Application Control – Zero Trust einfach gemacht!

Meine Erfahrungen und einfache Schritte

Jürgen Rinelli

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

Inhalt

1. Ein paar Worte

Application Control! Oder eher die Kontrolle darüber, was auf Endgeräten ausgeführt werden darf.

Ist ne Menge drauf auf den Rechnern und warum?

- Weil viele Unternehmen nach wie vor ALLES was benötigt werden KÖNNTE, Grundinstallieren.
- Bloatware die auf vorinstallierten Systemen mit kommt
- Bloatware über die AppStores
- Lokal Admin Berechtigungen der Mitarbeiter!
- …

Heutige Strategie sollte es sein, Software nur über das Self-Service Portal bereit zu stellen und damit nicht auf jedem Rechner alles zu installieren. Warum auch unnötige Sicherheitslücken ins Unternehmen holen? Warum auf 950 von 1.000 Computern Software aktualisieren – oder verbieten – wenn sie nicht benötigt wird?

Bloatware ist so eine andere Sache, die gelangt über vom Hersteller oder Dienstleister vorinstallierte Systeme drauf. Wenn die IT dann diese Systeme nutzt ohne sie neu mit nem Basis Image aufzusetzen, … malt es euch aus.

Lokale Admins sind die besonderen Lieblinge der IT. Oft werden diese Rechte vergeben, weil es auch heute noch Software gibt, welche zum Ausführen solche benötigen.

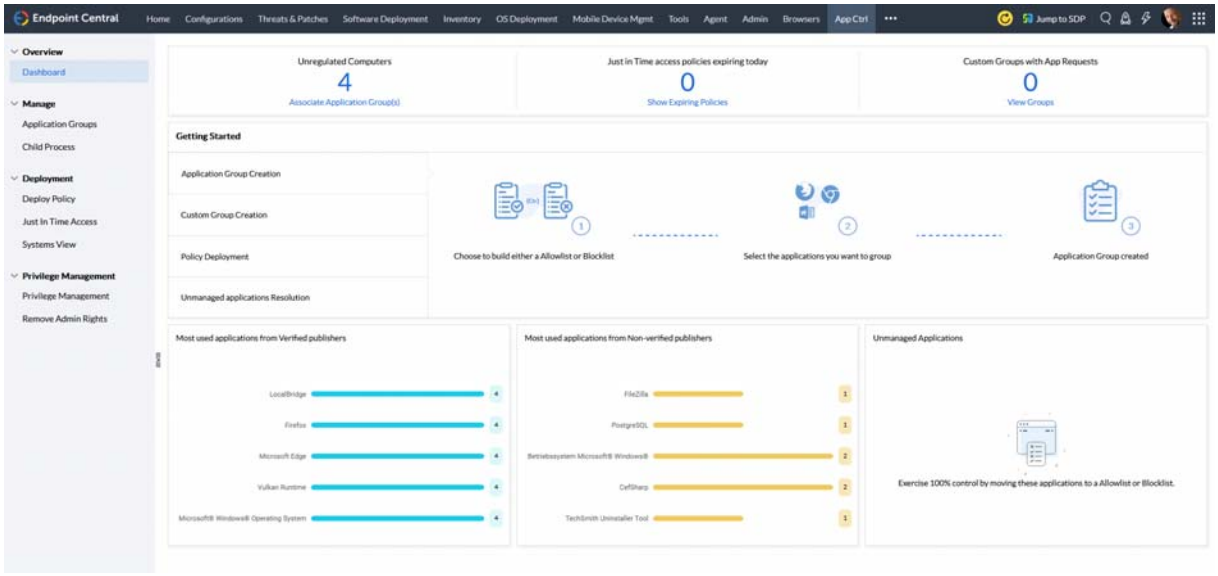
Heute will ich mich mit der Kontrolle – oder sanfter ausgedrückt – dem Management der Applikationen, befassen. Ich möchte anhand meines bevorzugten Tools „Endpoint Central“ und dem dazu gehörigen AddOn „App Ctrl“ zeigen, wie einfach man die Berechtigungen managen kann.

Was ich dadurch auch zeige ist, wie man sich im Applikations-Bereich an ein Zero Trust Szenario annähert um dieses Szenario dann durch eine strikte Whitelist endgültig umzusetzen.

