

ESET LiveGuard Advanced

User guide

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

Copyright ©2024 by ESET, spol. s r.o.

ESET LiveGuard Advanced was developed by ESET, spol. s r.o.

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

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

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

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

REV. 4/12/2024

1 Welcome	1
2 Product overview	2
2.1 How detection layers work	4
2.2 Requirements and supported products	9
2.3 Using a proxy with ESET LiveGuard Advanced	11
2.3 Apache HTTP Proxy	12
2.3 Linux Proxy configuration	13
2.3 Windows Proxy configuration	15
3 How to purchase the service	18
4 Activate ESET LiveGuard Advanced	18
4.1 Import licenses in EBA	19
4.2 Synchronize EBA with ESET PROTECT On-Prem	21
4.3 Add license in ESET MSP Administrator	24
4.4 Synchronize ESET MSP Administrator with ESET PROTECT On-Prem	29
4.5 Activate a group of computers	32
4.6 Activate selected computers	37
4.7 Remote installation and activation	39
5 How to enable and configure the ESET LiveGuard Advanced service	42
5.1 Configuration of ESET security product	42
5.2 Policy management	45
6 Using ESET LiveGuard Advanced	48
6.1 ESET Mail Security	50
6.2 ESET Endpoint Security and ESET Server Security	54
6.3 ESET Cloud Office Security	58
6.4 Proactive protection	60
6.5 List of submitted files	63
6.6 Create a report	67
6.7 Results of analysis	71
6.7 Behavioral report	72
6.8 Manual upload of a file for analysis	75
6.8 Submit file from ESET PROTECT On-Prem	76
6.8 Submit file from ESET Endpoint Security	77
6.8 Submit file from ESET Server Security	78
6.8 Submit file from ESET Mail Security	80
6.9 Add exclusion	81
6.10 Use exclusions to improve performance	84
6.10 Review list of submitted files	84
6.10 Exclude folders	91
6.10 Exclude process	95
6.10 Review number of submitted files	97
6.11 Notification for detected threats	101
7 FAQ	103
8 Test ESET LiveGuard Advanced functionality	106
9 Troubleshooting	109
9.1 Diagnostics	116
9.2 Troubleshooting Apache HTTP Proxy	119
10 Security for ESET LiveGuard Advanced	120
11 Fair Use policy	124
12 Privacy Policy	125

13 Terms of Use 128

 13.1 ESET Management Agent EULA 131

 13.2 Data Processing Agreement 138

 13.3 Standard Contractual Clauses 140

Welcome


Welcome to the ESET LiveGuard Advanced user guide. This document explains how to use and manage ESET LiveGuard Advanced. It also details the connection of ESET LiveGuard Advanced to other ESET business products.


We use a uniform set of symbols to highlight topics of specific interest or significance. Topics in this guide are divided into several chapters and sub-chapters. You can find relevant information by using the Search field at the top.


[Online Help](#) is the primary source of help content. The latest version of Online Help will automatically be displayed when you have a working internet connection.


- 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.
- The [ESET Forum](#) provides ESET users with an easy way to get help and to help others. You can post any problem or question related to your ESET products.
- You can post your rating and/or provide feedback on a specific topic in help, click **Was this information helpful?** to rate the article and add your comment.

Information boxes used in this guide:

 Notes can provide valuable information, such as specific features or a link to some related topic.

 This requires your attention and it should not be skipped. Usually, it provides non-critical but significant information.

 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 case which describes a user case relevant for the topic where it is included. Examples are used to explain more complicated topics.

Used text styles

Convention	Meaning
Bold type	Names of interface items such as boxes and option buttons.
Code	Code samples or commands.
Hyperlink	Provides quick and easy access to cross-referenced topics or external web location. Hyperlinks are highlighted in blue and may be underlined.
<code>%ProgramFiles%</code>	The Windows system directory where programs installed on Windows are stored.

Product overview

About the service

ESET LiveGuard Advanced is a paid service provided by ESET. Its purpose is to add a layer of protection specifically designed to mitigate new threats in the wild.

Change of the service name

On March 23, 2022, ESET Dynamic Threat Defense was re-branded to ESET LiveGuard Advanced. In ESET business products, you can find it also as ESET LiveGuard. Both names refer to the same service.

Service availability

The [ESET Status Portal](#) displays the current status of ESET cloud services, scheduled outages and past incidents. If you are experiencing an issue with a supported ESET service and do not see it listed in the Status Portal, contact [ESET Technical Support](#).

Monitoring teams verify potential issues internally, and confirmed incidents are posted and updated manually to maintain high credibility and accuracy. Therefore, they appear on the Status Portal with a slight delay. Incidents with a short duration may not be posted if they are resolved before being manually confirmed.

How it works

Suspicious samples that are not yet confirmed as malicious and may potentially carry malware are automatically submitted to the ESET cloud. Submitted samples are run in a sandbox and are evaluated by our [advanced malware detection engines](#). Malicious samples or suspicious spam emails are submitted to ESET LiveGrid®. Email attachments are handled separately and are subject to submission to ESET LiveGuard Advanced. Administrators or users can define the scope of files that are submitted and the retention period of the file in the ESET cloud. Documents and PDF files with active content (macros, javascript) are not submitted by default. See the detailed description of [How detection layers work](#).

In the **Submitted files** section of the remote management console, administrators get a brief report of the observed sample's behavior for each submitted file. If a file turns out to be malicious, it is blocked for all users participating in ESET LiveGrid® as a suspicious object. If evaluated as suspicious, it is blocked on all machines within the user's organization, depending on the sensitivity threshold.

Files can be submitted [manually](#) or automatically based on [policy configuration](#). [In the ESET PROTECT Web Console, a user can submit .exe files](#) reported from client machines.

[What are the differences between ESET LiveGuard Advanced, ESET LiveGrid® and ESET Threat Intelligence?](#)

Architecture

ESET security products and management console

Whenever a sample is uploaded to ESET LiveGuard Advanced for analysis, that sample's metadata is uploaded to the management console if the Client can connect to the Server. This provides the console Administrator with a list of samples uploaded to the ESET cloud.

ESET security products and ESET LiveGuard Advanced

Whenever an activated and configured ESET security product decides a sample needs to be analyzed, it uploads the sample to ESET LiveGuard Advanced. After ESET LiveGuard Advanced analyzes the sample, it provides the result to all machines in that company (or MSP customer) and to all companies that have ever submitted that file. The security product takes the appropriate action based on the policy in place. In ESET endpoint and ESET server products version 7.2 and later, you can select an action to take on suspicious files downloaded by browsers and email clients.

ESET signs all transferred packages to mitigate the risk of attack. When using an HTTP connection in the internal network, the product checks if the connection is upgraded to HTTPS behind a proxy. If the proxy is not configured correctly, the HTTPS connection is also used in the internal network.

ESET management consoles and ESET LiveGuard Advanced

The ESET LiveGuard Advanced is available in on-premises and cloud-based management consoles (ESET PROTECT On-Prem, ESET PROTECT). After ESET LiveGuard Advanced receives a sample from an ESET security product, it automatically informs the management console about the status of the analysis. When the analysis is complete, the result is transferred to the management console.

Roaming Endpoints and ESET LiveGuard Advanced

A roaming endpoint is any client with an ESET security product operating outside of your company's perimeter and has no connection to ESET PROTECT On-Prem. Usually, it is a computer at home or on a business trip without a VPN. A roaming client takes full advantage of ESET LiveGuard Advanced. However, it does not notify ESET PROTECT On-Prem about samples that have been submitted for analysis. When the client returns to your perimeter and connects to ESET PROTECT On-Prem, the client's metadata is synchronized, and the list of submitted files is updated. Other clients on your network can receive updates that result from discovered threats while a client is roaming even before it synchronizes with ESET PROTECT On-Prem.

ESET Cloud Office Security and ESET LiveGuard Advanced

ESET LiveGuard Advanced analyzes submitted files by executing suspicious code in an isolated environment to evaluate its behavior. ESET Cloud Office Security submits suspicious email attachments and files from Microsoft Exchange Online, OneDrive, Teams groups and SharePoint sites to ESET LiveGuard Advanced for analysis. ESET Cloud Office Security does not require or upload data to an ESET management console. Information about submitted files and their results are present in ESET Cloud Office Security.

Global Database

ESET LiveGuard Advanced uses two Azure data centers (the USA and Europe) to store hashes of the files and the results of their analysis. Data centers provide faster results for already analyzed files. The ESET Headquarters (located in Slovakia) stores all the submitted files and performs the analysis. Each customer's (company's) data is stored separately in one global database. ESET routes user connections to the nearest data center.

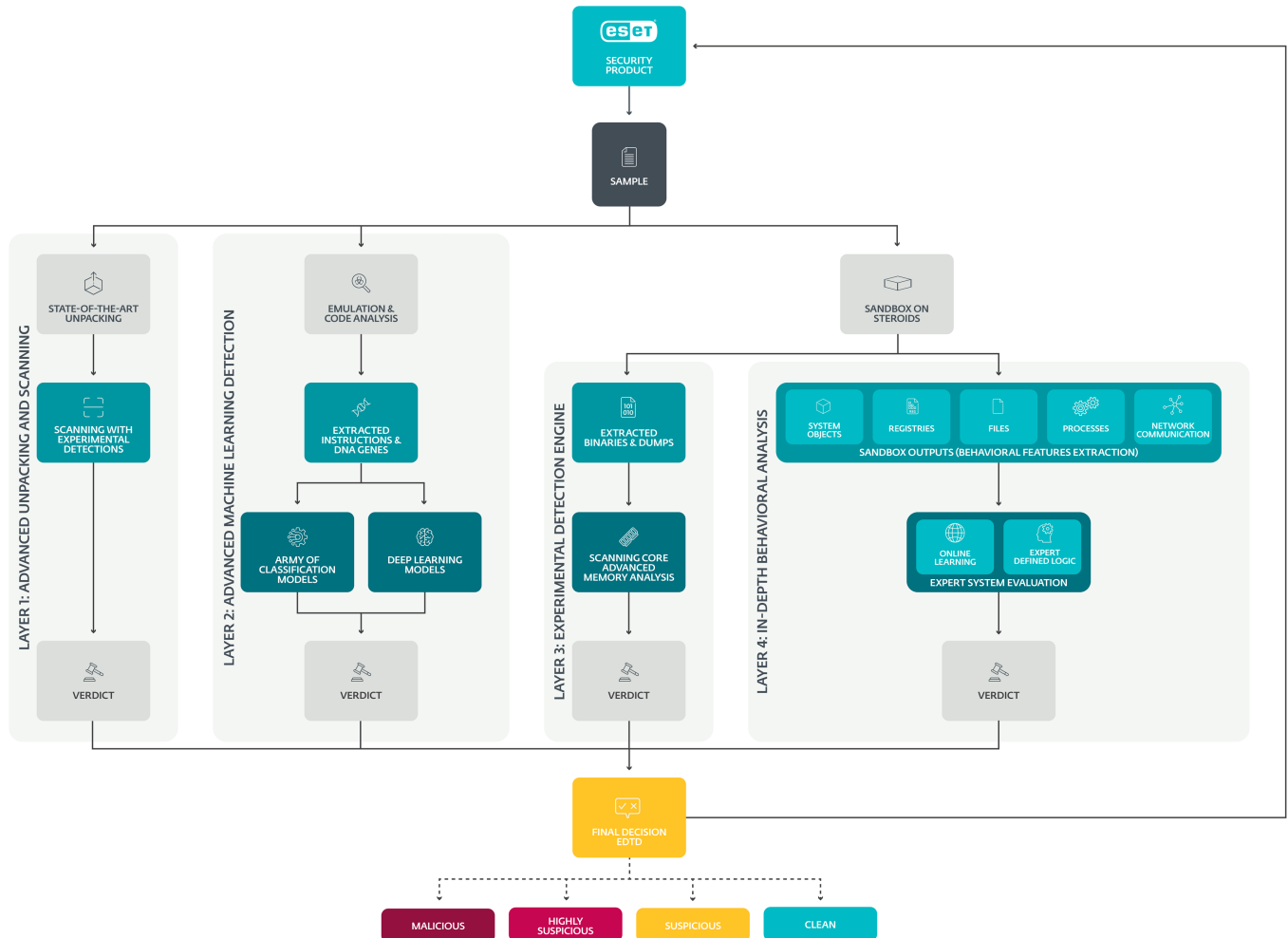


We highly recommend that you use a [Proxy](#) for caching responses from ESET servers, especially for users with a high number of client machines (hundreds or more), since using a Proxy can save significant network traffic.

You can [exclude selected folders and processes](#) to decrease the number of submitted files and improve the overall performance.

How detection layers work

ESET LiveGuard Advanced uses four separate detection layers to ensure the highest detection rate. Each layer uses a different approach and gives its verdict over the sample. The final assessment is the result of all information about the sample. See the overview of the process in the scheme below:

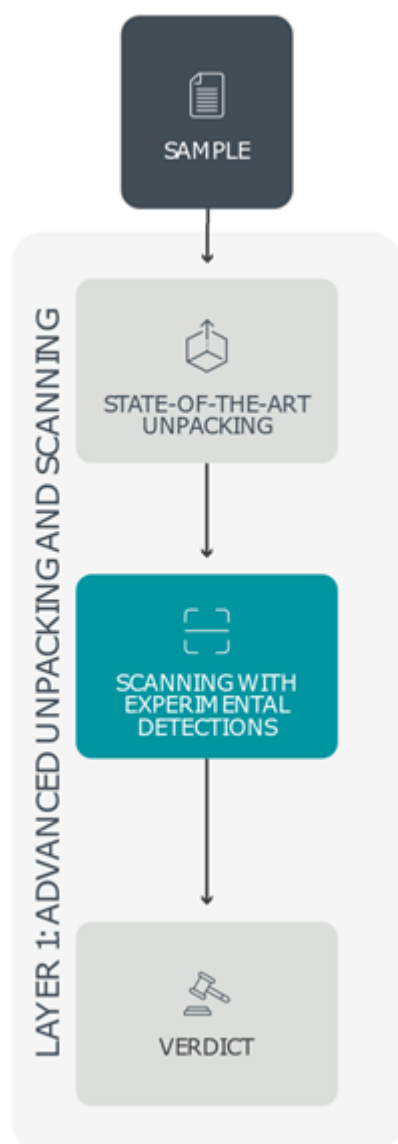


[Click the image for the full-size picture.](#)

Layer 1: Advanced unpacking and scanning

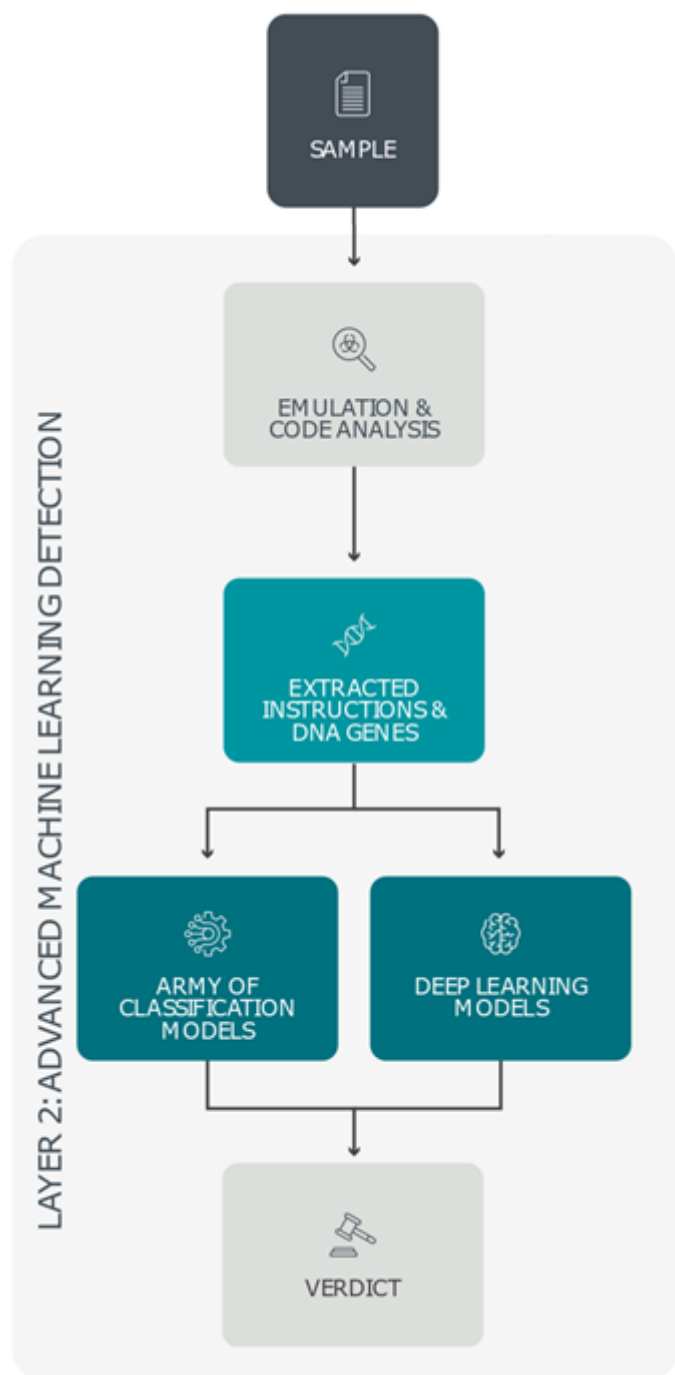
After entering the initial layer of ESET LiveGuard Advanced - the so-called Advanced unpacking and scanning layer - static samples are matched against ESET's threat database: enriched with experimental and yet to be distributed detections as well as against a comprehensive list of clean, potentially unwanted (PUA), and potentially unsafe (PUaA) items. Malware often tries to thwart detection by hiding its malicious core behind a range of packing layers; thus, this coating must be removed for proper analysis. ESET LiveGuard Advanced uses Advanced unpacking and scanning to achieve this by utilizing highly specialized tools based on packers that ESET researchers have found in malicious code. These specialized unpackers peel away malware's protective layer, allowing ESET LiveGuard Advanced to match the sample against the enriched threat database again. The Advanced unpacking

and scanning layer classifies the sample as malware, clean, PUA, or PUsA. Due to security risks and hardware demands associated with the unpackers and other incorporated procedures, a high-performance and secure environment are required. This unique environment is provided by ESET LiveGuard Advanced's robust and resilient cloud infrastructure.



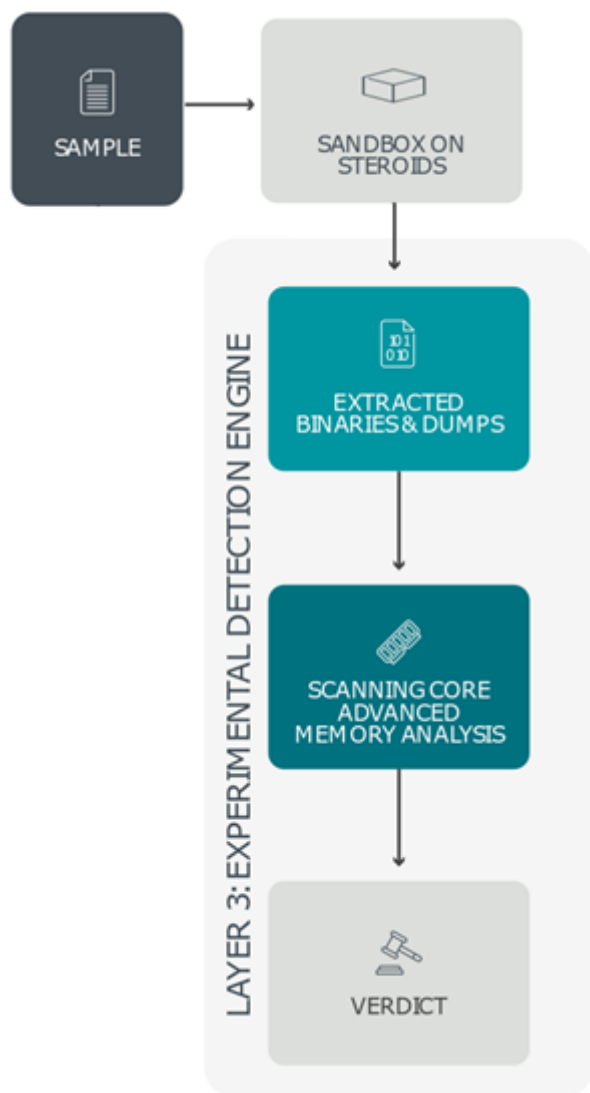
Layer 2: Advanced Machine Learning detection

Each item submitted to ESET LiveGuard Advanced is also subject to static analysis via Advanced Machine Learning detection, producing basic characteristics of the sample. As analyzing compressed or encrypted code with no further processing would only attempt to classify noise, the submitted item simultaneously undergoes another more dynamic analysis that extracts its instructions and DNA genes. By describing a sample's active features and behaviors, malicious characteristics of packed or obfuscated objects are uncovered even without executing it. Information extracted from all previous steps is further processed by a small army of carefully chosen classification models and deep learning algorithms. Finally, all this information is consolidated via a neural network that returns one of four probability levels – malicious, highly suspicious, suspicious, and clean. If this or any other ESET LiveGuard Advanced layer is not used, an “analysis not needed” message is displayed. Due to these procedures' complexity and hardware demands, a significantly more powerful infrastructure than the one provided by a user's endpoint is necessary. ESET engineers devised a superior and complex set of systems to handle the computation-heavy tasks – ESET LiveGuard Advanced.



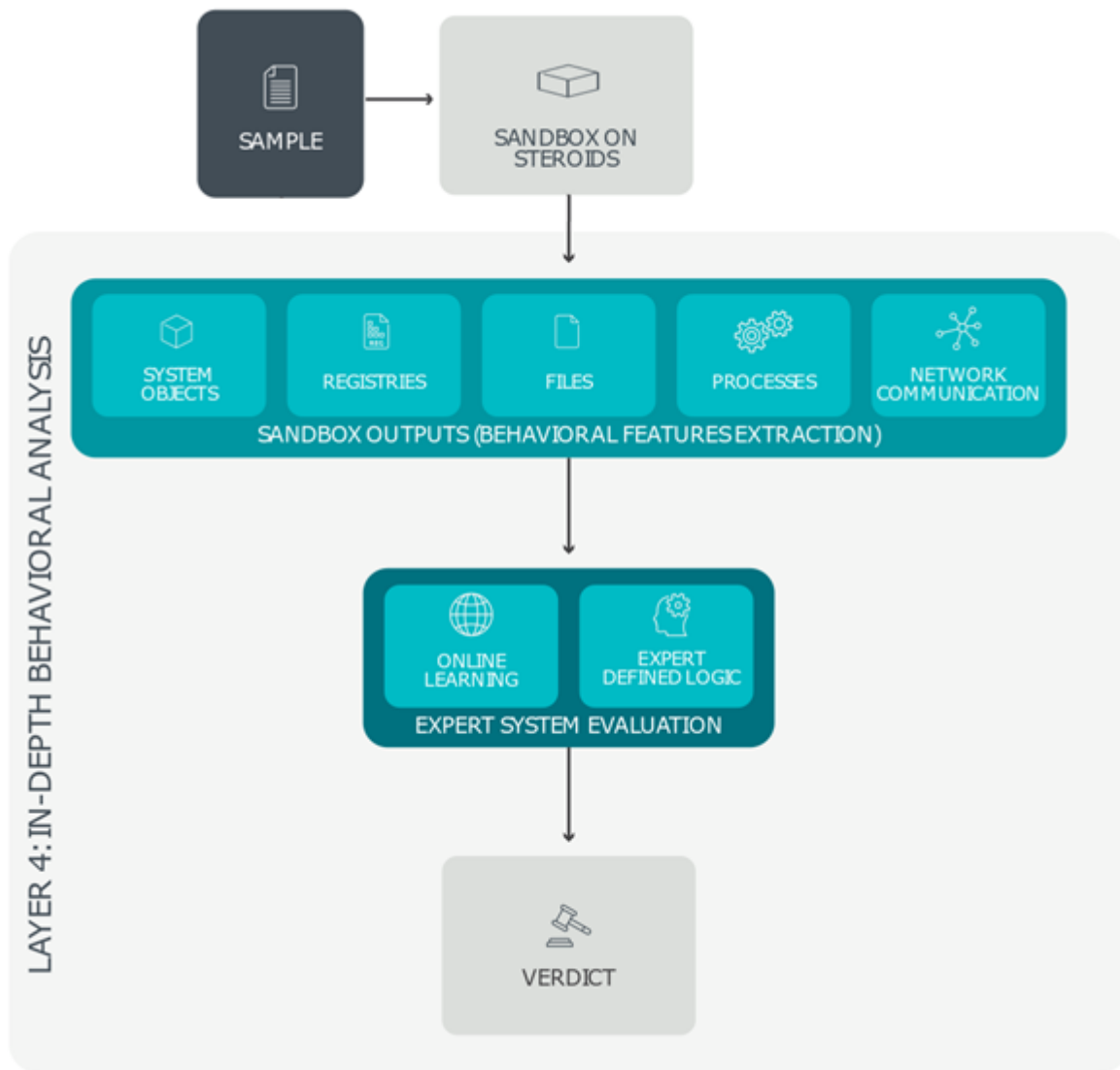
Layer 3: Experimental detection engine

To further analyze each sample, a deeper and behavior-focused analysis is necessary to complement the previous findings. To gather this type of threat intelligence, another ESET LiveGuard Advanced layer steps in – namely, the Experimental detection engine. It inserts the suspicious item into a set of precisely configured systems that resemble full-scale machines using various operating systems – a kind of “sandbox on steroids”. These highly controlled environments serve as monitoring cells fitted with a legion of ESET’s detection algorithms logging every action. To identify hidden malicious behavior, the Experimental detection engine also produces a large quantity of memory dumps. These are subsequently scanned and matched against ESET’s enriched threat database that incorporates unpublished and experimental detections, ensuring highly accurate detection results and an extremely low number of false positives. Intelligence gathered by the Experimental detection engine is also compiled into a comprehensive list of events detected by the sandbox, which is then used for further analysis in the final ESET LiveGuard Advanced detection layer – In-Depth Behavioral Analysis.



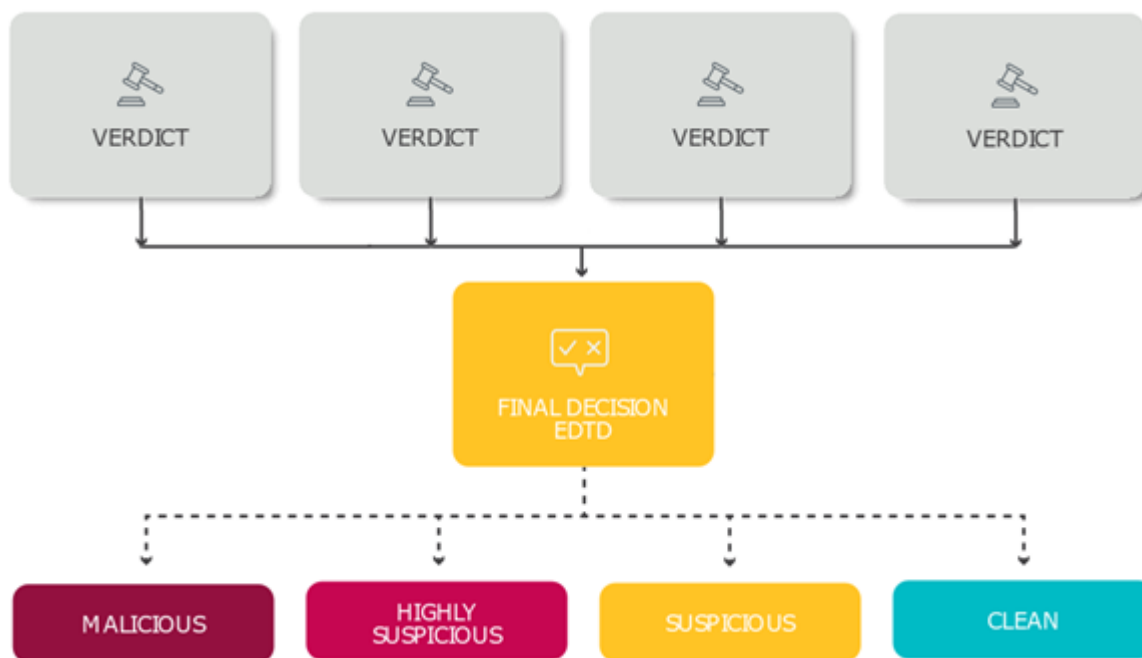
Layer 4: In-Depth Behavioral Analysis

In the final ESET LiveGuard Advanced layer, known as In-Depth Behavioral Analysis, all sandbox outputs – including files created or deleted on the hard-drive, entries added to or removed from the Windows system registry, all external communication attempts, and scripts that are being run – are subject to a thorough behavioral analysis. In this stage, ESET LiveGuard Advanced focuses on malicious and suspicious actions such as attempted connections to web locations with bad reputations, use of known malicious objects, and use of unique strings generated by specific malware families. In-Depth Behavioral Analysis also breaks up the sandbox outputs into logical blocks, which are then matched against an extensive and periodically reviewed database of previously analyzed patterns and chains of actions to identify even the slightest indication of malicious behavior.



Final result

ESET LiveGuard Advanced combines all available verdicts from the detection layers and evaluates the sample's status. The result is delivered to the user's ESET security product and their company's infrastructure first.



Requirements and supported products

Requirements for users of on-premises products

Your environment should meet the following prerequisites for the proper functioning of ESET LiveGuard Advanced:

- A working ESET Business Account or ESET MSP Administrator account synchronized with an ESET management console
- A supported ESET management console
- Version 7.x or later of compatible ESET security products installed
- [A Valid license for ESET LiveGuard Advanced](#)
- [Activated Security products with ESET LiveGuard Advanced License](#)
- [ESET LiveGuard Advanced enabled in policies for compatible Security products](#)
- Network requirements on opened ports are the same as for ESET LiveGrid®.
- If you are using the Apache HTTP Proxy or ESET Bridge, the network requirements on opened ports are the same as for ESET LiveGrid®. Otherwise, the port is 443 instead.

o Access to ESET LiveGuard Advanced online [servers](#)

Requirements for ESET Cloud Office Security users

To use the ESET LiveGuard Advanced in the ESET Cloud Office Security, the user needs the following:

- A working ESET Business Account or ESET MSP Administrator account connected to ESET Cloud Office

Security

- A valid [license](#) for ESET LiveGuard Advanced

ESET Cloud Office Security does not share any information about submitted files with ESET management consoles.

Access Rights in management consoles

In the Web Console, the submitted files and analysis results are only visible to a user with [access rights](#) to the device that submitted that file. You can manually submit an executable file reported from ESET Inspect from the Web Console. You need to have the **Use** permission for the computer that reported the detection and **Write** permissions for **Send File to ESET LiveGuard** functionality over your home group.

Roaming endpoints—if a device cannot reach the ESET PROTECT Server but can reach ESET cloud servers, files submitted by that device are only visible after the device is connected again to the server.

Performance

You can [use ESET Bridge to cache](#) the results coming from ESET LiveGuard Advanced. Caching can significantly decrease internet traffic on your network.

We recommend using a dedicated ESET Bridge server in enterprise environments (more than 1,000 managed computers). Caching high amounts of files would decrease the server's performance. In high availability environments, we recommend installing each component on a separate machine (ESET PROTECT Server, ESET Bridge, Database server). We also do not recommend running other resource-intensive applications besides the ESET PROTECT On-Prem on the same machine.

Another way to improve the overall performance is to decrease the number of submitted files. You can exclude files, folders, or processes to prevent sending your private files for analysis or to decrease the load. Refer to the [Use exclusions to improve performance](#) for more information.

Supported licenses

ESET LiveGuard Advanced can be activated by:

- One, two and three-year licenses and subscription license from EBA
- Subscription-like MSP licenses from ESET MSP Administrator

Supported products

Submitting files for analysis in ESET LiveGuard Advanced is supported only from certain products. The list of submitted files is only available in the supported version of the management console.

Security products

Product	Version
ESET Endpoint Antivirus for Windows* ESET Endpoint Security for Windows	✓ version 7 and later
ESET Mail Security for Microsoft Exchange	✓ version 7 and later

Product	Version
ESET File Security for Windows Server	✓ version 7.x
ESET Server Security for Windows Server (formerly ESET File Security for Windows Server)	✓ version 8 and later
ESET Endpoint Antivirus for Linux	✓ version 8.1 and later
ESET Server Security for Linux	✓ version 8.1 and later
ESET Cloud Office Security	✓ (from December 2021)

* ESET LiveGuard Advanced functionality is the same for both ESET Endpoint Antivirus and ESET Endpoint Security. This guide only refers to ESET Endpoint Security to make the text easier to understand. ESET Endpoint Antivirus users should follow the instructions for ESET Endpoint Security in this guide.

Management consoles

Product and version	Support
ESET PROTECT On-Prem 8 and later	✓
ESET Security Management Center 7.0 and 7.1	✗ The support for the consoles has ended.
ESET Security Management Center 7.2	✗
ESET Remote Administrator 6.x and earlier	✗
ESET PROTECT	✓

Operating systems not supported



ESET LiveGuard Advanced is not supported on client machines with Windows XP and Microsoft Windows Server 2003. These systems do not support TLS 1.2, which is necessary for the secure transfer of sample files.

Supported Proxy

[ESET Bridge](#) was released with ESET PROTECT On-Prem 10.0 as a substitute for [Apache HTTP Proxy](#) and is included in the [All-in-one installer](#) of the management console. You can also download it as a standalone installer from the ESET [download](#) site. Apache HTTP Proxy will stay functional, but we recommend using ESET Bridge.

Using a proxy with ESET LiveGuard Advanced

ESET LiveGuard Advanced can use [ESET Bridge](#) to forward the connection to ESET servers and cache transferred data. Caching saves the network traffic. Using the proxy is necessary if the client computer does not have network visibility to ESET servers. If you are using ESET Bridge to forward communication between ESET PROTECT Server and ESET Management Agents, you can use it to cache the results coming from ESET LiveGuard Advanced. ESET Bridge also supports [proxy chaining](#).

Proxy settings on client computers



It is necessary to set up proxy [settings](#) (**Settings** > **Tools** > **Proxy server**) in the ESET security product on the client computer. You can do it remotely via a [policy](#).

Users of ESET PROTECT

You should use ESET Bridge for caching the detection results if there are at least 10 computers on one network, for example, an office. If your client computers do not share an internal network or VPN, do not use a proxy. Read more about ESET Bridge in [ESET PROTECT documentation](#).

Apache HTTP Proxy users



Starting with ESET PROTECT 4.0 and ESET PROTECT On-Prem 10.0 (released in November 2022), ESET Bridge replaces Apache HTTP Proxy. Apache HTTP Proxy has reached Limited Support. If you use Apache HTTP Proxy, we recommend [migrating to ESET Bridge](#).

Users of ESET PROTECT Virtual Appliance

The appliance is based on CentOS 7, which is not supported by ESET Bridge. Users of ESET PROTECT Virtual Appliance can choose one of the following solutions:

- Use ESET Bridge installed on a separate machine (see the [list of ESET Bridge requirements](#)).
- Use the Apache HTTP Proxy solution built into the appliance.

Installation of ESET Bridge

You can [install ESET Bridge](#) in several ways. We recommend using the latest [ESET PROTECT All-in-one installer](#).

Caching of results provided by ESET LiveGuard Advanced

ESET Bridge has the correct configuration for caching results by default. Caching of results will start after you [configure ESET Bridge](#) to use a proxy solution for caching and enable ESET LiveGuard Advanced.

Apache HTTP Proxy

Recommendation

Apache HTTP Proxy is functional but has reached Limited Support. We recommend using [ESET Bridge](#) instead.

Proxy configuration file

Linux and Windows store the Apache configuration files at different locations, see the usual location in the table below.

Operating system	Configuration files
Windows	<i>C:\Program Files\Apache HTTP Proxy\conf\httpd.conf</i>
Linux (Debian-based)	<i>/etc/apache2/mods-available/proxy.conf</i>
Virtual Appliance (Linux)	<i>/etc/httpd/conf.d/proxy.conf</i>

Proxy chaining

You can set up more supported forward proxies to work in the chain. Add `ProxyRemote * AddressOfNextProxy` to your proxy configuration. All proxies that are connecting to next proxy need to have the setting.

Example, where 10.1.1.2 is the address of the next proxy:

```
ProxyRemote * http://10.1.1.2:3128
```

To apply the new configuration, restart the proxy service.

Third-party proxies (non-Apache)

Other forward proxy solutions are not supported by ESET. Under certain conditions, other proxies may work, but ESET does not provide configuration or support for these scenarios.

Troubleshooting

To get detailed [logs](#) from your proxy, change / add the parameter `LogLevel debug` in your proxy configuration and restart the proxy service. You can use logs to look for the problem or provide them to ESET Support for further assistance.



When using ESET LiveGuard Advanced in an enterprise-level environment (hundreds of machines or more), we recommend deploying HTTP Proxy on a dedicated server. Running the HTTP Proxy service on a heavily utilized server (e.g., besides the ESET PROTECT Server or database) may result in ESET LiveGuard Advanced connection problems.

You can [exclude selected folders and processes](#) to decrease the number of submitted files and improve the overall performance.

Linux Proxy configuration



This configuration is for Apache HTTP Proxy only. If you use ESET Bridge, [configure it through ESET PROTECT Web Console](#).

Check your proxy configuration file if it contains following lines, if not, add them.

1. Enable caching, Agent connection and HTTPS connection, set the log file.

```
CacheEnable disk http://
```

```
CacheDirLevels 4
```

```
CacheDirLength 2
```

```
CacheDefaultExpire 3600
```

```
CacheMaxFileSize 500000000
```

```
CacheMaxExpire 604800
```

CacheQuickHandler Off

CacheRoot /var/cache/httpd/proxy

AllowCONNECT 443 2222 53535

ProxyRequests On

ProxyVia On

CacheLock on

CacheLockMaxAge 10

ProxyTimeOut 900

SetEnv proxy-initial-not-pooled 1

ErrorLog "|/usr/sbin/rotatelogs -n 10 /var/log/httpd/error_log 1M"

Parameters `CacheRoot` and `ErrorLog` may be adjusted for your system, if necessary.

2. Add following segment of code after the last line of code listed above. It enables caching of ESET LiveGuard Advanced on your proxy:

```
<VirtualHost *:3128>
```

```
    ProxyRequests On
```

```
</VirtualHost>
```

```
<VirtualHost *:3128>
```

```
    ServerName r.edtd.eset.com
```

```
    <If "%{REQUEST_METHOD} == 'CONNECT'">
```

```
        Require all denied
```

```
    </If>
```

```
    ProxyRequests Off
```

```

CacheEnable disk /

SSLProxyEngine On


RequestHeader set Front-End-Https "On"

ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10
0 smax=10

ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On

</VirtualHost>

```

3. Save the configuration and restart the proxy service.

Enable necessary proxy mods

When using custom Linux Apache proxy with ESET LiveGuard Advanced, verify you have enabled mods: `headers ssl alias`.

For example, for Debian-based distributions use:



1. Load modules:

```
sudo a2enmod headers ssl alias
```

2. Restart the service:

```
service apache2 restart
```

Windows Proxy configuration



This configuration is for Apache HTTP Proxy only. If you use ESET Bridge, [configure it through ESET PROTECT Web Console](#).

If you use your own Apache HTTP Proxy for caching ESET LiveGuard Advanced files, you need to modify your *httpd.conf* file. It is usually located in the Apache in the *conf* folder.

Add the segments of configuration in the order as they are listed below.

4. ESET LiveGuard Advanced requires SSL, headers, alias modules available and enabled in your proxy. Verify whether modules are present and add the following lines to the proxy configuration file to load required modules:

```
LoadModule alias_module ..\modules\mod_alias.dll
```

```
LoadModule ssl_module ..\modules\mod_ssl.dll
```

```
LoadModule headers_module ..\modules\mod_headers.dll
```

```
<IfModule ssl_module>
```

```
SSLRandomSeed startup builtin
```

```
SSLRandomSeed connect builtin
```

```
</IfModule>
```

```
LoadModule proxy_module ..\modules\mod_proxy.dll
```

```
LoadModule proxy_http_module ..\modules\mod_proxy_http.dll
```

```
LoadModule proxy_connect_module ..\modules\mod_proxy_connect.dll
```

```
LoadModule cache_module ..\modules\mod_cache.dll
```

```
LoadModule cache_disk_module ..\modules\mod_cache_disk.dll
```

5. Enable caching, Agent connection and HTTPS connection, set the log file.

```
CacheEnable disk http://
```

```
CacheDirLevels 4
```

```
CacheDirLength 2
```

```
CacheDefaultExpire 3600
```

```
CacheMaxFileSize 200000000
```

```
CacheMaxExpire 604800
```

```
CacheQuickHandler Off
```

```
AllowCONNECT 443 563 2222 8883
```

```
ProxyRequests On
```

```
ProxyVia On
```

```
SetEnv proxy-initial-not-pooled 1
```

```
ErrorLog "logs/error.log"
```

```
LogLevel warn
```

ErrorLog and LogLevel may be adjusted for your system, if necessary.

6. Add following segment of code after the last line of code listed above. It enables caching of ESET LiveGuard Advanced data on your proxy:

```
AcceptFilter https none
AcceptFilter http none
EnableSendfile Off
EnableMMAP off

<VirtualHost *:3128>
    ProxyRequests On
</VirtualHost>

<VirtualHost *:3128>
    ServerName r.edtd.eset.com

    <If "%{REQUEST_METHOD} == 'CONNECT'">
        Require all denied
    </If>

    ProxyRequests Off
    CacheEnable disk /
    SSLProxyEngine On

    RequestHeader set Front-End-Https "On"
    ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10
    0 smax=10
    ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On
</VirtualHost>
```

7. Save the configuration file and restart the proxy service.

Purchase the service

MSP users

You can purchase an ESET LiveGuard Advanced license via the [ESET MSP program](#).

ESET MSP Administrator version 1 is not supported



If you are using ESET MSP Administrator, verify that you are using version 2 (available at msp.eset.com). ESET MSP Administrator version 1 was previously available at ema.eset.com. The address now redirects to ESET MSP Administrator 2. Version 1 does not support ESET LiveGuard Advanced.

ESET Business Account users

Purchase a license from your reseller and import it to your [ESET Business Account](#). Your ESET PROTECT On-Prem [synchronizes](#) the imported license and is ready to use.

ESET Cloud Office Security users

All ESET Cloud Office Security tier licenses include the ESET LiveGuard Advanced feature. You can see the ESET LiveGuard label next to the license ID. If you have the ESET Cloud Office Security standalone license, ESET migrates it automatically.

Try ESET LiveGuard Advanced for free in ESET PROTECT

ESET PROTECT users can [request a free 30-day trial](#) license for ESET LiveGuard Advanced from their cloud Console.

Contact Us

Locate your [ESET partner](#) for any questions related to licensing and buying the service. You can contact ESET support via email, chat or phone. For details, see our [contact information page](#).

Activate ESET LiveGuard Advanced

ESET Cloud Office Security users

The ESET LiveGuard Advanced feature is included in the [ESET Cloud Office Security license](#). You can [enable the ESET LiveGuard Advanced](#) by creating and assigning policies.

