ESET NOD32 Antivirus 4

User Guide

(intended for product version 4.2 and higher)

Microsoft® Windows® 7 / Vista / XP / NT4 / 2000 / 2003 / 2008

ESET®

ESET NOD32 Antivirus 4

Customer Care Worldwide: www.eset.eu/support
Customer Care North America: www.eset.com/support

REV.20100225-008

Content

1. ESET NOD32 Antivirus 4

ESET NOD32 Antivirus 4 is the successor to the award-winning product ESET NOD32 Antivirus 3.0. It utilizes the scanning speed and the precision of ESET NOD32 Antivirus, granted by the most recent version of the ThreatSense® scanning engine.

The implemented advanced techniques are capable of proactively blocking viruses, spyware, trojans, worms, adware and rootkits without slowing down the system or disrupting you as you work or play with your computer.

1.1 What's new

The long-time development experience of our experts is demonstrated by the entirely new architecture of the ESET NOD32 Antivirus program, which guarantees maximum detection with minimum system requirements.

- **Antivirus & antispyware**

This module is built upon the ThreatSense® scanning engine, which was used for the first time in the award-winning NOD32 Antivirus system. ThreatSense® is optimized and improved with the new ESET NOD32 Antivirus architecture.

Feature	Description
Improved Cleaning	The antivirus system now intelligently cleans and deletes most detected infiltrations without requiring user intervention.
Background Scanning Mode	Computer scanning can be launched in the background without slowing down performance.
Smaller Update Files	Core optimization processes keep the size of update files smaller than in version 2.7. Also, protection of update files against damage has been improved.
Popular EMail Client Protection	It is now possible to scan incoming mail not only in Microsoft Outlook but also in Outlook Express, Windows Mail, Windows Live Mail and Mozilla Thunderbird.
Variety of Other Minor Improvements	– Direct access to file systems for high speed and throughput. – Blocking access to infected files – Optimization for Windows Security Center, including Vista.

- **Others**

Feature	Description
ESET SysRescue	ESET SysRescue enables user to create a bootable CD/DVD/USB containing ESET Smart Security, which is capable of running independent of the operating system. It is best used to get the system rid of hard-to-remove infiltrations.
ESET SysInspector	ESET SysInspector, an application that thoroughly inspects your computer, is now integrated directly in ESET Smart Security. If you contact our Customer Care Service using the Help and support > Customer Care support request (recommended) option, you can opt to include an ESET SysInspector status snapshot from your computer.
Document protection	The Document protection serves to scan Microsoft Office documents before they are opened and files downloaded automatically by Internet Explorer, such as Microsoft ActiveX elements.
Self Defense	The new Self Defense technology protects ESET Smart Security components against deactivation attempts.
User interface	The user interface is now capable of working in the non-graphical mode, which allows for keyboard control of ESET Smart Security. The increased compatibility with screen-reading application lets sight-impaired people control the program more efficiently.

1.2 System requirements

For seamless operation of ESET NOD32 Antivirus, your system should meet the following hardware and software requirements:

ESET NOD32 Antivirus:

Windows NT4 SP6, 2000, XP	400 MHz 32-bit / 64-bit (x86 / x64) 128 MB RAM of system memory 130 MB available space Super VGA (800 × 600)
Windows 7, Vista	1 GHz 32-bit / 64-bit (x86 / x64) 512 MB RAM of system memory 130 MB available space Super VGA (800 × 600)

ESET NOD32 Antivirus Business Edition:

Windows NT4 SP6, 2000, 2000 Server, XP, 2003 Server	400 MHz 32-bit / 64-bit (x86 / x64) 128 MB RAM of system memory 130 MB available space Super VGA (800 × 600)
Windows 7, Vista, Windows Server 2008	1 GHz 32-bit / 64-bit (x86 / x64) 512 MB RAM of system memory 130 MB available space Super VGA (800 × 600)

NOTE: Anti-Stealth and Self Defense are not available on Windows NT4 SP6.

2. Installation

After purchase, the ESET NOD32 Antivirus installer can be downloaded from ESET's website as an .msi package. Launch the installer and the installation wizard will guide you through the basic setup. There are two types of installation available with different levels of setup details:

1. Typical installation

2. Custom installation
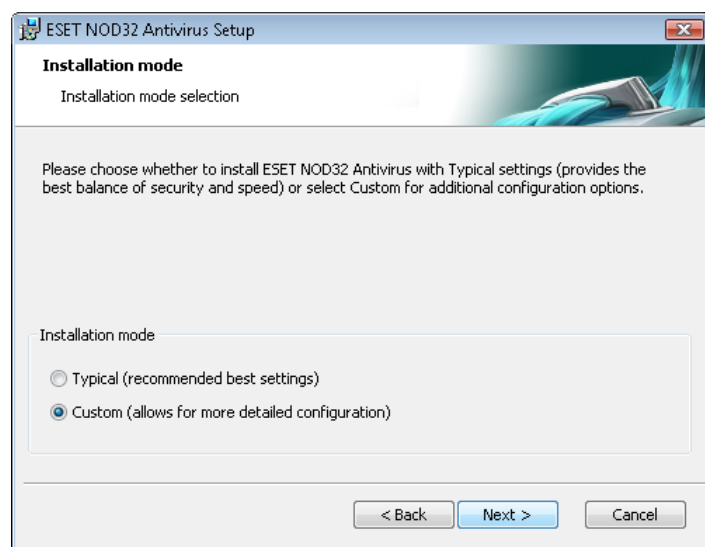
2.1 Typical installation

Typical installation provides configuration options appropriate for most users. The settings provide excellent security coupled with ease of use and high system performance. Typical installation is the default option and is recommended if you do not have particular requirements for specific settings.

After selecting the installation mode and clicking **Next**, you will be prompted to enter your username and password for automatic updates of the program. This plays a significant role in providing constant protection of your system.
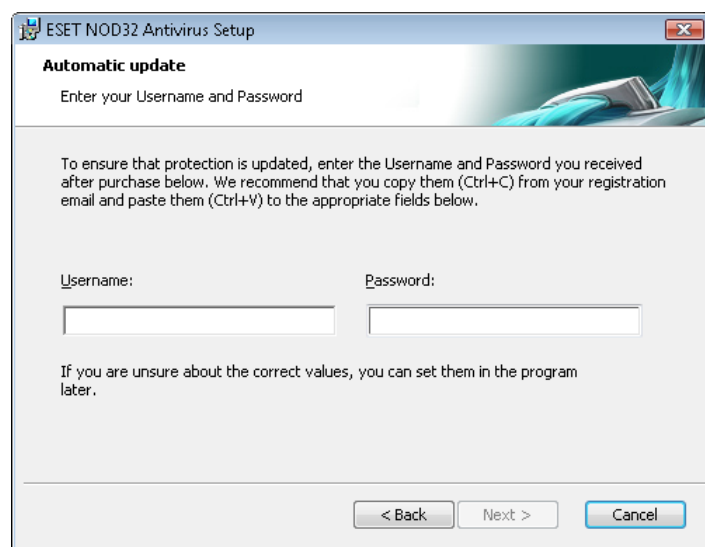
Enter your **Username** and **Password**, i.e., the authentication data you received after the purchase or registration of the product, into the corresponding fields. If you do not currently have your username and password available, authentication data can be inserted at any time later on, directly from the program.

The next step is configuration of the ThreatSense.Net Early Warning System. The ThreatSense.Net Early Warning System helps ensure that ESET is immediately and continuously informed about new

infiltrations in order to quickly protect its customers. The system allows for submission of new threats to ESET's Threat Lab, where they are analyzed, processed and added to the virus signature database.
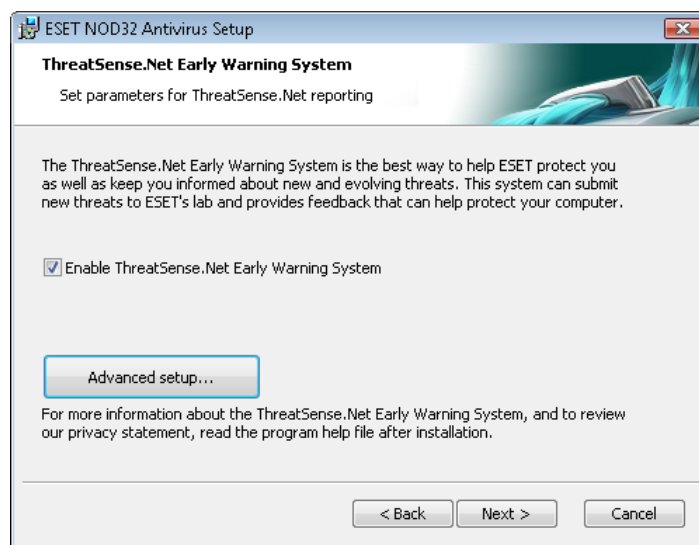
By default, the **Enable ThreatSense.Net Early Warning System** option is selected, which will activate this feature. Click **Advanced setup…** to modify detailed settings for the submission of suspicious files.

The next step in the installation process is to configure **Detection of potentially unwanted applications**. Potentially unwanted applications are not necessarily malicious, but can often negatively affect the behavior of your operating system.

These applications are often bundled with other programs and may be difficult to notice during the installation process. Although these applications usually display a notification during installation, they can easily be installed without your consent.
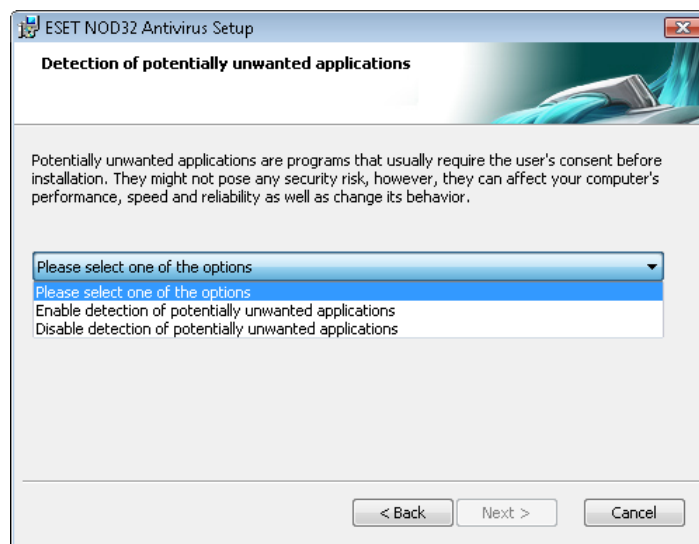
The final step in Typical installation mode is to confirm installation by clicking the Install button.
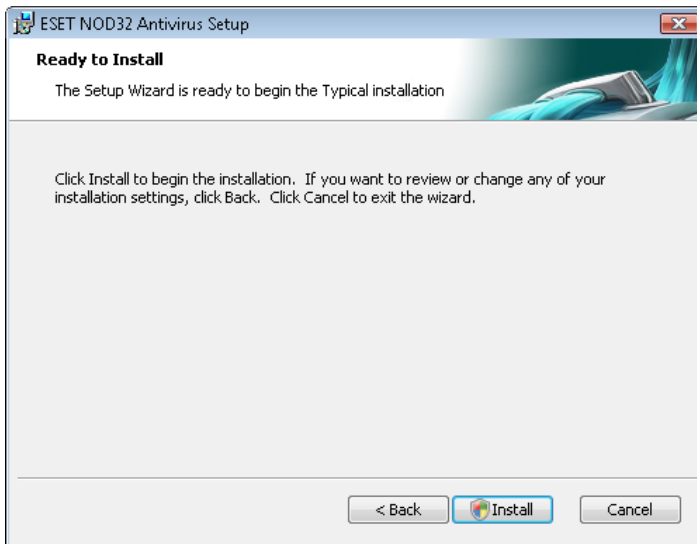
2.2 Custom installation

Custom installation is designed for users who have experience with fine-tuning programs and who wish to modify advanced settings during installation.

After selecting the installation mode and clicking **Next**, you will be prompted to select a destination location for the installation. By default, the program installs in C:\Program Files\ESET\ESET NOD32 Antivirus\. Click **Browse...** to change this location (not recommended).
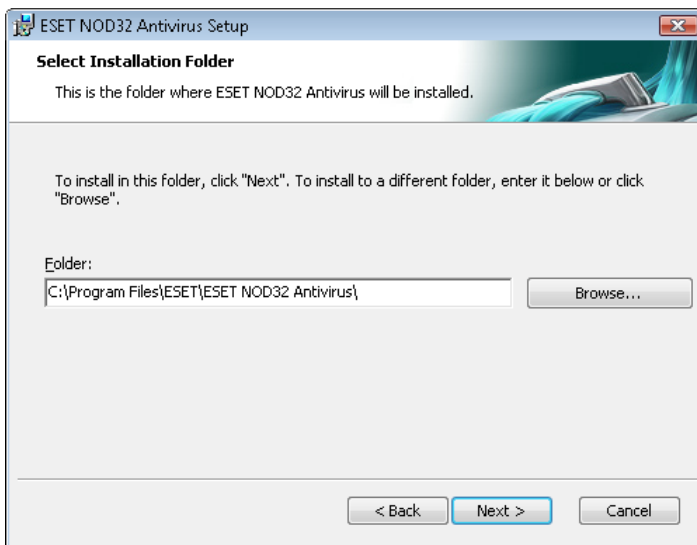
Next, Enter your **Username** and **Password**. This step is the same as in Typical installation (see section 2.1, "Typical installation").

After entering your username and password, click **Next** to proceed to **Configure your Internet connection**.
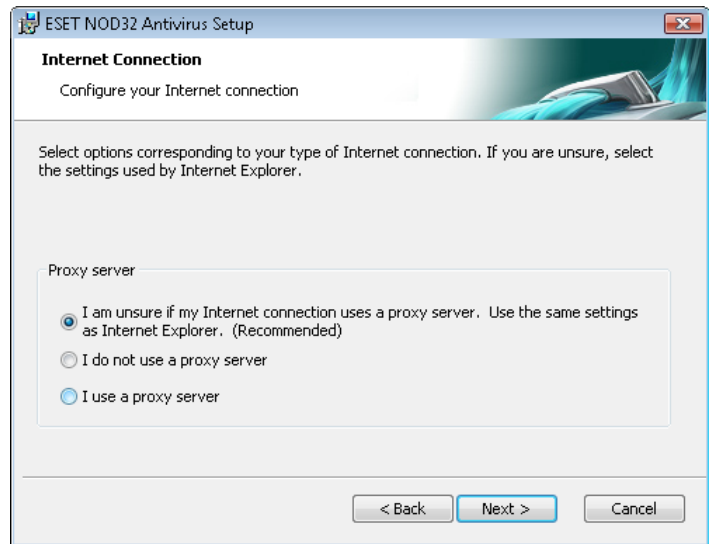
If you use a proxy server, it must be correctly configured for virus signature updates to work correctly. If you do not know whether you use a proxy server to connect to the Internet, leave the default setting **I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer (Recommended)** and click **Next**. If you do not use a proxy server, select the **I do not use a proxy server** option.
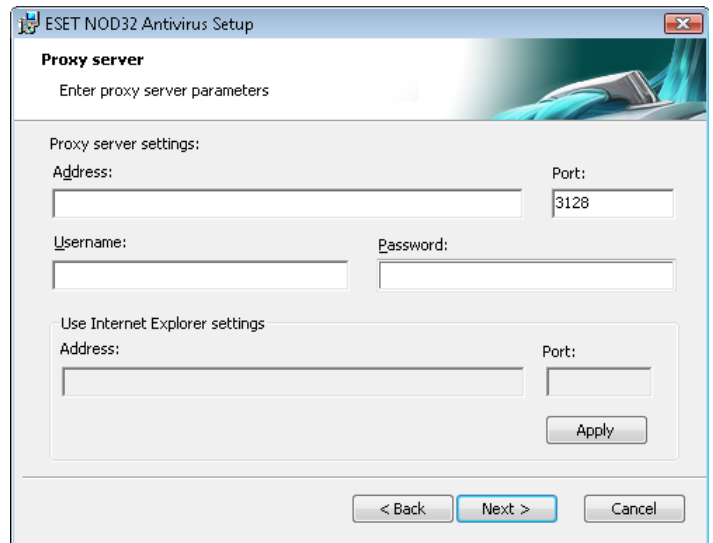
To configure your proxy server settings, select **I use a proxy server** and click **Next**. Enter the IP address or URL of your proxy server in the **Address** field**.** In the **Port** field, specify the port where the proxy server accepts connections (3128 by default). In the event that the proxy server requires authentication, enter a valid **Username** and **Password** to grant access to the proxy server. Proxy server settings can also be copied from Internet Explorer if desired. To do this, click **Apply** and confirm the selection.
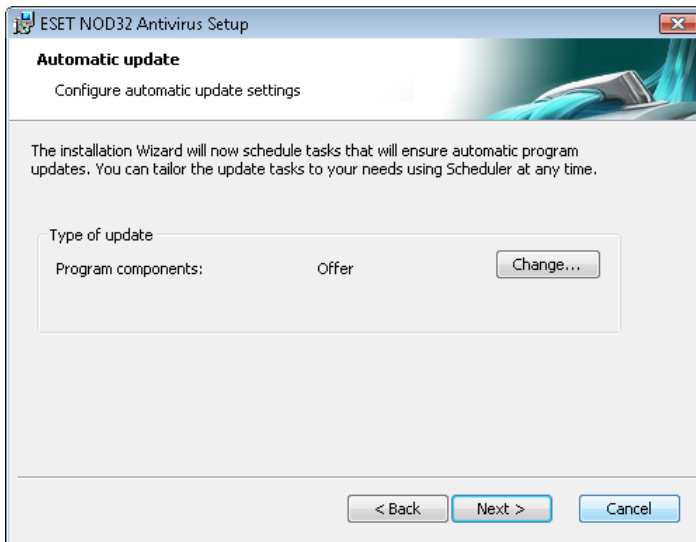
Click **Next** to proceed to **Configure automatic update settings**. This step allows you to designate how automatic program component updates will be handled on your system. Click **Change…** to access the advanced settings.

