# ESET ENDPOINT SECURITY 6

## User Guide

Microsoft® Windows® 10/8.1/8/7/Vista/XP x86 SP3/XP x64 SP2

Click here to download the most recent version of this document

ENJOY SAFER TECHNOLOGY™

# ESET **ENDPOINT SECURITY 6**



Worldwide Customer Support: www.eset.com/support

REV. 3/29/2016

# Contents

# Contents

# 1. ESET Endpoint Security

ESET Endpoint Security 6 represents a new approach to truly integrated computer security. The most recent version of the ThreatSense® scanning engine, combined with our custom Personal firewall and Antispam module, utilizes speed and precision to keep your computer safe. The result is an intelligent system that is constantly on alert for attacks and malicious software endangering your computer.

ESET Endpoint Security 6 is a complete security solution produced from our long-term effort to combine maximum protection and a minimal system footprint. The advanced technologies, based on artificial intelligence, are capable of proactively eliminating infiltration by viruses, spyware, trojan horses, worms, adware, rootkits, and other Internet-borne attacks without hindering system performance or disrupting your computer.

ESET Endpoint Security 6 is primarily designed for use on workstations in a small business/enterprise environment. It can be used with ESET Remote Administrator, allowing you to easily manage any number of client workstations, apply policies and rules, monitor detections and remotely configure from any networked computer.

## 1.1 What's new

The graphical user interface of ESET Endpoint Security has been completely redesigned to provide better visibility and a more intuitive user experience. Some of the many improvements included in ESET Endpoint Security version 6 include:

**Functional and usability improvements**

- Web control – Define a single rule for multiple URLs, or define different policies for different network locations. "Soft" blocking policies are new for version 6 along with the ability to partially customize the blocking and warning page.
- Personal Firewall – You can now create firewall rules directly from the log or IDS notification window and assign profiles to network interfaces.
- A new Botnet protection – helps discover malware through analyzing its network communication patterns and protocols.
- Device Control – Now includes the ability to determine device type and serial number, and to define single rules for multiple devices.
- A new Smart mode for HIPS – is placed between Automatic and Interactive mode. Ability to identify suspicious activities and malicious processes in the system.
- Updater/Mirror improvements – You can now resume failed downloads of virus signature database and/or product modules.
- New approach to remote manageability for your computers with ESET Remote Administrator – Resend logs in the case of an ERA reinstall or for testing, remote install ESET security solutions, get an overview of the security state of your networked environment and sort various data for later use.
- User Interface improvements – Adds the one-click option to run a manual update of the virus signature database and modules from the Windows System Tray. Support for touch-screens and high resolution displays.
- Improved detection and removal of third-party security solutions.

**New functionality**

- Anti-Phishing – protects you from attempts to acquire passwords and other sensitive information by restricting access to malicious websites that impersonate legitimate ones.
- Scanning speed improvements – using shared local cache in virtualized environments.

**Detection & Protection technologies**

- Improved installation speed and reliability.
- Advanced memory scanner – Monitors process behavior and scans malicious processes when they decloak in memory.
- Enhanced Exploit blocker – Designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. Exploit blocker now supports Java and helps improve detection and protection from these kind of vulnerabilities.
- Improved detection and removal of rootkits.
- Vulnerability shield – More advanced filtering options to detect various types of attacks and vulnerabilities.
- Idle state scanner – Performs a silent scan on all local drives when your computer is in idle state.

## 1.2 System requirements

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

**Processors Supported:**

• 32-bit (x86) or 64-bit (x64) processor, 1 GHz or higher (see Note 1)

**Operating Systems:** Microsoft ® Windows ® 10/8.1/8/7/Vista/XP SP3 32-bit/XP SP2 64-bit

• An operating system and the required service pack supported by the chosen ESET product version installed
• System requirements of the operating system and other software installed on the computer are fulfilled
• 0.3 GB of free system memory (see Note 2)
• 1 GB of free disk space(see Note 3)
• Minimum display resolution 1024x768
• Internet connection or a local area network connection to a source (see Note 4) of product updates

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

**NOTE:**

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

## 1.3 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 infiltrations and attacks. To provide maximum protection and convenience, it is essential that you use your antivirus solution correctly and adhere to several useful rules:

**Update regularly**

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

Update setup chapter.

**Download security patches**

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

**Back up important data**

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

**Regularly scan your computer for viruses**

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

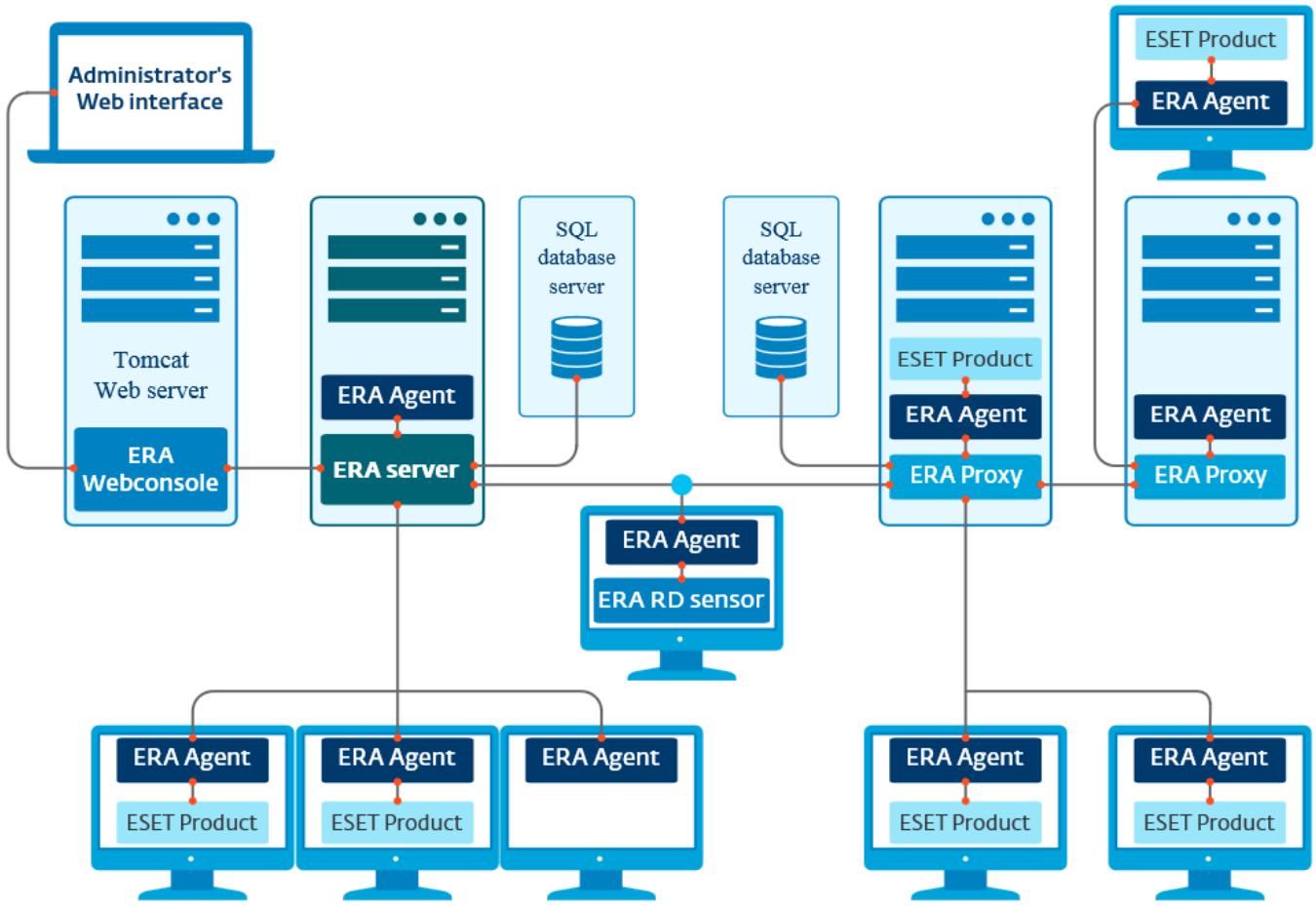
- Do not visit suspicious websites with multiple pop-ups and flashing advertisements.
- Be careful when installing freeware programs, codec packs, etc. Only use safe programs and only visit safe Internet websites.
- Be cautious when opening email attachments, particularly those from mass-mailed messages and messages from unknown senders.
- Don't use an Administrator account for everyday work on your computer.

# 2. Documentation for users connected via ESET Remote Administrator

ESET Remote Administrator (ERA) is an application that allows you to manage ESET products in a networked environment from one central location. The ESET Remote Administrator task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats. ESET Remote Administrator does not provide protection against malicious code on its own, it relies on the presence of an ESET security solution on each client.

ESET security solutions support networks that include multiple platform types. Your network can include a combination of current Microsoft, Linux-based, Mac OS and operating systems that run on mobile devices (mobile phones and tables).

The picture below depicts a sample architecture for a network protected by ESET security solutions managed by ERA:




**NOTE:** For more information see the ESET Remote Administrator User Guide.

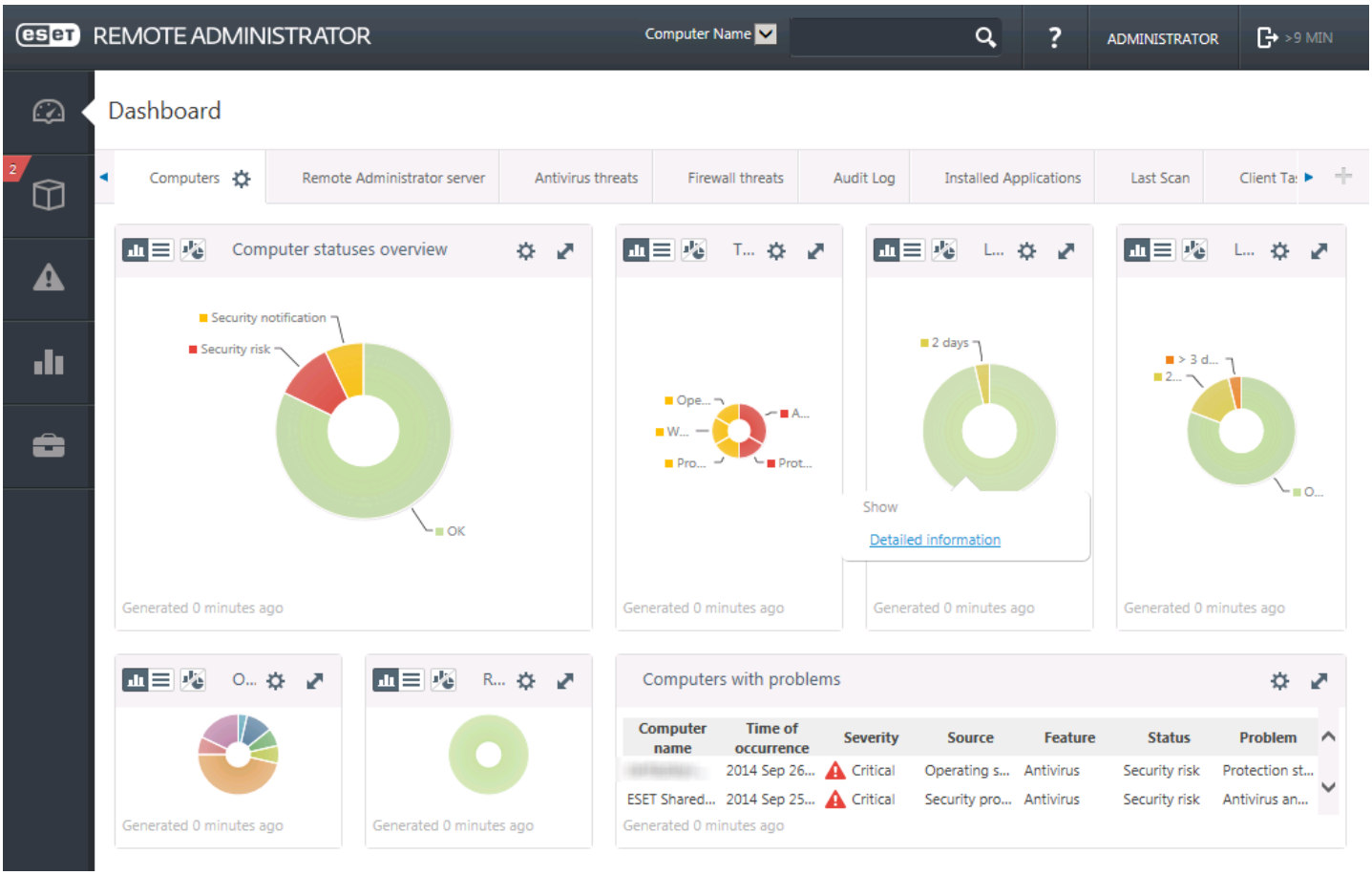
## 2.1 ESET Remote Administrator Server

**ESET Remote Administrator Server** is a primary component of ESET Remote Administrator. It is the executive application that processes all data received from clients that connect to the Server (through the ERA Agent). The ERA Agent facilitates communication between the client and the server. Data (Client logs, configuration, agent replication, etc.) are stored in a database. To correctly process the data, the ERA Server requires a stable connection to a Database server. We recommend that you install ERA Server and your database on separate servers to optimize performance. The machine on which ERA Server is installed must be configured to accept all Agent/Proxy/RD Sensor connections which are verified using certificates. Once installed, you can open ERA Web Console which connects to the ERA Server (as can be seen in the diagram). From the Web Console, all ERA Server operations are performed when managing ESET security solutions within your network.

## 2.2 Web Console

**ERA Web Console** is a web-based user interface that presents data from ERA Server and allows you to manage ESET security solutions in your network. Web Console can be accessed using a browser. It displays an overview of the status of clients on your network and can be used to deploy ESET solutions to unmanaged computers remotely. You can choose to make the web server accessible from the internet to allow for the use of ESET Remote Administrator from virtually any place or device.

This is the Web Console's Dashboard:




The **Quick Search** tool is located at the top of the Web Console. Select **Computer Name**, **IPv4/IPv6 Address** or **Threat Name** from the drop-down menu, type your search string into the text field and then click the magnifier symbol or press **Enter** to search. You will be redirected to the **Groups** section, where your search result will be displayed.

**NOTE:** For more information see the ESET Remote Administrator User Guide.

## 2.3 Proxy

**ERA Proxy** is another component of ESET Remote Administrator and serves two purposes. In a medium-sized or enterprise network with many clients (for example, 10,000 clients or more), you can use ERA Proxy to distribute load between multiple ERA Proxies facilitating the main ERA Server. The other advantage of the ERA Proxy is that you can use it when connecting to a remote branch office with a weak link. This means that the ERA Agent on each client is not connecting to the main ERA Server directly via ERA Proxy, which is on the same local network as the branch office. This configuration frees up the link to the branch office. The ERA Proxy accepts connections from all local ERA Agents, compiles data from them and uploads it to the main ERA Server (or another ERA Proxy). This allows your network to accommodate more clients without compromising the performance of your network and database queries.

Depending on your network configuration, it is possible for ERA Proxy to connect to another ERA Proxy and then connect to the main ERA Server.

For proper function of the ERA Proxy, the host computer where you install ERA Proxy must have an ESET Agent installed and must be connected to the upper level (either ERA Server or an upper ERA Proxy, if there is one) of your network.

## 2.4 Agent

**ERA Agent** is an essential part of the ESET Remote Administrator product. ESET security solutions on client machines (for example ESET Endpoint security) communicate with ERA Server through the Agent. This communication allows for the management of ESET security solutions on all remote clients from a one central location. The Agent collects information from the client and sends it to the Server. When the Server sends a task to a client, the task is sent to the Agent which then communicates with the client. All network communication happens between the Agent and the upper part of the ERA network – Server and Proxy.

The ESET Agent uses one of the following three methods to connect to the Server:

1. The Client's Agent is directly connected to the Server.
2. The Client's Agent is connected through a Proxy that is connected to the Server.
3. The Client's Agent is connected to the Server through multiple Proxies.

The ESET Agent communicates with ESET solutions installed on a client, collects information from programs on that client and passes configuration information received from the Server to the client.

**NOTE:** The ESET proxy has its own Agent which handles all communication tasks between clients, other proxies and the Server.

## 2.5 RD Sensor

**RD (Rogue Detection) Sensor** is a part of ESET Remote Administrator designed to find computers on your network. It provides a convenient way of adding new computers to ESET Remote Administrator without the need to find and add them manually. Every computer found on your network is displayed in the Web Console and added to the default **All** group. From here, you can take further actions with individual client computers.

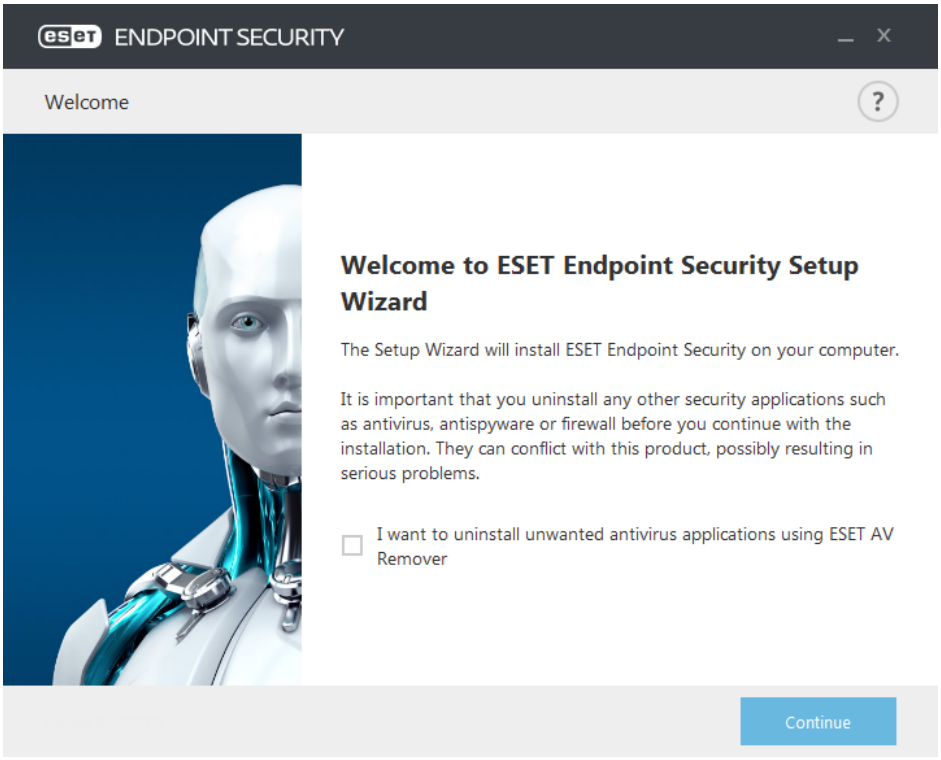
RD Sensor is a passive listener that detects computers that are present on the network and sends information about them to the ERA Server. The ERA Server evaluates whether the PCs found on the network are unknown or already managed.

# 3. Using ESET Endpoint Security by itself

This section of this User Guide is intended for users who are using ESET Endpoint Security without ESET Remote Administrator. All features and functionalities of ESET Endpoint Security are fully accessible depending on a user's account rights.

## 3.1 Installation with ESET AV Remover

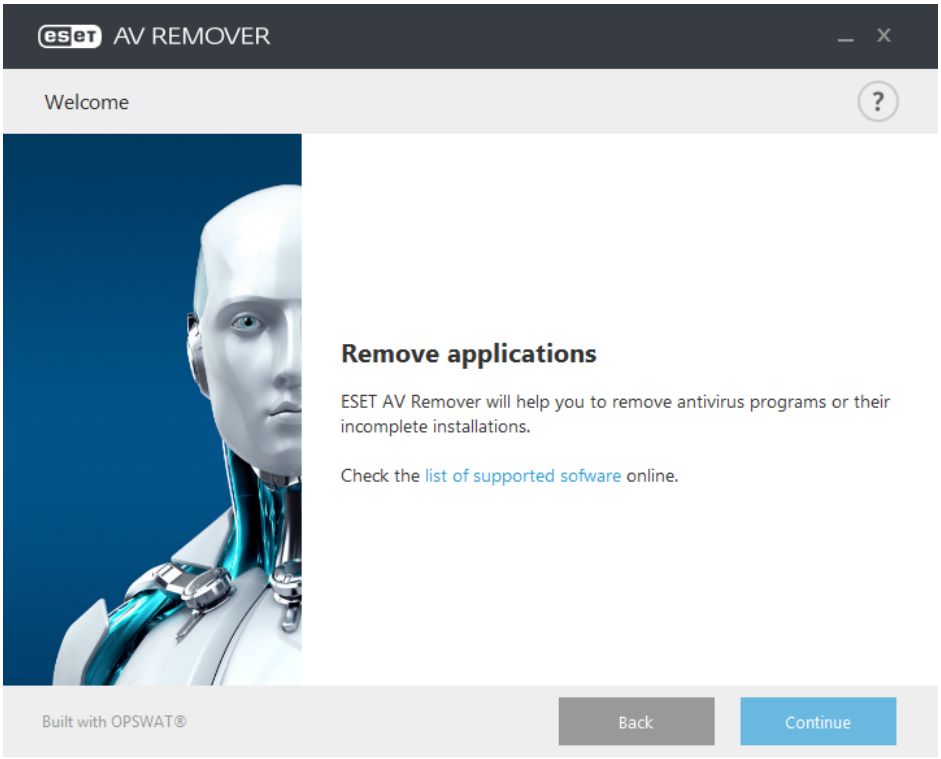
Before you continue with the installation process, it is important that you uninstall any existing security application on the computer. Select the check box next to **I want to uninstall unwanted antivirus applications using ESET AV Remover** to have ESET AV Remover scan your system and remove any supported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



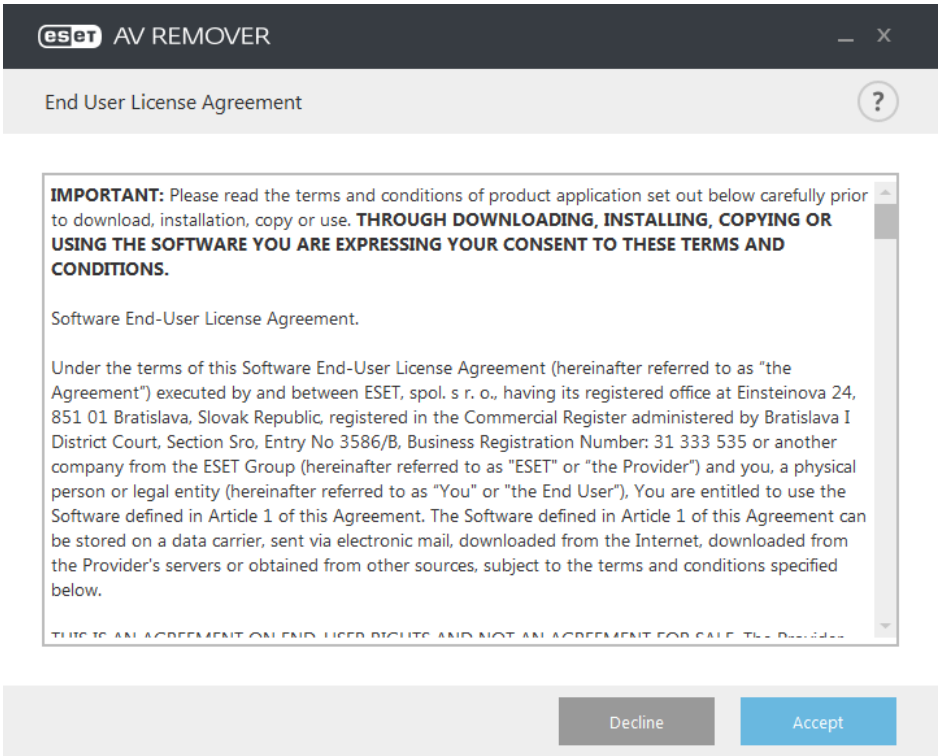
### 3.1.1 ESET AV Remover

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

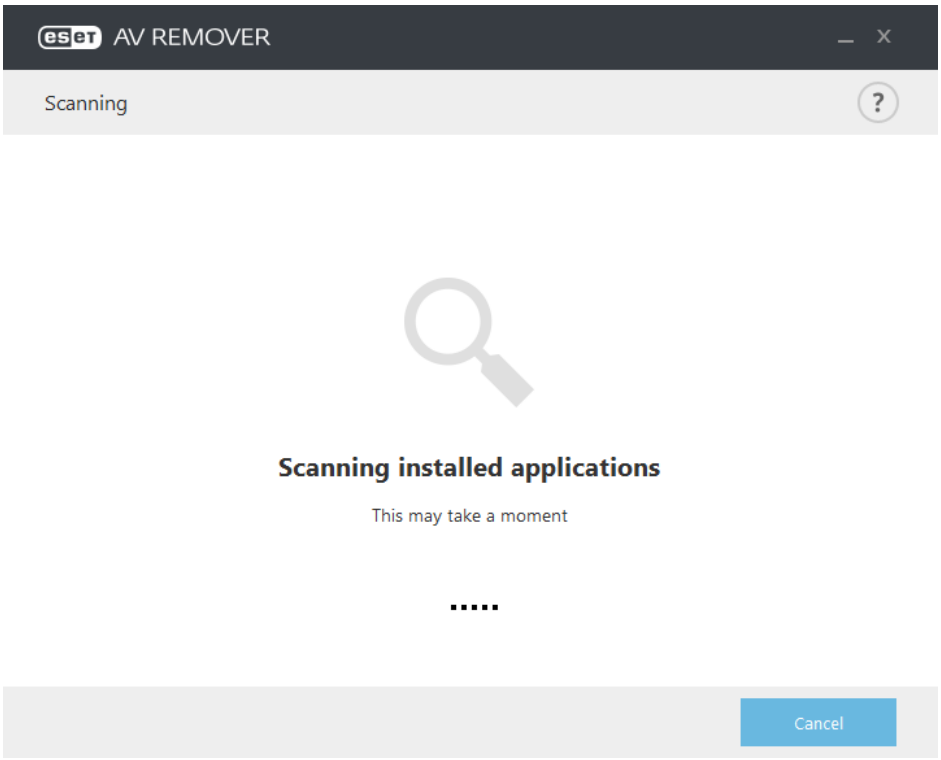
1. To view a list of antivirus software that ESET AV Remover can remove, visit ESET Knowledgebase article.



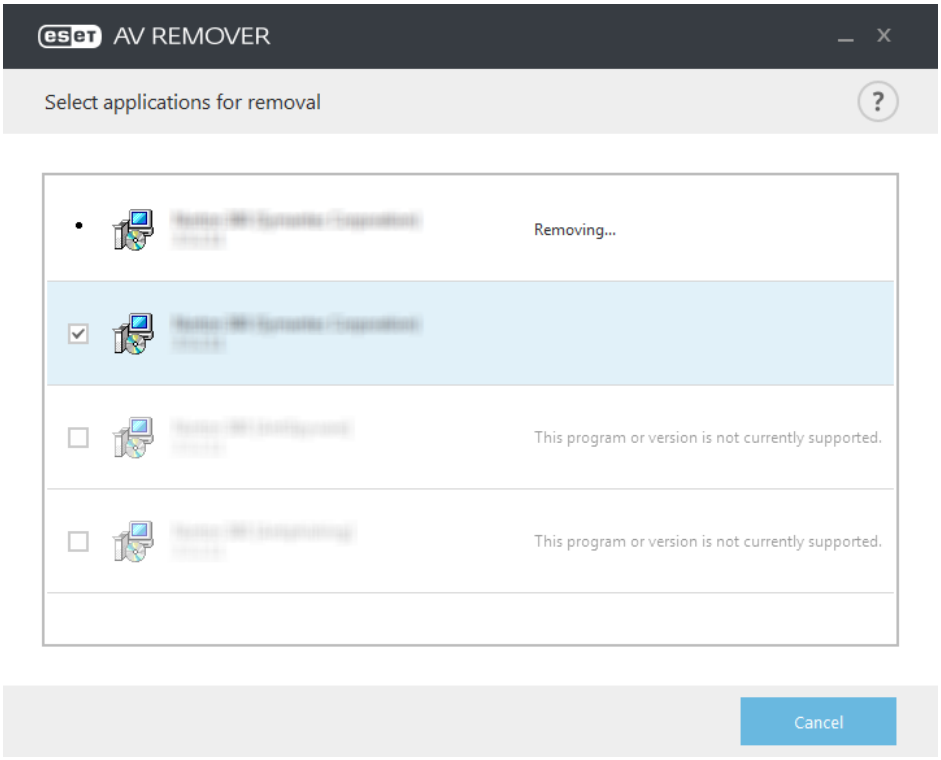

2. Read and click **Accept** to acknowledge your acceptance of the End-User License Agreement. Clicking **Decline** will continue to installation of ESET Endpoint Security without removal of existing security application on the computer.



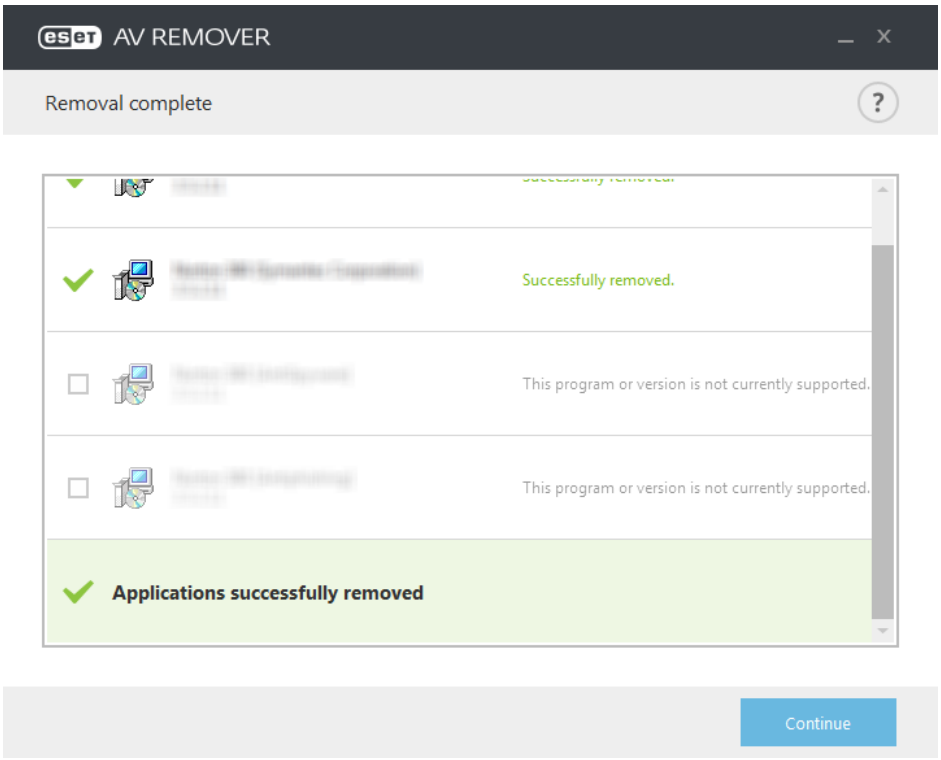
3. ESET AV Remover will begin searching your system for antivirus software.



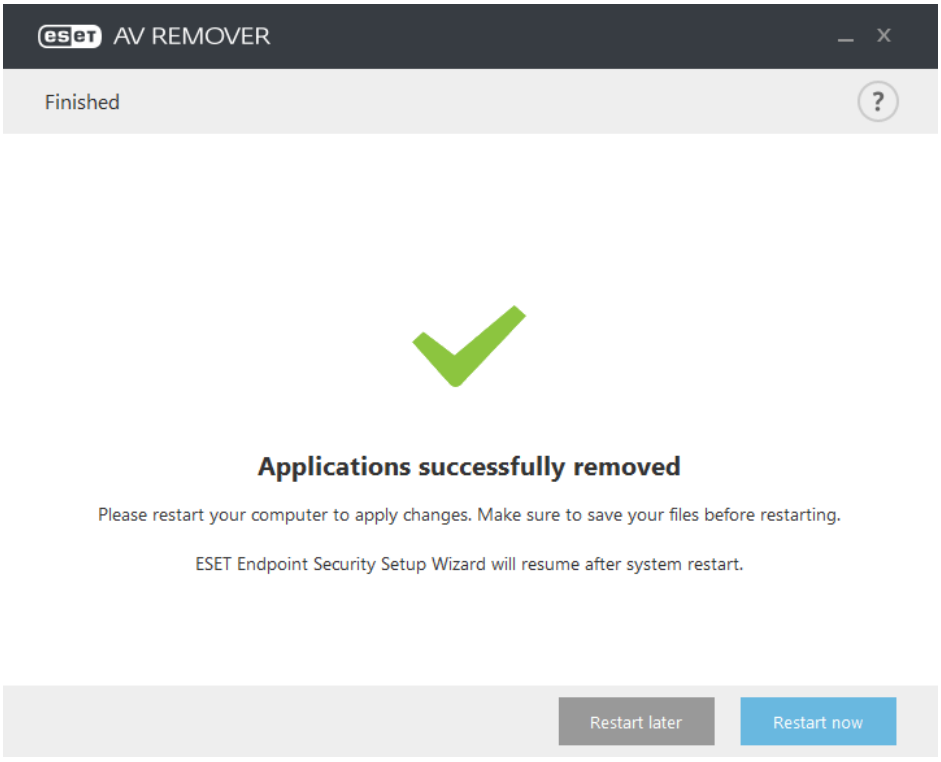

4. Select any listed antivirus applications and click **Remove**. Removal may take a moment.



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




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



### 3.1.2 Uninstallation using ESET AV Remover ended with error

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

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

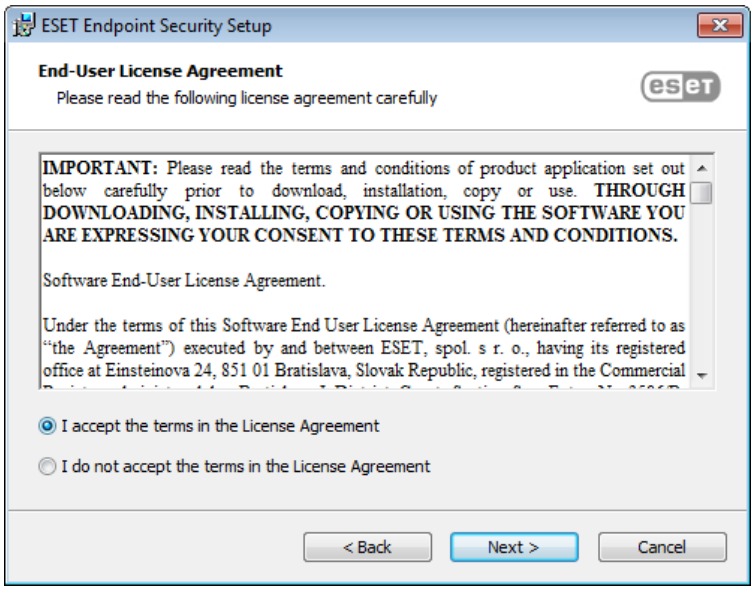
If necessary, contact ESET Customer Care to open a support request and have the **AppRemover.log** file available to assist ESET Technicians. The **AppRemover.log** file is located in the **eset** folder. Browse to *%TEMP%* in Windows Explorer to access this folder. ESET Customer Care will respond as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

## 3.2 Installation

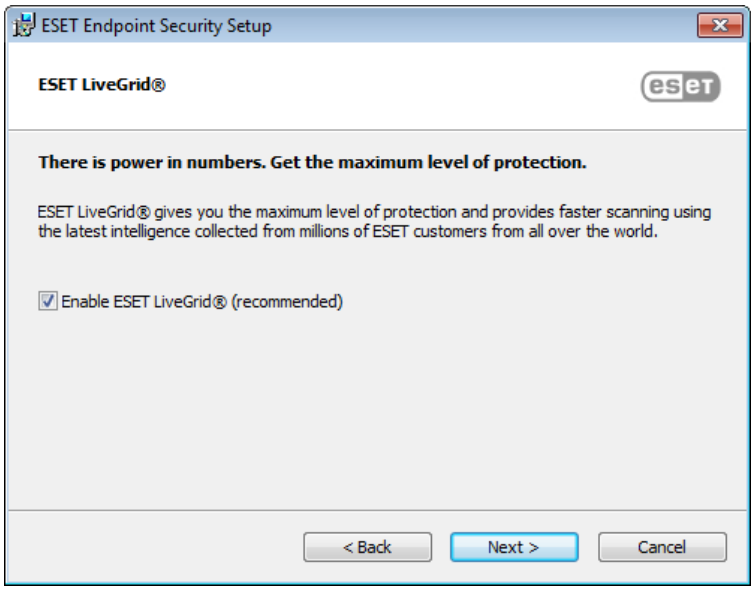
Once you launch the installer, the installation wizard will guide you through the installation process.

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

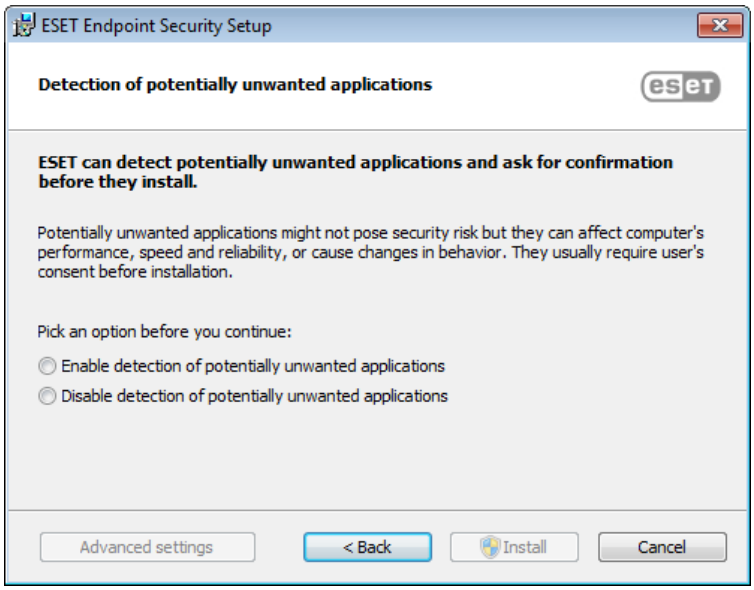
In the next step, the End-User License Agreement will be displayed. Please read and click **Accept** to acknowledge your acceptance of the End-User License Agreement. Click **Next** after you accept the terms to continue with installation.




After you select "I accept..." and click **Next**, you will be prompted to configure ESET LiveGrid®. ESET LiveGrid® helps ensure that ESET is immediately and continuously informed about new infiltrations, which allows us to better protect our customers. The system allows you to submit new threats to the ESET Virus Lab, where they are analyzed, processed and added to the virus signature database.



The next step in the installation process is to configure detection of Potentially unwanted applications which are not necessarily malicious, but can often negatively affect the behavior of your operating system. See the Potentially unwanted applications chapter for more details. You can access additional settings by clicking **Advanced settings** (for example to install your ESET product in a specific folder or enable automatic scan after the installation).




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

### 3.2.1 Advanced installation

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

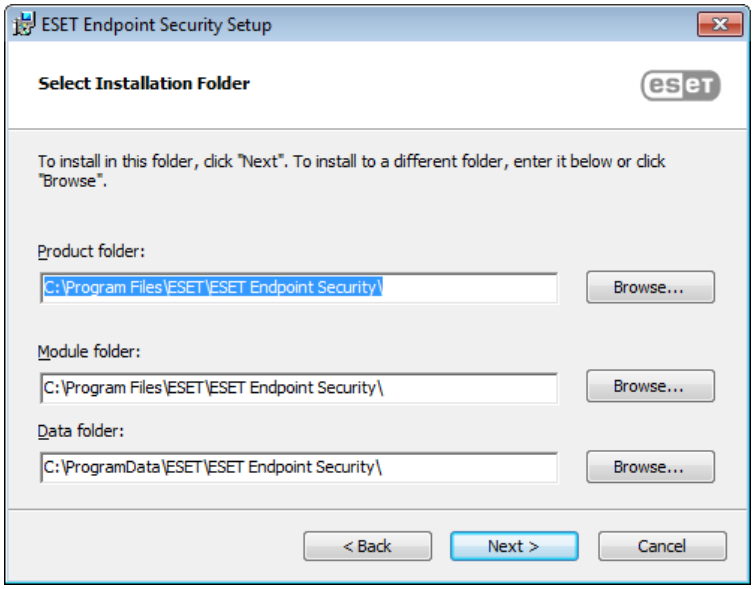
After selecting your preference for detection of potentially unwanted applications and clicking **Advanced settings**, you will be prompted to select a location for the installation Product folder. By default, the program installs to the following directory:

*C:\Program Files\ESET\ESET Endpoint Security*

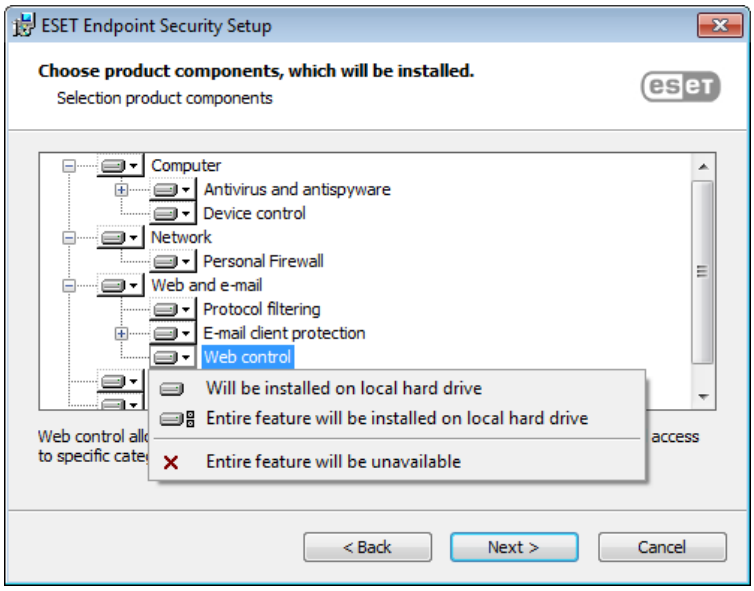
You can specify a location for program modules and data. By default, they are installed to the following directories, respectfully:

*C:\Program Files\ESET\ESET Endpoint Security*
*C:\ProgramData\ESET\ESET Endpoint Security*

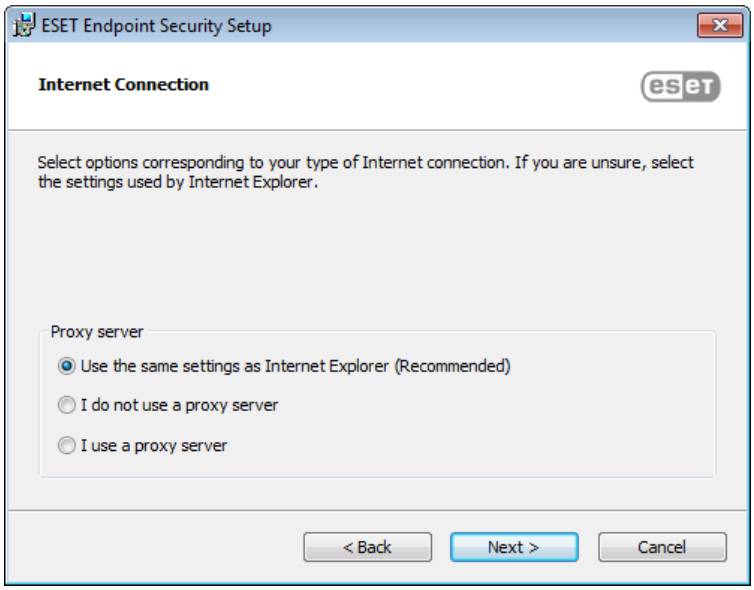
Click **Browse...** to change these locations (not recommended).



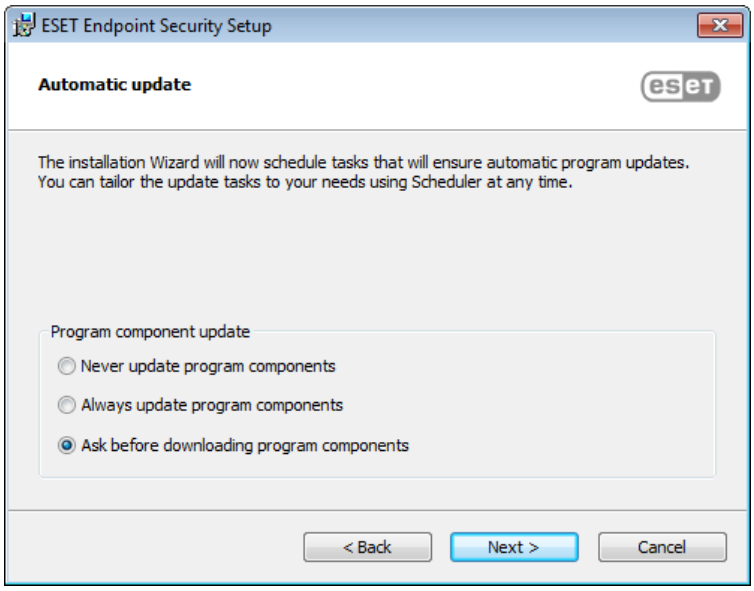
In the next window, you can choose which product components will be installed. Product components in the Computer section include Real-time file system protection, Computer scan, Document protection and Device control. Please note that the first two components are mandatory for your security solution to work. The Network section offers the option to install the Personal firewall, which monitors all incoming and outgoing network traffic and applies rules for individual network connections. Personal firewall also provides protection against attacks from remote computers. Components in the Web and email section are responsible for your protection while you are browsing the Internet and communicating via email. The Update mirror component can be used to update other computers on your network. The Microsoft NAP support section provides an agent from ESET to ensure full compatibility with the NAP architecture.




To configure your proxy server settings, select **I use a proxy server** and click **Next**. Enter the IP address or URL of your proxy server in the **Address** field. If you are not sure whether you use a proxy server to connect to the Internet, select **Use the same settings as Internet Explorer (Recommended)** and click **Next**. If you do not use a proxy server, select **I do not use a proxy server**. For more information see Proxy server.