ESET PROTECT On-Prem and ESET PROTECT users

Depending on your environment, there are various ways to deploy the ESET LiveGuard Advanced in your network. Follow the steps below:

I. Get the ESET LiveGuard Advanced license

- ESET Business Account users: [Obtain an ESET LiveGuard Advanced license](#). You will receive your License Key via email.

- ESET MSP Administrator users: [Add ESET LiveGuard Advanced license](#) to your customer in ESET MSP Administrator.

II. Import the license

- ESET Business Account users: [Synchronize ESET PROTECT On-Prem with your EBA account](#).
- ESET MSP Administrator users: [Synchronize](#) ESET PROTECT On-Prem with your ESET MSP Administrator account. (ESET PROTECT users have cloud licenses synchronized automatically)

 Only a license from EBA or ESET MSP Administrator can activate ESET LiveGuard Advanced.

III. Install an ESET security product

Select your case and follow the steps:

 [I have a compatible ESET security product installed and activated on my devices](#)

1. [Run the activation task with the ESET LiveGuard Advanced license selected](#).
2. Create and assign policies to [enable the ESET LiveGuard Advanced](#).

 [I only have the ESET Management Agent installed on my devices](#)

Follow the steps in [Remote installation and activation](#).

 [I use ESET PROTECT, and I do not have an ESET product installed on my devices](#)

1. Follow the [local deployment guide](#) to install the agent and security product on your endpoints.
2. [Run the activation task with the ESET LiveGuard Advanced license selected](#).
3. Create and assign policies to [enable the ESET LiveGuard Advanced](#).

 [I use ESET PROTECT On-Prem, and I do not have an ESET product installed on my devices](#)

1. Follow the [local deployment guide](#) to install agent and security products on your endpoints.
2. [Run the activation task with the ESET LiveGuard Advanced license selected](#).
3. Create and assign policies to [enable the ESET LiveGuard Advanced](#).

Import licenses in EBA

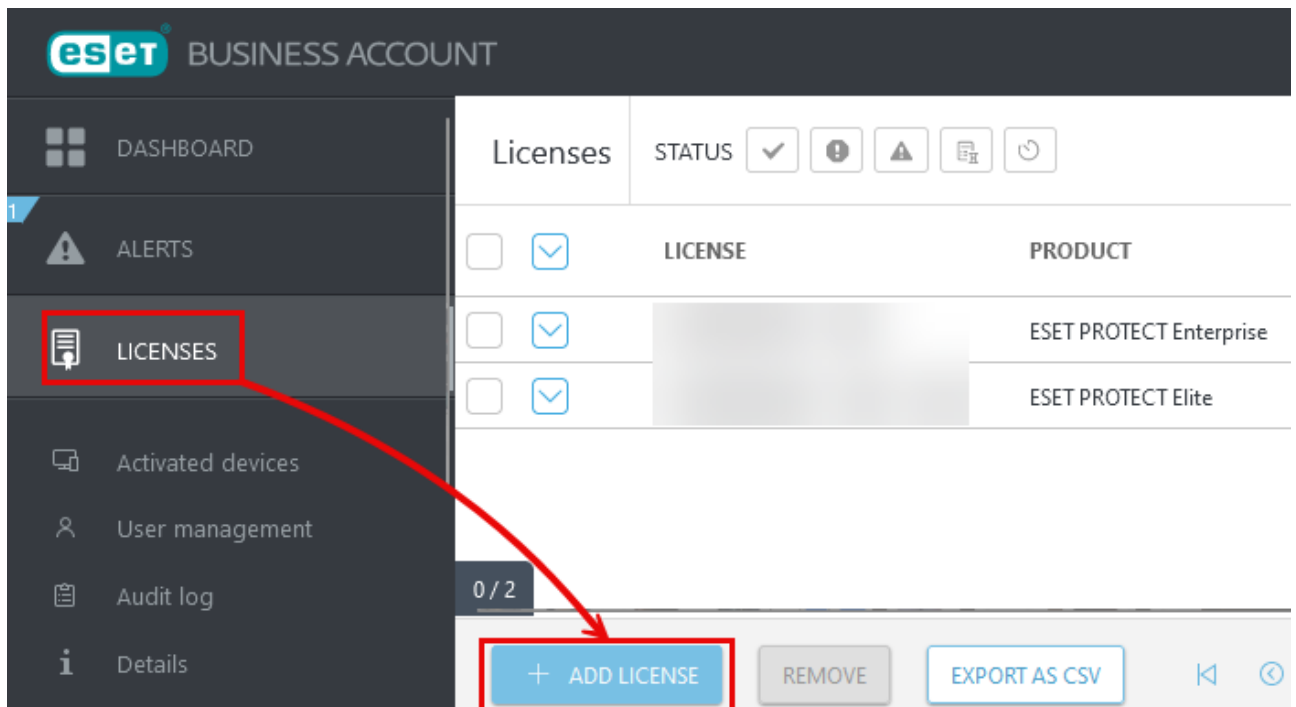
Prerequisites

- User account in EBA
- ESET LiveGuard Advanced license

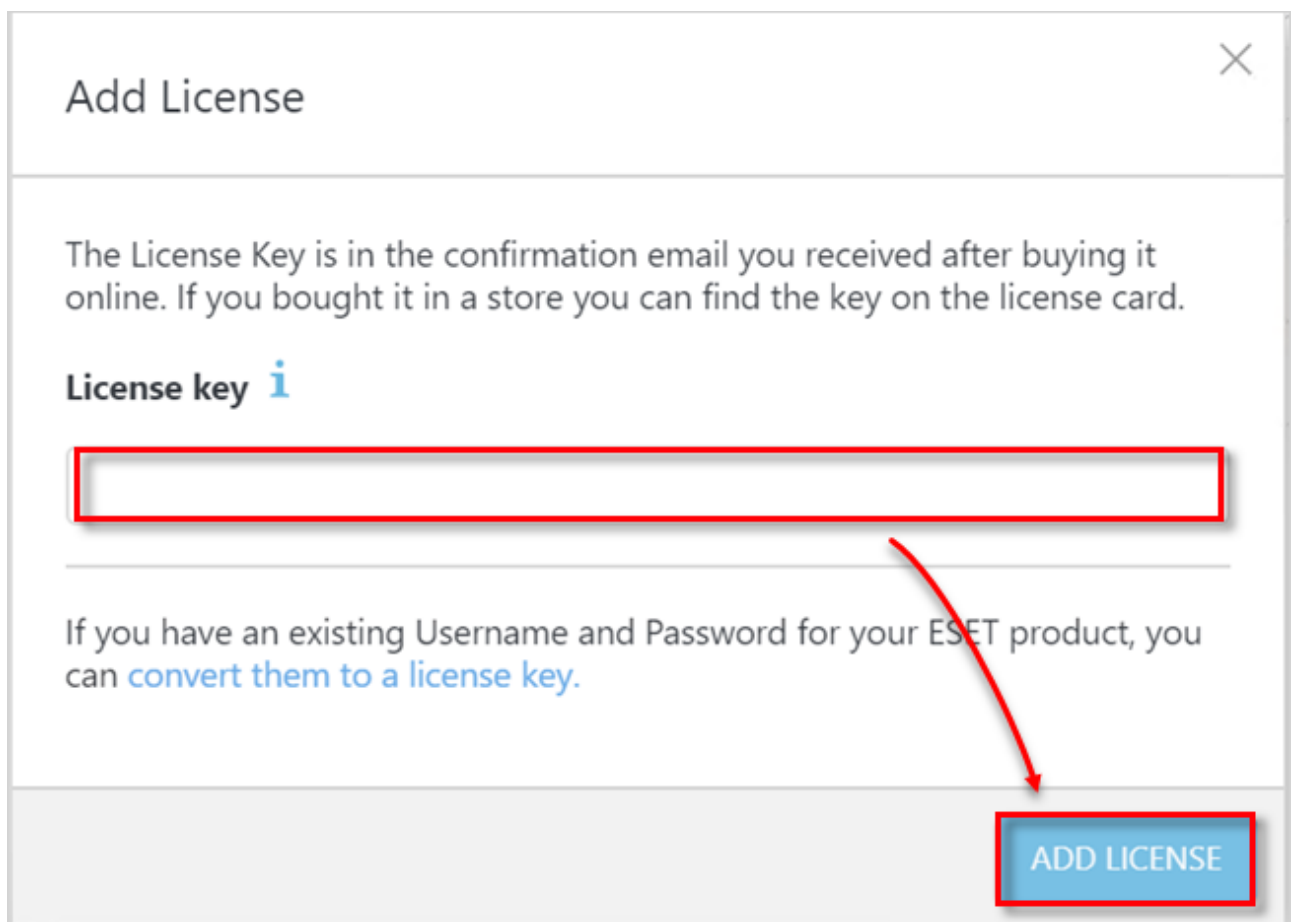
Import

1. Log in to your [EBA](#) account.

2. Click **Licenses > Add license > License Key**.



3. Type your ESET LiveGuard Advanced license key and click **Add License** to import the license.



4. Accept the end-user license agreement (EULA) if you agree with it. If the import was successful, a new

license item appears on your license list.

The ESET LiveGuard Advanced license can be bundled with other products or with seats of ESET LiveGuard Advanced for various ESET products:

- ESET LiveGuard Advanced for ESET Endpoint Security
- ESET LiveGuard Advanced for ESET Server Security
- ESET LiveGuard Advanced for ESET Mail Security

Synchronize EBA with ESET PROTECT On-Prem

Prerequisites

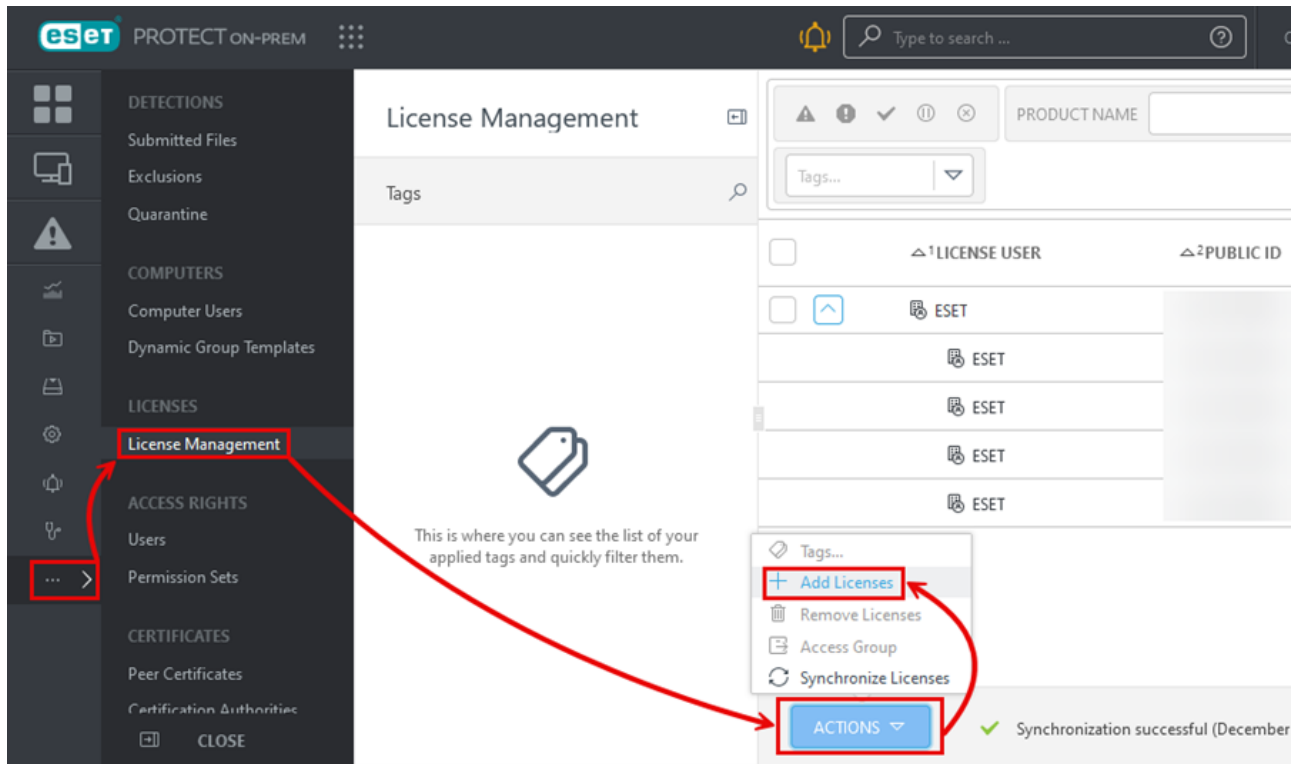
- ESET LiveGuard Advanced license imported in your EBA account
- ESET PROTECT On-Prem deployed
- working connection between ESET PROTECT Server and EBA portal



If you have already imported your EBA account to your ESET PROTECT Web Console, click **Synchronize** in the **License Management** section to force-update the license information in the Web Console. You do not need to add your EBA credentials again.

Synchronization

1. Log in to your ESET PROTECT Web Console as the Administrator or another user with sufficient [permissions](#).
2. Navigate to **More > License Management > Actions > Add license**.



3. Select **ESET Business Account** or **ESET MSP Administrator Login** and type your EBA account information.

4. Click **Add licenses** to add all licenses from your account to ESET PROTECT On-Prem.

Add License

You can add your license using one of the following options:

- ☒ ESET PROTECT HUB, ESET Business Account or ESET MSP Administrator
- ☐ License Key
- ☐ Offline License File

ESET PROTECT HUB, ESET Business Account or ESET MSP Administrator login



Password



[Show password](#)

4

ADD LICENSES

CANCEL

If you import the ESET LiveGuard Advanced license key directly to the Web Console, you get the following error:



"Failed to add license by license key: License is issued for a product that can not be managed with ESET PROTECT On-Prem. Please enter a different license."

Always import the ESET LiveGuard Advanced license via [EBA](#) or [ESET MSP Administrator](#).

Add license in ESET MSP Administrator

ESET MSP Administrator provides ESET LiveGuard Advanced license, which contains seats for:

- ESET LiveGuard Advanced for Endpoint Security and Server Security
- ESET LiveGuard Advanced for Mail Security



There are also tier licenses for ESET PROTECT, which contain seats for ESET LiveGuard Advanced:

- ESET PROTECT Complete
- ESET PROTECT Mail Plus
- ESET PROTECT Advanced

Verify if the ESET LiveGuard Advanced product is available

1. Log in to your ESET MSP Administrator account.

2. Click **Companies** > select the customer > **Details**.

3. In the **Available products** section, look for the **ESET LiveGuard Advanced** or a tier that contains ESET LiveGuard Advanced.

Accept the Terms of Use



Before you can add the license, you must accept the Terms of Use (for ESET LiveGuard Advanced) in the ESET MSP Administrator portal. If you do not have this option, your parent company, MSP Manager or a user with **Write** permission to your root company must accept the Terms of Use.

The screenshot displays the ESET MSP Administrator interface. On the left, a sidebar contains navigation links: 'License usage', 'Licenses', 'Activated units', 'Access rights', and 'Details'. The 'Details' link is highlighted with a red box and a red circle containing the number '2'. The main content area is titled 'Details' and shows information for 'My Second Company'. It includes fields for 'Email', 'Address' (Slovakia), 'Vat ID' (Not available), and 'Custom identifier' (Not available). Below this is the 'Available products' section, which lists several ESET products. 'ESET LiveGuard Advanced' is highlighted with a red box and a red circle containing the number '3'.

If your customer does not have one of the eligible tiers in the **Available products**, you need to add it to your account by your Distributor (or MSP Manager).

Add the ESET LiveGuard Advanced product

If the ESET LiveGuard Advanced product is not available in your customer's **Details** section, ask your Distributor or MSP manager to add the product to your ESET MSP Administrator account.

Follow the steps below to add a product to **Available products** from a Distributor account:

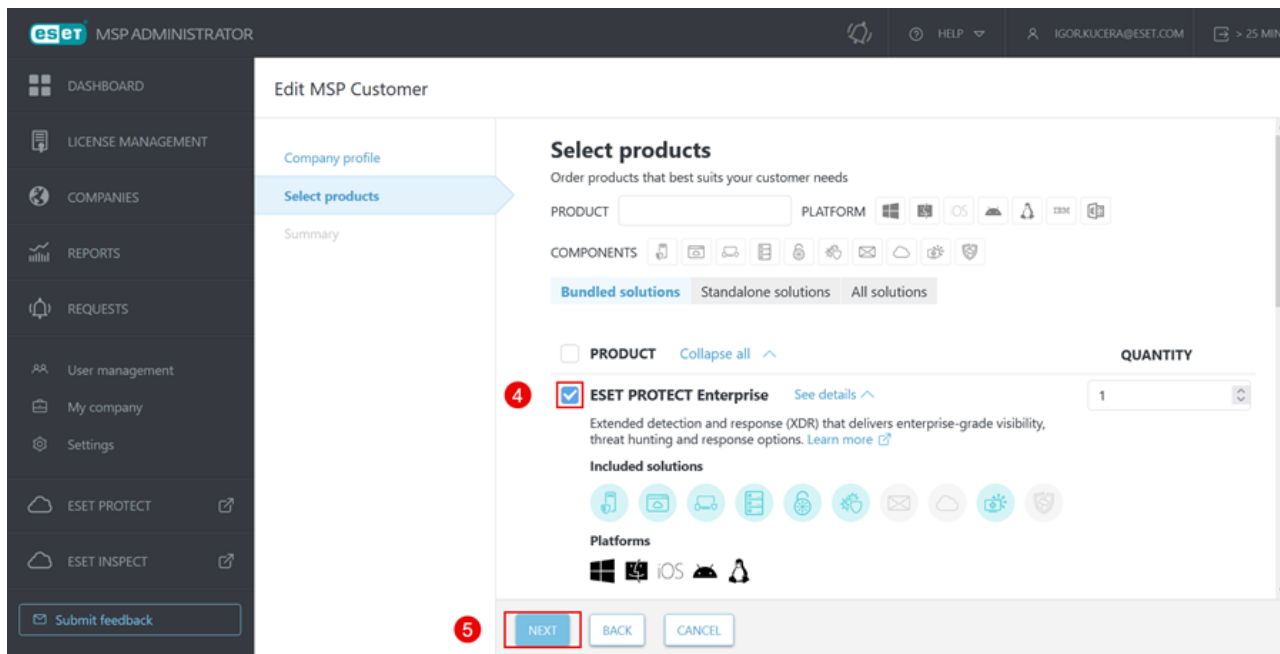
1. Log in to your ESET MSP Administrator Account.
2. Click **Companies** > select an MSP customer > **Details**.
3. Click **Edit**.

Details	
<div>License usage</div> <div>Licenses</div> <div>Activated units</div> <div>Access rights</div> <div> <div>i Details</div> <div>2</div> </div>	<div> <div> <div> <div>No description</div> </div> </div> </div> <div> <div>Email</div> <div>Address</div> <div>Vat ID Not available</div> <div>Custom identifier Not available</div> </div> <div> <div> <div>Available products</div> </div> <div>ESET Endpoint Antivirus for Windows</div> </div> <div> <div>3</div> <div>EDIT</div> <div>BACK</div> </div>

4.Click **Next**, and in the Select Products screen select ESET LiveGuard Advanced or another eligible license.

5.Click **Next**.

6.Review the changes in the **Summary** and click **Save**.



Add the ESET LiveGuard Advanced license to your MSP customer

If the customer has the ESET LiveGuard Advanced license available, you can add the license to the customer.

1. Log in to your ESET MSP Administrator Account.
2. Click **Companies** > select an MSP customer > **Licenses**.
3. Click **Add License** (or **Request License**).
4. Select the check box next to **ESET LiveGuard Advanced** and set the number of **Units**.
5. Click **Add**.

Units and subunits

The unit count is a number of ordered and billed seats of the license (tier). Each license tier can have a different ratio of units to subunits for each included product.

LICENSE	PRODUCT	CHANGE OPTIONS	STATUS	UNITS
FULL	ESET Endpoint Antivirus for Windows	↑↓	✓	0/1
FULL	ESET LiveGuard Advanced Tier unit	⌘	✓	0/1
	ESET LiveGuard Advanced for ESET Cloud Office Security	Subunit	0/2	
	ESET LiveGuard Advanced for Endpoint Security + Server Security	Subunit	0/1	
	ESET LiveGuard Advanced for Mail Security	Subunit	0/2	

Example of subunits distribution

ESET PROTECT Complete license tier:

esetMSP ADMINISTRATOR

Synchronize ESET MSP Administrator with ESET PROTECT On-Prem

Prerequisites

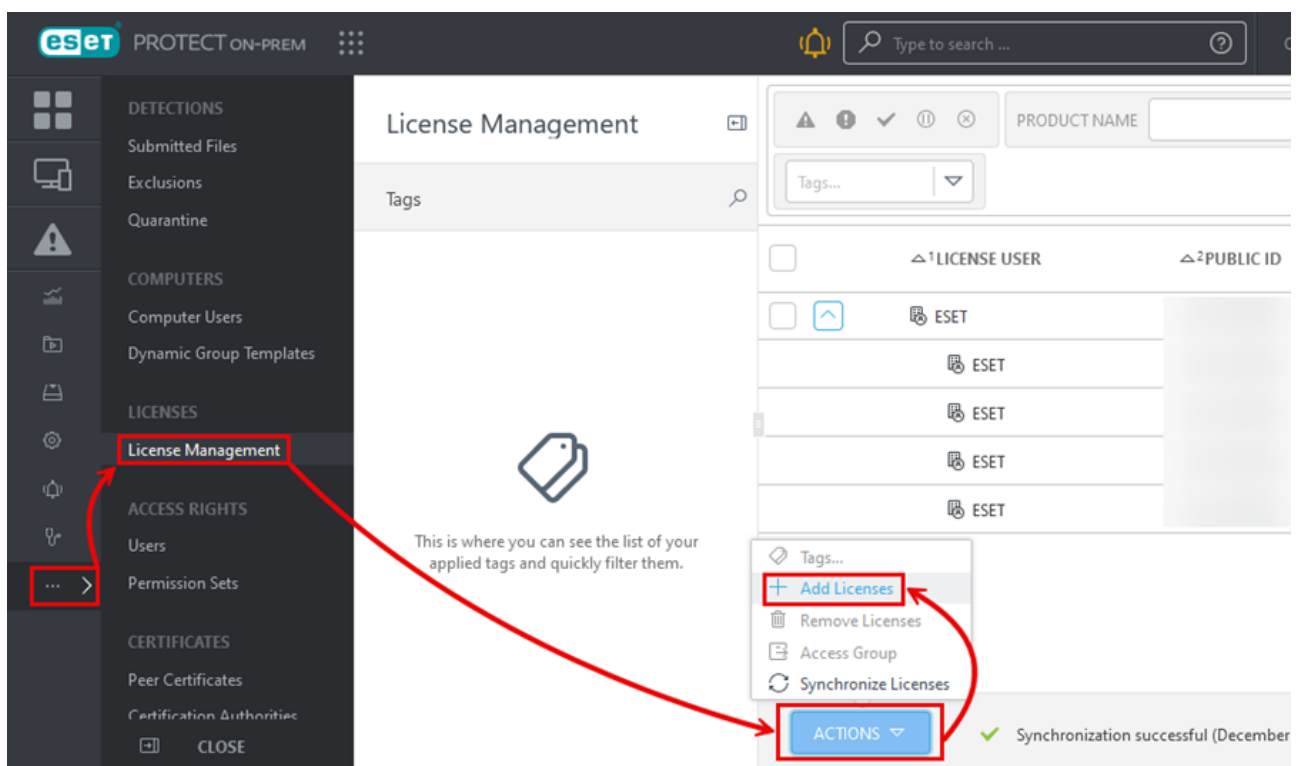
- ESET LiveGuard Advanced license in your ESET MSP Administrator account
- ESET PROTECT On-Prem deployed

- Must have a working connection between the ESET PROTECT Server and the ESET MSP Administrator portal

i If you have already imported your EBA account to your ESET PROTECT Web Console, click **Synchronize** in the **License Management** section to force-update the license information in the Web Console. You do not need to add your ESET MSP Administrator credentials again.

Synchronization

1. Log in to your ESET PROTECT Web Console as the Administrator or another user with sufficient [permissions](#).
2. Click **More > License Management > Actions > Add license**.



3. Select **ESET Business Account** or **ESET MSP Administrator Login** and type your ESET MSP Administrator account information.
4. Click **Add licenses** to add all licenses from your account to ESET PROTECT On-Prem.

Add License

You can add your license using one of the following options:

- ☒ ESET PROTECT HUB, ESET Business Account or ESET MSP Administrator
- ☐ License Key
- ☐ Offline License File

ESET PROTECT HUB, ESET Business Account or ESET MSP Administrator login



Password



[Show password](#)

4

ADD LICENSES

CANCEL

If you import the ESET LiveGuard Advanced license key directly to the Web Console, you get the following error:



"Failed to add license by license key: License is issued for a product that can not be managed with ESET PROTECT On-Prem. Please enter a different license."

Always import the ESET LiveGuard Advanced license via [EBA](#) or [ESET MSP Administrator](#).

Activate a group of computers

When activating a selection of computers on ESET PROTECT On-Prem or ESET PROTECT, use the [simplified activation process](#).

Prerequisites for ESET PROTECT On-Prem users

- ESET LiveGuard Advanced license imported in ESET PROTECT On-Prem
- Client machines with ESET Management Agent version not earlier than the version of the Server component
- Activated ESET security product with [support](#) for ESET LiveGuard Advanced

Prerequisites for ESET PROTECT users

- ESET LiveGuard Advanced license imported in EBA.
- ESET Management Agent is the latest version on all client computers.
- ESET security products on client computers (with [support](#) for ESET LiveGuard Advanced) are installed and activated.

Activation task

1. [Log in to the Web Console](#).
2. Click **Tasks > New > Client task**.

eset PROTECT ON-PREM

Search: Type to search ...

Tasks

Task Types

- Client Tasks
 - ESET Security Product
 - ESET PROTECT
 - Operating System
 - Mobile
 - Full Disk Encryption
- Server Tasks
 - Static Group Synchronization
 - Agent Deployment
 - User Synchronization
 - Generate Report
 - Rename Computers
 - Delete Not Connecting Computers

Tags

	NAME	TAGS	PR...	TYPE
<input type="checkbox"/>	Mod...		✓	Mod...
<input type="checkbox"/>	activ...		✓	Prod...
<input type="checkbox"/>	Upd...		✓	Ope...
<input type="checkbox"/>	Upd...		!	Ope...
<input type="checkbox"/>	Exp...		✓	Exp...
<input type="checkbox"/>	Upd...		!	Ope...
<input type="checkbox"/>	Reb...		✓	Shut...
<input type="checkbox"/>	Soft...		!	Soft...
<input type="checkbox"/>	Exp...		✓	Sysl...
<input type="checkbox"/>	Prod...		✓	Prod...

+ Client Task

+ Server Task

Client Task

NEW...

ACTIONS

^ I am using ESET PROTECT

The screenshot displays the ESET Protect web interface. On the left, a dark sidebar contains navigation options: DASHBOARD, MANAGED CUSTOMERS, COMPUTERS, DETECTIONS, VULNERABILITIES, Patch Management, Reports, **Tasks** (highlighted with a red box), Installers, Policies, Notifications, Status Overview, ESET Solutions, and More. A red arrow points from the 'Tasks' menu item to the 'NEW...' button at the bottom of the task list. The main content area is titled 'Tasks' and features a table with columns for checkboxes, task names, and actions. The task list includes items like 'Stop managing - via context menu', 'Product Activation (Enable Vulnerability & Patch Management) - via...', 'Update Operating System - via context menu', 'Modules Update', 'Product Activation (Enable Vulnerability & Patch Management) - via...', 'Product activation - via ESET LiveGuard', 'act', and 'Reboot Computer - via context menu'. The bottom of the interface shows a 'NEW...' button with a dropdown arrow, which is highlighted with a red box and pointed to by a red arrow from the sidebar 'Tasks' menu item.

3.Type a name for your activation task and select **Product Activation** as the **Task type**.

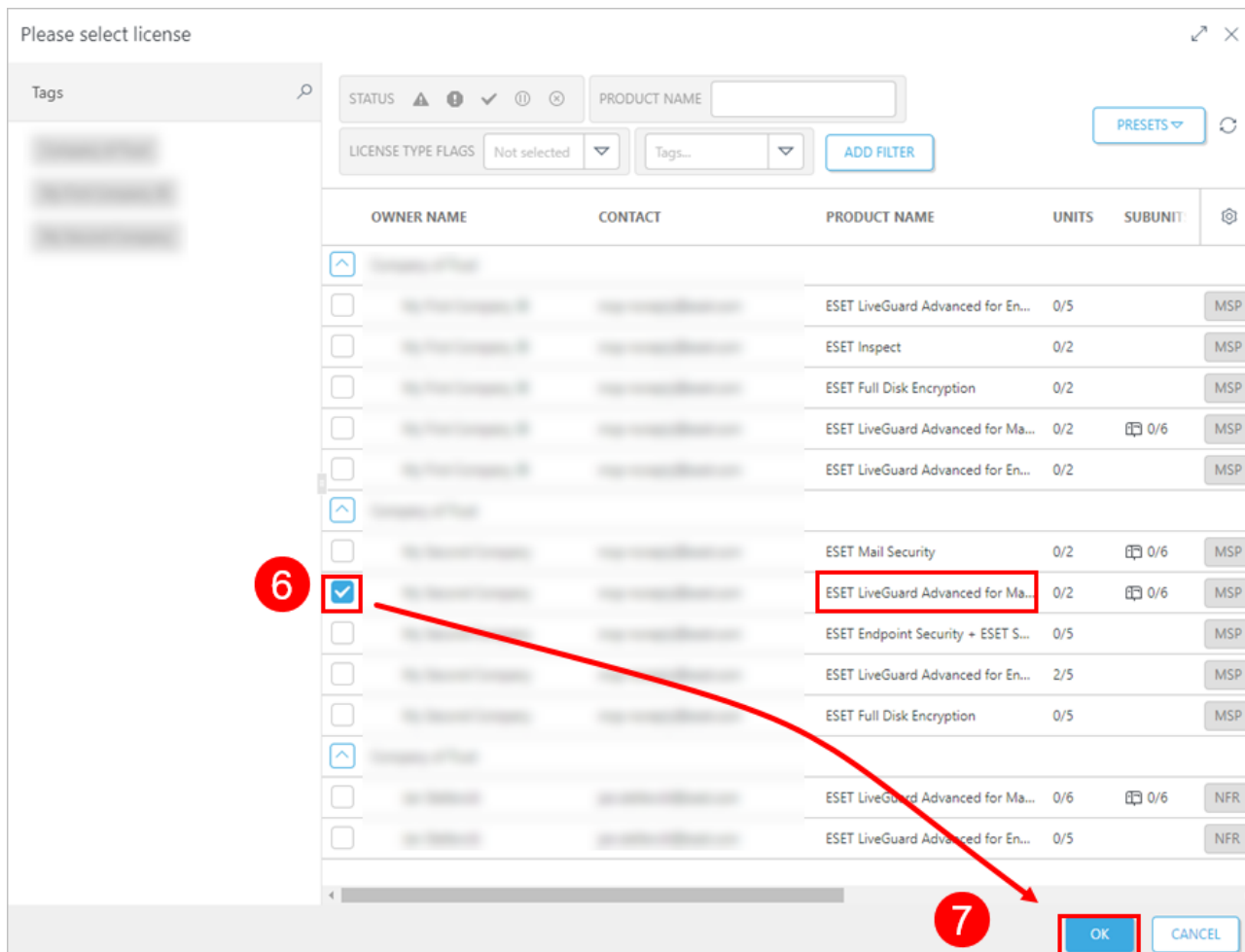
4.Click **Continue**.

The screenshot shows a web interface for creating a new client task. On the left is a sidebar with 'Basic' (selected), 'Settings', and 'Summary'. The main form has several fields: 'Name' (containing 'New Task'), 'Tags' (with a 'Select tags' link), 'Description' (empty), 'Task Category' (dropdown menu showing 'All Tasks'), and 'Task' (dropdown menu showing 'Product Activation'). A red circle with the number '3' is next to the 'Tags' field, and a red circle with the number '4' is at the bottom. A red arrow points from the 'Basic' tab to the 'Task' dropdown. At the bottom are four buttons: 'BACK', 'CONTINUE' (highlighted with a red box), 'FINISH', and 'CANCEL'.

5. Click the license to get to the license list and select the ESET LiveGuard Advanced license.

6. The ESET LiveGuard Advanced license is a part of a tier. Expand the tier and select a product license to use.

7. Click **OK**.



8. Click **Summary** for an overview of the task settings.

9. If the task is correct, click **Finish**.

10. After you create the task, you need to schedule it. Click **Create Trigger** in the alert window.

11. Type a **Trigger Description** and click **Continue**.

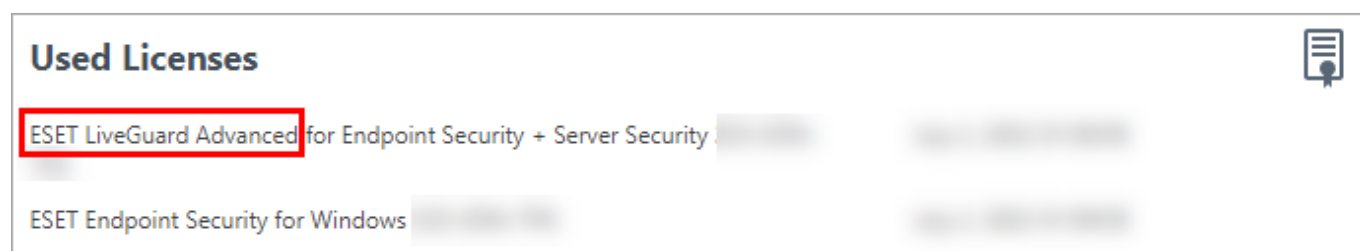
12. Click **Add Computers** or **Add Groups** to add machines to be activated. Ensure that the clients you select have products that are compatible with the license you selected in step 6. Click **OK** and then click **Continue**.

13. You can select a **Trigger type**. We recommend using the default option: **As Soon as Possible**, which runs the task immediately after the trigger. If you select another setting, [Advanced Settings - Throttling](#) becomes available.

14. Click **Finish** to schedule the activation task.

After you complete activation, the license will become visible in the machine details. In the Web Console, click

Computers, select a machine and then click **Show details > Details > Products and Licenses**.



Activate selected computers

Prerequisites for ESET PROTECT On-Prem and ESET PROTECT users

- ESET LiveGuard Advanced license or a protection tier imported in ESET PROTECT On-Prem
- Client machines with ESET Management Agent version compatible with the version of the Server component
- Activated ESET security product with [support](#) for ESET LiveGuard Advanced

Prerequisites for ESET PROTECT users

- ESET LiveGuard Advanced license or a protection tier imported in EBA.
- ESET Management Agent is the latest version on all client computers.
- ESET security products on client computers (with [support](#) for ESET LiveGuard Advanced) are installed and activated.

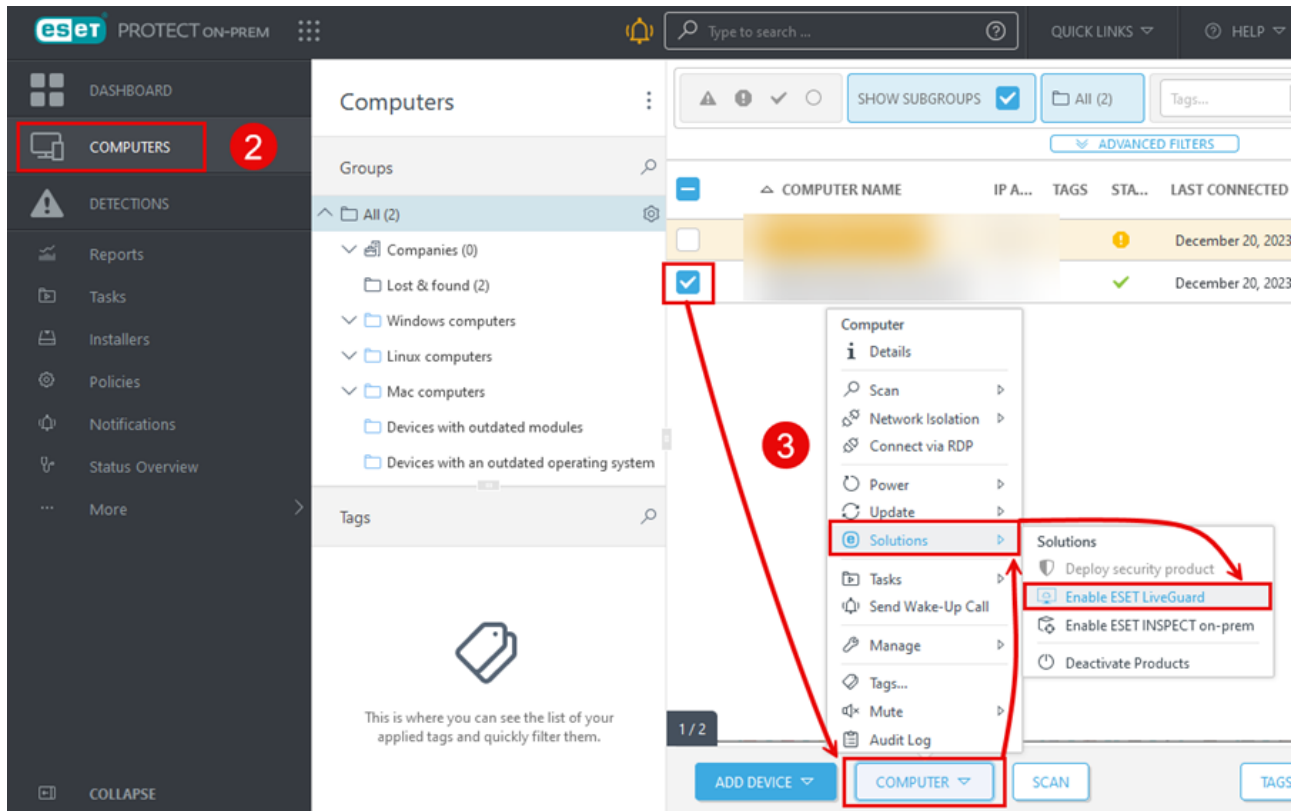


- Never use a ESET LiveGuard Advanced license imported to a remote management console using a license key. If you have such a license, remove it and re-import it [using EBA](#) or [ESET MSP Administrator](#).
- Always ensure your target computer has an activated and a [supported product](#) before using the ESET LiveGuard Advanced license.

Activate and enable ESET LiveGuard Advanced in ESET PROTECT On-Prem and ESET PROTECT

ESET PROTECT On-Prem and ESET PROTECT offer simplified activation:

1. [Log in to the Web Console](#).
2. Click the **Computers** menu icon.
3. Select the check box next to computers you want to activate and click **Actions > Enable ESET LiveGuard**.



4. Choose between **Optimal protection** and **Basic protection**.

5. Verify the computer where ESET LiveGuard Advanced will be activated in Targets.

6. Click **Enable** to execute the task.

Select the computers on which you want to enable ESET LiveGuard Advanced. A license and a policy will be assigned automatically. If no paid license is available, a trial license will be used.

How is a license selected? 

☒ **Optimal protection** **Recommended**

At-risk files, including document types that support macros, will be sent to a secure ESET server for automated scanning and behavioral analysis. Access to the files will be limited until they've been evaluated as safe. The ESET LiveGrid® feedback system will be enabled.

☐ **Basic protection**

This provides a basic level of security where only a limited set of files will be scanned. The protection is limited compared to the recommended setting. The ESET LiveGrid® feedback system will be enabled.

● **Targets**

Win 6 ✕

ENABLE

CANCEL

The management console sends the activation task and policy to the selected computer. ESET LiveGuard Advanced is enabled after the next connection of ESET Management Agent, usually within a few minutes.

Remote installation and activation

The ESET PROTECT On-Prem or ESET PROTECT installation task can install the ESET security product and activate and enable ESET LiveGuard Advanced in one action.

1. Log in to your ESET PROTECT Web Console.
2. Click **Tasks > New > Client task**.
3. Type a name for the task and select **Software install** in the **Task** drop-down menu.
4. Click **Continue**.
5. Click **<Choose package>** and select the appropriate ESET product.

6. Select an ESET license to activate the product.

7. Check the box next to **Activate ESET LiveGuard**.

8. Select the appropriate ESET LiveGuard Advanced license.

9. Check the box next to **I accept** if you agree with the security product's EULA and Privacy Policy.

10. Click **Finish**.

New Client Task

Tasks > Software install Task

Basic

Settings

Summary

Software installation settings

Package to install ?

☒ Install package from repository
☐ Install by direct package URL

Choose operating system

☒ Windows
☐ Linux
☐ macOS
☐ Android

Choose package from repository

ESET Endpoint Antivirus; version

Install the latest version

☒ Allow to install the latest product version for which the EULA is accepted

ESET license ?

ESET Endpoint Security + ESET Server Security.

☒ **Activate ESET LiveGuard**

ESET LiveGuard will be activated with the license below on the computers targeted by this task.

Important: To enable and use the functionality, it has to be switched on in the computer's configuration. For example, by assigning the "ESET LiveGuard - Enable" policy to those computers.
[More information about ESET LiveGuard](#)

License: ESET LiveGuard Advanced for Endpoint Security + Server Security

☒ I accept the [End User License Agreement](#) and acknowledge the [Privacy Policy](#).

Protection settings

The ESET LiveGrid® feedback system

☒ Enable The ESET LiveGrid® feedback system (recommended)

Detection of Potentially Unwanted Applications

☒ Enable detection of potentially unwanted applications

11. Click **Create Trigger**.

12. Type a name for the trigger and click **Continue**.

13. Click **Add targets** and select the appropriate computers or groups. Click **OK**.

14. Click **Finish** to execute the installation task immediately.

How to enable and configure the ESET LiveGuard Advanced service

Activation prerequisites

- [ESET Business Account](#) or [ESET MSP Administrator](#) account linked to a [supported management console](#)
- Installed or deployed [supported management console](#)
- Installed [compatible ESET security products](#)
- Valid ESET LiveGuard Advanced license
- [Activated Security products with ESET LiveGuard Advanced license](#)
- ESET LiveGuard Advanced enabled in policies for compatible Security products

Enable ESET LiveGuard Advanced on your security product

- [ESET Endpoint Security](#)
- [How do policies work and how do I create a new policy?](#)

Enable ESET LiveGuard Advanced on ESET Cloud Office Security

See the [ESET Cloud Office Security Online Help](#) or see the [step-by-step guide](#).

