# ESET Security for Microsoft SharePoint

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

Copyright ©2024 by ESET, spol. s r.o.

ESET Security for Microsoft SharePoint was developed by ESET, spol. s r.o.

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

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

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. 1/30/2024

1 Overview ..... 1
**1.1 Key Features** ..... 1
**1.2 What's new** ..... 2
**1.3 Deployment** ..... 3
1.3 SharePoint Farm deployment ..... 3
1.3 Installation in a cluster environment ..... 4
**1.4 SharePoint protection types** ..... 4
1.4 Integration into SharePoint ..... 4
1.4 On-access filter ..... 4
1.4 On-demand database scan ..... 5
2 Preparing for installation ..... 6
**2.1 System requirements** ..... 8
**2.2 ESET Security for Microsoft SharePoint installation steps** ..... 9
2.2 Export settings or remove installation ..... 12
2.2 Initial modules update ..... 12
**2.3 Silent / Unattended installation** ..... 13
2.3 Command line installation ..... 14
**2.4 Product activation** ..... 17
2.4 Activation successful ..... 19
2.4 Activation failure ..... 19
2.4 License ..... 19
**2.5 Upgrade to the latest version** ..... 19
2.5 Upgrading via ESET PROTECT ..... 20
2.5 Upgrading via ESET Cluster ..... 21
**2.6 Terminal server** ..... 24
3 Getting started ..... 24
**3.1 Managed via ESET PROTECT** ..... 25
**3.2 Monitoring** ..... 25
3.2 Windows update available ..... 27
3.2 Network isolation ..... 28
4 Using ESET Security for Microsoft SharePoint ..... 29
**4.1 Scan** ..... 29
4.1 Scan window and scan log ..... 31
**4.2 Log files** ..... 33
4.2 Log filtering ..... 36
**4.3 Update** ..... 38
**4.4 Setup** ..... 40
4.4 Server ..... 41
4.4 Computer ..... 42
4.4 Network ..... 44
4.4 Network troubleshooting wizard ..... 45
4.4 Web and email ..... 45
4.4 Tools - Diagnostic logging ..... 46
4.4 Import and export settings ..... 47
**4.5 Tools** ..... 48
4.5 Running processes ..... 49
4.5 Protection statistics ..... 51
4.5 Cluster ..... 53
4.5 Cluster wizard - Select nodes ..... 54
4.5 Cluster wizard - Cluster settings ..... 55

4.5 Cluster wizard - Cluster setup settings ..... 56
4.5 Cluster wizard - Nodes check ..... 56
4.5 Cluster wizard - Nodes install ..... 58
4.5 ESET Shell ..... 60
4.5 Usage ..... 62
4.5 Commands ..... 67
4.5 Keyboard shortcuts ..... 70
4.5 Batch files / Scripting ..... 71
4.5 ESET SysInspector ..... 72
4.5 ESET SysRescue Live ..... 72
4.5 Scheduler ..... 73
4.5 Scheduler - Add task ..... 74
4.5 Task type ..... 77
4.5 Task execution ..... 78
4.5 Event triggered ..... 78
4.5 Run application ..... 79
4.5 Skipped task ..... 79
4.5 Scheduled task overview ..... 79
4.5 Submit samples for analysis ..... 79
4.5 Suspicious file ..... 80
4.5 Suspicious site ..... 81
4.5 False positive file ..... 81
4.5 False positive site ..... 82
4.5 Other ..... 82
4.5 Quarantine ..... 82
5 Server protection settings ..... 84
**5.1 Performance Counters** ..... 85
**5.2 On-access filter** ..... 87
5.2 Antivirus and antispyware ..... 89
**5.3 On-demand database scan** ..... 90
5.3 On-demand database scan targets ..... 91
5.3 Antivirus and antispyware ..... 93
**5.4 Rules** ..... 94
5.4 Rules list ..... 94
5.4 Rule wizard ..... 95
5.4 Rule condition ..... 97
5.4 Rule action ..... 98
6 General settings ..... 99
**6.1 Computer** ..... 99
6.1 Machine learning protection ..... 101
6.1 Exclusions ..... 104
6.1 Performance exclusions ..... 104
6.1 Detection exlusions ..... 105
6.1 Create exclusion wizard ..... 107
6.1 Advanced options ..... 107
6.1 Automatic exclusions ..... 107
6.1 An infiltration is detected ..... 108
6.1 Real-time file system protection ..... 109
6.1 ThreatSense parameters ..... 111
6.1 Additional ThreatSense parameters ..... 114
6.1 File extenstions excluded from scanning ..... 114

6.1 Processes exclusions ... 114
6.1 Cloud-based protection ... 115
6.1 Exclusion filter ... 117
6.1 Malware scans ... 118
6.1 Profile manager ... 118
6.1 Profile targets ... 119
6.1 Scan targets ... 121
6.1 Idle-state scan ... 123
6.1 Startup scan ... 123
6.1 Automatic startup file check ... 123
6.1 Removable media ... 125
6.1 Document protection ... 125
6.1 Hyper-V scan ... 126
6.1 HIPS ... 128
6.1 HIPS rule settings ... 130
6.1 HIPS advanced settings ... 132
**6.2 Update configuration** ... 133
6.2 Update rollback ... 137
6.2 Scheduled Task - Update ... 138
6.2 Update mirror ... 138
**6.3 Network protection** ... 139
6.3 Known networks ... 140
6.3 Add network ... 140
6.3 Zones ... 142
**6.4 Network attack protection** ... 143
6.4 IDS exceptions ... 144
6.4 Suspected threat blocked ... 144
6.4 Temporary IP address blacklist ... 145
6.4 Brute-force attack protection ... 145
6.4 Brute-force attack protection rules ... 146
6.4 Brute-force attack protection exclusions ... 146
**6.5 Web and email** ... 146
6.5 Protocol filtering ... 147
6.5 Web and email clients ... 148
6.5 SSL/TLS ... 148
6.5 List of known certificates ... 149
6.5 Encrypted SSL communication ... 150
6.5 Email client protection ... 151
6.5 Email protocols ... 152
6.5 Email tags ... 153
6.5 Microsoft Outlook toolbar ... 153
6.5 Outlook Express and Windows Mail toolbar ... 154
6.5 Confirmation dialog ... 154
6.5 Rescan messages ... 154
6.5 Web access protection ... 155
6.5 URL address management ... 155
6.5 Create new list ... 156
6.5 Anti-Phishing web protection ... 158
**6.6 Device control** ... 159
6.6 Device rules ... 160
6.6 Device groups ... 162

**6.7 Tools configuration** ..... 163
6.7 Time slots ..... 164
6.7 Microsoft Windows update ..... 164
6.7 Command line scanner ..... 164
6.7 ESET CMD ..... 167
6.7 ESET RMM ..... 168
6.7 License ..... 169
6.7 WMI Provider ..... 169
6.7 Provided data ..... 170
6.7 Accessing Provided Data ..... 180
6.7 ESET Management console scan targets ..... 180
6.7 Override mode ..... 181
6.7 Log files ..... 183
6.7 Proxy server ..... 184
6.7 Presentation mode ..... 185
6.7 Diagnostics ..... 185
6.7 Technical support ..... 186
6.7 Cluster ..... 187
**6.8 User interface** ..... 188
6.8 Access setup ..... 189
6.8 ESET Shell ..... 190
6.8 Disable GUI on Terminal Server ..... 190
6.8 Icon in the Windows notification area ..... 191
**6.9 Notifications** ..... 192
6.9 Application statuses ..... 192
6.9 Disabled messages and statuses ..... 193
6.9 Desktop notifications ..... 193
6.9 Customization ..... 194
6.9 Desktop notifications ..... 195
6.9 Interactive alerts ..... 195
6.9 Forwarding ..... 196
**6.10 Revert to default settings** ..... 198
**6.11 Help and support** ..... 199
6.11 Submit support request ..... 199
6.11 About ESET Security for Microsoft SharePoint ..... 200
**6.12 Glossary** ..... 200
7 End User License Agreement ..... 200
8 Privacy Policy ..... 207

# Overview

ESET Security for Microsoft SharePoint is an integrated solution specifically designed for Microsoft SharePoint products running on Microsoft Windows Server in a standalone or farm configuration. It delivers effective and robust protection against various malware, viruses and other infiltrations. ESET Security for Microsoft SharePoint works by protecting files stored in the SharePoint content database. User-provided files stored in document libraries, asset libraries, wiki pages, ASP pages, (JavaScript) scripts, and images that form the SharePoint site are protected.

**ESET Security for Microsoft SharePoint protects your content by:**

- filtering during file access (on-access filter)
- using the on-demand database scan (On-demand scan)

The on-access filter is run at SharePoint's discretion, and its behavior differs slightly depending on the SharePoint generation installed. In general, an on-access filter is run when any file is first accessed, and the result of the scan is cached until the virus database version changes or sometimes elapses.

On-demand scan hierarchically crawls all the files and directories of a website the administrator selects. Files are accessed using the SharePoint object model (.NET based), which provides a unified view of all content stored on a SharePoint farm and abstracts the actual database server technology used.

**Both the on-access filter and On-demand scan apply the following checks:**

- Antivirus and antispyware protection
- User-defined rules with different condition types

# Key Features

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

| True 64-bit product core | Adding higher performance and stability to the product core components. |
|---|---|
| Performance Counters | ESET Security for Microsoft SharePoint Counters enable you to monitor the overall ESET Security for Microsoft SharePoint performance. |
| On-access filter | File protection that works by filtering during file access. |
| On-demand scan | File protection by database scan, initiated by user or scheduled to run at a certain time. |
| User defined rules | Allow administrators to create and manage custom rules for file filtering by defining conditions and actions to take with filtered files. |
| Automatic exclusions | Automatic detection and exclusion of critical applications and server files for smooth operation and performance. |
| Self-Defense | Protects ESET security solutions from being modified or deactivated. |
| Effective Troubleshooting | Built-in tools for resolving various issues: ESET SysInspector for system diagnostics and ESET SysRescue Live to create a bootable rescue CD or USB. |

| True 64-bit product core | Adding higher performance and stability to the product core components. |
| --- | --- |
| ESET Cluster | ESET server products are able to communicate with each other and exchange data such as configuration and notifications, as well as synchronize data necessary for correct operation of a group of product instances. This provides for same configuration of the product across the whole cluster. Windows Failover Clusters and Network Load Balancing (NLB) Clusters are supported by ESET Security for Microsoft SharePoint. Additionally, you can add ESET Cluster members manually without the need for a specific Windows Cluster. ESET Clusters work in both domain and workgroup environments. |
| Component-based installation | Choose which components you want to add or remove. |
| Storage scan | Scans all shared files on a local server. This makes it easy to selectively scan only user data that is stored on the file server. |
| Processes exclusions | Excludes specific processes from Antivirus on-access scanning. Due to the critical role of dedicated servers (application server, storage server, etc.) regular backups are mandatory to guarantee timely recovery from fatal incidents of any kind. To improve backup speed, process integrity and service availability, some techniques that are known to conflict with file-level antivirus 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 antivirus 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. |
| eShell (ESET Shell) | eShell 2.0 is now available in ESET Security for Microsoft SharePoint. eShell is a command line interface that offers advanced users and administrators more comprehensive options to manage ESET server products. |
| ESET PROTECT | Better integration with ESET PROTECT including the ability to schedule On-demand scan. For more information about ESET PROTECT, see ESET PROTECT Online Help. |
| Hyper-V scan | Is a new technology that allows for scanning of Virtual Machine (VM) disks on Microsoft Hyper-V Server without the need of any "Agent" on the specific VM. |

# What's new

New features and enhancements in ESET Security for Microsoft SharePoint:

- True 64-bit product core
- Direct access to SQL database
- Performance Counters
- ESET Inspect support
- ESET RMM
- Network isolation
- Machine learning protection

- Audit logs
- micro Program Component Updates
- Brute-force attack protection

See detailed changelogs for ESET Security for Microsoft SharePoint.

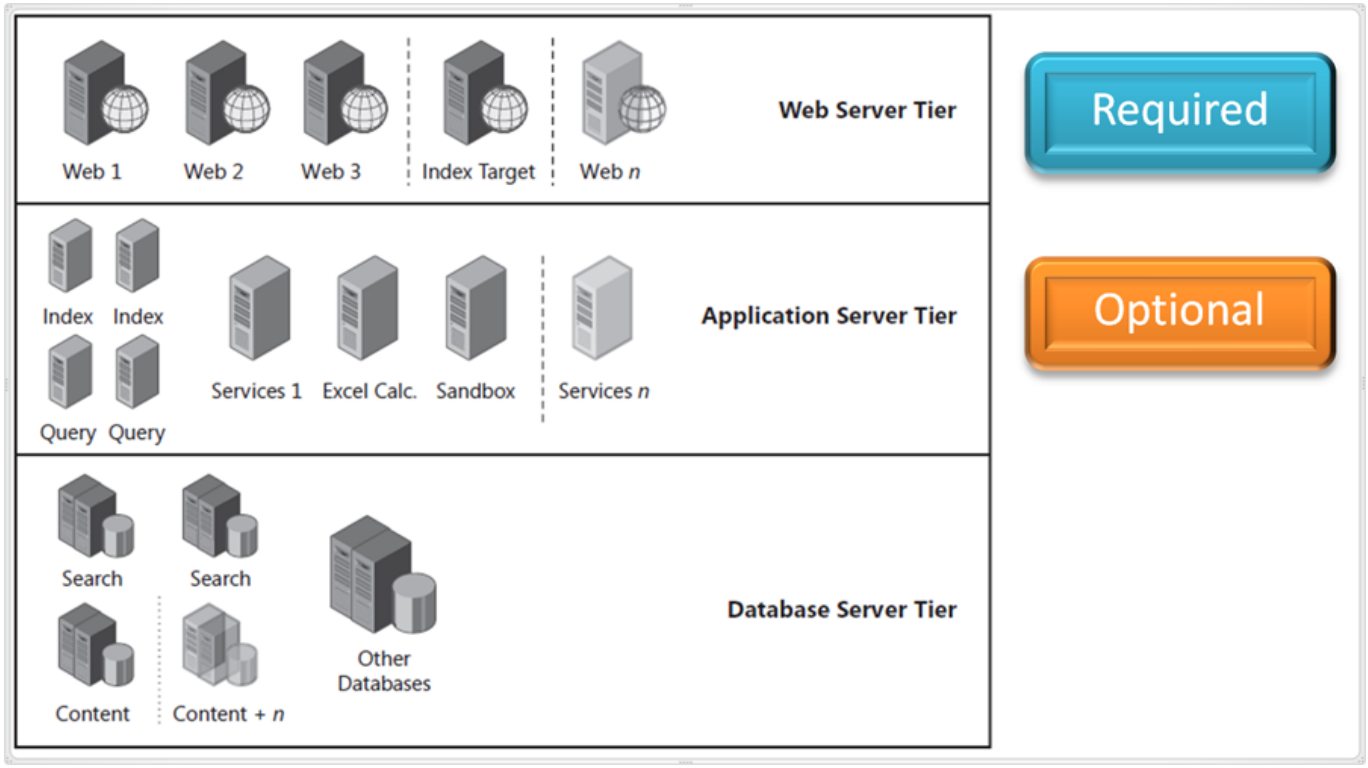
# Deployment

The following chapters will help plan the ESET Security for Microsoft SharePoint deployment to your SharePoint infrastructure, especially if you use a SharePoint Server Farm or cluster environment.

# SharePoint farm deployment

ESET Security for Microsoft SharePoint must be installed on all SharePoint machines with the Web Server role to guarantee user protection using the On-access file scanner. Any of those machines can be used to execute On-demand database scans. Optionally, ESET Security for Microsoft SharePoint can be installed on SharePoint machine(s) with the Application Server role, where it can be used to perform On-demand scans of the SharePoint content database, but cannot serve as an On-access filter.

In the diagram below, the server environment is divided to show the tiers where ESET protection is required and where it is optional.




> In a SharePoint farm setting, you only need to run the On-demand scan from one machine. The entire SharePoint farm database will be scanned.

Because On-demand scan is a resource-intensive operation, we recommend running it on a machine where increased load during the scan is not a problem. From a functional point of view, running the On-demand scan

from any SharePoint farm machine that can access the content database, regardless of its role, is fine.

The speed of On-demand scan depends heavily on the throughput of the database server and network. To increase database scanning throughput in large SharePoint farms, run On-demand scan on more than one machine and configure each machine to scan different (non-overlapping) parts of the content database. Note that this will increase the database server load, and its benefits should be evaluated by the farm administrator.

# Installation in a cluster environment

You can deploy ESET Security for Microsoft SharePoint in a cluster environment (for example, in a Failover cluster). We recommend that you install ESET Security for Microsoft SharePoint on an active node and then redistribute the installation on passive node(s) using ESET Security for Microsoft SharePoint's ESET Cluster feature. Apart from the installation, the ESET Cluster will replicate the ESET Security for Microsoft SharePoint configuration to ensure consistency between cluster nodes for correct operation.

# SharePoint protection types

**There are two ESET Security for Microsoft SharePoint SharePoint protection types:**

- Antivirus protection
- Antispyware protection

**This protection is provided by:**

- Filtering during file access (on-access filter)
- On-demand database scan (On-demand scan)

# Integration into SharePoint

This section describes the on-access filter and On-demand database scan features and how these integrate into SharePoint.

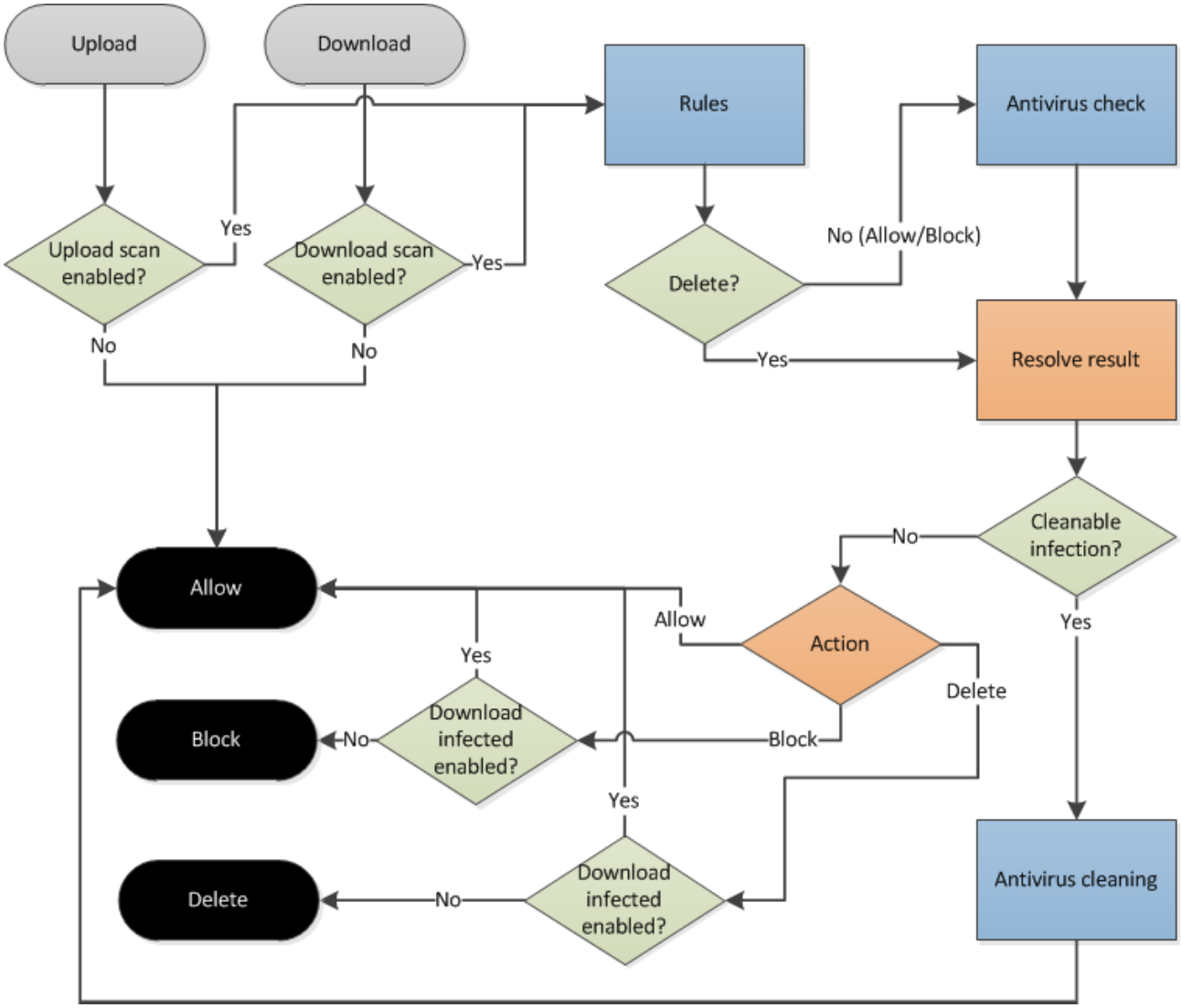
# On-access filter

The on-access filter scans all files according to ”SharePoint protection settings.“ For example, a Microsoft Office document stored in SharePoint, pictures, *.aspx* files (actual SharePoint pages), CSS styles and icons associated with the document will be scanned. The scope of the files that will be sent for scanning via VSAPI is determined by SharePoint settings.

ESET Security for Microsoft SharePoint cannot actively select which files will be scanned. When a file is sent for scanning/cleaning, its filename and size are recognized by ESET Security for Microsoft SharePoint. Details about the file, such as its owner, location and whether it will be scanned during upload or download, cannot be determined by ESET. If Scan document versions is enabled, only the current version's filename will display; for earlier versions, the alternate text will be used.

The on-access filter file scan process is shown in the diagram below. This diagram illustrates on-access filter file

scan actions:




# On-demand database scan

The On-demand database scan feature scans the SharePoint content database containing SharePoint Web sites and files. ESET Security will scan the hierarchy of files and folders corresponding to each website targeted for scanning.

If an infiltration is found, three actions (retain, clean and delete) can be performed. If deletion is executed for any reason, including during cleaning, the file is sent to the Recycle Bin. If the Recycle Bin is turned off, deletion is definitive.

If earlier versions of a specific file are present and the **Scan document versions** feature is enabled, the document's earlier versions are scanned first.

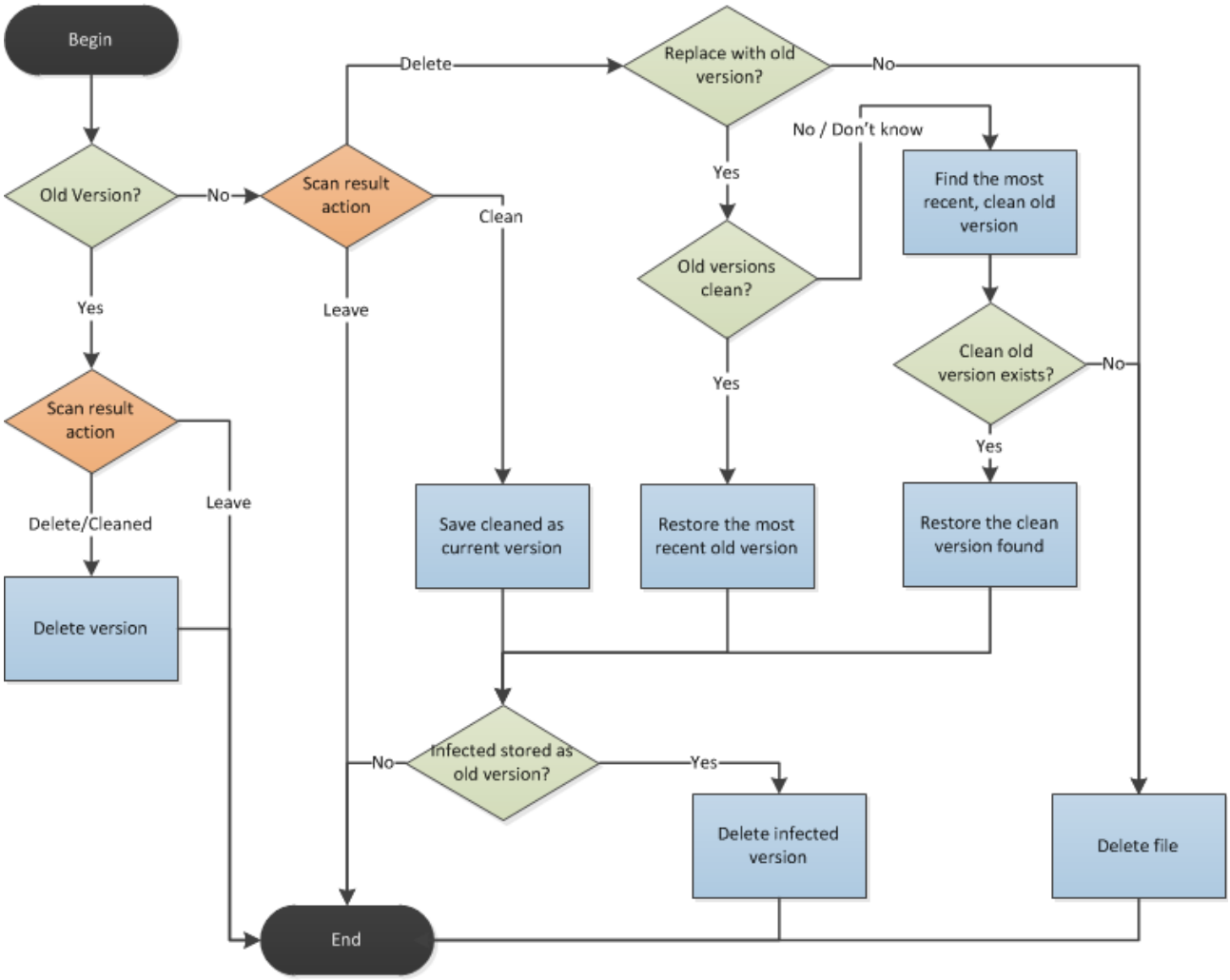
**Notes on document version scanning:**

- Earlier document versions can be scanned in ESET Security for Microsoft SharePoint settings (Scan document versions)

- If a document must be cleaned, a new version will be created, and the Infected version will be moved to the trash

- Earlier document versions cannot be cleaned; they can only be deleted
- If the most current document version is deleted, the earlier versions are kept
  - The most recent clean version will be used as the current document
  - This behavior can be activated in the settings (on document delete, restore the latest clean version) and works even if Scan document versions is disabled

This diagram illustrates file scan result processing and subsequent action(s) taken during the On-demand database scan:




# Preparing for installation

There are a few steps we recommend that you take in preparation for product installation:

- After purchasing ESET Security for Microsoft SharePoint, download the *.msi* installation package from ESET's website.
- Ensure that the server you plan to install ESET Security for Microsoft SharePoint meets system requirements.

- Log in to the server using an Administrator account.

- If you are performing an upgrade to an existing ESET Security for Microsoft SharePoint installation, we recommend that you back up the current configuration using the Export settings feature.

- Remove/uninstall any third-party antivirus software from your system. We recommend that you use the ESET AV Remover. See this Knowledgebase article for a list of third-party antivirus software that can be removed using the ESET AV Remover.

- If you are installing ESET Security for Microsoft SharePoint on Windows Server 2016, Microsoft recommends uninstalling Windows Defender (Microsoft Defender Antivirus) Features and withdrawing from Windows Defender ATP enrollment to prevent problems caused by having multiple antivirus products installed on a machine.

- If you are installing ESET Security for Microsoft SharePoint on Windows Server 2019 or Windows Server 2022, Microsoft recommends disabling Microsoft Defender Antivirus manually to prevent problems caused by having multiple antivirus products installed on a machine.

If **Windows Defender Features** are present on your Windows Server 2016, 2019 or 2022 during installation of ESET Security for Microsoft SharePoint, these features are turned off by ESET Security for Microsoft SharePoint to prevent collisions of real-time protection between multiple antivirus products. Also, Windows Defender Features are turned off by ESET Security for Microsoft SharePoint 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.

You can run ESET Security for Microsoft SharePoint installer in two installation modes:

- Main program window - The recommended installation is with the Installation Wizard.

- Silent/Unattended installation - In addition to the Installation Wizard, you can install ESET Security for Microsoft SharePoint silently via command line.

- Upgrading to the latest version - If you use an earlier ESET Security for Microsoft SharePoint version, you can choose a suitable upgrade method.

After you have successfully installed or upgraded your ESET Security for Microsoft SharePoint, further activities are:

Product activation

The available activation scenarios in the activation window may vary depending on the country and the means of distribution.

Configuring general settings

You can fine-tune your ESET Security for Microsoft SharePoint by modifying the advanced settings for each feature.

# System requirements

**Supported Operating Systems:**

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

Support for Azure Code Signing must be installed on all Windows operating systems to install or upgrade ESET products released after July 2023. More information.

**Small Business servers:**

- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials

**and any of the following application servers:**

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019 (x64) - all editions
- Microsoft SharePoint Server 2016 (x64) - all editions
- Microsoft SharePoint Server 2013 (x64) - all editions
- Microsoft SharePoint Server 2010 (x64) - all editions

**Supported Hyper-V Host Operating Systems:**

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

Hardware requirements depend on the operating system version in use. We recommend reading the Microsoft Windows Server and Microsoft SharePoint Server product documentation for detailed information on hardware requirements.

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

# ESET Security for Microsoft SharePoint installation steps

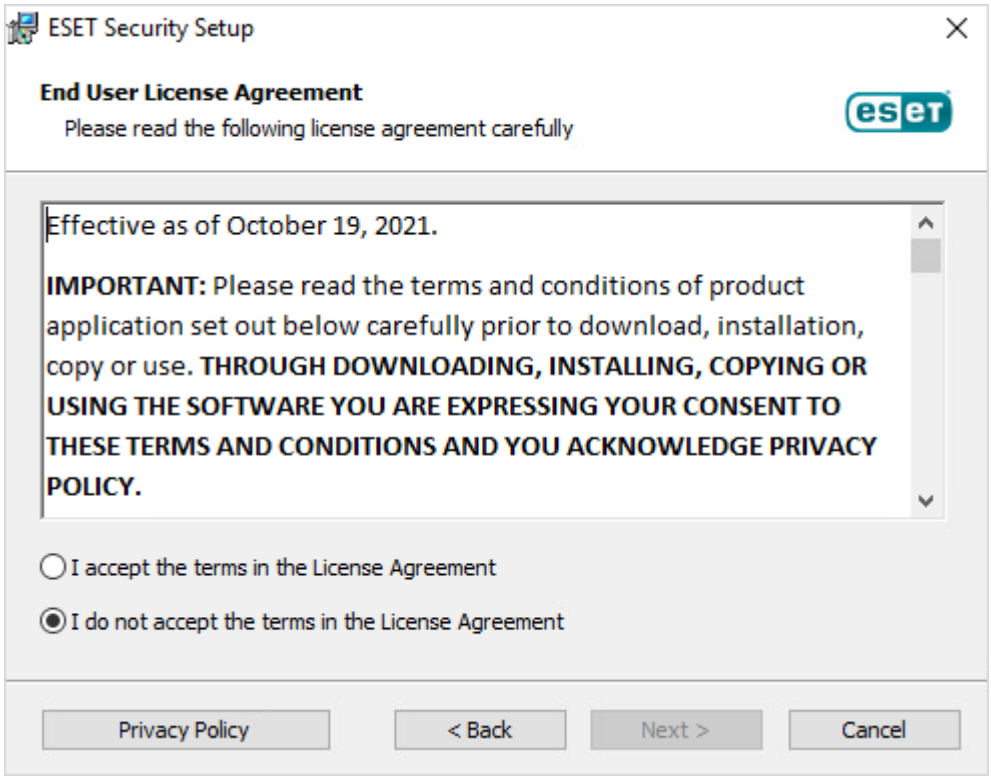
This is a typical GUI installation wizard. Double-click the .msi package and follow the steps to install ESET Security for Microsoft SharePoint:

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 Security for Microsoft SharePoint will be installed. Selected language for ESET Security for Microsoft SharePoint is independent of the language you see in the installation wizard.




3. Click **Next**, and the End User License Agreement will be displayed. After acknowledging your acceptance of the End User License Agreement and Privacy Policy, click **Next**.




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

### Complete

Installs all ESET Security for Microsoft SharePoint features.

> Installer contains only essential modules; all other modules are downloaded during the initial module update after the product activation.

### Core

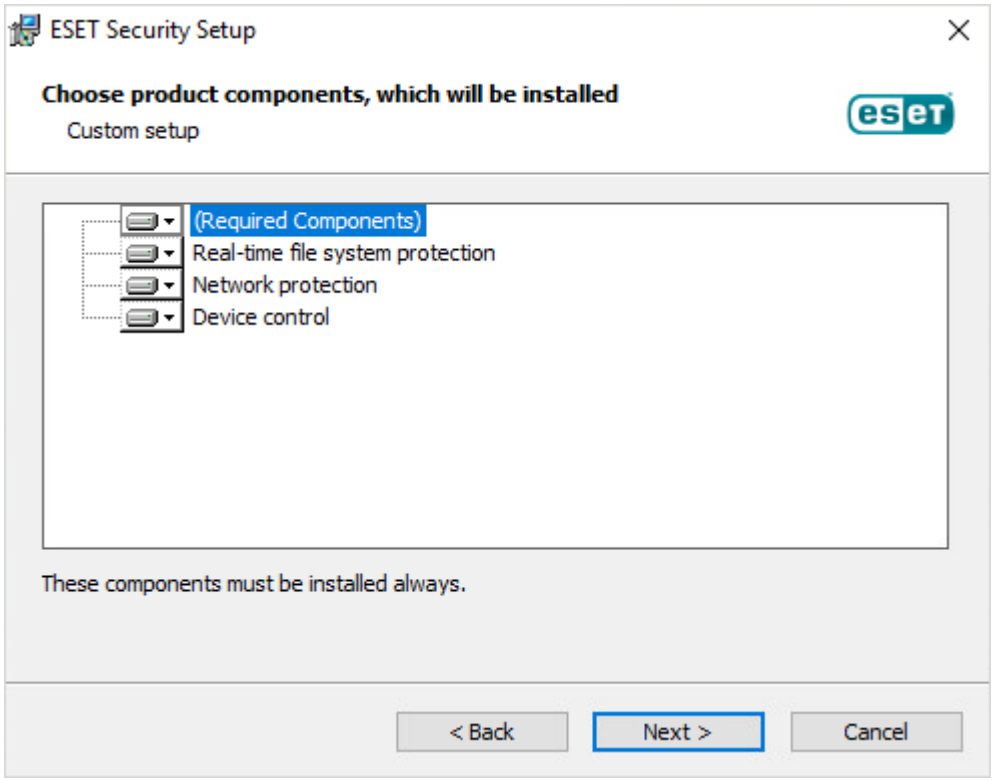
This installation type is intended for Windows Server Core editions. Installation steps are the same as a complete installation, but only core features and the command line user interface are installed.

Although core installation is mainly for use on Windows Server Core, you can still install it on regular Windows Servers if you prefer. ESET security products installed using core installation do not have a main program window. This means that you can only use the command line user interface when working with ESET Security for Microsoft SharePoint. See the Command line installation section for more detailed information and other special parameters.

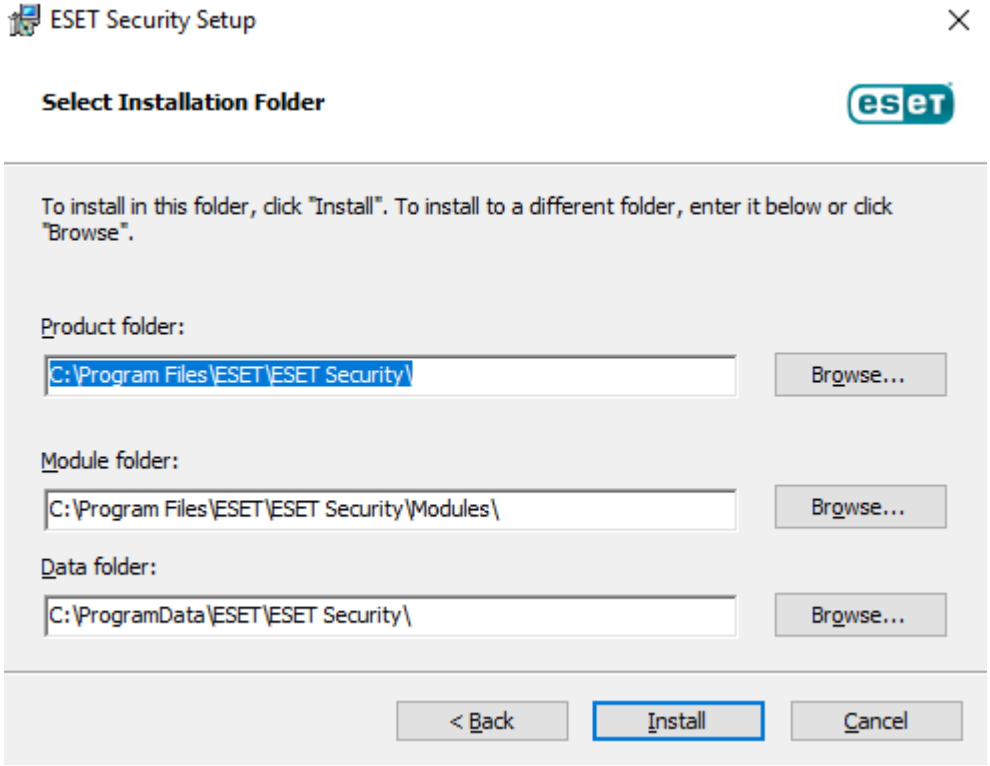
> To execute Core installation via command line, use the following sample command:
> `msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base`

### Custom

Custom installation lets you choose which features of ESET Security for Microsoft SharePoint will be installed on your system. A list of product modules and features displays before the installation starts. It is useful when you want to customize ESET Security for Microsoft SharePoint with only the necessary components.




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

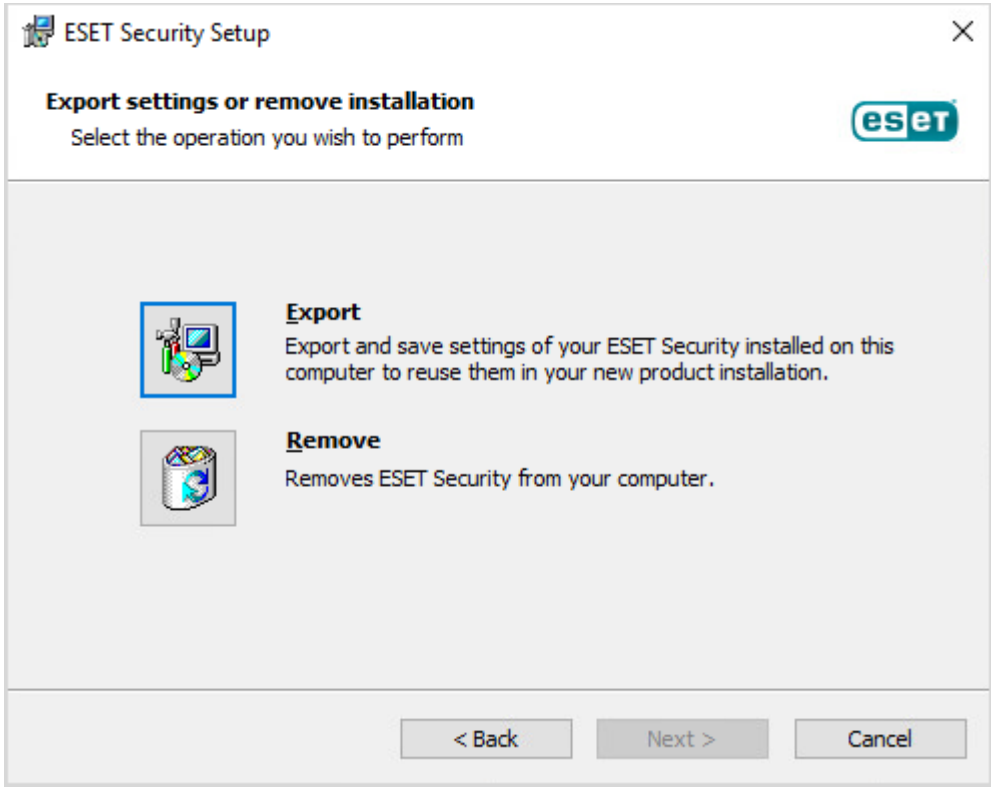



6. Click **Install** to begin the installation. After the installation, you are prompted to activate ESET Security for Microsoft SharePoint.

# Export settings or remove installation

You can export and save settings or remove the installation. To do so, either run the *.msi* installer package you used during the initial installation or go to **Programs and Features** (accessible from the Windows Control Panel), right-click ESET Security for Microsoft SharePoint and select **Change**.

You can **Export** your ESET Security for Microsoft SharePoint settings or **Remove** (uninstall) the ESET Security for Microsoft SharePoint completely.



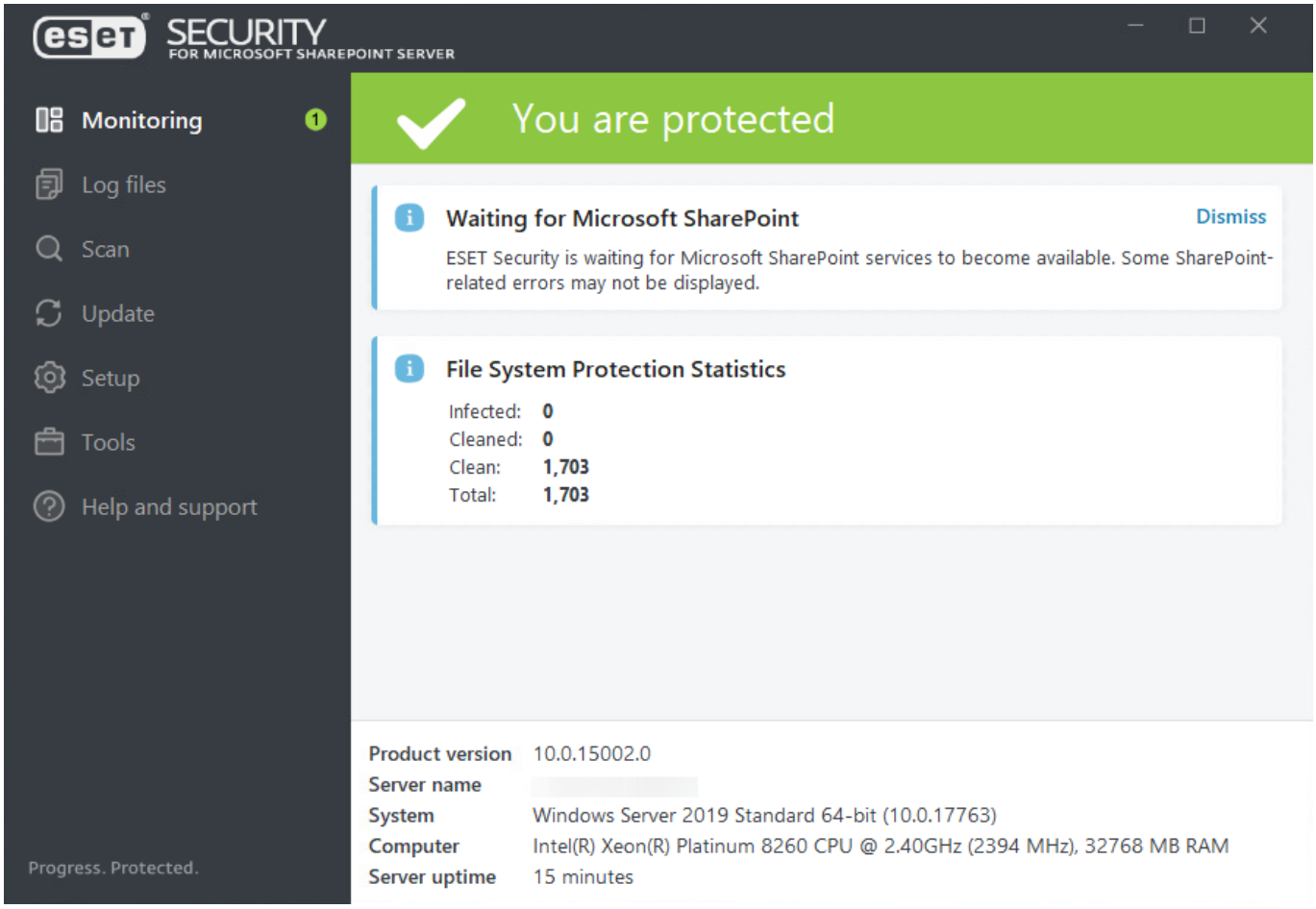

# Initial modules update

The installer contains only essential modules, which reduces network traffic related to the size of the installer and saves resources. After the product activation, all other modules will download during the initial module update. The main advantage is a significantly smaller installer, and ESET Security for Microsoft SharePoint downloads only the latest application modules when you activate the product.

The minimal module installer contains the following modules:

- Loaders
- Anti-Stealth support
- Direct Cloud communication
- Translation support
- Configuration
- SSL

After the product activation, you will see the **Initializing protection** status, which notifies you about the features initializing.




If you experience problems downloading the modules (for example, no network connection, firewall or proxy settings), a warning application status **Attention required** displays. Click **Update** > **Check for updates** in the main program window to start the updating process again.
After several unsuccessful attempts, a red application status **Protection setup failed** displays. If you cannot update the modules, download the full ESET Security for Microsoft SharePoint *.msi* installer.

If your server does not have an internet connection and needs updates, use the following methods to download update module files from ESET update servers:

- Updating from the Mirror
- Using Mirror Tool

# Silent / Unattended installation

Run the following command to complete installation via command line: `msiexec /i <packagename> /qn /l*xv msi.log`

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).

**Full installation** on a 64-bit system:
```
msiexec /i eshp_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 the icon will appear in the Windows notification area.

Installation of the product in **specified language** (German):
```
msiexec /i eshp_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.

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.

