ESET Inspect On-Prem

Administration guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

ESET Inspect On-Prem was developed by ESET, spol. s r.o.

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

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

REV. 4/12/2024

Get started with ESET Inspect Web Console

The following parts should help you get started with ESET Inspect:

Navigate the ESET Inspect Web Console

Look at what you can do with ESET Inspect Web Console.

Learning mode / Questions

Enable to allow the Rule learning mode automatically suggest exclusions. The exclusions will appear in Questions for you to review. If you decide to enable the Learning mode later, go to **More** > Settings > **Rule learning mode**.

Optimize your ESET Inspect

Before you begin fully using it, carry out recommended tweaks to optimize your ESET Inspect.

Dashboard

Gives you statistical information and a quick overview of security activities within your environment. Enables you to identify what may require your attention. The dashboard also includes the current status of ESET Inspect.

ESET Inspect Detections in ESET PROTECT On-Prem - Reporting and Management

The great advantage of ESET Inspect being interconnected with ESET PROTECT On-Prem is that it enables you to manage detections directly from ESET PROTECT On-Prem.

What's new

Version 2.0 brings you new features and improvements:

The following ESET business security solutions have been renamed:

Old name:	New name:	Renamed in version:
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	2.0
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0

Incident creator (Cloud only)

Incident creator

- Incidents are now the primary workflow for ESET Inspect and can be created automatically or using new incident rules.

Incident remediation

Automation for incident remediation

- Automatic and manual remediation of incidents.

Localization

New language support

- Product is now localized for Ukrainian, Simplified Chinese, and Japanese languages.

Log into the ESET Inspect Web Console

The ESET Inspect Web Console is accessible from any device with a compatible web browser. The ESET Inspect Web Console is a single-page application that communicates with the ESET Inspect Server via REST calls. The minimum supported screen resolution is 1280x768 pixels.

Log into the ESET Inspect Web Console using the user credentials defined in ESET PROTECT On-Prem account settings. Use the check box **Log into Domain** to log in as a domain user with access to the ESET PROTECT On-Prem. If required, you can enable two-factor authentication. Use the check box **Remember this device** to remember your trusted device when using two-factor authentication (available in the on-premises version only).

Create a new dedicated user account with appropriate permission settings. Do not use the Administrator user account you used during the installation process to log into ESET Inspect Web Console.

When you log into the ESET Inspect Web Console for the first time, initial notification windows will appear. The ESET Inspect / ESET Inspect Tour can be accessed again through **Help** > **ESET Inspect Product Tour**.

You can take advantage of the suggested options or dismiss the screens and configure them later:

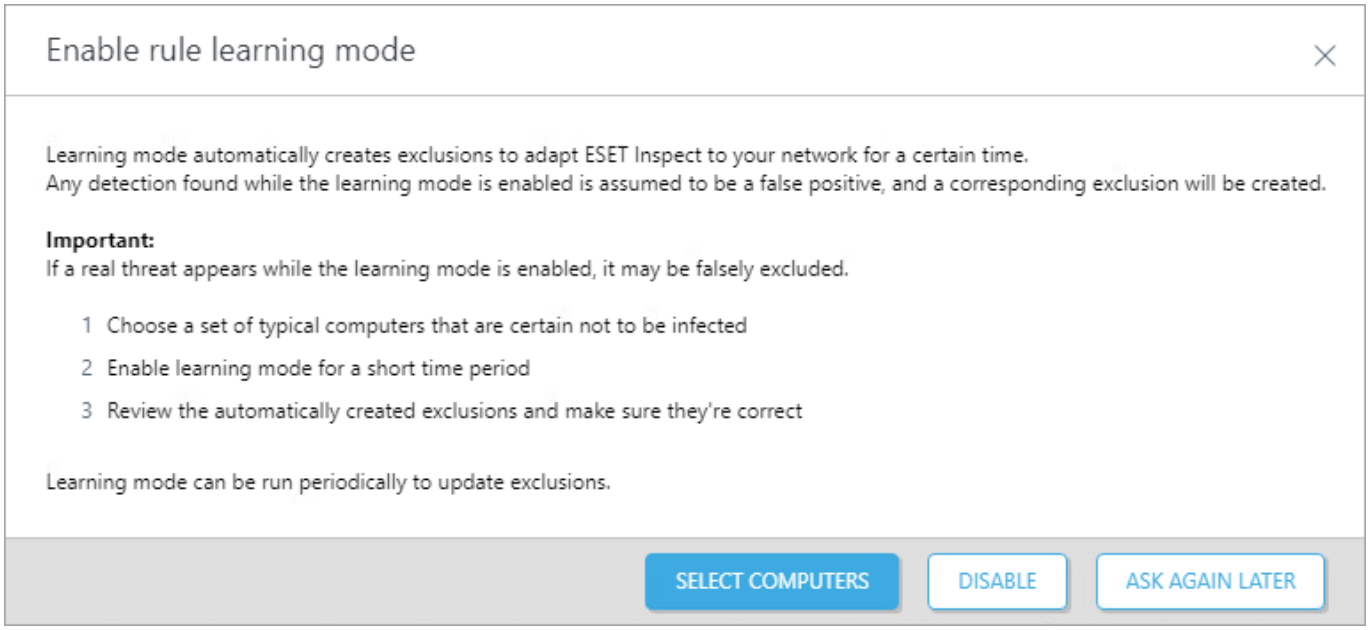
Rules sets

Select which new ESET Inspect detection rules will be available for the users. These are the rules sets chosen during the installation process. You can keep or change the selection for a more suitable option based on its environment. Click **Ask again later** if you plan to set up rules later.

Rule learning mode

Learning mode automatically creates exclusions to adapt ESET Inspect to your network on selected computers for a specified time (learning mode period). Any detection during the learning mode is assumed to be a false positive and will create a corresponding exclusion after the learning mode period ends. Before the end of the learning period, exclusions are not visible. Click the **Select Computers** and select groups/computers to enable learning mode for, and choose learning mode period (one to three weeks). New auto exclusions appear in the **More** > Exclusions tab after the learning mode concludes. To accept or reject a newly created exclusion, go to the Questions > tab.

Select computers you can ensure not to get infiltrated by malware or otherwise compromised during the learning mode period. Doing so prevents malware from being accidentally excluded from the detection by auto exclusion created during the learning process.



Troubleshooting ESET Inspect Web Console

The table below will give you some insight into the most common ESET Inspect Web Console login error messages and statuses:

Error message	Troubleshooting
Unexpected authorization error.	Contact Customer Care.
Login failed: Invalid username or password.	Make sure you typed your username and password correctly.
Login failed: Please contact technical support for further assistance.	Verify that database is running and there are no connection issues. If that is not the case, contact Customer Care.
Login failed: Cannot connect to ESET PROTECT On-Prem server host.	Verify that the ESET PROTECT On-Prem server is running and there are no connection issues.

Since the ESET Inspect Web Console uses a secure protocol (HTTPS), you may receive a warning in your web browser regarding an untrusted connection or a wrong security certificate (the exact wording of the message depends on the browser you use). The reason is that your browser wants you to verify the site's identity you are trying to access. If you are using Internet Explorer, click **Continue to this website**. With Firefox, click **Advanced** > **Add Exception** > **Confirm Security Exception**. In Google Chrome, click **Advanced** > **Proceed to** *xxxx* **(unsafe)**. The *xxxx* is the hostname or IP address of the ESET Inspect Web Console you tried to visit.

Navigate the ESET Inspect Web Console

Look at how to navigate your way through the ESET Inspect Web Console interface. You can soon become familiar with the navigational elements and tools of the ESET Inspect Web Console, which aim to be intuitive and easy to use while being interactive.

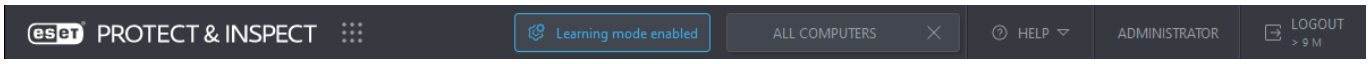
Here is an overview of most of the interface's elements:

Side bar

Use the navigation bar on the left side to switch between different parts of the ESET Inspect console:

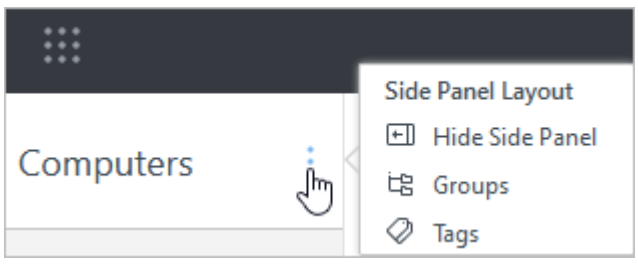
- Dashboard
- Computers
- Detections
- Search
- Incidents
- Executables
- Scripts
- Questions
- More

Toolbar at the top is available at all times:



- **ESET PROTECT On-Prem ecosystem / ESET Business ecosystem**—A quick access to the ESET PROTECT On-Prem Web Console and other useful links.
- **Learning mode / Questions**—Items that concern some of the ESET Inspect functionality (for example, automatic exclusions, database purge, LiveGrid®, etc.).
- **All Computers**—Acts as a quick filter. Click to view groups or computers and make your selection.
- **Help**—Links to Online Help for the current screen. ESET Inspect Product Tour shows main features of the product. License opens the web page with ESET Inspect End User License Agreement. The About page provides detailed information about the ESET Inspect version and links to legal documents.
- **User** (currently logged in)—Shows the username.
- **Logout**—Shows the time remaining until automatic logout. The timer is reset every time you interact with the ESET Inspect Web Console (click a button, tab, submenu or an item). Click Logout to leave the ESET Inspect Web Console, or to log in as a different user.

Side panel layout



Click the ⋮ icon next to the section name (Computers) to adjust the side panel layout using the context menu (available options may vary based on the current layout):

- Hide side panel
- Show side panel
- Groups
- Groups and Tags
- Tags

Preview panel

Click a Computer name or Detection to display the preview panel on the right side. While serving as a quick view, this panel contains vital information about the selected Computer or Detection.

Tags

You can use tags to further refine filtering of displayed items. Available tags are listed in the Tags side panel (click the ⋮ icon to adjust the view). To add tags to a computer, select a computer (or multiple computers) and use the action button **Tags** at the bottom.

Tables

Table view is present in many ESET Inspect Web Console sections. You can modify and rearrange the columns to your needs. To reorder, hover the mouse over the ✣ icon next to the column name and drag-and-drop to the desired position. To sort, click the column you want to sort by. This results in ascending (A–Z, 0–9) sorting, click again for descending (Z–A, 9–0). A small arrow before the column header indicates the sorting behavior. Click the gear ⚙ icon for table options, add or remove columns according to your needs. See the definition of each column.

Context menu / Action buttons

Right-click an item in the table for the context menu with all available actions. The buttons on the bottom of the page are unique for each section and function, and are described in detail in their respective chapters.

Filtering

Usually, there are too many results displayed in the table, and that is where filtering comes to the rescue. To narrow down the view when searching for specific items (computer, detection, incident, executable, script, etc.) use pre-defined filter(s) or add a custom one. To further refine the results, combine the filters. If you want to recall the filter combination in the future, click Presets button and save it.

Add filter and filter presets

To add filtering criteria, click **Add filter** and select item(s) from the list. Click **Presets** to manage or recall filter sets. See detailed information about filters.

Severity and Status (filter icons)

Click an icon to hide items. All icons are activated by default, meaning items with all seventies or statuses are displayed. Click an icon to deactivate (filter out) items with specific severity or status.

Threat	Detection(s) with threat severity present on this computer.
Warning	Detection(s) with warning severity present on this computer.
Information	Detection(s) with informational severity present on this computer.
OK	No detections were triggered on this computer, or all are resolved.
Unmonitored	ESET Inspect Connector is not installed on this computer. (ESET Inspect know about this computer because the ESET PROTECT On-Prem sent it from an Active Directory).

Priority (filter icons)

Click to show only items with specific priority. There are four types, no priority and priority I to III. All icons are deactivated by default, meaning the items with all priorities are displayed. Click the priority icon to activate the filter and show only items with selected priority.

OS type (filter icons)

Click an icon to hide items. Filter by Operating System platform to see or hide the executables for Windows, macOS or Linux.

Executable type (filter icons)

Click to see only EXE or DLL files, or both simultaneously, where:

EXE = executable file

DLL = library file

Blocked and Safe

You can filter executables to only see **Blocked** or **Safe** or both types of files.

Access group

You can filter items by access groups assigned to you.

Other control elements:

- Expand and **collapse** the navigation menu. Collapsing the panel provides more dashboard screen space. To

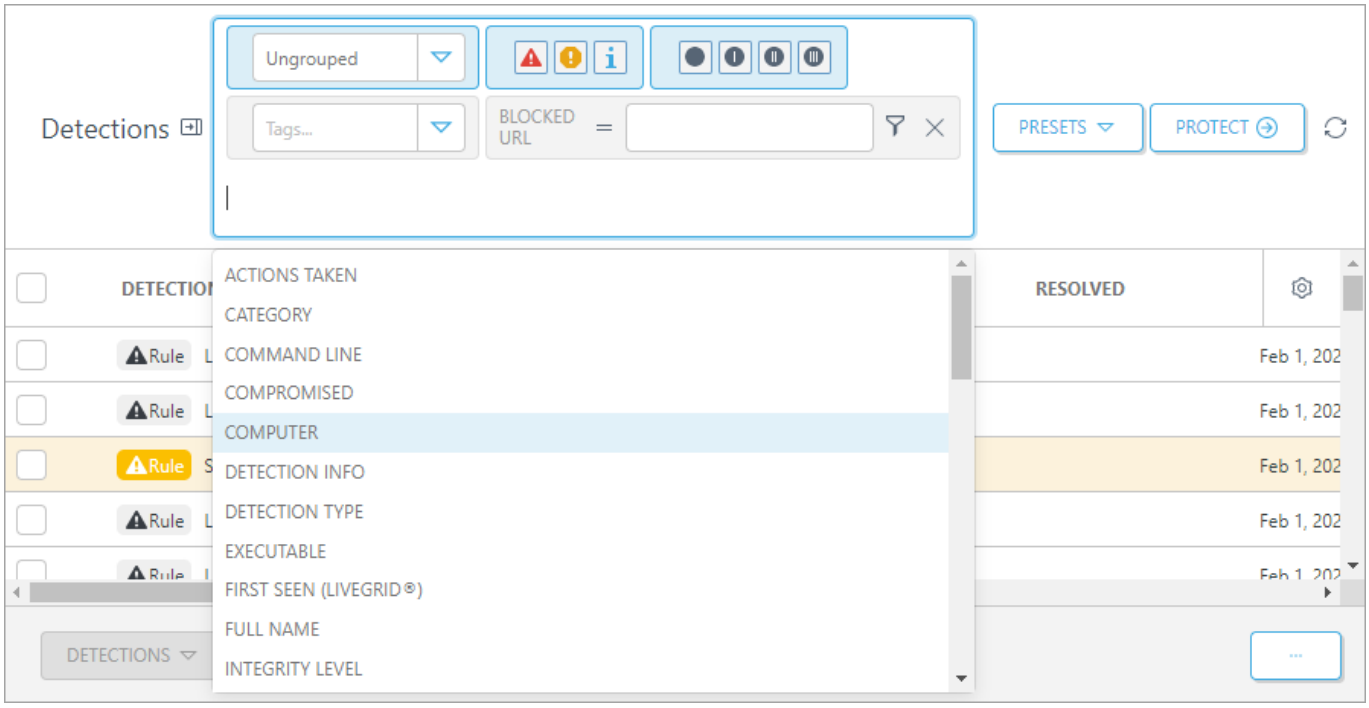
expand the navigation panel, click the icon.

- Click **refresh** icon to reload/refresh displayed information.
- If available, the **export** icon can be used to export the table grid to *CSV* format and use it in other applications to work with the list.
- Click the ESET Inspect logo to open the **Dashboard** screen.

Filters and layout customization

The ESET Inspect Web Console allows you to customize the layout of displayed items in the main sections (Computers, Detections, Incident, etc.) in several ways. To make searching for a specific detection easier, you can filter using multiple criteria. Filters can be saved to your user profile so that you can use them again in the future. Some tabs already have pre-defined filters. Active filters are highlighted in blue.

Click **Add filter** and select the filter type from the drop-down menu or type a string (repeat when combining criteria).



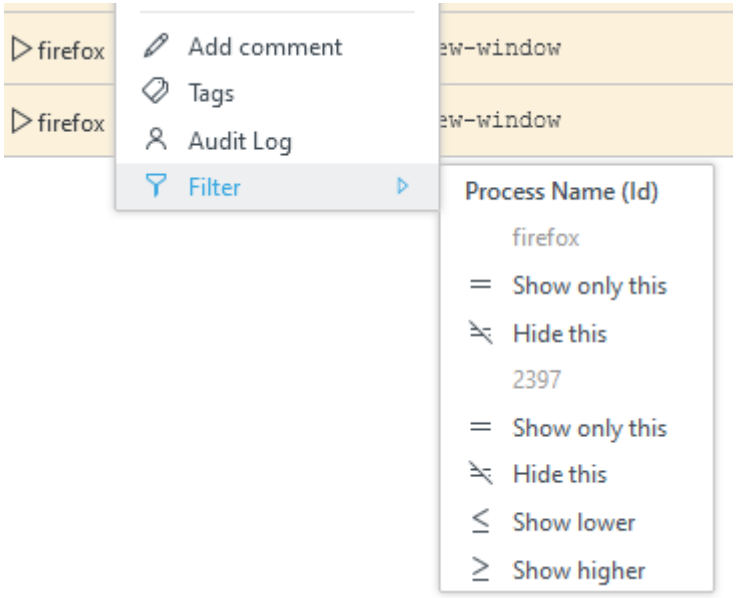
The definitions of the additional filters, follow List of filters.

Some of the filters have a funnel icon next to them with two or four options for further filtering:

- **Unknown**—The value in the filtered column is not available (probably not a known value at the time of occurrence).
- **Known**—The value is available.
- **None**—The value is an empty string.
- **Any**—The value is not empty. The negation of None filter.

Context menu quick Filter

Right-click an item and select **Filter** depending on the column where you activated the context menu:



Presets

Manage filter sets. These options are available:

- **Save filters**—This enables you to save the actual filter set. Select the check box **Include the visible columns and sorting** to save your selection, otherwise when loading saved filter without this option, you will get the default column setting.

- **Reset filters**—Resets active filter and return to default filter setting with default column setting.

- **Reset view**—Resets the active view without resetting the filter set.

- **Manage**—This option is available only when you have at least one set already saved. Select the check box next to the saved filter set that you want to delete and it is removed from the saved filters list. Deleting the filter does not delete the rule. You can delete the rule from the More tab.

- **Save Filters as Rule**—If available, enable you to save the filter as a rule. You can find it then in the list of rules under the Rules sub-tab of the More tab.

- **Default presets**—Commonly used presets, ready at your disposal.

If available, the export icon can be used to export the table grid to *CSV* format and use it in other applications to work with the list.

Refresh the table data by clicking the refresh icon.

List of filters

To make searching for a specific detection easier, you can filter using multiple criteria.

Click **Add filter** and select the filter type from the drop-down menu or type a string (repeat when combining criteria):

Dasboard

- **Time**—Filtering by the time of occurrence.