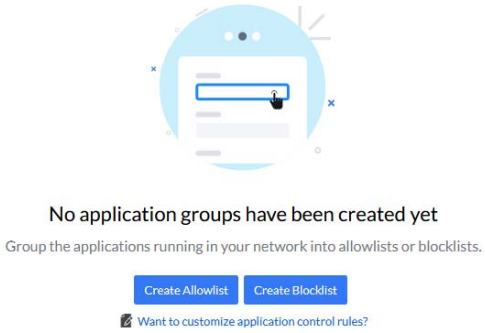
Also fangen wir an 😊

2. Application Group erstellen

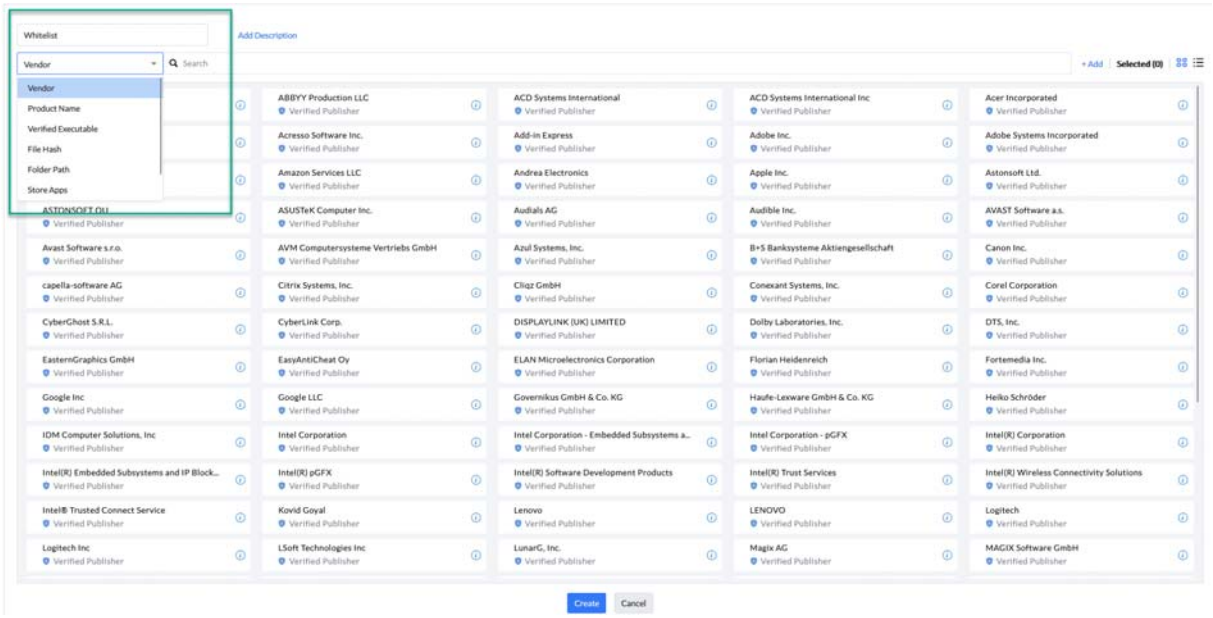
Noch sieht unser Dashboard sehr Jungfräulich aus 😊



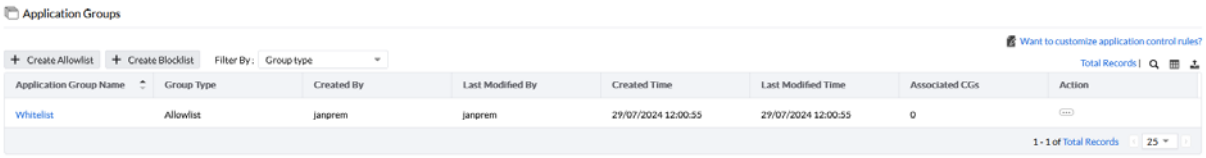
Also lasst uns als erstes eine Application Group über Manage/Application Groups, erstellen.



Wir beginnen mit einer Whitelist oder hier „Create Allowlist“.

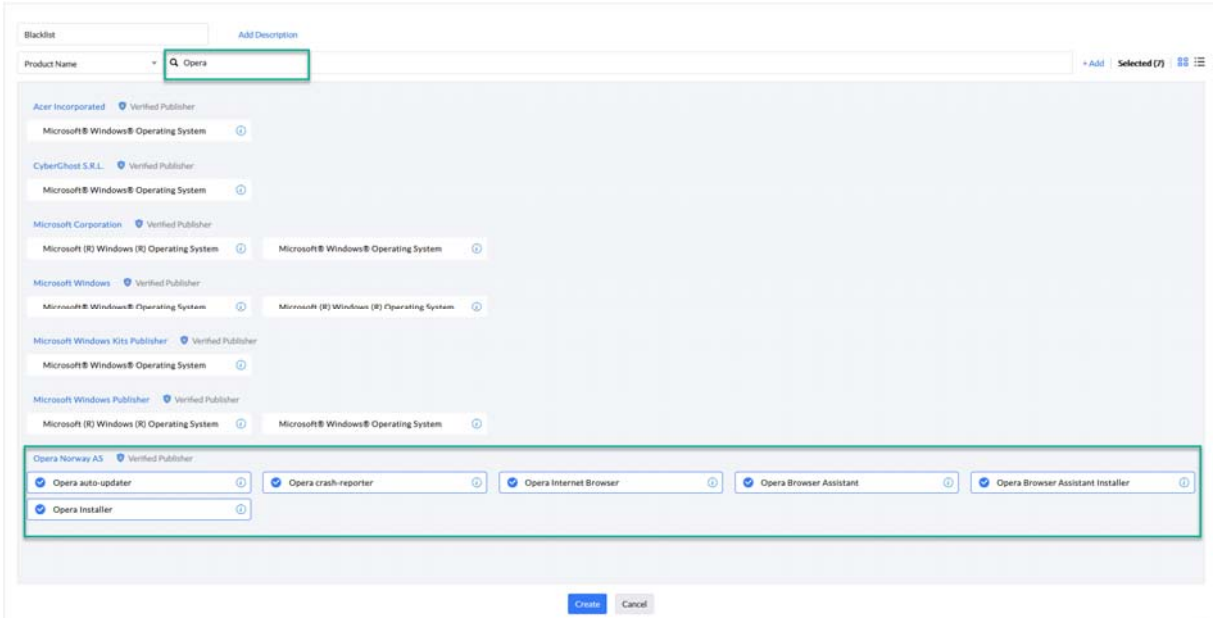


Ganz oben links vergebe ich den Namen „Whitelist“, einfach weils viel bekannter als „Allowlist“ ist. Dann kann ich alle mir bekannten Hersteller oder Produkte suchen und diese auswählen. Ich wähle hier für mein Beispiel, Produkt Name und dort suche ich nur Firefox, 7-zip und Winrar. Natürlich brauche ich auch alle Hardwaretreiber und alles was für das System relevant ist. Dazu kann ich auch einzelne neue Whitelists bauen. Also für HP, Lenovo, etc. einzelne Listen, wenn ich das möchte. Im Anschluss – genau! Gehen wir auf „Create“ um die Liste zu speichern.

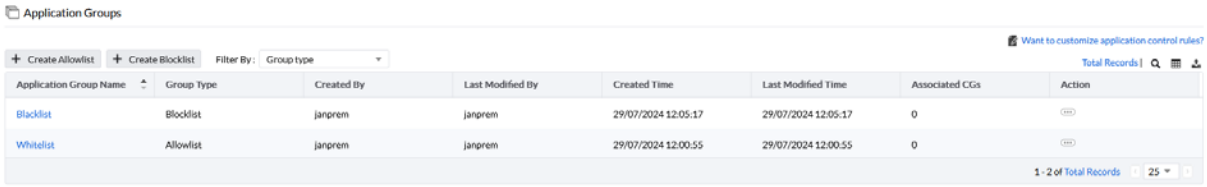


So haben wir die erste Application Group erstellt. Auf zur nächsten und diesmal eine „Blocklist“. Dazu oben auf „+ Create Blocklist“ gehen.

Ich bezeichne die Liste mit „Blacklist“ und gebe im Suchfeld nur `Opera´ ein und wähle alles das er findet. Nein! Ich habe nichts gegen den Browser. Ich mag ihn persönlich sogar sehr. Das ist nur ein Beispiel 😊

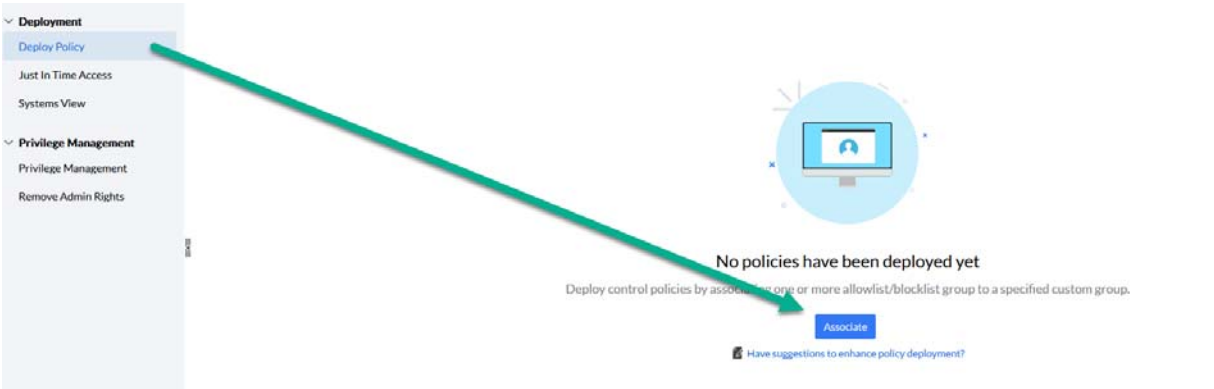


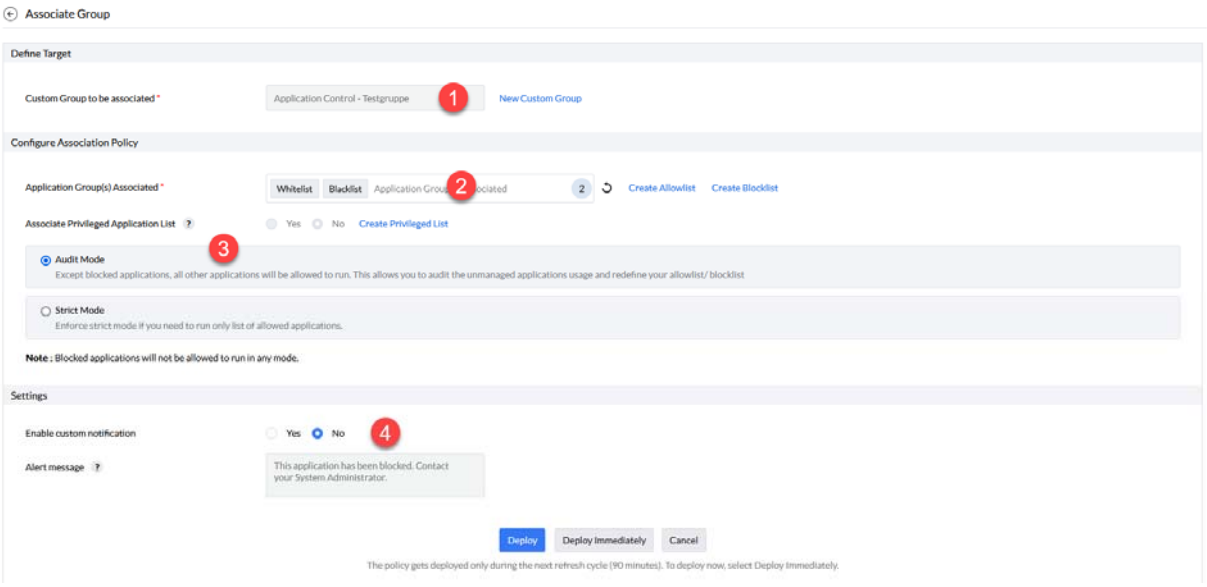
Nach dem notwendigen Speichern über `Create´ haben wir was wir brauchen um durch den Prozess zu gehen.



3. Deployment

Jetzt können wir unser erstes Deployment der erstellten Listen durchführen. Deploy Policy/Associate:





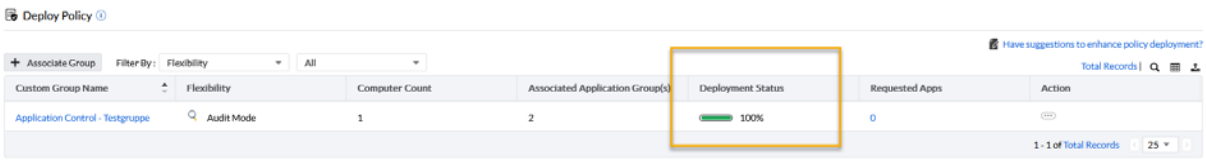
Punkt 1:
Eine über Custom Groups erstellte Gruppe an Systemen auswählen.

Punkt 2:
Die Whitelist/Allowlist sowie die Black/Blocklist auswählen.

Punkt 3:
Ein Audit Mode erlaubt es das alles das nicht auf der Whitelist steht, dennoch ausgeführt wird. Strikt Mode wäre dann der Zero Trust.

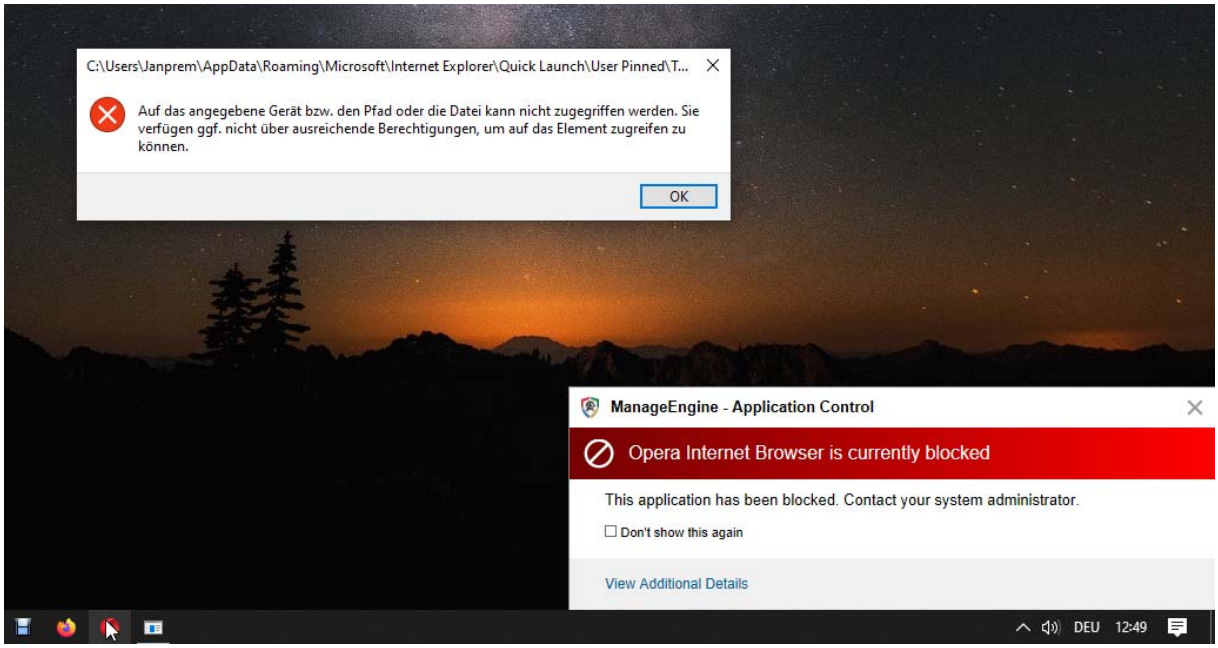
Punkt 4:
Ich kann – wenn ich will – auch eine eigene Mitteilung verfassen, welche aufpoppt wenn ein User eine blockierte Anwendung öffnen möchte.

Nach dem obligatorischen `Deploy´, wird die Sache scharf geschaltet und wenn der Deployment Status wie im Bild, Grün und auf 100% steht, ist sie auf allen Systemen angekommen.

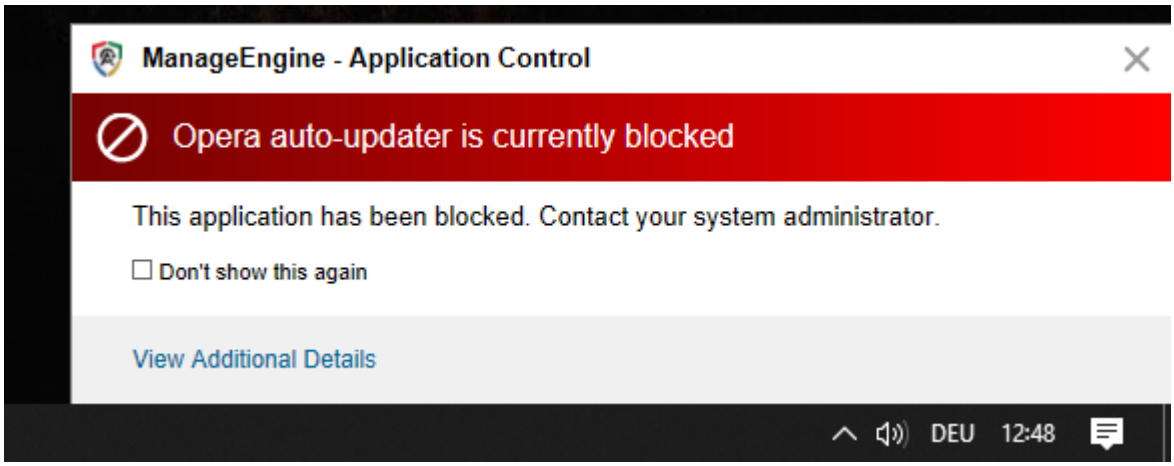


Sehen wir uns doch mal an was auf der Client-Seite passiert wenn ich Opera öffnen will.

Ohho … da geht doch wirklich nix mehr!



Selbst der Auto-Updater bringt sofort eine Meldung.

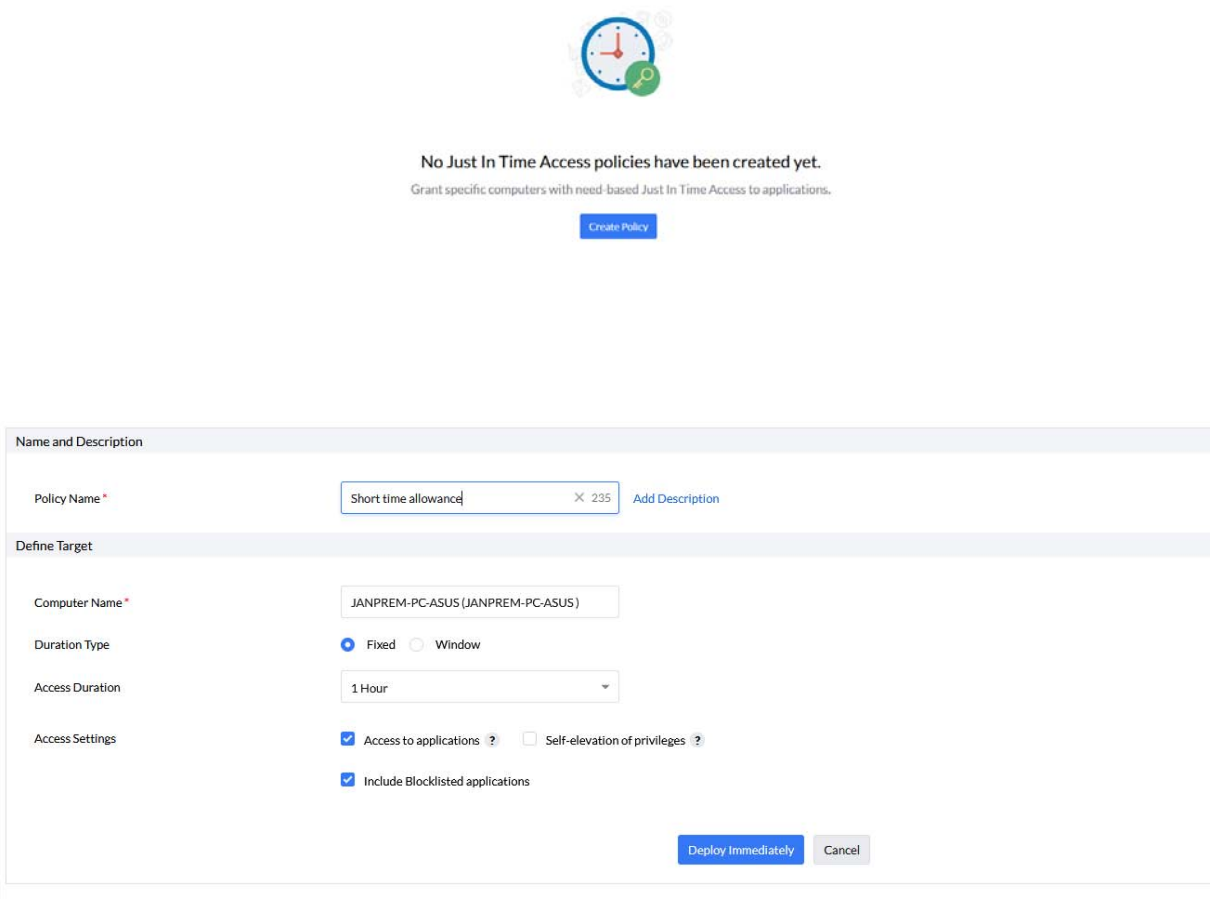


Ich kann die Meldungen natürlich dauerhaft verhindern. Auf jeden Fall läuft nun kein Opera. Mein Test zeigt das es sehr einfach ist solche Policies zu erstellen und zu verteilen.

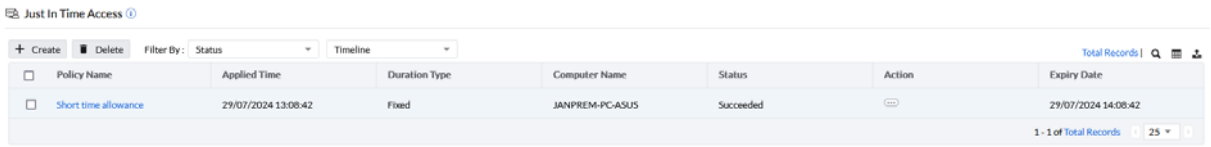
Im Strict Mode würde keine Applikation starten welche nicht auf der freigegebenen Liste steht. Hier kann ich auch mit User-Anfragen arbeiten.

4. Management

Über Just In Time Access kann ich Mitarbeitern auch zeitgebundenen Zugriff gewähren.



Namen vergeben, Computer wählen, Zeitfenster angeben und Access gewähren >> Deploy Immediately

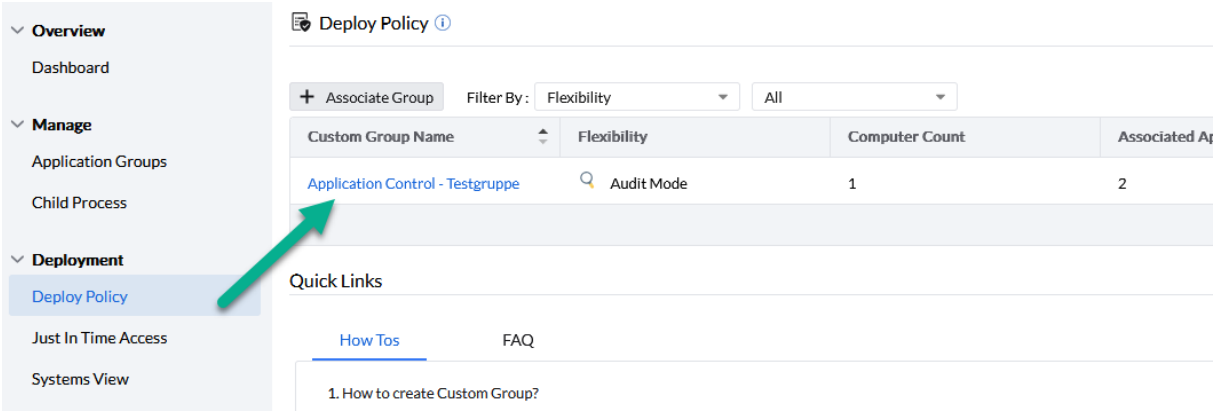


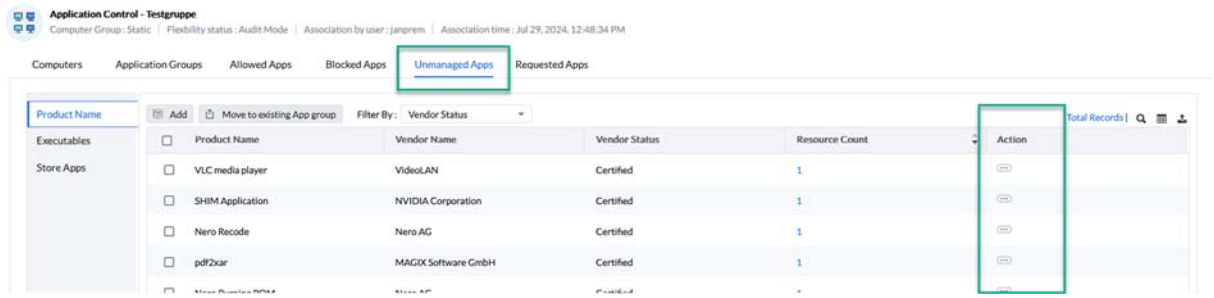
In derselben Minute besteht ein zeitgebundener Zugriff auf dem gewählten System. Schön dabei ist, dass ich so einem Techniker den vollen Zugriff gewähren kann und selbst wenn ich es vergesse, der Zugriff nach Ablauf der Zeit wieder eingeschränkt ist. Ich kann natürlich auch manuell sofort über den Action Button, die Policy löschen. Damit wird der Zugriff auch sofort wieder verweigert.

Wenn ich mich auf ein Zero Trust hinarbeiten will, dann benötige ich Zeit. In der Regel kenne ich nicht alle Applikationen welche für den sauberen Betrieb meiner Systeme notwendig sind. D.h. sollte ich sofort auf Strict Mode gehen, könnte es sein das meine Hotline wirklich Heiß läuft.

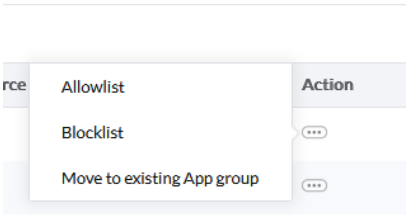
Deshalb empfehle ich mit Vorlauf zu arbeiten und alles was mir bekannt ist bereits auf eine der Listen zu setzen und dann nach und nach einzelne Applikationen aus der Liste der `Unmanaged Apps´ auszusortieren.

Dazu gehen wir auf die Deployment Policy welche wir für den Test erstellt haben.

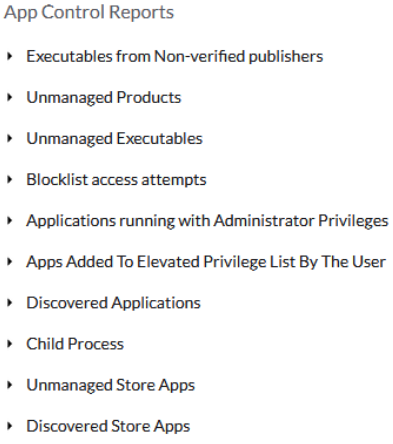




Über das Tab `Unmanaged Apps´ können wir dann die die Liste durchgehen und über die Action Buttons auf die Listen zuweisen.



Umfangreiche Reports helfen mir bei meinem weiteren Management.

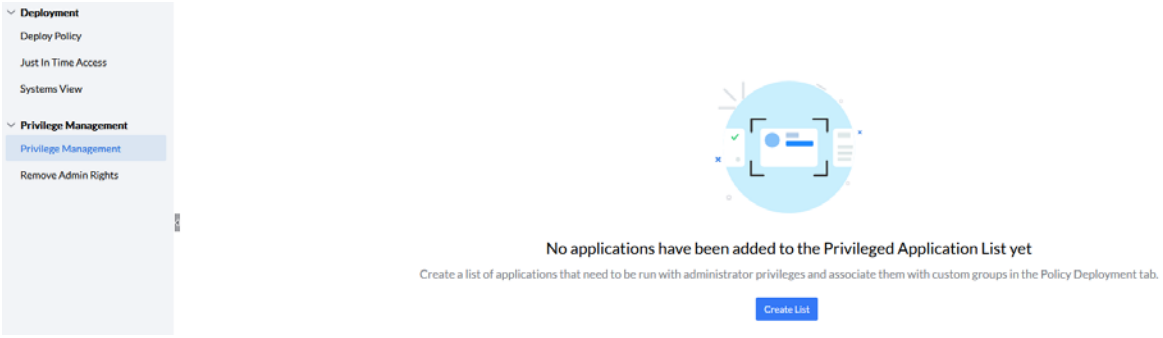


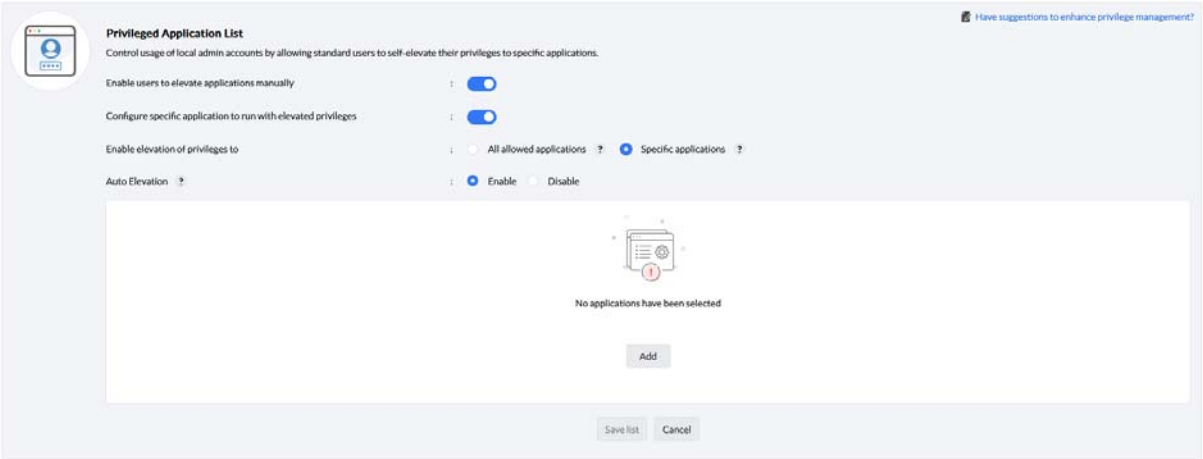
5. Privilege Management

Nun zu den Lokal Admins … ihr glaubt doch nicht das ich Euch vergessen habe?

In meiner Lieblingssuite gibt es natürlich auch die Möglichkeit, euch an den Kragen zu gehen 😊

Dazu kann ich eine Liste mit Applikationen erstellen, welche für die Ausführung, die Lokal Admin Rechte benötigen. Dann gebe ich vom System aus, diese Rechte mit – und befreie meine IT-Landschaft von unnötigen Lokal Admins.





Ich kann hier dem User erlauben manuell eine Applikation mit erhöhten Rechten zu versehen sowie nur spezielle Applikationen mit erhöhten Rechten zu versehen.

Die Applikationen kann ich über `Add´ auswählen.

Im letzten Schritt nehme ich dem User seine Lokal Admin Rechte.

6. Schlußworte

Ich hoffe, ich konnte einen Weg hin zur Application Control und einem Zero Trust aufzeigen. Zero Trust ist nichts das ich einfach mal eben scharf schalten kann, deshalb ist es wichtig frühzeitig damit zu beginnen. Klar – Heute kann es sein das ihr das nicht braucht. Doch kann es morgen bereits anders sein. Dann ist es von Vorteil, wenn ich bereits damit begonnen habe eine White und eine Black List zu erstellen. Denn wenn es heißt „Wir brauchen das“, dann wird es meist ein „Hätte Vorgestern schon da sein sollen!“

In diesem Sinne – Have Fun and stay safe 😊

Euer Jürgen Rinelli

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.