If you do not want program components to be updated, select the **Never update program components** option. Select the **Ask before downloading program components** option to display a confirmation window before downloading program components. To download program component upgrades automatically, select the **Always update program components** option.
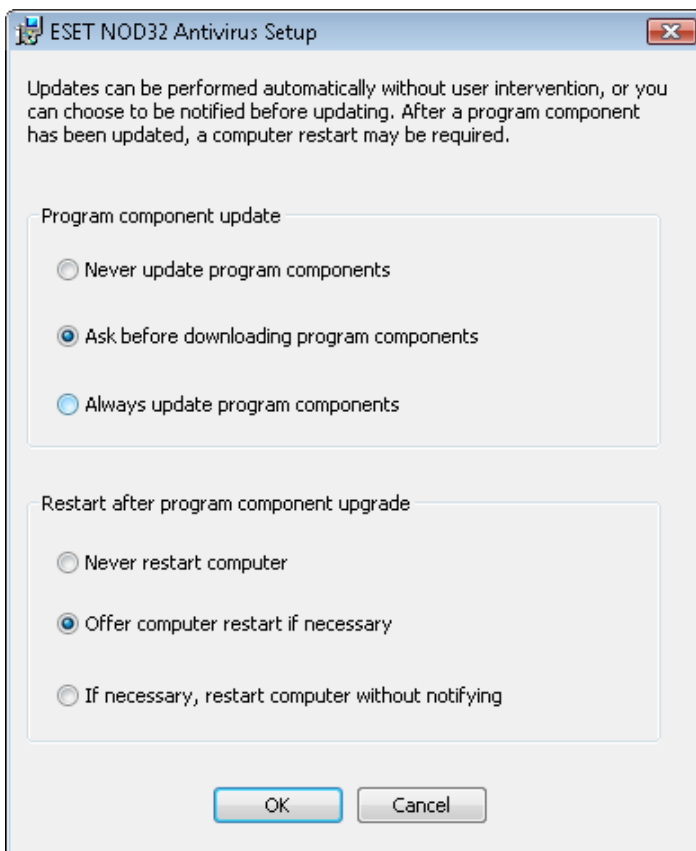
NOTE: After a program component update, a restart is usually required. We recommend selecting the **If necessary, restart computer without notifying** option.

The next installation window is the option to set a password to protect your program settings. Select the **Protect configuration settings with a password** option and choose a password to enter in

the **New password** and **Confirm new password** fields.

The next two installation steps, **ThreatSense.Net Early Warning System** and **Detection of potentially unwanted applications** are the same as in Typical installation (see section 2.1, "Typical installation").

Click **Install** in the **Ready to install window** to complete installation.

2.3   Using original settings

If you reinstall ESET NOD32 Antivirus, the **Use current settings** option will display. Select this option to transfer setup parameters from the original installation to the new one.
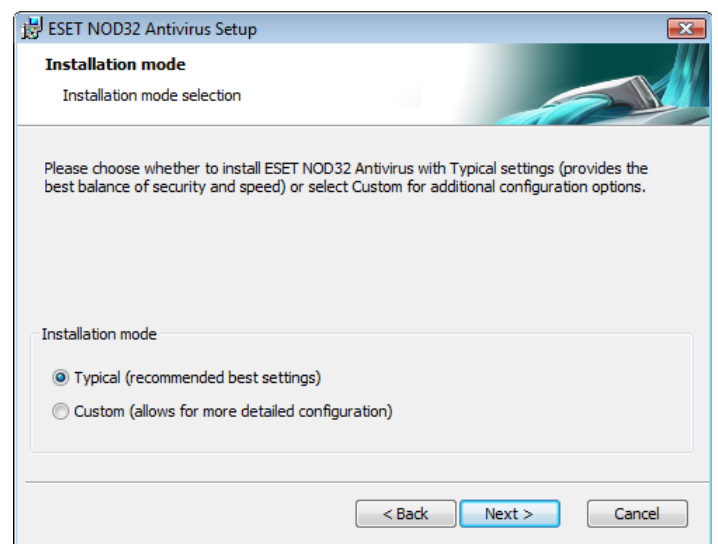
2.4   Entering Username and password

For optimal functionality, it is important that the program is automatically updated. This is only possible if the correct username and password are entered in the Update setup.

If you did not enter your username and password during installation, you can now. In the main program window, click **Update** and then click **Username and Password setup…**. Enter the license data you received with your ESET security product into the **License details** window.
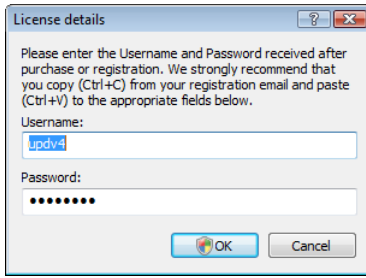
2.5 On-demand computer scan

After installing ESET NOD32 Antivirus, a computer scan for malicious code should be performed. From the main program window, click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see section 4.1.4, "On-demand computer scan".
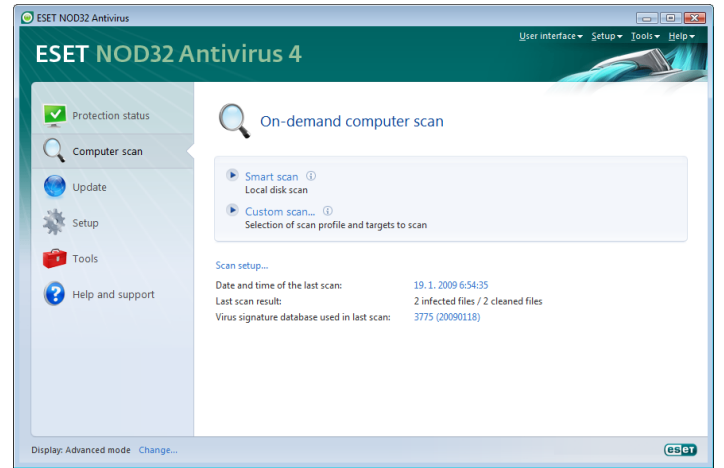
3. Beginner's guide

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

3.1   Introducing user interface design – modes

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

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

Protection status – Provides information about the protection status of ESET NOD32 Antivirus. If Advanced mode is activated, the Watch activity and Statistics submenus will display.

Computer scan – This option allows you to configure and launch the On-demand computer scan.

Update – Displays information about updates to the virus signature database.

Setup – Select this option to adjust your computer's security level. If Advanced mode is activated, the Antivirus and antispyware submenu will display.

Tools – Provides access to Log files, Quarantine, Scheduler and SysInspector. This option only displays in Advanced mode.

Help and support – Provides access to help files, the ESET Knowledgebase, ESET's website and links to open a Customer Care support request.

The ESET NOD32 Antivirus user interface allows users to toggle between Standard and Advanced mode. Standard mode provides access to features required for common operations. It does not display any advanced options. To toggle between modes, click **Change…** in the bottom left corner of the main program window, or press CTRL + M on your keyboard.

The Standard mode provides access to features required for common operations. It does not display any advanced options.
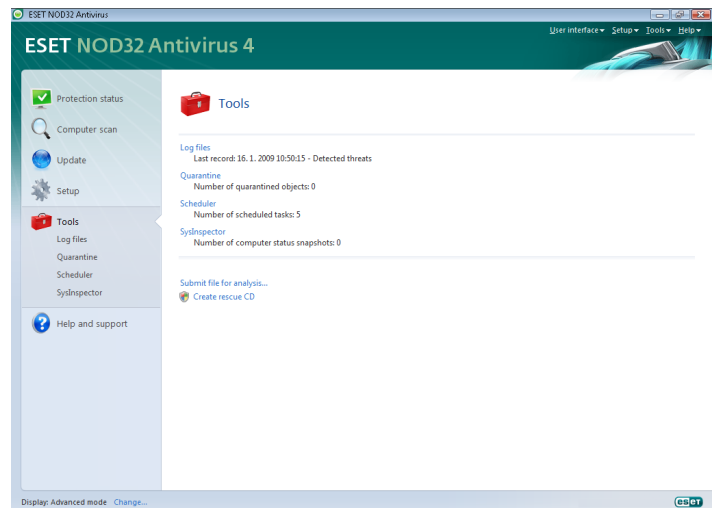
Toggling to Advanced mode adds the **Tools** option to the main menu. The Tools option allows you to access the submenus for Log files, Quarantine, Scheduler and SysInspector.

NOTE: All remaining instructions in this guide take place in Advanced mode.

3.1.1   Checking operation of the system

To view the **Protection status**, click the top option from the main menu. A status summary about the operation of ESET NOD32 Antivirus will display in the primary window, and a submenu with two items will appear: **Watch Activity** and **Statistics**. Select either of these to view more detailed information about your system.
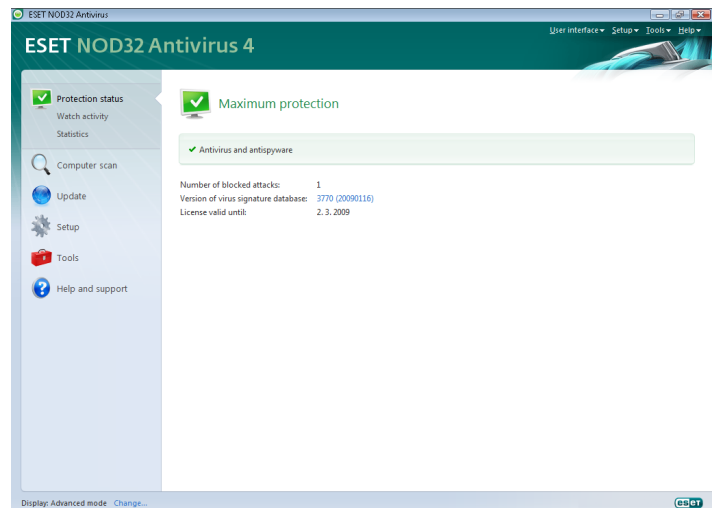
3.1.2   What to do if the program doesn't work properly

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, and 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 modules, click **Setup** in the main menu and click on the desired module.
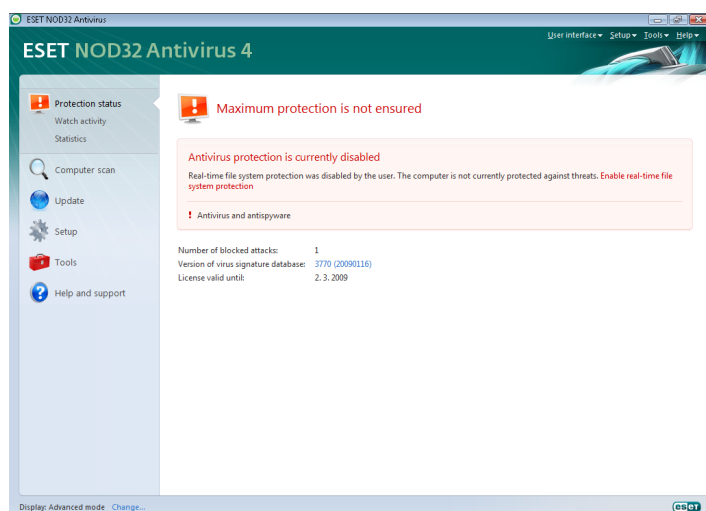
If you are unable to solve a problem using the suggested solutions, click **Help and support** to access the help files or search the Knowledgebase. If you still need assistance, you can submit an ESET Customer Care support request. ESET Customer Care will respond quickly to your questions and help determine a resolution.

3.2 Update setup

Updating the virus signature database and updating program components are an important part of providing complete protection against malicious code. Please pay attention to their configuration and operation. From the main menu, select **Update** and then click **Update virus signature database** in the primary window to check for a newer database update. **Username and Password setup…** displays a dialog box where the username and password received at the time of purchase should be entered.

If the username and password were entered during installation of ESET NOD32 Antivirus you will not be prompted for them at this point.
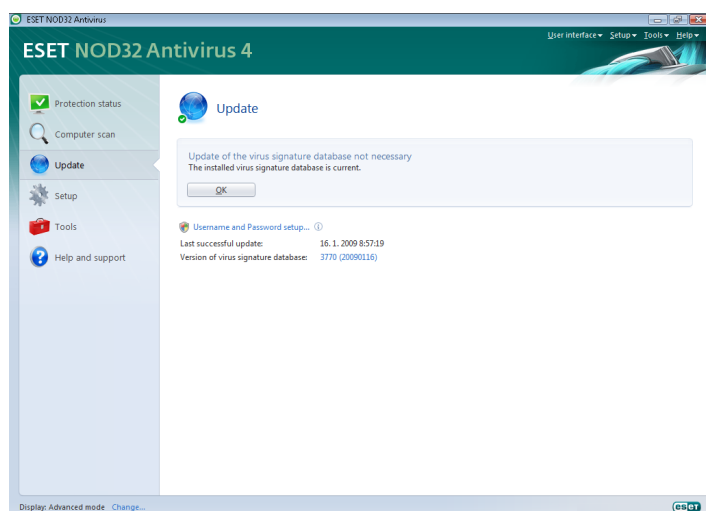
The Advanced Setup window (click **Setup** from the main menu and then click **Enter entire advanced setup tree…**, or press F5 on your keyboard) contains additional update options. Click **Update** from the Advanced Setup tree . The **Update server:** drop-down menu should be set to **Choose automatically**. To configure advanced update options such as the update mode, proxy server access, LAN connections and creating virus signature copies (ESET NOD32 Antivirus Business Edition), click the **Setup…** button.
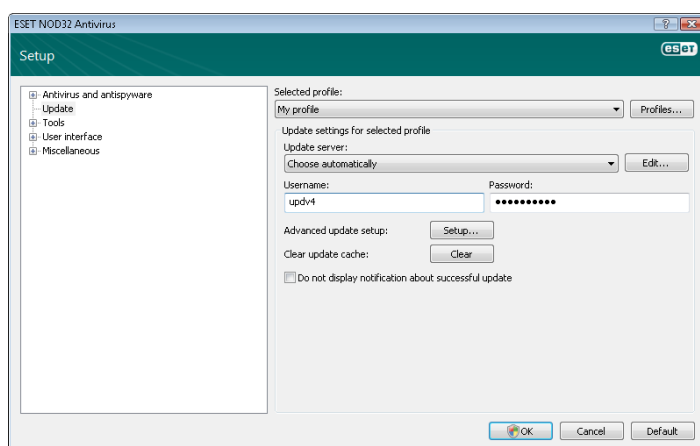
3.3 Proxy server setup

If you use a proxy server to control Internet connections on a system using ESET NOD32 Antivirus, it must be specified in Advanced Setup. To access the Proxy server configuration window, press F5 to open the Advanced Setup window and click **Miscellaneous > Proxy server** from the Advanced Setup tree. Select the **Use proxy server** option, and then fill in the **Proxy server** (IP address) and **Port** fields. If needed, select the **Proxy server requires authentication** option and then enter the **Username** and **Password**.
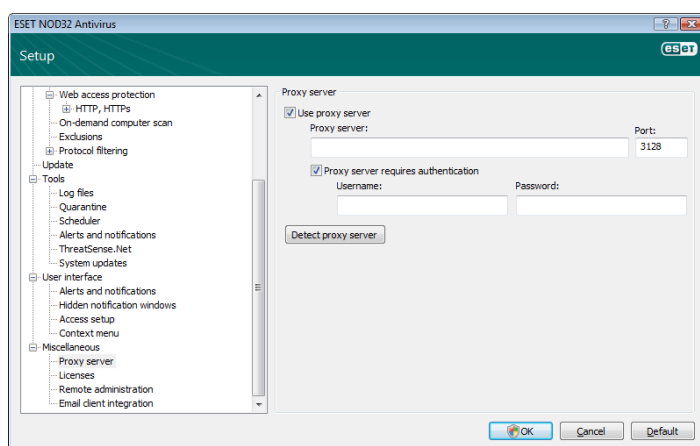
If this information is not available, you can attempt to automatically detect proxy server settings by clicking the **Detect proxy server** button.

NOTE: Proxy server options for various update profiles may differ. If this is the case, configure the different update profiles in Advanced Setup by clicking **Update** from the Advanced Setup tree.

3.4 Settings protection

ESET NOD32 Antivirus settings can be very important from the perspective of your organization's security policy. Unauthorized modifications can potentially endanger the stability and protection of your system. To password protect the setup parameters, from the main menu click **Setup > Enter entire advanced setup tree… > User interface > Access setup**, select the **Password protect settings** option and click the **Set password…** button.

Enter a password in the **New password** and **Confirm new password** fields and click **OK**. This password will be required for any future modifications to ESET NOD32 Antivirus settings.
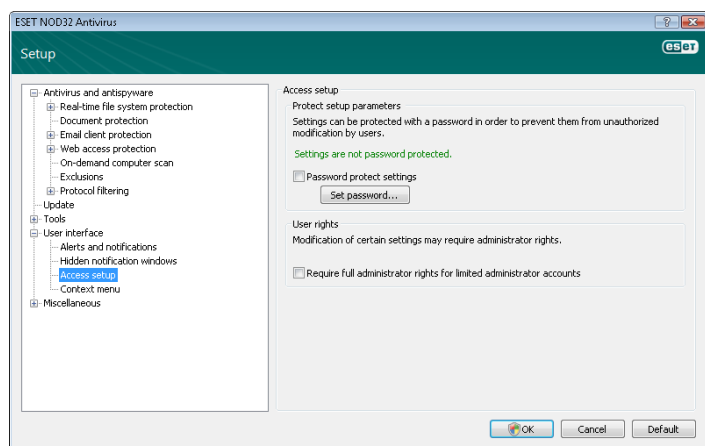
4. Work with ESET NOD32 Antivirus

4.1 Antivirus and antispyware protection

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

4.1.1 Real-time file system protection

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

4.1.1.1 Control setup

The Real-time file system protection checks all types of media, and control is triggered by various events. Using ThreatSense technology detection methods (described in section 4.1.6, "ThreatSense engine parameter setup"), real-time file system protection may vary for newly created files and existing files. For newly created files, it is possible to apply a deeper level of control.