Computers

- **ESET Inspect Connector version**—Filtering by the version of ESET Inspect Connector deployed on the specific computer.
- **Alert count**—Filtering by the number of ESET PROTECT On-Prem related alerts (outdated endpoint, etc.).
- **AVG Received events / 24H**—Filtering by the average number of received events during 24 hours.
- **AVG Stored events / 24H**—Filtering by the average number of stored events during 24 hours. This number depends on the Settings, Data Retention and Data collection setting.
- **Description**—Filtering by the description of the computer, taken from ESET PROTECT On-Prem.
- **Endpoint version**—Filtering by the version of Endpoint installed on that Computer
- **FQDN**—Filtering by the fully qualified domain name, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS).
- **Group**—Filtering by the name of the group of computers a specific computer belongs to.
- **Information**—Filtering by the total count of unresolved informational detections on computer.
- **Information (Unique)**—Filtering by count of unique unresolved informational detections on computer.
- **Isolated from network**—Filtering by the computer isolated from network (only connections between ESET Security products are available).
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **Last Connected**—Filtering by the permanent connection created to listen on notification about blocked hashes, requests to download some file, kill the process, etc. Refresh interval is 90 seconds.
- **Last event**—Filtering by the timestamp of the last event sent to the server. So the time when this event occurred on the computer, not when it was sent to ESET Inspect Server.
- **Name**—Filtering by the name of the computer/executable/exclusion/task/blocked hash/report.
- **OS Name**—Filtering by the name of the operation system (Windows, macOS, Linux).
- **OS Platform**—Filtering by the operating system that is running on the specific computer (32-bit or 64-bit).
- **OS Version**—Filtering by the version of EEA or EES deployed on the specific computer.
- **Received events from today**—Filtering by the number of events that occurred on the specific computer since midnight
- **Resolved**—Filtering by the total count of resolved detections on a computer with no regard for the severity. In case of detections view or tab, it Filtering by the status of the detection, whether it was resolved or not.
- **Severity Score**—Filtering by the more precise definition of severity. 1–39 > Info  40–69 > Warning  70–100 > Threat  .
- **Stored events from today**—Filtering by the number of computer events since midnight
- **Threats**—Filtering by the total count of unresolved threat detections on the computer.
- **Threats (Unique)**—Filtering by the count of unique unresolved threat detections on computer.
- **Unresolved**—Filtering by the total count of unresolved detections on computer.
- **Unresolved (Unique)**—Filtering by the count of unique unresolved detections on computer.
- **Warnings**—Filtering by the total count of unresolved warning detections on computer.
- **Warnings (Unique)**—Filtering by the count of unique unresolved warning detections on computer.

Alerts

- **Details**—Filtering by the text in the details column field.
- **Occurred**—Filtering by the time of occurrence of the alert. Select earlier than or later than, and the desired time range.
- **Problem**—Filtering by the text of the problem of the alert.
- **Product**—Filtering by the text of the product of the alert.
- **Status**—Filtering by the name of the ESET PROTECT On-Prem alert status.
- **Subproduct**—Filtering by the text of the Subproduct of the alert.

Detections

- **Actions taken**—Filtering by the actions taken.
- **Blocked URL**—Filtering by the URL of the blocked detection if applicable.
- **Category**—Filtering by the category name that you can find among category tags in the Edit Rule section.
- **Command Line**—Filtering by the detections by the command line filename.
- **Compromised**—Filtering by the compromised computers.
- **Computer**—Filtering by the computer name. Select equal/unequal to include/exclude specific name. In Scripts tab, Filtering by the name of the computer, where the detection triggered.
- **Detection Info**—Filtering by the detection of specific information (rule name in case of rule detection, malware info in case of Antivirus detections, etc.).
- **Detection Type**—Filtering by the type of the detection (Firewall, HIPS, Filtered Websites, Antivirus, Rule, Blocked).
- **Executable**—Filtering by the name of the executable found in the detection details or in the Executable column. Choose equal/unequal to include/exclude specific name.
- **First Seen (LiveGrid®)**—Filtering when an executable was first seen on any computer connected to LiveGrid®.
- **Full name**—Filtering by the users full name, if available from Active Directory.
- **Integrity Level**—Filtering by the level of integrity.
- **Job Position**—Filtering by the users job position, if available from Active Directory.
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **MITRE ATT&CK™ TECHNIQUES**—Filtering by the ID of the MITRE ATT&CK™ TECHNIQUE.
- **Note**—Filtering by the Note.
- **Time Occured**—Filtering by the time of occurrence. Select earlier than or later than, and the desired time range.
- **Parent Process ID**—Filtering by the ID of the parent process that created this child process.
- **Parent Process Name**—Filtering by the name of the parent process that created this child process.
- **Parent Process SHA-1**—Filtering by the hash of the parent process.
- **Parent Process Signature Type**—Filtering by the parent process's file signature type (Trusted/Valid/None/Invalid/Unknown).
- **Parent Process Signer Name**—Filtering by the parent process's file signer name.
- **Popularity (LiveGrid®)**—Filtering by how many computers reported an executable to LiveGrid®.
- **Process ID**—Filtering by the Process ID found in detection details or in Process Name (ID) column. You can choose whether it is bigger and equal or smaller and equal to the one you are looking for, Known—if the ID is known, Unknown—if the ID is unknown (for example, executable blocked by hash).
- **Process Name**—Filtering by the Process Name that you can find in the details of the Detection or in the column Process Name (ID). You can choose whether it is equal or unequal to the one you are looking for.
- **Reputation (LiveGrid®)**—Filtering by the number from 1 to 9, indicating how safe the file is. 1–2 Red is malicious, 3–7 Yellow is suspicious, 8–9 Green is safe
- **Resolved**—Filtering by the total count of resolved detections on a computer with no regard for the severity. In case of detections view or tab, it Filtering by the status of the detection, whether it was resolved or not.
- **Rule Actions**—Filtering by the rule actions.
- **Rule Name**—Filtering by the name of the rule (Default or Customized).
- **Scanner**—Filtering by the type of Endpoint scanner that prevented the potential threat.
- **Severity Score**—Filtering by the more precise definition of severity. 1–39 > Info 40–69 > Warning 70–100 > Threat  .
- **SHA-1**—Filtering by the hash of the executable.
- **Signature Type**—Filtering by the signature type (Trusted/Valid/None/Invalid/Unknown).
- **Signer Name** —Filtering by the signer of the file.
- **Task Name**—Filtering by the task name from Tasks tab.
- **Threat Name**—Filtering by the threat name, that can be found in this list http://www.virusradar.com/en/threat_encyclopaedia
- **Time Triggered**—Filtering by the time of triggering. Select earlier than or later than or equal, and the desired time.
- **URI**—Filtering by the URI which caused this detection to trigger.
- **User Department**—Filtering by users department, if available from Active Directory.
- **User Description**—Filtering by users description, if available from Active Directory.
- **Username**—Filtering by the user account that was logged on the computer at the time of detection trigger.

Search

- **Author**—Name of the currently logged user at the creation or edition.
- **Progress**—Filtering by the progress of the task.
- **Results**—Filtering by the results is based on the object type.

Incidents

- **Assignee**—Filtering by the name of the Assignee.
- **Author**—Name of the currently logged user at the creation or edition.
- **Computers**—Filtering by the number of computers that the reporter created the report for.
- **Creation Time**—Filtering by the time of creation of the report.
- **Description**—Filtering by the description of the computer, taken from ESET PROTECT On-Prem. In Incidents Filtering by the description provided by the reporter.
- **Detections**—Filtering by the number of detections triggered by this task. In Incidents Filtering by the number of detections that the report contains.
- **Executables**—Filtering by the number of executables that the report contains.
- **Last Update**—Filtering by the time of the last update of the report.
- **Name**—Filtering by the name of the computer/executable/exclusion/task/blocked hash/report.
- **Processes**—Filtering by the number of processes that the report contains.

Executables

• **Blocked**—Filtering by whether the executable's hash was blocked or not.
• **Company Name**—Filtering by the company that produced the executable (for example, "Microsoft Corporation" or "Standard Micro-systems Corporation, Inc.).
• **DNS events**—Filtering by the total number of DNS events, that the specific executable triggered.
• **Events / 24h**—Filtering by the total amount of events within 24 hours.
• **Executable Drops**—Filtering by the number of dropped executables made by this executable.
• **Executed on Computers**—Filtering by the number of computers on which the file was executed.
• **Executions**—Filtering by how many times this EXE file was executed on all computers.
• **File Description**—Filtering by the full description of the file, for example, "Keyboard Driver for AT-Style Keyboards".
• **File Modifications**—Filtering by how many files were modified (written to, deleted, renamed).
• **File Version**—Filtering by the version number of the file for example, "3.10" or "5.00.RC2".
• **First Executed**—Filtering when was executable first executed on this computer.
• **First Seen**—Filtering when an executable was first seen on any computer.
• **First Seen (LiveGrid®)**—Filtering when an executable was first seen on any computer connected to LiveGrid®.
• **HTTP Events**—Filtering by the total number of HTTP events, that the specific executable triggered.
• **Information**—Filtering by the total count of unresolved informational detections on computer.
• **Information (Unique)**—Filtering by count of unique unresolved informational detections on computer.
• **Internal Name**—Filtering by the internal name of the file, if one exists, for example, an executable name if the file is a dynamic-link library. If the file has no internal name, this string is the original filename, without extension.
• **Last Change Date**—Filtering by the date, when the object was changed the last time.
• **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
• **Last Changed By**—Filtering by the user which was the last one to change the object.
• **Last Executed**—Filtering by when was executable executed last time on any computer.
• **Last Processed on (ESET LiveGuard)**—Filtering by when was executable processed last time in ESET LiveGuard.
• **Name**—Filtering by the name of the computer/executable/exclusion/task/blocked hash/report.
• **Nearmiss Report**—Filtering if the detection is triggered due to malware, but we cannot hundred percent guarantee it is malware.
• **Network Connections**—Filtering by the number of network connections this file makes.
• **Note**—Filtering by the Note.
• **Original File Name**—Filtering by the original name of the file, not including the path. This information enables an application to determine whether a user has renamed a file. The format of the name depends on the file system for which the file was created.
• **Packer Name**—Filtering by the name of packer if an executable is packed.
• **Popularity (LiveGrid®)**—Filtering by how many computers reported an executable to LiveGrid®.
• **Product Name**—Filtering by the name of the product with which the file is distributed.
• **Product Version**—Filtering by the version of the product with which the file is distributed, for example, "3.10" or "5.00.RC2".
• **Registry Modifications**—Filtering by how many registry entries were modified.
• **Reputation (LiveGrid®)**—Filtering by the number from 1 to 9, indicating how safe the file is. 1–2 Red is malicious, 3–7 Yellow is suspicious, 8–9 Green is safe
• **Resolved**—Filtering whether the detection is marked as Resolved . This status can be changed via buttons at the bottom of the window.
• **Safe**—Filtering if the executable was marked as safe.
• **Seen on Computers**—Filtering by the number of computers the file was discovered.
• **Sent Bytes**—Filtering by the total number of bytes sent by this file, from all computers, all processes.
• **SFX Name**—Filtering by the self-extracting archive type if an executable is packed.
• **SHA-1**—Filtering by the hash of the executable.
• **Signature CN #1**—For macOS only. Same as product name column for windows.
• **Signature CN #2**—For macOS only. Same as file version column for windows.
• **Signature CN #3**—For macOS only. Same as product version column for windows.
• **Signature CN #4**—For macOS only. Same as internal name column for windows.
• **Signature CN #5**—For macOS only. Same as original filename column for windows.
• **Signature Id**—For macOS only. Same as company name column for windows.
• **Signature Type**—Filtering by the signature type (Trusted/Valid/None/Invalid/Unknown).
• **Signer Name** —Filtering by the signer of the file.
• **State (ESET LiveGuard)**—Filtering by the executable's present station in the analysis workflow.
• **Status (ESET LiveGuard)**—Filtering by the result of the behavioral analysis or the absence of a result (Unknown/Clean/Suspicious/Highly suspicious/Malicious).
• **Threats**—Filtering by the total count of unresolved threat detections on the computer.
• **Threats (Unique)**—Filtering by the count of unique unresolved threat detections on computer.
• **Unresolved**—Filtering by the total count of unresolved detections on computer.
• **Unresolved (Unique)**—Filtering by the count of unique unresolved detections on computer.
• **User Id**—For macOS only. Same as the file description column for windows.
• **Warnings**—Filtering by the total count of unresolved warning detections on computer.
• **Warnings (Unique)**—Filtering by the count of unique unresolved warning detections on computer.
• **Whitelist Type**—Filtering by the information if an executable is whitelisted.

Scripts

- **Command Line**—Filtering by the detections by the command line filename.
- **Command Line Length**—Filtering by the length of the command line command (Count of characters).
- **Computer**—Filtering by the computer name. Select equal/unequal to include/exclude specific name. In Scripts tab, Filtering by the name of the computer, where the detection triggered.
- **Ended**—Filtering by the time, when the process was terminated, caused by this process.
- **First Child Module Name**—Filtering by the child process name.
- **First HTTP Request**—Filtering by the source HTTP address, if the script access the network.
- **Full name**—Filtering by the users full name, if available from Active Directory.
- **Integrity Level**—Filtering by the level of integrity.
- **Job Position**—Filtering by the users job position, if available from Active Directory.
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **Note**—Filtering by the Note.
- **Parent Module Name**—Filtering by the parent process name.
- **Process ID**—Filtering by the Process ID found in detection details or in Process Name (ID) column. You can choose whether it is bigger and equal or smaller and equal to the one you are looking for, Known—if the ID is known, Unknown—if the ID is unknown (for example, executable blocked by hash).
- **Process Name**—Filtering by the Process Name that you can find in the details of the Detection or in the column Process Name (ID). You can choose whether it is equal or unequal to the one you are looking for.
- **Resolved Detections**—Filtering by the total count of resolved detections on the specific computer with no regard to severity.
- **Safe**—Filtering by the safe state.
- **Started**—Filter by the time, when the process was executed, caused by this process
- **Unresolved Detections (Unique)**—Filtering by the total count of unique unresolved detections on the specific computer.
- **User Department**—Filtering by users department, if available from Active Directory.
- **User Description**—Filtering by users description, if available from Active Directory.
- **Username**—Filtering by the user account that was logged on the computer at the time of detection trigger.

Questions

- **Status**—Filtering by the status of the questions (Active/Accepted/Rejected/Resolved/Don't show)
- **Timestamp**—Set the period (date and time).
- **Time**—Filtering by the time of occurrence.

Rules

- **Author**—Name of the currently logged user at the creation or edition.
- **Category**—Filtering by the category name that you can find among category tags in the Edit Rule section.
- **Enabled**—Filtering by the rule/exclusion. Enabled or disabled.
- **Hit Count**—Filtering by the count of detections that were excluded by this exclusion.
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **MITRE ATT&CK™ TECHNIQUES**—Filtering by the rule contains an ID of the MITRE ATT&CK™ TECHNIQUE.
- **OS Name**—Filtering by the name of the operation system (Windows, macOS, Linux).
- **Rule Actions**—Filtering by the rule actions.
- **Rule Body**—Filtering by the rule body.
- **Rule Name**—Filtering by the name of the rule (Default or Customized).
- **Severity Score**—Filtering by the more precise definition of severity. 1–39 > Info 40–69 > Warning 70–100 > Threat .
- **Valid**—Filtering by the rule with the wrong syntax, it gets an invalid tag.

Exclusions

- **Author**—Name of the currently logged user at the creation or edition.
- **Enabled**—Filtering by the rule/exclusion. Enabled or disabled.
- **Hit Count**—Filtering by the count of detections that were excluded by this exclusion.
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **Name**—Filtering by the name of the computer/executable/exclusion/task/blocked hash/report.
- **Note**—Filtering by the Note.
- **Rule Name**—Filtering by the name of the rule (Default or Customized).

Blocked Hashes

- **Cleaned**—Filtering by the file was clean, when the hash was added.
- **File Description**—Filtering by the full description of the file, for example, "Keyboard Driver for AT-Style Keyboards".
- **First Seen (LiveGrid®)**—Filtering when an executable was first seen on any computer connected to LiveGrid®.
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **Name**—Filtering by the name of the computer/executable/exclusion/task/blocked hash/report.
- **Popularity (LiveGrid®)**—Filtering by how many computers reported an executable to LiveGrid®.
- **Reputation (LiveGrid®)**—Filtering by the number from 1 to 9, indicating how safe the file is. 1–2 Red is malicious, 3–7 Yellow is suspicious, 8–9 Green is safe
- **SHA-1**—Filtering by the hash of the executable.
- **Signature Type**—Filtering by the signature type (Trusted/Valid/None/Invalid/Unknown).
- **Signer Name** —Filtering by the signer of the file.

Tasks

- **Author**—Name of the currently logged user at the creation or edition.
- **Created**—Filtering by the time when was the task created.
- **Detections**—Filtering by the number of detections triggered by this task.
- **From Date**—Filtering by the date when the task started.
- **Group**—Filtering by the name of the group of computers a specific computer belongs to.
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **Name**—Filtering by the name of the computer/executable/exclusion/task/blocked hash/report.
- **Note**—Filtering by the Note.
- **Progress**—Filtering by the progress of the started task.
- **Rule Name**—Filtering by the name of the rule (Default or Customized).
- **To date**—Filtering by the date when the task ended.

Event Filters

- **Author**—Name of the currently logged user at the creation or edition.
- **Enabled**—Filtering by the rule/exclusion. Enabled or disabled.
- **Filter Name**—Filtering by the name of the event filter.
- **Hit Count**—Filtering by the count of detections that were excluded by this exclusion.
- **Last Change Date**—Filtering by the date, when the object was changed the last time.
- **Last Change Type**—Filtering by the last change of the object (for example, marked as resolved, change of the priority).
- **Last Changed By**—Filtering by the user which was the last one to change the object.
- **OS Name**—Filtering by the name of the operation system (Windows, macOS, Linux).
- **Rule Actions**—Filtering by the rule actions.
- **Valid**—Filtering by the rule with the wrong syntax, it gets an invalid tag.

Audit Log

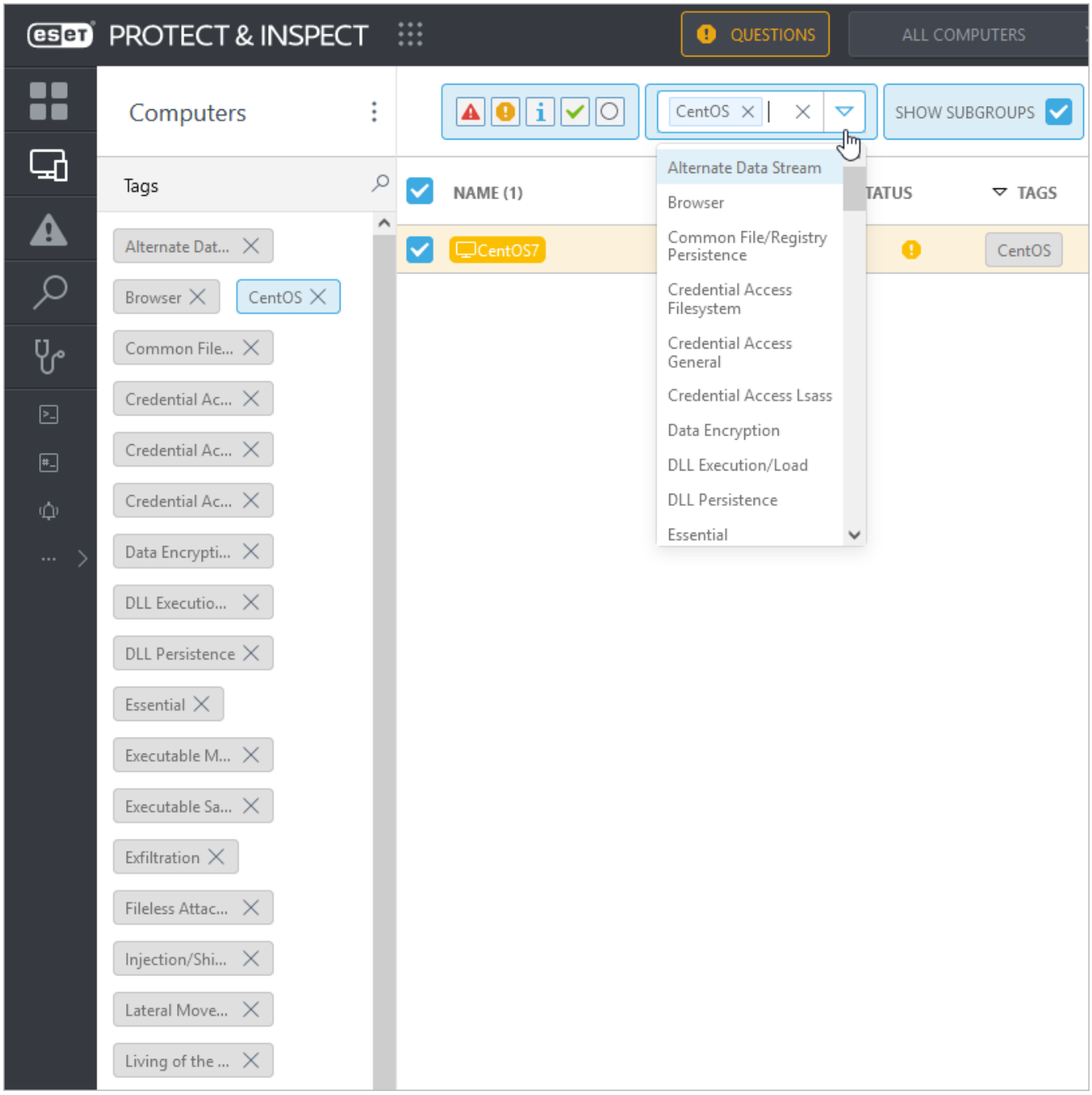
- **Action**—Select one of the available actions.
- **Section**—Select one of the available sections.
- **Timestamp**—Set the period (date and time).
- **User**—Select the user who performed changes.

