ESET Log Collector

User guide

Click here to display the Online help version of this document

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

REV. 10/1/2020

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.

NOTE
ESET Log Collector has the same systems requirements as your ESET security product. ESET Log Collector runs on any version of Microsoft Windows operating system.

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

The ESET Log Collector contains all languages in a single executable. This allows you to switch the language as needed upon startup without the need to download the correct localized version. The language to be used is either detected automatically or can be selected explicitly. There are two ways to specify language explicitly:

1. Use the command line switch `/lang:<language_code>`
2. Rename the file to *ESETLogCollector_<language_code>.exe*

Available values of language codes: ARE, BGR, CSY, DAN, DEU, ELL, ENU, ESL, ESN, ETI, FIN, FRA, FRC, HUN, CHS, CHT, ITA, JPN, KKZ, KOR, LTH, NLD, NOR, PLK, PTB, ROM, RUS, SKY, SLV, SVE, THA, TRK, UKR

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.

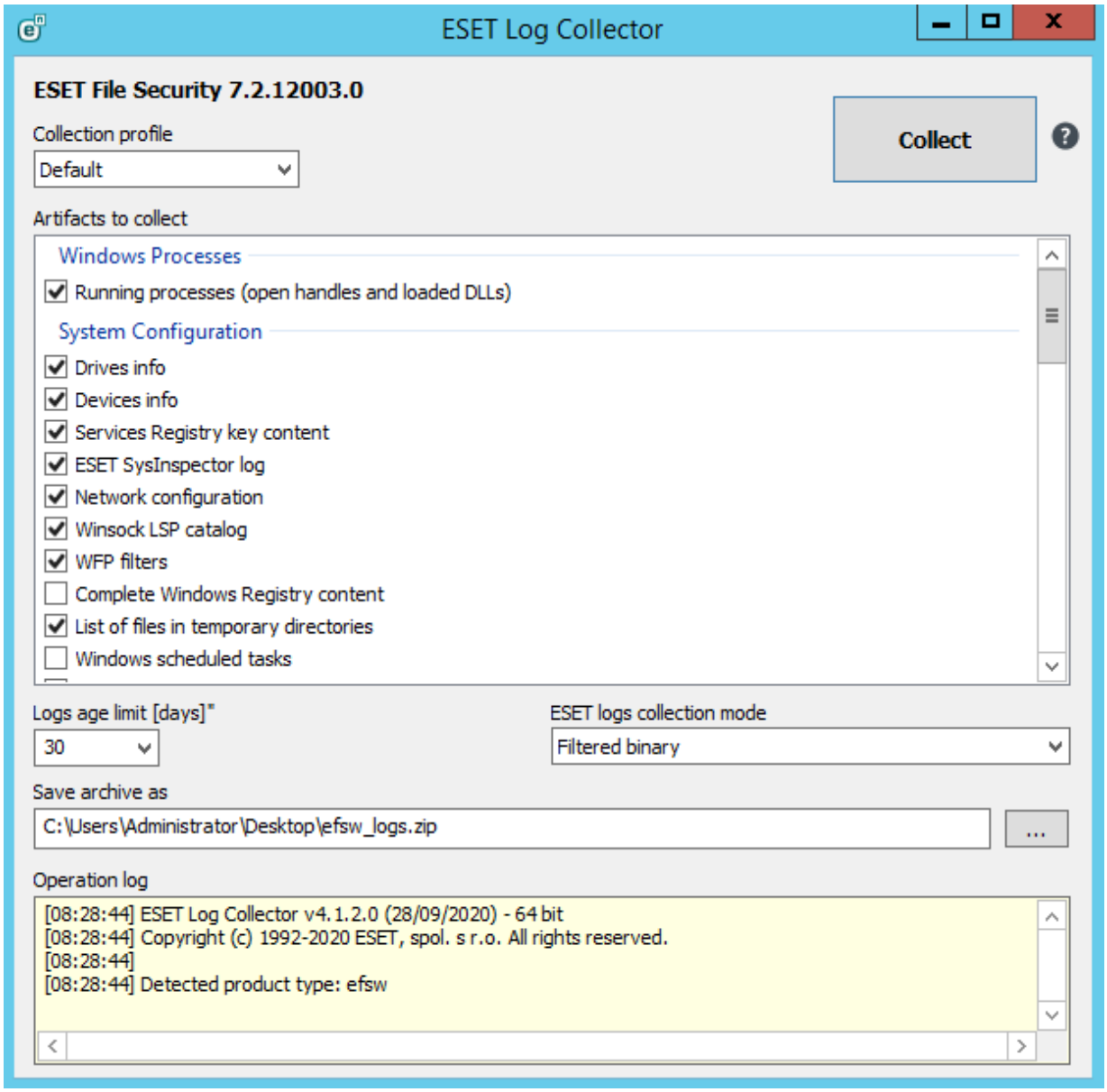
NOTE
An additional feature of ESET Log Collector is conversion of collected ESET binary log files (`.dat`) to XML or text file format. However, you can convert collected ESET binary log using ESET Log Collector Command line interface (CLI) only.

