ESET Mail Security

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

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

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

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

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

REV. 11/27/2023

Preface

This guide is intended to help you make the best use of ESET Mail Security. To learn more about any window in the program, press **F1** on your keyboard with the given window open. The help page related to the window you are currently viewing will be displayed.

For consistency and to help prevent confusion, terminology used throughout this guide is based on the ESET Mail Security parameter names. We also used a uniform set of symbols to highlight topics of particular interest or significance.

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

IMPORTANT
This requires your attention and is not recommended to skip over it. Important notes include significant but non-critical information.

WARNING
Critical information you should treat with increased caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Please read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.

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

If you see the following element in the upper-right corner of a help page, it indicates a navigation within the windows of a graphical user interface (GUI) of ESET Mail Security. Use these directions to get to the window that is being described on the respective help page.

Open ESET Mail Security
Click Setup > Server > OneDrive Scan setup > Register

Formatting conventions:

Convention	Meaning
Bold type	Section headings, feature names or user interface items, such as buttons.
Italic type	Placeholders for the information that you provide. For example, file name or path means you type the actual path or a name of file.

Convention	Meaning
`Courier New`	Code samples or commands.
Hyperlink	Provides quick and easy access to cross-referenced topics or external web locations. Hyperlinks are highlighted in blue and may be underlined.
%ProgramFiles%	The Windows system directory which stores installed programs of Windows and others.

ESET Mail Security online help pages are divided into several chapters and sub-chapters. You can find relevant information by browsing the contents of the help pages. Alternatively, you can use full-text search by typing words or phrases.

Overview

ESET Mail Security 7 for Microsoft Exchange Server is an integrated solution that protects mail servers and user's mailboxes from various types of malicious content including email attachments infected by worms or trojans, documents containing harmful scripts, phishing schemes and spam. ESET Mail Security provides four types of protection: Antivirus, Antispam, Anti-Phishing and Rules. ESET Mail Security filters malicious content in Mailbox databases as well as on Mail transport layer before it arrives in the recipient's mailbox.

ESET Mail Security supports Microsoft Exchange Server versions 2007 and later, as well as Microsoft Exchange Server in a cluster environment. Specific Exchange Server roles (mailbox, hub, edge) are also supported.

While providing Microsoft Exchange Server protection, ESET Mail Security also includes functionality to ensure the protection of the server itself (real-time file system protection, network protection, web-access protection and email client protection).

You can remotely manage ESET Mail Security in larger networks with the help of ESET Security Management Center. Also, ESET Mail Security enables you to use it with third-party Remote monitoring and management (RMM) tools.

Key Features

The following table provides a list of features that are available in the ESET Mail Security.

True 64-bit product core	Adding higher performance and stability to the product core components.
Anti-Malware	An award-winning and innovative defense against malware. This leading-edge technology prevents from attacks and eliminates all types of threats, including viruses, ransomware, rootkits, worms and spyware with cloud-powered scanning for even better detection rates. With a small footprint, it is light on the system resources not compromising its performance. It uses layered security model. Each layer, or a phase, has a number of core technologies. *Pre-execution* phase has technologies such as *UEFI Scanner, Network Attack Protection, Reputation & Cache, In-product Sandbox, DNA Detections. Execution* phase technologies are *Exploit Blocker, Ransomware Shield, Advanced Memory Scanner* and *Script Scanner (AMSI)*, and *Post-execution* phase uses *Botnet Protection, Cloud Malware Protection System* and *Sandboxing*. This feature-rich set of core technologies provides an unrivaled level of protection.

Antispam	Antispam is an essential component for any mail server. ESET Mail Security uses state-of-the-art Antispam engine that prevents from spam and phishing attempts with very high catch rates. ESET Mail Security has won consecutively spam filtering test by Virus Bulletin, a leading security testing authority, and received the VBSpam+ certification for a number years. Antispam engine have achieved a result of 99.99% spam catch rate with zero false positives making it industry-leading technology in spam protection. ESET Mail Security Antispam incorporates multiple technologies (RBL and DNSBL, Fingerprinting, Reputation checking, Content analysis, Rules, manual whitelisting/blacklisting, Backscatter protection and message validation using SPF and DKIM) to maximize detection. ESET Mail Security Antispam is cloud based and most of the cloud databases are located in ESET data centers. Antispam cloud services allow for prompt data updates which provides quicker reaction time in case of an emergence of new spam.
Anti-Phishing protection	A feature which prevents users from accessing web pages known for phishing. Email messages may contain links which lead to phishing web pages and ESET Mail Security uses sophisticated parser that searches message body and subject of incoming email messages to identify such links (URL's). The links are compared against phishing database.
Rules	The rules enables administrators to filter unwanted emails and attachments based on company's policy. Attachments such as executables, multimedia files, password protected archives, etc. Different actions can be performed with filtered email messages and their attachments, for example quarantine, delete, send notification or log to events.
Export to syslog server (Arcsight)	Allows for the contents of Mail server protection log to be duplicated to syslog server in Common Event Format (CEF) for use with log management solutions such as Micro Focus ArcSight. Events can be fed via SmartConnector to ArcSight, or exported to files. This provides for a convenient way of centralized monitoring and management of security events. You can benefit from this feature especially if you have a complex infrastructure with a large number of Microsoft Exchange Servers with ESET Mail Security solution.
Office 365 mailbox scan	For businesses who use hybrid Exchange environment, adds the capability to scan mailboxes in the cloud.
ESET Dynamic Threat Defense (EDTD)	ESET Cloud-based service. When ESET Mail Security evaluates an email message as suspicious, it is temporarily put it into the ESET Dynamic Threat Defense quarantine. A suspicious email message is automatically submitted to ESET Dynamic Threat Defense server for analysis by advanced malware detection engines. ESET Mail Security then receives a result of the analysis and suspicious email message is dealt with depending on the result.
Mail quarantine manager with web interface	Administrator can inspect quarantined objects and decide to delete or release them. This feature offers easy to use management tool. Quarantine web interface allows remote management of the content. It is possible to choose its administrators and/or delegate access. Additionally, users can view and manage their own spam after logging to the Mail Quarantine Web interface, having access to their messages only.
Mail quarantine reports	Quarantine reports are emails sent to selected users or administrators to provide information about all quarantined email messages. It also enables them to remotely manage quarantined content.
On-demand mailbox database scan	On-demand mailbox database scan gives administrators an option to scan selected mailboxes manually, or schedule the scan out of business hours. Mailbox database scanner uses the EWS (Exchange Web Services) API to connect to Microsoft Exchange Server via HTTP/HTTPS. Also, the scanner uses parallelism during scan process to improve the performance.
ESET Cluster	ESET Cluster allows for management of multiple servers from a single location. Similar to ESET File Security for Microsoft Windows Server, joining server nodes to a cluster makes management easier due to the ability to distribute one configuration across all cluster member nodes. ESET Cluster can also be used to synchronize greylisting databases and contents of the Local mail quarantine.

Processes exclusions	Excludes specific processes from Anti-Malware on-access scanning. Anti-Malware on-access scanning may cause conflicts in certain situations, for example during a backup process or live migrations of virtual machines. Processes exclusions help minimize the risk of such potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the whole system. The exclusion of a process / application is an exclusion of its executable file (*.exe*).
eShell (ESET Shell)	eShell 2.0 is now available in ESET Mail Security. eShell is a command line interface that offers advanced users and administrators more comprehensive options to manage ESET server products.
ESET Security Management Center	Better integration with ESET Security Management Center including the ability to schedule various tasks. For more information, see ESET Security Management Center Online help.
Component-based installation	Installation can be customized to contain only selected parts of the product.

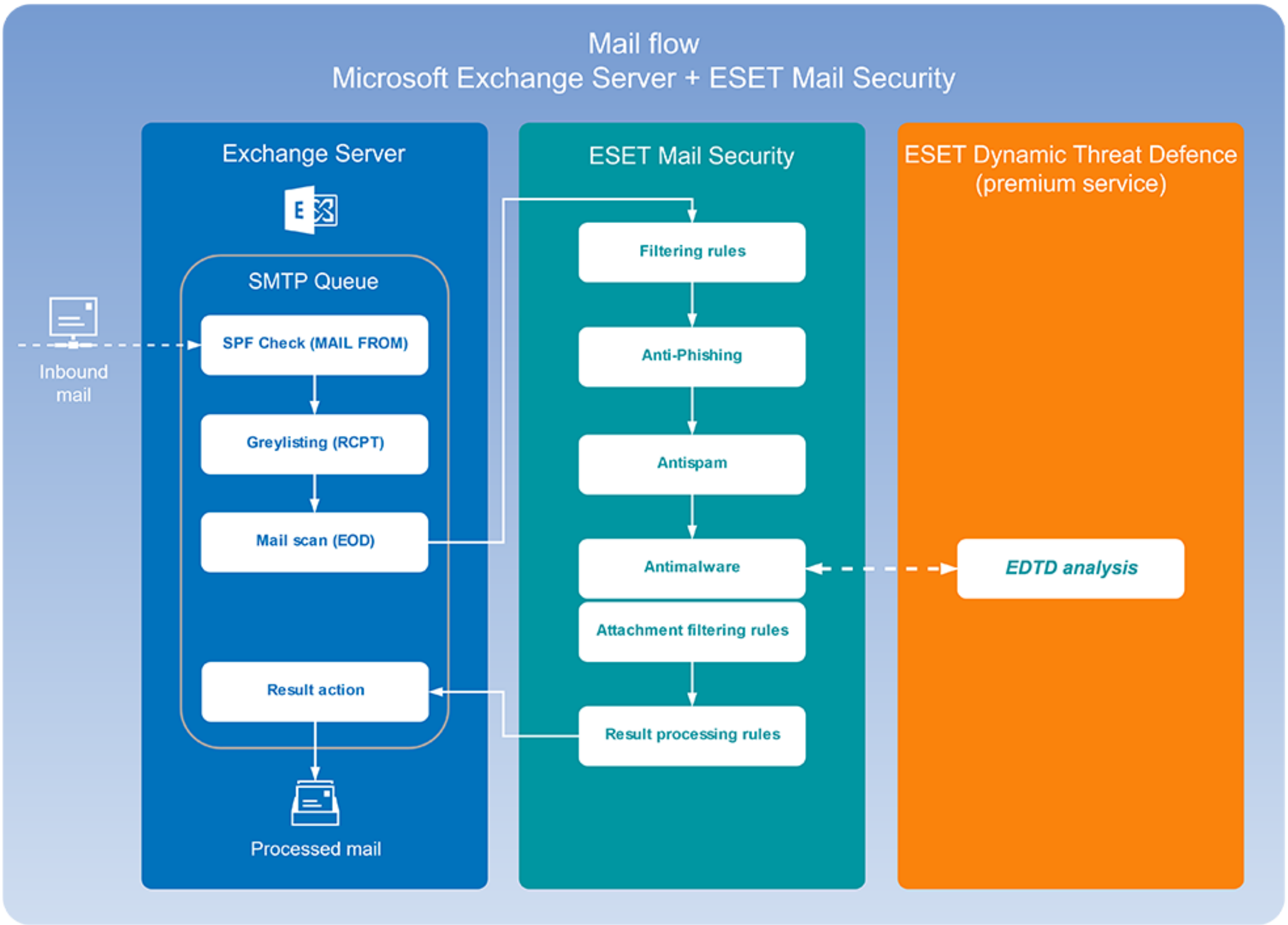
What's new

New features and enhancements in ESET Mail Security compared to the previous generation (version 6.x):

- True 64-bit product core
- Office 365 mailbox scan
- Anti-Phishing mail protection
- Backscatter protection
- Enhanced rules (new conditions and actions were added, for example Message body condition)
- Improved quarantining of email attachments
- Mail quarantine administrator reports
- Synchronization of Local mail quaratine over ESET Cluster
- SMTP protection log
- ESET Dynamic Threat Defense
- ESET Enterprise Inspector support
- ESET RMM
- Export to syslog server (Arcsight)
- Network isolation
- Machine learning protection

Mail flow

The following diagram shows mail flow within Microsoft Exchange Server and ESET Mail Security. For details about using ESET Dynamic Threat Defense (EDTD) with ESET Mail Security, see EDTD help pages.



ESET Mail Security features and Exchange Server Roles

The following table lets you identify what features are available for each supported version of Microsoft Exchange Server and their roles. ESET Mail Security installation wizard checks your environment during the installation and once installed, ESET Mail Security will display its features according to detected version of your Exchange Server and its roles.

Exchange Server version and server role	Antispam protection	Anti-Phishing protection	Rules	Mail transport protection	On-demand mailbox database scan	Mailbox database protection
Microsoft Exchange Server 2007 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2007 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2007 (Hub)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2007 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2010 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2010 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰

Exchange Server version and server role	Antispam protection	Anti-Phishing protection	Rules	Mail transport protection	On-demand mailbox database scan	Mailbox database protection
Microsoft Exchange Server 2010 (Hub)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2010 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2016 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2016 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2019 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2019 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Windows Small Business Server 2011 SP1	⍰	⍰	⍰	⍰	⍰	⍰

Exchange server roles

Edge role vs Hub role

Both Edge Transport and Hub Transport Servers have Antispam features disabled by default. This is the desired configuration in an Exchange organization with an Edge Transport server. We recommend that you have the Edge Transport server running ESET Mail Security Antispam configured to filter messages before they are routed into the Exchange organization.

The Edge role is the preferred location for Antispam scanning because it allows ESET Mail Security to reject spam early in the process without putting an unnecessary load on network layers. Using this configuration, incoming messages are filtered by ESET Mail Security on the Edge Transport server, so they can safely be moved to the Hub Transport server without the need for further filtering.

If your organization does not use an Edge Transport server and only has a Hub Transport server, we recommend that you enable Antispam features on the Hub Transport server that receives inbound messages from the Internet via SMTP.

NOTE
Due to the technical restrictions of Microsoft Exchange Server 2007 and newer, ESET Mail Security does not support Microsoft Exchange Server deployment with the CAS role only (standalone Client Access Server).

POP3 Connector and Antispam

Microsoft Windows Small Business Server (SBS) versions contain a native built-in POP3 Connector that enables the server to fetch email messages from external POP3 servers. Implementation of this Microsoft native POP3 Connector differs from one SBS version to another.

ESET Mail Security does support Microsoft SBS POP3 Connector, provided it is configured correctly. Messages downloaded via the Microsoft POP3 Connector are scanned for the presence of spam. Antispam protection for these messages is possible because the POP3 Connector forwards email messages from a POP3 account to Microsoft Exchange Server via SMTP.

ESET Mail Security has been tested with popular mail services such as Gmail.com, Outlook.com, Yahoo.com, Yandex.com and gmx.de on the following SBS system:

- Microsoft Windows Small Business Server 2011 SP1

IMPORTANT
If you are using a built-in Microsoft SBS POP3 Connector and have all email messages scanned for spam, press the **F5** key to access **Advanced setup**, navigate to **Server** > **Mail transport protection** > Advanced settings and for **Scan also messages received from authenticated or internal connections** setting choose **Antivirus, anti-phishing and antispam protection** from the drop-down list. This ensures Antispam protection for emails fetched from POP3 account(s).

You can also use a third party POP3 connector such as P3SS (instead of the built-in Microsoft SBS POP3 Connector).

Protection modules

The core functionality of ESET Mail Security include the following protection modules:

⊟ Antivirus

Antivirus protection is one of the basic functions of ESET Mail Security . 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 blocking it and then cleaning it, deleting it, or moving it to Quarantine.

⊟ Antispam

Antispam protection incorporates multiple technologies (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Rules, Manual whitelisting/blacklisting, etc.) to maximize detection of email threats.

ESET Mail Security Antispam is cloud based and most of the cloud databases are located in ESET data centers. Antispam cloud services allow for prompt data updates which provides quicker reaction time in case of an emergence of new spam. It also allows incorrect or false data to be removed from ESET blacklists. Communication with Antispam cloud services is done over a proprietary protocol on port 53535, whenever possible. If it is not possible to communicate through ESET's protocol, DNS services are used instead (port 53). However, using DNS is not as effective because it requires multiple requests to be sent during spam classification process of a single email message.

NOTE
We recommend you to open TCP/UDP port 53535 for the IP addresses listed in this KB article. This port is used by ESET Mail Security to send requests.

Normally, no email messages or their parts are sent during spam classification process. However, if ESET LiveGrid® is enabled and you have explicitly allowed samples to be submitted for analysis, only message marked as spam (or most likely spam) may be sent in order to help thorough analysis and cloud database enhancement.

If you want to report spam false positive or negative classification, see our KB article for details.

In addition, ESET Mail Security can also use Greylisting method (disabled by default) of spam filtering.

⊟ Anti-Phishing

ESET Mail Security includes Anti-Phishing protection which prevents users from accessing web pages known for phishing. In case of email messages that may contain links which lead to phishing web pages, ESET Mail Security uses sophisticated parser that searches message body and subject of incoming email messages to identify such links (URL's). The links are compared against phishing database and rules with condition Message body are evaluated.

⊟ Rules

The availability of rules for Mailbox database protection, On-demand mailbox database scan and Mail transport protection on your system depend on which Microsoft Exchange Server version is installed on the server with ESET Mail Security.

Rules enables you to manually define email filtering conditions and actions to take with filtered emails. There are different sets of conditions and actions. You can create individual rules that may also be combined. If one rule uses multiple conditions, the conditions will be linked using the logical operator **AND**. Consequently, the rule will be executed only if all its conditions are met. If multiple rules are created, the logical operator **OR** will be applied, meaning the program will run the first rule for which the conditions are met.

In the scanning sequence, the first technique used is greylisting - if it is enabled. Consequent procedures will always execute the following techniques: protection based on user-defined rules, followed by an Antivirus scan and, lastly, an Antispam scan.

Multilayered security

ESET Mail Security provides complex protection on different levels:

- Mailbox database protection
- Mail transport protection
- On-demand mailbox database scan
- Office 365 mailbox scan

NOTE
For comprehensive view, see matrix of ESET Mail Security features and Microsoft Exchange Server versions and their roles.

Mailbox database protection

The mailbox scanning process is triggered and controlled by the Microsoft Exchange Server. Emails in the Microsoft Exchange Server store database are scanned continuously. Depending on the version of Microsoft Exchange Server, the VSAPI interface version and the user-defined settings, the scanning process can be triggered in any of the following situations:

- When the user accesses email, for example, in an email client (email is always scanned with the latest detection engine).
- In the background, when use of the Microsoft Exchange Server is low.
- Proactively (based on the Microsoft Exchange Server's inner algorithm).

> NOTE
> Mailbox database protection is not available for Microsoft Exchange Server 2013, 2016 and 2019.

Mailbox database protection is available for the following systems:

Exchange Server version and server role	Antispam protection	Anti-Phishing protection	Rules	Mail transport protection	On-demand mailbox database scan	Mailbox database protection
Microsoft Exchange Server 2007 (Mailbox)	?	?	?	?	?	?
Microsoft Exchange Server 2007 (multiple roles)	?	?	?	?	?	?
Microsoft Exchange Server 2010 (Mailbox)	?	?	?	?	?	?
Microsoft Exchange Server 2010 (multiple roles)	?	?	?	?	?	?
Windows Small Business Server 2011 SP1	?	?	?	?	?	?

This type of scanning can be performed on a single server installation with multiple Exchange Server roles on one computer (as long as it includes the Mailbox or Back-End role).

Mail transport protection

SMTP server-level filtering is secured by a specialized plugin. In Microsoft Exchange Server 2007 and 2010, the plugin is registered as a transport agent on the Edge or the Hub roles of the Microsoft Exchange Server.

SMTP server-level filtering by a transport agent provides protection in the form of Antivirus, Antispam and user-defined rules. As opposed to VSAPI filtering, SMTP server-level filtering is performed before the scanned email arrives in the Microsoft Exchange Server mailbox.

Formerly known as Message filtering on the SMTP server level. This protection is provided by the transport agent and is only available for Microsoft Exchange Server 2007 or newer operating in the Edge Transport Server or Hub Transport Server role. This type of scanning can be performed on a single server installation with multiple Exchange Server roles on one computer (as long as it has one of mentioned server roles).

Mail transport protection is available for the following systems:

Exchange Server version and server role	Antispam protection	Anti-Phishing protection	Rules	Mail transport protection	On-demand mailbox database scan	Mailbox database protection
Microsoft Exchange Server 2007 (Hub)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2007 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2010 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2016 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2016 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2019 (Edge)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2019 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Windows Small Business Server 2011	⍰	⍰	⍰	⍰	⍰	⍰

On-demand mailbox database scan

Allows you to execute or schedule an Exchange mailbox database scan. This feature is only available for Microsoft Exchange Server 2007 or newer operating in the Mailbox server or Hub Transport role. This also applies to a single server installation with multiple Exchange Server roles on one computer (as long as it has one of mentioned server roles).

On-demand mailbox database scan is available for the following systems:

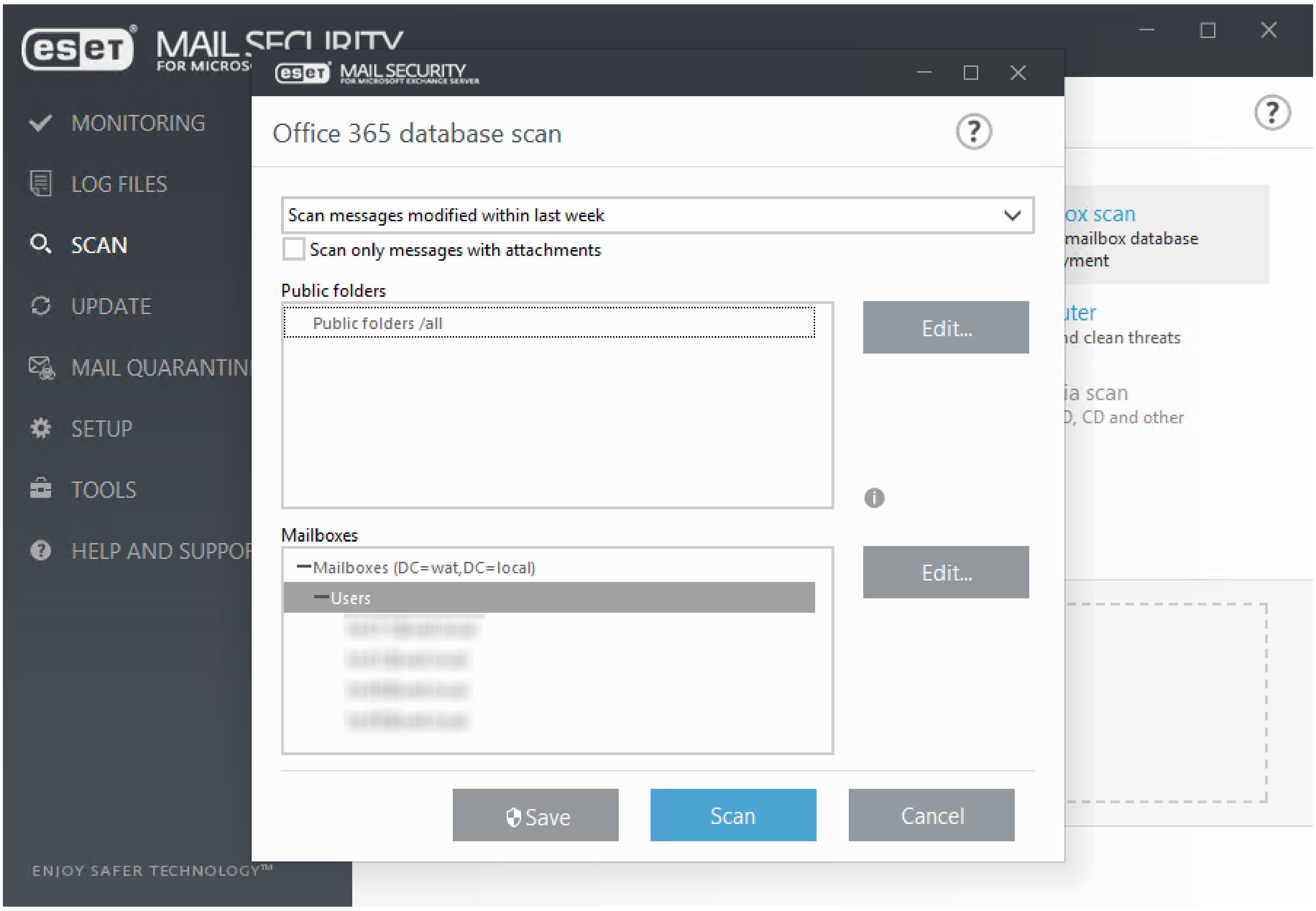
Exchange Server version and server role	Antispam protection	Anti-Phishing protection	Rules	Mail transport protection	On-demand mailbox database scan	Mailbox database protection
Microsoft Exchange Server 2007 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2007 (Hub)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2007 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2010 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2010 (Hub)	⍰	⍰	⍰	⍰	⍰	⍰

Exchange Server version and server role	Antispam protection	Anti-Phishing protection	Rules	Mail transport protection	On-demand mailbox database scan	Mailbox database protection
Microsoft Exchange Server 2010 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (multiple roles)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2013 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2016 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Microsoft Exchange Server 2019 (Mailbox)	⍰	⍰	⍰	⍰	⍰	⍰
Windows Small Business Server 2011 SP1	⍰	⍰	⍰	⍰	⍰	⍰

Office 365 mailbox scan

ESET Mail Security provides scanning functionality for Office 365 hybrid environments. It is available and visible in ESET Mail Security only if you have hybrid Exchange environment (on-premise and cloud). Both routing scenarios are supported, through **Exchange Online** or through **on-premises** organization. For more details see Transport routing in Exchange hybrid deployments.

You can scan Office 365 remote mailboxes and Public folders the same way you would with traditional On-demand mailbox database scan.



Office 365 database scan

Scan messages modified within last week

☐ Scan only messages with attachments

Public folders

Public folders /all

Mailboxes

Mailboxes (DC=wat,DC=local)

Users

Running a full email database scan in a large environments can result in undesired system loads. To avoid this issue, run a scan on specific databases or mailboxes. To further minimize system impact, use the time filter at the top of the window. For example, instead of using **Scan all messages**, you can select **Scan messages modified within last week**.

We recommend you to configure Office 365 account. Press **F5** key and navigate to **Server** > **On-demand mailbox database scan**. Also, see Database scan account details.

To see the activity of Office 365 mailbox scan, check **Log files** > **Mailbox database scan**.

System requirements

Supported Operating Systems:

- Microsoft Windows Server 2019 (Server Core and Desktop Experience)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 with KB4474419 and KB4490628 installed (read the SHA-2 required compatibility)
- Microsoft Windows Small Business Server 2011 SP1 (x64) with KB4474419 and KB4490628 installed

NOTE
On Windows Server 2008 R2 SP1, **Network protection** component is disabled by default in **Typical** installation. Use **Custom** installation to have this component installed.

IMPORTANT
Support for the Azure Code Signing needs to be installed on all Windows operating systems in order to install or upgrade ESET products released after the end of July, 2023. More information.
If you run Windows Server 2008 R2 SP1, ensure you have KB5006728 installed to support Azure Code Signing. The ESU (Extended Security Updates) is required to install KB5006728.

Supported Microsoft Exchange Server versions:

- Microsoft Exchange Server 2019 up to CU13
- Microsoft Exchange Server 2016 up to CU23
- Microsoft Exchange Server 2013 up to CU23 (CU1 and CU4 aka SP1 are not supported)
- Microsoft Exchange Server 2010 SP1, SP2, SP3 up to RU32
- Microsoft Exchange Server 2007 SP1, SP2, SP3

NOTE
Standalone Client Access Server (CAS) role is not supported, see Exchange server roles for more details.
We recommend that you refer to ESET Mail Security features and Exchange Server Roles to identify what features are available for each supported version of Microsoft Exchange Server and their roles.

Minimum hardware requirements:

Component	Requirement
Processor	Intel or AMD single core x64
Memory	256 MB of free memory

Component	Requirement
Hard drive	700 MB of free disk space
Screen resolution	800 x 600 pixels or higher

ESET Mail Security has the same recommended hardware requirements that apply to Microsoft Exchange Server. See the following Microsoft Technical Articles for details:

Microsoft Exchange Server 2007
Microsoft Exchange Server 2010
Microsoft Exchange Server 2013
Microsoft Exchange Server 2016

NOTE
We strongly recommend that you install the latest Service Pack for your Microsoft Server operating system and server application before installing ESET security product. We also recommend that you install the latest Windows updates and hotfixes whenever available.

SHA-2 required compatibility

Microsoft announced deprecation of Secure Hash Algorithm 1 (SHA-1) and started migration process to SHA-2 in early 2019. Therefore, all certificates signed with the SHA-1 algorithm will no longer be recognized and will cause security alerts. Unfortunately, the security of the SHA-1 hash algorithm has become less secure over time due to weaknesses found in the algorithm, increased processor performance, and the advent of cloud computing.

The SHA-2 hashing algorithm (as a successor to SHA-1) is now the preferred method to guarantee SSL security durability. See Microsoft Docs article about Hash and Signature Algorithms for further details.

NOTE
This change means that on operating systems without SHA-2 support, your ESET security solution will no longer be able to update its modules, including the detection engine, ultimately making your ESET Mail Security not fully functional and unable to provide sufficient protection.

If you are running **Windows Server 2008 R2 SP1** or **Microsoft Windows Small Business Server 2011 SP1** ensure your system is compatible with SHA-2. Apply the patches according to your particular operating system version as follows:

- **Microsoft Windows Server 2008 R2 SP1** — apply KB4474419 and KB4490628 (an additional system restart might be necessary)

- **Microsoft Windows Small Business Server 2011 SP1** (x64) — apply KB4474419 and KB4490628 (an additional system restart might be necessary)

IMPORTANT
Once you have installed the updates and restarted your system, open ESET Mail Security GUI to check its status. In case the status is orange, perform an additional system restart. The status should then be green indicating maximum protection.

NOTE
We strongly recommend that you install the latest Service Pack for your Microsoft Server operating system and server application. We also recommend that you install the latest Windows updates and hotfixes whenever available.

Preparing for installation

There are a few steps we recommend you to take in preparation of the product installation:

- After purchasing ESET Mail Security, download `.msi` installation package from ESET's website.

- Make sure that the server on which you plan to install ESET Mail Security meets system requirements.

- Log on to the server using an Administrator account.

NOTE
Please note that you must to execute the installer using the Built-in Administrator account or a domain Administrator account (in the event that local Administrator account is disabled). Any other user, despite being a member of Administrators group, will not have sufficient access rights. Therefore you need to use the Built-in Administrator account, as you will not be able to successfully complete installation under any other user account than local or domain Administrator.

- If you are going to do an upgrade from an existing installation of ESET Mail Security, we recommend you to backup its current configuration using the Export settings feature.

- Remove /uninstall any third-party antivirus software from your system, if applicable. We recommend that you use the ESET AV Remover. For a list of third-party antivirus software that can be removed using ESET AV Remover, see this KB article.

- If you are installing ESET Mail Security on Windows Server 2016, Microsoft recommends to uninstall Windows Defender Features and withdraw from Windows Defender ATP enrollment to prevent problems caused by having multiple antivirus products installed on a machine.

NOTE
If **Windows Defender Features** are present on your **Windows Server 2016** or **2019** during installation of ESET Mail Security, these features are turned off by ESET Mail Security to prevent collisions of real-time protection between multiple antivirus products. Also, Windows Defender Features are turned off by ESET Mail Security with every system start-up / restart.
There is an exception to this — if you are doing a component installation without **Real-time file system protection** component, Windows Defender Features on Windows Server 2016 are not being turned off.

- For comprehensive view, see matrix of ESET Mail Security features and Microsoft Exchange Server versions and their roles.

- You can check the number of mailboxes by running the **Mailbox Count tool**, see our Knowledgebase article for details. Once your ESET Mail Security is installed, it will display current mailbox count at the bottom of the Monitoring window.

You can run ESET Mail Security installer in two installation modes:

- Graphical user interface (GUI)
This is the recommended installation type in a from of an installation wizard.

- Silent / Unattended installation
In addition to the installation wizard, you can choose to install ESET Mail Security silently via command line.

> IMPORTANT
> We highly recommend installing ESET Mail Security on a freshly installed and configured OS, if possible. If you do need to install it on an existing system, we recommend that you uninstall previous version of ESET Mail Security, restart the server and install the new ESET Mail Security afterwards.

- Upgrading to a newer version
If you are using an older version of ESET Mail Security, you can choose suitable upgrade method.

After you've successfully installed or upgraded your ESET Mail Security, further activities are:

- Product activation
Availability of a particular activation scenario in the activation window may vary depending on the country, as well as the means of distribution.

- Post-installation tasks
See the list of recommended tasks you can perform after a successful installation of ESET Mail Security.

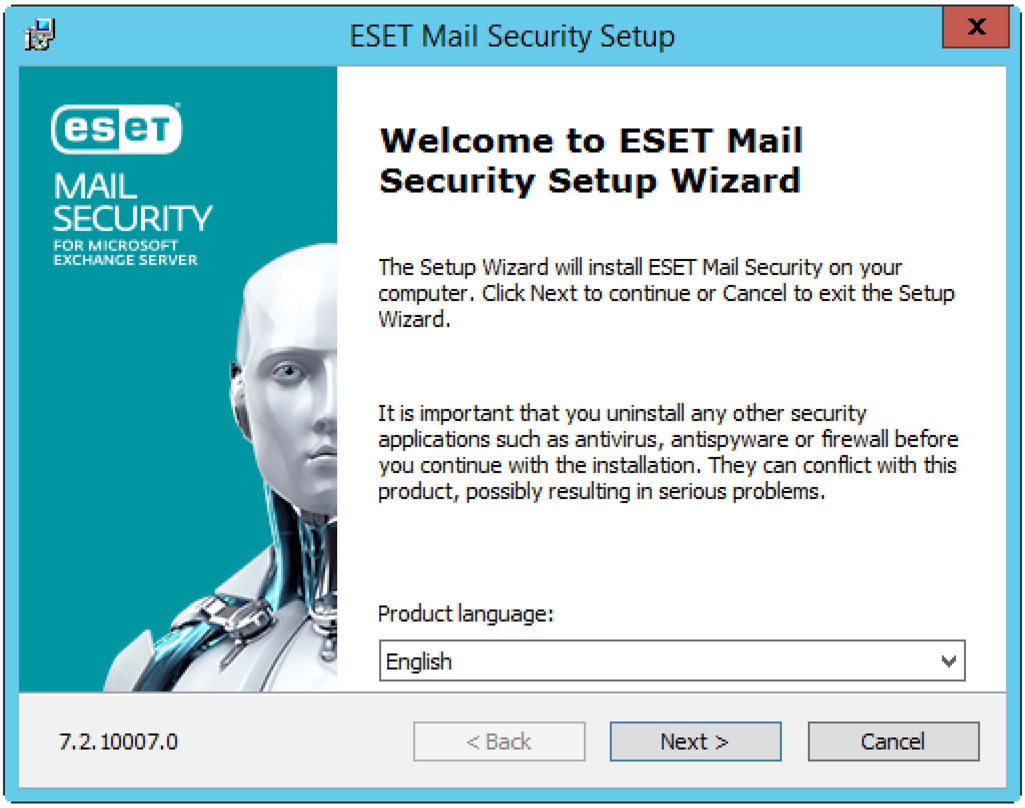
- Configuring server protection
You can fine-tune your ESET Mail Security by modifying advanced settings of each of its features to suite on your needs.

ESET Mail Security installation steps

This is a typical GUI installation wizard. Double-click the `.msi` package and follow the steps to install ESET Mail Security:

1. Click **Next** to continue or click **Cancel** if you want to quit the installation.

2. The installation wizard runs in a language that is specified as **Home location** of a **Region** > **Location** setting of your operating system (or **Current location** of a **Region and Language** > **Location** setting in older systems). Use the drop-down menu to select **Product language** in which your ESET Mail Security will be installed. Selected language for ESET Mail Security is independent of the language you see in the installation wizard.



ESET Mail Security Setup

Welcome to ESET Mail Security Setup Wizard

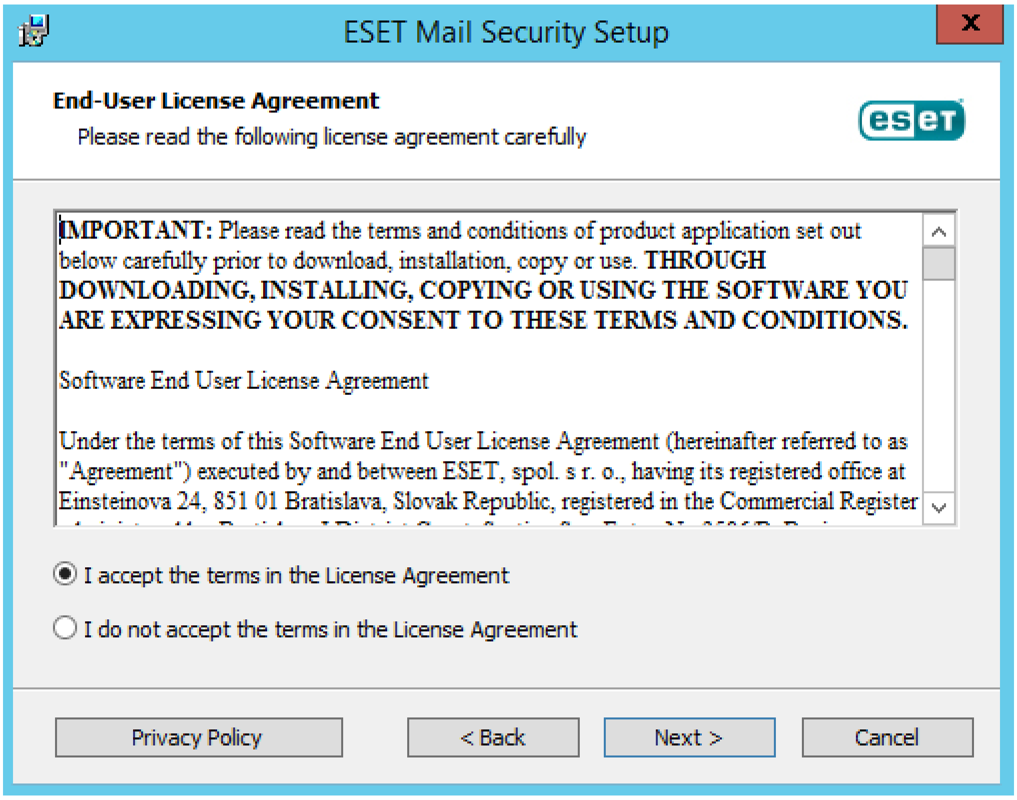
The Setup Wizard will install ESET Mail Security on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

It is important that you uninstall any other security applications such as antivirus, antispyware or firewall before you continue with the installation. They can conflict with this product, possibly resulting in serious problems.

Product language: English

7.2.10007.0

3.Click **Next**, the End-User License Agreement will be displayed. After you acknowledge your acceptance of the **End User License Agreement** and Privacy policy, click **Next**.



ESET Mail Security Setup

End-User License Agreement

Please read the following license agreement carefully

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS.

Software End User License Agreement

Under the terms of this Software End User License Agreement (hereinafter referred to as "Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register

● I accept the terms in the License Agreement

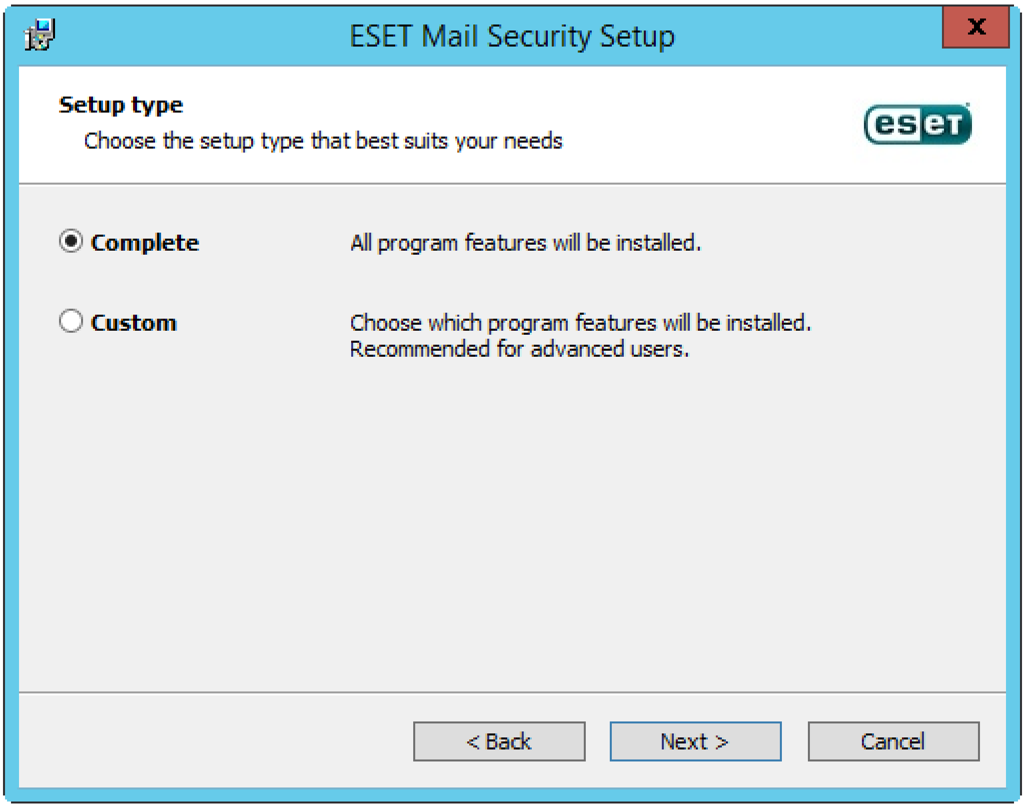
○ I do not accept the terms in the License Agreement

4.Choose one of available installation types (availability depend on your operating system):

Complete

Installs all ESET Mail Security features. Also called a full installation. This is the recommended installation type, available for **Windows Server 2012, 2012 R2, 2016 and 2019**.

NOTE
In case you are planning to use Local quarantine for email messages and do not want to have quarantined message files stored on your *C:* drive, change the path of **Data folder** to your preferred drive and location. However, keep in mind that all ESET Mail Security data files will be stored in this location.



Setup type
Choose the setup type that best suits your needs

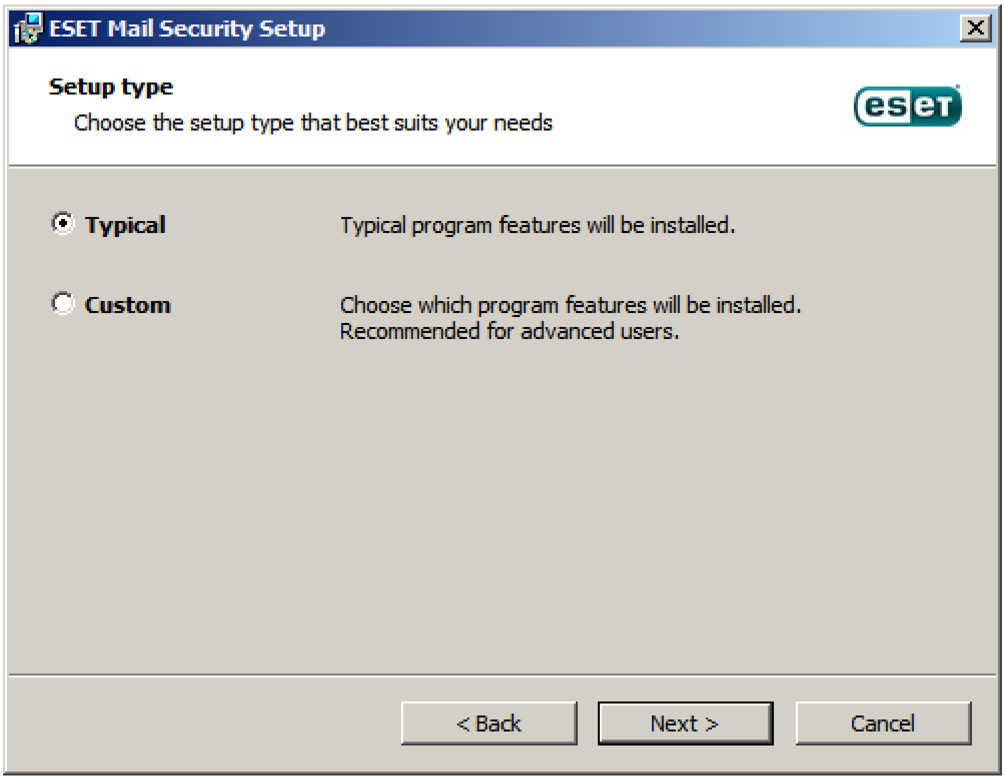
● **Complete** All program features will be installed.

○ **Custom** Choose which program features will be installed. Recommended for advanced users.

Typical

Installs recommended ESET Mail Security features. Available for Windows Server 2008 R2 SP1 and Windows Small Business Server 2011 SP1.

NOTE
On Windows Server 2008 R2 SP1, **Network protection** component is disabled by default (**Typical** installation). Use **Custom** installation to have this component installed.



ESET Mail Security Setup

Setup type

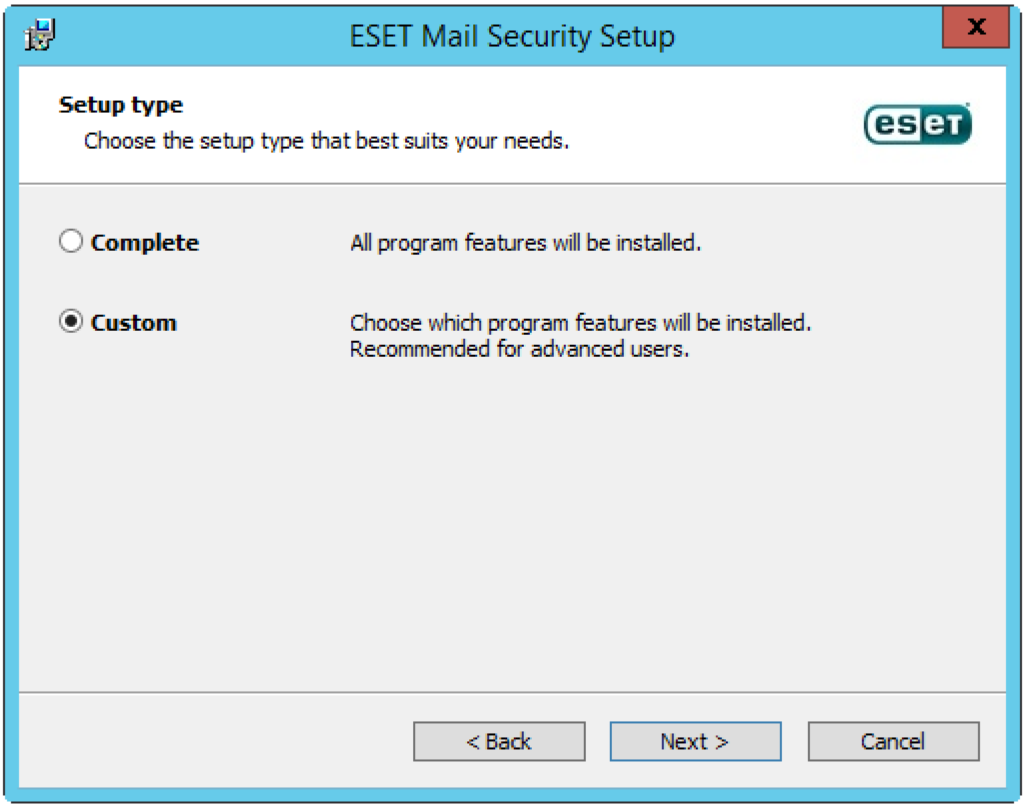
Choose the setup type that best suits your needs

● Typical — Typical program features will be installed.

○ Custom — Choose which program features will be installed. Recommended for advanced users.

Custom

Lets you choose which features of ESET Mail Security will be installed on your system. A list of product modules and features will be displayed before the installation starts. It is useful when you want to customize ESET Mail Security with only the components you need.



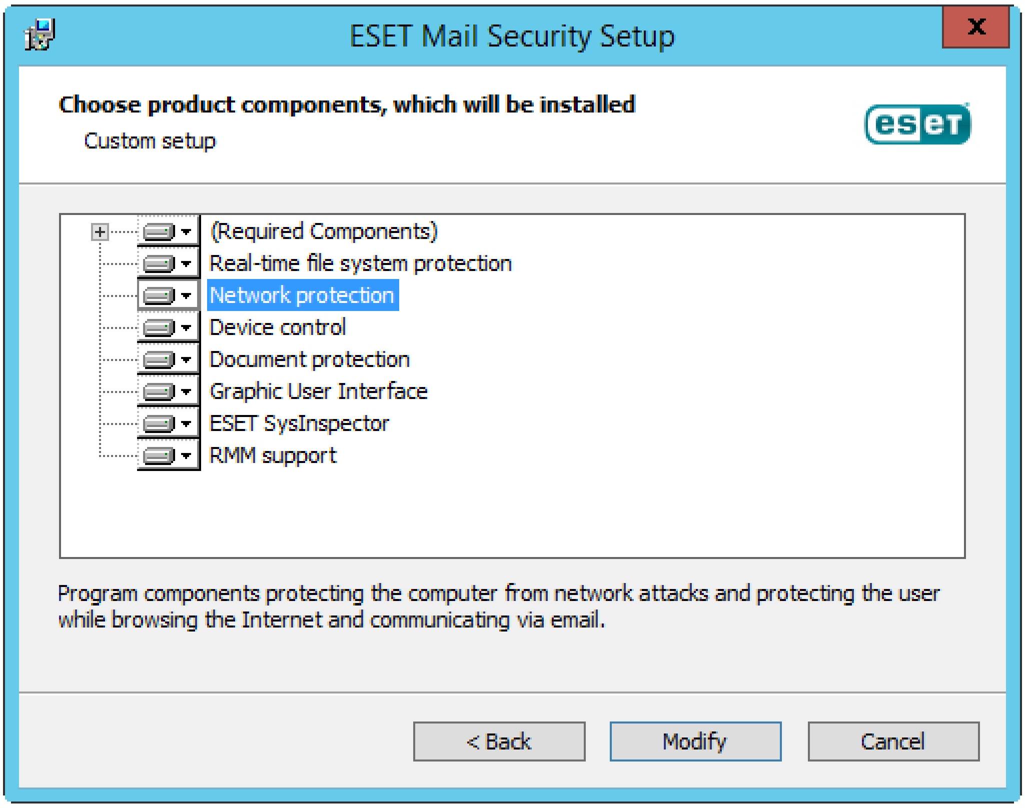
ESET Mail Security Setup

Setup type

Choose the setup type that best suits your needs.

○ Complete — All program features will be installed.

● Custom — Choose which program features will be installed. Recommended for advanced users.


ESET Mail Security Setup

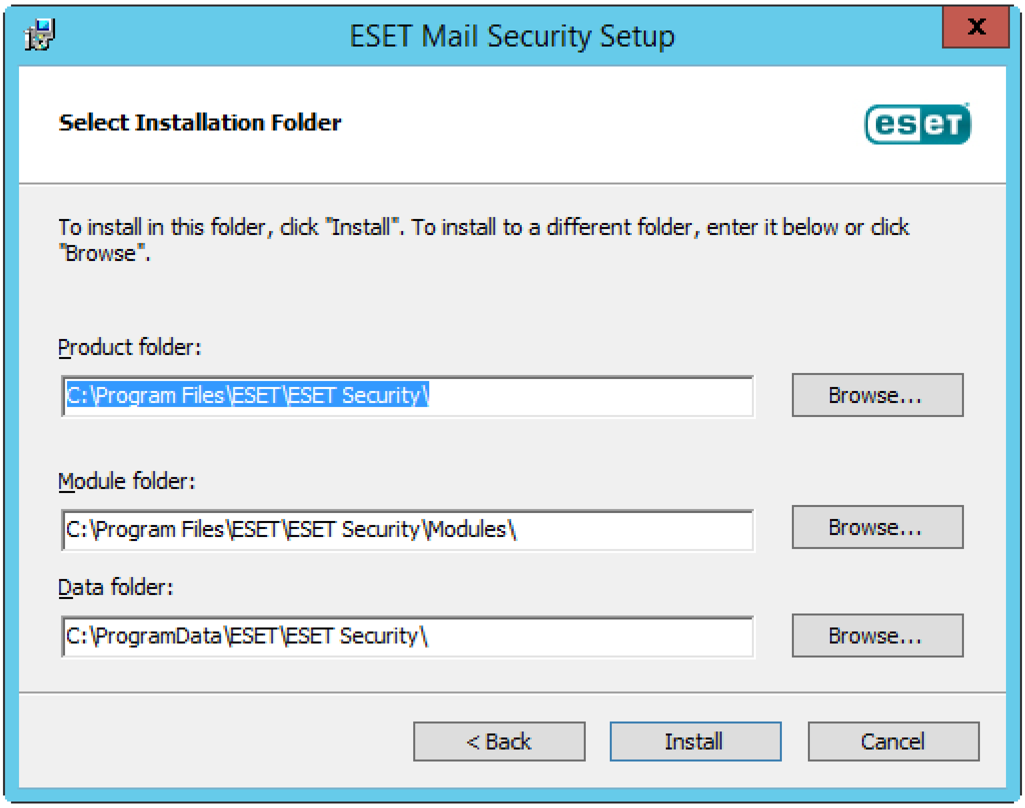
Choose product components, which will be installed

Custom setup

- (Required Components)
- Real-time file system protection
- Network protection
- Device control
- Document protection
- Graphic User Interface
- ESET SysInspector
- RMM support

Program components protecting the computer from network attacks and protecting the user while browsing the Internet and communicating via email.

5.You will be prompted to select the location where ESET Mail Security will be installed. By default, the program installs in *C:\Program Files\ESET\ESET Mail Security*. Click **Browse** to change this location (not recommended).


ESET Mail Security Setup

Select Installation Folder

To install in this folder, click "Install". To install to a different folder, enter it below or click "Browse".

Product folder: C:\Program Files\ESET\ESET Security\

Module folder: C:\Program Files\ESET\ESET Security\Modules\

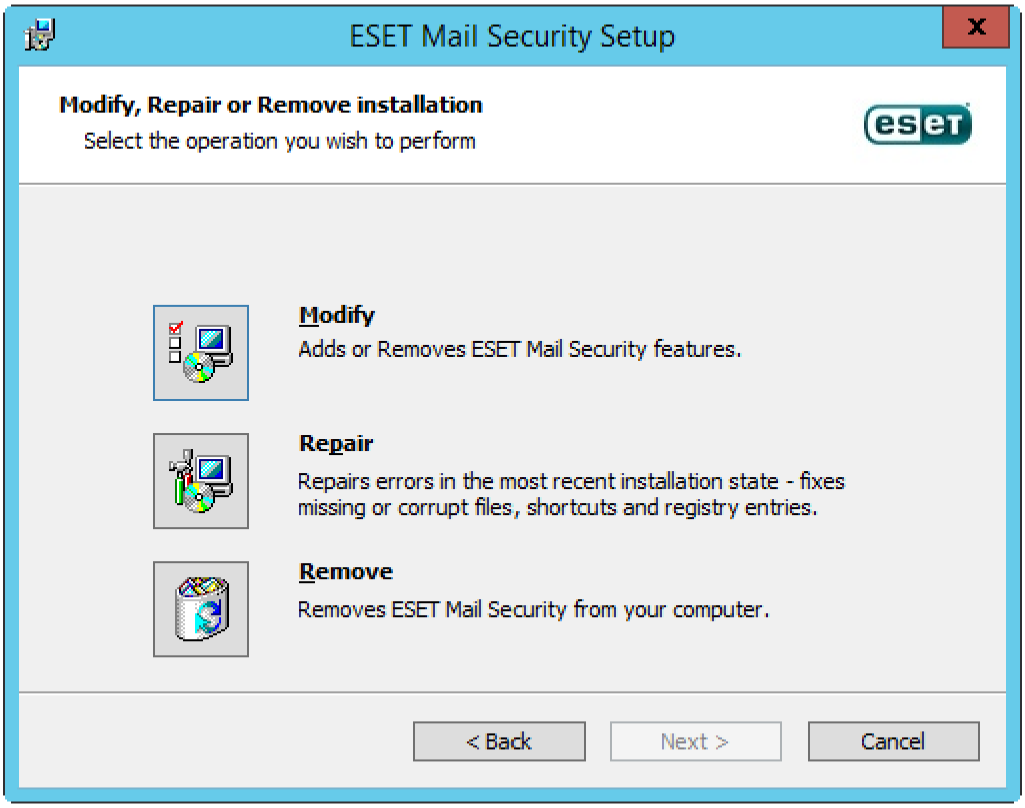
Data folder: C:\ProgramData\ESET\ESET Security\

6.Click **Install** to begin the installation. When the installation finishes, ESET GUI starts and tray icon ⓔ is displayed in the notification area (system tray).

Modifying an existing installation

You can add or remove components included in your installation. To do so, either run the `.msi` installer package you used during initial installation, or go to **Programs and Features** (accessible from the Windows Control Panel), right-click ESET Mail Security and select **Change**. Follow the steps below to add or remove components.

There are 3 options available. You can **Modify** installed components, **Repair** your installation of ESET Mail Security or **Remove** (uninstall) it completely.



ESET Mail Security Setup

Modify, Repair or Remove installation

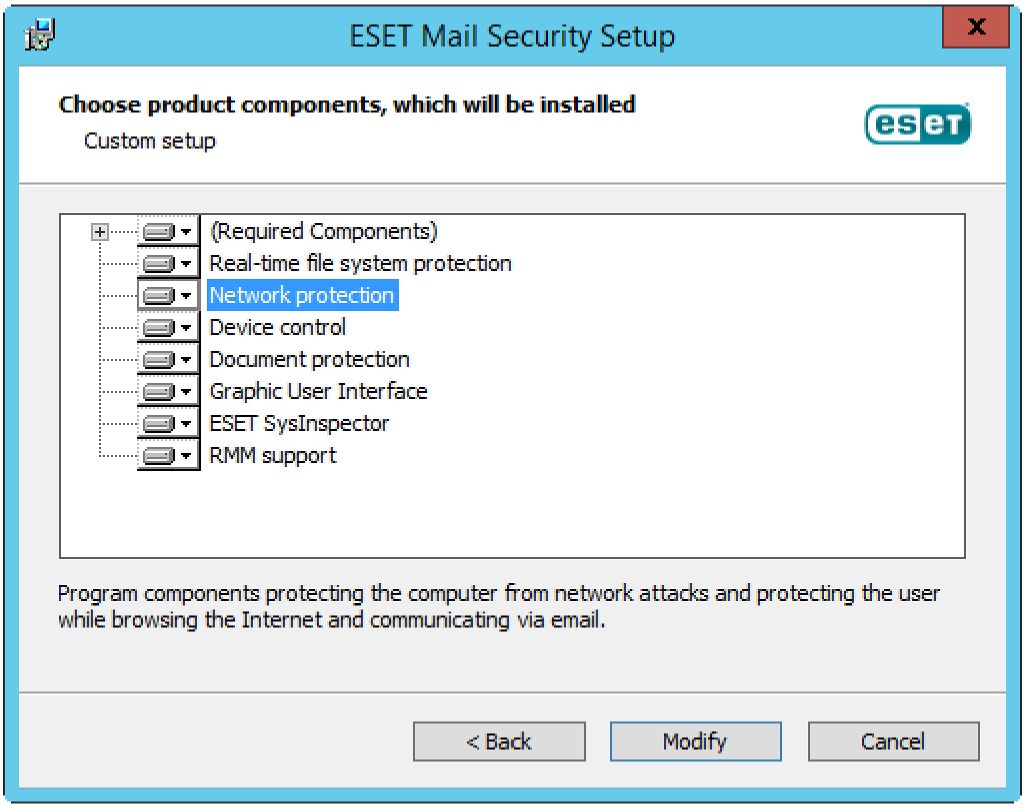
Select the operation you wish to perform

Modify
Adds or Removes ESET Mail Security features.

Repair
Repairs errors in the most recent installation state - fixes missing or corrupt files, shortcuts and registry entries.

Remove
Removes ESET Mail Security from your computer.

If you choose **Modify,** a list of available program components is displayed. Choose the components you want to add or remove. You can add/remove multiple components at the same time. Click the component and select an option from the drop-down menu:



ESET Mail Security Setup

Choose product components, which will be installed

Custom setup

- (Required Components)
- Real-time file system protection
- Network protection
- Device control
- Document protection
- Graphic User Interface
- ESET SysInspector
- RMM support

Program components protecting the computer from network attacks and protecting the user while browsing the Internet and communicating via email.

When you have selected an option, click **Modify** to perform the modifications.

> NOTE
> You can modify installed components at any time by running the installer. For most components, a server restart is not necessary to carry out the change. The GUI will restart and you'll only see only the components you chose to install. For components that require a server restart, the Windows Installer will prompt you to restart and new components will become available once the server is back online.

Silent / Unattended installation

Execute the following command to run the installation silently (no UI) via command line: `msiexec /i <packagename> /qn /l*xv msi.log`

> NOTE
> On Windows Server 2008 R2 SP1 the **Network protection** feature will not be installed.

To make sure the installation was successful or in case of any issues with the installation, use Windows Event Viewer to check the **Application Log** (look for records from Source: MsiInstaller).

> EXAMPLE
> **Full installation** on a 64-bit system:

```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

When the installation finishes, ESET GUI starts and tray icon ⓔ is displayed in the notification area (system tray).

EXAMPLE

Installation of the product in **specified language** (German):

```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```

See **Language parameters** in Command line installation for further details and the list of language codes.

IMPORTANT

When specifying values for `REINSTALL` parameter, you must list the rest of the features that are not used as values for `ADDLOCAL` or `REMOVE` parameter. It is necessary for the command line installation to run properly that you list all the features as values for `REINSTALL`, `ADDLOCAL` and `REMOVE` parameters. Adding or removing may not be successful if you do not use the `REINSTALL` parameter.

See Command line installation section for the complete list of features.

EXAMPLE

Complete removal (uninstallation) from a 64-bit system:

```
msiexec /x emsx_nt64.msi /qn /l*xv msi.log
```

NOTE

Your sever will reboot automatically after a successful uninstallation.

Command line installation

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

Supported parameters:

APPDIR=<path>

- path - Valid directory path
- Application installation directory
- For example: `emsx_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- path - Valid directory path
- Application Data installation directory

MODULEDIR=<path>

- path - Valid directory path
- Module installation directory

ADDLOCAL=<list>

- Component installation - list of non-mandatory features to be installed locally.
- Usage with ESET `.msi` packages: `emsx_nt64.msi /qn ADDLOCAL=<list>`
- For more information about the `ADDLOCAL` property see https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- The `ADDLOCAL` list is a comma-separated list of all feature that will be installed.

- When selecting a feature to be installed, the full path (all parent features) must be explicitly included in the list.

REMOVE=<list>

- Component installation - parent feature you do not want to have installed locally.
- Usage with ESET `.msi` packages: `emsx_nt64.msi /qn REMOVE=<list>`
- For more information about the `REMOVE` property see https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove
- The `REMOVE` list is a comma-separated list of parent features that will not be installed (or will be removed in case of existing installation).
- It is sufficient to specify parent feature only. There is no need to explicitly include every child feature to the list.

ADDEXCLUDE=<list>

- The `ADDEXCLUDE` list is a comma-separated list of all feature names not to be installed.
- When selecting a feature not to be installed, then the whole path (i.e., all its sub-features) and related invisible features must be explicitly included in the list.
- For example: `emsx_nt64.msi /qn ADDEXCLUDE=<list>`

NOTE
`ADDEXCLUDE` cannot be used with `ADDLOCAL`.

Feature Presence

- **Mandatory** - The feature is always installed.
- **Optional** - The feature may be deselected for install.
- **Invisible** - Logical feature mandatory for other features to work properly.

List of ESET Mail Security features:

IMPORTANT
Names of all the features are case sensitive, for example `RealtimeProtection` is not equal to `REALTIMEPROTECTION`.

Feature Name	Feature Presence
`SERVER`	Mandatory
`RealtimeProtection`	Mandatory
`MAILSERVER`	Mandatory
`WMIProvider`	Mandatory
`HIPS`	Mandatory
`Updater`	Mandatory
`eShell`	Mandatory
`UpdateMirror`	Mandatory
`DeviceControl`	Optional
`DocumentProtection`	Optional
`WebAndEmail`	Optional

Feature Name	Feature Presence
ProtocolFiltering	Invisible
NetworkProtection	Optional
IdsAndBotnetProtection	Optional
Rmm	Optional
WebAccessProtection	Optional
EmailClientProtection	Optional
MailPlugins	Invisible
Cluster	Optional
_Base	
eula	
ShellExt	Optional
_FeaturesCore	
GraphicUserInterface	Optional
SysInspector	Optional
SysRescue	Optional
EnterpriseInspector	Optional

If you want to remove any of the following features, you need to remove the whole group by specifying every feature that belongs to the group. Otherwise, the feature will not be removed. Here are two groups (each line represents one group):

```
GraphicUserInterface,ShellExt
```

```
NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

EXAMPLE
Exclude **NetworkProtection** section (including child features) from the installation using REMOVE parameter and specifying only parent feature:

```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

Alternatively, you can use ADDEXCLUDE parameter, but you must also specify all child features:

```
msiexec /i emsx_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

If you want your ESET Mail Security to be automatically configured after the installation, you can specify basic configuration parameters within the installation command.

EXAMPLE
Install ESET Mail Security and disable ESET LiveGrid®:

```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log CFG_LIVEGRID_ENABLED=0
```

List of all configuration properties:

Switch	Value
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 - Disabled, 1 - Enabled
CFG_LIVEGRID_ENABLED=1/0	0 - Disabled, 1 - Enabled
FIRSTSCAN_ENABLE=1/0	0 - Disable, 1 - Enable

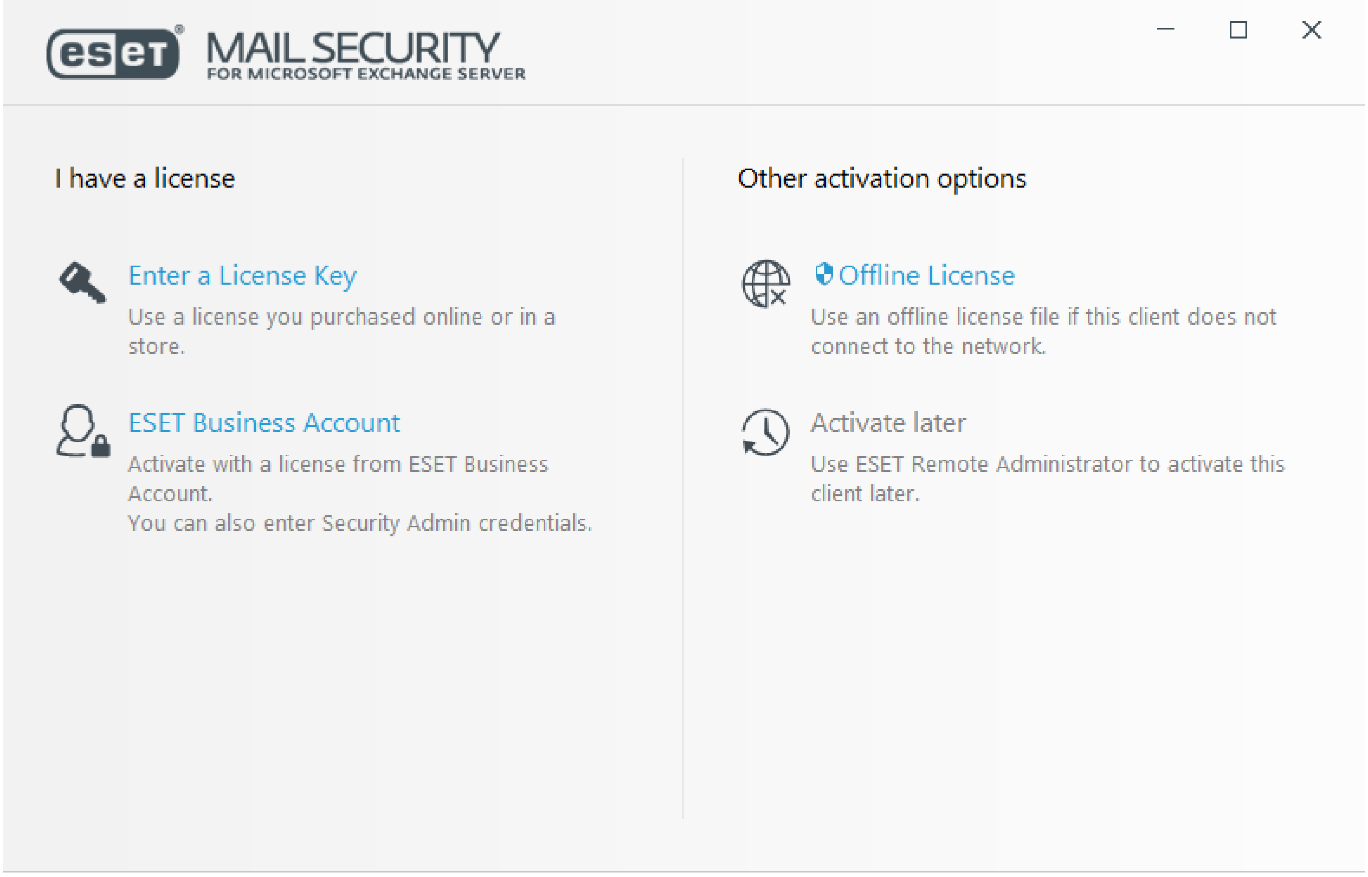
Switch	Value
CFG_PROXY_ENABLED=0/1	0 - Disabled, 1 - Enabled
CFG_PROXY_ADDRESS=<ip>	Proxy IP address
CFG_PROXY_PORT=<port>	Proxy port number
CFG_PROXY_USERNAME=<user>	User name for authentication
CFG_PROXY_PASSWORD=<pass>	Password for authentication

Language parameters: Product language (you must specify both parameters)

Switch	Value
PRODUCT_LANG=	LCID Decimal (Locale ID), for example 1033 for *English - United States*, see the list of language codes.
PRODUCT_LANG_CODE=	LCID String (Language Culture Name) in lowercase, for example en-us for *English - United States*, see the list of language codes.

Product activation

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


eset MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
I have a license
Enter a License Key
Use a license you purchased online or in a store.
ESET Business Account
Activate with a license from ESET Business Account.
You can also enter Security Admin credentials.
Other activation options
Offline License
Use an offline license file if this client does not connect to the network.
Activate later
Use ESET Remote Administrator to activate this client later.

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

Use a purchased License Key

> A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the the license owner and for activation of the license.

ESET Business Account

Use this option if you are registered and have your ESET Business Account (EBA) where your ESET Mail Security license has been imported. You can also enter **Security Admin** credentials that you use on ESET License Administrator portal.

Offline License file

An automatically generated file that will be transferred to the ESET product to provide license information. Your offline License file is generated from the license portal and is used in environments where the application cannot connect to the licensing authority.

Click **Activate later** with ESET Security Management Center if your computer is a member of a managed network, and your administrator will perform remote activation via ESET Security Management Center. You can also use this option if you want to activate this client at a later time.

Select **Help and support** > **Manage license** in the main program window to manage your license information at any time. You will see the public license ID used to identify your product by ESET and for license identification. Your Username, under which the computer is registered, is stored in the About section, which you can view by right-clicking the system tray icon ⓔ.

After you've successfully activated ESET Mail Security, the main program window will open and display your current status in the Monitoring page. Some attention may be required initially, for example, you'll be asked if you want to be part of ESET LiveGrid®.

The main program window will also display notifications about other items, such as system updates (Windows Updates) or detection engine updates. When all items that require attention are resolved, the monitoring status will turn green and display the status **You are protected**.

To activate your copy of ESET Mail Security directly from the program, click the system tray icon ⓔ and select **Product is not activated** from the menu. You can also activate your product from the main menu under **Help and support** > **Activate Product** or **Monitoring status** > **Product is not activated**.

> NOTE
> ESET Security Management Center is able to activate client computers silently using licenses made available by the administrator.

ESET Business Account

ESET Business Account allows you to manage multiple licenses. If you do not have ESET Business Account, click **Create account** and you will be redirected to the ESET Business Account portal where you can register.

> NOTE
> For more information, see the ESET Business Account (EBA) User Guide.

If you are using Security Admin credentials and have forgotten your password, click **I forgot my password** and you will be redirected to the ESET License Administrator portal. Enter your email address and click **Submit** to confirm. After that you will obtain a message with instructions to reset your password.

Activation successful

Activation was successful and ESET Mail Security is now activated. From now on, ESET Mail Security will receive regular updates to identify the latest threats and keep your computer safe. Click **Done** to finish product activation.

Activation failure

Activation of ESET Mail Security was not successful. Make sure you have entered the proper **License Key** or attached an **Offline License**. If you have a different **Offline License**, please enter it again. To check the license key you entered, click **recheck the License Key** or **enter a different license**.

If you are unable to activate, see the activation troubleshooting wizard.

License

You will be prompted to select a license associated with your account that will be used for ESET Mail Security. Click **Continue** proceed with activation.

Upgrading to a newer version

New versions of ESET Mail Security are issued to provide improvements or fix issues that cannot be resolved by automatic updates of program modules.

Upgrade methods:

- **Uninstall / Install** - Removing the older version before installing the new one. Download the latest version of ESET Mail Security. Export settings from your existing ESET Mail Security if you want to preserve configuration. Uninstall ESET Mail Security and restart the server. Perform a fresh installation with the installer you have downloaded. Import settings to load your configuration. We recommend this procedure if you have a single server running ESET Mail Security.

- **In-place** - An upgrade method without removing the existing version and installing the new ESET Mail Security over it.

> IMPORTANT
> It is necessary that you have **no pending Windows Updates** on your server, as well as **no pending restart** due to Windows Updates or for any other reason. If you try performing in-place upgrade with a pending Windows Updates or restart, the existing version of ESET Mail Security may not be removed correctly. You will also experience problems if you decide to remove the old version of ESET Mail Security manually afterward.

> NOTE
> A server restart will be required during the upgrade of ESET Mail Security.

- Remote - For use in large network environments managed by ESET Security Management Center. This is basically a clean upgrade method, but carried out remotely. It is useful if you have multiple servers running ESET Mail Security.

- ESET Cluster wizard - Can also be used as an upgrade method. We recommend this method for 2 or more servers with ESET Mail Security. This is basically an in-place upgrade method, but carried out via ESET Cluster. Once the upgrade is completed, you can continue using ESET Cluster and take advantage of its features.

> IMPORTANT
> Upgrade from version 4.x does not retain certain settings, specifically rules cannot be migrated. This is due to changes in the rules feature that were introduced in later product versions. We recommend that you make note of your rules settings before upgrading from version 4.x. You can setup rules after the upgrade is finished. New rules gives you greater flexibility and even more possibilities compared to rules in previous version of ESET Mail Security.

The following settings are preserved from previous versions of ESET Mail Security:

- General ESET Mail Security configuration.

Antispam protection settings:

- All settings that are identical in previous versions, any new settings will use defaults.
- Whitelist and blacklist entries.

> NOTE
> Once you've upgraded your ESET Mail Security, we recommend you to go through all the settings to make sure it is configured correctly and according to your needs.

Upgrading via ESET Security Management Center

ESET Security Management Center allows you to upgrade multiple servers that are running older version of ESET Mail Security. This method has the advantage of upgrading large number of servers at the same time while making sure each ESET Mail Security is configured identically (if this is desired).

The procedure consists of the following phases:

- **Upgrade the first server** manually by installing the latest version of ESET Mail Security over your existing version in order to preserve all of the configuration including rules, numerous whitelists and blacklists, etc. This phase is performed locally on the server running ESET Mail Security.

- **Request configuration** of the newly upgraded ESET Mail Security to version 7.x and **Convert to policy** in ESET Security Management Center. The policy will later be applied to all upgraded servers. This phase is performed remotely using ESMC as well as the following phases.

- **Run Software Uninstall** task on all servers running old version of ESET Mail Security.

- **Run Software Install** task on all servers which you want the latest version ESET Mail Security to run.

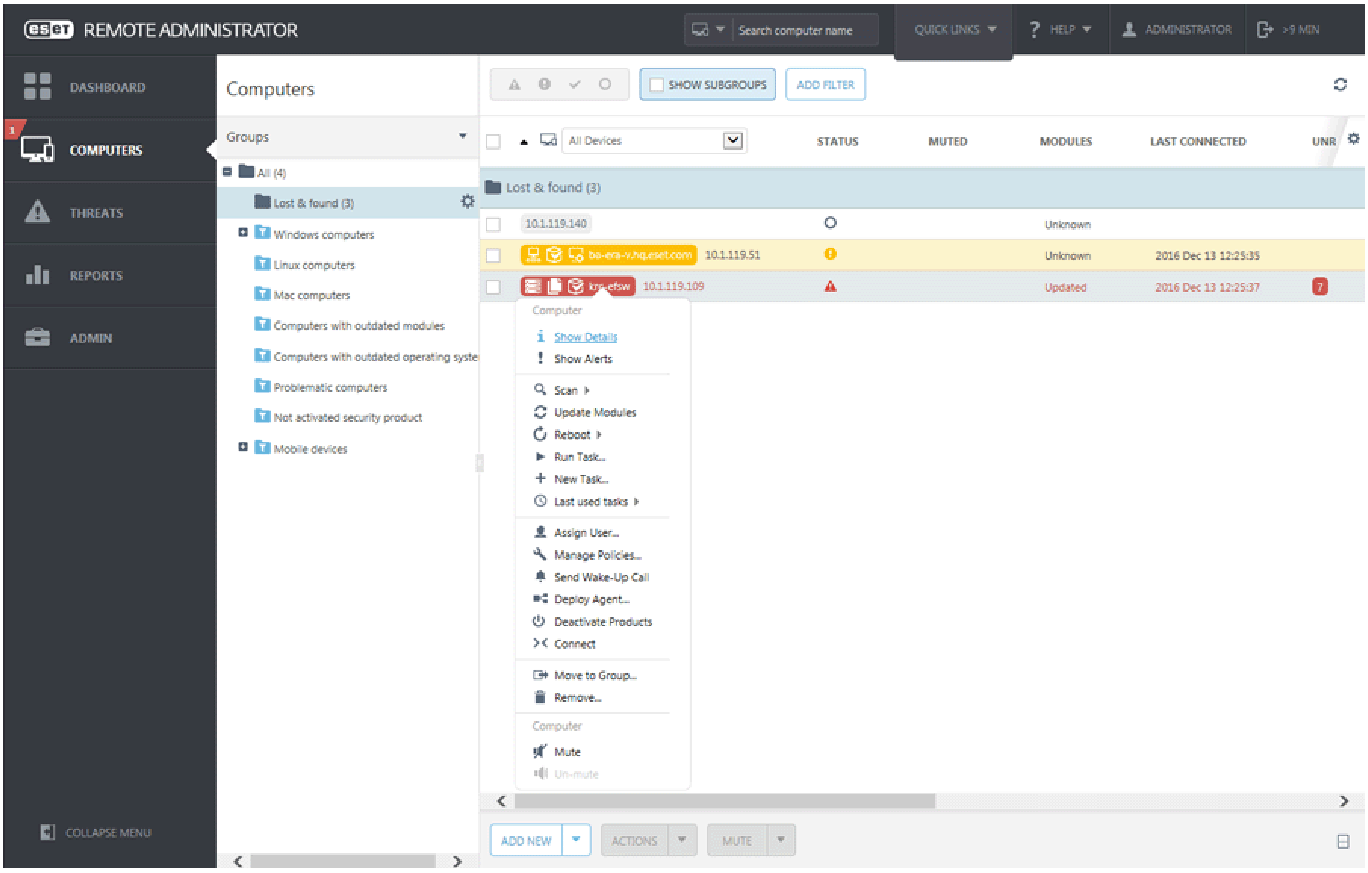
- **Assign configuration policy** to all the servers running the latest version ESET Mail Security.

Step-by-step procedure:

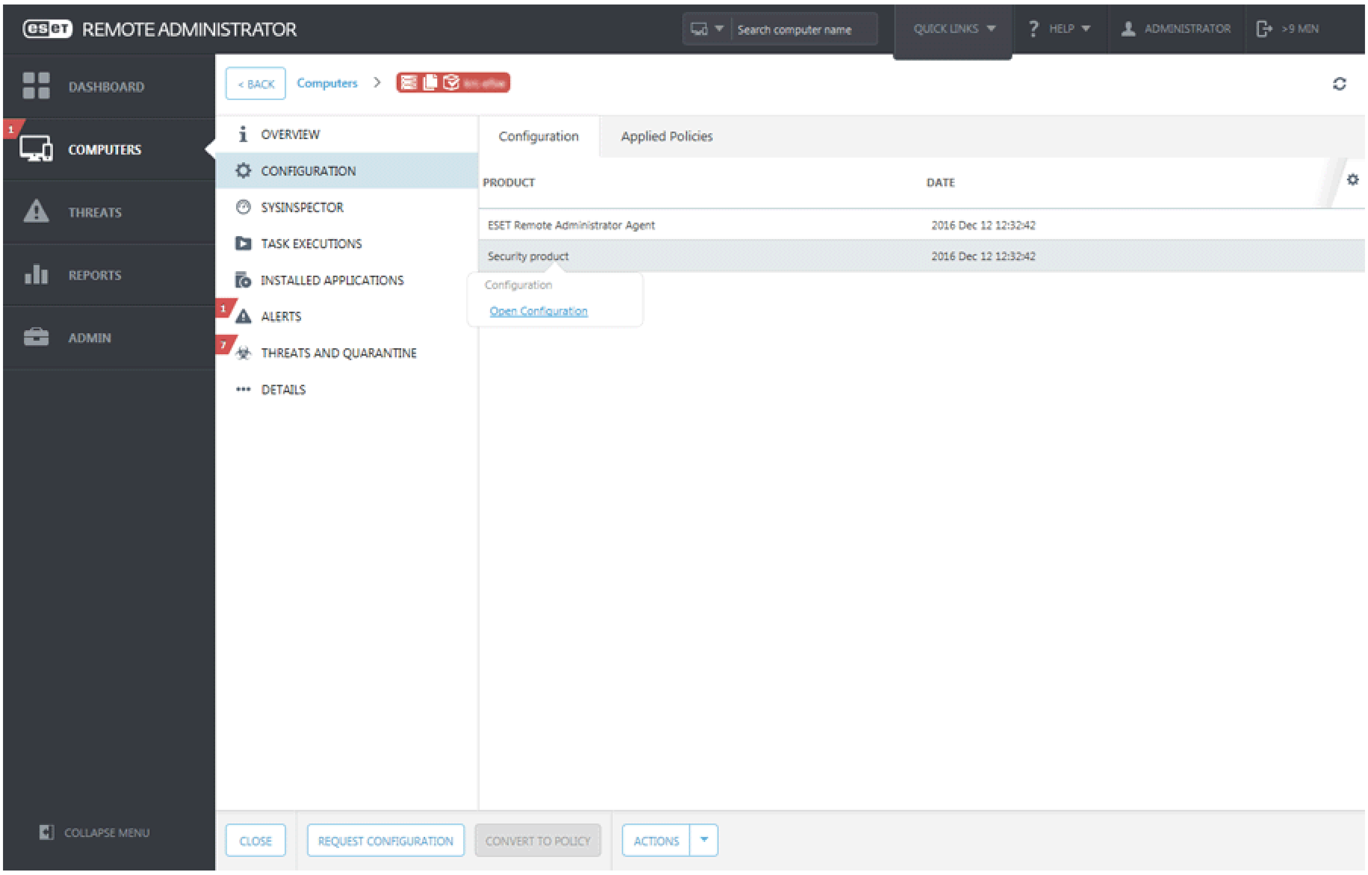
1. Log onto one of the servers running ESET Mail Security and upgrade it by downloading and installing the

latest version over your existing one. Follow the steps for regular installation. All of the original configuration of your old ESET Mail Security will be preserved during the installation.

2.Open the **ESET Security Management Center Web Console**, select a client computer from a Static or Dynamic group and click **Show Details**.

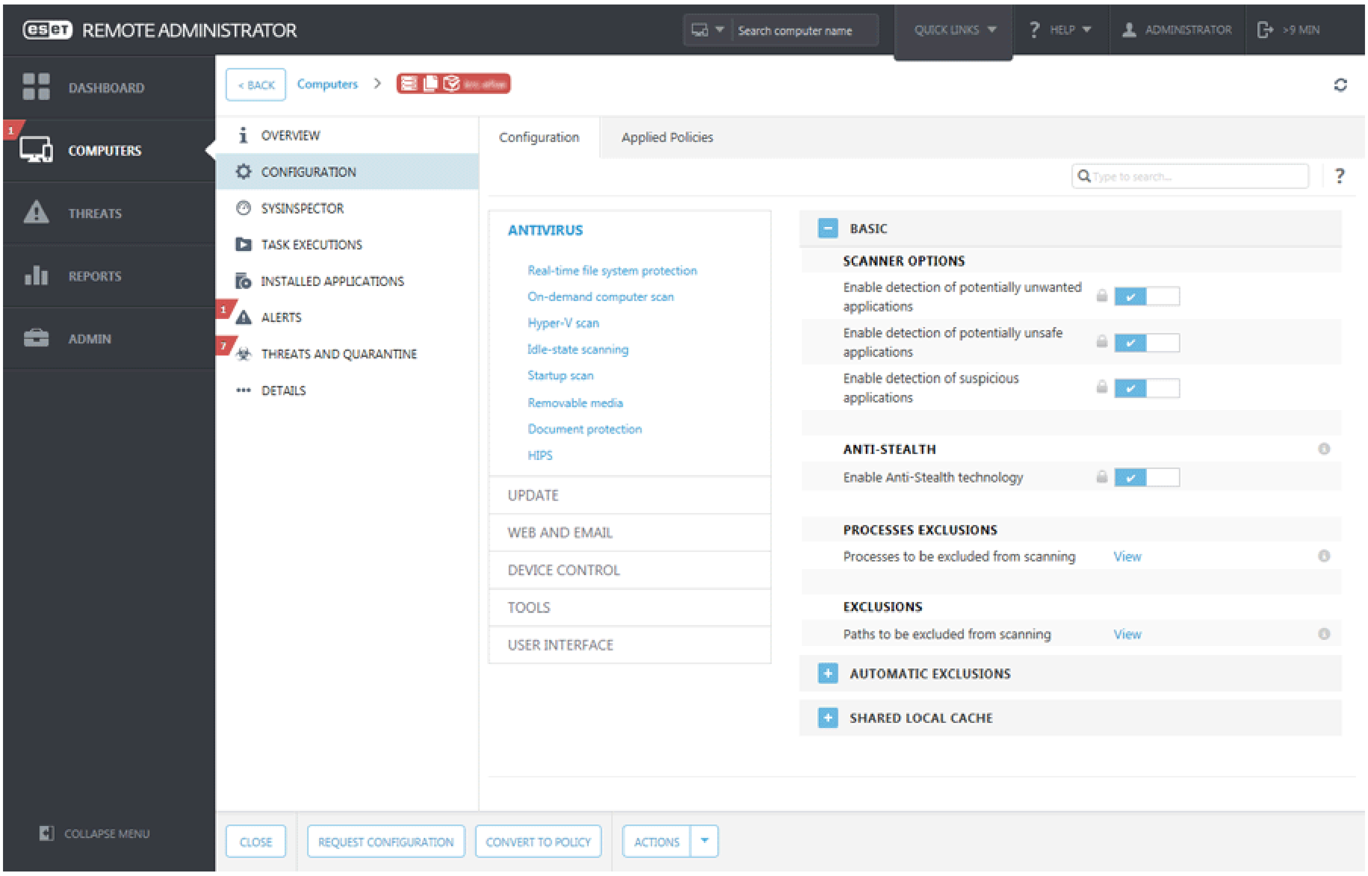


3.Navigate to Configuration tab and click the **Request configuration** button to collect all configuration of managed product. It will take a moment to get the configuration. Once the latest configuration appears in the list, click **Security product** and choose **Open Configuration**.



PRODUCT	DATE
ESET Remote Administrator Agent	2016 Dec 12 12:32:42
Security product	2016 Dec 12 12:32:42

4.Create configuration policy by clicking Convert to policy button. Enter the **Name** for a new policy and click **Finish**.



BASIC

SCANNER OPTIONS

Enable detection of potentially unwanted applications ✓

Enable detection of potentially unsafe applications ✓

Enable detection of suspicious applications ✓

ANTI-STEALTH

Enable Anti-Stealth technology ✓

PROCESSES EXCLUSIONS

Processes to be excluded from scanning View

EXCLUSIONS

Paths to be excluded from scanning View

AUTOMATIC EXCLUSIONS

SHARED LOCAL CACHE

5.Navigate to **Client Tasks** and choose Software Uninstall task. When creating the uninstall task, we recommend you to reboot the server after the uninstallation by selecting the check box **Automatically**

reboot when needed. Once the task is created, add all desired target computers for uninstallation.

6.Make sure ESET Mail Security is uninstalled from all the targets.

7.Create Software Install task in order to install the latest version of ESET Mail Security to all desired targets.

8.**Assign configuration policy** to all the servers running ESET Mail Security, ideally to a group.

Upgrading via ESET Cluster

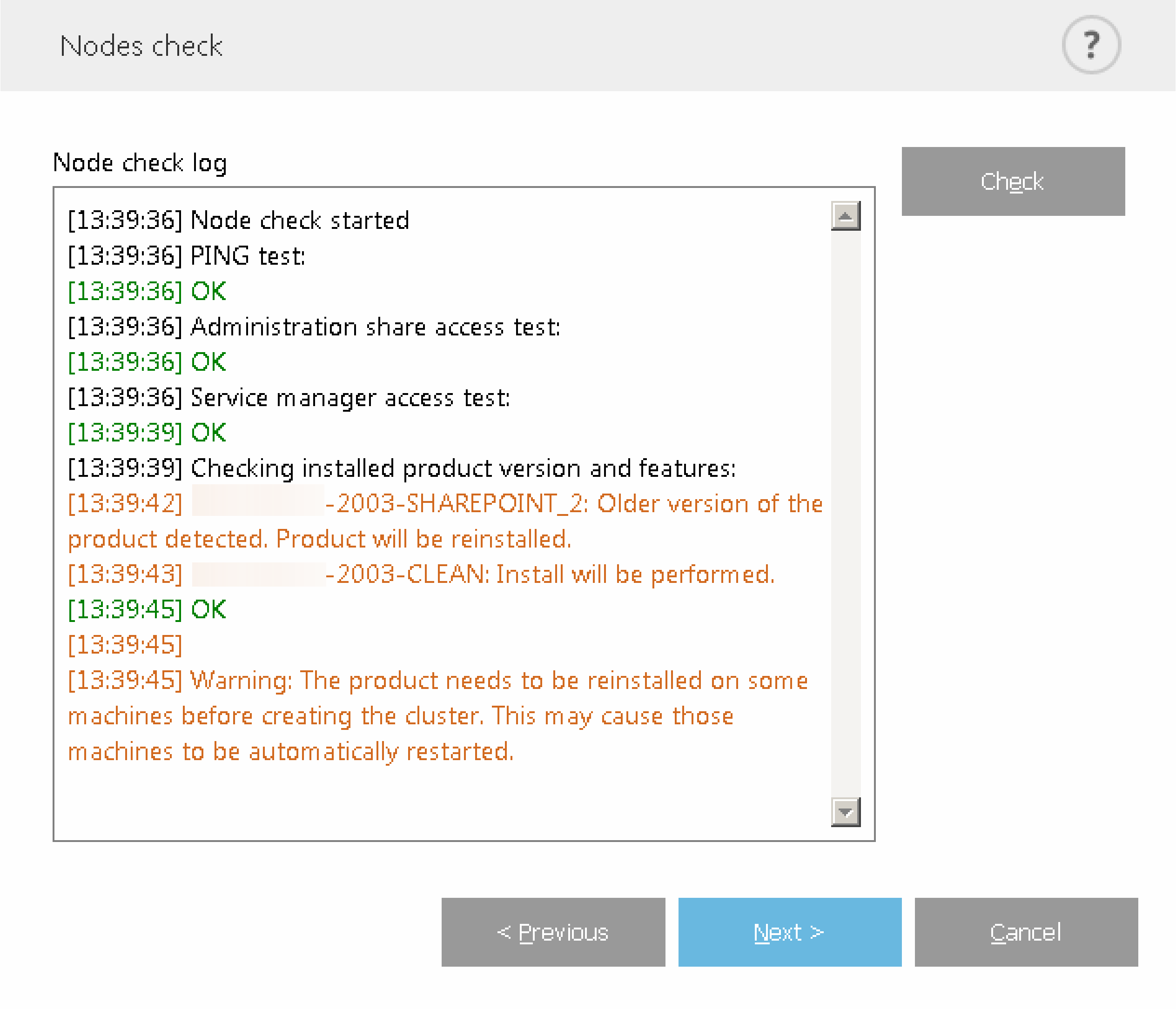
Creating an ESET Cluster lets you upgrade multiple servers using older versions of ESET Mail Security. We recommend using the ESET Cluster method if you have 2 or more servers with ESET Mail Security in your environment. Another benefit of this upgrade method is that you can continue using the ESET Cluster in so the configuration of ESET Mail Security will be synchronized on all member nodes.

Follow the steps below to upgrade using this method:

1.Log on to one of the servers running ESET Mail Security and upgrade it by downloading and installing the latest version over your existing one. Follow the steps for regular installation. All of the original configuration of your old ESET Mail Security will be preserved during the installation.

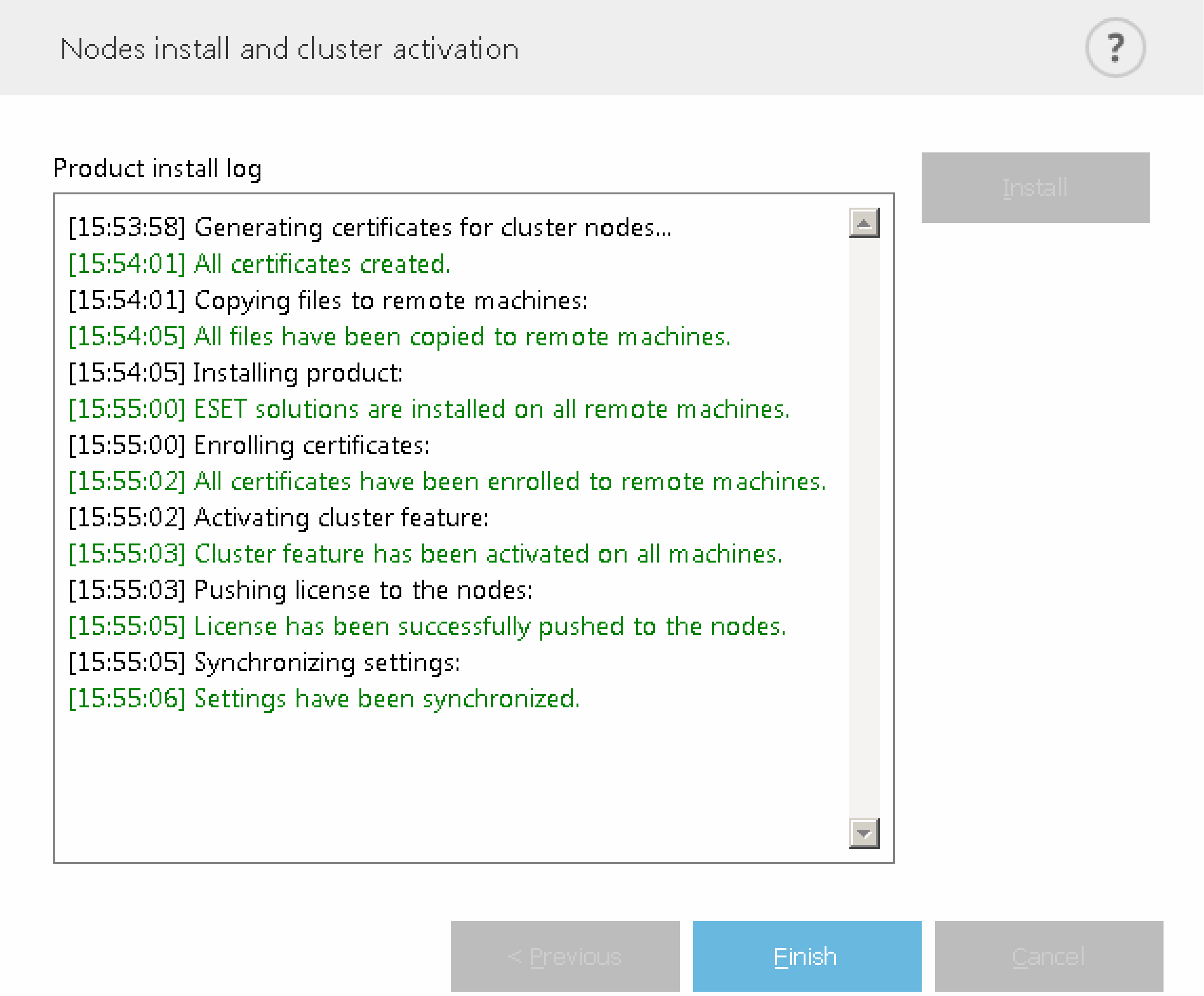
2.Run the ESET Cluster wizard and add cluster nodes (servers you want to upgrade ESET Mail Security on). If required, you can add other servers that do not run ESET Mail Security yet (an installation will be performed on these). We recommend that you to leave the default settings in place when specifying your Cluster name and install type (make sure **Push license to nodes without activated product** is selected).

3.Review the **Nodes check log** screen. It will list servers with older product versions and that the product will be reinstalled. ESET Mail Security will also be installed on any added servers where it is not currently installed.



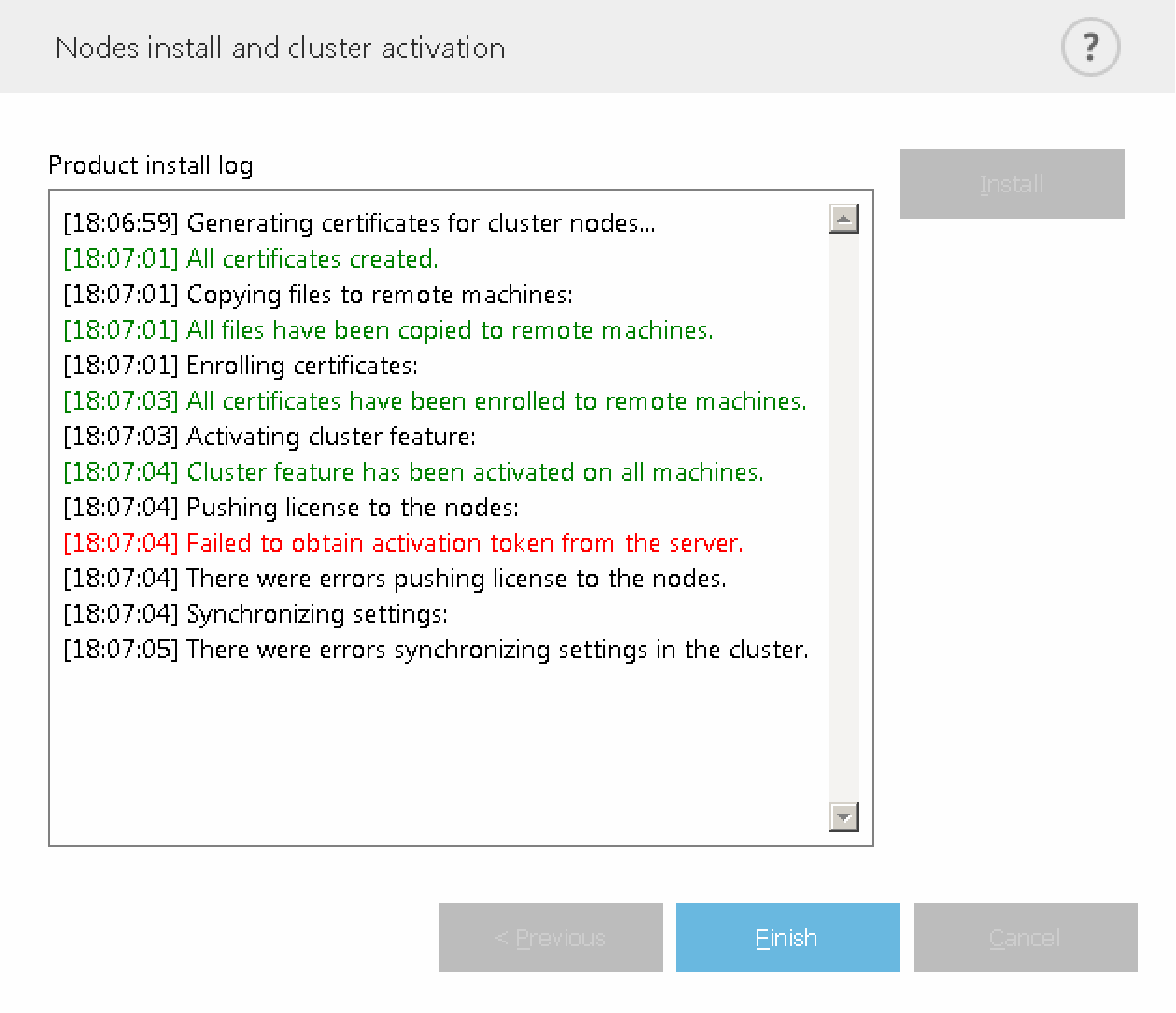
```
[13:39:36] Node check started
[13:39:36] PING test:
[13:39:36] OK
[13:39:36] Administration share access test:
[13:39:36] OK
[13:39:36] Service manager access test:
[13:39:39] OK
[13:39:39] Checking installed product version and features:
[13:39:42] [redacted]-2003-SHAREPOINT_2: Older version of the
product detected. Product will be reinstalled.
[13:39:43] [redacted]-2003-CLEAN: Install will be performed.
[13:39:45] OK
[13:39:45]
[13:39:45] Warning: The product needs to be reinstalled on some
machines before creating the cluster. This may cause those
machines to be automatically restarted.
```

4.The **Nodes install and cluster activation** screen will display installation progress. When installation is successfully completed, it should finish with results similar to these:



```
[15:53:58] Generating certificates for cluster nodes...
[15:54:01] All certificates created.
[15:54:01] Copying files to remote machines:
[15:54:05] All files have been copied to remote machines.
[15:54:05] Installing product:
[15:55:00] ESET solutions are installed on all remote machines.
[15:55:00] Enrolling certificates:
[15:55:02] All certificates have been enrolled to remote machines.
[15:55:02] Activating cluster feature:
[15:55:03] Cluster feature has been activated on all machines.
[15:55:03] Pushing license to the nodes:
[15:55:05] License has been successfully pushed to the nodes.
[15:55:05] Synchronizing settings:
[15:55:06] Settings have been synchronized.
```

If your network or DNS isn't configured correctly, you may receive the error message **Failed to obtain activation token from the server**. Try running the ESET Cluster wizard again. It will destroy the cluster and create a new one (without reinstalling the product) and activation should finish successfully this time. If the issue persists, check your network and DNS settings.



```
[18:06:59] Generating certificates for cluster nodes...
[18:07:01] All certificates created.
[18:07:01] Copying files to remote machines:
[18:07:01] All files have been copied to remote machines.
[18:07:01] Enrolling certificates:
[18:07:03] All certificates have been enrolled to remote machines.
[18:07:03] Activating cluster feature:
[18:07:04] Cluster feature has been activated on all machines.
[18:07:04] Pushing license to the nodes:
[18:07:04] Failed to obtain activation token from the server.
[18:07:04] There were errors pushing license to the nodes.
[18:07:04] Synchronizing settings:
[18:07:05] There were errors synchronizing settings in the cluster.
```

Installation in cluster environment

You can deploy ESET Mail Security in a cluster environment (for example, in a failover cluster). We recommend that you install ESET Mail Security on an active node and then redistribute the installation on passive node(s) using the ESET Cluster feature of ESET Mail Security. Apart from the installation, the ESET Cluster will serve as a replication of ESET Mail Security configuration to ensures consistency between cluster nodes necessary for correct operation.

Terminal Server

If you are installing ESET Mail Security on a Windows Server that acts as a Terminal Server, you may want to disable the ESET Mail Security GUI to prevent it from starting up every time a user logs in. See Disable GUI on Terminal Server for specific steps to disable the GUI.

Multiserver / DAG environment

ESET Mail Security supports for multiserver environments. If your infrastructure consists of multiple servers, for example Database availability group (DAG), you can install ESET Mail Security on each Exchange Server with Mailbox role.

The easiest way is to install ESET Mail Security all servers using ESET Cluster. Also, we recommend you to enable **Use ESET Cluster to store all quarantined messages on one node** in Mail Quarantine settings. If you are planing on using Greylisting, enable Synchronize greylisting databases across the ESET cluster.

Getting started

The following part should help you get started with ESET Mail Security.

Post-installation tasks

Intended to help you with initial configuration.

Monitoring

Gives you an immediate overview of the current status of ESET Mail Security. At the first glance, you will see if there any issues that require your attention.

Managed via ESET Security Management Center

You can use ESET Security Management Center to remotely manage ESET Mail Security.

Post-installation tasks

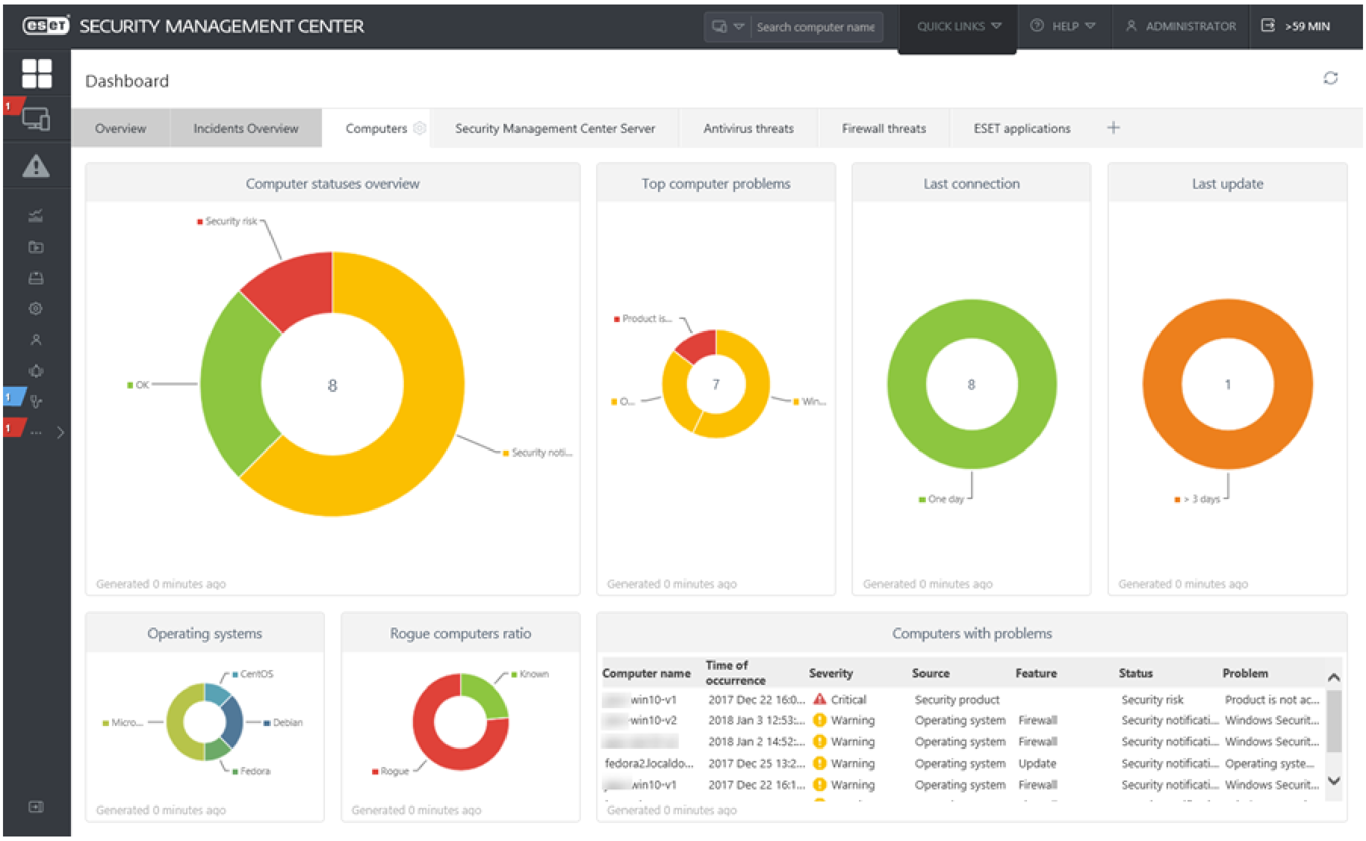
The following are recommended tasks that cover initial configuration of your ESET Mail Security.

Topic	Description
Product Activation	Make sure your ESET Mail Security is activated. You can perform activation in a number of different ways.
Update	Once the product is activated, module update runs automatically. Check the update status to see if the update was successful.
Mail Quarantine manager	Get to know the Mail Quarantine manager which is accessible from the program GUI. This feature enables you to manage quarantined messages such as spam, infected attachments containing malware, phishing messages and messages filtered out by rules. You can see details of each message and take an action (release or delete).
Mail Quarantine Web interface	Mail Quarantine Web interface is an alternative to the Mail Quarantine manager that enables you to manage quarantined items remotely. Additionally, Mail Quarantine Web interface allows users (email recipients) to manage their own quarantined messages. Users can be notified about newly quarantined content with Mail Quarantine reports sent via email. We recommend you to configure the reports.
Mail Quarantine reports	Create a scheduled task to send Mail Quarantine reports to yourself and to selected users to allow them to release (deliver) certain types of false positive messages and to manage their quarantined content via Mail Quarantine Web interface (online viewer). Users will be able to access the Web interface by a clicking a link provided in the Mail Quarantine reports and logging in using their domain credentials.
Antispam - Filtering and verification	Antispam is a sophisticated cloud based functionality that prevent your users (email recipients) from receiving spam. We recommend you to use filtering and verification and add your local IP addresses to the Ignored IP list. IP addresses within your network infrastructure will then be ignored during classification. You can configure and manage the rest of the Approved, Blocked and Ignored lists to customize filtering and verification. You can also enable Greylisting if you decide to use this feature.

Topic	Description
Rules	A powerful feature that enables you to filter email messages based on defined conditions and an actions. Use pre-defined rules (modify if required) or create new, customized rules to fit your needs. Rules can be configured for any of the protection layers (Mail transport protection, Mailbox database protection or On-demand mailbox database scan).
Antivirus test	Verify that Antivirus protection works correctly.
Antispam test	Verify that Antispam protection works correctly.
Anti-Phishing test	Verify that Anti-Phishing protection works correctly.

Managed via ESET Security Management Center

ESET Security Management Center (ESMC) is an application that allows you to manage ESET products in a networked environment from one central location. The ESET Security Management Center task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats. ESET Security Management Center does not provide protection against malicious code on its own, it relies on the presence of ESET security solutions on each client. ESET security solutions support networks that include multiple platform types. Your network can include a combination of current Microsoft, Linux-based, Mac OS and mobile operating systems.



Computer name	Time of occurrence	Severity	Source	Feature	Status	Problem
[redacted]win10-v1	2017 Dec 22 16:0...	Critical	Security product		Security risk	Product is not ac...
[redacted]win10-v2	2018 Jan 3 12:53:...	Warning	Operating system	Firewall	Security notificati...	Windows Securit...
[redacted]	2018 Jan 2 14:52:...	Warning	Operating system	Firewall	Security notificati...	Windows Securit...
fedora2.localdo...	2017 Dec 25 13:2...	Warning	Operating system	Update	Security notificati...	Operating syste...
[redacted]win10-v1	2017 Dec 22 16:1...	Warning	Operating system	Firewall	Security notificati...	Windows Securit...

For more information about ESMC, see ESET Security Management Center Online help.

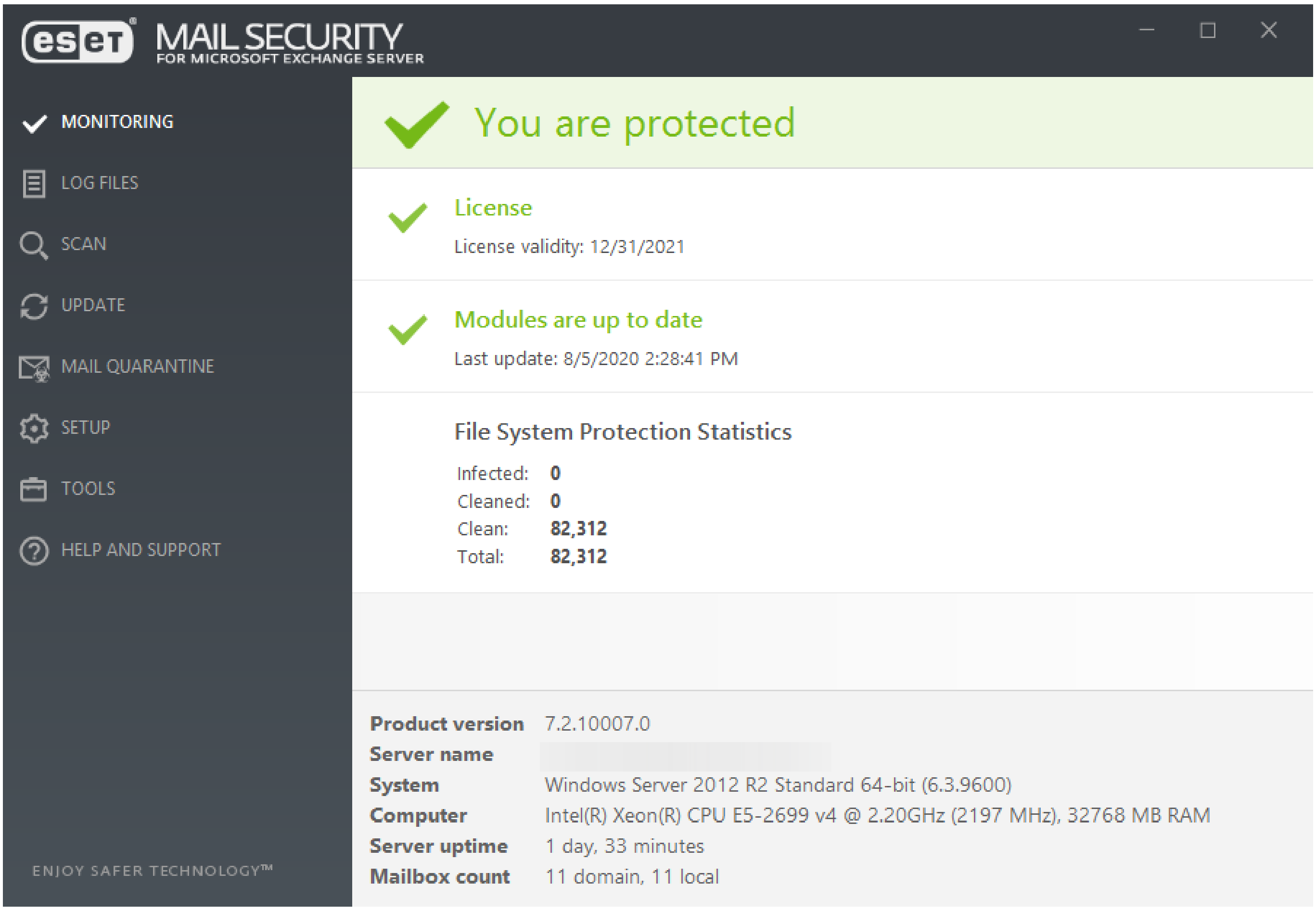
Monitoring

The protection status shown in the **Monitoring** section informs you about the current protection level of your computer. A status summary about the operation of ESET Mail Security will be displayed in the primary window.

✓ The green **You are protected** status indicates that maximum protection is ensured.

⚠ The red icon indicates critical problems - maximum protection of your computer is not ensured. For a list of possible protection statuses see the Status section.

! The orange icon indicates that your ESET product requires attention for a non-critical problem.



You are protected

License
License validity: 12/31/2021

Modules are up to date
Last update: 8/5/2020 2:28:41 PM

File System Protection Statistics

Infected:	0
Cleaned:	0
Clean:	82,312
Total:	82,312

Product version	7.2.10007.0
Server name	[redacted]
System	Windows Server 2012 R2 Standard 64-bit (6.3.9600)
Computer	Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz (2197 MHz), 32768 MB RAM
Server uptime	1 day, 33 minutes
Mailbox count	11 domain, 11 local

Modules that are working properly are assigned a green check. Modules that are not fully functional are assigned a red exclamation point or an orange notification icon. 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 an individual module, click Setup in the main menu and then click the desired module.

The Monitoring page also contains information about your system including:

- **Product version** - version number of ESET Mail Security.
- **Server Name** - machine Hostname or FQDN.
- **System** - operating system details.
- **Computer** - hardware details.
- **Server uptime** - shows how long the system is up and running, basically the opposite of downtime.

Mailbox count

ESET Mail Security detects the number of mailboxes and displays the count based on detection:

- **Domain** - count of all mailboxes in a particular domain to which the Exchange Server belongs.
- **Local** - reflects the count of mailboxes (if any) for the Exchange Server where ESET Mail Security is

installed.

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

Status

A status summary for ESET Mail Security will be displayed in the primary window with detailed information about your system. Normally, when everything is working without any issues, the protection status is ✓ green. However, the protection status might change in certain circumstances. Protection status will change to ❗ orange or ⚠ red, and a warning message will be displayed if one of the following occurs:

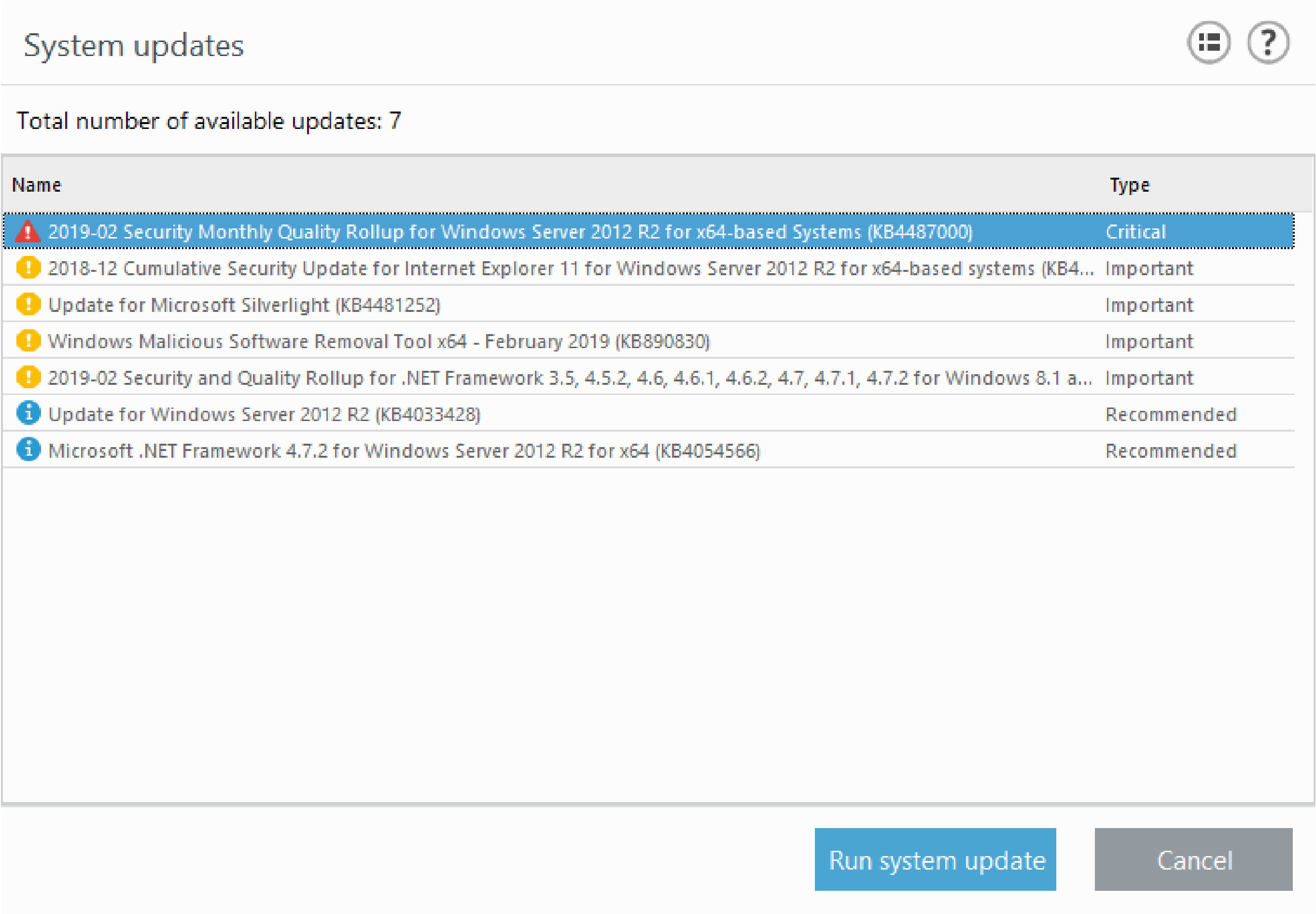
Warning message	Warning message detail
Mail server antivirus protection disabled	Click Enable antivirus protection in the **Monitoring** or re-enable **Antivirus and antispyware protection** in the Setup pane of the main program window.
Mail server integration disabled	Mail server integration was disabled by the user. Click Edit integration setting to enable Mail transport protection.
Antispam engine has limited cloud connectivity	This indicates connection issues. Make sure relevant ports are enabled.
Detection of potentially unwanted application is not configured	A potentially unwanted application (PUA) is a program that contains adware, installs toolbars or has other unclear objectives. There are some situations where a user may feel that the benefits of a potentially unwanted application outweigh the risks.
Product not activated or License expired	This is indicated by the protection status icon turning red. The program is not able to update after the license expires. Follow the instructions in the alert window to renew your license.
ESET LiveGrid® is disabled	This problem is indicated when ESET LiveGrid® disabled in **Advanced setup**.
Real-time file system protection is paused	Click Enable Real-time protection in the **Monitoring** tab or re-enable **Real-time file system protection** in the Setup tab of the main program window.
Operating system is not up to date	The System updates window shows the list of available updates ready to be downloaded and installed.
Your device will soon lose protection	Click See your options for details how to update your version of Microsoft Windows. If you are running **Microsoft Windows Server 2008 R2 SP1**, ensure your system is compatible with SHA-2. Apply the patches according to your particular operating system version.
Computer restart required	Click **Restart computer** if you want to restart your system immediately, or click **Dismiss** if you plan to restart later.
Network attack protection (IDS) is paused	Click Enable Network attack protection (IDS) to re-enable this feature.
Botnet protection is paused	Click Enable Botnet protection to re-enable this feature.
Web access protection is paused	Click Enable Web access protection in the **Monitoring** or re-enable **Web access protection** in the Setup pane of the main program window.
Anti-Phishing protection is non-functional	This feature is not functional because other required program modules are not active.

Warning message	Warning message detail
Policy override active	The configuration set by the policy is temporarily overridden, possibly until troubleshooting is complete. If you are managing ESET Mail Security using ESMC and have a policy assigned to it, the status link will be locked (grayed out) depending on what features belong to the policy.

If you are unable to solve a problem, search the ESET Knowledgebase. If you still need assistance, you can Submit support request. ESET Technical Support will respond quickly to your questions and help find a resolution.

Windows update available

The System updates window shows the list of available updates ready to be downloaded and installed. The update priority level is shown next to the name of the update. Right-click any update row and click **More information** to display a pop-up window with additional info:



System updates

Total number of available updates: 7

Name	Type
2019-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4487000)	Critical
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB4...	Important
Update for Microsoft Silverlight (KB4481252)	Important
Windows Malicious Software Removal Tool x64 - February 2019 (KB890830)	Important
2019-02 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 a...	Important
Update for Windows Server 2012 R2 (KB4033428)	Recommended
Microsoft .NET Framework 4.7.2 for Windows Server 2012 R2 for x64 (KB4054566)	Recommended

Click **Run system update** to open **Windows Update** window and proceed with system updates.

Network isolation

ESET Mail Security provides you with an option to block network connection of your server called network isolation. In some extreme scenarios, you may want to isolate a server from the network as preventive measure. For example, if you found the server has been infected with a malware or the machine has otherwise been compromised.

By activating the network isolation, all network traffic is blocked except the following:

- Connectivity to the Domain Controller remains
- ESET Mail Security is still able to communicate
- If present, ESET Management Agent and ESET Enterprise Inspector Agent can communicate over the network

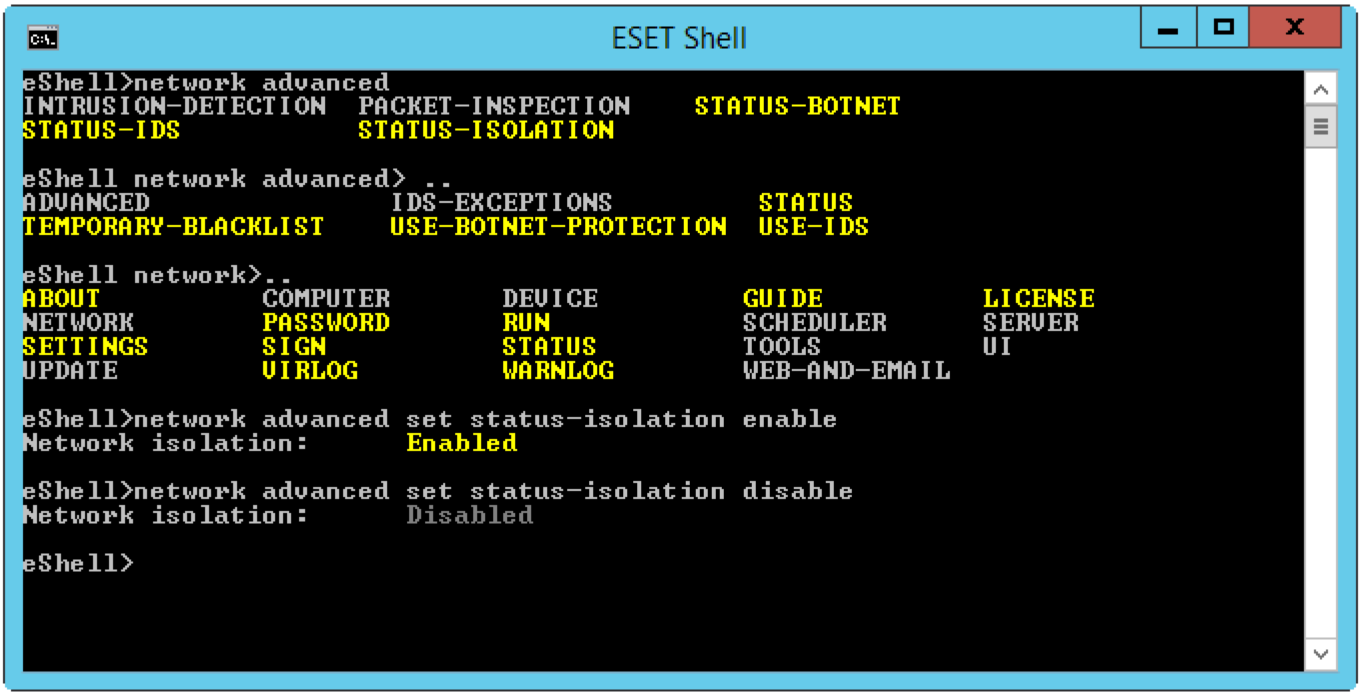
Activate and deactivate network isolation using eShell command or ESET Security Management Center client task.

eShell

In interactive mode:

- Activate network isolation: `network advanced set status-isolation enable`

- Deactivate network isolation: `network advanced set status-isolation disable`



```
eShell>network advanced
INTRUSION-DETECTION   PACKET-INSPECTION    STATUS-BOTNET
STATUS-IDS            STATUS-ISOLATION

eShell network advanced> ..
ADVANCED                IDS-EXCEPTIONS          STATUS
TEMPORARY-BLACKLIST     USE-BOTNET-PROTECTION   USE-IDS

eShell network>..
ABOUT          COMPUTER       DEVICE         GUIDE          LICENSE
NETWORK        PASSWORD       RUN            SCHEDULER      SERVER
SETTINGS       SIGN           STATUS         TOOLS          UI
UPDATE         VIRLOG         WARNLOG        WEB-AND-EMAIL

eShell>network advanced set status-isolation enable
Network isolation:        Enabled

eShell>network advanced set status-isolation disable
Network isolation:        Disabled

eShell>
```

Alternatively, you can create and run a batch file using Batch / Script mode.

ESET Security Management Center

- Activate network isolation via client task.

- Deactivate network isolation via client task.

When network isolation is activated, ESET Mail Security status changes to red with a message **Network access blocked**.

Using ESET Mail Security

This part contains detailed description of the program's user interface, and aims to explain how to use your ESET Mail Security.

The user interface enables you to quickly access commonly used features:

- Monitoring
- Log files
- Scan
- Update
- Mail quarantine
- Setup
- Tools

Scan

The On-demand scanner is an important part of ESET Mail Security. It is used to perform scans of files and folders on your computer. To ensure the security of your network, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. We recommend that you perform regular (for example, once a month) in-depth scans of your system to detect viruses not detected by Real-time file system protection. This can occur if a threat is introduced when Real-time file system protection is disabled, the detection engine has not been updated, or if a file was not detected when it was first saved to the disk.

Select available On-demand scans for ESET Mail Security:

Mailbox database scan

> Lets you run On-demand database scan. You can choose Public folders, Mail Servers and Mailboxes to scan. Also, you can use Scheduler to run the database scan at a specific time or at an event.

> NOTE
> If you are running Microsoft Exchange Server 2007 or 2010 you can choose between Mailbox database protection and On-demand database scan, only one protection type can be active at a time. If you decide to use On-demand database scan you will need to disable integration of Mailbox database protection in Advanced setup under Server. Otherwise On-demand database scan will not be available.

Office 365 mailbox scan

> Enables you to scan remote mailboxes in Office 365 hybrid environments. Works the same way as On-demand mailbox database scan.

Storage scan

> Scans all shared folders on the local server. If Storage scan is not available, there are no shared folders on your server.

Scan your computer

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

> NOTE
> We recommend that you run a computer scan at least once a month. Scanning can be configured as a scheduled task.

Custom scan

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

Removable media scan

Similar to Smart scan - quickly launch a scan of removable media (such as CD/DVD/USB) that are connected to the computer. This may be useful when you connect a USB flash drive to a computer and want to scan its content for malware and other potential threats. This type of scan can also be initiated by clicking **Custom scan** and then selecting **Removable media** from the **Scan targets** drop-down menu and clicking **Scan**.

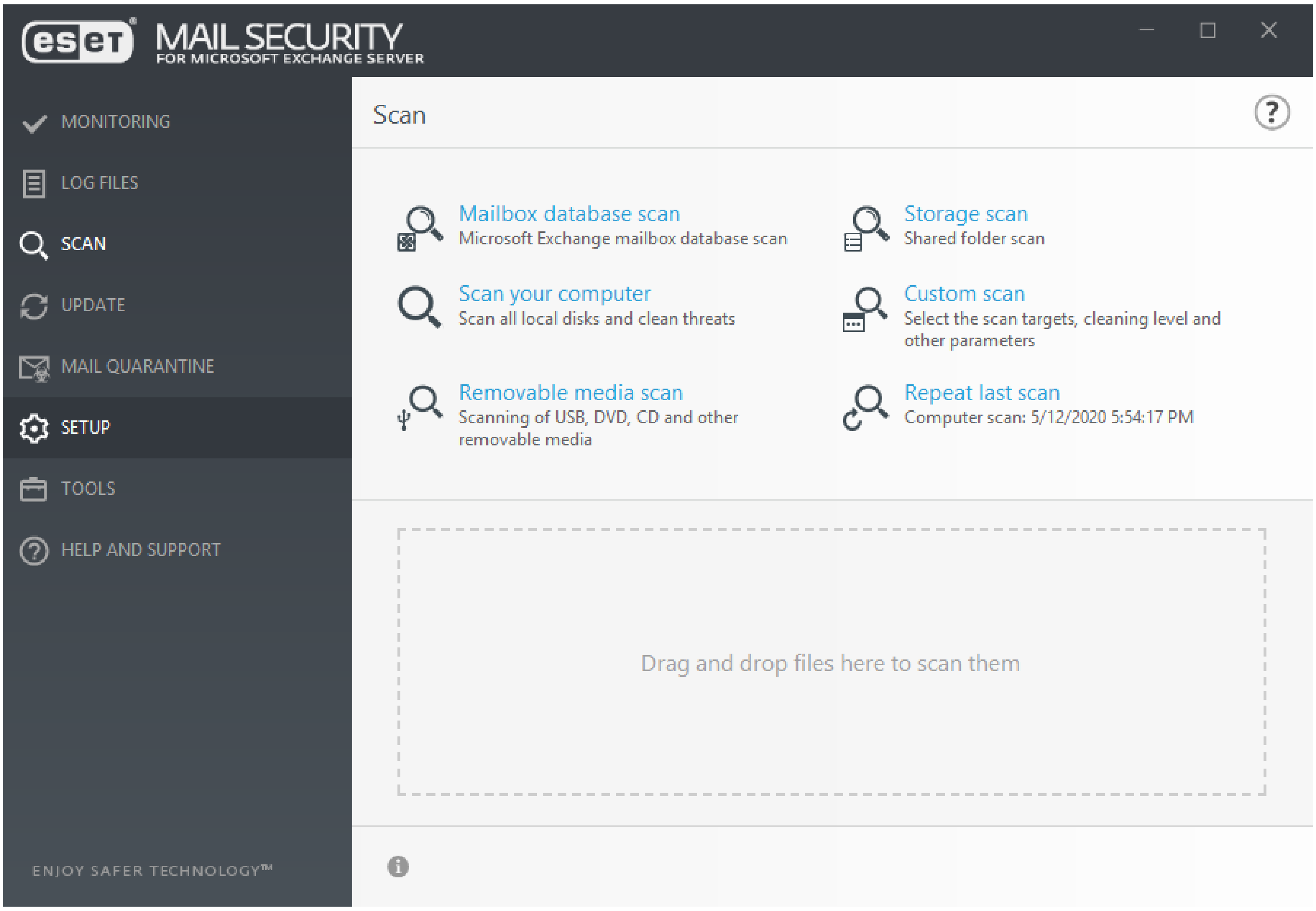
Hyper-V scan

This option is only visible in the menu if Hyper-V Manager is installed on the server that runs ESET Mail Security. Hyper-V scan allows for scanning of Virtual Machine (VM) disks on Microsoft Hyper-V Server without the need to have any "Agent" installed on the particular VM.

Repeat last scan

Repeats your last scan operation using exactly the same settings.

> NOTE
> Repeat last scan function is not available if On-demand database scan is present.


eset MAIL SECURITY FOR MICROSOFT EXCHANGE SERVER
MONITORING
LOG FILES
SCAN
UPDATE
MAIL QUARANTINE
SETUP
TOOLS
HELP AND SUPPORT
ENJOY SAFER TECHNOLOGY™
Scan
Mailbox database scan
Microsoft Exchange mailbox database scan
Storage scan
Shared folder scan
Scan your computer
Scan all local disks and clean threats
Custom scan
Select the scan targets, cleaning level and other parameters
Removable media scan
Scanning of USB, DVD, CD and other removable media
Repeat last scan
Computer scan: 5/12/2020 5:54:17 PM
Drag and drop files here to scan them

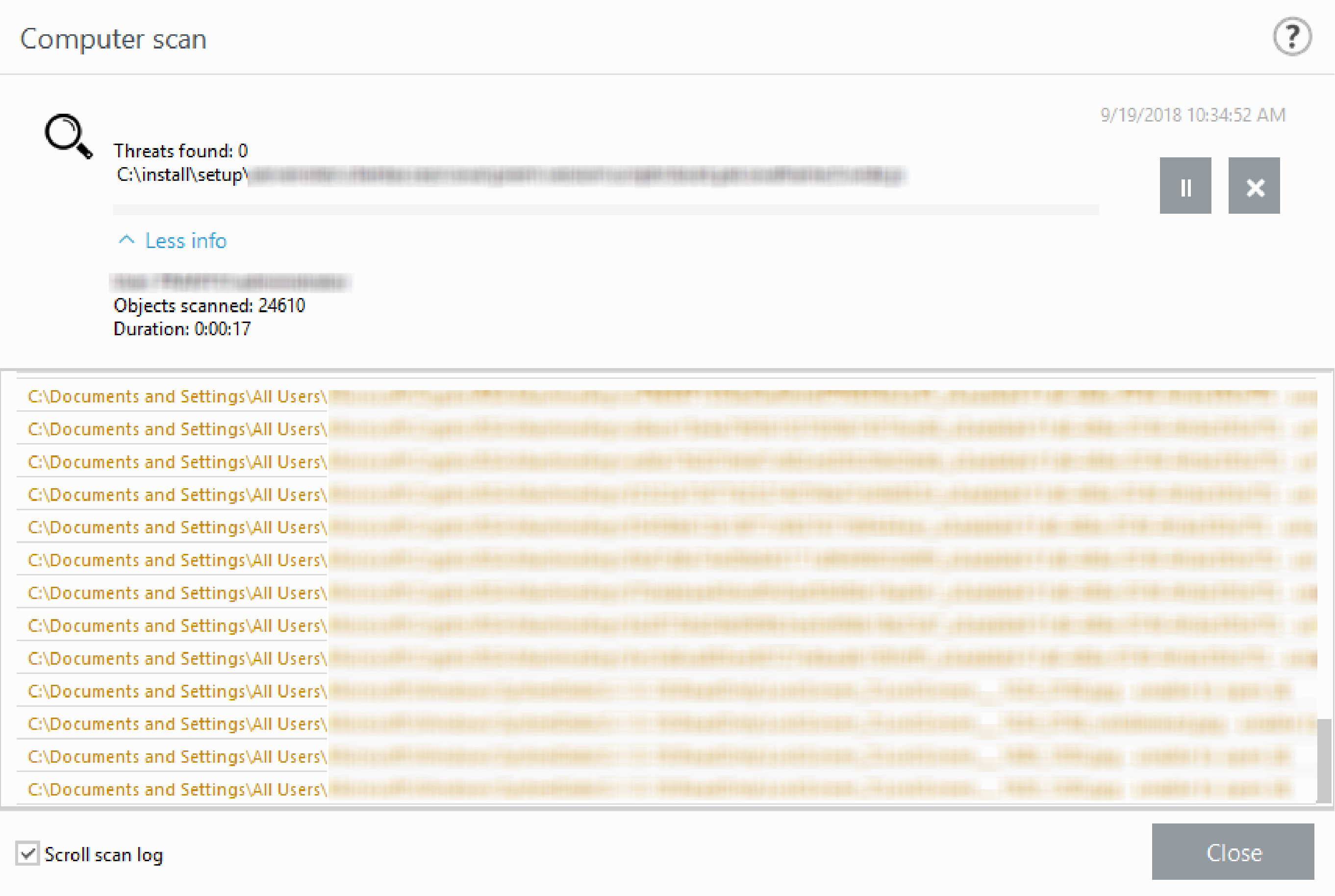
You can use options and shows more information about the scan statuses:

Drag and drop files	You can also drag and drop files into the ESET Mail Security scan window. These files will be virus scanned immediately.
Dismiss/ Dismiss all	Dismissing of give messages.
Scan statuses	Show the status of initial scan. This scan has finished completed or has been interrupted by user.
Show log	Shows more detailed information.
More info	During a scan to see details such as the **User** who executed the scan, number of **Objects scanned** and the scan **Duration**. If On-demand **Database scan** is running, it shows the user who executed the scan, not the actual Database scan account that is being used to connect to EWS (Exchange Web Services) during the scan process.
Open scan windows	The scan progress window shows the current status of the scan and information about the number of files found that contain malicious code.

Scan window and scan log

The scan window shows currently scanned objects including their location, number of threats found (if any), number of scanned objects and scan duration. The bottom part of the window is a scan log that shows detection engine version number, date and time when the scan started and target selection.

Once the scan is in progress, you can click **Pause** if you want to temporarily interrupt the scan. **Resume** option is available when the scan process is paused.



Computer scan

9/19/2018 10:34:52 AM

Threats found: 0
C:\install\setup\[redacted]

Less info

[redacted]
Objects scanned: 24610
Duration: 0:00:17

```
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
C:\Documents and Settings\All Users\[redacted]
```

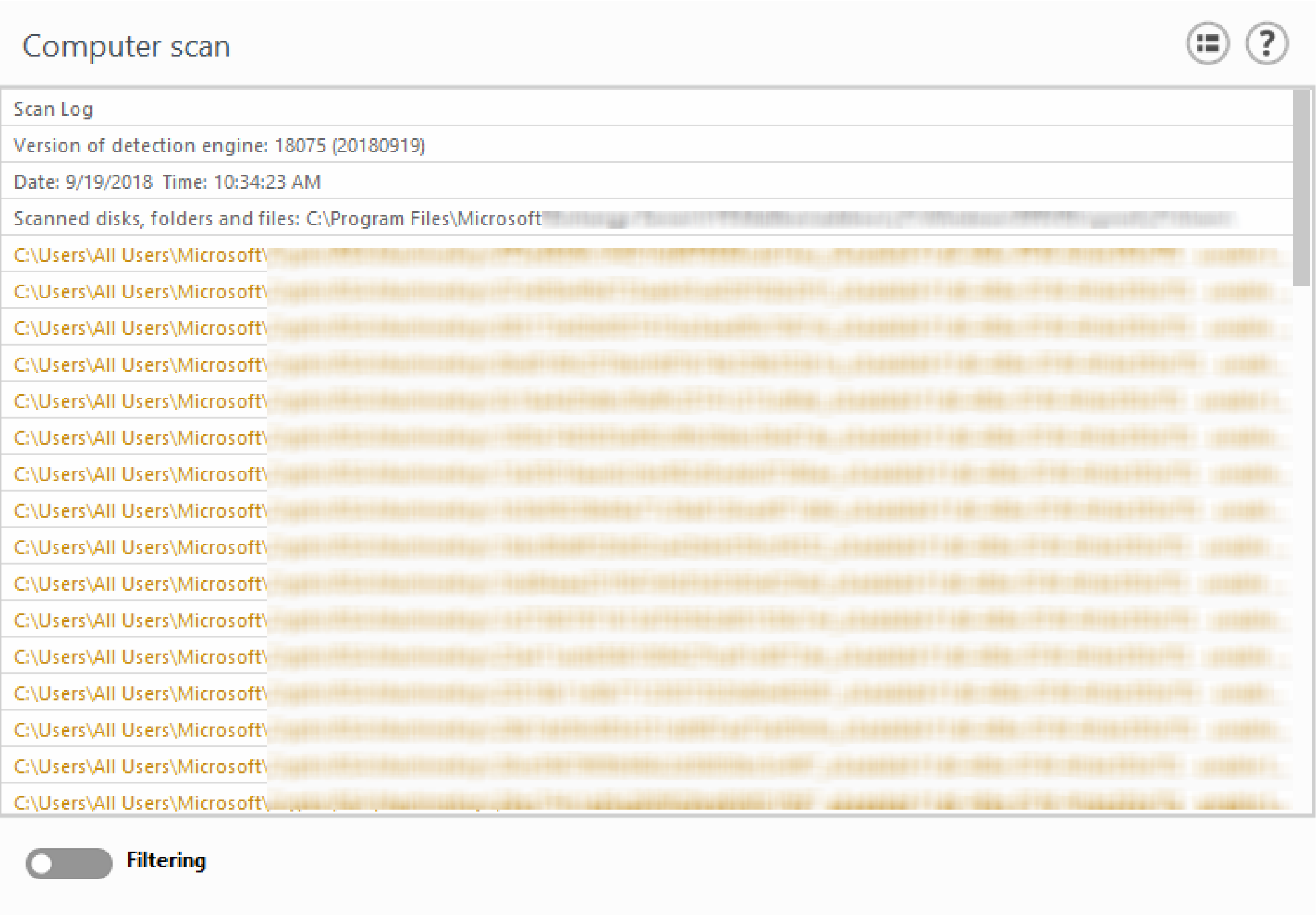
☑ Scroll scan log

Scroll scan log

Leave this option enabled to auto scroll old logs and view active logs in the Log files window.

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

After the scan has finished, you will see the scan log with all relevant information related to the particular scan.


Computer scan

```
Scan Log
Version of detection engine: 18075 (20180919)
Date: 9/19/2018  Time: 10:34:23 AM
Scanned disks, folders and files: C:\Program Files\Microsoft
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
C:\Users\All Users\Microsoft\
```

Click the switch icon **Filtering** to open Log filtering window where you can define filtering or search criteria. To view the context menu, right-click a specific log entry:

Action	Usage	Shortcut	See also
Filter same records	This activates log filtering, showing only records of the same type as the one selected.	Ctrl + Shift + F	
Filter...	After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.		Log filtering
Enable filter	Activates filter settings. The first time you activate filtering, you must define settings.		
Disable filter	Turns filtering off (same as clicking the switch at the bottom).		
Copy	Copies information of selected/highlighted record(s) into the clipboard.	Ctrl + C	
Copy all	Copies information from all records in the window.		
Export...	Exports information of selected/highlighted record(s) into an XML file.		
Export all...	Exports all the information in the window into an XML file.		

Log files

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

Choose the appropriate log type from the drop-down menu. The following logs are available:

Detections

The Detections log offers detailed information about infiltrations detected by ESET Mail Security modules. The information includes the time of detection, name of infiltration, location, the performed action and the name of the user logged in at the time the infiltration was detected. Double-click any log entry to display its details in a separate window. If required, you can create a detection exclusion – right-click a log record (detection) and click **Create exclusion**. This will open the exclusion wizard with pre-defined criteria. If there is a name of a detection next to an excluded file, it means that the file is only excluded for the given detection. If that file becomes infected later with other malware, it will be detected.

Events

All important actions performed by ESET Mail Security are recorded in the event log. The event log contains information about events and errors that have occurred in the program. It is designed to help system administrators and users resolve problems. Often the information found here can help you find a solution for a problem occurring in the program.

Computer scan

All scan results are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view the details of the respective scan.

Blocked files

Contains records of files that were blocked and could not be accessible. The protocol shows the reason and the source module that blocked the file, as well as the application and user that executed the file.

Sent files

Contains records of files Cloud-based protection, ESET Dynamic Threat Defense and ESET LiveGrid®.

HIPS

Contains records of specific rules that are marked for recording. The protocol shows the application that called the operation, the result (whether the rule was permitted or prohibited) and the name of the rule created.

Network protection

Contains records of files that were blocked by Botnet protection and IDS (Network attack protection).

Filtered websites

List of websites that were blocked by Web access protection and Anti-phishing mail protection. These logs display the time, URL, user and application that opened a connection to the particular website.

Device control

Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device type, serial number, vendor name and media size (if available).

Mail server protection

All messages detected by ESET Mail Security as infiltration or as a spam are recorded here. These logs apply to following protection types: Antispam, Anti-Phishing, Rules and Anti-Malware. When you double-click an item, a pop-up window will open with Additional information about detected email message, such as IP address, HELO domain, Message ID, Scan type showing the protection layer it was detected on. Also, you can see the result of Anti-Malware, Anti-Phishing and Antispam scan and the reason why it was detected or whether a Rule was activated.

> NOTE
> Not all processed messages are being logged into a Mail server protection log. However, all of the messages that were actually modified (deleted attachment, custom string added to a message header, etc.) are written into the log.

Mailbox database scan

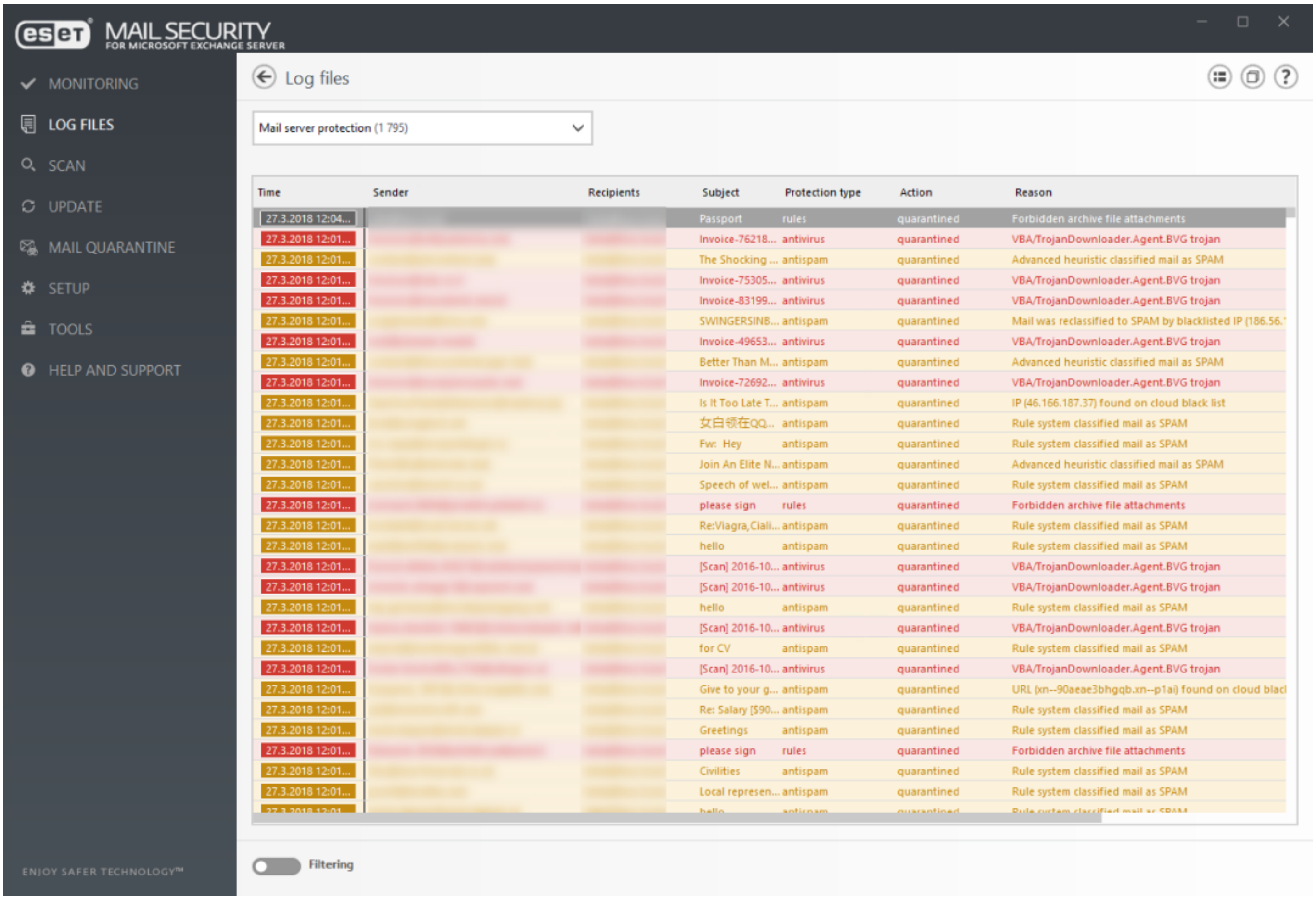
Contains the version of the detection engine, date, scanned location, number of scanned objects, number of threats found, number of rule hits and time of completion.

SMTP protection

All messages that have been evaluated using the greylisting method. SPF and Backscatter are also displayed here. Each record contains HELO Domain, IP sender's and recipient's address, Actions statuses (rejected, rejected [not verified] and verified incoming messages). There are a new action to add subdomain in the greylisting whitelist, see table below

Hyper-V scan

Contains a list of Hyper-V scan results. Double-click any entry to view the details of the respective scan.



Mail server protection (1 795)

Time	Sender	Recipients	Subject	Protection type	Action	Reason
27.3.2018 12:04...	[redacted]	[redacted]	Passport	rules	quarantined	Forbidden archive file attachments
27.3.2018 12:01...	[redacted]	[redacted]	Invoice-76218...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	The Shocking ...	antispam	quarantined	Advanced heuristic classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	Invoice-75305...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	Invoice-83199...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	SWINGERSINB...	antispam	quarantined	Mail was reclassified to SPAM by blacklisted IP (186.56.'
27.3.2018 12:01...	[redacted]	[redacted]	Invoice-49653...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	Better Than M...	antispam	quarantined	Advanced heuristic classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	Invoice-72692...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	Is It Too Late T...	antispam	quarantined	IP (46.166.187.37) found on cloud black list
27.3.2018 12:01...	[redacted]	[redacted]	女白领在QQ...	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	Fw: Hey	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	Join An Elite N...	antispam	quarantined	Advanced heuristic classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	Speech of wel...	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	please sign	rules	quarantined	Forbidden archive file attachments
27.3.2018 12:01...	[redacted]	[redacted]	Re:Viagra,Ciali...	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	hello	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	[Scan] 2016-10...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	[Scan] 2016-10...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	hello	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	[Scan] 2016-10...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	for CV	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	[Scan] 2016-10...	antivirus	quarantined	VBA/TrojanDownloader.Agent.BVG trojan
27.3.2018 12:01...	[redacted]	[redacted]	Give to your g...	antispam	quarantined	URL (xn--90aeae3bhgqb.xn--p1ai) found on cloud blacl
27.3.2018 12:01...	[redacted]	[redacted]	Re: Salary [$90...	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	Greetings	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	please sign	rules	quarantined	Forbidden archive file attachments
27.3.2018 12:01...	[redacted]	[redacted]	Civilities	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01...	[redacted]	[redacted]	Local represen...	antispam	quarantined	Rule system classified mail as SPAM
27.3.2018 12:01	[redacted]	[redacted]	hello	antispam	quarantined	Rule system classified mail as SPAM

Context menu (right-click) enables you to choose an action with selected log record:

Action	Usage	Shortcut	See also
Show	Shows more detailed information about the selected log in a new window (same as double-click).		
Filter same records	This activates log filtering, showing only records of the same type as the one selected.	Ctrl + Shift + F	
Filter...	After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.		Log filtering
Enable filter	Activates filter settings. The first time you activate filtering, you must define settings.		
Disable filter	Turns filtering off (same as clicking the switch at the bottom).		
Copy	Copies information of selected/highlighted record(s) into the clipboard.	Ctrl + C	
Copy all	Copies information from all records in the window.		
Delete	Deletes selected/highlighted record(s) - this action requires administrator privileges.	Del	
Delete all	Deletes all record(s) in the window - this action requires administrator privileges.		
Export...	Exports information of selected/highlighted record(s) into an XML file.		
Export all...	Exports all the information in the window into an XML file.		
Find...	Opens Find in log window and lets you define search criteria. You can use the find feature to locate a specific record even while filtering is on.	Ctrl + F	Find in log
Find next	Finds the next occurrence of your defined search criteria.	F3	

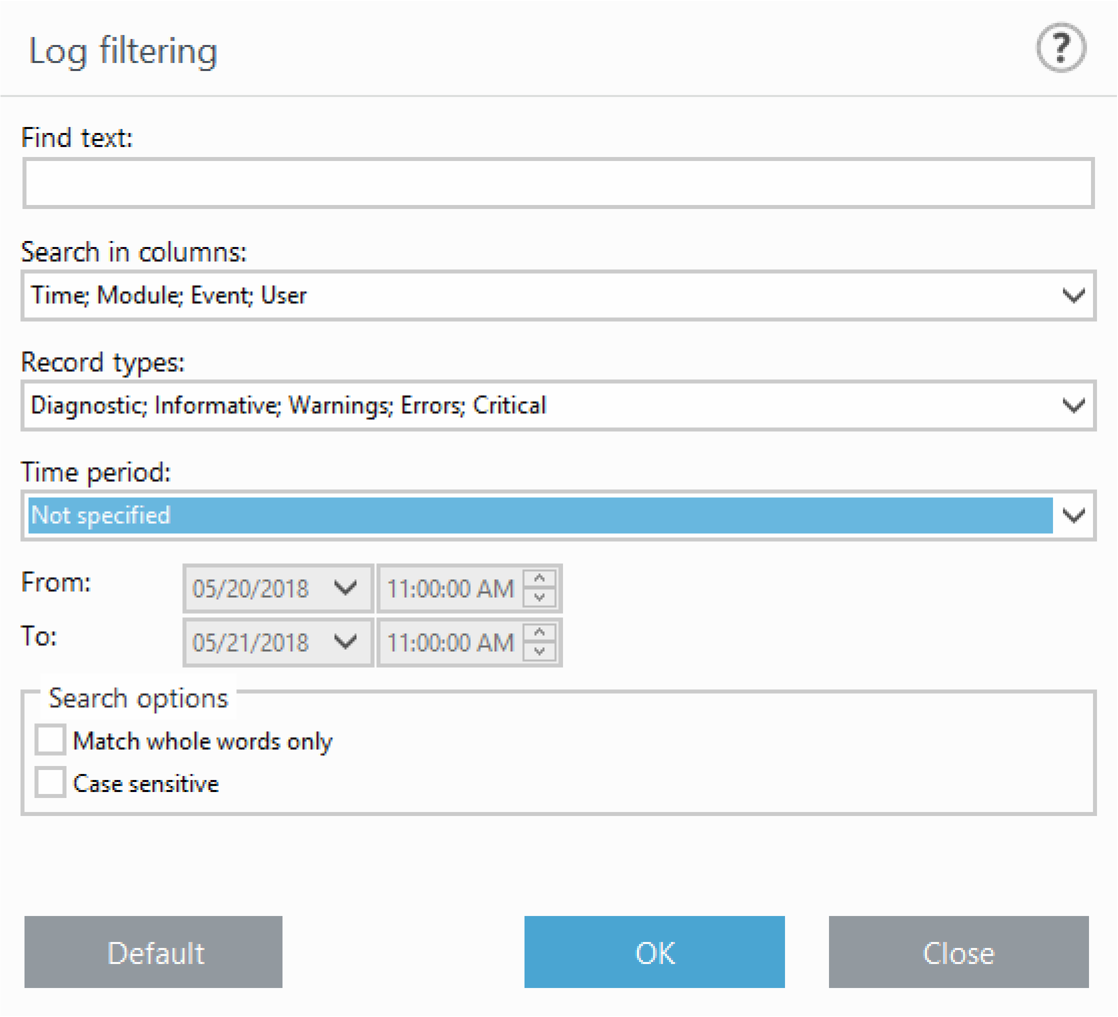
Action	Usage	Shortcut	See also
Find previous	Finds the previous occurrence.	Shift + F3	
Create exclusion	To exclude objects from cleaning using the detection name, path or its hash.		Create exclusion

Add IP address to greylisting whitelist	Adds sender's IP address to the IP whitelist. You can find the IP whitelist under Greylisting and SPF section of Filtering and verification. This applies to items logged by Greylisting or SPF.	
Add domain to greylisting and SPF whitelist	Adds sender's domain to the Domain to IP whitelist. Only domain is added, subdomain is ignored. For example, if sender's address is `sub.domain.com`, only `domain.com` is added to the whitelist. You can find the Domain to IP whitelist under Greylisting and SPF section of Filtering and verification. This applies to items logged by Greylisting.	
Add subdomain to greylisting and SPF whitelist	Adds sender's subdomain to the Domain to IP whitelist. Whole domain is added, including its subdomain (for example `sub.domain.com`). This gives you more flexibility for filtering, if required. You can find the Domain to IP whitelist under Greylisting and SPF section of Filtering and verification. This applies to items logged by Greylisting.	

Log filtering

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

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



Log filtering

Find text:

Search in columns: Time; Module; Event; User

Record types: Diagnostic; Informative; Warnings; Errors; Critical

Time period: Not specified

From: 05/20/2018 11:00:00 AM

To: 05/21/2018 11:00:00 AM

Search options

□ Match whole words only

□ Case sensitive

Find text

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

Search in columns

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

Record types

Choose one or more log record types from the drop-down menu:

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

Time period

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

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

Match whole words only

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

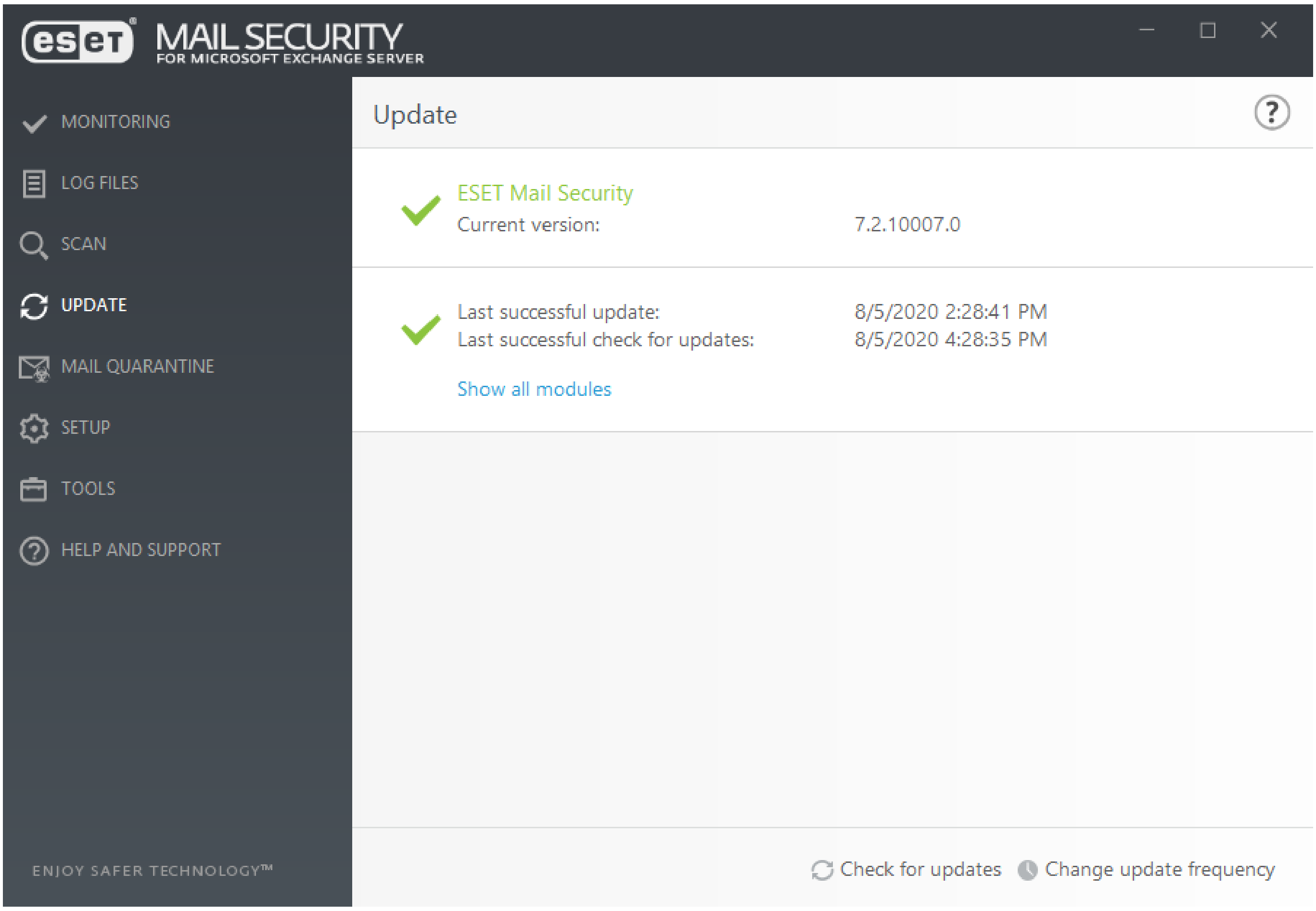
Case sensitive

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

Update

In the Update section, you can see the current update status of your ESET Mail Security, including the date and time of the last successful update. Regularly updating ESET Mail Security is the best method to maintain the maximum level of security on your server. The Update module ensures that the program is always up to date in two ways, by updating detection engine and system components. Updating detection engine and program components is an important part of providing complete protection against malicious code.

> NOTE
> If you did not enter License key yet, you will not be able to receive updates and will be prompted to activate your product. To do so, navigate to **Help and support** > **Activate Product**.



ESET Mail Security

Current version:	7.2.10007.0
Last successful update:	8/5/2020 2:28:41 PM
Last successful check for updates:	8/5/2020 4:28:35 PM

Current version

The ESET Mail Security build version.

Last successful update

The date of the last update. Make sure it refers to a recent date, which means that the modules is current.

Last successful check for updates

The date of the last attempt to update modules.

Show all modules

To open the list of installed modules.

Check for Updates

Updating modules is important parts of maintaining complete protection against malicious code.

Change update frequency

You can edit task timing for scheduler task Regular automatic update.

If you do not check for Updates as soon as possible, one of the following messages will be displayed:

Error message	Descriptions
Modules update is out of date	This error will appear after several unsuccessful attempts to module update. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured connection settings.
Modules update failed - Product is not activated	The license key has been entered incorrectly in update setup. We recommend that you check your authentication data. The **Advanced setup** (**F5**) contains additional update options. Click **Help and support** > Manage license from the main menu to enter a new license key.
An error occurred while downloading update files	This can be caused by Internet connection settings. We recommend that you check your Internet connectivity by opening any website in your web browser. If the website does not open, it is likely that an Internet connection is not established or there are connectivity problems with your computer. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.
Modules update failed Error 0073	Click **Update** > **Check for updates**, for more information visit this Knowledgebase article.

NOTE
Proxy server options for various update profiles may differ. If this is the case, configure the different update profiles in **Advanced setup** (**F5**) by clicking **Update** > Profile.

Mail Quarantine

Email messages and their components, such as attachments, are put into Mail quarantine instead of traditional file quarantine. The Mail Quarantine provides for a more convenient way of managing spam, infected attachments containing malware or phishing messages. There are different reasons why email messages are put into the Mail Quarantine, depending on which ESET Mail Security protection module handles the message (Anti-Malware, Antispam, Anti-Phishing, Sender Spoofing protection or Rules).

Filtering by icons

You can use icons to filter messages in order to see attachments, emails or emails with attachments only.

Timespan

Select the time span for which you want to see quarantined emails. When you select **Custom**, you can specify a range (**Date from** and **Date to**).

Quick search

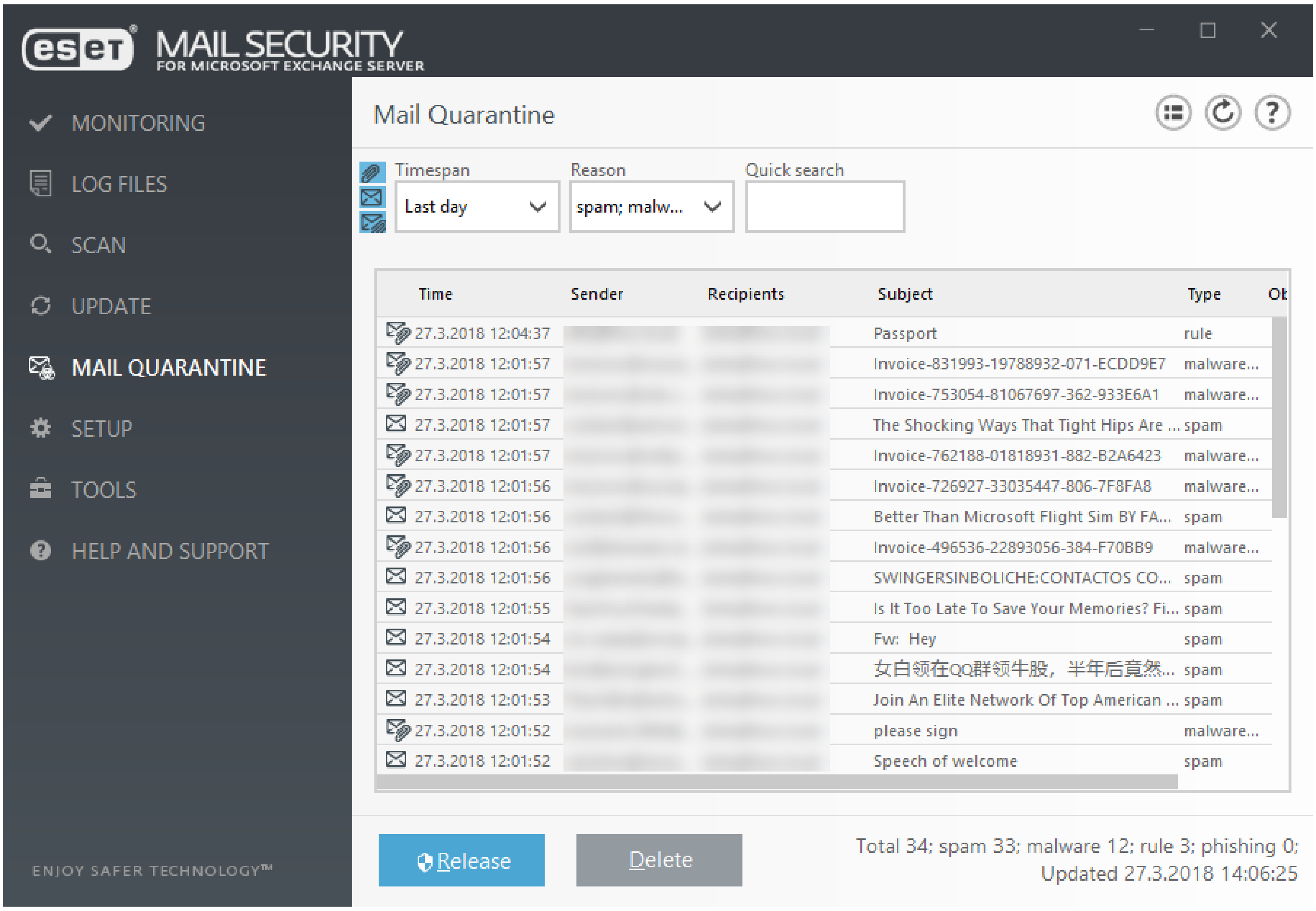
Enter a string into the text box to filter displayed emails (all columns are searched).

Reason

Use check boxes to further filter by type (spam, malware, rule or phishing).

IMPORTANT

Mail Quarantine manager data is not updated automatically, we recommend that you click **Refresh** ↻ regularly to see the most current items in the Mail Quarantine.



Mail Quarantine

Timespan: Last day

Reason: spam; malw...

Quick search:

Time	Sender	Recipients	Subject	Type	Ob
27.3.2018 12:04:37	[redacted]	[redacted]	Passport	rule	
27.3.2018 12:01:57	[redacted]	[redacted]	Invoice-831993-19788932-071-ECDD9E7	malware...	
27.3.2018 12:01:57	[redacted]	[redacted]	Invoice-753054-81067697-362-933E6A1	malware...	
27.3.2018 12:01:57	[redacted]	[redacted]	The Shocking Ways That Tight Hips Are ...	spam	
27.3.2018 12:01:57	[redacted]	[redacted]	Invoice-762188-01818931-882-B2A6423	malware...	
27.3.2018 12:01:56	[redacted]	[redacted]	Invoice-726927-33035447-806-7F8FA8	malware...	
27.3.2018 12:01:56	[redacted]	[redacted]	Better Than Microsoft Flight Sim BY FA...	spam	
27.3.2018 12:01:56	[redacted]	[redacted]	Invoice-496536-22893056-384-F70BB9	malware...	
27.3.2018 12:01:56	[redacted]	[redacted]	SWINGERSINBOLICHE:CONTACTOS CO...	spam	
27.3.2018 12:01:55	[redacted]	[redacted]	Is It Too Late To Save Your Memories? Fi...	spam	
27.3.2018 12:01:54	[redacted]	[redacted]	Fw: Hey	spam	
27.3.2018 12:01:54	[redacted]	[redacted]	女白领在QQ群领牛股，半年后竟然...	spam	
27.3.2018 12:01:53	[redacted]	[redacted]	Join An Elite Network Of Top American ...	spam	
27.3.2018 12:01:52	[redacted]	[redacted]	please sign	malware...	
27.3.2018 12:01:52	[redacted]	[redacted]	Speech of welcome	spam	

Total 34; spam 33; malware 12; rule 3; phishing 0;
Updated 27.3.2018 14:06:25

Release

Releases email to its original recipient(s) using Replay directory and deletes it from quarantine. Click **Yes** to confirm the action. If quarantined item is an attachment from mail-disabled public folder, Release button is not available.

> NOTE
> When releasing an email from quarantine, ESET Mail Security ignores `To:` MIME header because it can be easily spoofed. Instead, it uses the original recipient information from `RCPT TO:` command acquired during the SMTP connection. This ensures that correct email recipient receives the message which is being released from quarantine.

Delete

Deletes item from quarantine. Click **Yes** to confirm the action. Items deleted via GUI are removed from the quarantine view, but are still kept in storage. These are automatically deleted later (after 3 days by default).

Restore to

This option enables you to restore an attachment(s) to a specified location. It is available for attachments only (it will be grayed out for messages). If you need to process whole message, use **Release** feature for this purpose.

Quarantine mail details

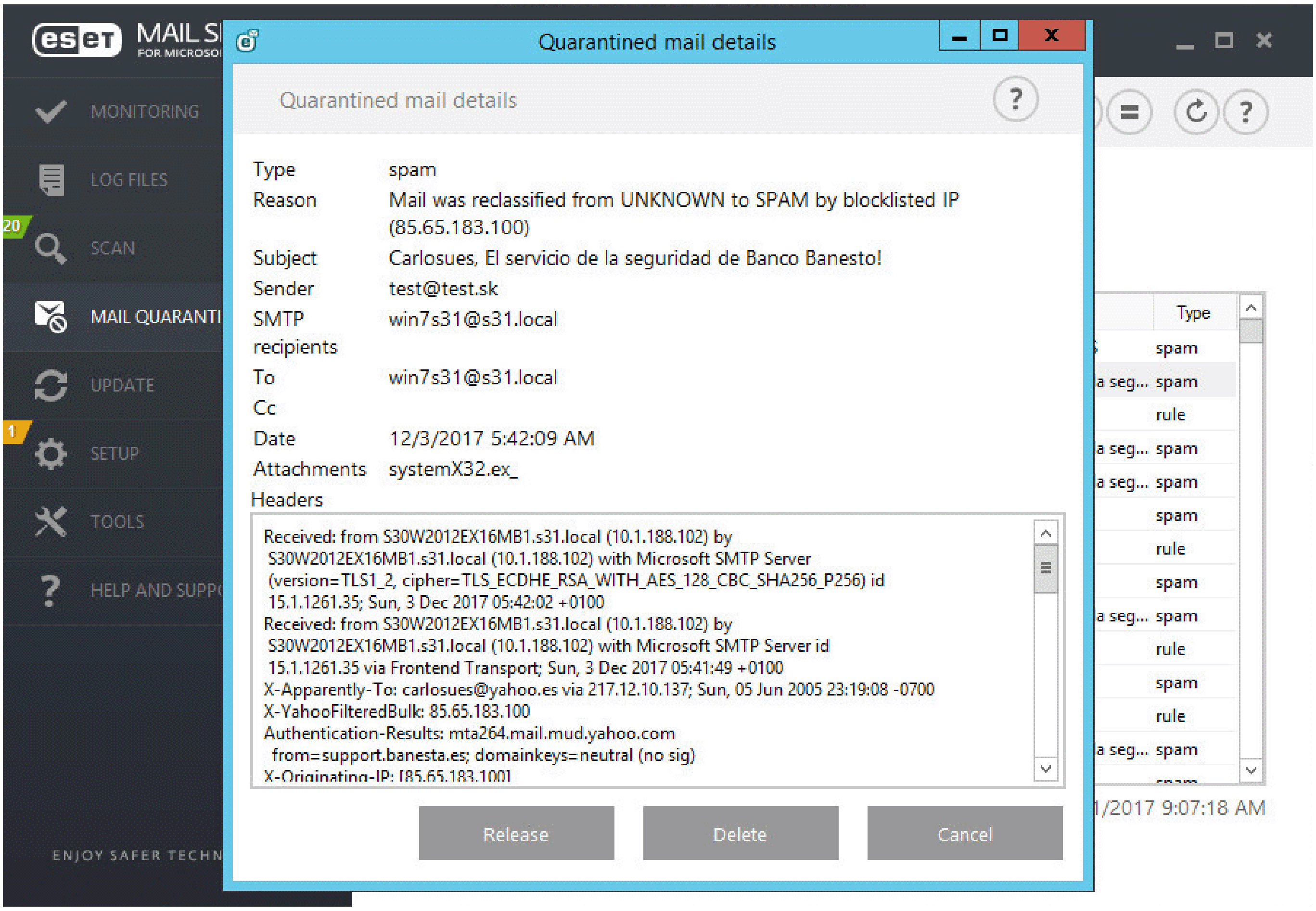
Double click quarantined message or right-click and select **Details**, a pop-up window will open with details about the quarantined email message. You can also find some additional information about the email in the

RFC email header.

Quarantine attachment details

When an attachment is double-clicked, the detail dialog is different compared to email message detail dialog. RFC headers are not available, instead an area with an attachment envelope text is displayed. You can enter custom text of attachment envelope when releasing it from mail quarantine.

Actions are also available from the context menu. If desired, click **Release**, **Delete** or **Delete permanently** to take an action with a quarantined email message. Click **Yes** to confirm the action. If you choose **Delete permanently** the message will be deleted from the file system as well, as opposed to **Delete** which will remove the item from Mail Quarantine manager view.



Type	spam
Reason	Mail was reclassified from UNKNOWN to SPAM by blocklisted IP (85.65.183.100)
Subject	Carlosues, El servicio de la seguridad de Banco Banesto!
Sender	test@test.sk
SMTP recipients	win7s31@s31.local
To	win7s31@s31.local
Cc	
Date	12/3/2017 5:42:09 AM
Attachments	systemX32.ex_

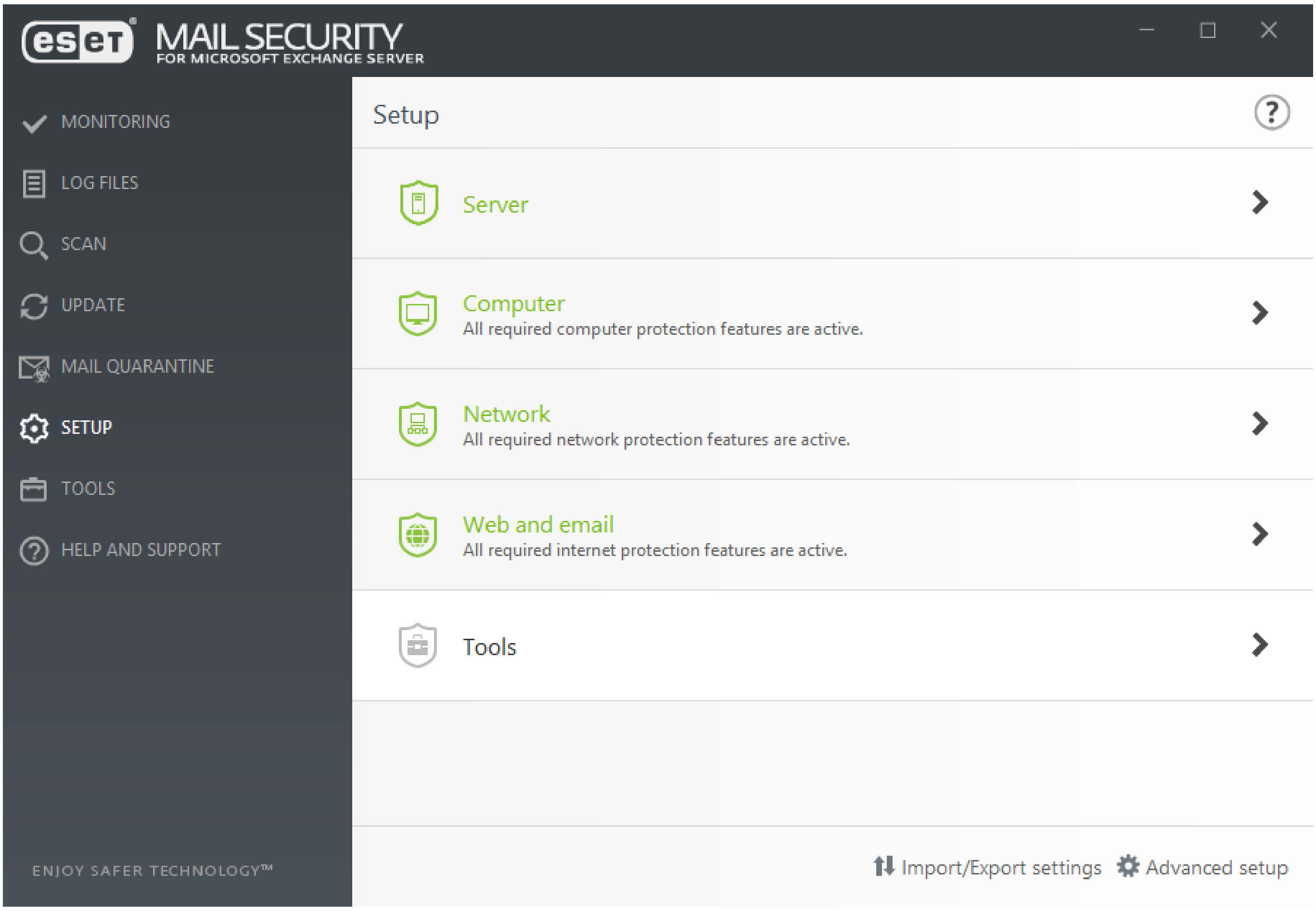
Headers