Tags and object tagging

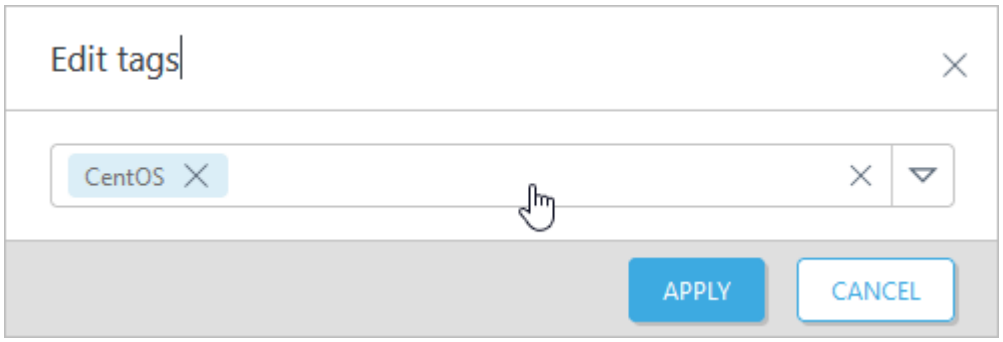
Tagging is a powerful feature that can be used for classification and serve mainly as an additional form of filtering. ESET Inspect enables you to tag most of the objects (computers, detections, incidents, executables, scripts, rules, exclusions, blocked hashes, tasks, and event filters). You can think of tags as virtual sticky notes or bookmarks. Utilizing the tags gives you the advantage to quickly sort, filter or find objects you need. Then you can take action or further process those objects.

To manage tags, click the expander icon to display the list of existing tags. In **Computers** view, click the ⋮ icon to access the tags panel. You can use the magnifying glass to search for a specific tag (if the tag name is too long, or you cannot find it).

Use the **Tags** selector (arrow icon) and choose a tag(s) to activate the filter on the listed objects. The results now contain only objects with selected tags (highlighted in blue).



Create a new tag by typing a name, then click **Apply**.

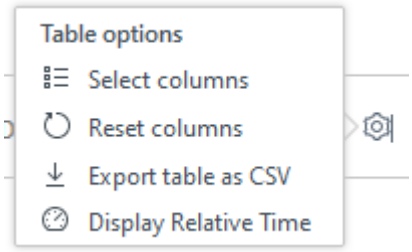


You can assign or unassign tag(s) to one or more objects. Also, you can assign multiple tags to a single object. Remove a tag by clicking the X, then click **Apply**.

Tags are synchronized between ESET Inspect and ESET PROTECT On-Prem.

Tables

Click the gear icon to manage table options. Click **Select columns** and choose from available columns. Alternatively, **Enter quick search pattern** to search for the column by typing its name or a partial string.



Display Absolute/Relative Time—Absolute time will show the time in format DD/MM/YYYY HH:MM:SS. Relative time will show the time in the format minutes/hours/months concerning present time (like 15 minutes ago or 6 days ago).

The export table as CSV icon can export the table grid to *CSV* format and use it in other applications to work with the list.

Click **Reset columns** to revert default columns selection.

The order of the columns can be organized by clicking the name of the column:

- Default (No icon)
- Ascending
- Descending

You can shuffle columns around. Hover the mouse over the icon next to the column name and drag-and-drop to the desired position.

Adjust the column width by the ↔ icon.

Emoji

ESET Inspect supports Unicode emoji. You can use it in many places, basically whenever typing text. Be it comments, tags, names, blocked hashes, script names, rule names, file names, executables, and so on. Use it even for filtering or when searching.

Refer to the emoji lists:

- https://www.unicode.org/emoji/charts/emoji-list.html
- https://apps.timwhitlock.info/emoji/tables/unicode

Most modern desktop or tablet operating systems support emoji, and you can use them readily. Earlier operating systems may require a different approach. For example:

- Windows 7—Open Internet Explorer 11, visit https://classic.getemoji.com and copy/paste emoji symbols.

- Windows 8—Use Touch Keyboard with emoji symbols, right-click Taskbar > Toolbars > Touch Keyboard.
- Windows 10—Press the Windows logo key + . (period) on your keyboard to access emoji (or use Touch Keyboard as with Windows 8).

Windows Server operating systems do not support emoji.

Dashboard

Provides an overview of your enterprise IT environment state concerning security. The Dashboard includes essential information in each tab (Detections, Executables, Computers, More, Server status and Events load).

The Detections is the main screen of the Dashboard that you see every time you click Dashboard. It displays statistical information about the top 10 unresolved detections categorized by their severity, as well as the timeline of detections. The Detections screen indicates any potential or existing attacks, what kind of detections were triggered, or if false positives flood needs to be taken care of by optimizing the detections.

The statistics screens are interactive. Click the pie charts, graphs and other items to see further information. The dashboard includes your ESET Inspect current performance under the Server status and Events load tabs. All of these dashboard screens aim to help you identify what may require your attention.

Use a **Time** filter within the statistics tabs. Specify the period (day, week, month) to filter statistical information.

Use the Dashboard tabs to switch between the screens:

Incidents

Displays the incidents statistics:

- Incidents by severity
- Incidents by status
- ESET Inspect On-Prem incidents (incidents per day)
- Incidents by author

Click the slice of a pie chart you are interested in, and the Incidents table opens with relevant items filtered for you to review.

Detections

Displays detection statistics:

- Top 10 Unresolved Threat and Warning Detections
- Top 10 Unresolved Informational Detections
- Threat and Warning Detections
- Informational Detections

Click the slice of a pie chart (or the threat name of listed detections) you are interested in, and the Detections table opens with relevant items filtered for you to review. If needed, you can further refine the list of items by using additional filters (for example: occurred time). Click the detections per day graph to get a list of detections occurred that day.

Executables

The Executables tab shows a hit-map of all discovered executables within your environment. The executables are displayed graphically as an intersection of Network & LiveGrid® popularity showing the file count. This view should help you distinguish safe or well-known executables from unique ones. The unique executables may indicate a targeted attack. Problematic Executables lists executables with suspicious behavior grouped by the number of detections (total and unique).

- **Executables popularity**—The bubbles contain file count that meet the following two conditions:
- **LiveGrid® Popularity**—How many computers reported an executable to the LiveGrid®. Red is evaluated by the LiveGrid® as malicious, Yellow as suspicious, Green as safe.
- **Network Popularity**—The number of computers which have the module in the enterprise.

Click a bubble for a list of executables filtered by popularity:

- **Executable status**—Shows the count of unresolved detections and executable status. Click the pie graph, or the status type (OK, Warning, Info, Threat), for a list of executables filtered by the status.
- **Problematic Executables**—Lists problematic executables detected. Click an executable to see its details.

Computers

Identifies computers with a potential risk, indicating that further investigation of suspicious behavior may be required.

- **Detections on Computers**—Graphical intersection of Resolved Detections and Unresolved Detections on all computers. The bubble shows computer count and of Resolved/Unresolved Detections, which is within a certain range (for example [8,16)/[2,4) means Unresolved Detections count from 8 to 16 excluded. Resolved Detections count from 2 to 4 excluded). Click the bubble, and you will be redirected to the Computers tab.
- **Computer statuses**—Shows a pie graph of computers sorted by statuses. By clicking the part of the pie graph, you are redirected to the specific Computers list with the selected filter.
- **Problematic Computers**—Provides a list of problematic computers. Click the name of a problematic computer to be redirected to the Computer details section.

More

Information and functionality available in this section. After clicking on the part of the pie graph, the Detections list with specified Severity filter is listed.

- **Unresolved Detections severity**—Threat , Warning , Informational.
- **Unresolved Detections priority**—No Priority, Priority I to III.
- **Resolved/unresolved detections**—Total number of Resolved/Unresolved detections.

- **Last connection**—Shows how many Computers were connected to ESET Inspect Server recently (Today, Last Day, More than 2 days).

- **Received Events From Today**—Average value of events on all monitored computers.

- **ESET Inspect Connector version**—Shows the versions of ESET Inspect Connector installed on all computers.

Server status (available in the the on-premises version only)

Displays information regarding the Server statistics an overview of the ESET Inspect Server usage. There is also a server status that indicates whether the ESET Inspect environment is in normal health and all system services are running correctly, without excessive use of system resources.

- CPU Time

- Memory Usage

- Networking

- Events Processed per Second

- Event Packet Queue Length

- Hover over a graph to see more information

If the SQL database is installed on a different machine than ESET Inspect Server, the information regarding CPU Time and Memory Usage of SQL is not shown.

Events load (available in the on-premises version only)

Shows information about the database size and amount of low-level events reported to and processed by ESET Inspect. A low-level event is something a process does. So, write a file, do a DNS lookup, create a registry entry, etc. ESET Inspect analysis low-level events to find suspicious activities and report detections. Low-level events account for most of the database size, so use Event Filters to selectively not store some events and reduce the disk usage. The charts on this page helps find executables that report most of the events and possibly filter them out. Information and functionality available in this section:

- **Events processed and stored per computer**—Shows an average number of low-level events received from a computer and stored in the database. The difference between received and stored values are caused by using Event Filters or configuring ESET Inspect not to store all data. Failed purge can indicate a problem with the disk space running low on the database machine, as this process also need free space to be successfully finished.

- **Database size**—Shows estimated database size (calculations are based on the current retention data settings, number of clients and events sent per day) and current size (real size calculated as size of the ESET Inspect database, temporary database, inndb logs files, binary logs if present). Estimated database size can be smaller than current if you changed settings to store less data or purge more data. After the purge removes old data, database size should reach estimated value.

- **Events per executable instance**—Shows the number of events executed per executable instance on a single computer.

- **Events per executable**—Shows the number of events executed by the executable on all computers within the network.

• **Top executable instances**—Shows the list of executable instances, sorted by the highest events count on a specific computer.

• **Top executables**—Shows the list of executables, sorted by the highest events count within the whole network.

The option to filter events is available through the Executables tab.

Optimize your ESET Inspect

To get the best of your ESET Inspect, we recommend you carry out the following tweaks to optimize ESET Inspect before you begin fully using it. It gives you two advantages, increases overall performance, and makes it easier for you to use ESET Inspect when managing detections and responding to them to mitigate the threats.

Tweak	Description
System Requirements	Ensure your ESET Inspect Server is up to specification and meets (or exceeds) software and hardware requirements. Having a dedicated machine with ample storage space to run the database system may further improve performance. This is not mandatory, you can run the ESET Inspect in a single server environment.
MySQL	If you have the option, **choose MySQL** to run the ESET Inspect Database. It currently outperforms the Microsoft SQL Server when running the ESET Inspect Database.
Number of threads	This applies only when your ESET Inspect Database is running on a different server than ESET Inspect Server. If your ESET Inspect Server and ESET Inspect Database runs on the same machine, this is configured automatically, you can skip this step. Set the number of cores to increase the performance, making your ESET Inspect Server more efficient. Navigate to **More** > Settings > **Database performance** (available in the on-premises version only) and specify the **Number of threads writing to database** according to this formula: 1.5x the number of physical cores of your server running the ESET Inspect Database
Performance check	We recommend you make sure your system is fit, capable, and performs well. Since ESET Inspect deals with a lot of data, you may experience performance issues. Generally, the database can be a bottleneck. Such performance issues are usually caused by undersized hardware specifications, especially insufficient disk space. However, the performance can also be hindered if there are too many events being collected by ESET Inspect. A **healthy** server have a **high** number of Events processed per second but a **low** Event Packet Queue Length. Do a performance check of your server to see how it is doing.
Minimize the number of events	**Events processed and stored per computer** (stored/received within 24 hours) has the biggest impact on performance. An event is an action done by a process. Such as file write, DNS lookup, new registry entry, etc. All these are individual events listed in the Raw Events view. An average workstation produces about 100 000 stored events per 24 hours (depending on the environment). Your goal is to lower the number of stored events. Some event filters (automatic exclusions) are proposed by ESET Inspect, click Questions to review the exclusions, then accept or reject. You can also customize, or manually create exclusions, to further optimize performance in Event Filters. Configure Settings > **Data collection** by choosing what type of data should be collected from endpoint computers. Available in the on-premises version only.

Tweak	Description
Events load	ESET Inspect collects events data, among which there are anomalies or outliers. Identify the outliers, for example, known executable events considered as safe and generate excessive occurrences. To reduce the number of events, create a filter for executable: 1.Navigate to **Dashboard** > **Events load** > **Events per executable**. Click the tallest column of events generated to see what executables are producing too many events. 2.Click the executable name to see its details. If you consider this event as safe, create an event filter. 3.Click the Filter events at the bottom right, follow the wizard and specify **Criteria** and **Event types** for this executable. Select event types that cause the most events. If you need further criteria, use the **Advanced editor** to create an in-depth filter. See the ESET Inspect rules guide for reference. Repeat this process until you have dealt with most of the outlier events. Also, follow the procedure for the other tables within the **Events load**. This optimization can have significant impact increasing performance.
Change events frequency	If there are still too many events, you can decide to decrease the interval when events are sent by creating a new policy in ESET PROTECT On-Prem: Navigate to Policies > **New policy** > **Settings** and select ESET Inspect Connector, and in the **Interval of sending events to the server**, specify desired time how often are events sent.
False positive detections	Get rid of false positives to unload the database and prevent future flooding with unnecessary data. Create rule exclusions for False positive detections. • Enable event filters (automatic exclusions) are proposed by ESET Inspect, click Questions to review the exclusions, then accept or reject. You can also customize or manually create exclusions to further optimize performance in Event Filters. • Reconsider the chosen type of ESET Inspect user. If you are not going to continuously analyze a large number of detections daily (in the case of the **Security Operations Center** user type), choose different ESET Inspect user type, such as **Security-focused IT Team** or even **IT Administrator**. This allows you to deal with fewer detections. • Enable **Rule learning mode** in Settings (if it is not running). • Use Mark as safe for executables considered not risky. Marking as safe can prevent some rules from triggering and producing false positives. • Disable rules that do not suit your environment. For example, if you are using VNC for remote connection, disable the `VNC connection from internal IP range [D0523a]` rule. • Modify default rules to match your network. For example, edit the `VNC connection from internal IP range [D0523a]` rule to accept connections only on specified IP addresses, ranges or ports, so that the rule is triggered only when a suspicious connection occurs. • Make sure the LiveGrid® connection works. Many rules rely on LiveGrid® information to function correctly. If there is an issue with LiveGrid®, you will see a warning in Questions section, also in **Dashboard** > **Server Status**. • Be careful when using Microsoft Signer Name while creating Exclusions. Microsoft executables are sometimes signed differently on different Microsoft Windows editions.

Tweak	Description
Tips	• Keep ESET Inspect Connectors and ESET Inspect Server up to date. Mismatching ESET Inspect Connector and ESET Inspect Server versions may cause unpredictable behavior. The latest ESET Inspect Server version usually contains several fixes and improvements. • If you are using a "golden master" image with a pre-installed ESET Inspect Connector to deploy client workstations, make sure to take the appropriate measures. Otherwise, all clones created from the image use the same database thread, causing very poor performance. To avoid issues, use the same methods that apply to ESET Management Agent. • Keep an eye on disk space. If the disk space on the ESET Inspect Database server falls below 10%, the database purge will stop working, which will consume even more disk space. This applies to the ESET Inspect on-premises version only. • Consider lowering the Database Retention settings (available in the on-premises version only). • Keep the operating system language in mind when creating Exclusions. `"NT AUTHORITY\NETWORK SERVICE"` on an English installation of windows is called `"NT AUTHORITY\Servicio de Red"` in Spanish. This can also differ between Microsoft Windows editions. In this case, use `"TriggeringUserSid"` and not `"TriggeringUserName"`. • Keep a copy of the ESET Inspect rules guide handy for reference. • Speed up loading the table view (for example, in Detections), use the gear icon to modify the table options and remove unnecessary columns and filters.

Performance check

To check the current performance of your ESET Inspect database server, navigate to **Dashboard** > Server Status. Inspect the following event statistics:

- Events processed per second—**higher** numbers are better
- Event Packet Queue Length—**lower** numbers are better

If your server has a low number of **Events processed per second** and high number of **Event Packet Queue Length**, it is too busy. For example, if the packet queue is at around 500 most of the time, this means you have a performance issue. Events cannot be processed fast enough by the database, and the data is placed in a queue on the disk. View the queue by browsing to:

%PROGRAMDATA%\ESET\Inspect Server\UnprocessedEvents

If the content size of this folder is larger than 10% of available system RAM, the server stops accepting new events.

Warnings about insufficient disk space are displayed in Questions section. Also, you can monitor estimated ESET Inspect Database size in **Dashboard** > Events load to prevent from running out of disk space.

Other reasons why performance problems might be occurring:

- Disk containing the database has less than 5% of free space remaining.
- Disk containing the Temp folder has less than 10% of free space remaining.

This can cause clients running the ESET Inspect Connector to have connection issues; you will be receiving

warning messages in ESET PROTECT On-Prem: “`Can't connect to Enterprise Inspector Server`”. Not all events will be available to you, and detections will be triggered with a delay. The clients will start caching events locally in their own temporary folders. If this folder grows above 1GB in size, the events will start getting discarded and never be received by the ESET Inspect Server.

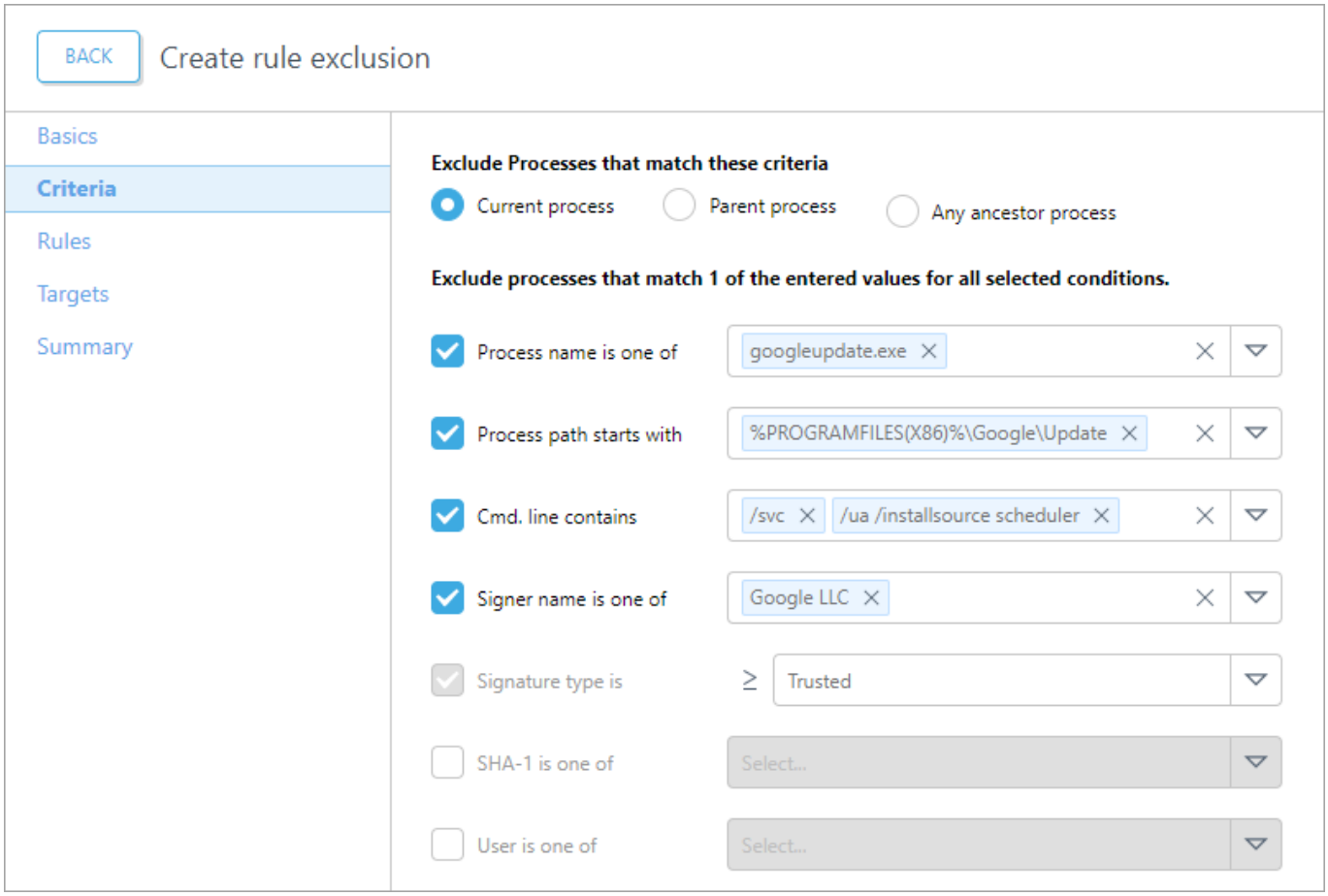
False positive detections

The following example use case shows you how to reduce false positive detections. You can use this approach on most of the false positives.

