ESET Tech Center

Knowledgebase > ESET PROTECT On-prem > Add and modify Device control rules and create a Device control report in ESET PROTECT (9.x-10.x)

Add and modify Device control rules and create a Device control report in ESET PROTECT (9.x-10.x)

Mitch | ESET Nederland - 2023-03-24 - Comments (0) - ESET PROTECT On-prem

lssue

- You want to manage Device control rules on client computers in ESET PROTECT
- You want to create a Device control report
- <u>Using Device control in ESET endpoint products</u>

Solution

- 1. Add a Device control rule on client workstations using a policy in ESET PROTECT
- 2. <u>Edit or remove an existing Device control rule on client workstations</u> <u>in ESET PROTECT</u>
- 3. <u>Create a Device control report template</u>
- 4. Add a new Device control Dashboard report

I. Add a Device control rule on client workstations using a policy in ESET PROTECT

In this example, we block access to all Bluetooth devices for all users.

- 1. Open the ESET PROTECT Web Console in your web browser and log in.
- 2. Click **Policies** → **New Policy**.

ese	PROTECT		G ♥ Computer Name QUICK LINKS ♥ ③ HELP ♥	옷 ADMINISTRATOR 글 LOGOUT
		Policies :	ACCESS GROUP Select 🖞 SHOW UNASSIGNED 🧹 🔯 Built-in Policies (35) Tags	
딮		Policies ,P	ADD FILTER	PRESETS V
		^ All	NAME POLICY PRODUCT TAGS	DESCRIPTION
ŭ		V 🖉 Custom Policies	Application reporting - Report FSET Management Agent	ESET Management Agent will
নি		 Built-in Policies 	Connection - Connect avery 6 ESET Management Agent	Agent default replication inter
		ESET Endpoint for Android (2+)	Connection - connect every o ESET Management Agent	Paglicetica internal forum to 1
_ @	Policies	ESET Endpoint for Mindows ESET Endpoint for Windows	Connection - Connect every 2 ESET Management Agent	Perfication interval for up to 1
<u>~</u>	Notifications	ESET File Security for Windows Ser	Connection - connect every o Eser Management Agent	The most ensure and ensure
ч 0,-		B ESET Full Disk Encryption	General - Maximum protection ESET Virtualization Security	Process and a third for 50
		ESET Mail Security for Microsoft Ex	General - Kecommended setti ESET Virtualization Security - S	Recommended settings for ES
		ESET Management Agent	Antivirus - Balanced ESET Endpoint for macUS (OS	ESET Security Product for OS
		③ ESET Virtualization Security - Prote 🗸	Antivirus - Maximum security ESET Endpoint for macOS (OS	Taking advantage of advanced
		Tags ,O	Device control - Maximum sec ESET Endpoint for Windows	All devices are blocked. When
		EVET	Device control - Read only ESET Endpoint for Windows	All devices can only be read
		Lati	Firewall - Block all traffic exce ESET Endpoint for Windows	Block all traffic except connect
			Logging - Full diagnostic logg ESET Endpoint for Windows	This template will ensure that
			Logging - Log important even ESET Endpoint for Windows	Policy ensures that warnings,
			Antivirus - Balanced ESET Endpoint for Windows	Security configuration recom
			Antivirus - Maximum security ESET Endpoint for Windows	Taking advantage of machine I
			Visibility - Balanced ESET Endpoint for Windows	Default setting for visibility. St
			Visibility - Invisible mode ESET Endpoint for Windows	Disabled notifications, alerts,
E				⊲ ⊗ 1 ⊙ ⊗

- In the **Basic** section, type the name of the new policy under **Name**. The **Description** section is optional.
- 1. Click **Settings** and select **ESET Endpoint for Windows** from the drop-down menu.
- Select **Device Control** and click the toggle next to **Enable Device** control to enable it. Restart the client device for this change to take effect.
- 1. Repeat steps 1 and 2 and click **Edit** next to **Rules**.

ese	PROTECT			Computer Name	QUICK LINKS 🔻 🔘) help 🗢 🕺 Administrator	E LOGOUT
		New Policy					
G		Policies > Device Control Policy	4				
A					-		
		Basic	ESET Endpoint for Windows	Ÿ	5 ^a	Type to search	?
		Assian	DETECTION ENGINE	BASIC		• • •	. +
		Summary	UPDATE	O 🔹 🖗 Enable Device control		4	0
	Policies		NETWORK PROTECTION	O ⊕ ∲ Rules		Edit	0
			WEB AND EMAIL	O		6	0
			OVERRIDE MODE				
			BACK CONTINUE FINISH	CANCEL			

1. Click **Add**.

Rules								? 🗆 X
Name	Enabled	Туре	Description	Action	Users	Severity	Notify	user Q
Add	Edit	Remov	ле Сору	£			•	¥
							Save	Cancel

 Next to Name, type a name for the new rule. Next to Device type, select Bluetooth Device from the drop-down menu. Next to Action, select Block from the drop-down menu. To make the rule more specific, type in the Vendor, Model, and Serial of devices you want to target. Next to Logging severity, select Warning from the drop-down menu and click OK.

Wildcards

For Vendor, Model, and Serial fields, the wildcards * and ? may be used in ESET Endpoint Security and ESET Endpoint Antivirus version 10 and later.

An asterisk (*) represents a string of zero or more characters. A question mark (?) represents a single character.



1. The new rule will be displayed in the **Rules** list. Click **Save**.

R	ules							?	οx
	News	Frablad	.	Description	A		c	N - 414	
	Name	Enabled	Туре	Description	Action	Users	Severity	Notity user	<u>u</u>
	Block Bluetooth	\checkmark	Bluetooth Device		Block	All	Always	\checkmark	
	Add Edi	it Rem	iove Copy		*		A	v	-
								Save Ca	ncel

1. Click **Assign → Assign.**

eser	PROTECT			G ▼ Computer Name	QUICK LINKS 🗢	⑦ HELP ♥ Å ADMINISTRATOR	LOGOUT S9 min
		New Policy					
딮		Policies > Device Control Policy					
A							
		Basic Settings	ASSIGN UNAS	IGN			
Đ		Assign	TARGET NAME	TAF	RGET DESCRIPTION	TARGET TYPE	۲
⇔		Summary					
	Policies				NO DATA AVAILABLE		
φ							
γ.							
۵	COLLAPSE		BACK CONTINU	FINISH CANCEL			

1. Select the check box next to each computer or group you want to

assign the rule to and click **OK**.

Select targets							×
Groups	* A O ~ O	SHOW SUBGROUPS Tags	. 🗸	ADD FILTER PRI	SETS 🗢		
∧ 🗀 All (4)							
Lost & found (4)		K NAME TAGS	STA	MU MO	LAST CONNECTED	ALE	10
└─ └─ Windows computers			A		2021 Feb 19 15:00:03	2	0
└ ✓ I Linux computers			0	Un	2021 Feb 19 14:59:55	1	0
Mac computers			~	Up	2021 Feb 19 14:59:55	0	0
Computers with outdated of Computers with outdated of	op 🗹 🖵 🖓 🖵	-	0	Up	2021 Feb 19 14:59:19	1	0
Problematic computers	L						
Not activated security proc	uct						
🗌 🗸 🛅 Mobile devices							
	2 ITEMS SELECTED						
	2 TEMS SELECTED.						
			\mathbf{i}		K	③ 1 ④	
TARGET NAME		TARGET DESCRIPTION		TARGET TYP	°E		6
				Computer			
				Computer			

1. Click **Finish** to apply the policy on the selected computers.

II. Edit or remove an existing Device control rule on client workstations in ESET PROTECT

 Click Policies, expand Custom Policies, click ESET Endpoint for Windows. Click the policy you want to edit and click Edit.

eser	PROTECT		Ga マ Comput	ter Name	QUICK LINKS 🗢 🕜 HELP 🗢	A ADMINISTRATOR ☐ LOGOUT
		Policies :	ACCESS GROUP Select	DW UNASSIGNED	ESET Endpoint for (3)	
돠		Policies ,O	ADD FILTER	Actions Show Details		
A		^ All	NAME	Audit Log	TAGS	DESCRIPTION
úu		Custom Policies	Exclusion Policy	Tags	ows	
Þ		ESET Management Agent	Example policy	Duplicate	ows	
 		C Built-in Policies	Device Control Policy	 Delete Export 	ows	
Ф Ъ 	Polices Notifications Status Overview More >	B ESEL ENDOINT for Marchael (L4) D ESET Endopoint for Marchael (L4) D ESET Endopoint for Windows ESET Field Diak Encryption D ESET Full Diak Encryption D ESET Mail Security for Microsoft Ex. Tags P ESET		Change Assignment + Assign computers + Assign groups Change Assignment Access Rights Access Group	5	
E			ACTIONS 🗢 NEW POLICY	Assign 🗢		

1. Click **Settings**, select **Device control** and click **Edit** next to **Rules**.

ese	PROTECT		Gマ Computer Na	me QUICK LINKS 🗢	⊘ help マ	∃ LOGOUT >9 min
		Edit Policy				
딮		Policies > Device Control Policy				
A						
		Basic	ESET Endpoint for Windows		Q Type to search	?
		Settings	DETECTION ENGINE	BASIC	2 0 • +	
Þ		Assign	UPDATE	○ ● ∮ Enable Device control	1	0
a		Summary		○ ● ∮ Rules	Edit 🖧 Replace 🗸 🖵 Replace 🗸	- 0
۲	Policies			O 🛛 🗲 Groups	Edit	0
φ			WEB AND EMAIL			
₽-			DEVICE CONTROL (2)			
			TOOLS			
			USER INTERFACE			
			OVERRIDE MODE			
E			BACK CONTINUE FINISH	SAVE AS CANCEL		

- 1. To edit or remove a rule:
 - **Edit a rule**-Select the rule and click **Edit**. After the edits are made, click **OK.** Click **Save** to confirm the changes.
 - Remove a rule-Select the rule and click Remove. Click Save to confirm the changes

ł	Rules								? 🗆 X	<
			_							
	Name	Enabled	Туре	Description	Action	Users	Severity	Notify	user 🔍	
	Block Bluetooth		Bluetooth Device		Block	All	Always	\checkmark		
			1							
			1							
			I							
	L 1		1							
									-	
	Add Edi	t Rem	love Copy		*		A		¥	
							-		A 1	
							- L	Save	Cancel	

1. Click **Finish** to save the changes in the policy.

III. Create a Device control report template

1. Click **Reports** → **New Report Template**.

ese	PROTECT			द्धि ⊽ Computer	Name QU	JICK LINKS ♥ ⑦ H	ELP ♥ Å ADMINI	STRATOR I LOGOUT
		Categories & Templates Scheduled Reports	:					
G		Templates ACCESS GROUP Select	Tags 🗢	P Type to search				C
A		Antivirus detections	Antivirus de	etections				Î
¥ 8 I © ¢ ÷ :	Reports Tasks Installers Policies Notifications Status Overview More	Audit and License Management Automation Computers Dynamic Threat Defense Email servers Enterprise Inspector Firewall detections Full Diak Encyption Hardware inventory Network Quarantine Server performance	New Report Template	 Control detections Active antivitys detections that weren't handled. To resolve an active detection. Control detections Control detections	Control of the stochastic	 Courts of Artive detections arreadward arreadwarreadward arreadward arreadward arreadward arreadward arre	Agrettes virtual activite last scath angenged byties angenged byties angenged byties angenged byties angenged angengenged angengenged angenged angenged angenged	 Control of the second of the se
E		NEW REPORT TEMPLATE	products in last 30 days grouped by Detections in last 30 days grouped by detection method	(a) High severity detection events in last 7 days Unresolved	Image: Scans with	Last scan Computer counts grouped by time elassed since last	Mobile device last scan Mobile devices counts grouped by	Cans in last 30 days Scans performed in last 30 days

In the Name field, type a name for your report. Select
 a Category for your report. The Description field is optional.

ese	PROTECT			Ga ♥ Computer Name	QUICK LINKS 🗢	③ HELP マ	A ADMINISTRATOR	B LOGOUT
		New Report Template						
됴		Reports > Device Control Logs						
A								
<i>ĩ</i> .	Reports	Basic	Basic					
		Data	Name					
		Sorting	Device Control Logs					
۲		Filter	Description					
¢		Summary						
η.			Tags					
			Select tags					
			Category					
			BACK	FINISH CANCEL				

1. Click **Chart** and select the check box under **Display Table**.

ese	PROTECT			Gor Computer Name	QUICK LINKS 🗢	⊘ HELP マ	& administrator	B LOGOUT
		New Report Template						
G		Reports > Device Control Logs						
A		Basic	Table					
	Reports	Chart	Display Table					
		🛦 Data 🔪						
		Sorting	Chart					
		Filter	Display Chart					
		Summary						
			Chart Type					
			Bar Chart	~				
			Title for X axis					
			Title for Y axis					
			Proviou					
			Freview					
			Show Preview					
								-
			BACK CONTINU	E FINISH CANCEL				

1. Click **Data** → **Add Column**.

ese) protect		[G 🗢 Computer Name	QUICK LINKS 🗢	⊘ HELP マ	A ADMINISTRATOR	B LOGOUT >9 min
		New Report Template						
돠		Reports > Device Control Logs						
A								
ži	Reports	Basic	A Table Columns					
Þ		A Data	Add Column					
		Sorting	Preview					
©		Filter						
φ γ		Summary						
E			BACK	FINISH CANCEL				

1. Expand the **Computer** category, select **Computer name** and click **OK**.

Please select item	×
✓ Type to search	*
Client tasks	^
 Client triggers Common 	
Computer	
Computer Computer	
Computer hardware status	
Computer is master	
Computer muted	d
Computer tags	
Is Mobile	
Managed computer	Ŧ
OK CANCEL	

 Repeat Steps 4 and 5 until all items listed in the table below are added to the **Table Columns** section and click **Finish**. You can select other items based on your preferences.

Category	Item			
Computer	Computer name			
Device control	Device			
Device control	Action performed			
Device control	Time of occurrence			
Device control	User			

ese	PROTECT		G ♥ Computer Name	QUICK LINKS ♥ ③ HELP ♥	온 ADMINISTRATOR 글 LOGO >9 min	DUT
		New Report Template				
G		Reports > Device Control Logs				
A						
	Reports	Basic	Table Columns			
Þ		Data	Computer . Computer name	↓ ~ ⁷ ∰		
		Sorting	Device control . Device	↓↑2		
۲		Filter				
ф 		Summary	Device control . Action performed	↓↑∠" ≞		
v-			Device control . Time of occurrence	↓↑27		
			Device control . User	↑ ~ ⁷ ₪		
			Add Column			
			Preview			
			i i concor			
			Show Preview			
E	COLLAPSE		BACK CONTINUE FINISH CANCEL	L		

- IV. Add a new Device control Dashboard report
 - 1. Click **Dashboard**. Click the plus icon to add a new dashboard.

eser) PROTECT								LOGOUT →9 min
	DASHBOARD	Dashboard 💿							0
돠	COMPUTERS	◀ Status Overview	Security Overview	Computers	Server Performance Status	Antivirus detections	s Firewall dete	ctions ESET applications	Dy. ▷ +
A	DETECTIONS								Â
	Reports	노	4	~	0	•	2	A	0
	Tasks	Total number	of devices	Ok		Attention require	ed	Security risks	
	Installers								
	Policies	_	Device	status			Connectio	n status	
	Notifications	Ļ	8		<u>VM</u>				
	Status Overview								
	More >			Ok Attention required Security risk Total	0 d 1 1 2	4		1 day	4
			Product ver	sion status			Manageme	nt status	
	COLLAPSE	100%	Endpoint Up to date Out	Server dated Unknown	Mobile	2 Managed & Protected ⑦	4 Managed ⊘	0 C Unmanaged Rc Ø)7 gue 3

1. Type a name for your new dashboard and click **Add Dashboard**.

?	Add Dashboard New dashboard's name	×
	Device control	
	ADD DASHBOARD CANCEL	

1. Click the plus icon.

eser	PROTECT			দািক বে	omputer Name	QUICK LINKS 🔝	③ HELP マ & ADMIN	STRATOR 🕞 LOGOUT
	DASHBOARD	Dashboard 💿						c
돠	COMPUTERS		Server Performance Status	Antivirus detections	Firewall detections	ESET applications	Dynamic Threat Defense	Device control ⊚ ▷ +
A	DETECTIONS							
	Reports							
	Tasks							
	Installers							
	Policies		+		+		+	
	Notifications							
	Status Overview							
	More >							
			+		+		+	
	COLLAPSE							

 Navigate to the report you created in <u>Section III</u> (Device Control Logs, in this example), select it and click OK.

Please select template ×
P Type to search
List of computers from where ESET Management Agent has first time connected to ESET PROTECT in last 7 days
Computers grouped by hardware detection reliability status Computers grouped by their hardware reliability status. Hardware reliability status indicates, whether machine is suitable for cl
Example Computers set as master for cloning List of computers that are set as masters for cloning. Cloning and re-imaging computers from such devices should not cause pr
Computers with cloning questions List of computers that have unresolved cloning questions. This might indicate that the same Management UUID is being report
Computers with problems Operating system or managed products reported problems, with their detail descriptions
Computers with unreliable hardware detection List of computers, which are not providing enough information for reliable hardware detection. Hardware detection should be d
O Detection engine update status ratio Ratio between updated and not updated detection engine reported by security products
I Device Control Logs
ESET Virtualization Security Appliances statuses overview Count of EVSAs grouped by their status
ESET Virtualization Security Appliances with problems Operating system or managed products reported problems, with their descriptions
Installed applications Overview of installed applications on computers. By default, only ESET applications are reported
OK EDIT TEMPLATE CANCEL

Your dashboard is now available. When a Bluetooth device is blocked by Device control, each blocked device is listed in the new dashboard report.