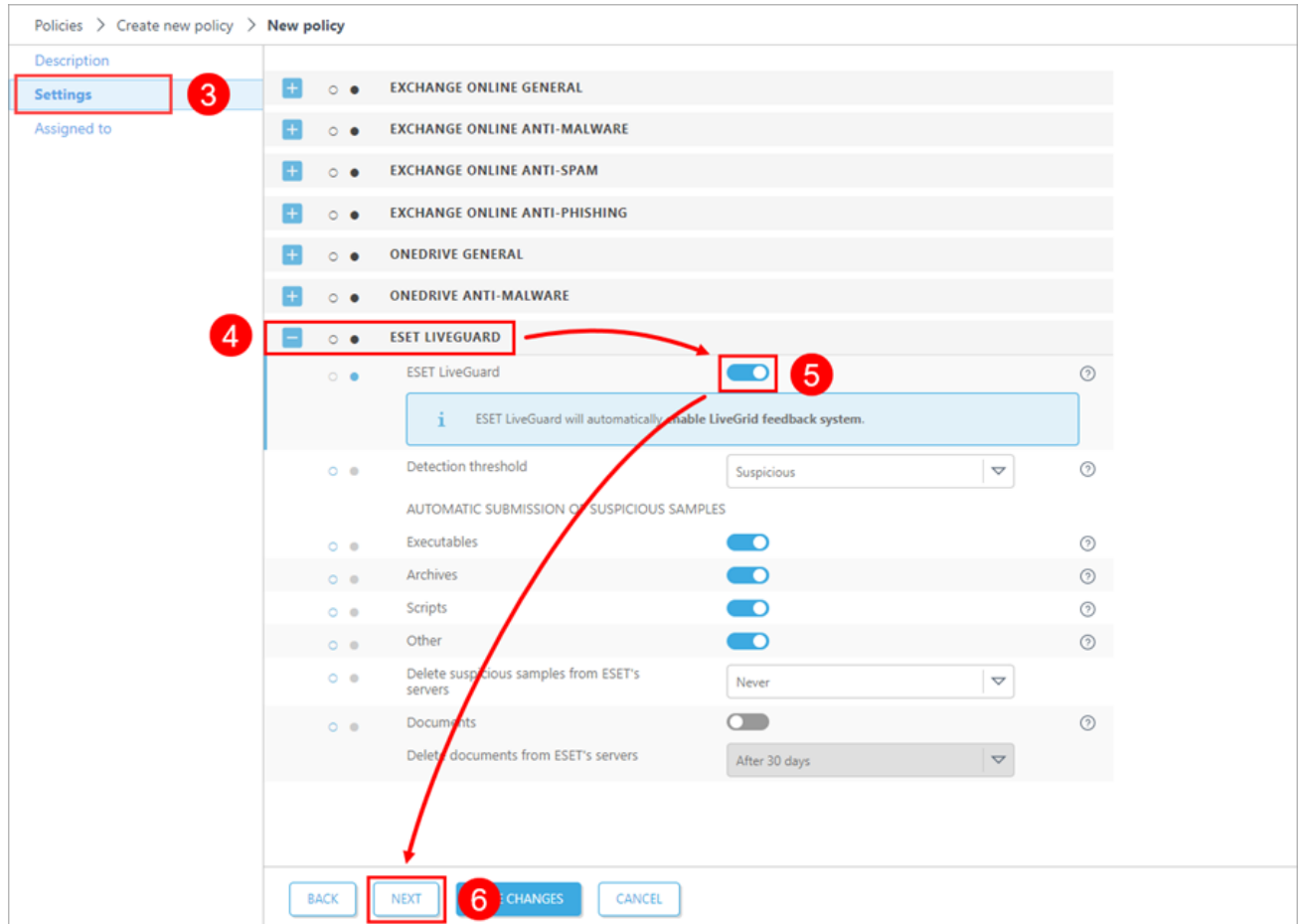
Configuration of ESET security product

ESET Cloud Office Security users

To use ESET LiveGuard Advanced in ESET Cloud Office Security, create a new policy or configure an existing one. Users or groups assigned with this policy will have additional protection. For more information, see [Protection settings for ESET LiveGuard Advanced](#).

 [Set up the ESET Cloud Office Security policy](#)

1. Log in to ESET Cloud Office Security.
2. Click **Policies**, select a policy and click **Edit**.
3. Click **Settings**.
4. Expand **ESET LiveGuard** section.
5. Click the **ESET LiveGuard** toggle.
6. Click **Next**.



ESET management console users

To enable ESET LiveGuard Advanced service on a client machine, a user needs to fulfill [requirements](#) and create a [policy](#) to set the service.

In the ESET PROTECT Web Console, create a new policy or edit an existing one and assign it to machines where you want to use the ESET LiveGuard Advanced.

i If you enable the ESET LiveGuard Advanced on a machine where the service is not [activated](#) by the license, the setting will not apply. Other settings in the policy would apply.

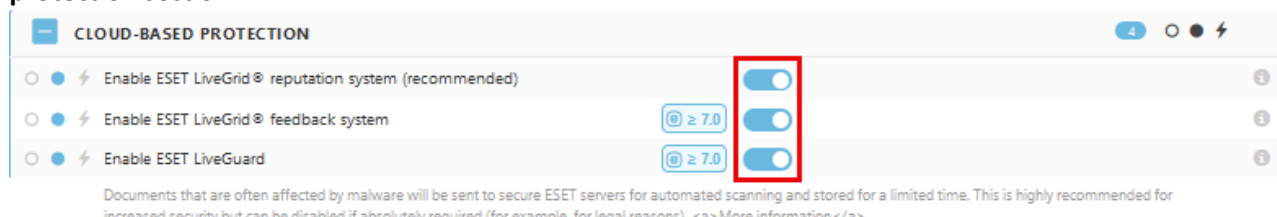
ESET LiveGuard Advanced Settings

1. [Log in to Web Console](#) of your ESET management console and create or edit a [policy](#).

2. In the **Settings** section, select your product and navigate to:

Policy	Setting
ESET Endpoint for Windows	Detection Engine > Cloud-Based protection
ESET Mail Security for Microsoft Exchange (V6+)	Computer > Cloud-Based protection
ESET Server Security for Microsoft Server (V6+)	Detection Engine > Cloud-Based protection
ESET Endpoint for Linux (V7+)	Detection Engine > Cloud-Based protection
ESET Server/File Security for Linux (V7+)	Detection Engine > Cloud-Based protection

3. To enable the ESET LiveGuard Advanced, you have to switch on all three settings in the **Cloud-Based protection** section.



i Starting from ESET Endpoint for Windows version 10.1 or later, submission of documents is enabled by default.

Section: Cloud-Based protection	Description
Enable ESET LiveGrid® reputation system (recommended)	Using reputation information from ESET LiveGrid®.
Enable ESET LiveGrid® feedback system	Submitting files to ESET cloud.
Enable ESET LiveGuard Advanced	Submitting files for analysis in ESET LiveGuard Advanced.

4. You can refine which files are sent to ESET cloud when they are detected or identified as suspicious.

Section: Submission of samples	Description and recommendation
Manual submission of samples	Enables the option to manually submit samples to ESET (Windows products only)
Automatic submission of detected samples	Select what kind of samples are automatically submitted to ESET for analysis when detected by the Detection engine.
Executables, Archives, Scripts, Other	Select types of files that are automatically submitted to the ESET cloud for analysis if the local Detection engine does not detect them. We recommend allowing submitting of all file types.
Possible Spam emails	Submission of possible spam emails. (ESET Endpoint for Windows only)
Delete executables, archives, scripts, other samples and possible spam emails from ESET's servers	Action after the analysis is done.
Documents	Submitting of documents. This option is enabled by default.
Delete documents from ESET's servers	Action after the analysis is done.
Exclusions	List of file extensions which excludes files from submitting. Extensions are added in the following format: *.ext? where: * stands for the filename ext stands for the file type extension ? stands for one optional character. This is optional.

Section: Submission of samples	Description and recommendation
Maximum size of samples (MB)	Maximum size of a submitted file.

5.Set up detection threshold and actions taken after a file has a positive result above the threshold.

Section: ESET LiveGuard Advanced	Description and recommendation
Detection threshold	Status of the result of the analysis which triggers the Action after detection .
Action after detection	Action which the ESET security product does if the analyzed file has a result equal to or above the Detection threshold .
Maximum wait time for the analysis (min)	Maximum wait time for the analysis result before the mail is delivered or the downloaded file is made available.
Proactive protection	Proactive protection setting. You can enable the execution of files whose analysis is not yet finished.

6.Finish the [policy](#) by selecting computers or groups to be assigned by the policy. New settings are applied after the next replication between Server and Agents (usually a few minutes).

Policy management

Policies allow you to enforce some or all client settings remotely from a [management console](#) to client machines. Each policy is specific to a single ESET business product, and you apply it to groups or individual client machines. When multiple policies are applied to a single machine, policies are combined and applied.

ESET Management Agent must be installed and configured to connect to the management console for policies to take effect on clients.

Create a new policy

1.[Log in to the Web Console](#).

2.Click **Policies > New Policy**.

ESET PROTECT ON-PREM

Policies

ACCESS GROUP [Select](#) [All \(62\)](#)

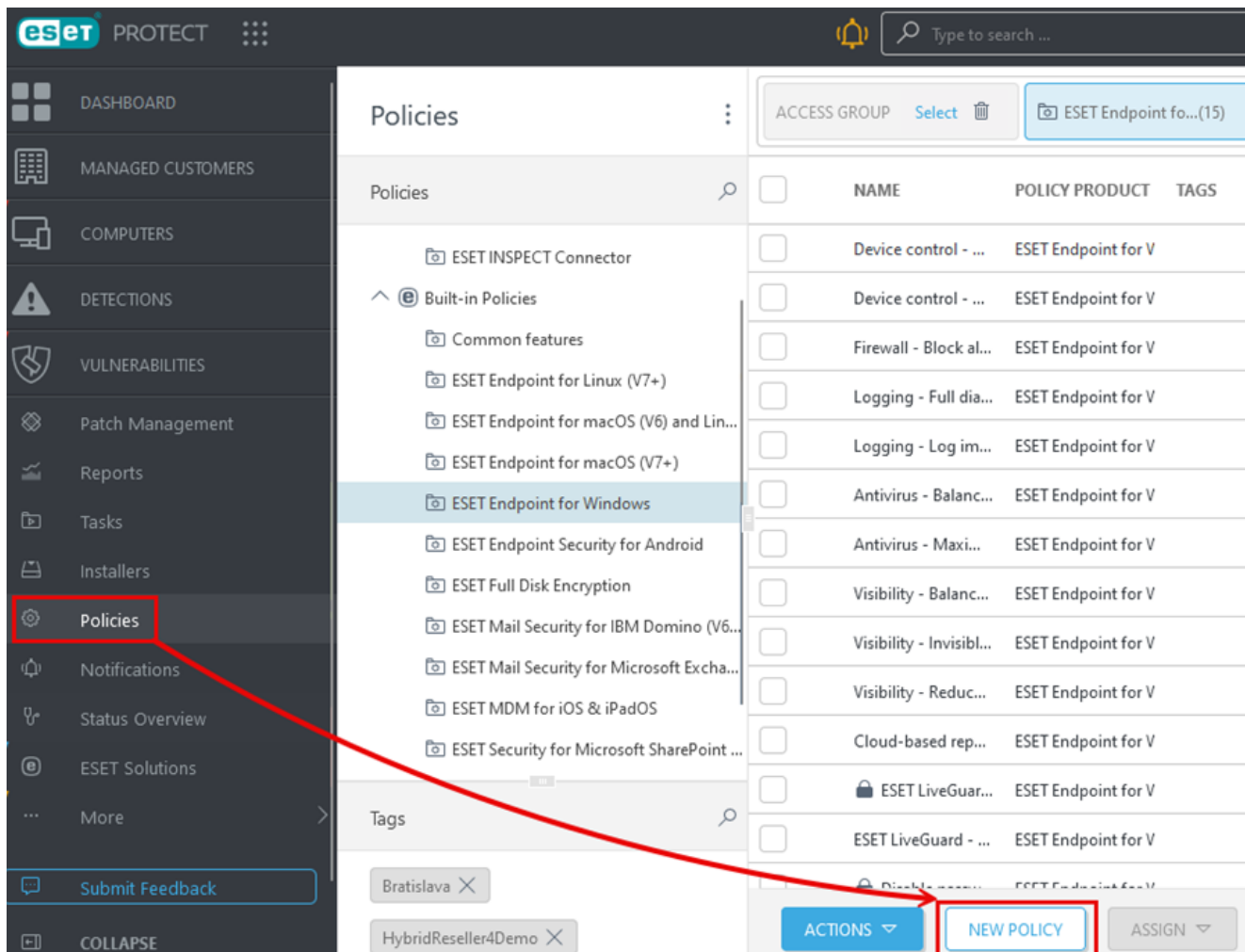
Tags...

<input type="checkbox"/>	NAME	POLI...	TAGS	DI
<input type="checkbox"/>	HTTP ...	ESET Eni		ES
<input type="checkbox"/>	HTTP ...	ESET Eni		ES
<input type="checkbox"/>	HTTP ...	ESET Eni		ES
<input type="checkbox"/>	HTTP ...	ESET Eni		ES
<input type="checkbox"/>	HTTP ...	ESET Mæ		ES
<input type="checkbox"/>	HTTP ...	ESET Ser		ES
<input type="checkbox"/>	HTTP ...	ESET Shi		ES
<input type="checkbox"/>	Appli...	ESET Mæ		ES
<input type="checkbox"/>	Conn...	ESET Mæ		Aç
<input type="checkbox"/>	Conn...	ESET Mæ		Re
<input type="checkbox"/>	Conn...	ESET Mæ		Re
<input type="checkbox"/>	Gener...	ESET Vir		Th

ACTIONS **NEW POLICY**

This is where you can see the list of your applied tags and quickly filter them.

^ I am using [ESET PROTECT](#)



3.Type the name and description for a policy and click **Continue**.

4.Select the applicable ESET security product for the policy and click **Continue**.

5.Select the applicable computers or computer groups that you want to assign the policy to and click **Continue**.

6.The **Summary** section gives an overview of policy settings. Click **Finish** to apply the policy.

[How to set up the ESET LiveGuard Advanced policy?](#)

How policies work

In the policy wizard, select the ESET product you want to create a policy for.

Each setting (line) consists of:

- Status
- Title
- Version limitation (optional)

- Setting value
- Tooltip (not all settings have tooltips)



A setting's status is displayed if the setting is defined in this policy and also if it is forced over other policies. Examples of setting status indicators are shown below:



If more policies are applied on a single machine, or their settings are inherited, policies are merged (based on order). Read more about policies in the ESET PROTECT On-Prem [documentation](#).

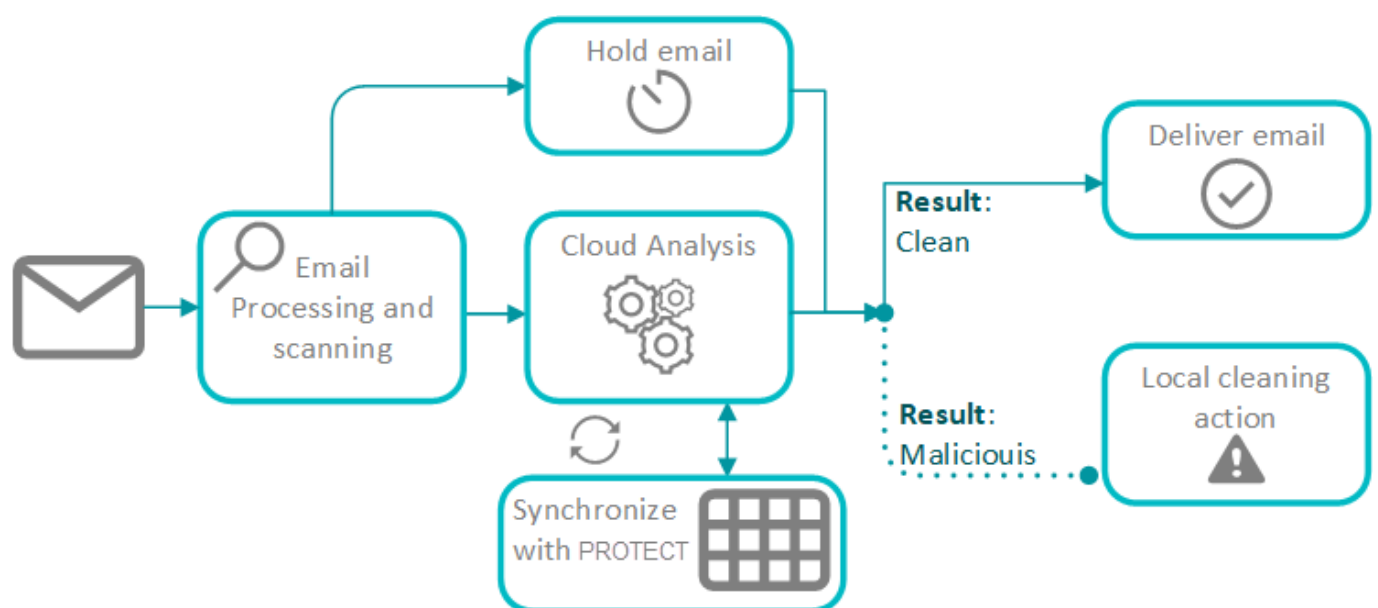
Using ESET LiveGuard Advanced

ESET LiveGuard Advanced workflow for ESET Mail Security

Each email received and detected by ESET Mail Security is scanned and delivered. If the email is evaluated as suspicious, it is held for a pre-set period and sent for analysis using [detection layers](#).

ESET LiveGuard Advanced analyzes files and delivers results back to your ESET security product. The product will perform local cleaning based on the results of the analysis and the policy settings of each machine.

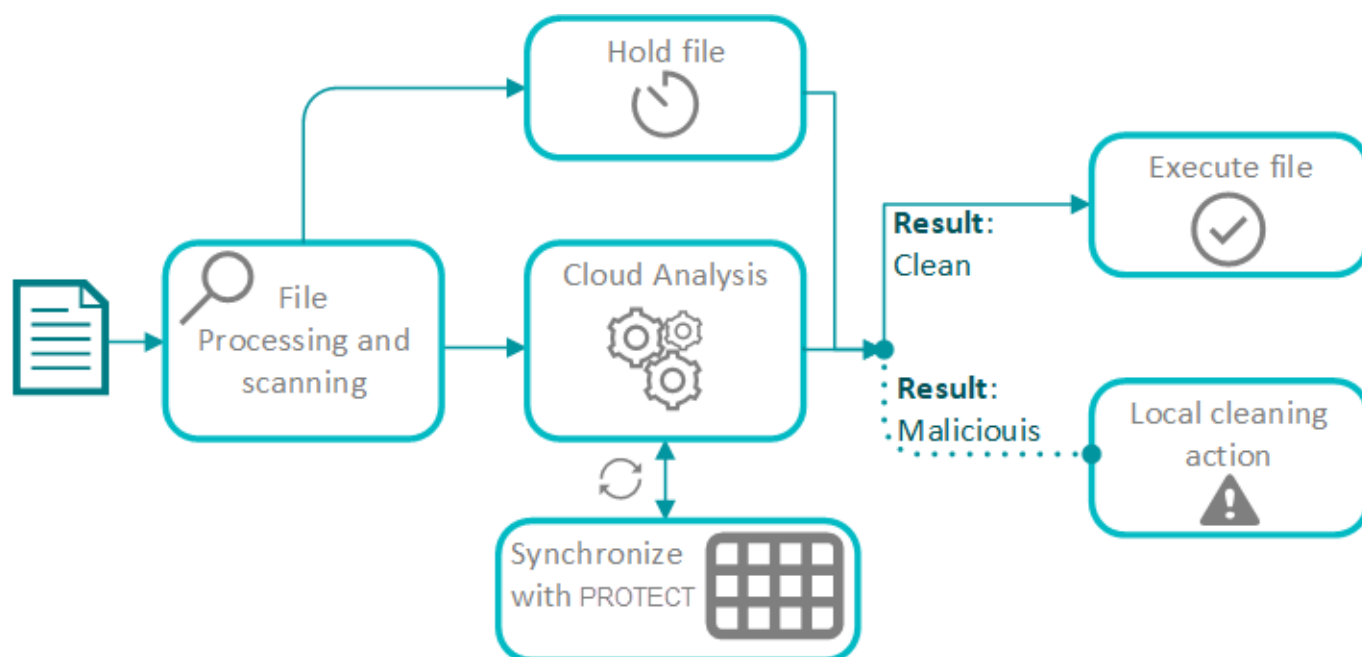
See the detailed workflow below for ESET Mail Security.



ESET LiveGuard Advanced workflow for ESET Endpoint Security / ESET Server Security

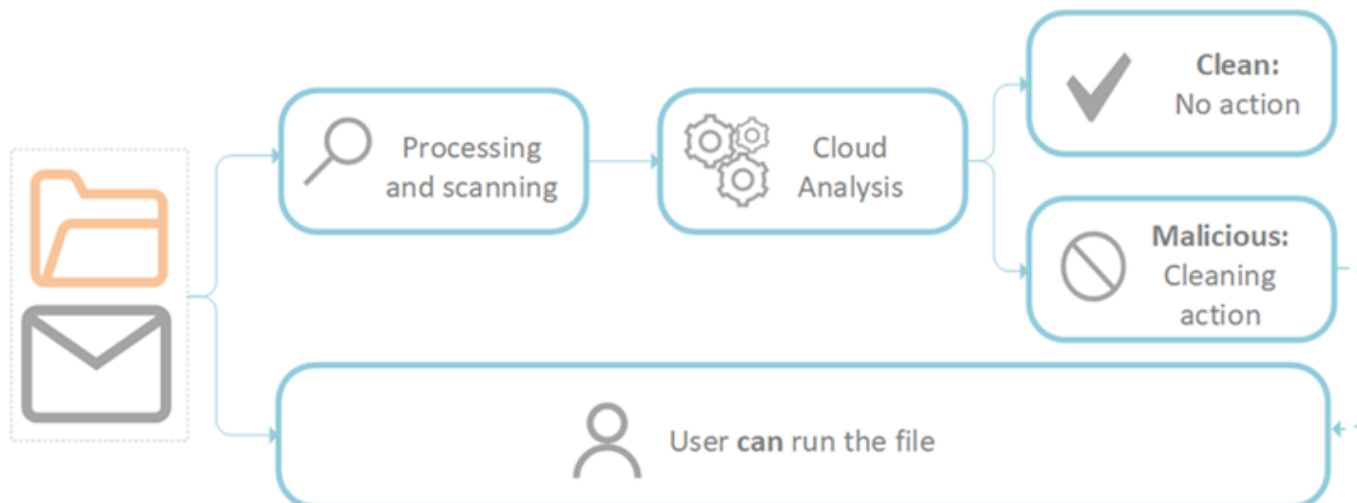
New or incoming files of the selected formats detected by ESET Endpoint Security / ESET Server Security are scanned and opened. If the file is evaluated as suspicious, it is sent for [analysis](#). This is a part of [proactive protection](#). You can set up the waiting period during which the file is blocked and the user needs to wait for the result of the analysis. The ESET cloud stores the results of the analysis to a cloud database. The ESET security product will perform local cleaning based on the results of the analysis and the policy settings of each machine (process is killed immediately or on next execution).

See the detailed workflow below for ESET Endpoint Security / ESET Server Security.



ESET LiveGuard Advanced workflow for ESET Cloud Office Security

Each file detected by ESET Cloud Office Security is scanned and opened. If the scanner considers the file suspicious, it sends it for analysis. The ESET cloud stores the results of the analysis to a cloud database. ESET Cloud Office Security performs cleaning actions based on the analysis results and the security policy settings. For more information on ESET Cloud Office Security policies, see [Protection settings for ESET LiveGuard Advanced](#).



ESET Mail Security

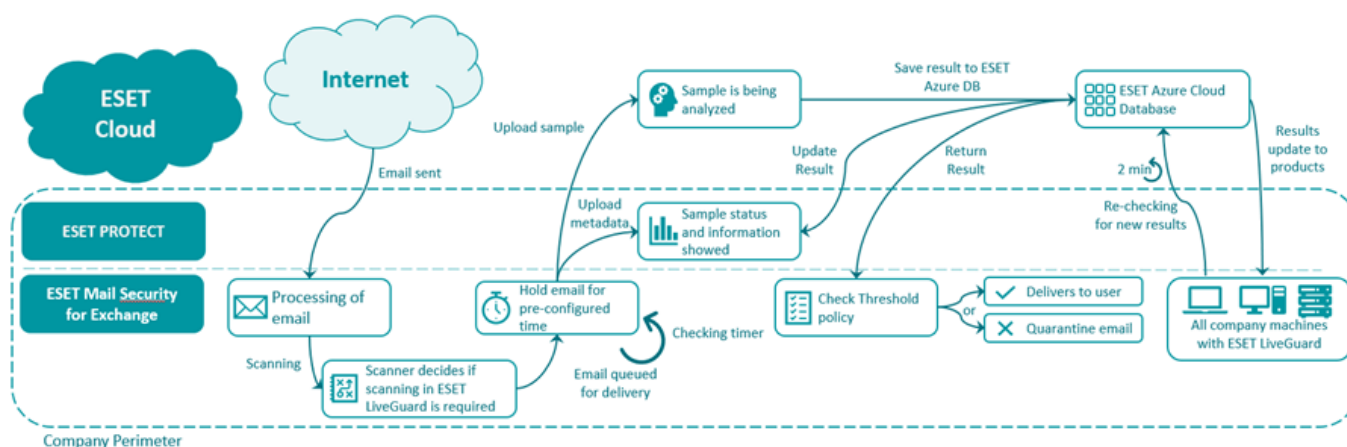
Each email detected by ESET Mail Security with ESET LiveGuard Advanced-activated follows the submission process shown below. Policy settings define the following:

- hold time (only for protection of mail boxes)
- specific security levels
- action after detection (only for protection of host server)

ESET Mail Security is protecting the host server and also mail boxes

! ESET Mail Security with ESET LiveGuard Advanced protects the mail boxes as described below. The protection of the host machine is the same as described for [ESET Server Security](#).

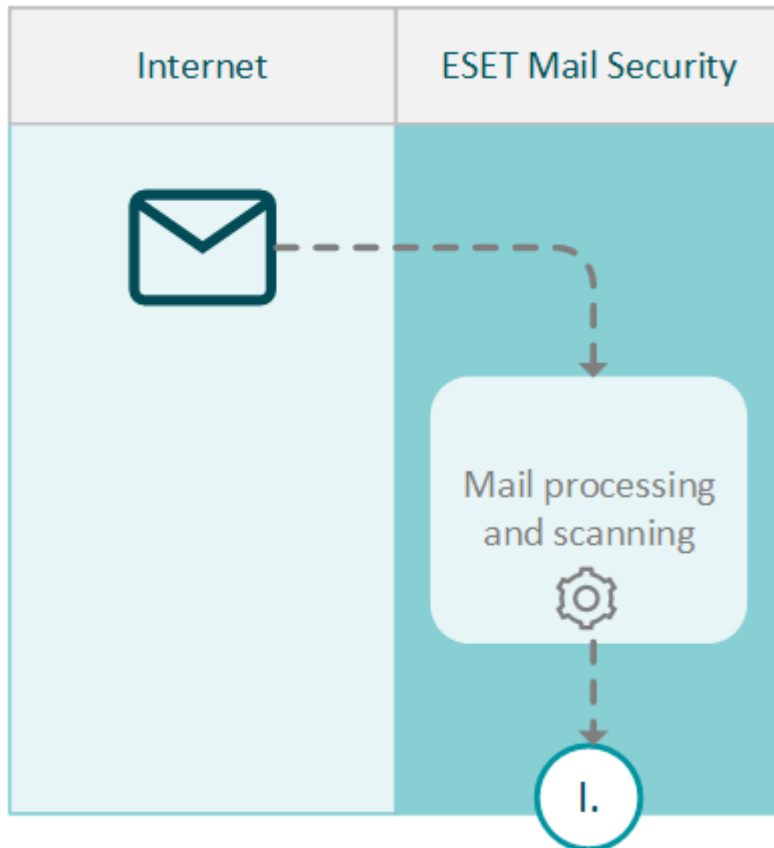
How ESET LiveGuard Advanced works for Mail Security for Exchange



Email analysis follows a four-step process:

1. Email scanning

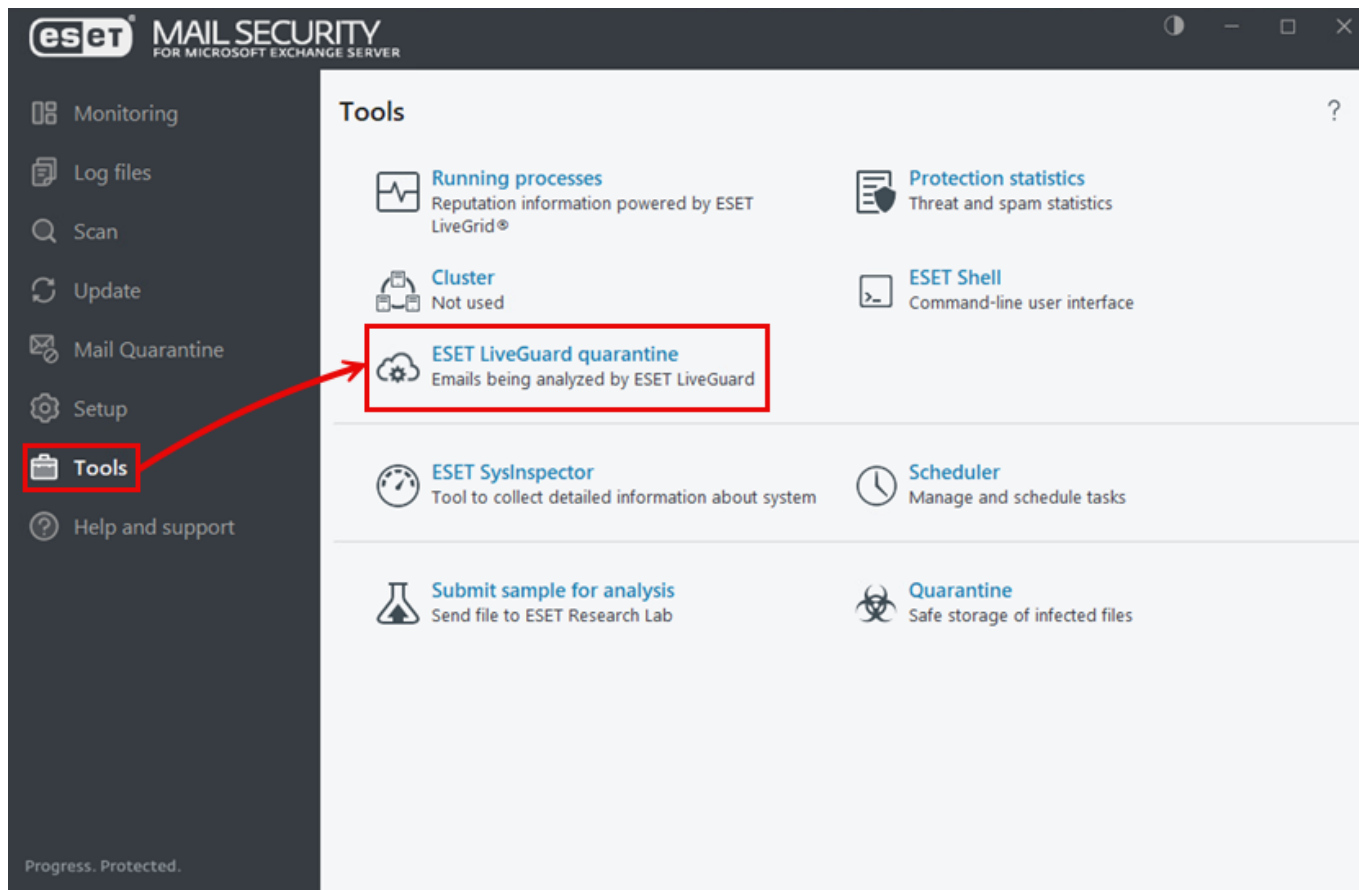
The mail is downloaded from the internet or another untrusted source. Your ESET security product processes and scans the mail.



2. Email analysis and delivery

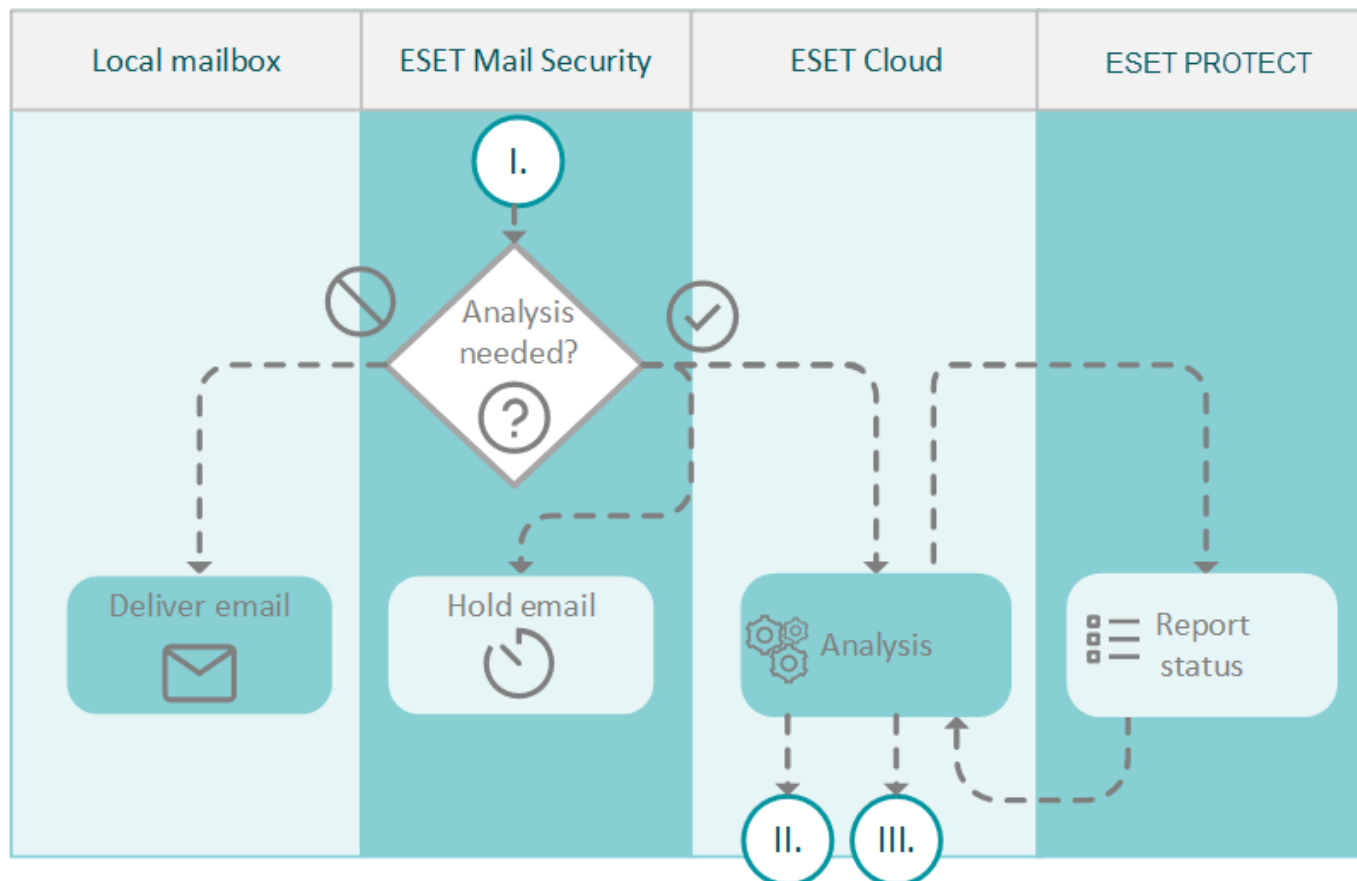
If your mail security product marks an email message for analysis, that email is held for a pre-set time period. While email is on hold, ESET LiveGuard Advanced is analyzing attachment. If the result of the analysis is clean, email is immediately delivered. If it is malicious, standard cleaning action takes place. If result of analysis does not come in pre-defined waiting time, security product releases the email to the recipient. When the result is available later, within 2 minutes, all computers block this attachment immediately.

- Emails in "hold" are listed in ESET Mail Security. Navigate to ESET Mail Security > **Tools** > **ESET LiveGuard Advanced** to see the list of emails on hold.



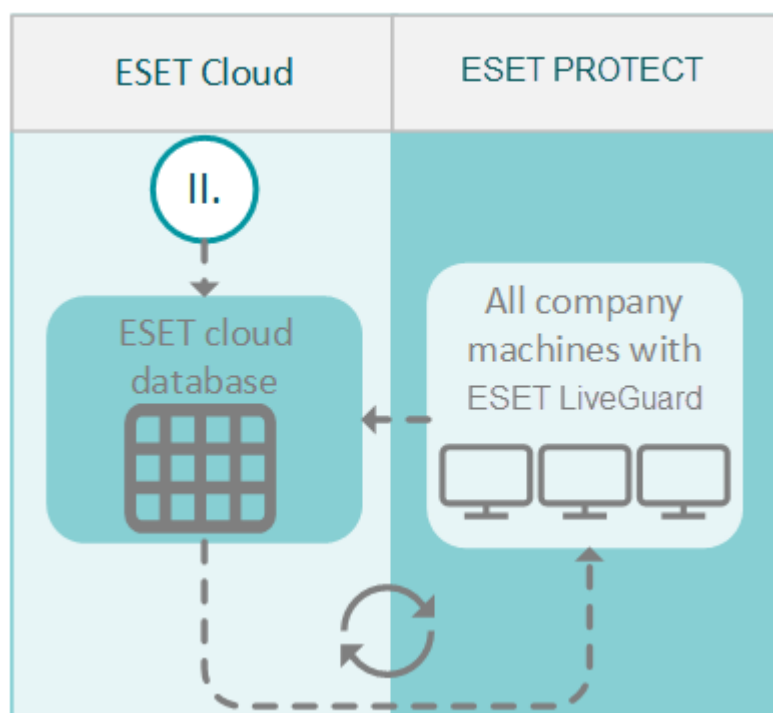
ESET LiveGuard quarantine					
Time	Estimated finish time	Envelope sender	Recipients	Subject	

- Maximum wait time for analysis is set in the ESET Mail Security policy under Computer > Cloud-based protection > ESET LiveGuard > Maximum wait time for the analysis results.



3. Analysis results are shared

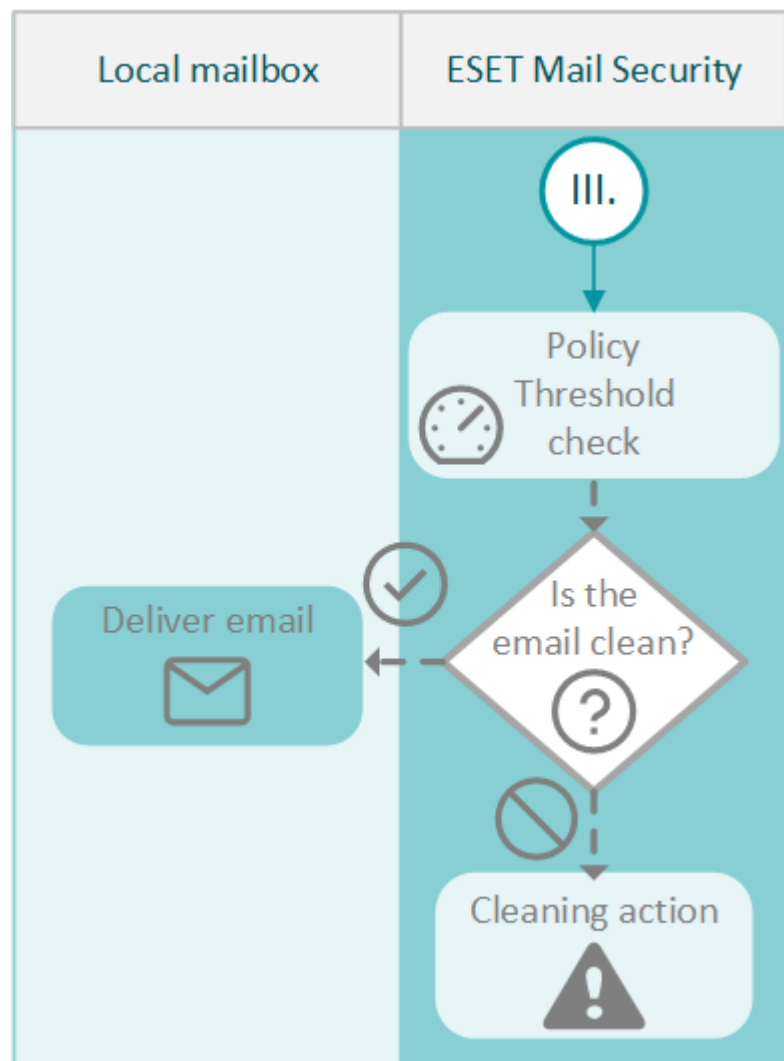
ESET LiveGuard Advanced uses four separate [detection layers](#) and the results of the analysis are saved to a database in the ESET cloud. The database is synchronized every single minute with ESET PROTECT On-Prem. All machines with activated ESET LiveGuard Advanced and ESET security product are also synchronized with ESET cloud every 2 minutes.



4. Evaluation and cleaning

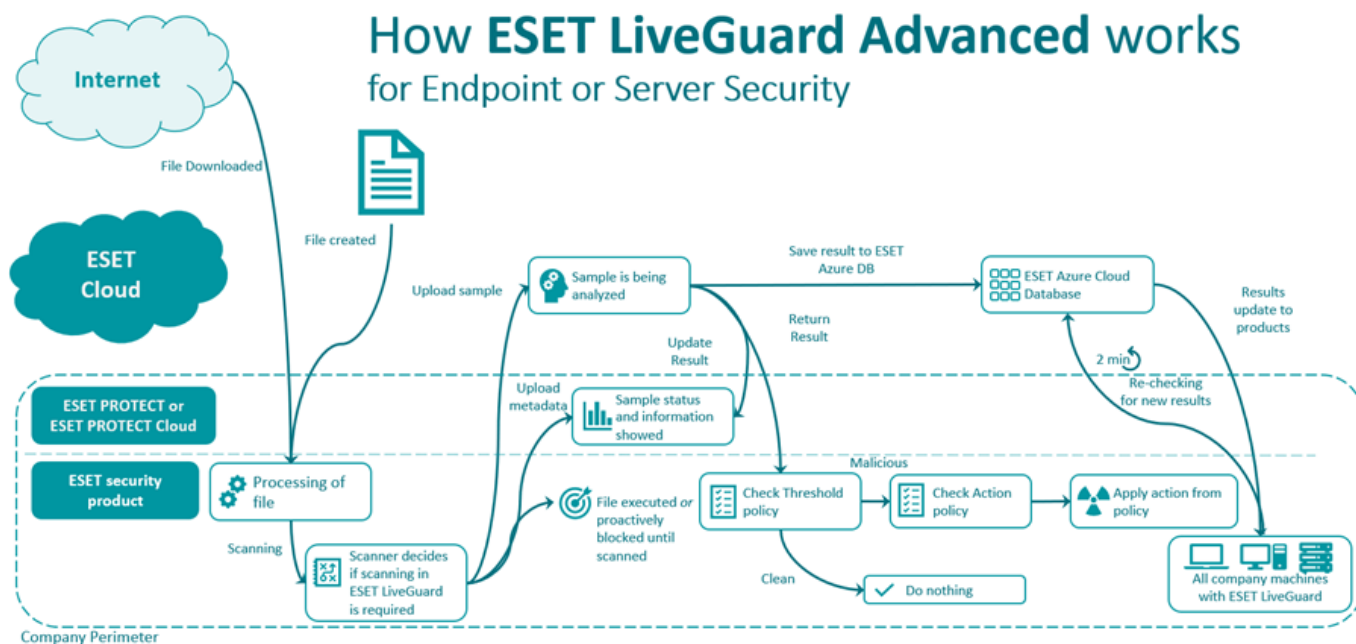
Analysis results are also sent back to your ESET security product and the email is scanned again. If the email is clean, it is delivered (unless the hold period has already passed).