```
Received: from S30W2012EX16MB1.s31.local (10.1.188.102) by
 S30W2012EX16MB1.s31.local (10.1.188.102) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1261.35; Sun, 3 Dec 2017 05:42:02 +0100
Received: from S30W2012EX16MB1.s31.local (10.1.188.102) by
 S30W2012EX16MB1.s31.local (10.1.188.102) with Microsoft SMTP Server id
 15.1.1261.35 via Frontend Transport; Sun, 3 Dec 2017 05:41:49 +0100
X-Apparently-To: carlosues@yahoo.es via 217.12.10.137; Sun, 05 Jun 2005 23:19:08 -0700
X-YahooFilteredBulk: 85.65.183.100
Authentication-Results: mta264.mail.mud.yahoo.com
  from=support.banesta.es; domainkeys=neutral (no sig)
X-Originating-IP: [85.65.183.100]
```

Setup

The Setup menu window contains the following sections:

- Server
- Computer
- Network
- Web and email
- Tools - Diagnostic logging



All required computer protection features are active.

All required network protection features are active.

All required internet protection features are active.

To temporarily disable individual modules, next to the appropriate module, click the green slider bar 🟩. This may decrease the protection level of your server.

To re-enable the protection of a disabled security component, next to the appropriate module, click the red slider bar 🟥. The component is returned to an enabled state.

To access detailed settings of a specific security component, click the gear icon ⚙.

Import/Export settings

Load setup parameters using an *.xml* configuration file or save the current setup parameters to a configuration file.

Advanced setup

Configure advanced settings and options based on your needs. To access the **Advanced setup** screen from anywhere in the program, press **F5**.

Server

You will see a list of components that you can enable/disable using the slider bar 🟩. To configure settings for a specific item, click the gear icon ⚙.

Antivirus protection

Guards against malicious system attacks by controlling file, email and Internet communication.

Antispam protection

Integrates several technologies (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Rules, Manual whitelisting/blacklisting, etc.) to achieve maximum detection of email threats.

Anti-phishing protection

Parses message body of incoming emails for phishing links (URL's).

Automatic exclusions

Identifies critical server applications and server operating system files and automatically adds them to the list of exclusions. This functionality will minimize the risk of potential conflicts and increase the overall performance of the server when running threat detection software.

Cluster

To configure and activate the ESET Cluster.

To temporarily disable individual modules, next to the appropriate module, click the green slider bar. This may decrease the protection level of your server.

To re-enable the protection of a disabled security component, next to the appropriate module, click the red slider bar. The component is returned to an enabled state.

To access detailed settings of a specific security component, click the gear icon ⚙.

Import/Export settings

Load setup parameters using an *.xml* configuration file or save the current setup parameters to a configuration file.

Advanced setup

Configure advanced settings and options based on your needs. To access the **Advanced setup** screen from anywhere in the program, press **F5**.

Computer

ESET Mail Security has all of the necessary components to ensure significant protection of the server as a computer. This module allows you to enable/disable and configure the following components:

Real-time file system protection

All files are scanned for malicious code when they are opened, created or run on your computer. For Real-time file system protection, there is also an option to **Configure** or **Edit exclusions** which will open the exclusions setup window where you can exclude files and folders from scanning.

Device control

This module allows you to scan, block or adjust extended filters/permissions and define a user's ability to access and work with a given device.

Host Intrusion Prevention System (HIPS)

System monitors events that occur within the operating system and reacts to them according to a customized set of rules.

- Advanced memory scanner
- Exploit blocker
- Ransomware shield

Presentation mode

A feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. You will receive a warning message (potential security risk) and the main program window will turn orange after enabling Presentation mode.

Pause Antivirus and antispyware protection

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

To temporarily disable individual modules, next to the appropriate module, click the green slider bar . This may decrease the protection level of your server.

To re-enable the protection of a disabled security component, next to the appropriate module, click the red slider bar . The component is returned to an enabled state.

To access detailed settings of a specific security component, click the gear icon .

Import/Export settings

Load setup parameters using an *.xml* configuration file or save the current setup parameters to a configuration file.

Advanced setup

Configure advanced settings and options based on your needs. To access the **Advanced setup** screen from anywhere in the program, press **F5**.

Network

This is accomplished by allowing or denying individual network connections based on your filtering rules. It provides protection against attacks from remote computers and blocks some potentially dangerous services.

The Network module allows you to enable/disable and configure the following components:

Network attack protection (IDS)

Analyzes the content of network traffic and protects from network attacks. Traffic that is considered harmful will be blocked.

Botnet protection

Detection and blocking of Botnet communication. Quickly and accurately identifies malware in the system.

Temporary IP address blacklist (blocked addresses)

View a list of IP addresses that have been detected as the source of attacks and added to the blacklist to block connection for a certain period of time.

Troubleshooting wizard (recently blocked applications or devices)

Helps you resolve connectivity problems caused by network attack protection.

To temporarily disable individual modules, next to the appropriate module, click the green slider bar . This may decrease the protection level of your server.

To re-enable the protection of a disabled security component, next to the appropriate module, click the red slider bar . The component is returned to an enabled state.

To access detailed settings of a specific security component, click the gear icon ⚙.

Import/Export settings

Load setup parameters using an *.xml* configuration file or save the current setup parameters to a configuration file.

Advanced setup

Configure advanced settings and options based on your needs. To access the **Advanced setup** screen from anywhere in the program, press **F5**.

Network troubleshooting wizard

The troubleshooting wizard monitors all blocked connections, and will guide you through the troubleshooting process to correct network attack protection issues with specific applications or devices. Next, the wizard will suggest a new set of rules to be applied if you approve them.

Web and email

Web and email allows you to enable/disable and configure the following components:

Web access protection

If enabled, all HTTP or HTTPS traffic is scanned for malicious software.

Email client protection

Monitors communication received through the POP3 and IMAP protocols.

Anti-Phishing protection

Protects you from attempts to acquire passwords, banking data and other sensitive information by illegitimate websites disguised as legitimate ones.

To temporarily disable individual modules, next to the appropriate module, click the green slider bar 🟩. This may decrease the protection level of your server.

To re-enable the protection of a disabled security component, next to the appropriate module, click the red slider bar 🟥. The component is returned to an enabled state.

To access detailed settings of a specific security component, click the gear icon ⚙.

Import/Export settings

Load setup parameters using an *.xml* configuration file or save the current setup parameters to a configuration file.

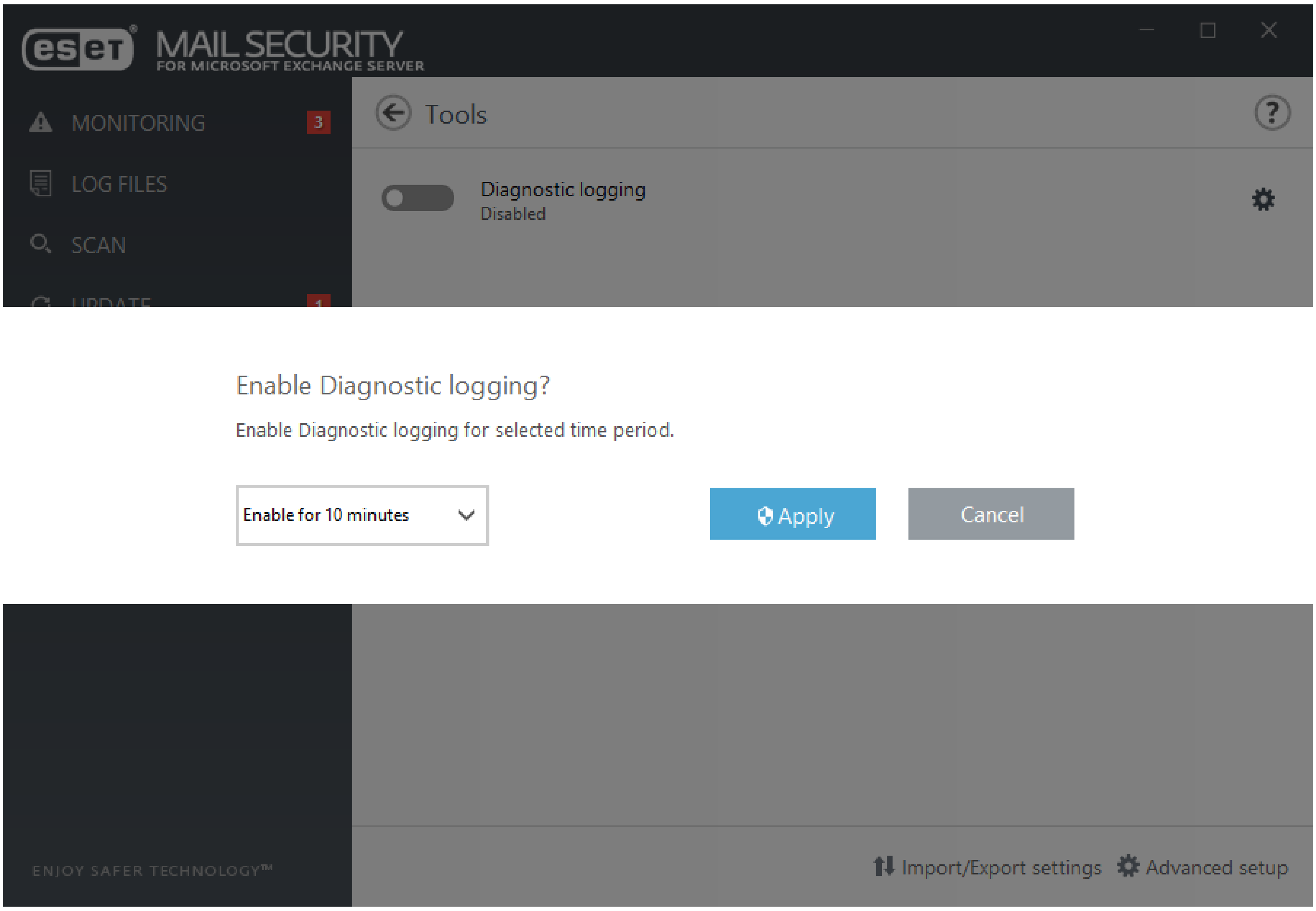
Advanced setup

Configure advanced settings and options based on your needs. To access the **Advanced setup** screen from anywhere in the program, press **F5**.

Tools - Diagnostic logging

You can enable Diagnostic logging when you need detailed information about the behavior of a specific ESET Mail Security feature, for example, when troubleshooting. When you click the gear icon ⚙, you can configure for what features should diagnostic logs be collected.

Choose how long it will be enabled (10 minutes, 30 minutes, 1 hour, 4 hours, 24 hours, until next server restart or permanently). Once diagnostic logging is turned on, ESET Mail Security will be collecting detailed logs according to what features are enabled.



Enable Diagnostic logging?

Enable Diagnostic logging for selected time period.

To temporarily disable individual modules, next to the appropriate module, click the green slider bar. This may decrease the protection level of your server.

To re-enable the protection of a disabled security component, next to the appropriate module, click the red slider bar. The component is returned to an enabled state.

To access detailed settings of a specific security component, click the gear icon ⚙.

Import/Export settings

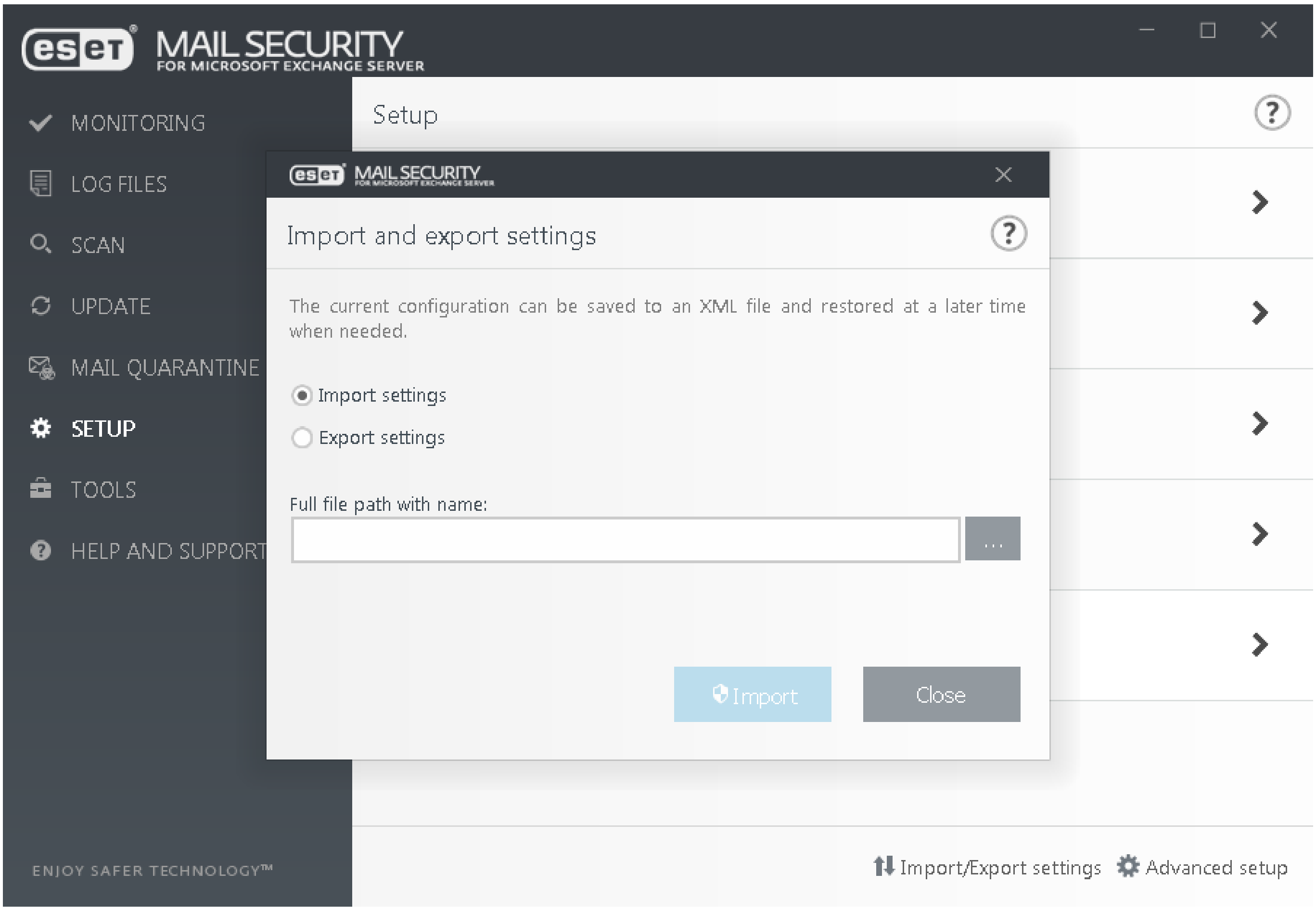
> Load setup parameters using an *.xml* configuration file or save the current setup parameters to a configuration file.

Advanced setup

> Configure advanced settings and options based on your needs. To access the **Advanced setup** screen from anywhere in the program, press **F5**.

Import and export settings

Import/export settings feature is useful if you need to back up current configuration of your ESET Mail Security. You can also use the import feature to distribute/apply the same settings to other server(s) with ESET Mail Security. Settings are exported to an *.xml* file.



Import and export settings

The current configuration can be saved to an XML file and restored at a later time when needed.

● Import settings
○ Export settings

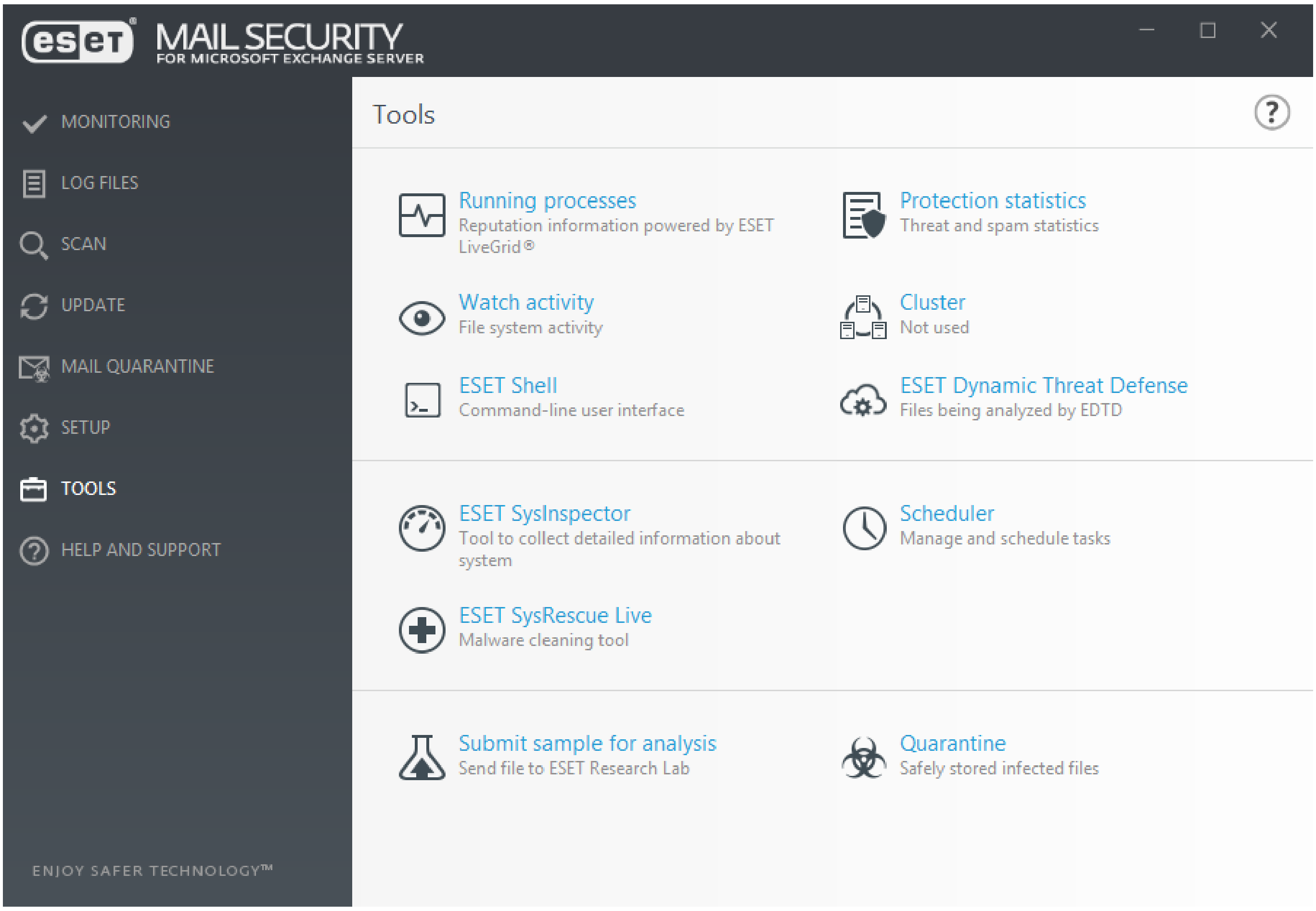
Full file path with name:

NOTE
If you do not have rights to write the exported file to specified directory, you may encounter an error when exporting settings.

Tools

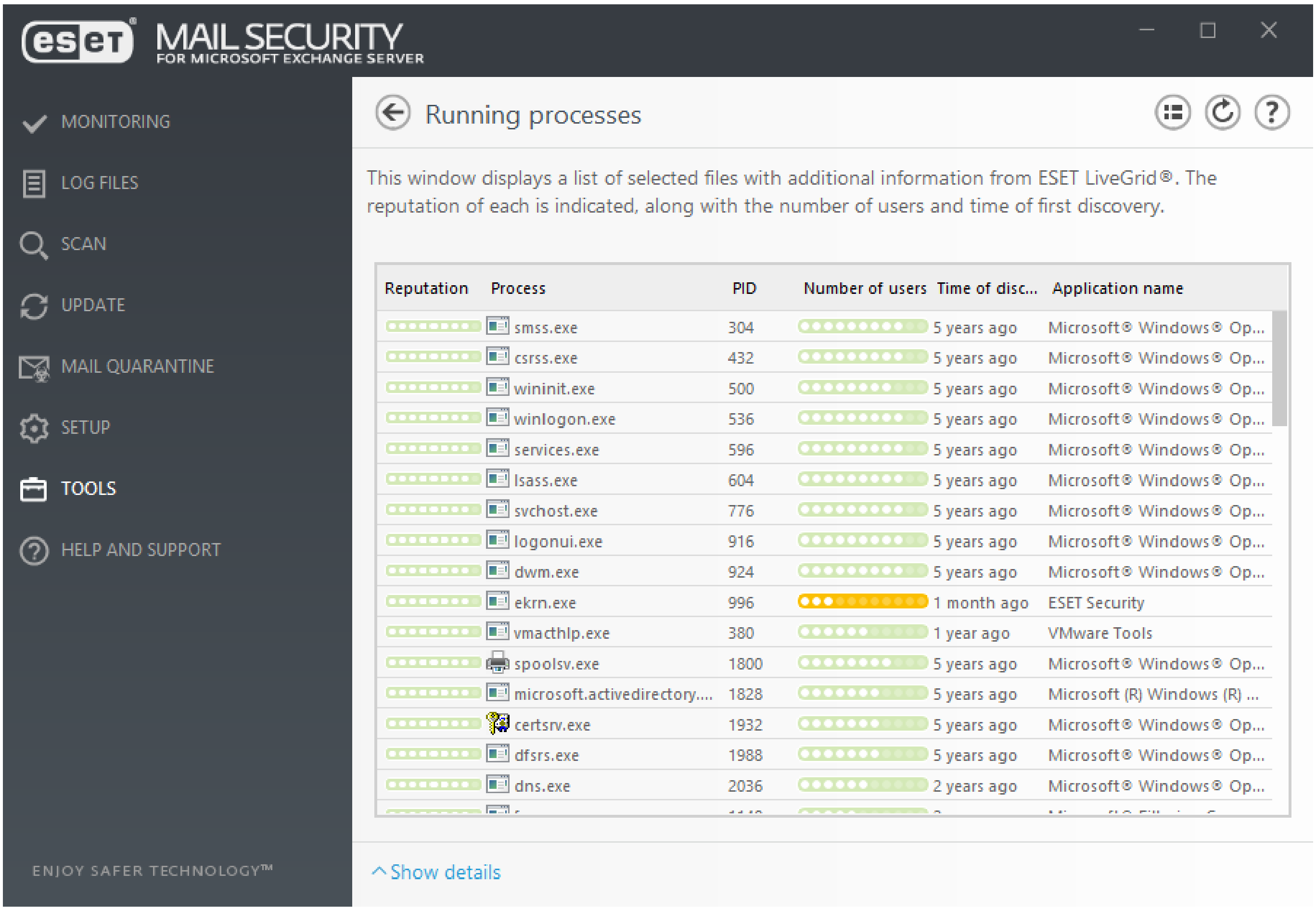
The following features are available for ESET Mail Security administration:

- Running processes
- Watch activity
- Protection statistics
- Cluster
- ESET Shell
- ESET Dynamic Threat Defense
- ESET SysInspector
- ESET SysRescue Live
- Scheduler
- Submit sample for analysis
- Quarantine


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
MONITORING
LOG FILES
SCAN
UPDATE
MAIL QUARANTINE
SETUP
TOOLS
HELP AND SUPPORT
ENJOY SAFER TECHNOLOGY™
Tools
Running processes
Reputation information powered by ESET LiveGrid®
Protection statistics
Threat and spam statistics
Watch activity
File system activity
Cluster
Not used
ESET Shell
Command-line user interface
ESET Dynamic Threat Defense
Files being analyzed by EDTD
ESET SysInspector
Tool to collect detailed information about system
Scheduler
Manage and schedule tasks
ESET SysRescue Live
Malware cleaning tool
Submit sample for analysis
Send file to ESET Research Lab
Quarantine
Safely stored infected files

Running processes

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



Running processes

This window displays a list of selected files with additional information from ESET LiveGrid®. The reputation of each is indicated, along with the number of users and time of first discovery.

Reputation	Process	PID	Number of users	Time of disc...	Application name
	smss.exe	304		5 years ago	Microsoft® Windows® Op...
	csrss.exe	432		5 years ago	Microsoft® Windows® Op...
	wininit.exe	500		5 years ago	Microsoft® Windows® Op...
	winlogon.exe	536		5 years ago	Microsoft® Windows® Op...
	services.exe	596		5 years ago	Microsoft® Windows® Op...
	lsass.exe	604		5 years ago	Microsoft® Windows® Op...
	svchost.exe	776		5 years ago	Microsoft® Windows® Op...
	logonui.exe	916		5 years ago	Microsoft® Windows® Op...
	dwm.exe	924		5 years ago	Microsoft® Windows® Op...
	ekrn.exe	996		1 month ago	ESET Security
	vmacthlp.exe	380		1 year ago	VMware Tools
	spoolsv.exe	1800		5 years ago	Microsoft® Windows® Op...
	microsoft.activedirectory....	1828		5 years ago	Microsoft (R) Windows (R) ...
	certsrv.exe	1932		5 years ago	Microsoft® Windows® Op...
	dfsrs.exe	1988		5 years ago	Microsoft® Windows® Op...
	dns.exe	2036		2 years ago	Microsoft® Windows® Op...

^ Show details

NOTE
Known applications marked as Best reputation (green) are clean (whitelisted) and will be excluded from scanning, as this will improve the scanning speed of on-demand computer scan or Real-time file system protection on your computer.

Reputation	**In most cases, ESET Mail Security and ESET LiveGrid® technology determines object reputation using a series of heuristic rules that examine the characteristics of each object (files, processes, registry keys, etc.) and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a reputation level from 9 - best reputation (green) to 0 - worst reputation (red).**
Process	Image name of the program or process that is currently running on your computer. You can also use the Windows Task Manager to see all running processes on your computer. You can open Task Manager by right-clicking an empty area on the taskbar and then clicking Task Manager, or by pressing Ctrl + Shift + Esc on your keyboard.
PID	Is an ID of processes running in Windows operating systems.
Number of users	The number of users that use a given application. This information is gathered by ESET LiveGrid® technology.
Time of discovery	Period of time since the application was discovered by ESET LiveGrid® technology.
Application name	Given name of a program this process belongs to.

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

Show details

The following information will appear at the bottom of the window:

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

Add to processes exclusions

Right-click a process in the Running processes window to exclude it from scanning. Its path will be added to the list of Processes exclusions.

Watch activity

To Watch activity contain activity in graph form, select from drop-down menu following activity:

File system activity

Amount of read or written data. The vertical axis of graph represents read data (blue) and written data (green).

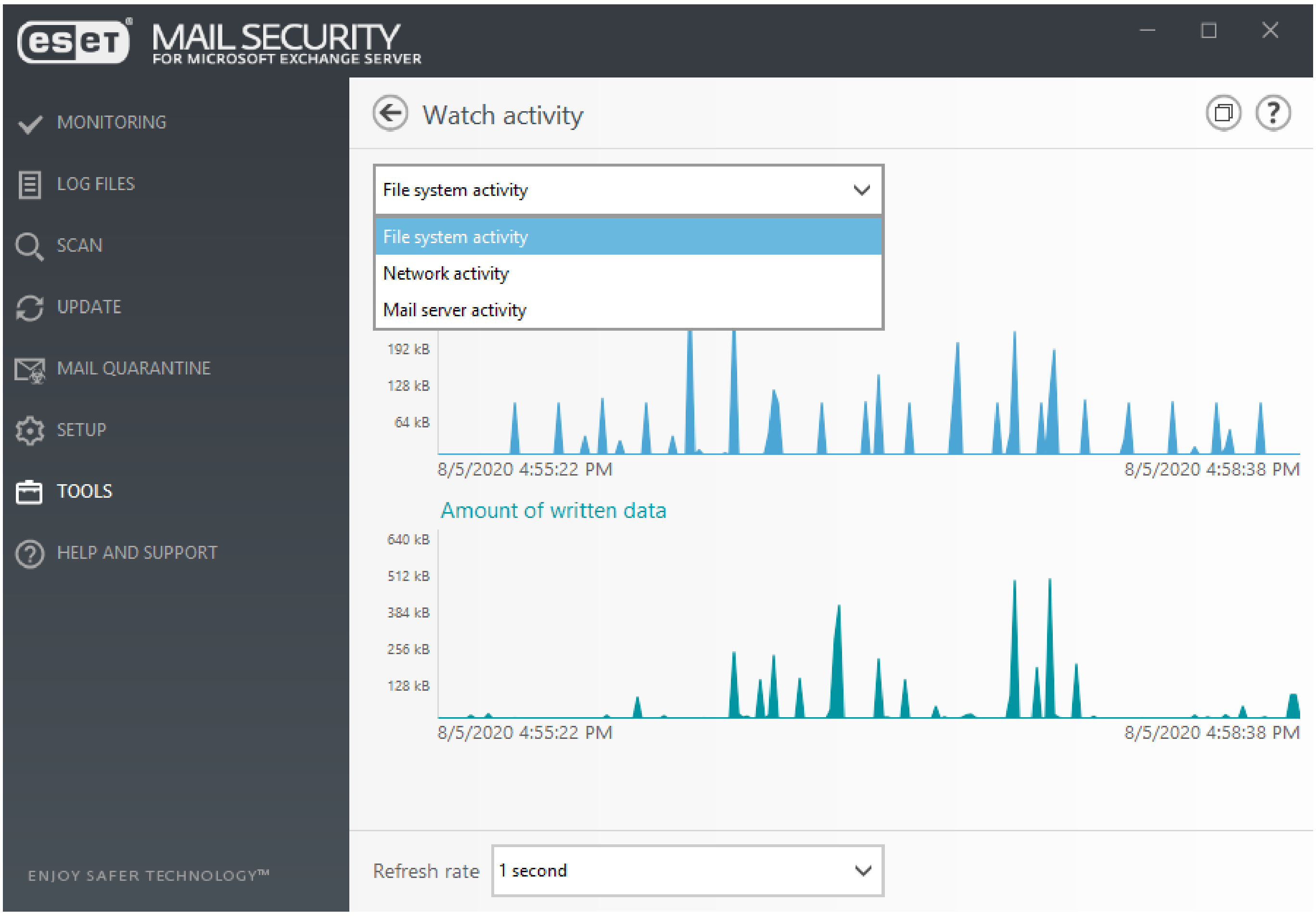
Network activity

Amount of received of sent data. The vertical axis of graph represents received data (blue) and sent data (green).

Mail server activity

Amount of processed data by Transport protection (blue) and Database protection (green).

At the bottom of the graph is a timeline that records file system activity in real-time based on the selected time span. Use the **Refresh rate** drop-down menu to change the frequency of updates.



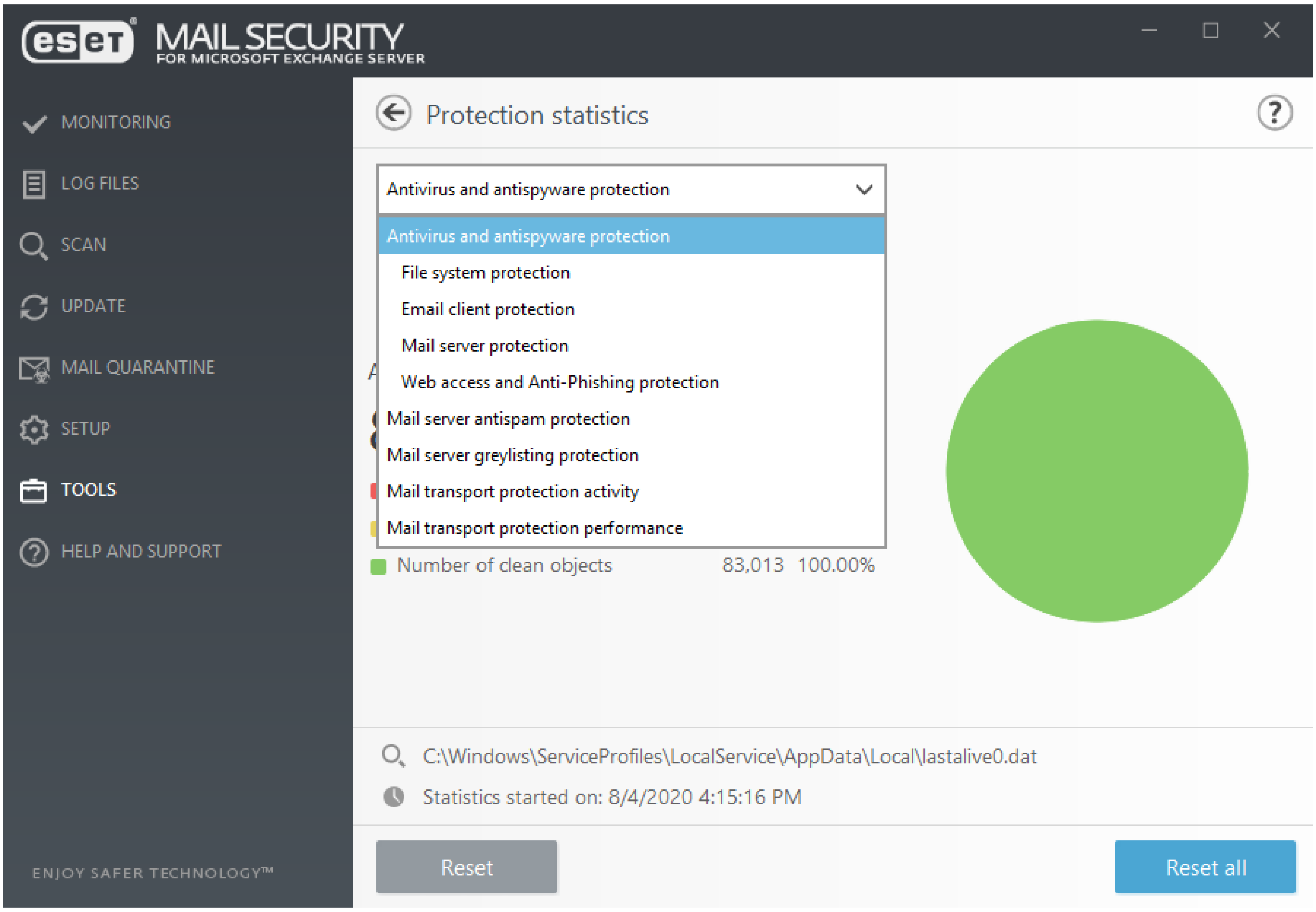
Refresh rate: 1 second

The following options are available:

1 second	**The graph refreshes every second and the timeline covers the last 10 minutes.**
1 minute (last 24 hours)	The graph is refreshed every minute and the timeline covers the last 24 hours.
1 hour (last month)	The graph is refreshed every hour and the timeline covers the last month.
1 hour (selected month)	The graph is refreshed every hour and the timeline covers the selected month. Select a month (and a year) from the drop-down menu to see activity. Click **Change**.

Protection statistics

To view statistical data related to protection modules of ESET Mail Security, select the applicable protection module from the drop-down menu. The statistics include information such as the number of all scanned objects, number of infected objects, number of cleaned objects and the number of clean objects. Hover your mouse over an object next to the graph and only the data for that specific object will display in the graph. To clear statistics information for the current protection module, click **Reset**. To clear data for all modules, click **Reset all**.


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
MONITORING
LOG FILES
SCAN
UPDATE
MAIL QUARANTINE
SETUP
TOOLS
HELP AND SUPPORT
ENJOY SAFER TECHNOLOGY™
Protection statistics
Antivirus and antispyware protection
Antivirus and antispyware protection
File system protection
Email client protection
Mail server protection
Web access and Anti-Phishing protection
Mail server antispam protection
Mail server greylisting protection
Mail transport protection activity
Mail transport protection performance
Reset
Reset all

🟩 Number of clean objects 83,013 100.00%

C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat

Statistics started on: 8/4/2020 4:15:16 PM

The following statistic graphs are available in ESET Mail Security:

Antivirus and antispyware protection

Displays the overall number of infected and cleaned objects.

File system protection

Displays objects that were read or written to the file system only.

Hyper-V protection

Displays the overall number of infected, cleaned and clean objects (on systems with Hyper-V only).

Email client protection

Displays objects that were sent or received by email clients only.

Web access and Anti-Phishing protection

Displays objects downloaded by web browsers only.

Mail server protection

Displays anti-malware mail server statistics.

Mail server antispam protection

Displays the history of antispam statistics. Number of Not scanned refers to objects excluded from scan (based on rules, internal messages, authenticated connections, etc.).

Mail server greylisting protection

Includes antispam statistic generated using the greylisting method.

Mail transport protection activity

Displays objects verified/blocked/deleted by the mail server.

Mail transport protection performance

Displays data processed by VSAPI/Transport Agent in B/s.

Mailbox database protection activity

Displays objects processed by VSAPI (number of verified, quarantined and deleted objects).

Mailbox database protection performance

Displays data processed by VSAPI (number of different averages for today, for last 7 days and averages since last reset).

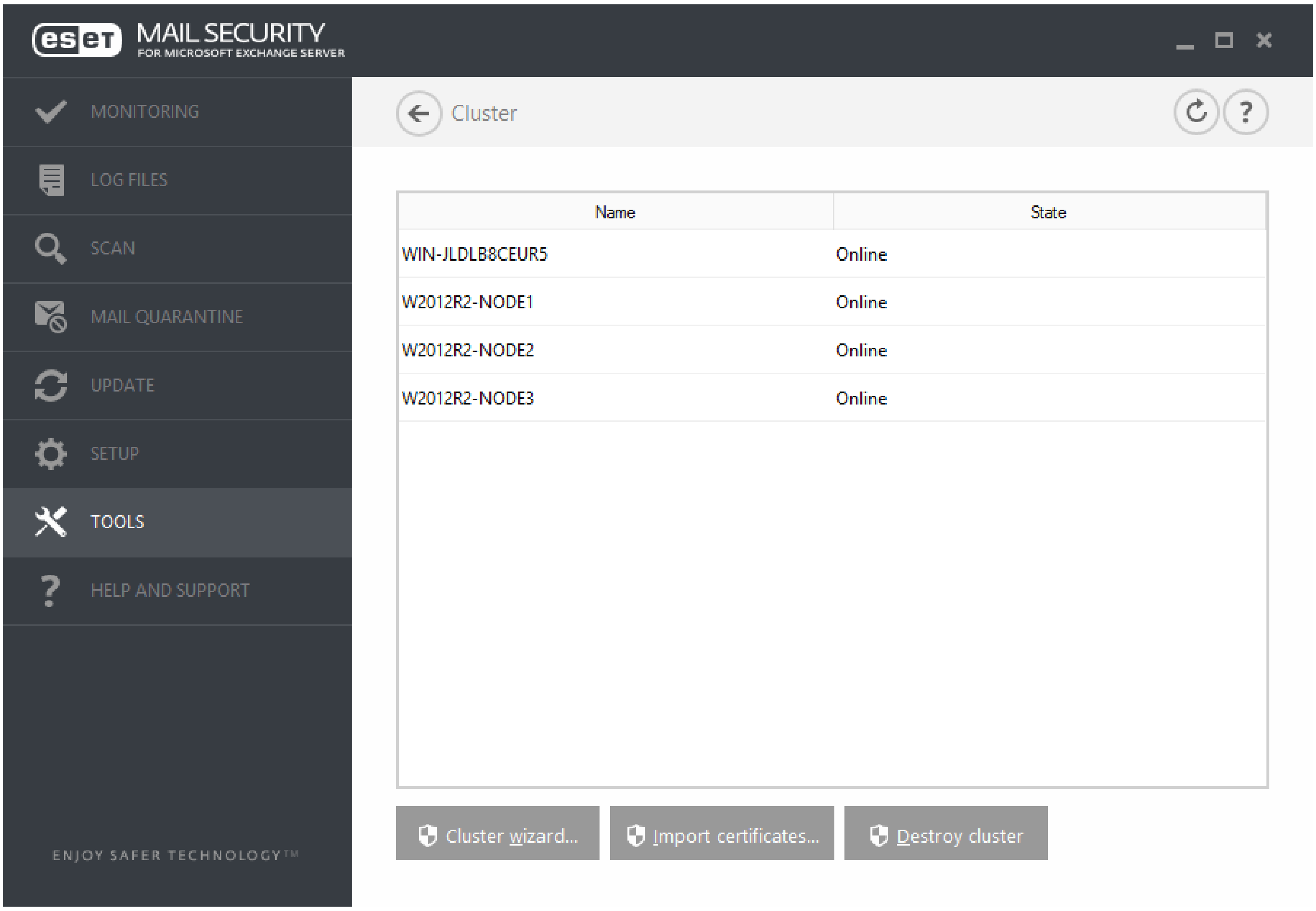
Cluster

The **ESET Cluster** is a P2P communication infrastructure of the ESET line of products for Microsoft Windows Server. Using ESET Cluster is ideal if you have Exchange infrastructure with multiple servers such as DAG.

This infrastructure enables ESET server products to communicate with each other and exchange data such as configuration and notifications, and can Synchronize greylisting databases as well as synchronize data necessary for correct operation of a group of product instances. An example of such group is a group of nodes in a Windows Failover Cluster or Network Load Balancing (NLB) Cluster with ESET products installed where there is a need to have the same configuration of the product across the whole cluster. ESET Cluster ensures this consistency between instances.

NOTE
Settings of the User interface are not synchronized between ESET Cluster nodes.

The ESET Cluster status page is accessible from the main menu in **Tools** > **Cluster** when properly configured, the status page should look like this:



Name	State
WIN-JLDLB8CEUR5	Online
W2012R2-NODE1	Online
W2012R2-NODE2	Online
W2012R2-NODE3	Online

NOTE
The creation of ESET Clusters between ESET Mail Security and ESET File Security for Linux is not supported.

When setting up the ESET Cluster, there two ways to add nodes:

Autodetect

If you have an existing Windows Failover Cluster / NLB Cluster, Autodetect will automatically add its member nodes to the ESET Cluster.

Browse

You can add nodes manually by typing in the server names (either members of the same Workgroup or members of the same Domain).

NOTE
Servers don't have to be members of a Windows Failover Cluster / NLB Cluster to use the ESET Cluster feature. A Windows Failover Cluster or NLB Cluster is not required in your environment for you to use ESET Clusters.

Once you have added nodes to your ESET Cluster, the next step is the installation of ESET Mail Security on each node. This is done automatically during ESET Cluster setup. Credentials that are required for remote installation of ESET Mail Security on other cluster nodes:

Domain scenario

Domain administrator credentials.

Workgroup scenario

You need to make sure that all nodes use the same local administrator account credentials.

In an ESET Cluster, you can also use a combination of nodes added automatically as members of an existing Windows Failover Cluster / NLB Cluster and nodes added manually (provided they are in the same Domain).

IMPORTANT
It is not possible to combine domain nodes with workgroup nodes.

Another requirement for the use of an ESET Cluster is that **File and Printer Sharing** must be enabled in Windows Firewall before pushing ESET Mail Security to ESET Cluster nodes.

You can add new nodes to an existing ESET Cluster anytime by running the Cluster wizard.

Import certificates

Certificates are used to provide strong machine to machine authentication when HTTPS is used. There is an independent certificate hierarchy for each ESET Cluster. The hierarchy has one root certificate and a set of node certificates signed by the root certificate. The private key of the root certificate is destroyed after all node certificates are created. When you add a new node to the cluster a new certificate hierarchy is created. Navigate to the folder that contains the certificates (that were generated during Cluster wizard). Select the certificate file and click **Open**.

Destroy cluster

ESET Clusters can be dismantled. Each node will write a record in their event log about the ESET Cluster being destroyed. After that, all ESET firewall rules are removed from the Windows Firewall. Former nodes will be ted to their previous state and can be used again in another ESET Cluster if necessary.

Cluster wizard - Select nodes

The first step when setting up an ESET Cluster is adding nodes. You can either use the **Autodetect** option or **Browse** to add nodes. Alternatively, you can type the server name into the text box and click **Add**.

Autodetect

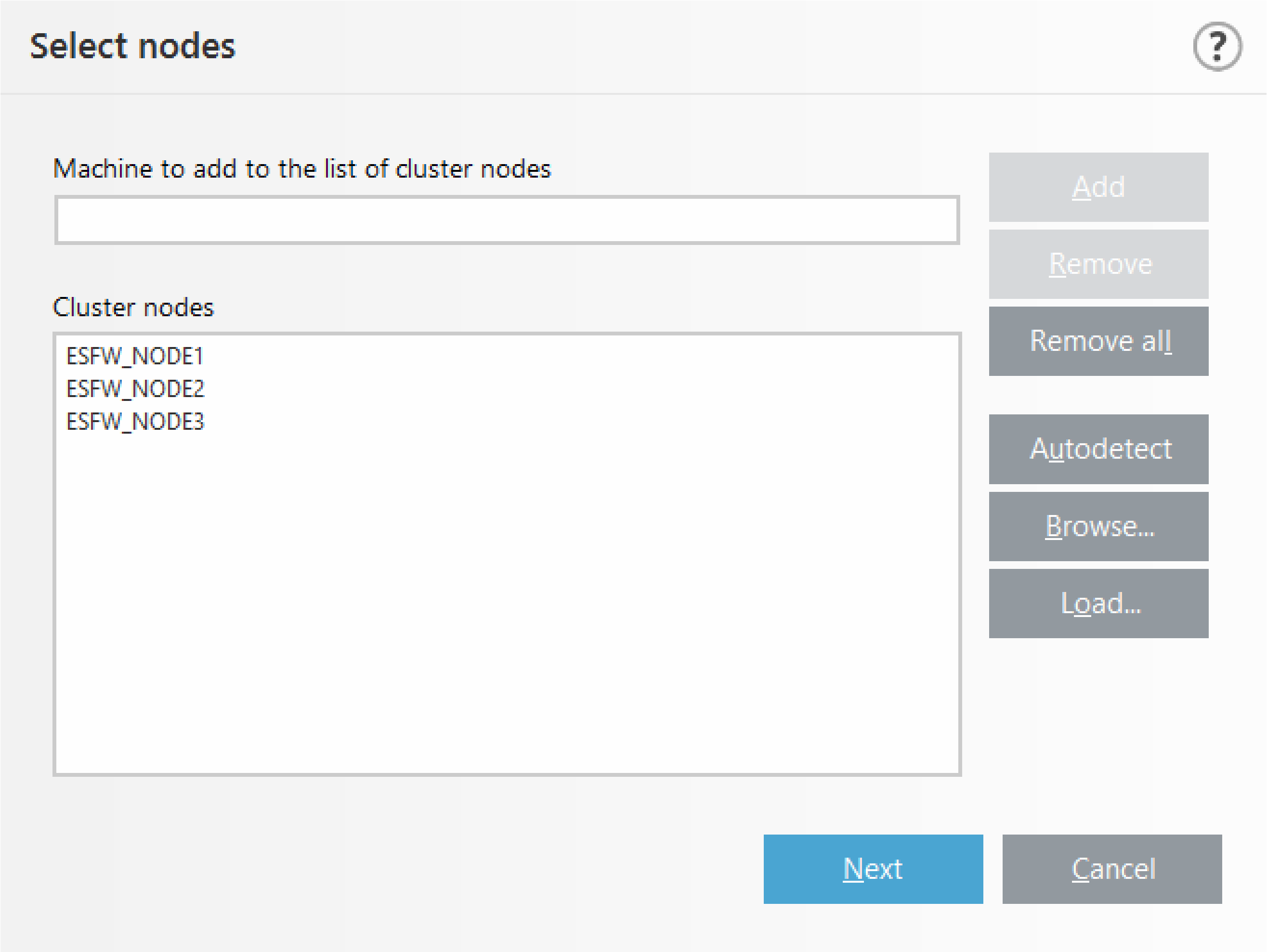
Automatically adds nodes from an existing Windows Failover Cluster / Network Load Balancing (NLB) Cluster. The server you are using to create the ESET Cluster from needs to be a member of this Windows Failover Cluster / NLB Cluster in order to automatically add the nodes. The NLB Cluster must have the **Allow remote control** feature enabled in cluster properties for the ESET Cluster to detect the nodes correctly. Once you have the list of newly added nodes, you can remove unwanted ones.

Browse

To find and select computers within a Domain or a Workgroup. This method allows for the manual addition of nodes to the ESET Cluster. Another way to add nodes is by typing the host name of the server you want add and clicking **Add**.

Load

To import list of nodes from file.



ESFW_NODE1
ESFW_NODE2
ESFW_NODE3

To modify **Cluster nodes** in the list, select the node you want to remove and click **Remove**, or to clear the list completely click **Remove all**.

If you already have an existing ESET Cluster, you can add new nodes to it at any time. The steps are the same as described above.

NOTE
All nodes that remain in the list must be online and reachable. Localhost is added into the cluster nodes by default.

Cluster wizard - Cluster settings

Define cluster name, and network specifics (if required).

Cluster name

Type a name for your cluster and click **Next**.

Listening port (default port is 9777)

If you are already using port 9777 in your network environment, specify other port number that is not being used.

Open port in Windows firewall

When selected a rule is created in the Windows Firewall.

Cluster wizard - Cluster setup settings

Define certificate distribution mode and whether to install the product on other nodes or not.

Certificate distribution

- **Automatic remote** - Certificate will be installed automatically.
- **Manual** - Click **Generate** and select the appropriate folder to store the certificates. A root certificate as well as a certificate for each node, including the one (local machine) from which you are setting up the ESET Cluster, will be created. To enroll the certificate on the local machine, click **Yes**.

Product install to other nodes

- **Automatic remote** - ESET Mail Security will be installed automatically on each node (provided their operating systems are the same architecture).
- **Manual** - Manually install ESET Mail Security (for example, when you have different OS architectures on some nodes).

Push license to nodes without activated product

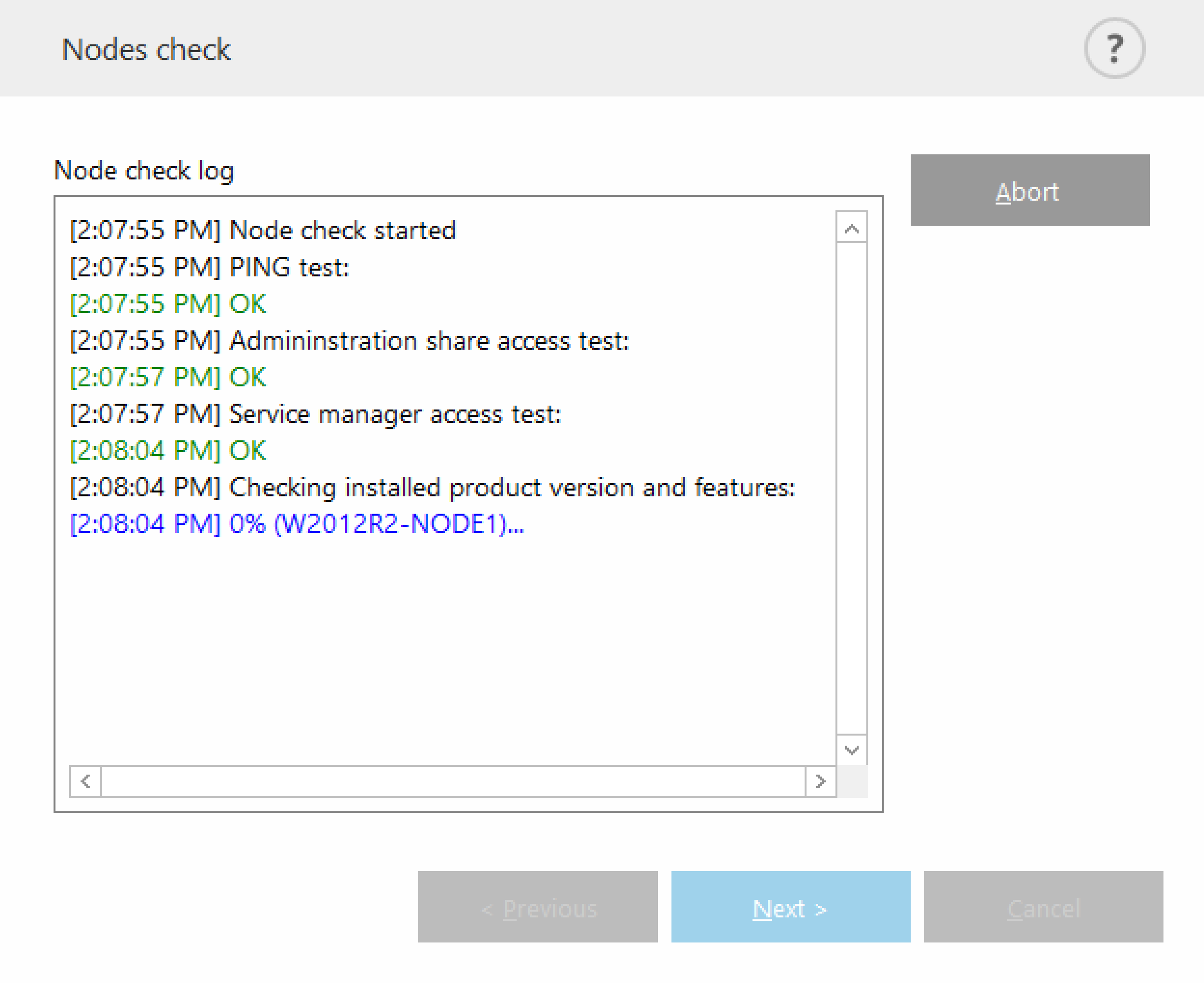
ESET Security automatically activates ESET Solutions installed on nodes without licenses.

> NOTE
> To create an ESET Cluster with a mixed operating system architecture (32 bit and 64 bit), install ESET Mail Security manually. Operating systems in use will be detected during next steps and you will see this information in the log window.

Cluster wizard - Nodes check

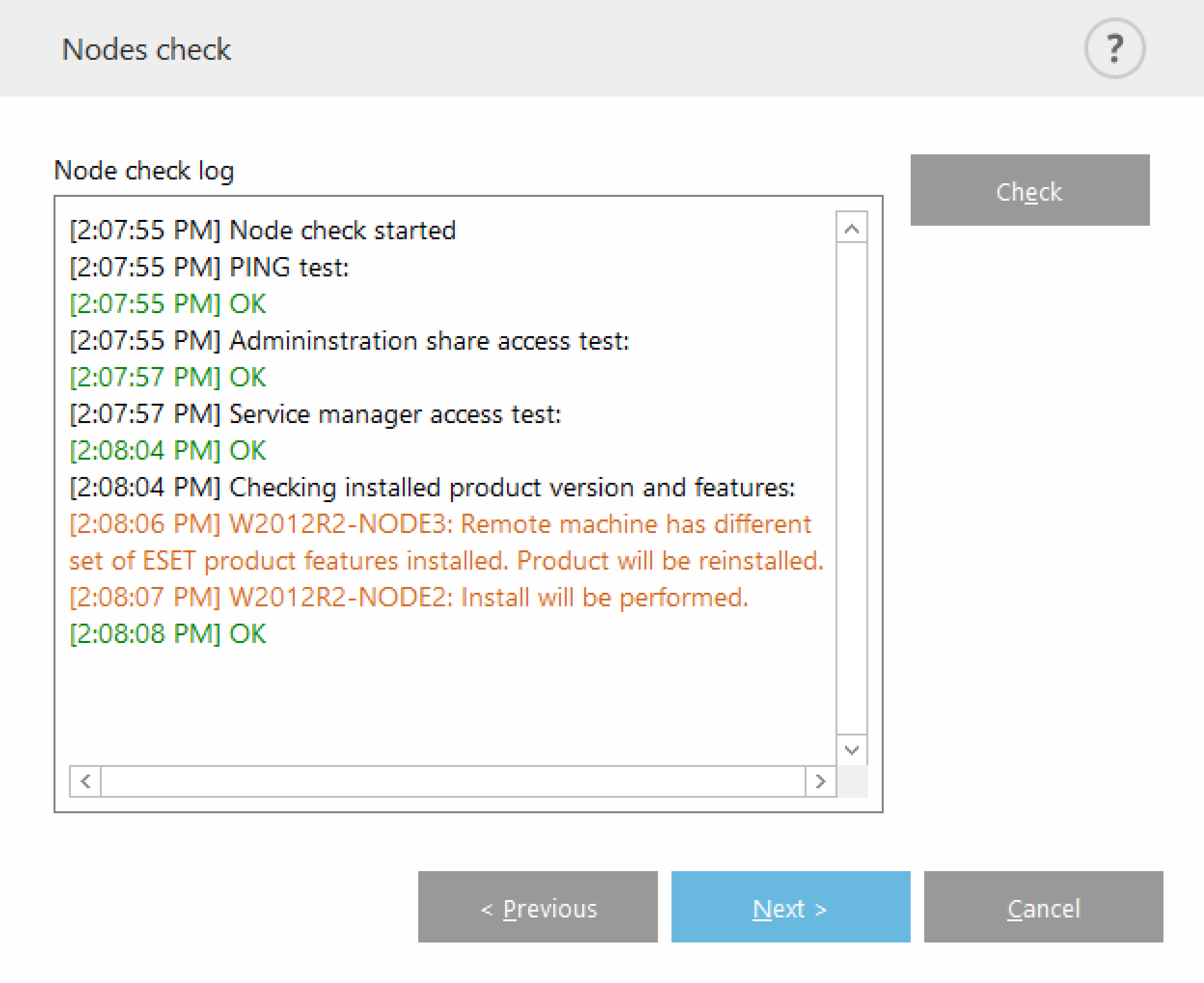
After specifying installation details a node check is run. The following information will be displayed in the **Nodes check log**:

- verify that all existing nodes are online
- verify that new nodes are accessible
- node is online
- admin share is accessible
- remote execution is possible
- correct product versions (or no product) are installed
- verify that the new certificates are present



```
[2:07:55 PM] Node check started
[2:07:55 PM] PING test:
[2:07:55 PM] OK
[2:07:55 PM] Admininstration share access test:
[2:07:57 PM] OK
[2:07:57 PM] Service manager access test:
[2:08:04 PM] OK
[2:08:04 PM] Checking installed product version and features:
[2:08:04 PM] 0% (W2012R2-NODE1)...
```

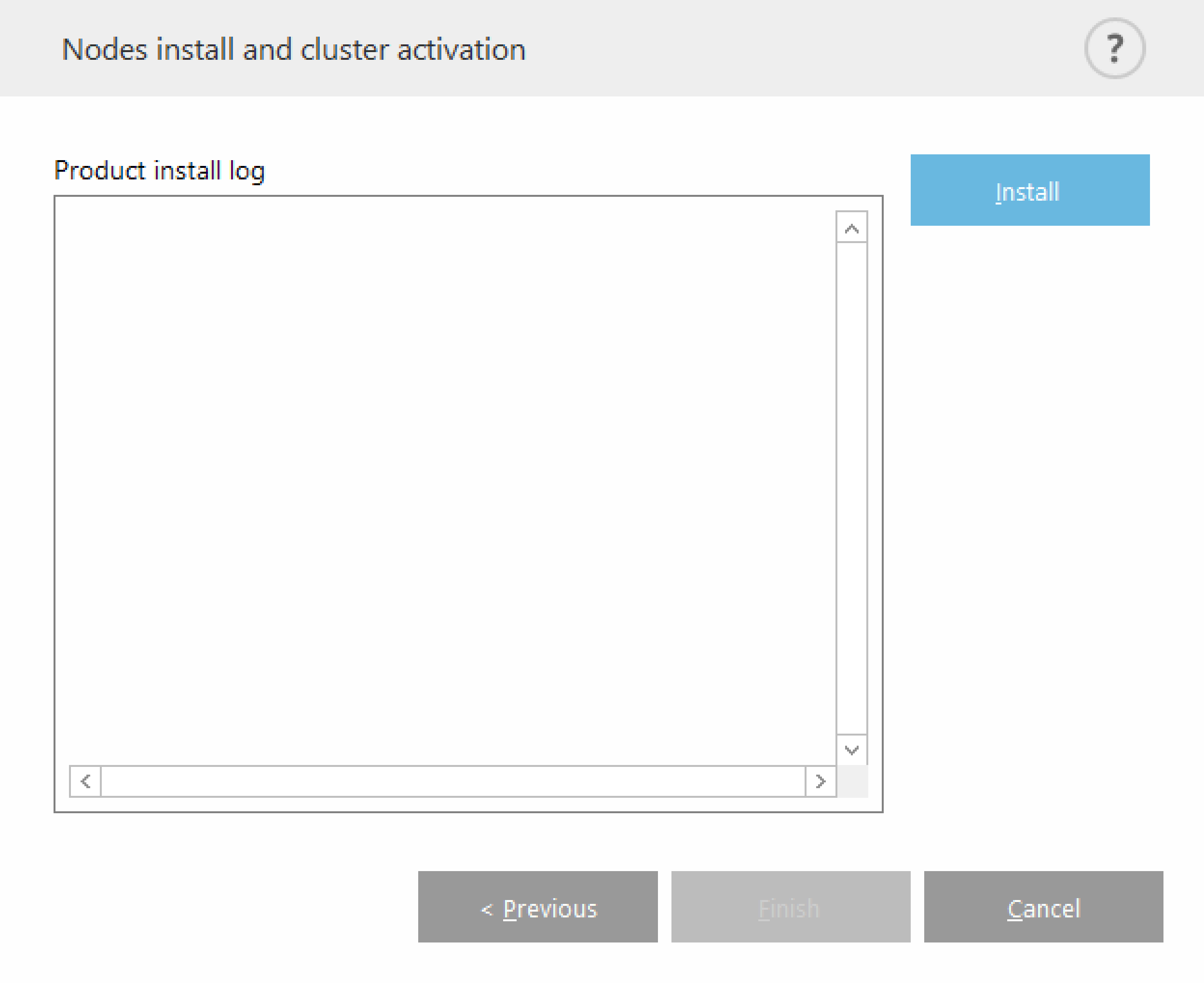
You will see the report once the node check is finished:



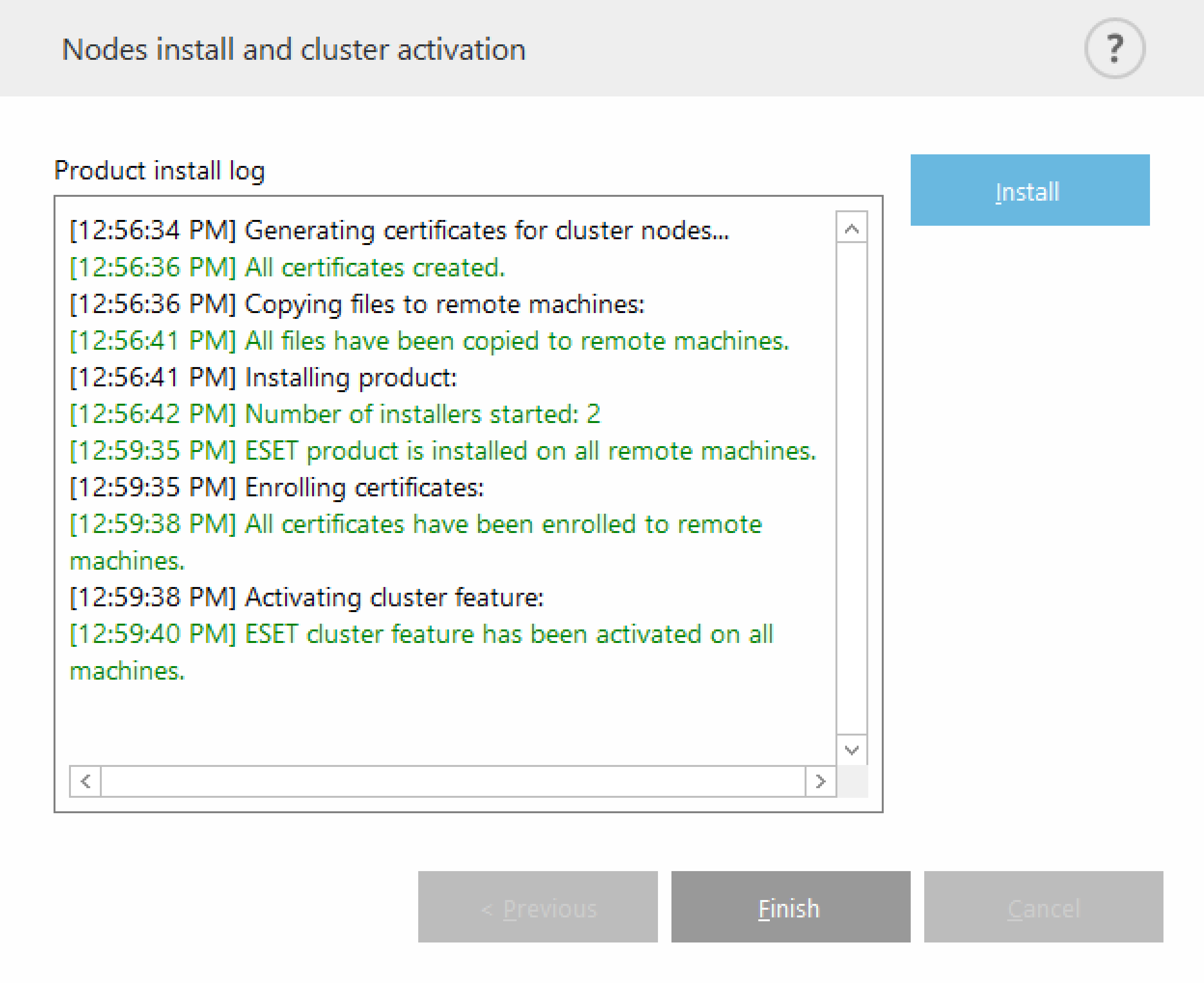
```
[2:07:55 PM] Node check started
[2:07:55 PM] PING test:
[2:07:55 PM] OK
[2:07:55 PM] Admininstration share access test:
[2:07:57 PM] OK
[2:07:57 PM] Service manager access test:
[2:08:04 PM] OK
[2:08:04 PM] Checking installed product version and features:
[2:08:06 PM] W2012R2-NODE3: Remote machine has different
set of ESET product features installed. Product will be reinstalled.
[2:08:07 PM] W2012R2-NODE2: Install will be performed.
[2:08:08 PM] OK
```

Cluster wizard - Nodes install

When installing to a remote machine during ESET Cluster initialization, the wizard will attempt to locate the installer in the directory *%ProgramData%\ESET\ESET Security\Installer*. If the installer package is not found there, you will be asked to locate the installer file.



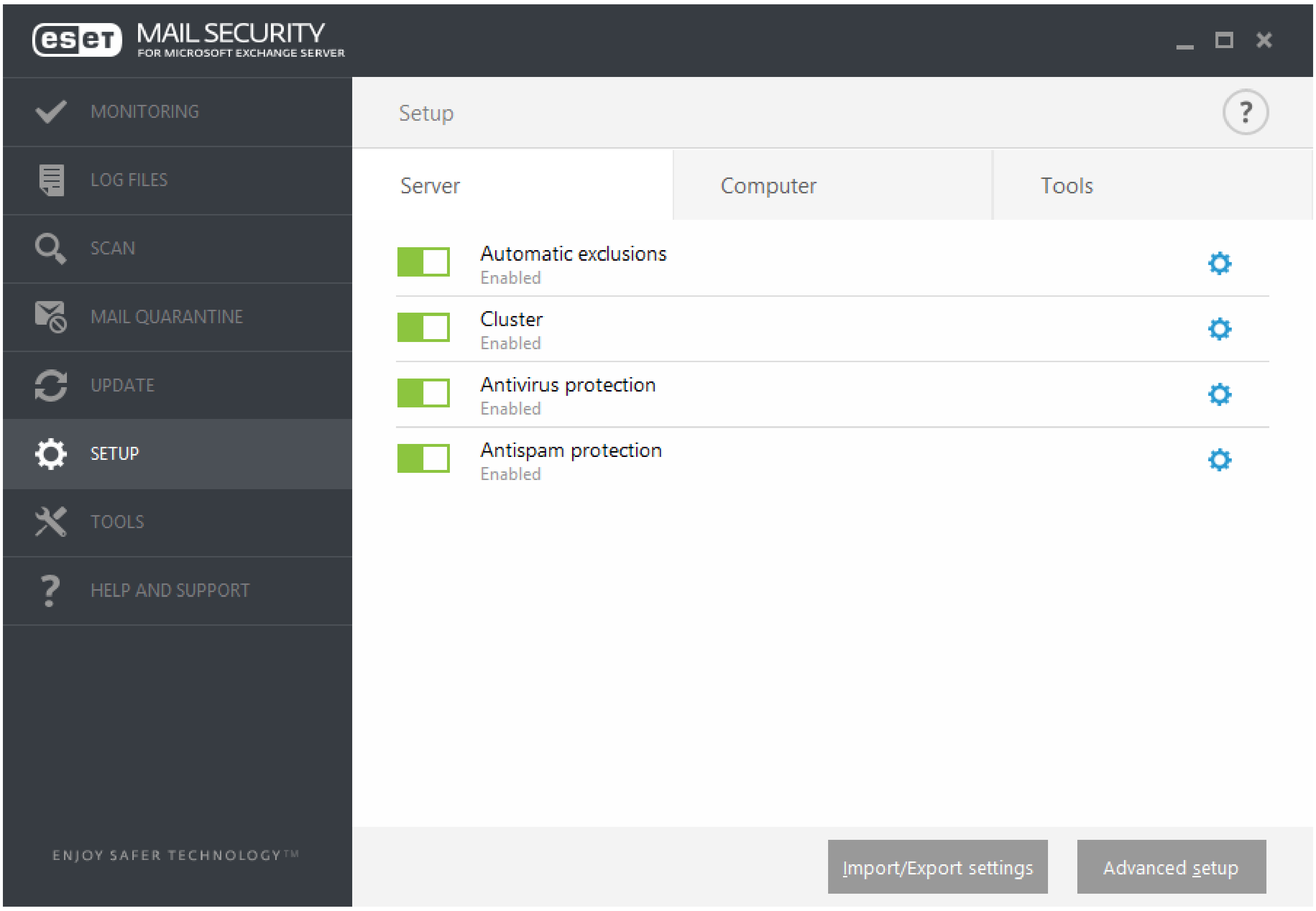
NOTE
When trying to use automatic remote installation for a node with different architecture (32-bit vs 64-bit), this will be detected and you will be prompted to perform manual installation.