**Complete removal** (uninstallation) from a 64-bit system:
```
msiexec /x eshp_nt64.msi /qn /l*xv msi.log
```
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: `eshp_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: `eshp_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: `eshp_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: `eshp_nt64.msi /qn ADDEXCLUDE=<list>`

`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 Security for Microsoft SharePoint features:**

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

| Feature Name | Feature Presence |
|---|---|
| `SERVER` | Mandatory |
| `RealtimeProtection` | Optional |

| Feature Name | Feature Presence |
|---|---|
| WMIProvider | Mandatory |
| HIPS | Mandatory |
| Updater | Mandatory |
| eShell | Mandatory |
| UpdateMirror | Mandatory |
| DeviceControl | Optional |
| DocumentProtection | Optional |
| WebAndEmail | Optional |
| ProtocolFiltering | Invisible |
| NetworkProtection | Optional |
| IdsAndBotnetProtection | Optional |
| Rmm | Optional |
| WebAccessProtection | Optional |
| EmailClientProtection | Optional |
| MailPlugins | Invisible |
| Cluster | Optional |
| _Base | Mandatory |
| eula | Mandatory |
| ShellExt | Optional |
| _FeaturesCore | Mandatory |
| 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
```

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

```
msiexec /i eshp_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

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

```
msiexec /i eshp_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection^
IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

**Core** installation example:
`msiexec /qn /i eshp_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm`

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

Install ESET Security for Microsoft SharePoint and disable ESET LiveGrid®:
`msiexec /qn /i eshp_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0`

**List of all configuration properties:**

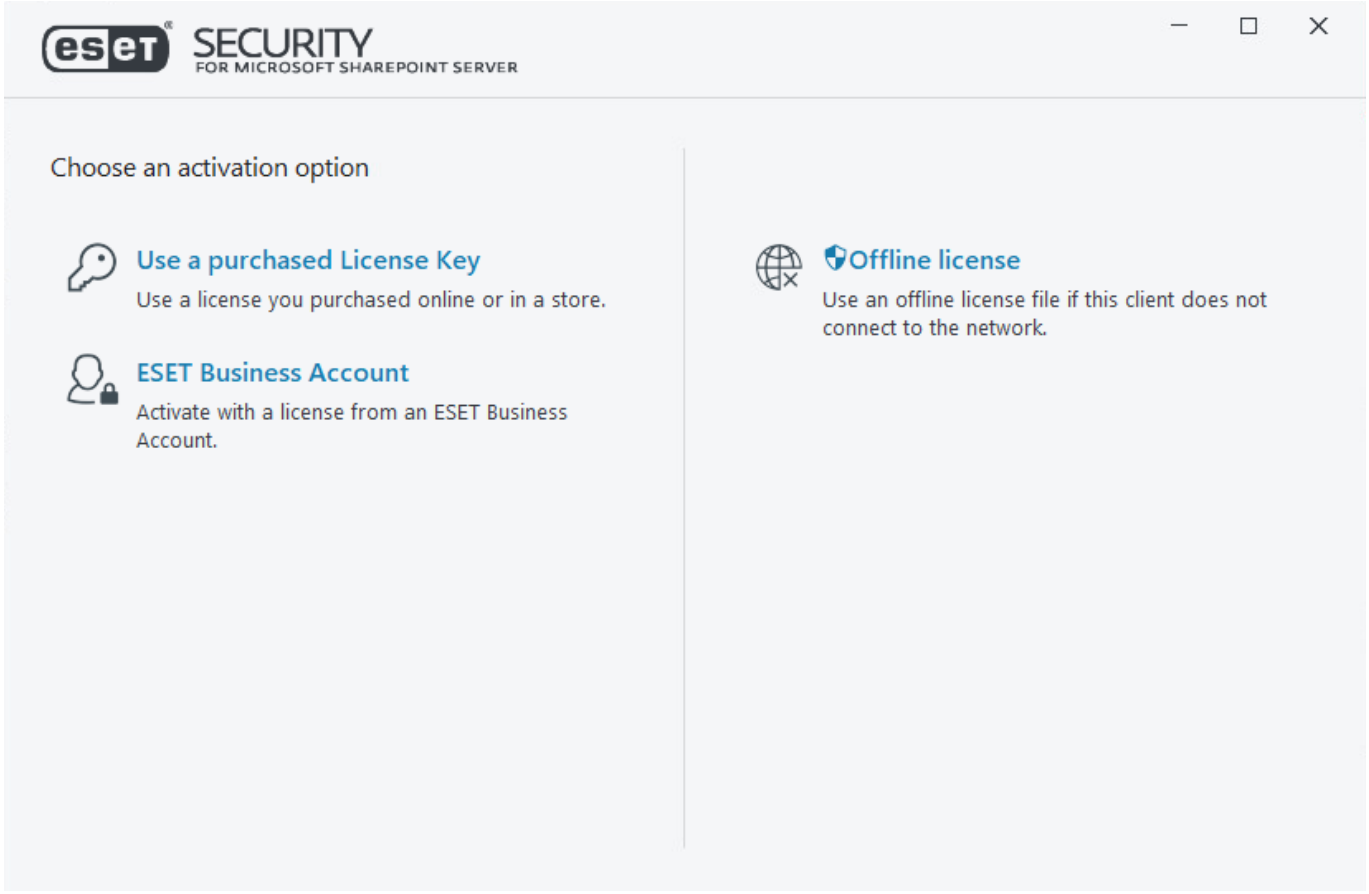
| Switch | Value |
|---|---|
| CFG_POTENTIALLYUNWANTED_ENABLED=1/0 | 0 - Disabled, 1 - Enabled |
| CFG_LIVEGRID_ENABLED=1/0 | 0 - Disabled, 1 - Enabled |
| FIRSTSCAN_ENABLE=1/0 | 0 - Disable, 1 - Enable |
| CFG_PROXY_ENABLED=0/1 | 0 - Disabled, 1 - Enabled |
| CFG_PROXY_ADDRESS=<ip> | Proxy IP address |
| CFG_PROXY_PORT=<port> | Proxy port number |
| CFG_PROXY_USERNAME=<user> | Username 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

You are prompted to activate your product when the installation is complete.




You can use any of the following methods to activate ESET Security for Microsoft SharePoint:

### A purchased License Key

Type or copy/paste your ESET-issued License Key into the **License Key** field and click **Continue**. Type the License Key exactly as it is, including the hyphens. If you copy/paste the license, ensure that you do not accidentally select additional space around the text.

### ESET Business Account

Use this option if you are registered and have your ESET Business Account where your ESET Security for Microsoft SharePoint license has been imported.

### An offline License file

This is an automatically generated file that is transferred to the ESET product. 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 PROTECT if your computer is a member of a managed network, and your administrator will perform remote activation via ESET PROTECT. You can also use this option if you want to activate this client later.

Select **Help and support** > **Change license** in the main program window to manage your license information. You will see the public license ID used to identify your product and license. Your Username, under which the computer is registered, is stored in the About section, and you can view it by right-clicking the Windows notification area icon .

After successfully activating ESET Security for Microsoft SharePoint, the main program window opens and displays your current status on the Monitoring page. Some attention may be required initially; for example, you are asked if you want to be part of ESET LiveGrid®.

The main program window also displays notifications about other items, such as system updates (Windows Updates) or detection engine updates. When everything requiring attention is resolved, the monitoring status turns green and displays the status **You are protected**.

You can activate your product from the main menu under **Help and support** > **Activate Product** or **Monitoring status** > **Product is not activated**.

ESET PROTECT can silently activate client computers using licenses made available by the administrator.

# Activation successful

ESET Security for Microsoft SharePoint is now activated. From now on, ESET Security for Microsoft SharePoint will receive regular updates identifying the latest threats and keeping your computer safe.

Click **Done** to finish product activation.

# Activation failure

In the case activation of ESET Security for Microsoft SharePoint was not successful, possible scenarios are:

- License Key already in use
- Invalid License Key—product activation form error
- Missing or invalid information must be addressed
- Communication with the activation database failed—try again in 15 minutes
- Connection to ESET activation servers is unavailable or disabled

Ensure you entered the proper **License Key** or attached an **Offline License** and attempt to activate again.

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

# License

You are prompted to select a license for ESET Security for Microsoft SharePoint that is associated with your account. Click **Continue** to proceed with activation.

# Upgrade to the latest version

New ESET Security for Microsoft SharePoint versions are issued to provide improvements or fix issues that program module automatic updates cannot resolve.

**Upgrade methods:**

- **Uninstall / Install** - Removing the earlier version before installing the new one. Download the latest version of ESET Security for Microsoft SharePoint. Export settings from your existing ESET Security for Microsoft SharePoint if you want to preserve configuration. Uninstall ESET Security for Microsoft SharePoint 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 Security for Microsoft SharePoint.

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

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 Security for Microsoft SharePoint may not be removed correctly. You will also experience problems if you decide to remove the old version of ESET Security for Microsoft SharePoint manually afterward.

A server restart will be required during the upgrade of ESET Security for Microsoft SharePoint.

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

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

When you upgrade your ESET Security for Microsoft SharePoint, we recommend you go through all the settings to ensure it is configured correctly according to your needs.

# Upgrading via ESET PROTECT

ESET PROTECT lets you upgrade multiple servers running an earlier ESET Security for Microsoft SharePoint version. This method has the advantage of upgrading many servers simultaneously while ensuring each ESET Security for Microsoft SharePoint is configured identically (if desired).

The procedure includes the following phases:

- **Upgrade the first server** manually by installing the latest ESET Security for Microsoft SharePoint version over your existing version to preserve your configuration, including rules and multiple whitelists/blacklists. This phase is performed locally on the server running ESET Security for Microsoft SharePoint.

- **Request configuration** of the newly upgraded ESET Security for Microsoft SharePoint to version 7.x and convert to policy in ESET PROTECT. The policy will be applied later to all upgraded servers. This phase and the following phases are performed remotely using ESET PROTECT.

- **Run the Software Uninstall task** on all servers running the old ESET Security for Microsoft SharePoint version.

- **Run the Software Install task** on all servers where you want the latest ESET Security for Microsoft SharePoint version.

- **Assign a configuration policy** to all servers running the latest ESET Security for Microsoft SharePoint version.

- **Specify SharePoint Farm Administrator account** on each server manually. This phase is performed locally.

### Follow the instructions below to upgrade via ESET PROTECT

1. Log on to one of the servers running ESET Security for Microsoft SharePoint and upgrade it by downloading and installing the latest version over your existing version. Follow the regular installation steps. Your original ESET Security for Microsoft SharePoint configurations are preserved during the installation.

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

3. Select the Configuration tab and click the **Request configuration** button to collect your managed product's configurations. Be aware that this process takes a moment. When the latest configuration appears in the list, click **Security product** and choose **Open Configuration**.

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

5. Select **Client Tasks** and choose the Software Uninstall task. When creating the uninstall task, we recommend you restart the server after the uninstallation by selecting the check box **Automatically reboot when needed**. Once you create the task, add all desired target computers for uninstallation.

6. Make sure ESET Security for Microsoft SharePoint is uninstalled from all the targets.

7. Create a Software Install task to install the latest ESET Security for Microsoft SharePoint version to all desired targets.

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

9. Log onto each server locally, open ESET Security for Microsoft SharePoint. You will see a red warning status message saying: *ESET SharePoint Helper Service is not running*. Specify **SharePoint Farm Administrator account** in advanced setup.

> This step must be performed on each server running ESET Security for Microsoft SharePoint. It is due to security reasons. ESET products do not store SharePoint admin credentials; thus, the credentials are not in the configuration policy and cannot be passed to other servers.

# Upgrading via ESET Cluster

Creating an ESET Cluster lets you upgrade multiple servers running earlier ESET Security for Microsoft SharePoint versions and is an alternative to the ESET PROTECT upgrade. We recommend using the ESET Cluster method if you have two or more servers with ESET Security for Microsoft SharePoint in your environment.

Another benefit of this upgrade method is that you can continue using the ESET Cluster so the ESET Security for

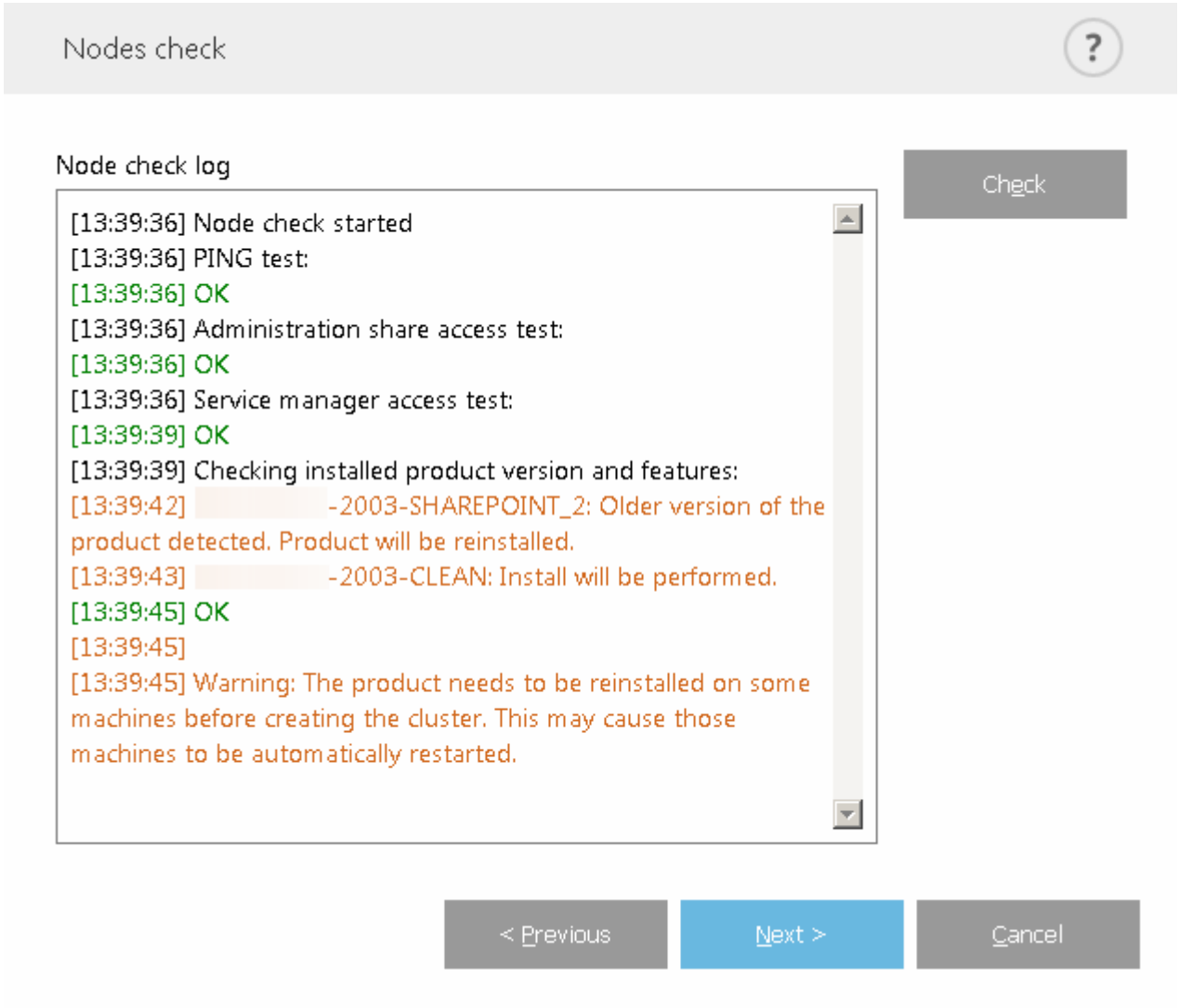
Microsoft SharePoint configuration will be synchronized on all member nodes.

### Follow the steps below to upgrade using ESET Cluster:

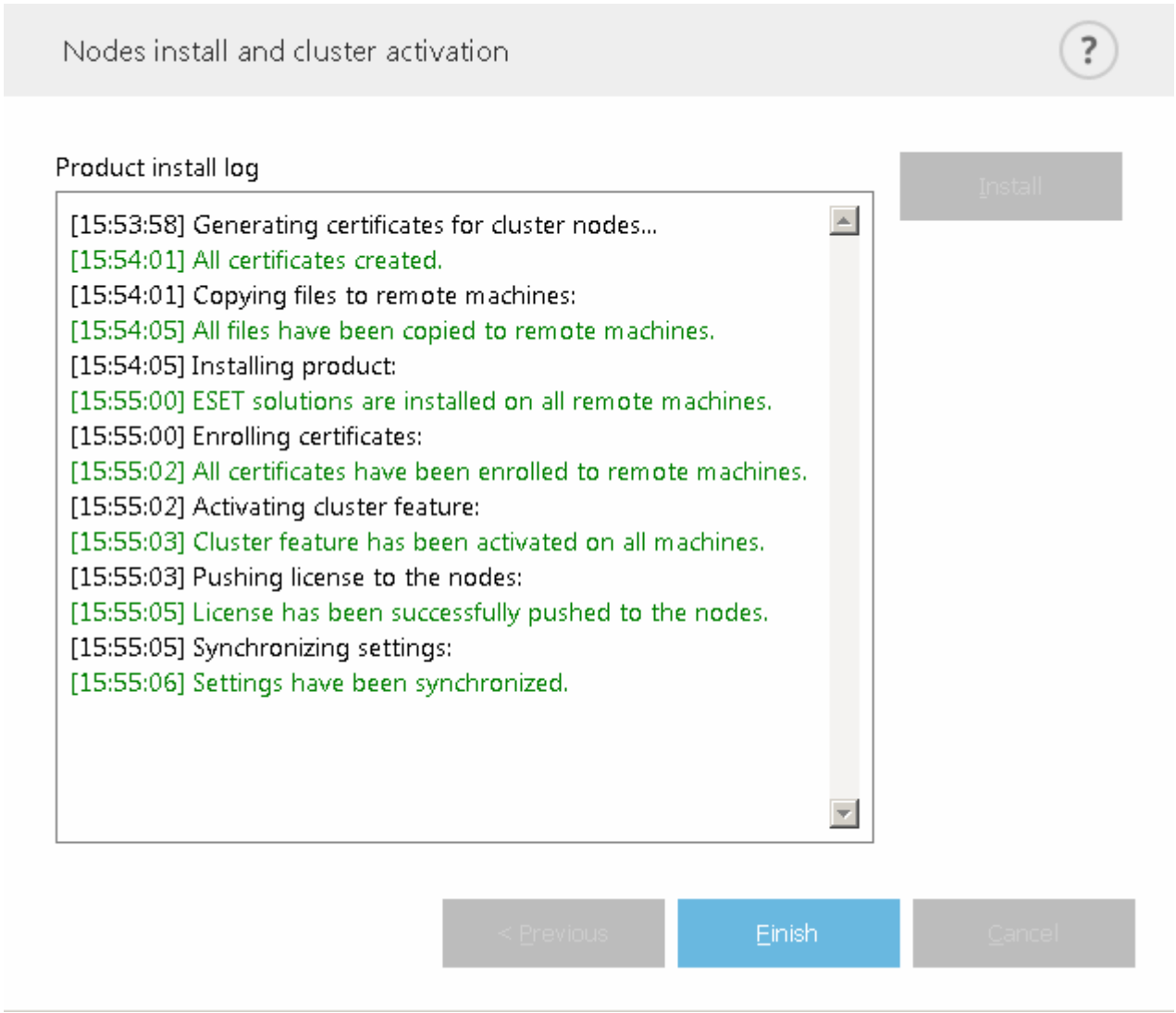
1. Log in to a server running ESET Security for Microsoft SharePoint and upgrade by downloading and installing the latest version over your existing one. Follow the steps for regular installation. Your original ESET Security for Microsoft SharePoint configuration is preserved during the installation.

2. Run the ESET Cluster wizard and add cluster nodes (the servers that need upgraded ESET Security for Microsoft SharePoint). If required, you can add other servers that do not run ESET Security for Microsoft SharePoint yet (a regular install will occur on these). We recommend that you to leave the default settings in place when specifying your Cluster name and install type (ensure **Push license to nodes without activated product** is selected).

3. Review the **Nodes check log** screen. Servers with earlier product versions are listed and marked for upgrade (reinstallation). ESET Security for Microsoft SharePoint will also install on any servers that do not already have ESET Security for Microsoft SharePoint.



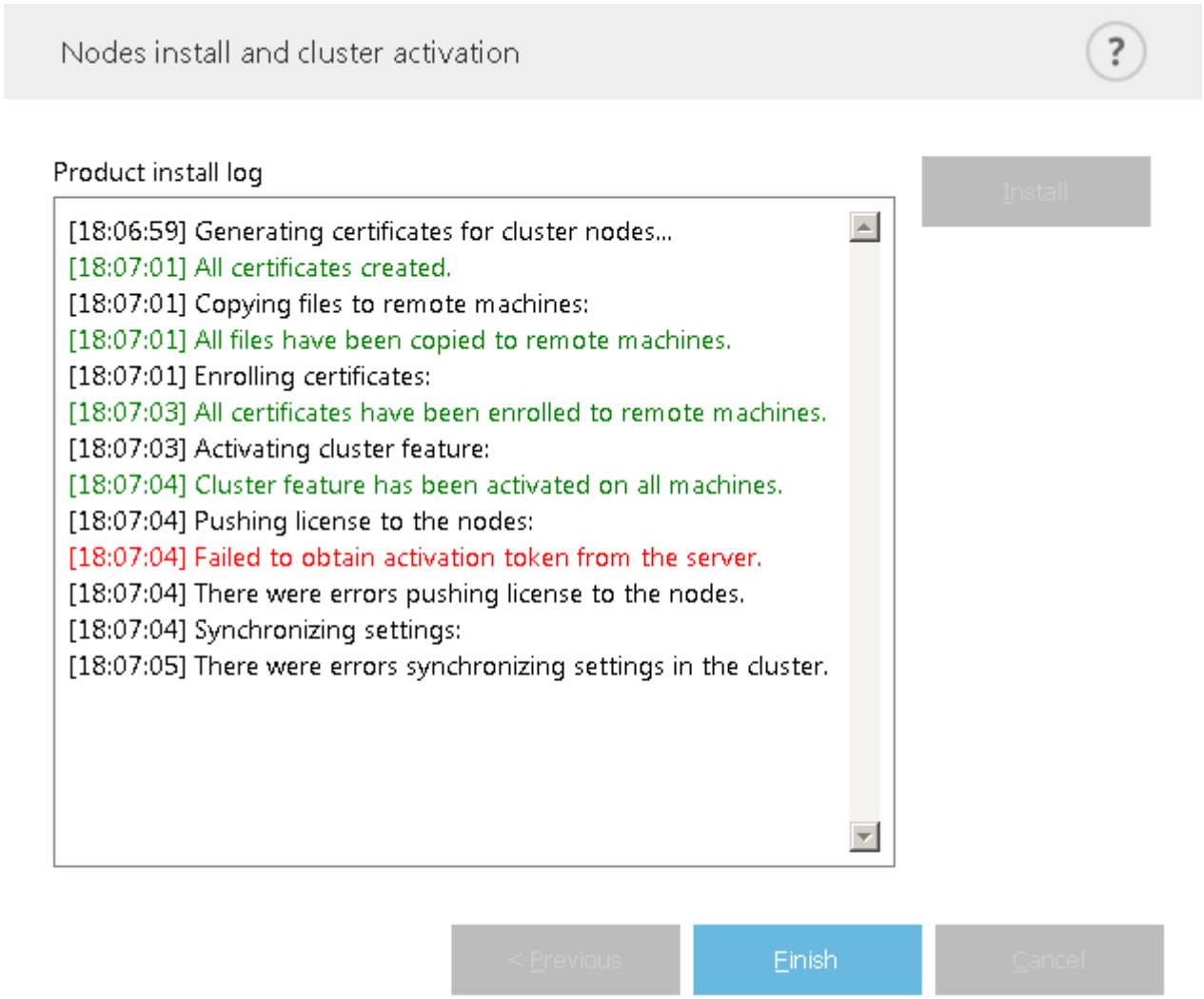

4. The Nodes install and cluster activation screen will display installation progress. When installation is successfully completed, it should finish with results similar to these:




5. Log onto each server locally and open ESET Security for Microsoft SharePoint. ESET SharePoint Helper Service is not running will be displayed. Specify your SharePoint Farm Administrator account in advanced setup.

This step must be performed on each server running ESET Security for Microsoft SharePoint. It is due to security reasons. ESET products do not store SharePoint admin credentials; thus, the credential is not in the configuration policy and cannot be passed to other servers.

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




# Terminal server

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

# Getting started

The following topics will help you get started with ESET Security for Microsoft SharePoint.

Monitoring

This is a quick overview of ESET Security for Microsoft SharePoint's current status, where you can easily see if any issues require your attention.

Managed via ESET PROTECT

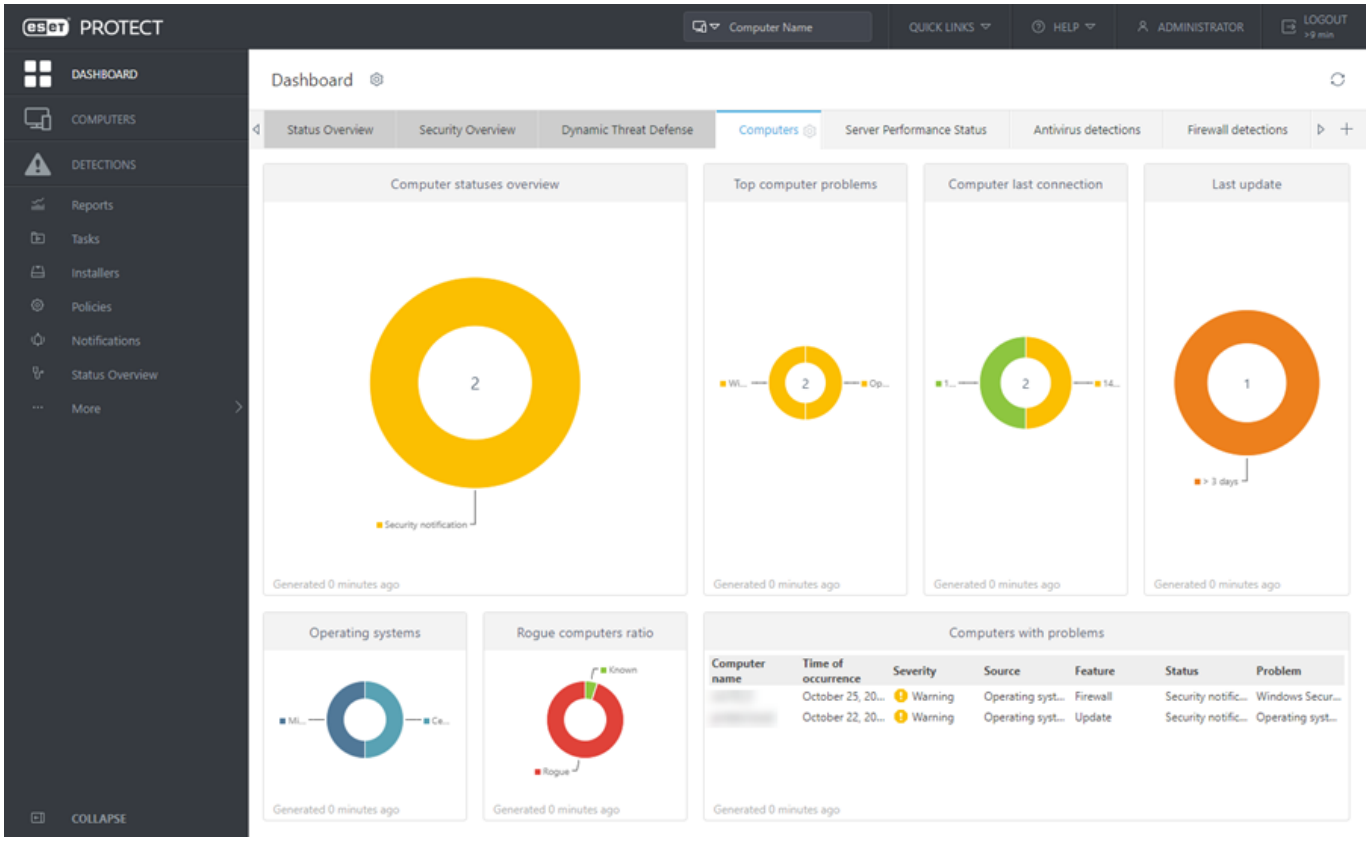
You can use ESET PROTECT to remotely manage ESET Security for Microsoft SharePoint.

# Managed via ESET PROTECT

ESET PROTECT is an application that lets you manage ESET products in a networked environment from one central location. The ESET PROTECT task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats.

ESET PROTECT does not protect 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, macOS and mobile operating systems.




For more information, see ESET PROTECT Online Help.

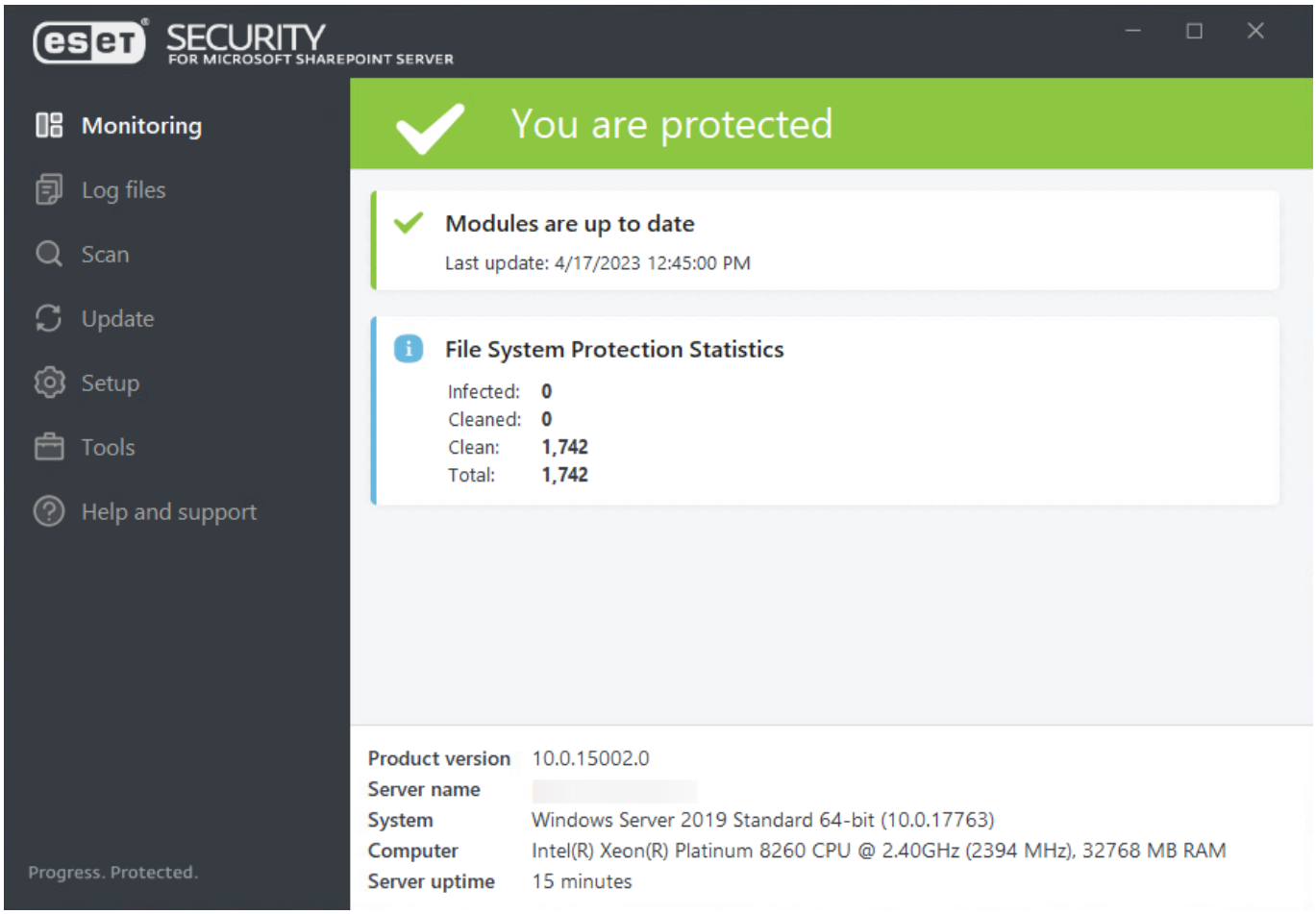
# Monitoring

The protection status shown in the **Monitoring** section informs you of your computer's current protection level. A status summary about ESET Security for Microsoft SharePoint's operation will display 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 system is not ensured. The error message detail should give you a better understanding of the current status. If you are unable to solve a problem, search the ESET Knowledgebase. If you still need assistance, you can submit a support request. ESET Technical Support will respond quickly to your questions and help find a resolution. For a complete list of statuses, open **Advanced setup** (**F5**) > **Notifications** > Application statuses and click **Edit**.

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




Modules that are working correctly 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 an individual module's status, 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 Security for Microsoft SharePoint
- **Server Name**—machine Hostname or FQDN
- **System**—operating system details
- **Computer**—hardware details
- **Server uptime**—shows how long the system is up and running (the opposite of downtime)

## User count

ESET Security for Microsoft SharePoint detects the number of users who use SharePoint. This count will be used for licensing purposes. There are two user types:

- **Domain**—The number of users listed in the SharePoint database who use Windows authentication when

logging in to SharePoint. Their presence is also verified directly in the Active Directory; if it matches, the users are counted. This verification avoids counting users who no longer exist within Active Directory, but are still present on the SharePoint list. Such users are not counted. ESET Security for Microsoft SharePoint supports trusted domains and includes their users in the user count when they log into SharePoint.

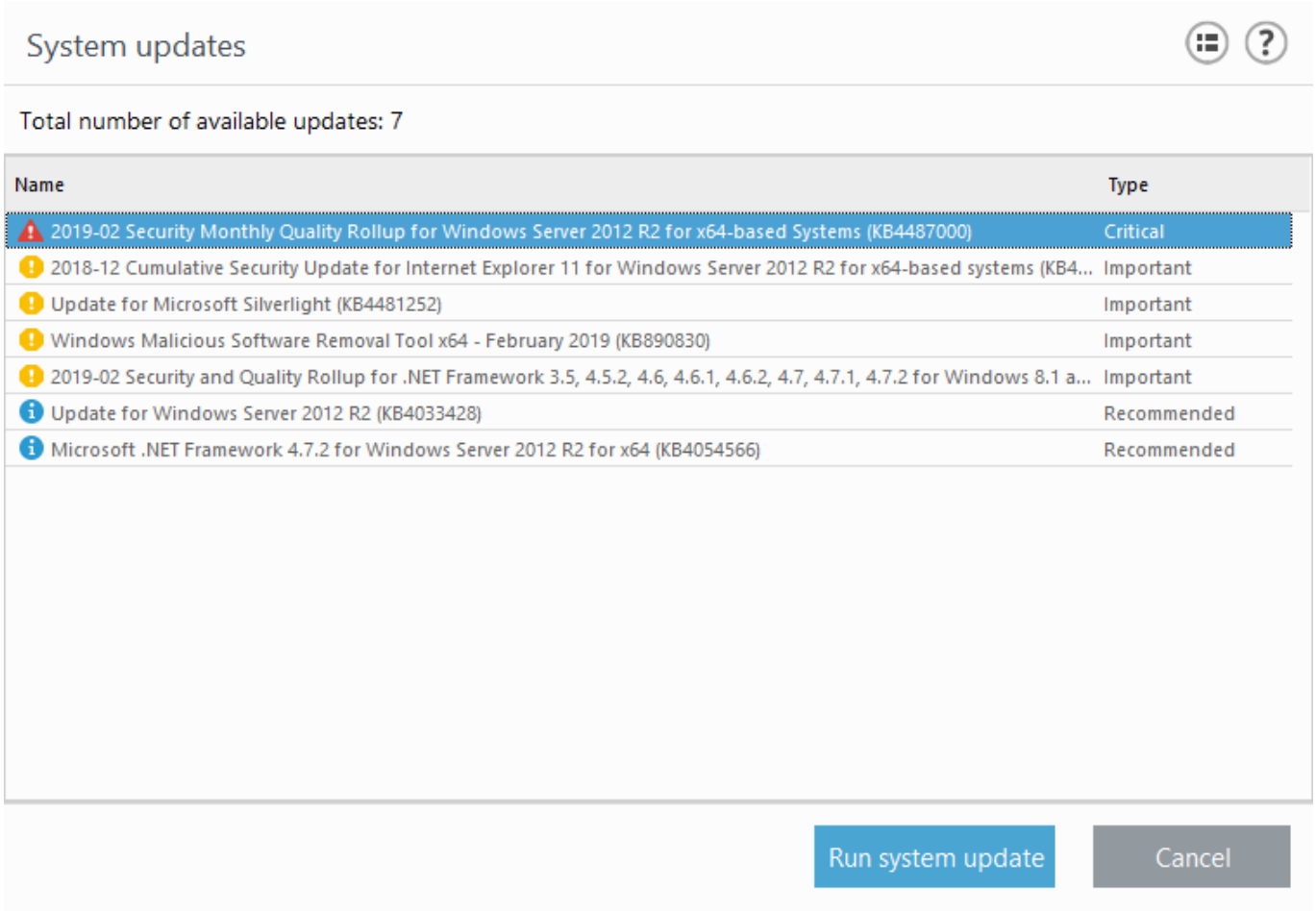
• **Other**—The User count of those who use other forms of authentication (regardless of their presence in Active Directory), for example, a Form-based or Claims-based authentication. The count is also based on the user list in the SharePoint database.

Users are recalculated 5 minutes after the system restarts or every 6 hours. Type valid SharePoint administrator account credentials to view user count information.

If you cannot 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 a 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 window with additional info:




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

# Network isolation

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

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

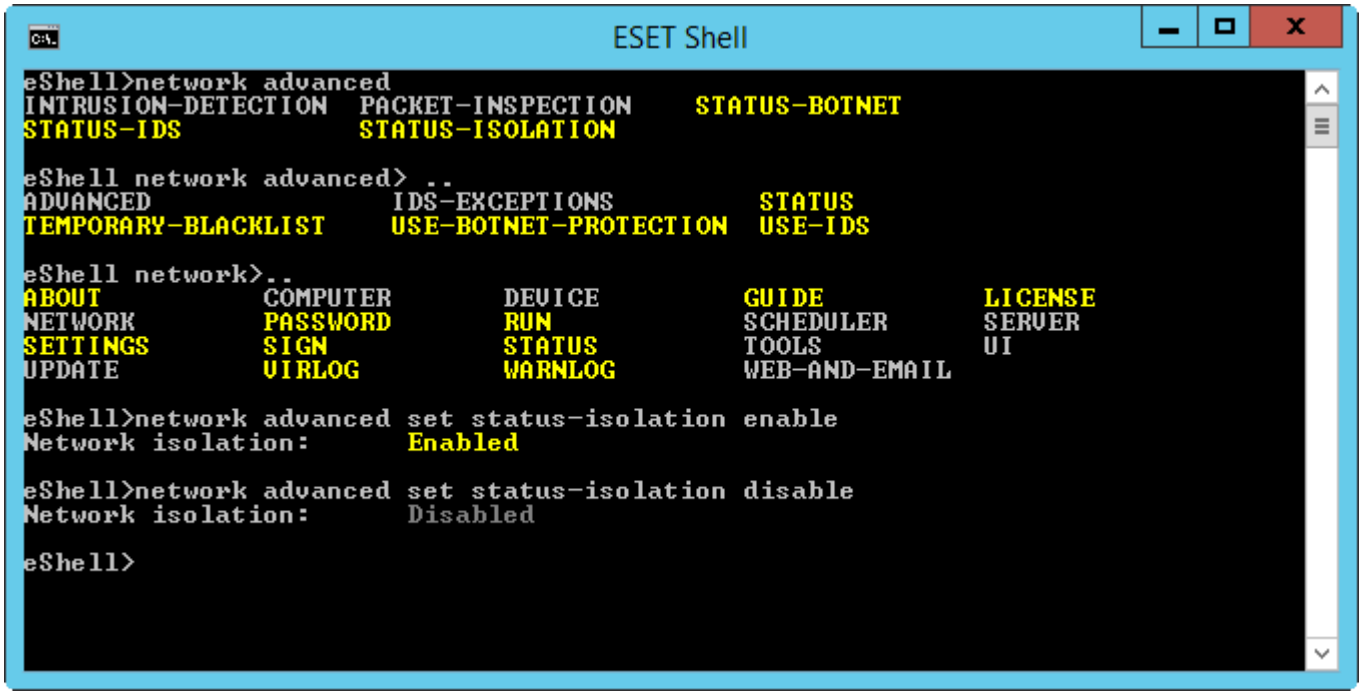
- Connectivity to the Domain Controller remains
- ESET Security for Microsoft SharePoint can still communicate
- If present, ESET Management Agent and ESET Inspect Connector can communicate over the network

Activate and deactivate network isolation using the eShell command or ESET PROTECT client task.

### eShell

In interactive mode:

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




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