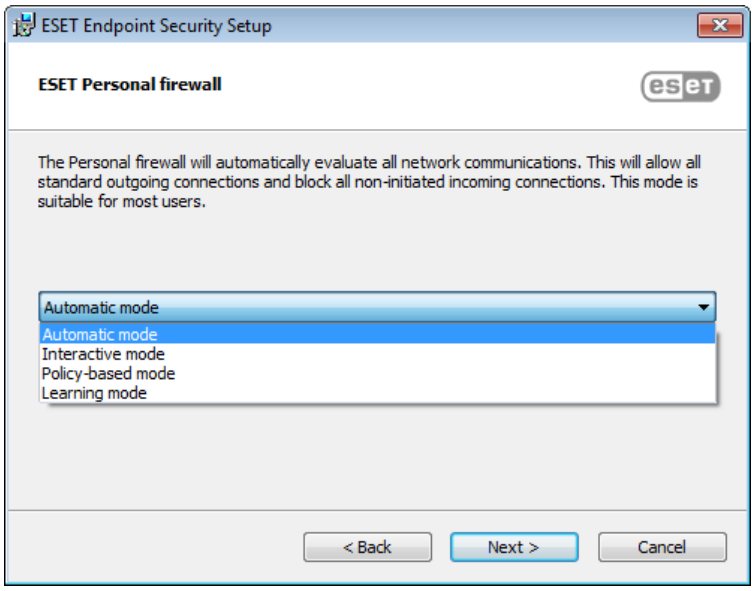


Custom installation allows you to define how automatic program updates will be handled on your system. Click **Change...** to access Advanced settings.

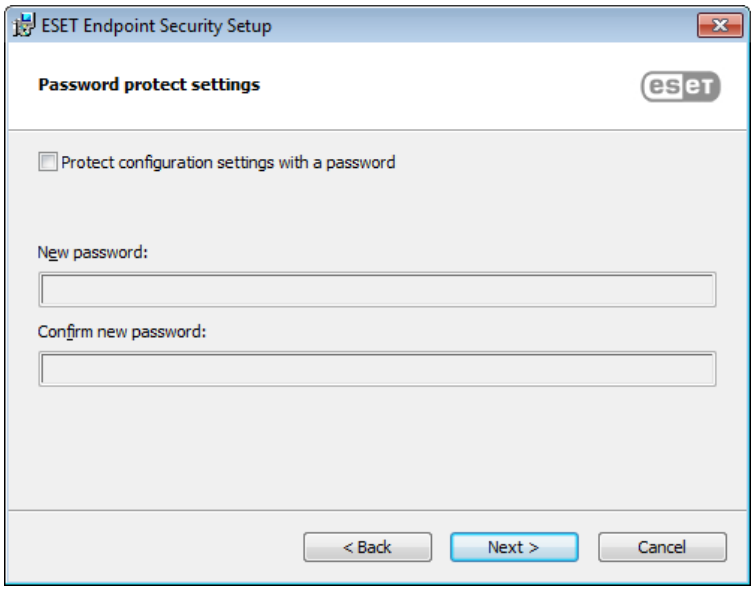



If you do not want program components to be updated, select **Never update program components**. Select **Ask before downloading program components** to display a confirmation window each time the system attempts to download program components. To download program component upgrades automatically, select **Always update program components**.

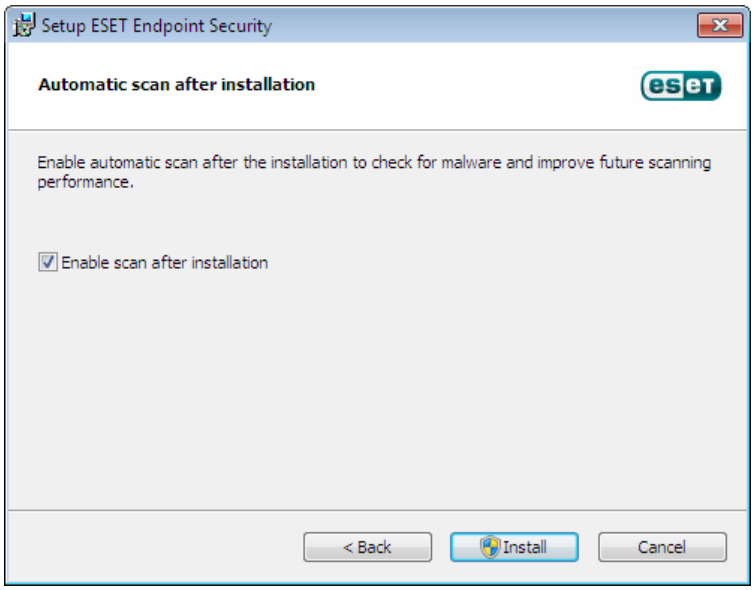
Next, select a filtering mode for the ESET Personal firewall. Four filtering modes are available for the ESET Endpoint Security Personal firewall. The behavior of the firewall changes based on the selected mode. Filtering modes also influence the level of user interaction required.



The next installation window offers the option to set a password to protect your program settings. Select **Protect configuration settings with a password** and enter your password into the the **New password** and **Confirm new password** fields. This password will be required to change or access the settings of ESET Endpoint Security. When both password fields match, click **Next** to continue.




To disable the first scan after installation, which is normally performed when installation finishes, deselect the check box next to **Enable scan after installation**.




Click **Install** to start installation.

## 3.3 Product installation via ERA (command line)

The following settings are intended for use **only with the reduced**, **basic and none** level of the user interface. See documentation for the **msiexec** version used for the appropriate command line switches.

**Supported parameters:**

**APPDIR=<path>**
- path - Valid directory path
- Application installation directory.
- For example: `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

**APPDATADIR=<path>**
- path - Valid directory path
- Application Data installation directory.

**MODULEDIR=<path>**

- path - Valid directory path
- Module installation directory.

**ADDLOCAL=<list>**

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

**Rules**

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

**Feature Presence**

- **Mandatory** - the feature will be always installed
- **Optional** - the feature may be deselected for install
- **Invisible** - logical feature mandatory for other features to work properly
- **Placeholder** - feature with no effect on the product, but must be listed with sub-features

Feature tree of Endpoint 6.1 is following:

| Feature tree | Feature Name | Feature Presence |
|---|---|---|
| Computer | Computer | Mandatory |
| Computer / Antivirus and antispyware | Antivirus | Mandatory |
| Computer / Antivirus and antispyware > Real-time file system protection | RealtimeProtection | Mandatory |
| Computer / Antivirus and antispyware > Computer scan | Scan | Mandatory |
| Computer / Antivirus and antispyware > Document protection | Document protection | Optional |
| Computer / Device control | DeviceControl | Optional |
| Network | Network | Placeholder |
| Network / Personal Firewall | Firewall | Optional |
| Web and e-mail | WebAndEmail | Placeholder |
| Web and e-mail ProtocolFiltering | ProtocolFiltering | Invisible |
| Web and e-mail / Web access protection | WebAccessProtection | Optional |
| Web and e-mail / E-mail client protection | EmailClientProtection | Optional |
| Web and e-mail / E-mail client protection / MailPlugins | MailPlugins | Invisible |
| Web and e-mail / E-mail client protection / Antispam protection | Antispam | Optional |
| Web and e-mail / Web control | WebControl | Optional |
| Update mirror | UpdateMirror | Optional |
| Microsoft NAP support | MicrosoftNAP | Optional |

**Additional rules**

- If any of the **WebAndEmail** feature/s is selected to be installed, the invisible **ProtocolFiltering** feature must be explicitly included in the list.
- If any of the **EmailClientProtection** sub-features/s is selected to be installed, the invisible **MailPlugins** feature must be explicitly included in the list

**Examples:**

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

**List of CFG_ properties:**

**CFG_POTENTIALLYUNWANTED_ENABLED=1/0**
• 0 - Disabled, 1 - Enabled
• PUA

**CFG_LIVEGRID_ENABLED**=1/0
• 0 - Disabled, 1 - Enabled
• LiveGrid

**FIRSTSCAN_ENABLE**=1/0
• 0 - Disable, 1 - Enable
• Schedule a new FirstScan after installation.

**CFG_EPFW_MODE**=0/1/2/3
• 0 - Automatic, 1 - Interactive, 2 - Policy, 3 - Learning

**CFG_PROXY_ENABLED**=0/1
• 0 - Disabled, 1 - Enabled

**CFG_PROXY_ADDRESS**=<ip>
• Proxy IP address.

**CFG_PROXY_PORT**=<port>
• Proxy port number.

**CFG_PROXY_USERNAME**=<user>
• User name for authentication.

**CFG_PROXY_PASSWORD**=<pass>
• Password for authentication.

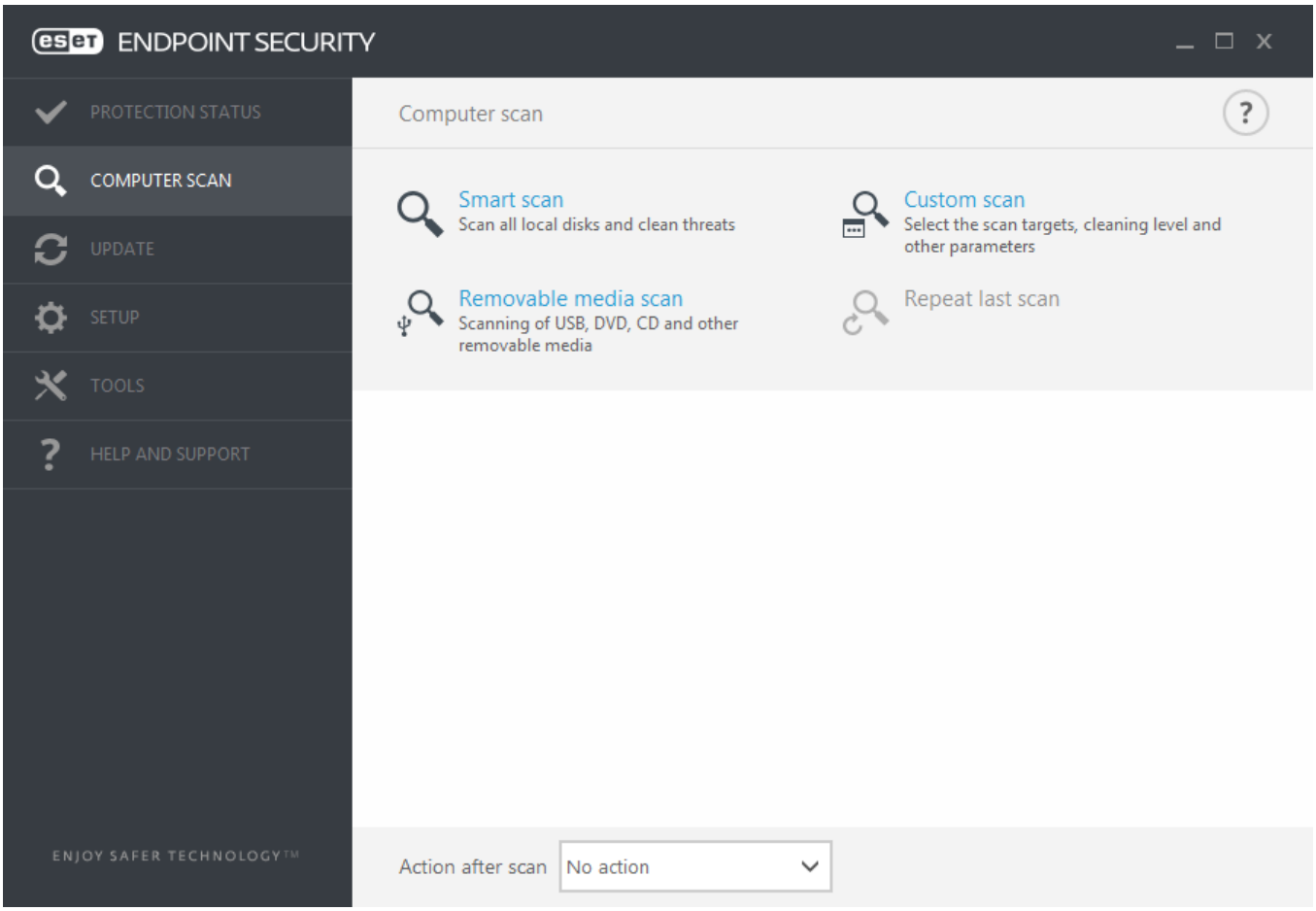
## 3.4 Product activation

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

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

## 3.5 Computer scan

No longer than 15 minutes after installation is complete (a computer restart may be necessary), ESET Endpoint Security will automatically perform a computer scan. In addition to the initial scan, we recommend that you perform regular computer scans, or schedule a regular scan, to check for threats. In the main program window, click **Computer scan** and then click **Smart scan**. For more information about computer scans, see Computer scan.




## 3.6 Upgrading to a more recent version

New versions of ESET Endpoint Security are issued to provide 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 impact certain system configurations, it is issued after a long testing period to function 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, by downloading and installing a more recent version over the previous one.
3. Manually, via automatic deployment in a network environment via ESET Remote Administrator.

## 3.7 Beginner's guide

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

### 3.7.1 The user interface

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

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

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

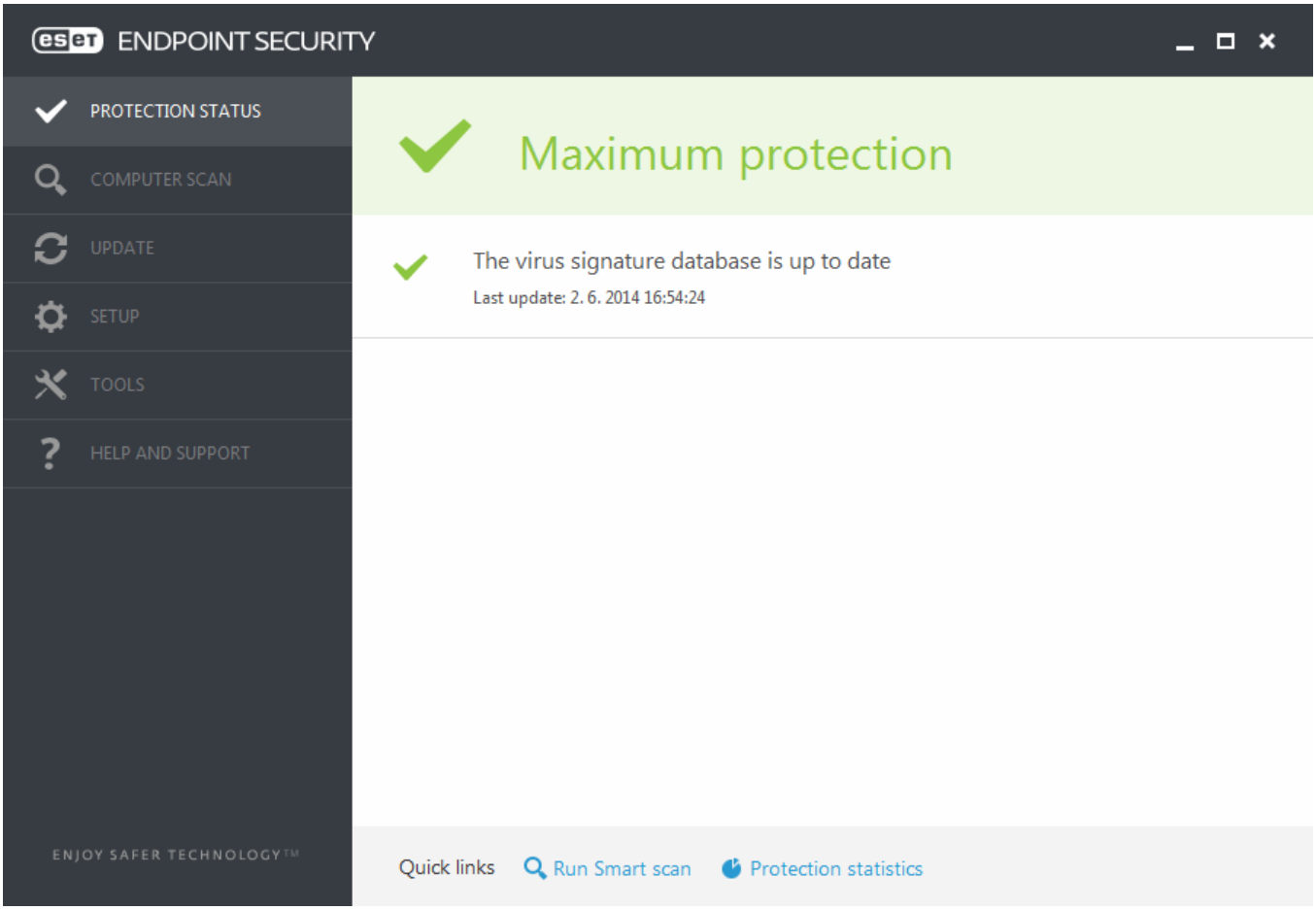
**Computer scan** – This option allows you to configure and launch of Smart scan, Custom scan, or Removable media scan. You can also repeat the last scan that was run.

**Update** – Displays information about the virus signature database.

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

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

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

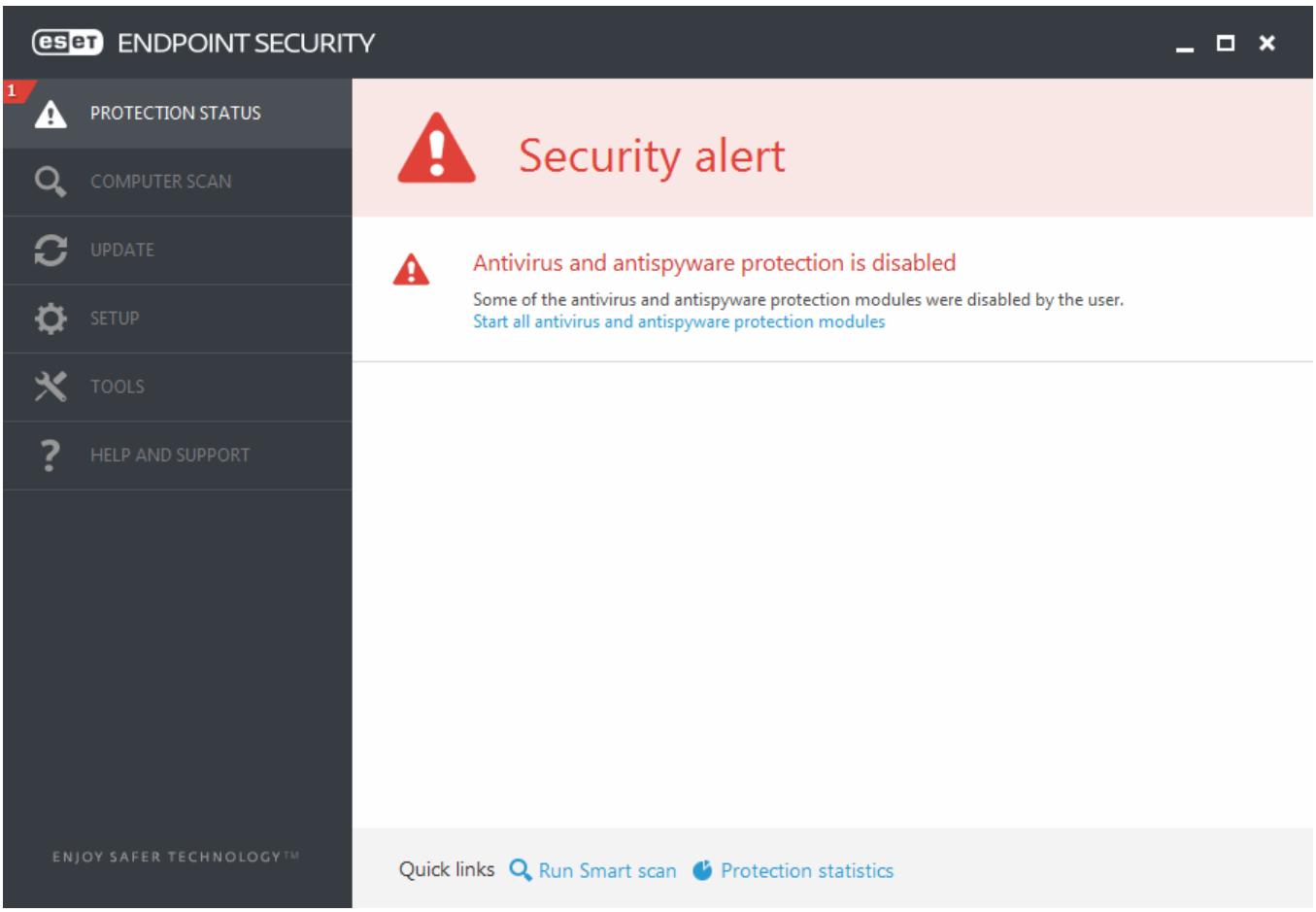



The **Protection status** screen informs you about the security and current protection level of your computer. The green **Maximum protection** status indicates that maximum protection is ensured.

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

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

If the modules enabled are working properly, they are assigned a green check. If not, a red exclamation point or orange notification icon is displayed. Additional information about the module is shown in the upper part of the window. A suggested solution for fixing the module is also displayed. To change the status of individual module, click **Setup** in the main menu and then click the desired module.




The red icon with a "!" signals critical problems – maximum protection of your computer is not ensured. Possible reasons are:

- **Antivirus and antispyware protection is disabled** – You can re-enable antivirus and antispyware protection by clicking on **Enable Real-time protection** in **Protection status** pane or **Enable Antivirus and antispyware protection** in **Setup** pane in the main program window.
- **The ESET Personal firewall is disabled** – This problem is indicated by a red icon and a security notification next to the **Network** item. You can re-enable network protection by clicking **Enable filtering mode**.
- **Virus signature database is out of date** – You are using an outdated virus signature database.
- **Product is not activated** or **License expired** – This is indicated by the Protection status icon turning red. The program is not able to update after the license expires. We recommend following the instructions in the alert window to renew your license.

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

- **Web access protection is disabled** – You can re-enable Web access protection by clicking on the security notification and then clicking **Enable Web access protection**.
- **Your license will expire soon** – This is indicated by the protection status icon displaying an exclamation point. After your license expires, the program will not be able to update and the Protection status icon will turn red.

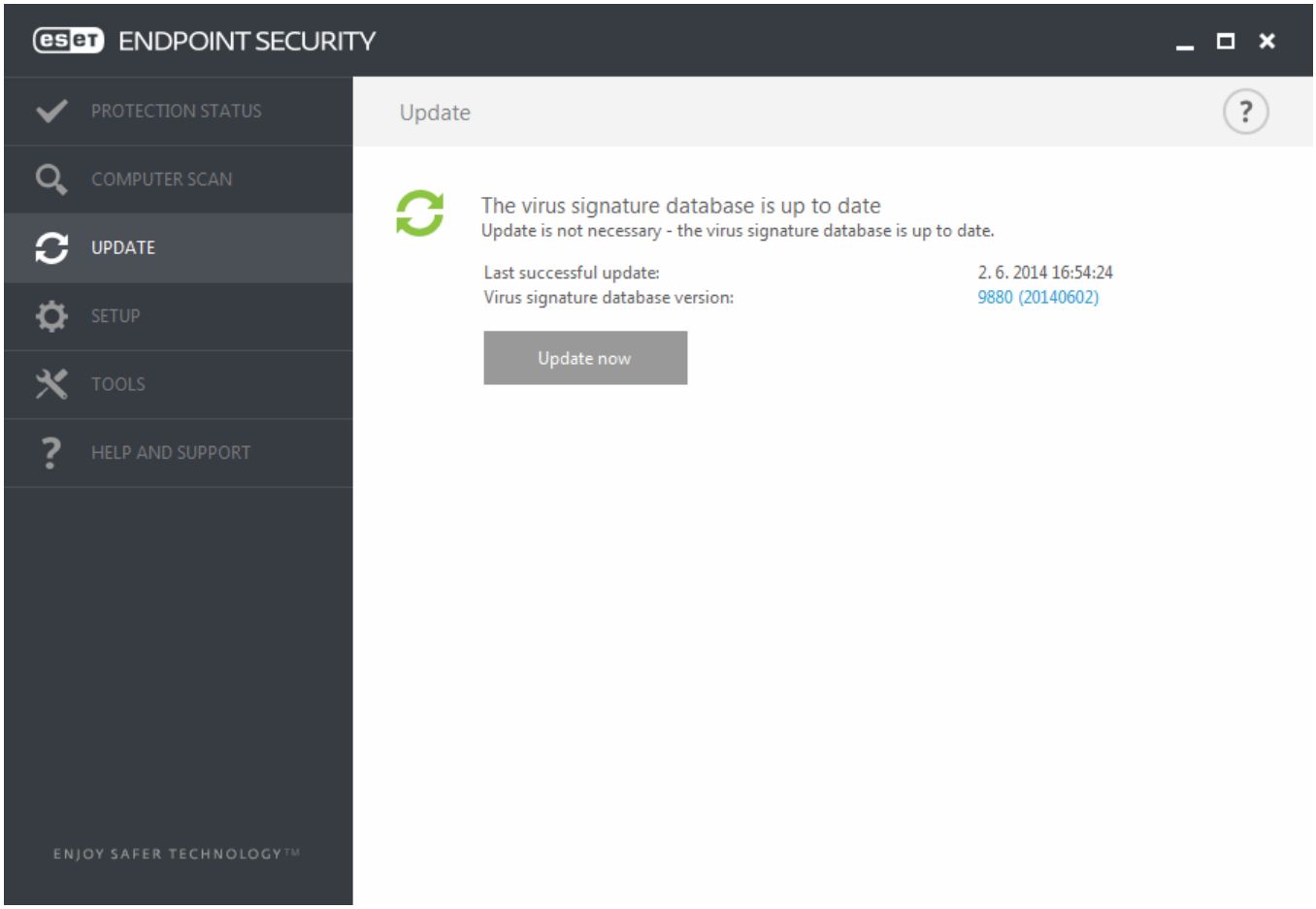
If you are unable to solve a problem using the suggested solutions, click **Help and support** to access the help files or search the ESET Knowledgebase. If you still need assistance, you can submit an ESET Customer Care support request.

ESET Customer Care will respond quickly to your questions and help find a resolution.

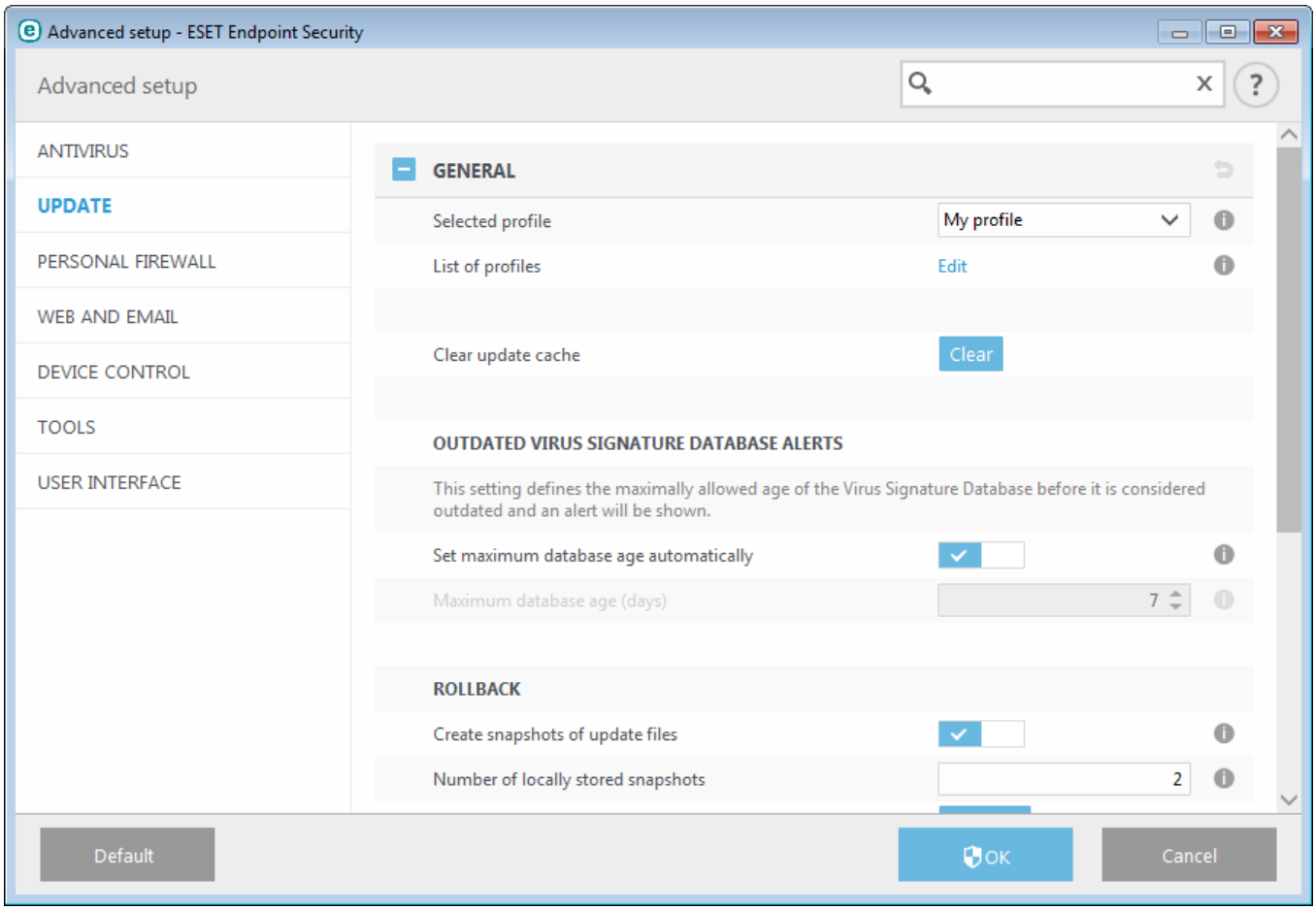
### 3.7.2 Update setup

Updating the virus signature database and program components is an important part of maintaining complete protection against malicious code. Please pay careful attention to update configuration and operation. From the main menu, select **Update** > **Update now** to check for a newer database update.

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



The Advanced setup window (click **Setup** > **Advanced setup** from the main menu, or press **F5** on your keyboard) contains additional update options. To configure advanced update options such as update mode, proxy server access, LAN connections and virus signature copy creation settings, click **Update** in the Advanced setup tree. If you experience problems with an update, click **Clear** to clear the temporary update cache. The **Update server** menu is set to **AUTOSELECT** by default. When using an ESET server, we recommend that you leave the **Choose automatically** option selected. If you do not want the system tray notification at the bottom right corner of the screen to appear, select **Disable display notification about successful update**.



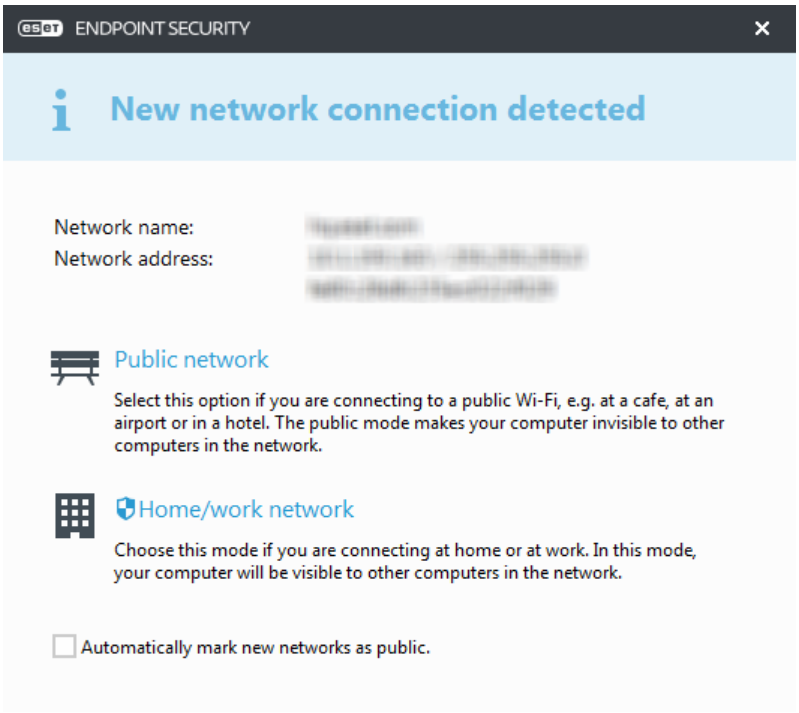

For optimal functionality, it is important that the program is automatically updated. This is only possible if the correct **License key** is entered in **Help and support** > **Activate Product**.

If you did not enter your **License key** after installation, you can do so at any time. For more detailed information about activation see How to activate ESET Endpoint Security and enter the credentials you received with your ESET security product in **License details** window.

### 3.7.3 Zones setup

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

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




***Warning:*** An incorrect trusted zone configuration may pose a security risk to your computer.

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

### 3.7.4 Web control tools

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

## 3.8 Common Questions

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

How to update ESET Endpoint Security
How to activate ESET Endpoint Security
How to use current credentials to activate a new product
How to remove a virus from my PC
How to allow communication for a certain application
How to create a new task in Scheduler
How to schedule a scan task (every 24 hours)
How to connect my product to ESET Remote Administrator
How to configure a mirror

If your problem is not included in the help pages listed above, try searching by keyword or phrase describing your

problem in the ESET Endpoint Security Help pages.

If you cannot find the solution to your problem/question in the Help pages, visit the ESET Knowledgebase where answers to common questions and issues are available.

How do I remove Sirefef (ZeroAccess) trojan?
Update Mirror troubleshooting checklist
What addresses and ports on my third-party firewall should I open to allow full functionality for my ESET product?

If necessary, you can contact our online technical support center with your questions or problems. The link to our online contact form can be found in the **Help and Support** pane in the main program window.

### 3.8.1 How to update ESET Endpoint Security

Updating ESET Endpoint Security can be performed either manually or automatically. To trigger the update, click **Update now** in the **Update** section in main menu.

The default installation settings create an automatic update task which is performed on an hourly basis. To change the interval, navigate to **Tools** > **Scheduler** (for more information on Scheduler, click here).

### 3.8.2 How to activate ESET Endpoint Security

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

There are several methods for activating your product. Availability of a particular activation scenario in the activation window may vary depending on the country, as well as the means of distribution (CD/DVD, ESET web page, etc.).

To activate your copy of ESET Endpoint Security directly from the program, click the system tray icon and select **Activate product license** from the menu. You can also activate your product from the main menu under **Help and support** > **Activate product** or **Protection status** > **Activate product**.

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

- **License Key** – A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the license owner and for activation of the license.
- **Security Admin** – An account created on the ESET License Administrator portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.
- **Offline License** – An automatically generated file that will be transferred to the ESET product to provide license information. If a license allows you to download an offline license file (.lf) that file can be used to perform offline activation. The number of offline licenses will be subtracted from the total number of available licenses. For more details about generation of an offline file see the ESET License Administrator User Guide.

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

If you have a Username and Password and do not know how to activate ESET Endpoint Security click **I have a Username and Password, what do I do**. You will be redirected to ESET License Administrator, where you can convert your credentials into a License key.

You can change your product license at any time. To do so, click **Help and support** > **Manage license** in the main program window. You will see the public license ID used to identify your license to ESET Support. The Username under which your computer is registered is stored in the **About** section, which you can view by right-clicking the system tray icon .

**NOTE:** ESET Remote Administrator can activate client computers silently using licenses made available by the administrator. For instructions to do so, see the ESET Remote Administrator User Guide.

### 3.8.3 How to use current credentials to activate a new product

If you already have your Username and Password and would like to receive a License Key, visit the ESET License Administrator portal, where you can convert your credentials to a new License Key.

### 3.8.4 How to remove a virus from my PC

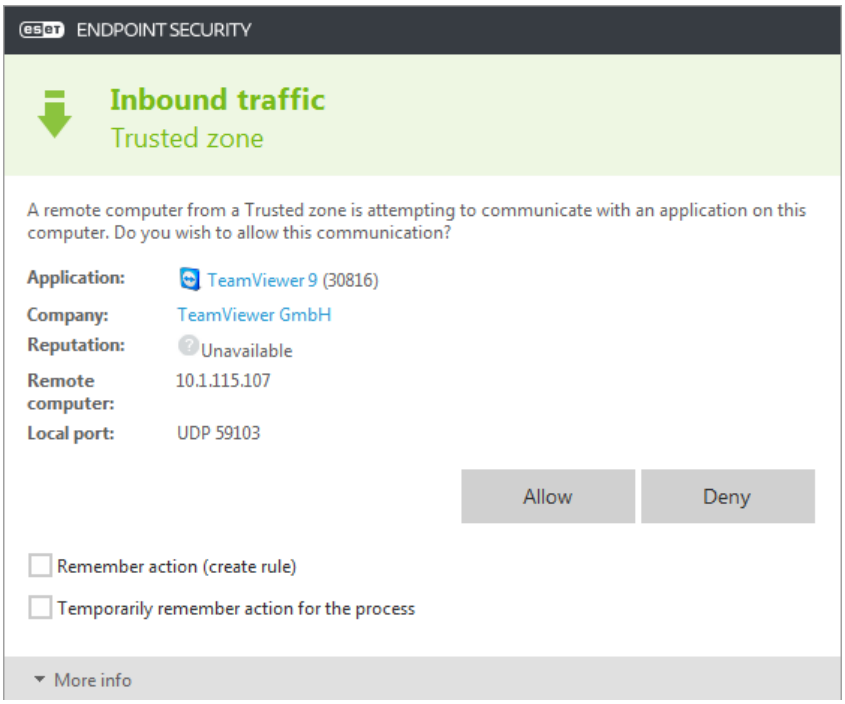
If your computer is showing symptoms of malware infection, for example it is slower, often freezes, we recommend that you do the following:

1. In the main program window, click **Computer scan**.
2. Click **Smart scan** to begin scanning your system.
3. After the scan has finished, review the log with the number of scanned, infected and cleaned files.
4. If you want to only scan a certain part of your disk click **Custom scan** and select targets to be scanned for viruses.

For additional information please see our regularly updated ESET Knowledgebase article.

### 3.8.5 How to allow communication for a certain application

If a new connection is detected in interactive mode and if there is no matching rule, you will be prompted to allow or deny the connection. If you want ESET Endpoint Security to perform the same action every time the application attempts to establish a connection, select the **Remember action (create rule)** check box.




You can create new Personal firewall rules for applications before they are detected by ESET Endpoint Security in the Personal firewall setup window, located under **Advanced setup** > **Personal firewall** > **Basic** > **Rules** by clicking **Edit**.

Click **Add** to add the rule. In the **General** tab, enter the name, direction and communication protocol for the rule. This window allows you to define the action to be taken when the rule is applied.

Enter the path to the application's executable and the local communication port in the **Local** tab. Click the **Remote** tab to enter the remote address and port (if applicable). The newly-created rule will be applied as soon as the application tries to communicate again.

### 3.8.6 How to create a new task in Scheduler

To create a new task in **Tools** > **Scheduler**, click **Add task** or right-click and select **Add...** from the context menu. Five types of scheduled tasks are available:

- **Run external application** – Schedules the execution of an external application.
- **Log maintenance** - Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** – Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** – Creates an ESET SysInspector computer snapshot – gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan** – Performs a computer scan of files and folders on your computer.
- **First scan** – By default, 20 minutes after installation or reboot a Computer scan will be performed as a low priority task.
- **Update** – Schedules an Update task by updating the virus signature database and program modules.

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

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

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

In the next step, a summary window with information about the current scheduled task is displayed. Click **Finish** when you are finished making changes.

A dialog window will appear, allowing you to select the profiles to be used for the scheduled task. Here you can set the primary and alternative profile. The alternative profile is used if the task cannot be completed using the primary profile. Confirm by clicking **Finish** and the new scheduled task will be added to the list of currently scheduled tasks.

### 3.8.7 How to schedule a scan task (every 24 hours)

To schedule a regular task, open the main program window and click **Tools** > **Scheduler**. Below, you can find a short guide on how to schedule a task that will scan your local drives every 24 hours.

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 **Repeatedly**.
4. Choose to run the task every 24 hours.
5. Select an action to perform if the scheduled task execution fails for any reason.
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.

### 3.8.8 How to connect ESET Endpoint Security to ESET Remote Administrator

When you have installed ESET Endpoint Security on your computer and you want to connect via ESET Remote Administrator, make sure that you have also installed ERA Agent on your client workstation. ERA Agent is an essential part of every client solution that communicates with ERA Server. ESET Remote Administrator uses the RD Sensor tool to search for computers on the network. Every computer on your network that is detected by RD Sensor is displayed in the Web Console.

Once the Agent is deployed, you can perform remote installation of ESET security products on your client computer. The exact steps for remote installation are described in the ESET Remote Administrator User Guide.

### 3.8.9 How to configure a mirror

ESET Endpoint Security can be configured to store copies of virus signature update files and distribute updates to other workstations that are running ESET Endpoint Security or ESET Endpoint Antivirus.

**Configuring ESET Endpoint Security as a Mirror server to provide updates via an internal HTTP server**

Press **F5** to access Advanced setup and expand **Update** > **Basic**. Make sure the **Update server** is set to **AUTOSELECT**. Select **Create update mirror** and **Provide update files via internal HTTP server** from **Advanced setup** > **Basic** > **Mirror**.

**Configuring a Mirror server to provide updates via a shared network folder**

Create a shared folder on a local or network device. This folder must be readable by all users running ESET security solutions and writable from the local SYSTEM account. Activate **Create update mirror** under **Advanced setup** > **Basic** > **Mirror**. Browse and select the created shared folder.

**NOTE**: If you do not want to update via internal HTTP server disengage **Provide update files via internal HTTP server**.

### 3.8.10 How do I upgrade to Windows 10 with ESET Endpoint Security

We highly recommend that you upgrade to the latest version of your ESET product, then download the latest virus signature database, before upgrading to Windows 10. This will ensure maximum protection and preserve your program settings and license information during the upgrade to Windows 10.

**Version 6.x and later:**

Click the appropriate link below to download and install the latest version to prepare for your upgrade to Microsoft Windows 10:

Download ESET Endpoint Security 6 32-bit  Download ESET Endpoint Antivirus 6 32-bit

Download ESET Endpoint Security 6 64-bit  Download ESET Endpoint Antivirus 6 64-bit

**Version 5.x and earlier:**

Click the appropriate link below to download and install the latest version to prepare for your upgrade to Microsoft Windows 10:

Download ESET Endpoint Security 5 32-bit  Download ESET Endpoint Antivirus 5 32-bit

Download ESET Endpoint Security 5 64-bit  Download ESET Endpoint Antivirus 5 64-bit

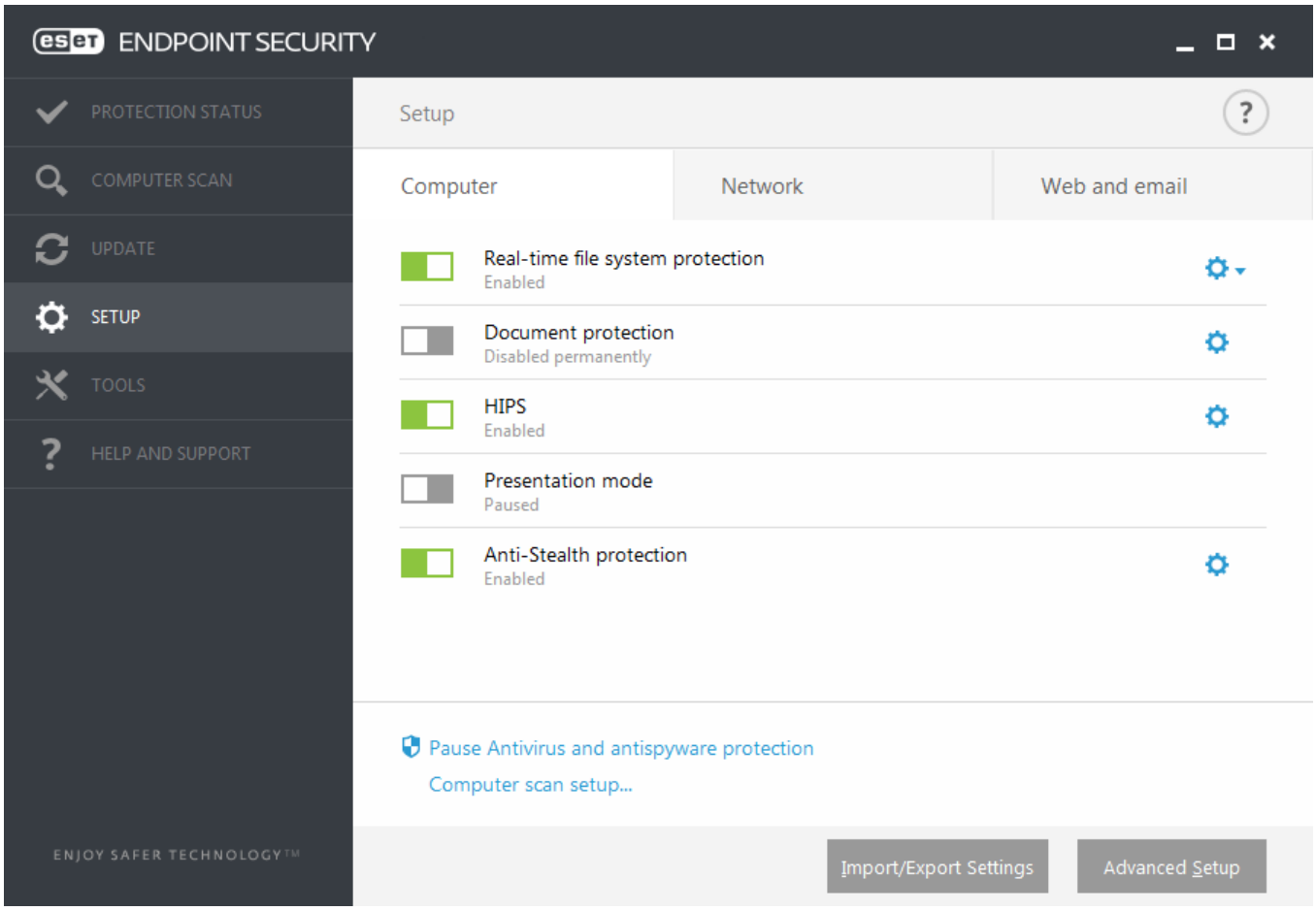
**Other language versions:**

If you are looking for another language version of your ESET endpoint product, please visit our download page.

**NOTE**: More information about compatibility of ESET products with Windows 10.

## 3.9 Work with ESET Endpoint Security

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




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

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

**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.
- **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.
- **HIPS** – The HIPS system monitors events that occur within the operating system and reacts to them according to a customized set of rules.
- **Presentation mode** – A feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. You will receive a warning message (potential security risk) and the main program window will turn orange after enabling Presentation mode.
- **Anti-Stealth protection** – Provides 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.

The **Network** section allows you to enable or disable the **Personal firewall**.

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

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

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

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

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

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

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

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

### 3.9.1 Computer

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

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

**NOTE:** Document protection status may not be available until you enable it in **Advanced setup** (F5) > **Antivirus** > **Document protection**. After you enable it, you need to restart your computer from Setup pane > Computer by clicking **Restart** under Device control or you can do it from Protection status pane by clicking **Restart computer**.

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

**Computer scan setup...** – Click to adjust the parameters of the computer scan (manually executed scan).

#### 3.9.1.1 Antivirus

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

To configure Antivirus module settings in detail, click **Advanced Setup** or press **F5**.

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

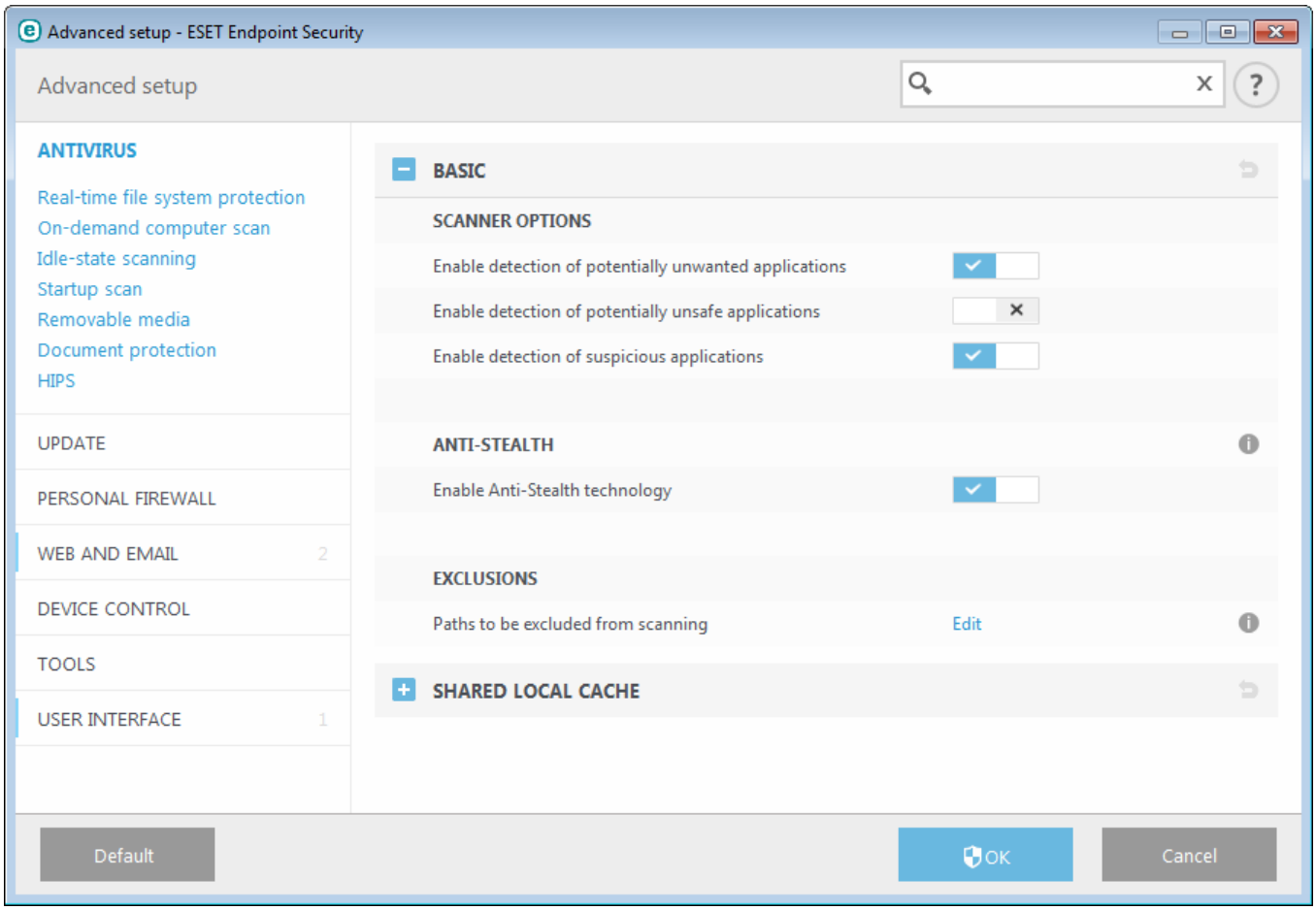
- **Potentially unwanted applications** (PUAs) are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way.
  Read more about these types of applications in the glossary.
- **Potentially unsafe applications** refers to legitimate commercial software 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.




### 3.9.1.1.1 An infiltration is detected

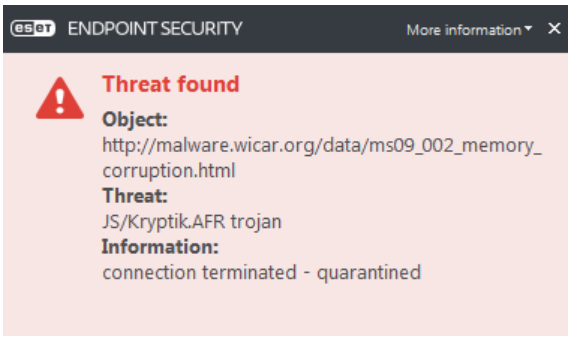
Infiltrations can reach the system from various entry points such as webpages, shared folders, via email or from removable devices (USB, external disks, CDs, DVDs, diskettes, etc.).

**Standard behavior**

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

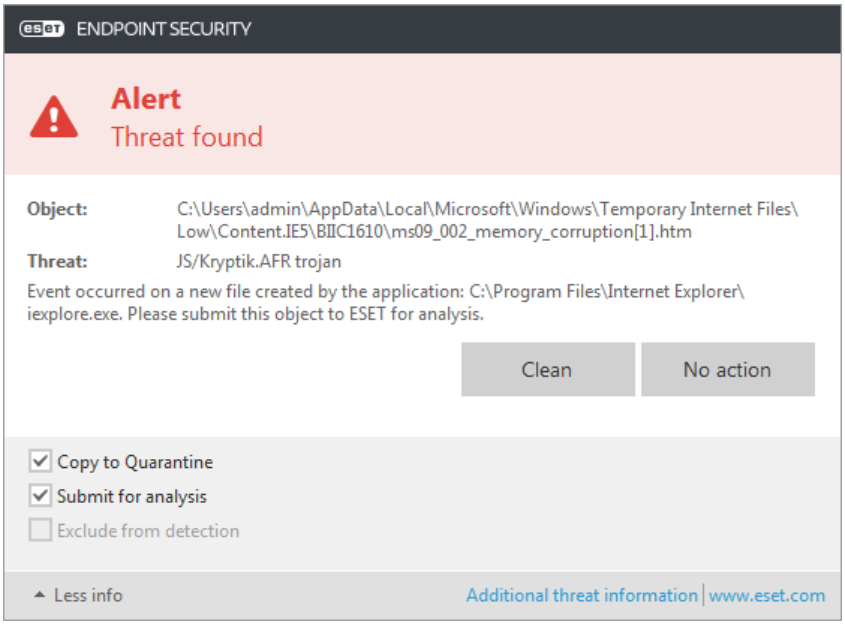
- Real-time file system protection
- Web access protection
- Email client protection
- On-demand computer scan

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




### Cleaning and deleting

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




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

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

### Multiple threats

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

### Deleting files in archives

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

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

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

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

### 3.9.1.2 Shared local cache

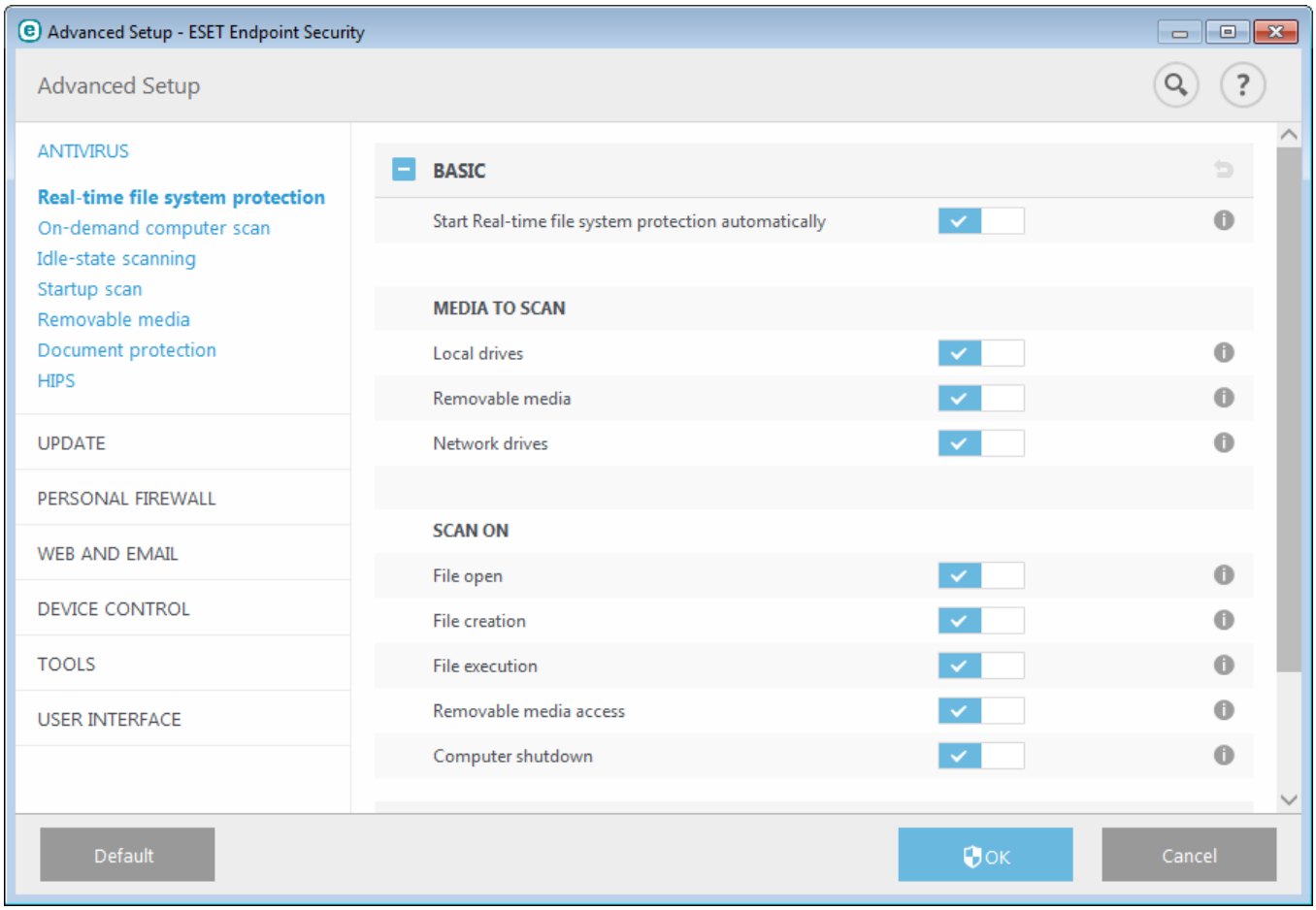
Shared local cache will boost performance in virtualized environments by eliminating duplicate scanning in the network. This ensures that each file will be scanned only once and stored in the shared cache. Turn on the **Caching option** switch to save information about scans of files and folders on your network to the local cache. If you perform a new scan, ESET Endpoint Security will search for scanned files in the cache. If files match, they will be excluded from scanning.

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

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

### 3.9.1.3 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 **Start Real-time file system protection automatically** 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.
- **Computer shutdown** – Enables or disables scanning triggered by computer shutdown.

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 virus signature database 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 **Antivirus** > **Real-time file system protection**. Click **ThreatSense parameter** > **Other** and select or deselect **Enable Smart optimization**.

#### 3.9.1.3.1 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. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before the virus signature database update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, disable **Default archive scan settings**.

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

**Additional ThreatSense parameters for executed files** – By default, Advanced heuristics is used when files are executed. When enabled, we strongly recommend keeping Smart optimization and ESET LiveGrid® enabled to mitigate impact on system performance.

#### 3.9.1.3.2 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 (Standard 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.

#### 3.9.1.3.3 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file is available for download at http://www.eicar.org/download/eicar.com

**NOTE:** Before performing a real-time protection check, it is necessary to disable the firewall. If the firewall is enabled, it will detect the file and prevent test files from downloading. Make sure that you re-enable the firewall immediately following your check of real-time file system protection.

#### 3.9.1.3.4 When to modify real-time protection configuration

Real-time file system protection is the most essential component for maintaining a secure system. Always be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases.

After installing ESET Endpoint Security, all settings are optimized to provide the maximum level of system security for users. To restore default settings, click ↩ next to each tab in the window (**Advanced setup** > **Antivirus** > **Real-time file system protection**).

#### 3.9.1.3.5 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 **Real-time file system protection**.

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

**If Real-time protection does not detect and clean infiltrations**

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

**Real-time protection does not start**

If real-time protection is not initiated at system startup (and **Start Real-time file system protection automatically** is enabled), it may be due to conflicts with other programs. For assistance resolving this issue, please contact ESET Customer Care.

### 3.9.1.4 On-demand computer scan

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

Two types of **Computer scan** are available. **Smart scan** quickly scans the system with no need for further configuration of the scan parameters. **Custom scan** allows you to select any of the predefined scan profiles and define specific scan targets.

See Scan progress for more information about the scanning process.

**Smart scan**

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

**Custom scan**

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

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

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

**Removable media scan**

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

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

You can use the **Action after scan** drop-down menu to choose the action (No action, Shut down and Reboot) to be performed after scanning.

**Enable shutdown after scan** – Enables a scheduled shutdown when the on-demand computer scan finishes. A shutdown confirmation dialog window will display a 60-second countdown. Click **Cancel** to deactivate the requested shutdown.

**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**.

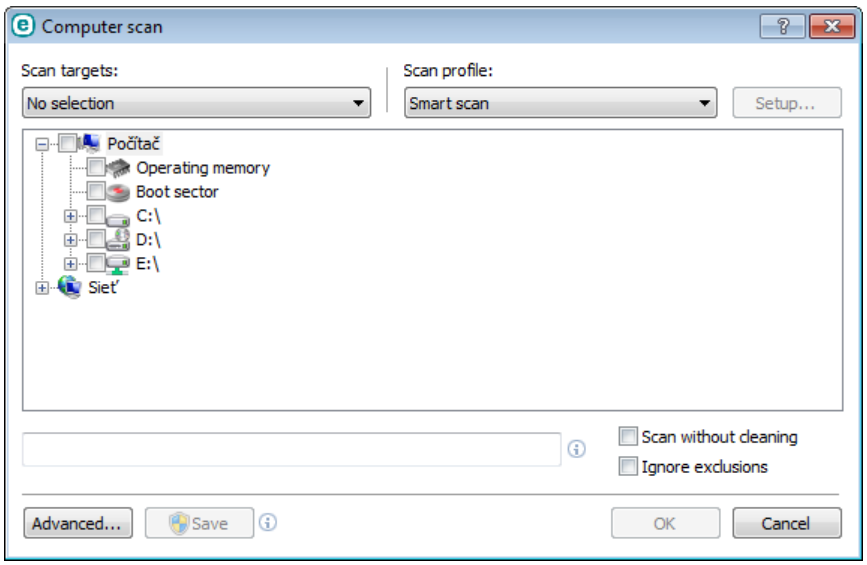
### 3.9.1.4.1 Custom scan launcher

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

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

- **By profile settings** – Selects targets set in the selected scan profile.
- **Removable media** – Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** – Selects all system hard drives.
- **Network drives** – Selects all mapped network drives.
- **No selection** – Cancels all selections.

To quickly navigate to a scan target or to directly add a desired target (folder or file(s)), enter it in the blank field below the folder list. This is only possible if no targets were selected in the tree structure and the **Scan targets** menu is set to **No selection**.




Infected items are not cleaned automatically. Scanning without cleaning can be used to obtain an overview of the current protection status. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. Furthermore, you can choose from three cleaning levels by clicking **Setup...** > **ThreatSense parameters** > **Cleaning**. Information about scanning is saved to a scan log.

You can choose a profile from the **Scan profile** drop-down menu to be used for scanning chosen targets. The default profile is **Smart scan**. There are two more pre-defined scan profiles called **In-depth scan** and **Context menu scan**. These scan profiles use different ThreatSense engine parameters. Click **Setup...** to set up chosen scan profile from the Scan profile menu in detail. The available options are described under section **Other** in ThreatSense engine parameters setup.

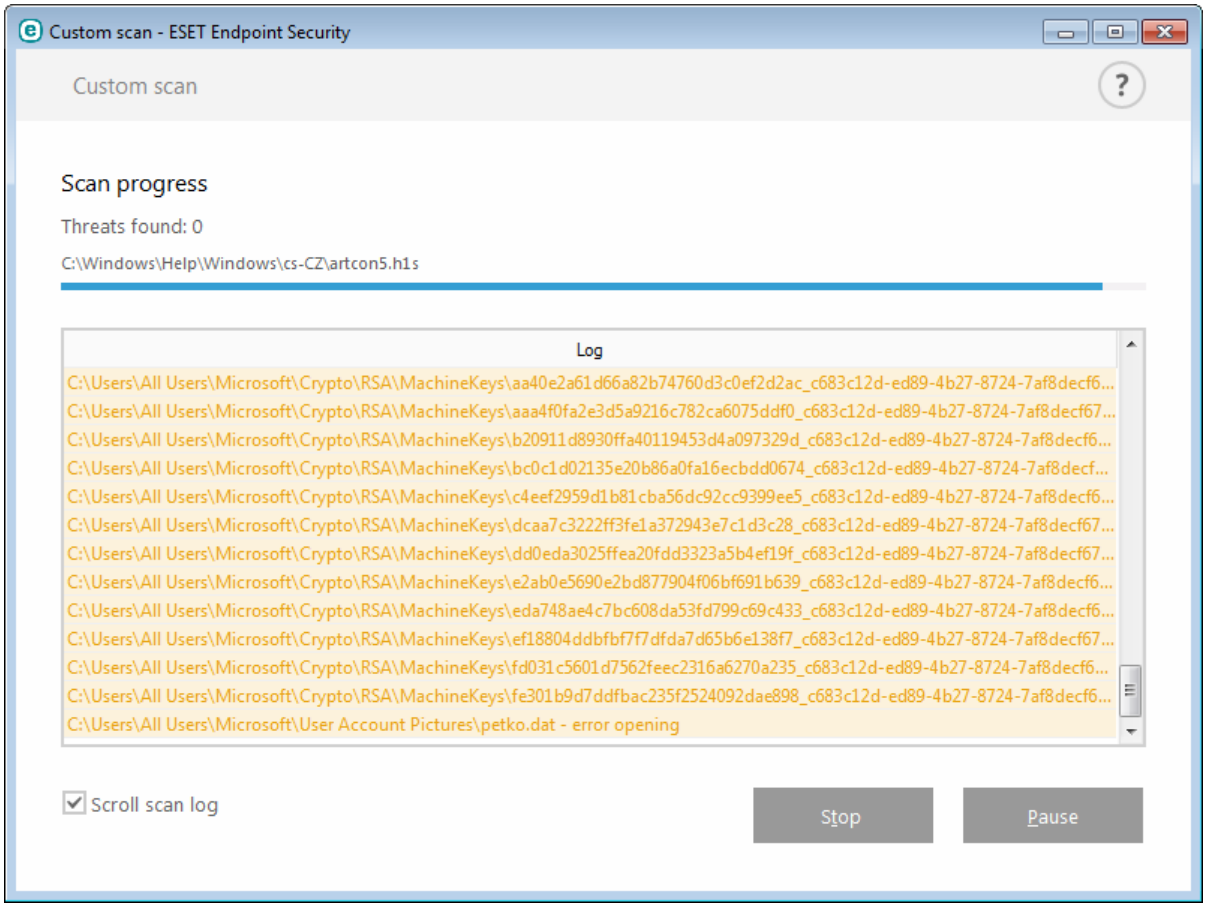
Click **Save** to save changes made to your target selection, including selections made within the folder tree structure.

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

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

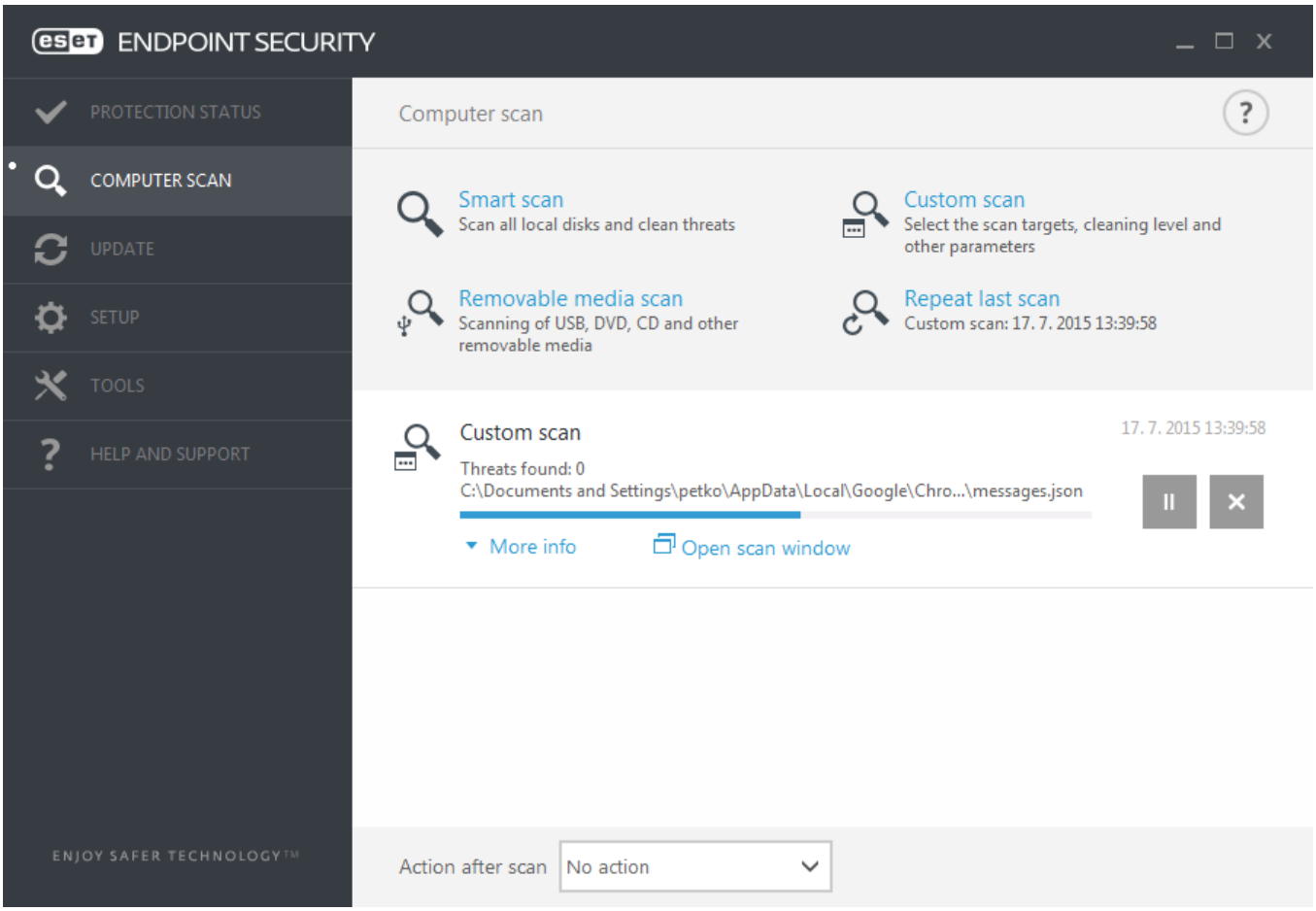
### 3.9.1.4.2 Scan progress

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 exclusively being used by the system (typically *pagefile.sys* and certain log files), cannot be scanned.

**Scan progress** – The progress bar shows the status of already-scanned objects compared to objects still waiting be scanned. The scan progress status is derived from the total number of objects included in scanning.
**Target** – The name of the currently scanned object and its location.
**Threats found** – Shows the total number of threats found during a scan.
**Pause** – Pauses a scan.
**Resume** – This option is visible when scan progress is paused. Click **Resume** to continue scanning.
**Stop** – Terminates the scan.
**Scroll scan log** – If enabled, the scan log will scroll down automatically as new entries are added so that the most recent entries are visible.




### 3.9.1.5 Device control

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

**Supported external devices:**

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

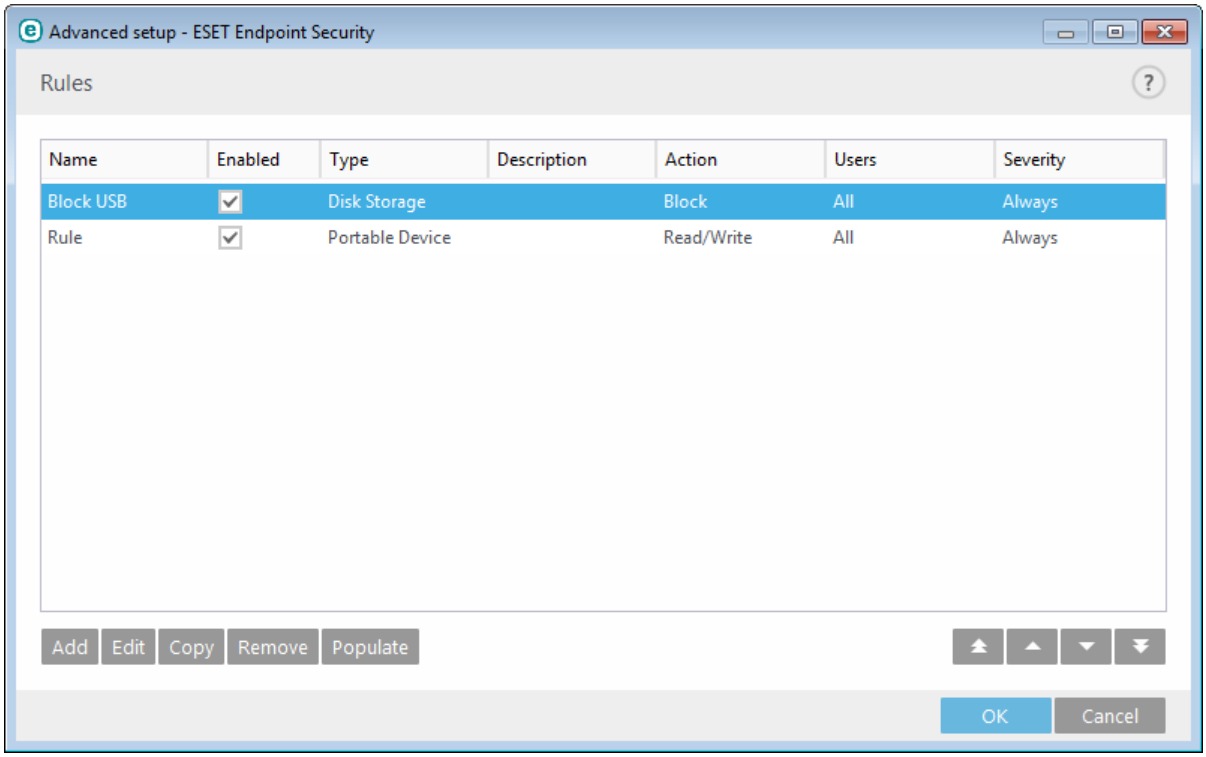
Device control setup options can be modified in **Advanced setup** (F5) > **Device control**.

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

If a device blocked by an existing rule is inserted, a notification window will be displayed and access to the device will not be granted.

### 3.9.1.5.1 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.




Specific devices can be allowed or blocked according to their user, user group, or any of several additional parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as name, type of external device, action to perform after connecting an external device to your computer and log severity.

Click **Add** or **Edit** to manage a rule. Deselect the **Enabled** check box next to a rule to disable it until you want to use it in the future. Select one or more rules and click **Remove** to delete the rule(s) permanently.

**Copy** – Creates a new rule with predefined options used for another selected rule.

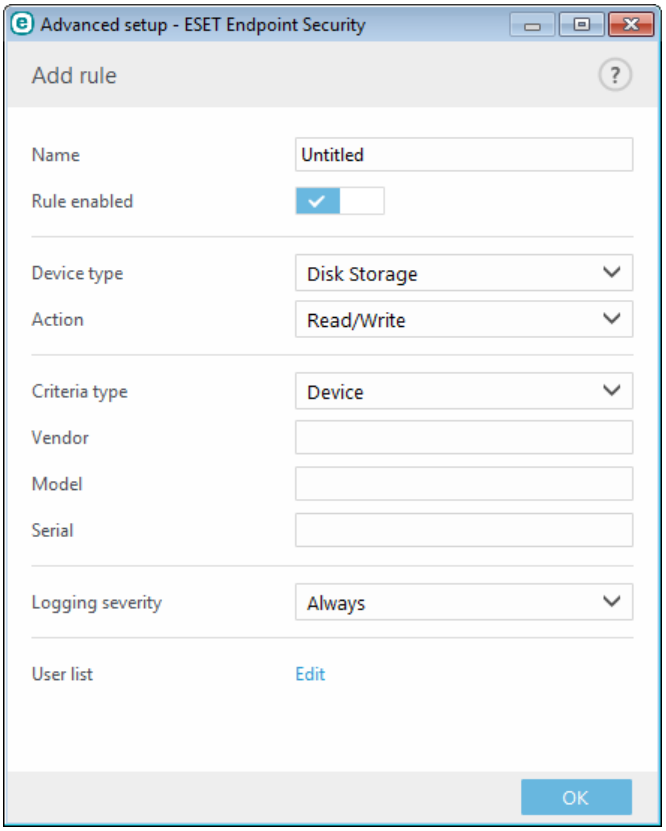
Click **Populate** to auto-populate removable media device parameters for devices connected to your computer.

Rules are listed in order of priority with higher-priority rules closer to the top. Rules can be moved by clicking **Top/Up/Down/Bottom** and can be moved individually or in groups.

The Device control log records all occurrences where Device control is triggered. Log entries can be viewed from the main program window of ESET Endpoint Security in **Tools** > **Log files**.

### 3.9.1.5.2 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 allowed/blocked, and a log entry will be made. Devices are not remembered, a notification will still be displayed upon subsequent connections of the same device.

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

**Criteria type** – Select **Device group** or **Device.**

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

**TIP:** 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.

**Severity**

- **Always** – Logs all events.
- **Diagnostic** – Logs information needed to fine-tune the program.
- **Information** – Records informative messages, including successful update messages, plus all records above.
- **Warning** – Records critical errors and warning messages.
- **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**: Not all devices can be filtered by user rules, (for example imaging devices do not provide information about users, only about actions).

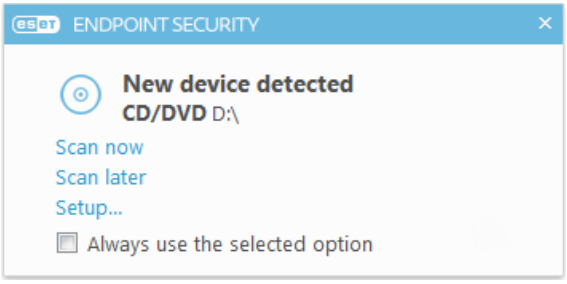
### 3.9.1.6 Removable media

ESET Endpoint Security 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:




**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 Endpoint Security features the Device control functionality, which allows you to define rules for the use of external devices on a given computer. More details on Device control can be found in the Device control section.

#### 3.9.1.7 Idle-state scanning

You can enable the idle-state scanner in **Advanced setup** under **Antivirus** > **Idle-state scanning** > **Basic**. 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. See Idle state detection triggers for a full list of conditions that must be met in order to trigger the idle-state scanner.

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 will run when your computer is in the following states:

- Turn off screen or screen saver
- Computer lock
- User logoff

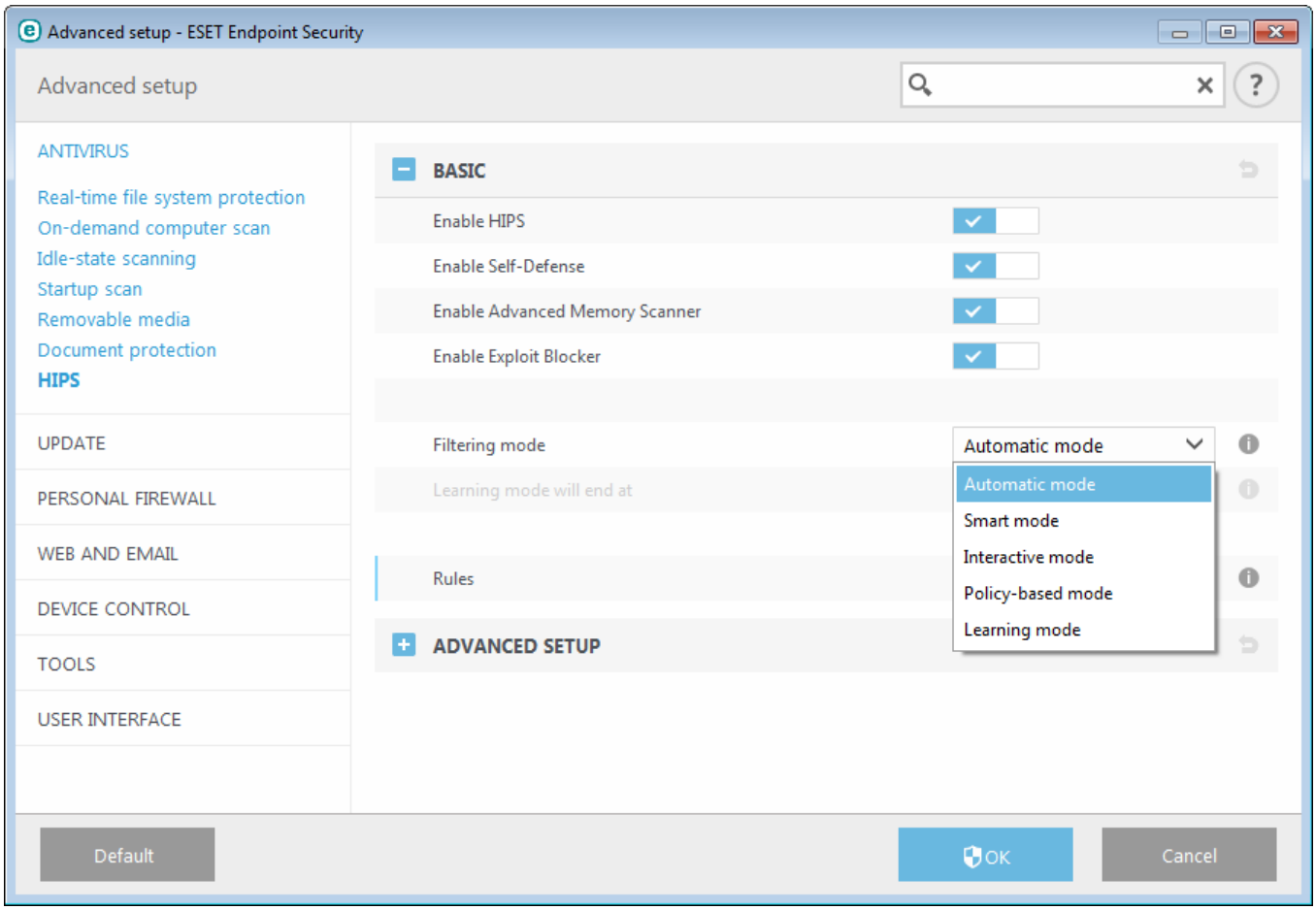
Click ThreatSense engine parameter setup to modify scan parameters (for example, detection methods) for the Idle-state scanner.

#### 3.9.1.8 Host-based Intrusion Prevention System (HIPS)


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

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

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




ESET Endpoint Security uses built-in Self-defense technology to prevent malicious software from corrupting or disabling your antivirus and antispyware protection, so you can be sure your system is protected at all times. It is necessary to restart Windows to disable HIPS or Self-Defense.

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

**Exploit Blocker** is 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.

Filtering 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.

**Interactive mode** – User will be prompted to confirm operations.

**Policy-based mode** – Operations are blocked.

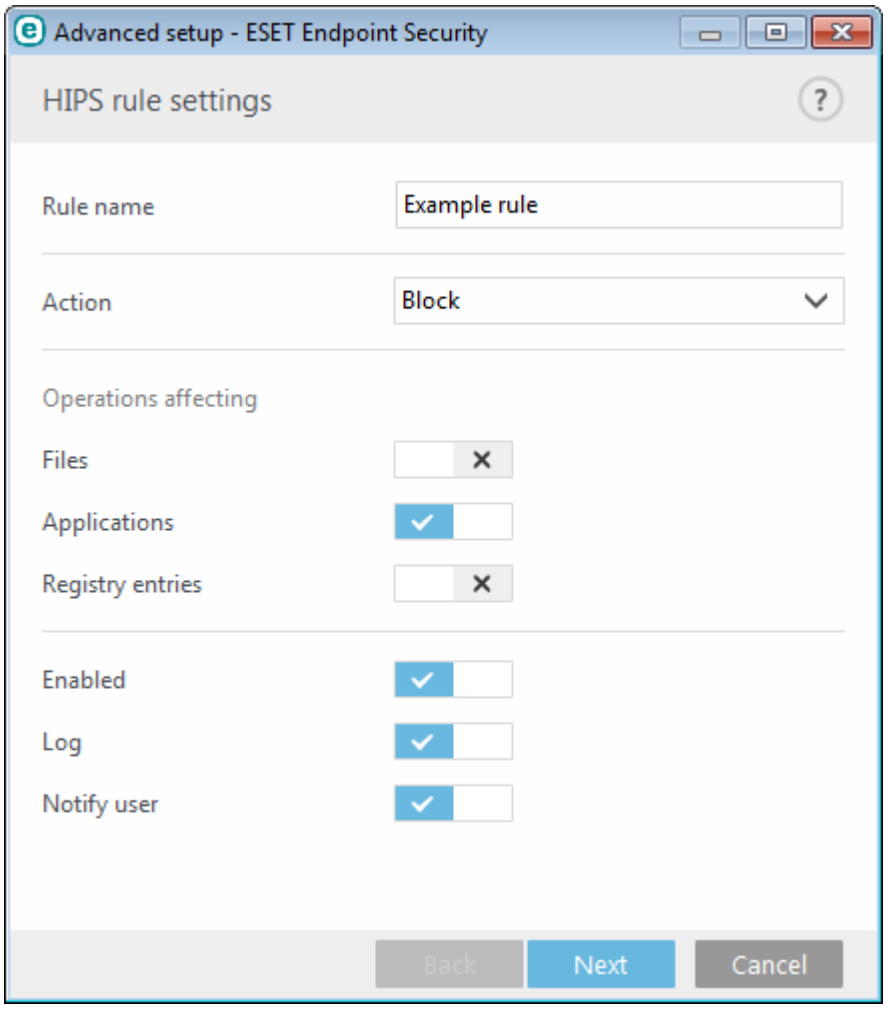
**Learning mode** – Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the Rule editor, but their priority is lower than the priority of rules created manually or rules created in the automatic mode. When you select Learning mode from the HIPS Filtering mode drop down menu, the **Learning mode will end at** setting will become available. Select the duration that you want to engage learning mode, 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.

**Smart mode** – The user will only be notified about very suspicious events.

The HIPS system monitors events inside the operating system and reacts accordingly based on rules similar to the rules used by the personal firewall. Click **Edit** to open the HIPS rule management window. Here you can select, create, edit or delete rules.

In the following example, we will demonstrate how to restrict unwanted behavior of applications:

1. Name the rule and select **Block** 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 for which the rule will be applied. In the **Source applications** window, select **All 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.
4. Select **Modify state of another application** (all operations are described in product help, which can be accessed by pressing F1).
5. Select **Specific applications** from the drop-down menu and **Add** one or several applications you want to protect.
6. Click **Finish** to save your new rule.




### 3.9.1.8.1 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.

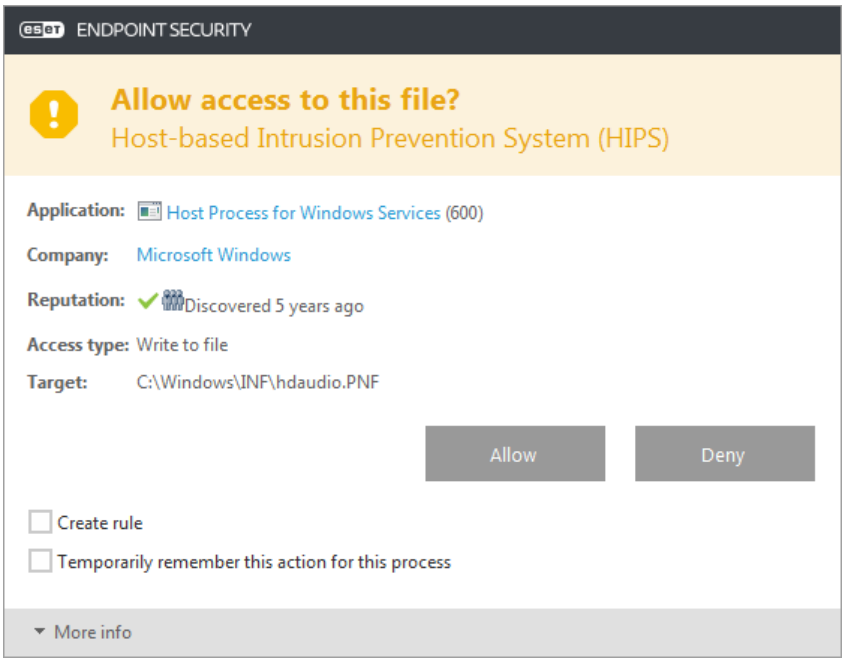
**Log all blocked operations** – All blocked operations will be written to the HIPS log.

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

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

#### 3.9.1.8.2 HIPS interactive window

If the default action for a rule is set to **Ask**, 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.




The dialog window allows you to create a rule based on any new action that HIPS detects and then define the conditions under which to allow or deny that action. Settings for the exact parameters can be accessed by clicking **More info**. Rules created like this are considered equal to rules created manually, so a rule created from a dialog window can be less specific than the rule that triggered that dialog window. This means that after creating such a rule, the same operation can trigger the same window.

**Temporarily remember this action for this process** 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.

### 3.9.1.9 Presentation mode

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

Click **Setup** > **Computer** and then click the switch next to **Presentation mode** to enable presentation mode manually. In **Advanced setup** (F5), click **Tools** > **Presentation mode**, and then click the switch next to **Enable Presentation mode when running applications in full-screen mode automatically** to have ESET Endpoint Security engage Presentation mode automatically when full-screen applications are run. Enabling Presentation mode is a potential security risk, so the protection status icon in the taskbar will turn orange and display a warning. You will also see this warning in the main program window where you will see **Presentation mode enabled** in orange.

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

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

**NOTE:** If the Personal firewall is in Interactive mode and Presentation mode is enabled, you might have trouble connecting to the Internet. This can be problematic if you start a game that connects to the Internet. Normally, you

would be asked to confirm such an action (if no communication rules or exceptions have been defined), but user interaction is disabled in Presentation mode. The solution is to define a communication rule for every application that might be in conflict with this behavior or to use a different Filtering mode in the Personal firewall. Keep in mind that if Presentation mode is enabled and you go to a webpage or an application that might be a security risk, it may be blocked but you will not see any explanation or warning because user interaction is disabled.

#### 3.9.1.10 Startup scan

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

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

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

##### 3.9.1.10.1 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.

#### 3.9.1.11 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 are not exposed to a high volume of Microsoft Office documents.

**Integrate into system** activates the protection system. To modify this option, press F5 to open the Advanced setup window and click **Antivirus** > **Document protection** in the Advanced setup tree.

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

### 3.9.1.12 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. 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 (for example, backup software).

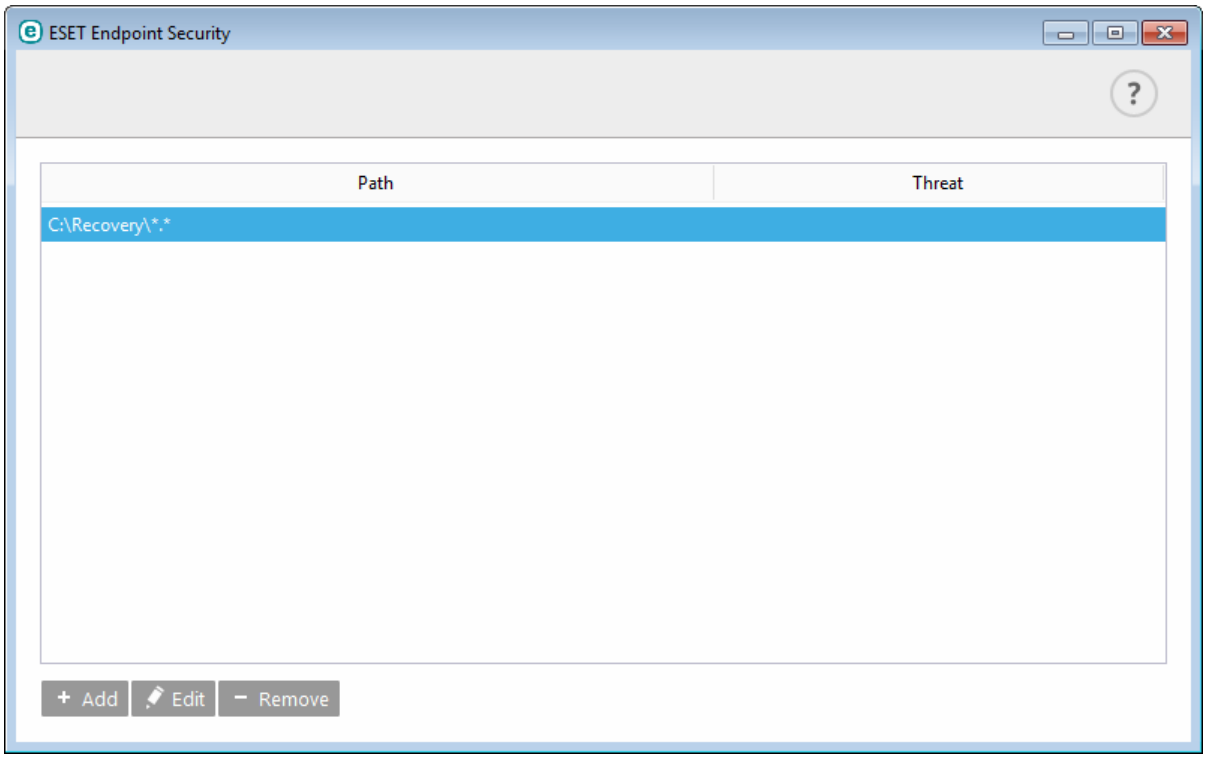
To exclude an object from scanning:

1. Click **Add**,
2. Enter the path to an object or select it in the tree structure.

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.




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

**Columns**

**Path** – Path to excluded files and folders.

**Threat** – If the name of a threat is displayed next to an excluded file, it means that the file is only excluded for the given threat. 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 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,** right-clicking the quarantined file and then selecting **Restore and exclude from detection** from the context menu.

**Control elements**

**Add** – Excludes objects from detection.

**Edit** – Enables you to edit selected entries.

**Remove** – Removes selected entries.

### 3.9.1.13 ThreatSense engine parameters setup

ThreatSense is technology 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 the 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 engine parameter setup** 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, and 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 a 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** – Scans boot sectors for the presence of viruses in the master boot record.

**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 needing no specialized programs – archives – to decompress 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 known by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.

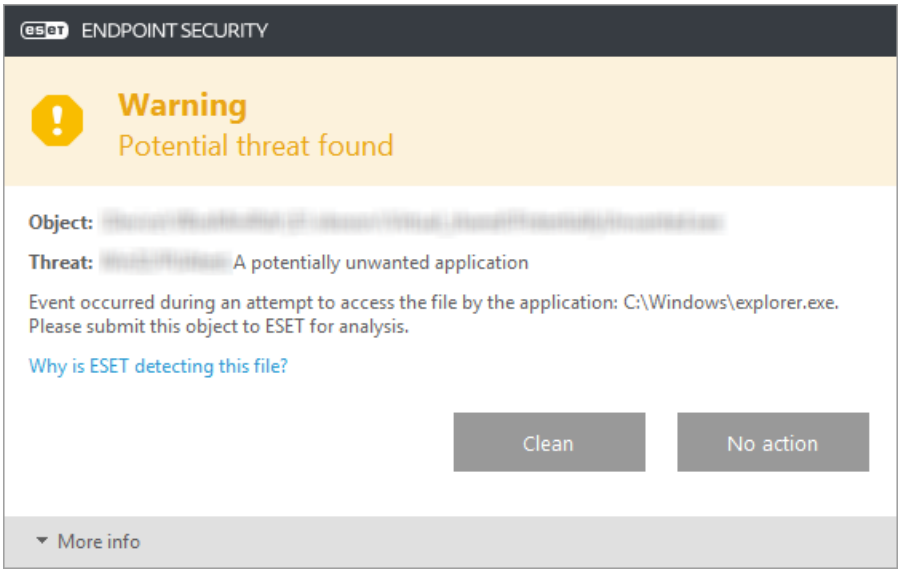
**Advanced heuristics/DNA/Smart signatures** – Advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high level programming languages. The use of advanced heuristics greatly increases the threat detection 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).

A potentially unwanted application is a program that contains adware, installs toolbars or has other unclear objectives. There are some situations where a user may feel that the benefits of a potentially unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software, such as trojan horses or worms.

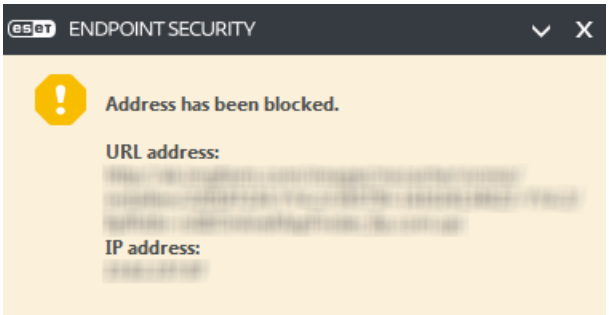
**Warning - Potential threat found**

When a potentially unwanted application is detected, you will be able to decide which action to take:

1. **Clean/Disconnect**: This option ends the action and prevents the potential threat from entering your system.
2. **No action**: This option allows a potential threat to enter your system.
3. To allow the application to run on your computer in the future without interruption, click **More info/Show advanced options** and then select the check box next to **Exclude from detection**.

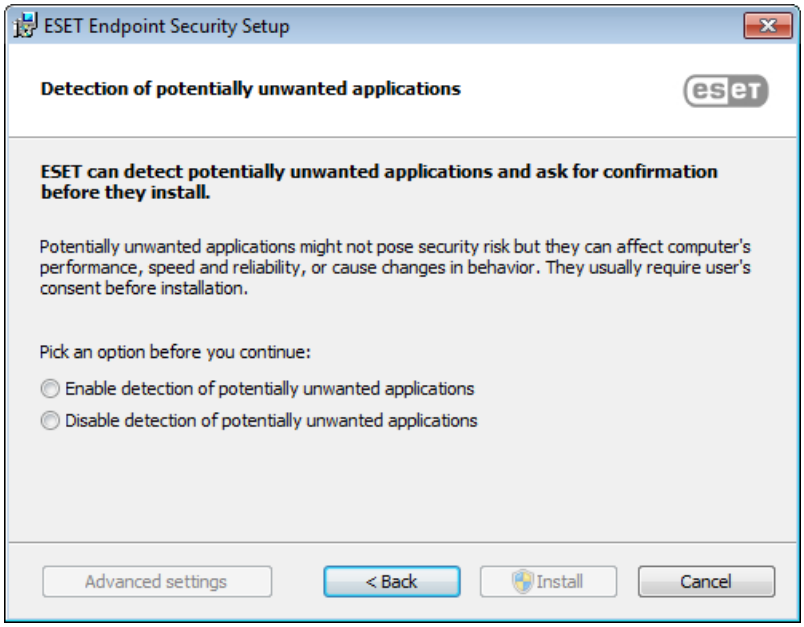



When a potentially unwanted application is detected and it is unable to clean, a notification window **Address has been blocked** will show at the bottom right corner of the screen. For more information about this event navigate to **Tools** > **Log files** > **Filtered websites** from the main menu.



### Potentially unwanted applications - Settings

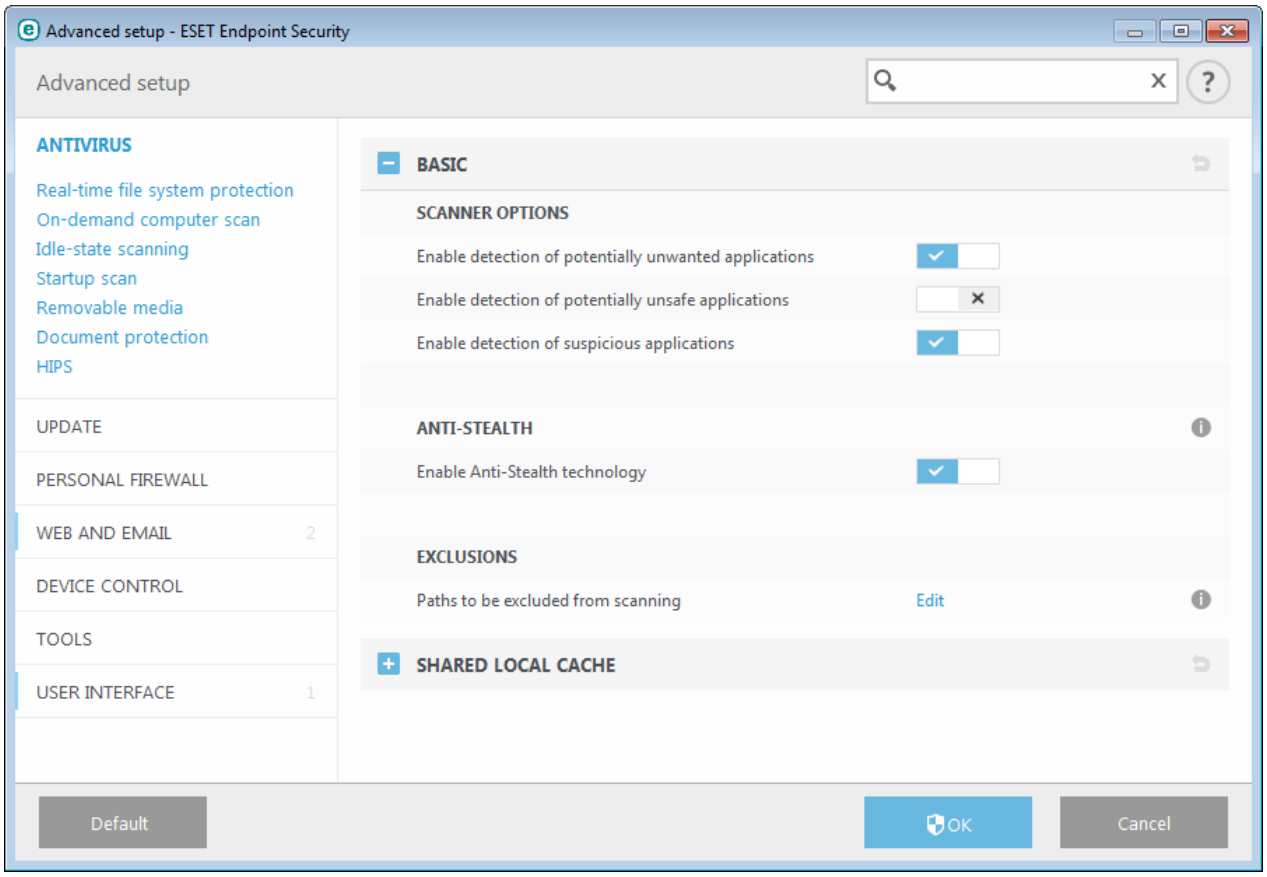
While installing your ESET product, you can decide whether to enable detection of potentially unwanted applications, as shown below:




Potentially unwanted applications may install adware, toolbars, or contain other unwanted and unsafe program features.

These settings can be modified in your program settings at any time. To enable or disable the detection of Potentially unwanted, unsafe or suspicious applications, follow these instructions:

1. Open your ESET product. How do I open my ESET product?
2. Press the **F5** key to access **Advanced setup**.
3. Click **Antivirus** and enable or disable options **Enable detection of potentially unwanted applications**, **Enable detection of potentially unsafe applications** and **Enable detection of suspicious applications** according to your preferences. Confirm by clicking **OK**.




**Potentially unwanted applications - Software wrappers**

A software wrapper is a special type of application modification that is used by some file-hosting websites. It is a third-party tool that installs the program you intended to download but adds additional software, such as toolbars or adware. The additional software may also make changes to your web browser's home page and search settings. Also, file-hosting websites often do not notify the software vendor or download recipient that modifications have been made and do not easily allow opting out of modification. For these reasons, ESET classifies software wrappers as a type of potentially unwanted application to allow users to accept the download or not.

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

**Potentially unsafe applications** – Potentially unsafe applications is the classification used for commercial, legitimate programs such as remote access tools, password-cracking applications and keyloggers (programs that record each keystroke typed by a user). This option is disabled by default.

**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 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 (Standard 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.

#### 3.9.1.13.1 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.

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.

Using the **Add** and **Remove** buttons, you can allow or prohibit the scanning of specific file extensions. To add a new extension to the list, click **Add** type the extension into the blank field and click **OK**. When you select **Enter multiple values**, you can add multiple file extensions delimited by lines, commas or semicolons. When multiple selection is enabled, extensions will be shown in the list. Select an extension in the list and click **Remove** to delete that extension from the list. If you want to edit a selected extension click **Edit**.

The special symbol ? (question mark) can be used. The question mark represents any symbol.

**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.

### 3.9.2 Network

The Personal firewall controls all network traffic to and from the system. This is accomplished by allowing or denying individual network connections based on your filtering rules. It provides protection against attacks from remote computers and blocks some potentially dangerous services. The Personal firewall also provides IDS/IPS functionality by inspecting the content of allowed network traffic and blocking traffic that is deemed potentially harmful.

**Personal firewall** configuration can be found in the **Setup** pane under **Network**. Here you can adjust the filtering mode for the ESET Personal firewall. You can also access more detailed settings by clicking the gear wheel > **Configure** next to **Personal firewall**, or by pressing **F5** to access Advanced setup.

**Network attack protection (IDS)** – Analyses the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked. You can disable Network attack protection for a specific period of time by clicking .

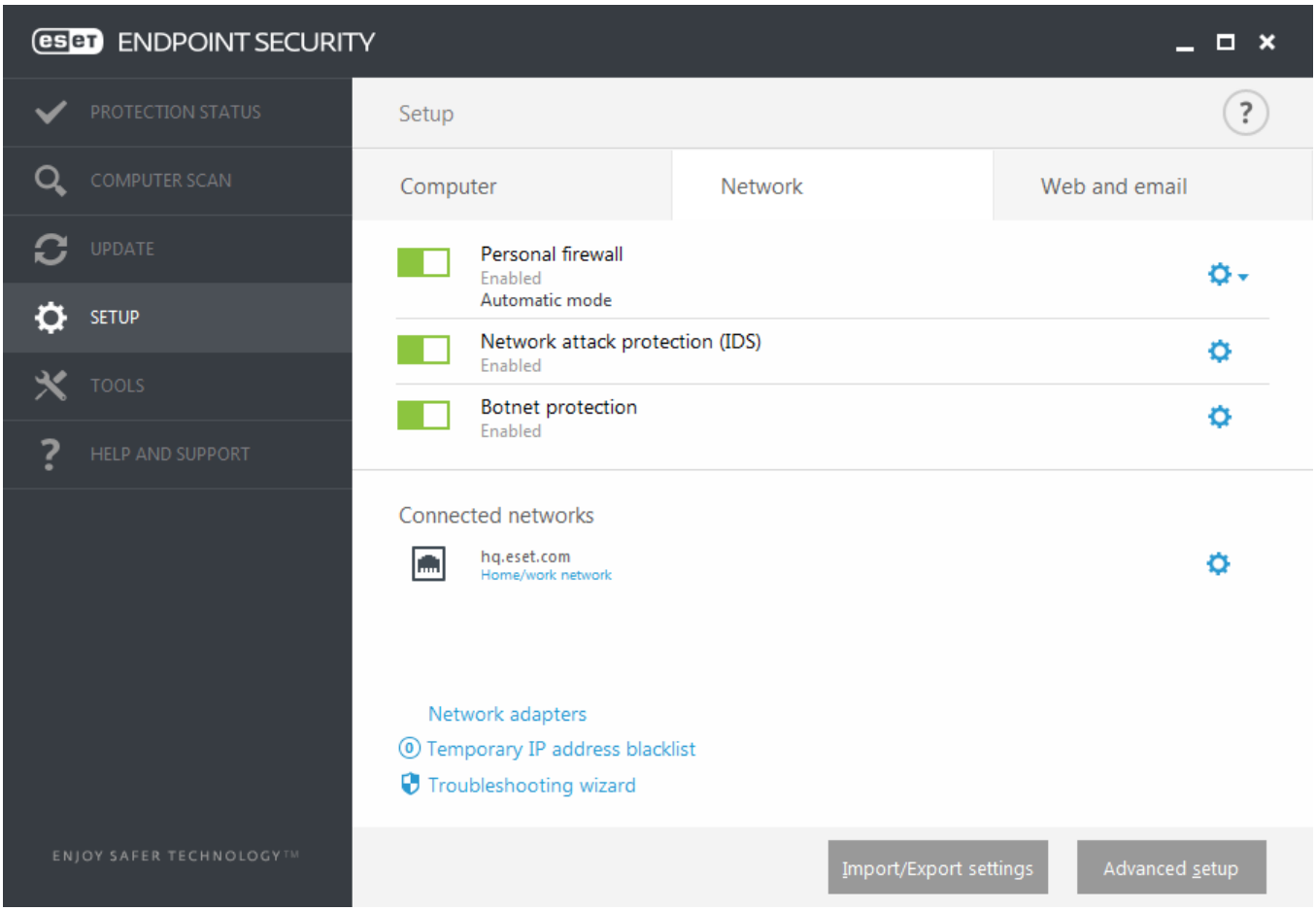
**Botnet protection** – Quickly and accurately spots malware on the system. You can disable Botnet protection for a specific period of time by clicking .

**Connected networks** – Shows the networks to which network adapters are connected. After clicking the gear wheel, you will be prompted to select a protection type for the network you are connected to via your network adapter.

**Network adapters** – Here you can see each network adapter and its assigned firewall profile and trusted zone. For more detailed information, see Network adapters.

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

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




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

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

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

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

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

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

### 3.9.2.1 Personal firewall

The Personal firewall controls all network traffic to and from the system. This is accomplished by allowing or denying individual network connections based on specified filtering rules. It provides protection against attacks from remote computers and enables blocking of some services. It also provides antivirus protection for HTTP, POP3 and IMAP protocols. This functionality represents a very important element of computer security.

**Enable Network attack protection (IDS)** – Analyses the content of network traffic and protects from network attacks. Any traffic which is considered harmful will be blocked.

**Enable Botnet protection** – Detects and blocks communication with malicious command and control servers based on typical patterns when the computer is infected and a bot is attempting to communicate.

Four filtering modes are available for the ESET Endpoint Security Personal firewall. Filtering mode settings can be

found in **Advanced setup** (F5) by clicking **Personal firewall**. The behavior of the firewall changes based on the filtering mode. Filtering modes also influence the level of user interaction required.

Filtering can be performed in one of four modes:

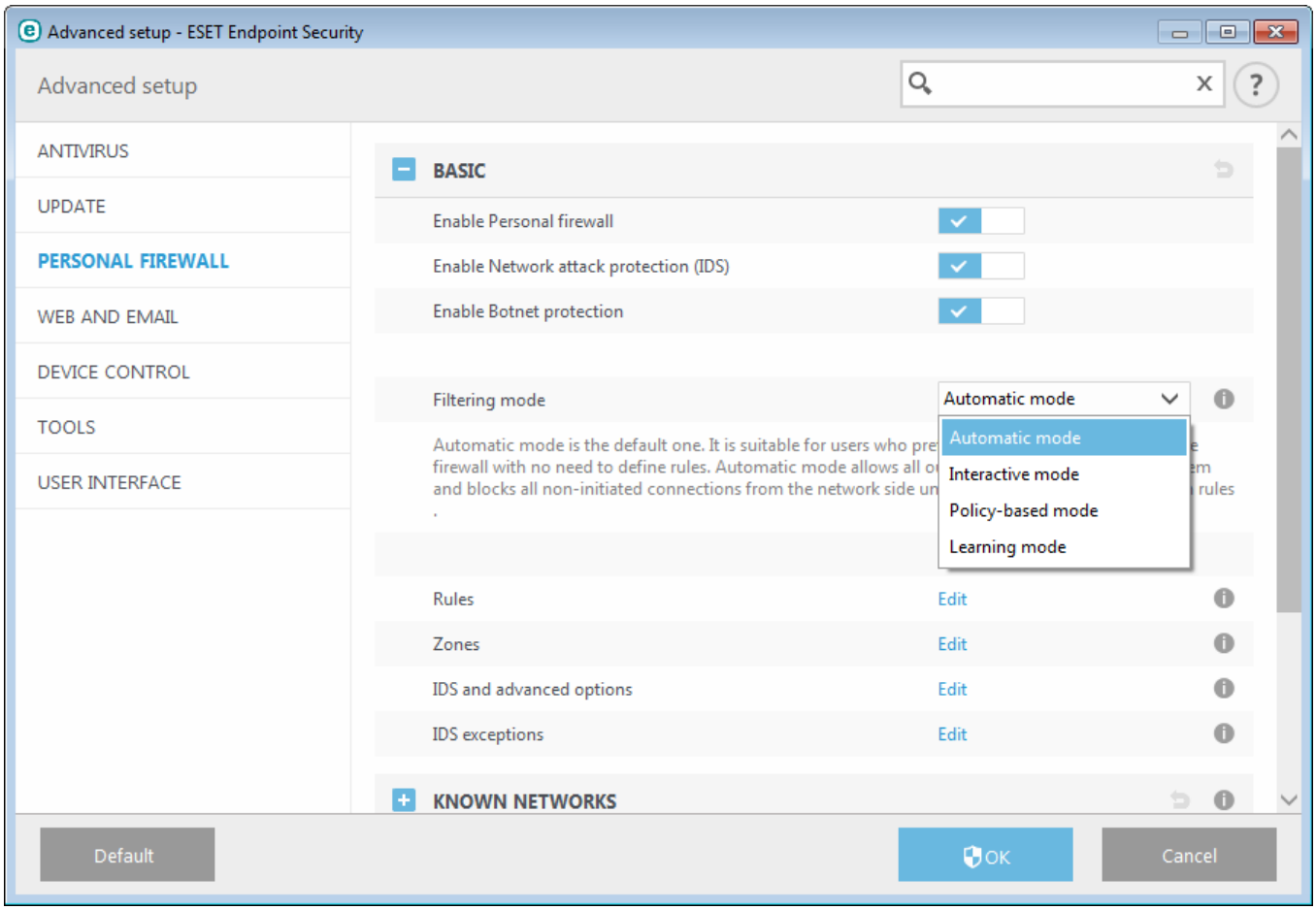
**Automatic mode** – The default mode. This mode is suitable for users who prefer easy and convenient use of the firewall with no need to define rules. Custom, user-defined rules can be created, but are not required in Automatic mode. Automatic mode allows all outbound traffic for the given system and blocks most inbound traffic (except some traffic from the Trusted Zone, as allowed in IDS and advanced option/Allowed services and inbound traffic responding to recent outbound communication to the same remote site).

**Interactive mode** – Allows you to build a custom configuration for your Personal firewall. When a communication is detected and no existing rules apply to that communication, a dialog window reporting an unknown connection will be displayed. The dialog window gives the option to allow or deny the communication, and the decision to allow or deny can be saved as a new rule for the Personal firewall. If you choose to create a new rule, all future connections of this type will be allowed or blocked according to that rule.

**Policy-based mode** – Blocks all connections that are not defined by a specific rule that allows them. This mode allows advanced users to define rules that permit only desired and secure connections. All other unspecified connections will be blocked by the Personal firewall.

**Learning mode** – Automatically creates and saves rules; this mode is suitable for initial configuration of the Personal firewall. No user interaction is required, because ESET Endpoint Security saves rules according to predefined parameters. Learning mode is not secure, and should only be used until all rules for required communications have been created.

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




**Rules** – Here you can add rules and define how the Personal firewall handles network traffic.

**Zones** – Here you can create zones that consist of several IP addresses.

**IDS and advanced options** – Allows you to configure advanced filtering options and the IDS functionality (used to

detect several types of attacks and exploits).

**IDS exceptions** – Allows you to add IDS exceptions and customize reactions to malicious activities.

#### 3.9.2.1.1 Learning mode

Learning mode automatically creates and saves a rule for each communication that has been established in the system. No user interaction is required, because ESET Endpoint Security saves rules according to the predefined parameters.

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

Activate Learning mode in **Advanced setup** (F5) > **Personal Firewall** > **Learning mode settings** to display Learning mode options. This section includes the following items:

***Warning:*** While in Learning mode, the Personal firewall does not filter communication. All outgoing and incoming communications are allowed. In this mode, your computer is not fully protected by the Personal firewall.

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

**Inbound traffic from the Trusted zone** – An example of an incoming connection within the trusted zone would be a remote computer from within the trusted zone attempting to establish communication with a local application running on your computer.

**Outbound traffic to the Trusted zone** – A local application attempting to establish a connection to another computer within the local network, or within a network in the trusted zone.

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

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

Each section allows you to define parameters to be added to newly created rules:

**Add local port** – Includes the local port number of the network communication. For outgoing communications, random numbers are usually generated. For this reason, we recommend enabling this option only for incoming communications.

**Add application** – Includes the name of the local application. This option is suitable for future application-level rules (rules that define communication for an entire application). For example, you can enable communication only for a web browser or email client.

**Add remote port** – Includes the remote port number of the network communication. For example you can allow or deny a specific service associated with a standard port number (HTTP – 80, POP3 – 110, etc.).

**Add remote IP address/Trusted zone** – A remote IP address or zone can be used as a parameter for new rules defining all network connections between the local system and that remote address / zone. This option is suitable if you want to define actions for a certain computer or a group of networked computers.

**Maximum number of different rules for an application** – If an application communicates through different ports to various IP addresses, etc., the firewall in learning mode creates appropriate count of rules for this application. This option allows you to limit the number of rules that can be created for one application.

### 3.9.2.2 Firewall profiles

Profiles can be used to control the behavior of the ESET Endpoint Security Personal firewall. When creating or editing a Personal firewall rule, you can assign it to a specific profile, or have it apply to every profile. When a profile is active on a network interface, only the global rules (rules with no profile specified) and the rules that have been assigned to that profile are applied to it. You can create multiple profiles with different rules assigned to network adapters or assigned to networks to easily alter Personal firewall behavior.

Click **Edit** next to **List of profiles** to open the **Firewall Profiles** window where you can edit profiles.

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

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

#### 3.9.2.2.1 Profiles assigned to network adapters

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

**Columns**

**Name** – Name of the network adapter.

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

**Prefer network's profile** – When **Prefer connected network's firewall profile** enabled, the network adapter will use the firewall profile assigned to a connected network whenever possible.

**Control elements**

**Add** – Adds a new network adapter.

**Edit** – Allows you to edit an existing network adapter.

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

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

### 3.9.2.3 Configuring and using rules

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

Unlike the previous version of ESET Endpoint Security, rules are evaluated from top to bottom. The action of the first matching rule is used for each network connection being evaluated. This is an important behavioral change from the previous version, in which the priority of rules was automatic and more specific rules had higher priority then more general ones.

Connections can be divided into incoming and outgoing connections. Incoming connections are initiated by a

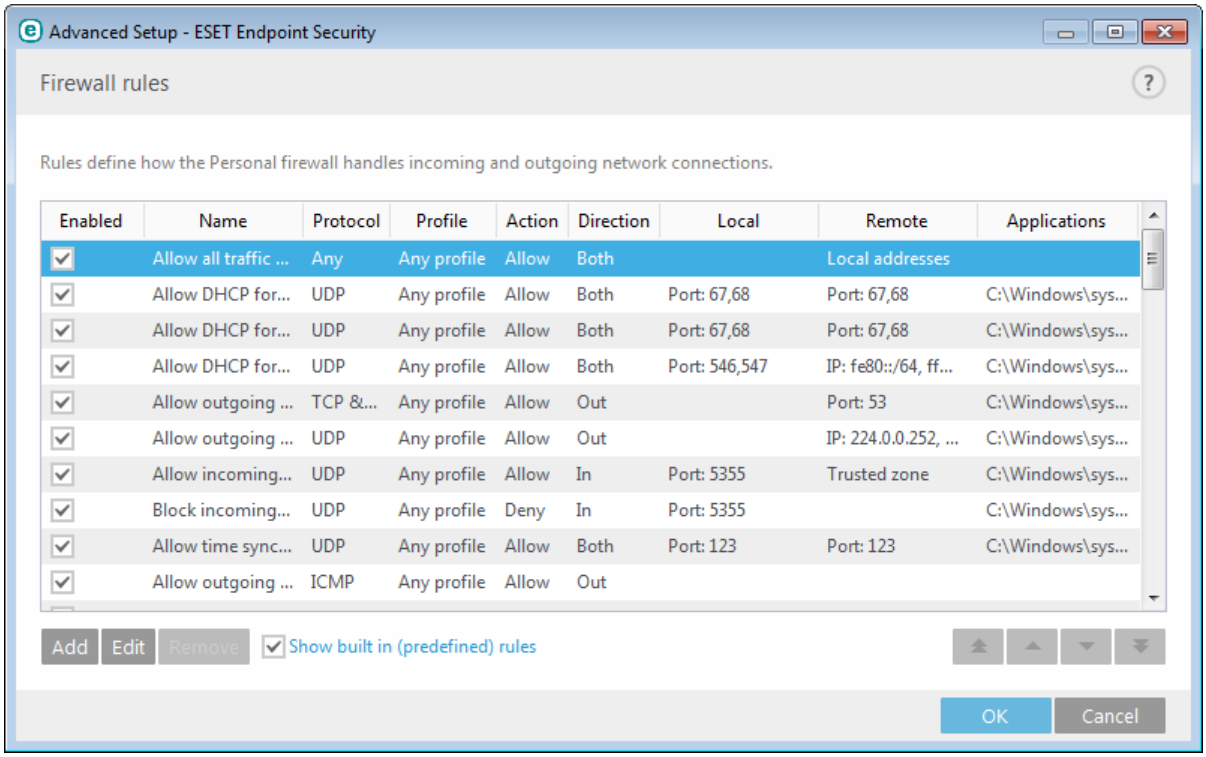
remote computer attempting to establish a connection with the local system. Outgoing connections work the opposite way – the local system contacts a remote computer.

If a new unknown communication is detected, consider carefully whether to allow or deny it. Unsolicited, unsecured or unknown connections pose a security risk to the system. If such a connection is established, we recommend that you pay particular attention to the remote computer and the application attempting to connect to your computer. Many infiltrations try to obtain and send private data, or download other malicious applications to host workstations. The Personal firewall allows you to detect and terminate such connections.

#### 3.9.2.3.1 Firewall rules

Click **Edit** next to **Rules** in the **Basic** tab section to display the **Firewall rules** window, where the list of all rules is displayed. **Add**, **Edit**, and **Remove** allow you to add, configure or delete rules. You can adjust the priority level of a rule by selecting a rule(s) and clicking **Top/Up/Down/Bottom**.

**TIP**: You can use the **Search** field to find a rule(s) by name, protocol or port.




**Columns**

**Name** – Name of rule.

**Enabled** – Shows if rules are enabled or disabled, the corresponding check box must be selected to activate a rule.

**Protocol** – The protocol this rule is valid for.

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

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

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

**Local** – IP address and port of local computer.

**Remote** – IP address and port of remote computer.

**Applications** – The application to which the rule applies.

**Control elements**

**Add** – Creates a new rule.

**Edit** – Allows you to edit existing rules.

**Remove** – Removes existing rules.

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

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

#### 3.9.2.3.2 Working with rules

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

The upper part of the window contains three tabs:

- **General** – Specify a rule name, the direction of the connection, the action (**Allow**, **Deny**, **Ask**), the protocol and the profile to which the rule will apply.
- **Local** – Displays information about the local side of the connection, including the number of the local port or port range and the name of the communicating application. Also allows you to add a predefined or created zone with a range of IP addresses here by clicking **Add**.
- **Remote** – This tab contains information about the remote port (port range). It allows you to define a list of remote IP addresses or zones for a given rule. You can also add a predefined or created zone with range of IP addresses here by clicking **Add**.

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

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

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

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

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

Below is an example in which we create a new rule to allow the web browser application to access the network. In this example, the following must be configured:

- In the **General** tab, enable outgoing communication via the TCP and UDP protocol.
- Add your browser application (for Internet Explorer it is iexplore.exe) in the **Local** tab.
- In the **Remote** tab, enable port number 80 if you want to allow standard Internet browsing.

**NOTE**: Please be aware that predefined rules can be modified in limited way.

### 3.9.2.4 Trusted zone

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

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

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

#### 3.9.2.5 Configuring zones

Zones are groups of IP addresses, useful when you need to reuse the same set of addresses in multiple rules. These zones can be configured in **Advanced setup** > **Personal firewall** > **Basic**, when click **Edit** button next to **Zones**. For adding a new zone click **Add** enter a **Name** for the zone, a **Description**, and add a remote IP address into the **Remote computer address (IPv4/IPv6, range, mask)** field.

In the **Firewall zones** setup window, you can specify a zone name, description, network address list (see also Known networks editor).

#### 3.9.2.6 Known networks

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

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

**NOTE**: When you engage **Automatically mark new networks as public**, the **New Network Connection Detected** dialog will not appear, and the network you are connected to will automatically be marked as public. This will cause certain features (for example file sharing and remote desktop) to become inaccessible from new networks.

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

##### 3.9.2.6.1 Known networks editor

Known networks can be configured manually in **Advanced setup** > **Personal firewall** > **Known Networks** by clicking **Edit**.

**Columns**

**Name** – Name of known network.

**Protection type** – Shows if the network is set to **Home/work** or **Public**.

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

**Control elements**

**Add** – Creates a new known network.

**Edit** – Click to edit an existing known network.

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

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

Network configuration settings are broken down into the following tabs:

### Network

Here you can define the network name and select the protection type (**Public** or **Home/work**) for the network. Use the **Firewall profile** drop-down menu to select the profile for this network. If the network uses the **Home/work** protection type, all directly connected network subnets are considered trusted. For example, if a network adapter is connected to this network with the IP address 192.168.1.5 and the subnet mask 255.255.255.0, the subnet 192.168.1.0/24 is added to that adapter's trusted zone. If the adapter has more addresses/subnets, all of them will be trusted, regardless of the **Network Identification** configuration of the known network.

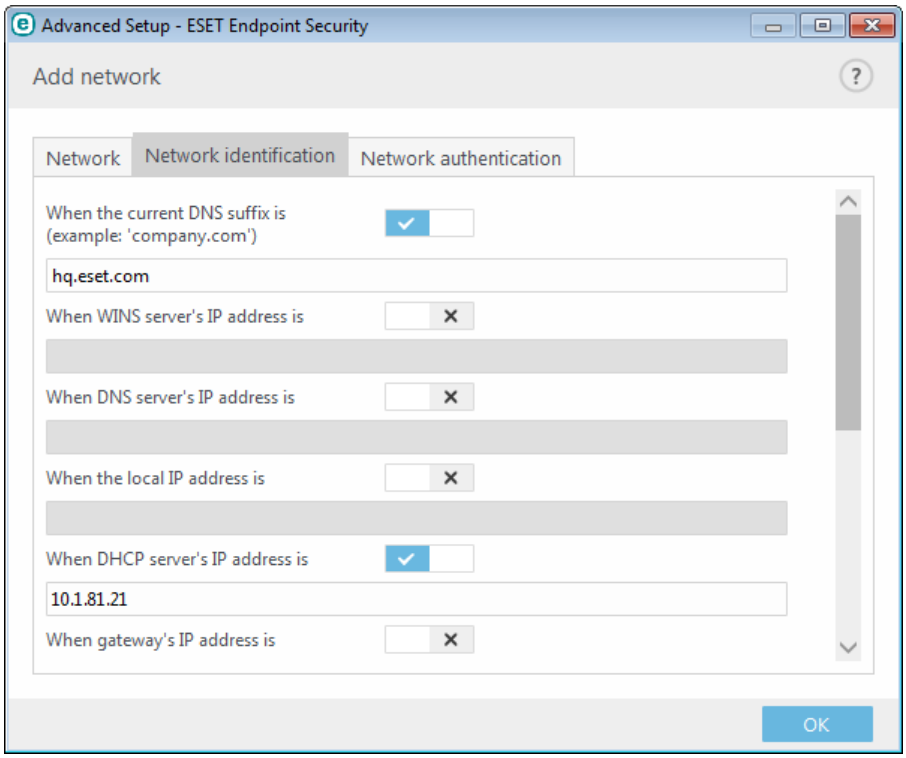
Additionally, addresses added under **Additional trusted addresses** are always added to the trusted zone of adapters connected to this network (regardless of the network's protection type).

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

- Network identification – All filled in parameters must match active connection parameters.
- Network authentication – if authentication server is selected, successful authentication with the ESET Authentication Server must take place.
- Network restrictions (Windows XP only) – all selected global restrictions must be fulfilled.

### Network identification

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

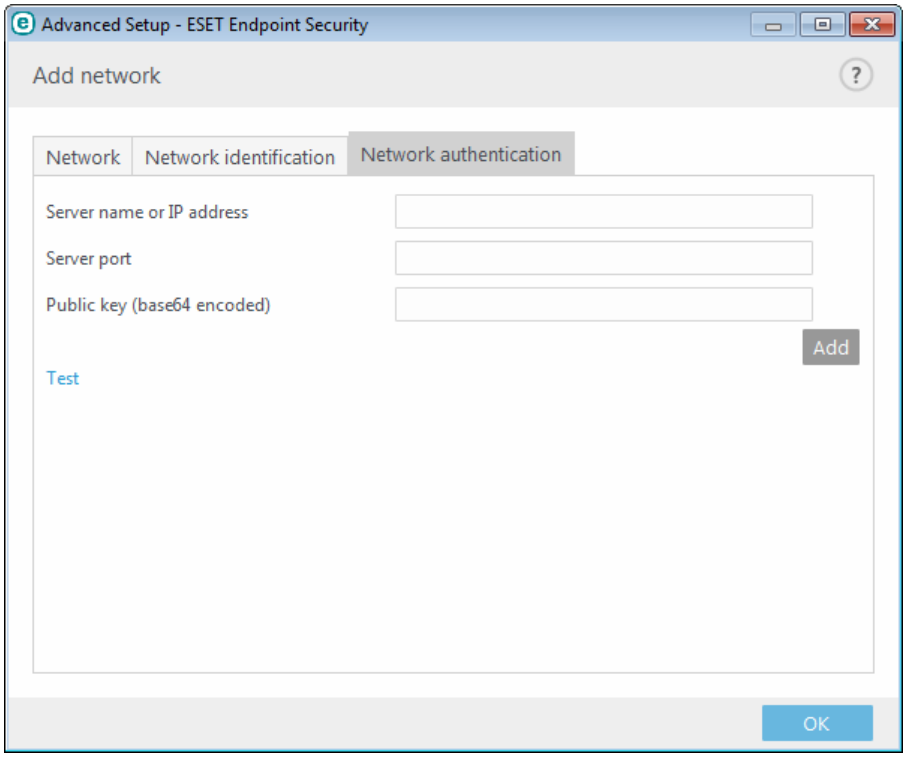



### Network authentication

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

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

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




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

*Server authentication failed. Invalid or mismatched signature.*
Server signature does not match the public key entered.

*Server authentication failed. Network name doesn't match.*
The configured network name does not correspond with the authentication server zone name. Review both names and ensure they are identical.

*Server authentication failed. Invalid or no response from server.*
No response is received if the server is not running or is inaccessible. An invalid response may be received if another HTTP server runs on the specified address.

*Invalid public key entered.*
Verify that the public key file you have entered is not corrupted.

**Network restrictions** (for Windows XP only)

On modern operating systems (Windows Vista and newer), each network adapter has its own trusted zone and active firewall profile. Unfortunately on Windows XP this layout is not supported, so all network adapters always share the same trusted zone and active firewall profile. That imposes a potential security risk when the machine is connected to multiple networks simultaneously. In such cases, traffic from an untrusted network may be evaluated using the trusted zone and firewall profile configured for the other connected network. To mitigate any security risk, you can use the following restrictions to avoid globally applying one network configuration while another (potentially untrusted) network is connected.

On Windows XP, connected networks settings (trusted zone and firewall profile) are applied globally unless at least one of these restrictions is enabled and not fulfilled:

a. Only one connection is active
b. No wireless connection is established
c. No unsecured wireless connection is established

#### 3.9.2.6.2 Network authentication - Server configuration

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

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

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

### 3.9.2.7 Logging

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

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

- **Time** – Date and time of event.
- **Event** – Name of event.
- **Source** – Source network address.
- **Target** – Target network address.
- **Protocol** – Network communication protocol.
- **Rule/worm name** – Rule applied, or name of worm, if identified.
- **Application** – Application involved.
- **User** – Name of the user logged in at the time the infiltration was detected.

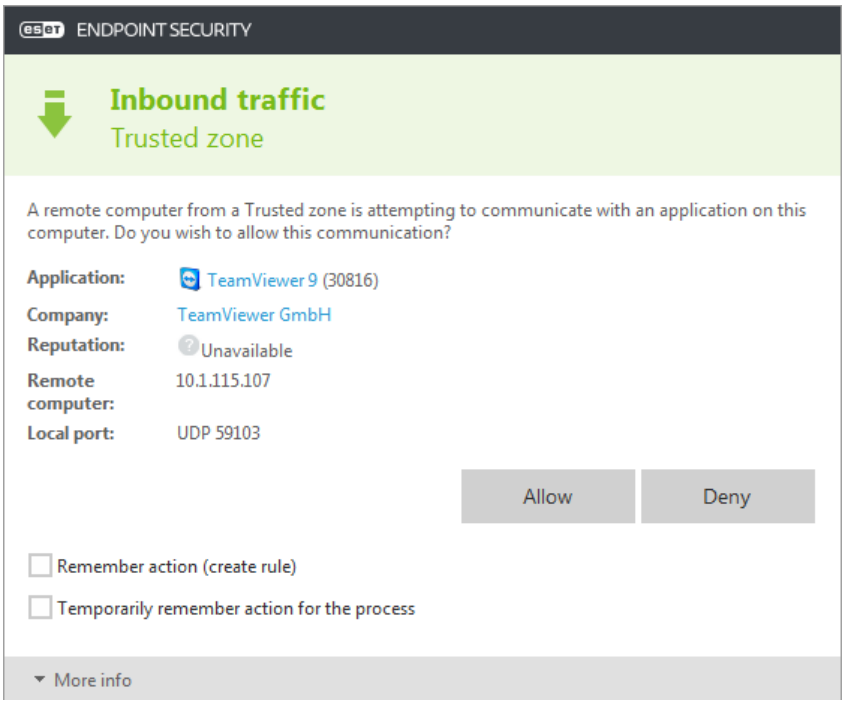
A thorough analysis of this data can help detect attempts to compromise system security. Many other factors indicate potential security risks and allow you to minimize their impact. Some examples of potential threat indicators include frequent connections from unknown locations, multiple attempts to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

### 3.9.2.8 Establishing connection - detection

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

Interactive mode displays an informational window that reports detection of a new network connection, supplemented with detailed information about the connection. You can opt to allow the connection or refuse (block) it. If you repeatedly allow the same connection in the dialog window, we recommend that you create a new rule for the connection. To do this, select **Remember action (create rule)** and save the action as a new rule for the Personal firewall. If the firewall recognizes the same connection in the future, it will apply the existing rule without requiring user interaction.

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




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

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

In order to proliferate, computer infiltrations often use the Internet and hidden connections to help them infect remote systems. If rules are configured correctly, a Personal firewall becomes a useful tool for protection against a variety of malicious code attacks.

### 3.9.2.9 Solving problems with ESET Personal firewall

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

See the following topics for help resolving problems with the ESET Personal firewall:

- Troubleshooting wizard
- Logging and creating rules or exceptions from log
- Creating exceptions from firewall notifications
- Advanced PCAP logging
- Solving problems with protocol filtering

#### 3.9.2.9.1 Troubleshooting wizard

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

#### 3.9.2.9.2 Logging and creating rules or exceptions from log

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

For more information about the log see Log files.

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

##### 3.9.2.9.2.1 Create rule from log

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

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

- set the minimum logging verbosity to **Diagnostic** in **Advanced setup** (F5) > **Tools** > **Log files**,
- enable **Display notifications also for incoming attacks against security holes** in **Advanced setup** (F5) > **Personal firewall** > **IDS and advanced options** > **Intrusion detection**.

#### 3.9.2.9.3 Creating exceptions from Personal firewall notifications

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

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

#### 3.9.2.9.4 Advanced PCAP logging

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

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

- Microsoft Windows Vista or newer

  *C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics*

- Microsoft Windows XP

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

#### 3.9.2.9.5 Solving problems with protocol filtering

If you experience problems with your browser or email client, the first step is to determine if protocol filtering is responsible. To do that, try temporarily disabling application protocol filtering in the advanced setup (remember to turn it back on after you're finished, otherwise your browser and email client will remain unprotected). If your problem disappears after turning it off, here is a list of common problems and a way to solve them:

**Update or secure communication problems**

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

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

**Problem accessing a device on your network**

If you are unable to use any functionality of a device on your network (this could mean opening a webpage of your webcam or playing video on a home media player), try adding its IPv4 and IPv6 addresses to the list of excluded addresses.

**Problems with a particular website**

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

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

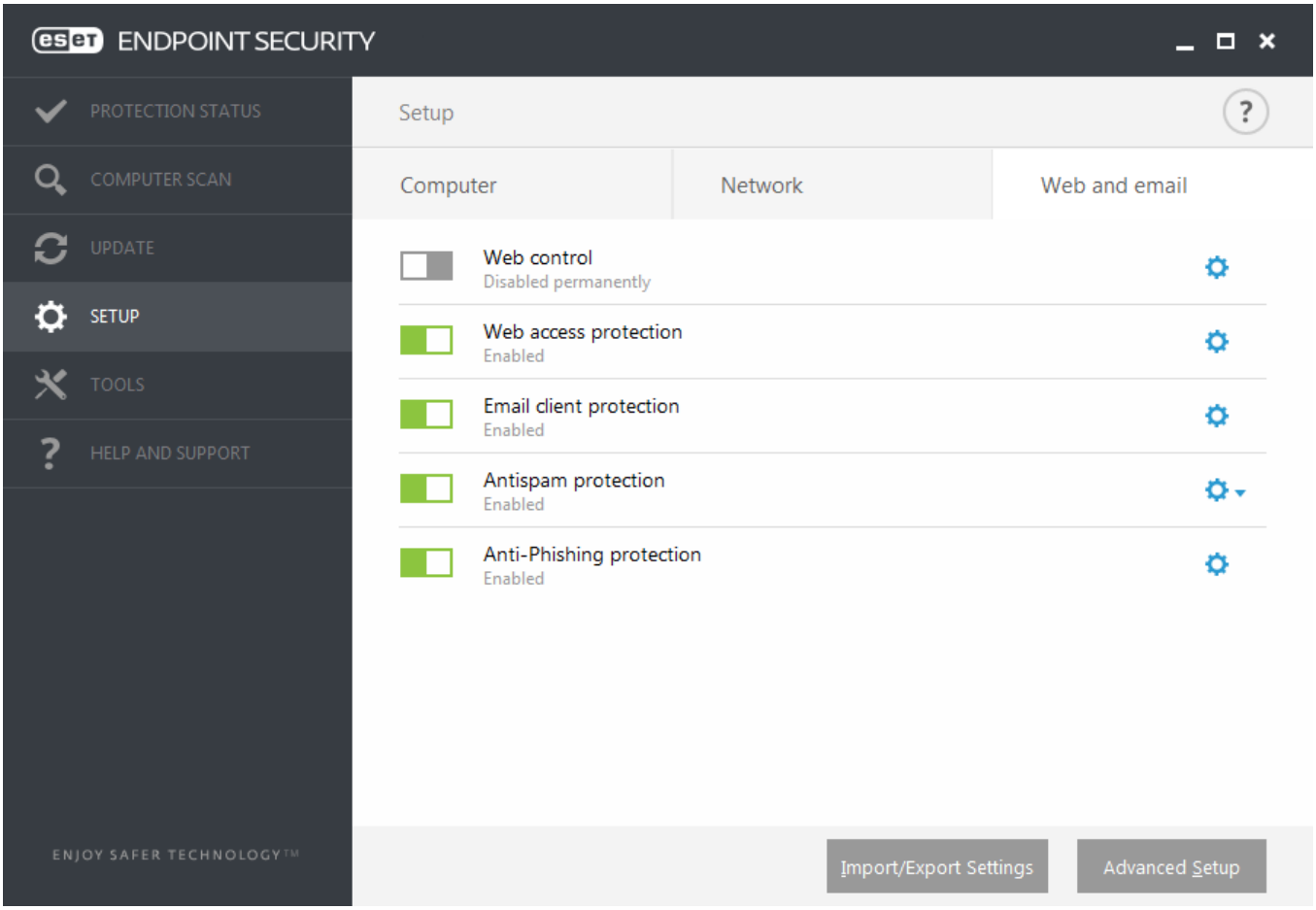
When you enable SSL protocol filtering, ESET Endpoint Security makes sure that installed applications trust the way it filters SSL protocol by importing a certificate to their certificate store. For some applications this is not possible while they are running. This includes Firefox and Opera. Make sure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

**Error about untrusted issuer or invalid signature**

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

### 3.9.3 Web and email

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




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

Internet connectivity is a standard feature for personal computers. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your **Web access protection**.

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

**Antispam protection** filters unsolicited email messages.

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

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

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

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

**Disable** – Click the switch to disengage web/email/antispam protection for web browsers and email clients .

#### 3.9.3.1 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) settings, go to **Web and email** > **SSL**.

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

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

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

**Web and email clients** – Used only on Windows XP operating systems, allows you to select applications for which all traffic is filtered by protocol filtering, regardless of ports used.

##### 3.9.3.1.1 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 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 Endpoint Security focuses on web browser security. Each application accessing the network can be marked as an Internet browser. Applications that already used protocols for communication or application from selected path can be entered to the list of Web and email clients.

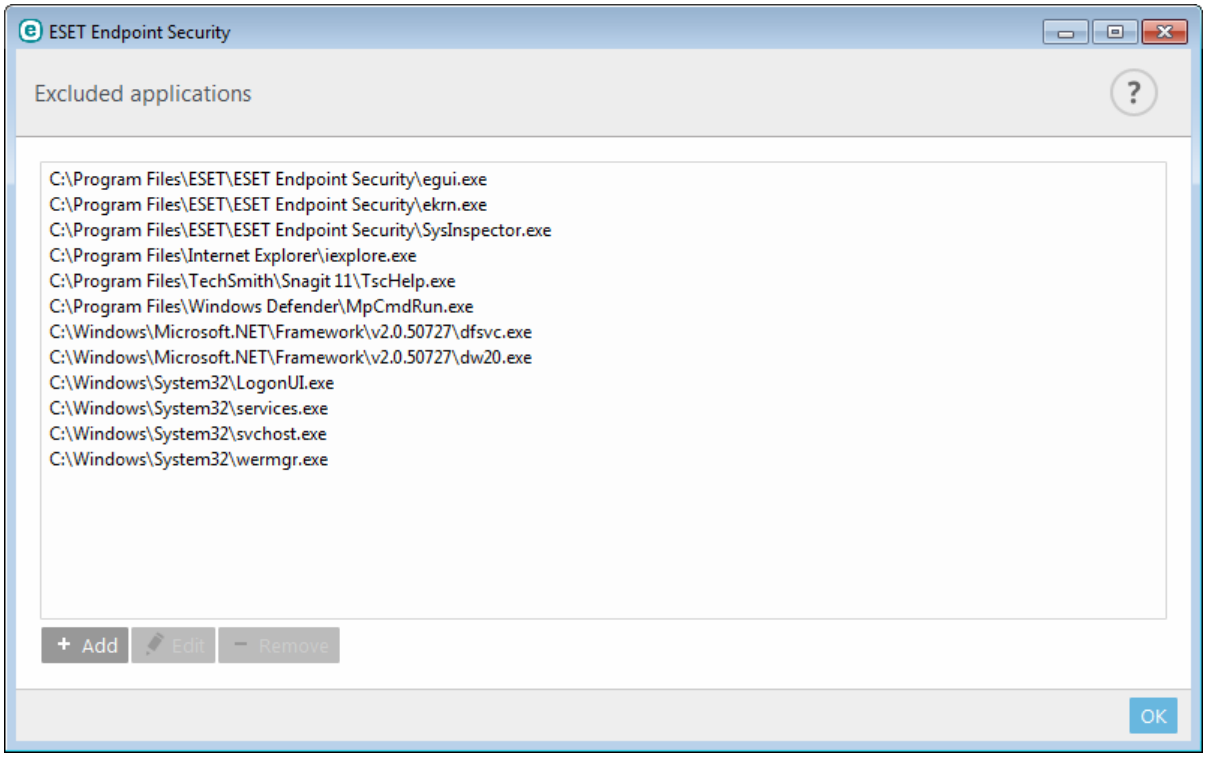
#### 3.9.3.1.2 Excluded applications

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

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

**Edit** – Edit selected entries from the list.

**Remove** – Remove selected entries from the list.



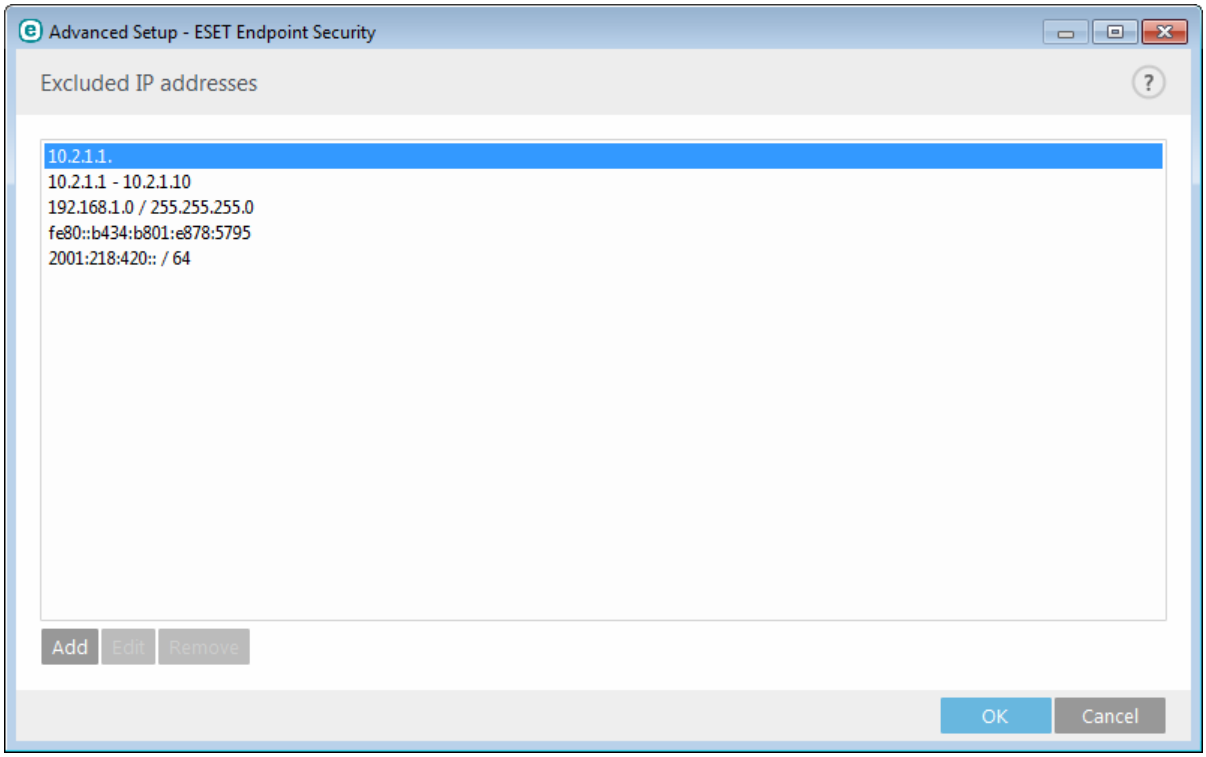
#### 3.9.3.1.3 Excluded IP addresses

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

**Add** – Click to add an IP address/address range/subnet of a remote point to which a rule is applied.

**Edit** – Edit selected entries from the list.

**Remove** – Remove selected entries from the list.




#### 3.9.3.1.4 SSL/TLS

ESET Endpoint Security 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** – 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.

**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 that will be excluded from scanning.

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

**Root certificate**

**Root certificate** – For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root certificates (publishers). **Add the root certificate to known browsers** should be enabled. Select this option to automatically add the ESET root certificate to known

browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (for example, in Internet Explorer).

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

**Certificate validity**

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

**If the certificate is 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.

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

#### 3.9.3.1.4.1 Encrypted SSL communication

If your system is configured to use SSL protocol scanning, a dialog window prompting you to choose an action will be displayed in two situations:

First, if a website uses an unverifiable or invalid certificate, and ESET Endpoint Security is configured to ask the user in such cases (by default yes for unverifiable certificates, no for invalid ones), a dialog box will ask you whether to **Allow** or **Block** the connection.

Second, if **SSL protocol filtering mode** is set to **Interactive mode**, a dialog box for each website will ask whether to **Scan** or **Ignore** the traffic. Some applications verify that their SSL traffic is not modified nor inspected by anyone, in such cases ESET Endpoint Security must **Ignore** that traffic to keep the application working.

In both cases, the user can choose to remember the selected action. Saved actions are stored in the **List of known certificates**.

#### 3.9.3.1.4.2 List of known certificates

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

The **List of known certificates** window consists of:

**Columns**

**Name** – Name of the certificate.

**Certificate issuer** – Name of the certificate creator.

**Certificate subject** – The subject field identifies the entity associated with the public key stored in the subject public key field.

**Access** – Select **Allow** or **Block** as the **Access action** to allow/block communication secured by this certificate regardless of its trustworthiness. Select **Auto** to allow trusted certificates and ask for untrusted ones. Select **Ask** to always ask user what to do.

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

**Control elements**

**Add** – A certificate can be loaded manually as a file with the extension *.cer*, *.crt* or *.pem*. Click File to upload a

local certificate or click **URL** to specify the location of a certificate online.

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

**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** to exit without saving.

### 3.9.3.2 Email client protection

#### 3.9.3.2.1 Email clients

Integration of ESET Endpoint Security 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 Endpoint Security. When integration is activated, the ESET Endpoint Security toolbar is inserted directly into the email client (toolbar for newer versions of Windows Live Mail is not inserted), allowing for more efficient email protection. Integration settings are located under **Setup** > **Advanced setup** > **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 are experiencing a system slowdown when working with your email client (MS Outlook only). 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, checking of email client 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 the folder** – 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 virus signature database 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 to have option **Enable email protection by client plugins** and **Enable email protection by protocol filtering** enabled.

### 3.9.3.2.2 Email protocols

The IMAP and POP3 protocols are the most widespread protocols used to receive email communication in an email client application. ESET Endpoint Security provides protection for these protocols regardless of the email client used, and without requiring re-configuration of the email client.

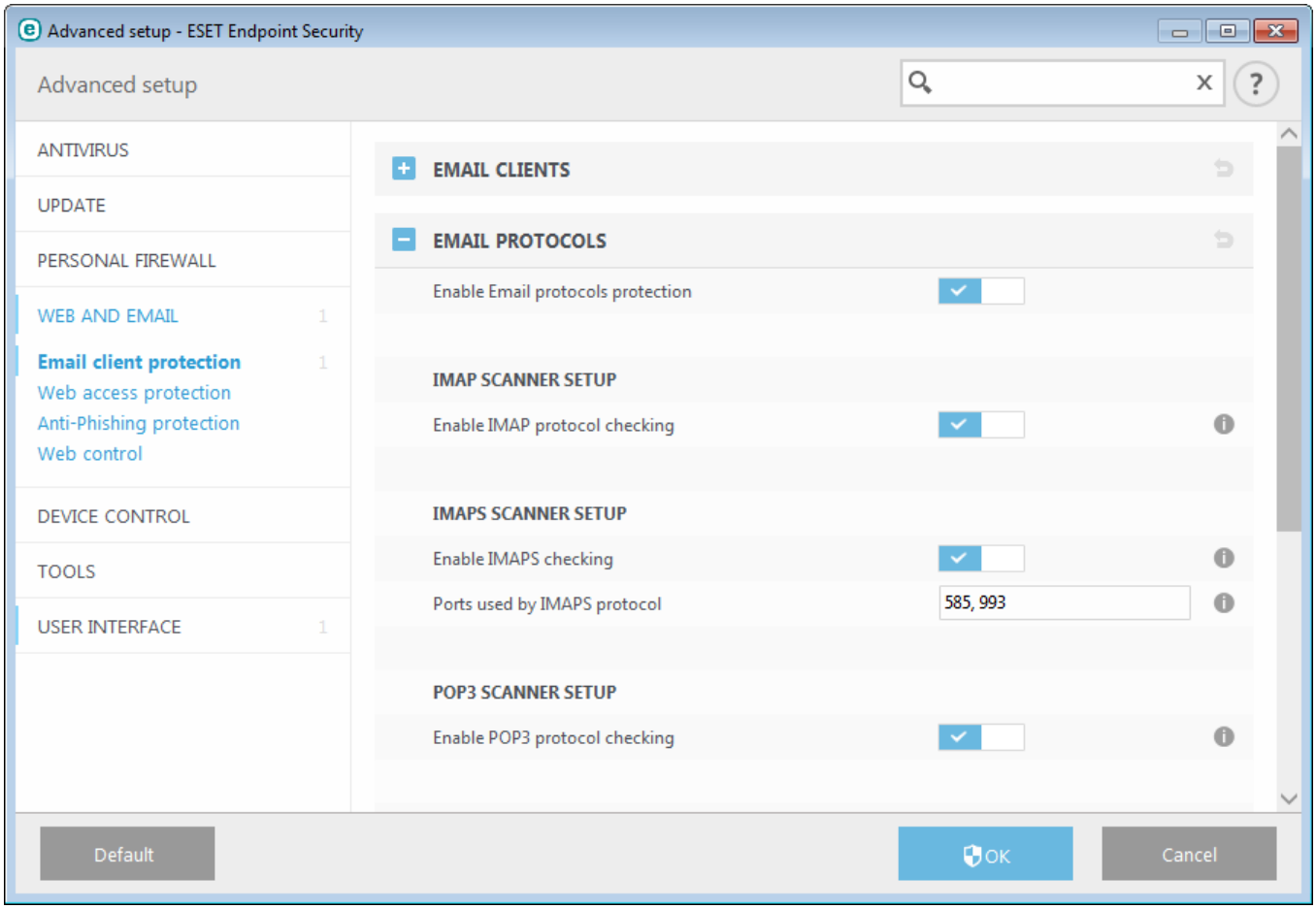
You can configure IMAP/IMAPS and POP3/POP3S protocol checking in Advanced setup. To access this setting, expand **Web and email** > **Email client protection** > **Email protocols**.

**Enable Email protocols protection** – 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 Endpoint Security also supports the scanning of IMAPS and POP3S protocols, which use an encrypted channel to transfer information between server and client. ESET Endpoint Security checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by IMAPS/POP3S protocol**, regardless of operating system version.

Encrypted communications will be not scanned when default settings are in use. To enable the scanning of encrypted communication, navigate to SSL/TLS in Advanced setup, click **Web and email** > **SSL/TLS** and select **Enable SSL/TLS protocol filtering**.



#### 3.9.3.2.3 Alerts and notifications

Email protection provides control of email communications received through the POP3 and IMAP protocols. Using the plug-in for Microsoft Outlook and other e-mail clients, ESET Endpoint Security provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP). When examining incoming messages, the program uses all the advanced scanning methods included in the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of POP3 and IMAP protocol communications is independent of the email client used.

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

**ThreatSense engine parameter setup** – The advanced virus scanner setup enables you to configure scan targets, detection methods, etc. Click to display the detailed virus scanner setup window.

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 mail, Append note to the subject of received and read infected email** or **Append tag messages to sent mail**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The available options are:

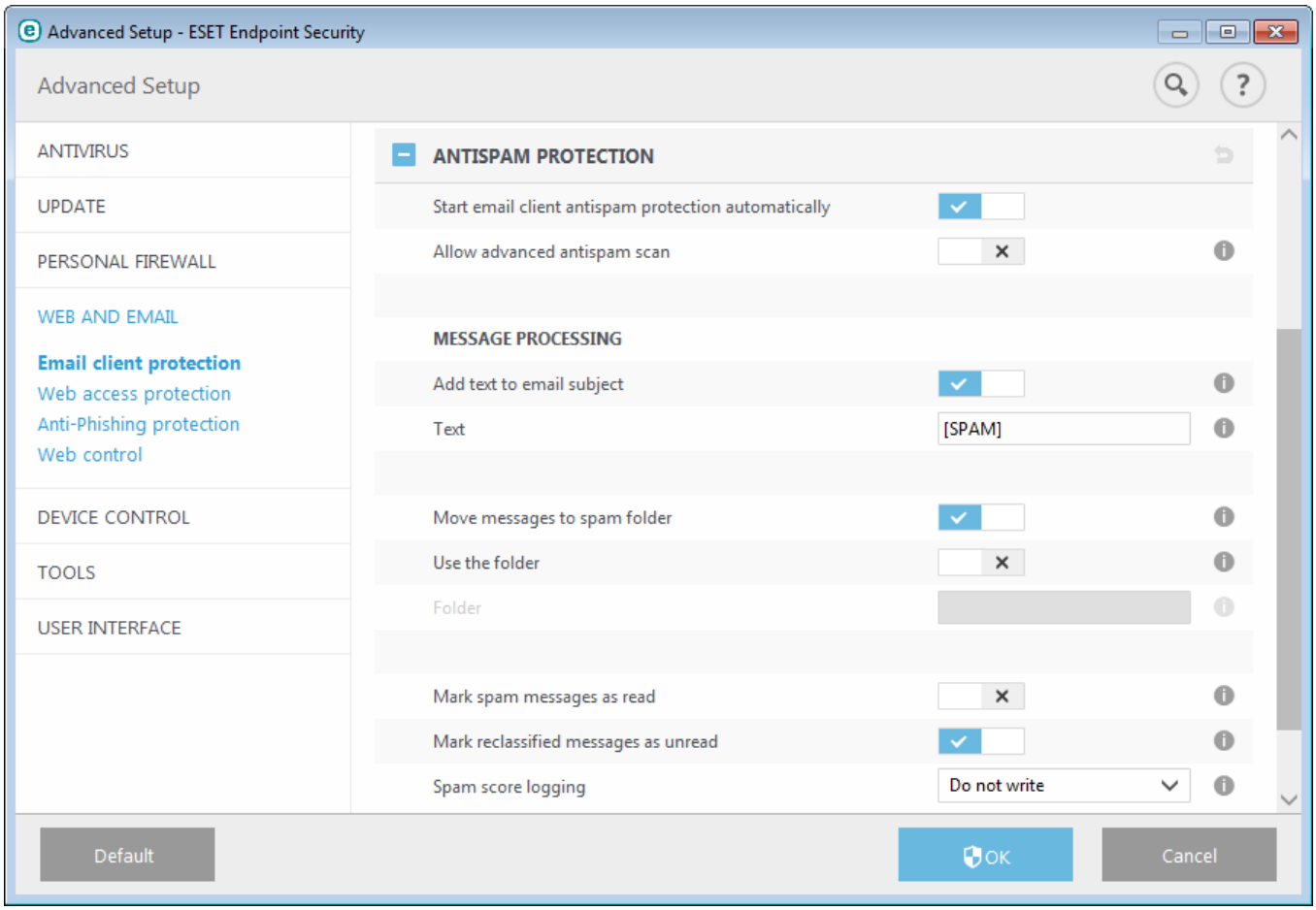
- **Never** – No tag messages will be added at all.
- **To infected email only** – Only messages containing malicious software will be marked as checked (default).
- **To all scanned email** – The program will append messages to all scanned email.

**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 and if an infiltration is detected, 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"* with a given prefix value *"[virus]"* to the following format: *"[virus] Hello"*. The variable *%VIRUSNAME%* represents the detected threat.

### 3.9.3.2.4 Antispam protection

Unsolicited email, called spam, ranks among the greatest problems of electronic communication. Spam represents up to 80 percent of all email communication. Antispam protection serves to protect against this problem. Combining several email security principles, the Antispam module provides superior filtering to keep your inbox clean.




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

The primary method used to detect spam is the scanning of email message properties. Received messages are scanned for basic Antispam criteria (message definitions, statistical heuristics, recognizing algorithms and other unique methods) and the resulting index value determines whether a message is spam or not.

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

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

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

**Message processing**

**Add text to email subject** – Enables you to add a custom prefix string to the subject line of messages that have been classified as spam. The default is "[SPAM]".

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

**Use the folder** – This option moves spam to a user-defined folder.

**Mark spam messages as read** – Enable this to automatically mark spam as read. It will help you to focus your attention on "clean" messages.

**Mark reclassified messages as unread** – Messages originally classified as spam, but later marked as “clean" will be displayed as unread.

**Spam score logging** – The ESET Endpoint Security Antispam engine assigns a spam score to every scanned message. The message will be recorded in the antispam log (**ESET Endpoint Security** > **Tools** > **Log files** > **Antispam protection**).

- **None** – The score from antispam scanning will not be logged.
- **Reclassified and marked as spam** – Select this if you want to record a spam score for messages marked as SPAM.
- **All** – All messages will be recorded to the log with a spam score.

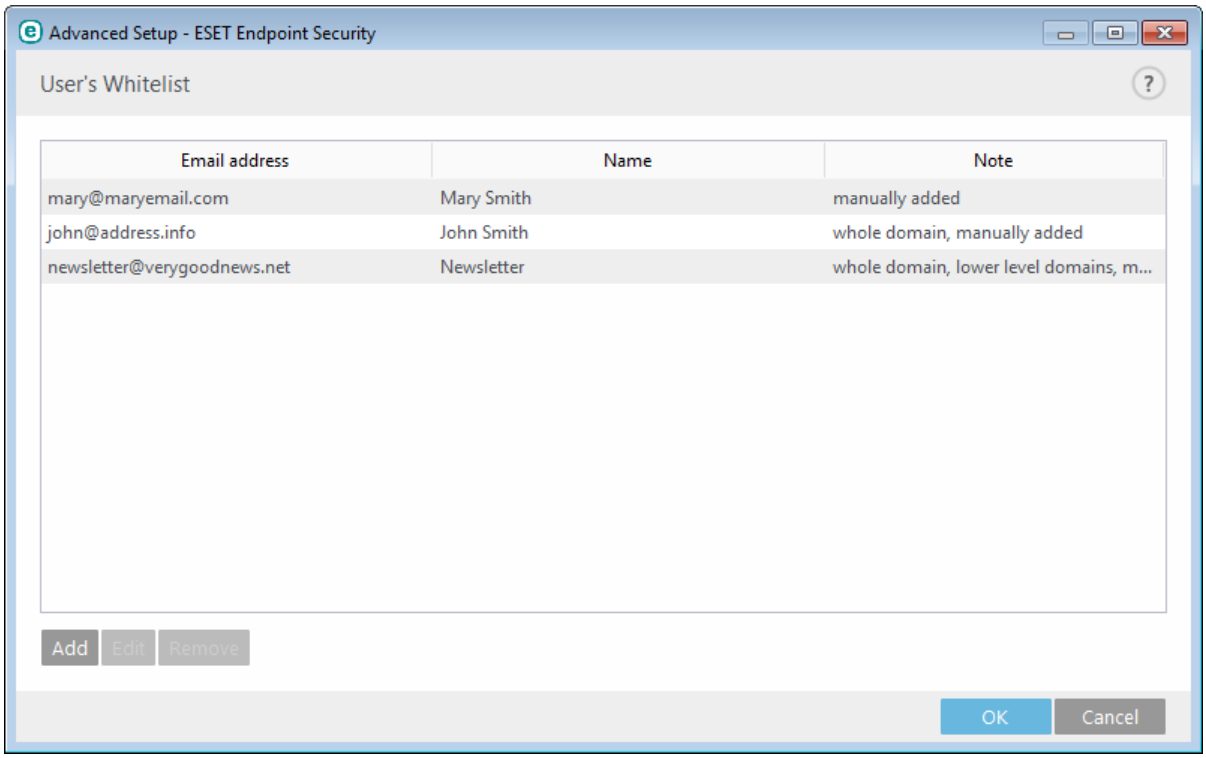
**NOTE**: When you click a message in junk email folder, you can choose **Reclassify selected messages as NOT spam** and the message will be moved to inbox. When you click a message you consider spam in inbox, select **Reclassify messages as spam** and the message will be moved to junk email folder.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

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

#### 3.9.3.2.4.1 Blacklist/Whitelist/Exceptions list

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

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




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

#### 3.9.3.2.4.2 Adding addresses to whitelist and blacklist

Email addresses belonging to people you communicate with frequently can be added to the whitelist to ensure that no message originating from a whitelist address is ever classified as spam. Known spam addresses can be added to the blacklist and always be classified as spam. To add a new address to the whitelist or blacklist, right-click the email and select **ESET Endpoint Security** > **Add to Whitelist** or **Add to Blacklist**, or click the **Trusted address** or **Spam address** button in the ESET Endpoint Security Antispam toolbar in your email client.

Similarly, the same process applies to spam addresses. If an email address is listed on the blacklist, each email message which arrives from that address is classified as spam.

#### 3.9.3.2.4.3 Marking messages as spam or not spam

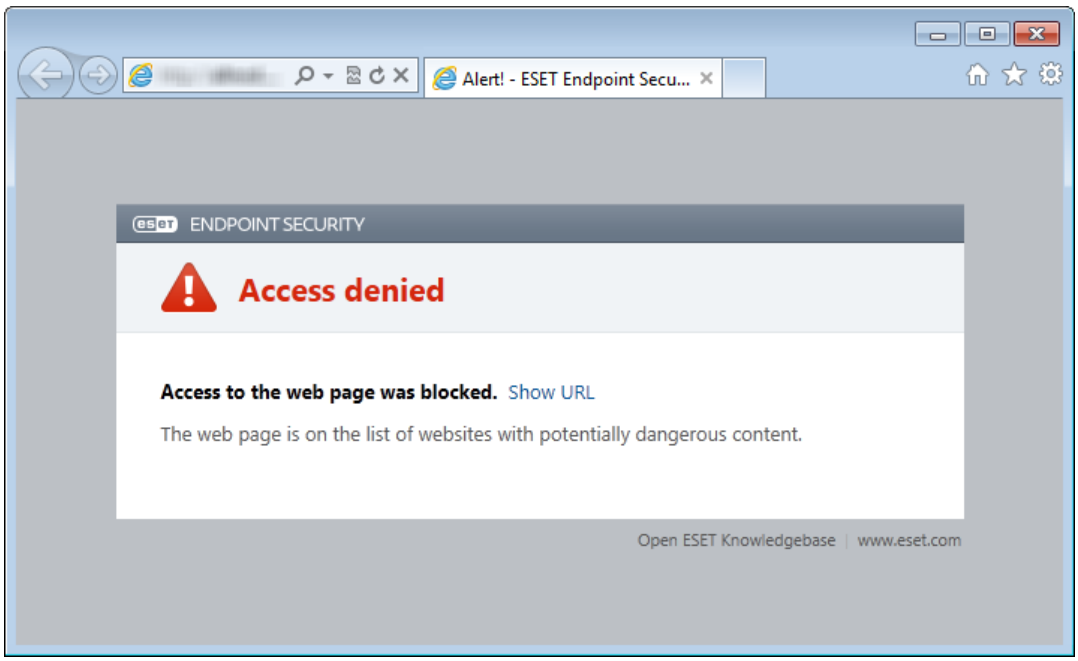
Any message viewed in your email client can be marked as spam. To do so, right-click the message and click **ESET Endpoint Security** > **Reclassify selected messages as spam**, or click **Spam** in the ESET Endpoint Security Antispam toolbar located in the upper section of your email client.

Reclassified messages are automatically moved to the SPAM folder, but the sender's email address is not added to the **Blacklist**. Similarly, messages can be classified as “not spam” by clicking **ESET Endpoint Security** > **Reclassify selected messages as not spam** or click **Not spam** in the ESET Endpoint Security Antispam toolbar located in the upper section of your email client. If messages from the **Junk E-mail** folder are classified as not spam, they are moved to the **Inbox** folder. Marking a message as not spam automatically adds the sender's address to the **Whitelist**.

### 3.9.3.3 Web access protection

Internet connectivity is a standard feature on most personal computers. 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 you leave Web access protection enabled. This option can be accessed from the main program window of ESET Endpoint Security by navigating to **Setup** > **Web and email** > **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 engine parameter setup** – 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.

#### 3.9.3.3.1 Web protocols

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

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 scanner setup**. HTTP traffic is monitored on the specified ports for all applications, and on all ports for applications marked as Web and email clients.

ESET Endpoint Security also supports HTTPS protocol checking. HTTPS communication uses an encrypted channel to transfer information between server and client. ESET Endpoint Security checks communication utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by HTTPS protocol**, regardless of operating system version.

Encrypted communication will be not scanned when default settings are in use. To enable the scanning of encrypted communication, navigate to SSL/TLS in Advanced setup, click **Web and email** > **SSL/TLS** and select **Enable SSL/TLS protocol filtering**.

#### 3.9.3.3.2 URL address management

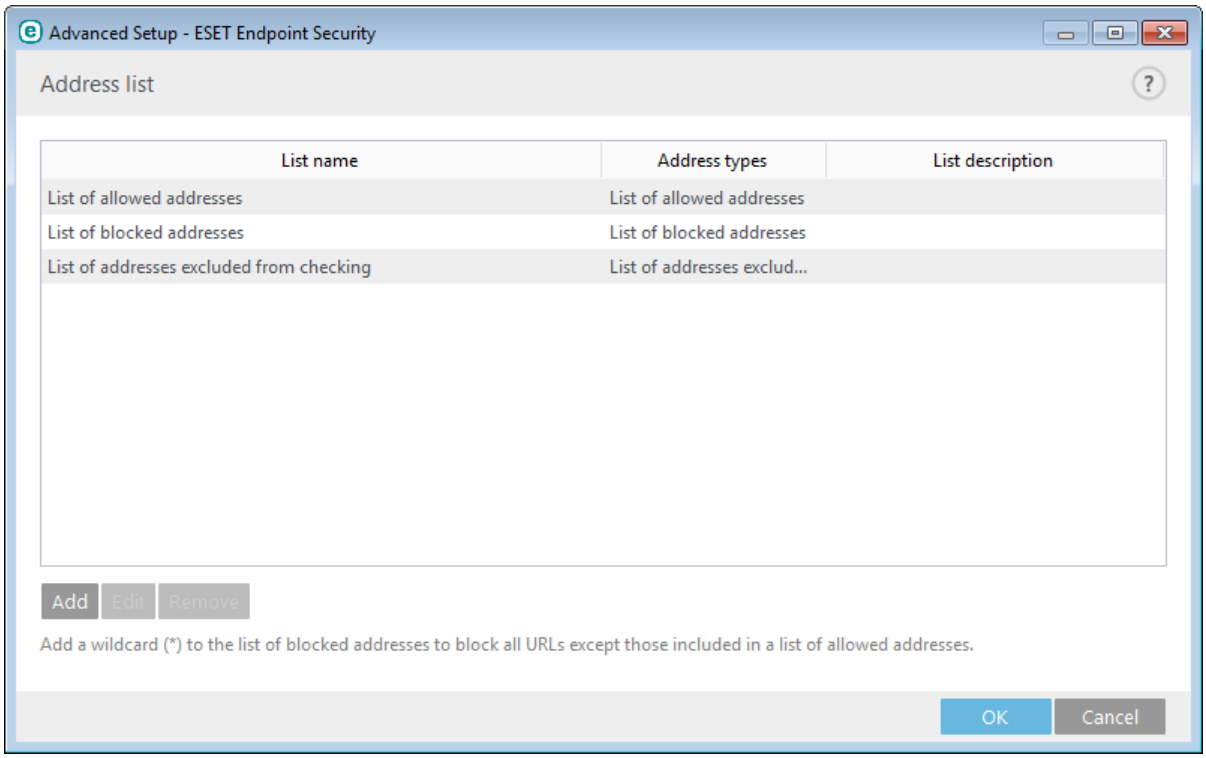
The URL address management section allows you to specify HTTP addresses to block, allow or exclude from checking.

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 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.

In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk represents any number or character, while the question mark represents any one character. 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, enable the **List active** option. If you want to be notified when entering an address from the current list, enable **Notify when applying**.

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**.




**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 some external public blacklist, and a second one may contain your own blacklist, which makes it easier to update the external list while keeping yours intact.

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

**Remove** – Deletes existing list. Only possible for lists created with **Add**, not for the default ones.

#### 3.9.3.4 Anti-Phishing protection

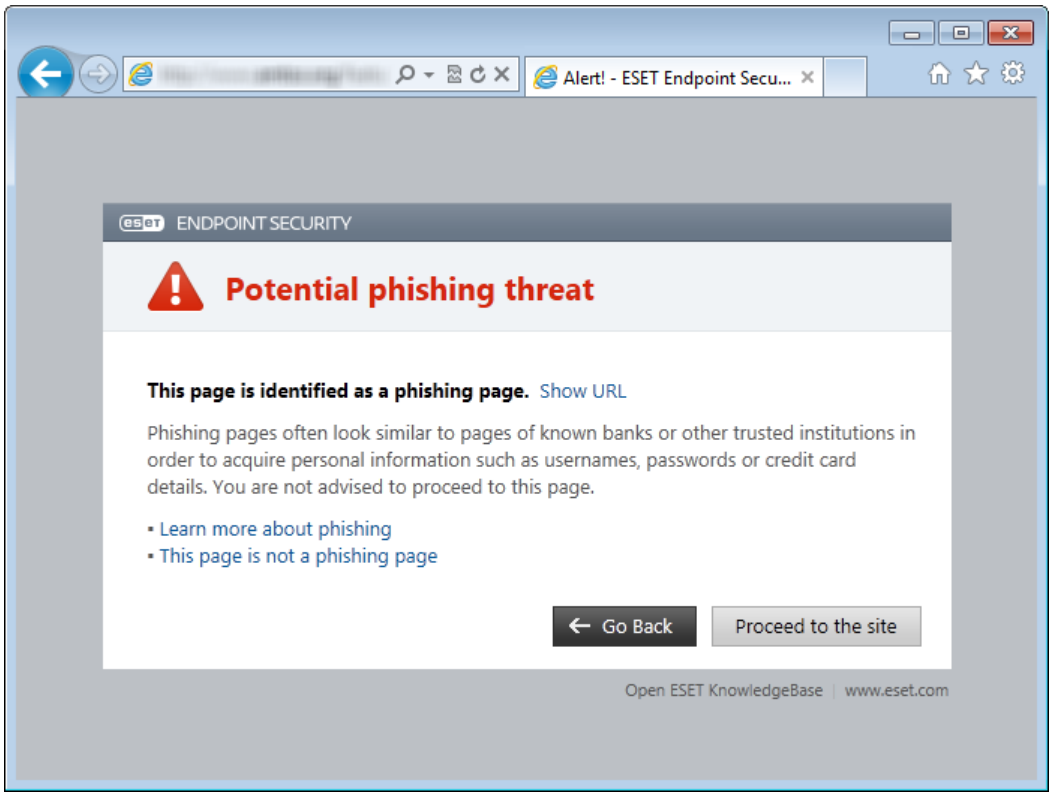
The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this activity in the glossary.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

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

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

**Accessing a phishing website**

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




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

**Phishing site reporting**

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

**NOTE:** Before submitting a website to ESET, make sure it meets one or more of the following criteria:
- the website is not detected at all,
- the website is incorrectly detected as a threat. In this case, you can Report a false-positive phishing site.

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

### 3.9.4 Web control

The Web control section allows you to configure settings that protect your company from risk of legal liability. Web control can regulate access to websites that violate intellectual property rights. The goal is to prevent employees from accessing pages with inappropriate or harmful content, or pages that may have a negative impact on productivity.

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

By default, Web control is disabled. To activate web control, press **F5** to enter **Advanced setup**, and expand **Web and email** > **Web control**. Select **Integrate into system** to activate Web control in ESET Endpoint Security. Click **Edit** next to **Rules**, to access the Web control rules editor window.

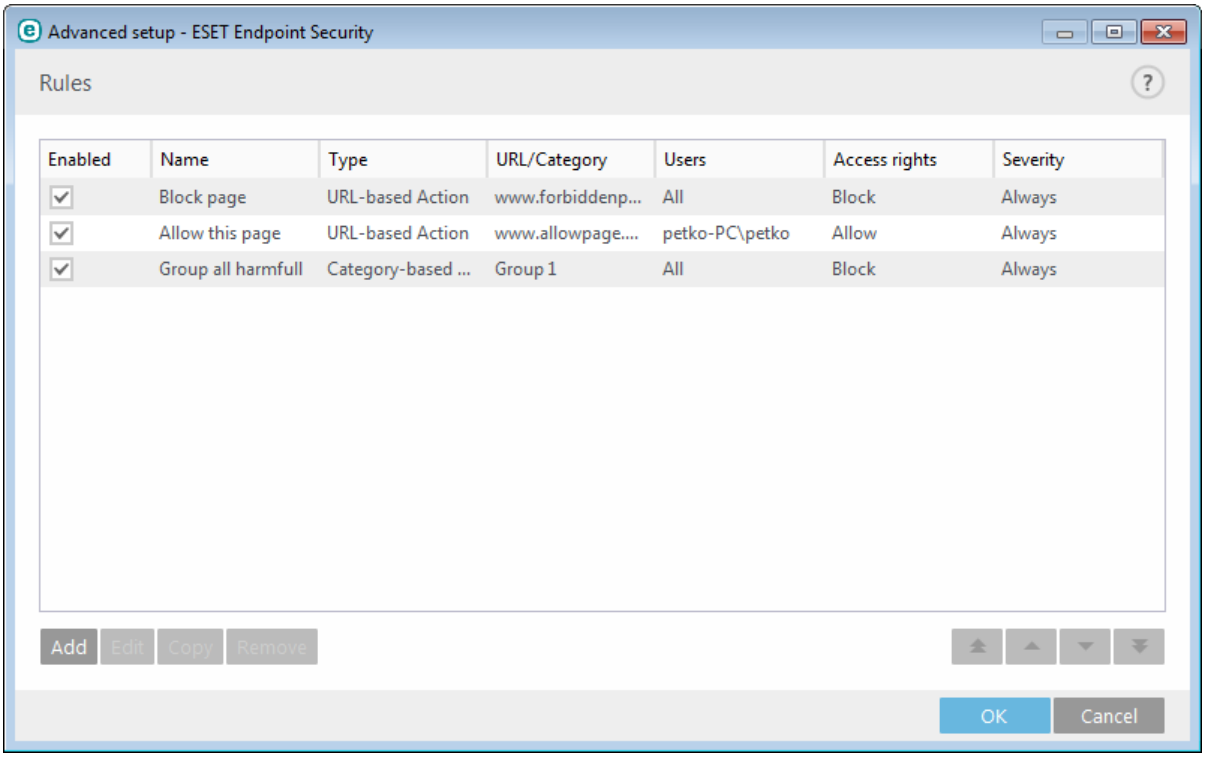
**Blocked webpage message** and **Block webpage graphic** fields allow you to easily customize the displayed message when a website is blocked.

**TIP**: An example of a blocked webpage message would be *The webpage was blocked because it is considered inappropriate or with harmful content. Please contact your administrator for details* and you can enter a web address or network path with custom image for example *http://test.com/test.jpg*. The custom image size is set automatically

to 90 x 30; images will automatically be scaled to this size if they are not already.

### 3.9.4.1 Rules

The **Rules** editor window displays existing URL-based or Category-based rules.



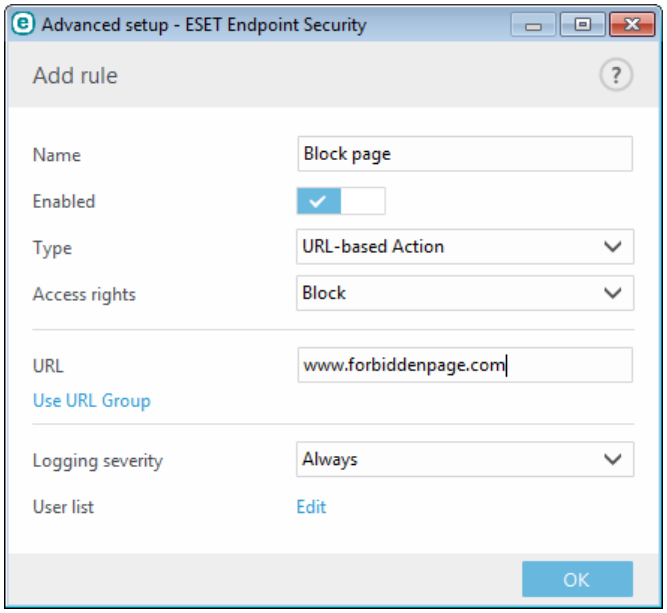

The list of rules contains several descriptions of rules such as name, type of blocking, action to perform after matching a Web control rule and log severity.

Click **Add** or **Edit** to manage a rule. Click **Copy** to create a new rule with predefined options used for another selected rule. By pressing **Ctrl** and clicking, you can select multiple rules and delete all selected rules. The **Enabled** check box disables or enables a rule; this can be useful if you don't want to delete a rule permanently because it might be used in the future.

Rules are sorted in the order determining their priority, with higher priority rules on top. Evaluation of rules based on URL always has higher priority than evaluation based on category. For example, if a rule based on a URL is under a rule based on category in the list of rules, the URL-based rule has higher priority and will be evaluated first.

### 3.9.4.1.1 Adding Web control rules

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




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

**Action type**

- **URL-based action** – For rules that control access to a given website, enter the URL in the **URL** field.
- **Category-based action** – When this is selected, set the category for your action using the drop-down menu.

The special symbols * (asterisk) and ? (question mark) cannot be used in the URL address list. When creating a URL group that contains a website with multiple top-level-domains (TLDs), each TLD must be added separately. If you add a domain to the group, all content located on this domain and all subdomains (for example, *sub.examplepage.com*) will be blocked or allowed based on your choice of URL-based action.

**Access rights**

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

**URL** or **Use URL group** - Uses the URL link or group of links to allow, block or warn the user when one of these URLs is detected.

**Logging severity:**

- **Always** – Logs all online communications.
- **Diagnostic** – Logs information needed to fine-tune the program.
- **Information** – Records informative messages, including successful update messages, plus all records above.
- **Warning** – Records critical errors and warning messages.
- **None** – No logs will be created.

**User list**

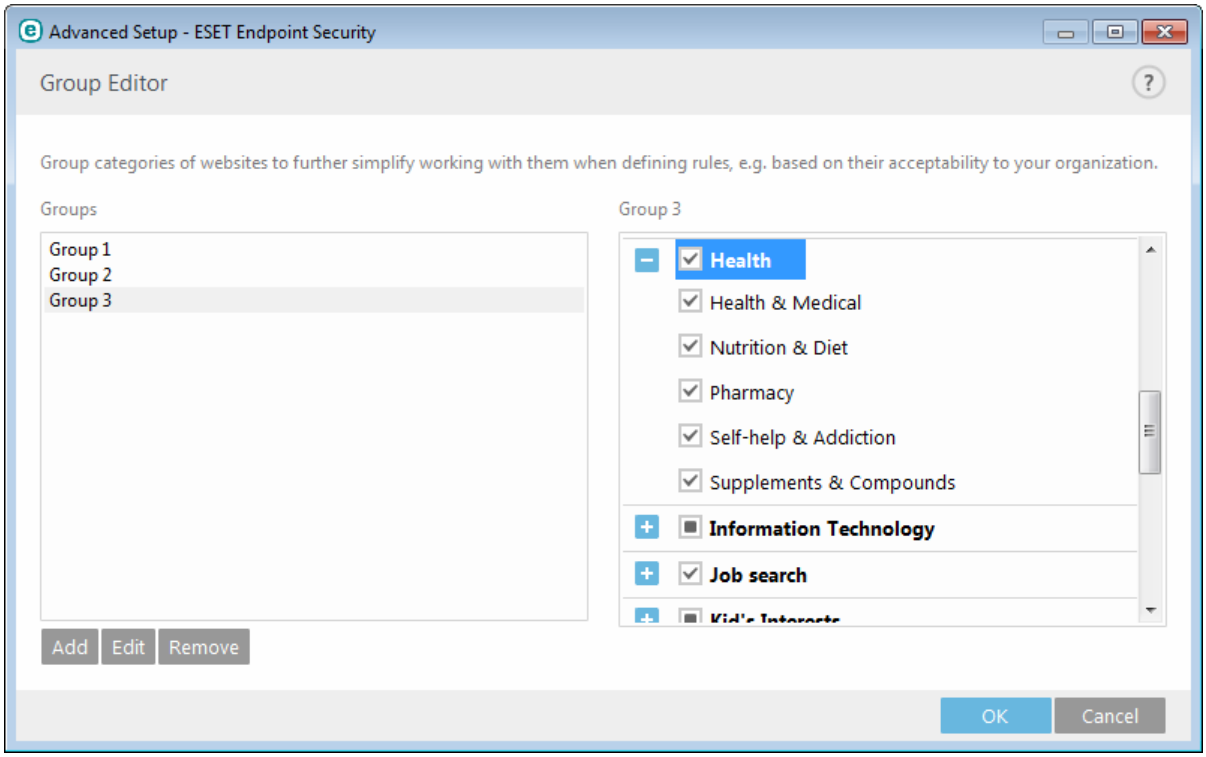
- **Add** – Opens the **Select Users or Groups** dialog window, which allows you to select desired users. When no user is entered the rule is applied for all users.
- **Remove** – Removes the selected user from the filter.

### 3.9.4.2 Category groups

The Category groups window is divided into two parts. The right part of the window contains a list of categories and subcategories. Select a category in the Category list to display its subcategories.

Each group contains adult and/or generally inappropriate subcategories as well as categories considered generally acceptable. When you open the Category groups window and click on first group, you can add or remove categories/ subcategories from the list of appropriate groups (for example Violence or Weapons). Web pages with inappropriate content can be blocked, or users can be informed after a rule with predefined actions is created.

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




Here are some examples of categories that users might not be familiar with:

**Miscellaneous** – Usually private (local) IP addresses such as intranet, 192.168.0.0/16, etc. When you get a 403 or 404 error code, the website will also match this category.
**Not resolved** – This category includes web pages that are not resolved because of an error when connecting to the Web control database engine.
**Not categorized** – Unknown web pages that are not yet in the Web control database.
**Proxies** – Web pages such as anonymizers, redirectors or public proxy servers can be used to obtain (anonymous) access to web pages that are usually prohibited by the Web control filter.
**File sharing** – These web pages contain large amounts of data such as photos, videos or e-books. There is a risk that these sites contain potentially offensive material or adult content.

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

#### 3.9.4.3 URL groups

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

To create a new URL group click **Add**. Select a URL group and click **Add** in the bottom right of the window to add a new URL address to the list, or click **Import** to import a file with a list of URL addresses (separate values with a line break, for example *.txt using encoding UTF-8). If you want to set an action to be performed for a specific URL group, open the **Web control rules editor**, select your URL group using the drop-down menu, adjust other parameters and then click **OK**.

**NOTE**: Blocking or allowing a specific web page can be more accurate than blocking or allowing a whole category of web pages. Be careful when changing these settings and adding a category/web page to the list.

