Offene Türen schließen mit Device Control!

Meine Erfahrungen und einfache Schritte

Jürgen Rinelli

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

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 😊

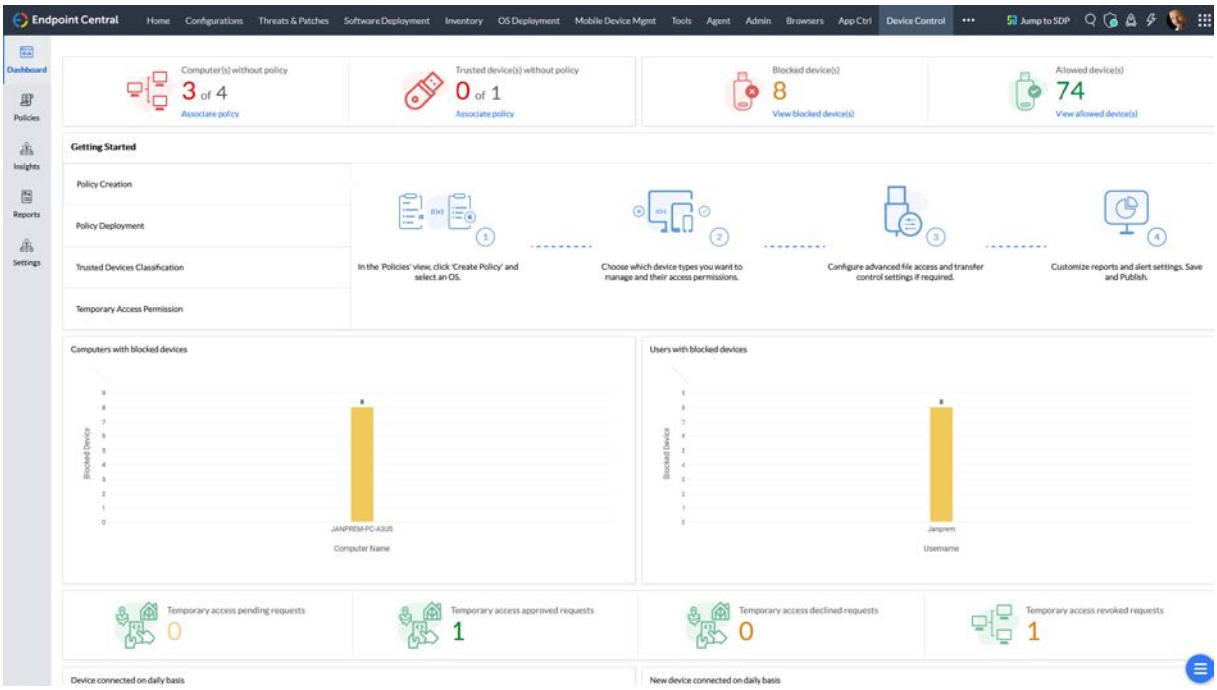
2. Device Control ein Überblick

Was eine Device Control für mich mitbringen soll, sind:

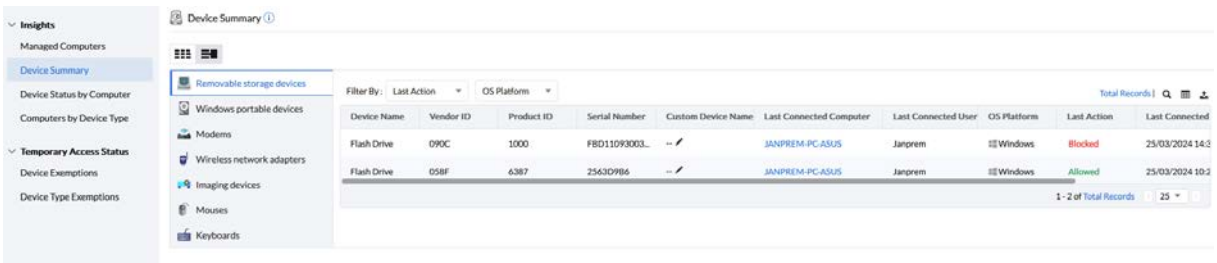
- Dashboards mit aktuellen Statusübersichten
- Die Möglichkeit, Trusted Devices in Gruppen zu definieren
- Temporären Zugriff gewähren, ohne selbst nacharbeiten zu müssen
- Übersichtliche Definition von Device Policies
- Insights und Reports

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.

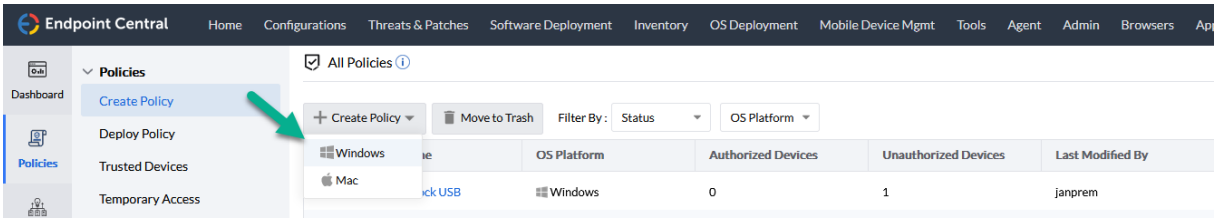


Beispiel von Device Übersichten

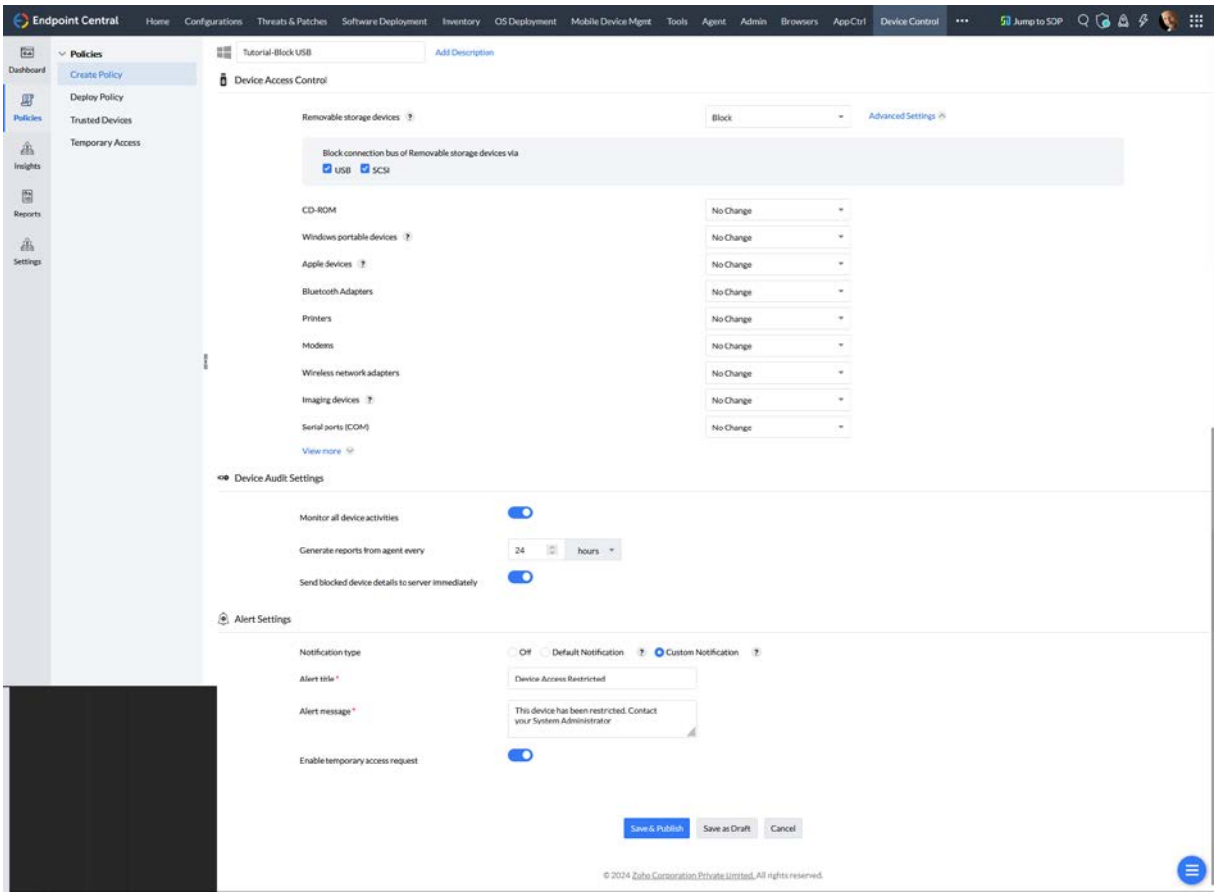


3. Devices Blocken

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

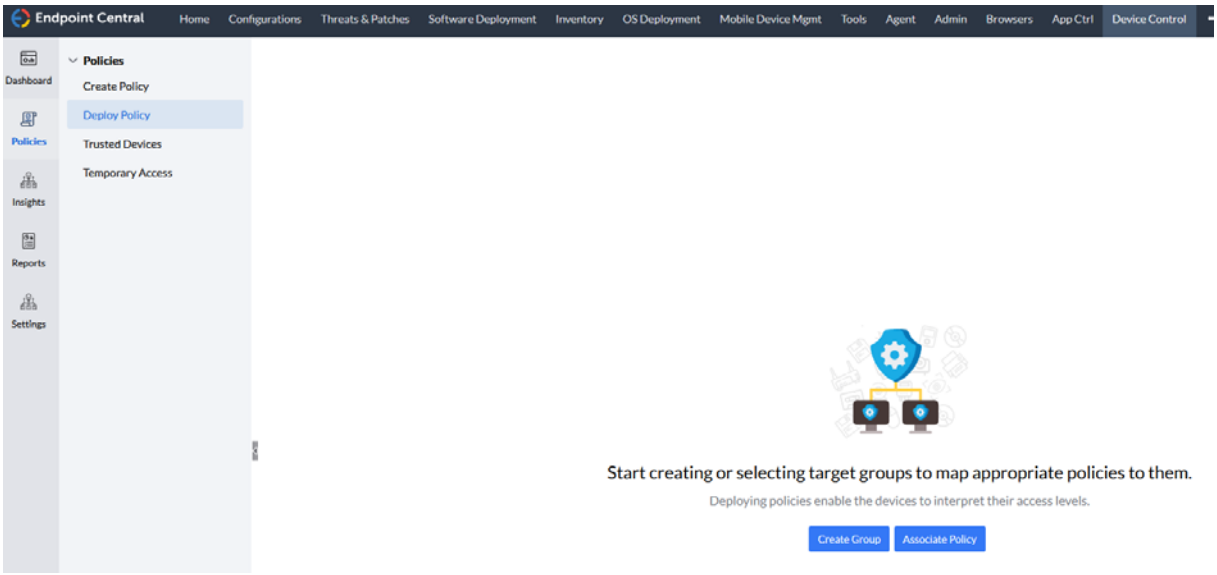


Im nächsten Dialog blocke ich einfach alle Removable Storage Devices. Ich belasse die Alertdialoge hier Standard.



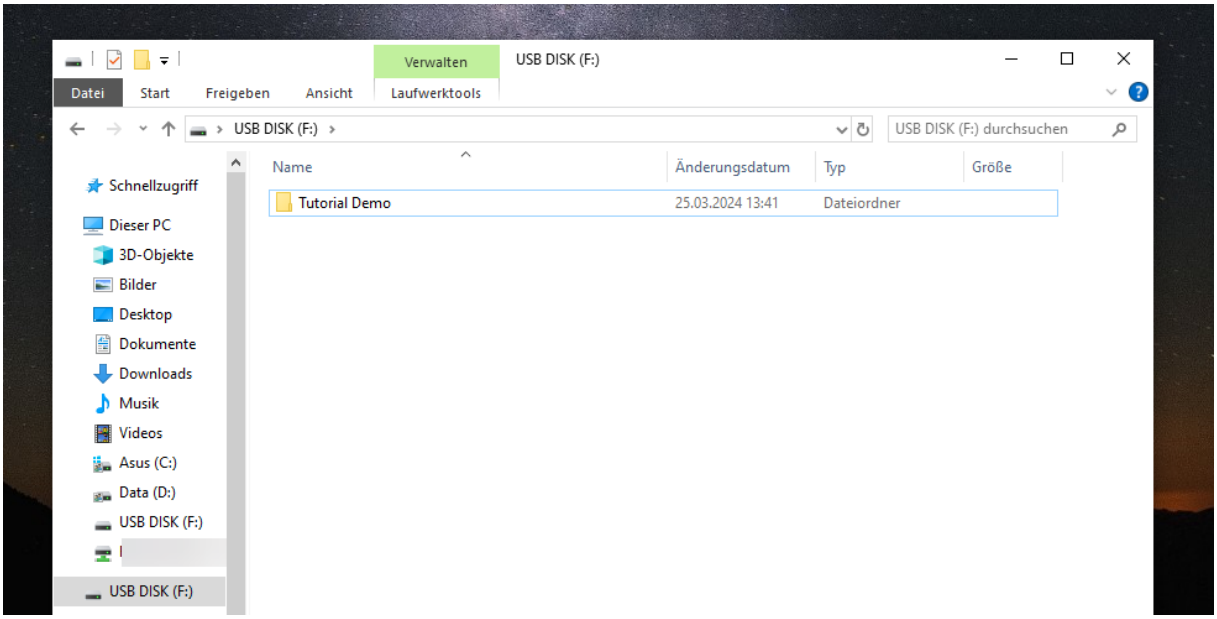
Nach Save & Publish wird die Policy abgespeichert. Keine Angst – da wird noch nichts verteilt. Das geschieht im nächsten Schritt, wenn ich diese Policy einer Gruppe zuweise.

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

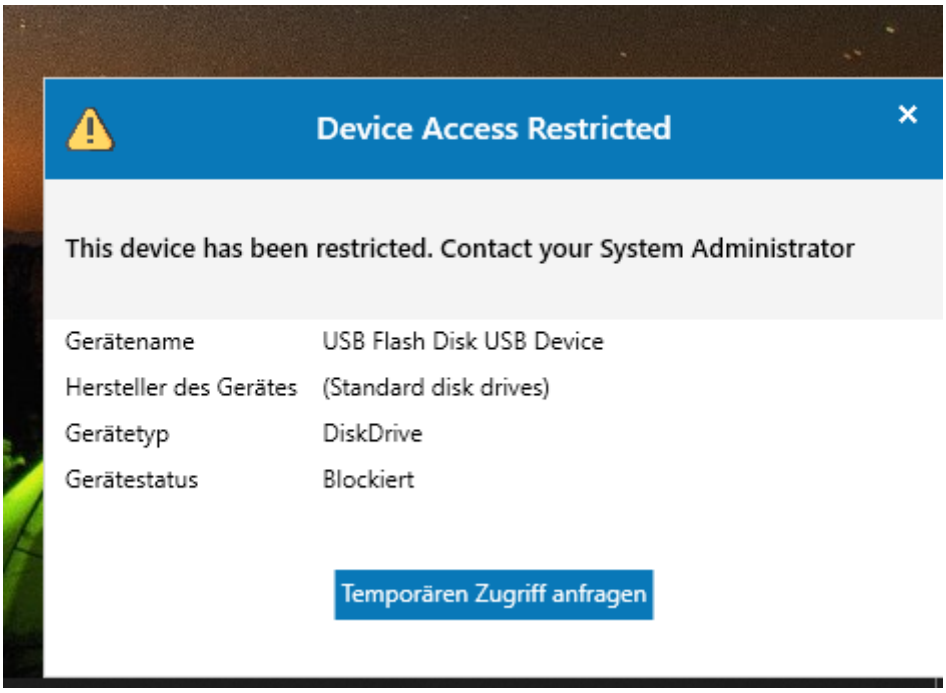


Hier wähle ich die Gruppe, auf welche ich eine Policy anwenden will (1) und wähle die gewünschte Policy aus (2) und (3). Durch Deploy (4) wird die Policy dann auch angewendet.

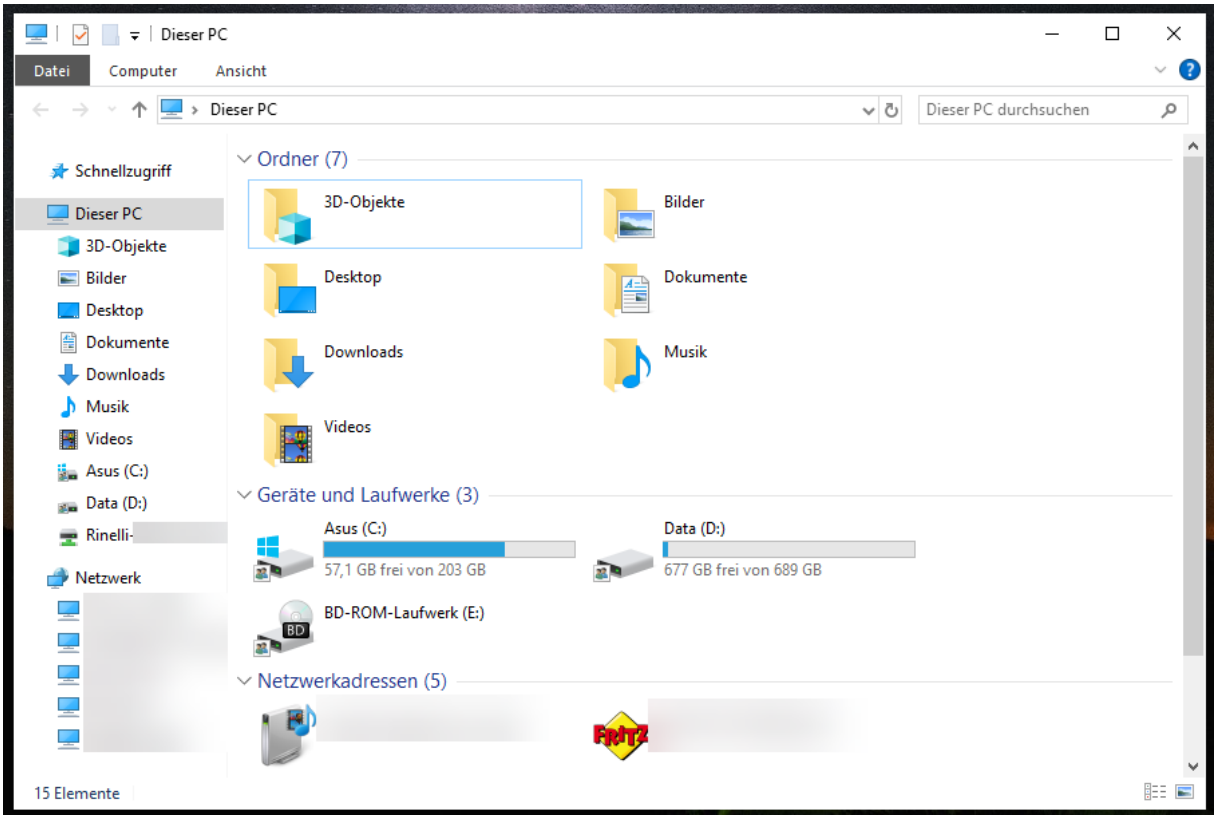
Auf meinem Testsystem hatte ich vor dem Deployment einen dieser tollen Gitarren Sticks eingesteckt und Zugriff erhalten:



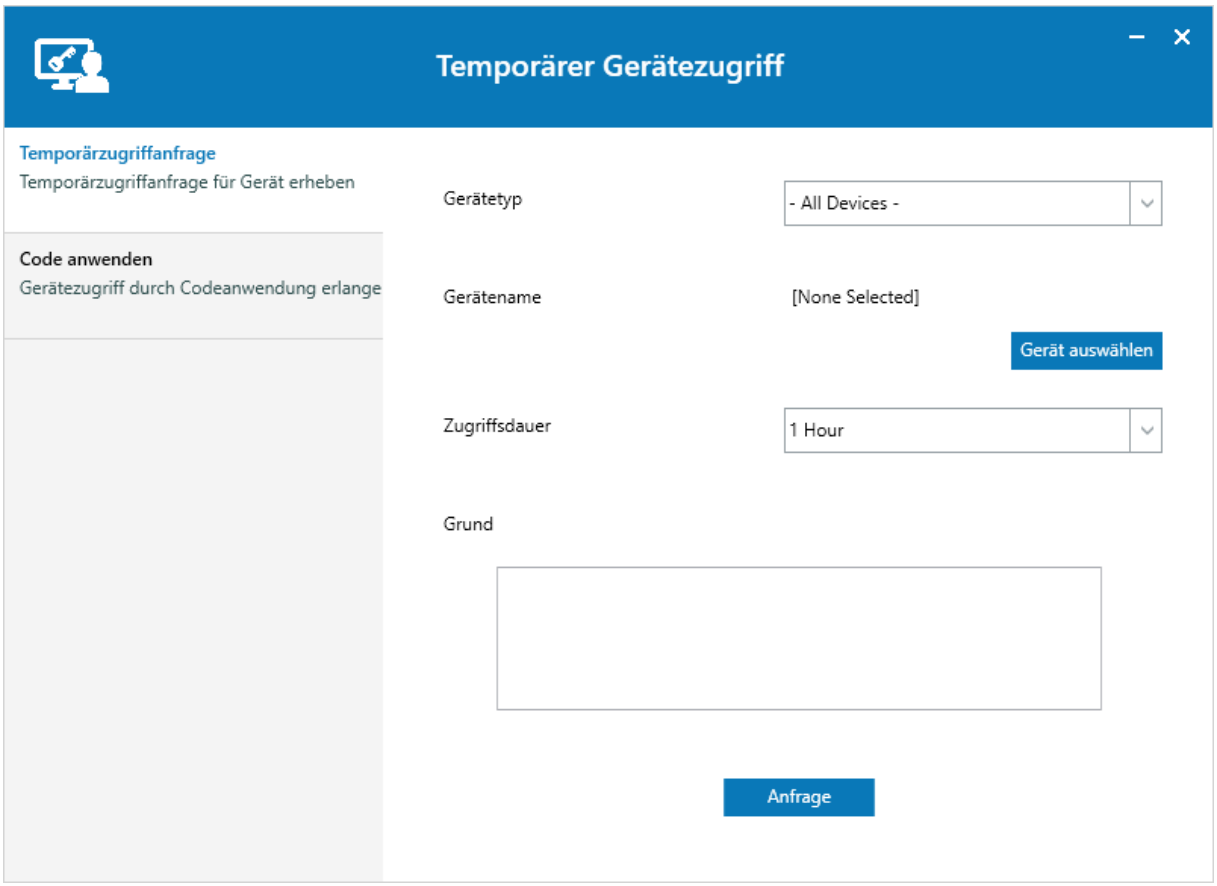
Nach dem Deployment sieht es nun so aus, wenn ich den Stick einstecke:



Auch über den Explorer wird kein USB Stick angezeigt:



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



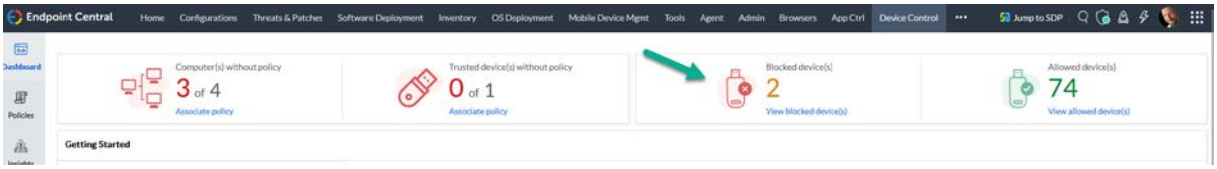
Nur, wer sagt mir, dass dieses Gerät auch wirklich sicher ist, wenn ich es nicht selbst auf einem Sicherheitssystem geprüft habe? Ich nutze hierfür immer gern eine vom Netz unabhängige Maschine mit Virenscannern.

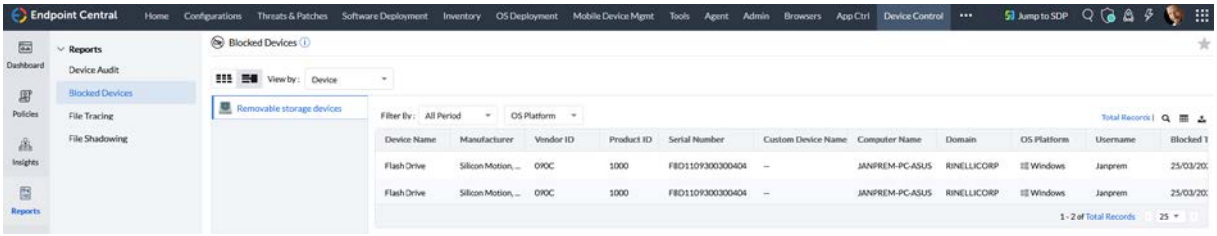
Es wird immer wieder Diskussionen geben, wenn ein Gerät geblockt ist und es wird auch immer ein ganz wichtiges Dokument sein, welches auf dem Stick ist. Ich für meinen Teil bin da immer sehr hart und kurz angebunden. Denn, was erlaubt ist, wird von mir ausgegeben. Dann wird das Gerät in einer Trusted 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

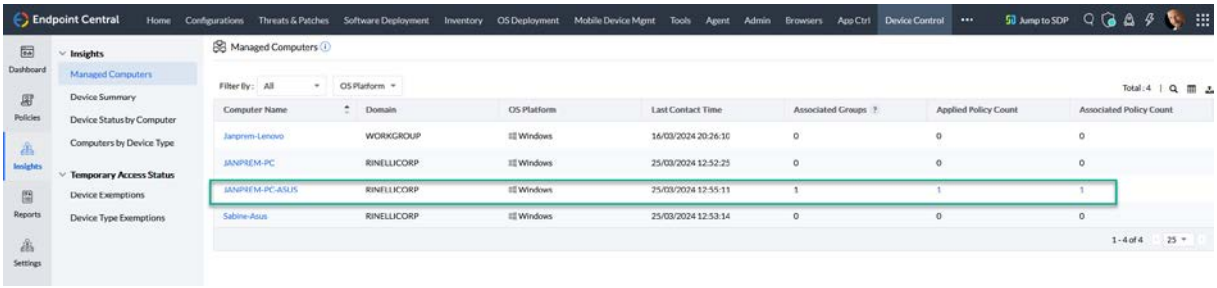
Über das Dashboard über die Blocked Devices sehe ich alle geblockten Geräte und auch, auf welchen Rechnern diese geblockt sind.



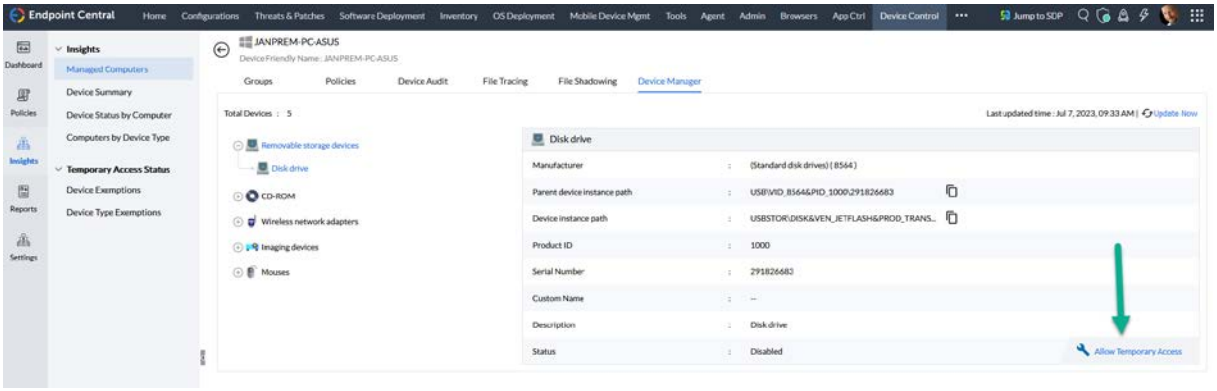


Hier kann ich mir die Geräte ansehen und auch die Serien Nummer finden.

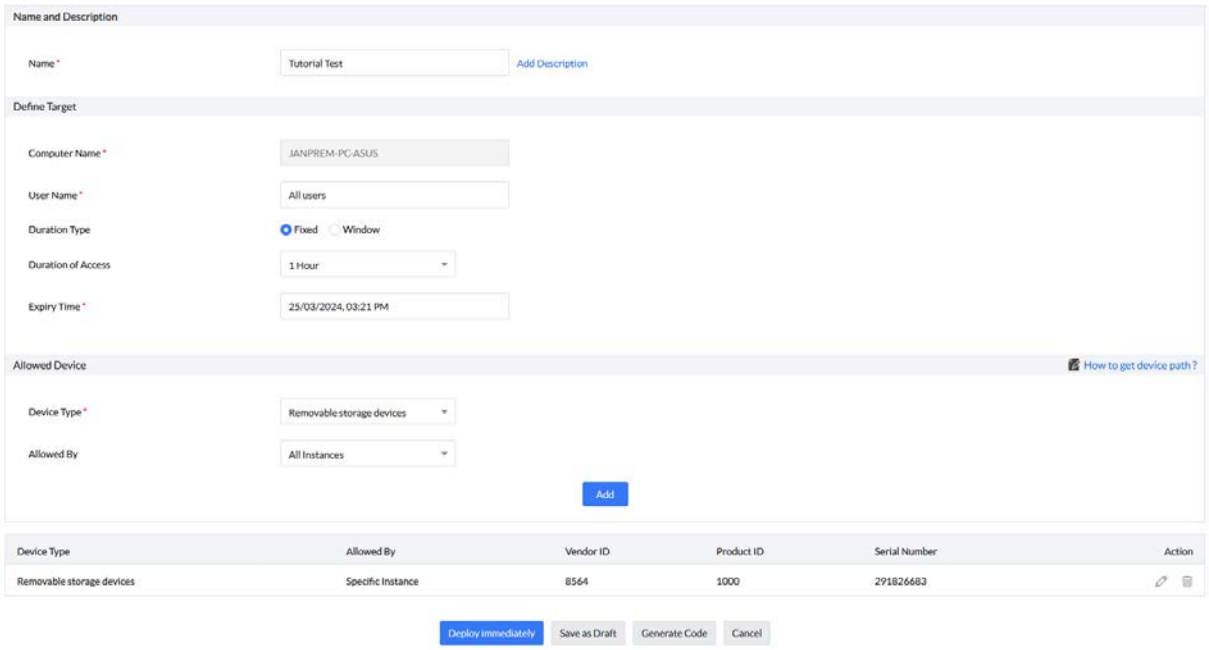
Einen temporären Zugriff gewähre ich ganz einfach über Insights / Managed Computers und die Auswahl des Rechners, an welchem der Stick hängt.

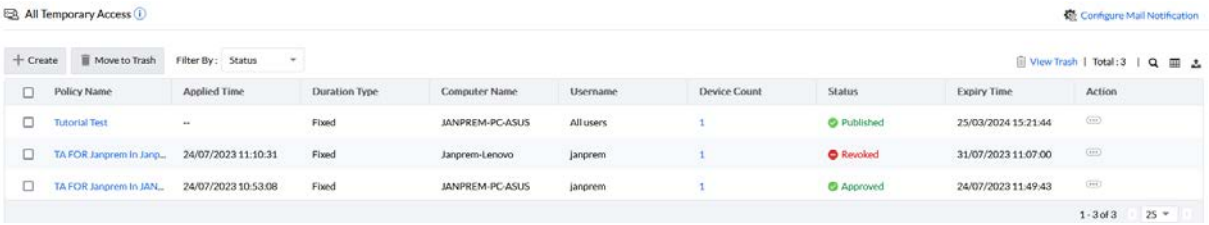


Es gibt jede Menge an Übersichten und Details, ich wechsle zum Tab „Device Manager“ und wähle „Allow Temporary Access“.



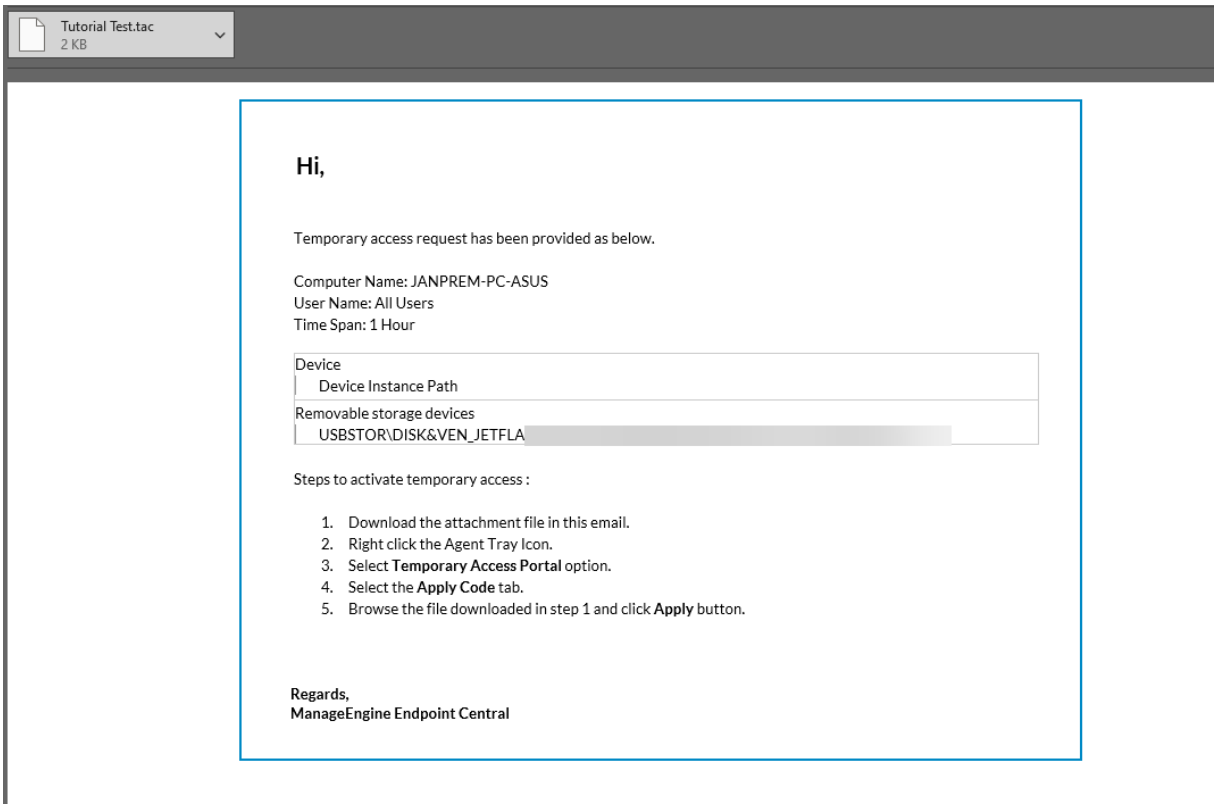
Hier wieder einen sprechenden Namen vergeben (in einer Produktivumgebung bitte eine Naming Convention verwenden), einen User auswählen, Zeitfenster und Device Type. Dann geht’s auch schon auf „Deploy Immediately“.

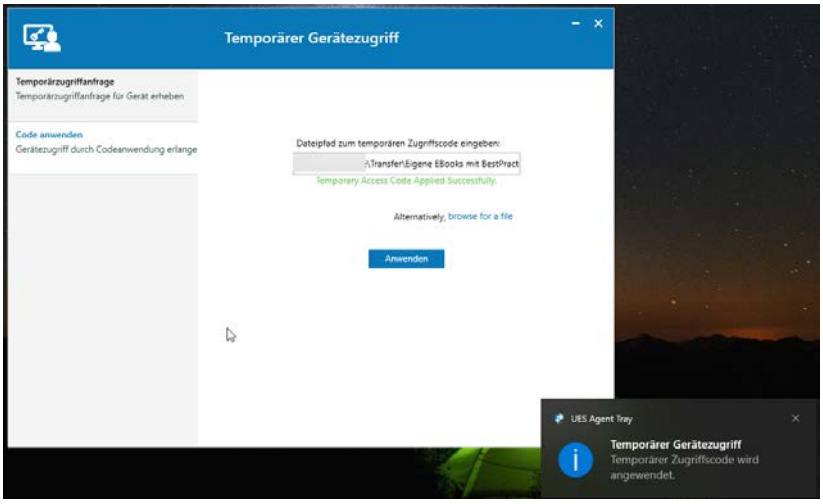




Auf dem Laptop poppt auch gleich eine Meldung auf:

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





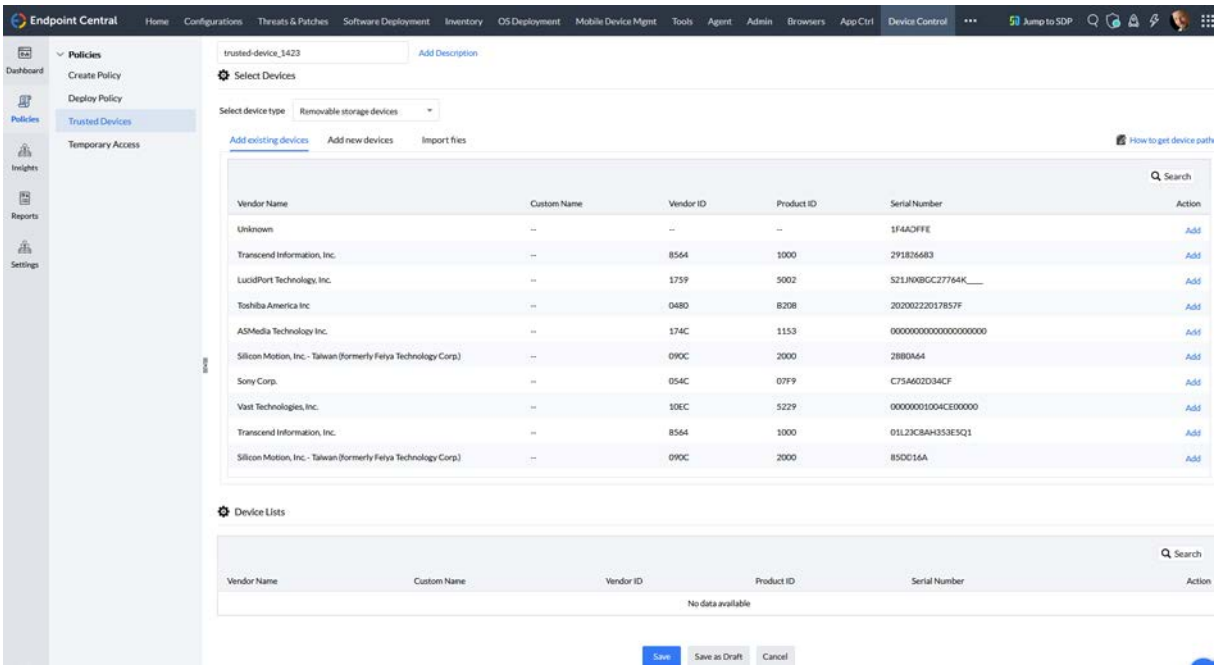
Nach Ablauf der Stunde wird das Device automatisch wieder geblockt.

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.

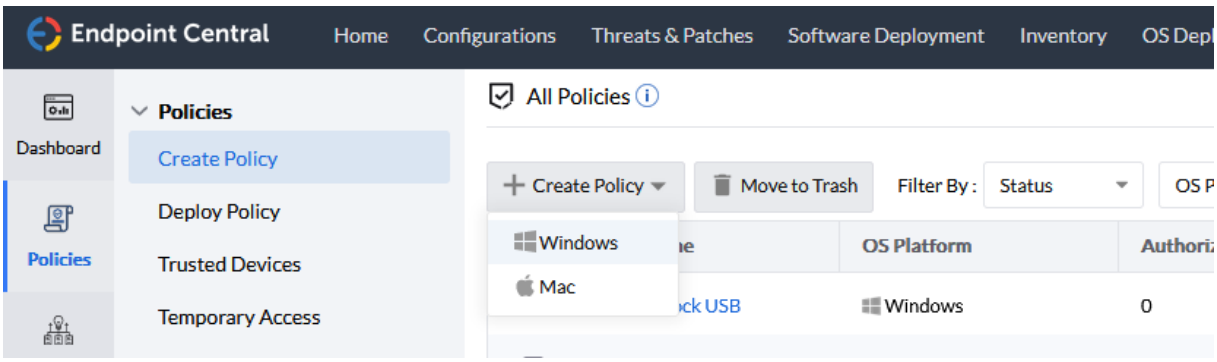
5. Trusted Device Listen und generelle Freigaben

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

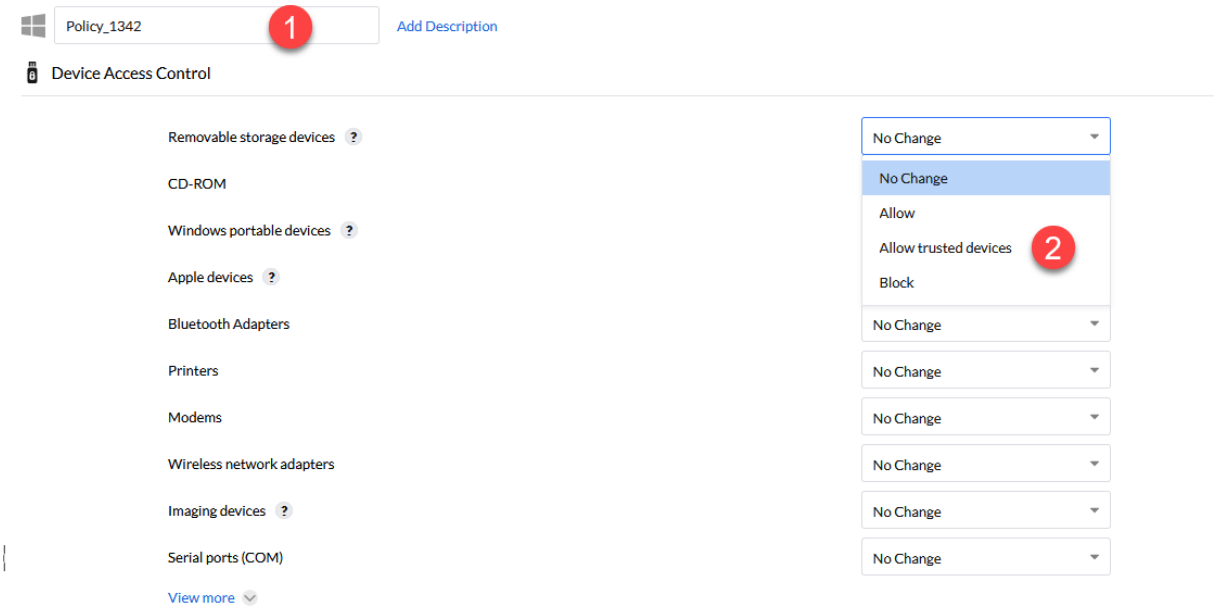
Hierzu eine Trusted Device Gruppe erstellen, einen sprechenden Namen vergeben, Device Typ auswählen und die gewünschten Geräte aus den Tabs.



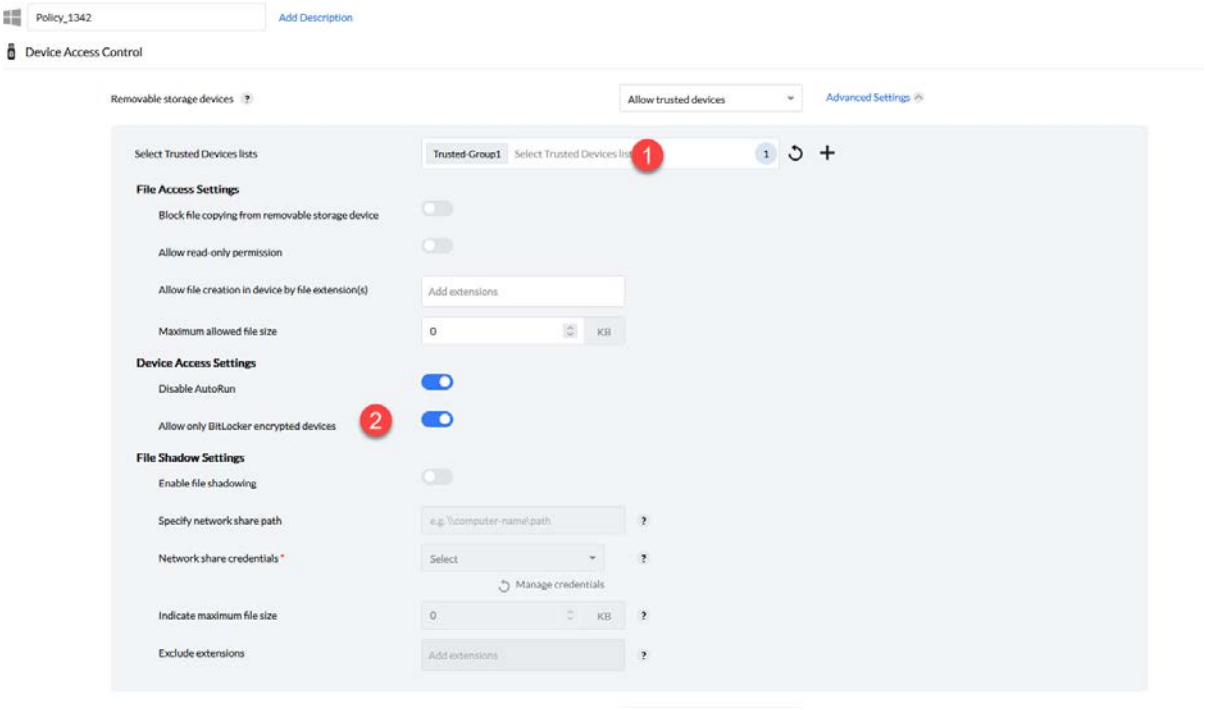
Dann benötige ich eine Policy über „Create Policy“:



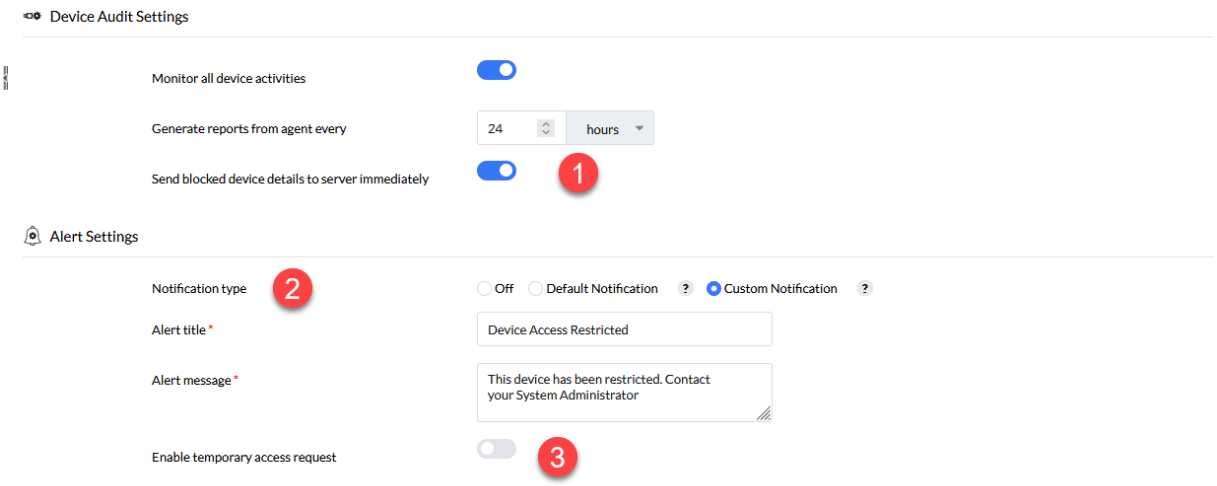
Hier wieder einen Namen vergeben (1) und aus der Liste dann in unserem Beispiel Removable storage devices / Allow trusted devices (2) auswählen.



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.



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).



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.