To provide the minimum system footprint when using real-time protection, files which 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 configured using Smart optimization. If this is disabled, all files are scanned each time they are accessed. To modify this option, open the Advanced Setup window and click **Antivirus and antispyware > Real-time file system protection** from the Advanced Setup tree. Then click the **Setup…** button next to T**hreatSense engine parameter setup**, click **Other** and select or deselect the **Enable Smart optimization** option.

By default, Real-time protection launches at system startup and provides uninterrupted scanning. In special cases (e.g., if there is a conflict with another real-time scanner), real-time protection can be terminated by deselecting the **Start Real-time file system protection automatically** option.
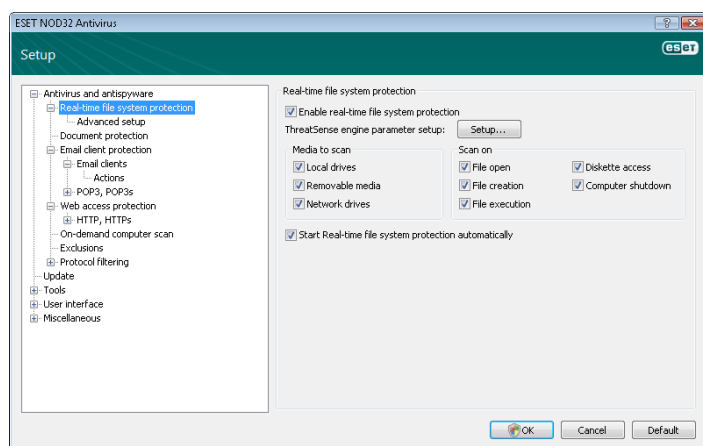
4.1.1.1.1 Media to scan

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

Local drives – Controls all system hard drives

Removable media – Diskettes, USB storage devices, etc.

Network drives – Scans all mapped drives

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

4.1.1.1.2 Scan on (Event-triggered scanning)

By default, all files are scanned upon opening, creation or execution. We recommend that you keep the default settings, as these provide the maximum level of real-time protection for your computer.

The **Diskette access** option provides control of the diskette boot sector when this drive is accessed. The **Computer shutdown** option provides control of the hard disk boot sectors during computer shutdown. Although boot viruses are rare today, we recommend that you leave these options enabled, as there is still the possibility of infection by a boot virus from alternate sources.

4.1.1.1.3 Advanced scan options

More detailed setup options can be found under **Antivirus and antispyware > Real-time system protection > Advanced setup**.

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. That is why the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics are used, which greatly improves detection rates. In addition to newly-created files, scanning is also 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, deselect the **Default archive scan settings** option.

Additonal ThreatSense parameters for executed files – By default, advanced heuristics are not used when files are executed. However, in some cases you may want to enable this option (by checking the **Advanced heuristics on file execution** option). Note that advanced heuristics may slow the execution of some programs due to increased system requirements.

4.1.1.2 Cleaning levels

The real-time protection has three cleaning levels (to access, click the **Setup…** button in the **Real-time file system protection** section and then click the **Cleaning** branch).

- The first level displays an alert window with available options for each infiltration found. You must choose an action for each infiltration individually. This level is designed for more advanced user who know what to do with every type of infiltration.

- The medium level automatically chooses and performs a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by an information message located in the bottom right corner of the screen. However, an automatic action is not performed if the infiltration is located within an archive which also contains clean files, and it is not performed on objects for which there is no predefined action.

- The third level is the most "aggressive" – all infected objects are cleaned. As this level could potentially result in the loss of valid files, we recommended that it be used only in specific situations.
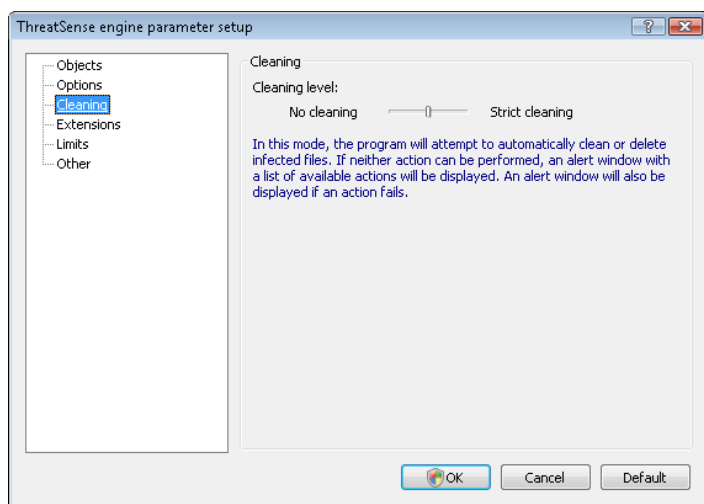
4.1.1.3   When to modify real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Therefore, please use caution when modifying its parameters. We recommend that you only modify its parameters in specific cases. For example, if there is a conflict with a certain application or real-time scanner of another antivirus program.

After installation of ESET NOD32 Antivirus, all settings are optimized to provide the maximum level of system security for users. To restore the default settings, click the **Default** button located at the bottom-right of the **Real-time file system protection** window (**Advanced Setup window > Antivirus and antispyware > Real-time file system protection**).

4.1.1.4   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 special 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 eicar.com is available for download at http://www.eicar.org/download/eicar.com

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

In the next chapter, we describe problem situations 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 > Antivirus and antispyware** and click **Enable** in the **Real-time file system protection** section of the main program window.

If real-time protection is not initiated at system startup, it is probably due to the disabled option **Automatic real-time file system protection startup**. To enable this option, navigate to Advanced Setup (F5) and click **Real-time file system protection** in the Advanced Setup tree. In the **Advanced setup** section at the bottom of the window, make sure that the **Automatic real-time file system protection startup** checkbox is selected.
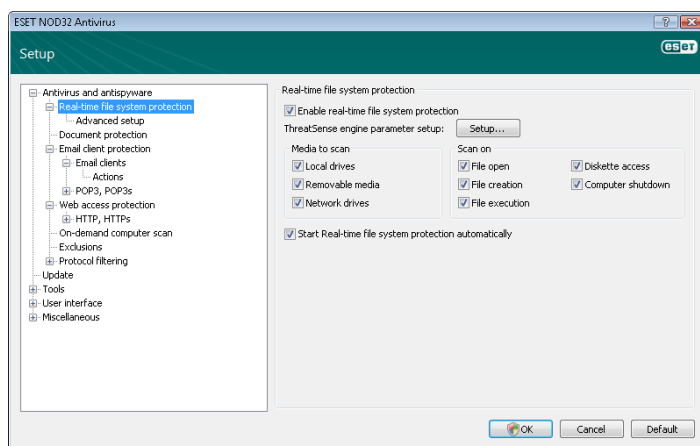
Real-time protection does not detect and clean infiltrations

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.

Real-time protection does not start

If real-time protection is not initiated at system startup (and the **Automatic real-time file system protection startup** option is enabled), it may be due to conflicts with other programs. If this is the case, please consult ESET's Customer Care specialists.

4.1.2   Host Intrusion Prevention System (HIPS)

Host Intrusion Prevention System (HIPS) protects your system from malware or any unwanted activity attempting to negatively affect the security of your computer. It utilizes advanced behavioral analysis coupled with the detection capabilities of network filter to monitor running processes, files and registry keys, actively blocking and preventing any such attempts.

4.1.3   Email client protection

Email protection provides control of email communication received through the POP3 protocol. Using the plug-in program for Microsoft Outlook, ESET NOD32 Antivirus provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP). When examining incoming messages, the program uses all advanced scanning methods provided by 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 protocol communications is independent of the email client used.

4.1.3.1   POP3 checking

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

The protection module providing this control is automatically initiated at system startup and is then active in memory. For the module to work correctly, please make sure it is enabled – POP3 checking is performed automatically with no need for reconfiguration of the email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

Encrypted communication is not controlled.
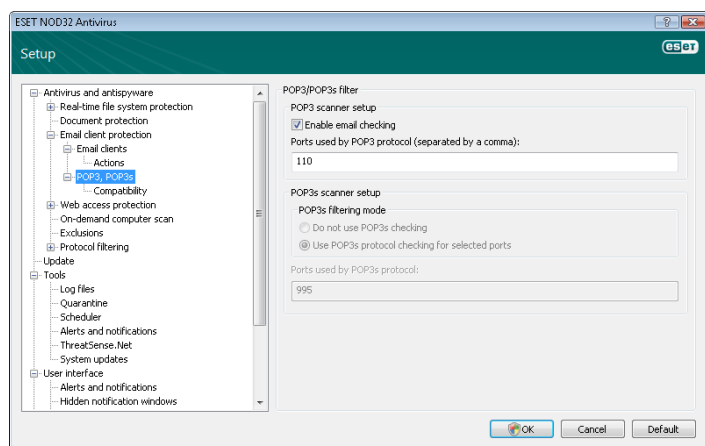
4.1.3.1.1 Compatibility

Certain email programs may experience problems with POP3 filtering (e.g., if receiving messages with a slow Internet connection, timeouts may occur due to checking). If this is the case, try modifying the way control is performed. Decreasing the control level may improve the speed of the cleaning process. To adjust the control level of POP3 filtering, from the Advanced Setup tree, navigate to **Antivirus and antispyware > Email protection > POP3, POP3s > Compatibility**.

If **Maximum efficiency** is enabled, infiltrations are removed from infected messages and information about the infiltration is inserted before the original email subject (the options **Delete** or **Clean** must be activated, or **Strict** or **Default** cleaning level must be enabled).

Medium compatibility modifies the way messages are received. Messages are gradually sent to the email client – after the last part of the message is transferred, it will be scanned for infiltrations. However, the risk of infection increases with this level of control. The level of cleaning and the handling of tag messages (notification alerts which are appended to the subject line and body of emails) is identical to the maximum efficiency setting.

With the **Maximum compatibility** level, you are warned by an alert window which reports the receipt of an infected message. No information about infected files is added to the subject line or to the email body of delivered messages and infiltrations are not automatically removed – you must delete infiltrations from the email client.
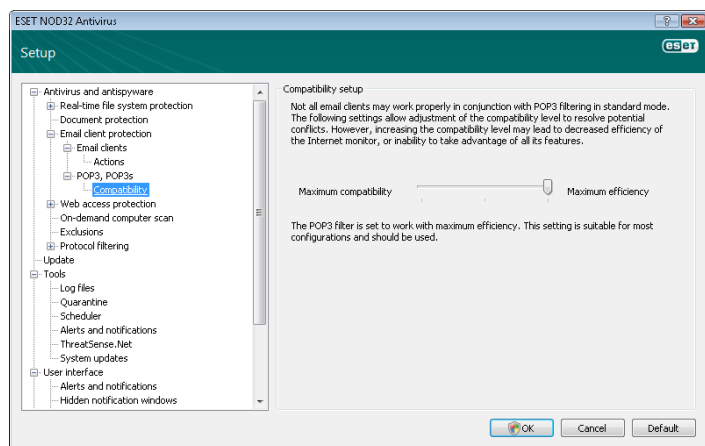
4.1.3.2 Integration with email clients

Integration of ESET NOD32 Antivirus with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, this integration can be enabled in ESET NOD32 Antivirus. If integration is activated, the ESET NOD32 Antivirus toolbar is inserted directly into the email client, allowing for more efficient email protection. The integration settings are available through **Setup > Enter entire advanced setup tree... > Miscellaneous >Email client integration**. Email client integration allows you to activate integration with supported email clients. Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail and Mozilla Thunderbird.

Select the **Disable checking upon inbox content change** option if you are experiencing a system slowdown when working with your email client. Such a situation may take place when downloading email from Kerio Outlook Connector Store

Email protection is activated by clicking **Setup > Enter entire advanced setup tree... > Antivirus and antispyware > Email client protection** and selecting the **Enable email client protection** option.
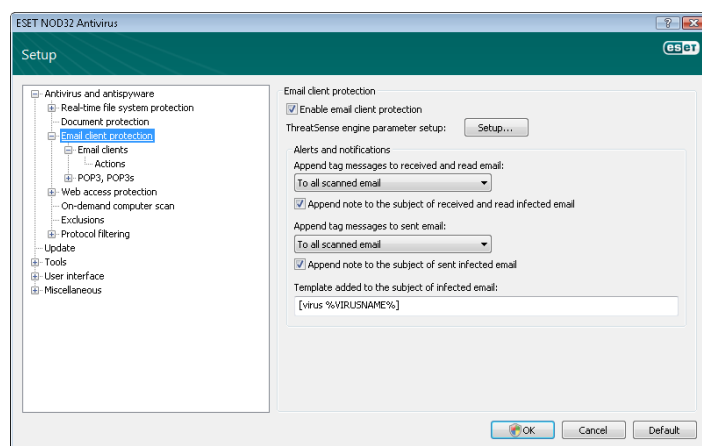
4.1.3.2.1 Appending tag messages to email body

Each email scanned by ESET NOD32 Antivirus can be marked by appending a tag message to the subject or email body. This feature increases the level of credibility for the recipient and if an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

The options for this functionality are available through **Advanced setup window > Antivirus and antispyware > Email client protection**. You can select to **Append tag messages to received and read mail**, as well as **Append tag messages to sent mail**. You also have the ability to decide whether tag messages are appended to all scanned email, to infected email only, or not at all.

ESET NOD32 Antivirus also allows you to append messages to the original subject of infected messages. To enable appending to the subject, select both the **Append note to the subject of received and read infected email** and **Append note to the subject of sent infected email** options.

The content of notifications can be modified in the **Template added to the subject of infected email** field. The above-mentioned modifications can help automate the process of filtering infected email, as it allows you to filter email with a specific subject (if supported in your email client) to a separate folder.

4.1.3.3 Removing infiltrations

If an infected email message is received, an alert window will display. The alert window shows the sender name, email and the name of the infiltration. In the lower part of the window the options **Clean**, **Delete** or **Leave** are available for the detected object. In almost all cases, we recommend that you select either **Clean** or **Delete**. In certain situations, if you wish to receive the infected file, select **Leave**. If **Strict cleaning** is enabled, an information window with no options available for infected objects will displayed.

4.1.4 Web access protection

Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your Web access protection. We strongly recommend that the **Enable web access protection** option is selected. This option is located in the Advanced Setup window (F5), **Antivirus and antispyware > Web access protection**.
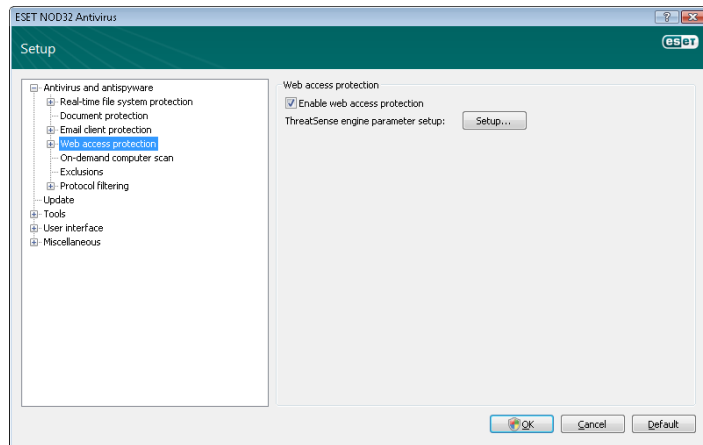
4.1.4.1 HTTP, HTTPs

Web access protection works by monitoring communication between Internet browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPs (encrypted communication) rules. By default, ESET NOD32 Antivirus is configured to use the standards of most Internet browsers. However, the HTTP scanner setup options can be modified in the Advanced Setup window (F5), **Antivirus and antispyware > Web access protection > HTTP, HTTPs**. In the main **HTTP filter** window, you can select or deselect the **Enable HTTP checking** option. You can also define the port numbers used for HTTP communication. By default, the port numbers 80, 8080 and 3128 are predefined. HTTPs checking can be performed in the following modes:

Do not use HTTPs protocol checking – Encrypted communication will not be checked

Use HTTPs protocol checking for selected ports – HTTPs checking is performed only for ports defined in **Ports used by HTTPs protocol**

Use HTTPs protocol checking for applications marked as Internet browsers that use selected ports – Only checks applications that are specified in the browsers section and uses ports defined in **Ports used by HTTPs protocol**
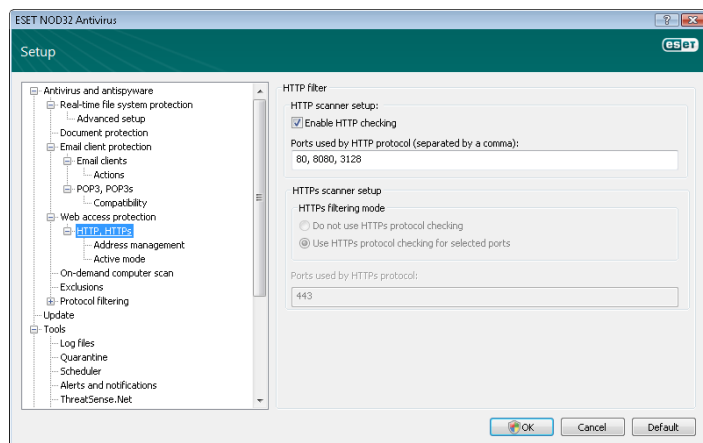
4.1.4.1.1 Address management

This section allows you to specify HTTP addresses to block, allow or exclude from checking. The buttons **Add, Edit, Remove** and **Export** are used to manage the lists of addresses. Websites in the list of blocked addresses will not be accessible. Websites in the list of excluded addresses are accessed without being scanned for malicious code. If you select the **Allow access only to HTTP addresses in the list of allowed addresses** option, only addresses present in the list of allowed addresses will be accessible, while all other HTTP addresses will be blocked.