```
[12:56:34 PM] Generating certificates for cluster nodes...
[12:56:36 PM] All certificates created.
[12:56:36 PM] Copying files to remote machines:
[12:56:41 PM] All files have been copied to remote machines.
[12:56:41 PM] Installing product:
[12:56:42 PM] Number of installers started: 2
[12:59:35 PM] ESET product is installed on all remote machines.
[12:59:35 PM] Enrolling certificates:
[12:59:38 PM] All certificates have been enrolled to remote
machines.
[12:59:38 PM] Activating cluster feature:
[12:59:40 PM] ESET cluster feature has been activated on all
machines.
```

Once you have correctly configured the ESET Cluster, it will appear in **Setup** > **Server** page as enabled.

NOTE
If an older version of ESET Mail Security is already installed on some nodes, you will be notified that the latest version is required on these machines. Updating ESET Mail Security may cause an automatic restart.



Automatic exclusions
Enabled

Cluster
Enabled

Antivirus protection
Enabled

Antispam protection
Enabled

Additionally, you can check its current status from the Cluster status page (**Tools** > **Cluster**).

ESET Shell

eShell (short for ESET Shell) is a command line interface for ESET Mail Security. It is an alternative to the graphical user interface (GUI). eShell includes all the features and options that the GUI normally gives you. eShell lets you configure and administer the whole program without the use of the GUI.

Apart from all the functions and features that are available in the GUI, it also provides you with the option of using automation by running scripts in order to configure, modify configuration or perform an action. Also, eShell can be useful for those who prefer to use the command line over the GUI.

> NOTE
> For full functionality we recommend you to open the eShell using Run as administrator. The same applies when executing a single command via Windows Command Prompt (cmd). Open the prompt using Run as administrator. Failing to run the command prompt as Administrator will stop you from running commands due to lack of permissions.

There are two modes in which eShell can be run:

1.**Interactive mode -** This is useful when you want to work with eShell (not just execute a single command) for tasks such as changing configuration, viewing logs, etc. You can use interactive mode if you are not familiar with all the commands yet. Interactive mode will make it easier for you when navigating through eShell. It also shows you available commands you can use within a particular context.

2.**Single command / Batch mode -** You can use this mode if you only need to execute a command without entering the interactive mode of eShell. This can be done from the Windows Command Prompt by typing in eshell with the appropriate parameters.

EXAMPLE
`eshell get status` or `eshell computer set real-time status disabled 1h`

In order to run certain commands (such as the second example above) in batch/script mode, there are a couple of settings that you need to configure first. Otherwise, you'll get an **Access Denied** message. This is for security reasons.

NOTE
Settings changes are required to allow the use of eShell commands from a Windows Command Prompt. For further information about running batch files click here.

There are two ways to enter interactive mode in eShell:

1. Via **Windows Start menu**: Start > All Programs > ESET > ESET Mail Security > ESET Shell

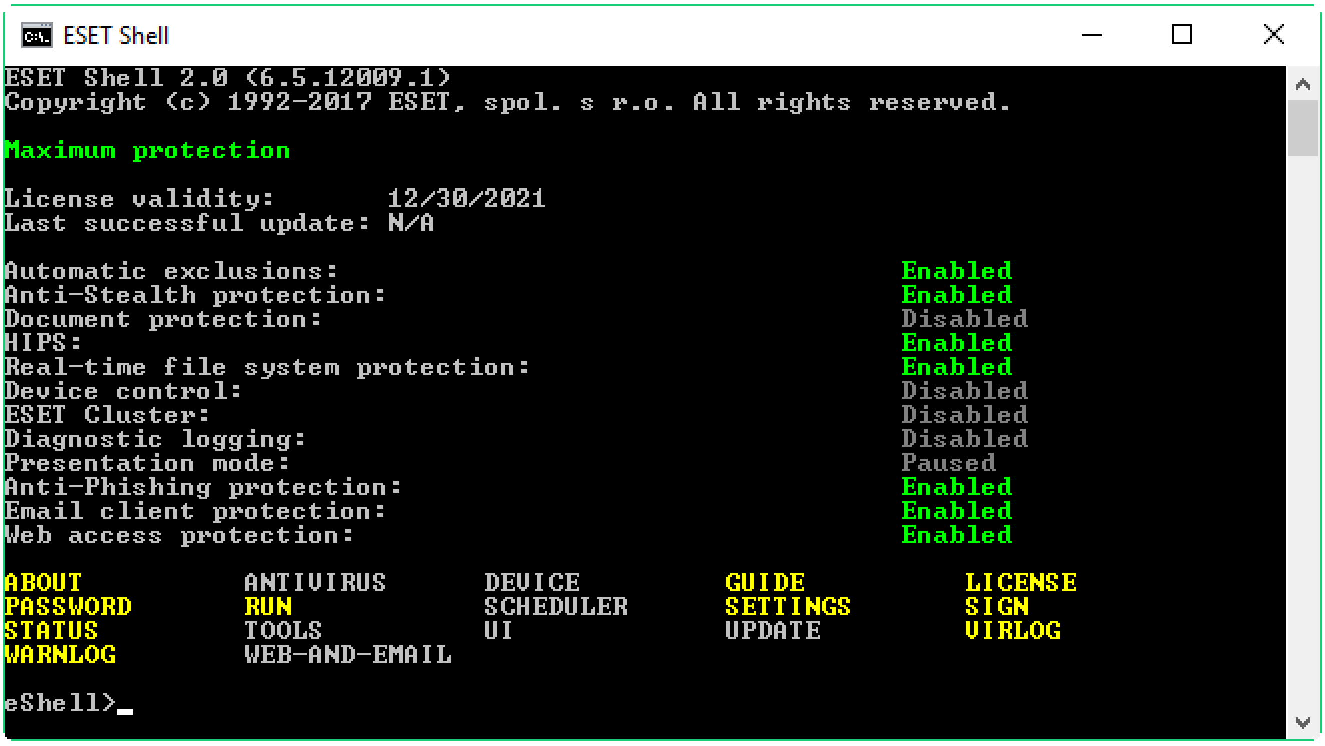
2. From **Windows Command Prompt** by typing in `eshell` and pressing the Enter key

IMPORTANT
If you get an error `'eshell' is not recognized as an internal or external command`, this is due to new Environment Variables not being loaded by your system after the installation of ESET Mail Security. You can open new Command Prompt and try starting eShell again. If you are still getting an error or have Core installation of ESET Mail Security, start eShell using absolute path, for example `"%PROGRAMFILES%\ESET\ESET Mail Security\eShell.exe"` (you must use "" in order for the command to work).

When you run eShell in interactive mode for the first time, a first run (guide) screen will display.

NOTE
If you want to display the first run screen in future, type in `guide` command. It shows you some basic examples how to use eShell with Syntax, Prefix, Command path, Abbreviated forms, Aliases, etc.

Next time you run eShell, you'll see this screen:



```
ESET Shell 2.0 (6.5.12009.1)
Copyright (c) 1992-2017 ESET, spol. s r.o. All rights reserved.

Maximum protection

License validity:       12/30/2021
Last successful update: N/A

Automatic exclusions:                                      Enabled
Anti-Stealth protection:                                   Enabled
Document protection:                                       Disabled
HIPS:                                                      Enabled
Real-time file system protection:                          Enabled
Device control:                                            Disabled
ESET Cluster:                                              Disabled
Diagnostic logging:                                        Disabled
Presentation mode:                                         Paused
Anti-Phishing protection:                                  Enabled
Email client protection:                                   Enabled
Web access protection:                                     Enabled

ABOUT           ANTIVIRUS       DEVICE          GUIDE           LICENSE
PASSWORD        RUN             SCHEDULER       SETTINGS        SIGN
STATUS          TOOLS           UI              UPDATE          VIRLOG
WARNLOG         WEB-AND-EMAIL

eShell>_
```

NOTE

Commands are not case sensitive. You can use upper case (capital) or lower case letters and the command will execute regardless.

Customizing eShell

You can customize eShell in `ui eshell` context. You can configure aliases, colors, language, execution policy for scripts, settings for hidden commands and more.

Usage

Syntax

Commands must be formatted in the correct syntax to function and can be composed of a prefix, context, arguments, options, etc. This is the general syntax used throughout eShell:

[<prefix>] [<command path>] <command> [<arguments>]

Example (this activates document protection):

```
SET COMPUTER SCANS DOCUMENT REGISTER ENABLED
```

`SET` - a prefix
`COMPUTER SCANS DOCUMENT` - path to a particular command, a context where this command belongs
`REGISTER` - the command itself
`ENABLED` - an argument for the command

Using `?` as an argument for command will display the syntax for that particular command. For example, `STATUS ?` will show you the syntax for `STATUS` command:

SYNTAX:

```
[get] status
```

OPERATIONS:

`get` - Show status of all protection modules

You may notice that `[get]` is in brackets. It designates that the prefix `get` is default for the `status` command. This means that when you execute `status` without specifying any prefix, it will actually use the default prefix (in this case `get status`). Using commands without a prefix saves time when typing. Usually `get` is the default prefix for most commands, but you need to be sure what the default prefix is for a particular command and that it is exactly what you want to execute.

> NOTE
> Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Prefix / Operation

A prefix is an operation. The `GET` prefix will give you information about how a certain feature of ESET Mail Security is configured or show you the status (such as `GET COMPUTER REAL-TIME STATUS` will show you current protection status of the Real-time module). The `SET` prefix will configure functionality or change its status (`SET COMPUTER REAL-TIME STATUS ENABLED` will activate Real-time protection).

These are the prefixes that eShell lets you use. A command may or may not support any of the prefixes:

GET	returns current setting/status
SET	sets value/status
SELECT	selects an item
ADD	adds an item
REMOVE	removes an item
CLEAR	removes all items/files
START	starts an action
STOP	stops an action
PAUSE	pauses an action
RESUME	resumes an action
RESTORE	restores default settings/object/file
SEND	sends an object/file
IMPORT	imports from a file
EXPORT	exports to a file

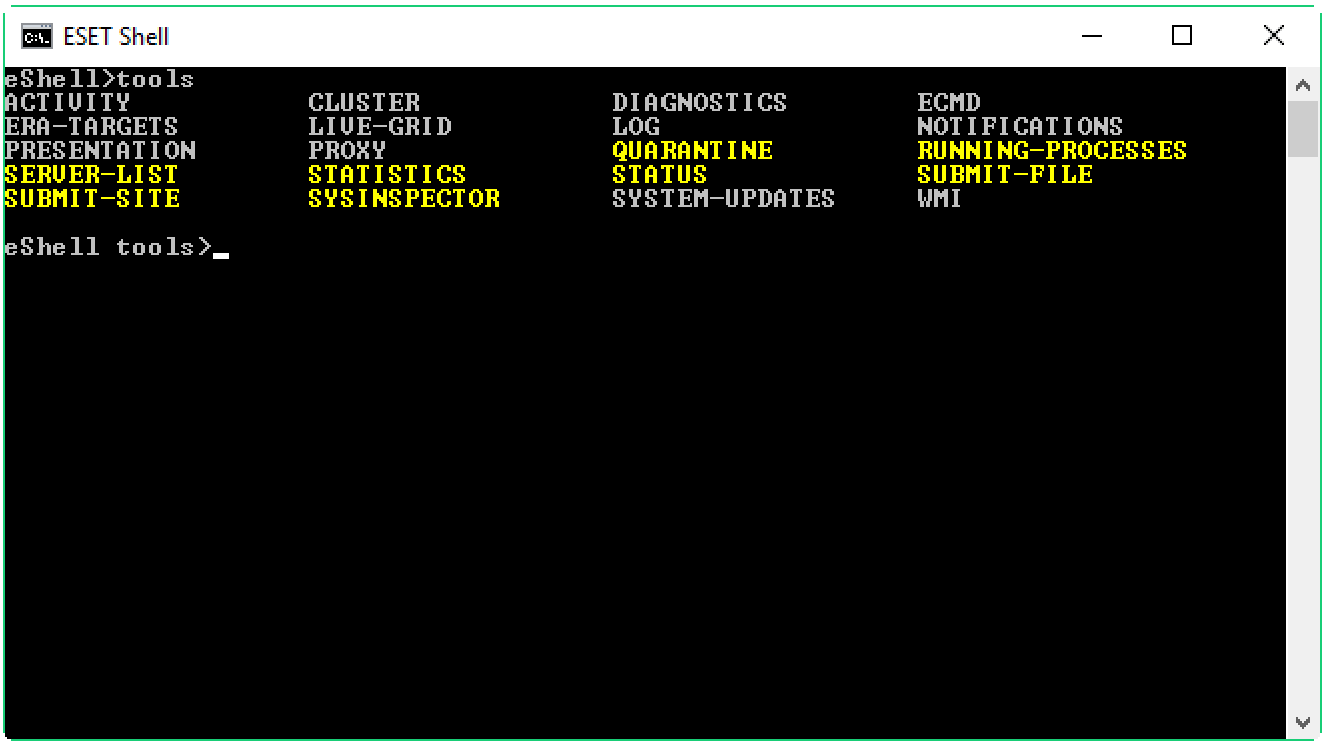
> NOTE
> Prefixes such as `GET` and `SET` are used with many commands, but some commands (such as `EXIT`) do not use a prefix.

Command path / Context

Commands are placed in contexts which form a tree structure. The top level of the tree is root. When you run eShell, you are at the root level:

```
eShell>
```

You can either execute a command from here, or enter the context name to navigate within the tree. For example, when you enter `TOOLS` context, it will list all commands and sub-contexts that are available from here.



```
eShell>tools
ACTIVITY            CLUSTER             DIAGNOSTICS         ECMD
ERA-TARGETS         LIVE-GRID           LOG                 NOTIFICATIONS
PRESENTATION        PROXY               QUARANTINE          RUNNING-PROCESSES
SERVER-LIST         STATISTICS          STATUS              SUBMIT-FILE
SUBMIT-SITE         SYSINSPECTOR        SYSTEM-UPDATES      WMI

eShell tools>_
```

Yellow items are commands you can execute and grey items are sub-contexts you can enter. A sub-context contain further commands.

If you need to return back to a higher level, use `..` (two dots).

EXAMPLE
Say you are here:
`eShell computer real-time>`
type `..` to go up one level, to:
`eShell computer>`

If you want to get back to root from `eShell computer real-time>` (which is two levels lower than root), simply type `.. ..` (two dots and two dots separated by space). By doing so, you will get two levels up, which is root in this case. Use backslash `\` to return directly to root from any level no matter how deep within the context tree you are. If you want to get to a particular context in upper levels, simply use the appropriate number of `..` commands to get to the desired level, using space as a separator. For example, if you want to get three levels higher, use `.. .. ..`

The path is relative to the current context. If the command is contained in the current context, do not enter a path. For example, to execute `GET COMPUTER REAL-TIME STATUS` enter:

`GET COMPUTER STATUS` - if you are in the root context (command line shows `eShell>`)
`GET STATUS` - if you are in the context `COMPUTER` (command line shows `eShell computer>`)
`.. GET STATUS` - if you are in the context `COMPUTER REAL-TIME` (command line shows `eShell computer real-time>`)

You can use single `.` (dot) instead of two `..` because single dot is an abbreviation of two dots.

EXAMPLE
`. GET STATUS` - if you are in the context `COMPUTER REAL-TIME` (command line shows `eShell computer real-time>`)

Argument

An argument an action which is performed for a particular command. For example, command `CLEAN-LEVEL` (located in `COMPUTER REAL-TIME ENGINE`) can be used with following arguments:

`rigorous` - Always remedy detection
`safe` - Remedy detection if safe, keep otherwise
`normal` - Remedy detection if safe, ask otherwise
`none` - Always ask the end-user

Another example are the arguments `ENABLED` or `DISABLED`, which are used to enable or disable a certain feature or functionality.

Abbreviated form / Shortened commands

eShell allows you to shorten contexts, commands and arguments (provided the argument is a switch or an alternative option). It is not possible to shorten a prefix or argument that are concrete values such as a number, name or path. You can use numbers `1` and `0` instead of enabled and disabled arguments.

EXAMPLE
```
computer set real-time status enabled    =>   com set real stat 1
computer set real-time status disabled    =>   com set real stat 0
```

Examples of the short form:

EXAMPLE
```
computer set real-time status enabled    =>   com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext    =>   com
excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1    =>   com excl rem det 1
```

In a case where two commands or contexts start with the same letters (such as `ADVANCED` and `AUTO-EXCLUSIONS`, and you enter `A` as shortened context), eShell will not be able to decide which context of these two you want to enter. An error message will display and list commands starting with "A" which you can choose from:

```
eShell>a

The following command is not unique: a
```

The following sub-contexts are available in `COMPUTER` context:

`ADVANCED`

`AUTO-EXCLUSIONS`

By adding one or more letter (for example, `AD` instead of just `A`) eShell will enter `ADVANCED` sub-context since it is unique now. The same applies to abbreviated commands.

> NOTE
> When you want to be sure that a command executes the way you need, we recommend that you do not abbreviate commands, arguments, etc. and use the full form. This way, eShell will execute exactly what you need and prevent unwanted mistakes. This is especially true for batch files / scripts.

Automatic completion

This new feature was introduced in eShell 2.0 and is very similar to automatic completion in Windows Command Prompt. While Windows Command Prompt completes file paths, eShell completes commands, context and operation names. Argument completion is not supported. When typing command simply, press Tab to complete or cycle through available variations. Press Shift + Tab to cycle backwards. Mixing abbreviated form and automatic completion is not supported. Use either one or the other. For example, when you type `computer real-time additional` hitting Tab will do nothing. Instead, type `com` and then Tab to complete `computer`, continue typing `real` + Tab, and `add` + Tab, hit Enter. Type `on` + Tab and continue hitting Tab to cycle through all available variations: `on-execute-ah`, `on-execute-ah-removable`, `on-write-ah`, `on-write-archive-default`, etc.

Aliases

An alias is an alternative name which can be used to execute a command (provided that the command has an alias assigned). There are a few default aliases:

`(global) close` - exit
`(global) quit` - exit
`(global) bye` - exit
`warnlog` - tools log events
`virlog` - tools log detections

"(global)" means that the command can be used anywhere regardless of current context. One command can have multiple aliases assigned, for example the command `EXIT` has aliases `CLOSE`, `QUIT` and `BYE`. When you want to exit eShell, you can use the `EXIT` command itself or any of its aliases. The alias `VIRLOG` is an alias for the command `DETECTIONS` which is located in the `TOOLS LOG` context. This way the detections command is available from the `ROOT` context, making it easier to access (you don't have to enter `TOOLS` and then `LOG` sub-context and run it directly from `ROOT`).

eShell allows you to define your own aliases. Command `ALIAS` can be found in `UI ESHELL` context.

Password protected settings

ESET Mail Security settings can be protected by a password. You can set a password using GUI or eShell using the `set ui access lock-password`. You'll then have to enter this password interactively for certain commands (such as those that change settings or modify data). If you plan to work with eShell for a longer period of time and do not want to enter the password repeatedly, you can get eShell to remember the password using the `set password` command (execute from `root`). Your password will then be filled-in automatically for each executed command that requires a password. It is remembered until you exit eShell, this means that you'll need to use `set password` again when you start a new session and want eShell to remember your password.

Guide / Help

When you run the `GUIDE` or `HELP` command, it will display a "first run" screen explaining how to use eShell. This command is available only from the ROOT context (eShell>).

Command history

eShell keeps a history of previously executed commands. This applies only to the current eShell interactive session. Once you exit eShell, the command history will be dropped. Use the Up and Down arrow keys on your keyboard to navigate through the history. Once you find the command you were looking for, you can execute it again, or modify it without having to type in the entire command from the beginning.

CLS / Clear screen

The CLS command can be used to clear the screen. It works the same way as it does with Windows Command Prompt or similar command line interfaces.

EXIT / CLOSE / QUIT / BYE

To close or exit eShell, you can use any of these commands (EXIT, CLOSE, QUIT or BYE).

Commands

This section lists a few basic eShell commands with descriptions.

> NOTE
> Commands are not case sensitive, you can use uppercase (capital) or lowercase letters and the command will execute regardless.

Example commands (contained within the ROOT context):

ABOUT

Lists information about the program. It shows information such as:

- Name of your ESET security product installed and its version number.
- Operating system and basic hardware details.
- Username (including domain), Full computer name (FQDN, if your server is a member of a domain) and Seat name.
- Installed components of your ESET security product, including version number of each component.

CONTEXT PATH:

```
root
```

PASSWORD

Normally, to execute password-protected commands, you are prompted to type in a password for security reasons. This applies to commands such as those that disable protection and those that may affect ESET Mail Security configuration. You will be prompted for a password every time you execute such a command. You can define this password in order to avoid entering a password every time. It will be remembered by eShell and automatically entered when a password-protected command is executed.

NOTE
Your password only works for the current eShell interactive session. Once you exit eShell, this defined password will be dropped. When you start eShell again, the password needs to be defined again.

Defined password can also be used when running unsigned batch files or scripts. Make sure to set ESET Shell execution policy to Full access when running unsigned batch files. Here is an example of such a batch file:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

This concatenated command above defines a password and disables protection.

IMPORTANT
We recommend you to use signed batch files whenever possible. This way, you'll avoid having plain text passwords in the batch file (if using the method described above). See Batch files / Scripting (Signed batch files section) for more details.

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERATIONS:

`get` - Show password

`set` - Set or clear password

`restore` - Clear password

ARGUMENTS:

`plain` - Switch to enter password as parameter

`password` - Password

EXAMPLES:

`set password plain <yourpassword>` - Sets a password which will be used for password-protected commands

`restore password` - Clears password

EXAMPLES:

`get password` - Use this to see whether the password is configured or not (this only shows asterisks "*", it does not list the password itself), when no asterisks are visible, it means that there is no password set

`set password plain <yourpassword>` - Use this to set a defined password

`restore password` - This command clears the defined password

STATUS

Shows information about the current Real-time protection status of ESET Mail Security, also enables you to pause / resume protection (similar to GUI).

CONTEXT PATH:

```
computer real-time
```

SYNTAX:

```
[get] status

set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]

restore status
```

OPERATIONS:

`get` - Returns current setting/status

`set` - Sets value/status

`restore` - Restores default settings/object/file

ARGUMENTS:

`enabled` - Enable protection/feature

`disabled` - Disable protection/feature

`10m` - Disable for 10 minutes

`30m` - Disable for 30 minutes

`1h` - Disable for 1 hour

`4h` - Disable for 4 hours

`temporary` - Disable until reboot

> NOTE
> It is not possible to disable all protection features with a single command. You can manage protection features and modules one by one using `status` command. Each protection feature or module has its own `status` command.

List of features with `status` command:

Feature	Context and command
Automatic exclusions	`COMPUTER AUTO-EXCLUSIONS STATUS`
Host Intrusion Prevention System (HIPS)	`COMPUTER HIPS STATUS`
Real-time file system protection	`COMPUTER REAL-TIME STATUS`
Device control	`DEVICE STATUS`

Feature	Context and command
Botnet protection	NETWORK ADVANCED STATUS-BOTNET
Network attack protection (IDS)	NETWORK ADVANCED STATUS-IDS
Network isolation	NETWORK ADVANCED STATUS-ISOLATION
ESET Cluster	TOOLS CLUSTER STATUS
Diagnostic logging	TOOLS DIAGNOSTICS STATUS
Presentation mode	TOOLS PRESENTATION STATUS
Anti-Phishing protection	WEB-AND-EMAIL ANTIPHISHING STATUS
Email client protection	WEB-AND-EMAIL MAIL-CLIENT STATUS
Web access protection	WEB-AND-EMAIL WEB-ACCESS STATUS

VIRLOG

This is an alias of the DETECTIONS command. It is useful when you need to view information about detected infiltrations.

WARNLOG

This is an alias of the EVENTS command. It is useful when you need to view information about various events.

Batch files / Scripting

You can use eShell as a powerful scripting tool for automation. To use a batch file with eShell, create one with an eShell and command in it.

EXAMPLE

```
eshell get computer real-time status
```

You can also chain commands, which is sometimes necessary, for instance if you want to type a particular scheduled task, enter the following:

```
eshell select scheduler task 4 "&" get scheduler action
```

Item selection (task number 4 in this case) usually applies only to a currently running instance of eShell. If you were to run these two commands one after the other, the second command would fail with the error "No task selected or selected task no longer exists".

For security reasons, the execution policy is set to **Limited Scripting** by default. This allows you to use eShell as a monitoring tool, but it won't let you make configuration changes to ESET Mail Security by running a script. If you try executing a script with commands that can affect security, for example, by disabling protection, an **Access Denied** message will be displayed. We recommend that you use signed batch files to execute commands that make configuration changes.

To change configuration using a single command entered manually in the Windows Command Prompt, you must grant eShell full access (not recommended). To grant full access, use `ui eshell shell-execution-policy` in the Interactive mode of eShell itself, or via GUI in **Advanced Setup** (**F5**)> **User interface** > ESET Shell.

Signed batch files

eShell allows you to secure common batch files (*.bat) with a signature. Scripts are signed with the same password that is used for settings protection. In order to sign a script you need to enable settings protection first. This can be done via the GUI, or from within eShell using `set ui access lock-password` command. Once the settings protection password is set up you can start signing batch files.

> NOTE
> If you change your settings protection password, you must sign all scripts again, otherwise the scripts will fail to execute the following the password change. The password entered when signing a script must match the settings protection password on the target system.

To sign a batch file, run `sign <script.bat>` from the root context of eShell, where *script.bat* is the path to the script you want to sign. Enter and confirm the password that will be used for signing. This password must match your settings protection password. A signature is placed at the end of the batch file in the form of a comment. If this script has already been signed, the signature will be replaced with a new one.

> NOTE
> When you modify a previously signed batch file, it must be signed again.

To execute a signed batch file from a Windows Command Prompt or as a scheduled task, use following command:

```
eshell run <script.bat>
```

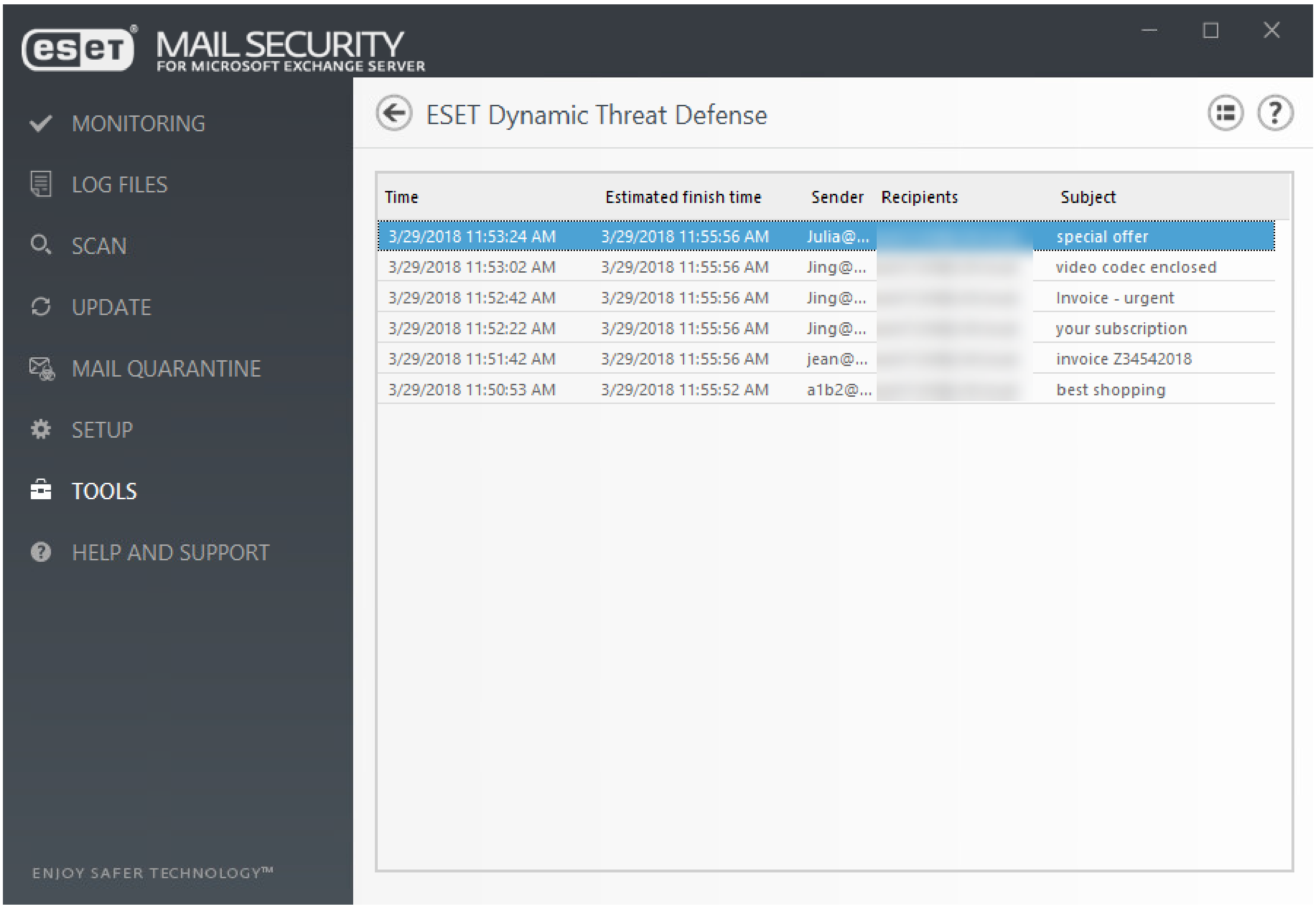
Where script.bat is the path to the batch file.

> EXAMPLE
> `eshell run d:\myeshellscript.bat`

ESET Dynamic Threat Defense

ESET Dynamic Threat Defense (EDTD) provides another layer of security by utilizing advanced ESET Cloud-based technology to detect new, never-before-seen type of threats. It is a paid service, while it is similar to ESET LiveGrid®, ESET Dynamic Threat Defense gives you the advantage of being protected against possible consequences caused by new threats. If ESET Dynamic Threat Defense detects suspicious code, or behavior, it prevents further threat activity by temporarily putting it into the ESET Dynamic Threat Defense quarantine. A suspicious sample (file or email message) is automatically submitted to the ESET Cloud where the ESET Dynamic Threat Defense server analyzes the sample using its cutting edge malware detection engines. While files or emails are in the ESET Dynamic Threat Defense quarantine, ESET Mail Security is waiting for the results from ESET Dynamic Threat Defense server. After the analysis is completed, your ESET Mail Security receives a report with a summary of the observed sample's behavior. If the sample proves to be harmless, it is released from the ESET Dynamic Threat Defense quarantine, otherwise, it is kept in quarantine. If it is a false positive, and you are sure the file or email is not a threat, you can manually release it from the ESET Dynamic Threat Defense quarantine before ESET Mail Security receives the ESET Dynamic Threat Defense server results.

ESET Dynamic Threat Defense results for samples usually arrive within a few minutes for email messages. However, the default waiting interval is set to 5 minutes. In a rare cases, when ESET Dynamic Threat Defense results do not arrive within the interval, the message is released. You can change the interval to your preferred time (anything between 5 to 60 minutes, in 1 minute increments).



Time	Estimated finish time	Sender	Recipients	Subject
3/29/2018 11:53:24 AM	3/29/2018 11:55:56 AM	Julia@...	[redacted]	special offer
3/29/2018 11:53:02 AM	3/29/2018 11:55:56 AM	Jing@...	[redacted]	video codec enclosed
3/29/2018 11:52:42 AM	3/29/2018 11:55:56 AM	Jing@...	[redacted]	Invoice - urgent
3/29/2018 11:52:22 AM	3/29/2018 11:55:56 AM	Jing@...	[redacted]	your subscription
3/29/2018 11:51:42 AM	3/29/2018 11:55:56 AM	jean@...	[redacted]	invoice Z34542018
3/29/2018 11:50:53 AM	3/29/2018 11:55:52 AM	a1b2@...	[redacted]	best shopping

ESET Dynamic Threat Defense feature is visible in ESET Mail Security regardless of its activation status. If you do not have a license, ESET Dynamic Threat Defense is inactive. ESET Dynamic Threat Defense license is managed by ESET Security Management Center and the activation itself must be performed from ESET Security Management Center using a policy.

Once you have ESET Dynamic Threat Defense activated, your own ESET Dynamic Threat Defense profile will be created on the ESET Dynamic Threat Defense server. This profile will store all of the ESET Dynamic Threat Defense analysis results of samples submitted by your ESET Mail Security.

To get the ESET Dynamic Threat Defense feature working, you must meet the following:

ESET Mail Security managed via ESET Security Management Center

ESET Mail Security activated using ESET Dynamic Threat Defense license

Enable ESET Dynamic Threat Defense in your ESET Mail Security using ESET Security Management Center policy

You are then able to take the full advantage of ESET Dynamic Threat Defense, as well as, manually submit a sample file for ESET Dynamic Threat Defense analysis.

ESET SysInspector

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

Click **Create** and enter a short **Comment** describing the log to be created. Wait until the ESET SysInspector log is generated (status will be shown as Created). Log creation may take some time depending on your hardware configuration and system data.

The ESET SysInspector window displays the following information about created logs:

- **Time** - The time of log creation.
- **Comment** - A short comment.
- **User** - The name of the user who created the log.
- **Status** - The status of log creation.

The following actions are available:

- **Show** - Opens the created log. You can also right-click a log and select Show from the context menu.
- **Compare** - Compares two existing logs.
- **Create** - Creates a new log. Enter a short comment describing the log to be created and click Create. Please wait until the ESET SysInspector log is complete (Status will be shown as Created).
- **Delete** - Removes selected logs from the list.

After right-clicking one or more selected logs, the following options are available from the context menu:

- **Show** - Opens the selected log in ESET SysInspector (same function as double-clicking a log).
- **Compare** - Compares two existing logs.
- **Create -** Creates a new log. Enter a short comment describing the log to be created and click **Create**. Please wait until the ESET SysInspector log is complete (**Status** will be shown as Created).
- **Delete** - Removes selected logs from the list.
- **Delete all** - Deletes all logs.
- **Export** - Exports the log to an .xml file or zipped .xml.

ESET SysRescue Live

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

The main advantage of ESET SysRescue Live is the fact that the ESET Security solution runs independent of the host operating system but has direct access to the disk and file system. This makes it possible to remove threats which normally could not be deleted (for example, when the operating system is running, etc.).

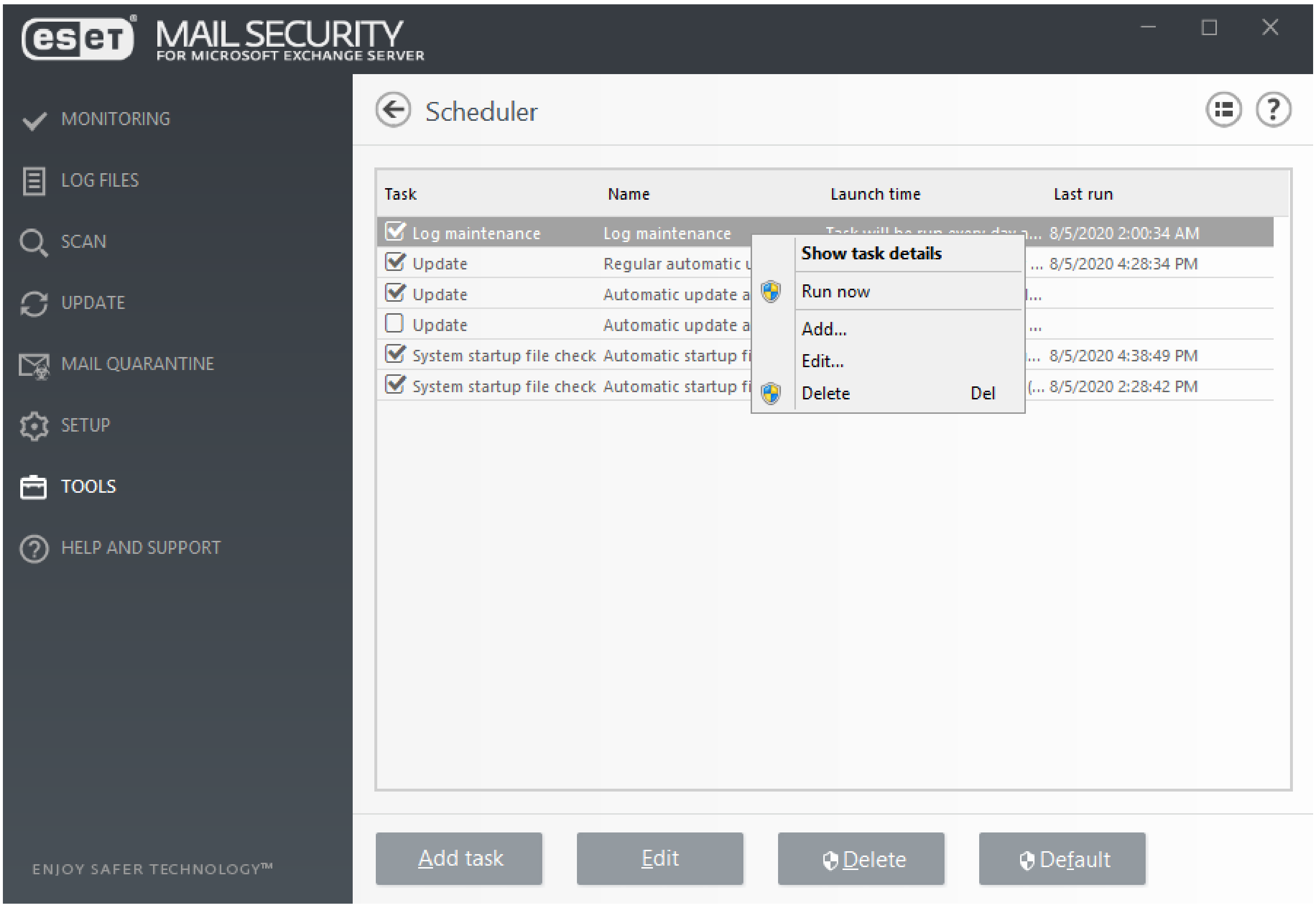
Scheduler

Scheduler manages and launches scheduled tasks according to defined parameters. You can see a list of all scheduled tasks in the form of a table which shows their parameters such as Task type and name, the launch time and last run when it was performed. You can also create new scheduled tasks by clicking Add task. To edit the configuration of an existing scheduled task click **Edit** button. Revert the list of scheduled tasks to the default settings, click **Default** and than **Revert to default** all changes that have been made will be lost and cannot be undone.

There is a set of predefined default tasks:

- Log maintenance
- Regular automatic update (use this task to update frequency)
- Automatic update after dial-up connection
- Automatic update after user logon
- Automatic startup file check (after user logs in)
- Automatic startup file check (after successful modules update)

> NOTE
> Select the appropriate check boxes to activate or deactivate tasks.



Task	Name	Launch time	Last run
☑ Log maintenance	Log maintenance	Task will be run every day a...	8/5/2020 2:00:34 AM
☑ Update	Regular automatic u	...	8/5/2020 4:28:34 PM
☑ Update	Automatic update a	l...	
□ Update	Automatic update a	...	
☑ System startup file check	Automatic startup fi	...	8/5/2020 4:38:49 PM
☑ System startup file check	Automatic startup fi	(...	8/5/2020 2:28:42 PM

To perform the following actions, right-click a task:

Show task details	Displays detailed information about a scheduled task when you double-click or right-click the scheduled task.
Run now	Runs a selected scheduler task and perform the task immediately.
Add...	Launches a wizard that will help you create a new scheduler task.
Edit...	Edit the configuration of an existing scheduled task (both default and user-defined).
Delete	Deletes an existing task.

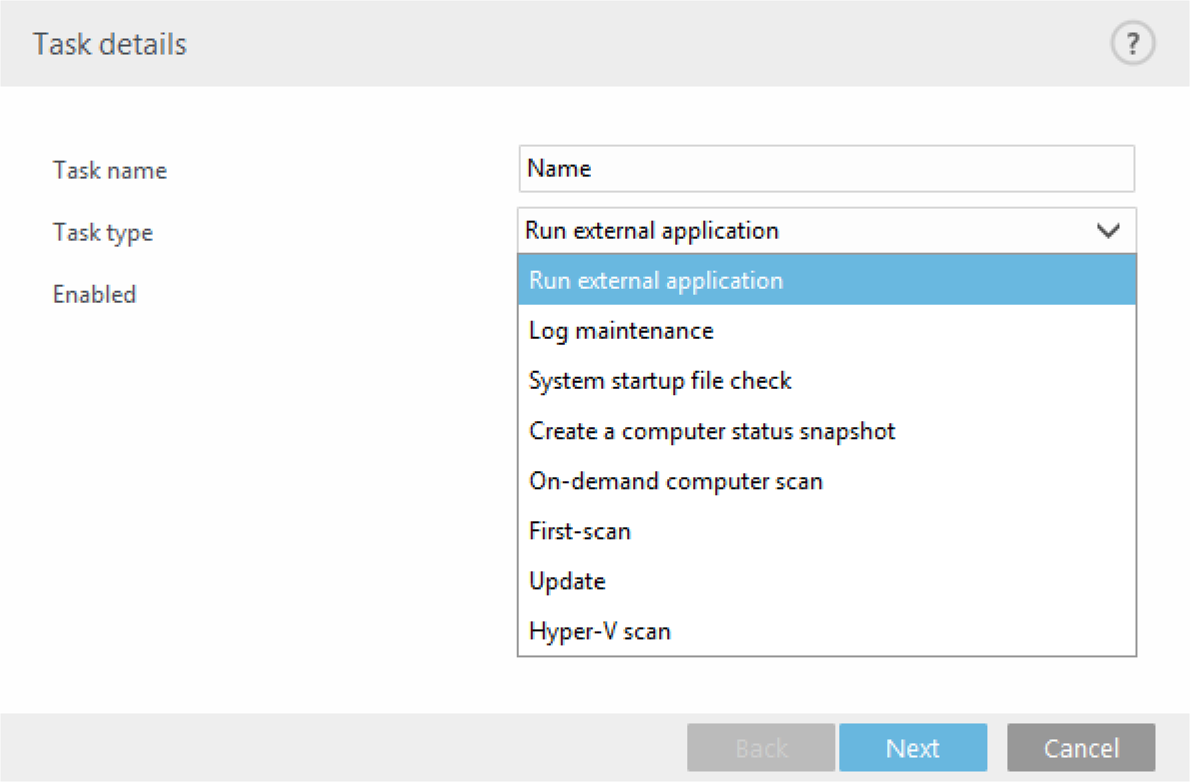
Scheduler - Add task

To create a new scheduled task:

1. Click **Add task**.

2.Enter a **Task name** and configure your custom scheduled task.

3.Task type - Select the applicable **Task type** from drop down menu.



Task details

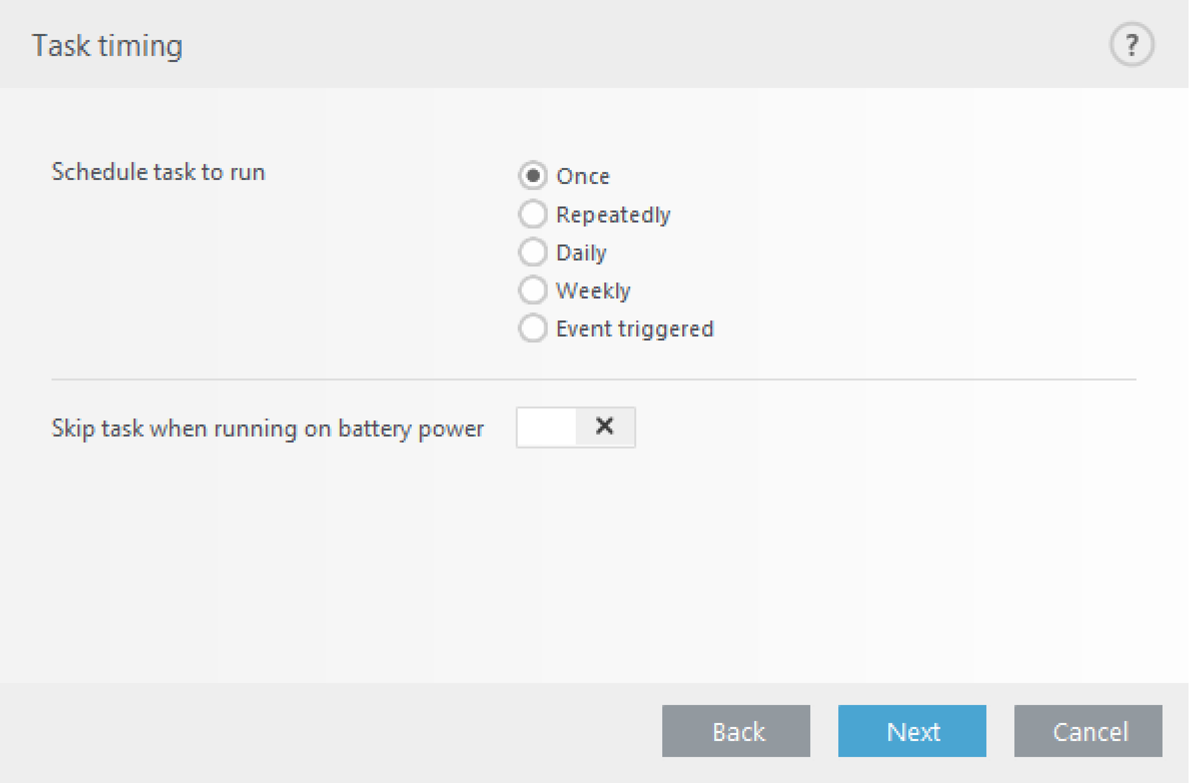
Task name: Name

Task type: Run external application

Enabled

NOTE
To deactivate a task, click the slide bar next to **Enabled**. To activate the task later, use the check box in the Scheduler view.

4.Task Timing - Select one of the options to define when you want your task to run. Depending on your choice, you will be prompted to choose a specific time, day, interval or an event.



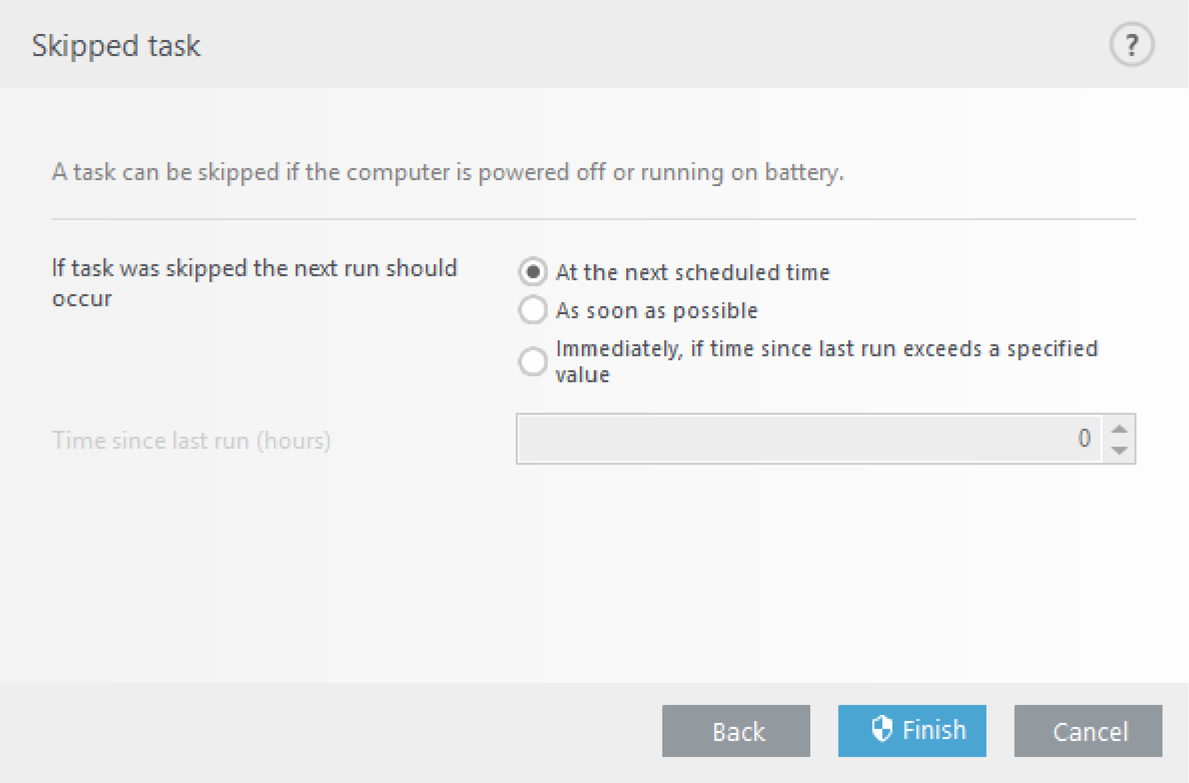
Task timing

Schedule task to run

● Once
○ Repeatedly
○ Daily
○ Weekly
○ Event triggered

Skip task when running on battery power ✕

5.Skipped task - If the task could not be run at the predefined time, you can specify when it will be performed.



Skipped task

A task can be skipped if the computer is powered off or running on battery.

If task was skipped the next run should occur

● At the next scheduled time
○ As soon as possible
○ Immediately, if time since last run exceeds a specified value

Time since last run (hours) 0

6.Run application - If the task is scheduled to run an external application, choose an executable file from the directory tree.

7.If you need to make changes, click **Back** to return to previous step(s) and modify parameters.

8.Click **Finish** to create the task or apply changes.

The new scheduled task will appear in the Scheduler view.

Task type

The configuration wizard is different for each **Task type** of a scheduled task. Enter **Task name** and select your desired **Task type** from the drop-down menu:

- **Run external application -** Schedules the execution of an external application.
- **Log maintenance -** Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check -** Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot -** Creates an ESET SysInspector computer snapshot - gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
- **On-demand computer scan -** Performs a computer scan of files and folders on your computer.
- **Update -** Schedules an update task to perform an update of detection engine and program modules.
- **Mailbox database scan -** Lets you schedule a database scan and choose items that will be scanned. It is basically an On-demand database scan.

NOTE
If you have Mailbox database protection enabled, you can still schedule this task, but the error message Mailbox database scan - Scan interrupted because of an error will be displayed in the Scan section of the main GUI. To prevent this, ensure that Mailbox database protection is disabled during the time that Mailbox Database scan is scheduled to run.

- **Send mail quarantine reports -** Schedules a Mail Quarantine report to be sent via email.
- **Send mail quarantine administrator reports -** Schedules a Mail Quarantine report to be sent via email.
- **Background scan -** Gives Exchange Server an opportunity to run database background scan if needed.
- **Hyper-V scan -** Schedules a scan of the virtual disks within Hyper-V.
- **Office 365 scan** - Schedules a scan for Office 365 Hybrid environments.

To deactivate a task once it is created, click the switch next to **Enabled**. To activate the task later, click the check box in the Scheduler view. Click **Next** to proceed to the next step.

Task timing

Select one of the following timing options:

- **Once -** The task will be performed only once at specified date and time. To run the task one time only, at a given moment. Specify the start date and time for one-time in **Task execution**.
- **Repeatedly -** The task will be performed at the specified time interval (in minutes). Specify the time at

which the task will be executed every day in **Task execution**.

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

- **Weekly -** The task will run one or more times a week, on the selected day(s) and time. To run the task repeatedly only in certain days of the week starting with specified day and time. Specify the start time in the Time of task execution. Select the day or days of week on which the task should be run.

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

If you enable **Skip task when running on battery power**, a task will not start if the system is running on batteries at the time the task should launch. For example, computers running on UPS.

Event triggered

When scheduling a task triggered by an event, you can specify the minimum interval between two completions of the task.

The task can be triggered by any of the following events:

- **Every time the computer starts**

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

- **Dial-up connection to the Internet/VPN**

- **Successful module update**

- **Successful product update**

- **User logon** - The task will deploy when the user logs on to the system. If you log on to your computer several times a day, choose 24 hours to perform the task only on the first logon of the day and then the next day.

- **Threat detection**

Run application

This task schedules the execution of an external application.

- **Executable file -** Choose an executable file from the directory tree, click **browse (...)** or enter the path manually.

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

- **Parameters -** Command line parameters for the application (optional).

Skipped task

If the task could not be run at the predefined time, you can specify when it will be performed:

- **At the next scheduled time -** The task will be executed at the specified time (for example after 24 hours).

- **As soon as possible -** The task will run as soon as possible, when the actions that prevent the task from executing are no longer valid.

- **Immediately, if time since last run exceeds a specified value - Time since last run (hours) -** After you select this option, your task will be always repeated after the specified amount of time (in hours).

Scheduled task overview

This dialog window displays detailed information about a scheduled task when you double-click the task in **Scheduler view**, or right-click the scheduled task and choose **Show task details**.

Submit samples for analysis

The sample submission dialog allows you to send a file or site to ESET for analysis. If you find a suspiciously behaving file on your computer or suspicious site on the Internet, submit it to the ESET Virus Lab for analysis. If the file turns out to be a malicious application or website, the detection will be added to an upcoming update.

To submit the file by email, compress the file(s) using a program like WinRAR or WinZip, protect the archive with the password *infected* and send it to samples@eset.com. Use a descriptive subject and enclose as much information about the file as possible (for example, the website you downloaded it from).

Before submitting a sample to ESET, verify it meets one or both of the following criteria:

- the file or website is not detected at all
- the file or website is incorrectly detected as a threat

If at least one of the requirements above is not met, you will not receive a response until further information is supplied.

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

- Suspicious file
- Suspicious site (a website that is infected by malware)
- False positive file (a file that is detected as infected, but it is not)
- False positive site
- Other

File/Site

The path to the file or website you intend to submit.

Contact email

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

Submit anonymously

Use the check box next to **Submit anonymously** to send suspicious file or website without entering your email address.

Suspicious file

Observed signs and symptoms of malware infection

Enter a description of the suspicious file behavior observed on your computer.

File origin (URL address or vendor)

Enter the file origin (source) and how you encountered this file.

Notes and additional information

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

> NOTE
> The first parameter - **Observed signs and symptoms of malware infection** - is required, but providing additional information will significantly help our laboratories with the identification process of samples.

Suspicious site

Select one of the following from the **What's wrong with the site** drop-down menu:

Infected

A website that contains viruses or other malware distributed by various methods.

Phishing

Often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this type of attack in the glossary.

Scam

A swindle or a fraudulent website.

Other

Use this option if none of the options above apply to the site you are going to submit.

Notes and additional information

You can enter further information or a description that might help analyzing the suspicious website.

False positive file

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

> NOTE
> **The** first three parameters are required to identify legitimate applications and distinguish them from malicious code. By providing additional information, you will help our laboratories significantly in the identification process and in the processing of samples.

Application name and version

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

File origin (URL address or vendor)

Enter a file origin (source) and note how you encountered this file.

Application's purpose

The general application description, type of application (for example, browser, media player, ...) and its functionality.

Notes and additional information

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

False positive site

We encourage you to submit sites that are detected as an infected, scam or phishing sites but are not. False positives (FP) may occur when a pattern of a file matches the same pattern contained in a detection engine. Please provide this website to improve our detection engine and help others to be protected.

Notes and additional information

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

Other

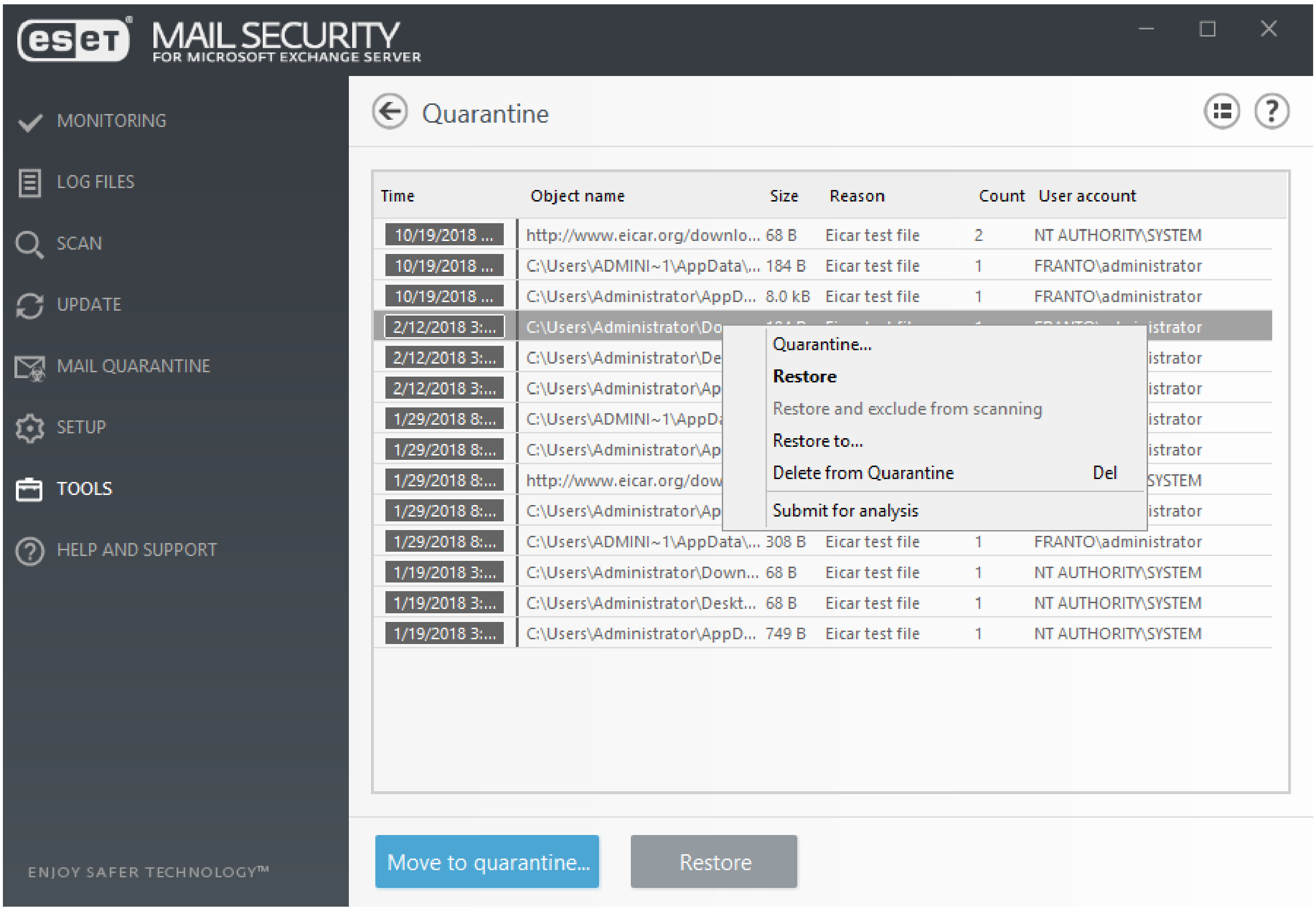
Use this form if the file cannot be categorized as a **Suspicious file** or **False positive**.

Reason for submitting the file

Enter a detailed description and the reason for sending the file.

Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are being falsely detected by ESET Mail Security. You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the malware scanner. Quarantined files can be submitted for analysis to the ESET Virus Lab.



Time	Object name	Size	Reason	Count	User account
10/19/2018 ...	http://www.eicar.org/downlo...	68 B	Eicar test file	2	NT AUTHORITY\SYSTEM
10/19/2018 ...	C:\Users\ADMINI~1\AppData\...	184 B	Eicar test file	1	FRANTO\administrator
10/19/2018 ...	C:\Users\Administrator\AppD...	8.0 kB	Eicar test file	1	FRANTO\administrator
2/12/2018 3:...	C:\Users\Administrator\Do				istrator
2/12/2018 3:...	C:\Users\Administrator\De				istrator
2/12/2018 3:...	C:\Users\Administrator\Ap				istrator
1/29/2018 8:...	C:\Users\ADMINI~1\AppDa				istrator
1/29/2018 8:...	C:\Users\Administrator\Ap				istrator
1/29/2018 8:...	http://www.eicar.org/dow				SYSTEM
1/29/2018 8:...	C:\Users\Administrator\Ap				istrator
1/29/2018 8:...	C:\Users\ADMINI~1\AppData\...	308 B	Eicar test file	1	FRANTO\administrator
1/19/2018 3:...	C:\Users\Administrator\Down...	68 B	Eicar test file	1	NT AUTHORITY\SYSTEM
1/19/2018 3:...	C:\Users\Administrator\Deskt...	68 B	Eicar test file	1	NT AUTHORITY\SYSTEM
1/19/2018 3:...	C:\Users\Administrator\AppD...	749 B	Eicar test file	1	NT AUTHORITY\SYSTEM

Files stored in the quarantine folder can be viewed in a table that displays: the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (for example, object added by user), and number of threats (for example, if it is an archive containing multiple infiltrations).

In the event an email message objects are put into the file quarantine, a path to the mailbox/folder/filename is displayed.

Quarantining files

ESET Mail Security automatically quarantines deleted files (if you have not disabled this option in the alert window). To manually quarantine any suspicious file, click **Quarantine**. Quarantined files will be removed from their original location. The context menu can also be used for this purpose; right-click in the **Quarantine** window and select **Quarantine**.

Restoring from Quarantine

Quarantined files can also be restored to their original location. Use the **Restore** feature, available from the context menu by right-clicking a given file in the Quarantine window, to do so. If a file is marked as a potentially unwanted application, the **Restore and exclude from scanning** option will be available. The context menu also offers the **Restore to...** option, which allows you to restore a file to a location other than the one from which it was deleted.

> NOTE
> If the program quarantines a harmless file by mistake, exclude the file from scanning after restoring it and send the file to ESET Customer Care.

Submitting a file from the Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was determined to be infected incorrectly (for example, by heuristic analysis of the code) and subsequently quarantined, please send the file to the ESET Virus Lab. To submit a file from quarantine, right-click the file and select Submit for analysis from the context menu.

Deleting from Quarantine

Right-click on a given item and select **Delete from Quarantine**. Or select the applicable item(s) and press **Delete** on your keyboard.

Server protection settings

This is the main integration option. Use the slider bar to enable or disable **integration** of Mailbox database protection or Mail transport protection into your Exchange Server.

> NOTE
> If you are running Microsoft Exchange Server 2007 or 2010, you can choose between Mailbox database protection and On-demand mailbox database scan, only one protection type can be active at a time. If you decide to use On-demand mailbox database scan you will need to disable integration of Mailbox database protection. Otherwise On-demand mailbox database scan will not be available.

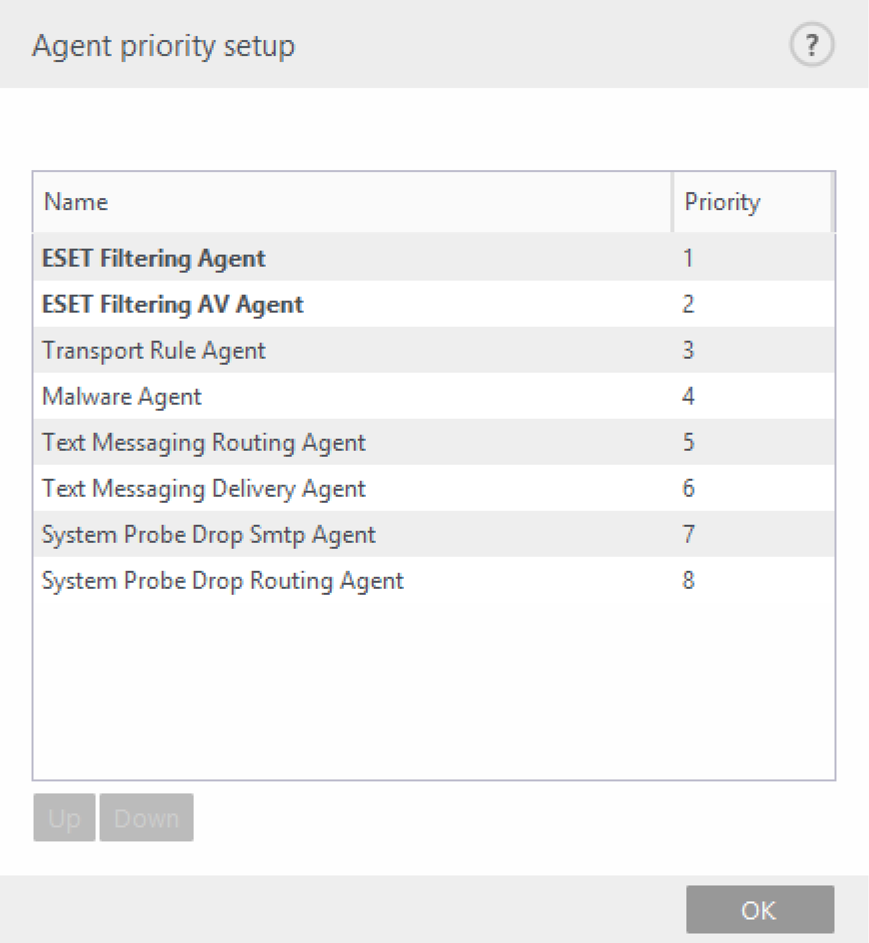
You can also modify Agent priority.

ESET Mail Security provides significant protection for your Microsoft Exchange Server using the following features:

- Antivirus and antispyware
- Antispam protection
- Anti-Phishing protection
- Rules
- Mail transport protection (Exchange Server 2007, 2010, 2013,2016, 2019)
- Mailbox database protection (Exchange Server 2007, 2010)
- On-demand mailbox database scan (Exchange Server 2007, 2010, 2013, 2016, 2019)
- Mail quarantine (Mail Quarantine type settings)

Agent priority setup

If required, you can specify the order in which ESET Mail Security Agents become active after the Microsoft Exchange Server has started. Numeric value defines the priority. Lower numbers denote higher priority. This applies to Microsoft Exchange Server 2007 and newer.



Agent priority setup

Name	Priority
ESET Filtering Agent	1
ESET Filtering AV Agent	2
Transport Rule Agent	3
Malware Agent	4
Text Messaging Routing Agent	5
Text Messaging Delivery Agent	6
System Probe Drop Smtp Agent	7
System Probe Drop Routing Agent	8

Up / Down

Increase or decrease the priority of a selected Agent by moving it up in the list of Agents.

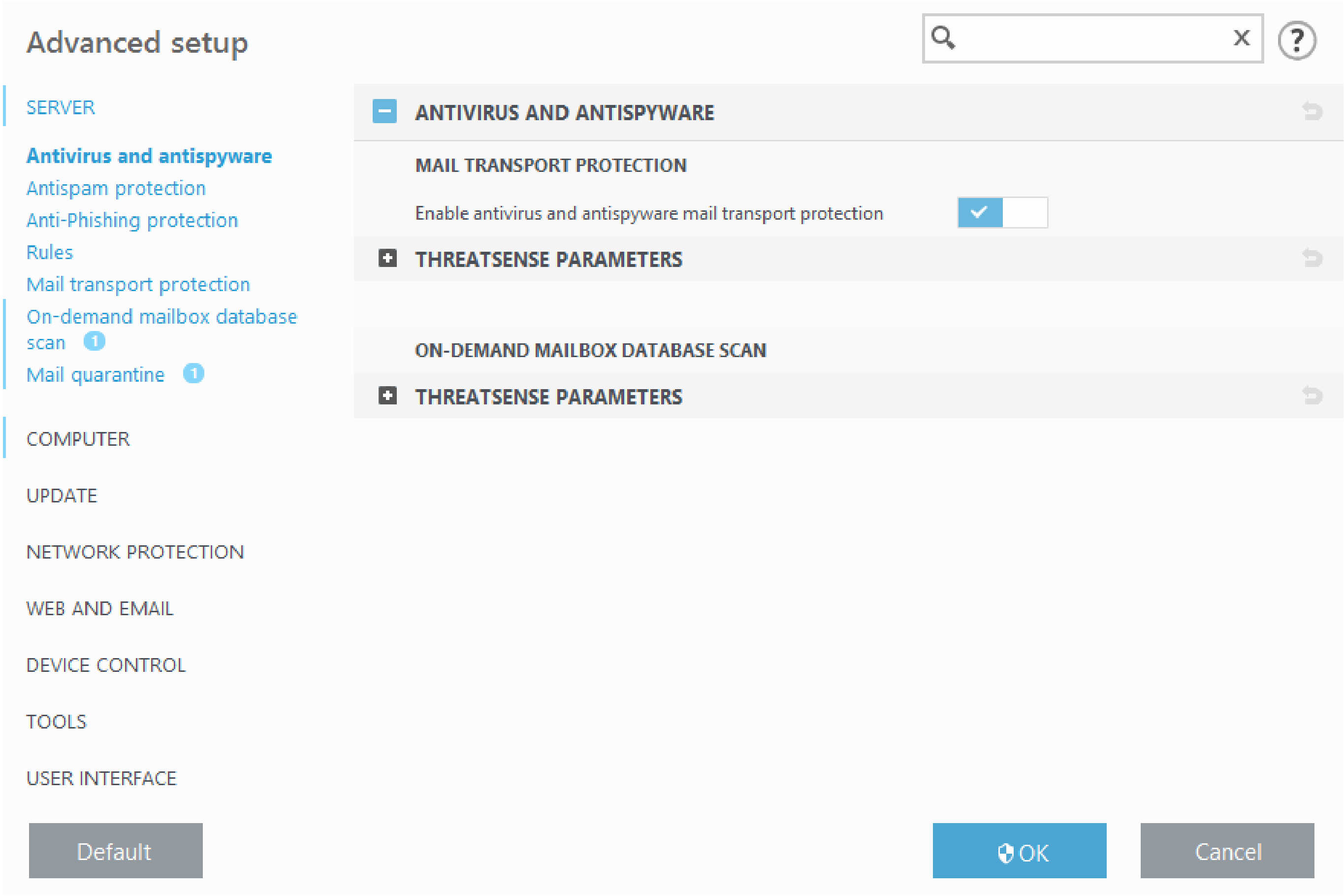
Antivirus and antispyware

In this section you can configure Antivirus and antispyware options for your mail server.

IMPORTANT
Mail transport protection is provided by transport agent and is only available for Microsoft Exchange Server 2007 and later, but your Exchange Server must have the **Edge Transport Server** or **Hub Transport Server role**. This also applies to a single server installation with multiple Exchange Server roles on one computer (as long as it has the Edge or Hub Transport role).

Mail transport protection

If you disable **Enable antivirus and antispyware mail transport protection**, the ESET Mail Security plug-in for Exchange server will not be unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses on the transport layer. Messages will still be scanned for viruses and spam on the database layer and existing rules will be applied.



ANTIVIRUS AND ANTISPYWARE

MAIL TRANSPORT PROTECTION

Enable antivirus and antispyware mail transport protection ✓

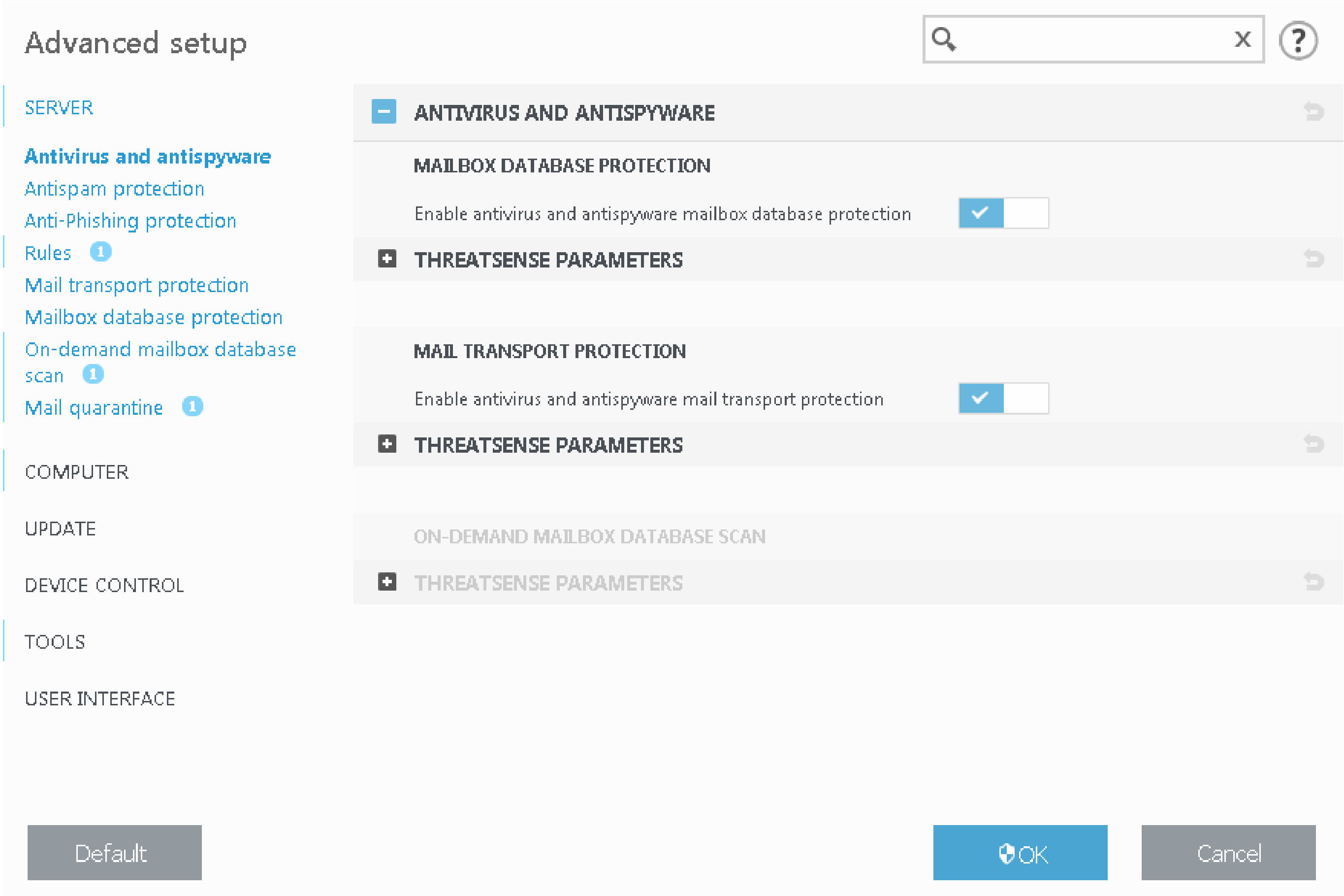
THREATSENSE PARAMETERS

ON-DEMAND MAILBOX DATABASE SCAN

THREATSENSE PARAMETERS

Mailbox database protection

If you disable **Enable antivirus and antispyware mailbox database protection**, the ESET Mail Security plug-in for Exchange server will not be unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses on database layer. Messages will still be scanned for viruses and spam on the transport layer and existing rules will be applied.



Advanced setup

SERVER

Antivirus and antispyware
Antispam protection
Anti-Phishing protection
Rules 1
Mail transport protection
Mailbox database protection
On-demand mailbox database scan 1
Mail quarantine 1

COMPUTER
UPDATE
DEVICE CONTROL
TOOLS
USER INTERFACE

ANTIVIRUS AND ANTISPYWARE

MAILBOX DATABASE PROTECTION

Enable antivirus and antispyware mailbox database protection ✓

THREATSENSE PARAMETERS

MAIL TRANSPORT PROTECTION

Enable antivirus and antispyware mail transport protection ✓

THREATSENSE PARAMETERS

ON-DEMAND MAILBOX DATABASE SCAN

THREATSENSE PARAMETERS

On-demand mailbox database scan

Is available after you disabled **Mailbox database protection** on Server section.

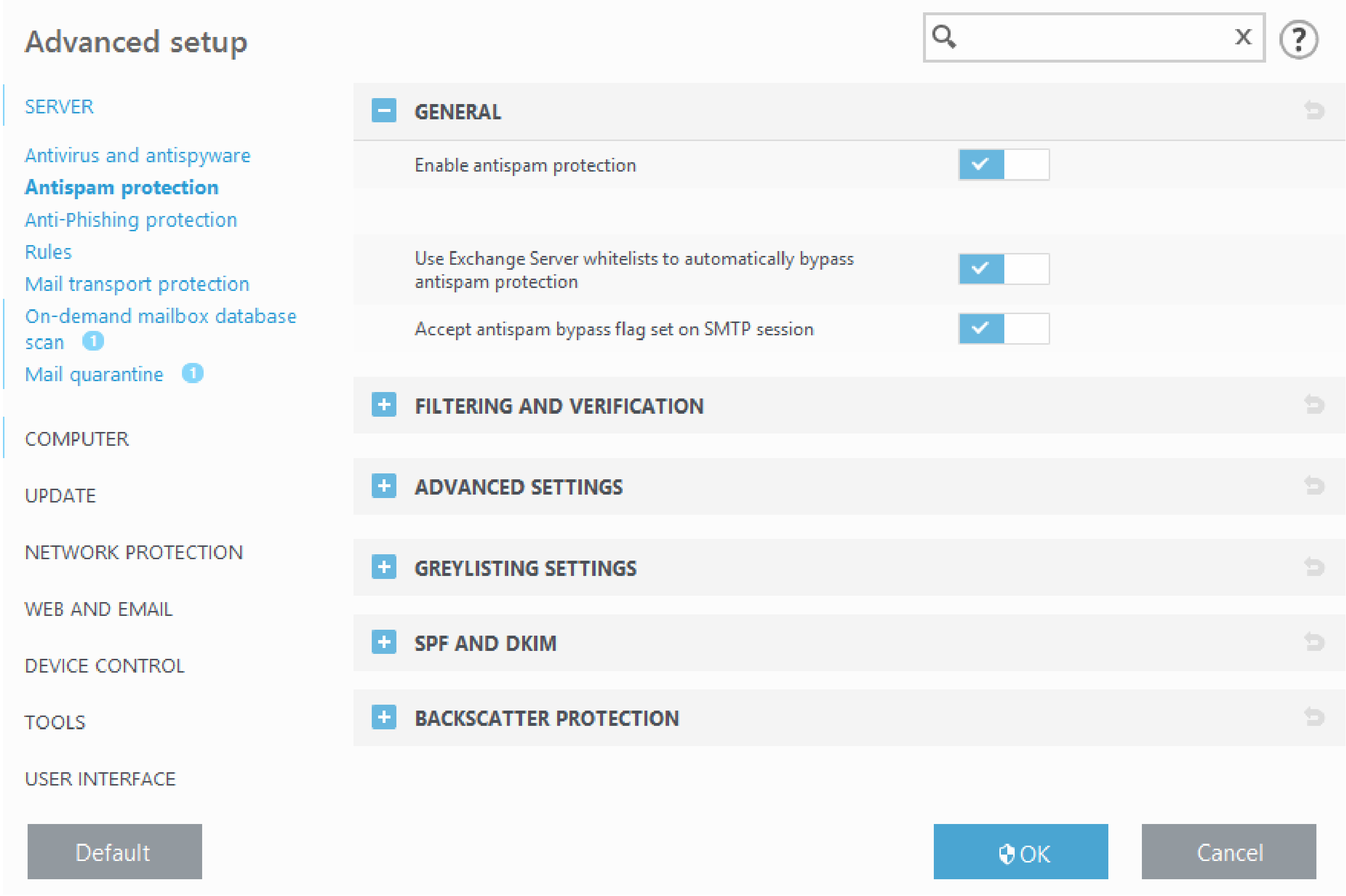
ThreatSense parameters

Modify scan parameters for the Mail transport protection, Mailbox database protection and On-demand mailbox database scan.

Antispam protection

Antispam protection for your mail server is enabled by default. To turn it off, use the slider bar next to **Enable antispam protection**.

> NOTE
> Disabling Antispam protection will not change the protection status. Even though the Antispam is disabled, you'll see the green **You are protected** is still displayed in the **Monitoring** section of the main GUI. Disabled Antispam is not considered a reduction in protection level.



Advanced setup

SERVER

Antivirus and antispyware
Antispam protection
Anti-Phishing protection
Rules
Mail transport protection
On-demand mailbox database scan 1
Mail quarantine 1

COMPUTER
UPDATE
NETWORK PROTECTION
WEB AND EMAIL
DEVICE CONTROL
TOOLS
USER INTERFACE

GENERAL

Enable antispam protection ✓

Use Exchange Server whitelists to automatically bypass antispam protection ✓

Accept antispam bypass flag set on SMTP session ✓

FILTERING AND VERIFICATION

ADVANCED SETTINGS

GREYLISTING SETTINGS

SPF AND DKIM

BACKSCATTER PROTECTION

Use Exchange Server whitelists to automatically bypass antispam protection

Lets ESET Mail Security use specific Exchange "whitelists". When enabled, the following is taken into consideration:

- The server IP address is on the Allowed IP list of the Exchange Server
- The message recipient has the Antispam Bypass flag set on his/her mailbox
- The message recipient has the sender's address on their Safe Senders List (make sure you have configured Safe Senders List Synchronization within your Exchange Server environment including Safelist Aggregation)

If any of the above applies to an incoming message, the Antispam check will be bypassed for this message, the message will not be evaluated for SPAM and will be delivered to the recipient's mailbox.

Accept antispam bypass flag set on SMTP session

Is useful when you have authenticated SMTP sessions between Exchange Servers with Antispam bypass setting. For example, when you have an Edge server and a Hub server, there is no need to scan the traffic between the two servers. The **Accept antispam bypass flag set on SMTP session** is enabled by default but only applies when the antispam bypass flag is configured for the SMTP session on your Exchange Server. If you disable **Accept antispam bypass flag set on SMTP session**, ESET Mail Security will scan the SMTP session for spam regardless of antispam bypass setting on your Exchange Server.

NOTE
It is necessary that the Antispam database be updated regularly for the Antispam module to provide the best possible protection. To allow regular updates to the Antispam database, make sure that ESET Mail Security has access to the correct IP addresses on the necessary ports. For further information on what IPs and ports to enable on your third-party firewall, see our KB article.

You'll find further settings for each feature in its own section:

- Filtering and verification
- Advanced settings
- Greylisting settings
- SPF and DKIM
- Backscatter protection

Filtering and verification

You can configure **Approved**, **Blocked** and **Ignored** lists by specifying criteria such as IP address or range, domain name, etc. To add, modify or remove criteria, click **Edit** for to the list you want to manage.

> NOTE
> IP addresses or Domains included in the **Ignored lists** will not be further tested by Antispam filtering, but other Antispam protection techniques will be applied.
> Ignored lists should contain all internal infrastructure IP addresses / domain names. You can also include IP addresses / domain names of your ISP's or external sending mail servers that are currently blacklisted by one of the RBL or DNSBL (cloud blacklist – ESET's Blackhole List or third-party Blackhole List). This allows you to receive emails from sources included in the ignored lists, even though their IP addresses are on the cloud blacklist. Such incoming emails are received and their content is further inspected by other Antispam protection techniques.

Approved IP list	Automatically whitelists emails originating from specified IP addresses. Email content will not be checked.
Blocked IP list	Automatically blocks emails originating from specified IP addresses.
Ignored IP list	List of IP addresses which will be ignored during classification. Email content will be checked. Use **Is part of internal infrastructure** slider bar if you are whitelisting your network's local IP addresses, see example below.
Blocked Body Domain list	Blocks email messages that contain specified domain in the message body. Only domains with real TLD (top-level domain) are accepted.
Ignored Body Domain list	Specified domains in the message body will be ignored during classification. Only domains with real TLD (top-level domain) are accepted.
Blocked Body IP list	Blocks email messages that contain specified IP address in the message body.
Ignored Body IP list	Specified IP addresses in the message body will be ignored during classification.
Approved Senders list	Whitelists emails originating from a specified sender. Only one sender address or a whole domain is used for verification based on the following priority: 1.SMTP 'MAIL FROM' address 2."Return-Path:" email header field 3."X-Env-Sender:" email header field 4."From:" email header field 5."Sender:" email header field 6."X-Apparently-From:" email header field
Blocked Senders list	Blocks emails originating from a specified sender. All identified sender addresses or whole domains are used for verification: SMTP 'MAIL FROM' address "Return-Path:" email header field "X-Env-Sender:" email header field "From:" email header field "Sender:" email header field "X-Apparently-From:" email header field

Approved Domain to IP list	Whitelists emails originating from IP addresses that are resolved from specified domains in this list. SPF (Sender Policy Framework) records are being recognized when resolving IP addresses.
Blocked Domain to IP list	Blocks emails originating from IP addresses that are resolved from specified domains in this list. SPF records are being recognized when resolving IP addresses.
Ignored Domain to IP list	List of domains that resolves to IP addresses which in turn will not be checked during classification. SPF records are being recognized when resolving IP addresses.
Blocked countries list	Blocks emails from specified countries. Blocking is based on GeoIP. If a spam message is sent from mail server with IP address listed in geolocation database for a country you have selected in the Blocked countries, it will automatically be marked as spam and an action will be taken according to **Action to take on spam messages** setting under Mail transport protection.

NOTE
Body Domain lists accept domains with real TLD (top-level domain) only, according to the official Root Zone Database of TLDs.

If you want to add more entries at once, click **Enter multiple values** in the **Add** pop-up window and choose what separator should be used, it can be Newline, Comma or Semicolon.

EXAMPLE
Objective: Exclude your infrastructure's local IP addresses from Antispam protection by adding them into the Ignore IP list
Navigate to **Advanced setup (F5)** > **Server** > **Antispam protection** > **Filtering and verification**.
Click **Edit** next to **Ignored IP list**.
Click **Add** and specify IP address range of your network infrastructure (IP address range format *1.1.1.1-1.1.1.255*). You can keep adding more ranges (or single IP addresses) to the list, if required.
Use the slider bar **Is part of internal infrastructure**.

Greylisting and SPF

Specify Domain to IP whitelist or IP whitelist to automatically bypass Greylisting and SPF. You can see **Log files** in the SMTP protection log. In order to use these options, you need to enable either Greylisting or SPF, or both. In case of SPF, you need to enable **Automatically reject messages if SPF check fails** and/or **Automatically bypass Greylisting if SPF check passes** setting.

Use antispam lists to automatically bypass Greylisting and SPF

When enabled, Approved and Ignored IP list will be used together with IP and Domain to IP whitelists to automatically bypass Greylisting and SPF.

IP whitelist

You can add IP address, IP address with mask, IP range. You can modify the list by clicking **Add**, **Edit** or **Delete**. Alternatively, you can import your custom list from a file instead of adding every single entry manually, click **Import** and browse for your file that contains entries you want to add to the list. Likewise, if you need to export your existing list to a file, select **Export** from the context menu.

NOTE
Whitelists take precedence over blacklists, i.e., if an email contains both whitelisted and blacklisted address, it is whitelisted. Only the last sender address and up to the Maximum number of verified addresses from Received: headers are checked against whitelists. All addresses are checked against local blacklists.

Domain to IP whitelist

This option allows you to specify domains (e.g. *domainname.local*). To manage the list, use **Add**, **Remove** or **Remove all**. If you want to import your custom list from a file instead of adding every single entry manually, click **Import** and browse for your file that contains entries you want to add to the list. Likewise, if you need to export your existing list to a file, select **Export** from the context menu.

> NOTE
> Greylisting and SPF is evaluated by Mail transport protection and allows you to use IP and Domain to IP whitelists, as well as Approved and Ignored IP list. However, if you are using SPF rules, none of these whitelists are taken into account for rules.

Antispam advanced settings

These settings allow for messages to be verified by external servers (defined as **RBL** - Realtime Blackhole List and **DNSBL** - DNS Blocklist) according to their predetermined criteria.

Maximum number of verified addresses from Received: headers

You can limit the number of IP addresses that are checked by Antispam. This concerns the IP addresses written in `Received: from` headers. The default value is 0, which means that only the last identified sender's IP address is checked.

Verify sender's address against end-user blacklist

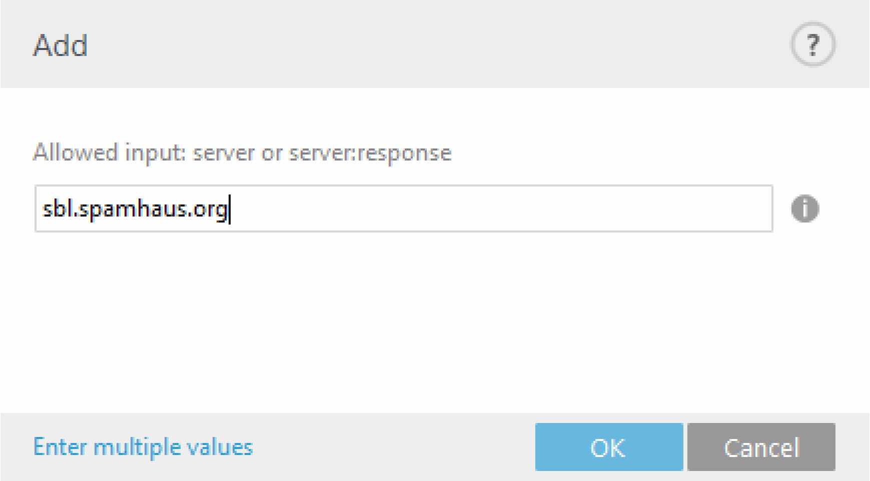
Email messages that are not sent from mail servers (computers that are not listed as mail servers) are verified to make sure the sender is not on the blacklist. This option is enabled by default. You can disable it if required, but messages not sent from mail servers will not be checked against the blacklist.

> NOTE
> Results of external third-party Blocklists have priority over end-user blacklist for IP addresses in `Received: from` headers. All IP addresses (up to the specified maximum number of verified addresses) are sent of evaluation by external third-party servers.

Additional RBL servers

Is a list of Realtime Blackhole List (RBL) servers which are queried when analyzing messages.

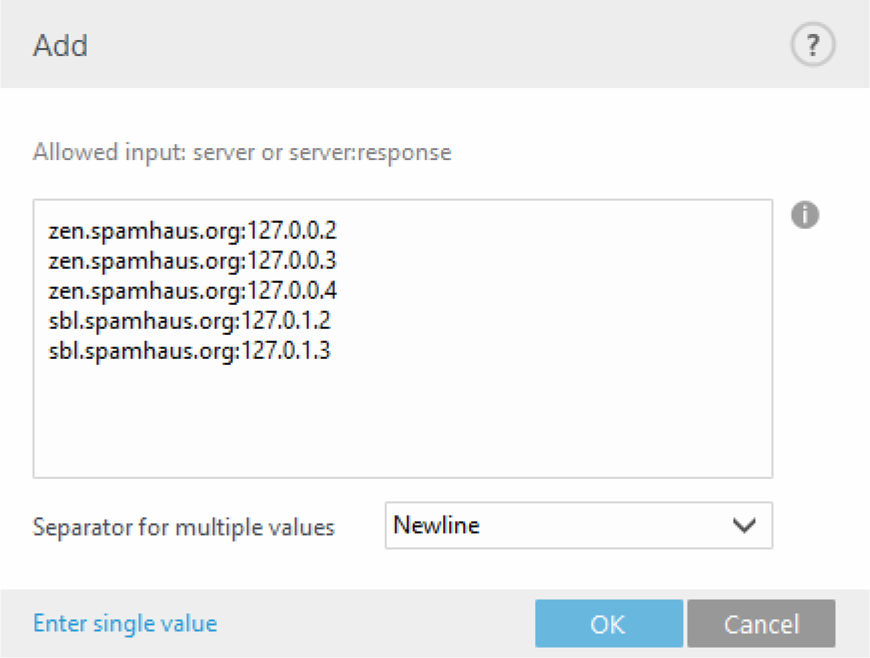
> NOTE
> When adding Additional RBL servers, enter the server's domain name (for example. `sbl.spamhaus.org`). It will work with any return codes that are supported by the server.



Allowed input: server or server:response

sbl.spamhaus.org

Alternatively, you can specify a server name with a return code in the format `server:response` (for example,. `zen.spamhaus.org:127.0.0.4`). When using this format, we recommend that you add each server name and return code separately, so that you'll have a complete list. Click **Enter multiple values** in the **Add** window to specify all server names with their return codes. Entries should look like the example below, your actual RBL server host names and return codes may vary:



Allowed input: server or server:response