Settings for cleaning actions and detection are set under category **Server** in the ESET Mail Security policy.



ESET Endpoint Security and ESET Server Security

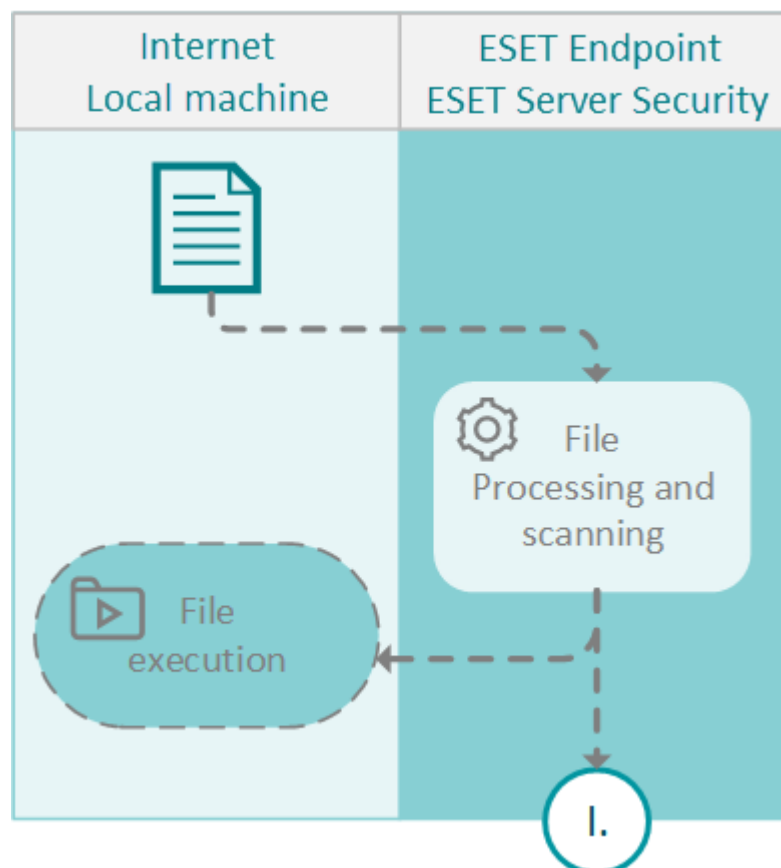
Each file detected by an ESET LiveGuard Advanced-through ESET Endpoint Security or ESET Server Security follows the submission process shown below. Use your policy settings to define security levels and cleaning actions for groups or single machines.



File analysis follows a four-step process:

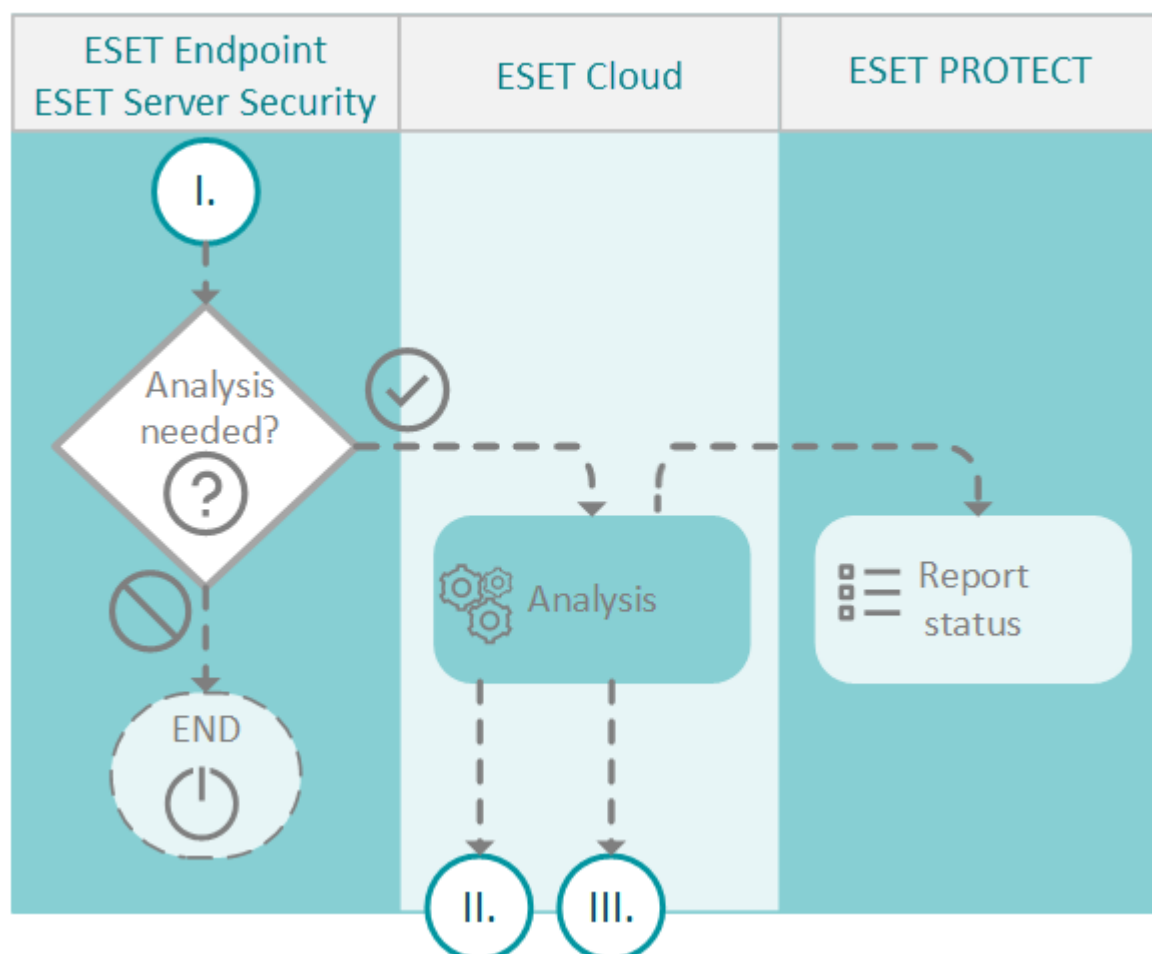
1. File scanning

The file is downloaded from the internet, copied to the computer or created. Your ESET security product processes and scans the file.



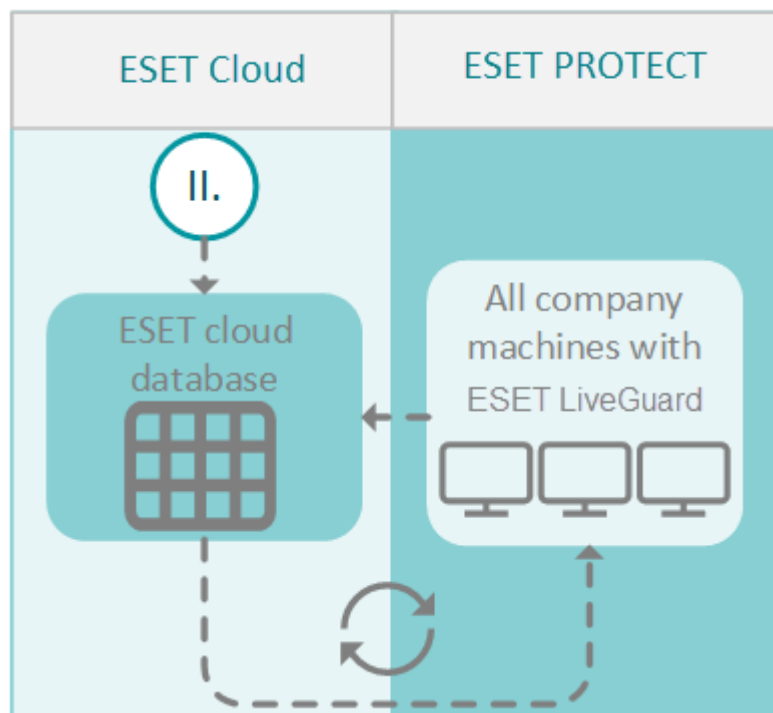
2. File analysis

If the ESET product decides the file needs to be analyzed, it sends it for analysis. Four separate [detection layers](#) process the file and provide a result. The results are reported to ESET PROTECT On-Prem. If the analysis is not needed, the process ends.



3. Analysis results are shared

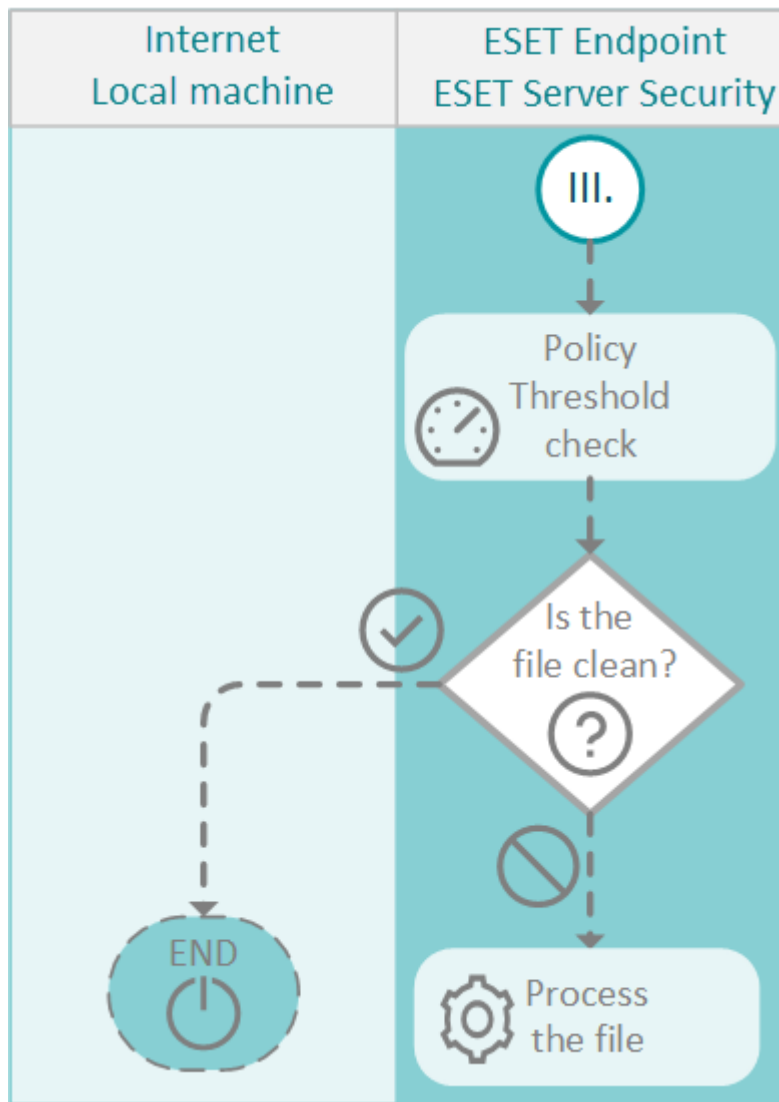
The results of the analysis are saved to a database in the ESET cloud. The database is synchronized every two minutes with ESET PROTECT On-Prem. All machines where ESET LiveGuard Advanced is active have up-to-date information from ESET cloud.



4. Evaluate local policy

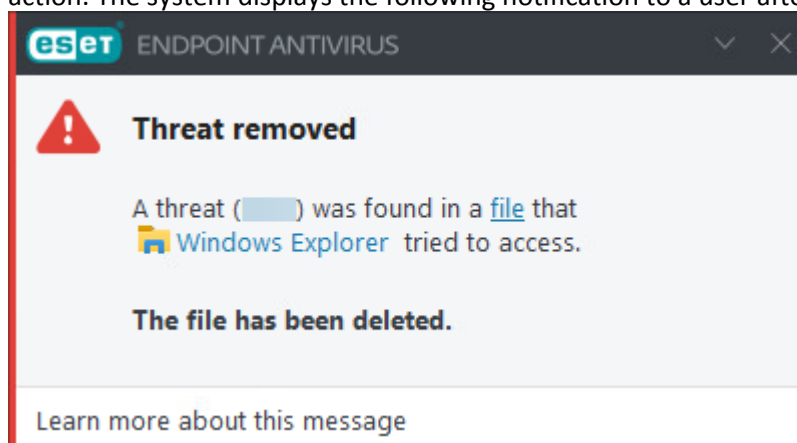
Analysis results are also sent back to your ESET security product. Your ESET security product will choose whether to take no action, clean or delete the file based on the cleaning settings defined in your security policy.

- The detection threshold is set in your ESET Endpoint Security / ESET Server Security policy under **Detection engine > Cloud-based protection > ESET LiveGuard Advanced > Detection threshold**
- Action taken after a threat is detected is set in your ESET Endpoint Security / ESET Server Security policy under **Detection engine > Cloud-based protection > ESET LiveGuard Advanced > Action after detection**



Notification example

If ESET LiveGuard Advanced evaluates a file as not clean, ESET Endpoint Security executes the cleaning action. The system displays the following notification to a user after deleting the file:

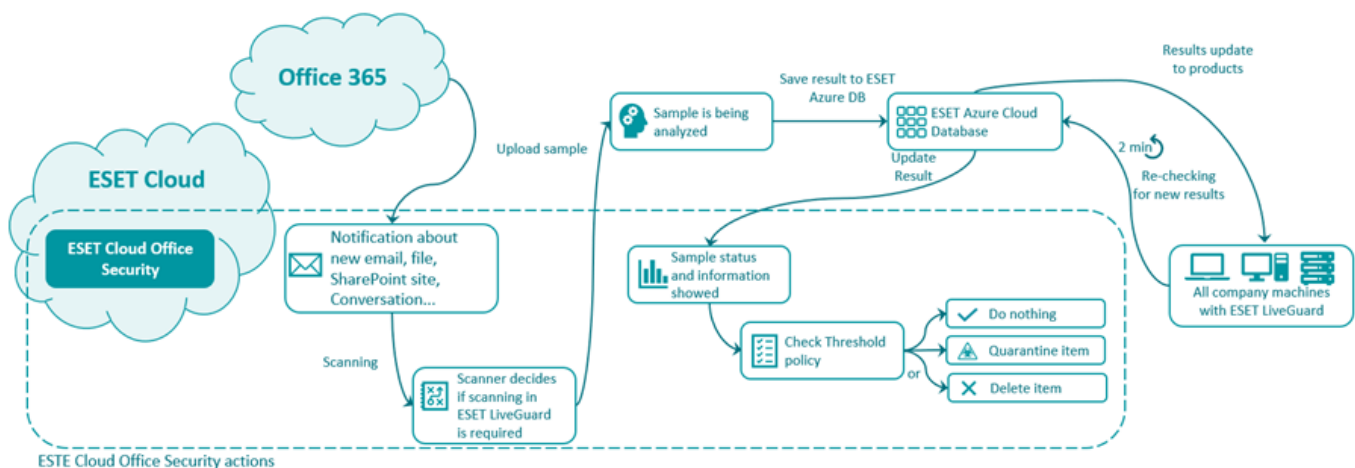


ESET Cloud Office Security

ESET Cloud Office Security utilizes ESET LiveGuard Advanced to analyze new threats. It does not require an ESET management console (ESET PROTECT On-Prem / ESET PROTECT). Information like a list of all submitted files and their results are present only in ESET Cloud Office Security.

- ESET Cloud Office Security does not report to ESET management consoles, even if the console is connected to the same license account.
- ESET Cloud Office Security shares information about detections with endpoints connected to the same license account.
- ESET Cloud Office Security can submit suspicious email attachments and samples shared in Microsoft SharePoint, Teams, and other parts of Office 365.

How ESET LiveGuard Advanced works for ESET Cloud Office Security



The analysis of a file from ESET Cloud Office Security follows a four-step process:

1. File scanning

A new file is detected in the cloud storage. ESET scanner processes and scans the file.

2. File analysis

If the ESET scanner decides the file needs to be analyzed, it sends it for analysis. Four separate [detection layers](#) process the file and provide a result, and the result is reported to ESET Cloud Office Security. If the analysis is not needed, the process ends.

3. Analysis results are shared

The results of the analysis are saved to a database in the ESET cloud. The results are immediately communicated to all machines activated using the same license account and where ESET LiveGuard Advanced is active.

4. ESET Cloud Office Security policy decides the action

Analysis results are sent back to your ESET Cloud Office Security. It chooses to take no action, clean or delete the file based on the cleaning settings defined in your [policy](#). For more information, see [Protection settings for ESET LiveGuard Advanced](#).

Proactive protection

Proactive protection detects only files from the following sources:

- Files downloaded using a supported web browser
- Downloaded from a mail client
- Files extracted from an unencrypted or encrypted archive using one of the supported archive utilities
- Executed and opened files located on a removable device

If a file is suspicious, Proactive protection blocks its execution until the [detection layers](#) complete the analysis.

Supported applications and devices

This function is available for products and devices running on:

- Windows - All [supported ESET Endpoint](#) products and ESET Server Security 7.2 and later, ESET Mail Security 7.2 and later.
- Linux - all [supported products](#).

Supported applications on Windows

Web browsers	Mail Clients	Archive utilities	Removable devices
Internet Explorer	Microsoft Outlook	WinRAR	USB flash drive
Microsoft Edge	Mozilla Thunderbird	WinZIP	USB hard drive
Chrome	Microsoft Mail	Microsoft Explorer built-in unpacker	CD/DVD
Firefox		7zip	Floppy disk
Opera			Built-in card reader
Brave Browser			

i Files copied using Microsoft Explorer from an excluded location to a protected location get blocked by Proactive protection because ESET LiveGuard Advanced recognizes `explorer.exe` as an archive utility.

Supported applications on Linux

Web browsers	Mail Clients	Archive utilities	Removable devices
Chrome	Mozilla Thunderbird	Not supported on Linux	USB flash drive
Firefox	Evolution		USB hard drive
Opera	Mailspring		CD/DVD
Brave Browser	KMail		Floppy disk
Vivaldi	Geary		Built-in card reader
	Mutt		
	claws mail		
	Alpine		

ESET Cloud Office Security users

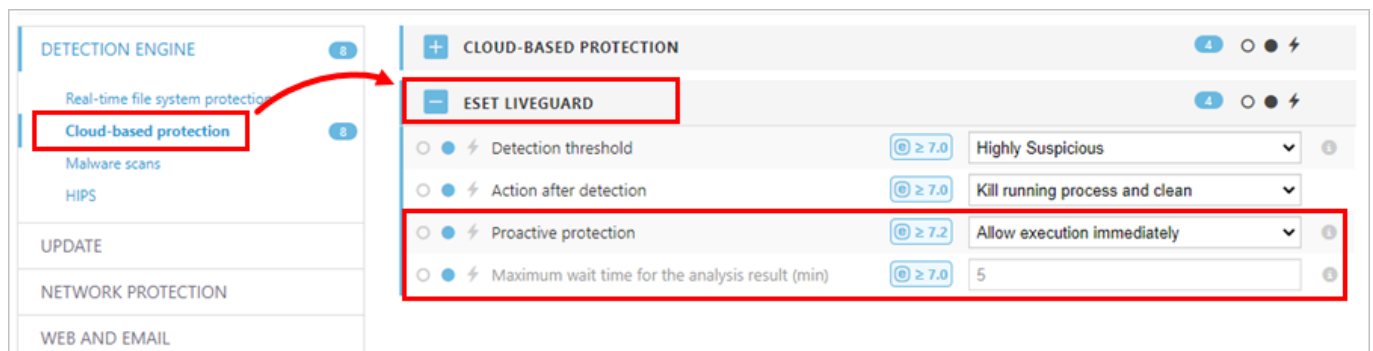
Proactive protection is not available in ESET Cloud Office Security.

Configuration of ESET Endpoint Antivirus

Configure the proactive protection settings using an [policy](#).

In the Web Console, navigate to [policies](#) > create a new one or edit existing policy > select target ESET product > **Detection Engine** > **Cloud-based protection** > **ESET LiveGuard Advanced** > **Proactive protection**.

- **Allow execution immediately** - The user can execute the file even if it is still being analyzed. When the result of the analysis is delivered, the ESET product responds accordingly.
- **Block execution until receiving the analysis result** - The user needs to wait until file analysis is complete to execute the file.

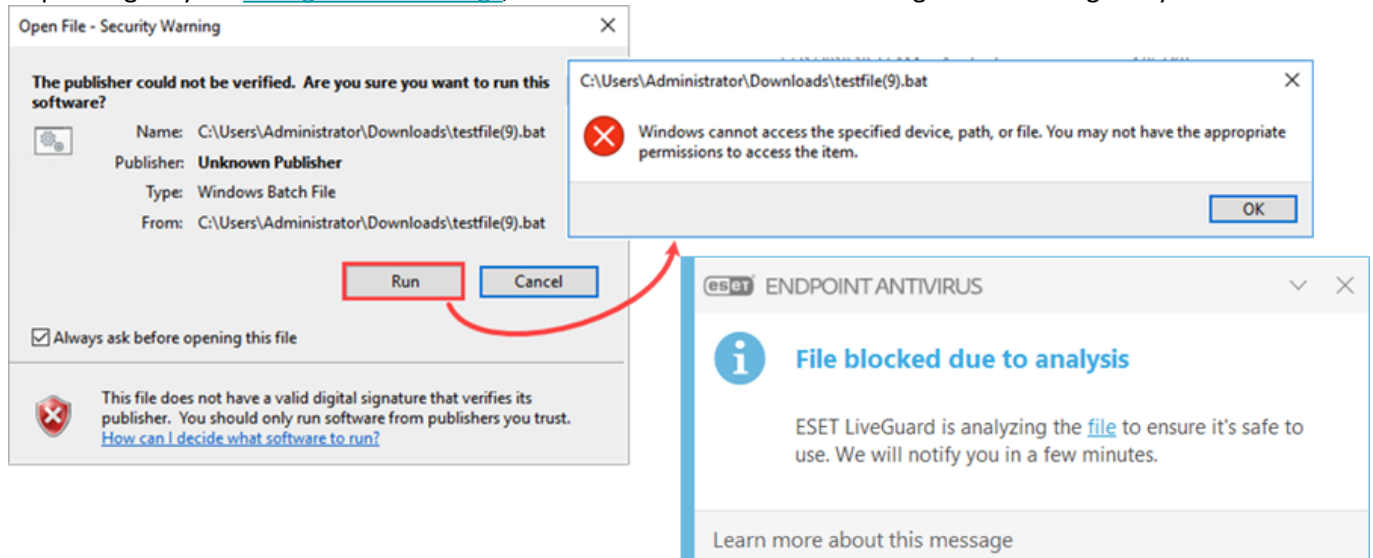


Using Proactive protection

When a suspicious file is detected, your operating system may display a warning when running the file for the first time. The ESET product displays information about the file being analyzed. If the analysis is completed before you execute the file for the first time, the **File in analysis** notice is not displayed.

Windows users

Depending on your [configuration settings](#), Windows allows or denies running the file during analysis.

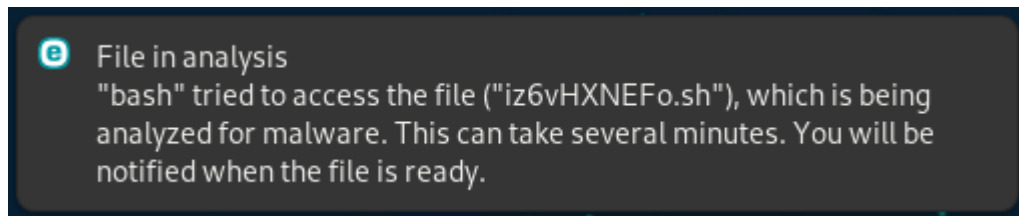


Linux users

ESET Server Security products on Linux do not display the warning about the ongoing analysis. If you try to run a file locked by proactive protection:

- Linux system displays the Access denied information.
- Linux terminal returns `Operation not permitted` message.

ESET Endpoint Security displays graphical warning, when used in Linux with graphical interface:

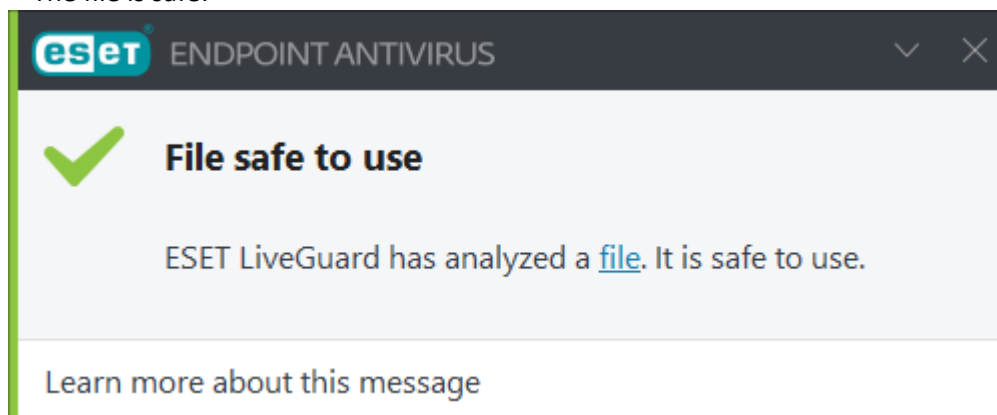


Result of analysis

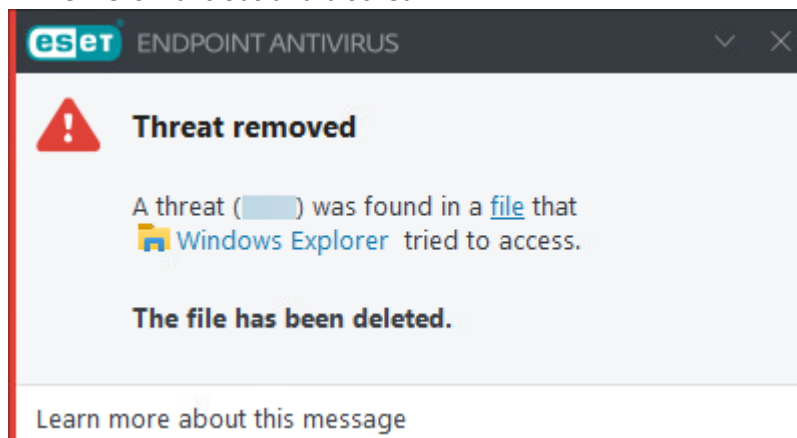
The result is delivered in time

In the configuration, you can set the maximum wait time for the analysis. Results delivered within this time are displayed on the screen:

- The file is safe:

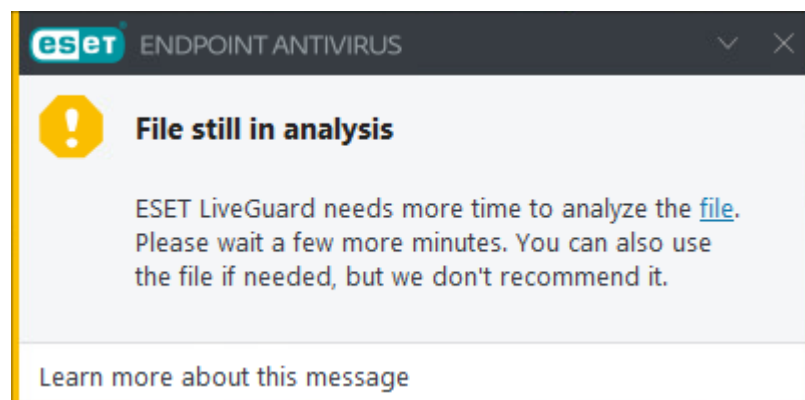


- The file is malicious and blocked:



The result could not be delivered in time

If analysis is taking longer than the maximum wait time, the file is released for use, and you will be informed about the ongoing analysis.



If the analysis proves the file to be malicious, the ESET product displays a warning and responds accordingly.

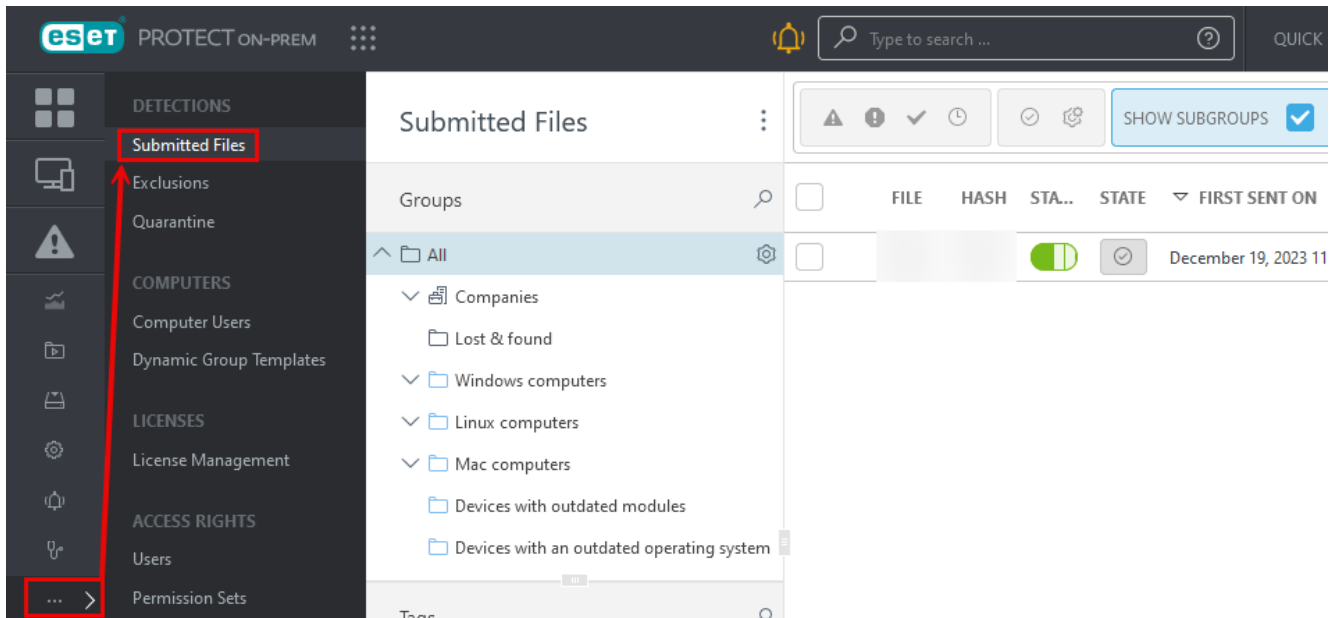
View a list of submitted files

In the **Submitted Files** section, you can view the list of files sent to ESET for analysis through ESET LiveGuard Advanced, ESET LiveGrid®, or email scanning. The Web Console administrator can see the complete list of submitted files. This functionality also works when a customer has not activated ESET LiveGuard Advanced. Only ESET LiveGrid® submissions are present by default.

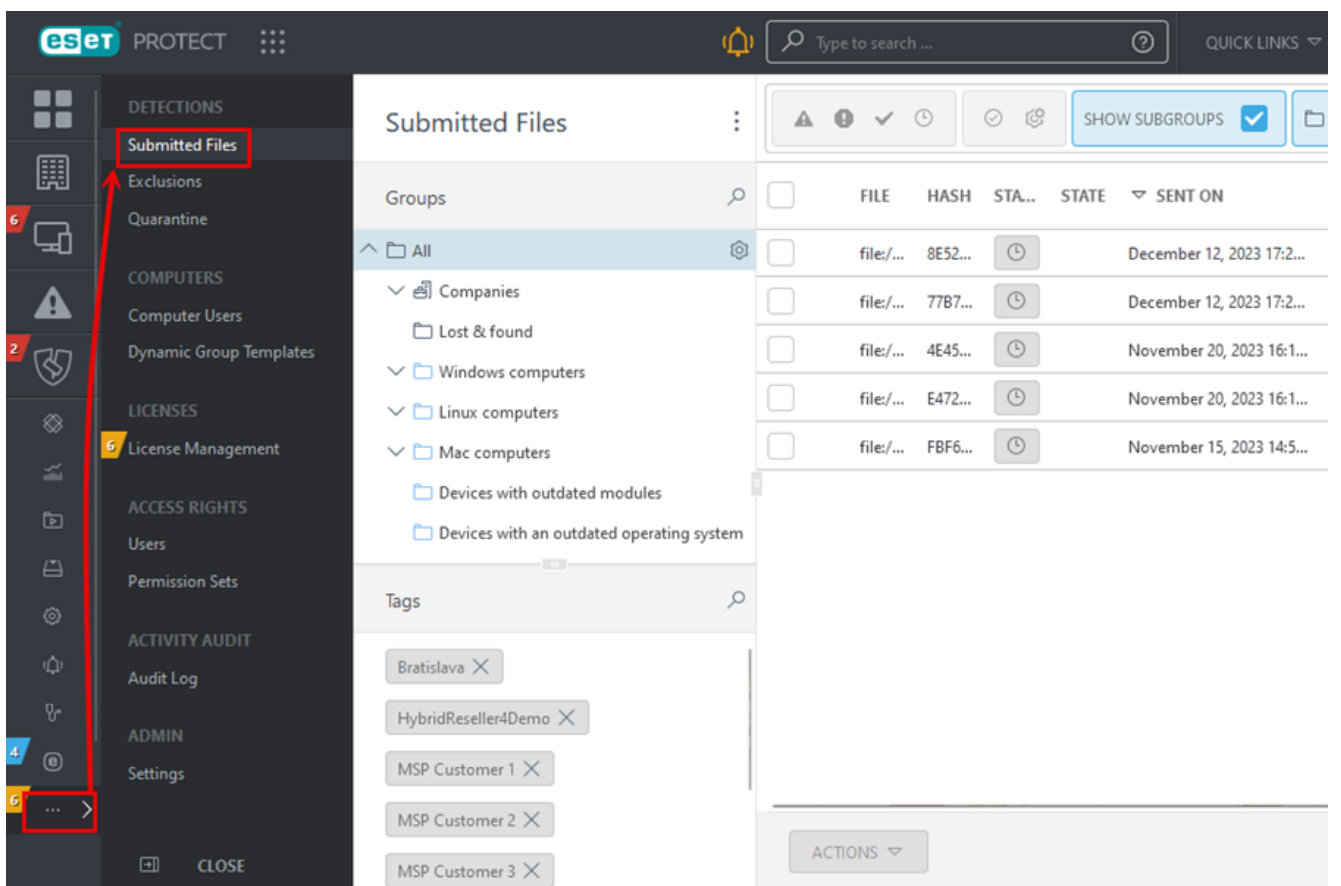
i In the **Submitted Files** menu, a user can only see files submitted from machines where the user has at least **Read** permission.

- **First Sent on** - This column shows the time when a user first submitted the file.
- **Last processed on** - A file can be submitted for analysis many times from multiple computers and companies. This column shows the last time a company has submitted the file.

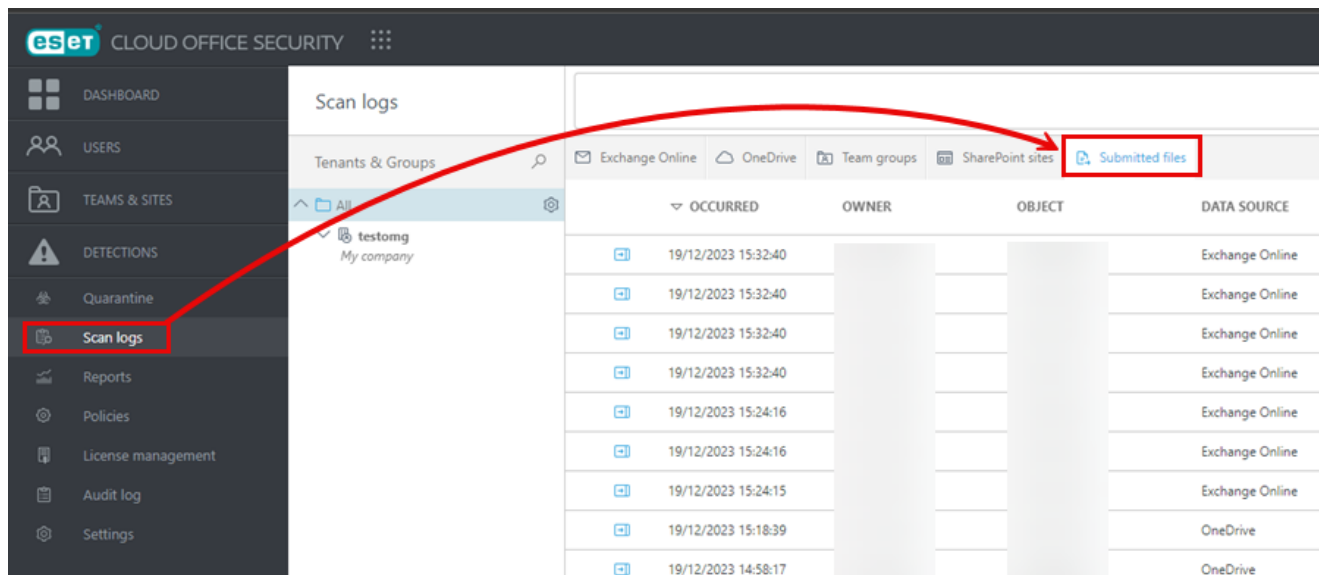
 [I am using ESET PROTECT On-Prem](#)



^ I am using ESET PROTECT



^ I am using ESET Cloud Office Security

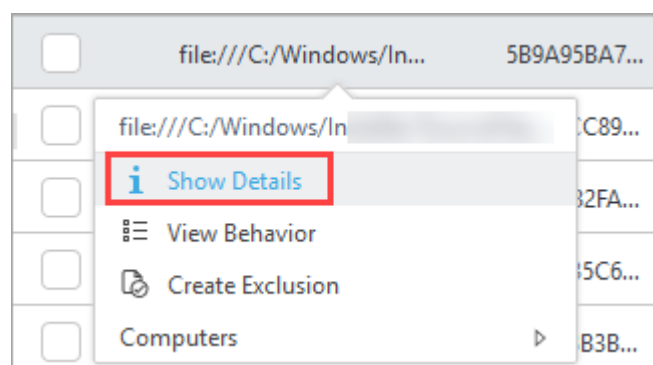


Details of analyzed files

[Details](#) of the analyzed file are in the Web Console in the **Submitted Files** section.

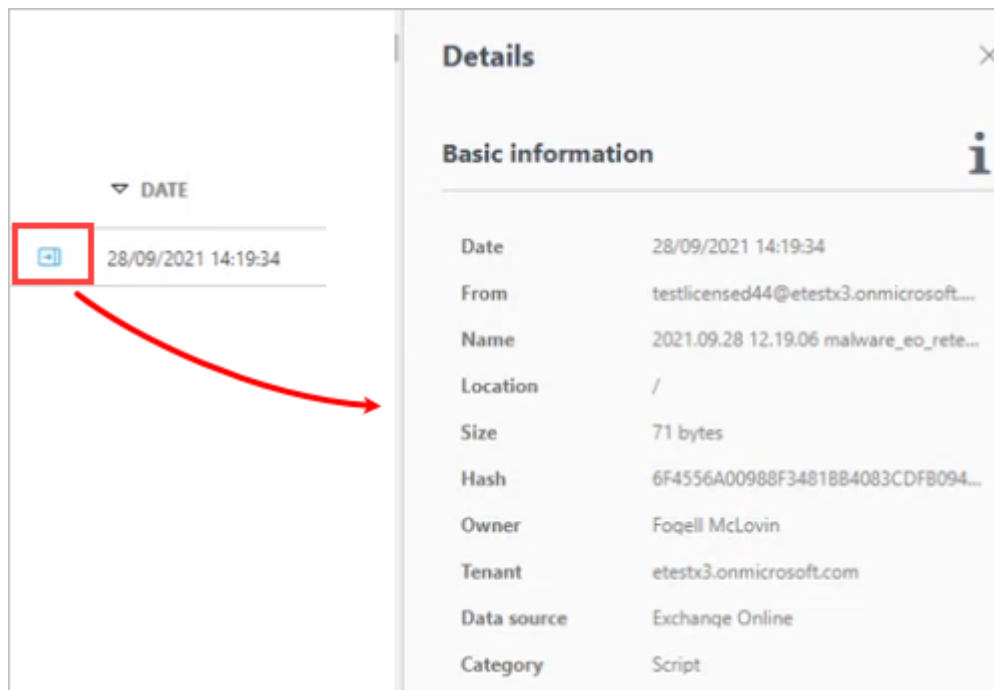
Management console users (ESET PROTECT On-Prem)

Select a file and click **Show Details**.



ESET Cloud Office Security users

In the Submitted files screen, click the blue icon in the file's row to show the file details in the sidebar.



Linux users

ESET Server Security for Linux

Users can list submitted files using the following commands from a Terminal window as a privileged user:

```
/opt/eset/efs/bin/lslog -n
```

or

```
/opt/eset/efs/bin/lslog --sent-files
```

[Read more](#) in ESET Server Security documentation.

If you use the [web Interface](#):

1. Log in to the web interface.

2. Click **Sent Files**.

ESET Endpoint Antivirus for Linux

Users can list submitted files using the following commands from a Terminal window as a privileged user:

```
/opt/eset/eea/sbin/lslog -n
```

or

```
/opt/eset/eea/sbin/lslog --sent-files
```

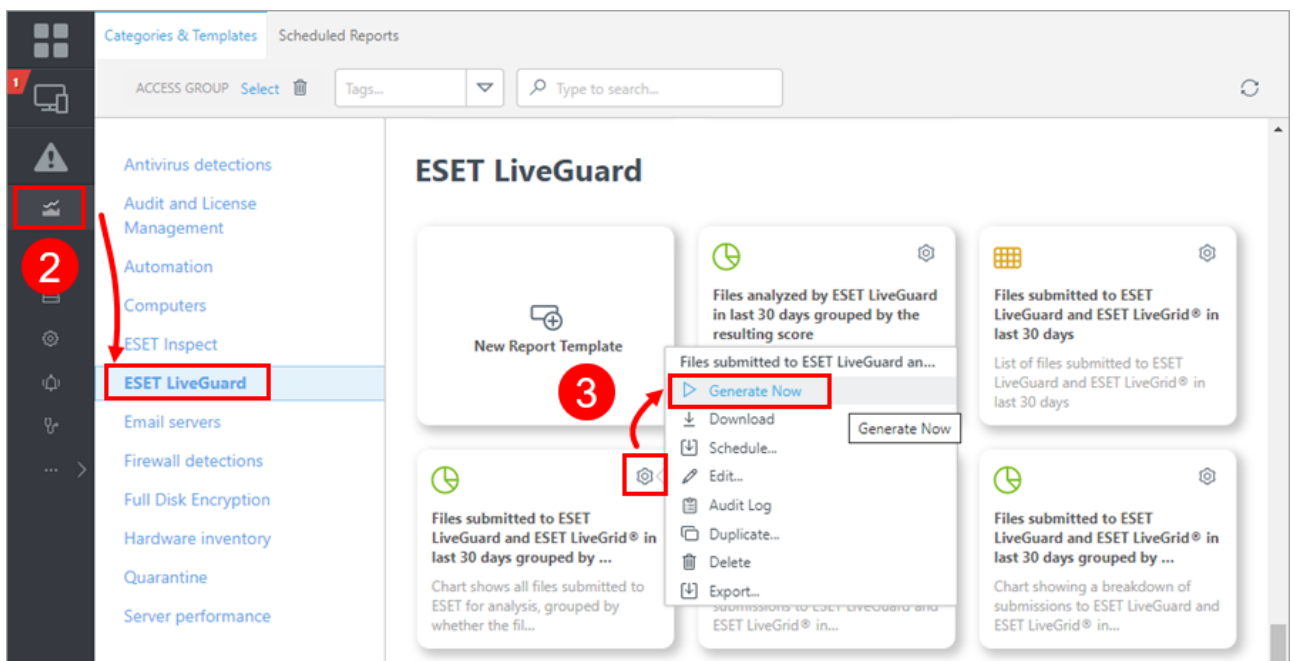
Create a report

You can create a report of ESET LiveGuard Advanced data in the remote management console. You can use one of the pre-defined reports or create a custom one.

