# ESET SECURITY

## FOR MICROSOFT SHAREPOINT SERVER

## Installation Manual and User Guide

Microsoft® Windows® Server 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016

Click here to display Online help version of this document

ENJOY SAFER TECHNOLOGY™

ESET **SECURITY**

Customer Care: www.eset.com/support

REV. 2/27/2017

# Contents

1. Introduction ....................6
1.1 What's new ....................7
1.2 Help pages ....................7
2. System requirements ....................9
3. Types of SharePoint protection ....................10
3.1 Integration into the SharePoint ....................10
3.1.1 On-access filter ....................11
3.1.2 On-demand database scan ....................11
4. User interface ....................13
5. Managed via ESET Remote Administrator ....................15
5.1 Override mode ....................16
6. Deployment ....................20
6.1 SharePoint Farm deployment ....................20
6.2 Installation in a cluster environment ....................21
6.3 Installation ....................21
6.3.1 ESET Security for Microsoft SharePoint installation steps ....................22
6.3.1.1 Command line installation ....................25
6.3.2 Post installation steps ....................27
6.3.3 Terminal server ....................28
6.3.4 ESET AV Remover ....................28
6.3.5 Upgrading to a newer version ....................29
6.3.5.1 Upgrading via ERA ....................29
6.3.5.2 Upgrading via ESET Cluster ....................32
7. Beginner's guide ....................35
7.1 Monitoring ....................35
7.1.1 Status ....................38
7.2 Log files ....................39
7.2.1 Scan log ....................41
7.3 Scan ....................42
7.3.1 Hyper-V scan ....................43
7.4 Update ....................45
7.4.1 Setting up virus DB update ....................47
7.4.2 Configuring Proxy server for updates ....................50
7.5 Setup ....................51
7.5.1 Server ....................52
7.5.2 Computer ....................53
7.5.3 Tools ....................54
7.5.4 Import and export settings ....................55
7.6 Tools ....................56
7.6.1 Running processes ....................57
7.6.2 Watch activity ....................59
7.6.2.1 Time period selection ....................59
7.6.3 Protection statistics ....................60
7.6.4 Cluster ....................61
7.6.4.1 Cluster wizard - page1 ....................63
7.6.4.2 Cluster wizard - page2 ....................64
7.6.4.3 Cluster wizard - page3 ....................65
7.6.4.4 Cluster wizard - page4 ....................67
7.6.5 ESET Shell ....................70
7.6.5.1 Usage ....................72
7.6.5.2 Commands ....................76
7.6.5.3 Batch files / Scripting ....................78
7.6.6 ESET SysInspector ....................79
7.6.6.1 Create a computer status snapshot ....................79
7.6.6.2 ESET SysInspector ....................79
7.6.6.2.1 Introduction to ESET SysInspector ....................79
7.6.6.2.1.1 Starting ESET SysInspector ....................80
7.6.6.2.2 User Interface and application usage ....................80
7.6.6.2.2.1 Program Controls ....................80
7.6.6.2.2.2 Navigating in ESET SysInspector ....................82
7.6.6.2.2.1 Keyboard shortcuts ....................83
7.6.6.2.2.3 Compare ....................84
7.6.6.2.3 Command line parameters ....................85
7.6.6.2.4 Service Script ....................86
7.6.6.2.4.1 Generating Service script ....................86
7.6.6.2.4.2 Structure of the Service script ....................86
7.6.6.2.4.3 Executing Service scripts ....................89
7.6.6.2.5 FAQ ....................89
7.6.7 ESET SysRescue Live ....................90
7.6.8 Scheduler ....................91
7.6.8.1 Scheduler - Add new task ....................92
7.6.9 Submit samples for analysis ....................92
7.6.9.1 Suspicious file ....................93
7.6.9.2 Suspicious site ....................93
7.6.9.3 False positive file ....................94
7.6.9.4 False positive site ....................94
7.6.9.5 Other ....................94
7.6.10 Quarantine ....................95
7.7 Help and support ....................96
7.7.1 How to ....................97
7.7.1.1 How to update ESET Security for Microsoft SharePoint ....................97
7.7.1.2 How to activate ESET Security for Microsoft SharePoint ....................97
7.7.1.3 How to create a new task in Scheduler ....................98
7.7.1.4 How to schedule a scan task (every 24 hours) ....................99
7.7.1.5 How to remove a virus from your server ....................99
7.7.2 Submit support request ....................99
7.7.3 ESET Specialized Cleaner ....................100
7.7.4 About ESET Security for Microsoft SharePoint ....................100
7.7.5 Product activation ....................101
7.7.5.1 Registration ....................102
7.7.5.2 Security Admin activation ....................102
7.7.5.3 Activation failure ....................102
7.7.5.4 License ....................102
7.7.5.5 Activation progress ....................102
7.7.5.6 Activation successful ....................102

8. Working with ESET Security for Microsoft SharePoint....................................103

8.1 Server....................................104
- 8.1.1 On-access filter....................................105
- 8.1.1.1 Antivirus and antispyware....................................105
- 8.1.2 On-demand database scan....................................106
- 8.1.2.1 On-demand database scan targets....................................107
- 8.1.2.1.1 Antivirus and antispyware....................................108
- 8.1.3 Rules....................................108
- 8.1.3.1 Rules list....................................108
- 8.1.3.1.1 Rule wizard....................................109
- 8.1.3.1.1.1 Rule condition....................................110
- 8.1.3.1.1.2 Rule action....................................111

8.2 Computer....................................112
- 8.2.1 An infiltration is detected....................................112
- 8.2.2 Processes exclusions....................................113
- 8.2.3 Automatic exclusions....................................114
- 8.2.4 Shared local cache....................................114
- 8.2.5 Real-time file system protection....................................115
- 8.2.5.1 Exclusions....................................116
- 8.2.5.1.1 Add or Edit exclusion....................................118
- 8.2.5.1.2 Exclusion format....................................118
- 8.2.5.2 ThreatSense parameters....................................118
- 8.2.5.2.1 File extenstions excluded from scanning....................................121
- 8.2.5.2.2 Additional ThreatSense parameters....................................121
- 8.2.5.2.3 Cleaning levels....................................122
- 8.2.5.2.4 When to modify real-time protection configuration....................................122
- 8.2.5.2.5 Checking real-time protection....................................122
- 8.2.5.2.6 What to do if real-time protection does not work....................................122
- 8.2.5.2.7 Submission....................................123
- 8.2.5.2.8 Statistics....................................123
- 8.2.5.2.9 Suspicious files....................................123
- 8.2.6 On-demand computer scan and Hyper-V scan....................................124
- 8.2.6.1 Custom scan and Hyper-V scan launcher....................................124
- 8.2.6.2 Scan progress....................................126
- 8.2.6.3 Profile manager....................................127
- 8.2.6.4 Scan targets....................................128
- 8.2.6.5 Advanced scan option....................................128
- 8.2.6.6 Pause a scheduled scan....................................128
- 8.2.7 Idle-state scanning....................................129
- 8.2.8 Startup scan....................................129
- 8.2.8.1 Automatic startup file check....................................129
- 8.2.9 Removable media....................................130
- 8.2.10 Document protection....................................130
- 8.2.11 HIPS....................................130
- 8.2.11.1 HIPS rules....................................132
- 8.2.11.1.1 HIPS rule settings....................................133
- 8.2.11.2 Advanced setup....................................135
- 8.2.11.2.1 Drivers always allowed to load....................................135

8.3 Update....................................135
- 8.3.1 Update rollback....................................138
- 8.3.2 Update mode....................................138
- 8.3.3 HTTP Proxy....................................140
- 8.3.4 Connect to LAN as....................................141
- 8.3.5 Mirror....................................142
- 8.3.5.1 Updating from the Mirror....................................143
- 8.3.5.2 Mirror files....................................145
- 8.3.5.3 Troubleshooting Mirror update problems....................................145

8.4 Web and email....................................146
- 8.4.1 Protocol filtering....................................146
- 8.4.1.1 Excluded applications....................................146
- 8.4.1.2 Excluded IP addresses....................................147
- 8.4.1.3 Web and email clients....................................147
- 8.4.2 SSL/TLS....................................147
- 8.4.2.1 Encrypted SSL communication....................................149
- 8.4.2.2 List of known certificates....................................149
- 8.4.3 Email client protection....................................150
- 8.4.3.1 Email protocols....................................151
- 8.4.3.2 Alerts and notifications....................................151
- 8.4.3.3 MS Outlook toolbar....................................152
- 8.4.3.4 Outlook Express and Windows Mail toolbar....................................152
- 8.4.3.5 Confirmation dialog....................................153
- 8.4.3.6 Rescan messages....................................153
- 8.4.4 Web access protection....................................153
- 8.4.4.1 Basic....................................154
- 8.4.4.2 URL address management....................................154
- 8.4.4.2.1 Create new list....................................154
- 8.4.4.2.2 Address list....................................156
- 8.4.5 Anti-Phishing protection....................................157

8.5 Device control....................................158
- 8.5.1 Device control rules editor....................................159
- 8.5.2 Adding Device control rules....................................160
- 8.5.3 Detected devices....................................161
- 8.5.4 Device groups....................................161

8.6 Tools....................................162
- 8.6.1 ESET LiveGrid....................................162
- 8.6.1.1 Exclusion filter....................................163
- 8.6.2 Microsoft Windows update....................................164
- 8.6.3 ESET CMD....................................164
- 8.6.4 WMI Provider....................................165
- 8.6.4.1 Provided data....................................166
- 8.6.4.2 Accessing Provided Data....................................169
- 8.6.5 ERA scan targets....................................170
- 8.6.6 Log files....................................171
- 8.6.6.1 Log filtering....................................174
- 8.6.6.2 Find in log....................................174
- 8.6.7 Proxy server....................................175
- 8.6.8 Email notifications....................................176
- 8.6.8.1 Message format....................................177
- 8.6.9 Presentation mode....................................177
- 8.6.10 Diagnostics....................................178
- 8.6.11 Customer Care....................................178
- 8.6.12 Cluster....................................179

# Contents

**8.7 User interface....180**
8.7.1 Alerts and notifications....181
8.7.2 Access setup....183
8.7.2.1 Settings protection....184
8.7.2.2 Password....185
8.7.2.3 Password setup....185
8.7.3 Help....185
8.7.4 ESET Shell....185
8.7.5 Disable GUI on Terminal Server....185
8.7.6 Disabled messages and statuses....186
8.7.6.1 Confirmation messages....186
8.7.6.2 Application statuses settings....186
8.7.7 System tray icon....187
8.7.7.1 Pause protection....188
8.7.8 Context menu....188
**8.8 Revert all settings in this section....189**
**8.9 Revert to default settings....189**
**8.10 Scheduler....189**
8.10.1 Task details....190
8.10.2 Task timing - Once....191
8.10.3 Task timing....191
8.10.4 Task timing - Daily....191
8.10.5 Task timing - Weekly....191
8.10.6 Task timing - Event triggered....191
8.10.7 Task details - Run application....192
8.10.8 Skipped task....192
8.10.9 Scheduled task overview....192
8.10.10 Update profiles....193
**8.11 Quarantine....193**
8.11.1 Quarantining files....193
8.11.2 Restoring from Quarantine....193
8.11.3 Submitting file from Quarantine....194
**8.12 Operating system updates....194**
**9. Glossary....195**
**9.1 Types of infiltration....195**
9.1.1 Viruses....195
9.1.2 Worms....196
9.1.3 Trojan horses....196
9.1.4 Rootkits....196
9.1.5 Adware....197
9.1.6 Spyware....197
9.1.7 Packers....197
9.1.8 Exploit Blocker....197
9.1.9 Advanced Memory Scanner....198
9.1.10 Potentially unsafe applications....198
9.1.11 Potentially unwanted applications....198

# 1. Introduction

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

ESET Security for Microsoft SharePoint protects your content:

- by filtering during file access (On-access filter)
- using 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 generation of SharePoint being used (2010 vs. 2007). In general, on-access filter is run when any file is first accessed and the result of the scan is cached until the version of the virus database has changed or some time elapses.

On-demand scan hierarchically crawls all the files and directories of a web site that are selected by the administrator. 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 on-access filter and on-demand scan apply following checks:

- Antivirus and antispyware protection
- User-defined rules with different types of conditions

Some key features of ESET Security for Microsoft SharePoint:

- 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.

- Storage scan - scans all shared files on a local server. This makes it easy to selectively scan only user data that are stored on the file server.

- Automatic Exclusions – automatic detection and exclusion of critical applications and server files for smooth operation and performance.

- 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.

- eShell (ESET Shell) - a command line control interface that offers advanced users and administrators more comprehensive options to manage ESET server products. eShell comes in new and improved version 2.0.

- ESET WMI Provider - gives administrators the option to remotely monitor ESET products in their enterprise environment by using any WMI compliant application or tool. There is a vast selection of such tools, for example PowerShell scripts, VB scripts or third-party enterprise monitoring applications such as SCOM, Nagios, etc.

ESET Security for Microsoft SharePoint supports most editions of Microsoft Windows Server 2003, 2008 and 2012 in standalone and clustered environments. You can remotely manage ESET Security for Microsoft SharePoint in larger networks with the help of ESET Remote Administrator.

## 1.1 What's new

Integration of the following features:

- Significant speedup of On-demand database scan by implementing parallel download and file scanning
- Clustering support
- Exclusions for processes (better compatibility with 3rd party software)
- GUI enhancements
- Rules - updated rules engine
- Anti-Phishing protection
- Optimization for virtualized environments
- 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 particular VM.

## 1.2 Help pages

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

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

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

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

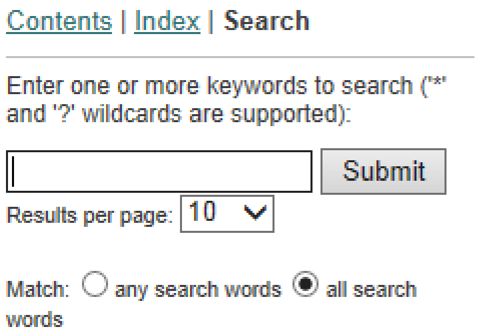
WARNING
Critical information you should treat with increased caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Please read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.

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

| Convention | Meaning |
|---|---|
| **Bold type** | Names of interface items such as boxes and option buttons. |
| *Italic type* | Placeholders for the information that you provide. For example, *file name* or *path* means you type the actual path or a name of file. |
| `Courier New` | Code samples or commands. |
| Hyperlink | Provides quick and easy access to cross-referenced topics or external web locations. Hyperlinks are highlighted in blue and may be underlined. |

| | |
|---|---|
| *%ProgramFiles%* | The Windows system directory which stores installed programs of Windows and others. |

- Topics in this guide are divided into several chapters and sub-chapters. You can find relevant information by browsing the **Contents** of the help pages. Alternatively, you can use the **Index** to browse by keywords or use full-text **Search**.



Contents | Index | **Search**

Enter one or more keywords to search ("*" and '?' wildcards are supported):

Submit

Results per page: 10

Match: ○ any search words ● all search words

ESET Security for Microsoft SharePoint allows you to search help topics by keyword or by typing words or phrases to search for within the User Guide. The difference between these two methods is that a keyword may be logically related to help pages which do not contain that particular keyword in the text. Searching by words and phrases will search the content of all pages and display only those containing the searched word or phrase in the actual text.

- You can post your rating and/or provide feedback on a particular topic in help, click the **Was this information helpful?** link or **Rate this article: Helpful** / **Not Helpful** in case of ESET Knowledgebase, underneath the help page.

# 2. System requirements

Supported Operating Systems:

- Microsoft Windows Server 2003 (x86) SP1 SP2
- Microsoft Windows Server 2003 R2 (x86) SP1 SP2
- Microsoft Windows Server 2008 (x64) SP2
- Microsoft Windows Server 2008 R2 (x64) SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Small Business servers:

- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2016 Essentials

and any of the following application servers:

- Microsoft SharePoint Server 2007 (x86 and x64) - all editions
- Microsoft SharePoint Server 2010 (x64) - all editions
- Microsoft SharePoint Server 2013 (x64) - all editions
- Microsoft SharePoint Server 2016 (x64) - all editions

Supported Hyper-V Host Operating Systems:

- Microsoft Windows Server 2008 R2 - Virtual Machines can be scanned only while they are offline
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

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.

**NOTE**

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

# 3. Types of SharePoint protection

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

- Antivirus protection
- Antispyware protection

This protection is provided by:

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

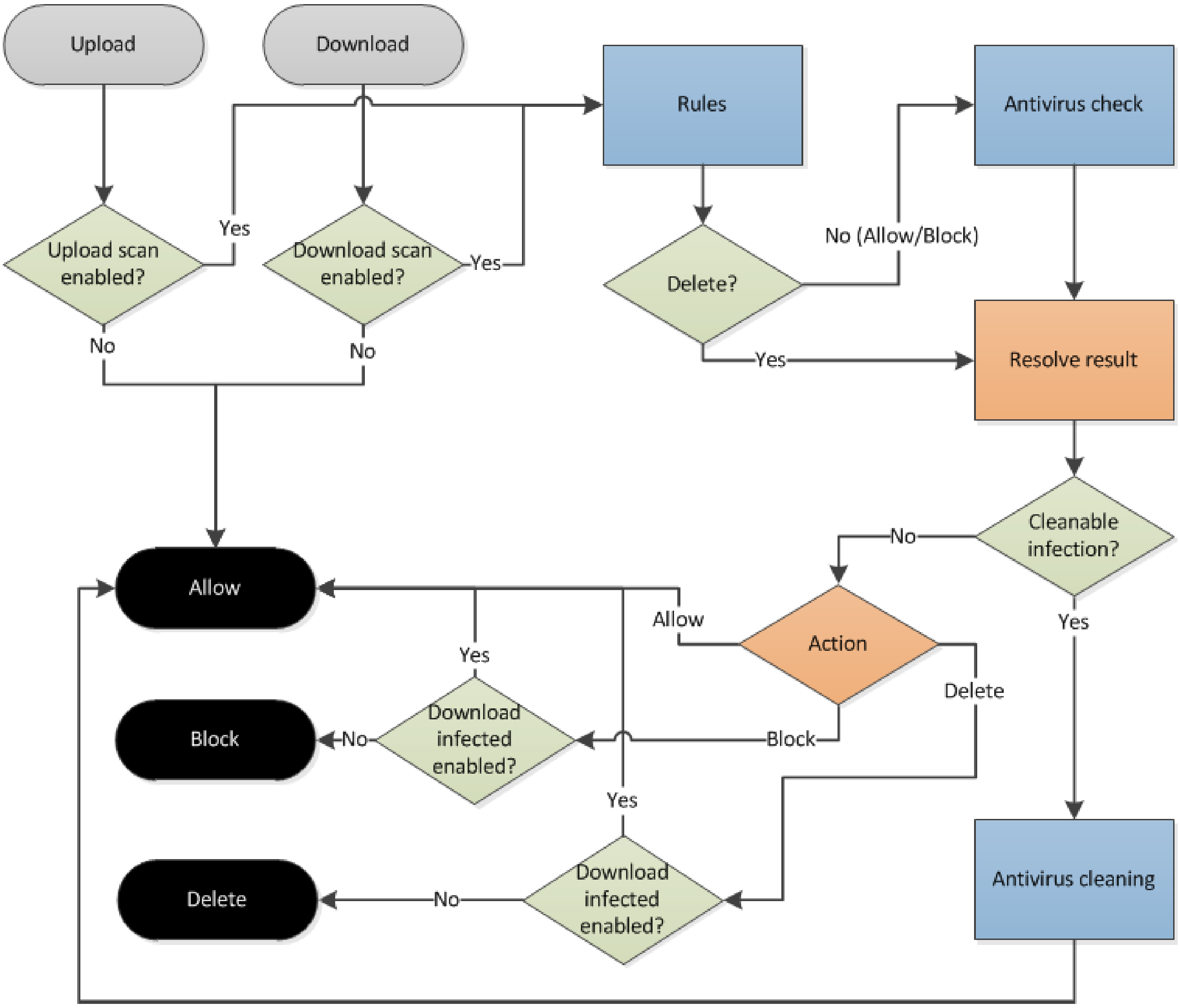
## 3.1 Integration into the SharePoint

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

### 3.1.1 On-access filter

The On-access filter scans all files according to ”SharePoint protection settings“. For example, an MS Office document stored in SharePoint, pictures, `.aspx` files (which are 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 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 file name 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 file name of the current version will be displayed, for older versions alternate text will be used.

The process of On-access filter file scan is shown in the diagram below. This diagram illustrates possible actions performed by the On-access filter file scan:



### 3.1.2 On-demand database scan

The On-demand database scan feature is used to scan the SharePoint content database that contains SharePoint Web sites and files. ESET Security will scan the hierarchy of files and folders that corresponds to each web site targeted for scanning.

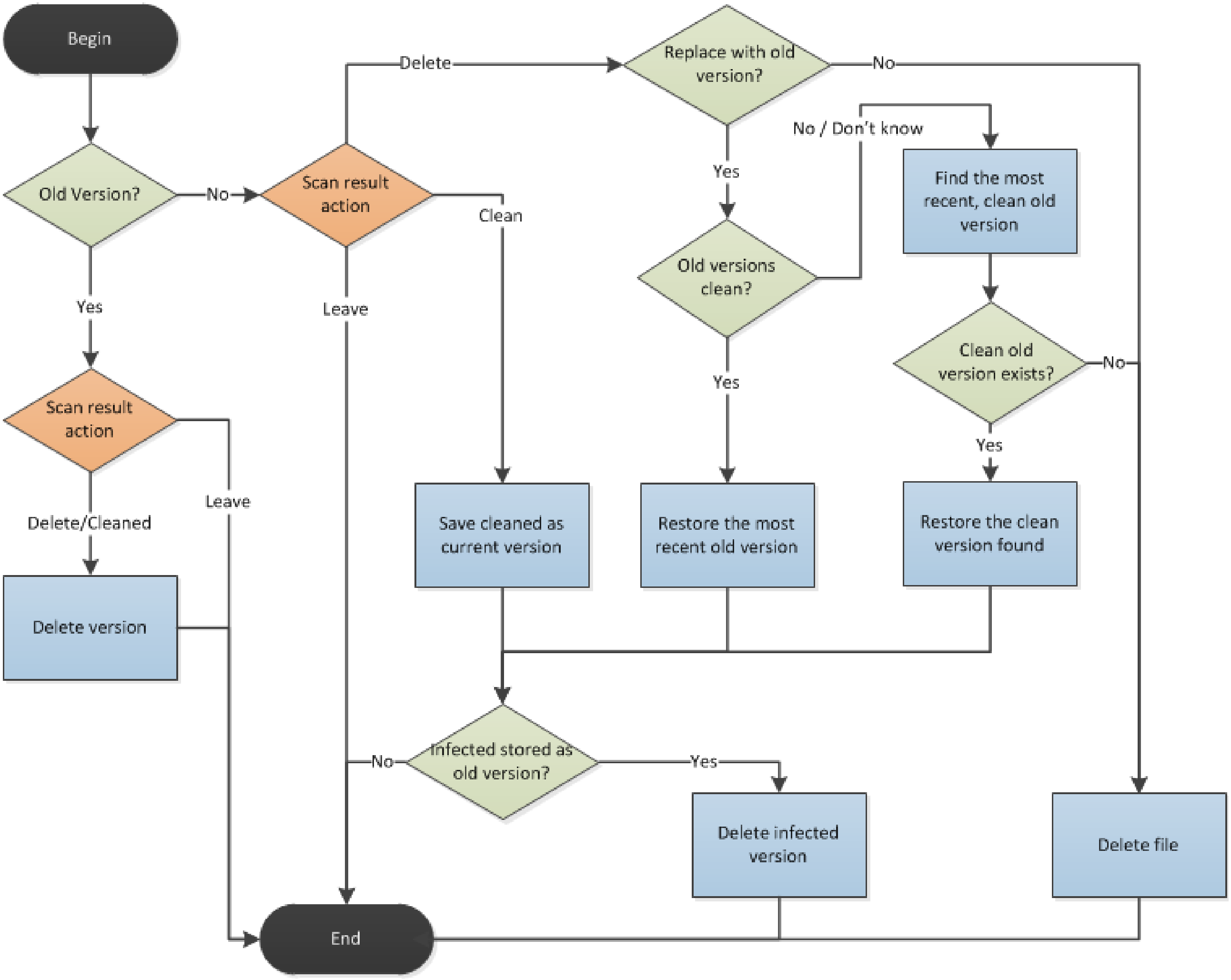
If an infiltration is found, there are three possible actions (retain, clean and delete) that can be performed. If deletion is executed for any reason, including during cleaning, the file is sent to the Recycle Bin. If the Recycle Bin is turned off deletion is definitive.

If older versions of a particular file are present and the **Scan document versions** feature is enabled, then the older versions of the document are scanned first.

Notes on document version scanning:

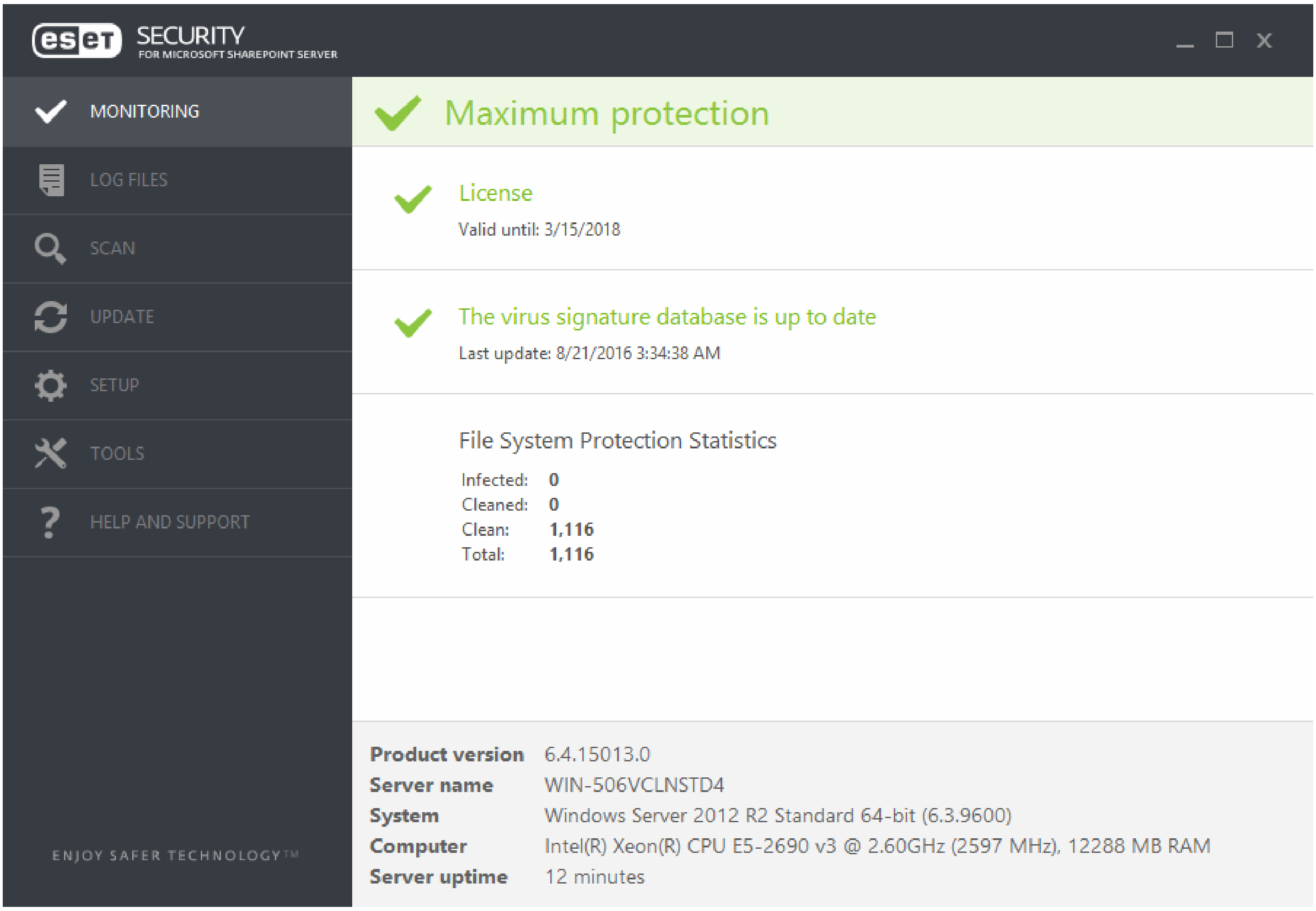
- Scanning of older document versions can be activated in ESET Security for Microsoft SharePoint settings (**Scan document versions**).
- If a document must be cleaned, a new version of the document will be created. The Infected version will be moved to trash.
- It is impossible to clean older versions of documents, they can only be deleted.
- If the most current version of a document is deleted, the older 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:


Begin
Old Version?
No
Yes
Scan result action
Delete/Cleaned
Leave
Delete version
Scan result action
Delete
Clean
Leave
Replace with old version?
No
Yes
No / Don't know
Old versions clean?
Yes
Find the most recent, clean old version
Clean old version exists?
No
Yes
Save cleaned as current version
Restore the most recent old version
Restore the clean version found
Infected stored as old version?
No
Yes
Delete infected version
Delete file
End

# 4. User interface

ESET Security for Microsoft SharePoint has a intuitive graphical user interface (GUI) that gives users easy access to main program functions. The main program window of ESET Security for Microsoft SharePoint is divided into two main sections. The primary window on the right displays the information that corresponds to the option selected from the main menu on the left.



Maximum protection

License
Valid until: 3/15/2018

The virus signature database is up to date
Last update: 8/21/2016 3:34:38 AM

File System Protection Statistics

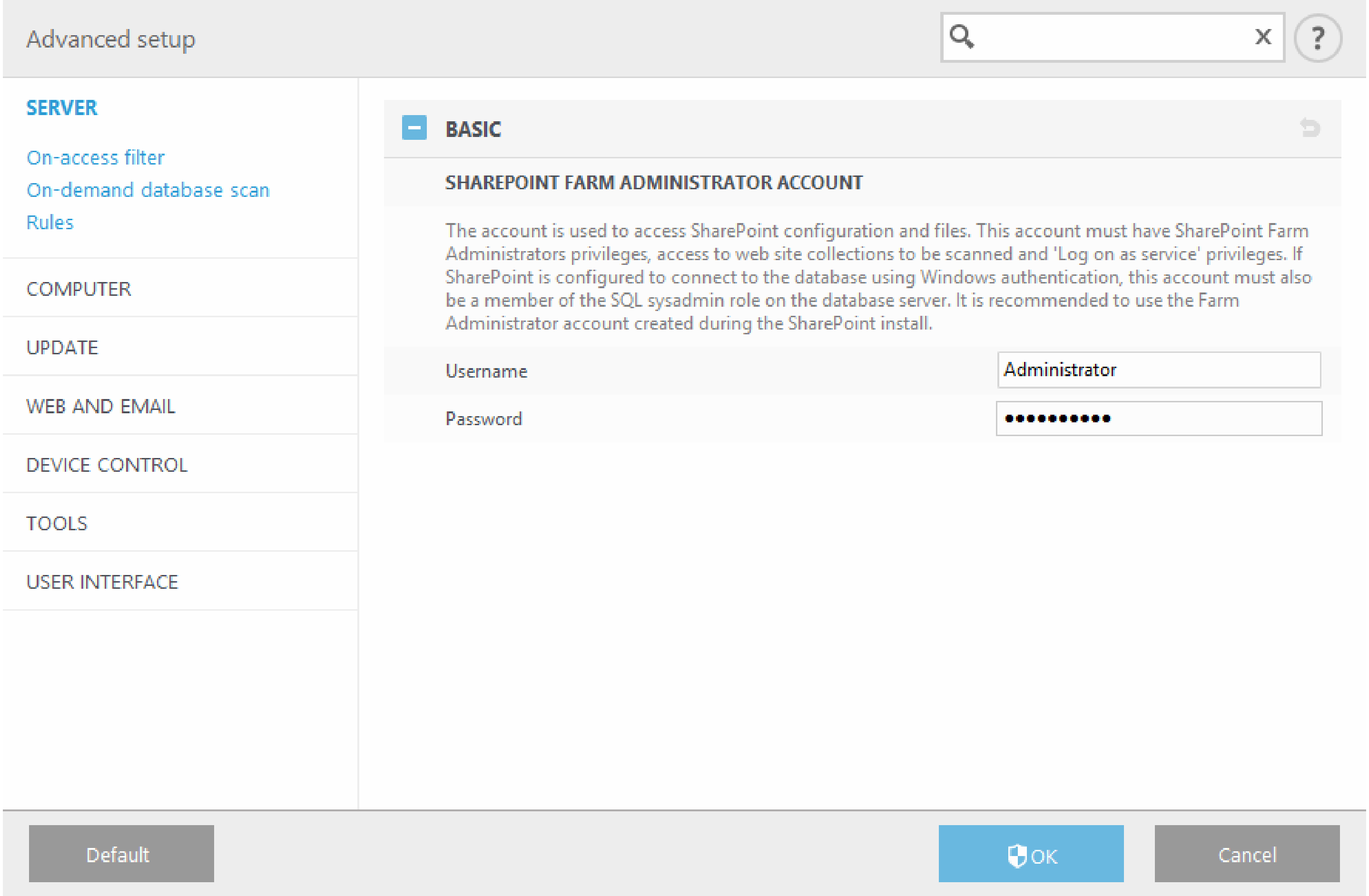
| | |
|---|---|
| Infected: | 0 |
| Cleaned: | 0 |
| Clean: | 1,116 |
| Total: | 1,116 |

| | |
|---|---|
| **Product version** | 6.4.15013.0 |
| **Server name** | WIN-506VCLNSTD4 |
| **System** | Windows Server 2012 R2 Standard 64-bit (6.3.9600) |
| **Computer** | Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz (2597 MHz), 12288 MB RAM |
| **Server uptime** | 12 minutes |

The different sections of the main menu are described below:

- Monitoring - Provides information about the protection status of ESET Security for Microsoft SharePoint, license validity, virus signature database updates, basic statistics and system information.
- Log files - Accesses log files that contain information about all important program events that have occurred. These files provide an overview of detected threats as well as other security related events.
- Scan - Allows you to configure and launch a Storage scan, Smart scan, Custom scan or Removable media scan. You can also repeat the last scan performed.
- Update - Provides information about the virus signature database and notifies you about available updates. Product activation can also be performed from this section.
- Setup - Adjust your server and computer security settings.
- Tools - Provides additional information about your system protection. Additional tools to help you manage your security. The Tools section contains the following items: Running processes, Watch activity, Protection statistics, Cluster, ESET Shell, ESET SysInspector, ESET SysRescue Live to create a rescue CD or USB and Scheduler. You can also Submit sample for analysis and check your Quarantine.
- Help and support - Provides access to help pages, the ESET Knowledgebase and other Support tools. Also available are links to open a Customer Care support request and information about product activation.

In addition to the main GUI, the **Advanced setup** window is accessible from anywhere in the program by pressing the **F5** key.



SHAREPOINT FARM ADMINISTRATOR ACCOUNT

The account is used to access SharePoint configuration and files. This account must have SharePoint Farm Administrators privileges, access to web site collections to be scanned 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. It is recommended to use the Farm Administrator account created during the SharePoint install.

Username: Administrator

Password: ••••••••••

From the **Advanced setup** window, you can configure settings and options based on your needs. The menu on the left includes the following categories:

- Server
- Computer
- Update
- Web and email
- Device control
- Tools
- User interface

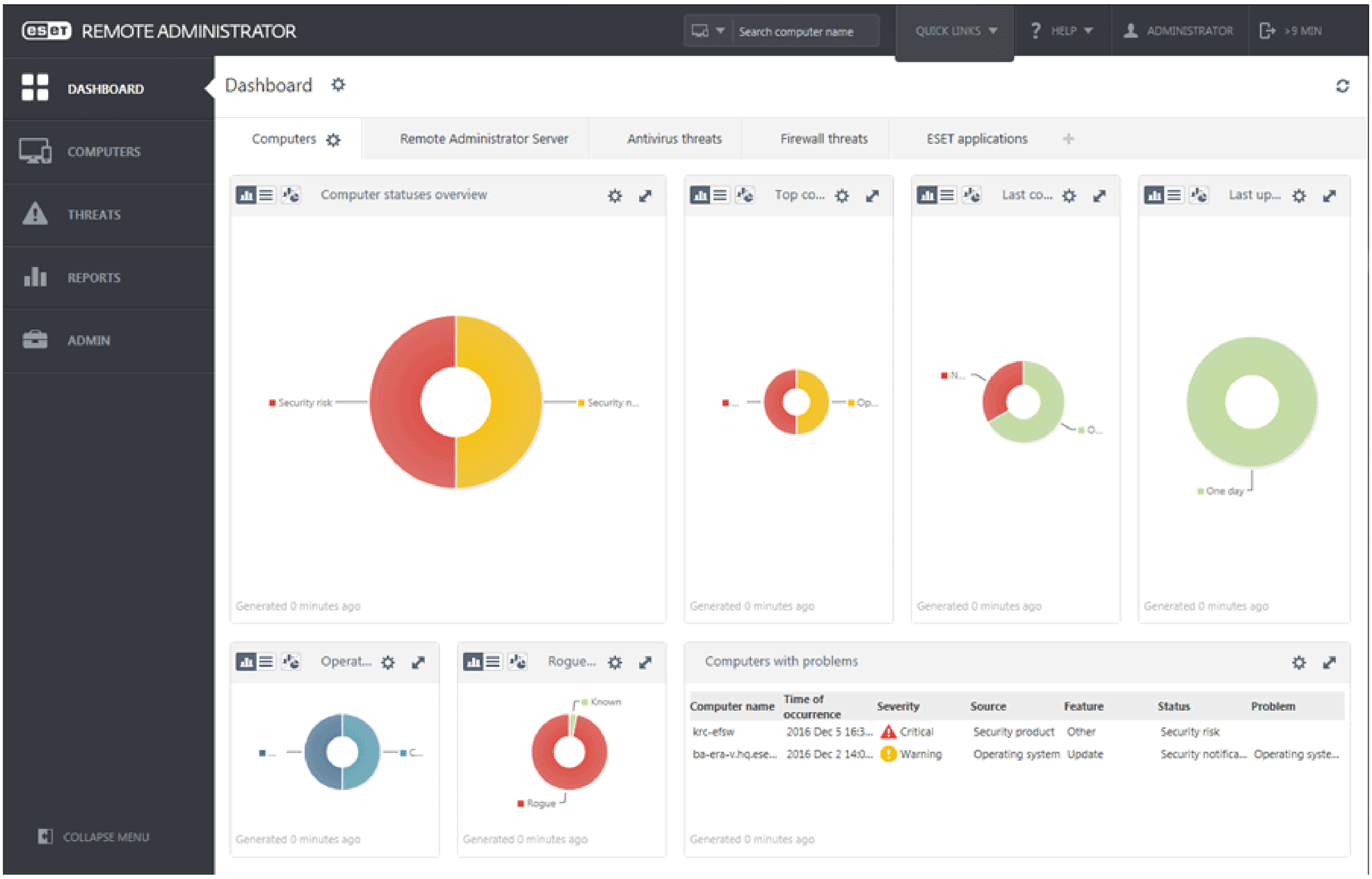
When you click an item (category or subcategory) in the menu on the left, the respective settings for that item are shown on the right pane.

# 5. Managed via ESET Remote Administrator

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

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

- ESET Remote Administrator Server - ERA Server can be installed on Windows as well as Linux servers and also comes as a Virtual Appliance. It handles communication with Agents, and collects and stores application data.
- ERA Web Console a web-based user interface that presents data from ERA Server and allows you to manage ESET security solutions in your environment. The Web Console can be accessed using a Web browser. It displays an overview of the status of clients on your network and can be used to deploy ESET solutions to unmanaged computers remotely. If you decide to make the web server accessible from the Internet, you can use ESET Remote Administrator from nearly any device with an active Internet connection.
- ERA Agent - The ESET Remote Administrator Agent facilitates communication between the ERA Server and client computers. You must install the Agent on any client computer to establish communication between that computer and the ERA Server. Because it is located on the client computer and can store multiple security scenarios, use of the ERA Agent significantly lowers reaction time to new threats. Using ERA Web Console, you can deploy the ERA Agent to unmanaged computers that have been recognized via your Active Directory or ESET RD Sensor.



Computers with problems

| Computer name | Time of occurrence | Severity | Source | Feature | Status | Problem |
|---|---|---|---|---|---|---|
| krc-efsw | 2016 Dec 5 16:3... | Critical | Security product | Other | Security risk | |
| ba-era-v.hq.ese... | 2016 Dec 2 14:0... | Warning | Operating system | Update | Security notifica... | Operating syste... |

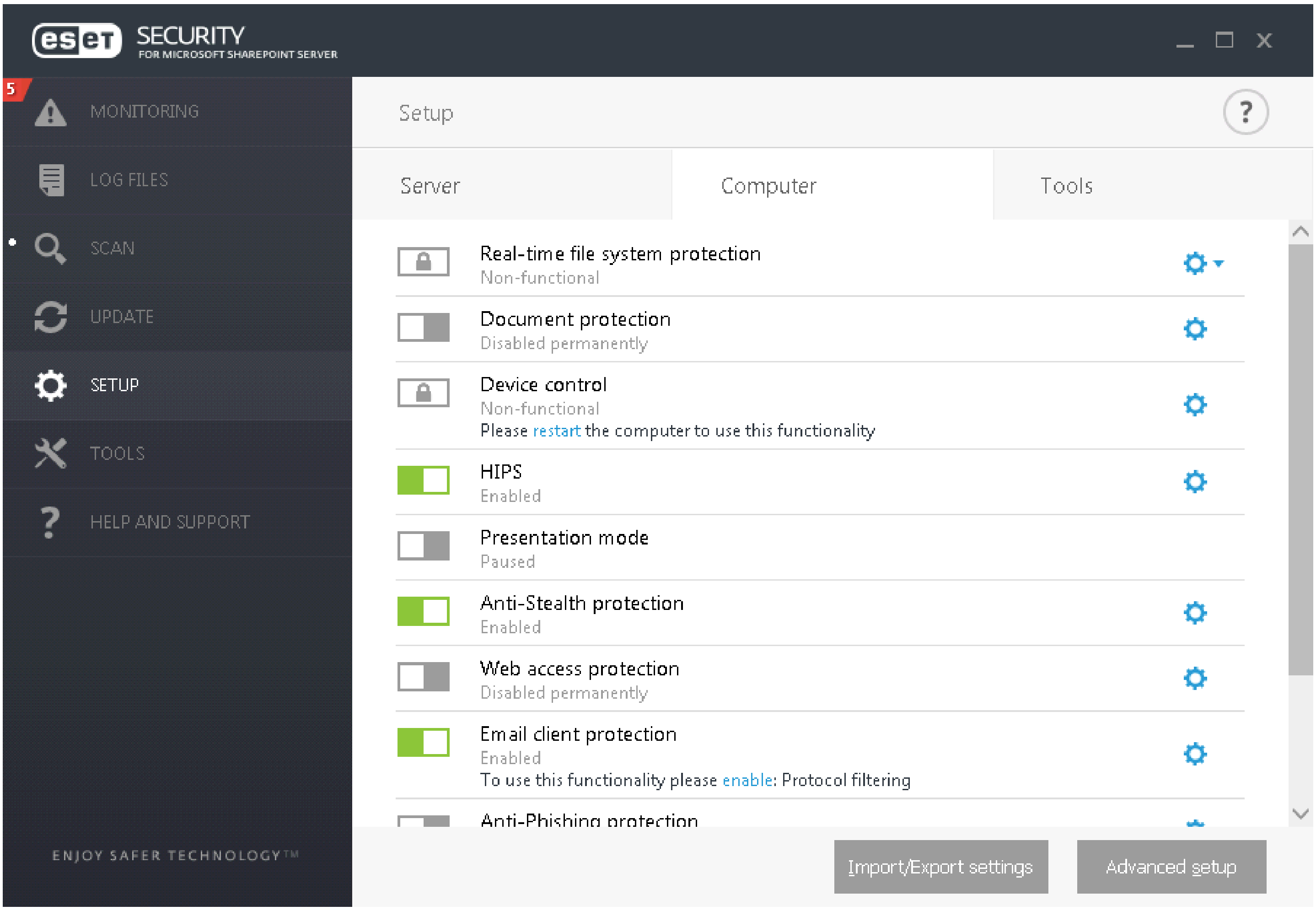
Generated 0 minutes ago

**NOTE**

For more information about ERA, see ESET Remote Administrator Online help. Online help is divided into three parts: Installation/Upgrade, Administration and VA Deployment. You can use the navigation tabs in the header to switch between the parts.

## 5.1 Override mode

If you have ESET Remote Administrator policy applied to ESET Security for Microsoft SharePoint, you'll see a lock icon 🔒 instead of Enable/Disable switch on Setup page and a lock icon next to the switch in **Advanced setup** window.



Real-time file system protection
Non-functional

Document protection
Disabled permanently

Device control
Non-functional
Please restart the computer to use this functionality

HIPS
Enabled

Presentation mode
Paused

Anti-Stealth protection
Enabled

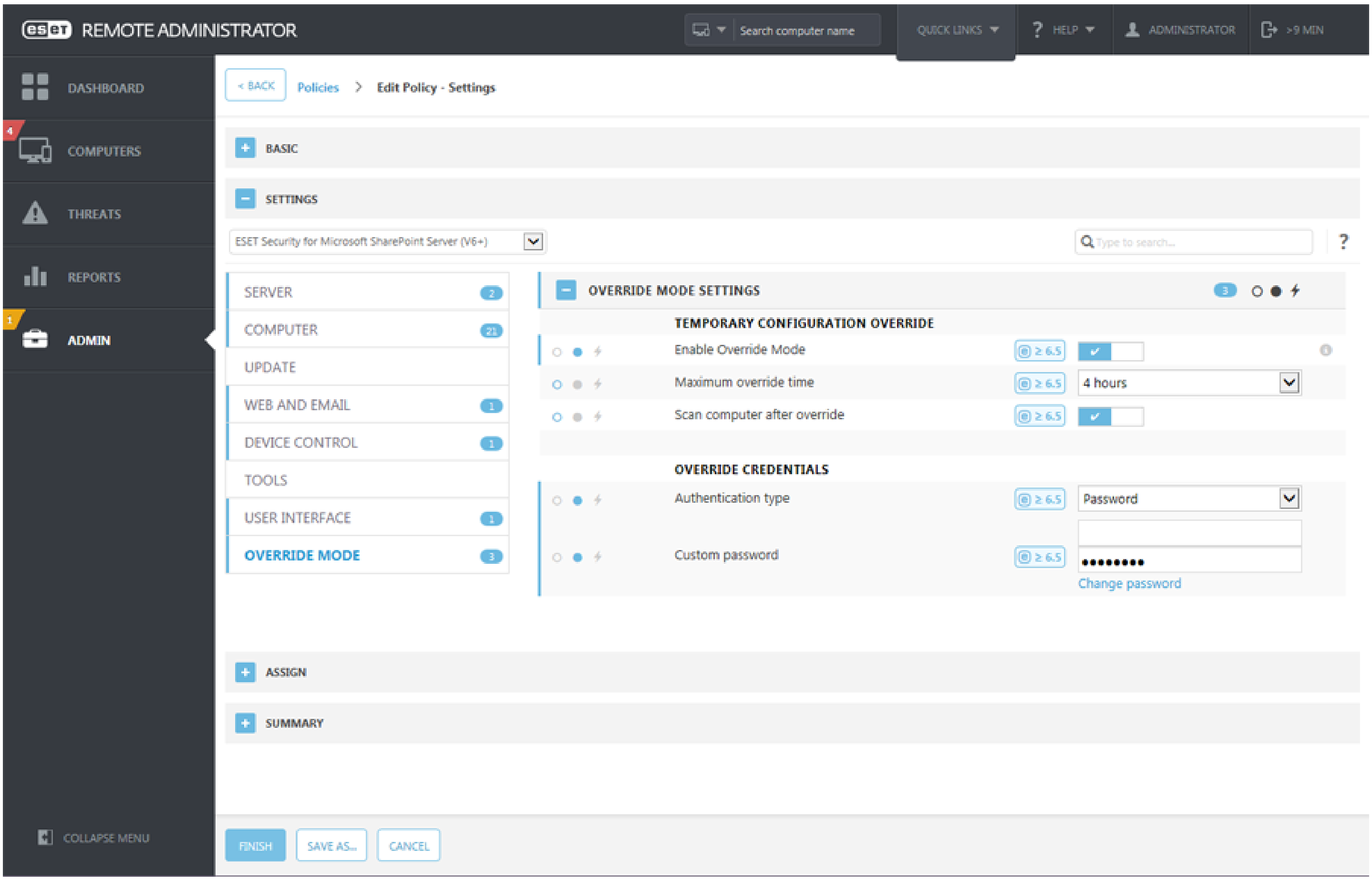
Web access protection
Disabled permanently

Email client protection
Enabled
To use this functionality please enable: Protocol filtering

Anti-Phishing protection

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

Log into ERA Web Console, navigate to **Admin** > **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**).



ESET Security for Microsoft SharePoint Server (V6+)

OVERRIDE MODE SETTINGS

TEMPORARY CONFIGURATION OVERRIDE

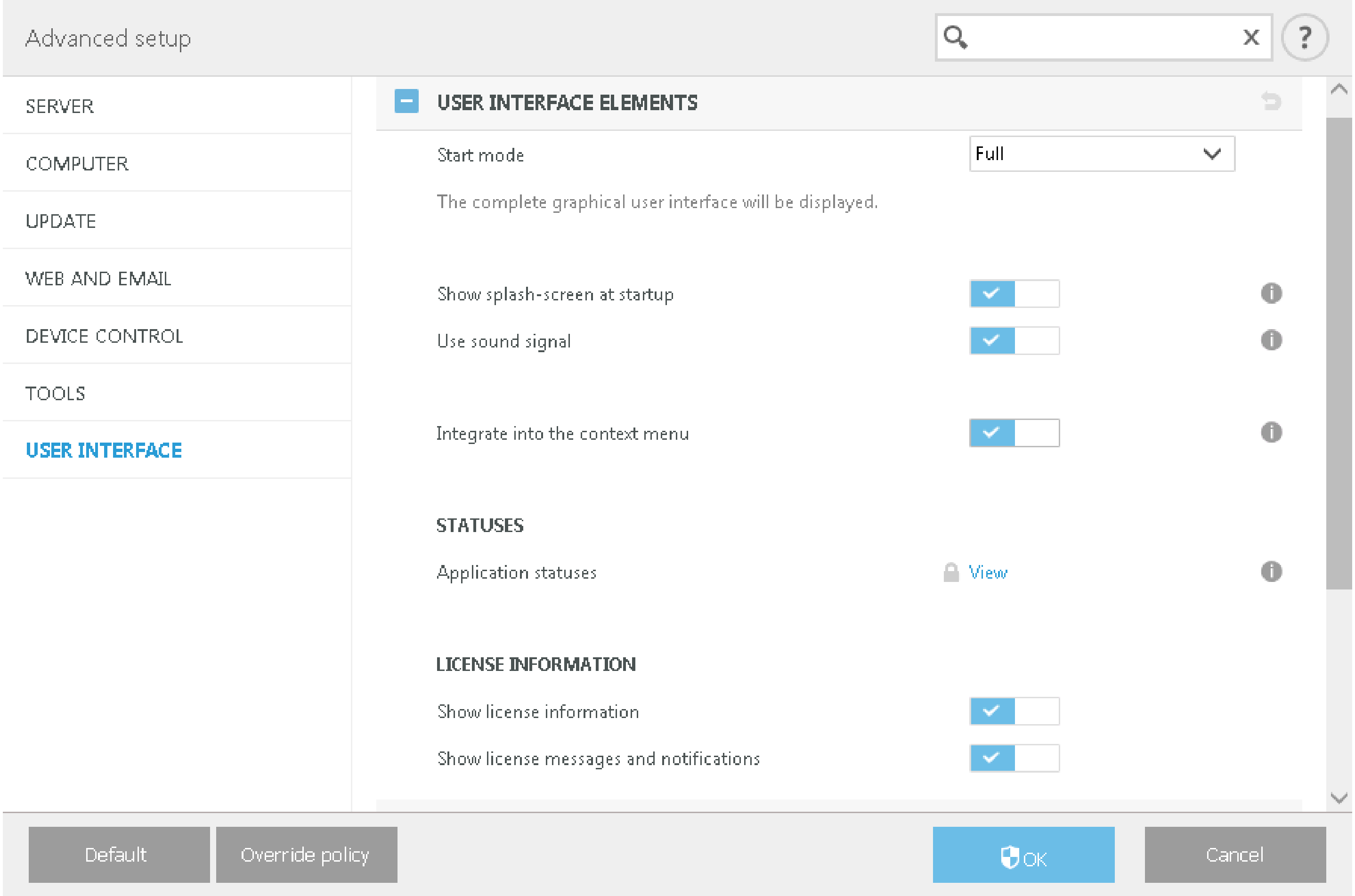
| | | |
|---|---|---|
| Enable Override Mode | ≥ 6.5 | ✓ |
| Maximum override time | ≥ 6.5 | 4 hours |
| Scan computer after override | ≥ 6.5 | ✓ |

OVERRIDE CREDENTIALS

| | | |
|---|---|---|
| Authentication type | ≥ 6.5 | Password |
| Custom password | ≥ 6.5 | •••••••• |

Change password

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



USER INTERFACE ELEMENTS

Start mode: Full

The complete graphical user interface will be displayed.

| | |
|---|---|
| Show splash-screen at startup | ✓ |
| Use sound signal | ✓ |
| Integrate into the context menu | ✓ |

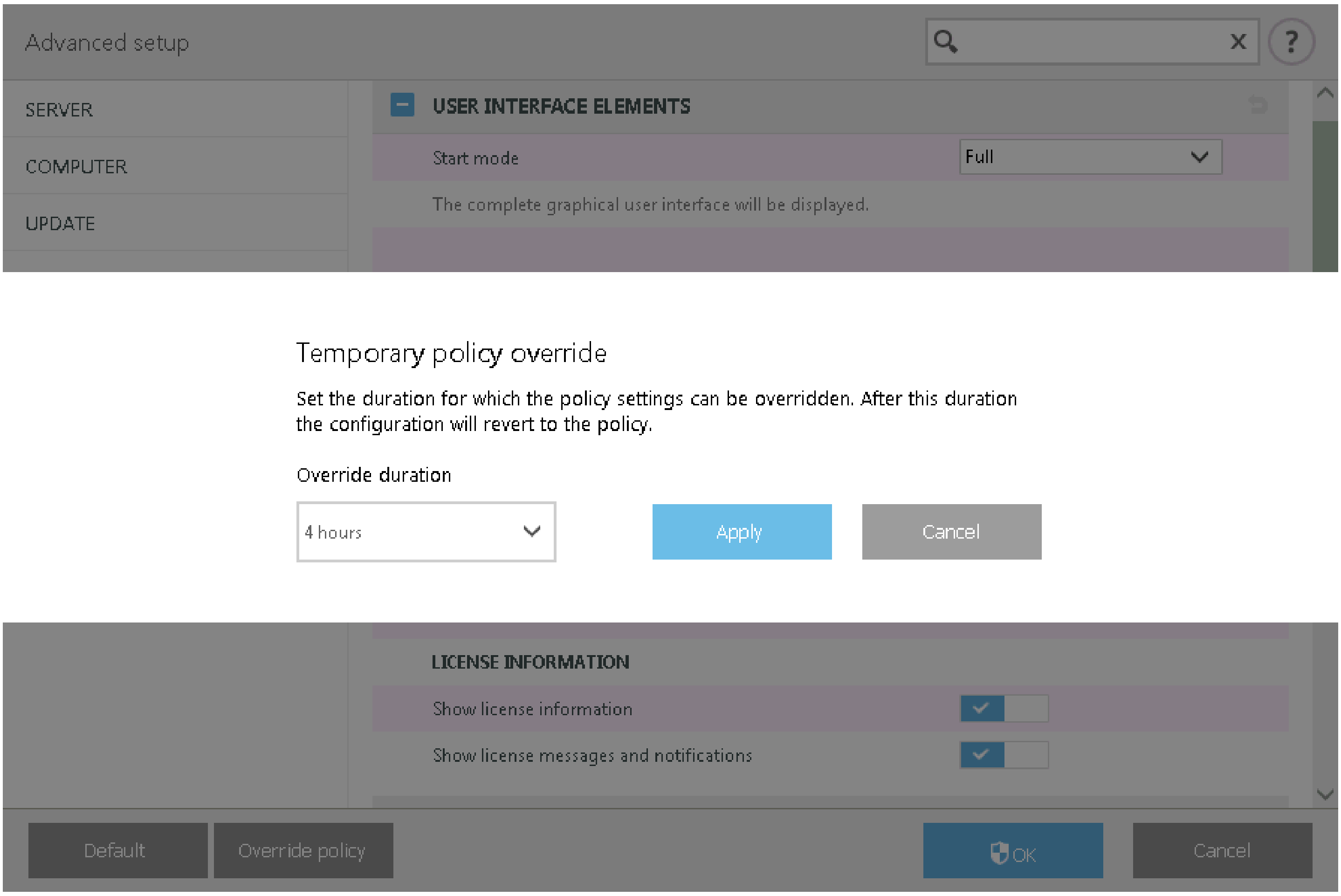
STATUSES

Application statuses: View

LICENSE INFORMATION

| | |
|---|---|
| Show license information | ✓ |
| Show license messages and notifications | ✓ |

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



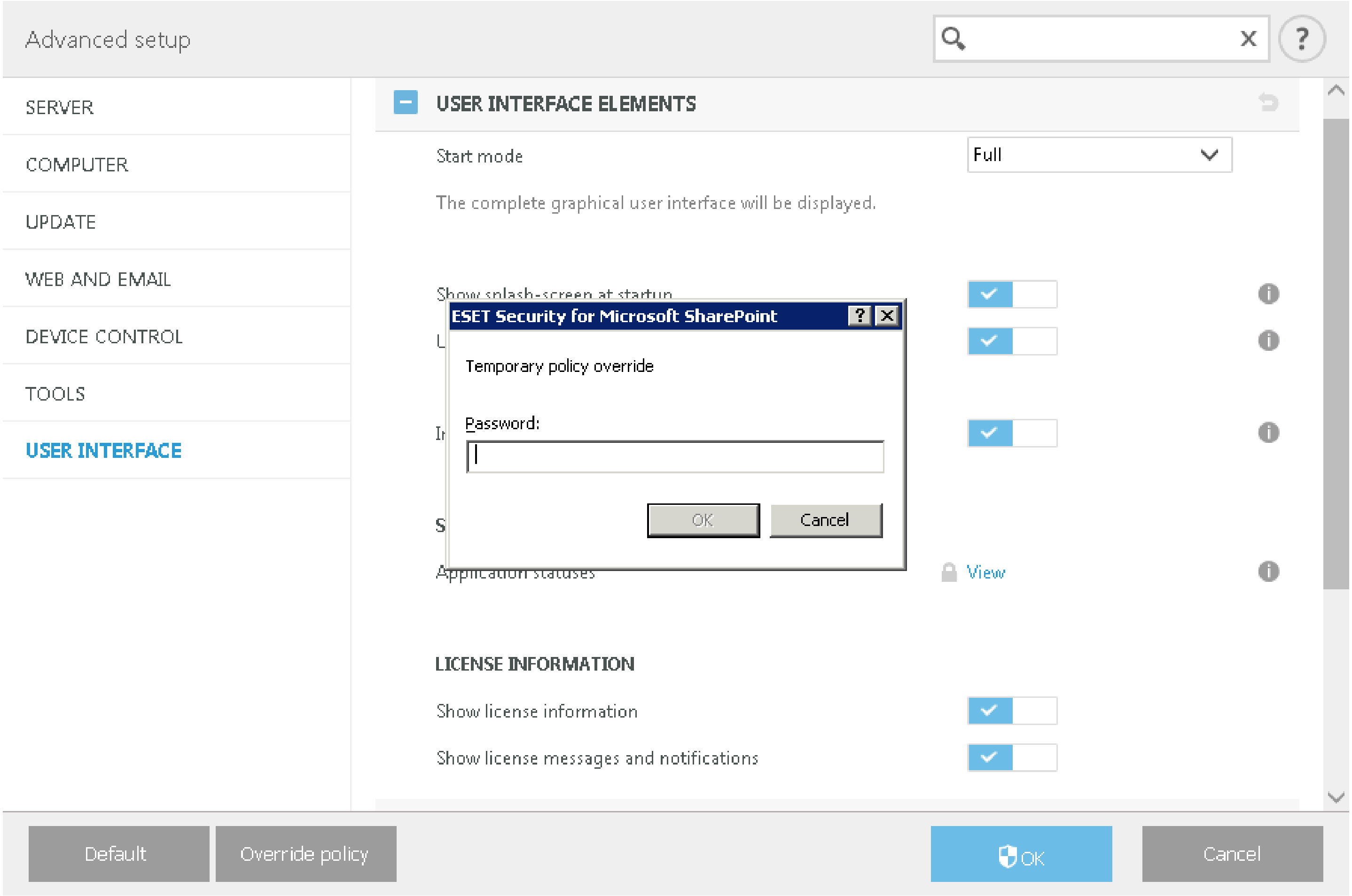
The complete graphical user interface will be displayed.

Temporary policy override

Set the duration for which the policy settings can be overridden. After this duration the configuration will revert to the policy.

Override duration: 4 hours

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



The complete graphical user interface will be displayed.

ESET Security for Microsoft SharePoint

Temporary policy override

Password:

Once the Override mode expires, any configuration changes you've made will revert back to original ESET Remote Administrator policy settings. You'll see a notification before the Override expires.

You can **End override** mode anytime before it expires on Monitoring page or in **Advanced setup** window.

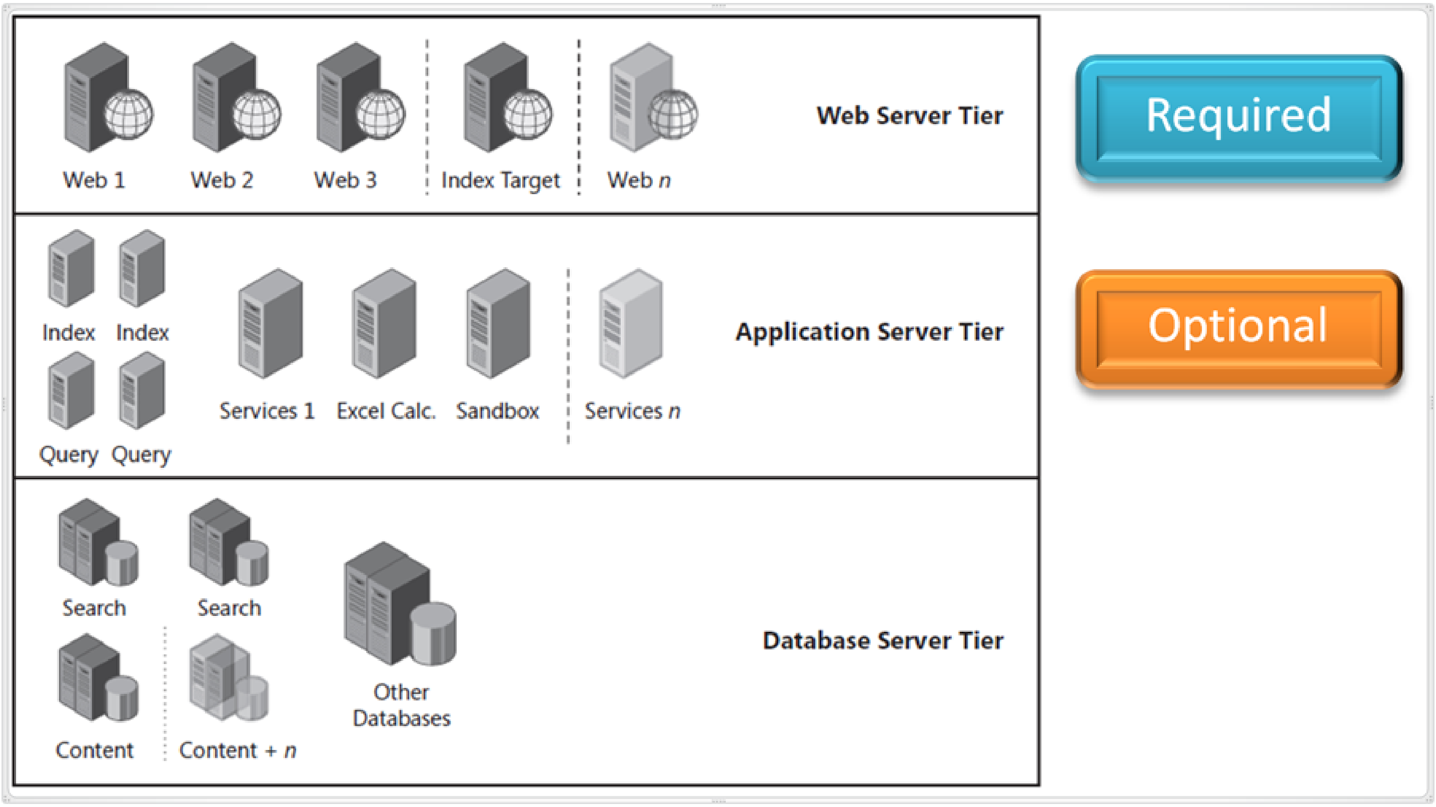
# 6. Deployment

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

## 6.1 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 also 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 database 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 tiers where ESET protection is required and tiers where it is optional.



**NOTE**
In a SharePoint farm setting, it is only necessary to run the On-demand database scan from one machine. The entire SharePoint farm database will be scanned.

Because On-demand scan is a resource intensive operation, we recommend that you run it on a machine where increased load during the scan is not a problem. From a functional point of view, it is perfectly fine to run the On-demand database scan from any SharePoint farm machine that can access the content database, regardless of its role.

The speed of On-demand database scan depends heavily on the throughput of the database server and of the network used. To increase database scanning throughput in large SharePoint farms, run On-demand database 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 database server load and its benefits should be evaluated by the farm administrator.

## 6.2 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 the ESET Cluster feature of ESET Security for Microsoft SharePoint. Apart from the installation, the ESET Cluster will serve as a replication of ESET Security for Microsoft SharePoint configuration to ensures consistency between cluster nodes necessary for correct operation.

## 6.3 Installation

After purchasing ESET Security for Microsoft SharePoint, the installer can be downloaded from ESET's website (www.eset.com) as an `.msi` package.

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

- You can log in locally using Administrator account credentials and simply run the installer
- You can execute the command as another user. To do so, open an administrative command prompt and run the `.msi` file (for example, `msiexec /i eshp_nt64_ENU.msi` but you need to replace `eshp_nt64_ENU.msi` with the exact file name of the msi installer you have downloaded).

Once you launch the installer and accept the End-User License Agreement (EULA) the installation wizard will guide you through setup. If you choose not to accept the terms in the License Agreement, the wizard will not continue.

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

There are three installation types available using the wizard:

**Complete**
This is the recommended installation type. It will install all features of ESET Security for Microsoft SharePoint. You can select the install location for ESET Security, however we recommend that you use default values.

**Core**
This installation type is intended for Windows Server Core editions. Installation steps are the same as complete installation, but only core features are and the command line user interface will be 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 solutions installed using core installation will not have any GUI. This means that you can only use the command line user interface when working with ESET Security for Microsoft SharePoint.

To execute Core installation via command line, use the following sample command:

```
msiexec /qn /i efsw_nt64_ENU.msi /l inst.log ADDLOCAL=HIPS,_Base,SERVER,_FeaturesCore,WMIProvider,Scan,Updat
```

**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 will be displayed when you begin installation.

In addition to the install wizard, you can choose to install ESET Security for Microsoft SharePoint silently via command line. This installation type does not require any interaction and is also referred to as an unattended installation.

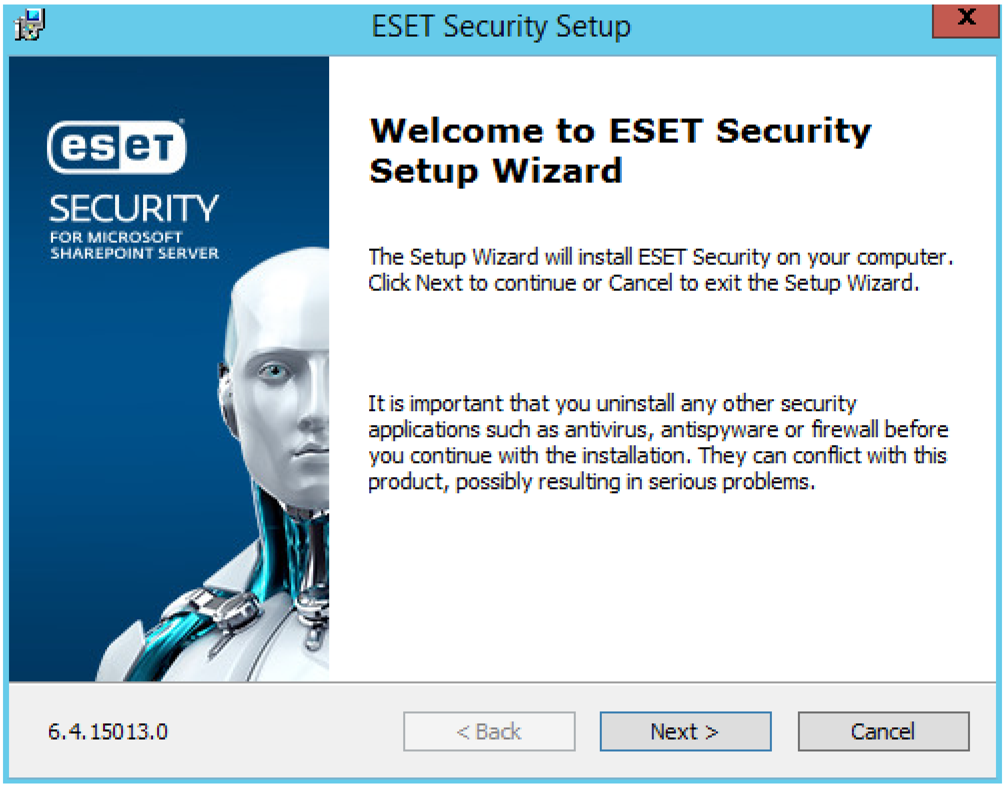
**Silent / Unattended installation**
Run the following command to complete installation via command line: `msiexec /i <packagename> /qn /l*xv msi.log`

NOTE

If you have previously used other third-party antivirus software on your system, we recommend that you uninstall it completely prior to the installation of ESET Security for Microsoft SharePoint. You can use ESET AV Remover to assist in the removal of third-party software.

### 6.3.1 ESET Security for Microsoft SharePoint installation steps

Follow the steps below to install ESET Security for Microsoft SharePoint using the Setup Wizard:



**Welcome to ESET Security Setup Wizard**

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

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

6.4.15013.0

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

Choose one of available installation types. Installation types available depend on your operating system.