1. Navigate to **Dashboard** and switch to **Executables** tab. You will see **Problematic Executables** at the bottom right. Sort the table by ▽ **Unresolved** (descending) to see the executables that are responsible for the most detections.

2. Right-click the top executable and choose **Detections**. In this example, the *googleupdate.exe* process has a high number of detections. Use the filter to group detections by **Rules**. You will see the rule was triggered 2475 times:

3. The **Potential credential dumping** rule was triggered on several computers, all with a similar command line. Select a rule and click **Create exclusion**. In **Criteria**, select **Process path starts with** and **Cmd. line contains** check boxes. It is better to use generic attributes such as folders, signatures, and command line options. Avoid using hashes in exclusions. Otherwise, you will be hiring a new colleague only to keep up with changing hashes.



4. Click **Continue** and make sure the **Auto-resolving** option is selected to have all future detections resolved. Enabling this option will also resolve all past detections matching this exclusion (this could take one day to happen).

5. Click **Continue**, then click **Assign** to select computers or groups where you want this exclusion to apply and click **OK**.

6. Click **Continue** and review the summary of configured settings in the **Exclusion preview**. Verify all the settings for this exclusion and click **Create exclusion**.

7. Navigate to **More** > **Tasks** tab to view the progress of the resolving task. Depending on the size of your database, this could take several hours or days. It shows you how many detections were hit by this exclusion.

ℹ Repeat this process on other false positives until you create exclusions for most outlier detections.

Computers

Your environment structure of computers and devices managed via ESET PROTECT On-Prem. The table with computer provides you with a detailed view of essential information about each machine, its status, time of the last communication and last event.

The view aims to give emphasis on the severity and unresolved detections, enabling the security team to perform computer-centric investigation. Focus on the computers with the highest rate, severity, and frequency of detections. These computers may indicate an acute need for further investigation, or a false positives to be resolved.

You can quickly perform actions, like initiate Reboot or Shutdown of the computer. A useful feature is the Terminal for PowerShell connection to any computer.

Preview panel

Click a computer name to display the preview panel on the right side. The computer preview panel contains the most important information about the select computer. Some items are interactive.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

The Computer details window consists of the following parts:

Details

Click a computer to display comprehensive details.

Terminal

The terminal is a nifty feature for advanced security professionals in allowing PowerShell to be invoked remotely on an endpoint without breaking the end-user's workflow (or an attacker noticing that someone is onto him). PowerShell provides many options for detailed investigation and remediation of an endpoint without relying solely on the actions built into ESET Inspect.

Alerts

Shows a potential issue with the connectivity to the ESET Inspect Server. These alerts are obtained from ESET PROTECT On-Prem.

Detections

Provides the main Detections for the selected computer. Select a detection to display Detection details to view the changes, including displaying the name of the triggering Rule with a link and Rule category name, Event link, Occurred time and date, triggering process link, Command line, and information about the user to whom the detection is related.

Executables

This screen provides you with the same options as the main Executables tab, except the list contains only executables triggered on a specific computer.

Scripts

Display the same options as the main Scripts tab, except the list contains only scripts triggered on a specific computer.

Events

The Events screen shows the list of all events that occurred on this computer. To view event in the Raw events, right-click the name of the event and click **Show in Process's Raw Events**. To find out details about a event, select a event to open the Process details. A low-level event is something a process does. So, write a file, do a DNS lookup, create a registry entry, etc. ESET Inspect analysis low-level events to find suspicious activities and report detections.

Click a computer to take further actions:

Details	Go to the Computer details tab.
Details (Protect)	Go to the ESET PROTECT On-Prem Web Console.
Detections	Go to the Detections tab.
Executables	Go to the Executables tab.
Scripts	Go to the Scripts tab.
Events	Go to the Events tab.
Scan	Sends the command to Endpoint to start an immediate scan of the computer (or use the Action button).
Network Isolation	Isolate the computer from the network (only connections between ESET Security products are available). If required, you can also End isolation (available only for Windows endpoints; File Security from 7.2.12003.0).
Connect via Terminal	Go to the Terminal tab.
Power	Sends the command to reboot or shut down the computer.
Log Out	Logs the currently logged user out.
Send wake-up call	Sends the Wake-Up command to force the computer to send all events since the last connection (or use Action button).
Generate SysInspector log	Generate the SysInspector log and review it in the computer's details (or use the Action button).
Tags	Assign tag(s) to a computer from the list of existing, or create a new custom tag(s).
Audit log	Go to the Audit log tab.
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).
Incident	Create an incident report, add to currently active, or add to (last 3 incidents).

Filter the computers by the following statutes:

Threat	Detection(s) with threat severity present on this computer.
Warning	Detection(s) with warning severity present on this computer.
Information	Detection(s) with informational severity present on this computer.
OK	No detections were triggered on this computer, or all are resolved.
Unmonitored	ESET Inspect Connector is not installed on this computer. (ESET Inspect know about this computer because the ESET PROTECT On-Prem sent it from an Active Directory).

Computer details

There are the following tiles with details about the computer:

- **Computer**—Name of the computer.

- **Select Tags**—Assign tag(s) to a computer from the list of existing, or create a new custom tag(s).
- **FQDN**—Fully qualified domain name if your server is a member of a domain.
- **Parent Group**—The name of a group of computers where this specific computer is assigned. The computer's group can be changed in the ESET PROTECT On-Prem.
- **Last connected**—Permanent connection created to listen on notification about blocked hashes, requests to download some file, kill the process, etc. The refresh interval is 90 seconds.
- **Last event**—The timestamp of the last event is sent to the server. This event occurred on the computer, not when it was sent to the ESET Inspect Server.
- **ESET Inspect Connector version**—Version of the ESET Inspect Connector, deployed on the specific computer.
- **OS Name**—The operating system's name running on the specific computer.
- **OS Version**—The name of the OS running on this specific computer

Unresolved Detections (Unique / Total):

Threats	**Detection(s) with threat severity present on this computer.**
Warnings	Detection(s) with warning severity present on this computer.
Informational	Detection(s) with informational severity present on this computer.

- **Group**—The name of a group of computers where this specific computer is assigned. The computer's group can be changed in the ESET PROTECT On-Prem.
- **Isolated From Network**—The information whether the computer was isolated from the network.
- **Received Events From Today**—Count of events that appear today.
- **Stored Events From Today**—Count of events stored today in the database. The difference against the received events from today is caused by Event Filters.
- **Endpoint Version**—The version of installed ESET Endpoint Security on this specific computer.
- **OS Platform**—The bit version of OS running on this specific computer.
- **Network Adapters**—Shows information about all network adapters.
- **Sysinspector Logs**—Shows the list of Sysinspector logs requested for this computer.
- **Comments**—Add an optional comment to recognize the detection easily.

Action buttons:

Details (Protect)	**Go to the ESET PROTECT On-Prem Web Console.**
Detections	Go to the Detections tab.

Details (Protect)	Go to the ESET PROTECT On-Prem Web Console.
Executables	Go to the Executables tab.
Scripts	Go to the Scripts tab.
Events	Go to the Events tab.
Scan	Sends the command to Endpoint to start an immediate scan of the computer (or use the Action button).
Network Isolation	Isolate the computer from the network (only connections between ESET Security products are available). If required, you can also End isolation (available only for Windows endpoints; File Security from 7.2.12003.0).
Connect via Terminal	Go to the Terminal tab.
Power	Sends the command to reboot or shut down the computer.
Log out	Logs the currently logged user out.
Send wake-up call	Sends the Wake-Up command to force the computer to send all events since the last connection (or use Action button).
Generate SysInspector log	Generate the SysInspector log and review it in the computer's details (or use the Action button).
Tags	Assign tag(s) to a computer from the list of existing, or create a new custom tag(s).
Audit log	Go to the Audit log tab.
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).
Incident	Create an incident report, add to currently active, or add to (last 3 incidents).

Terminal

Use the terminal tab to connect to a client computer when investigating detected issues remotely.

The terminal access is available only for computers running Microsoft Windows. Ensure the client computer is using Powershell version 5.1 or later.

Log in to the terminal using the ESET Inspect user account. User account requirements:

- **Remote Shell Access** permission in ESET PROTECT On-Prem under the **Granted ESET Inspect Functionality**.
- **2FA** (two-factor authentication) to minimize security risk.

The terminal limitations:

- Supported—Single command line tools and scripts.
- Not supported—Full screen text applications (for example, Vim).

Processes

Here you can find the list of all processes triggered by the executable. When you open the **Computer** details > click **Events** tab and select a process to get to the Process details.

Click a process name to take further actions:

Details	Go to the Executable details tab.
Aggregated Events	Go to the Aggregated events of this concrete process.
Detections	Go to the Raw Events tab.
Raw Events	Go to the Events tab.
Loaded Modules (DLLs)	Sends the command to Endpoint to start an immediate scan of the computer.
Scripts	Displays scripts executed by this concrete process.
Tags	Assign tag(s) to a process from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Process details

There are the following tiles with details about the processes:

- **Name**—Name of the process is shown here. By clicking on the name, you are redirected to the Executable details.
- **SHA-1**—Hash of the executable.

By clicking the gear icon next to the hash, the context menu shows up, where you can use two options:

- Open the **Virus Total search page** that you can define in the Settings tab.
- **Copy to clipboard**—The hash to your clipboard for further use.

- **Signer Name**—If the file is signed, here you can see the signer of the file.
- **Seen on**—The number of computers on which the file was discovered. After clicking on it, you are redirected to the Computers view, with a filtered computers list.
- **Signature Type**—Information whether the file is signed or not and how it is signed (Trusted/Valid/None/Invalid/Unknown). If the value is Present, the executable is signed, but the ESET Inspect does not know the certificate's status. This is uncommon for Windows, but on MacOS, a signature is never verified by Endpoint, and as a result, the only possible states are Present and None.
- **Seen on**—The number of computers on which the file was discovered. After clicking on it, you are redirected to the Computers view, with a filtered computers list.
- **File Description**—The full description of the file, for example, Keyboard Driver for AT-Style Keyboards.
- **First Seen**—When an executable was first seen on any computer in a monitored network.
- **Last Executed**—When an executable was last executed on any computer in a monitored network.

LiveGrid®

- **Reputation (LiveGrid®)**—Is a number from 1 to 9, indicating how safe the file is. 1–2 Red is malicious, 3–7 Yellow is suspicious, 8–9 Green is safe.
- **Popularity (LiveGrid®)**—How many computers reported an executable to LiveGrid®.

- **First Seen (LiveGrid®)**—When an executable was first seen on any computer connected to LiveGrid®.

Popularity	On how many computers it was seen in LiveGrid®	Color	Description
0	0	red	Not seen
1	1–9	red	Low
2	10–99	yellow	Medium
3	100–999	yellow	Medium
4	1 000–9 999	yellow	Medium
5	10 000–99 999	green	High
6	100 000–999 999	green	High
7	1 000 000–9 999 999	green	High
8	10 000 000–99 999 999	green	High
9	100 000 000–999 999 999	green	High
10	1 000 000 000–9 999 999 999	green	High
11	10 000 000 000–99 999 999 999	green	High

Events

- **File**—How many file modifications were made by this executable.
- **Registry**—How many registry modifications were made by this executable.
- **Network**—How many network connections were made by this executable.

Computer

Shows the name of the computer where the detection triggered. Click the computer name, you are redirected to Computer details. You can also click **View detections on this computer** open the Computer detection list of this specific computer.

- **Parent Group**—The name of a group of computers where this specific computer is assigned. The computer's group can be changed in the ESET PROTECT On-Prem.
- **Last connected**—Permanent connection created to listen on notification about blocked hashes, requests to download some file, kill the process, etc. The refresh interval is 90 seconds.
- **Last event**—The timestamp of the last event is sent to the server. This event occurred on the computer, not when it was sent to the ESET Inspect Server.
- **ESET Inspect Connector version**—Version of the ESET Inspect Connector, deployed on the specific computer.
- **OS Name**—The operating system's name running on the specific computer.
- **OS Version**—The name of the OS running on this specific computer

- **Process**—The name and the ID of the process. After clicking the executable name, you are redirected to the Executable details
- **Command line**—A command line command that executes this process.
- **Path**—Path on the disk where the executable is located.
- **Started**—The time when the process was executed.
- **Ended**—The time when the process was executed.
- **Parent process**—The process that created this child process. After clicking its name, you are redirected to the Process details of that specific process
- **First dropper**—The first recorded process that has dropped (created on disk) module(executable file) of a given process on a given computer (that given process was run). By clicking it, you are redirected to the Process details of that process.
- **Compromised**—If available shows if the process is compromised.
- **LnkPath**—The string contains a path to a shortcut execution.
- **Note**—Add the note by clicking the **Set note**.
- **Executable**—The name of the executable dropped by the first dropper and the one that started the process.

Integrity Level

Represented by the arrow in the process tree, the grid of Detections tab, and everywhere where the process name is present. These levels are present:

- **Untrusted**—blue arrow down. Blocks most write access to a majority of objects.
- **Low**—blue arrow down. Blocks most write access to registry keys and file objects.
- **Medium**—no icon. This is the default setting for most processes when UAC has been enabled on the system.
- **High**—red icon up. Most processes will have this setting if UAC is disabled and the currently logged on user is the administrator.
- **System**—red icon up. This is a setting reserved for system level components.
- **Protected process**—red icon up. Is used by some anti-malware services, only allows trusted, signed code to load, and has a built-in defense against code injection attacks.

Username

The name of the user/account that was logged in when the detection was raised.

- **Full name**—User's full name, if available from Active Directory.
- **Job Position**—User's job position, if available from Active Directory.
- **User Department**—User's department, if available from Active Directory.
- **User Description**—User's description, if available from Active Directory.

To display the user details, you need to define the following parameters for user in Active Directory:

ESET Inspect On-Prem parameter name	Attribute name
Full Name	cn
Job Position	title
User Department	division
User Description	description

Then run synchronization task to update user information.

Comments

Add an optional comment to recognize the detection easily.

Audit Log

You see actions that were taken on this detection. At the moment, Resolved, Unresolved, Commented, and Priority Changed.

The process tree on the right side

The process tree reflects the parent-child relationship between processes where child processes are shown directly beneath their parent and right-indented. Processes that are on the left are orphans, and their parent has exited.

Process details action buttons:

- **Incident**—Create an incident report, add to currently active, or add to (last 3 incidents).
- **Download file**—To download the executable file for further investigation.
- **Kill process**—Kill the process, if it is still active in the operation memory.
- **Submit to ESET LiveGuard**—Manually submitting file to the ESET LiveGuard analysis.

Do not **Block** or **Kill** any process or executable of any Windows system processes and files. (for example, `svchost.exe`) Otherwise, this may cause a crash of the Operating system.

Aggregated Events

Events that are grouped into categories, providing count and path. Click the path to get to the Computer Events view.

- File modifications
- File reads
- Registry modifications
- Network connections
- URL connections
- Dropped Executables
- DNS resolutions

> Character limitations were implemented for all types of events to limit the database growth. These character limitations were set to 260.

The process tree on the right side

The process tree reflects the parent-child relationship between processes where child processes are shown directly beneath their parent and right-indented. Processes that are on the left are orphans, and their parent has exited.

Show Sub-Process Events—If you want to see the child process events.

Argument—Specify, for example, the path to the file modifications, registry key in registry modifications. Search by event argument, depending on the event type it can be a patch, filename, directory name, IP address.

If there are too many results, only a part of them is loaded. If you use **Load more** or **Load all** events, it may take a considerable amount of time to load all the results.

Process detections

List of Detections triggered by this specific process. All columns, filters, and buttons are the same as in the Detections tab.

The process tree on the right side

The process tree reflects the parent-child relationship between processes where child processes are shown directly beneath their parent and right-indented. Processes that are on the left are orphans, and their parent has exited.

Raw Events

If you click the name of the process, you are redirected to the Process details of the selected process. To view event in the Computer events, right-click the name of the raw event and click **Show in Computer's Events**. Use filters at the top of the screen to refine the list of displayed items. Click **Show Sub-Process Events**—If you want to see the child process events as well.

The process tree on the right side

The process tree reflects the parent-child relationship between processes where child processes are shown directly beneath their parent and right-indented. Processes that are on the left are orphans, and their parent has exited.

Earlier versions of Windows do not produce WMI events. This functionality is available since Windows 10 version 1803.
Some of the events provide only partial information:
- **File write events**—Only the first file change is recorded (This is per process. If two processes change the same file, both changes are recorded).
- **Registry related events**—Only the first registry key change is recorded (first time by a process).
- **DLLLoad**—Only dll's which AV does not whitelist are recorded.
- **TcpIp events**—Only the first connection is recorded (first time by a process).
- **Http events**—Only the first request is recorded (first time by a process).
- **ModuleDrop** (a.k.a PEDrop)—It is reported only for the first drop of a given module (first time on a computer).
- **AmsiTriggerEvent**—Only the first execution is recorded (first time on a computer).

Use the action buttons to limit the view of listed processes.

Loaded Modules (DLLs)

The list of all DLLs loaded by this process. You can select all DLLs available on the screen or select individual one and **Mark as Safe**, **Mark as Unsafe**, **Block**, **Unblock**, **Mark as Inspected**, **Mark as Not inspected** them, or click **Seen On** button to get the list of computers on which these DLLs were seen on by using the buttons located at the bottom of the screen.

The process tree on the right side

The process tree reflects the parent-child relationship between processes where child processes are shown directly beneath their parent and right-indented. Processes that are on the left are orphans, and their parent has exited.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

Click a loaded module to take further actions:

Details	Go to the Executable details tab.
Statistics	Go to the Statistics tab.
Detections	Go to the Detections tab.
Seen On	Go to the Seen On tab.
Sources	Go to the Sources tab.
Block	Go to the Block Hashes tab.
Unblock	Hash from Blocked Hash section is removed.
Mark as Safe	Safe state, many rules determine the risk. Mark as Safe does have an impact on detections. Select the targets you want to mark as safe from target window. Mark as Safe does not necessarily guarantee that a specific module will never be included in detections. There are a few hundred rules, and some raise detections, regardless of which module executed the suspicious action. For example, a popular instance, trusted modules as PowerShell, can do it. Other rules try to evaluate risk based on the module. Such rules consider the “safe” flag. This flag means that the user analyzed the module, and it is unlikely that the module is malicious, so rules assume that the risk is earlier during the evaluation.
Mark as Unsafe	If you marked as safe some executable by mistake, you could use this to unmark it.
Download File	The download window for the affected DLL appears.
Tags	Assign tag(s) to a loaded module from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Process scripts

This feature is available only on Windows 10 endpoint machines.

