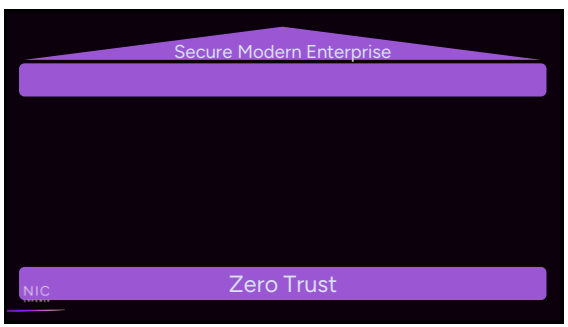
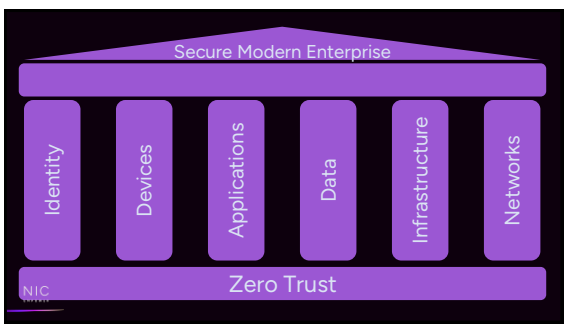
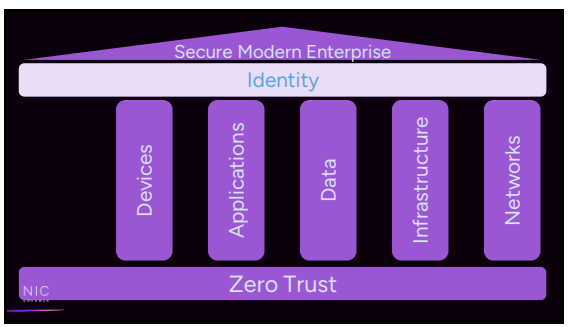

NIC
EMPOWER
November 13-15, Oslo Spektrum

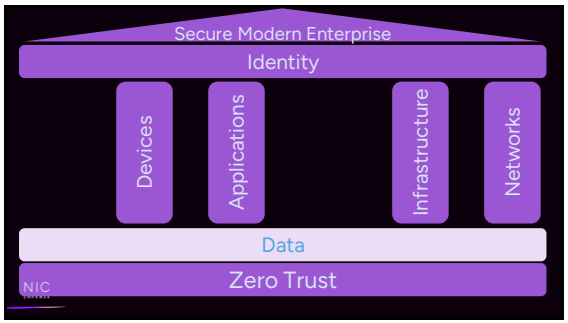

Intune-Driven Approaches
to Minimize
Local Admin Risks
Simon Skotheimsvik
Senior Cloud Consultant,
CloudWay
/in/simonskotheimsvik
@sskotheimsvik
@sskotheimsvik.bsky.social
skotheimsvik.no
linktr.ee/simonskotheimsvik
NIC

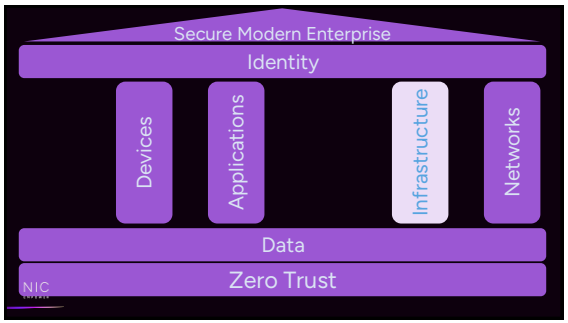

1 Why?
NIC

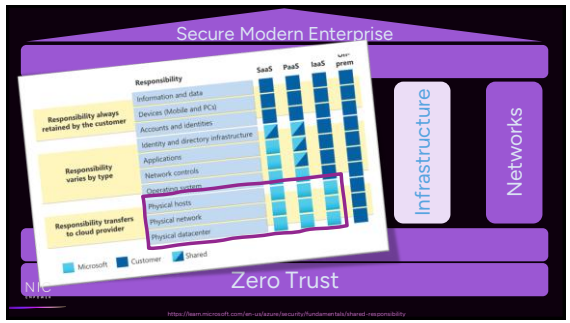

Secure Modern Enterprise
NIC
Zero Trust

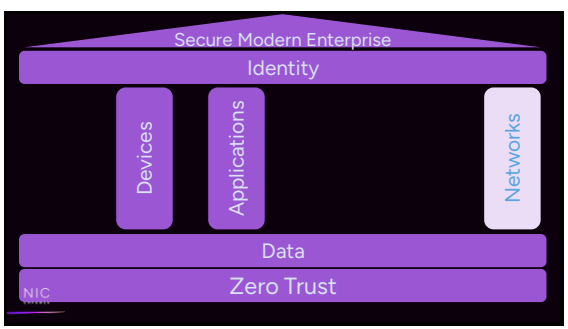

Secure Modern Enterprise
Identity
Devices
Applications
Data
Infrastructure
Networks
NIC
Zero Trust

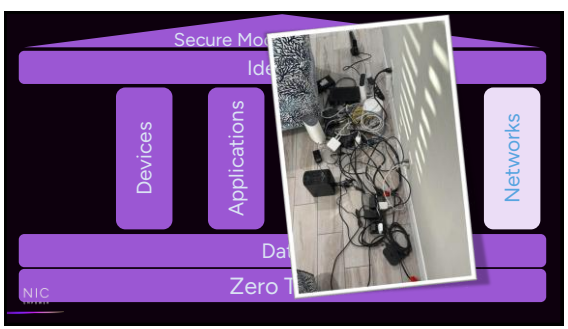

Secure Modern Enterprise
Identity
Devices
Applications
Data
Infrastructure
Networks
NIC
Zero Trust

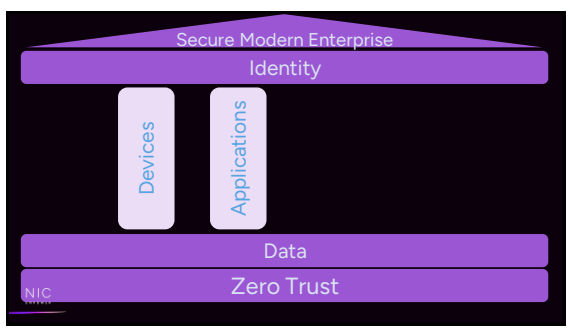

Secure Modern Enterprise
Identity
Devices
Applications
Infrastructure
Networks
Data
NIC
Zero Trust


Secure Modern Enterprise
Identity
Devices
Applications
Infrastructure
Networks
Data
NIC
Zero Trust


Secure Modern Enterprise
Responsibility always retained by the customer
Responsibility varies by type
Responsibility transfers to cloud provider
Information and data
Devices (Mobile and PCs)
Accounts and identities
Identity and directory infrastructure
Applications
Network controls
Operating system
Physical hosts
Physical network
Physical datacenter
SaaS
PaaS
IaaS
prem
Microsoft
Customer
Shared
Infrastructure
Networks
NIC
Zero Trust

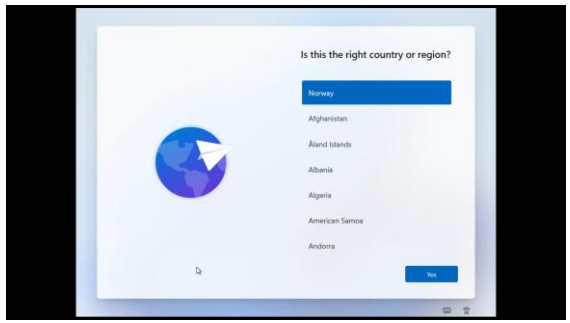

Secure Modern Enterprise
Identity
Devices
Applications
Networks
Data
NIC
Zero Trust

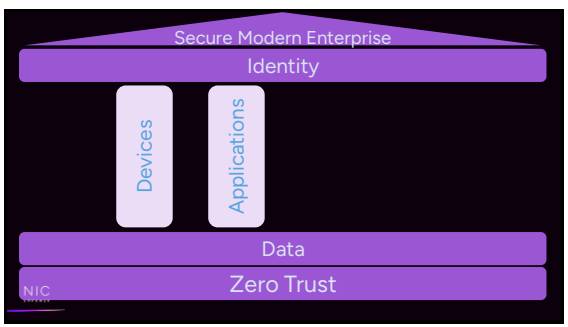

Devices
Applications
Networks
NIC

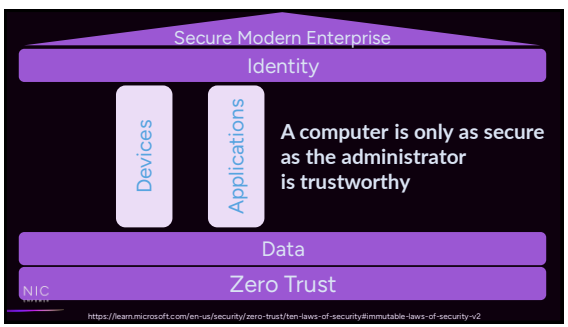

Secure Modern Enterprise
Identity
Devices
Applications
Data
NIC
Zero Trust

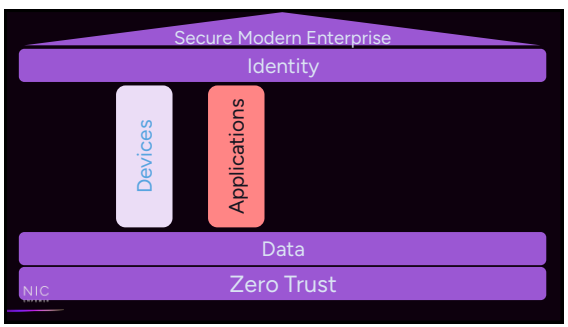
1 Why?

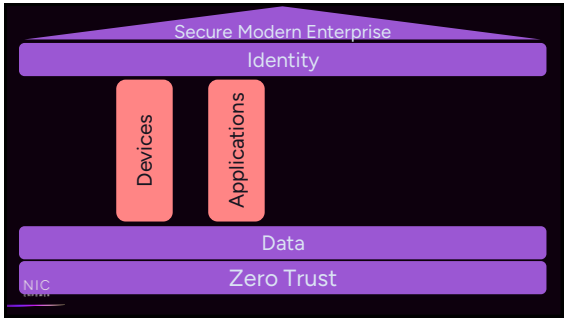
2 Why?
We must know, and trust our devices!

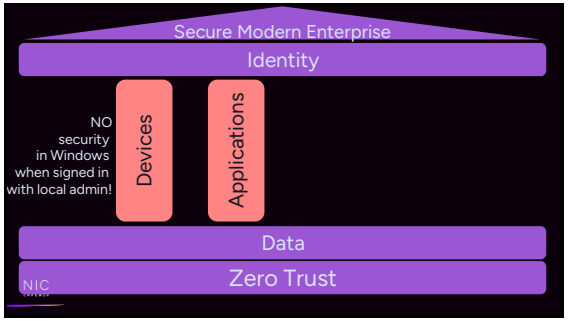






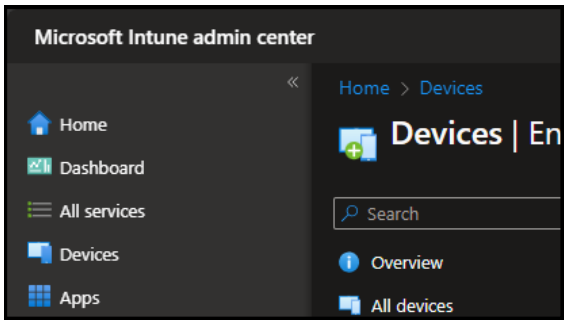


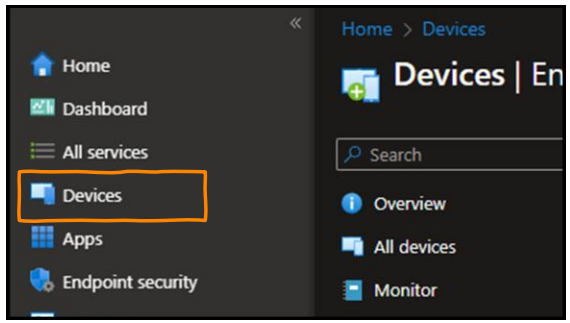

Secure Modern Enterprise
Identity
Devices
Applications
Data
Zero Trust
NIC

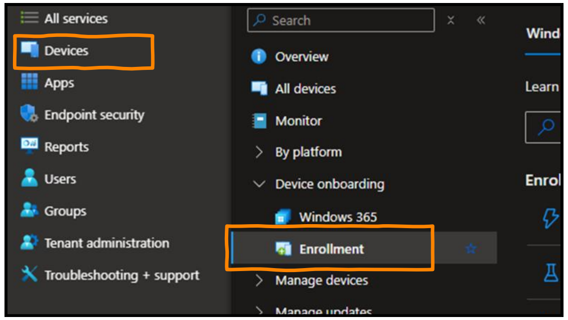

Secure Modern Enterprise
Identity
NO security in Windows when signed in with local admin!
Devices
Applications
Data
Zero Trust
NIC

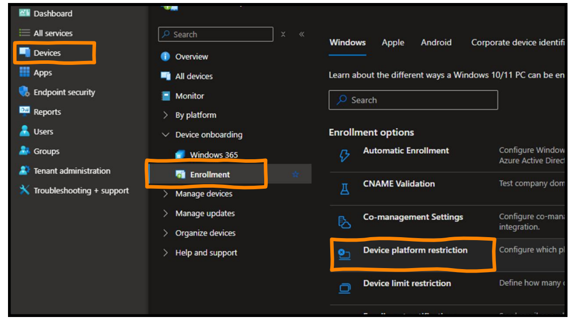

2
Why?
We must know, and trust our devices!
NIC

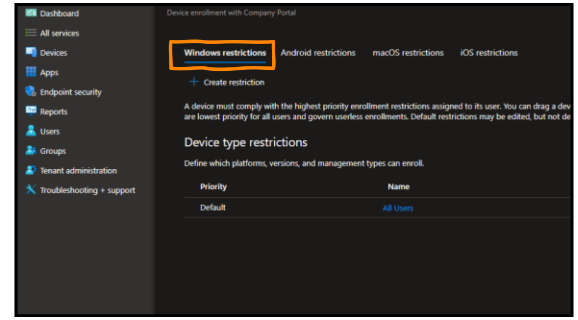

3
How?
Can we know, and trust our devices?
NIC

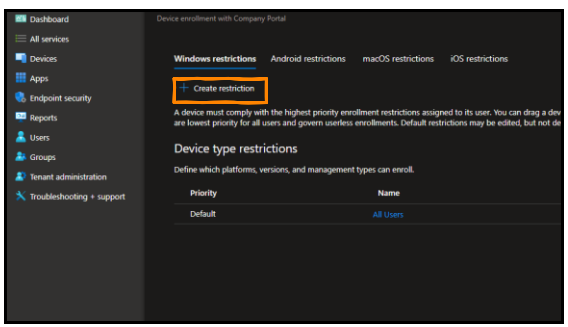

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Home > Devices
Devices | En
Search
Overview
All devices

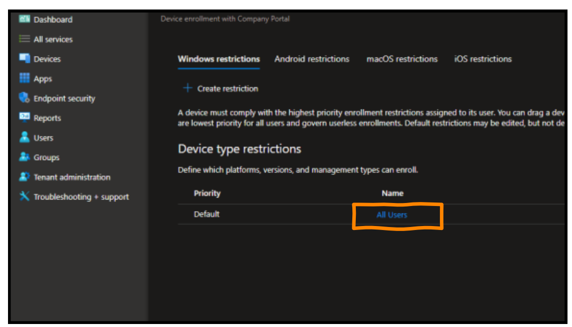

Home
Dashboard
All services
Devices
Apps
Endpoint security
Home > Devices
Devices | En
Search
Overview
All devices
Monitor

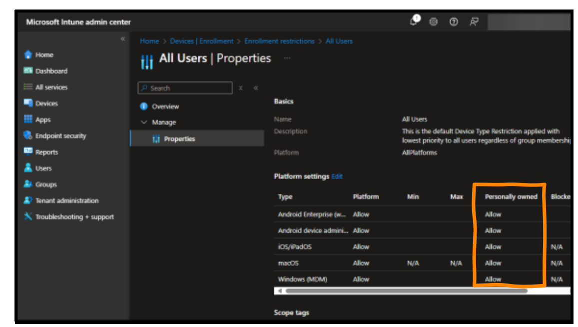

All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Search
Overview
All devices
Monitor
By platform
Device onboarding
Windows 365
Enrollment
Manage devices

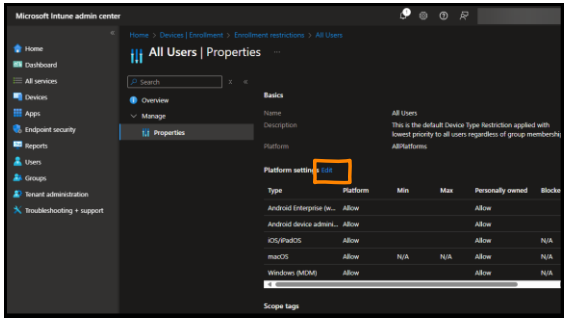

Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Overview
All devices
Monitor
By platform
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates
Organize devices
Help and support
Windows
Apple
Android
Enrollment options
Automatic Enrollment
CNAME Validation
Co-management Settings
Device platform restriction
Device limit restriction