The following process is valid for ESET PROTECT On-Prem and ESET PROTECT.

Built-in reports

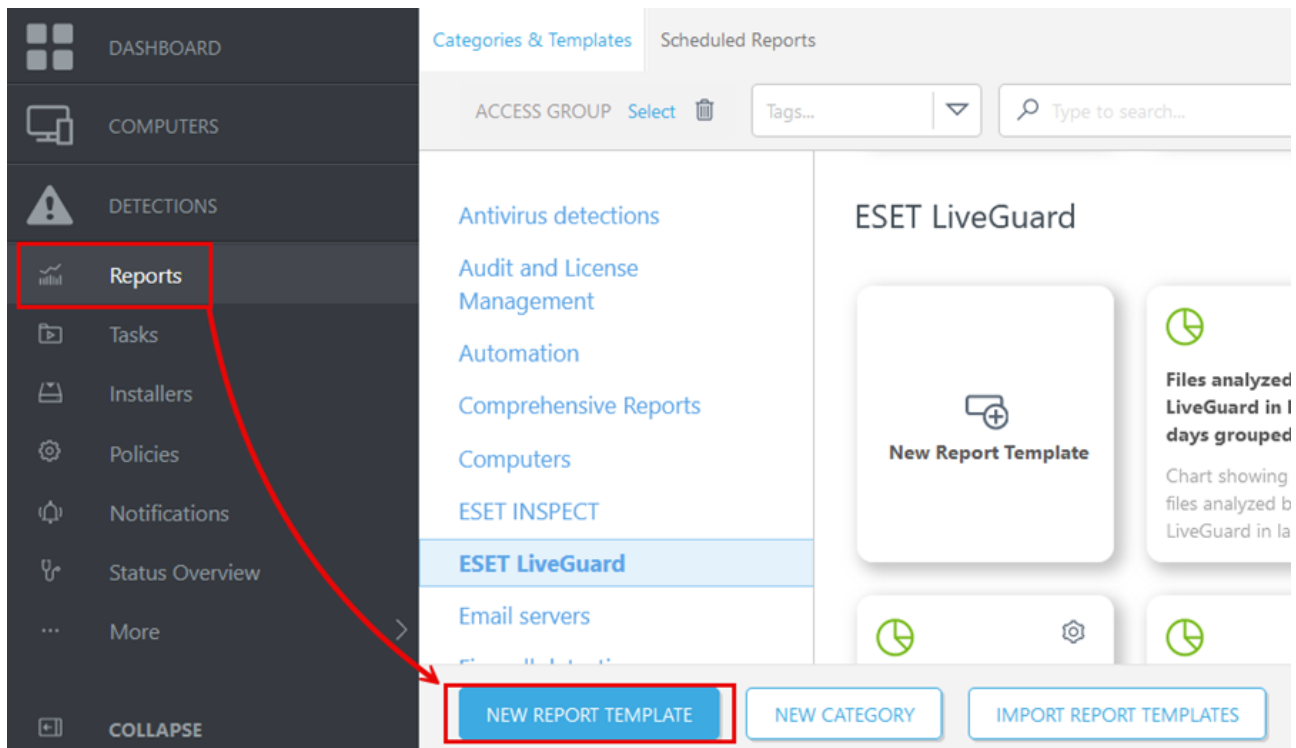
1. Log in to your Web Console.
2. Click **Reports** > **ESET LiveGuard**.
3. Select the applicable report and click the gear icon > **Generate now**.



Create a custom report

To create a custom report to display the score, destination and type of submitted files:

1. Log in to the Web Console.
2. Click **Reports** > **New Report Template**.



3.Type a **Name** for the template and select **ESET LiveGuard** as **Category**.

This screenshot shows the 'New Report Template' form. The 'Basic' tab is selected and highlighted with a blue arrow. The form has a sidebar on the left with options: 'Basic' (selected), 'Chart', 'Data', 'Sorting', 'Filter', and 'Summary'. The main form area has the following fields: 'Name' (with 'Score report' entered and highlighted by a red box), 'Description' (empty), 'Tags' (with a 'Select tags' link), and 'Category' (with 'ESET LiveGuard' selected and highlighted by a red box). A red arrow points from the 'Name' field to the 'Category' field. At the bottom of the form are four buttons: 'BACK', 'CONTINUE' (highlighted with a blue bar), 'FINISH', and 'CANCEL'.

4.Click **Continue**.

5. Select **Display Table** and **Continue**.

New Report Template

Reports > New Report Template

Basic

Chart

⚠ Data

Sorting

Filter

Summary

Table

Display Table ☒

Chart

Display Chart ☐

Chart Type

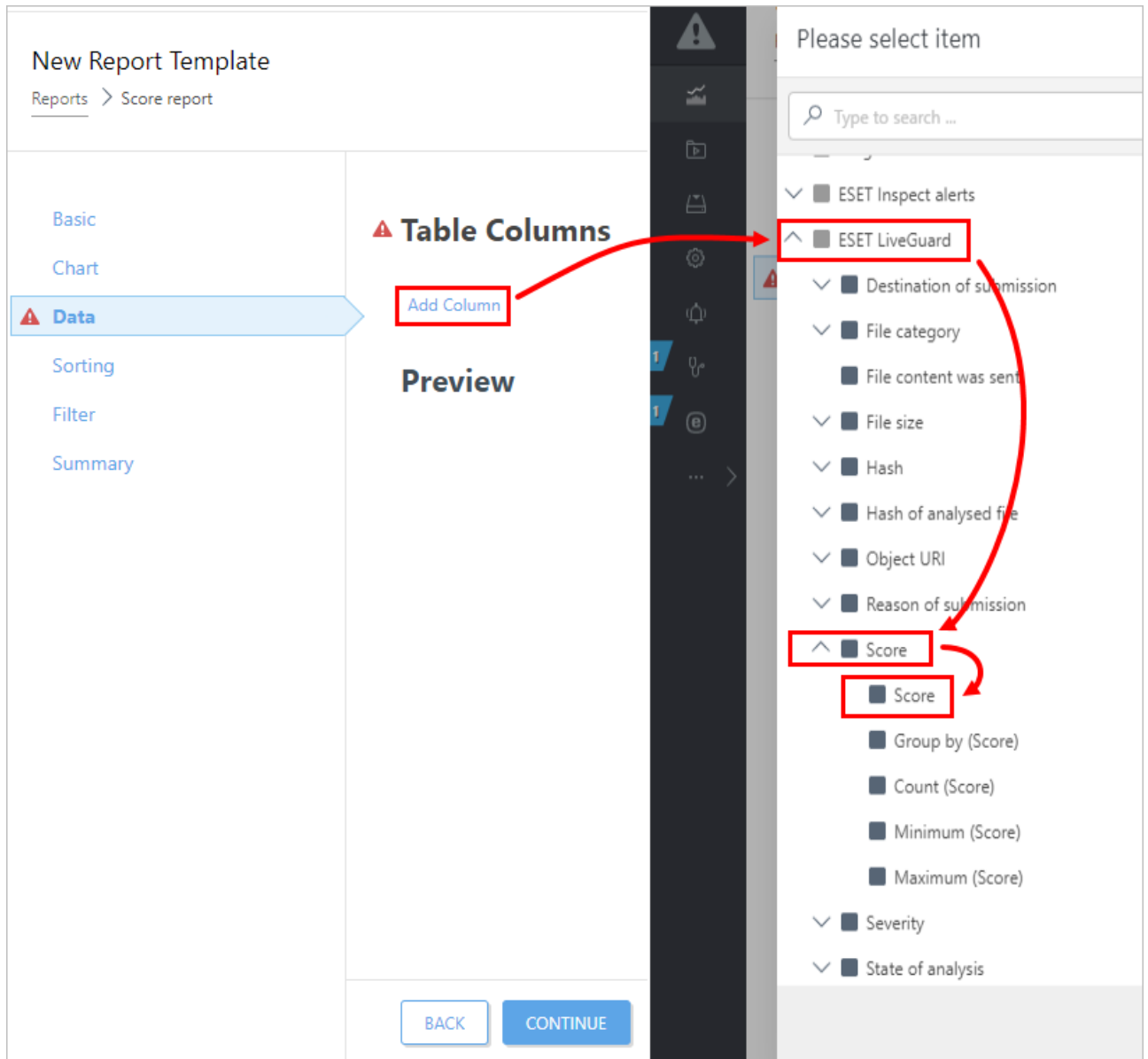
Bar Chart

Title for X axis

Title for Y axis

BACK CONTINUE FINISH CANCEL

6. Click **Add Column** and select **ESET LiveGuard > Score > Score**. To confirm, click **OK**.

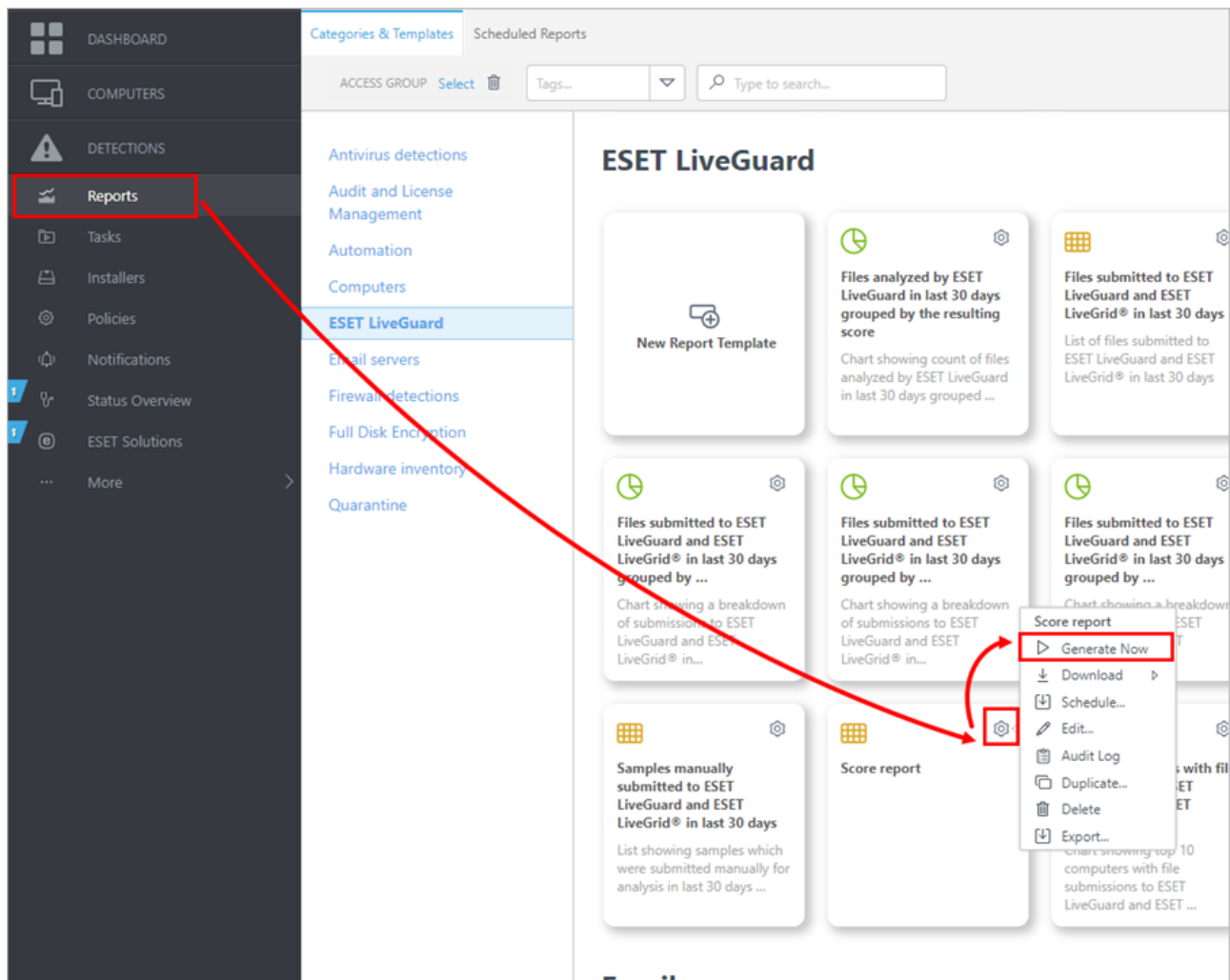


7. Click **Add Column** and select **ESET LiveGuard > File category**. To confirm, click **OK**.

8. Click **Add Column** and select **ESET LiveGuard > Destination of submission**. To confirm, click **OK**.

9. Click **Finish** to save the template.

10. To run the report, click **Reports**, click the new report template gear icon > **Generate now**.



Results of analysis

After a file is [analyzed](#), ESET cloud sends it to ESET management console (or ESET Cloud Office Security), where the status of the analyzed file is changed from **Unknown** to one of the statuses listed below. Information about the file and short results of the analysis can be viewed in the **File details** window.

ESET Cloud Office Security users can find the list of submitted files and their results in [Logs](#).

Clean

Status ✓ Clean

State ✓ Finished

Last processed on 2018 Feb 04 12:00:00

Sent on 2018 Feb 04 17:05:20

Behaviors [View behavior](#)

file:///C:/work/em001_64.dll

Computer ESET Endpoint Security

User EDTPM\Administrator

Reason Automatic

Sent to ESET LiveGuard



Hash C1092A9AC0D334BAF81E35A14C7343546C499284

File parameters	Description
Computer	Name of the computer that submitted the file.





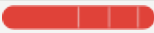
File parameters	Description
User	User on the source computer that submitted the file. In some cases, this can be a system user.
Reason	Reason for submission (Automatic, Manual).
Sent to	Part of the ESET cloud that received the file.
Hash	SHA-1 and SHA-256 hash of the submitted file.
Filename	Filename and its full path in the submitter's file system.
Size	Size of the file.
Category	Category (file type) of the file. Category is used in submission configuration .

Each sample has two key parameters: **State** and **Status**.

State expresses the file's present station in the analysis workflow.

State	Description
Sent to LiveGrid(R)	File was sent to the ESET cloud, but the result will not be available.
Sent to ESET LiveGuard	File was sent to the ESET cloud for ESET LiveGuard Advanced analysis .
Analyzing 	The analysis is in progress.
Finished 	The file was successfully analyzed.
Re-analyzing	The prior result is available, but the file is undergoing analysis again.

Status expresses the [result](#) of the behavioral analysis or the absence of a result.

Icon	Status	Score	Description
	Unknown		The file was not analyzed.
	Clean	1 - 74	No detection engine identifies the sample as malicious.
	Suspicious	75 - 89	Detection engine has evaluated the file behavior as suspicious but not as clearly malicious.
	Highly suspicious	90 - 99	
	Malicious	100	File behavior is considered malicious.

Recommendations for users with suspicious samples

If your file is evaluated as suspicious or highly suspicious, you should consider the following:

- if your license allows it, inspect the [behavioral report](#) for details on the file's activities.
- inspect the source of the file (where did the file come from), do you trust it?
- upload the file to an external virus analysis tool, for example, [VirusTotal](#).
- if you consider your organization to be at a high risk of attack, set the [Detection threshold](#) to **Suspicious**.

Behavioral report

In the Web Console, navigate to [Submitted Files](#). Select the file and click **Show Details** > **View Behavior** to see the **File Behavior Report**. This report contains essential data about the inspected file and observed behavior from the

[sandbox analysis](#). Each sample can have multiple observed behaviors. Depending on the license type you own, you can see two different behavior report layouts and results.

Non-EDR/XDR license users

The report consists of the following:

1. **Result**—Final assessment of the file.
2. **Advanced scanning engines**—Results from the scanning layer.
3. **Behavioral analysis sandbox**—Results from the behavioral layer.
4. **Analyzed behaviors**—List of analyzed behaviors and their results.

1

MALICIOUS

SHA-1

Category Executable

2

ADVANCED SCANNING ENGINES

Advanced Unpacking And Scanning

The sample undergoes static analysis and state-of-the-art unpacking and is then matched against an enriched threat database.

Sample is clean

Advanced Machine Learning Detection

Static and dynamic analysis is performed by an army of machine learning algorithms, including deep learning.

Sample is suspicious

3

BEHAVIORAL ANALYSIS SANDBOX

Experimental Detection Engine

A sample is inserted into "sandboxes on steroids" that closely resemble full-scale user devices and that are subsequently monitored for any sign of malicious behavior.

Sample is suspicious

In-Depth Behavioral Analysis

The memory dumps produced by previous EDTD layers are subject to an in-depth behavioral analysis that identifies known malicious patterns and chains of actions.

Sample is clean

4

ANALYZED BEHAVIORS

	Suspicious Registry Entry	Behavior not detected
	Suspicious DLL Load	Behavior not detected
	Elevation Of Privileges	Behavior not detected
	Service Stop	Behavior not detected

EDR/XDR license users

You can download Behavioral report via the **Download PDF** button.

The report consists of the following:

- 1.**Result**—Final assessment of the file.
- 2.**File details**—Results from the scanning layer.
- 3.**SHA-1 hash**—Contains hash and a link to VirusTotal.

4.**SHA-256 hash**—Contains SHA-256 hash.

5.**Sandbox details**—Results from the behavioral layer.

6.**Analyzed behaviors**—List of detected behaviors and their results. You can use the Search bar to navigate through the details after analysis.

Behavioral report example

ESET LIVEGUARD

Thursday, December 21, 2023

✓ **No threats found**

1

SHA-1 a3415e12db99e3d5b6f9e93be6717292c702b6d2
SHA-256 67933b617b3029844db5c9ff4c8feebfadcd658c77bb9d2d0d1270f384eb17
Category Script

DOWNLOAD PDF

File
Details

2

File name RemoteAggregatorTriggerCriteria.dat
SHA-1 a3415e12db99e3d5b6f9e93be6717292c702b6d2
SHA-256 67933b617b3029844db5c9ff4c8feebfadcd658c77bb9d2d0d1270f384eb17
Category Script
Size 426 B

3

Sandbox
Details

5

Replication was not performed.

4

Analyzed behaviors

6



LiveGuard doesn't detect any suspicious behavior.

Type to search...

Process

Operations

API Logs

No logged processes are available.

Manual upload of a file for analysis

Suspicious files are uploaded to the ESET cloud automatically based on the [policy configuration](#) of your ESET security product. A user can also submit a file manually from any ESET LiveGuard Advanced-enabled ESET security product. Use the links below to view instructions for your product.

- [Submit from ESET PROTECT On-Prem](#)
- [Submit from ESET Endpoint Security](#)

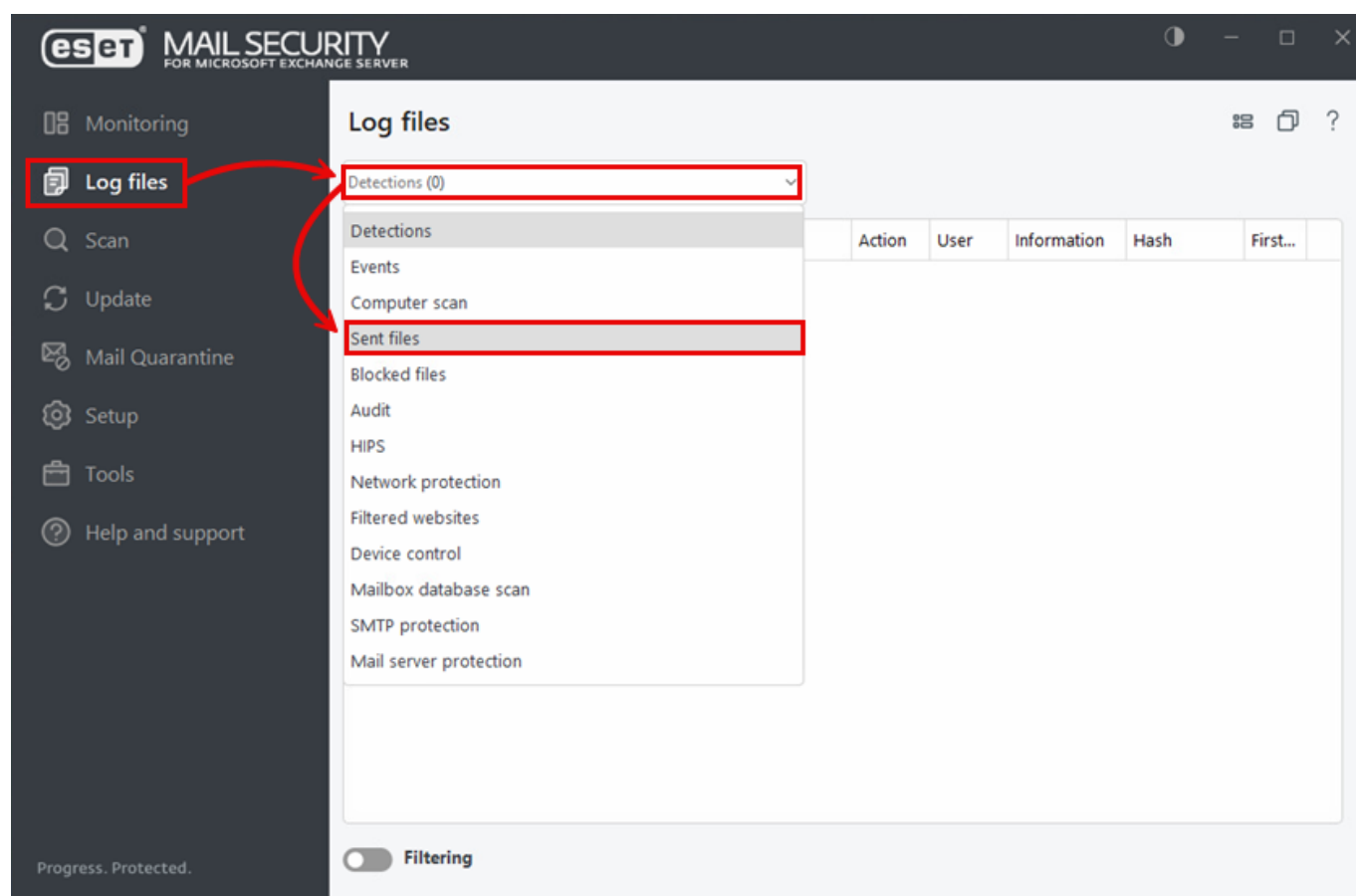
- [Submit from ESET Server Security](#)
- [Upload from ESET Mail Security](#)

List of locally submitted files

You can view a list of files submitted from the client machine in your ESET LiveGuard Advanced-compatible ESET security product.

To view files in **ESET Server Security** and **ESET Mail Security** click **Log files** and select **Sent files** from the drop-down menu.

To view files in **ESET Endpoint Security**, click **Tools > Log files** and select **Sent files** from the drop-down menu.



Submit file from ESET PROTECT On-Prem

In ESET PROTECT On-Prem, you can submit **Blocked files** [reported](#) by ESET Inspect On-Prem. Follow the steps below to submit files for analysis:

1. Log in to the Web Console.

i User can only access and upload detections from computers where the user has [permissions](#).

2. Click **Detections**, select the detection you want to submit. You can submit only files in **Detection Category: Blocked Files**.

DETECTION CATEGORY

Blocked Files
X
X
▼
X

ADD FILTER

3.Select a file and click **Send file to ESET LiveGuard** to schedule the client task that sends the file from the client machine to the ESET cloud.

	STATUS	DETECTION CATEGOR	DETECTION TYPE	CAUSE	ACTION	OCCUR	RESOLV
<input type="checkbox"/>	!	Blocked Files	ESET Inspect			1	0/1
<input type="checkbox"/>	!	Blocked Files	ESET Inspect			1	0/1
<input type="checkbox"/>	!	Blocked Files	ESET Inspect			1	0/1

Detection
Details
Investigate (Inspect)
Mark as Resolved
Mark as Unresolved
Send File to ESET LiveGuard
Audit Log
Computer



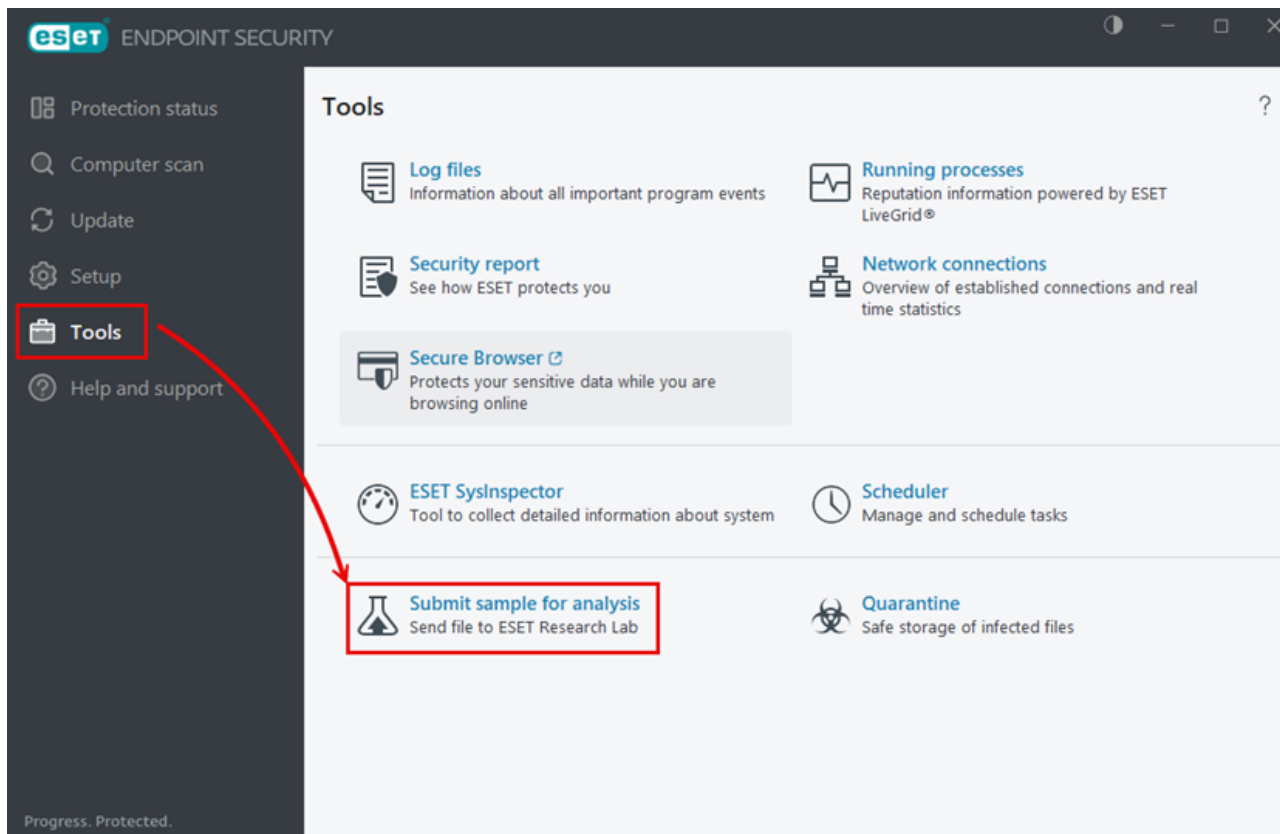
- You can [submit a sample](#) from machines where ESET LiveGuard Advanced is not active.
- Results for these files are not delivered to the user, but they are distributed via ESET LiveGrid®.
- The manual upload is available only when ESET LiveGrid® system is enabled on the machine.

Submit file from ESET Endpoint Security

Follow the steps below to submit a file for analysis from ESET Endpoint Security:

Windows users

- 1.Open ESET Endpoint Security.
- 2.Click **Tools > Submit sample for analysis**.



3.Type the required information in the **Select sample for analysis** form and click **Next**.

4.Optionally, add more information about the file and then click **Send**.

Linux users

The suspicious files are submitted automatically. Users cannot manually submit a file from ESET Endpoint Security for Linux.



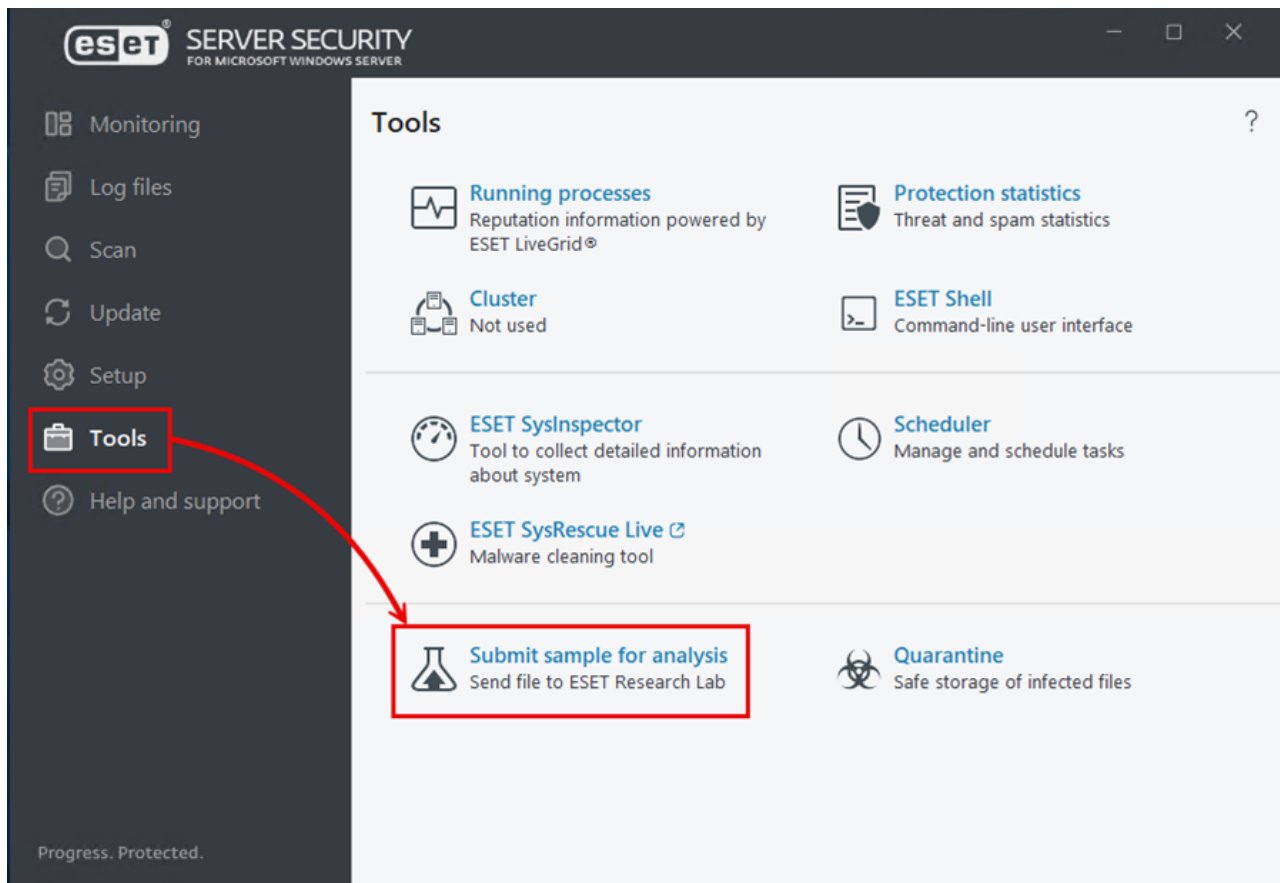
- You can [submit a sample](#) from machines where ESET LiveGuard Advanced is not active.
- Results for these files are not delivered to the user, but they are distributed via ESET LiveGrid®.
- The manual upload is available only when ESET LiveGrid® system is enabled on the machine.

Submit a file from ESET Server Security

Follow the steps below to upload a file from ESET Server Security for ESET LiveGuard Advanced analysis.

Windows users

- 1.Open ESET Server Security.
- 2.Click **Tools > Submit sample for analysis**.



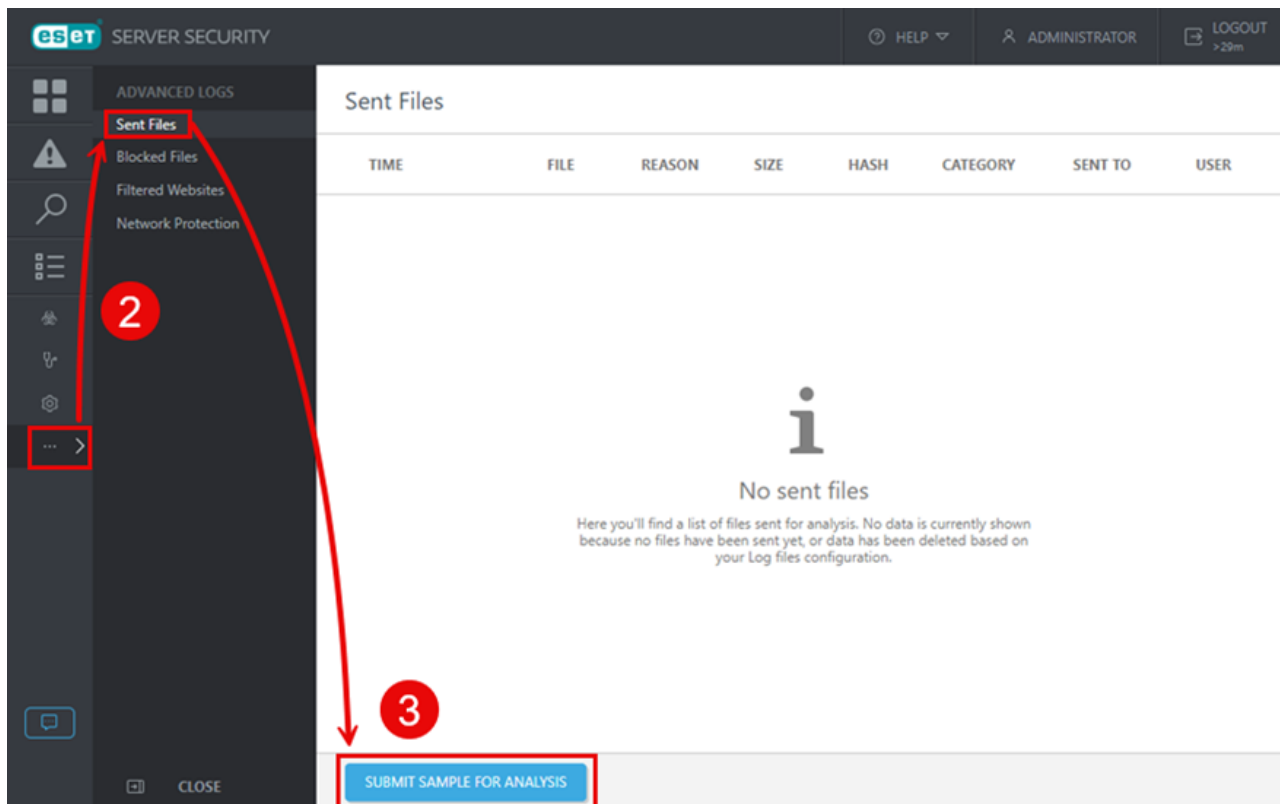
3.Type the required information in the **Select sample for analysis** form and click **Next**.

4.Optionally, add more information about the file and click **Send**.

Linux users

To submit a sample for analysis from the [web Interface](#):

- 1.Log in to the web interface.
- 2.Click **Sent Files**.
- 3.Click **Submit sample for analysis**.



4. Select a **Reason** for submitting the sample.

5. Type the site address or file path.

6. Type your email address or select **Submit anonymously**.

7. Click **Next**.

8. Type additional information.

9. Click **Send**.



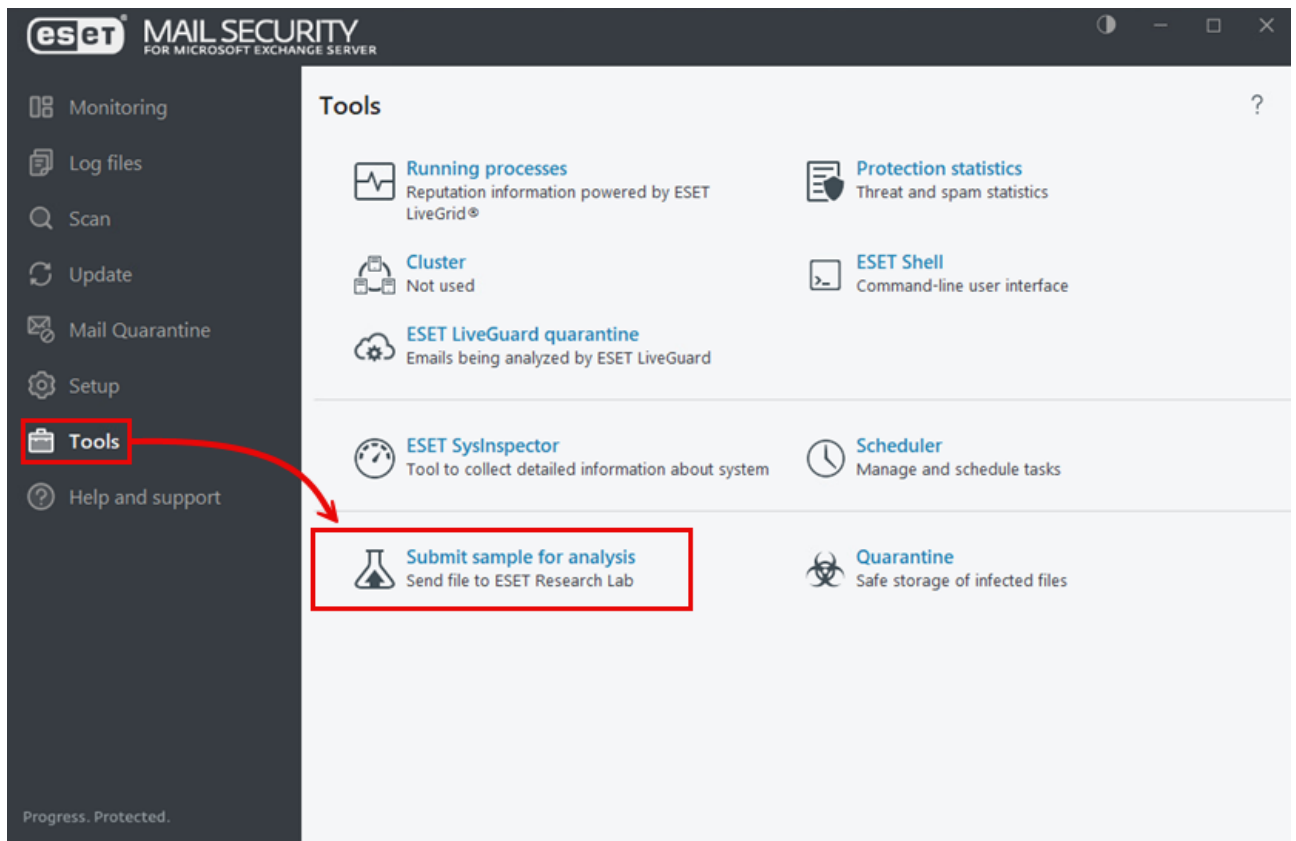
- You can [submit a sample](#) from machines where ESET LiveGuard Advanced is not active.
- Results for these files are not delivered to the user, but they are distributed via ESET LiveGrid®.
- The manual upload is available only when ESET LiveGrid® system is enabled on the machine.

Submit file from ESET Mail Security

Follow the steps below to upload a file from ESET Mail Security for ESET LiveGuard Advanced analysis:

1. Open ESET Mail Security.

2.Navigate to **Tools > Submit sample for analysis**.



3.Type the required information in the **Select sample for analysis** form and click **Next**.

4.Optionally, add more information about the file and click **Send**.



- You can [submit a sample](#) from machines where ESET LiveGuard Advanced is not active.
- Results for these files are not delivered to the user, but they are distributed via ESET LiveGrid®.
- The manual upload is available only when ESET LiveGrid® system is enabled on the machine.

Add exclusion

Typically, when a file is analyzed and evaluated as not clean, your ESET security product automatically [takes the action defined in your policy settings](#). If Quarantine is enabled on the machine, the file is moved to Quarantine (**Tools > Quarantine**). However, you can create an exclusion for a specific file if you know it to be safe or need to ensure that it is not cleaned for other reasons. File exclusions created by roaming agents will not be added in Web Console until the agent checks in to the [remote management](#) server.

Exclusions can create a risk

- While the exclusion policy is in place, ESET security products never scan the file. Be very careful when creating the exclusions.

Prerequisites for whitelisting a file:

- The file is sent for analysis in the ESET LiveGuard Advanced.
- This information is synchronized to the [remote management](#) server.

To whitelist a file from the scanning process:

1. An management console Administrator adds the file's hash as an [exclusion to a policy](#).

2. The policy is applied to selected machines. The file can be used freely on those machines.

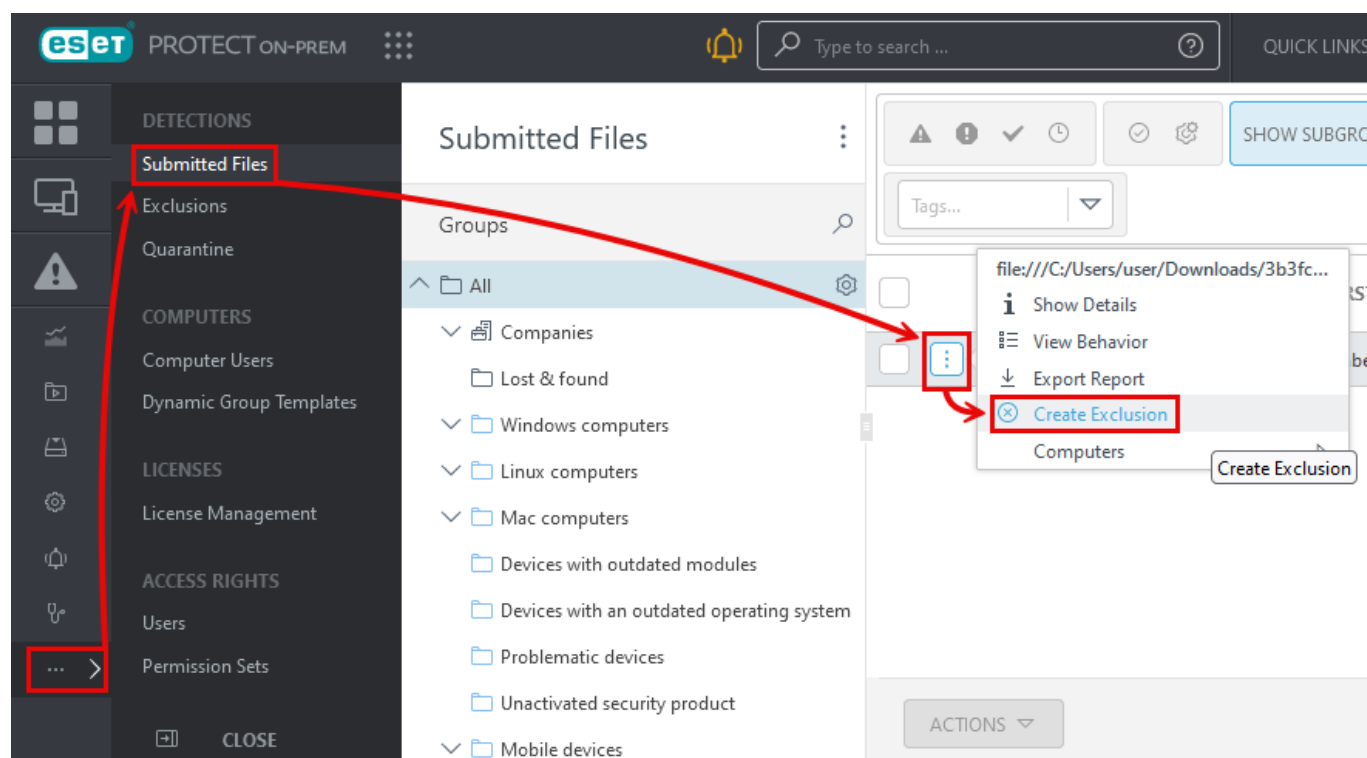
You can create a separate policy for exclusions. Create the policy before you add the exclusion.