```
zen.spamhaus.org:127.0.0.2
zen.spamhaus.org:127.0.0.3
zen.spamhaus.org:127.0.0.4
sbl.spamhaus.org:127.0.1.2
sbl.spamhaus.org:127.0.1.3
```

Separator for multiple values: Newline

RBL query execution limit (in seconds)

This option allows you to set a maximum time for RBL queries. RBL responses are only used from those RBL servers which respond in time. If the value is set to "0" no timeout is enforced.

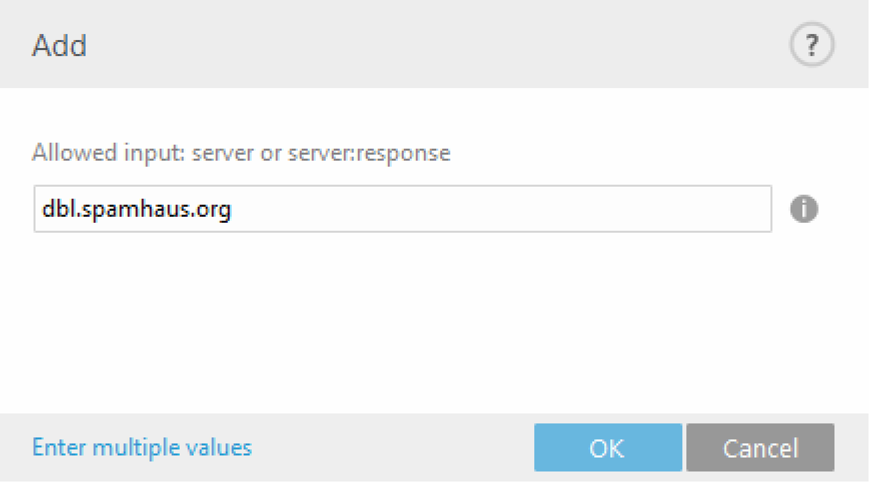
Maximum number of verified addresses against RBL

This option allows you to limit how many IP addresses are queried against the RBL server. Note that the total number of RBL queries will be the number of IP addresses in the Received: headers (up to a maximum of RBL maxcheck IP addresses) multiplied by the number of RBL servers specified in RBL list. If the value is set to "0" an unlimited number of received headers are checked. Note that IPs on the ignored IP list do not count towards the RBL IP addresses limit.

Additional DNSBL servers

Is a list of DNS Blocklist (DNSBL) servers which are queried with domains and IP addresses extracted from the message body.

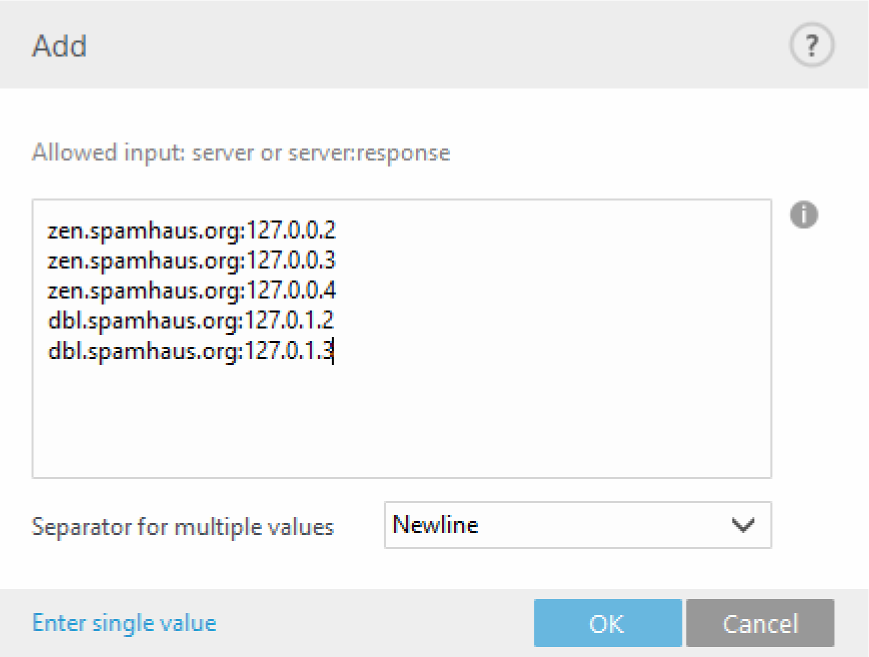
> NOTE
> When adding Additional DNSBL servers, enter the server's domain name (for example, `dbl.spamhaus.org`). It will work with any return codes that are supported by the server.



Allowed input: server or server:response

dbl.spamhaus.org

Alternatively, you can specify a server name with a return code in a form of `server:response` (for example, `zen.spamhaus.org:127.0.0.4`). In this case we recommend that you add each server name and return code separately, so that you have a complete list. Click **Enter multiple values** in the **Add** window to specify all server names with their return codes. Entries should look like the example below, your actual DNSBL server host names and return codes may vary:



Allowed input: server or server:response

```
zen.spamhaus.org:127.0.0.2
zen.spamhaus.org:127.0.0.3
zen.spamhaus.org:127.0.0.4
dbl.spamhaus.org:127.0.1.2
dbl.spamhaus.org:127.0.1.3
```

Separator for multiple values: Newline

DNSBL query execution limit (in seconds)

Allows you to set a maximum timeout for all DNSBL queries to complete.

Maximum number of verified addresses against DNSBL

Allows you to limit how many IP addresses are queried against the DNS Blocklist server.

Maximum number of verified domains against DNSBL

Allows you to limit how many domains are queried against the DNS Blocklist server.

Maximum message scan size (kB)

Limits Antispam scan for messages larger than the specified value. Default value 0 means unlimited message size scan. Normally, there is no reason to limit Antispam scan, but if you need to set a limit in certain situations, change the value to required size. When set, Antispam engine will process messages up to the specified size and ignore larger messages.

> NOTE
> The smallest possible limit is 12 kB. If you set the value from 1 to 12, Antispam engine will always read at least 12 kB.

Enable temporary rejecting of undetermined messages

If the Antispam engine is not able to determine whether the message is or isn't SPAM, which means the message has some suspicious SPAM characteristics but not enough to be marked as SPAM (for example the first email of a campaign, or an email originating from an IP range with mixed ratings), then this setting (when enabled) allows ESET Mail Security to temporarily reject the message - the same way Greylisting does - and keep rejecting it for a specific time period, until:

- The interval has elapsed and the message is accepted upon the next delivery attempt. This message is left with the initial classification (SPAM or HAM).
- Antispam cloud gathers enough data and is able to properly classify the message before the interval elapses.

The rejected message is not kept by ESET Mail Security as it must be re-sent by the sending mail server in accordance with the SMTP RFC.

Enable submitting of temporary rejected messages for analysis

The message content is automatically sent for further analysis. This helps improve message classification of future email messages.

> IMPORTANT
> It is possible that temporarily rejected messages which are sent for analysis could in fact be HAM. In rare cases, temporarily rejected messages may be used for manual evaluation. Enable this feature only if there are no risks of leaking any potentially sensitive data.

Greylisting settings

The **Enable Greylisting** function activates a feature that protects users from spam using the following technique: The transport agent will send a “temporarily reject” SMTP return value (default is 451/4.7.1) for any received email that is not from a recognized sender. A legitimate server will try to resend the message after a delay. Spam servers will typically not attempt to resend the message, as they usually go through thousands of email addresses and do not waste time resending. Greylisting is an additional layer of Antispam protection, and does not have any effect on the spam evaluation capabilities of the Antispam module.

When evaluating the message source, the Greylisting method takes into account the **Approved IP list**, the **Ignored IP list**, **Safe Senders** and the **Allow IP lists** on the Exchange server as well as Antispam bypass settings for the recipient mailbox. Emails from these IP addresses/senders lists or emails delivered to a mailbox that has the Antispam bypass option enabled will be bypassed by the Greylisting detection method.

Use only domain part of sender address

Ignores sender's name in the email address; only domain is taken into account.

Synchronize greylisting databases across the ESET cluster

Greylisting database entries are shared in real time between the servers in ESET cluster. When on one of the servers receives a message that is processed by greylisting, this information is broadcast by ESET Mail Security over to the rest of the nodes in ESET cluster.

Time limit for the initial connection denial (min.)

When a message is delivered for the first time and temporarily refused, this parameter defines the time period during which the message will always be refused (measured from the first refusal). After the defined time period has elapsed, the message will be successfully received. The minimum value you can enter is 1 minute.

Unverified connections expiration time (hours)

This parameter defines the minimum time interval for which the triplet data will be stored. A valid server must resend a desired message before this period expires. This value must be greater than the value of **Time limit for the initial connection denial**.

Verified connections expiration time (days)

The minimum number of days for which the triplet information is stored, during which emails from a particular sender will be received without any delay. This value must be greater than the value of **Unverified connections expiration time**.

SMTP response (for temporarily denied connections)

Specify a **Response code**, **Status code** and **Response message**, which define the SMTP temporary denial response sent to the SMTP server if a message is refused. Example of a SMTP reject response message:

Response code	Status code	Response message
451	4.7.1	Please try again later

WARNING
Incorrect syntax in SMTP response codes may lead to the malfunction of Greylisting protection. As a result, spam messages may be delivered to clients or messages may not be delivered at all.

NOTE
You can also use system variables when defining the SMTP reject response.

All messages that have been evaluated using the greylisting method are recorded in the SMTP protection log.

SPF and DKIM

Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are used as validation methods to check that an incoming email message claimed to come from a specific domain was authorized by the owner of that domain. This helps protect recipients from receiving spoofed email messages. ESET Mail Security also uses Domain-based Message Authentication (DMARC), Reporting and Conformance evaluation to further enhance upon SPF and DKIM.

SPF

Check is performed to verify if an email was sent by a legitimate sender. A DNS lookup for SPF records of the sender's domain is performed to get a list of IP addresses. If any of the IP addresses from SPF records matches the actual IP address of the sender, the result of the SPF check is a **Pass**. If the sender's actual IP address does not match, the result is a **Fail**. However, not all domains have SPF records specified in DNS. If there are no SPF records present in DNS, the result is **Not available**. A DNS request may timeout occasionally, in which case the result is also **Not available**.

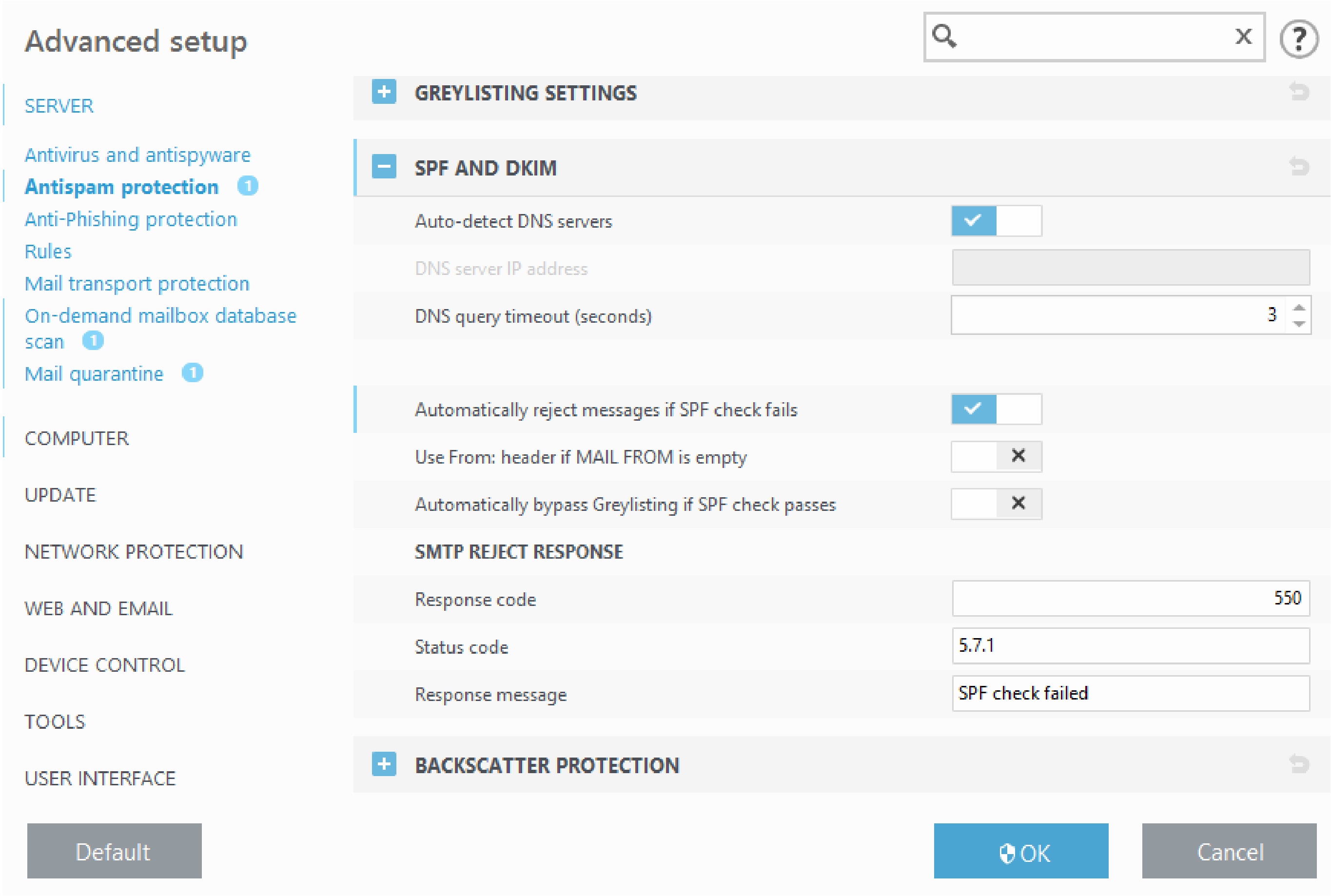
DKIM

Is used by organizations to prevent email message spoofing by adding a digital signature to the headers of outgoing messages according to the DKIM standard. This involves using a private domain key to encrypt your domain's outgoing mail headers, and adding a public version of the key to the domain's DNS records. ESET Mail Security can then retrieve the public key to decrypt incoming headers and verify that the message really comes from your domain and its headers hasn't been changed along the way.

> NOTE
> Exchange Server 2010 and older are not fully compatible with DKIM, because headers included in digitally signed incoming messages may get modified during DKIM validation.

DMARC

Is built on top of the two existing mechanisms, SPF and DKIM. You can use Mail Transport protection rules to evaluate **DMARC result** and **Apply DMARC policy** action.



SPF AND DKIM

Auto-detect DNS servers	✓
DNS server IP address	
DNS query timeout (seconds)	3
Automatically reject messages if SPF check fails	✓
Use From: header if MAIL FROM is empty	✗
Automatically bypass Greylisting if SPF check passes	✗

SMTP REJECT RESPONSE

Response code	550
Status code	5.7.1
Response message	SPF check failed

Auto detect DNS servers

Uses settings of your network adapter.

DNS server IP address

If you want to use specific DNS servers for SPF and DKIM, enter the IP address (in IPv4 or IPv6 format) of the DNS server you want to use.

DNS query timeout (seconds)

Specify timeout for DNS reply.

Automatically reject messages if SPF check fails

If your SPF check results in an immediate fail, an email message can be rejected before it is downloaded.

EXAMPLE

SPF check is done on the SMTP layer. However, it can be rejected either automatically on the SMTP layer or during rules evaluation.

It is not possible to log rejected messages into the Events log if you use automatic rejection on the SMTP layer. This is because logging is done by rule action and the automatic reject is done directly on the SMTP layer which happens before rule evaluation. Since the messages will get rejected before rules are evaluated, there is no information to be logged at the time of rule evaluation.

You can log rejected messages, but only if you reject the messages by a rule action. To reject messages that did not pass SPF check and log such rejected messages, disable **Automatically reject messages if SPF check fails** and create the following rule for **Mail transport protection**:

Condition

Type: **SPF result**

Operation: **is**

Parameter: **Fail**

Actions

Type: **Reject message**

Type: **Log to events**

Use From: header if MAIL FROM is empty

The header MAIL FROM can be empty, and can also be easily spoofed. When this option is enabled and MAIL FROM is empty, the message is downloaded and the header *From:* is used instead.

Automatically bypass Greylisting if SPF check passes

There is no reason to use Greylisting for a message if its SPF check result was Pass.

SMTP reject response

You can specify a **Response code**, **Status code** and **Response message** which define the SMTP temporary denial response sent to the SMTP server if a message is refused. You can enter a response message in the following format:

Response code	Status code	Response message
550	5.7.1	SPF check failed

Backscatter protection

Spam backscatter are misdirected bounce messages sent by mail servers. Backscatter is undesirable side effect of spam. When a spam message is rejected by recipient's mail server, a Non-Delivery Report (NDR), also known as bounce message, is sent to a supposed sender (an email address which was forged as a sender of the original spam message), not an actual sender of the spam. A user, who owns the email address, receives NDR message, even though the user wasn't involved with the original spam message at all. This is when **Backscatter protection** comes in. You can prevent spam NDR's being delivered to users' mailboxes within your organization using ESET Mail Security Backscatter protection.

When you **Enable NDR check**, you must specify **Signature seed** (a string of at least 8 characters, something like a passphrase). ESET Mail Security Backscatter protection writes `X-Eset-NDR: <hash>` into the header of each outgoing email message. The `<hash>` is an encrypted signature that also contains **Signature seed** you have specified.

If legitimate email message could not be delivered, your mail server usually receives NDR, which is checked by

ESET Mail Security looking for the `X-Eset-NDR: <hash>` in the headers. If the `X-Eset-NDR:` is present and the signature `<hash>` matches, the NDR is delivered to the sender of the legitimate email message indicating the message delivery failed. If the `Eset-NDR:` is not present or signature `<hash>` is incorrect, it proves to be a spam Backscatter and the NDR is rejected.

Automatically drop NDR messages if check fails

If your NDR check results in an immediate fail, an email message can be rejected before it is downloaded.

You can see **Backscatter protection** activity in the SMTP protection log.

Anti-Phishing protection

Phishing is an attempt to obtain sensitive information such as usernames, passwords, bank account or credit card details and PIN numbers via email or web pages disguised as a trustworthy entity. This activity is usually done for malicious reasons. It is a form of social engineering (manipulation of users in order to obtain confidential information).

ESET Mail Security includes Anti-Phishing protection which prevents users from accessing web pages known for phishing. In case of email messages that may contain links which lead to phishing web pages, ESET Mail Security uses sophisticated parser that searches message body and subject of incoming email messages to identify such links (URL's). The links are compared against phishing database. If the result of evaluation is positive, email is considered to be a phishing message and ESET Mail Security deals with it according to **Action to take on phishing message** setting for each protection layer (Mail transport protection, Mailbox database protection and On-demand mailbox database scan). Also rule actions are executed.

Supported email format standards:

- Plain text
- HTML-only
- MIME
- Multipart MIME (an email that includes both, an HTML and plain text part)

Supported HTML entities:

Phishing messages might contain HTML entities to obfuscate Anti-Phishing engine. The Anti-Phishing protection also parses and translates symbols of HTML entities to find and correctly evaluate obfuscated URL's.

A single character can be represented in different forms. For example, a period can be represented in the following forms:

How links usually appear in the email message to the user	Value	Obfuscated links contained in the message body	Type
http://www.example-phishing-domain.com/Fraud	**.**	http://www.example-phishing-domain.com/Fraud	character
http://www.example-phishing-domain.com/Fraud	**&period;**	http://www.example-phishing-domain**&period;**com/Fraud	entity **name**
http://www.example-phishing-domain.com/Fraud	**&#x0002E;**	http://www.example-phishing-domain**&#x0002E;**com/Fraud	entity **hexadecimal** number
http://www.example-phishing-domain.com/Fraud	**&#46;**	http://www.example-phishing-domain**&#46;**com/Fraud	entity **decimal** number

To see the activity of Anti-Phishing mail protection, check **Log files** > Mail server protection log. It will contains information about email messages and their phishing links that were found.

Report a phishing site

Click Report enables you to report a phishing or otherwise malicious web site to ESET for analysis.

Rules

Enables you to manually define email filtering conditions and actions to take with filtered emails. You can also define conditions and actions that differ for rules specific to Mail transport protection, Mailbox database protection and On-demand mailbox database scan. This is because each of these protection types use a little different approach when processing messages, especially Mail transport protection.

> NOTE
> The availability of rules for Mailbox database protection, On-demand mailbox database scan and Mail transport protection on your system depends on which Microsoft Exchange Server version is installed on the server with ESET Mail Security.

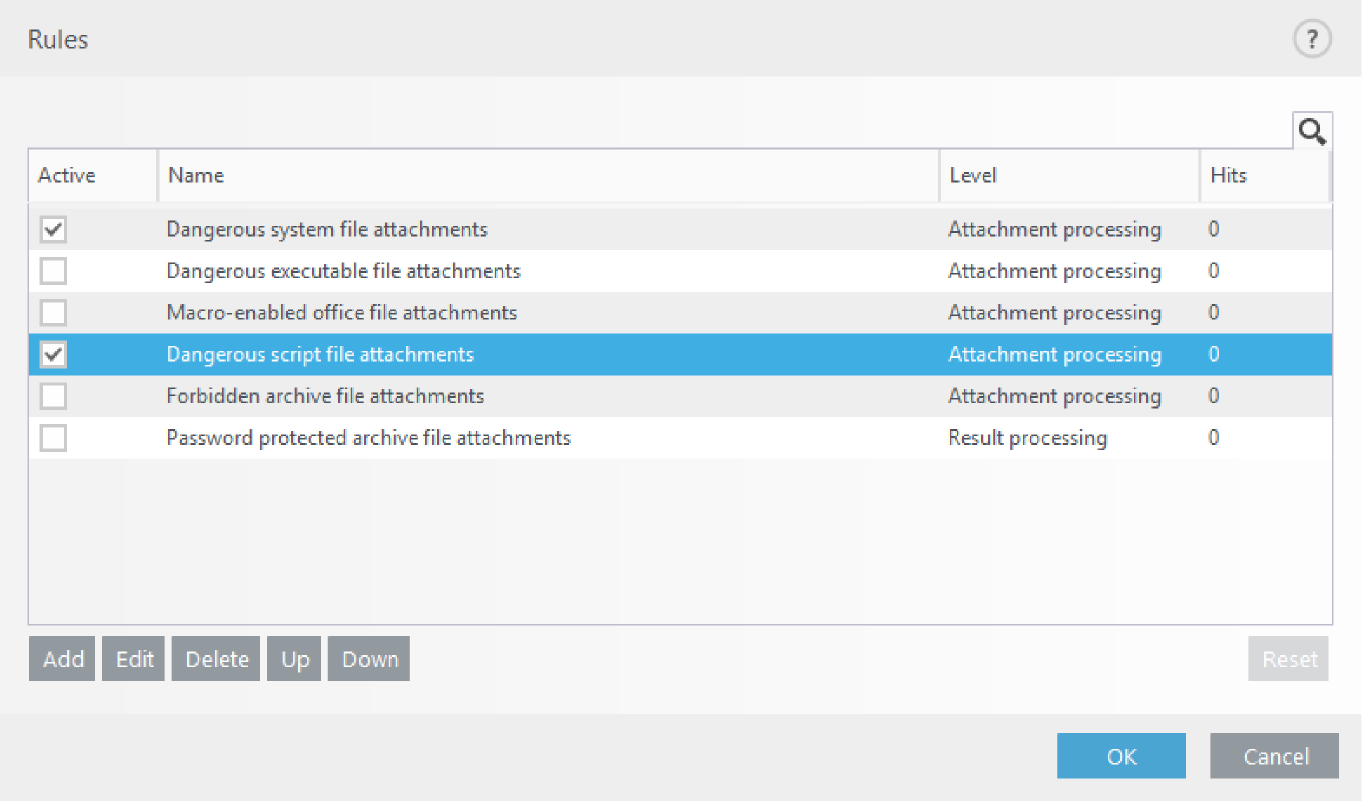
> IMPORTANT
> Incorrectly defined rules for **On-demand mailbox database scan** can cause irreversible changes to Mailbox databases. Always make sure you have the most recent backup of your Mailbox databases before running On-demand mailbox database scan with rules in place for the first time. Also, we highly recommend you to verify the rules are running according to expectations. For verification, define rules with **Log to events** action only, because any other actions can make changes to your Mailbox databases. Once verified, you can add destructive rule actions such as **Delete attachment**.

Rules are classified into three levels and are evaluated in this order:

- **Filtering rules (1)** - rules evaluated before Antispam, Antivirus and Anti-Phishing scanning
- **Attachment processing rules (2)** - rules evaluated during Antivirus scan
- **Result processing rules (3)** - rules evaluated after Antispam, Antivirus and Anti-Phishing scanning

Rules with the same level are evaluated in the same order as they are displayed in the rules window. You can only change the rule order for rules of the same level. When you have multiple filtering rules, you can change the order they are applied in. You cannot change their order by putting **Attachment processing** rules before **Filtering** rules, the **Up**/**Down** buttons will not be available. In other words, you cannot mix rules of different **Levels**.

The **Hits** column displays the number of times the rule was successfully applied. Deselecting a check box (to the left of each rule name) deactivates the corresponding rule until you select the check box again.



Active	Name	Level	Hits
☑	Dangerous system file attachments	Attachment processing	0
□	Dangerous executable file attachments	Attachment processing	0
□	Macro-enabled office file attachments	Attachment processing	0
☑	Dangerous script file attachments	Attachment processing	0
□	Forbidden archive file attachments	Attachment processing	0
□	Password protected archive file attachments	Result processing	0

Click **Reset** the counter for the selected rule (the **Hits** column). Select **View** allows you to view a configuration assigned from ESET Security Management Center policy.

IMPORTANT
Normally, if a rule's conditions are met, rules evaluation stops for further rules with lower priority. However, if required, you can use special Rule action called **Evaluate other rules** to let the evaluation to continue.

Rules are checked against a message when it is processed by the Mail transport protection, Mailbox database protection or On-demand mailbox database scan. Each protection layer has a separate set of rules.

When Mailbox database protection or On-demand mailbox database scan rule conditions are matched, the rule counter may increase by 2 or more. This is because these protection layers access the body and attachments of a message separately, so rules are applied to each part individually. Mailbox database protection rules are also applied during background scanning (for example, when ESET Mail Security performs a mailbox scan following the download of a new virus signature database), which can increase the rule counter (Hits).

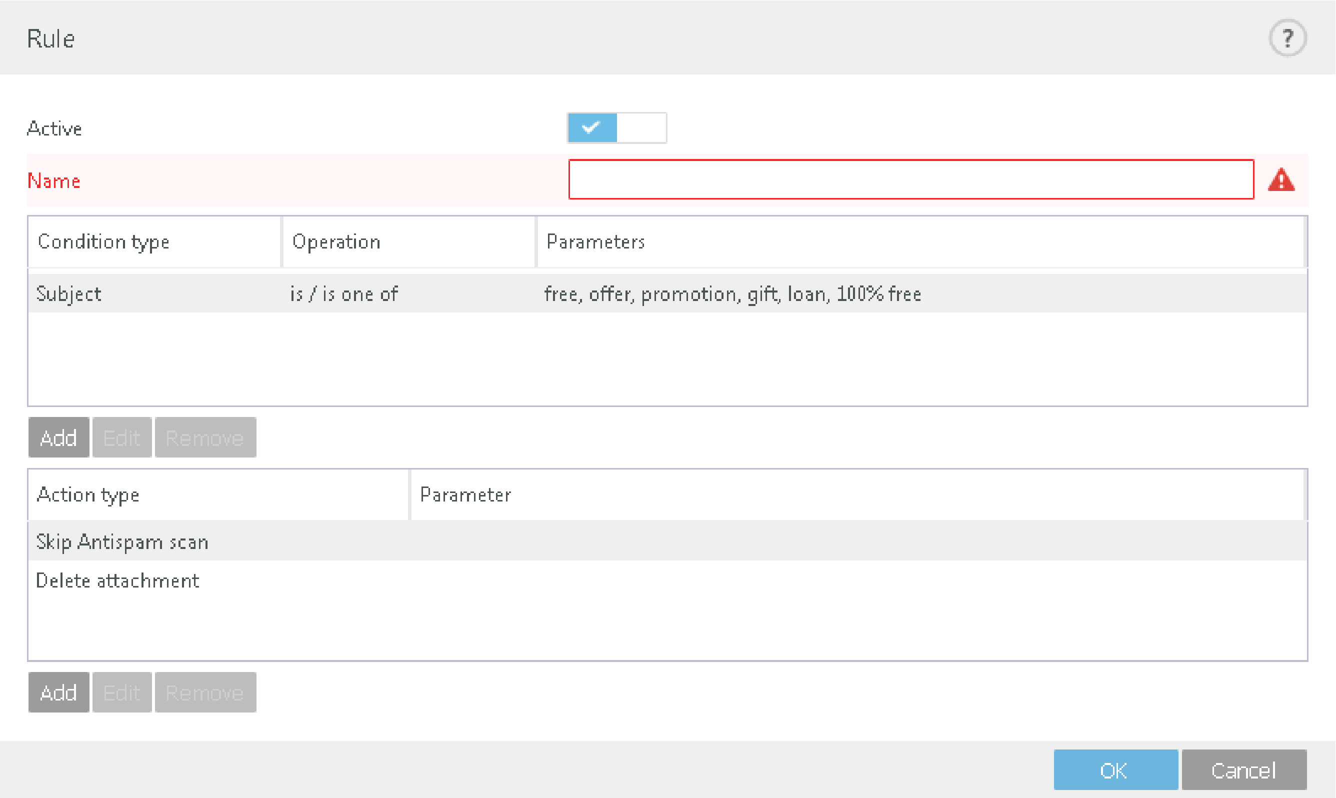
Rule wizard

1.Click **Add** (in the middle) and a Rule condition window will appear where you can select condition type, operation and value. Define condition(s) first, then action(s).

IMPORTANT
You can define multiple conditions. If you do so, all of the conditions must be met for the rule to be applied. All conditions are connected using the logical operator **AND**. Even if most of the conditions are met and only a single one isn't, the condition evaluation result is considered *not met* and the rule's action cannot be taken.

2.Click **Add** (at the bottom) to add a Rule action.

NOTE
It is possible to add multiple actions for one rule.



Active ✓

Name

Condition type	Operation	Parameters
Subject	is / is one of	free, offer, promotion, gift, loan, 100% free

Action type	Parameter
Skip Antispam scan	
Delete attachment	

3. Once conditions and actions are defined, type a **Name** for the rule (something that you'll recognize the rule by), this name will be displayed in the Rules list. **Name** is a mandatory field, if it is highlighted in red, type a rule name into the text box and click **OK** to create the rule. Red highlight does not disappear even though you've entered rule name, it disappears only after you've clicked **OK**.

4. If you want to prepare rules but plan to use them later, you can click the slider bar next to **Active** to deactivate the rule. To activate the rule, select the check box next to the rule you want to activate.

NOTE
If a new rule is added or an existing rule has been modified, message rescan will automatically start using the new/modified rules.

See Rule examples that show how rules can be used.

Rule condition

This wizard lets you add conditions for a rule. Select condition **Type** and an **Operation** from the drop-down list. The list of operations changes depending on what rule type you've chosen. Then select a **Parameter**. Parameter fields will change depending on rule type and operation. For example, choose **File size** > **is greater than** and under **Parameter** specify 10 MB. Using these settings, any file that is larger than 10 MB will be processed using rule actions you have specified. For this reason you should specify the action that is taken when a given rule is triggered if you have not done so when setting parameters for that rule.

If you want to import your custom list from a file instead of adding every single entry manually, right-click in the middle of the window and select **Import** from the context menu, then browse for your file (*.xml* or *.txt*) that contains entries (delimited by new lines) you want to add to the list. Likewise, if you need to export your existing list to a file, select **Export** from the context menu.

Alternatively, you can specify **Regular expression**, select **Operation**: **matches regular expression** or **does not match regular expression**.

NOTE
ESET Mail Security uses std::regex. Refer to ECMAScript syntax for constructing regular expressions. Regular expression syntax is not case sensitive, as well as search result.

IMPORTANT
You can define multiple conditions. If you do so, all of the conditions must be met for the rule to be applied. All conditions are connected using the logical operator **AND**. Even if most of the conditions are met and only a single one isn't, the condition evaluation result is considered *not met* and the rule's action cannot be taken.

The following condition types are available for Mail transport protection, Mailbox database protection and On-demand mailbox database scan (some of the options might not display depending on your previously selected conditions):

Condition name	Mail transport protection	Mailbox database protection	On-demand mailbox database scan	**Description**
Subject	⍰	⍰	⍰	Applies to messages which contain or do not contain a specific string (or a regular expression) in the subject.
Sender	⍰	⍰	⍰	Applies to messages sent by a specific sender.
SMTP sender	⍰	⍰	⍰	MAIL FROM envelope attribute used during SMTP connection. Also used for SPF verification.
Sender's IP address	⍰	⍰	⍰	Applies to messages sent from a specific IP address.
Sender's domain	⍰	⍰	⍰	Applies to messages from a sender with a specific domain in their email addresses.
SMTP sender's domain	⍰	⍰	⍰	Applies to messages from a sender with a specific domain in their email addresses.
From header - address	⍰	⍰	⍰	"From:" value contained in message headers. This is the address that is visible to the recipient, but no checks are done that the sending system is authorized to send on behalf of that address. It is often used for spoofing the sender.
From header - display name	⍰	⍰	⍰	"From:" value contained in message headers. This is the display name that is visible to the recipient, but no checks are done that the sending system is authorized to send on behalf of that address. It is often used for spoofing the sender.
Recipient	⍰	⍰	⍰	Applies to messages sent to a specific recipient.
Recipient's organizational units	⍰	⍰	⍰	Applies to messages sent to a recipient of a specific organizational unit.

Condition name	Mail transport protection	Mailbox database protection	On-demand mailbox database scan	Description
Recipient validation result	⍰	⍰	⍰	Applies to messages sent to a recipient validated in Active Directory.
Attachment name	⍰	⍰	⍰	Applies to messages containing attachments with a specific name.
Attachment size	⍰	⍰	⍰	Applies to messages with an attachment that does not meet a specified size, is within a specified size range, or exceeds a specified size.
Attachment type	⍰	⍰	⍰	Applies to messages with a specific file type attached. File types are categorized in groups for easy selection, you can select multiple file types or whole categories.
Message size	⍰	⍰	⍰	Applies to messages with attachments that do not meet a specified size, are within a specified size range or exceed a specified size.
Mailbox	⍰	⍰	⍰	Applies to messages located in a specific mailbox.
Message headers	⍰	⍰	⍰	Applies to messages with specific data present in the message header.
Message body	⍰	⍰	⍰	Message body is searched for specified phrase. You can use Strip HTML tags feature to get rid off HTML tags, attributes and values, and preserve text only. The body text will then be searched.
Internal message	⍰	⍰	⍰	Applies depending on whether a message is internal or not internal.
Outgoing message	⍰	⍰	⍰	Applies to outgoing messages.
Signed message	⍰	⍰	⍰	Applies to signed messages.
Encrypted message	⍰	⍰	⍰	Applies to encrypted messages.
Antispam scan result	⍰	⍰	⍰	Applies to messages flagged or not flagged as Ham or Spam. (see example)
Antivirus scan result	⍰	⍰	⍰	Applies to messages flagged as malicious or not malicious.
Anti-Phishing scan result	⍰	⍰	⍰	Applies to messages which were evaluated as phishing.
Received time	⍰	⍰	⍰	Applies to messages received before or after a specific date, or during a specific date range.
Contains password protected archive	⍰	⍰	⍰	Applies to messages with archive attachments that are protected by a password.
Contains damaged archive	⍰	⍰	⍰	Applies to messages with archive attachments that are damaged (most likely impossible to open).
Attachment is password protected archive	⍰	⍰	⍰	Applies to attachments that are protected by a password.
Attachment is damaged archive	⍰	⍰	⍰	Applies to attachments that are damaged (most likely impossible to open).

Condition name	Mail transport protection	Mailbox database protection	On-demand mailbox database scan	Description
Folder Name	⍰	⍰	⍰	Applies to messages located in a specific folder, if the folder doesn't exist, it will be created. This does not apply to Public folders.
DKIM result	⍰	⍰	⍰	Applies to messages that passed or failed verification by DKIM, alternatively if not available.
SPF result	⍰	⍰	⍰	Applies to messages for which SPF evaluation result is: **Pass** - the IP address is authorized to send from the domain (SPF qualifier "+") **Fail** - SPF record does not contain the sending server or IP address (SPF qualifier "-") **Soft fail** - the IP address may or may not be authorized to send from the domain (SPF qualifier "~") **Neutral** - means the domain owner stated in the SPF record that they do not want to assert that the IP address is authorized to send from the domain (SPF qualifier "?") **Not available** - SPF result of None means that no records were published by the domain or that no checkable sender domain could be determined from the given identity You can read RFC 4408 for more details about SPF. If you use SPF result, whitelists within Filtering and verification are not taken into account for rules.
DMARC result	⍰	⍰	⍰	Applies to messages that passed or failed verification by SPF, DKIM or both, alternatively if not available.
Has reverse DNS record	⍰	⍰	⍰	Applies to messages with sender's domain that has reverse DNS record.
NDR result	⍰	⍰	⍰	Applies to messages that failed verification by NDR.

Condition type has associated the following **Operations**:

- **String:** is, is not, contains, doesn't contain, matches, doesn't match, is in, is not in, matches regular expression, does not match regular expression
- **Number:** is less than, is greater than, is between
- **Text:** contains, doesn't contain, matches, doesn't match
- **Date-time:** is less than, is greater than, is between
- **Enum:** is, is not, is in, is not in

NOTE

If **Attachment name** or **Attachment type** is Microsoft Office (2007+) file it is treated by ESET Mail Security as an archive. This means that its content is extracted and each file contained in the Office file archive (for example `.docx`, `.xlsx`, .xltx, `.pptx`, `.ppsx`, `.potx`, etc.) is scanned separately.

If you disable **Antivirus protection** in Setup menu or **Advanced setting** (**F5**) > **Server** > **Antivirus and Antispyware** for Mail transport and Mailbox database protection layer, it will affect these rule conditions:

- Attachment name
- Attachment size
- Attachment type
- Antivirus scan result
- Attachment is password protected
- Attachment is damaged archive
- Contains damaged archive
- Contains password protected archive

Rule action

You can add actions that will be taken with messages and/or attachments that match rule conditions.

> NOTE
> It is possible to add multiple actions for one rule.

The list of available actions for Mail transport protection, Mailbox database protection and On-demand mailbox database scan (some of the options might not show up depending on your selected conditions):

Action name	Mail transport protection	Mailbox database protection	On-demand mailbox database scan	Description
Quarantine message	⍰	⍰	⍰	The message will not be delivered to the recipient and will be moved to the mail quarantine. Non-administrator users to release emails quarantine by this rule (using web interface or quarantine reports).
Quarantine attachment	⍰	⍰	⍰	Puts the email attachment into file quarantine. The email will be delivered to the recipient with the attachment truncated to zero length.
Delete attachment	⍰	⍰	⍰	Deletes a message attachment. The message will be delivered to the recipient without the attachment.
Reject message	⍰	⍰	⍰	Deletes a message. For incoming emails received via SMTP a NDR (Non-Delivery Report) should be generated by the sending server.
Drop message silently	⍰	⍰	⍰	Deletes a message without generating a NDR.
Set SCL value	⍰	⍰	⍰	Changes or sets a specific SCL value.

Action name	Mail transport protection	Mailbox database protection	On-demand mailbox database scan	Description
Send event notification to administrator	⍰	⍰	⍰	Sends event notifications to a recipient specified in Email notifications. You need to enable Send event notification by email feature. You can then customize the format of event messages (use the tooltip for suggestions) while creating the rule. Also, you can select verbosity for event messages, however this depends on the minimum verbosity setting in Email notifications section.
Skip Antispam scan	⍰	⍰	⍰	Message will not be scanned by the Antispam engine.
Skip Antivirus scan	⍰	⍰	⍰	Message will not be scanned by the Antivirus engine.
Skip Anti-Phishing scan	⍰	⍰	⍰	Message will not be parsed by the Anti-Phishing protection.
Evaluate other rules	⍰	⍰	⍰	Allows the evaluation of other rules, enabling the user to define multiple sets of conditions and multiple actions to take given the conditions.
Log to events	⍰	⍰	⍰	Writes information about the applied rule to the program log and define the format of event messages (use the tooltip for suggestions). If you configure the action type **Log to events** for **Mailbox database protection** with the parameter **%IPAddress%**, the Event column in the Log files will be empty for this particular event. This is because there is no IP address on the Mailbox database protection level. Some options are not available on all protection levels: **%IPAddress%** - ignored by **On-demand mailbox database scan** and **Mailbox database protection** **%Mailbox%** - ignored by **Mail transport protection** The following options apply to **Attachment processing rules** only: **%Attname%** - ignored by **Filtering rules** and **Result processing rules** **%Attsize%** - ignored by **Filtering rules** and **Result processing rules**
Add header field	⍰	⍰	⍰	Adds a custom string to a message header.
Add subject prefix	⍰	⍰	⍰	Adds a prefix to a subject.
Replace attachment with action information	⍰	⍰	⍰	Replaces attachment with a text file that contains detailed information about an action taken.
Remove header fields	⍰	⍰	⍰	Removes fields from message header according to specified parameters.
Delete message	⍰	⍰	⍰	Deletes an infected message.

Action name	Mail transport protection	Mailbox database protection	On-demand mailbox database scan	Description
Move message to folder	⍰	⍰	⍰	The message will be moved to the specific folder.
Move message to trash	⍰	⍰	⍰	Puts an email message into the trash folder on the email client's side.
Apply DMARC policy	⍰	⍰	⍰	If a DMARC result condition is met, the email message is handled according to the policy specified in the DMARC DNS record for the sender's domain.

If you disable **Antivirus protection** in Setup menu or **Advanced setting** (**F5**) > **Server** > **Antivirus and Antispyware** for **Mail transport protection**, it will affect these rule actions:

- Quarantine attachment
- Delete attachment

Rule examples

⊟ Quarantine messages that contain malware or attachment that is password protected, encrypted or damaged

EXAMPLE
Objective: Quarantine messages that contain malware or attachment that is password protected, encrypted or damaged
Create the following rule for **Mail transport protection**:
Condition
Type: **Antivirus scan result**
Operation: **is not**
Parameter: **Clean**
Action
Type: **Quarantine message**

⊟ Move messages that failed SPF check to a Junk folder

EXAMPLE
Objective: Move messages that failed SPF check to a Junk folder
Create the following rule for **Mail transport protection**:
Condition
Type: **SPF result**
Operation: **is**
Parameter: **Fail**
Action
Type: **Set SCL value**
Value: **5** (Set the value according to `SCLJunkThreshold` parameter of `Get-OrganizationConfig` cmdlet of your Exchange server. For more details, see SCL threshold actions article)

⊟ Drop messages from specific senders

EXAMPLE
Objective: Drop messages from specific senders
Create the following rule for **Mail transport protection**:
Condition
Type: **Sender**
Operation: **is / is one of**
Parameter: **spammer1@domain.com, spammer2@domain.com**
Action
Type: **Drop message silently**

⊟ Customize predefined rule

EXAMPLE
Objective: Customize predefined rule
Details: Allow archive attachments in messages from specified IP addresses (in case of internal systems, for example) while using Forbidden archive file attachments rule
Open **Mail transport protection** rule set, select **Forbidden archive file attachments** and click **Edit**.
Condition
Type: **Sender's IP address**
Operation: **is not / is not any**
Parameter: **1.1.1.2, 1.1.1.50-1.1.1.99**

⊟ Message body

EXAMPLE
Objective: Quarantine messages that contain certain string in Message body
Create the following rule for **Mail transport protection**:
Condition
Type: **Message body**
Operation: **contains/contains one of**, click **Add** type web site URL or part of URL
Action
Type: **Quarantine message**

⊟ Store messages for non-existent recipients

EXAMPLE
Objective: Store messages for non-existent recipients
Details: If you want to have all messages to non-existent recipients quarantined (regardless of being marked by Antivirus or Antispam protection)
Condition
Type: **Recipient validation result**
Operation: **is**
Parameter: **Contains invalid recipient**
Action
Type: **Quarantine message**

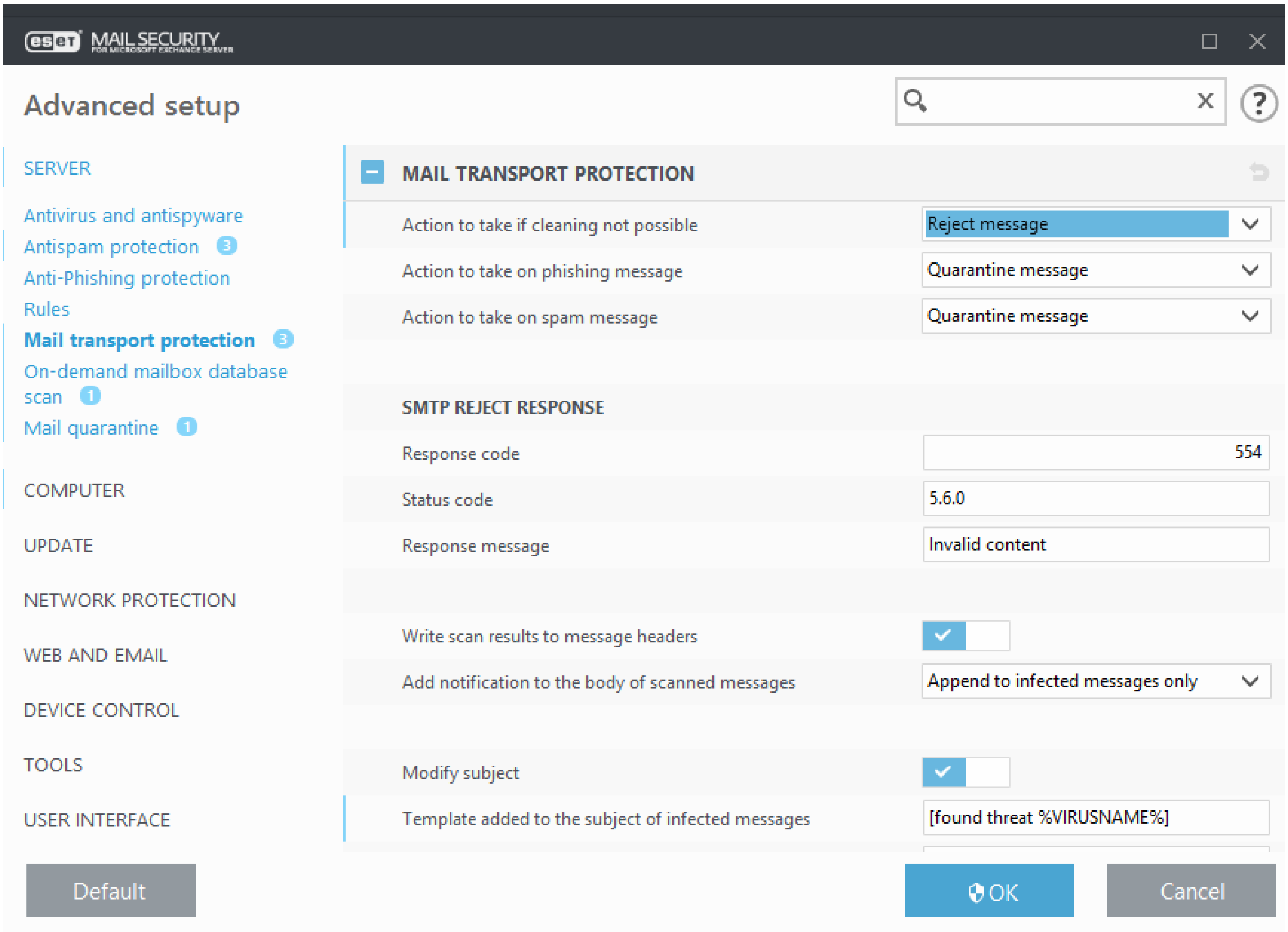
Mail transport protection

You can configure actions for detected threats on the transport layer for each ESET Mail Security module (Antivirus, Anti-Phishing and Antispam) separately.

Actions to take if cleaning not possible:

- **No action** - Retain infected messages that cannot be cleaned
- **Quarantine message** - Puts infected messages to the quarantine mailbox
- **Reject message** - Reject an infected message
- **Drop message silently** - Delete messages without sending NDR (Non-Delivery Report)

NOTE
If you select **No action** and at the same time have **Cleaning level** set to **No cleaning** in ThreatSense parameters of Antivirus and antispyware, then the protection status will change to yellow. This is because it is a security risk and we do not recommend that you use this combination. Change one or the other setting in order to achieve a good level of protection.



MAIL TRANSPORT PROTECTION

Action to take if cleaning not possible: Reject message
Action to take on phishing message: Quarantine message
Action to take on spam message: Quarantine message

SMTP REJECT RESPONSE

Response code: 554
Status code: 5.6.0
Response message: Invalid content

Write scan results to message headers: ✓
Add notification to the body of scanned messages: Append to infected messages only

Modify subject: ✓
Template added to the subject of infected messages: [found threat %VIRUSNAME%]

Action to take on phishing message:

- **No action** - Keep the message even if it is marked as phish
- **Quarantine message** - Puts messages marked as phish to the quarantine mailbox
- **Reject message** - Reject messages marked as phish
- **Drop message silently** - Delete messages without sending NDR (Non-Delivery Report)

Action to take on spam messages:

- **No action** - Keep the message even if it is marked as spam
- **Quarantine message** - Puts messages marked as spam to the quarantine mailbox
- **Reject message** - Reject messages marked as spam

- **Drop message silently** - Delete messages without sending NDR (Non-Delivery Report)

SMTP Reject Response

You can specify a **Response code**, **Status code** and **Response message** which define the SMTP temporary denial response sent to the SMTP server if a message is refused. You can enter a response message in the following format:

Response code	Status code	Response message
250	2.5.0	Requested mail action okay, completed
451	4.5.1	Requested action aborted:local error in processing
550	5.5.0	Requested action not taken:mailbox unavailable
554	5.6.0	Invalid content

NOTE
You can also use system variables when configuring SMTP Reject Responses.

Write scan results to message headers

When enabled, scan results are written into message headers. These message headers start with `X_ESET` making them easy to recognize (for example `X_EsetResult` or `X_ESET_Antispam`).

Add notification to the body of scanned messages offers three options:

- **Do not append to messages** - Information will not be added.
- **Append to infected messages only** - Affect only infected messages.
- **Append to all messages** (doesn't apply to internal messages) - All messages will be marked.

Modify subject

When enabled, you can modify templates added to the subject of infected messages, spam or phish messages.

Template added to the subject of infected messages

ESET Mail Security will append a notification tag to the email subject with the value defined in the **Template added to the subject of infected messages** text field (predefined default text is `[found threat %VIRUSNAME%]`). This modification can be used to automate filtering of infected messages by filtering emails with a specific subject, for example using rules or alternatively on the client side (if supported by the email client) to put such email messages into a separate folder.

Template added to the subject of spam messages

ESET Mail Security will append a notification tag to the email subject with the value defined in the **Template added to the subject of spam messages** text field (predefined default text it `[SPAM]`). This modification can be used to automate spam filtering by filtering emails with a specific subject, for example using rules or alternatively on a client side (if supported by the email client) to put such email messages into a separate folder.

Template added to the subject of phish messages

ESET Mail Security will append a notification tag to the email subject with the value defined in the **Template**

added to the subject of phish messages text field (predefined default text it `[PHISH]`). This modification can be used to automate spam filtering by filtering emails with a specific subject, for example using rules or alternatively on a client side (if supported by the email client) to put such email messages into a separate folder.

> NOTE
> You can also use system variables when editing text which will be added to the subject.

Mail transport advanced settings

You can further customize mail transport protection settings.

Scan also messages received from authenticated or internal connections by

You can choose what type of scan should be performed on messages received from authenticated sources or local servers. Scanning of such messages is recommended as it increases protection, but necessary if you are using the built-in Microsoft SBS POP3 Connector to fetch email messages from external POP3 servers or mail services (for example Gmail.com, Outlook.com, Yahoo.com, gmx.dem, etc.). For more information see POP3 Connector and Antispam. Choose level of protection from the drop-down menu. We recommend you to use **Antivirus protection** (default setting), especially for internal connections as it is unlikely that phishing or spam messages will be distributed via your local servers. However, you can increase the protection for Microsoft SBS POP3 Connector by choosing **Antivirus and anti-phishing protection** or even **Antivirus, anti-phishing and antispam protection**.

> NOTE
> This setting turns Antispam protection on/off for authenticated users and internal connections. Emails from non-authenticated connections are always scanned, even if you select **Do not scan**.

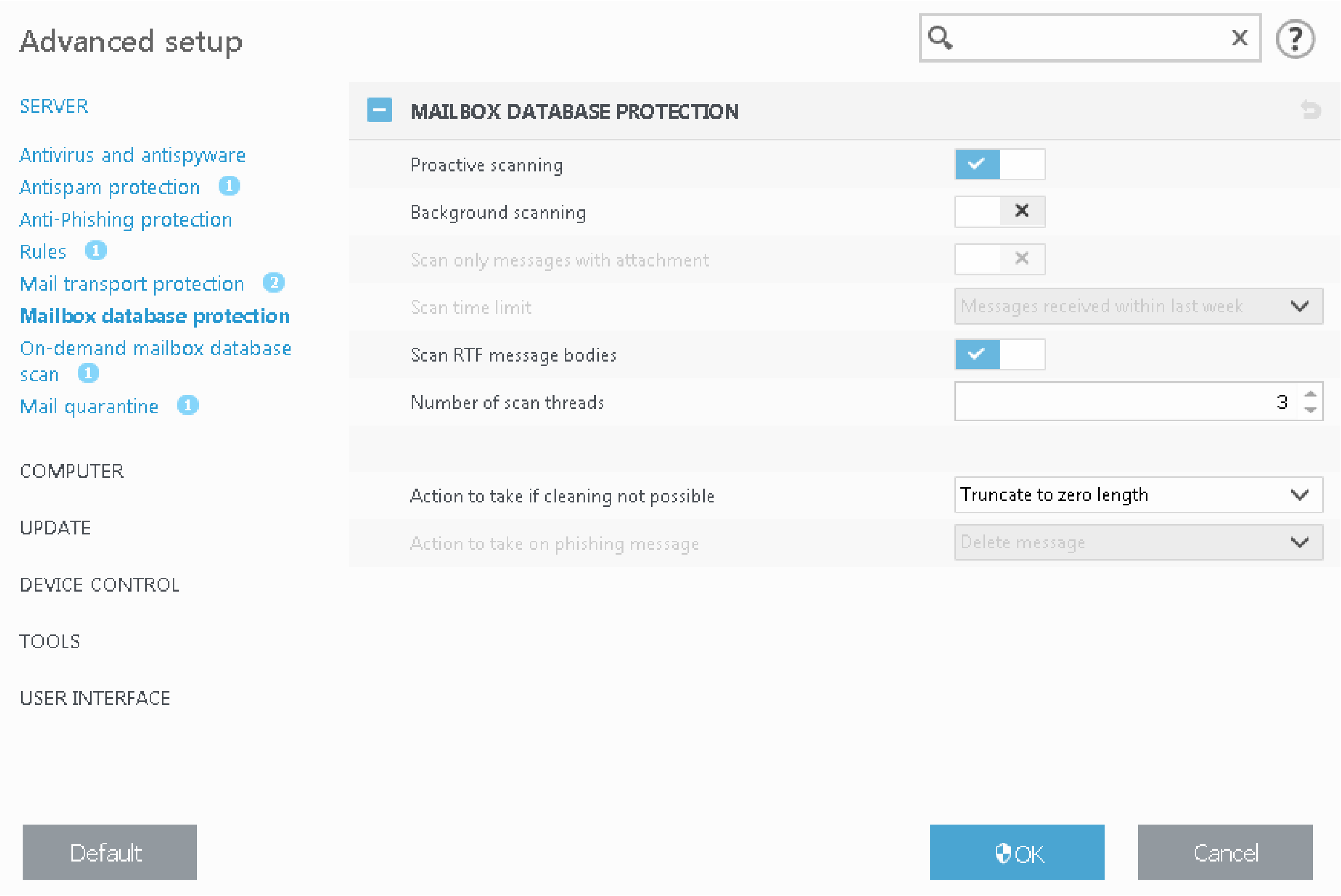
> NOTE
> Internal messages from Outlook inside the organization are sent in the TNEF format (Transport Neutral Encapsulation Format). TNEF is not supported by Antispam. Therefore, internal TNEF formatted emails will not be scanned for SPAM regardless of **Scan also messages received from authenticated or internal connections by** setting.

Remove existing SCL header before the scan

This option is enabled by default. You can disable it your requirement is to keep Spam Confidence Level (SCL) header.

Mailbox database protection

If **Proactive scanning** is enabled, new inbound messages will be scanned in the same order they are received. If this option is enabled and a user opens a message that has not been scanned yet, this message will be scanned before other messages in the queue.



Proactive scanning ✓
Background scanning ☒
Scan only messages with attachment ☒
Scan time limit: Messages received within last week
Scan RTF message bodies ✓
Number of scan threads: 3
Action to take if cleaning not possible: Truncate to zero length
Action to take on phishing message: Delete message

Background scanning

Allows scanning of all messages to run in the background (scanning runs on the mailbox and public folders store, for example the Exchange database). Microsoft Exchange Server decides whether a background scan will run or not based on various factors such as the current system load, number of active users, etc. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used. If you are opening a message that has not been scanned by the most current virus signature database, Microsoft Exchange Server sends the message to ESET Mail Security to be scanned before opening the message in your email client.
You can choose to **Scan only messages with attachments** and filter based on time received using the following **Scan time limit** options:

- All messages
- Messages received within last year
- Messages received within last 6 months
- Messages received within last 3 months
- Messages received within last months
- Messages received within last week

Since background scanning can affect system load (scanning is performed after each detection engine update), we recommend that you schedule scans to run during non-work hours. Scheduled background scanning can be configured via a special task in the Scheduler/Planner. When you schedule a Background scanning task you can set the launch time, the number of repetitions and other parameters available in the Scheduler/Planner. After the task has been scheduled, it will appear in the list of scheduled tasks and you can modify its parameters, delete it or temporarily deactivate the task.

Number of scan threads

Number of scan threads can be in range from 1 to 21. You can set the number of independent scan threads which used at same time. More threads on multiprocessor machines can increase the scan rate. For the best program performance we advise using an equal number for ThreatSense scan engines and scan threads.

Scan RTF message bodies

Option activates scanning of RTF message bodies. RTF message bodies may contain macro viruses.

NOTE
Plain text email bodies are not scanned by VSAPI.

Actions to take if cleaning not possible:

- **No action** - No changes in message will apply
- **Truncate to zero length** - Attachment will be shortened to zero length
- **Replace content with action information** - Original body will be replaced with action information. Content of attachment will be replaced with action information.
- **Delete message** - Message will be deleted

Action to take on phishing message:

- **No action** - No changes in message will apply
- **Delete message** - Message will be deleted

NOTE
Public folders are treated the same way as mailboxes. This means that public folders are scanned as well.

Background scan

This task type allows for database scan via VSAPI in the background. It lets your Exchange Server to run background scan if needed. The scan is triggered by the Exchange Server itself, this means that it is up to the Exchange Server whether the scan will be executed within allowed time.

We recommend you allow this task to run outside of peak hours when your Exchange Server is not busy, for example, at night-time. This is because the database background scan might puts certain amount of load on your system. Also, the time frame should not collide with any backups that might be running on your Exchange Server in order to prevent performance or availability issues.

NOTE
Mailbox database protection must be enabled in order for the scheduled task to run. This type of protection is only available for Microsoft Exchange Server 2010 and 2007 operating in the Mailbox Server (Microsoft Exchange 2010 and 2007).

Timeout (hours)

Specify how many hours is your Exchange Server allowed to run the database background scan from the time this scheduled task is executed. Once it reaches the timeout, Exchange will be instructed to stop its background scan.

On-demand mailbox database scan

NOTE
If you are running Microsoft Exchange Server 2007 or 2010, you can choose between Mailbox database protection and **On-demand mailbox database scan**, only one protection type can be active at a time. If you decide to use **On-demand mailbox database scan** you will need to disable integration of **Mailbox database protection** in **Advanced setup** (**F5**) under Server. Otherwise **On-demand mailbox database scan** will not be available.

Host address

Name or IP address of server running EWS (Exchange Web Services).

Username

Specify credentials of a user that has appropriate access to EWS (Exchange Web Services).

User password

Click **Set** next to **User password** and type password for this user account.

IMPORTANT
In order to scan Public folders, the user account used for On-demand mailbox database scan needs to have a mailbox. Otherwise, *Failed to load public folders* will be displayed in the Database scan log, along with a more specific message returned by Exchange.

Mailbox access method

Allow you to select preferred mailbox access method:

- **Impersonation**

Easier and faster setup is **ApplicationImpersonation role** which has to be assigned to the scanning account.

Assign ApplicationImpersonation role to user

If this option is grayed out, you need to specify a **Username**. Click **Assign** to automatically assign the ApplicationImpersonation role to selected user. Alternatively, you can assign the ApplicationImpersonation role manually to a user account. A new unlimited EWS Throttling Policy is created for the user account. For more information see Database scan account details.

- **Delegation**

Use this access type if you want to requires access rights set on individual mailboxes, but can provide higher speeds when scanning large amounts of data.

Assign delegated access to user

If this option is grayed out, you need to specify a Username. Click Assign to automatically grant selected user full access to all user and shared mailboxes. A new unlimited EWS Throttling Policy is created for the user account. For more information see Database scan account details.

Use SSL

Needs to be enabled if EWS (Exchange Web Services) is set to **Require SSL** in IIS. If SSL is enabled, the Exchange Server certificate must be imported on the system with ESET Mail Security (in case Exchange Server roles are on different servers). Settings for EWS can be found in IIS under *Sites/Default web site/EWS/SSL Settings*.

> NOTE
> Disable **Use SSL** only if you have EWS configured in IIS not to Require SSL.

Ignore server certificate error

If you are using a Self-signed certificate, you can ignore server certificate error.

Client certificate

Needs to be set only if Exchange Web Services (EWS) requires a client certificate. Click **Select** to select a certificate.

Action to take if cleaning not possible

This actions field allows you to block infected content.

- **No action** - Take no action on the infected content of the message.
- **Move message to trash** - Is not supported for Public folder items, the Delete object action will be applied instead.
- **Delete object** - Deletes infected content of the message.
- **Delete message** - Delete the entire message including its infected content.
- **Replace object with action information** - Removes an object and includes an information that the object was removed.

Action to take on phishing message:

- **No action** - Keep the message even if it is marked as phishing.
- **Move message to trash** - Is not supported for Public folder items, the Delete object action will be applied instead.
- **Delete message** - Delete the entire message including its infected content.

Number of scan threads

You can specify how many threads should ESET Mail Security use when scanning the databases. The higher the number, the better the performance. However, this has an effect on how much resources are used. The default value is set to 4 scan threads.

> NOTE
> If you configure On-demand mailbox database scan to use too many threads, it may put too much of a load on your system, which in turn might slow down other processes or even the whole system. You may encounter an error message saying "*Too many concurrent connections opened*".

Office 365 account

Visible only if you have Office 365 hybrid environment.

Username

Specify credentials of a user that has appropriate access to EWS (Exchange Web Services).

User password

Click **Set** next to **User password** and type password for this user account.

Assign ApplicationImpersonation role to user

If this option is grayed out, you need to specify a **Username**. Click **Assign** to automatically assign the ApplicationImpersonation role to selected user. Alternatively, you can assign the ApplicationImpersonation role manually to a user account. A new unlimited EWS Throttling Policy is created for the user account. For more information see Database scan account details.

Mailbox database scan

Running a full email database scan in large environments can result in undesired system loads. To avoid this issue, run a scan on specific databases or mailboxes. Further minimize server system impact by filtering scan targets using message timestamps.

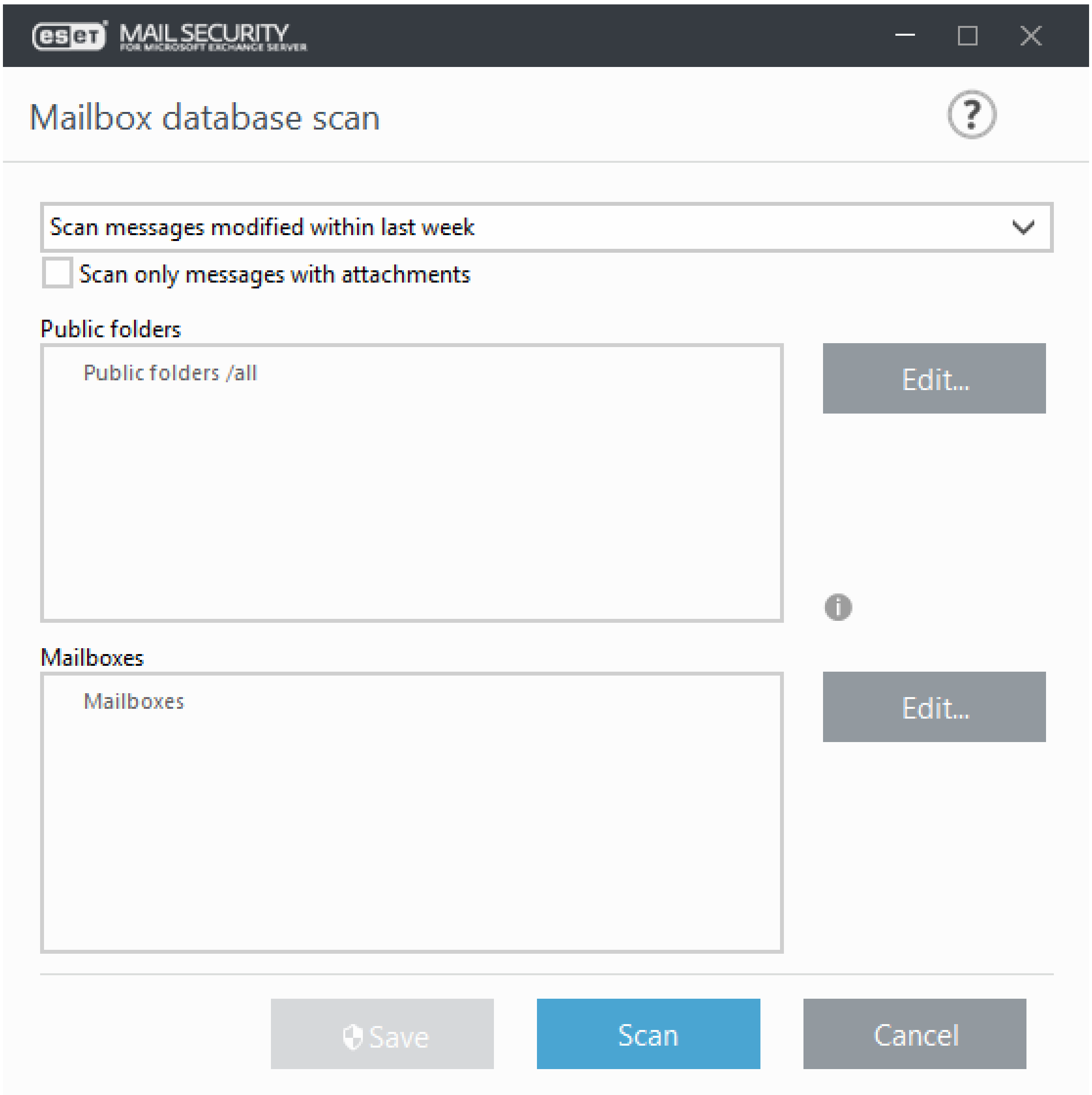
IMPORTANT
Incorrectly defined rules for On-demand mailbox database scan can cause irreversible changes to Mailbox databases. Always make sure you have the most recent backup of your Mailbox databases before running On-demand mailbox database scan with rules in place for the first time. Also, we highly recommend you to verify the rules are running according to expectations. For verification, define rules with **Log to events** action only, because any other actions can make changes to your Mailbox databases. Once verified, you can add destructive rule actions such as **Delete attachment**.

The following item types are scanned in both **Public folders** and in user **Mailboxes**:

- Email
- Post
- Calendar items (meetings/appointments)
- Tasks
- Contacts
- Journal

Use the drop-down list to choose which messages to scan according to their time-stamp. For example, **Scan messages modified within the last week**, you can also choose to **Scan all messages** if required.

To enable or disable message attachment scanning, select the check box next to **Scan only messages with attachments**. Click **Edit** to select the public folder that will be scanned.



Mailbox database scan

Scan messages modified within last week

□ Scan only messages with attachments

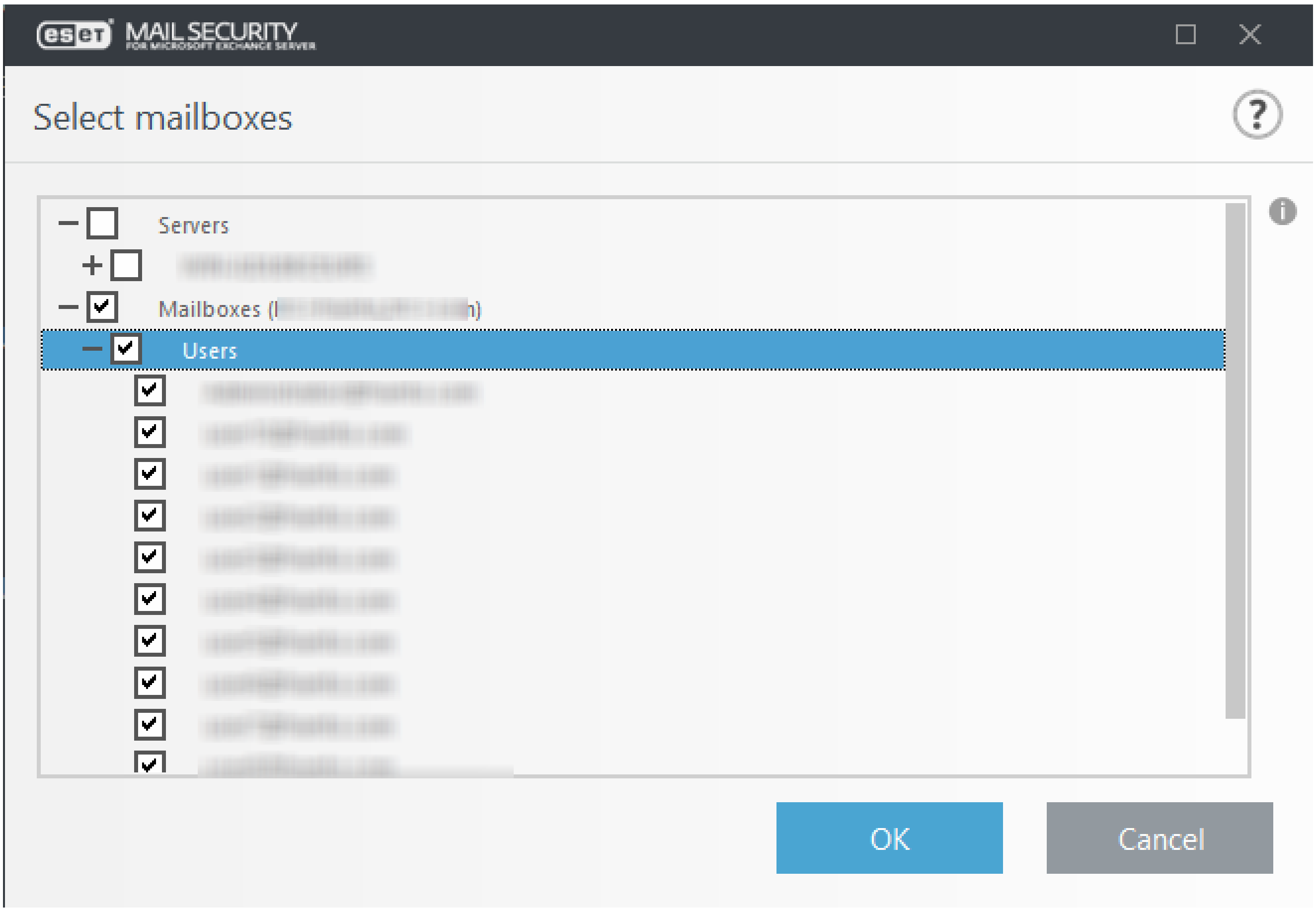
Public folders

Public folders /all

Mailboxes

Mailboxes

Select the check box(es) next to Server databases and Mailboxes you want to scan. Filter lets you find databases and mailboxes quickly, especially if there are a large number of mailboxes in your Exchange infrastructure.



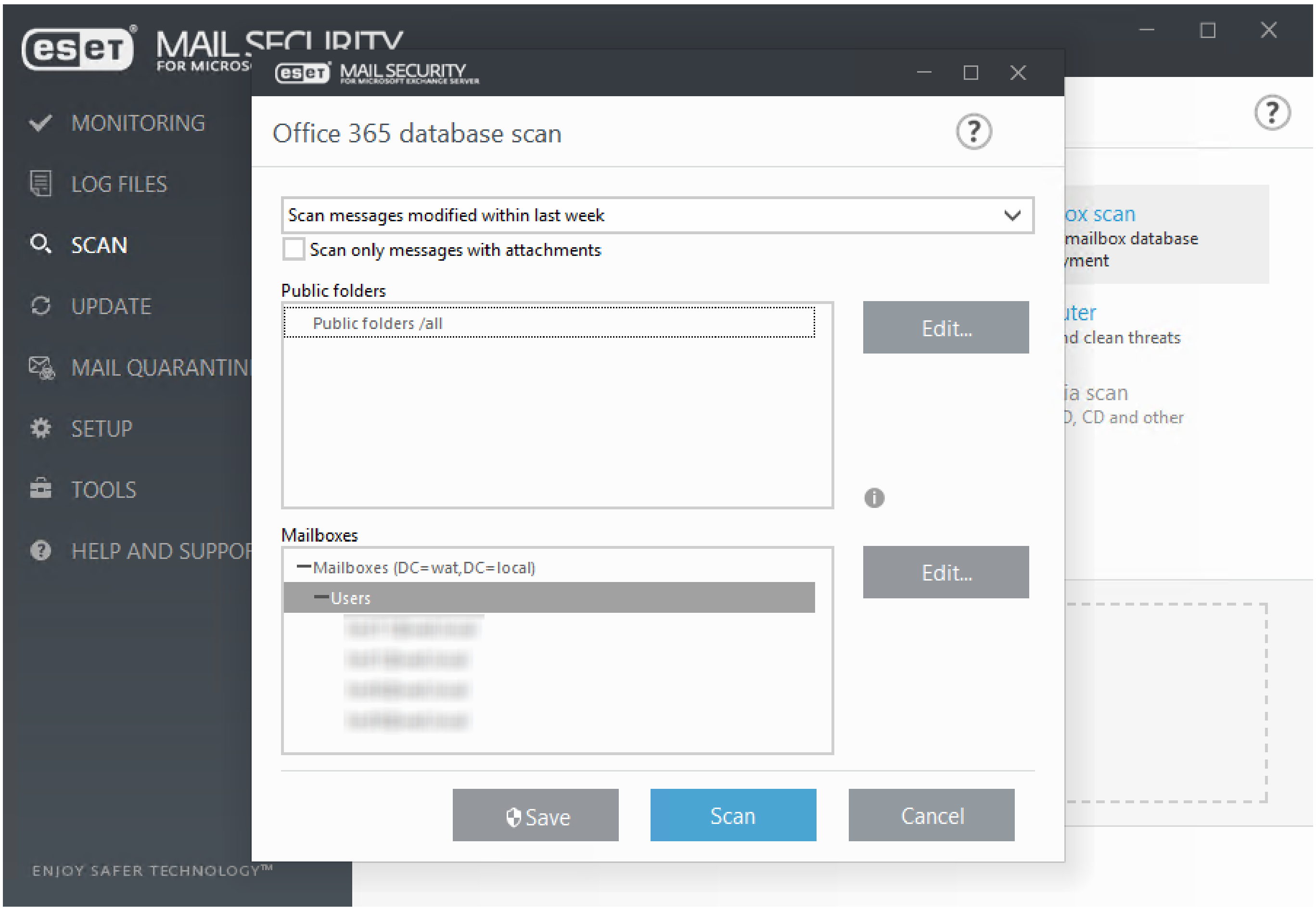
Click **Save** scan targets and parameters to the On-demand scan profile. You can now click **Scan**. In case you have not previously specified Database scan account details a pop-up window will open asking for credentials. Otherwise, On-demand mailbox database scan will start.

NOTE
If you are running Microsoft Exchange Server 2007 or 2010 you can choose between Mailbox database protection and On-demand mailbox database scan, only one protection type can be active at a time. If you decide to use **On-demand mailbox database scan** you will need to disable integration of **Mailbox database protection** in **Advanced setup** under **Server**. Otherwise On-demand mailbox database scan will not be available.

Office 365 mailbox scan

ESET Mail Security provides scanning functionality for Office 365 hybrid environments. It is available and visible in ESET Mail Security only if you have hybrid Exchange environment (on-premise and cloud). Both routing scenarios are supported, through **Exchange Online** or through **on-premises** organization. For more details see Transport routing in Exchange hybrid deployments.

You can scan Office 365 remote mailboxes and Public folders the same way you would with traditional On-demand mailbox database scan.



Office 365 database scan

Scan messages modified within last week

☐ Scan only messages with attachments

Public folders

Public folders /all

Mailboxes

Mailboxes (DC=wat,DC=local)

Users

Running a full email database scan in a large environments can result in undesired system loads. To avoid this issue, run a scan on specific databases or mailboxes. To further minimize system impact, use the time filter at the top of the window. For example, instead of using **Scan all messages**, you can select **Scan messages modified within last week**.

We recommend you to configure Office 365 account. Press **F5** key and navigate to **Server** > **On-demand mailbox database scan**. Also, see Database scan account details.

To see the activity of Office 365 mailbox scan, check **Log files** > **Mailbox database scan**.

Additional mailbox items

On-demand mailbox database scanner settings lets you enable or disable scanning of other mailbox item types:

- Scan calendar
- Scan tasks
- Scan contacts
- Scan journal

NOTE
If you experience performance issues, you can disable scanning of these items. Scans will take longer when these items are enabled.

Proxy server

In case you use a proxy server between your Exchange Server with CAS role and Exchange Server where ESET Mail Security is installed, specify parameters of your proxy server. This is required because ESET Mail Security connects to Exchange Web Services (EWS) API via HTTP/HTTPS. Otherwise, Quarantine mailbox and MS Exchange quarantine will not work.

Proxy server

Enter IP address or name of the proxy server you use.

Port

Enter port number of the proxy server.

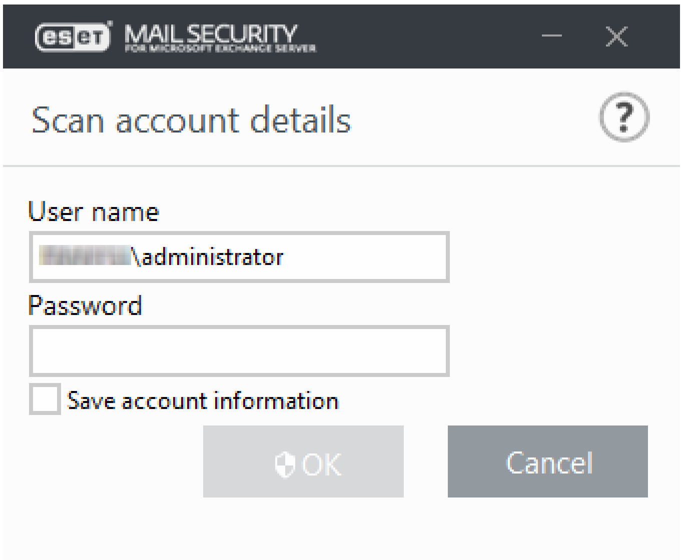
Username, Password

Enter credentials if your proxy server requires authentication.

Database scan account details

This dialog window displays if you have not specified a user name and a password for **Database scan**. Specify the credentials of the user who has access to EWS (Exchange Web Services) in this pop-up window and click **OK**. Alternatively, go to **Advanced setup** by pressing **F5** and navigate to **Server** > On-demand mailbox database scan. Type the **Username**, click **Set**, enter the password for this user account and click **OK**.

Click the check box next to **Save account information** to save account settings. Otherwise, you will be prompted to enter the account information every time you run an On-demand mailbox database scan.



Scan account details

User name: [redacted]\administrator

Password:

□ Save account information

If a user account does not have appropriate access to Exchange Web Services (EWS), you can select **Create "ApplicationImpersonation" role assignment** to assign this role to the user account. Alternatively, you can assign the ApplicationImpersonation role manually, see the note below for details.

IMPORTANT
Scan account must have the **ApplicationImpersonation role** assigned to allow the scan engine to scan user mailboxes within Exchange mailbox database(s). If you are running Exchange Server 2010 or newer, a new unlimited EWS Throttling Policy is created for the user account. Make sure to configure the EWS Throttling Policy for the scan account to avoid too many operation requests by ESET Mail Security, which might otherwise cause some of the requests to timeout. See EWS Best Practices and Understanding Client Throttling Policies articles to learn about the Throttling Policies. Also, see Change user throttling settings for specific users article for further details and examples.

If you want to assign **ApplicationImpersonation role** to a user account manually and create new EWS Throttling Policy for this account, you can use the following commands (replace `ESET-user` with an actual account name in your system, you can also set limits for the EWS Throttling Policy by replacing `$null` with numbers):

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-
EPI-Impersonation
Get-MailboxDatabase | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-
May-Impersonate
```

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

This might take a few moments to apply

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -
EWSFastSearchTimeoutInSeconds $null -EWSMaxConcurrency $null -EWSPercentTimeInAD
$null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null
Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-
ThrottlingPolicy
```

Exchange Server 2013, 2016 and 2019

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

This might take a few moments to apply

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -
EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited
Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-
ThrottlingPolicy
```

Mail Quarantine types

The Mail Quarantine manager is available for all three Quarantine types:

- Local quarantine
- Quarantine mailbox
- MS Exchange quarantine

You can see the contents of the Mail Quarantine in Mail Quarantine manager for all Quarantine types. Additionally, the local quarantine can also be viewed in the Mail Quarantine Web interface.