### ESET PROTECT

- Activate network isolation via client task.
- Deactivate network isolation via client task.

When network isolation is activated, the ESET Security for Microsoft SharePoint status changes to red and displays the message **Network access blocked**.

# Using ESET Security for Microsoft SharePoint

This section contains a detailed description of the program's user interface and explains how to use ESET Security for Microsoft SharePoint.

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

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

# Scan

The On-demand scanner is an important part of ESET Security for Microsoft SharePoint. 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 Security for Microsoft SharePoint:

SharePoint database scan

Lets you select SharePoint Web sites that you want to scan and run the scanning process.

**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.

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.

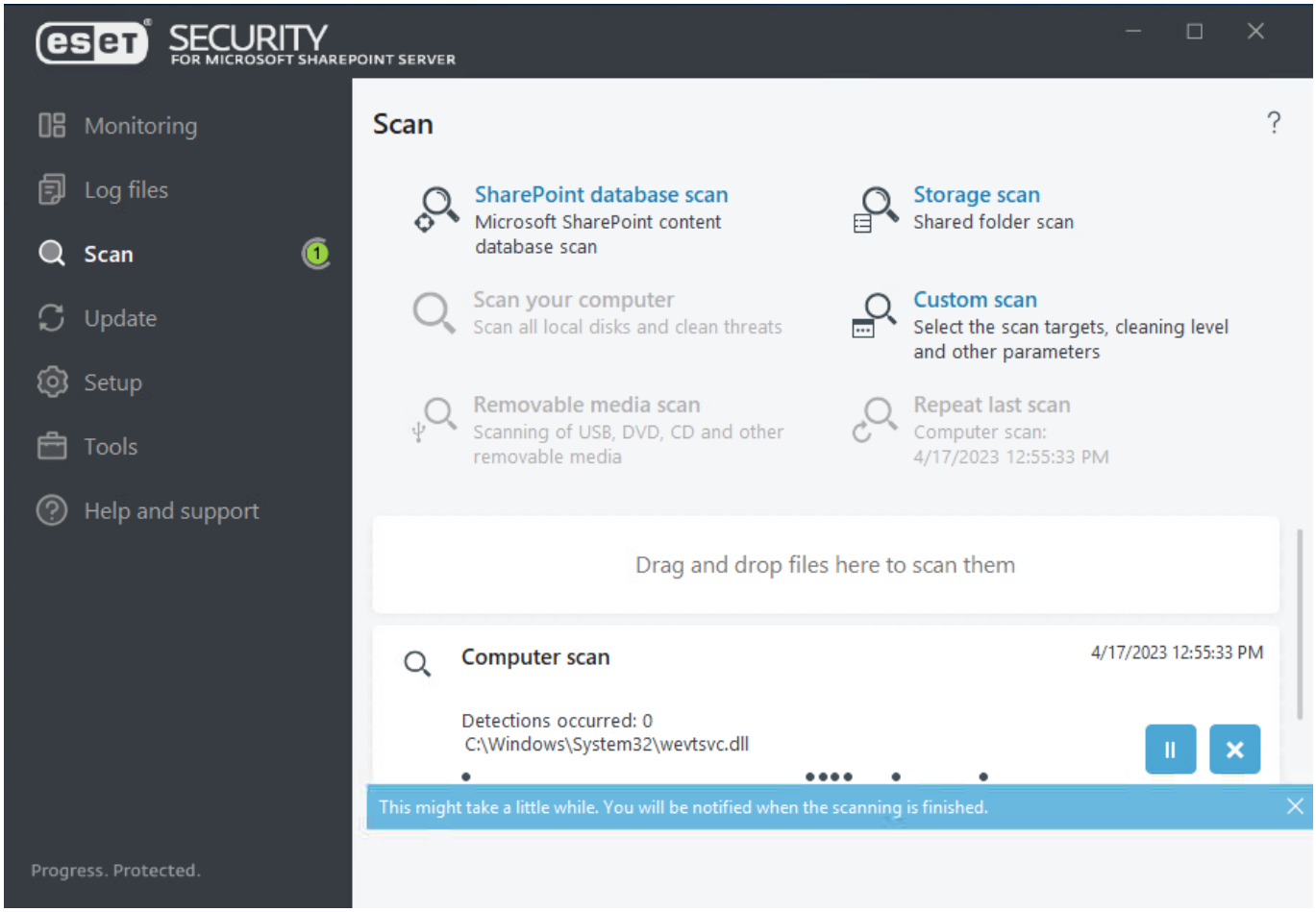
Hyper-V scan

This option is only visible in the menu if Hyper-V Manager is installed on the server that runs ESET Security for Microsoft SharePoint. 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 specific VM.

**Repeat last scan**

Repeats your last scan operation using exactly the same settings.

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



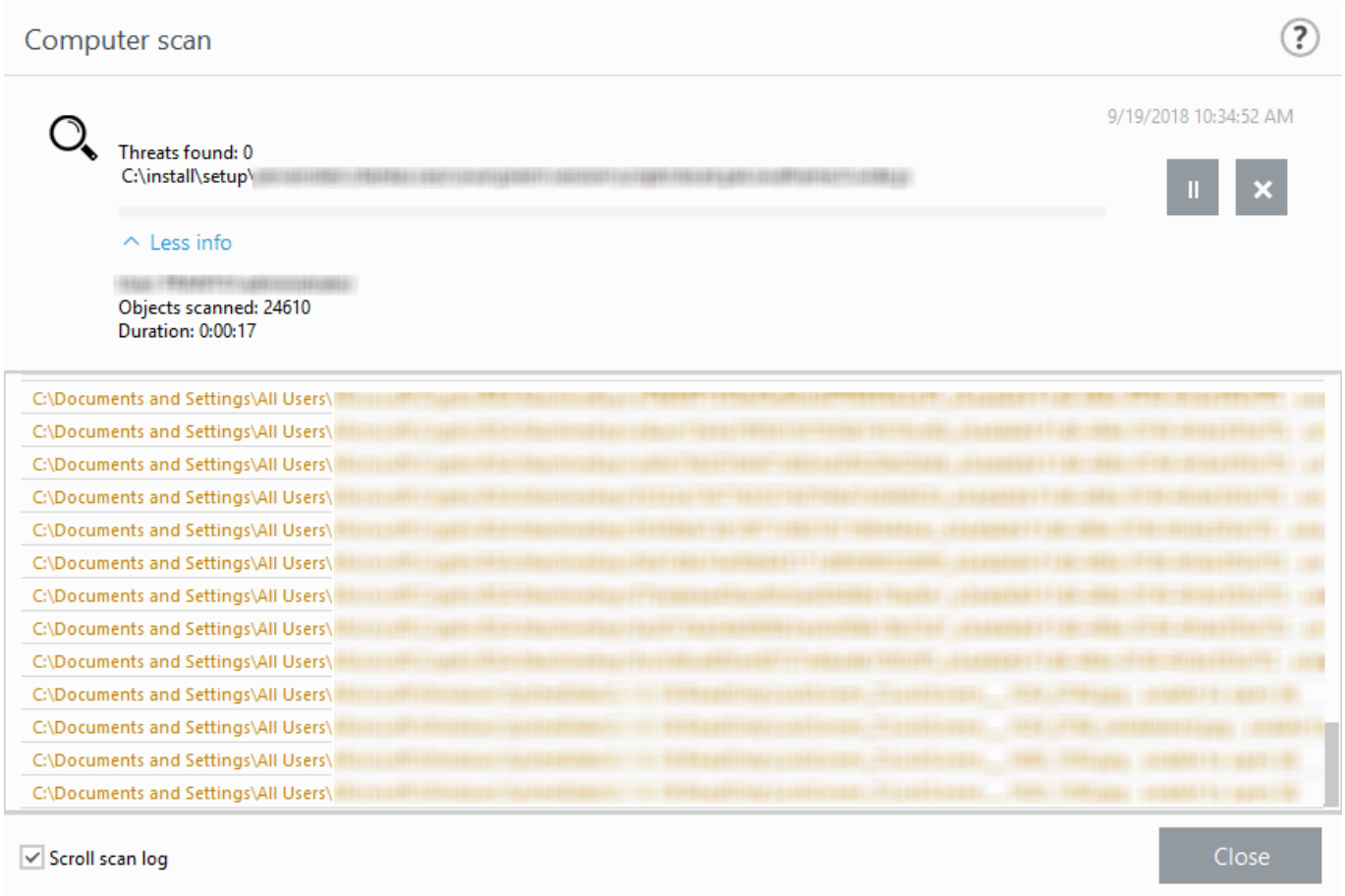

You can use options and shows more information about the scan statuses:

| Drag and drop files | You can also drag and drop files into the ESET Security for Microsoft SharePoint 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**. |
| 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.

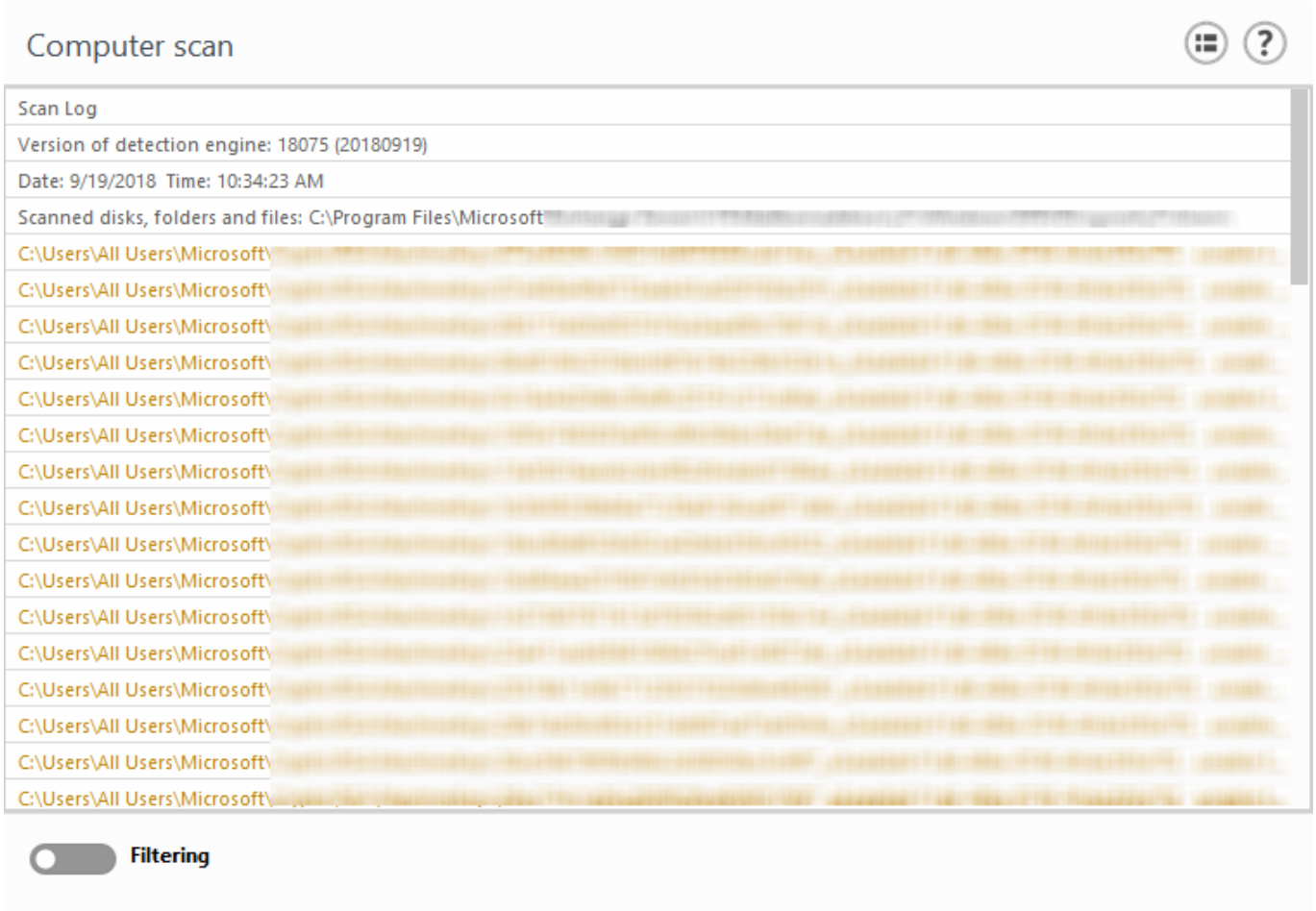



**Scroll scan log**

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

> 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 specific scan.




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. You can view text messages and logs directly from the ESET Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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. You can create a detection exclusion if required by right-clicking a log record (detection) and clicking **Create exclusion**. 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 Security for Microsoft SharePoint 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 LiveGuard and ESET LiveGrid®.

**Audit logs**

Contains records of changes in configuration or protection state and create snapshots for later reference. Right-click any record of setting changes type and select Show from the context menu to display detailed information about the performed change. If you want to you previous setting select Restore. You can also use Delete all to remove log records. If you want to deactivate Audit logging, navigate to Advanced setup > Tools > Log files > Audit log.

**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 . These logs display the time, URL, user and

application that opened a connection to the specific website.

**Device control**

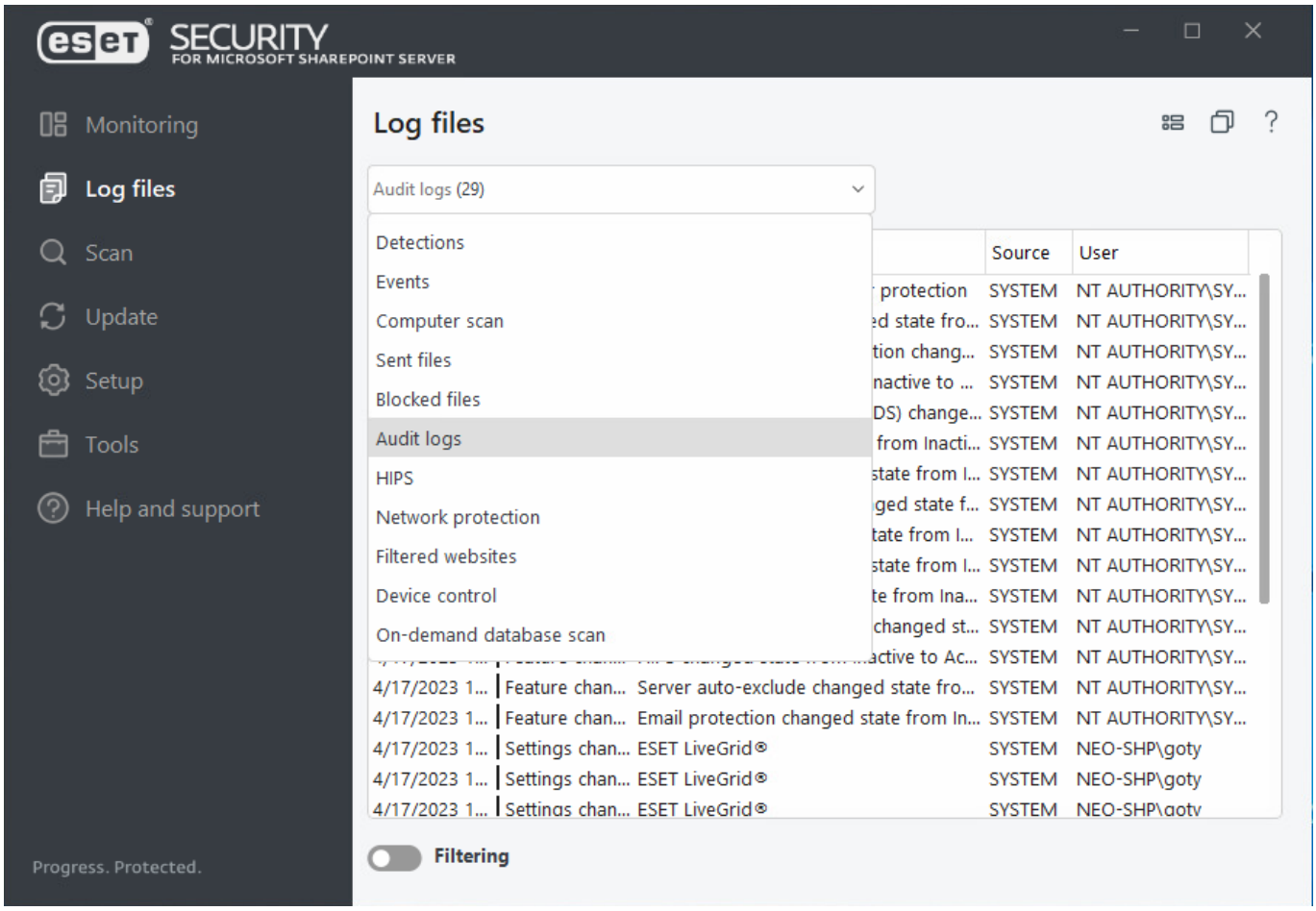
Contains records of removable media or devices that were connected to the computer. Only devices with a Device control rule will be recorded to the log file. If the rule does not match a connected device, a log entry for a connected device will not be created. Here you can also see details such as device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

**On-demand database scan**

Contains a list of SharePoint content database scans. For each scan, the following information is displayed: version of the detection engine, date, scanned location, number of scanned objects, number of threats found, number of rule hits and time of completion.

**Hyper-V scan**

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




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 | |

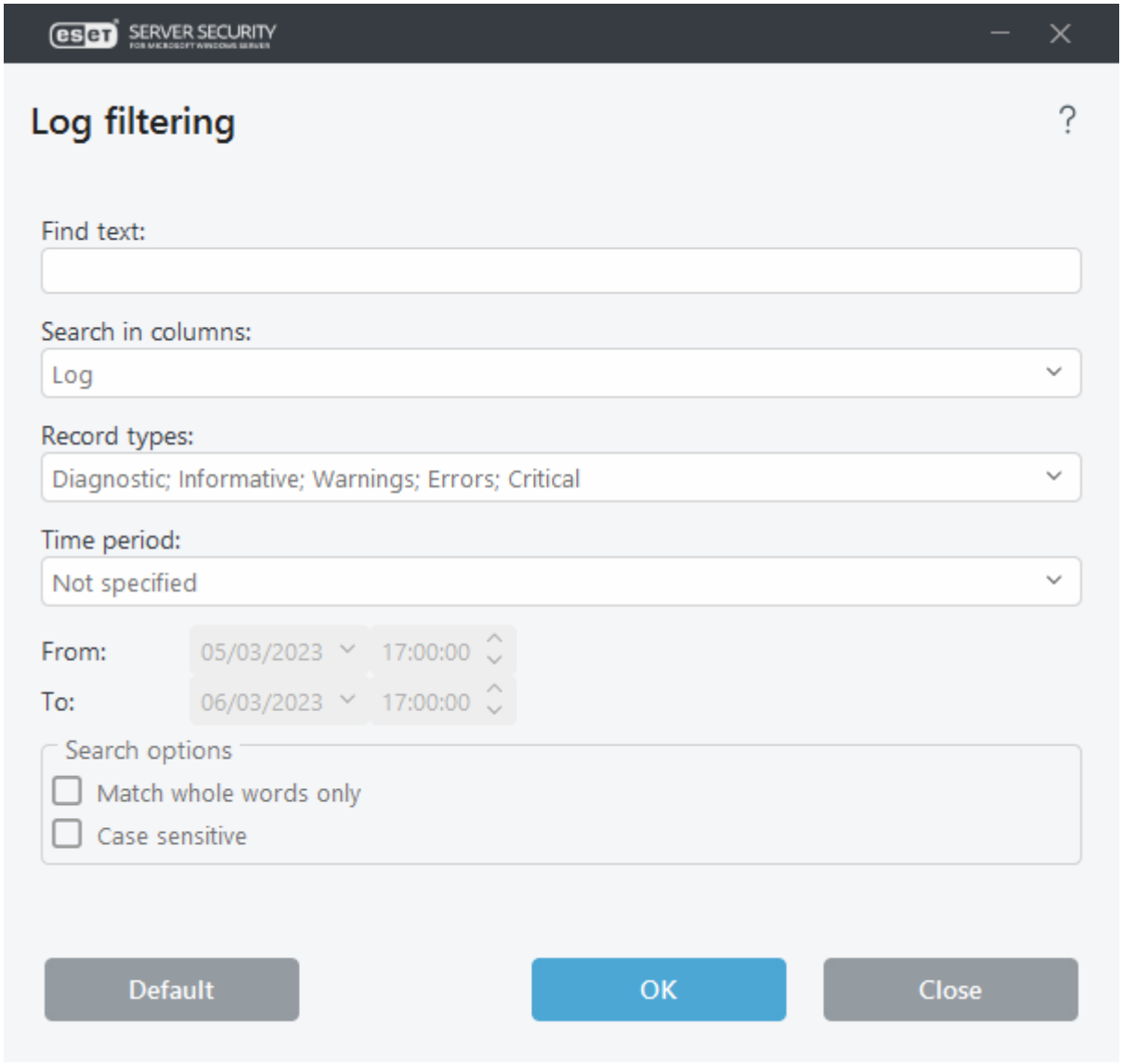
| Action | Usage | Shortcut | See also |
|---|---|---|---|
| Filter... | After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries. | | Log filtering |
| Enable filter | Activates filter settings. The first time you activate filtering, you 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 | |
| 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 |

# 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**.




**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 lowercase letters while filtering. When configuring your filtering/search options, click **OK** to show filtered log records or **Find** to start searching.

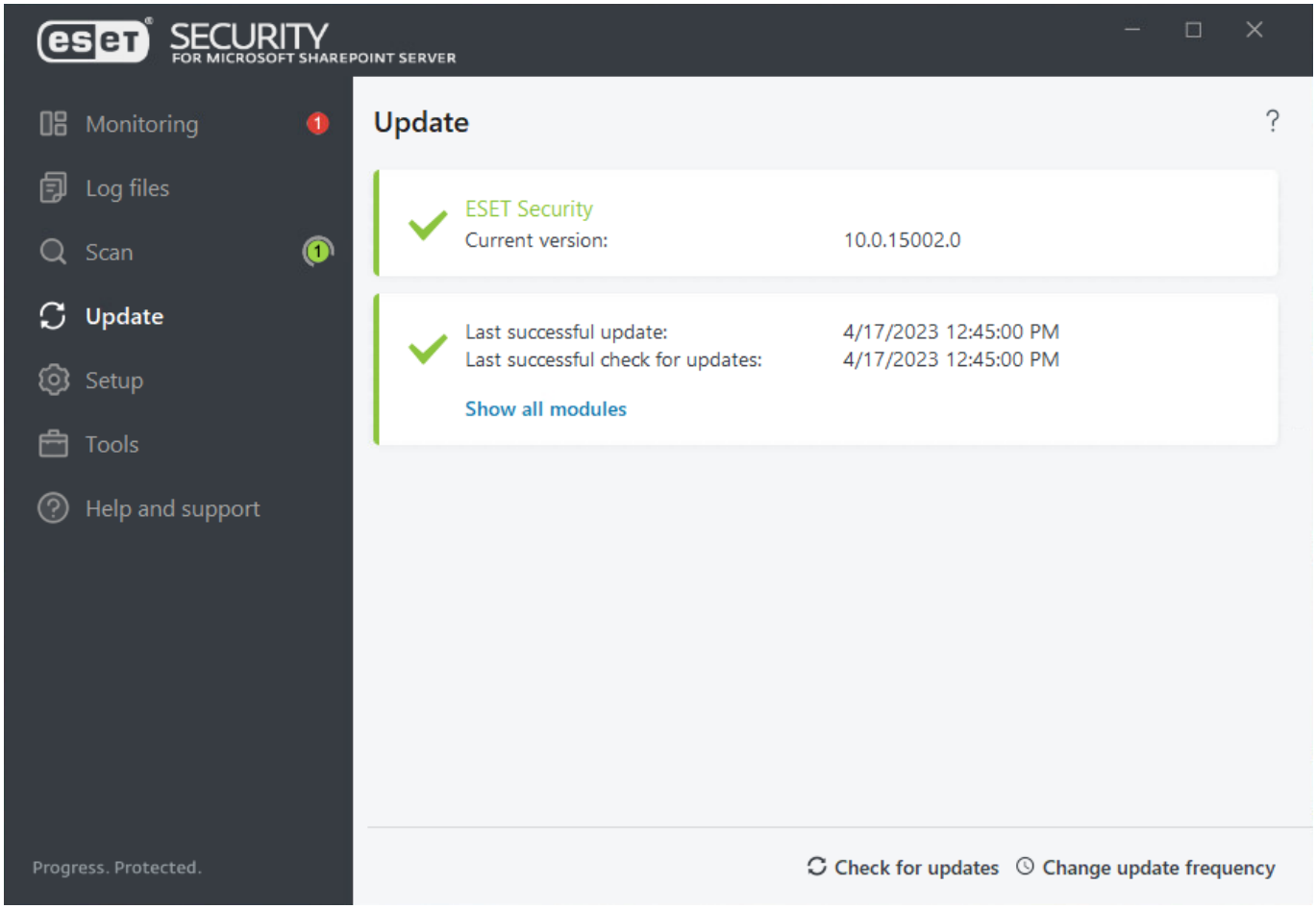
The log files are searched from top to bottom, starting from your current position (the highlighted record). The search stops when it finds the first corresponding record. Press **F3** to search for the next record, or right-click and select **Find** to refine your search options.

# Update

In the Update section, you can see the current update status of your ESET Security for Microsoft SharePoint, including the date and time of the last successful update. Regularly updating ESET Security for Microsoft SharePoint 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.

> If you did not type your 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**.




**Current version**

The ESET Security for Microsoft SharePoint 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:

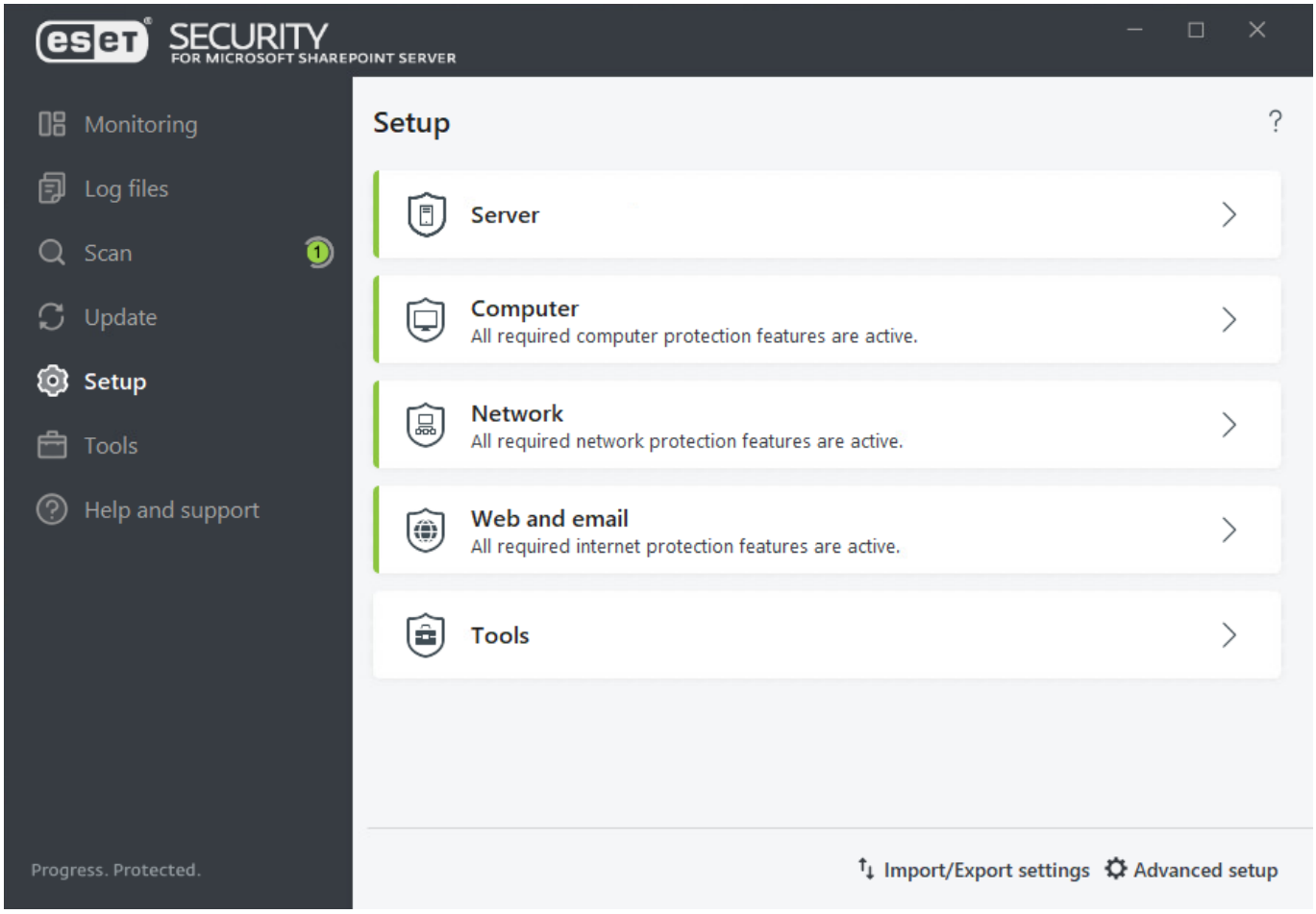
| Error message | Descriptions |
| --- | --- |
| Modules update is out of date | This error will appear after several unsuccessful attempts to module update. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly 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. |

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.

# Setup

The Setup menu window contains the following sections:

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




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 .

**Real-time SharePoint Server protection**

Is an On-access filter which you can further configure if required. Click the gear icon to open SharePoint

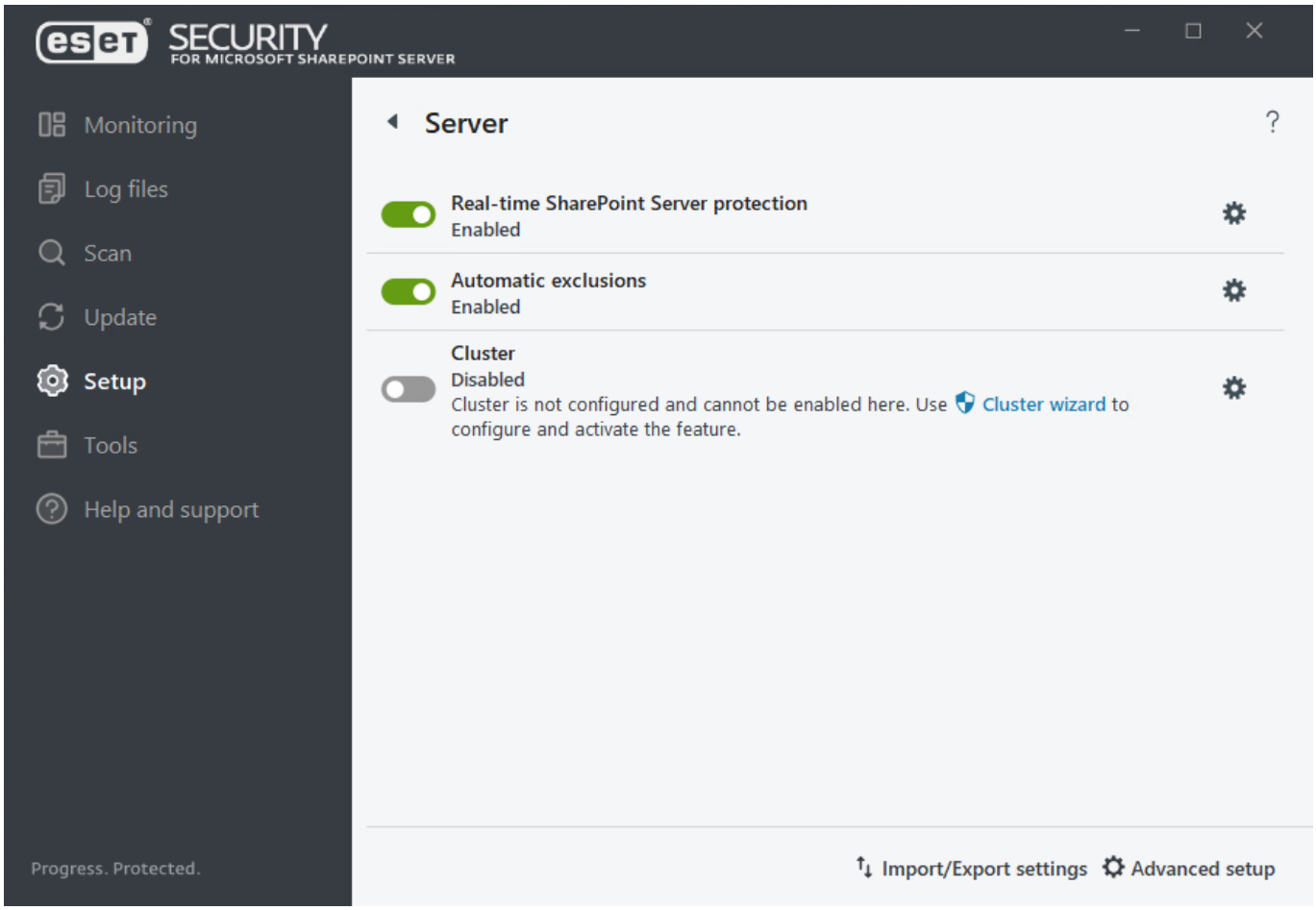
protection settings window.

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.




# Computer

ESET Security for Microsoft SharePoint 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.

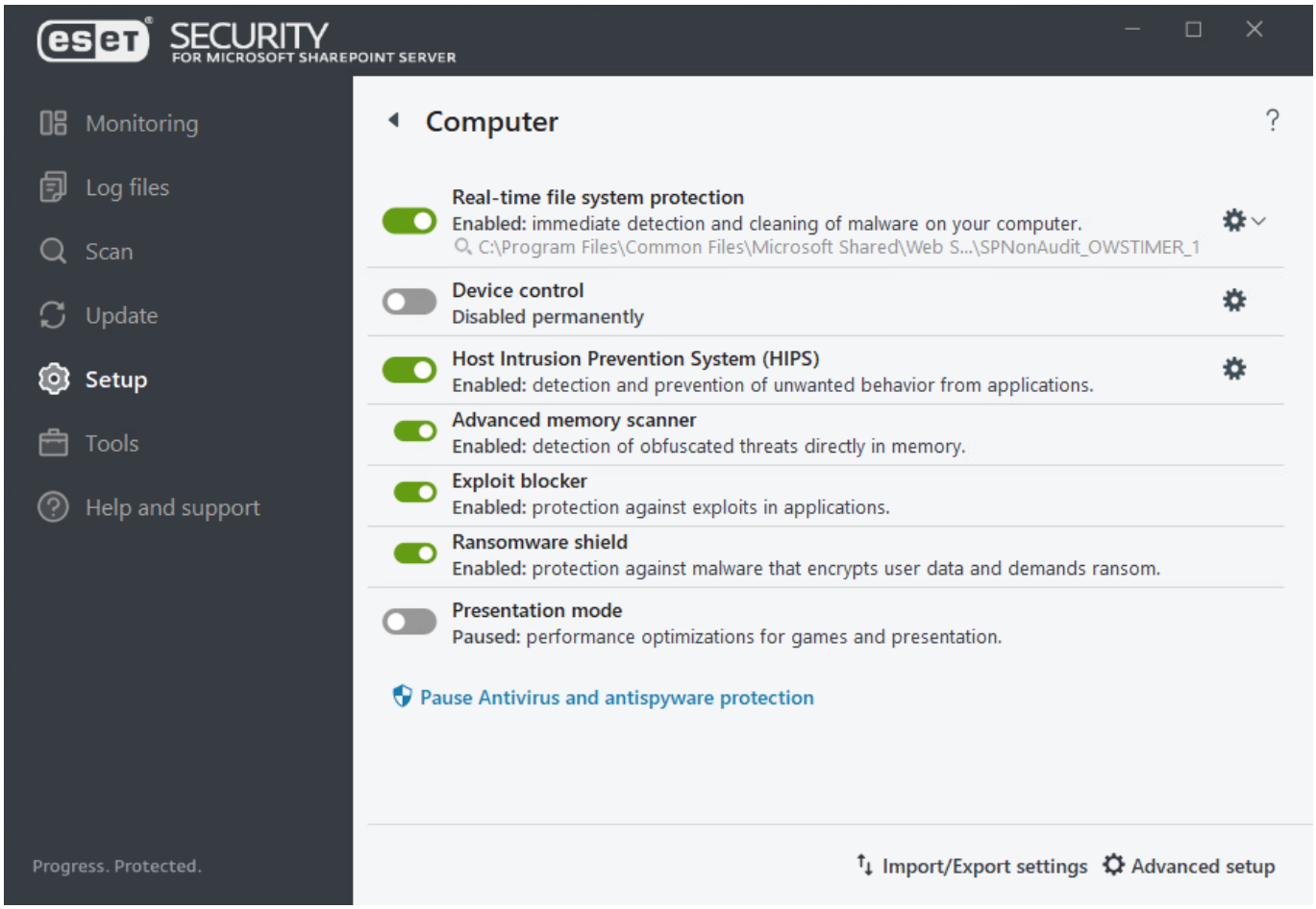
- Advanced memory scanner
- Exploit blocker
- Ransomware shield

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.



# 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

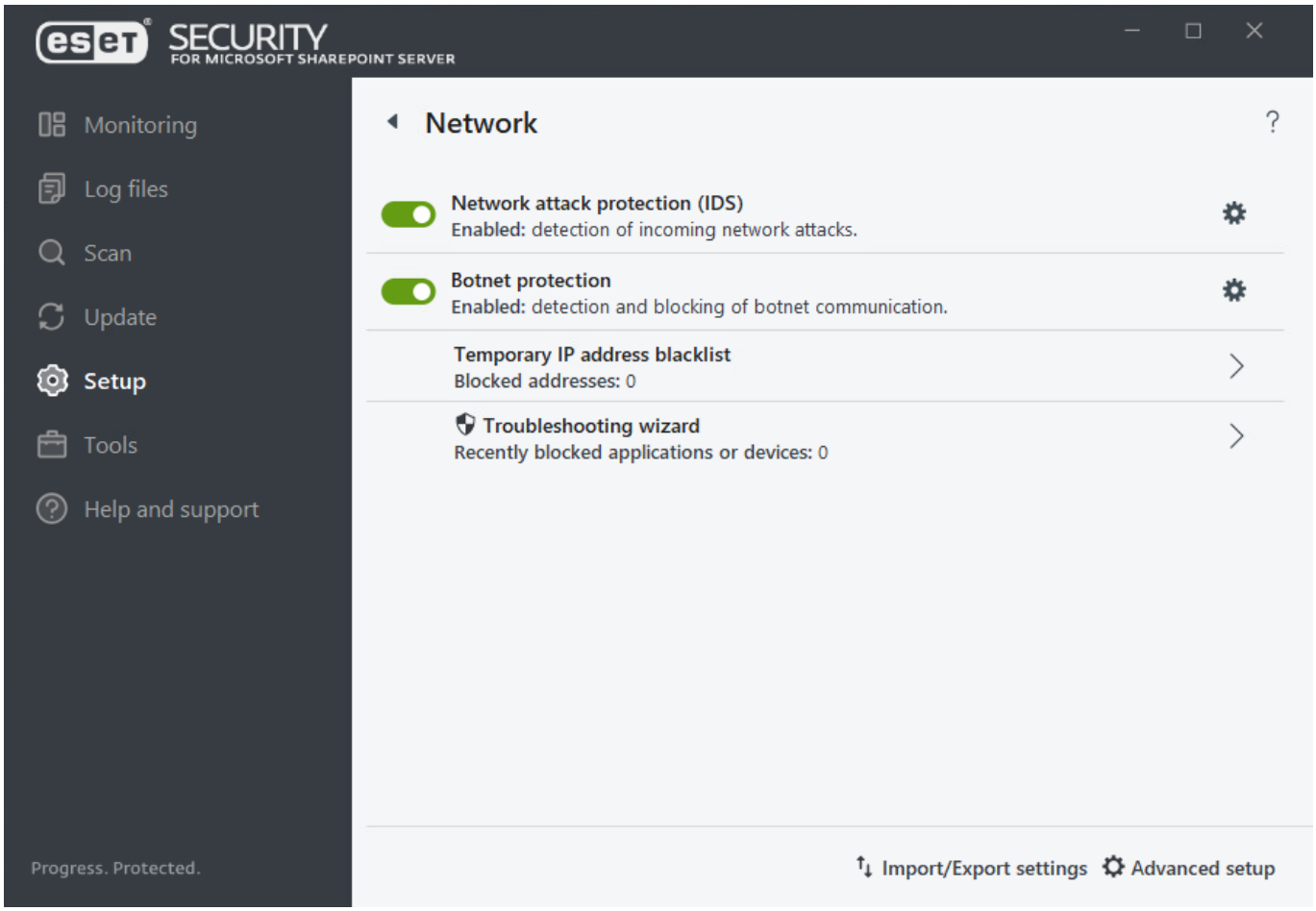
Detection and blocking of Botnet communication. Quickly and accurately identifies malware in the system.

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.



# 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.

Select a time period from the drop-down menu during which communication has been blocked. A list of recently blocked communications gives you an overview of the application type or device, reputation, and the total number of applications and devices blocked during that period. For more details about blocked communication, click **Details**.

The next step is to unblock the application or device you are experiencing connectivity problems.

When you click Unblock, the previously blocked communication will be allowed. If you continue to experience problems with an application or your device does not work as expected, click **The application still doesn't work**. All communications previously blocked for that device will now be allowed. If the issue persists, restart the computer.

Click **Show changes** to see rules created by the wizard.

Click **Unblock another** to troubleshoot communications issues with a different device or application.

# Web and email

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

Web access protection

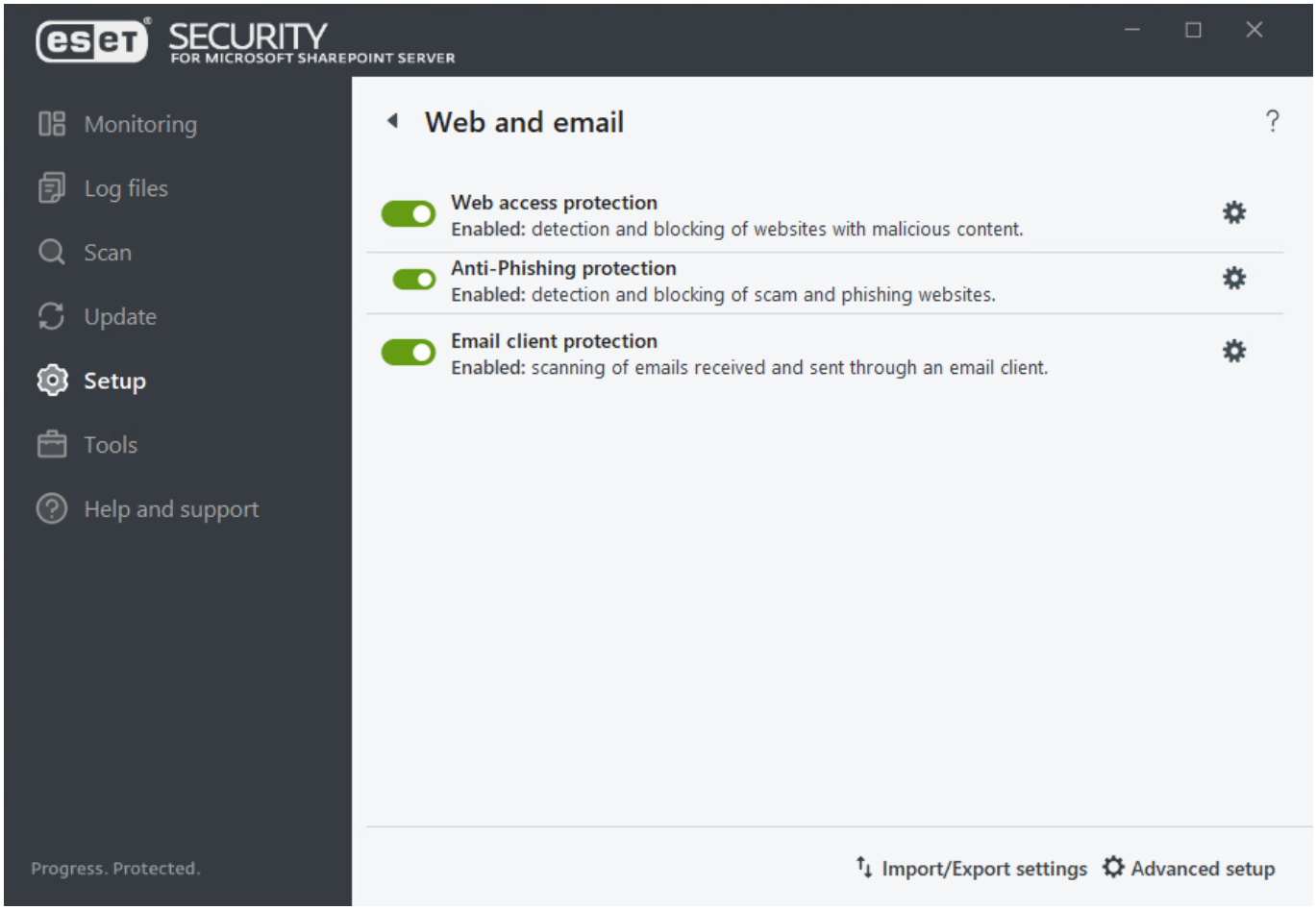
If enabled, all HTTP or HTTPS traffic is scanned for malicious software.

Anti-Phishing protection

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

Email client protection

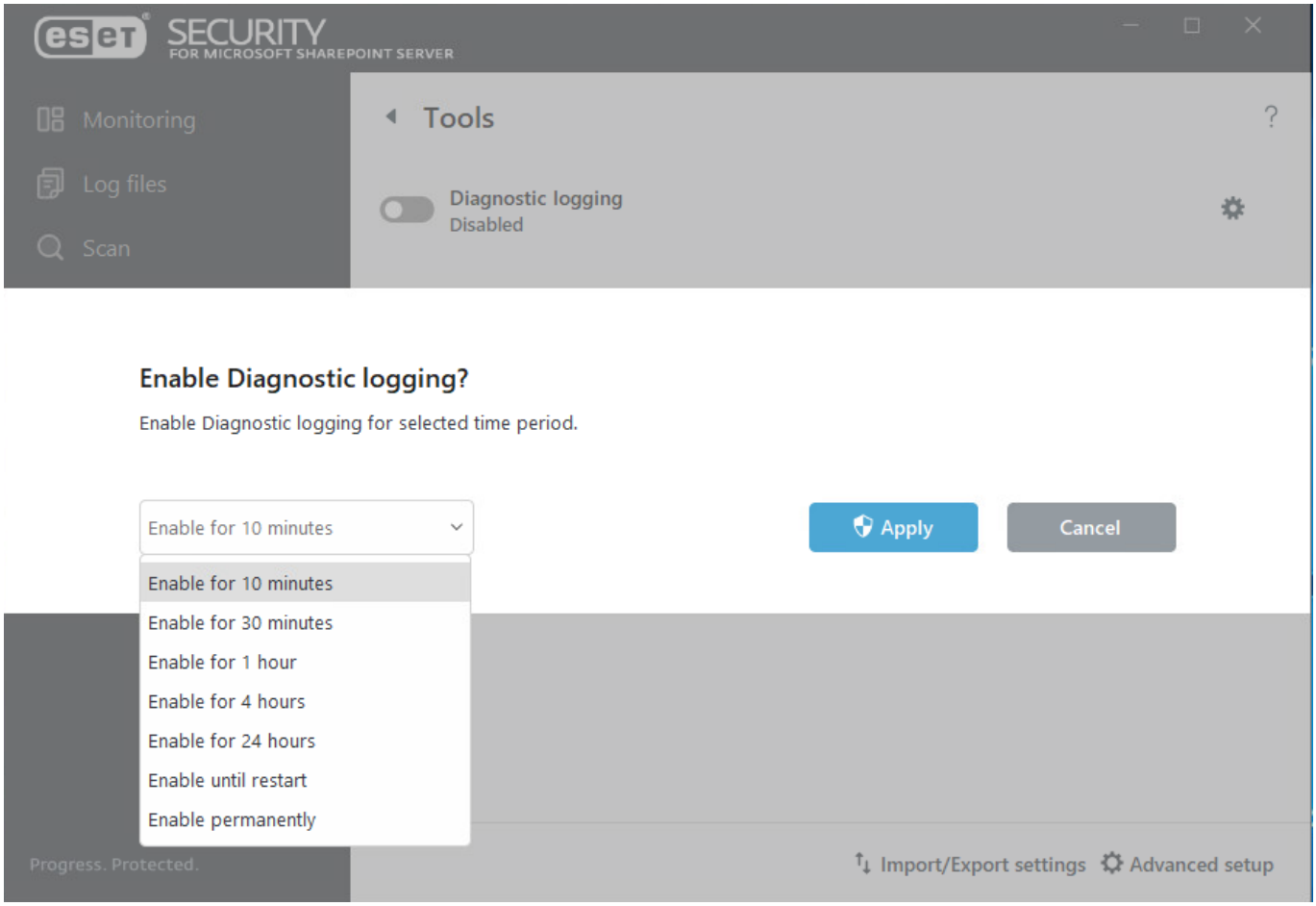
Monitors communication received through the POP3 and IMAP protocols.




# Tools - Diagnostic logging

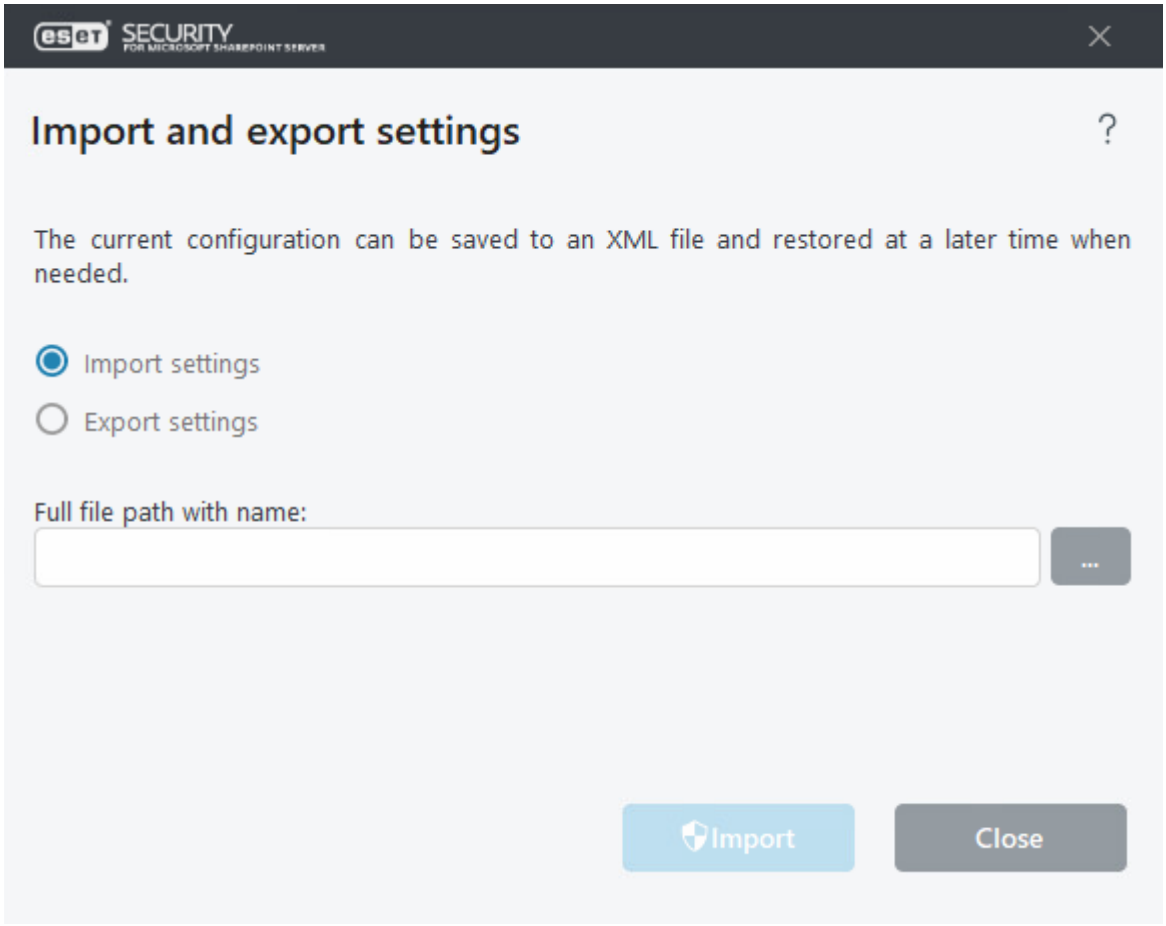
You can enable Diagnostic logging when you need detailed information about the behavior of a specific ESET Security for Microsoft SharePoint feature, for example, when troubleshooting. When you click the gear icon, you can configure for what features should diagnostic logs be collected.

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 Security for Microsoft SharePoint will be collecting detailed logs according to what features are enabled.




# Import and export settings

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

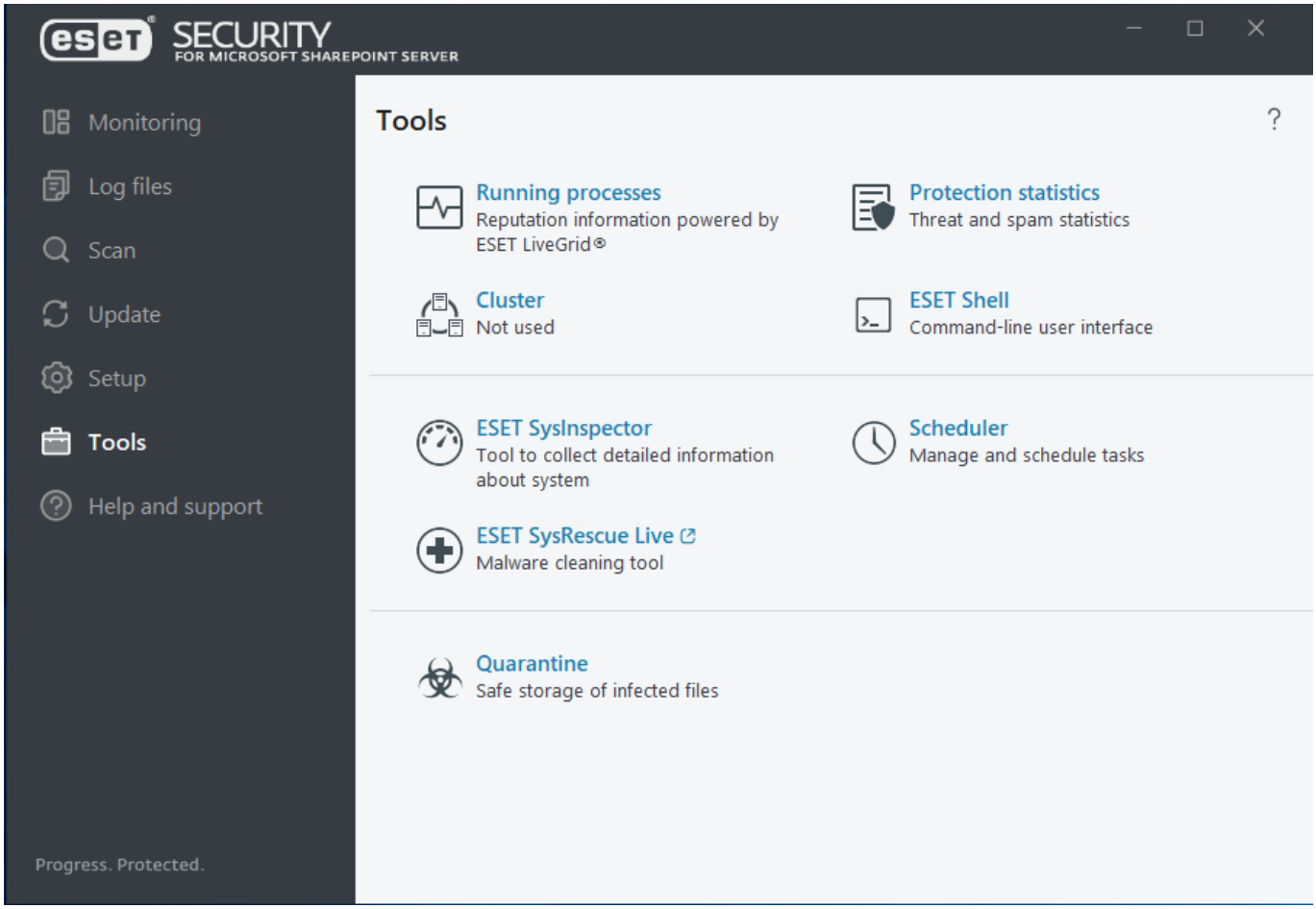



If you do not have rights to write the exported file to specified directory, you may encounter an error when exporting settings.

# Tools

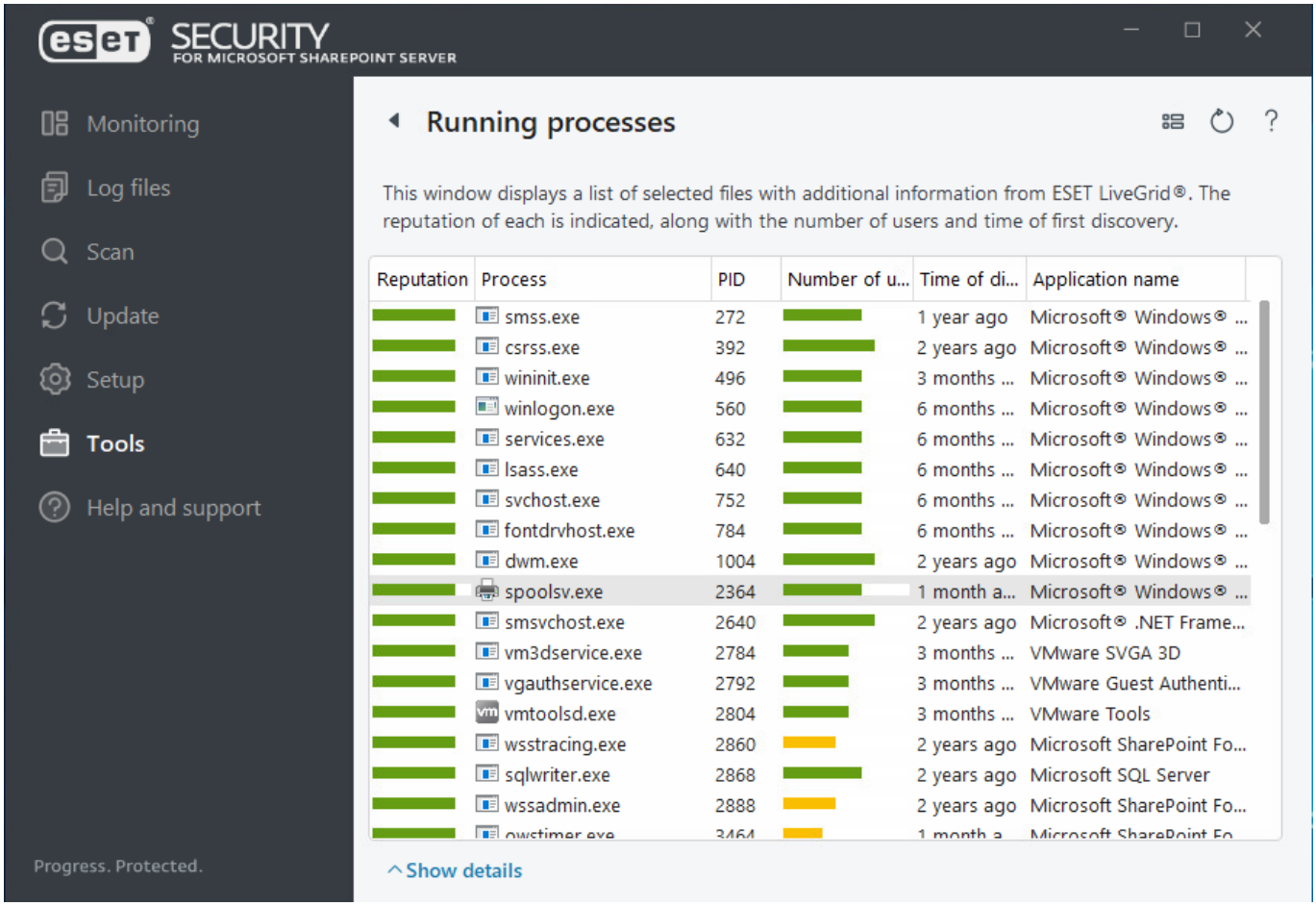
The following features are available for ESET Security for Microsoft SharePoint administration:

- Running processes
- Protection statistics
- Cluster
- ESET Shell
- ESET SysInspector
- ESET SysRescue Live
- Scheduler
- Submit sample for analysis
- Quarantine




# Running processes

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




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 Security for Microsoft SharePoint 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 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. |

An application is not necessarily malicious software when marked as Unknown (orange). Usually, it is just a newer application. If unsure about the file, use the Submit sample for analysis feature to send the file to the ESET virus Lab. If the file is 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.

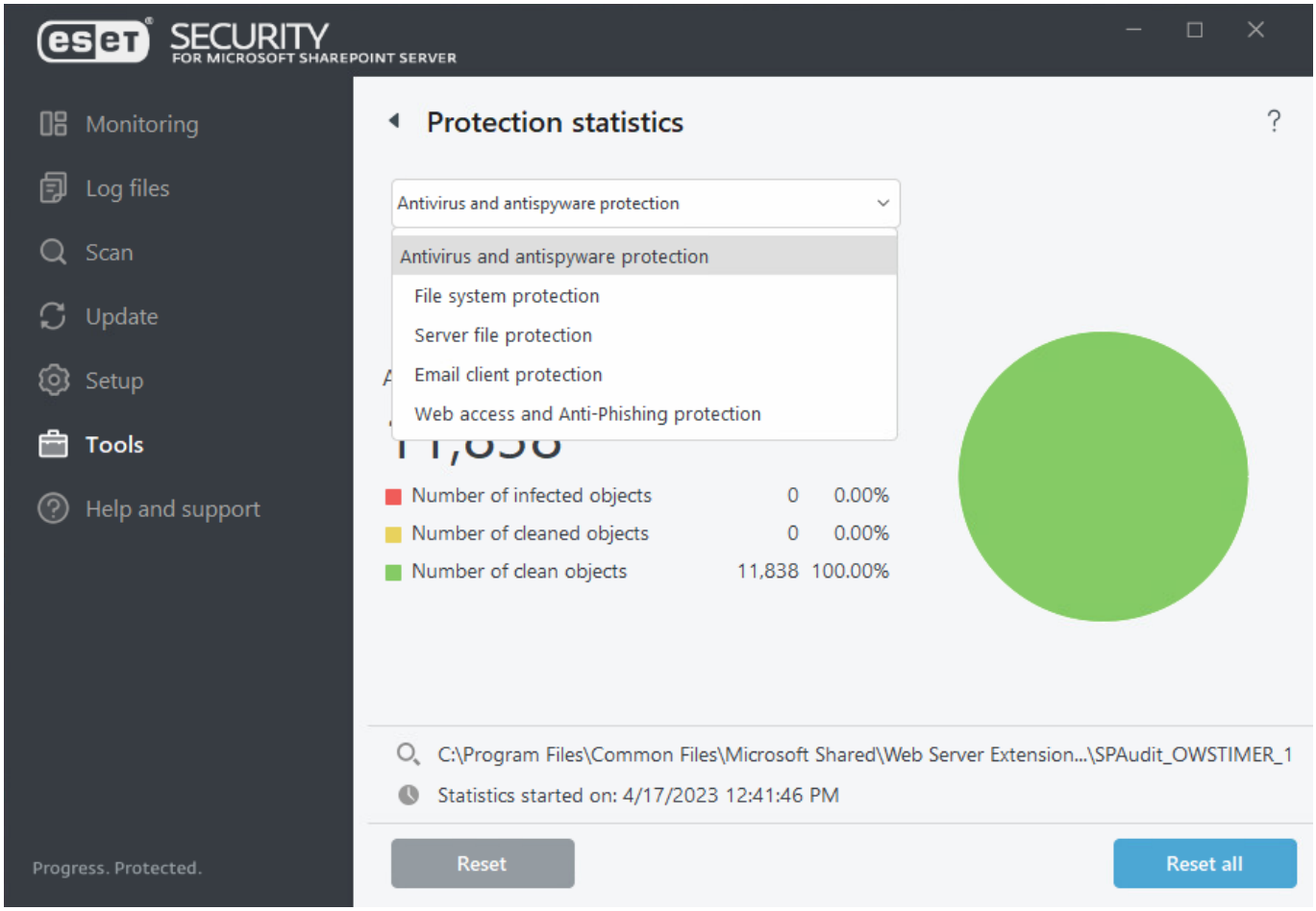
Add to processes exclusions

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.

# Protection statistics

To view statistical data related to protection modules of ESET Security for Microsoft SharePoint, 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**.




The following statistic graphs are available in ESET Security for Microsoft SharePoint:

**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.

**Server file protection**

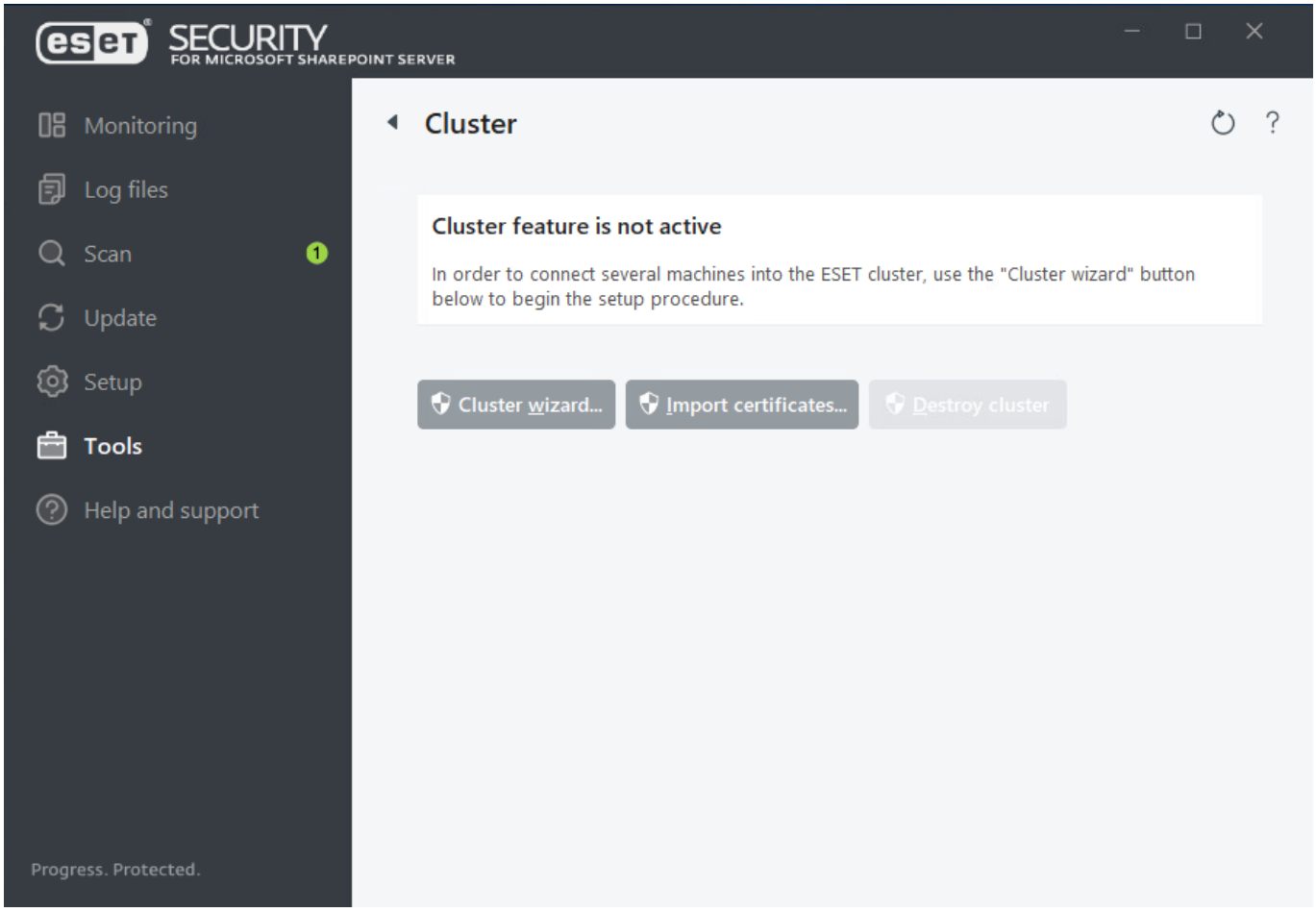
Displays SharePoint objects that were uploaded or downloaded.

# Cluster

The ESET Cluster is a P2P communication infrastructure of the ESET line of products for Microsoft Windows Server.

This infrastructure enables ESET server products to communicate with each other and exchange data such as configuration and notifications, and can 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.

Settings of the User interface and Scheduled tasks are not synchronized between ESET Cluster nodes. This is on purpose.




The creation of ESET Clusters between ESET Security for Microsoft SharePoint 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).

When releasing an email from quarantine, ESET Security for Microsoft SharePoint 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.

When you have added nodes to your ESET Cluster, the next step is the installation of ESET Security for Microsoft SharePoint on each node. This is done automatically during ESET Cluster setup. Credentials that are required for remote installation of ESET Security for Microsoft SharePoint 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).

You cannot 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 Security for Microsoft SharePoint 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**

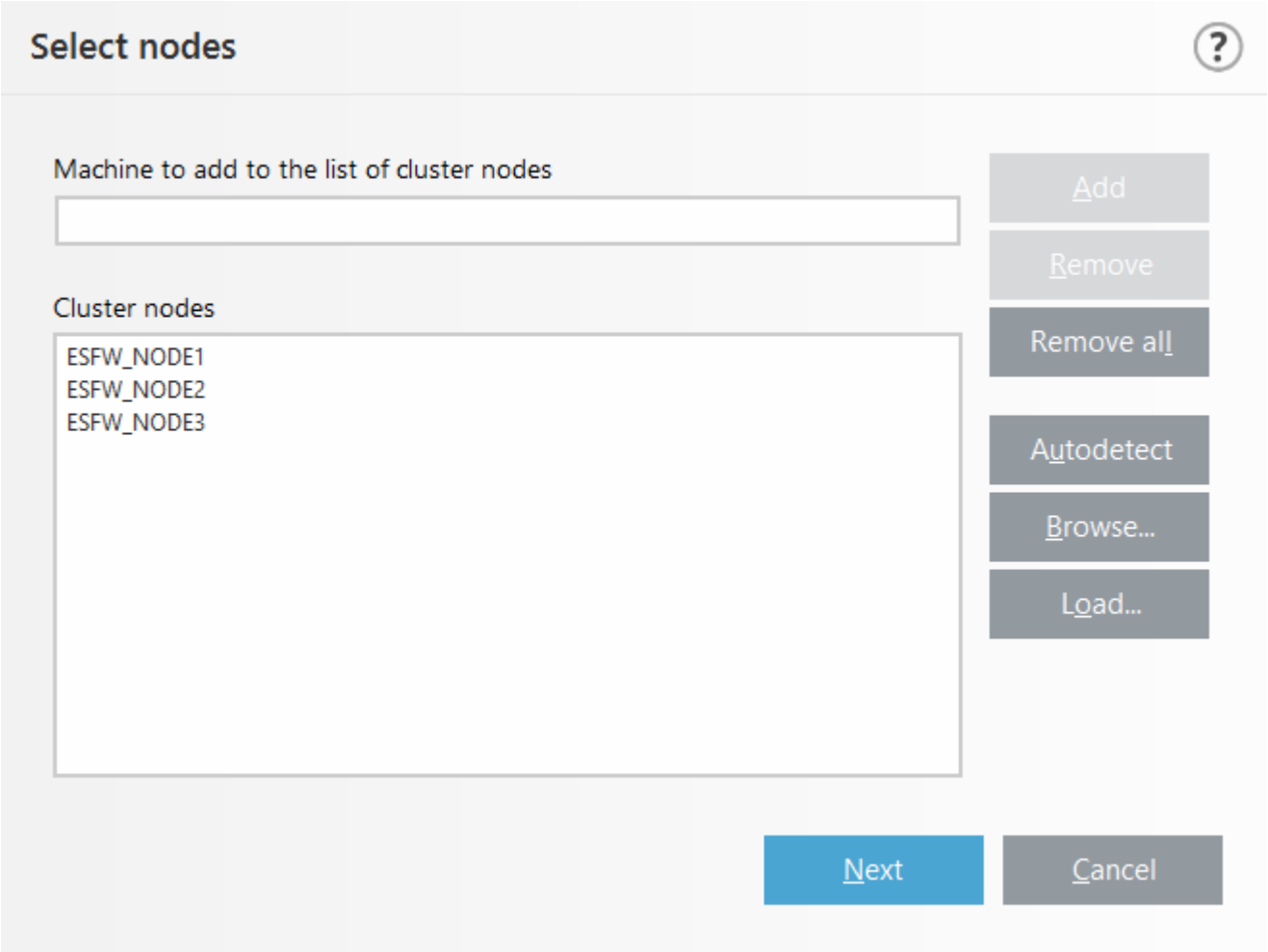
Automatically adds nodes from an existing Windows Failover Cluster / Network Load Balancing (NLB) Cluster. The server you are using to create the ESET Cluster from needs to be a member of this Windows Failover Cluster / NLB Cluster to automatically add the nodes. The NLB Cluster must have the **Allow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

**Browse**

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

**Load**

To import list of nodes from file.




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.

> 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 Security for Microsoft SharePoint will be installed automatically on each node (provided their operating systems are the same architecture).
- **Manual** - Manually install ESET Security for Microsoft SharePoint (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.

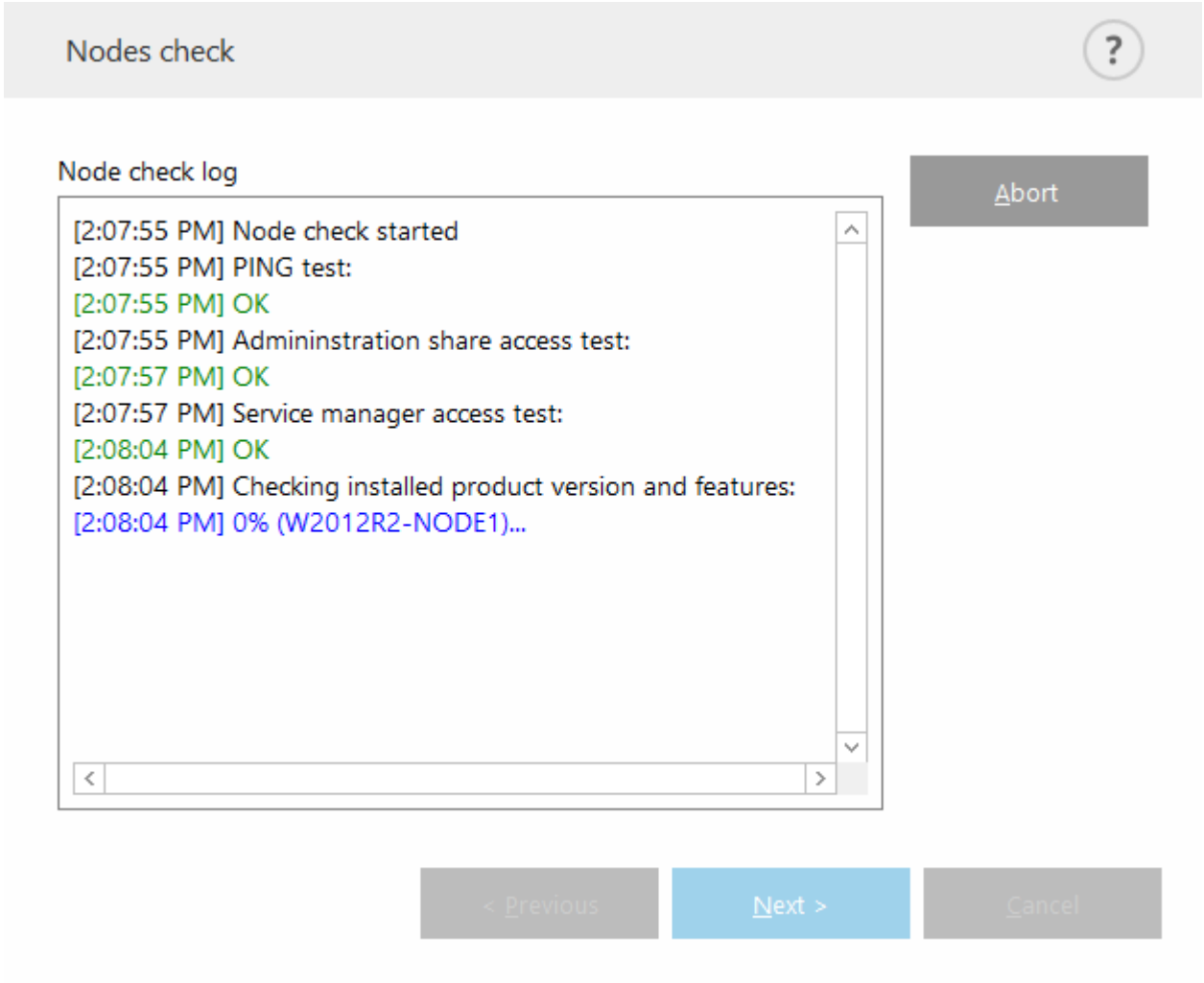
> To create an ESET Cluster with a mixed operating system architecture (32 bit and 64 bit), install ESET Security for Microsoft SharePoint manually. Operating systems in use will be detected during next steps and you will see this information in the log window.

# Cluster wizard - Nodes check

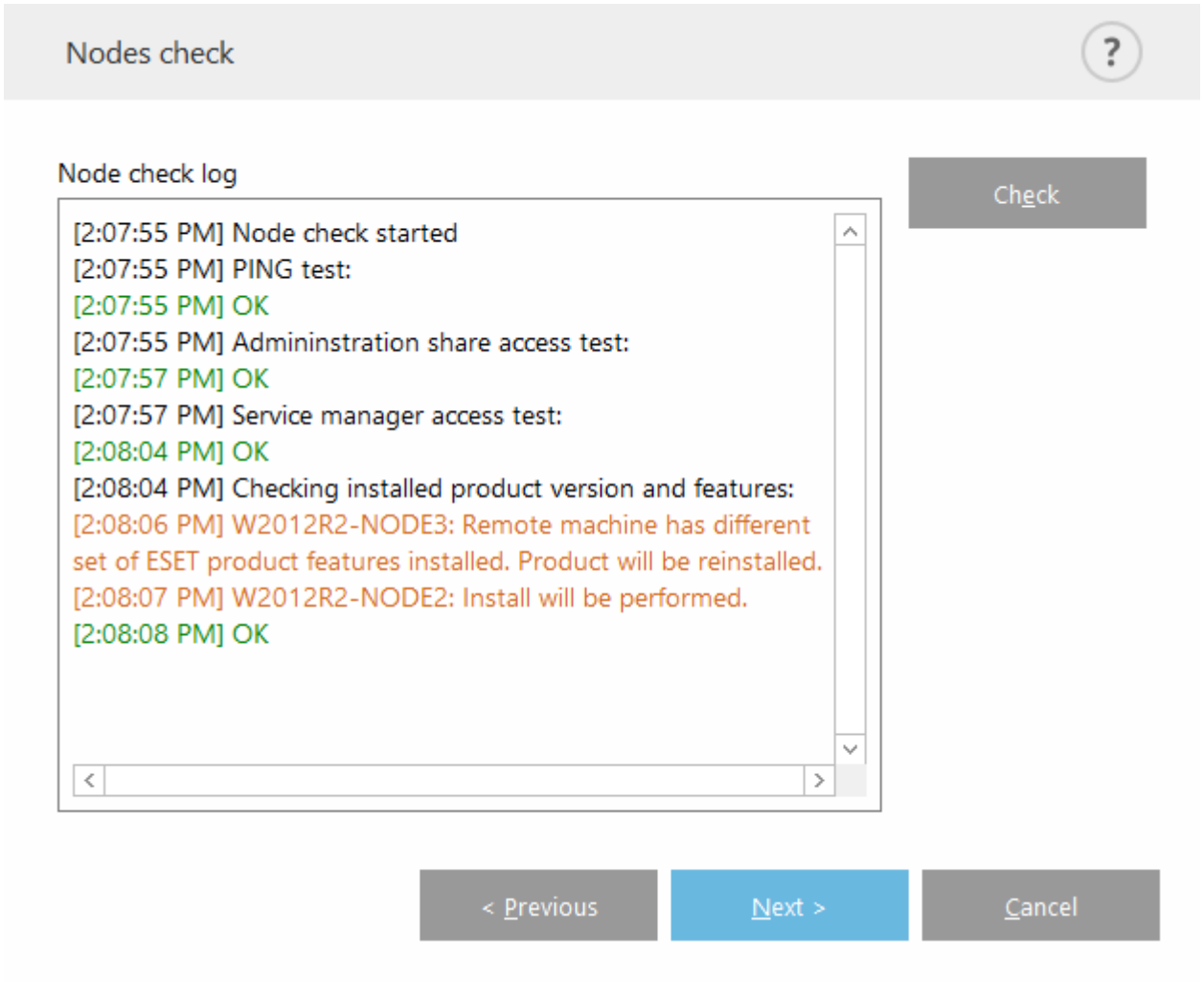
After specifying installation details a node check is run. The following information will be displayed in the **Nodes check log**:

- 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

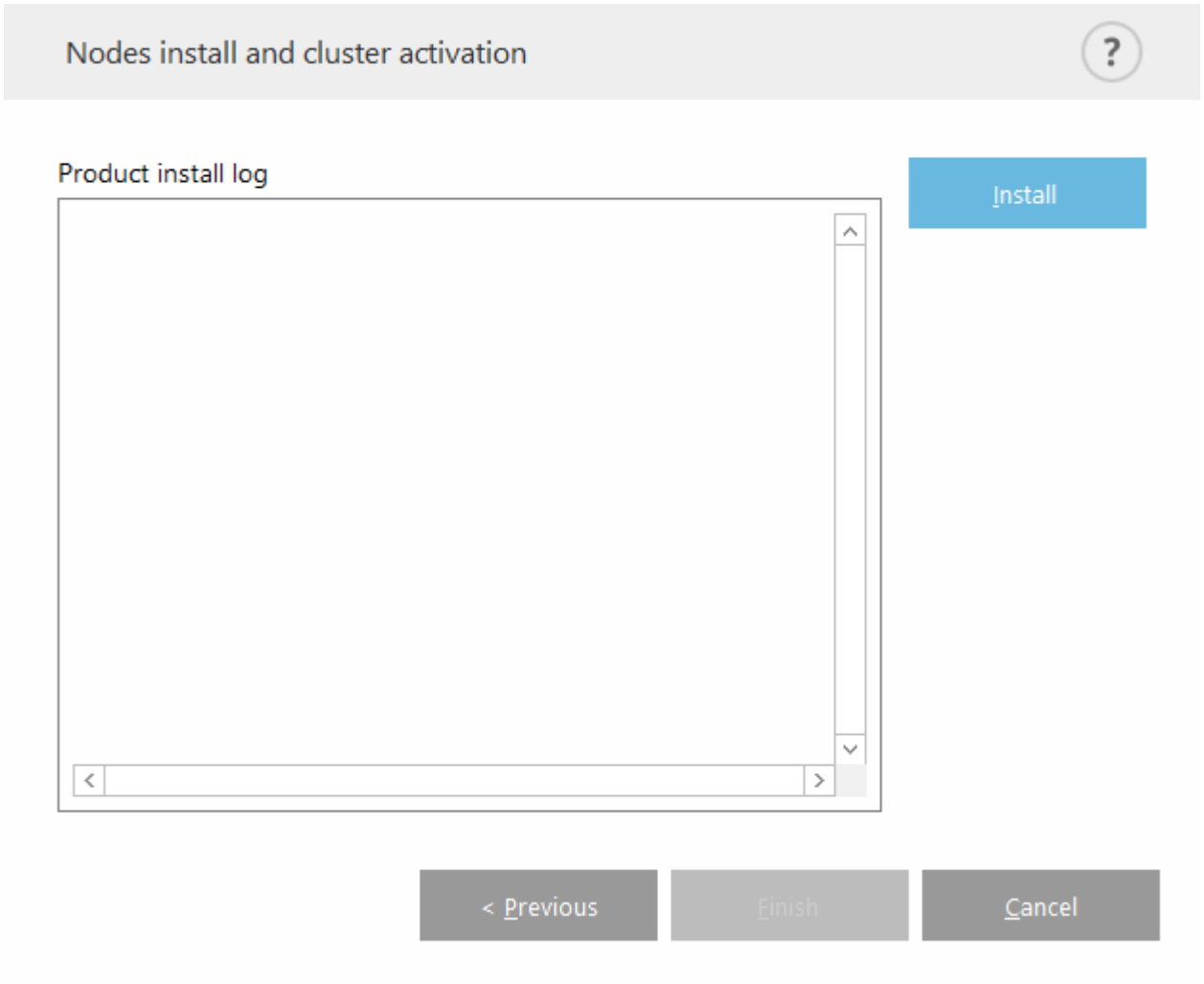



You will see the report once the node check is finished:

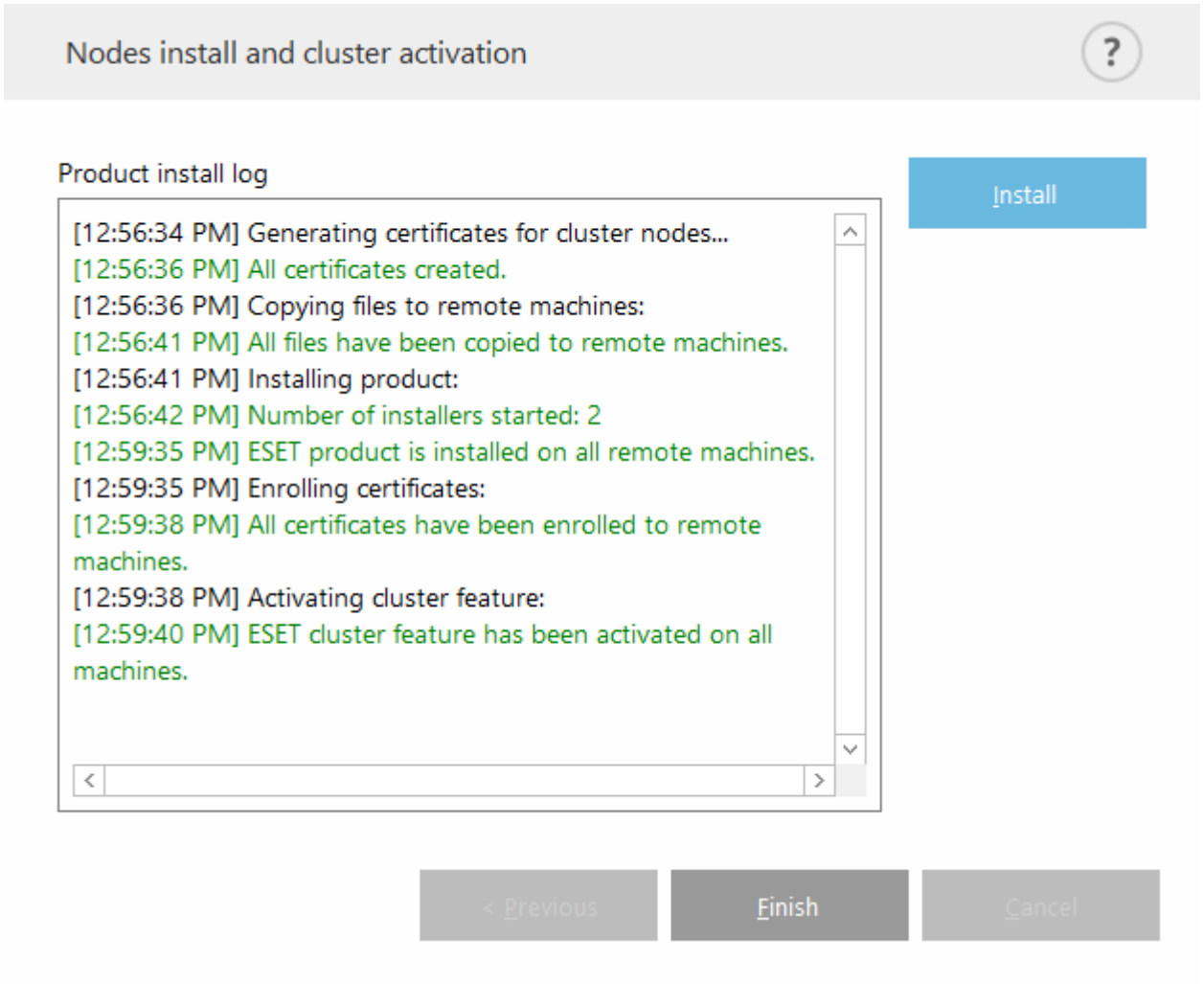



# Cluster wizard - Nodes install

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.




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




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

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

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 Security for Microsoft SharePoint. 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 using 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 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.

> We recommend you open the eShell using Run as Administrator for full functionality. The same applies to executing a single Windows Command Prompt (cmd) command. Open the prompt using **Run as Administrator**. Failing to run the command prompt as Administrator will stop you from running commands due to a 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 unfamiliar with all the commands. Interactive mode will make it easier for you when navigating through eShell. It also shows you available commands you can use within a specific 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.

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

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 will get an **Access Denied** message. This is for security reasons.

Settings changes are required to use eShell commands from the Windows Command Prompt. Read more about running batch files.

There are two ways to enter an Interactive mode in eShell:

1. Via **Windows Start menu**: Start > All Programs > ESET > ESET Security for Microsoft SharePoint > ESET Shell

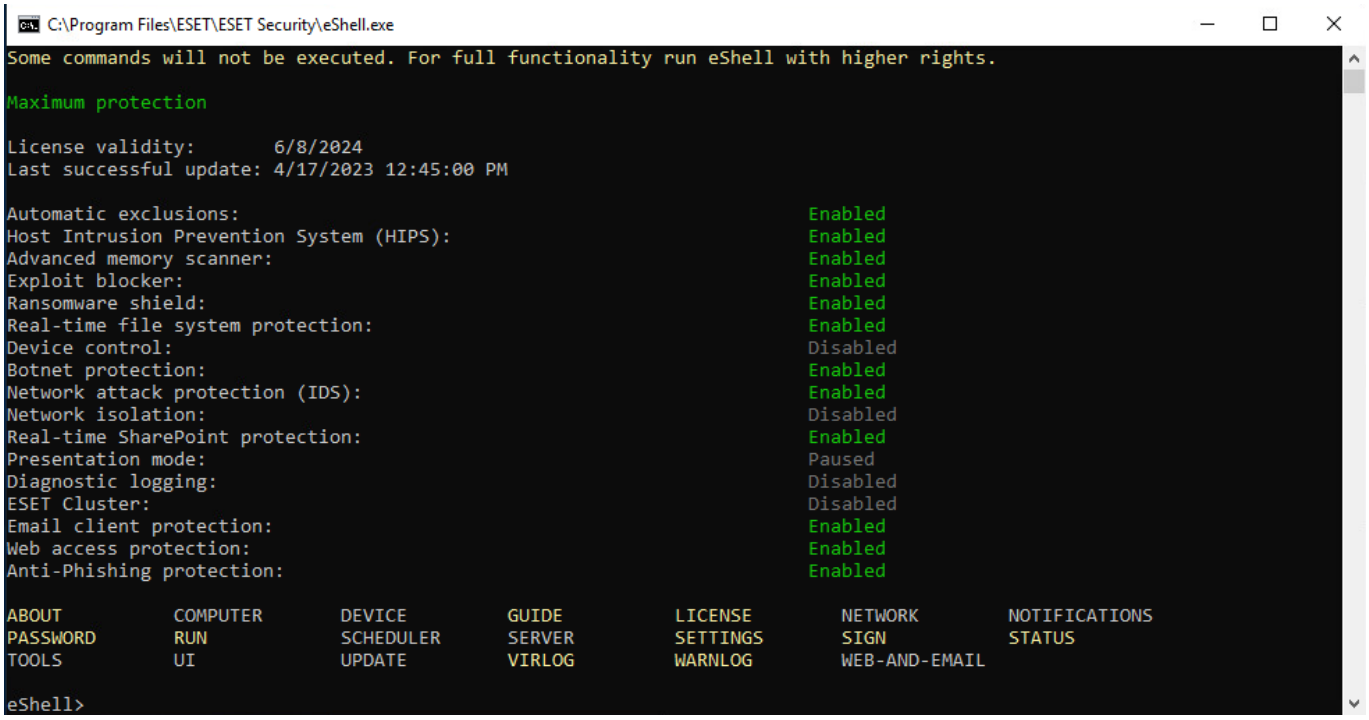
2. From **Windows Command Prompt** by typing in `eshell` and pressing the Enter key

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

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

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

Next time you run eShell, you will see this screen:




Commands are not case-sensitive. You can use uppercase (capital) or lowercase letters; 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 specific 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 specific 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 specific command and that it is exactly what you want to execute.

> **i** Commands are not case-sensitive. You can use uppercase (capital) or lowercase letters; 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 Security for Microsoft SharePoint 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 enables to 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 |

> **i** 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 execute a command from here or type the context name to navigate within the tree. For example, when you type the `TOOLS` context, it will list all commands and sub-contexts available.




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).

> ✓ 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 specific 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. Do not type a path if the command is contained in the current context. 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.

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

### Argument

An argument is an action that is performed for a specific command. For example, the command `CLEAN-LEVEL` (located in `COMPUTER REAL-TIME ENGINE`) can be used with the 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 is the arguments `ENABLED` or `DISABLED`, which enable or disable a certain feature or functionality.

### Abbreviated form / Shortened commands

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