Windows Server 2003, 2003 R2, 2012, 2012 R2, 2016, Windows Small Business Server 2003 and 2003 R2, Windows Server 2012 Essentials, 2012 R2 Essentials and 2016 Essentials:

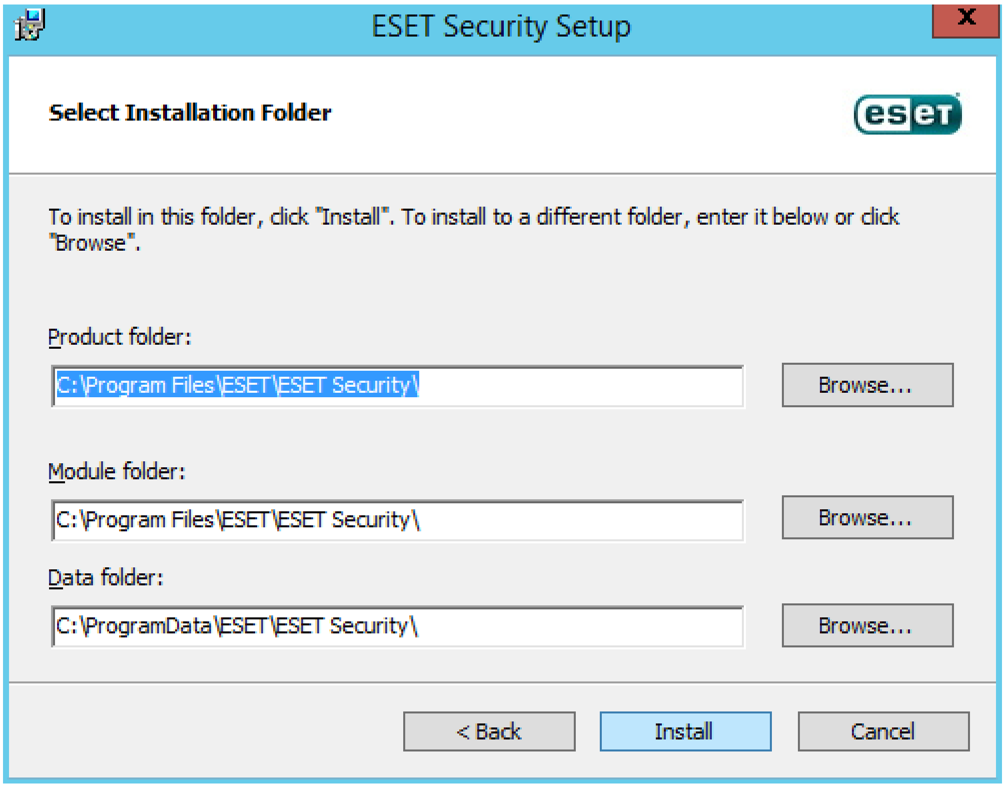
- **Complete** - installs all ESET Security for Microsoft SharePoint features.
- **Core** - This installation type is intended for use on Windows Server Core. The process is similar to complete installation but only core components are installed. Using this method, ESET Security for Microsoft SharePoint will have no GUI. You can also run core installation on a regular Windows Server if necessary. For more details about core installation click here.
- **Custom** - lets you select which ESET Security for Microsoft SharePoint features will be installed on your system.

Windows Server 2008, 2008 R2, Windows Small Business Server 2008 and 2011:

- **Typical** - installs recommended ESET Security for Microsoft SharePoint features.
- **Core** - This installation type is intended for use on Windows Server Core. The process is similar to complete installation but only core components are installed. Using this method, ESET Security for Microsoft SharePoint will have no GUI. You can also run core installation on a regular Windows Server if necessary. For more details about core installation click here.
- **Custom** - lets you select which ESET Security for Microsoft SharePoint features will be installed on your system.

**Complete installation:**

Also called full installation. This will install all ESET Security for Microsoft SharePoint components. You will be prompted to select an install location. By default, the program installs in C:\Program Files\ESET\ESET Security for Microsoft SharePoint. Click **Browse** to change this location (not recommended).



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

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

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

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

**Typical installation:**

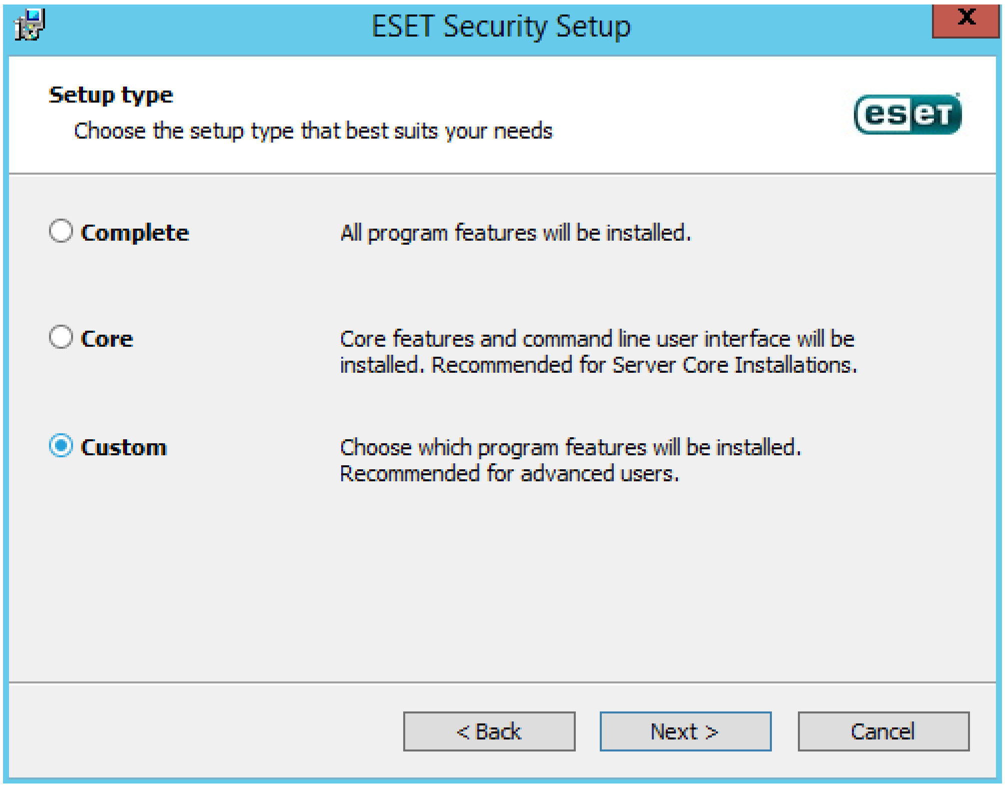
Choose this installation type to install recommended ESET Security for Microsoft SharePoint features.

NOTE
On Windows Server 2008, Windows Server 2008 R2, Small Business Server 2008 and Small Business Server 2011, installation of **Web and email** component is disabled by default (**Typical** installation). If you want to have this component installed, choose **Custom** installation type.

**Core installation:**

Core features and the command line user interface will be installed. This method is recommended for use on Windows Server Core.

**Custom installation:**



**Setup type**

Choose the setup type that best suits your needs

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

○ **Core** Core features and command line user interface will be installed. Recommended for Server Core Installations.

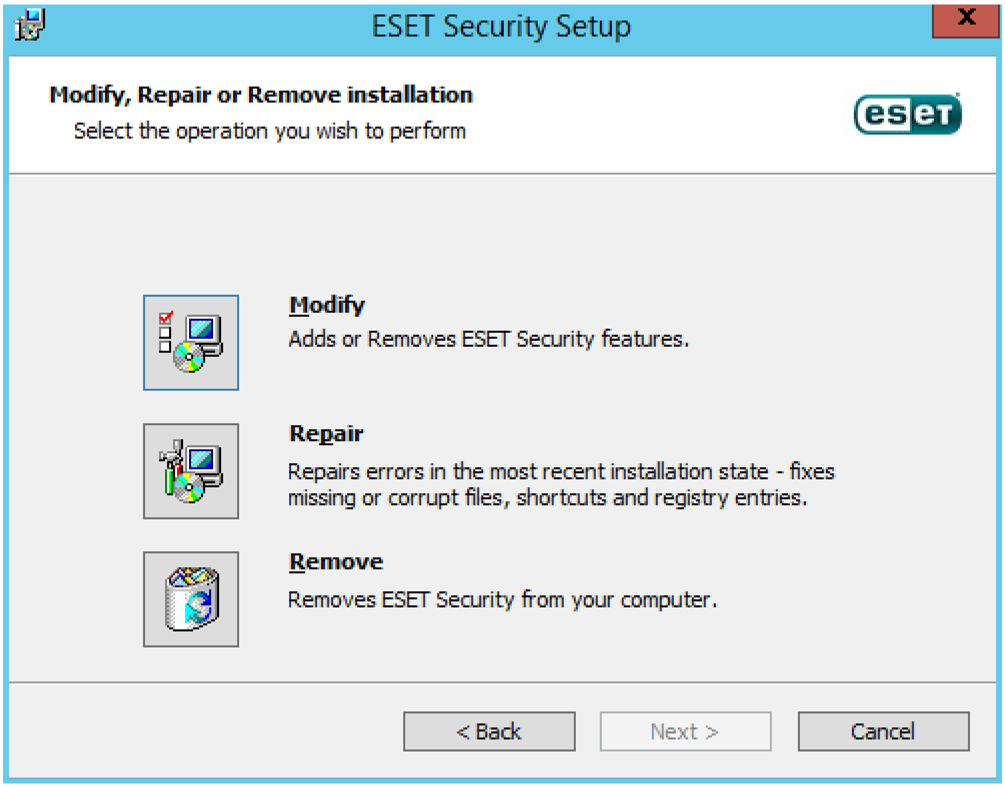
● **Custom** Choose which program features will be installed. Recommended for advanced users.

Lets you choose which features you want to install. Useful when you want to customize ESET Security for Microsoft SharePoint with only the components you need.

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

**Component modification (Add/Remove) process, Repair and Remove:**

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



**Modify, Repair or Remove installation**

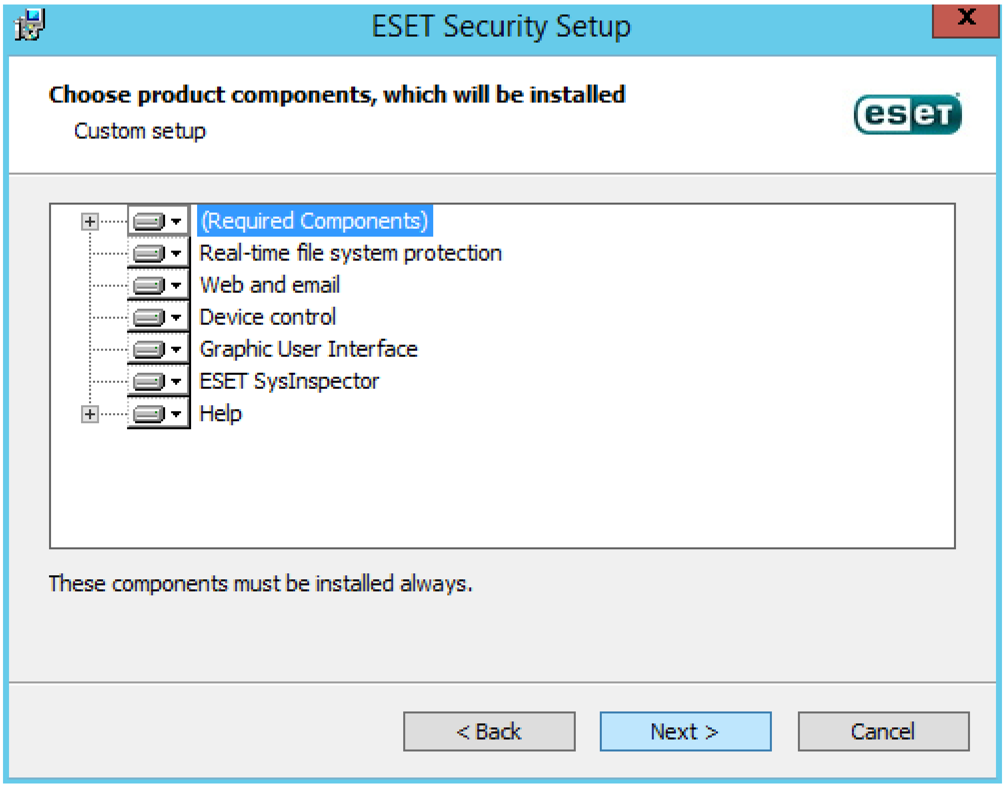
Select the operation you wish to perform

**Modify**
Adds or Removes ESET Security features.

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

**Remove**
Removes ESET Security from your computer.

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



Choose product components, which will be installed

Custom setup

- (Required Components)
- Real-time file system protection
- Web and email
- Device control
- Graphic User Interface
- ESET SysInspector
- Help

These components must be installed always.

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

NOTE

You can modify installed components any time by running the installer. Modifications do not require a server restart.

### 6.3.1.1 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: `efsw_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

**APPDATADIR=<path>**

- path - Valid directory path
- Application Data installation directory

**MODULEDIR=<path>**

- path - Valid directory path
- Module installation directory

**ADDEXCLUDE=<list>**

- The ADDEXCLUDE list is a comma-separated list of all feature names not to be installed, as a replacement for the obsolete REMOVE.
- When selecting a feature not to install, then the whole path (i.e., all its sub-features) and related invisible features must be explicitly included in the list.
- For example: `efsw_nt64_ENU.msi /qn ADDEXCLUDE=<list>`

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

**ADDLOCAL=<list>**

- Component installation - list of non-mandatory features to be installed locally.
- Usage with ESET .msi packages: `efsw_nt64_ENU.msi /qn ADDLOCAL=<list>`
- For more information about the **ADDLOCAL** property see http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

### Rules

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

### 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
- **Placeholder** - feature with no effect on the product, listed with sub-features

Below is an example of the ESET Security for Microsoft SharePoint feature tree:

| Feature tree | Feature Name | Feature Presence |
|---|---|---|
| Computer | Computer | Mandatory |
| Computer / Antivirus and antispyware | Antivirus | Mandatory |
| Computer / Antivirus and antispyware > Real-time file system protection | RealtimeProtection | Mandatory |
| Computer / Antivirus and antispyware > Computer scan | Scan | Mandatory |
| Computer / Antivirus and antispyware > Document protection | DocumentProtection | Optional |
| Computer / Device control | DeviceControl | Optional |
| Web and e-mail ProtocolFiltering | ProtocolFiltering | Invisible |
| Web and e-mail / Web access protection | WebAccessProtection | Optional |
| Web and e-mail / E-mail client protection | EmailClientProtection | Optional |
| Web and e-mail / E-mail client protection / MailPlugins | MailPlugins | Invisible |
| Web and e-mail  / Web control | WebControl | Optional |
| Update mirror | UpdateMirror | Optional |

### Additional rules

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

Example command: `efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering`

### Command line Core installation examples:

```
msiexec /qn /i efsw_nt64_ENU.msi /l inst.log ADDLOCAL=HIPS,_Base,SERVER,_FeaturesCore,WMIProvider,Scan,Updat
```

```
msiexec /qn /i efsw_nt64_ENU.msi /l*xv msi.log ADDLOCAL=SERVER,eShell,RealtimeProtection CFG_POTENTIALLYUNWA
```

### List of CFG_ properties:

**CFG_POTENTIALLYUNWANTED_ENABLED=1/0**

- 0 - Disabled, 1 - Enabled

**CFG_LIVEGRID_ENABLED=1/0**

- 0 - Disabled, 1 - Enabled

- LiveGrid

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

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

**CFG_PROXY_ADDRESS=<ip>**
- Proxy IP address

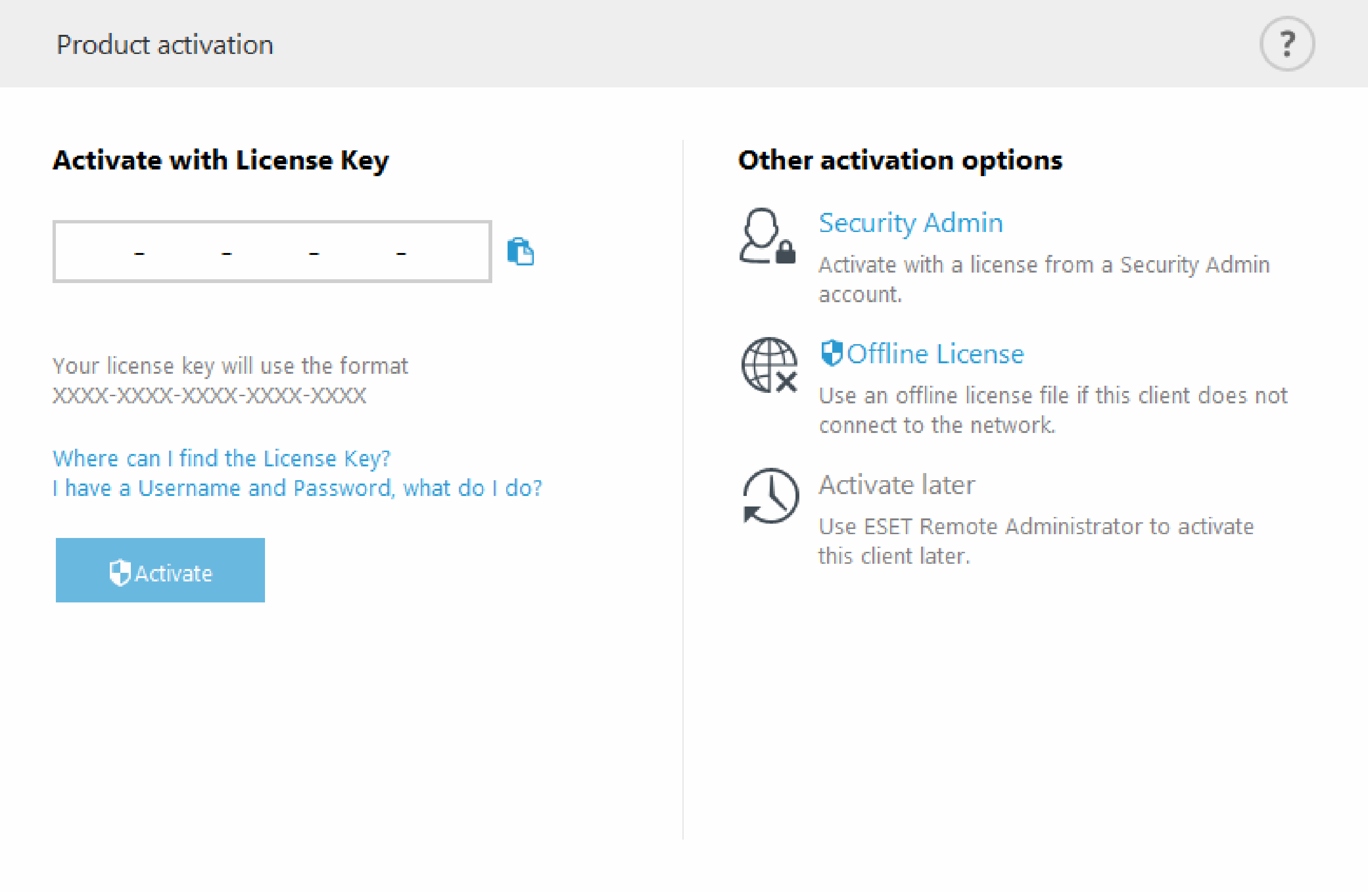
**CFG_PROXY_PORT=<port>**
- Proxy port number

**CFG_PROXY_USERNAME=<user>**
- User name for authentication

**CFG_PROXY_PASSWORD=<pass>**
- Password for authentication

### 6.3.2 Post installation steps

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


Product activation

Activate with License Key

Your license key will use the format XXXX-XXXX-XXXX-XXXX-XXXX

Where can I find the License Key?
I have a Username and Password, what do I do?

Other activation options

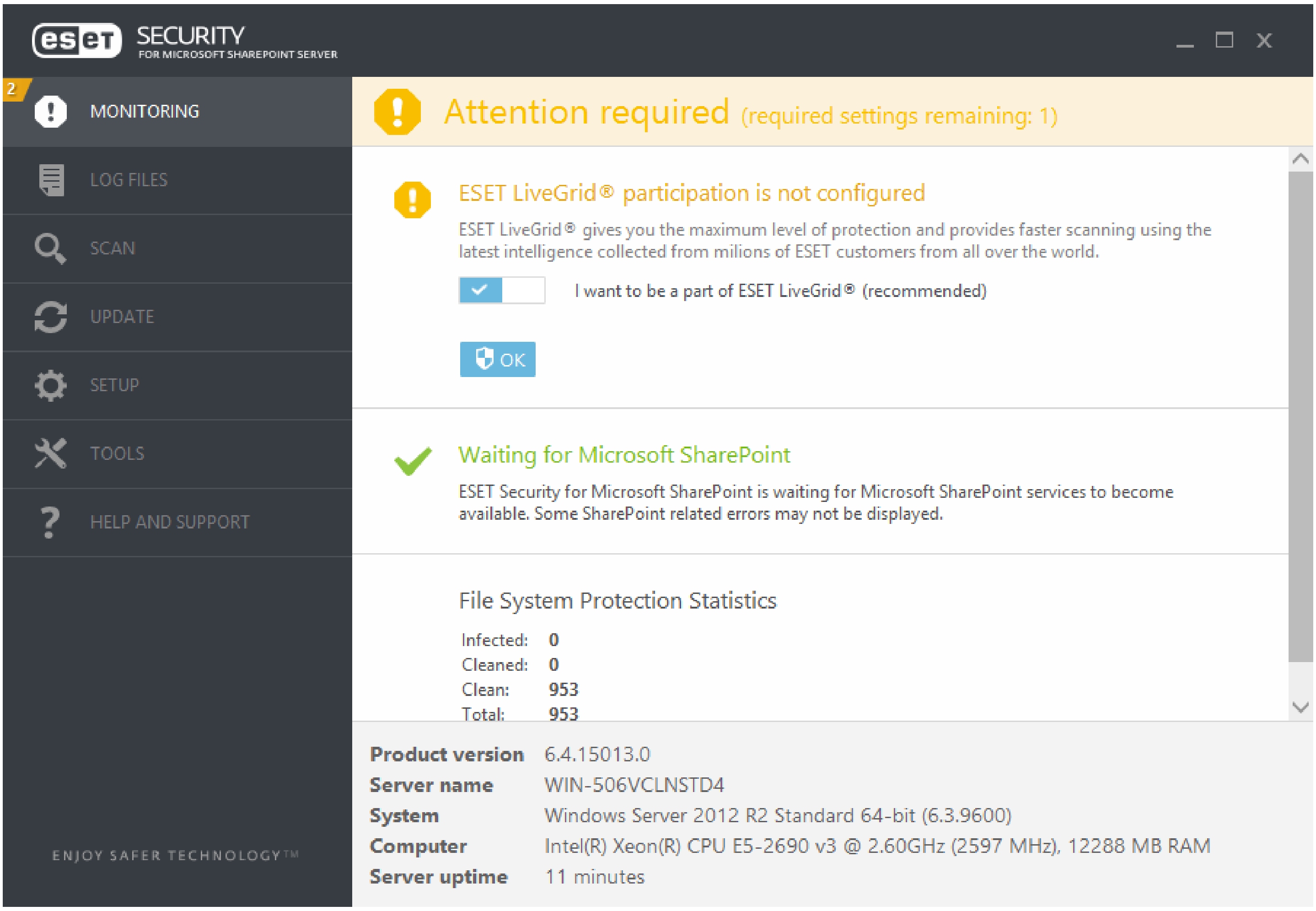
Security Admin
Activate with a license from a Security Admin account.

Offline License
Use an offline license file if this client does not connect to the network.

Activate later
Use ESET Remote Administrator to activate this client later.

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

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



Attention required (required settings remaining: 1)

ESET LiveGrid® participation is not configured

ESET LiveGrid® gives you the maximum level of protection and provides faster scanning using the latest intelligence collected from milions of ESET customers from all over the world.

☑ I want to be a part of ESET LiveGrid® (recommended)

OK

✓ Waiting for Microsoft SharePoint

ESET Security for Microsoft SharePoint is waiting for Microsoft SharePoint services to become available. Some SharePoint related errors may not be displayed.

File System Protection Statistics

|  |  |
|---|---|
| Infected: | 0 |
| Cleaned: | 0 |
| Clean: | 953 |
| Total: | 953 |

|  |  |
|---|---|
| **Product version** | 6.4.15013.0 |
| **Server name** | WIN-506VCLNSTD4 |
| **System** | Windows Server 2012 R2 Standard 64-bit (6.3.9600) |
| **Computer** | Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz (2597 MHz), 12288 MB RAM |
| **Server uptime** | 11 minutes |

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

### 6.3.3 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 GUI to prevent it from starting up every time a user logs in. See Disable GUI on Terminal Server for specific steps to disable the GUI.

### 6.3.4 ESET AV Remover

To remove/uninstall third-party antivirus software from your system, we recommend that you use the ESET AV Remover. To do so, follow these steps:

1. Download the ESET AV Remover from ESET website Utilities download page.
2. Click **I accept, start search** to accept the EULA and begin searching your system.
3. Click **Launch uninstaller** to remove the installed antivirus software.

For a list of third-party antivirus software that can be removed using ESET AV Remover see this KB article.

### 6.3.5 Upgrading to a newer version

New versions of ESET Security for Microsoft SharePoint are issued to provide improvements or fix issues that cannot be resolved by automatic updates to program modules. The following upgrade methods can be used:

- Manual - download and install a more recent version over your existing version. Simply run the installer and perform an installation as usual, ESET Security for Microsoft SharePoint will transfer your existing configuration automatically. We recommend this procedure if you have a single server running ESET Security for Microsoft SharePoint. Applicable for upgrades from any legacy version to 6.x.
- Remote - for use in large network environments managed by ESET Remote Administrator. This method is useful if you have multiple servers running ESET Security for Microsoft SharePoint. Applicable for upgrades from version 4.x to 6.x.
- 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. Applicable for upgrades from version 4.x to 6.x. Once the upgrade is completed, you can continue using ESET Cluster and take advantage of its features.

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

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

#### 6.3.5.1 Upgrading via ERA

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

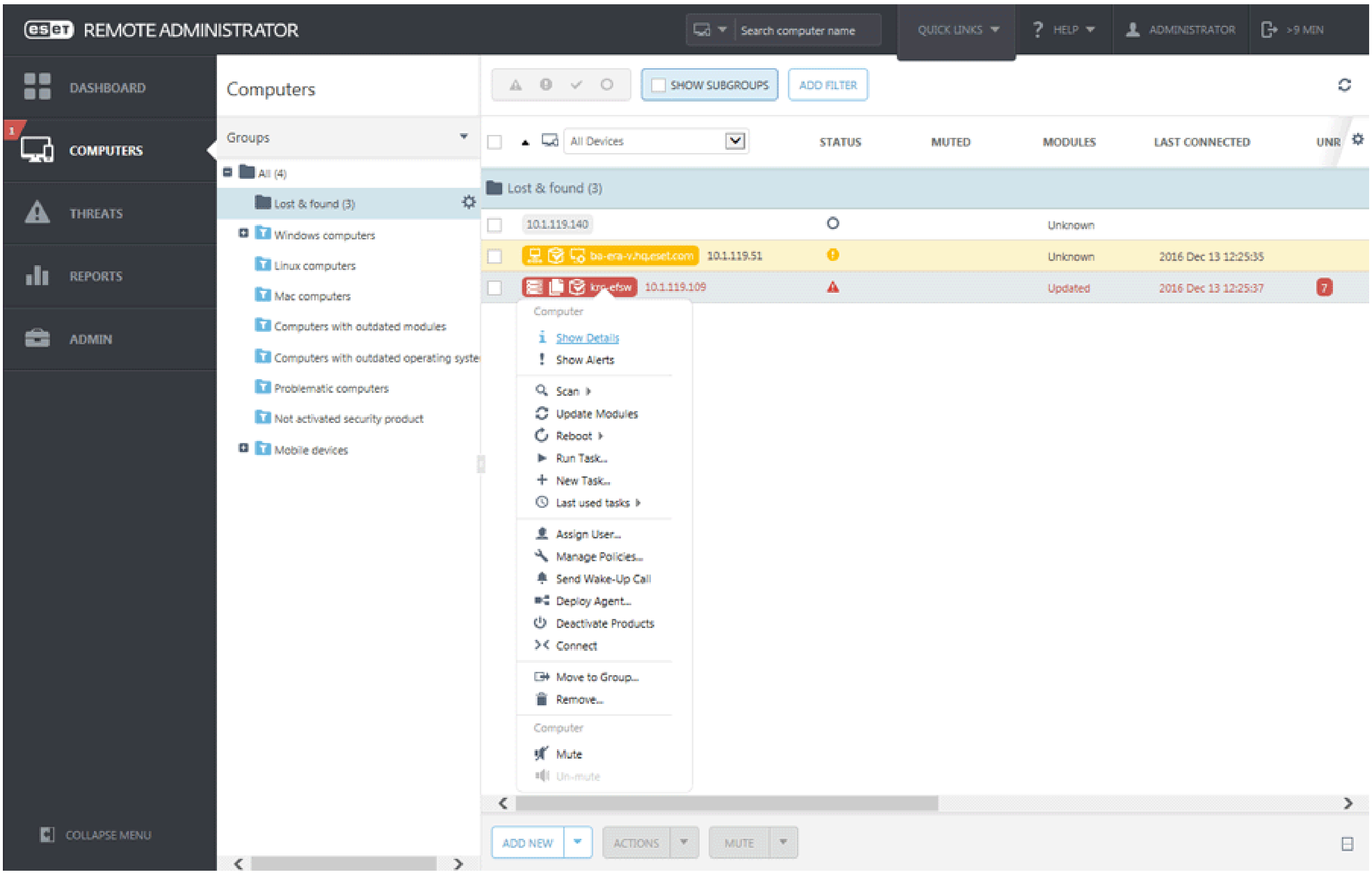
NOTE
Applicable for upgrades from version 4.x to 6.x.

The procedure consists of the following phases:

- **Upgrade the first server** manually by installing the latest version of ESET Security for Microsoft SharePoint over your existing version in order to preserve all of the configuration including rules, etc. 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 6.x and **Convert to policy** in ERA. The policy will later be applied to all upgraded servers. This phase is performed remotely using ERA as well as the following phases.
- **Run Software Uninstall** task on all servers running old version of ESET Security for Microsoft SharePoint.
- **Run Software Install** task on all servers which you want the latest version ESET Security for Microsoft SharePoint to run.
- **Assign configuration policy** to all the servers running the latest version ESET Security for Microsoft SharePoint.
- **Specify SharePoint Farm Administrator account** on each server manually. This phase is performed locally.

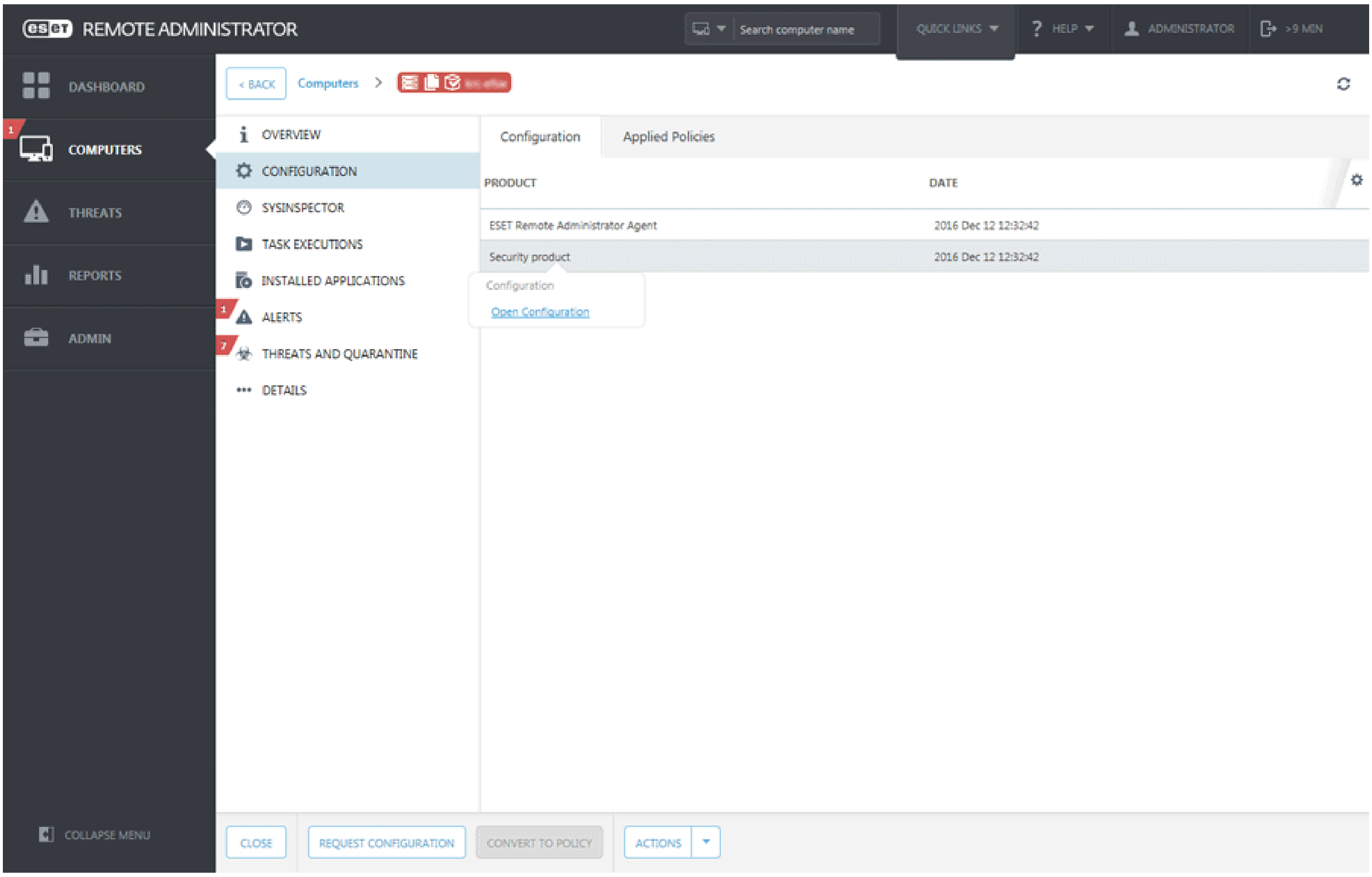
Step-by-step procedure:

1. Log onto one of the servers running ESET Security for Microsoft SharePoint and upgrade it by downloading and installing the latest version over your existing one. Follow the steps for regular installation. All of the original configuration of your old ESET Security for Microsoft SharePoint will be preserved during the installation.
2. Open the **ERA Web Console**,select a client computer from a Static or Dynamic group and click **Show Details**.



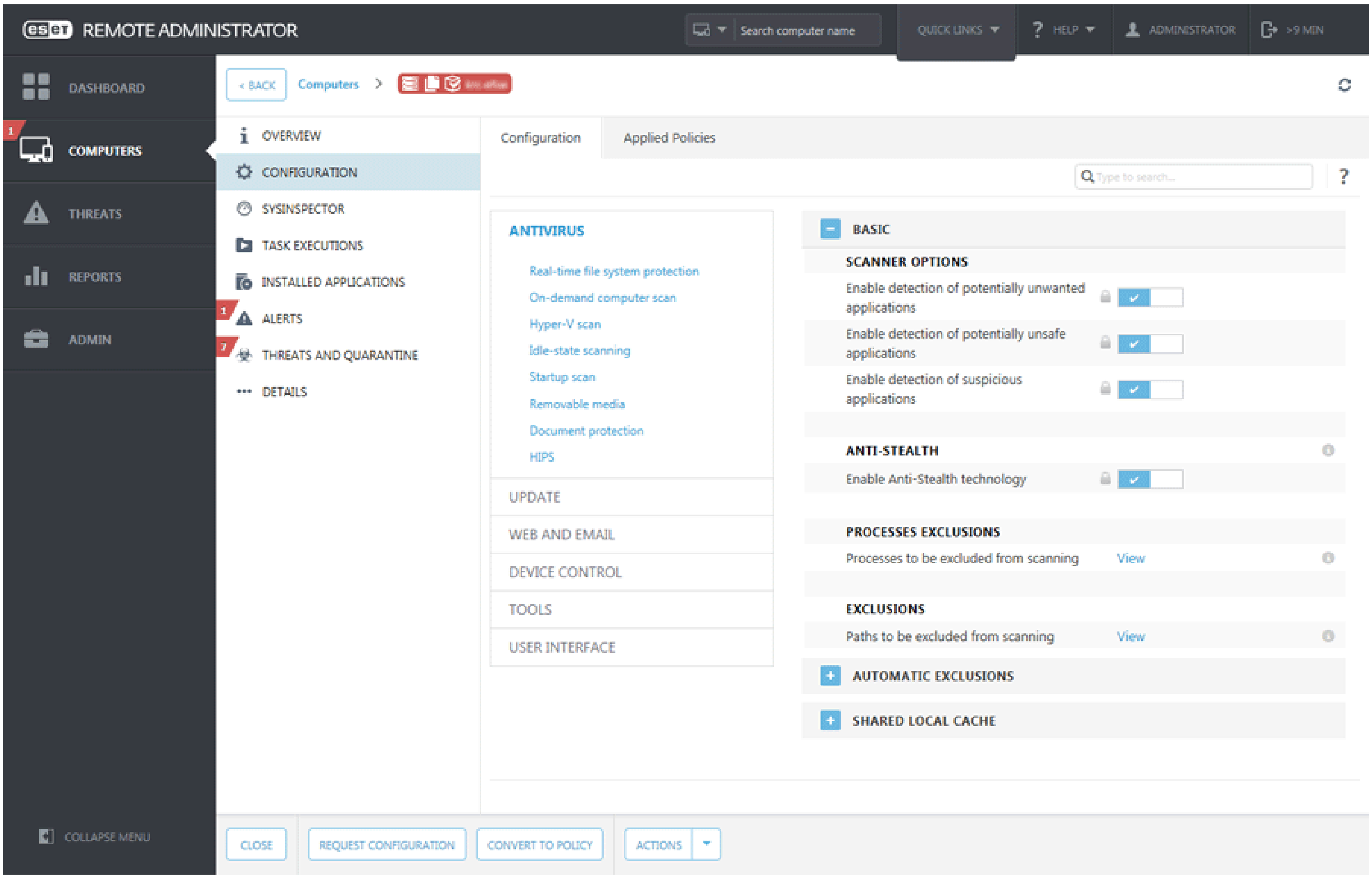
| | STATUS | MUTED | MODULES | LAST CONNECTED | UNR |
|---|---|---|---|---|---|
| Lost & found (3) | | | | | |
| 10.1.119.140 | ○ | | Unknown | | |
| ba-era-v.hq.eset.com 10.1.119.51 | ● | | Unknown | 2016 Dec 13 12:25:35 | |
| krp-efsw 10.1.119.109 | ▲ | | Updated | 2016 Dec 13 12:25:37 | 7 |

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



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

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



BASIC

SCANNER OPTIONS

Enable detection of potentially unwanted applications ✓

Enable detection of potentially unsafe applications ✓

Enable detection of suspicious applications ✓

ANTI-STEALTH

Enable Anti-Stealth technology ✓

PROCESSES EXCLUSIONS

Processes to be excluded from scanning View

EXCLUSIONS

Paths to be excluded from scanning View

AUTOMATIC EXCLUSIONS

SHARED LOCAL CACHE

5. Navigate to **Admin** > **Client Tasks** and choose Software Uninstall task. When creating the uninstall task, we recommend you to reboot the server after the uninstallation by selecting the checkbox **Automatically reboot when needed**. Once the task is created, add all desired target computers for uninstallation.

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

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

8. **Assign 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'll see a red warning status message saying: *ESET SharePoint Helper Service is not running*. Specify **SharePoint Farm Administrator account** in advanced setup.

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

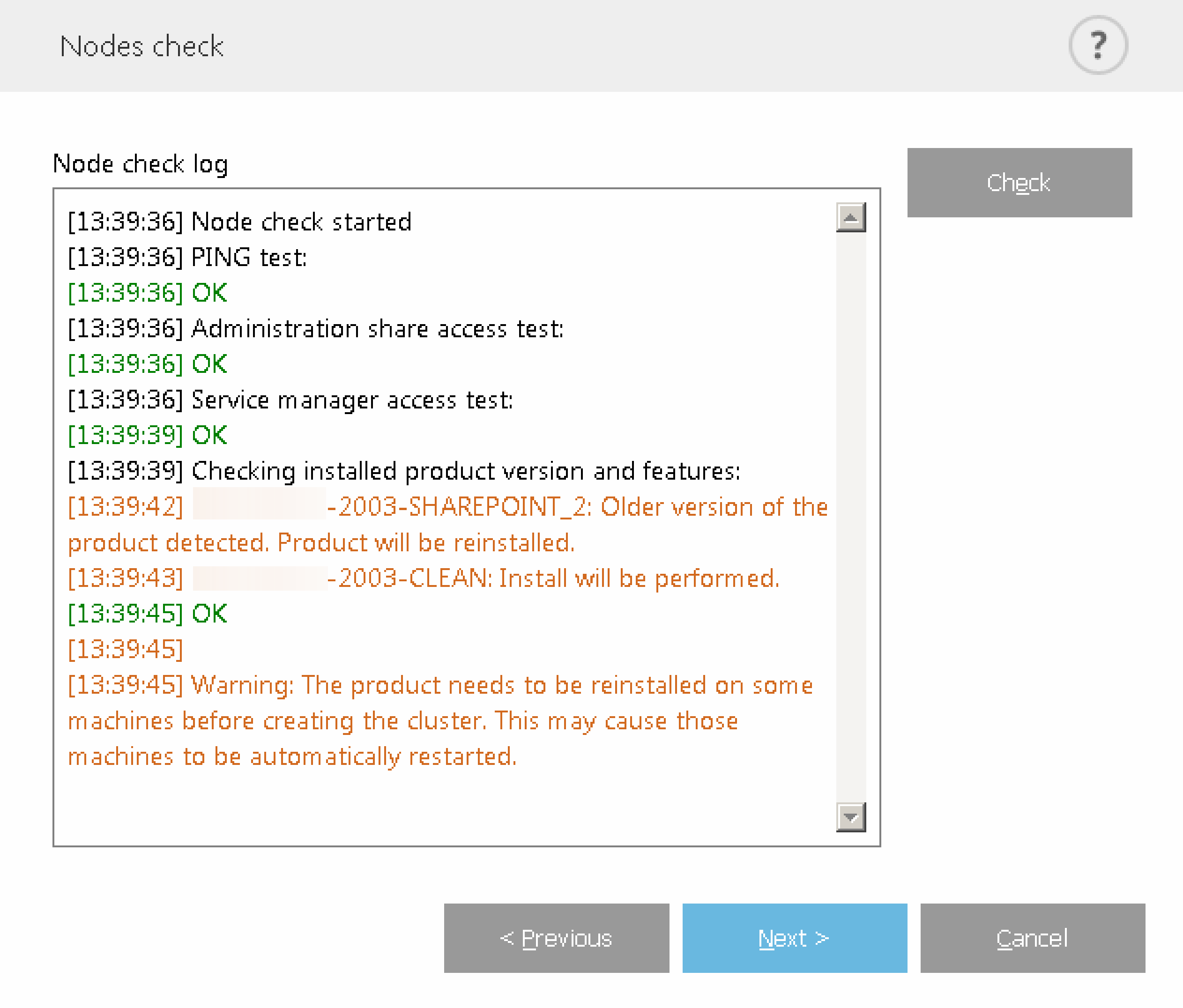
### 6.3.5.2 Upgrading via ESET Cluster

Creating an ESET Cluster lets you upgrade multiple servers using older versions of ESET Security for Microsoft SharePoint. It is an alternative to the ERA upgrade. We recommend using the ESET Cluster method if you have 2 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 in so the configuration of ESET Security for Microsoft SharePoint will be synchronized on all member nodes.

**NOTE**
Applicable for upgrades from version 4.x to 6.x.

Follow the steps below to upgrade using this method:

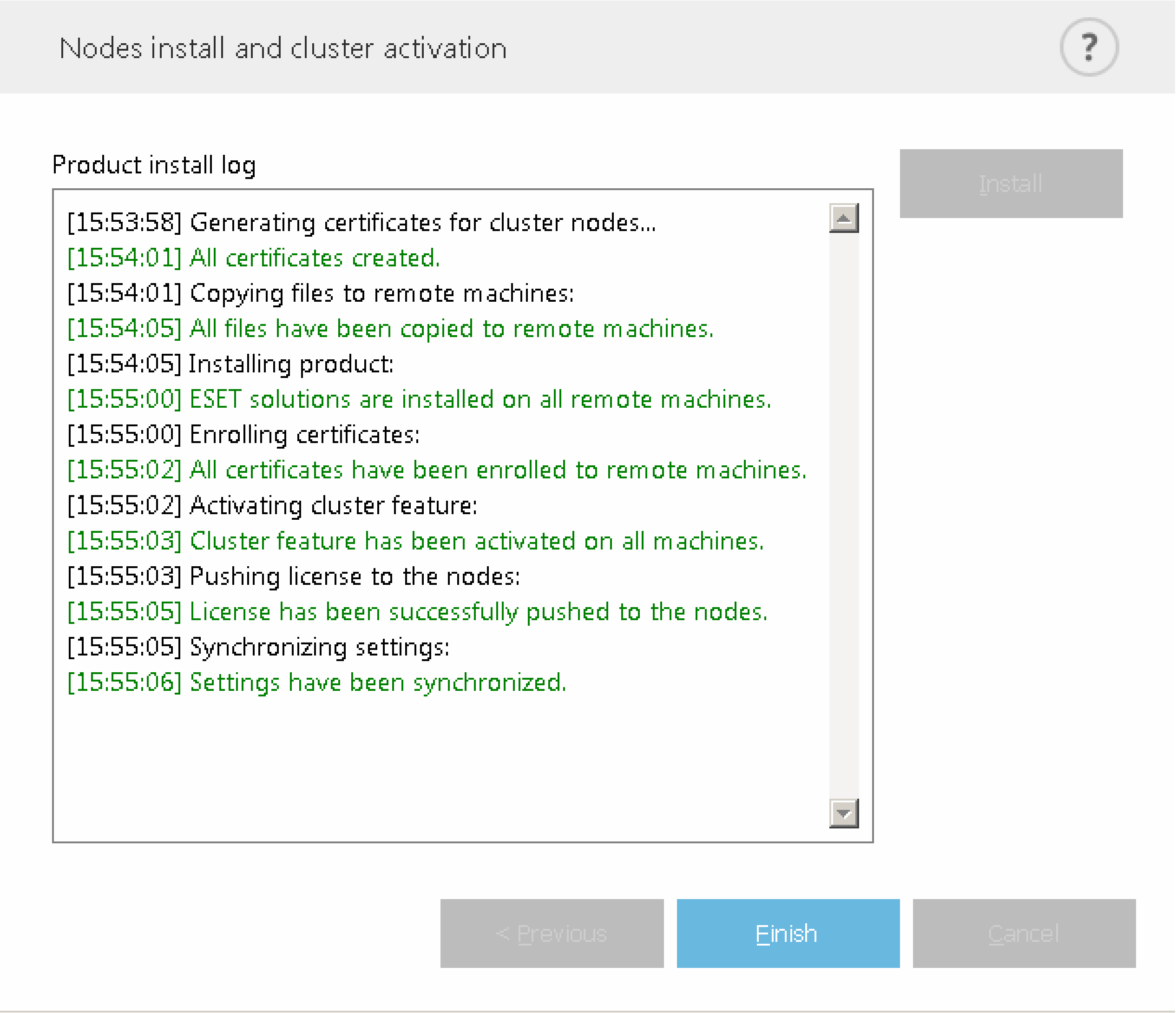
1. Log on to one of the servers running ESET Security for Microsoft SharePoint and upgrade it by downloading and installing the latest version over your existing one. Follow the steps for regular installation. All of the original configuration of your old ESET Security for Microsoft SharePoint will be preserved during the installation.
2. Run the ESET Cluster wizard and add cluster nodes (servers you want to upgrade ESET Security for Microsoft SharePoint on). If required, you can add other servers that do not run ESET Security for Microsoft SharePoint yet (an installation will be performed on these). We recommend that you to leave the default settings in place when specifying your Cluster name and install type (make sure **Push license to nodes without activated product** is selected).
3. Review the **Nodes check log** screen. It will list servers with older product versions and that the product will be reinstalled. ESET Security for Microsoft SharePoint will also be installed on any added servers where it is not currently installed.



Node check log

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

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

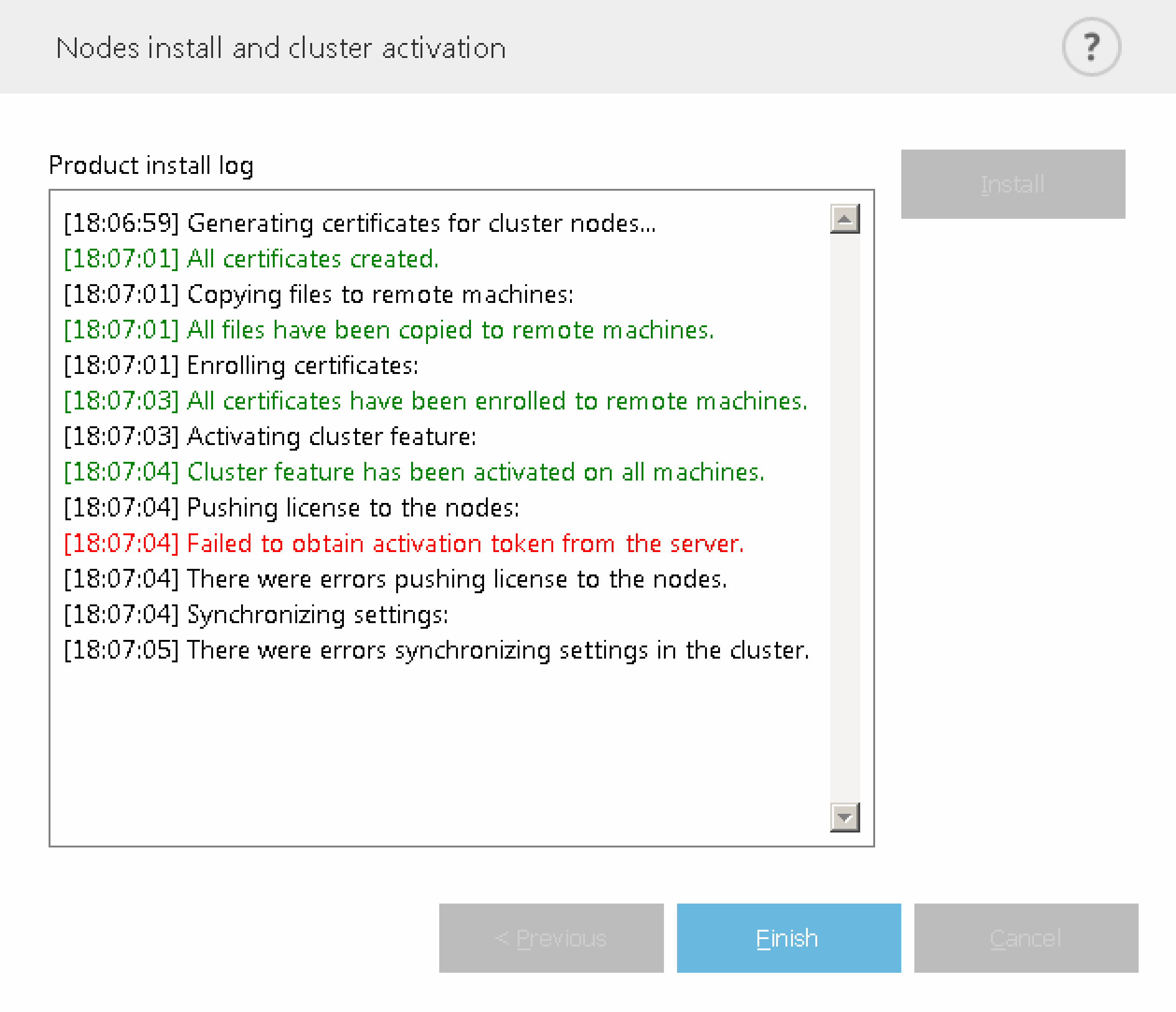


```
[15:53:58] Generating certificates for cluster nodes...
[15:54:01] All certificates created.
[15:54:01] Copying files to remote machines:
[15:54:05] All files have been copied to remote machines.
[15:54:05] Installing product:
[15:55:00] ESET solutions are installed on all remote machines.
[15:55:00]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

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.

IMPORTANT
This step needs to be performed on each server running ESET Security for Microsoft SharePoint. It is due to the security reasons. ESET products does not store SharePoint admin credentials, thus cannot pass the credentials to other servers.

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



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

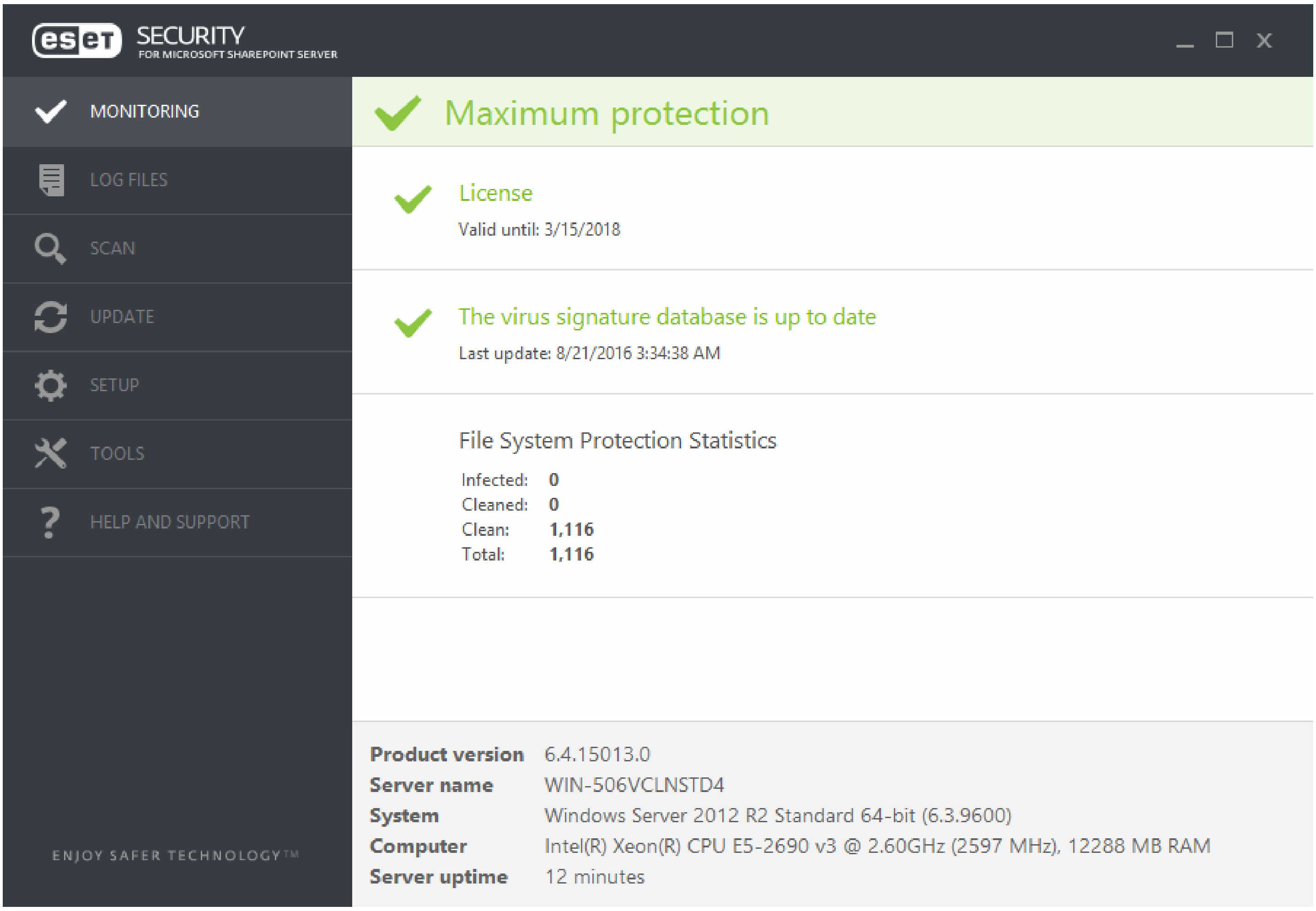
# 7. Beginner's guide

This chapter provides an overview of ESET Security for Microsoft SharePoint, the main parts of the menu, functionalities and basic settings.

## 7.1 Monitoring

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

✓ The green status indicates that **Maximum protection** is ensured. The status window also displays information about the License, Last update and Protection Statistics.



Maximum protection

License

Valid until: 3/15/2018

The virus signature database is up to date

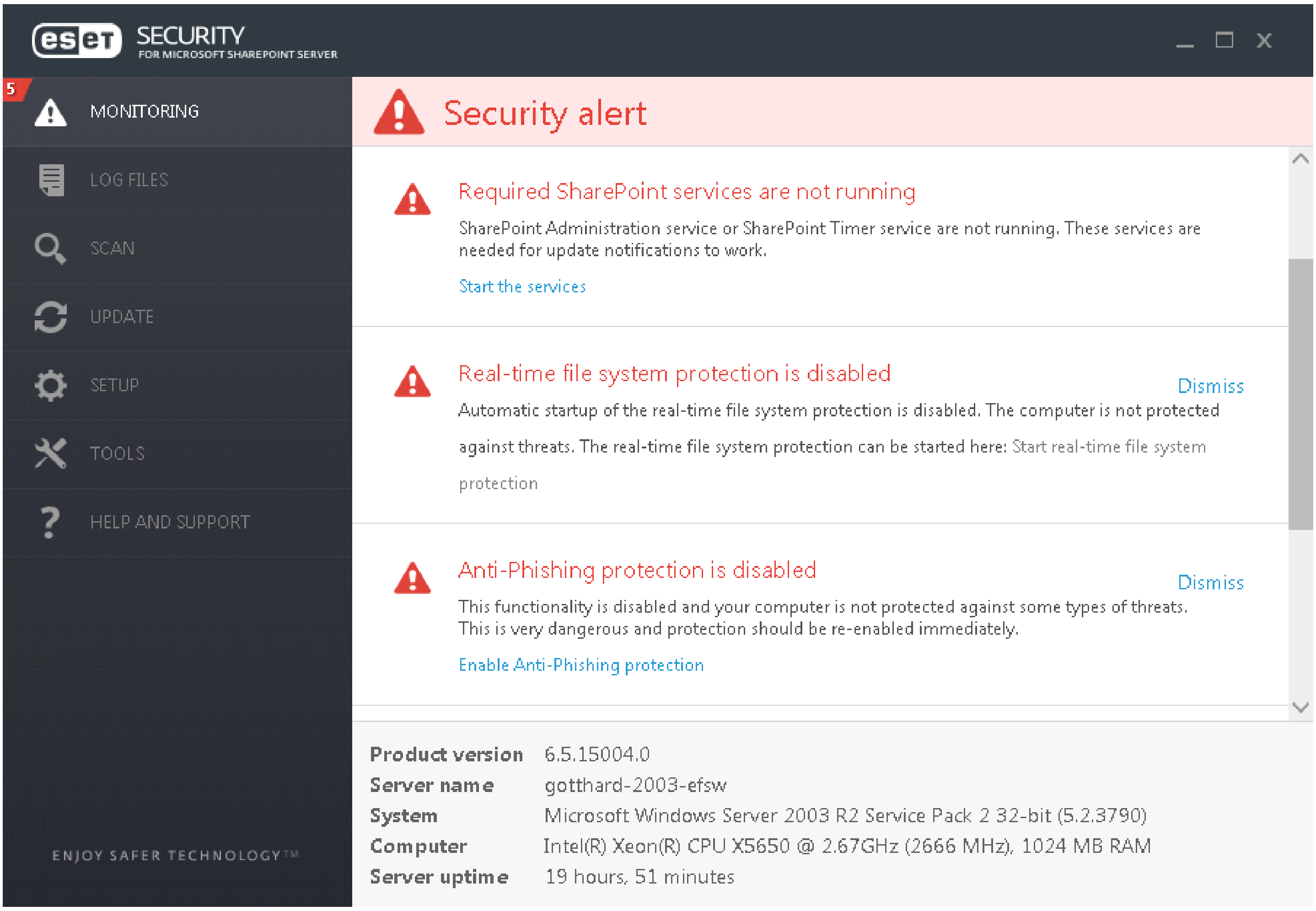
Last update: 8/21/2016 3:34:38 AM

File System Protection Statistics

| | |
|---|---|
| Infected: | 0 |
| Cleaned: | 0 |
| Clean: | 1,116 |
| Total: | 1,116 |

| | |
|---|---|
| **Product version** | 6.4.15013.0 |
| **Server name** | WIN-506VCLNSTD4 |
| **System** | Windows Server 2012 R2 Standard 64-bit (6.3.9600) |
| **Computer** | Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz (2597 MHz), 12288 MB RAM |
| **Server uptime** | 12 minutes |

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



Security alert

Required SharePoint services are not running

SharePoint Administration service or SharePoint Timer service are not running. These services are needed for update notifications to work.

Start the services

Real-time file system protection is disabled

Automatic startup of the real-time file system protection is disabled. The computer is not protected against threats. The real-time file system protection can be started here: Start real-time file system protection

Anti-Phishing protection is disabled

This functionality is disabled and your computer is not protected against some types of threats. This is very dangerous and protection should be re-enabled immediately.

Enable Anti-Phishing protection

| | |
|---|---|
| Product version | 6.5.15004.0 |
| Server name | gotthard-2003-efsw |
| System | Microsoft Windows Server 2003 R2 Service Pack 2 32-bit (5.2.3790) |
| Computer | Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2666 MHz), 1024 MB RAM |
| Server uptime | 19 hours, 51 minutes |

⚠ The red icon indicates critical problems - maximum protection of your computer is not ensured. A red icon will be displayed to signal the following scenarios:

- **Anti-Phishing protection is disabled -** Click **Enable Anti-Phishing protection** in the **Monitoring** tab or re-enable **Anti-Phishing protection** in the Setup tab of the main program window.
- **You are using an outdated virus signature database**.
- **The product is not activated**.
- **Your license is expired** - This is indicated by the protection status icon turning red. The program is not able to update after the license expires. We recommend following the instructions in the alert window to renew your license.

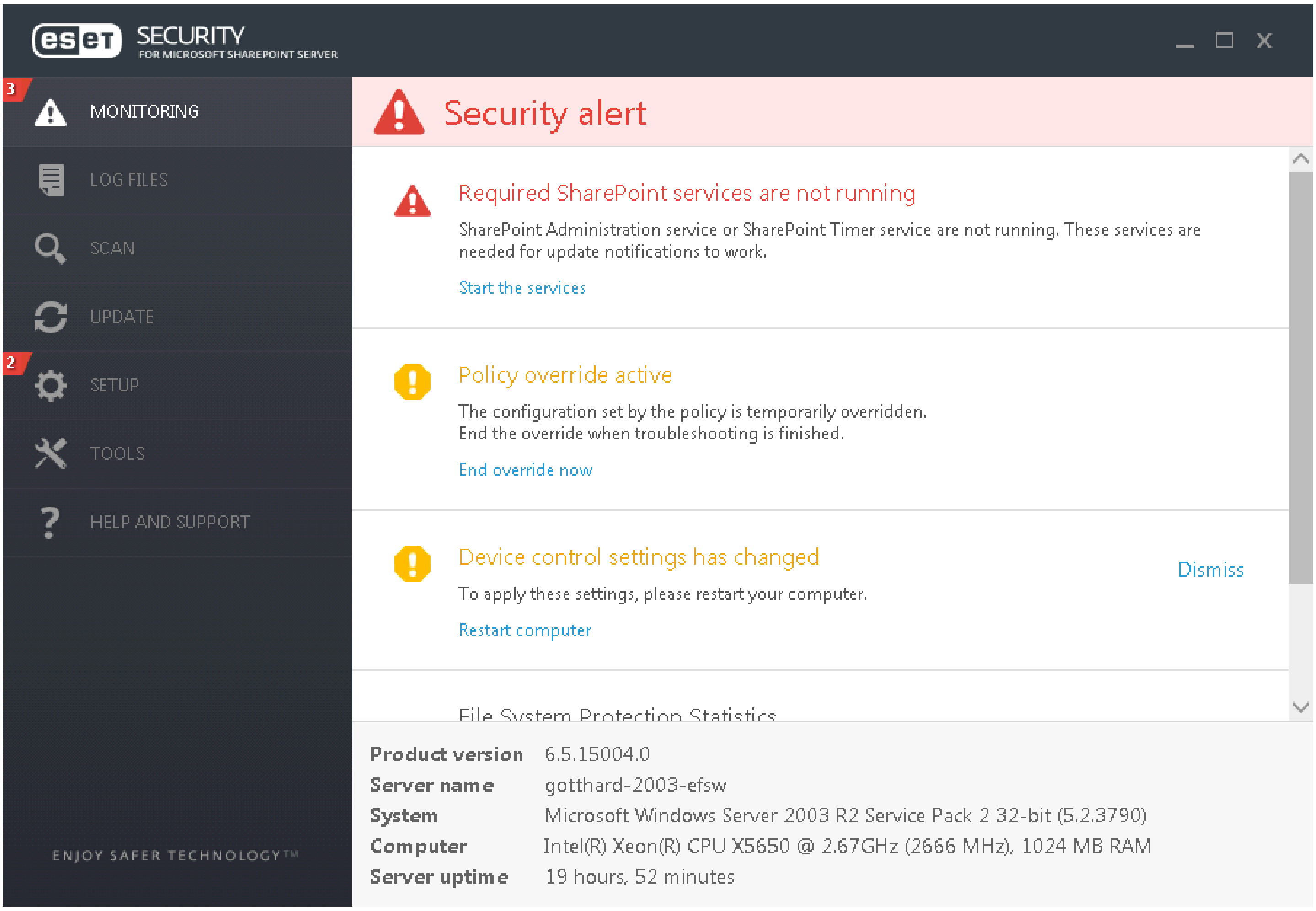
ℹ NOTE
If you are managing ESET Security for Microsoft SharePoint using ERA and have a policy assigned to it, the status link will be locked (grayed out) depending on what features belong to the policy.

❗ The orange icon indicates that your ESET product requires attention for a non-critical problem. An orange icon will be displayed to signal the following scenarios:

- **Web access protection is disabled** - You can re-enable Web access protection by clicking the security notification and then clicking **Enable Web access protection**.

- **Your license will expire soon** - This is indicated by the protection status icon displaying an exclamation point. After your license expires, the program will not be able to update and the Protection status icon will turn red.

- Policy override active - the configuration set by the policy is temporarily overridden, possibly until troubleshooting is complete.



Security alert

Required SharePoint services are not running

SharePoint Administration service or SharePoint Timer service are not running. These services are needed for update notifications to work.

Start the services

Policy override active

The configuration set by the policy is temporarily overridden.
End the override when troubleshooting is finished.

End override now

Device control settings has changed

To apply these settings, please restart your computer.

Restart computer

Dismiss

File System Protection Statistics

| | |
|---|---|
| Product version | 6.5.15004.0 |
| Server name | gotthard-2003-efsw |
| System | Microsoft Windows Server 2003 R2 Service Pack 2 32-bit (5.2.3790) |
| Computer | Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2666 MHz), 1024 MB RAM |
| Server uptime | 19 hours, 52 minutes |

**NOTE**
For a list of possible protection statuses see the Status section.

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, it's basically 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 types of users:

- **Domain** - count of users listed in the SharePoint database who use Windows authentication when logging into SharePoint. Their presence is also verified directly in Active Directory, if it matches, the users are counted. This verification is done in order to avoid counting users who no longer exist within Active Directory, but are still present on the SharePoint list. Such users are not counted.
- **Other** - user count of those who use other forms of authentication (regardless of their presence in Active Directory), for example a Form-based authentication or Claims-based authentication. The count is also based on the user list in SharePoint database.

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

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

### 7.1.1 Status

A status summary for ESET Security for Microsoft SharePoint will be displayed in the primary window with detailed information about your system. Normally, when everything is working without any issues, the protection status is ✓ Green. However, the protection status might change in certain circumstances.

Protection status will change to ❗ Orange or ⚠ Red warning message will be displayed if one of the following occurs:

> ℹ NOTE
> This is a list of SharePoint plug-in messages. There are also other messages, related to file server protection, that might be displayed (not shown in the table below).

| Warning message | Warning message detail |
|---|---|
| **SharePoint not installed** | Installation of Microsoft SharePoint Server was not detected or an unsupported version is installed. Please install one of the supported servers. |
| **SharePoint Server is not supported** | The installed version of  by ESET Security for Microsoft SharePoint in not supported, install one of the supported servers. |
| **SharePoint on-access filter is temporarily disabled** | Microsoft SharePoint Server is not protected against threats and no rule will be applied. Click Enable on-access filter. |
| **SharePoint on-access filter is not in use** | Microsoft SharePoint Server on-access filter is not scanning documents on upload nor on download. Enable upload and download scan. |
| **SharePoint on-access filter is disabled** | Microsoft SharePoint Server is not protected against threats and no rule will be applied. Click Enable on-access filter. |
| **Unable to access SharePoint configuration** | SharePoint administrator account has no access to SharePoint configuration objects. Verify that the SharePoint administrator account is configured properly. |
| **Unable to access SharePoint web site objects** | SharePoint administrator account has no access to SharePoint web site objects. It will not be possible to perform on-demand database scan. Verify that SharePoint administrator account is configured properly. |
| **Unable to access some of the SharePoint web site objects** | SharePoint administrator account has no access to some of the SharePoint web site objects. It will not be possible to perform on-demand database scan of those web sites. |
| **Waiting for Microsoft SharePoint** | ESET Security for Microsoft SharePoint is waiting for Microsoft SharePoint services to become available. Some SharePoint related errors may not be displayed. |
| **Required SharePoint services are not running** | SharePoint Administration service or SharePoint Timer service are not running. These services are needed for update notifications to work. |
| **Invalid SharePoint administrator account** | Provided SharePoint administrator account name does not exist, click change the account. |
| **SharePoint administrator account is not configured** | Click Enable on-access filter. |
| **The SharePoint Helper Service is not running** | The ESET SharePoint Helper Service is stopped or unable to start. SharePoint administrator account is required to run ESET SharePoint Helper Service. Check |

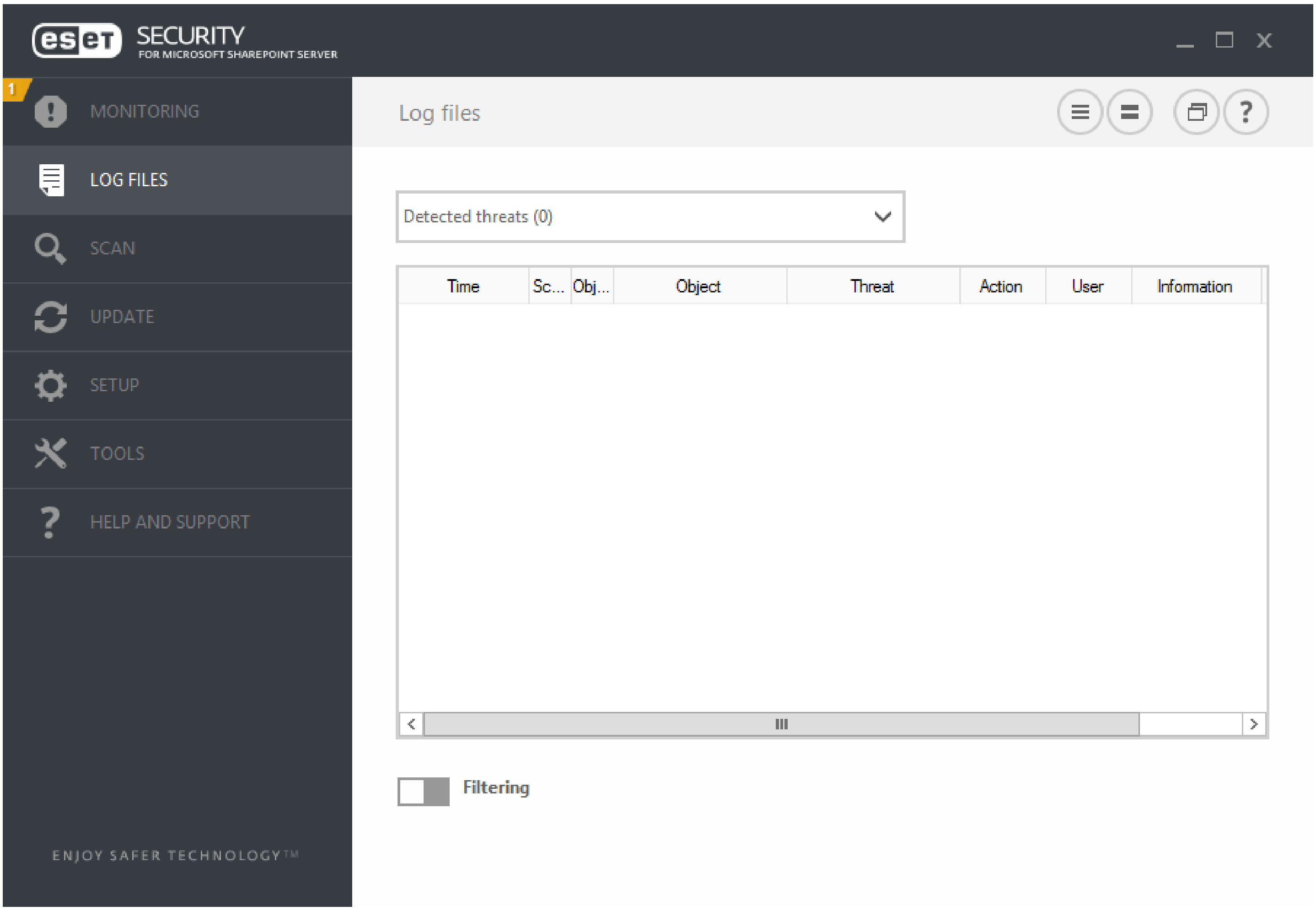
| Warning message | Warning message detail |
|---|---|
|  | if the supplied account credentials are valid and if the account has 'Log on as service' privileges. |

**NOTE**
The last two status messages are deferred for up to 5 minutes after server startup. During this time the ESET SharePoint helper service is being initialized and waits for SharePoint to become available. It usually takes a few seconds, but can take up to 5 minutes if load is high. The end of this initial delay is indicated by the following report in the event log: Initial wait for SharePoint services has finished.

If you are unable to solve a problem, search the ESET Knowledgebase. If you still need assistance, you can submit an ESET Customer Care support request.

## 7.2 Log files

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



Detected threats (0)

| Time | Sc... | Obj... | Object | Threat | Action | User | Information |
|---|---|---|---|---|---|---|---|

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

- **Detected threats** - The threat 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.

- **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.

- **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.

- **Filtered websites** - This list is useful if you want to view a list of websites that were blocked by Web access protection. In these logs you can see the time, URL, user and application that opened a connection to the particular website.

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

- **On-demand database scan** - Contains a list of On-demand database scans of SharePoint content database. For each scan, the following information is displayed: version of the virus signature database, 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.

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

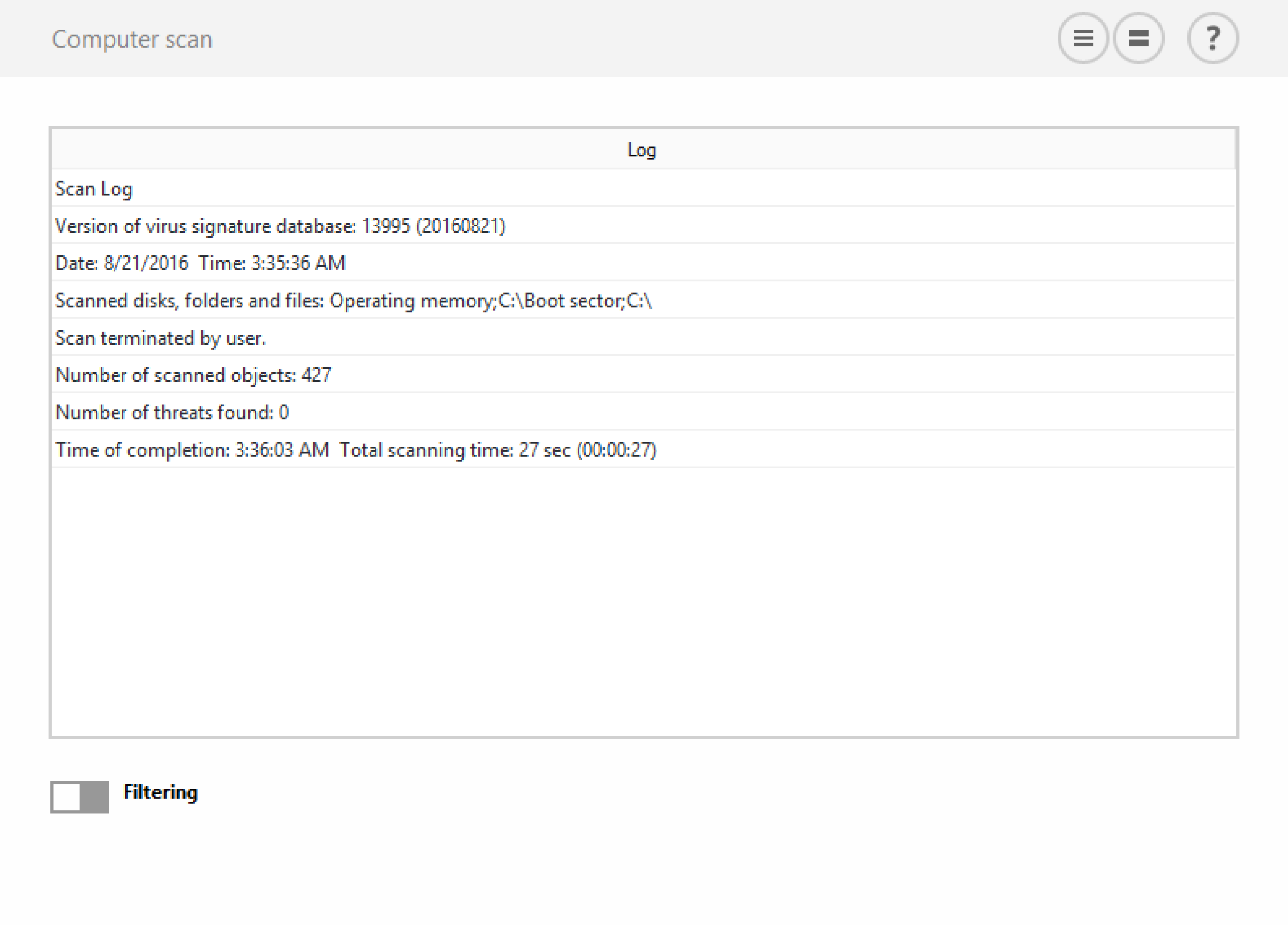
Click the switch icon **Filtering** to open the Log filtering window where you can define the filtering criteria.

You can bring up the context menu by right-clicking a specific record. The following options are available in the context menu:

- **Show** - Shows more detailed information about the selected log in a new window (same as double-click).
- **Filter same records** - This activates log filtering, showing only records of the same type as the one selected.
- **Filter...** - After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.
- **Enable filter** - Activates filter settings. 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.
- **Copy all** - Copies information from all records in the window.
- **Delete** - Deletes selected/highlighted record(s) - this action requires administrator privileges.
- **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.
- **Find next** - Finds the next occurrence of your defined search criteria.
- **Find previous** - Finds the previous occurrence.
- **Scroll log** - Leave this enabled to auto scroll old logs and view active logs in the **Log files** window.

### 7.2.1 Scan log

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