In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list. To activate a list, select the **List active** option. If you wish to be notified when entering an address from the current list, select **Notify when applying address from the list** option.
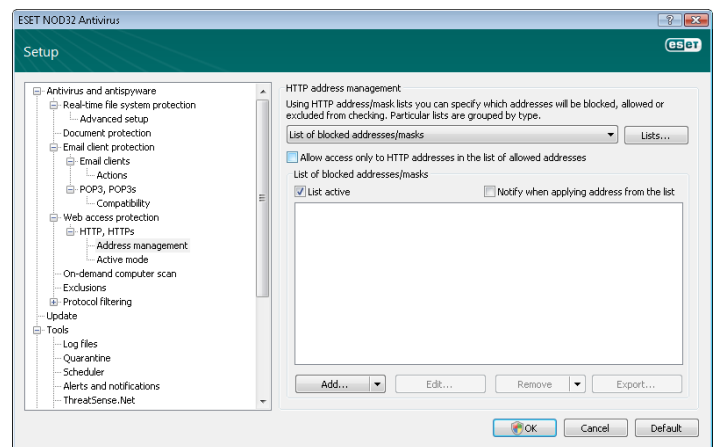
4.1.4.1.2 Web browsers

ESET NOD32 Antivirus also contains the Web browsers feature, which allows you to define whether the given application is a browser or not. If an application is marked as a browser, all communication from this application is monitored regardless of the port numbers involved.

The Web browsers feature complements the HTTP checking feature, as HTTP checking only takes place on predefined ports. However, many Internet services utilize dynamically changing or unknown port numbers. To account for this, the Web browser feature can establish control of port communications regardless of the connection parameters.
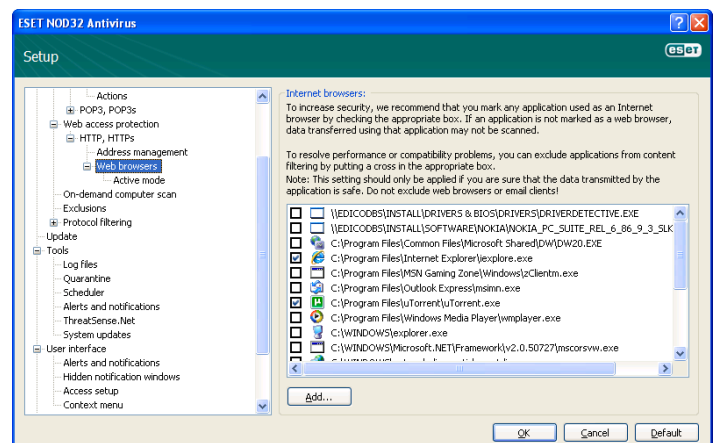
The list of applications marked as web browsers is accessible directly from the **Web browsers** submenu of the **HTTP** branch. This section

also contains the submenu **Active mode**, which defines the checking mode for Internet browsers.

Active mode is useful because it examines transferred data as a whole. If it is not enabled, communication of applications is monitored gradually in batches. This decreases the effectiveness of the data verification process, but also provides higher compatibility for listed applications. If no problems occur while using it, we recommend that you enable active checking mode by selecting the checkbox next to the desired application.
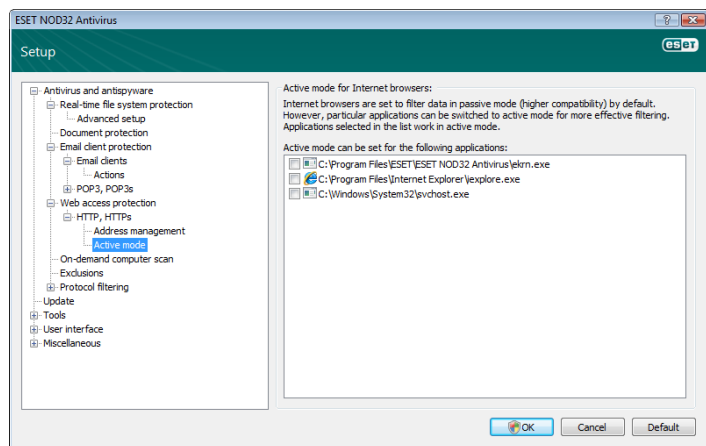
4.1.5 On-demand computer scan

If you suspect that your computer is infected (it behaves abnormally), run an On-demand computer scan to examine your computer for infiltrations. 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. Regular scanning can detect infiltrations that were not detected by the real-time scanner when they were saved to the disk. This can happen if the real-time scanner was disabled at the time of infection, or if the virus signature database is not up-to-date.

We recommend that you run an On-demand computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools > Scheduler**.

4.1.5.1 Type of scan

Two types of On-demand computer scans 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, as well as choose specific scan targets.

4.1.5.1.1 Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantages

16

are easy operation with no 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 section 4.1.6.3, "Cleaning".

4.1.5.1.2 Custom scan

Custom scan is an optimal solution if you wish 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. The configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with 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 more precisely specified by entering the path to the folder or file(s) you wish to include. If you are only interested in scanning the system without additional cleaning actions, select the **Scan without cleaning** option. Furthermore, you can choose from three cleaning levels by clicking **Setup… > Cleaning**.

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

4.1.5.2 Scan targets

The Scan targets drop-down menu allows you to select files, folders and devices (disks) to be scanned for viruses.

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 drives

No selection – Cancels all selections
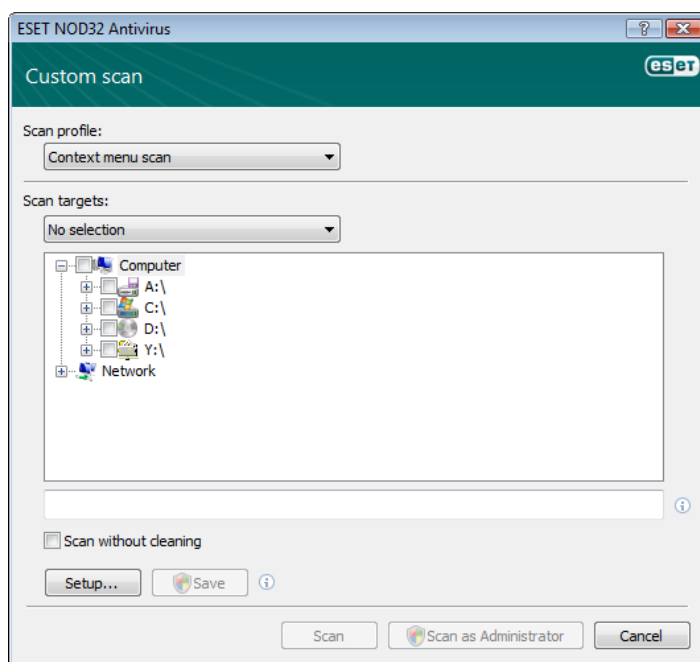
A scan target can also be more precisely specified by entering the path to the folder or file(s) you wish to include in scanning. Select targets from the tree structure listing all devices available on the computer.

4.1.5.3   Scan profiles

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.
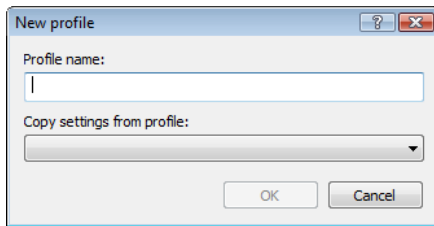
To create a new profile, open the Advanced Setup window (F5) and click **On-demand computer scan > Profiles…** The **Configuration profiles** window has a drop-down menu of existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see section 4.1.6, "ThreatSense engine parameters setup" 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**. From the **Configuration profiles** window, click the **Add…** button. Enter the name of your new profile in the **Profile name** field, and select **Smart scan** from the **Copy settings from profile:** drop-down menu. Then adjust the remaining parameters to meet your requirements.

4.1.6   Protocol filtering

Antivirus protection for the application protocols POP3 and HTTP is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. The control works automatically regardless of the Internet browser or email client used. The following options are available for protocol filtering (if the **Enable application protocol content filtering** option is selected):

HTTP and POP3 ports - Limits scanning of communication to known HTTP and POP3 ports.

Applications marked as Internet browsers and email clients – Enable this option to only filter communication of applications marked as browsers (**Web access protection > HTTP, HTTPS > Web browsers**) and email clients (**Email client protection > POP3, POP3s > Email clients**).

Ports and applications marked as Internet browsers or email clients – Both ports and browsers are checked for malware

NOTE: Starting with Windows Vista Service Pack 1 and Windows Server 2008, a new communication filtering is used. As a result, the Protocol filtering section is not available.

4.1.6.1   SSL

ESET NOD32 Antivirus enables you to check protocols encapsulated in SSL protocol. You can use various scanning modes for SSL protected communications using trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Always scan SSL protocol – 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 about the fact and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked as trusted (it is added to the trusted certificates list), communication to the server is allowed and the content of the communication

channel is filtered.

Ask about non-visited sites (exclusions can be set) - If you enter a new SSL protected site (with an unknown certificate), an action selection dialog is displayed. This mode enables you to create a list of SSL certificates that will be excluded from scanning.

Do not scan SSL protocol - If selected, the program will not scan communications over SSL.

If the certificate cannot be verified using the Trusted Root Certification Authorities store (**protocol filtering > SSL > Certificates**):

Ask about certification validity – Prompts you to select an action to take.

Block communication that uses the certificate – Terminates connection to the site that uses the certificate.

If the certificate is invalid or corrupt (**protocol filtering > SSL > Certificates**):

Ask about certificate validity – Prompts you to select an action to take.

Block communication that uses the certificate – Terminates connection to the site that uses the certificate.

4.1.6.1.1   Trusted certificates

In addition to the integrated Trusted Root Certification Authorities store, where ESET NOD32 Antivirus stores trusted certificates, you can create a custom list of trusted certificates that can be viewed in **Advanced Setup** (F5) > **Protocol filtering** > **SSL** > **Certificates >Trusted certificates**.

4.1.6.1.2   Excluded certificates

The Excluded certificates section contains certificates that are considered to be safe. The program will not check the content

of encrypted communications utilizing certificates in this list. We recommend installing only those web certificates which are guaranteed to be safe and have no need for content filtering.

4.1.7   ThreatSense engine parameters setup

ThreatSense is the name of the technology consisting of complex threat detection methods. This technology is proactive, which means it also provides protection during the early hours of the spread of a new threat. It uses a combination of several methods (code analysis, code emulation, generic signatures, 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.

The ThreatSense technology 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 the **Setup…** button located in any module's setup window which uses ThreatSense technology (see below). Different security scenarios could require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection

- System startup file check

- Email protection

- Web access protection

- On-demand computer scan

The 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). Therefore, we recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

4.1.7.1 Objects setup

The **Objects** 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.

Files – Provides scanning of all common file types (programs, pictures, audio, video files, database files, etc.).

Email files – Scans special files where email messages are contained.

Archives – Provides scanning of files compressed in archives (.rar, .zip, .arj, .tar, etc.).

Self-extracting archives – Scans files which are contained in self-extracting archive files, but typically presented with an .exe file extension.

Runtime packers – Runtime packers (unlike standard archive types) decompress in memory, in addition to standard static packers (UPX, yoda, ASPack, FGS, etc.).
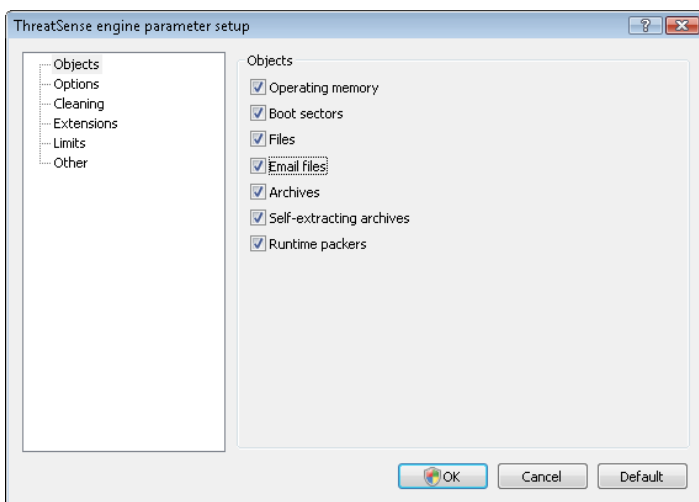
4.1.7.2 Options

In the **Options** section, you can select the methods to be used when scanning the system for infiltrations. The following options are available:
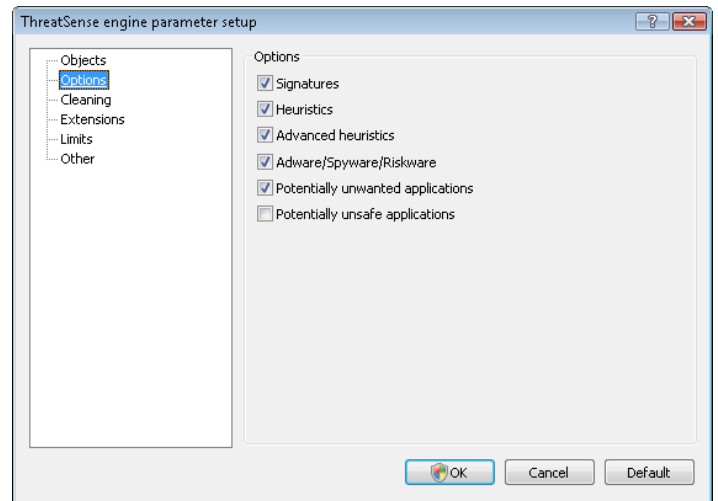
Signatures – Signatures can exactly and reliably detect and identify infiltrations by their name using virus signatures.

Heuristics – Heuristics use an algorithm that analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist, or was not included in the list of known viruses (virus signatures database).

Advanced heuristics – Advanced heuristics comprise a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. Due to advanced heuristics, the detection intelligence of the program is significantly higher.

Adware/Spyware/Riskware – This category includes software which collects various sensitive information about users without their informed consent. This category also includes software which displays advertising material.

Potentially unwanted applications – Potentially unwanted applications are not necessarily intended to be malicious, but they may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.

Potentially unsafe applications – Potentially unsafe applications is the classification used for commercial, legitimate software. It includes programs such as remote access tools, which is why this option is disabled by default.

4.1.7.3 Cleaning

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

No cleaning – Infected files are not cleaned automatically. The program will display a warning window and allow you to choose an action.

Standard cleaning – The program will attempt to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program will offer a choice of follow-up actions. The choice of follow-up actions will also be displayed if a predefined action could not be completed.

Strict cleaning – The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean them, you will be offered an action to take in a warning window.

Warning: In the Default mode, the entire archive file is deleted only if all files in the archive are infected. If the archive also contains legitimate files, it will not be deleted.If an infected archive file is detected in Strict cleaning mode, the entire archive will be deleted, even if clean files are present.
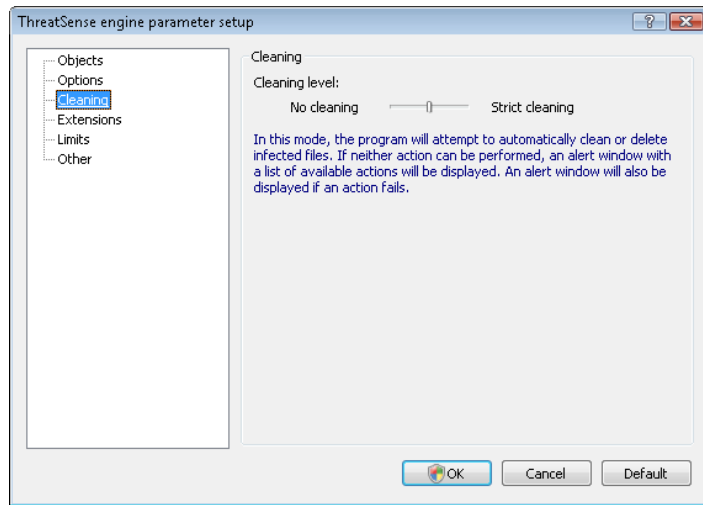
4.1.7.4 Extensions

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

By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. If the **Scan all files** option is unchecked, the list changes to show all currently scanned file extensions. Using the **Add** and **Remove** buttons, you can enable or prohibit scanning of desired extensions.

To enable scanning of files with no extension, select the **Scan extensionless files** option.

Excluding files from scanning is sometimes necessary if the scanning of certain file types prevents the program which is using the extensions from running properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using the Microsoft Exchange servers.

4.1.7.5 Limits

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

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. We do not recommend changing the default value, as there is usually no reason to modify it. This option should only be changed by advanced users who have specific reasons for excluding larger objects from scanning.

Maximum scan time for object (sec.): – Defines the maximum time value for scanning 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.

Archive nesting level: –Specifies the maximum depth of archive scanning. We do not recommend changing the default value of 10; under normal circumstances, there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive will remain unchecked.

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. If this causes scanning an archive to be prematurely terminated, the archive will remain unchecked.

4.1.7.6 Other

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

Run background scans with low priority – Scanning sequences consume 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.

Enable Smart optimization – Select this option so that files which have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update.

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

Scroll log – This option allows you to enable/disable log scrolling. If selected, information scrolls upwards within the display window.

Display notification about scan completion in a separate window – Opens a window containing information about scan results.
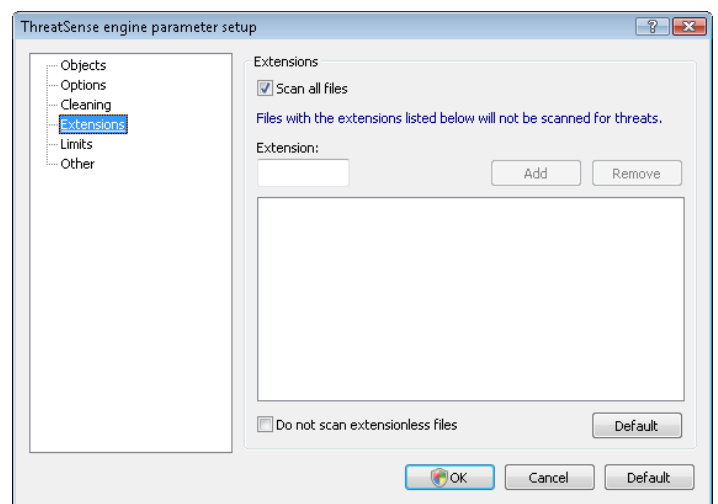
4.1.8 An infiltration is detected

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

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

• Open ESET NOD32 Antivirus and click **Computer scan**

• Click **Smart scan** (for more information, see section 4.1.4.1.1, "Smart scan")

• After the scan has finished, review the log for the number of scanned, infected and cleaned files.

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

As a general example of how infiltrations are handled in ESET NOD32 Antivirus, suppose that an infiltration is detected by the real-time file system monitor, which uses the Default cleaning level. It will attempt to clean or delete the file. If there is no predefined action to take for

the real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **Leave** are available. Selecting **Leave** is not recommended, since the infected file(s) would be left untouched. The exception to this is when you are sure that the file is harmless and has been detected by mistake.
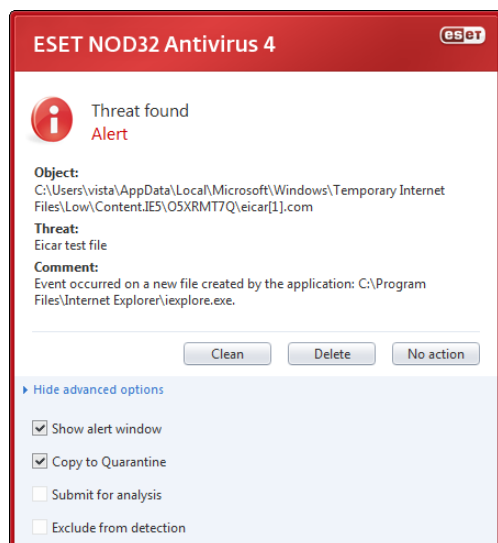
Cleaning and deleting – Apply cleaning if a file has been attacked by a virus which has attached malicious code to the file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.

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).

Deleting files in archives – In the 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. However, use caution when performing a Strict cleaning scan – with Strict cleaning the archive will be deleted if it contains at least one infected file, regardless of the status of other files in the archive.

4.2   Updating the program

Regular updating of ESET NOD32 Antivirus is the basic premise for obtaining the maximum level of security. 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** from the main menu, 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, as well as basic setup options such as the username and password to access ESET's update servers.

Use the **Product activation** link to open a registration form that will activate your ESET security product and send you an email with your authentication data (username and password).
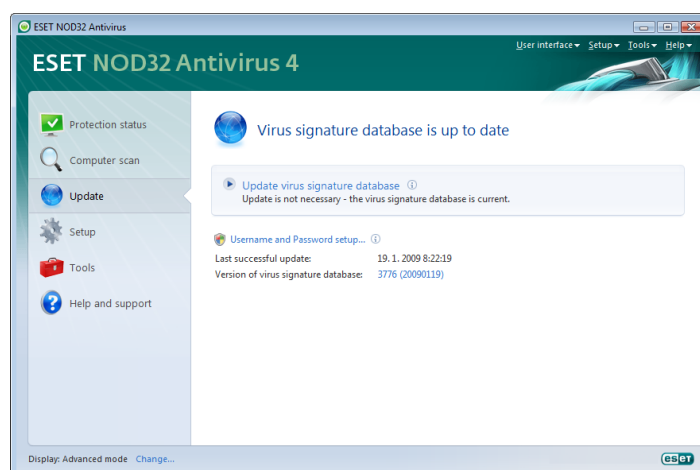
NOTE: The username and password are provided by ESET after purchasing ESET NOD32 Antivirus.

4.2.1   Update setup

The update setup section specifies update source information such as the update servers and authentication data for these servers. By default, the **Update server** drop-down menu is set to **Choose automatically** to ensure that update files will automatically download from the ESET server with the least network traffic. The update setup options are available from the Advanced Setup tree (F5), under **Update**.
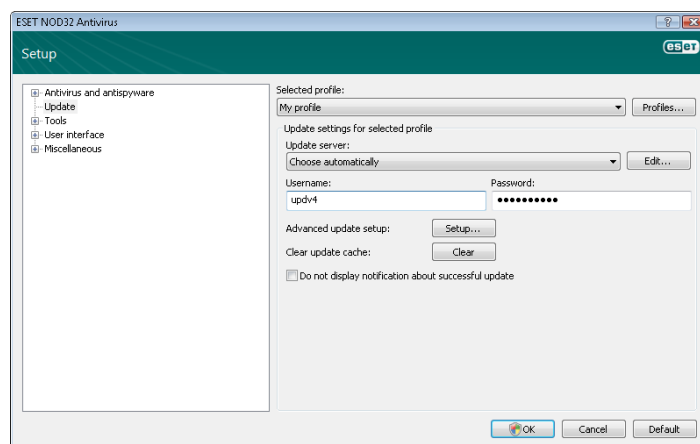
The list of available update servers is accessible via the **Update server** drop-down menu. To add a new update server, click **Edit…** in the **Update settings for selected profile** section and then click the **Add** button. Authentication for update servers is based on the **Username** and **Password** generated and sent to you after purchase.

4.2.1.1   Update profiles

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

The **Selected profile** drop-down menu displays the currently selected profile, set to **My profile** by default. To create a new profile, click the **Profiles…** button and then click the **Add…** button and enter your own **Profile name**. When creating a new profile, you can copy settings from an existing one by selecting it from the **Copy settings from profile** drop-down menu.
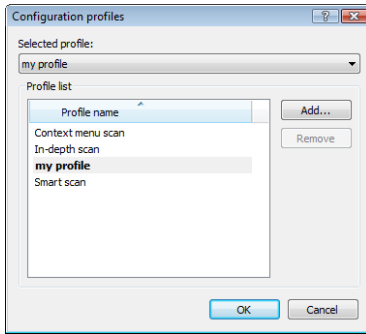
In the profile setup you can specify the update server from a list of available servers, or a new server can be added. The list of existing update servers is accessible via the **Update server:** drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button.

4.2.1.2 Advanced update setup

To view the Advanced update setup, click the **Setup…** button. Advanced update setup options include configuration of **Update mode, HTTP Proxy, LAN** and **Mirror**.

4.2.1.2.1 Update mode

The **Update mode** tab contains options related to the program component update.

In the **Program component update** section, three options are available:

- **Never update program components:** New program component updates will not be downloaded.

- **Always update program components:** New program component updates will occur automatically**.**

- **Ask before downloading program components:** The default option. You will be prompted to confirm or refuse program component updates when they are available.
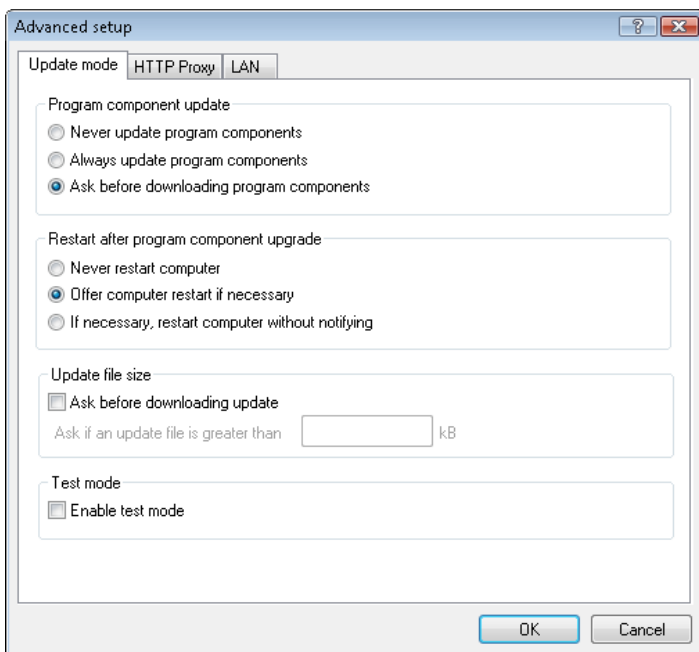
After a program component update, you may need to restart your computer to provide full functionality. In the **Restart after program component upgrade** section you can select one of three options:

- **Never restart computer**

- **Offer computer restart if necessary**

- **If necessary, restart computer without notifying**

The default option is **Offer computer restart if necessary**. Selection of 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 – e.g., restarting the server automatically after a program upgrade could cause serious damage.

4.2.1.2.2 Proxy server

To access the proxy server setup options for a given update profile: Click **Update** in the Advanced Setup tree (F5) and then click the **Setup…** button to the right of **Advanced update setup.** Click the **HTTP Proxy** tab and select one of the three following options:

- **Use global proxy server settings**

- **Do not use proxy server**

- **Connection through a proxy server** (connection defined by the connection properties)

Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified within the **Miscellaneous > Proxy server** branch of the Advanced Setup tree.
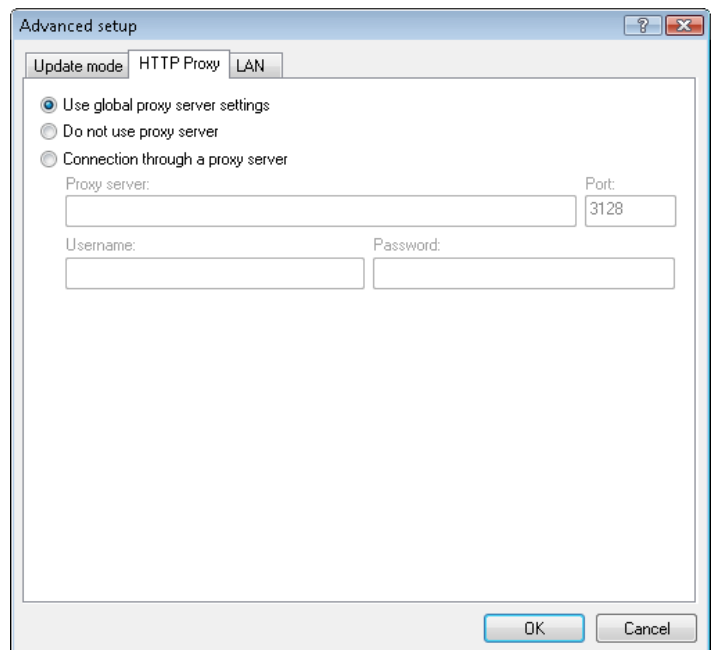
Select the **Do not use proxy server** option to specify that no proxy server will be used to update ESET NOD32 Antivirus.

The **Connection through a proxy server** option should be selected if a proxy server should be used to update ESET NOD32 Antivirus and is different from the proxy server specified in the global settings (**Miscellaneous > Proxy server**). If so, the settings should be specified here: **Proxy server** address, communication **Port**, plus **Username** and **Password** for the proxy server, if required.

This option should also be selected if the proxy server settings were not set globally, but ESET NOD32 Antivirus will connect to a proxy server for updates.

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

4.2.1.2.3 Connecting to the LAN

When updating from a local server with an NT-based operating

system, authentication for each network connection is required by default. In most cases, a local system account does not have sufficient rights to access the Mirror folder (the Mirror folder contains copies of update files). If this is the case, enter the username and password in the update setup section, or specify an existing account under which the program will access the update server (Mirror).

To configure such an account, click the **LAN** tab. The **Connect to LAN as** section offers the **System account (default)**, **Current user**, and **Specified user** options.
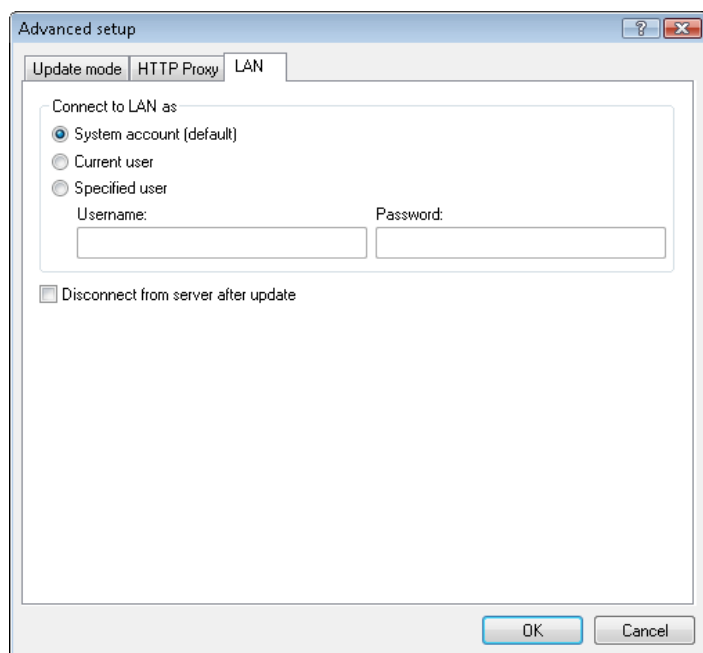
Select the **System account (default)** option to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

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.

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 inserting 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 the user's password. When updating from the HTTP version of the local server, no authentication is required.

4.2.1.2.4   Creating update copies – Mirror

ESET NOD32 Antivirus Business Edition allows you to create copies of update files which can be used to update other workstations located in the network. Updating client workstations from a Mirror optimizes network load balance and saves Internet connection bandwidth.

Configuration options for the local Mirror server are accessible (after adding a valid license key in the license manager, located in the ESET NOD32 Antivirus Business Edition Advanced Setup section) in the **Advanced update setup:** section (to access this section, press F5 and click **Update** in the Advanced Setup tree, then click the **Setup…** button next to **Advanced update setup:** and select the **Mirror** tab).
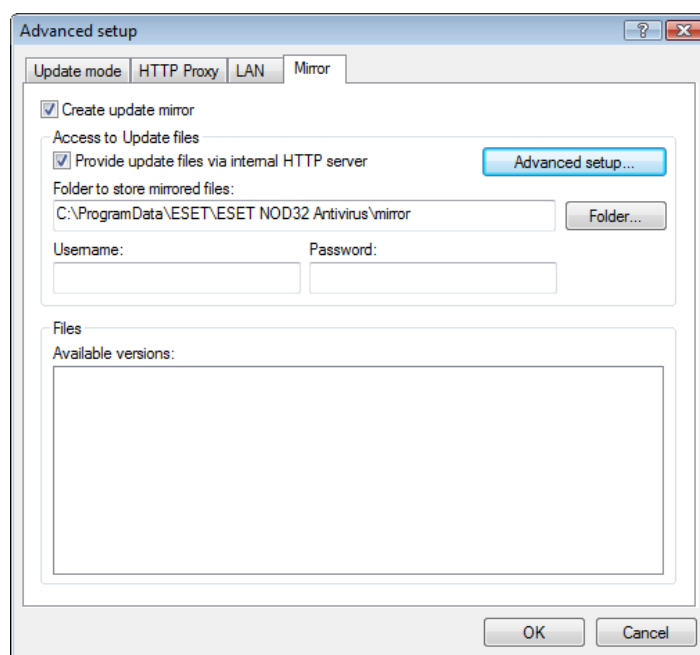
The first step in configuring the Mirror is to select the **Create update mirror** option. Selecting this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

The methods of Mirror activation are described in detail in section 4.2.1.2.4.1, "Updating from the Mirror". For now, note that there are two basic methods for accessing the Mirror – the folder with update files can be presented as a shared network folder or as an HTTP server.

The folder dedicated to storing update files for the Mirror is defined in the **Folder to store mirrored files** section. 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 supplied in the **Username** and **Password** fields. The username and password should be entered in the format *Domain/User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

When configuring the Mirror, you can also specify the language versions for which you want to download update copies. Language version setup is accessible in the section **Files - Available versions:**.

4.2.1.2.4.1   Updating from the Mirror

There are two basic methods of configuring the Mirror – 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. In order to allow access to the Mirror using the HTTP server, navigate to **Advance update setup** (the **Mirror** tab) and select the **Create update mirror** option.

In the **Advanced setup** 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 the 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 should be located on the same computer as the ESET NOD32 Antivirus instance creating it.
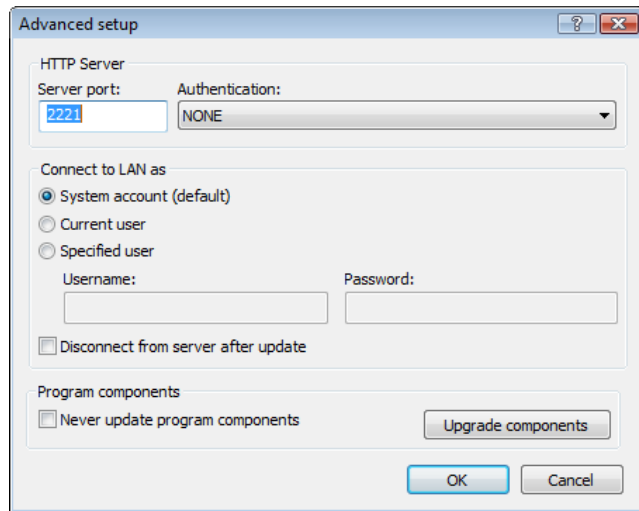
After configuration of the Mirror is complete, go to the workstations and add a new update server in the format **http://IP_address_of_your_server:2221**. To do this, follow the steps below:

- Open ESET NOD32 Antivirus **Advanced Setup** and click the **Update** branch.