```
✔ 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:

```
  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
```

If two commands or contexts start with the same letters (such as `ADVANCED` and `AUTO-EXCLUSIONS`, and you type `A` as shortened context), eShell will not be able to decide which context of these two you want to type. 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.

ℹ 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 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.

Press Tab to complete or cycle through available variations when typing a command.

Press SHIFT + Tab to cycle backward. Mixing abbreviated forms 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 that 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)` The command can be used anywhere, regardless of the 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 or any of its aliases.

The alias `VIRLOG` is an alias for the command `DETECTIONS` located in the `TOOLS LOG` context. This way, the detections command is available from the `ROOT` context, making it easier to access (you do not have to type `TOOLS` and then `LOG` sub-context and run it directly from `ROOT`).

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

### Password protected settings

ESET Security for Microsoft SharePoint settings can be protected by a password. You can set a password using GUI or eShell using the `set ui access lock-password`.

You must type this password interactively for certain commands (such as changing settings or modifying data). If you plan to work with eShell for a longer period and do not want to type 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; you must use the `set password` again when you start a new session and want eShell to remember it.

### 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 your keyboard's Up and Down arrow keys to navigate the history. When you find the command you were looking for, you can execute it again or modify it without typing 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 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.

> Commands are not case-sensitive. You can use uppercase (capital) or lowercase letters; 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 the version number of each component.

### CONTEXT PATH:

```
root
```

### PASSWORD

To execute password-protected commands, you are prompted to type in a password for security reasons. This applies to commands that disable protection and those that may affect ESET Security for Microsoft SharePoint

configuration. You will be prompted for a password every time you execute such a command. You can define this password to avoid entering a password every time. It will be remembered by eShell and automatically entered when a password-protected command is executed.

Your password only works for the current eShell interactive session. This defined password will be dropped when you exit eShell. 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.

We recommend that you use signed batch files whenever you can. This way, you will avoid plain text passwords in the batch file (if the method is 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 type password as parameter

`password` - Password

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

`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 Security for Microsoft SharePoint and

enables you to pause / resume protection (similar to main program window).

**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

> You cannot disable all protection features with a single command. Using the `status` command, you can manage protection features and modules one by one. Each protection feature or module has its `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` |
| 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` |

| Feature | Context and command |
| --- | --- |
| 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.

# Keyboard shortcuts

The eShell supports keyboard shortcuts (similar to Microsoft Windows *cmd.exe* command prompt). Use certain keys (key combinations) on your keyboard to perform actions in eShell. For example, show the history of commands, repeat part of the history command, move a word or erase a line.

Available shortcuts:

F1 - print characters of the actual history command one by one.

F2, X - repeat part of the history command; up to character X.

F3 - write actual history command.

F4, X - beginning from the current cursor position on the actual command; delete up to character X.

F5 - the same as the UP ARROW.

F7 - show the history of commands.

ALT + F7 - clear command history.

F8 - Move backward through the command history, but only display commands matching the current text at the command prompt.

F9 - run a specific command from the command history.

RIGHT ARROW - the same as F1.

CTRL + HOME - erase line to the left.

CTRL + END - erase line to the right.

CTRL + LEFT ARROW - move one word to the left.

CTRL + RIGHT ARROW - move one word to the right.

# 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.

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

You can also chain commands, which is sometimes necessary. For instance, if you want to type a specific scheduled task, type 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 eShell instance. 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"`.

The execution policy is set to **Limited Scripting** by default for security reasons. It enables you to use eShell as a monitoring tool, but it will not let you make configuration changes to ESET Security for Microsoft SharePoint 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 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 the main program window in **Advanced Setup** (**F5**)> **User interface** > ESET Shell.

### Signed batch files

eShell enables you to secure common batch files (**.bat*) with a signature. Scripts are signed with the same password that is used for settings protection. To sign a script you need to enable settings protection first. This can be done via the main program window or within eShell using `set ui access lock-password` command. You can start signing batch files when the protection password is set up.

> You must sign all scripts again if you change your settings protection password. Otherwise, the scripts will fail to execute 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. Type 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.

> 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.

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

# ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer, 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 type 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 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.
- **Create** - Creates a new log. Type a short comment describing the log to be created and click **Create**. 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).
- **Create** - Creates a new log. Type a short comment describing the log to be created and click **Create**. 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 *.esil* file. Alternatively, choose a *.xml* file or zipped *.xml*.

