ESET Log Collector

User guide

[Click here to display the online version of this document]

ESET Log Collector was developed by ESET, spol. s r.o.

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

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

REV. 3/19/2023

Introduction

The purpose of the ESET Log Collector application is to collect specific data, such as configuration and logs, from a machine of interest in order to facilitate a collection of the information from the customer's machine during a support case resolution. You can specify what information to collect from the predefined list of artifacts, maximum age of log records collected, format of the collected ESET logs and the name of the output ZIP file that will contain all collected files and information. If you run ESET Log Collector on a machine that does not have an ESET security product installed, only Windows event logs and running processes dumps can be collected.

ESET Log Collector collects selected information automatically from your system in order to help resolve issues quicker. When you have a case opened with ESET Technical Support, you may be asked to provide logs from your computer. ESET Log Collector will make it easy for you to collect the needed information.

DOWNLOAD ESET LOG COLLECTOR

> **NOTE**
> The ESET Log Collector is distributed as a 32-bit application. To ensure its full operation on a 64-bit system, it contains a 64-bit executable of ESET Log Collector embedded as a resource, which is extracted into a *Temp* directory and executed when a 64-bit system is detected.

You can use ESET Log Collector in two modes:

- Graphical user interface (GUI)
- Command line interface (CLI) (since version 1.8). When no command line parameters are specified, the ESET Log Collector will start in the GUI mode.

ESET product's logs are collected either as **original binary files** or **filtered binary files** (default is filtered binary files) when the ESET Log Collector is operated using a GUI. In the case of a filtered binary export, you can select the maximum age of exported records. Maximum number of exported records is 1 million per log file.

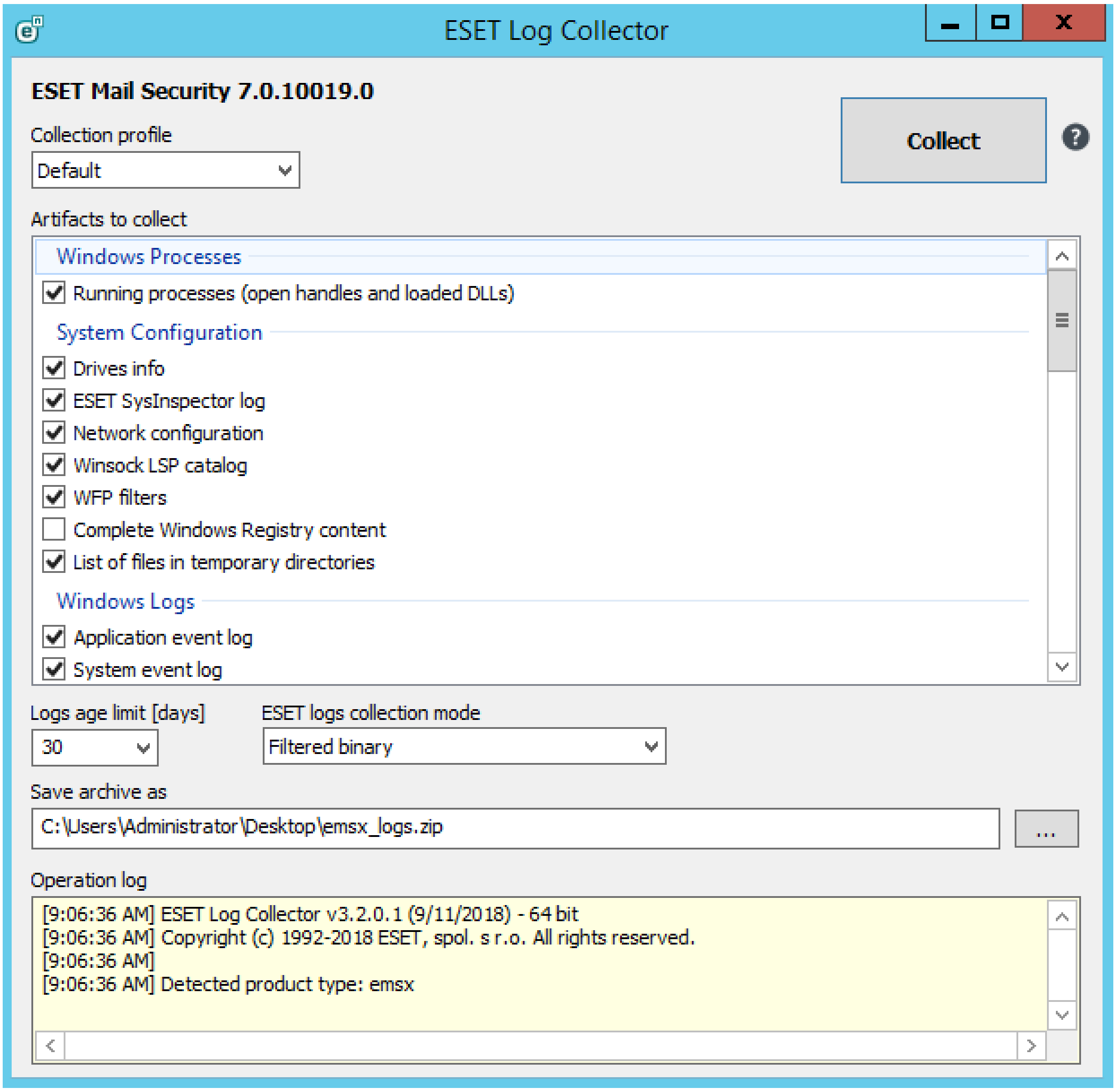
> **NOTE**
> An additional feature of ESET Log Collector is conversion of collected ESET binary log files (`.dat`) to XML or text file format. However, you can convert collected ESET binary log using ESET Log Collector Command line interface (CLI) only.

