

# ESET Tech Center

Knowledgebase > ESET PROTECT On-prem > Migrate exclusions from ESET Inspect on-premises to ESET Inspect Cloud

## Migrate exclusions from ESET Inspect on-premises to ESET Inspect Cloud

Lesley | ESET Nederland - 2022-10-24 - Comments (0) - ESET PROTECT On-prem

### Issue

- You want to migrate customized settings from ESET Inspect on-premises to ESET Inspect Cloud
- [Export Exclusions](#)
- [Export Event Filters](#)
- [Export Any Custom Rules](#)
- [Blocked Hashes](#)

### Solution

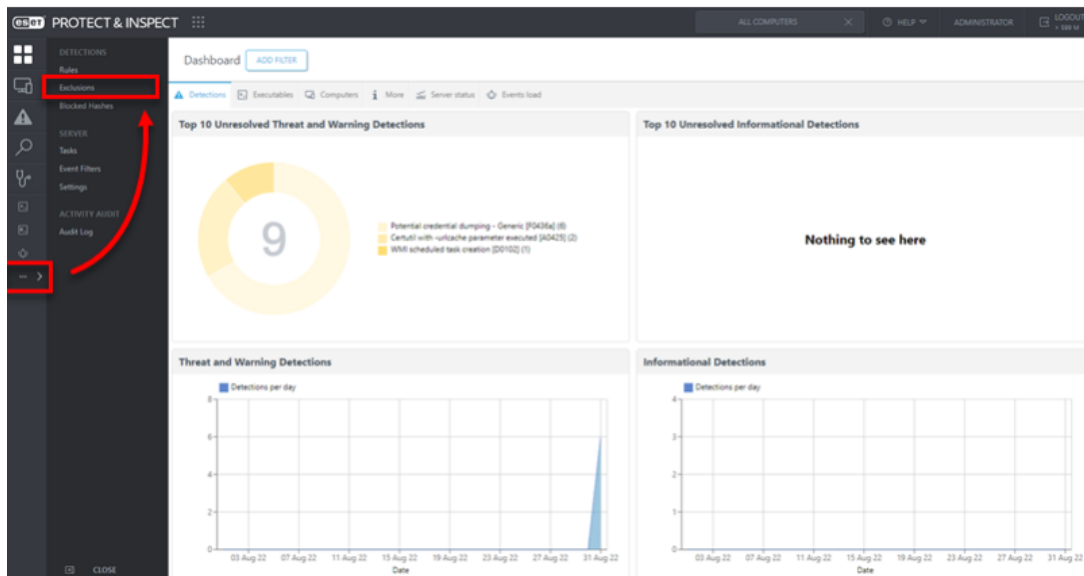


ESET Security Services for ESET Inspect and ESET Inspect Cloud

ESET offers various [security service packages and additional support](#) for these products. Support for ESET Inspect on-premises and ESET Inspect Cloud is limited and managing rules or exclusions are not included without an ESET Security Service package. Contact a sales representative for further assistance.


### Export Exclusions

1. Click **More** → **Exclusions**.




2. Remove all filters, select the check box next to **Name** and click **Export**.

The screenshot shows the 'Admin' page in ESET Protect & Inspect. The 'Exclusions' tab is active, displaying a table of exclusion rules. The 'Name' column header is highlighted with a red box. A red arrow points from this box to the 'Export' button located at the bottom right of the table. The table contains various exclusion rules with columns for Name, Author, Creation Date, Enabled status, Criteria, and Rules Names.


 Add recommended exclusions to ESET Inspect Cloud  
[See our Knowledgebase article](#) to view the additional exclusions we recommend adding in ESET Inspect Cloud.

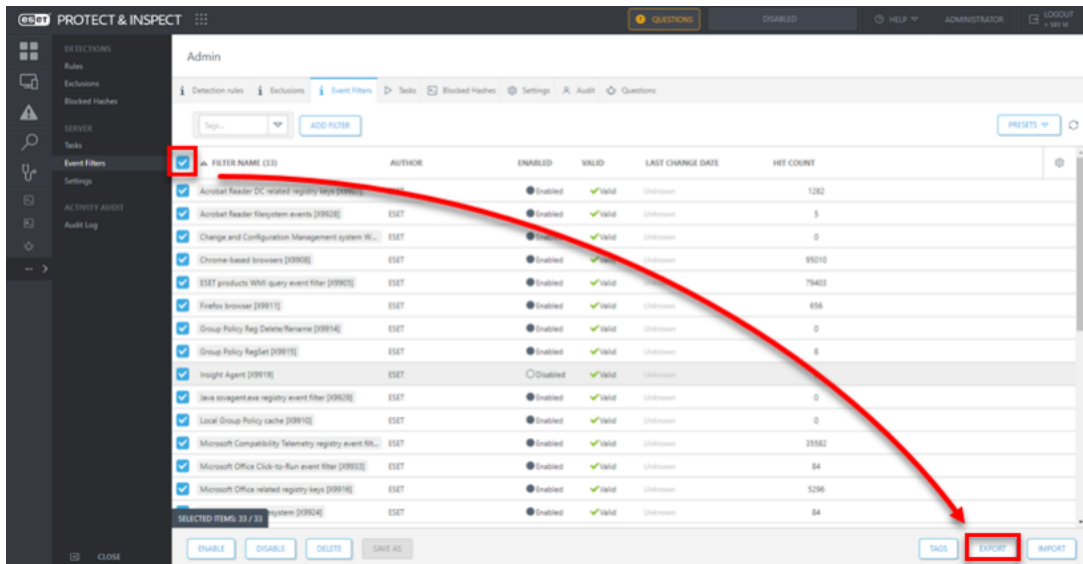
## Export event filter as backup


**Export as a backup only**  
 Event filters can only be exported as a backup and will not import into ESET inspect Cloud

1. Click **More** → **Event Filters**.

The screenshot shows the 'Dashboard' page in ESET Protect & Inspect. The left sidebar has 'Event Filters' highlighted with a red box. A red arrow points from this box to the 'Event Filters' section of the dashboard. The dashboard displays 'Top 10 Unresolved Threat and Warning Detections' with a donut chart showing 9 detections. Below this are two line charts: 'Threat and Warning Detections' and 'Informational Detections', both showing 'Detections per day' over time.

2. Remove all filters, select the check box next to **Name** and click **Export**.



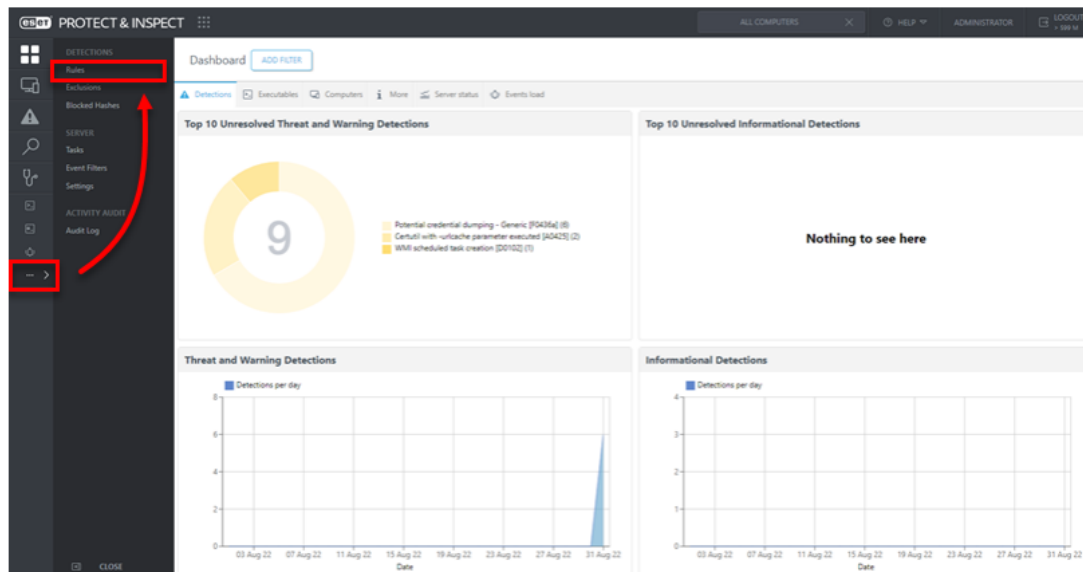
## Export Any Custom Rules



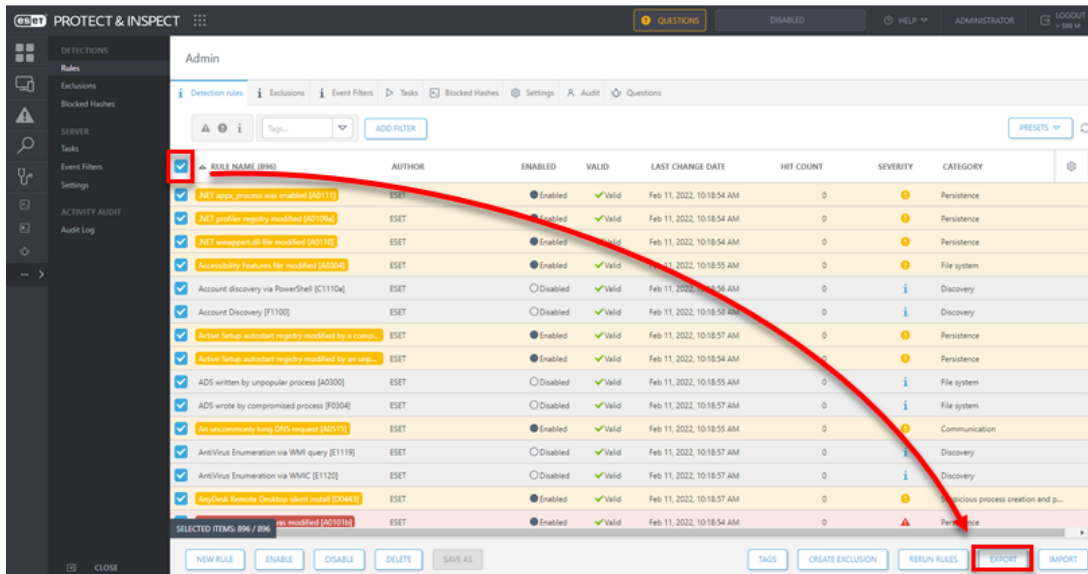
Only export custom rules

We recommend only exporting custom rules that were created by the user.

1. Click **More** → **Rules**.

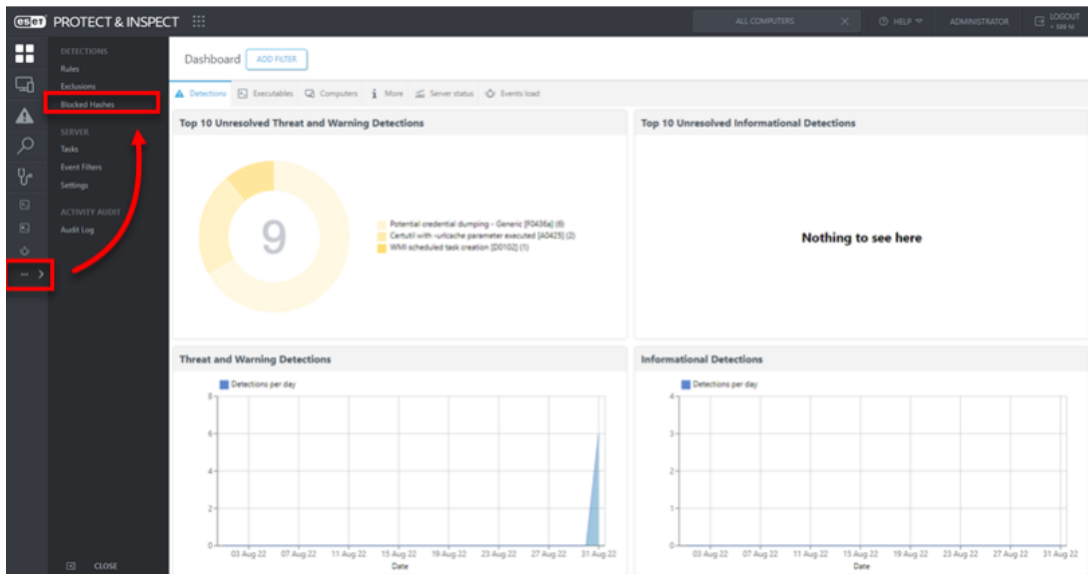


2. Filter for **Author isNot ESET**, select the check box next to **Name** and click **Export**.



## Blocked Hashes

1. Click **More** → **Blocked Hashes**.



2. Any blocked hashes must be manually copied over to ESET Inspect Cloud.

The screenshot shows the 'Admin' interface for 'Blocked Hashes'. The table contains the following data:

NAME (2)	SHA-1	CLEANED	REPUTATION (LIVEGRID#)	POPULARITY (LIVEGRID#)	FIRST SEEN (LIVEGRID#)	SIGNATURE
<input checked="" type="checkbox"/> C:\comul.exe		<input checked="" type="radio"/> Yes	★★★★★	★★★★★	6 months ago	Trusted
<input checked="" type="checkbox"/> C:\programdata.exe		<input checked="" type="radio"/> Yes	★★★★★	★★★★★	6 months ago	Trusted



**ESET Security Services for ESET Inspect and ESET Inspect Cloud**

ESET offers various [security service packages and additional support](#) for these products. Support for ESET Inspect on-premises and ESET Inspect Cloud is limited and managing rules or exclusions are not included without an ESET Security Service package. Contact a sales representative for further assistance.