# ESET SysRescue Live

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

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

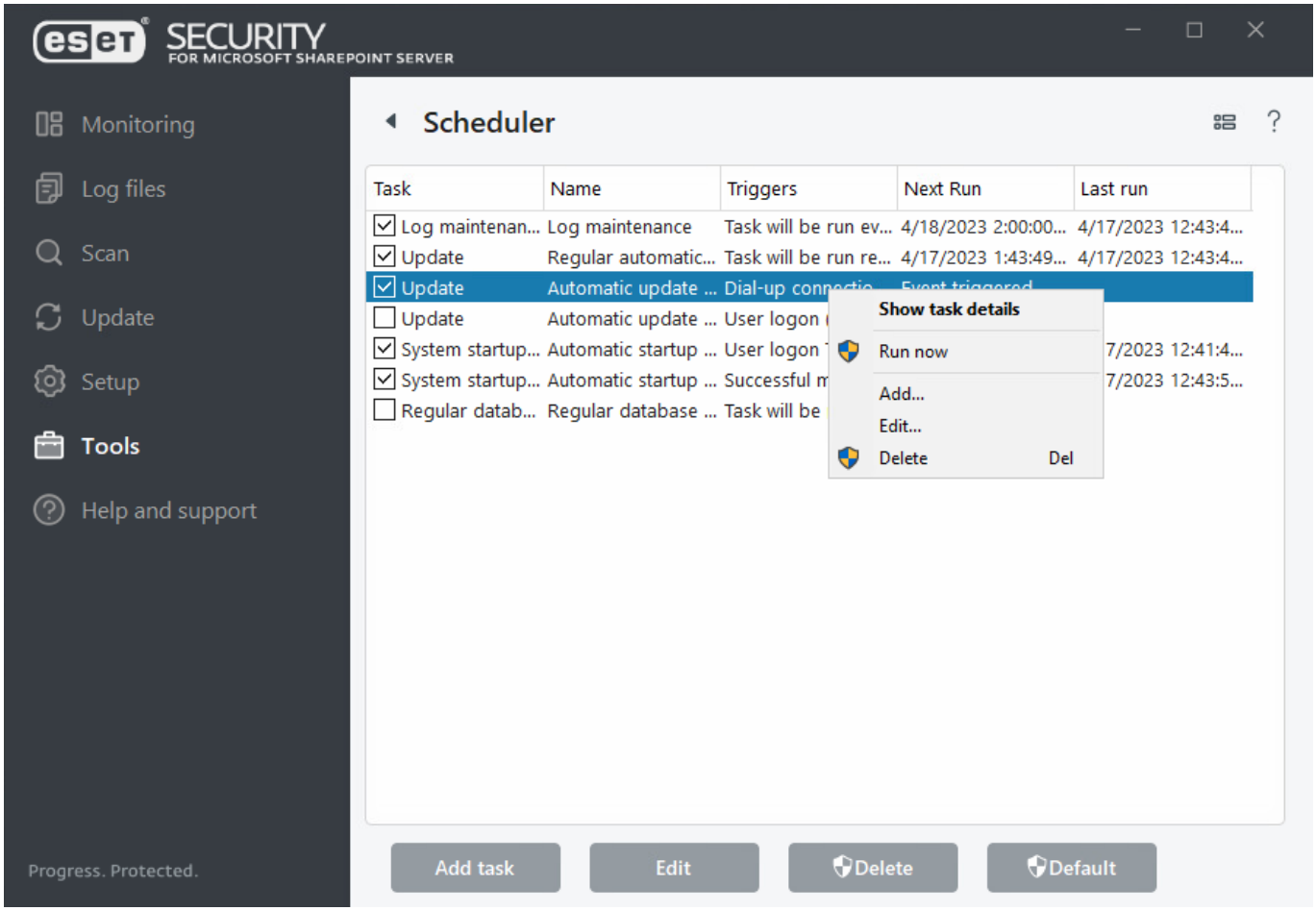
# Scheduler

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 pre-defined default tasks:

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

Select the appropriate check boxes to activate or deactivate tasks.



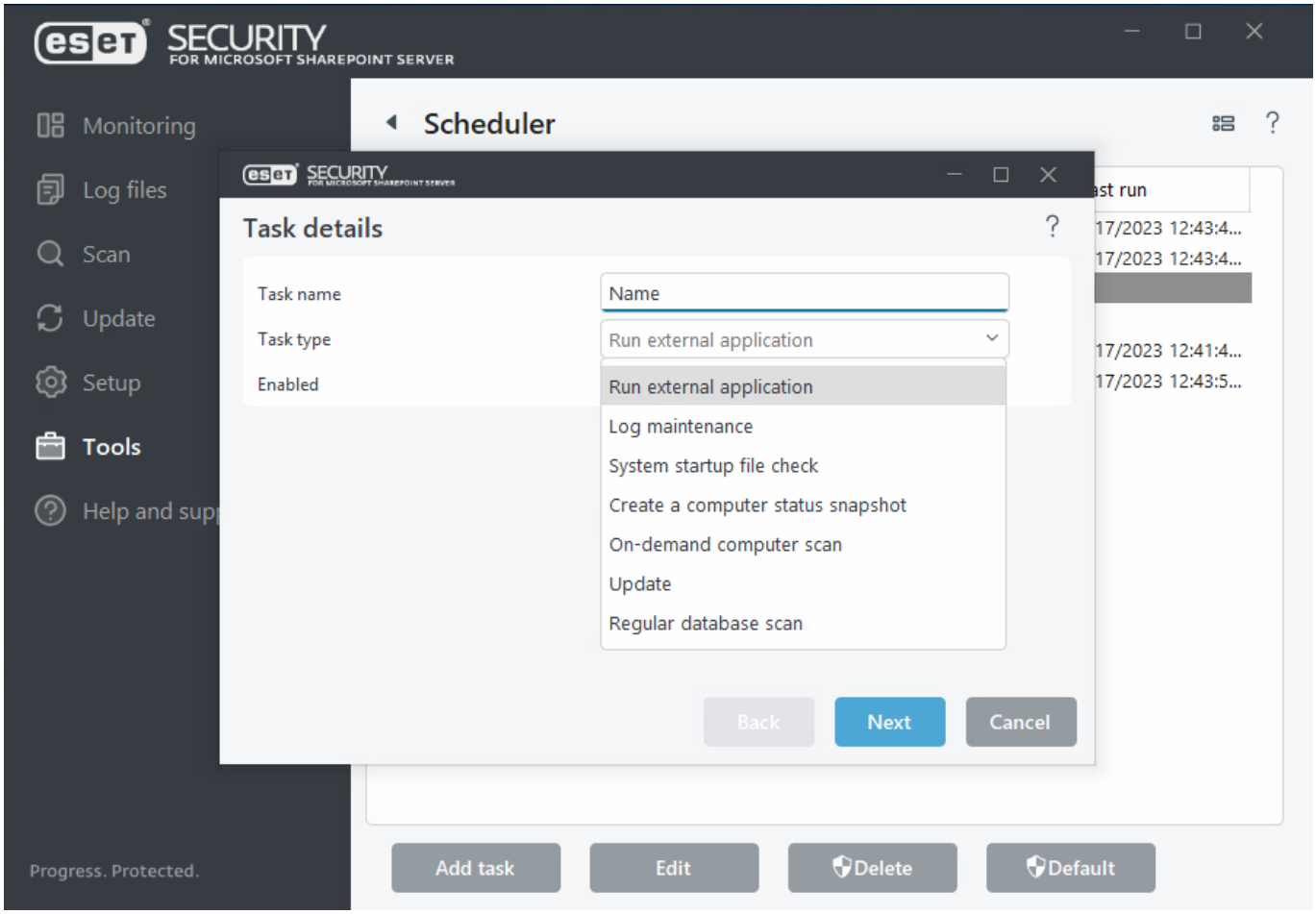

To perform the following actions, right-click a task:

| 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

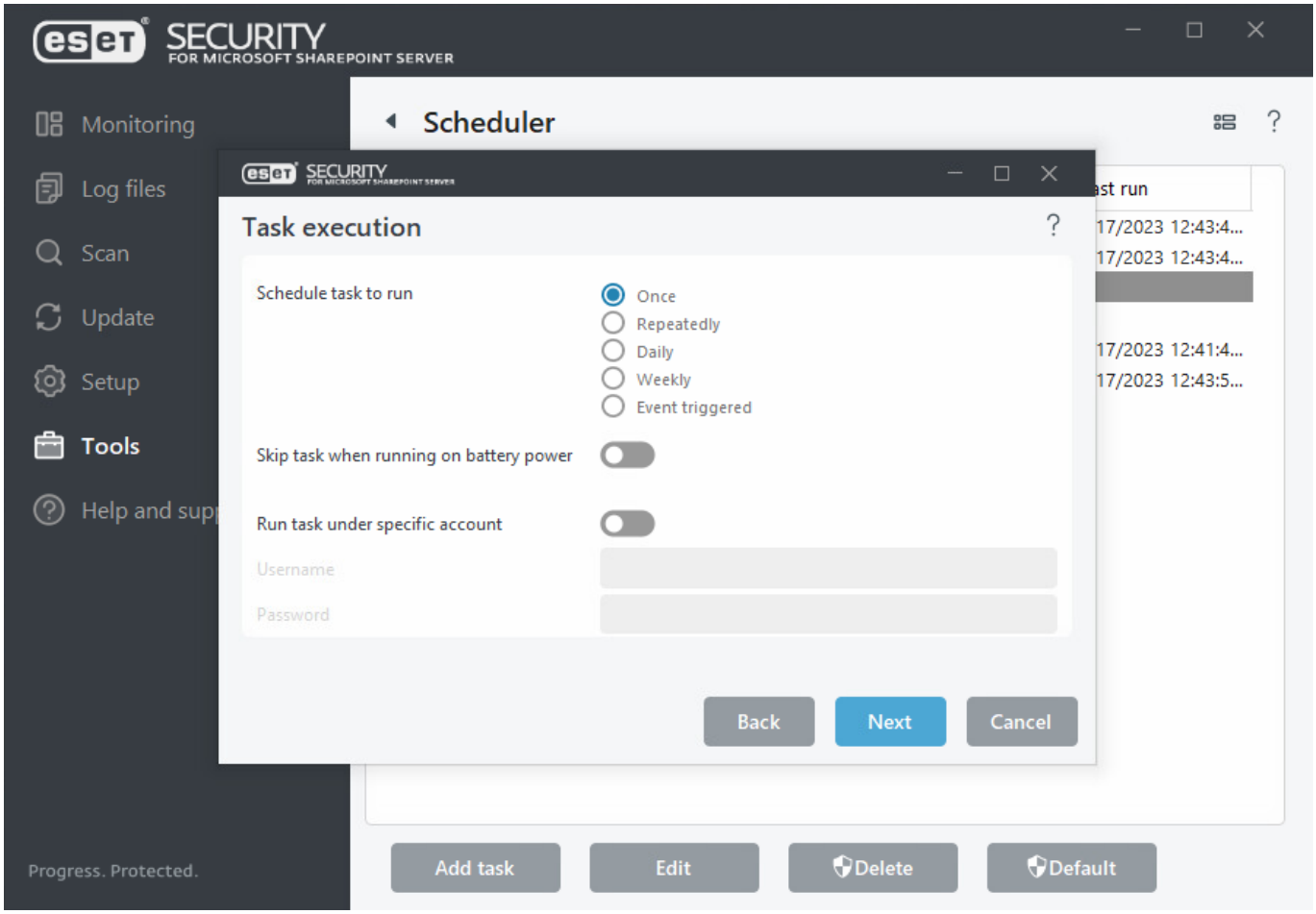
To create a new scheduled task:

1. Click **Add task**.
2. Type a **Task name** and configure your custom scheduled task.
3. Task type - Select the applicable **Task type** from drop-down menu.

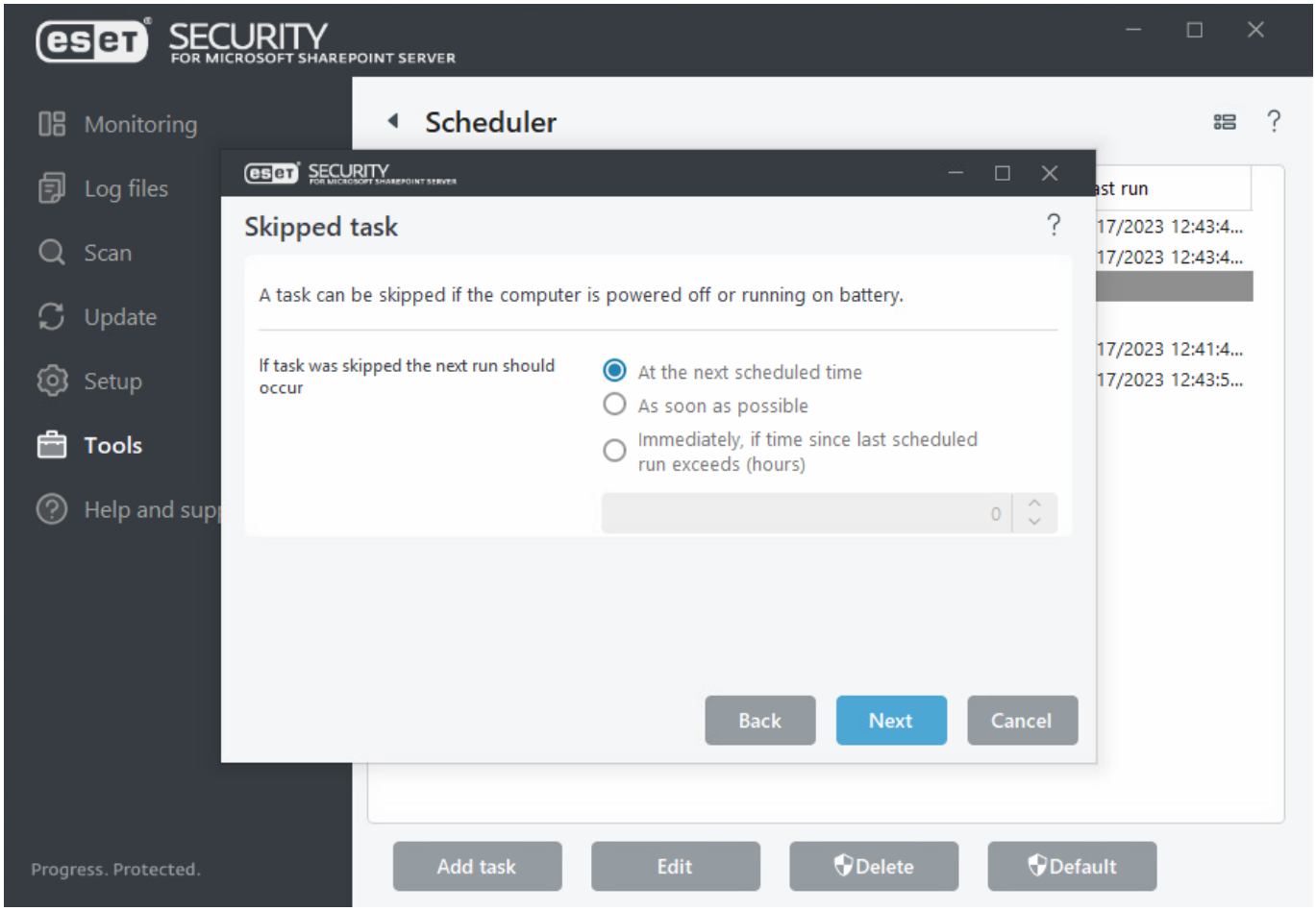



To deactivate a task, click the slide bar next to **Enabled**. To activate the task later, use the check box in the Scheduler view.

4. Task execution - 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.




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




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. Type **Task name** and select your desired **Task type** from the drop-down menu:

- **Run external application** - Schedules the execution of an external application. You can use specific account to run the scheduled task as (Run task under specific account option).

- **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 login.

- **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** - Scan files and folders stored locally or on a network share (shared storage, such as NAS). Use specific account to run the scheduled task as (Run task under specific account option).
- **Update** - Schedules an update task to perform an update of detection engine and program modules.
- **Regular database scan** - Lets you schedule a Database scan and choose items that will be scanned. It is basically an On-demand database scan.
- **Hyper-V scan** - Schedules a scan of the virtual disks within Hyper-V.

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 execution

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.

**Skip task when running on battery power** - When enabled, the task will not start if the system runs on batteries at the time the task should launch (for example, computers running on UPS).

**Run task under specific account** - Set username and password of a specific account to run scheduled task **Run external application** or **On-demand computer scan**. Use it to run **On-demand computer scan** if you want to scan network share, for example, NAS or other shared storage.

> Ensure the user account you are using to **Run task under specific account** is allowed to **Log on as a batch job** (SeBatchLogonRight). You can check the Policy Settings using Group Policy Management tool (Security Settings > Local Policies > User Rights Assignment > Log on as a batch job).

# Event triggered

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

Any of the following events can trigger the task:

- 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 login - The task will deploy when the user logs on to the system. If you log in to your computer several times a day, and choose 24 hours to perform the task only on the first login 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 type the path manually.
- **Work folder** - Define the external application's working directory. All temporary files of the selected Executable file will be created within this directory.
- **Parameters** - Command line parameters for the application (optional).

# Skipped task

If the task could not be run at the pre-defined 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 the time since the last run exceeds a specified value** - Time since the last run (hours). After you select this option, your task will always be repeated after the specified amount of time (in hours).

0

# Scheduled task overview

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

# Submit samples for analysis

The sample submission dialog lets you send a file or site to ESET for analysis. If you find a suspiciously behaving file on your computer or a suspicious site online, 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
- We do not accept your personal files (that you would like to scan for malware by ESET) as samples (ESET Research Lab does not perform on-demand scans for users)
- Use a descriptive subject line and enclose as much information about the file as possible (for example, a screenshot or the website you downloaded it from)

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. Type 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**

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

**File origin (URL address or vendor)**

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

**Notes and additional information**

Here you can type additional info or a description that will help identify the suspicious file.

> 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 type 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.

> 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)**

Type 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 site 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**

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

# Other

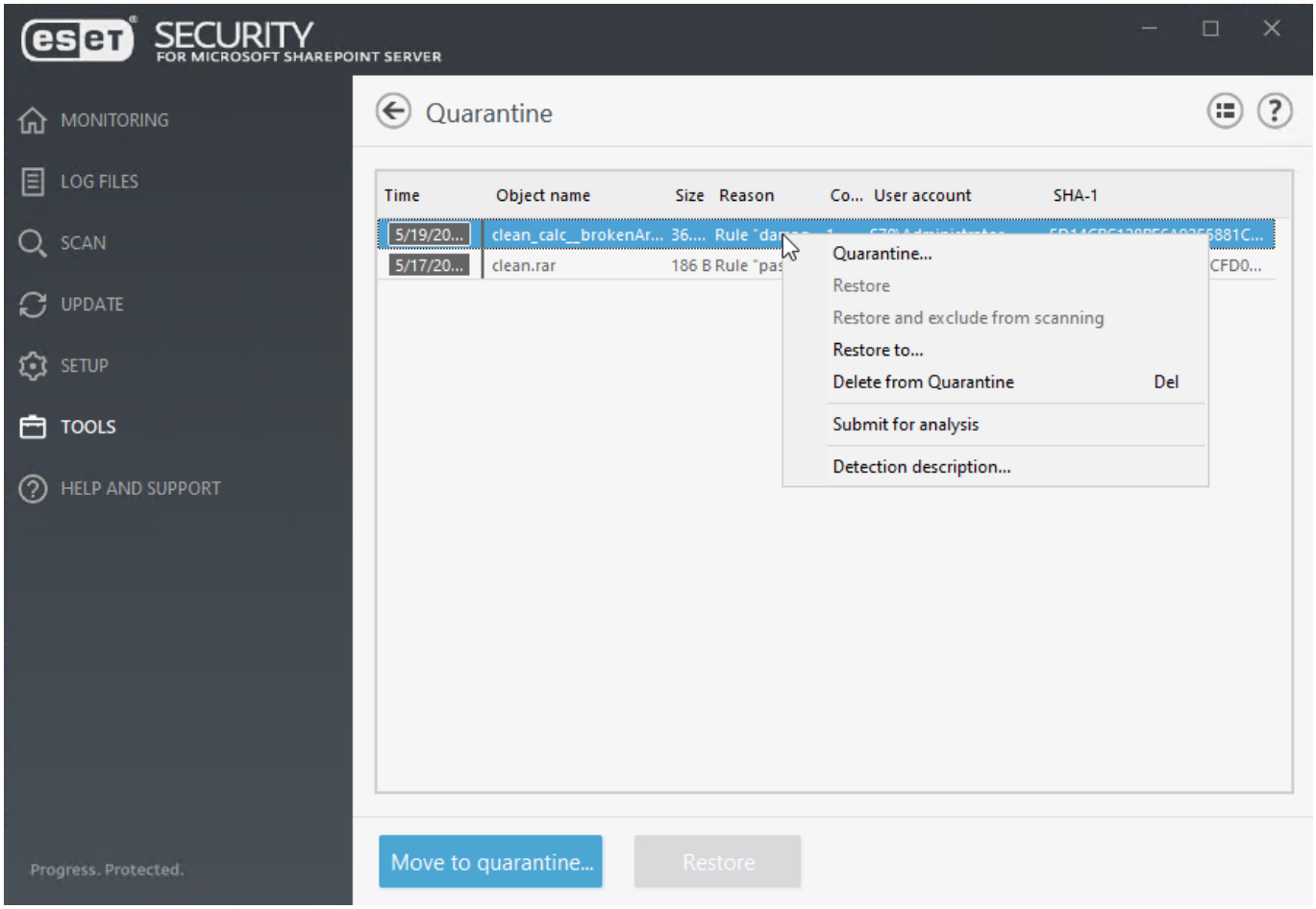
Use this form if the file cannot be categorized as a Suspicious file or False positive.

**Reason for submitting the file**

Type 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 Security for Microsoft SharePoint. 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.




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 Security for Microsoft SharePoint 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. 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 enables you to restore a file to a location other than the one from which it was deleted.

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

# Server protection settings

ESET Security for Microsoft SharePoint protects your Microsoft SharePoint Server using the following features:

- On-access filter
- On-demand database scan
- Rules

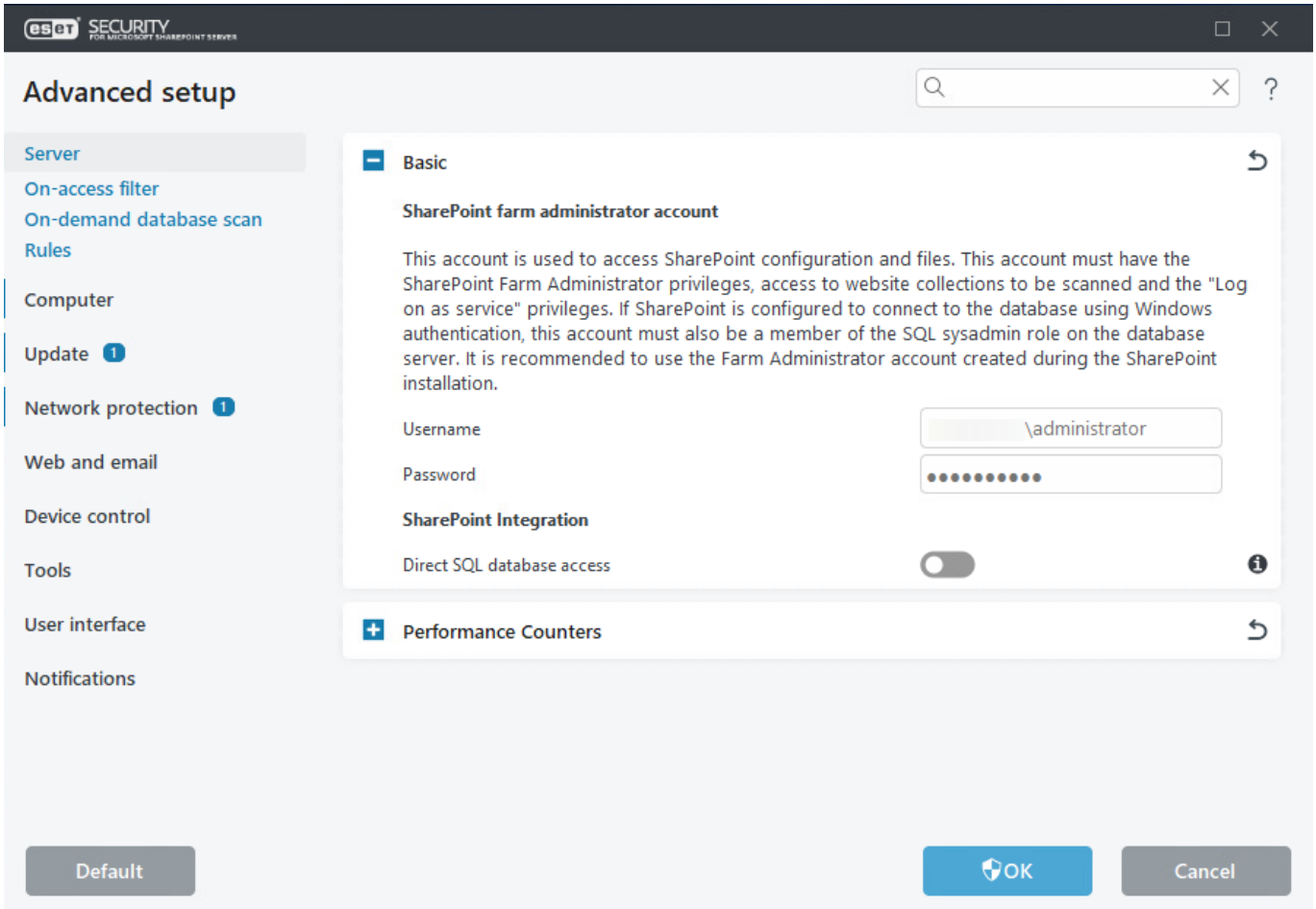
This account must have SharePoint Farm Administrator privileges to access website collections for scanning and "Log on as service" privileges. If SharePoint is configured to connect to the database using Windows authentication, this account must also be a member of the SQL Sysadmin role on the database server.
We recommend that you use the Farm Administrator account created during SharePoint installation. If you do not type valid login credentials, ESET Security for Microsoft SharePoint will not be functional after the installation. If the installation is performed without GUI, you must type the SharePoint administrator account via the GUI or eShell afterward; otherwise, the product will not work.
In an ESET PROTECT managed environment, you can use a **Client Task** called Run Command to execute eShell commands. This is especially useful in a large farm with many SharePoint instances, or if you want to supply credentials remotely. When creating a new ESET PROTECT Client Task, specify **Command line to run**:

```
powershell eshell server set farm-username <domain\user> && eshell server set farm-password plain <password>
```

Ensure you have the ESET Shell execution policy set to **Full access** for the command to take effect.

Even if you do not have a large SharePoint farm, you can use the eShell command (see above) to populate the credentials of the SharePoint farm administrator account. Alternatively, you can do it while upgrading to the latest version rather than manually entering the Username and Password.

To ensure continuous protection, you must update SharePoint administrator account credentials whenever they change. If the credentials entered here do not match the SharePoint administrator account, ESET Security for Microsoft SharePoint will not function properly and will not provide maximum protection.




**Direct SQL database access**

This feature enables read-only access to SharePoint databases for On-demand scan only. It enables ESET Security for Microsoft SharePoint to read data directly from the SQL Server (SharePoint Content databases). Direct database access has several advantages over the SharePoint object model. Direct database access is faster, performs better, and uses fewer system resources. Direct database access is used for all read operations, while all write operations (Clean, Delete, etc.) are executed via the SharePoint object model. If you disable Direct SQL database access, the SharePoint object model is used for all operations (read and write).

Both Direct SQL database access and the SharePoint object model support download parallelism. You can configure parallelism by specifying **Number of concurrent downloads** in On-demand database scan.

Performance Counters

To monitor and track ESET Security for Microsoft SharePoint performance, use ESET Security for Microsoft SharePoint Performance Counters.

# Performance Counters

ESET Security for Microsoft SharePoint Performance Counters allows you to monitor ESET Security for Microsoft SharePoint's scan process performance. The Counters provide information, including the number of processed and scanned files, the amount of data downloaded from Microsoft SharePoint and average scanning time. Refer to the tables below for the available counters. ESET Security for Microsoft SharePoint Performance Counters are divided into two groups based on the protection type (On-demand and On-access). Both groups have the same performance counters.

ESET Security for Microsoft SharePoint Performance Counters are automatically registered in the operating system during the ESET Security for Microsoft SharePoint installation. When you enable Performance Counters, your ESET Security for Microsoft SharePoint provides performance data. If you disable Performance Counters, the Counters remain registered in the system, and the ESET Security for Microsoft SharePoint stops providing performance data. When you uninstall ESET Security for Microsoft SharePoint, its Performance Counters are unregistered from the system automatically.

ESET Security for Microsoft SharePoint uses new architecture (version 2.0) when providing Performance Counter data. The ESET Security for Microsoft SharePoint Performance Counter data can be processed and displayed directly by the Windows Server Performance Monitor. Alternatively, the Performance Data Helper (PDH) interface can use the data.

When you enable ESET Security for Microsoft SharePoint Performance Counters, open Performance Monitor and add the Counters you want to receive data from. You can choose Counters from two groups:

- **ESET Security for Microsoft SharePoint - On-access Scan**
- **ESET Security for Microsoft SharePoint - On-access Scan - On-demand Scan**

To learn more about Performance Monitor, see Microsoft's Windows Performance Monitor Overview article.

## The list of available Counters:

**On-access Performance Counters** (group name: ESET Security for Microsoft SharePoint - On-access Scan)

| Counter Name | Description |
|---|---|
| OA - Processed Files | The total number of processed files since ESET Security for Microsoft SharePoint started. |
| OA - Processed Files/sec | Number of processed files per second. |
| OA - Processed Files/sec (Average) | Moving average of the number of processed files. |
| OA - Scanned Files | The total number of scanned files since ESET Security for Microsoft SharePoint started. |
| OA - Scanned Files/sec | Number of scanned files per second. |
| OA - Scanned Files/sec (Average) | Moving average of the number of scanned files. |
| OA - File Processing Time (ms) (Average) | The average time to process a file in milliseconds (file processing covers downloading, rule evaluation and file scan). |
| OA - File Downloading Time (ms) (Average) | The average time to download a file from Microsoft SharePoint in milliseconds. |
| OA - File Scanning Time (ms) (Average) | The average time to scan a file for threats in milliseconds. |
| OA - File Rule Checking Time (ms) (Average) | The average time to evaluate rules on a file in milliseconds. |
| OA - Downloaded MB | The total amount of data downloaded from Microsoft SharePoint in MB since ESET Security for Microsoft SharePoint started. |
| OA - Download Speed KB/sec (Average) | The average download speed from Microsoft SharePoint in KB per second. |

**On-demand Performance Counters** (group name: ESET Security for Microsoft SharePoint - On-demand Scan)

| Counter Name | Description |
|---|---|
| OD - Processed Files | The total number of processed files since ESET Security for Microsoft SharePoint started. |

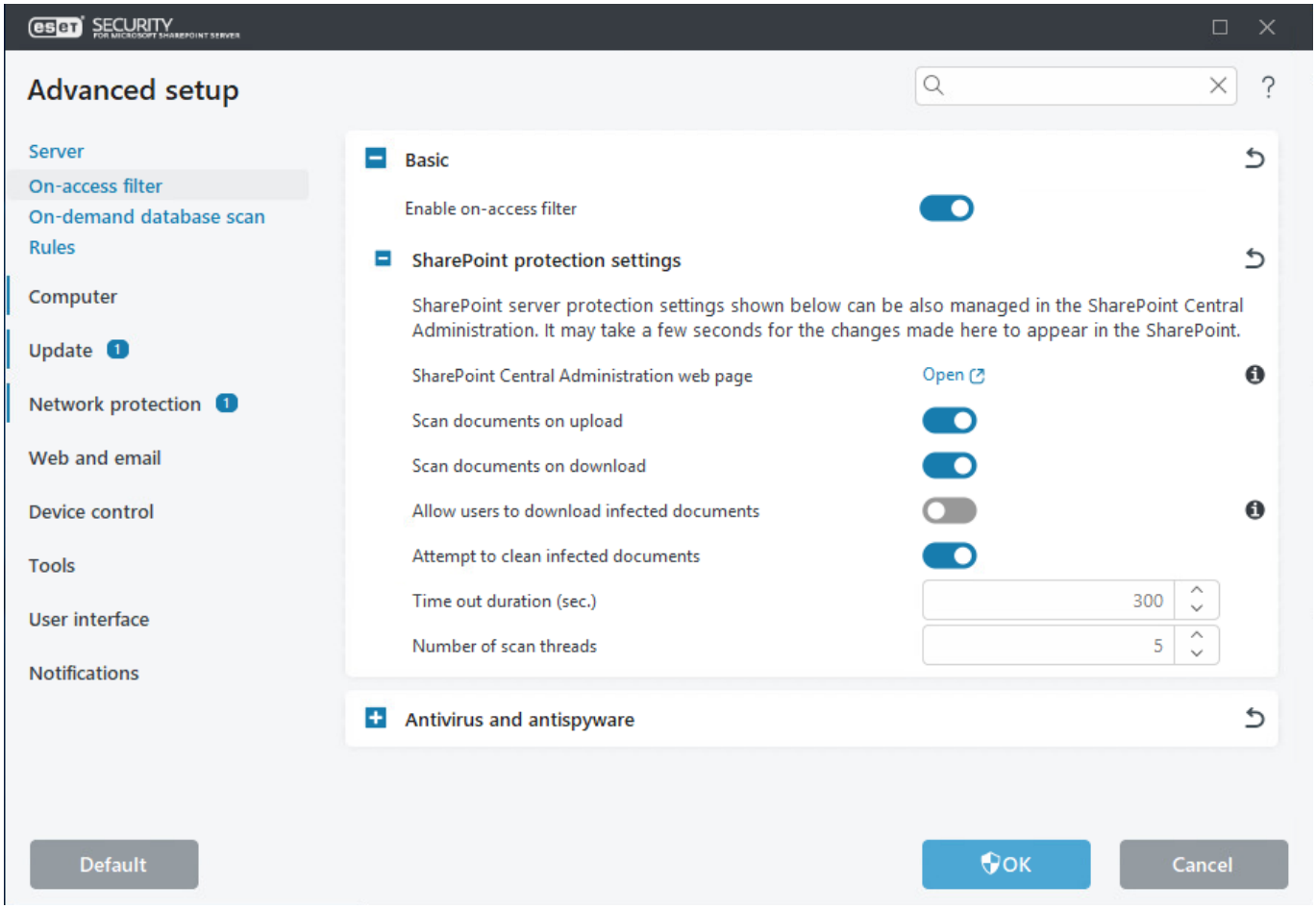
| Counter Name | Description |
| --- | --- |
| OD - Processed Files/sec | Number of processed files per second. |
| OD - Processed Files/sec (Average) | Moving average of the number of processed files. |
| OD - Scanned Files | The total number of scanned files since ESET Security for Microsoft SharePoint started. |
| OD - Scanned Files/sec | Number of scanned files per second. |
| OD - Scanned Files/sec (Average) | Moving average of the number of scanned files. |
| OD - File Processing Time (ms) (Average) | The average time to process a file in milliseconds (file processing covers downloading, rule evaluation and file scan). |
| OD - File Downloading Time (ms) (Average) | The average time to download a file from Microsoft SharePoint in milliseconds. |
| OD - File Scanning Time (ms) (Average) | The average time to scan a file for threats in milliseconds. |
| OD - File Rule Checking Time (ms) (Average) | The average time to evaluate rules on a file in milliseconds. |
| OD - Downloaded MB | The total amount of data downloaded from Microsoft SharePoint in MB since ESET Security for Microsoft SharePoint started. |
| OD - Download Speed KB/sec (Average) | The average download speed from Microsoft SharePoint in KB per second. |

# On-access filter

In this window, you can customize the on-access filter parameters. Choose whether you want to have **Enable on-access filter** enabled (default) or disabled. If you disable the on-access filter, the options below become inactive.

When the on-access filter is disabled, ESET Security for Microsoft SharePoint does not scan documents on upload/download, on-access filter rules are not be applied and a warning message is displayed in Monitoring.

i We recommend that you leave **Enable on-access filter** enabled to ensure maximum protection.




SharePoint Protection Settings (these settings can also be managed from the SharePoint Central Administration):

**Link to SharePoint Central Administration**

Click the URL to open your SharePoint Central Administration site - Antivirus settings. If you change settings from within SharePoint Central Administration, allow time for the changes to appear in ESET Security for Microsoft SharePoint.

**Scan documents on upload**

Documents uploaded to SharePoint are scanned via the web interface whenever they are saved in Microsoft Office programs and during synchronization via the SharePoint workspace.

**Scan documents on download**

Documents downloaded from SharePoint via a web interface are scanned while downloading. This includes pictures and documents opened from Microsoft Office programs during synchronization via SharePoint workspace.

**Allow users to download infected documents**

When enabled, SharePoint displays a warning about infected files when they are found, but you are still able to open infected files, and these files are blocked rather than deleted. If disabled, a message is shown saying the document is infected and the download is impossible. The SharePoint administrator can always download infected files regardless of this setting.

**Attempt to clean infected documents**

When enabled, infected documents that are cleanable are cleaned.

**Time out duration (sec.)**

The maximum time SharePoint will wait for a response from ESET Security for Microsoft SharePoint. If no response is received, it reports an AV scanner error. The default is 300 seconds.

**Number of scan threads**

The number of instances for each w3wp process. SharePoint usually uses three w3wp processes. A total of 15 (3x5) scanner objects are available. This limits the maximum number of files downloaded/uploaded at the same time. This is not the same as the number of ThreatSense scan engines.

# Antivirus and antispyware

**Action to take if cleaning not possible**

This actions field enables you to select the action to take when an infected file is found, and cleaning is not possible:

- **No action** - No changes are made. If uploaded, infected files will be stored on SharePoint, and users will have access.
- **Block** - The infected file is blocked and will not be uploaded/downloaded. Also, a message will be shown notifying the user of why the file was not uploaded/downloaded.
- **Mark for deletion** - File is suggested to be deleted and SharePoint will decide on deletion on its own. It is usually impossible to delete the file when a user is accessing it (during download) as the user does not have write/delete rights. This option is not available when the ThreatSense engine parameter cleaning level is set to No cleaning. However, if the user downloading the file has appropriate rights the file will be deleted. The Message type shown to the user is handled by SharePoint.



If the document is deleted, its earlier versions are deleted as well. Therefore, we recommend using the Block action. To remove infected documents from SharePoint, use on-demand database scan instead.

**Quarantine infected files**

When enabled, files that are marked for deletion will be put into quarantine. Deselect this setting to disable quarantine so that files do not accumulate in quarantine. For instance, if the partition on which the quarantine is located is too small and could potentially become too full. The quarantine should not be disabled. This option affects quarantine policy for both cleanable and non-cleanable files. The use of quarantine does not have an effect on rules.

**Template of a message displayed on threat detection**

You can customize the message displayed in a user's browser when a threat or infiltration is detected and was cleaned, blocked or deleted. Type your text into the Template of a message displayed on threat detection field. The message is shown only within the web interface.

You can use the following variables in the message:

- %VIRUSNAME% - infiltration name from the scan engine.

- %FILENAME% - filename.
- %FILESIZE% - file size.
- %PRODUCTNAME% - product name, in this case: ESET Security for Microsoft SharePoint.

ThreatSense parameters

To modify scan parameters for On-access filter.

On-access filter & Machine learning protection

Reporting is performed by detection engine and the Machine learning component.

# On-demand database scan

Each selected website's hierarchy of folders and files is scanned. Each file, user document or other SharePoint internal file is stored in a temporary file and sent to the kernel for scanning. If there are also earlier versions of a specific file and the Scan document versions feature is enabled, the earlier versions are scanned first.

**Scan in read-only mode**

Infected documents will not be cleaned or deleted. The delete rule action will not be applied.

**Scan document versions**

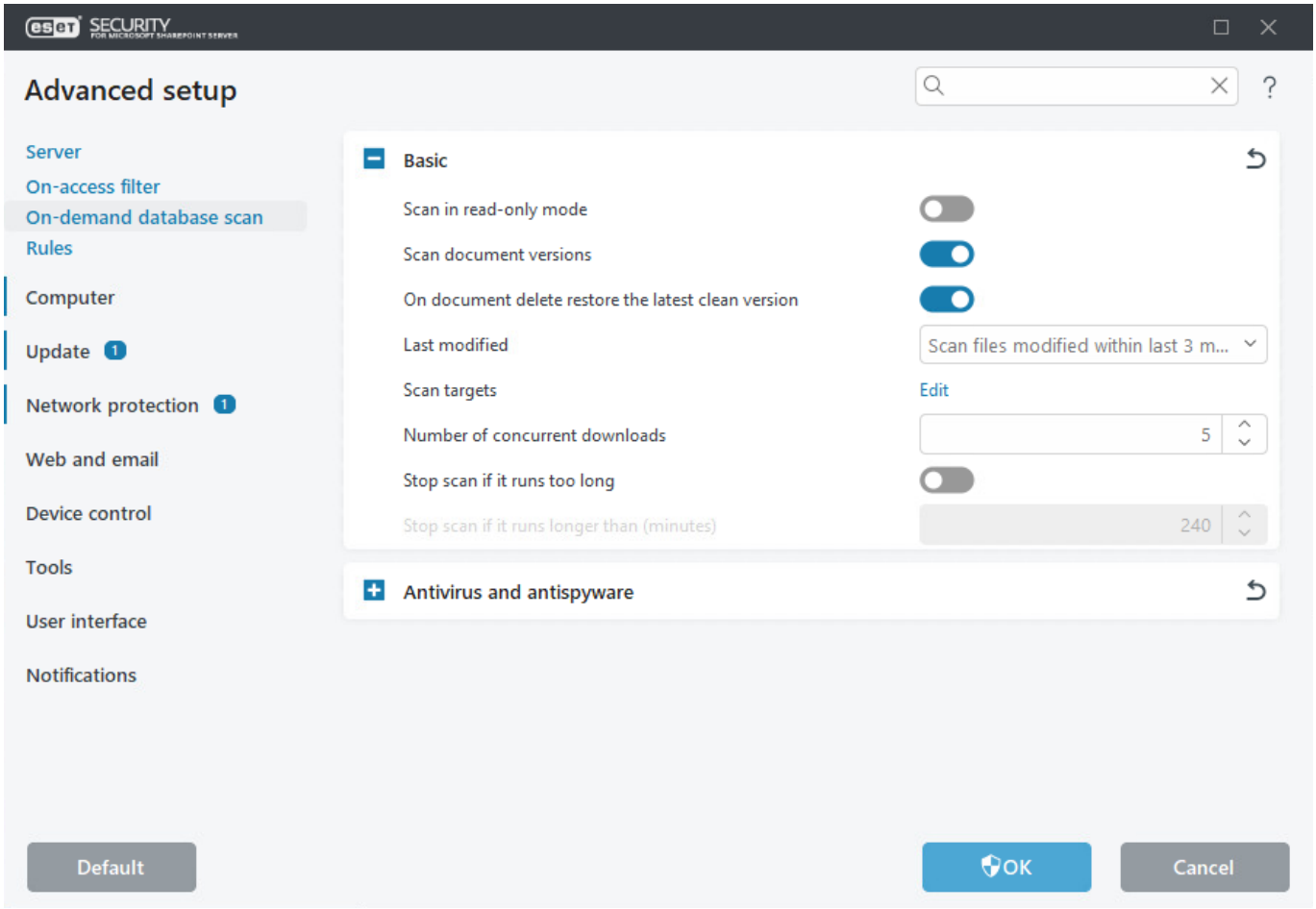
If other versions of the same document exist within the SharePoint database, these will also be scanned.

**On document delete restore the latest clean version**

When an infected document is deleted, earlier non-infected versions are scanned. If earlier versions are not infected, the most recent clean version will be restored and made the current version. This option is not available when Scan in read-only mode is enabled.

**Last modified**

Select a time restriction from the drop-down menu to only scan files modified within a specific time interval.




**Scan targets**

A window will open where you can scan all targets or select your specific targets. For more information, refer to On-demand database scan targets.

**Number of concurrent downloads**

This parameter enables scanning in parallel by multiple threads. When set to 0, legacy sequential processing is used.

Enable **Stop scan if it runs too long** and modify the interval **Stop scan if it runs longer than (minutes)** to change to preferred time (anything between 1 to 2880 minutes).

# On-demand database scan targets

In this dialog window, you can select SharePoint websites to scan and run the scanning process. A list of websites will be displayed.

Click the gear icon to access the **Scan targets** and **Last modified** menus.

In the **Scan targets** drop-down menu, you can choose **All targets** or **Custom targets**.

- **Scan in read-only mode**—Infected documents will not be cleaned or deleted. The delete rule action will not be applied.
- **Scan document versions**—If other versions of the same document exist within the SharePoint database,

these will also be scanned.

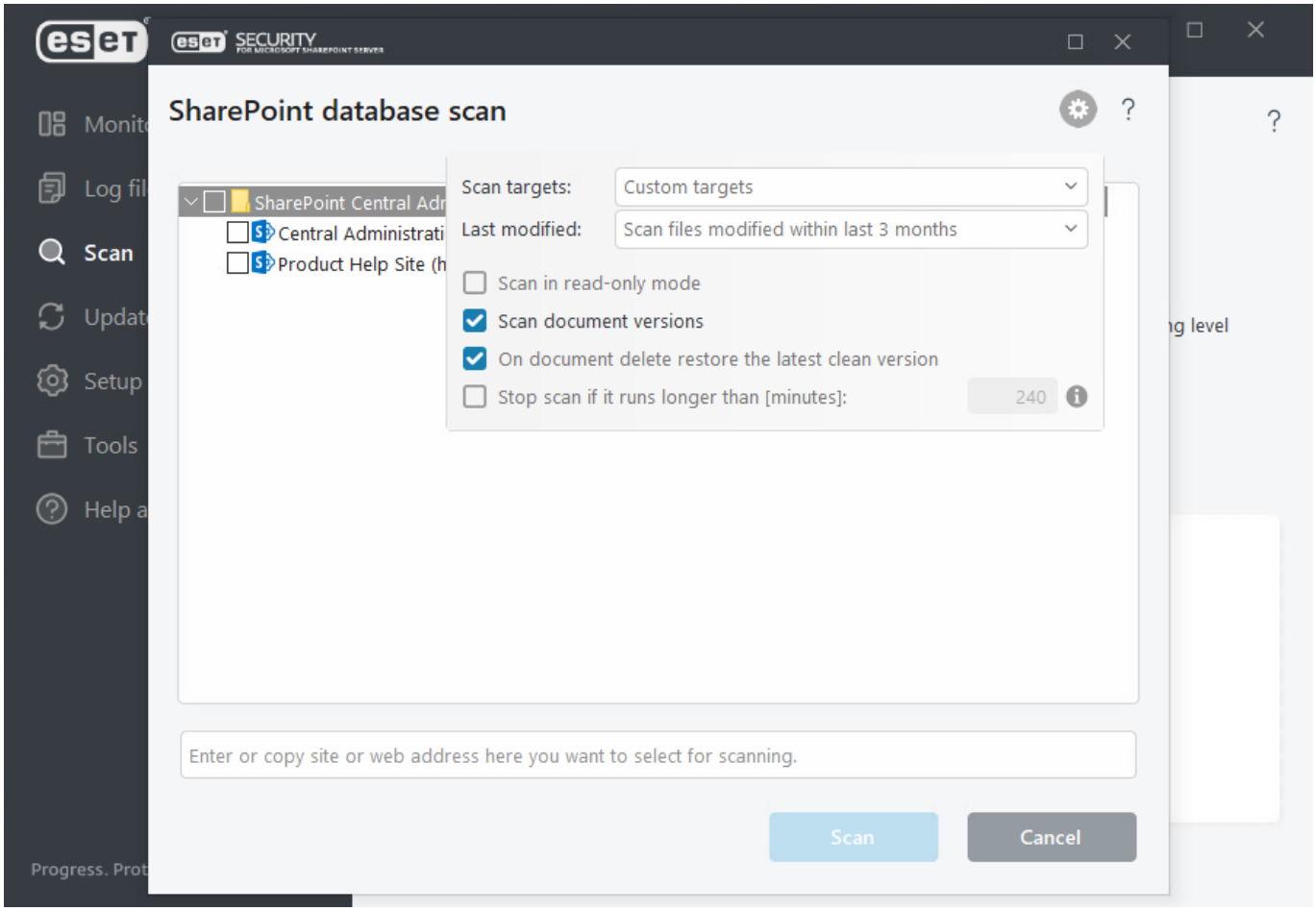
- **On document delete restore the latest clean version**—When an infected document is deleted, earlier non-infected versions are scanned. If earlier versions that are not infected exist, the most recent clean version will be restored and made the current version. This option is not available when Scan in read-only mode is enabled.