Help

To access the latest version of Online Help, press the **F1** key or click the **?** button.

ESET Log Collector User interface

After you have downloaded ESET Log Collector from the ESET website, launch the ESET Log Collector. Once you accept the End-User License Agreement (EULA) ESET Log Collector will open. If you choose not to accept the terms in the End-User License Agreement (EULA), click **Cancel** and ESET Log Collector will not open.



ESET Mail Security 7.0.10019.0

Collection profile: Default

Artifacts to collect

Windows Processes

☑ Running processes (open handles and loaded DLLs)

System Configuration

☑ Drives info
☑ ESET SysInspector log
☑ Network configuration
☑ Winsock LSP catalog
☑ WFP filters
☐ Complete Windows Registry content
☑ List of files in temporary directories

Windows Logs

☑ Application event log
☑ System event log

Logs age limit [days]: 30

ESET logs collection mode: Filtered binary

Save archive as: C:\Users\Administrator\Desktop\emsx_logs.zip

Operation log

```
[9:06:36 AM] ESET Log Collector v3.2.0.1 (9/11/2018) - 64 bit
[9:06:36 AM] Copyright (c) 1992-2018 ESET, spol. s r.o. All rights reserved.
[9:06:36 AM]
[9:06:36 AM] Detected product type: emsx
```

You can choose a **Collection profile** or make your own artifact selection. Collection profile is a defined set of artifacts:

- **Default** - Default profile with most of the artifacts selected. It is used for generic support cases. (See the List of artifacts section for detailed list of selected artifacts).
- **Threat detection** - Overlaps with the Default profile in many artifacts, but in contrast to the Default profile, the Threat detection profile focuses on collecting artifacts that helps with resolution of malware detection-related support cases. (See the List of artifacts section for detailed list of selected artifacts).
- **All** - Selects all available artifacts.
- **None** - Deselects all artifacts and allows you to select the appropriate check boxes for the logs that you want to collect.
- **Custom** - This collection profile is switched to automatically when you make a change to a previously chosen profile and your current combination of selected artifacts does not fit any of the above mentioned profiles.

NOTE

The list of displayed artifacts that can be collected changes depending on the detected type of ESET security product installed on your system, your system configuration, as well as other software such as Microsoft Server applications. Only relevant artifacts are available.

Select the **Logs age limit [days]** and ESET logs collection mode (default option is **Filtered binary**).

ESET logs collection mode:

- **Filtered binary** - Records are filtered by the number of days specified by **Logs age limit [days]**, which means that only records for the last number of days will be collected.
- **Original binary from disk** - Copies ESET binary log files ignoring **Logs age limit [days]** value for ESET logs in order to collect all records regardless of their age. However, age limit still applies to non-ESET logs, such as Windows Event Logs, Microsoft SharePoint logs or IBM Domino logs.

You can specify the location where you want to save archive files and then click **Save**. The archive file name is already predefined. Click **Collect**. Application's operation can be interrupted anytime during the processing by pressing the same button – button's caption changes to **Cancel** during processing. Success or failure is indicated by a pop-up message. In case of failure, the log panel contains additional error information.

During the collection, you can view the operation log window at the bottom to see what operation is currently in progress. When collection is finished, all the collected and archived data will be displayed. This means that collection was successful and the archive file (for example, *emsx_logs.zip, ees_logs.zip or eea_logs.zip*) has been saved in the specified location. (See the List of artifacts section for detailed information).

List of artifacts / Collected files

This section describes the files contained in the resulting *.zip* file. Description is divided into subsections based on the information type (files and artifacts).

Location / File name	Description
metadata.txt	Contains the date of the .zip archive creation, ESET Log Collector version, ESET product version and basic licensing information.
collector_log.txt	A copy of the log file from the GUI, contains data up to the point when the .zip file is being created.

Windows Processes

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
Running processes (open handles and loaded DLLs)	⍰	⍰	*Windows\Processes\Processes.txt*	Text file containing a list of running processes on the machine. For each process, the following items are printed: oPID oParent PID oNumber of threads oNumber of open handles grouped by type oLoaded modules oUser account it is running under oMemory usage oTimestamp of start oKernel and user time oI/O statistics oCommand line
Running processes (open handles and loaded DLLs)	⍰	⍰	*Windows\ProcessesTree.txt*	Text file containing a tree of running processes on the machine. For each process following items are printed: oPID oUser account it is running under oTimestamp of start oCommand line