### 3.9.5 Updating the program

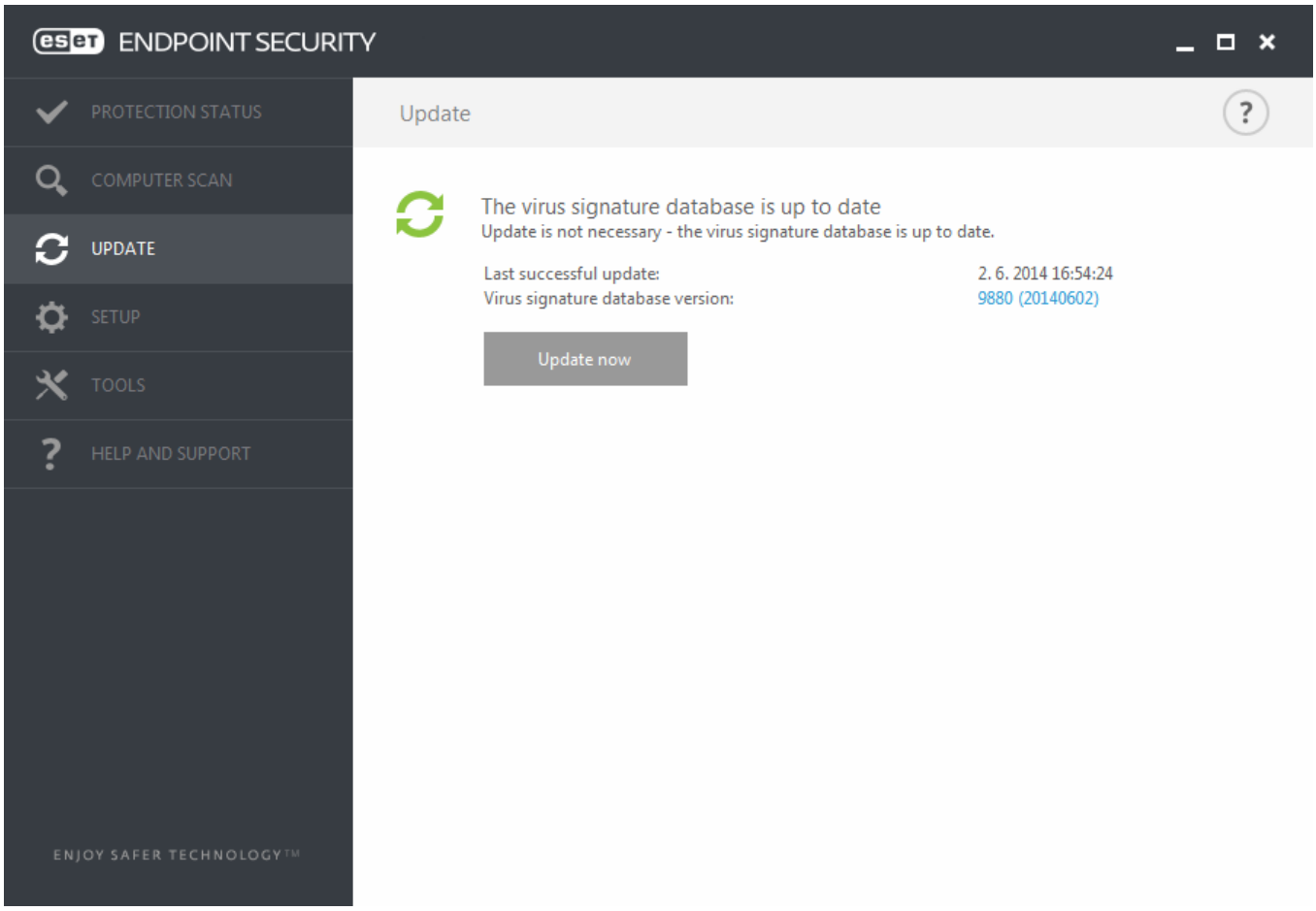
Regularly updating ESET Endpoint Security is the best method to obtain the maximum level of security on your computer. The Update module ensures that the program is always up to date in two ways, by updating the virus signature database and by updating system components.

By clicking **Update** in the main program window, you can find the current update status including the date and time of the last successful update and if an update is needed. The primary window also contains the virus signature database version. This numeric indicator is an active link to ESET's website, listing all signatures added within the given update.

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

If you activate ESET Endpoint Security with Offline license file without Username and Password and try to update, the red information **Virus signature database update ended with an error** signals you can download updates from the mirror only.

**NOTE**: Your license key is provided by ESET after purchasing ESET Endpoint Security.

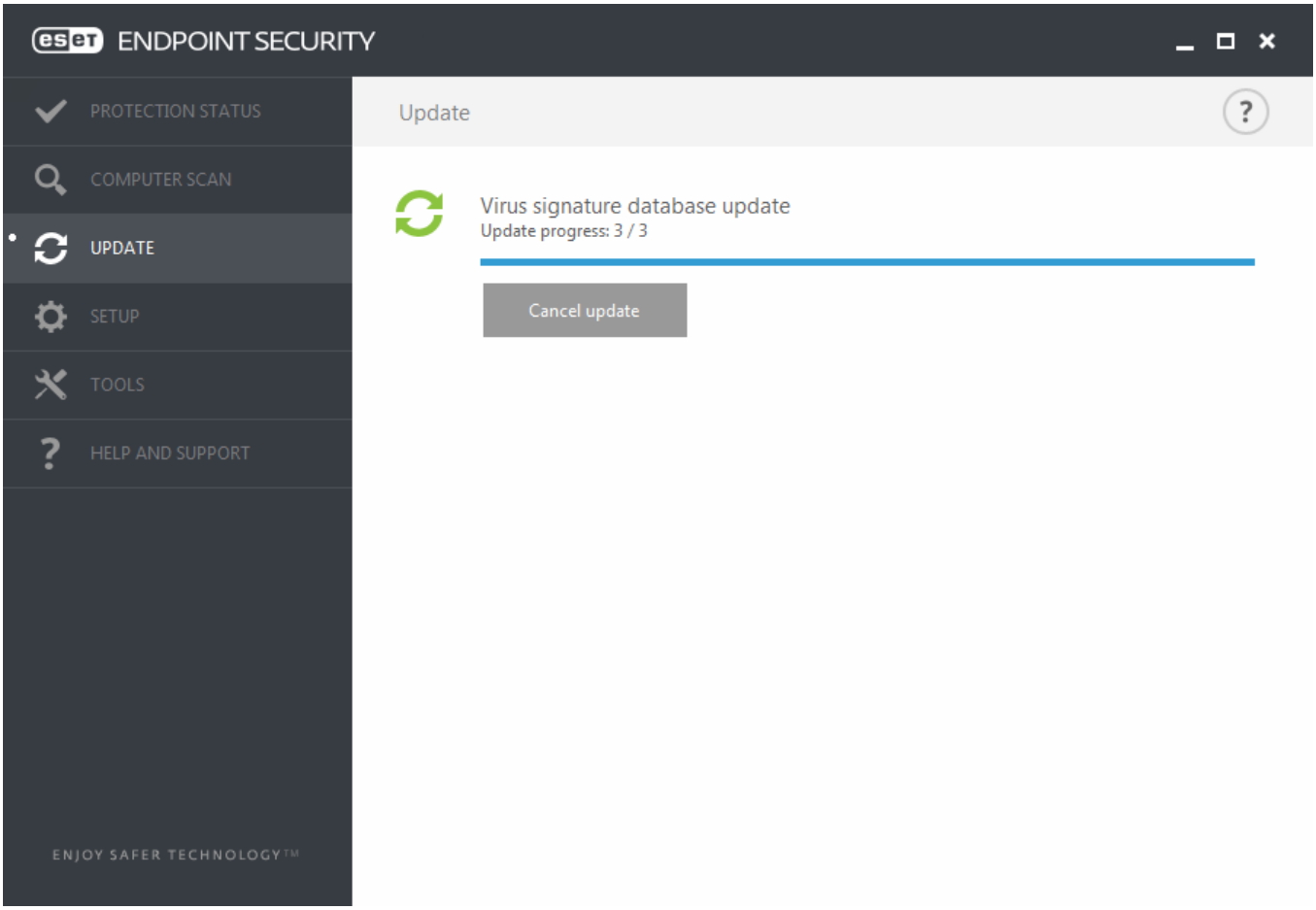



**Last successful update** – The date of the last update. Make sure it refers to a recent date, which means that the virus signature database is current.

**Virus signature database version** – The virus signature database number, which is also an active link to ESET's website. Click it to view a list of all signatures added within the given update.

**Update process**

After clicking **Update virus signature database**, the download process begins. A download progress bar and remaining time to download will be displayed. To interrupt the update, click **Cancel update**.

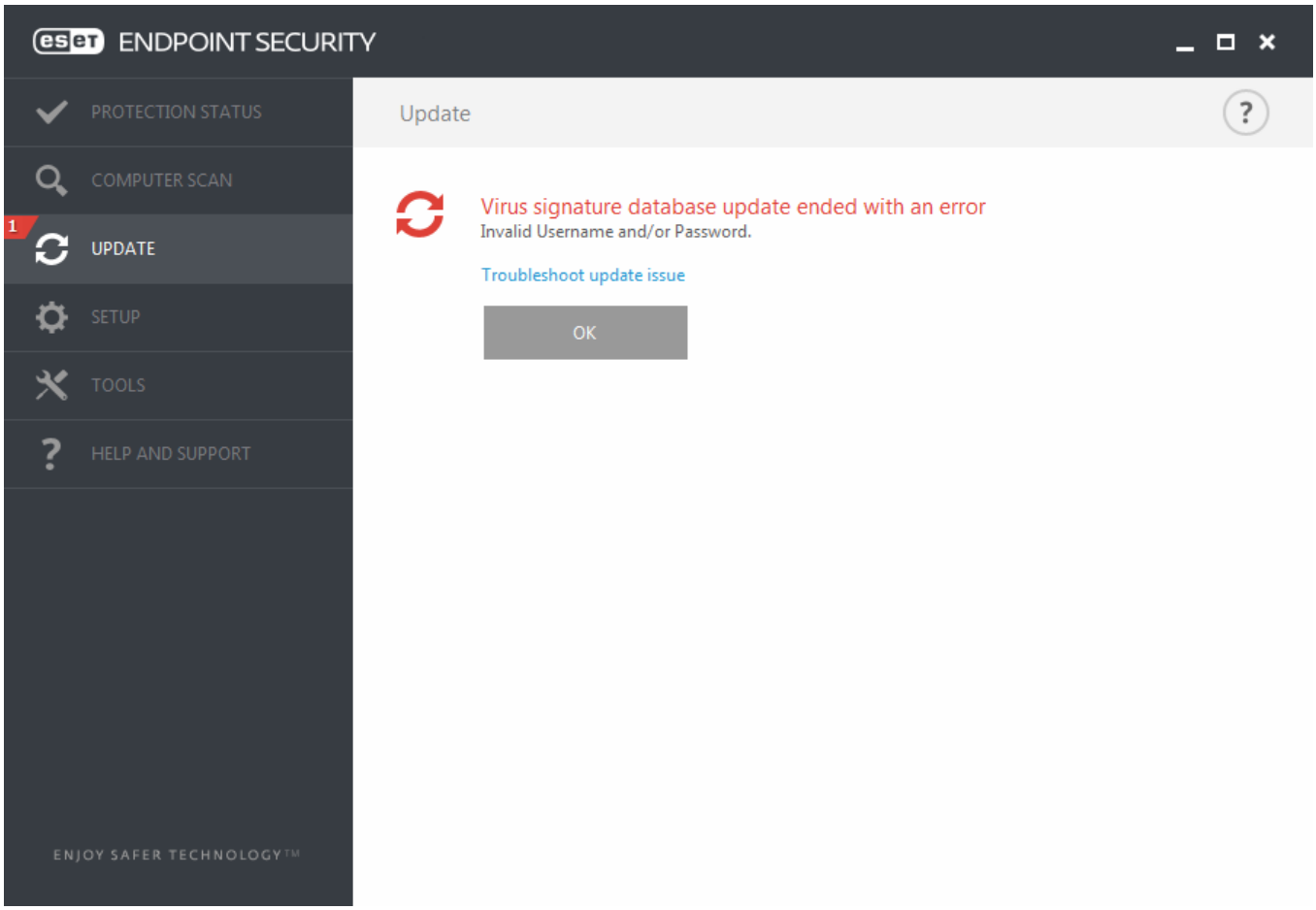



***Important:*** Under normal circumstances, when updates are downloaded properly the message **Update is not necessary – Virus signature database is up to date** will appear in the **Update** window. If this is not the case, the program is out of date and more vulnerable to infection. Please update the virus signature database as soon as possible.

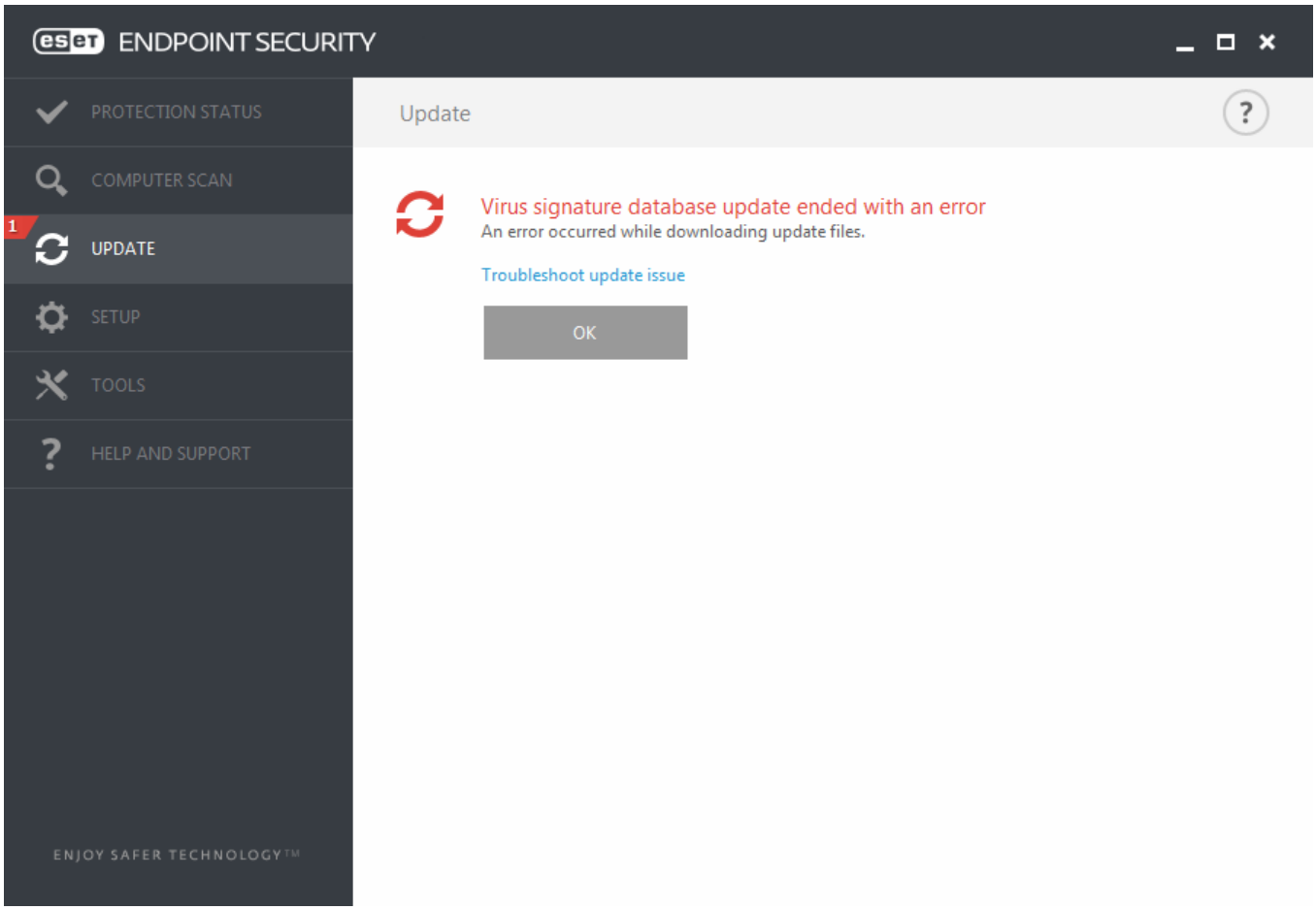
**Virus signature database is out of date** – This error will appear after several unsuccessful attempts to update the virus signature database. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured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

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

1. **Invalid license** – The license key has been incorrectly entered in update setup. We recommend that you check your authentication data. The Advanced setup window (click **Setup** from the main menu and then click **Advanced setup**, or press F5 on your keyboard) contains additional update options. Click **Help and support** > **Manage license** from the main menu to enter a new license key.



2. **An error occurred while downloading update files** – A possible cause of the error is incorrect Internet connection settings. We recommend that you check your Internet connectivity (by opening any website in your web browser). If the website does not open, it is likely that an Internet connection is not established or there are connectivity problems with your computer. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.




**NOTE:** For more information please visit this ESET Knowledgebase article.

### 3.9.5.1 Update setup

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.

#### General

The update profile that is currently in use is displayed in the **Selected profile** drop-down menu. To create a new profile, click **Edit** next to **List of profiles**, enter your own **Profile name** and then click **Add**.

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

**Outdated virus signature database alerts**

**Set maximum database age automatically** – Allows to set maximum time (in days) after which the virus signature database will be reported as out of date. Default value is 7.

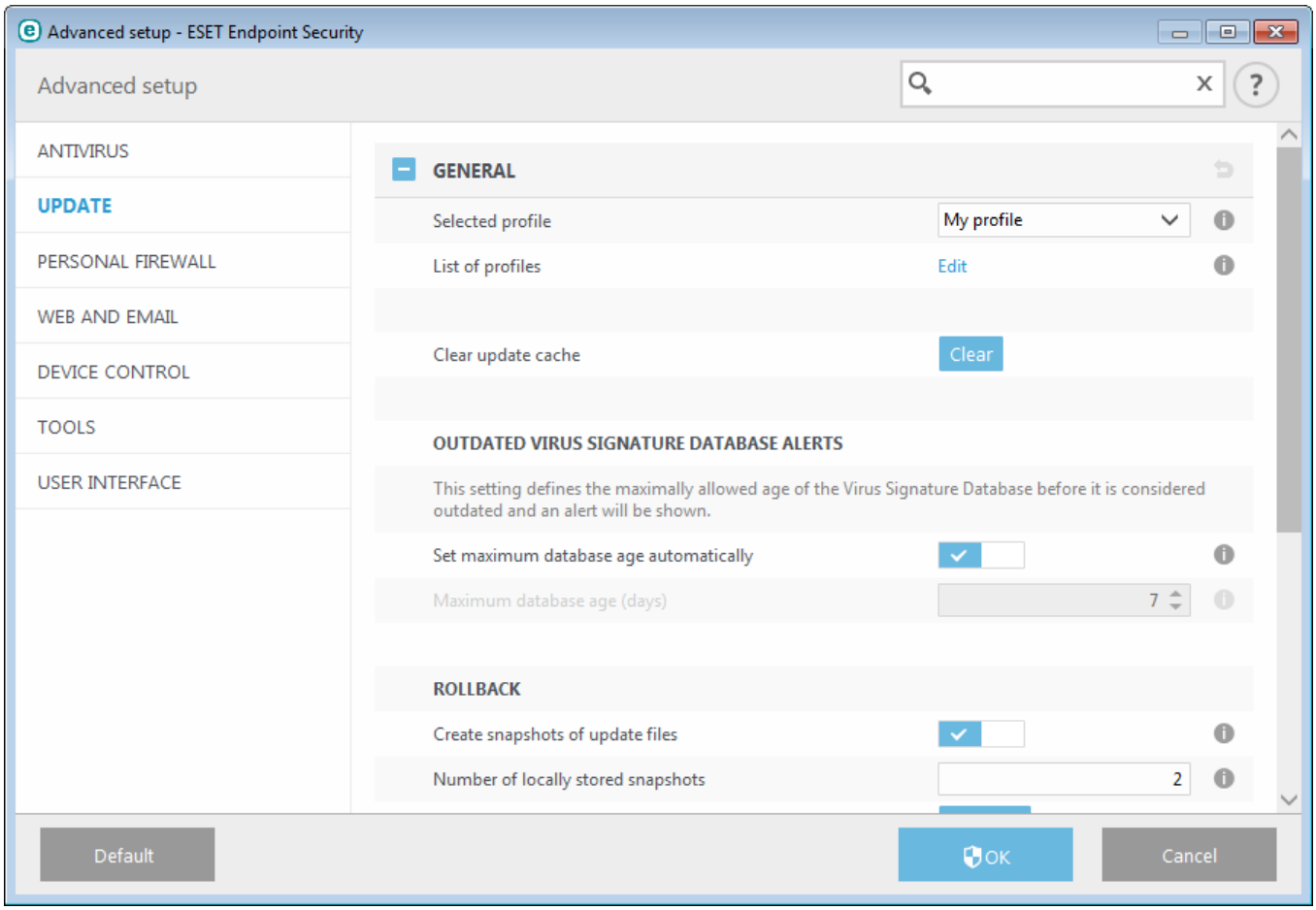
**Rollback**

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 Endpoint Security records snapshots of virus signature database and program modules for use with the *rollback* feature. In order to create virus database snapshots, leave the **Create snapshots of update files** 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** > **General**), you have to select a time interval from the drop-down menu that represents the period of time that the virus signature database and program module updates will be paused.




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).

## Basic

By default, the **Update type** is set to **Regular update** to ensure that update files will automatically be download from the ESET server with the least network traffic. Pre-release updates (the **Pre-release update** option) are updates that have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times and SHOULD NOT be used on production servers and workstations where maximum availability and stability is required. **Delayed update** allows updating from special update servers providing new versions of virus databases with a delay of at least X hours (i.e. databases tested in a real environment and therefore considered as stable).

**Disable display 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 Presentation mode will turn off all notifications.

**Update from removable media** – Allows you to update from removable media if contains created mirror. When **Automatic** selected, update will run on background. If you want to show update dialogs select **Always ask**.

The **Update server** menu is set to AUTOSELECT by default. The Update server is the location where updates are stored. If you use an ESET server, we recommend that you leave the default option selected.

When using a local HTTP server – also known as a Mirror – the update server should be set as follows:
*http://computer_name_or_its_IP_address:2221*

When using a local HTTP server with SSL – the update server should be set as follows:
*https://computer_name_or_its_IP_address:2221*

When using a local shared folder – the update server should be set as follows:
*\\computer_name_or_its_IP_address\shared_folder*

**Updating from Mirror**

Authentication for update servers is based on the **Licensing key** generated and sent to you after purchase. When using a local Mirror server, you can define credentials for clients to log in to the Mirror server before receiving updates. By default, no verification is required and the **Username** and **Password** fields are left empty.

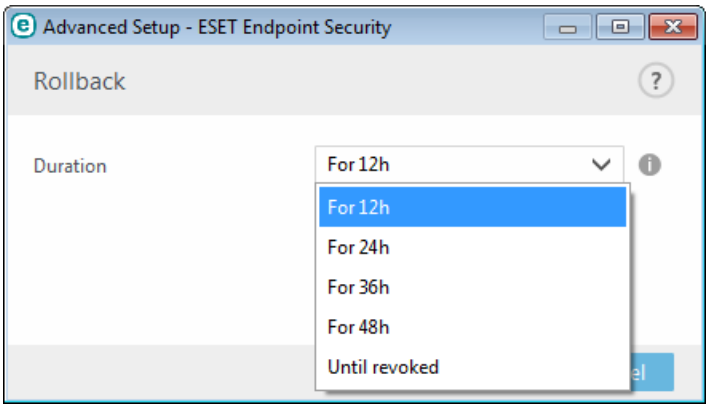
#### 3.9.5.1.1 Update profiles

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 **Selected profile** 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**.

#### 3.9.5.1.2 Update rollback

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




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

The virus signature database version is downgraded to the oldest available and stored as a snapshot in the local computer file system.

**Example:** Let the number 10646 be the most recent version of virus signature database. 10645 and 10643 are stored as a virus signature database snapshots. Note that 10644 is not available because, for example, the computer was turned off and a more recent update was made available before 10644 was downloaded. If the **Number of locally stored snapshots** field is set to 2 and you click **Rollback**, the virus signature database (including program modules) will be restored to version number 10643. This process may take some time. Check whether the virus signature database version has downgraded from the main program window of ESET Endpoint Security in the Update section.

#### 3.9.5.1.3 Update mode

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

Program component updates brings new features or makes changes to those that already exist from previous versions. It can be performed automatically without user intervention, or you can choose to be notified. After a program component update has been installed, a computer restart may be required. In the **Program component update** section, three options are available:

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

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

If the **Ask before downloading update** option is active, a notification will display when a new update is available.

If the update file size is greater than the value specified in the **Ask if an update file is greater than (kB)** field, the program will display a notification.

#### 3.9.5.1.4 HTTP Proxy

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

Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified in the **Tools** > **Proxy server** branch of the Advanced setup tree.

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

The **Connection through a proxy server** option should be selected if:

- A proxy server should be used to update ESET Endpoint Security that is different from the proxy server specified in the global settings (**Tools** > **Proxy server**). If so, the settings should be specified here: **Proxy server** address, communication **Port** (3128 by default), plus **Username** and **Password** for the proxy server if required.
- The proxy server settings were not set globally, but ESET Endpoint Security will connect to a proxy server for updates.
- Your computer is connected to the Internet via a proxy server. The settings are taken from Internet Explorer during program installation, but if they are subsequently changed (e.g. if you change your ISP), please check that the HTTP proxy settings listed in this window are correct. Otherwise the program will not be able to connect to the update servers.

The default setting for the proxy server is **Use global proxy server settings**.

**NOTE:** Authentication data such as **Username** and **Password** is intended for accessing the proxy server. Complete these fields only if a username and password are required. Please note that these fields are not for your Username/ Password for ESET Endpoint Security, and should only be completed if you know you need a password to access the internet via a proxy server.

#### 3.9.5.1.5 Connect to LAN as

When updating from a local server with a version of the Windows NT operating system, authentication for each network connection is required by default.

To configure such an account, select from the **Local user type** drop-down menu:

- **System account (default)**,
- **Current user**,
- **Specified user**.

Select **System account (default)** to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authenticates using a currently logged-in user account, select **Current user**. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

Select **Specified user** if you want the program to use a specific user account for authentication. Use this method when the default system account connection fails. Please be aware that the specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

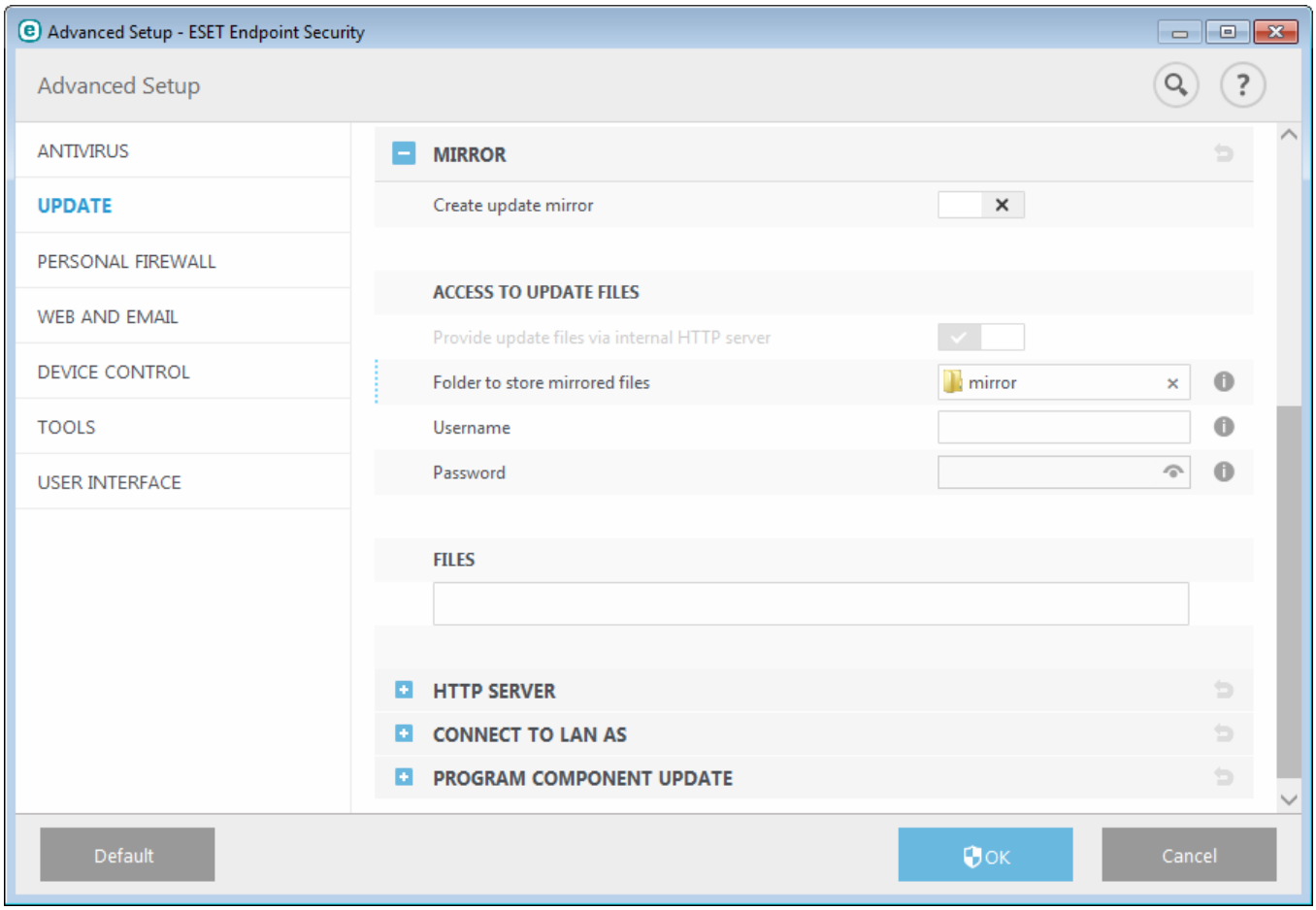
***Warning***: When either **Current user** or **Specified user** is selected, an error may occur when changing the identity of the program to the desired user. We recommend entering the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be entered as follows: *domain_name**user* (if it is a workgroup, enter *workgroup_name**name*) and password. When updating from the HTTP version of the local server, no authentication is required.

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

### 3.9.5.1.6 Mirror

ESET Endpoint Security allows you to create copies of update files that can be used to update other workstations on the network. The use of a *"mirror"* – a copy of the update files in the LAN environment is convenient because the update files do not need to be downloaded from the vendor update server repeatedly by each workstation. Updates are downloaded to the local mirror server and then distributed to all workstations to avoid the risk of network traffic overload. Updating client workstations from a Mirror optimizes network load balance and saves Internet connection bandwidth.

Configuration options for the local Mirror server are located in Advanced setup under **Update.** To access this section press **F5** to access Advanced setup, click **Update** and select the **Mirror** tab.




To create a mirror on a client workstation, enable **Create update mirror**. Enabling this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

**Access to update files**

**Provide update files via the internal HTTP server** – If enabled, update files can be accessed through HTTP, no credentials are required.

**NOTE:** Windows XP requires service pack 2 or later to use the HTTP server.

Methods to access the Mirror server are described in detail in Updating from the Mirror. There are two basic methods for accessing the Mirror – the folder with update files can be presented as a shared network folder, or clients can access the mirror located on an HTTP server.

The folder dedicated to storing update files for the Mirror is defined under **Folder to store mirrored files**. Click **Folder** to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be entered in the **Username** and **Password** fields. If the selected destination folder is located on a network disk running the Windows NT/2000/XP operating system, the username and password specified must have write privileges for the selected folder. The username and password should be entered in the format *Domain/User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

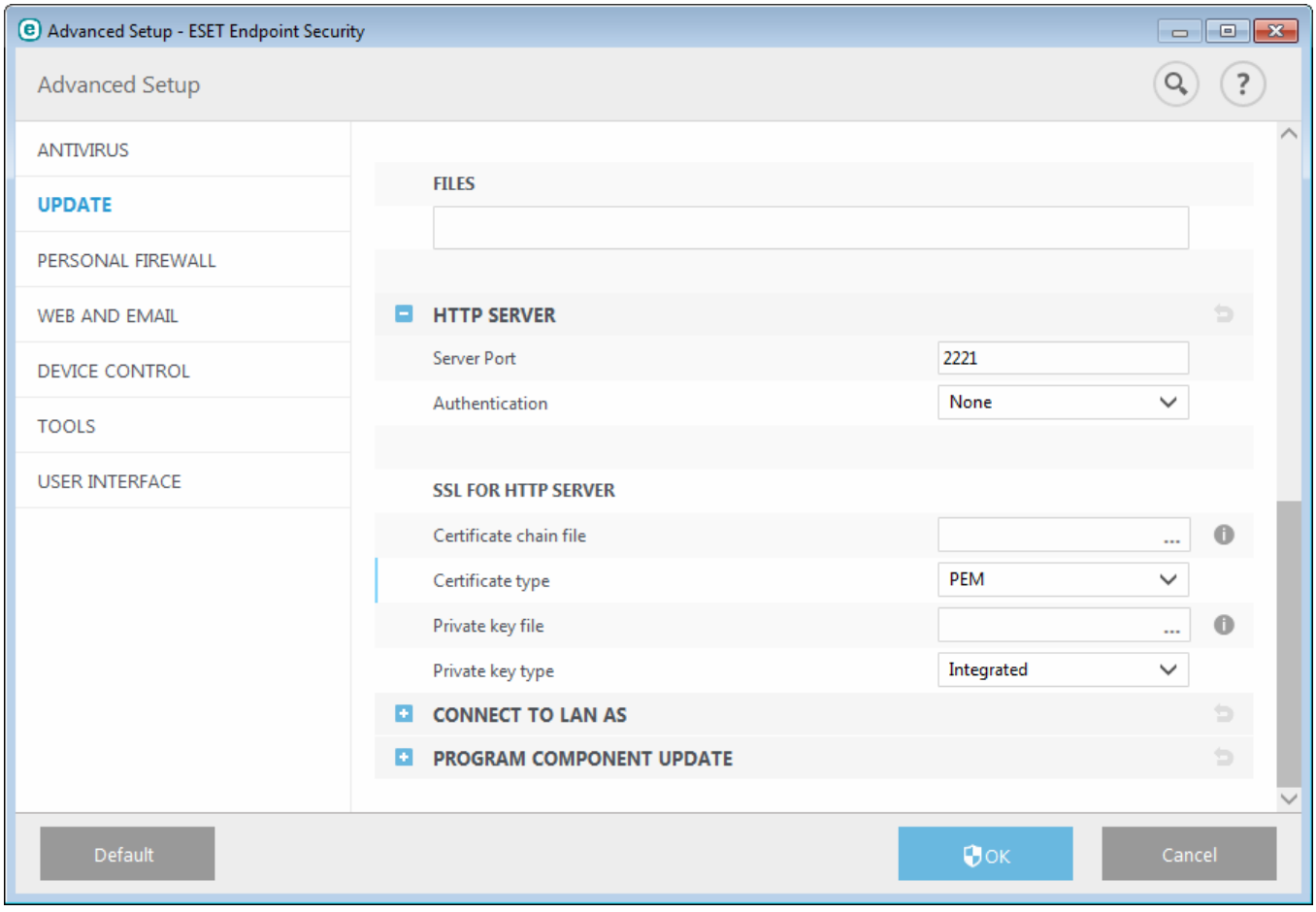
**Files** – When configuring the Mirror you can specify the language versions of updates you want to download. Languages selected must be supported by the mirror server configured by the user.

### HTTP server

**Server port** – By default, the Server port is set to 2221.

**Authentication** – Defines the method of authentication used for accessing update files. The following options are available: **None**, **Basic** and **NTLM**. Select **Basic** to use base64 encoding with basic username and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **None**, which grants access to the update files with no need for authentication.

Append your **Certificate chain file**, or generate a self-signed certificate if you want to run HTTP server with HTTPS (SSL) support. The following certificate types are available: ASN, PEM and PFX. For additional security, you can use HTTPS protocol to download update files. It is almost impossible to track data transfers and login credentials using this protocol. The **Private key type** option is set to **Integrated** by default (and therefore the **Private key file** option is disabled by default). This means that the private key is a part of the selected certificate chain file.




### Connect to LAN as

**Local user type** – The **System account (default)**, **Current user**, and **Specified user** settings will be displayed in their corresponding drop-down menus. **Username** and **Password** settings are optional. See Connect to LAN as.

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

### Program component update

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

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

### 3.9.5.1.6.1 Updating from the Mirror

There are two basic methods to configure a Mirror, which is essentially a repository where clients can download update files. The folder with update files can be presented as a shared network folder or as an HTTP server.

#### Accessing the Mirror using an internal HTTP server

This configuration is the default, specified in the predefined program configuration. To allow access to the Mirror using the HTTP server, navigate to **Advanced setup** > **Update** > **Mirror** and select **Create update mirror**.

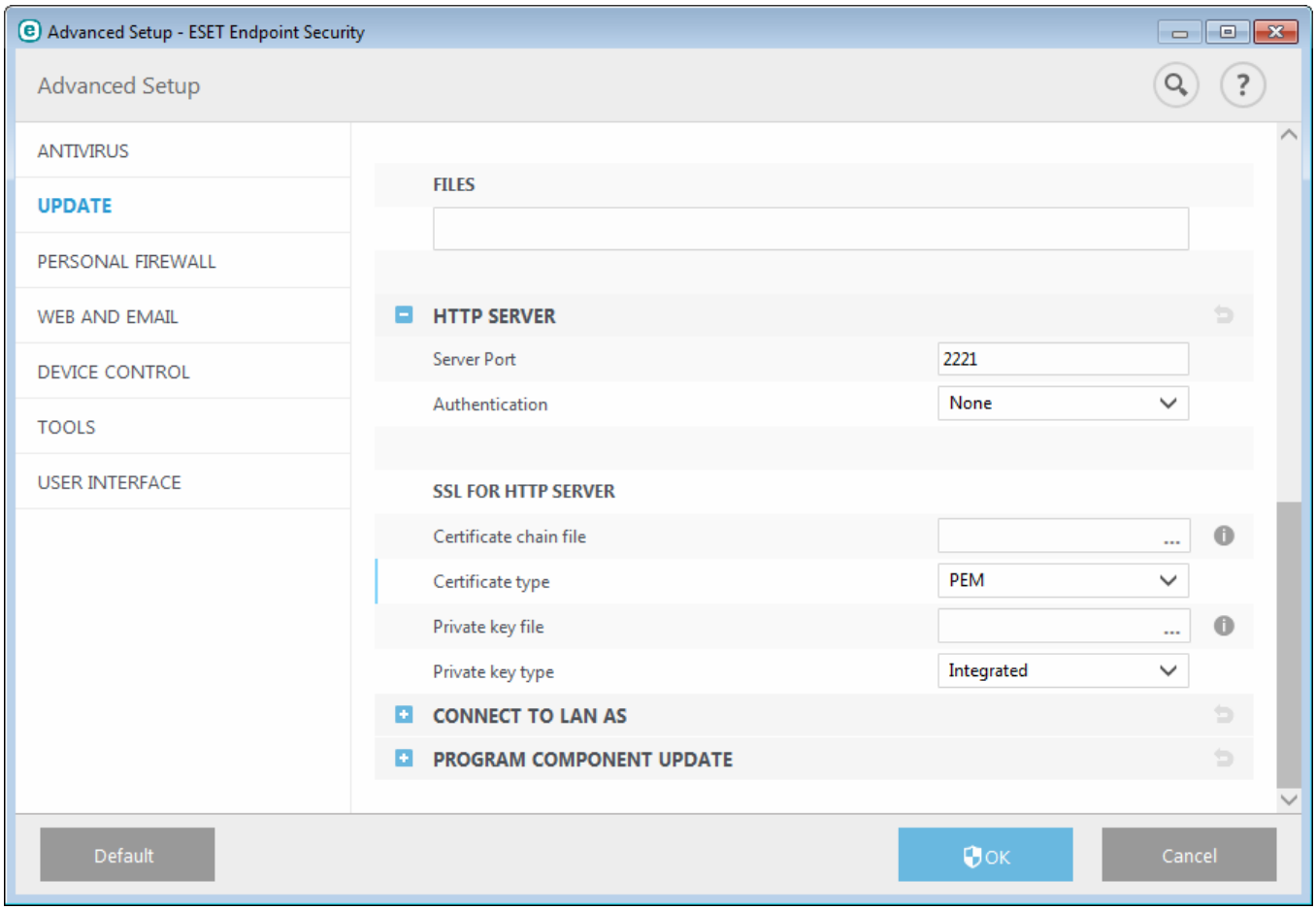
In the **HTTP Server** section of the **Mirror** tab you can specify the **Server port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to **2221**. The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **None**, **Basic**, and **NTLM**. Select **Basic** to use base64 encoding with basic username and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **None**, which grants access to the update files with no need for authentication.

***Warning:*** If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Endpoint Security instance creating it.

#### SSL for HTTP Server

Append your **Certificate chain file**, or generate a self-signed certificate if you want to run HTTP server with HTTPS (SSL) support. The following certificate types are available: **PEM, PFX** and **ASN**. For additional security, you can use HTTPS protocol to download update files. It is almost impossible to track data transfers and login credentials using this protocol. **Private key type** is set to **Integrated** by default, which means that the private key is a part of the selected certificate chain file.

**NOTE**: An error **Invalid Username and/or Password** will appear in the Update pane from the main menu after several unsuccessful attempts to update the virus signature database from the Mirror. We recommend that you navigate to **Advanced setup** > **Update** > **Mirror** and check the Username and Password. The most common reason for this error is incorrectly entered authentication data.



After your Mirror server is configured, you must add the new update server on client workstations. To do this, follow the steps below:

- Access **Advanced setup** (F5) and click **Update** > **Basic**.
- Disengage **Choose automatically** and add a new server to the **Update server** field using one of the following formats:
  *http://IP_address_of_your_server:2221*
  *https://IP_address_of_your_server:2221* (if SSL is used)

**Accessing the Mirror via system shares**

First, a shared folder should be created on a local or network device. When creating the folder for the Mirror, you must provide *"write"* access for the user who will save update files to the folder and *"read"* access for all users who will update ESET Endpoint Security from the Mirror folder.

Next, configure access to the Mirror in **Advanced setup** > **Update** > **Mirror** tab by disabling **Provide update files via internal HTTP server**. This option is enabled by default in the program install package.

If the shared folder is located on another computer in the network, you must enter authentication data to access the other computer. To enter authentication data, open ESET Endpoint Security **Advanced setup** (F5) and click **Update** > **Connect to LAN as**. This is the same setting used for updating, as described in the Connect to LAN as section.

After the Mirror configuration is complete, on client workstations set *UNC**PATH* as the update server using the steps below:

1. Open ESET Endpoint Security **Advanced setup** and click **Update** > **Basic**.
2. Click the **Update server** field and add a new server using the *UNC**PATH* format.

**NOTE**: For updates to function properly, the path to the Mirror folder must be specified as a UNC path. Updates from mapped drives may not work.

The last section controls program components (PCUs). By default, downloaded program components are prepared to copy to the local mirror. If **Program component update** is activated, there is no need to click **Update**, because files are copied to the local mirror automatically when they are available. See Update mode for more information about program component updates.

#### 3.9.5.1.6.2 Troubleshooting Mirror update problems

In most cases, problems during an update from a Mirror server are caused by one or more of the following: incorrect specification of the Mirror folder options, incorrect authentication data to the Mirror folder, incorrect configuration on local workstations attempting to download update files from the Mirror, or by a combination of the reasons above. Below is an overview of the most frequent problems which may occur during an update from the Mirror:

**ESET Endpoint Security reports an error connecting to Mirror server** – Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates. To verify the folder, click the Windows **Start** menu, click **Run**, enter the folder name and click **OK**. The contents of the folder should be displayed.

**ESET Endpoint Security requires a username and password** – Likely caused by incorrect authentication data (username and password) in the update section. The username and password are used to grant access to the update server, from which the program will update itself. Make sure that the authentication data is correct and entered in the correct format. For example, *Domain/Username*, or *Workgroup/Username*, plus the corresponding Passwords. If the Mirror server is accessible to "Everyone", please be aware that this does not mean that any user is granted access. "Everyone" does not mean any unauthorized user, it just means that the folder is accessible for all domain users. As a result, if the folder is accessible to "Everyone", a domain username and password will still need to be entered in the update setup section.

**ESET Endpoint Security reports an error connecting to the Mirror server** – Communication on the port defined for accessing the HTTP version of the Mirror is blocked.

### 3.9.5.2 How to create update tasks

Updates can be triggered manually by clicking **Update virus signature database** in the primary window displayed after clicking **Update** from the main menu.

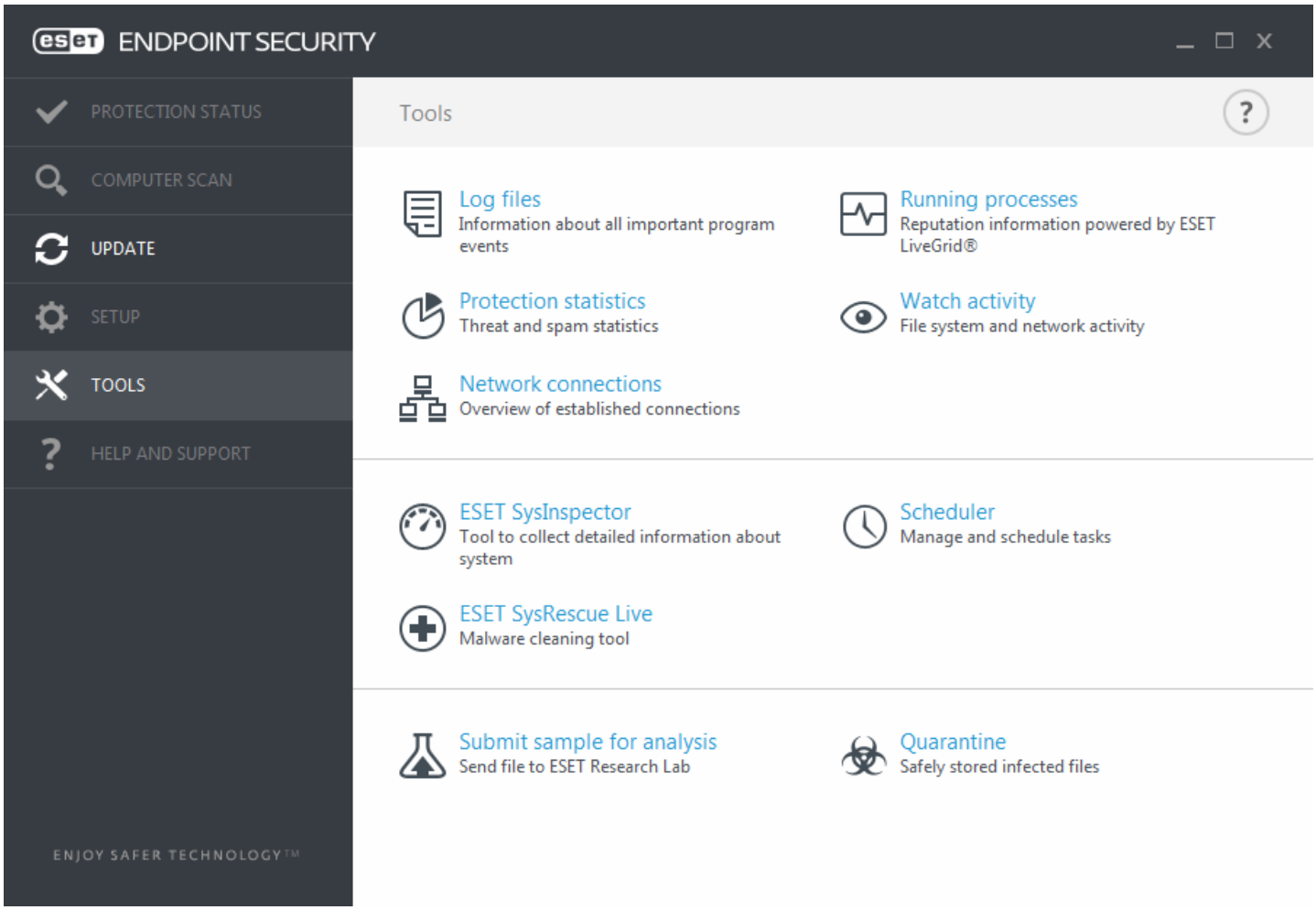
Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following tasks are activated in ESET Endpoint Security:

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

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

## 3.9.6 Tools

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



This menu includes the following tools:

- Log files
- Protection statistics
- Watch activity
- Running processes (if ESET LiveGrid® is enabled in ESET Endpoint Security)
- Scheduler
- Quarantine
- Network connections (if Personal firewall is enabled in ESET Endpoint Security)
- ESET SysInspector

**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 the Submission of samples for analysis section.

**ESET SysRescue** – Redirects you to the ESET SysRescue Live page, where you can download the ESET SysRescue Live image or Live CD/USB Creator for Microsoft Windows operating systems.

