ESET Tech Center

Knowledgebase > ESET PROTECT On-prem > What's new in ESET PROTECT (v8)

What's new in ESET PROTECT (v8)

Steef | ESET Nederland - 2025-03-06 - Comments (0) - ESET PROTECT On-prem

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
- <u>Audit Log</u>
- Improved Exclusions
- <u>Management for Secure Browser</u>
- 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.

(ESET) PROTECT			
DASHEGARD Computers > 🖵 🕲 mache	ok-pro focal		0
□ communities i overset/even ▲ contractions ● contraction ✓ reports ● loss b tack ● none ■ instation ▲ Matter		Agrience, MacDoolfvell,1 Agrience, MacDoolfvell,1 Stri DOMILARCOI With Communications With Communications Wit	Everything is OK Alarts No alerts Unresolved Detections Count 0 Last Conneme 70
Notification Notification Notification Status Overview Nore Nore	n for the Parken 0 Const Member of Dynamic //ASAde computers Groups //ASAde computers/ encryption product	28000 808 23408 28000	Derection remine 22227 (2020103) Derection angle 22227 (2020103) Updated Updated
	EEF Endpoint Security & 10,500.1 Up-to-date version EEF Endpoint Security & 10,500.1 Up-to-date version EEF Management Agent? 22,321.0 Up-to-date version 3806-5964-BPT EEF Endpoint Security for Mac. 2002 Cd.114.00.00	Encryption inactive	Visers Users
	SAE HATOMAR **	CBMPCCMUITZ	ASSINTABLE

ese	PROTECT			UT
::		< BACK Computes > 🖵 🛱 😢	seminik by east com	0
"Gð		i overview		
		OVEREEN CONFIGURATION CONFIGURATION CONFIGURATION DISC EXECUTIONS AUSTLE APPLICATIONS AUSTLE APPLICATIONS AUSTLE APPLICATIONS DISC EXECUTIONS DIS	Construction Construction <th></th>	
		CLOSE COMPUTE *	ME MARANE -	

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.

(CSET)	PROTECT					QUICK LINKS T	⑦ HELP	A ADMINISTRATOR	⊡ LOGOUT
		Audit Log	ADD FILTER					PRESE	ets 🔻 🖸
⊊} ▲			OCCURRED	AUDIT DOMAIN	ACTION	DETAIL	RESULT	LOGIN	0
*			2020 Oct 30 15:12:30	Firevall	Marked as Unresolved	Unresolved by User	Success	Administrator	
			2020 Oct 30 15:12:30	Firewall	Marked as Unresolved	Unresolved by User	Success	Administrator	
	Dynamic Group Templates		2020 Oct 30 15:12:30	Firewall	Marked as Unresolved	Unresolved by User	Success	Administrator	
			2020 Oct 30 15:12:30	Firevall	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 15:11:08	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		
	Audit Log		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 12:19:12	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 10:19:55	Server task	Start	Starting server task 'Automatic renaming of synchronized computers to FQDN format' of type 'R	Success	Administrator	
		1 / 1000	2020 Oct 30 09:51:57	Update modules	Update	Modules successfully updated.	Success	system	
									0100

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:

es et	PROTECT					Computer Name	QUICK LINKS 🗢		STRATOR I LOGO
		Audit Lo	Select						PRESETS 🔝
ш,			OC S OCCURRED						8
A			≥ OCCURRED 20 ACTION						
			20 AUDIT DOMAIN						
			20 AUDIT USER						
			RESULT 20Lo - Color - Color - Color	1 Martin Mart	wayer with the	Anti-terreting there ages Anti-terreting			
			2020 Oct 30 14:42:40	Single-sign-on token	Single sign on token issue	Single Sign On Session Token "******** i	Success		
			2020 Oct 30 14:42:40	Native user	Login attempt	Authenticating native user 'Administrato	Success		
			2020 Oct 30 14:29:02	Native user	Logout	Logging out native user 'Administrator'.	Success	Administrator	
			2020 Oct 30 14:17:41	Native user	Logout	Logging out native user 'Administrator'.	Success	Administrator	
			2020 Oct 30 14:15:44	Single-sign-on token	Single sign on token issue	Single Sign On Session Token "******** i	Success		
			2020 Oct 30 14:15:44	Native user	Login attempt	Authenticating native user 'Administrato			
			2020 Oct 30 14:15:41	Single-sign-on token	Single sign on token issue	Single Sign On Session Token "******* i			
		0	2020 Oct 30 14:15:41	Native user	Login attempt	Authenticating native user 'Administrato			
			2020 Oct 30 14:15:26	Server task	Start	Starting server task 'Automatic renamin		Administrator	
	ACTIVITY AUDIT		2020 Oct 30 14:15:12 2020 Oct 30 14:15:07	Native user	Login attempt	Authenticating native user 'Administrato Authenticating native user 'Administrato			
			2020 Oct 30 14:12:16	Native user	Login attempt	Authenticating native user 'Administrato			
		0	2020 Oct 30 14:12:07	Native user	Login attempt	Authenticating native user 'Administrato			
			2020 Oct 30 14:12:02	Native user	Login attempt	Authenticating native user 'Administrato			
			2020 Oct 30 14:11:57	Native user	Login attempt	Authenticating native user 'Administrato	Access denied		
			2020 Oct 30 14:11:57	Native user	Login attempt	Authenticating native user 'Administrato	Access denied		
			2020 Oct 30 14:11:47	Native user	Login attempt	Authenticating native user 'Administrato	Access denied		
									K © 1 ©

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:

Bet) P	ROTECT					Computer Name QUICK LI	NKS 🗢 🛞 HELP 🗢	A ADMINISTRATOR	⊡ LOGO
		Audit Log	ADD FILTER					PRES	ETS 🗢
	Exclusions Quarantine		OCCURRED	Audit Log	ACTION	DETAIL	RESULT	LOGIN	10
			2020 Oct 30 15:12:30	i Show Object Details	Marked as Unresolved	Unresolved by User	Success	Administrator	
			2020 Oct 30 15:12:30	A Show User Details	Marked as Unresolved	Unresolved by User	Success	Administrator	
			2020 Oct 30 15:12:30	C Audit Log for selected User	Marked as Unresolved	Unresolved by User	Success	Administrator	
			2020 Oct 30 15:12:30	I'me window for selected object	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 15:12:30	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 tok	en 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 tok	en 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	e 'R Success	Administrator	

(ESET)	PROTECT						
::	< BACK Audit Log > Detection Det	tails					0
됴	i OVERVIEW						A
2 A 	I≡ OCCURRENCES	Communication allowed by		W10-AUTOTEST-88 Select tags	W10-AUTOTEST-BB		_
		Occurred Occurrences	2020 Sep 4 22:00:01 - 2020 Sep 4 22:57:38 Total 186	Last connected time	2020 Oct 30 15:18:25		
0			 ⊘ Resolved 0 ⊗ Handled by product 186 		680 No alerts		
٥		Event	Communication allowed by rule		/All/Lost & found		
8-		OPEN ENTERPRISE INSPECTOR		SHOW DETAILS			
>		OPEN ENTERPAISE INSPECTOR		SHOW DEIAILS			
		1 More details					
		Process name	C/Windows\System32\svchost.exe				
		Rule name	all UDP & TCP				
		Rule ID					
		Hash	66F5E6DADE65D7DBA979602830D58E53E60FDFFB 🗸				
		Source address	10.1.181.98				
		Source port	51739				
		Target address	10.1.179.28				
		Target port	7680				
		Protocol	тср				
		Observed worldwide (Estimate)	SET LiveGrid®)				
	CLOSE	RESOLVE 🤝 CREATE EXCU	USION COMPUTER 🗢				

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

From Computers:

Set	PROTECT								G ♥ Computer Name	QUICK LINKS 🗢	⑦ HELP ♥	8 ADMINI	
	DASHBQARD	Computers	:	A 0 - · ·	SHOW SUBGROU	JPS 🔽 🖿 All (24) Tagi		ADD FILTER				PRESETS 🖤
-2 ·	COMPUTERS	Groups	Q	COMPUTE	NAME	1	AGS	STATUS	LAST CONNECTED	OS NAME	DETECTIONS	ALERTS	SECURITY PRODUC
a '	DETECTIONS	^ □ All (24)	•	D C No	-e01 10.1.222.97			~	2020 Oct 30 11:50:30	Microsoft Windows 10 Enterprise	5	0	ESET Endpoint Security
	Reports	C DW (5)	Т	D C Ho	-e02 10.1.222.117	7		×	2020 Oct 30 11:52:23	Microsoft Windows 10 Enterprise	0	0	ESET Endpoint Antivirus
	Tasks	Lost & found (0)	н	C 🗟 Ho	-e03 10 Compu	iter		×	2020 Oct 30 11:49:31	Microsoft Windows 10 Enterprise	0	0	ESET Endpoint Security
	Installers	D MY (9)	T.			ow Details	ERVER	×	2020 Oct 30 11:51:10	Microsoft Windows Server 2016 Da	0	0	ESET File Security
	Policies	✓ □ VIRT (8)	н					×	2020 Oct 30 11:57:33	Ubuntu	0	0	ESET File Security
	Notifications	V 🗈 Windows computers	н	🖵 🗟 ma			/8	×	2020 Oct 29 16:17:40	macOS 10.15 (Catalina)	0	0	ESET Endpoint Security
	Status Overview	V 🛅 Linux computers	T.	🗆 🔍 dw		boot >		×	2020 Oct 30 11:52:40	Microsoft Windows 10 Home	436	0	ESET Endpoint Antivirus
	More >	V 🕅 Mac computers				slate from network		0	2020 Oct 30 11:54:05	Microsoft Windows 10 Home	133	0	ESET Endpoint Antiviru
		Computers with outdated modules	г		L 02 1	d network isolation m Task		×	2020 Oct 30 11:49:32	Microsoft Windows 10 Home	0	0	ESET Endpoint Antiviru
		Problematic computers	1	🗆 🔍 ma		ew Task	18	×	2020 Oct 26 11:22:17	macOS 10.13 (High Sierra)	0	0	ESET Endpoint Security
		NO Max actioned	*		JNK 15	st used tasks >		×	2020 Oct 30 11:55:43	Microsoft Windows 10 Home	14	0	ESET Endpoint Security
		Tags	9	🔍 🔍 de		anage Policies		×	2020 Oct 29 22:07:00	Microsoft Windows 10 Home	0	0	ESET Endpoint Security
		HYPER-V		D 🖗 Hb	c-e05 10 *	nd Wake-Up Call activate Products		×	2020 Oct 30 11:55:13	Microsoft Windows 10 Pro	0	0	ESET Endpoint Security
		NB		💭 🖗 AS			18	×	2020 Oct 30 11:51:27	Microsoft Windows 10 Home	0	0	ESET Endpoint Security
		SERVER		D hb-c-e		able encryption		×	2020 Oct 30 11:58:15	Microsoft Windows 10 Enterprise	0	0	
				C C HE	0.0007	able EDTD name multiple items		×	2020 Oct 30 11:52:17	Microsoft Windows 7 Enterprise	0	0	ESET Endpoint Security
						ove to Group	ERVER	×	2020 Oct 30 11:54:12	Microsoft Windows Server 2019 Sta	0	0	ESET File Security
					AD-SL 1		IVPER-V	×	2020 Oct 30 11:57:00	Microsoft Windows Server 2019 Sta	0	0	ESET File Security
				🕑 lucas-a				A	2020 Oct 30 11:55:19	macOS 10.15 (Catalina)	0	0	
					tob-SvajBa 192.16	8.1.12	NB	×	2020 Oct 30 11:53:58	Microsoft Windows 10 Home	0	0	ESET Endpoint Security
	COLLAPSE			ADD NEW -	ACTIONS V	MUTE 🗢							

ISer	PROTECT					Computer Name	QUICK LINKS 🛩	() HELP ♥ A ADMINISTRATOR I LOGO
		Audit Lo) FUTER				PRESETS ♥
<u>_</u>]		Ð	OCCURRED	AUDIT DOMAIN	ACTION	DETAIL	RESULT	LOGIN
A			2020 Oct 13 21:35:54	Client trigger	Assign	Assigning client task 'Upgrade OS' to computer 'All		Administrator
			2020 Oct 13 21:34:07	Client trigger	Assign	Assigning client task 'Update Operating System - v	e _ Success	Administrator
			2020 Oct 3 22:29:34	Client trigger	Assign	Assigning client task 'Reboot Computer - via conte	t Success	Administrator
			2020 Oct 2 13:56:38	Client trigger	Assign	Assigning client task 'Software Installation (ESET En	i Success	Administrator
			2020 Oct 1 15:52:39	Client trigger	Assign	Assigning client task 'Update Operating System - w	e Success	Administrator
			2020 Sep 1 18:55:41	Client trigger	Assign	Assigning client task: Update Operating System - v	a Success	Administrator
			2020 Jul 25 22:54:37	Client trigger	Assign	Assigning client task Reboot Computer - via conte	t Success	Administrator
	More	> □	2020 Jul 25 17:32:13	Client trigger	Assign	Assigning client task 'Software Installation (ESET En	s Success	Administrator
		0	2020 Jul 17 10:34:18	Client trigger	Assign	Assigning client task 'Software Installation (ESET En	á Success	Administrator
			2020 Jul 3 17:38:42	Computer	Modify	Renaming and possibly modifying computer 'msi' i	Success	Administrator
			2020 Jul 3 17:38:15	Computer	Medify	Modifying computer 'msi' in group 'All/MY'.	Success	Administrator
			2020 Jun 12 13:29:30	Client trigger	Assign	Assigning client task 'Upgrade Agent - via context i	n Success	Administrator
			2020 May 3 20:29:48	Computer	Create	Creating computer 'msi' in group 'All\MY'.	Success	Administrator

From Detections:

(CSet)	PROTECT															
::	Detections	:	▲ 0) i	SHOW SUBGROUPS	All (12) Tags		DETECTION CATE	SORY	Antivirus X					PRESETS 🗢	0
도 <u>라</u>	Groups) م		STAT	U DETECTION T	i Show Details	E	ACTIO	∞ 00	RESO	COMPUTER NAME	OBJECT	PROCE	USER	OCCURRED	۲
A	∩ □ All	۱		9	O Antivirus	1 Show in El		conn	4	\odot	🖵 🔓 💂 🖗 w10-autote	https:	CI/Pr	W10	2020 Sep 22 13:31:22	
1 11	🗀 Lost & found				① Antivirus	Mark As Resolved Mark As Not Resolved	sBot	retai	3		□ G 뮤 @ w10-autote	file://	C:\Pr	W10	2020 Sep 11 12:16:52	
te	V 💟 Windows computers				Antivirus		sBot.CIL	retai	2	0	□ G 🖁 © w10-autote	file://_	CIPr	W10	2020 Sep 11 12:16:52	
	Cinux computers Mac computers				Antivirus	Actions	sBot	retai	2	0/2	□ G 👷 @ w10-autote	file://_	C:\Pr	Admi	2020 Sep 11 20:35:23	
0	Computers with outdated modules				① Antivirus	Scan Path Create Exclusion	sBot.CIL	retai	1	Ø	□ G 田 @ w10-autote	file://	C1/Pr	Admi	2020 Sep 11 20:38:09	
ò	Computers with outdated operating system	em (Antivirus		C/SdBot.CIL	retai	1	0/1	□ G 💂 @ w10-autote	file://	CI/Pr	W10	2020 Sep 17 09:41:50	
 %-	Problematic computers			0	① Antivirus	trojan Wi	n32/TrojanD	clean	1	0	□ G 🖫 🕅 w10-autote	file://	Cito	W10	2020 Sep 22 09:35:53	
	Not activated security product				O Antivirus	trojan IR	L/SdBot	clean	1	\odot	口 G 品 @ w10-autote	file://	Cito	W10	2020 Sep 11 12:17:47	
	V 🕅 Mobile devices			0	O Antivirus	trojan IR	C/SdBot.CGM	clean	1	0	□ G 🔒 🕅 w10-autote	file://	C\to	W10	2020 Sep 11 12:17:53	
				0	O Antivirus	trojan IR	C/SdBot	clean	1	0	및 🕼 开 🖉 w10-autote	file://	C/\Pr	W10	2020 Sep 11 12:29:43	
					① Antivirus	trojan IR:	C/SdBot.CGM	retai	1	0	□ G 🔒 🖄 w10-autote	file://	C/\Pr	W10	2020 Sep 11 12:16:52	
	Tags	۹ (\mathbf{V} Antivirus	trojan IR:	:/SdBot.CRD	retai	1	0	□ G 且 🕅 w10-autote	file://	C/Pr	W10	2020 Sep 3 11:37:48	
	ELTITIN CA Boyur															

	ED AUDIT DOMAIN	ACTION	DETAIL			
	30 15:30:18 Antivirus			RESULT	LOGIN	
2020 Oct 3		Marked as Resolved	Resolved by User	Success	Administrator	
	30 15:30:18 Antivirus	Marked as Resolved	Resolved by User	Success	Administrator	
2020 Oct 3	30 15:30:18 Antivirus	Marked as Resolved	Resolved by User	Success	Administrator	
2020 Oct 3	30 15:30:15 Antivirus	Marked as Unresolved	Unresolved by User	Success	Administrator	
2020 Oct 3	30 15:30:15 Antivirus					
2020 Oct 3		Marked as Unresolved	Unresolved by User	Success	Administrator	

SCAN COMPUTERS RESOLVE T ACTIONS

From Policies:

•		Policies	ACCESS GRO	UP Select 🗎	SHOW UNASSIGNED 🔽	Tags		FILTER			PRESETS	, v	
-0		Policies ,0		NAME		POLICY PRODUCT		TAGS		DESCRIPTION		1	
Â.		∧ at	· U	Antivirus - Balanced		ESET Endpoint for Windows				Security configuration	on recommended for mo		
		^ ℓ Custom Policies		Antivirus - Maximum	security	ESET Endpoint for Windows				Taking advantage of	f machine learning, deep		
		ESET Endpoint for Windows		Visibility - Balanced		ESET Endpoint for Windows				Default setting for vi	isibility. Statuses and noti		
		ESET Management Agent	0	Visibility - Invisible m	ode	ESET Endpoint for Windows				Disabled notification	ns, alerts, GUI, integration		
		 Built-in Policies 		Visibility - Reduced in	teraction with user	ESET Endpoint for Windows				Disabled statuses, d	isabled notifications, GUI		
	Policies	(2) ESET Endpoint for Android (2+) (3) ESET Endpoint for macOS (OS X) a	0	Antivirus - Real-time	scanner only	ESET File Security for Windows S	ierver (V6+)			Optimized performa	ance for server. Real-time		
		 ESET Endpoint for macUs (US X) a ESET Endpoint for Windows 	Ō	Antivirus - Maximum	security - Recommended	ESET File Security for Windows S	ierver (V6+)			Taking advantage of	fadvanced heuristic, Live		
		ESET File Security for Windows Ser	Visibility - Silent mode Cloud-based reputation and feedback system			ESET File Security for Windows S				Suitable for multi-user server, e.o. Terminal S			
	ESET File Security for	ESET Full Disk Encryption				ESET Endpoint for Windows		Enables ESET LiveGrid ® cloud-based reputati					
		E ESET Mail Security for Microsoft Ex			on and feedback system	ESET Mail Security for Microsoft	Furhanne IV				id® cloud-based reputati		
		ESET Management Agent			on and feedback system	ESET File Security for Windows S					id® cloud-based reputati		
		Tags		Encrypt all disks - Rec		ESET Full Disk Encryption				Enables full disk enc			
		iags /~		Encrypt boot disk on	Actions	ESET Full Disk Encryption					ryption for boot disk only.		
		ESET ERA QA - Bognar		General - Maximum p	i Show Details	ESET Endpoint for Android (2+)					ct for Android uses all op		
				General - Maximum p	E Hour wy	ESET Endpoint for Android (2+)							
					Q Tags						ct for Android uses confi		
				General - Maximum p	/ Edit	ESET Endpoint for Android (2+)				ESET Security Produ	ct for Android combines		
				agent full log +10s co	18 Delete	ESET Management Agent							
				Policy - Device contro	Export	ESET Endpoint for Windows							
					D Change Assignment	ESET Endpoint for Windows					nic Threat Defense witho		
				ESET Dynamic Threat	D + Assign computers + Assign groups	ESET Endpoint for Windows				Enables ESET Dynam	nic Threat Defense to aut		
				Aggressive detection	Change Assignments	ESET Endpoint for Windows							
			ACTIONS 1	NEW POLIC	Access Rights							1 0	
					Access Group >								

(US el	PROTECT								
	DASHBOARD	Audit Log	SELECTED TARGET X ADD FILTE	R				PRESETS 🗢 🕻	c
돠	COMPUTERS		OCCURRED	AUDIT DOMAIN	ACTION	DETAIL	RESULT	LOGIN	0
A	DETECTIONS		2020 Oct 30 15:35:39	Policy	Modify	Modifying policy 'Aggressive detections'.	Success	Administrator	
	Reports		2020 Oct 30 15:34:41	Policy	Modify	Modifying policy 'Aggressive detections'.	Success	Administrator	
	Tasks		2020 Oct 30 15:34:15	Policy	Modify	Modifying policy 'Aggressive detections'.	Success	Administrator	
	Installers		2020 Oct 30 15:12:09	Policy	Modify	Renaming and possibly modifying policy 'TEST Policy' to 'Aggressive detections'.	Success	Administrator	
	Policies		2020 Oct 30 15:11:52	Policy	Create	Creating policy 'TEST Policy'.	Success	Administrator	
	Notifications								

K © 1 0 🗣

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.

eset PROTECT	г							- 8	Gr ⊂ Comput	er Name	QUICK LINKS 🔻 🛞	HELP ♥ .	R. ADMINISTRA	ATOR I LOGOUT
DASHBOARD	Detections	:	A 0	i	SHOW SUBGROUPS 🔽	Ali (965)	Tags	ADD FILTER	2					PRESETS 🔻 🔿 🔿
	Groups	م ر		STAT	DETECTION T	YPE	CAUSE	ACTIC	▼ 00	RESO	COMPUTER NAME	OBJEC	PROC	USER 💿
	AII	٥		0	A Firewall	Communicati	all UDP & TCP	Allo	238		□ G 및 ⓒ w10-autote	10.1	Ch	202
	🗀 Lost & found			0		Communicati	all UDP & TCP	Allo	196		口 G 品 @ w10-autote	10.1	C3,	202
	V 🕅 Windows computers			0	å Firewall	Communicati	all UDP & TCP	Allo	189	ø	口 G 品 @ w10-autote	10.1	C3,	202
	C Linux computers Mac computers			0	₿ Firewall	Communicati	all UDP & TCP	Allo	187	ø	□ 15 🔜 @ w10-autote	10.1	C/),	202
	Computers with outdated modul	/es		θ	🛕 Firewall	Communicati	all UDP & TCP	Allo	186	0/186	口 G 品 @ w10-autote	10.1	C/),	202
	Computers with outdated operat			0	🚓 Firewall	Communicati	all UDP & TCP	Allo	185	0/185	口 16 品 @ w10-autote	10.1	CA	202
	Problematic computers			0	▲ Firewall	Communicati	all UDP & TCP	Allo	183	ø	□ G □ w10-autote	10.1	Cô,	202
	Not activated security product			0	& Firewall	Communicati	all UDP & TCP	Allo	180	ø	다. 다 묘 @ w10-autote	10.1	C3,	202
	V 🖿 Mobile devices			θ	₿ Firewall	Communicati	all UDP & TCP	Allo	177	ø	□ G 🔜 © w10-autote	10.1	C/),	202
				θ	♣ Firewall	Communicati	all UDP & TCP	Allo	173	ø	다. 다 뮤 @ w10-autote	10.1	Cô,	202
				0	💩 Firewall	Communicati	all UDP & TCP	Allo	173	ø	口 16 品 @ w10-autote	10.1	C3	202
	Tags	ρ,		0	& Firewall	Communicati	all UDP & TCP	Allo	173	ø	□ 6 🖫 © w10-autote	10.1	C.h,	202
	ESET ERA QA - Bognar			0	å Firewall	Communicati	all UDP & TCP	Allo	172	ø	및 C 및 ② w10-autote	10.1	Cð,	202
				0	& Firewall	Communicati	all UDP & TCP	Allo	170	0	□ 다 묘 @ w10-autote	10.1	¢3,	202
				0	A Firewall	Communicati	all UDP & TCP	Allo	170		및 🖏 🖫 🖉 w10-autote	10.1	C3,	202
				θ	A Firewall	Communicati	all UDP & TCP	Allo	165	ø	口 G 品 @ w10-autote	10.1	CA	202
				0	A Firewall	Communicati	all UDP & TCP	Allo	165	ø	C C R v10-autote	10.1	CA	202
				0	. A Firewall	Communicati	all UDP & TCP	Allo	165	ø	□ Co II © w10-autote	10.1	C3,	202
				0	di Firewall	Communicati P Run Task	all UDP & TCP	Allo	156	0	□ Cộ 묘 ⓒ w10-autote	10.1	C?,	202
		- L		θ	🏚 Firewall	,O Scan Path	all UDP & TCP	Allo	155	0	□ \$ \$ \$ \$ w10-autote	10.1	C3,	202
		- 1	3 / 965			Create Excl	usion							+
			SCAN COM	APUTERS	RESOLVE 🗢	ACTIONS 1	~							K © 1 © 🖨
eser PROTECT	r								G⊽ Comput	er Name	QUICK LINKS 👻 🕜	HELP 🗢 💡	R ADMINISTRA	
DASHBQARD														
	Settings	Do not t	trigger networl	k detectio	ons for:									
	Target Preview				ng the selection criteria.									
					xclusion criteria:									
		😑 fo	und in network	traffic be	etween C:\Windows\Syst etween C:\Windows\Syst	tem32\svchost.ea	e and 40.69.218.62							í.
		😑 fo	und in network	traffic be	etween C:\Windows\Syst etween C:\Windows\Syst	tem32\svchost.ea	e and 192.168.30.186							
		🤒 fo	und in network	traffic be	etween C:\Windows\Sys	tem32\svchost.ex	e and 10.1.190.13							-
		· ·	Some versio	ons of the	security products may p	ot support all excl	usion criteria. More informatio							
					Detection & context									
	>				Exclude by detection,	application & IP a	ddress							
					IP address Exclude detections fro	The state of the s								
		Exclusio			Elicipoe detections ind	im in address								
				0	Detection Exclude each detection									
					Exclude each detectio									
				0	O Application Exclude application fro	om network detect	ions							
					cicate approximation in									
		Auto-re	solving	~	Resolve matching alert	ts								
		Target		All										
		Commer (for all er	nt											
		(tor all ei	iciusions)											
											li			
				FINISH	CANCEL									
				T PRIMIT	Connect									

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:

eser	PROTECT		G ⊂ Computer Name QUICK LIN	iks ⊽ ⊘ help ⊽ Å a	
	New Policy Policies > Enable Secure Browser				
A	Basic Settings	ESET Endpoint for Windows	~	Q Type to search	? ^
व		DETECTION ENGINE	BASIC		• • •
ä	Assign	UPDATE	 	(8) ≥ 8.0	0
0	Summary	NETWORK PROTECTION	WEBSITES REDIRECTION		
-		WEB AND EMAIL	○ ●	(€ ≥ 8.0	0
φ			 Protected websites 	(8) ≥ 8.0 Edit	0
°°		Email client protection	 Secure online banking and payment payment payment 	ges	0
··· >		Web access protection	SECURED BROWSER		
		Anti-Phishing protection	 Enable enhanced memory protection 	€ ≥ 8.0	0
		Web control	🔾 🌒 🖩 Enable keyboard protection	(€ ≥ 8.0 ✓	0
		Secure Browser 1	○ ● 🗲 Configure Secure Browser interactive al	erts	
		DEVICE CONTROL			
		TOOLS			
		USER INTERFACE			
		OVERRIDE MODE			
		OVERRIDE MODE			-
•		BACK CONTINUE FINISH	CANCEL		

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