[Create a management policy](#).

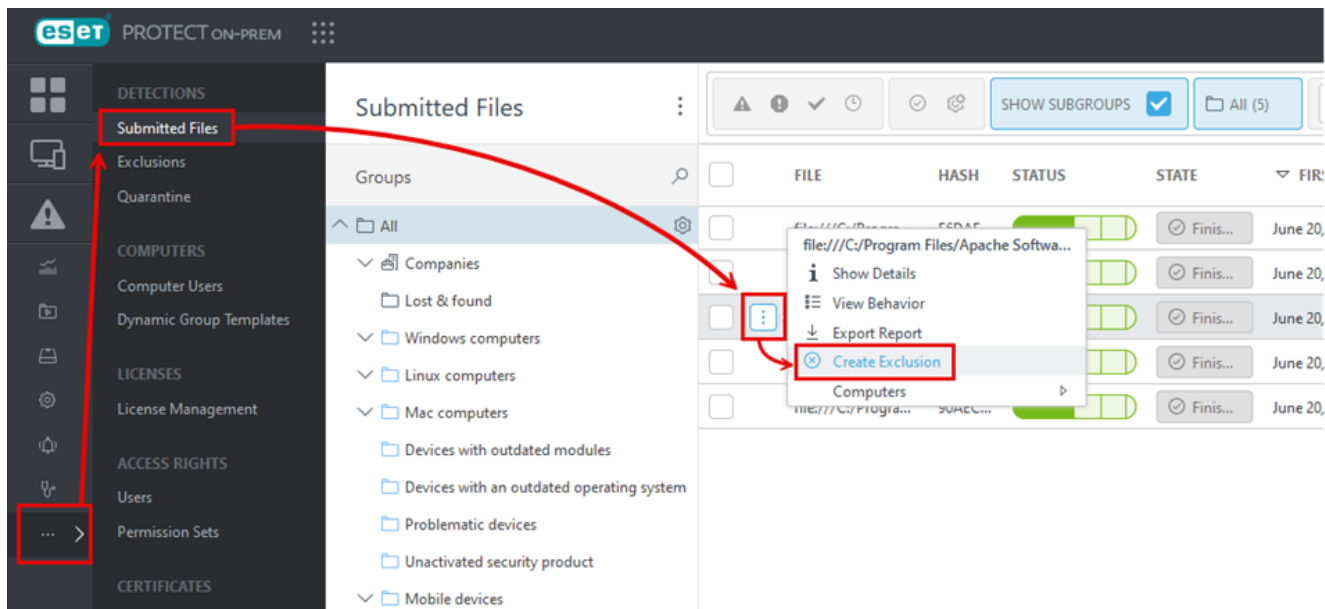
Add an exclusion

To create an exclusion for a file that has been detected and listed in the **Submitted files** window in the Web Console:

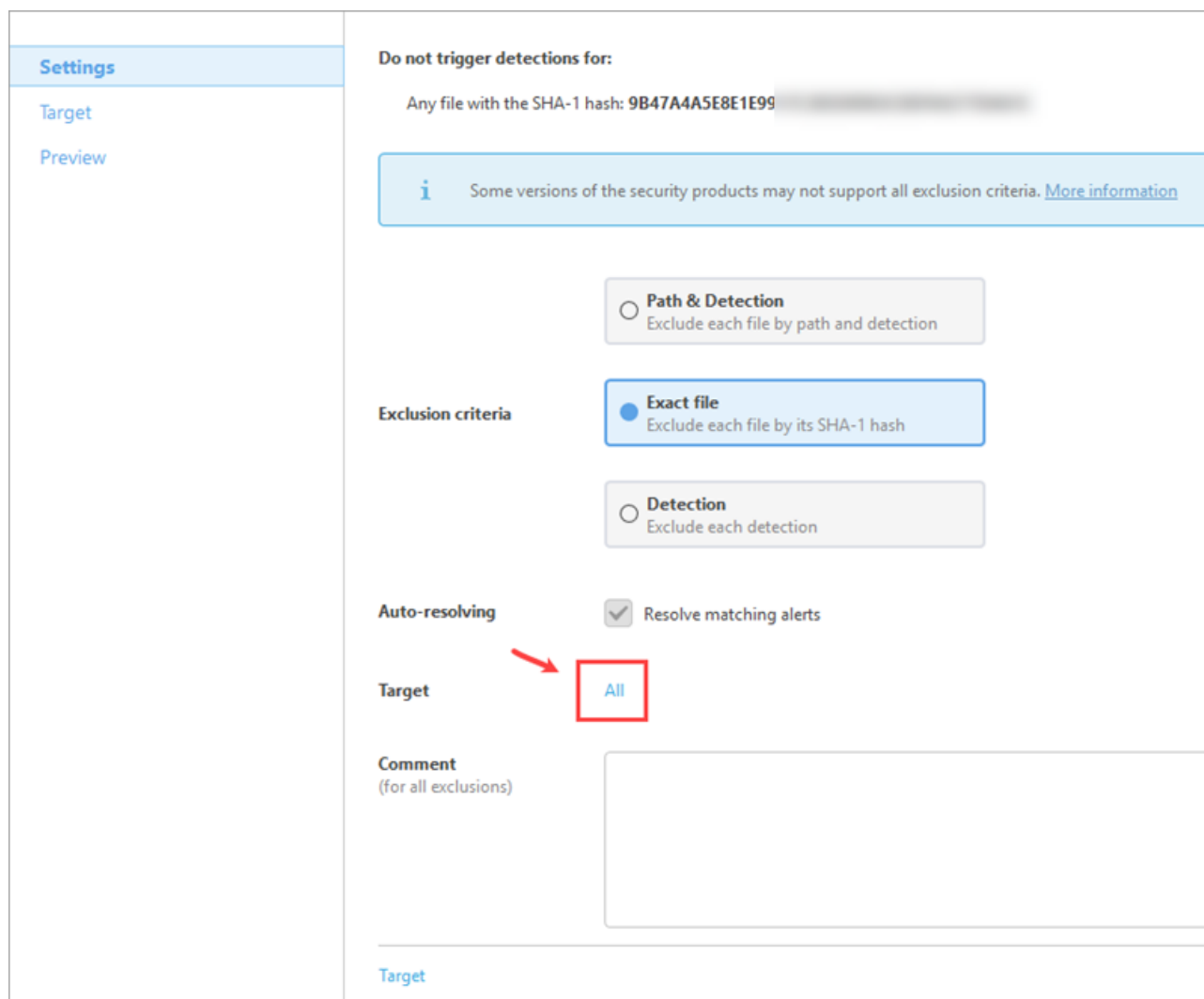
- Log in to the Web Console as an Administrator or another user with sufficient permissions for the target computer.
- Navigate to **Submitted Files**, select the hash of the file you want to exclude from scanning and then click **Create Exclusion**.



 [I am using ESET PROTECT](#)



3. Select a **Target** machine(s) for the exclusion. The group **All** is the pre-defined target. The exclusion will be applied to all supported ESET products on the target machine.



4. Click **Finish** to save and apply the exclusion. It can take up to two replication intervals for the exclusion to take effect. You can see the list of exclusions in the **Exclusions** menu.

Use exclusions to improve performance

ESET LiveGuard Advanced is capable of automatic analysis; a user can decide to exclude files and locations from the submission process such as sensitive data or trusted files or locations. By excluding files and locations, you can decrease the load on your network components. A high number of submitted files can cause a slowdown in network components (e. g. Proxy) and delay the delivery of analysis results. Follow the 3 step guide below to decrease the overall number of submitted files and improve the performance of your system.



Always be very careful when excluding a location from ESET LiveGuard Advanced submissions. The exclusion can pose a security risk to your system. Always consider possible implications and attack vectors.

I. [Review the submitted files](#)

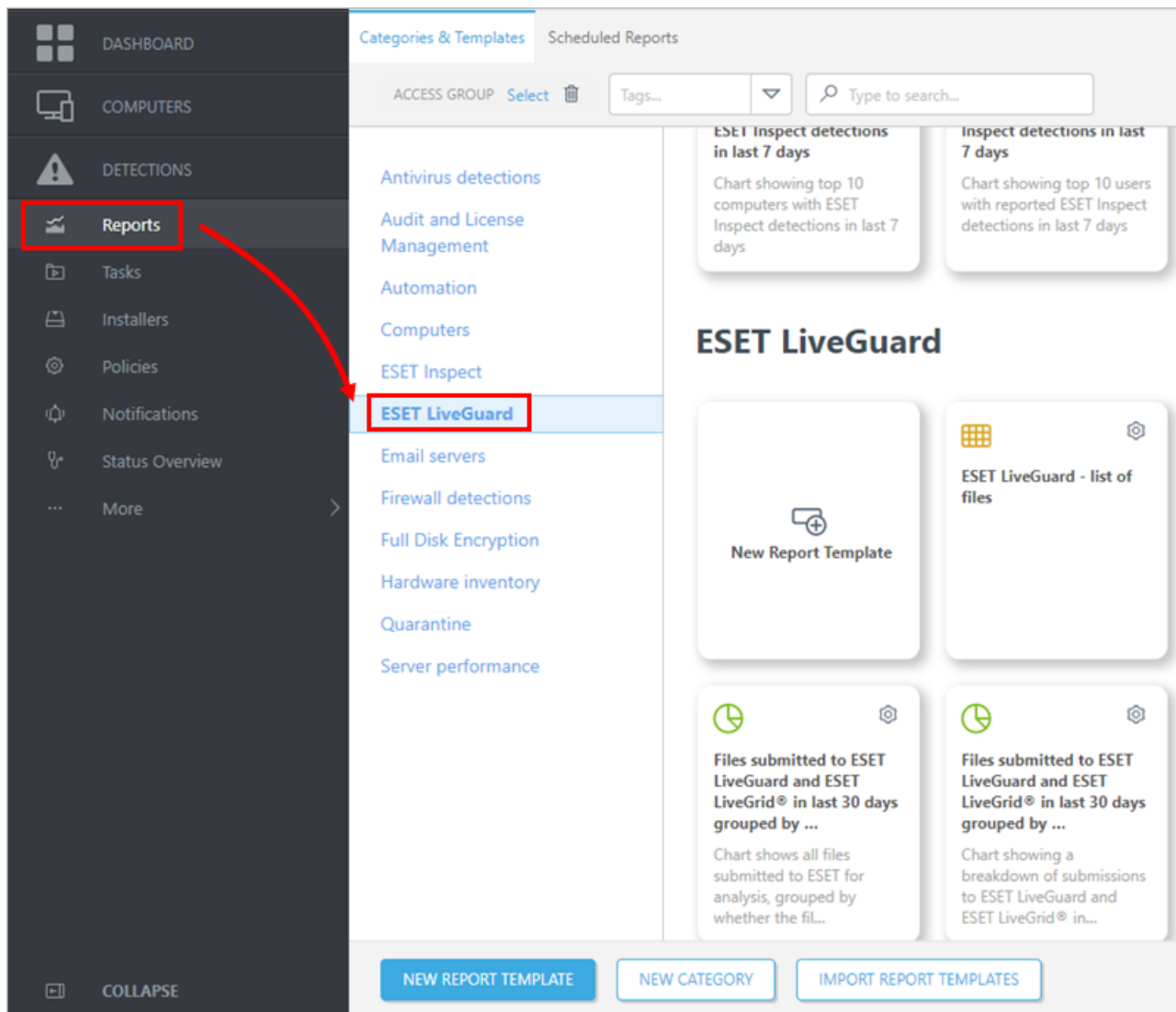
II. [Exclude folders](#)

III. [Exclude process](#)

Review list of submitted files

Create a list of top submitting computers

1. Click **Reports** > **ESET LiveGuard**.



2. Find the **Top 10 computers with file submissions to ESET LiveGuard and ESET LiveGrid in last 30 days** report template.

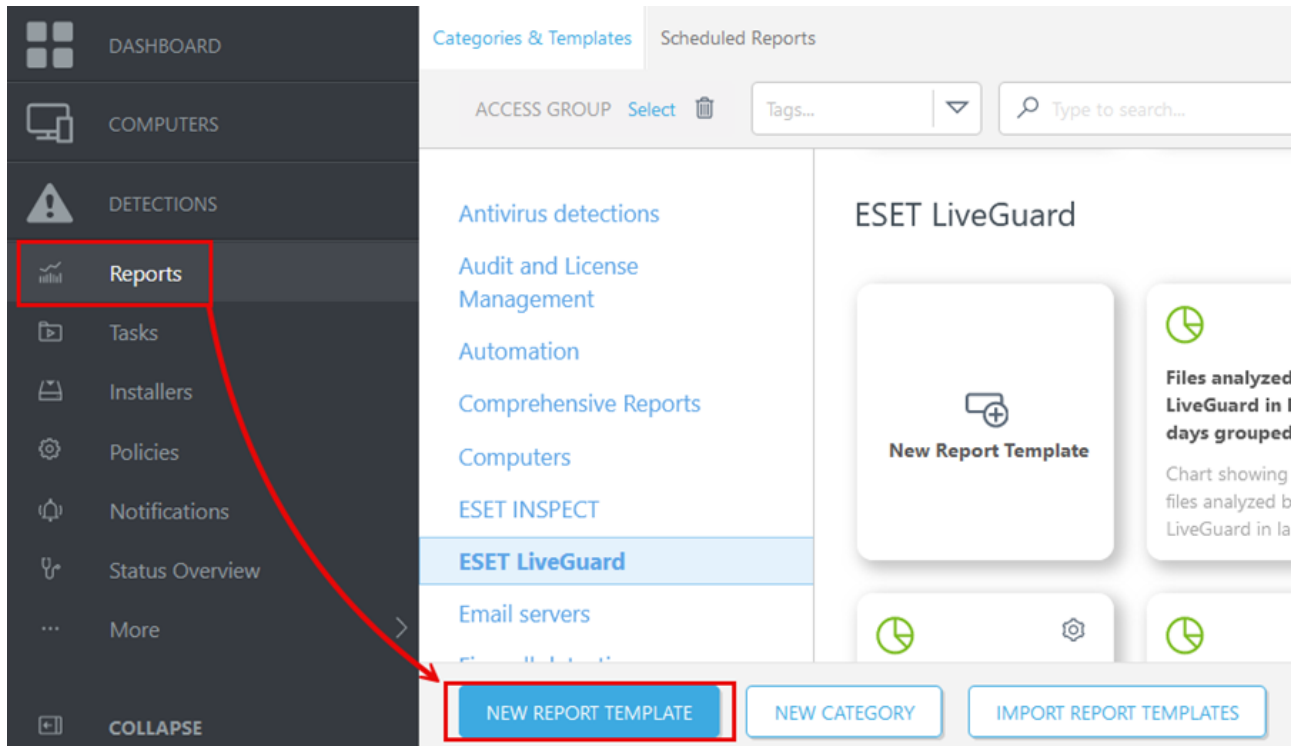
i You can edit the template first and change the computers count (10) or time frame (the last 30 days) to another value. You may need to change that if the situation in your network requires it.

3. Click **Generate now** and save the report (the list of top computers).

Create the list of submitted files for the top computers

You need the list of top submitting computers from the procedure above to complete the following steps.

1. In the Web Console, click **Reports > New Report Template**.



2. Give the template an appropriate **Name** and **Category**.

3. Continue to the **Chart** section.

New Report Template

Reports > ESET LiveGuard - list of files

Basic

Chart

Data

Sorting

Filter

Summary

Basic

Name

ESET LiveGuard - list of files

Description

Tags

Select tags

Category

ESET LiveGuard

BACK CONTINUE FINISH CANCEL

4. In the **Chart** section, select only the **Display Table** check box and continue to the **Data** section.

New Report Template

Reports > New Report Template

Basic

Chart

Data

Sorting

Filter

Summary

Table

Display Table

☒

Chart

Display Chart

☐

Chart Type

Bar Chart

5. In the **Data** section, click **Add Column** and add the following:

Computer - Computer name

ESET LiveGuard - Object URI

6. Click **Filter**.

New Report Template

Reports > ESET LiveGuard - list of files

Basic

Chart

Data

Sorting

Filter

Summary

Table Columns

Computer . Computer name	↓ ↗ 🗑️
ESET LiveGuard . Object URI	↑ ↗ 🗑️

Add Column

Preview

Show Preview

7. Click **Add column**, select **ESET LiveGuard . Relative time interval (Time of occurrence)**.

8. Set the interval to the last 30 days or other values relevant to your system.

Select time interval

Preset Select

Units Days

Start n day(s) ago : 30

End Now

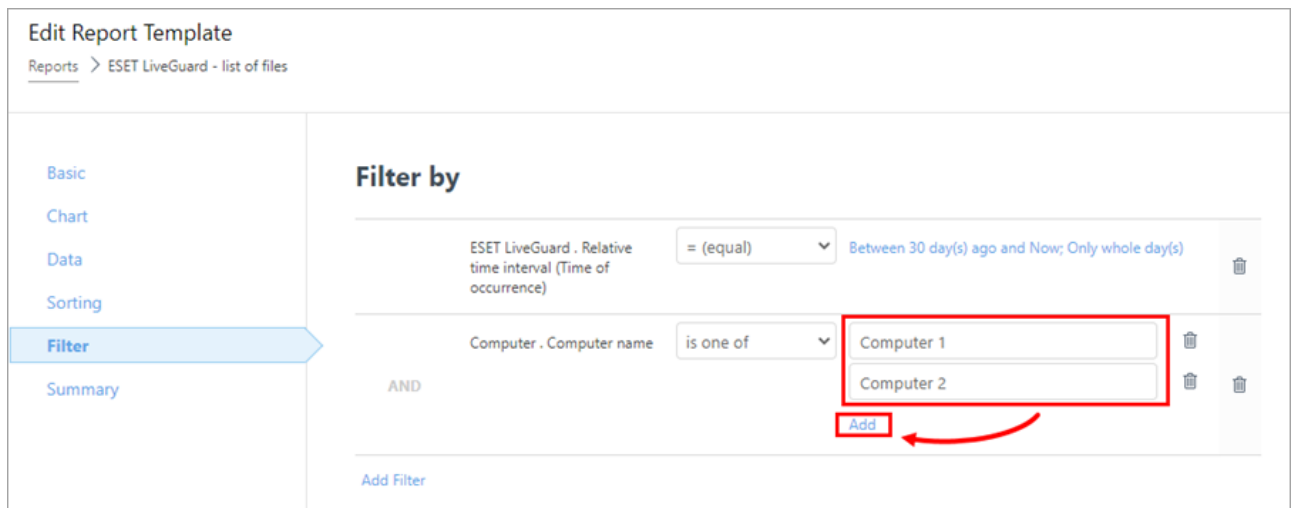
☒ Only whole day(s)

Example: between

OK CANCEL

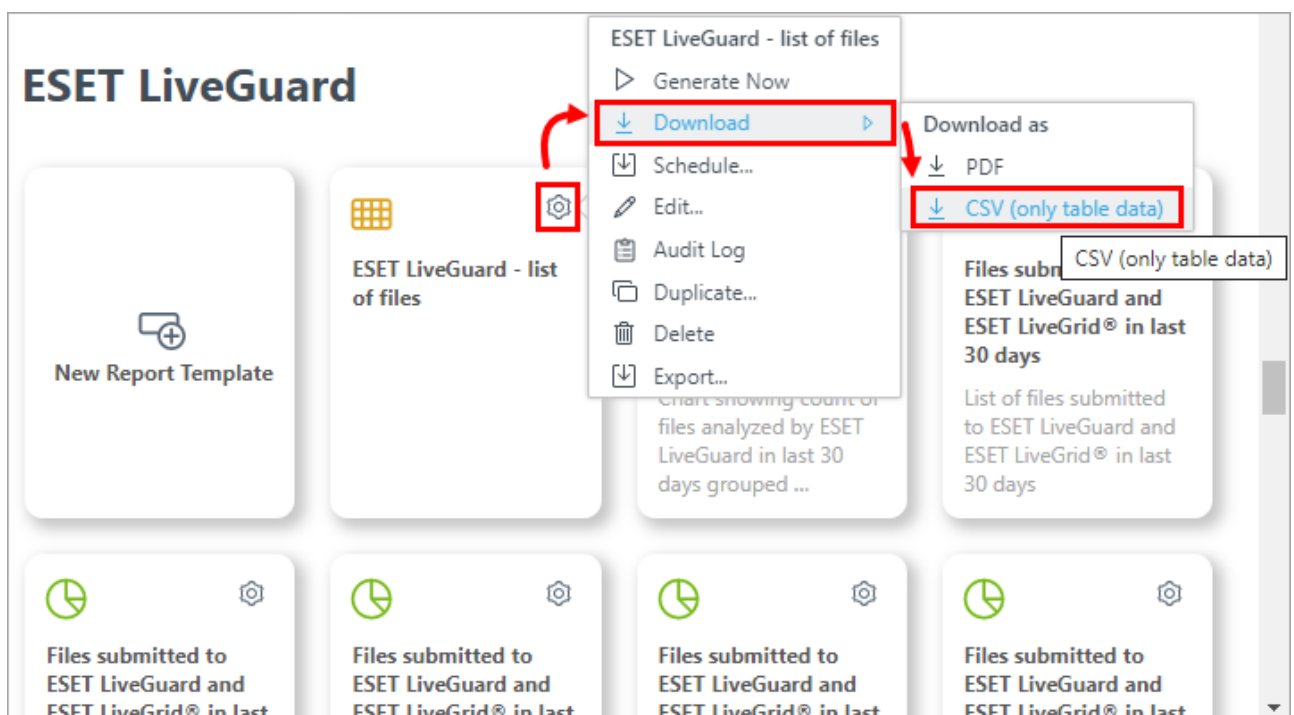
9. Click **Add Column** again and add **Computer . Computer name** item.

10. Add all the names of top computers from the previous procedure (top 10 substituting computers).



11. Click **Finish** to save the report template.

12. Find the new report template and generate a CSV file.

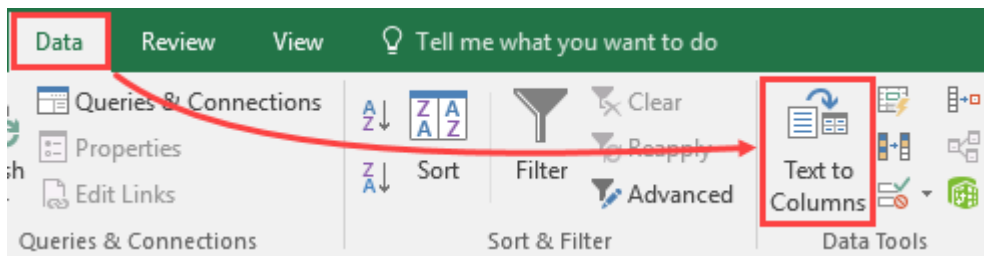


Data analysis

The following procedure requires third-party software (a spreadsheet editor and basic data analysis skills).

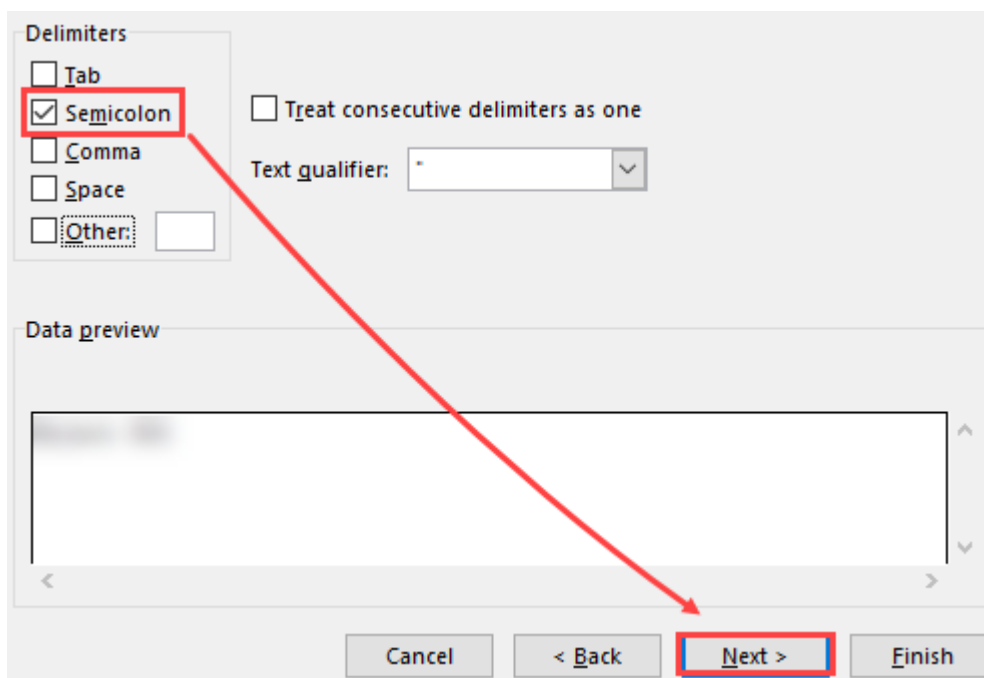
1. Open the CSV exported file in a spreadsheet editor, for example, Microsoft Excel.

2. Separate the data into two columns. In Microsoft Excel, select the first column, and navigate to **Data > Text to Columns**.



3. Select **Delimited > Next**.

4. Select the **Semicolon** delimiter and click **Next > Finish**.



Analyze the data.

Look for a pattern in submitted files and their locations. Find a pattern, usually a folder, from which the vast majority of files is submitted. When you have a pattern, suspicious computer, or application, you need to investigate the pattern.



Look for answers to the following:

- Which application is using this folder?
- What is this computer used for, what makes it stand out from others?
- What is the origin of those files?

The ultimate goal of the investigation is to find a pattern for exclusion.

When you have found the pattern, continue with [Exclude Folders](#).

Exclude folders

Consider project folders

Users with development software (e.g., Visual Studio) can exclude folders where they compile their projects. The compilation process creates many new files that ESET LiveGuard Advanced could submit for analysis. You can prevent sending an excessive number of files to the ESET LiveGuard Advanced. For example, you can exclude your project folder D:\Projects*

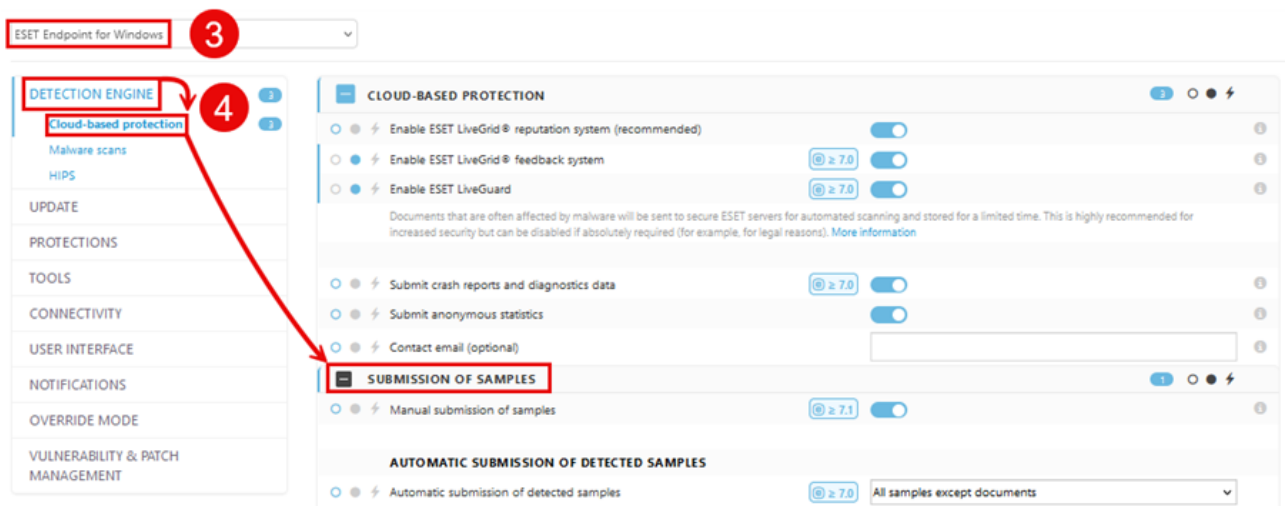
Folder exclusion process

Allows you to exclude specific files or folders from being sent to ESET LiveGuard Advanced. The excluded files will never be sent to ESET labs for analysis.

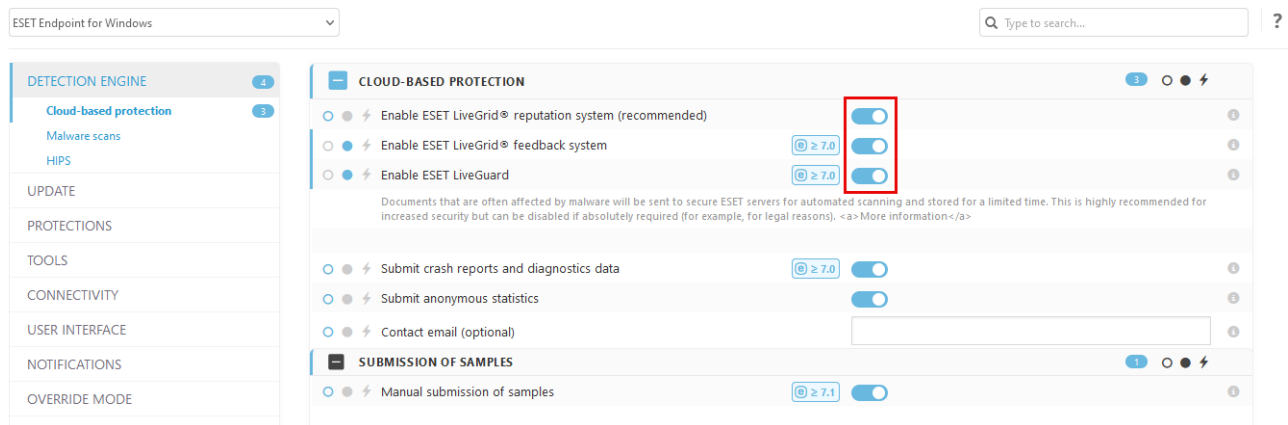


Always consider your security when you add an exclusion. Determine which applications can write to the excluded location and how excluding that locality could be misused by others.

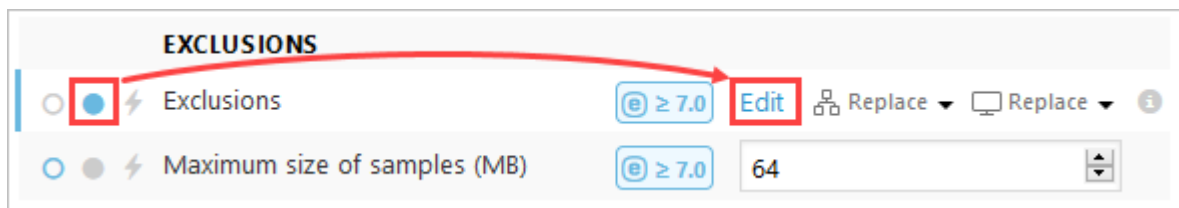
1. Log in to the Web Console, click **Policies > New Policy**.
2. In the **Basic** section, give the policy a proper **Name**.
3. In the **Settings** section, select **ESET Endpoint for Windows** (or the applicable [compatible product](#)).
4. Click **Detection Engine > Cloud-based protection**.



5. Enable the **ESET LiveGrid** and **ESET LiveGuard Advanced** toggles.



6. Under the **Exclusions** section, enable **Exclusions** and click **Edit**.



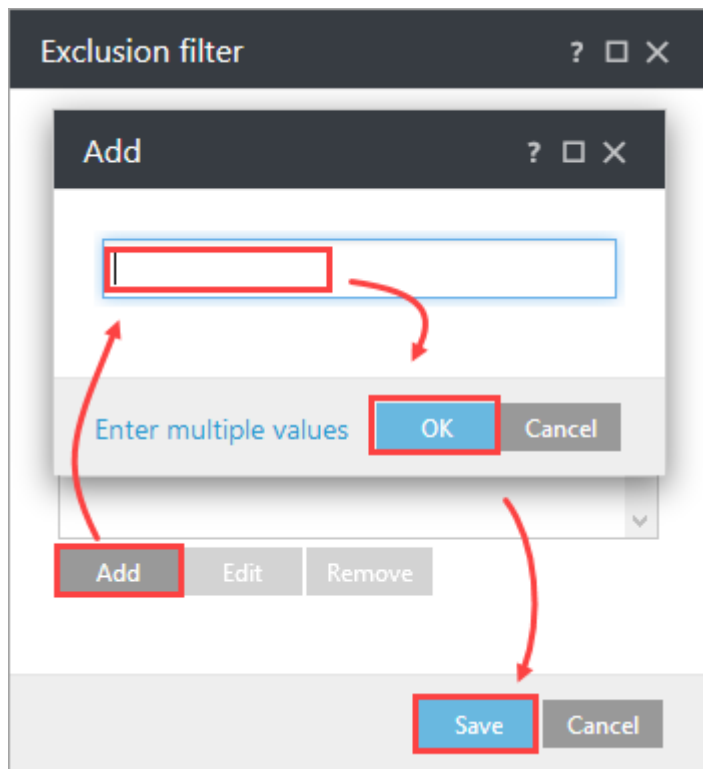
7. Click **Add** and type in the exclusion. To confirm, click **OK** > **Save**.

Exclusion examples:

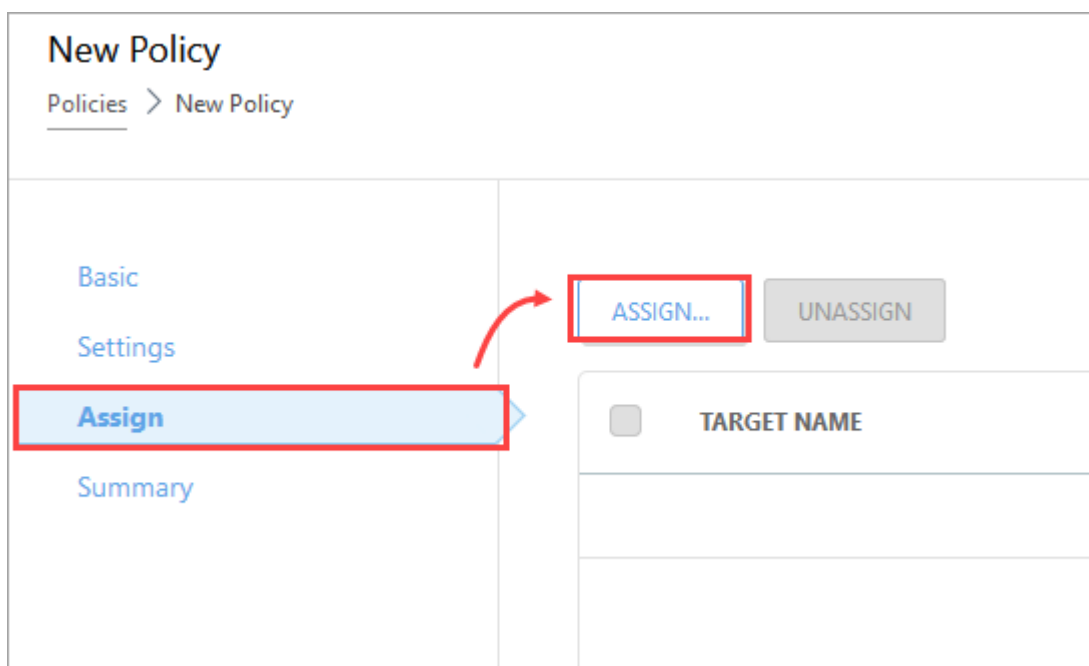
C:\MyProjects\
\DEVtool\debug



- You can use * and ? in exclusions. (* - for any string, ? - for any single character)
- Exclusions are not case-sensitive.
- Exclusions do not accept system variables and RegEx expressions.



8. Click **Assign** > **Assign** and select the applicable computers or groups.



9. To save and apply the policy, click **OK** > **Finish**.

Folder performance exclusion process

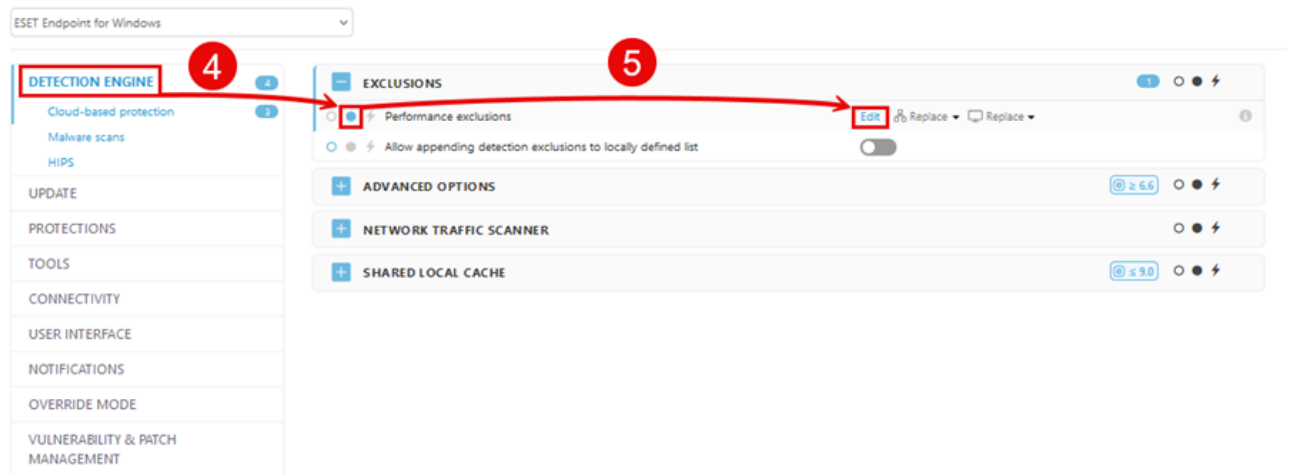
You can exclude specific files or folders from being scanned or sent to ESET LiveGuard Advanced. When you move the files outside the specified path or folder, they will be sent to the ESET LiveGuard Advanced.

1. Log in to the Web Console, click **Policies** > **New Policy**.

2. In the **Basic** section, give the policy a proper **Name**.

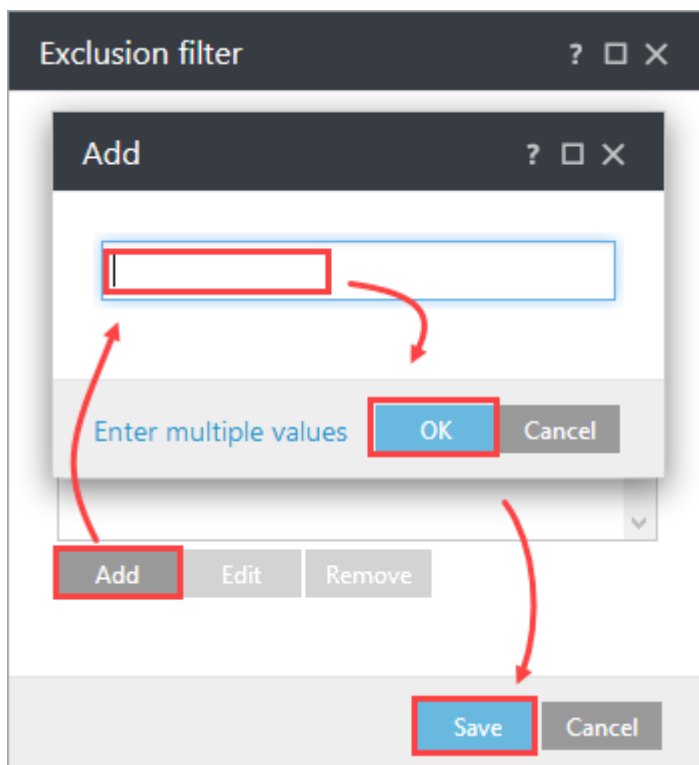
3. In the **Settings** section, select **ESET Endpoint for Windows** (or the applicable [compatible product](#)).

4. Click **Detection Engine**.



5. Under the **Exclusions** section, enable **Performance exclusions** and click **Edit**.

6. Click **Add** and type in the exclusion. To confirm, click **OK** > **Save**.



7. Click **Assign** > **Assign** and select the applicable computers or groups.

8. To save and apply the policy, click **OK** > **Finish**.

You can also investigate and [exclude processes](#).

Exclude process

Sometimes, you cannot specify a reliable pattern of the file locations and names, but you can exclude a process name instead.



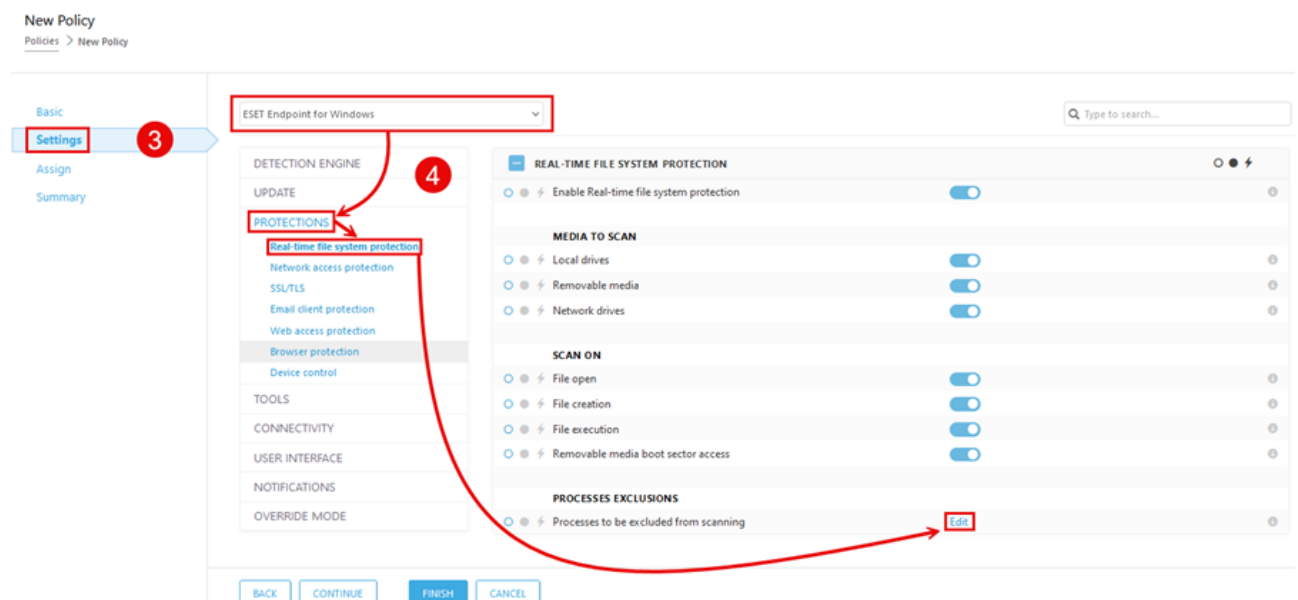
When you exclude the process, files created or manipulated by that process are not scanned for threats and submitted.