```
Scan Log
Version of virus signature database: 13995 (20160821)
Date: 8/21/2016  Time: 3:35:36 AM
Scanned disks, folders and files: Operating memory;C:\Boot sector;C:\
Scan terminated by user.
Number of scanned objects: 427
Number of threats found: 0
Time of completion: 3:36:03 AM  Total scanning time: 27 sec (00:00:27)
```

**NOTE**

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

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

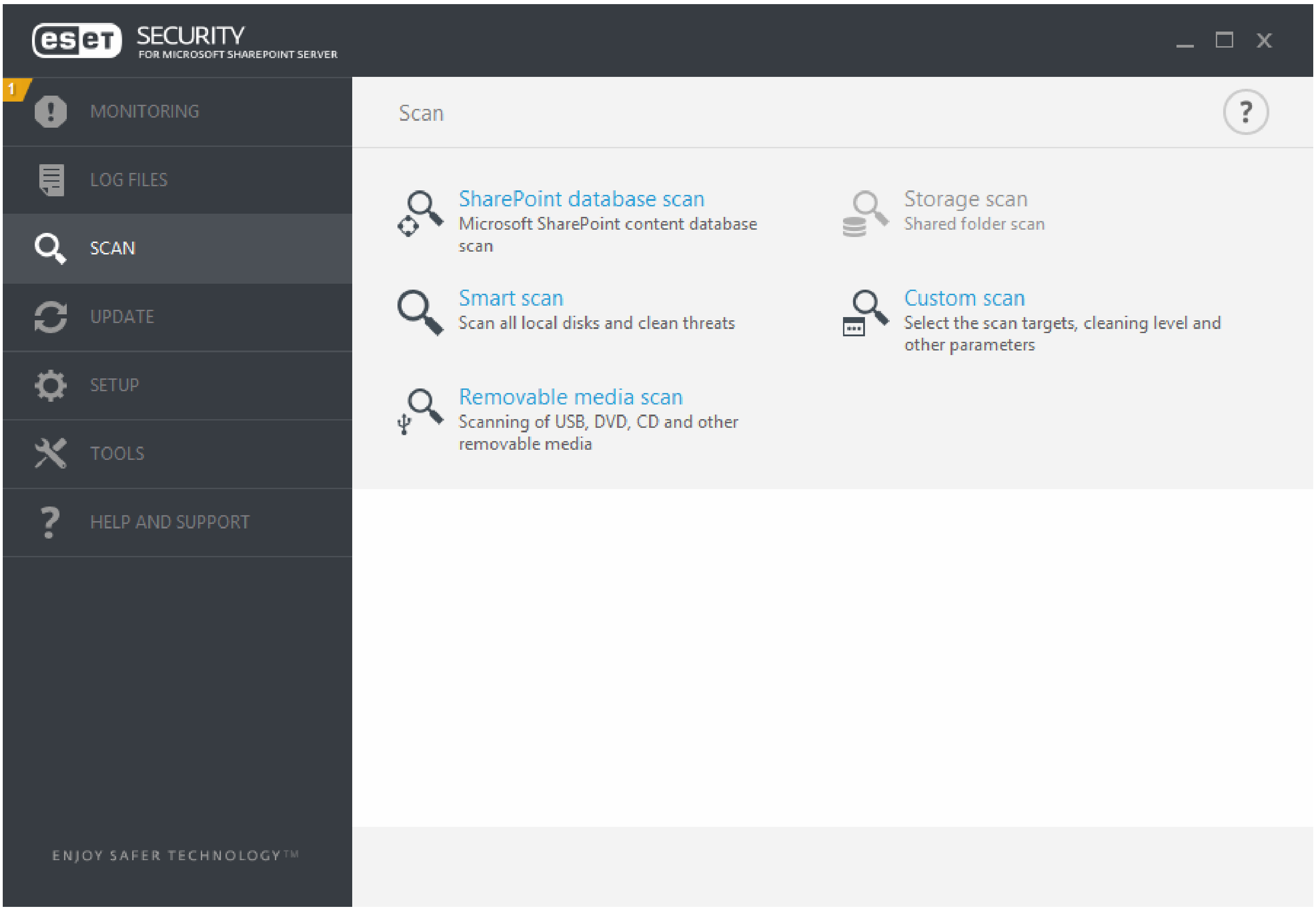
You can bring up the context menu by right-clicking a specific record. The following options are available in the context menu:

- **Show** - Shows more detailed information about the selected log in a new window (same as double-click).
- **Filter same records** - This activates log filtering, showing only records of the same type as the one selected.
- **Filter...** - After clicking this option, the Log filtering window will allow you to define filtering criteria for specific log entries.
- **Enable filter** - Activates filter settings. 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.
- **Copy all** - Copies information from all records in the window.
- **Delete** - Deletes selected/highlighted record(s) - this action requires administrator privileges.
- **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.

- **Find next** - Finds the next occurrence of your defined search criteria.
- **Find previous** - Finds the previous occurrence.
- **Scroll log** - Leave this enabled to auto scroll old logs and view active logs in the **Log files** window.

## 7.3 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 virus signature database has not been updated, or if a file was not detected when it was first saved to the disk.



SharePoint database scan
Microsoft SharePoint content database scan

Storage scan
Shared folder scan

Smart scan
Scan all local disks and clean threats

Custom scan
Select the scan targets, cleaning level and other parameters

Removable media scan
Scanning of USB, DVD, CD and other removable media

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

See Scan progress for more information about the scanning process.

**SharePoint database scan**

Lets you select SharePoint Web sites that you want to scan and run the scanning process. Additionally, you can use Scheduler to run a SharePoint database scan at a specific time or at an event.

**Storage scan**

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

**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 particular VM. See Hyper-V scan for more information (including supported host operating systems and limitations).

### Smart scan

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

### Custom scan

Custom scan is an optimal solution if you want to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure 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.

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

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

### Removable media scan

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

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

### Repeat last scan

Repeats your last scan operation using the exact same settings.

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

## 7.3.1 Hyper-V scan

This type of scan allows you to scan the disks of a Microsoft Hyper-V Server, which is a virtual machine (VM), without the need to have any Agent installed on the VM. The ESET security is installed using Administrative privileges for the Hyper-V server.

### Supported Host Operating Systems with the Hyper-V role

- Windows Server 2008 R2 - Virtual Machines can be scanned only while they are offline
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

### 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 is not supported due to the nature of Dynamic Disks. Therefore, we recommend that you avoid using the Dynamic Disk type in your VMs if possible.
- Scanning is always performed 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.
- Virtual Machines on a Hyper-V host running on Windows Server 2008 R2 can only be scanned in read-only mode (**No cleaning**), regardless of what cleaning level is selected in ThreatSense parameters.

ℹ NOTE
While ESET Security supports the scan of virtual disk MBRs, read-only scanning is the only method supported for these targets. This setting can be changed in **Advanced setup** > **Antivirus** > **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 content of the virtual disks it does when accessing data and files on any generic drive.

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

ESET Security for Microsoft SharePoint uses Hyper-V Management to detect virtual disks. Actual connection to these the disks is not possible. Therefore, ESET Security for Microsoft SharePoint creates a checkpoint/snapshot of the Virtual Machine, then connects to the checkpoint/snapshot. Once the scan is completed, the checkpoint/snapshot is deleted. This means that read-only scan can be performed because the running Virtual Machine(s) are unaffected by scan activity.

Allow up to one minute for ESET Security to create a snapshot or checkpoint during scanning. You should take this into account when running a Hyper-V scan on a larger number of Virtual Machines.

**Naming convention**

The module of Hyper-V Scan uses the following naming convention:
`VirtualMachineName\DiskX\VolumeY`

where X is the number of disks and Y is the number of volumes.
for example, “`Computer\Disk0\Volume1`”.

The number suffix is added based on the order of detection, and is identical to the order seen in the Disk Manager of the VM.
This naming convention is used in the tree-structured list of targets to be scanned, in the progress bar and also in the log files.

**Executing a scan**

A scan can be executed 3 ways:

- 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**.
- Via the scheduler
- Via ESET Remote Administrator as a Client Task called Server Scan.

It is possible to execute several Hyper-V scans simultaneously.

You will receive a notification with a link to log files when a scan is complete.

**Possible issues**

- When executing the scan of an online Virtual Machine, a checkpoint/snapshot of the particular Virtual Machine has to be created and during the creation of a checkpoint/snapshot some generic actions of the Virtual Machine might be limited or disabled.

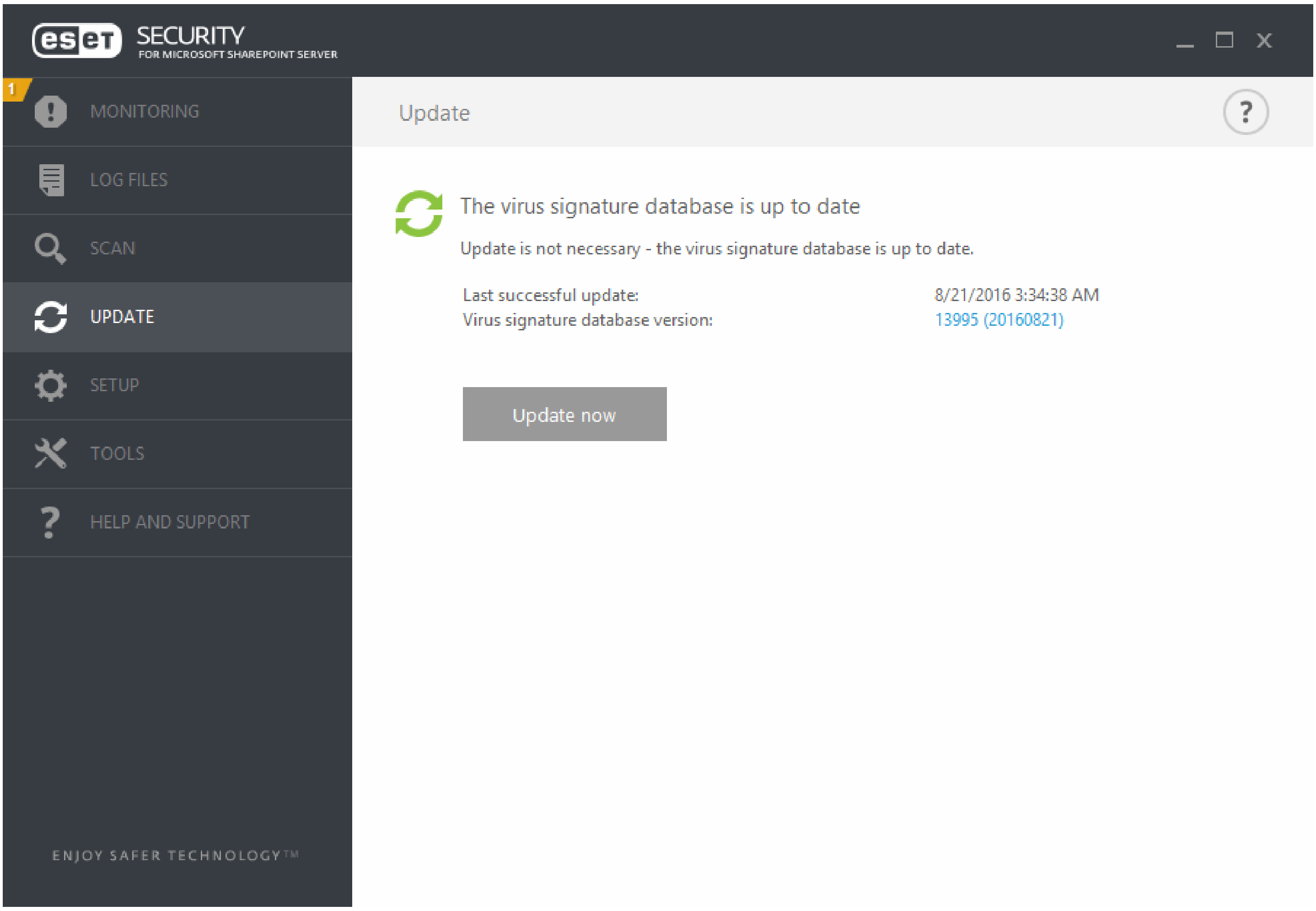
- If an offline Virtual Machine is being scanned, it cannot be turned on until the scan is finished.
- Hyper-V Manager allows you to name two different Virtual Machines identically and this presents an issue when trying to differentiate the machines while reviewing the scan logs.

## 7.4 Update

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

Click Update in the main program window to view the current update status of your system, including the date and time of the last successful update. The primary window also contains the virus signature database version. The update version number is an active link to information about signatures added in the given update.

Click **Update now** to check for updates. Updating the virus signature database and updating program components are important parts of maintaining complete protection against malicious code.



The virus signature database is up to date

Update is not necessary - the virus signature database is up to date.

Last successful update: 8/21/2016 3:34:38 AM
Virus signature database version: 13995 (20160821)

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

**Virus signature database version** - The virus signature database number, which is also an active link to the ESET website. Click this to view a list of all signatures added in a given update.

### Update process

After clicking **Update now**, the download process begins and the progress of the update is displayed. To interrupt the update click **Cancel update**.

IMPORTANT
Under normal circumstances, when updates are downloaded properly the message **Update is not necessary - the**

**virus signature database is up to date** will appear in the **Update** window. If this is not the case, the program is out of date and more vulnerable to infection.

Please update the virus signature database as soon as possible. Otherwise, one of the following messages will be displayed:

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

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

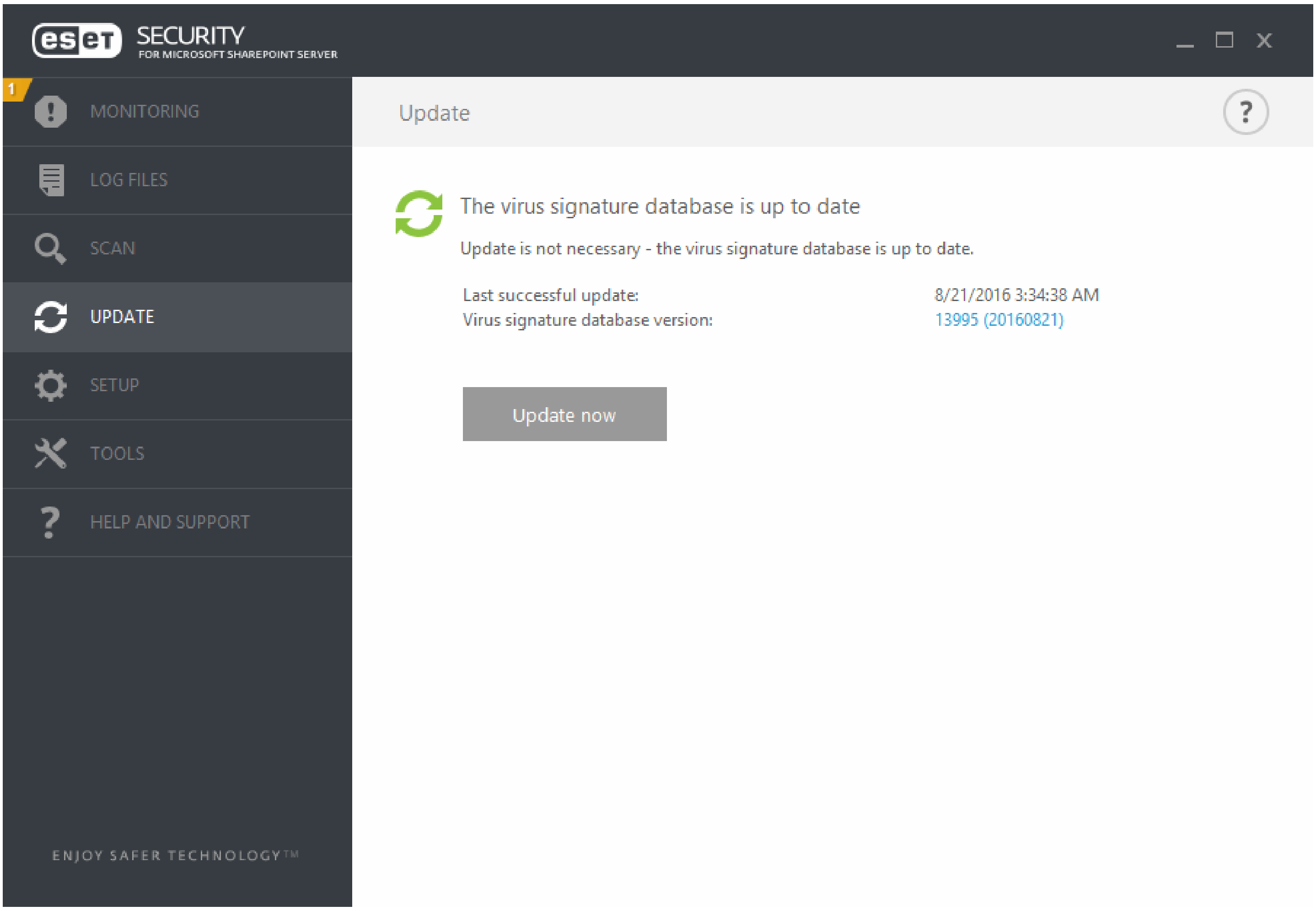
**Invalid license** - The license key has been entered incorrectly in update setup. We recommend that you check your authentication data. The **Advanced setup** window (press **F5** on your keyboard) contains additional update options. Click **Help and support** > **Manage license** from the main menu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

**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.

ℹ NOTE
For more information please visit this Knowledgebase article.

### 7.4.1 Setting up virus DB update

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



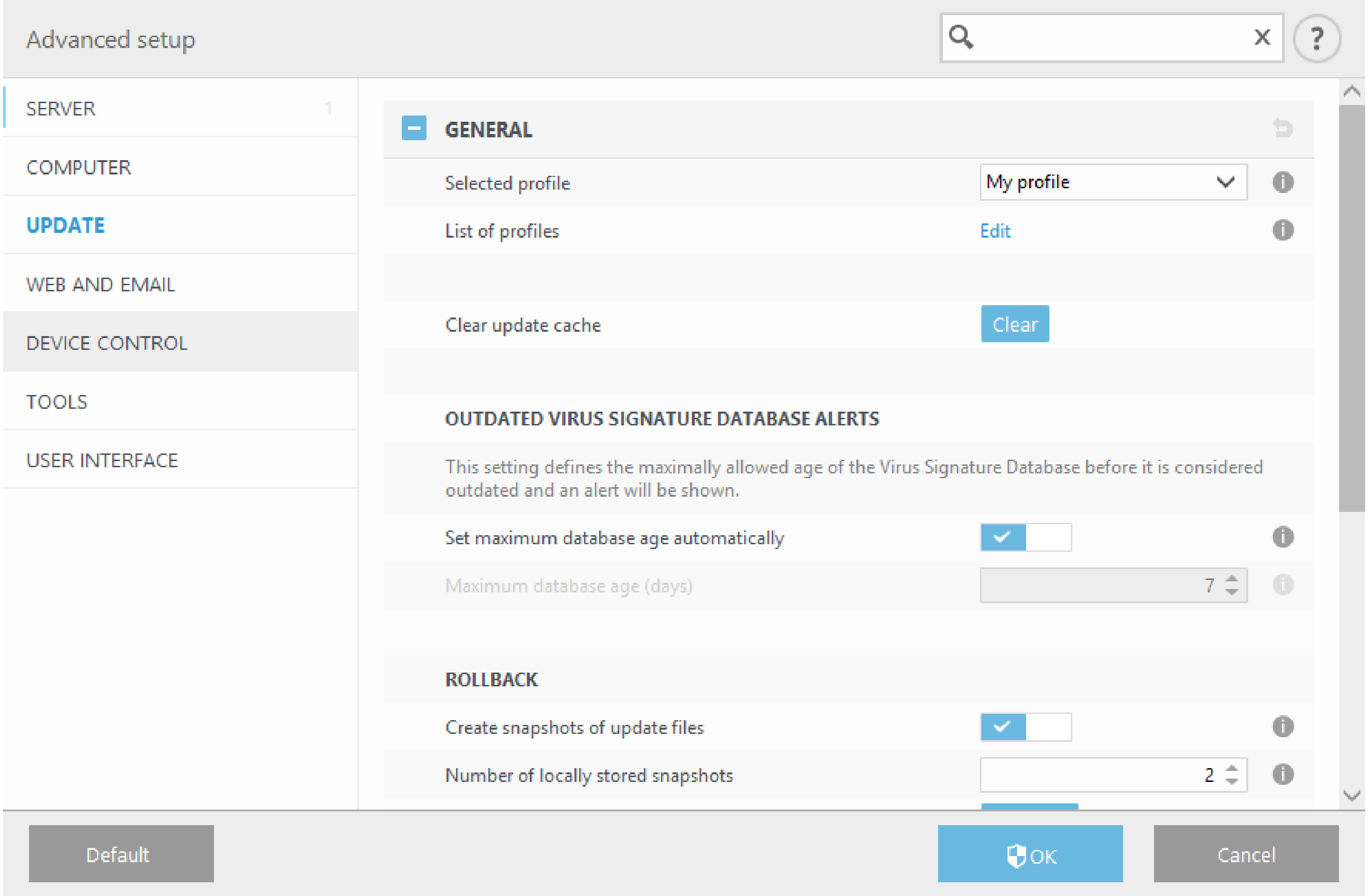
The virus signature database is up to date

Update is not necessary - the virus signature database is up to date.

Last successful update: 8/21/2016 3:34:38 AM

Virus signature database version: 13995 (20160821)

You can configure update settings from the **Advanced setup** window (press the **F5** key on your keyboard). To configure advanced update options such as the update mode, proxy server access, LAN connection and virus signature copy settings (Mirror), click **Update** > **Profiles**. If you experience problems with an update, click **Clear** to clear the temporary update cache.



GENERAL

Selected profile: My profile

List of profiles: Edit

Clear update cache: Clear

OUTDATED VIRUS SIGNATURE DATABASE ALERTS

This setting defines the maximally allowed age of the Virus Signature Database before it is considered outdated and an alert will be shown.

Set maximum database age automatically: ✓

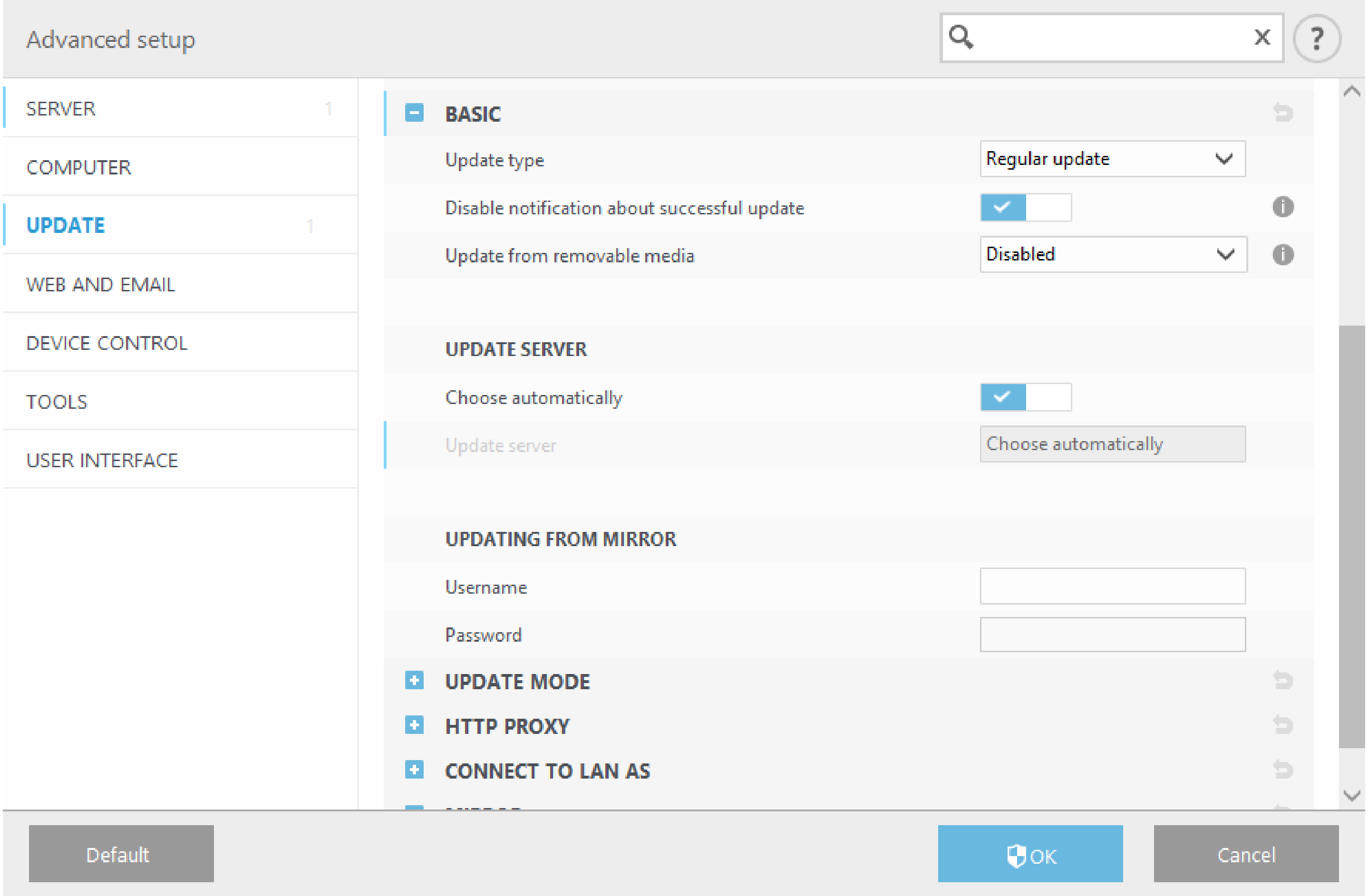
Maximum database age (days): 7

ROLLBACK

Create snapshots of update files: ✓

Number of locally stored snapshots: 2

The **Update server** menu is set to **Choose automatically** by default. **Choose automatically** means that the update server, from which the virus signature updates are downloaded, is chosen automatically. We recommend that you leave the default option selected. If you do not want the the system tray notification at the bottom right corner of the screen to appear, select **Disable display notification about successful update**.



BASIC

Update type: Regular update

Disable notification about successful update: ✓

Update from removable media: Disabled

UPDATE SERVER

Choose automatically: ✓

Update server: Choose automatically

UPDATING FROM MIRROR

Username

Password

UPDATE MODE

HTTP PROXY

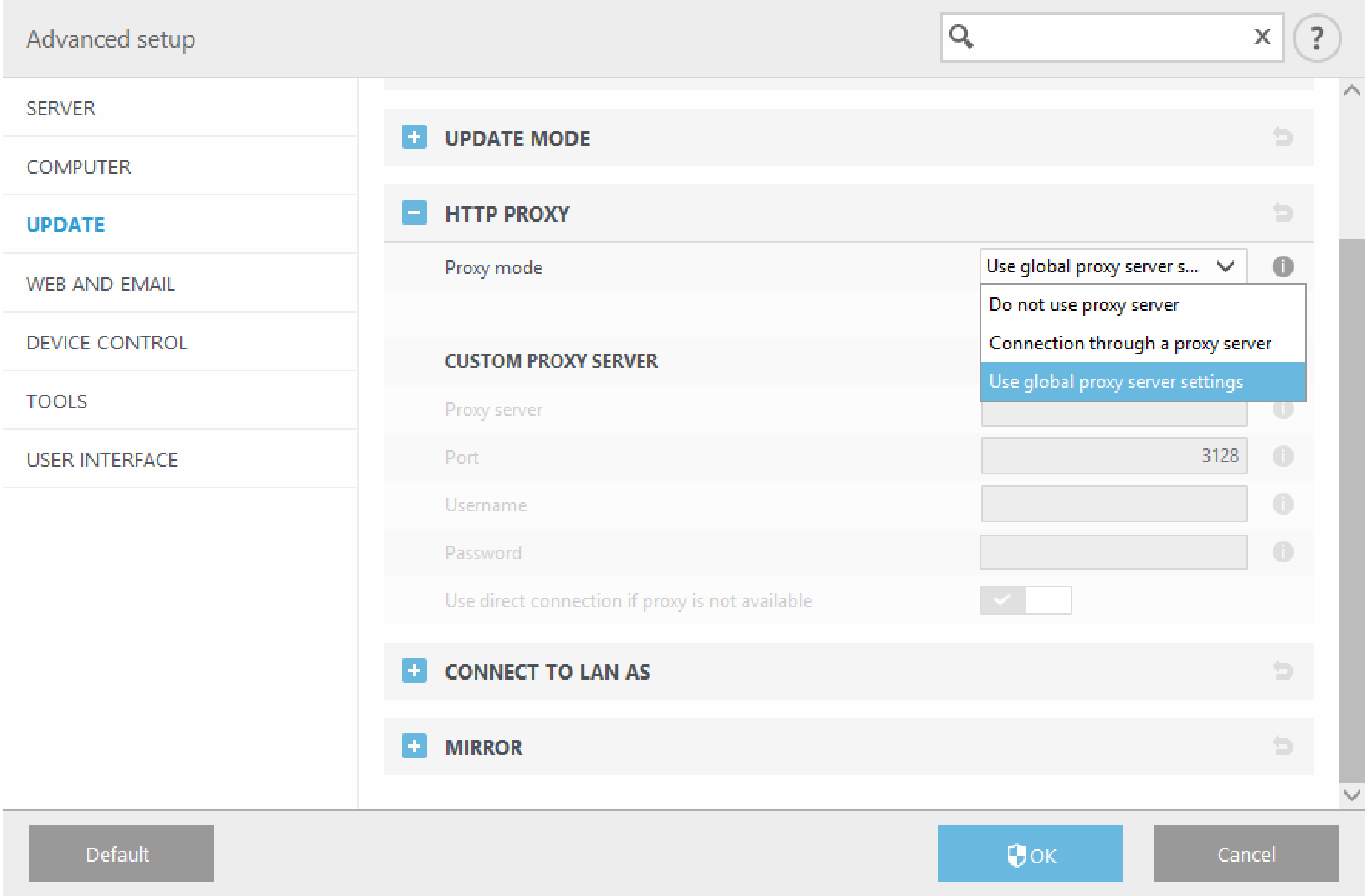
CONNECT TO LAN AS

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

If you did not activate your product following installation, you can do so at any time. For more detailed information about activation see How to activate ESET Security for Microsoft SharePoint and enter the license data you received with your ESET security product into the License details window.

### 7.4.2 Configuring Proxy server for updates

If you use a proxy server for the Internet connection on a system where ESET Security for Microsoft SharePoint is installed, proxy settings must be configured in **Advanced setup**. To access the proxy server configuration window, press **F5** to open the Advanced setup window and click **Update** > **Profiles** > **HTTP proxy**. Select **Connection through a proxy server** from the **Proxy mode** drop-down menu and fill in your proxy server details: **Proxy server** (IP address), **Port** number and **Username** and **Password** (if applicable).



Proxy mode: Use global proxy server s...

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

CUSTOM PROXY SERVER

Proxy server:

Port: 3128

Username:

Password:

Use direct connection if proxy is not available: ✓

If you are unsure about proxy server details, you can select **Use global proxy server settings** from the drop-down list to auto-detect your proxy settings.

**NOTE**

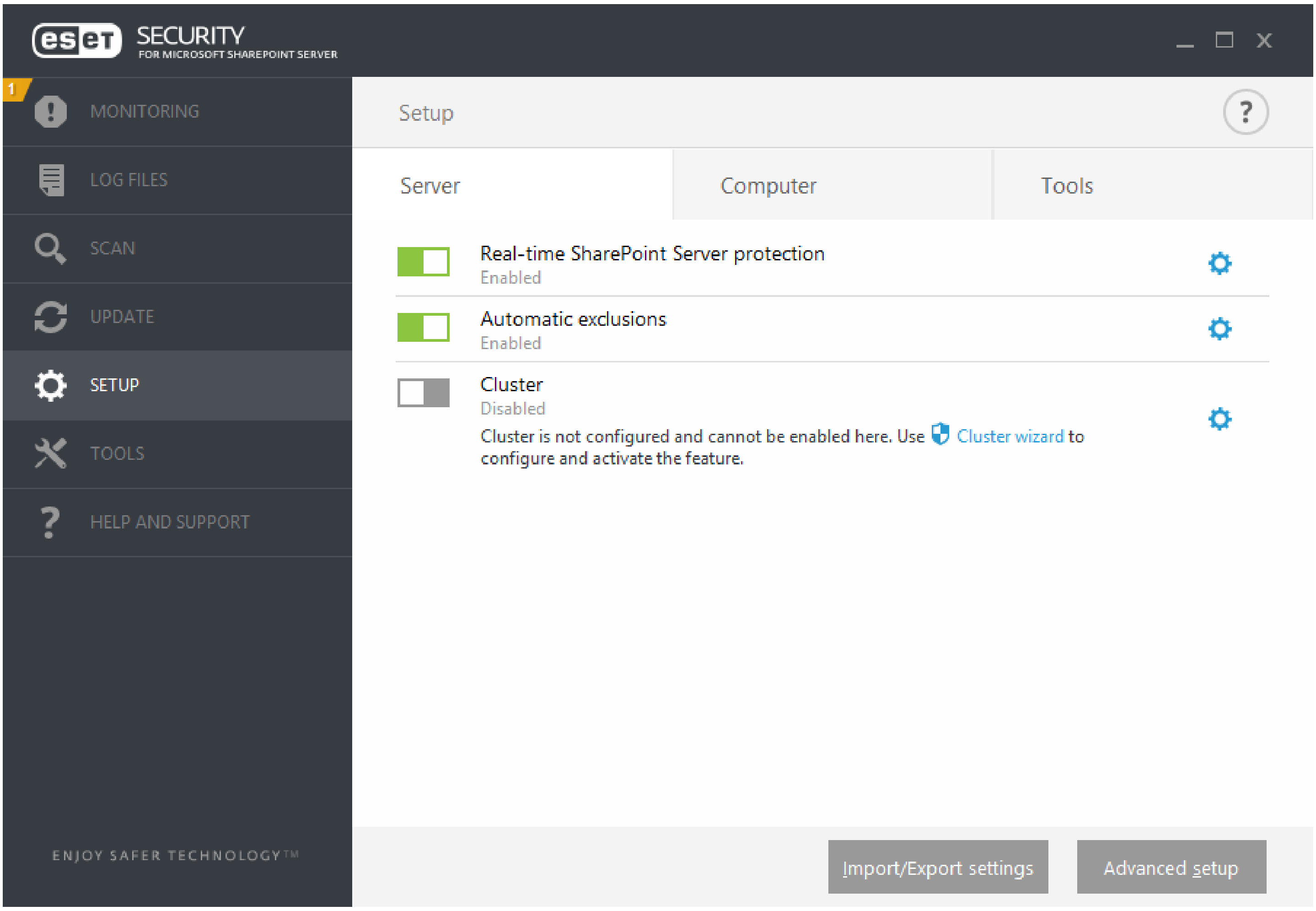
Proxy server options for various update profiles may differ. If this is the case, configure the different update profiles in **Advanced setup** by clicking **Update** > **Profile**.

**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.

## 7.5 Setup

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

- Server
- Computer
- Tools



Real-time SharePoint Server protection
Enabled

Automatic exclusions
Enabled

Cluster
Disabled
Cluster is not configured and cannot be enabled here. Use Cluster wizard to configure and activate the feature.

To temporarily disable individual modules, click the green switch 🟩 next to the desired module. Note that this may decrease the protection level of your computer.
To re-enable the protection of a disabled security component, click the red switch 🟥 to return a component to its enabled state.
To access detailed settings for a particular security component, click the gear icon ⚙.

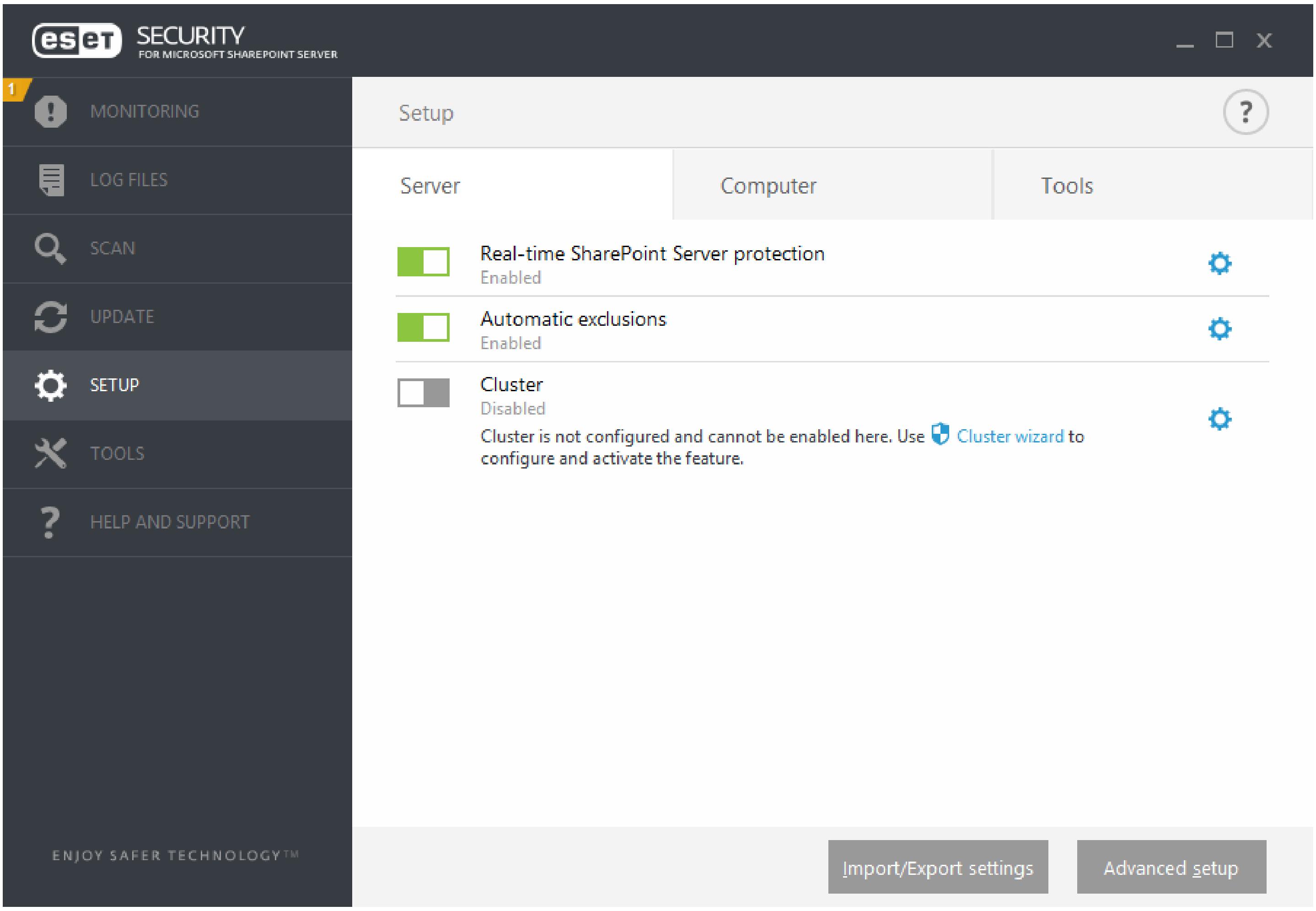
Click **Advanced setup** or press **F5** to configure advanced settings.

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

### 7.5.1 Server

You'll see a list of components which you can enable/disable using the switch 🟩. 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 antivirus software.
- To set up the ESET Cluster click **Cluster wizard**. For details on how to set up the ESET Cluster using the wizard, click here.



Real-time SharePoint Server protection
Enabled

Automatic exclusions
Enabled

Cluster
Disabled
Cluster is not configured and cannot be enabled here. Use Cluster wizard to configure and activate the feature.

If you want to set more detailed options, click **Advanced setup** or press **F5**.

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

### 7.5.2 Computer

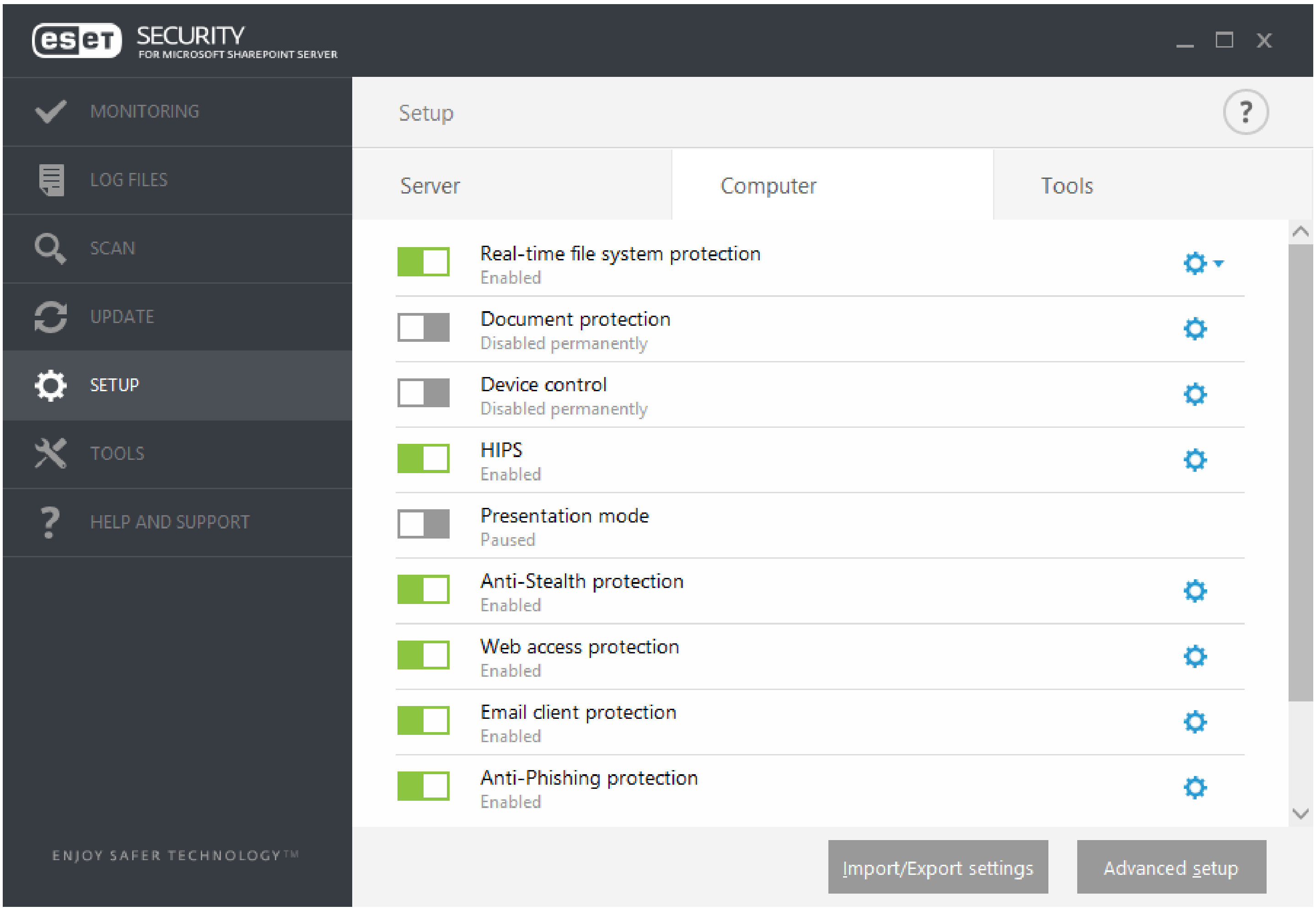
ESET Security for Microsoft SharePoint has all of the necessary components to ensure significant protection of the server as a computer. Each component provides a specific type of protection, such as: Antivirus and Antispyware, Real-time file system protection, Web-access, Email client, Anti-Phishing protection, etc.

The **Computer** section can be found under **Setup** > **Computer**. You'll see a list of components which you can enable/ disable using the switch 🟩. To configure settings for a specific item, click the gear icon ⚙.

For **Real-time file system protection**, there is also an option to **Edit exclusions**, which will open the exclusions setup window where you can exclude files and folders from scanning.

**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**.

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



Real-time file system protection
Enabled

Document protection
Disabled permanently

Device control
Disabled permanently

HIPS
Enabled

Presentation mode
Paused

Anti-Stealth protection
Enabled

Web access protection
Enabled

Email client protection
Enabled

Anti-Phishing protection
Enabled

- **Real-time file system protection** - All files are scanned for malicious code when they are opened, created or run on your computer.
- **Document protection** - The document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer, such as Microsoft ActiveX elements.

**NOTE**
Document protection is disabled by default. If you want, you can easily enable it by clicking the switch icon.

- **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.
- **HIPS** - The HIPS system monitors events that occur within the operating system and reacts to them according to a customized set of rules.

- **Presentation mode** - A feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. You will receive a warning message (potential security risk) and the main program window will turn orange after enabling Presentation mode.
- **Anti-Stealth protection** - Provides detection of dangerous programs, such as rootkits, which are able to hide themselves from the operating system. This means it is not possible to detect them using ordinary testing techniques.
- **Web access protection** - If enabled, all HTTP or HTTPS traffic is scanned for malicious software.
- **Email client protection** - Monitors communication received through the POP3 and IMAP protocols.
- **Anti-Phishing protection -** Protects you from attempts to acquire passwords, banking data and other sensitive information by illegitimate websites disguised as legitimate ones.

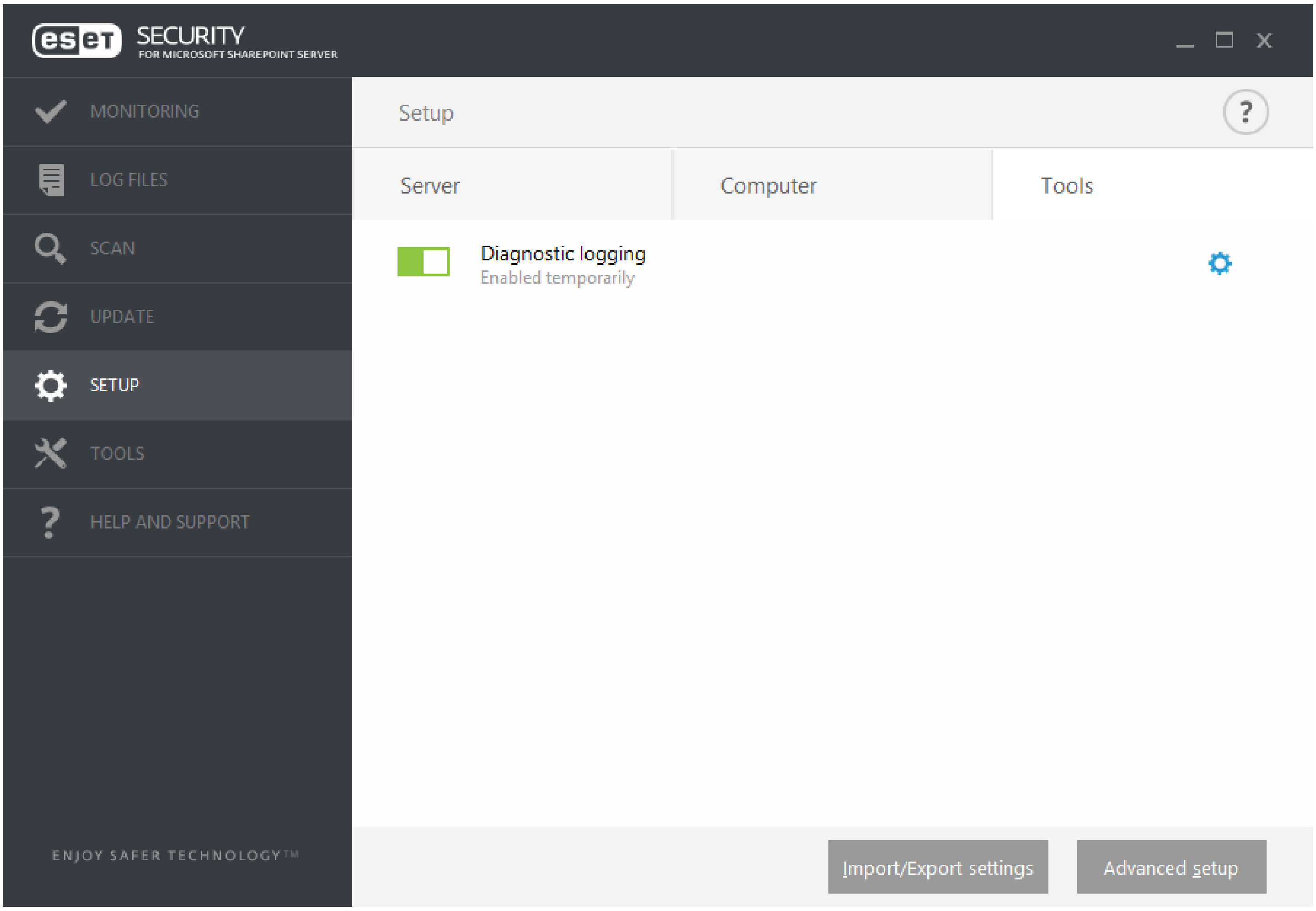
There are additional options at the bottom of the setup window. To load setup parameters using an *.xml* configuration file, or to save the current setup parameters to a configuration file, use **Import/Export settings**. Please see Import/Export settings for more detailed information.

If you want to set more detailed options, click **Advanced setup** or press **F5**.

### 7.5.3 Tools

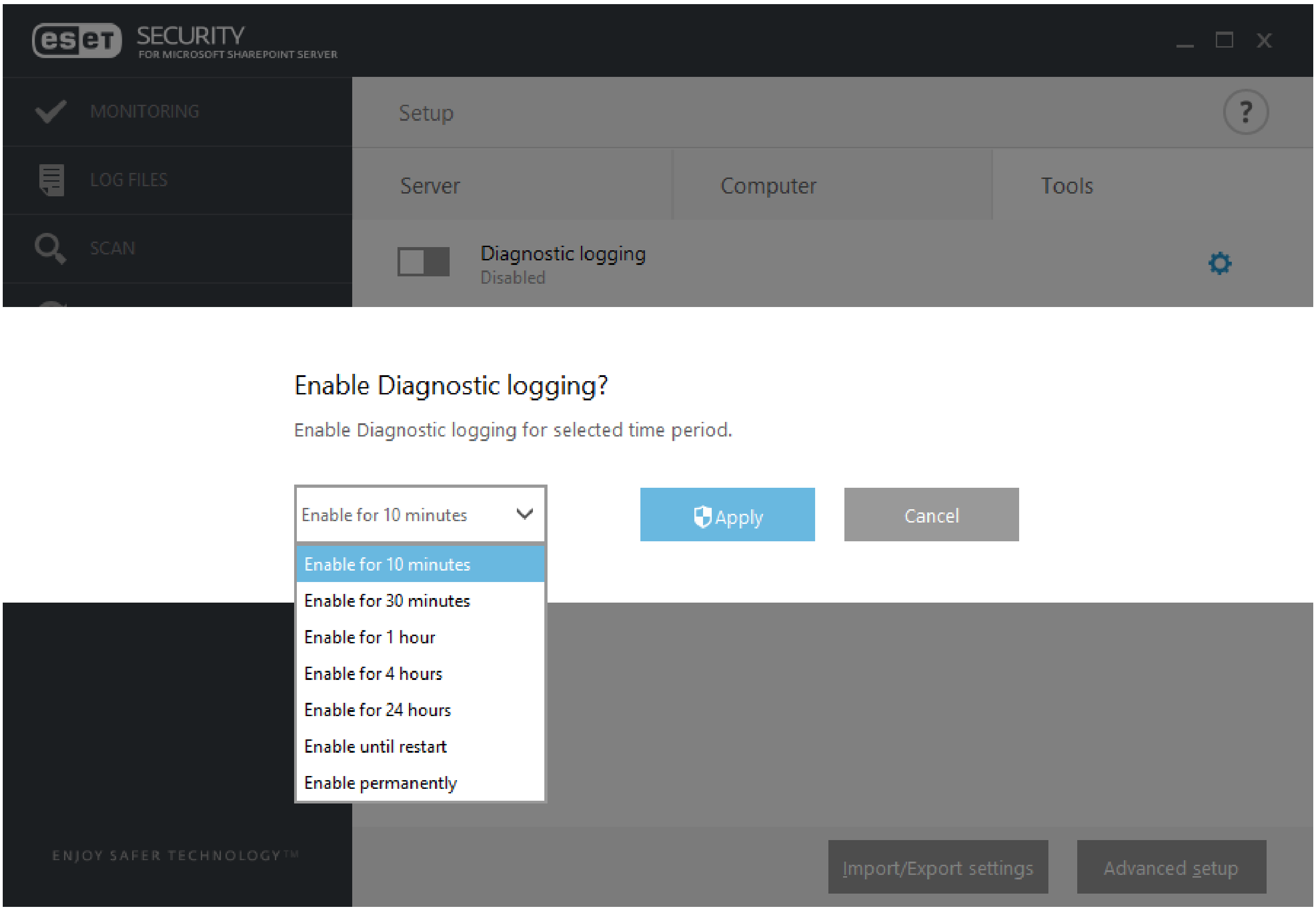
**Diagnostic logging** - when you click the switch to enable diagnostic logging, you can choose for how long it will be enabled (10 minutes, 30 minutes, 1 hour, 4 hours, 24 hours, until next server restart or permanently).

When you click the gear icon ⚙, the **Advanced setup** window where you can configure which components will write diagnostic logs (when diagnostic logging is enabled) will open.



Diagnostic logging
Enabled temporarily

- **Enable** Diagnostic logging for selected time period.



Enable Diagnostic logging?

Enable Diagnostic logging for selected time period.

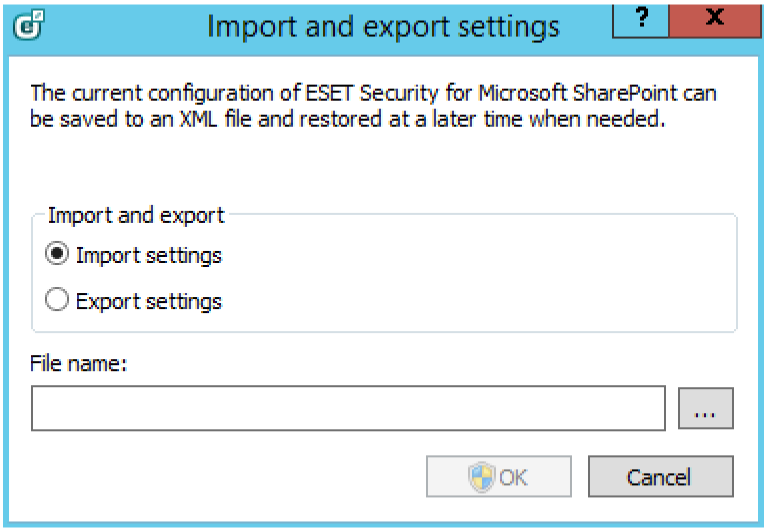
Enable for 10 minutes

- Enable for 10 minutes
- Enable for 30 minutes
- Enable for 1 hour
- Enable for 4 hours
- Enable for 24 hours
- Enable until restart
- Enable permanently

### 7.5.4 Import and export settings

Click **Setup** > **Import/Export settings** to access import/export settings for your ESET Security for Microsoft SharePoint.

Both import and export use the *.xml* file type. Import and export are useful if you need to back up the current configuration of ESET Security for Microsoft SharePoint. It can be used later to apply the same settings to other computer(s).



Import and export settings

The current configuration of ESET Security for Microsoft SharePoint can be saved to an XML file and restored at a later time when needed.

Import and export

● Import settings

○ Export settings

File name:

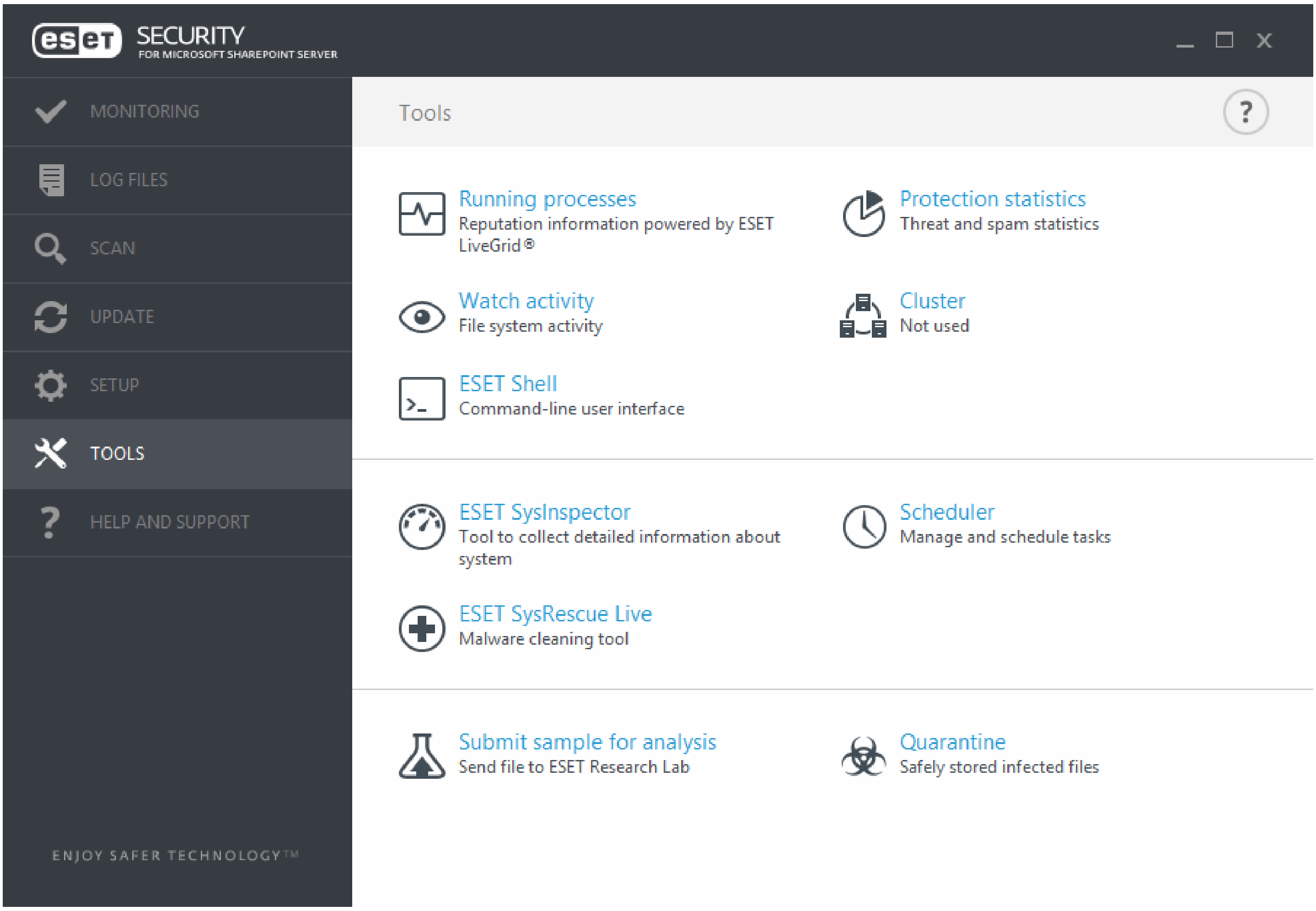
ℹ NOTE

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

## 7.6 Tools

The Tools menu includes modules that help simplify program administration and offer additional options. It includes the following tools:

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



Running processes
Reputation information powered by ESET LiveGrid®

Protection statistics
Threat and spam statistics

Watch activity
File system activity

Cluster
Not used

ESET Shell
Command-line user interface

ESET SysInspector
Tool to collect detailed information about system

Scheduler
Manage and schedule tasks

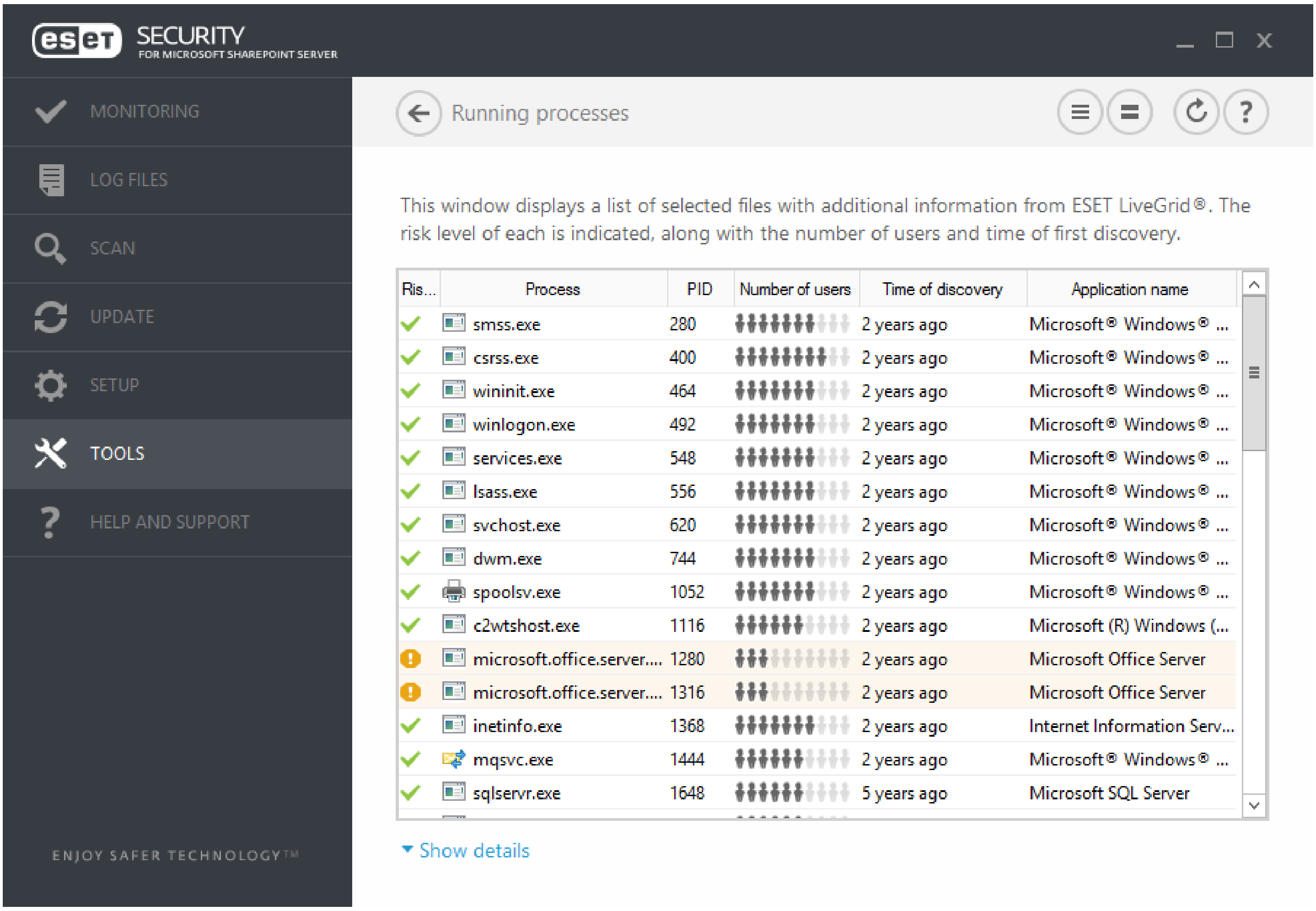
ESET SysRescue Live
Malware cleaning tool

Submit sample for analysis
Send file to ESET Research Lab

Quarantine
Safely stored infected files

### 7.6.1 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.



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

| Ris... | Process | PID | Number of users | Time of discovery | Application name |
|---|---|---|---|---|---|
| ✓ | smss.exe | 280 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | csrss.exe | 400 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | wininit.exe | 464 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | winlogon.exe | 492 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | services.exe | 548 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | lsass.exe | 556 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | svchost.exe | 620 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | dwm.exe | 744 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | spoolsv.exe | 1052 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | c2wtshost.exe | 1116 | | 2 years ago | Microsoft (R) Windows (... |
| ! | microsoft.office.server.... | 1280 | | 2 years ago | Microsoft Office Server |
| ! | microsoft.office.server.... | 1316 | | 2 years ago | Microsoft Office Server |
| ✓ | inetinfo.exe | 1368 | | 2 years ago | Internet Information Serv... |
| ✓ | mqsvc.exe | 1444 | | 2 years ago | Microsoft® Windows® ... |
| ✓ | sqlservr.exe | 1648 | | 5 years ago | Microsoft SQL Server |

**Risk level** - In most cases, ESET Security for Microsoft SharePoint and ESET LiveGrid technology assign risk levels to objects (files, processes, registry keys, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1- Fine (green) to 9- Risky (red).

**Process** - Image name of the program or process that is currently running on your computer. You can also use the Windows Task Manager to see all running processes on your computer. You can open Task Manager by right-clicking an empty area on the taskbar and then clicking Task Manager, or by pressing **Ctrl+Shift+Esc** on your keyboard.

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

NOTE
Known applications marked as Fine (green) are definitely clean (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.

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

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

NOTE
When an application is marked as Unknown (orange), it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, use the Submit sample for analysis feature to send the file

to the ESET Virus Lab. If the file turns out to be a malicious application, its detection will be added to one of the upcoming Virus Signature Database updates.

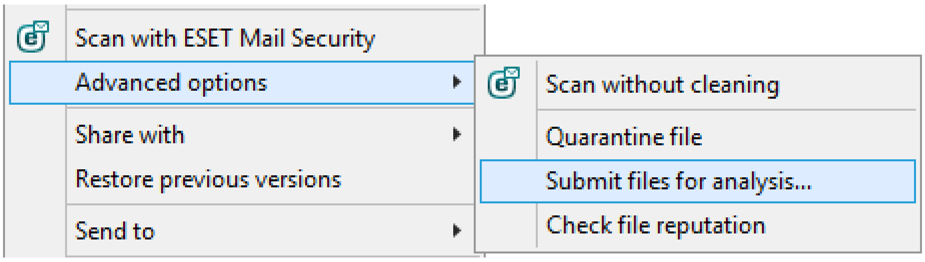
**Application name** - Given name of a program this process belongs to.

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

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

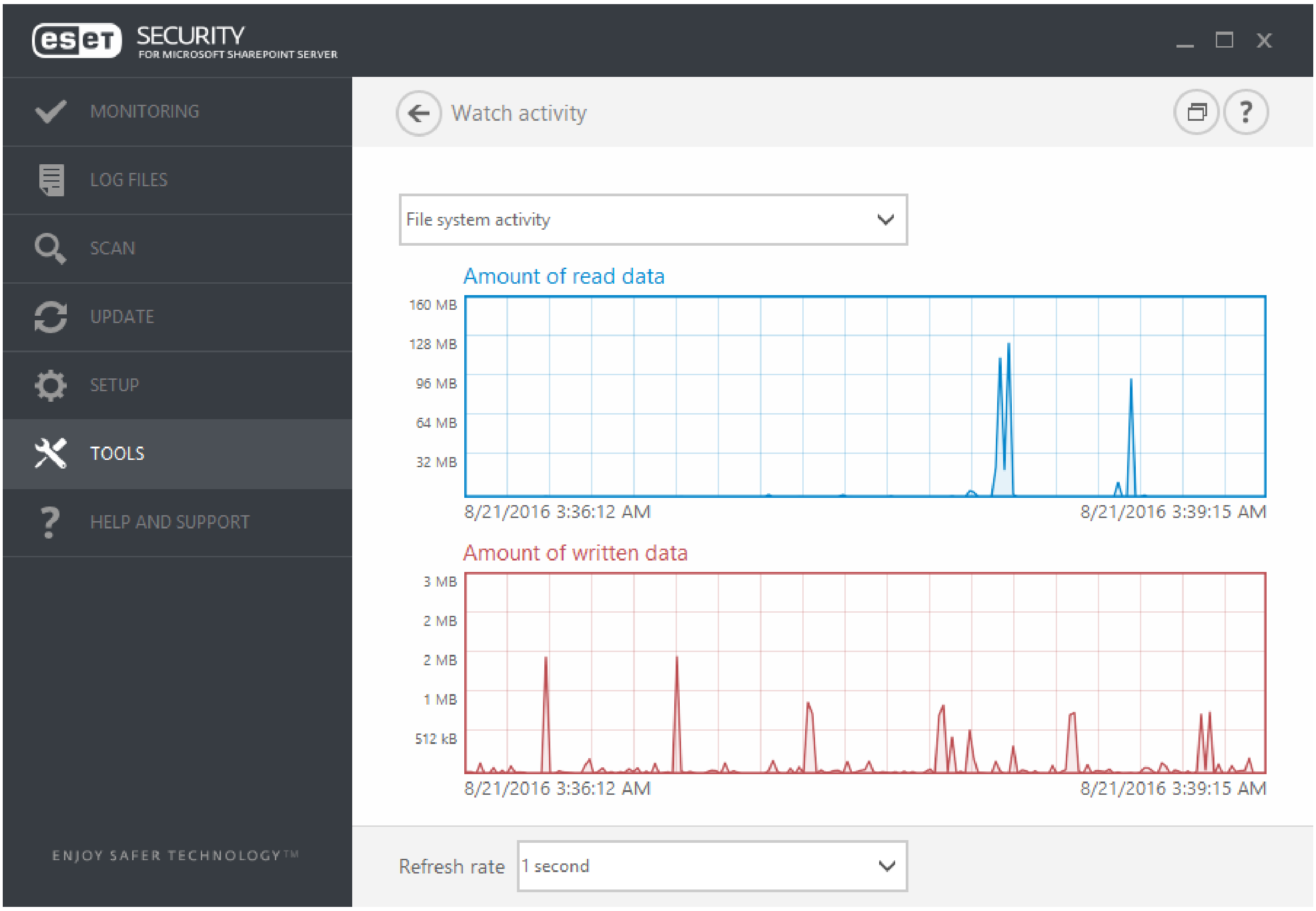
NOTE

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



### 7.6.2 Watch activity

To see current **File system activity** and **SharePoint Server protection performance** in graph form, click **Tools** > **Watch activity**. At the bottom of the graph is a timeline that records file system activity in real-time based on the selected time span. Use the **Refresh rate** drop-down menu to change the frequency of updates.



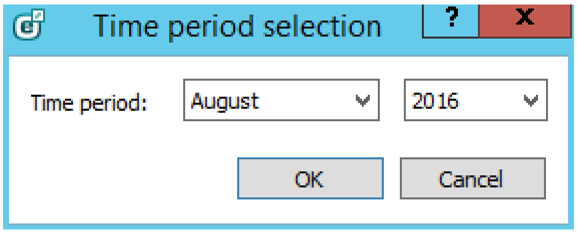
The following options are available:

- **1 second** - The graph refreshes every second and the timeline covers the last 10 minutes.
- **1 minute (last 24 hours)** - The graph is refreshed every minute and the timeline covers the last 24 hours.
- **1 hour (last month)** - The graph is refreshed every hour and the timeline covers the last month.
- **1 hour (selected month)** - The graph is refreshed every hour and the timeline covers the selected month. Click **Change month** button to make another selection.

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

#### 7.6.2.1 Time period selection

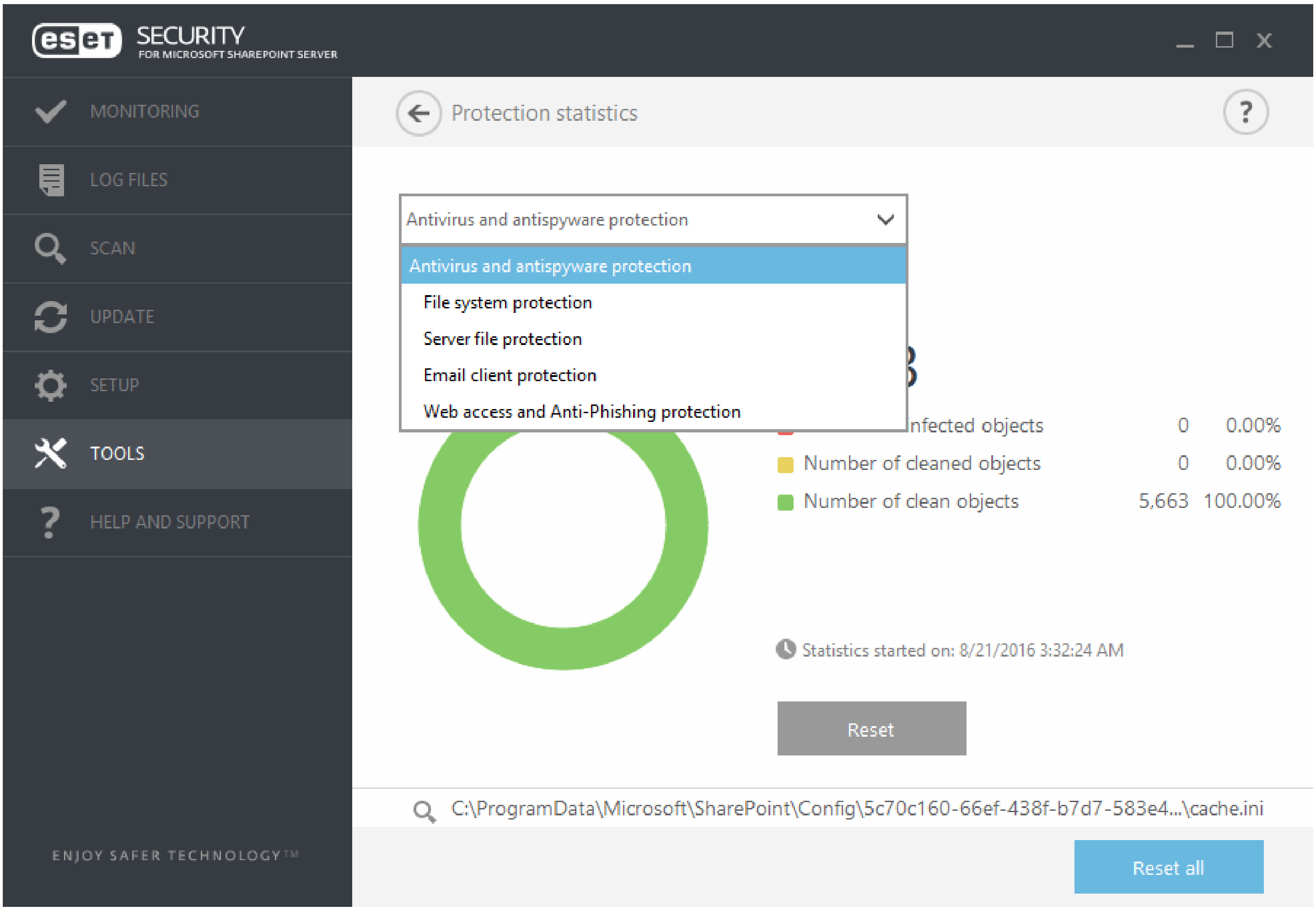
Select a month (and a year) for which you want to see **File system activity** or **SharePoint Server protection performance** in the graph.



Time period: August 2016

### 7.6.3 Protection statistics

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



| | | |
|---|---|---|
| 🟥 Number of infected objects | 0 | 0.00% |
| 🟨 Number of cleaned objects | 0 | 0.00% |
| 🟩 Number of clean objects | 5,663 | 100.00% |

Statistics started on: 8/21/2016 3:32:24 AM

C:\ProgramData\Microsoft\SharePoint\Config\5c70c160-66ef-438f-b7d7-583e4...\cache.ini

The following statistic graphs are available:

- **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.
- **Server file protection** - Displays SharePoint objects that were uploaded or downloaded.
- **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.

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

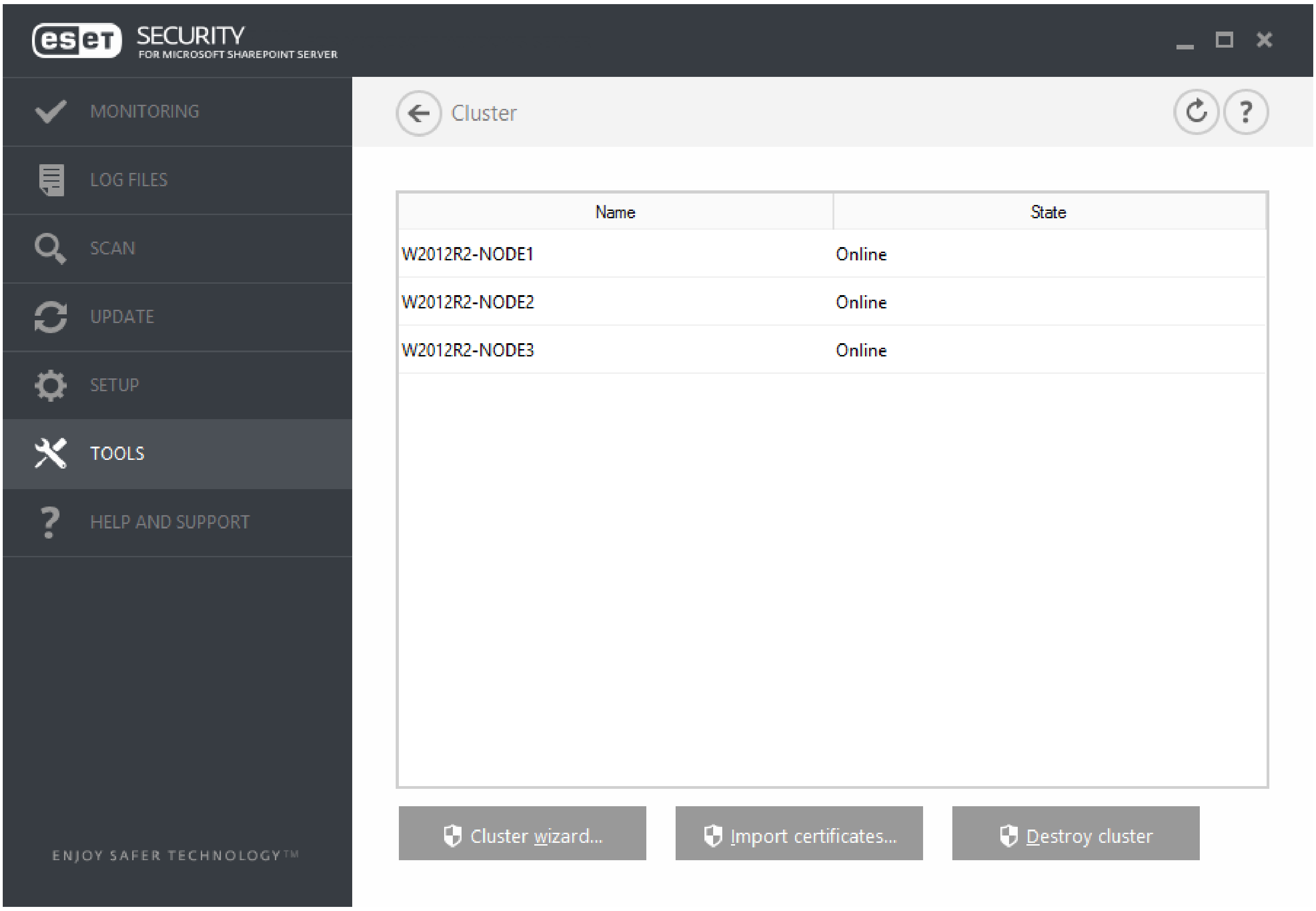
### 7.6.4 Cluster

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 as well as synchronize data necessary for correct operation of a group of product instances. An example of such group is a group of nodes in a Windows Failover Cluster or Network Load Balancing (NLB) Cluster with ESET products installed where there is a need to have the same configuration of the product across the whole cluster. ESET Cluster ensures this consistency between instances.

NOTE
User interface settings are not synchronized between ESET Cluster nodes.

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



| Name | State |
|---|---|
| W2012R2-NODE1 | Online |
| W2012R2-NODE2 | Online |
| W2012R2-NODE3 | Online |

To set up the ESET Cluster click **Cluster wizard...** For details on how to set the ESET Cluster up using the wizard click here.

When setting up the ESET Cluster, there two ways to add nodes - automatically using existing Windows Failover Cluster / NLB Cluster or manually by browsing for computers that are in a Workgroup or in a Domain.

**Autodetect** - Automatically detects nodes that are already members of a Windows Failover Cluster / NLB Cluster and adds them to the ESET Cluster.
**Browse** - You can add nodes manually by typing in the server names (either members of the same Workgroup or members of the same Domain).

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

Once you have added nodes to your ESET Cluster, the next step is the installation of ESET 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).

> **NOTE**
> It is not possible to combine domain nodes with workgroup nodes.

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

ESET Clusters can be dismantled by clicking **Destroy cluster**. 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 reverted to their previous state and can be used again in another ESET Cluster if necessary.

> **NOTE**
> The creation of ESET Clusters between ESET Security for Microsoft SharePoint and ESET File Security for Linux is not supported.

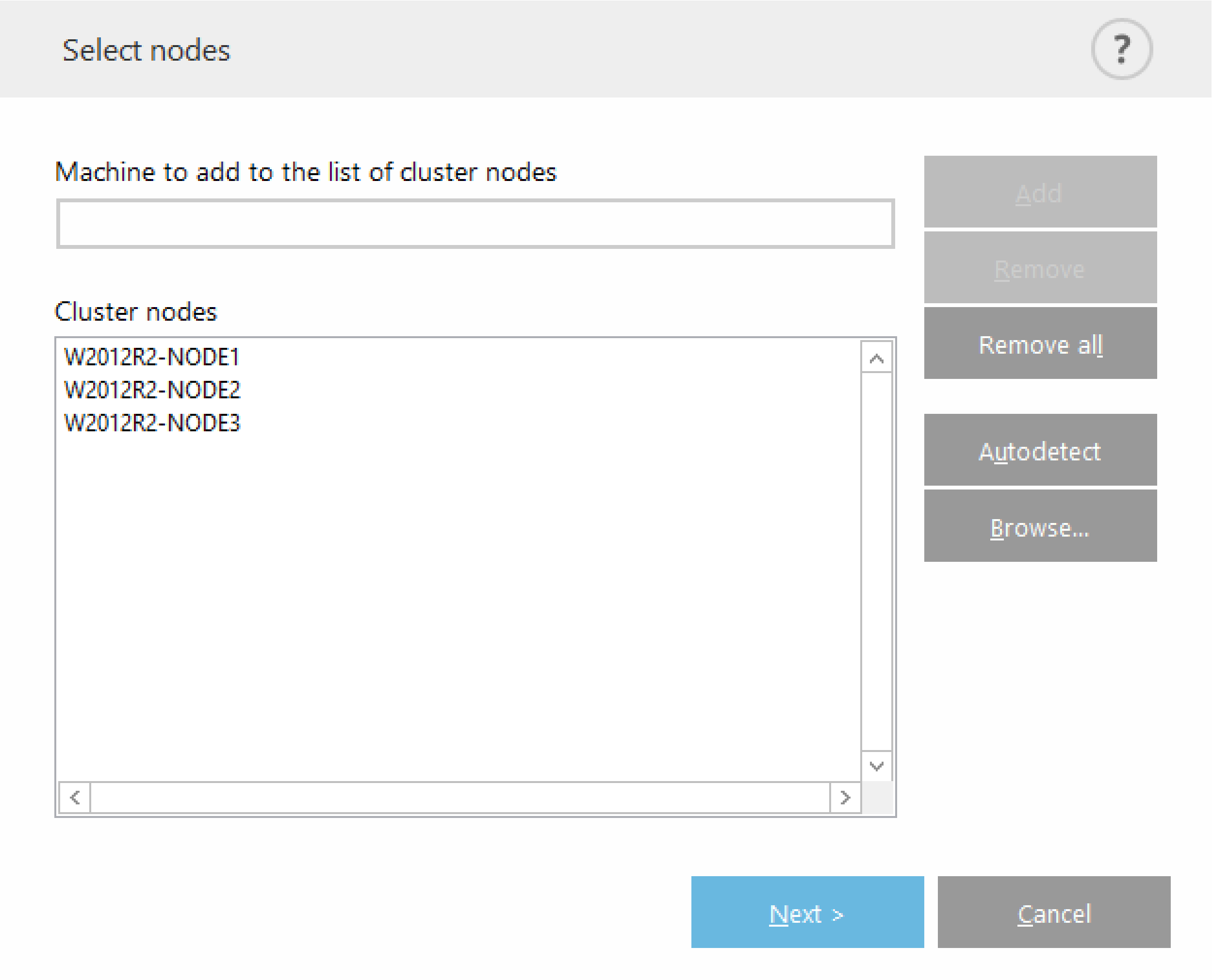
Adding new nodes to an existing ESET Cluster can be done anytime by running the **Cluster wizard** as described above and here.

### 7.6.4.1 Cluster wizard - page1

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

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

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



Cluster nodes

W2012R2-NODE1
W2012R2-NODE2
W2012R2-NODE3

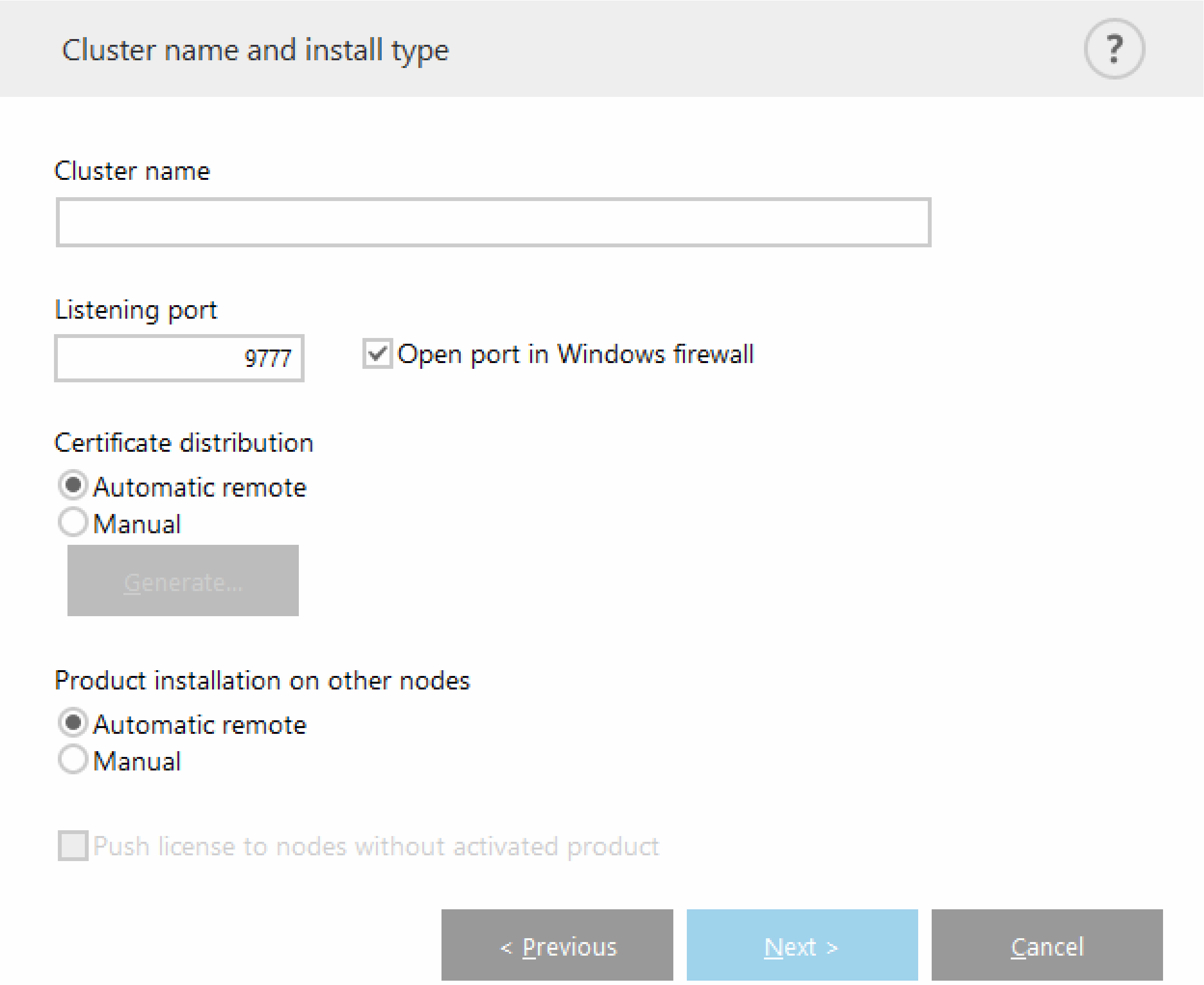
To modify **Cluster nodes** in the list, select the node you want to remove and click **Remove**, or to clear the list completely click **Remove all**.

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

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

### 7.6.4.2 Cluster wizard - page2

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



Cluster name and install type

Cluster name:

Listening port: 9777

☑ Open port in Windows firewall

Certificate distribution

● Automatic remote

○ Manual

Product installation on other nodes

● Automatic remote

○ Manual

□ Push license to nodes without activated product

**Cluster name -** type your cluster name.
**Listening port -** (default port is 9777)
**Open port in Windows firewall -** when selected a rule is created in the Windows Firewall.

**Certificate distribution:**
**Automatic remote -** certificate will be installed automatically.
**Manual** - when you click **Generate** a browse window will open - select the folder in which to store 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. You can then choose to enroll the certificate on the local machine by clicking **Yes**. You will later need to import certificates manually as described here.

**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** - choose this if you want to install ESET Security for Microsoft SharePoint manually (for example when you have different OS architectures on some of the nodes).

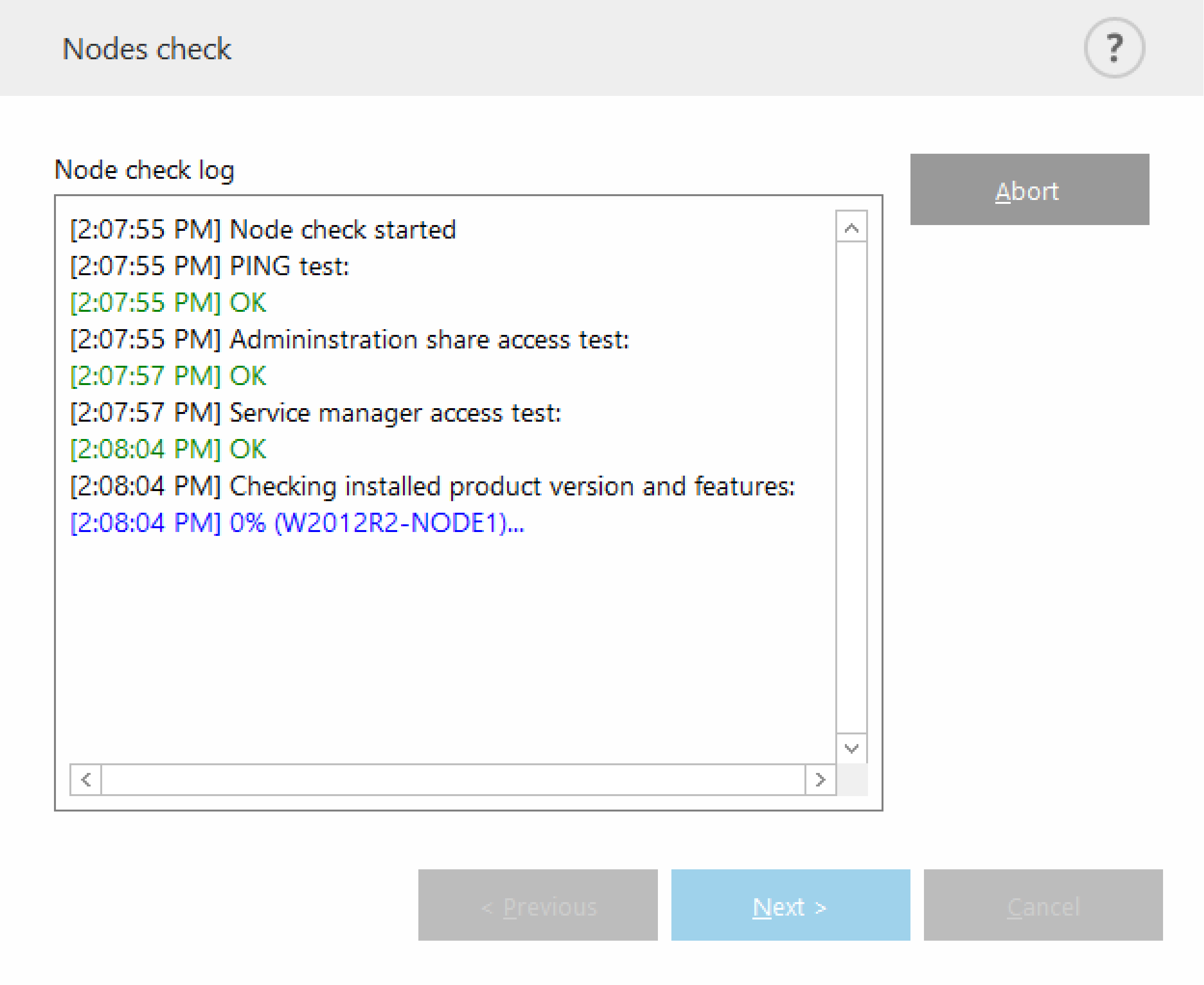
**Push license to nodes without activated product** - select this to have ESET Security automatically activate ESET Solutions installed on nodes without licenses.

i NOTE
If you want to create an ESET Cluster with mixed operating system architectures (32 bit and 64 bit), then you will need to install ESET Security for Microsoft SharePoint manually. Operation systems in use will be detected during next steps and you'll see this information in the log window.

### 7.6.4.3 Cluster wizard - page3

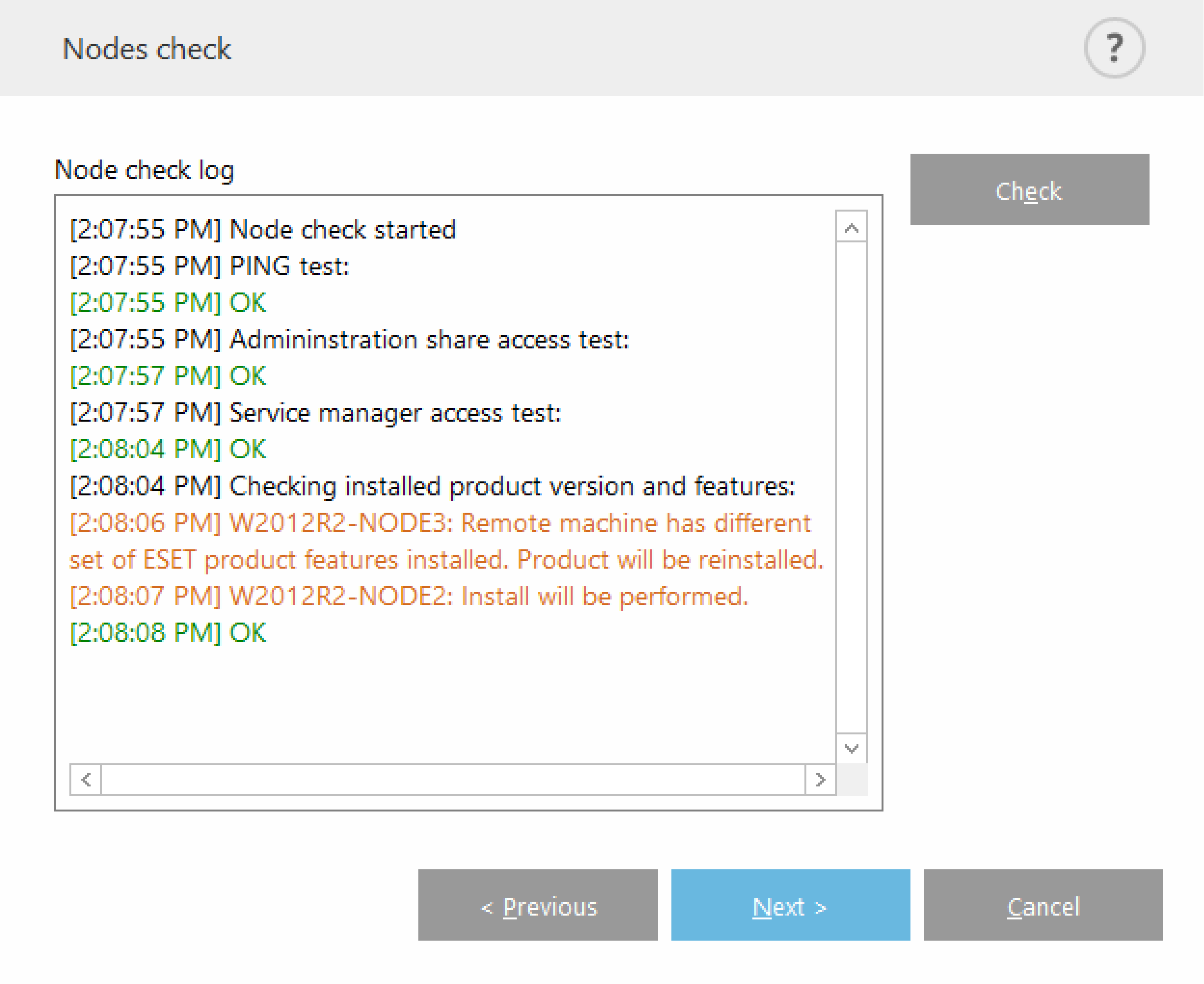
After specifying installation details a node check is run. The following information will be displayed in the **Nodes check log**:

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



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

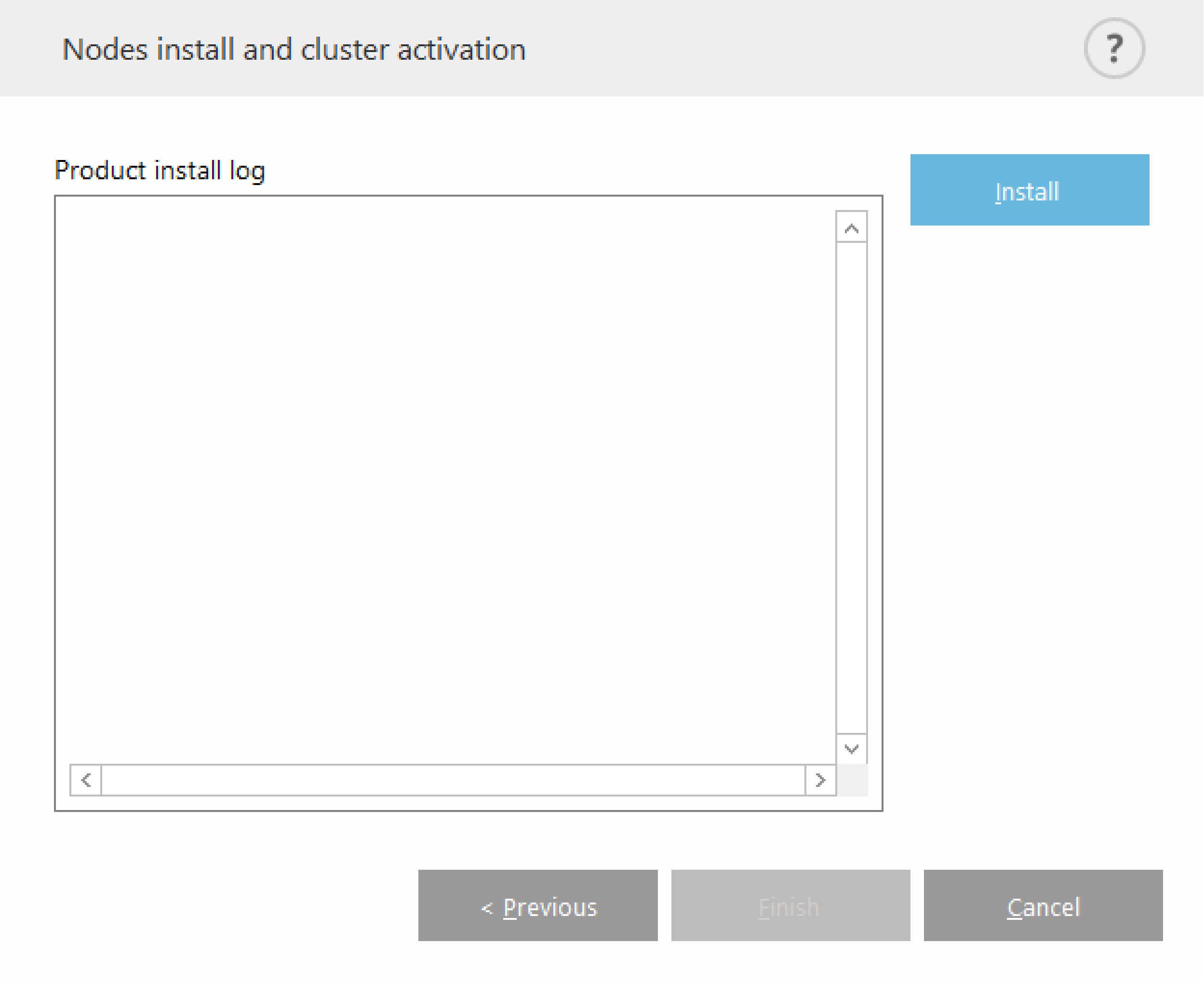
You will see the report once the node check is finished:



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

### 7.6.4.4 Cluster wizard - page4

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

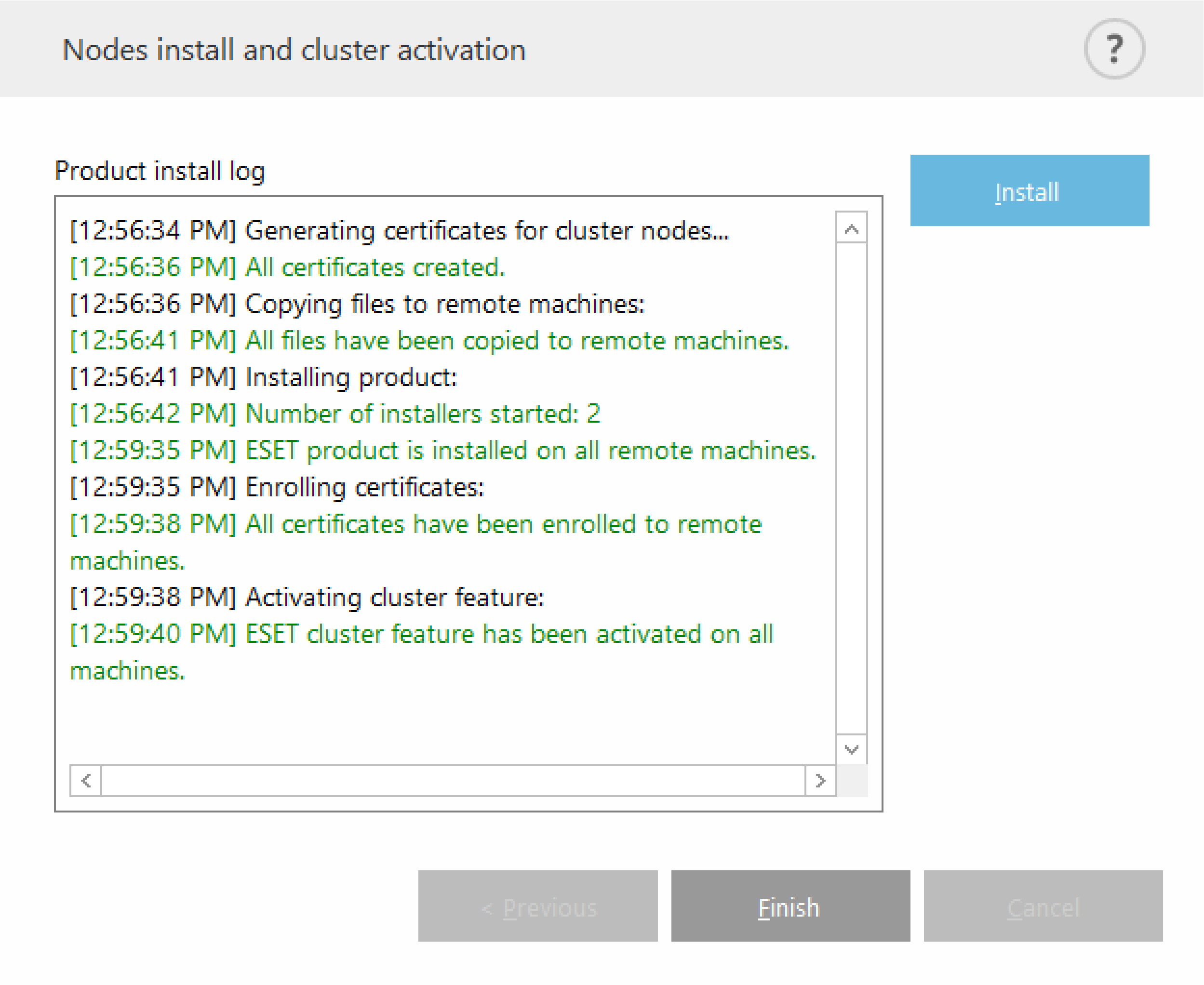


**NOTE**

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

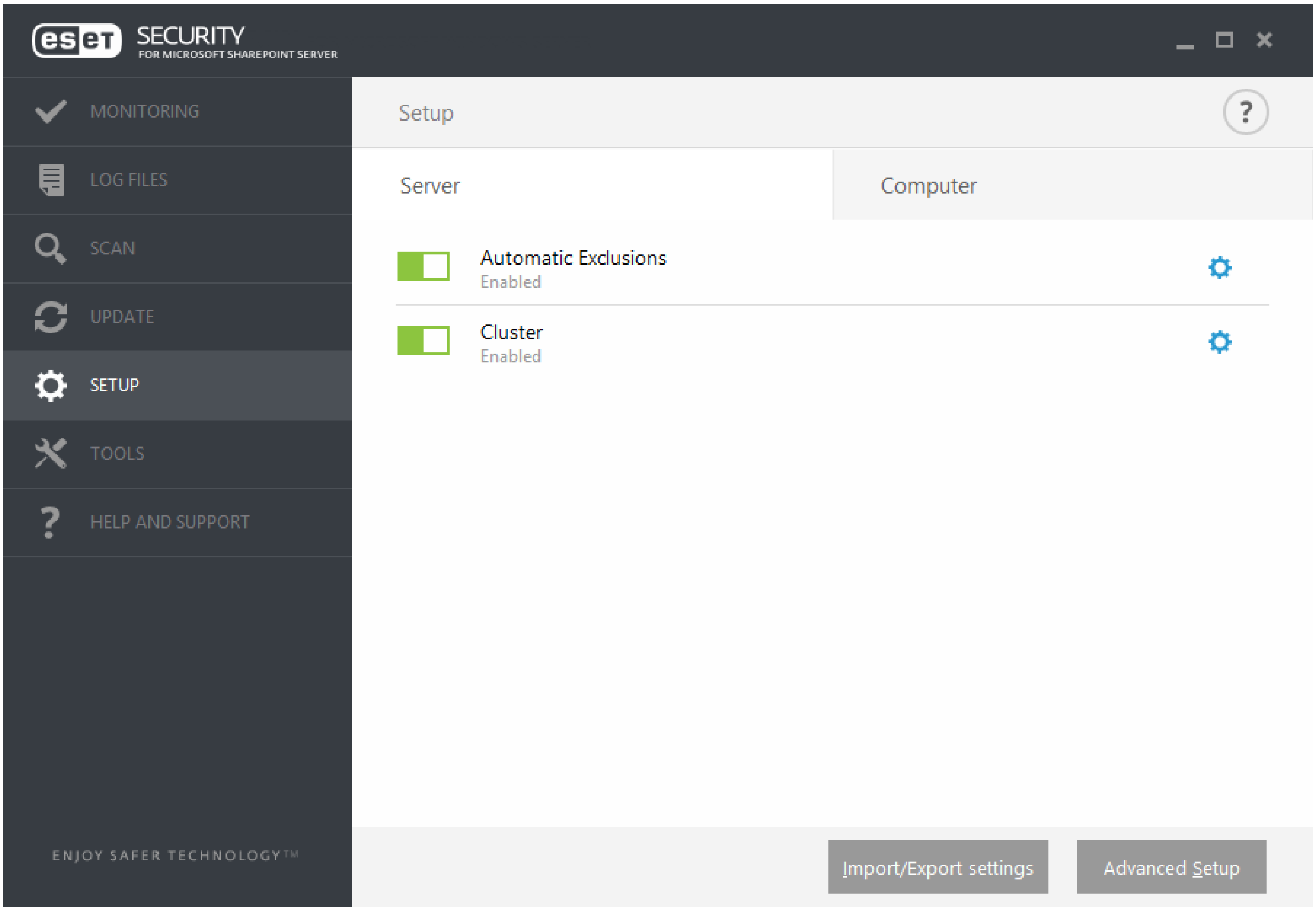
**NOTE**

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.



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

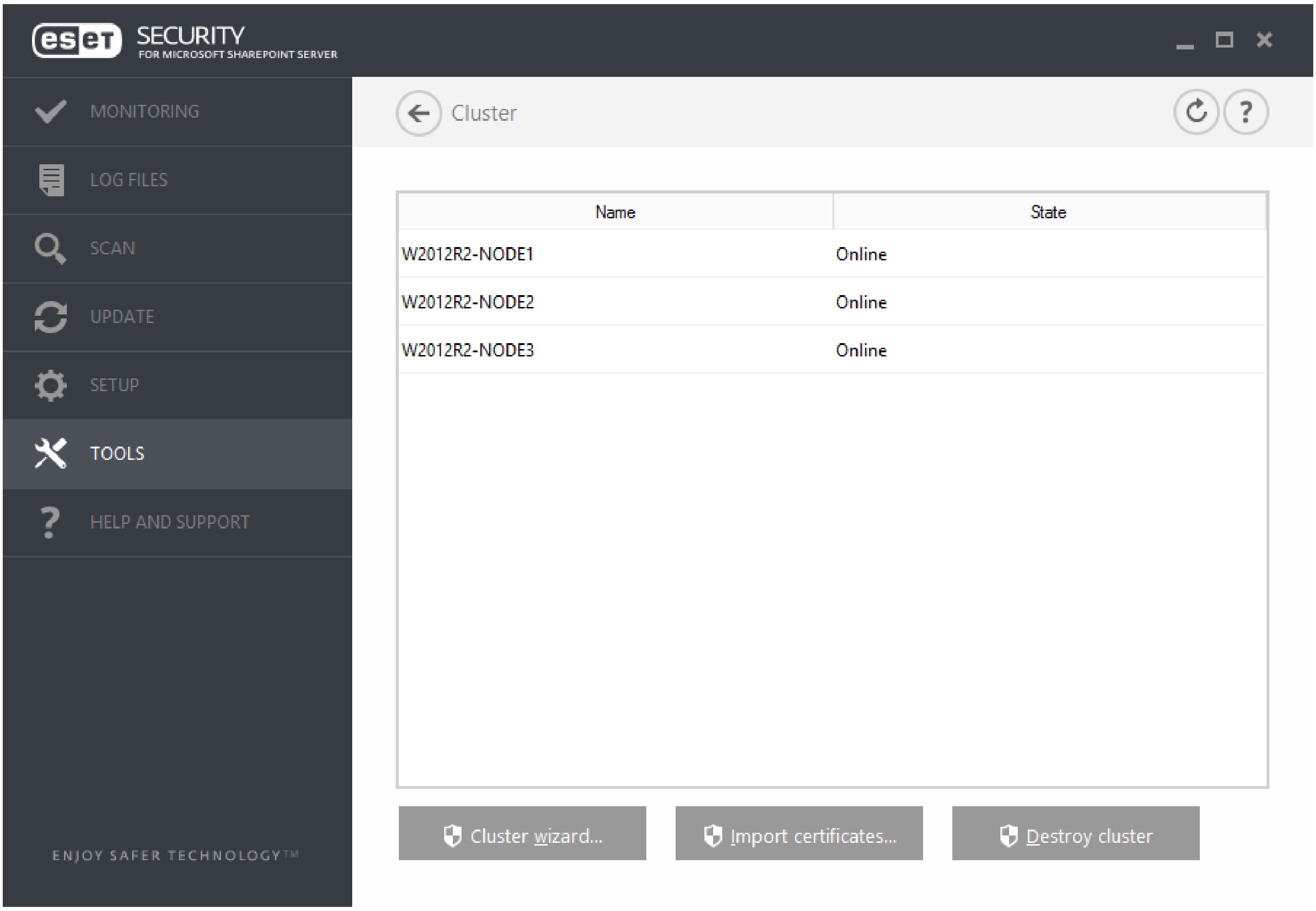
Once you have correctly configured the ESET Cluster, it will appear in **Setup** > **Server** page as enabled.



Automatic Exclusions
Enabled

Cluster
Enabled

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



| Name | State |
|---|---|
| W2012R2-NODE1 | Online |
| W2012R2-NODE2 | Online |
| W2012R2-NODE3 | Online |

**Import certificates -** Navigate to the folder that contains the certificates (generated during the use of Cluster wizard). Select the certificate file and click **Open**.

### 7.6.5 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 the use of the GUI.

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

There are two modes in which eShell can be run:

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

`eshell get status` or `eshell set antivirus status disabled`

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

NOTE

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

NOTE

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

There are two ways to enter interactive mode in eShell:

- Via Windows Start menu: **Start** > **All Programs** > **ESET** > **ESET Security for Microsoft SharePoint** > **ESET shell**
- From Windows Command Prompt by typing in `eshell` and pressing the **Enter** key

IMPORTANT

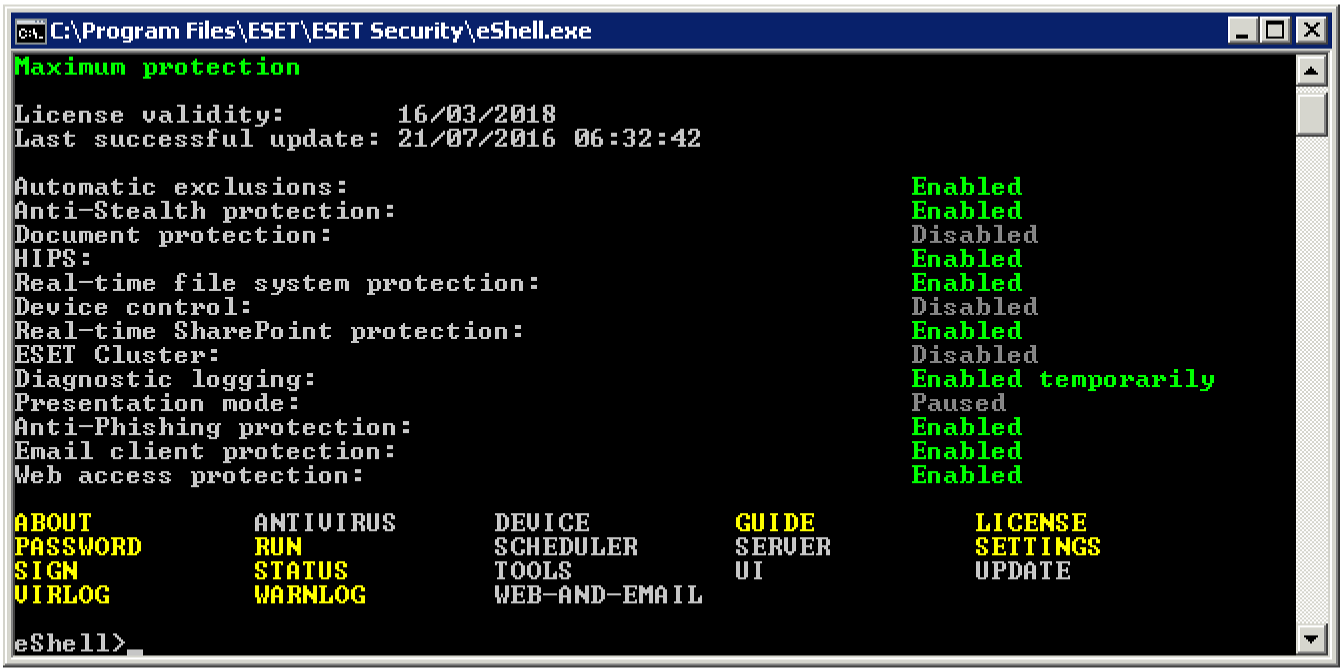
If you get an error `'eshell' is not recognized as an internal or external command`, this is due to new Environment Variables not being loaded by your system after the installation of ESET Security for Microsoft SharePoint. You can open new Command Prompt and try starting eShell again. If you are still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

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

NOTE

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

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



C:\Program Files\ESET\ESET Security\eShell.exe