- Click **Edit...** to the right of the **Update server** drop-down menu and add a new server using the following format: http://IP_address_of_your_server:2221 .

- Select this newly-added server from the list of update servers.

Accessing the Mirror via system shares

First, a shared folder should be created on a local or a 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 NOD32 Antivirus from the Mirror folder.

Next, configure access to the Mirror in the **Advanced update setup** section (**Mirror** tab) by disabling the **Provide update files via internal HTTP server** option. 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 specify authentication data to access the other computer. To specify authentication data, open ESET NOD32 Antivirus Advanced Setup (F5) and click the **Update** branch. Click the **Setup…** button and then click the **LAN** tab. This setting is the same as for updating, as described in section 4.2.1.2.3, "Connecting to LAN".

After the Mirror configuration is complete, proceed to the workstations and set \\UNC\PATH as the update server. This operation can be completed using the following steps:

- Open ESET NOD32 Antivirus Advanced Setup and click **Update**

- Click **Edit…** next to the Update server and add a new server using the \\UNC\PATH format.

- Select this newly-added server from the list of update servers

NOTE: For proper functioning, the path to the Mirror folder must be specified as a UNC path. Updates from mapped drives may not work.

4.2.1.2.4.2 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. Here we give an overview of the most frequent problems which may occur during an update from the Mirror:

- **ESET NOD32 Antivirus 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**, insert the folder name and click **OK**. The contents of the folder should be displayed.

- **ESET NOD32 Antivirus requires a user name 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 NOD32 Antivirus reports an error connecting to the Mirror server** –Communication on the port defined for accessing the HTTP version of the Mirror is blocked.

4.2.2   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 NOD32 Antivirus:

- **Regular automatic update**

- **Automatic update after dial-up connection**

- **Automatic update after user logon**

Each of the aforementioned update tasks can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see section 4.3, "Scheduler".

4.3   Scheduler

Scheduler is available if Advanced mode in ESET NOD32 Antivirus is activated. **Scheduler** can be found in the ESET NOD32 Antivirus main menu under **Tools**. Scheduler contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile used.
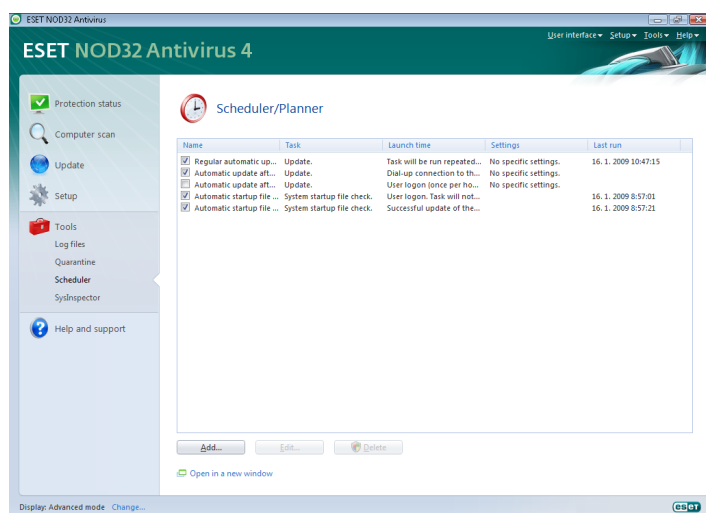
By default, the following scheduled tasks are displayed in **Scheduler**:

- **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**

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

4.3.1 Purpose of scheduling tasks

Scheduler manages and launches scheduled tasks with predefined configuration and properties. The configuration and properties contain information such as the date and time as well as specified profiles to be used during execution of the task.

4.3.2 Creating new tasks

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

- **Run external application**

- **System startup file check**

- **Create a computer status snapshot**

- **On-demand computer scan**
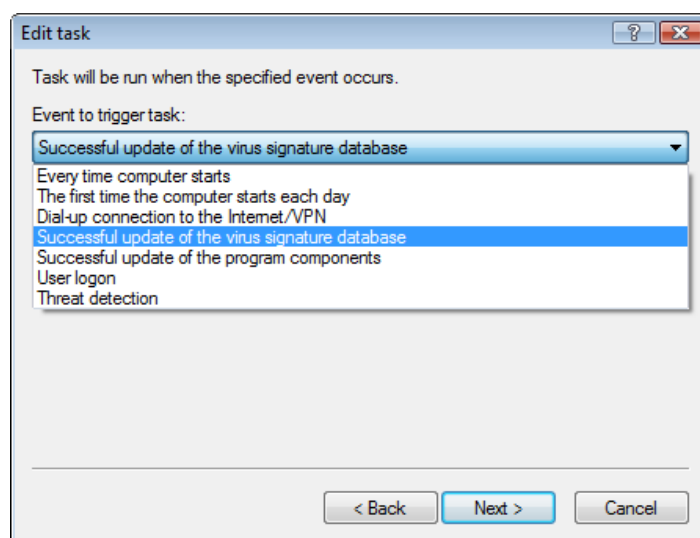
- **Update**

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

From the **Scheduled task:** drop-down menu, select **Update**. Click **Next** and enter the name of the task into the **Task name:** field. Select the frequency of the task. The following options are available: **Once, Repeatedly, Daily**, **Weekly** and **Event triggered**. Based on the frequency selected, you will be prompted with different update parameters. Next, define what action to take if the task cannot be performed or completed at the scheduled time. The following three options are available:

- **Wait until the next scheduled time**

- **Run task as soon as possible**

- **Run task immediately if the time since its last execution exceeds specified interval** (the interval can be defined using the Task interval scroll box)

In the next step, a summary window with information about the current scheduled task is displayed; the option **Run task with specific parameters** should be automatically enabled. Click the **Finish** button.

A dialog window will appear, allowing you to select profiles to be used for the scheduled task. Here you can specify a primary and alternative profile, which is used in case the task cannot be completed using the primary profile. Confirm by clicking OK in the Update profiles window. The new scheduled task will be added to the list of currently scheduled tasks.

4.4 Quarantine

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

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to ESET's Threat Lab.
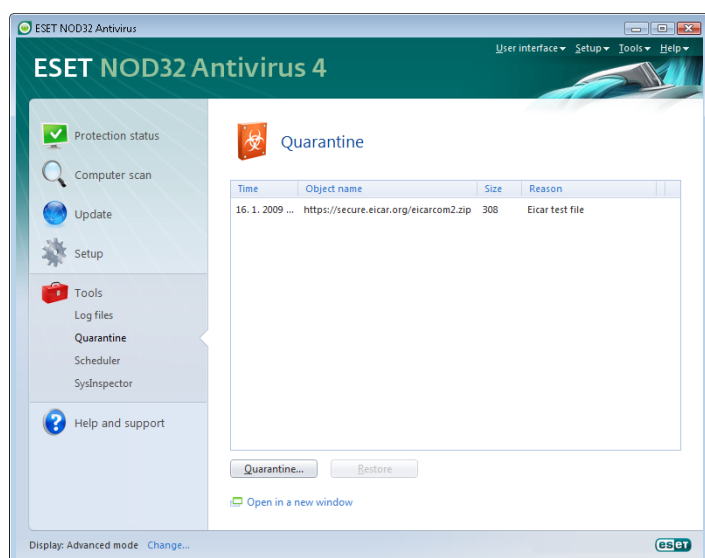
Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (**added by user...**), and number of threats (e.g., if it is an archive containing multiple infiltrations).

4.4.1 Quarantining files

ESET NOD32 Antivirus automatically quarantines deleted files (if you have not cancelled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking the **Quarantine…** button. If this is the case, the original file is not removed from its original location. The context menu can also be used for this purpose – right-click in the **Quarantine** window and select **Add…**

4.4.2 Restoring from Quarantine

Quarantined files can also be restored to their original location. Use the **Restore** feature for this purpose; this is available from the context menu by right-clicking on the given file in the Quarantine window. The context menu also offers the option **Restore to**, which allows you to restore a file to a location other than the one from which it was deleted.

NOTE: If the program quarantined a harmless file by mistake, please exclude the file from scanning after restoring and send the file to ESET Customer Care.

4.4.3 Submitting file from Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly evaluated as infected (e.g., by heuristic analysis of the code) and subsequently quarantined, please send the file to ESET's Threat Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.
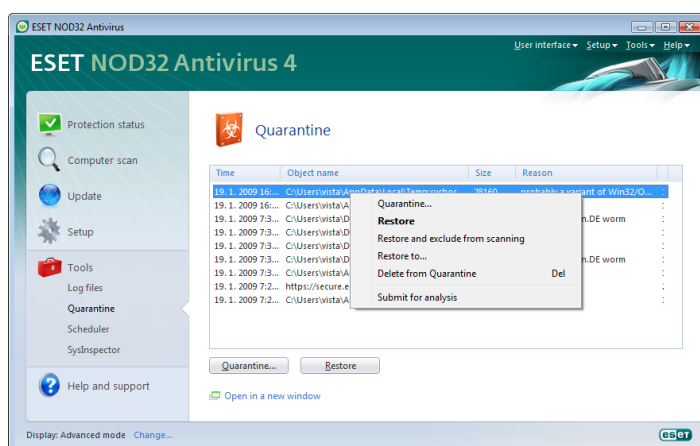
4.5 Log files

The Log files contain information about all important program events that have occurred and provide an overview of detected threats. Logging acts as 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 NOD32 Antivirus environment, as well as to archive logs.

Log files are accessible from the ESET NOD32 Antivirus main menu by clicking **Tools > Log files**. Select the desired log type using the **Log:** drop-down menu at the top of the window. The following logs are available:

1. **Detected threats** – Use this option to view all information about events related to the detection of infiltrations.

2. **Events** – This option is designed for system administrators and users to solve problems. All important actions performed by ESET NOD32 Antivirus are recorded in the Event logs.

3. **On-demand computer scan** – Results of all completed scans are displayed in this window. Double-click any entry to view details of the respective On-demand scan.
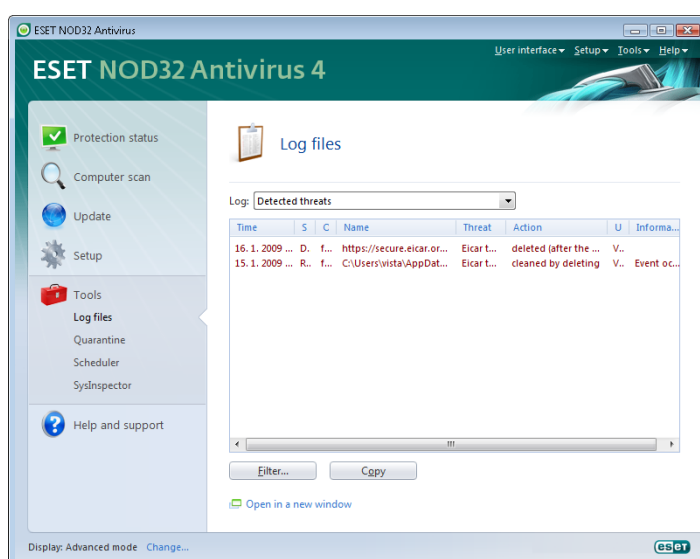
In each section, the displayed information can be directly copied to the clipboard by selecting the entry and clicking on the **Copy** button. To select multiple entries, the CTRL and SHIFT keys can be used.

4.5.1 Log maintenance

The Logging configuration of ESET NOD32 Antivirus is accessible from

the main program window. Click **Setup > Enter entire advanced setup tree... > Tools > Log files**. You can specify the following options for log files:

- **Delete records automatically:** Log entries older than the specified number of days are automatically deleted

- **Optimize log files automatically**: Enables automatic defragmentation of log files if the specified percentage of unused records has been exceeded

- **Minimum logging verbosity:** Specifies the logging verbosity level. Available options:

  - **Diagnostic records** – Logs information needed for fine-tuning of the program and all records above

  - **Informative records** – Records informative messages including successful update messages plus all records above

  - **Warnings** – Records critical errors and warning messages

  - **Errors** – Only "Error downloading file" messages are recorded, plus critical errors

  - **Critical warnings** – Logs only critical errors (error starting Antivirus protection, etc...)
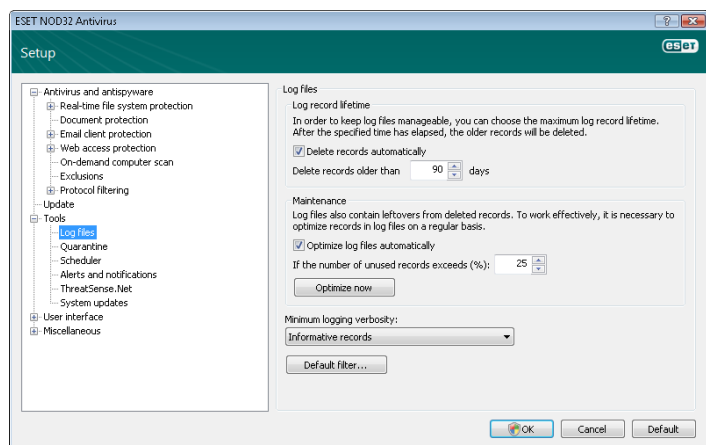
4.6   User interface

The user interface configuration options in ESET NOD32 Antivirus allow you to adjust the working environment to fit your needs. These configuration options are accessible from the **User interface** branch of the ESET NOD32 Antivirus Advanced Setup tree.

In the **User interface elements** section, the **Advanced mode** option gives users the ability to allow toggling to Advanced mode. Advanced mode displays more detailed settings and additional controls to ESET NOD32 Antivirus.

The **Graphical user interface** option should be disabled if the graphical elements slow the performance of your computer or cause other problems. The graphical interface may also need to be turned off for visually impaired users, as it may conflict with special applications that are used for reading text displayed on the screen.

If you wish to deactivate the ESET NOD32 Antivirus splash-screen, deselect the **Show splash-screen at startup** option.

At the top of the ESET NOD32 Antivirus main program window is a Standard menu which can be activated or disabled based on the **Use standard menu** option.

If the **Show tooltips** option is enabled, a short description of any option will be displayed if the cursor is placed over the option. The **Select active control element** option will cause the system to

highlight any element which is currently under the active area of the mouse cursor. The highlighted element will be activated after a mouse click.

To decrease or increase the speed of animated effects, select the **Use animated controls** option and move the **Speed** slider bar to the left or right.

To enable the use of animated icons to display the progress of various operations, select the **Use animated icons for progress indication** option. If you want the program to sound a warning if an important event takes place, select the **Use sound signal** option.
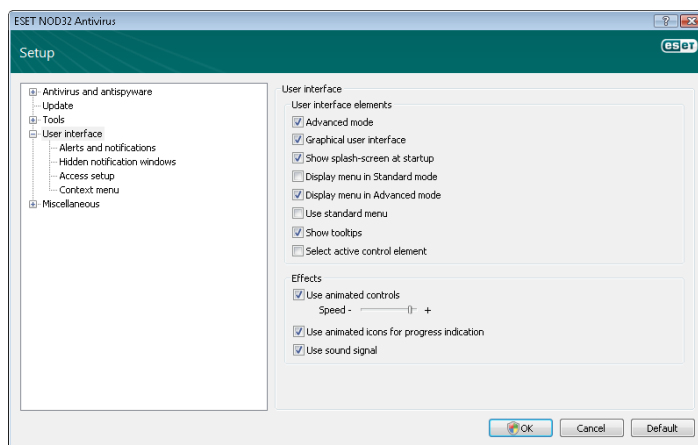
The **User interface** features also include the option to password-protect the ESET NOD32 Antivirus setup parameters. This option is located in the **Settings protection** submenu under **User interface**. In order to provide maximum security for your system, it is essential that the program be correctly configured. Unauthorized modifications could result in the loss of important data. To set a password to protect the setup parameter, click **Set password...**
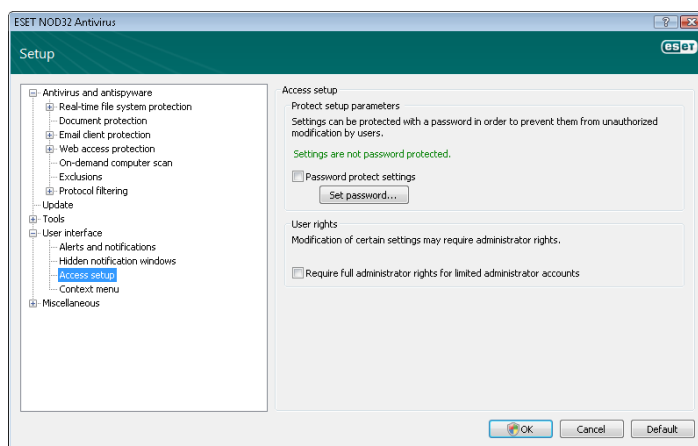
4.6.1   Alerts and notifications

The **Alerts and notifications setup** section under **User interface** allows you to configure how threat alerts and system notifications are handled in ESET NOD32 Antivirus.

The first item is **Display alerts**. Disabling this option 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 to its default setting (enabled).

To close pop-up windows automatically after a certain period of time, select the option **Close messageboxes automatically after (sec.)**. If they are not closed manually, alert windows are automatically closed after the specified time period has expired.

Notifications on the Desktop and balloon tips are informative only,

and do not require or offer user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate displaying Desktop notifications, select the **Display notifications on desktop** option. More detailed options – notification display time and window transparency can be modified by clicking the **Configure notifications…** button.