Windows Logs

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		

Windows Logs

Application event log	⍰	⍰	*Windows\Logs\Application.xml*	XML containing Windows Application event logs in a custom XML format suitable for viewing in Microsoft Excel. Only messages from the last 30 days are included. All string references are translated on the source machine so that the viewing machine does not need access to referenced resource DLLs.
System event log	⍰	⍰	*Windows\Logs\System.xml*	XML containing Windows System event logs in a custom XML format suitable for viewing in Microsoft Excel. Only messages from the last 30 days are included. All string references are translated on the source machine so that the viewing machine does not need access to referenced resource DLLs.
Terminal services - LSM operational event log*	⍰	⍰	*Windows\Logs\LocalSessionManager-Operational.evtx*	Windows XML Event Log. It contains information about RDP sessions. A user can specify maximum age of exported records.
Drivers install logs	⍰	⍰	*Windows\Logs\catroot2_dberr.txt*	Contains information about catalogs that have been added to "catstore" during driver installation.
SetupAPI logs*	⍰	⍰	*Windows\Logs\SetupAPI\setupapi*.log*	Device and application installation text logs.

**Windows Vista and newer*

System Configuration

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
Drives info	⍰	⍰	*Windows/drives.txt*	Collected text file containing information about disk drives.
Devices info	⍰	⍰	*Windows/devices/*.txt*	Collected multiple text files containing classes and interfaces information about devices.
Network configuration	⍰	⍰	*Config\network.txt*	Collected text file containing network configuration. (Result of executing `ipconfig /all`)
ESET SysInspector log	⍰	⍰	*Config\SysInspector.xml*	SysInspector log in the XML format.
Winsock LSP catalog	⍰	⍰	*Config/WinsockLSP.txt*	Collect the output of netsh winsock show catalog command.
WFP filters*	⍰	⍰	*Config\WFPFilters.xml*	Collected WFP filters configuration in the XML format.
Complete Windows Registry content	⍰	⍰	*Windows\Registry\**	Collected multiple binary files containing Windows Registry data.
List of files in temporary directories	⍰	⍰	*Windows\TmpDirs\*.txt*	Collected multiple text files with content of system's user temp directories, *%windir%/temp*, *%TEMP%* and *%TMP%* directories.

**Windows 7 and newer*

ESET Installer

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
ESET Installer logs	⍰	⍰	ESET\Installer\*.log	Installation logs that were created during the installation of ESET NOD32 Antivirus and ESET Smart Security 10 Premium products.

ESET Remote Administrator logs applies to ESET Security Management Center as well.

ESET Security Management Center (ESMC) and ESET Remote Administrator (ERA)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
ESMC/ERA Server logs	⍰	⍰	*ERA\Server\Logs\RemoteAdministratorServerDiagnostic<datetime>.zip*	Create Server product logs in the ZIP archive. It contains trace, status and last-error logs.
ESMC/ERA Agent logs	⍰	⍰	*ERA\Agent\Logs\RemoteAdministratorAgentDiagnostic<datetime>.zip*	Create Agent product logs in the ZIP archive. It contains trace, status and last-error logs.
ESMC/ERA process information and dumps*	⍰	⍰	*ERA\Server\Process and old dump\RemoteAdministratorServerDiagnostic<datetime>.zip*	Server process dump(s).
ESMC/ERA process information and dumps*	⍰	⍰	*ERA\Agent\Process and old dump\RemoteAdministratorAgentDiagnostic<datetime>.zip*	Agent process dump(s).
ESMC/ERA configuration	⍰	⍰	*ERA\Server\Config\RemoteAdministratorServerDiagnostic<datetime>.zip*	Server configuration and application information files in the ZIP archive.
ESMC/ERA configuration	⍰	⍰	*ERA\Agent\Config\RemoteAdministratorAgentDiagnostic<datetime>.zip*	Agent configuration and application information files in the ZIP archive.
ESMC/ERA Rogue Detection Sensor logs	⍰	⍰	*ERA\RD Sensor\Rogue Detection SensorDiagnostic<datetime>.zip*	A ZIP containing RD Sensor trace log, last-error log, status log, configuration, dump(s) and general information files.

ESET Security Management Center (ESMC) and ESET Remote Administrator (ERA)

ESMC/ERA MDMCore logs	⍰	⍰	*ERA\MDMCore\RemoteAdministratorMDMCoreDiagnostic<datetime>.zip*	A ZIP containing MDMCore trace log, last-error log, status log, dump(s) and general information files.
ESMC/ERA Proxy logs	⍰	⍰	*ERA\Proxy\RemoteAdministratorProxyDiagnostic<datetime>.zip*	A ZIP containing ERA Proxy trace log, last-error log, status log, configuration, dump(s) and general information files.

**ESMC/ERA Server or ESMC/ERA Agent*

ESET Configuration

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
ESET product configuration	⍰	⍰	*info.xml*	Informational XML that details the ESET product installed on a system. It contains basic system information, installed product information and a list of product modules.
ESET product configuration	⍰	⍰	*versions.csv*	Exported when the generation of *info.xml* has failed for any reason. Contains installed product information.
ESET product configuration	⍰	⍰	*features_state.txt*	Contains information about ESET product features and their states (Active, Inactive, Not integrated). The file is always collected and is not tied to any selectable artifact.
ESET product configuration	⍰	⍰	*Configuration\product_conf.xml*	Create XML with exported product configuration.
ESET data and install directory file list	⍰	⍰	*ESET\Config\data_dir_list.txt*	Create text file containing list of files in *ESET AppData* directory and all their subdirectories.