```
Maximum protection

License validity:        16/03/2018
Last successful update: 21/07/2016 06:32:42

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

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

eShell>_
```

NOTE

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

**Customizing eShell**

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

### 7.6.5.1 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 ANTIVIRUS DOCUMENT STATUS ENABLED
```

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

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

SYNTAX:

```
    [get] | status
    set status enabled | disabled
```

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

**NOTE**

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

**Prefix / Operation**

A prefix is an operation. The `GET` prefix will give you information about how a certain feature of ESET Security for Microsoft SharePoint is configured or show you the status (such as `GET ANTIVIRUS STATUS` will show you current protection status). The `SET` prefix will configure functionality or change its status (`SET ANTIVIRUS STATUS ENABLED` will activate protection).

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

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

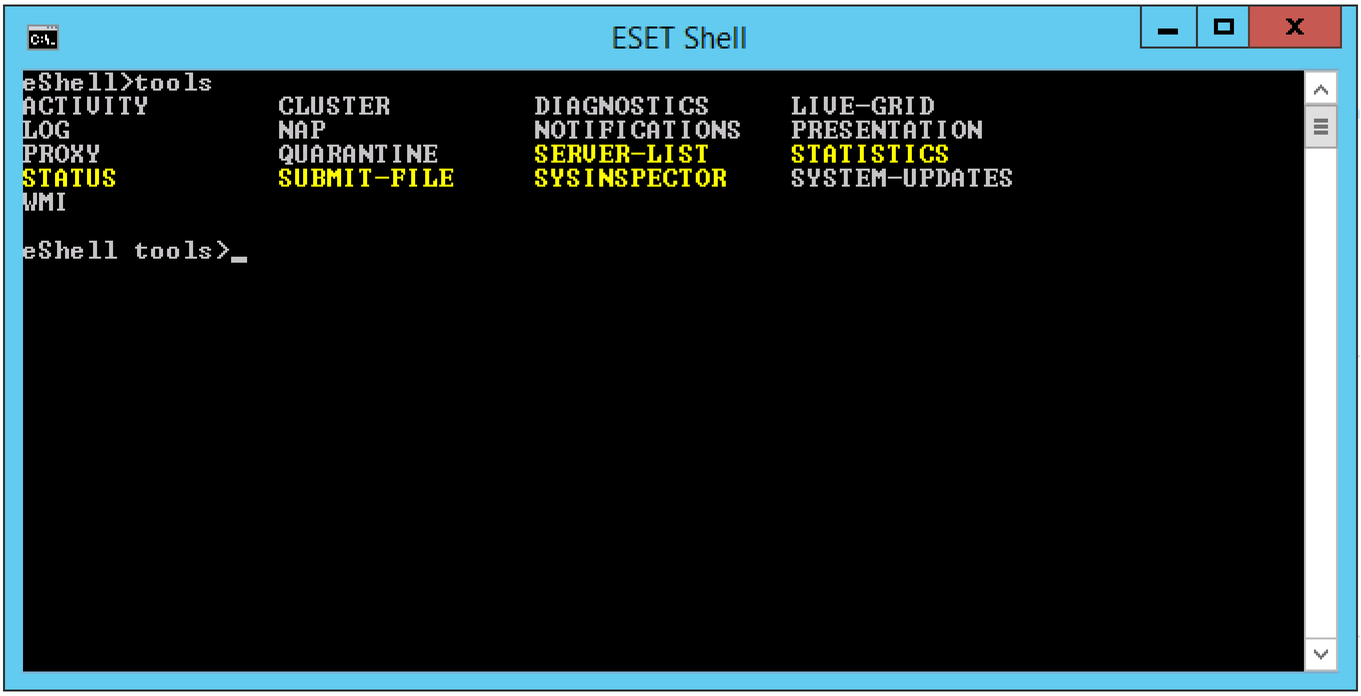
Prefixes such as `GET` and `SET` are used with many commands, but some commands (such as `EXIT`) do not use a prefix.

### Command path / Context

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

```
eShell>
```

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



```
eShell>tools
ACTIVITY        CLUSTER         DIAGNOSTICS     LIVE-GRID
LOG             NAP             NOTIFICATIONS   PRESENTATION
PROXY           QUARANTINE      SERVER-LIST     STATISTICS
STATUS          SUBMIT-FILE     SYSINSPECTOR    SYSTEM-UPDATES
WMI

eShell tools>_
```

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

If you need to return back to a higher level, use `..` (two dots). For example, say you are here:

```
eShell antivirus startup>
```

type `..` to go up one level, to:

```
eShell antivirus>
```

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

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

`GET ANTIVIRUS STATUS` - if you are in the root context (command line shows `eShell>`)
`GET STATUS` - if you are in the context `ANTIVIRUS` (command line shows `eShell antivirus>`)
`.. GET STATUS` - if you are in the context `ANTIVIRUS STARTUP` (command line shows `eShell antivirus startup>`)

**NOTE**

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

`. GET STATUS` - if you are in the context `ANTIVIRUS STARTUP` (command line shows `eShell antivirus startup>`)

### Argument

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

`no` - No cleaning
`normal` - Normal cleaning
`strict` - Strict cleaning

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

### Abbreviated form / Shortened commands

eShell allows you to shorten contexts, commands and arguments (provided the argument is a switch or an alternative option). It is not possible to shorten a prefix or argument that are concrete values such as a number, name or path.

**NOTE**

You can use numbers `1` and `0` instead of `enabled` and `disabled` arguments. For example:

```
set status enabled    =>   set stat 1
set status disabled    =>   set stat 0
```

Examples of the short form:

```
set status enabled    =>   set stat en
add antivirus common scanner-excludes C:\path\file.ext    =>    add ant com scann C:\path\file.ext
```

In a case where two commands or contexts start with the same letters (such as `ABOUT` and `ANTIVIRUS`, and you enter `A` as shortened command), eShell will not be able to decide which command of these two you want to run.  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 commands are available in this context:
   ABOUT - Shows information about program
   ANTIVIRUS - Changes to context antivirus
```

By adding one or more letters (for example, `AB` instead of just `A`) eShell will execute `ABOUT` command since it is unique now.

**NOTE**

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

### Automatic completion

This new feature introduced in eShell 2.0 eShell is very similar to automatic completion in Windows Command Prompt. While Windows Command Prompt completes file paths, eShell completes commands, context and operation names. Argument completion is not supported. When typing command simply, press **TAB** to complete or cycle through available variations. Press **SHIFT** + **TAB** to cycle backwards. Mixing abbreviated form and automatic completion is not supported. Use either one or the other. For example, when you type `antivir real scan` hitting **TAB** will do nothing. Instead, type `antivir` and then **TAB** to complete `antivirus`, continue typing real + **TAB** and scan + **TAB**. You can then cycle through all available variations: scan-create, scan-execute, scan-open, etc.

### Aliases

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

- `(global) close` - exit
- `(global) quit` - exit
- `(global) bye` - exit
- `warnlog` - tools log events
- `virlog` - tools log detections
- `antivirus on-demand log` - tools log scans

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

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

### Password protected settings

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

### Guide / Help

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

### Command history

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

### CLS / Clear screen

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

### EXIT / CLOSE / QUIT / BYE

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

#### 7.6.5.2 Commands

This section lists a few basic eShell commands with descriptions.

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

Example commands (contained within the ROOT context):

**ABOUT**

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

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

CONTEXT PATH:

```
root
```

**PASSWORD**

Normally, to execute password-protected commands, you are prompted to type in a password for security reasons. This applies to commands such as those that disable antivirus 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 in order to avoid entering a password every time. It will be remembered by eShell and automatically  entered when a password-protected command is executed.

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

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

```
eshell set password plain <yourpassword> "&" set status disabled
```

This concatenated command above defines a password and disables protection.

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

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore password

set password [plain <password>]
```

OPERATIONS:

`get` - Show password

`set` - Set or clear password

`restore` - Clear password

ARGUMENTS:

`plain` - Switch to enter password as parameter

`password` - Password

EXAMPLES:

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

`restore password` - Clears password

EXAMPLES:

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

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

`restore password` - This command clears the defined password

### STATUS

Shows information about the current protection status of ESET Security for Microsoft SharePoint (similar to GUI).

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERATIONS:

`get` - Show antivirus protection status

`set` - Disable/Enable antivirus protection

`restore` - Restores default settings

ARGUMENTS:

`disabled` - Disable antivirus protection

`enabled` - Enable antivirus protection

EXAMPLES:

`get status` - Shows current protection status

`set status disabled` - Disables protection

`restore status` - Restores protection to default setting (Enabled)

### 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.

### 7.6.5.3 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. For example:

```
eshell get antivirus status
```

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

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

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

For security reasons, the execution policy is set to **Limited Scripting** by default. This allows you to use eShell as a monitoring tool, but it won't let you make configuration changes to ESET 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 that you use signed batch files to execute commands that make configuration changes.

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

**Signed batch files**

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

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

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

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

To 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. For example `eshell run d:\myeshellscript.bat`

### 7.6.6 ESET SysInspector

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

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:

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

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

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

#### 7.6.6.1 Create a computer status snapshot

Enter a short comment describing the log to be created and click the **Add** button. Please wait until the ESET SysInspector log is complete (status will be shown as **Created**). Log creation may take some time depending on your hardware configuration and system data.

#### 7.6.6.2 ESET SysInspector

##### 7.6.6.2.1 Introduction to ESET SysInspector

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

You can access ESET SysInspector two ways: From the integrated version in ESET Security solutions or by downloading the standalone version (SysInspector.exe) for free from ESET's website. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The standalone and integrated versions each allow you to export system snapshots to an *.xml* file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools** > **ESET SysInspector** (except ESET Remote Administrator).

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

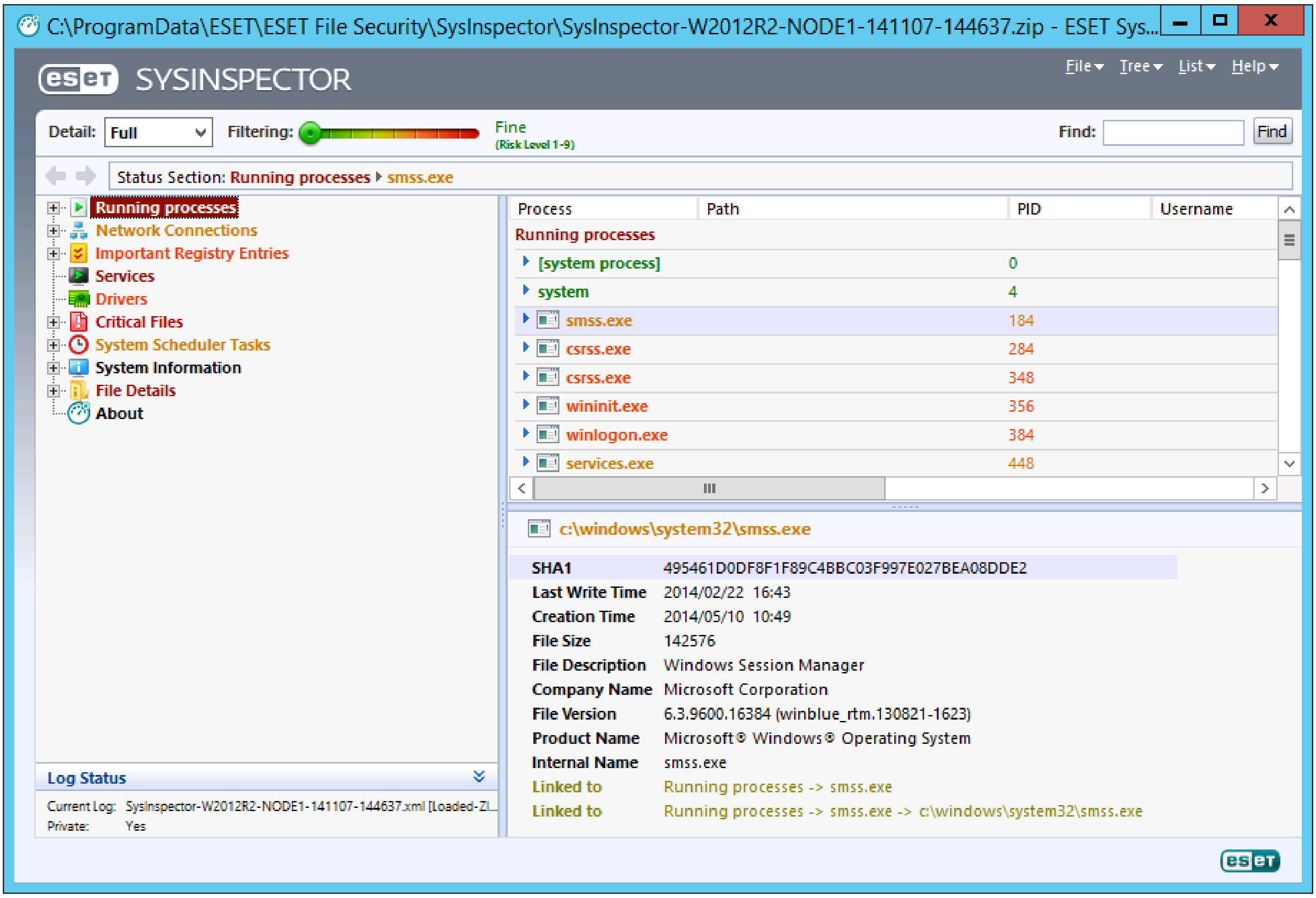
### 7.6.6.2.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website.

Please wait while the application inspects your system, which could take up to several minutes.

## 7.6.6.2.2 User Interface and application usage

For clarity the main program window is divided into four major sections – Program Controls located on the top of the main program window, Navigation window to the left, the Description window to the right and the Details window at the bottom of the main program window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).



C:\ProgramData\ESET\ESET File Security\SysInspector\SysInspector-W2012R2-NODE1-141107-144637.zip - ESET Sys...

Status Section: Running processes ▸ smss.exe

- Running processes
- Network Connections
- Important Registry Entries
- Services
- Drivers
- Critical Files
- System Scheduler Tasks
- System Information
- File Details
- About

| Process | Path | PID | Username |
|---|---|---|---|
| Running processes | | | |
| [system process] | | 0 | |
| system | | 4 | |
| smss.exe | | 184 | |
| csrss.exe | | 284 | |
| csrss.exe | | 348 | |
| wininit.exe | | 356 | |
| winlogon.exe | | 384 | |
| services.exe | | 448 | |

c:\windows\system32\smss.exe

| | |
|---|---|
| SHA1 | 495461D0DF8F1F89C4BBC03F997E027BEA08DDE2 |
| Last Write Time | 2014/02/22 16:43 |
| Creation Time | 2014/05/10 10:49 |
| File Size | 142576 |
| File Description | Windows Session Manager |
| Company Name | Microsoft Corporation |
| File Version | 6.3.9600.16384 (winblue_rtm.130821-1623) |
| Product Name | Microsoft® Windows® Operating System |
| Internal Name | smss.exe |
| Linked to | Running processes -> smss.exe |
| Linked to | Running processes -> smss.exe -> c:\windows\system32\smss.exe |

Log Status

Current Log: SysInspector-W2012R2-NODE1-141107-144637.xml [Loaded-ZI...
Private: Yes

### 7.6.6.2.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

**File**

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

**NOTE:** You may open previously stored ESET SysInspector reports by dragging and dropping them into the main program window.

**Tree**

Enables you to expand or close all nodes and export selected sections to Service script.

### List

Contains functions for easier navigation within the program and various other functions like finding information online.

### Help

Contains information about the application and its functions.

### Detail

This setting influences the information displayed in the main program window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

### Filtering

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current risk level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose a security risk. If you are not using a security solution from ESET, we recommend that you scan your system with ESET Online Scanner if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

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

### Compare

When comparing two logs, you can choose to display all items, display only added items, display only removed items or to display only replaced items.

### Find

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

### Return

By clicking the back or forward arrows, you can return to previously displayed information in the Description window. You can use the backspace and space keys instead of clicking back and forward.

### Status section

Displays the current node in Navigation window.

***Important:*** Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

### 7.6.6.2.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or click ⊞ or ⊟ next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

**Running processes**

This node contains information about applications and processes running at the time of generating the log. In the Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

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

**NOTE:** An operating system is comprised of several important kernel components running constantly that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with \??\. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

**Network Connections**

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

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

**Important Registry Entries**

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

**Services**

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

**Drivers**

A list of drivers installed in the system.

**Critical Files**

The Description window displays content of critical files related to the Microsoft windows operating system.

**System Scheduler Tasks**

Contains a list of tasks triggered by Windows Task Scheduler at a specified time/interval.

**System Information**

Contains detailed information about hardware and software along with information about set environmental variables, user rights and system event logs.

### File Details

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

### About

Information about version of ESET SysInspector and the list of program modules.

Key shortcuts that can be used when working with the ESET SysInspector include:

### File

| | |
|---|---|
| Ctrl+O | opens existing log |
| Ctrl+S | saves created logs |

### Generate

| | |
|---|---|
| Ctrl+G | generates a standard computer status snapshot |
| Ctrl+H | generates a computer status snapshot that may also log sensitive information |

### Item Filtering

| | |
|---|---|
| 1, O | fine, risk level 1-9 items are displayed |
| 2 | fine, risk level 2-9 items are displayed |
| 3 | fine, risk level 3-9 items are displayed |
| 4, U | unknown, risk level 4-9 items are displayed |
| 5 | unknown, risk level 5-9 items are displayed |
| 6 | unknown, risk level 6-9 items are displayed |
| 7, B | risky, risk level 7-9 items are displayed |
| 8 | risky, risk level 8-9 items are displayed |
| 9 | risky, risk level 9 items are displayed |
| - | decreases risk level |
| + | increases risk level |
| Ctrl+9 | filtering mode, equal level or higher |
| Ctrl+0 | filtering mode, equal level only |

### View

| | |
|---|---|
| Ctrl+5 | view by vendor, all vendors |
| Ctrl+6 | view by vendor, only Microsoft |
| Ctrl+7 | view by vendor, all other vendors |
| Ctrl+3 | displays full detail |
| Ctrl+2 | displays medium detail |
| Ctrl+1 | basic display |
| BackSpace | moves one step back |
| Space | moves one step forward |
| Ctrl+W | expands tree |
| Ctrl+Q | collapses tree |

### Other controls

| | |
|---|---|
| Ctrl+T | goes to the original location of item after selecting in search results |
| Ctrl+P | displays basic information about an item |
| Ctrl+A | displays full information about an item |
| Ctrl+C | copies the current item's tree |
| Ctrl+X | copies items |
| Ctrl+B | finds information about selected files on the Internet |
| Ctrl+L | opens the folder where the selected file is located |
| Ctrl+R | opens the corresponding entry in the registry editor |
| Ctrl+Z | copies a path to a file (if the item is related to a file) |
| Ctrl+F | switches to the search field |

| | |
|---|---|
| Ctrl+D | closes search results |
| Ctrl+E | run service script |

**Comparing**

| | |
|---|---|
| Ctrl+Alt+O | opens original / comparative log |
| Ctrl+Alt+R | cancels comparison |
| Ctrl+Alt+1 | displays all items |
| Ctrl+Alt+2 | displays only added items, log will show items present in current log |
| Ctrl+Alt+3 | displays only removed items, log will show items present in previous log |
| Ctrl+Alt+4 | displays only replaced items (files inclusive) |
| Ctrl+Alt+5 | displays only differences between logs |
| Ctrl+Alt+C | displays comparison |
| Ctrl+Alt+N | displays current log |
| Ctrl+Alt+P | opens previous log |

**Miscellaneous**

| | |
|---|---|
| F1 | view help |
| Alt+F4 | close program |
| Alt+Shift+F4 | close program without asking |
| Ctrl+I | log statistics |

### 7.6.6.2.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting malicious code.

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

The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, click **File** > **Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

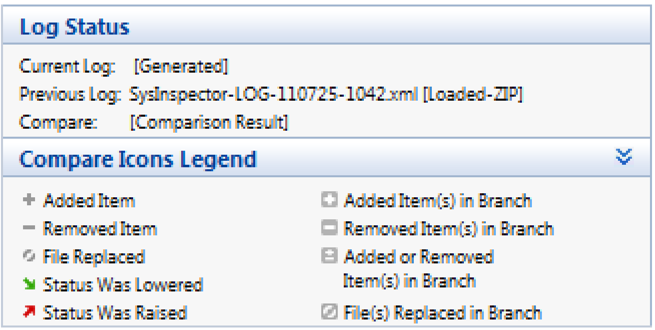
**NOTE:** If you compare two log files, click **File** > **Save log** to save it as a ZIP file; both files will be saved. If you open this file later, the contained logs are automatically compared.

Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Description of all symbols that can be displayed next to items:

- + new value, not present in the previous log
- ⊞ tree structure section contains new values
- - removed value, present in the previous log only
- ⊟ tree structure section contains removed values
- ↻ value / file has been changed
- ▨ tree structure section contains modified values / files
- ↘ the risk level has decreased / it was higher in the previous log
- ↗ the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.