ESET Inspect uses AMSI to get the content of scripts executed on ESET Inspect Connector machines through Endpoint Security.

ESET Inspect Connector machine needs EES 7.2 or later with AMSI option enabled in **Advanced Settings** > **Detection Engine** > **Advanced Options** section. It should be enabled by default.

On Windows 10, AMSI provides us information about:

- PowerShell (scripts, interactive use, and dynamic code evaluation)
- Windows Script Host (wscript.exe and cscript.exe)
- JavaScript and VBScript
- Office VBA macros

To detect suspicious VBA scripts on monitored machines, ESET Inspect needs Office 365 version 1808 and enabled macro scanning. To enable the macro scanning, the user should set the *HKEY_CURRENT_USER\Software\Microsoft\Office\%VERSION%\Common\Security\MacroRuntimeScanScope* register value to 1 or run the following script in the command line:

```
powershell.exe -command "if (Test-Path -Path HKCU:\Software\Microsoft\Office) {
foreach ($reg_path in Get-ChildItem -Path HKCU:\Software\Microsoft\Office |
Where-Object {($_.Name.Contains(\".\"))}) { $reg_sub_path = (Join-Path -Path
$reg_path.Name -ChildPath '').Replace(\"HKEY_CURRENT_USER\", \"HKCU:\");
$reg_sub_path_common = (Join-Path -Path $reg_path.Name -ChildPath
'Common').Replace(\"HKEY_CURRENT_USER\", \"HKCU:\");
$reg_sub_path_common_security = (Join-Path -Path $reg_path.Name -ChildPath
'Common\Security').Replace(\"HKEY_CURRENT_USER\", \"HKCU:\"); if (!(Test-Path -
Path $reg_sub_path_common)) { New-Item –Path $reg_sub_path –Name \"Common\"; } if
(!(Test-Path -Path $reg_sub_path_common_security)) { New-Item –Path
$reg_sub_path_common –Name \"Security\"; } Set-ItemProperty -Path
$reg_sub_path_common_security -Name \"MacroRuntimeScanScope\" -Value 1; }}"
```

That means the script mentioned above that was run on the ESET Inspect Connector machine displays content in the ESET Inspect Web Console.

Incidents

The Incident management system includes multiple tools such as commenting, editing incident attributes, or assigning them to various users and changing their status to reflect current progress.

You can create new incidents in Computers, Detections, and Executables details.

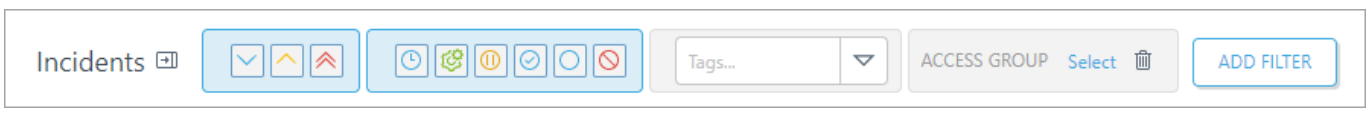
Incidents inspected by ESET Services Representative (ESR) will have the new flag **Investigated by ESET** added after the name of the incident.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

Choose one of the options to create a new incident or add the detection to an existing incident.

- **Create incident**—This option redirects the user to the wizard window.
- **Add to current incident**—Add elements to the current incident.
- **Add to incident**—Depending on the order of the items, you can add an element to the last three incidents.



Incident severity

- **Low severity**—The severity of the incident is set as low.
- **Medium severity**—The severity of the incident is set as medium.

- **High severity**—The severity of the incident is set as high.

Incident statuses

- **Open**—The report is in an open state or was reopened by a security administrator or other user.
- **In-progress**—The report is in-progress currently being investigated.
- **On Hold**—The report is in status on hold, waiting for other inputs from the report analysis.
- **Resolved (true positive)**—The report is in state resolved and waiting for closure.
- **Closed**—The report is closed.
- **Invalid (false positive)**—The report is in an invalid state.

Select incident to open the information window consists of the following parts:

Timeline

Shows detailed time-stamped information about incident changes. The right side shows info regarding the Status, Severity, Assigned user, number of Detections, Executables, Computers, Processes, and Tags, if present, added to the report. The right side of the screen provides additional information based on the selected object type. Use the button **Details** to get into the selected object's details page.
- **Incident**—Comprehensive details of the incident.
- **Details**—Comprehensive details of the computer.
- **Process Tree**—The process tree related to the process.
- **Related objects**—List of related objects to the incident.

Relation graph

Displays interactive node graph visualization of selected incident with listed detections, computers, executables and a timeline describing the sequence of events. Right-click on any node in the graph to open a context menu containing a drop-down menu of actions related to the selected node. You can move and reposition any node of the graph to better suit your needs. Use the **Graph** menu for additional actions:
- **Fit**— Center the graph to display all nodes on the screen.
- **Reset**— Reset the position of all nodes to their initial state.
- **Redraw**— Update the displayed information in the graph.

The right side of the screen provides additional information based on the selected element in the graph:
- **Incident**— Comprehensive details of the incident
- **Timeline**— Shows detailed time-stamped information about Incident changes. Highlights the node in the graph based on the selected event in the timeline.
- **Details**— Comprehensive information about the selected element in the graph.
- **Process tree**— Displays selected element's position from the graph in the process tree.
- **Related objects**— List of related objects to the selected element in the graph.

Detections

If the report contains any detections, the list of these detections is shown in this tab. It contains the same options to work with detections as the Detections tab, except a **Remove** button, that allows the user to remove selected detection from the report.

Computers

If the report contains any computers, the list of these computers is shown in this tab. It contains the same options to work with computers, except a Remove button, that allows the user to remove selected computers from the report.

Executables

If the report contains any executables, the list of these executables is shown in this tab. It contains the same options to work with executables, except a Remove button, that allows the user to remove selected executables from the report.

Processes

If the report contains any processes, the list of these processes is shown in this tab. You can remove selected processes from the report.

Click an incident name to take further actions:

- **Details**—Go to incident details tab.
- **Make current incident**—Use to indicate current incident. Highlights the incident in the blue color.
- **Assign**—To assign the report to a specific user to investigate it.
- **Progress**— Change the progress state of selected incident.
  - **Start progress**—Use to change the report status to In progress state.
  - **On hold**—Use to change the report status to On hold state.
  - **Resolve (true positive)**—Use to change the report status to Resolved state.
  - **Close**—Use to change the report status to Closed state.
  - **Reopen**—If you consider that the report needs reinvestigation.
  - **Invalid (false positive)**—Use to change the report status to Invalid state.
  - **Delete incident**—Deletes the incident.
- **Access group**—Displays currently assigned access group. Click **Move** to assign different access group.
- **Tags**—Assign tag(s) to an incident from the list of existing, or create new custom tag(s).
- **Filter**—Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

- **Threat indicators** — If enabled. displays indicators of the threat in the timeline.
- **Behaviours** — If enabled, displays behavior of the threat in the timeline.
- **Analyst actions** — if enabled, displays analyst actions in the timeline.

Create incident

You can create new incidents in Computers, Detections, and Executables details. Select a Detection of interest for further investigation and create an incident.

Incident creator is available only in ESET Inspect On-Prem Cloud.

Choose one of the options to create a new incident or add the detection to an existing incident.

- **Create incident**—This option redirects the user to the wizard window.
- **Add to current incident**—Add elements to the current incident.
- **Add to incident**—Depending on the order of the items, you can add an element to the last three incidents.

1. Click **Create incident** to open an incident template and specify custom settings.
2. Type an incident **Name** and **Description**.
3. Choose **Severity**.
4. Specify **Assignee** to investigate the incident.
5. Assign **Tags** from the list of available tags, or create a new custom tag(s).
6. Click **Create** to finish. The incident is created and will appear in the Incident view.

Search

Use search when looking for any object. **Basic search** enables you to search wit pre-defined parameters. **Advanced events search** is fully customizable using the expression.

Basic Search

Available parameter combinations for the basic search:
1.**Object Type**—Select a category (Detections, Computers, Events, Executables and Processes).
2.**Related objects** (optional)—Select if you want to narrow down the search result.
3.**Attributes**—Select from the available attributes.
4.Type your query (value), press Enter, and click **Search**.
The list of available attributes:
• **Rule Name**—Search by the name of the rule.
• **Note**—Search by the name of the note that was made in Detections, Executables and Processes.
• **Comment**—Search by the comment that was made in Detection, Executables, Computers and Processes.
• **Description**—Search by the description of the computer, taken from ESET PROTECT On-Prem.
• **Name**—Search by the name of the computer, executable or process.
• **IP Address**—Search by the IP address of the computer.
• **MAC Address**—Search by the MAC address of the computer.
• **Argument**—Search by event argument, depending on the event type it can be a patch, filename, directory name, IP address.
• **SHA-1**—Search by the SHA-1 of the executable.
• **SHA-256**—Search by the SHA-256 of the executable.
• **MD5**—Search by the MD5 of the executable.
• **Version Info**—Search by the module version info (file description, internal filename, original filename, company name, file version, product version).
• **Signer**—Search by the signer of the executable.
• **Origins**—Search by the origin of the executable.
• **Dropper SHA-1**—Search by the SHA-1 of the dropper.
• **Command Line**—Search by the command line of the process.

Advanced Event Search

Enables you to define complex criteria to filter out events. Choose the object type Computers, Executables or Events.
Customize the expression according to your needs. Refer to the Rules Guide for details.

Search result

The search result table is refreshed automatically when the search is running. The view of the search results is based on object type, in case of two parameter search, on object type and related object type in case of three parameter search.
Click a search result to take further actions:
• **Details**—Redirects you to the relevant section depending on the Object type.
• **Start**—Starts selected search results.
• **Pause**—Pause selected search results.
• **Duplicate query**—Duplicates selected search result.
• **Delete**—Deletes selected search results.
• **Rename**—Enables you to rename the search result for better distinguish.
• **Tags**—Used to tag the search. After choosing this option, new window for tag edition opens. in the Select field, you can type new tag or select already existing one.
• **Filter**—Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Detections

ESET Inspect includes rule-based detection engine for Indicators of Attack.

Rules that are written to identify suspicious, malicious behavior trigger detections with defined severity. Each triggered detection is displayed in the detection section with clear identification of where it happened

(Computer), which executable has triggered it, even which specific process triggered it. It is accompanied by severity information as defined in the rule and assigns a priority to each detections (later available as a filtering option). Detections are also 1:1 shown in the Threats section of ESET PROTECT On-Prem under a specific log type labeled ESET Inspect. When detection is resolved from ESET Inspect/ESET PROTECT On-Prem, it is also resolved in the other system (the systems are synchronized).

Detections view allows advanced grouping and filtering by any column in the view. It is also possible to save filter sets per user preference. The user can drill down into details of every detection, where further details about the executable/process/user, computer, and explanation of possible cause, with suggested next steps, are displayed. The user can navigate to Details of the executable, Process, Rule from detections and continue the further investigation. Detection detail layout is similar to the design language used in the ESET PROTECT On-Prem, focusing on easy readability.

Preview panel

Click a detection to display the preview panel on the right side. The detection preview contains the most important information about the select detection. Some items are interactive.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

Detection types

Click the detection type to display comprehensive details.

Firewall

Shows detections triggered by ESET Endpoint Security itself, for example, if some Firewall rule was triggered.

HIPS

Shows detections triggered by ESET Endpoint Security itself when HIPS protection detects intrusion.

Filtered Websites

Shows detections triggered by ESET Endpoint Security itself if the website is from (PUA, Internal or Anti-Phishing) blacklist.

Antivirus

Shows detections triggered by ESET Endpoint Security itself, after Scan or after Real-time detection.

Rule

Filters detections triggered based on rules.

Blocked Executables

Shows detections triggered by matching the Blocked hashes listed in the **More** section.

Detection Groups

Ungrouped	**This is the default view. When you open the Detections tab for the first time, you see each detection separately.**
Types	In this filter, detections are grouped based on detection type (trigger was a rule or a file blocked based on a hash).
Computers	Detections grouped by a computer on which they occurred.
Rules	Grouped by rules that raised detections.
Processes	Grouped by processes that raised detections.
Executables	Grouped by executables that raised detections.
Uniqueness	Grouped by the uniqueness of the detection type.

Priority (filter icons)

Click to show only items with specific priority. There are four types, no priority and priority I to III. All icons are deactivated by default, meaning the items with all priorities are displayed. Click the priority icon to activate the filter and show only items with selected priority.

Severity

Shows the severity of the detection: Threat  , Warning  , Info 

Click a detection to take further actions:

Computer Details	**Go to the Computer details tab.**
Toggle Group	Not available if ungrouped is selected. Expand or contract the group.
Mark as Resolved	Marks the detection as Resolved.
Mark as not Resolved	Marks the detection as Unresolved.
Create Exclusion	Create an exclusion task for selected rules. You are redirected to the Create Rule Exclusion.
Edit Rule	Redirected to the Edit Rule section if the detection was raised by a rule.
Edit User Actions	Edit user actions for selected detection rule. Opens the Edit User Actions window.
Priority	Marks the detection as **No priority**/**Priority I**/**Priority II**/**Priority III**.
Add Comment	Optionally, you can add a comment.
Open	**Open Computer**—Opens Computer details of the Computer on which the detection was triggered. **Open Process**—If the detection was triggered by Rule, redirect to Process details of the process that caused the detection. **Open Parent Process**—If the detection has a parent process, it redirects you to the Process details of that parent process.
Tags	Assign tag(s) to a detection from the list of existing, or create new custom tag(s).
Audit log	Go to the Audit log tab.
Incident	Create an incident report, add to currently active, or add to (last 3 incidents).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Detection details

There are the following tiles with details about the detection:

- **Name**—The name of the threat.
- **Occurred**—Date and time of occurrence.
- **Triggering process**—Shows the name of the triggering process with its integrity level.
- **Command Line**—Shows command line that the triggering process used.
- **Username**—Shows the name of the user that was logged when the event happened.
- **User Role**—Show the role of the user that is listed in the Username.
- **Computer**—Shows the name of the computer that raised the detection. After clicking the computer name, you are redirected to Computer details.
- **Parent Group**—The name of a group of computers where this specific computer is assigned. The computer's group can be changed in the ESET PROTECT On-Prem.
- **Last connected**—Permanent connection created to listen on notification about blocked hashes, requests to download some file, kill the process, etc. The refresh interval is 90 seconds.

- **Priority**—The priority of the detection. This can be changed via Priority buttons.
- **Severity**—Shows the severity of the detection: Threat, Warning, Info
- **Severity Score**—A more precise definition of severity. 1–39 > Info 40–69 > Warning 70–100 > Threat
- **Resolved**—Shows whether the detection is marked as Resolved. This can be changed via Priority buttons.
- **Note**—You can add the note by clicking the **Set note** blue string on the right side of the window.
- **Triggering Process**—The name of the process (with corresponding Process ID) that triggered the detection. After clicking the name, you are redirected to the Process details.
- **Command Line**—Show the name of the Command line filename.
- **Path**—Appears if detection was triggered by a blocked hash or ESET Endpoint Security.

Detection Type

- **Rule**—Filters detections triggered based on rules.
- **Blocked**—Shows detections triggered by matching the Blocked hashes listed in the **More** section.
- **Antivirus**—Shows detections triggered by ESET Endpoint Security itself, after Scan or after Real-time

detection.

• **Firewall**—Shows detections triggered by ESET Endpoint Security itself, for example, if some Firewall rule was triggered.

• **HIPS**—Shows detections triggered by ESET Endpoint Security itself when HIPS protection detects intrusion.

• **Filtered Websites**—Shows detections triggered by ESET Endpoint Security itself if the website is from (PUA, Internal or Anti-Phishing) blacklist.

Threat Type

Appears only if the detection was triggered by a blocked hash or the ESET Endpoint Security:

• **Malware**—Potentially unwanted applications

• **Potentially unwanted application**—(PUAs) are not necessarily intended to be malicious but may affect the performance of your computer in a negative way.

• **Hash blocked by ESET Inspect**—The file was blocked by hash, that was added in Blocked Hashes section.

• **Suspicious applications**—Include programs compressed by packers or protectors. Malware authors often exploit these types of protectors to evade detection.

• **Threat Name**—The name of the threat that can be found in this list http://www.virusradar.com/en/threat_encyclopaedia

Triggering Executable

The executable that triggered the detection. After clicking the name, you are redirected to the Executable details.

• **SHA-1**—Hash of the executable.

By clicking the gear icon next to the hash, the context menu shows up, where you can use two options:

- Open the **Virus Total search page** that you can define in the Settings tab.
- **Copy to clipboard**—The hash to your clipboard for further use.

• **Signature Type**—Information whether the file is signed or not and how it is signed (Trusted/Valid/None/Invalid/Unknown). If the value is Present, the executable is signed, but the ESET Inspect does not know the certificate's status. This is uncommon for Windows, but on MacOS, a signature is never verified by Endpoint, and as a result, the only possible states are Present and None.

• **Signer Name**—If the file is signed, here you can see the signer of the file.

• **Seen on**—The number of computers on which the file was discovered. After clicking on it, you are redirected to the Computers view, with a filtered computers list.

• **File Description**—The full description of the file, for example, Keyboard Driver for AT-Style Keyboards.

• **First Seen**—When an executable was first seen on any computer in a monitored network.

• **Reputation (LiveGrid®)**—Is a number from 1 to 9, indicating how safe the file is. 1–2 Red is malicious, 3–7 Yellow is suspicious, 8–9 Green is safe.

• **Popularity (LiveGrid®)**—How many computers reported an executable to LiveGrid®.

• **First Seen (LiveGrid®)**—When an executable was first seen on any computer connected to LiveGrid®.

Popularity	On how many computers it was seen in LiveGrid®	Color	Description
0	0	red	Not seen
1	1–9	red	Low
2	10–99	yellow	Medium
3	100–999	yellow	Medium
4	1 000–9 999	yellow	Medium
5	10 000–99 999	green	High
6	100 000–999 999	green	High
7	1 000 000–9 999 999	green	High
8	10 000 000–99 999 999	green	High
9	100 000 000–999 999 999	green	High
10	1 000 000 000–9 999 999 999	green	High
11	10 000 000 000–99 999 999 999	green	High

• **IP Protocol**—which IP Protocol was used.

• **Source Socket**—The IP Address from which the possible attack was made.

• **Destination Socket**—The IP Address that was the target of the possible attack.

• **Reporting interface**—If available, MAC address of the network adapter on which we received the packet that caused the alarm.

• **Occurred**—Shows the date and time of occurrence of the process.

• **Triggered**—Shows the date and time when the detection was triggered.

• **Threat Handled**—Shows whether an action was taken against this detection.

• **Restart Needed**—Shows if the restart is needed to resolve this detection.

Action Taken

• **Cleaned**—Executable was cleared from harmful code.

• **Deleted**—Executable was deleted.

• **Connection terminated**—The connection was terminated before the infection could do a harm.

• **Cleaned by deleting**—Executable was deleted.

- **Was a part of the deleted object**—Executable was a part of a deleted archive.
- **Marked for deletion**—Executable is inaccessible and marked for manual deletion.
- **Blocked**—The access to the executable was blocked, but the executable remains.

> Do not **Block** or **Kill** any process or executable of any Windows system processes and files. (for example, `svchost.exe`) Otherwise, this may cause a crash of the Operating system.

Integrity Level

Represented by the arrow in the process tree, the grid of Detections tab, and everywhere where the process name is present. These levels are present:

- **Untrusted**—blue arrow down. Blocks most write access to a majority of objects.
- **Low**—blue arrow down. Blocks most write access to registry keys and file objects.
- **Medium**—no icon. This is the default setting for most processes when UAC has been enabled on the system.
- **High**—red icon up. Most processes will have this setting if UAC is disabled and the currently logged on user is the administrator.
- **System**—red icon up. This is a setting reserved for system level components.
- **Protected process**—red icon up. Is used by some anti-malware services, only allows trusted, signed code to load, and has a built-in defense against code injection attacks.

Computer

Shows the name of the computer where the detection triggered. Click the computer name, you are redirected to Computer details. You can also click **View detections on this computer** open the Computer detection list of this specific computer.

Username

The name of the user/account that was logged in when the detection was raised.