- **Stop scan if it runs longer than (minutes)**—Change to preferred time (anything between 1 to 2880 minutes).

In the **Last modified** drop-down menu, select a time restriction to scan files modified within a specified time period:

- Scan all files
- Scan files modified within last year
- Scan files modified within last 3 months (default setting)
- Scan files modified within last month
- Scan files modified within last week
- Scan files modified within last 24hrs

> The default setting for **Last modified** is set to **Scan files modified within last 3 months** and can be modified in **Advanced Setup** > Last modified.
> If you upgraded ESET Security for Microsoft SharePoint and have custom On-demand scan scheduled tasks, review their settings to ensure the last modified parameter is correct.




When selecting targets manually, click the check box next to a website to add it to the scan.

To add a website, copy/paste its URL into the dialog window. The URL must refer to a SharePoint website, not a specific file. Adding procedure might take a few moments to populate, depending on the number and complexity of sites in the list. If any changes to the sites are made, you can refresh the list by pressing **F5**. When you see the list, you can use the check boxes to select the websites you want to scan.

In the hierarchy displayed below, there is a SharePoint web application on the top that contains one or more SharePoint website collections, which in turn contain SharePoint websites. Websites are arranged hierarchically, one of them always being the root.

When you have specified targets and parameters, click **Scan** to start the scanning process.

The website hierarchy is retrieved from SharePoint the first time it is displayed and cached in the ESET SharePoint Helper Service for faster access. The website hierarchy is refreshed automatically after a certain amount of time has elapsed, and it can also be refreshed by pressing the **F5** key.

# Antivirus and antispyware

**Action to take if cleaning not possible** - Select what action you should take when an infected file is found and it cannot be cleaned (delete is not considered cleaning):

- **No action**—No changes are made, and files will be uploaded/downloaded.
- **Delete**—The file is deleted from the database. If an error occurs during deletion, the error is written into the database scan log. This option is unavailable when the ThreatSense engine parameter cleaning level is

set to No cleaning.

**Quarantine infected files**

When enabled, files marked for deletion will be put into quarantine. By disabling this option, you can deactivate the quarantine to prevent accumulating large numbers of files. For instance, if the partition where the quarantine is located is too small and could potentially get clogged. However, the quarantine should not normally be disabled. This option affects quarantine policy for both cleanable and non-cleanable files. Using quarantine does not affect rules.

ThreatSense parameters

To modify scan parameters for On-demand database scan.

On-demand database scan & Machine learning protection

Reporting is performed by the detection engine and the machine learning component.

# Rules

Rules enable you to manually define and manage file filtering conditions and actions to take with filtered files. Rules are applied according to set of combined conditions and have different conditions and actions available during On-access filter or On-demand database scan. There are a two rule sets:

- On-access filter
- On-demand database scan

Click **Edit** to open the rules list, and click **Add** and follow the Rule wizard to create a new rule.

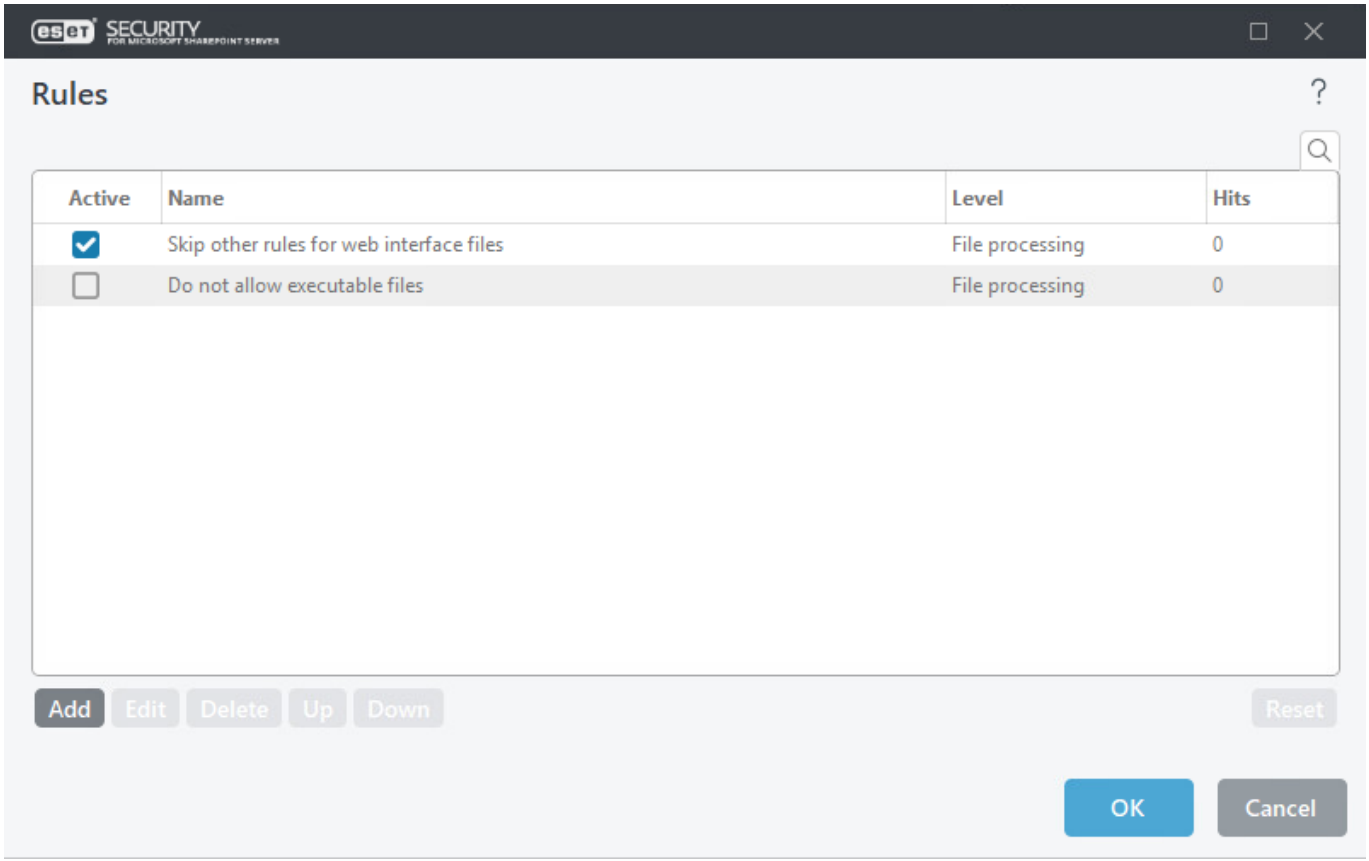
# Rules list

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

- **Filtering rules** (1)—evaluated before antispam, antivirus and anti-phishing scanning
- **Attachment processing rules** (2)—evaluated during an antivirus scan
- **Result processing rules** (3)—evaluated after antispam, antivirus and anti-phishing scanning

Rules with the same evaluation level are reviewed in the order displayed in the rules window. You can only change the order for same-level rules. When you have multiple filtering rules, you can change their order. You cannot change their order by putting **Attachment processing** rules before **Filtering** rules, and the **Up**/**Down** buttons are unavailable. You cannot mix rules from 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.




Click **Reset** the counter for the selected rule (displayed in the **Hits** column). Select **View** to view a configuration assigned from ESET PROTECT policy.

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

- **Add**—adds a new rule
- **Edit**—modifies an existing rule
- **View**—enables you to view a configuration assigned from ESET PROTECT policy
- **Delete**—removes the selected rule
- **Up**—moves the selected rule up in the list
- **Down**—moves the selected rule down in the list
- **Reset**—resets the counter for the selected rule (the Hits column)

If a new rule is added or an existing rule is modified, the message rescan will automatically start using the new or modified rules.

# Rule wizard

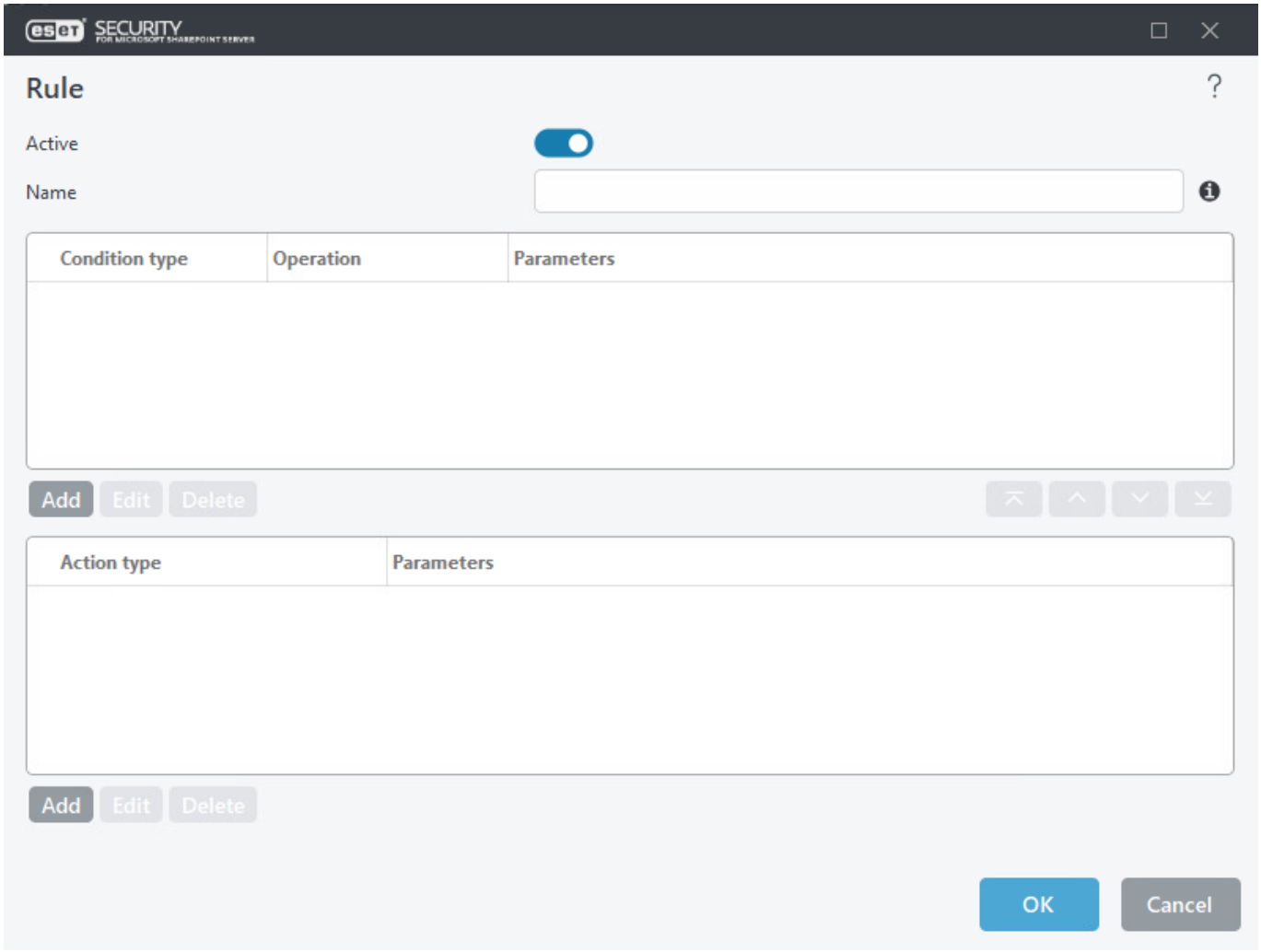
You can define conditions and actions using the Rule wizard. Define condition(s) first, then action(s). Some conditions and actions differ for rules specific to On-access filter or On-demand database scan. This is because the

protection types use a different approach when processing messages. Click **Add** (in the middle), and a Rule condition window will appear where you can select a condition type, operation and value. Define condition(s) first, then action(s).

You can define multiple conditions. If you do so, all conditions must be met for the rule apply. All conditions are connected using the logical operator **AND**. Even if most conditions are met and one is not, the condition evaluation result is *not met* and the rule's action cannot be applied.

1. Click **Add** (at the bottom) to add a Rule action.

You can add multiple actions for one rule.




2. When conditions and actions are defined, type a rule **Name** (something that you will recognize). The name will display 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**. Red highlighting does not disappear even though you have entered a rule name; it disappears after you click **OK**.

3. If you want to prepare rules and plan to use them later, you can click the toggle next to **Active** to deactivate the rule. To activate the rule, select the check box next to the rule you want to activate.

If a new rule is added or an existing rule is modified, the message rescan will automatically start using the new or modified rule.

# Rule condition

The Rules condition wizard lets you add conditions for a rule. Select the condition **Type** and an **Operation** from the drop-down menu. The list of operations changes depending on what rule type you have chosen. Then select a **Parameter**. Parameter fields will change depending on the 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 the rule actions you have specified. For this reason, you should specify the action taken when a given rule is triggered if you have not already done so when setting that rule's parameters.

If you want to import your custom list from a file instead of adding entries manually, right-click in the middle of the window and select **Import** from the context menu. Then you can browse for your file (*.xml* or *.txt*, and containing entries delimited by new lines) that you want to add to the list. Likewise, select **Export** from the context menu if you need to export your existing list to a file.

Alternatively, you can specify **Regular expression** by selecting **Operation: matches regular expression** or **does not match regular expression**.

> 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 is not, the condition evaluation result is considered *not met* and the rule's action cannot be taken.

The following conditions types are available for On-access filter or On-demand database scan (some of the options might not display depending on your previously selected conditions):

| Condition name | On-access filter | On-demand database scan | Descriptions |
|---|---|---|---|
| File name | ✓ | ✓ | Applies to files with a specific name, if this condition is chosen, it allows you to specify a mask for the specified filename, you can use wildcards *? etc.<br>This condition applies to the filename only, regardless of file path. |
| File size | ✓ | ✓ | Applies to files exceeding the defined size. If this condition is selected you can specify a maximum file size and when file size exceeds the set value the rule will be applied. |
| File URL | ⍰ | ✓ | Applies to files located at specific URL, if this condition is chosen, it allows you to specify URL and a mask for the specified filename, you can use wildcards *? etc. |
| File type | ✓ | ✓ | Applies to files of a specified type (actual file type is detected by its contents, regardless of filename or extension), if this condition is chosen, it allows you to select one or more file types for which the rule is applied, for a complete list of file types detected see our Knowledgebase article. |
| Time modified | ⍰ | ✓ | Applies to files that were last modified before or after a specified date, alternatively you can specify a date range and a rule condition will then apply to files modified within this range. |
| Antivirus scan result | ✓ | ✓ | Applies to files that are considered malicious or clean based on an Antivirus scan. |

| Condition name | On-access filter | On-demand database scan | Descriptions |
|---|---|---|---|
| Contains password protected archive | ✓ | ✓ | Applies to archive files that are protected by a password. |
| Contains damaged archive | ✓ | ✓ | Applies to damaged archive files (most likely impossible to open). |
| Modified by user | ☐ | ✓ | Applies to files that were last modified by specified user. |

> The number of **Rules hits count** in scan log can be higher than the **Number of scanned objects** for rules that contain **File type** condition. This may happen when scanned objects are archives or container files that package other files inside them (for example *.docx*). In such case, each inner file is being matched against the rules with **File type** condition, which may result in **Rules hits count** exceeding the **Number of scanned objects**.

# Rule action

You can add actions for messages and/or attachments that match rule conditions.

> You can to add multiple actions for one rule.

The following is a 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 | On-access filter | On-demand database scan | Descriptions |
|---|---|---|---|
| Quarantine file | ✓ | ✓ | Moves file into quarantine, even if antivirus quarantine is disabled. |
| Delete | ☐ | ✓ | File is deleted from the database. |
| Mark for deletion | ✓ | ☐ | Will not upload the file on upload attempt, will delete file during indexing, will mark the file for deletion on download attempt. |
| Block | ✓ | ☐ | File upload or download is blocked. |
| Send event notification | ✓ | ✓ | Sends event notification to the administrator, enable Send event notification by email and define the format of event messages (use the tooltip for suggestions). |
| Evaluate other rules | ✓ | ✓ | Allows the evaluation of other rules, providing the administrator with the ability to define multiple sets of conditions and multiple actions to take given conditions. If this is disabled, no rules will be evaluated but antivirus scan will still be performed. |
| Log to events | ✓ | ✓ | Writes information about the applied rule to Events log. You can choose the Severity and define the format of event messages (use the tooltip for suggestions). |
| Skip Antivirus scan | ✓ | ✓ | File will not be scanned by the antivirus engine. |
| Do not evaluate other rules | ✓ | ✓ | If this option is used as an action, it will skip any further rules that would normally follow. |

# 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 applications 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 scans 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 and more.

Network protection

Manage network protection - Known networks, Zones, Network attack protection (IDS), Brute-force attack protection and Botnet protection.

Web and email

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

Customize tools, such as ESET CMD, ESET RMM, WMI provider, ESET PROTECT scan targets, Windows Update notifications, Log files, Proxy server, Email notifications, Diagnostics, Cluster and more.

Notifications

Configure notifications to be shown on desktop or sent by email for Application statuses, Desktop notification, Interactive alerts and Forwarding.

User interface

Configure the main program window, License information, Password protection, eShell execution policy and more.

# 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 malicious code 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 takes 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.**<br>ℹ 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.<br>ℹ 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.<br>ℹ 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.

ℹ 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 malicious code 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 takes 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.**<br>ℹ 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.<br>ℹ 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.

On-access filter & 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-access filter 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 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
```

On-demand 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 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 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
```

# 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).

Not to be confused with excluded extensions, processes exclusions or exclusion filter.

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.

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 filename.

**Comment**

Add an optional Comment to easily recognize the exclusion in the future.

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 specific file located in the exact path

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)

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 form:
*%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 exclusions

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.

> 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 filename.

**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 PROTECT 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.

> 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 specific file located in the exact path

> 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

> 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)

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 filename) 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**

A sophisticated system that detects dangerous programs, such as rootkits, that can hide from the operating system. These types of programs are usually undetectable using standard techniques.

**AMSI**

Let Microsoft Antimalware Scan Interface (AMSI) 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.

The automatic exclusions feature is enabled after you activate ESET Security for Microsoft SharePoint with a valid license and perform the initial update to include the latest modules.

> Automatic exclusions for Microsoft SQL Server database files work for default location. If you have Microsoft SQL Server databases in different locations (other than the default), you have two options. Manually add the exclusions, or have the database files automatically excluded. For the automatic exclusion, ESET Security for Microsoft SharePoint needs read access to the Microsoft SQL Server instance to find what paths are used for database files. If ESET Security for Microsoft SharePoint displays an error message about insufficient rights, solve it by granting the NO_AUTHORITY\SYSTEM account **View any definition** permission to each Microsoft SQL Server instance you run on the server with ESET Security for Microsoft SharePoint.
> For further details, see Knowledgebase article on how to Add permission to get database data locations to generate automatic exclusions for Microsoft SQL Server.

ESET Security for Microsoft SharePoint 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.

To identify and generate automatic exclusions, ESET Security for Microsoft SharePoint 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 -?`.

# 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 Security for Microsoft SharePoint, 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 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 Security for Microsoft SharePoint is compatible with machines using Azure File Sync agent with cloud tiering enabled. ESET Security for Microsoft SharePoint 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.

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:

- On-access filter
- On-demand database scan
- 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 lets you define which computer components and files will be scanned for infiltration.

**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.

**WMI database**

Scans whole WMI database, searching for references to infected files or malware embedded as data.

**System registry**

Scans system registry, all keys and subkeys, searching for references to infected files or malware embedded as data.

**Email files**

The program supports the following extensions: DBX (Outlook Express) and EML.

**Archives**

The program supports the following extensions: *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE*, and many others.

**Self-extracting archives**

Self-extracting archives (SFX) are archives needing no specialized programs – archives – to decompress themselves.

**Runtime packers**

After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

## Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

**Heuristics**

A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not known by the previous 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. Real-time protection and other protection modules have the following remediation (i.e. cleaning) levels.

**Always remedy detection**

Attempt to remediate the detection while cleaning objects without any user intervention. System files are an exception. Such objects are left in their original location if the detection cannot be remediated.

**Remedy detection if safe, keep otherwise**

Attempt to remediate the detection while cleaning objects without any user intervention. If a detection cannot be remediated for system files or archives (with clean and infected files), the reported object is kept in its original location.

**Remedy detection if safe, ask otherwise**

Attempt to remediate the detection while cleaning objects. In some cases, if ESET Security for Microsoft SharePoint cannot perform automatic action, you will be prompted to choose an action (delete or ignore). This setting is recommended in most cases.

**Always ask the end-user**

No automatic action will be attempted by ESET Security for Microsoft SharePoint. You will be prompted to choose an action.

## Exclusions

An extension is the part of a filename 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 specific modules are applied when performing a scan.

**Preserve last access timestamp**

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

## Limits

The Limits section 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 Security for Microsoft SharePoint 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.

> 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.

> 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 filename 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.

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`).

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.

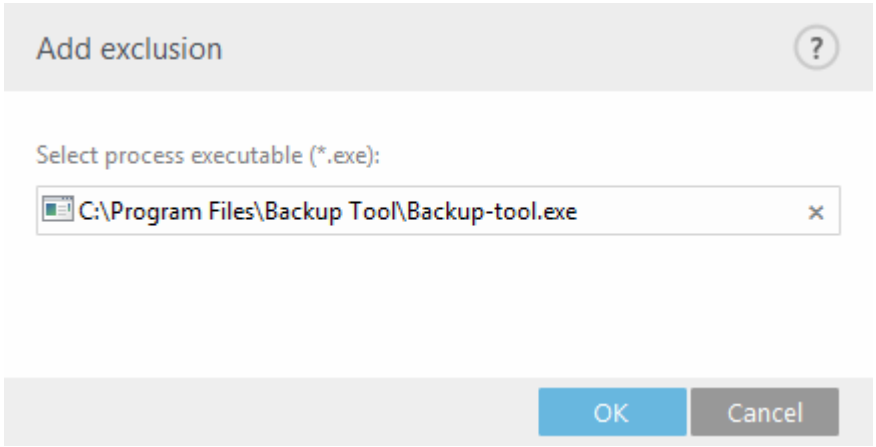
Processes exclusions help minimize the risk of potential conflicts and improve the performance of excluded applications, which in turn has a positive effect on the overall performance and stability of the operating system. The exclusion of a process / application is an exclusion of its executable file (*.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.

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 Security for Microsoft SharePoint and no scanning is run on any file operations performed by this process.

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




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

Web access protection does not take into account this exclusion, so if you exclude the executable file of your web browser, downloaded files are still scanned. This way an infiltration can still be detected. This scenario is an example only, and we do not recommend that you create exclusions for web browsers.

# 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 Security for Microsoft SharePoint, 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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 specific 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, filename, 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 PDFs 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 submitted automatically.

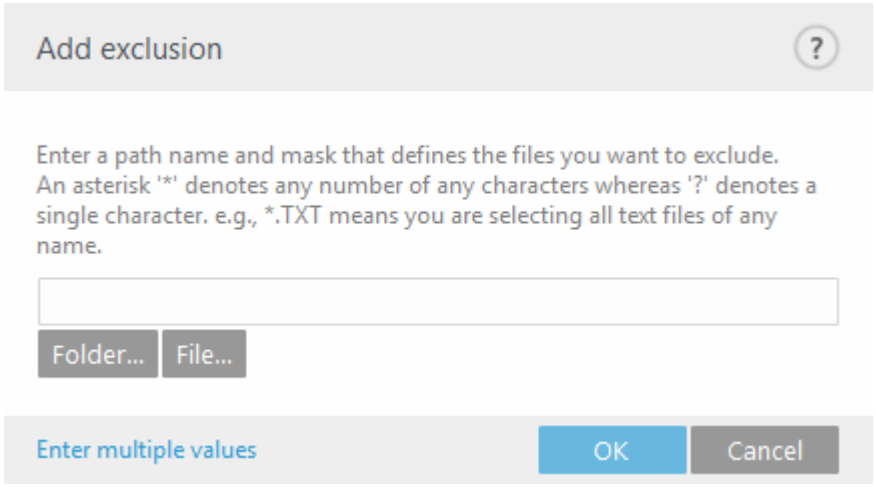
# Exclusion filter

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*). You can add to the list of excluded files if desired.

If you have used ESET LiveGrid® before and have disabled it, there may still be data packages to send. Even after deactivating, such packages will be sent to ESET. After all current information is sent, no further packages will be created.




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.

This scan profile selector applies to **On-demand scan** and Hyper-V scan.

Selected profile

A specific 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.

# 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 Security for Microsoft SharePoint.

**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.

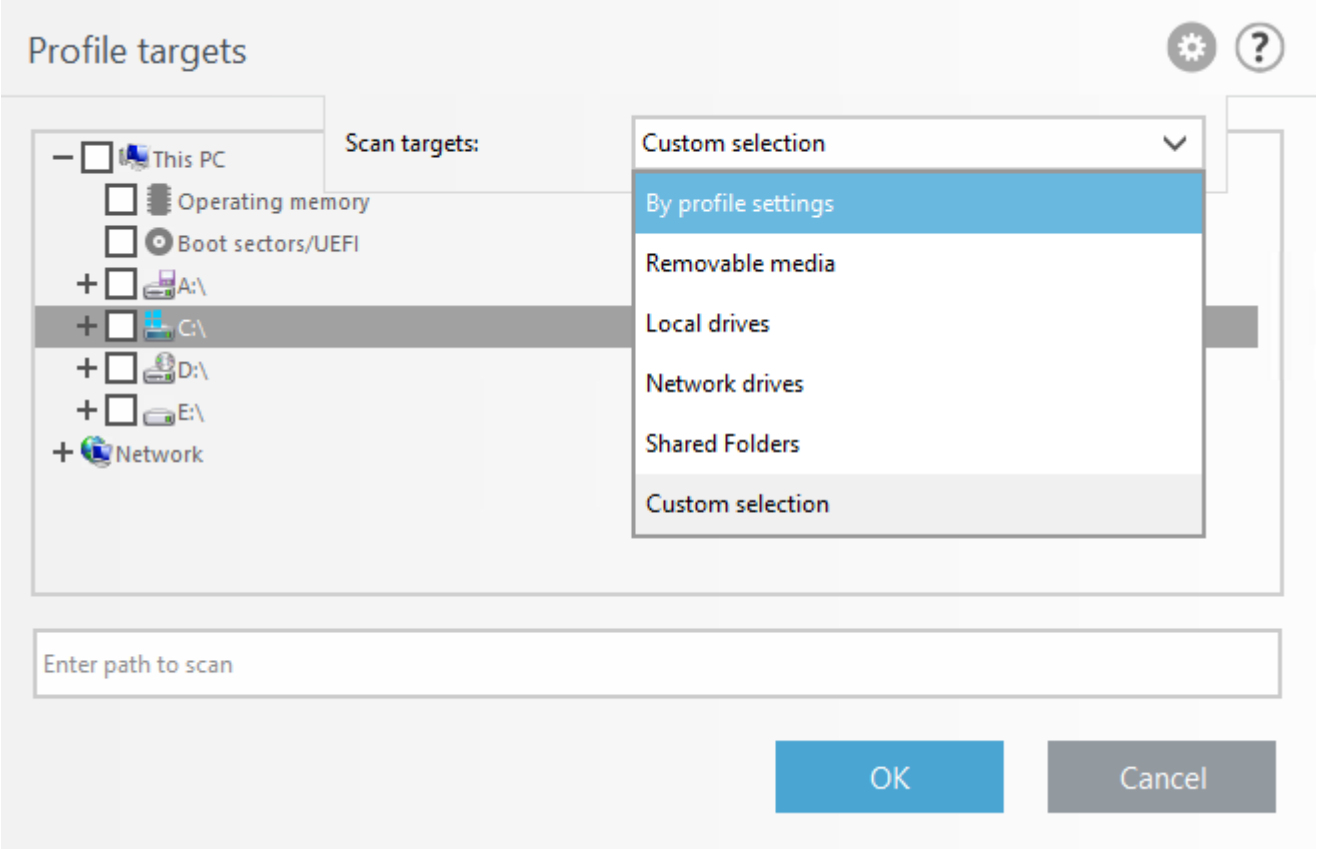
# Profile targets

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. Click the gear icon in the top-left corner to access the **Scan targets** and **Scan profile** drop-down menus.

ℹ This scan profile selector applies to On-demand scan and Hyper-V scan.

| **Operating memory** | **Scans all processes and data currently used by operating memory.** |
|---|---|
| Boot sectors/UEFI | Scans Boot sectors and UEFI for the presence of malware. Read more about the UEFI scanner in the glossary. |
| WMI database | Scans the whole Windows Management Instrumentation (WMI) database, all namespaces, all class instances, and all properties. Searches for references to infected files or malware embedded as data. |
| System registry | Scans the whole system registry, all keys, and subkeys. Searches for references to infected files or malware embedded as data. When cleaning the detections, the reference remains in the registry to make sure no important data will be lost. |

To quickly navigate to a scan target or add a target folder or file(s), enter the target directory in the blank field below the folder list.




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) 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
- Computer 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 its name 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**.

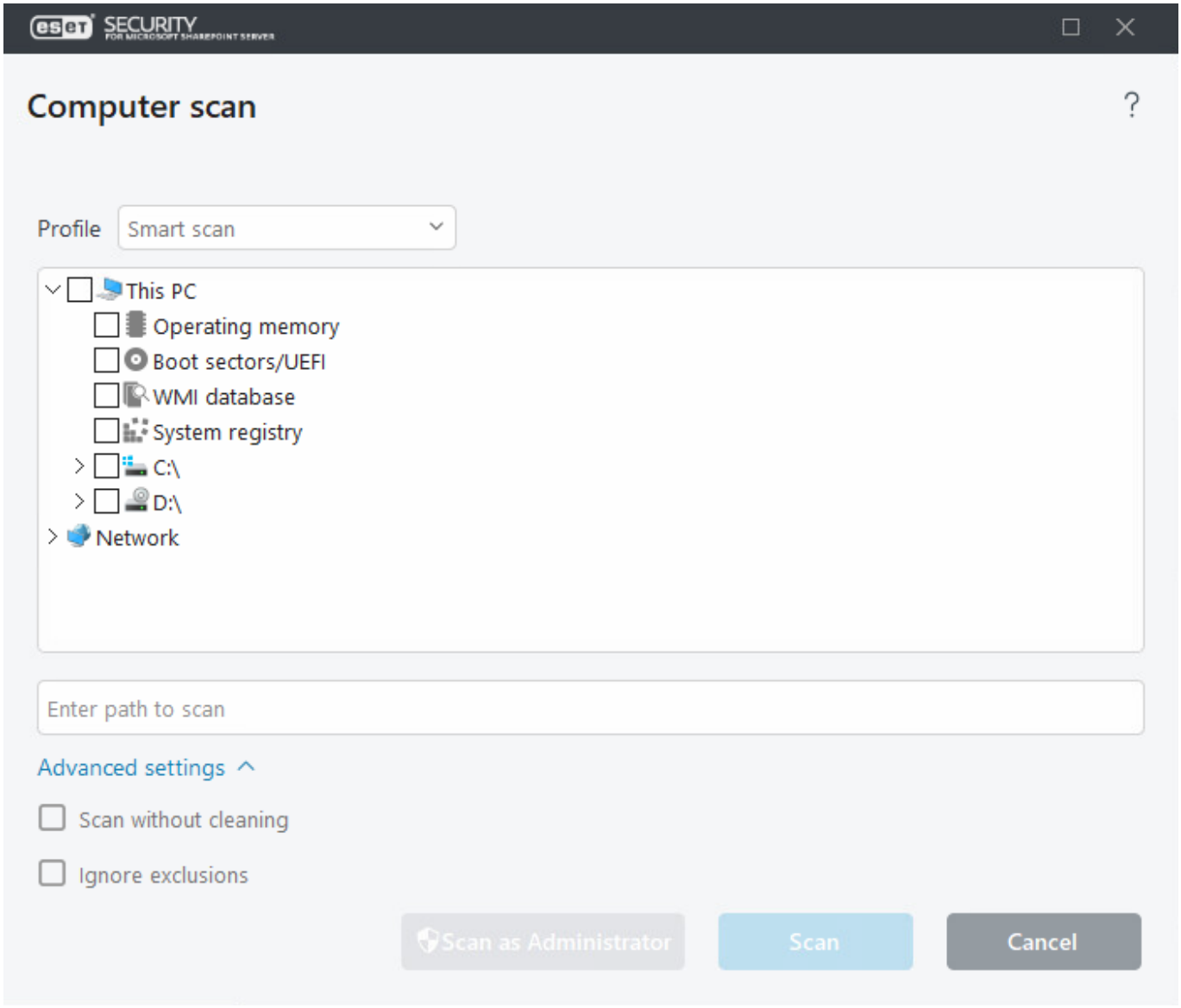
| **Operating memory** | **Scans all processes and data currently used by operating memory.** |
|---|---|
| Boot sectors/UEFI | Scans Boot sectors and UEFI for the presence of malware. Read more about the UEFI scanner in the glossary. |
| WMI database | Scans the whole Windows Management Instrumentation (WMI) database, all namespaces, all class instances, and all properties. Searches for references to infected files or malware embedded as data. |
| System registry | Scans the whole system registry, all keys, and subkeys. Searches for references to infected files or malware embedded as data. When cleaning the detections, the reference remains in the registry to make sure no important data will be lost. |

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 scan chosen targets. The default profile is **Smart scan**. There are two more pre-defined scan profiles: In-depth scan and **Context menu scan**. These scan profiles use different ThreatSense engine parameters.

The **Custom scan** window:




**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.

**Action after Scan** - Choose action to take after the scan finishes from the drop-down menu.

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

**The scan may be paused by user for (min)** - Enable the limited user to pause the computer scan for the specified time limit.

**Interrupt scan automatically after (min)** - To cancel the scan if it takes longer than the specified time limit.

**Scan as Administrator** - It enables you to execute the scan under the Administrator account. Click this if the current user does not 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:

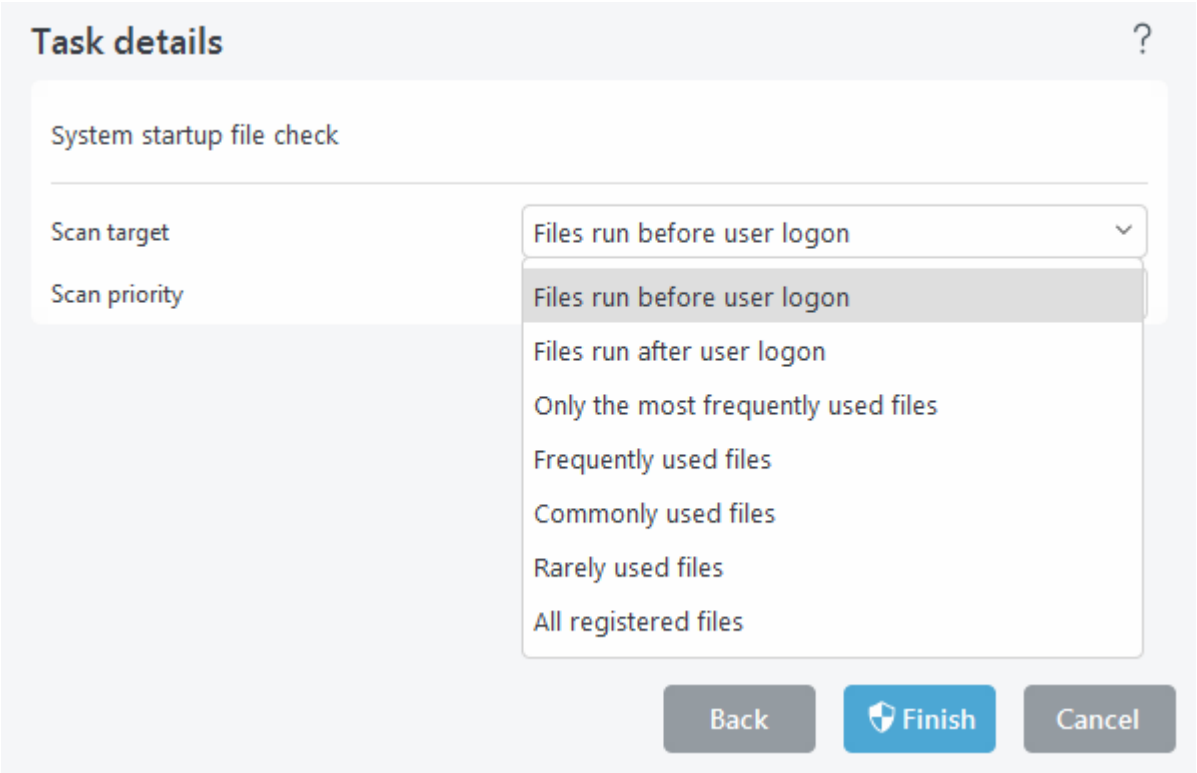
**Files run before user logon**

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 Security for Microsoft SharePoint 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.

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

- **Scan now**—This will trigger a scan of removable media.
- **Do not scan**—Removable media will not be scanned.
- **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 Security for Microsoft SharePoint features Device control, which enables you to define rules for external devices on a given computer.

To access settings for removable media scan, open **Advanced setup** (**F5**) > **Notifications** > **Interactive alerts** > **Edit**. If the **Ask user** is not selected, choose the action performed when a removable media is inserted into the computer:

- **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.
- **Forced device scan**—A computer scan of the inserted removable media device will be performed and cannot be canceled.
- **Show scan options**—Opens the **Interactive alerts** setup section.

# Document protection

The Document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements. Document protection provides a layer of protection in addition to Real-time file system protection, and can be disabled to enhance performance on systems that 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.

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

# Hyper-V scan

The current version of the Hyper-V scan supports scanning of the online or offline virtual system in Hyper-V. Supported types of scanning according to hosted Windows Hyper-V system and the state of the virtual system are shown here:

| Virtual systems with Hyper-V feature | Online VM | Offline VM |
|---|---|---|
| Windows Server 2022 Hyper-V | read-only | read-only/cleaning |
| Windows Server 2019 Hyper-V | read-only | read-only/cleaning |
| Windows Server 2016 Hyper-V | read-only | read-only/cleaning |
| Windows Server 2012 R2 Hyper-V | read-only | read-only/cleaning |
| Windows Server 2012 Hyper-V | read-only | 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 you avoid using the Dynamic Disk type in your VMs.
- 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 Security for Microsoft SharePoint.

> 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 Security for Microsoft SharePoint uses Hyper-V Management to detect and to connect to virtual disks. This way, ESET Security for Microsoft SharePoint has the same access to the virtual disk content when accessing data and files on any generic drive.

**Virtual Machine to be scanned is "online" – Running, Paused, Saved state**

ESET Security for Microsoft SharePoint uses Hyper-V Management to detect virtual disks. An actual connection to these disks is not possible. Therefore, ESET Security for Microsoft SharePoint creates a checkpoint/snapshot of the Virtual Machine, then connects to the checkpoint/snapshot. After 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.

Enable up to one minute for ESET Security for Microsoft SharePoint to create a snapshot or checkpoint during scanning. It would help if you considered this 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 detection order and is identical to the order seen in the Disk Manager of the VM. This naming convention is used in the tree-structured drop-down menu of targets to be scanned in the progress bar and 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 PROTECT as a Client Task called Server Scan.
- Hyper-V scan can be managed and started via eShell.

You can 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 specific Virtual Machine has to be created. While creating 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 enables you to name two different Virtual Machines identically, which presents an issue when trying to differentiate the machines while reviewing the scan logs.

To create a new profile, select **Edit** next to **List of profiles**, enter your own **Profile name** and then click **Add**. New profile will be displayed in the **Selected profile** drop-down menu that lists existing scan profiles.

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 the gear icon, modify the interval to **Stop scan if it runs longer than (minutes)**, and change to preferred time (anything between 1 to 2880 minutes).

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.

Hyper-V & Machine learning protection

Reporting is performed by detection engine and the machine learning component.

ThreatSense parameters

To modify scan parameters for Hyper-V scan.

# 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.

> ⚠ 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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 Microsoft 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.

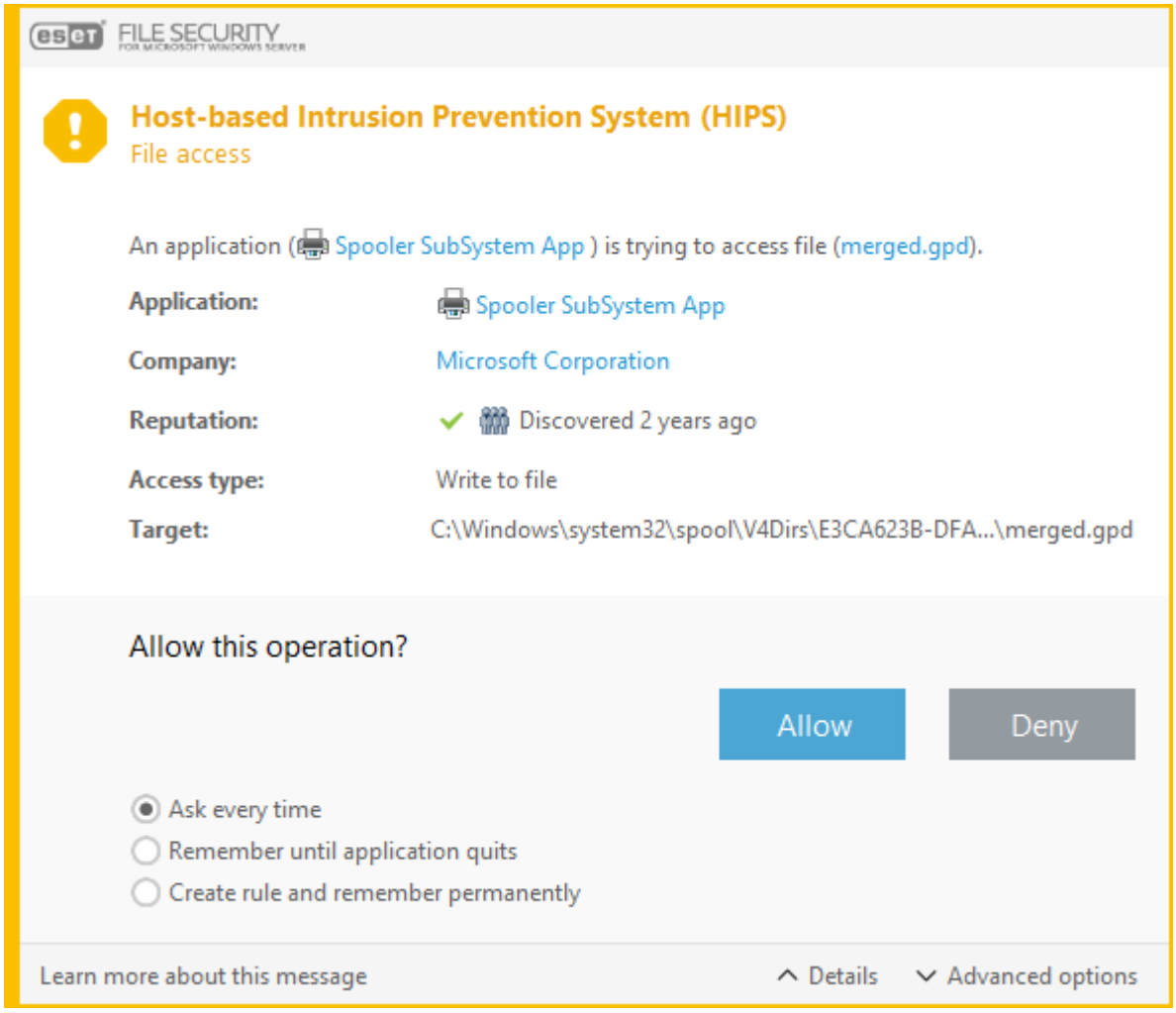
- **Policy-based mode** – Operations are blocked. Accepts only user/pre-defined rules.

- **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.




**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. |

| Rule | User-defined or automatically chosen rule name. |
|---|---|
| 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 window appears in the Windows notification area 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.

> 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.

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

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.

> 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. Use this feature only when troubleshooting or requested by ESET Technical Support, as it might generate a huge log file and slow down the system.

**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.

> 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.
**Automatic profile switching**
Assign an update profile according to Known networks in Firewall. Automatic profile switching allows to change the profile for specific network depending on the setting in Scheduler. Check help pages for more information
**Configure update notifications**
Click **Edit** to select what application notifications are displayed. You can choose if the notifications Show on a desktop or Forward to email.
**Clear update cache**
If you experience problems with an update, click **Clear** to clear the temporary update cache.

## Product updates

**Auto-updates**
Enabled by default. Use the slider to disable auto-updates if you need to stop the ESET Security for Microsoft SharePoint from being updated temporarily. We recommend that you keep this setting enabled to ensure your ESET Security for Microsoft SharePoint has the latest Program Component Updates (PCU), and micro Program Component Updates (µPCU) applied when a new update is available.

The updates are applied after the next server restart.

## Outdated detection engine alerts

**Set maximum detection engine age automatically / Maximum detection engine age (days)**
Use the slider to disable automatic detection engine age and set the maximum time manually (in 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 Security for Microsoft SharePoint records snapshots of detection engine and program modules for use with the Rollback feature. To create detection engine snapshots, leave **Create snapshots of modules** enabled.
**Number of locally stored snapshots**
Defines the number of previous module snapshots stored.
**Rollback to previous modules**
Click Rollback to revert program modules to previous version and temporarily disable updates.

Profiles
To create a custom update profile, select **Edit** next to **List of profiles**. Type 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).

