Application Control – Zero Trust made easy!

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 3
2. Create Application Group 4
3. Deployment 6
4. Management 9
5. Privilege Management 11
6. Closing words 12
7. About the author 13

1. A few words

Application control! Or rather the control over what can be executed on end devices.

There´s a lot on the computers and why?

- Because many companies still install EVERYTHING that COULD be needed.
- Bloatware that comes with pre-installed systems
- Bloatware via the AppStores
- Local admin authorisations for employees!
- ...

Today's strategy should be to provide software only via the self-service portal and not to install everything on every computer. Why introduce unnecessary security vulnerabilities into the company? Why update - or prohibit - software on 950 out of 1,000 computers if it is not needed?

Bloatware is another matter, it is installed via systems pre-installed by the manufacturer or service provider. If the IT then uses these systems without setting them up again with a base image ... picture it!

Local admins are the special favourites of IT. These rights are often assigned because there is still software that requires them to run.

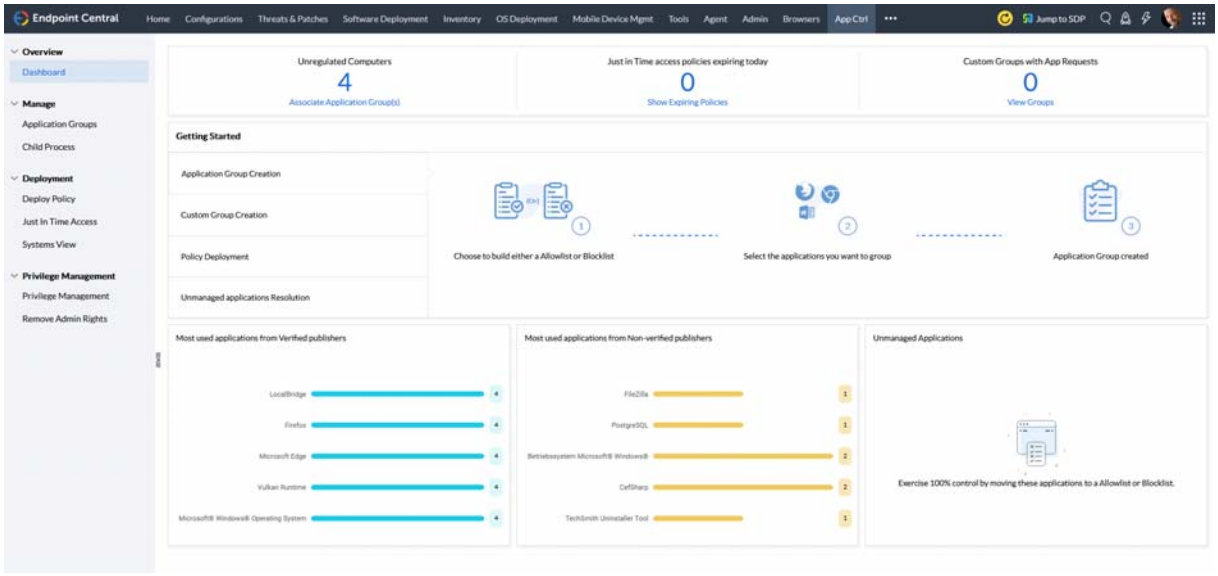
Today I want to look at the control - or to put it more gently - the management of applications. Using my favourite tool 'Endpoint Central' and the associated add-on 'App Ctrl', I would like to show you how easy it is to manage permissions.

I will also show you how to approach a zero trust scenario in the application area and then finally implement this scenario with a strict whitelist.

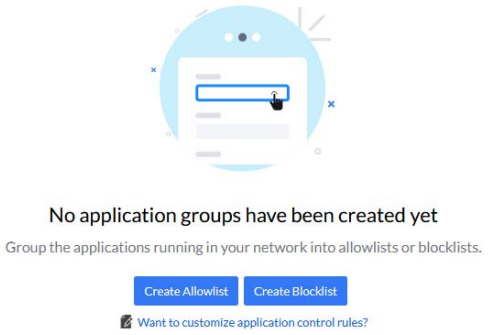
So let's get started 😊

2. Create Application Group

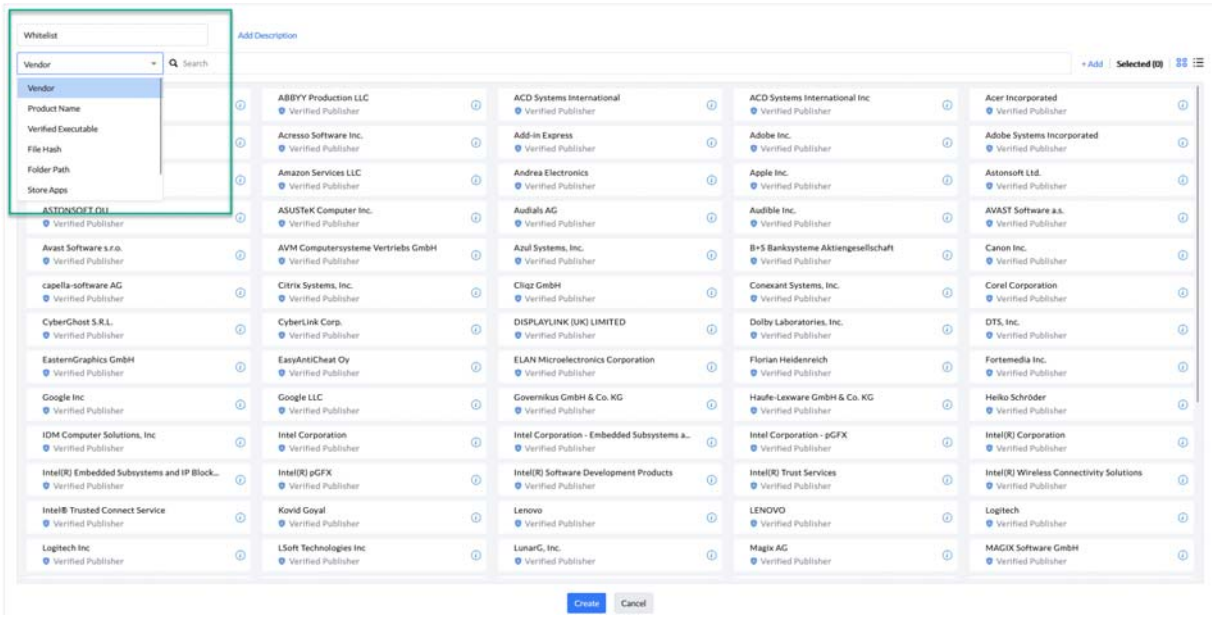
Our dashboard still looks very virgin 😊



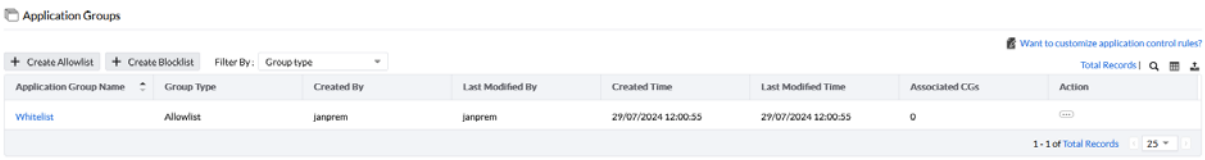
So let's start by creating an application group via Manage/Application Groups.



We start with a whitelist or here ‘Create Allowlist’.

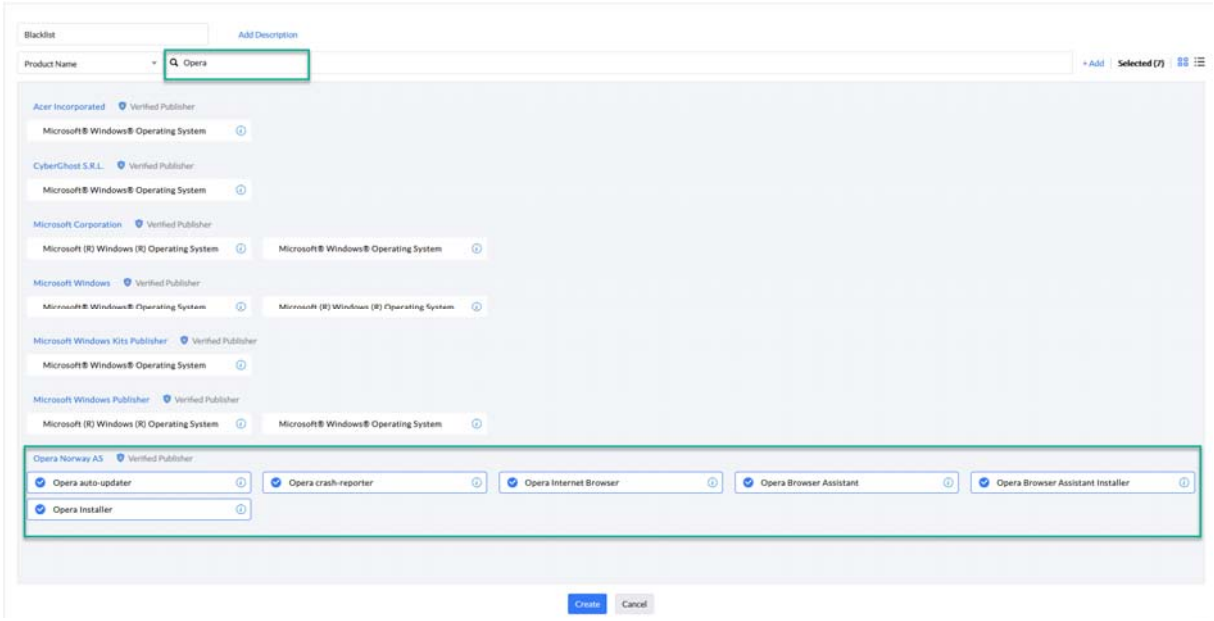


At the top left I assign the name ‘Whitelist’, simply because it is much better known than ‘Allowlist’. I can then search for all known manufacturers or products and select them. For my example, I choose Product Name and search only for Firefox, 7-zip and Winrar. Of course, I also need all hardware drivers and everything that is relevant for the system. I can also create individual new whitelists. So individual lists for HP, Lenovo, etc., if I want to. Afterwards - exactly! Let's go ‘Create’ to save the list.

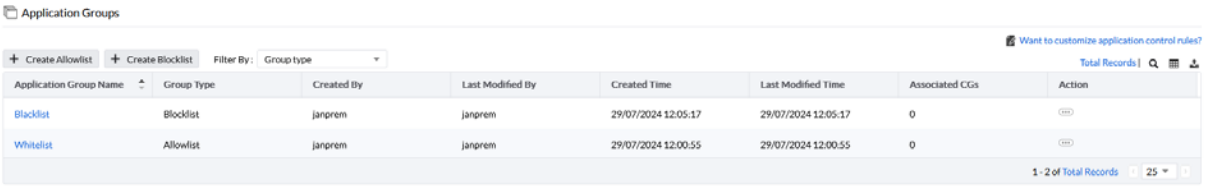


So we have created the first application group. On to the next one and this time a ‘Blocklist’. To do this, go to ‘+ Create Blocklist’ at the top.

I label the list ‘Blacklist’ and enter only ‘Opera’ in the search field and select everything it finds. No! I have nothing against the browser. In fact, I personally like it a lot. This is just an example 😊

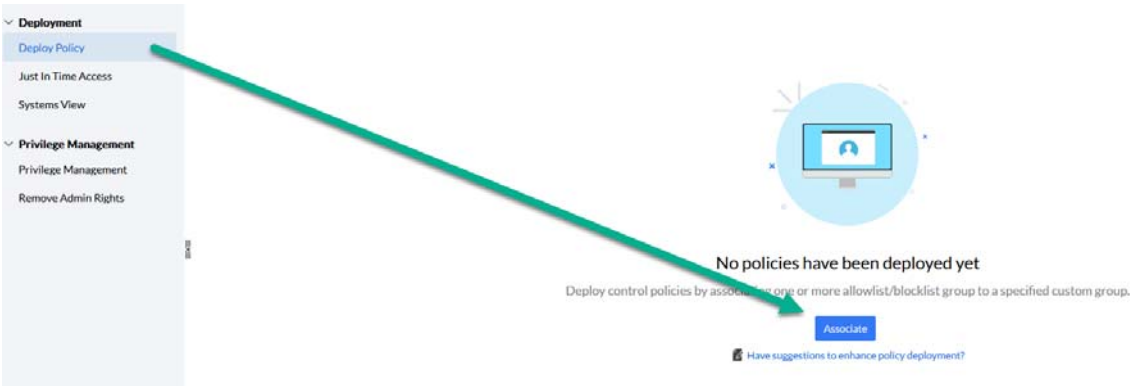


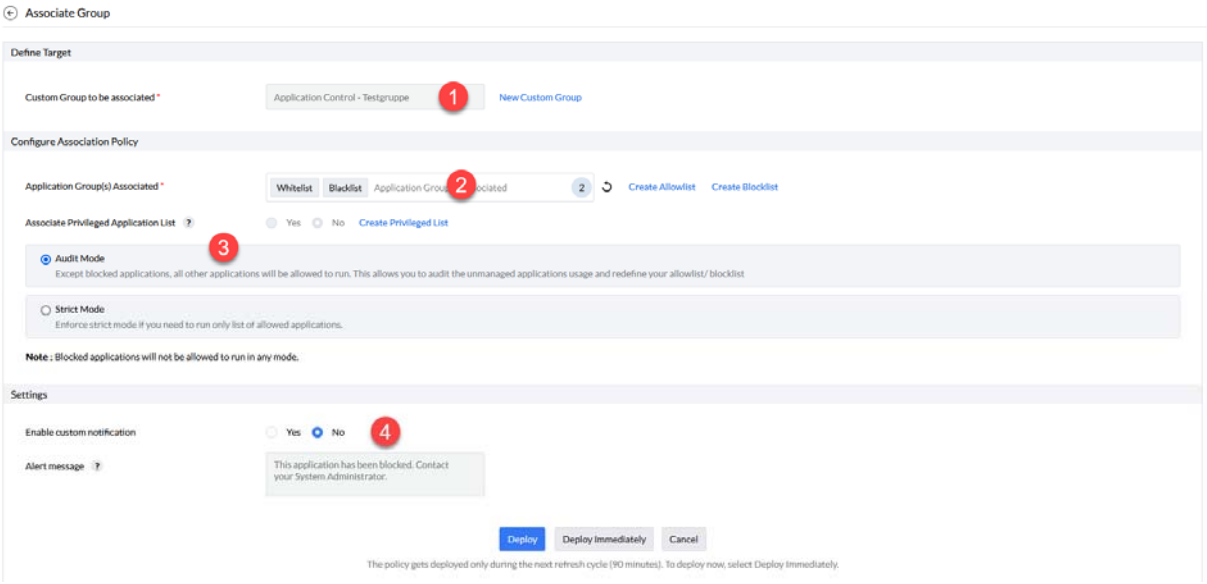
After the necessary saving via `Create' we have what we need to go through the process.



3. Deployment

Now we can carry out our first deployment of the created lists. Deploy Policy/Associate:





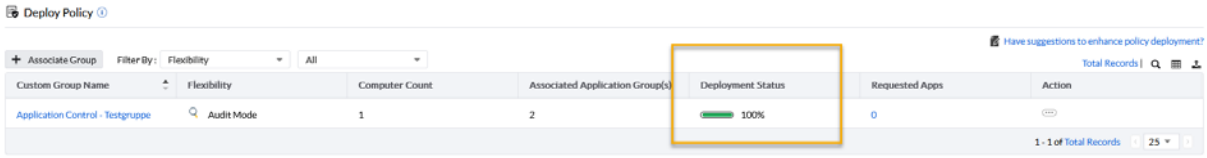
Point 1:
Select a group of systems created via Custom Groups.

Point 2:
Select the whitelist/allowlist and the blacklist/blocklist.

Point 3:
An audit mode allows everything that is not on the whitelist to still be executed. Strict mode would then be zero trust.

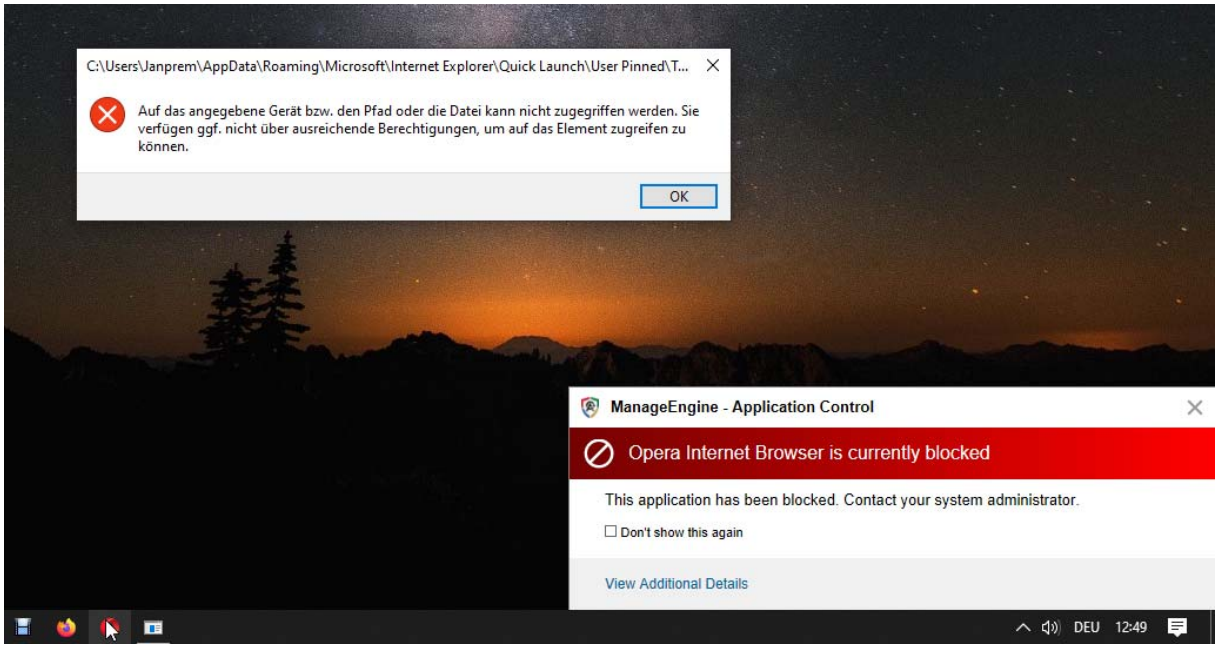
Point 4:
If I want, I can also create my own message that pops up when a user wants to open a blocked application.

After the obligatory 'Deploy', the system is activated and when the deployment status is green and at 100%, as shown in the picture, it has arrived on all systems.

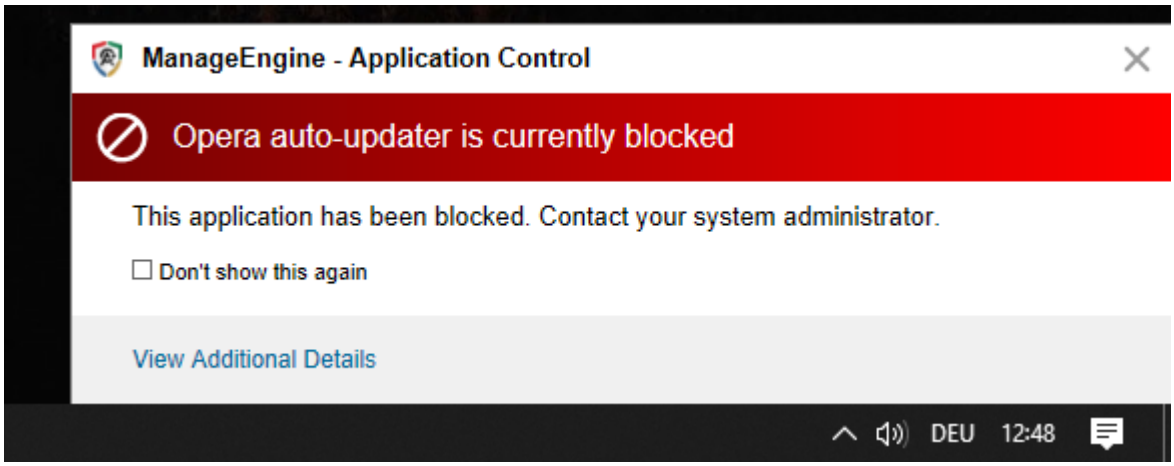


Let's take a look at what happens on the client side when I want to open Opera.

Ohho … nothing really works anymore!



Even the auto-updater immediately displays a message.

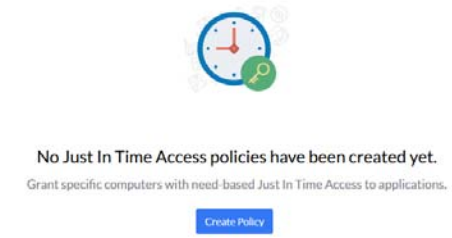


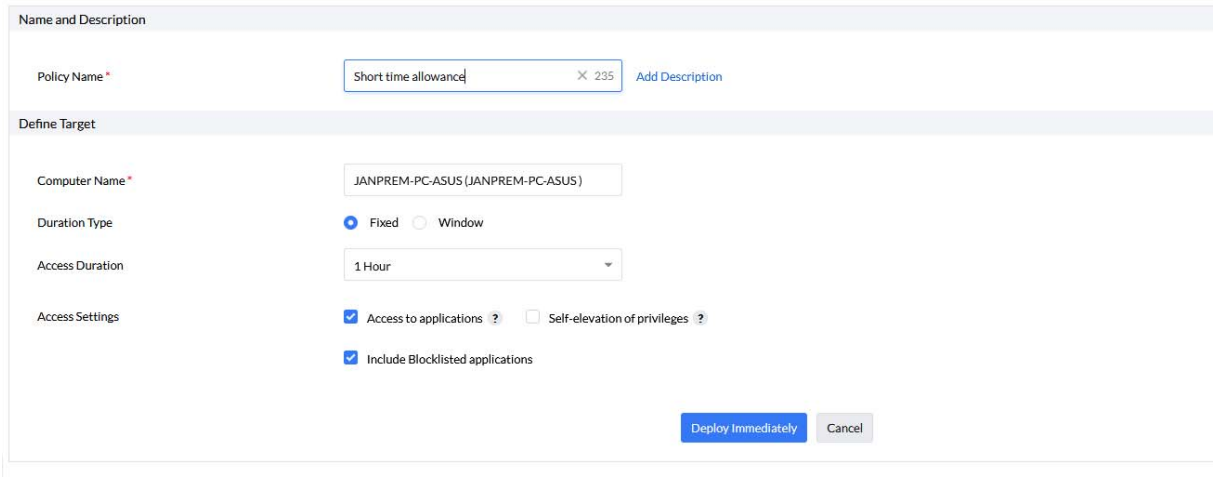
I can of course prevent the messages permanently. In any case, Opera is now not running. My test shows that it is very easy to create and distribute such policies.

In strict mode, no application would start that is not on the approved list. Here I can also work with user requests.

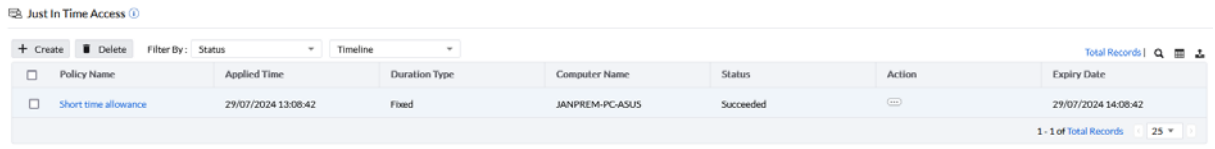
4. Management

With Just In Time Access I can also grant employees time-limited access.





Assign name, select computer, specify time window and grant access >> Deploy Immediately

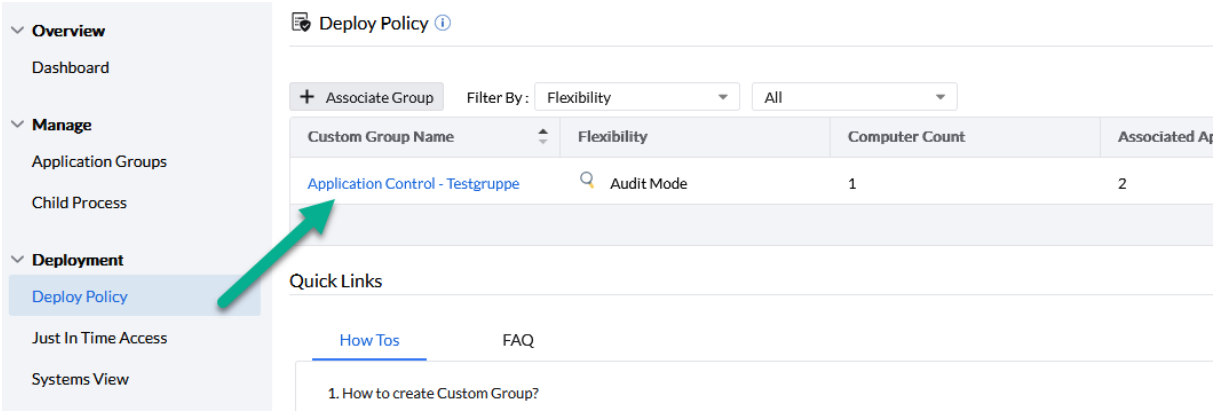


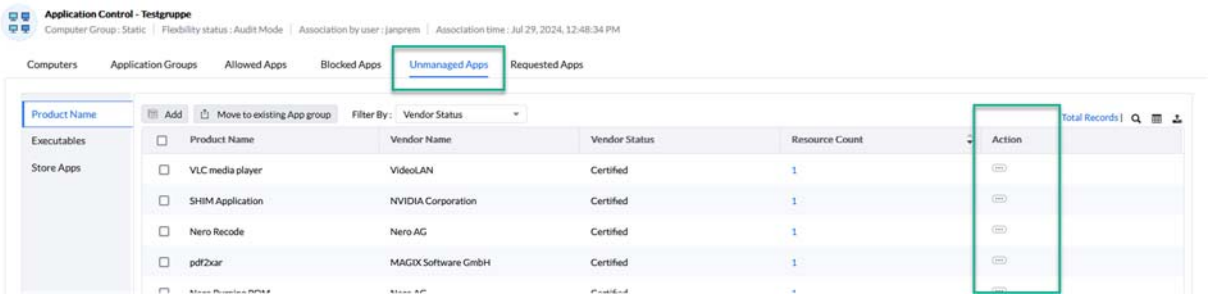
In the same minute, there is time-limited access to the selected system. The nice thing about this is that I can grant a technician full access and even if I forget, access is restricted again after the time has expired. Of course, I can also delete the policy manually immediately using the action button. This as well immediately denies access again.

If I want to work towards a Zero Trust, then I need time. Normally I don't know all the applications that are necessary for the clean operation of my systems. This means that if I go to strict mode straight away, my hotline could run really hot.

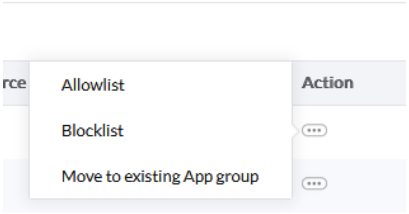
I therefore recommend working in advance and adding everything I know to one of the lists and then gradually removing individual applications from the ‘Unmanaged Apps’ list.

To do this, we go to the deployment policy that we created for the test.

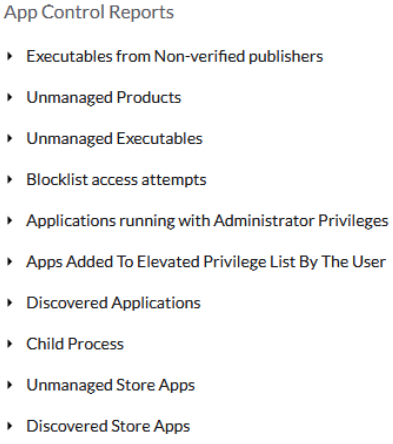




We can go through the list via the 'Unmanaged Apps' tab and assign them to the lists using the action buttons.



Comprehensive reports help me with my further management.

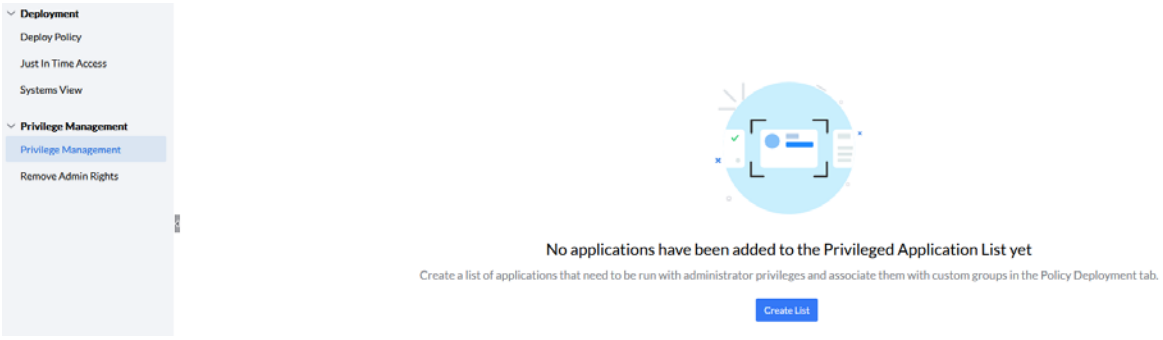


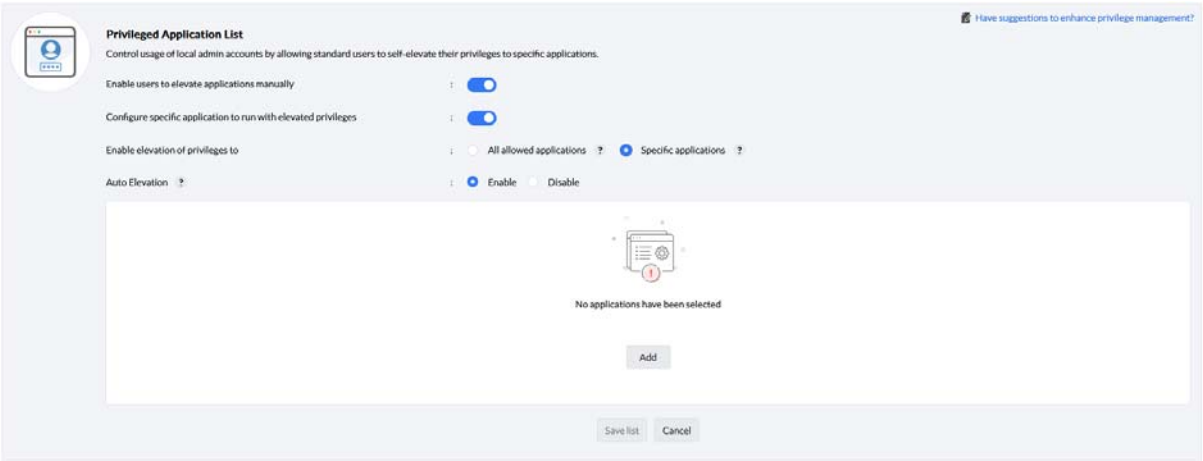
5. Privilege Management

Now to the local admins ... you don't think I've forgotten you, do you?

In my favourite suite, of course, there is also the opportunity to go for your collar 😊

To do this, I can create a list of applications that require local admin rights to run. I then assign these rights from the system - and rid my IT landscape of unnecessary local admins.





I can allow the user to manually assign elevated rights to an application or to assign elevated rights only to specific applications.

I can select the applications via ‘Add’.

In the last step, I remove the user's local admin rights.

6. Closing words

I hope I have been able to show you a way towards application control and zero trust. Zero Trust is not something I can just switch on, so it is important to start early. Sure - you may not need it today. But it could be different tomorrow. Then it is an advantage if I have already started to create a white list and a black list. Because when it says ‘We need this’, it usually becomes ‘Should have been there the day before yesterday!’

With this in mind - Have fun and stay safe 😊

Cheers

Jürgen Rinelli

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.