ESET Configuration

ESET data and install directory file list	⍰	⍰	*ESET\Config\install_dir_list.txt*	Create text file containing list of files in *ESET Install* directory and all their subdirectories.
ESET drivers	⍰	⍰	*ESET\Config\drivers.txt*	Collect information about installed ESET drivers.
ESET Personal firewall configuration	⍰	⍰	*ESET\Config\EpfwUser.dat*	Copy file with ESET Personal firewall configuration.
ESET Registry key content	⍰	⍰	*ESET\Config\ESET.reg*	Contains a registry key content of *HKLM\SOFTWARE\ESET*
Winsock LSP catalog	⍰	⍰	*Config/WinsockLSP.txt*	Collect the output of netsh winsock show catalog command.
Last applied policy	⍰	⍰	*ESET\Config\lastPolicy.dat*	The policy applied by ERA.

Quarantine

Artifact name	**Collection profile**		**Location / File name**	**Description**
	Default	**Threat detection**		
Info about quarantined files	⍰	⍰	*ESET\Quarantine\quar_info.txt*	Create text file with a list of quarantined objects.
Quarantined files	⍰	⍰	*ESET\Quarantine\<username>*	Collect NDF and NQF files from ESET Security product.

ESET Logs

Artifact name	**Collection profile**		**Location / File name**	**Description**
	Default	**Threat detection**		
ESET Events log	⍰	⍰	*ESET\Logs\Common\warnlog.dat*	ESET Product event log in binary format.
ESET Detected threats log	⍰	⍰	*ESET\Logs\Common\virlog.dat*	ESET Detected threats log in binary format.
ESET Computer scan logs	⍰	⍰	*ESET\Logs\Common\eScan\*.dat*	ESET Computer scan log(s) in binary format.
ESET HIPS log*	⍰	⍰	*ESET\Logs\Common\hipslog.dat*	ESET HIPS log in binary format.
ESET Parental control logs*	⍰	⍰	*ESET\Logs\Common\parentallog.dat*	ESET Parental control log in binary format.
ESET Device control log*	⍰	⍰	*ESET\Logs\Common\devctrllog.dat*	ESET Device control log in binary format.

ESET Logs

ESET Webcam protection log*	⍰	⍰	*ESET\Logs\Common\webcamlog.dat*	ESET Webcam protection log in binary format.
ESET On-demand server database scan logs	⍰	⍰	*ESET\Logs\Common\ServerOnDemand\*.dat*	ESET server On-demand log(s) in binary format.
ESET Hyper-V server scan logs	⍰	⍰	*ESET\Logs\Common\HyperVOnDemand\*.dat*	ESET Hyper-V server scan log(s) in binary format.
MS OneDrive scan logs	⍰	⍰	*ESET\Logs\Common\O365OnDemand\*.dat*	MS OneDrive scan log(s) in binary format.
ESET Blocked files log	⍰	⍰	*ESET\Logs\Common\blocked.dat*	ESET Blocked files log(s) in binary format.
ESET Sent files log	⍰	⍰	*ESET\Logs\Common\sent.dat*	ESET Sent files log(s) in binary format.

**Option is displayed only when the file exists.*

ESET Network Logs

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
ESET Network protection log*	⍰	⍰	*ESET\Logs\Net\epfwlog.dat*	ESET Network protection log in binary format.
ESET Filtered websites log*	⍰	⍰	*ESET\Logs\Net\urllog.dat*	ESET Websites filter log in binary format.
ESET Web control log*	⍰	⍰	*ESET\Logs\Net\webctllog.dat*	ESET Web control log in binary format.
ESET pcap logs	⍰	⍰	*ESET\Logs\Net\EsetProxy*.pcapng*	Copy ESET pcap logs.

**Option is displayed only when the file exists.*

ESET Diagnostics

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
Local cache database	⍰	⍰	*ESET\Diagnostics\local.db*	ESET scanned files database.
General product diagnostics logs	⍰	⍰	*ESET\Diagnostics\*.**	Files (mini-dumps) from ESET diagnostics folder.

ESET Diagnostics

ECP diagnostic logs	⍰	⍰	*ESET\Diagnostics\ECP\*.xml*	ESET Communication Protocol diagnostic logs are generated in case of problems with product activation and communication with activation servers.

ESET Secure Authentication

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
ESA logs	⍰	⍰	*ESA*.log*	Exported log(s) from the ESET Secure Authentication.