To preview the behavior of notifications, click the **Preview** button. To configure the duration of the balloon tips display time, see the option **Display balloon tips in taskbar (for sec.)**.
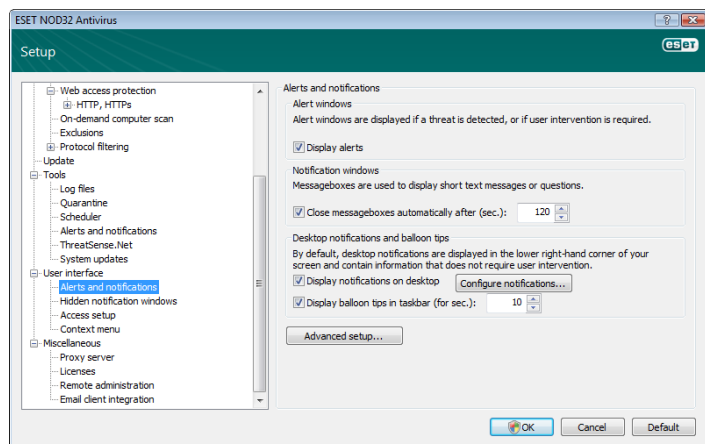
Click **Advanced setup…** to enter additional **Alerts and notification** setup options that include the **Display only notifications requiring user's interaction**. This option allows you to turn on/off displaying of alerts and notifications that require no user interaction. Select **Display only notifications requiring user's interaction when running applications in full screen mode** to suppress all non-interactive notifications. From the **Minimum verbosity of events to display** drop-down menu you can select the starting severity level of alerts and notification to be displayed.

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 the user:** field allows you to define who will receive important notifications from ESET NOD32 Antivirus. 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.

4.7   ThreatSense.Net

The ThreatSense.Net Early Warning System keeps ESET immediately and continuously informed about new infiltrations. The bidirectional ThreatSense.Net Early Warning System has a single purpose – to improve the protection that we can offer you. The best way to ensure that we see new threats as soon as they appear is to "link" to as many to as many of our customers as possible and use them as our Threat Scouts. There are two options:

1. You can decide not to enable the ThreatSense.Net Early Warning System. You will not lose any functionality in the software, and you will still receive the best protection that we offer.

2. You can configure the ThreatSense.Net Early Warning System to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

The ThreatSense.Net Early Warning System 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.

While there is a chance this may occasionally disclose some information about you or your computer (usernames in a directory path, etc.) to ESET's Threat Lab, this information will not be used for ANY purpose other than to help us respond immediately to new threats.

By default, ESET NOD32 Antivirus is configured to ask before submitting suspicious files for detailed analysis to ESET's Threat 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 wants to avoid sending.

The ThreatSense.Net setup is accessible from the Advanced Setup tree, under **Tools > ThreatSense.Net**. Select the **Enable ThreatSense. Net Early Warning System** option to activate and then click the **Advanced setup…** button.
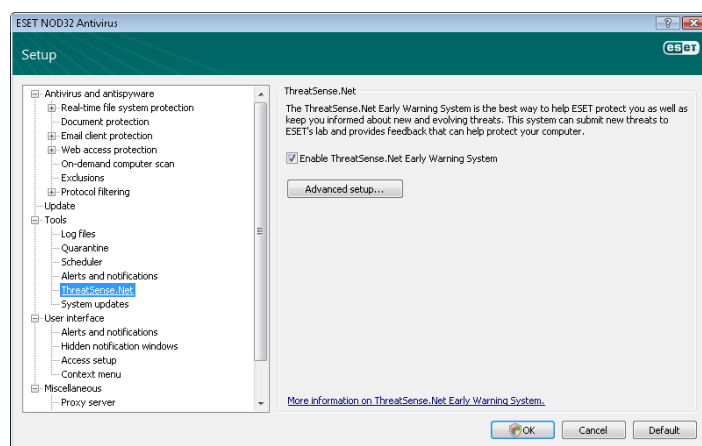
4.7.1   Suspicious files

The **Suspicious files** tab allows you to configure the manner in which threats are submitted to ESET's Threat Lab for analysis.

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

File submission can be set to occur automatically, or select the **Ask before submitting** option if you wish to know which files have been sent for analysis and confirm the submission.
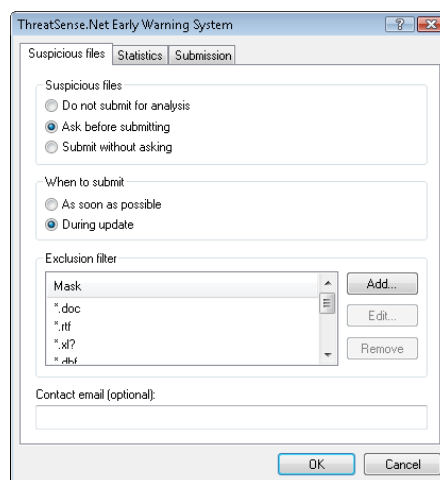
If you do not want any files to be submitted, select the **Do not submit for analysis** option. Selecting not to submit files for analysis does not affect submission of statistical information which is configured in its own setup (see section 4.7.2, "Statistics").

When to submit – By default, the **As soon as possible** option is selected for suspicious files to be sent to ESET's Threat Lab. This is

recommended if a permanent Internet connection is available and suspicious files can be delivered without delay. Select the **During update** option for suspicious files to uploaded to ThreatSense.Net during the next update.

Exclusion filter – The Exclusion filter allows you to exclude certain files/folders from submission. For example, it may be useful to exclude files which may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

Contact email – Your **Contact email [optional]** can sent 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.

4.7.2 Statistics

The ThreatSense.Net Early Warning System collects anonymous information about your computer related to newly detected threats. This information may include the name of the infiltration, the date and time it was detected, the ESET security product version, your operating system version and the location setting. The statistics are typically delivered to ESET's servers once or twice a day.

Below is an example of a statistical package submitted:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

When to submit – You can define when the statistical information will be submitted. If you choose to submit **As soon as possible** statistical information will be sent immediately after it is created. This setting is suitable if a permanent Internet connection is available. If the **During update** option is selected, statistical information will be submitted collectively during the next update.

4.7.3 Submission

You can select how files and statistical information will be submitted to ESET. Select the **By means of Remote Administrator or directly to ESET** option for files and statistics to be submitted 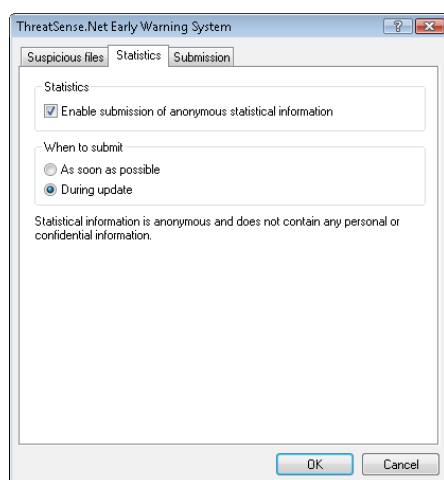by any available means. Select the **By means of Remote Administrator** option to submit files and statistics to the remote administration server, which will ensure their subsequent submission to ESET's Threat Lab. If the option **Directly to ESET** is selected, all suspicious files and statistical information are sent to ESET's virus lab directly from the program.
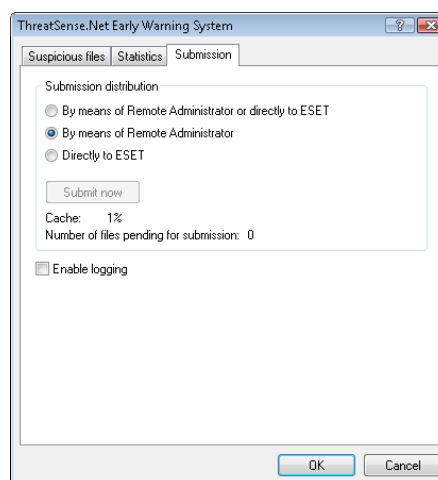
When there are files pending submission, the **Submit now** button will be active. Click this button to immediately submit files and statistical information.

Select the **Enable logging** option to create a log to record file and statistical information submissions.

4.8 Remote administration

ESET Remote Administrator (ERA) is a powerful tool to manage security policy and to obtain an overview of the overall security within a network. It is especially useful when applied to larger networks. ERA not only increases the security level, but also provides ease-of-use in the administration of ESET NOD32 Antivirus on client workstations.

Remote administration setup options are available from the main ESET NOD32 Antivirus program window. Click **Setup > Enter the entire advanced setup tree… > Miscellaneous > Remote administration**.
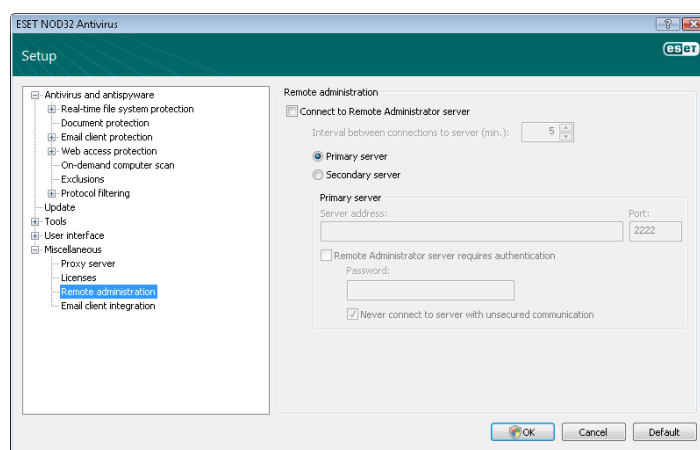
Activate remote administration by selecting the **Connect to Remote Administration server** option. You can then access the other options described below:

- **Server address** – Network address of the server where the ERA Server is installed.

- **Port** – This field contains a predefined server port used for connection. We recommend that you leave the default port setting of 2222

- **Interval between connections to server (min.)** – This designates the frequency that ESET NOD32 Antivirus will connect to the ERA Server. If it is set to 0, information will be submitted every 5 seconds.

• **Remote Administrator requires authentication** – Allows you to enter a password to connect to the ERA Server, if required.

Click **OK** to confirm changes and apply the settings. ESET NOD32 Antivirus will use these settings to connect to the ERA Server.

4.9 Licenses

The **Licenses** branch allows you to manage the license keys for ESET NOD32 Antivirus and other ESET products. After purchase, license keys are delivered along with your username and password. To **Add/Remove** a license key, click the corresponding button in the license manager (**Licenses**) window. The license manager is accessible from the Advanced Setup tree under **Miscellaneous > Licenses.**
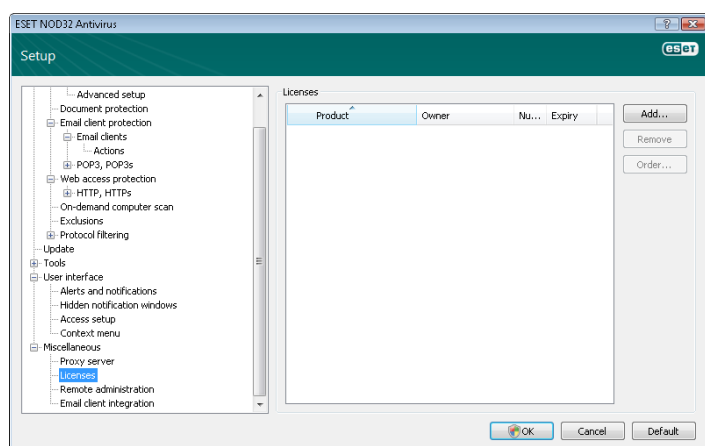
The license key is a text file containing information about the purchased product: the owner, number of licenses, and the expiration date.

The license manager window allows you to upload and view the content of a license key using the **Add**... button – the information contained is displayed in the manager. To delete license files from the list, click **Remove**.

If a license key has expired and you are interested in purchasing a renewal, click the **Order...** button – you will be redirected to our online store.

5. Advanced user

This chapter describes features of ESET NOD32 Antivirus which may be useful for more advanced users. Setup options for these features are accessible only in Advanced mode. To switch to Advanced mode, click **Change…** in the bottom left corner of the main program window or press CTRL + M on your keyboard.

5.1 Proxy server setup

In ESET NOD32 Antivirus, proxy server setup is available in two different sections within the Advanced Setup tree.

First, proxy server settings can be configured under **Miscellaneous > Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET NOD32 Antivirus. Parameters here will be used by all modules requiring connection to the Internet.

To specify proxy server settings for this level, select the **Use proxy server** checkbox and then enter the address of the proxy server into the **Proxy server:** field, along with the **Port** number of the proxy server.
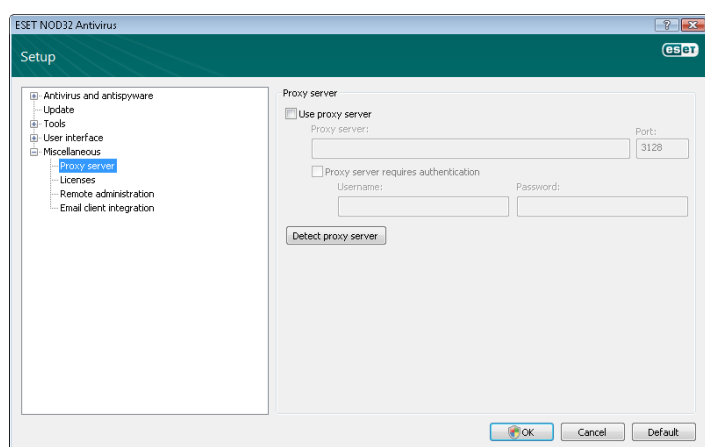
If communication with the proxy server requires authentication, select the **Proxy server requires authentication** checkbox and enter a valid **Username** and **Password** into the respective fields. Click the **Detect proxy server** button to automatically detect and insert proxy server settings. The parameters specified in Internet Explorer will be copied.

NOTE: This feature does not retrieve authentication data (username and password), it must be supplied by you.

Proxy server settings can also be established within Advanced update setup (**Update** branch of the Advanced Setup tree). This setting applies for the given update profile and is recommended for laptops, as they often receive virus signature updates from different locations. For more information about this setting, see Section 4.2, "Updating the program".
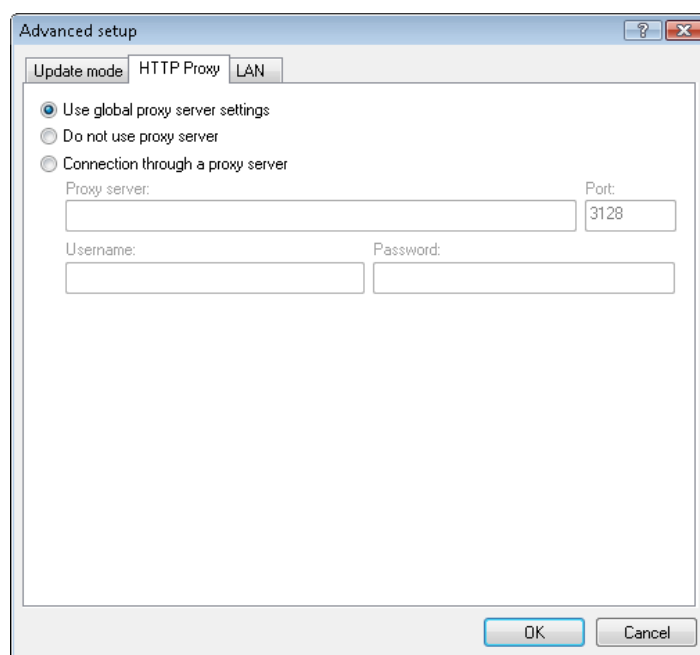
5.2 Export / import settings

Importing and exporting configurations of ESET NOD32 Antivirus is available in Advanced mode under **Setup**.

Both import and export use the .xml file type. Import and export are useful if you need to backup the current configuration of ESET NOD32 Antivirus to be able to use it later. The export settings option is also convenient for users who wish to use their preferred configuration of ESET NOD32 Antivirus on multiple systems - they can easily import an .xml file to transfer the desired settings.
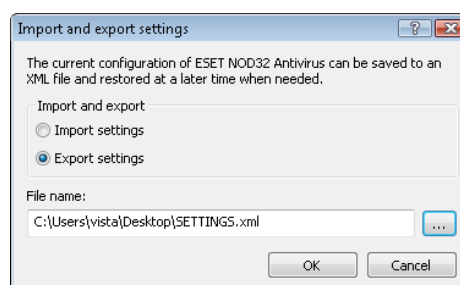
5.2.1 Import settings

Importing a configuration is very easy. From the main menu, click **Setup > Import and export settings**, and then select the **Import settings** option. Enter the name of the configuration file or click the **…** button to browse for the configuration file you wish to import.

5.2.2 Export settings

The steps to export a configuration are very similar. From the main menu, click **Setup > Import and export settings…**. Select the **Export settings** option and enter the name of the configuration file. Use the browser to select a location on your computer to save the configuration file.

5.3 Command Line

ESET NOD32 Antivirus's antivirus module can be launched via the command line – manually (with the "ecls" command) or with a batch ("bat") file.