- **Full name**—User's full name, if available from Active Directory.
- **Job Position**—User's job position, if available from Active Directory.
- **User Department**—User's department, if available from Active Directory.
- **User Description**—User's description, if available from Active Directory.

To display the user details, you need to define the following parameters for user in Active Directory:

ESET Inspect On-Prem parameter name	Attribute name
Full Name	cn
Job Position	title
User Department	division
User Description	description

Then run synchronization task to update user information.

Audit Log

You see actions that were taken on this detection. At the moment, Resolved, Unresolved, Commented, and Priority Changed.

Comments

Add an optional comment to recognize the detection easily.

Action buttons

You can manage the detection by using the buttons in the lower part of the screen.

Detections

- **Open computer**—Opens Computer details of the Computer on which the detection was triggered.
- **Open process**—If the detection was triggered by Rule, redirect to Process details of the process that caused the detection.
- **Open parent process**—If the detection has a parent process, it redirects you to the Process details of that parent process.
- **Mark as resolved**—Marks the detection as Resolved.
- **Mark as not resolved**—Marks the detection as Unresolved.
- **Create exclusion**—Create an exclusion task for selected rules. You are redirected to the Create Rule Exclusion.
- **Edit rule**—Redirected to the Edit Rule section if the detection was raised by a rule.
- **Edit user actions**—Edit user actions for selected detection rule. Opens the Edit User Actions window.
- **Priority**—Marks the detection as **No priority**/**Priority I**/**Priority II**/**Priority III**.
- **Add comment**—Optionally, you can add a comment.
- **Tags**—Assign tag(s) to a detection from the list of existing, or create new custom tag(s).
- **Audit log**—Go to the Audit log tab.

- **Diagnostic information**— Enable collection of additional diagnostic data for a selected rule.
  - **Start Collection**— The next time the rule triggers an alarm, diagnostic information will be collected and prepared for download.
  - **Download**— Download the password-protected ZIP archive containing diagnostic data for a selected rule. The password is displayed on the download screen. After the download is finished, the collection will stop.

Incident

Create an incident report, add to currently active, or add to (last 3 incidents).

Remediation

- **Protect network**
- **Block executable**—Prevent the executable from running by blocking it based on the SHA-1 hash. The blocked executable will appear in the Blocked Hashes section.
- **Clean & block executable**—Delete the executable file and add it to Blocked Hashes to prevent future occurrences.
- **Isolated from Network**—Block all network communication on the computer, except the connection between ESET security products.
- **Protect computer**
- **Kill process on this computer**—Kill the running process that triggered the detection.
- **Scan computer for malware**—Run On-demand computer scan.
- **Shutdown computer**—Send the command to shut the computer down.

Kill process

Kill selected process on this computer.

Computer

- **scan**—Sends the command to Endpoint to start an immediate scan of the computer.
- **SysInspector log**—Generate the SysInspector log and review it in the computer's details (or use the Action button).
- **Reboot/Shutdown**—Sends the command to reboot or shut down the computer.
- **Isolate**—Isolate the computer from the network (only connections between ESET Security products are available). If required, you can also End isolation (available only for Windows endpoints; File Security from 7.2.12003.0).
- **Details (Protect)**—Go to the ESET PROTECT On-Prem Web Console.

Executable

- **Block**—Go to the Block Hashes tab.
- **Download file**—The download window for the affected process appears.
- **Submit to ESET LiveGuard**—Manually submitting file to the ESET LiveGuard analysis. This feature is available from ESET PROTECT On-Prem version 10.1 or later.

Executables

The executables table represents an entire repository of all of the discovered executables (and DLLs) within the network monitored by ESET Inspect.

For each executable granular statistics are provided, such as Reputation/popularity in LiveGrid®, First seen by LiveGrid®, on how many computers it was seen/executed. How many file operations, established network connections, what modifications it made, and further metadata, which is helpful to identify the potentially suspicious behavior of any executable.

The most data-dense view in ESET Inspect. It enables the most powerful customization options from the perspective of displayed columns and filtering. You can see details about how many detections each executable triggered and what the highest severity of a triggered detection was.

You can check the details of every executable, including the statistical data mentioned above and the detections of the executable triggered, the origin of the executable, and registry entries. All information will help you with the investigation based on what behavior the executable was evaluated as malicious.

You can also drill down to aggregated/raw events to examine them to figure out any activity that might be violating the company policy. It is also possible to perform remediation action - download executable for further investigation, add it to a block list (by hash) and kill a specific process.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

OS type (filter icons)

Click an icon to hide items. Filter by Operating System platform to see or hide the executables for Windows, macOS or Linux.

Executable type (filter icons)

Click to see only EXE or DLL files, or both simultaneously, where:

EXE = executable file

DLL = library file

Status

You can filter executables to see or hide executables marked as Threat, Warning, Information, OK

The Executables details window consists of the following parts:

Details

Click the name of the executable to display comprehensive details.

Statistics

Statistical information about a specific executable or executable with the same file checksum is listed here.
- **Seen on**—Number of computers on which the executable occurred.
- **Executed on**—Number of computers on which the executable executed.
- **Executions count**—Total number of executions of the executable.
- **Sent bytes**—Total number of bytes sent by the file, from all computers, for all processes.
- **Network connections**—Number of network connections made by the file.
- **File modifications**—Number of files that were modified (written to, deleted, renamed).
- **Registry modifications**—Number of registry entries that were modified.
- **Executable drops**—Number of dropped executables made by this executable.
- **HTTP Events**—Number of HTTP events made by this executable.
- **DNS Events**—Number of DNS events made by this executable.
- **Events/24H**—Number of events made by this executable within 24 hours.

Detections

This tab provides the same options as the main Detections, but only detections triggered by this specific executable. After clicking on a Detection, you are redirected to its Detection details.

Seen on

List of all computers on which the executable or executables with the same file checksum was seen.

Sources

List of dropped executables and additional information.

Click an executable name to take further actions:

Details	Go to the Executable details tab.
Statistics	Go to the Statistics tab.
Detections	Go to the Detections tab.
Seen On	Go to the Seen On tab.
Sources	Go to the Sources tab.
Block	Go to the Block Hashes tab.
Unblock	Hash from Blocked Hash section is removed.

Details	Go to the Executable details tab.
Mark as Safe	Safe state, many rules determine the risk. Mark as Safe does have an impact on detections. Select the targets you want to mark as safe from target window. Mark as Safe does not necessarily guarantee that a specific module will never be included in detections. There are a few hundred rules, and some raise detections, regardless of which module executed the suspicious action. For example, a popular instance, trusted modules as PowerShell, can do it. Other rules try to evaluate risk based on the module. Such rules consider the “safe” flag. This flag means that the user analyzed the module, and it is unlikely that the module is malicious, so rules assume that the risk is earlier during the evaluation.
Mark as Unsafe	If you marked as safe some executable by mistake, you could use this to unmark it.
Download File	The download window for the affected DLL appears.
Submit to ESET LiveGuard	Manually submitting file to the ESET LiveGuard analysis. This feature is available from ESET PROTECT On-Prem version 10.1 or later.
Filter events	Go to the Create event storage filter.
Tags	Assign tag(s) to an executable from the list of existing, or create a new custom tag(s).
Audit log	Go to the Audit log tab.
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Do not **Block** or **Kill** any process or executable of any Windows system processes and files. (for example, `svchost.exe`) Otherwise, this may cause a crash of the Operating system.

Executable details

There are the following tiles with details about the executable:

- **Name**—The name of the executable or DLL is shown.
- **Select Tags**—Assign tag(s) to a computer from the list of existing, or create a new custom tag(s).
- **Signature Type**—Information whether the file is signed or not and how it is signed (Trusted/Valid/None/Invalid/Unknown). If the value is Present, the executable is signed, but the ESET Inspect does not know the certificate's status. This is uncommon for Windows, but on MacOS, a signature is never verified by Endpoint, and as a result, the only possible states are Present and None.
- **Seen on**—The number of computers on which the file was discovered. After clicking on it, you are redirected to the Computers view, with a filtered computers list.
- **First Seen**—When an executable was first seen on any computer in a monitored network.
- **Last Executed**—When an executable was last executed on any computer in a monitored network.
- **Reputation (LiveGrid®)**—Is a number from 1 to 9, indicating how safe the file is. 1–2 Red is malicious, 3–7 Yellow is suspicious, 8–9 Green is safe.
- **Popularity (LiveGrid®)**—How many computers reported an executable to LiveGrid®.
- **First Seen (LiveGrid®)**—When an executable was first seen on any computer connected to LiveGrid®.

Popularity	On how many computers it was seen in LiveGrid®	Color	Description
0	0	red	Not seen
1	1–9	red	Low
2	10–99	yellow	Medium
3	100–999	yellow	Medium
4	1 000–9 999	yellow	Medium
5	10 000–99 999	green	High
6	100 000–999 999	green	High
7	1 000 000–9 999 999	green	High
8	10 000 000–99 999 999	green	High
9	100 000 000–999 999 999	green	High
10	1 000 000 000–9 999 999 999	green	High
11	10 000 000 000–99 999 999 999	green	High

- **File**—How many file modifications were made by this executable.
- **Registry**—How many registry modifications were made by this executable.
- **Network**—How many network connections were made by this executable.

Unresolved Detections(Unique / Total):

Threats	Detection(s) with threat severity present on this computer.
Warnings	Detection(s) with warning severity present on this computer.
Informational	Detection(s) with informational severity present on this computer.

The executable that triggered the detection. After clicking the name, you are redirected to the Executable details.

- **SHA-1**—Hash of the executable.

By clicking the gear icon next to the hash, the context menu shows up, where you can use two options:

- Open the **Virus Total search page** that you can define in the Settings tab.
- **Copy to clipboard**—The hash to your clipboard for further use.

- **SHA-256**—If available the 256 bit hash is present.
- **MD5**—if available the MD5 hash is present.
- **Signature Type**—Information whether the file is signed or not and how it is signed (Trusted/Valid/None/Invalid/Unknown). If the value is Present, the executable is signed, but the ESET Inspect does not know the certificate's status. This is uncommon for Windows, but on MacOS, a signature is never verified by Endpoint, and as a result, the only possible states are Present and None.
- **User Id**—For macOS only. Same as the file description column for windows.

- **Signature CN #1**—For macOS only. Same as product name column for windows.
- **Signature CN #2**—For macOS only. Same as file version column for windows.
- **Signature CN #3**—For macOS only. Same as product version column for windows.
- **Signature CN #4**—For macOS only. Same as internal name column for windows.
- **Signature CN #5**—For macOS only. Same as original filename column for windows.
- **Signature Id**—For macOS only. Same as company name column for windows.
- **Whitelist type**—Information if an executable is whitelisted:
  - **Certificate**—The executable is whitelisted because it is signed by the trusted certificate.
  - **LiveGrid®**—The executable is whitelisted because the trustworthiness of the file was confirmed by ESET.
- **File description**—File description of the file, for example, "Keyboard Driver for AT-Style Keyboards".
- **File version**—Version number of the file, for example, "3.10" or "5.00.RC2".
- **Company name**—Company that produced the file, Microsoft Corporation or Standard Micro-systems Corporation, Inc.
- **Product name**—The name of the product with which the file is distributed.
- **Product version**—Version of the product with which the file is distributed.
- **Internal name**—Internal name of the file, if one exists, for example, an executable name if the file is a dynamic-link library. If the file has no internal name, this string will be the original filename, without extension.
- **Original file name**—The original name of the file, not including a path. This information allows an application to determine whether a file has been renamed by a user. The format of the name depends on the file system for which the file was created
- **Packer name**—The name of packer if a executable is packed.
- **SFX name**—Self-extracting archive type, if an executable is packed.
- **File size**—The size of the file on the disk.
- **First seen**—When was executable first identified by ESET Inspect on any computer.
- **First executed**—When was executable first executed on any computer. When clicked you are redirected to the Process details of this executable.
- **Last Executed**—When an executable was last executed on any computer in a monitored network.
- **Marked as safe**—Marked as safe by security engineers (users of ESET Inspect Web Console). If the status is "No" you can change with the action button.
- **Blocked**—Blocked by Security Engineer (user of ESET Inspect Web Console).

• **Nearmiss report**—If the detection triggered due to malware, but we cannot hundred percent guarantee it is a malware.

• **Note**—You can add the note by clicking the **Set note** blue string on the right side of the window.

• **Status**—Expresses the result of the behavioral analysis or the absence of a result (Unknown/Clean/Suspicious/Highly suspicious/Malicious).

• **State**—Expresses the executable's present station in the analysis workflow.

• **Sent On**—The time when was the executable sent to ESET LiveGuard.

• **Last Processed On**—The time when was the executable last processed on.

• **Behavior**—The link to the behavioral report of the executable.

• **Audit Log**—You see actions that were taken on this detection. At the moment, Resolved, Unresolved, Commented, and Priority Changed.

• **Comments**—Add an optional comment to recognize the detection easily.

Action buttons:

Incident	Create an incident report, add to currently active, or add to (last 3 incidents).
Block	Go to the Block Hashes tab.
Unblock	Hash from Blocked Hash section is removed.
Mark as Safe	Safe state, many rules determine the risk. Mark as Safe does have an impact on detections. Select the targets you want to mark as safe from target window. Mark as Safe does not necessarily guarantee that a specific module will never be included in detections. There are a few hundred rules, and some raise detections, regardless of which module executed the suspicious action. For example, a popular instance, trusted modules as PowerShell, can do it. Other rules try to evaluate risk based on the module. Such rules consider the “safe” flag. This flag means that the user analyzed the module, and it is unlikely that the module is malicious, so rules assume that the risk is earlier during the evaluation.
Mark as Unsafe	If you marked as safe some executable by mistake, you could use this to unmark it.
Download File	The download window for the affected DLL appears.
Submit to ESET LiveGuard	Manually submitting file to the ESET LiveGuard analysis. This feature is available from ESET PROTECT On-Prem version 10.1 or later.
Filter Events	Create event storage filter.
Tags	Assign tag(s) to an executable from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Seen on

List of all computers on which the executable (based on checksum) was seen.

If the executable was seen on a computer that was part of the database Purge, its row will be gray.

Click a computer to take further actions:

Details	Go to the Executable details tab.
Detections	Go to the Detections tab.
Executables	Go to the Executables tab.
Scripts	Go to the Scripts tab.
Events	Go to the Events tab.
Aggregated Events	Go to the Aggregated Events tab.
Processes	Go to the Processes tab.
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Sources

List of dropped executables and additional information is shown here:

- **Origin Executables**—Executable or DLL responsible for the creation of this specific executable. When you click the executable's name, you are redirected to Executable details.
- **Origin Emails**—The executable that comes from an email attachment. Includes information **From** which email address the email was sent, **To** who was sent and what was the **Subject** of email.
- **Origin Websites**—If the executable was downloaded from the website, the URL is shown here, but only if downloaded from HTTP, not HTTPS, as HTTPS is encrypted connection. This information is not present if SSL processing is disabled in ESET Endpoint Security product (Setup > Advanced setup > Web and email > SSL/TLS > Enable SSL/TLS protocol filtering).
- **Dropped Executables**—List of executables dropped by this executable. When you click the executable's name, you are redirected to Executable details.

Scripts

Many recent attacks/infections are performed using file-less malware, which happens by executions of scripts that deliver a malicious payload or do any harmful activity.

ESET Inspect provides granular insight into all scripts executed within the company. Shows details about what changes were done and if any of the scripts triggered a specific behavior-based detection.

Security engineers can see details about the Event, entire process tree, detailed Command line parameters (arguments). All of that is needed for a detailed forensic investigation.

Use filters and group scripts by the Command line to easily spot anomalies or potentially suspicious activities.

Visual Basic scripts and scripts for PowerShell (WScript and CScript) are supported.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

Process Groups

- **Ungrouped**—List of scripts sorted by Process Name (ID).
- **First child executable**—Grouped by the first child process that is a successor of the script. Name and the process ID in Task Manager.
- **Parent executable**—Grouped by parent process that is an ancestor of the script. Name and the process ID in Task Manager. in Task Manager.
- **Command line**—Grouped by the Command line / Process Name (ID) used to execute the executable.

Create Exclusion

Enables you to create an exclusion for a specified script(s). In the **Basics** section, type basic information about the task, such as a **Exclusion Name** and **Note** (optional) for a more in-depth description of the exclusion. Click **Continue** to configure the task settings.

Criteria

You can use pre-defined criteria:

- **Process name is one of**—Type the names of the process that you want to apply the exclusion.
- **Cmd. line contains**—Type in the process parameters if you want to exclude them by parameters.
- **User is one of**—Type in the names of all users you want to apply the exclusion.

Targets

Click **Assign** to select computers or groups where you want this exclusion to apply and click **OK**.

Summary

Review the summary of configured settings in the **Exclusion preview**. Verify all the settings for this exclusion and click **Create exclusion**.

After creating the exclusion, you are redirected to the Exclusions in the More tab.

Click process name to take further actions:

Details	Go to the Process details tab.
Aggregated Events	Go to the Aggregated events of of this specific process.
Detections	Go to the Detections tab with a list of detections for this specific script.
Raw Events	Go to the Raw Events tab of this specific process.
Loaded Modules	Go to the Loaded Modules tab.
Parent Process	Go to parent process details tab of this specific process.
First Child Process	Go to first child process details tab of this specific process if available.

Details	Go to the Process details tab.
Mark as Safe	Safe state, many rules determine the risk. Mark as Safe does have an impact on detections. Select the targets you want to mark as safe from target window. Mark as Safe does not necessarily guarantee that a specific module will never be included in detections. There are a few hundred rules, and some raise detections, regardless of which module executed the suspicious action. For example, a popular instance, trusted modules as PowerShell, can do it. Other rules try to evaluate risk based on the module. Such rules consider the “safe” flag. This flag means that the user analyzed the module, and it is unlikely that the module is malicious, so rules assume that the risk is earlier during the evaluation.
Mark as Unsafe	If you marked as safe some executable by mistake, you could use this to unmark it.
Create Exclusion	Create an exclusion for a specified script(s).
Download Script	The download window for the script for further investigation. Only if the script is still available in the network.
Tags	Assign tag(s) to a process from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Questions

Questions are items that concern some of the ESET Inspect functionality (for example, automatic exclusions, database purge, LiveGrid®).

There are multiple scenarios which can result in a notification that may require your attention and a decision to be made. This include, for example, automatically created exclusions, warnings of database storage issues and/or database optimizations, issues with network and LiveGrid® connectivity and others. These questions, or notifications, can be managed (accept/reject for Exclusions and resolve for general) and filtered.

Click the active question, and a notification window with questions details will shows up. Perform the appropriate action using the **Resolve** or **Cancel** button.

Click **Add filter** and select one of the available: **Status** or **Type** to reduce the number of items.

The Question icon appears at the top of the screen whenever a new or unresolved notification in the system occurs.

More

Contains a sub-menu with more features and configuration possibilities for Detections, Server, and Activity Audit. One of the features is the ESET Inspect Settings. You can use it to configure your ESET Inspect environment and ESET Inspect Database settings. Create rules and add hashes that security engineers want to block from executing on the network. Run tasks from the event filters, and create exclusions for processes.

The following quick links are available:

Detections

Rules

Exclusions

Blocked Hashes

Server

Tasks

Event Filters

Settings

Activity audit

Audit log

Rules

Rules are the behavior- and reputation-based descriptions that ESET Inspect can identify from the received events and metadata.

Security engineers can add and edit their rules, but there is also a set of rules provided by ESET that security engineers cannot modify.

A rule is defined using XML-based language. Rules are matched on the server asynchronously, so there is some time interval when recent events are sent from client to server and then processed by rules. A matched rule can only notify security engineers by raising the detection.

The detection is displayed in the Detections view, but it is exported to ESET PROTECT On-Prem and eventually to a connected SIEM tool. An email can be automatically sent when the detection is triggered using the ESET PROTECT On-Prem notification mechanism.

Based on the result of the investigation, the security engineer can perform a manual remediation action.

With improvements of ESET PROTECT On-Prem Orchestration framework, it will be possible to define automated incident response criteria that will be executed dynamically after rule-based detection.

> Rules with severity 22 and below are telemetry rules. They are usually used only as additional information for investigating an incident and can often be triggered by legitimate behavior. If some of these rules generate too much traffic in your environment, you may consider turning them off.

Since version 1.8 you can evaluate detection rules in ESET Inspect Connector, you need to enable LiveGrid® in ESET Endpoint to use this feature. Enabled LiveGrid® in ESET Endpoint is required for ESET Inspect version 1.8 or later.

Suppose there are performance issues on the ESET Endpoint using ESET Inspect Connector version 1.8 or later. In that case, you can switch detection rules evaluation to be done by ESET Inspect Server. This option is only available for on-premises.

Activate detection rules evaluation on ESET Inspect Server.

1. In ESET PROTECT On-Prem, click **Policies** > **New policy** and type the name of the policy.
2. Click **Settings** and select ESET Inspect Connector from the drop-down menu.
3. Click **Advanced Settings** and click the slider next to **Evaluate detections on ESET Inspect Server**.

If the connection between ESET Inspect Server and ESET Inspect Connector is interrupted:

- ESET Inspect Connector will perform the evaluation and send the triggered detections, and collected raw events to the ESET Inspect Server after the restored connection
- ESET Inspect Connector finds a match between the raw event and detection rule, which has response action assigned, and only the **Kill process** is executed immediately

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

The rule window consists of the following parts:

Rule details

Summary of the rule.
- **Rule**—The name of the rule.
- **Author**—The name of the user that was logged at the time of the rule creation.
- **Last Edit**—Date of the last edit of the rule.
- **Category**—Category name that you can find among category tags in the Edit Rule section.
- **Severity**—Shows the severity of the detection: Threat, Warning, Info
- **Severity Score**—A more precise definition of severity. 1–39 > Info 40–69 > Warning 70–100 > Threat
- **Remediation actions**—Click **Select user actions** to open rule options and choose what action(s) to apply.
- **Explanation**—Explanation of the behavior of the file.
- **Malicious Causes**—What can be a result of a file execution.
- **Benign Causes**—Detail about possibly unharmful activity.
- **MITRE ATT&CK™ TECHNIQUES**—If the rule contains an ID of the MITRE ATT&CK™ TECHNIQUE it is shown here.
- **Rerun Tasks**—The number of rerunning the tasks containing this rule.
- **Exclusions**—The number of exclusions created for this rule.
- **Tags**—Assign tag(s) to a rule from the list of existing, or create new custom tag(s).

Edit Rule

You can add or edit the rules. On the right side, you can see the Syntax Reference,where on the bottom, you can find the link to the Rules Guide.

Targets

You can see and assign or unassign computers or groups in this window.

Rerun Tasks

Provides the same information as the sub-tab Tasks in the More tab, except it shows only tasks created for this specific rule.

Exclusions

Provides the same options as the Exclusions sub-tab in the More tab. After clicking on an Detection, you are redirected to its Detection details.

Click a rule name to take further actions:

Details	Opens summary of the rule.
Detections	Redirect to the Detections view of the specific rule.
Exclusions	Go to the Exclusions view of the specific rule.
Edit Rule	Redirect to Edit Rule section if the detection was raised by a rule.
Edit User Actions	Redirect to Edit User Actions section of the specific rule.
Change assignment	Go to the Targets view of the specific rule.
Rerun Tasks	Go to the Rerun Tasks view of the specific rule.
Create Exclusion	Create an exclusion task for selected rules. You are redirected to the Create Rule Exclusion.
Enable	
Disable	
Delete	
Save As	Creates a new rule with the desired name and opens rule editor.
Access group	Displays currently assigned access group. Click **Move** to assign different access group.
Tags	Assign tag(s) to a rule from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).
Rerun Rules	Redirects you to Create rerun task window.
Export	Starts the export process of the rule, depending on the used web browser. The format of the file is XML.
Import	Opens the window for import the XML rule file.

Edit rule

Lets you modify the parameters of the rules.

> On the right side, you can see the **Syntax Reference** where on the bottom you can find the link to the **Rules Guide**.

These actions are available in the edit rule window:

Finish—When you are done editing or creating rule, click **Finish** to save the rule.

Check syntax—This is used to check whether there is a problem with the rule.

Close—This button will trigger the notification window with these options (only for Customized rules and if they were edited):

- **Save**—Saves the rule.
- **Do not Save**—Discards any changes made.
- **Cancel**—Returns you to the edit window.

Delete—If you want to delete the opened rule.

Save as—Saves the rule with the customized name.

Rerun rules—Redirects you to Create rerun task window.

Export—Starts the export process of the rule, depending on the used web browser. The format of the file is XML.

Edit User Actions/Remediation

Lets you modify and execute user actions taken triggered by the rule.

Edit User Actions

To open select rule actions window, right-click a rule/detection name and select **Edit User Actions**.

In the select rule actions window you can find the following details:

- **Rule**—The name of the rule. Click the rule name to open details of the rule in the new window.
- **Unresolved Detections**—The number of the unresolved detections triggered by this rule.
- **Built-in actions**—Actions that are set by default (Report detection, Store event).

These actions are available in the select rule actions window:

Protect network—Actions to prevent executable spread across the network.

- **Block executable**—Prevents the executable from running by blocking the executable based on the SHA-1 hash. The blocked executable will appear in the Blocked Hashes section.
- **Clean & block executable**—Deletes the executable file and adds the executable to the Blocked Hashes.
- **Isolate computer from network**—Blocks all network communication on the computer except the connection between ESET security products.
- **Block suspicious modules used by process**—Blocks all suspicious modules loaded by the process. The other processes cannot use these modules.

Protect Computer—Actions to prevent executable harm the computer.

- **Kill process on this computer**—Kills the running process that triggered the detection.
- **Shutdown computer**—Sends the command to shut the computer down.
- **Log out**—Sends the command to log the currently logged user out.

Apply rule actions—Depending which action boxes you checked , these rule actions will be applied when the rule is triggered.

Cancel—Closes the select rule actions window.

Remediation

To open remediate threat window, open details of the detection and click **Remediation**.

In the remediate threat window you can find the following details:

- **Computer**—The name of the computer, where the detection was raised by the rule. Click the name of the computer to open the computer details in the new window.
- **Executable**—The name of the executable, which triggered the rule. Click the name of the executable to open the executable details in the new window.
- **Reputation**—Displays reputation score from LiveGrid®. 1–2 Red is malicious, 3–7 Yellow is suspicious, 8–9 Green is safe.

These actions are available in the remediate threat window:

Protect network—Actions to prevent executable spread across the network.

- **Block executable**—Prevents the executable from running by blocking the executable based on the SHA-1 hash. The blocked executable will appear in the Blocked Hashes section.
- **Clean & block executable**—Deletes the executable file and adds the executable to the Blocked Hashes.
- **Isolate computer from network**—Blocks all network communication on the computer except the connection between ESET security products.

Protect Computer—Actions to prevent executable harm the computer.

- **Kill process on this computer**—Kills the running process that triggered the detection.
- **Shutdown computer**—Sends the command to shut the computer down.
- **Scan computer for malware**—Starts on-demand scan on the affected computer.

Trigger actions automatically for this rule—When checked, actions you set in the select rule actions window after clicking **Remediate** will be applied.

Remediate—Execute user actions immediately. Additional confirmation window with selected actions will appear.

Cancel—Closes the remediate threat window.

Rerun tasks

Provides the same information as the sub-tab Tasks in the More tab, except it shows only tasks created for this specific rule.

The **Rerun rules** have the same functionality as creating a New task in Tasks tab.

Exclusions

ESET Inspect provides the ability to match incoming events against the rules. Rules are defined using an XML-based language to predicate conditions over events property (Module name, Hash, Signer, Popularity).

Rules can be edited/enabled/disabled when events reception is provided to the RuleEngine component to be compiled and matched against the events, eventually raising a detection.

For this reason, the possibility to filter/exclude some detections is needed.

As most of the filtering is going to be based on exactly the same property used in the rules, exclusions are defined using the same language used by the rules. This has the notable advantage of allowing for fair reuse of much of the existing machinery.

Provides an editing tool wizard, as exclusions are usually strictly related to some existing rule. Starting from an existing detection, this wizard will provide some initial values for the exclusion rule conditions.

Set of pre-defined exclusions (enabled by default) that you can enable later.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

Right-click an exclusion name to take further actions:

Edit	Go to the update exclusion window.
Enable	
Disable	
Delete	
Access group	Displays currently assigned access group. Click **Move** to assign different access group.
Tags	Assign tag(s) to an exclusion from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).
New exclusion	Go to the Create exclusion window.
Export	Starts the export process of the rule, depending on the used web browser. The format of the file is XML.
Import	Opens the window for import the XML rule file.

Create exclusion

This topic covers both the rule exclusion and script exclusion creation process.

> If the create exclusion button was used for the selected rule(s), for example on Detection rules page or Detections, some data specific to rule(s) are prefilled.

To create a new exclusion, click **Exclusion** > **New exclusion**.

In the **Basics** section, type basic information about the exclusion, such as an **Exclusion name** and **Note** (optional) for a more in-depth description.

Criteria

Click **Continue** to configure the exclusion settings. Exclude processes is divided into three parts:

- **Current process**—Criteria created for the currently selected process.
- **Parent process**—Criteria created for the parent process of actual selection.
- **Any ancestor process**—Criteria created for any ancestor process.

You can use pre-defined criteria:

- **Process name is one of**—Type the names of the process that you want to apply the exclusion.
- **Process path starts with**—The path to the specified process (C:\Windows or %SYSTEM% can be used).
- **Cmd. line contains**—Type in the process parameters if you want to exclude them by parameters.
- **Signer is one of**—Type the names of the signer for exclusion.
- **Signature type is**—Choose comparison operators, is, is not, greater than or equal, less or equal and then the type of Signer can be Trusted, Valid, None, Invalid, Unknown. It is a mandatory field when Signer is selected.
- **SHA-1 is one of**—Type the SHAs of the processes you want to exclude if known.
- **User is one of**—Type in the names of all users you want to apply the exclusion.

Optionally, use **Advanced editor** to further modify the criteria by changing the **Rule syntax**.

Rules

Select rules that you want to exclude. Click **Add filter**, and select **Rule name** and type string to search.

Auto-resolving—When selected, all detections (already detected in the past) fulfilling the exclusion criteria will be marked as resolved. They will not appear in the default view in detections views.

Targets

Click **Assign** to select computers or groups where you want this exclusion to apply and click **OK**.

Summary

Review the summary of configured settings in the **Exclusion preview**. Verify all the settings for this exclusion and click **Create exclusion**.

After creating the exclusion, you are redirected to the Exclusions sub-tab from the More tab.

Create an exclusion for a specified script

In the **Basics** section, type basic information about the exclusion, such as an **Exclusion name** and **Note** (optional) for a more in-depth description.

Criteria

You can use pre-defined criteria:

- **Process name is one of**—Type the names of the process that you want to apply the exclusion.
- **Cmd. line contains**—Type in the process parameters if you want to exclude them by parameters.
- **User is one of**—Type in the names of all users you want to apply the exclusion.

Optionally, use **Advanced editor** to further modify the criteria by changing the **Rule syntax**.

Targets

Click **Assign** to select computers or groups where you want this exclusion to apply and click **OK**.

Summary

Review the summary of configured settings in the **Exclusion preview**. Verify all the settings for this exclusion and click **Create exclusion**.

Create event storage filter

In the **Basics** section, type basic information about the exclusion, such as an **Exclusion name** and **Note** (optional) for a more in-depth description.

Criteria

You can use pre-defined criteria:

- **Process name is one of**—Type the names of the process that you want to apply the exclusion.
- **Process path starts with**—The path to the specified process (C:\Windows or %SYSTEM% can be used).
- **Cmd. line contains**—Type in the process parameters if you want to exclude them by parameters.
- **Signer is one of**—Type the names of the signer for exclusion.
- **Signature type is**—Choose comparison operators, is, is not, greater than or equal, less or equal and then the type of Signer can be Trusted, Valid, None, Invalid, Unknown. It is a mandatory field when Signer is

selected.

- **SHA-1 is one of**—Type the SHAs of the processes you want to exclude if known.

- **User is one of**—Type in the names of all users you want to apply the exclusion.

Optionally, use **Advanced editor** to further modify the criteria by changing the **Rule syntax**.

Targets

Click **Assign** to select computers or groups where you want this exclusion to apply and click **OK**.

Summary

Review the summary of configured settings in the **Exclusion preview**. Verify all the settings for this exclusion and click **Create exclusion**.

Event types

- File system events
- TCP events
- Registry events
- HTTP events
- DNS events

After creating the exclusion, you are redirected to the Event filters sub-tab from the More tab.

Blocked Hashes

Blocked hashes contain a list of executables/hashes blocked by all security products connected to ESET Inspect. You can add blocked hashes from executables or executables detail, or type manually from any other source.

Hashes support only SHA-1. It enables companies to remediate any malicious code (prevent its execution ex-post, or even proactively, getting the hashes in an IoC feed).

Whenever an attempt to execute a blocked executable occurs, it is reported as a security incident to ESET PROTECT On-Prem and listed under a specific threats section category - blocked files.

The Blocked hashes enable you to interact with the list of hashes. It enables blocking hashes from external tools as well.

Click an executable name to take further actions:

Details	Go to the Executable details tab.
Statistics	Go to the Statistics tab.
Detections	Go to the Detections tab.
Seen On	Go to the Seen On tab.

Details	Go to the Executable details tab.
Sources	Go to the Executable sources tab.
Unblock	Unblocks the hash and make it possible to work with the executable without blocking it. Available only if some blocked hashes are selected. You can select all blocked hashes by selecting the check box on the left side of the Name column header, or you can select each blocked hash individually by selecting its corresponding check box.
Clean & Quarantine	Deletes the file and put it to quarantine in the Endpoint. Available only if some blocked hashes are selected. You can select all blocked hashes by clicking the check box on the left side of the Name column header, or you can select each blocked hash individually by selecting its corresponding check box.
Tags	Assign tag(s) to a blocked hash from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).
Add hashes	Redirects you to Block Hashes window.

Do not **Block** or **Kill** any process or executable of any Windows system processes and files. (for example, `svchost.exe`) Otherwise, this may cause a crash of the Operating system.

Block Hashes

You can add SHA-1 hashes that you want to be blocked when they appear on monitored computers.

A blocked hashes window appears where you can type the **SHA-1 hashes** in the text field below. If you clicked **Block** from the Detection details, Executables, Executable details, Loaded Modules, the SHA-1 hashes are prefilled.

Clean & quarantine file—If checked, file will be also deleted and quarantined in addition to a raised detection.

In the **Targets** window, click **Assign** to select groups or computers where you want block these hashes, and click **OK**.

In the **Confirmation** window you can see details of the blocked hashes. Check the box next to the hash to confirm blocking the hash and click **Block hashes**. The hashes are added to the list of blocked hashes.

Block Hashes From External Tools

The action of blocking executables in ESET Inspect can be achieved by calling REST API from script languages like Python. First, the user needs to log in to ESET Inspect Server by typing their username and password, and as a result, a token will be retrieved. Then the user can call the function for blocking hashes, giving the hash and previously received token. Here are the details of both REST calls:

Login request

Method: “PUT”

URL: “[server_address]/ FRONTEND/LOGIN”

Body: JSON object with fields:

“username”—string

“password”—string

Response:

As a result, the following token is received in response header “X-Security-Token”.

Ban hash request

Method: “PUT”

URL: “[server_address]/ FRONTEND/HASHES/BLOCK”

Body: JSON object with fields:

“sha1”—an array of strings with hexadecimal sha1 of executables which will be blocked (even one hash has to be in an array)

“shouldClean”—bool indicating if executables should be cleaned

“comment”—the string that will be displayed in ESET Inspect in a list of blocked hashes

Headers:

“Authorization”—string: “Bearer ” + token

Python code example:

```
import requests


# disable warnings caused by using requests with verify=False argument
requests.packages.urllib3.disable_warnings(requests.packages.urllib3.exceptions.Inse
cureRequestWarning)


# helper function to check request response; may raise Exception
def _check_response(res, error_message):
    if res.status_code != 200:
        message = "EI Server replied with: {0} ({1}).".format(res.status_code, res.r
eason)
        if error_message:
            message = "{0}. {1}".format(error_message, message)
        raise Exception(message)
```

```
def get_token(user, password, server_address, server_port):
    server = "https://{0}:{1}/".format(server_address, server_port)
    response = requests.put(server + "FRONTEND/LOGIN", verify=False,
                            json={"username": user, "password": password})
    _check_response(response, "Login failed")
    return {"server": server, "token": response.headers.get("X-Security-Token")}


def ban_hash(token, sha1, should_clean=True, comment=""):
    headers = {"Authorization": "Bearer {0}".format(token["token"])}
    response = requests.put(token["server"] + "FRONTEND/HASHES/BLOCK", headers=heade
rs, verify=False,
                            json={"sha1": [sha1], "shouldClean": should_clean, "comm
ent": comment})
    _check_response(response, "Ban hash failed")


token = get_token("More", "supersecretpassword", "localhost", 8889)
ban_hash(token, "1234567890abcdef1234567890abcdef12345678")
```

JavaScript code example:

```
function getConnection() {
    var http = new ActiveXObject("WinHttp.WinHttpRequest.5.1");
    // bypassing certificate error -
 set option WinHttpRequestOption_SslErrorIgnoreFlags(4)
    http.Option(4) = 0x1100;

    return http;
}


function checkResponse(res, errorMessage) {
    if (res.Status != 200) {
        var message = "EI Server replied with: " + res.Status + " (" + res.StatusTex
t + ")."
        if (errorMessage) {
            message = errorMessage + ". " + message;
        }
        throw new Error(message);
    }
}


function getToken(user, password, server_address, server_port) {
    var connection = getConnection();
    var server = "https://" + server_address + ":" + server_port + "/";

    connection.Open("PUT", server + "FRONTEND/LOGIN", false);

    var body = '{"username": "' + user + '", "password": "' + password + '"}';
    connection.Send(body);
    checkResponse(connection, "Login failed");
```

```
    return {token: connection.GetResponseHeader("X-Security-
Token"), server: server};
}


function banHash(token, sha1, shouldClean, comment) {
    var connection = getConnection();
    connection.Open("PUT", token.server + "FRONTEND/HASHES/BLOCK", false);

    connection.SetRequestHeader("Authorization", "Bearer " + token.token);

    var body = '{"sha1": ["' + sha1 + '"], "shouldClean": ' + shouldClean.toString()
 + ', "comment": "' + comment + '"}';
    connection.Send(body);

    checkResponse(connection, "Ban hash failed")
}


var token = getToken("More", "supersecretcode", "localhost", 8889);
banHash(token, "1234567890abcdef1234567890abcdef12345678", true, "")
```

Tasks

Enable you to rescan the database for a defined period with either newly added or adjusted detection rules. This means that whenever you adjust your security policy to define what is suspicious. You can easily trigger the re-scanning of your database to get a backward detection. This further improves the threat hunting capabilities, as you are not searching only for a specific IOC. Still, you searching for a complex definition of malicious behavior instead, emphasizing ESET's unique approach.

You can select all tasks by selecting the check box on the left side of the **Name**, or select task individually. Available actions:

Rerun tasks

- **Details**—Redirects you to the relevant section.
- **Detections**—You are redirected to the Detections tab.
- **Start**—Starts selected task.
- **Pause**—Pause selected task.
- **Duplicate query**—Duplicates selected task.
- **Delete**—Deletes selected task.
- **Rename**—Enables you to rename the search result for better distinguish.
- **Access group**—Displays currently assigned access group. Click **Move** to assign different access group.

• **Tags**—Used to tag the task. After choosing this option, new window for tag edition opens. In the Select field, you can type new tag or select already existing one.

• **Filter**—Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

Details

When you click the name of the task, the **Task Details** displays. Here you can find a summary of the task:
• **Name**—The name of the task.
• **Author**—The name of the user that was logged in at the time of the task creation.
• **Created**—The time when was the task created.
• **Status**—These four possible statuses are shown (Completed, Running, Paused or Pending - For performance reasons the maximum amount of running tasks at when is set to 10, so all other tasks over 10 have status pending. This limit will be configurable in the future releases).
• **Groups/Computers**—List of selected Groups/Computers
• **Time frame**—The time range of detections, that this task is executed on.
• **Detections**—The number of Detections that was triggered by this task.
• **Detection limit** - The limit of Detections that can be triggered by this task.
• **Rules**—The list of rules used in this task. If you click the rule name, you are redirected to the Rule details.
• **Note**—The note text for the task.
• **Comment**—The comment text for the task (if used; otherwise None).

Detections

This tab provides the same options as the main Detections tab. For the specific rule and except the button **Add to main table** will add selected detections to the main detection table in the Detections tab. After clicking on a Detection, you are redirected to its Detection details.

Create a **New task** and follow Create rerun task wizard.

Create rerun task

To create a new task, click **Tasks** > **New Task**. In the **Basics** section, type basic information about the task, such as a **Name** and **Note** (optional) for a more in-depth description of the task.

Click **Continue** to configure the task settings.

Rerun settings

• **Rerun rule(s) on selected targets**—Select the group of computers or individual computers on which you want to rerun the task.

• **Rerun evaluate events in time frame**—Select the time frame of events that you want to run the rerun task on.

• **Limit detections to**—Limit the number of detections that will appear in a rerun task result.

• **Add detections to the main detections table immediately**—Select the check box if you want the result detections to be moved to the main Detections tab list.

• **Ignore exclusions for this task**—Select the check box if you want the task to ignore/exclude detections that match rules picked from the next step of rerun task creation process.

Rules

Select rules that you want to rerun. Click **Add filter**, and select **Rule name** and type string to search. Each selected rule will be evaluated in a rerun tasks.

Summary

Review the summary of configured settings in **Task preview**. Verify all the settings for this task and click **Create task**.

Event Filters

This view shows the list of all event filters created in the Executables section. Event Filters are special rules in ESET Inspect determining which low-level events should not be stored in the database. The database size is proportional to the number of stored low-level events. By reducing the number of stored events, Event Filters help to lower the disk usage and improve performance.

Event Filters do not need to be used if ESET Inspect is configured to **Store only the most important data** or **Store data related directly to detections** in **More** > Settings.

The **Dashboard** > Events Load helps to find executables and computers that report most of the low-level events. Event filters can be created using the **Filter events** button on the Executable details page.

Filtering, Tags and Table options

Use filters at the top of the screen to refine the list of displayed items. Tags are also powerful when searching for a specific computer, detection, incident, executable, or script. Also you can click the gear icon for table options to manage the main table.

Click a filter name to take further actions:

Details	Go to the **Rule details** tab.
Edit Rule	Go to the Edit rule tab.
Change assignment	Go to the Targets view of the selected filter.
Enable	Enables selected filters.
Disable	Disables selected filters.
Delete	Deletes selected filters
Save As	Saves selected filters under the desired name.
Export	Starts the export process of the filter, depending on the used web browser. The format of the file is XML.

Details	Go to the Rule details tab.
Import	Opens the window for import the XML filter file. The following information is shown: • Total count of imported filters • Count of imported filters with correct syntax • Count of imported filters with incorrect syntax • Count of not imported filters
Tags	Assign tag(s) to an event filter from the list of existing, or create a new custom tag(s).
Filter	Quick filters, depending on the column where you activated the context menu (Show only this, Hide this).

There is an option to Filter Events through ESET PROTECT On-Prem policy, but this is deprecated, so we recommend not use this way anymore.

Events storage filter

Creating the event filter is the same as in Creating Exclusion, except for some differences. Instead of the Rules section, there is an Event types section:

- File system events
- TCP events
- Registry events
- HTTP events
- DNS events

Settings

Configure your ESET Inspect environment. ESET Inspect Database settings are available in the on-premises version only. No database maintenance is necessary for ESET Inspect.

Database retention

To prevent a database overload, you can use these options to clean logs regularly. The database cleanup process runs every night at midnight. If there is a problem with a cleanup process, a warning is displayed in the Questions view, and failed purge is displayed in the Events load view.
Store low-level data for—Choose the interval database clean-up (events and processes records), or click **Invoke purge** for immediate clean-up.
Store detections for—Choose the interval database clean-up (detections and executables records), or click **Invoke purge** for immediate clean-up.

Database collection

Provides the same options as during the ESET Inspect Server installation process on the Data Collection window. Use pre-defined options or the **Advanced** button to choose which data you want to store.

Database performance

Number of threads writing to database—Set the number of cores to increase the performance, making your ESET Inspect Server more efficient. according to this formula: *1.5x the number of physical cores of your server running the ESET Inspect Database*.

Search engines integration

Add preferred search engine for executables hashes.

Rule learning mode

Click **Enable** for notification window with details.

ESET Inspect Web Console certificate

Change the certificate used for ESET Inspect Web Console communication with ESET Inspect Server.

Server certificate

Select the certificate used for communication between ESET Inspect Connector and ESET Inspect Server.

HTTP Proxy

To use HTTP proxy specify server settings.

Miscellaneous

Set the ESET Inspect instance name that will be displayed in a web browser tab (page title). You can use emoji in the instance name.

Remote Access Connector

Enable if you want to provide remote access to the ESET Inspect Web Console to the ESET Support team. Keep the link safe from misuse by an unauthorized person.

Ensure the ESET Inspect Server allows TCP outbound connection on ports 443 and 5671.

Logging

Choose preferred Trace log verbosity to determine the level of information collected and logged. Alternatively, use ESET PROTECT On-Prem policy to achieve the same logging.

Product Improvement Program

Select the check box if you want to automatically send crash reports and Telemetry data to ESET.

User settings

To access the user settings, click your username next to the **Log out**.

Theme settings

Choose preferred color theme. You have three options:
Default (light) theme
Dark theme
System color theme—Based on the system preferences, either **Default (light) theme** or **Dark theme** will be chosen.

Audit log

Tracks changes in configuration or protection. Audit logs are created if a ESET Inspect Web Console object (rules, detections, executable details) is created or modified. The Audit log enables the Administrator to inspect the activities performed in the ESET Inspect Web Console, especially if there are more Web Console users.

Click **Add filter** and select a filter type from the drop-down menu or type a string. Also you can click the gear icon for table options to manage the main table.

Timestamp	Set the period (date and time).
Action	Select one of the available actions.
Statuses	Select the action result (Failure, Forbidden and Success).
User	Select the user who performed changes.
Section	Select one of the available sections.
Open Secondary Object	Provides detailed view of secondary object (if available).
Display Absolute/Relative Time	Absolute time will show the time in format DD/MM/YYYY HH:MM:SS. Relative time will show the time in the format minutes/hours/months concerning present time, like 15 minutes ago or six days ago.

REST API

API is based on the JSON format.

Authentication

HTTP request:

```
PUT api/v1/authenticate

POST api/v1/authenticate
```

Both commands work the same.

URL query: None

Request body: JSON object with username, password and domain fields

Response Header: X-Security-Token

Example:

```
import json

import requests

import warnings
```

```
warnings.filterwarnings('ignore')


EEI_USER = "Administrator" # Use your credentials here

EEI_PASSWORD = "admin123"

EEI_SERVER = 'localhost'


response = requests.put(f"https://{EEI_SERVER}/api/v1/authenticate", json.dumps({"us
ername": EEI_USER, "password": EEI_PASSWORD, "domain":False}), verify=False)

if response.status_code == 200:

    session = requests.Session()

    session.headers={"Authorization": f"Bearer {response.headers['X-Security-
Token']}"}

    session.verify=False


    UNRESOLVED_FILTER = "resolved eq 0"

    response = session.get(f"https://{EEI_SERVER}/api/v1/detections", params={"$coun
t": 1, "$filter": UNRESOLVED_FILTER})

    count = response.json()["count"]


    PAGE_SIZE = 100

    for i in range(0, count, PAGE_SIZE):

        response = session.get(f"https://{EEI_SERVER}/api/v1/detections", params ={"
$skip": i, "$top": PAGE_SIZE, "$filter": UNRESOLVED_FILTER})

        detections = response.json()["value"]

        for d in detections:

            print(d)
```

REST API Detections

List of detections

HTTP request:

```
GET api/v1/detections
```

URL query:

Pagination:

`$top`	Request the number of items in the queried collection included in the result.
`$skip`	Request the number of items in the queried collection to be skipped and excluded from the result.
`$count`	Enable clients to request a count of the matching resources included with the resources in the response. If set to $count=1, the number of detections is returned.

Sorting:

`$orderBy`	Enable clients to request resources in ascending order using `$orderBy=asc` or descending order using `$orderBy=desc`. The default order is ascending.

Filtering:

`$filter`	Enable clients to filter resources addressed by a request URL. The query supports the following operators `eq, ne, gt, ge, lt, le, and, or`, and `()`. Combine operators with values to filter data. For instance, resolved eq 0 will report unresolved detections.

Example:

✔ `GET api/v1/detections?$skip=100&$orderBy=creationTime desc`

For other examples, follow System Query Options

Request header: Authorization token

Request body: none

Response: JSON object with the following properties:

Value	Description
`computerId`	Unique identifier of a computer in ESET Inspect Database
`computerName`	The computer's name that raised the detection
`computerUuid`	Unique identifier of a computer in ESET Inspect Database
`creationTime`	Time of the detection
`id`	Unique identifier of detection in ESET Inspect Database
`moduleId`	Unique identifier of the executable in ESET Inspect Database
`moduleLgAge`	Number of days visible in the LiveGrid®
`moduleLgPopularity`	How many computers reported an executable to LiveGrid®
`moduleLgReputation`	LiveGrid® reputation is a number from 1 to 9, indicating how safe the file is. 1-2 Red is malicious, 3-7 Yellow is suspicious, 8-9 Green is safe
`moduleName`	The executable that triggered the detection
`moduleSha1`	The hash of the executable that triggered the detection

Value	Description
`moduleSignatureType`	Inform if the file is signed or not, and how it is signed. Based on its return value: 90 = Trusted 80 = Valid 75 = AdHoc 70 = None 60= Invalid
`moduleSigner`	The file's signer (if signed).
`note`	If available, show a note.
`priority`	The detection's priority (default 0, otherwise set by ESET Inspect Administrator)
`processCommandLine`	Show the argument used with the command
`processId`	Unique identifier of a process in ESET Inspect Database
`processUser`	The user account logged on to the computer at the time of a detection trigger
`processCommandLine`	The argument used with the command
`processId`	Unique identifier of a process in ESET Inspect Database
`processUser`	The user account logged on to the computer at the time of a detection trigger
`resolved`	True/false depends if the user marked the detection as resolved
`ruleName`	The name of the rule that triggered the detection
`ruleId`	A rule's integer ID
`ruleUuid`	A rule's Uuid ID
`severity`	The detection's severity
`severityScore`	A more precise severity definition. 1–39 > Info 40–69 > Warning 70–100 > Threat
`threatName`	The threat's name, that can be found in this list http://www.virusradar.com/en/threat_encyclopaedia
`threatUri`	The URI (uniform resource identifier) that caused the detection to trigger
`type`	ESET type of the detections: UnknownAlarm = 0 RuleActivated = 1 rule based detection MalwareFoundOnDisk = 2 malware found on disk by Endpoint MalwareFoundInMemory = 3 malware found in memory by Endpoint ExploitDetected = 4 exploit detected by Endpoint FirewallDetection = 5 BlockedAddress = 7 URL blocked by firewall CryptoBlockerDetection = 8 cryptoBlocker detection
`uuid`	A detection's unique identifier.

List of detections - filtering

URL query:

`$filter`	Allows the user to filter detections with an expression built from: Fields: `id, resolved, creationTime` Operators: `eq, ne, gt, ge, lt, le, and, or`, and `()`

Example:

```
GET api/v1/detections?$filter=resolved eq false and creationTime ge 2020-01-20T20:11
:00Z
```

Get detection details

HTTP request:

```
GET api/v1/detections/{id}
```

URL query:

`$idType`	if `$idType=sha1 {id}` in URL is interpreted as sha1 of a module

Request header: Authorization token

Request body: none

Response: JSON object with detection data:

`computerId`	Unique identifier of a computer in ESET Inspect Database
`computerName`	Displays the computer's name that raised the detection
`computerUuid`	Unique identifier of a computer in ESET Inspect Database
`creationTime`	The time of the detection
`handled`	Shows whether an action was taken against this detection
`id`	Unique identifier of detection in ESET Inspect Database
`moduleFirstSeenLocally`	When an executable was first seen on any computer
`moduleId`	Unique identifier of the executable in ESET Inspect Database
`moduleLastExecutedLocally`	When the executable executed last time on any computer
`moduleLgAge`	Number of days visible in the LiveGrid®
`moduleLgPopularity`	How many computers reported an executable to LiveGrid®
`moduleLgReputation`	LiveGrid® reputation is a number from 1 to 9, indicating the file's safety . 1-2 Red is malicious, 3-7 Yellow is suspicious, 8-9 Green is safe
`moduleName`	The executable that triggered the detection.
`moduleSha1`	The hash of the executable that triggered the detection
`moduleSignatureType`	Informs if the file is signed or not and how it is signed. (Trusted/Valid/None/Invalid/Unknown)
`moduleSigner`	The file's signer (if signed).
`note`	If available, shows a comment.
`priority`	The detection's priority(default 0, otherwise set by the ESET Inspect Administrator)
`processCommandLine`	The argument used with the command
`processId`	A process's unique identifier in the ESET Inspect Database
`processPath`	The disk path where the executable is located
`processUser`	The user account that was logged on the computer at the time of the detection trigger

`resolved`	True/false depends if the user marked the detection as resolved
`ruleName`	The rule's name that triggered the detection
`ruleId`	A rule's integer id
`ruleUuid`	A rule's uuid id
`severity`	The detection's severity.
`severityScore`	A more precise severity definition. 1-39 > Info 40-69 > Warning 70 - 100 > Threat
`threatName`	The threat's name found in this list http://www.virusradar.com/en/threat_encyclopaedia
`threatUri`	The URI (uniform resource identifier) that caused the detection to trigger
`type`	ESET type of the detections: UnknownAlarm = 0 RuleActivated = 1 - rule based detection MalwareFoundOnDisk = 2 - malware found on disk by Endpoint MalwareFoundInMemory = 3 - malware found in memory by Endpoint ExploitDetected = 4 - exploit detected by Endpoint FirewallDetection = 5 BlockedAddress = 7 - url blocked by firewall CryptoBlockerDetection = 8 - cryptoBlocker detection
`uuid`	A detection's unique identifier.

Update detection

HTTP request:

```
PATCH api/v1/detections/{id}
```

URL query:

`$idType`	if `$idType=sha1 {id}` in URL is interpreted as sha1 of a module

Request header: Authorization token

Request body: JSON object with the following properties:

`resolved`	When set to true, the detection is marked as resolved
`priority`	
`note`	Enable to add a note

REST API Response

Allow the user to block / unblock an executable and kill running processes:

HTTP request:

```
POST api/v1/executables/{id}/block
```

```
POST api/v1/executables/{id}/unblock
```

URL query:

`$idType`	if `$idType=sha1 {id}` in URL is interpreted as sha1 of a module

Request header: Authorization token

Request body: JSON object with the following properties:

`clean`	When set to true, running processes will be killed, and the module moved to the quarantine
`note`	Enable adding a note

These properties are effective only when blocking.

POST - Updates machine's state

HTTP request:

`POST api/v1/machines/{computerId}/isolate`	Isolate the computer from the network
`POST api/v1/machines/{computerId}/integrate`	Reconnect the computer to the network

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as uuid of a rule

Request: none

Response: none

POST - Updates machine's state

HTTP request:

`POST api/v1/machines/{processId}/kill`	Kills the specific process if available

Request: none

Response: none

REST API Rules

URL api/v1/rules support the following HTTP verbs:

POST - Creates a new rule

HTTP request:

```
POST api/v1/rules
```

Request header: Authorization token

Request body: The new rule's XML

Response: 201 HTTP Code and HTTP Location header contains URL to `GET` request with ID to newly created rule (for example, *HTTP://<<SERVER_NAME>>/api/v1/rules/121* where 121 is the new rule's ID). Response body returns JSON with newly created rules object. This JSON is identical to the response to `GET`.

Invalid rules are not saved.

GET - Lists rules

HTTP request:

```
GET api/v1/rules
```

Request header: Authorization token

Request body: none

Similarly to how API gets detections supports `$top, $skip, $count, $orderBy` in the URL.

Request body: none

Response: JSON object fields: value and count (only if `$count` is present in the URL query). The value field contains an array of objects with the following fields:

```
id
```

```
name
```

```
enabled
```

```
severity
```

```
severityScore
```

GET - Gets a single rule

HTTP request:

```
GET api/v1/rules/{id}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as uuid of a rule

Request header: Authorization token

Request body: none

Response: Besides fields returned by the rules listing, the response should have a “rule” field with rule's XML.

PUT - Edits rule body

HTTP request:

```
PUT api/v1/rules/{id}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as uuid of a rule

Request header: Authorization token

Request body: The rule's new XML.

Response: Returns an updated object from requests. Similar to `POST`, returns a `GET` response.

DELETE - Deletes a rule

HTTP request:

```
DELETE api/v1/rules/{id}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as rule's uuid.

Request header: Authorization token

Request body: none

Response body: none

PATCH - Updates specific rule

HTTP request:

```
PATCH api/v1/rules/{ruleId}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as rule's uuid.

JSON request body:

`enabled`	(bool) value true (1) to enable, false (0) to disable

Request header: Authorization token

Response body: none

Enables/disables a specific rule

If successful, returns a 204 code

All requests require an authorization token in the header.

REST API Exclusions

POST – Creates a new exclusion

HTTP request:

```
POST api/v1/exclusions
```

JSON request body:

`body`	(string) - a new exclusion's XML
`autoResolve`	(bool) - whether to resolve a detection automatically or not
`name`	(string) - an exclusion's name.
`ruleIds`	(array) - an array of rule ids (uuids as strings); can be used simultaneously with ruleIds
`ruleUuids`	(array) - an array of rule ids (integers); can be used simultaneously with ruleUuids
`note`	(optional, string) - up to 2048 characters stored in the note section

JSON response body:

success	201 HTTP Code and HTTP Location. The header contains the URL for `GET` request with ID for the newly created exclusion. Response body returns JSON with the newly created exclusion object
failure	404 HTTP Code with body explanation

Invalid exclusions are not stored in the ESET Inspect Database.

GET – List exclusions

HTTP request:

```
GET api/v1/exclusions
```

URL query:

Similar to API for getting detections, supports: `$top, $skip, $count, $orderBy`

Request body: none

JSON response body: Value and count (only if `$count` is present in the URL query). The value field contains an array of objects with the following fields:

`id`

`uuid`

`name`

`enabled`

`note`

GET – Gets a single exclusion

HTTP request:

```
GET api/v1/exclusions/{exclusionId}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as a rule's uuid

Request body: none

JSON response body: Apart from fields returned by the exclusions listing, the response will contain the “exclusion” field with XML:

`body (xml)`

`id`

`uuid`

`name`

`enabled`

`note`

`ruleIds (integers)`

`ruleUuids (uuids as strings)`

PUT – Edits exclusion body

HTTP request:

```
PUT api/v1/exclusions/{exclusionId}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as uuid of a rule

JSON Request body: same as for POST new exclusion.

JSON response body: returns updated object from requests. Similar to a `POST`, returns `GET` response.

DELETE – Deletes an exclusion

HTTP request:

```
DELETE api/v1/exclusions/{exclusionId}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as a rule's uuid.

Request body: none

Response body: none

GET – Get exclusions associated with a rule

HTTP request:

```
GET api/v1/exclusions/rule/{ruleId}
```

URL query:

`$idType`	if `$idType=uuid {id}` in URL is interpreted as a rule's uuid

Request body: none

JSON response body: Same as for GET – List exclusions. Returns an array of exclusions associated with a rule.

Example:

```
https://192.168.197.200/api/v1/executables/066F8964A44161825BE6F4E10B05CD66F3C115FC/block?$idType=sha1
which is eq with https://192.168.197.200/api/v1/executables/1605/block (so id = sha1 or ID of module
in database)
```

Rules guide

A rule is defined using XML-based language.

Rules are matched on the server. They have matched asynchronously, so there can be a small delay between when recent events are sent from client to server and processed by rules. A matched rule triggers associated actions and notifies a security engineer by raising a detection. The detection is displayed in the Detections view, but it is also exported to ESET PROTECT On-Prem (or SIEM), or an email can be automatically sent when the detection is triggered.

Link to the Rules Guide is available below the **Syntax Reference** on the right side.