1. Log in to the Web Console, click **Policies** > **New Policy**.

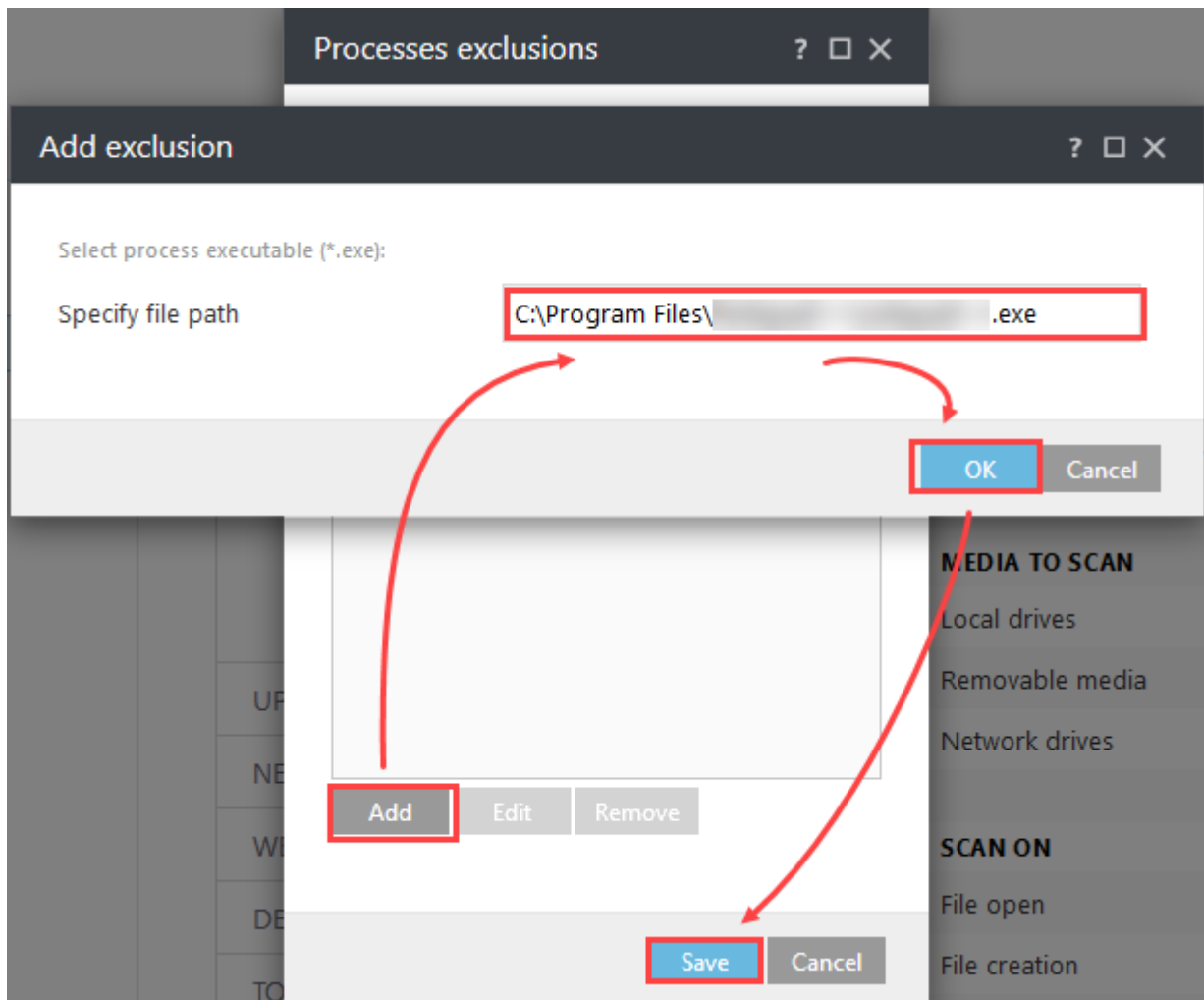
2. In the **Basic** section, give the policy a proper **Name**.

3. In the **Settings** section, select **ESET Endpoint for Windows** (or the applicable [compatible product](#)).

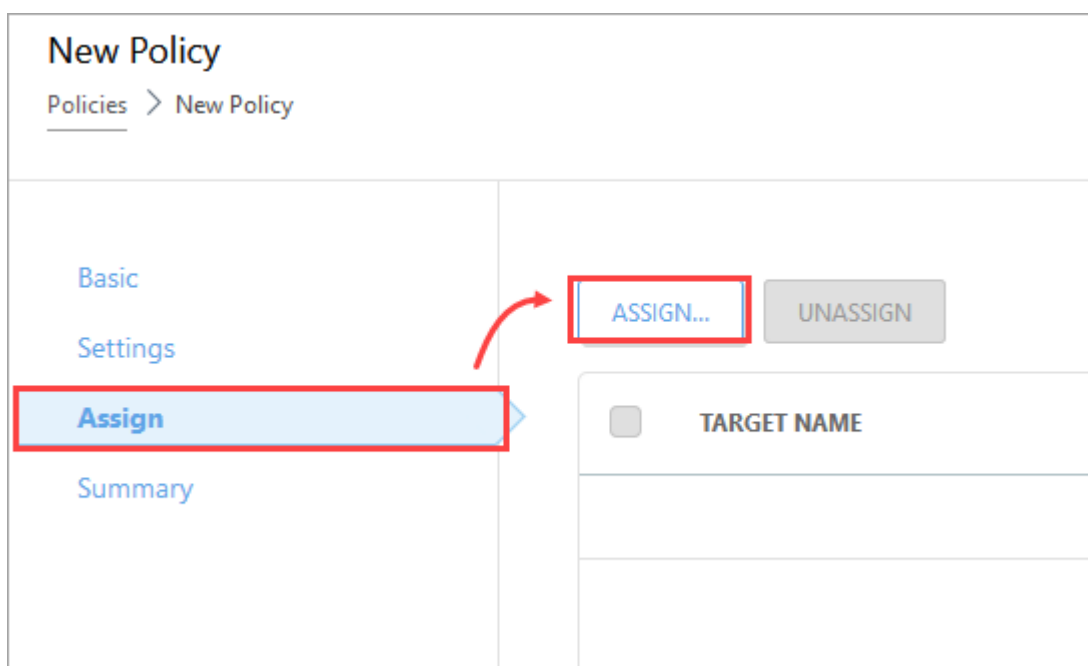
4. Click **Protections** > **Real-time file system protection** > **Real-time file system protection** > **Processes to be excluded from scanning** > **Edit**.



5. Click **Add**, type a process name (full executable address) and then click **OK** > **Save**.



6. Click **Assign** > **Assign** and select the applicable computers or groups.



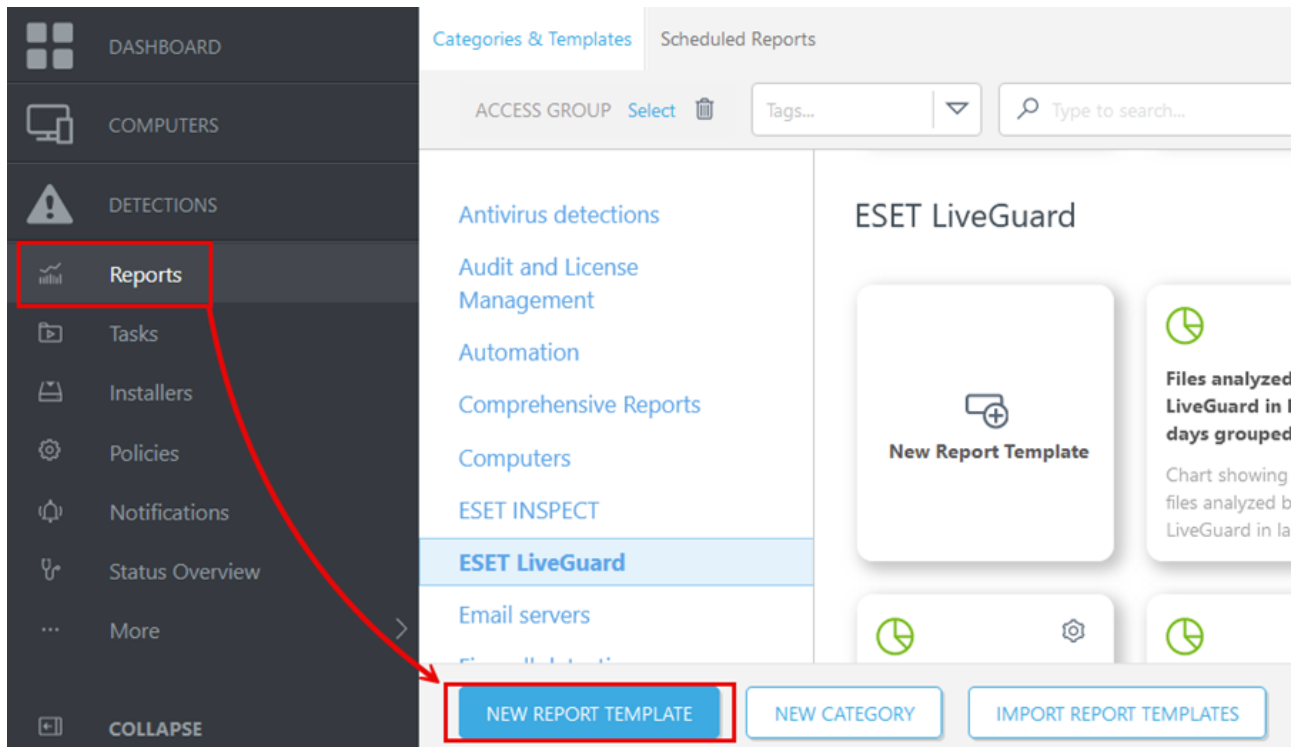
7. To save and apply the policy, click **OK** > **Finish**.

Review number of submitted files

Use the management console reporting tool to count the files you upload to ESET LiveGuard Advanced servers.

I. Create the list of submitted files

1. In the Web Console, navigate to **Reports > New Report Template**.



2. Give the template an appropriate **Name** and **Category**.

3. Continue to the **Chart** section.

New Report Template

Reports > ESET LiveGuard - list of files

Basic

Chart

Data

Sorting

Filter

Summary

Basic

Name

ESET LiveGuard - list of files

Description

Tags

Select tags

Category

ESET LiveGuard

BACK CONTINUE FINISH CANCEL

4. In the **Chart** section, select the **Display Table** check box and continue to the **Data** section.

New Report Template

Reports > New Report Template

Basic

Chart

Data

Sorting

Filter

Summary

Table

Display Table

☒

Chart

Display Chart

☐

Chart Type

Bar Chart

5. In the **Data** section, click **Add Column** and add the following:

Computer - Computer name

ESET LiveGuard - Object URI

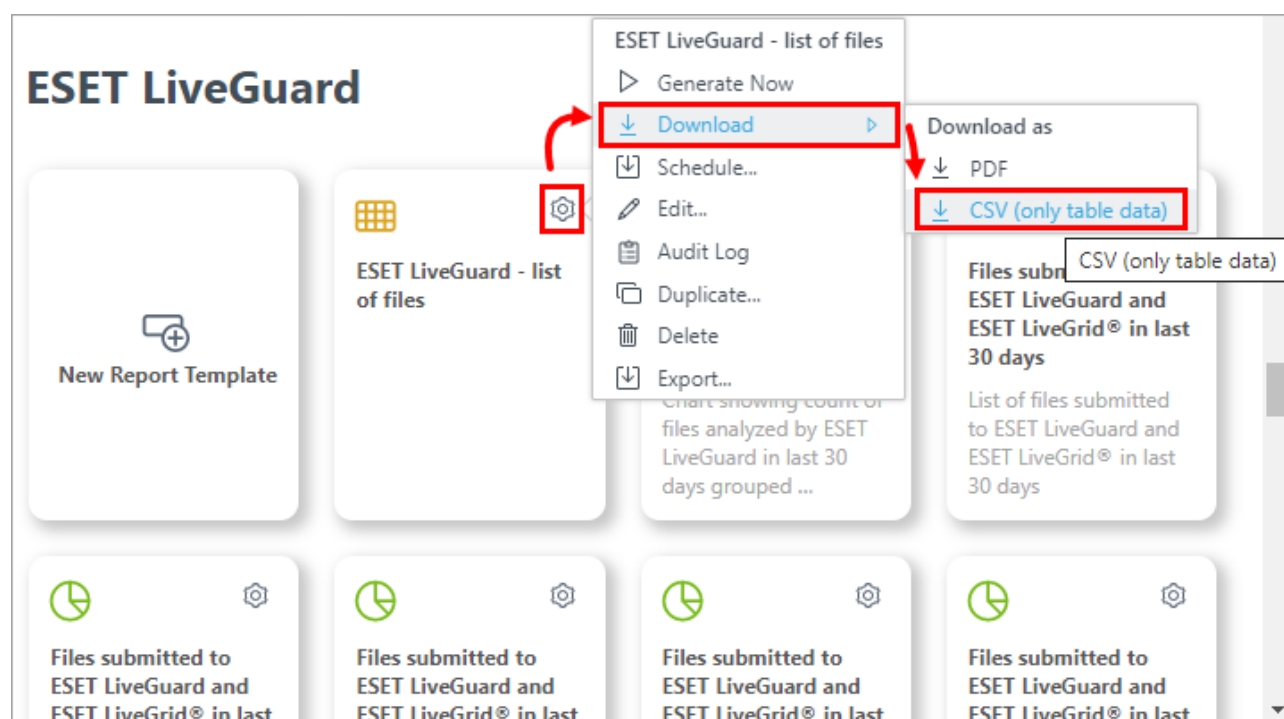
ESET LiveGuard - Time of occurrence

ESET LiveGuard - File content was sent

6. Click **Finish** to save the report template.

7. In the **Reports** menu, navigate to **ESET LiveGuard** reports.

8. Find the new report template and generate a CSV file.

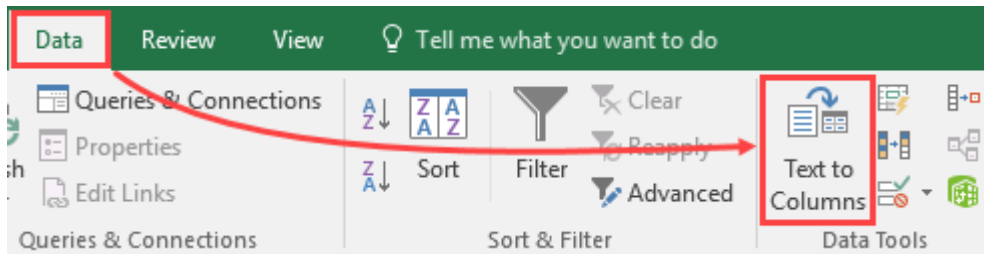


Data analysis

The following procedure requires third-party software (a spreadsheet editor and basic data analysis skills).

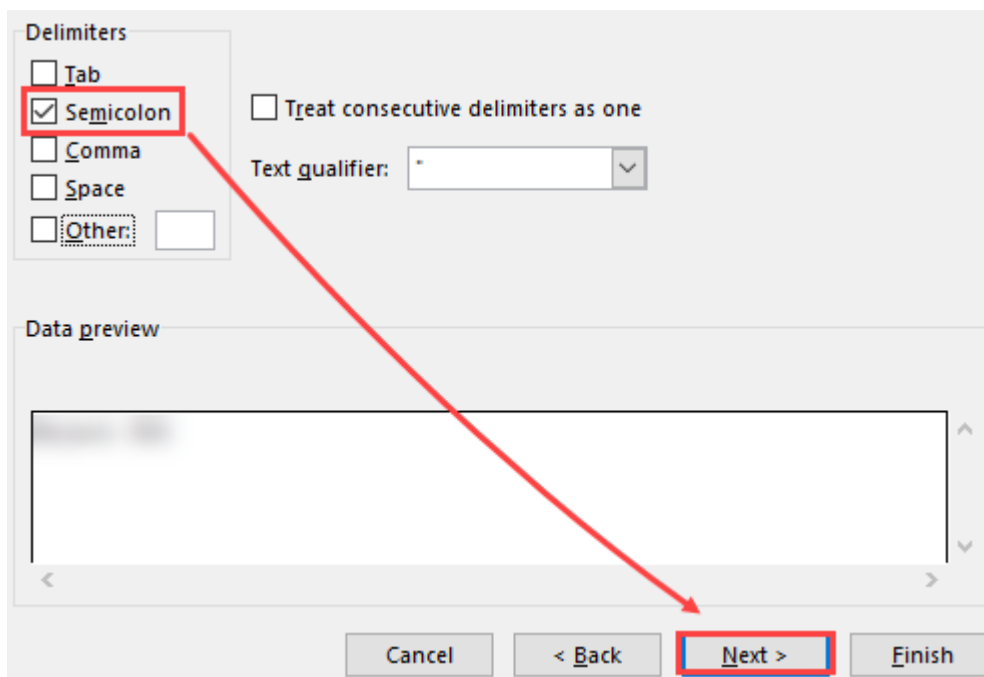
1. Open the CSV exported file in a spreadsheet editor, for example, Microsoft Excel.

2. Separate the data into two columns. In Microsoft Excel, select the first column, and navigate to **Data > Text to Columns**.



3. Select **Delimited** > **Next**.

4. Select the **Semicolon** delimiter and click **Next** > **Finish**.



Analyze the data.

Suggested steps for analysis

1. Remove lines where the **File content was sent** has value **No**.
2. Sort the data descending based on column **Time of occurrence**.
3. Select the desired time frame, for example, the last 30 days and copy the date to the next sheet.
4. In the next sheet, sort the data based on the column **Computer name**.
5. Count the number of lines (submitted files) for each distinct computer name.

Notification for detected threats

In the [remote management console](#) you can create a notification to be notified for each file marked by ESET LiveGuard Advanced a threat.

1. [Log in to the Web Console](#).

2. Click **Notifications > New Notification**.

The screenshot displays the ESET Web Console interface. On the left, a dark sidebar contains a menu with items like DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Installers, Policies, Computer Users, **Notifications** (highlighted with a red box), Status Overview, and More. A red arrow originates from this box and points to the 'NEW NOTIFICATION...' button located at the bottom right of the main content area. The main content area is titled 'Notifications' and features a table with columns: NAME, TAGS, and ENABLED. The table lists various notifications such as 'Malware outb...', 'Network attac...', 'Computers re...', 'Outdated mo...', 'Expiring CA c...', 'Expiring peer ...', 'Expiring licens...', 'Overused lice...', 'License limit a...', 'ESET Security ...', 'Managed clie...', 'Outdated ESE...', 'Failing server ...', 'Malicious file ...', 'Notification h...', 'New version o...', and 'Outdated vers...'. Each row has a checkbox in the 'ENABLED' column, all of which are currently disabled. A tooltip in the center of the main content area states: 'This is where you can see the list of your applied tags and quickly filter them.'

3. Type a name and optionally a description for the new notification.

4. Click the toggle below to enable the notification and click **Continue**.

New Notification

Notifications > ESET LiveGuard detection

Basic

Configuration

Advanced Settings - Throttling

⚠ Distribution

Name

ESET LiveGuard detection

Description

Tags

Select tags

Enabled

☒

BACK CONTINUE FINISH CANCEL

5. In the **Configuration** section, select **Events on managed computers** from the **Event** drop-down menu, and then select **Antivirus detection** from the **Category** drop-down menu.

6. Optionally, you can change the monitored static group. Only computers in this group and its sub-groups, where the user has permissions, are monitored for this notification.

7. Keep the operator **AND**, click **Add filter** and select **Detection name**.

8. Set the filter operator to **is one of** and type the string *ESET LiveGuard* to the text field and click **Continue**.

New Notification
Notifications > New Notification

Basic
Configuration
Advanced Settings - Throttling
⚠ Distribution

Event
Events on managed computers or groups

Category
Antivirus detection

Monitored static group ⓘ
All

Skip muted devices ⓘ
☐

Settings

Operator
AND (All conditions have to be true)

Filter By ⓘ
Antivirus detection . Detection name contains ESET LiveGuard

Add filter

BACK **CONTINUE** **FINISH** **CANCEL**

9. In the **Advanced Settings - Throttling**, you can set up [advanced timing](#) for notification distribution.

10. In the [Distribution](#) window, set up the proper distribution channel for you.

11. Save the notification.

ESET File Security For Windows users

i Before Jun 2021, the detection name reported from ESET Server Security was: **Blocked EDTD**. This has since been unified to **Dynamic Threat Defense** and later renamed to **ESET LiveGuard**.

FAQ

What files are sent to the sandbox?

If a file is submitted manually for ESET LiveGuard Advanced analysis, the system sends the selected file with no regard for file type. For automatic file submissions, the ESET security product only submits files that have not been scanned before and have the defined file type. The file type is determined based on the contents of a file, not its file extension since a user or malware can easily change the file extension.

ESET Mail Security and ESET Endpoint Security use a different approach. Different file types are processed differently in each of them.



















- ESET Mail Security - Processing is synchronized, the system waits for the result.
- ESET Endpoint Security and ESET Server Security - Processing is asynchronous. The system does not wait for the result.

Whether a file is submitted or not depends on the source of the file (web / mail / https).

Table of actions according to file type

Legend

 - Send  - Do not send

File type	Action (ESET Mail Security)	Action (ESET Endpoint Security, ESET Server Security)	Send only
Archives (.zip, .rar, .7z, .bzip2 and others)			<ul style="list-style-type: none"> • If the archive is unencrypted • If the contents of the archive are submitted for scanning (in this case, the entire archive is sent) Mail Security only
Documents (.docm, .xism, .pdf and others)			If active (containing JavaScript or any other active element)
Rich Text Format documents (.rtf)			
Executables (.exe, .dll, .sys, .elf, .so files and others)			<ul style="list-style-type: none"> • Only Linux products submit the following file formats: <ul style="list-style-type: none"> oLinux executable (.elf) oLinux libraries (.so)
Others (.jar, .lnk, .reg, .msi, .swf and others)			
Scripts (.bat, .cmd, .js, .vbs, .ps, .py, .sh, .pl and others)			<ul style="list-style-type: none"> • Only Linux products submit the following file formats: <ul style="list-style-type: none"> oPerl scripts (.pl) oPython scripts (.py) oShell scripts (.sh) oall executable text files (flagged with "x")
Images			
Ole2			If active (containing JavaScript or any other active element) - Mail Security only
.hta			

What is the maximum size of a file which can be sent?

ESET Security products can submit files up to 64 MB in size. You can define a maximum size to send in your policy for ESET LiveGuard Advanced.

What do the states of analysis and file statuses mean?

Refer to the [related chapter](#).

How to prevent ESET security product from deleting certain file?

You can add an [exclusion](#) on hash of a file and after the exclusion is applied, restore the file. Such a file will not be scanned by ESET security product again.

How is ESET LiveGuard Advanced updated?

ESET LiveGuard Advanced is updated remotely on the ESET cloud. You do not have to update the service manually. Update your installed security products when there is a new version available to get new features.

What happens to settings on product after the ESET LiveGuard Advanced license expires?


All settings stay unchanged, and [Web Console displays warning](#) about the expired license. [Apply another policy](#) to turn off the settings.

How long does it take to analyze the sample?

It typically takes up to five minutes to analyze a sample that has never been analyzed by ESET LiveGuard Advanced before. If a sample has already been analyzed, the user will receive the result in the next product request cycle, taking up to two minutes.

Can a computer benefit from ESET LiveGuard Advanced but submit no files?

You can set up an individual [policy](#) for a computer (or computers) with higher security requirements, which would not submit any files. If such the machine has [ESET LiveGuard Advanced activated](#), it receives priority results from analysis of other files submitted from its company. Files evaluated as malicious are afterward detected also by ESET LiveGrid®, which helps to protect other connected machines.

 You can find more questions and answers in our [FAQ](#) article.

Is ESET LiveGuard Advanced sharing results of analysis across my accounts or customers?

- ESET LiveGuard Advanced shares results immediately across all machines activated from a single ESET Business Account even with multiple licenses in the account.
- When using an ESET MSP Administrator account, ESET LiveGuard Advanced shares results immediately only within one MSP customer. Customers of a single MSP do not share their results.

When are the detection results from ESET LiveGuard Advanced available in ESET LiveGrid®?

The most severe detections are available several hours after the result, the less severe detections later.

Test ESET LiveGuard Advanced functionality

To test ESET LiveGuard Advanced functionality with and ability, follow the steps below:

 [Users with ESET PROTECT On-Prem](#)

I. Prerequisites

Ensure that ESET LiveGuard Advanced is [activated](#), [enabled](#), and running correctly.

II. Prepare the test file

1. Create a new folder on your computer.

2. Exclude this folder using [Performance exclusions](#).

3. Download the test file to an [excluded](#) folder:

Windows [test file](#)

Linux [test file](#)

4. Extract the downloaded archive into the excluded folder. The archive is password-protected, and the password is: infected

5. Windows users: To make the file unique, open the command line by pressing **Win+R** and type **powershell**. Navigate to the folder with the excluded test file. Run the command below, it adds the current timestamp to the end of the file, and the file gets a new hash:

```
Add-Content .\EdtdTestFile.exe $(date)
```

Linux users: To make the file unique, open the terminal, navigate to the folder with the excluded test file and type **date**
>> **create_eicar.bin** (optionally, you can rename the file). This command adds the current timestamp to the end of the file, and the file gets a new hash.

III. Test ESET LiveGuard Advanced

1. Copy the file prepared in section II. to a not excluded folder. The file is immediately sent to ESET LiveGuard Advanced because it is a new executable file.

2. Optionally, you can verify if the file was submitted:

In the ESET security product: Click **Tools > Log files > Sent files**.

In the ESET PROTECT Web Console: Click **More > Submitted files**.

3. After a few moments, the file is deleted from the computer, and you get a notification about the malware removal. You can see the information:

In the ESET security product: Click **Log files > Detections**.

In the ESET PROTECT Web Console: Click **More > Submitted files**.

4. If you run the test file before the analysis finishes, you get information that the ESET LiveGuard Advanced test file has run. The test file drops Eicar (a standard malware test file), which is immediately deleted. After the analysis is complete, the test file is cleaned.

IV. Test multiple files

After the test file is detected, its hash is saved locally. If you copy it from an excluded folder, it is detected immediately. You can make the file unique by repeating step II. 5. so it is sent for analysis again. Then you can follow instructions from section III.

V. Test proactive protection

1. Verify that the [proactive protection is enabled](#). In the ESET security product, (press F5 or) navigate to **Advanced Setup > Detection Engine > Cloud-based protection > ESET LiveGuard Advanced > Proactive protection = Block execution** until receiving the analysis result.

2. Ensure that the proper communication dialogs are enabled. In the ESET security product, press F5 or click **Advanced preferences > Notifications > Desktop notifications > Desktop notifications > Edit** and enable:

File analyzed

File in analysis

File not analyzed

3. Download the second test file to a non-excluded path and execute the file.

Windows [test file](#)

Linux [test file](#)

4. You will get a [notification](#) about a not-permitted operation. You cannot execute a file during the analysis.

5. When the analysis is finished, and the file is clean, you can execute the file.

I. Prerequisites

Ensure that ESET LiveGuard Advanced policy in ESET Cloud Office Security is enabled.

II. Prepare the test file

1. Download the [test file](#) to a location (or a machine) not protected by ESET LiveGuard Advanced [policy](#).

2. Extract the downloaded file. The file is an archive, and it is password-protected. The password is: `infected`.

3. To make the file unique, open the command line by pressing `Win+R` and type `powershell`.

4. Navigate to the folder with the test file.

5. Run the command below. It adds the current timestamp to the end of the file, and the file gets a new hash:

```
Add-Content .\EdtdTestFile.exe $(date)
```

III. Test ESET LiveGuard Advanced

1. Use the file from step II in one of the following ways:

- Move the file to OneDrive

- Create an email draft (using Microsoft Outlook) with the test file as an attachment

- Save the file to a protected location on Sharepoint

2. The file is immediately sent to ESET LiveGuard Advanced.

3. To verify the file was submitted in ESET Cloud Office Security, click **Logs > Submitted files**.

4. After a few moments, the file is deleted. You can see the analysis result in the **Submitted files**.

FAQ

Is this actual malware?

No, this `EdtdTestFile.exe` is just a dropper of Eicar (a standard malware test file). This event is being detected during analysis in a sandbox in ESET LiveGuard Advanced.

How can I be sure?

Here are the source codes of the test files:

- Windows executable

```
#include <fstream>
```

```
#include "tchar.h"
```

```
#include "windows.h"
```

```
int main()
```

```
{
```

```

std::ofstream dropped;

dropped.open(_T("eicar.com"));

dropped << "X50!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*";

dropped.close();

::MessageBox(nullptr, _T("EDTD test file has been executed.\n2020.4.15 10:34"),
_T("EDTD test file"), MB_OK);

return 0;
}

```

- Linux binary

```

#include <fstream>

#include <iostream>

#include <stdio.h>

int main()
{
    std::ofstream dropped;

    dropped.open("eicar.com");

    dropped << "X50!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*";

    dropped.close();

    std::cout << "EDTD test file has been executed." << std::endl;

    getchar();

    return 0;
}

```

Troubleshooting

- [Service does not work](#)
- [I have configured ESET LiveGuard Advanced, but it is still not working](#)
- [How to get logs?](#)

- [I do not see some submitted files in ESET PROTECT Web Console](#)
 - [Behavioral flags do not seem to be correct](#)
 - [How can I exclude a detected file from being moved to the Quarantine?](#)
 - [What if the license expires?](#)
 - [What if the Status field in the Submitted files window is empty?](#)
 - [ESET PROTECT On-Prem is not downloading the ESET LiveGuard Advanced data](#)
 - [Results are missing for submitted files in the ESET PROTECT Web Console](#)
 - [What if I am getting "Sent to LiveGrid" status for files submitted to ESET LiveGuard Advanced](#)
 - [The product refuses my ESET LiveGuard Advanced license](#)
 - [I am getting one of the following error messages under Computer Details > Alerts](#)
 - [Files sent to ESET LiveGuard Advanced do not display in Web Console](#)
 - [I am getting the following error: Your license does not include a file behavior report](#)
 - [I have a suspicious sample, what should I do?](#)
 - [Activation of ESET LiveGuard Advanced fails](#)
-

Service does not work

Verify ESET LiveGuard Advanced is [activated](#) and [configured](#).

Also, verify the following items:

- Is the ESET LiveGuard Advanced [license](#) used?
- Is the ESET LiveGuard Advanced [Policy](#) applied?

I have configured ESET LiveGuard Advanced, but it is still not working

Verify there is a working network [connection](#) between the ESET Management Agent and the ESET PROTECT Server.

View connectivity issues between the remote management server and ESET LiveGuard Advanced directly in the Web Console in **Dashboards > ESET PROTECT Server > ESET PROTECT On-Prem network peers with problems**.

You can also check the **HTTP Proxy** settings in [ESET PROTECT Settings](#).

Collect the log files

You can review the log files section in the [ESET PROTECT On-Prem Online Help guide](#).

I do not see some submitted files in the Web Console

This is typical behavior if you are using [a roaming endpoint](#).

Behavioral flags do not seem to be correct

If the reported behavioral flag does not seem to be correct, you can:

- Report it to [ESET support](#) or send the sample to samples@eset.com. See [our article](#) about submitting samples.
- Visit the [ESET Security Forum](#) and consult the ESET community for information about issues you may encounter.

How can I exclude a detected file from being moved to the Quarantine?

If you are sure that the detected file is safe, you can [whitelist](#) it.

What if the license expires?

When the ESET LiveGuard Advanced license expires, you are still able to [submit](#) suspicious files for malware analysis. However, you will not receive the file analysis [results](#) or the [file behavior report](#).

What if the Status field in the Submitted files window is empty?

Are you a user of ESET PROTECT?

i This troubleshooting method is for users of on-premises remote management console ESET PROTECT On-Prem.

1. Check the **Dashboard** (in your remote management console) as described here: [I have configured the ESET LiveGuard Advanced, but it is still not working](#)
2. Click **Reports > Audit and License Management > Audit log > Generate and download > PDF**. You can attach this log when requesting support from ESET Technical Support or inspect it for yourself.

If there are ESET LiveGuard Advanced related errors or problems, get the trace logs and contact ESET Technical Support (see the steps below). Otherwise, you can [restart](#) the results retrieval process at the remote management server.

How to get the trace log:

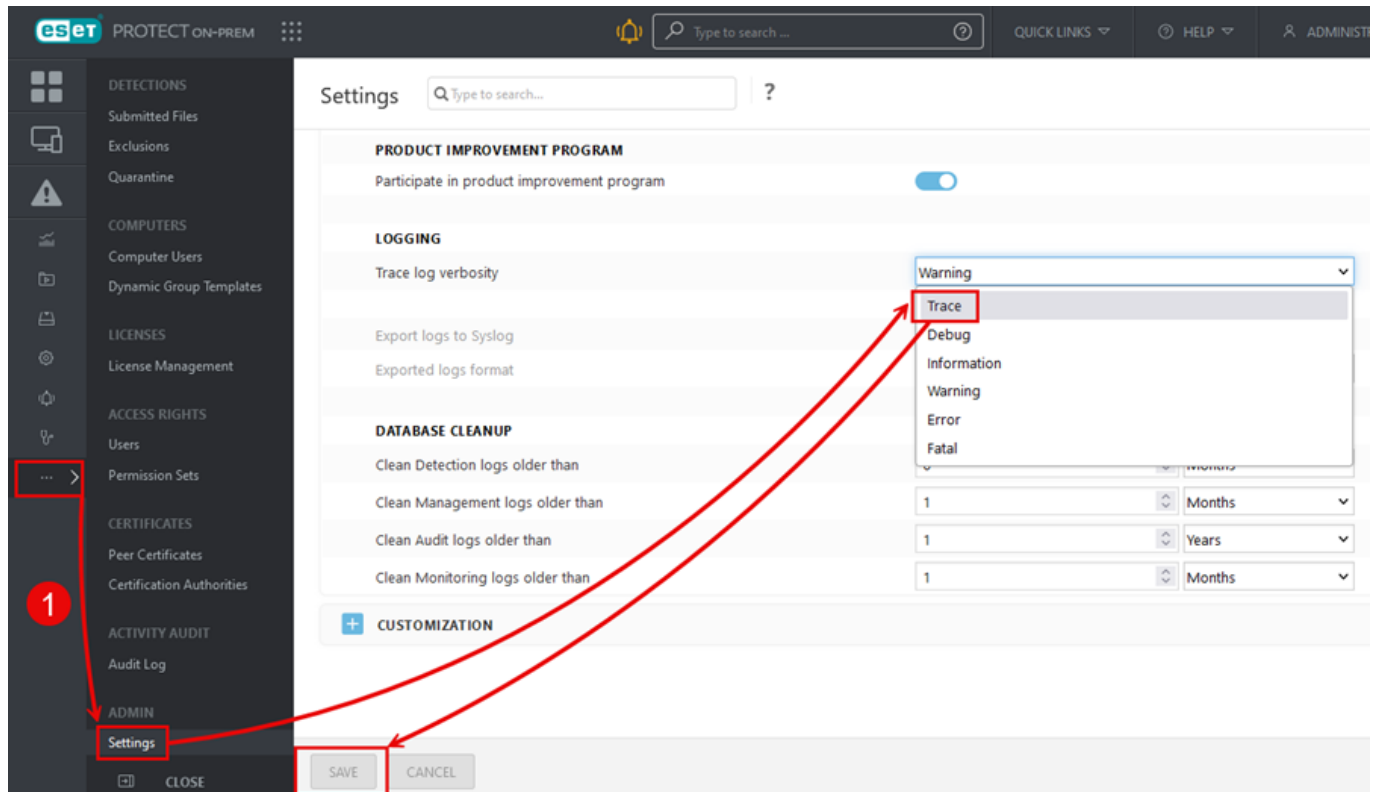
1. To enable trace verbosity logging in the Web Console, click **More > Settings > Advanced Settings > Logging > Trace log verbosity > Trace**.

2.Restart the ESET PROTECT On-Prem service or the machine and wait 15 - 20 minutes.

3.Logs are located on the ESET PROTECT Server machine:

I.Windows: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

II.Linux: */var/log/eset/RemoteAdministrator/Server/*



How to restart the download of the ESET LiveGuard Advanced results

Restart the data retrieval process on the ESET PROTECT Server. A restart can help when the Server is not downloading new data from the ESET cloud, or the download is too slow.

1.Turn off the ESET PROTECT Server service.

2.Log in to the ESET PROTECT database using SQL Server Management Studio or the MySQL client on Linux systems.

3.Modify the table `tbl_key_value_pairs` in the ESET PROTECT database:

When using SSMS, open the table and remove the line containing the string `eset-dynamic-threat-detection-customers`

When using MySQL, open the database and execute the command `delete from tbl_key_value_pairs where pair_key = 'eset-dynamic-threat-detection-customers';`

When using ESET PROTECT Virtual Appliance:

a)Log in to the Terminal on the virtual machine where the appliance is running.

b)Log in to the database: `mysql -u root -p era_db`

c)Type the password. It is usually the same as your Web Console Administrator's password.

d)Run the following command:

```
delete from tbl_key_value_pairs where pair_key = 'eset-dynamic-threat-detection-customers';
```

4.Turn on the ESET PROTECT Server and do not restart or switch it off for 24 hours.

Results are missing for submitted files in the ESET PROTECT Web Console

Possible causes:

- ESET LiveGuard Advanced was activated using a license key instead of an EBA account

Solution:

- 1.Remove the current license from ESET PROTECT On-Prem
- 2.Add the license eligible for ELGA to ESET Business Account
- 3.Add the license using the EBA account to ESET PROTECT On-Prem
- 4.Re-activate ESET LiveGuard Advanced for the client
- 5.Restart the ESET PROTECT server service

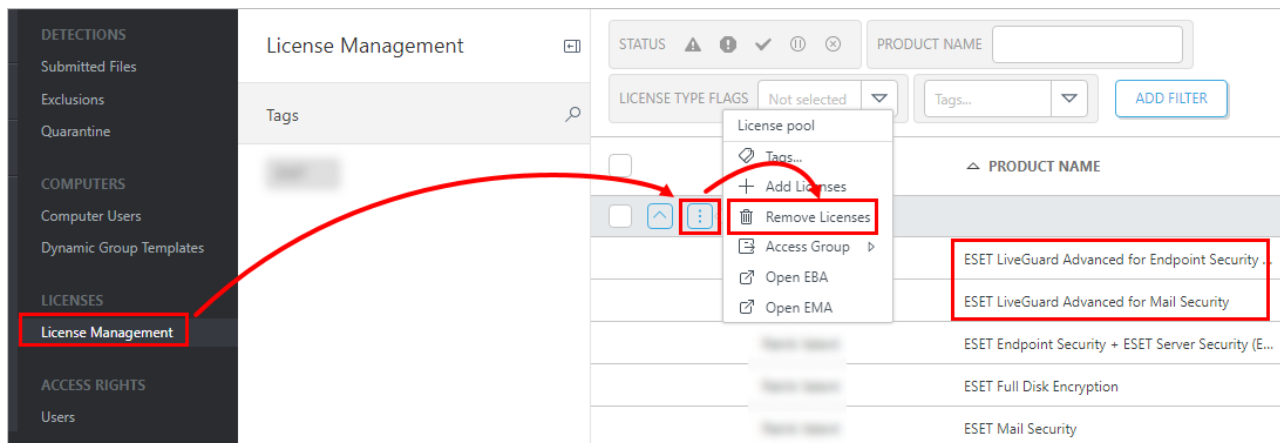
What if I am getting "Sent to LiveGrid" status for files submitted to ESET LiveGuard Advanced

Possible causes:

- The file or spam email you submitted was already detected.
- The ESET LiveGuard Advanced license was not [imported](#) using EBA but was directly imported to the security product or the remote management console.

To enable sending files to ESET LiveGuard Advanced:

- 1.Remove the license from your **License Management**.



2. [Import](#) your license to EBA.

3. [Synchronize](#) your EBA with your remote management Server (ESET PROTECT On-Prem).

4. Certain modules need to be reloaded on client machines. There are two options to reload modules:

- Wait for a few hours until the modules are reloaded.
- For immediate reload, you can "restart" ESET LiveGuard Advanced on clients. To restart, send a deactivation [policy](#) for ESET LiveGuard Advanced, and when the policy is applied, send another one for [activation](#).

The product refuses my ESET LiveGuard Advanced license

- After entering your ESET LiveGuard Advanced license key in the Web Console, you received the following error message:

Failed to add license by license key: License is issued for a product that can not be managed with ESET PROTECT On-Prem. Please enter a different license.

- After entering your ESET LiveGuard Advanced license key directly in the security product, you received the following error message:

Activation failed. License and product do not match.

The license must be entered only via EBA. [Read more about importing the license.](#)

I am getting one of the following error messages under Computer Details > Alerts

Problem	Problem detail	Cause and solution
ESET LiveGuard Advanced is not accessible	ESET LiveGuard Advanced is not working. Connection to authentication servers failed.	<p>The ESET license servers are not accessible.</p> <ul style="list-style-type: none"> • Firewall (another setting) is blocking the communication. • The service is temporarily unavailable. Check your firewall settings.

Problem	Problem detail	Cause and solution
ESET LiveGuard Advanced is not accessible	ESET LiveGuard Advanced license has expired.	Your ESET LiveGuard Advanced license was functional and is now expired. Renew the license or disable the ESET LiveGuard Advanced setting in the policy .
ESET LiveGuard Advanced is not accessible	The ESET LiveGuard Advanced servers cannot be reached. This could be due to an outage or a problem with the network connection.	Your machine cannot reach ESET LiveGuard Advanced servers . This is usually caused by a proxy service failure. Try to restart your proxy service. If the problem persists, the proxy could be overloaded. You can: <ul style="list-style-type: none"> • Divide the load from agents to more proxies • Upgrade hardware on the proxy machine • Use the Apache HTTP Proxy 64-bit build (if you are using the 32-bit, and your system is x64 architecture) • Temporarily stop using the proxy to confirm that it is causing the issue • If you are using Apache HTTP Proxy, you can move to ESET Bridge.
Web Console is not showing any results	Analysis results are not delivered to the ESET PROTECT Server.	The HTTP Proxy could be overloaded. Try moving the HTTP Proxy to a different server or/and adding more resources. When you move the HTTP Proxy to a new address, you need to update the endpoints' policy too.
ESET LiveGuard Advanced is not accessible	ESET LiveGuard Advanced offline license error.	ESET LiveGuard Advanced does not support offline license activation. Check your license.
ESET LiveGuard Advanced is not accessible	ESET LiveGuard Advanced is not working. Unknown authentication error.	ESET authentications servers are not reachable from the client machine. Verify you can reach <i>edf.eset.com</i> .