**Log Status**

Current Log: [Generated]
Previous Log: SysInspector-LOG-110725-1042.xml [Loaded-ZIP]
Compare: [Comparison Result]

**Compare Icons Legend**

|  |  |
|---|---|
| + Added Item | ⊞ Added Item(s) in Branch |
| − Removed Item | ⊟ Removed Item(s) in Branch |
| ↻ File Replaced | ⊟ Added or Removed Item(s) in Branch |
| ↘ Status Was Lowered | ▨ File(s) Replaced in Branch |
| ↗ Status Was Raised |  |

Any comparative log can be saved to a file and opened at a later time.

**Example**

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

In order to track changes between those two logs, click **File** > **Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

*SysIsnpector.exe current.xml previous.xml*

### 7.6.6.2.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

|  |  |
|---|---|
| **/gen** | generate log directly from the command line without running GUI |
| **/privacy** | generate log with sensitive information omitted |
| **/zip** | save outcome log in compressed zip archive |
| **/silent** | suppress progress window when generating log from the command line |
| **/blank** | launch ESET SysInspector without generating/loading log |

**Examples**

Usage:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

To load specific log directly into the browser, use: *SysInspector.exe .\clientlog.xml*
To generate log from the command line, use: *SysInspector.exe /gen=.\mynewlog.xml*
To generate log excluding sensitive information directly in a compressed file, use: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
To compare two log files and browse differences, use: *SysInspector.exe new.xml old.xml*

**NOTE:** If the name of the file/folder contains a gap, then should be taken into inverted commas.

### 7.6.6.2.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspector by easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

**Example**

If you suspect that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

1. Run ESET SysInspector to generate a new system snapshot.
2. Select the first item in the section on the left (in the tree structure), press Shift and select the last item to mark all items.
3. Right click the selected objects and select **Export Selected Sections To Service Script**.
4. The selected objects will be exported to a new log.
5. This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
6. Open ESET SysInspector, click **File** > **Run Service Script** and enter the path to your script.
7. Click **OK** to run the script.

#### 7.6.6.2.4.1 Generating Service script

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

**NOTE:** It is not possible to export the service script when two logs are being compared.

#### 7.6.6.2.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

**01) Running processes**

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

**02) Loaded modules**

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khbekhb.dll was marked by a “+”. When the script runs, it will recognize the processes using that specific module and end them.

### 03) TCP connections

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

### 04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

### 05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

### 06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

### 07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

The services marked and their dependent services will be stopped and uninstalled when the script is executed.

### 08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

### 09) Critical files

This section contains information about files that are critical to proper function of the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

### 7.6.6.2.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script "%Scriptname%"?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

### 7.6.6.2.5 FAQ

**Does ESET SysInspector require Administrator privileges to run?**

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

**Does ESET SysInspector create a log file?**

ESET SysInspector can create a log file of your computer's configuration. To save one, click **File** > **Save Log** in the main program window. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

**How do I view the ESET SysInspector log file?**

To view a log file created by ESET SysInspector, run the program and click **File** > **Open Log** in the main program window. You can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

**Is a specification available for the log file format? What about an SDK?**

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

**How does ESET SysInspector evaluate the risk posed by a particular object?**

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 - Fine (green) to 9 - Risky (red). In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

**Does a risk level of "6 - Unknown (red)" mean an object is dangerous?**

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

**Why does ESET SysInspector connect to the Internet when run?**

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published by ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

**What is Anti-Stealth technology?**

Anti-Stealth technology provides effective rootkit detection.

If the system is attacked by malicious code that behaves as a rootkit, the user may be exposed to data loss or theft. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

**Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time?**

When trying to identify the digital signature of an executable, ESET SysInspector first checks for a digital signature embedded in the file. If a digital signature is found, the file will be validated using that information. If a digital signature is not found, the ESI starts looking for the corresponding CAT file (Security Catalog - *%systemroot%\system32\catroot*) that contains information about the executable file processed. If the relevant CAT file is found, the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

## 7.6.7 ESET SysRescue Live

ESET SysRescue Live is a utility that enables you to create a bootable disk containing one of the ESET Security solutions - ESET NOD32 Antivirus, ESET Smart Security or certain server-oriented products. The main advantage of ESET SysRescue Live is the fact that the ESET Security solution runs independent of the host operating system but has direct access to the disk and file system. This makes it possible to remove infiltrations which normally could not be deleted, for example, when the operating system is running, etc.

### 7.6.8 Scheduler

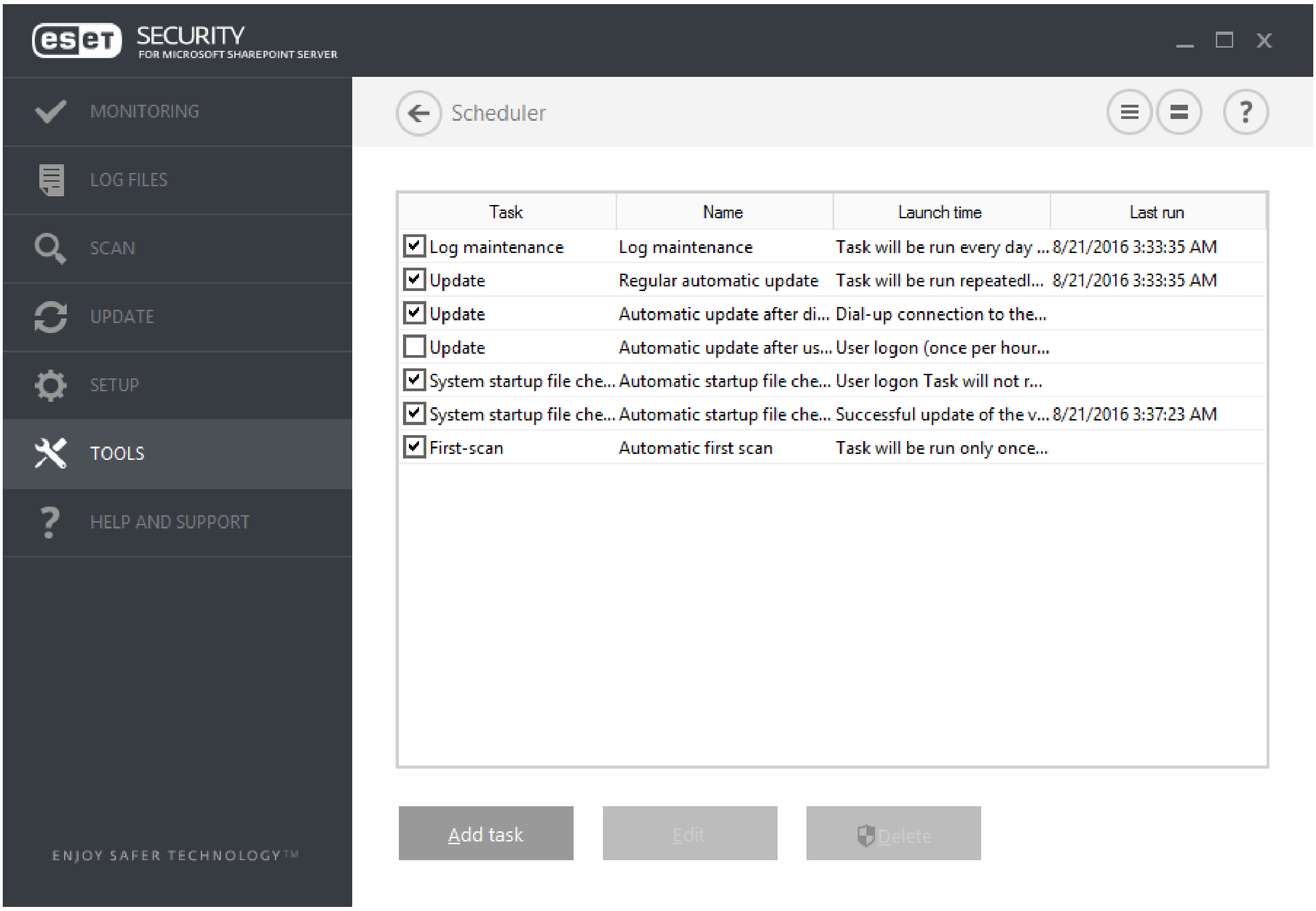
**Scheduler** can be found in the **Tools** section of the main program window. Scheduler manages and launches scheduled tasks according to defined parameters.

Scheduler contains a list of all scheduled tasks in the form of a table which shows their parameters such as **Task** type, task **Name**, **Launch time** and **Last run**. For more details, double-click a task to see its Scheduled task overview. After the installation, there is a set of predefined tasks. You can also create new scheduled tasks by clicking Add task.

When you right-click a task, you can choose an action to perform. Available actions are:

**Show task details**
**Run now**
**Add...**
**Edit...**
**Delete**

Use the check box next a task to activate/deactivate it. To edit the configuration of a scheduled task, right-click the task and click **Edit...** or select the task you want to modify and click **Edit**.



| Task | Name | Launch time | Last run |
|---|---|---|---|
| ☑ Log maintenance | Log maintenance | Task will be run every day ... | 8/21/2016 3:33:35 AM |
| ☑ Update | Regular automatic update | Task will be run repeatedl... | 8/21/2016 3:33:35 AM |
| ☑ Update | Automatic update after di... | Dial-up connection to the... | |
| □ Update | Automatic update after us... | User logon (once per hour... | |
| ☑ System startup file che... | Automatic startup file che... | User logon Task will not r... | |
| ☑ System startup file che... | Automatic startup file che... | Successful update of the v... | 8/21/2016 3:37:23 AM |
| ☑ First-scan | Automatic first scan | Task will be run only once... | |

The default (predefined) scheduled tasks are:

- **Log maintenance**
- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon** (this task is not activated be default)
- **Automatic startup file check** (after user logon)
- **Automatic startup file check** (after successful update of the virus signature database)
- **Automatic first scan**
- **Regular database scan**

### 7.6.8.1 Scheduler - Add new task

To create a new task in Scheduler, click **Add task** or right-click and select **Add** from the context menu. A wizard will open to help you create a scheduled task. See below for step-by-step instructions:

1. Enter a **Task name** and select your desired **Task type** from the drop-down menu:
   - **Run external application** - schedules the execution of an external application.
   - **Log maintenance** - log files also contain leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
   - **System startup file check** - checks files that are allowed to run at system startup or logon.
   - **Create a computer status snapshot** - creates an ESET SysInspector computer snapshot - gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
   - **On-demand computer scan** - performs a computer scan of files and folders on your computer.
   - **First-scan** - by default, 20 minutes after installation or reboot a computer scan will be performed as a low priority task.
   - **Update** - schedules an update task to perform an update of virus signature database and program modules.
   - **Hyper-V scan** - schedules a scan of the virtual disks within Hyper-V.
   - **Regular database scan** - lets you schedule a database scan and choose items that will be scanned. It is basically an On-demand database scan.
2. If you want to deactivate the task once it is created, click the switch next to **Enabled**. You can activate the task later using the check box in the Scheduler view. Click **Next**.
3. Select when you want the **Scheduled task to run**:
   - **Once** - the task will be performed only once at specified date and time.
   - **Repeatedly** - the task will be performed at the specified time interval (in minutes).
   - **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.
   - **Event triggered** - the task will be performed after a specified event.
4. If you want to prevent the task from being executed when the system is running on batteries (for example UPS), click the switch next to **Skip task when running on battery power**. Click **Next**.
5. If the task could not be run at the scheduled time, you can choose when it will be run:
   - **At the next scheduled time**
   - **As soon as possible**
   - **Immediately, if the time since the last run exceeds a specified value** (the interval can be defined using the **Time since last run** selector)
6. Click **Next**. Depending on the Task type, **Task details** might need to be specified. Once done, click **Finish**. The new scheduled task will appear in the Scheduler view.

### 7.6.9 Submit samples for analysis

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

Alternatively, you can submit the file by email. To do so, 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. Please remember to use a descriptive subject and enclose as much information about the file as possible (for example, the website you downloaded it from).

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

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

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

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

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

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

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

### 7.6.9.1 Suspicious file

**Observed signs and symptoms of malware infection** - Enter a description of the suspicious file behavior observed on your computer.

**File origin (URL address or vendor)** - Please enter the file origin (source) and how you encountered this file.

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

NOTE

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

### 7.6.9.2 Suspicious site

Please 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.
- Select **Other** if the aforementioned options do not refer the site you are going to submit.

**Notes and additional information** - Here you can enter additional info or a description that will help while analyzing the suspicious website.

### 7.6.9.3 False positive file

We request that you submit files that are detected as an infection but are not infected  to improve our antivirus and antispyware 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 virus signature database.

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

**File origin (URL address or vendor)** - Please enter a file origin (source) and note how you encountered this file.

**Application's purpose** - The general application description, type of application (for example, browser, media player, ...) and its functionality.

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

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

### 7.6.9.4 False positive site

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

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

### 7.6.9.5 Other

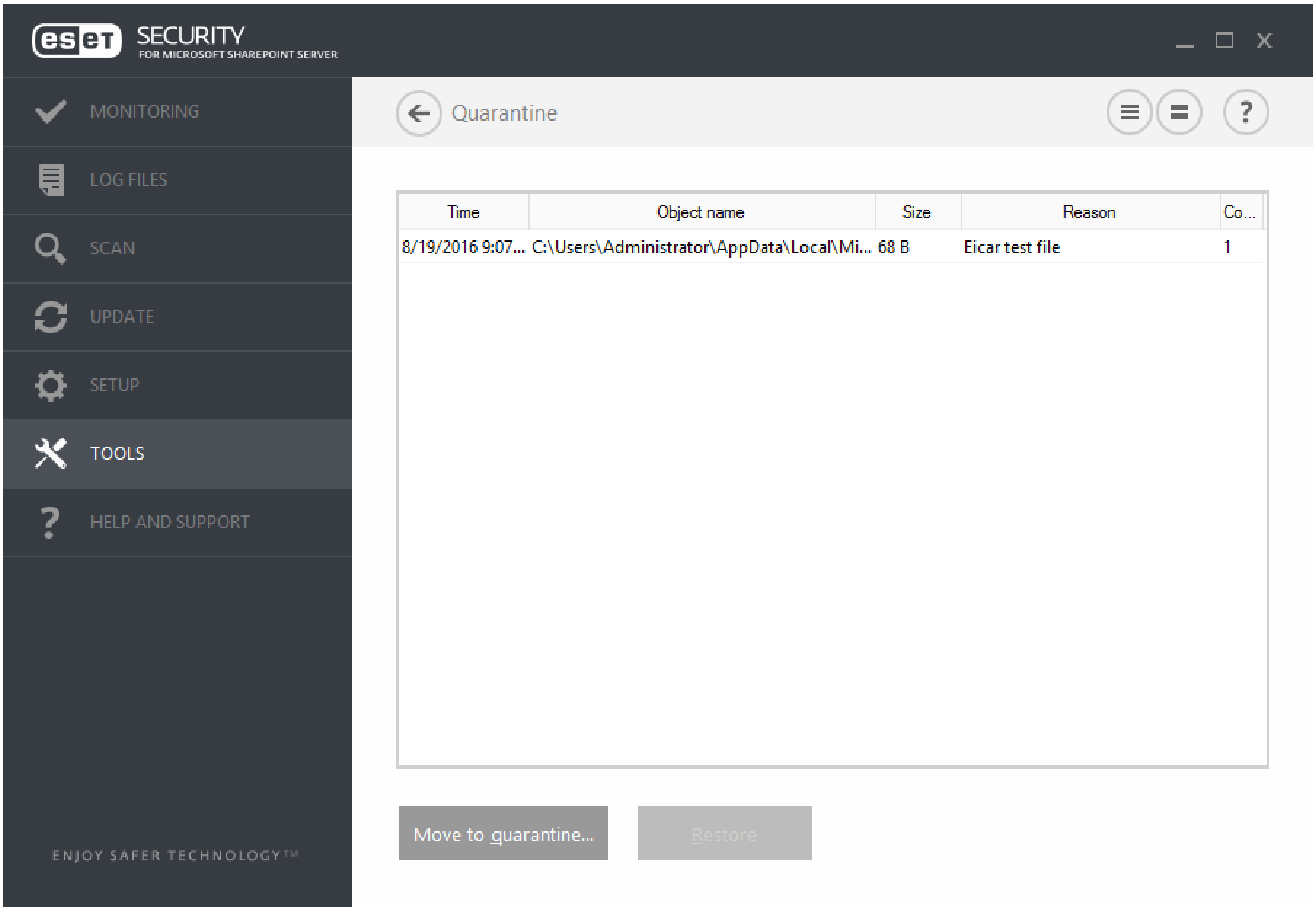
Use this form if the file cannot be categorized as a **Suspicious file** or **False positive**.

**Reason for submitting the file** - Please enter a detailed description and the reason for sending the file.

### 7.6.10 Quarantine

The main function of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET 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 antivirus scanner. Quarantined files can be submitted for analysis to the ESET Virus Lab.



| Time | Object name | Size | Reason | Co... |
|---|---|---|---|---|
| 8/19/2016 9:07... | C:\Users\Administrator\AppData\Local\Mi... | 68 B | Eicar test file | 1 |

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

**Quarantining files**

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

**Restoring from Quarantine**

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

NOTE

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

### Submitting a file from the Quarantine

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

## 7.7 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.

### Help

- **Search ESET Knowledgebase** - The ESET Knowledgebase contains answers to the most frequently asked questions as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various types of problems.
- **Open help** - Click this link to launch the ESET Security for Microsoft SharePoint help pages.
- **Find quick solution** - Select this to find solutions to the most frequently encountered problems. We recommend that you read this section before contacting technical support.

### Customer Care

- **Submit support request** - If you cannot find an answer to your problem, you can also use this form located on the ESET website to quickly contact our Customer Care department.

### Support Tools

- **Threat encyclopedia -** Links to the ESET Threat Encyclopedia, which contains information about the dangers and symptoms of different types of infiltration.
- **ESET Log Collector** - Links to the ESET Log Collector download page. Log Collector is an application that automatically collects information, such as configuration and logs from your server in order to help resolve issues more quickly. For more information about ESET Log Collector see Online help.
- **Virus signature database history** - Links to ESET Virus radar, which contains information about versions of the ESET Virus signature database.
- **ESET Specialized cleaner** - This cleaner automatically identifies and removes common malware infections, for more information please visit this ESET Knowledgebase article.

### Product and License information

- **About ESET Security for Microsoft SharePoint -** Displays information about your copy of ESET Security for Microsoft SharePoint.
- Activate product / Manage license - Click to launch the Product activation window. Select one of the available methods to activate ESET Security for Microsoft SharePoint.

### 7.7.1 How to

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

How to update ESET Security for Microsoft SharePoint

How to activate ESET Security for Microsoft SharePoint

How to schedule a scan task (every 24 hours)

How to remove a virus from my server

How Automatic exclusions work

If your problem is not included in the help pages list above, try searching by keyword or phrase describing your problem and search within the ESET Security for Microsoft SharePoint Help Pages.

If you cannot find the solution to your problem/question within the Help Pages, you can try our regularly updated online Knowledgebase.

If necessary, you can directly contact our online technical support center with your questions or problems. The contact form can be found in the **Help and Support** tab of your ESET program.

#### 7.7.1.1 How to update ESET Security for Microsoft SharePoint

Updating ESET Security for Microsoft SharePoint can be performed either manually or automatically. To trigger the update, click **Update now**. You will find this in the **Update** section of the program.

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

#### 7.7.1.2 How to activate ESET Security for Microsoft SharePoint

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

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

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

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

- **License Key** - A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the the license owner and for activation of the license.
- **Security Admin** - An account created on the ESET License Administrator portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.
- **Offline License file** - An automatically generated file that will be transferred to the ESET product to provide license information. Your offline License file is generated from the license portal and is used in environments where the application cannot connect to the licensing authority.
- Click **Activate later** with ESET Remote Administrator if your computer is a member of a managed network, and your administrator will perform remote activation via ESET Remote Administrator. You can also use this option if you want to activate this client at a later time.

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

> **NOTE**
> ESET Remote Administrator is able to activate client computers silently using licenses made available by the administrator.

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

To create a new task in Scheduler, click **Add task** or right-click and select **Add** from the context menu. A wizard will open to help you create a scheduled task. See below for step-by-step instructions:

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

   - **Run external application** - schedules the execution of an external application.
   - **Log maintenance** - log files also contain leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
   - **System startup file check** - checks files that are allowed to run at system startup or logon.
   - **Create a computer status snapshot** - creates an ESET SysInspector computer snapshot - gathers detailed information about system components (for example, drivers, applications) and assesses the risk level of each component.
   - **On-demand computer scan** - performs a computer scan of files and folders on your computer.
   - **First-scan** - by default, 20 minutes after installation or reboot a computer scan will be performed as a low priority task.
   - **Update** - schedules an update task to perform an update of virus signature database and program modules.
   - **Hyper-V scan** - schedules a scan of the virtual disks within Hyper-V.
   - **Regular database scan** - lets you schedule a database scan and choose items that will be scanned. It is basically an On-demand database scan.

2. If you want to deactivate the task once it is created, click the switch next to **Enabled**. You can activate the task later using the check box in the Scheduler view. Click **Next**.

3. Select when you want the **Scheduled task to run**:

   - **Once** - the task will be performed only once at specified date and time.
   - **Repeatedly** - the task will be performed at the specified time interval (in minutes).
   - **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.
   - **Event triggered** - the task will be performed after a specified event.

4. If you want to prevent the task from being executed when the system is running on batteries (for example UPS), click the switch next to **Skip task when running on battery power**. Click **Next**.

5. If the task could not be run at the scheduled time, you can choose when it will be run:

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

6. Click **Next**. Depending on the Task type, **Task details** might need to be specified. Once done, click **Finish**. The new scheduled task will appear in the Scheduler view.

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

To schedule a regular task, go to **ESET Security for Microsoft SharePoint** > **Tools** > **Scheduler**. The steps below will walk you through the creation of a task to scan your local drives every 24 hours.

To schedule a scan task:

1. Click **Add task** in the main **Scheduler** screen and Enter a **Task name**.
2. Select **On-demand computer scan** from the drop-down menu.
3. If you want to deactivate the task once it is created, click the switch next to **Enabled**. You can activate the task later using the check box in the Scheduler view.
4. Set the scheduler task to run **Repeatedly**. The task will be performed at the specified time interval (1440 minutes).
5. 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**.
6. Click **Next**.
7. Select an action to perform if the scheduled task execution fails for any reason.
   - **At the next scheduled time**
   - **As soon as possible**
   - **Immediately, if the time since the last run exceeds a specified value** (the interval can be defined using the **Time since last run** selector)
8. Click **Next**.
9. From the **Targets** drop-down menu, select **Local drives**.
10. Click **Finish** to apply the task.

#### 7.7.1.5 How to remove a virus from your server

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

1. From the main ESET Security for Microsoft SharePoint window, click **Computer scan**.

2. Click **Smart scan** to begin scanning your system.

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

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

For additional information please see our regularly updated Knowledgebase article.

### 7.7.2 Submit support request

In order to provide assistance as quickly and accurate as possible, ESET requires information about your ESET Security for Microsoft SharePoint configuration, detailed system system information, running processes (ESET SysInspector log file) and registry data. ESET will only use this data to provide technical assistance to the customer.

When you submit the web form, your system configuration data will be submitted to ESET. Select **Always submit this information** to remember this action for this process. To submit the form without sending any data select **Don't submit data** and you can contact ESET customer care using the online support form.

This setting can also be configured from the **Advanced setup** window (press the **F5** key on your keyboard). Click **Tools** > **Diagnostics** > **Customer Care**.

**NOTE**

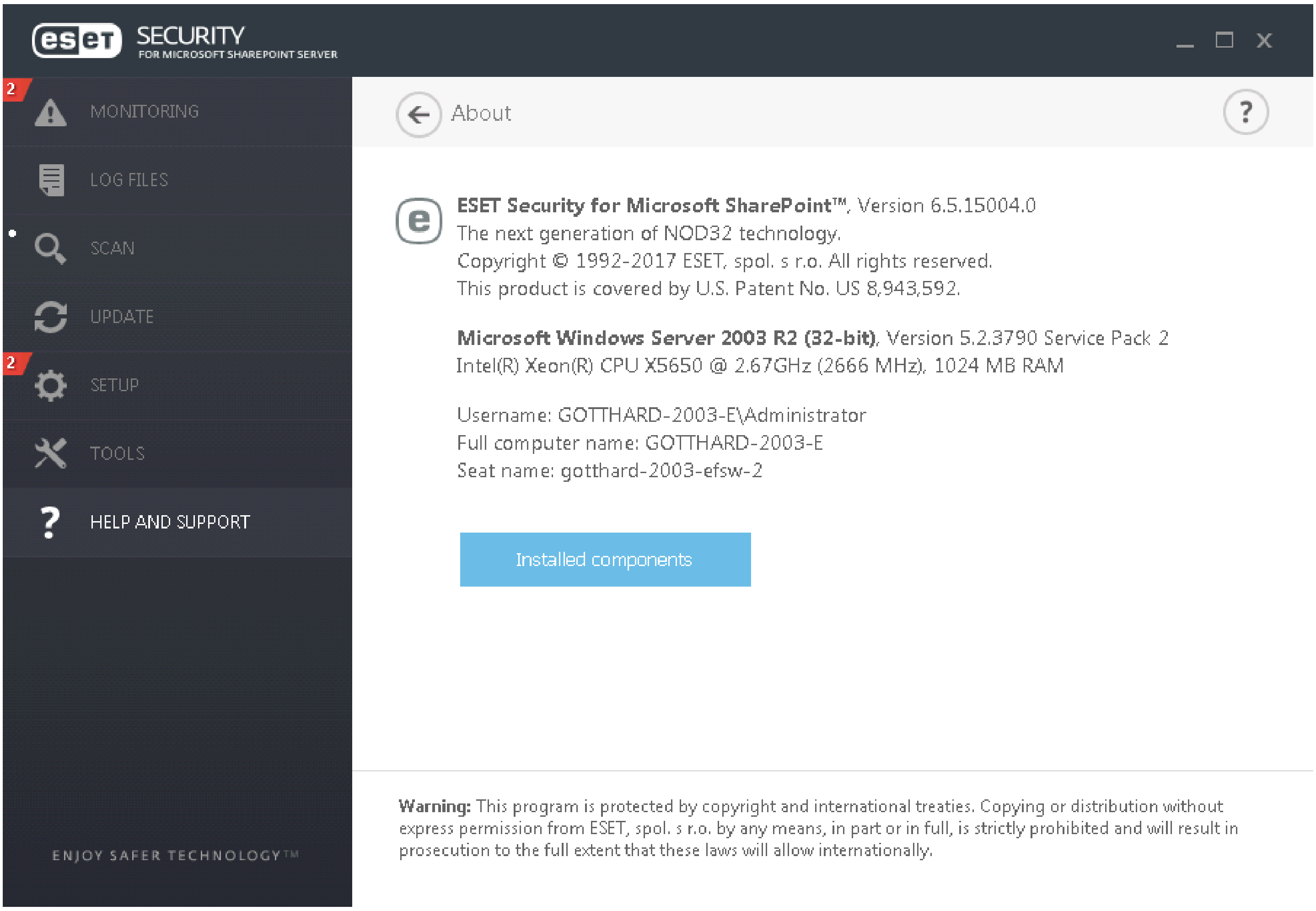
If you choose to submit system data you must fill and submit the web form, otherwise your ticket will not be created and your system data will be lost.

### 7.7.3 ESET Specialized Cleaner

The ESET Specialized Cleaner is a removal tool for common malware infections such as Conficker, Sirefef or Necurs. For more information please visit this [ESET Knowledgebase article](#).

### 7.7.4 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.



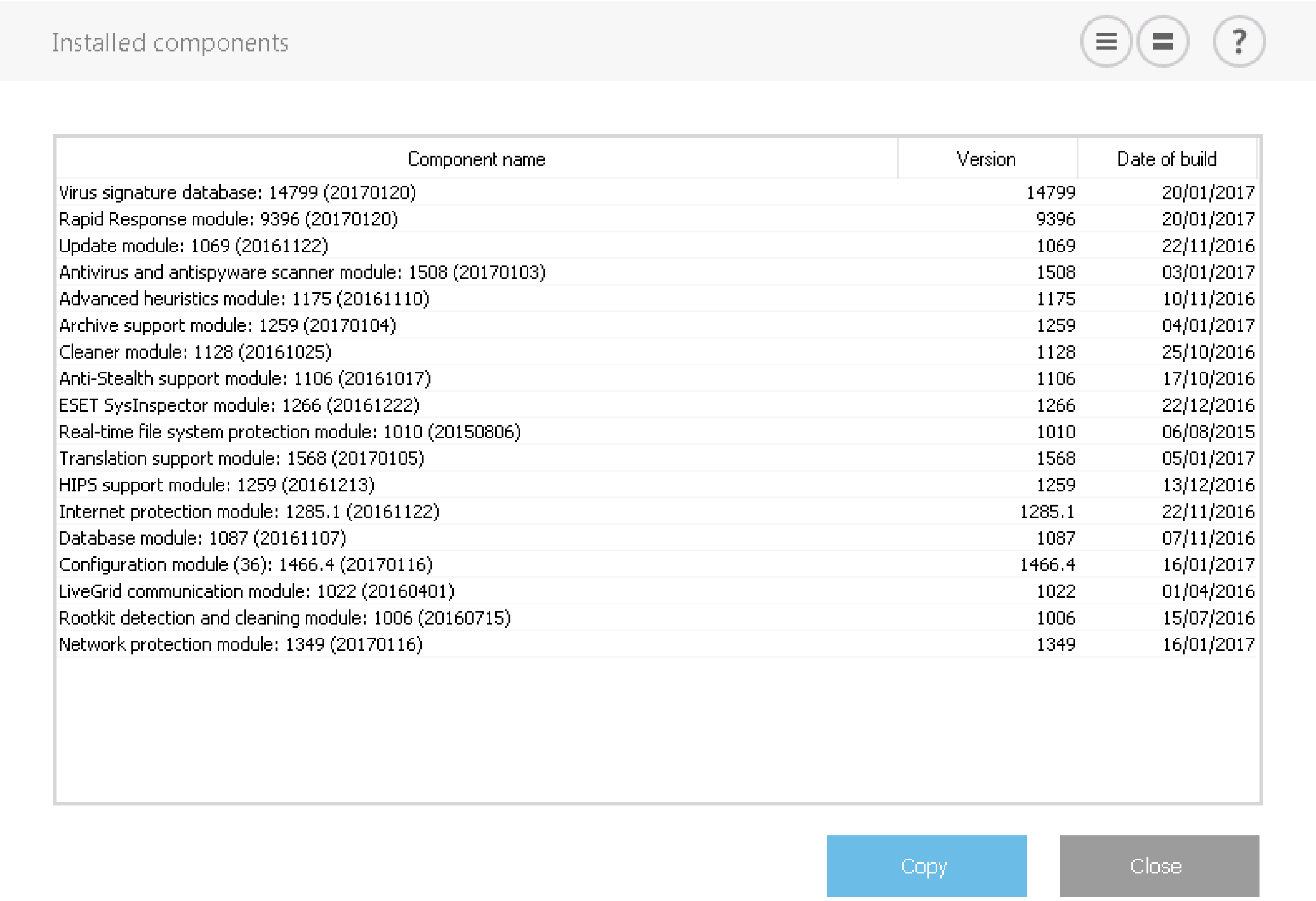
**ESET Security for Microsoft SharePoint™**, Version 6.5.15004.0
The next generation of NOD32 technology.
Copyright © 1992-2017 ESET, spol. s r.o. All rights reserved.
This product is covered by U.S. Patent No. US 8,943,592.

**Microsoft Windows Server 2003 R2 (32-bit)**, Version 5.2.3790 Service Pack 2
Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2666 MHz), 1024 MB RAM

Username: GOTTHARD-2003-E\Administrator
Full computer name: GOTTHARD-2003-E
Seat name: gotthard-2003-efsw-2

**Warning:** This program is protected by copyright and international treaties. Copying or distribution without express permission from ESET, spol. s r.o. by any means, in part or in full, is strictly prohibited and will result in prosecution to the full extent that these laws will allow internationally.

**Installed components** contain information about modules. Click **Installed components** 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.



| Component name | Version | Date of build |
|---|---|---|
| Virus signature database: 14799 (20170120) | 14799 | 20/01/2017 |
| Rapid Response module: 9396 (20170120) | 9396 | 20/01/2017 |
| Update module: 1069 (20161122) | 1069 | 22/11/2016 |
| Antivirus and antispyware scanner module: 1508 (20170103) | 1508 | 03/01/2017 |
| Advanced heuristics module: 1175 (20161110) | 1175 | 10/11/2016 |
| Archive support module: 1259 (20170104) | 1259 | 04/01/2017 |
| Cleaner module: 1128 (20161025) | 1128 | 25/10/2016 |
| Anti-Stealth support module: 1106 (20161017) | 1106 | 17/10/2016 |
| ESET SysInspector module: 1266 (20161222) | 1266 | 22/12/2016 |
| Real-time file system protection module: 1010 (20150806) | 1010 | 06/08/2015 |
| Translation support module: 1568 (20170105) | 1568 | 05/01/2017 |
| HIPS support module: 1259 (20161213) | 1259 | 13/12/2016 |
| Internet protection module: 1285.1 (20161122) | 1285.1 | 22/11/2016 |
| Database module: 1087 (20161107) | 1087 | 07/11/2016 |
| Configuration module (36): 1466.4 (20170116) | 1466.4 | 16/01/2017 |
| LiveGrid communication module: 1022 (20160401) | 1022 | 01/04/2016 |
| Rootkit detection and cleaning module: 1006 (20160715) | 1006 | 15/07/2016 |
| Network protection module: 1349 (20170116) | 1349 | 16/01/2017 |

### 7.7.5 Product activation

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

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

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

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

- **License Key** - A unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX which is used for identification of the the license owner and for activation of the license.
- **Security Admin** - An account created on the ESET License Administrator portal with credentials (email address + password). This method allows you to manage multiple licenses from one location.
- **Offline License file** - An automatically generated file that will be transferred to the ESET product to provide license information. Your offline License file is generated from the license portal and is used in environments where the application cannot connect to the licensing authority.
- Click **Activate later** with ESET Remote Administrator if your computer is a member of a managed network, and your administrator will perform remote activation via ESET Remote Administrator. You can also use this option if

you want to activate this client at a later time.

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

NOTE
ESET Remote Administrator is able to activate client computers silently using licenses made available by the administrator.

### 7.7.5.1 Registration

Register your license by completing the fields in the registration form and clicking **Continue**. The fields marked as required in brackets are mandatory. This information will only be used for matters involving your ESET License.

### 7.7.5.2 Security Admin activation

The Security Admin account is an account created on the license portal with your **email address** and **password**, which is able to see all seat authorizations.

A **Security Admin** account allows you to manage multiple licenses. If you do not have a Security Admin account, click **Create account** and you will be redirected to the ESET License Administrator web page where you can register with your credentials.

If you have forgotten your password click **Forgotten password?** and you will be redirected to the ESET Business portal. Enter your email address and click **Submit** to confirm. After that you will obtain a message with instructions to reset your password.

NOTE
For more information about using ESET License Administrator, see the ESET License Administrator User Guide.

### 7.7.5.3 Activation failure

Activation of ESET Security for Microsoft SharePoint was not successful. Make sure you have entered the proper **License Key** or attached an **Offline License**. If you have a different **Offline License**, please enter it again. To check the license key you entered, click **recheck the License Key** or click **purchase a new license** and you will be redirected to our webpage where you can buy a new license.

### 7.7.5.4 License

If you choose the **Security Admin** activation option, you will be prompted to select a license associated with your account that will be used for ESET Security for Microsoft SharePoint. Click **Activate** to continue.

### 7.7.5.5 Activation progress

ESET Security for Microsoft SharePoint is now activating, please be patient. This may take a few moments.

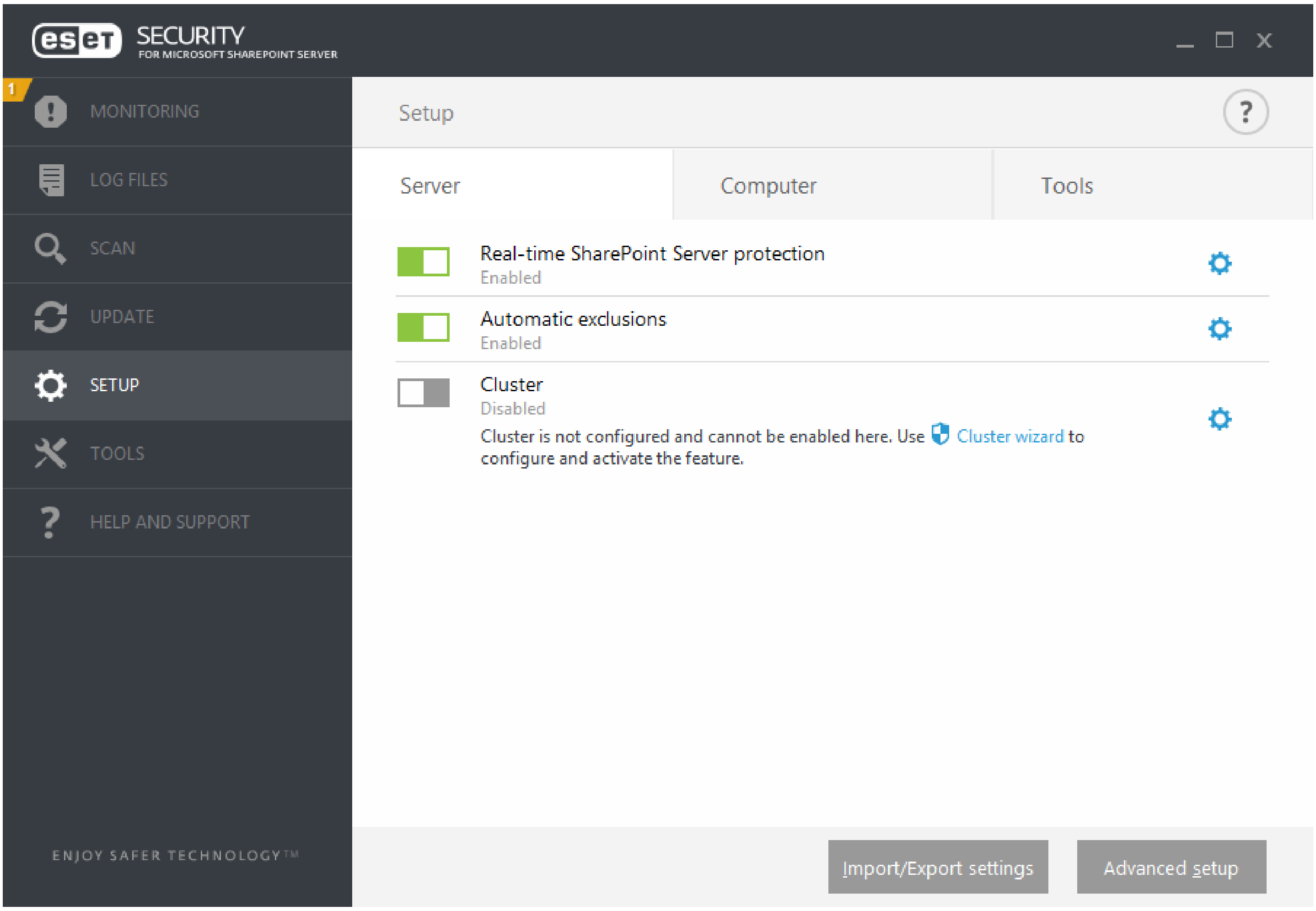
### 7.7.5.6 Activation successful

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

# 8. Working with ESET Security for Microsoft SharePoint

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

- Server
- Computer
- Tools



Real-time SharePoint Server protection
Enabled

Automatic exclusions
Enabled

Cluster
Disabled
Cluster is not configured and cannot be enabled here. Use Cluster wizard to configure and activate the feature.

To temporarily disable individual modules, click the green switch 🟩 next to the desired module. Note that this may decrease the protection level of your computer.
To re-enable the protection of a disabled security component, click the red switch 🟥 to return a component to its enabled state.
To access detailed settings for a particular security component, click the gear icon ⚙.

Click **Advanced setup** or press **F5** to configure advanced settings.

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

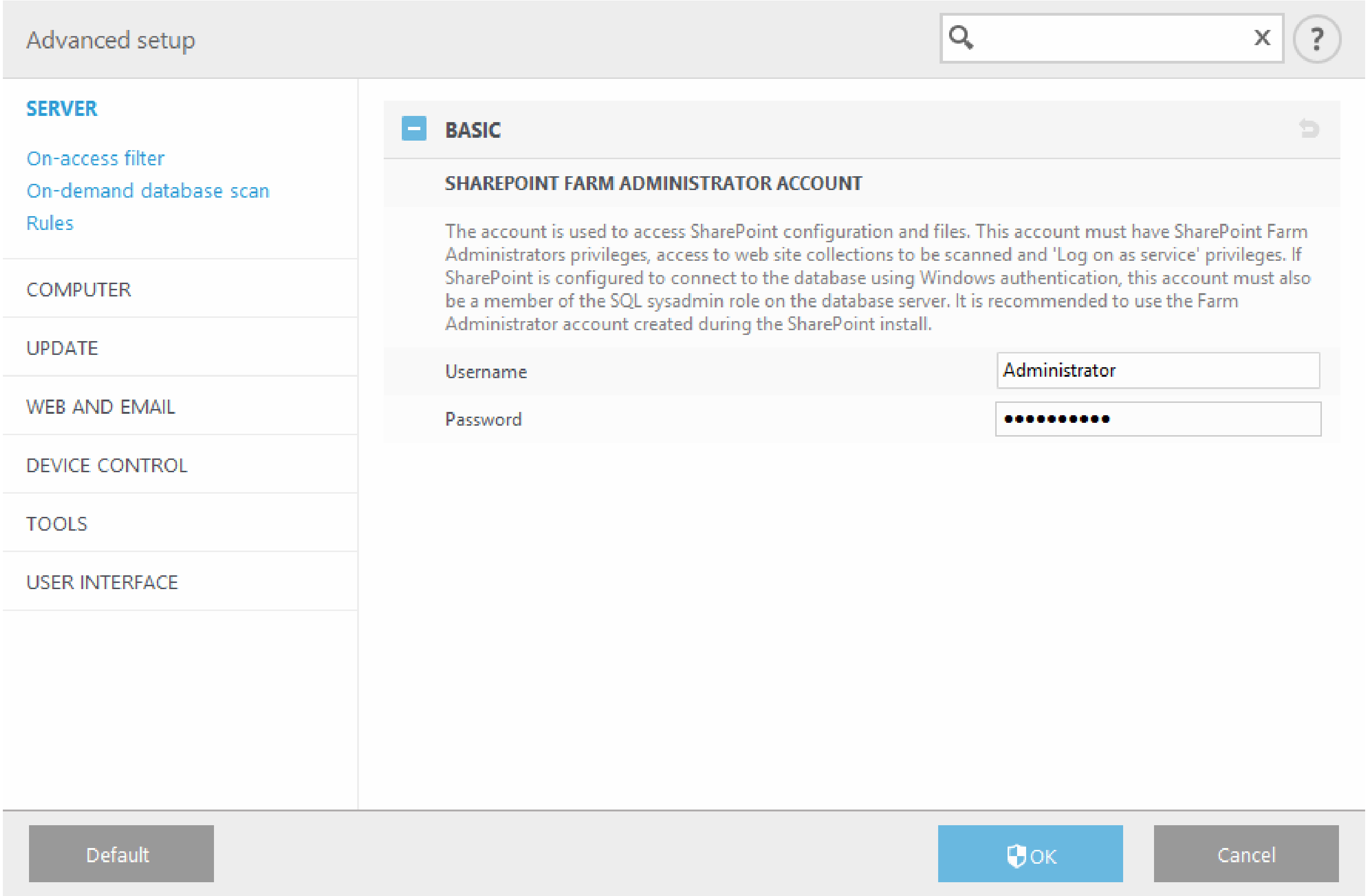
## 8.1 Server

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

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

IMPORTANT
This account must have SharePoint Farm Administrator privileges to access website collections for scanning as well as '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 enter valid logon credentials, ESET Security for Microsoft SharePoint will not be functional after the installation. If the installation is performed without the use of GUI, you will need to enter the SharePoint administrator account via GUI or eShell afterwards, otherwise the product will not work.

NOTE
To ensure continuous protection, you must update SharePoint administrator account credentials any time 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.



SHAREPOINT FARM ADMINISTRATOR ACCOUNT

The account is used to access SharePoint configuration and files. This account must have SharePoint Farm Administrators privileges, access to web site collections to be scanned 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. It is recommended to use the Farm Administrator account created during the SharePoint install.

Username: Administrator

Password: ●●●●●●●●●●

### 8.1.1 On-access filter

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

While **On-access filter** is disabled, ESET Security for Microsoft SharePoint does not scan documents on upload/ download, no On-access filter rules will be applied, and a warning message will be displayed in Monitoring.

> NOTE
> 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 will be scanned via the web interface whenever they are saved in MS Office programs and during synchronization via SharePoint workspace.
- **Scan documents on download** - documents downloaded from SharePoint via a web interface will be scanned when downloading. This includes pictures and documents opened from MS Office programs during synchronization via SharePoint workspace.
- **Allow users to download infected documents** - when enabled, SharePoint will display a warning about infected files when they are found, but you will still be able to open infected files and these files will be blocked rather than deleted. If disabled, a message will be shown saying the document is infected and the download is not possible. Note that the SharePoint administrator is always allowed to download infected files regardless of this setting.
- **Attempt to clean infected documents** - when enabled, infected documents that are cleanable will be 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 will report an AV scanner error. Default is 300 seconds.
- **Number of scan threads** - 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 number of ThreatSense scan engines.

#### 8.1.1.1 Antivirus and antispyware

**Action to take if cleaning not possible -** this actions field allows 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 to them.
- **Block** - infected file is blocked and will not be uploaded/downloaded, also, if possible a message will be shown notifying the user of why the file wasn’t 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. In SharePoint 2010 and 2013, a correct message is shown. In SharePoint 2007 the message will say the file was deleted, even if the user does not have the rights and the file was not actually deleted.

> NOTE

If the document is deleted, its older 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.

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. The default message differs for SharePoint 2007 and SharePoint 2010 / SharePoint 2013. You can use the following variables in the message:

%VIRUSNAME% - infiltration name from the scan engine.
%FILENAME% - file name.
%FILESIZE% - file size.
%PRODUCTNAME% - product name, in this case: ESET Security for Microsoft SharePoint.

Click ThreatSense parameters to modify scan parameters for On-access filter.

### 8.1.2 On-demand database scan

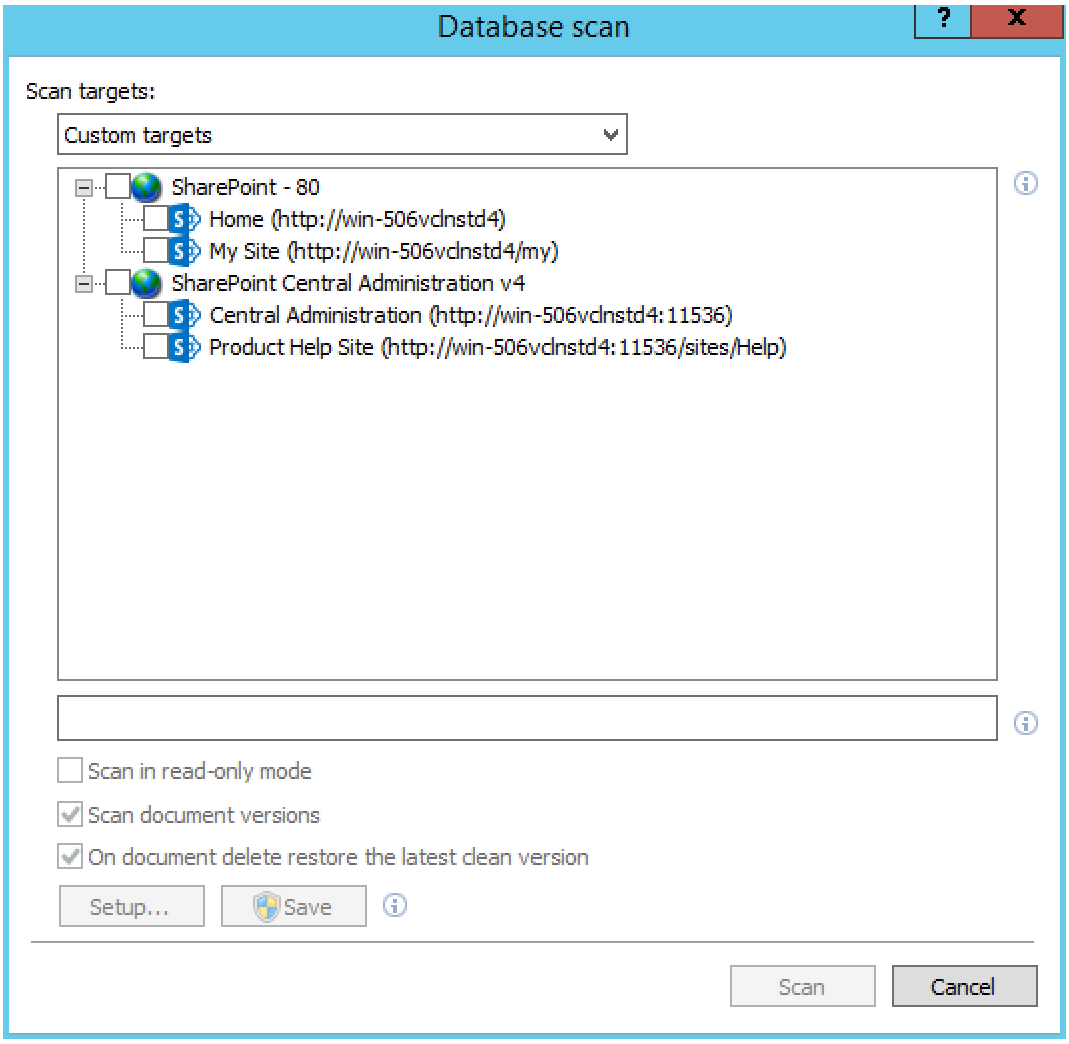
For each selected web site, its hierarchy of folders and files is scanned. Each file, user document or other SharePoint internal file is stored in a temporary file which is then sent to the kernel for scanning. If there are also older versions of a particular file and the **Scan document versions** feature is enabled, then the older 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, older non-infected versions are scanned. If older 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.
- **Scan targets** - a window will open where you can scan all targets or select your specific targets. For more information see On-demand database scan targets.
- **Number of concurrent downloads** - this parameter allows scanning in parallel by multiple threads. When set to 0, the legacy sequential processing is used.

### 8.1.2.1 On-demand database scan targets

In this dialog window you can select SharePoint websites that you want to scan and run the scanning process. A list of websites will be displayed. In the **Scan targets** drop-down menu, you can choose **All targets** or **Custom targets**. When selecting targets manually, click the check box next to a website to add it to the scan.
To add a website, copy and paste its URL into the dialog window. The list might take a few moments to populate, depending on the number and complexity of sites in the list. Also, 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 web site collections, which in turn contain SharePoint websites themselves. Websites are arranged in a hierarchical manner, one of them always being the root.



Database scan

Scan targets: Custom targets

- □ SharePoint - 80
  - □ Home (http://win-506vclnstd4)
  - □ My Site (http://win-506vclnstd4/my)
- □ SharePoint Central Administration v4
  - □ Central Administration (http://win-506vclnstd4:11536)
  - □ Product Help Site (http://win-506vclnstd4:11536/sites/Help)

□ Scan in read-only mode

☑ Scan document versions

☑ On document delete restore the latest clean version

- **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, older non-infected versions are scanned. If older 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.
- Click **Setup** to open Advanced setup for On-demand Database scan.
- Click to **Save** your selected scan targets or parameters.

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

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

#### 8.1.2.1.1 Antivirus and antispyware

**Action to take if cleaning not possible -** select what action should be taken when an infected file is found and cleaning is not possible (Delete is not considered cleaning):

- **No action** - no changes are made, 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 not available when ThreatSense engine parameter cleaning level is set to No cleaning.

**Quarantine infected files** - when enabled, files that are marked for deletion will be put into quarantine. Allows you to disable quarantine so that a lot of files are not accumulating in quarantine. For instance, if partition, on which the quarantine is located, is too small and could potentially get clogged up. But the quarantine should not usually 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.

Click ThreatSense parameters to modify scan parameters for On-demand database scan.

### 8.1.3 Rules

**Rules** allow administrators to manually define and manage file filtering conditions and actions to take with filtered files. Rules are applied according to set of combined conditions. There are a two separate sets of rules:

- On-access filter
- On-demand database scan

Rules have a different sets of conditions and actions available during On-access filer or On-demand database scan. Select **Edit** next to define Conditions and Actions using the Rule wizard.

#### 8.1.3.1 Rules list

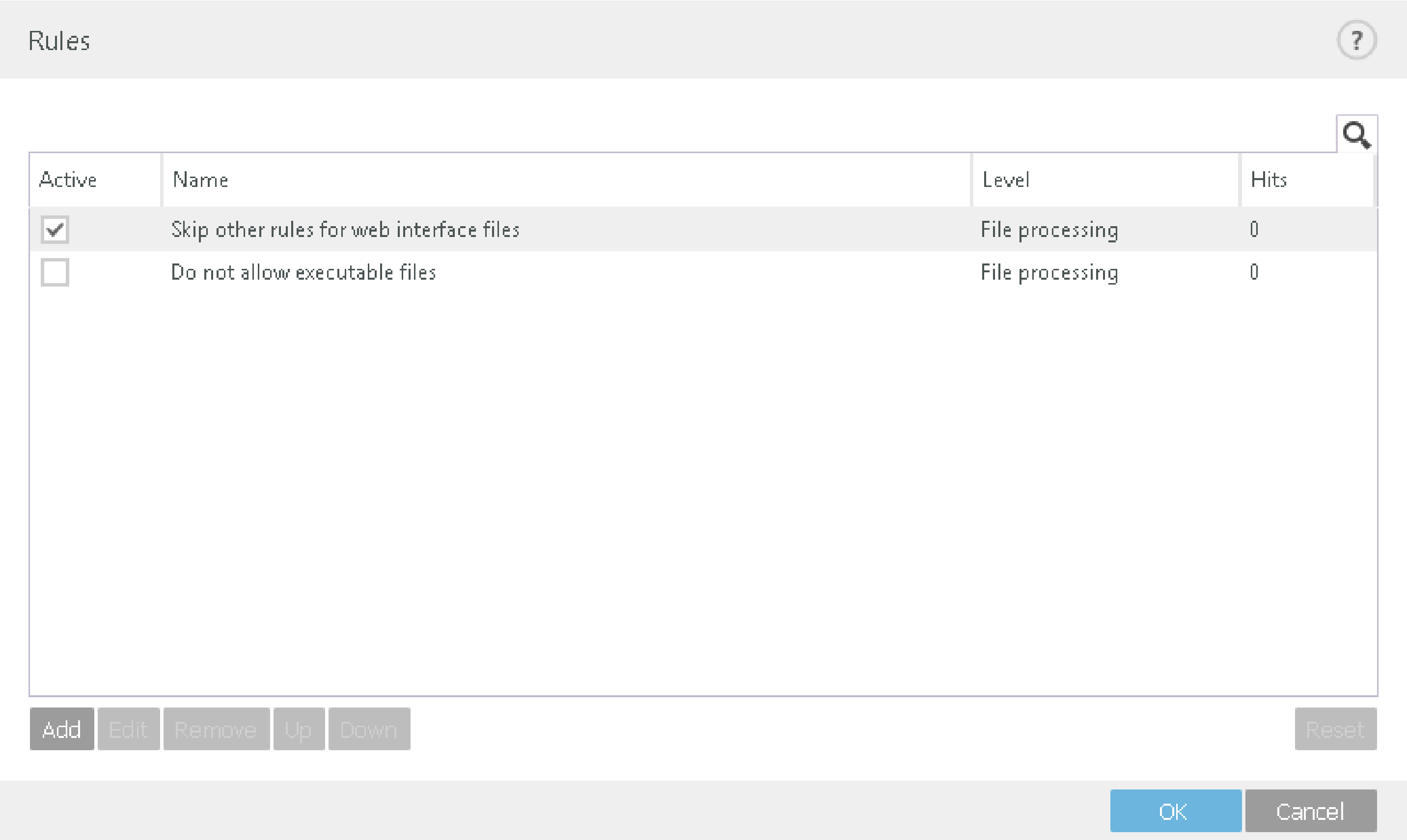
**Rules** list window displays existing rules. Rules are classified into three levels and are evaluated in this order:

- **Filtering rules (1) -** rule evaluated before AV scan
- **File processing rules (2) -** rule evaluated during file scanning
- **Result processing rules (3) -** rule evaluated after AV scan

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

**IMPORTANT**

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



| Active | Name | Level | Hits |
|---|---|---|---|
| ☑ | Skip other rules for web interface files | File processing | 0 |
| □ | Do not allow executable files | File processing | 0 |

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

- **Add** - adds a new rule
- **Edit** - modifies an existing rule
- **View** - allows you to view a configuration assigned from ERA policy
- **Remove** - removes 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)

> **NOTE**
> If a new rule is added or an existing rule has been modified, message rescan will automatically start using the new/modified rules.

### 8.1.3.1.1 Rule wizard

You can define **Conditions** and **Actions** using the **Rule** wizard. Define Condition(s) first, then Action(s).

- Click **Add** and a Rule condition window will appear where you can select condition type, operation and value.
- From here you can add a Rule action.
- Once conditions and actions are defined, type a **Name** for the rule (something that you'll recognize the rule by), this name will be displayed in the Rules list.
- If you want to prepare rules but plan to use them later, you can click the switch next to **Active** to deactivate the rule. To activate the rule, select the check box next to the rule you want to activate from the Rules list.

> **NOTE**
> **Name** is a mandatory field, if it is highlighted in red, type rule name in the text box and click **OK** button to create the rule. The red highlight does not disappear even though you've entered a rule name, it disappears only after you've clicked **OK**.

Some **Conditions** and **Actions** differ for rules specific to On-access filter and On-demand database scan. This is because each of these protection types use a little different approach when processing messages.

IMPORTANT
If you define multiple conditions, all of the conditions must be met for the rule to be applied. All conditions are connected using the logical operator AND. Even if most of the conditions are met and only a single one isn't, the condition evaluation result is considered *not met* and the rule's action cannot be taken.

### 8.1.3.1.1.1 Rule condition

This wizard lets you add conditions for a rule. Files will be evaluated according to defined conditions.

Select **Type** and **Operation** (if available) from the drop-down list (the list of operations changes depending on what rule type you've chosen), then select **Parameter**. Parameter fields will change depending on rule type and operation.

EXAMPLE
Choose **File size** > **is greater than** and under **Parameter** specify 10 MB. Using these settings, any file that is larger than 10 MB will be processed using rule actions you have specified. For this reason you should specify the action that is taken when a given rule is triggered if you have not done so when setting parameters for that rule.

NOTE
It is possible to add multiple conditions for one rule.

The following **Conditions** 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 file name, you can use wildcards `* ?` etc.<br>This condition applies to the file name 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 file name, you can use wildcards `* ?` etc. |
| **File type** | ✓ | ✓ | Applies to files of a specified type (actual file type is detected by its contents, regardless of file name 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. |

NOTE

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**.

### 8.1.3.1.1.2 Rule action

This window lets you to add actions that will be taken with files that match conditions defined in rules.

NOTE

It is possible to add multiple actions for one rule.

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

| 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. |

## 8.2 Computer

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

- Real-time file system protection
- On-demand computer scan
- Idle-state scanning
- Startup scan
- Removable media
- Document protection
- HIPS

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

- **Potentially unwanted applications** (PUAs) are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way.
  Read more about these types of applications in the glossary.
- **Potentially unsafe applications** refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications include remote access tools, password-cracking applications, and keyloggers (programs that record each keystroke typed by a user). This option is disabled by default.
  Read more about these types of applications in the glossary.
- **Potentially suspicious applications** include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.

**Anti-Stealth technology** is a sophisticated system that detects dangerous programs such as rootkits which are able to hide themselves from the operating system, making it impossible to detect them using ordinary testing techniques.

Processes exclusions allows you to exclude specific processes. For example processes of the backup solution, all file operations attributed to such excluded process are being ignored and considered safe, thus minimizing the interference with the backup process.

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

### 8.2.1 An infiltration is detected

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

**Standard behavior**

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

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

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

### Multiple threats

If any infected files were not cleaned during Computer scan (or the Cleaning level was set to **No Cleaning**), an alert window prompting you to select actions for those files is displayed. Select an action individually for each threat in the list or you can use **Select action for all listed threats** and choose one action to take on all the threats in the list, then click **Finish**.

### Deleting files in archives

In Default cleaning mode, the entire archive will only be deleted if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. Use caution when performing a Strict cleaning scan, with Strict cleaning enabled an archive will be deleted if it contains at least one infected file regardless of the status of other files in the archive.
If your computer is showing signs of a malware infection, for example, it is slower, often freezes, etc., we recommend that you do the following:

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

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

## 8.2.2 Processes exclusions

This feature allows you to exclude application processes from Antivirus On-access scanning only. These 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 of the operating system.

When a process is excluded, its executable file is not monitored. Activity of excluded process is not monitored by ESET Security for Microsoft SharePoint and no scanning is performed on any file operations performed by the process.

Click **Add, Edit** and **Remove** to manage Processes exclusions.

EXAMPLE
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 creating exclusions for web browsers.

NOTE
HIPS is involved in the evaluation of excluded processes, therefore we recommend that you test newly excluded processes with HIPS enabled (or disabled if you experience problems). Disabling HIPS will not affect process exclusions. If HIPS is disabled, the identification of excluded processes is based on path only.

### 8.2.3 Automatic exclusions

The developers of server applications and operating systems recommend excluding sets of critical working files and folders from antivirus scans for most of their products. Antivirus scans may have a negative influence on a server's performance, 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 antivirus software.

ESET Security for Microsoft SharePoint identifies critical server applications and server operating system files, and automatically adds them to the list of Exclusions. You can see a list of detected server applications under **Automatic exclusions to generate** for which exclusions were created. All automatic exclusions are enabled by default. You can disable/enable each server application by clicking the switch with the following result:

- If an application/operating system exclusion remains enabled, any of its critical files and folders will be added to the list of files excluded from scanning (**Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**). Every time the server is restarted, the system performs an automatic check of exclusions and restores any exclusions that may have been deleted from the list. This is the recommended setting if you want to make sure the recommended Automatic exclusions are always applied.

- If the user disables an application/operating system exclusion, its critical files and folders remain on the list of files excluded from scanning (**Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**). However, they will not be automatically checked and renewed on the **Exclusions** list every time the server is restarted (see point 1 above). We recommend this setting for advanced users, who wish to remove or modify some of the standard exclusions. If you wish to remove the exclusions from the list without restarting the server, you will need to remove them manually from the list (**Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**).

Any user-defined exclusions entered manually (under **Advanced setup** > **Computer** > **Basic** > **Exclusions** > **Edit**) will not be affected by the settings described above.

### 8.2.4 Shared local cache

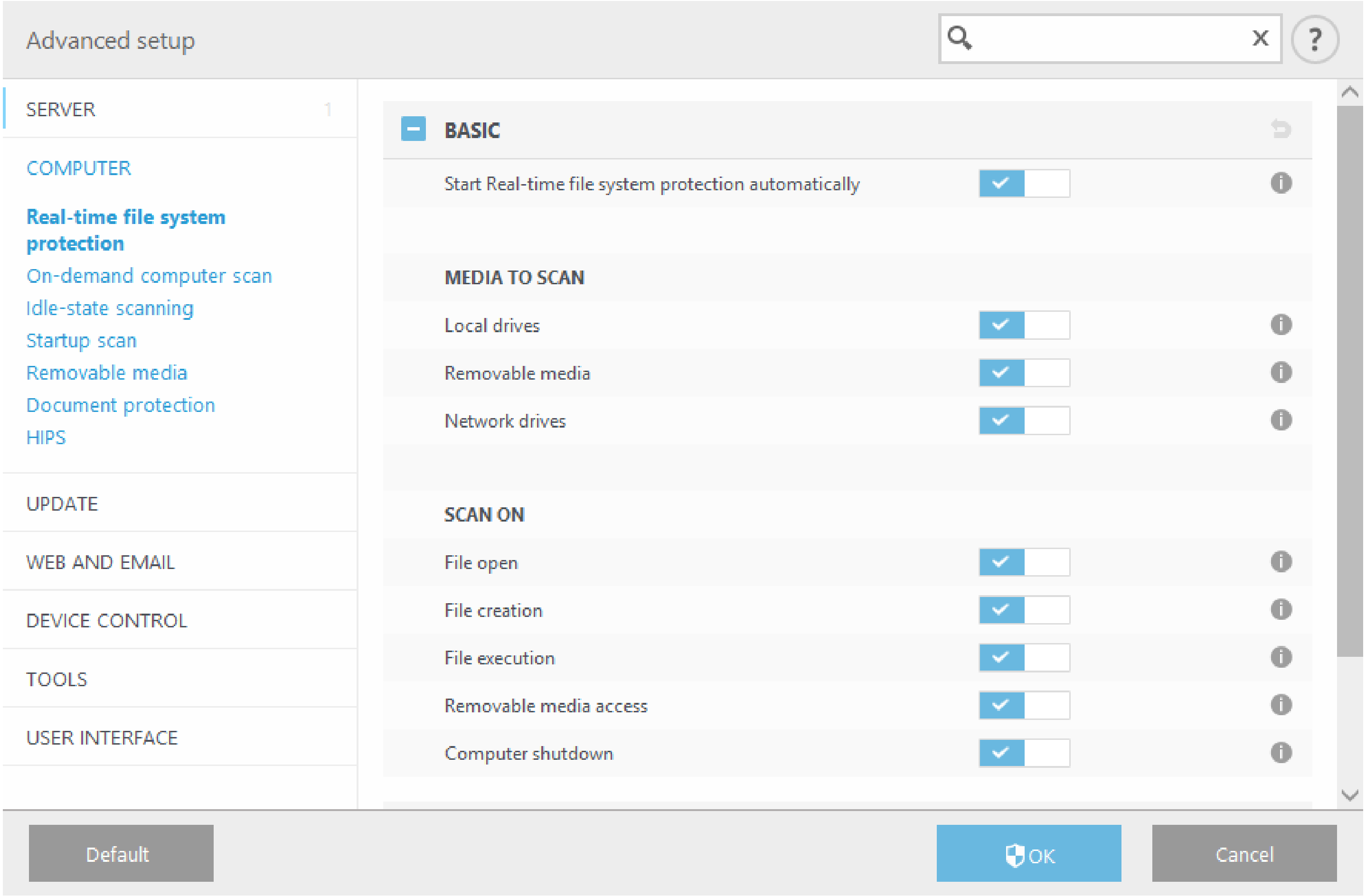
ESET Shared local cache will boost performance in virtualized environments by eliminating duplicate scanning in the network. This ensures that each file will be scanned only once and stored in the shared cache. Turn on the **Caching option** switch to save information about scans of files and folders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

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

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

### 8.2.5 Real-time file system protection

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



BASIC

Start Real-time file system protection automatically ✓

MEDIA TO SCAN

Local drives ✓

Removable media ✓

Network drives ✓

SCAN ON

File open ✓

File creation ✓

File execution ✓

Removable media access ✓

Computer shutdown ✓

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

#### Media to scan

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

- **Local drives** - Controls all system hard drives.
- **Removable media** - Controls CD/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** - Enables or disables scanning when files are opened.
- **File creation** - Enables or disables scanning when files are created.
- **File execution** - Enables or disables scanning when files are run.
- **Removable media access** - Enables or disables scanning triggered by accessing particular removable media with storage space.

- **Computer shutdown** - Enables or disables scanning triggered by computer shutdown.

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

To ensure a minimal system footprint when using real-time protection, files that have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update. This behavior is controlled using **Smart optimization**. If **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**.

### 8.2.5.1 Exclusions

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

⚠ WARNING

Not to be confused with Excluded extensions**.**

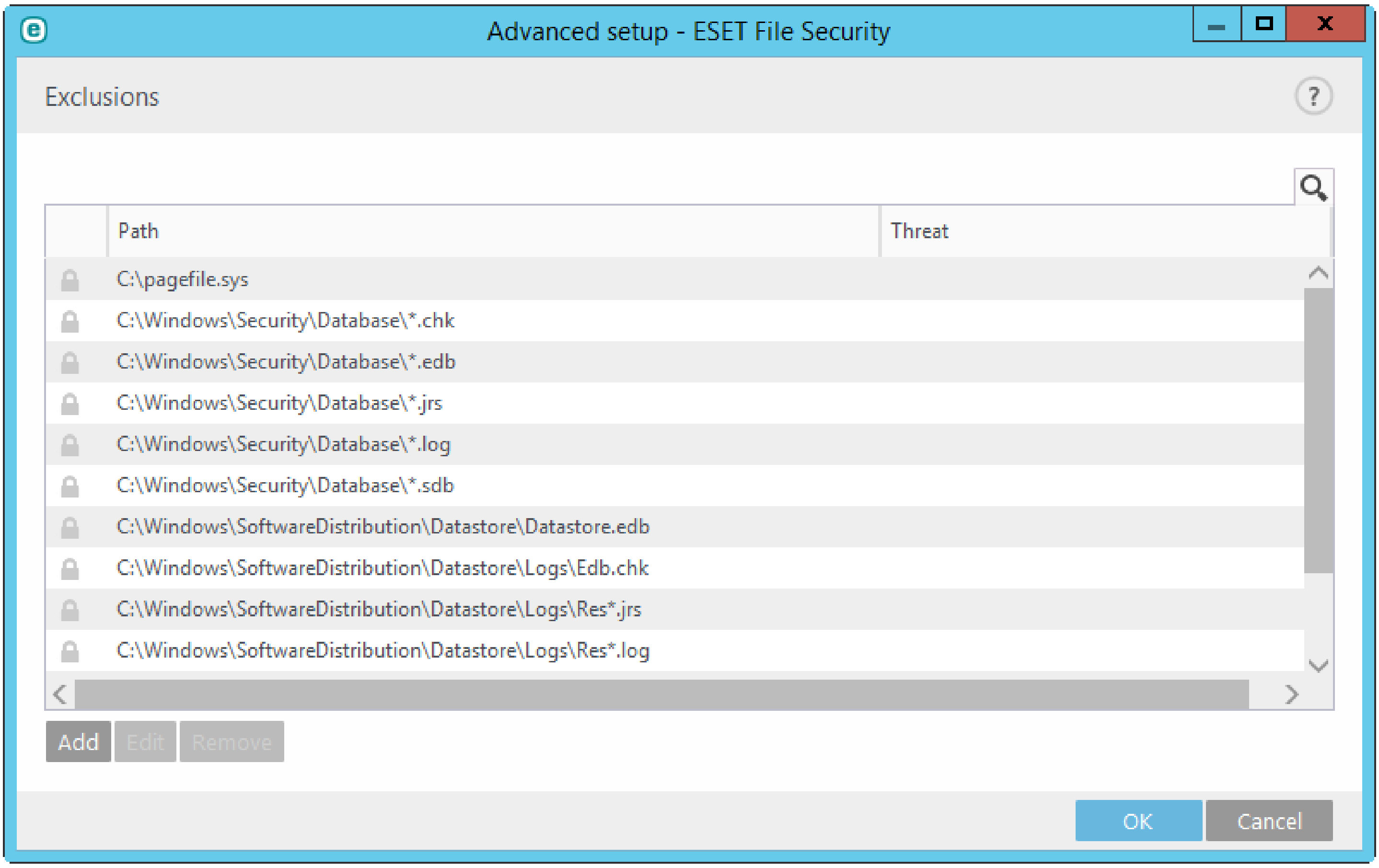
To exclude an object from scanning:

Click Add and enter the path to an object or select it in the tree structure.