The following parameters and switches can be used while running the On-demand scanner from the command line:

General options:

–	help	show help and quit
–	version	show version information and quit
–	base-dir = FOLDER	load modules from FOLDER
–	quar-dir = FOLDER	quarantine FOLDER
–	aind	show activity indicator
--	auto	scans all hard drives in the cleaning mode

Targets:

–	files	scan files (default)
–	no-files	do not scan files
–	boots	scan boot sectors (default)
–	no-boots	do not scan boot sectors
–	arch	scan archives (default)
–	no-arch	do not scan archives
–	max-archive-level = LEVEL	maximum archive nesting LEVEL
–	scan-timeout = LIMIT	scan archives for LIMIT seconds at maximum. If the scanning time reaches this limit, the scanning of the archive is stopped and the scan will continue with the next file
–	max-arch-size=SIZE	scan only the first SIZE bytes in archives (default 0 = unlimited)
–	mail	scan email files
–	no-mail	do not scan email files
–	sfx	scan self-extracting archives
–	no-sfx	do not scan self-extracting archives
–	rtp	scan runtime packers
–	no-rtp	do not scan runtime packers
–	exclude = FOLDER	exclude FOLDER from scanning
–	subdir	scan subfolders (default)
–	no-subdir	do not scan subfolders
–	max-subdir-level = LEVEL	maximum subfolder nesting LEVEL (default 0 = unlimited)
–	symlink	follow symbolic links (default)
–	no-symlink	skip symbolic links
–	ext-remove = EXTENSIONS	
–	ext-exclude = EXTENSIONS	exclude EXTENSIONS delimited by colon from scanning

Methods:

–	adware	scan for Adware/Spyware/Riskware
–	no-adware	do not scan for Adware/Spyware/Riskware
–	unsafe	scan for potentially unsafe applications
–	no-unsafe	do not scan for potentially unsafe applications
–	unwanted	scan for potentially unwanted applications
–	no-unwanted	do not scan for potentially unwanted applications
–	pattern	use signatures
–	no-pattern	do not use signatures
–	heur	enable heuristics
–	no-heur	disable heuristics
–	adv-heur	enable advanced heuristics
–	no-adv-heur	disable advanced heuristics

Cleaning:

–	action = ACTION	perform ACTION on infected objects. Available actions: none, clean, prompt
–	quarantine	copy infected files to Quarantine (supplements ACTION)
–	no-quarantine	do not copy infected files to Quarantine

Logs:

–	log-file=FILE	log output to FILE
–	log-rewrite	overwrite output file (default – append)
–	log-all	log also clean files
–	no-log-all	do not log clean files (default)

Possible exit codes of the scan:

0	– no threat found
1	– threat found but not cleaned
10	– some infected files remained
101	– archive error
102	– access error
103	– internal error

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

5.4 ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays system data in a comprehensive way. Information about installed drivers and applications, network connections or important registry entries can help you investigate suspicious system behavior and determine whether it is due to software/hardware incompatibility or malware infection.

You can access SysInspector two ways: From the integrated version in ESET NOD32 Antivirus or by downloading the standalone version (SysInspector.exe) for free from ESET's website. To open SysInspector, activate Advanced mode by pressing CTRL + M and clicking **Tools > SysInspector**. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The downloaded 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 > SysInspector** (for more information see section 5.4.1.4, "SysInspector as part of ESET NOD32 Antivirus 4").

Please allow some time while ESET SysInspector scans your computer. It may take from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

5.4.1 User Interface and application usage

The main window includes four sections – Program Controls on the top, the Navigation window on the left, and the Description window on the right which is directly above the Details window.
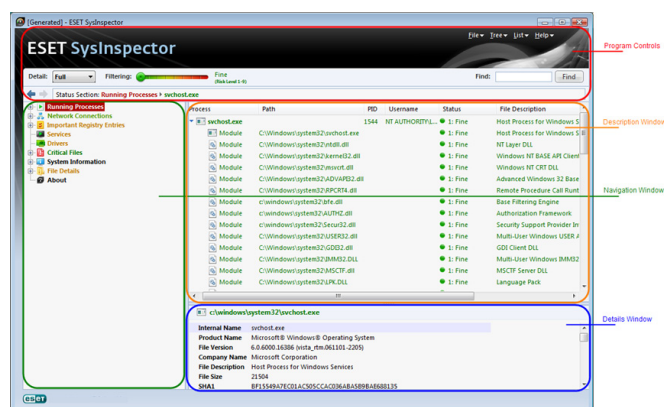
5.4.1.1 Program Controls

This section contains descriptions of all program controls available in ESET SysInspector

File – Click here to store your current report status for later investigation or to open a previously stored report. If you want to publish your report we recommend you choose **Generate > Suitable for sending**. This report format omits sensitive information.

NOTE: You can open previously stored ESET SysInspector reports by dragging-and-dropping them into the main window.

Tree – Allows you to expand or close all nodes.

List – Contains functions for easier navigation within the program as

well as various other functions like finding information online.

NOTE: Items highlighted in red are unknown and are therefore considered 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 the files are truly dangerous or not needed.

Help – Contains information about the application and its functions.

Detail – Influences information displayed in other sections of SysInspector. In Basic mode you have access to information used to find solutions for common problems in your system. In Medium mode the program displays less used details. In Full mode ESET SysInspector displays detailed information needed to solve more complex problems.

Item filtering – The most effective use of Item filtering is 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 to the far left (Risk Level 1) then all items are displayed. By moving the slider to the right, the program filters out items that are less risky than the current Risk Level and only displays items that are more suspicious than the displayed level. With the slider on the far right, the program displays only known harmful items.

All items within the range 6 to 9 can pose a security risk. If you do not have an ESET security solution installed, we recommend you scan your system with the ESET Online scanner after the program has found any high-risk items. ESET Online scanner is a free service and can be found at http://www.eset.com/onlinescan/.

NOTE: The Risk level of an item can be determined quickly by comparing the color of the item with the color on the Risk Level slider.

Search – Search can be used to quickly find a specific item by its name or part of its name. The results of search requests are displayed in the Description window.

Return – By clicking the back or forward arrow you can return to previously displayed information in the Description window.

Status section – Displays the current node in the Navigation window.

5.4.1.2   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 just 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 display in the Details window.

Below are 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 the report was generated. The Description window displays 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, the risk level of the file, etc.

The Details window contains additional information about items selected in the Description window such as the file size or its hash.

NOTE: An operating system is comprised of several important kernel processes which run continually in order to provide basic functions vital to other applications. In certain cases, such processes are displayed in ESET SysInspector as a file path beginning with \??\. These symbols indicate a safe and accurate configuration.

Network connections – The Description window contains a list of processes and applications communicating over the network. The communication protocol used is shown in the Navigation window (TCP or UDP) along with the remote address to which the application is connecting. You can also check DNS assigned IP addresses.

The Details window contains additional information about items selected in the Description window such as the file size or its hash.

Important Registry Entries – Contains a list of selected registry entries often related to various problems with your system such as 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 about the file in the Details window.

Drivers – The list of drivers installed on the system.

Critical files – The Description window displays content of critical files related to the Microsoft Windows®operating system.

System information – Contains detailed information about hardware and software along with information about set environmental variables and user rights.

File details – A list of important system files and files in the Program Files folder. Additional information specific to the files can be found in the Description and Details windows.

About – Information about ESET SysInspector

5.4.1.3   Compare

The Compare feature allows you to compare two existing SysInspector logs in order to highlight common to both logs. This feature is useful if you want to keep track of changes to the system and may allow you to detect the activity of malicious code.

After launching, ESET SysInspector creates a new log, which is displayed in a new window. Navigate to **File > Save Log** to save a log to a file. Log files can later be opened and viewed. To open an existing log, click **File > Open Log**. In the main program window, ESET SysInspector always displays one log at a time.

If you are comparing two logs, it's important to compare a currently active log to a log saved in a file. To compare logs, use the option **File > Compare Log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The resulting, so called comparative log will display only differences between those two logs.

NOTE: If you compare two log files, select **File > Save Log**, and save it as a .zip file, both files are saved. If you later open this file, the contained logs are automatically compared.

Next to the displayed items, SysInspector shows symbols identifying differences between the compared logs. Items marked by a ━ can only be found in the active log and were not present in the opened comparative log. Items marked by a ➕ on the other hand, were present only in the opened log and are missing in the active one.

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 only

□ 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 bottom left 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.

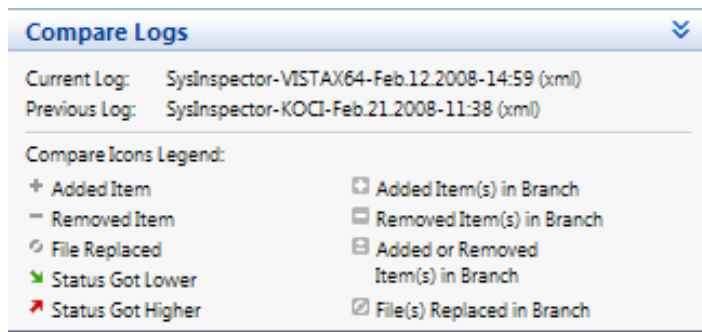**Example:** – Generate and save a log, recording original information about the system, to a file named previous.xml. After changes to the system have been made, open SysInspector and let it generate a new log. Save it to a file named current.xml.

In order to track changes between those two logs, click **File > Compare Log**. 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

5.4.1.4 SysInspector as a part of ESET NOD32 Antivirus 4

To open SysInspector in ESET NOD32 Antivirus, click **Tools > SysInspector**. The management system in the 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 SysInspector window contains basic information about the created snapshots such as create time, short comment, name of the user that created the snapshot and snapshot status.

To **Compare, Add...** or **Remove** snapshots, use the corresponding buttons located below the list of snapshots in the SysInspector window. Those options are also available from the context menu.

To view the selected system snapshot, use the **View** context menu option. To export the selected snapshot to a file, right-click it and select **Export…**. A detailed description of the available options is shown below:

Compare - Allows you to compare two existing logs. This feature is useful 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.

Add – Creates a new record. Before that you must enter a short comment about the record. To see the snapshot creation progress (of the currently generated snapshot) in percent, see the Status column.

All completed snapshots are marked by the Created status.

Remove – Removes entries from the list

Show – Displays the selected snapshot. Alternatively, you can double-click the selected entry.

Export… – Saves the selected entry in an .xml file (as well as a .zip version)

5.4.1.5 Service script

Service script is a tool that directly influences the operating system and installed applications, allowing users to execute scripts that remove problematic components in the system, including viruses, remnants of viruses, blocked files, virus records in the registry, etc. The script is stored in a text file generated from a pre-existing .xml file. The data in the .txt script file is ordered simply and legibly, for ease of use. The script will initially exhibit neutral behavior. In other words, it will not have any impact on the system while in its original form. The user needs to edit the script for it to have any effect.

Warning:
This tool is intended for advanced users only. Incorrect use may result in damage to programs or the operating system.

5.4.1.5.1 Generating Service scripts

To generate a script, right-click any item from the menu tree (in the left pane) in the SysInspector main window. From the context menu, select either the **Export All Sections To Service Script** option or the **Export Selected Sections To Service Script** option.

5.4.1.5.2 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 dependant 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 unregistered from the system and removed.

09) Critical files

This section contains information about files 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.

5.4.1.5.3   How to execute Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the 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 successful execution of the script.

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.

Your script was not recognized as valid and will not be run if you see the following message: **Are there any issues with the script consistency (damaged heading, corrupt 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.

5.5   ESET SysRescue

ESET SysRescue (ESR) is a utility which enables you to create a bootable disk containing ESET NOD32 Antivirus 4 (EAV). The main advantage of ESET Recovery CD is that EAV runs independent of the host operating system, while it has direct access to the disk and the entire file system. This makes it possible to remove those infiltrations that normally could not be deleted, e.g., when the operating system is running, etc.

5.5.1   Minimum requirements

ESET SysRescue (ESR) works in the Microsoft Windows Preinstallation Environment (Windows PE) version 2.x, which is based on Windows Vista. Windows PE is a part of the free package Windows Automated Installation Kit (Windows AIK), and therefore Windows AIK must be installed before creating ESR. Due to the support of the 32-bit version of Windows PE, ESR can be created in the 32-bit version of EAV only. ESR supports Windows AIK 1.1 and later. ESR is available in EAV 4.0 and later.

5.5.2   How to create a rescue CD

If the minimum requirements for the creation of ESET SysRescue (ESR) CD are met, it is quite an easy task to accomplish. To launch the ESR wizard, click **Start > Programs > ESET > ESET NOD32 Antivirus > ESET SysRescue**.

First, the wizard checks for the presence of Windows AIK and a suitable device for the boot media creation.

In the next step select the target media where ESR will be located. In addition to CD/DVD/USB you can choose to save ESR in an .iso file. Later, you can burn the .iso image on CD/DVD, or use it in other ways (e.g., in a virtual environment such as VmWare or Virtualbox).

After you have specified all parameters, you will see a compilation preview in the last step of ESET SysRescue wizard. Check the parameters and start the compilation. The available options include:

Folders
ESET Antivirus
Advanced
Bootable USB device
Burning

5.5.2.1   Folders

Temporary folder – Working directory for files required during ESET SysRescue compilation.

ISO folder – Folder where the resulting .iso file is saved after the compilation is completed.

The list on this tab shows all local and mapped network drives together with the available free space. If any of the folders here are located on a drive with insufficient free space, we recommend that you select another drive with more free space available. Otherwise compilation may exit prematurely due to insufficient free disk space.

External applications – Allows you to specify additional programs that will be run or installed after booting from a SysRescue medium.

Include external applications – Allows you to add external programs to the SysRescue compilation

Selected folder – Folder in which programs to be added to the SysRescue disk are located

5.5.2.2   ESET Antivirus

To create an ESET SysRescue CD, you can select two sources of ESET files to be used by the compiler.

EAV folder – Files already contained in the folder to which the ESET product is installed on your computer

MSI file – Files contained in the .msi installer are used

Profile – You can use one of the following two sources of username and password:

Installed EAV – Username and password are copied from the currently installed ESET security product

From user – Username and password entered in the corresponding text boxes below are used

NOTE: The ESET security product on the ESET SysRescue CD is updated either from the Internet or from the computer running the ESET SysRescue CD.

5.5.2.3   Advanced

The **Advanced** tab lets you optimize ESET SysRescue CD according to your computer's memory capacity. Select **512 MB and more** to write the content of the CD to the operating memory (RAM). If you select **less than 512 MB**, the recovery CD will be permanently accessed when WinPE is running.

External drivers – This section explains how to add drivers for your specific hardware (e.g., network adapter). Although WinPE is based on Windows Vista SP1, which supports a large range of hardware, occasionally hardware is not recognized. This will required that you add a driver manually.

There are two ways of introducing a driver into an ESET SysRescue compilation - manually (the **Add** button) and automatically (the **Aut. Search** button). If you manually add a driver, you need to select the path to the corresponding .inf file (applicable *.sys file must also be present in this folder). Using the **Aut. Search** button automatically locates the driver in the operating system of the given computer. We recommend you use this option only if the original computer on which the SysRescue disc was created and the computer you are restoring to use the same network adapter. During creation, the ESET SysRescue the driver is introduced into the compilation so you do not need to look for it later.

5.5.2.4   Bootable USB device

If you have selected USB device as your target medium, you can select one of the available USB media on the Bootable USB device tab (in case there are more USB devices).

Warning: **The** selected USB device will be formatted during ESET SysRescue creation. All data on the device will be deleted.

5.5.2.5   Burn

If you have selected CD/DVD as your target medium, you can specify additional burning parameters on the **Burn** tab.

Delete ISO file – Select this option to delete .iso files after the ESET Rescue CD is created.

Deletion enabled – Allows you to select fast erasing and complete erasing.

Burning device – Select the drive to be used for burning.

Warning: This is the default option. If a rewritable CD/DVD is used, all data on the CD/DVD will be erased.

The Medium section contains information about the current medium inserted in your CD/DVD device.

Burning speed – Select the desired speed from the drop-down menu. The capabilities of your burning device and the type of CD/DVD used should be considered when selecting the burning speed.

5.5.3   Working with ESET SysRescue

For the rescue CD/DVD/USB to work effectively, you must start your computer from the ESET SysRescue boot media. Boot priority can be modified in the BIOS. Alternatively, you can invoke the boot menu during computer startup - usually using one of the F9 - F12 keys depending on the version of your motherboard/BIOS.

After booting up, EAV will start. Since ESET SysRescue is used only in specific situations, some protection modules and program features present in the standard version of EAV are not needed; their list is narrowed down to Computer scan, Update, and some sections in Setup. The ability to update the virus signature database is the most important feature of ESET SysRescue, we recommend that you update the program prior starting a Computer scan.

5.5.3.1   Using ESET SysRescue

Suppose that computers in the network have been infected by a virus which modifies executable (.exe) files. EAV is capable of cleaning all infected files except for explorer.exe, which cannot be cleaned, even in Safe mode.

This is because explorer.exe, as one of the essential Windows processes, is launched in Safe mode as well. EAV would not be able to perform any action with the file and it would remain infected.

In this type of scenario, you could use ESET SysRescue to solve the problem. ESET SysRescue does not require any component of the host operating system and is therefore capable of processing (cleaning, deleting) any file on the disk.

6. Glossary

6.1 Types of infiltrations

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

6.1.1 Viruses

A computer virus is an infiltration that corrupts existing files on your computer. Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.

Computer viruses mainly attack executable files and documents. To replicate, a virus attaches its "body" to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its predefined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program by him/herself.

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.

It is important to note that viruses (when compared to trojans or spyware) are increasingly rare because they are not commercially enticing for malicious software authors. Additionally, the term "virus" is often used incorrectly to cover all types of infiltrations. This usage is gradually being overcome and replaced by the new, more accurate term "malware" (malicious software).

If your computer is infected with a virus, it is necessary to restore infected files to their original state – i.e., to clean them by using an antivirus program.

Examples of viruses are: OneHalf, Tenga, and Yankee Doodle.

6.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves – they are not dependent on host files (or boot sectors). Worms spread through 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 of their release – in some cases, even in minutes. 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.

Examples of well-known worms are: Lovsan/Blaster, Stration/Warezov, Bagle, and Netsky.

6.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations which attempt to present themselves as useful programs, thus tricking users into letting them run. But it is important to note that this was true for trojan horses in the past–today, there is no longer a need for them to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. "Trojan horse" has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories:

Downloader – A malicious program with the ability to download other infiltrations from the Internet.

Dropper – A type of trojan horse designed to drop other types of malware onto compromised computers.

Backdoor – An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it.

Keylogger – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers.

Dialer – Dialers are programs designed to connect to premium-rate numbers. 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.

Trojan horses usually take the form of executable files with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

Examples of well-known trojans are: NetBus, Trojandownloader.Small.ZL, Slapper

6.1.4 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 NOD32 Antivirus users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

6.1.5 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.

6.1.6   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.

6.1.7   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 NOD32 Antivirus 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.

6.1.8   Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

•   New windows you haven't seen previously are opened

•   Activation and running of hidden processes

•   Increased usage of system resources

•   Changes in search results

•   Application communicates with remote servers