ESET Email Logs (ESET Mail Security for Exchange, ESET Mail Security for Domino)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
ESET Spam log	⍰	⍰	*ESET\Logs\Email\spamlog.dat*	ESET Spam log in binary format.
ESET SMTP protection log	⍰	⍰	*ESET\Logs\Email\smtpprot.dat*	ESET SMTP protection log in binary format.
ESET mail server protection log	⍰	⍰	*ESET\Logs\Email\mailserver.dat*	ESET Mail server protection log in binary format.
ESET diagnostic e-mail processing logs	⍰	⍰	*ESET\Logs\Email\MailServer\*.dat*	ESET diagnostic e-mail processing logs in binary format, direct copy from disk.
ESET Spam log*	⍰	⍰	*ESET\Logs\Email\spamlog.dat*	ESET Spam log in binary format.
ESET Antispam configuration and diagnostic logs	⍰	⍰	*ESET\Logs\Email\Antispam\antispam.*.log*	Copy ESET Antispam configuration and diagnostic logs.
ESET Antispam configuration and diagnostic logs	⍰	⍰	*ESET\Config\Antispam\*.**	Copy ESET Antispam configuration and diagnostic logs.

**Option is displayed only when the file exists.*

ESET SharePoint logs (ESET Security for SharePoint)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
ESET SHPIO.log	⍰	⍰	*ESET\Log\ESHP\SHPIO.log*	ESET Diagnostic log from the *SHPIO.exe* utility.

Product specific logs - options are available for specific product.

Domino (ESET Mail Security for Domino)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
Domino IBM_TECHNICAL_SUPPORT logs + notes.ini	⍰	⍰	*LotusDomino\Log\notes.ini*	IBM Domino configuration file.
Domino IBM_TECHNICAL_SUPPORT logs + notes.ini	⍰	⍰	*LotusDomino\Log\IBM_TECHNICAL_SUPPORT\*.**	IBM Domino logs, not older than 30 days.

MS SharePoint (ESET Security for SharePoint)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
MS SharePoint logs	⍰	⍰	*SharePoint\Logs\*.log*	MS SharePoint logs, not older than 30 days.
SharePoint Registry key content	⍰	⍰	*SharePoint\WebServerExt.reg*	Contains a registry key content of *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions*. Available only when ESET Security for SharePoint is installed.

MS Exchange (ESET Mail Security for Exchange)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
MS Exchange transport agents registration	⍰	⍰	*Exchange\agents.config*	MS Exchange transport agents registration config file. For Microsoft Exchange Server 2007 and newer.

MS Exchange (ESET Mail Security for Exchange)

MS Exchange transport agents registration	⍰	⍰	*Exchange\sinks_list.txt*	MS Exchange event sinks registration dump. For Microsoft Exchange Server 2000 and 2003.
MS Exchange EWS logs	⍰	⍰	*Exchange\EWS\*.log*	Collecting of EWS Exchange Server logs.

Kerio Connect (ESET Security for Kerio)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
Kerio Connect configuration	⍰	⍰	*Kerio\Connect\mailserver.cfg*	Kerio Connect configuration file.
Kerio Connect logs	⍰	⍰	*Kerio\Connect\Logs\{mail,error,security,debug,warning}.log*	Selected Kerio Connect log files.

Kerio Control (ESET Security for Kerio)

Artifact name	Collection profile		Location / File name	Description
	Default	Threat detection		
Kerio Control configuration	⍰	⍰	*Kerio\Connect\winroute.cfg*	Kerio Control configuration file.
Kerio Control logs	⍰	⍰	*Kerio\Connect\Logs\{alert,error,security,debug,warning}.log*	Selected Kerio Control log files.

ESET Log Collector Command line

Command line interface is a feature that allows you to use ESET Log Collector without the GUI. For example, on Server Core or Nano Server installation, also if you require or simply wish to use command line instead of the GUI. There is also an extra command line only function available that converts the ESET binary log file to an XML format or to a text file.

Command line help - Run `start /wait ESETLogCollector_ENU.exe /?` to display the syntax help. It also lists available targets (artifacts) that can be collected. Contents of the list depend on the detected type of ESET security product installed on the system you are running ESET Log Collector on. Only relevant artifacts are available.

NOTE
We recommend you use `start /wait` prefix when executing any command because the ESET Log Collector is primarily a GUI tool and Windows command-line interpreter (shell) does not wait for the executable to terminate and instead returns immediately and displays a new prompt. When you use `start /wait` prefix, you will make Windows shell wait for ESET Log Collector's termination.

If you are running ESET Log Collector for the first time, ESET Log Collector requires the End-User License Agreement (EULA) to be accepted. To accept EULA, run the very first command with `/accepteula` parameter. Any subsequent commands will run without the need of the `/accepteula` parameter. If you choose not to accept the terms in the End-User License Agreement (EULA) and do not use the `/accepteula` parameter, your command will not be executed. Also, the `/accepteula` parameter must be specified as the first parameter, for example: `start /wait ESETLogCollector_ENU.exe /accepteula /age:90 /otype:fbin /targets:prodcnf,qinfo,warn,threat,ondem collected_eset_logs.zip`

Usage:

`[start /wait] ESETLogCollector.exe [options] <out_zip_file>` - collects logs according to specified options and creates output archive file in a ZIP format.

`[start /wait] ESETLogCollector.exe /Bin2XML [/All] <eset_binary_log> <output_xml_file>` - converts collected ESET binary log file (`.dat`) to an XML file.

`[start /wait] ESETLogCollector.exe /Bin2Txt [/All] <eset_binary_log> <output_txt_file>` - converts collected ESET binary log file (`.dat`) to a text file.

Options:

`/Age:<days>` - Maximum age of collected log records in days. Value range is 0-999, 0 means infinite, default is 30.