Files sent to ESET LiveGuard Advanced do not display in the Web Console

- If your OS—usually an earlier Windows Server—does not trust the *ts.eset.com* certificate, files are not sent to the ESET LiveGuard Advanced servers. To fix this trust issue, import [DigiCert Global Root G2](#) and [Thawte TLS RSA CA G1](#) root certificates to your operating system.
- The Web Console can display submitted files only when the client Management Agent is connecting (replicating) to the ESET PROTECT Server. Files submitted from [roaming endpoints](#) are displayed after the Agent connects the Server again.



When using ESET LiveGuard Advanced in an enterprise-level environment (hundreds of machines or more), we recommend deploying HTTP Proxy on a dedicated server. Running the HTTP Proxy service on a heavily utilized server (e.g., besides the ESET PROTECT Server or database) may result in ESET LiveGuard Advanced connection problems.

You can [exclude selected folders and processes](#) to decrease the number of submitted files and improve the overall performance.

I am getting the following error: Your license does not include a file behavior report

If you are using EBA to manage your licenses and your total seat count for ESET LiveGuard Advanced licenses is below 100, you are not eligible for full Behavioral report. [Some versions](#) of management console does not provide

the behavior report at all. You need to raise your seat count to 100 or more to get the report.

I have a suspicious sample, what should I do?

See the [Recommendations for users with a suspicious sample](#).

Activation of ESET LiveGuard Advanced fails

If you have added a license via License Key and then converted to a cloud protection tier, you will see ESET LiveGuard Advanced license in the Console, but the activation would fail. You need to remove the protection tier from license management and [add it via EBA](#).

Perform diagnostics


If ESET LiveGuard Advanced is not working:

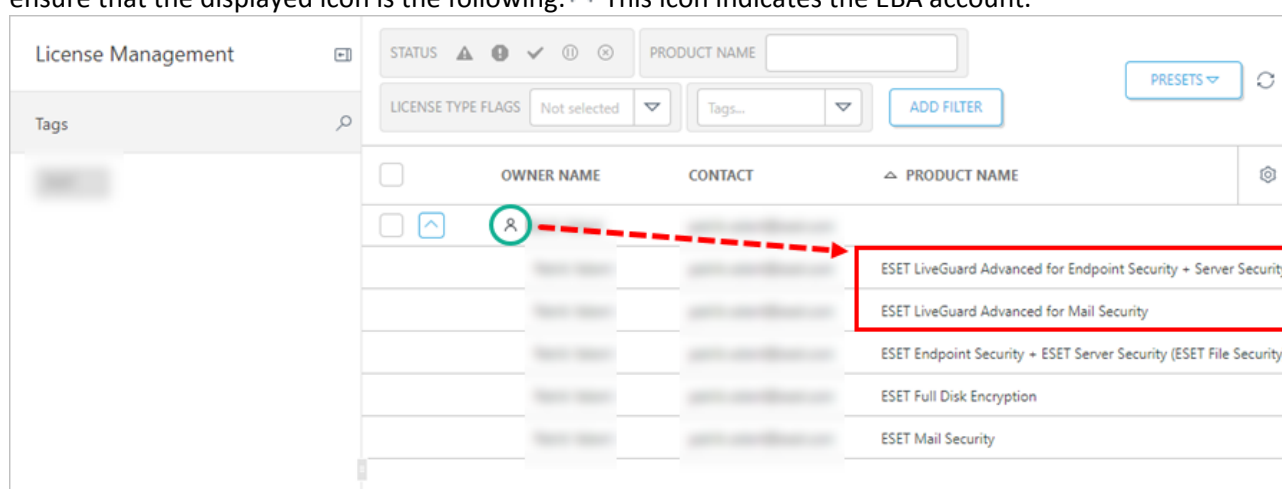
- Ensure that you meet all [requirements](#).
- In the Web Console, look for a cause using the following instructions.

ESET LiveGuard Advanced license

1. [Log in to the Web Console](#).

2. Click **More > License Management**.

3. Verify if your ESET LiveGuard Advanced license is listed. If the license is not there, [add it](#) using your ESET Business Account or ESET MSP Administrator. If you are getting your licenses from ESET Business Account, ensure that the displayed icon is the following:  This icon indicates the EBA account.

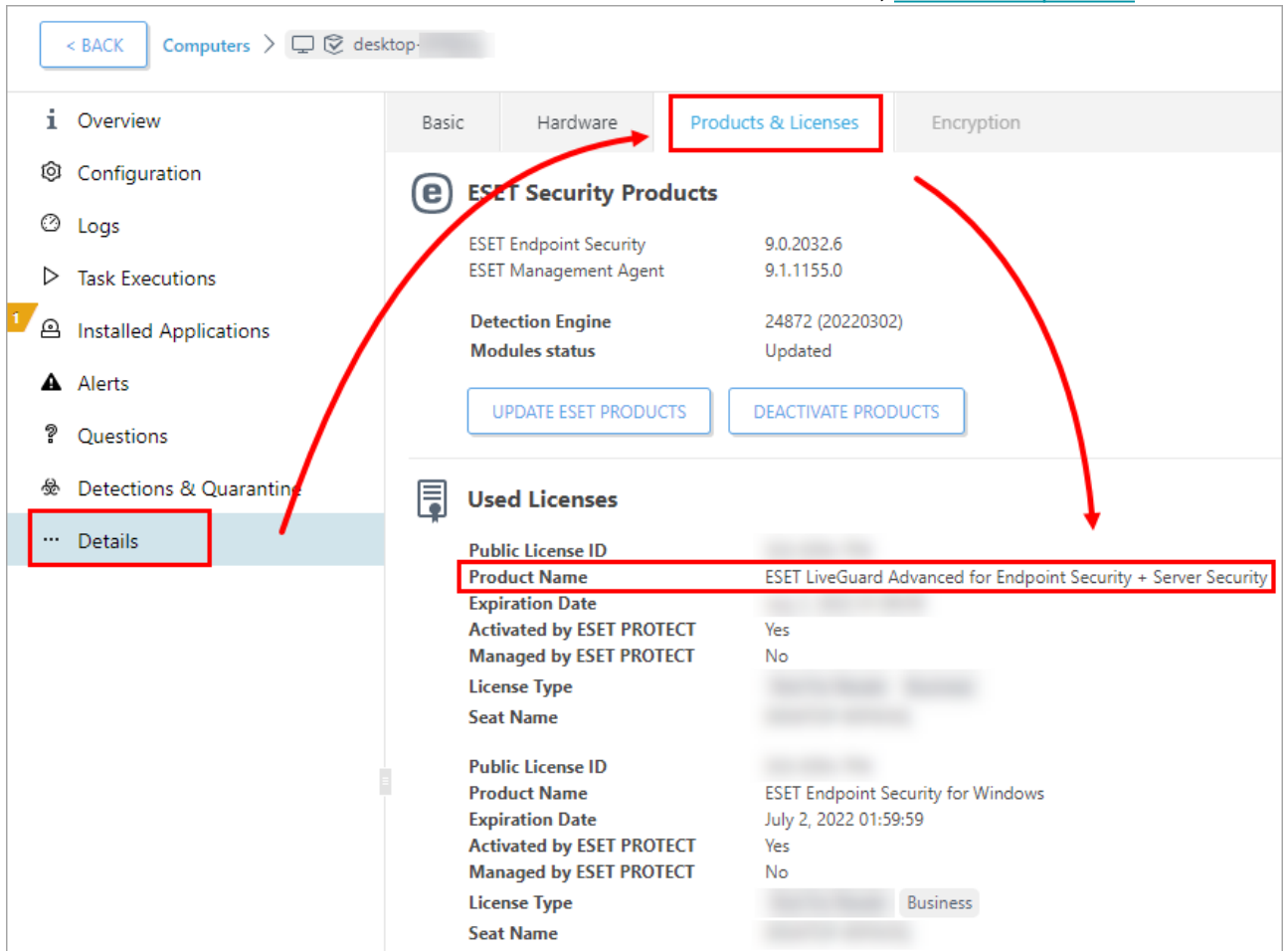


Users running supported Linux products can verify their license and seat ID locally using a Linux terminal.

- [Verify the license on ESET Server Security for Linux](#).
- [Verify the license on ESET Endpoint Security for Linux](#).

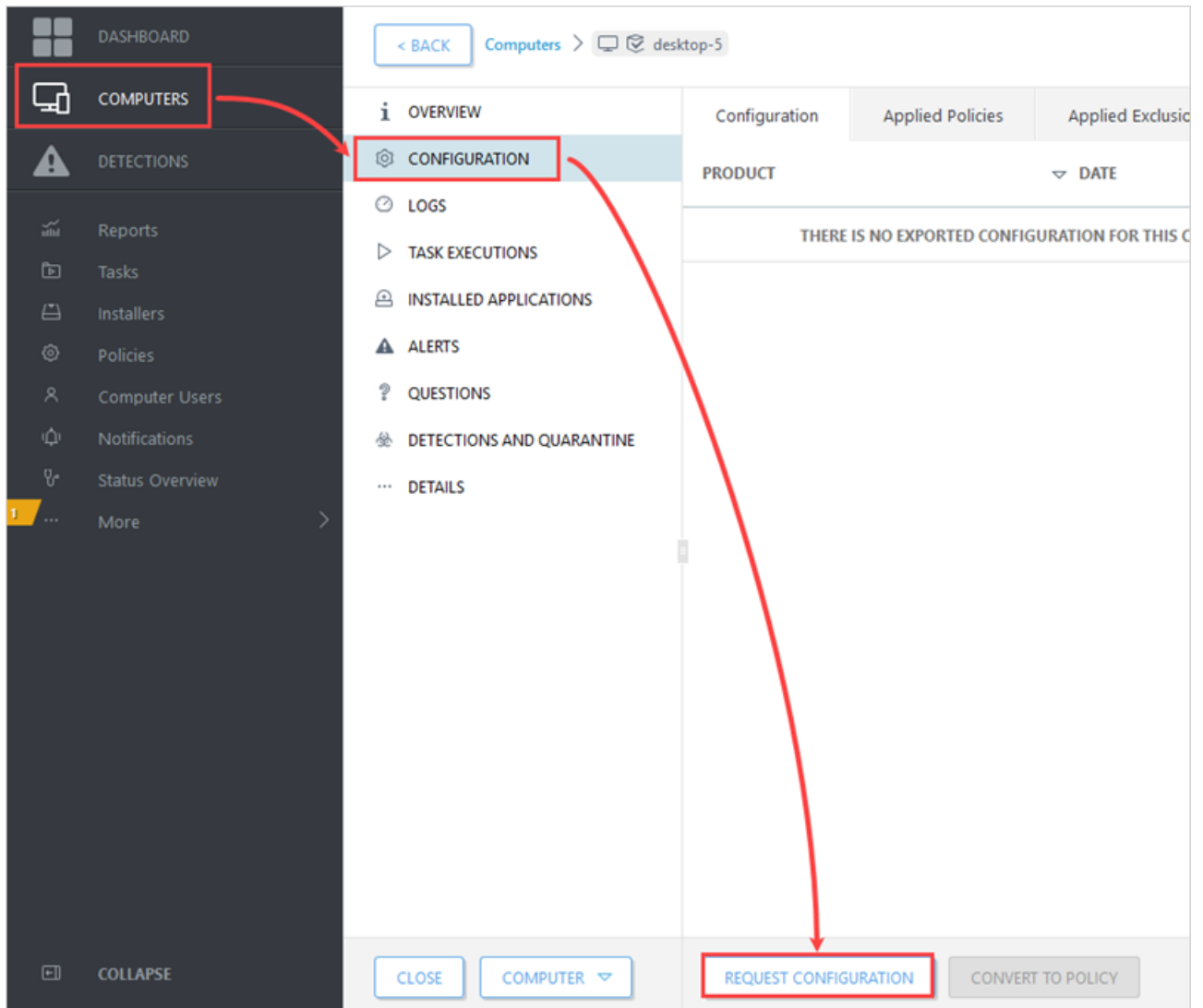
Product activation


1. Navigate to **Computers** menu.
2. Click the computer > **Show Details**.
3. Open the **Details** section > click **Product & Licenses** tab.
4. Look for the ESET LiveGuard Advanced license. If the license is not there, [activate the product](#).

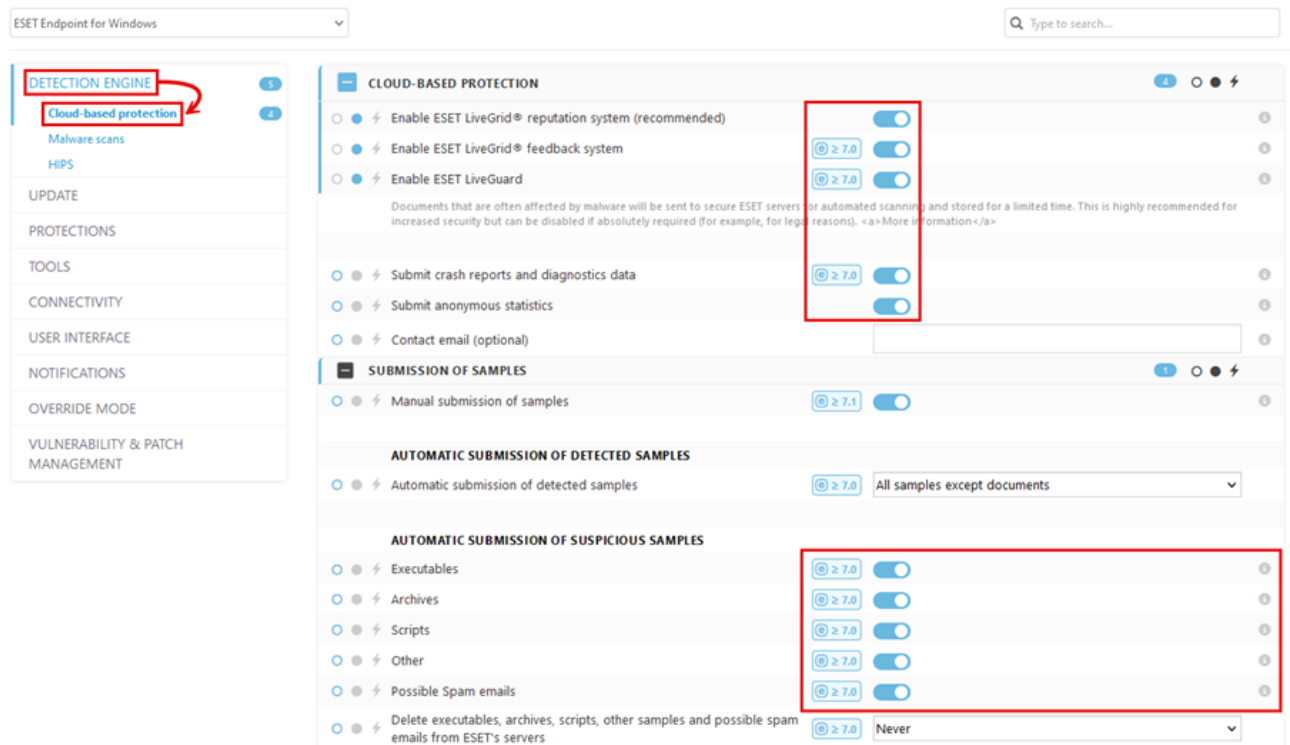


Product configuration

1. Click **Computers** > click the computer > **Show Details** > **Configuration** and click **Request configuration**.



2. When the configuration is received (click the reload () button to refresh your view) , click **Security product > Open Configuration**, click **Detection engine > Cloud-based protection**, and check if ESET LiveGrid® and ESET LiveGuard Advanced are enabled. For server products, click **Computer > Cloud-based protection**. If needed, [configure the policy](#) to enable ESET LiveGuard Advanced on your machine.



3.If there is no **Security product** on the **Configuration** tab after the configuration is received, install a [supported ESET security product](#) on the target machine.

Troubleshooting Apache HTTP Proxy

ESET Bridge is the preferred proxy solution for ESET products
 ESET distributes ESET Bridge with ESET PROTECT On-Prem 10.0 (and later) as a Proxy component replacing the former Apache HTTP Proxy. See the [comparison of ESET Bridge and Apache HTTP Proxy](#).

If the ESET LiveGuard Advanced is failing and Apache HTTP Proxy is used to cache the communication, you can enable diagnostic logging for the Apache HTTP Proxy to investigate the problem. You can provide the logs to ESET Technical Support for further analysis.

The diagnostic logging is a performance intensive process. Be aware of the possible loss of performance and use it only temporarily. Enable the logging only for a necessary time period.

Enable diagnostic logging for Apache HTTP Proxy

- 1.Stop the Apache HTTP Proxy service using the command: `sc stop ApacheHttpProxy`
- 2.Back up the configuration file `httpd.conf`. It is usually located at `C:\Program Files\Apache HTTP Proxy\conf`
- 3.Modify the configuration file as described below:
 - a)Un-comment (delete the `#` at the beginning):
`LoadModule log_config_module modules/mod_log_config.dll`
 - b)Add the line below in the beginning of the `<IfModule log_config_module>` section:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" \"%{cache-status}e\"" combined-cache
```

c)Comment the line (add # at the beginning):

```
CustomLog "logs/access.log" common
```

d)Change the line `CacheLockMaxAge 10` to `CacheLockMaxAge 15`

e)Change the line `ProxyTimeout 900` to `ProxyTimeout 1200`

f)In the section `<VirtualHost *:3128>`, below the line `ServerName r.edtd.eset.com`, add the lines:

```
<If "%{REQUEST_METHOD} == 'CONNECT'">
Require all denied
</If>
```

g)Change the line:

```
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=0n ttl=100 max=10
smax=10
```

to following:

```
ProxyPass / https://r.edtd.eset.com/ timeout=300 enablereuse=0n keepalive=0n
ttl=100 max=100 smax=10
```

h)Add the following lines to the end of the file:

```
ErrorLog "|C:/Program Files/Apache HTTP Proxy/bin/rotatelog.exe" -
n 10 "C:/Program Files/Apache HTTP Proxy/logs/error.log" 1M'
```

```
CustomLog "|C:/Program Files/Apache HTTP Proxy/bin/rotatelog.exe" -
n 10 "C:/Program Files/Apache HTTP Proxy/logs/access.log" 100M' combined-cache
```

4.Save the `httpd.conf` file and start the Apache HTTP Proxy service:

```
sc start ApacheHttpProxy
```

Next steps

Keep the logging on only for a necessary time period and copy the logs after it is disabled. Logs are located at:

```
C:/Program Files/Apache HTTP Proxy/logs/error.log
```

```
C:/Program Files/Apache HTTP Proxy/logs/access.log
```

To disable the diagnostic logging:

1.Stop the Apache HTTP Proxy service.

2.Revert the configuration file from the backup.

3.Start the Apache HTTP Proxy service.

Security for ESET LiveGuard Advanced

Introduction

The purpose of this document is to summarize the security practices and security controls applied within ESET LiveGuard Advanced. Security practices and controls are designed to protect customer information confidentiality, integrity, and availability. Note that security practices and controls may change.

Scope

The scope of this document is to summarize security practices and security controls for ESET LiveGuard Advanced infrastructure, organization, personnel, and operational processes. Security practices and controls include:

1. Information security policies
2. Organization of information security
3. Human resource security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications security
10. System acquisition, development, and maintenance
11. Supplier relationship
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

Security Concept

ESET, spol. s r.o. company is ISO 27001:2013 certified with integrated management system scope explicitly covering ESET LiveGuard Advanced services.

Therefore, the concept of information security uses the ISO 27001 framework to implement a layered defense security strategy when applying security controls on the layer of the network, operating systems, databases, applications, personnel, and operating processes. Applied security practices and security controls are intended to overlap and complement each other.

Security Practices and Controls

1. Information Security Policies

ESET uses information security policies to cover all aspects of the ISO 27001 standard, including information security governance and security controls and practices. Policies are reviewed annually and updated after significant change to ensure their continuing suitability, adequacy, and effectiveness.

ESET performs annual reviews of this policy and internal security checks to ensure consistency with this policy. Non-compliance with information security policies is subject to disciplinary actions for ESET employees or contractual penalties up to contract termination for suppliers.

2. Organization of Information Security

The organization of information security for ESET LiveGuard Advanced consists of multiple teams and individuals

involved in information security and IT, including:

- ESET executive management
- ESET internal security teams
- Business applications IT teams
- Other supporting teams

Information security responsibilities are allocated in line with information security policies in place. Internal processes are identified and assessed for any risk of unauthorized or unintentional modification or misuse of ESET assets. Risky or sensitive activities of internal processes adopt the segregation of duties principle to mitigate the risk.

The ESET legal team is responsible for contacts with government authorities including, Slovak regulators on cybersecurity and personal data protection. The ESET Internal Security team is responsible for contacting special interest groups like ISACA. The ESET Research lab team is responsible for communication with other security companies and the greater cybersecurity community.

Information security is accounted for in project management using the applied project management framework from conception to project completion.

Remote work and telecommuting are covered through the use of a policy implemented on mobile devices that include the use of strong cryptographic data protection on mobile devices while traveling through untrusted networks. Security controls on mobile devices are designed to work independently of ESET internal networks and internal systems.

3. Human Resource Security

ESET uses standard human resource practices, including policies designed to uphold information security. These practices cover the whole employee lifecycle, and they apply to all teams that access the ESET LiveGuard Advanced environment.

4. Asset Management

The ESET LiveGuard Advanced infrastructure is included in ESET asset inventories with strict ownership and rules applied according to asset type and sensitivity. ESET has an internal classification scheme defined. All ESET LiveGuard Advanced data and configurations are classified as confidential.

5. Access Control

ESET's Access control policy governs every access in ESET LiveGuard Advanced. Access control is set on the infrastructure, network services, operating system, database, and application level. Full user access management on the application level is autonomous.

ESET backend access is strictly limited to authorized individuals and roles. Standard ESET processes for user (de)registration, (de)provisioning, privilege management, and review of user access rights are used to manage ESET employee access to ESET LiveGuard Advanced infrastructure and networks.

Strong authentication is in place to protect access to all ESET LiveGuard Advanced data.

6. Cryptography

Strong cryptography (SSL) is in place to encrypt data in transit to protect ESET LiveGuard Advanced data.

7. Physical and Environmental Security

ESET LiveGuard Advanced is cloud-based. ESET relies on a private cloud and the Microsoft Azure cloud. The physical location of the private cloud data center is exclusively in the European Union (EU). Microsoft Azure is not limited to the EU territory; however, it is only used to store one-way hashes created from submitted files without including personal data. Strong cryptography is in place to protect customer data during transport.

8. Operations Security

The ESET LiveGuard Advanced service is operated via automated means based on strict operational procedures and configuration templates. All changes, including configuration changes and new package deployment, are approved and tested in a dedicated testing environment before deployment to production. Development, test, and production environments are segregated from each other. ESET LiveGuard Advanced data is located only in the production environment.

The ESET LiveGuard Advanced environment is supervised using operational monitoring to swiftly identify problems and provide sufficient capacity to all services on the network and host levels.

All configuration data is stored in our regularly backed-up repositories to allow for automated recovery of an environment's configuration. ESET LiveGuard Advanced data backups are stored both on-site and off-site.

Backups are encrypted and regularly tested for recoverability as a part of business continuity testing.

Auditing on systems is performed according to internal standards and guidelines. Logs and events from the infrastructure, operating system, database, application servers, and security controls are collected continuously. The logs are further processed by IT and internal security teams to identify operational and security anomalies and information security incidents.

ESET uses a general technical vulnerability management process to handle the occurrence of vulnerabilities in ESET infrastructure, including ESET LiveGuard Advanced and other ESET products. This process includes proactive vulnerability scanning and repeated penetration testing of infrastructure, products, and applications.

ESET states internal guidelines for the security of internal infrastructure, networks, operating systems, databases, application servers, and applications. These guidelines are checked via technical compliance monitoring and our internal information security audit program.

9. Communications Security

The ESET LiveGuard Advanced environment is segmented via native cloud segmentation with network access limited only to necessary services among network segments. The availability of network services is achieved via native cloud controls like availability zones, load-balancing, and redundancy. Dedicated load-balancing components are deployed to provide specific endpoints for ESET LiveGuard Advanced instance routing that enforce authorization of traffic and load-balancing. Network traffic is continuously monitored for operational and security anomalies. Potential attacks can be resolved by using native cloud controls or deployed security solutions. All network communication is encrypted via generally available techniques, including IPsec and TLS.

10. System Acquisition, Development, and Maintenance

Development of ESET LiveGuard Advanced systems is performed in accordance with the ESET secure software development policy. Internal security teams are included in the ESET LiveGuard Advanced development project from the initial phase and overlook all development and maintenance activities. The internal security team defines and checks the fulfillment of security requirements in various stages of software development. The security of all services, including newly developed ones, is tested continuously after release.

11. Supplier relationship

A relevant supplier relationship is conducted according to valid ESET guidelines, which cover whole relationship management and contractual requirements from the information security and privacy perspective. The quality and security of services provided by the critical service provider are assessed regularly.

Furthermore, ESET utilizes the principle of portability for ESET LiveGuard Advanced to avoid supplier lockout.

12. Information Security Incident Management

Information security incident management in ESET LiveGuard Advanced is performed similarly to other ESET infrastructures and relies on defined incident response procedures. Roles within incident response are defined and allocated across multiple teams, including IT, security, legal, human resources, public relations, and executive management. The incident response team for an incident is established based on incident triage by the internal security team. That team will provide further coordination of other teams handling the incident. The internal security team is also responsible for evidence collection and lessons learned. Incident occurrence and resolution are communicated to affected parties. ESET legal team is responsible for notifying regulatory bodies if needed according to the General Data Protection Regulation (GDPR) and Cybersecurity Act transposing Network and Information Security Directive (NIS).

13. Information Security Aspects of Business Continuity Management

Business continuity of the ESET LiveGuard Advanced service is coded in the robust architecture used to maximize the availability of the provided services. Complete restoration from off-site backup and configuration data is possible in the event of a catastrophic failure of all redundant nodes for ESET LiveGuard Advanced components or the ESET LiveGuard Advanced service. The restoration process is tested regularly.

14. Compliance

Compliance with the regulatory and contractual requirements of ESET LiveGuard Advanced is regularly assessed and reviewed similarly to other infrastructure and processes of ESET, and necessary steps are taken to provide compliance on a continuous basis. ESET is registered as a digital service provider for Cloud Computing digital service covering multiple ESET services, including ESET LiveGuard Advanced. Note that ESET compliance activities do not necessarily mean that the overall compliance requirements of customers are satisfied as such.

Fair Use policy

Fair Use policy description

The Fair Use policy states a limit for number of files uploaded from a customer. The file limit applies to selected ESET LiveGuard Advanced protection tiers. See the table below for more information.

The file limit is: **50 files / seat / month**. The number of files is counted for all computers together, so one machine can send more, if another is sending less.

For example:

- Customer with 500 seats can upload up to 25,000 samples per month.
- Customer with 10,000 seats can upload up to 500,000 samples per month.

ESET LiveGuard Advanced tiers' properties

See the table below for the list of available ESET LiveGuard Advanced tiers and their properties.

Tier name	Minimum seat count	Available for ESET PROTECT On-Prem	Available for ESET PROTECT	License allows user to create ESET PROTECT instance	Available in ESET MSP Administrator 2	File limit
ESET LiveGuard Advanced	5	✓	✓	✗	✓	No
ESET PROTECT Complete	5	✓	✓	✓	✓	Yes
ESET PROTECT Mail Plus		✓	✓	✓	✓	Yes
ESET PROTECT Advanced	5	✓	✓	✓	✓	Yes
ESET Dynamic Endpoint Protection	5	✓	✗	✗	✗	Yes
ESET Dynamic Endpoint Protection - Antivirus Level	5	✓	✗	✗	✗	Yes
ESET Targeted Attack Protection	250	✓	✗	✗	✗	Yes

Get no file limit

Contact your ESET partner to get more information about the protection tier with no file limit.

Check the number of sent files

Use the report in management console to get the [number of uploaded files](#).

Exclude certain files from sending

If you are overreaching file upload limit, review the files you are sending and consider excluding folders with an excessive number of submitted files, which you are sure are safe. Some applications or developer tools can generate an excessive number of files which are not a threat or need not be submitted. Decrease the number of uploaded files by [analyzing your upload statistics and adding exclusions](#).

Privacy Policy

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

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

Processing of Your Personal Data

Services provided by ESET implemented in our web-based product are provided under the Terms of Use ("Terms"), but some of them might require specific attention. We would like to provide You with more details on data processing connected with the provision of our products and services. We render various services described in the [Terms](#) and the product [documentation](#). To make it all work, We need to collect the following information:

- Samples such as files predefined and selected by End User are uploaded to ESET service for analysis and result is send back to you. Meta data are collected in your locally installed management console which needs to listed as supported.
- Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.
- Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it. Accidentally collected data may be included in malware itself (collected without your knowledge or approval) or as part of documents and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

Data Sharing and Confidentiality

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

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

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these

countries does not require any special authorization or agreement.

We rely on third-party services related to cloud computing provided by Microsoft as a cloud service provider.

Data Subject's Rights

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

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

Right to Object. Right to object the processing is applicable in case of processing based on the legitimate interest of ESET or third party. If We process your personal data to protect a legitimate interest, You as the data subject have the right to object to the legitimate interest named by us and the processing of your personal data at any time. Your objection is only effective for the future and does not affect the lawfulness of the data processed before the objection. If we process your personal data for direct marketing purposes, it is not necessary to give reasons for your objection. This also applies to profiling, insofar as it is connected with such direct marketing. In all other cases, we ask you to briefly inform us about your complaints against the legitimate interest of ESET to process your personal data.

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

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

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

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

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

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

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

ESET in the xls format.

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

We believe that every information we process is valuable and necessary for the purpose of our legitimate interest which is provision of services and products to our customers.

Contact Information

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

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

Terms of Use

Effective as of January 31, 2024.

These Terms of Use (hereinafter referred to as "Terms") constitute a special agreement between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (hereinafter referred to as "ESET" or "Provider") and you, a natural person or legal entity (hereinafter referred to as "You" or "User") who uses ESET LiveGuard Advanced online service owned, controlled and provided by ESET (hereinafter referred to as "ESET LiveGuard Advanced"). If you use ESET LiveGuard Advanced on behalf of an organization, then you agree to these Terms for that organization and guarantee that you have the authority to bind that organization to these Terms. In that case You and User will refer to that organization. Read these Terms carefully, they relate also to services provided by ESET through or in relation to ESET LiveGuard Advanced. The specific conditions for using individual services beyond these Terms are stated with each service, with their acceptance being part of the service activation process.

Security and Data Protection

ESET LiveGuard Advanced renders access to services provided by ESET. The user's full name, company name, country, valid email address, phone number, licensing data and statistics are required for registration and use of ESET LiveGuard Advanced and for the purpose of provision and maintenance of ESET LiveGuard Advanced services. You hereby agree to data being collected and transferred to Provider's servers or those of its partners, the purpose of which is to ensure functionality of and authorization to use the Software and protection of the Provider's rights. Following conclusion of these Terms, the Provider or its partners shall be entitled to transfer, process and store essential data identifying You for support purposes, and for the purpose of performance of these Terms. You are authorized to use ESET LiveGuard Advanced solely for the purposes and manner for which it is intended under these Terms, individual service terms and documentation.

In order to provide ESET LiveGuard Advanced, the submission of files is required (hereinafter referred to as "Data"). Data are provided by You to ESET solely for the purpose of provision of ESET LiveGuard Advanced service.

Data will be processed and stored in compliance with security policies and practices of ESET as well as in compliance with Privacy Policy.

Details about privacy, personal data protection and rights as a data subject can be found in [Privacy Policy](#).

Fair Use Policy

You are obliged to comply with technical limitations stipulated in documentation. You agree that You will only use the Account and its functions in a way which does not limit the possibilities of other Users to access these services. The Provider reserves the right to limit the scope of services provided to individual Users, to enable use of the services by the highest possible number of Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Account and deletion of data and information.

Details about Fair Use Policy can be found in [Fair Use Policy](#).

Software

ESET or its respective suppliers own or may exercise copyright to all software available on the Account websites (hereinafter referred to as "Software"). The Software can be used only in accordance with the End User License Agreement (hereinafter referred to as "EULA"). EULA is supplied together with the Software, or comprises part of it. Software supplied with the EULA cannot be installed without the User's consent to the EULA. Other information regarding licensing, copyright, documentation and trademarks are stipulated in the [Legal Information](#).

Restrictions

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

- (a) You may not use, modify, translate or reproduce the Account or transfer rights to use the Account or its components in any manner other than as provided for in these Terms.
- (b) You may not sell, sub-license, lease or rent or borrow the Account or use the Account for the provision of commercial services.
- (c) You may not reverse engineer, reverse compile or disassemble the Account or otherwise attempt to discover the source code of the Account, except to the extent that this restriction is expressly prohibited by law.
- (d) You agree that You will only use the Account in a manner that complies with all applicable laws in the jurisdiction in which You use the Account, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

Disclaimers

AS THE USER, YOU HEREBY ACKNOWLEDGE THAT THE ACCOUNT AS WELL AS SERVICES ARE 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 ACCOUNT OR SERVICES WILL NOT INFRINGE ANY THIRD PARTY'S PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THE PROVIDER OR ANY OTHER PARTY MAKE NO GUARANTEE THAT THE ACCOUNT OR SERVICES WILL MEET YOUR

REQUIREMENTS OR THAT THE OPERATION OF ACCOUNT OR SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF ACCOUNT AND SERVICES TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE RESULTS OBTAINED FROM IT.

These Terms create no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR CONTRACTORS 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 ACCOUNT, EVEN IF THE PROVIDER, ITS CONTRACTORS 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, CONTRACTORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE SERVICE OR ACCOUNT IN QUESTION.

Trade control compliance

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

- i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under these Terms are to be performed, or in which ESET or any of its Affiliates are incorporated or operate and
- ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under these Terms are to be performed, or in which ESET or any of its Affiliates are incorporated or operate (legal acts referred to in points i, and ii. above together as "Trade Control Laws").

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

- i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of section (a) of this Trade control compliance clause of these Terms; or
- ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under these Terms could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

(c) Nothing in these Terms is intended, and nothing should be interpreted or construed, to induce or require

either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

Governing Law and Language

These Terms shall be governed by and construed in accordance with Slovak law. The End User and the Provider agree that conflict provisions of the governing law and United Nations Convention on Contracts for the International Sale of Goods shall not apply. If You are a consumer with habitual residence in the EU, You are also afforded additional protection granted to You by mandatory provisions of law applicable in your country of residence.

You expressly agree that exclusive jurisdiction for any claim or dispute with the Provider or relating in any way to your use of the Software, Account or Services or arising from these Terms or Special Terms (if applicable) resides in District Court Bratislava I, Slovakia and You further agree and expressly consent to the exercise of the personal jurisdiction in the District Court Bratislava I in connection with any such dispute or claim. If You are a consumer and have a habitual residence in the EU, You may also bring a claim to enforce your consumer rights in the place of exclusive jurisdiction or in the EU country in which You live. Moreover, You may also use an online dispute resolution platform, which can be accessed here: <https://ec.europa.eu/consumers/odr/>. However, consider contacting us first before raising any claim officially.

General provisions

ESET reserves the right to revise these Terms and documentation or any portion thereof at any time by updating the relevant document to reflect changes to the law or changes to Account. You will be notified about any revision of these Terms by email or via your Account. If You disagree with the changes to these Terms, You may cancel your Account. Unless You cancel your Account after being notified about the changes, You are bound by any amendments or revisions of these Terms. You are encouraged to periodically visit this page to review the current Terms that apply to your use of Account.

Notices

All notices must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Annex no. 1

[ESET Management Agent EULA](#)

Annex no. 2

[Data Processing Agreement](#)

Annex no. 3

[Standard Contractual Clauses](#)

ESET Management Agent EULA

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE**

SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE [PRIVACY POLICY](#).

End User License Agreement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Functions with data collection and internet connection requirements. To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for functioning of the Software and for updating and upgrading the Software. The Provider shall be entitled to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on

https://go.eset.com/eol_business. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

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

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

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

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

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

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

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

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

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

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

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

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or

generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

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

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

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

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

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

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

13. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR

AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

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

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

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

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

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

19. **Trade control compliance.**

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

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

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on

transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

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

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

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

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

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

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

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

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

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

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior

representations, discussions, undertakings, communications or advertising relating to the Software.

ADDENDUM TO THE AGREEMENT

Communication and Managing Data. Additional provisions apply to the Communication and Managing Data as follows:

The Software contains a function, which enables transfer of information between Computer and remote management software. Information, which are subject to transfer contains management data such as hardware and software information of managed computer and managing instructions from the remote management software. Other content of data transferred from Computer shall be determined by the settings of software installed on Computer. The content of instructions from management software shall be determined by settings of remote management software.

EULAID: EULA-PRODUCT-AGENT; 3537.0

Data Processing Agreement

According to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (hereinafter referred to as the "GDPR"), Provider (hereinafter referred to as the "Processor") and You (hereinafter referred to as the "Controller") are entering into the data processing contractual relationship in order to define the terms and conditions for the processing of personal data, the manner of its protection, as well as to define other rights and obligations of both parties in the processing of personal data of data subjects on behalf of the Controller during the course of performing the subject matter of these Terms as the main contract.

1. Personal Data Processing. The services provided in compliance with these Terms include processing information relating to an identified or identifiable natural person listed in the [Privacy Policy](#) (hereinafter referred to as the "Personal Data").

2. Authorization. The Controller authorizes the Processor to process Personal Data, including the following instructions:

(i) Purpose of Processing shall mean the provision of services in compliance with these Terms. The Processor is only allowed to process Personal Data on behalf of the Controller regarding the provision of services requested by the Controller. All information collected for additional purposes is processed outside of Controller-Processor contractual relationship.

(ii) Processing Period shall mean the period from entering cooperation under these Terms to termination of services,

(iii) Scope and Categories of Personal Data. The Services are intended for the processing of general personal data only. However, the Controller is solely responsible for the personal data scope determination.

(iv) Data Subject shall mean a natural person as an authorized user of Controller's devices,

(v) Processing Activities shall mean every and all operation necessary for processing,

(vi) Documented Instructions shall mean instructions described in these Terms, its Annexes, Privacy Policy, and service documentation. The Controller shall be responsible for the legal admissibility of the processing of Personal Data by the Processor regarding the respectively applicable provisions of data protection law.

3. Obligations of Processor. The Processor shall be obliged to:

(i) process Personal Data only on the grounds of Documented instructions and for the purpose defined in Terms, its Annexes, Privacy Policy, and service documentation,

(ii) to instruct the persons authorized to process the Personal Data (hereinafter referred to as the "Authorized Persons") about their rights and duties according to the GDPR, on their liability in case of breach and ensure that Authorized Persons have committed themselves to confidentiality and follow the Documented instructions,

(iii) implement and follow the measures described in the Terms, its Annexes, Privacy Policy, and service documentation,

(iv) assist the Controller with responding to requests from Data Subjects related to their rights. The Processor shall not correct, delete or restrict the processing of Personal Data without the instruction from the Controller. All requests from Data Subject related to Personal Data processed on behalf of the Controller shall be forwarded to the Controller without delay.

(v) assist the Controller with notification of personal data breach to the supervisory authority and Data Subject. The Processor shall notify the Controller of any breach of Personal Data processing or personal data security immediately after the discovery. The Processor shall cooperate to a reasonable extent in an investigation and remediation of such breach, and take reasonable measures to limit further negative implications.

(vi) at the choice of the Controller to delete or return all the Personal Data to the Controller after the end of the Processing Period. The Controller undertakes to inform the Processor about its decision within ten (10) days upon the end of the Processing Period. This provision shall not affect the Processor's right to keep the Personal Data to the necessary extent for archiving purposes in the public interest, scientific research purposes, statistical purposes or for the purpose of establishment, exercise or defense of legal claims.

(vii) keep an up-to-date register of all the categories of Processing Activities carried out on behalf of the Controller,

(viii) make all information necessary to demonstrate compliance as part of the Terms, its Annexes, Privacy Policy, and service documentation available to the Controller. In case of the audit or control of the Personal Data processing from the Controller's side, the Controller shall be obliged to inform the Processor in writing at least thirty (30) days before the planned audit or control.

4. Engaging Another Processor. The Processor is entitled to engage another processor for carrying out specific processing activities, such as the provision of cloud storage and infrastructure for the service in compliance with the Terms, its Annexes, Privacy Policy, and service documentation. Currently, Microsoft provides cloud storage and infrastructure as part of Azure Cloud Service. In such a case, the Processor shall remain the only point of contact and the party responsible for compliance. The Processor hereby undertakes to inform the Controller about any addition or replacement of another processor for purposes of possibility to object such change.

5. Territory of Processing. The Processor ensures that processing takes place in the European Economic Area or a country designated as safe by the decision of the European Commission based on the decision of the Controller. Standard Contractual Clauses shall apply in case of transfers and processing located outside of the European Economic Area or a country designated as safe by the decision of the European Commission upon the request of the Controller.

6. Security. The Processor is ISO 27001:2013 certified and uses the ISO 27001 framework to implement a layered defense security strategy when applying security controls on the layer of the network, operating systems, databases, applications, personnel, and operating processes. Compliance with the regulatory and contractual requirements is regularly assessed and reviewed similarly to other infrastructure and operations of the Processor,

and necessary steps are taken to provide compliance on a continuous basis. The Processor has organized the data security using ISMS based on ISO 27001. The security documentation includes mainly policy documents for information security, physical security, security of equipment, incident management, handling of data leaks and security incidents, etc.

7. Technical and Organizational Measures. The Processor shall protect the Personal Data against casual and unlawful damage and destruction, casual loss, change, unauthorized access and disclosure. For this purpose, the Processor shall adopt adequate technical and organizational measures corresponding to the mode of processing and to the risk presented by processing for the rights of the Data Subjects in compliance with the requirements of the GDPR. A detailed description of the technical and organizational measures is stated in the [Security Policy](#).

8. Processor's Contact Information. All notifications, requests, demands and other communication concerning personal data protection shall be addressed to ESET, spol. s.r.o., attention of: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the

fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

- (i) of its identity and contact details;
- (ii) of the categories of personal data processed;
- (iii) of the right to obtain a copy of these Clauses;
- (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records

concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or

returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the

controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation,

the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the

processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lay down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under

Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured

or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

Clause 18 Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as defined in Terms.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts as defined in Terms.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Controller as defined in Data Processing Agreement
2. Processor as defined in Data Processing Agreement

(based on the flow of data)

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As defined in Data Processing Agreement.

Categories of personal data transferred: As defined in Data Processing Agreement and Privacy Policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As defined in Data Processing Agreement and Privacy Policy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: Automated.

Purpose(s) of the data transfer and further processing: Provision of service as defined in Terms, its Annexes, Privacy Policy, and service documentation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As defined in Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As defined in Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: As defined in Privacy Policy

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: As defined in Security Policy

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors: As defined in Data Processing Agreement

References:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into

Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.