**Enable update delivery optimization**

When enabled, update files are downloaded from CDN (content delivery network). Disabling this setting may cause download interruptions and slowdowns when dedicated ESET update servers are overloaded. Disabling is useful when a firewall is limited to access ESET update server IP addresses only or a connection to CDN services is not working.

**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.

## 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**.

## Product updates

Pausing auto-updates for specific update profiles temporarily disables automatic product updates, for example while connected to the internet using other networks or metered connections. Keep this setting enabled to have constant access to the latest features and the highest possible protection.

In some cases, a server restart may be required for the updates to take place.

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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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.

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 Security for Microsoft SharePoint, 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.

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

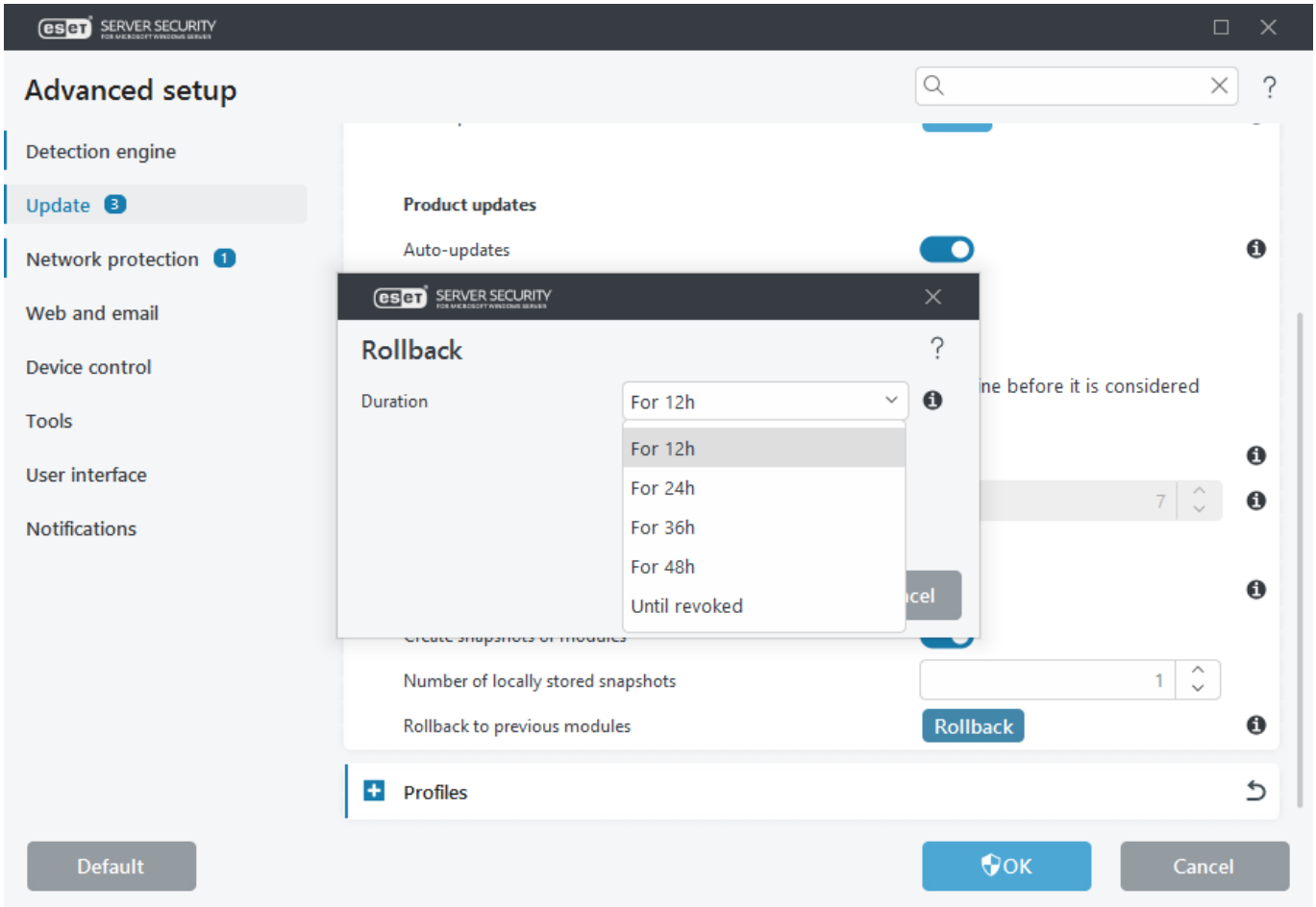
ESET Security for Microsoft SharePoint records snapshots of the detection engine and program modules for use with the rollback feature. To create virus database snapshots, keep **Create snapshots of modules** enabled.

When **Create snapshots of modules** enabled, the first snapshot is created during the first update. The next one is created after 48 hours.

The **Number of locally stored snapshots** field defines the number of stored detection engine snapshots.

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

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. Since it represents a potential security risk, we recommend not selecting this option.

If a rollback is performed, the **Rollback** button changes to **Allow updates**. Updates are not allowed for the time interval selected from the **Suspend updates** drop-down menu.

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

# Scheduled Task - Update

If you want to update the program from two update servers, then it is necessary to create two different update profiles. If the first one fails to download 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.

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

ESET Security for Microsoft SharePoint 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.

To minimize internet traffic on networks where ESET PROTECT is used to manage many clients, we recommend using ESET Bridge rather than configuring a client as a mirror. ESET Bridge can be installed with ESET PROTECT using the All-in-one installer or as a standalone component. For more information and differences between ESET Bridge, Apache HTTP Proxy, Mirror Tool, and direct connectivity, see ESET PROTECT Online Help page.

Update mirror

**Create update mirror**
Activates mirror configuration options.

### Access to update files

**Enable HTTP server**
If enabled, update files can be accessed through HTTP, no credentials are required.
**Storage folder**
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.
Click **Clear** if you want to change a defined default folder to store mirrored files *C:\ProgramData\ESET\ESET Security\mirror*.

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.

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 Security for Microsoft SharePoint 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 the program authenticates using the currently logged-in user account. The drawback of this solution is that the program cannot 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. Be aware that the specified user account must have access to the updated files directory on the local server. If the user does not have access, the program cannot establish a connection and download updates.

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

Manage network protection, click **Edit** to add a new one or modify the existing:

- Known networks
- Zones

# Known networks

When using a computer that frequently connects to public networks or networks outside of your normal work network, we recommend that you verify the network credibility of new networks that you are connecting to. Once networks are defined, ESET Security for Microsoft SharePoint can recognize trusted (Home/office) networks using various network parameters configured in Network Identification.

Computers often enter networks with IP addresses that are similar to the trusted network. In such cases, ESET Security for Microsoft SharePoint may consider an unknown network to be trusted (Home/office). We recommend that you use Network authentication to avoid this type of situation.

When a network adapter is connected to a network or its network settings are reconfigured, ESET Security for Microsoft SharePoint will search the known network list for a record that matches the new network. If Network identification and Network authentication (optional) match, the network will be marked connected in this interface.

When no known network is found, network identification configuration will create a new network connection to identify the network the next time that you connect to it. By default, the new network connection uses the Public network protection type.

The new Network Connection Detected dialog window will prompt you to choose between the Public network, Home or office network or Use Windows setting protection type. If a network adapter is connected to a known network and that network is marked as Home or office network, local subnets of the adapter will be added to the Trusted zone.

**Protection type of new networks**

Select which of the following options: **Use Windows setting**, **Ask user** or **Mark as public** is used by default for new networks. When you select **Use Windows setting** a dialog will not appear and the network you are connected to will automatically be marked according to your Windows settings. This will cause certain features (for example file sharing and remote desktop) to become accessible from new networks.

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

# Add network

Network configuration settings are arranged in the following tabs:

### Network

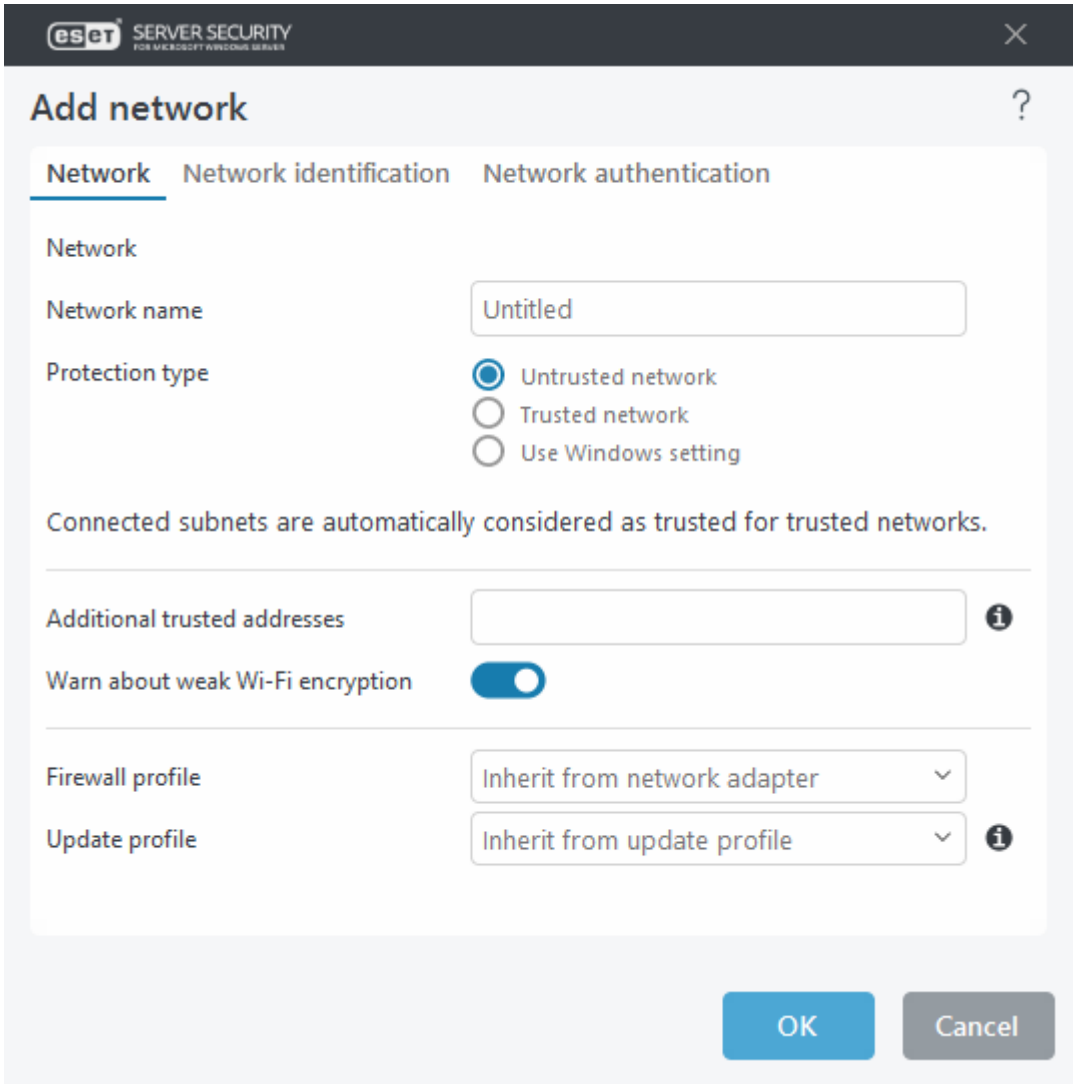
You can define the **Network name** and select the **Protection type** for the network. Shows if the network is set to **Trusted network**, **Untrusted network** or **Use Windows setting**.

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

- **Warn about weak WiFi encryption**—ESET Security for Microsoft SharePoint will inform you when you connect to an unprotected wireless network or network with weak protection.

- **Firewall profile** will be inherited from the network adapter.

- **Update profile**—Select update profile that will be used when connected to this network.




### Network identification

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

### Network authentication

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

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

- PEM encrypted public key (.pem), this key can be generated using the ESET Authentication Server.
- Encrypted public key

- Public key certificate (.crt)

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

| Server authentication failed. Invalid or mismatched signature. | Server signature does not match the public key entered. |
|---|---|
| Server authentication failed. Network name does not match. | Deactivate this switch if you want to keep the rule in the list but do not want to use it. |
| Server authentication failed. Invalid or no response from server. | No response is received if the server is not running or is inaccessible. An invalid response may be received if another HTTP server is running on the specified address. |
| Invalid public key entered. | Verify that the public key file you have entered is not corrupted. |

# Zones

A zone represents a collection of network addresses that create one logical group of IP addresses, which is useful when you reuse the same set of addresses in multiple rules. Each address in a given group is assigned similar rules defined centrally for the whole group. One example of such a group is a **Trusted zone**. A Trusted zone represents a group of network addresses that are not blocked by the Firewall in any way.

To add a trusted zone:

1. Open **Advanced setup** (**F5**) > **Network protection** > **Basic** > **Zones**.
2. Click **Edit** next to the **Zones**.
3. Click **Add**, type **Name** and **Description** for the new zone, and add a remote IP address into the **Remote computer address (IPv4/IPv6, range, mask)** field.
4. Click **OK**.

**Columns**

- **Name**—Name of a group of remote computers.
- **IP addresses**—Remote IP addresses that belong to a zone.

**Control elements**

When you add or edit a zone, the following fields are available:

- **Name**—Name of a group of remote computers.
- **Description**—A general description of the group.
- **Remote computer address (IPv4, IPv6, range, mask)**—A remote address, address range or subnet.
- **Delete**—Removes a zone from the list.

Pre-defined zones cannot be removed.

# Network attack 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.

> If your environment runs a high-speed network (10GbE and above), read the KB article for information on network speed performance and ESET Security for Microsoft SharePoint.

**Brute-force attack protection**

ESET Security for Microsoft SharePoint inspects network traffic content and blocks the attempts of password-guessing attacks.

**Advanced options**

Configure the advanced filtering options to detect the various types of attacks and vulnerabilities than can be carried out against your computer.

**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 Windows notification area 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 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 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 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**).

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.

# Suspected threat blocked

This situation can occur when an application on your computer is trying to transmit malicious traffic to another computer on the network, exploiting a security hole or if someone is trying to scan ports on your network.

- Threat – Name of the threat.
- Source – Source network address.

- Target – Target network address.
- Stop blocking – Creates an IDS rule for the suspected threat with settings to allow communication.
- Keep blocking – Blocks the detected threat. To create an IDS rule with settings to block communication for this threat, select Do not notify me again.

> The information shown in this notification window may vary depending on the type of threat detected. For more information about threats and other related terms, see Types of remote attacks or Types of detections.

# 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 (up to one hour). Shows **IP address** that have been locked.

**Block reason**

Shows type of attack that has been prevented from the address (for example security vulnerability exploitation attempt).

**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.

# Brute-force attack protection

Brute-force attack protection blocks password-guessing attacks for RDP and SMB services. A brute-force attack is a method of discovering a targeted password by systematically trying all possible combinations of letters, numbers, and symbols.

- **Enable Brute-force attack protection** – ESET Security for Microsoft SharePoint inspects network traffic content and blocks the attempts of password-guessing attacks.
- Rules – To create, edit and view rules for incoming and outgoing network connections.
- Exclusions – List of excluded detections defined by an IP address or application path. You can create and edit exclusions in ESET PROTECT Web Console.

# Brute-force attack protection rules

Brute-force attack protection rules to create, edit and view rules for incoming and outgoing network connections. The pre-defined rules cannot be edited or deleted.

Create a new rule, click **Add** new Brute-force attack protection rule, or **Edit** selected entries.

This window gives you an overview of existing Brute-force attack protection rules.

| Name | 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 or Deny – that should be performed if the conditions are right. |
| Protocol | The communication protocol this rule will inspect. |
| Profile | Custom rules can be set and applied for specific profiles. |
| Max attempts | The maximum number of allowed attempts of attack repetition until the IP address is blocked and added to the blacklist. |
| Blacklist retention period (min) | Sets the time for the address expiration from the blacklist. The default time period for counting the number of attempts is 30 minutes. |
| Source IP | A list of IP addresses/ranges/subnets. Multiple addresses must be separated by a comma. |
| Source zones | Enables you to add a pre-defined or created zone with a range of IP addresses here by clicking Add. |

# Brute-force attack protection exclusions

Brute-force exclusions can be used to suppress Brute-force detection for specific criteria. These exclusions are created from ESET PROTECT based on Brute-force detection. The exclusions will be displayed if an administrator creates Brute-force exclusions in ESET PROTECT Web Console. Exclusions can contain allowing rules only and are evaluated before IDS rules.

- **Detection** – Type of detection.
- **Application** – Select the file path of an excepted application by clicking ... (for example *C:\Program Files\Firefox\Firefox.exe*). Do not type the name of the application.
- **Remote IP** – A list of remote IPv4 or IPv6 address/ranges/subnets. Multiple addresses must be separated by a comma.

# 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 web browser or email client used. If protocol filtering is enabled, ESET Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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.

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.

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.

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 Security for Microsoft SharePoint focuses on web browser security. Each application accessing the network can be marked as a web 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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.

When 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 Automatic mode and ask in Interactive mode.

• **Scan or Ignore**—To scan or ignore communication secured by this certificate.

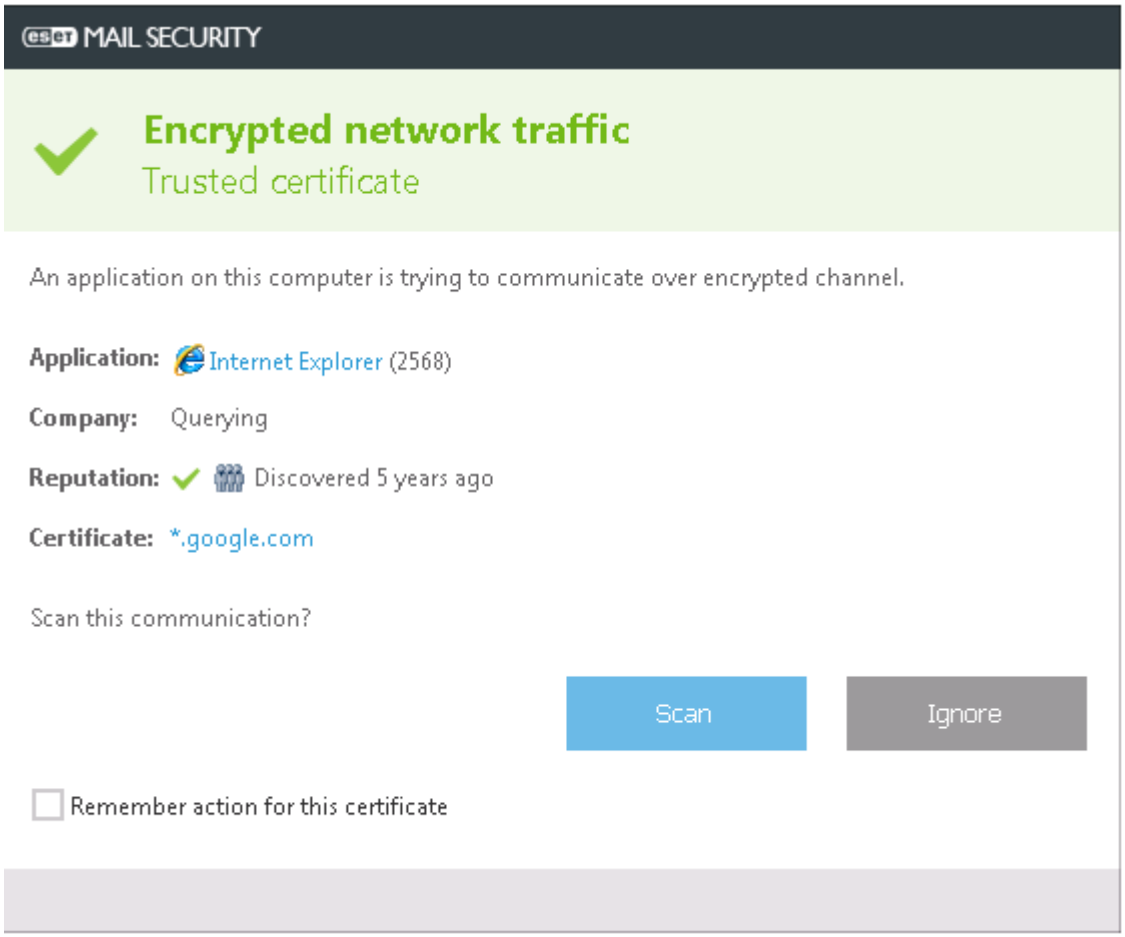
• **Ask**—Receive a prompt when a specific certificate is encountered.

# 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint must **Ignore** that traffic to keep the application working.



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

# Email client protection

Integration of ESET Security for Microsoft SharePoint 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 Security for Microsoft SharePoint. When integration is activated, the ESET Security for Microsoft SharePoint toolbar is inserted directly into the email client for more efficient email protection. Integration settings are located under **Advanced setup** (**F5**) > **Web and email** > **Email client protection** > **Email client integration**.

**Email client integration**

Microsoft Outlook is currently the only supported email client. Email protection works as a plugin. The main advantage of the plugin is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner. For a complete list of supported email clients and their versions, refer to the following Knowledgebase article.

**Attachment handling optimization**—If optimization is disabled all attachments are scanned immediately. When disabled, it can slow down email client performance.

**Advanced email client processing**—If you are experiencing a system slowdown when working with your email client, disable this option.

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).

**Disable checking upon inbox content change**

If you are experiencing a system slowdown when working with your email client (Microsoft 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.
- **Modified email** – Toggles checking of modified messages.

**Action to be performed on infected email**

- **No action** – If enabled, the program will identify infected attachments, but will leave emails without taking any action.

- **Delete email** – The program will notify the user about infiltration(s) and delete the message.
- **Move email to the Deleted items folder** – Infected emails will be moved automatically to the Deleted items folder.
- **Move email to folder** – 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 Security for Microsoft SharePoint provides protection for these protocols regardless of the email client used.

ESET Security for Microsoft SharePoint also supports the scanning of IMAPS and POP3S protocols, which use an encrypted channel to transfer information between server and client. ESET Security for Microsoft SharePoint 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. |

# Email tags

Email protection provides control of email communications received through the POP3 and IMAP protocols. Using the plug-in for Microsoft Outlook and other email clients, ESET Security for Microsoft SharePoint 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 select **Append tag messages to received and read email** or **Append tag messages to sent email**.

Be aware that on rare occasions, tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both.

The available options are:

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

**Text to add to subject of detected email**

Edit this template if you want to modify the subject prefix format of an infected email. This function will replace the message subject `Hello` with the following format: `"[detection %DETECTIONNAME%] Hello`. The variable `%DETECTIONNAME%` represents the detection.

# Microsoft Outlook toolbar

Microsoft Outlook protection works as a plug-in module. After ESET Security for Microsoft SharePoint is installed, this toolbar containing the malware protection options is added to Microsoft Outlook:

**ESET Security for Microsoft SharePoint**

Click the icon to open the main program window of ESET Security for Microsoft SharePoint.

**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 Security for Microsoft SharePoint is installed, this toolbar containing the malware protection options is added to Outlook Express or Windows Mail:

**ESET Security for Microsoft SharePoint**

Click the icon to open the main program window of ESET Security for Microsoft SharePoint.

**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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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 web browsers. By default, ESET Security for Microsoft SharePoint is configured to monitor the HTTP protocol used by most web browsers.

ESET Security for Microsoft SharePoint also supports HTTPS protocol checking. HTTPS communication uses an encrypted channel to transfer information between server and client. ESET Security for Microsoft SharePoint 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.

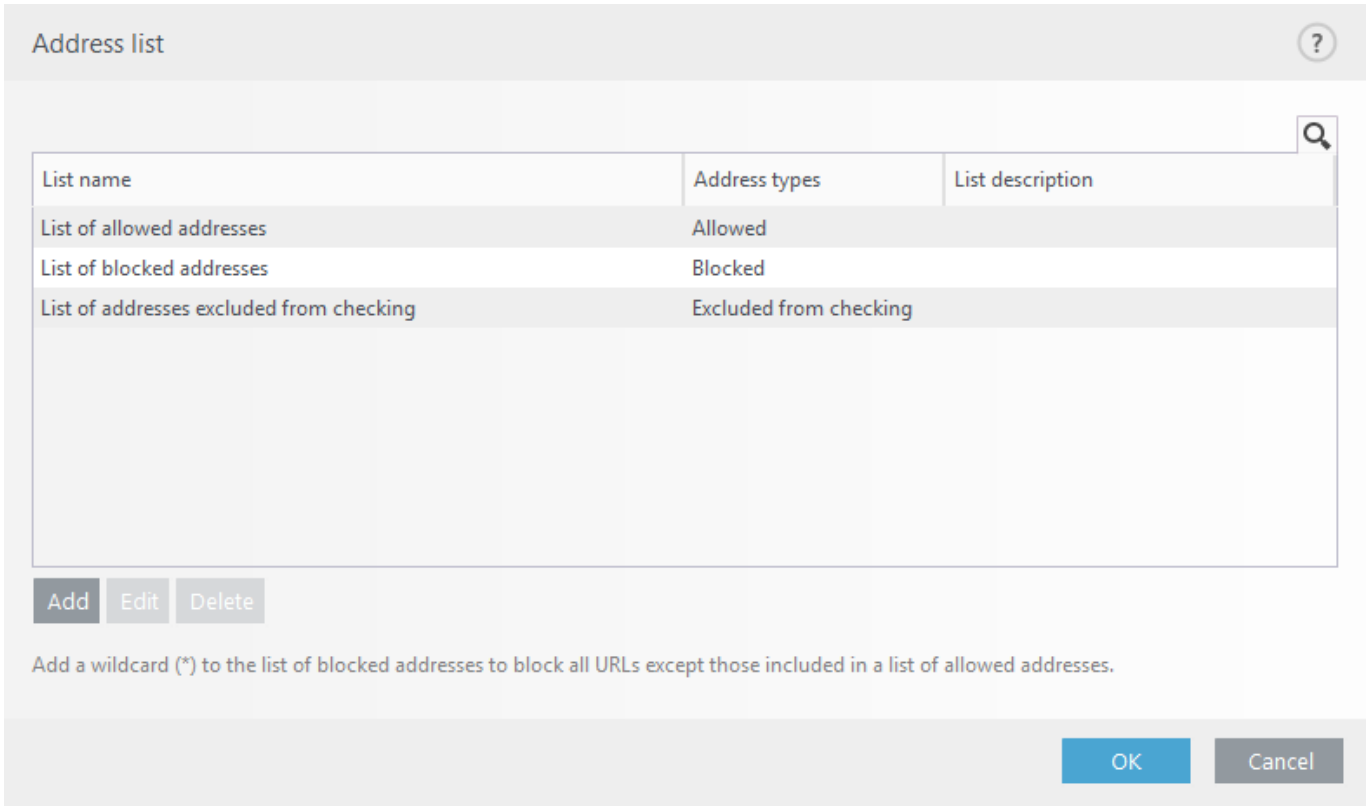
One list of blocked addresses may contain addresses from some external public blacklist, and a second one may contain your own blacklist, which makes it easier to update the external list while keeping yours intact.

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.




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. Carefully specify 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.

> 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 specific 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 PROTECT.

ESET Security for Microsoft SharePoint enables user to block access to specified websites and prevent the web 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 want to specify a whole group of remote servers, so-called masks can be used to identify such a group.

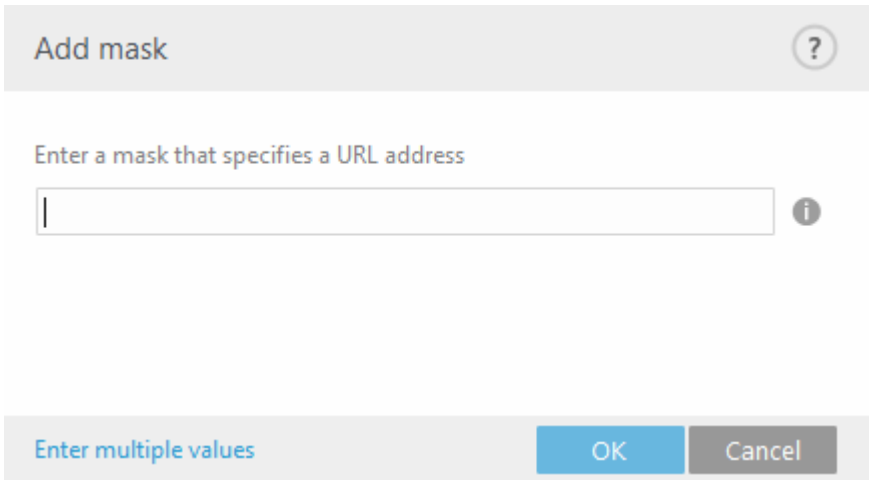
The masks include the symbols ? and *:

• use ? to substitute a symbol

• use * to substitute a text string

✓ **.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).

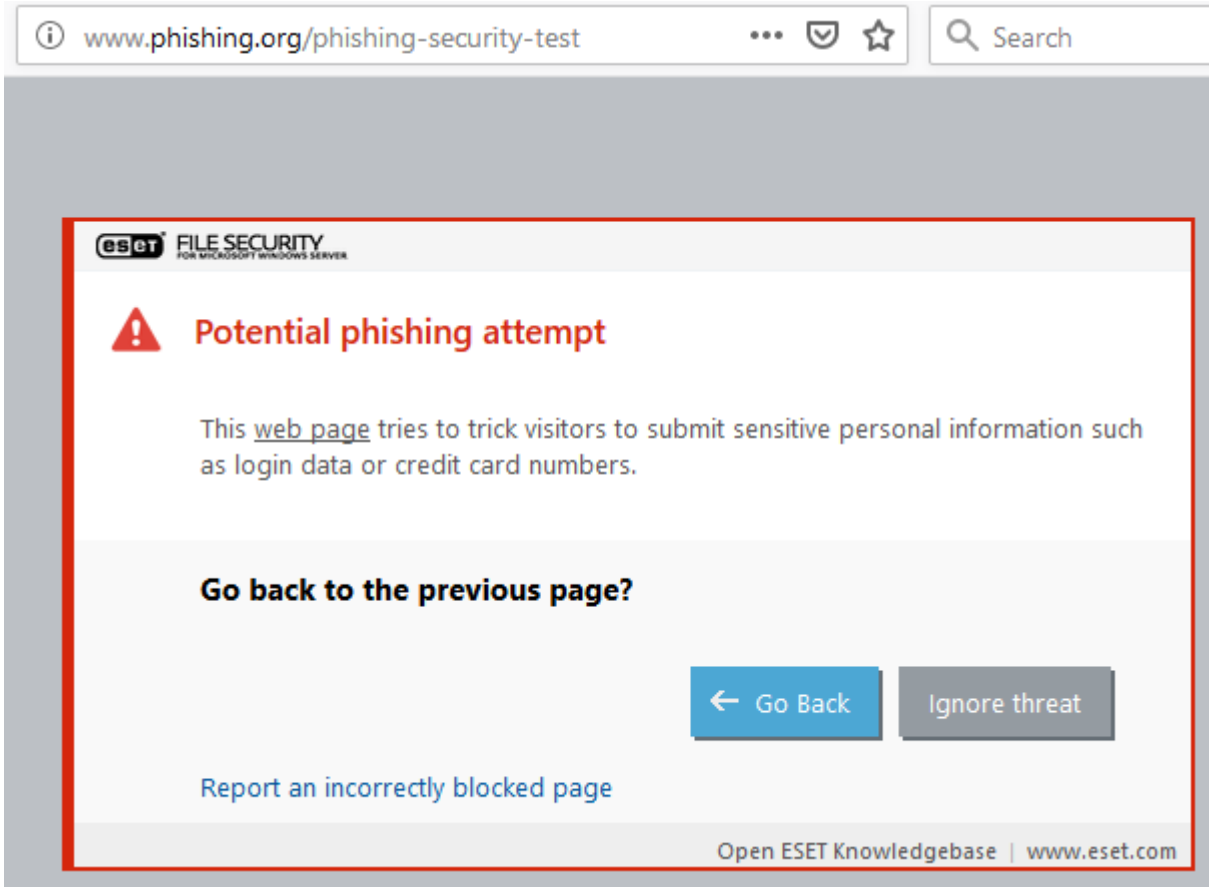



# Anti-Phishing web protection

The term phishing defines a criminal activity that uses social engineering (the manipulation of users to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more.

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

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).




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 Security for Microsoft SharePoint 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.

When you enable device control using **Integrate into system** switch, the Device control feature of ESET Security for Microsoft SharePoint 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.

> 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 do not 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.

> 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).

**Criteria type**

Additional parameters below can be used to fine-tune rules and tailor them to devices. All parameters are case-sensitive and support wildcards (*, ?):

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

> If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-sensitive and support wildcards (a question mark (?) represents a single character, whereas an asterisk (*) represents a string of zero or more characters).

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.

> 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 do not want to delete a rule permanently so that you can use it in the future.

**Populate**

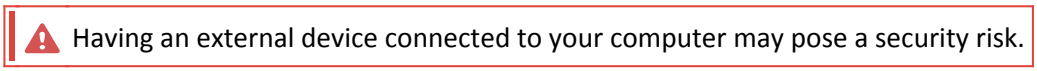
Provides an overview of all currently connected devices with the following information: device type, device vendor, model and serial number (if available). When you select a device (from the list of Detected devices) and click **OK**, a rule editor window appears with pre-defined information (you can 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.




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. Each device starts at the new line.

**Vendor**, **Model**, and **Serial** must be present for each device and separated with a comma.

Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

**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).

**Add device**

Click Add in the right window to add a device to an existing group. Additional parameters shown below can be used to fine-tune rules for different devices. All parameters are case-sensitive and support wildcards (*, ?):

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

If these parameters are undefined, the rule will ignore these fields while matching. Filtering parameters in all text fields are case-sensitive and support wildcards (a question mark (?) represents a single character, whereas an asterisk (*) represents a string of zero or more characters).

After creating a device group, you have to add a new device control rule for the created device group and choose the action to take.

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

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
- Microsoft Windows update
- ESET CMD
- ESET RMM

- License
- WMI Provider
- ESET management console scan targets
- Log files
- Proxy server
- 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 Security for Microsoft SharePoint 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.

# Command line scanner

As an alternative to eShell, you can run ESET Security for Microsoft SharePoint On-demand scanner via command line using `ecls.exe` located in the installation folder.

The following is a list of parameters and switches:

**Options:**

| | |
|---|---|
| /base-dir=FOLDER | load modules from FOLDER |
| /quar-dir=FOLDER | quarantine FOLDER |
| /exclude=MASK | exclude files matching MASK from scanning |
| /subdir | scan subfolders (default) |
| /no-subdir | do not scan subfolders |
| /max-subdir-level=LEVEL | maximum sub-level of folders within folders to scan |
| /symlink | follow symbolic links (default) |
| /no-symlink | skip symbolic links |
| /ads | scan ADS (default) |
| /no-ads | do not scan ADS |
| /log-file=FILE | log output to FILE |
| /log-rewrite | overwrite output file (default – append) |
| /log-console | log output to console (default) |
| /no-log-console | do not log output to console |
| /log-all | also log clean files |
| /no-log-all | do not log clean files (default) |
| /aind | show activity indicator |
| /auto | scan and automatically clean all local disks |

**Scanner options:**

| | |
|---|---|
| /files | scan files (default) |
| /no-files | do not scan files |
| /memory | scan memory |
| /boots | scan boot sectors |
| /no-boots | do not scan boot sectors (default) |
| /arch | scan archives (default) |
| /no-arch | do not scan archives |
| /max-obj-size=SIZE | only scan files smaller than SIZE megabytes (default 0 = unlimited) |
| /max-arch-level=LEVEL | maximum sub-level of archives within archives (nested archives) to scan |
| /scan-timeout=LIMIT | scan archives for LIMIT seconds at maximum |
| /max-arch-size=SIZE | only scan the files in an archive if they are smaller than SIZE (default 0 = unlimited) |
| /max-sfx-size=SIZE | only scan the files in a self-extracting archive if they are smaller than SIZE megabytes (default 0 = unlimited) |
| /mail | scan email files (default) |
| /no-mail | do not scan email files |
| /mailbox | scan mailboxes (default) |
| /no-mailbox | do not scan mailboxes |
| /sfx | scan self-extracting archives (default) |

| | |
|---|---|
| /no-sfx | do not scan self-extracting archives |
| /rtp | scan runtime packers (default) |
| /no-rtp | do not scan runtime packers |
| /unsafe | scan for potentially unsafe applications |
| /no-unsafe | do not scan for potentially unsafe applications (default) |
| /unwanted | scan for potentially unwanted applications |
| /no-unwanted | do not scan for potentially unwanted applications (default) |
| /suspicious | scan for suspicious applications (default) |
| /no-suspicious | do not scan for suspicious applications |
| /pattern | use signatures (default) |
| /no-pattern | do not use signatures |
| /heur | enable heuristics (default) |
| /no-heur | disable heuristics |
| /adv-heur | enable Advanced heuristics (default) |
| /no-adv-heur | disable Advanced heuristics |
| /ext-exclude=EXTENSIONS | exclude file EXTENSIONS delimited by colon from scanning |
| /clean-mode=MODE | use cleaning MODE for infected objects<br>The following options are available:<br>• none (default) – No automatic cleaning will occur.<br>• standard – ecls.exe will attempt to automatically clean or delete infected files.<br>• strict – ecls.exe will attempt to automatically clean or delete infected files without user intervention (you will not be prompted before files are deleted).<br>• rigorous – ecls.exe will delete files without attempting to clean regardless of what the file is.<br>• delete – ecls.exe will delete files without attempting to clean, but will refrain from deleting sensitive files such as Windows system files. |
| /quarantine | copy infected files (if cleaned) to Quarantine (supplements the action carried out while cleaning) |
| /no-quarantine | do not copy infected files to Quarantine |

**General options:**

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

**Exit codes:**

| | |
|---|---|
| 0 | no threat found |
| 1 | threat found and cleaned |
| 10 | some files could not be scanned (may be threats) |
| 50 | threat found |
| 100 | error (exit codes greater than 100 mean the file was not scanned and cannot be considered clean) |

# 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint configurations. You can do it manually or create a script for the purpose of automation.

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

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

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

Advanced ecmd commands can only be run locally. Executing the client task **Run command** using ESET PROTECT will not work.

Signing an *.xml* configuration file:

1. Download XmlSignTool executable.

2. Open a Windows Command Prompt (cmd) using **Run as administrator**.

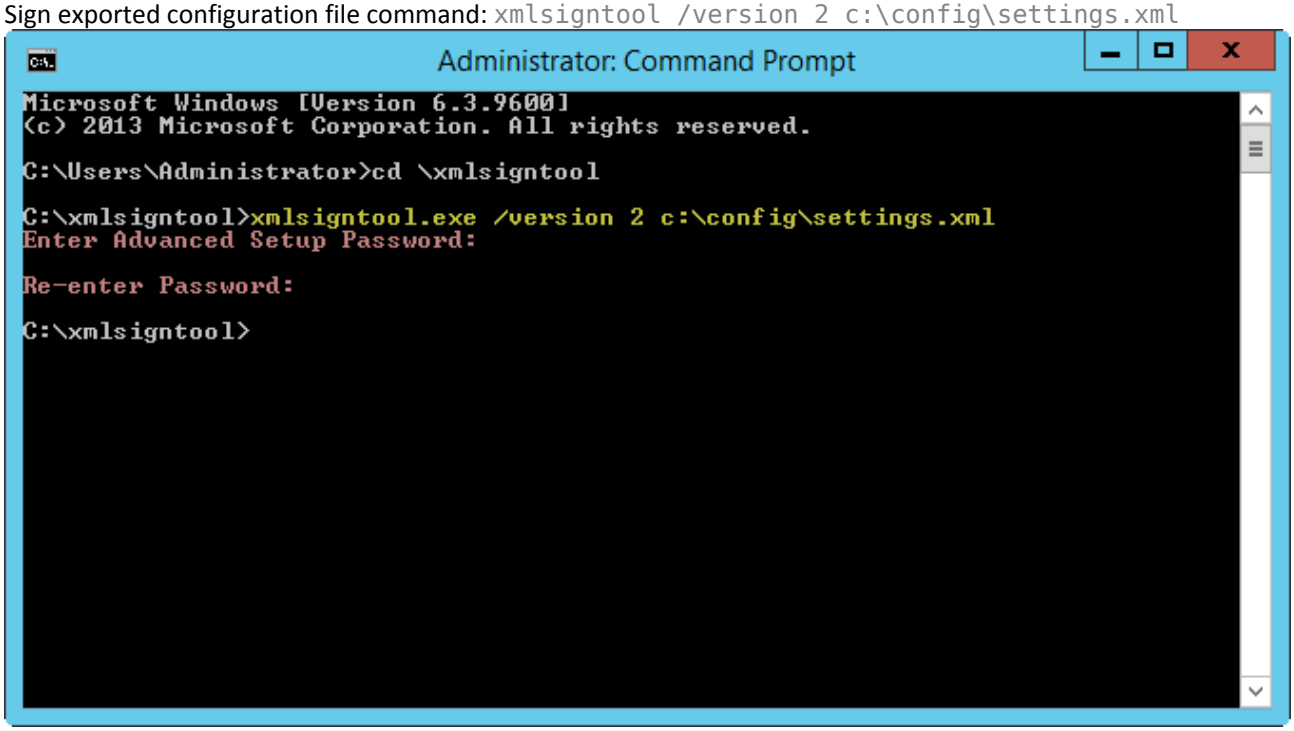
3. Navigate to the location of `xmlsigntool.exe`

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

Value of the parameter `/version` depends on the version of your ESET Security for Microsoft SharePoint. Use `/version 2` for ESET Security for Microsoft SharePoint 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 Security for Microsoft SharePoint with ESET CMD using the password authorization method.

Sign exported configuration file command: `xmlsigntool /version 2 c:\config\settings.xml`




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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint installation contains file *ermm.exe* located in ESET Security for Microsoft SharePoint (default path *c:\Program Files\ESET\ESET Security for Microsoft SharePoint* ). *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 Security for Microsoft SharePoint.

