NOD32® ANTIVIRUS

USER GUIDE

(intended for product version 12.0 and higher)

Microsoft® Windows® 10 / 8.1 / 8 / 7 SP1 / Vista SP2 / Home Server 2011

Click here to display Online help version of this document
## Contents

1. **ESET NOD32 Antivirus** ........................................ 5
   1.1 What’s new in this version? .......................... 5
   1.2 Which product do I have? .......................... 6
   1.3 System requirements ................................ 7
   1.4 Prevention ........................................... 7

2. **Installation** .................................................... 9
   2.1 Live installer ......................................... 9
   2.2 Offline installation .................................. 10
   2.3 Product activation .................................... 11
      2.3.1 Entering your License Key during activation .... 12
      2.3.2 Use License Manager ............................ 12
      2.3.3 Activate Trial License ........................... 13

2.4 Common installation problems .......................... 13
   2.4.1 Activation failed .................................. 13

2.5 First scan after installation ............................ 14

2.6 Upgrading to a more recent version ............... 14

2.7 Referring ESET product to a friend ............... 15

3. **Beginner’s guide** .......................................... 16
   3.1 The main program window ....................... 16
   3.2 Updates ............................................. 18

4. **Working with ESET NOD32 Antivirus** ............ 20
   4.1 Computer protection ................................ 21
      4.1.1 Detection engine .............................. 22
      4.1.1.1 Real-time file system protection ........... 23
      4.1.1.1.1 Additional ThreatSense parameters ...... 24
      4.1.1.1.2 Cleaning levels .................................. 24
      4.1.1.1.3 When to modify real-time protection configuration .... 25
      4.1.1.1.4 Checking real-time protection ............ 25
      4.1.1.1.5 What to do if real-time protection does not work .......... 25
      4.1.1.1.6 Processes exclusions .................... 26
      4.1.1.2 Computer scan ................................ 27
      4.1.1.2.1 Custom scan launcher .................. 28
      4.1.1.2.2 Scan progress .......................... 29
      4.1.1.2.3 Computer scan log ........................ 30
      4.1.1.2.4 Malware scans ............................ 31
      4.1.1.2.4.1 Idle-state scan ........................ 31
      4.1.1.2.4.2 Scan profiles ................................ 31
      4.1.1.2.4.3 Scan targets ................................ 32
      4.1.1.2.4.4 Advanced scan options ............... 32
      4.1.1.3 Startup scan .................................. 32
      4.1.1.3.1 Automatic startup file check .......... 33
      4.1.1.4 Exclusions .................................... 33
      4.1.1.4.1 Add or Edit exclusion .................. 34
      4.1.1.4.2 Exclusion format .......................... 35
      4.1.1.5 ThreatSense parameters .................... 36
      4.1.1.5.1 Cleaning .................................... 38
      4.1.1.5.2 File extensions excluded from scanning ........ 38

   4.1.1.6 An infiltration is detected .................. 39
   4.1.1.7 Removable media .............................. 41
   4.1.1.8 Document protection ......................... 41
   4.1.2 Device control and Webcam protection ........ 42
   4.1.2.1 Device control rules editor ................. 43
   4.1.2.1.1 Detected devices .......................... 43
   4.1.2.2 Device groups .................................. 44
   4.1.2.3 Adding Device control rules ................. 45
   4.1.3 Host-based Intrusion Prevention System (HIPS) .... 46
   4.1.3.1 HIPS interactive window ................. 48
   4.1.3.1.1 Potential ransomware behavior detected ...... 50
   4.1.3.2 HIPS rule management ........................ 50
   4.1.3.2.1 HIPS rule settings .......................... 51
   4.1.3.2.2 Add application/registry path for HIPS .......... 53
   4.1.3.3 HIPS exclusions ................................ 54
   4.1.3.4 HIPS advanced setup .......................... 54
   4.1.3.4.1 Drivers always allowed to load ............ 54
   4.1.4 Gamer mode ...................................... 54

4.2 **Internet protection** .................................... 55
   4.2.1 Protocol filtering ................................ 55
   4.2.1.1 Web and email clients ...................... 56
   4.2.1.2 Excluded applications ....................... 56
   4.2.1.3 Excluded IP addresses ....................... 57
   4.2.1.3.1 Add IPv4 address ......................... 57
   4.2.1.3.2 Add IPv6 address .......................... 57
   4.2.1.4 SSL/TLS ........................................ 58
   4.2.1.4.1 Certificates ................................. 59
   4.2.1.4.1.1 Encrypted network traffic ............... 59
   4.2.1.4.2 List of known certificates ................ 59
   4.2.1.4.3 List of SSL/TLS filtered applications .... 60
   4.2.2 Email client protection ......................... 60
   4.2.2.1 Email protocols ............................. 61
   4.2.2.2 Email alerts and notifications .............. 62
   4.2.2.3 Integration with email clients ............. 63
   4.2.2.3.1 Email client protection configuration .... 63
   4.2.2.4 POP3, POP3S filter .......................... 63
   4.2.3 Web access protection .......................... 64
   4.2.3.1 Basic .......................................... 64
   4.2.3.2 Web protocols ................................ 65
   4.2.3.3 URL address management .................... 65
   4.2.3.3.1 URL addresses list ....................... 66
   4.2.3.3.2 Create new URL address list ............. 67
   4.2.3.3.3 How to add URL mask .................... 68
   4.2.4 Anti-Phishing protection ......................... 68

4.3 **Updating the program** ................................ 70
   4.3.1 Update settings .................................. 72
   4.3.1.1 Advanced update setup ...................... 74
   4.3.1.1.1 Update mode ................................ 74
   4.3.1.1.2 Connection options ....................... 74
   4.3.2 Update rollback .................................. 75
   4.3.3 How to create update tasks ...................... 76

4.4 **Tools** ..................................................... 77
4.4.1 Tools in ESET NOD32 Antivirus ...........................................77
4.4.1.1 Log files.................................................................78
4.4.1.1.1 Log filtering......................................................79
4.4.1.1.2 Logging configuration......................................80
4.4.1.2 Running processes..............................................81
4.4.1.3 Security report...................................................83
4.4.1.4 Watch activity....................................................84
4.4.1.5 ESET SysInspector.............................................84
4.4.1.6 Scheduler............................................................85
4.4.1.7 System cleaner..................................................87
4.4.1.8 ESET SysRescue Live..........................................87
4.4.1.9 Cloud-based protection...................................87
4.4.1.9.1 Suspicious files .............................................89
4.4.1.10 Quarantine..........................................................90
4.4.1.11 Proxy server....................................................91
4.4.1.12 Email notifications.........................................92
4.4.1.12.1 Message format..........................................93
4.4.1.13 Select sample for analysis.............................93
4.4.1.14 Microsoft Windows® update.............................94
4.4.1.15 ESET CMD...........................................................95

4.5 User interface ..................................................................96
4.5.1 User interface elements...........................................97
4.5.2 Alerts and notifications.........................................98
4.5.2.1 Confirmation messages...................................99
4.5.3 Access setup..........................................................99
4.5.4 System tray icon...................................................100
4.5.5 Help and support..................................................101
4.5.5.1 About ESET NOD32 Antivirus .........................103
4.5.5.2 ESET News.......................................................103
4.5.5.3 Submit system configuration data....................104

5. Advanced user.............................................................105
5.1 Profiles.......................................................................105
5.2 Keyboard shortcuts....................................................105
5.3 Diagnostics.................................................................106
5.4 Import and export settings........................................107
5.5 Command Line..........................................................107
5.6 Idle-state detection.....................................................109

6. Common Questions ..................................................110
6.1 How to update the ESET NOD32 Antivirus.....................110
6.2 How to remove a virus from my PC...............................110
6.3 How to create a new task in Scheduler.........................111
6.4 How to schedule a weekly computer scan..................111
6.5 How to unlock Advanced setup...................................112
1. 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 endanger 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redesigned user interface</td>
<td>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.</td>
</tr>
<tr>
<td>Antivirus and antispyware</td>
<td>Proactively detects and cleans more known and unknown viruses, worms, trojans and rootkits. Advanced heuristics flags even never-before-seen malware, protecting you from unknown threats and neutralizing them before they can do any harm. Web access protection and Anti-Phishing works by monitoring communication between web browsers and remote servers (including SSL). Email client protection provides control of email communication received through the POP3(S) and IMAP(S) protocols.</td>
</tr>
<tr>
<td>Regular updates</td>
<td>Regularly updating the detection engine (previously known as &quot;virus signature database&quot;) and program modules is the best way to ensure the maximum level of security on your computer.</td>
</tr>
<tr>
<td>ESET LiveGrid® (Cloud-powered Reputation)</td>
<td>You can check the reputation of running processes and files directly from ESET NOD32 Antivirus.</td>
</tr>
<tr>
<td>Device control</td>
<td>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.</td>
</tr>
<tr>
<td>HIPS functionality</td>
<td>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.</td>
</tr>
<tr>
<td>Gamer mode</td>
<td>Postpones all pop-up windows, updates or other system-intensive activities to conserve system resources for gaming and other full-screen activities.</td>
</tr>
</tbody>
</table>

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.

1.1 What's new in this version?

The new version of ESET NOD32 Antivirus features the following improvements:

- **One-click logging** – You can create advanced logs with just one click.

- **Unified Extensible Firmware Interface (UEFI) Scanner** – Adds elevated levels of malware protection by detecting and removing threats that potentially launch before the operating system boots up. Read more about this type of technology in the [glossary](#).

- **High performance and low system impact** – This version is designed for efficient use of system resources, allowing you to enjoy your computer’s performance while defending against new types of threats.
• **Reorganized Advanced setup** – The ESET LiveGrid® settings were moved to the Detection engine section, Antispam advanced logging moved to Diagnostic section, etc.

• **Improved screen reader support** – ESET NOD32 Antivirus supports the most popular screen readers (JAWS, NVDA, Narrator).

• **Drag and drop files scan** – You can scan a file or folder by just by dragging it to the marked area.

• **Referring ESET product to a friend** - ESET NOD32 Antivirus now offers referral bonuses, so you can share your ESET product experience with your family or friends.

• ESET NOD32 Antivirus is now being installed in a compact format to make the installation faster. After the product is installed and activated, the modules start downloading.

• ESET NOD32 Antivirus informs you when you connect to an unprotected wireless network or a network with weak protection.

For more details about the new features in ESET NOD32 Antivirus please read the following ESET Knowledgebase article:

[What's new in this version of ESET home products](#)

### 1.2 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 (see the [Knowledgebase article](#)) and you will see the name of the product at the top of the window (header).

<table>
<thead>
<tr>
<th>Feature</th>
<th>ESET NOD32 Antivirus</th>
<th>ESET Internet Security</th>
<th>ESET Smart Security Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Antispyware</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exploit Blocker</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Script-Based Attack Protection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anti-Phishing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web access protection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HIPS (including Ransomware shield)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Antispam</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected Home Monitor</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Webcam Protection</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Attack Protection</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Botnet Protection</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banking &amp; Payment Protection</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Parental Control  
Anti-Theft  
ESET Password Manager  
ESET Secure Data

Note
Some of the products above may not be available for your language / region.

1.3 System requirements

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

Processors Supported
Intel® or AMD x86-x64

Supported Operating Systems
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1
Microsoft® Windows® Vista SP2
Microsoft® Windows® Home Server 2011 64-bit

1.4 Prevention

When you work with your computer, and especially when you browse the Internet, please keep in mind that no antivirus system in the world can completely eliminate the risk of detections and remote attacks. To provide maximum protection and convenience, it is essential that you use your antivirus solution correctly and adhere to several useful rules:

Update regularly
According to statistics from ESET LiveGrid®, thousands of new, unique infiltrations are created each day in order to bypass existing security measures and bring profit to their authors – all at the expense of other users. The specialists at the ESET Research Lab analyze these threats on a daily basis and prepare and release updates in order to continually improve the level of protection for our users. To ensure the maximum effectiveness of these updates it is important that updates are configured properly on your system. For more information on how to configure updates, see the Update setup chapter.

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

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

Detection of more known and unknown viruses, worms, trojans and rootkits are handled by the Real-time file system protection module. This means that every time you access or open a file, it is scanned for a malware activity. We recommend that you run a full Computer scan at least once a month because malware signatures may vary and the detection engine updates itself each day.

**Follow basic security rules**

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

- Do not visit suspicious websites with multiple pop-ups and flashing advertisements.
- Be careful when installing freeware programs, codec packs, etc. Only use safe programs and only visit safe Internet websites.
- Be cautious when opening email attachments, particularly those from mass-mailed messages and messages from unknown senders.
- Don’t use an Administrator account for everyday work on your computer.
2. 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** can be downloaded from the ESET website. The installation package is universal for all languages (choose a desired language). Live installer itself is a small file; additional files required to install ESET NOD32 Antivirus will be downloaded automatically.