`/OType:<xml|fbin|obin>` - Collection format for ESET logs:

`xml` - Filtered XML
`fbin` - Filtered binary (default)
`obin` - Original binary from disk

`/All` - Translate also records marked as deleted. This parameter is applicable only when converting collected ESET binary log file to XML or TXT.

`/Targets:<id1>[,<id2>...]` - List of artifacts to collect. If not specified, a default set is collected. Special value 'all' means all targets.

`/NoTargets:<id1>[,<id2>...]` - List of artifacts to skip. This list is applied after the Targets list.

`/Profile:<default|threat|all>` - Collection profile is a defined set of targets:

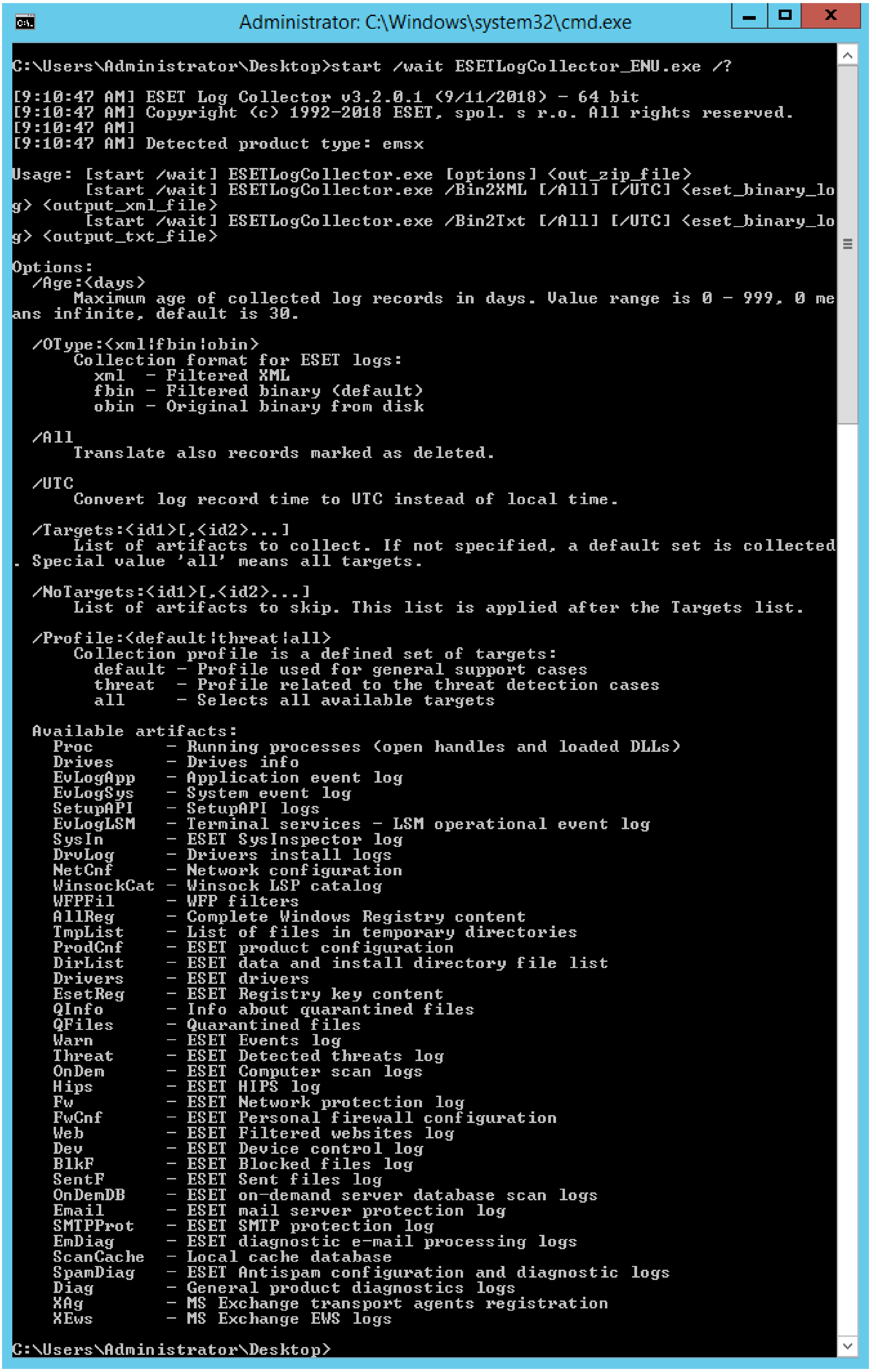
`Default` - Profile used for general support cases
`Threat` - Profile related to the threat detection cases
`All` - Selects all available targets

ℹ **NOTE**

When you choose **Filtered XML** or **Filtered binary** collection format, the filtering means that only records for the last number of days will be collected (specified by `/Age:<days>` parameter). If you choose **Original binary from disk**, parameter `/Age:<days>` will be ignored for all ESET logs. For other logs, such as Windows Event Logs, Microsoft SharePoint logs or IBM Domino logs, parameter `/Age:<days>` will be applied so that you can limit non-ESET log records to a specified number of days and have original ESET binary files collected (copied) without age limit.