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

✓ EXAMPLE

- If you want to exclude all files in a folder, type the path to the folder and use the mask “*.*”.
- To exclude an entire drive including all files and subfolders, use the mask "D:\*".
- If you want to exclude doc files only, use the mask “*.doc“.
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for sure (say “D”), use the following format: “D????.exe”. Question marks replace the missing (unknown) characters.



| Path | Threat |
|---|---|
| C:\pagefile.sys | |
| C:\Windows\Security\Database\*.chk | |
| C:\Windows\Security\Database\*.edb | |
| C:\Windows\Security\Database\*.jrs | |
| C:\Windows\Security\Database\*.log | |
| C:\Windows\Security\Database\*.sdb | |
| C:\Windows\SoftwareDistribution\Datastore\Datastore.edb | |
| C:\Windows\SoftwareDistribution\Datastore\Logs\Edb.chk | |
| C:\Windows\SoftwareDistribution\Datastore\Logs\Res*.jrs | |
| C:\Windows\SoftwareDistribution\Datastore\Logs\Res*.log | |

NOTE

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

### Columns

**Path** - Path to excluded files and folders.
**Threat** - If the name of a threat is displayed next to an excluded file, it means that the file is only excluded for the given threat. If that file becomes infected later with other malware, it will be detected by the antivirus module. This type of exclusion can only be used for certain types of infiltrations, and can be created either in the threat alert window reporting the infiltration (click **Show advanced options** and then select **Exclude from detection**), or select **Tools** > **Quarantine**, right-clicking the quarantined file and then selecting **Restore and exclude from scanning** from the context menu.

### Control elements

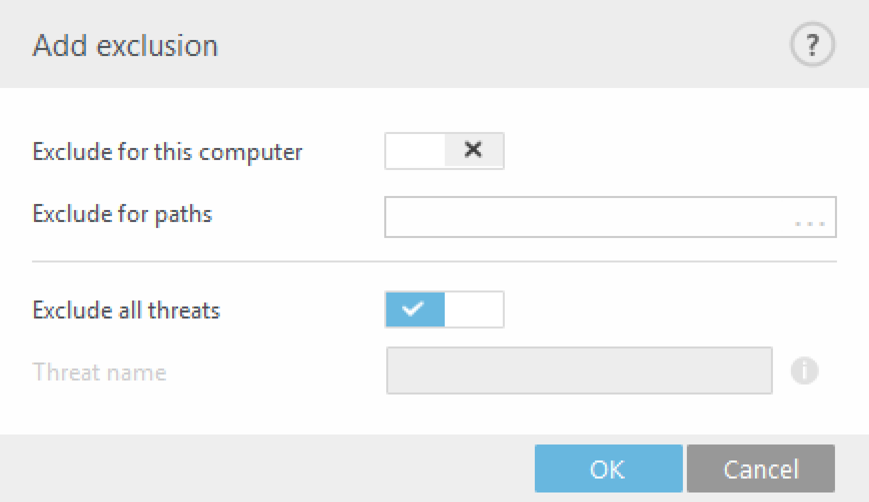
**Add** - Excludes objects from detection.
**Edit** - Enables you to edit selected entries.
**Remove** - Removes selected entries.

### 8.2.5.1.1 Add or Edit exclusion

This dialog window enables you to add or edit exclusions. It can be done in two ways:

- by typing the path to an object to be excluded
- by selecting it in the tree structure (click the **...** at the end of the text field to browse)

If using the first method, wildcards described in the Exclusion format section can be used.



Add exclusion

Exclude for this computer ☒

Exclude for paths

Exclude all threats ☑

Threat name

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

**Exclude all threats / Threat name** – Exclusions apply to potentially unwanted applications, potentially unsafe applications and suspicious applications.

### 8.2.5.1.2 Exclusion format

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

EXAMPLE

- If you want to exclude all files in a folder, type the path to the folder and use the mask “*.*”.
- To exclude an entire drive including all files and subfolders, use the mask "D:\*".
- If you want to exclude doc files only, use the mask “*.doc“.
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for sure (say “D”), use the following format: “D????.exe”. Question marks replace the missing (unknown) characters.

### 8.2.5.2 ThreatSense parameters

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

NOTE
For details about automatic startup file check, see Startup scan.

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

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

To enter the setup window, click **ThreatSense engine parameter setup** in the **Advanced setup** 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
- Idle-state scanning
- Startup scan
- Document protection
- Email client protection
- Web access protection
- Computer scan

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

### Objects to scan

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

- **Operating memory** - Scans for threats that attack the operating memory of the system.
- **Boot sectors** - Scans boot sectors for the presence of viruses in the MBR (Master Boot Record). In case of a Hyper-V Virtual Machine, its disk MBR is scanned in read - only mode.
- **Email files** - The program supports the following extensions: DBX (Outlook Express) and EML.
- **Archives** - The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.
- **Self-extracting archives** – Self-extracting archives (SFX) are archives needing no specialized programs – archives – to decompress themselves.
- **Runtime packers** - After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

### Scan options

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

- **Heuristics** - A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not known by the previous virus signatures database.

- **Advanced heuristics/DNA signatures** - Advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

### Cleaning

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

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

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

**Strict cleaning** - The program will clean or delete all infected files. The only exceptions are system files. If it is not possible to clean a file, the user will be asked what type of action should be taken.

WARNING

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

IMPORTANT

If a Hyper-V host is running on Windows Server 2008 R2, **Normal cleaning** and **Strict cleaning** are not supported. Scanning of Virtual Machine disks is done in read-only mode, no cleaning will be performed. Regardless of the cleaning level selected, the scan is always performed in read-only mode.

### Exclusions

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

### Other

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

- **Scan alternate data streams (ADS)** - Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.
- **Run background scans with low priority** - Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.
- **Log all objects** - If this option is selected, the log file will show all the scanned files, even those not infected. For example, if an infiltration is found within an archive, the log will also list clean files contained within the archive.
- **Enable Smart optimization** - With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.
- **Preserve last access timestamp** - Select this option to keep the original access time of scanned files instead of updating them (for example, for use with data backup systems).

## Limits

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

### Object settings

**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 antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: *unlimited*.

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

**Archive scan setup**

**Archive nesting level** - Specifies the maximum depth of archive scanning. Default value: *10*. For objects detected by Mailbox transport protection, actual nesting level is +1 because archive attachment in an email is considered first level. For example, if you have nesting level set to 3, an archive file with nesting level 3 will only be scanned on a transport layer up to its actual level 2. Therefore, if you want to have archives scanned by Mailbox transport protection up to level 3, set the value for **Archive nesting level** to 4.

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

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

### 8.2.5.2.1 File extenstions excluded from scanning

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

By default, all files are scanned. Any extension can be added to the list of files excluded from scanning.

It may be necessary to exclude a file extension if scanning certain file types prevents the program that uses these extensions from running properly. For example, it may be advisable to exclude the `.edb`, `.eml` and `.tmp` extensions when using Microsoft Exchange servers.

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

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

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

### 8.2.5.2.2 Additional ThreatSense parameters

**Additional ThreatSense parameters for newly created and modified files** - The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before the virus signature database update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, disable **Default archive scan settings**.

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

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

### 8.2.5.2.3 Cleaning levels

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

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

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

**Strict cleaning** - The program will clean or delete all infected files. The only exceptions are system files. If it is not possible to clean a file, the user will be asked what type of action should be taken.

⚠ WARNING

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

❗ IMPORTANT

If a Hyper-V host is running on Windows Server 2008 R2, **Normal cleaning** and **Strict cleaning** are not supported. Scanning of Virtual Machine disks is done in read-only mode, no cleaning will be performed. Regardless of the cleaning level selected, the scan is always performed in read-only mode.

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

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

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

### 8.2.5.2.5 Checking real-time protection

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

### 8.2.5.2.6 What to do if real-time protection does not work

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

**Real-time protection is disabled**

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup** in the main program window and click **Real-time file system protection**.

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

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

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

**Real-time protection does not start**

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

### 8.2.5.2.7 Submission

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

When there are files pending submission, the **Submit now** button will be active. Click this button to immediately submit files and statistical information.

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

### 8.2.5.2.8 Statistics

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

Below is an example of a statistical package submitted:

```
# utc_time=2005-04-14 07:21:28
# country=“Slovakia“
# language=“ENGLISH“
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

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

### 8.2.5.2.9 Suspicious files

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

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 virus signature update.

File submission can be set to occur automatically, or select **Ask before submitting** if you want to know which files have been sent for analysis and confirm the submission.

If you do not want any files to be submitted, select **Do not submit for analysis**. Selecting not to submit files for analysis does not affect submission of statistical information which is configured in its own setup (see section Statistics).

**When to submit** - By default, **As soon as possible** is selected for suspicious files to be sent to ESET‘s Threat Lab. This is recommended if a permanent Internet connection is available and suspicious files can be delivered without delay. Select the **During** update option for suspicious files to be uploaded to ThreatSense.Net during the next update.

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

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

### 8.2.6 On-demand computer scan and Hyper-V scan

This section provides options to select scanning parameters.

> NOTE
> This scan profile selector applies to both On-demand computer scan and Hyper-V scan.

**Selected profile** - A particular set of parameters used by the on-demand scanner. To create a new one, click **Edit** next to **List of profiles**.

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

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

- **By profile settings** - Selects targets set in the selected scan profile.
- **Removable media** - Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** - Selects all system hard drives.
- **Network drives** - Selects all mapped network drives.
- **Shared Folders** - Selects all folders on the local server that are shared.
- **No selection** - Cancels all selections.

Click ThreatSense parameters to modify scan parameters (for example, detection methods) for the On-demand computer scanner.

### 8.2.6.1 Custom scan and Hyper-V scan launcher

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

> NOTE
> This scan target selector applies to both Custom scan and Hyper-V scan.

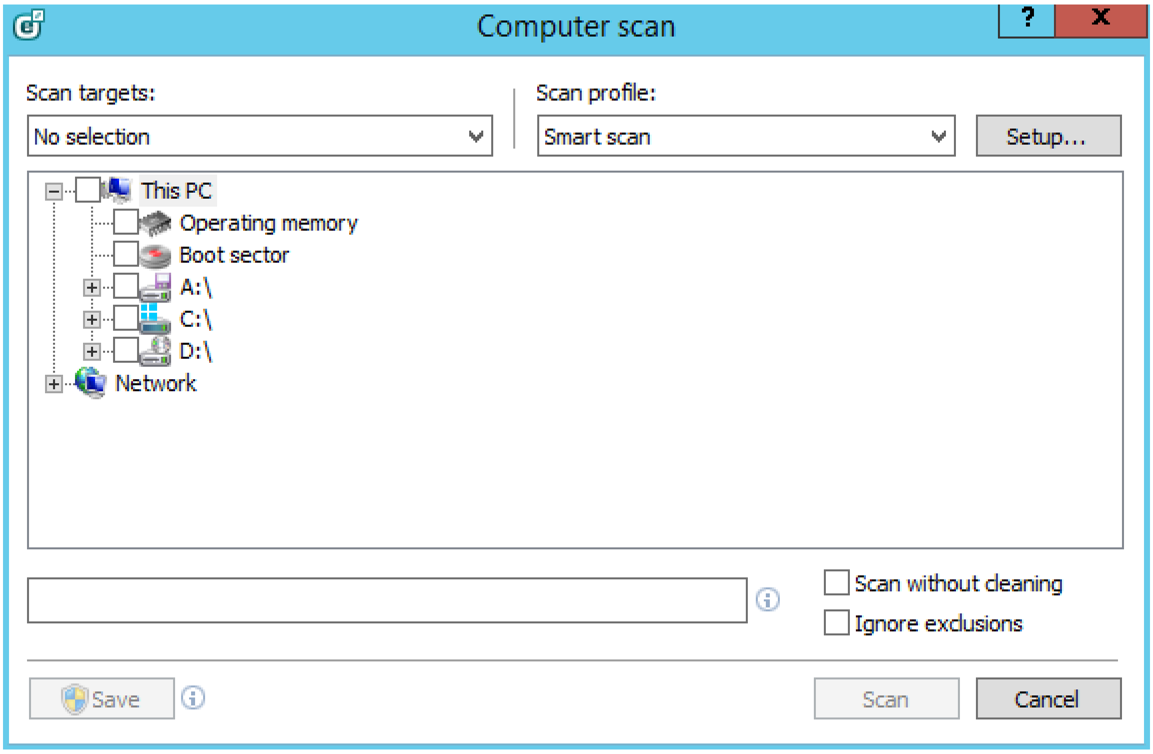
The scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. Select targets from the tree structure, which lists all devices available on the computer. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** - Selects targets set in the selected scan profile.
- **Removable media** - Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** - Selects all system hard drives.
- **Network drives** - Selects all mapped network drives.
- **Shared Folders** - Selects all folders on the local server that are shared.
- **No selection** - Cancels all selections.

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

**selection**.

**Custom scan** pop-up window:



Scan targets: No selection

Scan profile: Smart scan

- □ This PC
  - □ Operating memory
  - □ Boot sector
  - □ A:\
  - □ C:\
  - □ D:\
- Network

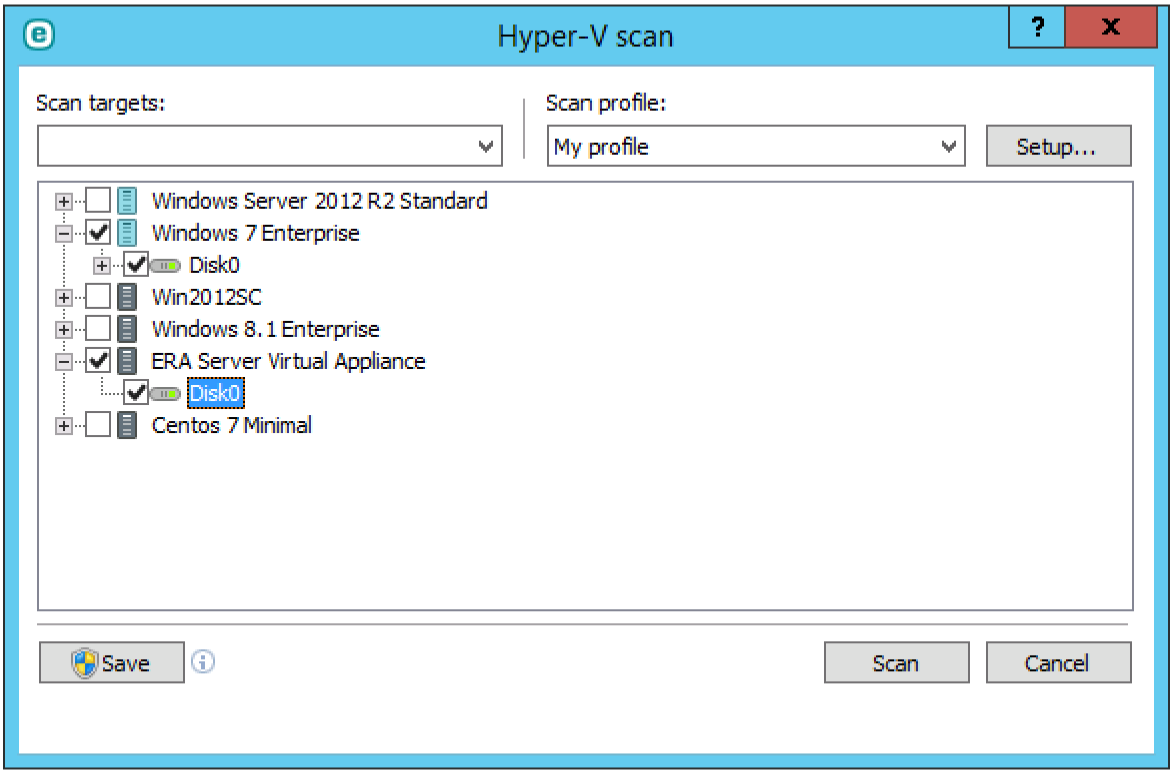
□ Scan without cleaning

□ Ignore exclusions

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.

When you select **Ignore exclusions**, it lets you perform a scan while ignoring exclusions that otherwise apply.

The **Hyper-V scan** pop-up window (see Hyper-V scan for more information):



Scan targets:

Scan profile: My profile

- □ Windows Server 2012 R2 Standard
- ☑ Windows 7 Enterprise
  - ☑ Disk0
- □ Win2012SC
- □ Windows 8.1 Enterprise
- ☑ ERA Server Virtual Appliance
  - ☑ Disk0
- □ Centos 7 Minimal

You can choose a profile from the **Scan profile** drop-down menu to be used for scanning chosen targets. The default profile is **Smart scan**. There are two more pre-defined scan profiles called **In-depth scan** and **Context menu scan**. These scan profiles use different ThreatSense engine parameters. Click **Setup...** to configure a scan profile from the

Scan profile menu in detail. Available options are described in [ThreatSense engine parameters setup].

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

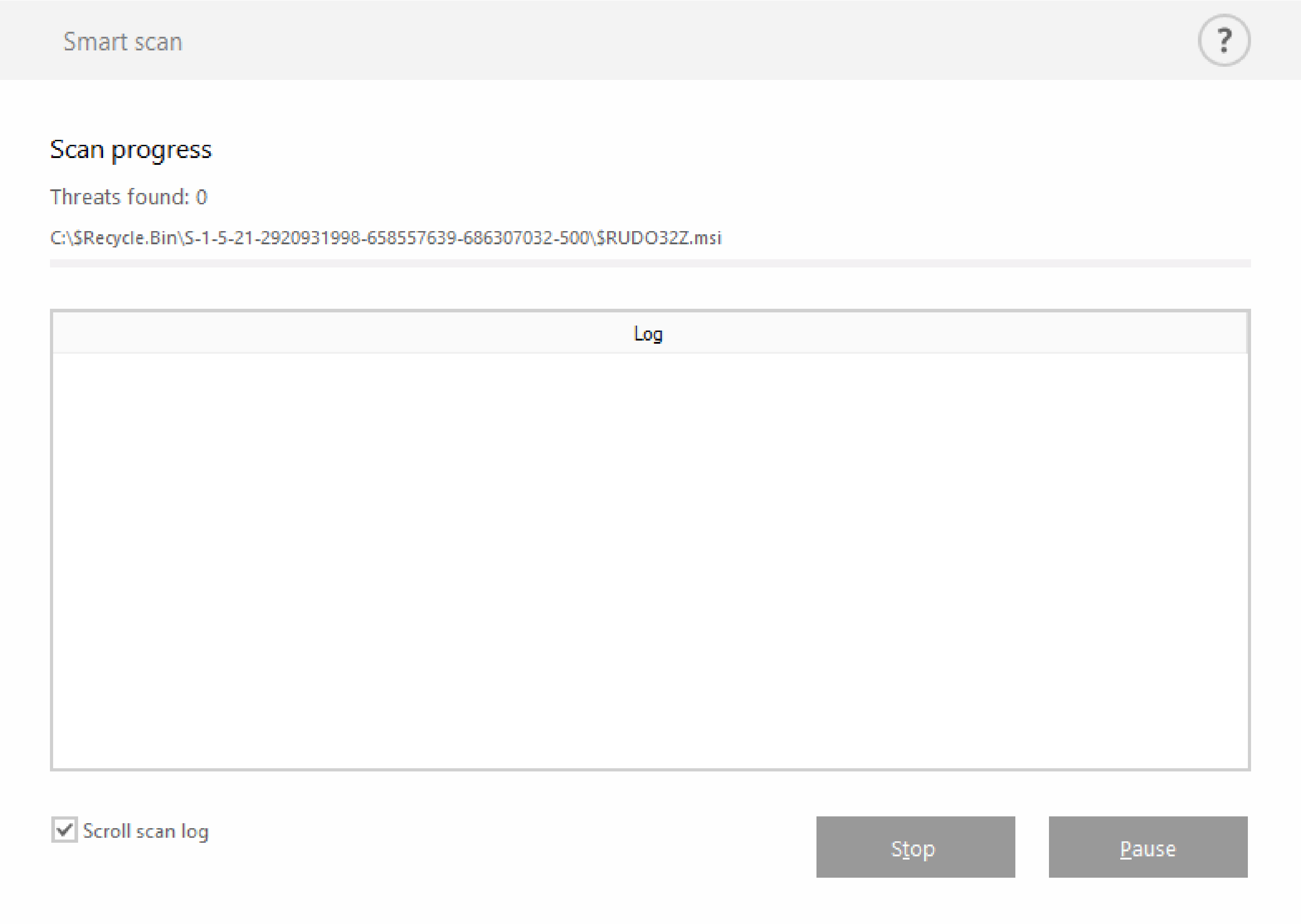
Click **Scan** to execute the scan using the custom parameters that you have set.

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

### 8.2.6.2 Scan progress

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

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



Smart scan

Scan progress

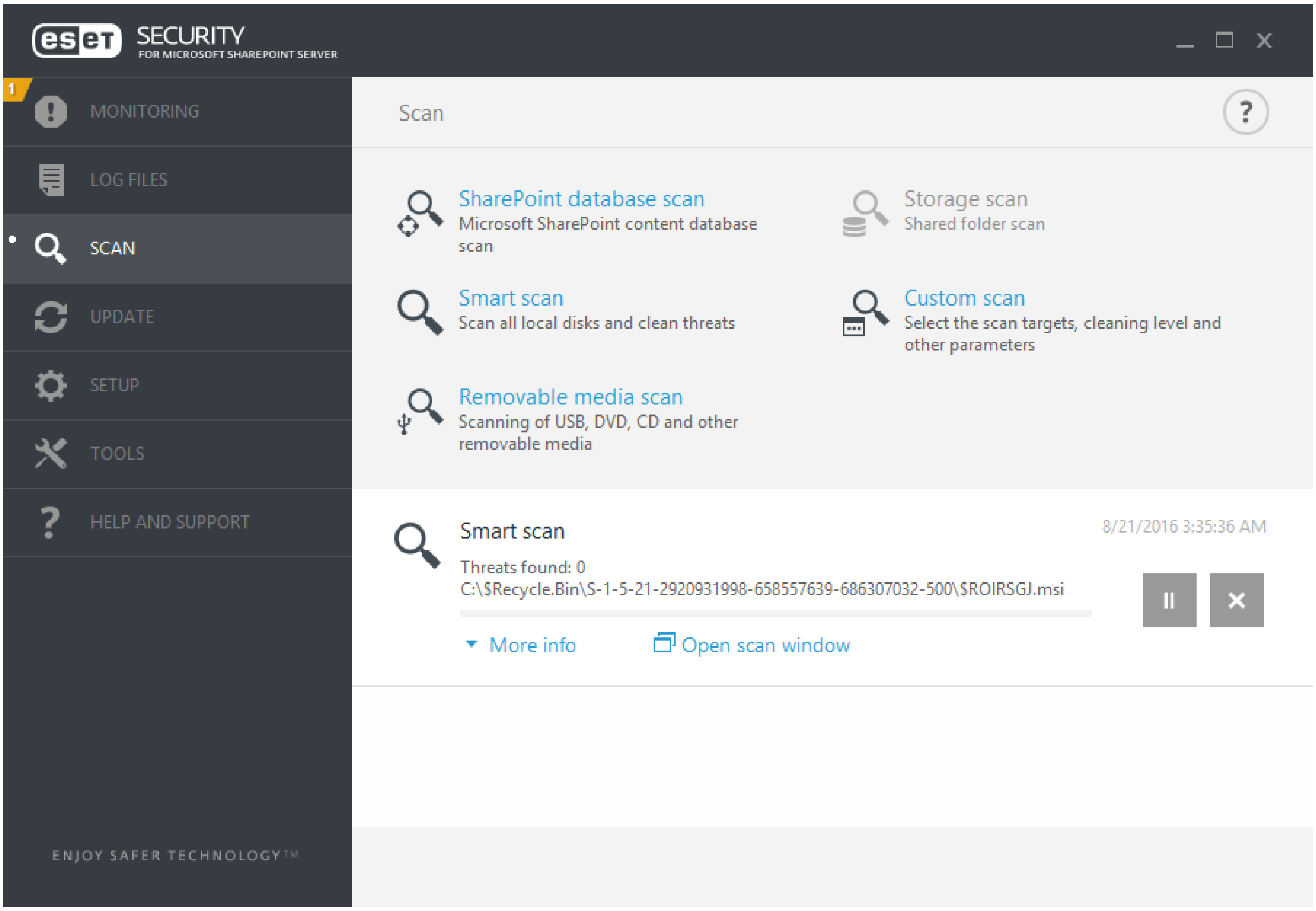
Threats found: 0

C:\$Recycle.Bin\S-1-5-21-2920931998-658557639-686307032-500\$RUDO32Z.msi

Log

☑ Scroll scan log

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



SharePoint database scan
Microsoft SharePoint content database scan

Storage scan
Shared folder scan

Smart scan
Scan all local disks and clean threats

Custom scan
Select the scan targets, cleaning level and other parameters

Removable media scan
Scanning of USB, DVD, CD and other removable media

Smart scan 8/21/2016 3:35:36 AM
Threats found: 0
C:\$Recycle.Bin\S-1-5-21-2920931998-658557639-686307032-500\$ROIRSGJ.msi

You can click **More info** during a scan to see details such as the **User** who executed the scan, number of **Objects scanned** and the scan **Duration**.

### 8.2.6.3 Profile manager

Profile manager is used in two places within ESET Security for Microsoft SharePoint - in the **On-demand computer scan** section and in the **Update** section.

#### On-demand computer scan

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

To create a new profile, open the **Advanced setup** window (**F5**) and click **Computer** > **On-demand computer scan** and then **Edit** next to **List of profiles**. The **Selected profile** drop-down menu that lists existing scan profiles. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

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

#### Update

The profile editor in the **Update setup** section allows users to create new update profiles. It is only necessary to create custom update profiles if your computer uses multiple means to connect to update servers.

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

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

**List of profiles** - Create new or edit update profiles.

### 8.2.6.4 Scan targets

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

- **By profile settings** - Selects targets set in the selected scan profile.
- **Removable media** - Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** - Selects all system hard drives.
- **Network drives** - Selects all mapped network drives.
- **Shared Folders** - Selects all folders on the local server that are shared.
- **No selection** - Cancels all selections.

### 8.2.6.5 Advanced scan option

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

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

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

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

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

See the Scan progress chapter for more information.

### 8.2.6.6 Pause a scheduled scan

The scheduled scan can be postponed. Set a value for the **Stop scheduled scans in (min)** option, if you wish to postpone the computer scan.

### 8.2.7 Idle-state scanning

You can enable the idle-state scanner in **Advanced setup** or press **F5,** navigate to **Computer** > **Idle-state scanning** > **Basic**. Set the switch next to **Enable Idle-state scanning** to enable this feature. When the computer is in idle state, a silent computer scan is performed on all local drives.

By default, the Idle-state scanner will not run when the computer (notebook) is operating on battery power. You can override this setting by selecting the check box next to **Run even if computer is powered from battery**.

Turn on the **Enable logging** switch in **Advanced setup** or press **F5** 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).

**Idle-state detection** will run when your computer is in the following states:

- **Turned off screen or screen saver**
- **Computer lock**
- **User logoff**

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

### 8.2.8 Startup scan

By default, the automatic startup file check will be performed on system startup and during virus signature database updates. 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**, click **Automatic startup file check** and then click **Edit**. In the last step, the Automatic startup file check window will appear (see the following chapter for more details).

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

#### 8.2.8.1 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:

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

### 8.2.9 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.

**Action to take after inserting removable media** - select the default action that will be performed when a removable media device is inserted into the computer (CD/DVD/USB). If **Show scan options** is selected, a notification will display which allows you to choose a desired action:

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

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

- **Scan now** - This will trigger a scan of removable media.
- **Scan later** - Scanning of removable media will be postponed.
- **Setup** - Opens Advanced setup.
- **Always use the selected option** - When selected, the same action will be performed when removable media is inserted another time.

In addition, ESET Security for Microsoft SharePoint features Device control, which allows you to define rules for the use of external devices on a given computer. More details on Device control can be found in the Device control section.

### 8.2.10 Document protection

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

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

- See Threatsense parameters for more information about Document protection settings.

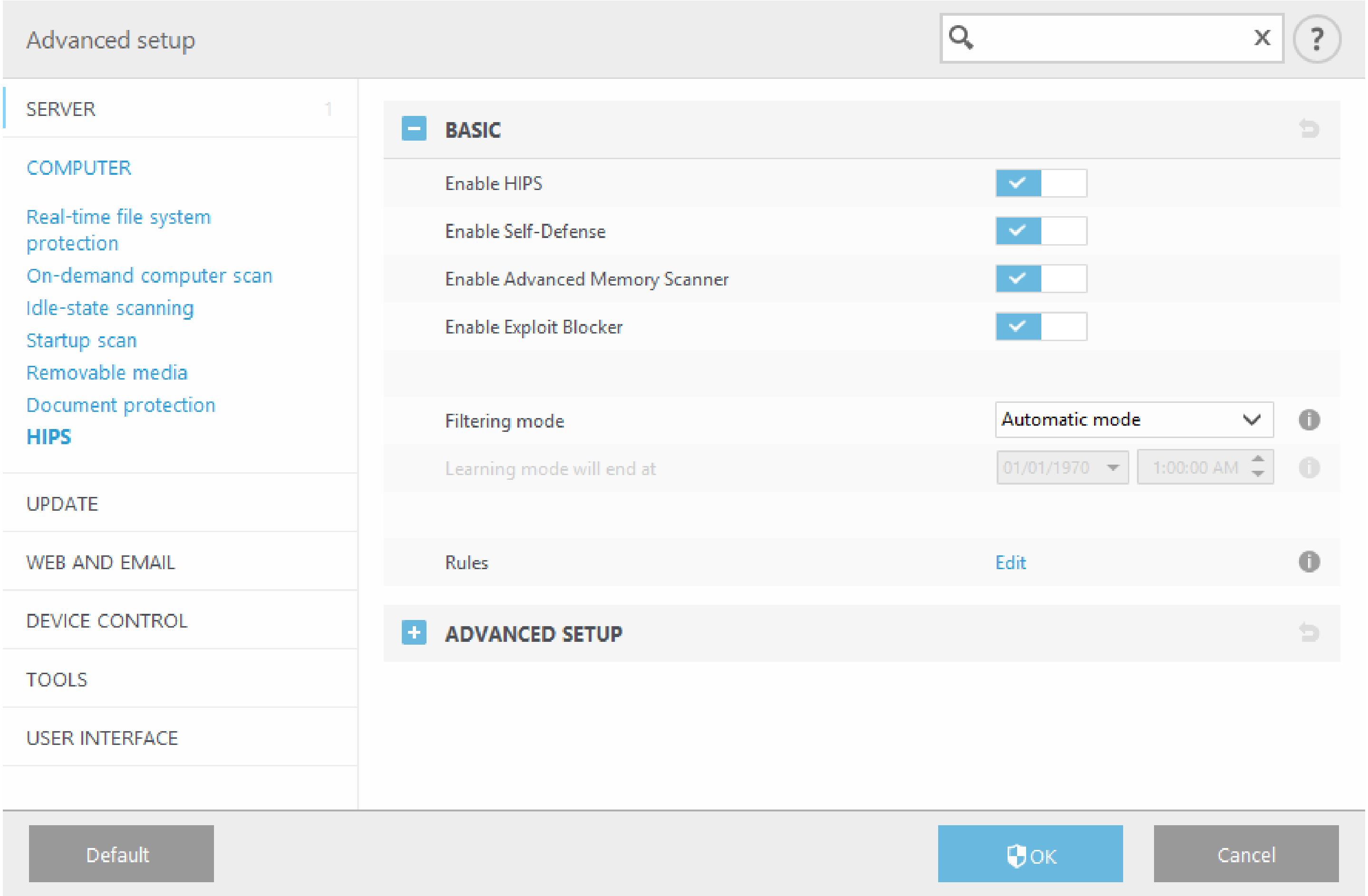
This feature is activated by applications that use the Microsoft Antivirus API (for example, Microsoft Office 2000 and higher, or Microsoft Internet Explorer 5.0 and higher).

### 8.2.11 HIPS

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

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

HIPS settings can be found in **Advanced setup** tree (F5) > **Computer** > **HIPS**. The HIPS state (enabled/disabled) is shown in the ESET Security for Microsoft SharePoint main program window, in the **Setup** tab, on the right side of the **Computer** section.



BASIC

| | |
|---|---|
| Enable HIPS | ✓ |
| Enable Self-Defense | ✓ |
| Enable Advanced Memory Scanner | ✓ |
| Enable Exploit Blocker | ✓ |
| Filtering mode | Automatic mode |
| Learning mode will end at | 01/01/1970 1:00:00 AM |
| Rules | Edit |

ADVANCED SETUP

ESET Security for Microsoft SharePoint has built-in *Self-defense* technology that prevents malicious software from corrupting or disabling your antivirus and antispyware 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.

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

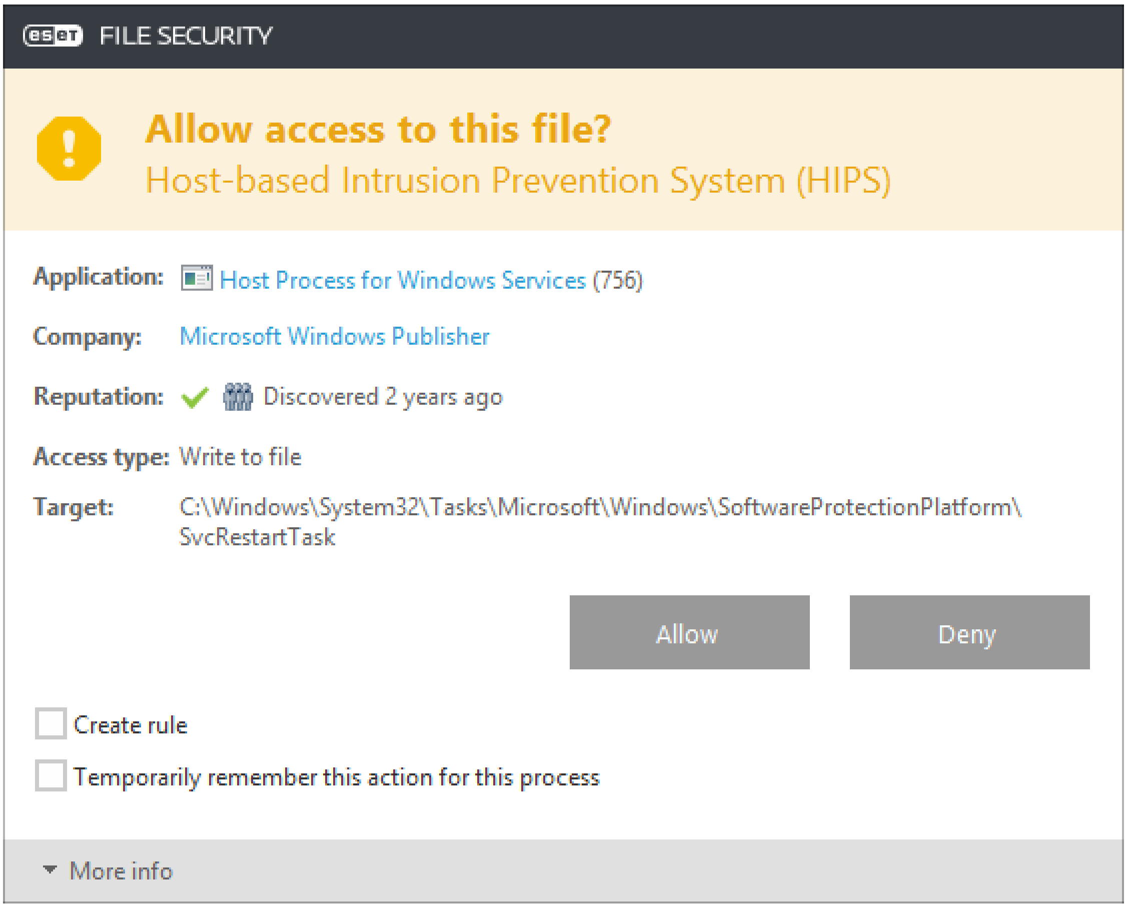
**Exploit Blocker** is designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. Exploit Blocker is enabled by default. Read more about this type of protection in the glossary.

Filtering can be performed in one of four modes:

- **Automatic mode** - Operations are enabled with the exception of those blocked by pre-defined rules that protect your system.
- **Smart mode** - The user will only be notified about very suspicious events.
- **Interactive mode** - The user will be prompted to confirm operations.
- **Policy-based mode** - Operations are blocked.
- **Learning mode** - Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the Rule editor, but their priority is lower than the priority of rules created manually or rules created in automatic mode. When you select **Learning mode** from the HIPS Filtering mode drop down menu, the **Learning mode will end at** setting will become available. Select the 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.

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

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.



Allow access to this file?
Host-based Intrusion Prevention System (HIPS)

Application: Host Process for Windows Services (756)
Company: Microsoft Windows Publisher
Reputation: ✓ Discovered 2 years ago
Access type: Write to file
Target: C:\Windows\System32\Tasks\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask

□ Create rule
□ Temporarily remember this action for this process

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. Settings for the exact parameters can be accessed by clicking **More info**. Rules created like this are considered equal to rules created manually, so a rule created from a dialog window can be less specific than the rule that triggered that dialog window. This means that after creating such a rule, the same operation can trigger the same window.

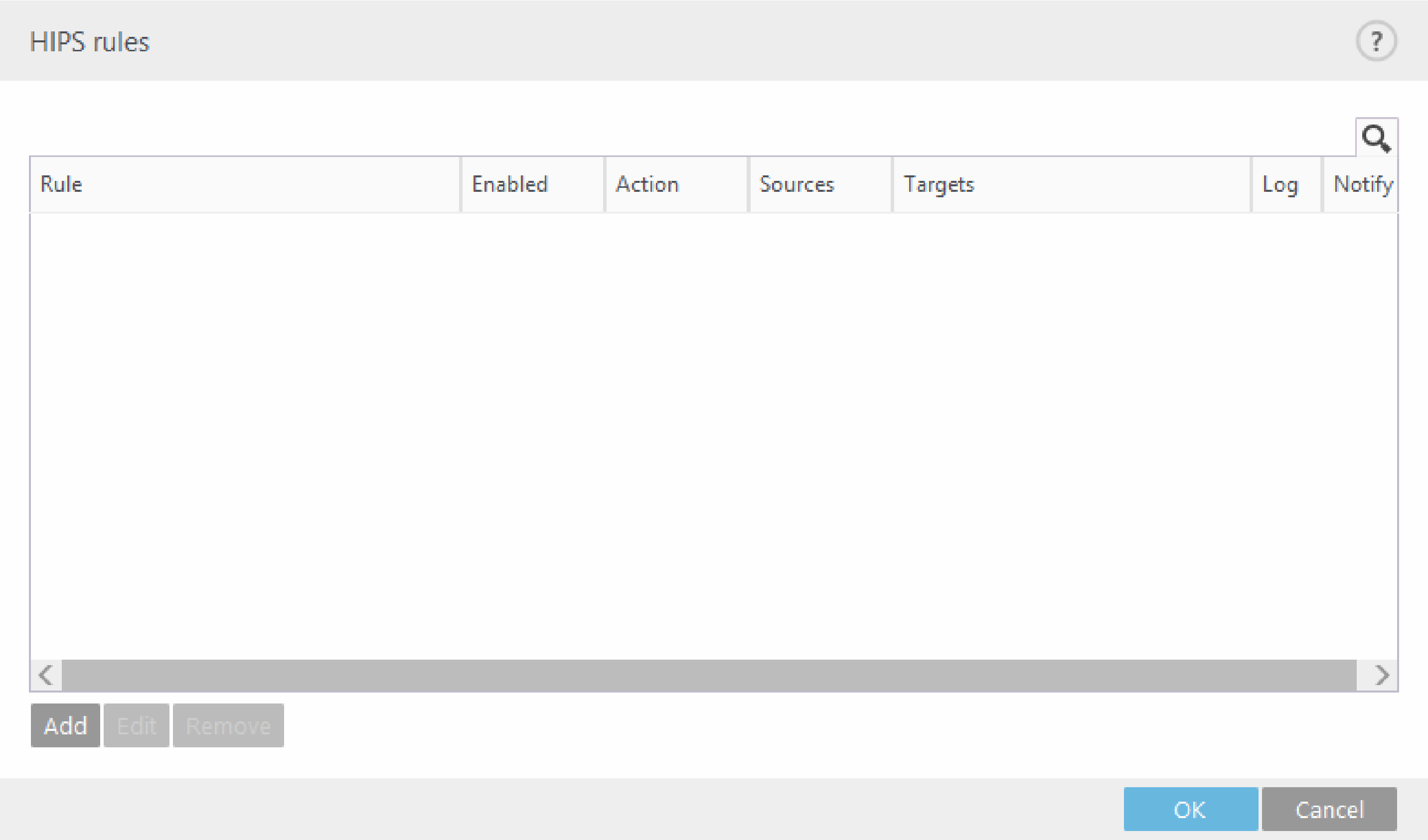
**Temporarily remember this action for this process** causes the action (**Allow/Block**) to be used until a change of rules or filtering mode, a HIPS module update or a system restart. After any of these three actions, temporary rules will be deleted.

### 8.2.11.1 HIPS rules

This window gives you an overview of existing HIPS rules.

**Columns**

**Rule** - User-defined or automatically chosen rule name.
**Enabled** - Deactivate this switch if you want to keep the rule in the list but do not want to use it.
**Action** - The rule specifies an action - **Allow**, **Block** or **Ask** - that should be performed if the conditions are right.
**Sources** - The rule will be used only if the event is triggered by an application(s).
**Targets** - The rule will be used only if the operation is related to a specific file, application or registry entry.
**Log** - If you activate this option, information about this rule will be written to the HIPS log.
**Notify** - A small pop-up window appears in the lower-right corner if an event is triggered.



**Control elements**

**Add** - Creates a new rule.
**Edit** - Enables you to edit selected entries.
**Remove** - Removes selected entries.

EXAMPLE

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

1. Name the rule and select **Block** from the **Action** drop-down menu.
2. Enable the **Notify user** switch to display a notification any time that a rule is applied.
3. Select at least one operation for which the rule will be applied. In the **Source applications** window, select **All applications** from the drop-down menu to apply your new rule to all applications attempting to perform any of the selected application operations on the applications you specified.
4. Select **Modify state of another application** (all operations are described in product help, which can be accessed by pressing F1).
5. Select **Specific applications** from the drop-down menu and **Add** one or several applications you want to protect.
6. Click **Finish** to save your new rule.

### 8.2.11.1.1 HIPS rule settings

- **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.

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

drop-down menu and click **Add** to add new files or folders or you can select All entries from the drop-down menu to add all applications.

- **Enabled** - Deactivate this switch if you want to keep the rule in the list but do not want to use it.
- **Log** - If you activate this option, information about this rule will be written to the HIPS log.
- **Notify user** - A small pop-up window appears in the lower-right corner if an event is triggered.

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

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

**Files** - 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 drop-down menu to add all applications.

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

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

Descriptions of important operations:

### File operations

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

### Application operations

- **Debug another application** - Attaching a debugger to the process. While debugging an application, many details of its behavior can be viewed and modified and its data can be accessed.
- **Intercept events from another application** - The source application is attempting to catch events targeted at a specific application (for example a keylogger trying to capture browser events).
- **Terminate/suspend another application** - Suspending, resuming or terminating a process (can be accessed directly from Process Explorer or the Processes 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.

### Registry operations

- **Modify startup settings** - Any changes in settings that define which applications will be run at Windows startup. These can be found, for example, by searching for the Run key in the Windows Registry.
- **Delete from registry** - Deleting a registry key or its value.
- **Rename registry key** - Renaming registry keys.

- **Modify registry** - Creating new values of registry keys, changing existing values, moving data in the database tree or setting user or group rights for registry keys.

NOTE

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

WARNING

You may receive a notification if you create an overly generic rule.

### 8.2.11.2 Advanced setup

The following options are useful for debugging and analyzing an application's behavior:

- Drivers always allowed to load - selected drivers are always allowed to load regardless of configured filtering mode, unless explicitly blocked by user rule.
- **Log all blocked operations** - all blocked operations will be written to the HIPS log.
- **Notify when changes occur in Startup applications** - displays a desktop notification each time an application is added to or removed from system startup.

### 8.2.11.2.1 Drivers always allowed to load

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

**Add** - adds a new driver.
**Edit** - edit the path for a selected driver.
**Remove** - removes a driver from the list.
**Reset** - reloads a set of system drivers.

NOTE

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

## 8.3 Update

Update setup options are available in the **Advanced setup** window (press the **F5** key on your keyboard) under **Update** > **General**. This section specifies update source information like the update servers being used and authentication data for these servers.

NOTE

For updates to be downloaded properly, it is essential that you fill in all update parameters correctly. If you use a firewall, please make sure that your ESET program is allowed to communicate with the Internet (for example, HTTP communication).

**General**

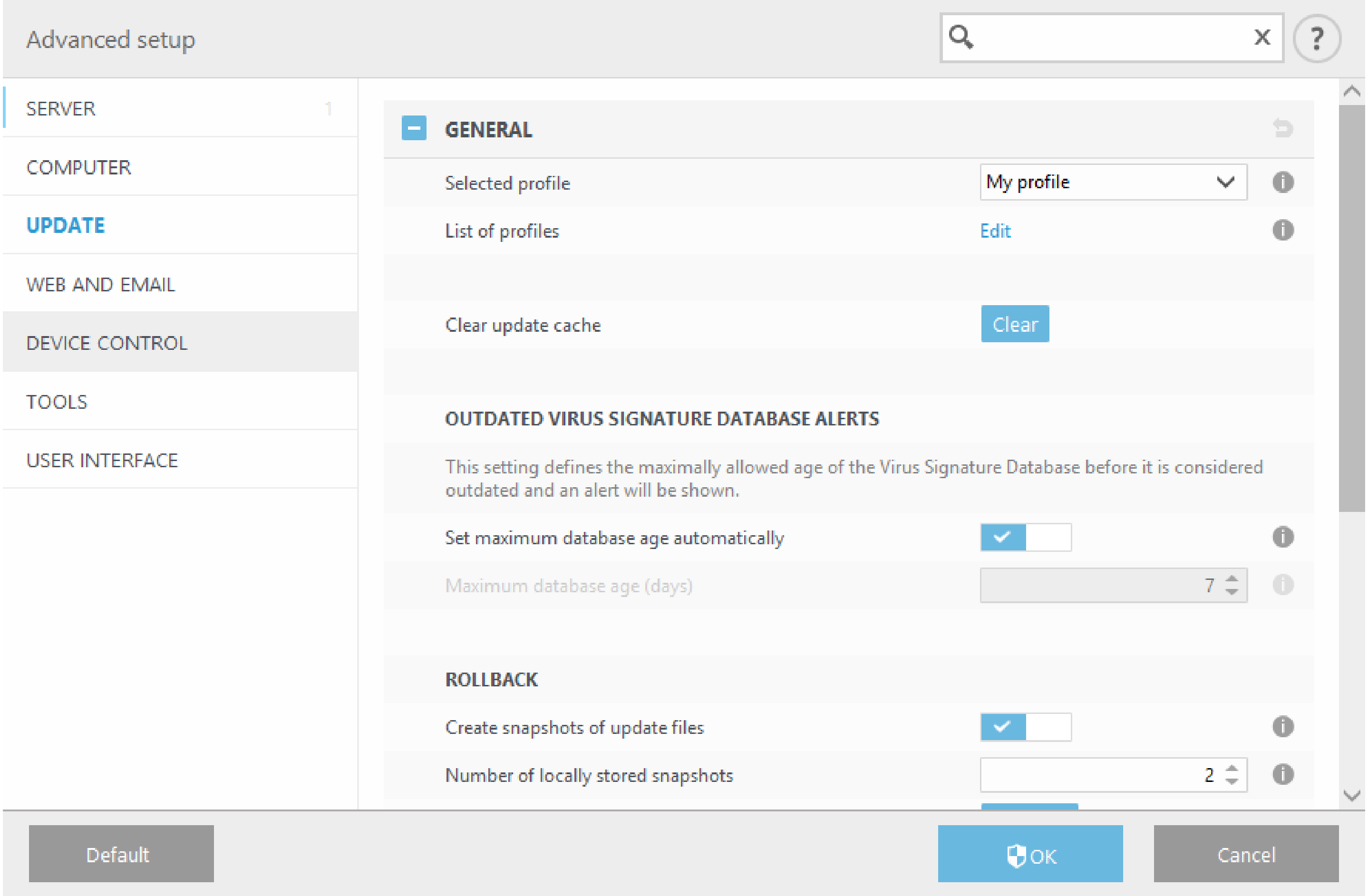
- The **Update profile** that is currently in use is displayed in the selected profile drop-down menu. If you experience problems with an update, click **Clear** to clear the temporary update cache.

**Outdated virus signature database alerts**

- **Set maximum database age automatically / Maximum database age (days)** - allows you to set maximum time (in days) after which the virus signature database will be reported as out of date. The default value is 7.

**Rollback**

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



Selected profile: My profile

List of profiles

Clear update cache

OUTDATED VIRUS SIGNATURE DATABASE ALERTS

This setting defines the maximally allowed age of the Virus Signature Database before it is considered outdated and an alert will be shown.

Set maximum database age automatically ✓

Maximum database age (days) 7

ROLLBACK

Create snapshots of update files ✓

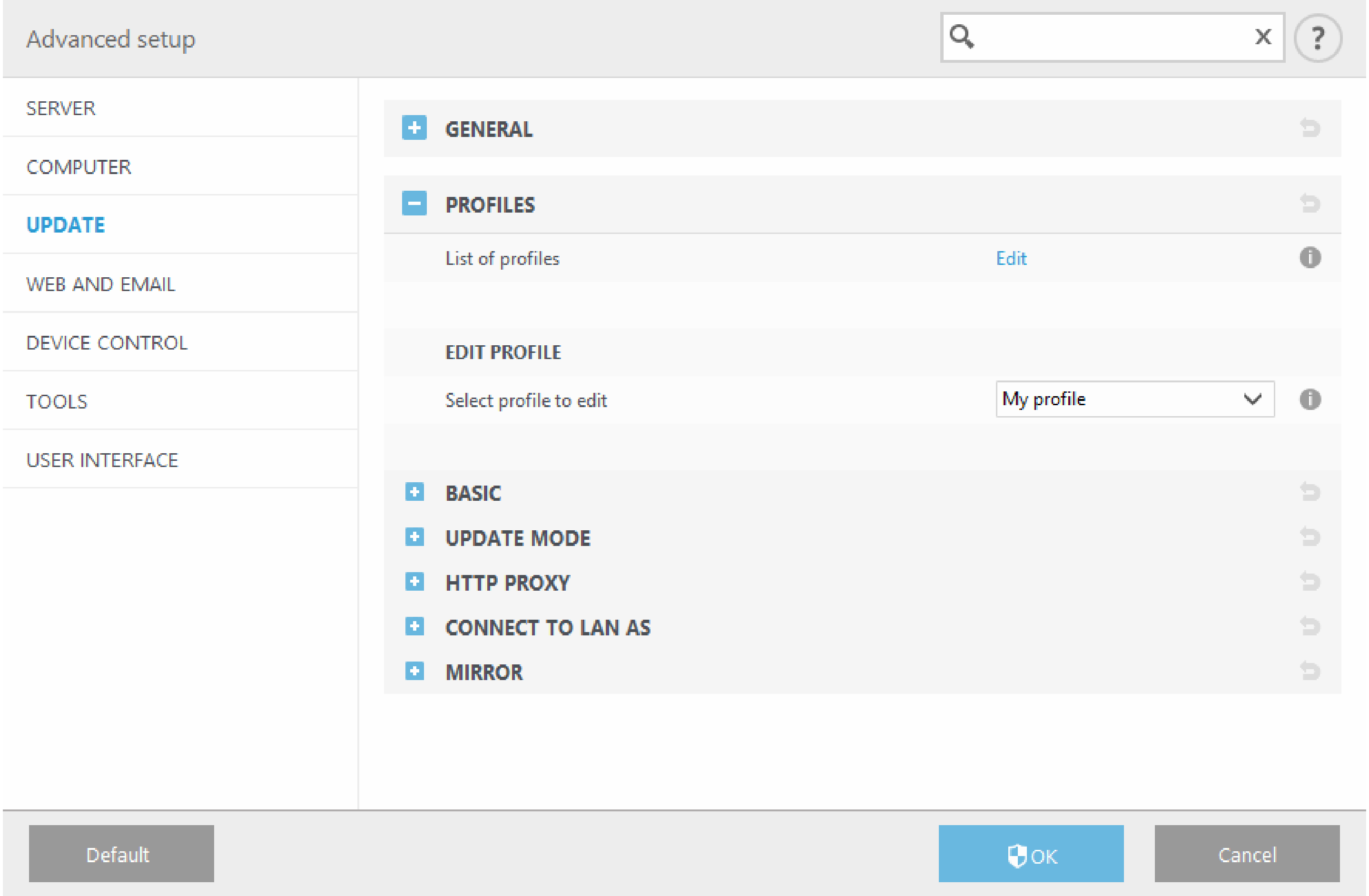
Number of locally stored snapshots 2

**EXAMPLE**

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

### Profiles

To create a new profile, select **Edit** next to **List of profiles**, enter your own **Profile name** and then click **Add**. You can **Edit profile** with the following options:



⊟ Basic

**Update type** - 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 (i.e. databases tested in a real environment and therefore considered as stable).

**Disable notification about successful update** - turns off the system tray notification at the bottom right corner of the screen. It is useful to select this option if a full screen application or a game is running. Please note that Presentation mode will turn off all notifications.

**Update from removable media** - allows you to update from removable media if contains created mirror. When **Automatic** selected, updates will run in the background. If you want to show update dialogs select **Always ask**.

- The **Update server** menu is 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*

- **Updating from a Mirror**

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

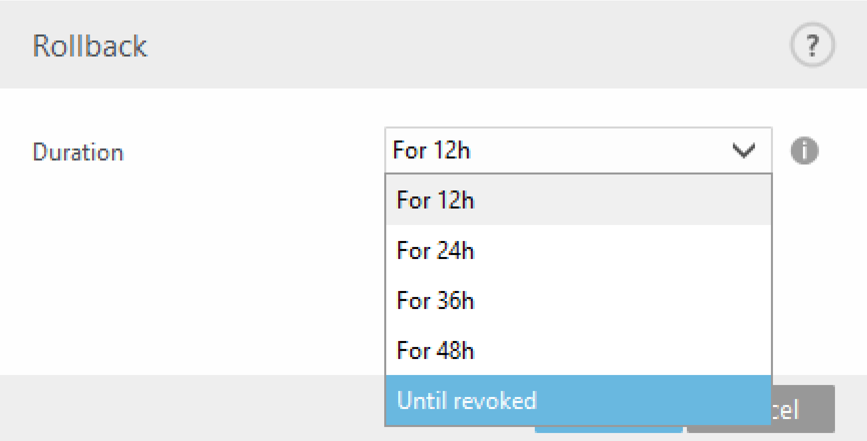
- Update mode
- HTTP Proxy
- Connect to LAN as
- Mirror

### 8.3.1 Update rollback

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

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

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



Rollback

Duration: For 12h

### 8.3.2 Update mode

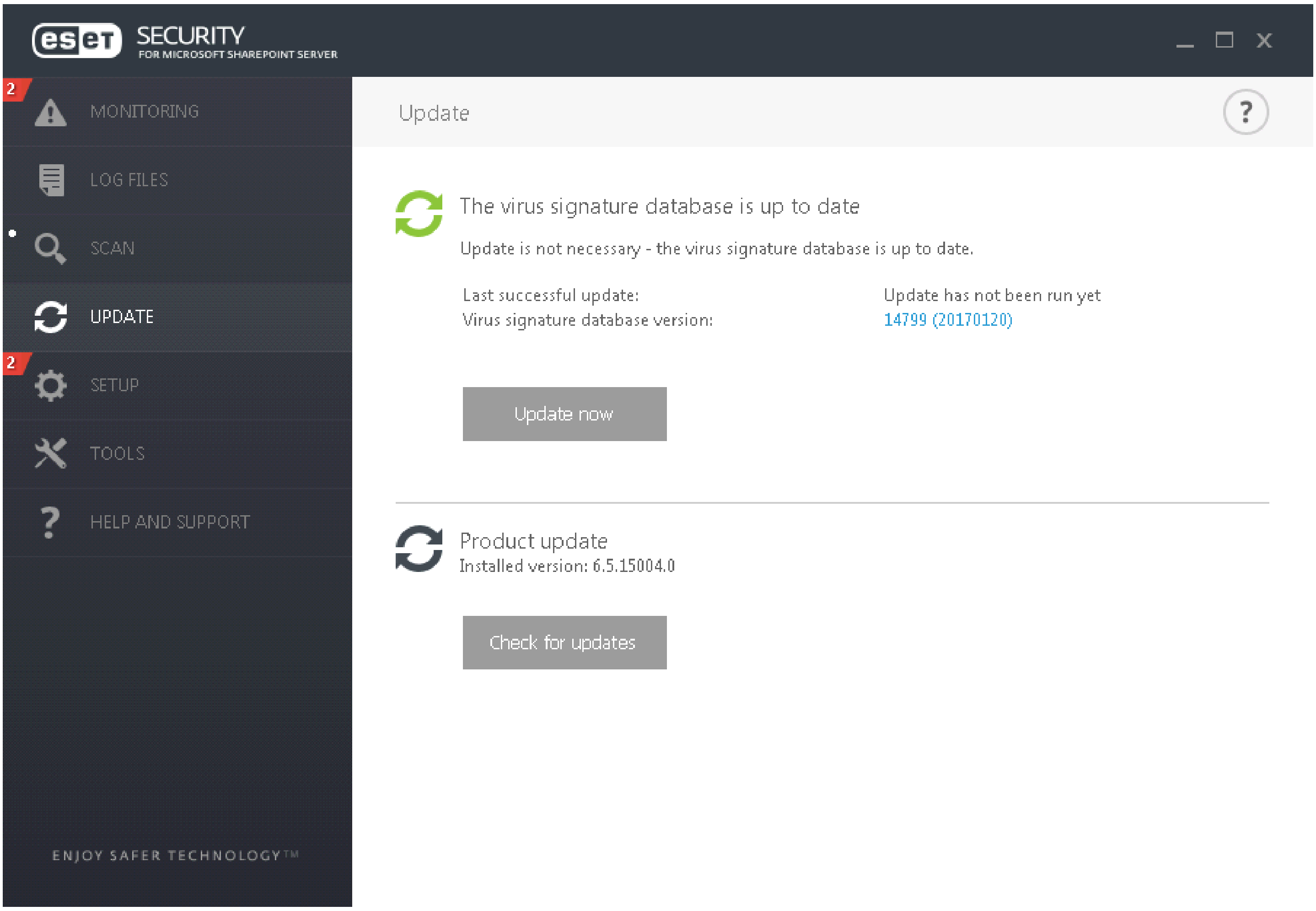
The **Update mode** tab contains options related to the program component update. The program enables you to predefine its behavior when a new program component upgrade is available.

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

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

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

If you want to upgrade to a newer version of ESET Security for Microsoft SharePoint **Enable manual program component update**. This is disabled  by default, when enabled and a newer version of ESET Security for Microsoft SharePoint is available, **Check for updates** appears in **Update** tab.



The virus signature database is up to date

Update is not necessary - the virus signature database is up to date.

Last successful update: Update has not been run yet
Virus signature database version: 14799 (20170120)

Product update
Installed version: 6.5.15004.0

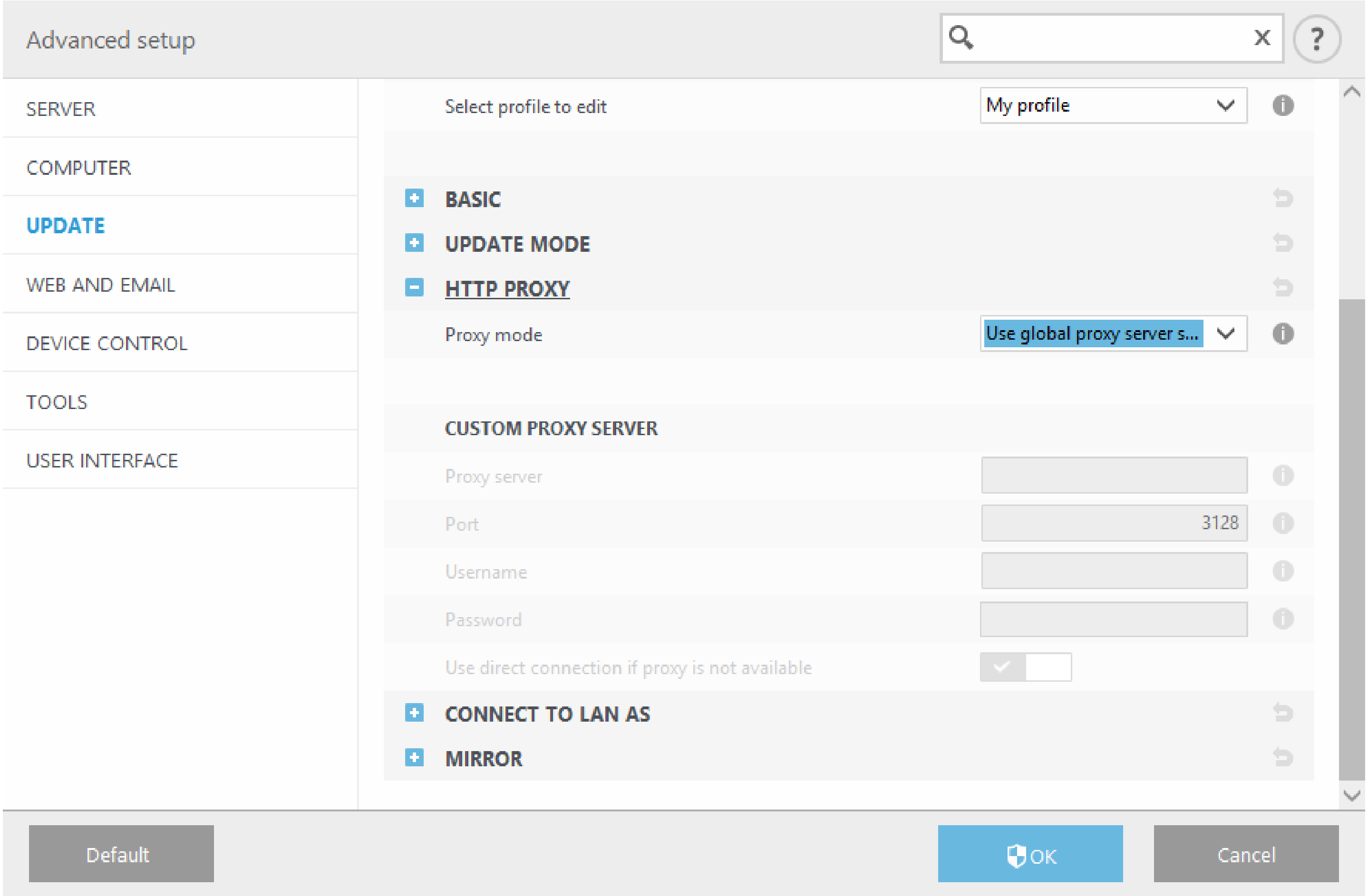
If the **Ask before downloading update** option is active, a notification will display when a new update is available.

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

### 8.3.3 HTTP Proxy

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

- **Do not use proxy server** - selecting the Use global proxy server settings option will use the proxy server configuration options already specified in the **Tools** > **Proxy server** branch of the Advanced setup tree.



Select profile to edit: My profile

Proxy mode: Use global proxy server s...

CUSTOM PROXY SERVER

Port: 3128

- **Connection through a proxy server** - select **Do not use proxy server** to specify that no proxy server will be used to update ESET Security for Microsoft SharePoint.

- **Use global proxy server settings** - the **Connection through a proxy server** option should be selected 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), please check that the HTTP proxy settings listed in this window are correct. Otherwise the program will not be able to connect to the update servers.

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

**NOTE**

Authentication data such as **Username** and **Password** is intended for accessing the proxy server. Complete these fields only if a username and password are required. Please note that these fields are not for your Username/Password for ESET 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.

### 8.3.4 Connect to LAN as

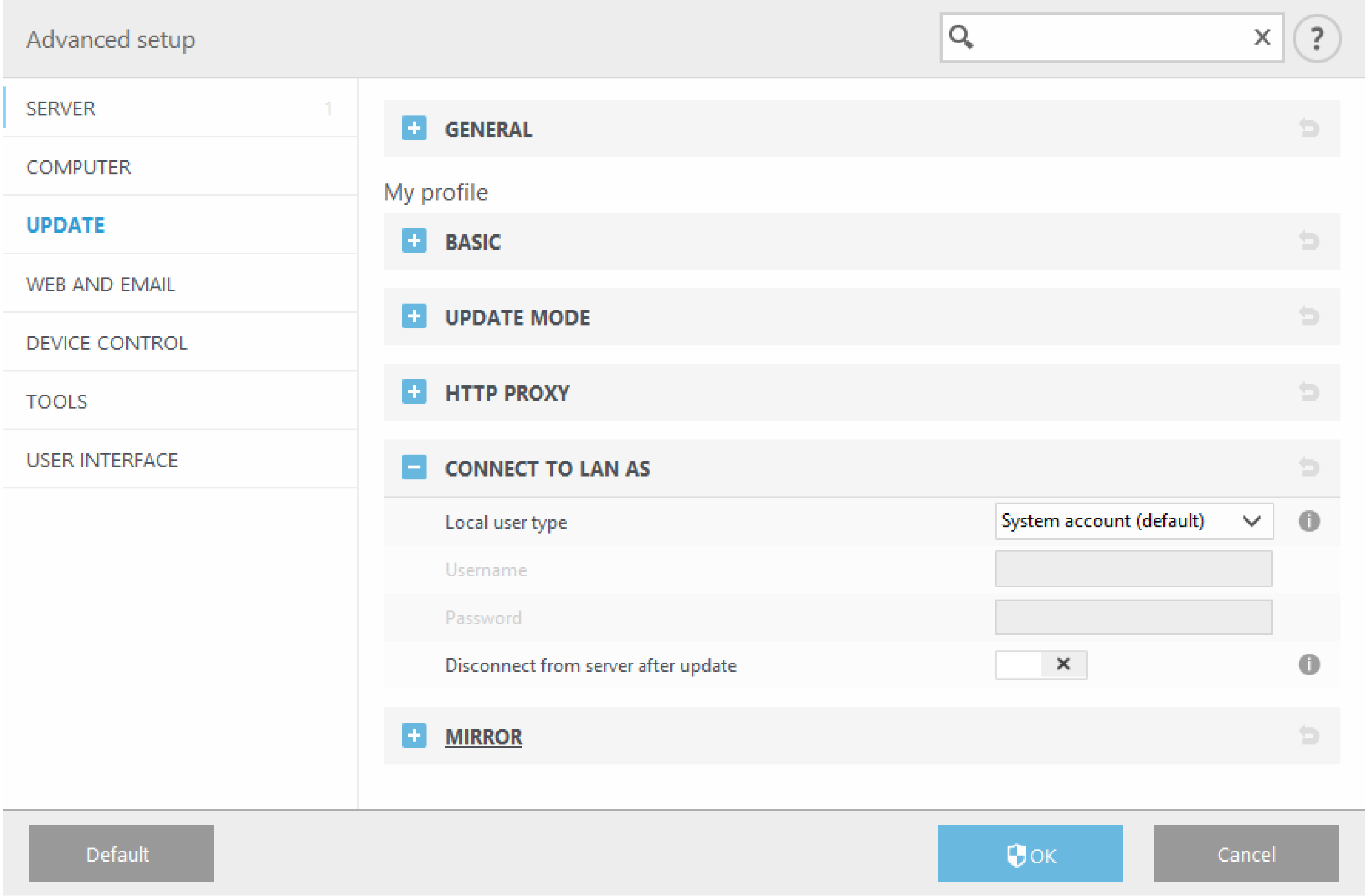
When updating from a local server running Windows, authentication for each network connection is required by default. Configuration options are located in the **Advanced setup** tree (F5) under **Update** > **Profiles** > **Connect to LAN as**. To configure your account, select one of the following options from the **Local user type** drop-down menu:

- **System account (default) -** use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.
- **Current user** - select this to ensure that the program authenticates using the currently logged-in user account. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.
- **Specified user** - select this to use a specific user account for authentication. Use this method when the default system account connection fails. Please be aware that the specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

WARNING

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

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


Advanced setup

Local user type: System account (default)
Username
Password
Disconnect from server after update: ☒

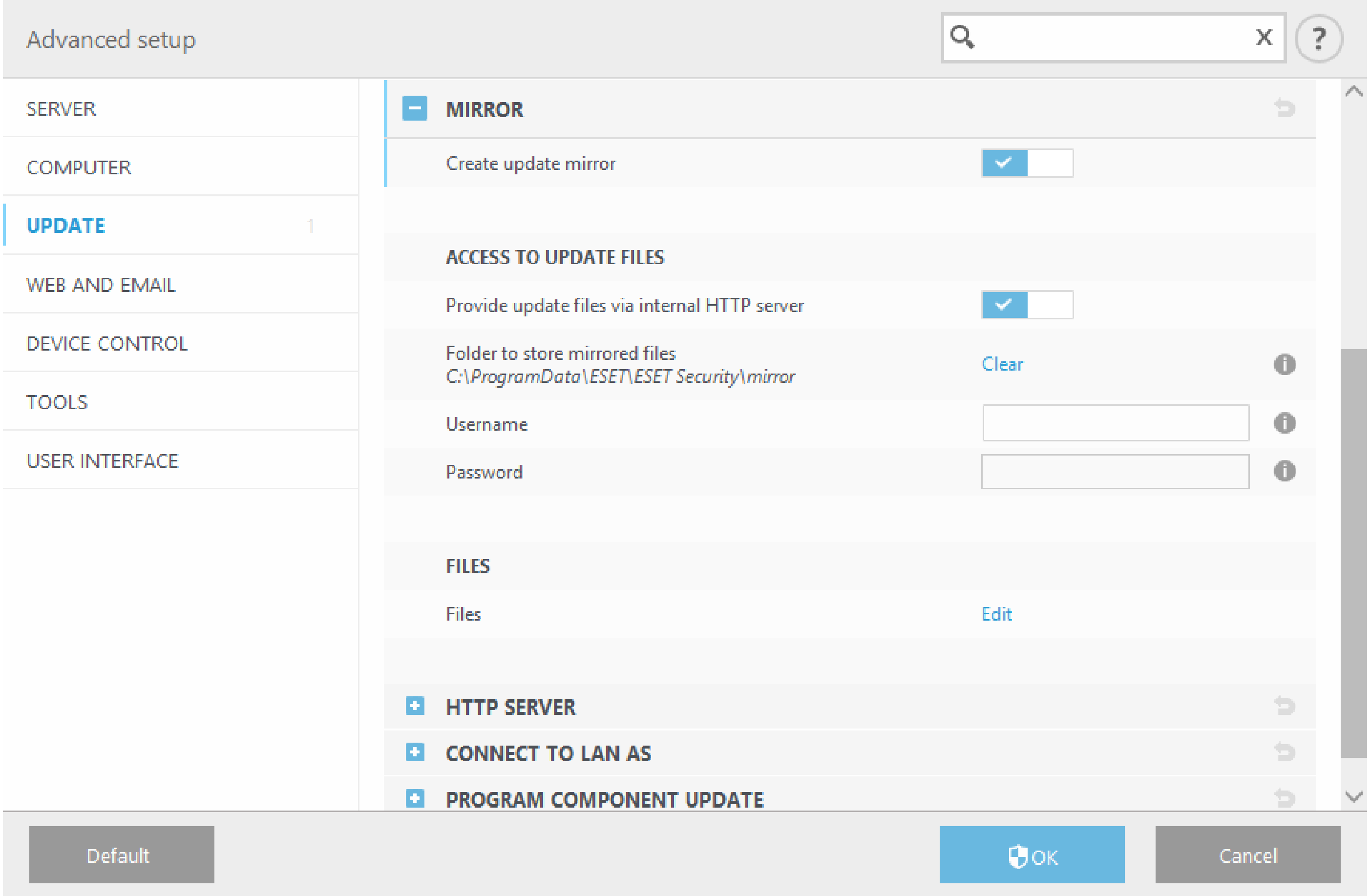
### 8.3.5 Mirror

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.

Configuration options for the local Mirror server are located in the **Advanced setup** tree (F5) in the **Update** > **Profiles** > **Mirror** tab.

Create update mirror

**Create update mirror** - Enabling this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.



Create update mirror ☑

Provide update files via internal HTTP server ☑

Folder to store mirrored files
C:\ProgramData\ESET\ESET Security\mirror

Username

Password

Files

#### Access to update files

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

> **NOTE**
> Windows XP requires Service Pack 2 or later to use the HTTP server.

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

- **Folder to store mirrored files** - click **Clear** if you want to change a defined default folder to store mirrored files *C:\ProgramData\ESET\ESET File Security\mirror.* Click **Edit** to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be entered in the **Username** and **Password** fields. If the selected destination folder is located on a network disk running the Windows NT/2000/XP operating system, the username and password specified must have write privileges for the selected folder. The username and password should be entered in the format *Domain/User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

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

HTTP server

- **Server port** - by default, the Server port is set to 2221.
- **Authentication** - defines the method of authentication used for accessing update files. The following options are available: **None**, **Basic** and **NTLM**.

Select **Basic** to use base64 encoding with basic username and password authentication.
The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **NONE**, which grants access to the update files with no need for authentication.

**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.

Connect to LAN as

- **Local user type** - the **System account (default)**, **Current user**, and **Specified user** settings will be displayed in their corresponding drop-down menus. **Username** and **Password** settings are optional. See Connect to LAN as.
- Select **Disconnect from server after update** to force a disconnection if a connection to the server remains active after updates have been downloaded.

Program component update

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

### 8.3.5.1 Updating from the Mirror

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

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

This configuration is the default, specified in the predefined program configuration. To allow access to the Mirror using the HTTP server, navigate to **Advanced setup** (F5) > **Update** > **Profiles** > **Mirror** and select **Create update mirror**.

In the **HTTP Server** section of the **Mirror** tab you can specify the **Server port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to **2221**. The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **None**, **Basic**, and **NTLM**.

- Select **Basic** to use base64 encoding with basic username and password authentication.
- The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the

workstation sharing the update files is used.
- The default setting is **None**, which grants access to the update files with no need for authentication.

WARNING

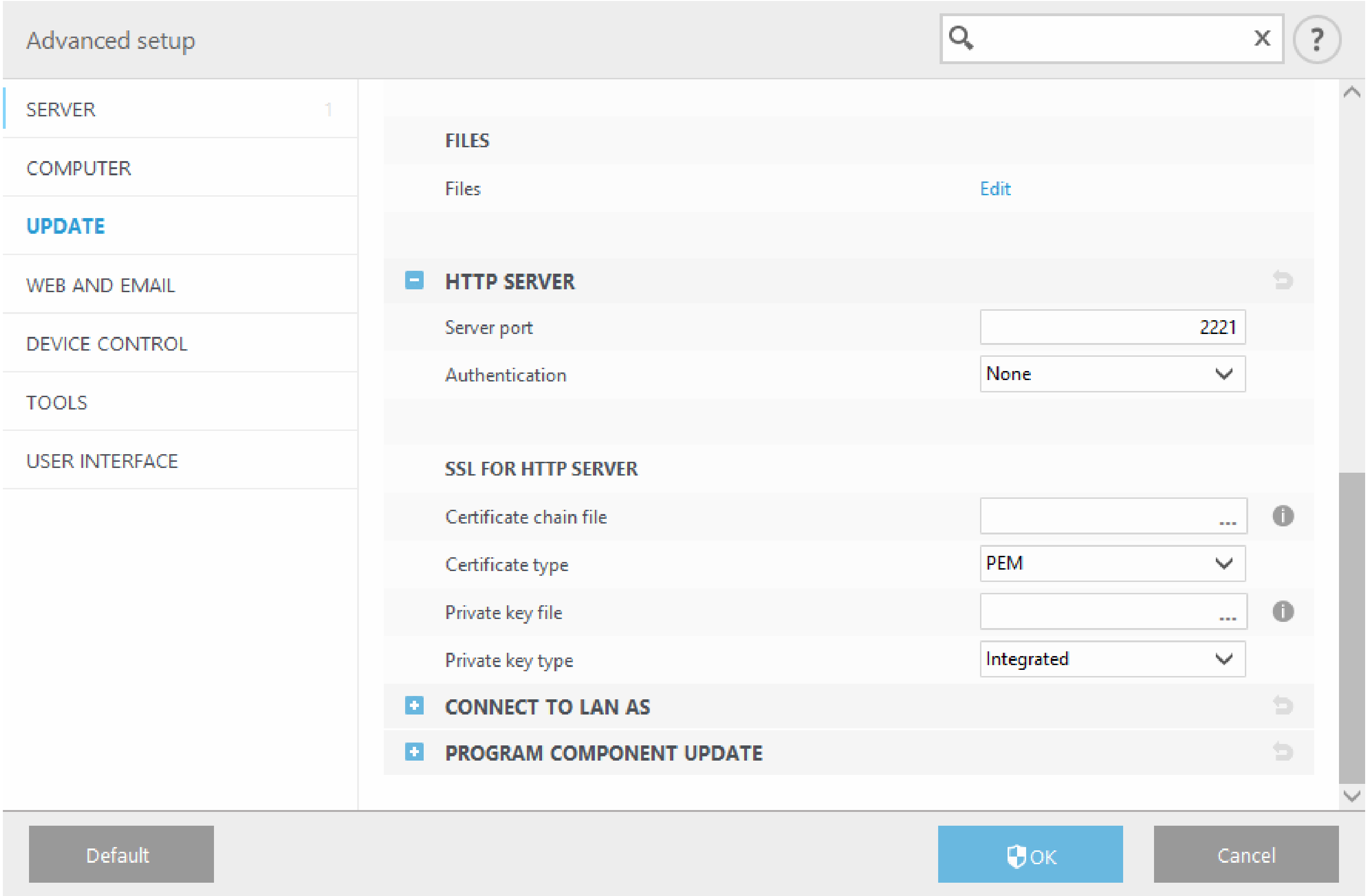
If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Security for Microsoft SharePoint instance creating it.

### 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. **Private key type** is set to **Integrated** by default, which means that the private key is a part of the selected certificate chain file.

NOTE

An error **Invalid Username and/or Password** will appear in the Update tab from the main menu after several unsuccessful attempts to update the virus signature database from the Mirror. We recommend that you navigate to **Advanced setup** (F5) > **Update** > **Profiles** > **Mirror** and check the Username and Password. The most common reason for this error is incorrectly entered authentication data.



Files: Edit

Server port: 2221

Authentication: None

Certificate chain file: ...

Certificate type: PEM

Private key file: ...

Private key type: Integrated

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

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

**Accessing the Mirror via system shares**

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

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

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

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

1. Open ESET Security for Microsoft SharePoint **Advanced setup** (F5) and click **Update** > **Profiles** > **Basic**.
2. Click **Update server** and add a new server using the *\\UNC\PATH* format.

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

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

### 8.3.5.2 Mirror files

List of available and localized program component files.

### 8.3.5.3 Troubleshooting Mirror update problems

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

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

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

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

## 8.4 Web and email

The **Web and email** section allows you to configure Email client protection, protect your Internet communication using the Web access protection and control Internet protocols by configuring Protocol filtering. These features are vital for protecting your computer when communicating through the Internet.

**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.

> ℹ NOTE
> On Windows Server 2008, Windows Server 2008 R2, Small Business Server 2008 and Small Business Server 2011, installation of the **Web and email** component is disabled by default. If you want this feature to be installed, choose the **Custom** installation type. If you have ESET Security for Microsoft SharePoint already installed, you can run the installer again to modify your existing installation adding Web and email component.

### 8.4.1 Protocol filtering

Antivirus protection for application protocols is provided by the ThreatSense scanning engine, which integrates multiple advanced malware scanning techniques. Protocol filtering works automatically, regardless of the Internet browser or email client used. If protocol filtering is enabled, ESET 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** - can be used to disable protocol filtering. Note that many ESET Security for Microsoft SharePoint components (Web access protection, Email protocols protection and Anti-Phishing) depend on this and will not function without it.
- Excluded applications - allows you to exclude specific applications from protocol filtering. Click **Edit** to select them from the list of applications.
- Excluded IP addresses - allows you to exclude specific remote addresses from protocol filtering.

> ℹ NOTE
> Exclusions are useful when protocol filtering causes compatibility issues.

#### 8.4.1.1 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.

> ! IMPORTANT
> We recommend only using this option for applications that do not work properly with their communication being checked.

The following functions are available:

- **Add -** display applications and services that were already affected by protocol filtering.
- **Edit** - selected application from the list.
- **Remove** - selected application from the list.

### 8.4.1.2 Excluded IP addresses

IP addresses in this list will be excluded from protocol content filtering. HTTP/POP3/IMAP communication from/to the selected addresses will not be checked for threats.

> **IMPORTANT**
> We recommend that you only use this option for addresses that are known to be trustworthy.

The following functions are available:

- **Add** - add an IP address /address range/ subnet of a remote point to which a rule is 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 excluded IP addresses.

- **Edit** - edit the selected IP address.
- **Remove** - remove the selected IP address from the list.

### 8.4.1.3 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 an Internet browser. Applications that already use protocols for communication or applications from selected paths can be added to the list of Web and email clients.

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

### 8.4.2 SSL/TLS

ESET Security for Microsoft SharePoint is capable of checking for threats in communications that use the SSL/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.

**SSL/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.

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

**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.

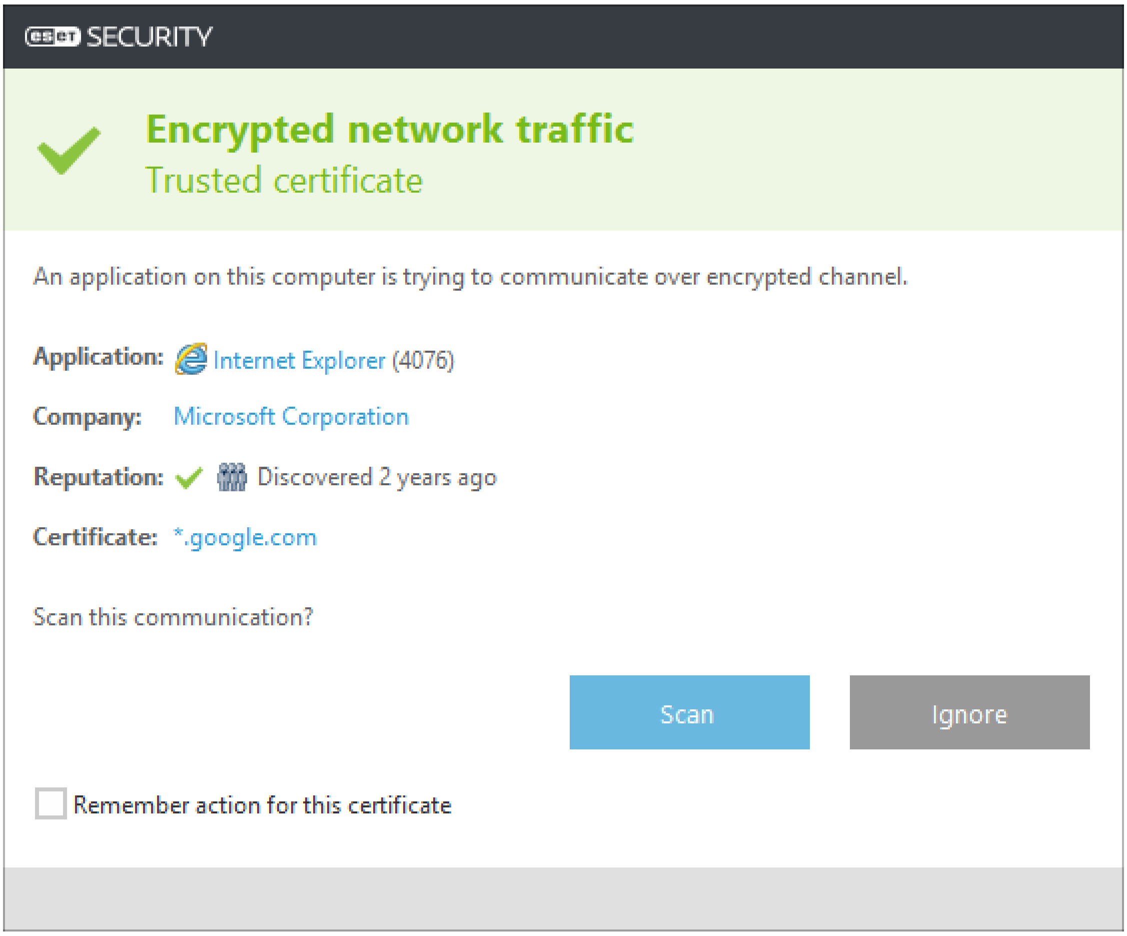
**If the certificate is invalid or corrupt** - this means that the certificate expired or was incorrectly signed. In this case, we recommend that you leave **Block communication that uses the certificate** selected.

### 8.4.2.1 Encrypted SSL communication

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

First, if a website uses an unverifiable or invalid certificate, and ESET 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.



Encrypted network traffic
Trusted certificate

An application on this computer is trying to communicate over encrypted channel.

Application: Internet Explorer (4076)

Company: Microsoft Corporation

Reputation: ✓ Discovered 2 years ago

Certificate: *.google.com

Scan this communication?

□ Remember action for this certificate

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

### 8.4.2.2 List of known certificates

The **List of known certificates** can be used to customize ESET Security for Microsoft SharePoint behavior for specific SSL/TLS certificates, and to remember actions chosen if **Interactive mode** is selected in **SSL/TLS protocol filtering mode**. The list can be viewed and manged by clicking **Edit** next to **List of known certificates**.

You can choose from the following actions:

- **Add** - add a certificate from a URL or File.
- **Edit** - select the certificate that you want to configure and click **Edit**.
- **Remove** - select the certificate that you want to delete and click **Remove**.

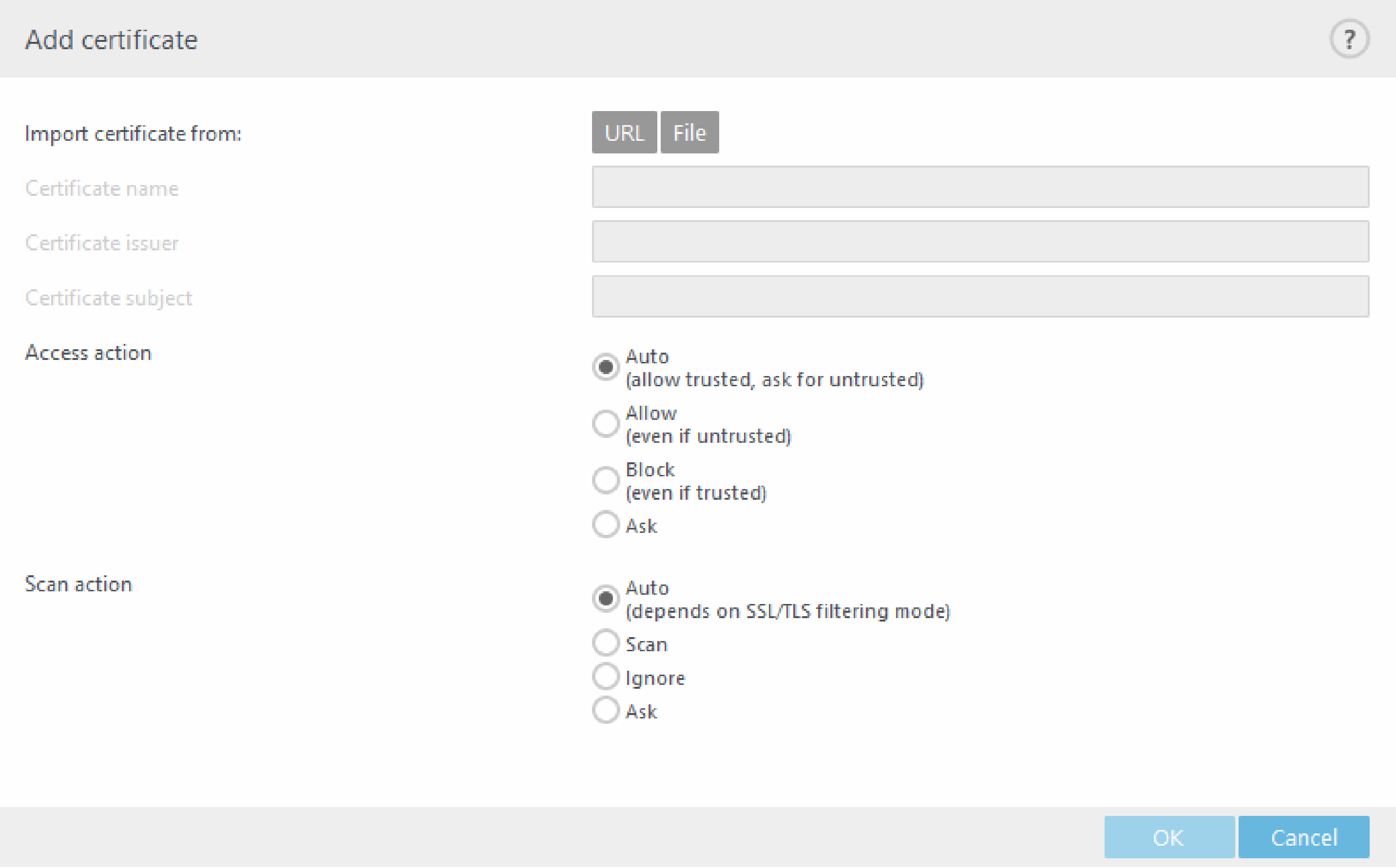
Once you are in **Add certificate** window, click **URL** or **File** and specify the certificate URL or browse for a certificate file. The following fields will automatically be filled using data from the certificate:

- **Certificate name** - name of the certificate.
- **Certificate issuer** - name of the certificate creator.

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

Options you can configure:

- Select **Allow** or **Block** as the **Access action** to allow/block communication secured by this certificate regardless of its trustworthiness. Select **Auto** to allow trusted certificates and ask for untrusted ones. Select **Ask** to receive a prompt when a specific certificate is encountered.
- Select **Scan** or **Ignore** as the **Scan action** to scan or ignore communication secured by this certificate. Select **Auto** to scan in automatic mode and ask in interactive mode. Select **Ask** receive a prompt when a specific certificate is encountered.


Add certificate

Import certificate from: URL File

Certificate name

Certificate issuer

Certificate subject

Access action
● Auto (allow trusted, ask for untrusted)
○ Allow (even if untrusted)
○ Block (even if trusted)
○ Ask

Scan action
● Auto (depends on SSL/TLS filtering mode)
○ Scan
○ Ignore
○ Ask

Click **OK** to save your changes or click **Cancel** to exit without saving.

### 8.4.3 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 (toolbar for newer versions of Windows Live Mail is not inserted), allowing for more efficient email protection. Integration settings are located under **Setup** > **Advanced setup** > **Web and email** > **Email client protection** > **Email clients**.

#### Email client integration

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

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

Turn on **Disable checking upon inbox content change** if you are experiencing a system slowdown when working with your email client (MS Outlook only). This can occur when retrieving email from the Kerio Outlook Connector Store.

**Email to scan**

**Received email** - Toggles checking of received messages.
**Sent email** - Toggles checking of sent messages.
**Read email** - Toggles checking of read messages.

**Action to be performed on infected email**

**No action** - If enabled, the program will identify infected attachments, but will leave emails without taking any action.
**Delete email** - The program will notify the user about infiltration(s) and delete the message.
**Move email to the Deleted items folder** - Infected emails will be moved automatically to the Deleted items folder.
**Move email to the folder** - Infected emails will be moved automatically to the specified folder.

**Folder** - Specify the custom folder where you want to move infected emails when detected.

**Repeat scan after update** - Toggles rescanning after a virus signature database update.

**Accept scan results from other modules** - If this is selected, the email protection module accepts scan results of other protection modules (POP3, IMAP protocols scanning).

### 8.4.3.1 Email protocols

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.

You can configure IMAP/IMAPS and POP3/POP3S protocol checking in **Advanced setup** tree (F5). To access this setting, expand **Web and email** > **Email client protection** > **Email protocols**.

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.

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

### 8.4.3.2 Alerts and notifications

Email protection provides control of email communications received through the POP3 and IMAP protocols. Using the plug-in for Microsoft Outlook and other e-mail clients, ESET 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 signature database. Scanning of POP3 and IMAP protocol communications is independent of the email client used.

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

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

After an email has been checked, a notification with the scan result can be appended to the message. You can elect to **Append tag messages to received and read mail, Append note to the subject of received and read infected email** or **Append tag messages to sent email**. Be aware that on rare occasions tag messages may be omitted in problematic HTML messages or if messages are forged by malware. The tag messages can be added to received and read email, sent email or both. The available options are:

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

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

**Template added to the subject of infected email** - Edit this template if you wish to modify the subject prefix format of an infected email. This function will replace the message subject *"Hello"* with a given prefix value *"[virus]"* to the following format: *"[virus] Hello"*. The variable *%VIRUSNAME%* represents the detected threat.

### 8.4.3.3 MS Outlook toolbar

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

**ESET Security for Microsoft SharePoint** - Click on icon opens 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.

### 8.4.3.4 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 antivirus protection options is added to Outlook Express or Windows Mail:

**ESET Security for Microsoft SharePoint** - click on icon opens 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.

**User interface**

**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.

#### 8.4.3.5 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.

#### 8.4.3.6 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.

### 8.4.4 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 webpages 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.

We strongly recommend that you leave Web access protection enabled. The following options are available in **Advanced setup** (F5) > **Web and email** > **Web access protection**:

- Basic - lets you enable or disable Web access protection. When disabled, options below will become inactive.

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

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

> **NOTE**
>
> In Windows Vista and later, HTTP traffic is always monitored on all ports for all applications. In Windows XP/2003, you can modify the **Ports used by HTTP protocol** in **Advanced setup** (F5) > **Web and email** > **Web access protection** > **Web protocols** > **HTTP scanner setup**. HTTP traffic is monitored on the specified ports for all applications, and on all ports for applications marked as Web and email clients.

ESET 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 SSL (Secure Socket Layer), and TLS (Transport Layer Security) protocols. The program will only scan traffic on ports defined in **Ports used by HTTPS protocol**, regardless of operating system version.

Encrypted communication will be not scanned when default settings are in use. To enable the scanning of encrypted communication, navigate to SSL protocol checking in Advanced setup (**F5**), click **Web and email** > **SSL protocol checking** and select **Enable SSL protocol filtering**.

- URL address management - allows you to specify HTTP addresses to block, allow or exclude from checking.
- ThreatSense engine parameter setup - **Advanced virus scanner setup** - allows you to configure settings such as types of scan (emails, archives, etc.), detection methods for Web access protection etc.

### 8.4.4.1 Basic

Choose whether you want to have **Web access protection** enabled (default) or disabled. When disabled, options below will become inactive.

NOTE
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** > **Computer** > **Web access protection**.

### 8.4.4.2 URL address management

The URL address management allows you to specify HTTP addresses to block, allow or exclude from checking. Click **Edit** to create a new list in addition to the predefined ones. This can be useful if you want to logically split different groups of addresses.

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

- 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.

In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk represents any number or character, while the question mark represents any one character. Particular care should be taken when specifying excluded addresses because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list.

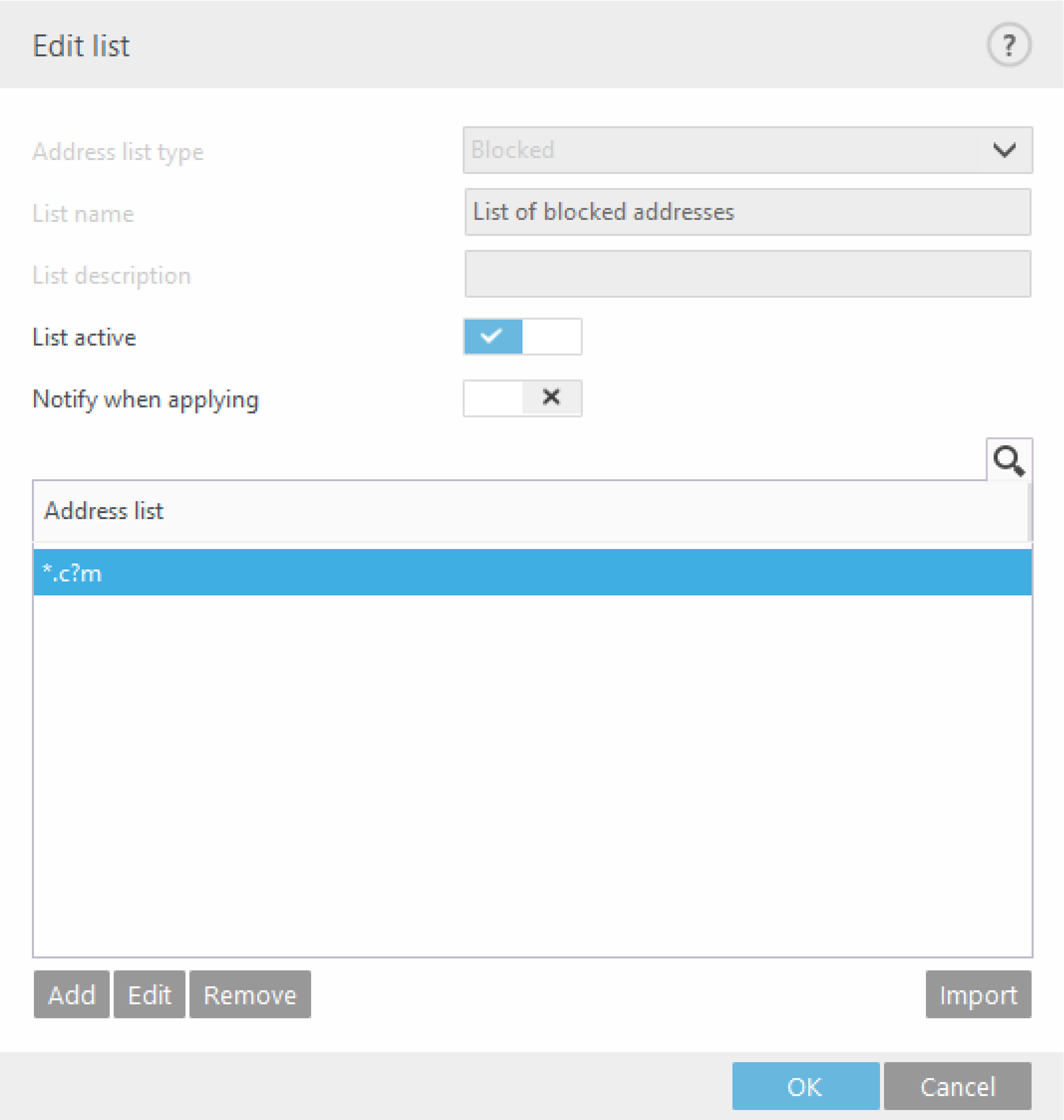
NOTE
If you want to block all HTTP addresses except addresses present in the active **List of allowed addresses**, add * to the active **List of blocked addresses.**

#### 8.4.4.2.1 Create new list

You can create a new list in addition to the predefined Address lists. 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 predefined lists.
- **List description** - type a short description for the list (optional). Will be grayed out when editing one of three predefined list.
- **List active** - use the switch to deactivate the list. You can activate it later when required.
- **Notify when applying** - if you want to be notified when a particular list is used in evaluation of an HTTP site that you visited.

EXAMPLE
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.



Edit list

Address list type: Blocked

List name: List of blocked addresses

List description:

List active: ✓

Notify when applying: ✗

Address list

*.c?m

Click **Add** to specify a URL address/domain mask. Select an address in the list and click **Remove** to delete it.Click **Edit** to make changes to an existing entry**.**

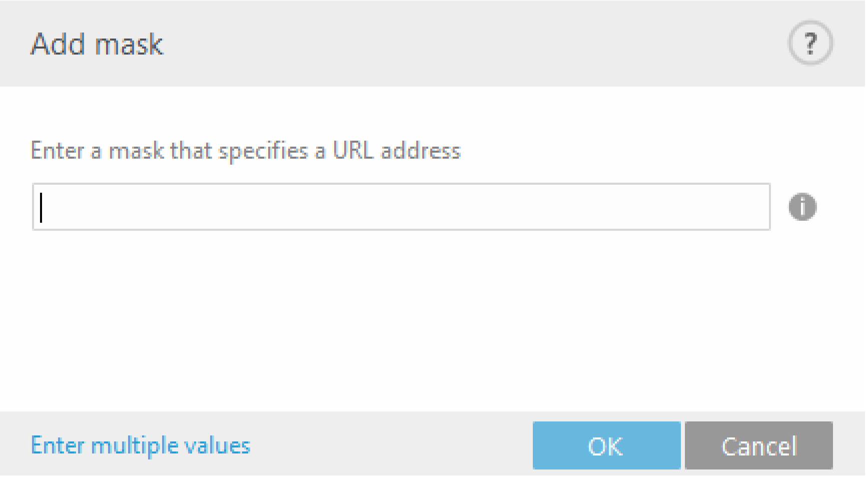
**NOTE**
Only custom address lists can be removed.

ESET Security for Microsoft SharePoint enables user to block access to specified websites and prevent the Internet browser from displaying their content. Furthermore, it allows user to specify addresses, which should be excluded from checking. If the complete name of the remote server is unknown, or the user wishes to specify a whole group of remote servers, so called masks can be used to identify such a group. The masks include the symbols ? and *:

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

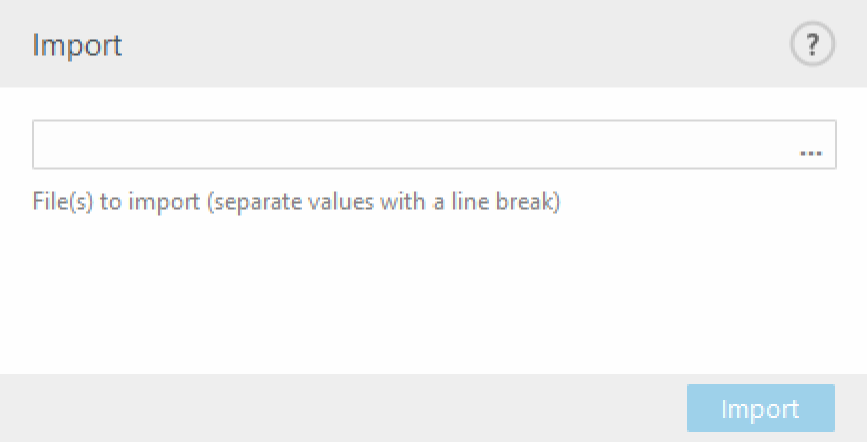
**EXAMPLE**
**.c?m* applies to all addresses where the last part begins with the letter c, ends with the letter m and contains an unknown symbol in between them (.com, .cam, etc.).

A leading *. sequence is treated specially if used at the beginning of a domain name. First, the * wildcard cannot represent a slash character ('/') in this case. This is to avoid circumventing the mask, for example the mask *.domain.com will not match *http://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 *http://domain.com*. Using **domain.com* would be incorrect, as that would also match *http://anotherdomain.com*.



When you select **Enter multiple values**, you can add multiple file extensions delimited by new lines, commas or semicolons. When multiple selection is enabled, addresses will be shown in the list.

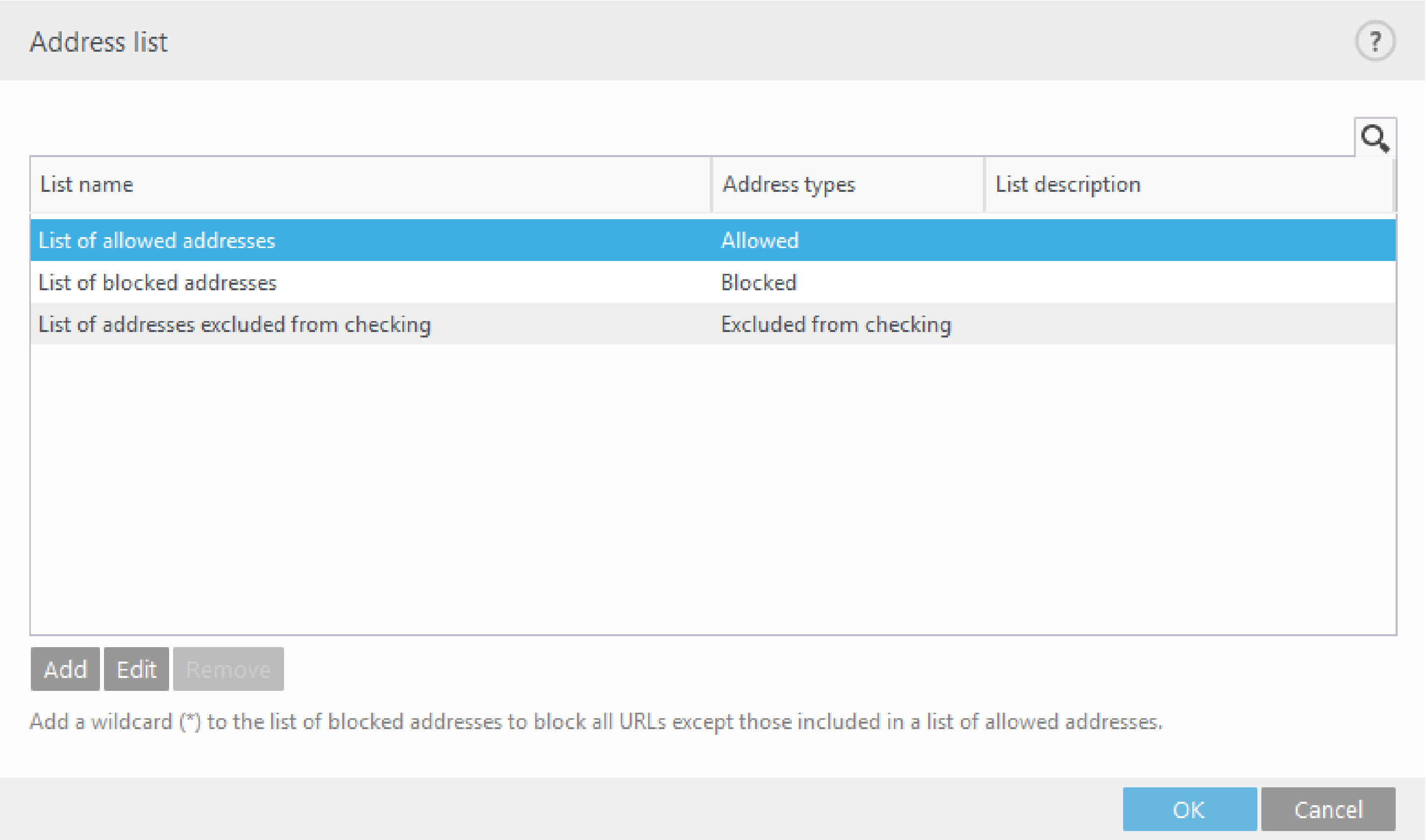
- **Import** - import a text file with URL addresses (separate values with a line break, for example `*.txt` using encoding UTF-8).



### 8.4.4.2.2 Address list

By default, the following three lists are available:

- **List of addresses excluded from checking** - No checking for malicious code will be performed for any address added to this list.
- **List of allowed addresses** - If **Allow access only to HTTP addresses in the list of allowed addresses** is enabled and the list of blocked addresses contains * (match everything), the user will be allowed to access addresses specified in this list only. The addresses in this list are allowed even if they are included in the list of blocked addresses.
- **List of blocked addresses** - The user will not be allowed to access addresses specified in this list unless they also occur in the list of allowed addresses.



| List name | Address types | List description |
|---|---|---|
| List of allowed addresses | Allowed | |
| List of blocked addresses | Blocked | |
| List of addresses excluded from checking | Excluded from checking | |

Add a wildcard (*) to the list of blocked addresses to block all URLs except those included in a list of allowed addresses.

**Add** - add a new URL address to the list (enter multiple values with separator).

**Edit** - modifies existing address in the list. Only possible for addresses created with **Add**.

**Remove** - deletes existing addresses in the list. Only possible for addresses created with **Add**.

### 8.4.5 Anti-Phishing protection

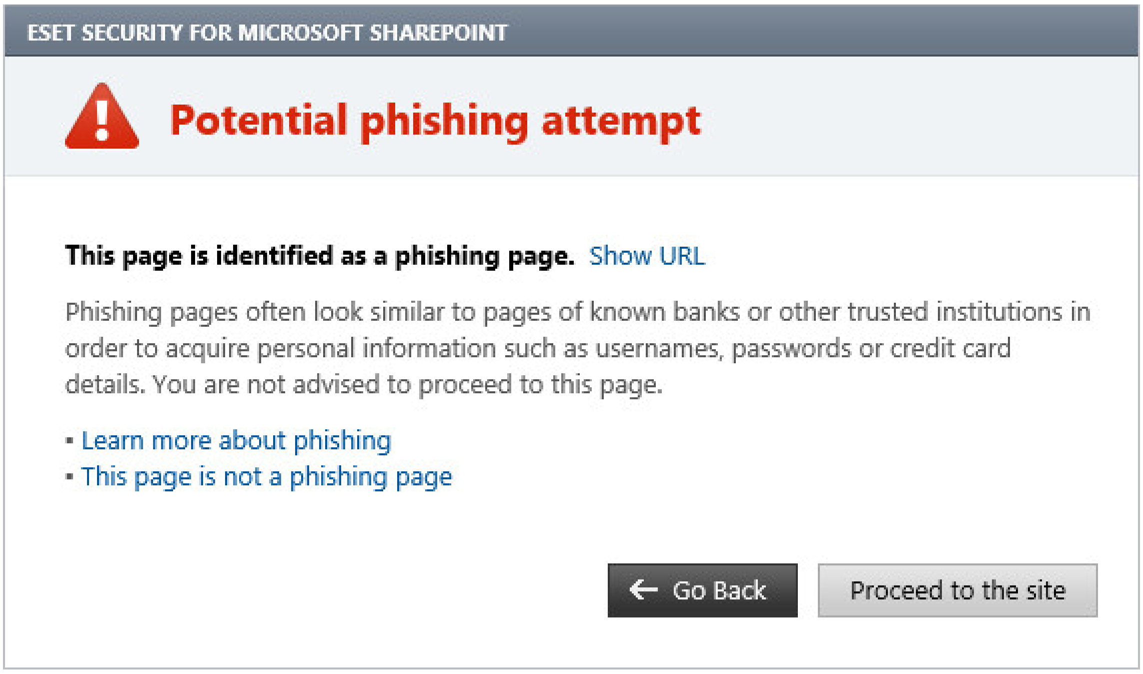
The term phishing defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more. Read more about this activity in the glossary. ESET 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. To do so, open **Advanced setup** (F5) and navigate to **Web and email** > **Anti-Phishing protection**.

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

**Accessing a phishing website**

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



ESET SECURITY FOR MICROSOFT SHAREPOINT

Potential phishing attempt

**This page is identified as a phishing page.** Show URL

Phishing pages often look similar to pages of known banks or other trusted institutions in order to acquire personal information such as usernames, passwords or credit card details. You are not advised to proceed to this page.

- Learn more about phishing
- This page is not a phishing page

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

**Phishing site reporting**

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

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

- the website is not detected at all
- the website is incorrectly detected as a threat. In this case, you can Report a false-positive phishing site.

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

## 8.5 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 unsolicited content.

**Supported external devices:**

- Disk storage (HDD, USB removable disk)
- CD/DVD
- USB printer
- FireWire Storage
- Bluetooth Device
- Smart card reader
- Imaging Device

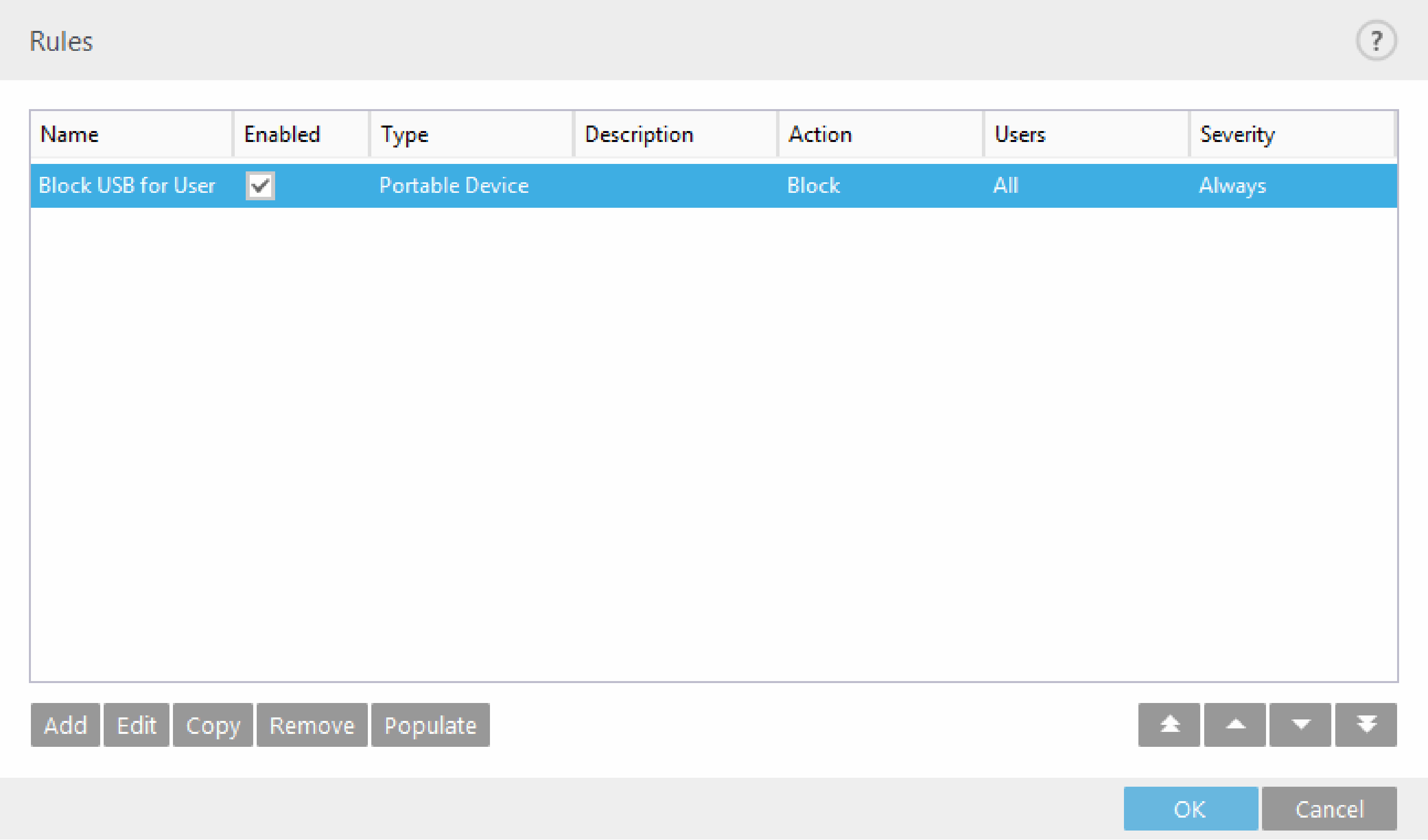
- Modem
- LPT/COM port
- Portable Device
- All device types

Enabling the switch next to **Integrate into system** activates the Device control feature in ESET Security for Microsoft SharePoint; you will need to restart your computer for this change to take effect. Device control Rules and Groups 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.

## 8.5.1 Device control rules editor

The Device control rules editor window displays existing rules and allows for precise control of external devices that users connect to the computer.



Rules

| Name | Enabled | Type | Description | Action | Users | Severity |
|---|---|---|---|---|---|---|
| Block USB for User | ☑ | Portable Device | | Block | All | Always |

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.

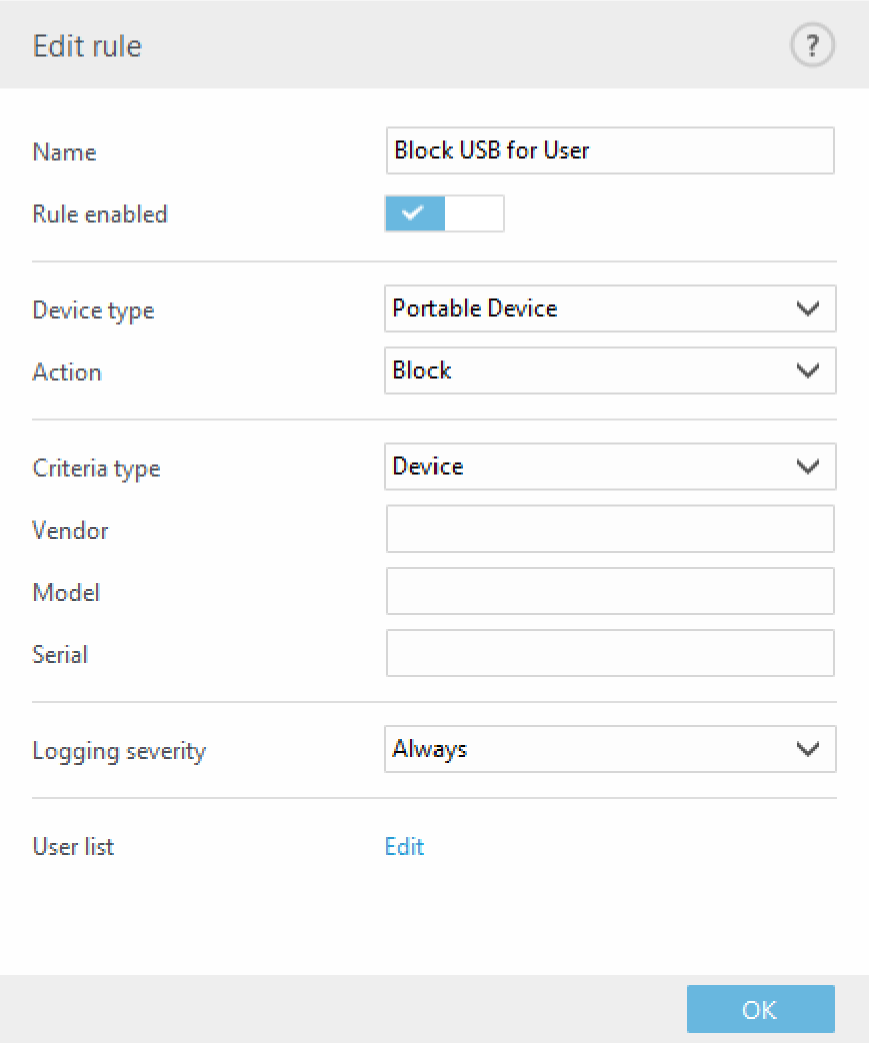
Use the following buttons at the bottom of the window to manage rules:

- Add - lets you add a new rule.
- Edit **-** lets you modify settings of an existing rule.
- **Copy** - creates a new rule based on the parameters of the selected rule.
- **Remove** - if you want to delete the selected rule. Alternatively, you can use the check box next to a given rule to disable it. This can be useful if you don't want to delete a rule permanently so that you can use it in the future.
- Populate - detects removable media device parameters for devices connected to your computer.
- 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).

Log entries can be viewed from the main program window of ESET Security for Microsoft SharePoint in **Tools** > Log files.

## 8.5.2 Adding Device control rules

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



Edit rule

| | |
|---|---|
| Name | Block USB for User |
| Rule enabled | ✓ |
| Device type | Portable Device |
| Action | Block |
| Criteria type | Device |
| Vendor | |
| Model | |
| Serial | |
| Logging severity | Always |
| User list | Edit |

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

### Device type

Choose the external device type from the drop-down menu (Disk storage/Portable device/Bluetooth/FireWire/...). 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.

Please note that not all rights (actions) are available for all device types. If a device has storage space, all four actions are made available. For non-storage devices, there are only two (for example **Read Only** is not available for Bluetooth , so Bluetooth devices can only be allowed or blocked).

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

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

> **NOTE**
> If these three descriptors are empty, the rule will ignore these fields when matching. Filtering parameters in all text fields are case-insensitive and no wildcards (*, ?) are supported.

In order to figure out the parameters of a device, create a rule to allow that type of device, connect the device to your computer and then review the device details in the Device control log.

**Severity**

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

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

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

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

### 8.5.3 Detected devices

The **Populate** button 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 predefined information (you can adjust all the settings).

### 8.5.4 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.

> **WARNING**
> Having an external device connected to your computer may pose a security risk.

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

ℹ NOTE
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** - 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).
- **Remove** - deletes the selected group or device depending on where in the window you clicked.
- **Import** - imports a serial number list of devices from a file.
- Populate - detects removable media device parameters for devices connected to your computer.

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

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

## 8.6 Tools

The following are advanced settings for all the tools ESET Security for Microsoft SharePoint offers under the **Tools** tab in the main GUI window.

- Log files
- Proxy server
- Email notification
- Presentation mode
- Diagnostics
- Cluster

### 8.6.1 ESET LiveGrid

ESET LiveGrid is an advanced early warning system comprised of several cloud-based technologies. It helps detect emerging threats based on reputation and improves scanning performance by means of whitelisting. New threat information is streamed in real-time to the cloud, which enables the ESET Malware Research Lab to provide timely response and consistent protection at all times. Users can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid. When installing ESET Security for Microsoft SharePoint, select one of the following options:

1. You can decide not to enable ESET LiveGrid. Your software will not lose any functionality, but in some cases ESET Security for Microsoft SharePoint may respond slower to new threats than virus signature database update.
2. You can configure ESET LiveGrid to submit anonymous information about new threats and where the new threatening code was detected. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

ESET LiveGrid will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer‘s operating system.

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

The ESET LiveGrid reputation system provides cloud-based whitelisting and blacklisting. To access settings for ESET LiveGrid, press **F5** to enter **Advanced setup** and expand **Tools** > **ESET LiveGrid**.

**Enable ESET LiveGrid reputation system (recommended)** - The ESET LiveGrid reputation system improves the efficiency of ESET anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.

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

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

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

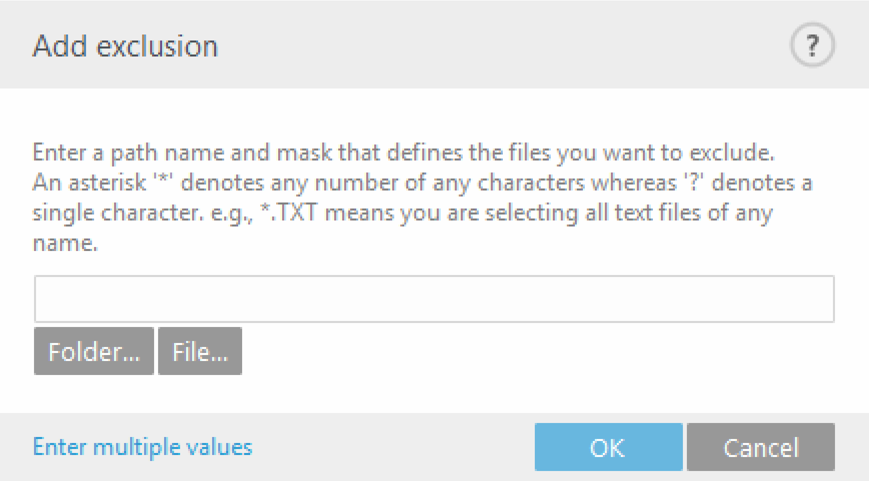
**Contact email (optional)** - Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

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

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

### 8.6.1.1 Exclusion filter

The **Edit** option next to Exclusions in ESET LiveGrid allows you to configure how threats are submitted to ESET Virus Labs for analysis.



Add exclusion

Enter a path name and mask that defines the files you want to exclude. An asterisk '*' denotes any number of any characters whereas '?' denotes a single character. e.g., *.TXT means you are selecting all text files of any name.

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

### 8.6.2 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.

### 8.6.3 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 you this method because it allows importation of any unsigned configuration, which is a potential risk.
- **Advanced setup password** - a password is required to import a configuration from an *.xml* file, this file must be signed (see 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.

IMPORTANT

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

EXAMPLE

Export settings command:

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

Import settings command:

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

NOTE

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

Signing an *.xml* configuration file:

1. Download **XmlSignTool** from the ESET Tools and Utilities download page and extract it.
2. Open a Windows Command Prompt (cmd) using **Run as administrator**.

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

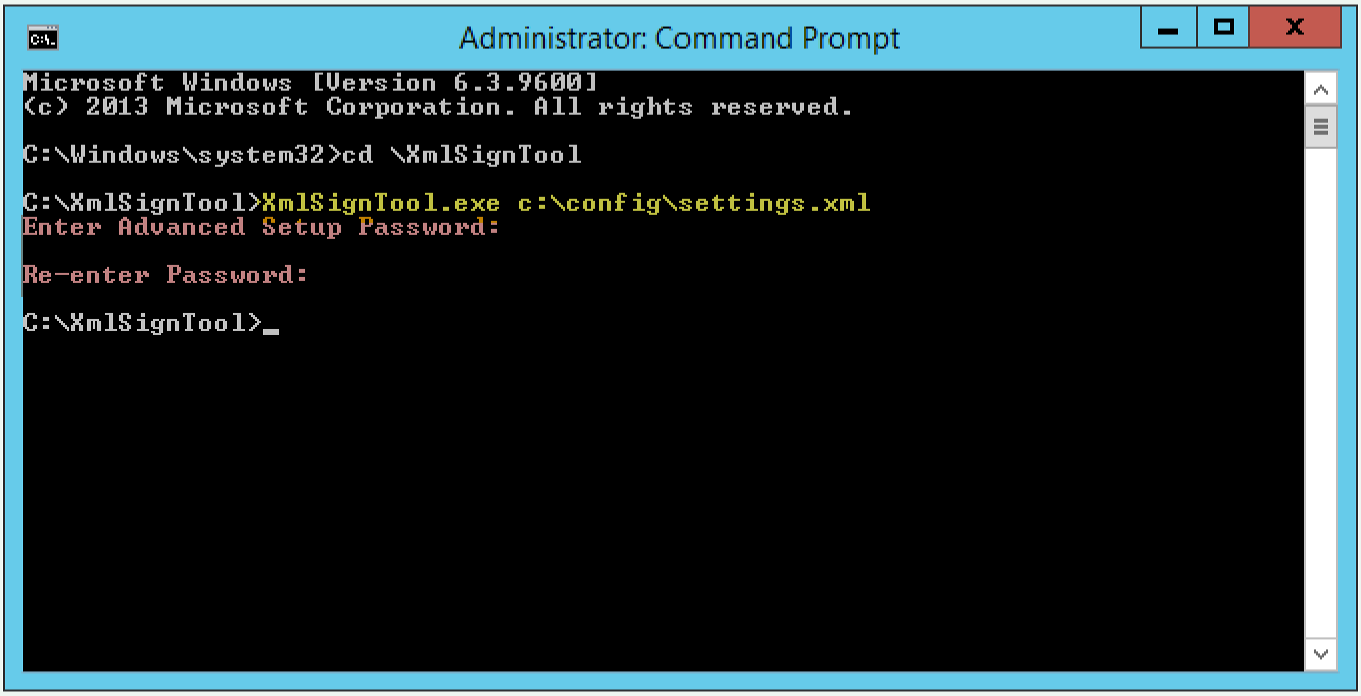
4. Execute a command to sign the *.xml* configuration file, for example: `XmlSignTool <xml_file_path>`

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.

EXAMPLE

Sign exported configuration file commnad:

`XmlSignTool c:\config\settings.xml`



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \XmlSignTool

C:\XmlSignTool>XmlSignTool.exe c:\config\settings.xml
Enter Advanced Setup Password:

Re-enter Password:

C:\XmlSignTool>_
```