Store messages for non-existent recipients

This setting applies to messages that are marked to be quarantined by Antivirus protection, Antispam protection or based on Rules. When enabled, messages which were sent to recipients that do not exist in your Active Directory are stored in Mail quarantine. Disable this feature if you do not want to keep such messages in your Mail quarantine. When disabled, messages to unknown recipients will be dropped silently.

See example - If you want to have all messages to non-existent recipients quarantined.

Skip evaluation of rules when releasing emails

If you want to release a message from the quarantine, this message will not be evaluated by rules. This is to prevent the message from being put back into the quarantine, and the released message will be successfully delivered to the recipient. This feature is used only when the Administrator releases the message. If you disable this feature, or if a message is released by a user other than the Administrator, the message will be evaluated by rules.

> NOTE
> The two settings above are only available for Microsoft Exchange Server 2007 and newer.

Mail signature seed for multi-server environment

Allows you to skip evaluation of rules when releasing emails in multi-server environment. Enter the same seed value (a string of characters, something like a passphrase) on all server between which you want to establish trust.

Format for attachment envelope

When email message is being released from the quarantine, it is put as an attachment to a new message (attachment envelope) which is then delivered to the recipient. The recipient receives the original message that is being release from the mail quarantine as an attachment. You can use predefined format of the envelope or modify it to your requirements using available variables.

Use ESET Cluster to store all quarantined messages on one node

If you are using ESET Cluster, this option will become available. We recommend you to use this function, because it enables you to keep the Local quarantine file store in one place, the master node.

Master node

Choose one of the nodes to become the master for Local quarantine file store. You will manage your mail quarantine on the master node (you can use Mail Quarantine manager from the main GUI or Mail Quarantine Web interface).

Local quarantine

The Local quarantine uses your local file system to store quarantined emails and a SQLite database as an index. Stored quarantined email files, as well as database files, are encrypted for security reasons. These files are located under *C:\ProgramData\ESET\ESET Mail Security\MailQuarantine* (on Windows Server 2012).

> NOTE
> If you want to have quarantined files stored on a different disk, other than the default *C:* drive, change the **Data folder** to your preferred path during installation of ESET Mail Security.

Local quarantine features:

- SPAM and quarantined email messages will be stored in a local file system, not an Exchange mailbox database.

- Encryption and compression of locally stored quarantined email files.
- Mail Quarantine Web interface as an alternative to Mail quarantine manager.
- Quarantine reports can be sent to a specified email address using a scheduled task.
- Quarantined email files removed from the quarantine window (after 21 days by default), are stored in a file system (until automatic deletion occurs after a specified number of days).
- Automatic deletion of old email files (after 3 days by default). For more information see File storage settings.
- You can restore removed quarantined email files using eShell (assuming that they've not been deleted from the file system yet).
- Inspect quarantined email messages and decide to delete or release any of them. To view and manage locally quarantined email messages, you can use Mail Quarantine manager from the main GUI or Mail Quarantine Web interface.

NOTE
The disadvantage of using Local quarantine is, if you run ESET Mail Security multiple servers with Hub Transport Server role, you need to manage each server's Local quarantine separately. The more mail servers you have, the more quarantines you will need to manage.

File storage

In this section you can change settings for File storage used by the local quarantine.

Compress quarantined files

Compressed quarantined files take up less disk space, but if you decide not to have files compressed then use the slider bar to turn off compression.

Clear old files after (days)

When messages reach specified number of days, these are removed from the quarantine window. However, files will not be deleted from the disk for the amount of days specified in **Clear deleted files after (days)**. Since files are not deleted from the file system, it is possible to recover such files using eShell.

Clear deleted files after (days)

Deletes files from the disk after specified number of days, no recovery is possible after these were deleted (unless you have file system backup solution in place).

Web interface

The Mail Quarantine Web interface is an alternative to Mail Quarantine manager, however, it is only available for the Local quarantine.

NOTE
Mail Quarantine Web interface is not available on a server with Edge Transport Server role because the Active Directory is not accessible for authentication.

The Mail Quarantine Web interface allows you to view the state of the mail quarantine. It also lets you to manage quarantined email objects. This web interface is accessible via links from quarantine reports or directly by entering a URL into a your web browser. To access the Mail Quarantine Web interface, you must authenticate using domain credentials. Internet Explorer will automatically authenticate a domain user. However, the web page certificate must be valid, Automatic logon must be enabled in Microsoft Internet Explorer, and you must add the Mail Quarantine website to Local intranet sites.

Any user that exists in the Active Directory can access the Mail Quarantine Web interface, but will only see quarantined items that were sent to his email address (this includes the user's aliases as well). The Administrator is able to see all quarantined items for all recipients.

> IMPORTANT
> ESET Mail Security is not using IIS to run Mail Quarantine Web interface. Instead, it is using HTTP server API which includes SSL support to allow data exchange over secure HTTP connections.

Web url

This is the URL on which the Web interface of Mail Quarantine will be available. By default, it is FQDN of the server with `/quarantine` (e.g. `mailserver.company.com/quarantine`). You can specify your own virtual directory instead of the default `/quarantine`. You can change the **Web url** anytime by editing the value.

The **Web url** value needs to be specified without a scheme (HTTP, HTTPS) and without a port number, use only `fqdn/virtualdirectory` form. Also, you can use wildcards instead of FQDN.

Once you modify the **Web url**, it is not possible to revert it back to default by clicking the revert icon. Remove the entry and leave the text box blank. Restart your server. When ESET Mail Security starts and finds the Web url is empty, it will automatically fill this field with the default `fqdn/quarantine` value.

> NOTE
> ESET Mail Security supports Web urls in four different forms:
> Strong wildcard (`+/quarantine`)
> Explicit (`mydomain.com/quarantine`)
> IP-bound weak wildcard (`192.168.0.0/quarantine`)
> Weak wildcard (`*/quarantine`)
> See the **Host-Specifier Categories** section of UrlPrefix Strings article for more information.

Web and report languages

Enables you to set language of quarantine Web interface and Quarantine reports.

HTTPS port

Used for the Web interface. Default port number is 443.

HTTP port

Used for releasing emails from quarantine via email reports.

> IMPORTANT
> If you do not have SSL certificate installed on IIS, configure HTTPS port binding. If you change the port number for HTTPS or HTTP, make sure to add corresponding port binding in IIS.

Log release action to events

When releasing items from mail quarantine, this action is written to Log files.

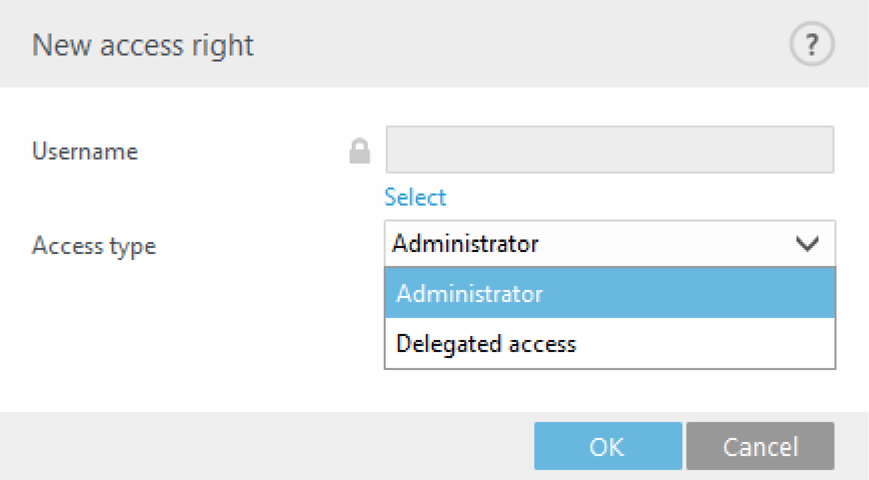
Enable default administrators

By default, members of Administrators group are granted admin access to the Mail Quarantine Web interface. Admin access has no restrictions and let the Admin to see all quarantined items for all recipients. If you disable this option, only Administrator user accounts have access to the Mail Quarantine Web interface.

Additional access rights

Grant users additional access to the Mail Quarantine Web interface and choose **Access type**. Click **Edit** to open the Additional access rights window, click **Add** to grant access to a user. In the New access right pop-up window, click **Select** and choose a user from the Active Directory (you can choose only one user), and select the **Access type** from the drop-down list:

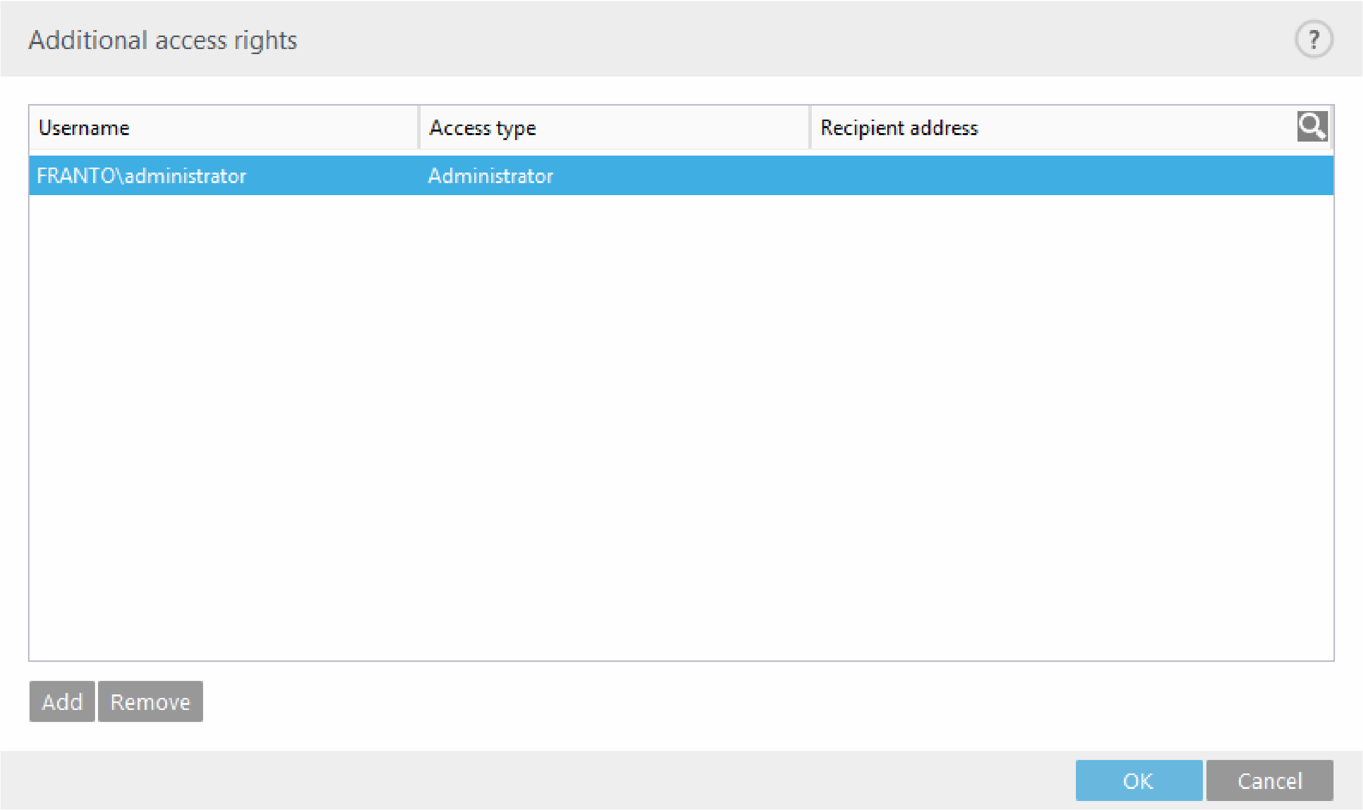
- **Administrator** - User has admin access to the Mail Quarantine Web interface.
- **Delegated access** - Use this access type if you want to let a user (delegate) to see and manage quarantined messages of another recipient. Specify the **Recipient address** by typing an email address for a user, whose quarantined messages will be managed by the delegate. If a user has aliases in the Active Directory, you can add additional access rights to each alias, if desired.


New access right

Username

Access type: Administrator

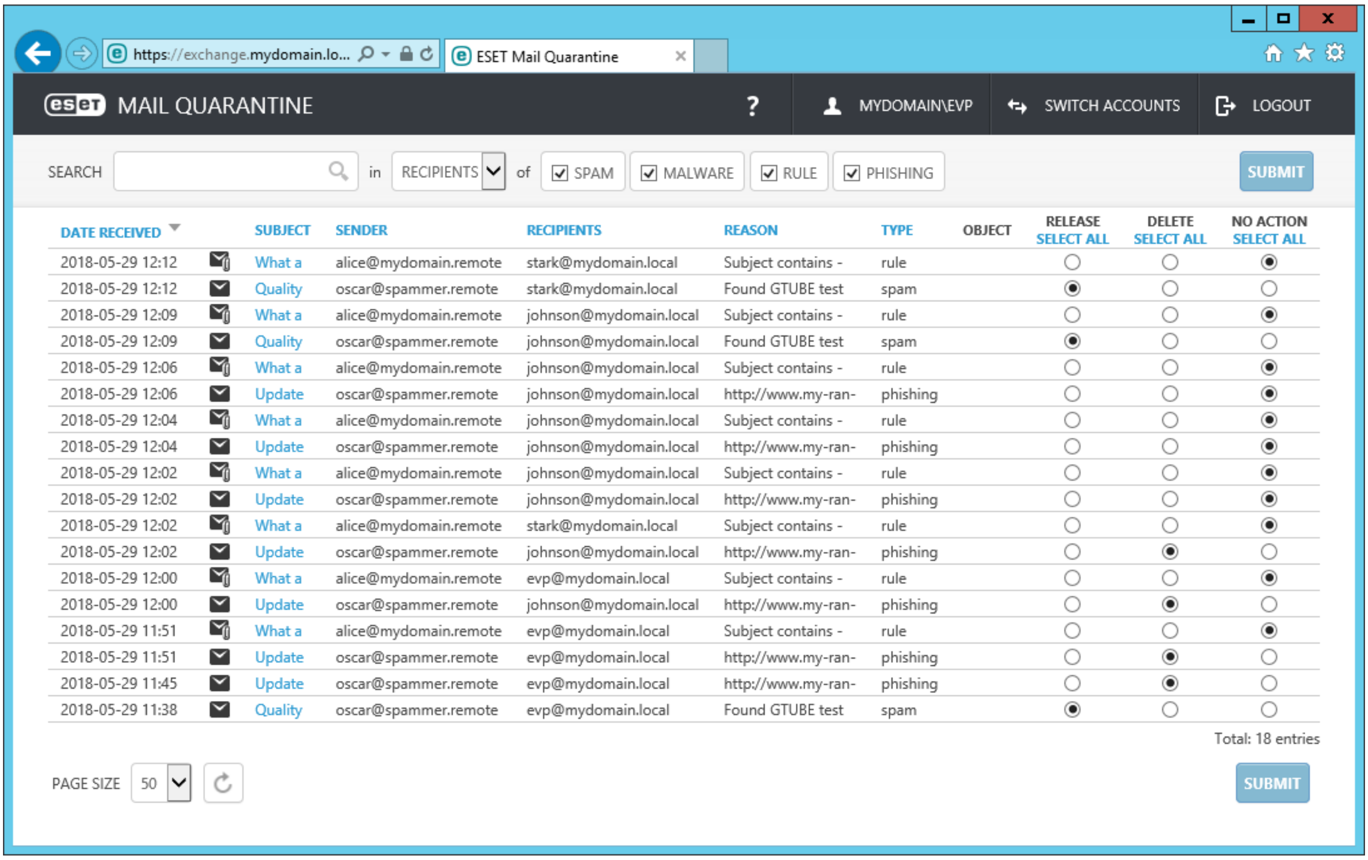
An example of users that were granted additional access rights to the Mail Quarantine Web interface:



Additional access rights

Username	Access type	Recipient address
FRANTO\administrator	Administrator	

To access the Web interface of Mail Quarantine, open your web browser and use the URL specified in **Advanced setup** (**F5**) > **Server** > **Mail quarantine** > **Web interface** > **Web url**.



DATE RECEIVED		SUBJECT	SENDER	RECIPIENTS	REASON	TYPE	OBJECT	RELEASE SELECT ALL	DELETE SELECT ALL	NO ACTION SELECT ALL
2018-05-29 12:12	✉	What a	alice@mydomain.remote	stark@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 12:12	✉	Quality	oscar@spammer.remote	stark@mydomain.local	Found GTUBE test	spam		●	○	○
2018-05-29 12:09	✉	What a	alice@mydomain.remote	johnson@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 12:09	✉	Quality	oscar@spammer.remote	johnson@mydomain.local	Found GTUBE test	spam		●	○	○
2018-05-29 12:06	✉	What a	alice@mydomain.remote	johnson@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 12:06	✉	Update	oscar@spammer.remote	johnson@mydomain.local	http://www.my-ran-	phishing		○	○	●
2018-05-29 12:04	✉	What a	alice@mydomain.remote	johnson@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 12:04	✉	Update	oscar@spammer.remote	johnson@mydomain.local	http://www.my-ran-	phishing		○	○	●
2018-05-29 12:02	✉	What a	alice@mydomain.remote	johnson@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 12:02	✉	Update	oscar@spammer.remote	johnson@mydomain.local	http://www.my-ran-	phishing		○	○	●
2018-05-29 12:02	✉	What a	alice@mydomain.remote	stark@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 12:02	✉	Update	oscar@spammer.remote	johnson@mydomain.local	http://www.my-ran-	phishing		○	●	○
2018-05-29 12:00	✉	What a	alice@mydomain.remote	evp@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 12:00	✉	Update	oscar@spammer.remote	johnson@mydomain.local	http://www.my-ran-	phishing		○	●	○
2018-05-29 11:51	✉	What a	alice@mydomain.remote	evp@mydomain.local	Subject contains -	rule		○	○	●
2018-05-29 11:51	✉	Update	oscar@spammer.remote	evp@mydomain.local	http://www.my-ran-	phishing		○	●	○
2018-05-29 11:45	✉	Update	oscar@spammer.remote	evp@mydomain.local	http://www.my-ran-	phishing		○	●	○
2018-05-29 11:38	✉	Quality	oscar@spammer.remote	evp@mydomain.local	Found GTUBE test	spam		●	○	○

Total: 18 entries

Release

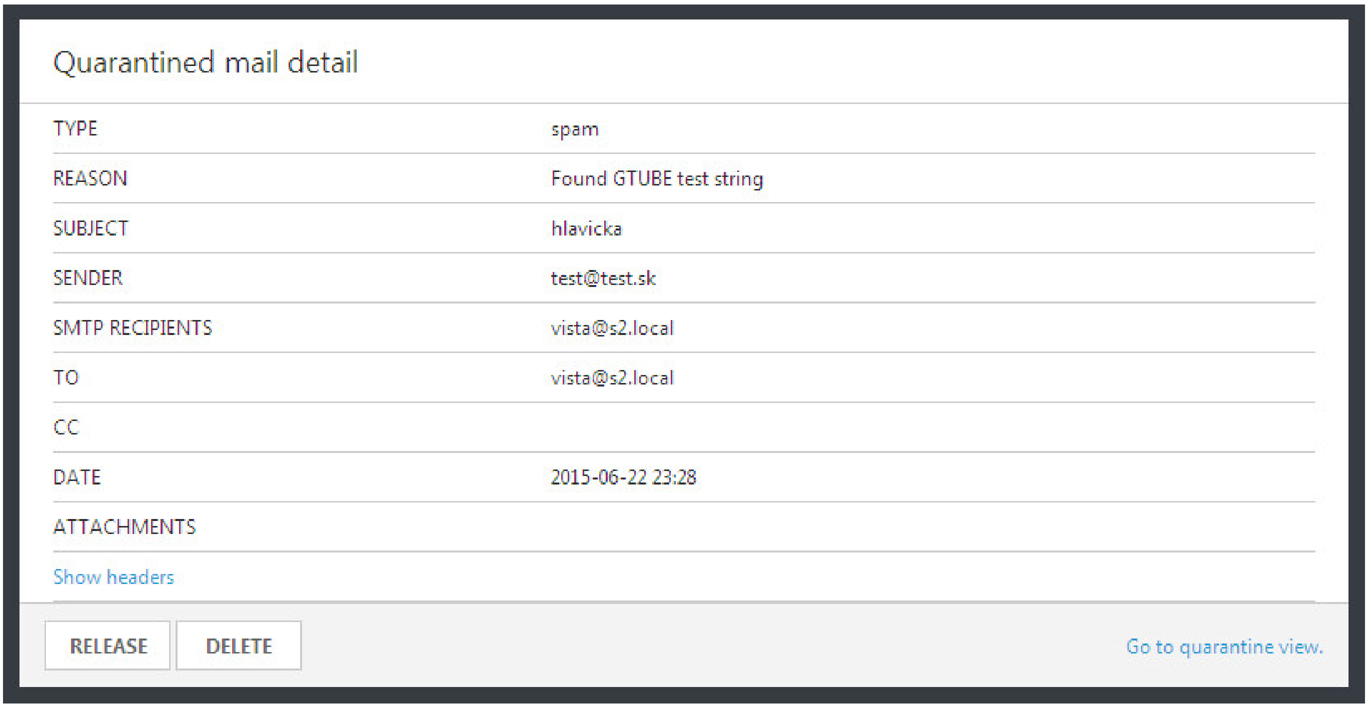
Releases email(s) to its original recipient(s) using the Replay directory and deletes it from quarantine. Click **Submit** to confirm the action.

NOTE
When releasing an email from quarantine, ESET Mail Security ignores the To: MIME header because it can be easily spoofed. Instead, it uses the original recipient information from `RCPT TO:` command acquired during the SMTP connection. This ensures that the correct email recipient receives the message being released from quarantine.

Delete

Deletes item from quarantine. Click **Submit** to confirm the action.

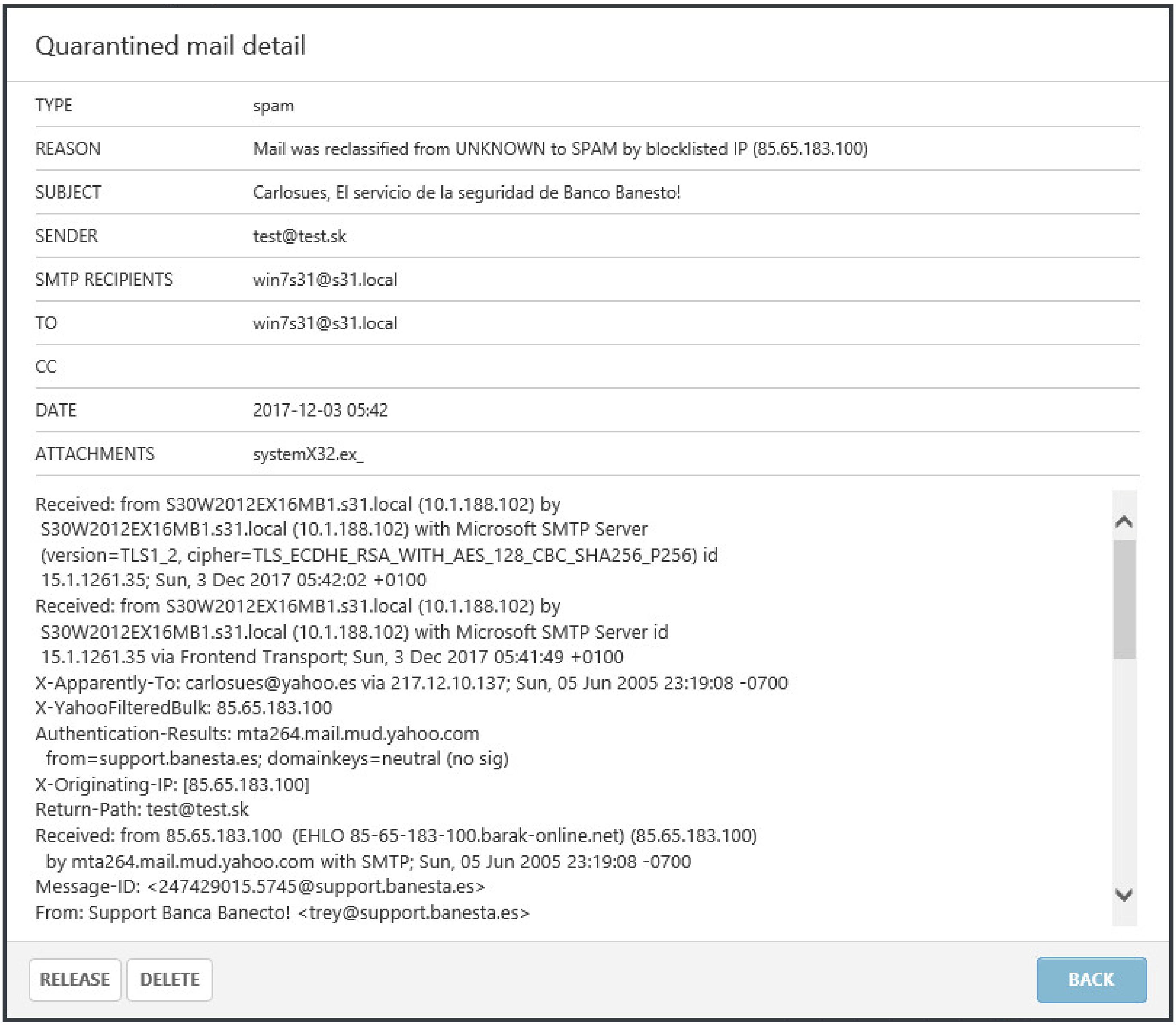
When you click **Subject,** a pop-up window will open with details about the quarantined email, such as Type, Reason, Sender, Date, Attachments, etc.



Quarantined mail detail

TYPE	spam
REASON	Found GTUBE test string
SUBJECT	hlavicka
SENDER	test@test.sk
SMTP RECIPIENTS	vista@s2.local
TO	vista@s2.local
CC	
DATE	2015-06-22 23:28
ATTACHMENTS	

Click **Show headers** to review the header of the quarantined email.



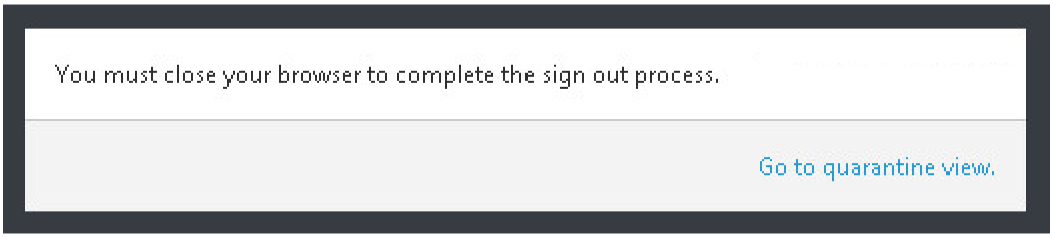
Quarantined mail detail

TYPE	spam
REASON	Mail was reclassified from UNKNOWN to SPAM by blocklisted IP (85.65.183.100)
SUBJECT	Carlosues, El servicio de la seguridad de Banco Banesto!
SENDER	test@test.sk
SMTP RECIPIENTS	win7s31@s31.local
TO	win7s31@s31.local
CC	
DATE	2017-12-03 05:42
ATTACHMENTS	systemX32.ex_

```
Received: from S30W2012EX16MB1.s31.local (10.1.188.102) by
 S30W2012EX16MB1.s31.local (10.1.188.102) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1261.35; Sun, 3 Dec 2017 05:42:02 +0100
Received: from S30W2012EX16MB1.s31.local (10.1.188.102) by
 S30W2012EX16MB1.s31.local (10.1.188.102) with Microsoft SMTP Server id
 15.1.1261.35 via Frontend Transport; Sun, 3 Dec 2017 05:41:49 +0100
X-Apparently-To: carlosues@yahoo.es via 217.12.10.137; Sun, 05 Jun 2005 23:19:08 -0700
X-YahooFilteredBulk: 85.65.183.100
Authentication-Results: mta264.mail.mud.yahoo.com
  from=support.banesta.es; domainkeys=neutral (no sig)
X-Originating-IP: [85.65.183.100]
Return-Path: test@test.sk
Received: from 85.65.183.100  (EHLO 85-65-183-100.barak-online.net) (85.65.183.100)
  by mta264.mail.mud.yahoo.com with SMTP; Sun, 05 Jun 2005 23:19:08 -0700
Message-ID: <247429015.5745@support.banesta.es>
From: Support Banca Banecto! <trey@support.banesta.es>
```

If desired, click **Release** or **Delete** to take action with a quarantined email message.

NOTE
You must close your browser window to completely log out of the Mail Quarantine Web interface. Otherwise, click **Go to quarantine view** to return to the previous screen.



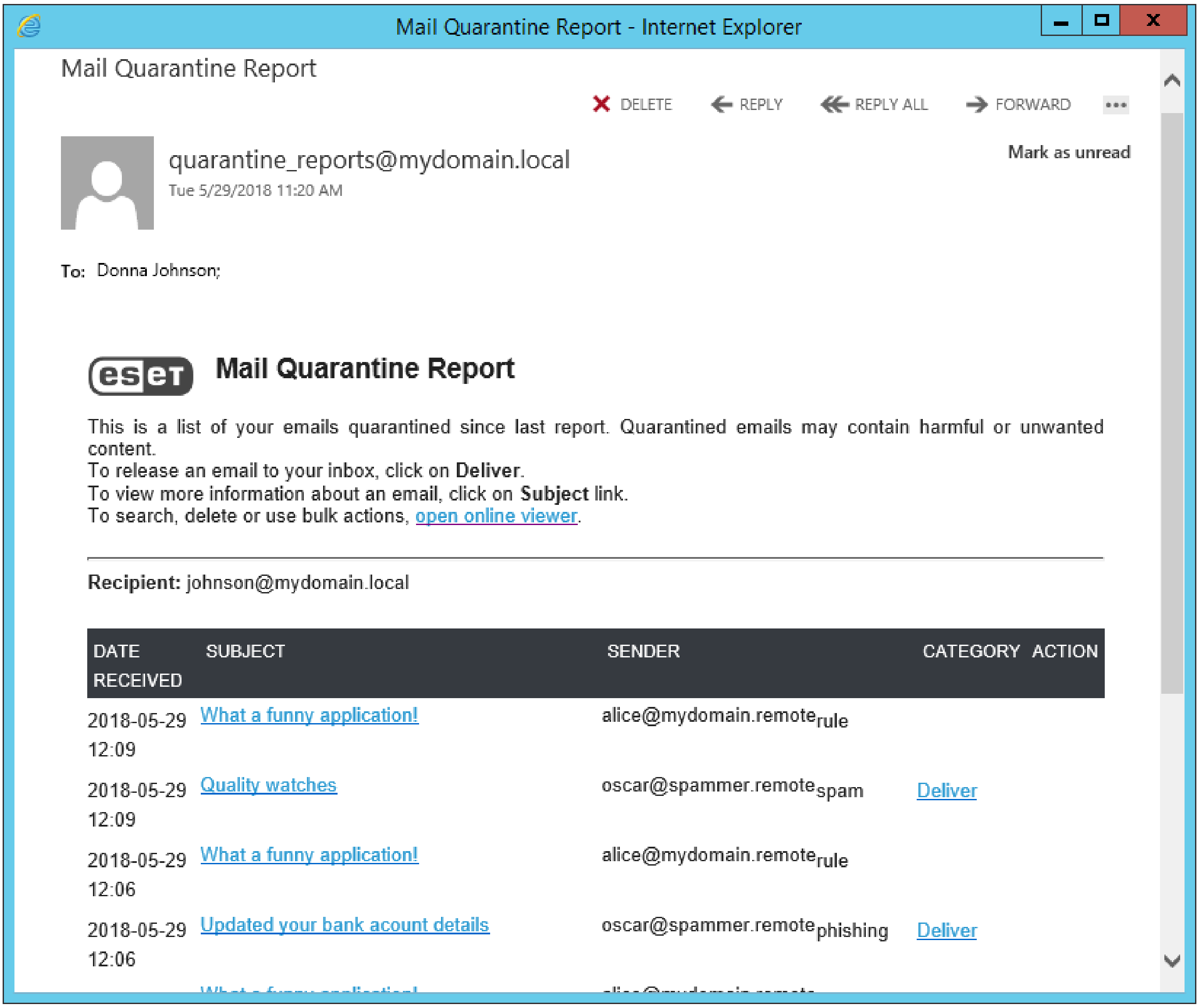
You must close your browser to complete the sign out process.

IMPORTANT
If you are having problems accessing the Mail Quarantine Web interface from your browser or are getting the error `HTTP Error 403.4 - Forbidden` or similar, check to see which Quarantine type is selected and make sure it is **Local quarantine** and that **Enable web interface** is enabled.

Send Mail Quarantine reports - scheduled task

Mail Quarantine reports are notification emails sent to selected users and administrators to inform them about their email messages that were quarantined by ESET Mail Security. Reports contain links that enables you, as well as users who receive the Mail Quarantine reports, to delete or release (deliver) false positive (FP) email message directly. Delivery of certain messages that were filtered out by rules or put into Mail Quarantine by Antivirus protection is not permitted for regular users.

The Send mail quarantine reports / Send mail quarantine administrator reports task sends a Mail Quarantine report via email according to the specified scheduled task. This is an example of user Mail Quarantine report:



quarantine_reports@mydomain.local
Tue 5/29/2018 11:20 AM

To: Donna Johnson;

Mail Quarantine Report

This is a list of your emails quarantined since last report. Quarantined emails may contain harmful or unwanted content.
To release an email to your inbox, click on **Deliver**.
To view more information about an email, click on **Subject** link.
To search, delete or use bulk actions, open online viewer.

Recipient: johnson@mydomain.local

DATE RECEIVED	SUBJECT	SENDER	CATEGORY	ACTION
2018-05-29 12:09	What a funny application!	alice@mydomain.remote	rule	
2018-05-29 12:09	Quality watches	oscar@spammer.remote	spam	Deliver
2018-05-29 12:06	What a funny application!	alice@mydomain.remote	rule	
2018-05-29 12:06	Updated your bank acount details	oscar@spammer.remote	phishing	Deliver
	What a funny application!	alice@mydomain.remote		

Mail Quarantine report also contains a link to User Mail Quarantine Web interface (open online viewer).

NOTE
Send mail quarantine reports task is available only when you are using **Local quarantine**. You will not be able to use it with Quarantine mailbox and MS Exchange quarantine.

Sender address

Specify an email address which to display as a sender of the Mail Quarantine report.

Max count of records in report

You can limit the number of entries per report. Default count is set to 50.

Web URL

This URL will be included in the Mail Quarantine report so that the recipient can simply click the link to access the web interface of Mail Quarantine.

Recipients

Choose users who will be receiving Mail Quarantine reports. Click **Edit** to select the mailboxes for specific recipients.

> NOTE
> Mail Quarantine report will be sent only if there are quarantined messages. If the quarantine is empty, report will not be sent.

> EXAMPLE
> Objective: Create a scheduled task to send Mail Quarantine reports on a regular basis to yourself as an administrator, or to inform users of their spam messages currently stored in the mail quarantine
> Navigate to **Tools** > **Scheduler** > **Add task** and open the wizard.
> Enter **Task name**.
> Select **Task type** from the drop -down menu: **Send mail quarantine reports** (the report will contain only particular user's spam messages) or **Send mail quarantine administrator reports** (the report will contain all messages, the whole quarantine), click **Next**.
> Select one of the options to define when you want the task run. For example, **Weekly** at **10.00.00 AM** on **Friday**.
> Specify **Sender address** (administrator@mydomain.com).
> Click **Edit** to add **Recipients** from the list. Select user's mailboxes who will be receiving Mail Quarantine reports.

User Mail Quarantine Web interface

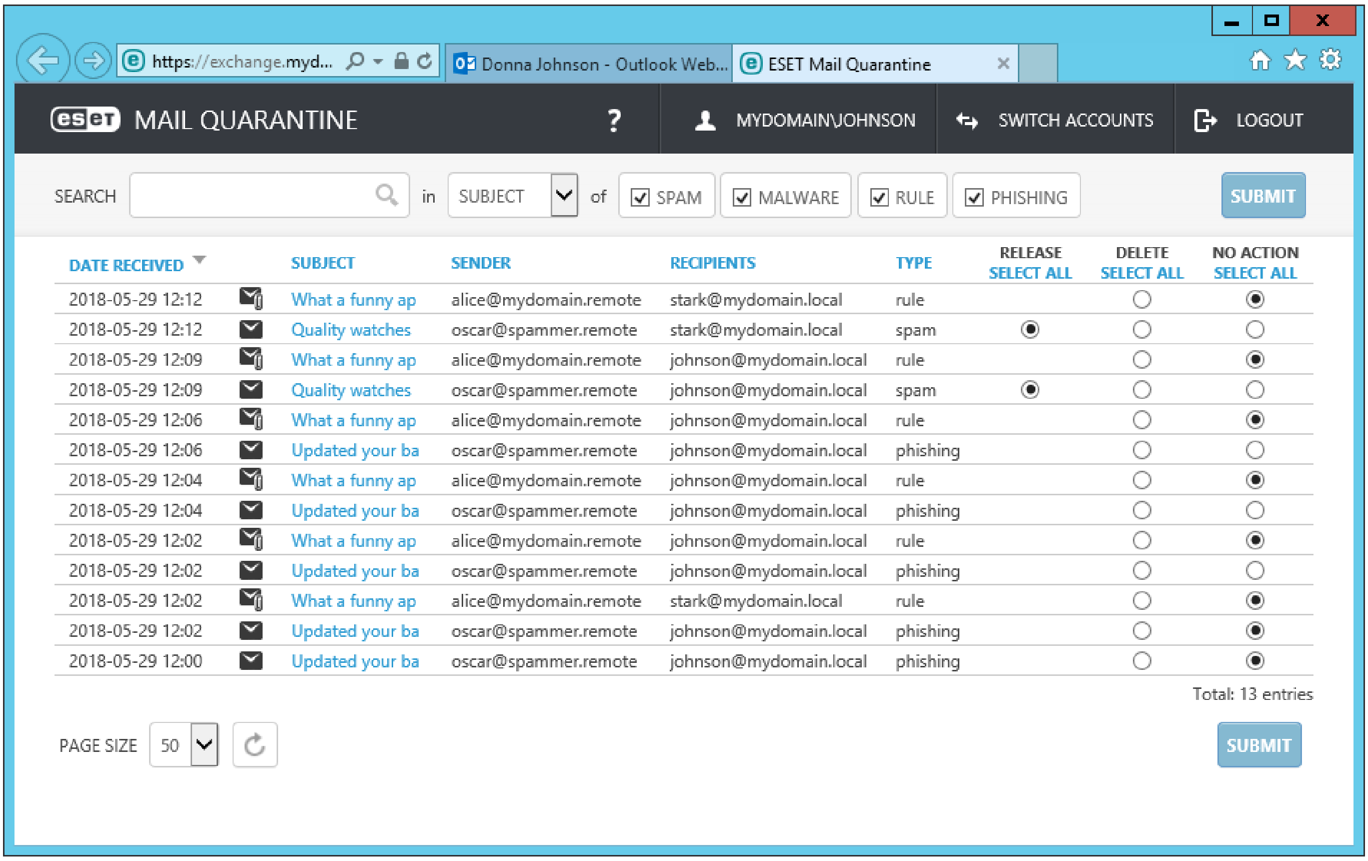
You have been given access to a web interface where you can manage quarantined messages such as spam or phishing, and messages filtered out by rules that were set by administrator. Normally, you can see only messages that were sent to your email address and were quarantined. However, if you have been delegated to manage other users' quarantined messages, you will also see messages of those users. You can distinguish messages by recipients. Use the search function to filter messages by recipient, for example.

You can choose an action to perform with a messages, or multiple messages, such as **release**, **delete** or **no action**. Availability of actions depend on the access level and rule settings, for example, you might not be able to release or delete certain types of messages.

If you have been assigned administrator access, you will see all quarantined messages for all users and can perform any action.

Managing your quarantined messages:

- The Mail Quarantine Web interface allows you to view what has been quarantined. If you have delegated access or even administrator, you will see other quarantined messages as well.



eset MAIL QUARANTINE ? MYDOMAIN\JOHNSON SWITCH ACCOUNTS LOGOUT

SEARCH in SUBJECT of ☑ SPAM ☑ MALWARE ☑ RULE ☑ PHISHING SUBMIT

DATE RECEIVED		SUBJECT	SENDER	RECIPIENTS	TYPE	RELEASE SELECT ALL	DELETE SELECT ALL	NO ACTION SELECT ALL
2018-05-29 12:12	✉	What a funny ap	alice@mydomain.remote	stark@mydomain.local	rule		○	●
2018-05-29 12:12	✉	Quality watches	oscar@spammer.remote	stark@mydomain.local	spam	●	○	○
2018-05-29 12:09	✉	What a funny ap	alice@mydomain.remote	johnson@mydomain.local	rule		○	●
2018-05-29 12:09	✉	Quality watches	oscar@spammer.remote	johnson@mydomain.local	spam	●	○	○
2018-05-29 12:06	✉	What a funny ap	alice@mydomain.remote	johnson@mydomain.local	rule		○	●
2018-05-29 12:06	✉	Updated your ba	oscar@spammer.remote	johnson@mydomain.local	phishing		○	○
2018-05-29 12:04	✉	What a funny ap	alice@mydomain.remote	johnson@mydomain.local	rule		○	●
2018-05-29 12:04	✉	Updated your ba	oscar@spammer.remote	johnson@mydomain.local	phishing		○	○
2018-05-29 12:02	✉	What a funny ap	alice@mydomain.remote	johnson@mydomain.local	rule		○	●
2018-05-29 12:02	✉	Updated your ba	oscar@spammer.remote	johnson@mydomain.local	phishing		○	○
2018-05-29 12:02	✉	What a funny ap	alice@mydomain.remote	stark@mydomain.local	rule		○	●
2018-05-29 12:02	✉	Updated your ba	oscar@spammer.remote	johnson@mydomain.local	phishing		○	●
2018-05-29 12:00	✉	Updated your ba	oscar@spammer.remote	johnson@mydomain.local	phishing		○	●

Total: 13 entries

PAGE SIZE 50 SUBMIT

- You can change the number of entries per page (page size) in the lower left corner of the window.

- If there are too many messages, use the **Search** feature in the upper bar to search for a particular email or to filter the content by **Subject**, **Sender** or **Recipient** (Recipient is only available for users with delegated or administrator access). Additionally, you can use the check boxes to show only message of a certain type (**spam**, **malware**, **rule**, **phishing**).

- To release (deliver) a message that was quarantined as a result of false positive during classification, use radio buttons on the right and select **Release**. To delete a message, select **Delete** action. You can select multiple messages with the appropriate action at the same time. Once your selection is complete, click **Submit**. Messages marked to be released are then delivered to your mailbox, or to the original recipient's mailbox if you have delegated access and are releasing messages for other user(s). Messages marked to be deleted are removed from the quarantine permanently.

NOTE
Both actions, **Release** and **Delete**, are irreversible once you click **Submit**.

- The view automatically refreshes when you click Submit, but you can refresh the view manually by using the refresh button on your web browser, or by pressing **F5** key on your keyboard.

NOTE
Only spam messages can be released. It is not allowed to release messages of malware, phishing and rule type. If you need to release such a message, ask your administrator for assistance.

- You do not need to regularly delete quarantined messages, they are removed automatically after a period of time specified by administrator.

NOTE
You must close your web browser window to completely log out of the Mail Quarantine Web interface. Otherwise, click **Go to quarantine view** to return to the previous screen.

Quarantine mailbox and MS Exchange quarantine

If you decide not to use Local quarantine you have two options, either **Quarantine mailbox** or **MS Exchange quarantine**. Whichever option you choose, you need to create dedicated user with a mailbox (for example, main_quarantine@company.com) which will then be used to store quarantined email messages. This user and mailbox will also be used by Mail Quarantine manager to view and manage items in the quarantine. You will need to specify account details of this user in Quarantine manager settings.

NOTE
The advantage of using Quarantine mailbox/MS Exchange quarantine over Local quarantine is that mail quarantine items are managed from one place regardless of how many servers with Hub Transport Server role. Unlike Local quarantine, Quarantine mailbox/MS Exchange quarantine, SPAM and quarantined email messages are stored within Exchange mailbox database(s). Anyone with access to the quarantine mailbox can manage quarantined messages.

When comparing **Quarantine mailbox** and **MS Exchange quarantine**, both options use a dedicated mailbox as an underlying mechanism for storing quarantined messages, but they differ slightly in the way how email messages are delivered to the mailbox. Quarantine mailbox vs MS Exchange quarantine:

Quarantine mailbox

ESET Mail Security creates a separate wrapper email with additional information and the original emails as an attachment and delivers it to the mailbox.

Specify message quarantine address (for example, main_quarantine@company.com).

IMPORTANT
We do not recommend you using the Administrator user account as the quarantine mailbox.

MS Exchange quarantine

Exchange Server is responsible for delivering the email to the mailbox itself. The mailbox must be set as a Quarantine at the organization level in the Active Directory (by a PowerShell command listed below).

NOTE
By default, internal quarantine is not activated within Microsoft Exchange Server. Unless you have it activated, open Exchange Management Shell and type in following command (replace `Name@domain.com` with an actual address of your dedicated mailbox):

```
Set-ContentFilterConfig -QuarantineMailbox name@domain.com
```

ESET Mail Security uses Microsoft Exchange quarantine system (this applies to Microsoft Exchange Server 2007 and newer). In this case, the Exchange's internal mechanism is used to store potentially infected messages and SPAM.

Quarantine manager settings

Host address

Will appear automatically if your Exchange Server with Client Access Server (CAS) role is present locally. Alternatively, if the CAS role is not present on the same server with ESET Mail Security installed but it can be found within Active Directory (AD), the host address will appear automatically. If it does not appear, you can type the host name manually. Automatic detection will not work on an Edge Transport Server role. IP address is not supported, you need to use the host name of the CAS server.

Username

Dedicated quarantine user account you have created for storing quarantined messages (or an account that has access to this mailbox via access delegation). On Edge Transport Server role that is not part of the domain, it is necessary to use the whole email address (for example *main_quarantine@company.com*).

Password

Type password of your quarantine account.

Use SSL

Needs to be enabled if Exchange Web Services (EWS) is set to **Require SSL** in IIS. If SSL is enabled, Exchange Server certificate must be imported on the system with ESET Mail Security (in case Exchange Server roles are on different servers). Settings for the EWS can be found in IIS in *Sites/Default web site/EWS/SSL Settings*.

NOTE
Only disable **Use SSL** when Exchange Web Services (EWS) is configured in IIS to not require SSL.

Ignore server certificate errors

Ignores following states: *self-signed, wrong name in certificate, wrong usage, expired*.

Proxy server

In case you use a proxy server between your Exchange Server with CAS role and Exchange Server where ESET Mail Security is installed, specify parameters of your proxy server. This is required because ESET Mail Security connects to Exchange Web Services (EWS) API via HTTP/HTTPS. Otherwise, Quarantine mailbox and MS Exchange quarantine will not work.

Proxy server

Enter IP address or name of the proxy server you use.

Port

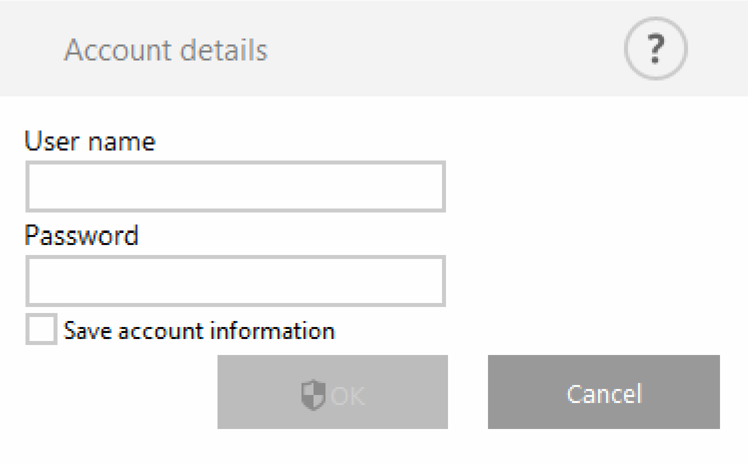
Enter port number of the proxy server.

Username, Password

Enter credentials if your proxy server requires authentication.

Quarantine manager account details

This dialog window will display if you have not specified account details (user name and password) for your Quarantine manager. Specify credentials for a user with access to the Quarantine mailbox and click **OK**. Alternatively, press **F5** to access **Advanced setup** and navigate to **Server** > **Mail Quarantine** > Quarantine manager settings. Type the **User name** and **Password** for your quarantine mailbox.



Click the check box next to **Save account information** to save account settings for future use when accessing Quarantine manager.

Antivirus test

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a harmless file detectable by all Antivirus programs. It was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of Antivirus programs.

To test your Antivirus functionality, create a text file that contain the following string:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

For more information, also to download test files in different forms, visit http://2016.eicar.org/85-0-Download.html.

Antispam test

Using a special test string know as GTUBE (Generic Test for Unsolicited Bulk Email), you can verify that Antispam feature of ESET Mail Security works and detects incoming spam messages.

To test Antispam functionality, send an email with the following 68-byte string in the message body:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Use the string as is (one line, without any whitespace or line breaks). You can download suitable email message in RFC-822 format.

Anti-Phishing test

To test Anti-Phishing functionality, send an email with the following link (URL) in the message body or subject:

```
https://www.amtso.org/check-desktop-phishing-page/
```

To see the activity of Anti-Phishing mail protection, check **Log files** > Mail server protection log. It will contains information about email messages and their phishing links that were found.

General settings

You can configure general settings and options based on your needs. The menu on the left includes the following categories:

Computer

Enable or disable detection of potentially unwanted, unsafe, suspicious application and Anti-Stealth protection. Specify exclusions of processes or files and folders. Configure Real-time file system protection, ThreatSense parameters, Cloud-based protection (ESET LiveGrid®), Malware scans (On-demand computer scan and other scan options), Hyper-V scan and HIPS.

Update

Configure update options such as profiles, detection engine age, snapshots for module rollback, update type, custom update server, connection/proxy server, update mirror, access to update files, HTTP server, user account details for network connection, etc.

Web and email

Enables you to configure Protocol filtering and exclusions (Excluded applications and IP addresses), SSL/TLS protocol filtering options, Email client protection (integration, email protocols, alerts and notifications), Web access protection (HTTP/HTTPS web protocols and URL address management) and email client Anti-Phishing protection.

Device control

Enable integration and configure Device control Rules and Groups.

Tools configuration

Allows you to customize tools, such as ESET CMD, ESET RMM, WMI provider, ESET Security Management Center scan tragets, Windows Update notifications, Log files, Proxy server, Email notifications, Diagnostics, Cluster, etc.

User interface

Configure the behavior of the program's GUI, Statuses, License information, Alerts and notifications, Password protection, eShell execution policy, etc.

Computer

Detection engine guards against malicious system attacks by scanning files, emails and network communication. If an object classified as malware is detected, remediation will start. Detection engine can eliminate it by first blocking it and then taking action such as cleaning, deleting or moving to quarantine.

Real-time & Machine learning protection

Advanced machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection based on machine learning. Read more about this type of protection in the glossary. You can configure Reporting and Protection levels of the following categories:

Malware

> A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term “virus” is often misused. "Malware” (malicious software) is a more accurate term. Malware detection is performed by the detection engine module combined with the machine learning component. Read more about these types of applications in the glossary.

Potentially unwanted applications (PUAs)

> A Potentially unwanted application is a software with an intent not unequivocally malicious, however; it may install additional unwanted software, change the behavior of the digital device, perform activities not approved or expected by the user or has unclear objectives.
> This category includes advertising display software, download wrappers, various browser toolbars, software with misleading behavior, bundleware, trackware, etc.
> Read more about these types of applications in the glossary.

Potentially suspicious applications

> Is a software compressed with packers or protectors frequently used to deter reverse engineering or to obfuscate the content of the executable (for example, to hide the presence of malware) by proprietary methods of compression and/or encryption.
> This category includes: all unknown applications that are compressed with a packer or protector frequently used to compress malware.

Potentially unsafe applications

> This classification is given for commercial, legitimate software that might be misused for malicious purposes. An unsafe application refers to legitimate commercial software that has the potential to be misused for malicious purposes.
> This category includes: cracking tools, license key generators, hacking tools, remote access or control tools, password-cracking applications and keyloggers (programs that record each keystroke typed by a user). This option is disabled by default.
> Read more about these types of applications in the glossary.

Read the following before modifying a threshold (or level) for category Reporting or Protection:

Reporting

Reporting is performed by the detection engine and machine learning component. You can set the reporting threshold to better suit your environment and needs. There is not a single correct configuration. Therefore, we recommend that you monitor the behavior within your environment and decide whether a different Reporting setting is more suitable.

Reporting does not take action with objects, it passes information to a respective protection layer, and the protection layer taks action accordingly.

Aggressive	**Reporting configured to maximum sensitivity. More detections are reported. While the Aggressive setting may appear to be the safest, it can often be too sensitive, which might even be counterproductive.** NOTE The aggressive setting may falsely identify objects as malicious, and action will be taken with such objects (depending on Protection settings).
Balanced	This setting is an optimal balance between performance and accuracy of detection rates and the number of falsely reported objects.
Cautious	Reporting configured to minimize falsely identified objects while maintaining a sufficient level of protection. Objects are reported only when the probability is evident and matches malicious behavior.
Off	Reporting is not active. Detections are not found, reported or cleaned. NOTE Malware reporting cannot be deactivated; therefore, the **Off** setting is not available for Malware.

If you want to Revert settings in this section to their default values, click the "U-turn" arrow next to the section header. Any changes you have made in this section will be lost.

Protection

When an object is reported based on the configuration above and the machine learning results, it is blocked and and action is taken (cleaned, deleted or moved to Quarantine).

Aggressive	**Reported aggressive (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started.**
Balanced	Reported balanced (or lower) level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Cautious	Reported cautious level detections are blocked, and automatic remediation (i.e., cleaning) is started.
Off	Reporting is not active, no detections are not found, reported or cleaned. NOTE Malware reporting cannot be deactivated, therefore the **Off** setting is not available for Malware.

If you want to Revert settings in this section to their default values, click the "U-turn" arrow next the to section header. Any changes you have made in this section will be lost.

NOTE
By default, the above machine learning protection settings apply to On-demand computer scan as well. If required, you can configure **On-demand & Machine learning protection** settings separately. Click the switch icon to disable **Use real-time protection settings** and proceed with configuration.

Machine learning protection

Detection engine guards against malicious system attacks by scanning files, emails and network communication. If an object classified as malware is detected, remediation will start. Detection engine can eliminate it by first blocking it and then taking action such as cleaning, deleting or moving to quarantine.

Real-time & Machine learning protection

Advanced machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection based on machine learning. Read more about this type of protection in the glossary. You can configure Reporting and Protection levels of the following categories:

Malware

A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term “virus” is often misused. "Malware” (malicious software) is a more accurate term. Malware detection is performed by the detection engine module combined with the machine learning component. Read more about these types of applications in the glossary.

Potentially unwanted applications (PUAs)

A Potentially unwanted application is a software with an intent not unequivocally malicious, however; it may install additional unwanted software, change the behavior of the digital device, perform activities not approved or expected by the user or has unclear objectives.
This category includes advertising display software, download wrappers, various browser toolbars, software with misleading behavior, bundleware, trackware, etc.
Read more about these types of applications in the glossary.

Potentially suspicious applications

Is a software compressed with packers or protectors frequently used to deter reverse engineering or to obfuscate the content of the executable (for example, to hide the presence of malware) by proprietary methods of compression and/or encryption.
This category includes: all unknown applications that are compressed with a packer or protector frequently used to compress malware.

Potentially unsafe applications

This classification is given for commercial, legitimate software that might be misused for malicious purposes. An unsafe application refers to legitimate commercial software that has the potential to be misused for malicious purposes.
This category includes: cracking tools, license key generators, hacking tools, remote access or control tools, password-cracking applications and keyloggers (programs that record each keystroke typed by a user). This option is disabled by default.
Read more about these types of applications in the glossary.

Read the following before modifying a threshold (or level) for category Reporting or Protection:

Reporting

Reporting is performed by the detection engine and machine learning component. You can set the reporting threshold to better suit your environment and needs. There is not a single correct configuration. Therefore, we recommend that you monitor the behavior within your environment and decide whether a different Reporting setting is more suitable.

Reporting does not take action with objects, it passes information to a respective protection layer, and the protection layer taks action accordingly.

Aggressive	**Reporting configured to maximum sensitivity. More detections are reported. While the Aggressive setting may appear to be the safest, it can often be too sensitive, which might even be counterproductive.** NOTE The aggressive setting may falsely identify objects as malicious, and action will be taken with such objects (depending on Protection settings).
Balanced	This setting is an optimal balance between performance and accuracy of detection rates and the number of falsely reported objects.
Cautious	Reporting configured to minimize falsely identified objects while maintaining a sufficient level of protection. Objects are reported only when the probability is evident and matches malicious behavior.
Off	Reporting is not active. Detections are not found, reported or cleaned. NOTE Malware reporting cannot be deactivated; therefore, the **Off** setting is not available for Malware.

If you want to Revert settings in this section to their default values, click the "U-turn" arrow next to the section header. Any changes you have made in this section will be lost.

Mail Transport & Machine learning protection

Reporting

Performed by detection engine and the machine learning component. Reporting does not take an action with objects (this is done by respective protection layer).

Protection

Configure parameters in Mail transport protection to affect what action is taken with reported objects. Also, you can configure a custom rule:

> EXAMPLE
> Objective: Quarantine messages that contain malware or attachment that is password protected, encrypted or damaged
> Create the following rule for **Mail transport protection**:
> **Condition**
> Type: **Antivirus scan result**
> Operation: **is**
> Parameter: **Infected - not cleaned**
> **Action**
> Type: **Quarantine message**

If you want to Revert settings in this section to their default values, click the "U-turn" arrow next the to section header. Any changes you have made in this section will be lost.

Configure Machine learning protection using eShell. The Context name in eShell is **MLP**. Open eShell in interactive mode and navigate to MLP:

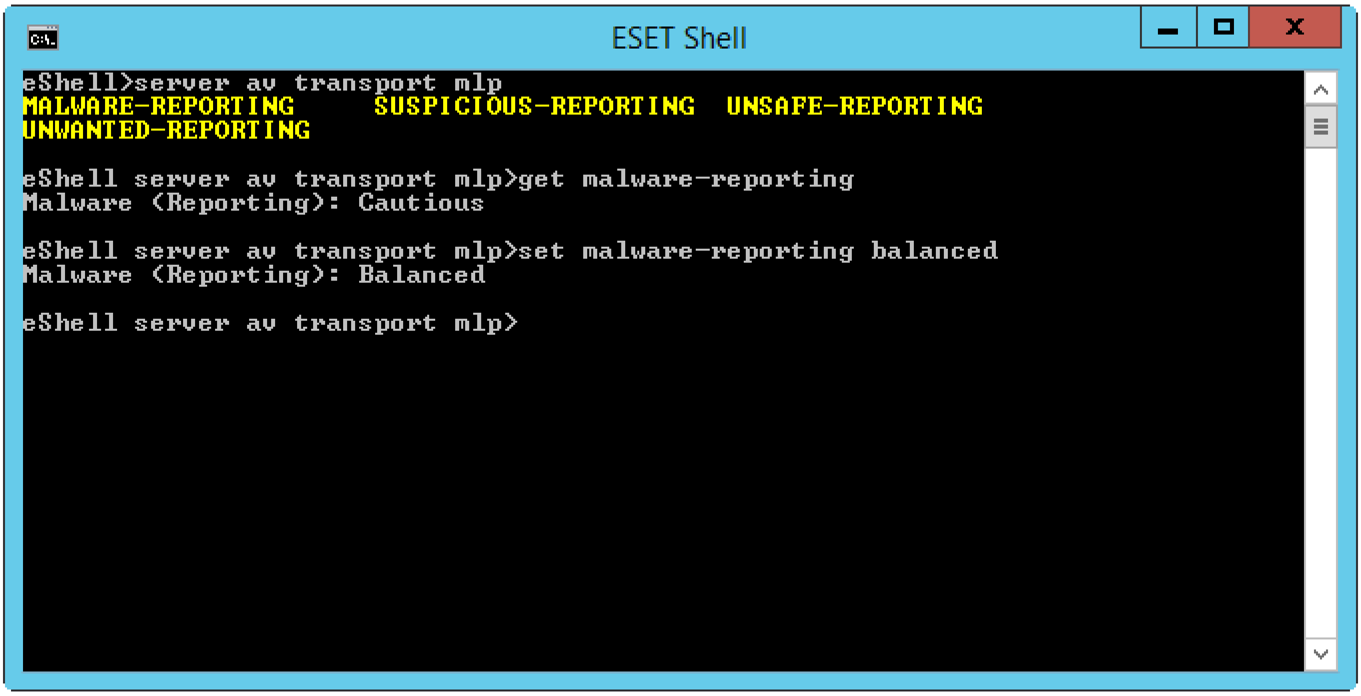
```
server av transport mlp
```

See what is the current reporting setting for Suspicious applications:

```
get suspicious-reporting
```

If you want less strict reporting, change the setting to Cautious:

```
set suspicious-reporting cautious
```



```
eShell>server av transport mlp
MALWARE-REPORTING      SUSPICIOUS-REPORTING  UNSAFE-REPORTING
UNWANTED-REPORTING

eShell server av transport mlp>get malware-reporting
Malware (Reporting): Cautious

eShell server av transport mlp>set malware-reporting balanced
Malware (Reporting): Balanced

eShell server av transport mlp>
```

Mailbox Database Protection & Machine learning protection

Reporting

Performed by detection engine and the machine learning component. Reporting does not take an action with objects (this is done by respective protection layer).

Protection

Configure parameters in Mailbox database protection to affect what action is taken with reported objects.

If you want to Revert settings in this section to their default values, click the "U-turn" arrow next the to section header. Any changes you have made in this section will be lost.

Configure Machine learning protection using eShell. The Context name in eShell is **MLP**. Open eShell in interactive mode and navigate to MLP:

```
server av database mlp
```

See what is the current reporting setting for Suspicious applications:

```
get suspicious-reporting
```

If you want less strict reporting, change the setting to Cautious:

```
set suspicious-reporting cautious
```

⌄ On-demand mailbox database scan & Machine learning protection

Reporting

Performed by detection engine and the machine learning component. Reporting does not take an action with objects (this is done by respective protection layer).

Protection

Configure parameters in On-demand mailbox database scan to affect what action is taken with reported objects.

If you want to Revert settings in this section to their default values, click the "U-turn" arrow next the to section header. Any changes you have made in this section will be lost.

Configure Machine learning protection using eShell. The Context name in eShell is **MLP**. Open eShell in interactive mode and navigate to MLP:

```
server av on-demand mlp
```

See what is the current reporting setting for Suspicious applications:

```
get suspicious-reporting
```

If you want less strict reporting, change the setting to Cautious:

```
set suspicious-reporting cautious
```

Exclusions

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

> WARNING
> Not to be confused with excluded extensions, processes exclusions or exclusion filter.

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

Select the exclusions type and click **Edit** to add a new one or modify existing:

- Performance exclusions - Exclude files and folders from scanning.
- Detection exclusions - Exclude objects from scanning using specific criteria – path, file hash or detection name.

Performance exclusions

This feature allows you to exclude files and folders from scanning. Performance exclusions are useful to exclude file-level scanning of mission critical applications or when scanning causes abnormal system behavior or decreases performance.

Path

Excludes specific path (file or directory) for this computer. Do not use wildcards - asterisk (*) in the middle of a path. See the following Knowledgebase article for more information.

NOTE
To exclude folder contents, do not forget to add the asterisk (*) at the end of the path (*C:\Tools\**). *C:\Tools* will not be excluded, because from the scanner's perspective, *Tools* can also be a file name.

Comment

Add an optional **Comment** to easily recognize the exclusion in the future.

EXAMPLE
Path exclusions using an asterisk:
C:\Tools\* - path must end with the backslash (\) and asterisk (*) to indicate that it is a folder and all folder content (files and subfolders) will be excluded
*C:\Tools\*.** - the same behavior as *C:\Tools\**, which means, it works recursively
C:\Tools\*.dat - will exclude *dat* files in the Tools folder
C:\Tools\sg.dat - will exclude this particular file located in the exact path

EXAMPLE
To exclude all files in a folder, type the path to the folder and use the mask **.**
- To exclude doc files only, use the mask **.doc*
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for certain (say “D”), use the following format:

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

EXAMPLE

Use system variables like *%PROGRAMFILES%* to define scan exclusions.

- To exclude the Program Files folder using this system variable, use the path *%PROGRAMFILES%*\ (make sure to add the backslash at the end of path when adding to exclusions)
- To exclude all files in a *%HOMEDRIVE%* subdirectory, use the path *%HOMEDRIVE%\Excluded_Directory\*.**

The following variables can be used in the path exclusion format:

%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%

User-specific system variables (like *%TEMP%* or *%USERPROFILE%*) or environment variables (like *%PATH%*) are not supported.

Detection exlusions

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

The easiest way to create a detection-based exclusion is using an existing detection from the **Log files** > Detections. Right-click a log record (detection) and click **Create exclusion**. This will open the exclusion wizard with pre-defined criteria.

To manually create a detection exclusion, click **Edit** > **Add** (or **Edit** when modifying existing) and specify one or more of the following criteria (can be combined):

Path

Excludes specific path (file or directory). You can browse for a specific location/file, or enter the string manually. Do not use wildcards - asterisk (*) in the middle of a path. See the following Knowledgebase article for more information.

NOTE

To exclude folder contents, do not forget to add the asterisk (*) at the end of the path (*C:\Tools\**). *C:\Tools* will not be excluded, because from the scanner's perspective, *Tools* can also be a file name.

Hash

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

Detection name

Enter a valid detection (threat) name. Creating an exclusion based on the detection name alone may pose a security risk. We recommend you combine the detection name with the Path. This exclusion criteria can be used only for certain types of detections.

Comment

Add an optional **Comment** to easily recognize the exclusion in the future.

ESET Security Management Center includes detection exclusions management to create a detection exclusions and apply it to more computers/group(s).

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

EXAMPLE
Path exclusions using an asterisk:
C:\Tools\* - path must end with the backslash (\) and asterisk (*) to indicate that it is a folder and all folder content (files and subfolders) will be excluded
*C:\Tools\*.** - the same behavior as *C:\Tools\**, which means, it works recursively
C:\Tools\*.dat - will exclude *dat* files in the Tools folder
C:\Tools\sg.dat - will exclude this particular file located in the exact path

EXAMPLE
To exclude a threat, enter the valid detection name in the following format:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

EXAMPLE
To exclude all files in a folder, type the path to the folder and use the mask **.**

- To exclude an entire drive including all files and subfolders, use the mask *D:\**
- To exclude doc files only, use the mask **.doc*
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for certain (say “D”), use the following format:

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

EXAMPLE

Use system variables like *%PROGRAMFILES%* to define scan exclusions.

- To exclude the Program Files folder using this system variable, use the path *%PROGRAMFILES%*\ (make sure to add the backslash at the end of path when adding to exclusions)
- To exclude all files in a *%HOMEDRIVE%* subdirectory, use the path *%HOMEDRIVE%\Excluded_Directory\*.**

The following variables can be used in the path exclusion format:

%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%

User-specific system variables (like *%TEMP%* or *%USERPROFILE%*) or environment variables (like *%PATH%*) are not supported.

Create exclusion wizard

The recommended exclusion is pre-selected based on the detection type, but you can further specify exclusion criteria for detections. Click **Change criteria**:

- **Exact files** – Exclude each file by its SHA-1 hash.
- **Detection** – Specify the detection name to exclude each file that contains such detection.
- **Path + Detection** – Specify the detection name and path (including file name) to exclude each file with a detection located in the specified location.

Add an optional **Comment** to easily recognize the exclusion in the future.

Advanced options

Anti-Stealth technology

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

AMSI

Let Microsoft Antimalware Scan Interface (AMSI) to scan Powershell scripts executed by Windows script Host.

Automatic exclusions

The developers of server applications and operating systems recommend excluding sets of critical working files and folders from malware scan for most of their products. Malware scan may have a negative influence on a server's performance, which may lead to conflicts and even prevent some applications from running on the server. Exclusions help minimize the risk of potential conflicts and increase the overall performance of the server when running Anti-Malware software. See the complete list of files excluded from scanning for ESET server products.

ESET Mail Security identifies critical server applications and server operating system files, and automatically adds them to the list of Exclusions. All automatic exclusions are enabled by default. You can disable/enable each server application exclusions using the slider bar with the following result:

- When enabled, any of its critical files and folders will be added to the list of files excluded from scanning. Every time the server is restarted, the system performs an automatic check of exclusions and updates the list if there were system or application changes (for example when a new server application was installed). This setting ensures the recommended Automatic exclusions are always applied.

- When disabled, automatically excluded files and folders will be removed from the list. Any user-defined exclusions entered manually will not be affected.

The Automatic exclusions for Exchange Servers are based on Microsoft's recommendations. ESET Mail Security applies "Directory/Folder exclusions" only ("Process exclusions" and "File name extension exclusions" are not applied). See the following Microsoft Knowledge Base articles for details:

- Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows
- Recommendations for troubleshooting an Exchange Server computer with antivirus software installed
- File-Level Antivirus Scanning on Exchange 2007
- File-Level Antivirus Scanning on Exchange 2010
- Anti-Virus Software in the Operating System on Exchange Servers (Exchange 2013)
- Running Windows antivirus software on Exchange 2016 servers

> NOTE
> There are also Exchange database file exclusions for Active and Passive databases in DAG (Database Availability Group) hosted on local server. List of Automatic exclusions is updated every 30 minutes. If there is a new Exchange database file created, it will automatically get excluded regardless of its state, whether it is Active or Passive.

To identify and generate automatic exclusions, ESET Mail Security uses dedicated application *eAutoExclusions.exe*, located in the installation folder. No interaction is needed from your side, but you can use command line to list detected server applications on your system by executing `eAutoExclusions.exe -servers`. To display full syntax, use `eAutoExclusions.exe -?`.

Shared local cache

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

Cache server setup contains the following:

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

An infiltration is detected

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

Standard behavior

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

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

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

Cleaning and deleting

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

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

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

Multiple threats

If any infected files were not cleaned during Computer scan (or the Cleaning level was set to **No Cleaning**), an alert window prompting you to select actions for those files is displayed. Select an action individually for each threat in the list or you can use **Select action for all listed threats** and choose one action to take on all the threats in the list, then click **Finish**.

Deleting files in archives

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

Real-time file system protection

Real-time file system protection controls all malware-related events in the system. All files are scanned for malicious code when they are opened, created, or run on your computer. By default, Real-time file system protection launches at system start-up and provides uninterrupted scanning. In special cases (for example, if there is a conflict with another real-time scanner), real-time protection can be disabled by disengaging **Start Real-time file system protection automatically** in **Advanced setup** (**F5**) under **Real-time file system protection** > **Basic**.

ESET Mail Security is compatible with machines using Azure File Sync agent with cloud tiering enabled. ESET Mail Security recognizes files with attribute *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Media to scan

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

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

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

Scan on

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

- **File open** - Scanning when files are opened / accessed.
- **File creation** - Scanning when files are created / modified.
- **File execution** - Scanning when files are executed.
- **Removable media access** - Scanning when accessing removable storage. When removable media that contains a boot sector is inserted in the device, the boot sector is immediately scanned. This option does not enable removable media file scanning. Removable media file scanning is located **Media to scan** > **Removable media**. For Removable media boot sector access to work correctly, keep **Boot sectors/UEFI enabled** in ThreatSense parameters.

Processes exclusions

Enables you to exclude specific processes. For example, processes of the backup solution, all file operations attributed to such excluded process are ignored and considered safe, thus minimizing the interference with the backup process.

ThreatSense parameters

Real-time file system protection checks all types of media and is triggered by various system events such as accessing a file. Real-time file system protection can be configured to treat newly created files differently than existing files. For example, you can configure Real-time file system protection to more closely monitor newly created files.

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each detection engine database update. This behavior is controlled using **Smart optimization**. If **Smart optimization** is disabled, all files are scanned each time they are accessed. To modify this setting, press **F5** to open **Advanced setup** and expand **Computer** > **Real-time file system protection**. Click **ThreatSense parameters** > **Other** and select or deselect **Enable Smart optimization**.

Additional ThreatSense parameters

You can modify detailed options of the **Additional ThreatSense parameters for newly created and modified files** or **Additional ThreatSense parameters for executed files**.

ThreatSense parameters

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

> NOTE
> For details about automatic startup file check, see Startup scan.

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

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

To enter the setup window, click **ThreatSense engine parameter setup** in the **Advanced setup** (**F5**) window for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Mail transport protection
- On-demand mailbox database protection
- Mailbox database protection
- Hyper-V scan
- Real-time file system protection
- Malware scans
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection

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

⊟ Objects to scan

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

Operating memory

Scans for threats that attack the operating memory of the system.

Boot sectors/UEFI

Scans boot sectors for the presence of viruses in the MBR (Master Boot Record). In case of a Hyper-V Virtual Machine, its disk MBR is scanned in read - only mode.

Email files

The program supports the following extensions: DBX (Outlook Express) and EML.

Archives

The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives

Self-extracting archives (SFX) are archives needing no specialized programs – archives – to decompress themselves.

Runtime packers

After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

> NOTE
> For the Mailbox database protection feature, attached email files (for example *.eml files*) are scanned regardless of the setting under **Objects to scan**. This is because Exchange Server parses the attached .eml file before it is submitted for scanning by ESET Mail Security. The VSAPI plug-in gets extracted files from the .eml attachment instead of receiving the original .eml file.

⊟ Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics

A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not known by the previous detection engine.

Advanced heuristics/DNA signatures

Advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high-level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

⊟ Cleaning

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

No cleaning

Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Normal cleaning

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

Strict cleaning

The program will clean or delete all infected files. The only exceptions are system files. If it is not possible to clean a file, the user will be asked what type of action should be taken.

WARNING

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

IMPORTANT

If a Hyper-V host is running on Windows Server 2008 R2 SP1, **Normal cleaning** and **Strict cleaning** are not supported. Scanning of Virtual Machine disks is done in read-only mode, no cleaning will be performed. Regardless of the cleaning level selected, the scan is always performed in read-only mode.

⊟ Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file.

This section of the ThreatSense parameter setup lets you define the types of files to exclude from scan.

Other

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

Scan alternate data streams (ADS)

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

Run background scans with low priority

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

Log all objects

If this option is selected, the log file will show all the scanned files, even those not infected.

Enable Smart optimization

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

Preserve last access timestamp

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

⊟ Limits

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

Default object settings

Enable to use default settings (no limits). ESET Mail Security will be ignoring your custom settings.

Maximum object size

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

Maximum scan time for object (sec.)

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

Archive scan setup

To modify archive scan settings, deselect **Default archive scan settings**.

Archive nesting level

Specifies the maximum depth of archive scanning. Default value: 10. For objects detected by Mailbox transport protection, actual nesting level is +1 because archive attachment in an email is considered first level.

> EXAMPLE
> If you have nesting level set to 3, an archive file with nesting level 3 will only be scanned on a transport layer up to its actual level 2. Therefore, if you want to have archives scanned by Mailbox transport protection up to level 3, set the value for **Archive nesting level** to 4.

Maximum size of file in archive

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

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

Additional ThreatSense parameters

Additional ThreatSense parameters for newly created and modified files

The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before module update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, disable **Default archive scan settings**.

Additional ThreatSense parameters for executed files

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

File extenstions excluded from scanning

An extension is the part of a file name delimited by a period. The extension defines the type of a file. Normally, all files are scanned. However, if you need to exclude files with a specific extension, ThreatSense parameter setup lets you exclude files from scanning based on their extension. Excluding may be useful if scanning of certain file types prevents an application from running properly.

EXAMPLE
To add a new extension to the list, click **Add**. Type the extension into the text field (for example `tmp`) and click **OK**. When you select **Enter multiple values**, you can add multiple file extensions delimited by lines, commas or semicolons (for example, choose **Semicolon** from the drop-down menu as a separator, and type `edb;eml;tmp`).
You can use a special symbol ? (question mark). The question mark represents any symbol (for example `?db`).

NOTE
To display the extension (file type) for all files in a Windows operating system, deselect **Hide extensions for known file types** under **Control Panel** > **Folder Options** > **View**.

Processes exclusions

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

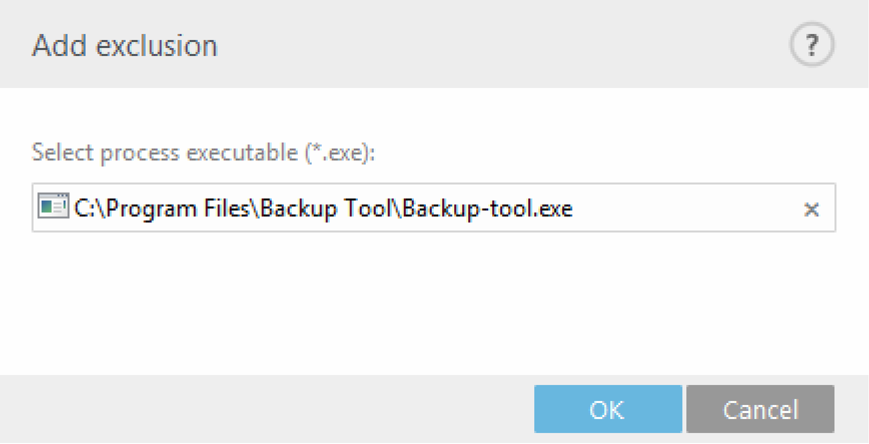
Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (*.exe*).

You can add executable files into the list of excluded processes via **Advanced setup** (**F5**) > **Computer** > **Real-time file system protection** > **Basic** > **Processes exclusions** or using the list of running processes from the main menu **Tools** > **Running processes**.

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

EXAMPLE
Click **Edit** to open the **Processes exclusions** management window, where you can **Add** exclusions and browse for executable file (for example *Backup-tool.exe*), which will be excluded from scanning.
As soon as the *.exe* file is added to the exclusions, activity of this process is not monitored by ESET Mail Security and no scanning is run on any file operations performed by this process.

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



Add exclusion

Select process executable (*.exe):

C:\Program Files\Backup Tool\Backup-tool.exe

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

NOTE
Web access protection does not take into account this exclusion, so if you exclude the executable file of your web browser, downloaded files are still scanned. This way an infiltration can still be detected. This scenario is an example only, and we do not recommend you to create exclusions for web browsers.

Cloud-based protection

ESET LiveGrid® is an advanced early warning system comprised of several cloud-based technologies. It helps detect emerging threats based on reputation and improves scanning performance by means of whitelisting. New threat information is streamed in real-time to the cloud, which enables the ESET Malware Research Lab to provide timely response and consistent protection at all times. Users can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid®.

When installing ESET Mail Security, select one of the following options:

- You can decide not to enable ESET LiveGrid®. Your software will not lose any functionality, but in some cases ESET Mail Security may respond slower to new threats than detection engine database update.

- You can configure ESET LiveGrid® to submit anonymous information about new threats and where the new threatening code was detected. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

ESET LiveGrid® will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer‘s operating system.

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

Enable ESET LiveGrid® reputation system (recommended)

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

Enable ESET LiveGrid® feedback system

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

Submit crash reports and diagnostic data

Submit data such as crash reports, modules or memory dumps.

Submit anonymous statistics

Allow ESET to collect information about newly detected threats such as the threat name, date and time of detection, detection method and associated metadata, scanned files (hash, file name, origin of the file, telemetry), blocked and suspicious URL's, product version and configuration, including information about your system.

Contact email (optional)

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

⊟ Submission of samples

Automatic submission of infected samples

This will submit all infected samples to ESET for analysis and to improve future detection.

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

Automatic submission of suspicious samples

Suspicious samples resembling threats, and/or samples with unusual characteristics or behavior are submitted to ESET for analysis.

- **Executable** -Includes executable files: *.exe, .dll, .sys*
- **Archives** - Includes archive file types: *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- **Scripts** - Includes script file types: *.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *.js*, *.ps1*
- **Other** - Includes file types: *.jar*, *.reg*, *.msi*, *.swf*, *.lnk*
- **Possible Spam emails** - Improves global detection of spam.
- **Documents** - Includes Microsoft Office documents or PDF's with active content.

Exclusions

Click Edit option next to Exclusions in ESET LiveGrid® allows you to configure how threats are submitted to ESET Virus Labs for analysis.