ℹ **NOTE**

Parameter `/All` allows for conversion of all log records, including those that were deleted via GUI but are present in the original binary file marked as deleted (log records not visible in the GUI).



```
C:\Users\Administrator\Desktop>start /wait ESETLogCollector_ENU.exe /?

[9:10:47 AM] ESET Log Collector v3.2.0.1 (9/11/2018) - 64 bit
[9:10:47 AM] Copyright (c) 1992-2018 ESET, spol. s r.o. All rights reserved.
[9:10:47 AM]
[9:10:47 AM] Detected product type: emsx

Usage: [start /wait] ESETLogCollector.exe [options] <out_zip_file>
       [start /wait] ESETLogCollector.exe /Bin2XML [/All] [/UTC] <eset_binary_lo
g> <output_xml_file>
       [start /wait] ESETLogCollector.exe /Bin2Txt [/All] [/UTC] <eset_binary_lo
g> <output_txt_file>

Options:
  /Age:<days>
      Maximum age of collected log records in days. Value range is 0 - 999, 0 me
ans infinite, default is 30.

  /OType:<xml|fbin|obin>
      Collection format for ESET logs:
        xml  - Filtered XML
        fbin - Filtered binary (default)
        obin - Original binary from disk

  /All
      Translate also records marked as deleted.

  /UTC
      Convert log record time to UTC instead of local time.

  /Targets:<id1>[,<id2>...]
      List of artifacts to collect. If not specified, a default set is collected
. Special value 'all' means all targets.

  /NoTargets:<id1>[,<id2>...]
      List of artifacts to skip. This list is applied after the Targets list.

  /Profile:<default|threat|all>
      Collection profile is a defined set of targets:
        default - Profile used for general support cases
        threat  - Profile related to the threat detection cases
        all     - Selects all available targets

  Available artifacts:
    Proc        - Running processes (open handles and loaded DLLs)
    Drives      - Drives info
    EvLogApp    - Application event log
    EvLogSys    - System event log
    SetupAPI    - SetupAPI logs
    EvLogLSM    - Terminal services - LSM operational event log
    SysIn       - ESET SysInspector log
    DrvLog      - Drivers install logs
    NetCnf      - Network configuration
    WinsockCat  - Winsock LSP catalog
    WFPFil      - WFP filters
    AllReg      - Complete Windows Registry content
    TmpList     - List of files in temporary directories
    ProdCnf     - ESET product configuration
    DirList     - ESET data and install directory file list
    Drivers     - ESET drivers
    EsetReg     - ESET Registry key content
    QInfo       - Info about quarantined files
    QFiles      - Quarantined files
    Warn        - ESET Events log
    Threat      - ESET Detected threats log
    OnDem       - ESET Computer scan logs
    Hips        - ESET HIPS log
    Fw          - ESET Network protection log
    FwCnf       - ESET Personal firewall configuration
    Web         - ESET Filtered websites log
    Dev         - ESET Device control log
    BlkF        - ESET Blocked files log
    SentF       - ESET Sent files log
    OnDemDB     - ESET on-demand server database scan logs
    Email       - ESET mail server protection log
    SMTPProt    - ESET SMTP protection log
    EmDiag      - ESET diagnostic e-mail processing logs
    ScanCache   - Local cache database
    SpamDiag    - ESET Antispam configuration and diagnostic logs
    Diag        - General product diagnostics logs
    XAg         - MS Exchange transport agents registration
    XEws        - MS Exchange EWS logs

C:\Users\Administrator\Desktop>
```

EXAMPLE

This example command collects ESET product configuration, Info about quarantined files, ESET Events log, ESET Detected threats log and ESET Computer scan logs in Filtered binary collection mode with records for last 90 days:

```
start /wait ESETLogCollector_ENU.exe /age:90 /otype:fbin
/targets:prodcnf,qinfo,warn,threat,ondem collected_eset_logs.zip
```

EXAMPLE

This example command collects Running processes, System event log, ESET SysInspector log, ESET product configuration, ESET Events log and General product diagnostics logs in Original binary from disk collection mode:

```
start /wait ESETLogCollector_ENU.exe /otype:obin
/targets:proc,evlogsys,sysin,prodcnf,warn,diag collected_diag_logs.zip
```

EXAMPLE

This example command collects ERA Agent logs, ERA Server logs, ERA configuration and ERA Rogue Detection Sensor logs in Filtered XML collection mode with records for last 10 days:

```
start /wait ESETLogCollector_ENU.exe /age:10 /otype:xml
/targets:eraag,erasrv,eraconf,erard collected_era_logs.zip
```

EXAMPLE

This example command converts collected ESET binary log file (Computer scan log) to an XML file format with all records (including logs marked as deleted):

```
start /wait ESETLogCollector_ENU.exe /bin2xml /all
C:\collected_eset_logs\ESET\Logs\Common\eScan\ndl27629.dat scan_log.xml
```

Similarly, collected Computer scan log file conversion to a text file, but omitting logs marked as deleted:

```
start /wait ESETLogCollector_ENU.exe /bin2txt
C:\collected_eset_logs\ESET\Logs\Common\eScan\ndl27629.dat scan_log.txt
```

Available targets

This is a complete list of all possible targets that can be collected using ESET Log Collector Command line specified by `/Targets:` option.