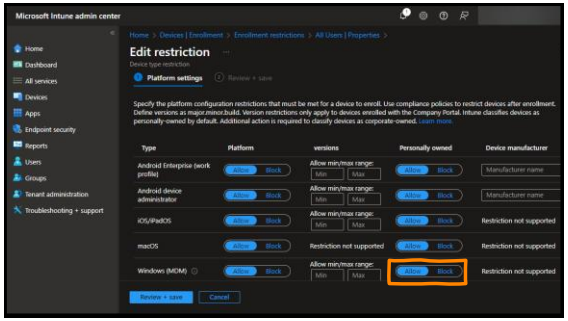

Windows restrictions
Android restrictions
macOS restrictions
iOS restrictions
Create restriction
Device type restrictions
Define which platforms, versions, and management types can enroll.
Priority
Name
Default
All Users

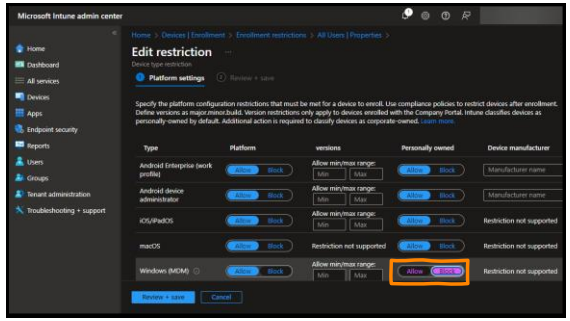

Windows restrictions
Android restrictions
macOS restrictions
iOS restrictions
Create restriction
Device type restrictions
Define which platforms, versions, and management types can enroll.
Priority
Name
Default
All Users

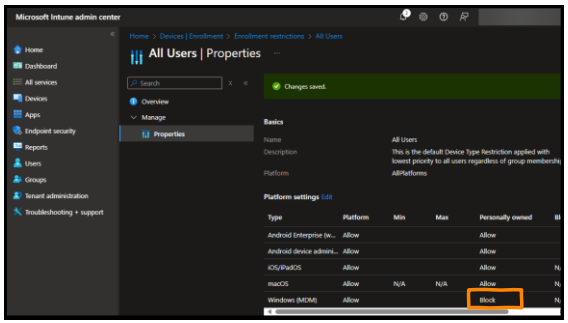

Windows restrictions
Android restrictions
macOS restrictions
iOS restrictions
Create restriction
Device type restrictions
Define which platforms, versions, and management types can enroll.
Priority
Name
Default
All Users


Microsoft Intune admin center
All Users | Properties
Basics
Platform settings
Personally owned
Scope tags


Microsoft Intune admin center
All Users | Properties
Platform settings Edit

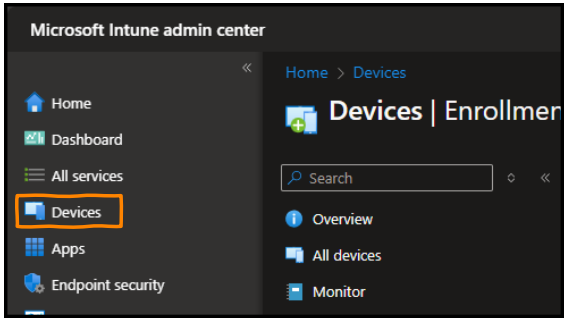

Microsoft Intune admin center
Edit restriction
Platform settings

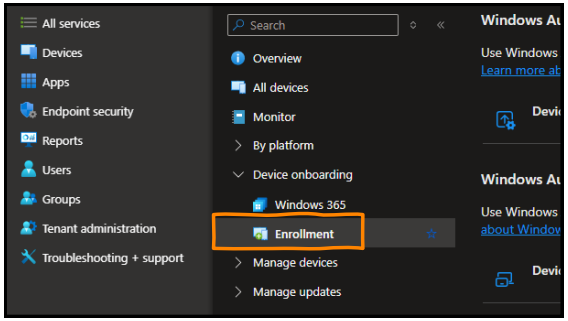

Microsoft Intune admin center
Edit restriction
Platform settings

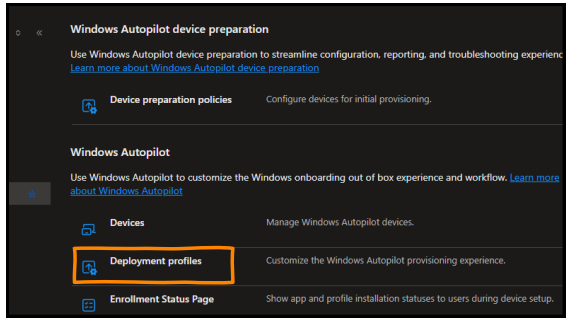

Microsoft Intune admin center
All Users | Properties
Changes saved
Platform settings Edit

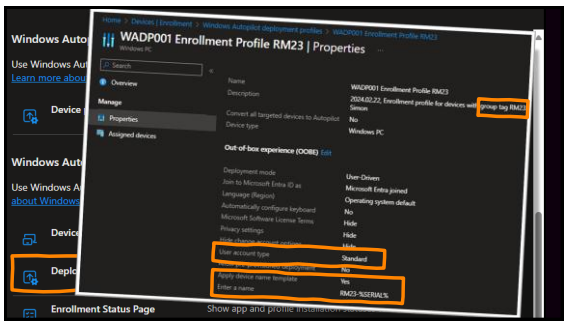

3
How?
Can we know,
and trust
our devices?
NIC

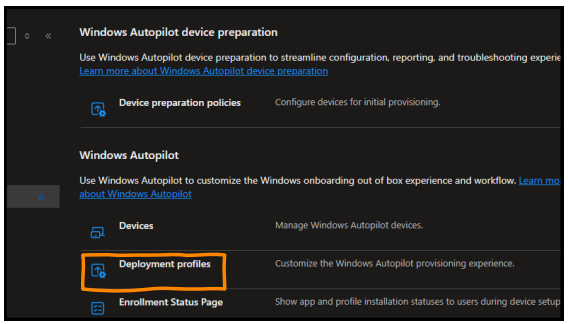

4
How?
Can we know,
and trust
our devices?
Windows Autopilot
NIC

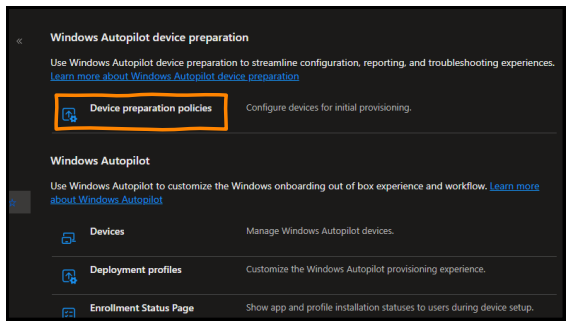

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Home > Devices
Devices | Enrollmer
Search
Overview
All devices
Monitor

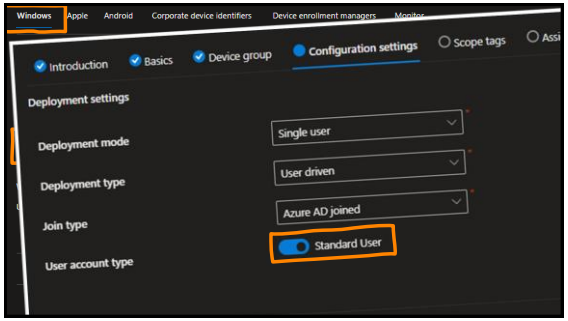

All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Search
Overview
All devices
Monitor
By platform
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates


Windows Autopilot device preparation
Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting
Learn more about Windows Autopilot device preparation
Device preparation policies
Configure devices for initial provisioning.
Windows Autopilot
Use Windows Autopilot to customize the Windows onboarding out of box experience and workflow.
Devices
Manage Windows Autopilot devices.
Deployment profiles
Customize the Windows Autopilot provisioning experience.
Enrollment Status Page
Show app and profile installation statuses to users during device setup.


WADP001 Enrollment Profile RM23 | Properties
Overview
Manage
Properties
Assigned devices
Out-of-box experience (OOBE)
Enrollment Status Page

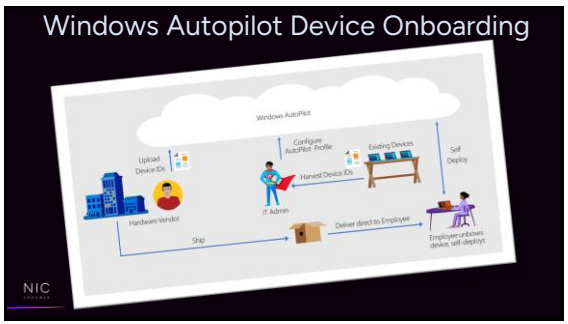

Windows Autopilot device preparation
Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting
Learn more about Windows Autopilot device preparation
Device preparation policies
Configure devices for initial provisioning.
Windows Autopilot
Use Windows Autopilot to customize the Windows onboarding out of box experience and workflow.
Devices
Manage Windows Autopilot devices.
Deployment profiles
Customize the Windows Autopilot provisioning experience.
Enrollment Status Page
Show app and profile installation statuses to users during device setup.

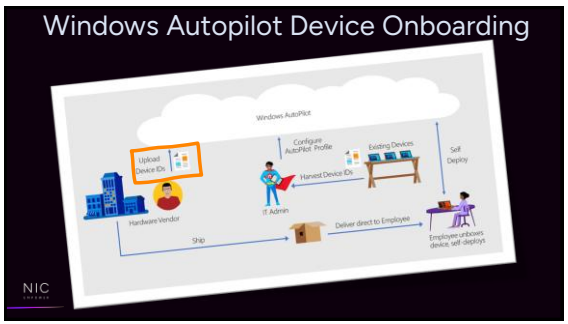

Windows Autopilot device preparation
Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting experiences.
Learn more about Windows Autopilot device preparation
Device preparation policies
Configure devices for initial provisioning.
Windows Autopilot
Use Windows Autopilot to customize the Windows onboarding out of box experience and workflow.
Devices
Manage Windows Autopilot devices.
Deployment profiles
Customize the Windows Autopilot provisioning experience.
Enrollment Status Page
Show app and profile installation statuses to users during device setup.

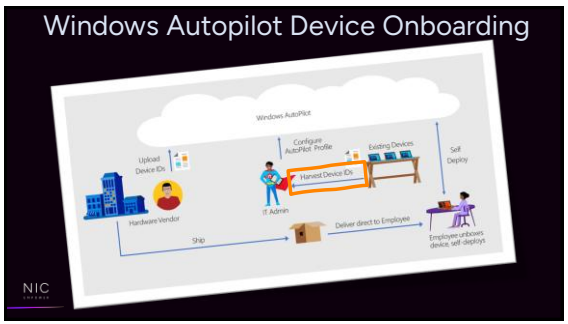

Windows
Apple
Android
Corporate device identifiers
Device enrollment managers
Introduction
Basics
Device group
Configuration settings
Scope tags
Deployment settings
Deployment mode
Single user
Deployment type
User driven
Join type
Azure AD joined
User account type
Standard User

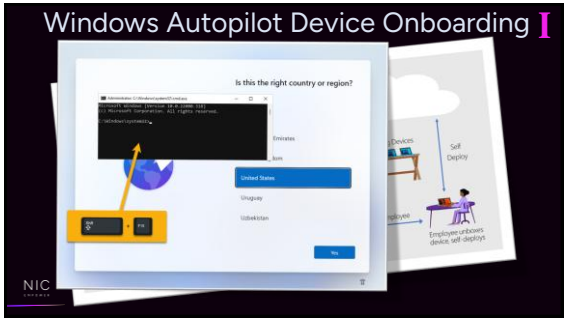

4
How?
Can we know,
and trust
our devices?
Windows Autopilot
NIC

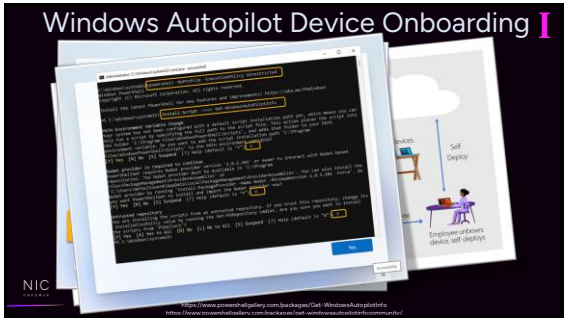

4
How?
Can we know,
and trust
our devices?
Windows Autopilot
Device Onboarding
NIC


Windows Autopilot Device Onboarding
NIC

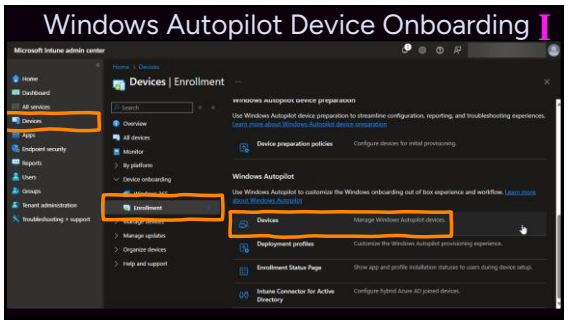

Windows Autopilot Device Onboarding
NIC

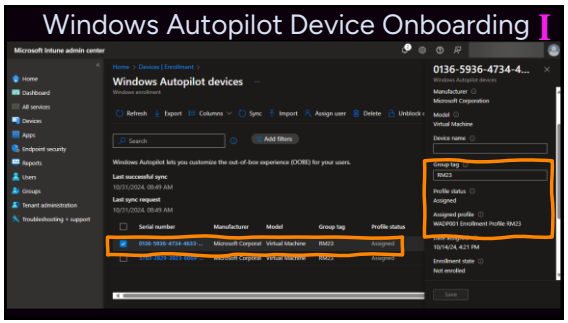

Windows Autopilot Device Onboarding
NIC


Windows Autopilot Device Onboarding
Is this the right country or region?
United States
Uruguay
Uzbekistan
Self Deploy
Employee unboxes device, self-deploys
NIC

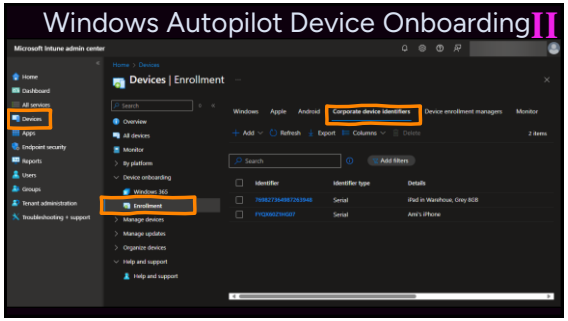

Windows Autopilot Device Onboarding
Self Deploy
Employee unboxes device, self-deploys
NIC

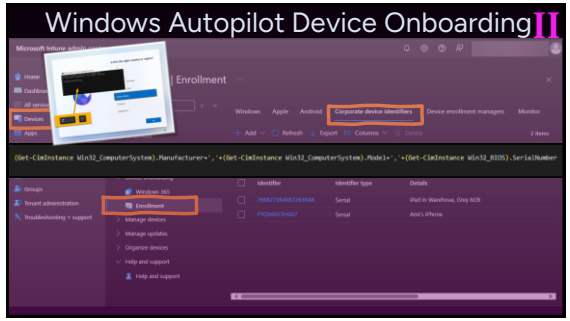

Windows Autopilot Device Onboarding
Is this the right country or region?
United States
Afghanistan
Self Deploy
Employee unboxes device, self-deploys
NIC

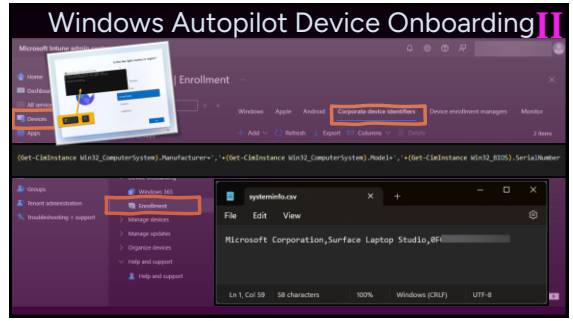

Windows Autopilot Device Onboarding
Microsoft Intune admin center
Devices | Enrollment
Windows Autopilot device preparation
Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting experiences.
Device preparation policies
Configure devices for initial provisioning.
Windows Autopilot
Use Windows Autopilot to customize the Windows onboarding out of box experience and workflow.
Devices
Manage Windows Autopilot devices
Deployment profiles
Customize the Windows Autopilot provisioning experience.
Enrollment Status Page
Show app and profile installation statuses to users during device setup.
Intune Connector for Active Directory
Configure hybrid Azure AD joined devices.

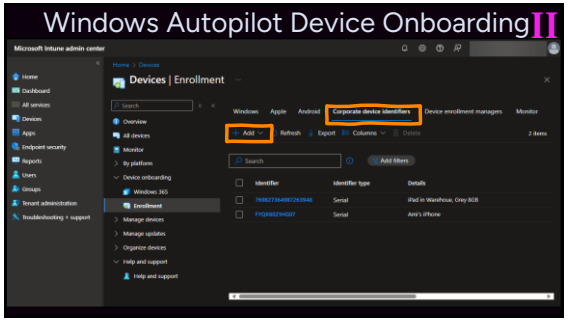

Windows Autopilot Device Onboarding
Microsoft Intune admin center
Windows Autopilot devices
0136-5936-4734-4...
Refresh
Export
Columns
Sync
Import
Assign user
Delete
Unblock
Add filters
Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.
Last successful sync
10/31/2024, 08:49 AM
Last sync request
10/31/2024, 08:49 AM
Serial number
Manufacturer
Model
Group tag
Profile status
Microsoft Corporation
Virtual Machine
RM23
Assigned
Manufacturer
Microsoft Corporation
Model
Virtual Machine
Device name
Group tag
RM23
Profile status
Assigned
Assigned profile
WAUTOP01 Enrollment Profile RM23
10/14/24, 4:21 PM
Enrollment state
Not enrolled

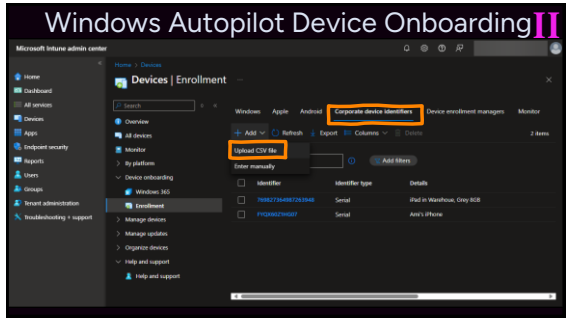

Windows Autopilot Device Onboarding
Microsoft Intune admin center
Autopilot Profile | Properties
Windows PC
Overview
Manage
Properties
Assigned devices
Out-of-box experience (OOBE)
Autopilot Profile
No Description
No
Windows PC
User-Driven
Microsoft Entra joined
Operating system default
No
Hide
Hide
Show
Standard
No
Yes
LETSDO-%SERIAL%

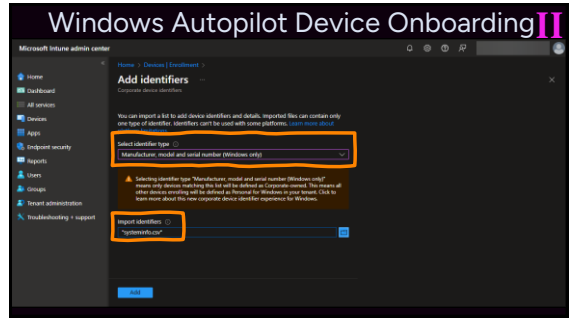

Windows Autopilot Device Onboarding II
Devices | Enrollment
Corporate device identifiers
Enrollment

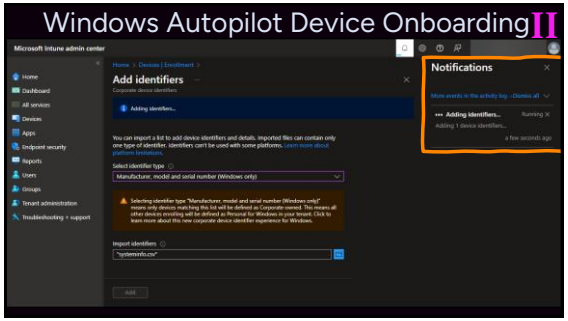

Windows Autopilot Device Onboarding II
Enrollment
Corporate device identifiers

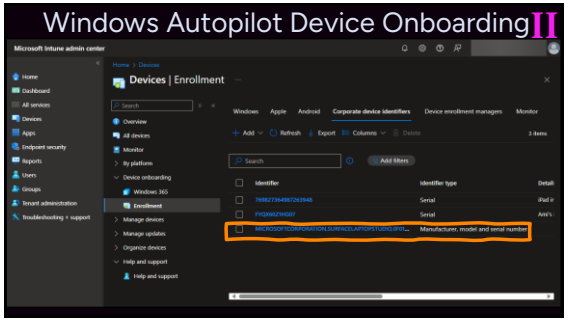

Windows Autopilot Device Onboarding II
Enrollment
Corporate device identifiers
systeminfo.csv
File Edit View
Microsoft Corporation,Surface Laptop Studio,BF

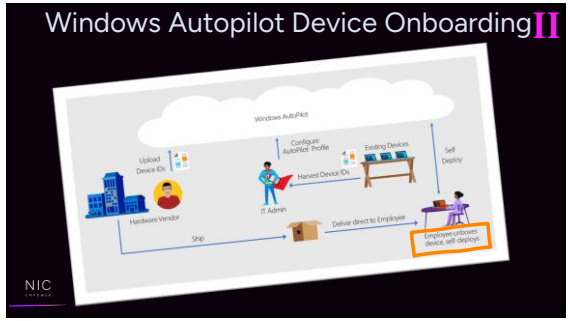

Windows Autopilot Device Onboarding II
Devices | Enrollment
Corporate device identifiers
Add

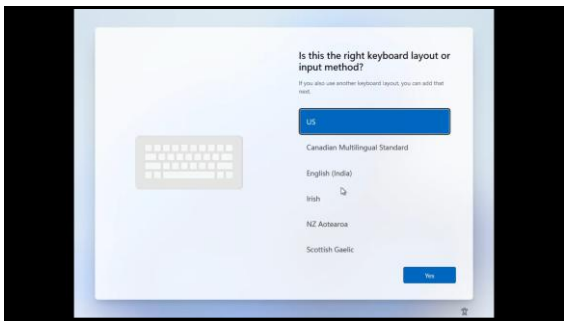

Windows Autopilot Device Onboarding II
Devices | Enrollment
Corporate device identifiers
Upload CSV file
Enter manually


Windows Autopilot Device Onboarding II
Add identifiers
Import identifiers
"systeminfo.csv"


Windows Autopilot Device Onboarding II
Notifications
Add identifiers

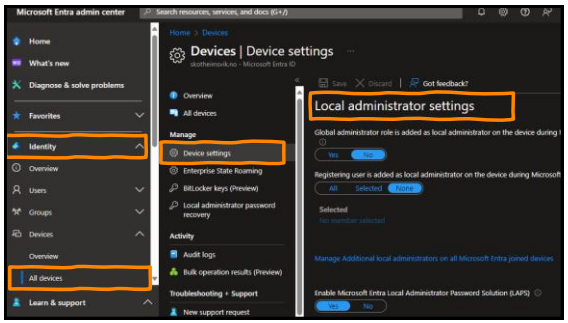

Windows Autopilot Device Onboarding II
Devices | Enrollment

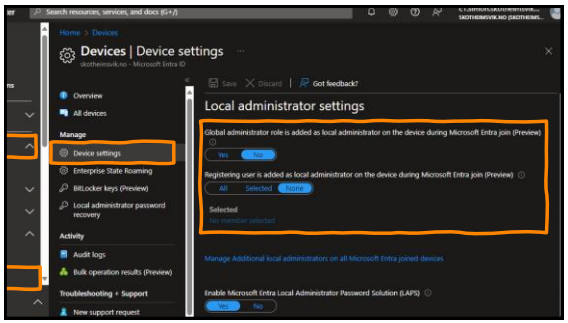

Windows Autopilot Device Onboarding II
NIC

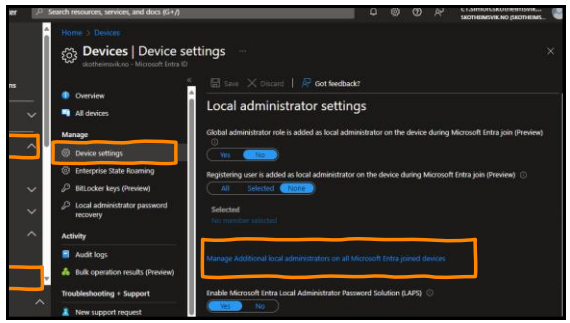

Is this the right keyboard layout or input method?
US
Canadian Multilingual Standard
English (India)
Irish
NZ Aotearoa
Scottish Gaelic

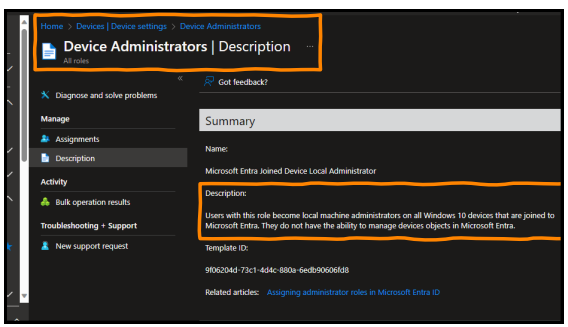

5
How?
Can we do stuff?
NIC

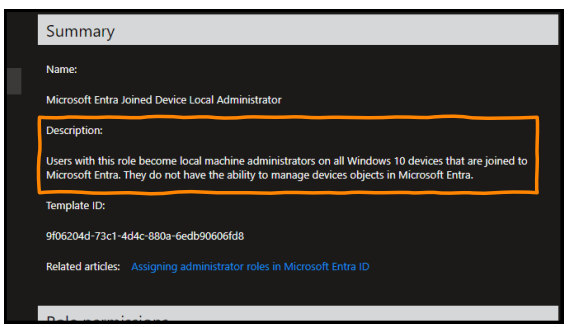

5
How?
Can we do stuff?
I NEED LOCAL ADMIN!
NIC


Microsoft Entra admin center
Devices | Device settings
Local administrator settings
Global administrator role is added as local administrator on the device during
Registering user is added as local administrator on the device during Microsoft
Selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)


Devices | Device settings
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
Selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)


Devices | Device settings
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
Selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)


Device Administrators | Description
Summary
Name:
Microsoft Entra Joined Device Local Administrator
Description:
Users with this role become local machine administrators on all Windows 10 devices that are joined to Microsoft Entra. They do not have the ability to manage devices objects in Microsoft Entra.
Template ID:
9f06204d-73c1-4d4c-880a-6edb90606fd8
Related articles:
Assigning administrator roles in Microsoft Entra ID


Summary
Name:
Microsoft Entra Joined Device Local Administrator
Description:
Users with this role become local machine administrators on all Windows 10 devices that are joined to Microsoft Entra. They do not have the ability to manage devices objects in Microsoft Entra.
Template ID:
9f06204d-73c1-4d4c-880a-6edb90606fd8
Related articles:
Assigning administrator roles in Microsoft Entra ID


NIC


NIC


NIC

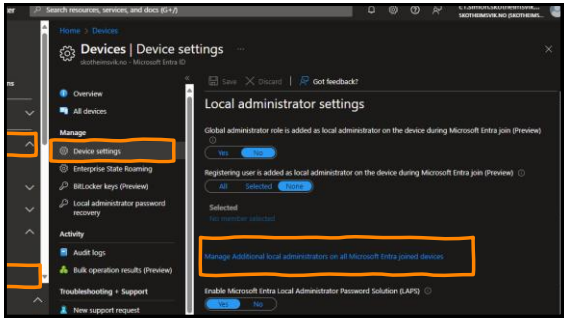

NIC

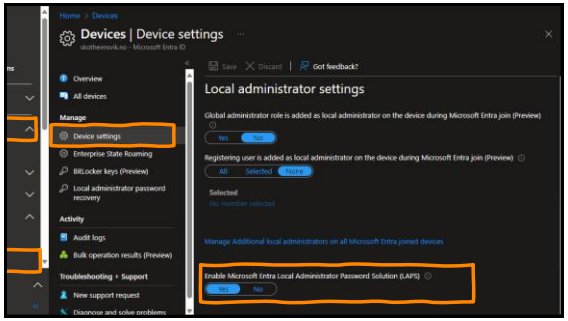

NIC


NIC


5
How?
Can we do stuff?
I NEED LOCAL ADMIN!
NIC

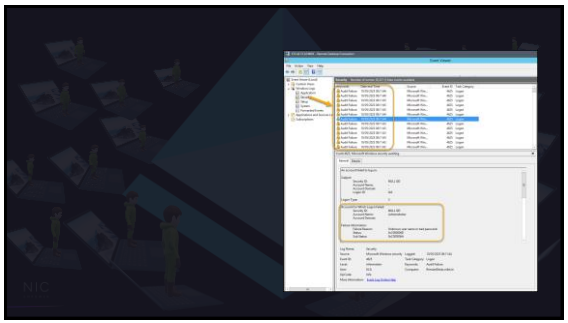

6
How?
Can we do stuff?
I NEED LAPS!
NIC


Devices | Device settings
Local administrator settings
Device settings
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)

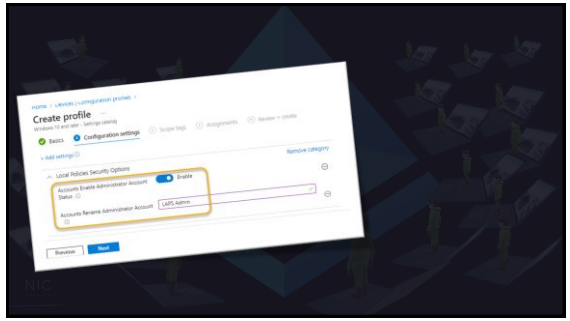

Devices | Device settings
Local administrator settings
Device settings
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)

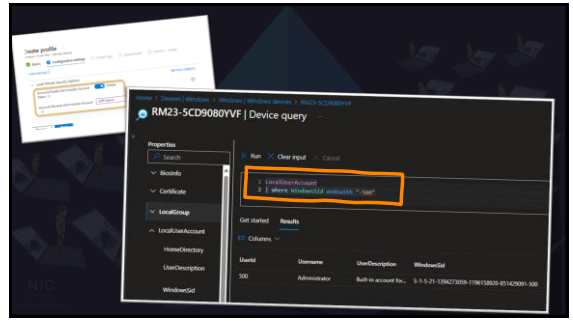

NIC

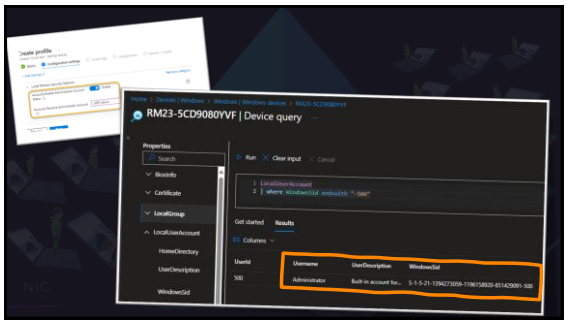

NIC

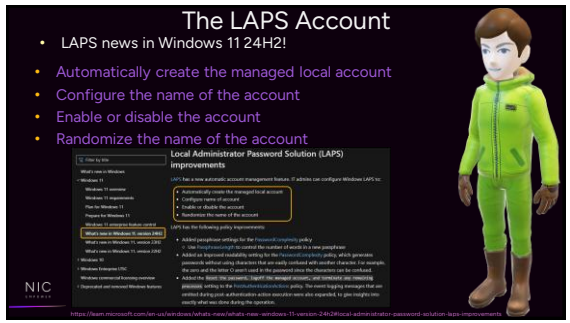


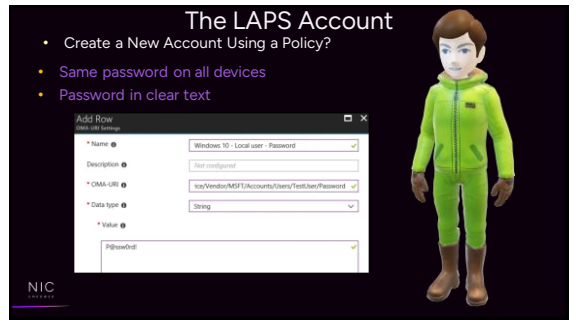

10 Immutable Laws of Security Administration
Law #6: There really is someone out there trying to guess your passwords

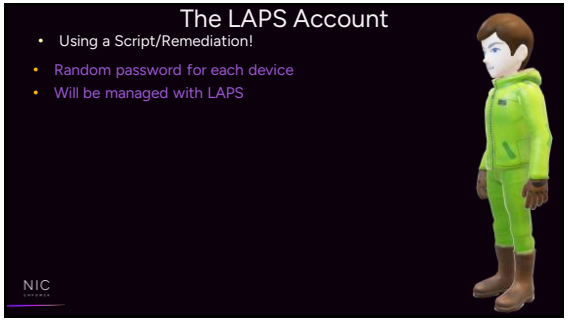

Create profile
Local Policies Security Options
Accounts Rename Administrator Account
LAPS Admin

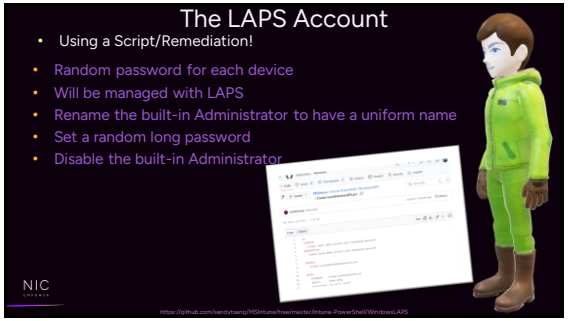

RM23-5CD9080YVF | Device query

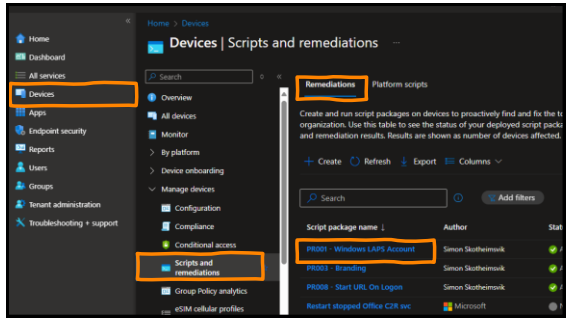

RM23-5CD9080YVF | Device query

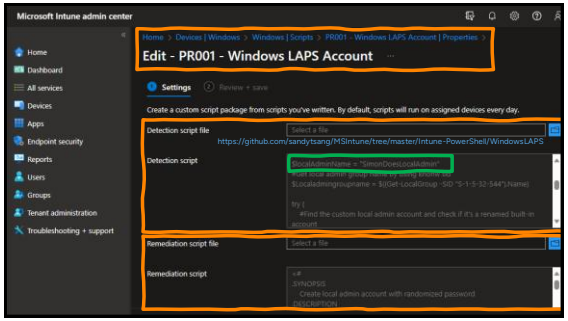

The LAPS Account
LAPS news in Windows 11 24H2!
Automatically create the managed local account
Configure the name of the account
Enable or disable the account
Randomize the name of the account
Local Administrator Password Solution (LAPS) improvements
NIC

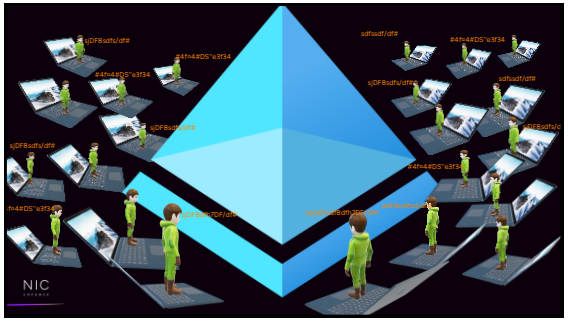

The LAPS Account
Create a New Account Using a Policy?
Same password on all devices
Password in clear text
Add Row
NIC

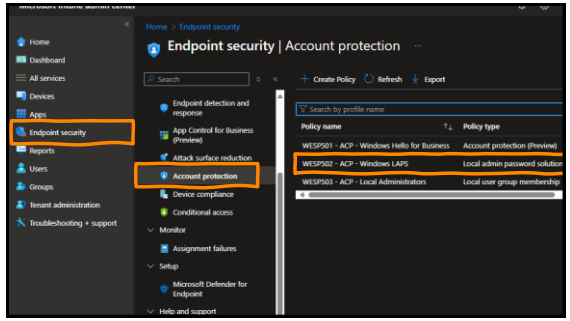

The LAPS Account
Using a Script/Remediation!
Random password for each device
Will be managed with LAPS
NIC

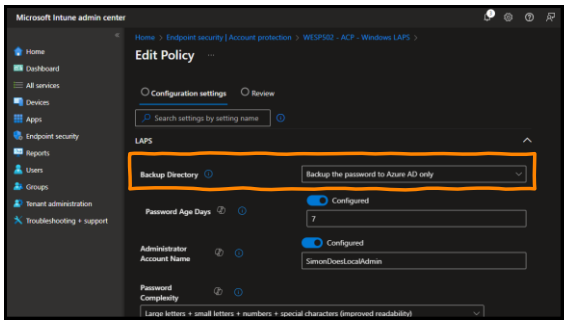

The LAPS Account
Using a Script/Remediation!
Random password for each device
Will be managed with LAPS
Rename the built-in Administrator to have a uniform name
Set a random long password
Disable the built-in Administrator
NIC

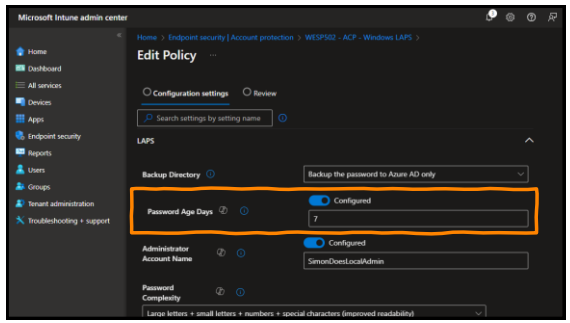

Devices | Scripts and remediations
Remediations
Platform scripts
Scripts and remediations
PR001 - Windows LAPS Account
PR003 - Branding
PR008 - Start URL On Logon

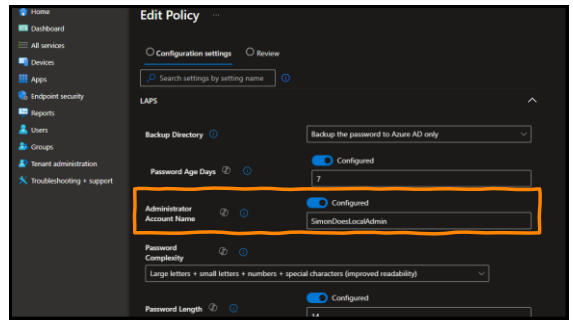

Microsoft Intune admin center
Edit - PR001 - Windows LAPS Account
Settings
Detection script file
Detection script
Remediation script file
Remediation script

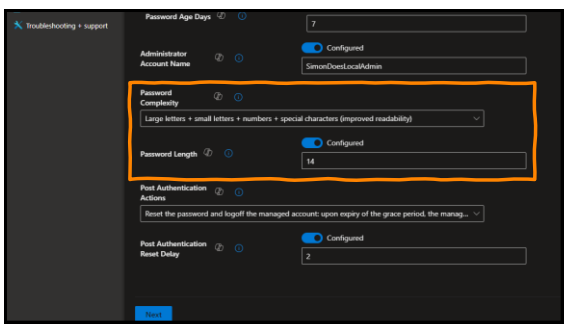

NIC

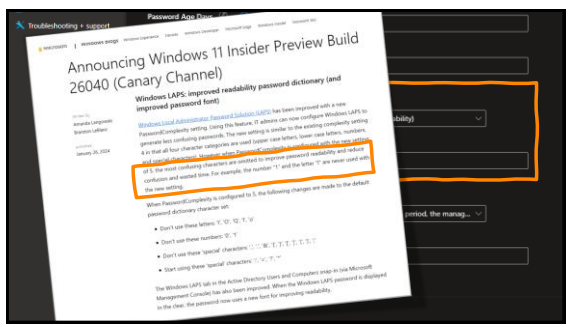

Endpoint security | Account protection
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Assignment failures
Microsoft Defender for Endpoint

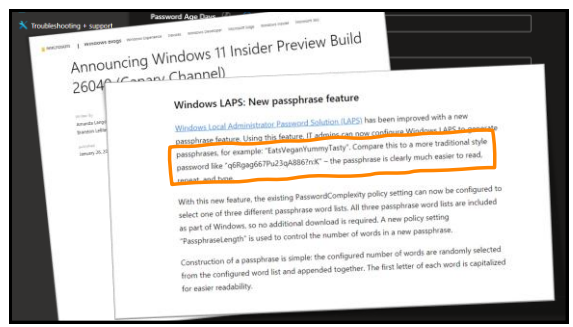

Microsoft Intune admin center
Edit Policy
Configuration settings
Review
LAPS
Backup Directory
Backup the password to Azure AD only
Password Age Days
Configured
7
Administrator Account Name
SimonDoesLocalAdmin
Password Complexity
Large letters + small letters + numbers + special characters (improved readability)

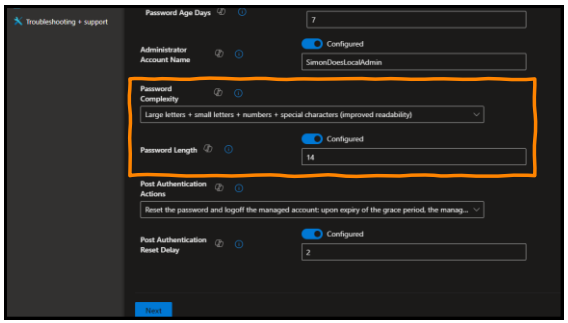

Microsoft Intune admin center
Edit Policy
Configuration settings
Review
LAPS
Backup Directory
Backup the password to Azure AD only
Password Age Days
Configured
7
Administrator Account Name
SimonDoesLocalAdmin
Password Complexity
Large letters + small letters + numbers + special characters (improved readability)

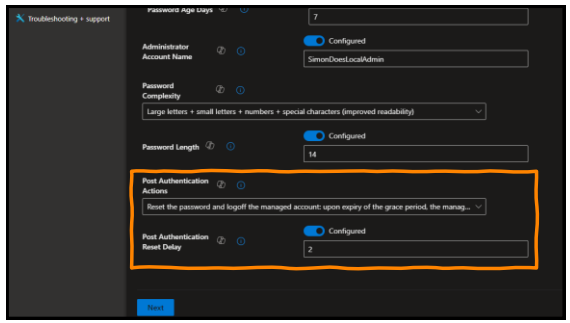

Edit Policy
Configuration settings
Review
LAPS
Backup Directory
Backup the password to Azure AD only
Password Age Days
Configured
7
Administrator Account Name
Configured
SimonDoesLocalAdmin
Password Complexity
Large letters + small letters + numbers + special characters (improved readability)
Password Length
Configured

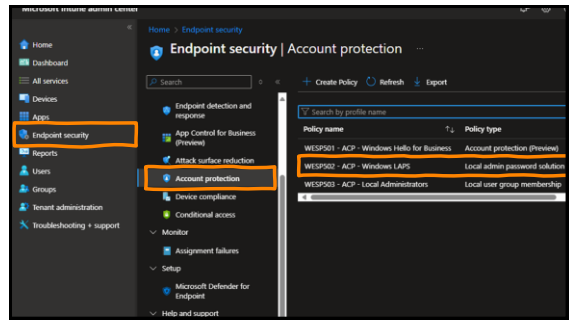

Troubleshooting + support
Password Age Days
7
Administrator Account Name
Configured
SimonDoesLocalAdmin
Password Complexity
Large letters + small letters + numbers + special characters (improved readability)
Password Length
Configured
14
Post Authentication Actions
Reset the password and logoff the managed account; upon expiry of the grace period, the manag...
Post Authentication Reset Delay
Configured
2

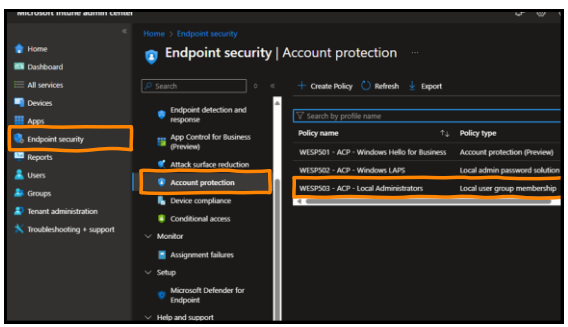

Troubleshooting + support
Announcing Windows 11 Insider Preview Build 26040 (Canary Channel)
Windows LAPS: improved readability password dictionary (and improved password font)

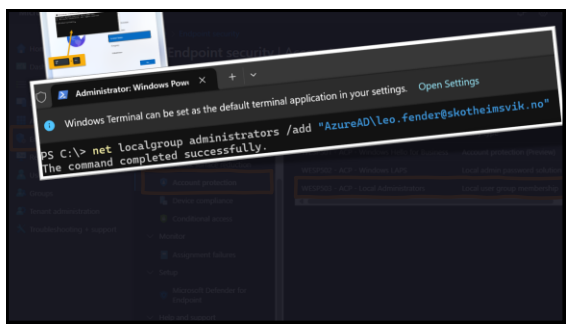

Troubleshooting + support
Announcing Windows 11 Insider Preview Build
Windows LAPS: New passphrase feature
Windows Local Administrator Password Solution (LAPS) has been improved with a new passphrase feature. Using this feature, IT admins can now configure Windows LAPS to generate passphrases, for example: "EatsVeganYummyTasty". Compare this to a more traditional style password like "q6Rgag667Pu23qA886?n3K" – the passphrase is clearly much easier to read, repeat, and type.
With this new feature, the existing PasswordComplexity policy setting can now be configured to select one of three different passphrase word lists. All three passphrase word lists are included as part of Windows, so no additional download is required. A new policy setting "PassphraseLength" is used to control the number of words in a new passphrase.
Construction of a passphrase is simple: the configured number of words are randomly selected from the configured word list and appended together. The first letter of each word is capitalized for easier readability.

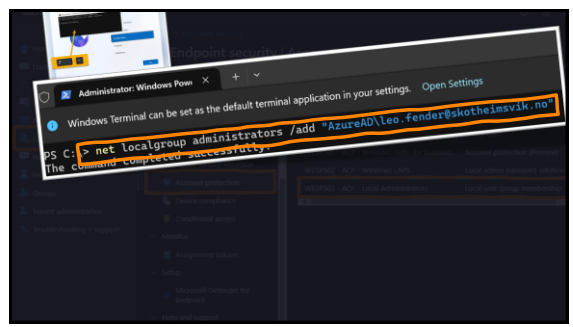

Troubleshooting + support
Password Age Days
7
Administrator Account Name
Configured
SimonDoesLocalAdmin
Password Complexity
Large letters + small letters + numbers + special characters (improved readability)
Password Length
Configured
14
Post Authentication Actions
Reset the password and logoff the managed account: upon expiry of the grace period, the manag...
Post Authentication Reset Delay
Configured
2
Next

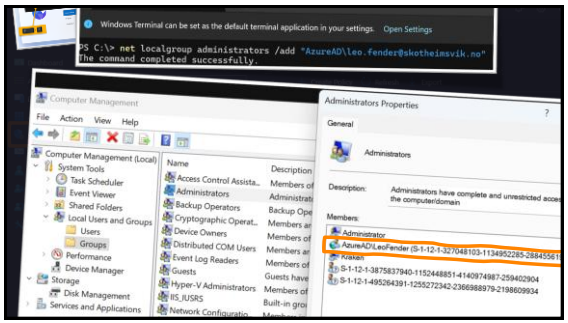

Troubleshooting + support
Password Age Days
7
Administrator Account Name
Configured
SimonDoesLocalAdmin
Password Complexity
Large letters + small letters + numbers + special characters (improved readability)
Password Length
Configured
14
Post Authentication Actions
Reset the password and logoff the managed account: upon expiry of the grace period, the manag...
Post Authentication Reset Delay
Configured
2
Next

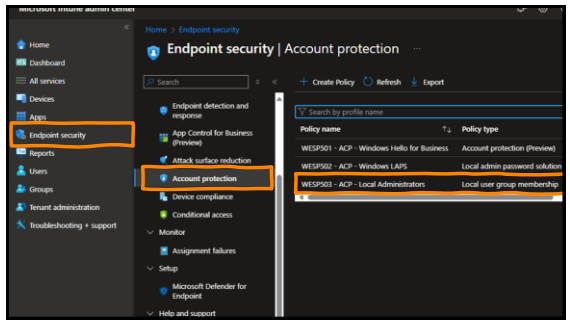

Home
Endpoint security
Endpoint security | Account protection
Create Policy
Refresh
Export
Search by profile name
Policy name
Policy type
WESP501 - ACP - Windows Hello for Business
Account protection (Preview)
WESP502 - ACP - Windows LAPS
Local admin password solution
WESP503 - ACP - Local Administrators
Local user group membership
Endpoint security
Account protection

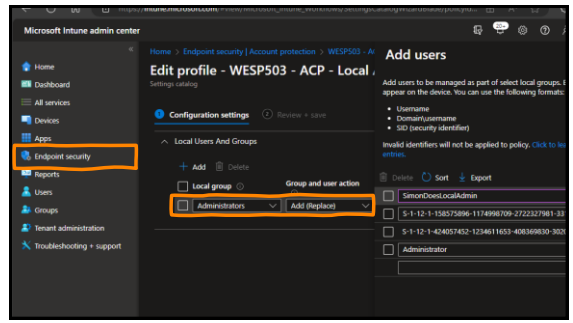

Home
Endpoint security
Endpoint security | Account protection
Create Policy
Refresh
Export
Search by profile name
Policy name
Policy type
WESP501 - ACP - Windows Hello for Business
Account protection (Preview)
WESP502 - ACP - Windows LAPS
Local admin password solution
WESP503 - ACP - Local Administrators
Local user group membership
Endpoint security
Account protection

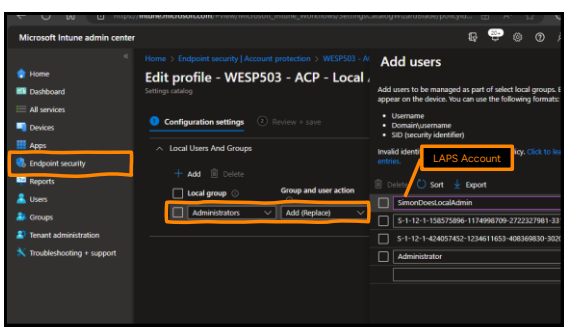

Administrator: Windows Powe
Windows Terminal can be set as the default terminal application in your settings.
Open Settings
PS C:\> net localgroup administrators /add "AzureAD\leo.fender@skotheimsvik.no"
The command completed successfully.

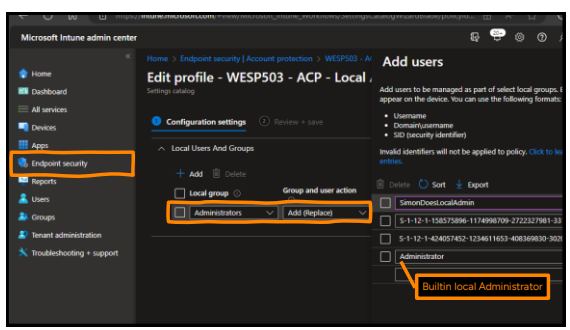

Administrator: Windows Powe
Windows Terminal can be set as the default terminal application in your settings.
Open Settings
PS C:\> net localgroup administrators /add "AzureAD\leo.fender@skotheimsvik.no"

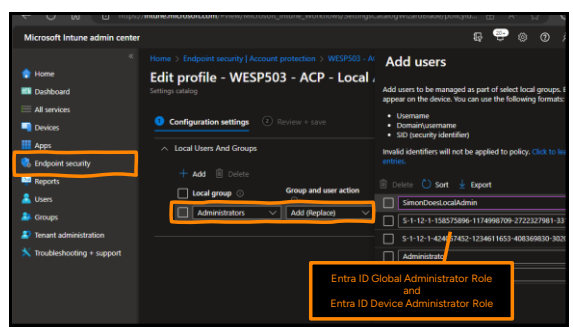

Windows Terminal can be set as the default terminal application in your settings. Open Settings
PS C:\> net localgroup administrators /add "AzureAD\leo.fender@skotheimsvik.no"
The command completed successfully.
Computer Management
Administrators Properties
Administrators
AzureAD\LeoFender (S-1-12-1-327048103-1134952285-2884556

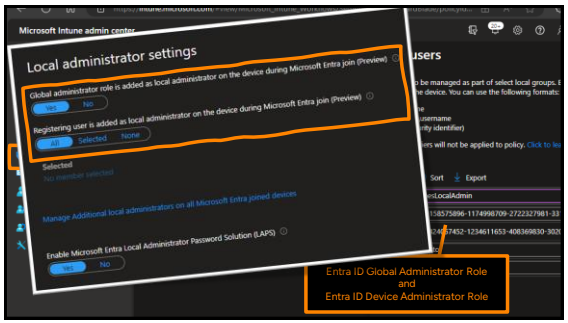

Endpoint security | Account protection
Endpoint security
Account protection
WESP501 - ACP - Windows Hello for Business
WESP502 - ACP - Windows LAPS
WESP503 - ACP - Local Administrators

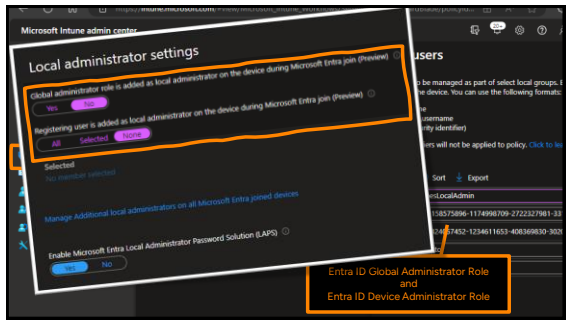

Microsoft Intune admin center
Edit profile - WESP503 - ACP - Local
Add users
Configuration settings
Local Users And Groups
Administrators
Add (Replace)
SimonDoesLocalAdmin
Administrator

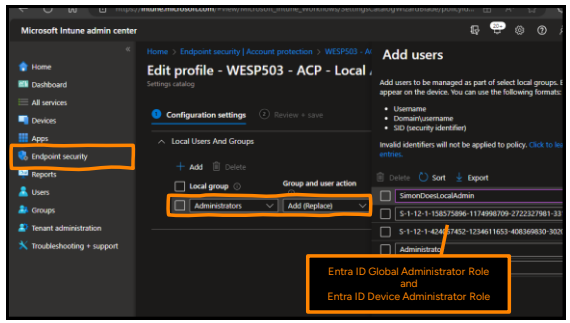

Microsoft Intune admin center
Edit profile - WESP503 - ACP - Local
Add users
LAPS Account
SimonDoesLocalAdmin

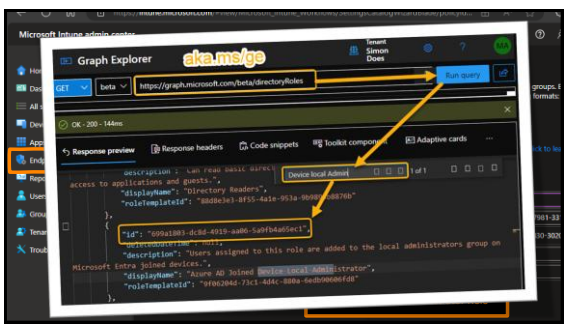

Microsoft Intune admin center
Edit profile - WESP503 - ACP - Local
Add users
Builtin local Administrator

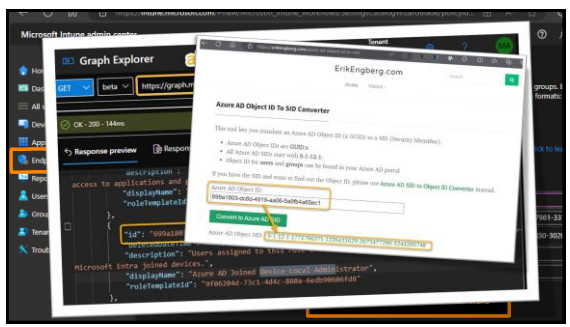

Microsoft Intune admin center
Edit profile - WESP503 - ACP - Local
Add users
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

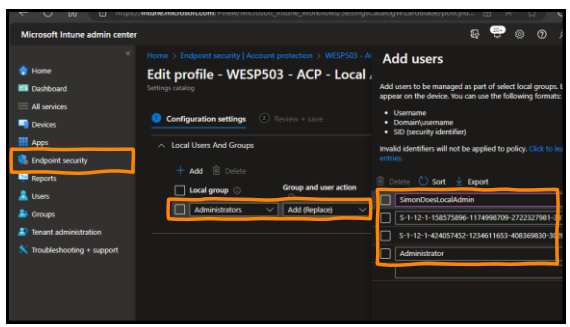

Microsoft Intune admin center
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

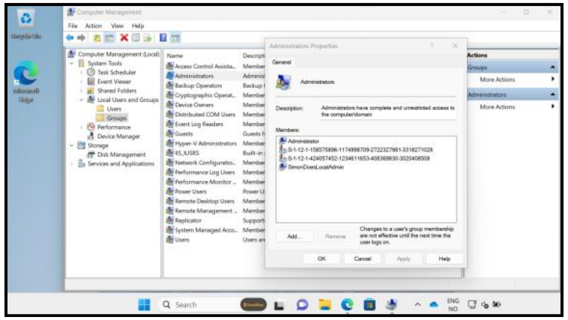

Microsoft Intune admin center
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

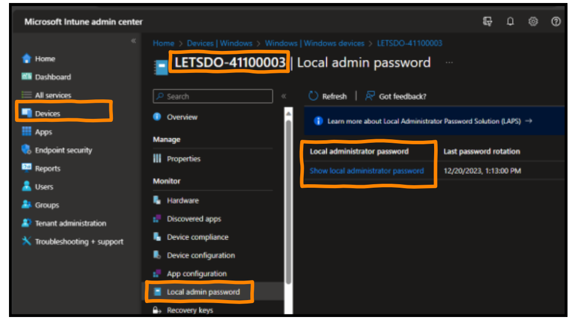

Microsoft Intune admin center
Edit profile - WESP503 - ACP - Local
Configuration settings
Local Users And Groups
Add users
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

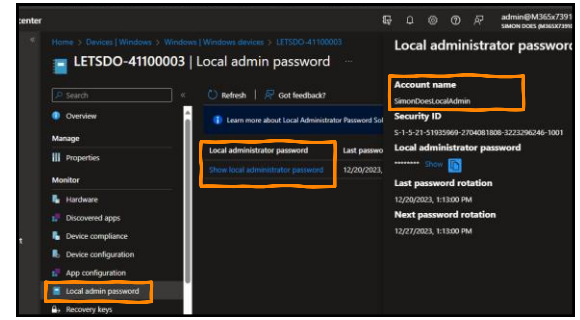

Graph Explorer
aka.ms/ge
https://graph.microsoft.com/beta/directoryRoles
Run query
Device local Admin

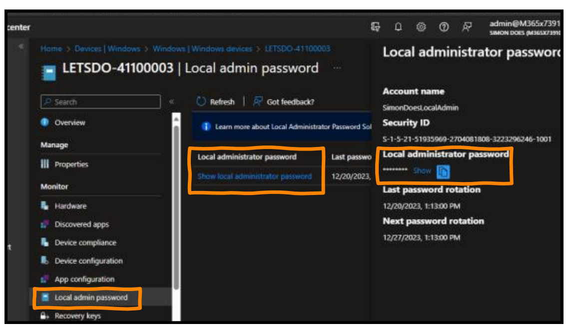

Graph Explorer
ErikEngberg.com
Azure AD Object ID To SID Converter

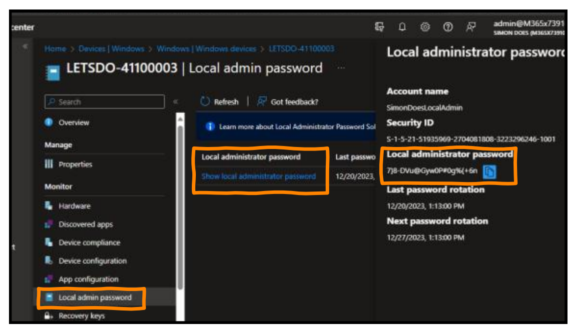

Microsoft Intune admin center
Edit profile - WESP503 - ACP - Local
Configuration settings
Local Users And Groups
Add users
Administrator

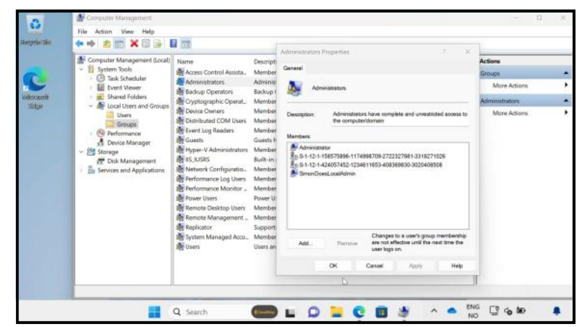



Microsoft Intune admin center
LETSDO-41100003 | Local admin password
Local administrator password
Show local administrator password
Last password rotation
12/20/2023, 1:13:00 PM


LETSDO-41100003 | Local admin password
Local administrator password
Account name
SimonDoesLocalAdmin
Security ID
Last password rotation
12/20/2023, 1:13:00 PM
Next password rotation
12/27/2023, 1:13:00 PM


LETSDO-41100003 | Local admin password
Local administrator password
Account name
SimonDoesLocalAdmin
Security ID
Last password rotation
12/20/2023, 1:13:00 PM
Next password rotation
12/27/2023, 1:13:00 PM


LETSDO-41100003 | Local admin password
Local administrator password
Account name
SimonDoesLocalAdmin
Security ID
Last password rotation
12/20/2023, 1:13:00 PM
Next password rotation
12/27/2023, 1:13:00 PM




6
How?
Can we do stuff?
I NEED LAPS!
NIC


6
How?
Can we do stuff?
I NEED LAPS!
Local Admin Access
NIC


6
How?
Can we do stuff?
I NEED LAPS!
Local Admin Access
NIC


Local Admin Access
NIC


Local Admin Access
Usermode Space
Admin Space
System Space
NIC


Local Admin Access
Usermode Space
Admin Space
System Space
NIC


Local Admin Access
Usermode Space
Admin Space
System Space
NIC


Local Admin Access
Usermode Space
Admin Space
System Space
NIC


6
How?
Can we do stuff?
I NEED LAPS!
Local Admin Access
NIC

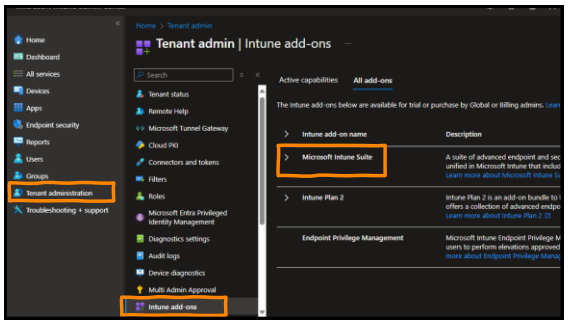

7
How?
Can we do stuff?
I NEED EPM!
NIC

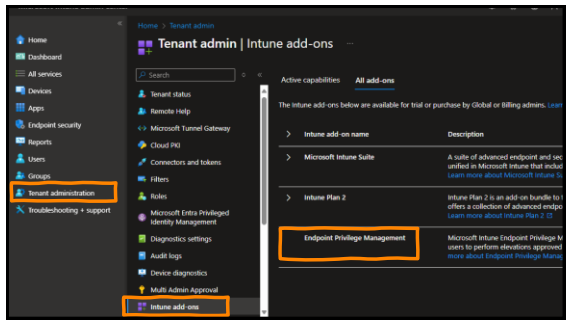

Endpoint Privilege Management
1010
1010
Usermode Space
Admin Space
System Space
NIC


Endpoint Privilege Management
Usermode Space
1010
1010
Admin Space
System Space
NIC

Endpoint Privilege Management

Capability	Standalone add-on	Intune Plan 2	Intune Suite
Advanced endpoint analytics			✓
Endpoint Privilege Management	✓		✓
Firmware-over-the-air update		✓	✓
Microsoft Tunnel for Mobile Application Management		✓	✓
Remote help	✓		✓
Specialized devices management		✓	✓





Endpoint Privilege Management (EPM)

- Overview

Built-in to Microsoft Intune

Allow Standard users to approve processes to Admin

Three main pieces

- Client side config
- Policy
- Rules

NIC

Endpoint Privilege Management (EPM)

- Trigger detection

EPM identifies a process

- Based on rules

User selects 'Run Elevated'

- Right click menu

NIC

Endpoint Privilege Management (EPM)

- Elevation Actions

Automatic

- Every time a binary launches, it is elevated

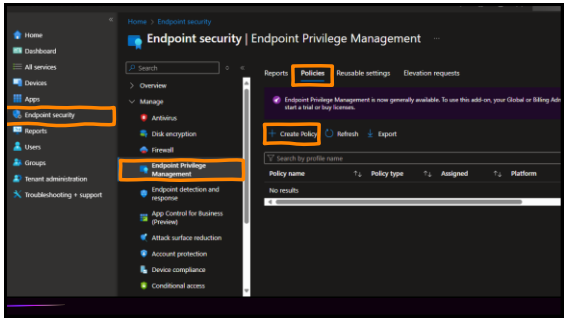
User confirmed

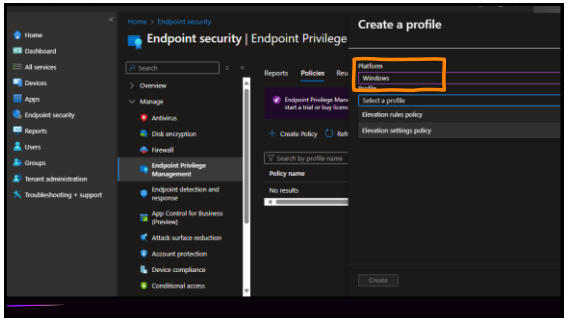
- On request from user

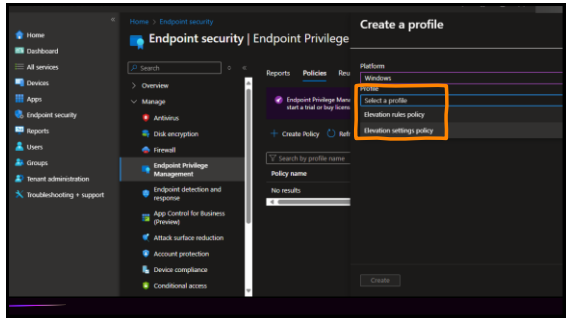
Support approved

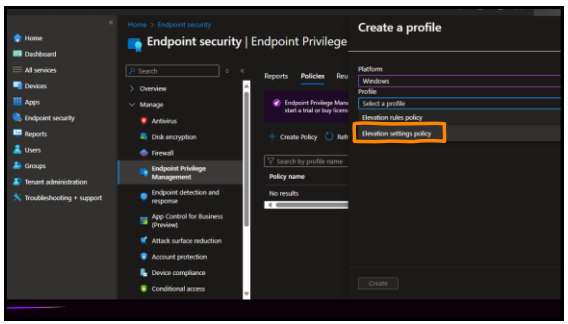
- IT must approve the request

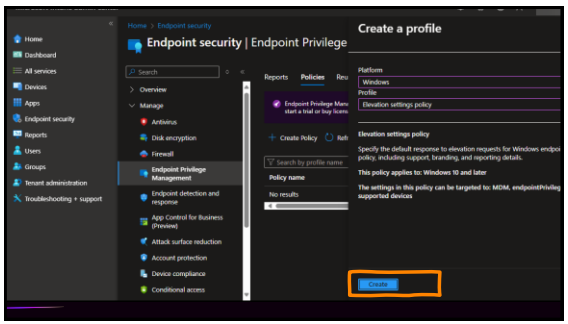
NIC

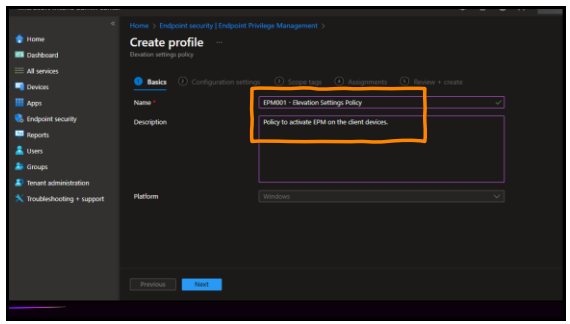

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation requests
Create Policy
Refresh
Export
Policy name
Policy type
Assigned
Platform
No results

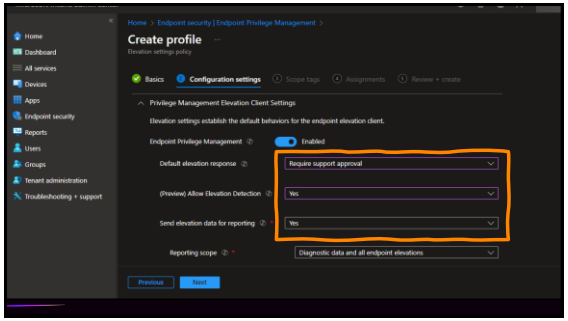

Endpoint security | Endpoint Privilege
Create a profile
Platform
Windows
Profile
Select a profile
Elevation rules policy
Elevation settings policy
Create

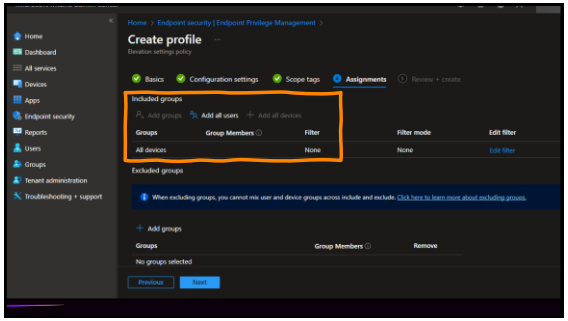

Endpoint security | Endpoint Privilege
Create a profile
Platform
Windows
Profile
Select a profile
Elevation rules policy
Elevation settings policy
Create

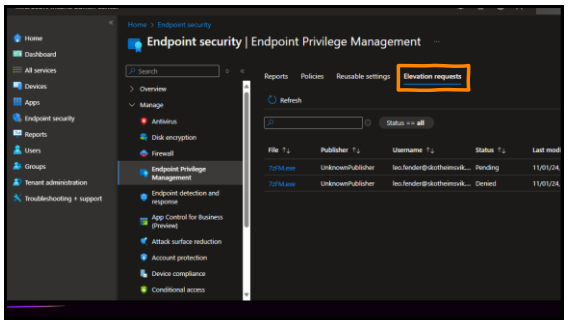

Endpoint security | Endpoint Privilege
Create a profile
Platform
Windows
Profile
Select a profile
Elevation rules policy
Elevation settings policy
Create

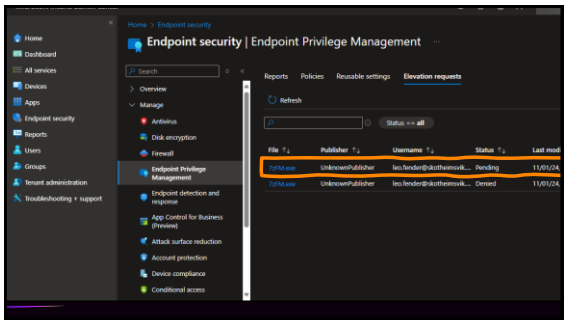

Endpoint security | Endpoint Privilege
Create a profile
Platform
Windows
Profile
Elevation settings policy
Elevation settings policy
This policy applies to: Windows 10 and later
Create

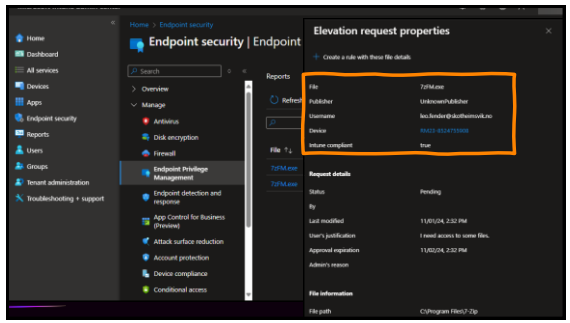

Create profile
Elevation settings policy
Basics
Name
EPM001 - Elevation Settings Policy
Description
Policy to activate EPM on the client devices.
Platform
Windows
Previous
Next

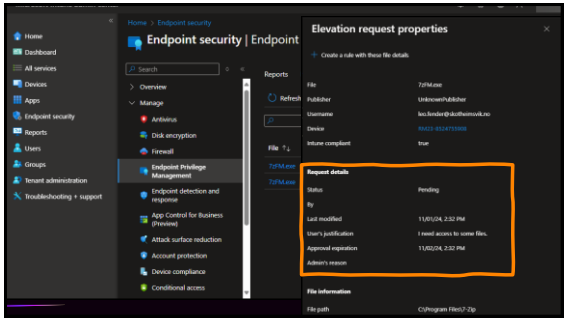

Create profile
Basics
Configuration settings
Scope tags
Assignments
Review + create
Privilege Management Elevation Client Settings
Endpoint Privilege Management
Enabled
Default elevation response
Require support approval
(Preview) Allow Elevation Detection
Yes
Send elevation data for reporting
Yes
Reporting scope
Diagnostic data and all endpoint elevations
Previous
Next

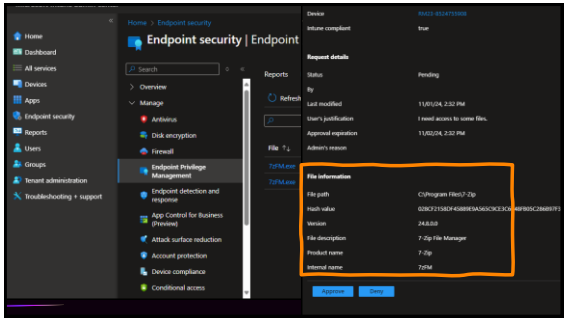

Create profile
Basics
Configuration settings
Scope tags
Assignments
Included groups
Add all users
Groups
Group Members
Filter
Filter mode
Edit filter
All devices
None
Excluded groups
Add groups
No groups selected
Previous
Next

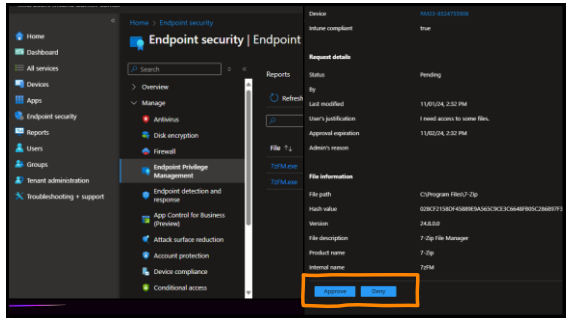

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation requests
Refresh
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access

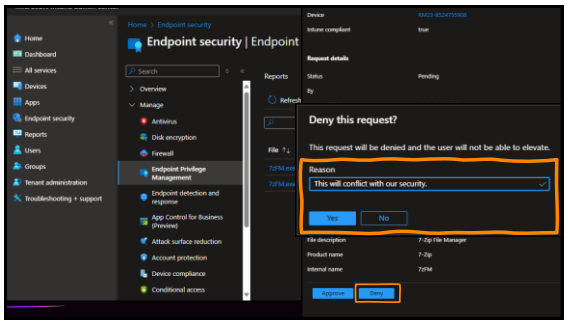

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation requests
Refresh
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access

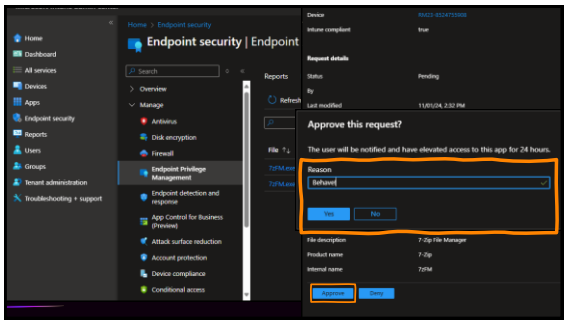

Endpoint security | Endpoint
Elevation request properties
Reports
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access

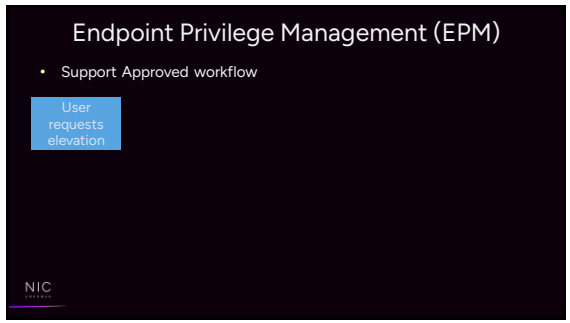

Endpoint security | Endpoint
Elevation request properties


Endpoint security | Endpoint


Endpoint security | Endpoint


Endpoint security | Endpoint
Deny this request?
This request will be denied and the user will not be able to elevate.
Reason
This will conflict with our security.
Yes
No

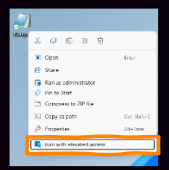

Endpoint security | Endpoint
Approve this request?
The user will be notified and have elevated access to this app for 24 hours.
Reason
Behave
Yes
No


Endpoint Privilege Management (EPM)
Support Approved workflow
User requests elevation
NIC

Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation

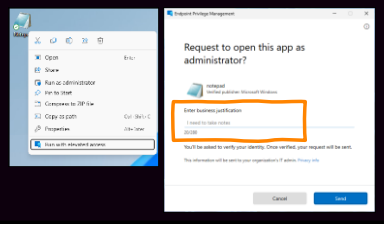


NIC

Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation



NIC

Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation → Request submitted

NIC

Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation → Request submitted → Request approved

NIC

Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation → Request submitted → Request approved → Short lived rule created

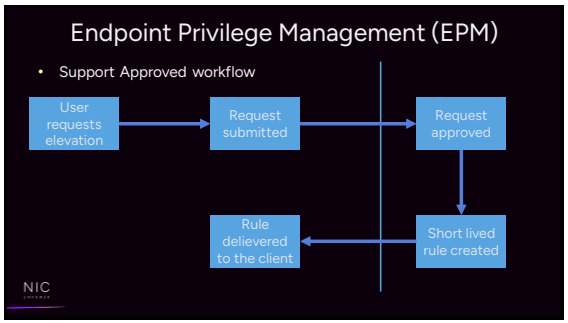
NIC

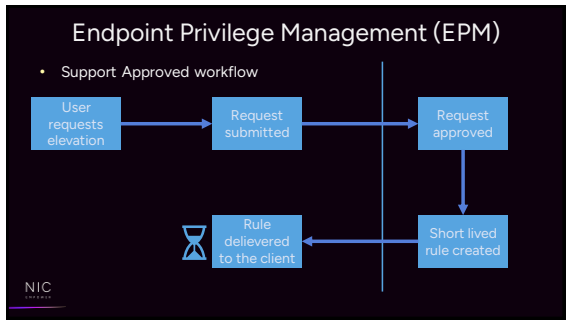
Endpoint Privilege Management (EPM)

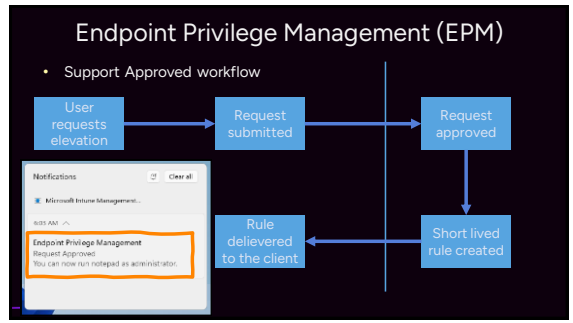
- Support Approved workflow

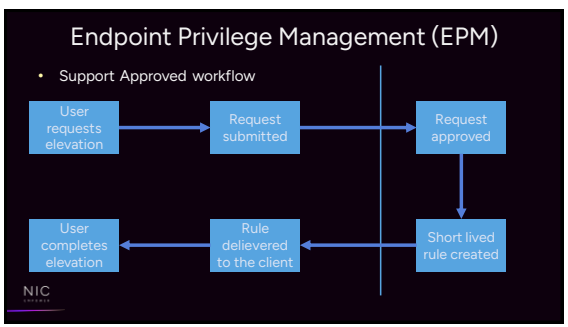
User requests elevation → Request submitted → Request approved → Short lived rule created

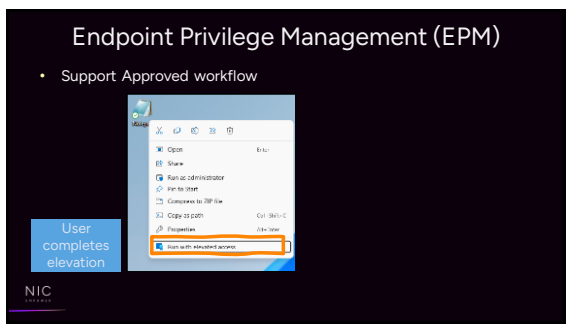
NIC

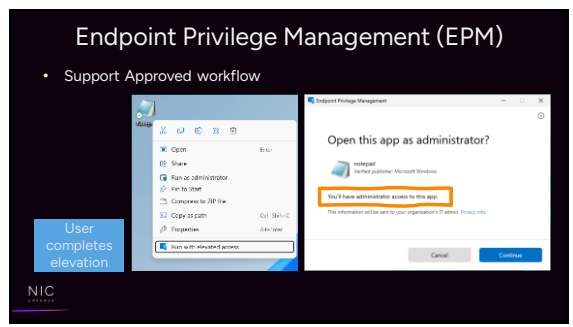

Endpoint Privilege Management (EPM)
Support Approved workflow
User requests elevation
Request submitted
Request approved
Rule delievered to the client
Short lived rule created
NIC

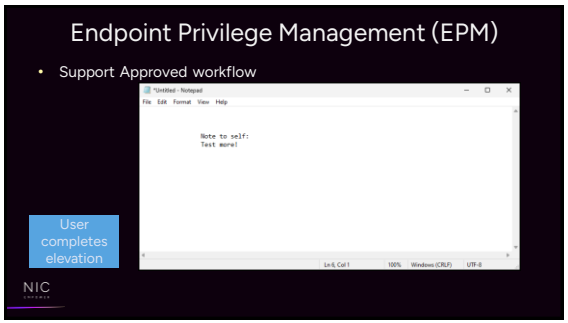

Endpoint Privilege Management (EPM)
Support Approved workflow
User requests elevation
Request submitted
Request approved
Rule delievered to the client
Short lived rule created
NIC

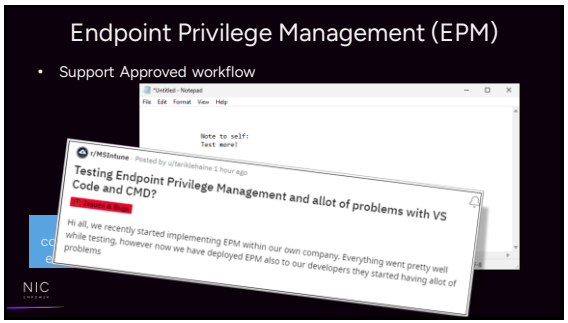

Endpoint Privilege Management (EPM)
Support Approved workflow
User requests elevation
Request submitted
Request approved
Notifications
Clear all
Endpoint Privilege Management
Request Approved
You can now run notepad as administrator.
Rule delievered to the client
Short lived rule created

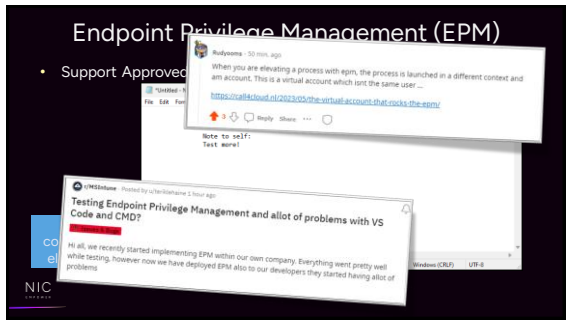

Endpoint Privilege Management (EPM)
Support Approved workflow
User requests elevation
Request submitted
Request approved
User completes elevation
Rule delievered to the client
Short lived rule created
NIC

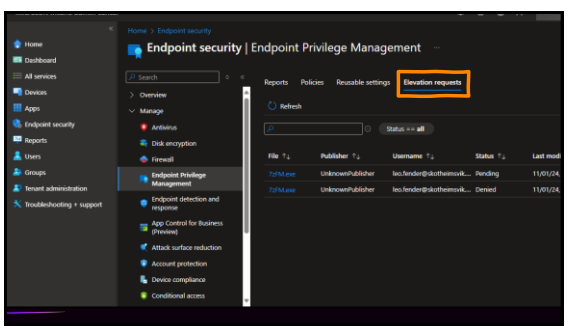

Endpoint Privilege Management (EPM)
Support Approved workflow
User completes elevation
NIC

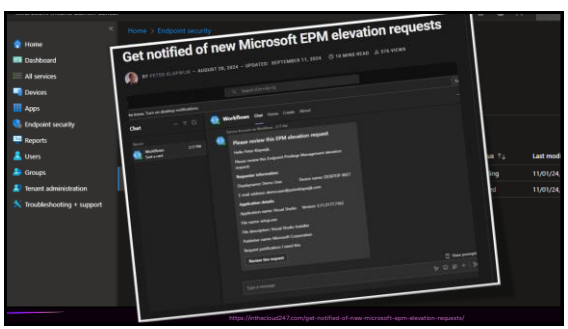

Endpoint Privilege Management (EPM)
Support Approved workflow
Open this app as administrator?
User completes elevation
NIC

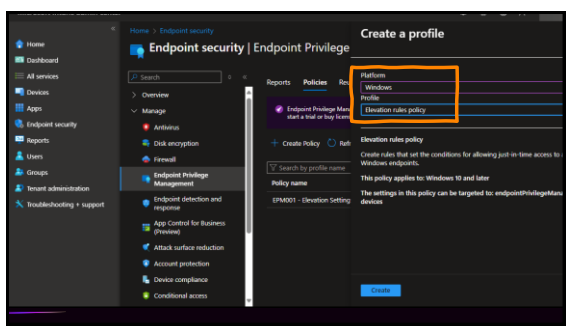

Endpoint Privilege Management (EPM)
Support Approved workflow
User completes elevation
NIC

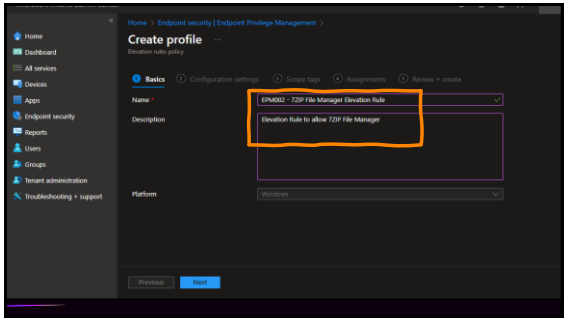

Endpoint Privilege Management (EPM)
Support Approved workflow
Testing Endpoint Privilege Management and allot of problems with VS Code and CMD?
NIC

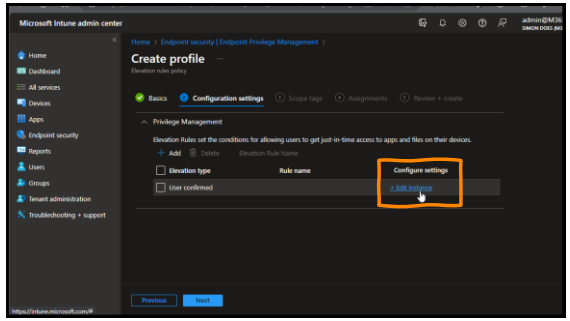

Endpoint Privilege Management (EPM)
Support Approved
Testing Endpoint Privilege Management and allot of problems with VS Code and CMD?
NIC

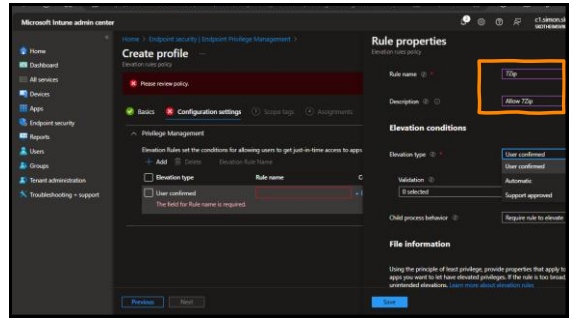

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation requests

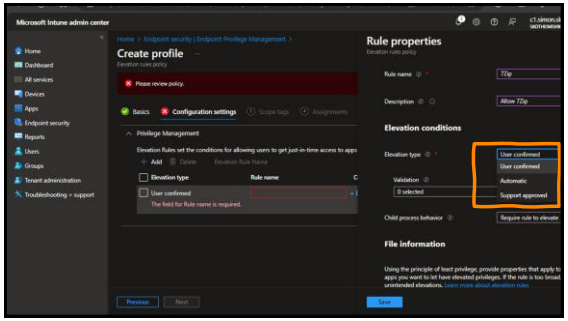

Get notified of new Microsoft EPM elevation requests

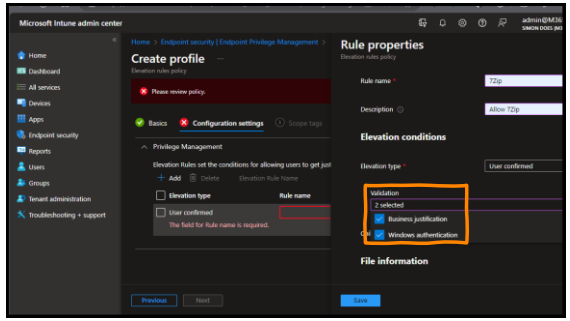

Endpoint security | Endpoint Privilege
Create a profile
Platform
Windows
Profile
Elevation rules policy

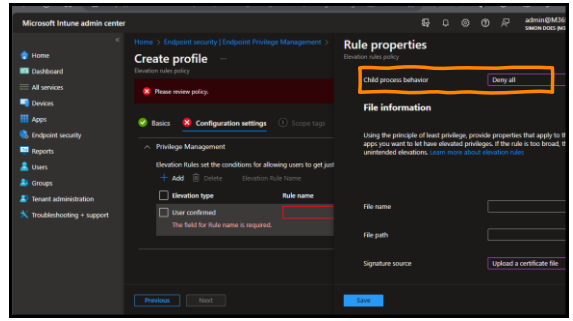

Create profile
Basics
Configuration settings
Scope tags
Assignments
Review + create
Name
EPM002 - 7ZIP File Manager Elevation Rule
Description
Elevation Rule to allow 7ZIP File Manager
Platform
Windows
Previous
Next

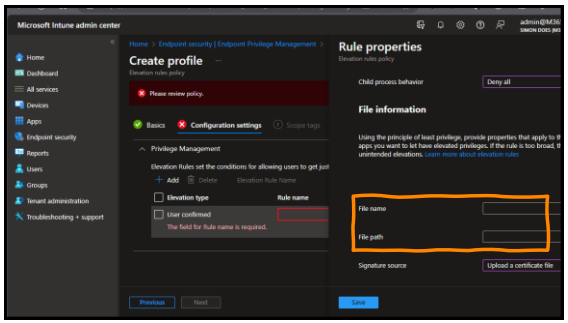

Microsoft Intune admin center
Create profile
Basics
Configuration settings
Scope tags
Assignments
Review + create
Privilege Management
Elevation type
Rule name
User confirmed
Configure settings
Edit instance
Previous
Next

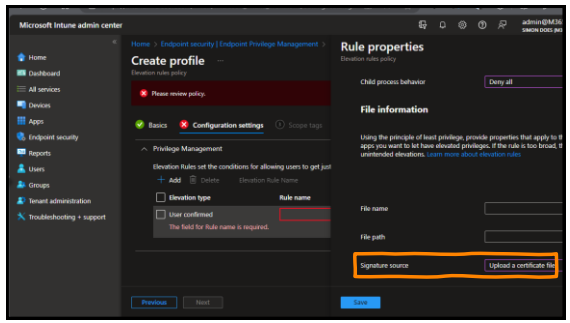

Microsoft Intune admin center
Create profile
Rule properties
Rule name
7Zip
Description
Allow 7Zip
Elevation conditions
Elevation type
User confirmed
Validation
Automatic
Support approved
Child process behavior
Require rule to elevate
File information
Previous
Next
Save

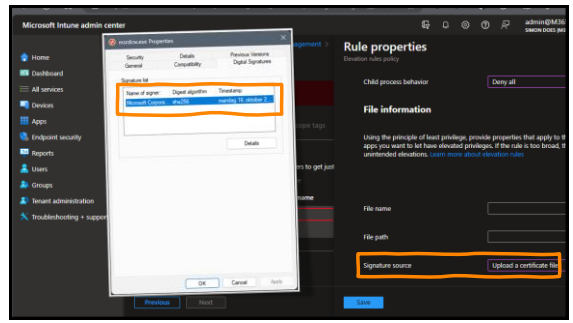

Microsoft Intune admin center
Create profile
Rule properties
Rule name
7Zip
Description
Allow 7Zip
Elevation conditions
Elevation type
User confirmed
Automatic
Support approved
Require rule to elevate
File information
Previous
Next
Save

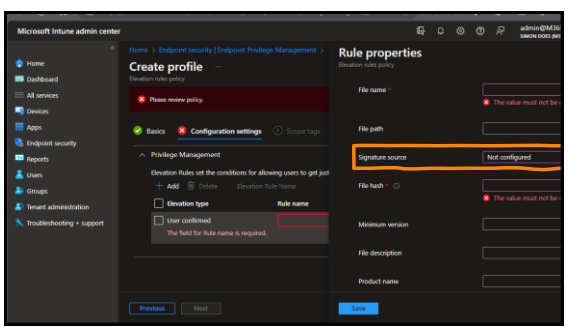

Microsoft Intune admin center
Create profile
Rule properties
Rule name
7Zip
Description
Allow 7Zip
Elevation conditions
Elevation type
User confirmed
Validation
2 selected
Business justification
Windows authentication
File information
Previous
Next
Save

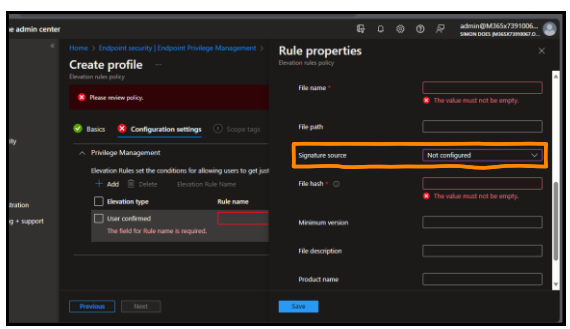

Microsoft Intune admin center
Create profile
Rule properties
Child process behavior
Deny all
File information
File name
File path
Signature source
Upload a certificate file
Previous
Next
Save

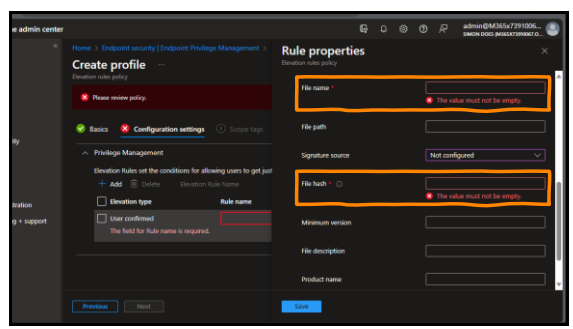

Microsoft Intune admin center
Create profile
Rule properties
File information
File name
File path
Signature source
Upload a certificate file

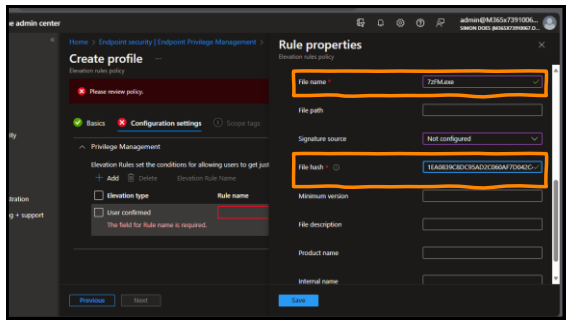

Microsoft Intune admin center
Create profile
Rule properties
File information
File name
File path
Signature source
Upload a certificate file

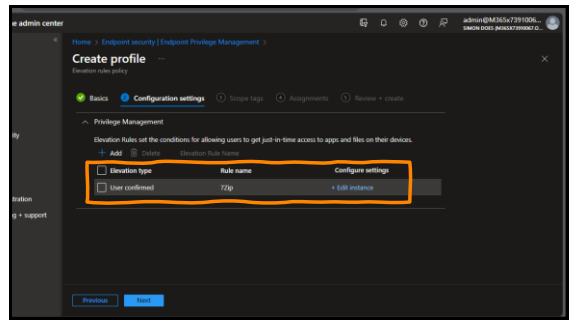

Microsoft Intune admin center
Create profile
Rule properties
File information
File name
File path
Signature source
Upload a certificate file

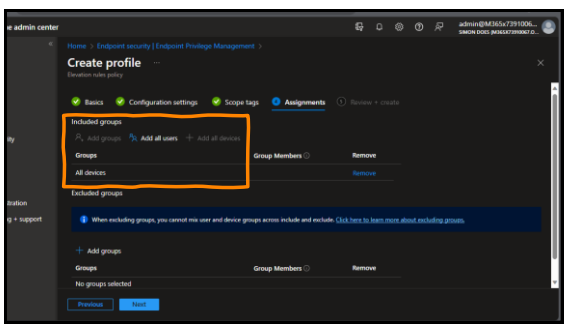

Microsoft Intune admin center
Create profile
Rule properties
File name
File path
Signature source
Not configured
File hash
Minimum version
File description
Product name

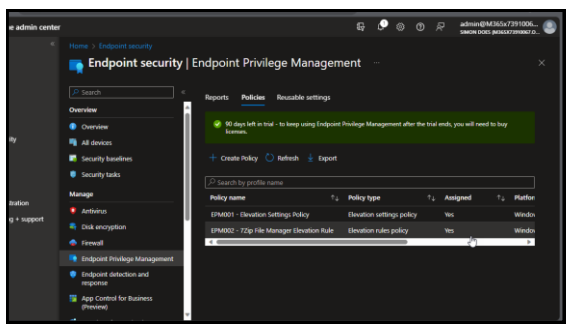

Create profile
Rule properties
File name
File path
Signature source
Not configured
File hash
Minimum version
File description
Product name

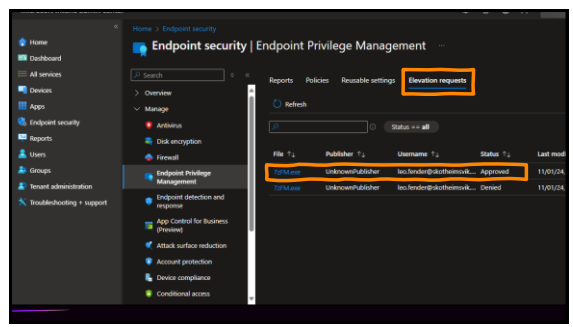

Create profile
Rule properties
File name
File path
Signature source
Not configured
File hash
Minimum version
File description
Product name

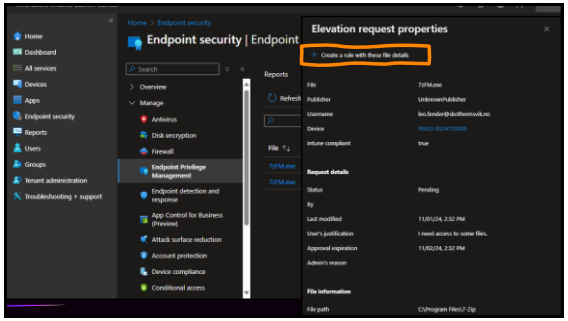

Create profile
Rule properties
Basics
Configuration settings
Privilege Management
File name
File path
Signature source
File hash
Minimum version
File description
Product name
Internal name
Previous
Next
Save

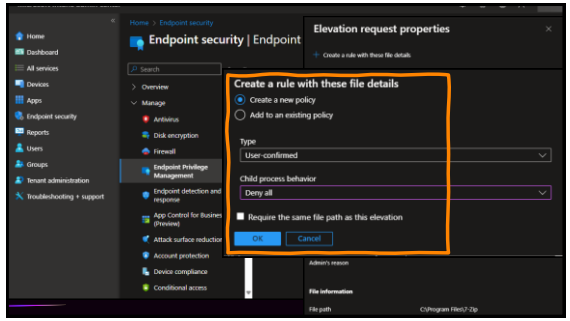

Create profile
Basics
Configuration settings
Privilege Management
Elevation type
Rule name
Configure settings
User confirmed
7Zip
Previous
Next

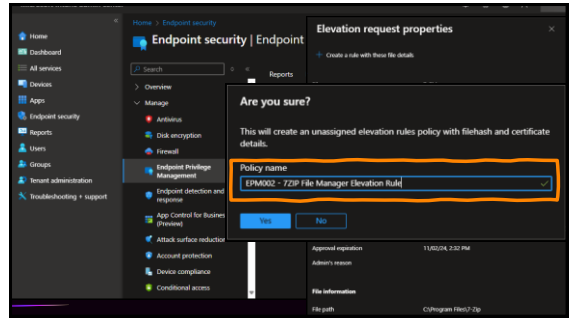

Create profile
Basics
Configuration settings
Scope tags
Assignments
Included groups
Add all users
Groups
Group Members
Remove
All devices
Excluded groups
No groups selected
Previous
Next

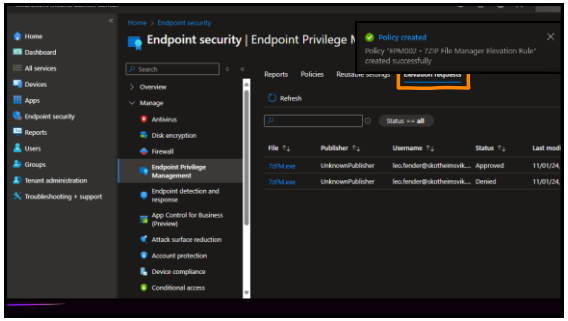

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Overview
Manage
Create Policy
Refresh
Export
Policy name
Policy type
Assigned
EPM001 - Elevation Settings Policy
EPM002 - 7Zip File Manager Elevation Rule

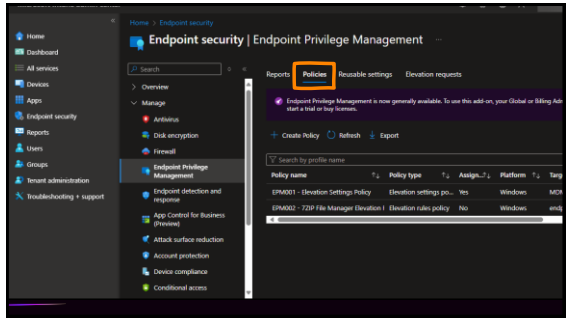

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation requests
Refresh
File
Publisher
Username
Status
UnknownPublisher
Approved
Denied

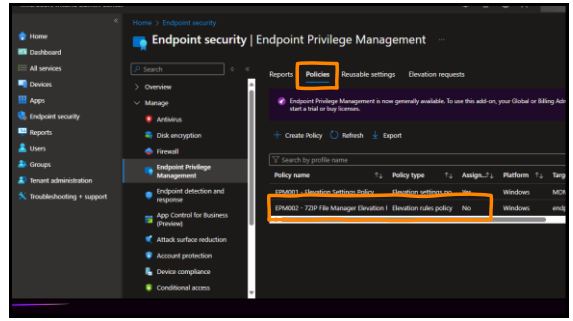

Endpoint security | Endpoint
Elevation request properties
Create a rule with these file details

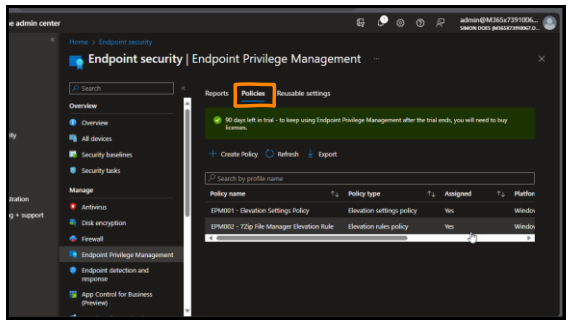

Endpoint security | Endpoint
Elevation request properties
Create a rule with these file details
Create a new policy
Add to an existing policy
Type
User-confirmed
Child process behavior
Deny all
Require the same file path as this elevation
OK
Cancel

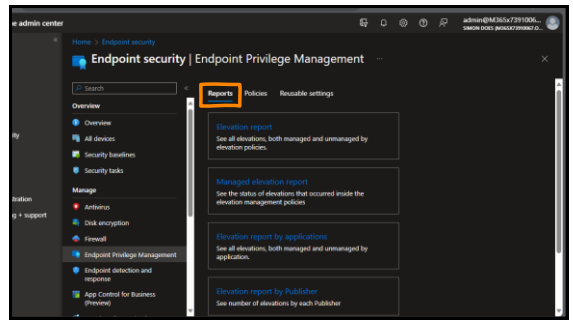

Endpoint security | Endpoint
Elevation request properties
Are you sure?
This will create an unassigned elevation rules policy with filehash and certificate details.
Policy name
EPM002 - 7ZIP File Manager Elevation Rule
Yes
No

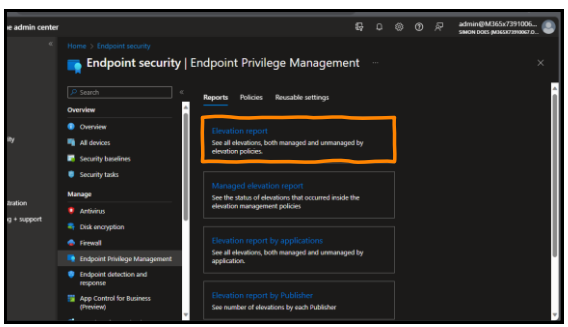

Endpoint security | Endpoint Privilege
Policy created
Reports
Policies
Reusable settings
Elevation requests

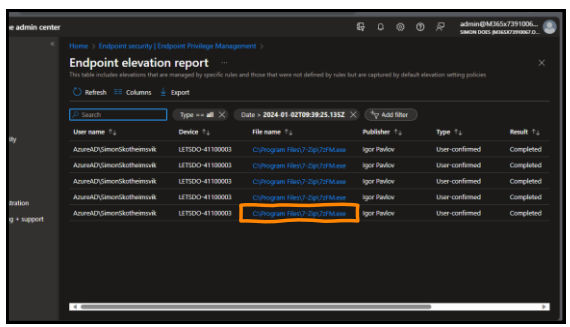

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation requests

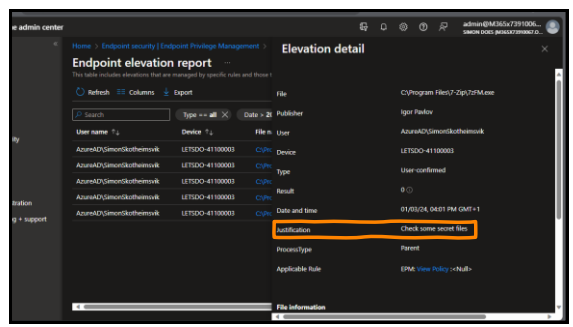

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation requests

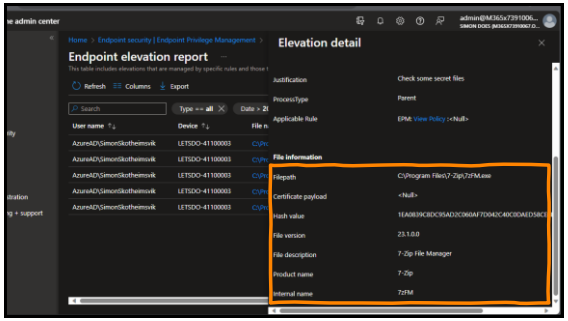

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Create Policy
Refresh
Export

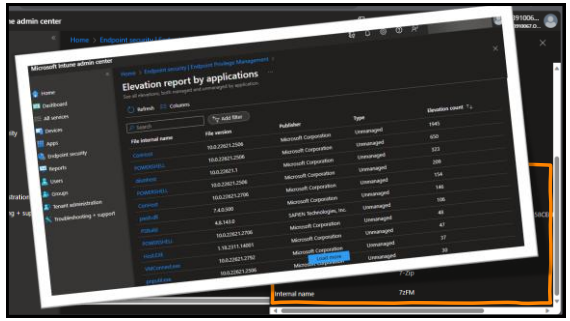

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation report
See all elevations, both managed and unmanaged by elevation policies.
Managed elevation report
See the status of elevations that occurred inside the elevation management policies
Elevation report by applications
See all elevations, both managed and unmanaged by application.
Elevation report by Publisher
See number of elevations by each Publisher

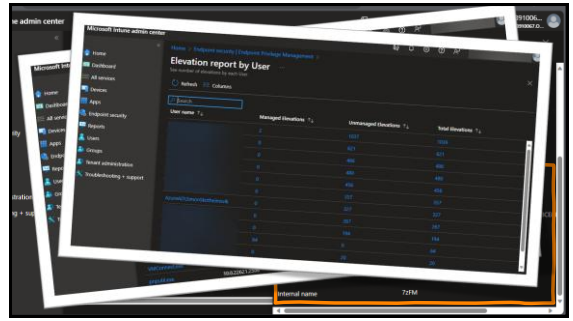

Endpoint security | Endpoint Privilege Management
Reports
Policies
Reusable settings
Elevation report
See all elevations, both managed and unmanaged by elevation policies.
Managed elevation report
See the status of elevations that occurred inside the elevation management policies
Elevation report by applications
See all elevations, both managed and unmanaged by application.
Elevation report by Publisher
See number of elevations by each Publisher


Endpoint elevation report
User name
Device
File name
Publisher
Type
Result


Endpoint elevation report
Elevation detail
Justification
Check some secret files


Endpoint elevation report
Elevation detail
Justification
Check some secret files
ProcessType
Parent
Applicable Rule
File information
Filepath
C:\Program Files\7-Zip\7zFM.exe
Certificate payload
Hash value
File version
23.1.0.0
File description
7-Zip File Manager
Product name
7-Zip
Internal name
7zFM


Elevation report by applications
Internal name
7zFM


Elevation report by User
Internal name
7zFM


7
How?
Can we do stuff?
NIC


8
How?
Can we do stuff?
Embrace Modern
NIC


Embrace Modern
1010
1010
Usermode Space
Admin Space
System Space
NIC

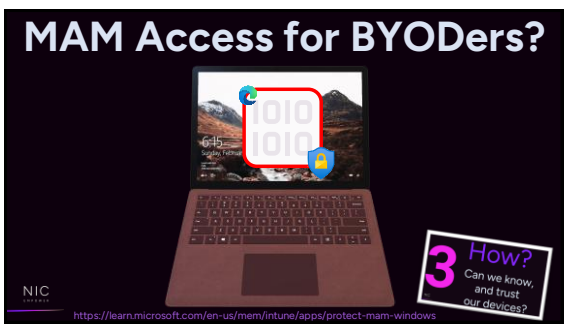

Embrace Modern
Usermode Space
Admin Space
System Space

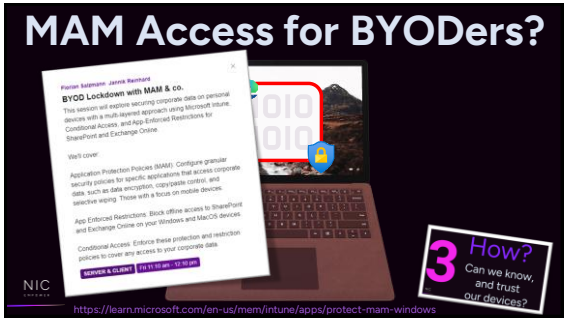

8
How?
Can we do stuff?
NIC

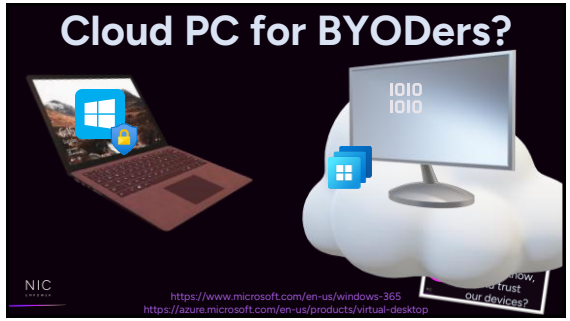

9
How?
Can we do stuff?
BYODers
NIC


9
How?
Can we do stuff?
BYODers
3
How?
Can we know, and trust our devices?
NIC


No Access for BYODers?
Zero Trust policy enforcement
Microsoft Conditional Access
3
How?
Can we know, and trust our devices?
NIC


MAM Access for BYODers?
3
How?
Can we know, and trust our devices?
NIC
https://learn.microsoft.com/en-us/mem/intune/apps/protect-mam-windows

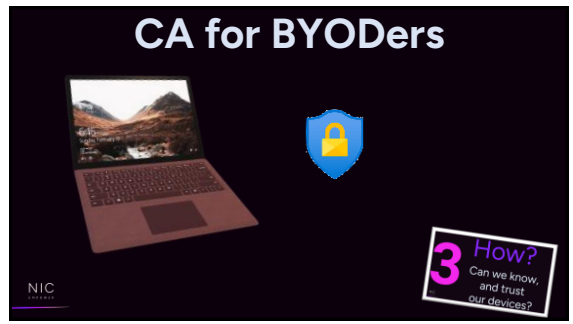

MAM Access for BYODers?
BYOD Lockdown with MAM & co.
3 How? Can we know, and trust our devices?
https://learn.microsoft.com/en-us/mem/intune/apps/protect-mam-windows

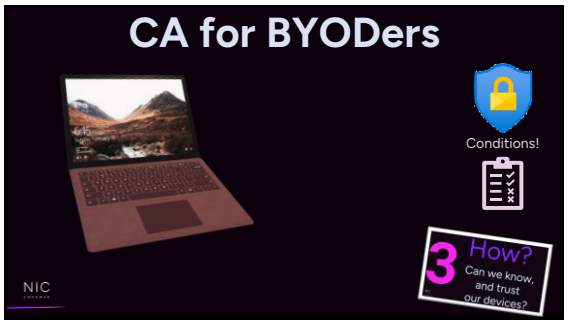

Cloud PC for BYODers?
https://www.microsoft.com/en-us/windows-365
https://azure.microsoft.com/en-us/products/virtual-desktop

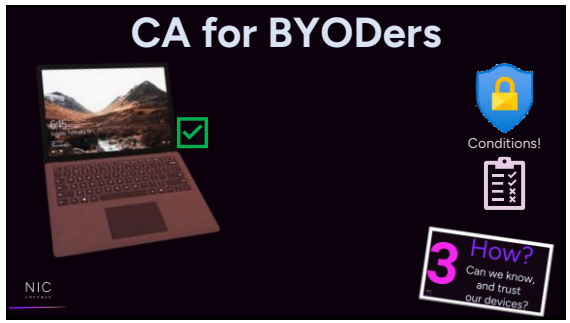

Cloud PC for BYODers?
Army University continues innovation with mass adoption of remote desktop

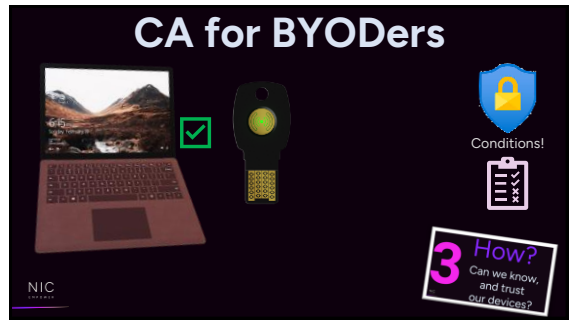

Cloud PC for BYODers?
https://www.microsoft.com/en-us/windows-365
https://azure.microsoft.com/en-us/products/virtual-desktop


Cloud PC for BYODers?
Unleash the power of Intune and Azure Virtual Desktop
Reach out to the sky with Azure Virtual Desktop
https://www.microsoft.com/en-us/windows-365
https://azure.microsoft.com/en-us/products/virtual-desktop


CA for BYODers
3 How? Can we know, and trust our devices?


CA for BYODers
Conditions!
3 How?
Can we know, and trust our devices?
NIC


CA for BYODers
Conditions!
3 How?
Can we know, and trust our devices?
NIC

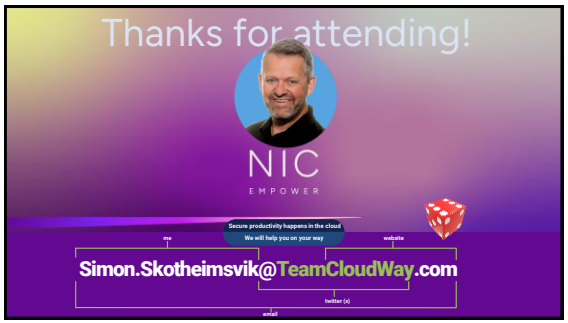

CA for BYODers
Conditions!
3 How?
Can we know, and trust our devices?
NIC


10 DON'T BE
The Hackers Dream Customer
NIC


10 DON'T BE
The Hackers Dream Customer
Remove LOCAL ADMIN!
NIC


10 DON'T BE
The Hackers Dream Customer
Remove LOCAL ADMIN!
NIC


Simon Says
Remove
LOCAL ADMIN!
NIC


Thanks for attending!
NIC
EMPOWER
Secure productivity happens in the cloud
We will help you on your way
me
website
Simon.Skotheimsvik@TeamCloudWay.com
twitter (x)
email