Maximum size of samples (MB)

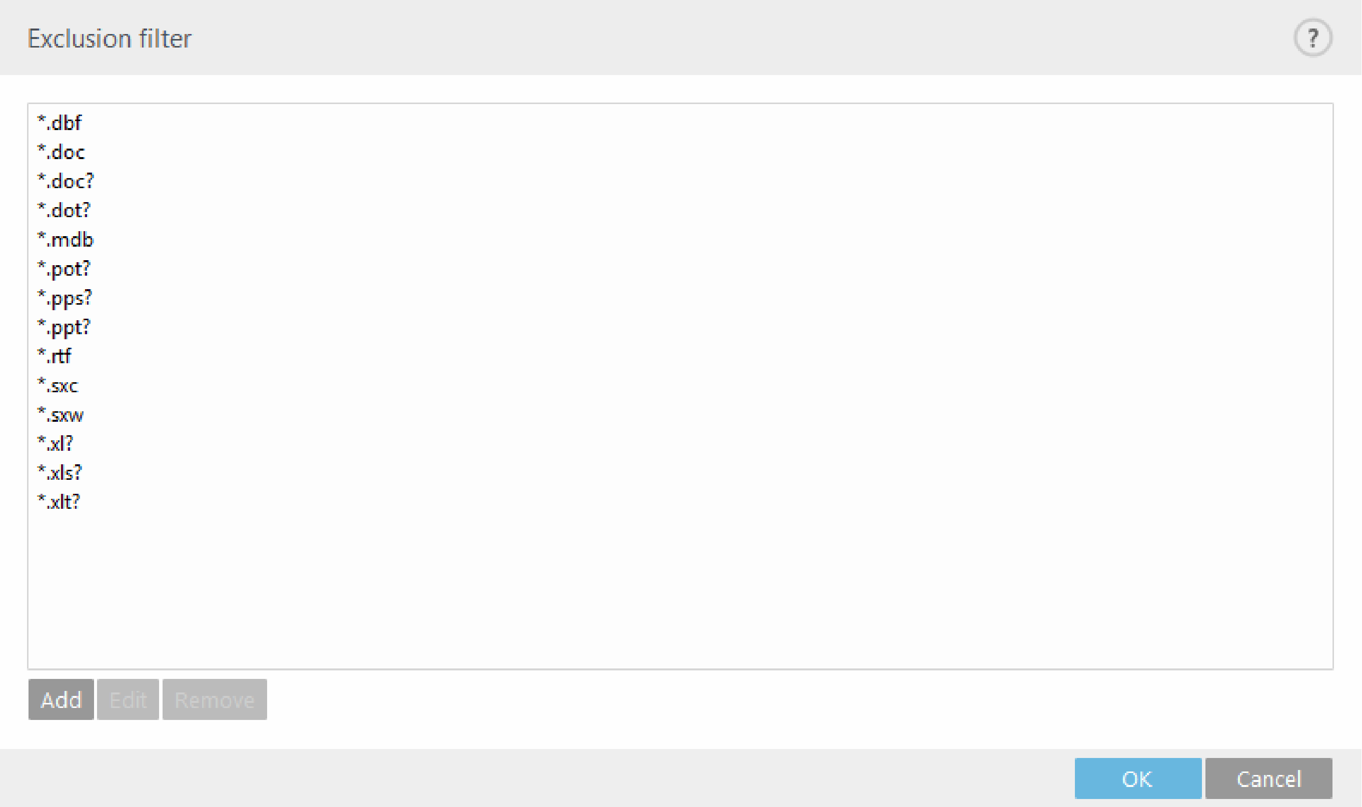
Define the maximum size of samples to be scanned.

ESET Dynamic Threat Defense

To enable ESET Dynamic Threat Defense service on a client machine using ESMC Web Console. In the ESET Security Management Center Web Console create a new policy or edit an existing one and assign it on machines where you want to use the ESET Dynamic Threat Defense.

Exclusion filter

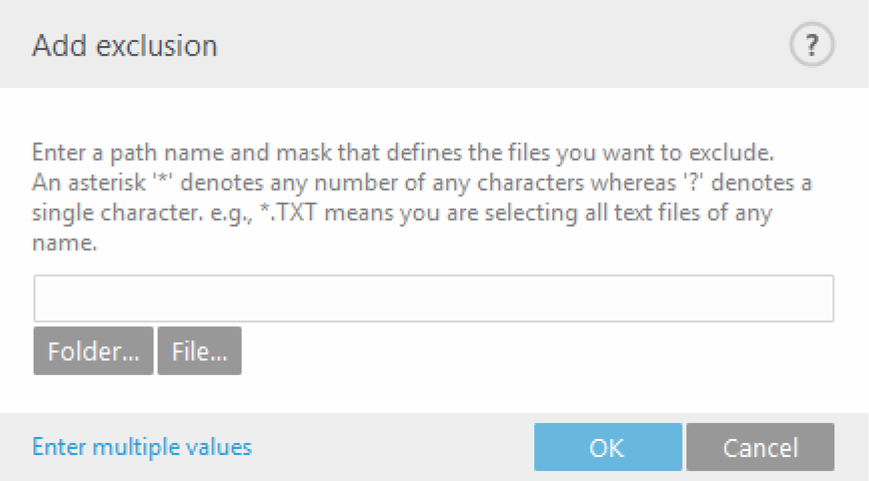
The Exclusion filter allows you to exclude certain files/folders from submission (for example, it may be useful to exclude files that may carry confidential information, such as documents or spreadsheets). The files listed will never be sent to ESET labs for analysis, even if they contain suspicious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



Exclusion filter

*.dbf
*.doc
*.doc?
*.dot?
*.mdb
*.pot?
*.pps?
*.ppt?
*.rtf
*.sxc
*.sxw
*.xl?
*.xls?
*.xlt?

If you have used ESET LiveGrid® before and have disabled it, there may still be data packages to send. Even after deactivating, such packages will be sent to ESET. Once all current information is sent, no further packages will be created.


Add exclusion

Enter a path name and mask that defines the files you want to exclude. An asterisk '*' denotes any number of any characters whereas '?' denotes a single character. e.g., *.TXT means you are selecting all text files of any name.

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

Malware scans

This section provides options to select scanning parameters.

> NOTE
> This scan profile selector applies to **On-demand scan** and Hyper-V scan.

Selected profile

A particular set of parameters used by the On-demand scanner. You can use one of the pre-defined scan profile or create a new profile. The scan profiles use different ThreatSense engine parameters.

List of profiles

To create a new one, click **Edit**. Type name for profile and click **Add**. New profile will be displayed in the **Selected profile** drop-down menu that lists existing scan profiles.

Scan targets

To scan a specific target, click **Edit** and choose an option from drop-down menu or selecting specific targets from the folder (tree) structure.

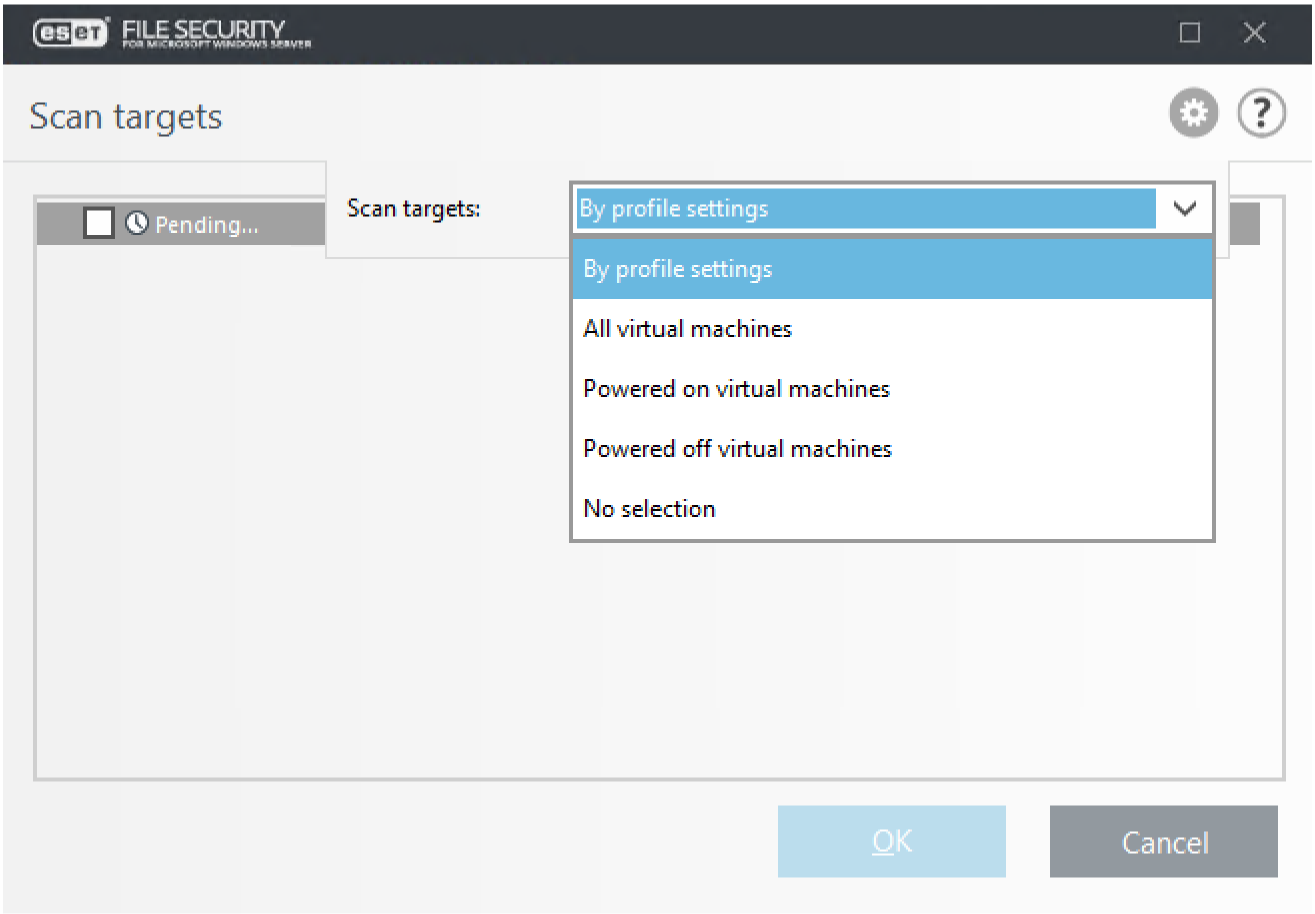
ThreatSense parameters

Modify scan parameters for the On-demand computer scanner.

On-Demand & Machine learning protection

Reporting is performed by detection engine and the machine learning component.

The **Hyper-V scan** pop-up window:



The **Scan targets** for **Hyper-V** drop-down menu allows you to select pre-defined scan targets:

By profile settings	**Selects targets set in the selected scan profile.**
All virtual machines	Selects all virtual machines.
Powered on virtual machines	Selects all online VMs.
Powered off virtual machines	Selects all offline VMs.
No selection	Clears all selections.

Click **Scan** to execute the scan using the custom parameters that you have set. After all scans are finished, check **Log files** > Hyper-V scan.

Profile manager

The **Scan profile** drop-down menu lets you select pre-defined scan profiles.

- **Smart scan**
- **Context menu scan**
- **In-depth scan**
- **My profile** (applies to Hyper-V scan, Update profiles)

To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

Profile manager is used in three places within ESET Mail Security.

On-demand computer scan

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

Update

The profile editor allows users to create new update profiles. It is only necessary to create custom update profiles if your computer uses multiple means to connect to update servers.

Hyper-V scan

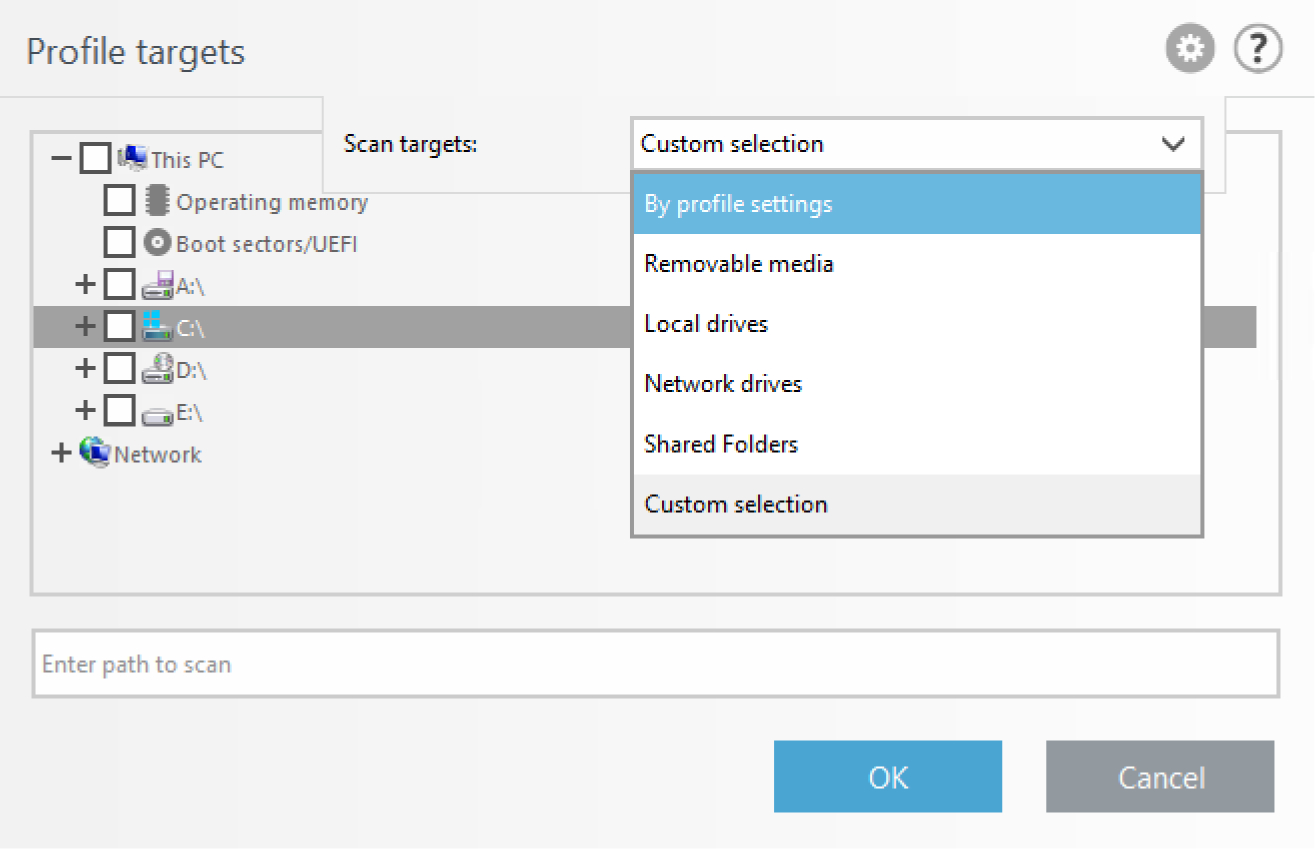
Create a new profile, select **Edit** next to **List of profiles**. New profile will be displayed in the **Selected profile** drop-down menu that lists existing scan profiles.

Profile targets

You can specify what will be scanned for infiltrations. Choose objects (memory, boot sectors and UEFI, drives, files and folders or network) from the tree structure that lists all available targets on your system.

> NOTE
> This scan profile selector applies to **On-demand scan** and Hyper-V scan.

Click the gear icon in the top-left corner to access the **Scan targets** and **Scan profile** drop-down menus.



Profile targets

Scan targets: Custom selection

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

By profile settings	Selects targets set in the selected scan profile.
Removable media	Selects diskettes, USB storage devices, CD/DVD.
Local drives	Selects all system hard drives.
Network drives	Selects all mapped network drives.
Shared Folders	Selects all folders on the local server that are shared.
Custom selection	Clears all selections. Ones cleared, you can make your custom selection.

To quickly navigate to a scan target (file or folder) in order to include it for scanning, enter its path into the text field below the tree structure. The path entry is case sensitive.

The **Scan profile** drop-down menu enables you to select pre-defined scan profiles:

- **Smart scan**
- **Context menu scan**
- **In-depth scan**

These scan profiles use different ThreatSense engine parameters.

Scan without cleaning

If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. This is useful when you only want to obtain an overview whether there are infected items and get details about these infections, if there are any. You can choose from three cleaning levels by clicking **Setup** > **ThreatSense parameters** > **Cleaning**. Information about scanning is saved to a scan log.

Ignore exclusions

When you select **Ignore exclusions**, it lets you perform a scan while ignoring exclusions that otherwise apply.

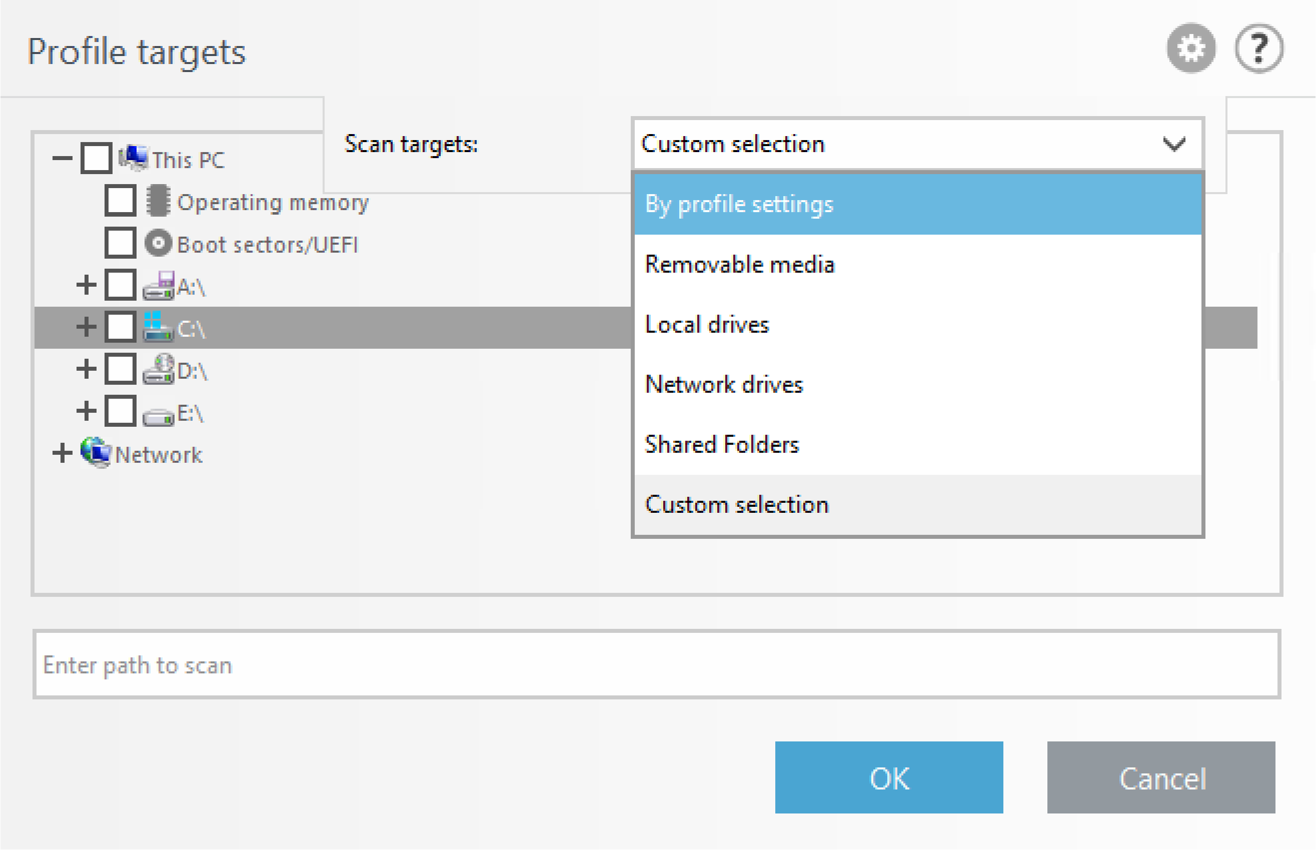
Scan targets

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

Scan targets profile selector applies to:

- On-demand scan
- Hyper-V scan

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



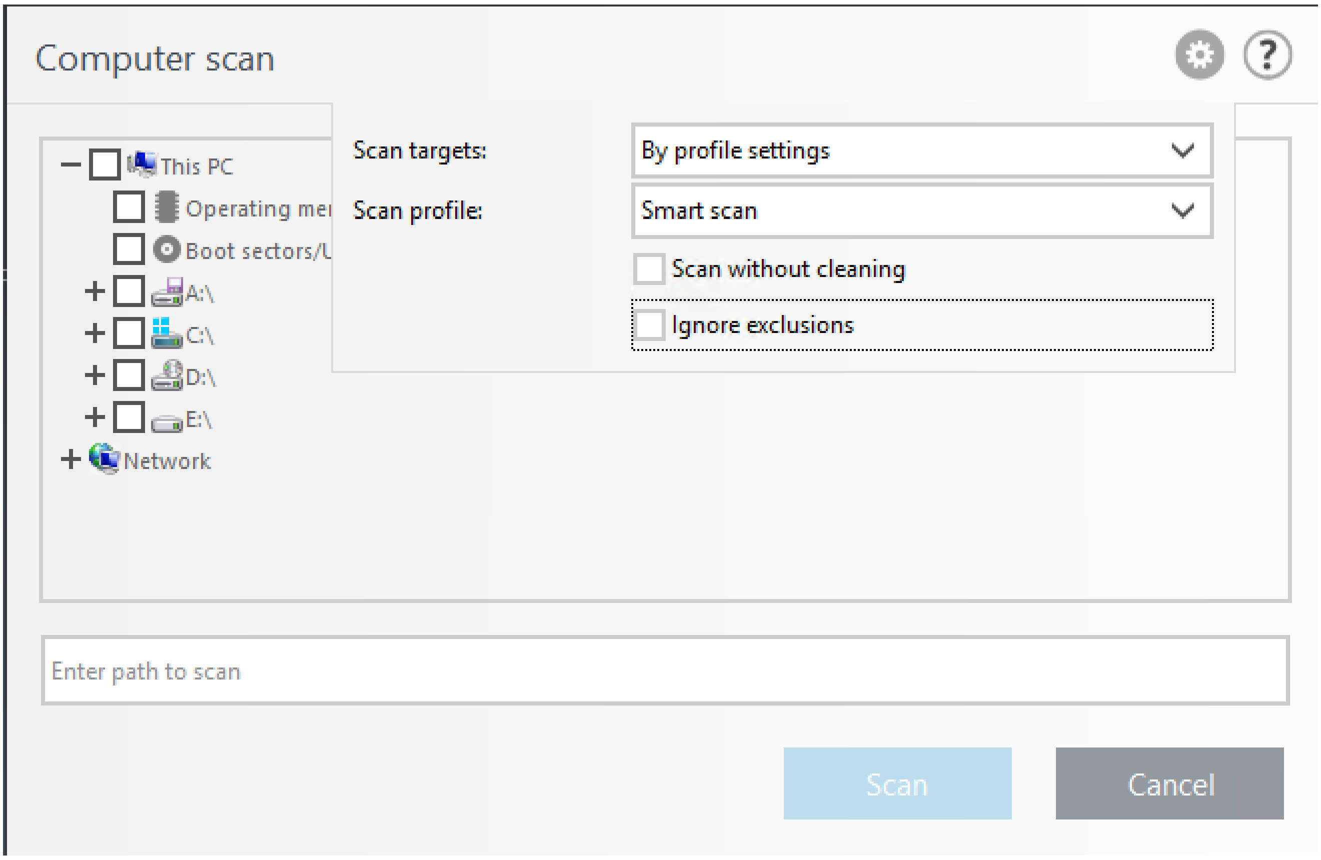
Scan targets: Custom selection

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

By profile settings	**Selects targets set in the selected scan profile.**
Removable media	Selects diskettes, USB storage devices, CD/DVD.
Local drives	Selects all system hard drives.
Network drives	Selects all mapped network drives.
Shared Folders	Selects all folders on the local server that are shared.
Custom selection	Clears all selections. Ones cleared, you can make your custom selection.

You can choose a profile from the **Scan** profile drop-down menu to be used for scanning chosen targets. The default profile is **Smart scan**. There are two more pre-defined scan profiles called **In-depth scan** and **Context menu scan**. These scan profiles use different ThreatSense engine parameters.

The **Custom scan** pop-up window:



Scan targets: By profile settings

Scan profile: Smart scan

□ Scan without cleaning

□ Ignore exclusions

Scan without cleaning

If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. This is useful when you only want to obtain an overview whether there are infected items and get details about these infections, if there are any. You can choose from three cleaning levels by clicking **Setup** > **ThreatSense parameters** > **Cleaning**. Information about scanning is saved to a scan log.

Ignore exclusions

You can perform a scan while ignoring exclusions that otherwise apply.

Scan

To execute the scan using the custom parameters that you have set.

Scan as Administrator

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

Idle-state scan

When the computer is in idle state, a silent computer scan is performed on all local drives. **Idle-state detection** will run when your computer is in the following states:

- **Turned off screen or screen saver**
- **Computer lock**

- **User logoff**

Run even if computer is powered from battery

By default, the Idle-state scanner will not run when the computer (notebook) is operating on battery power.

Enable logging

To record a computer scan output in the Log files section (from the main program window click Log files and select log type Computer scan from the drop-down menu).

ThreatSense parameters

Modify scan parameters for the Idle-state scanner.

Startup scan

By default, the automatic startup file check will be performed on system start (user logon) and after a successful module update. This scan is controlled by the Scheduler configuration and tasks.

Startup scan options are a part of the **System startup file check** scheduler task.

To modify Startup scan settings, navigate to **Tools** > **Scheduler**, select one of the tasks named **Automatic startup file check** (user logon or module update) and click **Edit**. Click through the wizard and in the last step, you can modify detailed options of the Automatic startup file check.

Automatic startup file check

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

The Scan target drop-down menu specifies the scan depth for files run at system startup. Files are arranged in ascending order according to the following criteria:

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

Two specific Scan target groups are also included:

Files run before user logon

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

Files run after user logon

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

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

Scan priority

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

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

Removable media

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

Action to take after inserting removable media

Select which action will be performed when a removable media device is inserted into the computer (CD/DVD/USB).

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

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

- **Scan now** - This will trigger a scan of removable media.
- **Scan later** - Scanning of removable media will be postponed.
- **Setup** - Opens Advanced setup.
- **Always use the selected option** - When selected, the same action will be performed when removable media is inserted another time.

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

Document protection

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

Integrate into system

This option enhances the protection of Microsoft Office documents (not required under normal circumstances).

ThreatSense parameters

Modify parameters for the Document protection.

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

Hyper-V scan

Current version of Hyper-V scan supports scanning of online or offline virtual system in Hyper-V. Supported types of scanning according to hosted Windows Hyper-V system and state of virtual system are shown here:

Virtual systems with Hyper-V feature	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V
Online VM	no scan	read-only	read-only	read-only	read-only
Offline VM	read-only/cleaning	read-only/cleaning	read-only/cleaning	read-only/cleaning	read-only/cleaning

Hardware requirements

The server should have no performance issues running Virtual Machines. Scanning activity primarily uses CPU resources. To scan online VMs, free disk space is required. Disk space must be at least double the space used by checkpoints/snapshots and virtual disks.

Specific limitations

- Scanning on RAID storage, Spanned Volumes and Dynamic Disks are not supported due to the nature of Dynamic Disks. Therefore, we recommend that you avoid using the Dynamic Disk type in your VMs if possible.
- Scanning is always performed on the current VM and does not affect checkpoints or snapshots.
- Hyper-V running on a host in a cluster is currently not supported by ESET Mail Security.
- Virtual Machines on a Hyper-V host running on Windows Server 2008 R2 SP1 can only be scanned in read-only mode (No cleaning), regardless of what cleaning level is selected in ThreatSense parameters.

NOTE
While ESET Security supports the scan of virtual disk MBRs, read-only scanning is the only method supported for these targets. This setting can be changed in **Advanced setup** (**F5**) > **Computer** > **Hyper-V scan** > ThreatSense parameters > **Boot sectors**.

Virtual Machine to be scanned is "offline" - switched Off state

ESET Mail Security uses Hyper-V Management to detect and to connect to virtual disks. This way, ESET Mail Security has the same access to the content of the virtual disks it does when accessing data and files on any generic drive.

Virtual Machine to be scanned is "online" - Running, Paused, Saved state

ESET Mail Security uses Hyper-V Management to detect virtual disks. Actual connection to these the disks is not possible. Therefore, ESET Mail Security creates a checkpoint/snapshot of the Virtual Machine, then connects to the checkpoint/snapshot. Once the scan is completed, the checkpoint/snapshot is deleted. This means that read-only scan can be performed because the running Virtual Machine(s) are unaffected by scan activity.

Allow up to one minute for ESET Mail Security to create a snapshot or checkpoint during scanning. You should take this into account when running a Hyper-V scan on a larger number of Virtual Machines.

Naming convention

The module of Hyper-V Scan uses the following naming convention:

```
VirtualMachineName\DiskX\VolumeY
```

Where X is the number of disks and Y is the number of volumes. For example:

```
Computer\Disk0\Volume1
```

The number suffix is added based on the order of detection, and is identical to the order seen in the Disk Manager of the VM. This naming convention is used in the tree-structured list of targets to be scanned, in the progress bar and also in the log files.

Executing a scan

- On-demand - Click **Hyper-V Scan** to view a list of Virtual Machines and volumes available for scanning. Select the Virtual Machine(s), disk(s) or volume(s) you want to scan and click **Scan**.
- To create a scheduler task.
- Via ESET Security Management Center as a Client Task called Server Scan.
- Hyper-V scan can be managed and started via eShell.

It is possible to execute several Hyper-V scans simultaneously. You will receive a notification with a link to log files when a scan is complete.

Possible issues

- When executing the scan of an online Virtual Machine, a checkpoint/snapshot of the particular Virtual Machine has to be created and during the creation of a checkpoint/snapshot some generic actions of the Virtual Machine might be limited or disabled.
- If an offline Virtual Machine is being scanned, it cannot be turned on until the scan is finished.
- Hyper-V Manager allows you to name two different Virtual Machines identically and this presents an issue when trying to differentiate the machines while reviewing the scan logs.

HIPS

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

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

Enable Self-Defense

ESET Mail Security has built-in Self-defense technology that prevents malicious software from corrupting or disabling your malware protection, so you can be sure your system is protected at all times. Changes to the Enable HIPS and Enable SD (Self-Defense) settings take effect after the Windows operating system is restarted. Disabling the entire HIPS system will also require a computer restart.

Enable Protected Service

Microsoft has introduced a concept of protected services with Microsoft Windows Server 2012 R2. It prevents a service against malware attacks. Kernel of ESET Mail Security is running as a protected service by default. This feature is available on Microsoft Windows Server 2012 R2 and newer server operating systems.

Enable Advanced Memory Scanner

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

Enable Exploit Blocker

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

Enable Ransomware shield

To use this functionality enable HIPS and ESET Live Grid. Read more about Ransomware in the glossary.

Filtering mode

You can choose one of the following filtering modes:

- **Automatic mode** - Operations are enabled with the exception of those blocked by pre-defined rules that protect your system. Everything is allowed except actions denied by rule.
- **Smart mode** - The user will only be notified about very suspicious events.
- **Interactive mode** - The user will be prompted to confirm operations. Allow / deny access, Create rule, Temporarily remember this action.

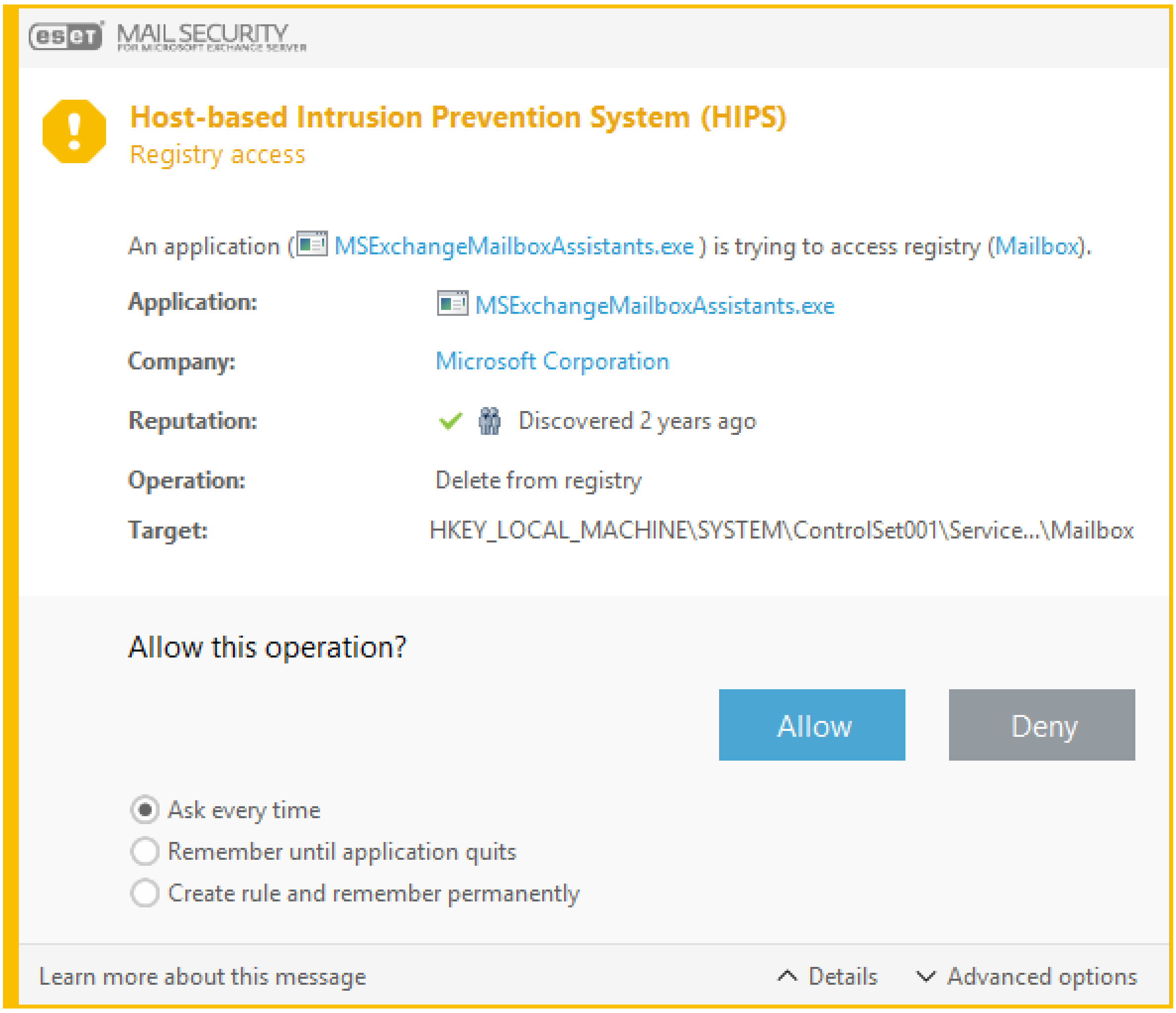
- **Policy-based mode** - Operations are blocked. Accepts only user/pre-defined rules.

- **Learning mode** - Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the Rule editor, but their priority is lower than the priority of rules created manually or rules created in automatic mode. When you select **Learning mode** from the HIPS Filtering mode drop-down menu, the **Learning mode will end at** setting will become available. Select the duration for which you want to engage learning mode (the maximum duration is 14 days). When the specified duration has passed, you will be prompted to edit the rules created by HIPS while it was in learning mode. You can also choose a different filtering mode, or postpone the decision and continue using learning mode.

Rules

Rules determine which applications will be granted access to which files, parts of registry or other applications. The HIPS system monitors events inside the operating system and reacts accordingly based on rules similar to the rules used by the personal firewall. Click Edit to open the HIPS rule management window. If the default action for a rule is set to **Ask**, a dialog window will be displayed each time that the rule is triggered. You can choose to **Block** or **Allow** the operation. If you do not choose an action in the given time, a new action is selected based on the rules.

The dialog window allows you to create a rule based on any new action that HIPS detects and then define the conditions under which to **Allow** or **Block** that action. Click **Details** to see further information. Rules created like this are considered equal to rules created manually, so a rule created from a dialog window can be less specific than the rule that triggered that dialog window. This means that after creating such a rule, the same operation can trigger the same window.



Host-based Intrusion Prevention System (HIPS)
Registry access

An application (MSExchangeMailboxAssistants.exe) is trying to access registry (Mailbox).

Application:	MSExchangeMailboxAssistants.exe
Company:	Microsoft Corporation
Reputation:	✓ Discovered 2 years ago
Operation:	Delete from registry
Target:	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Service...\Mailbox

Allow this operation?

● Ask every time
○ Remember until application quits
○ Create rule and remember permanently

Ask every time

Dialog window will be displayed each time that the rule is triggered. You can choose to **Deny** or **Allow** the operation.

Remember until application quits

Choosing an action **Deny** or **Allow** will create a temporary HIPS rule that will be used until the application in question is closed. Also, if you change filtering mode, modify rules, or when HIPS module is updated, and if you restart the system, temporary rules will be deleted.

Create rule and remember permanently

Create a new HIPS rule. You can later modify this rule in the HIPS rule management section.

HIPS rule settings

This window gives you an overview of existing HIPS rules.

Rule	User-defined or automatically chosen rule name.
Enabled	Deactivate this switch if you want to keep the rule in the list but do not want to use it.
Action	The rule specifies an action – **Allow**, **Block** or **Ask** – that should be performed if the conditions are right.
Sources	The rule will be used only if the event is triggered by an application(s).
Targets	The rule will be used only if the operation is related to a specific file, application or registry entry.
Log severity	If you activate this option, information about this rule will be written to the HIPS log.
Notify	A small pop-up window appears in the lower-right corner if an event is triggered.

Create a new rule, click **Add** new HIPS rules or **Edit** selected entries.

Rule name

User-defined or automatically chosen rule name.

Action

The rule specifies an action **Allow**, **Block** or **Ask** that should be performed if the conditions are right.

Operations affecting

You must select the type of operation for which the rule will be applied. The rule will be used only for this type of operation and for the selected target. The rule consists of parts that describe the conditions triggering this rule.

Source applications

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

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

Descriptions of important operations:

File operations:

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

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

Application operations:

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

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

Registry operations:

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

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

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

WARNING
You may receive a notification if you create an overly generic rule.

HIPS advanced settings

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

Drivers always allowed to load

Selected drivers are always allowed to load regardless of configured filtering mode, unless explicitly blocked by user rule. Drivers shown in this list will always be allowed to load regardless of HIPS filtering mode, unless explicitly blocked by user rule. You can **Add** new driver, **Edit** or **Delete** selected driver from the list.

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

Log all blocked operations

All blocked operations will be written to the HIPS log.

Notify when changes occur in Startup applications

Displays a desktop notification each time an application is added to or removed from system startup.

Update configuration

This section specifies update source information like the update servers being used and authentication data for these servers.

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

⊟ Basic

Select default update profile

Choose existing or create new profile that will be applied by default for updates.

Clear update cache

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

Set maximum detection engine age automatically / Maximum detection engine age (days)

Allows you to set maximum days after which the detection engine age will be reported as out of date. The default value is 7.

Module Rollback

If you suspect that a new update of detection engine and/or program modules may be unstable or corrupt, you can rollback to the previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely. ESET Mail Security records snapshots of detection engine and program modules for use with the Rollback feature. In order to create detection engine snapshots, leave **Create snapshots of modules enabled**.

Number of locally stored snapshots

Defines the number of previous module snapshots stored.

⊟ Profiles

To create a custom update profile, select **Edit** next to **List of profiles**, enter your own **Profile name** and click **Add**. **Select profile to edit** and modify parameters for **module updates** types or create an **Update mirror**.

⊟ Updates

Select the type of update to use from the drop-down menu:

- **Regular update** - By default, the Update type is set to Regular update to ensure that update files will automatically be downloaded from the ESET server with the least network traffic.
- **Pre-release update** - Are updates that have gone through thorough internal testing and will be available

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

- **Delayed update** - Allows updating from special update servers providing new versions of virus databases with a delay of at least X hours (that is, databases tested in a real environment and therefore considered as stable).

Ask before downloading update

When a new update is available, you will be prompted before downloading it.

Ask if an update file size is greater than (KB)

If the update file size is greater than the value specified in the field, a notification will be displayed.

Disable notification about successful update

Turns off the system tray notification at the bottom right corner of the screen. It is useful to select this option if a full-screen application is running. Note that Presentation mode will turn off all notifications.

Modules updates

Module updates are set to **Choose automatically** by default. The update server is the location where updates are stored. If you use an ESET server, we recommend that you leave the default option selected.

When using a local HTTP server - also known as a Mirror - the update server should be set as follows: *http://computer_name_or_its_IP_address:2221*
When using a local HTTP server with SSL - the update server should be set as follows: *https://computer_name_or_its_IP_address:2221*
When using a local shared folder - the update server should be set as follows: *\\computer_name_or_its_IP_address\shared_folder*

Enable more frequent updates of detection signatures

Detection engine will be updated in shorter intervals. Disabling this option may negatively impact detection rate.

Allow module updates from removable media

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

Program component update

Use the **Update mode** drop-down menu to choose how ESET Mail Security component updates are applied when a new update is available. Component updates usually modify existing features, but may also include new features. Depending on chosen update mode, the component update can be performed automatically without an intervention or confirmation. Alternatively, you can choose to be notified before the updates are installed. A server restart may be required after the component update. The following update modes are available:

- **Ask before update** - You will be prompted to confirm or refuse product updates when they are available. This is the default option. A server restart may be required after the component update.

- **Auto-update** - Component updates will be downloaded and installed automatically. Keep in mind that server restart may be required.

- **Never update** - Component updates will not be performed at all. We recommend you this option because it enables you to run the component updates manually and restart your server during scheduled maintenance window.

IMPORTANT
Auto-update mode restarts your server automatically after the component update has been completed.

⊟ Connection options

Proxy Server

To access the proxy server setup options for a given update profile, click the **Proxy mode** and select one of the three following options:

- **Do not use proxy server** - No proxy server will be used by ESET Mail Security when performing updates.

- **Use global proxy server settings** - Proxy server configuration specified in the **Advanced setup** (**F5**)> **Tools** > Proxy server will be used.

- **Connection through a proxy server** - Use this option if:

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

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

Use direct connection if proxy is not available

If a product is configured to utilize HTTP Proxy and the proxy is unreachable, the product will bypass the proxy and communicate directly with ESET servers.

Windows shares

When updating from a local server running Windows, authentication for each network connection is required by default.

Connect to LAN as

To configure your account, select one of the following options:

- **System account (default)** - Use the system account for authentication. Typically, no authentication process takes place if there is no authentication data supplied in the main update setup section.

- **Current user** - Select this option to ensure that the program authenticates using the currently logged-in user account. 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.

- **Specified user** - Select this option to use a specific user account for authentication. Use this method when the default system account connection fails. Be aware that the specified user account must have access to the update files directory on the local server. If the user does not have access, the program will not be able to establish a connection or download updates.

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

Disconnect from server after update

To force a disconnect if a connection to the server remains active even after updates have been downloaded.

⊟ Update mirror

Configuration options for the local Mirror server are located in the **Advanced setup** (**F5**) in the **Update** > **Profiles** > Update Mirror tab.

Update rollback

If you click **Rollback**, you have to select a time interval from the drop-down menu that represents the period of time that the detection engine database and program module updates will be paused.

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

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

Scheduled Task - Update

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

EXAMPLE
The steps below will walk you through a task to edit existing **Regular automatic update**.
1.In the main **Scheduler** screen, select task **Update** with name **Regular automatic update** and click **Edit** the configuration wizard will be open.
2.Set the scheduler task to run, select one of the following timing options to define when you want the scheduled task to run.
3.If you want to prevent the task from being executed when the system is running on battery power (for example UPS), click the switch next to **Skip task when running on battery power**.
4.Select update profile to use for update. Select an action to perform if the scheduled task execution fails for any reason.
5.Click **Finish** to apply the task.

Update mirror

Open ESET Mail Security
Press F5 > Update > Profiles > Update mirror

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

⊟ Update mirror

Create update mirror

Activates mirror configuration options.

Storage folder

Click **Clear** if you want to change a defined default folder to store mirrored files *C:\ProgramData\ESET\ESET Security\mirror.* Click **Edit** to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be entered in the Username and Password fields. If the selected destination folder is located on a network disk running the Windows NT/2000/XP operating system, the username and password specified must have write privileges for the selected folder.
The username and password should be entered in the format *Domain/User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

Program component update

Files

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

Update components automatically

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

Update components now

Updates your program components to the latest version.

⊟ HTTP server

Server port

Default port is set to 2221. Change this value if you are using different port.

Authentication

Defines the method of authentication used for accessing update files. The following options are available: **None**, **Basic** and **NTLM**.

- Select **Basic** to use base64 encoding with basic username and password authentication.
- The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used.
- The default setting is **None**, which grants access to the update files with no need for authentication.

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

SSL for HTTP server

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

⊟ Connection options

Windows shares

When updating from a local server running Windows, authentication for each network connection is required by default.

Connect to LAN as

To configure your account, select one of the following options:

- **System account (default)** - 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.

- **Current user** - Select this to ensure that the program authenticates using the currently logged-in user account. 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.

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

WARNING

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

Disconnect from server after update

To force a disconnect if a connection to the server remains active even after updates have been downloaded.

Network protection

Enable Network attack protection (IDS)

Allows you to configure access to some of the services running on your computer from the Trusted zone and enable/disable detection of several types of attacks and exploits that might be used to harm your computer.

Enable Botnet protection

Detects and blocks communication with malicious command and control servers based on typical patterns when the computer is infected and a bot is attempting to communicate

IDS exceptions

You can think of Intrusion Detection System (IDS) exceptions as network protection rules. Click edit to define IDS exceptions.

Intrusion detection:

Protocol SMB - Detects and blocks various security problems in SMB protocol
Protocol RPC - Detects and blocks various CVEs in the remote procedure call system developed for the Distributed Computing Environment (DCE).
Protocol RDP - Detects and blocks various CVEs in the RDP protocol (see above).
Block unsafe address after attack detection - IP addresses that have been detected as sources of attacks are added to the Blacklist to prevent connection for a certain period of time.
Display notification after attack detection - Turns on the system tray notification at the bottom right corner of the screen.
Display notifications also for incoming attacks against security holes - Alerts you if attacks against security holes are detected or if an attempt is made by a threat to enter the system this way.

Packet inspection:

Allow incoming connection to admin shares in SMB protocol - The administrative shares (admin shares) are the default network shares that share hard drive partitions (C$, D$, ...) in the system together with the system folder (ADMIN$). Disabling connection to admin shares should mitigate many security risks. For example, the Conficker worm performs dictionary attacks in order to connect to admin shares.
Deny old (unsupported) SMB dialects - Deny SMB sessions that use an old SMB dialect unsupported by IDS. Modern Windows operating systems support old SMB dialects due to backward compatibility with old operating systems such as Windows 95. The attacker can use an old dialect in an SMB session in order to evade traffic inspection. Deny old SMB dialects if your computer does not need to share files (or use SMB communication in general) with a computer with an old version of Windows.
Deny SMB sessions without extended security - Extended security can be used during the SMB session negotiation in order to provide a more secure authentication mechanism than LAN Manager Challenge/Response (LM) authentication. The LM scheme is considered weak and is not recommended for use.
Allow communication with the Security Account Manager service - For more information about this service see [MS-SAMR].
Allow communication with the Local Security Authority service - For more information about this service see [MS-LSAD] and [MS-LSAT].
Allow communication with the Remote Registry service - For more information about this service see [MS-RRP].
Allow communication with the Service Control Manager service - For more information about this service see [MS-SCMR].
Allow communication with the Server service - For information about this service see [MS-SRVS].
Allow communication with the other services - Other MSRPC services.

IDS exceptions

Intrusion Detection System (IDS) exceptions are essentially network protection rules. The exceptions are evaluated from top to bottom. IDS exceptions editor allows you to customize network protection behavior upon various IDS exceptions. First matching exception is applied, for each action type (Block, Notify, Log) separately. **Top**/**Up**/**Down**/**Bottom** allows you to adjust the priority level of exceptions. To create a new IDS exception, click **Add**. Click **Edit** to modify an existing IDS exception, or **Delete** to remove it.

Choose **Alert** type from the drop-down list. Specify the **Threat name** and **Direction**. Browse for an **Application** you want to create the exception for. Specify a list of IP addresses (IPv4 or IPv6) or subnets. For multiple entries use comma as a delimiter.

Configure **Action** for IDS exception by selecting one of the options from the drop-down menu (**Default**, **Yes**, **No**). Do this for each Action type (**Block**, **Notify**, **Log**).

> EXAMPLE
> If want a notification to be displayed in case of an IDS exception alert, as well as have the time of the event logged, leave the **Block** action type **Default** and for the other two action types (**Notify** and **Log**) choose **Yes** from the drop-down menu.

Temporary IP address blacklist

View a list of IP addresses that have been detected as the source of attacks and added to the blacklist to block connections for a certain period of time. Shows **IP address** that have been locked.

Block reason

Shows type of attack that has been prevented from the address (for example TCP Port Scanning attack).

Timeout

Shows time and date when the address will expire from the blacklist.

Remove / Remove all

Removes selected IP address from the temporary blacklist before it will expire or removes all addresses from the blacklist immediately.

Add exception

Adds a firewall exception into IDS filtering for selected IP address.

Web and email

You can configure protocol filtering, Email client protection, Web access protection and Anti-phishing to protect your server during internet communication.

Email client protection

Controls all email communication, protects against malicious code and lets you choose the action taken when an infection is detected.

Web access protection

Monitors the communication between web browsers and remote servers and complies with the HTTP and HTTPS rules. This feature also allows you to block, allow or exclude certain URL addresses.

Protocol filtering

Offers advanced protection for application protocols and it is provided by the ThreatSense scanning engine. This control works automatically, regardless of whether a web browser or an email client is used. It also works for encrypted (SSL/TLS) communication.

Anti-Phishing protection

Allows you to block web pages known to distribute phishing content.

Protocol filtering

Malware protection for application protocols is provided by the ThreatSense scanning engine, which integrates multiple advanced malware scanning techniques. Protocol filtering works automatically, regardless of the Internet browser or email client used. If protocol filtering is enabled, ESET Mail Security will be checking communications that uses the SSL/TLS protocol, go to **Web and email** > SSL/TLS.

Enable application protocol content filtering

If you disable protocol filtering, note that many ESET Mail Security components (**Web access protection**, **Email protocols protection** and **Anti-Phishing protection**) depend on it and not all their features will be available.

Excluded applications

To exclude the communication of specific network-aware applications from content filtering, select them in the list. HTTP/POP3 communication of the selected applications will not be checked for threats. Enables you to exclude specific applications from protocol filtering. Click **Edit** and **Add** to select an executable from the list of applications to exclude it from protocol filtering.

IMPORTANT
We recommend only using this option for applications that do not work properly with their communication being checked.

Excluded IP addresses

Allows you to exclude specific remote addresses from protocol filtering. IP addresses in this list will be excluded from protocol content filtering. HTTP/POP3/IMAP communication from/to the selected addresses will not be checked for threats.

IMPORTANT
We recommend that you only use this option for addresses that are known to be trustworthy.

Click **Edit** and **Add** to specify IP address, address range or subnet to which the exclusion will be applied. When you select **Enter multiple values**, you can add multiple IP addresses delimited by newlines, commas or semicolons. When multiple selection is enabled, addresses will be shown in the list of excluded IP addresses.

NOTE
Exclusions are useful when protocol filtering causes compatibility issues.

Web and email clients

Because of the enormous amount of malicious code circulating the Internet, safe Internet browsing is a very important aspect of computer protection. Web browser vulnerabilities and fraudulent links help malicious code enter the system unnoticed, which is why ESET Mail Security focuses on web browser security. Each application accessing the network can be marked as an Internet browser. Applications that already use protocols for communication or applications from selected paths can be added to the list of Web and email clients.

SSL/TLS

ESET Mail Security is capable of checking for threats in communications that use the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol.

You can use various scanning modes to examine SSL protected communications with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Enable SSL/TLS protocol filtering

If protocol filtering is disabled, the program will not scan communications over SSL/TLS. The Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol filtering mode is available in following options:

- **Automatic mode** - Select this option to scan all SSL/TLS protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked as trusted (it is on the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.
- **Interactive mode** - If you enter a new SSL/TLS protected site (with an unknown certificate), an action selection dialog is displayed. This mode allows you to create a list of SSL/TLS certificates that will be excluded from scanning.
- **Policy mode** - All SSL/TLS connections are filtered, except configured exclusions.

List of SSL/TLS filtered application

Add filtered application and set one of the scan actions. The List of SSL/TLS filtered applications can be used to customize ESET Mail Security behavior for specific applications, and to remember actions chosen if **Interactive mode** is selected in **SSL/TLS protocol filtering mode**.

List of known certificates

Allows you to customize ESET Mail Security behavior for specific SSL certificates. The list can be viewed and managed by clicking Edit next to **List of known certificates**.

Exclude communication with trusted domains

To exclude communication using Extended validation certificates from protocol checking (internet banking).

Block encrypted communication utilizing the obsolete protocol SSL v2

Communication using this earlier version of the SSL protocol will automatically be blocked.

Root certificate

For SSL/TLS communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET be added to the list of known root certificates (publishers). Add the root certificate to known browsers should be enabled. Select this option to automatically add the ESET root certificate to known browsers (for example, Opera and Firefox). For browsers using the system certification store, the certificate is added automatically (for example, in Internet Explorer).

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

Certificate validity

If the certificate cannot be verified using the TRCA certificate store

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

If the certificate is invalid or corrupt

This means that the certificate expired or was incorrectly signed. In this case, we recommend that you leave **Block communication that uses the certificate** selected.

List of known certificates

To customize ESET Mail Security behavior for specific Secure Sockets Layer (SSL) / Transport Layer Security (TLS) certificates, and to remember actions chosen if **Interactive mode** is selected in SSL/TLS protocol filtering mode. You can configure selected certificate or **Add** a certificate from a URL or File. Once you are in Add certificate window, click URL or File and specify the certificate URL or browse for a certificate file. The following fields will automatically be filled using data from the certificate:

- **Certificate name** - name of the certificate.
- **Certificate issuer** - name of the certificate creator.
- **Certificate subject** - the subject field identifies the entity associated with the public key stored in the subject public key field.

Access action

- **Auto** - to allow trusted certificates and ask for untrusted ones.
- **Allow or Block** - to allow/block communication secured by this certificate regardless of its trustworthiness.
- **Ask** - to receive a prompt when a specific certificate is encountered.

Scan action

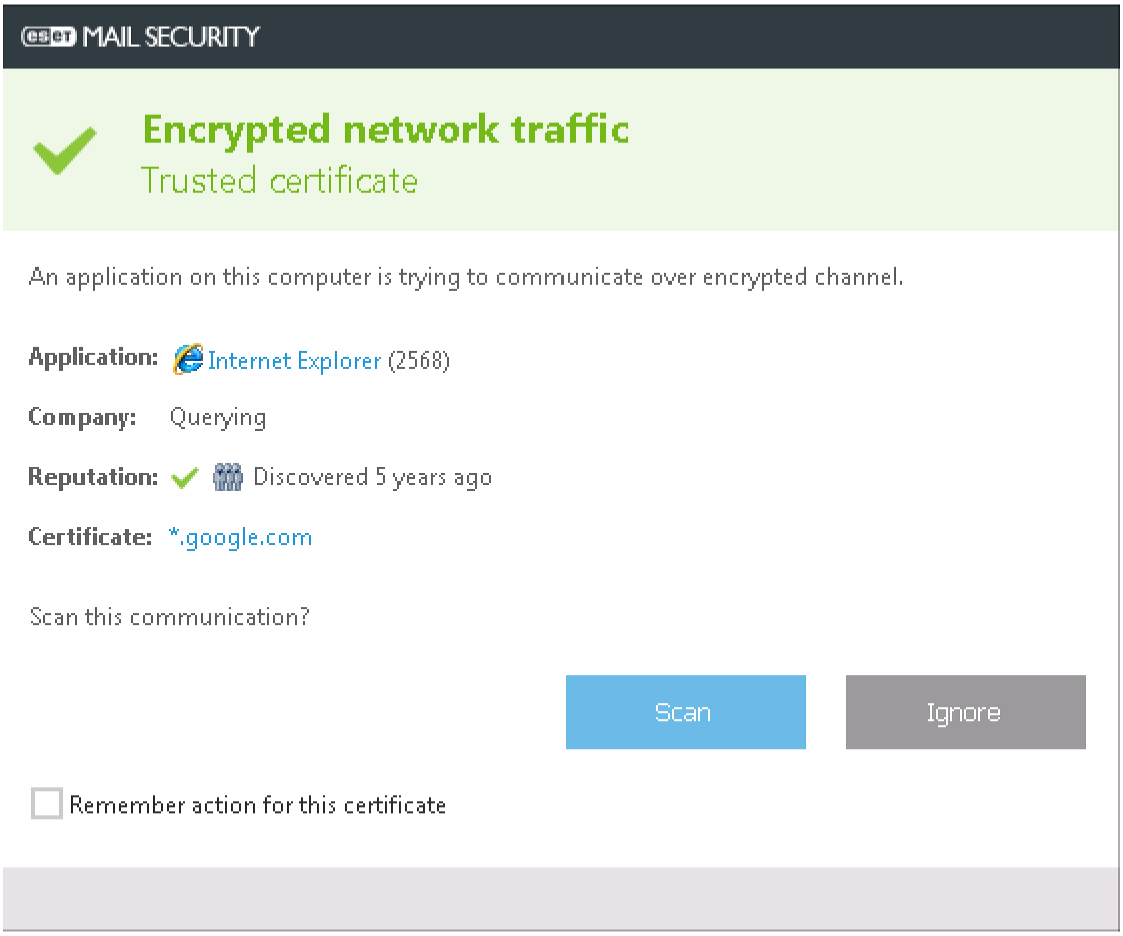
- **Auto** - to scan in automatic mode and ask in interactive mode.
- **Scan or Ignore** - to scan or ignore communication secured by this certificate.
- **Ask** - receive a prompt when a specific certificate is encountered.

Encrypted SSL communication

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

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

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



Encrypted network traffic
Trusted certificate

An application on this computer is trying to communicate over encrypted channel.

Application: Internet Explorer (2568)

Company: Querying

Reputation: ✓ Discovered 5 years ago

Certificate: *.google.com

Scan this communication?

□ Remember action for this certificate

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

Email client protection

Integration of ESET Mail Security with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, integration can be enabled in ESET Mail Security. When integration is activated, the ESET Mail Security toolbar is inserted directly into the email client (toolbar for newer versions of Windows Live Mail is not inserted), allowing for more efficient email protection.

Email client integration

Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. Email protection works as a plug-in for these programs. The main advantage of the plug-in is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. Even if integration is not enabled, email communication is still protected by the email client protection module (POP3, IMAP). For a complete list of supported email clients and their versions, refer to the following Knowledgebase article.

Disable checking upon inbox content change

If you are experiencing a system slowdown when working with your email client (MS Outlook only). This may occur when retrieving an email from the Kerio Outlook Connector Store, for example.

Enable email protection by client plugins

Lets you disable email client protection without removing integration into your email client. You can disable all plugins at once, or disable selectively the following:

- **Received email** - Toggles checking of received messages.
- **Sent email** - Toggles checking of sent messages.
- **Read email** - Toggles checking of read messages.

Action to be performed on infected email

- **No action** - If enabled, the program will identify infected attachments, but will leave emails without taking any action.
- **Delete email** - The program will notify the user about infiltration(s) and delete the message.
- **Move email to the Deleted items folder** - Infected emails will be moved automatically to the Deleted items folder.
- **Move email to the folder** - Infected emails will be moved automatically to the specified folder.
- **Folder** - Specify the custom folder where you want to move infected emails when detected.

Repeat scan after update

Toggles rescanning after a detection engine update.

Accept scan results from other modules

If this is selected, the email protection module accepts scan results of other protection modules (POP3, IMAP protocols scanning).

Email protocols

Enable email protection by protocol filtering

The IMAP and POP3 protocols are the most widespread protocols used to receive email communication in an email client application. ESET Mail Security provides protection for these protocols regardless of the email client used.

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

IMAPS / POP3S scanner setup

Encrypted communications will not be scanned when default settings are in use. To enable the scanning of encrypted communication, navigate to SSL/TLS protocol checking.

The port number identifies what type of port it is. Here are the default email ports for:

Port name	Port numbers	Description
POP3	110	Default POP3 non-encrypted port.
IMAP	143	Default IMAP non-encrypted port.
Secure IMAP (IMAP4-SSL)	585	Enable SSL/TLS protocol filtering. Multiple port numbers must be delimited by a comma.
IMAP4 over SSL (IMAPS)	993	Enable SSL/TLS protocol filtering. Multiple port numbers must be delimited by a comma.
Secure POP3 (SSL-POP)	995	Enable SSL/TLS protocol filtering. Multiple port numbers must be delimited by a comma.

Alerts and notifications

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

After an email has been checked, a notification with the scan result can be appended to the message. You can elect to **Append tag messages to received and read mail**, **Append note to the subject of received and read infected email** or **Append tag messages to sent email**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The available options are:

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

Append note to the subject of sent infected email

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

Template added to the subject of infected email

Edit this template if you wish to modify the subject prefix format of an infected email. This function will replace the message subject `Hello` with a given prefix value `[virus]` to the following format: `[virus] Hello`. The variable `%VIRUSNAME%` represents the detected threat.

MS Outlook toolbar

Microsoft Outlook protection works as a plug-in module. After ESET Mail Security is installed, this toolbar containing the malware protection options is added to Microsoft Outlook:

ESET Mail Security

Click on **icon** opens the main program window of ESET Mail Security.

Rescan messages

Allows you to launch email checking manually. You can specify messages that will be checked and you can activate rescanning of received email. For more information see Email client protection.

Scanner setup

Displays the Email client protection setup options.

Outlook Express and Windows Mail toolbar

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

ESET Mail Security

Click on **icon** opens the main program window of ESET Mail Security.

Rescan messages

Enables you to launch email checking manually. You can specify messages that will be checked and you can activate rescanning of received email. For more information see Email client protection.

Scanner setup

Displays the Email client protection setup options.

Customize appearance

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

- **Show text** - displays descriptions for icons.
- **Text to the right** - option descriptions are moved from the bottom to the right side of icons.
- **Large icons** - displays large icons for menu options.

Confirmation dialog

This notification serves to verify that the user really wants to perform the selected action, which should eliminate possible mistakes. The dialog also offers the option to disable confirmations.

Rescan messages

The ESET Mail Security toolbar integrated in email clients enables users to specify several options for email checking. The option **Rescan messages** offers two scanning modes:

- **All messages in the current folder** - Scans messages in the currently displayed folder.
- **Selected messages only** - Scans only messages marked by the user.
- **Rescan already scanned messages** - Provides the user with the option to run another scan on messages that have been scanned before.

Web access protection

Web access protection works by monitoring communication between web browsers and remote servers to protect you from online threats, and complies with HTTP (Hypertext Transfer Protocol) and HTTPS (encrypted communication) rules.

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

⊟ Basic

We strongly recommend that you leave **Web access protection** enabled. This option can also be accessed from the main program window of ESET Mail Security by navigating to **Setup** > **Web and email** > **Web access protection**.

Enable advanced scanning of browser scripts

By default, all JavaScript programs executed by web browsers will be checked by the detection engine.

⊟ Web protocols

Allows you to configure monitoring for these standard protocols which are used by most Internet browsers. By default, ESET Mail Security is configured to monitor the HTTP protocol used by most Internet browsers.

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

Encrypted communication will be not scanned when default settings are in use. To enable the scanning of encrypted communication **Advanced setup** (**F5**) > **Web and email** > SSL/TLS.

ThreatSense parameters

Configure settings such as types of scan (emails, archives, exclusions, limits, etc.) and detection methods for Web access protection.

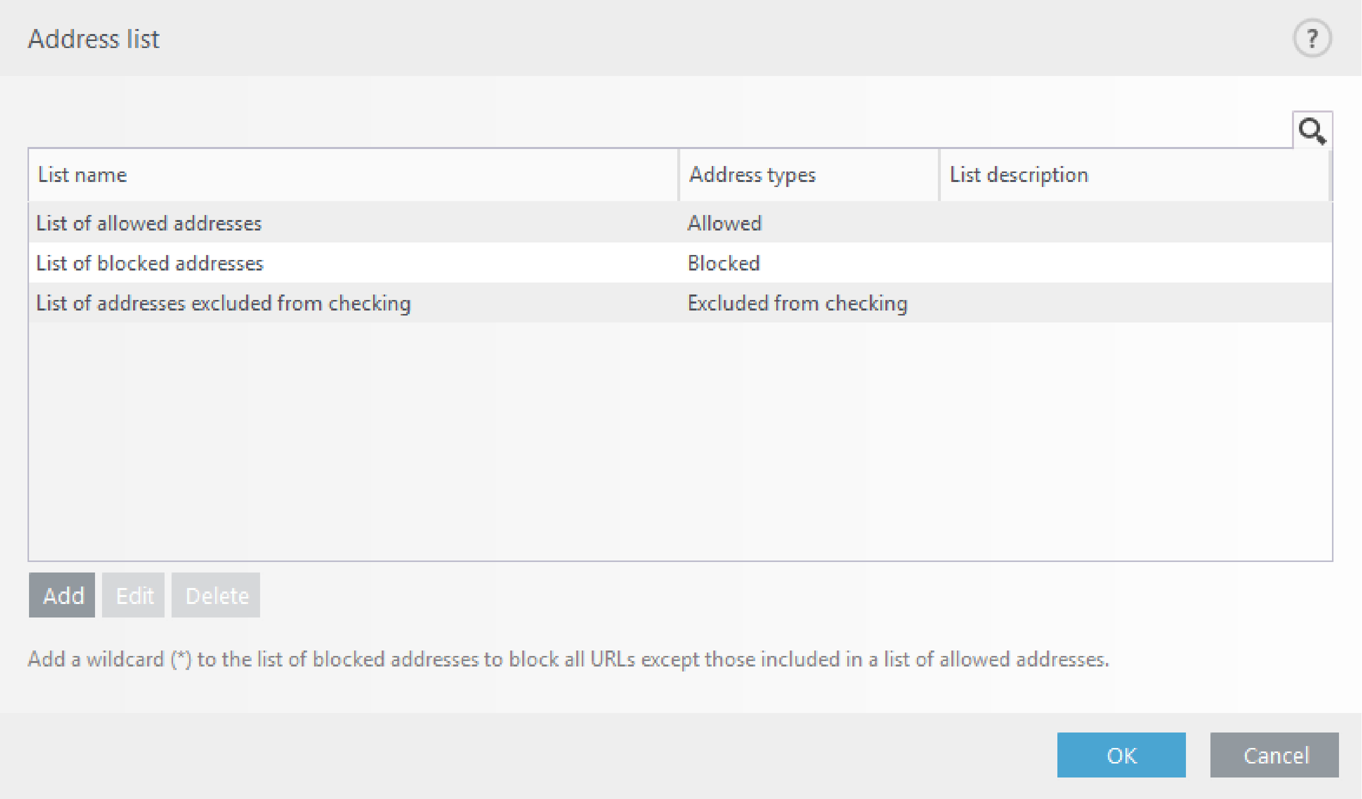
URL address management

The URL address management allows you to specify HTTP addresses to block, allow or exclude from checking. Websites in the List of blocked addresses will not be accessible unless they are also included in the List of allowed addresses. Websites in the List of addresses excluded from checking are not scanned for malicious code when accessed. SSL/TLS protocol filtering must be enabled if you want to filter HTTPS addresses in addition to HTTP web pages. Otherwise, only the domains of HTTPS sites that you have visited will be added, the full URL will not be.

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

Click **Edit** and **Add** to create a new address list in addition to the pre-defined ones. This can be useful if you want to logically split different groups of addresses. By default, the following three lists are available:

- **List of addresses excluded from checking** - No checking for malicious code will be performed for any address added to this list.
- **List of allowed addresses** - If Allow access only to HTTP addresses in the list of allowed addresses is enabled and the list of blocked addresses contains * (match everything), the user will be allowed to access addresses specified in this list only. The addresses in this list are allowed even if they are included in the list of blocked addresses.
- **List of blocked addresses** - The user will not be allowed to access addresses specified in this list unless they also occur in the list of allowed addresses.



List name	Address types	List description
List of allowed addresses	Allowed	
List of blocked addresses	Blocked	
List of addresses excluded from checking	Excluded from checking	

Add a wildcard (*) to the list of blocked addresses to block all URLs except those included in a list of allowed addresses.

You can **Add** a new URL address into the list. You can also enter multiple values with separator. Click **Edit** to modify an existing address in the list, or **Delete** to delete it. Deleting is only possible for addresses created with **Add**, not the ones that were imported.

In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk represents any number or character, while the question mark represents any one character. Particular care should be taken when specifying excluded addresses because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list.

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

Create new list

The list will include the desired URL addresses/domain masks that will be blocked, allowed or excluded from checking. When creating a new list, specify the following:

- **Address list type** - Choose the type (Excluded from checking, Blocked or Allowed) from the drop-down list.
- **List name** - Specify the name of the list. This field will be grayed out when editing one of the three pre-defined lists.
- **List description** - Type a short description for the list (optional). Will be grayed out when editing one of three pre-defined list.
- **List active** - Use the switch to deactivate the list. You can activate it later when required.
- **Notify when applying** - If you want to be notified when a particular list is used in evaluation of an HTTP / HTTPS site that you visited. A notification will be issued if a website is blocked or allowed because it is included in the list of blocked or allowed addresses. The notification will contain the name of the list containing the specified website.
- **Logging severity** - Choose the logging severity (None, Diagnostic, Information or Warning) from the drop-down list. Records with **Warning** verbosity can be collected by ESET Security Management Center.

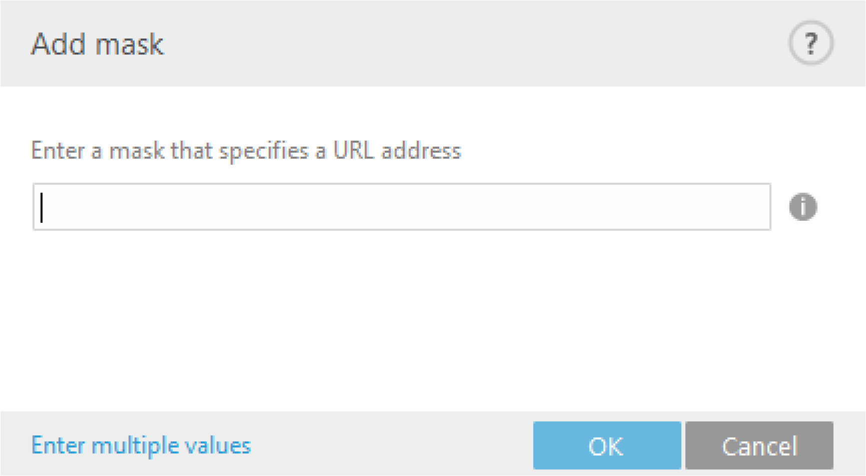
ESET Mail Security enables user to block access to specified websites and prevent the Internet browser from displaying their content. Furthermore, it allows user to specify addresses, which should be excluded from checking. If the complete name of the remote server is unknown, or the user wishes to specify a whole group of remote servers, so-called masks can be used to identify such a group.

The masks include the symbols ? and *:

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

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

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

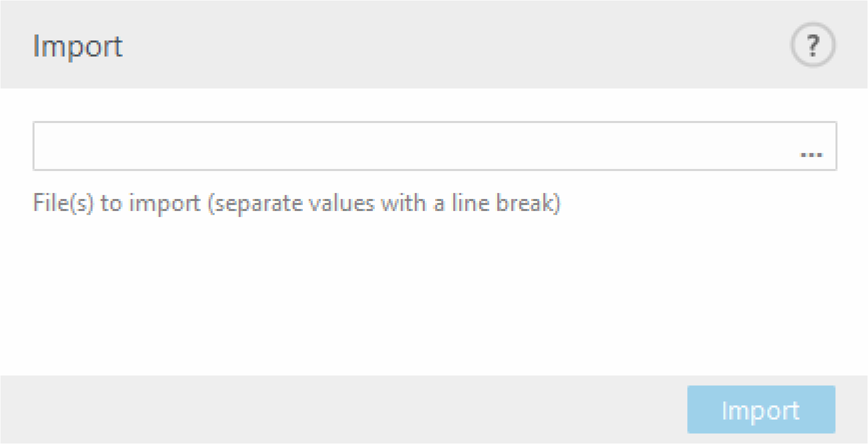


Enter multiple values

Add multiple URL addresses delimited by new lines, commas or semicolons. When multiple selection is enabled, addresses will be shown in the list.

Import

Text file with URL addresses to import (separate values with a line break, for example `*.txt` using encoding UTF-8).

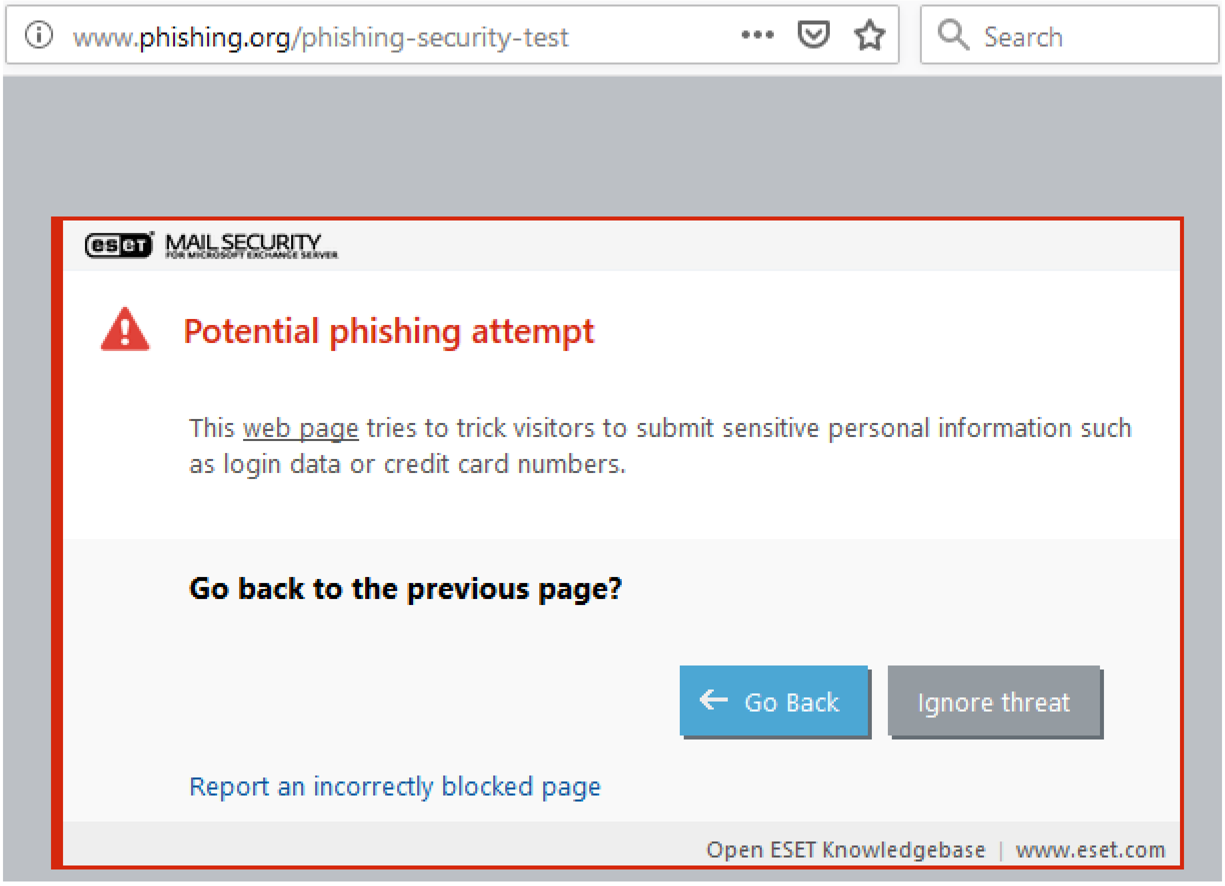


Anti-Phishing web protection

The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more.

ESET Mail Security includes anti-phishing protection, which blocks web pages known to distribute this type of content. We strongly recommend that you enable Anti-Phishing in ESET Mail Security. Visit our Knowledgebase article for more information on Anti-Phishing protection in ESET Mail Security.

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



www.phishing.org/phishing-security-test

Search

MAIL SECURITY FOR MICROSOFT EXCHANGE SERVER

Potential phishing attempt

This web page tries to trick visitors to submit sensitive personal information such as login data or credit card numbers.

Go back to the previous page?

Go Back

Ignore threat

Report an incorrectly blocked page

Open ESET Knowledgebase | www.eset.com

NOTE
Potential phishing websites that have been whitelisted will expire after several hours by default. To allow a website permanently, use the URL address management tool.

Report a phishing site

If you run across a suspicious website that appears to be phishing or otherwise malicious, you can report it to ESET for analysis. Before submitting a website to ESET, make sure it meets one or more of the following criteria:

- the website is not detected at all
- the website is incorrectly detected as a threat. In this case, you can Report a false-positive phishing site
- .

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

Device control

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

NOTE
When you enable device control using **Integrate into system** switch, the Device control feature of ESET Mail Security will be activated. However, a restart your system is required for this change to take effect.

Device control will become active, allowing you to edit their settings. If a device blocked by an existing rule is detected, a notification window will be displayed and access to the device will not be granted.

Rules

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

Groups

When you click Edit, you can manage Device groups. Create a new Device group or select an existing one to add or remove devices from the list.

> NOTE
> You can view device control log entries in Log files.

Device rules

Specific devices can be allowed or blocked by user, user group, or any of several additional parameters that can be specified in the rule configuration. The list of rules contains several descriptions of a rule such as its name, the type of external device, the action to perform when a device is detected, and log severity.

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

Apply during

You can limit rules using Time slots. Create the time slot first, it will then appear in the drop-down menu.

Device type

Choose the external device type from the drop-down menu (Disk storage/Portable device/Bluetooth/FireWire/...). The types of devices are inherited from the operating system and can be seen in the system Device manager assuming the device is connected to the computer. Storage devices include external disks or conventional memory card readers connected via USB or FireWire. Smart card readers include all readers of smart cards with an embedded integrated circuit, such as SIM cards or authentication cards. Examples of imaging devices are scanners or cameras, these devices do not provide information about users, only about their actions. This means that imaging devices can only be blocked globally.

Action

Access to non-storage devices can either be allowed or blocked. In contrast, rules for storage devices allow you to select one of the following rights settings:

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

> NOTE
> Note that not all rights (actions) are available for all device types. If a device has storage space, all four actions are made available. For non-storage devices, there are only two (for example **Read Only** is not available for Bluetooth , so Bluetooth devices can only be allowed or blocked).

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

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

> NOTE
> If these three descriptors are empty, the rule will ignore these fields when matching. Filtering parameters in all text fields are case-insensitive and no wildcards (*, ?) are supported.

In order to figure out the parameters of a device, create a rule to allow that type of device, connect the device to your computer and then review the device details in the Device control log.

Choose the **Logging severity** from the drop-down list:

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

Rules can be limited to certain users or user groups by adding them to the **User list**. Click **Edit** to manage the User list.

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

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

The following functions are available:

Edit

Lets you modify the name of a selected rule or parameters for the devices contained therein (vendor, model, serial number).

Copy

Creates a new rule based on the parameters of the selected rule.

Delete

If you want to delete the selected rule. Alternatively, you can use the check box next to a given rule to disable it. This can be useful if you don't want to delete a rule permanently so that you can use it in the future.

Populate

Provides an overview of all currently connected devices with the following information: device type, device vendor, model and serial number (if available). When you select a device (from the list of Detected devices) and click **OK**, a rule editor window appears with pre-defined information (you can adjust all the settings).

Rules are listed in order of priority with higher-priority rules at the top. You can select multiple rules and apply actions, such as deleting or moving them up or down the list by clicking **Top**/**Up**/**Down**/**Bottom** (arrow buttons).

Device groups

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

You can create different groups of devices for which different rules will be applied. You can also create a single group of devices that are set to **Read/Write** or **Read-only**. This ensures that unrecognized devices will be blocked by Device control when connected to your computer.

> WARNING
> Having an external device connected to your computer may pose a security risk.

The following functions are available:

Add

Create a new device group by entering its name or add a device to an existing group (optionally, you can specify details such as vendor name, model and serial number) depending on where in the window you clicked the button.

Edit

Lets you modify the name of a selected group or parameters for the devices contained therein (vendor, model, serial number).

Delete

Deletes the selected group or device depending on where in the window you clicked. Alternatively, you can use the check box next to a given rule to disable it. This can be useful if you do not want to delete a rule permanently so that you can use it in the future.

Import

Imports a serial number list of devices from a file.

Populate

Provides an overview of all currently connected devices with the following information: device type, device vendor, model and serial number (if available). When you select a device (from the list of Detected devices) and click **OK**, a rule editor window appears with pre-defined information (you can adjust all the settings).

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

> NOTE
> Please note that not all rights (actions) are available for all device types. If a device has storage space, all four actions are made available. For non-storage devices, there are only two (for example, Read Only is not available for Bluetooth, so Bluetooth devices can only be allowed or blocked).

Tools configuration

You can customize advanced settings for the following:

- Time slots
- ERA/ESMC scan targets
- Override mode
- ESET CMD
- ESET RMM
- License
- WMI Provider
- Log files
- Proxy server
- Email notifications
- Presentation mode
- Diagnostics
- Cluster

Time slots

Time slots are used within Device control rules, limiting the rules when they are being applied. Create a time slot and select it when adding new or modifying existing rules (**Apply during** parameter). This enables you to define commonly used time slots (work time, weekend, etc.) and reuse them easily without redefining the time ranges for every rule. A time slot should be applicable to any relevant type of rule that supports time-based control.

Microsoft Windows update

Windows updates provide important fixes to potentially dangerous vulnerabilities and improve the general security level of your computer. For this reason, it is vital that you install Microsoft Windows updates as soon as they become available. ESET Mail Security notifies you about missing updates according to the level you specify. The following levels are available:

- **No updates** - No system updates will be offered for download.
- **Optional updates** - Updates marked as low priority and higher will be offered for download.
- **Recommended updates** - Updates marked as common and higher will be offered for download.

- **Important updates** - Updates marked as important and higher will be offered for download.

- **Critical updates** - Only critical updates will be offered for download.

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

ESET CMD

This is a feature that enables advanced ecmd commands. It allows you to export and import settings using the command line (ecmd.exe). Until now, it was only possible to export settings using the GUI. ESET Mail Security configuration can be exported to an *.xml* file.

When you have enabled ESET CMD, there are two authorization methods available:

- **None** - No authorization. We do not recommend this method because it allows importation of any unsigned configuration, which is a potential risk.

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

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

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

> EXAMPLE
> Export settings command:
> `ecmd /getcfg c:\config\settings.xml`
>
> Import settings command:
> `ecmd /setcfg c:\config\settings.xml`

> NOTE
> Advanced ecmd commands can only be run locally. Executing the client task **Run command** using ESET Security Management Center will not work.

Signing an *.xml* configuration file:

1. Download XmlSignTool executable.

2.Open a Windows Command Prompt (cmd) using **Run as administrator**.

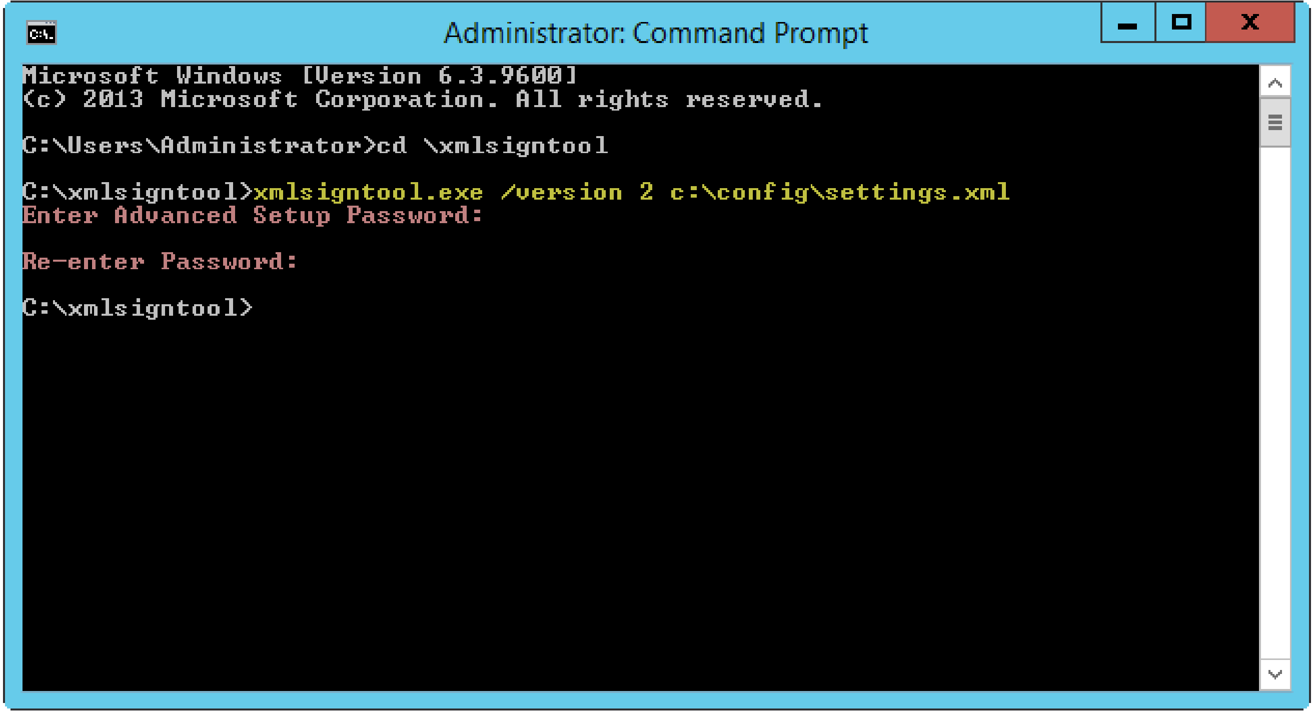
3.Navigate to the location of `xmlsigntool.exe`

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

IMPORTANT
Value of the parameter `/version` depends on the version of your ESET Mail Security. Use `/version 2` for ESET Mail Security 7 and newer.