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.



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**		
Application event log	✓	✓	*Windows\Logs\Application.xml*	Windows Application event logs in a custom XML format. Only messages from the last 30 days are included.
System event log	✓	✓	*Windows\Logs\System.xml*	Windows System event logs in a custom XML format. Only messages from the last 30 days are included.
Terminal services - LSM operational event log*	✓	✓	*Windows\Logs\LocalSessionManager-Operational.evtx*	Windows event log containing information about RDP sessions.
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.
WMI Activity operating event log	✓	✓	*Windows\Logs\WMI-Activity.evtx*	Windows event log containing WMI Activity tracing data. Only messages from the last 30 days are included.
Application event log	✓	✓	*Windows\Logs\Application.evtx*	Windows Application event log file. Only messages from the last 30 days are included.
System event log	✓	✓	*Windows\Logs\System.evtx*	Windows System event log file. Only messages from the last 30 days are included.
Services Registry key content			*Windows\Services.reg*	Contains a registry key content of *KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*. Collecting this key may be helpful in case of issues with drivers.

**Windows Vista and newer*

System Configuration				
Artifact name	**Collection profile**		**Location / File name**	**Description**
	Default	**Threat detection**		
Drives info	✓	✓	*Windows\drives.txt* *Windows\volumes.txt*	Collected text file containing information about disk drives and volumes.
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 scheduled tasks	✗	✓	*Windows\Scheduled Tasks*.**	Collected multiple *xml* files containing all tasks from the Windows Task Scheduler to help detect malware that exploits the Task Scheduler. Since the files are located in subfolders, the whole structure is collected.
WMI repository	✗	✓	*Windows\WMI Repository*.**	Collected multiple binary files containing WMI database data (meta-information, definition and static data of WMI classes). Collecting these files may help identify malware that uses WMI for persistence (such as Turla). Since WMI files may be located in subfolders, the whole structure is collected.
Windows Server roles & features	✓	✗	*Windows\server_features.txt*	Text file containing a tree of all Windows Server features. Each feature contains the following information: oInstalled state oLocalized name oCode name oState (available on Microsoft Windows Server 2012 and newer)

**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.

ESET Security Management Center (ESMC) and ESET Remote Administrator (ERA)				
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.
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 Agent database	✓	✗	*ERA\Agent\Database\data.db*	ESMC/ERA Agent database file.
Apache Tomcat configuration	✓	✗	*ERA\Apache\Tomcat\conf*.**	Apache Tomcat configuration files, it contains a copy of *server.xml* file without sensitive information.
Apache Tomcat logs	✓	✗	*ERA\Apache\Tomcat\logs*.log* *ERA\Apache\Tomcat\EraAppData\logs*.log* *ERA\Apache\Tomcat\EraAppData\WebConsole*.log*	Apache Tomcat log(s) in text format located in Apache Tomcat install or application directory. It also contains WebConsole logs.
Apache HTTP Proxy configuration	✓	✗	*ERA\Apache\Proxy\conf\httpd.conf*	Apache HTTP Proxy configuration file.

ESET Security Management Center (ESMC) and ESET Remote Administrator (ERA)				
Apache HTTP Proxy logs	✓	✗	*ERA\Apache\Proxy\logs*.log*	Apache HTTP Proxy log(s) in text format located.

