Offene Türen schließen mit Device Control!

Meine Erfahrungen und einfache Schritte

Jürgen Rinelli



P

Inhalt

1. Ein paar Worte	3
2. Device Control ein Überblick	4
3. Devices Blocken	5
4. Temporären Zugriff gewähren	9
5. Trusted Device Listen und generelle Freigaben	12
6. Schlussworte	14
7. Über den Autor	15

1. Ein paar Worte

"Hey Liebling, ich hab da einen USB Stick gefunden, der hat die Form einer Gitarre Was da wohl drauf ist?"

"Cool, lass uns nachsehen."

Schnell ist der Stick in Form der schwarzen Gitarre eingesteckt. Nach dem bekannten `Pling´, der anzeigt, das Windows das Gerät erkannt hat, ertönt auch gleich laute Metal Musik aus den Lautsprechern. Als dann eine Animation eine sich auflösende Gitarre zeigt, die einem Totenkopf platz macht, erkennt Paul, dass es wohl keine so gute Idee war, den Stick in den Firmenrechner zu stecken. Schnell steckt er ihn aus, doch das Bild bleibt. Die Tastatur ist gesperrt. Hartes Ausschalten und ein erneutes Einschalten des Systems bringen auch keine Besserung. Zittrig ruft er daraufhin bei der IT an, die ihn schnell abwimmelt.

"Paul, ich hab keine Zeit! Wir wurden angegriffen. Unsere Datenspeicher wurden verschlüsselt. Die Produktion steht still, alles steht."

...

Kennt ihr das? Wenn nicht selbst, dann habt ihr sicher schon einmal von solchen Vorfällen gehört. Was ist hier passiert? Wer ist schuld?

Passiert ist, dass jemand etwas an den Firmenlaptop angeschlossen hat und damit das Firmennetz mit Schadsoftware infizierte.

Wer ist hier schuld? Zum Einen kann man die Schuld sicher auf den armen Paul aus dem obigen Beispiel schieben. Zum Anderen jedoch, muss ich auch eine Schuld an die Firmenleitung geben. Firmenleitung, nicht unbedingt rein die IT-Leitung. Denn aus meiner Erfahrung heraus weiß ich, dass wir IT'ler gern auf Gefahren hinweisen und Tools einführen wollen, um solche Szenarien abzuwehren. Leider gibt es dafür selten Budget. Zu oft noch – auch Heute 2024 – wird die Gefahr der Cyberkriminalität unterschätzt.

Ich empfehle jedem IT'ler, sich hier immer abzusichern und schriftlich auf Gefahren und notwendige Tools hinzuweisen. Das ist unser Job. Die Entscheidung … liegt dann bei der Firmenleitung, welche die Gelder dazu bewilligen muss.

Das die Device Control ein wichtiges Instrument in der Absicherung der Endpoints darstellt, ist jedem Admin bewusst. Ich möchte in diesem E-Book zeigen, dass es auch einfach und übersichtlich eingerichtet und gepflegt werden kann.

Wie in jedem E-Book dieser Serie verwende ich Endpoint Central von ManageEngine mit dem Endpoint Security AddOn als mein präferiertes Produkt, als ein Beispiel wie einfach ich mir mein Leben als digitaler Hausmeister machen kann.

Viel Spaß 😊

2. Device Control ein Überblick

Was eine Device Control für mich mitbringen soll, sind:

- Dashboards mit aktuellen Statusübersichten
- Die Möglichkeit, Trusted Devices in Gruppen zu definieren
- Temporären Zugriff gewähren, ohne selbst nacharbeiten zu müssen
- Übersichtliche Definition von Device Policies
- Insights und Reports

Ich will mir schnell einen Überblick verschaffen können und auch schnell Devices blocken oder freigeben können. Nach Möglichkeit sollte ein User über den Block-Dialog auch eine Anfrage auf Freigabe stellen können.

All das habe ich in der Device Control von ManageEngine. Während ich sie im Endpoint Central als AddOn bekommen kann oder in der Security Edition enthalten habe, gibt es sie auch als Einzelsoftware.



Beispiel von Device Übersichten

\sim Insights	Device Summary ①										
Managed Computers	115 108										
Device Summary Device Status by Computer	Removable storage devices	Filter By: Last A	ction *	OS Platform *						Total Reco	rdsiQ III ±
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	Vireless network adapters	Flash Drive	090C	1000	FBD11093003_	-1	JANPREM-PC-ASUS	Janprem	III Windows	Blocked	25/03/2024 14:3
Device Exemptions	Imaging devices Mouses Mouses	Flash Drive	4860	6367	23630706		JANPREM-PC-ASUS	Janprem	all Windows	1 - 2 of Total Records	25/05/2024 10:5

3. Devices Blocken

Removable Storage Devices an USB Ports blocken, ist ein einfacher Task. Hierzu gehe ich auf Policies / Create Policy / Windows

🗧 End	point Central	Home Conf	figurations Threat	s & Patches	Software Deployment	Inventory	OS Deployment	Mobile Device Mgmt	Tools Agent	Admin Browsers A
0-lt	✓ Policies		All Policies)						
Dashboard	Create Policy			= E Mar	a to Treak	Status =	OS Blatform			
P	Deploy Policy		- Create Policy		e to Trash Filter By :	Status *	OS Platform *			
Policies	Trusted Devices		Windows	ie	OS Platform		Authorized Device	s Unauthoriz	ed Devices	Last Modified By
	T		📹 Mac	ick USB	Windows		0	1		janprem
	Temporary Access									

Im nächsten Dialog blocke ich einfach alle Removable Storage Devices. Ich belasse die Alertdialoge hier Standard.

v Policies	Tutorial-Block USB Add Descrip	ation					
Create Policy	Device Access Control						
Deploy Policy							
Trusted Devices	Removable storage devices ?		Block	-	Advanced Settings 🐣		
Temporary Access	Block connection bus of Removable storage	devices via					
	CD-ROM		No Change				
	Windows portable devices ?		No Change				
	Apple devices 1		No Change				
	Bluetooth Adapters		No Change				
	Printers		No Change				
	Moderns		No Change				
	Wineless network adapters		No Change	÷4			
	Imaging devices 2		No Change				
	Serial ports (COM)		No Change	17			
	Viewmore 😔						
	Monitor all device activities						
	Generate reports from agent every	24 C bours *					
	Send blocked device details to server immediately						
	(e) Alert Settings						
	Notification type	Off Off Default Notification 😨 😋	Custom Notification (2)				
	Alert title "	Device Access Restricted					
	Alert message *	This device has been restricted. Contact your System Administrator					
	Enable temporary access request						
		Save & P	Save as Draft Cancel				

Nach Save & Publish wird die Policy abgespeichert. Keine Angst – da wird noch nichts verteilt. Das geschieht im nächsten Schritt, wenn ich diese Policy einer Gruppe zuweise.

Ich habe zur Demonstration bereits eine Testgruppe mit einem Laptop erstellt, daher gehe ich nun auf "Associate Policy":



Hier wähle ich die Gruppe, auf welche ich eine Policy anwenden will (1) und wähle die gewünschte Policy aus (2) und (3). Durch Deploy (4) wird die Policy dann auch angewendet.

Auf meinem Testsystem hatte ich vor dem Deployment einen dieser tollen Gitarren Sticks eingesteckt und Zugriff erhalten:



Nach dem Deployment sieht es nun so aus, wenn ich den Stick einstecke:

	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	

Auch über den Explorer wird kein USB Stick angezeigt:

💻 🛃 🔚 🖛 Dieser P	с			_	_ ×
Datei Computer	Ansicht				~ 🕐
← → ~ ↑)ieser PC		ٽ ~	Dieser PC durchsuchen	م
Schnellzugriff	✓ Ordner (7) 3D-Objekte	Bilder	r		^
3D-Objekte					
📰 Bilder	Desktop	Doku	mente		
E. Desktop					
🗄 Dokumente	Downloads	Musil	k		
Downloads		,			
Musik	Videos				
Videos					
Data (D:)	✓ Geräte und Laufwerke (3)				
Rinelli-	Asus (C:)	Data	(D:)		
Netzwerk	57,1 GB frei von 203 GB	677 G	B frei von 689 GB		
-	BD-ROM-Laufwerk (E:)				
-					
	✓ Netzwerkadressen (5)				
		FRITZ			
15 Elemente	User-	*			*

Ich könnte über den Dialog oder das Taskleistensymbol, für dieses Gerät eine Freigabe anfragen. Diese Anfrage sieht so aus:

<u></u>	Temporärer Gerätezugri	- ×
Temporärzugriffanfrage Temporärzugriffanfrage für Gerät erheben	Gerätetyp	- All Devices -
Code anwenden Gerätezugriff durch Codeanwendung erlange	Gerätename	[None Selected]
	Zugriffsdauer	1 Hour
	Grund	
		Anfrage

Nur, wer sagt mir, dass dieses Gerät auch wirklich sicher ist, wenn ich es nicht selbst auf einem Sicherheitssystem geprüft habe? Ich nutze hierfür immer gern eine vom Netz unabhängige Maschine mit Virenscannern.

Es wird immer wieder Diskussionen geben, wenn ein Gerät geblockt ist und es wird auch immer ein ganz wichtiges Dokument sein, welches auf dem Stick ist. Ich für meinen Teil bin da immer sehr hart und kurz angebunden. Denn, was erlaubt ist, wird von mir ausgegeben. Dann wird das Gerät in einer Trusted Device Gruppe stehen oder nach einem Scannen des Sticks auf einer der sicheren Maschinen, von mir temporär freigegeben. Eine temporäre Freigabe kann erforderlich sein, wenn ich z.B. einen Consultant einer Fremdfirma im Haus habe, der z.B. eine Präsentation auf dem Stick hat.

Wie das aussieht, sehen wir im nächsten Punkt.

4. Temporären Zugriff gewähren

Über das Dashboard über die Blocked Devices sehe ich alle geblockten Geräte und auch, auf welchen Rechnern diese geblockt sind.

🛟 Endp	oint Central Home	Configurations Threats & Patches Softw	vare Deployment Invento	ry OS Daployment Mobil	le Device Mgnt	Tools Agent Ad	min Browsers App	Ctrl Device Contro	· ··· · · · ·	Jump to SDP	Q 🕝 🛆 🖗	\$
Dashteourd Policies		Computer(s) without policy 3 of 4 Associate policy	O Asso	ted device(s) without policy of 1 clate policy		`	Blocked device(s) 2 View blocked device(s)			74	l device(s) swed device(s)	
A builder	Getting Started point Central Home	Configurations Threads & Patches Soft	ware Deployment Invent	ory OSDeployment Mot	bile Device Ment	Tools Agent A	dmin Browsers Ap	p Ctrl Device Contr	a	5 Jump to SDP	0669	· 🚯 :::
Deshboard	✓ Reports	Blocked Devices 1										*
œP	Blocked Devices	III III Viewby: Device										
Policies	File Tracing	Removable storage devices	Filter Ilv: All Period	* OS Platform *							Total Records	I Q ■ 4
a.	File Shadowing		Device Name M	anufacturer Vendor ID	Product ID	Serial Number	Custom Device Name	Computer Name	Domain	OS Platform	Username	Blocked T
Insights			Flash Orive Sil	licon Motion _ 070C	1000	F8D1109300300404	-	JANPREM-PC-ASUS	RINELLICORP	III Windows	Janprem	25/03/20
Reports			Flash Drive Sil	licon Motion, 0/0C	1000	F8D1109300300404	-	JANPREM-PC-ASUS	RINELLICORP	III Windows	Janprem af Total Records	25/03/20: 25 *

Hier kann ich mir die Geräte ansehen und auch die Serien Nummer finden.

Einen temporären Zugriff gewähre ich ganz einfach über Insights / Managed Computers und die Auswahl des Rechners, an welchem der Stick hängt.

😑 End	point Central Home	Configurations Threats & Patches	Software Deployment	Inventory OS Deployment	Mobile Device Mgmt Tools Ager	t Admin Browsers AppCtrl	Device Control ••• 50 Aut	ptoSDP Q 🕝 🛆 🖇 🧊 🏭
	~ Insights	Anaged Computers						
Dashboard	Managed Computers	Filter Dy: All *	OS Platform *					
Policies	Device Summary Device Statusby Computer	Computer Name	t Domain	OS Platform	Last Contact Time	Associated Groups	? Applied Policy Count	Associated Policy Count
A	Computers by Device Type	Janprem-Lenovo	WORKGROUP	III Windows	16/00/2024 20:26:1	c 0	0	0
Insights	✓ Temporary Access Status	JANPREM-PC	RINELLICORP	II Windows	25/03/2024 12:52:2	5 0	0	0
	Device Exemptions	IANPREM-PC-ASUS	RINFLUCORP	III Windows	25/03/2024 12:55:1	1 1	1	3
Reports	Device Type Exemptions	Sabine-Asus	RINELLICORP	12 Windows	25/03/2024 12:53:1	4 0	0	0
dh Settings								1-4of4

Es gibt jede Menge an Übersichten und Details, ich wechsle zum Tab "Device Manager" und wähle "Allow Temporary Access".

Insights	Extra Friendly Name: JANPREM-PCASUS							
Managed Computers	Groups Policies Device Audit File Tra	cing File Shadowing Device Manager						
Device Summary	Total Devices 1 5						I set updated time : http://	d 7 2022 09 22 AMI CHINGS
Computers by Device Type		Disk drive					Can sponto time . A	n, mail or an and of share
ights V Temporary Access Status	Bolsk drive	Manufacturer		(Standard dsk drives	0(8564)			
Device Exemptions	🕑 🔘 CD-ROM	Parent device instance path	S# 3	USB/VID_85646.PID	1000/291826683	6		
orts Device Type Exemptions	⊙ 💣 Wireless network adapters	Device instance path	S (USBSTOR\DISK&VE	N_JETFLASH&PROD_TRA	NS. 🖸		
6	PR Imaging devices	Product ID	- 1	1000				
ngi	⊙ ∰ Mouses	Serial Number	12	291826683				
		Custom Name	1	12				
		Description	33	Diskdrive				•
		Status	14	Disabled				Allow Temporary Access

Hier wieder einen sprechenden Namen vergeben (in einer Produktivumgebung bitte eine Naming Convention verwenden), einen User auswählen, Zeitfenster und Device Type. Dann geht's auch schon auf "Deploy Immediately".

Offene Türen schließen mit Device Control! – von Jürgen Rinelli

JANPREM-PC ASUS . All users				
JANPREM-PC ASUS				
JANPREM-PC-ASUS All users				
All users				
Fixed Window				
1 Hour *				
25/03/2024, 03:21 PM				
				👩 How to get device path
Remarable storage devices				
NUMBER OF THE				
All Instances *				
	Add			
Allowed By	Vendor ID	Product ID	Serial Number	Action
Specific Instance	8564	1000	291826683	0 5
	1 Hour System 23/03/2024, 03:21 PM Removable storage devices All instances Allowed By Specific Instance	1 Hour	1 Hour * 25/03/2024, 08:21 PM Removable storage devices * All Instances * Allowed By Vendor ID Product ID Specific Instance B544 1000	1 Hour * 25/03/2024, 03:21 PM * Removable storage devices * All Instances * Allowed By Vendor ID Product ID Serial Number Seeiffer Instances 8564 1000 29183483

All Ter	nporary Access 🕕								Configure M	fail Notification
+ Create	I Move to Trash	Filter By: Status +						View Tro	sh Total:3	IQ II 🕹
	Policy Name	Applied Time	Duration Type	Computer Name	Username	Device Count	Status	Expiry Time	Action	
	utorial Test	2	Fixed	JANPREM-PC-ASUS	All users	1	Published	25/03/2024 15:21:44	(11)	
	A FOR Janprem In Janp	24/07/2023 11:10:31	Fixed	Janprem-Lenovo	Janprem	1	Revoked	31/07/2023 11:07:00	(11)	
	A FOR Janprem In JAN	24/07/2023 10:53:08	Fixed	JANPREM-PC-ASUS	janprem	1	Approved	24/07/2023 11:49:43	œ	
									1-3 of 3	25 *

Auf dem Laptop poppt auch gleich eine Meldung auf:



Über das Tray Icon im Dialog für den temporären Gerätezugriff kann ich dann den Code, welcher mir gemailt wurde, anwenden.

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 :
 Download the attachment file in this email. Right click the Agent Tray Icon. Select Temporary Access Portal option. Select the Apply Code tab.
5. Browse the file downloaded in step 1 and click Apply button.
Regards,



Nach Ablauf der Stunde wird das Device automatisch wieder geblockt.

Da wir aber auch Geräte haben die wir im Unternehmen wirklich brauchen, bedarf es genereller Freigaben. Wie das Aussehen kann, zeige ich im nächsten Punkt.

5. Trusted Device Listen und generelle Freigaben

Bekannte Geräte wie Tastaturen, Mäuse, Drucker, Modems, Biometric Devices, etc., können in einer Liste einfach zusammengefasst werden.

Hierzu eine Trusted Device Gruppe erstellen, einen sprechenden Namen vergeben, Device Typ auswählen und die gewünschten Geräte aus den Tabs.

6 .4	✓ Policies		trusted-device_1423 Add Description					
Dashboard	Create Policy	1	Select Devices					
æ	Deploy Policy		Select device type Ramovable storage devices *					
Policies dis	Trusted Devices							
	Temporary Access		Add new devices Import files					👩 How to get device path
0.0000								Q, Search
Bassata			Vendor Name	Custom Name	Vendor ID	Product ID	Serial Number	Action
rispon ta			Unknown	32	25	(注)	1F4ADFFE	Add
高			Transcend Information, Inc.	÷+	8564	1000	291826683	Add
Settings			LucidPort Technology, Inc.	74	1759	5002	S21JNX/BGC27764K	Add
			Toshiba America Inc		0480	8208	20200222017857F	Add
			ASMedia Technology Inc.	14	174C	1153	000000000000000000000000000000000000000	Add
			Silicon Motion, Inc Taiwan (formerly Feiya Technology Corp.)	57	0900	2000	2880464	Add
			Sony Corp.		054C	07F9	C75A602D34CF	Add
			Vast Technologies, Inc.		10EC	5229	00000001004CE00000	Add
			Transcend Information, Inc.	54 C	8564	1000	01L23C8AH353E5Q1	Add
			Silicon Motion, Inc Taiwan (formerly Felya Technology Corp.)	动	0900	2000	85DD16A	Add
			C Device Lists					
								Q, Search
			Vendor Name Custom Name	Ven	dor ID	Product ID	Serial Number	Action
					No data ava	ilable		

Dann benötige ich eine Policy über "Create Policy":

Endpoint Central Home			Configurations	Threats & Pa	itches So	ftware Deployment	Inventory	OS Depl
0.h	✓ Policies			olicies (i)				
Dashboard	Create Policy		+ Cross	to Doligy -		Troch Filter By	Status	05.0
e	Deploy Policy		T Crea		Move to	frash Filter by .	Status	USP
Policies	Trusted Devices		Win	dows ie		OS Platform		Authoria
<u>t@t</u> BBB	Temporary Access	5	Wat		USB	Nindows		0

Hier wieder einen Namen vergeben (1) und aus der Liste dann in unserem Beispiel Removable storage devices / Allow trusted devices (2) auswählen.

Policy_1342	Add Description				
Device Access Control					
Removable storage devices (?)	No	Change	Ŧ		
CD-ROM	No	o Change			
Windows portable devices ?	Alle	low			
Apple devices ?	Alle	low trusted devices			
Bluetooth Adapters	No	Change	Ŧ		
Printers	No	Change	Ŧ		
Modems	No	Change	Ŧ		
Wireless network adapters	No	Change	Ŧ		
Imaging devices ?	No	Change	Ŧ		
Serial ports (COM)	No	Change	Ŧ		
View more 😒					

Nun öffnen sich mir viele weitere Möglichkeiten. Ich wähle die Trusted Gruppe aus die ich möchte (1) und gebe auf jeden Fall an das nur BitLocker verschlüsselte Geräte erlaubt sind (2). In der Device Control von ManageEngine stehen mir auch File Access und File Shadow Settings, zur Verfügung.

ccess Control			
Removable storage devices (2)		Allow trusted devices	Advanced Settings 🔗
Select Trusted Devices lists	Trusted-Group1 Select Trusted Devices	• 1 (1)	5 +
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	2	
Network share credentials *	Select *	7	
todieska navimum kla sira	5 Manage credentials		
Exclude extensions	add automotions		

Weiter unten gebe ich dann noch an, wie das Audit erfolgen soll (1), welche Benachrichtigung auf dem Monitor angezeigt wird (2) und ob ich einen Antrag auf temporären Zugriff ermöglichen möchte (3).

4	Device Audit Settings				
	Monitor all device activities				
	Generate reports from agent every	24 🗘 hours 💌			
	Send blocked device details to server immediately	• 1			
l) 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	· 3			

Zum Schluss noch diese Policy auf die gewünschten Gruppen verteilen, wie wir es bereits am Anfang diese E-Books einmal getan haben.

6. Schlussworte

Device Control ist heute ebenso wichtig wie das Patchen der Systeme. Ich hoffe, ich konnte einen Einblick geben wie einfach man verhindern kann das Geräte wie oben in der Kurzgeschichte von Paul geschildert, mal eben für Chaos sorgen können, wenn diese eingesteckt werden. Es ist sicher jedem von uns – auch erfahrenen Admins – bereits passiert das wir einfach mal eben ein Gerät angeschlossen haben. Durch eine Device Control helfe ich mir selbst. Weil ich weiß, dass meine Chefs mit den unmöglichsten neuen Aufgaben auf mich warten die schon gestern erledigt sein müssen.

Mit der Device Control habe ich übrigens auch diese erwähnten Chefs gut im Griff. 🤤

So sollte es sein und so lieben wir es 😊

7. Über den Autor

MCITP, MCTS, MCP, MOS, Enterprise Administrator, Senior Software Consultant, SCCM-Spezialist, Autor, Coach, Reiki-Lehrer ...

Jürgen Rinelli wurde 1970 in Deutschland geboren. In seinem ereignisreichen und oft abenteuerlichen Leben hat er in vielen Ländern gelebt und gearbeitet. Ob als Geschäftsmann, Manager, Mechaniker, Trainer, Taucher oder IT-Experte, er findet immer einen Weg, seine Träume zu verfolgen.