NOTE

You may not see all the targets listed here. This is because available targets for your system only are listed when you run command line help `start /wait ESETLogCollector_ENU.exe /?` Targets not listed do not apply to your system or configuration.

`Proc`	Running processes (open handles and loaded DLLs)
`Drives`	Drives info
`EvLogApp`	Application event log
`EvLogSys`	System event log
`SetupAPI`	SetupAPI logs
`EvLogLSM`	Terminal services - LSM operational event log
`SysIn`	ESET SysInspector log
`DrvLog`	Drivers install logs
`NetCnf`	Network configuration
`WFPFil`	WFP filters
`InstLog`	ESET Installer logs
`EraAg`	ERA Agent logs

`EraSrv`	ERA Server logs
`EraConf`	ERA configuration
`EraDumps`	ERA process information and dumps
`EraRD`	ERA Rogue Detection Sensor logs
`EraMDM`	ERA MDMCore logs
`EraProx`	ERA Proxy logs
`EsaLogs`	ESA logs
`ProdCnf`	ESET product configuration
`DirList`	ESET data and install directory file list
`Drivers`	ESET drivers
`EsetReg`	ESET Registry key content
`QInfo`	Info about quarantined files
`QFiles`	Quarantined files
`Warn`	ESET Events log
`Threat`	ESET Detected threats log
`OnDem`	ESET Computer scan logs
`Hips`	ESET HIPS log
`Fw`	ESET Network protection log
`FwCnf`	ESET Personal firewall configuration
`Web`	ESET Filtered websites log
`Paren`	ESET Parental control logs
`Dev`	ESET Device control log
`WCam`	ESET Webcam protection log
`WebCtl`	ESET Web control log
`OnDemDB`	ESET On-demand server database scan logs
`HyperV`	ESET Hyper-V server scan logs
`Spam`	ESET Spam log
`SMTP`	ESET SMTP protection log
`Email`	ESET mail server protection log
`EmDiag`	ESET diagnostic e-mail processing logs
`ScanCache`	Local cache database
`SpamDiag`	ESET Antispam configuration and diagnostic logs
`Diag`	General product diagnostics logs
`ECPDiag`	ECP diagnostics logs
`pcap`	ESET pcap logs
`XAg`	MS Exchange transport agents registration
`XEws`	MS Exchange EWS logs
`Domino`	Domino IBM_TECHNICAL_SUPPORT logs + notes.ini
`SHPIO`	ESET SHPIO.log

`SP`	MS SharePoint logs
`SHPReg`	SharePoint Registry key content
`KConnCnf`	Kerio Connect configuration
`KConn`	Kerio Connect logs
`KCtrlCnf`	Kerio Control configuration
`KCtrl`	Kerio Control logs
`AllReg`	Complete Windows Registry content
`WinsockCat`	Winsock LSP catalog
`TmpList`	List of files in temporary directories
`LastPol`	Last applied policy
`BlkF`	ESET Blocked files log
`SentF`	ESET Sent files log
`OneDrive`	MS OneDrive scan logs

End-User License Agreement (EULA)

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

Software End-User License Agreement.

Under the terms of this Software End-User License Agreement (hereinafter referred to as “the Agreement”) executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31 333 535 or another company from the ESET Group (hereinafter referred to as “ESET” or “the Provider”) and you, a physical person or legal entity (hereinafter referred to as “You” or “the End User”), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

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

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

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

1. **Software**. As used in this Agreement the term “Software” means: (i) the computer program and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with

which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software (hereinafter referred to as "Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the computer on which You install the Software.

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

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

b) **Stipulation of the number of licenses**. The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to installation of the Software on one computer system. You must not use the same License at the same time on more than one computer.

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

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

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

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

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

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

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

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

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

(f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

6. **Copyright.** The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 5(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

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

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

9. **Commencement and termination of the Agreement.** This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all back-up copies and all related materials provided by the Provider or its business partners. Irrespective of the manner of termination of this Agreement, the provisions of Articles 6, 7, 10, 12, 19 and 21 shall continue to apply for an unlimited time.

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

11. **No other obligations.** This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

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

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

14. **Technical support.** ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion.

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

16. **Verification of the genuineness of the Software.** The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password).

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

18. **Export and re-export control.** The Software, the Documentation or components thereof, including information about the Software and components thereof, shall be subject to import and export controls under legal regulations which may be issued by governments responsible for issue thereof under applicable law, including US Export Administration Regulations, and end-user, end-use and destination restrictions issued by the US Government and other governments. You agree to comply strictly with all applicable import and export regulations and acknowledge that You have the responsibility to obtain all licenses required to export, re-export, transfer or import the Software.

19. **Notices.** All notices and return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

20. **Applicable law.** This Agreement shall be governed by and construed in accordance with the laws of the Slovak

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

21. **General provisions.** Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable in accordance with the conditions stipulated therein. This Agreement may only be modified in written form, signed by an authorized representative of the Provider or a person expressly authorized to act in this capacity under the terms of a power of attorney.

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