

ESET Tech Center

Kennisbank > ESET PROTECT > What's new in ESET PROTECT (v8)

What's new in ESET PROTECT (v8)

Steeff | 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

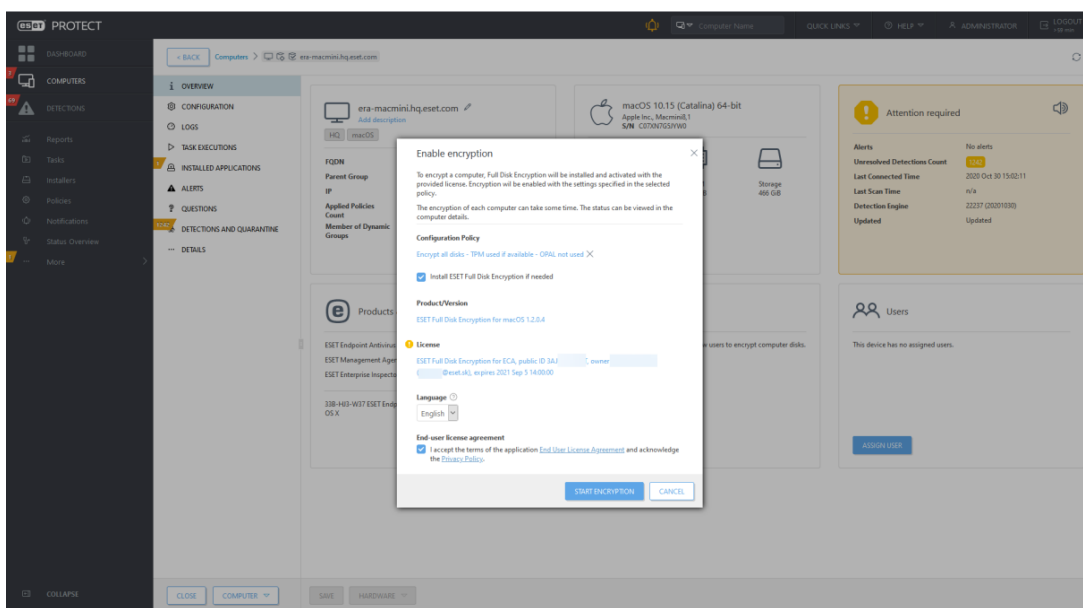
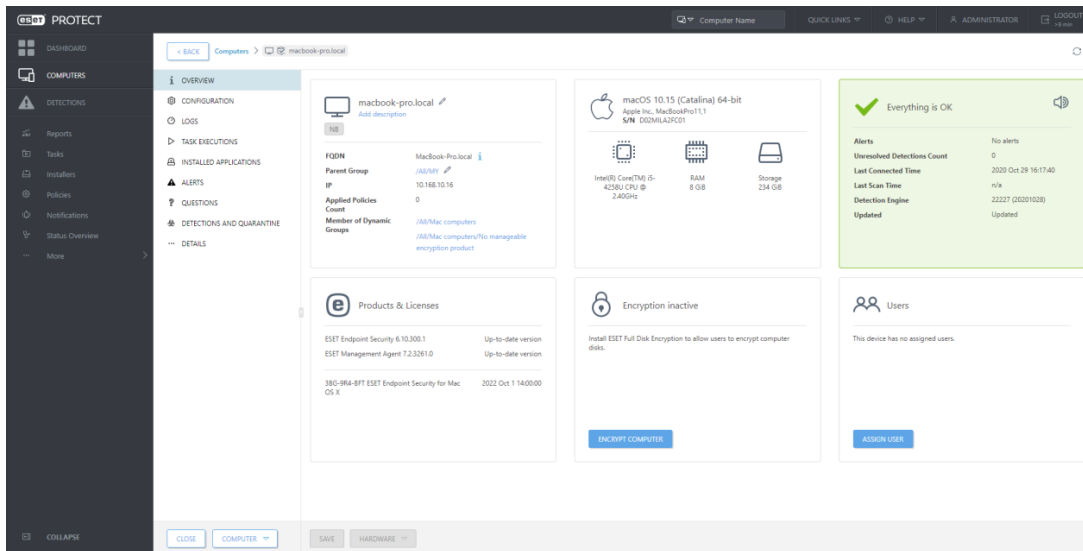
- [ESET Full Disk Encryption now also for macOS](#)
- [Audit Log](#)
- [Improved Exclusions](#)
- [Management for Secure Browser](#)
- [Improvements and other usability changes](#)

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.

OCURRED	AUDIT DOMAIN	ACTION	DETAIL	RESULT	LOGIN
2020 Oct 30 15:12:30	Firewall	Marked as Unresolved	Unresolved by User	Success	Administrator
2020 Oct 30 15:12:30	Firewall	Marked as Unresolved	Unresolved by User	Success	Administrator
2020 Oct 30 15:12:30	Firewall	Marked as Unresolved	Unresolved by User	Success	Administrator
2020 Oct 30 15:12:30	Firewall	Marked as Unresolved	Unresolved by User	Success	Administrator
2020 Oct 30 15:12:09	Policy	Modify	Renaming and possibly modifying policy 'TEST Policy' to 'Aggressive detections'.	Success	Administrator
2020 Oct 30 15:11:52	Policy	Create	Creating policy 'TEST Policy'.	Success	Administrator
2020 Oct 30 15:11:15	Single-sign-on token	Single sign on token ...	Single Sign-On Session Token ***** issued for native user: 'Administrator'.	Success	
2020 Oct 30 15:11:15	Native user	Login attempt	Authenticating native user: 'Administrator'.	Success	
2020 Oct 30 15:11:12	Native user	Login attempt	Authenticating native user: 'john'.	Access denied	
2020 Oct 30 15:11:06	Native user	Login attempt	Authenticating native user: 'Administrator'.	Access denied	
2020 Oct 30 15:11:02	Native user	Login attempt	Authenticating native user: 'Administrator'.	Access denied	
2020 Oct 30 15:10:53	Native user	Logout	Logging out native user: 'Administrator'.	Success	Administrator
2020 Oct 30 15:10:14	Single-sign-on token	Single sign on token ...	Single Sign-On Session Token ***** issued for native user: 'Administrator'.	Success	
2020 Oct 30 15:10:14	Native user	Login attempt	Authenticating native user: 'Administrator'.	Success	
2020 Oct 30 14:15:58	Server task	Start	Starting server task 'Automatic renaming of synchronized computers to FQDN format' of type 'R...	Success	Administrator
2020 Oct 30 13:17:26	Server task	Start	Starting server task 'Automatic renaming of synchronized computers to FQDN format' of type 'R...	Success	Administrator
2020 Oct 30 12:18:12	Server task	Start	Starting server task 'Automatic renaming of synchronized computers to FQDN format' of type 'R...	Success	Administrator
2020 Oct 30 11:15:26	Server task	Start	Starting server task 'Automatic renaming of synchronized computers to FQDN format' of type 'R...	Success	Administrator
2020 Oct 30 10:18:55	Server task	Start	Starting server task 'Automatic renaming of synchronized computers to FQDN format' of type 'R...	Success	Administrator
2020 Oct 30 09:51:57	Update modules	Update	Modules successfully updated.	Success	system

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.

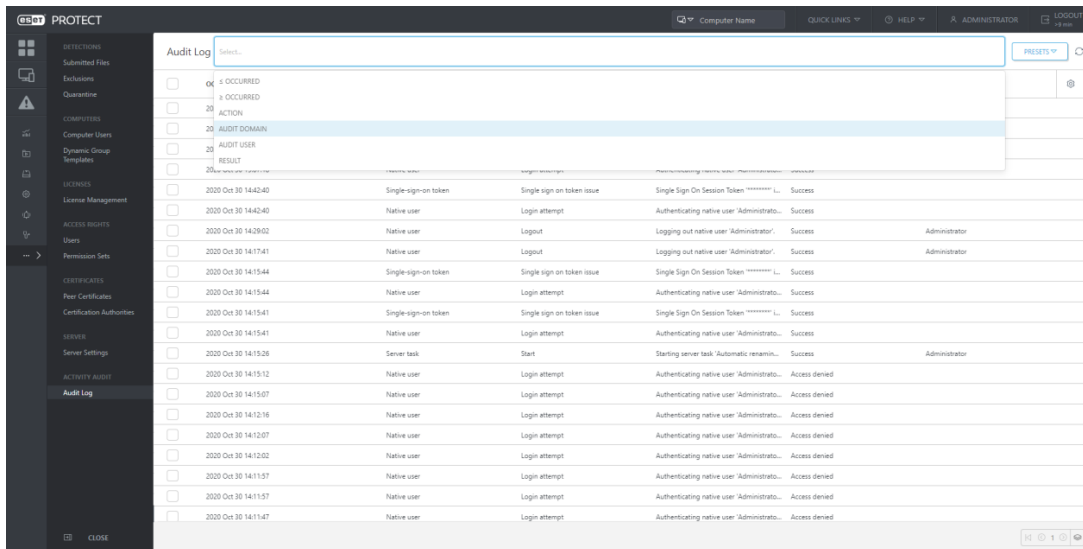
Use case 4: The Administrator wants to know who and when has performed a scanning task over the particular machine.

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:

The screenshot shows the ESET PROTECT interface with the Audit Log section active. A table lists various events with columns for Occurred, Action, Detail, Result, and Login. A context menu is open over the first row, showing options: Show Object Details, Show User Details, Audit Log, and Time window for selected object.

OCCURRED	ACTION	DETAIL	RESULT	LOGIN	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:30	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 30 15:12:09	Modify	Renaming and possibly modifying policy 'TEST Policy' to 'Aggressive detections'.	Success	Administrator	
2020 Oct 30 15:11:52	Create	Creating policy 'TEST Policy'.	Success	Administrator	
2020 Oct 30 15:11:15	Single sign-on token	Single Sign On Session Token ***** issued for native user 'Administrator'.	Success		
2020 Oct 30 15:11:15	Native user	Login attempt	Authenticating native user 'Administrator'.	Success	
2020 Oct 30 15:11:12	Native user	Login attempt	Authenticating native user 'John'.	Access denied	
2020 Oct 30 15:11:08	Native user	Login attempt	Authenticating native user 'Administrator'.	Access denied	
2020 Oct 30 15:11:02	Native user	Login attempt	Authenticating native user 'Administrator'.	Access denied	
2020 Oct 30 15:10:53	Native user	Logout	Logging out native user 'Administrator'.	Success	Administrator
2020 Oct 30 15:10:14	Single sign-on token	Single sign on token ...	Single Sign On Session Token ***** issued for native user 'Administrator'.	Success	
2020 Oct 30 15:10:14	Native user	Login attempt	Authenticating native user 'Administrator'.	Success	
2020 Oct 30 14:15:58	Server task	Start	Starting server task 'Automatic renaming of synchronized computers to FQDN format' of type 'R...	Success	Administrator

The screenshot shows the ESET PROTECT interface with the Detection Details section active. It displays a Firewall rule with the following details:

- Occurred:** 2020 Sep 4 22:00:01 - 2020 Sep 4 22:57:30
- Occurrences:** Total 186, Resolved 0, Handled by product 186
- Event:** Communication allowed by rule
- More details:** Process name: C:\Windows\System32\svchost.exe, Rule name: all UDP & TCP, Rule ID: 66F35EAD655078A87960283D08E356F0FB8, Source address: 10.1.181.88, Source port: 51739, Target address: 10.1.179.28, Target port: 7660, Protocol: TCP
- Observed worldwide (ESET LiveGrid®):** W10-AUTOTEST-88
- FGDN:** W10-AUTOTEST-88
- Last connected time:** 2020 Oct 30 15:18:25
- Unresolved detections:** 186
- Alerts:** 186 (All Cool & found)
- Parent group:** All Cool & found

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

From Computers:

ESSENTIAL PROTECT Dashboard | Computer Name | QUICK LINKS | HELP | ADMINISTRATOR | LOGOUT

Computers

SHOW SUBGROUPS | All (24) | TAGS | ADD FILTER | PRESETS

GROUPS	COMPUTER NAME	TAGS	STATUS	LAST CONNECTED	OS NAME	DETECTION	ALERTS	SECURITY PRODUCT
All (24)	nb-c+01		✓	2020 Oct 30 11:50:30	Microsoft Windows 10 Enterprise	0	0	ESET Endpoint Security
Windows computers	nb-c+02		✓	2020 Oct 30 11:52:23	Microsoft Windows 10 Enterprise	0	0	ESET Endpoint Security
Linux computers	nb-c+03		✓	2020 Oct 30 11:49:31	Microsoft Windows 10 Enterprise	0	0	ESET Endpoint Security
Mac computers	nb-c+04		✓	2020 Oct 30 11:51:10	Microsoft Windows Server 2016 Da...	0	0	ESET File Security
Computers with outdated modules	nb-c+05		✓	2020 Oct 30 11:57:33	Ubuntu	0	0	ESET File Security
Computers with outdated operating system	nb-c+06		✓	2020 Oct 29 16:17:40	macOS 10.15 (Catalina)	0	0	ESET Endpoint Security
Problematic computers	nb-c+07		✓	2020 Oct 30 11:52:40	Microsoft Windows 10 Home	436	0	ESET Endpoint Antivirus
Not activated security product	nb-c+08		✗	2020 Oct 30 11:54:05	Microsoft Windows 10 Home	113	1	ESET Endpoint Antivirus
	nb-c+09		✓	2020 Oct 30 11:49:32	Microsoft Windows 10 Home	0	0	ESET Endpoint Antivirus
	nb-c+10		✓	2020 Oct 29 11:23:11	macOS 10.13 (High Sierra)	0	0	ESET Endpoint Security
	nb-c+11		✓	2020 Oct 30 11:55:43	Microsoft Windows 10 Home	14	0	ESET Endpoint Security
	nb-c+12		✓	2020 Oct 29 22:07:00	Microsoft Windows 10 Home	0	0	ESET Endpoint Security
	nb-c+13		✓	2020 Oct 30 11:55:13	Microsoft Windows 10 Pro	0	0	ESET Endpoint Security
	nb-c+14		✓	2020 Oct 30 11:51:27	Microsoft Windows 10 Home	0	0	ESET Endpoint Security
	nb-c+15		✓	2020 Oct 30 11:58:15	Microsoft Windows 10 Enterprise	0	0	ESET Endpoint Security
	nb-c+16		✓	2020 Oct 30 11:52:17	Microsoft Windows 7 Enterprise	0	0	ESET Endpoint Security
	nb-c+17		✓	2020 Oct 30 11:54:12	Microsoft Windows Server 2019 Sta...	0	0	ESET File Security
	nb-c+18		✓	2020 Oct 30 11:57:00	Microsoft Windows Server 2019 Sta...	0	0	ESET Endpoint Security
	nb-c+19		✗	2020 Oct 30 11:55:19	macOS 10.15 (Catalina)	0	1	ESET Endpoint Security
	nb-c+20		✓	2020 Oct 30 11:53:58	Microsoft Windows 10 Home	0	0	ESET Endpoint Security

ADD NEW | ACTIONS | MUTE

ESSENTIAL PROTECT Dashboard | Computer Name | QUICK LINKS | HELP | ADMINISTRATOR | LOGOUT

Audit Log

SELECTED TARGET | ADD FILTER | PRESETS

OCCURRED	AUDIT DOMAIN	ACTION	DETAIL	RESULT	LOGIN
2020 Oct 13 21:35:54	Client trigger	Assign	Assigning client task 'Upgrade OS' to computer 'All...	Success	Administrator
2020 Oct 13 21:34:07	Client trigger	Assign	Assigning client task 'Update Operating System - via...	Success	Administrator
2020 Oct 3 22:28:34	Client trigger	Assign	Assigning client task 'Reboot Computer - via context...	Success	Administrator
2020 Oct 2 13:56:38	Client trigger	Assign	Assigning client task 'Software Installation (ESET End...	Success	Administrator
2020 Oct 1 15:52:39	Client trigger	Assign	Assigning client task 'Update Operating System - via...	Success	Administrator
2020 Sep 1 18:55:41	Client trigger	Assign	Assigning client task 'Update Operating System - via...	Success	Administrator
2020 Jul 25 20:54:37	Client trigger	Assign	Assigning client task 'Reboot Computer - via context...	Success	Administrator
2020 Jul 25 17:33:13	Client trigger	Assign	Assigning client task 'Software Installation (ESET End...	Success	Administrator
2020 Jul 17 10:34:18	Client trigger	Assign	Assigning client task 'Software Installation (ESET End...	Success	Administrator
2020 Jul 3 17:36:42	Computer	Modify	Renaming and possibly modifying computer 'msi' in...	Success	Administrator
2020 Jul 3 17:38:15	Computer	Modify	Modifying computer 'msi' in group 'ARMY'.	Success	Administrator
2020 Jun 12 13:29:30	Client trigger	Assign	Assigning client task 'Upgrade Agent - via context in...	Success	Administrator
2020 May 9 20:29:48	Computer	Create	Creating computer 'msi' in group 'ARMY'.	Success	Administrator

From Detections:

ESSENTIAL PROTECT Dashboard | Computer Name | QUICK LINKS | HELP | ADMINISTRATOR | LOGOUT

Detections

SHOW SUBGROUPS | All (22) | TAGS | DETECTION CATEGORY | Antivirus | ADD FILTER | PRESETS

STATUS	DETECTION TYPE	ACTION	RESOLVED	COMPUTER NAME	OBJECT	PROG.	USER	OCCURRED
✗	Antivirus	conn...	4	w10-autote...	https://...	C:\P...	W10...	2020 Sep 22 13:31:22
✗	Antivirus	net...	3	w10-autote...	file://...	C:\P...	W10...	2020 Sep 11 12:16:52
✗	Antivirus	net...	2	w10-autote...	file://...	C:\P...	W10...	2020 Sep 11 12:16:52
✗	Antivirus	net...	2	w10-autote...	file://...	C:\P...	Admin...	2020 Sep 11 20:35:23
✗	Antivirus	net...	1	w10-autote...	file://...	C:\P...	Admin...	2020 Sep 11 20:38:09
✗	Antivirus	trojan	1	w10-autote...	file://...	C:\P...	W10...	2020 Sep 17 09:41:50
✗	Antivirus	trojan	1	w10-autote...	file://...	C:\P...	W10...	2020 Sep 22 09:35:53
✗	Antivirus	trojan	1	w10-autote...	file://...	C:\P...	W10...	2020 Sep 11 12:17:47
✗	Antivirus	trojan	1	w10-autote...	file://...	C:\P...	W10...	2020 Sep 11 12:17:53
✗	Antivirus	trojan	1	w10-autote...	file://...	C:\P...	W10...	2020 Sep 11 12:29:43
✗	Antivirus	trojan	1	w10-autote...	file://...	C:\P...	W10...	2020 Sep 11 12:16:52
✗	Antivirus	trojan	1	w10-autote...	file://...	C:\P...	W10...	2020 Sep 11 12:16:52

SCAN COMPUTERS | RESOLVE | ACTIONS

ESET PROTECT

Computer Name QUICK LINKS HELP ADMINISTRATOR LOGOUT

Audit Log SELECTED TARGET X ADD FILTER PRESETS

OCCURRED	AUDIT DOMAIN	ACTION	DETAIL	RESULT	LOGIN
2020 Oct 30 15:30:18	Antivirus	Marked as Resolved	Resolved by User	Success	Administrator
2020 Oct 30 15:30:18	Antivirus	Marked as Resolved	Resolved by User	Success	Administrator
2020 Oct 30 15:30:18	Antivirus	Marked as Resolved	Resolved by User	Success	Administrator
2020 Oct 30 15:30:15	Antivirus	Marked as Unresolved	Unresolved by User	Success	Administrator
2020 Oct 30 15:30:15	Antivirus	Marked as Unresolved	Unresolved by User	Success	Administrator
2020 Oct 30 15:30:15	Antivirus	Marked as Unresolved	Unresolved by User	Success	Administrator

From Policies:

ESET PROTECT

Computer Name QUICK LINKS HELP ADMINISTRATOR LOGOUT

Policies ACCESS GROUP Select SHOW UNASSIGNED All (34) Tags ADD FILTER PRESETS

NAME	POLICY PRODUCT	TAGS	DESCRIPTION
Antivirus - Balanced	ESET Endpoint for Windows		Security configuration recommended for mo...
Antivirus - Maximum security	ESET Endpoint for Windows		Taking advantage of machine learning, deep ...
Visibility - Balanced	ESET Endpoint for Windows		Default setting for visibility. Statuses and not...
Visibility - Invisible mode	ESET Endpoint for Windows		Disabled notifications, alerts, GUI, integratio...
Visibility - Reduced interaction with user	ESET Endpoint for Windows		Disabled statuses, disabled notifications, GUI ...
Antivirus - Real-time scanner only	ESET File Security for Windows Server (V6+)		Optimized performance for server. Real-time ...
Antivirus - Maximum security - Recommended	ESET File Security for Windows Server (V6+)		Taking advantage of advanced heuristic, Live...
Visibility - Silent mode	ESET File Security for Windows Server (V6+)		Suitable for multi-user server, e.g. Terminal S...
Cloud-based reputation and feedback system	ESET Endpoint for Windows		Enables ESET LiveGrid® cloud-based reputat...
Cloud-based reputation and feedback system	ESET Mail Security for Microsoft Exchange (V...		Enables ESET LiveGrid® cloud-based reputat...
Cloud-based reputation and feedback system	ESET File Security for Windows Server (V6+)		Enables ESET LiveGrid® cloud-based reputat...
Encrypt all disks - Recommended	ESET Full Disk Encryption		Enables full disk encryption for all disks
Encrypt boot disk only	ESET Full Disk Encryption		Enables full disk encryption for boot disk only
General - Maximum pro...	ESET Endpoint for Android (2+)		ESET Security Product for Android uses all op...
General - Balanced setu...	ESET Endpoint for Android (2+)		ESET Security Product for Android uses conf...
General - Maximum per...	ESET Endpoint for Android (2+)		ESET Security Product for Android combines ...
agent full log - 10s con...	ESET Management Agent		
Policy - Device control	ESET Endpoint for Windows		
ESET Dynamic Threat D...	ESET Endpoint for Windows		Enables ESET Dynamic Threat Defense witho...
ESET Dynamic Threat D...	ESET Endpoint for Windows		Enables ESET Dynamic Threat Defense to aut...
Aggressive detections	ESET Endpoint for Windows		

ESET PROTECT

Computer Name QUICK LINKS HELP ADMINISTRATOR LOGOUT

Audit Log SELECTED TARGET X ADD FILTER PRESETS

OCCURRED	AUDIT DOMAIN	ACTION	DETAIL	RESULT	LOGIN
2020 Oct 30 15:35:39	Policy	Modify	Modifying policy 'Aggressive detections'.	Success	Administrator
2020 Oct 30 15:34:41	Policy	Modify	Modifying policy 'Aggressive detections'.	Success	Administrator
2020 Oct 30 15:34:15	Policy	Modify	Modifying policy 'Aggressive detections'.	Success	Administrator
2020 Oct 30 15:12:09	Policy	Modify	Renaming and possibly modifying policy 'TEST Policy' to 'Aggressive detections'.	Success	Administrator
2020 Oct 30 15:11:52	Policy	Create	Creating policy 'TEST Policy'.	Success	Administrator

[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.

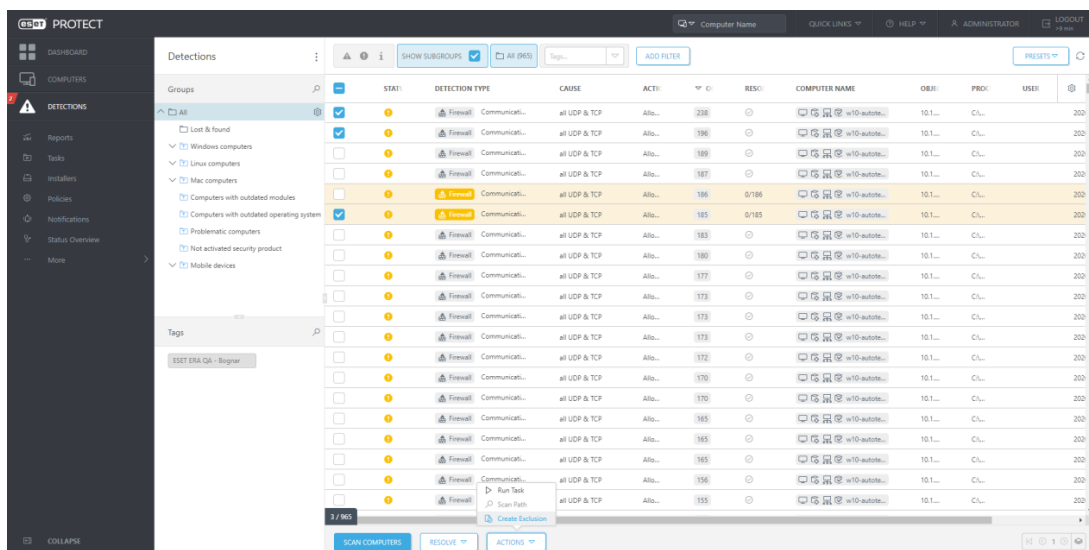
You can create an exclusion using a new Wizard by performing the following actions:

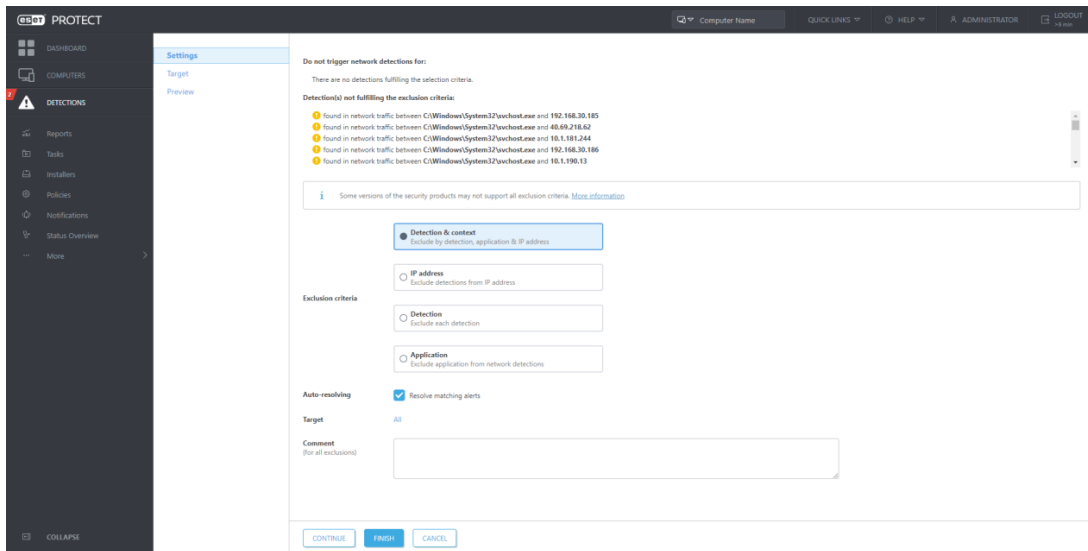
- Create multiple exclusions at once
- Specify the exclusion based on the recommended set of criteria (for example, not exclude ML detection by detection name because that would disable the ML engine entirely)
- See the affected detections that will be suppressed by the created exclusion (not only the 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.



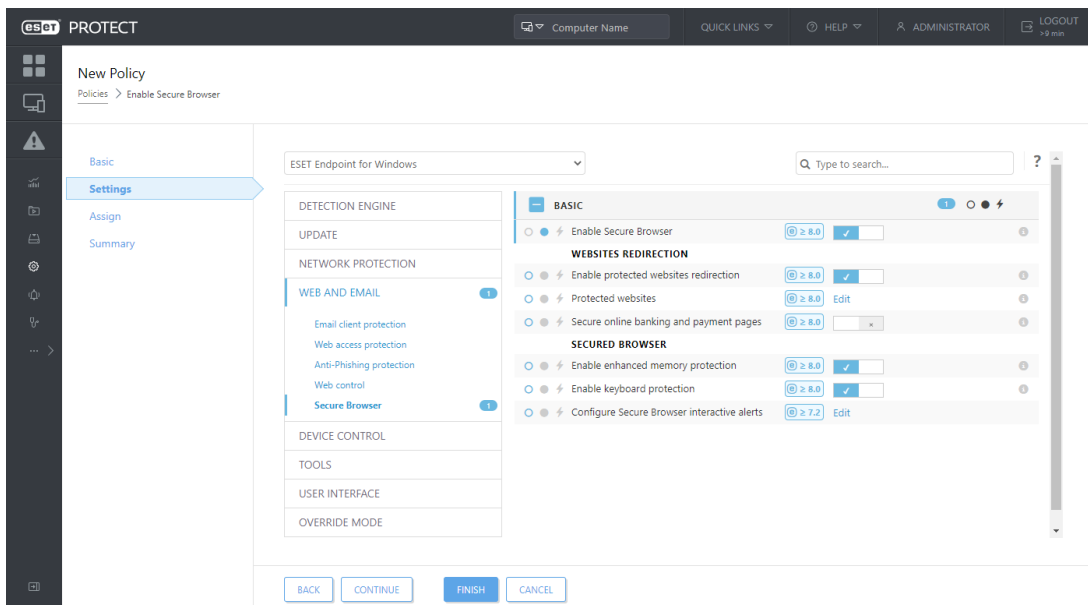


[Back to top](#)

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](#)