### 3.9.6.1 Log files

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

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

- **Detected threats** – The threat log offers detailed information about infiltrations detected by ESET Endpoint Security modules. The information includes the time of detection, name of infiltration, location, the performed action and the name of the user logged in at the time the infiltration was detected. Double-click any log entry to display its details in a separate window.
- **Events** – All important actions performed by ESET Endpoint Security are recorded in the event log. The event log contains information about events and errors that have occurred in the program. It is designed to help system administrators and users resolve problems. Often the information found here can help you find a solution for a problem occurring in the program.
- **Computer scan** – All scan results are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view the details of the respective scan.
- **HIPS** – Contains records of specific rules that are marked for recording. The protocol shows the application that called the operation, the result (whether the rule was permitted or prohibited) and the name of the rule created.
- **Personal firewall** – The firewall log displays all remote attacks detected by the Personal firewall. Here you will find information about any attacks on your computer. The *Event* column lists the detected attacks. The *Source* column tells you more about the attacker. The *Protocol* column reveals the communication protocol used for the attack. Analysis of the firewall log may help you to detect system infiltration attempts in time to prevent unauthorized access to your system. For more details on particular network attacks, see IDS and advanced options.
- **Filtered websites** – This list is useful if you want to view a list of websites that were blocked by Web access protection or Web control. In these logs you can see the time, URL, user and application that opened a connection to the particular website.
- **Antispam protection** – Contains records related to email messages that were marked as spam.
- **Web control** – Shows blocked or allowed URL addresses and details about how they are categorized. The *Action performed* column tells you how filtering rules were applied.
- **Device control** – Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device type, serial

number, vendor name and media size (if available).

In each section, the displayed information can be copied to the clipboard (keyboard shortcut **Ctrl + C**) by selecting the entry and clicking **Copy**. The **Ctrl** and **Shift** keys can be used to select multiple entries.

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

You can bring up the context menu by right-clicking a specific record. 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.../Find...** – After clicking this option, the Search in log 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.
- **Scroll log** – Leave this option enabled to auto scroll old logs and view active logs in the **Log files** window.

#### 3.9.6.1.1 Search in log

Logs store information about important system events. The log filtering feature allows you to display records about a specific type of event.

Enter the search keyword into the **Find text** field. If you wish to search the keyword in specific columns, change the filter in the **Search in columns** drop-down menu.

**Record types** – Choose one or more record log 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, built-in firewall, etc...).

**Time period** – Define the time period from which you want the results to be displayed.

**Match whole words only** – Select this check box if you want to search for specific 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.

**Search upwards** – Search results that appear higher in the document will be displayed first.

### 3.9.6.2 Proxy server setup

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

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

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

If communication with the proxy server requires authentication, select **Proxy server requires authentication** and enter a valid **Username** and **Password** into the respective fields. Click **Detect** 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.

Proxy server settings can also be established from Advanced update setup (**Advanced setup** > **Update** > **HTTP Proxy** 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.

### 3.9.6.3 Scheduler

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

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

The Scheduler serves to schedule the following tasks: virus signature database update, scanning task, system startup file check and log maintenance. You can add or delete tasks directly from the main Scheduler window (click **Add task** or **Delete** at the bottom). Right click anywhere in the Scheduler window to perform the following actions: display detailed information, perform the task immediately, add a new task, and delete an existing task. Use the 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**
- **Automatic startup file check** (after user logon)
- **Automatic startup file check** (after successful update of the virus signature database)
- **Automatic first scan**

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

**Add a new task**

1. Click **Add task** at the bottom of the window.
2. Enter a name of the task.

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

- **Run external application** – Schedules the execution of an external application.
- **Log maintenance** – Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** – Checks files that are allowed to run at system startup or logon.
- **Create a computer scan** – 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.
- **First-scan** – By default, 20 minutes after installation or reboot a Computer scan will be performed as a low priority task.
- **Update** – Schedules an Update task by updating the virus signature database and program modules.

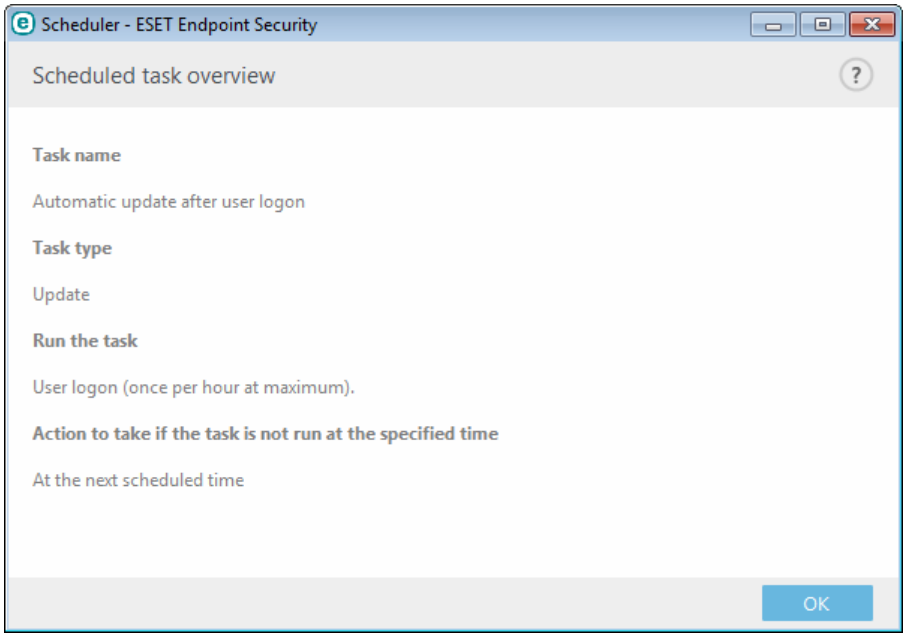
4. Turn on the **Enabled** switch if you want to activate the task (you can do this later by selecting/deselecting checkbox in the list of scheduled tasks), click **Next** and select one of the timing options:

- **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 be run on the selected day and time.
- **Event triggered** – The task will be performed on a specified event.

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

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

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



### 3.9.6.4 Protection statistics

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

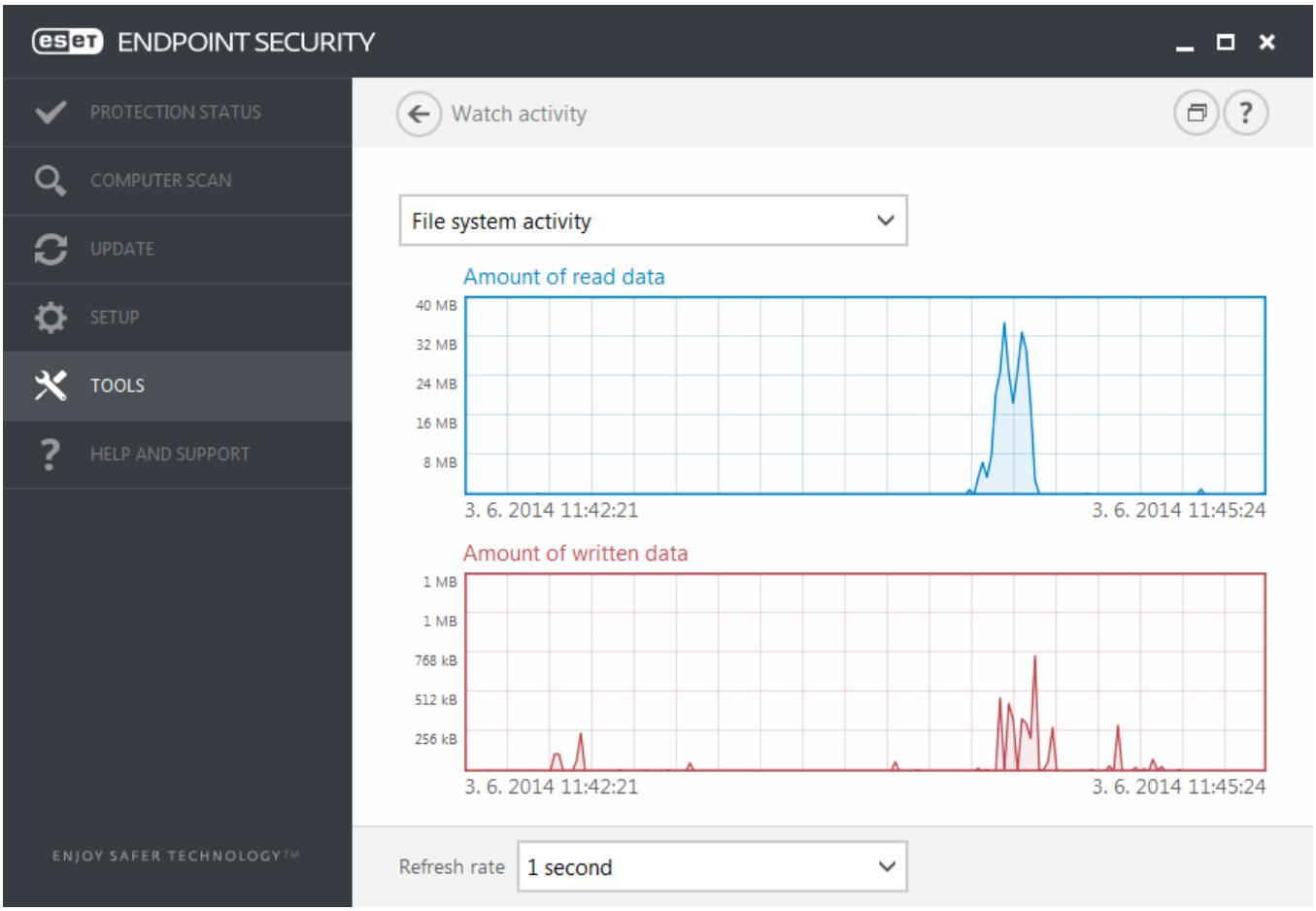
The following statistic graphs are available:

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

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

### 3.9.6.5 Watch activity

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




The following options are available:

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

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

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

### 3.9.6.6 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.

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:

- **Open** – 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 all** – Deletes all logs.
- **Export...** – Exports the log to an *.xml* file or zipped *.xml*.

### 3.9.6.7 ESET LiveGrid®

ESET LiveGrid® is an advanced early warning system comprised of several cloud-based technologies. It helps detect emerging threats based on reputation and improves scanning performance by means of whitelisting. New threat information is streamed in real-time to the cloud, which enables the ESET Malware Research Lab to provide timely response and consistent protection at all times. Users 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®. When installing ESET Endpoint Security, select one of the following options:

1. You can decide not to enable ESET LiveGrid®. Your software will not lose any functionality, but in some cases ESET Endpoint Security may respond slower to new threats than virus signature database update.
2. You can configure ESET LiveGrid® to submit anonymous information about new threats and where the new threatening code was detected. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat 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 Endpoint Security is configured to submit suspicious files for detailed analysis to the ESET Virus Lab. Files with certain extensions such as *.doc* or *.xls* are always excluded. You can also add other extensions if there are

particular files that you or your organization want to avoid sending.

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 **Tools** > **ESET LiveGrid®**.

**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.

**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.

**Submit files** – Suspicious files resembling threats, and/or files with unusual characteristics or behavior are submitted to ESET for analysis.

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.

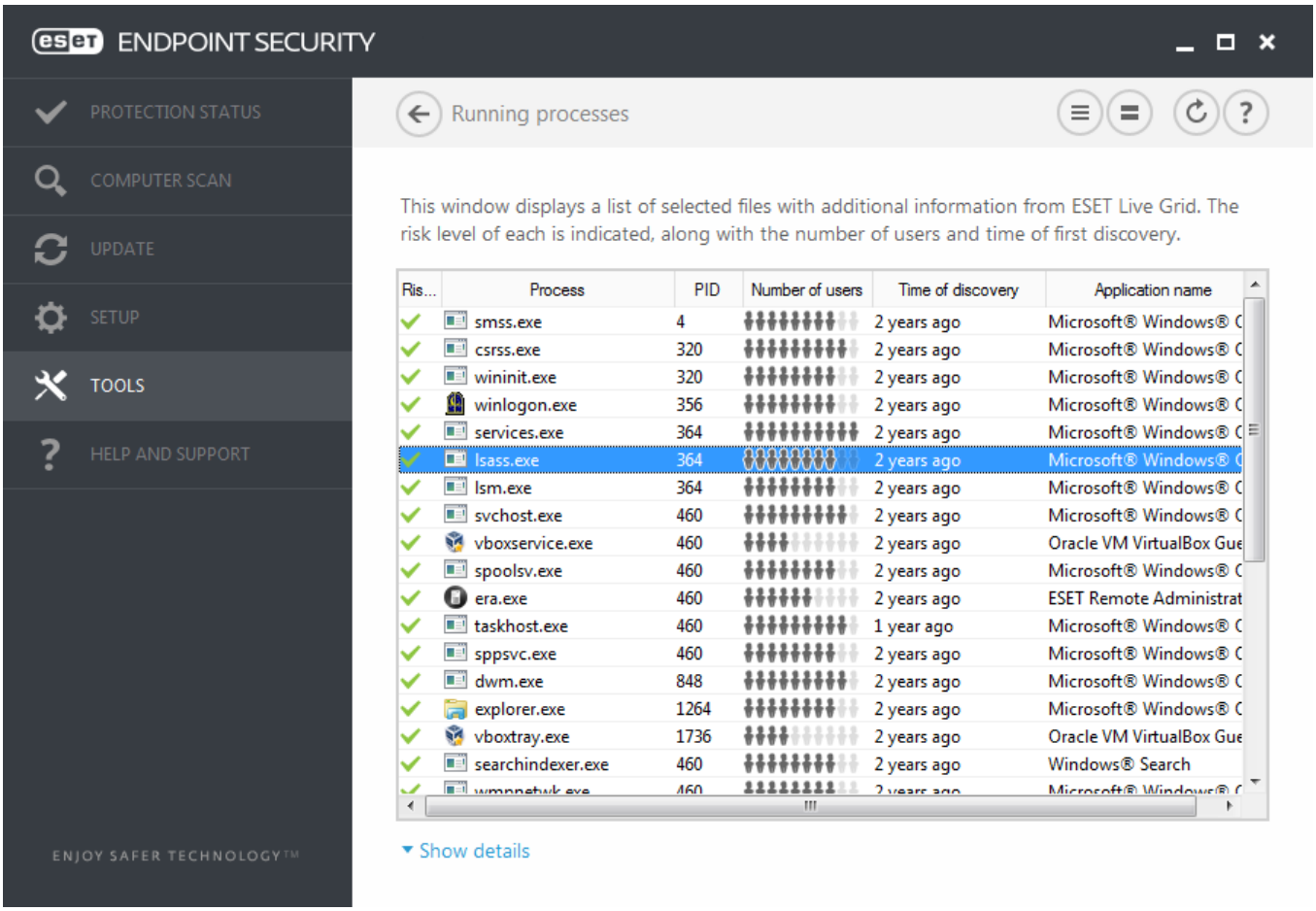
**Contact email (optional)** – Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

**Exclusion** – 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.

### 3.9.6.8 Running processes

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




**Risk level** – In most cases, ESET Endpoint Security and ESET LiveGrid® technology assign risk levels to objects (files, processes, registry keys, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a 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. You can open Task Manager by right-clicking an empty area on the taskbar and then clicking Task Manager, or by pressing **Ctrl**+**Shift**+**Esc** on your keyboard.

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

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

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

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

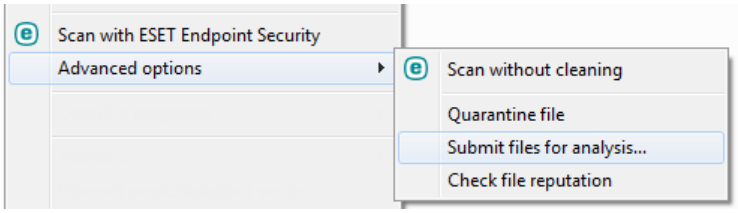
**Note:** When an application is marked as Unknown (orange) security level, it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, use the submit file for analysis feature to send the file to the ESET Virus Lab. If the file turns out to be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

**Application name** – The given name of a program or process.

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

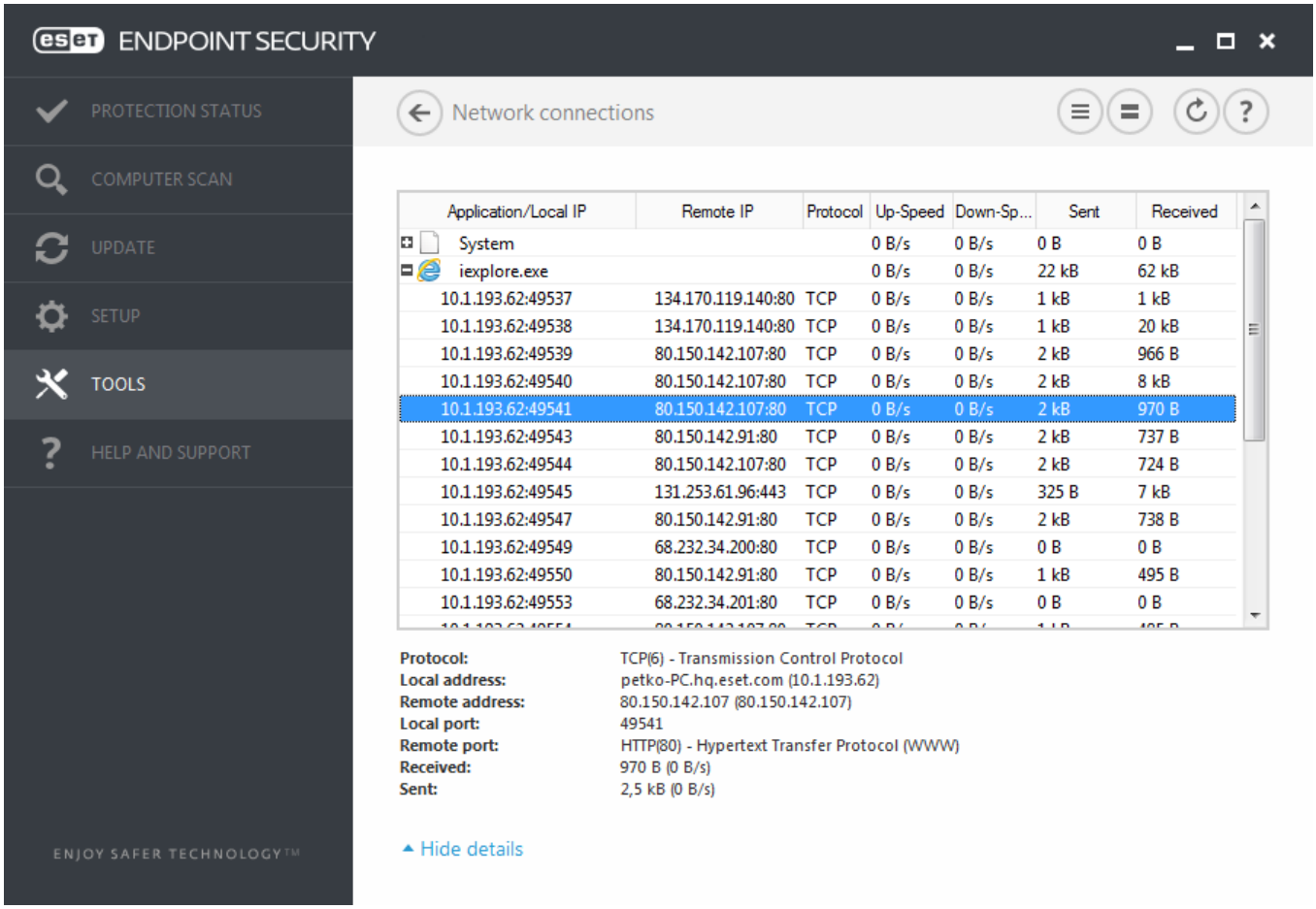
- **Path** – Location of an application on your computer.
- **Size** – File size either in kB (kilobytes) or MB (megabytes).
- **Description** – File characteristics based on the description from the operating system.
- **Company** – Name of the vendor or application process.
- **Version** – Information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

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




### 3.9.6.9 Network connections

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




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

**Columns**

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

**Remote IP** – IP address and port number of the particular remote computer.

**Protocol** – Transfer protocol used.

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

**Sent/Received** – Amount of data exchanged within the connection.

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

Select an application or IP address in the Network connections screen and right-click on it will show context menu with following structure:

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

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

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

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

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

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

**Refresh speed** – Choose the frequency to refresh the active connections.

**Refresh now** – Reloads the Network connections window.

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

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

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

### 3.9.6.10 Submission of samples for analysis

The sample submission dialog enables you to send a file or a site to ESET for analysis and can be found in **Tools** > **Submit sample for analysis**. If you find a suspiciously behaving file on your computer or suspicious site on the Internet, you can submit it to the ESET Virus Lab for analysis. If the file turns out to be a malicious application or website, its detection will be added to an upcoming update.

Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using WinRAR/ZIP, protect the archive with the password "infected" and send it to samples@eset.com. Please remember to use a descriptive subject and enclose as much information about the file as possible (for example, the website you downloaded it from).

**NOTE:** Before submitting a sample to ESET, make sure it meets one or more of the following criteria:
- the file or website is not detected at all
- the file or website is incorrectly detected as a threat

You will not receive a response unless further information is required for analysis.

Select the description from the **Reason for submitting the sample** drop-down menu that best fits your message:

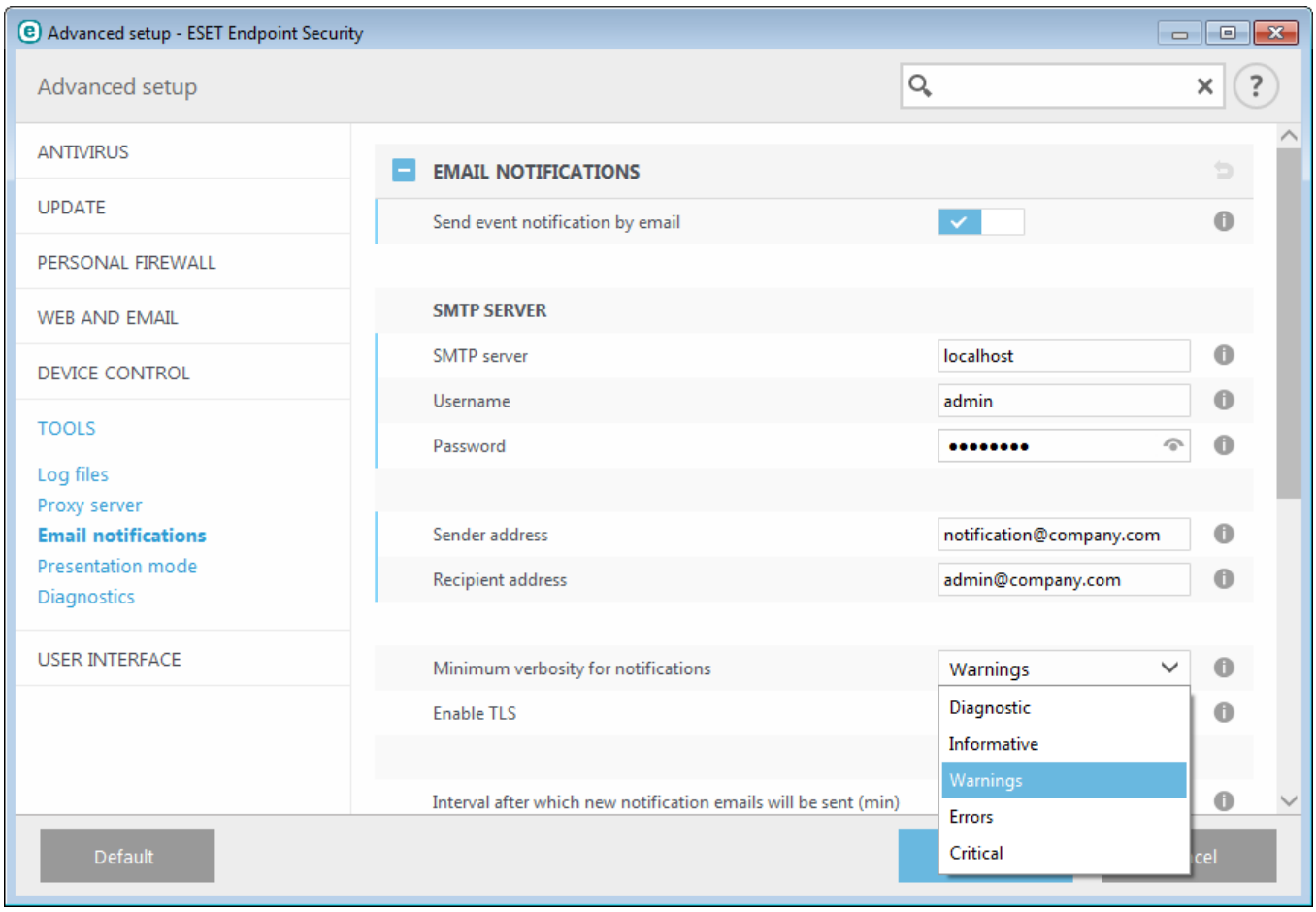
- **Suspicious file**
- **Suspicious site** (a website that is infected by any malware),
- **False positive file** (file that is detected as an infection but are not infected),
- **False positive site**
- **Other**

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

**Contact email** – This contact email is sent along with suspicious files to ESET and may be used to contact you if further information is required for analysis. Entering a contact email is optional. You will not get a response from ESET unless more information is required, since each day our servers receive tens of thousands of files, making it impossible to reply to all submissions.

### 3.9.6.11 Email notifications

ESET Endpoint Security 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 (e.g. *smtp.provider.com:587*, predefined port is 25).

**NOTE:** SMTP servers with TLS encryption are supported by ESET Endpoint Security.

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

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

**Recipient address** – This field specifies the recipient address that will be displayed in the header of notification emails.

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.

**Sent 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.

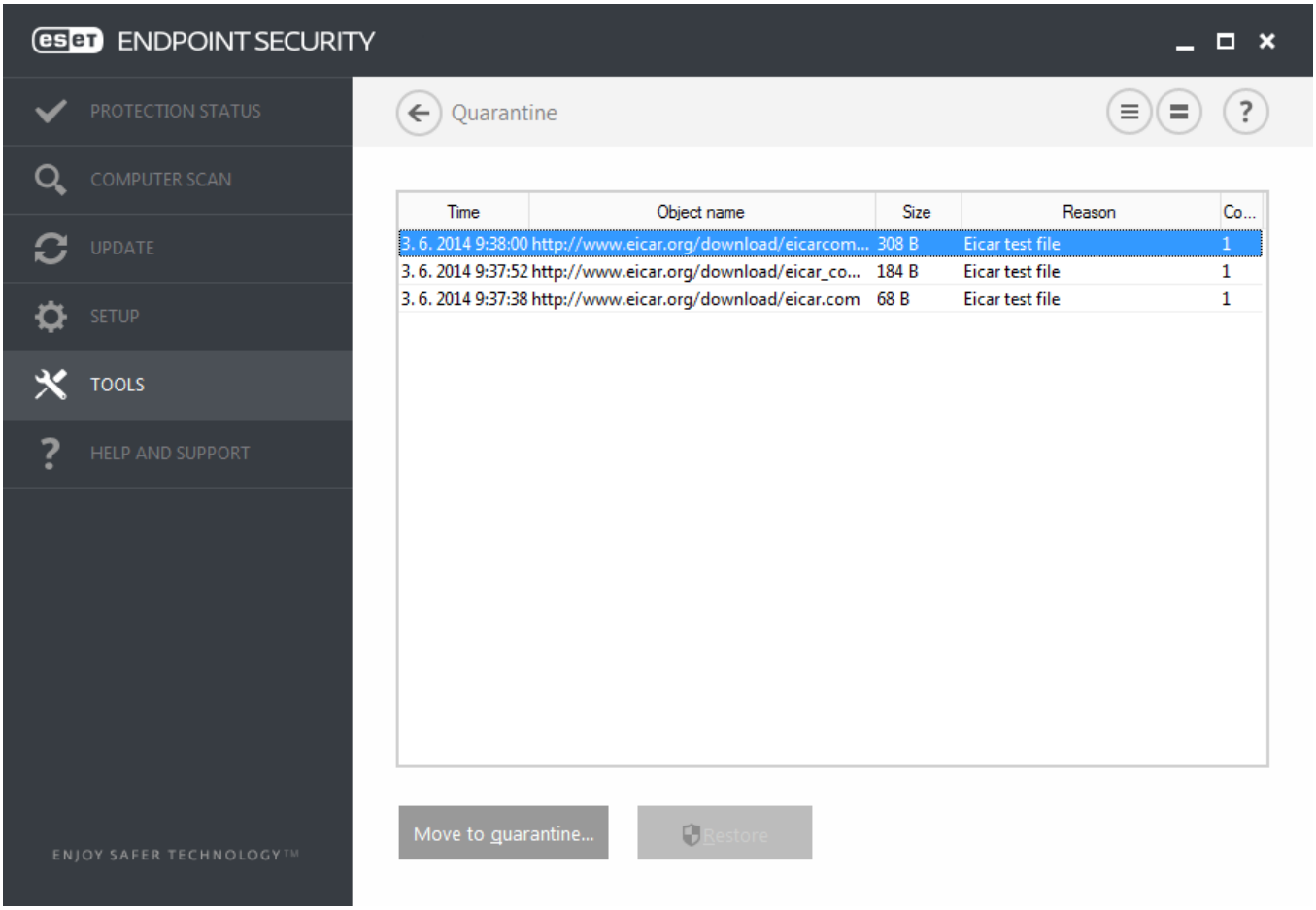
**Use local alphabetic characters** – Converts an email message to the ANSI character encoding based upon Windows Regional settings (for example, windows-1250). If you leave this deselected, a message will be converted and encoded in ACSII 7-bit (for example "á" will be changed to "a" and an unknown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

### 3.9.6.12 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 Endpoint Security.

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 Virus 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 Endpoint Security automatically quarantines deleted files (if you have not disabled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking **Quarantine**. The original file will 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. To restore a quarantined file, right-click it in the Quarantine window and select **Restore** from the context menu. If a file is marked as a potentially unwanted application, **Restore and exclude from scanning** will also be available. The context menu also contains 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 has quarantined a harmless file by mistake, exclude the file from scanning after restoring it and send the file to ESET Customer Care.

**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 incorrectly detected as a threat 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.

#### 3.9.6.13 Microsoft Windows update

The Windows update feature is an important component of protecting users from malicious software. For this reason, it is vital that you install Microsoft Windows updates as soon as they become available. ESET Endpoint Security notifies you about missing updates according to the level you specify. The following levels are available:

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

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

### 3.9.7 User interface

The **User interface** section allows you to configure the behavior of the program's Graphical user interface (GUI).

Using the User Interface elements tool, you can adjust the program's visual appearance and effects used.

To provide maximum security of your security software, you can prevent any unauthorized changes using the Access setup tool.

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

If you choose not to display some notifications, they will be displayed in **User interface elements** > **Application statuses**. Here you can check their status or alternatively prevent to display these notifications.

The Context menu integration is displayed after right-clicking on the selected object. Use this tool to integrate the ESET Endpoint Security control elements into the context menu.

Presentation mode is useful for users, who want to work with an application and not be interrupted by pop-up windows, scheduled tasks and any components that could load the processor and RAM.

#### 3.9.7.1 User interface elements

User interface configuration options in ESET Endpoint Security allow you to adjust the working environment to fit your needs. These configuration options are accessible in the **User interface** > **User interface elements** branch of the ESET Endpoint Security Advanced setup tree.

In the **User interface elements** section, you can adjust the working environment. Use the **GUI start mode** drop-down menu to select from the following Graphical user interface (GUI) start modes:

**Full** – The complete GUI will be displayed.

**Minimal** – The GUI is available, but only notifications are displayed to the user.

**Manual** – No notifications, or alerts will be displayed.

**Silent** – Neither the GUI, nor notifications and alerts will be displayed. This mode can be useful in situations where you need to preserve system resources. Silent mode can only be started by the Administrator.

**NOTE**: Once the Minimal GUI start mode is selected and your computer is restarted, notifications will be displayed but the graphical interface will not. To revert to full graphical user interface mode, run the GUI from the Start menu under **All Programs** > **ESET** > ESET Endpoint Security as an administrator, or you can do this via ESET Remote Administrator using a policy.

If you want to deactivate the ESET Endpoint Security splash-screen, deselect **Show splash-screen at startup**.

To have ESET Endpoint Security play a sound when important events occur during a scan, for example when a threat is discovered or when the scan has finished, select **Use sound signal**.

**Integrate into the context menu** – Integrate the ESET Endpoint Security control elements into the context menu.

**Statuses**

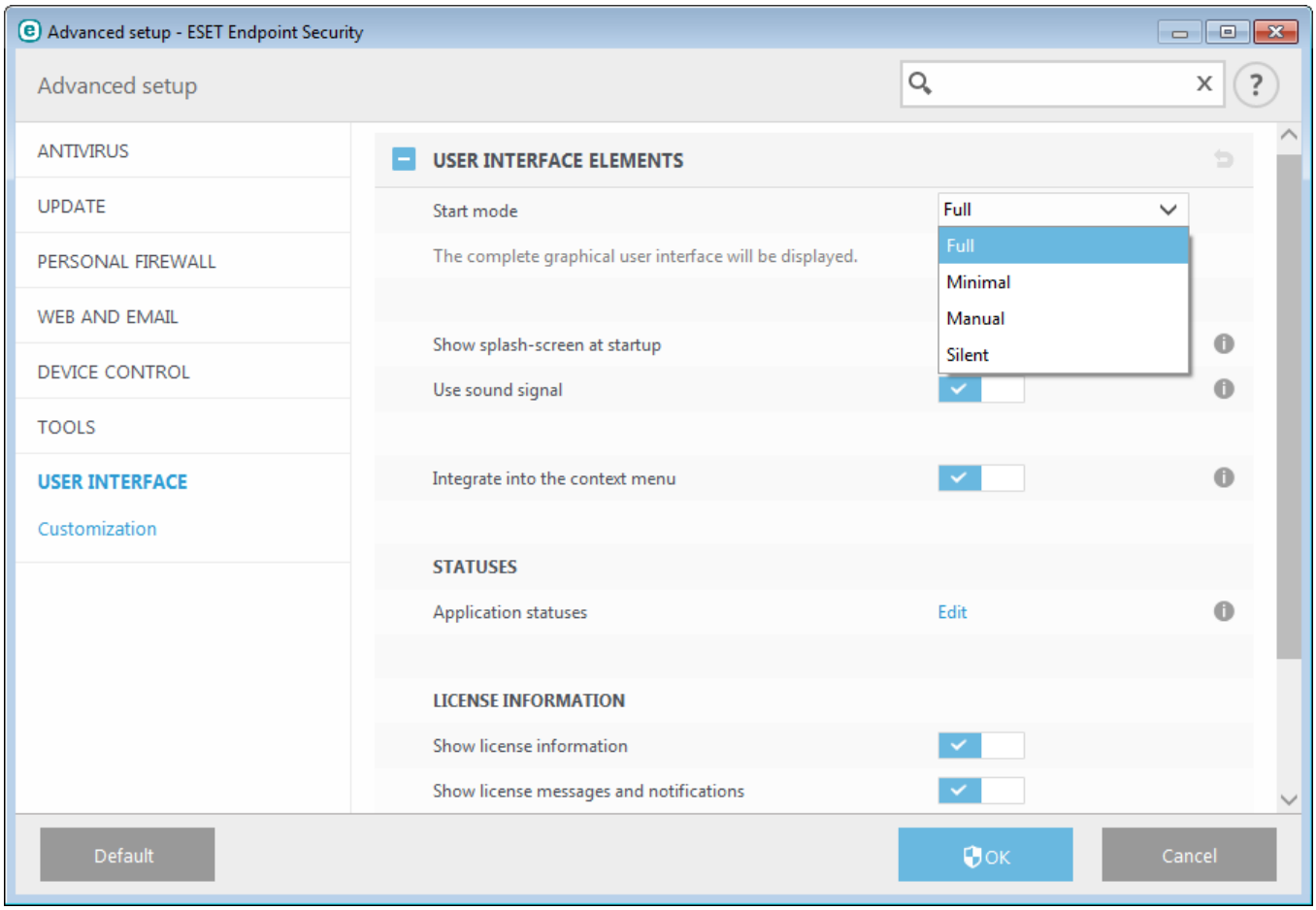
**Application statuses** – Click **Edit** button to manage (disable) statuses that are displayed in the **Protection status** pane in main menu.

**License information**

**Show license information** – When disabled, the license information on **Protection status** and **Help and support** screen will not be displayed.

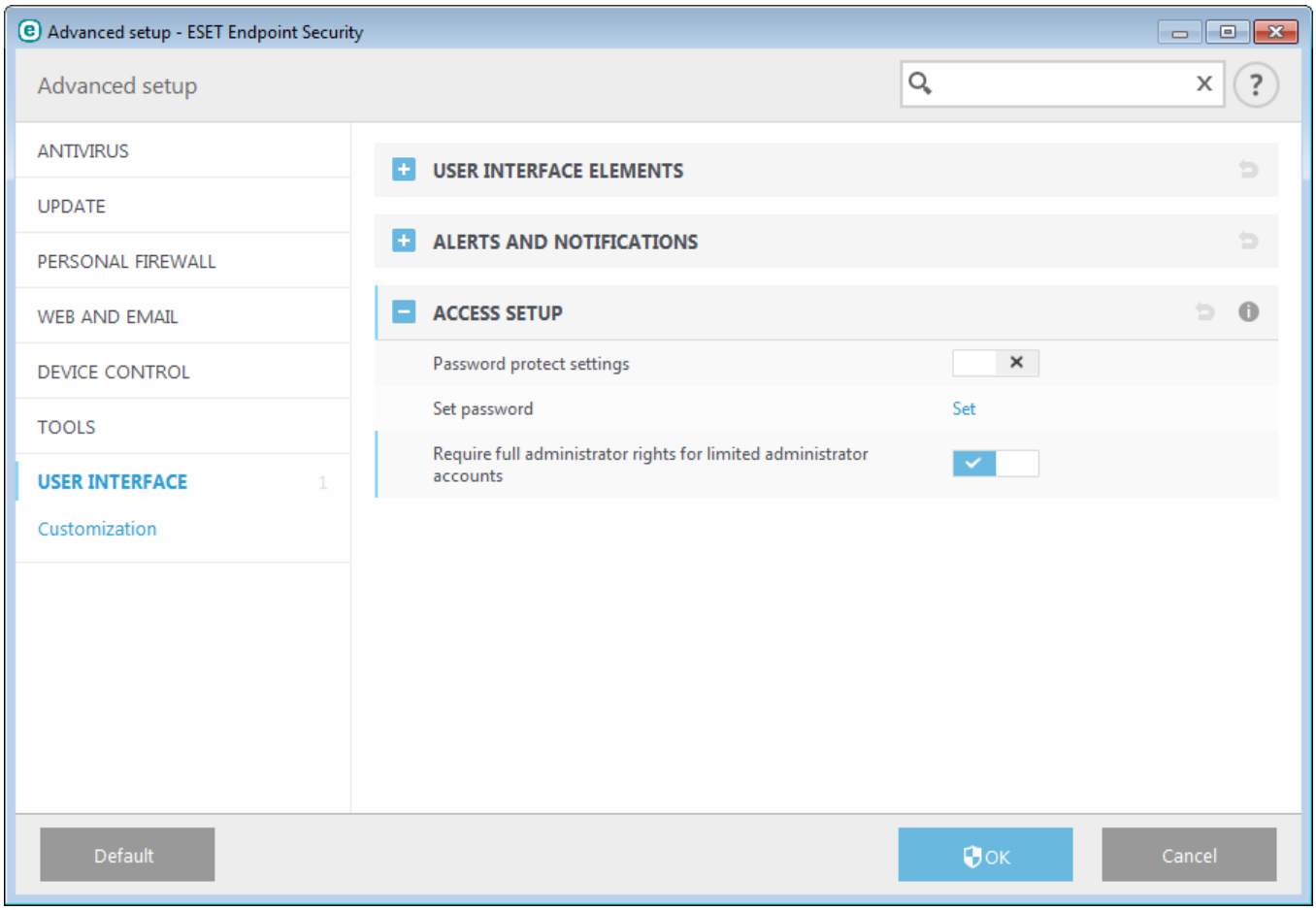
**Show license messages and notifications** – When disabled, the notifications and messages will only be displayed when license expired.

**NOTE**: License information settings are applied but not accessible for ESET Endpoint Security activated with MSP license.



### 3.9.7.2 Access setup

In order to provide maximum security for your system, it is essential that ESET Endpoint Security is correctly configured. Any unqualified change may result in a loss of important data. To avoid unauthorized modifications, the setup parameters of ESET Endpoint Security can be password protected. Configuration settings for password protection are located in **Advanced setup** (F5) under **Access setup** > **User interface**.




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

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

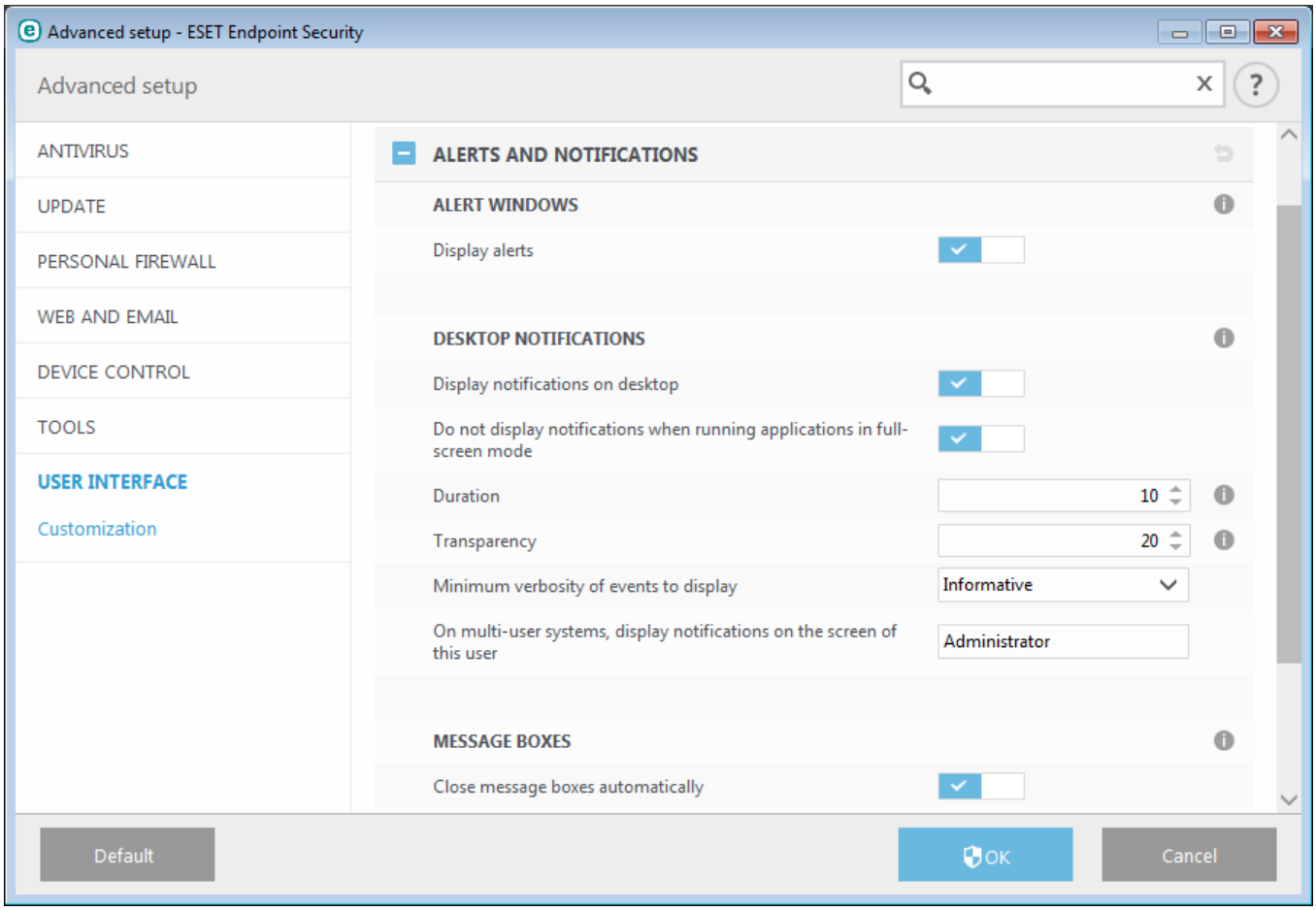
**Require full administrator rights for limited administrator accounts** – Leave this option active to prompt the current user (if he or she does not have administrator rights) to enter the administrator username and password when modifying certain system parameters (similar to the UAC in Windows Vista). The modifications include disabling protection modules or turning off the firewall.

For Windows XP only:

**Require administrator rights (system without UAC support)** – Enable this option to have ESET Endpoint Security prompt for administrator credentials.

### 3.9.7.3 Alerts and notifications

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 Endpoint Security. 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).

#### 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**. Turn the **Do not display notifications when running applications in full screen mode** switch on to suppress all non-interactive notifications. More detailed options, such as notification display time and window transparency can be modified below.

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 , built-in firewall, 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.

