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

"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

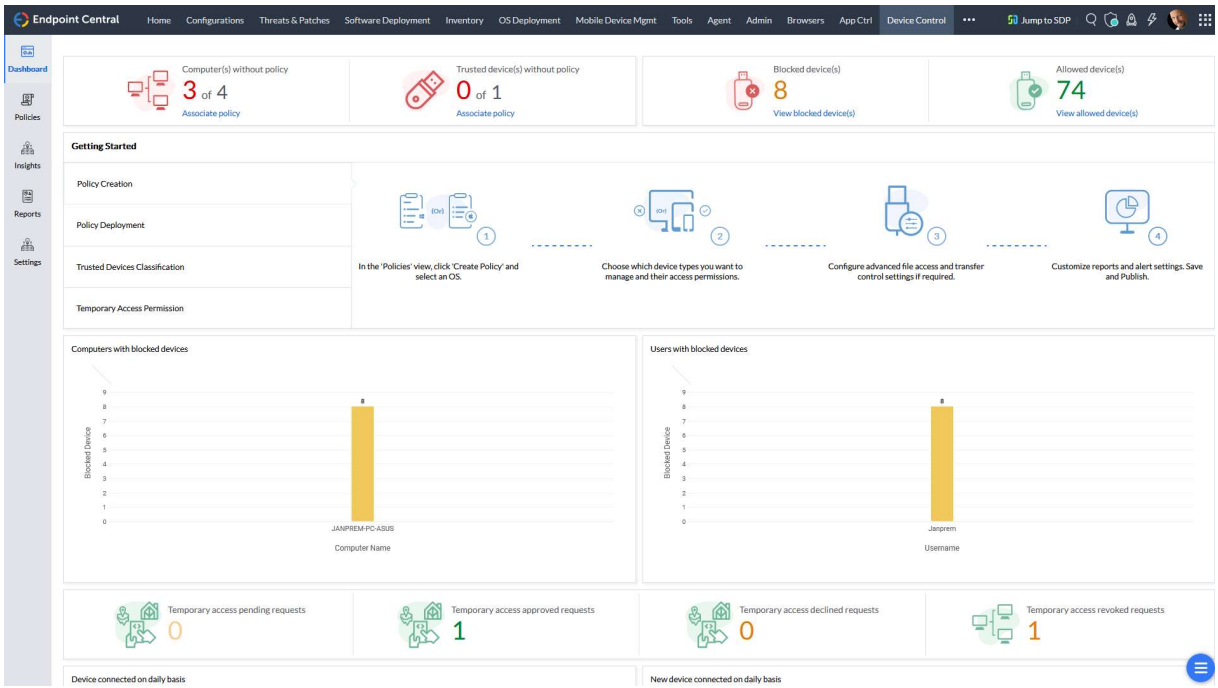
- Grant temporary access without having to rework it yourself

- Clear definition of device policies

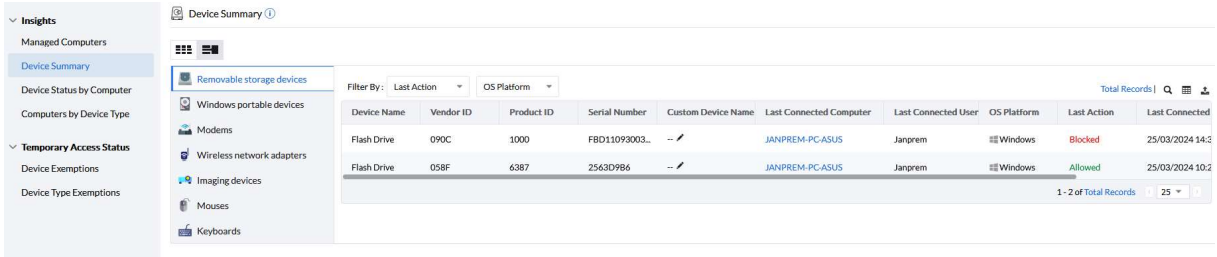
- Insights and reports

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.

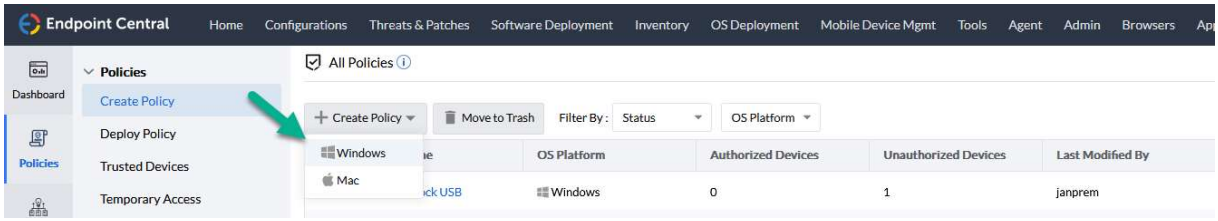


Example of device overviews

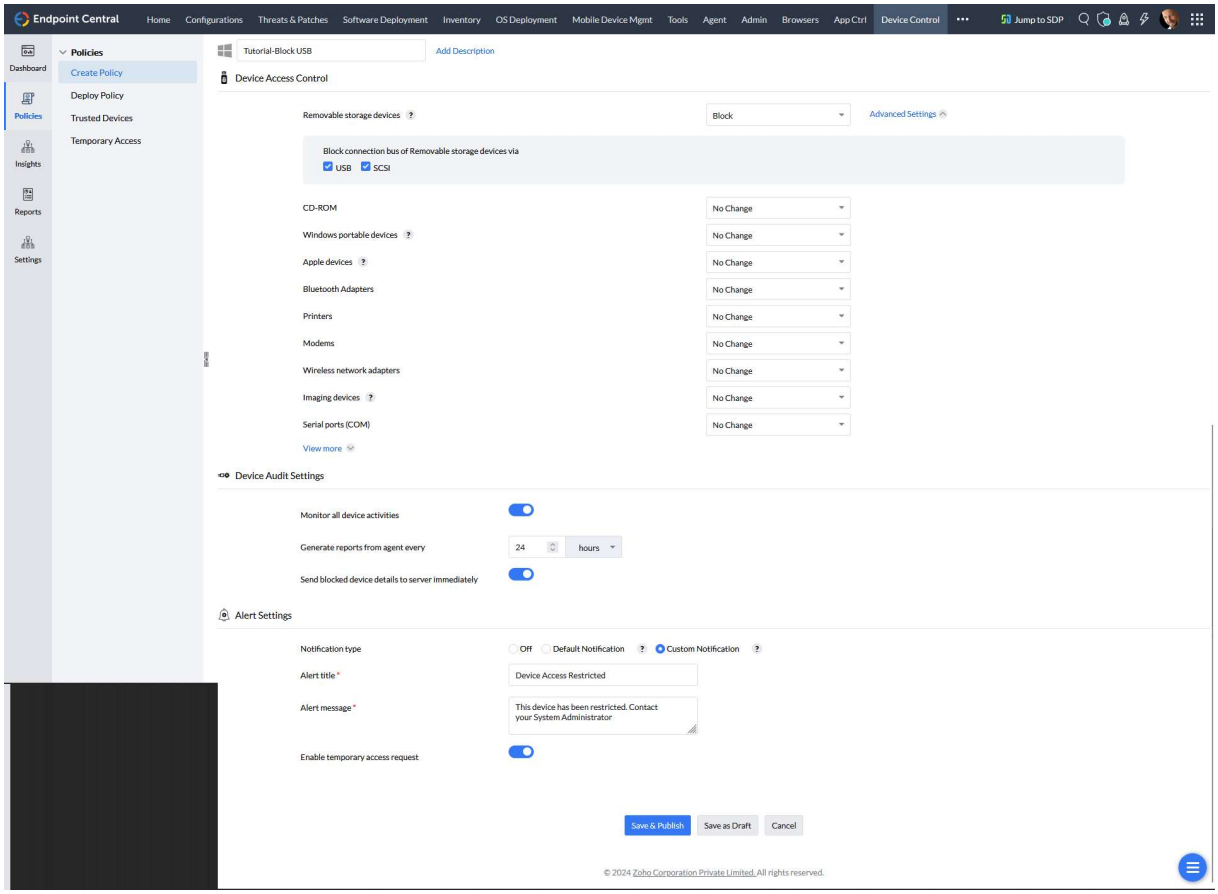


3. Blocking Devices

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

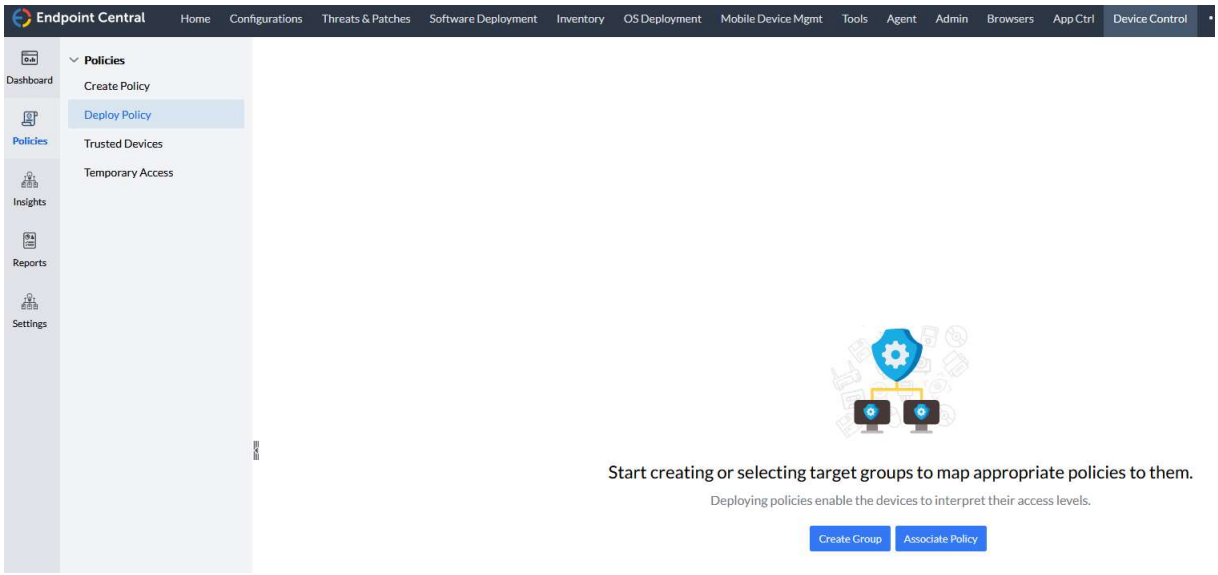


In the next dialogue, I simply block all Removable Storage Devices. I leave the alert dialogues here as standard.



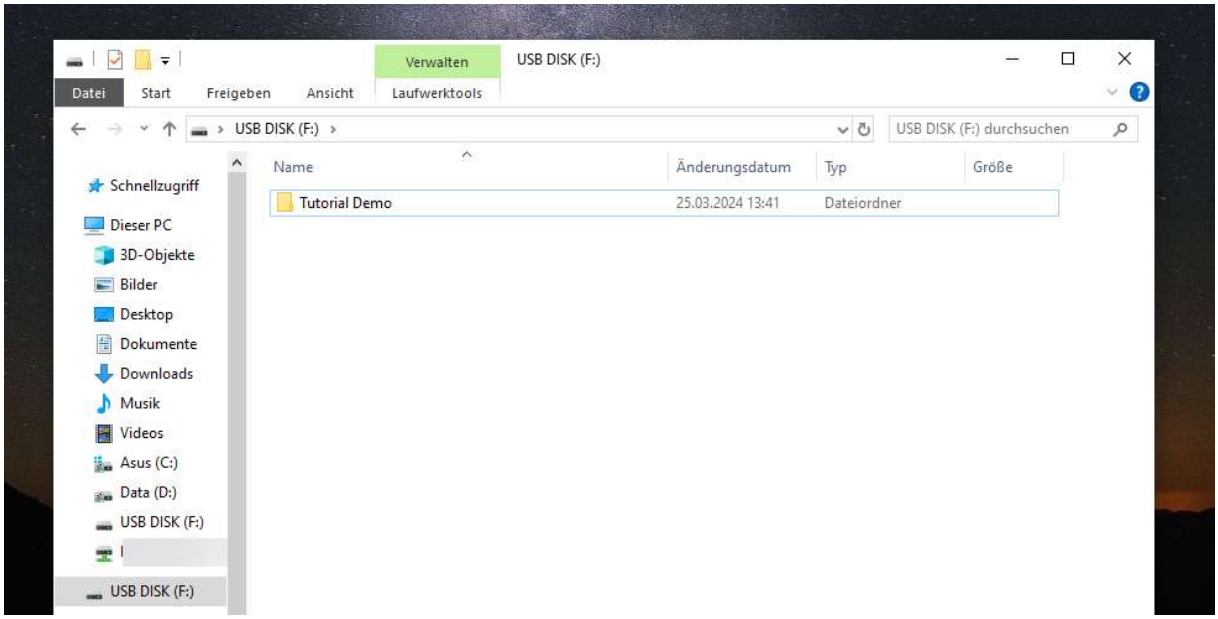
The policy is saved after Save & Publish. Don't worry - nothing is distributed yet. This happens in the next step when I assign this policy to a group.

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



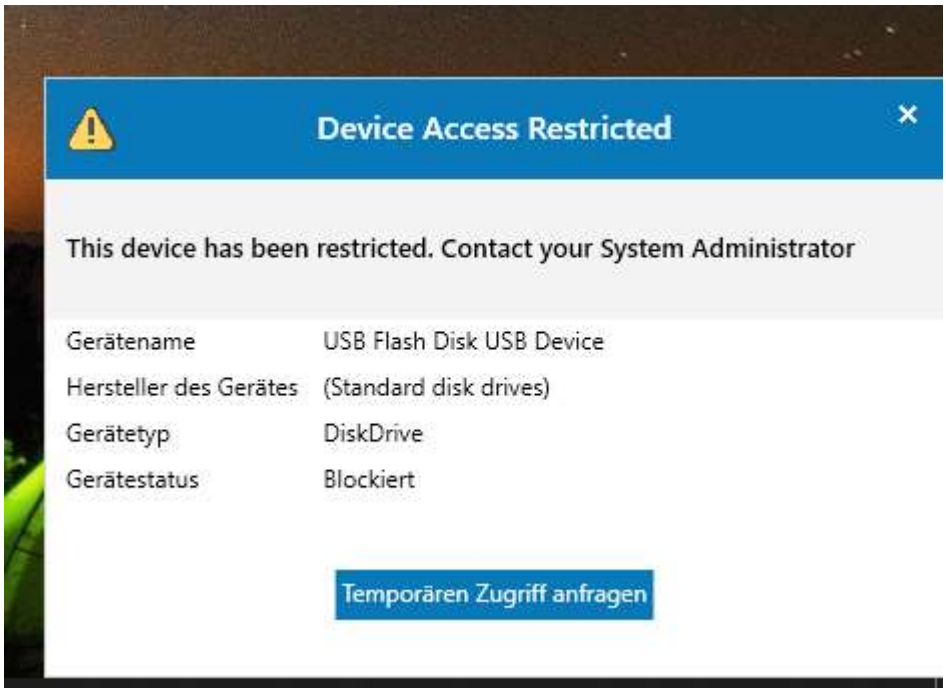
Here I select the group to which I want to apply a policy (1) and select the desired policy (2) and (3). Deploy (4) then applies the policy.

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

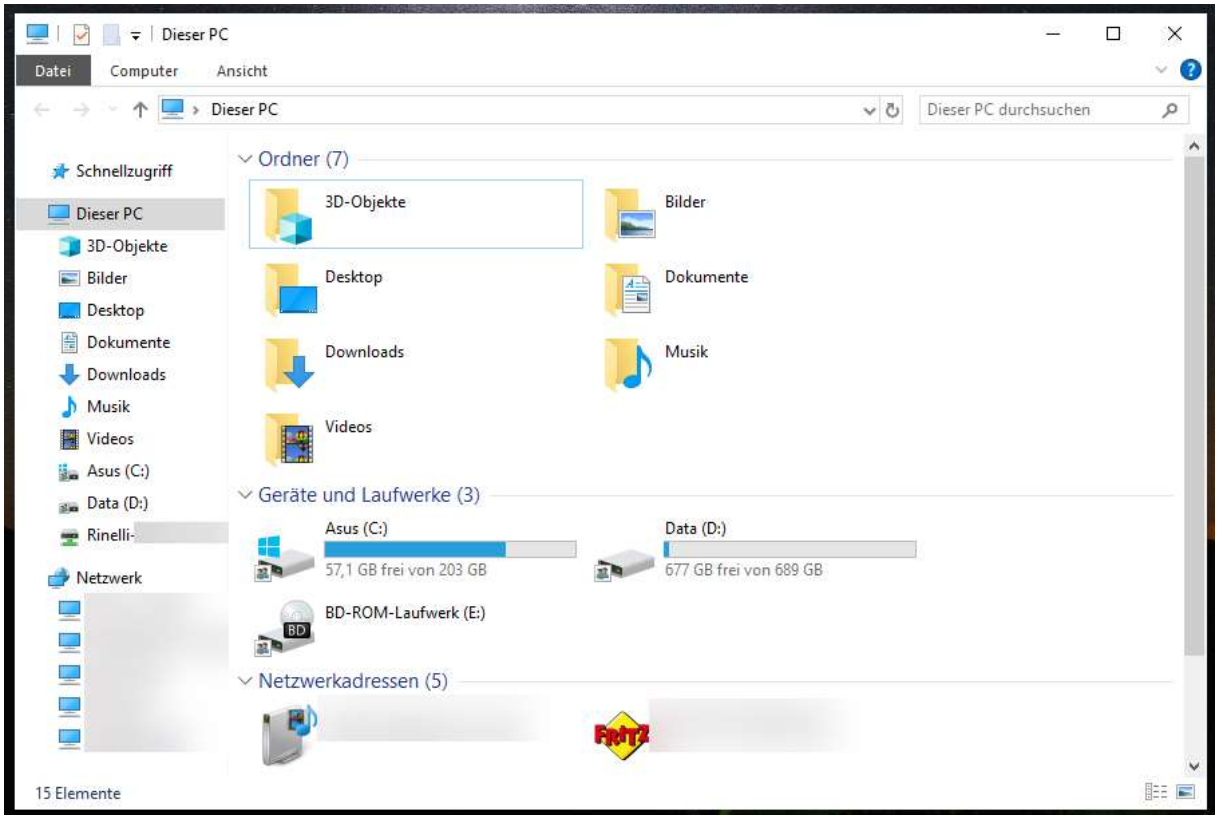


Close open doors with Device Control! – from Jürgen Rinelli

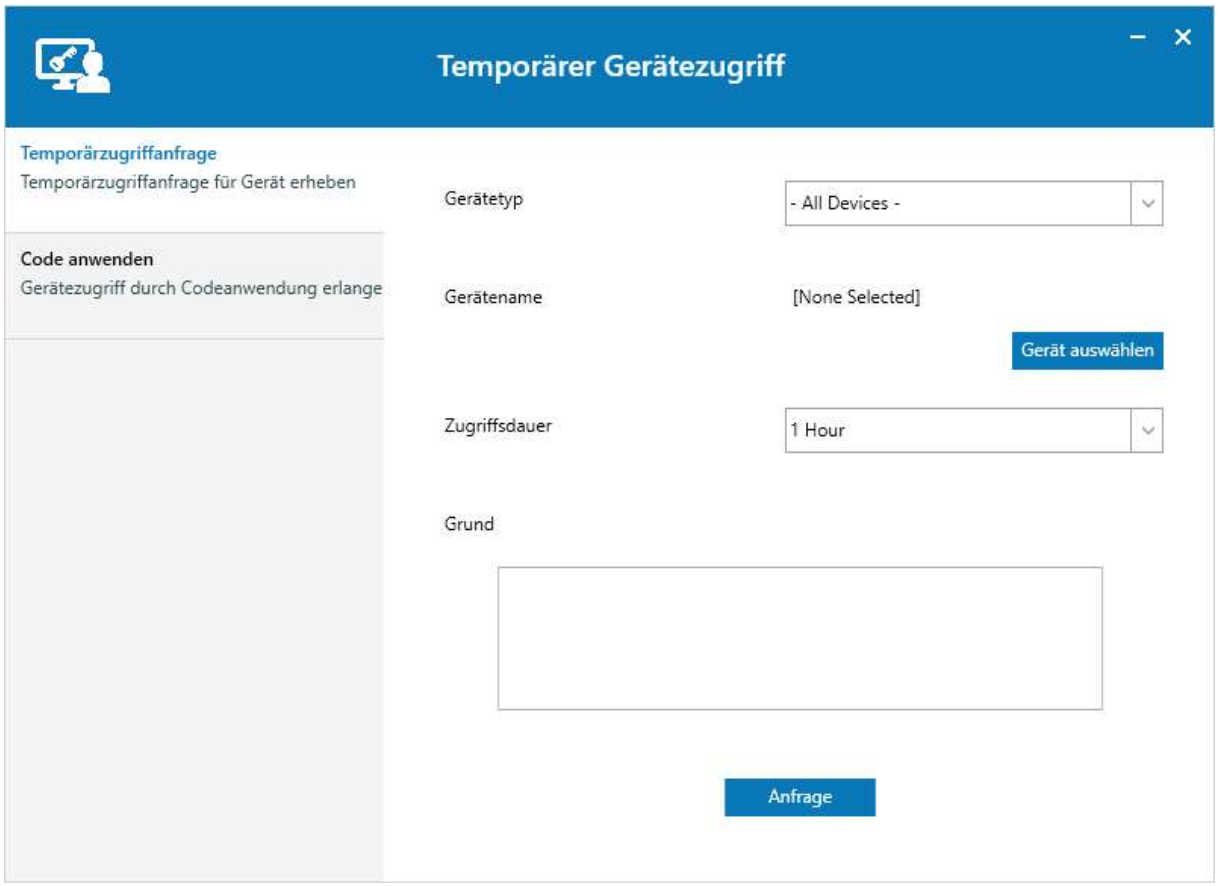
After deployment, it now looks like this when I plug in the stick:



No USB stick is displayed in Explorer either:



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)



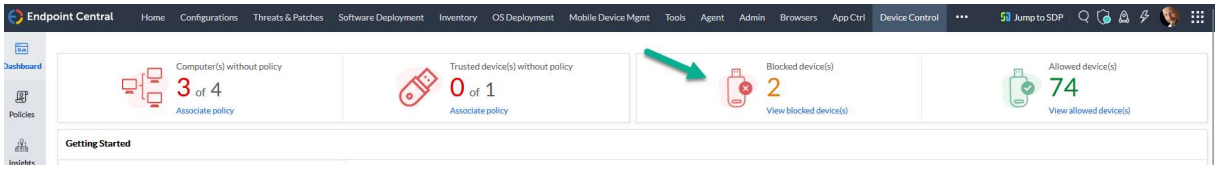
But who can tell me that this device is really secure if I haven't checked it myself on a security system? I always like to use a machine with a virus scanner that is independent of the network.

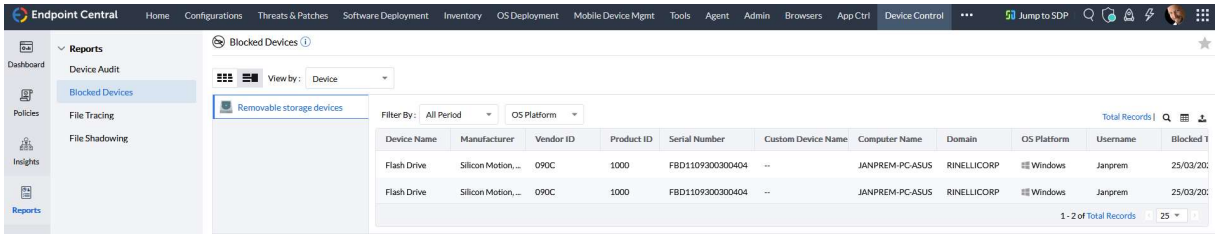
There will always be discussions if a device is blocked and there will always be a very important document on the stick. For my part, I am always very tough and short-tempered. Because what is allowed is what I issue. The device is then placed in a trusted device group or temporarily released by me after 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

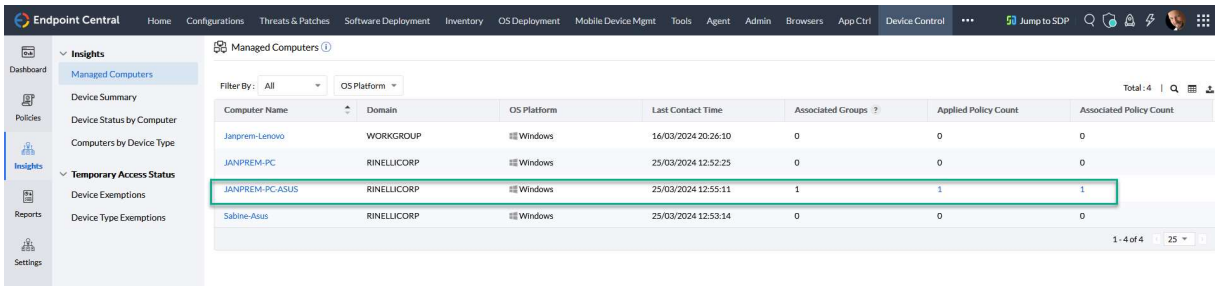
I can see all blocked devices and on which computers they are blocked via the Blocked Devices dashboard.



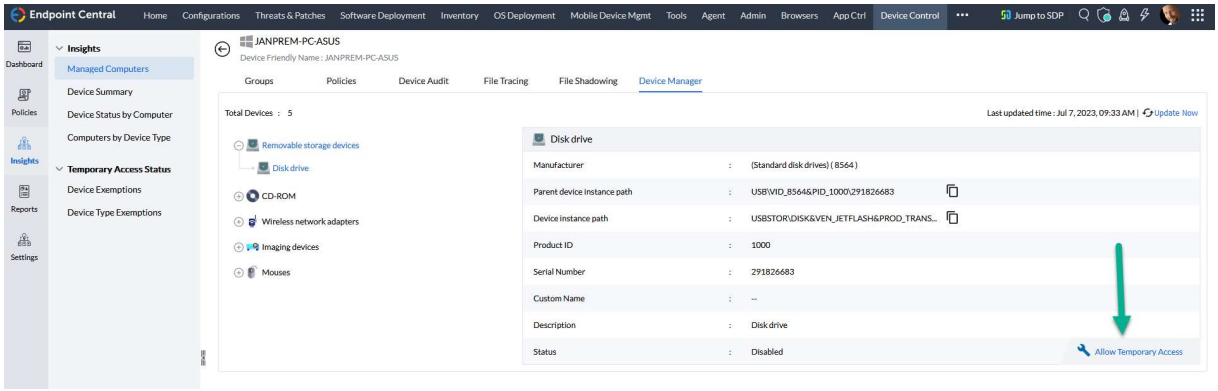


Here I can view the devices and also find the serial number.

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

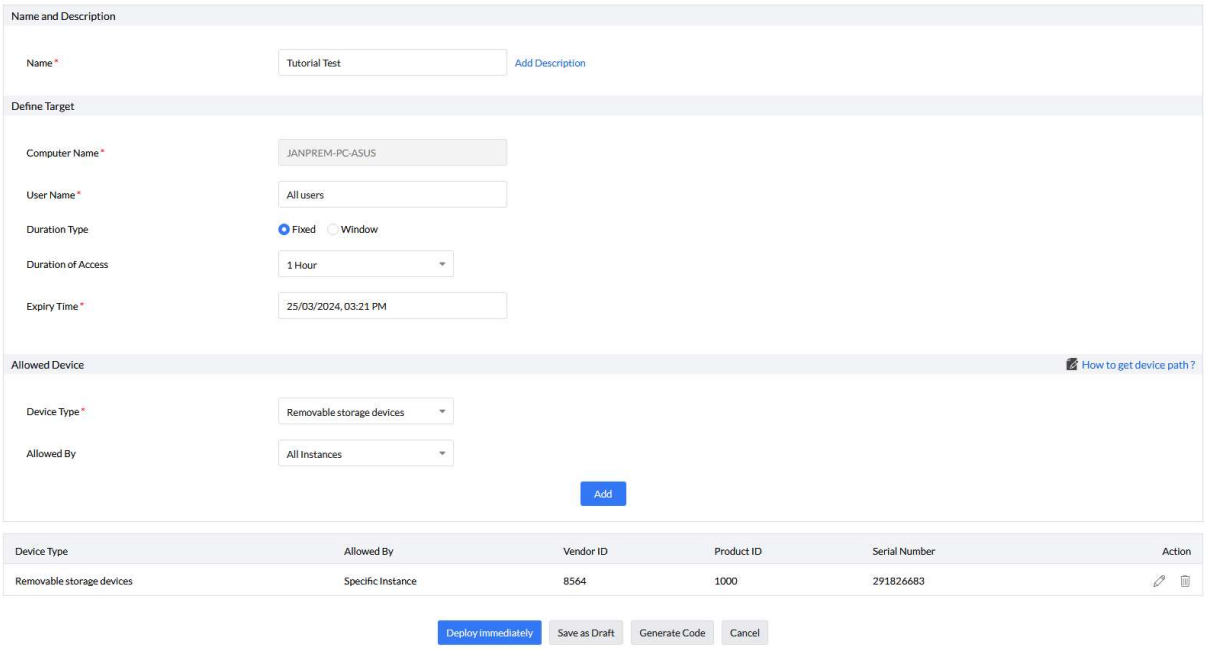


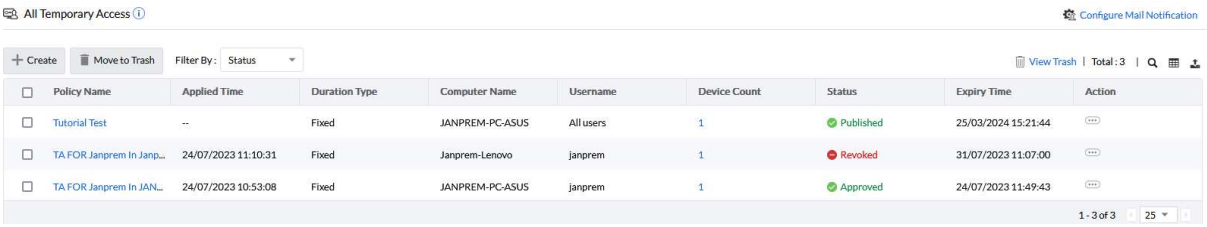
There are lots of overviews and details, I switch to the "Device Manager" tab and select "Allow Temporary Access".



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".

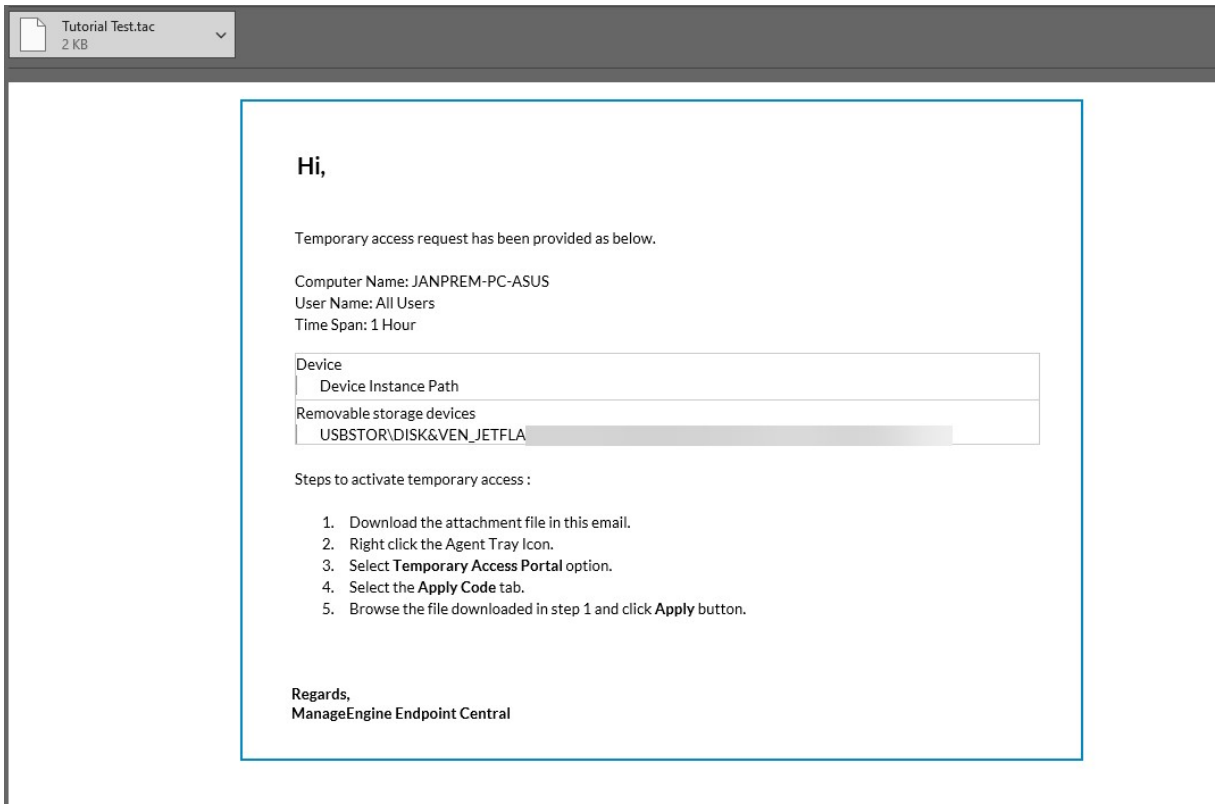
Close open doors with Device Control! – from Jürgen Rinelli

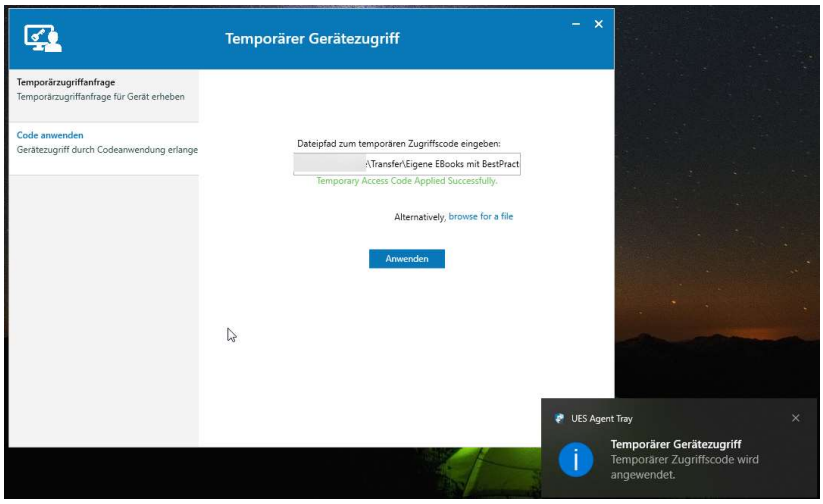




A message pops up on the laptop immediately:

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





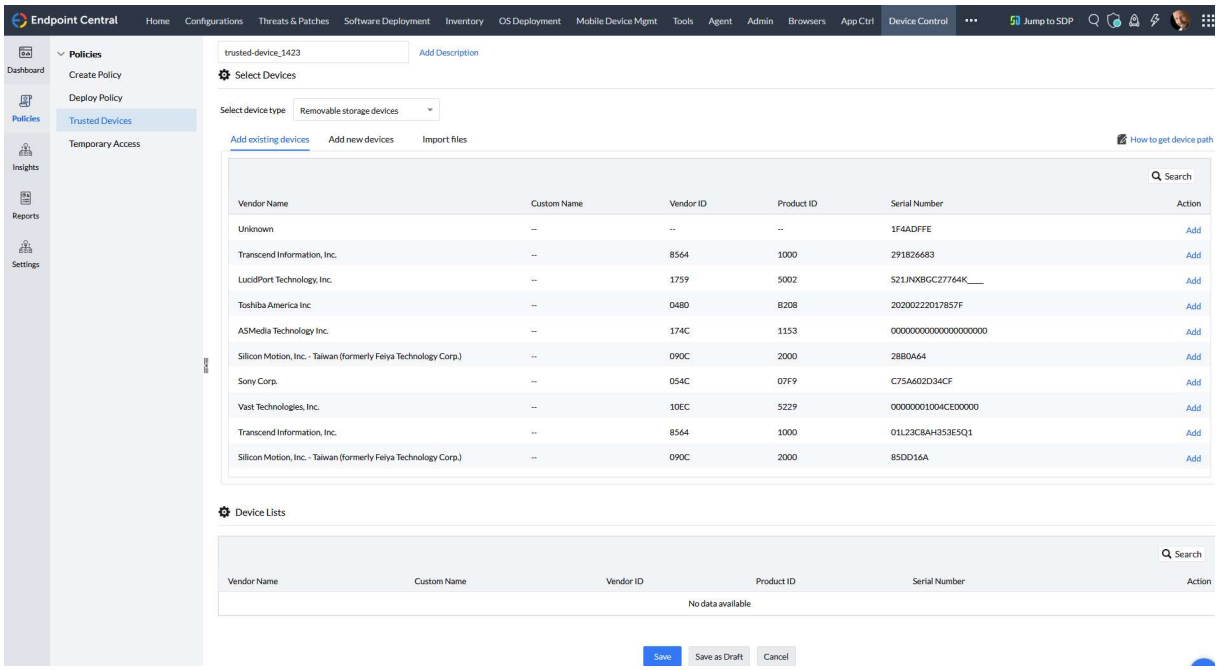
At the end of the hour, the device is automatically blocked again.

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.

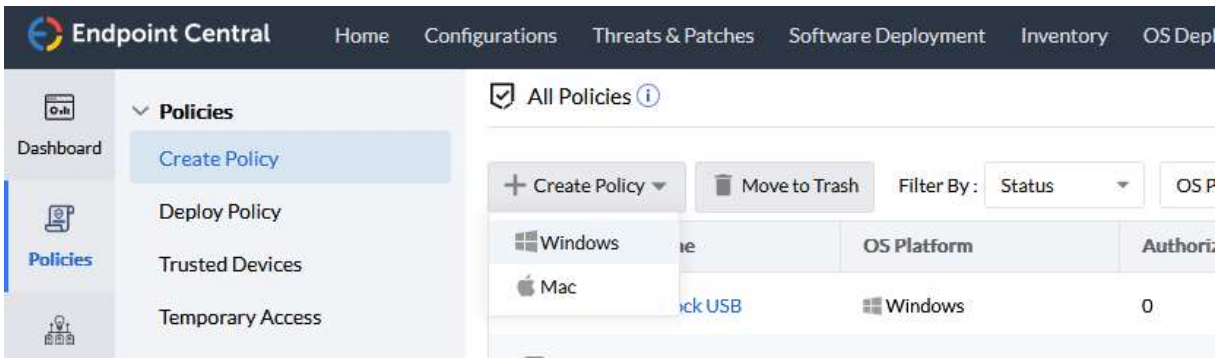
5. Trusted device lists and general authorisations

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

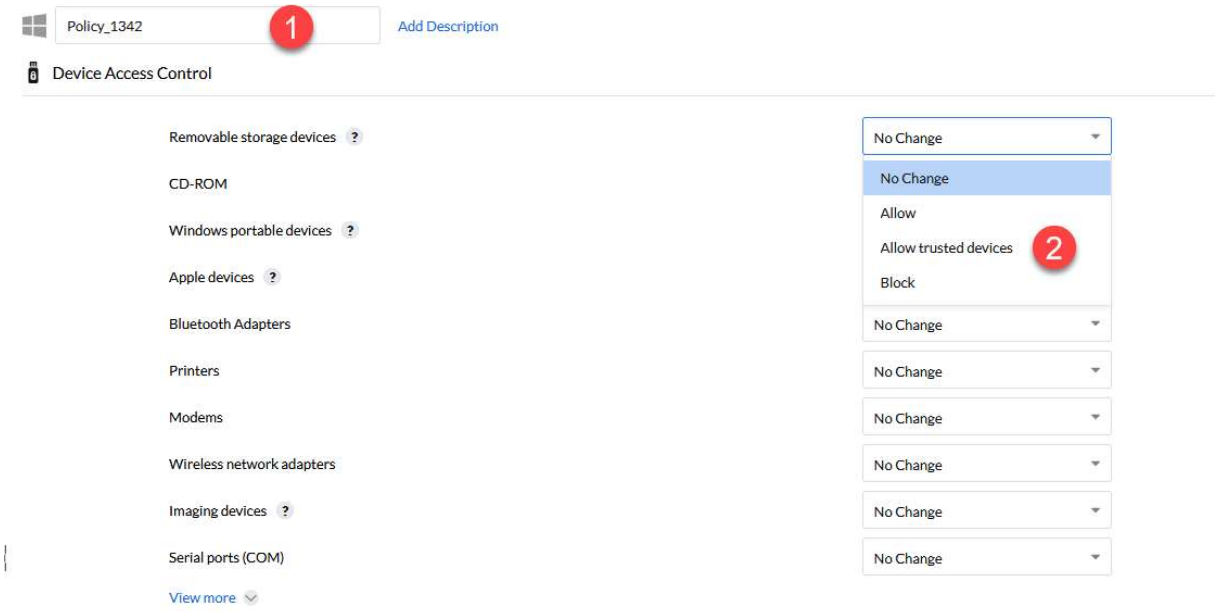
To do this, create a Trusted Device group, assign a descriptive name, select the device type and select the desired devices from the tabs.



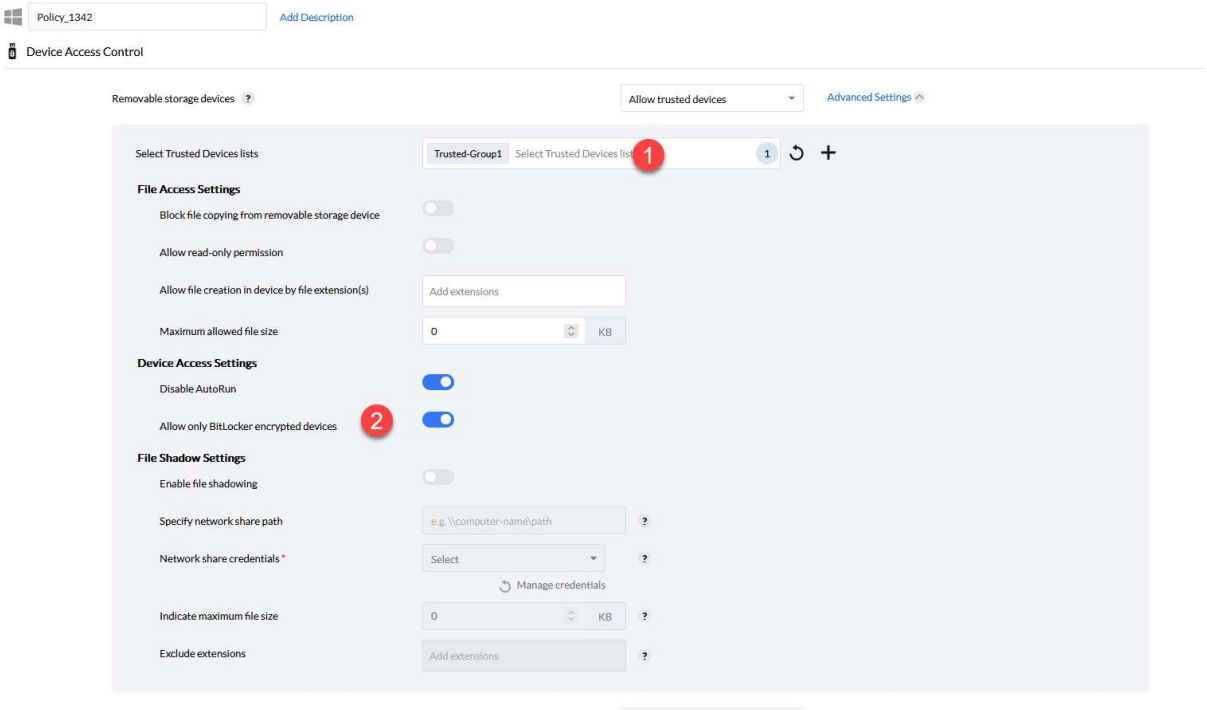
Then I need a policy via "Create Policy":



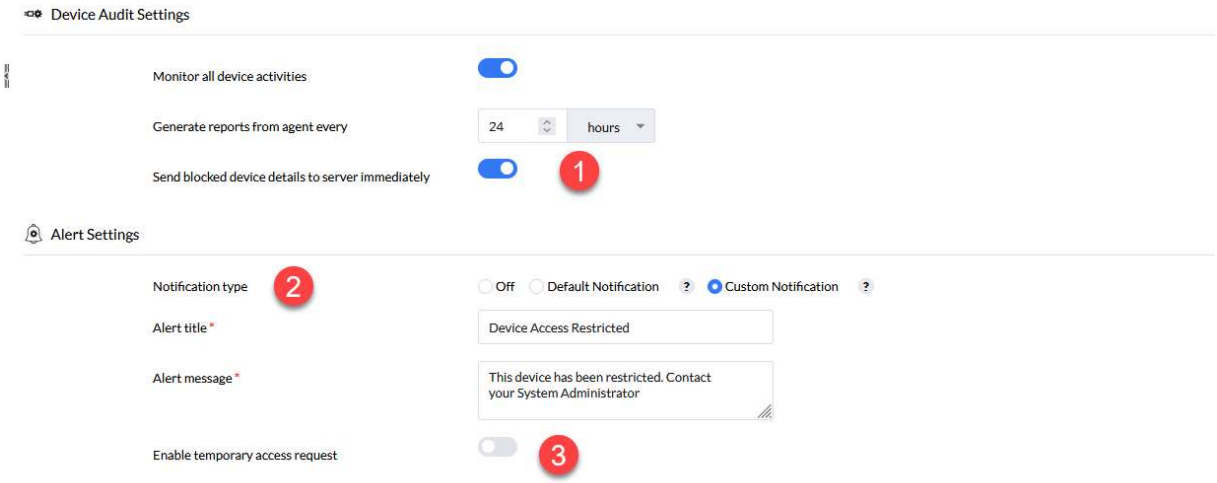
Assign a name here again (1) and then select Removable storage devices / Allow trusted devices (2) from the list in our example.



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.



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).



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.