- **Offline installation** – This type of installation is used when installing from a product CD/DVD. It uses an .exe file that is larger than the Live installer file and does not require an internet connection or additional files for the completion of installation.

**Important**

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).

2.1 Live installer

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

**Important**

For this type of installation you must be connected to Internet.

1. Select your desired language from the drop-down menu and click Continue. Allow a few moments for installation files to download.

2. Read and accept the End-User License Agreement.

3. The next step is to choose an activation option. If you are installing a more recent version over the previous one, your license key will be entered automatically.
4. Select your preference for ESET LiveGrid® feedback system and Detection of potentially unwanted applications. Grayware or Potentially Unwanted Application (PUA) is a broad category of software, whose intent is not as unequivocally malicious as with other types of malware, such as viruses or trojan horses. See the Potentially unwanted applications chapter for more details.

5. Select your preference for participation in Customer Experience Improvement Program. By joining the Customer Experience Improvement Program you provide ESET with anonymous information relating to the use of our products. The collected data will help us to improve the experience for you and will never be shared with third parties. What information do we collect?

6. Click **Install** to start the installation process. It may take a few moments.

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

---

**Note**

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.

**Note**

If you have a license that allows you to install other versions of a product, then you can select product according to your preferences. More information about features in each specific product.

---

### 2.2 Offline installation

Once you launch the offline installation (.exe), the Installation Wizard will guide you through the setup process.

1. Select your desired language from the drop-down menu and click **Continue**. Allow a few moments for installation files to download.

2. Read and accept the **End-User License Agreement**.

3. The next step is to choose an **activation option**. If you are installing a more recent version over the previous one, your license key will be entered automatically.

4. Select your preference for ESET LiveGrid® feedback system and Detection of potentially unwanted applications. Grayware or Potentially Unwanted Application (PUA) is a broad category of software, whose intent is not as
unequivocally malicious as with other types of malware, such as viruses or trojan horses. See the Potentially unwanted applications chapter for more details.

5. Select your preference for participation in Customer Experience Improvement Program. By joining the Customer Experience Improvement Program you provide ESET with anonymous information relating to the use of our products. The collected data will help us to improve the experience for you and will never be shared with third parties. What information do we collect?

6. Click Install to start the installation process. It may take a few moments.

7. Click Done to exit the Installation Wizard.

---

**Note**

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.

**Note**

If you have a license that allows you to install other versions of a product, then you can select product according to your preferences. More information about features in each specific product.

---

### 2.3 Product activation

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

- If you purchased a retail boxed version of the product, activate your product by clicking **Enter a License Key**. The License Key is usually located inside or on the back side of the product package. The License Key must be entered as supplied for activation to be successful. License Key – 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 activation of the license.
- After selecting **Use License Manager** you will be asked for your my.eset.com credentials in a new window.
- If you would like to evaluate ESET NOD32 Antivirus before making a purchase, select **Free trial**. Enter 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 would like to buy one, click **Purchase license**. This will redirect you to the website of your local ESET distributor.

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.

If you have a Username and Password used for activation of older ESET products and do not know how to activate ESET NOD32 Antivirus, convert your legacy credentials to a License Key.
2.3.1 Entering your License Key during activation

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

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

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

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

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

2.3.2 Use License Manager

After selecting Use License Manager you will be asked for your my.eset.com credentials in a new window. Enter your my.eset.com credentials and click Sign in to use a license in ESET License Manager. Choose a license for activation, click Continue and your ESET NOD32 Antivirus will be activated.

Note
If you do not have a my.eset.com account yet, register by clicking the Create account button.

Note
If you forgot your password click I forgot my password and follow the steps on the web page you will be redirected to.
ESET License Manager helps you manage all your ESET licenses. You can easily renew, upgrade or extend your license and see the important license details. First, enter your License Key. After that, you will see the product, associated device, the number of available seats and the expiration date. You can deactivate or rename specific devices. When you click Renew you will be redirected to the online store where you can confirm the purchase and buy the renewal.

If you want to upgrade your license (for example from ESET NOD32 Antivirus to ESET Smart Security Premium) or would like to install an ESET security product on another device, you will be redirected to the online store to complete the purchase.

In ESET License Manager, you can also add different licenses, download products to your devices, or share licenses through email.

2.3.3 Activate Trial License
Enter your name and email address to activate your ESET NOD32 Antivirus trial version. The trial may 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.

Enter a valid email address into the Email address field. After activation, your Username and Password required for updating ESET NOD32 Antivirus will be generated and sent to your email. This email address will also be used for product expiration notifications and other communication with ESET.

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

2.4.1 Activation failed
In the case activation of ESET NOD32 Antivirus was not successful, the most-common possible scenarios are:

- License key already in use
- Invalid License key. Product activation form error
- Additional information necessary for activation is missing or invalid
- Communication with the activation database failed. Please try to activate again in 15 minutes
- No or disabled connection to ESET activation servers, for more information see Ports and addresses required to use your ESET product with a third-party firewall

Make sure you have entered the proper License key and attempt to activate again.

If you are unable to activate, please read Resolve ACT or ECP errors during activation.
2.5 First scan after installation

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

You can also start a computer scan manually from the main program window by clicking **Computer scan > Scan your computer**. For more information about computer scans, see the section **Computer scan**.

![Computer scan](image)

2.6 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 more recent 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 newer version immediately after its release, use one of the methods below.

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.
2.7 Referring ESET product to a friend

This version of ESET NOD32 Antivirus now offers referral bonuses, so you can share your ESET product experience with your family or friends. You can even share referrals from a product activated with a trial license. When you are a trial user, for each successful referral you send that results in a product activation, both you and your friend will receive an extra time on the trial license.

You can refer using your installed ESET NOD32 Antivirus. The product you can refer depends on the product you are referring from, see the table below.

<table>
<thead>
<tr>
<th>Your installed product</th>
<th>Product you can refer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET NOD32 Antivirus</td>
<td>ESET Internet Security</td>
</tr>
<tr>
<td>ESET Internet Security</td>
<td>ESET Internet Security</td>
</tr>
<tr>
<td>ESET Smart Security Premium</td>
<td>ESET Smart Security Premium</td>
</tr>
</tbody>
</table>

Referring a product

To send a referral link, click Refer a friend in the ESET NOD32 Antivirus main menu. Click Share referral link. Your product will generate a referral link that will be displayed in a new window. Copy the link and send it to your family and friends. You can share your referral link directly from your ESET product by using Share on Facebook, Refer your Gmail contacts and Share on Twitter options.

When your friend clicks the referral link you send to them, they will be redirected to a web page where they can download the product and use it for an additional one month of FREE protection. As a trial user, you will receive a notification for each referral link that is successfully activated and your license will be automatically extended for an additional one month of FREE protection. This way you can extend your FREE protection by up to 5 months. You can check the number of successfully activated referral links in the Refer a friend window of your ESET product.
3. Beginner's guide

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

3.1 The main program window

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

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

- **Home** – Provides information about the protection status of ESET NOD32 Antivirus.
- **Computer scan** – Configure and launch a scan of your computer or create a custom scan.
- **Update** – Displays information about detection engine updates.
- **Tools** – Provides access to Log files, Protection statistics, Watch activity, Running processes, Scheduler, ESET SysInspector and ESET SysRescue. For more information about tools, see the Tools in ESET NOD32 Antivirus chapter.
- **Setup** – Select this option to adjust the security level for Computer, Internet.
- **Help and support** – Provides access to help files, the ESET Knowledgebase, the ESET website, and links to submit support request.

The **Home** screen contains important information about the current protection level of your computer. The status window displays frequently used features in ESET NOD32 Antivirus. Information about the most recent update and your program’s expiration date is also found here.

The green icon and green **Maximum protection** status indicates 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, will be displayed under Home. To change the status of individual modules, click Setup and select the desired module.

The red icon and red Maximum protection is not ensured status indicate critical problems. There are several reasons this status may be displayed, for example:

- **Product not activated** – You can activate ESET NOD32 Antivirus from Home by clicking Activate product or Buy now under Protection status.

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

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

- **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.

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 pop-up windows and stops any scheduled tasks.

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

### 3.2 Updates

Updating the detection engine and updating program components is an important part of protecting your system against malicious code. Pay careful attention to their configuration and operation. In the main menu, click **Update** and then click **Check for updates** to check for a detection engine update.

If the License key was not entered during the activation of ESET NOD32 Antivirus you will be prompted for them at this point.
The Advanced setup window (click Setup in the main menu and then click Advanced setup, or press F5 on your keyboard) contains additional update options. To configure advanced update options such as update mode, proxy server access and LAN connections, click on particular tab in the Update window.
4. Working with ESET NOD32 Antivirus

ESET NOD32 Antivirus setup options allow you to adjust the protection levels of your computer.

The Setup menu is divided into the following sections:

- **Computer protection**
- **Internet protection**

Click a component to adjust advanced settings for the corresponding protection module.

**Computer protection** setup allows you to enable or disable the following components:

- **Real-time file system protection** – All files are scanned for malicious code when they are opened, created, or run on your computer.
- **Device control** – This module allows you to scan, block or adjust extended filters/permissions and select how the user can access and use a given device (CD/DVD/USB...).
- **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.

**Internet protection** setup allows you to enable or disable the following components:

- **Web access protection** – If enabled, all traffic through HTTP or HTTPS is scanned for malicious software.
- **Email client protection** – Monitors communication received through POP3(S) and IMAP(S) protocols.
- **Anti-Phishing protection** – Filters websites suspected of distributing content intended to manipulate users into submitting confidential information.

To re-enable a disabled security component, click the slider so that it displays a green check mark.
Note
When disabling protection using this method, all disabled protection modules will be enabled after a computer restart.

Additional options are available at the bottom of the setup window. Use the Advanced setup link to setup 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.

4.1 Computer protection

Click Computer Protection from the Setup window to see an overview of all protection modules. To turn off individual modules temporarily, click . Note that this may decrease the protection level of your computer. Click next to a protection module to access advanced settings for that module.

Click ➔ Edit exclusions next to Real-time file system protection to open the Exclusion setup window, which allows you to 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 where you can determine how long protection is disabled using the Time interval drop-down menu. Click Apply to confirm.
4.1.1 Detection engine

Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by first blocking it and then cleaning, deleting or moving it to quarantine.

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

- **Potentially unwanted applications** – Grayware or Potentially Unwanted Application (PUA) is a broad category of software, whose intent is not as unequivocally malicious as with other types of malware, such as viruses or trojan horses. It may however install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user. Read more about these types of applications in the glossary.

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

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

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

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, 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. To exclude an object from scanning see Exclusions.
Enable advanced scanning via AMSI – Microsoft Antimalware Scan Interface tool that allows application developers new malware defenses (Windows 10 only).

4.1.1.1 Real-time file system protection
Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code when they are opened, created, or run on your computer. Real-time file system protection is launched at system startup.

By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. In special cases (for example, if there is a conflict with another real-time scanner), real-time protection can be disabled by disengaging Enable Real-time file system protection in Advanced setup under Real-time file system protection > Basic.

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

- **Local drives** – Controls all system hard drives.
- **Removable media** – Controls CD/DVDs, USB storage, Bluetooth devices, etc.
- **Network drives** – Scans all mapped drives.

We recommend that you use default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

Scan on
By default, all files are scanned upon opening, creation, or execution. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:
- **File open** – Enables or disables scanning when files are opened.
- **File creation** – Enables or disables scanning when files are created.
- **File execution** – Enables or disables scanning when files are run.
- **Removable media access** – Enables or disables scanning triggered by accessing particular removable media with storage space.

Real-time file system protection checks all types of media and is triggered by various system events such as accessing a file. Using ThreatSense technology detection methods (as described in the ThreatSense engine parameter setup section), Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to more closely monitor newly created files.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each 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, press F5 to open Advanced setup and expand Detection engine > Real-time file system protection. Click ThreatSense parameter > Other and select or deselect Enable Smart optimization.

### 4.1.1.1 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.

### 4.1.1.2 Cleaning levels

Real-time protection has three cleaning levels (to access cleaning level settings, click ThreatSense engine parameter setup in the Real-time file system protection section and then click Cleaning).

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

If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (Normal cleaning), the whole archive would be deleted if all the files it contains are infected files. In \textit{Strict cleaning} mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

4.1.1.1.3 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 each tab in the window (Advanced setup > Detection engine > Real-time file system protection).

4.1.1.1.4 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from \texttt{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

4.1.1.1.5 What to do if real-time protection does not work

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

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to Setup in the main program window and click 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 make sure this option is enabled, navigate to Advanced setup (FS) and click Detection engine > Real-time file system protection.

If Real-time protection does not detect and clean infiltrations

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

Real-time protection does not start

If real-time protection is not initiated at system startup (and Enable Real-time file system protection is enabled), it may be due to conflicts with other programs. For assistance resolving this issue, please contact ESET Technical Support.
4.1.1.1.6 Processes exclusions

The Processes exclusions feature allows you to exclude application processes from Real-time file system protection. To improve backup speed, process integrity and service availability, some techniques that are known to conflict with file-level malware protection are used during backup. Similar problems can occur when attempting live migrations of virtual machines. The only effective way to avoid both situations is to deactivate Anti-Malware software. By excluding specific process (for example those of the backup solution) all file operations attributed to such excluded process are ignored and considered safe, thus minimizing interference with the backup process. We recommend that you use caution when creating exclusions – a backup tool that has been excluded can access infected files without triggering an alert which is why extended permissions are only allowed in the real-time protection module.

**Note**

Do not be confused with Excluded file extensions, HIPS exclusions or File/folder 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 via Advanced setup (F5) > Detection engine > Processes exclusions.

This feature was designed to exclude backup tools. Excluding the backup tool’s process from scanning not only ensures system stability, but it also does not affect backup performance as the backup is not slowed down while it is running.

**Example**

Click Edit to open the Processes exclusions management window, where you can Add exclusions and browse for executable file (for example Backup-tool.exe), which will be excluded from scanning.

As soon as the .exe file is added to the exclusions, activity of this process is not monitored by ESET NOD32 Antivirus and no scanning is run on any file operations performed by this process.

**Important**

If you do not use browse function when selecting process executable, you need to manually enter a full path to the executable. Otherwise, the exclusion will not work correctly and HIPS may report errors.

You can also Edit existing processes or Delete them from exclusions.

**Note**

Web access protection does not take into account this exclusion, so if you exclude the executable file of your web browser, downloaded files are still scanned. This way an infiltration can still be detected. This scenario is an example only, and we do not recommend you to create exclusions for web browsers.
4.1.1.2 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 the need to specify scan parameters. Custom scan allows you to select from predefined scan profiles designed to target specific locations, as well as choose specific scan targets.

See Scan progress for more information about the scanning process.

Scan your computer

Scan your computer allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Scan your computer is that 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 on types of cleaning, 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 scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed 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 be also initiated by clicking Custom scan, selecting Removable media from the Scan targets drop-down menu and clicking Scan.

Repeat last scan

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

You can select No action, Shutdown, or Reboot from Action after scan drop-down menu. The selected action will start after all of the running scans are finished.

Use the Action after scan drop-down menu at the bottom if you prefer to choose the action to be performed after scanning. See Advanced scan options for more details.

---

**Note**

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

---

4.1.1.2.1 Custom scan launcher

You can use the Customer Scan to scan specific parts of a disk, rather than the entire disk. To do so, click Advanced scans > Custom scan and select an option from the Scan targets drop-down menu, or select specific targets from the folder (tree) structure.

The Scan targets drop-down menu allows you to select predefined 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.
- **No selection** – Cancels all selections.

To quickly navigate to a scan target or add a target folder or file(s), enter the target directory in the blank field below the folder list. This is only possible if no targets are selected in the tree structure and the Scan targets menu is set to No selection.
You can configure cleaning parameters for the scan under Advanced setup > Detection engine > On-demand scan > ThreatSense parameters > Cleaning. To run a scan with no cleaning action, select Scan without cleaning. Scan history is saved to the scan log.

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

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

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

Scan as Administrator allows you to execute the scan under the Administrator account. 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 Administrator.

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

4.1.1.2.2 Scan progress

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

Note
It is normal that some files, such as password protected files or files being exclusively used by the system (typically pagefile.sys and certain log files), cannot be scanned. More details can be found in our Knowledgebase article.
Scan progress – The progress bar shows the status of already-scanned objects compared to objects still waiting be scanned. The scan progress status is derived from the total number of objects included in scanning.

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

Threats found – Shows the total number of scanned files, threats found and threats cleaned during a scan.

Pause – Pauses a scan.

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

Stop – Terminates the scan.

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

Note
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 Custom scan.

Action after scan – Triggers a scheduled shutdown, reboot or sleep when the computer scan finishes. Once the scan has finished, a shutdown confirmation dialog window will open with a 60 second timeout.

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

- Time of completion
- Total scanning time
- Number of threats found
- Number of scanned objects
- Scanned disk, folders and files
- Date and time of scan
- Version of detection engine
4.1.1.2.4 Malware scans

The Malware scans section is accessible from Advanced setup (F5) > Detection engine > Malware scans and provides options to select scanning parameters. This section includes the following items:

Selected profile – A particular set of parameters used by the on-demand scanner. To create a new one, click Edit next to List of profiles. See Scan profiles for more details.

Scan targets – If only want to scan a specific target, you can click Edit next to Scan targets and choose an option from drop-down menu or selecting specific targets from the folder (tree) structure. See Scan targets for more details.

ThreatSense parameters – Advanced setup options, such as file extensions you want to control, detection methods used, etc. can be found in this section. Click to open a tab with advanced scanner options.

4.1.1.2.4.1 Idle-state scan

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

Idle-state scan

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

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

Turn on the Enable logging switch in Advanced setup to record a computer scan output in the Log files section (from the main program window click Tools > Log files and select Computer scan from the Log drop-down menu).

Idle-state detection

See Idle state detection triggers for a full list of conditions that must be met in order to trigger the idle-state scanner.

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

4.1.1.2.4.2 Scan profiles

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

To create a new profile, open the Advanced setup window (F5) and click Detection engine > Malware scans > On-demand scan > List of profiles. The Profile manager window includes the Selected profile drop-down menu that lists existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

Note

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

The **Scan targets** drop-down menu allows you to select predefined 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.
- **No selection** – Cancels all selections.

4.1.1.2.4.4 Advanced scan options

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

- **Shut down** – The computer turns off after a scan finishes.
- **Reboot** – Closes all open programs, and restarts the computer after a scan finishes.
- **Sleep** – Saves your session and puts the computer in a low-power state so that you can quickly resume working.
- **Hibernate** – Takes everything you have running on RAM and moves it to a special file on your hard drive. Your computer shuts down, but will resume its previous state the next time you start it.
- **No action** – After a scan finishes, no action will be performed.

**Note**

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

Select **Action cannot be canceled by user** to deny non-privileged users the ability to stop actions taken after scanning.

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

See also the **Scan progress** chapter.

4.1.1.3 Startup scan

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

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

For detailed instructions about Scheduler task creation and management, see **Creating new tasks**.
4.1.1.3.1 Automatic startup file check

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

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

- All registered files (most files scanned)
- Rarely used files
- Commonly used files
- Frequently used files
- Only the most frequently used files (least files scanned)

Two specific groups are also included:

- Files run before user logon – Contains files from locations that may be accessed without the user being logged in (includes almost all startup locations such as services, browser helper objects, winlogon notify, Windows scheduler entries, known dll’s, etc.).
- Files run after user logon - Contains files from locations that may only be accessed after a user has logged in (includes files that are only run by a specific user, typically files in HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run).

Lists of files to be scanned are fixed for each aforementioned group.

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

- When idle – the task will be performed only when the system is idle,
- Lowest – when the system load is the lowest possible,
- Lower – at a low system load,
- Normal – at an average system load.

4.1.1.4 Exclusions

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

You can add files and folder to be excluded from scanning into the list of exclusions via Advanced setup (F5) > Detection engine > Exclusions > Files and folders to be excluded from scanning > Edit.

**Note**

Do not be confused with Excluded file extensions, File/folder exclusions or Processes exclusions.

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

### Columns

- **Path** – Path to excluded files and folders.
- **Threat** – If there is a name of a threat next to an excluded file, it means that the file is only excluded for the given threat, not completely. If that file becomes infected later with other malware, it will be detected by the antivirus module. This type of exclusion can only be used for certain types of infiltrations and it can be created either in the threat alert window reporting the infiltration (click **Show advanced options** and then select **Exclude from detection**), or by clicking **Tools > Quarantine** and then right-clicking the quarantined file and selecting **Restore and exclude from detection** from the context menu.

### Control elements

- **Add** – Excludes objects from detection.
- **Edit** – Enables you to edit selected entries.
- **Delete** – Removes selected entries.

#### 4.1.1.4.1 Add or Edit exclusion

This dialog window enables you to add or edit exclusions. Choose the exclusion type from the **Type** drop-down menu:

- **Exclude path**
  
  Excludes specific threats or a specific path for this computer. You are not able to create exclusion when both settings are enabled.

- **Exclude threat**
  
  Exclusions apply to **Potentially unwanted applications**, potentially unsafe applications and suspicious applications.
Exclude hash

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

You can use wildcards to cover a group of files. A question mark (?) represents a single variable character whereas an asterisk (*) represents a variable string of zero or more characters. If using the first method, wildcards described in the Exclusion format section can be used.

**Example**

- If you want to exclude all files in a folder, type the path to the folder and use the mask `*. *`.
- To exclude an entire drive including all files and subfolders, use the mask `D:\*`.
- 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 (and characters vary) and you only know the first one for sure (say “D”), use the following format: `D?????.exe` (question marks replace the missing / unknown characters).

**Example**

If you want to exclude a threat, enter valid threat name in the following format:

- `@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt`  
- `@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan`  
- `@NAME=Win32/Bagle.D@TYPE=worm`

**Example**

A few more exclusion examples using an asterisk:

- `C:\Tools` - will be automatically converted to `C:\Tools\*.*`
- `C:\Tools\*.dat` - will exclude dat files in the Tools folder
- `C:\Tools\sg.dat` - will exclude this particular file located in the exact path

4.1.1.4.2 Exclusion format

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

**Examples**

- If you wish to exclude all files in a folder, type the path to the folder and use the mask “*. *”.
- To exclude an entire drive including all files and subfolders, use the mask “D:\*”.
- 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 (and characters vary) and you only know the first one for sure (say “D”), use the following format: “D?????.exe”. Question marks replace the missing (unknown) characters.
4.1.1.5 ThreatSense parameters

ThreatSense is comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window, click ThreatSense parameters in the Advanced setup window for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

ThreatSense parameters are highly optimized for each module, their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section allows you to define which computer components and files will be scanned for infiltrations.

- Operating memory – Scans for threats that attack the operating memory of the system.
- Boot sectors/UEFI – Scans boot sectors for the presence of viruses 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 virus signatures database. 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 the scanner while cleaning infected files. There are 3 levels of cleaning:

**No cleaning** – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

**Normal cleaning** – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification in the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.

**Strict cleaning** – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

**Warning**

If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (Normal cleaning), the whole archive would be deleted if all the files it contains are infected files. In **Strict cleaning** mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters setup for a On-demand computer scan, the following options in Other section are also available:

**Scan alternate data streams (ADS)** – Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

**Run background scans with low priority** – Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

**Log all objects** – If this option is selected, the log file will show all the scanned files, even those not infected. For example, if an infiltration is found within an archive, the log will list also clean files contained within the archive.

**Enable Smart optimization** – With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

**Preserve last access timestamp** – Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

**Limits**

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:
Object settings

**Maximum object size** – Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: *unlimited*.

**Maximum scan time for object (sec.)** – Defines the maximum time value for scanning of an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished. Default value: *unlimited*.

Archive scan setup

**Archive nesting level** – Specifies the maximum depth of archive scanning. Default value: *10*.

**Maximum size of file in archive** – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: *unlimited*.

---

**Note**

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

---

### 4.1.1.5.1 Cleaning

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning.

### 4.1.1.5.2 File extensions excluded from scanning

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

---

**Note**

Do not 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.

---

**Example**

To add a new extension to the list, click Add. Type the extension into the blank field (for example tmp) and click OK. When you select Enter multiple values, you can add multiple file extensions delimited by lines, commas or semicolons (for example, choose Semicolon from drop-down menu as a separator, and type edb; eml; tmp).

You can use a special symbol ? (question mark). The question mark represents any symbol (for example ?db).

---

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

4.1.1.6 An infiltration is detected

Infiltrations can reach the system from various entry points such as webpages, shared folders, via email or from removable devices (USB, external disks, CDs, DVDs, diskettes, 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 more information about cleaning levels and behavior, see Cleaning.
Cleaning and deleting

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

![Threat found]

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

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

**Multiple threats**

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

### 4.1.1.7 Removable media

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

**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). If **Show scan options** is selected, a notification will display which allows you to choose a desired action:

- **Do not scan** – No action will be performed and the New device detected window will be closed.
- **Automatic device scan** – An on-demand computer scan of the inserted removable media device will be performed.
- **Show scan options** – Opens the Removable media setup section.

When a removable media is inserted, following dialog will shown:

![New device detected](image)

**Scan now** – This will trigger scan of removable media.

**Scan later** – Scan of removable media will be postponed.

**Setup** – Opens the Advanced setup.

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

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

### 4.1.1.8 Document protection

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

To activate Document protection, open the Advanced setup window (press **F5**) > Detection engine > Malware scans > Document protection and click the Integrate into system switch.

---

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

### 4.1.2 Device control and Webcam protection

#### Device control

ESET NOD32 Antivirus provides automatic device (CD/DVD/USB/...) control. This module allows you to 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 the use of devices containing unsolicited content.

**Supported external devices:**

- Disk Storage (HDD, USB removable disk)
- CD/DVD
- USB Printer
- FireWire Storage
- Bluetooth Device
- Smart card reader
- Imaging Device
- Modem
- LPT/COM port
- Portable Device
- All device types

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

Turning the switch on next to **Integrate into system** activates the Device control feature in ESET NOD32 Antivirus; you will need to restart your computer for this change to take effect. Once Device control is enabled, the **Rules** will become active, allowing you to open the **Rules editor** window.

**Note**

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

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.
4.1.2.1 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.

Particular 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 log severity.

Click Add or Edit to manage a rule. Click Copy to create a new rule with predefined options used for another selected rule. XML strings displayed when clicking a rule can be copied to the clipboard to help system administrators to 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 don't wish to delete a rule permanently in case you wish to use it in the future.

The control is accomplished by rules that are sorted in the order determining their priority, with higher priority rules on top.

Log entries can be viewed from the main window of ESET NOD32 Antivirus in Tools > Log files.

The Device control log records all occurrences where Device control is triggered.

4.1.2.1.1 Detected devices

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

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

Warning
Device connected to your computer may pose a security risk.

The Device groups window is divided into two parts. The right part of the window contains a list of devices belonging to respective group and the left part of the window contains created groups. Select a group with a list of devices you want to display in the right pane.

When you open the Device groups window and select a group, you can add or remove devices from the list. Another way to add devices to the group is to import them from a file. Alternatively, you can click Populate button and all devices connected to your computer will be listed in the Detected devices window. Select a devices from the populated list to add it to the group by clicking OK.

Control elements

- **Add** – You can add a group by entering its name, or a device to existing group (optionally, you can specify details such as vendor name, model and serial number) depending on which part of the window you clicked the button.
- **Edit** – Lets you modify the name of selected group or device's parameters (vendor, model, serial number).
- **Remove** – Deletes selected group or device depending on which part of the window you clicked on the button.
- **Import** – Imports a list of devices from a file.

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

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

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

Note that not all Actions (permissions) are available for all device types. If it is a device of storage type, all four Actions are available. For non-storage devices, there are only three Actions available (for example Read Only is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).
4.1.2.3 Adding Device control rules

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

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

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

- **Read/Write** – Full access to the device will be allowed.
- **Block** – Access to the device will be blocked.
- **Read Only** – Only read access to the device will be allowed.
- **Warn** – Each time that a device is connected, the user will be notified if it is allowedblocked, and a log entry will be made. Devices are not remembered, a notification will still be displayed upon subsequent connections of the same device.

Note that not all Actions (permissions) are available for all device types. If it is a device of storage type, all four Actions are available. For non-storage devices, there are only three Actions available (for example **Read Only** is not available for Bluetooth, therefore Bluetooth devices can only be allowed, blocked or warned).
Criteria type – Select Device group or Device.

Additional parameters shown below can be used to fine-tune rules and tailor them to devices. All parameters are case-insensitive:

- **Vendor** – Filter by vendor name or ID.
- **Model** – The given name of the device.
- **Serial** – External devices usually have their own serial numbers. In the case of a CD/DVD, this is the serial number of the given media, not the CD drive.

Note

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

Note

To view information about a device, create a rule for that type of device, connect the device to your computer and then check the device details in the Device control log.

Logging severity

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.

Rules can be limited to certain users or user groups by adding them to the **User list**:

- **Add** – Opens the **Object types: Users or Groups** dialog window that allows you to select desired users.
- **Remove** – Removes the selected user from the filter.

Note

All devices can be filtered by user rules, (for example imaging devices do not provide information about users, only about actions).

4.1.3 Host-based Intrusion Prevention System (HIPS)

Warning

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

The Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.
HIPS settings can be found under **Advanced setup** (F5) > **Detection engine** > **HIPS** > **Basic**. The HIPS state (enabled/disabled) is shown in the ESET NOD32 Antivirus main program window, under **Setup** > **Computer protection**.

![Advanced setup settings](image)

**Basic**

**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 kernel protection (this option is available in Windows 8.1 and Windows 10).

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

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

**Deep Behavioral Inspection**

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

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

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

HIPS settings

Filtering mode can be performed in one of four modes:

- Automatic mode – Operations are enabled with the exception of those blocked by pre-defined rules that protect your system.
- Smart mode – The user will only be notified about very suspicious events.
- Interactive mode – User will be prompted to confirm operations.
- Policy-based mode – Operations are blocked.

Learning mode – Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the Rule 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 HIPS 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.

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 rule management window. 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.

4.1.3.1 HIPS interactive window

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

Rules created from the notification window are considered to be equivalent to rules created manually. A rule created from a notification window can be less specific than the rule that triggered that dialog window. This means that after creating a rule in the dialog box, the same operation can trigger the same window. For more information see Priority for HIPS rules.

If the default action for a rule is set to Ask every time, a dialog window will be displayed each time that the rule is triggered. You can choose to Deny or Allow the operation. If you do not choose an action in the given time, a new action is selected based on the rules.

Remember until application quits causes the action (Allow/Deny) to be used until a change of rules or filtering mode, a HIPS module update or a system restart. After any of these three actions, temporary rules will be deleted.

The Create rule and remember permanently option will create a new HIPS rule which can be later altered in the HIPS rule management section (requires administration privileges).

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

Settings for the more detailed rule parameters can be accessed by clicking Advanced options. The options below are available if you 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.
Endless HIPS notifications?
To stop the notifications from appearing, change the filtering mode to **Automatic mode** in **Advanced setup** (F5) > **Detection engine** > **HIPS** > **Basic**.
4.1.3.1 Potential ransomware behavior detected

This interactive window will appear when potential ransomware behavior is detected. You can choose to Deny or Allow the operation.

Click Details to view specific detection parameters. The dialog window allows you Submit for analysis or Exclude from detection.

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

4.1.3.2 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 chapter. See also General principle of HIPS.

Columns
- **Rule** – User-defined or automatically chosen rule name.
- **Enabled** – Deactivate this switch 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.
- **Log** – If you activate this option, information about this rule will be written to the HIPS log.
- **Notify** – A small pop-up 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.
Remove – 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)

4.1.3.2.1 HIPS rule settings

See HIPS rule management as first.

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

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

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

Enabled – Disable this switch if you want to keep the rule in the list but not apply it.

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

Notify user – A small pop-up window appears in the lower-right corner if an event is triggered.

The rule consists of parts that describe the conditions triggering this rule:

Source applications – The rule will be used only if the event is triggered by this application(s). Select Specific applications from drop-down menu and click Add to add new files or you can select All applications from the drop-down menu to add all applications.

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

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.

Note

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

Descriptions of important operations:
File operations

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

Application operations

- **Debug another application** – Attaching a debugger to the process. While debugging an application, many details of its behavior can be viewed and modified and its data can be accessed.
- **Intercept events from another application** – The source application is attempting to catch events targeted at a specific application (for example a keylogger trying to capture browser events).
- **Terminate/suspend another application** – Suspending, resuming or terminating a process (can be accessed directly from Process Explorer or the Processes pane).
- **Start new application** – Starting of new applications or processes.
- **Modify state of another application** – The source application is attempting to write into the target applications’ memory or run code on its behalf. This functionality may be useful to protect an essential application by configuring it as a target application in a rule blocking the use of this operation.

Note

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

Registry operations

- **Modify startup settings** – Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for the `Run` key in the Windows Registry.
- **Delete from registry** – Deleting a registry key or its value.
- **Rename registry key** – Renaming registry keys.
- **Modify registry** – Creating new values of registry keys, changing existing values, moving data in the database tree or setting user or group rights for registry keys.

Note

You can use wildcards with certain restrictions when entering a target. Instead of a particular 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 (*).

Warning

If you create a very generic rule, the warning about this type of rule will be shown.

In the following example, we will demonstrate how to restrict unwanted behavior of a specific application:
1. Name the rule and select **Block** (or **Ask** if you prefer to choose later) from the **Action** drop-down menu.
2. Enable the **Notify user** switch to display a notification any time that a rule is applied.
3. Select **at least one operation** in the **Operations affecting** section for which the rule will be applied.
4. Click **Next**.
5. In the **Source applications** window, select **Specific applications** from the drop-down menu to apply your new rule to all applications attempting to perform any of the selected application operations on the applications you specified.
6. Click **Add** and then ... to choose a path to a specific application and then press **OK**. Add more applications if you prefer.
   For example: `C:\Program Files (x86)\Untrusted application\application.exe`
7. Select the **Write to file** operation.
8. Select **All files** from the drop-down menu. This will block any attempts to write to any files by the selected application(s) from the previous step.
9. Click **Finish** to save your new rule.

**4.1.3.2.2 Add application/registry path for HIPS**

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

The **Run RegEdit...** option will start the Windows registry editor (regedit). While adding a registry path, enter 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`
4.1.3.3 HIPS exclusions
Exclusions enable you to exclude processes from HIPS Deep Behavioral Inspection.

**Note**
Do not be confused with Excluded file extensions, File/folder exclusions or Processes exclusions.

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

4.1.3.4 HIPS advanced setup
The following options are useful for debugging and analyzing an application’s behavior:

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

**Log all blocked operations** — All blocked operations will be written to the HIPS log.

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

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

- **Add** — Adds a new driver.
- **Edit** — Edits a selected driver.
- **Remove** — Removes a driver from the list.
- **Reset** — Reloads a set of system drivers.

**Note**
Click Reset if you do not want drivers that you have added manually to be included. This can be useful if you have added several drivers and you cannot delete them from the list manually.

4.1.4 Gamer mode
Gamer mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. 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 under Advanced setup (FS) > 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.
4.2 Internet protection

Web and email configuration can be found in the Setup pane by clicking Internet protection. From here you can access more detailed program settings.

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

Click to open web/email/anti-phishing protection settings in Advanced setup.

Email client protection provides control of email communications received through POP3 and IMAP protocols. Using the plug-in program for your email client, ESET NOD32 Antivirus provides control of all communications to and from your email client (POP3, MAPI, IMAP, HTTP).

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

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

4.2.1 Protocol filtering

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

Enable application protocol content filtering – Can be used to disable protocol filtering. Note that many ESET NOD32 Antivirus components (Web access protection, Email protocols protection, Anti-Phishing, Web control) depend on this and will be non-functional without it.

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

### 4.2.1.1 Web and email clients

**Note**

Starting with Windows Vista Service Pack 1 and Windows Server 2008, the new Windows Filtering Platform (WFP) architecture is used to check network communication. Since the WFP technology uses special monitoring techniques, the **Web and email clients** section is not available.

Because of the enormous amount of malicious code circulating the Internet, safe Internet browsing is a very important aspect of computer protection. Web browser vulnerabilities and fraudulent links help malicious code enter the system unnoticed which is why ESET NOD32 Antivirus focuses on web browser security. Each application accessing the network can be marked as an Internet browser. The check box is two-state:

- **Deselected** – Communication of applications is filtered only for specified ports.
- **Selected** – Communication is always filtered (even if a different port is set).

### 4.2.1.2 Excluded applications

To exclude communication of specific network-aware applications from content filtering, select them in the list. HTTP/POP3/IMAP 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 checked.

Running applications and services will be available here automatically. Click **Add** to add an application manually if it is not shown on the protocol filtering list.
4.2.1.3   Excluded IP addresses

The entries in the list will be excluded from protocol content filtering. HTTP/POP3/IMAP communication from/to the selected addresses will not be checked for threats. We recommend that you only use this option for addresses that are known to be trustworthy.

Click **Add** to exclude an IP address/address range/subnet of a remote point not shown on the protocol filtering list.

Click **Delete** to remove the selected entries from the list.

### 4.2.1.3.1   Add IPv4 address

This allows you to add an IP address/address range/subnet of a remote point to which a rule is applied. Internet Protocol version 4 is the older but still the most widely used.

**Single address** – Adds the IP address of an individual computer for which the rule is to be applied (for example 192.168.0.10).

**Address range** – Enter the starting and ending address IP address to specify the IP range (of several computers) for which the rule is to be applied (for example 192.168.0.1 to 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 192.168.1.0/24 prefix, that means 192.168.1.1 to 192.168.1.254 address range.

### 4.2.1.3.2   Add IPv6 address

This allows you to add an IPv6 address/subnet of a remote point for which the rule is applied. It is the newest version of the Internet protocol and will replace the older version 4.

**Single address** – Adds the IP address of an individual computer for which the rule is to be applied (for example 2001:718:1c01:16:214:22ff:fe9:ca5).

**Subnet** – Subnet (a group of computers) is defined by an IP address and mask (for example: 2002:c0a8:6301:1::1/64).
4.2.1.4 SSL/TLS

ESET NOD32 Antivirus is capable of checking for threats in communications that use the SSL protocol. You can use various scanning modes to examine SSL protected communications with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Enable SSL/TLS protocol filtering – If protocol filtering is disabled, the program will not scan communications over SSL.

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

- **Automatic mode** – Default mode will only scan appropriate applications such as web browsers and email clients. You can override it by selecting applications for which their communications will be scanned.

- **Interactive mode** – If you enter a new SSL protected site (with an unknown certificate), an action selection dialog is displayed. This mode allows you to create a list of SSL certificates / applications that will be excluded from scanning.

- **Policy mode** – Select this option to scan all SSL protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked as trusted (it is on the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.

**List of SSL filtered applications** – Allows you to customize ESET NOD32 Antivirus behavior for specific applications.

**List of known certificates** – Allows you to customize ESET NOD32 Antivirus behavior for specific SSL certificates.

**Exclude communication with trusted domains** – When enabled, communication with trusted domains will be excluded from checking. Domain trustiness is determined by built-in whitelist.

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

**Root certificate**

- **Add the root certificate to known browsers** – 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 root certificate to known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (for example, in Internet Explorer).

  To apply the certificate to unsupported browsers, click View Certificate > Details > Copy to File... and manually import it into the browser.

**Certificate validity**

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

- **If the certificate is invalid or corrupt** – This means that the certificate expired or was incorrectly signed. In this case, we recommend that you leave **Block communication that uses the certificate** selected.
4.2.1.4.1 Certificates

For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for
ESET be added to the list of known root certificates (publishers). Add the root certificate to known browsers should
be enabled. Select this option to automatically add the ESET root certificate to the known browsers (for example,
Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (e.g.
Internet Explorer). To apply the certificate to unsupported browsers, click View Certificate > Details > Copy to File...
and then manually import it into the browser.

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

You can select Block communication that uses the certificate to always terminate an encrypted connection to the
site that uses the unverified certificate.

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

4.2.1.4.1.1 Encrypted network traffic

If the computer is configured for SSL protocol scanning, a dialog window prompting you to choose an action may be
opened when there is an attempt to establish encrypted communication (using an unknown certificate).

The dialog window contains the following information:

- name of the application that initiated the communication
- name of the certificate used
- action to perform - whether to scan the encrypted communication and whether to remember the action for
  the application / certificate

If the certificate is not located in the Trusted Root Certification Authorities store (TRCA), it is considered untrusted.

4.2.1.4.2 List of known certificates

The List of known certificates can be used to customize ESET NOD32 Antivirus behavior for specific SSL certificates,
and to remember actions chosen if Interactive mode is selected in SSL/TLS protocol filtering mode. The list can be
viewed and edited in Advanced setup (F5) > Web and email > SSL/TLS > List of known certificates.

The List of known certificates window consists of:

Columns

Name – Name of the certificate.
Certificate issuer – Name of the certificate creator.
Certificate subject – The subject field identifies the entity associated with the public key stored in the subject
public key field.
Access – Select Allow or Block as the Access action to allow/block communication secured by this certificate
regardless of its trustworthiness. Select Auto to allow trusted certificates and ask for untrusted ones. Select Ask
to always ask user what to do.
Scan – Select Scan or Ignore as the Scan action to scan or ignore communication secured by this certificate.
Select Auto to scan in automatic mode and ask in interactive mode. Select Ask to always ask the user what to do.
Control elements

Add – 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.

Remove – 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.

4.2.1.4.3 List of SSL/TLS filtered applications

The List of SSL/TLS filtered applications can be used to customize ESET NOD32 Antivirus behavior for specific applications, and to remember actions chosen if Interactive mode is selected in SSL/TLS protocol filtering mode. The list can be viewed and edited in Advanced setup (F5) > Web and email > SSL/TLS > List of SSL/TLS filtered applications.

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

Columns

Application – Name of the application.

Scan action – Select Scan or Ignore to scan or ignore communication. Select Auto to scan in automatic mode and ask in interactive mode. Select Ask to always ask the user what to do.

Control elements

Add – Add filtered application.

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

Remove – 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.

4.2.2 Email client protection

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, integration can be enabled in ESET NOD32 Antivirus. When integrated into your email client, the ESET NOD32 Antivirus toolbar is inserted directly into the email client (the toolbar for newer versions of Windows Live Mail is not inserted), for more efficient email protection.

Integration settings are located under Advanced setup (F5) > Web and email > Email client protection > Email clients.

Email client integration

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.

Even if integration is not enabled, email communication is still protected by the email client protection module (POP3, IMAP).

Turn on Disable checking upon inbox content change if you experience system slowdown when working with Microsoft Outlook. This can occur when retrieving email from the Kerio Outlook Connector store.
Email to scan

Enable email protection by client plugins – When email client protection by email client is disabled, email client protection by protocol filtering will be still enabled.
Received email – Toggles checking of received messages.
Sent email – Toggles checking of sent messages.
Read email – Toggles checking of read messages.

Action to be performed on infected email

No action – If enabled, the program will identify infected attachments, but will leave emails without taking any action.
Delete email – The program will notify the user about infiltration(s) and delete the message.
Move email to the Deleted items folder – Infected emails will be moved automatically to the Deleted items folder.
Move email to folder (default action) – Infected emails will be moved automatically to the specified folder.
Folder – Specify the custom folder where you want to move infected emails when detected.
Repeat scan after update – Toggles rescanning after a detection engine update.
Accept scan results from other modules – If this is selected, the email protection module accepts scan results of other protection modules (POP3, IMAP protocols scanning).

Note
We recommend that you enable Enable email protection by client plugins and Enable email protection by protocol filtering. These settings are located under Advanced setup (F5) > Web and email > Email client protection > Email protocols).

4.2.2.1 Email protocols

The IMAP and POP3 protocols are the most widespread protocols used to receive email communication in an email client application. The Internet Message Access Protocol (IMAP) is another Internet protocol for email retrieval. IMAP has some advantages over POP3, for example, multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. ESET NOD32 Antivirus provides protection for these protocols regardless of the email client used, and without requiring re-configuration of the email client.

The protection module providing this control is automatically initiated at system startup and is then active in memory. IMAP protocol control is performed automatically without the need to reconfigure the email client. By default, all communication on port 143 is scanned, but other communication ports can be added if necessary. Multiple port numbers must be delimited by a comma.

You can configure IMAP/IMAPS and POP3/POP3S protocol checking in Advanced setup. To access this setting, expand Web and email > Email client protection > Email protocols.

Enable email protection by protocol filtering – Enables checking of email protocols.

In Windows Vista and later, IMAP and POP3 protocols are automatically detected and scanned on all ports. In Windows XP, only the configured Ports used by the IMAP/POP3 protocol are scanned for all applications, and all ports are scanned for applications marked as Web and email clients.

ESET NOD32 Antivirus also supports the scanning of IMAPS and POP3S 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. The program will only scan traffic on ports defined in Ports used by IMAPS/POP3S protocol, regardless of operating system version.

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

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

After an email has been checked, a notification with the scan result can be appended to the message. You can elect to Append tag messages to received and read email, Append note to the subject of received and read infected 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.
- **To infected email only** – Only messages containing malicious software will be marked as checked (default).
- **To all scanned email** – The program will append messages to all scanned email.

**Append note to the subject of sent infected email** – Disable this if you do not want email protection to include a virus warning in the subject of an infected email. This feature allows for simple, subject-based filtering of infected emails (if supported by your email program). It also increases the level of credibility for the recipient. If an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

**Template added to the subject of infected email** – Edit this template if you wish to modify the subject prefix format of an infected email. This function will replace the message subject “Hello” to the following format: “[virus DETECTION NAME] Hello”. The variable %VIRUSNAME% represents the detection.
4.2.2.3 Integration with email clients

Integration of ESET NOD32 Antivirus with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, integration can be enabled in ESET NOD32 Antivirus. When integration is activated, the ESET NOD32 Antivirus toolbar is inserted directly into the email client, allowing for more efficient email protection. Integration settings are available through Setup > Advanced setup > Web and email > Email client protection > Email clients.

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. For a complete list of supported email clients and their versions, refer to the following ESET Knowledgebase article.

Select the check box next to Disable checking upon inbox content change if you are experiencing a system slowdown when working with your email client. This can occur when retrieving email from the Kerio Outlook Connector Store.

Even if integration is not enabled, email communication is still protected by the email client protection module (POP3, IMAP).

4.2.2.3.1 Email client protection configuration

The Email client protection module supports the following email clients: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner.

4.2.2.4 POP3, POP3S filter

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET NOD32 Antivirus provides protection for this protocol regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. For the module to work correctly, please make sure it is enabled – POP3 protocol checking is performed automatically without requiring re-configuration of the email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Multiple port numbers must be delimited by a comma.

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

In this section, you can configure POP3 and POP3S protocol checking.

Enable POP3 protocol checking – If enabled, all traffic through POP3 is monitored for malicious software.

Ports used by POP3 protocol – A list of ports used by the POP3 protocol (110 by default).

ESET NOD32 Antivirus also supports POP3S protocol checking. This type of communication uses an encrypted channel to transfer information between server and client. ESET NOD32 Antivirus checks communications utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) encryption methods.

Do not use POP3S checking – Encrypted communication will not be checked.

Use POP3S protocol checking for selected ports – Check this option to enable POP3S checking only for ports defined in Ports used by POP3S protocol.

Ports used by POP3S protocol – A list of POP3S ports to check (995 by default).
4.2.3 Web access protection

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

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

We strongly recommend that Web access protection is enabled. This option can be accessed from the main window of ESET NOD32 Antivirus by navigating to **Setup > Internet protection > Web access protection**.

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

- **Web protocols** – enables you to configure monitoring for these standard protocols which are used by most Internet browsers.

- **URL address management** – enables you to specify HTTP addresses to block, allow or exclude from checking.

- **ThreatSense parameters** – Advanced virus scanner setup – enables you to configure settings such as types of objects to scan (emails, archives, etc.), detection methods for Web access protection etc.

### 4.2.3.1 Basic

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

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

Note

We strongly recommend you leave Web access protection enabled.
4.2.3.2 Web protocols

By default, ESET NOD32 Antivirus is configured to monitor the HTTP protocol used by most Internet browsers.

HTTP Scanner setup

In Windows Vista and later, HTTP traffic is always monitored on all ports for all applications. In Windows XP, you can modify the Ports used by HTTP protocol in Advanced setup (F5) > Web and email > Web access protection > Web protocols. HTTP traffic is monitored on the specified ports for all applications, and on all ports for applications marked as Web and email clients.

HTTPS Scanner setup

ESET NOD32 Antivirus also supports HTTPS protocol checking. HTTPS communication 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.

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

4.2.3.3 URL address management

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

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 checking are not scanned for malicious code when accessed.

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

If you add a URL address to the List of addresses excluded from filtering, the address will be excluded from scanning. You can also allow or block certain addresses by adding them to the List of allowed addresses or List of blocked addresses.

If you want to block all HTTP addresses except addresses present in the active List of allowed addresses, add * to the active List of blocked addresses.

The special symbols * (asterisk) and ? (question mark) can be used in lists. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list. See Add HTTP address / domain mask for how a whole domain including all subdomains can be matched safely. To activate a list, select List active. If you want to be notified when entering an address from the current list, select Notify when applying.

Block or allow specific file extensions

URL address management also allows you to block or allow the opening of specific file types during internet browsing. For example, if you do not want executable files to be opened, select the list where you want to block these files from the drop-down menu and then enter the mask "**.exe".
Control elements

Add – Creates a new list in addition to the predefined ones. This can be useful if you want to logically split different groups of addresses. For example, one list of blocked addresses may contain addresses from an external public blacklist, and a second one may contain your own blacklist, making it easier to update the external list while keeping yours intact.

Edit – Modifies existing lists. Use this to add or remove addresses.

Delete – Deletes existing lists. Only available for lists created with Add, not for default lists.

4.2.3.3.1 URL addresses list

In this section you can specify lists of HTTP addresses that will be blocked, allowed or excluded from checking.

By default, the following three lists are available:

- **List of addresses excluded from checking** – 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.
Block a website example

The following ESET Knowledgebase article may not be available in your language (except English):

- Block a website using ESET Windows home products

For more information see URL address management.

4.2.3.3.2 Create new URL address list

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

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

Address list type – Three list types are available:

- Excluded from checking – No checking for malicious code will be performed for any address added to this list.
- Blocked – The user will not be allowed to access addresses specified in this list.
- Allowed – If the Allow access only to HTTP addresses in the list of allowed addresses option is enabled and the list of blocked addresses contain * (match everything), user will be allowed to access addresses specified in this list only. The addresses in this list are allowed even if they also match by the list of blocked addresses.

List name – Specify the name of the list. This field will be grayed out when editing one of the three predefined lists.

List description – Type a short description for the list (optional). Will be grayed when editing one of three predefined list.

To activate a list, select List active next to that list. If you want to be notified when a particular list is used in evaluation of an HTTP site that you visited, select Notify when applying. For example, a notification will be issued if 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 containing the specified website.

Control elements

- Add – Add a new URL address to the list (enter multiple values with separator).
- Edit – Modifies existing address in the list. Only possible for addresses created with Add.
- Remove – Deletes existing addresses in the list. Only possible for addresses created with Add.
Import – Import a file with URL addresses (separate values with a line break, for example * .txt using encoding UTF-8).

### 4.2.3.3 How to add URL mask

Please refer to the instructions in this dialog before you enter 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 allows user to specify addresses, which should be excluded from checking. If the complete name of the remote server is unknown, or the user wishes to specify a whole group of remote servers, so called masks can be used to identify such a group. The masks include the symbols “?” and “*”:

- use ? to substitute a symbol
- use * to substitute a text string.

For example * .c?m applies to all addresses, where the last part begins with the letter c, ends with the letter m and contains an unknown symbol in between them (.com, .cam, etc.)

A leading "*. " sequence is treated specially if used at the beginning of domain name. First, the * wildcard does not match the slash character ('/') in this case. This is to avoid circumventing the mask, for example the mask *. domain.com will not match http://anydomain.com/anypath#.domain.com (such suffix can be appended to any URL without affecting the download). And second, the "*. " also matches an empty string in this special case. This is to allow matching whole domain including any subdomains using a single mask. For example the mask *. domain.com also matches http://domain.com. Using *domain.com would be incorrect, as that would also match http://anotherdomain.com.

### 4.2.4 Anti-Phishing protection

The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this activity in the glossary. ESET NOD32 Antivirus includes anti-phishing protection, which blocks web pages known to distribute this type of content.

We strongly recommend that you enable Anti-Phishing in ESET NOD32 Antivirus. To do so, open Advanced setup (F5) and navigate to Web and email > Anti-Phishing protection.

Visit our Knowledgebase article for more information on Anti-Phishing protection in ESET NOD32 Antivirus.

### Accessing a phishing website

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

Potential phishing websites that have been whitelisted will expire after several hours by default. To allow a website permanently, use the URL address management tool. From Advanced setup (F5) expand Web and email > Web access protection > URL address management > Address list, click Edit and then add the website that you want to edit to the list.

Phishing site reporting

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

Note

Before submitting a website to ESET, make sure it meets one or more of the following criteria:

- the website is not detected at all,
- the website is incorrectly detected as a threat. In this case, you can Report an incorrectly blocked page.

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.).
4.3 Updating the program

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 enter your License key to activate your product in order to access ESET update servers while updating.

**Note**

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 detect 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**.

---

**Important**

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 key has been incorrectly entered in update setup. We recommend checking that your license key was entered correctly. The Advanced setup window (click **Setup** from the main menu and then click **Advanced setup**, or press the F5 key on your keyboard) contains additional update options. Click **Help and support > Change license** from the main menu to enter a new license key.

2. **An error occurred while downloading update files** – 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, it is likely that an Internet connection is not established or there are connectivity problems with your computer. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.
Important

We recommend restarting your computer after a successful ESET NOD32 Antivirus update to a newer product version to ensure that all program modules were updated correctly. It is not necessary to restart your computer after regular modules updates.

Note

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

4.3.1 Update settings

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

Basic

The update profile that is currently in use (unless a specific one is set under Advanced setup > Firewall > Known networks) is displayed in the Select default update profile drop-down menu.

Automatic profile switching – Allows you to change the profile for specific network.

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

Module rollback

If you suspect that a new update of the virus database and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely.
ESET NOD32 Antivirus records snapshots of detection engine and program modules for use with the rollback feature. In order to create virus database snapshots, leave the Create snapshots of modules switch enabled. The Number of locally stored snapshots field defines the number of previous virus database snapshots stored.

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

Advanced setup

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, enter your own Profile name and then click Add.

Updates

By default, the Update type is set to Regular update to ensure that update files will automatically be download from the ESET server with the least network traffic. Pre-release updates (the Pre-release update option) are updates that have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times and SHOULD NOT be used on production servers and workstations where maximum availability and stability is required.

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 notification if the update file size is greater than specified value.
Disable notification about successful update – Turns off the system tray notification at the bottom right corner of the screen. It is useful to select this option if a full screen application or a game is running. Please note that Gamer mode will turn off all notifications.

Module updates

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

Program component update

Application update – A confirmation dialog will be displayed if reinstallation is needed.

4.3.1 Advanced update setup

Advanced update setup options include the configuration of Update mode, HTTP Proxy.

4.3.1.1 Update mode

The Update mode tab contains options related to regular program updates. These settings enable you to predefine program behavior when new version of detection engine or program component updates are available.

Program component updates include new features or makes changes to features from previous versions, and are included as part of regular (detection engine) updates. After a program component update has been installed, a computer restart may be required.

The following settings are available:

Application update – When enabled, each program component upgrade will be performed automatically and silently without full product upgrading.

Enable manual program component update – By default disabled. When enabled and newer version of ESET NOD32 Antivirus is available, you can check for updates in Update pane and install the newer version.

Ask before downloading update – When this option is active, a notification will be displayed and you will be asked to confirm the installation of any available updates before they are installed.

Ask if an update file is greater than (kB) – If the update file is larger than the size specified here, a notification will be displayed and you will be asked to confirm the installation of any available updates before they are installed.

4.3.1.2 Connection options

To access the proxy server setup options for a given update profile, click Update in the Advanced setup tree (F5) and then click Profiles > Updates > Connection options. Click the Proxy mode drop-down menu and select one of the three following options:

- Do not use proxy server
- Connection through a proxy server
- Use global proxy server settings

Select Use global proxy server settings to use the proxy server configuration options already specified in the Tools > Proxy server branch of the Advanced setup tree.

Select Do not use proxy server to specify that no proxy server will be used to update ESET NOD32 Antivirus.
Connection through a proxy server option should be selected if:

- A different proxy server than the one defined in Tools > Proxy server is used to update ESET 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.

Note

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.

4.3.2 Update rollback

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

ESET NOD32 Antivirus records snapshots of detection engine and program modules for use with the rollback feature. In order to create detection engine snapshots, leave Create snapshots of modules check box selected. The Number of locally stored snapshots field defines the number of previous detection engine snapshots stored.

If you click Rollback (Advanced setup (F5) > Update > Basic), 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. Because it represents a potential security risk, we do not recommend selecting this option.

If a rollback is performed, the Roll back button changes to Allow updates. No updates will be allowed for the time interval selected from the Suspend updates drop-down menu. The version of detection engine is downgraded to the oldest available and stored as a snapshot in the local computer file system.
Note

Let the number 6871 be the most recent version of detection engine. 6870 and 6868 are stored as a detection engine snapshots. Note that 6869 is not available because, for example, the computer was turned off and a more recent update was made available before 6869 was downloaded. If the Number of locally stored snapshots field is set to 2 and you click Roll back, the detection engine (including program modules) will be restored to version number 6868. This process may take some time. Check whether the version of detection engine has downgraded from the main program window of ESET NOD32 Antivirus in the Update section.

4.3.3 How to create update tasks

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

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

- Regular automatic update
- Automatic update after dial-up connection
- Automatic update after user logon

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

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

Click More tools to display other tools to protect your computer.

4.4.1 Tools in ESET NOD32 Antivirus

This section includes features that help simplify program administration and offers additional options for advanced users.

This menu includes the following tools:

- **Log files**
- **Security report**
- **Watch activity**
- **Running processes** (if ESET LiveGrid® is enabled in ESET NOD32 Antivirus)
- **ESET SysInspector**
- **ESET SysRescue Live** – Redirects you to the ESET SysRescue Live website, where you can download the ESET SysRescue Live .iso CD/DVD image.
- **Scheduler**
- **System cleaner** – Helps you restore the computer to a usable state after cleaning the threat.
- **Submit sample for analysis** – Allows you to submit a suspicious file for analysis to the ESET Research Lab. The dialog window displayed after clicking this option is described in this section.
- **Quarantine**
4.4.1.1 Log files

Log files contain information about important program events that have occurred 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. It is possible to 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 **Log** drop-down menu. The following logs are available:

- **Detections** – This log offers detailed information about detections and infiltrations detected by ESET NOD32 Antivirus. Log information includes the time of detection, name of detection, location, the action taken and the name of the user logged in at the time the infiltration was detected. Double-click any log entry to display its details in a separate window. Not cleaned infiltrations are always marked with red text on a light red background, cleaned infiltrations are marked with yellow text on white background. Not cleaned PU As 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 that have occurred in the program. It is designed for system administrators and users to solve problems. Often the information found here can help you find a solution for a problem occurring in the program.

- **Computer scan** – Results of all completed manual or planned scans are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view the details of the respective scan.

- **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 particular 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 + 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, ...).
- **Filter...** – After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.
- **Enable filter** – Activates filter settings.
- **Disable filter** – Clears all filter settings (as described above).
- **Copy/Copy all** – Copies information about all the records in the window.
- **Delete/Delete all** – Deletes the selected record(s) or all the records displayed – this action requires administrator privileges.
- **Export...** – Exports information about the record(s) in XML format.
- **Export all...** – Export information about all records in XML format.
- **Find/Find next/Find previous** – After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.

### 4.4.1.1 Log filtering

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

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

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

**Find text**

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

**Search in columns**

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

**Record types**

Choose one or more log record types from the drop-down menu:
- **Diagnostic** - Logs information needed to fine-tune the program and all records above.
- **Informative** - Records informative messages, including successful update messages, plus all records above.
- **Warnings** - Records critical errors and warning messages.
- **Errors** - Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical** - Logs only critical errors (error starting antivirus protection).

**Time period**

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

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

**Match whole words only**

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

**Case sensitive**

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

4.4.1.1.2 Logging configuration

The Logging configuration of ESET NOD32 Antivirus is accessible from the main program window. Click Setup > Advanced Setup > Tools > Log files. The logs section is used to define how the logs will be managed. The program automatically deletes older logs in order to save hard disk space. You can specify the following options for log files:

**Minimum logging verbosity** – Specifies the minimum verbosity level of events to be logged.

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

**Note**

All blocked connections will be recorded when you select the Diagnostic verbosity level.

Log entries older than the specified number of days in the **Automatically delete records older than (days)** field will automatically be deleted.

**Optimize log files automatically** – 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 Log files:
• **Target directory** – The directory where log files will be stored (only applies to Text/CSV). Each log section has its own file with a predefined 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.

---

**Note**

In order to help resolve issues more quickly, ESET may ask you to provide logs from your computer. ESET Log Collector makes it easy for you to collect the information needed. For more information about ESET Log Collector, please visit our ESET Knowledgebase article.

---

### 4.4.1.2 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.
**Note**

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.

**Note**

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 in B (bytes).
- **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).

**Note**

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.
4.4.1.3  Security report

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

- **Web pages blocked** – 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 mail objects that have been detected.
- **PUA detected** – Displays the number of Potentially unwanted applications (PUA).
- **Spam emails detected** – Displays the number of detected spam emails.
- **Documents checked** – Displays the number of scanned document objects.
- **Apps checked** – Displays the number of scanned executable objects.
- **Other objects checked** – Displays the number of other scanned objects.
- **Web page objects scanned** – Displays the number of scanned web page objects.
- **Email objects scanned** – Displays the number of scanned email objects.