**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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint

- SERVER_EMAIL_AV - Anti-virus protection of emails of protected server product, for example, emails in Microsoft Exchange or IBM Domino

- SERVER_EMAIL_AS - Anti-spam protection of emails of protected server product, for example, emails in Microsoft 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 specific 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 an instance of a specific scan log is required, it must be filtered only 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 an instance of a specific scan log is required, it must be filtered only 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 - Email 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 an instance of a specific scan log is required, it must be filtered only 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 an instance of a specific scan log is required, it must be filtered only 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
```

# ESET Management console scan targets

This functionality lets ESET PROTECT use scan target (On-demand mailbox database scan and Hyper-V scan) when running the Server Scan client task on a server with ESET Security for Microsoft SharePoint. ESET PROTECT scan targets setting is available only if you have ESET Management Agent installed, otherwise it will be grayed out.

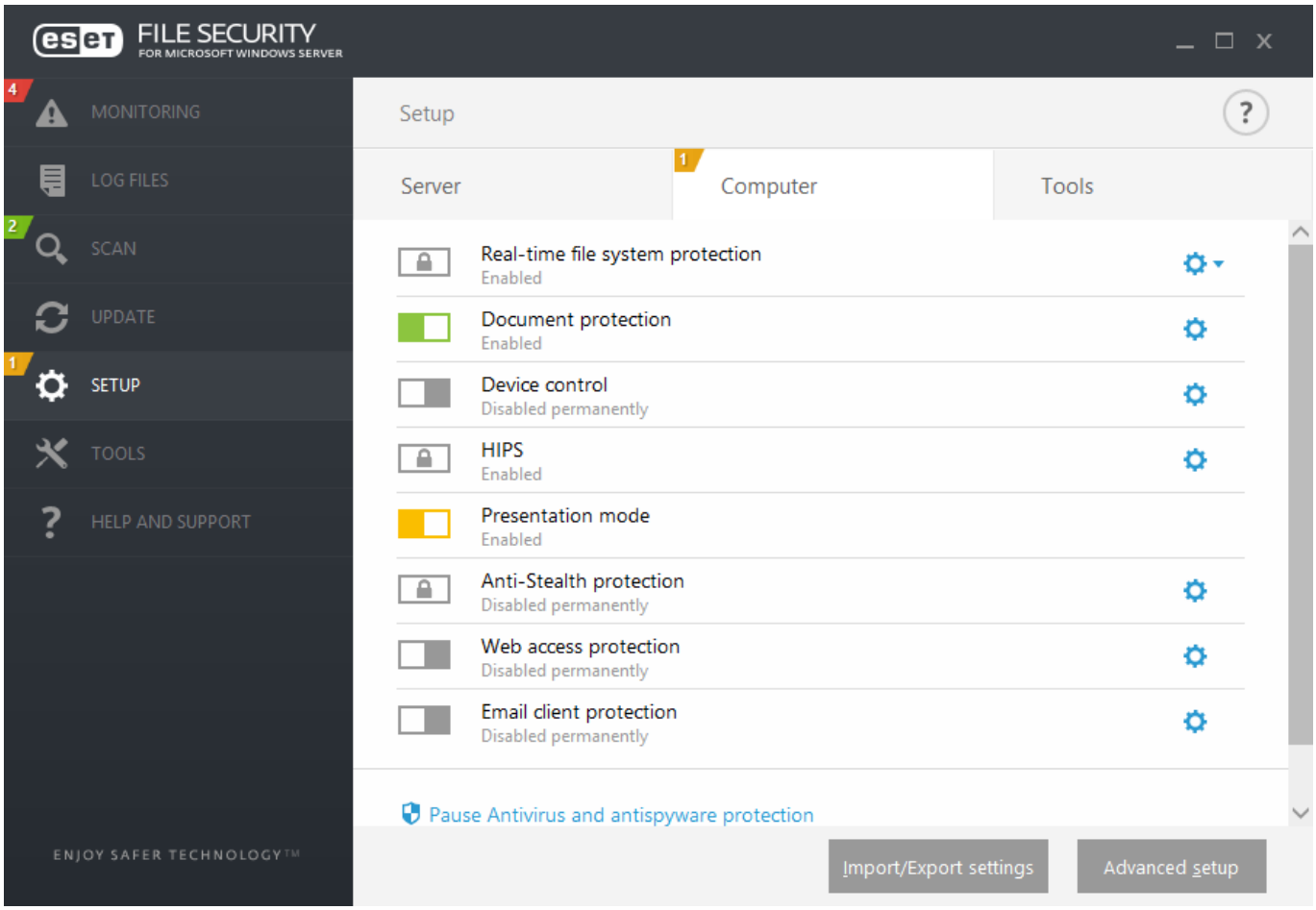
When you enable **Generate target list** ESET Security for Microsoft SharePoint creates a list of available scan targets. This list is generated periodically, according to your **Update period**.

When **Generate target list** is enabled for the first time, it takes ESET PROTECT about half of the specified **Update period** to pick it up. So if **Update period** is set to 60 minutes, it will take ESET PROTECT about 30 minutes to receive the list of scan targets. If you need ESET PROTECT to collect the list earlier, set the update period to a smaller value. You can always increase it later.

When ESET PROTECT 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 specific server.

# Override mode

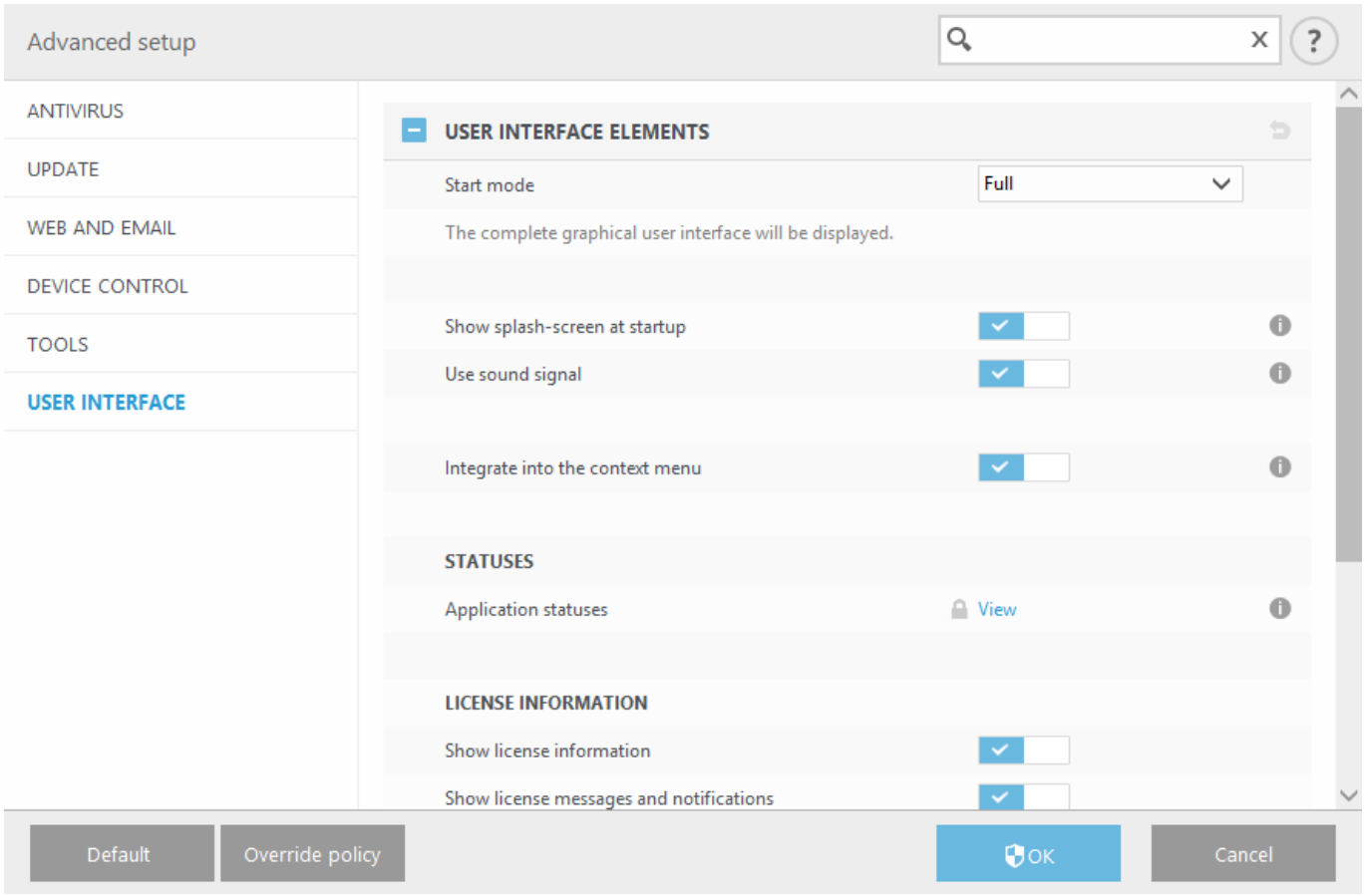
If you have ESET PROTECT policy applied to ESET Security for Microsoft SharePoint, you will see a lock icon instead of enable/disable switch on Setup page and a lock icon next to the switch in **Advanced setup** window.



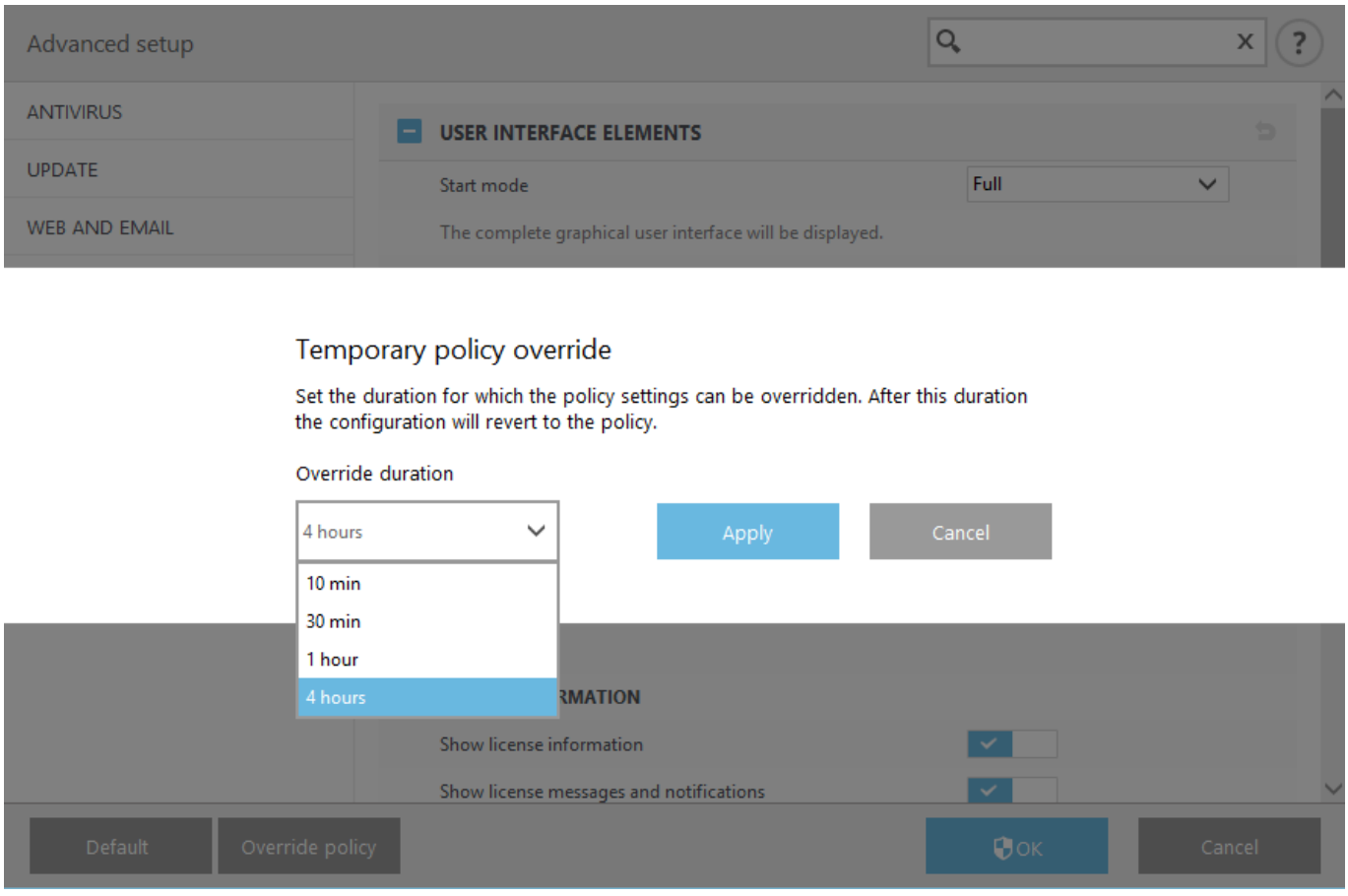

Normally, settings that are configured via ESET PROTECT policy cannot be modified. Override mode allows you to temporarily unlock these settings. However, you need to enable **Override mode** using ESET PROTECT policy.

Log into ESET PROTECT Web Console, navigate to **Policies**, select and edit existing policy that is applied to ESET Security for Microsoft SharePoint 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).

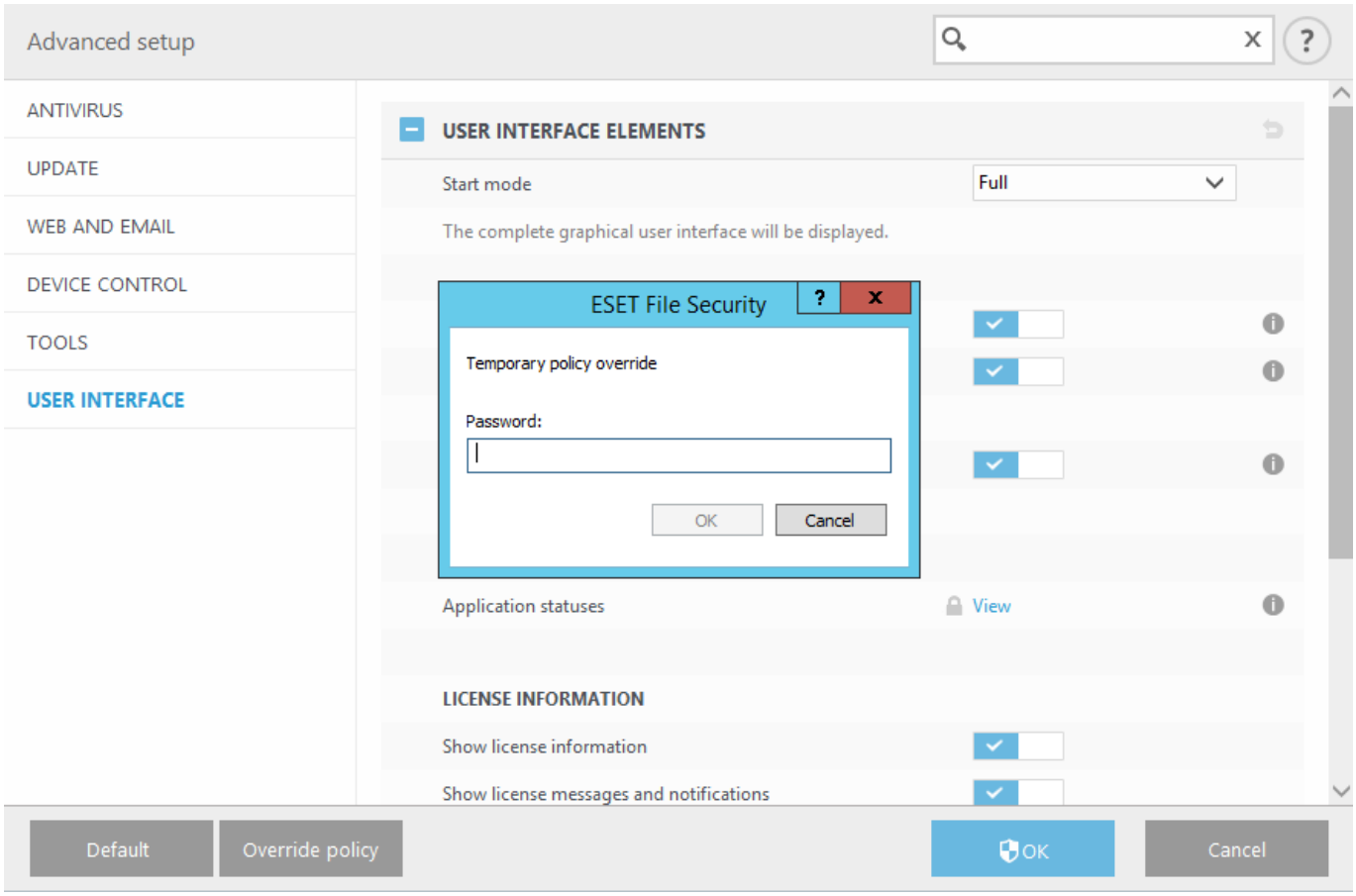
After the policy is modified, or new policy is applied to ESET Security for Microsoft SharePoint, Override policy button will appear in **Advanced setup** window.




Click **Override policy** button, set the duration and click **Apply**.




If you selected **Password** as Authentication type, enter the policy override password.




After the Override mode expires, any configuration changes you have made will revert back to original ESET PROTECT policy settings. You will 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 Security for Microsoft SharePoint logging.

## Logging filter

Produces a significant amount of data because all the logging options are enabled by default. We recommend that you selectively disable logging of the components which are not useful or related to the problem.

> To start the actual logging you need to turn on general **Diagnostic logging** on product level in main menu **Setup** > Tools. After the logging itself is turned on, ESET Security for Microsoft SharePoint will collect detailed logs according to what features are enabled in this section.

Use the switches to enable or disable specific feature. This options also be combined depending on the availability of individual components in the ESET Security for Microsoft SharePoint.

- **SharePoint related diagnostic logging** - Writes detailed information into logs, especially when troubleshooting is necessary.
- **Cluster diagnostic logging** - Cluster logging will be included in general diagnostic logging.
- **OneDrive diagnostic logging** - OneDrive logging will be included in general diagnostic logging.
-

## 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 to save disk space.

**Delete records automatically**

Log entries older than the specified number of days (below) will get deleted.

**Delete records older than (days)**

Specify the number of days.

**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 filename (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.

> 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.

**Audit Log**

Tracks changes in configuration or protection. Since the modification of the product configuration may dramatically affect how the product operates, you might want to track the changes for auditing purposes. You will see log records of changes in **Log files** > Audit log section.

# 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 Security for Microsoft SharePoint, 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 Security for Microsoft SharePoint. 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.

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.

# Presentation mode

Presentation mode is a feature for users that demand uninterrupted usage of their software, do not want to be disturbed by the notification windows, and want to minimize CPU usage. Presentation mode can also be used during presentations that cannot be interrupted by activity of ESET Security for Microsoft SharePoint. When enabled, all notification 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 Security for Microsoft SharePoint.

**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 Security for Microsoft SharePoint 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 Computer Scanner advanced logging** - Record all events that occur while scanning files and folders by Computer scan or Real-time file system protection.
**Enable Device control advanced logging** - Record all events that occur in Device control to allow diagnosing and solving problems.
**Enable Direct Cloud advanced logging** - Record all product communication between the product and Direct Cloud servers.
**Enable Document protection advanced logging** - Record all events in Document protection 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 the license server.
**Enable Memory tracing** - Record all events, which will help developers diagnose memory leaks.
**Enable Network protection advanced logging** - Record all network data passing through network protection in PCAP format to help developers diagnose and fix the problems related to network protection.
**Enable Operating System logging** - Additional information about Operating system such as running processes, CPU activity, disc operations will be gathered. This can help developers to diagnose and fix problems related to ESET product running on your operating system.
**Enable Protocol filtering advanced logging** - Record all data passing through the Protocol filtering engine in PCAP format to help developers diagnose and fix the problems related to Protocol filtering.
**Enable push messaging advanced logging** - Record all events during push messaging to allow diagnostics and problem-solving.
**Enable Real-time file system protection advanced logging** - Record all events in Real-time file system protection to allow diagnosing and problem-solving.
**Enable Update engine advanced logging** - Record all events that occur during the update process to help developers diagnose and fix the problems related to the Update engine.

### Log files location

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

# Technical support

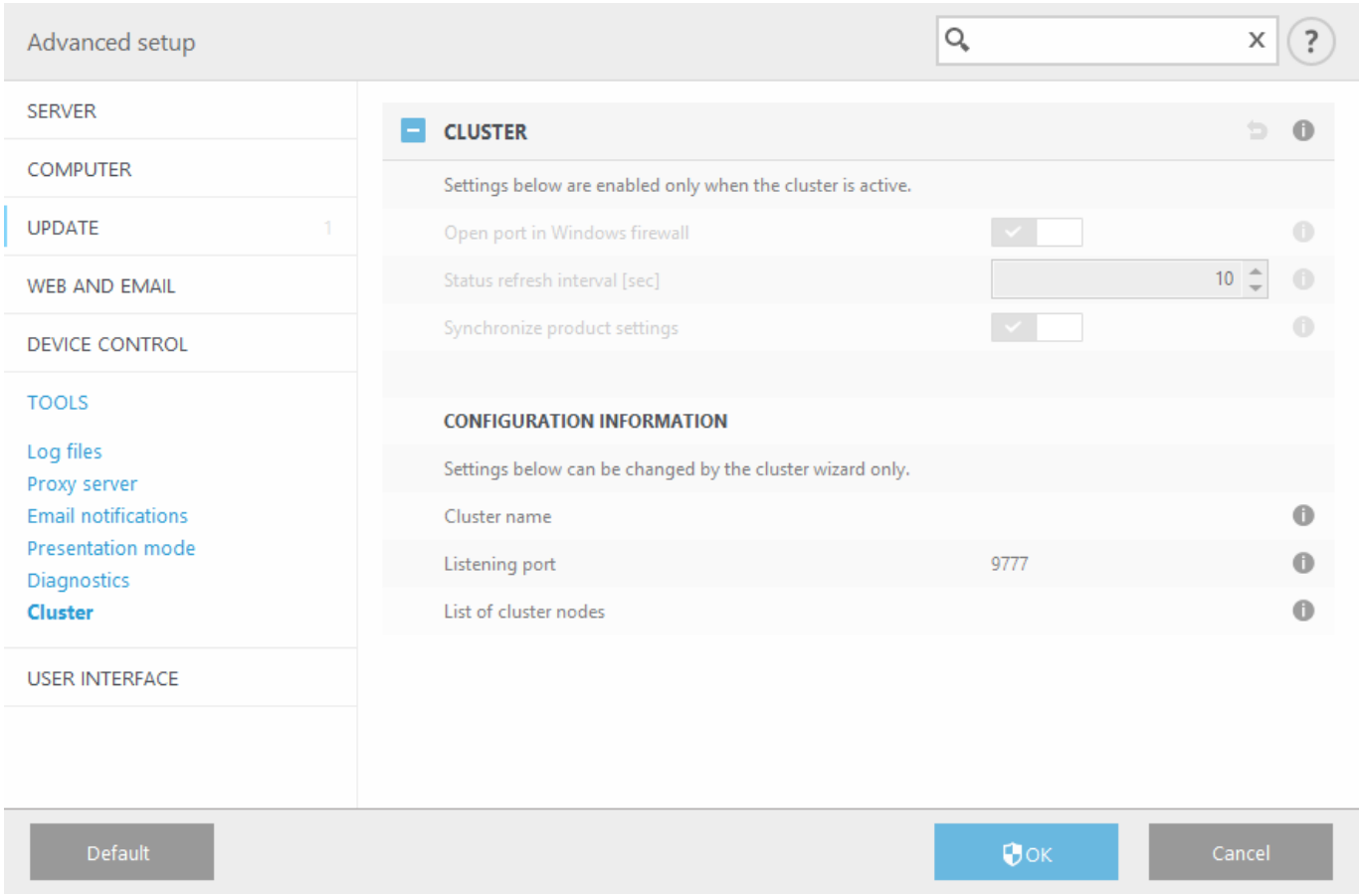
**Submit system configuration data**

Select **Always submit** not to be prompted before submitting your ESET Security for Microsoft SharePoint configuration data to customer care, or use **Ask before submission**.

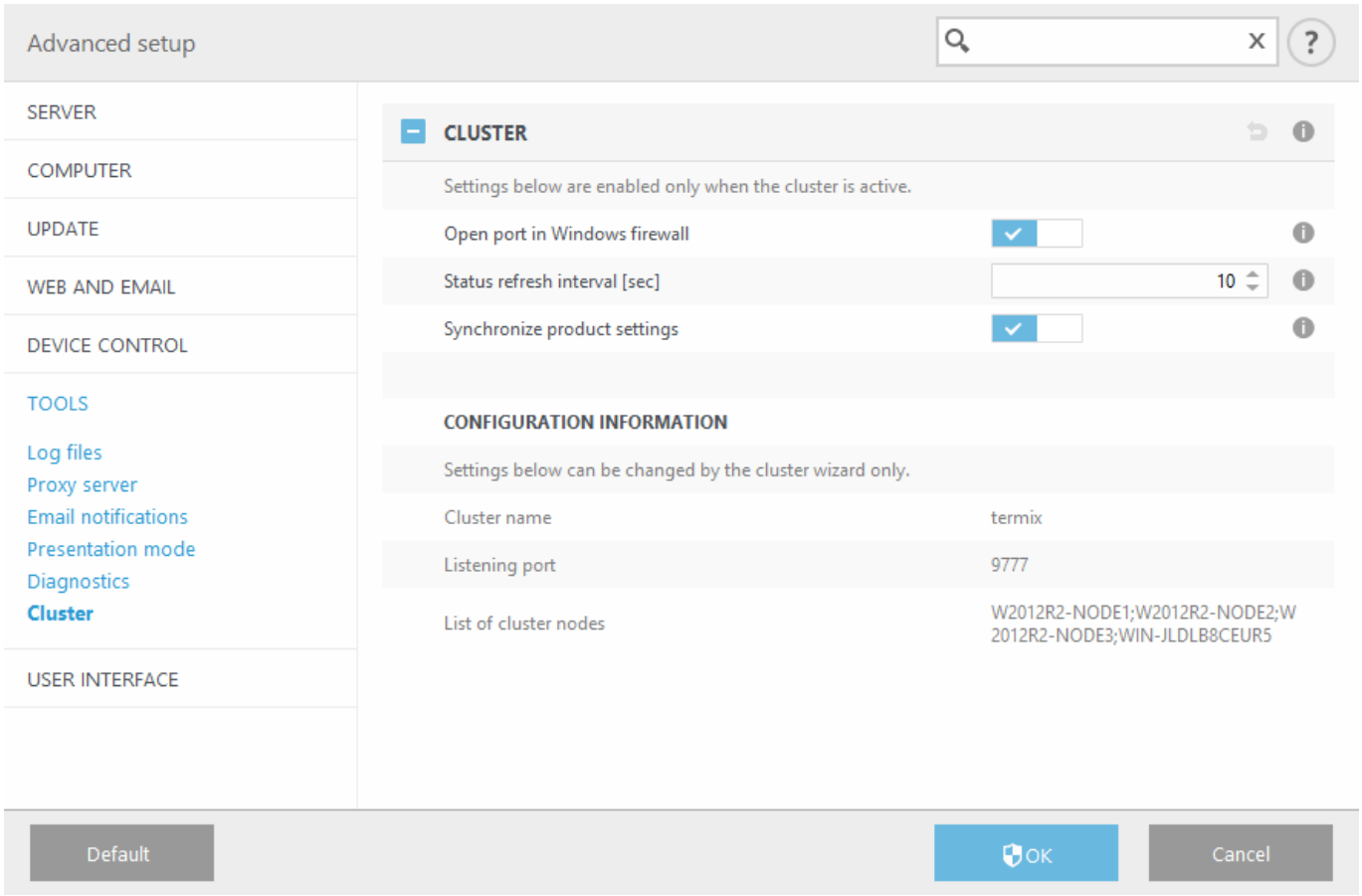
# Cluster

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:




ESET Cluster properly configured with its details and options:




# User interface

Configure the Graphical user interface (GUI) behavior of ESET Security for Microsoft SharePoint. You can adjust the program's visual appearance and effects.

Use the GUI start mode drop-down menu to select from the following Graphical user interface (GUI) start modes:

- **Full**—The complete user interface 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 Security for Microsoft SharePoint installed on Terminal server, see Disable GUI on Terminal Server topic.

**Color mode**

Select the color scheme of the ESET Security for Microsoft SharePoint graphical user interface (GUI) from the drop-down menu:

- **Same as the system color**—The ESET Security for Microsoft SharePoint color scheme is based on your operating system settings.

- **Dark**—The ESET Security for Microsoft SharePoint will use a dark color scheme (dark mode).

- **Light**—The ESET Security for Microsoft SharePoint will use a light color scheme (standard).

**Show splash-screen at startup** - Disable this option if you prefer not to have the splash screen displayed when main program window of your ESET Security for Microsoft SharePoint starts, for example, when logging into the system.

**Use sound signal** - ESET Security for Microsoft SharePoint 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 Security for Microsoft SharePoint 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.

### License Information

When enabled, messages and notifications about your license will be displayed.

**Show license information** - When disabled, the license expiration date on **Protection status** and **Help and support** screen will not be displayed.

**Configure license-related application statuses** - Opens the list of license-related application statuses.

**Configure license notifications** - When disabled, the notifications and messages will only be displayed when the license expired.

Access setup - You can prevent any unauthorized changes using the **Access setup** tool to ensure that security remains high.

ESET Shell - Configure access rights to product settings, features and data via eShell by changing the ESET Shell execution policy.

Icon in the Windows notification area

Revert all settings in this section

# Access setup

For maximum security of your system, it is essential that ESET Security for Microsoft SharePoint 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 Security for Microsoft SharePoint configuration password protected.



If you are uninstalling ESET Security for Microsoft SharePoint while using access setup password protection, you will be prompted to enter the password. You will otherwise not be able to uninstall ESET Security for Microsoft SharePoint.

**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 Security for Microsoft SharePoint and 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 Security for Microsoft SharePoint.

**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.

> 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 Security for Microsoft SharePoint 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 Security for Microsoft SharePoint running on Windows Terminal Server for user sessions.

Normally, the ESET Security for Microsoft SharePoint 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`

> If you have installed ESET Security for Microsoft SharePoint on a Citrix server, we recommend using the settings described in our Knowledgebase article.

# Icon in the Windows notification area

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

> To access the system tray (Windows notification area) icon menu, ensure the start mode of User Interface elements is set to Full.

**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. The **Time interval** drop-down menu enables you to specify how long the protection will be disabled.

Advanced setup

Opens the ESET Security for Microsoft SharePoint Advanced setup.

Log files

Contains information about all important program events that have occurred and provides an overview of detected threats.

**Reset window layout**

Resets the ESET Security for Microsoft SharePoint window to its default size and position on the screen.

**Color mode**

Opens User Interface settings where you can change the color of the graphical user interface.

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 Security for Microsoft SharePoint 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.

# 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.

Manage ESET Security for Microsoft SharePoint notifications, open the **Advanced setup** (**F5**) > **Notifications**. You can configure the following types:

Application statuses – Click **Edit** to select which application statuses will be displayed in the home section of the main program window.

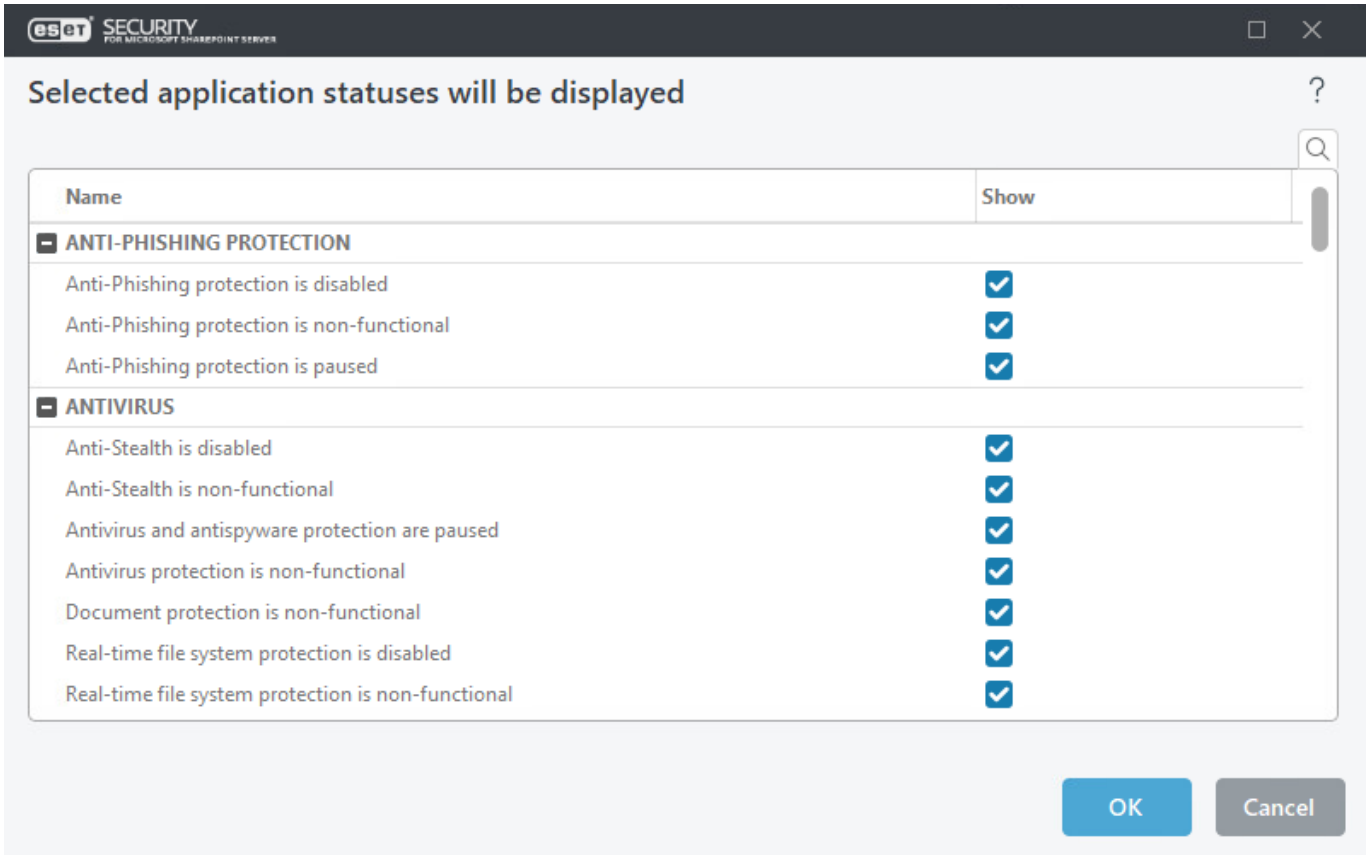
Desktop notifications – Small pop-up windows next to the system taskbar.

Interactive alerts – Alert windows and message boxes that require user interaction.

Forwarding (email notifications) – Notifications are sent to a specified email address.

# Application statuses

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 on the Monitoring page. 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 PROTECT policies.




# Disabled messages and statuses

Confirmation messages

It shows you a list of confirmation messages you can select to display or not to display.

Application statuses

Enable or disable display status in the Monitoring page in the main menu.

# Desktop notifications

Desktop notification is represented by a small notification window next to the system taskbar. It is default set to show for 10 seconds, then it slowly disappears. ESET Security for Microsoft SharePoint communicates with the user by notifying them about successful product updates, new devices connected, virus scans, task completion or new detections found.

**Display desktop notifications**

We recommend keeping this option enabled so the product can inform you when a new event occurs.

**Desktop notifications**

Click **Edit** to select what Desktop notifications to communicate various events.

Turn the **Do not display notifications when running applications in full screen mode** switch on to suppress all non-interactive notifications.

**Display time in seconds**

Set the notification visibility duration. The value must be between 3-30 seconds.

**Transparency**

Set the notification transparency percentage. The supported range is 0 (no transparency) to 80 (very high transparency).

**Minimum verbosity of events to display** 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.

**Allow notifications to take screen focus** - Notifications will take screen focus and be accessible by Alt+Tab.

# Customization

In this window, you can customize the messaging used in notifications.

**Notification message** - A default message to be shown in the notification footer.

## Detection

**Do not close detection notifications automatically**

Enables detection notifications to stay on screen until you close them manually.

**Use default message**

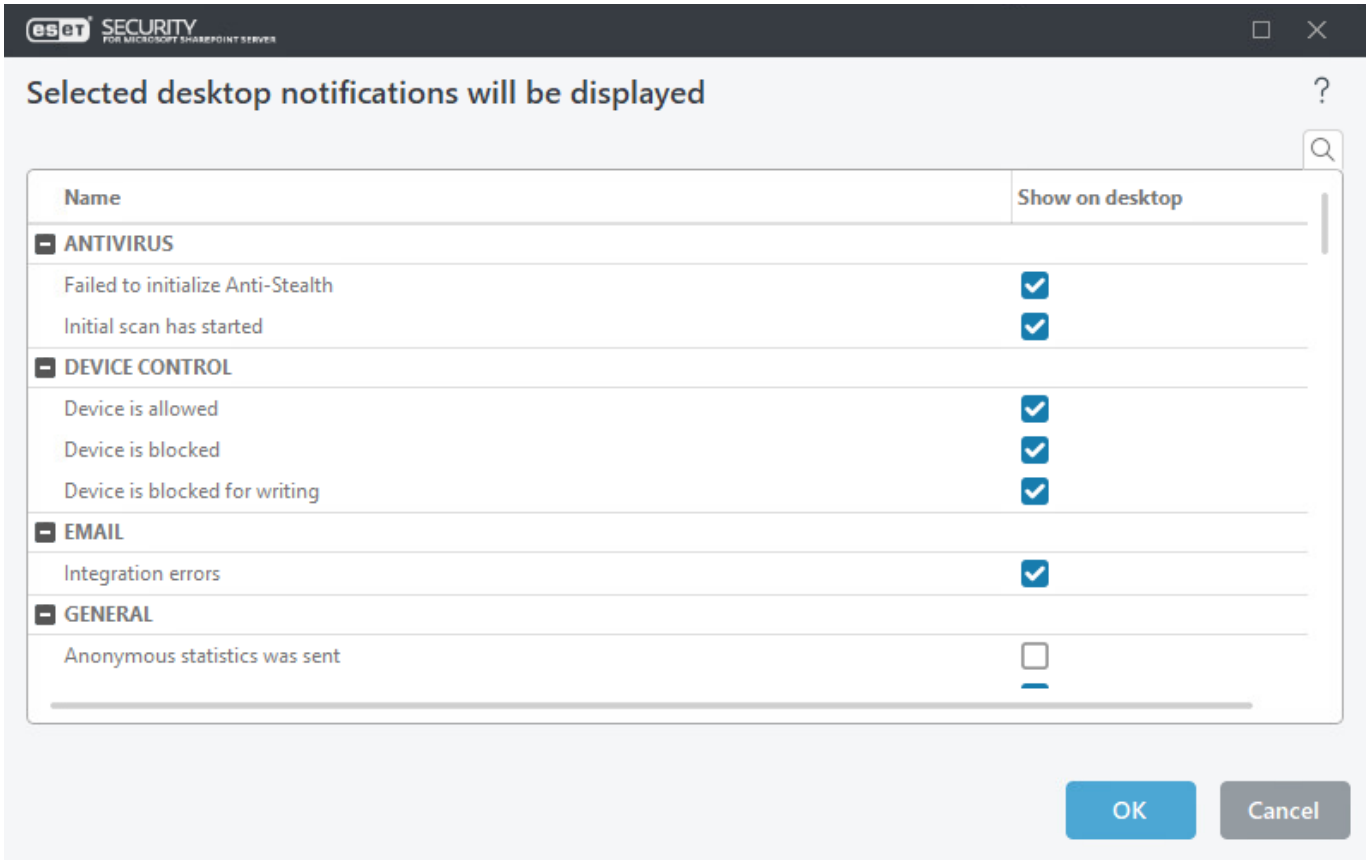
You can turn off default message and specify custom detection notification message that will be displayed when a detection is blocked.

**Detection notification message**

Type a custom message to display when a detection is blocked.

# Desktop notifications

You can configure ESET Security for Microsoft SharePoint notifications to be shown on desktop.




# Interactive alerts

You can configure how threat alerts and system notifications (such as successful update messages) are handled by ESET Security for Microsoft SharePoint. For example, the display time **Duration** and **Transparency** in the Windows notification area (this applies only to the systems that support notifications).

**Display interactive alerts**

Disable this feature, if you want to prevent ESET Security for Microsoft SharePoint 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 notification 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 window will open with a list of confirmation messages that ESET Security for Microsoft SharePoint displays before an action is performed. Use the check boxes to customize your preferences for confirmation messages.

# Forwarding

ESET Security for Microsoft SharePoint can automatically send notification emails if an event with the selected verbosity level occurs.

**Forward to email**

Enable Forward notifications to email to activate email notifications.

**Forwarded notifications**

Select which desktop notifications are forwarded to email.

## Email settings

**Minimum verbosity for notifications** - Specifies the minimum verbosity level of notifications to be sent.

- **Diagnostic**—Logs information needed to fine-tune the program and all records above.
- **Informative**—Records informative messages such as non-standard network events, including successful update messages, plus all records above.
- **Warnings**—Records critical errors and warning messages (Anti-Stealth is not running properly or update failed).
- **Errors**—Errors such as "Error downloading file" and critical errors will be recorded.
- **Critical**—Logs only critical errors.

**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.

**Interval after which new notification emails will be sent (min)**

After the interval in minutes, a new notification will be sent via email. Set this value to 0 if you want to send those notifications immediately.

**Sender address**

Type the 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 the recipient's email address that will be displayed in the header of notification emails. Use a semi-colon ";" to separate multiple email addresses.

## SMTP server

The name of the SMTP server used for sending alerts and notifications. This is typically the name of your Microsoft Exchange Server.

SMTP servers with TLS encryption are supported by ESET Security for Microsoft SharePoint.

**Username and password**

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

**Enable TLS**

Enable alert and notification messages supported by TLS encryption.

**Test SMTP connection**

A test email will be sent to the recipient's email address.

## 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 alert messages and notification format will be optimal for most situations. In some circumstances, you may need to change the message format of event messages.

**Format of event messages**

Specify format of the email event notification messages.

**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.
- %DetectionObject%—Name of infected file, message, etc.

- %DetectionName%—Identification of the infection.
- %ErrorDescription%—Description of a non-virus event.

The keywords **%DetectionObject%** and **%DetectionName%** 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. Converts an email message to the ANSI character encoding based on Windows Regional settings (for example, windows-1250, Unicode (UTF-8), ACSII 7-bit, or Japanese (ISO-2022-JP)). As the result, "á" will be changed to "a" and an unknown symbol to "?".

**Use Quoted-printable encoding**

The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

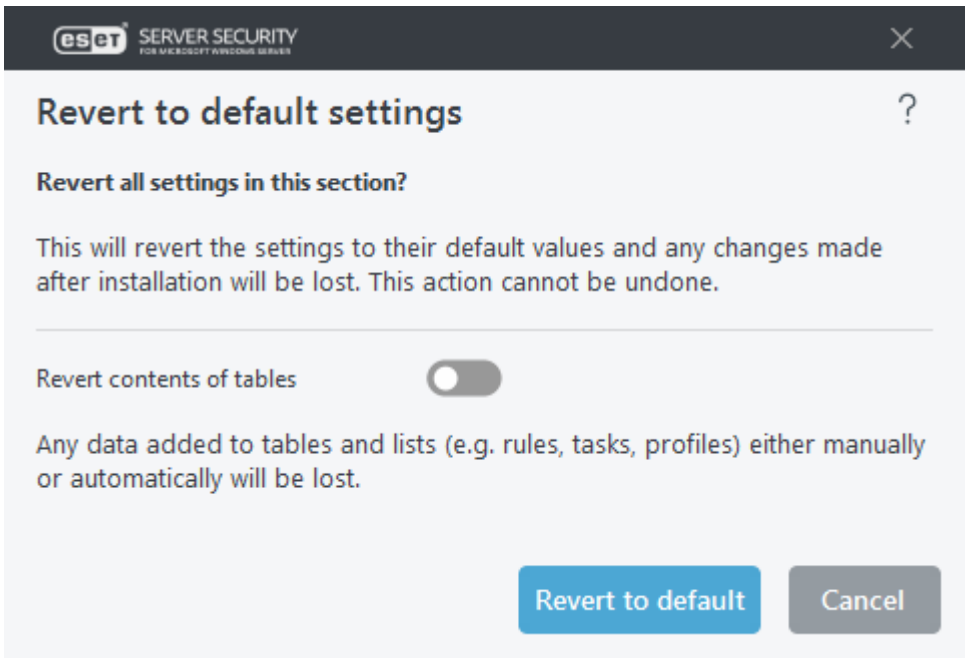
# Revert to default settings

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 specific 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 Security for Microsoft SharePoint. You can think of it as Restore Factory Defaults.

> After 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 default values. Any changes you have made in this section will be lost.



**Revert contents of tables** - When enabled, the rules, tasks or profiles added manually or automatically will be lost.

# Help and support

ESET Security for Microsoft SharePoint contains troubleshooting tools and support information that will assist you in solving issues that you may encounter.

**Installed product**

Product and License information

- About ESET Security for Microsoft SharePoint – Displays information about your copy of ESET Security for Microsoft SharePoint.
- Product troubleshooting – To find solutions to the most frequently encountered problems. We recommend that you read this section before contacting technical support.
- License troubleshooting – To find solutions for problems with activation or license change.
- Change license – Click to launch the activation window and activate your product.

**Help pages**

Launches online help pages for ESET Security for Microsoft SharePoint.

**Knowledgebase**

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

Technical Support

- Advanced logging – To create advanced logs for all available features to help developers diagnose and solve issues.
- Request support – If you cannot find an answer to your problem, contact our Technical Support department.
- Details for Technical Support – Display details information (Product name, Product version,etc.) for Technical Support.
- ESET Log Collector – ESET Log Collector is an application that automatically collects information, such as configuration and logs from your server to help resolve issues more quickly.

# Submit support request

To assist as quickly and accurately as possible, ESET requires information about your ESET Security for Microsoft SharePoint 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**.

> 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 want to submit data. You will be redirected to ESET Technical Support web page.

# About ESET Security for Microsoft SharePoint

This window provides details about the installed version of ESET Security for Microsoft SharePoint. 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

Effective as of October 19, 2021.

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

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of

Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software.** The Provider shall be entitled from time to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

b) **Forwarding of infiltrations and information to the Provider.** The Software contains functions which collect samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames ("Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed and, information about the operations and functionality of the Software ("Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations

to Provider. This function is enabled under the Software's standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

**Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.**

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of

other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement.** This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other

than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software.** The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws

which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET's right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes,

Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

EULAID: EULA-PRODUCT-LG; 3537.0

# Privacy Policy

The protection of personal data is of particular importance to ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We"). We want to comply with the transparency requirement as legally standardized under the EU General Data Protection Regulation ("GDPR"). To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") as a data subject about following personal data protection topics:

- Legal Basis of Personal Data Processing,
- Data Sharing and Confidentiality,
- Data Security,
- Your Rights as a Data Subject,
- Processing of Your Personal Data
- Contact Information.

## Processing of Your Personal Data

Services provided by ESET implemented in our product are provided under the terms of EULA, but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and the product documentation. To make it all work, We need to collect the following information:

- 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 Sharing and Confidentiality

We do not share your data with third parties. However, ESET is a company that operates globally through affiliated companies or partners as part of our sales, service and support network. Licensing, billing and technical support information processed by ESET may be transferred to and from affiliates or partners for the purpose of fulfilling the EULA, such as providing services or support.

ESET prefers to process its data in the European Union (EU). However, depending on your location (use of our products and/or services outside the EU) and/or the service you choose, it may be necessary to transfer your data to a country outside the EU. For example, we use third-party services in connection with cloud computing. In these cases, we carefully select our service providers and ensure an appropriate level of data protection through contractual as well as technical and organizational measures. As a rule, we agree on the EU standard contractual clauses, if necessary, with supplementary contractual regulations.

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these countries does not require any special authorization or agreement.

## Data Subject’s Rights

The rights of every End User matter and We would like to inform you that all End Users (from any EU or any non-EU country) have the following rights guaranteed at ESET. To exercise your data subject’s rights, you can contact us via support form or by e-mail at dpo@eset.sk. For identification purposes, we ask you for the following information: Name, e-mail address and - if available - license key or customer number and company affiliation. Please refrain from sending us any other personal data, such as the date of birth. We would like to point out that to be able to process your request, as well as for identification purposes, we will process your personal data.

**Right to Withdraw the Consent.** Right to withdraw the consent is applicable in case of processing based on consent only. If We process your personal data on the basis of your consent, you have the right to withdraw the consent at any time without giving reasons. The withdrawal of your consent is only effective for the future and does not affect the legality of the data processed before the withdrawal.

**Right to Object.** Right to object the processing is applicable in case of processing based on the legitimate interest of ESET or third party. If We process your personal data to protect a legitimate interest, You as the data subject have the right to object to the legitimate interest named by us and the processing of your personal data at any

time. Your objection is only effective for the future and does not affect the lawfulness of the data processed before the objection. If we process your personal data for direct marketing purposes, it is not necessary to give reasons for your objection. This also applies to profiling, insofar as it is connected with such direct marketing. In all other cases, we ask you to briefly inform us about your complaints against the legitimate interest of ESET to process your personal data.

Please note that in some cases, despite your consent withdrawal or your objection processing, we are entitled to further process your personal data on the basis of another legal basis, for example, for the performance of a contract.

**Right of Access.** As a data subject, you have the right to obtain information about your data stored by ESET free of charge at any time.

**Right to Rectification.** If we inadvertently process incorrect personal data about you, you have the right to have this corrected.

**Right to Erasure.** As a data subject, you have the right to request the deletion or restriction of the processing of your personal data. If we process your personal data, for example, with your consent, you withdraw it and there is no other legal basis, for example, a contract, We delete your personal data immediately. Your personal data will also be deleted as soon as they are no longer required for the purposes stated for them at the end of our retention period.

**Right to Restriction of Processing.** If we use your personal data for the sole purpose of direct marketing and you have revoked your consent or objected to the underlying legitimate interest of ESET, We will restrict the processing of your personal data to the extent that we include your contact data in our internal black list in order to avoid unsolicited contact. Otherwise, your personal data will be deleted.

Please note that We may be required to store your data until the expiry of the retention obligations and periods issued by the legislator or supervisory authorities. Retention obligations and periods may also result from the Slovak legislation. Thereafter, the corresponding data will be routinely deleted.

**Right to Data Portability.** We are happy to provide You, as a data subject, with the personal data processed by ESET in the xls format.

**Right to Lodge a Complaint.** As a data subject, You have a right to lodge a complaint with a supervisory authority at any time. ESET is subject to the regulation of Slovak laws and We are bound by data protection legislation as part of the European Union. The relevant data supervisory authority is The Office for Personal Data Protection of the Slovak Republic, located at Hraničná 12, 82007 Bratislava 27, Slovak Republic.

# Contact Information

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk