ESET Tech Center

What's new in ESET PROTECT (v8)

Steef | ESET Nederland - 2020-12-09 - Reacties (0) - ESET PROTECT

The new ESET PROTECT platform replaces ESET Security Management Center (v7)

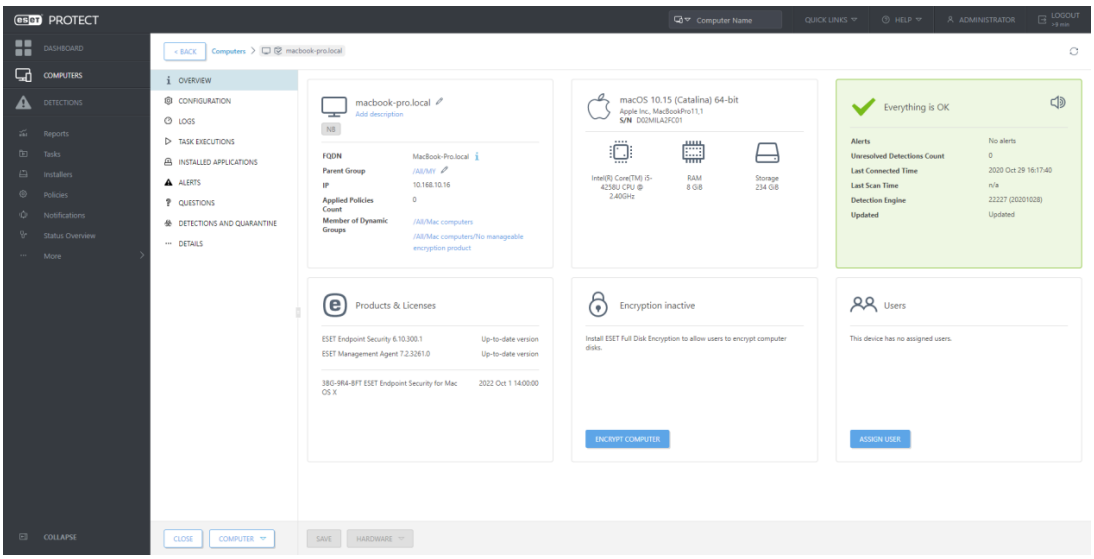
What's new in ESET PROTECT

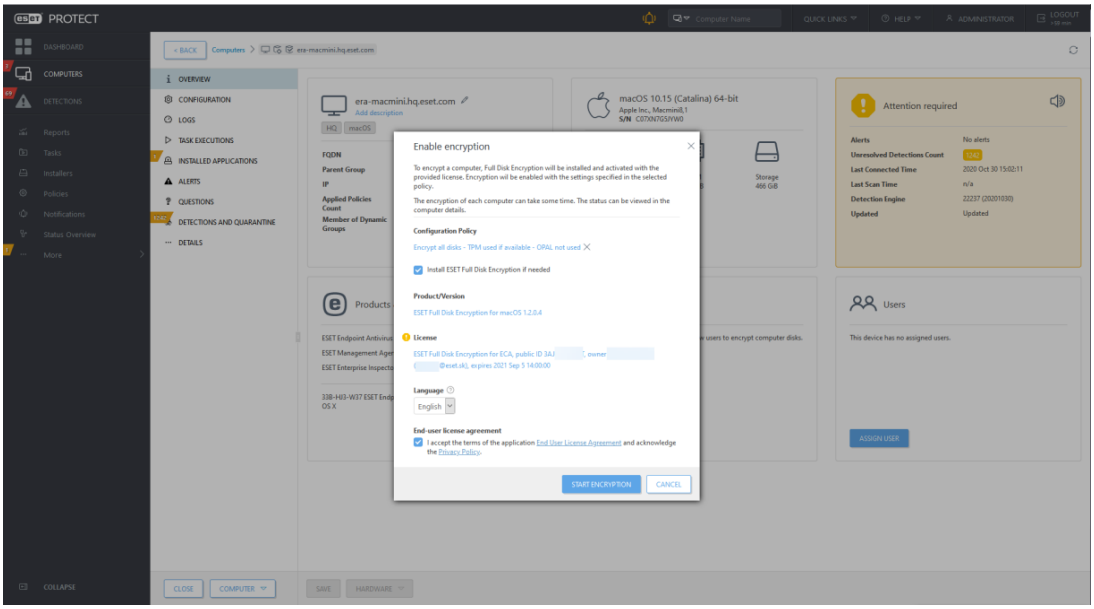
ESET Full Disk Encryption now also for macOS

ESET Full Disk Encryption is an add-on feature natively integrated into ESET remote management consoles – ESET PROTECT and ESET PROTECT Cloud (cloud console). It allows admins to deploy, activate and encrypt endpoints via one-click action, after which they can monitor and manage the encryption status of data stored on connected endpoints from a single console. ESET Full Disk Encryption significantly increases the organization's data security and helps comply with GDPR and other regulations. The client's side requires minimal user interaction and user training, reducing to a minimum the time needed to implement encryption across your entire organization.

We have extended platform coverage, and now it is possible to encrypt disks not only on Windows but also on Mac computers where we are leveraging native FileVault technology and centralizing management under ESET PROTECT 8.0

> Use case: The Administrator wants to prevent stealing and abusing company data in case of losing or device theft. The Administrator wants to encrypt Windows devices as well as macOS devices.

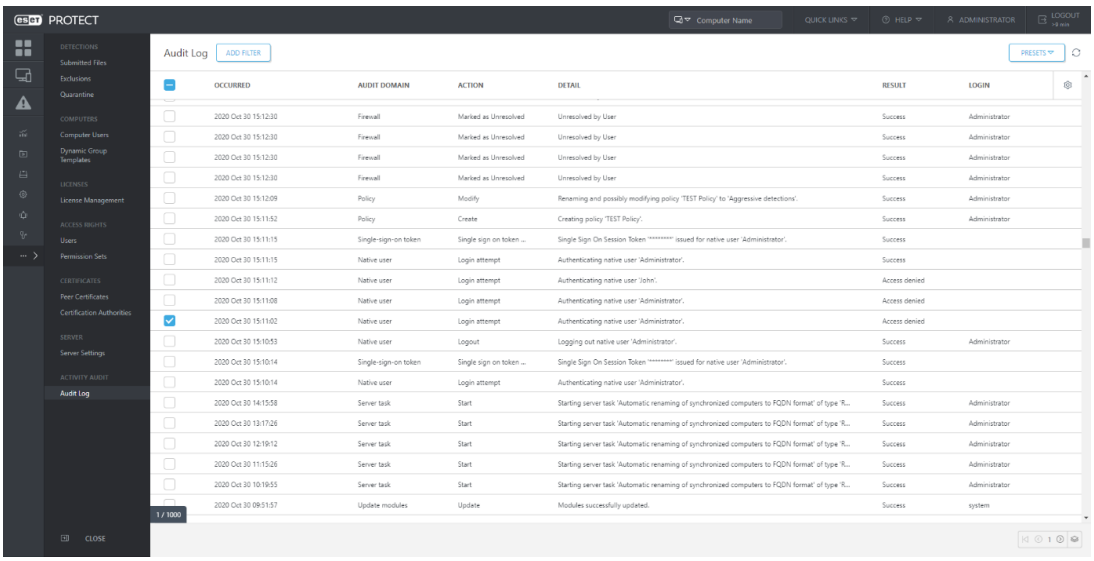




Back to top

Audit Log

With this feature, we are moving console user management in multi-tenant deployments or larger companies with multiple administrators to the next level. The Audit Log helps identify what was done with the object, when and by whom. The Administrator can easily navigate to this section also from the context menu over Detections, Users, Computers, and other objects like Task or Policies.



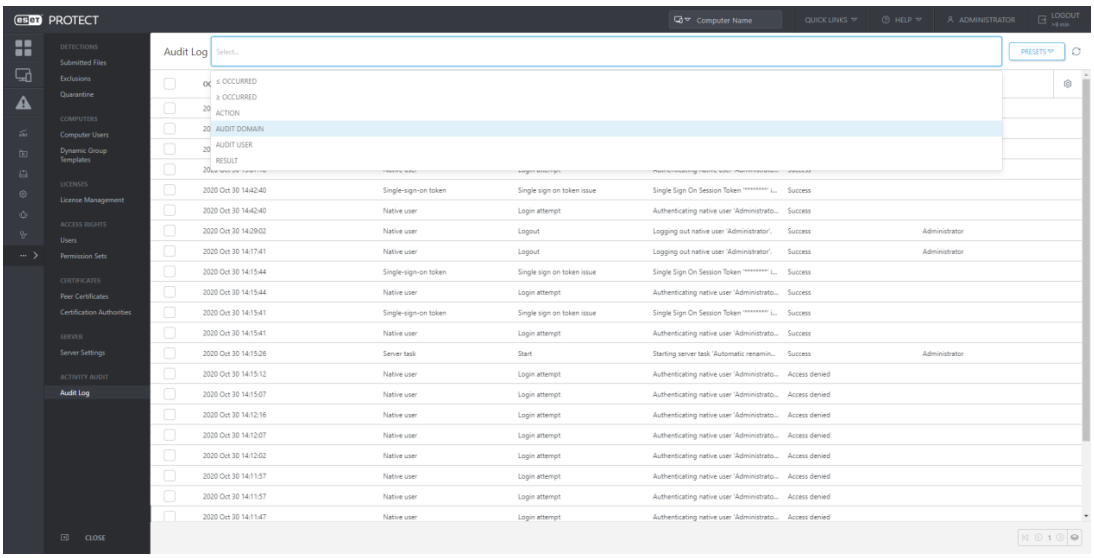
Use case 1: The Administrator wants to know who changed the policy affecting the security setting on endpoints.
Use case 2: The Administrator wants to know who has tried to log-in to the console with the wrong password (“Access denied”).
Use case 3: The Administrator wants to know who and when marked the particular detection as resolved.
Use case 4: The Administrator wants to who and when has performed a scanning task over the particular machine.

When a user performs an action in the ESET PROTECT Web Console, the action is logged. Audit logs are created if an ESET PROTECT Web Console object (computer, policy, detection, etc.) is created or modified.

The Audit Log is a new screen available in the ESET PROTECT. The Audit Log contains the same information as the Audit log report, but it allows convenient filtering of the displayed data. In addition, you can directly view the filtered audit log for various Web Console objects by clicking on the object in the Web Console and selecting “Audit Log”.

Auditing allows the Administrator to have an overview of activities performed in the ESET PROTECT Web Console, especially if there are more Web Console users.

In the dedicated “Auditing” section, the Administrator can filter audit information according to their needs:



ESET PROTECT supports these Audit Domains:

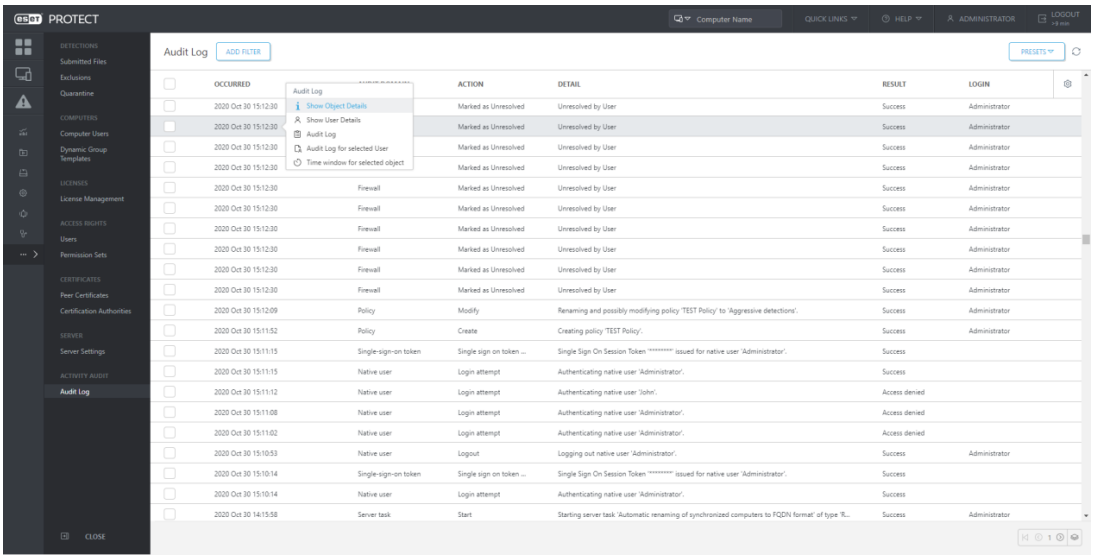
- Certificate
- Certificate revocation
- Certification authority
- Client task
- Client trigger
- Computer
- Configuration
- Dashboards
- Domain group
- Dynamic group
- Dynamic group template
- Email
- End User License Agreement
- Enrollment token
- Enterprise Inspector
- Exclusion
- Full disk encryption recovery
- License
- Native user
- Notification
- Permission set
- Policy
- Report template
- Report template category
- Repository
- Server
- Server task
- Server trigger
- Server trigger task relation
- Static group
- Stored installer
- Update modules
- User
- User group
- User to computer relation

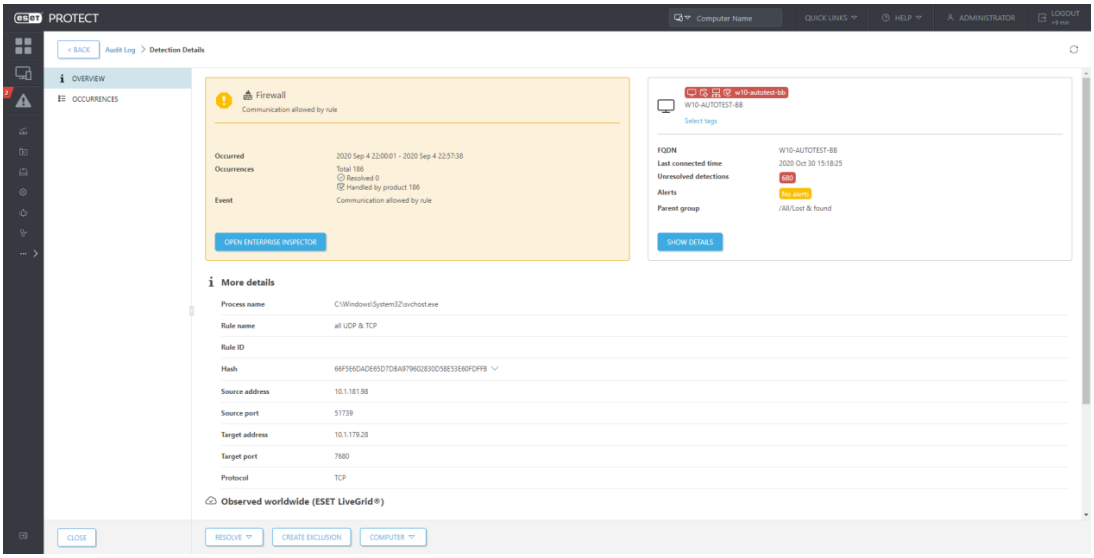
Click on the line in Auditing and you can perform the following actions:

Show Object Details	Show the details of the audited object

Show User Details	Show details of the user who performed the action on the object
Audit Log	Show the Audit Log for the selected object
Audit Log for selected user	Show the Audit Log for the selected user
Time window for selected object	Show the Audit Log for the selected object with an activated filter of time occurrence

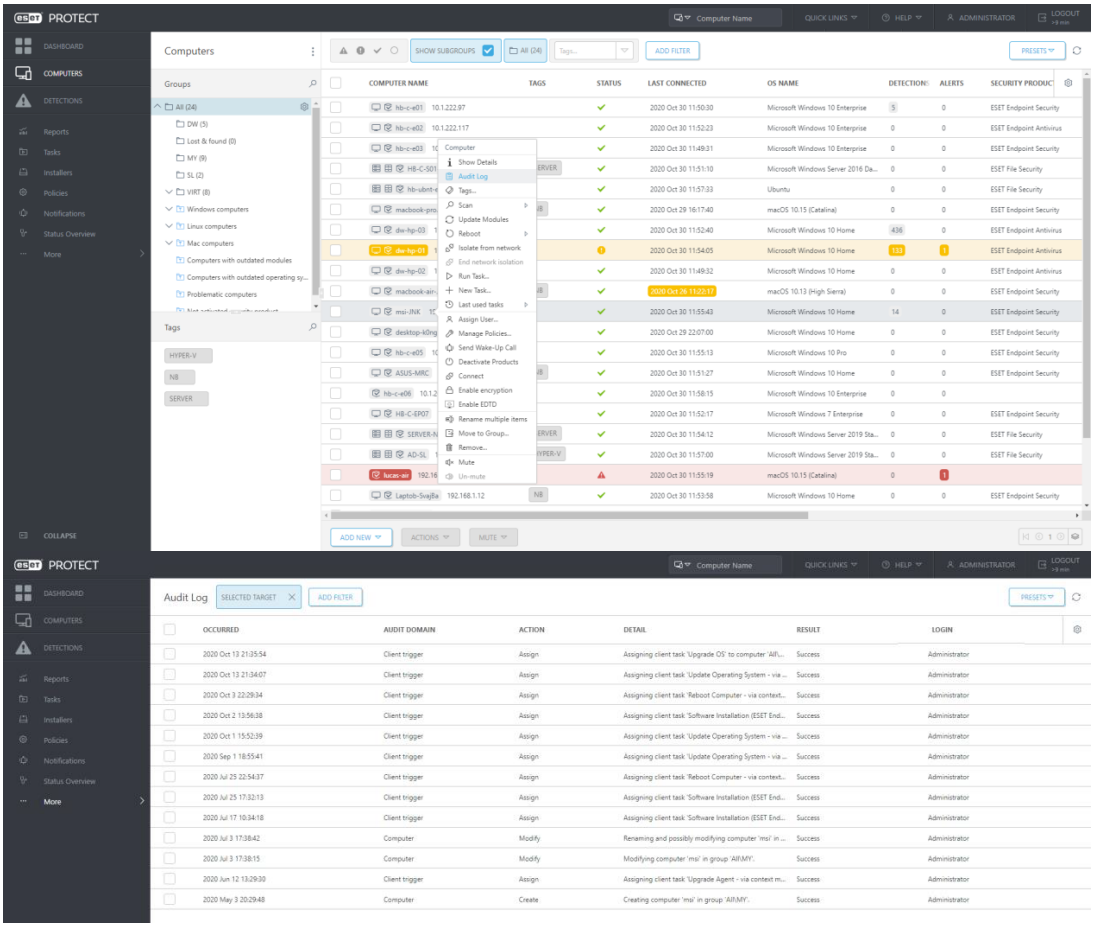
From the Audit Log section Administrator can easily navigate to the proper object:



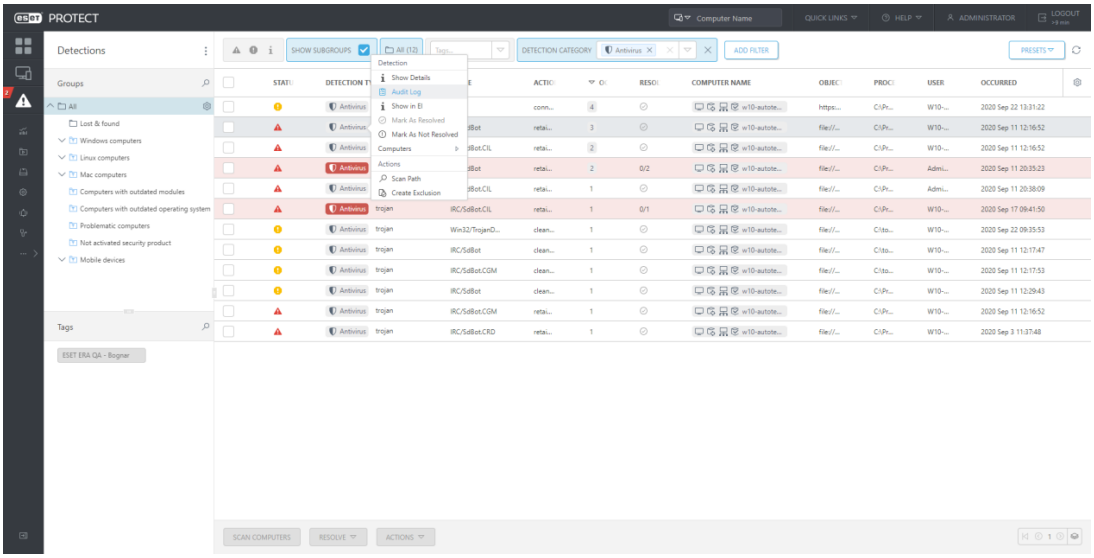


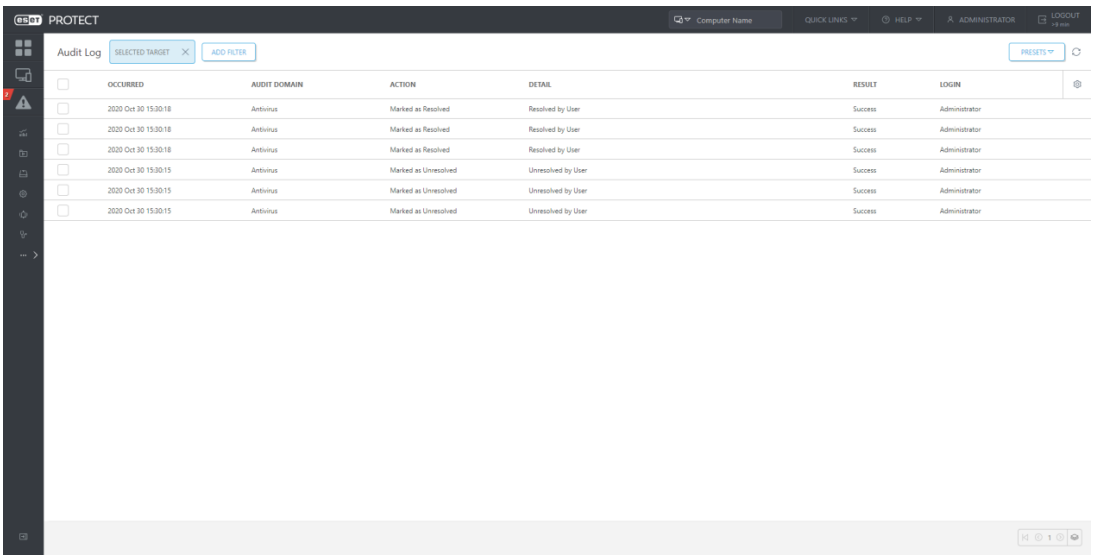
Useful is the context menu action over objects, which navigates the Administrator to the Auditing section.

From Computers:

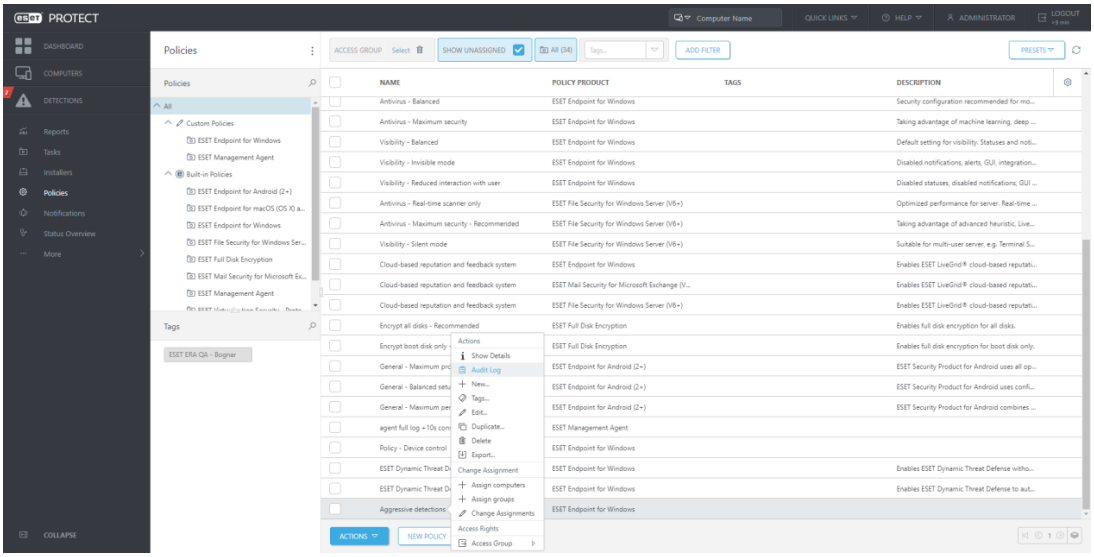


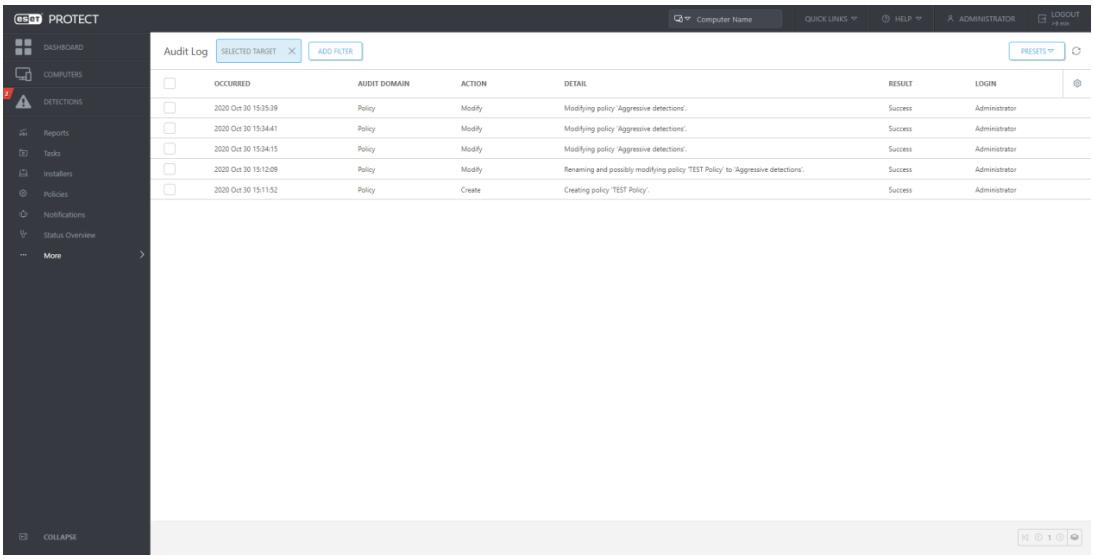
From Detections:





From Policies:





[Back to top]

Improved Exclusions

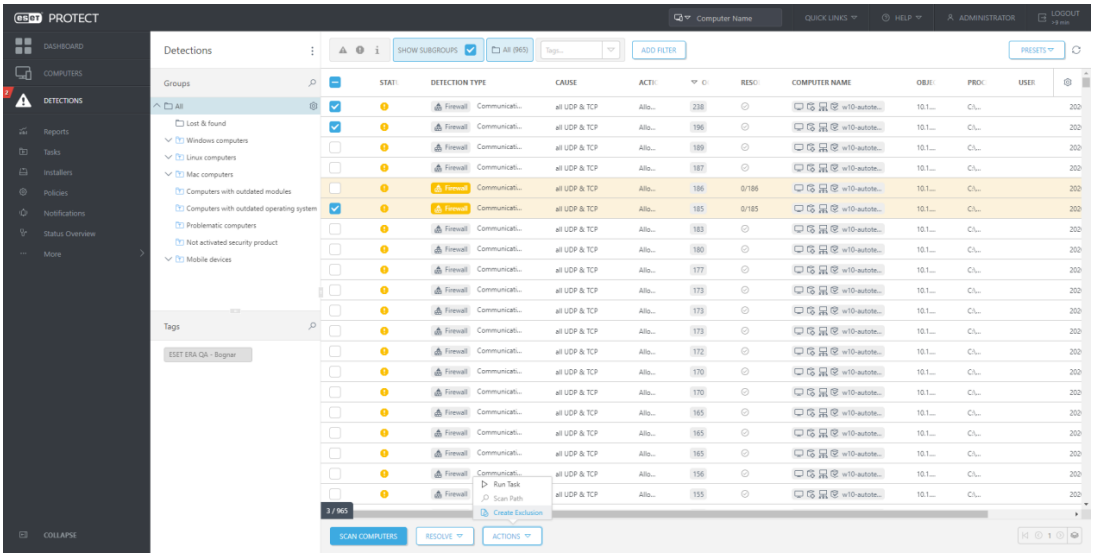
To improve the detection quality of our products by adding the possibility to set sensitivity in "Real-time & Machine Learning Protection" locally in customer-installed products, we also need to address the potentially higher rate of false positives. This is addressed by an "exclusion creation workflow" that considers the broader context of the detection and recommends or pre-selects the relevant exclusion criteria. Exclusions are displayed in a dedicated window.

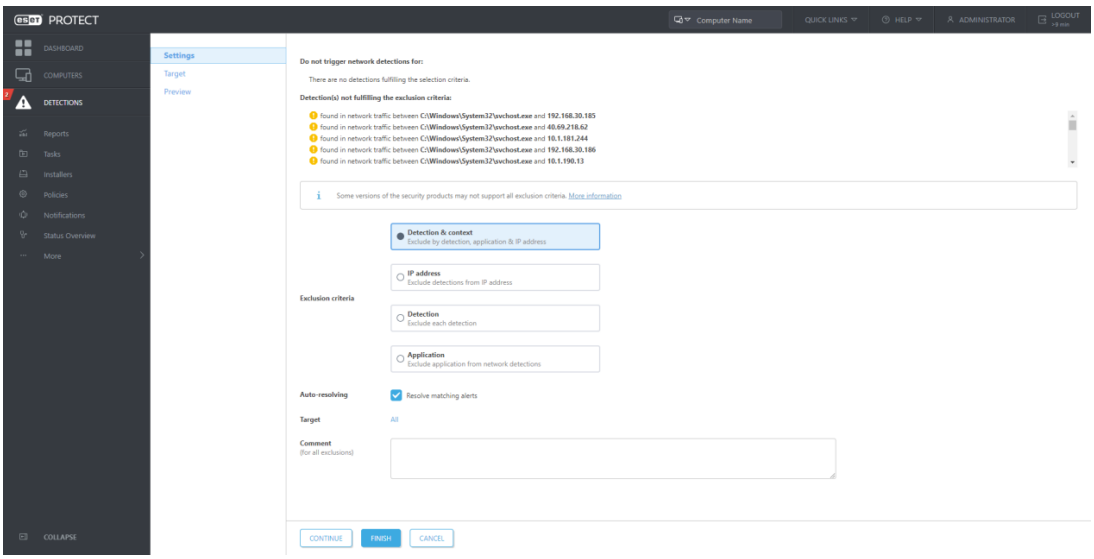
You can create an exclusion using a new Wizard by performing the following actions:

- Create multiple exclusions at once
- Specify the exclusion based on the recommended set of criteria (for example, not exclude ML detection by detection name because that would disable the ML engine entirely)
- See the affected detections that will be suppressed by the created exclusion (not only the one entry but all of them that exist in the DB)
- Trigger that resolves all of the affected detections

In ESET PROTECT 8.0, we have improved this mechanism even more, and now it is possible to exclude also firewall threats. It is very helpful because some applications, otherwise trustworthy from the admin's perspective, may generate large amounts of alerts when trying to connect to a specific IP address. With ESET PROTECT, you can easily exclude such communication to avoid a vast amount of false positives.

> Use case 1: The Administrator of the company which develops games would like to easily avoid future detection of a particular application that was detected as suspicious but isn't. He would ideally apply this exclusion to all computers for the department of application development.
> Use case 2: The Administrator wants to avoid repeated connection blocking of some application, trustworthy from his perspective. He wants to deploy this exception to the whole network easily from the console.



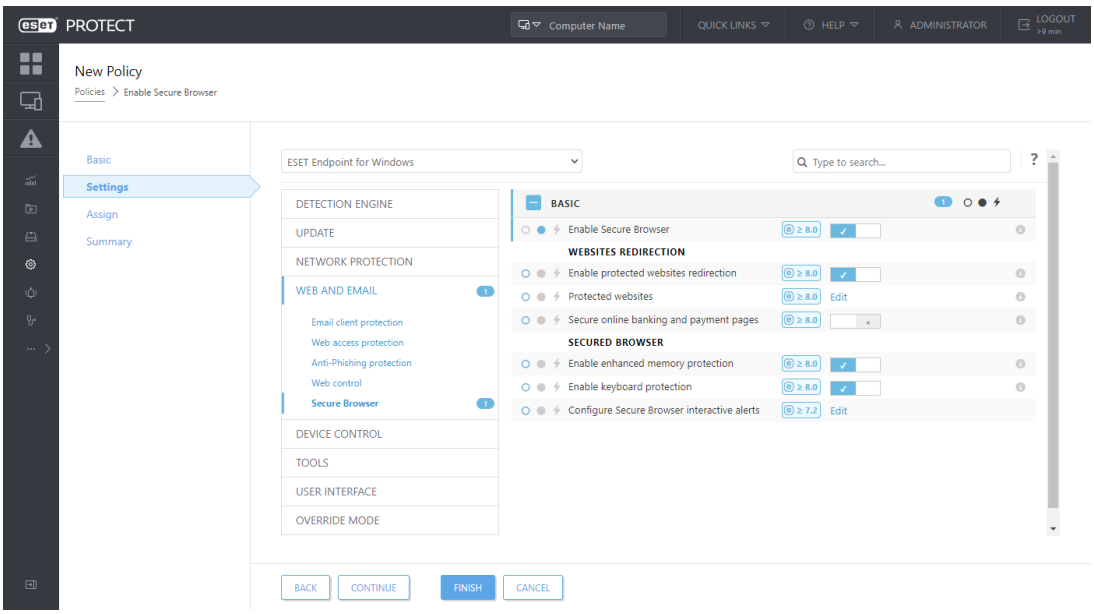


Back to top

Management for Secure Browser

Secure Browser protects a web-browser against other processes running on the computer. Conceptually, the idea supports a zero-trust approach and assumes that the computer or its protection capabilities are compromised or insufficient, and does not allow to tamper with the browser's memory space and consequently with the content of the browser window.

You can manage the Secure Browser feature from ESET PROTECT through standard Endpoint policy:



Use case: The Administrator wants to reduce the risk of leaking personal data from the internal information system. So he wants to configure all workstations in a way that the particular URL will be opened in a secured browser, mitigating the risk of data-stealing by malware.

Back to top

Improvements and other usability changes

We are continuously performing usability testing and customer research. Based on user feedback, we are focusing on improving primary workflows and enhancing the overall experience with the web interface. In the latest version, we are bringing multiple smaller improvements such as the following:

- Support for site licenses
- Trial license upgrade
- Close to expire license renew
- Improved Network isolation
- EULA Update notifications
- Streamlining of EDTD enablementImproved Detection details (LiveGrid, Observed in the organization, VT link)
- New EFDE management actions in tile
- New Dynamic groups and Reports for EFDE
- Reworked pop up with search option
- Improved Breadcrumbs
- Unification of invalid items
- Improved columns ordering
- Show in EEI also for other detection types
- Unsupported browser warning

Back to top