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

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

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

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

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

4.4.1.5 ESET SysInspector
ESET SysInspector is an application that thoroughly inspects your computer and gathers detailed information about system components such as drivers and applications, network connections or important registry entries and assesses the risk level of each component. This information can help determine the cause of suspicious system behavior that may be due to software or hardware incompatibility or malware infection. See also Online user guide for ESET SysInspector.

The SysInspector window displays the following information about created logs:
- **Time** – The time of log creation.
- **Comment** – A short comment.
- **User** – The name of the user who created the log.
- **Status** – The status of log creation.
The following actions are available:

- **Show** – Opens created log. You can also right-click a given log file and select **Show** from the context menu.
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as **Created**) before attempting to access the log.
- **Delete** – Removes the selected log(s) from the list.

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

- **Show** – Opens the selected log in ESET SysInspector (same function as double-clicking a log).
- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until ESET SysInspector is finished (log status will display as **Created**) before attempting to access the log.
- **Delete** – Removes the selected log(s) from the list.
- **Delete all** – Deletes all logs.
- **Export...** – Exports the log to an .xml file or zipped .xml.

### 4.4.1.6 Scheduler

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

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

The Scheduler serves to schedule the following tasks: 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 dial-up connection
- Automatic update after user logon
- Regular checking for latest product version (see **Update mode**)  
- 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. Enter 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 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. Turn on the **Enabled** switch if you want 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 predefined date and time.
- **Repeatedly** – The task will be performed at the specified time interval.
- **Daily** – The task will run repeatedly each day at the specified time.
- **Weekly** – The task will run on the selected day and time.
- **Event triggered** – The task will be performed on a specified event.

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

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

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

---

**Note**

Only a user with Administrator rights can perform actions in the System cleaner.

---

4.4.1.8 ESET SysRescue Live

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

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

- [Online Help for ESET SysRescue Live](#)

4.4.1.9 Cloud-based protection

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

A user 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®. There are two options:

1. 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 than detection engine update when ESET LiveGrid® is enabled.
2. You can configure ESET LiveGrid® to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its detection capabilities.
ESET LiveGrid® will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer’s operating system.

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

---

**Related information**

Read more about ESET LiveGrid® in the glossary.

See our illustrated instructions available in English and several other languages on how to enable or disable ESET LiveGrid® in ESET NOD32 Antivirus.

---

The ESET LiveGrid® reputation system provides cloud-based whitelisting and blacklisting. To access settings for ESET LiveGrid®, press F5 to enter Advanced setup and expand Detection Engine > Cloud-based Protection.

### Cloud-based protection in Advanced setup

**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** – Data will be sent to the ESET Research Lab for further analysis.

**Submit crash reports and diagnostics data** – Submit data such as crash reports, modules memory dumps.

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

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

### Submission of samples

**Automatic submissions of infected samples**

This will submit all infected samples to ESET for analysis and to improve future detection. The following options are available:

- All infected samples
- All samples except documents
- Do not submit

**Automatic submissions of suspicious samples**

- **Executables** – Includes files like .exe, .dll, .sys.
- **Archives** – Includes filetypes like .zip, .rar, .7z, .arch, .arj, .bzzip, .gzip, .ace, .arc, .cab.
- **Scripts** – Includes filetypes like .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Other** – Includes filetypes like .jar, .reg, .msi, .sfw, .lnk.
- **Possible Spam emails** – This will allow sending possible spam parts or whole possible spam emails with attachment to ESET for further analysis. Enabling this option improve Global detection of spam including improvements to future spam detection for you.
- **Documents** – Include Microsoft Office documents or PDFs with active content.

### Exclusions
The Exclusion filter allows you to exclude certain files/folders from submission (for example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets). The files listed will never be sent to ESET labs for analysis, even if they contain suspicious code. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

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. Once all current information is sent, no further packages will be created.

4.4.1.9.1 Suspicious files

If you find a suspicious file, you can submit it for analysis to our ESET Research Lab. If it is a malicious application, its detection will be added to the next virus signature update.

Exclusion filter – The Exclusion filter allows you to exclude certain files/folders from submission. The files listed will never be sent to ESET Research Lab for analysis, even if they contain a suspicious code. For example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

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

Select Enable logging to create an event log to record file and statistical information submissions. This will enable logging to the Event log when files or statistics are sent.
4.4.1.10 Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET NOD32 Antivirus.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to the ESET Research Lab.

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 infected file, its size in bytes, reason (for example, object added by user), and number of threats (for example, 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). If desired, you can quarantine any suspicious file manually by clicking Quarantine... If this is the case, the original file will not be removed from its original location. The context menu can also be used for this purpose; right-click in the Quarantine window and select Quarantine....

Restoring from 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 window. If a file is marked as potentially unwanted application, the Restore and exclude from scanning option is enabled. Read more about this type of application in the glossary. The context menu also offers the Restore to... option which allows you to restore a file to a location other than the one from which it was deleted.

Deleting from Quarantine – Right-click on a given item and select Delete from Quarantine, or select the item you want to delete and press Delete on your keyboard. You can also select multiple items and delete them together.
Note

If the program quarantined a harmless file by mistake, please **exclude the file from scanning** after restoring and send the file to ESET Technical Support.

**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 file to the ESET Virus Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.

**4.4.1.11 Proxy server**

In large LAN networks, communication between your computer and the internet can be mediated by a proxy server. Using this configuration, the following settings need to be defined. Otherwise the program will not be able to update itself automatically. In ESET NOD32 Antivirus, proxy server setup is available from two different sections of the Advanced setup tree.

First, proxy server settings can be configured in **Advanced setup** under **Tools > Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET NOD32 Antivirus. Parameters here will be used by all modules that require a connection to the Internet.

To specify proxy server settings for this level, select **Use proxy server** and enter the address of the proxy server into the **Proxy server** field along with the **Port** number of the proxy server.

If communication with the proxy server requires authentication, select **Proxy server requires authentication** and enter a valid **Username** and **Password** into the respective fields. Click **Detect** to automatically detect and populate proxy server settings. The parameters specified in Internet Explorer will be copied.

**Note**

You must manually enter your **Username** and **Password** in **Proxy server** settings.

**Use direct connection if proxy is not available** – If a product is configured to utilize HTTP Proxy and the proxy is unreachable, the product will bypass the proxy and communicate directly with ESET servers.

Proxy server settings can also be established from Advanced update setup (**Advanced setup > Update > Profiles > Updates > Connection options** by selecting **Connection through a proxy server** from the **Proxy mode** drop-down menu). This setting applies for the given update profile and is recommended for laptops that often receive virus signature updates from remote locations. For more information about this setting, see **Advanced update setup**.
### 4.4.1.12 Email notifications

ESET NOD32 Antivirus can automatically send notification emails if an event with the selected verbosity level occurs. Enable **Send event notifications by email** to activate email notifications.

#### SMTP server

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

<table>
<thead>
<tr>
<th>Note</th>
<th>SMTP servers with TLS encryption are supported by ESET NOD32 Antivirus.</th>
</tr>
</thead>
</table>

**Username** and **password** – If the SMTP server requires authentication, these fields should be filled in with a valid username and password to access the SMTP server.

**Sender address** – Define the sender address that will be displayed in the header of notification emails.

**Recipient addresses** – Define the recipient addresses that will be displayed in the header of notification emails. Multiple values are supported, please use semi-colon as separator.

From the **Minimum verbosity for notifications** drop-down menu, you can select the starting severity level of notifications to be sent.

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages such as non-standard network events, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages (Antistealth is not running properly or update failed).
- **Errors** – Errors (document protection not started) and critical errors will be recorded.
- **Critical** – Logs only critical errors error starting antivirus protection or infected system.

**Enable TLS** – Enable sending alert and notification messages supported by TLS encryption.
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.

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

Message format

Format of event messages – Format of event messages that are displayed on remote computers.

Format of threat warning messages – Threat alert and notification messages have a predefined default format. We advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format.

Charset – Converts an email message to the ANSI character encoding based upon Windows Regional settings (for example, windows-1250), Unicode (UTF-8), ASCII 7-bit (for example "á" will be changed to "a" and an unknown symbol to "?"), or Japanese (ISO-2022-JP).

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).

4.4.1.12.1 Message format

Here you can set up the format of event messages that are displayed on remote computers.

Threat alert and notification messages have a predefined default format. We advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format.

Keywords (strings separated by % signs) are replaced in the message by the actual information as specified. The following keywords are available:

- %TimeStamp% – Date and time of the event
- %Scanner% – Module concerned
- %ComputerName% – Name of the computer where the alert occurred
- %ProgramName% – Program that generated the alert
- %InfectedObject% – Name of infected file, message, etc
- %VirusName% – Identification of the infection
- %Action% – Action taken over infiltration
- %ErrorDescription% – Description of a non-virus event

The keywords %InfectedObject% and %VirusName% are only used in threat warning messages, and %ErrorDescription% is only used in event messages.

Use local alphabetic characters – Converts an email message to the ANSI character encoding based upon Windows Regional settings (e.g. windows-1250). If you leave this deselected, a message will be converted and encoded in ASCII 7-bit (for example "á" will be changed to "a" and an unknown symbol to "?").

Use local character 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).

4.4.1.13 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.

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**.
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 file (file that is detected as an infection but are not infected)
- False positive site
- Other

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

**Contact email** – This contact email is sent along with 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.

**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.

### 4.4.1.14 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. The following levels are available:

- **No updates** – No system updates will be offered for download.
- **Optional updates** – Updates marked as low priority and higher will be offered for download.
- **Recommended updates** – Updates marked as common and higher will be offered for download.
- **Important updates** – Updates marked as important and higher will be offered for download.
- **Critical updates** – Only critical updates will be offered for download.

Click **OK** to save changes. The System updates window will be displayed after status verification with the update server. Accordingly, the system update information may not be immediately available after saving changes.
4.4.1.15  ESET CMD

This is a feature that enables advanced ecmd commands. It allows you to export and import settings using the command line (ecmd.exe). Until now, it was only possible to export settings using the GUI. 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 importation of any unsigned configuration, which is a potential risk.

- **Advanced setup password** – a password is required to import a configuration from an .xml file, this file must be signed (see signing .xml configuration file further down). The password specified in Access Setup must be provided before a new configuration can be imported. If you do not have access setup enabled, your password does not match or the .xml configuration file is not signed, the configuration will not be imported.

Once ESET CMD is enabled, you can use the command line to import or export ESET NOD32 Antivirus configurations. You can do it manually or create a script for the purpose of automation.

### Important

To use advanced ecmd commands, you need to run them with administrator privileges, or open a Windows Command Prompt (cmd) using **Run as administrator**. Otherwise, you'll get **Error executing command**. Also, when exporting a configuration, the destination folder must exist. The export command still works when the ESET CMD setting is switched off.

### Example

**Export settings command:**
ecmd /getcfg c:\config\settings.xml

**Import settings command:**
ecmd /setcfg c:\config\settings.xml

### Note

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 xsigntool.exe
4. Execute a command to sign the .xml configuration file, usage: xsigntool /version 1|2 <xml_file_path>

### Important

The value of the /version parameter depends on your version of 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.

Example

Sign exported configuration file command:
xmlsign tool /version 1 c:\config\settings.xml

![Command prompt screen](image)

Note

If your Access Setup password changes and you want to import a configuration that was signed earlier with an old password, you need to sign the xml configuration file again using your current password. This allows you to use an older configuration file without exporting it to another machine running ESET NOD32 Antivirus before the import.

4.5 User interface

The User interface section allows you to configure the behavior of the program's Graphical user interface (GUI). Using the Graphics tool, you can adjust the program's visual appearance and effects used.

By configuring Alerts and notifications, you can change the behavior of detection alerts and system notifications. These can be customized to fit your needs.

To provide maximum security of your security software, you can prevent any unauthorized changes by protecting the settings by a password using the Access setup tool.
4.5.1 User interface elements

User interface configuration options in ESET NOD32 Antivirus allow you to adjust the working environment to fit your needs. These configuration options are accessible in the Advanced setup > User interface > User interface elements.

- If you want to deactivate the ESET NOD32 Antivirus splash-screen, deselect Show splash-screen at startup.
- To have ESET NOD32 Antivirus play a sound when important events occur during a scan, for example when a threat is discovered or when the scan has finished, select Use sound signal.
- **Integrate into the context menu** – Integrate the ESET NOD32 Antivirus control elements into the context menu.
- **Application statuses** – Click Edit button to manage (disable) statuses that are displayed in the first pane in main menu.

See also:

- Alerts and notifications
- Access setup
- Customer Experience Improvement Program
4.5.2 Alerts and notifications

Looking for information about common alerts and notifications?
- Threat found
- Address has been blocked
- Product not activated
- Update is available
- Troubleshooting for "Modules update failed" message

The Alerts and notifications section under User interface allows you to configure how threat alerts and system notifications (for example, successful update messages) are handled by ESET NOD32 Antivirus. You can also set the display time and transparency of system tray notifications (this applies only on systems that support system tray notifications).

Alert windows
Disabling Display alerts will cancel all alert windows, and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left in its default setting (enabled).

In-product messaging
Display marketing messages – In-product messaging has been designed to inform users of ESET news and other communications. Sending marketing messages requires the consent of a user. Therefore, 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 option.

Desktop notifications
Notifications on the Desktop and balloon tips are informative only, and do not require user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate Desktop notifications, select Display notifications on desktop.
Enable **Do not display notifications when running applications in full-screen mode** to suppress all non-interactive notifications. More detailed options, such as notification display time and window transparency can be modified below.

**Display Security report notifications** – You can enable or disable Security report notifications.

The **Minimum verbosity of events to display** drop-down menu allows you to select the severity level of alerts and notifications to be displayed. The following options are available:

- **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...).

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of this user** field specifies which user will receive system and other notifications on systems allowing multiple users to connect at the same time. Normally, this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

**Message boxes**

To close pop-up windows automatically after a certain period of time, select **Close message boxes automatically**. If they are not closed manually, alert windows are automatically closed after the specified time period elapses.

**Confirmation messages** – Shows you a list of confirmation messages that you can select to display or not to display.

**4.5.2.1 Confirmation messages**

This dialog window displays confirmation messages that ESET NOD32 Antivirus will display before any action is performed. Select or deselect the check box next to each confirmation message to allow or disable it.

**4.5.3 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 of ESET NOD32 Antivirus can be password protected.

**Password protect settings** – Indicate password settings. Click to open the Password setup window.

To set or change a password to protect setup parameters, click **Set** next to **Set password**.

**Note**

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 enter 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**

**Require full administrator rights for limited administrator accounts** – Select this to prompt the current user (if he or she does not have administrator rights) to enter an administrator username and password when modifying certain system parameters (similar to the User Account Control (UAC) in Windows Vista and Windows 7). Such modifications include disabling protection modules.

**Require administrator rights (system without UAC support)** – On Windows XP systems where UAC is not running, users will have the **Require administrator rights (system without UAC support)** option available.
4.5.4 System tray icon

Some of the most important setup options and features are available by right-clicking the system tray icon.

**Quick links** – Displays the most frequently used parts of ESET NOD32 Antivirus. You can quickly access these from the program menu.

**Pause protection** – Displays the confirmation dialog box that disables Detection engine, which guards against malicious system attacks by controlling file, web and email communication.

The **Time interval** drop-down menu represents the period of time that the protection will be disabled for.
Advanced setup – Select this option to enter the Advanced setup tree. There are also other ways to open Advanced setup, such as pressing the F5 key or navigating to Setup > Advanced setup.

Log files – Log files contain information about important program events that have occurred and provide an overview of detections.

Open ESET NOD32 Antivirus – Opens the ESET NOD32 Antivirus main program window from the tray icon.

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

Check for updates – Starts updating the detection engine (previously known as "virus signature database") to ensure your level of protection against malicious code.

About – Provides system information, details about the installed version of ESET NOD32 Antivirus and the installed program modules. Here you can also find the license expiration date and information about the operating system and system resources.

4.5.5 Help and support
ESET NOD32 Antivirus contains troubleshooting tools and support information that will help you solve issues that you may encounter.

Help

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

Open help – Click this link to launch the ESET NOD32 Antivirus help pages.

Find quick solution – Click this link to find solutions to the most frequently encountered problems. We recommend that you read this section before contacting Technical Support.

Technical Support

Submit support request – If you could not find an answer to your problem, you can use this form located on the ESET website to quickly contact our Technical Support department.

Details for Technical Support – When prompted, you can copy and send information to ESET Technical Support (such as product name, product version, operating system and processor type). Enable Advanced logging to create advanced logs for all available features in order 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.
Support Tools

**Threat encyclopedia** – Links to the ESET Threat Encyclopedia, which contains information about the dangers and symptoms of different types of infiltration.

**Detection Engine history** – Links to ESET Virus radar, which contains information about each version of the ESET detection database (previously known as “virus signature database”).

**ESET Log Collector** – Links to the [ESET Knowledgebase article](#), where you can download ESET Log Collector, an application that automatically collects information and logs from a computer in order to help resolve issues more quickly. For more information see the [ESET Log Collector online user guide](#).

**ESET Specialized Cleaner** – Removal tools for common malware infections, for more information please visit this [ESET Knowledgebase article](#).

Product and License Information

**About ESET NOD32 Antivirus** – Displays information about your copy of [ESET NOD32 Antivirus](#).

**Activate Product/Change License** – Click to launch the activation window and activate your product.

**Change product** – Click to see if ESET NOD32 Antivirus can be changed to a different product line with the current license.
4.5.5.1 About ESET NOD32 Antivirus
This window provides details about installed version of ESET NOD32 Antivirus, your operating system and system resources.

Click **Installed components** to see information about the list of installed 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.

4.5.5.2 ESET News
In this window ESET NOD32 Antivirus informs you of ESET news.

If you want to receive marketing messages via pop-up window, enable option **Display marketing messages** in Advanced setup (F5) > **User interface** > **Alerts and notifications**.
4.5.5.3 Submit system configuration data

In order 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 for providing technical assistance to the customer.

When submit the web form, your system configuration data will be submitted to ESET. Select **Always submit this information** if you want to remember this action for this process. To submit the form without sending any data click **Don’t submit data** and you can contact ESET Technical Support by using the online support form.

This setting can also be configured in **Advanced setup > Tools > Diagnostics > Technical Support**.

---

**Note**

If you have decided to submit system data it is needed to fill and submit the web form, otherwise your ticket will not be created and your system data will be lost.
5. Advanced user

5.1 Profiles

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

Computer scan

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

To create a new profile, open the Advanced setup window (F5) and click Detection engine > Malware scans > On-demand scan > List of profiles. The Profile manager window includes the Selected profile drop-down menu that lists existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

Note

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

Update

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

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

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

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

5.2 Keyboard shortcuts

For better navigation in ESET NOD32 Antivirus, the following keyboard shortcuts can be used:

<table>
<thead>
<tr>
<th>Keyboard shortcut</th>
<th>Action taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>opens help pages</td>
</tr>
<tr>
<td>F5</td>
<td>opens Advanced setup</td>
</tr>
<tr>
<td>Up/Down</td>
<td>navigation in product through items</td>
</tr>
<tr>
<td>TAB</td>
<td>moves the cursor in a window</td>
</tr>
<tr>
<td>Esc</td>
<td>closes the active dialog window</td>
</tr>
<tr>
<td>Ctrl+U</td>
<td>shows information about ESET license and your computer</td>
</tr>
</tbody>
</table>
Ctrl+R resets product window to its default size and position on the screen

5.3 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 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 Licensing advanced logging – Record all product communication with license server.

Enable Operating System advanced logging – Additional information about Operating system such as running processes, CPU activity, disc operations will be gathered. This can help developers to diagnose and fix problems related to ESET product running on your operating system (available for Windows 10).

Enable Parental control advanced logging – Record all events that occur in Parental control. This can help developers diagnose and fix problems related to Parental control.

Enable Protocol filtering advanced logging – Record all data passing through the Protocol filtering engine in PCAP format in order to help the developers diagnose and fix the problems related to Protocol filtering.

Enable Update engine advanced logging – Record all events that occur during update process. This can help developers diagnose and fix problems related to the Update engine.

Log files location

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Log files directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Vista and later</td>
<td>C:\ProgramData\ESET\ESET NOD32 Antivirus\Diagnostics\</td>
</tr>
<tr>
<td>Earlier versions of Windows</td>
<td>C:\Documents and Settings\All Users...</td>
</tr>
</tbody>
</table>
5.4 Import and export settings

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

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

Importing a configuration is very easy. In the main program window click Setup > Import and export settings, and then select Import settings. Enter the file name of the configuration file or click the ... button to browse for the configuration file you want to import.

The steps to export a configuration are very similar. In the main program window, click Setup > Import and export settings. Select Export settings and enter the file name of the configuration file (i.e. export.xml). Use the browser to select a location on your computer to save the configuration file.

![Import and export settings](image)

**Note**

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

5.5 Command Line

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
Scanner options

/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
/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=EXTENSIONS scan only EXTENSIONS delimited by colon
/ext-exclude=EXTENSIONS exclude EXTENSIONS delimited by colon from scanning
/clean-mode=MODE use cleaning MODE for infected objects

The following options are available:
- none – No automatic cleaning will occur.
- standard (default) – 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
/no-quarantine (supplements the action carried out while cleaning)

General options
/help show help and quit
/version show version information and quit
/preserve-time preserve last access timestamp

Exit codes
0 no threat found
1 threat found and cleaned
10 some files could not be scanned (may be threats)
50 threat found
100 error

Note
Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

5.6 Idle-state detection

Idle state detection settings can be configured in Advanced setup under Detection engine > Malware scans > Idle-state scanning > Idle state detection. These settings specify a trigger for Idle-state scanning, when:
- the screen saver is running,
- the computer is locked,
- a user logs off.

Use the switches for each respective state to enable or disable the different idle state detection triggers.
6. Common Questions

This chapter covers some of the most frequently asked questions and problems encountered. Click the topic title to find out how to solve your problem:

- How to update ESET NOD32 Antivirus
- How to remove a virus from my PC
- How to create a new task in Scheduler
- How to schedule a scan task (every 24 hours)
- How to unlock Advanced setup

If your problem is not included in the help pages list above, try searching the ESET NOD32 Antivirus help pages.

If you cannot find the solution to your problem/question in the help pages, you can visit our regularly updated online ESET Knowledgebase. Links to our most popular Knowledgebase articles are included below to help you resolve common issues:

- I received an activation error while installing my ESET product. What does it mean?
- Activate my ESET Windows home product using my Username, Password, or License Key
- Uninstall or reinstall my ESET home product
- I receive 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?
- How to start Windows in Safe Mode or Safe Mode with networking

If necessary, you can contact our Technical Support with your questions or problems.

6.1 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, please navigate to Tools > Scheduler (for more information on Scheduler, click here).

6.2 How to remove a virus from my PC

If your computer is showing symptoms of malware infection, e.g. it is slower, 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 wish to only scan a certain part of your disk, click Custom scan and select targets to be scanned for viruses.

For additional information please see our regularly updated ESET Knowledgebase article.
6.3 How to create a new task in Scheduler

To create a new task in Tools > More tools > Scheduler, click Add 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 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.

Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task below:

From the **Scheduled task** drop-down menu, select **Update**. Enter the name of the task into the **Task name** field and click **Next**. Select the frequency of the task. The following options are available: Once, Repeatedly, Daily, Weekly and Event triggered. Select **Skip task when running on battery power** to minimize system resources while a laptop is running on battery power. The task will be run on the specified date and time in **Task execution** fields. Next, define the action to take if the task cannot be performed or completed at the scheduled time. The following options are available:

- At the next scheduled time
- As soon as possible
- Immediately, if time since last 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, allowing you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of currently scheduled tasks.

6.4 How to schedule a weekly computer scan

To schedule a regular task, open the main program window and click **Tools > More tools > Scheduler**. Below is a short guide on how to schedule a task that will scan your local drives every 24 hours. See our Knowledgebase article for more detailed instructions.

To schedule a scan task:

1. Click **Add** in the main Scheduler screen.
2. Select **On-demand computer scan** from the drop-down menu.
3. Enter a name for the task and select **Weekly** for the task frequency.
4. Set the day and time the task will execute.
5. Select **Run the task as soon as possible** to perform the task later if the scheduled task does not run for any reason (for example, if the computer was turned off).
6. Review the summary of the scheduled task and click **Finish**.
7. From the **Targets** drop-down menu, select **Local drives**.
8. Click **Finish** to apply the task.
6.5 How to unlock Advanced setup

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 enter the email address you used for license registration. ESET will send you an email with the verification code. Enter the verification code and then write and confirm the new password. The verification code is valid for 7 days.

You can also **restore password via your my.eset.com account**. Use this option, if the license is associated with your ESET License Manager.

If you cannot remember your email address, click **I don’t know my email address** and you will be redirected to the ESET website to quickly contact our Technical Support department.

**Generate code for Technical Support** – This option will generate the code to be provided to Technical Support. Copy the code provided by Technical Support and click **I have a verification code**. Enter the verification code and then write and confirm the new password. The verification code is valid for 7 days.

For more information, read the **ESET Knowledgebase article**.