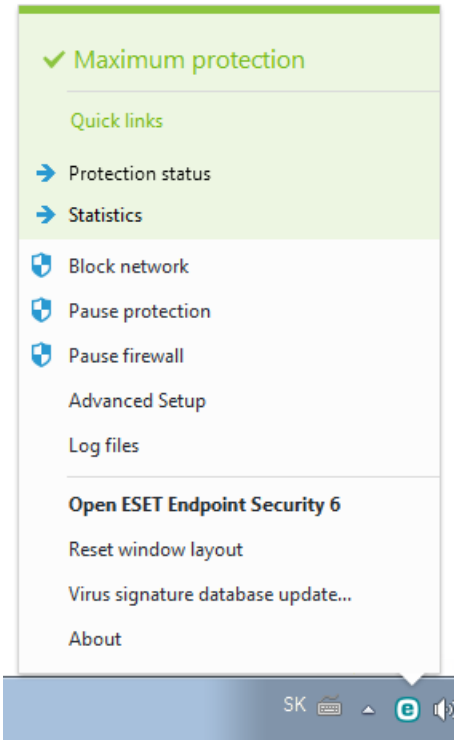
**Message boxes**

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.

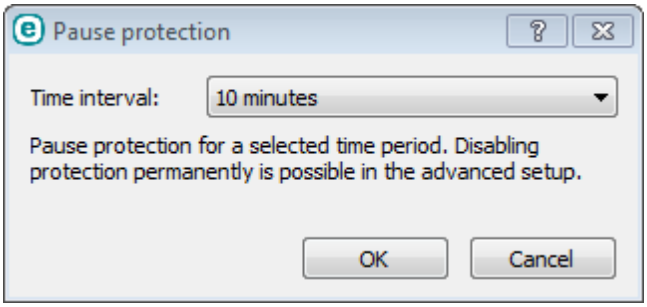
### 3.9.7.4 System tray icon

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




**Block network** – Personal firewall will block all outgoing / incoming network and internet traffic.

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




The **Time interval** drop-down menu represents the period of time that Antivirus and antispyware protection will be disabled for.

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

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

**Advanced setup** – Select this option to enter the **Advanced setup** tree. You can also access Advanced setup by pressing the F5 key or navigating to **Setup** > **Advanced setup**.

**Log files** – Log files contain information about all important program events that have occurred and provide an overview of detected threats.

**Hide ESET Endpoint Security** – Hide the ESET Endpoint Security window from the screen.

**Reset window layout** – Resets the ESET Endpoint Security window to its default size and position on the screen.

**Virus signature database update** – Starts updating the virus signature database to ensure your level of protection against malicious code.

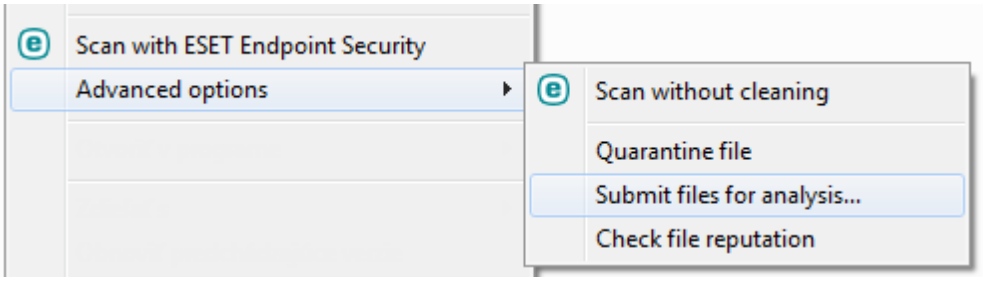
**About** – Provides system information, details about the installed version of ESET Endpoint Security and the installed program modules as well as your license expiration date. Information about your operating system and system resources can be found at the bottom of the page.

#### 3.9.7.5 Context menu

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

It is possible to integrate ESET Endpoint Security control elements into the context menu. Setup option for this functionality are available in the Advanced setup tree under **User Interface** > **User interface elements**.

**Integrate into the context menu** – Integrate the ESET Endpoint Security control elements into the context menu.




## 3.10 Advanced user

### 3.10.1 Profile manager

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

#### On-demand computer scan

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

To create a new profile, open the Advanced setup window (F5) and click **Antivirus** > **On-demand computer scan** and then **Edit** next to **List of profiles**. The **Selected profile** drop-down menu that lists existing scan profiles. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

**Example:** Suppose that you want to create your own scan profile and the Smart scan configuration is partially suitable, but you don't 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 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.

**Selected 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.

### 3.10.2 Diagnostics

Diagnostics provides application crash dumps of ESET processes (for example, *ekrn*). If an application crashes, a dump will be generated. This can help developers debug and fix various ESET Endpoint Security problems. Click the drop-down menu next to **Dump type** and select one of three available options:

- Select **Disable** (default) to disable this feature.
- **Mini** – 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.

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

Log files can be found in:
*C:\ProgramData\ESET\ESET Smart Security\Diagnostics* in Windows Vista and later or *C:\Documents and Settings\All Users\...* in older versions of Windows.

**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.

### 3.10.3 Import and export settings

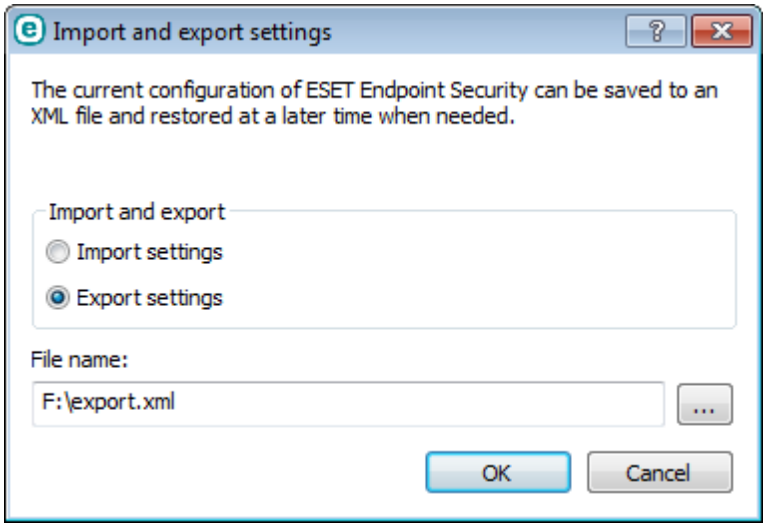
You can import or export your customized ESET Endpoint Security .xml configuration file from the **Setup** menu.

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

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

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

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




### 3.10.4 Command Line

ESET Endpoint Security's antivirus module can be launched via the command line – manually (with the "ecls" command) or with a batch ("bat") file. ESET Command-line scanner usage:

```
ecls [OPTIONS..] FILES..
```

The following parameters and switches can be used while running the on-demand scanner from the command line:

**Options**

| | |
|---|---|
| /base-dir=FOLDER | load modules from FOLDER |
| /quar-dir=FOLDER | quarantine FOLDER |
| /exclude=MASK | exclude files matching MASK from scanning |
| /subdir | scan subfolders (default) |
| /no-subdir | do not scan subfolders |
| /max-subdir-level=LEVEL | maximum sub-level of folders within folders to scan |
| /symlink | follow symbolic links (default) |
| /no-symlink | skip symbolic links |
| /ads | scan ADS (default) |
| /no-ads | do not scan ADS |
| /log-file=FILE | log output to FILE |
| /log-rewrite | overwrite output file (default – append) |
| /log-console | log output to console (default) |
| /no-log-console | do not log output to console |
| /log-all | also log clean files |
| /no-log-all | do not log clean files (default) |

| | |
|---|---|
| /aind | show activity indicator |
| /auto | scan and automatically clean all local disks |

**Scanner options**

| | |
|---|---|
| /files | scan files (default) |
| /no-files | do not scan files |
| /memory | scan memory |
| /boots | scan boot sectors |
| /no-boots | do not scan boot sectors (default) |
| /arch | scan archives (default) |
| /no-arch | do not scan archives |
| /max-obj-size=SIZE | only scan files smaller than SIZE megabytes (default 0 = unlimited) |
| /max-arch-level=LEVEL | maximum sub-level of archives within archives (nested archives) to scan |
| /scan-timeout=LIMIT | scan archives for LIMIT seconds at maximum |
| /max-arch-size=SIZE | only scan the files in an archive if they are smaller than SIZE (default 0 = unlimited) |
| /max-sfx-size=SIZE | only scan the files in a self-extracting archive if they are smaller than SIZE megabytes (default 0 = unlimited) |
| /mail | scan email files (default) |
| /no-mail | do not scan email files |
| /mailbox | scan mailboxes (default) |
| /no-mailbox | do not scan mailboxes |
| /sfx | scan self-extracting archives (default) |
| /no-sfx | do not scan self-extracting archives |
| /rtp | scan runtime packers (default) |
| /no-rtp | do not scan runtime packers |
| /unsafe | scan for potentially unsafe applications |
| /no-unsafe | do not scan for potentially unsafe applications (default) |
| /unwanted | scan for potentially unwanted applications |
| /no-unwanted | do not scan for potentially unwanted applications (default) |
| /suspicious | scan for suspicious applications (default) |
| /no-suspicious | do not scan for suspicious applications |
| /pattern | use signatures (default) |
| /no-pattern | do not use signatures |
| /heur | enable heuristics (default) |
| /no-heur | disable heuristics |
| /adv-heur | enable Advanced heuristics (default) |
| /no-adv-heur | disable Advanced heuristics |
| /ext=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<br><br>The following options are available:<br>• none – No automatic cleaning will occur.<br>• standard (default) – ecls.exe will attempt to automatically clean or delete infected files.<br>• strict – ecls.exe will attempt to automatically clean or delete infected files without user intervention (you will not be prompted before files are deleted).<br>• rigorous – ecls.exe will delete files without attempting to clean regardless of what the file is.<br>• 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<br>(supplements the action carried out while cleaning) |
| /no-quarantine | do not copy infected files to Quarantine |

**General options**

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

**Exit codes**

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

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

### 3.10.5 Idle-state detection

Idle state detection settings can be configured in **Advanced setup** under **Antivirus** > **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.

### 3.10.6 ESET SysInspector

#### 3.10.6.1 Introduction to ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays gathered data in a comprehensive way. Information like installed drivers and applications, network connections or important registry entries can help you to investigate suspicious system behavior be it due to software or hardware incompatibility or malware infection.

You can access ESET SysInspector two ways: From the integrated version in ESET Security solutions or by downloading the standalone version (SysInspector.exe) for free from ESET's website. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The standalone and integrated versions each allow you to export system snapshots to an *.xml* file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools** > **ESET SysInspector** (except ESET Remote Administrator). For more information see section ESET SysInspector as part of ESET Endpoint Security.

Please allow some time while ESET SysInspector scans your computer. It may take anywhere from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

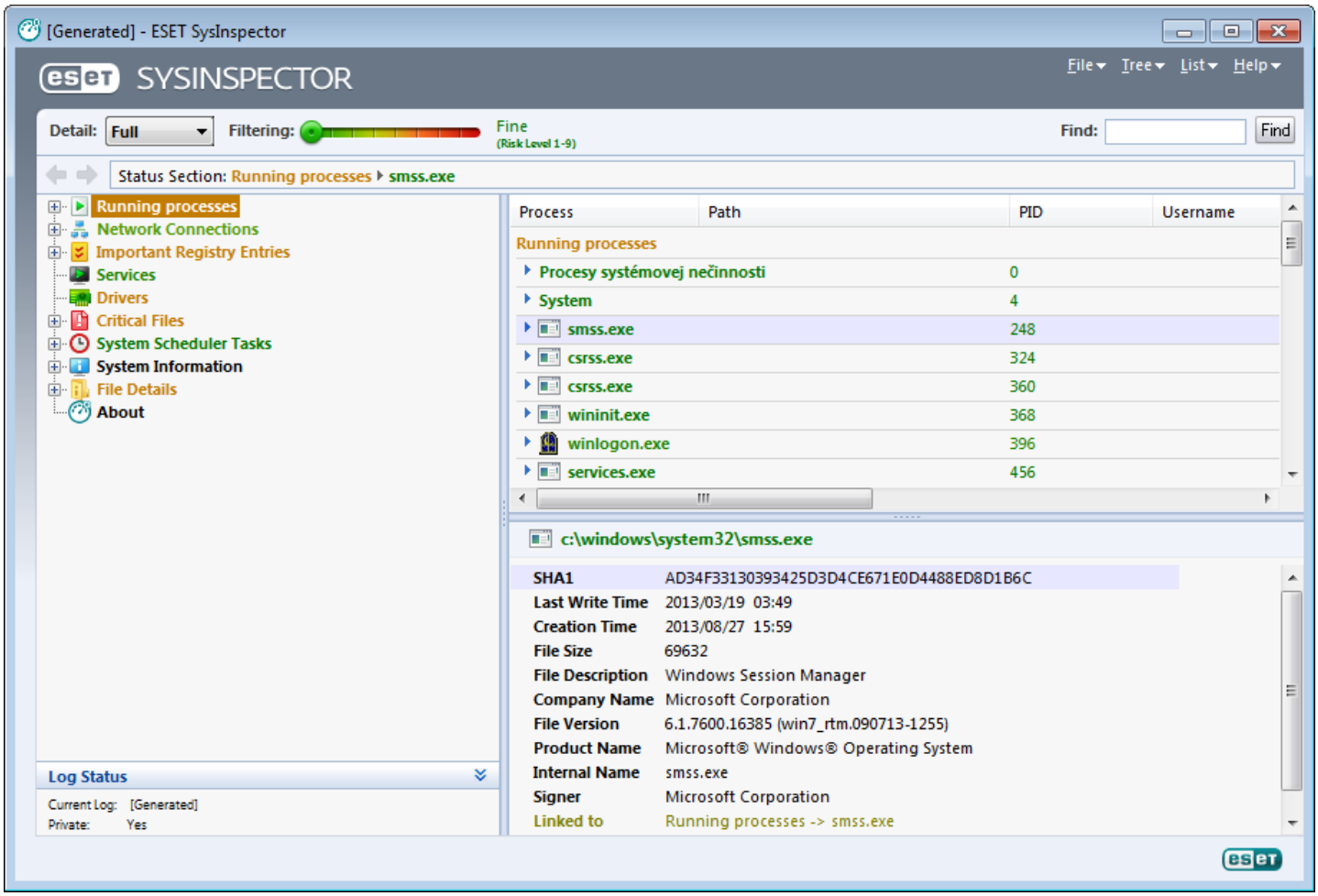
##### 3.10.6.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website. If you already have one of the ESET Security solutions installed, you can run ESET SysInspector directly from the Start Menu (click **Programs** > **ESET** > **ESET Endpoint Security**).

Please wait while the application inspects your system, which could take up to several minutes.

### 3.10.6.2 User Interface and application usage

For clarity the main program window is divided into four major sections – Program Controls located on the top of the main program window, Navigation window to the left, the Description window to the right and the Details window at the bottom of the main program window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).




#### 3.10.6.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

**File**

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

**NOTE:** You may open previously stored ESET SysInspector reports by dragging and dropping them into the main program window. This functionality is not available in Windows Vista operating system for security reasons.

**Tree**

Enables you to expand or close all nodes and export selected sections to Service script.

**List**

Contains functions for easier navigation within the program and various other functions like finding information online.

**Help**

Contains information about the application and its functions.

**Detail**

This setting influences the information displayed in the main program window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

**Filtering**

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current risk level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose a security risk. If you are not using a security solution from ESET, we recommend that you scan your system with ESET Online Scanner if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

**NOTE:** The Risk level of an item can be quickly determined by comparing the color of the item with the color on the **Risk Level** slider.

**Compare**

When comparing two logs, you can choose to display all items, display only added items, display only removed items or to display only replaced items.

**Find**

Search can be used to quickly find a specific item by its name or part of its name. The results of the search request are displayed in the Description window.

**Return**

By clicking the back or forward arrows, you can return to previously displayed information in the Description window. You can use the backspace and space keys instead of clicking back and forward.

**Status section**

Displays the current node in Navigation window.

***Important:*** Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

### 3.10.6.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or click ⊞ or ⊟ next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

**Running processes**

This node contains information about applications and processes running at the time of generating the log. In the

Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

**NOTE:** An operating system is comprised of several important kernel components running constantly that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with \??\. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

**Network connections**

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

**Important Registry Entries**

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

**Services**

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

**Drivers**

A list of drivers installed in the system.

**Critical files**

The Description window displays content of critical files related to the Microsoft windows operating system.

**System Scheduler Tasks**

Contains a list of tasks triggered by Windows Task Scheduler at a specified time/interval.

**System information**

Contains detailed information about hardware and software along with information about set environmental variables, user rights and system event logs.

**File details**

A list of important system files and files in the Program Files folder. Additional information specific for the files can be found in the Description and Details windows.

**About**

Information about version of ESET SysInspector and the list of program modules.

#### 3.10.6.2.2.1 Keyboard shortcuts

Key shortcuts that can be used when working with the ESET SysInspector include:

**File**

| | |
|---|---|
| Ctrl+O | opens existing log |
| Ctrl+S | saves created logs |

**Generate**

| | |
|---|---|
| Ctrl+G | generates a standard computer status snapshot |
| Ctrl+H | generates a computer status snapshot that may also log sensitive information |

**Item Filtering**

| | |
|---|---|
| 1, O | fine, risk level 1-9 items are displayed |
| 2 | fine, risk level 2-9 items are displayed |
| 3 | fine, risk level 3-9 items are displayed |
| 4, U | unknown, risk level 4-9 items are displayed |
| 5 | unknown, risk level 5-9 items are displayed |
| 6 | unknown, risk level 6-9 items are displayed |
| 7, B | risky, risk level 7-9 items are displayed |
| 8 | risky, risk level 8-9 items are displayed |
| 9 | risky, risk level 9 items are displayed |
| - | decreases risk level |
| + | increases risk level |
| Ctrl+9 | filtering mode, equal level or higher |
| Ctrl+0 | filtering mode, equal level only |

**View**

| | |
|---|---|
| Ctrl+5 | view by vendor, all vendors |
| Ctrl+6 | view by vendor, only Microsoft |
| Ctrl+7 | view by vendor, all other vendors |
| Ctrl+3 | displays full detail |
| Ctrl+2 | displays medium detail |
| Ctrl+1 | basic display |
| BackSpace | moves one step back |
| Space | moves one step forward |
| Ctrl+W | expands tree |
| Ctrl+Q | collapses tree |

**Other controls**

| | |
|---|---|
| Ctrl+T | goes to the original location of item after selecting in search results |
| Ctrl+P | displays basic information about an item |
| Ctrl+A | displays full information about an item |
| Ctrl+C | copies the current item's tree |
| Ctrl+X | copies items |
| Ctrl+B | finds information about selected files on the Internet |
| Ctrl+L | opens the folder where the selected file is located |
| Ctrl+R | opens the corresponding entry in the registry editor |
| Ctrl+Z | copies a path to a file (if the item is related to a file) |
| Ctrl+F | switches to the search field |
| Ctrl+D | closes search results |
| Ctrl+E | run service script |

**Comparing**

| | |
|---|---|
| Ctrl+Alt+O | opens original / comparative log |

| | |
|---|---|
| Ctrl+Alt+R | cancels comparison |
| Ctrl+Alt+1 | displays all items |
| Ctrl+Alt+2 | displays only added items, log will show items present in current log |
| Ctrl+Alt+3 | displays only removed items, log will show items present in previous log |
| Ctrl+Alt+4 | displays only replaced items (files inclusive) |
| Ctrl+Alt+5 | displays only differences between logs |
| Ctrl+Alt+C | displays comparison |
| Ctrl+Alt+N | displays current log |
| Ctrl+Alt+P | opens previous log |

**Miscellaneous**

| | |
|---|---|
| F1 | view help |
| Alt+F4 | close program |
| Alt+Shift+F4 | close program without asking |
| Ctrl+I | log statistics |

### 3.10.6.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting malicious code.

After it is launched, the application creates a new log which is displayed in a new window. Click **File** > **Save log** to save a log to a file. Log files can be opened and viewed at a later time. To open an existing log, click **File** > **Open log**. In the main program window, ESET SysInspector always displays one log at a time.

The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, click **File** > **Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

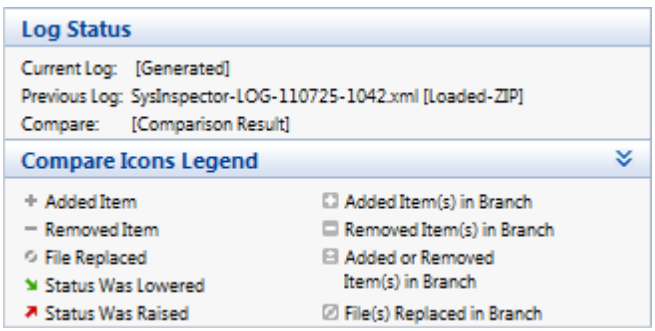
**NOTE:** If you compare two log files, click **File** > **Save log** to save it as a ZIP file; both files will be saved. If you open this file later, the contained logs are automatically compared.

Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Description of all symbols that can be displayed next to items:

- + new value, not present in the previous log
- tree structure section contains new values
- – removed value, present in the previous log
- tree structure section contains removed values
- value / file has been changed
- tree structure section contains modified values / files
- the risk level has decreased / it was higher in the previous log
- the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.




Any comparative log can be saved to a file and opened at a later time.

**Example**

Generate and save a log, recording original information about the system, to a file named previous.xml. After changes to the system have been made, open ESET SysInspector and allow it to generate a new log. Save it to a file named *current.xml*.

In order to track changes between those two logs, click **File** > **Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

*SysIsnpector.exe current.xml previous.xml*

### 3.10.6.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

| | |
|---|---|
| **/gen** | generate log directly from the command line without running GUI |
| **/privacy** | generate log with sensitive information omitted |
| **/zip** | save outcome log in compressed zip archive |
| **/silent** | suppress progress window when generating log from the command line |
| **/blank** | launch ESET SysInspector without generating/loading log |

**Examples**

Usage:
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

To load specific log directly into the browser, use: *SysInspector.exe .\clientlog.xml*
To generate log from the command line, use: *SysInspector.exe /gen=.\mynewlog.xml*
To generate log excluding sensitive information directly in a compressed file, use: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
To compare two log files and browse differences, use: *SysInspector.exe new.xml old.xml*

**NOTE:** If the name of the file/folder contains a gap, then should be taken into inverted commas.

### 3.10.6.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspector by easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

**Example**

If you suspect that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

1. Run ESET SysInspector to generate a new system snapshot.
2. Select the first item in the section on the left (in the tree structure), press Shift and select the last item to mark all items.
3. Right click the selected objects and select **Export Selected Sections To Service Script**.
4. The selected objects will be exported to a new log.
5. This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
6. Open ESET SysInspector, click **File** > **Run Service Script** and enter the path to your script.
7. Click **OK** to run the script.

#### 3.10.6.4.1 Generating Service script

To generate a script, right-click any item from the menu tree (in the left pane) in the ESET SysInspector main window. From the context menu, select either **Export All Sections To Service Script** or **Export Selected Sections To Service Script**.

**NOTE:** It is not possible to export the service script when two logs are being compared.

#### 3.10.6.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

**01) Running processes**

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

**02) Loaded modules**

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khbekhb.dll was marked by a "+". When the script runs, it will recognize the processes using that specific module and end them.

**03) TCP connections**

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

### 04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

### 05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

### 06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

### 07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

The services marked and their dependent services will be stopped and uninstalled when the script is executed.

### 08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

**09) Critical files**

This section contains information about files that are critical to proper function of the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

#### 3.10.6.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script "%Scriptname%"?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

### 3.10.6.5 FAQ

**Does ESET SysInspector require Administrator privileges to run?**

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

**Does ESET SysInspector create a log file?**

ESET SysInspector can create a log file of your computer's configuration. To save one, click **File** > **Save Log** in the main program window. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

**How do I view the ESET SysInspector log file?**

To view a log file created by ESET SysInspector, run the program and click **File** > **Open Log** in the main program window. You can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

**Is a specification available for the log file format? What about an SDK?**

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

**How does ESET SysInspector evaluate the risk posed by a particular object?**

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 - Fine (green) to 9 - Risky (red). In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

**Does a risk level of "6 - Unknown (red)" mean an object is dangerous?**

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

**Why does ESET SysInspector connect to the Internet when run?**

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published by ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

**What is Anti-Stealth technology?**

Anti-Stealth technology provides effective rootkit detection.

If the system is attacked by malicious code that behaves as a rootkit, the user may be exposed to data loss or theft. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

**Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time?**

When trying to identify the digital signature of an executable, ESET SysInspector first checks for a digital signature embedded in the file. If a digital signature is found, the file will be validated using that information. If a digital signature is not found, the ESI starts looking for the corresponding CAT file (Security Catalog - *%systemroot%\system32\catroot*) that contains information about the executable file processed. If the relevant CAT file is found,

the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

#### 3.10.6.6 ESET SysInspector as part of ESET Endpoint Security

To open the ESET SysInspector section in ESET Endpoint Security, click **Tools** > **ESET SysInspector**. The management system in the ESET SysInspector window is similar to that of computer scan logs, or scheduled tasks. All operations with system snapshots – create, view, compare, remove and export – are accessible within one or two clicks.

The ESET SysInspector window contains basic information about the created snapshots such as create time, a short comment, name of the user that created the snapshot and snapshot status.

To compare, create, or delete snapshots, use the corresponding buttons located below the list of snapshots in the ESET SysInspector window. Those options are also available from the context menu. To view the selected system snapshot, select **Show** from the context menu. To export the selected snapshot to a file, right-click it and select **Export...**.

Below is a detailed description of the available options:

- **Compare** – Allows you to compare two existing logs. It is suitable if you want to track changes between the current log and an older log. For this option to take effect, you must select two snapshots to be compared.
- **Create...** – Creates a new record. Before that, you must enter a short comment about the record. To find out the snapshot creation progress (of the currently generated snapshot), see the **Status** column. All completed snapshots are marked by the **Created** status.
- **Delete/Delete all** – Removes entries from the list.
- **Export...** – Saves the selected entry in an XML file (also in a zipped version).

## 3.11 Glossary

### 3.11.1 Types of threats

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

#### 3.11.1.1 Viruses

A computer virus is a piece of malicious code that is pre-pended or appended to existing files on your computer. Viruses are named after biological viruses because they use similar techniques to spread from one computer to another. As for the term "virus", it is often used incorrectly to mean any type of a threat. This usage is gradually being overcome and replaced with a more accurate term "malware" (malicious software).

Computer viruses mainly attack executable files and documents. In short, this is how a computer virus works: after execution of an infected file, the malicious code is called and executed prior to the execution of the original application. A virus can infect any files that the current user has write permissions for.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

If your computer is infected with a virus and cleaning is not possible, submit it to the ESET lab for perusal. In certain cases infected files can be modified to such an extent that cleaning is not possible and the files must be replaced with a clean copy.

#### 3.11.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via network. The basic difference between a virus and a worm is that worms have the ability to propagate by themselves; they are not dependant on host files (or boot sectors). Worms spread to email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes after their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

#### 3.11.1.3 Trojans

Historically, computer Trojans (Trojan horses) have been defined as a class of threats which attempt to present themselves as useful programs and thus trick users into running them.

Since Trojans are a very broad category, it is often divided into several subcategories:

- **Downloader** – Malicious programs with the ability to download other threats from the Internet.
- **Dropper** – Malicious programs with the ability to drop other types of malware onto compromised computers.
- **Backdoor** – Malicious programs which communicate with remote attackers, allowing them to gain access to the computer and take control over it.
- **Keylogger** – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers.
- **Dialer** – Malicious programs designed to connect via premium-rate numbers instead of the user's Internet service provider. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.

If a file on your computer is detected as a Trojan, it is advisable to delete it, since it most likely contains nothing but malicious code.

#### 3.11.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1. When they try to access a system: They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
2. When they are hidden from the usual testing: ESET Endpoint Security users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

#### 3.11.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry.If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

#### 3.11.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

#### 3.11.1.7 Packers

Packer is a runtime self-extracting executable that rolls up several kinds of malware into a single package.

The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

#### 3.11.1.8 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET Endpoint Security provides the option to detect such threats.

**Potentially unsafe applications** is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

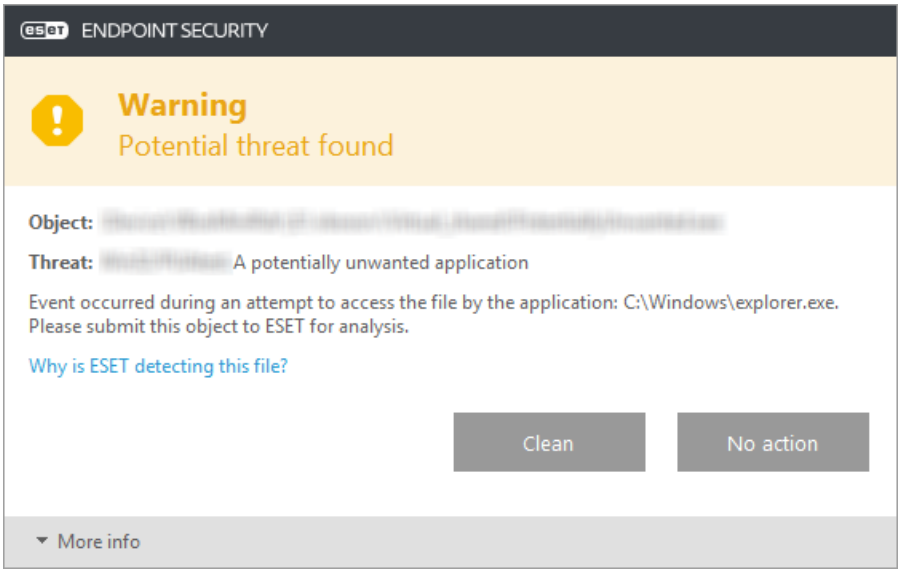
### 3.11.1.9 Potentially unwanted applications

A potentially unwanted application is a program that contains adware, installs toolbars or has other unclear objectives. There are some situations where a user may feel that the benefits of a potentially unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software, such as trojan horses or worms.

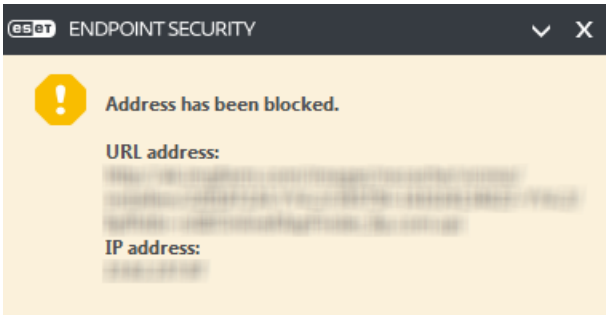
**Warning - Potential threat found**

When a potentially unwanted application is detected, you will be able to decide which action to take:

1. **Clean/Disconnect**: This option ends the action and prevents the potential threat from entering your system.
2. **No action**: This option allows a potential threat to enter your system.
3. To allow the application to run on your computer in the future without interruption, click **More info/Show advanced options** and then select the check box next to **Exclude from detection**.

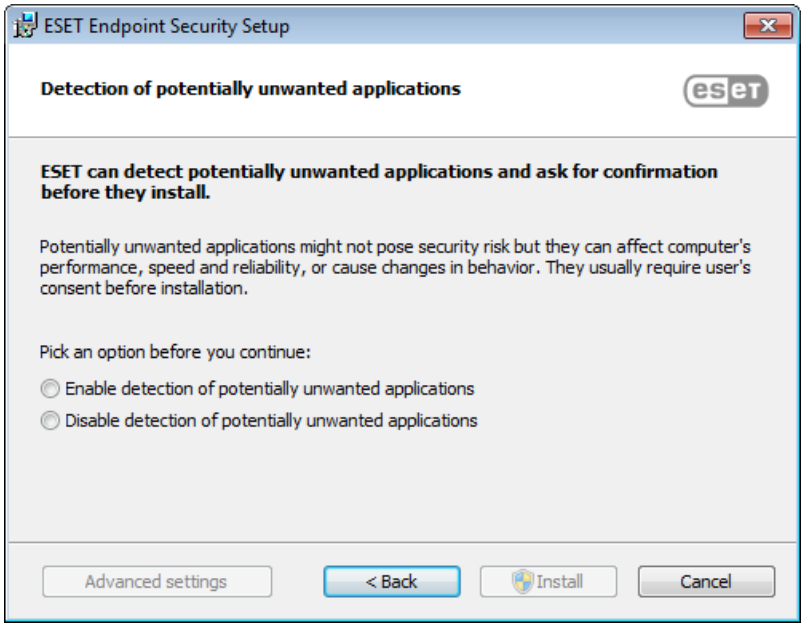



When a potentially unwanted application is detected and it is unable to clean, a notification window **Address has been blocked** will show at the bottom right corner of the screen. For more information about this event navigate to **Tools** > **Log files** > **Filtered websites** from the main menu.



### Potentially unwanted applications - Settings

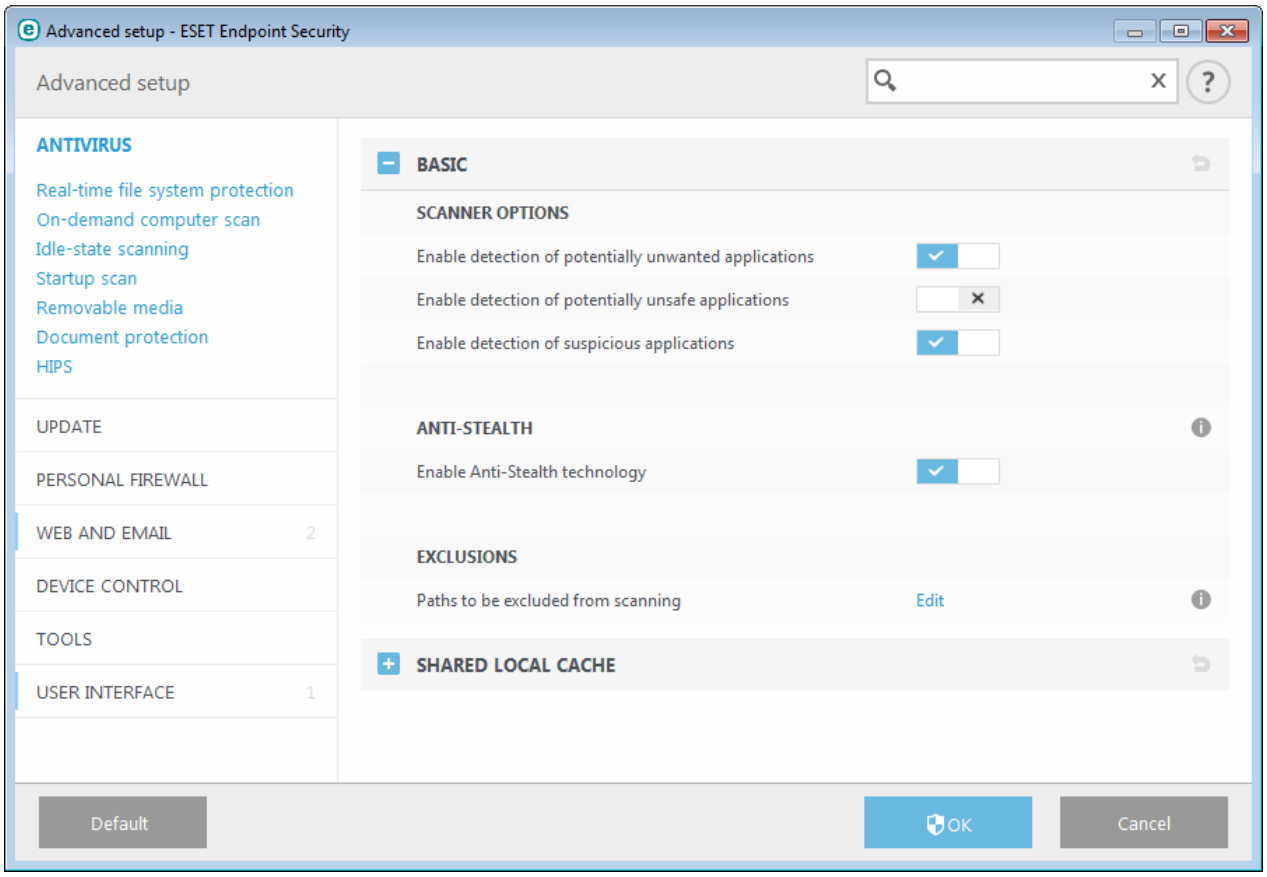
While installing your ESET product, you can decide whether to enable detection of potentially unwanted applications, as shown below:




Potentially unwanted applications may install adware, toolbars, or contain other unwanted and unsafe program features.

These settings can be modified in your program settings at any time. To enable or disable the detection of Potentially unwanted, unsafe or suspicious applications, follow these instructions:

1. Open your ESET product. How do I open my ESET product?
2. Press the **F5** key to access **Advanced setup**.
3. Click **Antivirus** and enable or disable options **Enable detection of potentially unwanted applications**, **Enable detection of potentially unsafe applications** and **Enable detection of suspicious applications** according to your preferences. Confirm by clicking **OK**.




**Potentially unwanted applications - Software wrappers**

A software wrapper is a special type of application modification that is used by some file-hosting websites. It is a third-party tool that installs the program you intended to download but adds additional software, such as toolbars or adware. The additional software may also make changes to your web browser's home page and search settings. Also, file-hosting websites often do not notify the software vendor or download recipient that modifications have been made and do not easily allow opting out of modification. For these reasons, ESET classifies software wrappers as a type of potentially unwanted application to allow users to accept the download or not.

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

### 3.11.1.10 Botnet

A bot or web robot is an automated malware program that scans blocks of network addresses and infects vulnerable computers. This type of program allows hackers to take control of many computers at the same time and turn them into bots (also known as a zombies). Hackers typically use bots to infect large numbers of computers. This large group of infected computers is referred to as a botnet. If your computer is infected and becomes a member of a botnet, it can be used in distributed denial of service (DDoS) attacks, and can also can be used to perform automated tasks over the Internet unbeknownst to you (for example sending spam, viruses or stealing personal and private information such as bank credentials or credit card numbers).

## 3.11.2 Types of remote attacks

There are many special techniques which allow attackers to compromise remote systems. These are divided into several categories.

#### 3.11.2.1 Worm attacks

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. Network worms exploit security vulnerabilities in various applications. Due to the availability of the Internet, they can spread all over the world within a few hours of their release.

Most worm attacks can be avoided by using default security settings in the firewall. Also, it is important to choose **Public network** protection type in public networks and to keep your operating system and programs up to date with the most recent security patches.

#### 3.11.2.2 DoS attacks

DoS, or *Denial of Service*, is an attempt to make a computer or network unavailable for its intended users. The communication between afflicted users is obstructed and can no longer continue in a functional way. Computers exposed to DoS attacks usually need to be restarted in order to work properly.

In most cases, the targets are web servers and the aim is to make them unavailable to users for a certain period of time.

#### 3.11.2.3 Port scanning

Port scanning is used to determine which computer ports are open on a network host. A port scanner is software designed to find such ports.

A computer port is a virtual point which handles incoming and outgoing data – this is crucial from a security point of view. In a large network, the information gathered by port scanners may help to identify potential vulnerabilities. Such use is legitimate.

Still, port scanning is often used by hackers attempting to compromise security. Their first step is to send packets to each port. Depending on the response type, it is possible to determine which ports are in use. The scanning itself causes no damage, but be aware that this activity can reveal potential vulnerabilities and allow attackers to take control of remote computers.

Network administrators are advised to block all unused ports and protect those that are in use from unauthorized access.

#### 3.11.2.4 DNS Poisoning

Using DNS (Domain Name Server) poisoning, hackers can trick the DNS server of any computer into believing that the fake data they supplied is legitimate and authentic. The fake information is cached for a certain period of time, allowing attackers to rewrite DNS replies of IP addresses. As a result, users trying to access Internet websites will download computer viruses or worms instead of their original content.

### 3.11.3 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct, and played a crucial role in the proliferation of the Internet in the early 1990's.

Unfortunately, with a high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and proliferation of malicious software – malware. The inconvenience and danger to you is increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database. Some hints for prevention:

- If possible, don't publish your email address on the Internet
- Only give your email address to trusted individuals
- If possible, don't use common aliases – with more complicated aliases, the probability of tracking is lower
- Don't reply to spam that has already arrived in your inbox
- Be careful when filling out Internet forms – be especially cautious of options such as "Yes, I want to receive information".
- Use "specialized" email addresses – for example, one for business, one for communication with your friends, etc.
- From time to time, change your email address
- Use an Antispam solution

#### 3.11.3.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what's more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

#### 3.11.3.2 Hoaxes

A hoax is misinformation which is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

#### 3.11.3.3 Phishing

The term phishing defines a criminal activity which uses techniques of social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email masquerading as a trustworthy person or business (for example, financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

#### 3.11.3.4 Recognizing spam scams

Generally, there are a few indicators which can help you identify spam (unsolicited emails) in your mailbox. If a message fulfills at least some of the following criteria, it is most likely a spam message.

- Sender address does not belong to someone on your contact list.
- You are offered a large sum of money, but you have to provide a small sum first.
- You are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data – bank account numbers, usernames and passwords, etc.
- It is written in a foreign language.
- You are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable vendor (consult the original product manufacturer).
- Some of the words are misspelled in an attempt to trick your spam filter. For example “vaigra” instead of “viagra”, etc.

##### 3.11.3.4.1 Rules

In the context of Antispam solutions and email clients, rules are tools for manipulating email functions. They consist of two logical parts:

1. Condition (for example, an incoming message from a certain address)
2. Action (e.g., deletion of the message, moving it to a specified folder)

The number and combination of rules varies with the Antispam solution. These rules serve as measures against spam (unsolicited email). Typical examples:

- 1. Condition: An incoming email message contains some of the words typically seen in spam messages
  2. Action: Delete the message
- 1. Condition: An incoming email message contains an attachment with an .exe extension
  2. Action: Delete the attachment and deliver the message to the mailbox
- 1. Condition: An incoming email message arrives from your employer
  2. Action: Move the message to the “Work” folder

We recommend that you use a combination of rules in Antispam programs in order to facilitate administration and to more effectively filter spam.

#### 3.11.3.4.2 Whitelist

In general, a whitelist is a list of items or persons who are accepted, or have been granted permission. The term "email whitelist" defines a list of contacts from whom the user wishes to receive messages. Such whitelists are based on keywords searched for in email addresses, domain names, or IP addresses.

If a whitelist works in "exclusivity mode", then messages from any other address, domain, or IP address will not be received. If a whitelist is not exclusive, such messages will not be deleted, but filtered in some other way.

A whitelist is based on the opposite principle to that of a blacklist. Whitelists are relatively easy to maintain, more so than blacklists. We recommend that you use both the Whitelist and Blacklist to filter spam more effectively.

#### 3.11.3.4.3 Blacklist

Generally, a blacklist is a list of unaccepted or forbidden items or persons. In the virtual world, it is a technique enabling acceptance of messages from all users not present on such a list.

There are two types of blacklist: Those created by users within their Antispam application, and professional, regularly updated blacklists which are created by specialized institutions and can be found on the Internet.

It is essential to use blacklists to successfully block spam, but they are difficult to maintain, since new items to be blocked appear every day. We recommended you use both a whitelist and a blacklist to most effectively filter spam.

#### 3.11.3.4.4 Exception list

The Exception list usually contains email addresses that may be spoofed and used for sending spam. Email messages received from addresses listed in the Exception list will always be scanned for spam. By default, the Exception list contains all email addresses from existing email client accounts.

#### 3.11.3.4.5 Server-side control

Server-side control is a technique for identifying mass spam based on the number of received messages and the reactions of users. Each message leaves a unique digital "footprint" based on the content of the message. The unique ID number tells nothing about the content of the email. Two identical messages will have identical footprints, while different messages will have different footprints.

If a message is marked as spam, its footprint is sent to the server. If the server receives more identical footprints (corresponding to a certain spam message), the footprint is stored in the spam footprints database. When scanning incoming messages, the program sends the footprints of the messages to the server. The server returns information on which footprints correspond to messages already marked by users as spam.

### 3.11.4 ESET Technology

#### 3.11.4.1 Exploit Blocker

Exploit Blocker is designed to fortify commonly exploited applications such as web browsers, PDF readers, email clients or MS Office components. It monitors behavior of processes for suspicious activity that might indicate an exploit. It adds another layer of protection, one step closer to attackers, by using a completely different technology compared to techniques focusing on detection of malicious files themselves.

When Exploit Blocker identifies a suspicious process, it can stop the process immediately and record data about the threat, which is then sent to the ESET LiveGrid® cloud system. This data is processed by the ESET Threat Lab and used to better protect all users from unknown threats and zero-day attacks (newly released malware for which there is no pre-configured remedy).

#### 3.11.4.2 Advanced Memory Scanner

Advanced Memory Scanner works in combination with Exploit Blocker to provide better protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation and/or encryption. In cases where ordinary emulation or heuristics might not detect a threat, the Advanced memory Scanner is able to identify suspicious behavior and scan threats when they reveal themselves in system memory. This solution is effective against even heavily obfuscated malware. Unlike Exploit Blocker, this is a post-execution method, which means that there is a risk that some malicious activity could have been performed prior to its detecting a threat. However in the case that other detection techniques have failed, it offers an additional layer of security.

#### 3.11.4.3 ESET LiveGrid®

Built on ThreatSense.Net® advanced early warning system, ESET LiveGrid® utilizes data that ESET users have submitted worldwide and sends it to the ESET Virus Lab. By providing suspicious samples and metadata from the wild, ESET LiveGrid® enables us to react immediately to the needs of our customers and keep ESET responsive to the latest threats. ESET malware researchers use the information to build an accurate snapshot of the nature and scope of global threats, which helps us focus on the right targets. ESET LiveGrid® data plays an important role in setting priorities in our automated processing.

Additionally, it implements a reputation system that helps to improve the overall efficiency of our anti-malware solutions. When an executable file or archive is being inspected on a user's system, its hash tag is first compared against a database of white- and blacklisted items. If it is found on the whitelist, the inspected file is considered clean and also flagged to be excluded from future scans. If it is on the blacklist, appropriate actions are taken based on the nature of the threat. If no match is found, the file is scanned thoroughly. Based on the results of this scan, files are categorized as threats or non-threats. This approach has a significant positive impact on scanning performance.

This reputation system allows for effective detection of malware samples even before their signatures are distributed to users via virus signature database updates several times a day.

#### 3.11.4.4 Botnet protection

Botnet protection discovers malware by analyzing its network communication protocols. Botnet malware changes frequently in contrast to network protocols, which have not changed in recent years. This new technology helps ESET defeat malware that tries to connect your computer to botnet networks.

#### 3.11.4.5 Java Exploit Blocker

Java Exploit Blocker is an extension to existing ESET Exploit Blocker protection. It monitors Java for exploit-like behavior. Blocked samples can be reported to malware analysts so they can create signatures to block attempted Java exploits on different layers (URL blocking, file downloads, etc.).