**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*	Since version 4.0.3.0 the file is always included (without any dependences). It contains installed product info. *versions.csv* must exist in ESET AppData directory to be included.
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 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 ESMC/ERA.
ESET components	✓	✓	*ESET\Config\msi_features.txt*	Collected information about available ESET product MSI installer components.
HIPS configuration	✓	✓	*ESET\Config\HipsRules.bin*	HIPS rules data.
Connected Home configuration	✓	✓	*ESET\Config\homenet.dat*	Connected Home data.

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.
Small quarantined files *(< 250KB)*	✓	✗	*ESET\Quarantine*.*(< 250KB)*	Quarantine files smaller than 250 KB.
Big quarantined files *(> 250KB)*	✗	✓	*ESET\Quarantine*.*(> 250KB)*	Quarantine files larger than 250 KB.

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 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.
ESET Audit log	✓	✓	*ESET\Logs\Common\audit.dat*	ESET Audit 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.
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 Enterprise Inspector				
Artifact name	**Collection profile**		**Location / File name**	**Description**
	Default	**Threat detection**		
EEI Server logs	✓	✗	*EEI\Server\Logs*.log*	Server product text logs.
EEI Agent logs	✓	✗	*EEI\Agent\Logs*.log*	Agent product text logs.
EEI Server configuration	✓	✗	*EEI\Server\eiserver.ini*	An *.ini* file containing Server product configuration.
EEI Agent configuration	✓	✗	*EEI\Agent\eiagent.ini*	An *.ini* file containing Agent product configuration.
EEI Server policy	✓	✗	*EEI\Server\eiserver.policy.ini*	An *.ini* file containing Server product policy.

ESET Enterprise Inspector				
EEI Agent policy	✓	✗	*EEI\Agent\eiagent.policy.ini*	An *.ini* file containing Agent product policy.
EEI Server certificates	✓	✗	*EEI\Server\Certificates*.**	Contains certification files used by Server product. Since the files are located in subfolders, the whole structure is collected.
EEI Agent certificates	✓	✗	*EEI\Agent\Certificates*.**	Contains certification files used by Agent product. Since the files are located in subfolders, the whole structure is collected.
EEI Server dumps	✓	✗	*EEI\Server\Diagnostics*.**	Server product dump files.
MySQL Server configuration	✓	✗	*EEI\My SQL\my.ini*	An *.ini* file containing MySQL Server configuration used by EEI Server product.
MySQL Server logs	✓	✗	*EEI\My SQL\EEI.err*	An error text log of MySQL Server used by EEI Server product.

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 Greylist log	✓	✗	*ESET\Logs\Email*greylistlog*.dat*	ESET Greylist 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* *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 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 (ESET Security for Kerio)				
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.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.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.