NOTE

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

### 8.6.4 WMI Provider

**About WMI**

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.

### 8.6.4.1 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_MailServerLog

**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 MS Exchange or IBM Domino
- **SERVER_EMAIL_AS** - anti-spam protection of emails of protected server product, for example, emails in MS Exchange or IBM Domino
- **SERVER_GATEWAY_AV** - anti-virus protection of protected network protocols on the gateway
- **SERVER_GATEWAY_AS** - anti-spam protection of protected network protocols on the gateway

### ESET_Statistics class

The ESET_Statistics class has multiple instances, depending on the number of scanners in the product. Each instance contains:

- Scanner - string code for the particular scanner, for example, “CLIENT_FILE”
- Total - total number of files scanned
- Infected - number of infected files found
- Cleaned - number of cleaned files
- Timestamp - timestamp of the last change of this statistics. In WMI datetime format, for example, “20130118115511.000000+060”
- ResetTime - timestamp of when the statistics counter was last reset. In WMI datetime format, for example, “20130118115511.000000+060”
- List of strings representing currently recognized scanners:
- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

### ESET_ThreatLog class

The ESET_ThreatLog class has multiple instances, each one representing a log record from the “Detected threats” log. Each instance contains:

- **ID** - unique ID of this 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]. 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

### 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 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
- **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 on-demand 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_ODFileScanLogRecords**

The ESET_ODFileScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_ODFileScanLogs class. Instances of this class provide log records of all the on-demand scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each class instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_ODFileScanLogs class)
- **ID** - unique ID of this scan log record
- **Timestamp** - creation timestamp of the log 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_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 on-demand 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
- **RuleHits** - Total number of rule hits
- **Status** - Status of the scan process

**ESET_ODServerScanLogRecords**

The ESET_ODServerScanLogRecords class has multiple instances, each one representing a log record in one of the scan logs represented by instances of the ESET_ODServerScanLogs class. Instances of this class provide log records of all the on-demand scans/logs. When instance of a particular scan log are required only, they must be filtered by the LogID property. Each class instance contains:

- **LogID** - ID of the scan log this record belongs to (ID of one of the instances of the ESET_ ODServerScanLogs class)
- **ID** - unique ID of this scan log record
- **Timestamp** - creation timestamp of the log record (in the WMI date/time format)
- **LogLevel** - severity of the log record expressed as a number in the [0-8] interval. Values correspond to the following named levels: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - The actual log message

**ESET_GreylistLog**

The ESET_GreylistLog class has multiple instances, each one representing a log record from the “Greylist” 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
- **HELODomain** - Name of the HELO domain
- **IP** - Source IP address
- **Sender** - Email sender
- **Recipient** - Email recipient
- **Action** - Action performed
- **TimeToAccept** - Number of minutes after which the email will be accepted

### 8.6.4.2 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 predefined 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'
```

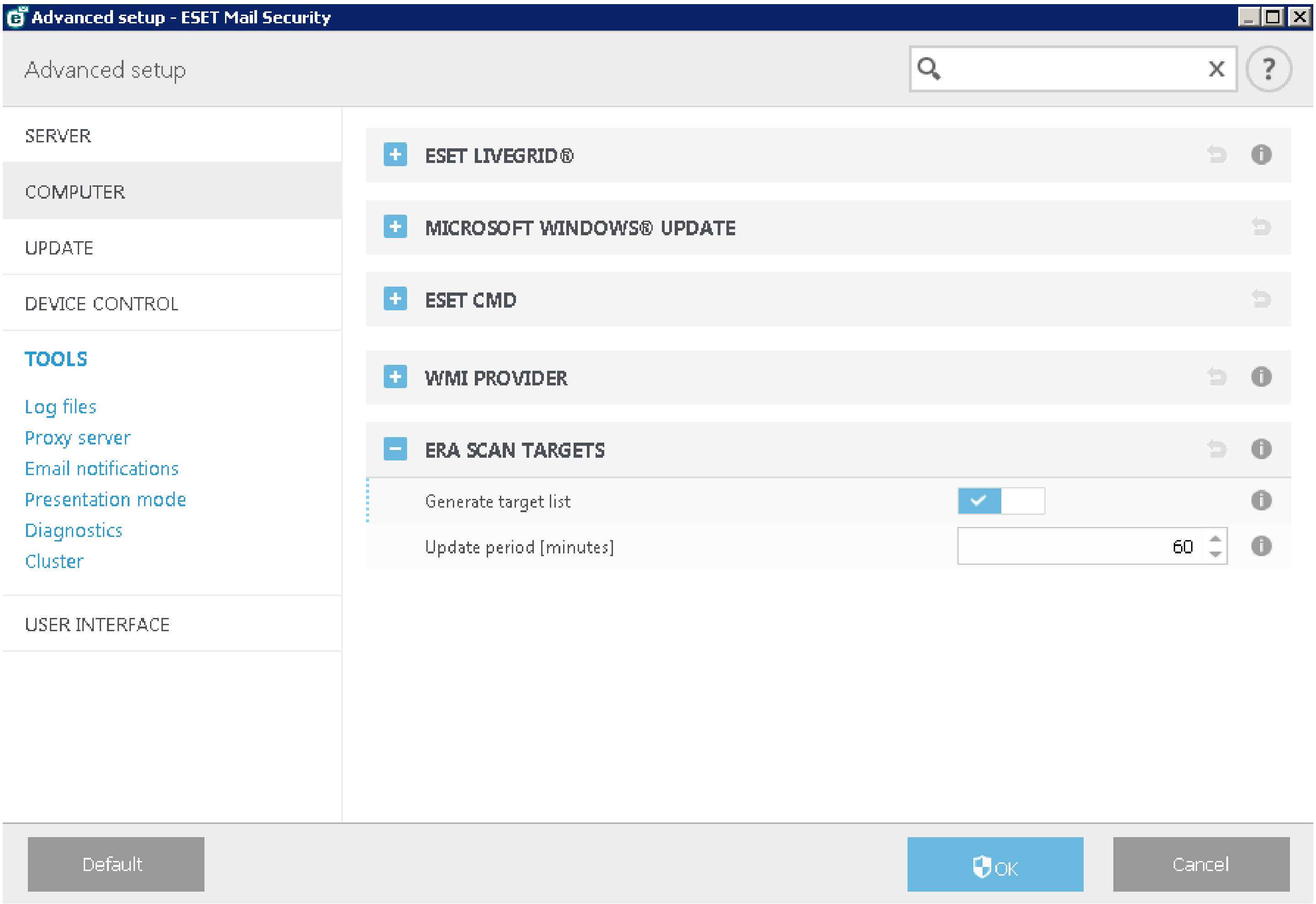
Get and display complete info about product on a remote machine with IP 10.1.118.180:

```
$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
```

### 8.6.5 ERA scan targets

This functionality lets ESET Remote Administrator use the appropriate scan target (SharePoint database scan, On-demand computer scan and Hyper-V) when running the **Server Scan** Client task on a server with ESET Security for Microsoft SharePoint.

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**.



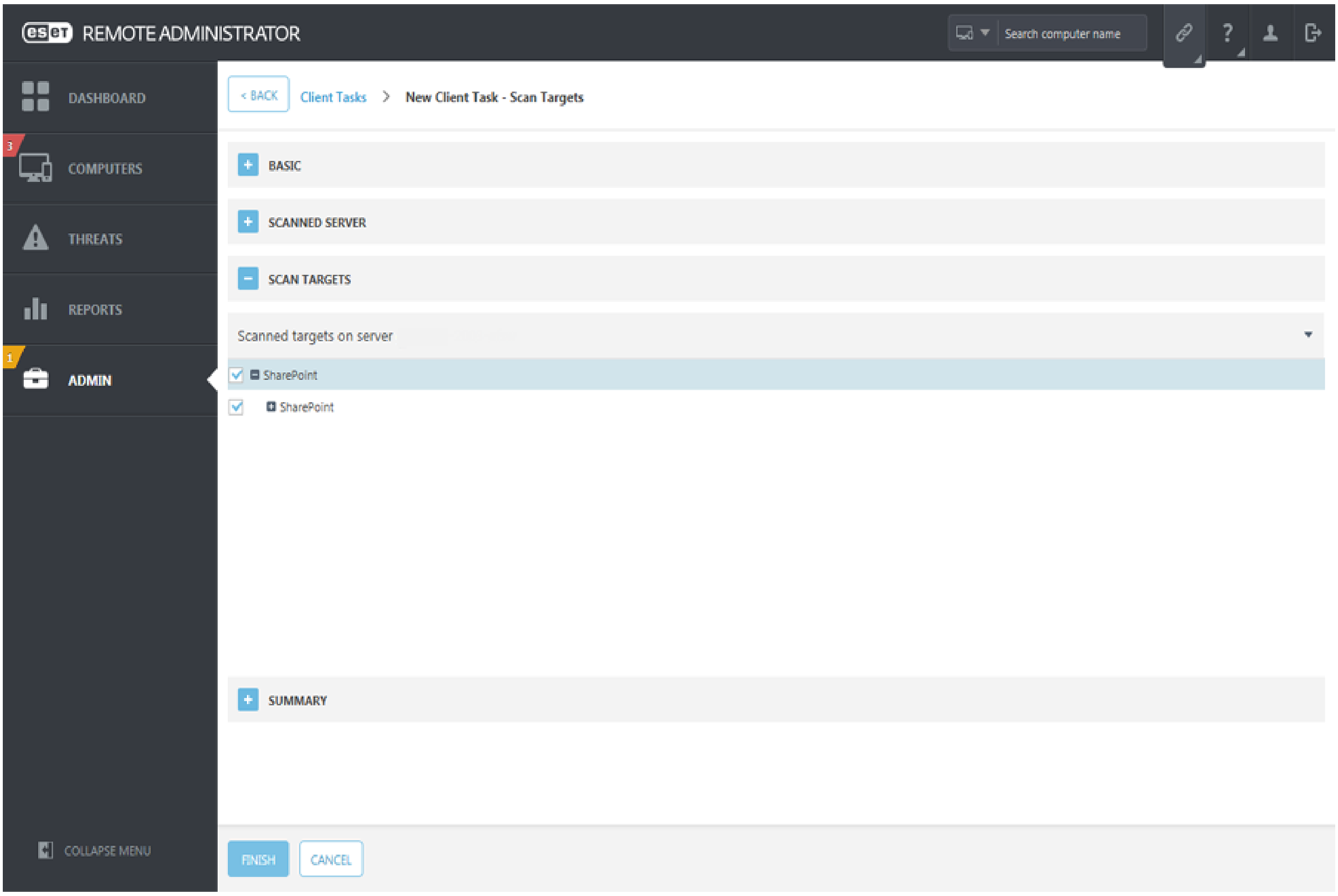
Generate target list ☑

Update period [minutes] 60

**NOTE**

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

When ERA runs a **Server Scan** Client task, it will collect the list and you will be asked to select scan targets for SharePoint database scan on that particular server.

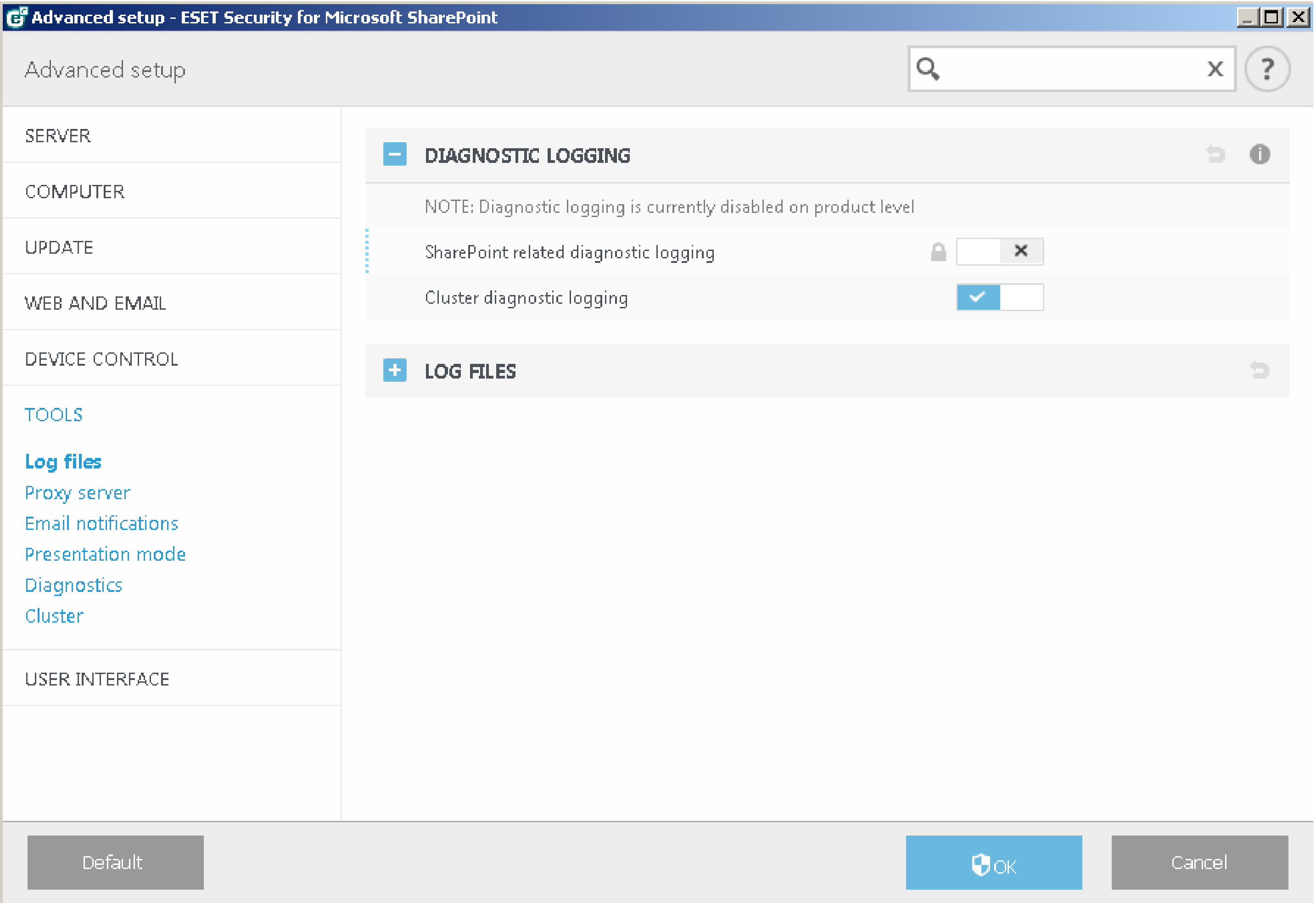


## 8.6.6 Log files

This section let's you modify configuration of ESET Security for Microsoft SharePoint logging. You can use the switches to disable or enable particular feature. All records are written to the **Events** log ( `C:\ProgramData\ESET\ESET Mail Security\Logs\warnlog.dat`) and can be viewed in Log files viewer.

- **Diagnostic logging** - use the switches to disable or enable particular feature **SharePoint related diagnostic logging** and **Cluster diagnostic logging** if required.

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



DIAGNOSTIC LOGGING

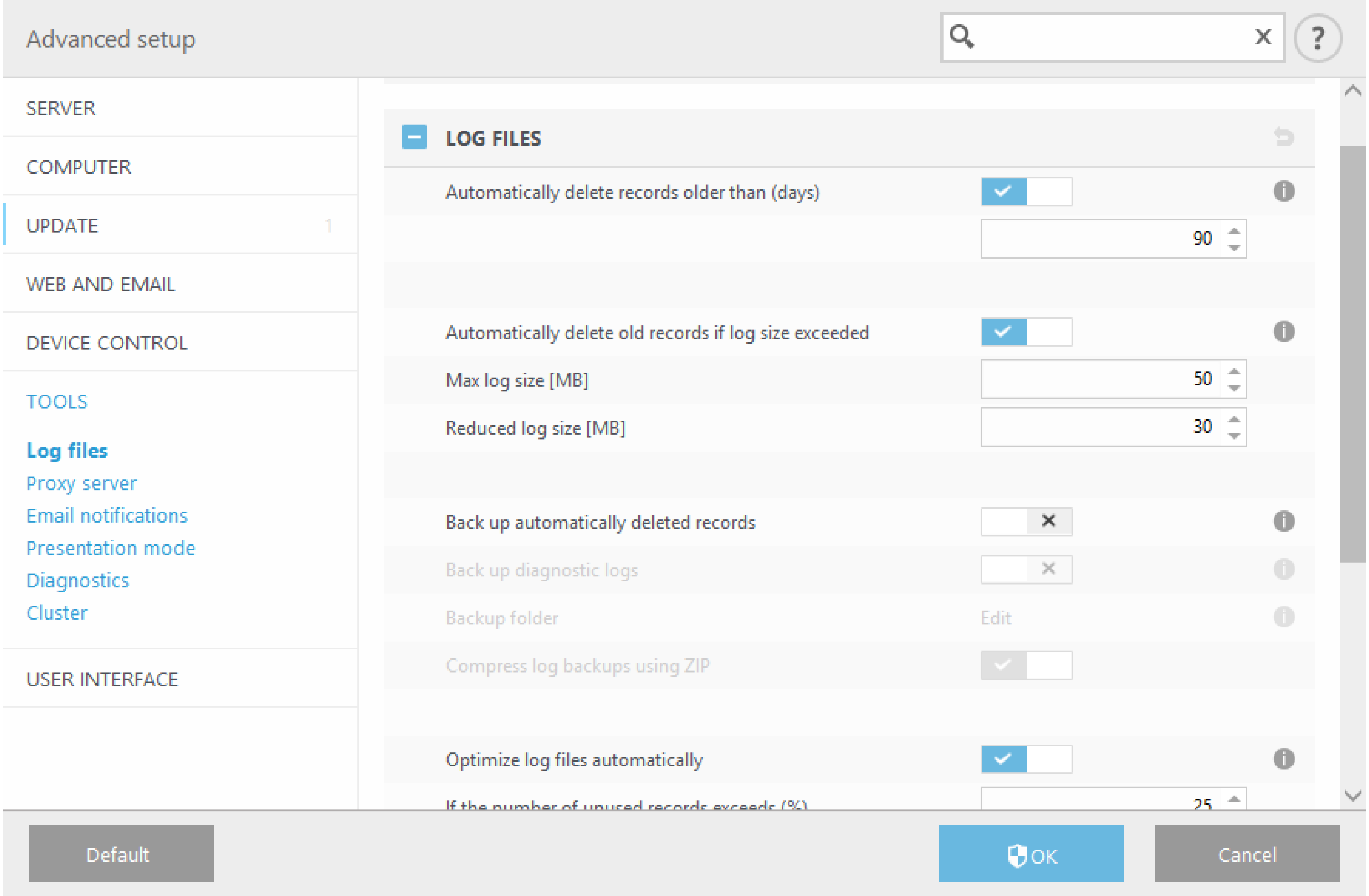
NOTE: Diagnostic logging is currently disabled on product level

SharePoint related diagnostic logging ✗

Cluster diagnostic logging ✓

LOG FILES

- **Log files** - to open advanced setup to define how the logs will be managed. The program automatically deletes older logs to save disk space.



LOG FILES

| | |
|---|---|
| Automatically delete records older than (days) | ✓ |
| | 90 |
| Automatically delete old records if log size exceeded | ✓ |
| Max log size [MB] | 50 |
| Reduced log size [MB] | 30 |
| Back up automatically deleted records | ✕ |
| Back up diagnostic logs | ✕ |
| Backup folder | Edit |
| Compress log backups using ZIP | ✓ |
| Optimize log files automatically | ✓ |
| If the number of unused records exceeds (%) | 25 |

Log entries older than the specified number of days in the **Automatically delete records older than (days)** field will automatically be deleted.
**Automatically delete old records if log size exceeded** - when log size exceeds **Max log size [MB]**, old log records will be deleted until **Reduced log size [MB]** is reached.

**Back up automatically deleted records -** automatically deleted log records and files will be backed up to the specified directory and optionally compressed as ZIP files
**Back up diagnostic logs** - will back up automatically deleted diagnostic logs. If not enabled, diagnostic log records are not backed up.
**Backup folder** - folder where log backups will be stored. You can enable compressed log backups using ZIP.

**Optimize log files automatically** - When engaged, log files will automatically be defragmented, if 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.

Turn on **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 predefined file name (for example, *virlog.txt* for **Detected threats** section of Log files, if you use plain text file format to store logs).

**Type** - If you select the **Text** file format, logs will be stored in a text file; data will be separated by tabs. The same applies to the comma-separated **CSV** file format. If you choose **Event**, logs will be stored in the Windows Event log (can be viewed using Event Viewer in Control panel) as opposed to file.

**Delete all log files** - erases all stored logs currently selected in the **Type** drop-down menu.

ℹ NOTE
In order to help resolve issues more quickly, ESET Customer Care 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.

### 8.6.6.1 Log filtering

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

Enter the search keyword into the **Find text** field. Use the **Search in columns** drop-down menu to refine your search.

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

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

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

**Match whole words only** - Select this check box if you want to search for specific whole words for more precise results.

**Case sensitive** - Enable this option if it is important for you to use capital or lower case letters while filtering.

### 8.6.6.2 Find in log

In addition to Log filtering, you can use the search functionality within Log files, however you can also use it independently from log filtering. This is useful when you are looking for particular records in logs. Like Log filtering, this search feature will help you find the information you are looking for, especially when there are too many records.

When using search in log, you can **Find text** by typing a specific string, use the **Search in columns** drop-down menu to filter by column, select **Record types** and set a **Time period** to only search for records from a specific time period. By specifying certain search options, only records that are relevant (according to those search options) will be searched in the Log files window.

**Find text:** Type a string (word, or part of a word). Only records that contain this string will be found. 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. By default, all columns are selected:

- **Time**
- **Scanned folder**
- **Event**
- **User**

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

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

**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 (date and time) to search only those records from a specified time period.

**Match whole words only** - Finds only records that match the string as a whole word in the **What** text box.

**Match case sensitive** - Finds only records that match the string with exact capitalization in the **What** text box.

**Search upwards** - Searches from the current position upwards.

Once you have configured your search options, click **Find** to start searching. The search stops when it finds the first corresponding record. Click **Find** again to see additional records. The Log files are searched from top to bottom, starting from your current position (the record that is highlighted).

### 8.6.7 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. Otherwise 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).

First, proxy server settings can be configured in **Advanced setup** under **Tools** > **Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET 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.

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

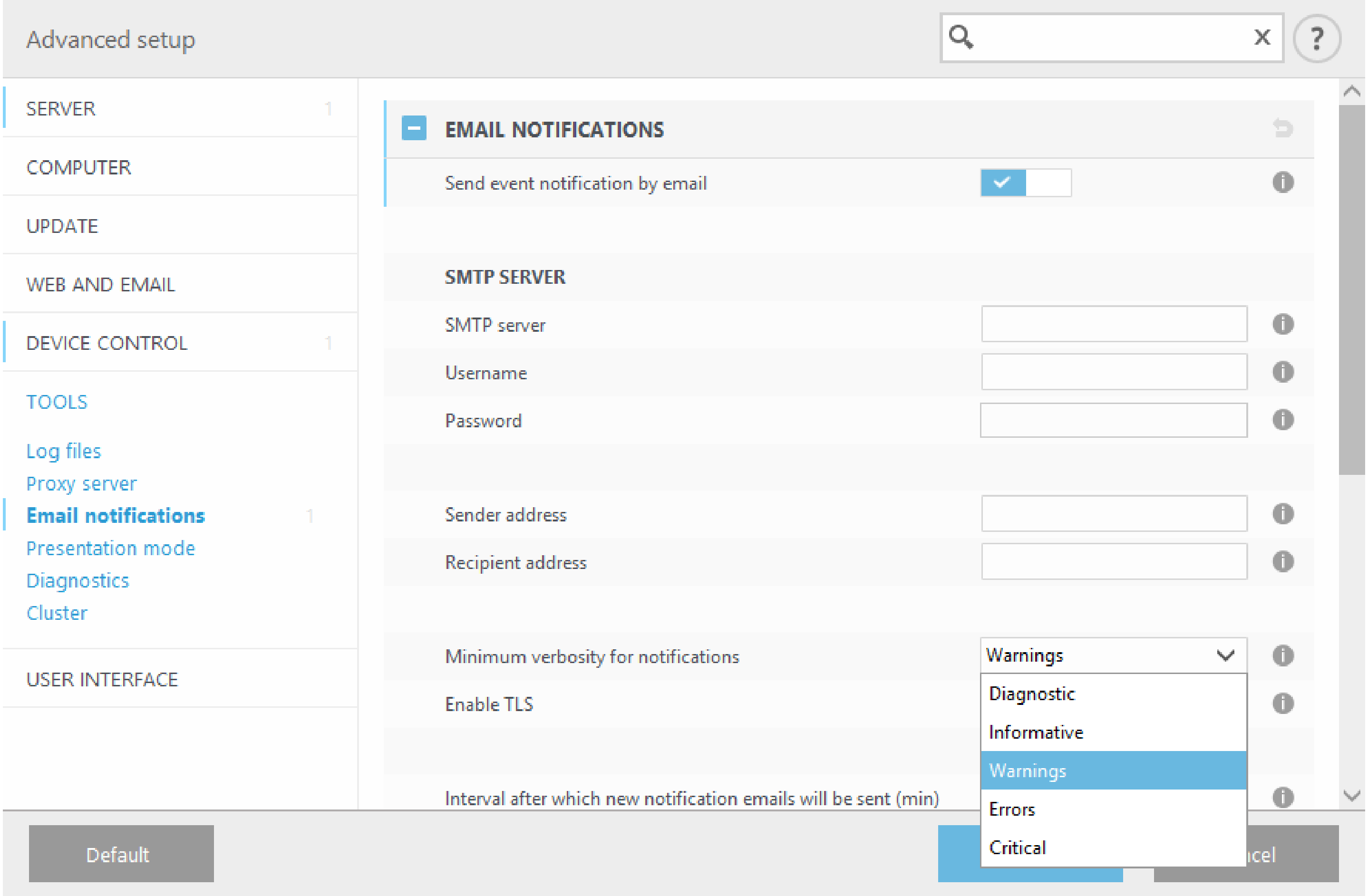
> **NOTE**
> This feature does not retrieve authentication data (username and password); it must be supplied by you.

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

**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.

### 8.6.8 Email notifications

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



EMAIL NOTIFICATIONS

Send event notification by email ✓

SMTP SERVER

SMTP server

Username

Password

Sender address

Recipient address

Minimum verbosity for notifications: Warnings

Enable TLS

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

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

- **SMTP server -** The SMTP server used for sending notifications.
- **Username and password -** If the SMTP server requires authentication, these fields should be filled in with a valid username and password to access the SMTP server.
- **Sender address** - Enter sender's address that will appear in the header of notification emails. This is what the recipient will see in the **From** field.
- **Recipient address -** Specify recipient's email address **To** whom notifications will be delivered.
- **Minimum verbosity for notifications** - Specifies the minimum verbosity level of notifications to be sent.
- **Enable TLS** - Enable alert and notification messages supported by TLS encryption.
- **Interval after which new notification emails will be sent (min)** - Interval in minutes after which new notification will be sent via email. Set this value to 0 if you want to send those notifications immediately.
- **Send each notification in a separate email** - When enabled, the recipient will receive a new email for each individual notification. This may result in a large number of emails being received in a short period of time.

**Message format**

- **Format of event messages** - Format of event messages that are displayed on remote computers. Also see Edit format.
- **Format of threat warning messages** - Threat alert and notification messages have a predefined default format. We

advise against changing this format. However, in some circumstances (for example, if you have an automated email processing system), you may need to change the message format. Also see Edit format.

- **Use local alphabetic characters -** Converts an email message to the ANSI character encoding based on Windows Regional settings (for example, windows-1250). If you leave this deselected, a message will be converted and encoded in ACSII 7-bit (for example "á" will be changed to "a" and an unknown symbol to "?").
- **Use local character encoding -** The email message source will be encoded to Quoted-printable (QP) format which uses ASCII characters and can correctly transmit special national characters by email in 8-bit format (áéíóú).

### 8.6.8.1 Message format

Communications between the program and a remote user or system administrator are done via emails or LAN messages (using the Windows messaging service). The default format of the alert messages and notifications will be optimal for most situations. In some circumstances, you may need to change the message format of event messages.

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

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

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

### 8.6.9 Presentation mode

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

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

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

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

### 8.6.10 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:

- Select **Disable** (default) to disable this feature.
- **Mini** - Records the smallest set of useful information that may help identify why the application crashed unexpectedly. This kind of dump file can be useful when space is limited. However, because of the limited information included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.
- **Full** - Records all the contents of system memory when the application stops unexpectedly. A complete memory dump may contain data from processes that were running when the memory dump was collected.

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

**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.

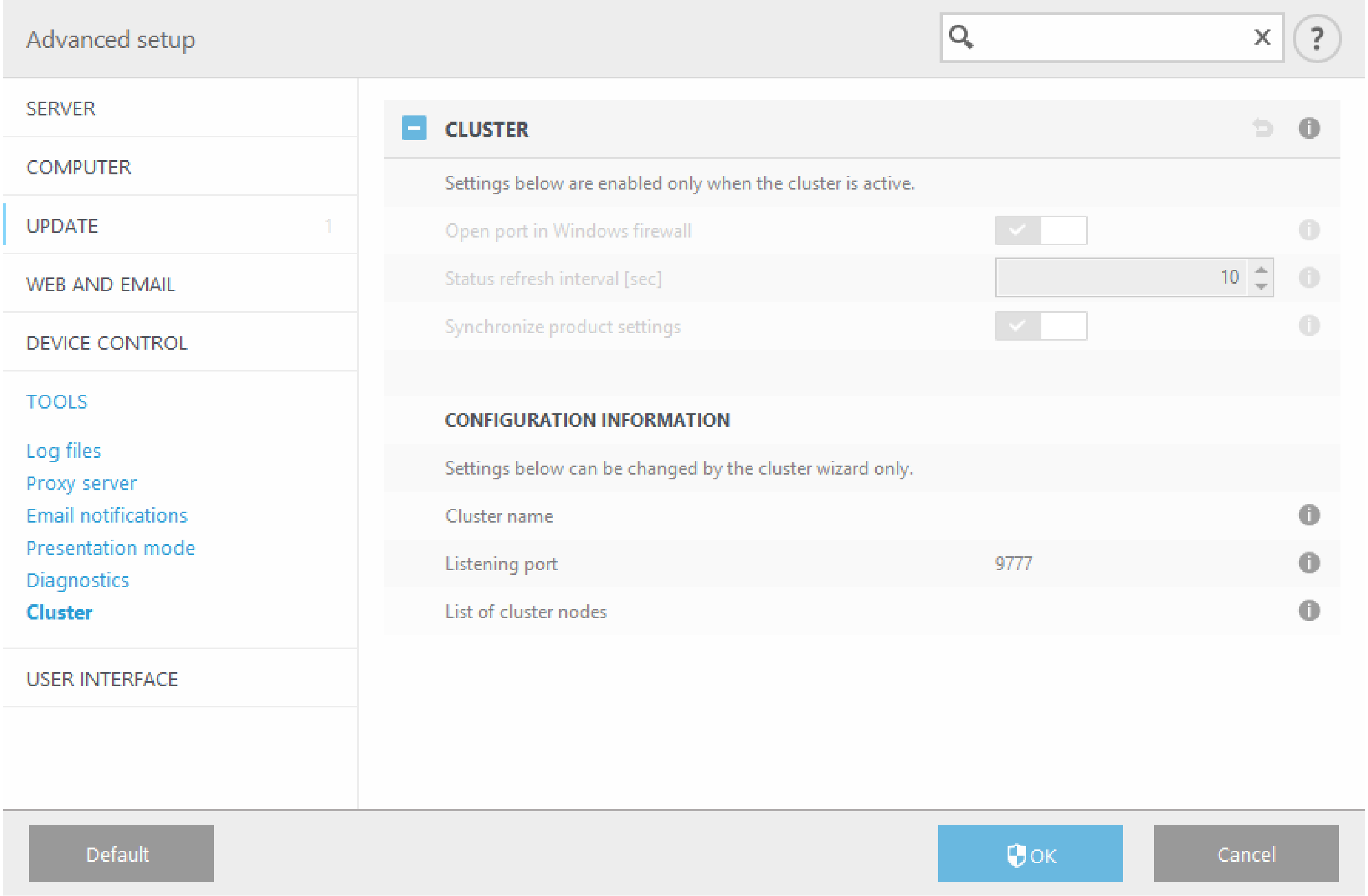
### 8.6.11 Customer Care

**Submit system configuration data** - Select **Always submit** from the drop-down menu, or select **Ask before submission** to be prompted before submitting data.

### 8.6.12 Cluster

**Enable Cluster** is automatically enabled when the ESET Cluster is configured. You can disable it manually in the **Advanced setup** window by clicking the switch icon (it is suitable 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:



CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall ✓

Status refresh interval [sec] 10

Synchronize product settings ✓

CONFIGURATION INFORMATION

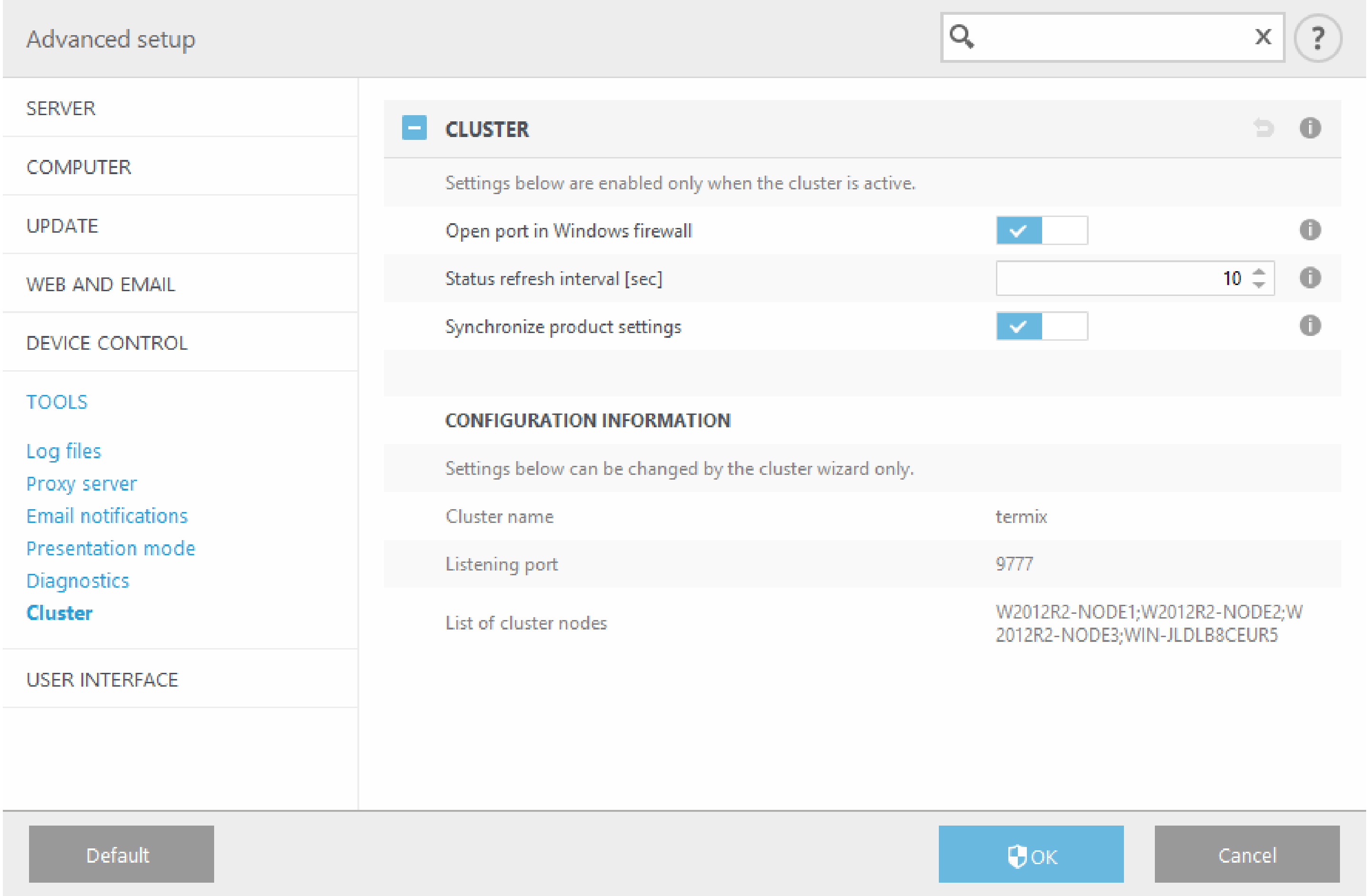
Settings below can be changed by the cluster wizard only.

Cluster name

Listening port 9777

List of cluster nodes

ESET Cluster properly configured with its details and options:



CLUSTER

Settings below are enabled only when the cluster is active.

| | |
|---|---|
| Open port in Windows firewall | ✓ |
| Status refresh interval [sec] | 10 |
| Synchronize product settings | ✓ |

CONFIGURATION INFORMATION

Settings below can be changed by the cluster wizard only.

| | |
|---|---|
| Cluster name | termix |
| Listening port | 9777 |
| List of cluster nodes | W2012R2-NODE1;W2012R2-NODE2;W2012R2-NODE3;WIN-JLDLB8CEUR5 |

For more information on the ESET Cluster click here.

## 8.7 User interface

The **User interface** section allows you to configure the behavior of the program's Graphical user interface (GUI). You can adjust the program's visual appearance and effects.

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

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

If you choose not to display some notifications, they will be displayed in the Disabled messages and statuses area. Here you can check their status, show more details or remove them from this window.

Right-click an item to display the ESET Security for Microsoft SharePoint context menu integration. Use this tool to integrate ESET Security for Microsoft SharePoint control elements into the context menu.

Presentation mode is useful for users who want to work with an application and not be interrupted by pop-up windows, scheduled tasks and other processes that might stress system resources.

### User interface elements

User interface configuration options in ESET Security for Microsoft SharePoint allow you to adjust the working environment to fit your needs. These configuration options are accessible in the **User interface** > **User interface elements** branch of the ESET Security for Microsoft SharePoint **Advanced setup** tree (F5).

In the **User interface elements** section you can adjust the working environment. 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.

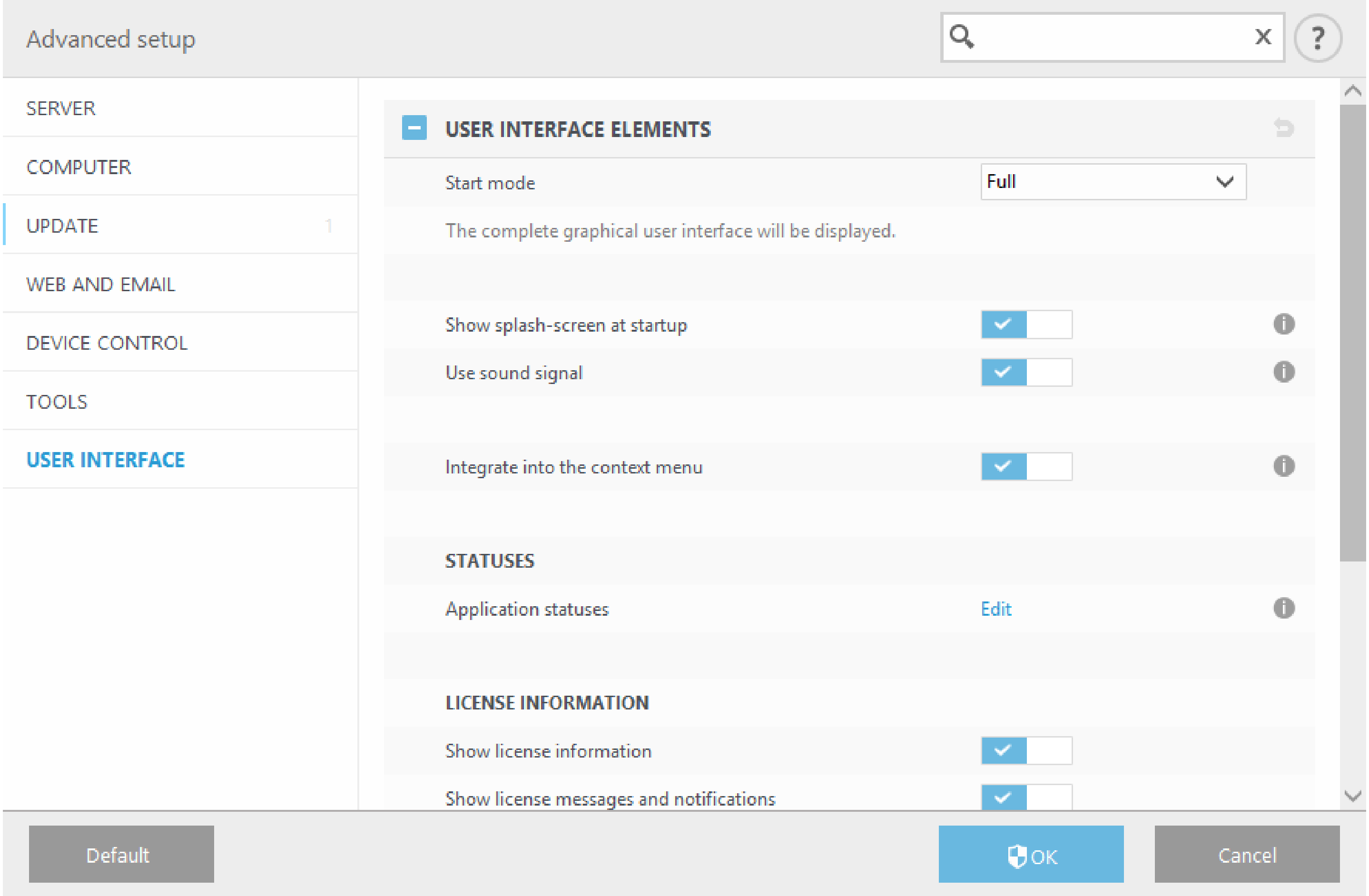
Click the **Start mode** drop-down menu to select from the following Start modes:

- **Full** - The complete GUI will be displayed.
- **Terminal** - No notifications or alerts will be displayed. GUI can only be started by the Administrator.

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

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

**Integrate into the context menu** - Integrate the ESET Security for Microsoft SharePoint control elements into the context menu.



USER INTERFACE ELEMENTS

Start mode: Full

The complete graphical user interface will be displayed.

Show splash-screen at startup ✓

Use sound signal ✓

Integrate into the context menu ✓

STATUSES

Application statuses: Edit

LICENSE INFORMATION

Show license information ✓

Show license messages and notifications ✓

**Application statuses** - click Edit to manage (enable or disable) statuses that are displayed in the Monitoring tab in main menu. Alternatively, you can use ESET Remote Administrator policies to configure your application statutes.

**License Information** - when enabled, messages and notifications about your license will be displayed.

## 8.7.1 Alerts and notifications

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

### Alert windows

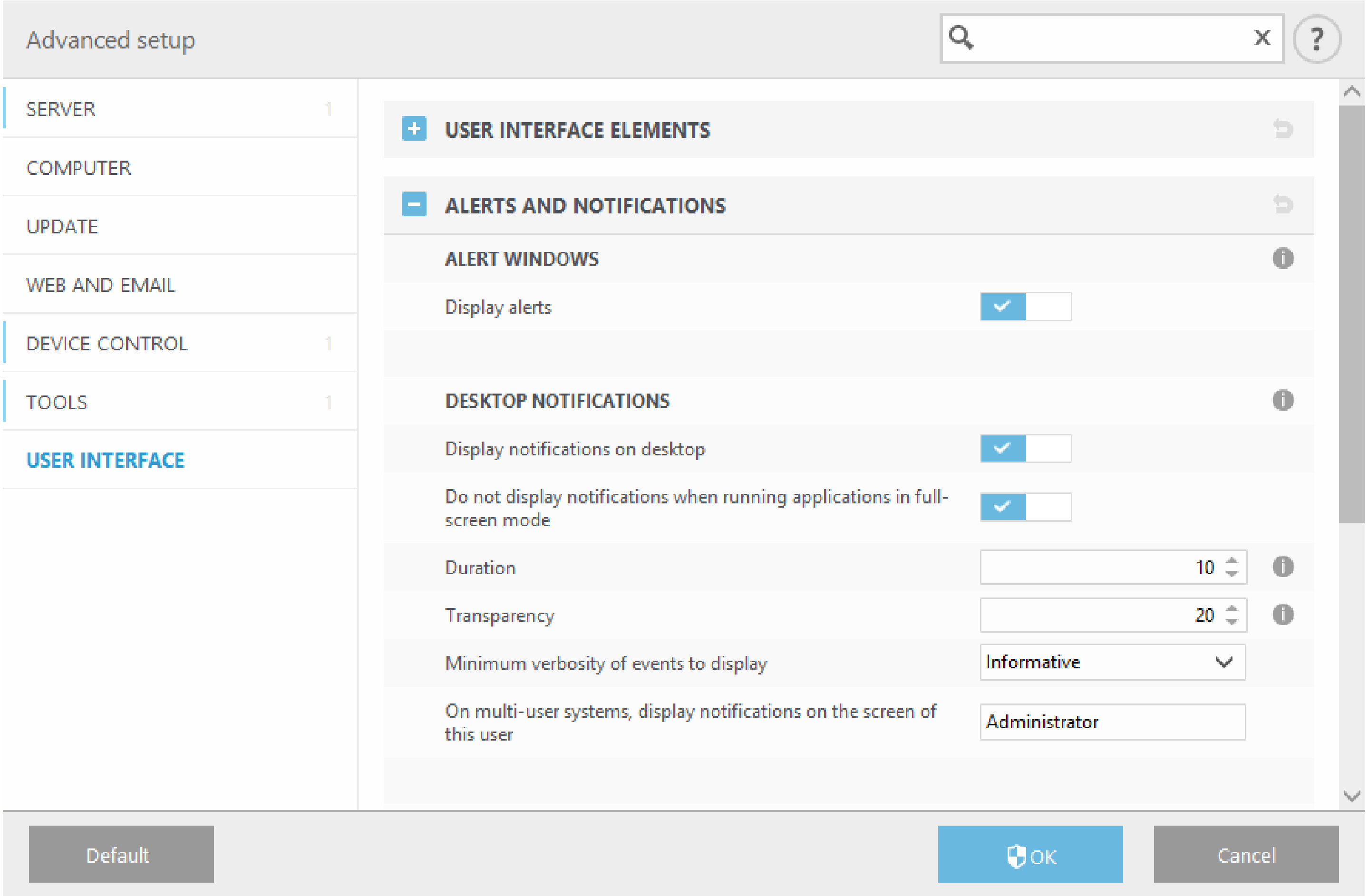
Disabling **Display alerts** will cancel all alert windows, and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left in its default setting (enabled).

### Desktop notifications

Notifications on the Desktop and balloon tips are informative only, and do not require user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate Desktop notifications, select

**Display notifications on desktop**. More detailed options, such as notification display time and window transparency can be modified below.

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



Display alerts ✓

Display notifications on desktop ✓

Do not display notifications when running applications in full-screen mode ✓

Duration 10

Transparency 20

Minimum verbosity of events to display Informative

On multi-user systems, display notifications on the screen of this user Administrator

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

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

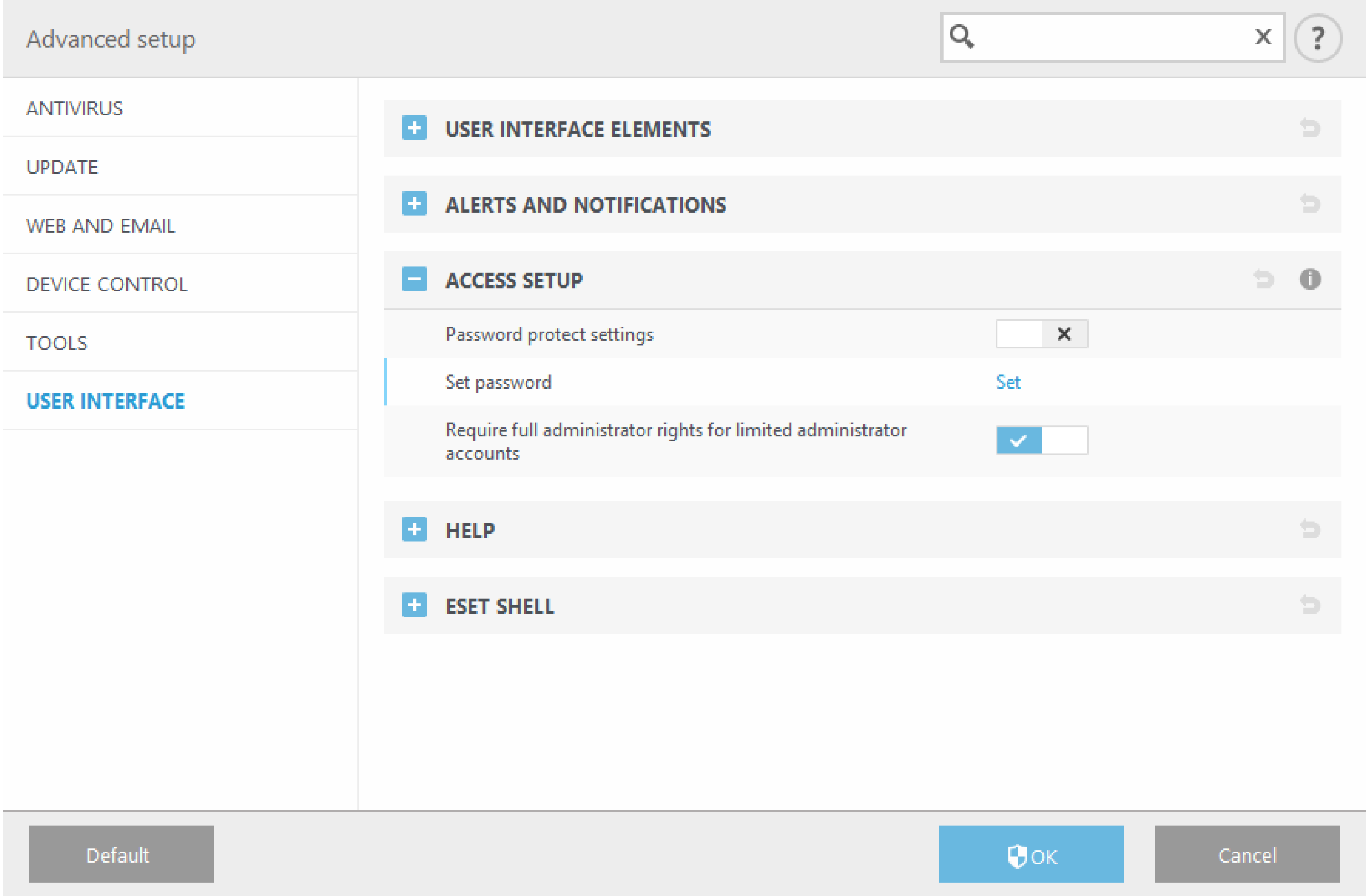
The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of this user** field specifies which user will receive system and other notifications on systems allowing multiple users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

### Message boxes

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

### 8.7.2 Access setup

In order to provide maximum security for your system, it is essential that ESET Security for Microsoft SharePoint is correctly configured. Any unqualified change may result in a loss of important data. To avoid unauthorized modifications, the setup parameters of ESET Security for Microsoft SharePoint can be password protected. Configuration settings for password protection are located in the **Access setup** submenu under **User interface** in the **Advanced setup** tree (F5).



Password protect settings ☒

Set password: Set

Require full administrator rights for limited administrator accounts ✓

**Password protect settings** - Locks/unlocks the program's setup parameters. Click to open the Password setup window.

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

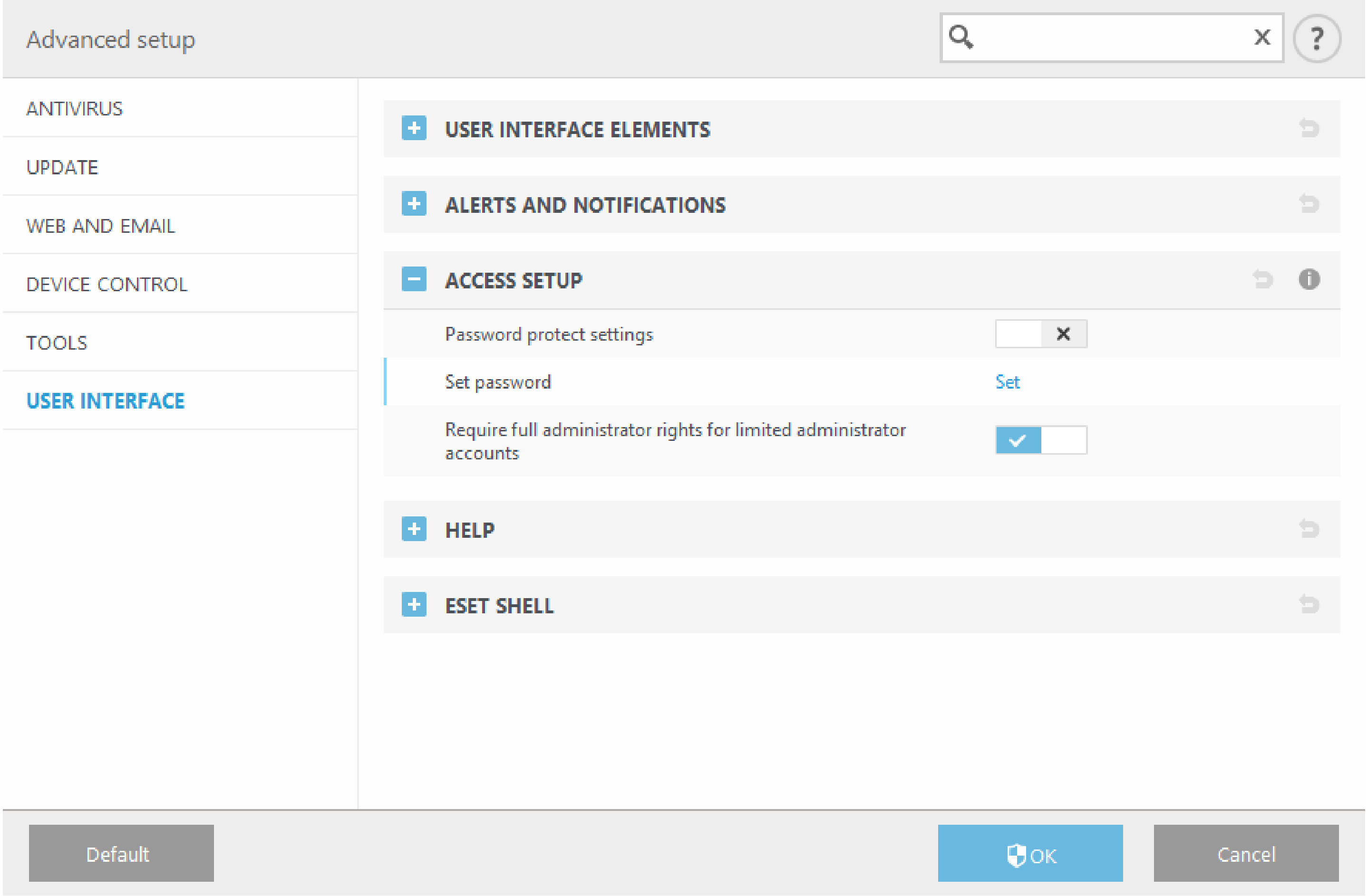
**Require full administrator rights for limited administrator accounts** - Select this option to prompt the current user (if he or she does not have administrator rights) to enter an administrator username and password when modifying certain system parameters (similar to UAC in Windows Vista). The modifications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

**NOTE**

If the Access Setup password changes and you want to import an existing *.xml* configuration file (that was signed before the password change) using the ESET CMD command line, make sure to sign it again using your current password. This allows you to use older configuration file without the need to export it on the other machine running ESET Security for Microsoft SharePoint before the import.

### 8.7.2.1 Settings protection

ESET Security for Microsoft SharePoint settings can be very important from the perspective of your organization’s security policy. Unauthorized modifications can potentially endanger the stability and protection of your system. To access **User interface** setup, click **Setup** in the main menu and then click **Advanced setup**, or press **F5** on your keyboard. Click **User interface** > **Access setup**, select **Password protect settings** and click **Set password**.



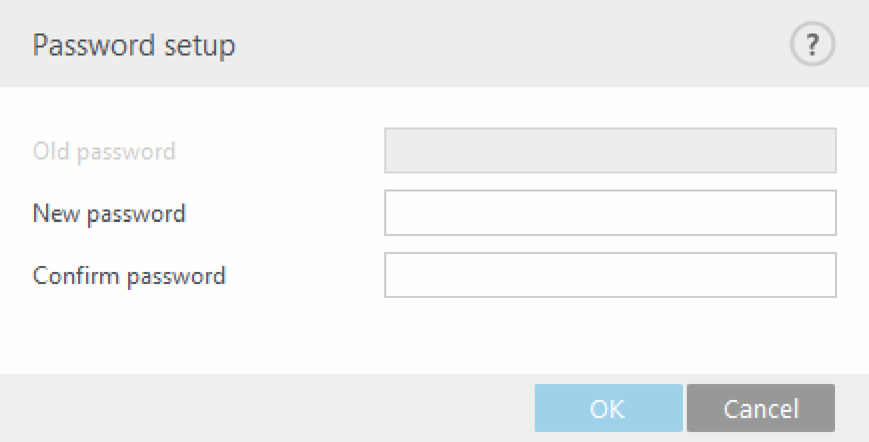
Advanced setup

Password protect settings ☒

Set password Set

Require full administrator rights for limited administrator accounts ✓

Enter a password in the **New password** and **Confirm password** fields and click **OK**. This password will be required for any future modifications to ESET Security for Microsoft SharePoint.



Password setup

Old password

New password

Confirm password

#### 8.7.2.2 Password

To avoid unauthorized modification, the setup parameters of ESET Security for Microsoft SharePoint can be password protected.

#### 8.7.2.3 Password setup

To protect the setup paramaters of ESET Security for Microsoft SharePoint in order to avoid unauthorized modification, a new password must be set. When you want to change an existing password, type your old password in the **Old password** field, enter your new password in the **New password** and **Confirm password** fields and then click **OK**. This password will be required for any future modifications to ESET Security for Microsoft SharePoint.

### 8.7.3 Help

When you press the **F1** key or click the **?** button, an online help window will open. This is the primary source of help content. However, there is also an offline copy of help that comes installed with the program. Offline help opens in cases such as when there is no connection to the Internet.

The latest version of Online help will automatically be displayed when you have a working internet connection.

### 8.7.4 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.

### 8.7.5 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 terminal` 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 terminal
```

If you want to find out what mode is currently in use, run the command `get ui ui gui-start-mode`.

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

### 8.7.6 Disabled messages and statuses

Confirmation messages - shows you a list of confirmation messages that you can select to display or not to display.

Application statuses settings - allows you to enable or disable display status in the **Monitoring** tab in main menu.

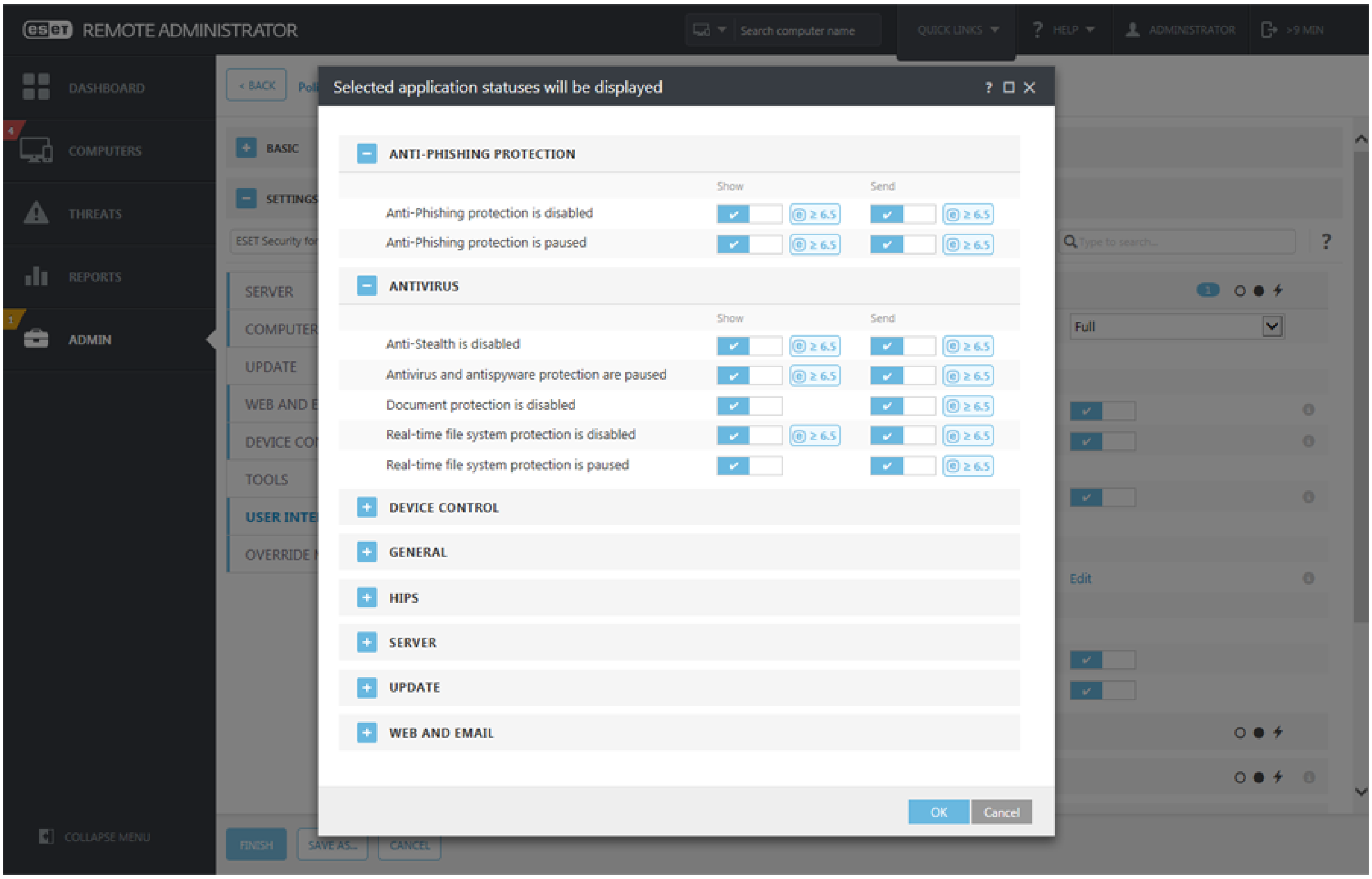
### 8.7.6.1 Confirmation messages

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

### 8.7.6.2 Application statuses settings

This dialog window lets you select or deselect which application statuses will be or will not be displayed. For example, when you pause Antivirus and antispyware protection that will result in a change of protection status which will appear in Monitoring page. An application status will also be displayed if your product is not activated or if your license has expired.

Application statuses can be managed via ESET Remote Administrator policies. Categories and statutes are shown in a list with two options **Show** and **Send** the status. Send column for application statuses is visible only in ESET Remote Administrator policy configuration. ESET Security for Microsoft SharePoint shows settings with lock icon. You can use Override mode to temporarily change Application statuses.



Selected application statuses will be displayed

**ANTI-PHISHING PROTECTION**

| | Show | | Send | |
|---|---|---|---|---|
| Anti-Phishing protection is disabled | ✓ | ≥ 6.5 | ✓ | ≥ 6.5 |
| Anti-Phishing protection is paused | ✓ | ≥ 6.5 | ✓ | ≥ 6.5 |

**ANTIVIRUS**

| | Show | | Send | |
|---|---|---|---|---|
| Anti-Stealth is disabled | ✓ | ≥ 6.5 | ✓ | ≥ 6.5 |
| Antivirus and antispyware protection are paused | ✓ | ≥ 6.5 | ✓ | ≥ 6.5 |
| Document protection is disabled | ✓ | | ✓ | ≥ 6.5 |
| Real-time file system protection is disabled | ✓ | ≥ 6.5 | ✓ | ≥ 6.5 |
| Real-time file system protection is paused | ✓ | | ✓ | ≥ 6.5 |

**DEVICE CONTROL**

**GENERAL**

**HIPS**

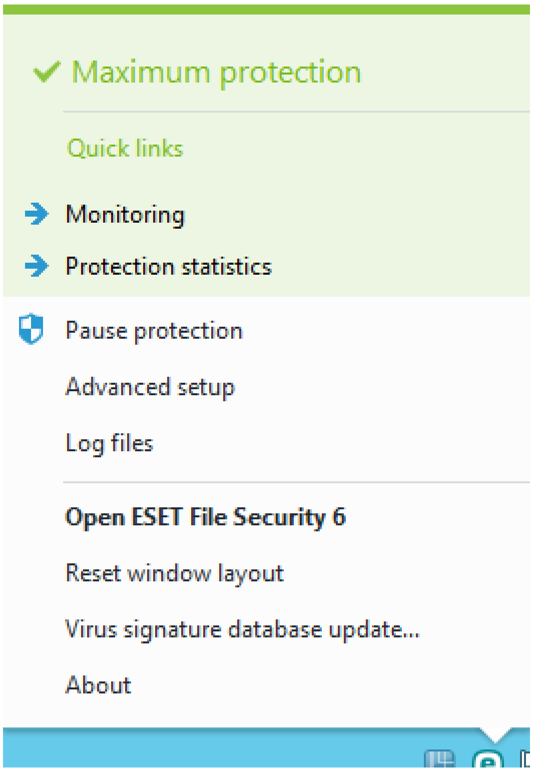
**SERVER**

**UPDATE**

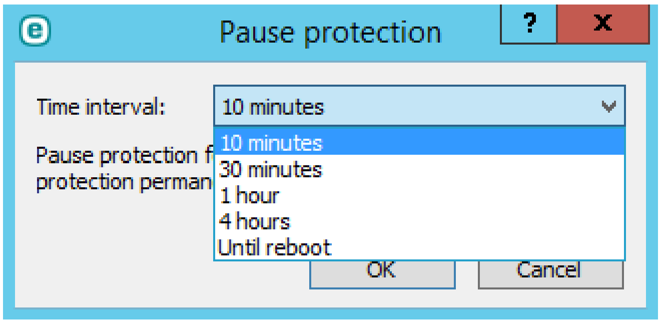
**WEB AND EMAIL**

### 8.7.7 System tray icon

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



**Pause protection** - Displays the confirmation dialog box that disables Antivirus and antispyware protection, which guards against attacks by controlling file, web and email communication.



The **Time interval** drop-down menu represents the period of time that Antivirus and antispyware protection will be disabled for.

**Advanced setup** - Select this option to enter the **Advanced setup**. You can also access **Advanced setup** by pressing the F5 key or navigating to **Setup** > **Advanced setup**.

**Log files** - Log files contain information about all important program events that have occurred and provide an overview of detected threats.

**Hide ESET Security for Microsoft SharePoint** - Hide the ESET Security for Microsoft SharePoint window from the screen.

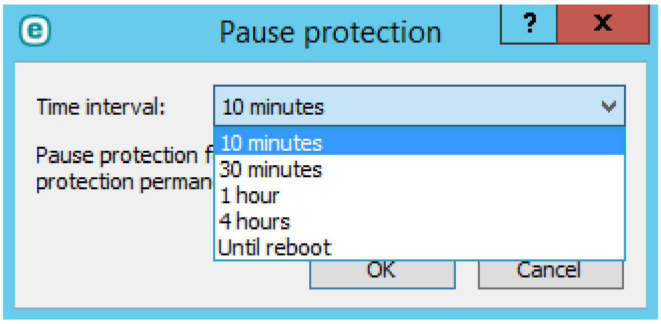
**Reset window layout** - Resets the ESET Security for Microsoft SharePoint window to its default size and position on the screen.

**Virus signature database update** - Starts updating the virus signature database to ensure your level of protection against malicious code.

**About** - Provides system information, details about the installed version of ESET 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.

### 8.7.7.1 Pause protection

Any time that you temporarily pause the Antivirus and antispyware protection sing the system tray icon ⓔ, the **Pause protection** dialog box will appear. This will disable malware-related protection for the selected time period (to disable protection permanently, you must use **Advanced setup**). Use caution, disabling protection can expose your system to threats.

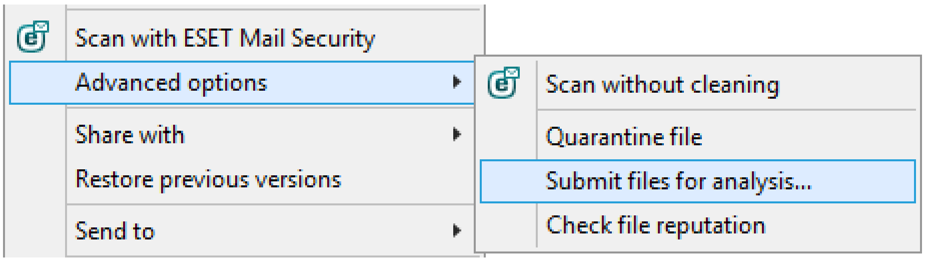


## 8.7.8 Context menu

The context menu is displayed after right-clicking an object (file). The menu lists all of the actions that you can perform on an object.

It is possible to integrate ESET Security for Microsoft SharePoint control elements into the context menu. Setup option for this functionality are available in the **Advanced setup** tree under **User Interface** > **User interface elements**.

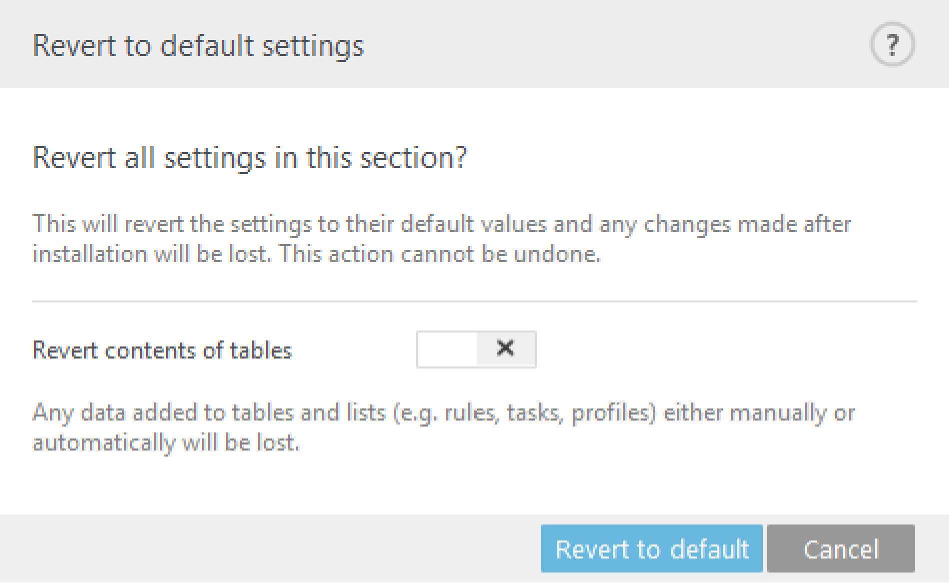
**Integrate into the context menu** - Integrate the ESET Security for Microsoft SharePoint control elements into the context menu.



## 8.8 Revert all settings in this section

Reverts module settings to the default settings defined by ESET. Please note, any changes that have been made will be lost after you click **Revert to default**.

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



Revert to default settings

Revert all settings in this section?

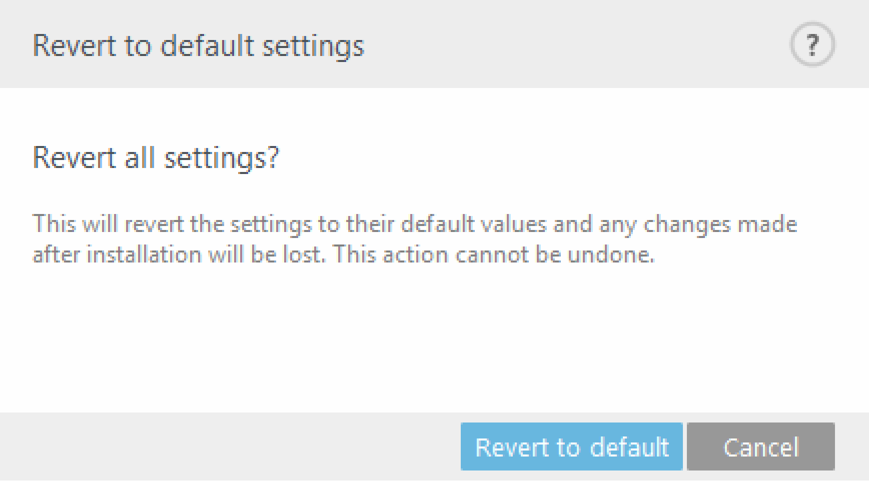
This will revert the settings to their default values and any changes made after installation will be lost. This action cannot be undone.

Revert contents of tables ☒

Any data added to tables and lists (e.g. rules, tasks, profiles) either manually or automatically will be lost.

## 8.9 Revert to default settings

All program settings, for all modules, will be reset to the status they would have had after a new installation.



Revert to default settings

Revert all settings?

This will revert the settings to their default values and any changes made after installation will be lost. This action cannot be undone.

## 8.10 Scheduler

**Scheduler** can be found in the **Tools** section of the main program window. Scheduler manages and launches scheduled tasks according to defined parameters.

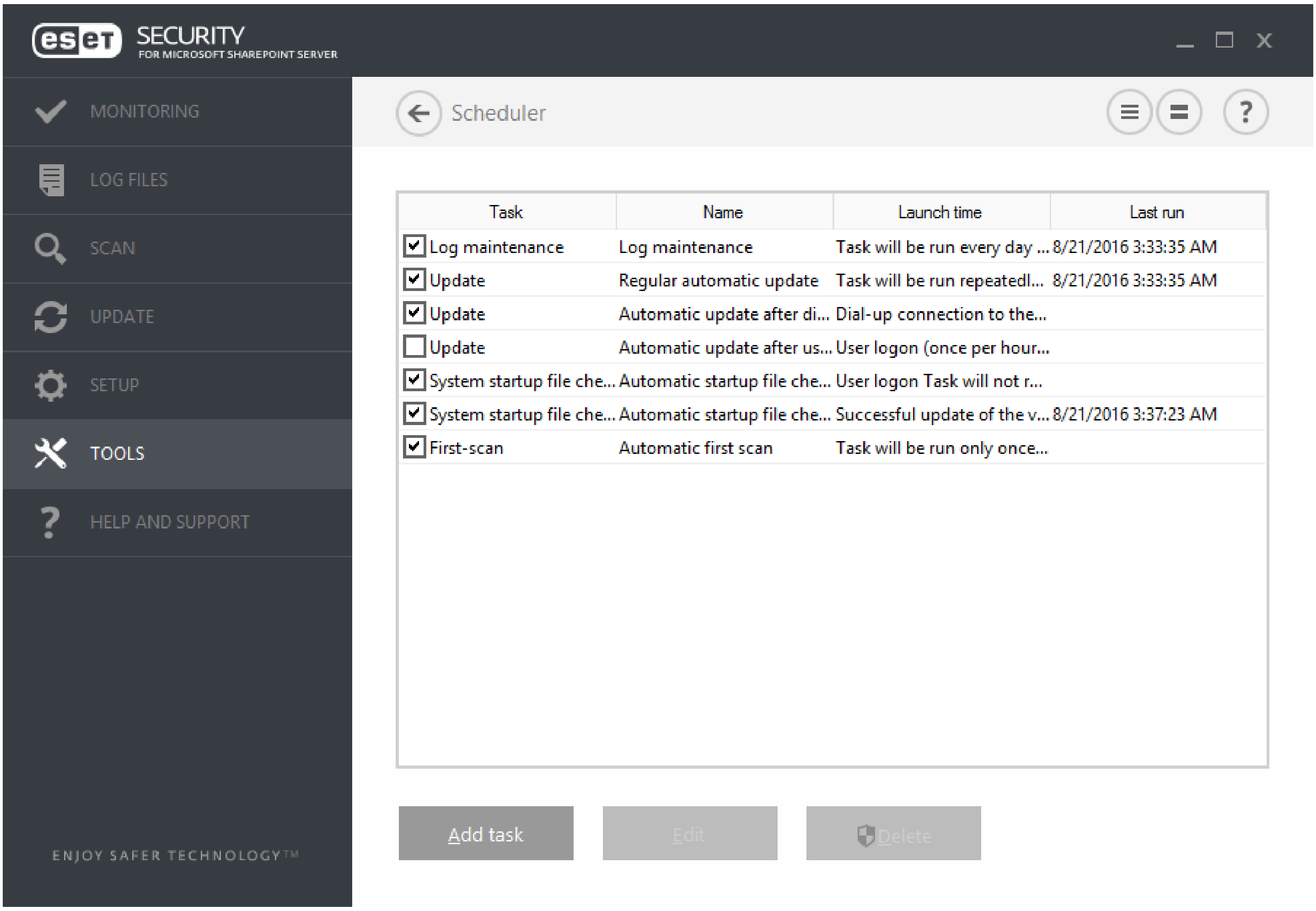
Scheduler contains a list of all scheduled tasks in the form of a table which shows their parameters such as **Task** type, task **Name**, **Launch time** and **Last run**. For more details, double-click a task to see its Scheduled task overview. After the installation, there is a set of predefined tasks. You can also create new scheduled tasks by clicking Add task.

When you right-click a task, you can choose an action to perform. Available actions are:

**Show task details**
**Run now**

**Add...**
**Edit...**
**Delete**

Use the check box next a task to activate/deactivate it. To edit the configuration of a scheduled task, right-click the task and click **Edit...** or select the task you want to modify and click **Edit**.



| Task | Name | Launch time | Last run |
|---|---|---|---|
| ☑ Log maintenance | Log maintenance | Task will be run every day ... | 8/21/2016 3:33:35 AM |
| ☑ Update | Regular automatic update | Task will be run repeatedl... | 8/21/2016 3:33:35 AM |
| ☑ Update | Automatic update after di... | Dial-up connection to the... | |
| ☐ Update | Automatic update after us... | User logon (once per hour... | |
| ☑ System startup file che... | Automatic startup file che... | User logon Task will not r... | |
| ☑ System startup file che... | Automatic startup file che... | Successful update of the v... | 8/21/2016 3:37:23 AM |
| ☑ First-scan | Automatic first scan | Task will be run only once... | |

The default (predefined) scheduled tasks are:

- **Log maintenance**
- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon** (this task is not activated be default)
- **Automatic startup file check** (after user logon)
- **Automatic startup file check** (after successful update of the virus signature database)
- **Automatic first scan**
- **Regular database scan**

### 8.10.1 Task details

Enter a **Task name** and select your desired **Task type** from the drop-down menu:

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

task.

- **Update** - schedules an update task to perform an update of virus signature database 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.

If you want to deactivate the task once it is created, click the switch next to **Enabled**. You can activate the task later using the check box in the Scheduler view. Click **Next** to proceed to the next step.

### 8.10.2 Task timing - Once

Specify the date and time for one-time **Task execution**.

### 8.10.3 Task timing

Select one of the following timing options to define when you want the **Scheduled task to run**:

- Once - the task will be performed only once at specified date and time.
- Repeatedly - the task will be performed at the specified time interval (in minutes).
- 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.
- Event triggered - the task will be performed after a specified event.

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

Click **Next** to proceed to the next step.

### 8.10.4 Task timing - Daily

Specify the time at which the task will be executed every day.

### 8.10.5 Task timing - Weekly

The task will run on the selected day and time.

### 8.10.6 Task timing - Event triggered

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

- **Every time the computer starts**
- **The first time the computer starts each day**
- **Dial-up connection to the Internet/VPN**
- **Successful update of the virus signature database**
- **Successful update of the program components**
- **User logon**
- **Threat detection**

When scheduling a task triggered by an event, you can specify the minimum interval between two completions of the task. For example, if you log on to your computer several times a day, choose 24 hours to perform the task only on the first logon of the day and then the next day.

### 8.10.7 Task details - Run application

This task schedules the execution of an external application.

- **Executable file** - choose an executable file from the directory tree, click **browse (...)** or enter the path manually.
- **Work folder** - define the external application's working directory. All temporary files of the selected **Executable file** will be created within this directory.
- **Parameters** - command line parameters for the application (optional).

Click **Finish** to create the task or apply changes, if you have modified an existing scheduled task.

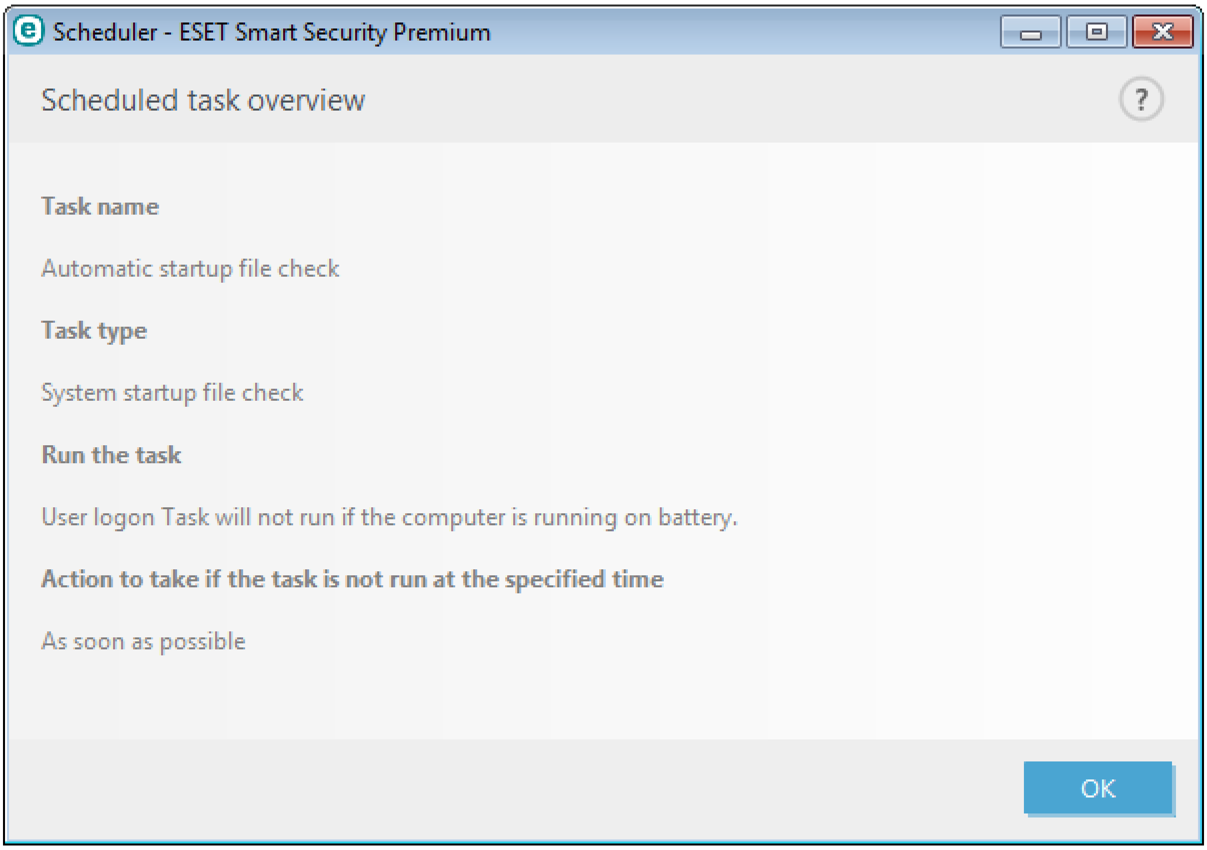
### 8.10.8 Skipped task

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

- **At the next scheduled time** - the task will be executed at the specified time (for example after 24 hours).
- **As soon as possible** - the task will run as soon as possible - when the actions that prevent the task from executing are no longer valid.
- **Immediately, if time since last run exceeds a specified value** - **Time since last run (hours)** - after you select this option, your task will be always repeated after the specified amount of time (in hours).

### 8.10.9 Scheduled task overview

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



Scheduled task overview

Task name

Automatic startup file check

Task type

System startup file check

Run the task

User logon Task will not run if the computer is running on battery.

Action to take if the task is not run at the specified time

As soon as possible

### 8.10.10 Update profiles

If you wish to update the program from two update servers, then it is necessary to create two different update profiles. If the first one fails to download update files, then the program automatically switches to the alternative one. This is suitable, for example, for notebooks which normally update from a local LAN update server, but their owners often connect to the Internet using other networks. So, if the first profile fails, the second one will automatically download update files from ESET's update servers.

You will find more information on update profiles in chapter Update.

## 8.11 Quarantine

Quarantining files

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

Restoring from Quarantine

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

NOTE

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

Submitting a file from the Quarantine

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

### 8.11.1 Quarantining files

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

### 8.11.2 Restoring from Quarantine

Quarantined files can also be restored to their original location. To restore a quarantined file, right-click it in the Quarantine window and select **Restore** from the context menu. If a file is marked as a potentially unwanted application, **Restore and exclude from scanning** will also be available. The context menu also contains the **Restore to...** option, which allows you to restore a file to a location other than the one from which it was deleted.

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

NOTE

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

### 8.11.3 Submitting file from Quarantine

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

## 8.12 Operating system updates

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.

Click **Run system update** to start downloading and installing operating system updates.

Right-click any update row and click **Show information** to display a pop-up window with additional info.

# 9. Glossary

The glossary contains many of the technical terms about threats and internet security.

Choose category (or see a Virus Radar Glossary online):

- Types of infiltration
- Email

## 9.1 Types of infiltration

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

- Viruses
- Worms
- Trojan horses
- Rootkits
- Adware
- Spyware
- Packers
- Exploit Blocker
- Advanced Memory Scanner
- Potentially unsafe applications
- Potentially unwanted applications

### 9.1.1 Viruses

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

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

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage - they only serve to annoy the user and demonstrate the technical skills of their authors.

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

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

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

### 9.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves - they are not dependent on host files (or boot sectors). Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes of their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a “means of transport“ for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

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

### 9.1.3 Trojan horses

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

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

- **Downloader** - A malicious program with the ability to download other infiltrations from the Internet.
- **Dropper** - A type of trojan horse designed to drop other types of malware onto compromised computers.
- **Backdoor** - An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it.
- **Keylogger** - (keystroke logger) - A program which records each keystroke that a user types and sends the information to remote attackers.
- **Dialer** - Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.

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

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

### 9.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data, etc. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1) When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
2) When they are hidden from the usual testing. ESET Security for Microsoft SharePoint users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

### 9.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous - users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry. If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

### 9.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user‘s contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program‘s installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory - they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

### 9.1.7 Packers

A packer is a runtime self-extracting executable that combines several kinds of malware into a single package.

The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

### 9.1.8 Exploit Blocker

Exploit Blocker is designed to fortify commonly exploited applications such as web browsers, PDF readers, email clients or MS Office components. It monitors behavior of processes for suspicious activity that might indicate an exploit. It adds another layer of protection, one step closer to attackers, by using a completely different technology compared to techniques focusing on detection of malicious files themselves.

When Exploit Blocker identifies a  suspicious process, it can stop the process immediately and record data about the threat, which is then sent to the ESET LiveGrid cloud system. This data is processed by the ESET Threat Lab and used to better protect all users from unknown threats and zero-day attacks (newly released malware for which there is no pre-configured remedy).

### 9.1.9 Advanced Memory Scanner

Advanced Memory Scanner works in combination with Exploit Blocker to provide better protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation and/or encryption. In cases where ordinary emulation or heuristics might not detect a threat, the Advanced Memory Scanner is able to identify suspicious behavior and scan threats when they reveal themselves in system memory. This solution is effective against even heavily obfuscated malware. Unlike Exploit Blocker, this is a post-execution method, which means that there is a risk that some malicious activity could have been performed prior to its detecting a threat. However in the case that other detection techniques have failed, it offers an additional layer of security.

### 9.1.10 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET Security for Microsoft SharePoint provides the option to detect such threats.

**Potentially unsafe applications** is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

### 9.1.11 Potentially unwanted applications

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

- New windows you haven’t seen previously (pop-ups, ads)
- Activating and running of hidden processes
- Increased usage of system resources
- Changes in search results
- Application communicates with remote servers

When a PUA is detected, you will be able to decide which action to take:

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