ESET Tech Center

Knowledgebase > Endpoint Solutions > Using Device control in ESET endpoint products

Using Device control in ESET endpoint products

Ondersteuning | ESET Nederland - 2022-12-28 - Comments (0) - Endpoint Solutions

Solution

- <u>Define rules</u>
- <u>Supported external devices</u>
- Logs and reporting
- Example

Details

Device control is designed to monitor the use of devices on endpoint machines. You can specify how users can access devices (CD/DVD/USB, etc.) by defining rules for media, devices and users on client workstations. Device control blocks unauthorized media and prevents malware from spreading via removable media.

Define rules

Administrators can define rules for specific types of devices to be used on endpoint machines. Rules can be set either per user or per group of users. Device control is integrated with directory services to make use of Active Directory groups for configurations.

The flexible Device control rules allow access to be controlled by individual users or user groups using the device parameters such as serial number, manufacturer ID, model and more. The control permissions can be set to read-only, read/write or block access for individual users or user groups. The detailed access and scan logs simplify policy enforcement and compliance reporting.

Supported external devices

- Disk Storage
- CD/DVD
- USB storage
- USB printer
- FileWare Storage
- Bluetooth Device

- Smart card reader
- Imaging Device
- Modem
- LPT/COM port
- Portable Device
- All device types

If you set a rule that blocks access to an inserted external device, a notification window will alert the user when they insert a CD/DVD, or connect an external storage device. The notification window will prompt them to scan its contents for malware. The user can then select **remember this action** so that it is automatically performed in the future.

Logs and reporting

Detailed logging is available for Device control. Logs include the following information:

- Time of event
- Device
- User name
- User SID
- Group name
- Group SID
- Status
- Device details
- Event details

Example

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

- 1. Open the main program window of your Windows ESET product.
- 2. Press the F5 key to open Advanced Setup.
- 3. Click **Device Control** and click the slider bar next to **Enable Device control**. Restart your computer for the change to take effect.

(EGET) ENDPOINT SECURITY			σ×
Advanced setup		Q,	× ?
DETECTION ENGINE	BASIC	A computer restart is needed for this	change to take effect.
UPDATE 1	Enable Device control		0
NETWORK PROTECTION	Rules	Edit	0
WEB AND EMAIL	Groups	Edit	0
DEVICE CONTROL			
TOOLS			5
USER INTERFACE			
			5
Default		Ф ОК	Cancel

1. Repeat steps 1-2 and click **Device Control** \rightarrow **Edit** next to **Rules**.

			οx
Advanced setup		Q,	× ?
DETECTION ENGINE	BASIC	A computer restart is needed for this cha	ange to take effect.
UPDATE 1	Enable Device control	× .	0
NETWORK PROTECTION	Rules	Edit	0
WEB AND EMAIL	Groups	Edit	0
TOOLS			5
USER INTERFACE			
			3
Default		© ОК	Cancel

1. Click **Add**. Type a **Name** that does not use any special characters for your new rule. Do not include extra spaces after the product name, as

this can keep your rule from functioning correctly. Select **Bluetooth Device** from the **Device type** drop-down menu and select **Block** from the **Action** drop-down menu. To make the rule more specific, type the **Vendor**, **Model**, and **Serial** number of devices you want to target. Next to **Logging severity**, select an option 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.

(International Contraction Contractico Con	SECURITY		□ ×
Rules		(ENDPOINT SECURITY	×
		Add rule	?
Name	Enabled Type	Name	Example1
		Rule enabled	
		Apply during	Always
		Device type	Bluetooth device ~
		Action	Block
		Criteria type	Device ~
		Vendor	
		Model	
Add Edit	Delete Copy Populat	te Serial	
		Logging severity	Always
			Edit
		Notify user	
			ок

1. Click $\mathbf{OK} \rightarrow \mathbf{OK}$ to save your rule and exit Advanced setup.

Your new rule will be listed in the **Rules** window. You can disable or reenable the rule, edit its properties, make a copy, etc. If you add more rules, you will be able to manage them the same way.

(ESET) ENDPOINT SECURIT	Y						ПХ	
Advanced setu	e Advanced setu	p - ESET Endpoir	nt Security				- 0	×
ANTIVIRUS	Rules							?
UPDATE								Q,
FIREWALL	Name	Enabled	Туре	Description	Action	Users	Severity	
WEB AND EMAIL	Example1	~	Bluetooth Device	2	Block	All	Always	
DEVICE CONTROL								
TOOLS								
USER INTERFACE								
								_
	Add Edit		e Populate				* ^ Y	
							ОК Са	ncel
Default					6	ок	Cancel	