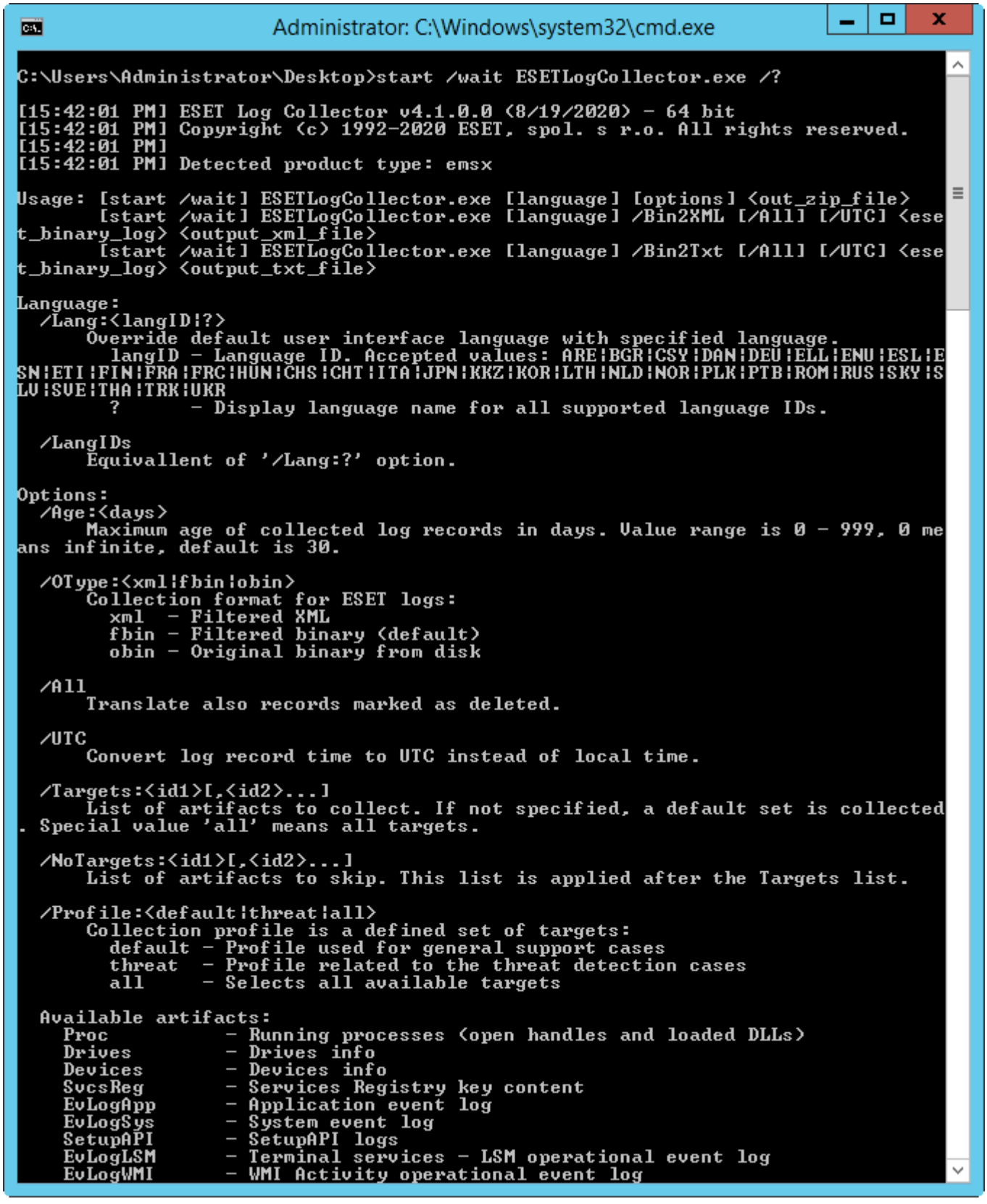
`/NoTargets:<id1>[,<id2>...]` - List of artifacts to skip. This list is applied after the Targets list.

`/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

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.

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).



EXAMPLE

This example command changes the language to Italian. You can use any of the available languages: ARE, BGR, CSY, DAN, DEU, ELL, ENU, ESL, ESN, ETI, FIN, FRA, FRC, HUN, CHS, CHT, ITA, JPN, KKZ, KOR, LTH, NLD, NOR, PLK, PTB, ROM, RUS, SKY, SLV, SVE, THA, TRK, UKR

```
/lang: ITA
```

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.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.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.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.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.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.exe /?` Targets not listed do not apply to your system or configuration.

`Proc`	Running processes (open handles and loaded DLLs)
`Drives`	Drives info
`Devices`	Devices info
`SvcsReg`	Services Registry key content
`EvLogApp`	Application event log
`EvLogSys`	System event log
`SetupAPI`	SetupAPI logs
`EvLogLSM`	Terminal services - LSM operational event log
`EvLogWMI`	WMI Activity operational event log
`SysIn`	ESET SysInspector log
`DrvLog`	Drivers install logs
`NetCnf`	Network configuration
`WFPFil`	WFP filters
`InstLog`	ESET Installer logs
`EraAgLogs`	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
EraTomcatCfg	Apache Tomcat configuration
EraTomcatLogs	Apache Tomcat logs
EraProxyCfg	Apache HTTP Proxy configuration
EraProxyLogs	Apache HTTP 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
EsetCmpts	ESET components
QInfo	Info about quarantined files
QFiles	Quarantined files
QSmallFiles	Small quarantined files
QBigFiles	Big 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
Grey	ESET Greylist log
SMTPProt	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
SchedTaks	Windows scheduled tasks
Wmirepo	WMI repository
WinSrvFeat	Windows Server roles&features
LastPol	Last applied policy
BlkF	ESET Blocked files log
SentF	ESET Sent files log
OneDrive	MS OneDrive scan logs
Audit	ESET Audit logs
HipsCfg	HIPS configuration
HomeNetCfg	Connected Home configuration

End User License Agreement