5.Enter and Re-enter your Advanced Setup Password when prompted by the XmlSignTool. Your *.xml* configuration file is now signed and can be used to import on another instance of ESET Mail Security with ESET CMD using the password authorization method.

EXAMPLE
Sign exported configuration file command: `xmlsigntool /version 2 c:\config\settings.xml`



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \xmlsigntool

C:\xmlsigntool>xmlsigntool.exe /version 2 c:\config\settings.xml
Enter Advanced Setup Password:

Re-enter Password:

C:\xmlsigntool>
```

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

ESET RMM

Remote monitoring and management (RMM) is the process of supervising and controlling software systems (such as those on desktops, servers and mobile devices) by means of a locally installed agent that can be accessed by a management service provider.

Enable RMM

Enables Remote monitoring and management command are functional. You must have administrator privileges to use RMM utility.

Working mode

Select the working mode of RMM from the drop-down menu:

- **Safe separation only -** If you want to enable RMM interface for safe and read only operations
- **All operations -** If you want to enable RMM interface for all operations

Authorization method

Set the RMM authorization method from the drop-down menu:

- **None** -No application path check will be performed, you can run *ermm.exe* from any application
- **Application path** - Specify application which is allowed to run *ermm.exe*

Default ESET Endpoint Security installation contains file *ermm.exe* located in ESET Mail Security (default path *c:\Program Files\ESET\ESET Mail Security*). *ermm.exe* exchange data with RMM Plugin, which communicates with RMM Agent, linked to a RMM Server.

- *ermm.exe* - Command line utility developed by ESET that allows managing of Endpoint products and communication with any RMM Plugin.
- RMM Plugin - A third party application running locally on Endpoint Windows system. The plugin was designed to communicate with specific RMM Agent (e.g. Kaseya only) and with *ermm.exe*.
- RMM Agent - A third party application (e.g. from Kaseya) running locally on Endpoint Windows system. Agent communicates with RMM Plugin and with RMM Server.
- RMM Server - Running as a service on a third party server. Supported RMM systems are by Kaseya, Labtech, Autotask, Max Focus and Solarwinds N-able.

Visit our Knowledgebase article for more information on ESET RMM in ESET Mail Security.

ESET Direct Endpoint Management plugins for third-party RMM solutions

RMM Server is running as a service on a third-party server. For more information see the following ESET Direct Endpoint Management online user guides:

- ESET Direct Endpoint Management Plug-in for ConnectWise Automate

- ESET Direct Endpoint Management Plugin for DattoRMM

- ESET Direct Endpoint Management for Solarwinds N-Central

- ESET Direct Endpoint Management for NinjaRMM

License

ESET Mail Security connects to the ESET License server a few times per hour to preform checks. The **Interval check** parameter is set to **Automatic** by default. If you want to decrease network traffic caused by licensing checks, change the Interval check to **Limited** and the licensing check will be done only once a day (also after server restart).

With the Interval check set to **Limited**, all license-related changes done to your ESET Mail Security via ESET Business Account and ESET MSP Administrator may take up to one day to apply.

WMI Provider

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

For more information on WMI, see
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI Provider

The purpose of the ESET WMI Provider is to allow for the remote monitoring of ESET products in an enterprise environment without requiring any ESET-specific software or tools. By exposing the basic product, status and statistics information via WMI, we greatly expand the possibilities of enterprise administrators when monitoring the ESET products. Administrators can take advantage of the number of access methods offered by WMI (command line, scripts and third-party enterprise monitoring tools) to monitor the state of their ESET products.

The current implementation provides read-only access to basic product information, installed features and their protection status, statistics of individual scanners, and product log files.

The WMI Provider allows for the use of standard Windows WMI infrastructure and tools to read the state of the product and product logs.

Provided data

All the WMI classes related to ESET product are located in the “root\ESET“ namespace. The following classes, which are described in more detail below, are currently implemented:

General

- **ESET_Product**
- **ESET_Features**
- **ESET_Statistics**

Logs

- **ESET_ThreatLog**
- **ESET_EventLog**
- **ESET_ODFileScanLogs**
- **ESET_ODFileScanLogRecords**
- **ESET_ODServerScanLogs**
- **ESET_ODServerScanLogRecords**
- **ESET_HIPSLog**
- **ESET_URLLog**
- **ESET_DevCtrlLog**
- **ESET_GreylistLog**
- **ESET_MailServeg**
- **ESET_HyperVScanLogs**
- **ESET_HyperVScanLogRecords**

ESET_Product class

There can only be one instance of the ESET_Product class. Properties of this class refer to basic information about your installed ESET product:

- **ID** - Product type identifier, for example, “emsl”
- **Name** - Name of the product, for example, "ESET Mail Security"
- **FullName** - Full name of the product, for example, "ESET Mail Security for IBM Domino"
- **Version** - Product version, for example, "6.5.14003.0"
- **VirusDBVersion** - Version of the virus database, for example, "14533 (20161201)"
- **VirusDBLastUpdate** - Timestamp of the last update of the virus database. The string contains the timestamp in WMI datetime format. for example, “20161201095245.000000+060”
- **LicenseExpiration** - License expiration time. The string contains timestamp in WMI datetime format
- **KernelRunning** - Boolean value indicating whether the ekrn service is running on the machine, for example, “TRUE”
- **StatusCode** - Number indicating the protection status of the product: 0 - Green (OK), 1 - Yellow (Warning), 2 - Red (Error)
- **StatusText** - Message describing the reason for a non-zero status code, otherwise it is null

ESET_Features class

The ESET_Features class has multiple instances, depending on the number of product features. Each instance contains:

- **Name** - Name of the feature (list of names is provided below)
- **Status** - Status of the feature: 0 - inactive, 1 - disabled, 2 - enabled

A list of strings representing currently recognized product features:

- **CLIENT_FILE_AV** - Real-time file system anti-virus protection
- **CLIENT_WEB_AV** - Client web anti-virus protection
- **CLIENT_DOC_AV** - Client document anti-virus protection
- **CLIENT_NET_FW** - Client personal firewall
- **CLIENT_EMAIL_AV** - Client email anti-virus protection
- **CLIENT_EMAIL_AS** - Client email anti-spam protection
- **SERVER_FILE_AV** - Real-time anti-virus protection of files on the protected file server product, for example, files in SharePoint’s content database in the case of ESET Mail Security
- **SERVER_EMAIL_AV** - Anti-virus protection of emails of protected server product, for example, emails in MS Exchange or IBM Domino
- **SERVER_EMAIL_AS** - Anti-spam protection of emails of protected server product, for example, emails in MS Exchange or IBM Domino
- **SERVER_GATEWAY_AV** - Anti-virus protection of protected network protocols on the gateway
- **SERVER_GATEWAY_AS** - Anti-spam protection of protected network protocols on the gateway

ESET_Statistics class

The ESET_Statistics class has multiple instances, depending on the number of scanners in the product. Each instance contains:

- **Scanner** - String code for the particular scanner, for example, “CLIENT_FILE”
- **Total** - Total number of files scanned

- **Infected** - Number of infected files found
- **Cleaned** - Number of cleaned files
- **Timestamp** - Timestamp of the last change of this statistics. In WMI datetime format, for example, “20130118115511.000000+060”
- **ResetTime** - Timestamp of when the statistics counter was last reset. In WMI datetime format, for example, “20130118115511.000000+060”

List of strings representing currently recognized scanners:

- **CLIENT_FILE**
- **CLIENT_EMAIL**
- **CLIENT_WEB**
- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog class

The ESET_ThreatLog class has multiple instances, each one representing a log record from the “Detected threats” log. Each instance contains:

- **ID** - Unique ID of this scan log record
- **Timestamp** - Creation timestamp of the log (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number in the [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Scanner** - Name of the scanner that created this log event
- **ObjectType** - Type of object that produced this log event
- **ObjectName** - Name of the object that produced this log event
- **Threat** - Name of the threat that has been found in the object described by ObjectName and ObjectType properties
- **Action** - Action performed after the threat was identified
- **User** - User account that caused this log event to be generated
- **Information** - Additional description of the event
- **Hash** - Hash of the object that produced this log event

ESET_EventLog

The ESET_EventLog class has multiple instances, each one representing a log record from the “Events” log. Each instance contains:

- **ID** - Unique ID of this scan log record
- **Timestamp** - Creation timestamp of the log (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number in the [0-8] interval. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Module** - Name of the module that created this log event
- **Event** - Description of the event
- **User** - User account that caused this log event to be generated

ESET_ODFileScanLogs

The ESET_ODFileScanLogs class has multiple instances, each one representing an on-demand file scan record. This is equivalent to the GUI “On-demand computer scan” list of logs. Each instance contains:

- **ID** - Unique ID of this scan log record
- **Timestamp** - Creation timestamp of the log (in the WMI date/time format)
- **Targets** - Target folders/objects of the scan
- **TotalScanned** - Total number of objects scanned
- **Infected** - Number of infected objects found
- **Cleaned** - Number of objects cleaned
- **Status** - Status of the scan process

ESET_ODFileScanLogRecords

The ESET_ODFileScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_ODFileScanLogs class. Instances of this class provide log records of all the on-demand scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each class instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_ODFileScanLogs class)
- **ID** - Unique ID of this scan log record
- **Timestamp** - Creation timestamp of the log (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - The actual log message

ESET_ODServerScanLogs

The ESET_ODServerScanLogs class has multiple instances, each one representing a run of the on-demand server scan. Each instance contains:

- **ID** - Unique ID of this scan log record
- **Timestamp** - Creation timestamp of the log (in the WMI date/time format)
- **Targets** - Target folders/objects of the scan
- **TotalScanned** - Total number of objects scanned
- **Infected** - Number of infected objects found
- **Cleaned** - Number of objects cleaned
- **RuleHits** - Total number of rule hits
- **Status** - Status of the scan process

ESET_ODServerScanLogRecords

The ESET_ODServerScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_ODServerScanLogs class. Instances of this class provide log records of all the on-demand scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each class instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_ ODServerScanLogs class)
- **ID** - Unique ID of this scan log record

- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number in the [0-8] interval. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - The actual log message

ESET_SmtpProtectionLog

The ESET_SmtpProtectionLog class has multiple instances, each one representing a log record from the “Smtp protection” log. Each instance contains:

- **ID** - Unique ID of this scan log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **HELODomain** - Name of the HELO domain
- **IP** - Source IP address
- **Sender** - Email sender
- **Recipient** - Email recipient
- **ProtectionType** - Type of protection used
- **Action** - Action performed
- **Reason** - Reason for action
- **TimeToAccept** - Number of minutes after which the email will be accepted

ESET_HIPSLog

The ESET_HIPSLog class has multiple instances, each one representing a log record from the “HIPS” log. Each instance contains:

- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number in the [0-8] interval. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Application** - Source application
- **Target** - Type of operation
- **Action** - Action taken by HIPS, e.g. allow, deny, etc.
- **Rule** - Name of the rule responsible for the action
- **AdditionalInfo**

ESET_URLLog

The ESET_URLLog class has multiple instances, each one representing a log record from the “Filtered websites” log. Each instance contains:

- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

- **URL** - The URL
- **Status** - What happened to URL, e.g. "Blocked by Web control"
- **Application** - Application that tried to access the URL
- **User** - User account the application was running under

ESET_DevCtrlLog

The ESET_DevCtrlLog class has multiple instances, each one representing a log record from the “Device control” log. Each instance contains:

- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Device** - Device name
- **User** - User account name
- **UserSID** - User account SID
- **Group** - User group name
- **GroupSID** - User group SID
- **Status** - What happened to the device, e.g. "Writing blocked"
- **DeviceDetails** - Additional info regarding the device
- **EventDetails** - Additional info regarding the event

ESET_MailServerLog

The ESET_MailServerLog class has multiple instances, each one representing a log record from the “Mail server” log. Each instance contains:

- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **IPAddr** - Source IP address
- **HELODomain** - Name of the HELO domain
- **Sender** - Email sender
- **Recipient** - Email recipient
- **Subject** - E-mail subject
- **ProtectionType** - Protection type that has performed the action described by the current log record, i.e. malware, antispam or rules.
- **Action** - Action performed
- **Reason** - The reason why was the action performed on the object by the given ProtectionType.

ESET_HyperVScanLogs

The ESET_HyperVScanLogs class has multiple instances, each one representing a run of the Hyper-V file scan. This is equivalent to the GUI “Hyper-V scan” list of logs. Each instance contains:

- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)

- **Targets** - Target machines/disks/volumes of the scan
- **TotalScanned** - Total number of objects scanned
- **Infected** - Number of infected objects found
- **Cleaned** - Number of objects cleaned
- **Status** - Status of the scan process

ESET_HyperVScanLogRecords

The ESET_HyperVScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_HyperVScanLogs class. Instances of this class provide log records of all the Hyper-V scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each class instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_HyperVScanLogs class)
- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - The actual log message

ESET_NetworkProtectionLog

The ESET_NetworkProtectionLog class has multiple instances, each one representing a log record from the “Network protection” log. Each instance contains:

- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Event** - Event triggering network protection action
- **Action** - Action performed by network protection
- **Source** - Source address of network device
- **Target** - Destination address of network device
- **Protocol** - Network communication protocol
- **RuleOrWormName** - Rule or worm name related to the event
- **Application** - Application that initiated the network communication
- **User** - User account that caused this log event to be generated

ESET_SentFilesLog

The ESET_SentFilesLog class has multiple instances, each one representing a log record from the “Sent files” log. Each instance contains:

- **ID** - Unique ID of this log record
- **Timestamp** - Creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

- **Sha1** - Sha-1 hash of sent file
- **File** - Sent File
- **Size** - Sent file size
- **Category** - Sent file category
- **Reason** - Reason of sending the file
- **SentTo** - ESET department the file was sent to
- **User** - User account that caused this log event to be generated

ESET_OneDriveScanLogs

The ESET_OneDriveScanLogs class has multiple instances, each one representing a run of the OneDrive scan. This is equivalent to the GUI “OneDrive scan” list of logs. Each instance contains:

- **ID** - Unique ID of this OneDrive log
- **Timestamp** - Creation timestamp of the log (in the WMI date/time format)
- **Targets** - Target folders/objects of the scan
- **TotalScanned** - Total number of objects scanned
- **Infected** - Number of infected objects found
- **Cleaned** - Number of objects cleaned
- **Status** - Status of the scan process

ESET_OneDriveScanLogRecords

The ESET_OneDriveScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_OneDriveScanLogs class. Instances of this class provide log records of all the OneDrive scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_OneDriveScanLogs class)
- **ID** - Unique ID of this OneDrive log
- **Timestamp** - Creation timestamp of the log (in the WMI date/time format)
- **LogLevel** - Severity of the log record expressed as a number [0-8]. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - The actual log message

Accessing Provided Data

Here are a few examples of how to access ESET WMI data from Windows command line and PowerShell, which should work from any current Windows operating system. There are, however, many other ways of accessing the data from other scripting languages and tools.

Command line without scripts

The `wmic` command line tool can be used to access various pre-defined or any custom WMI classes.

To display complete info about product on the local machine:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

To display product version number only of the product on the local machine:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

To display complete info about product on a remote machine with IP 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Get and display complete info about product on the local machine:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Get and display complete info about product on a remote machine with IP 10.1.118.180:

```
$cred = Get-Credential # promts the user for credentials and stores it in the
variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred
$cred
```

ERA/ESMC scan targets

This functionality lets ESET Security Management Center use scan target (On-demand mailbox database scan and Hyper-V scan) when running the **Server Scan** client task on a server with ESET Mail Security. ERA/ESMC scan targets setting is available only if you have ESET Management Agent installed, otherwise it will be grayed out.

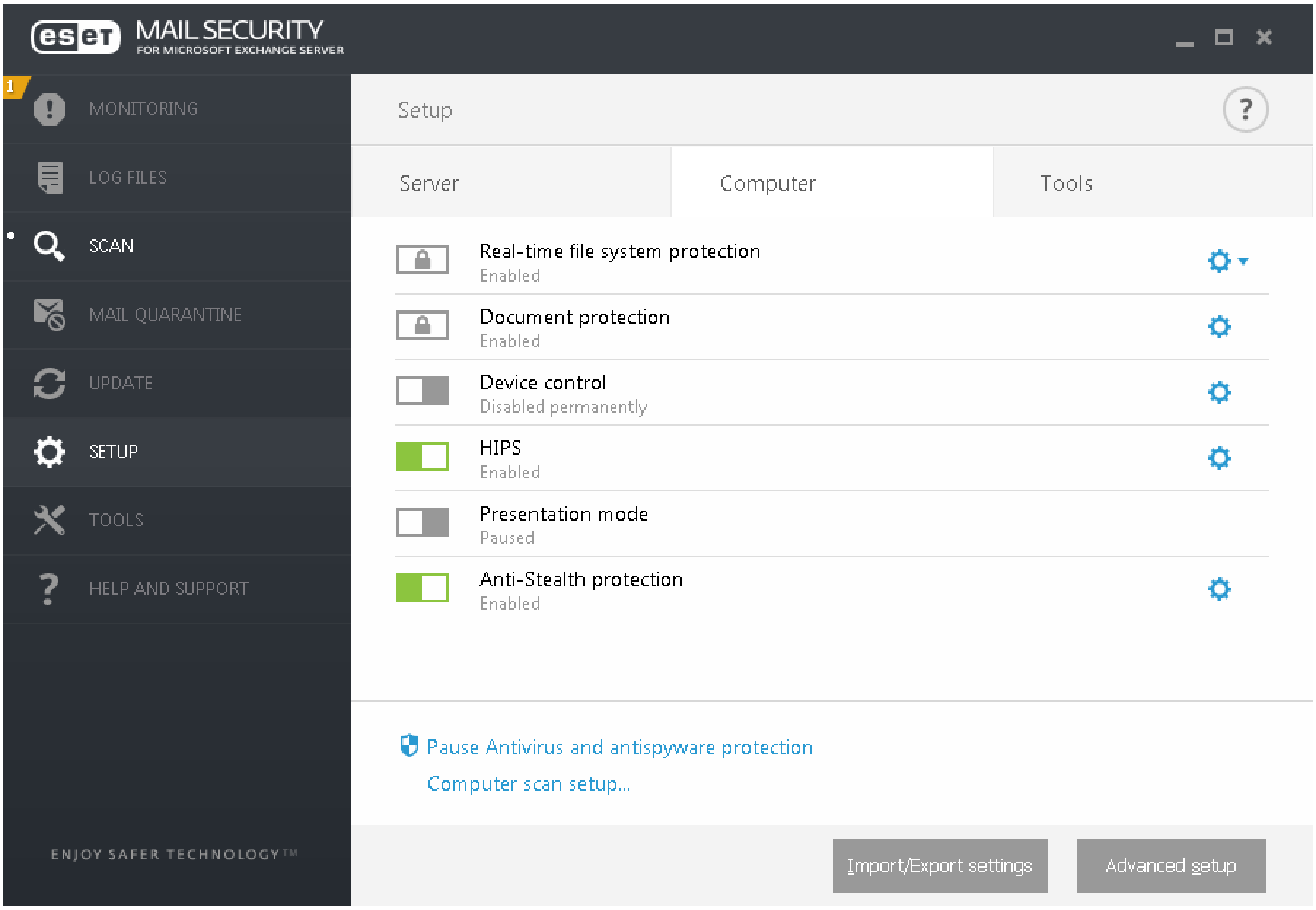
When you enable **Generate target list** ESET Mail Security creates a list of available scan targets. This list is generated periodically, according to your **Update period**.

> NOTE
> When **Generate target list** is enabled for the first time, it takes ESET Security Management Center about half of the specified **Update period** to pick it up. So if **Update period** is set to 60 minutes, it'll take ESMC about 30 minutes to receive the list of scan targets. If you need ESET Security Management Center to collect the list earlier, set the update period to a smaller value. You can always increase it later.

When ESET Security Management Center runs a **Server Scan** client task, it will collect the list and you will be asked to select scan targets for Hyper-V scan on that particular server.

Override mode

If you have ESET Security Management Center policy applied to ESET Mail Security, you'll see a lock icon 🔒 instead of enable/disable switch on Setup page and a lock icon next to the switch in **Advanced setup** window.



Real-time file system protection
Enabled

Document protection
Enabled

Device control
Disabled permanently

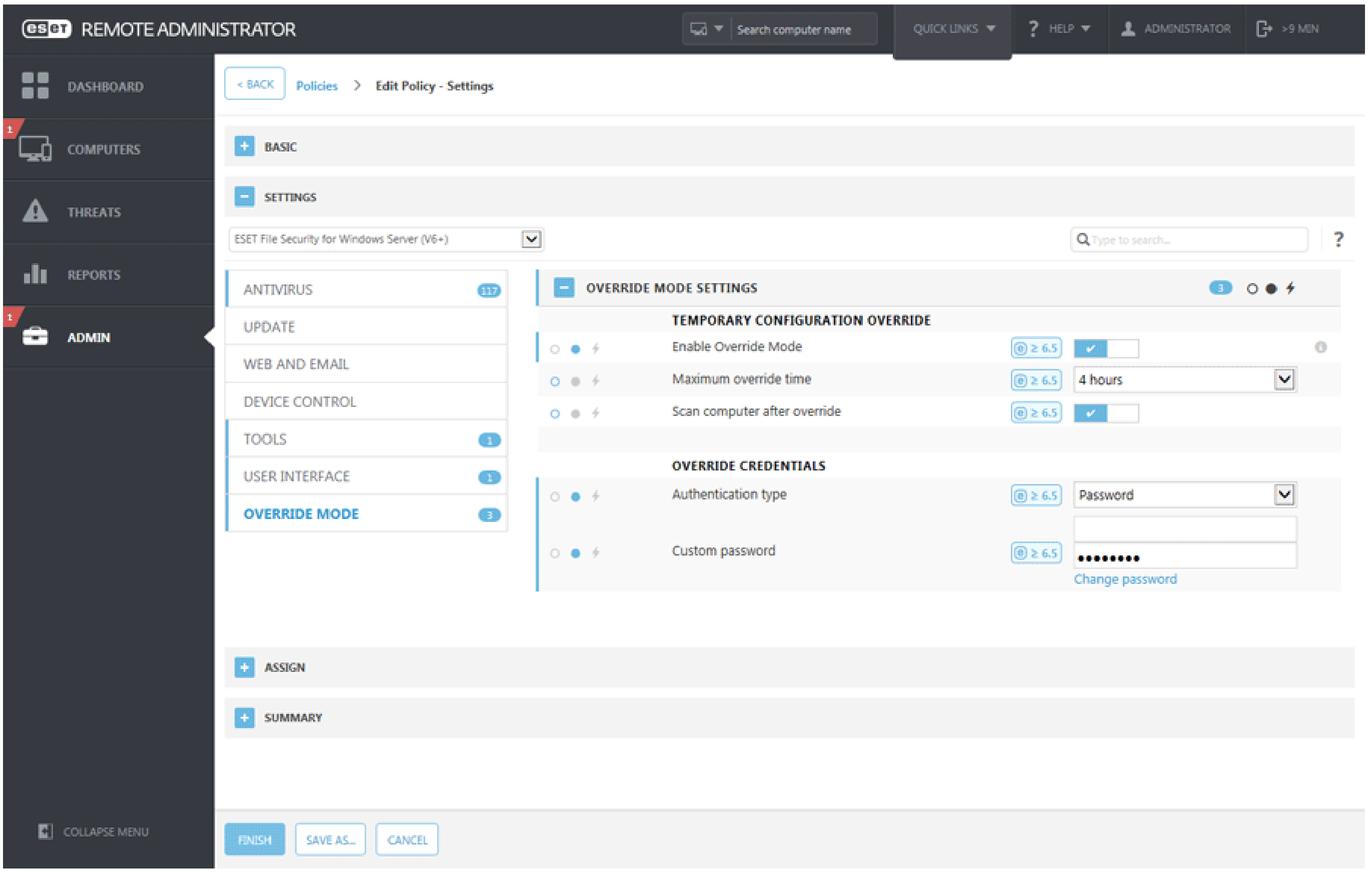
HIPS
Enabled

Presentation mode
Paused

Anti-Stealth protection
Enabled

Normally, settings that are configured via ESET Security Management Center policy cannot be modified. Override mode allows you to temporarily unlock these settings. However, you need to enable **Override mode** using ESET Security Management Center policy.

Log into ESMC Web Console, navigate to **Policies**, select and edit existing policy that is applied to ESET Mail Security or create a new one. In **Settings**, click **Override Mode**, enable it and configure the rest of its settings including Authentication type (**Active directory user** or **Password**).



ESET File Security for Windows Server (V6+)

OVERRIDE MODE SETTINGS

TEMPORARY CONFIGURATION OVERRIDE

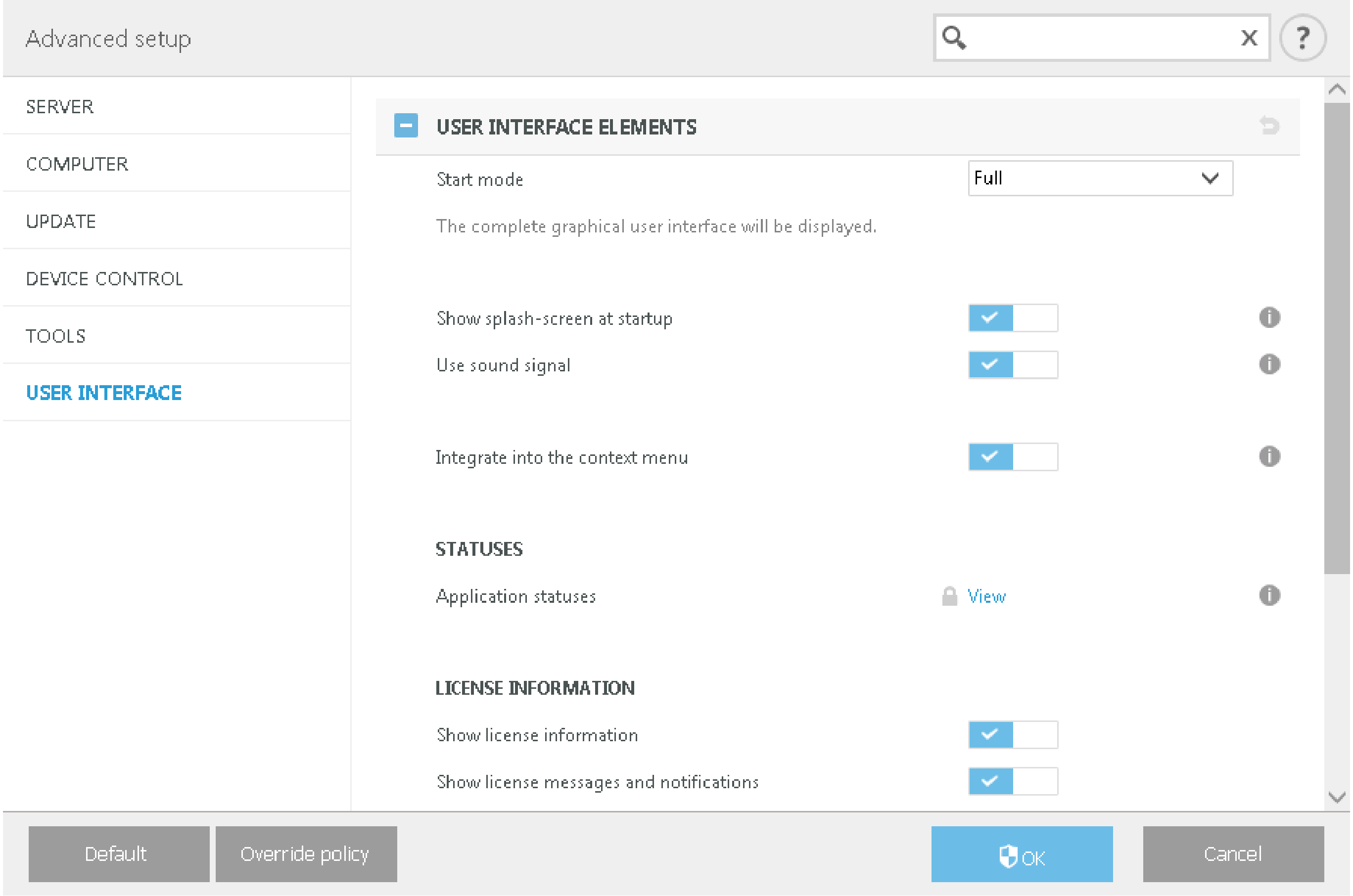
Enable Override Mode	≥ 6.5	✓
Maximum override time	≥ 6.5	4 hours
Scan computer after override	≥ 6.5	✓

OVERRIDE CREDENTIALS

Authentication type	≥ 6.5	Password
Custom password	≥ 6.5	••••••••

Change password

Once the policy is modified, or new policy is applied to ESET Mail Security, Override policy button will appear in Advanced setup window.



USER INTERFACE ELEMENTS

Start mode: Full

The complete graphical user interface will be displayed.

Show splash-screen at startup	✓
Use sound signal	✓
Integrate into the context menu	✓

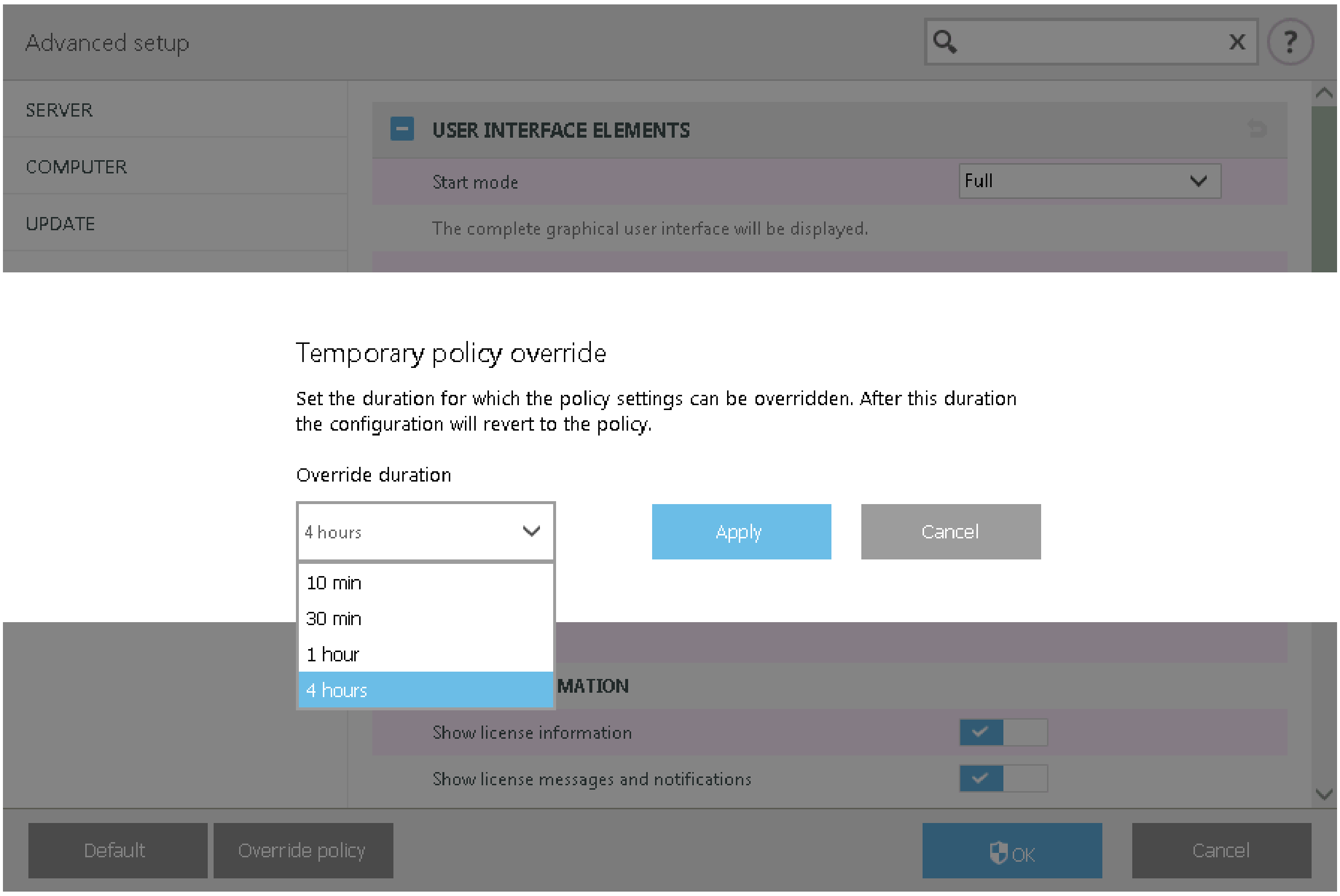
STATUSES

Application statuses: View

LICENSE INFORMATION

Show license information	✓
Show license messages and notifications	✓

Click **Override policy** button, set the duration and click **Apply**.



Start mode: Full

The complete graphical user interface will be displayed.

Temporary policy override

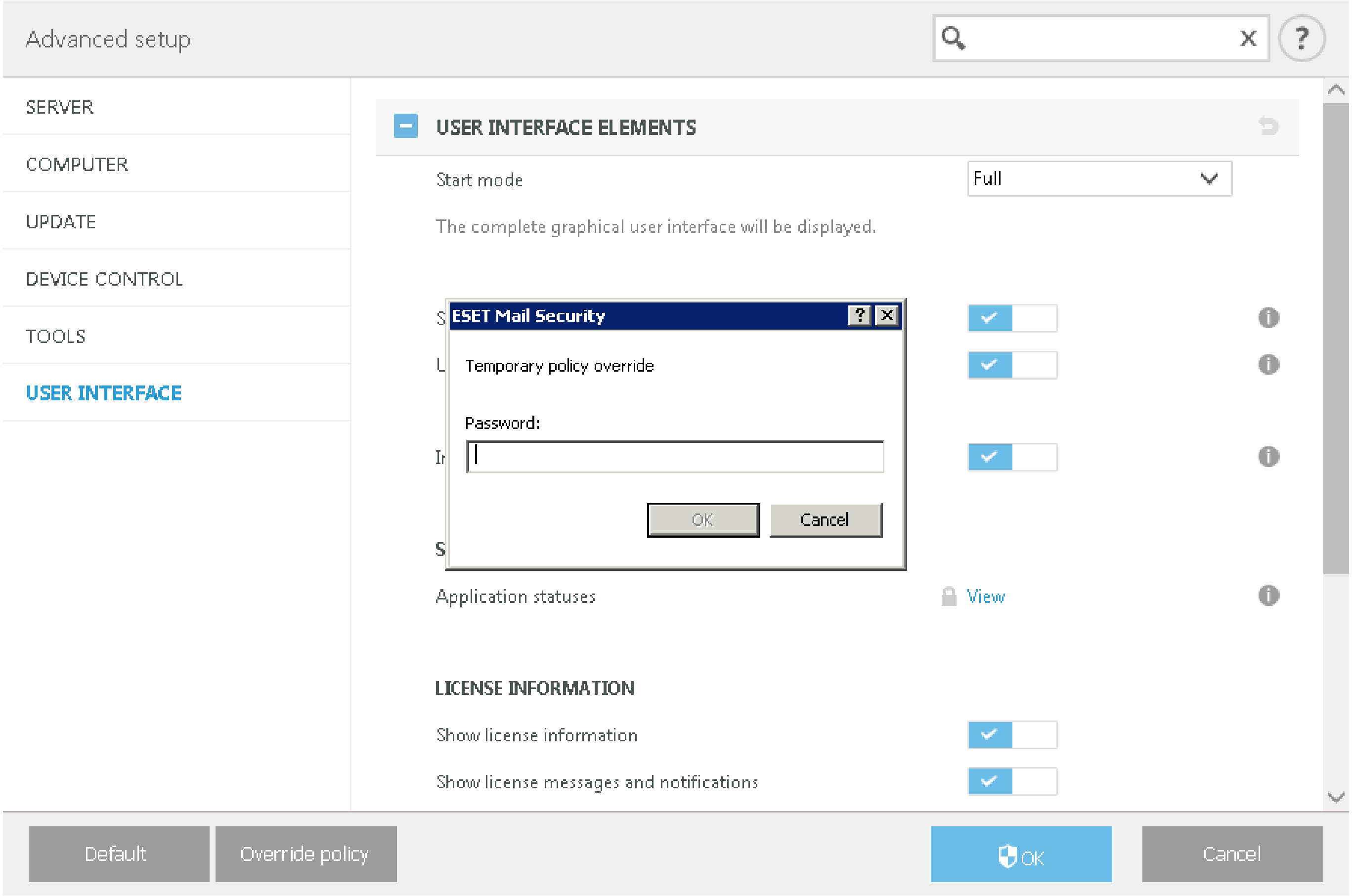
Set the duration for which the policy settings can be overridden. After this duration the configuration will revert to the policy.

Override duration: 4 hours

Show license information

Show license messages and notifications

If you selected **Password** as Authentication type, enter the policy override password.



Start mode: Full

The complete graphical user interface will be displayed.

Temporary policy override

Password:

Application statuses

Show license information

Show license messages and notifications

Once the Override mode expires, any configuration changes you've made will revert back to original ESET Security

Management Center policy settings. You'll see a notification before the Override expires.

You can **End override** mode anytime before it expires on Monitoring page or in **Advanced setup** window.

Log files

This section lets you modify configuration of ESET Mail Security logging.

⊟ Log records

Records are written to the Events log (*C:\ProgramData\ESET\ESET Security\Logs*) and can be viewed in Log files viewer. Use the switches to enable or disable particular feature:

Log mail transport errors

If this option is enabled and should there be problems on the mail transport layer, error messages are written into Events log.

Log mail transport exceptions

If there are any exceptions on the mail transport layer, details about it are written into Events log.

⊟ Logging filter

Produces a significant amount of data because all the logging options are enabled by default. We recommend you to selectively disable logging of the components which are not useful or related to the problem.

> NOTE
> To start the actual logging you need to turn on general **Diagnostic logging** on product level in main menu **Setup** > Tools. Once the logging itself is turned on, ESET Mail Security will collect detailed logs according to what features are enabled in this section.

Use the switches to enable or disable particular feature. This options also be combined depending on the availability of individual components in the ESET Mail Security.

- **Mail transport diagnostic logging**

> IMPORTANT
> When resolving issues with Database scan that is run in a normal operation, we recommend you to disable the **Mail transport diagnostic logging**. Otherwise, this could clog up the resulting log and make it difficult to analyze.

- **On-demand database scan diagnostic logging** - Writes detailed information into logs, especially when troubleshooting is necessary.
- **Cluster diagnostic logging** - Cluster logging will be included in general diagnostic logging.
- **Antispam engine diagnostic logging** - When you need to troubleshoot, you will see detailed antispam

engine information in the logs. Writes detailed information about the Antispam engine into the log file for diagnostic purposes. The Antispam engine doesn't use the **Events log** (`warnlog.dat` file) and therefore cannot be viewed in the Log files viewer. It writes records directly into a dedicated text file (for example `C:\ProgramData\ESET\ESET Mail Security\Logs\antispam.0.log`) so that all Antispam engine diagnostic data is kept in one place. This way, performance of ESET Mail Security is not compromised in a case of a huge email traffic.

⊟ Log files

Define how the logs will be managed. This is important mostly to prevent the disk being used up. Default settings allow for automatic deletion of older logs in order to save disk space.

Automatically delete records older than (days)

Log entries older than the specified number of days will get deleted.

Automatically delete old records if log size exceeded

When log size exceeds **Max log size [MB]**, old log records will be deleted until **Reduced log size [MB]** is reached.

Back up automatically deleted records

Automatically deleted log records and files will be backed up to the specified directory and optionally compressed as ZIP files.

Back up diagnostic logs

Will back up automatically deleted diagnostic logs. If not enabled, diagnostic log records are not backed up.

Backup folder

Folder where log backups will be stored. You can enable compressed log backups using ZIP.

Optimize log files automatically

When engaged, log files will automatically be defragmented if the fragmentation percentage is higher than value specified in the **If the number of unused records exceeds (%)** field. Click **Optimize** to begin defragmenting the log files. All empty log entries are removed to improve performance and log processing speed. This improvement can be observed especially if the logs contain a large number of entries.

Enable text protocol

To enable the storage of logs in another file format separate from Log files:

- **Target directory** - The directory where log files will be stored (only applies to **Text/CSV**). Each log section has its own file with a pre-defined file name (for example, *virlog.txt* for Detected threats section of Log files, if you use plain text file format to store logs).
- **Type** - If you select the **Text** file format, logs will be stored in a text file; data will be separated by tabs. The same applies to comma-separated **CSV** file format. If you choose **Event**, logs will be stored in the

Windows Event log (can be viewed using Event Viewer in Control panel) as opposed to file.

- **Delete all log files** - Erases all stored logs currently selected in the **Type** drop-down menu.

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

⊟ Log export

Export to Windows Application and Services Logs

Allows you to duplicate records from the Mail server protection log to the Applications and Services Logs. To view the Mail server protection log, open Windows **Event Viewer** and navigate to **Applications and Services Logs** > **ESET** > **Security** > **ExchangeServer** > **MailProtection**. The Application and Services logs are supported on Microsoft Windows Server 2008 R2 SP1 or newer.

Export to syslog server

You can have Mail server protection logs duplicated to syslog server in Common Event Format (CEF). CEF is a standardized extensible, text-based format, that can be used to facilitate data collection and aggregation for later analysis by an enterprise management system. In this case, you can use it with Security Information and Event Management (SIEM) and log management solutions such as Micro Focus ArcSight. See Syslog event mapping for details on exported event fields and description.

Server address

Enter IP address or server host name. In case of ArcSight, specify server with SmartConnector installed.

Protocol

Select the protocol that will be used, either TCP or UDP protocol.

Port

The default value is 514 for both protocols.

Export to file

Allows for the logs to be exported locally to a file in CEF format. Logging storage capacity is limited, therefore a circular logging is used. Records are written sequentially into the files (from `mailserver.0.log` to `mailserver.9.log`). The latest records are stored in `mailserver.0.log`, once it reaches its size limit, the oldest file `mailserver.9.log` is deleted and the rest of the log files are renamed in sequence (`mailserver.0.log` is renamed to `mailserver.1.log` and so on).

File path

Default path is C:\ProgramData\ESET\ESET Security\Logs. You can change the location if required.

Syslog event mapping

The following tables show ESET Mail Security event mapping to ArcSight data fields. You can use these tables as a reference of what is being fed to ArcSight via SmartConnector.

Header		
Device Vendor	"ESET"	
Device Product	"EMSX"	"EMSX" or "ESET Mail Security for MS Exchange Server"
Device Version	e.g. "7.1.10005.0"	
Device Event Class ID	e.g. "101"	Device Event Category unique identifier: 100-199 malware 200-299 phish 300-399 spam 400-499 policy
Event Name	e.g. "MailScanResult: malware"	A brief description of what happened in the event: MailScanResult: malware MailScanResult: phishing link MailScanResult: spam MailScanResult: policy

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
rt	deviceReceiptTime	Time event was generated	The time at which the event was generated, in milliseconds since Jan 1st 1970
src	sourceAddress	Sender's IP	IP address of the sending mail server
shost	sourceHostName (1023)	Sender's HELO domain	HELO domain of the sending mail server
flexString1	flexString1	Message-ID	Message-ID header from the email
dhost	destinationHostName (1023)	Receiving server	Hostname of the machine that received the communication
msg	message (1023)	Message subject	Subject of the message, from the RFC5233 header "Subject:"
suser	sourceUserName (1023)	SMTP sender	SMTP sender of the email (MAIL FROM)
duser	destinationUserName (1023)	SMTP recipient(s)	SMTP recipient(s) of the email (RCPT TO)
act	deviceAction (63)	Action taken	Action taken (cleaned, quarantined, etc.)
cat	deviceEventCategory (1023)	Detection category	Most significant detection (malware >> phish >> spam >> SPF/DKIM >> policy)
sourceServiceName	sourceServiceName	Type of protection	"SMTP Transport agent", "On-demand database scan", etc.
deviceExternalId	deviceExternalId	Engine version	Anti-Malware engine version, antispam engine version, e.g. "18620,7730"

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
cs1	deviceCustomString1	Anti-Malware result	Result of Anti-Malware scan, including threat name
cs1Label	deviceCustomString1Label	"Anti-Malware result"	
cs2	deviceCustomString2	Antispam result	Result of Antispam scan, including reason for marking as spam
cs2Label	deviceCustomString2Label	"Antispam result"	
cs3	deviceCustomString3	Anti-Phishing result	Result of Anti-Phishing scan, including detected URL
cs3Label	deviceCustomString3Label	"Anti-Phishing result"	
cs4	deviceCustomString4	SPF/DKIM/DMARC result	Result of SPF/DKIM/DMARC check, in RFC7601 format
cs4Label	deviceCustomString4Label	"SPF/DKIM/DMARC result"	
cs5	deviceCustomString5	"From:" sender	Sender address from RFC5322 header "From:"
cs5Label	deviceCustomString5Label	"From header"	
cs6	deviceCustomString6	"To:" and "Cc:" recipients	Recipients addresses from RFC5322 headers "To:" and "Cc:"
cs6Label	deviceCustomString6Label	"To and Cc headers"	
fname	filename (1023)	Attachment name	Name of the first detected attachment
fileHash	fileHash (255)	Attachment hash	Hash of the first detected attachment
fsize	fileSize	Attachment size	Size of the first detected attachment
reason	reason (1023)	Rule/policy activated	Name of the policy triggered by the email or it's content
ESETEMSXFileDetails	ESETEMSXFileDetails	File details	Information about all detected attachments, their names, hashes and sizes

Optional

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
end	endTime	Time event has ended	The time at which the activity ended, in milliseconds since Jan 1st 1970. Useful only if sand boxing technology is used, i.e. ESET Dynamic Threat Defense.
dtz	deviceTimeZone (255)	Timezone of the server	
request	requestURL	Detected URL	Malign or blacklisted URL extracted from mail body or mail headers. **Note:** ESET Mail Security does not provide single URL in logs due to the fact that multiple URL's can be detected in email messages by various detection components.

Proxy server

In large LAN networks, the connection of your computer to the internet can be mediated by a proxy server. If this is the case, the following settings need to be defined. If you do not define the settings, the program will not be able to update itself automatically. In ESET Mail Security, proxy server setup is available in two different sections within the **Advanced setup** window (**F5**):

1. **Advanced setup** (**F5**) > **Update** > **Profiles** > **Updates** > **Connection options** > HTTP Proxy
This setting applies for the given update profile and is recommended for laptops that often receive modules from different locations.

2. **Advanced setup** (**F5**) > **Tools** > **Proxy server**
Specifying the proxy server at this level defines global proxy server settings for all of ESET Mail Security. Parameters here will be used by all modules that connect to the internet.

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

Proxy server requires authentication

If network communication via proxy server requires authentication, enable this option and specify **Username** and **Password**.

Detect proxy server

Click **Detect** to automatically detect and populate proxy server settings. The parameters specified in Internet Explorer will be copied.

> NOTE
> This feature does not retrieve authentication data (username and password); you must supply it.

Use direct connection if proxy is not available

If a product is configured to utilize HTTP Proxy and the proxy is unreachable, the product will bypass the proxy and communicate directly with ESET servers.

Notifications

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

Show notification about successful update

When an update is successful, a pop-up notification will be displayed.

Send event notifications by email

Enable to activate email notifications.

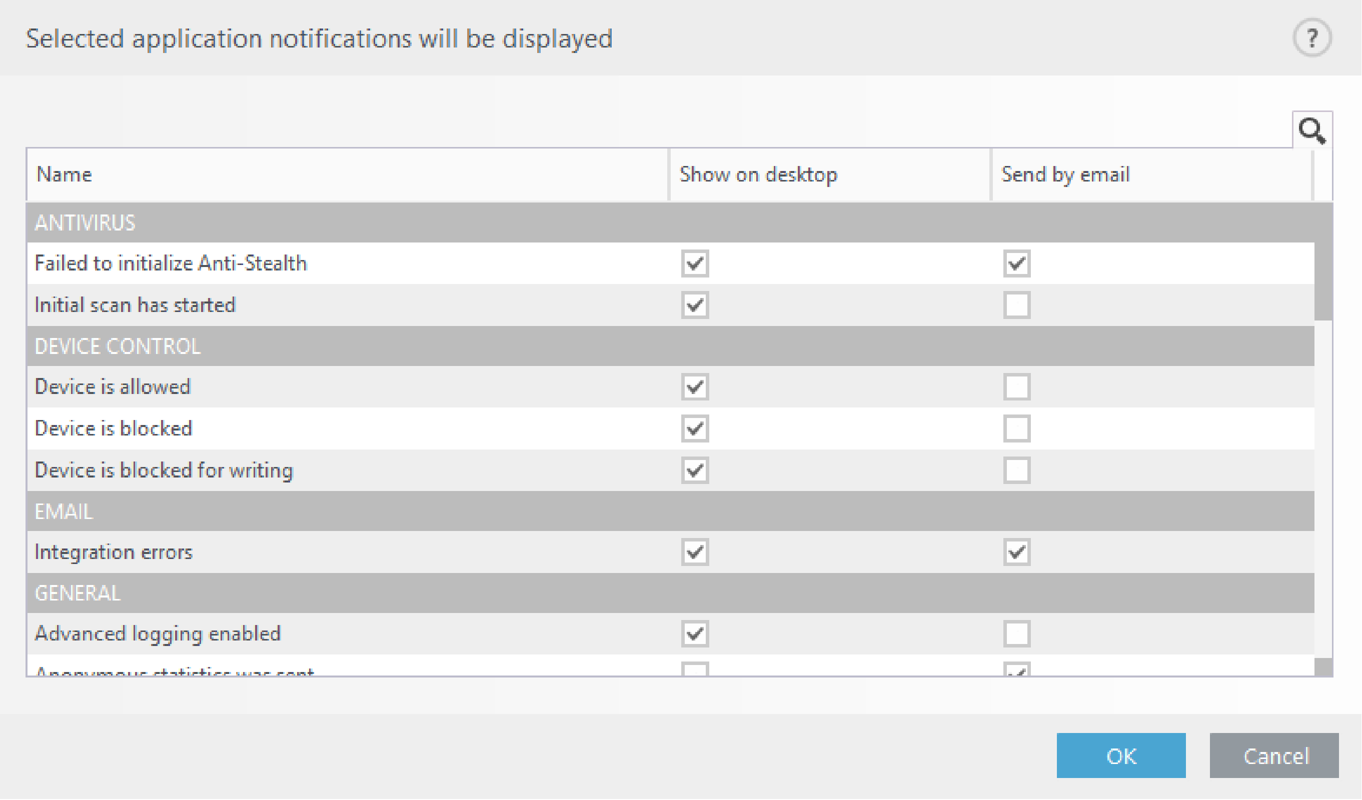
Application notifications

Click Edit to enable or disable display application notifications.

Application notifications

You can configure ESET Mail Security notifications to be shown on desktop and/or be sent by email.

NOTE
For email notifications, make sure to enable **Send event notifications by email** in **Basic** section, then configure SMTP server and other details as needed.



Selected application notifications will be displayed

Name	Show on desktop	Send by email
ANTIVIRUS		
Failed to initialize Anti-Stealth	☑	☑
Initial scan has started	☑	□
DEVICE CONTROL		
Device is allowed	☑	□
Device is blocked	☑	□
Device is blocked for writing	☑	□
EMAIL		
Integration errors	☑	☑
GENERAL		
Advanced logging enabled	☑	□
Anonymous statistics was sent	□	☑

Desktop notifications

You can configure how threat alerts and system notifications (such as successful update messages) are handled by ESET Mail Security. For example, the display time **Duration** and **Transparency** of system tray notifications (this applies only to the systems that support system tray notifications).

Minimum verbosity of events to display drop-down menu enables you to select the severity level of alerts and notification. The following options are available:

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

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

Email notifications

ESET Mail Security can automatically send notification emails if an event with the selected verbosity level occurs.

> NOTE
> SMTP servers with TLS encryption are supported by ESET Mail Security.

SMTP server

The name of the SMTP server used for sending alerts and notifications. This is typically the name of your Microsoft Exchange Server.

Username and password

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

Sender address

Enter sender's address that will appear in the header of notification emails. This is what the recipient will see in the **From** field.

Recipient address

Specify recipient's email address **To** whom notifications will be delivered.

Enable TLS

Enable alert and notification messages supported by TLS encryption.

Email settings

Minimum verbosity for notifications

Specifies the minimum verbosity level of notifications to be sent.

Interval after which new notification emails will be sent (min)

Interval in minutes after which new notification will be sent via email. Set this value to 0 if you want to send those notifications immediately.

Send each notification in a separate email

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

Message format

Communications between the program and a remote user or system administrator are done via emails or LAN messages (using the Windows messenger service). The default format of the alert messages and notifications will be optimal for most situations. In some circumstances, you may need to change the message format of event messages.

Format of event messages

Format of event messages that are displayed on remote computers.

Format of threat warning messages

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

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

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

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

Charset

You can choose encoding from the drop-down menu. Email message will be converted according to the selected character encoding.

Use Quoted-printable encoding

The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

Customization

This message will be shown in the footer of all selected notifications.

Default notification message

A default message to be shown in the notification footer.

Threats

Do not close malware notifications automatically

Enables malware notifications to stay on screen until you close them manually.

Use default message

You can turn off default message and specify custom **Treat notification message** that will be displayed when a threat is blocked.

Threat notification message

Enter a custom message to display when a threat is blocked.

Presentation mode

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

Enable Presentation mode when running applications in full-screen mode automatically

Presentation mode is activated automatically whenever you run a full-screen application. With Presentation mode engaged, you will not be able to see notifications or a status change of your ESET Mail Security.

Disable Presentation mode automatically after

To define the amount of time in minutes after which Presentation mode will automatically be disabled.

Diagnostics

Diagnostics provides application crash dumps of ESET processes (for example, *ekrn*). If an application crashes, a dump will be generated. This can help developers debug and fix various ESET Mail Security problems.

Click the drop-down menu next to **Dump type** and select one of three available options:

- **Disable** - To disable this feature.
- **Mini** - (default) Records the smallest set of useful information that may help identify why the application crashed unexpectedly. This kind of dump file can be useful when space is limited. However, because of the limited information included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.
- **Full** - Records all the contents of system memory when the application stops unexpectedly. A complete memory dump may contain data from processes that were running when the memory dump was collected.

Target directory

Directory where the dump during the crash will be generated.

Open diagnostics folder

Click **Open** to open this directory within a new *Windows Explorer* window.

Create diagnostic dump

Click **Create** to create diagnostic dump files in the Target directory.

⊟ Advanced logging

Enable Device control advanced logging

Record all events that occur in Device control to allow diagnosing and solving problems.

Enable Kernel advanced logging

Record all events that occur in ESET kernel service (`ekrn`) to allow diagnosing and solving problems.

Enable Licensing advanced logging

Record all product communication with license server.

Enable Network protection advanced logging

Record all network data passing through network protection in PCAP format in order to help developers diagnose and fix the problems related to network protection.

Enable Operating System advanced logging

Additional information about Operating system such as running processes, CPU activity, disc operations will be gathered.

Enable Protocol filtering advanced logging

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

Enable Update engine advanced logging

Record all events that occur during update process to help developers diagnose and fix the problems related to Update engine.

Technical support

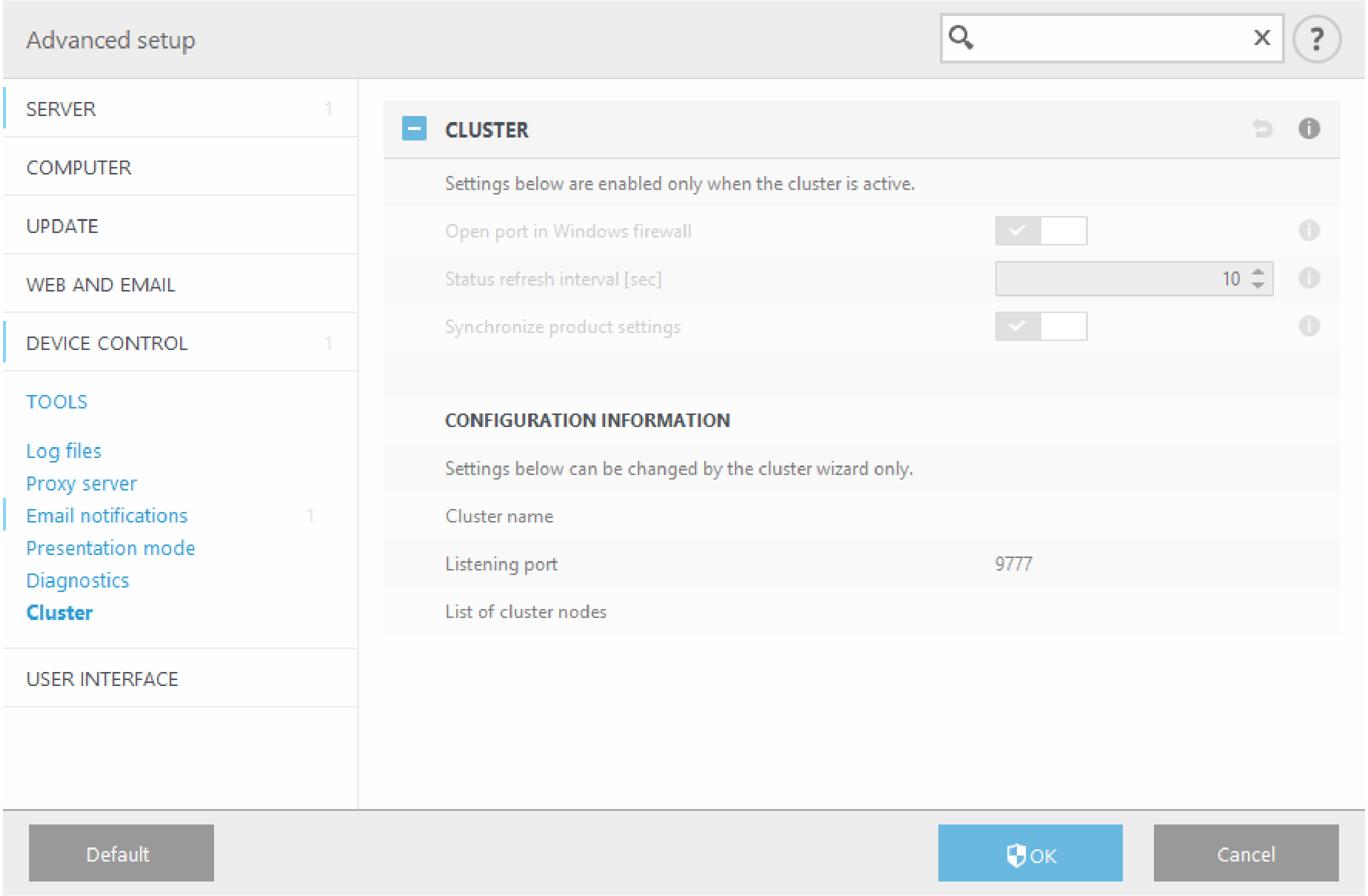
Submit system configuration data

Select **Always submit** not to be prompted before submitting your ESET Mail Security configuration data to customer care, or use **Ask before submission**.

Cluster

Enable Cluster is automatically enabled when the ESET Cluster is configured. You can disable it manually in the **Advanced setup** (**F5**) window by clicking the switch icon (for example, when you need to change configuration without affecting other nodes in the ESET Cluster). This switch only enables or disables the ESET Cluster functionality. To set up or destroy the cluster, to use the Cluster wizard or **Destroy** the cluster located in the **Tools** > **Cluster** section of the main program window.

ESET Cluster not configured and disabled:



Advanced setup

CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall ✓

Status refresh interval [sec] 10

Synchronize product settings ✓

CONFIGURATION INFORMATION

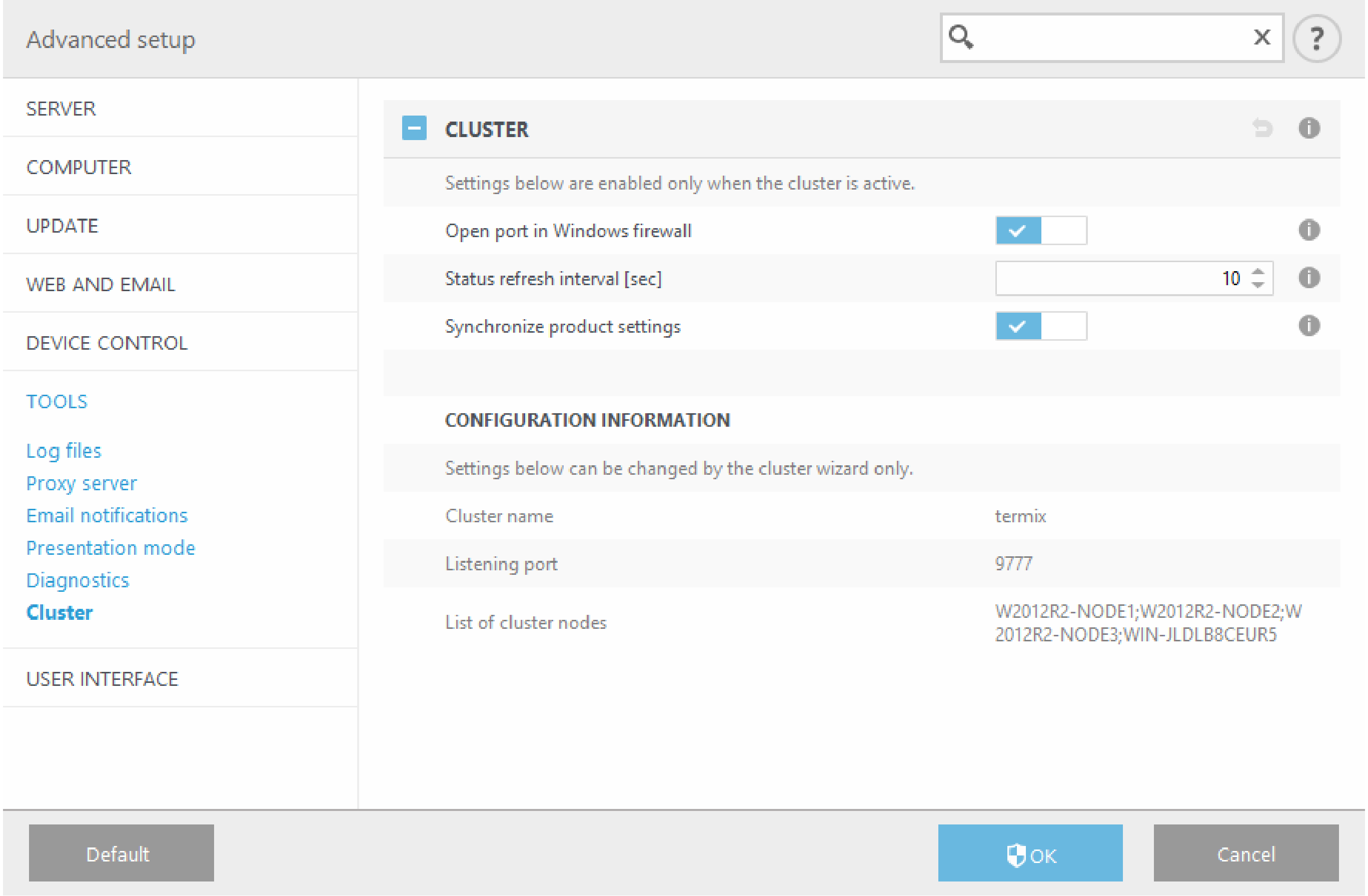
Settings below can be changed by the cluster wizard only.

Cluster name

Listening port 9777

List of cluster nodes

ESET Cluster properly configured with its details and options:



CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall ✓

Status refresh interval [sec] 10

Synchronize product settings ✓

CONFIGURATION INFORMATION

Settings below can be changed by the cluster wizard only.

Cluster name	termix
Listening port	9777
List of cluster nodes	W2012R2-NODE1;W2012R2-NODE2;W2012R2-NODE3;WIN-JLDLB8CEUR5

User interface

Configure the Graphical user interface (GUI) behavior of ESET Mail Security. You can adjust the program's visual appearance and effects.

⊟ User interface elements

Use the GUI start mode drop-down menu to select from the following Graphical user interface (GUI) start modes:

- **Full** - The complete GUI will be displayed.
- **Terminal** - No notifications or alerts will be displayed. GUI can only be started by the Administrator. The user interface should be set to Terminal if graphical elements slow the performance of your computer or cause other problems. You may also want to turn off the GUI on a Terminal server. For more information about ESET Mail Security installed on Terminal server, see Disable GUI on Terminal Server topic.

Show splash-screen at startup

Disable this option if you prefer not to have the splash-screen displayed when GUI of your ESET Mail Security starts, for example when logging into the system.

Use sound signal

ESET Mail Security plays a sound when important events occur during a scan, for example, when a threat is discovered or when the scan has finished.

Integrate into the context menu

When enabled, ESET Mail Security control elements are integrated into the context menu. The context menu is displayed after right-clicking an object (file). The menu lists all of the actions that you can perform on an object.

Application statuses

Click Edit to select statuses that are displayed in the Monitoring window. Alternatively, you can use ESET Security Management Center policies ↗ to configure your application statutes. An application status will also be displayed if your product is not activated or if your license has expired.

License Information / Show license information

When enabled, messages and notifications about your license will be displayed.

Alerts and message boxes

By configuring Alerts and notifications, you can change the behavior of detected threat alerts and system notifications. These can be customized to fit your needs. If you choose not to display some notifications, they will be displayed in the Disabled messages and statuses area. Here you can check their status, show more details or remove them from this window.

Access setup

You can prevent any unauthorized changes using the Access setup tool to ensure that security remains high.

ESET Shell

You can configure access rights to product settings, features and data via eShell by changing the ESET Shell execution policy.

System tray icon

Revert all settings in this section

Alerts and message boxes

You can configure how threat alerts and system notifications (such as successful update messages) are handled by ESET Mail Security. For example, the display time **Duration** and **Transparency** of system tray notifications (this applies only to the systems that support system tray notifications).

Display interactive alerts

Disable this feature, if you want to prevent ESET Mail Security from displaying alerts in Windows notification area.

List of interactive alerts

Useful for automation. Deselect **Ask user** for items you want to automate, and choose what action will be taken instead of the alert window waiting for you interaction.

Message boxes are used to display short text messages or questions.

Close message boxes automatically

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

Confirmation messages

When you click **Edit**, a pop-up window will open with a list of confirmation messages that ESET Mail Security displays before an action is performed. Use the check boxes to customize your preferences for confirmation messages.

Access setup

For maximum security of your system, it is essential that ESET Mail Security is correctly configured. Any unqualified modifications may result in issues or even a loss of important data. To avoid unqualified modifications, you can have your ESET Mail Security configuration password protected.

> IMPORTANT
> If you are uninstalling ESET Mail Security while using access setup password protection, you will be prompted to enter the password. You will otherwise not be able to uninstall ESET Mail Security.

Password protect settings

Locks/unlocks the program's setup parameters. Click to open the **Password setup** window.

Set password

To set or change a password to protect setup parameters, click **Set**. To protect the setup parameters of ESET Mail Security in order to avoid unauthorized modification, a new password must be set. When you want to change an existing password, type your old password in the **Old password** field, enter your new password in the **New password** and **Confirm password** fields and then click **OK**. This password will be required for any future modifications to ESET Mail Security.

Require full administrator rights for limited administrator accounts

Select this option to prompt the current user (who does not have administrator's rights) to enter administrator account credentials when modifying certain parameters, such as disabling protection modules.

> NOTE
> If the Access Setup password changes and you want to import an existing *.xml* configuration file (that was signed before the password change) using the ESET CMD command line, make sure to sign it again using your current password. This allows you to use older configuration file without the need to export it on the other machine running ESET Mail Security before the import.

ESET Shell

You can configure access rights to product settings, features and data via eShell by changing the **ESET Shell execution policy**. The default setting is **Limited scripting**, but you can change it to Disabled, Read-only or Full access if needed.

Disabled

eShell cannot be used at all. Only the configuration of eShell itself is allowed - in `ui eshell` context. You can customize the appearance of eShell, but cannot access product settings or data.

Read only

eShell can be used as a monitoring tool. You can view all settings in both Interactive and Batch mode, but you cannot modify any settings or features or modify any data.

Limited scripting

In Interactive mode, you can view and modify all settings, features and data. In Batch mode eShell will function as if you were in Read-only mode; however, if you use signed batch files, you will be able to edit settings and modify data.

Full access

Access to all settings is unlimited in both Interactive and Batch mode (when running batch files). You can view and modify any setting. You must use an administrator account to run eShell with full access. If UAC is enabled, elevation is also required.

Disable GUI on Terminal Server

This chapter describes how to disable the GUI of ESET Mail Security running on Windows Terminal Server for user sessions.

Normally, the ESET Mail Security GUI starts up every time a remote user logs onto the server and creates a terminal session. This is usually undesirable on Terminal Servers. If you want to turn off the GUI for terminal sessions, you can do so via eShell by running `set ui ui gui-start-mode none` command. This will put the GUI into terminal mode. These are the two available modes for GUI startup:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

If you want to find out what mode is currently in use, run the command `get ui ui gui-start-mode`.

NOTE
If you have installed ESET Mail Security on a Citrix server, we recommend that you use the settings described in our Knowledgebase article.

Disabled messages and statuses

Confirmation messages

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

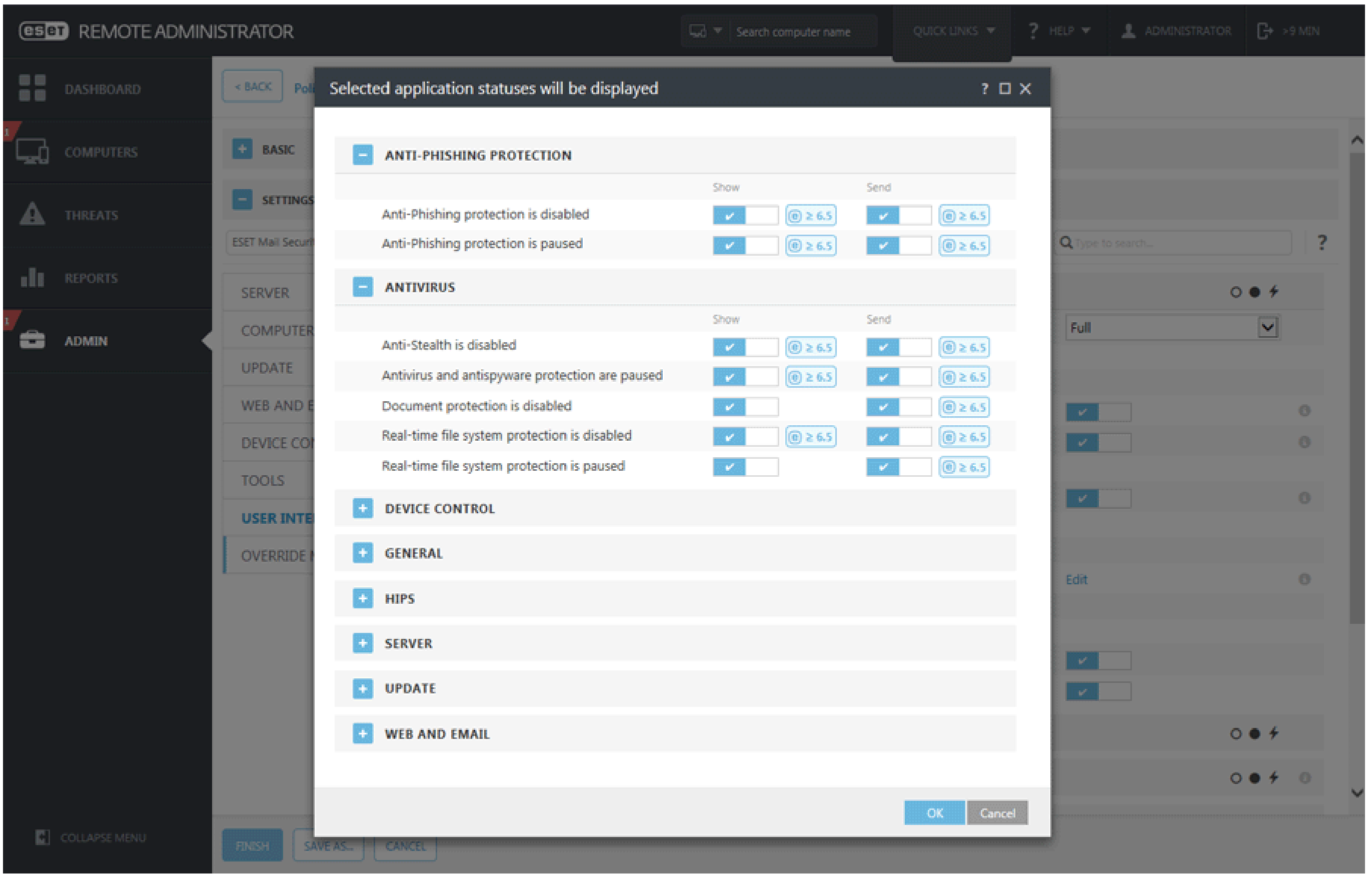
Application statuses settings

Allows you to enable or disable display status in the Monitoring page in main menu.

Application statuses settings

This dialog window lets you select or deselect which application statuses will be or will not be displayed. For example, when you pause Antivirus and antispyware protection that will result in a change of protection status which will appear in Monitoring page. An application status will also be displayed if your product is not activated or if your license has expired.

Application statuses can be managed via ESET Security Management Center policies. Categories and statutes are shown in a list with two options **Show** and **Send** the status. Send column for application statuses is visible only in ESET Security Management Center policy configuration. ESET Mail Security shows settings with lock icon. You can use Override mode to temporarily change Application statuses.



Selected application statuses will be displayed

ANTI-PHISHING PROTECTION

	Show		Send	
Anti-Phishing protection is disabled	✓	≥ 6.5	✓	≥ 6.5
Anti-Phishing protection is paused	✓	≥ 6.5	✓	≥ 6.5

ANTIVIRUS

	Show		Send	
Anti-Stealth is disabled	✓	≥ 6.5	✓	≥ 6.5
Antivirus and antispyware protection are paused	✓	≥ 6.5	✓	≥ 6.5
Document protection is disabled	✓		✓	≥ 6.5
Real-time file system protection is disabled	✓	≥ 6.5	✓	≥ 6.5
Real-time file system protection is paused	✓		✓	≥ 6.5

DEVICE CONTROL

GENERAL

HIPS

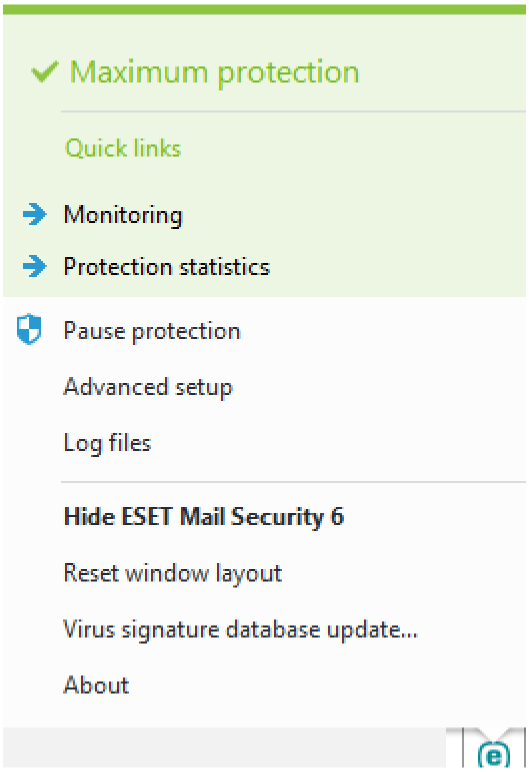
SERVER

UPDATE

WEB AND EMAIL

System tray icon

Serves as a quick access to frequently used items and features of ESET Mail Security. These are available by right-clicking the system tray icon ⓔ.



More information

Opens Monitoring page to show you the current protection status and messages.

Pause protection

Displays the confirmation dialog box that disables Antivirus and antispyware protection, which guards against attacks by controlling file, web and email communication. When you temporarily pause the Antivirus and antispyware protection using the system tray icon ⓔ, the **Pause protection** dialog box will appear. This will disable malware-related protection for the chosen period of time. To disable protection permanently, you can do so in **Advanced setup**. Use caution when disabling protection, your system will be exposed to threats.

Advanced setup

Use this option to enter the **Advanced setup**.

Log files

Contains information about all important program events that have occurred and provide an overview of detected threats.

Hide ESET Mail Security

Hide the ESET Mail Security window from the screen.

Reset window layout

Resets the ESET Mail Security window to its default size and position on the screen.

Check for updates

Starts updating modules to ensure your level of protection against malicious code.

About

Provides system information, details about the installed version of ESET Mail Security and the installed program modules as well as your license expiration date. Information about your operating system and system resources can be found at the bottom of the page.

Revert to default settings

You can restore settings to their default values within **Advanced setup**. There are two options. You can revert everything to default or revert settings only for a particular section (settings in other sections will remain unchanged).

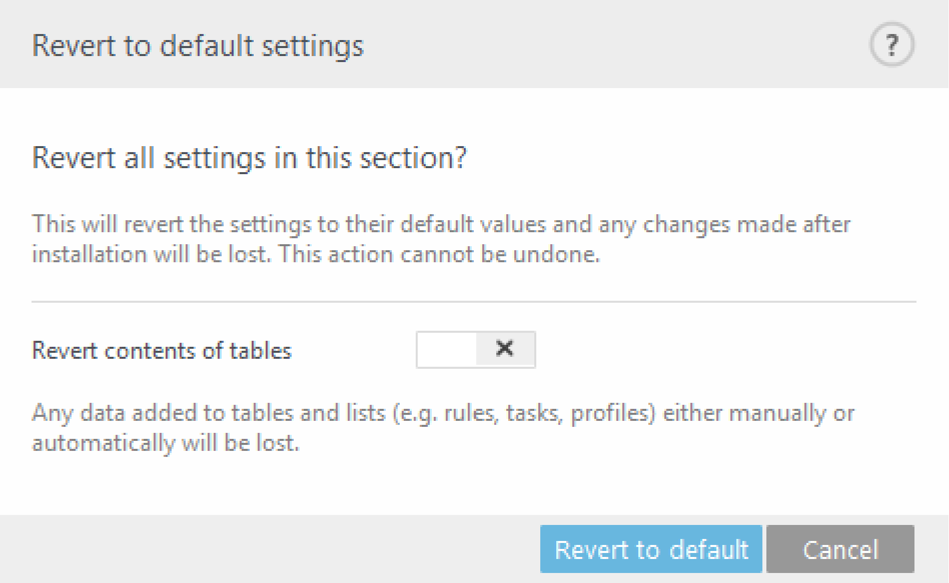
Revert all settings

All settings in all sections of advanced setup will be restored to the state they were after you have installed ESET Mail Security. You can think of it as *Restore Factory Defaults*.

> NOTE
> Once you click **Revert to default**, all changes that have been made will be lost. This action cannot be undone.

Revert all settings in this section

Reverts module settings in selected section to values. Any changes you have made in this section will be lost.



Revert to default settings

Revert all settings in this section?

This will revert the settings to their default values and any changes made after installation will be lost. This action cannot be undone.

Revert contents of tables ☒

Any data added to tables and lists (e.g. rules, tasks, profiles) either manually or automatically will be lost.

Revert contents of tables

When enabled, the rules, tasks or profiles, which were added manually or automatically, will be lost.

Help and support

ESET Mail Security contains troubleshooting tools and support information that will assist you in solving issues that you may encounter.

Help

Search ESET Knowledgebase

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

Open help

Launches online help pages for ESET Mail Security.

Find quick solution

Select this to find solutions to the most frequently encountered problems. We recommend that you read this section before contacting technical support.

Technical Support

Submit support request

If you cannot find an answer to your problem, you can also use this form located on the ESET website to quickly contact our Technical Support department.

Details for Technical Support

Display details information (Product name, Product version,etc.) for Technical Support.

Support Tools

Threat encyclopedia

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

ESET Log Collector

Log Collector is an application that automatically collects information, such as configuration and logs from your server in order to help resolve issues more quickly.

Detection Engine history

Links to ESET Virus radar, which contains information about versions of the ESET detection modules.

ESET Specialized Cleaner

The ESET Specialized Cleaner is a removal tool for common malware infections such as Conficker, Sirefef, Necurs, etc.

Product and License information

Activate product / Change license

Click to launch the Product activation window. Select one of the available methods to activate ESET Mail Security.

About ESET Mail Security

Displays information about your copy of ESET Mail Security.

Submit support request

In order to provide assistance as quickly and accurate as possible, ESET requires information about your ESET Mail Security configuration, detailed system information, running processes (ESET SysInspector log file) and registry data. ESET will only use this data to provide technical assistance to the customer. This setting can also be configured from the **Advanced setup** (**F5**) > **Tools** > **Diagnostics** > **Technical Support**.

> NOTE
> If you choose to submit system data you must fill and submit the web form, otherwise your ticket will not be created and your system data will be lost.

When you submit the web form, your system configuration data will be sent to ESET. Select **Always submit this information** to remember this action for this process.

Don't submit data

Use this option if you do not wish to submit data. You will be redirected to ESET Technical Support web page.

About ESET Mail Security

This window provides details about the installed version of ESET Mail Security. The top part of the window contains information about your operating system and system resources, the current user and full computer name.

Installed components

Contain information about modules, to view a list of installed components and their details. Click **Copy** to copy the list to your clipboard. This may be useful during troubleshooting or when contacting Technical Support.

Glossary

Visit Glossary page for more information about technical terms, threats and internet security.

End User License Agreement

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement (hereinafter referred to as "the Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement. If You do not agree to all of the terms and conditions of this Agreement, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software (hereinafter referred to as " Documentation "); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smart phones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights (hereinafter referred to as "License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one computer system; or (ii) if the extent of a license is bound to the number of mail boxes, then one End User shall be taken to refer to a computer user who accepts electronic mail via a Mail User Agent (hereinafter referred to as "MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent in which has the right to use the Software in accordance the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Business Edition.** A Business Edition version of the Software must be obtained to use the Software on mail servers, mail relays, mail gateways or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** OEM Software shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall be also entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software.** The Provider shall be entitled from time to issue updates to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled automatic installation of Updates. For the purpose of provisioning of Updates, License authenticity verification is required including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

b) **Forwarding of infiltrations and information to the Provider.** The Software contains functions which collect samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames (hereinafter referred to as "Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed, information about the operations and functionality of the Software and information about devices in local network such as type, vendor, model and/or name of device (hereinafter referred to as "Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations to Provider. This function is enabled under the Software's standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer. You hereby agree to receive notification and messages including but not limited to marketing information.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival back-up copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement**. This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all back-up copies and all related materials provided by the Provider or its business partners. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE

WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software**. The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities,

including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any act, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. In case of a discrepancy between language versions of this Agreement, the English version shall prevail. This Agreement may only be modified in written form, signed by an authorized representative of the Provider, or a person expressly authorized to act in this capacity under the terms of a power

of attorney.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

EULA ID: BUS-STANDARD-20-01

Privacy Policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Update and other statistics covering information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, IP address, MAC address, configuration settings of product.
- One-way hashes related to infiltrations as part of ESET LiveGrid® Reputation System which improves the efficiency of our anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.
- Suspicious samples and metadata from the wild as part of ESET LiveGrid® Feedback System which enables ESET to react immediately to needs of our end users and keep us responsive to the latest threats providing. We are dependent on You sending us
    - infiltrations such as potential samples of viruses and other malicious programs and suspicious; problematic, potentially unwanted or potentially unsafe objects such as executable files, email messages reported by You as spam or flagged by our product;
    - information about devices in local network such as type, vendor, model and/or name of device;
    - information concerning the use of internet such as IP address and geographic information, IP packets, URLs and ethernet frames;
    - crash dump files and information contained.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it.

Accidentally collected data may be included in malware itself (collected without your knowledge or approval) or as part of filenames or URLs and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

- Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.
- Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject’s Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

- right to request access to your personal data from ESET,
- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),
- right to request erasure of your personal data,
- right to request restriction of processing your personal data,
- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk