services and for the purpose of maintenance, security and improvement of our backend infrastructure.

This information is kept apart from the identification information required for the licensing and billing purposes since it does not require the identification of End User. The retention period is up to 4 years.

ESET LiveGrid® Reputation System. One-way hashes related to infiltration are processed for the purpose 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. The End User is not identified during this process.

ESET LiveGrid® Feedback System. Suspicious samples and metadata from the wild are collected 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 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 our 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.

All information obtained and processed through the ESET LiveGrid® Feedback System are meant to be used without the identification of End User.

Network Connected Devices Security Assessment. To provide the security assessment function, We process the local network name and information about devices in your local network, such as presence, type, name, IP address and MAC address of the device in your local network in connection with license information. The information also includes wireless security type and wireless encryption type for router devices. The license information identifying the End User will be anonymized no later than 12 months after the expiration of the license.

Technical Support. The contact and licensing 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. The data processed for technical support is stored for 4 years.

Protection Against Misuse of Data. If the ESET HOME Account on https://home.eset.com is created and the function is activated by End User in connection with theft of computer, following information will be collected and processed: the location data, screenshots, data about the configuration of computer and data recorded by computer's camera. The collected data are stored on our servers or on the servers of our service providers with retention period of 3 months.

Password Manager. If You choose to activate the function of Password Manager, the data related to your login details are stored in an encrypted form only on your computer or other designated device. If You activate the synchronization service, the encrypted data are stored on our servers or on the servers of our service providers to ensure such service. Neither ESET nor the service provider have access to the encrypted data. Only You have the key to decrypt the data. The data will be removed upon the deactivation of the function.

ESET LiveGuard. If You choose to activate the ESET LiveGuard function, it requires the submission of samples such as files predefined and selected by the End User. The samples You choose for the remote analysis will be uploaded to the ESET service, and the result of the analysis will be sent back to Your computer. Any suspicious samples are processed in the manner of information collected by ESET LiveGrid® Feedback System.

Customer Experience Improvement Program. If You chose to activate Customer Experience Improvement Program , the anonymous telemetry information relating to the use of Our products will be collected and used, based on Your consent.

Please note that if the person using our products and services is not the End User who has purchased the product or service and concluded the EULA with Us, (e.g. an employee of the End User, a family member or a person

otherwise authorized to use the product or service by the End User in compliance with EULA, the processing of the data is carried out in the legitimate interest of ESET within the meaning of Art. 6 (1) f) GDPR to enable the user authorized by End User to use the products and services provided by Us in accordance with EULA.

Contact Information

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk