Close open doors with Device Control!

My experiences and simple steps

Jürgen Rinelli



Jürgen Rinelli Am Eichet 6a 85302 Alberzell info@success.eu.com

Table of contents

1. A few words	
2. Device Control an overview	4
3. Blocking Devices	5
4. Permit temporary access	9
5. Trusted device lists and general authorisations	
6. Closing words	14
7. About the author	

1. A few words

"Hey darling, I've found a USB stick that's shaped like a guitar. I wonder what's on it?"

"Cool, let's go and have a look."

The stick in the shape of a black guitar is quickly inserted. After the familiar 'ping' that indicates that Windows has recognised the device, loud metal music sounds from the speakers. When an animation then shows a guitar disintegrating to make way for a skull, Paul realises that it was probably not such a good idea to plug the stick into the company computer. He quickly unplugs it, but the image remains. The keyboard is locked. Switching off hard and switching on the system again does not help. Trembling, he calls IT, who quickly brushes him off.

"Paul, I don't have time! We've been attacked. Our data storage has been encrypted. Production is at a standstill, everything is down."

...

Do you know this? If not yourself, then you've probably heard of such incidents. What happened here? Who is to blame?

What happened is that someone connected something to the company laptop and infected the company network with malware.

Who is to blame here? On the one hand, you can certainly blame poor Paul from the example above. On the other hand, however, I also have to blame the company management. Company management, not necessarily just the IT management. Because from my experience I know that we IT people like to point out dangers and introduce tools to avert such scenarios. Unfortunately, there is rarely a budget for this. Too often - even today in 2024 - the danger of cybercrime is still underestimated.

I recommend that every IT professional always protect themselves in pointing out dangers and necessary tools, in writing official e-mails. That's our job. The decision ... then lies with the company management, which has to authorise the funds.

Every admin is aware that device control is an important instrument in securing endpoints. In this e-book, I would like to show that it can also be set up and maintained easily and clearly.

As in every e-book in this series, I use Endpoint Central from ManageEngine with the Endpoint Security Add-on as my preferred product, as an example of how easy I can make my life as a digital caretaker.

Have fun 😊

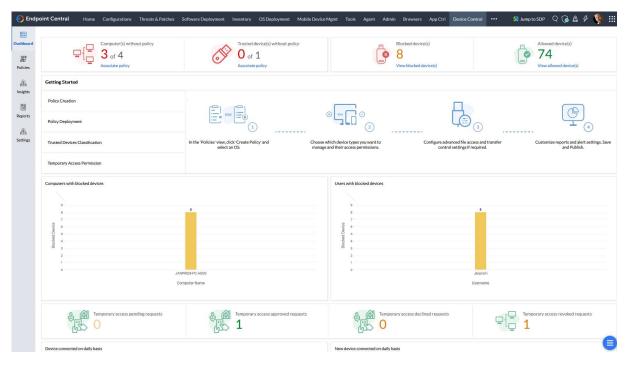
2. Device Control an overview

What a device control should provide for me are

- Dashboards with current status overviews
- The ability to define trusted devices in groups
- Grant temporary access without having to rework it yourself
- Clear definition of device policies
- Insights and reports

I want to be able to get a quick overview and also quickly block or release devices. If possible, a user should also be able to make a request for release via the block dialogue.

I have all this in the Device Control of ManageEngine. While I can get it as an add-on in Endpoint Central or included in the Security Edition, it is also available as standalone software.



Example of device overviews

✓ Insights	Device Summary (1)										
Managed Computers											
Device Summary	Removable storage devices										
Device Status by Computer		Filter By: Last A	ction *	OS Platform *						Total Reco	ords Q 🏛 🏄
Computers by Device Type	Windows portable devices	Device Name	Vendor ID	Product ID	Serial Number	Custom Device Name	Last Connected Computer	Last Connected User	OS Platform	Last Action	Last Connected
 Temporary Access Status 	Modems	Flash Drive	090C	1000	FBD11093003	-1	JANPREM-PC-ASUS	Janprem	##Windows	Blocked	25/03/2024 14:
Device Exemptions	Wireless network adapters	Flash Drive	058F	6387	2563D9B6	-1	JANPREM-PC-ASUS	Janprem	# Windows	Allowed	25/03/2024 10:
Device Type Exemptions	Reading devices		0501	0007	2000700		341110110100	Surpren		1 - 2 of Total Records	
Device Type Exemptions	Mouses									1-2 of total Records	23
	Keyboards										

3. Blocking Devices

Blocking removable storage devices on USB ports is a simple task. To do this, I go to Policies / Create Policy / Windows

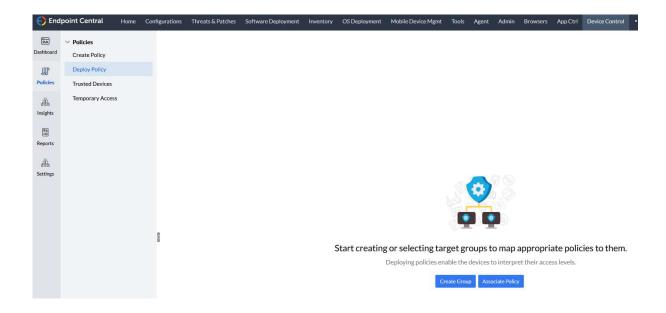
🛟 Endj	point Central Horr	e Configurations T	hreats & Patches	Software Deployment	Inventory	OS Deployment	Mobile Device Mgmt	Tools Agent	Admin Browsers	A
Dashboard	 Policies Create Policy 	All Polic	ies 🕕							
@ Policies	Deploy Policy Trusted Devices	+ Create P		to Trash Filter By : OS Platform	Status *	OS Platform * Authorized Device		ed Devices	Last Modified By	
	Temporary Access	É Mac	ick USB	## Windows		0	1		janprem	

In the next dialogue, I simply block all Removable Storage Devices. I leave the alert dialogues here as standard.

🜔 End	point Central Home Conf	igurations Threats & Patches Software Deployment Inventory	OS Deployment Mobile Device Mgmt Tools	Agent Admin Browsers App (Ctrl Device Control •••	51 Jump to SDP 🛛 🌀 🧟 🔗 😻 🏭
0-b	✓ Policies	Tutorial-Block USB Add Descrip	tion			
Dashboard	Create Policy	Device Access Control				
Ø	Deploy Policy					
Policies	Trusted Devices	Removable storage devices ?		Block *	Advanced Settings 🗞	
品 Insights	Temporary Access	Block connection bus of Removable storage	devices via			
Reports		CD-ROM		No Change *		
186		Windows portable devices ?		No Change 👻		
Settings		Apple devices ?		No Change *		
		Bluetooth Adapters		No Change *		
		Printers		No Change *		
		Modems		No Change *		
		Wineless network adapters		No Change *		
		Imaging devices ?		No Change 👻		
		Serial ports (COM)		No Change 👻		
		View more 😔				
		• Device Audit Settings				
		Monitor all device activities				
		Generate reports from agent every	24 🗘 hours -			
		Send blocked device details to server immediately				
		Alert Settings				
		Notification type	Off Default Notification ? Ocustom ?	Notification ?		
_		Alert title *	Device Access Restricted			
		Alert message "	This device has been restricted. Contact your System Administrator			
		Enable temporary access request				
			Save & Publish	Save as Draft Cancel		
			© 2024 Zoho Corporation	Private Limited. All rights reserved.		

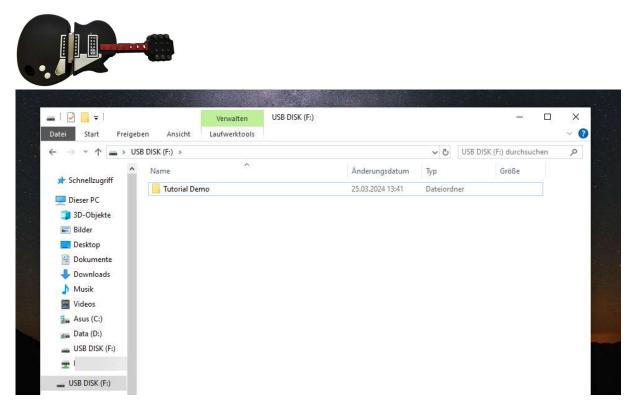
The policy is saved after Save & Publish. Don't worry - nothing is distributed yet. This happens in the next step when I assign this policy to a group.

I have already created a test group with a laptop for demonstration purposes, so I will now go to "Associate Policy":



Here I select the group to which I want to apply a policy (1) and select the desired policy (2) and (3). Deploy (4) then applies the policy.

On my test system, I had plugged in one of these great guitar sticks before deployment and gained access:



Close open doors with Device Control! - from Jürgen Rinelli

After deployment, it now looks like this when I plug in the stick:

	Device Access Restricted
This device has been	restricted. Contact your System Administrator
Gerätename	USB Flash Disk USB Device
Hersteller des Gerätes	(Standard disk drives)
Gerätetyp	DiskDrive
Gerätestatus	Blockiert
	Temporären Zugriff anfragen

No USB stick is displayed in Explorer either:

💻 📝 📗 🖛 Dieser	PC		– 🗆 X
Datei Computer	Ansicht		~ 📀
$\leftrightarrow \rightarrow \neg \uparrow \blacksquare \flat$	Dieser PC	~ Ö	Dieser PC durchsuchen
📌 Schnellzugriff	V Ordner (7)		^
📃 Dieser PC	3D-Objekte	Bilder	
3D-Objekte			
📰 Bilder	Desktop	Dokumente	
C Desktop			
Dokumente	Downloads	Musik	
🕹 Downloads		- - '	
J Musik	Videos		
Videos	Nucos		
🚂 Asus (C:)	Constant I autoratio (2)		
🚛 Data (D:)	✓ Geräte und Laufwerke (3)		
🛫 Rinelli-	Asus (C:)	Data (D:)	
🥩 Netzwerk	57,1 GB frei von 203 GB	677 GB frei von 689 GB	
	BD-ROM-Laufwerk (E:)		
	✓ Netzwerkadressen (5)		
		FRITZ	
		× .	~
15 Elemente			

I could request a permission for this device via the dialogue or the taskbar icon. This request looks like this: (Sorry for the German dialog – it's a German system I am running my tests)

4	Temporärer Gerätezu	ıgriff	- ×
Temporärzugriffanfrage Temporärzugriffanfrage für Gerät erheben Code anwenden	Gerätetyp	- All Devices -	~
Gerätezugriff durch Codeanwendung erlange	Gerätename	[None Selected]	erät auswählen
	Zugriffsdauer	1 Hour	~
	Grund	Anfrage	

But who can tell me that this device is really secure if I haven't checked it myself on a security system? I always like to use a machine with a virus scanner that is independent of the network.

There will always be discussions if a device is blocked and there will always be a very important document on the stick. For my part, I am always very tough and short-tempered. Because what is allowed is what I issue. The device is then placed in a trusted device group or temporarily released by me after the stick has been scanned on one of the security machines. Temporary authorisation may be necessary if, for example, I have a consultant from an external company in the building who has a presentation on the stick - after I scanned it.

We will see what this looks like in the next point.

4. Permit temporary access

 ${\rm I}$ can see all blocked devices and on which computers they are blocked via the Blocked Devices dashboard.

board F icies	무튼 3	omputer(s) without policy 3 of 4 ssociate policy	Trusted device(s 0 of 1 Associate policy	without policy		Blocked device(s) 2 View blocked device(s)			Allowed 74 View allo		
ehts	Getting Started										
Endp	oint Central Home	Configurations Threats & Patches	Software Deployment Inventory OS E	Neployment Mobile Devi	evice Mgmt Tools Agent Ad	dmin Browsers App	Ctrl Device Contre	ol ••• I	Jump to SDP	Q 🔂 🙆 🤣	1
_	oint Central Home	Blocked Devices ()	Software Deployment Inventory OS E	Deployment Mobile Dev	evice Mgmt Tools Agent Ad	dmin Browsers App	Ctrl Device Contro	əl ••• <u>5</u>	Jump to SDP	Q 🐻 💩 🦨	÷ 🚯
	✓ Reports		*	Deployment Mobile Devi	evice Mgmt Tools Agent Ad	dmin Browsers App	Ctrl Device Contro	<u>ء</u> נ	il Jump to SDP		
icoard P cies	 Reports Device Audit Blocked Devices 	Blocked Devices ()	*	DS Platform *	evice Mgmt Tools Agent Ad	dmin Browsers App		Domain	Jump to SDP	Q 🍙 💩 🦨 Total Records J Username	
) oard	 Reports Device Audit Blocked Devices File Tracing 	Blocked Devices ()	Filter By: All Period V	DS Platform * Vendor ID Pr						Total Records	I Q ==

Here I can view the devices and also find the serial number.

I can easily grant temporary access via Insights / Managed Computers and by selecting the computer to which the stick is connected.

🛟 Endr	ooint Central Home Ci	onfigurations Threats & Patches	Software Deployment Inve	ntory OS Deployment Mobile De	evice Mgmt Tools Agent Admi	n Browsers App Ctrl Devi	ce Control ••• 50 Jump t	osdp 🔾 🕝 🗟 🔗 🔇 🎛
0.6	✓ Insights	🔀 Managed Computers 🛈						
Dashboard	Managed Computers							
P	Device Summary		OS Platform *					Total:4 Q 🌐
Policies	Device Status by Computer	Computer Name	Domain	OS Platform	Last Contact Time	Associated Groups ?	Applied Policy Count	Associated Policy Count
#	Computers by Device Type	Janprem-Lenovo	WORKGROUP	III Windows	16/03/2024 20:26:10	0	0	D
Insights	✓ Temporary Access Status	JANPREM-PC	RINELLICORP	III Windows	25/03/2024 12:52:25	0	0	0
51	Device Exemptions	JANPREM-PC-ASUS	RINELLICORP	## Windows	25/03/2024 12:55:11	1	1	1
Reports	Device Type Exemptions	Sabine-Asus	RINELLICORP	11 Windows	25/03/2024 12:53:14	0	0	0
æ								1-4 of 4 25 💌
Settings								

There are lots of overviews and details, I switch to the "Device Manager" tab and select "Allow Temporary Access".

🜔 Endş	coint Central Home Co	nfigurations Threats & Patches Software Deployment Inventory OS De	eployment Mobile Device Mgmt Tools Ag	ent Admin Browsers App Ctrl Device Control	50 Jump to SDP Q 🕝 🗟 & 🦻 👯
Dashboard	 Insights Managed Computers 	JANPREM-PC-ASUS Device Friendly Name: JANPREM-PC-ASUS			
Policies	Device Summary Device Status by Computer	Groups Policies Device Audit File Trac	ing File Shadowing Device Manager		Last updated time : Jul 7, 2023, 09:33 AM 🎝 Update Now
285 Insights	Computers by Device Type	Removable storage devices Disk drive	Disk drive Manufacturer	: (Standard disk drives) (8564)	
Reports	Device Exemptions		Parent device Instance path	: U58\VID_8564&PID_1000\291826683	
A	Device Type Exemptions		Device instance path Product ID	: USBSTOR\DISK&VEN_JETFLASH&PROD_TRANS [
Settings		⊕ 🖗 Mouses	Serial Number	: 291826683	
			Custom Name Description	: : Disk drive	+
		E C C C C C C C C C C C C C C C C C C C	Status	: Disabled	Allow Temporary Access

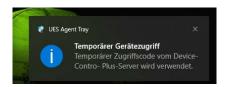
Assign a descriptive name here again (please use a naming convention in a production environment), select a user, time window and device type. Then click on "Deploy Immediately".

Close open doors with Device Control! - from Jürgen Rinelli

Name and Description					
Name*	Tutorial Test	Add Description			
Define Target					
Computer Name *	JANPREM-PC-ASUS				
User Name*	All users				
Duration Type	Fixed Window				
Duration of Access	1Hour *				
Expiry Time*	25/03/2024, 03:21 PM				
Allowed Device					How to get device path ?
					_
Device Type *	Removable storage devices *				
Allowed By	All Instances *				
		Add			
Device Type	Allowed By	Vendor ID	Product ID	Serial Number	Action
Removable storage devices	Specific Instance	8564	1000	291826683	0 D
	Deploy imr	nediately Save as Draft Gener	rate Code Cancel		

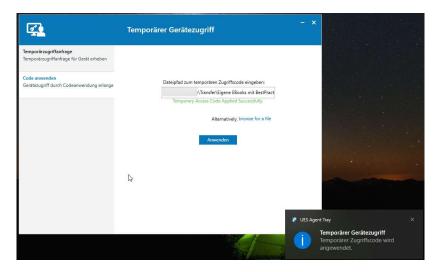
									276 8 C
+ Cre	ate 🔋 Move to Trash	Filter By: Status						🗍 View Tra	ash Total:3 Q
	Policy Name	Applied Time	Duration Type	Computer Name	Username	Device Count	Status	Expiry Time	Action
	Tutorial Test	, cita	Fixed	JANPREM-PC-ASUS	All users	1	Published	25/03/2024 15:21:44	
	TA FOR Janprem In Janp	24/07/2023 11:10:31	Fixed	Janprem-Lenovo	janprem	1	Revoked	31/07/2023 11:07:00	
	TA FOR Janprem In JAN	24/07/2023 10:53:08	Fixed	JANPREM-PC-ASUS	janprem	1	Approved	24/07/2023 11:49:43	

A message pops up on the laptop immediately:



I can then use the code that was emailed to me via the tray icon in the dialogue for temporary device access.

Hi,
Temporary access request has been provided as below.
Computer Name: JANPREM-PC-ASUS
User Name: All Users
Time Span: 1 Hour
Device
Device Instance Path
Removable storage devices
USBSTOR\DISK&VEN_JETFLA
Steps to activate temporary access :
1. Download the attachment file in this email.
 Right click the Agent Tray Icon.
3. Select Temporary Access Portal option.
4. Select the Apply Code tab.
5. Browse the file downloaded in step 1 and click Apply button.
Regards,
ManageEngine Endpoint Central



At the end of the hour, the device is automatically blocked again.

However, as we also have devices that we really needed in the company, general authorisations are required. I will show you how this can look in the next section.

5. Trusted device lists and general authorisations

Known devices such as keyboards, mice, printers, modems, biometric devices, etc., can be easily summarised in a list.

To do this, create a Trusted Device group, assign a descriptive name, select the device type and select the desired devices from the tabs.

shboard	✓ Policies	trusted-device_1423 Add Descripti	on				
En tolicies	Create Policy Deploy Policy Trusted Devices	Select Devices Select device type Removable storage devices *					
å	Temporary Access	Add existing devices Add new devices Import files					😰 How to get device p
sights							Q Search
eports		Vendor Name	Custom Name	Vendor ID	Product ID	Serial Number	Action
		Unknown	ω.		ω.	1F4ADFFE	Add
ettings		Transcend Information, Inc.	-	8564	1000	291826683	Add
		LucidPort Technology, Inc.	-	1759	5002	S21JNXBGC27764K	Add
		Toshiba America Inc	-	0480	B208	20200222017857F	Add
		ASMedia Technology Inc.		174C	1153	000000000000000000000000000000000000000	Add
		Silicon Motion, Inc Taiwan (formerly Feiya Technology Corp.)	-	090C	2000	28B0A64	Ado
		Sony Corp.	-	054C	07F9	C75A602D34CF	Add
		Vast Technologies, Inc.	-	10EC	5229	00000001004CE00000	Add
		Transcend Information, Inc.	-	8564	1000	01L23C8AH353E5Q1	Add
		Silicon Motion, Inc Taiwan (formerly Feiya Technology Corp.)		090C	2000	85DD16A	Add
		Device Lists					
							Q Search
		Vendor Name Custom Name	Vendor		Product ID	Serial Number	Act
				No data availa	Die		
				Save Save as Draft	t Cancel		

Then I need a policy via "Create Policy":

point Central Home	Configurations Threats &	& Patches	Software Deployment	Inventory	OS Depl
✓ Policies	All Policies (i)				
Create Policy	- Courte Participan	÷	La Trach	-	or
Deploy Policy	- Create Policy +	Move	to Trash Fliter By:	Status	OS P
Trusted Devices	Windows	ie	OS Platform		Authoria
Temporary Access	🗯 Mac	ick USB	Windows		0
	 Policies Create Policy Deploy Policy Trusted Devices 	 ✓ Policies Create Policy Deploy Policy Trusted Devices ✓ All Policies ① + Create Policy ▼ Windows ✓ Mac 	 ✓ Policies Create Policy Deploy Policy Trusted Devices ✓ All Policies (i) ← Create Policy ▼ Move ✓ Mac 	 ✓ Policies Create Policy Deploy Policy Trusted Devices ✓ All Policies ① ← Create Policy ● Move to Trash Filter By: ✓ Move to Trash Filter By: ✓ Mac ✓ Windows 	 ✓ Policies Create Policy Deploy Policy Trusted Devices ✓ All Policies i ✓ Create Policy ✓ Move to Trash Filter By: Status ✓ ✓ Mac ✓ Mac

Assign a name here again (1) and then select Removable storage devices / Allow trusted devices (2) from the list in our example.

ccess Control	
Removable storage devices ?	No Change 👻
CD-ROM	No Change
Windows portable devices ?	Allow Allow trusted devices
Apple devices ?	Block
Bluetooth Adapters	No Change 👻
Printers	No Change 👻
Modems	No Change 👻
Wireless network adapters	No Change 👻
Imaging devices ?	No Change 🔻
Serial ports (COM)	No Change

Now many more options open up to me. I select the trusted group I want (1) and specify that only BitLocker encrypted devices are allowed (2). File Access and File Shadow Settings are also available to me in the Device Control of ManageEngine.

Policy_1342 Add Description			
Device Access Control			
Removable storage devices 2		Allow trusted devices *	Advanced Settings 🔨
Select Trusted Devices lists	Trusted-Group1 Select Trusted Devices	ist 1 3	+
File Access Settings Block file copying from removable storage device		-	
Allow read-only permission			
Allow file creation in device by file extension(s)	Add extensions		
Maximum allowed file size	0 С КВ		
Device Access Settings			
Disable AutoRun			
Allow only BitLocker encrypted devices			
File Shadow Settings Enable file shadowing			
Specify network share path	e.g. \\computer-name\path		
Network share credentials *	Select 💌	?	
	Manage credentials		
Indicate maximum file size	0 🗘 КВ	2	
Exclude extensions	Add extensions	2	

Further down, I then specify how the audit should take place (1), which notification is displayed on the monitor (2) and whether I want to enable a request for temporary access (3).

	Monitor all device activities	
	Generate reports from agent every	24 🗘 hours 💌
	Send blocked device details to server immediately	• 1
Alert Setting	re .	
		Off Default Notification ? Ocustom Notification ?
	Notification type 2 Alert title *	Off Default Notification 2 Custom Notification 2 Device Access Restricted
	Notification type	

Finally, distribute this policy to the desired groups, as we did at the beginning of this e-book.

6. Closing words

Device control is just as important today as patching the systems. I hope I have been able to give you an insight into how easy it is to prevent devices such as those described in Paul's short story above from causing chaos when they are plugged in. It has certainly happened to all of us - even experienced admins - that we have simply plugged in a device. I help myself with device control. Because I know that my bosses are waiting for me with the most impossible new tasks that need to be done by yesterday.

With device control, I also have these aforementioned bosses well under control 😁

That's how it should be and how we love it 😊

7. About the author

MCITP, MCTS, MCP, MOS, Enterprise Administrator, Senior Software Consultant, SCCM Specialist, Author, Coach, Reiki Teacher ...

Jürgen Rinelli was born in Germany in 1970. In his eventful and often adventurous life, he has lived and worked in many countries. Whether as a businessman, manager, mechanic, trainer, diver or IT expert, he always finds a way to pursue his dreams.

