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 EMPOWER

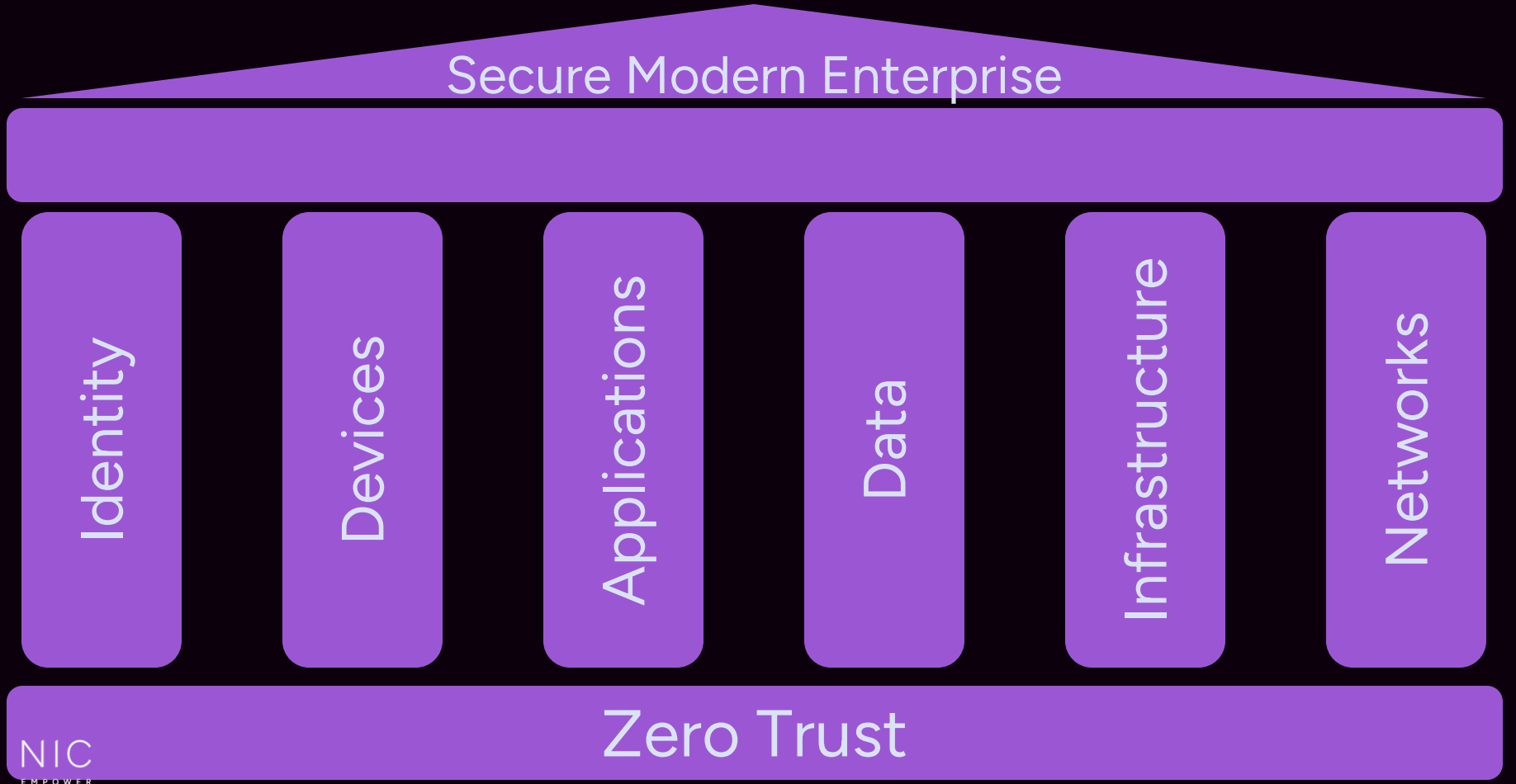
1 Why?

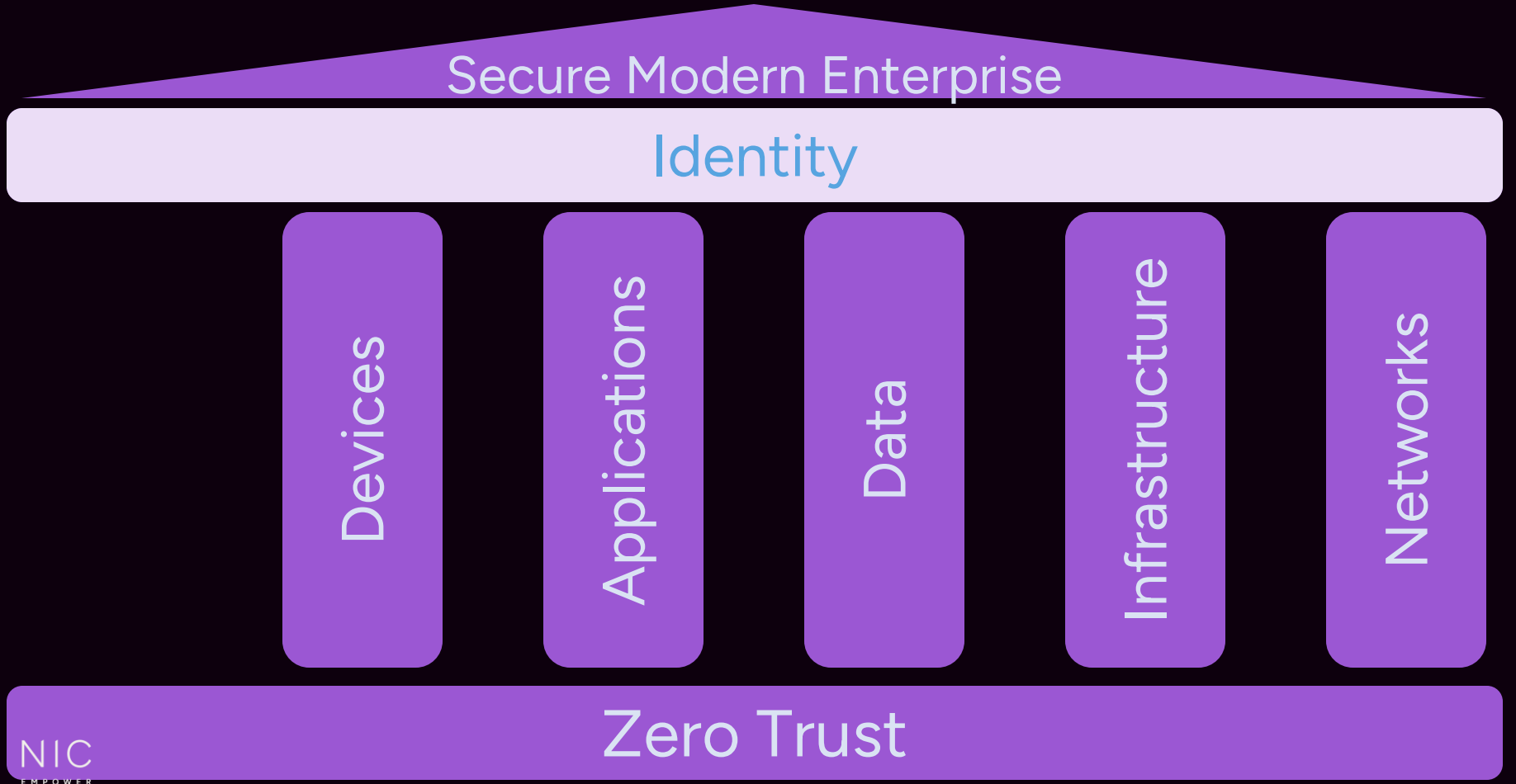
NIC
EMPOWER

Secure Modern Enterprise

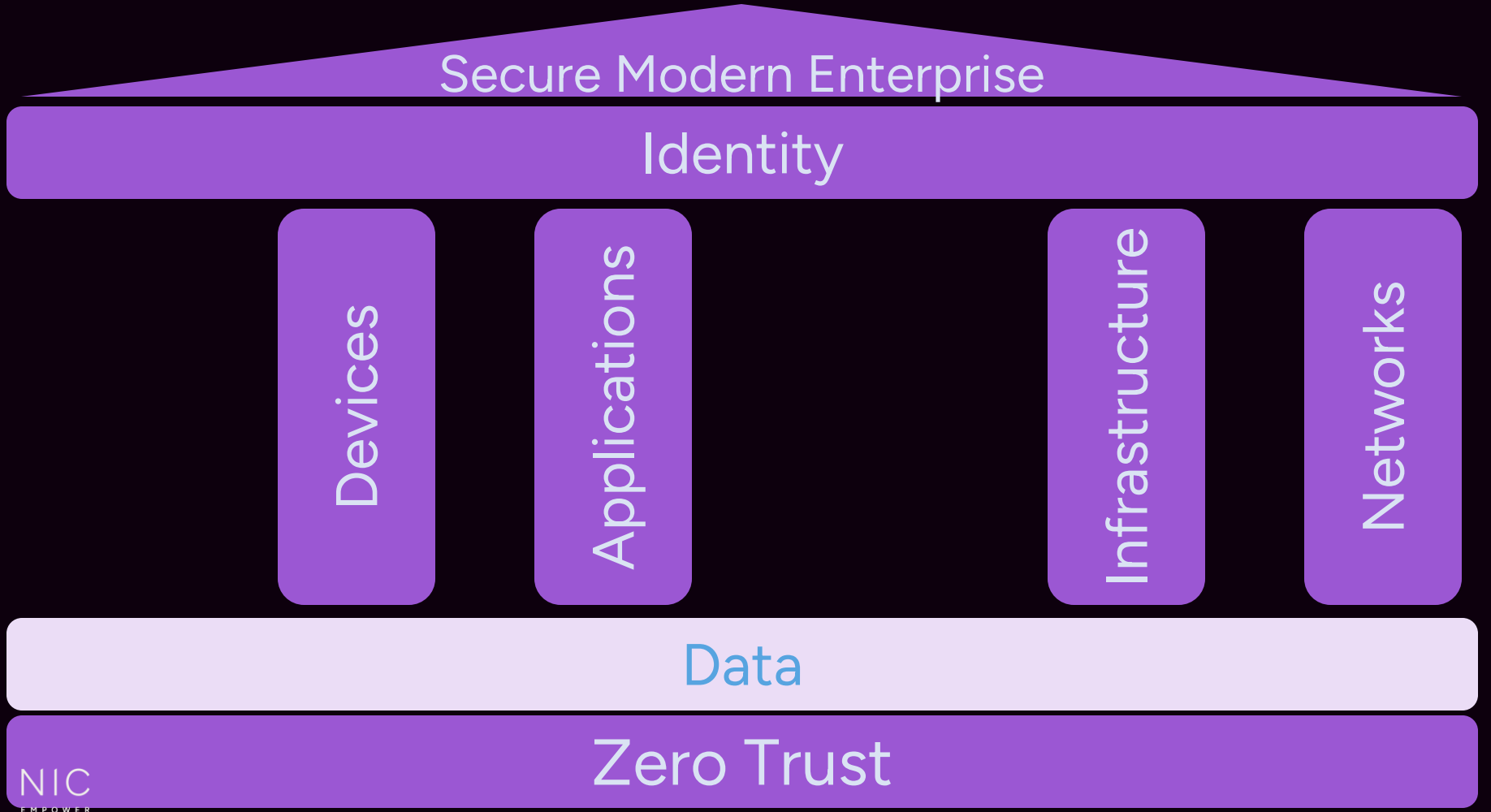
Zero Trust

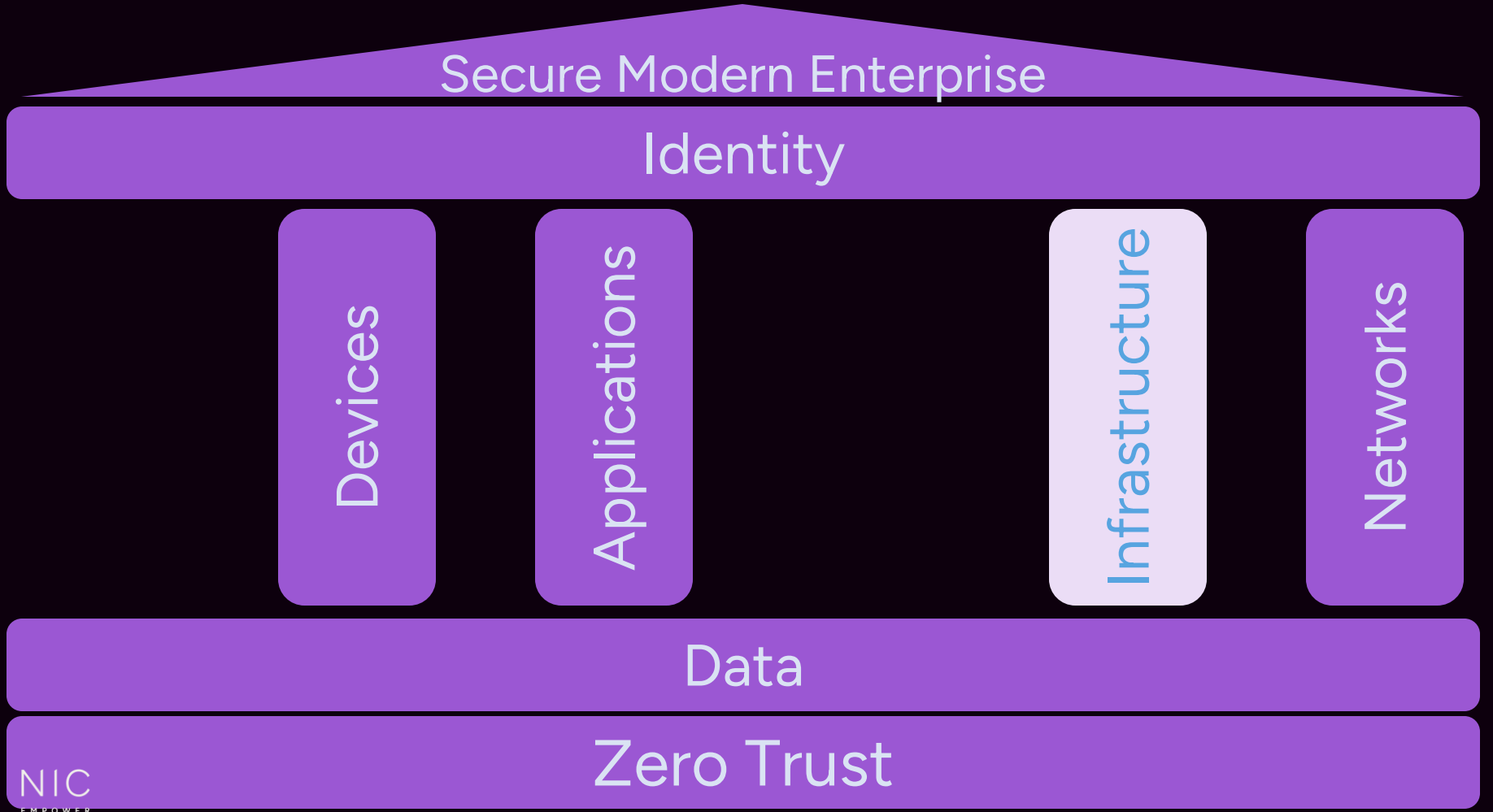
NIC
EMPOWER


Secure Modern Enterprise
Identity
Devices
Applications
Data
Infrastructure
Networks
Zero Trust

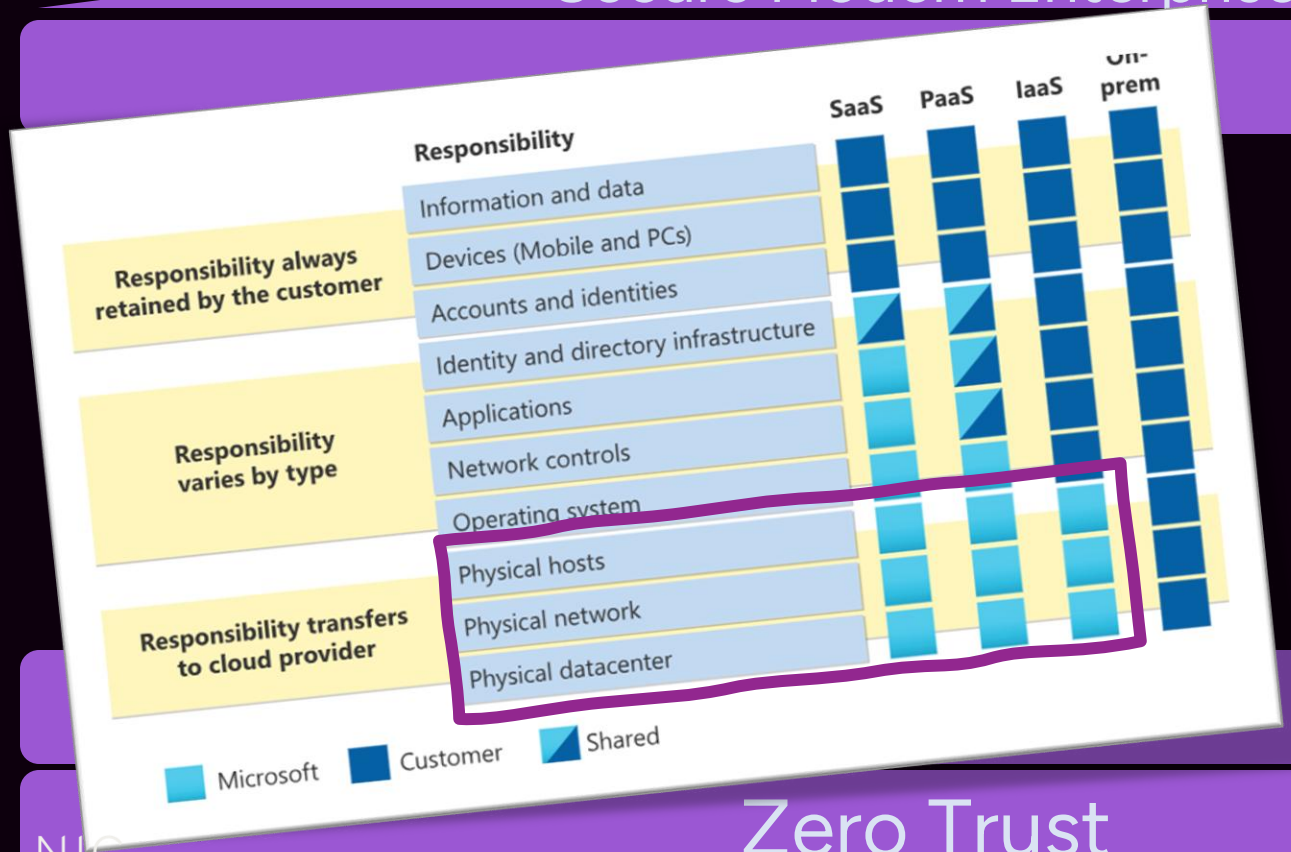

Secure Modern Enterprise
Identity
Devices
Applications
Data
Infrastructure
Networks
Zero Trust

NIC
EMPOWER


Secure Modern Enterprise
Identity
Devices
Applications
Infrastructure
Networks
Data
Zero Trust


Secure Modern Enterprise
Identity
Devices
Applications
Infrastructure
Networks
Data
Zero Trust

Secure Modern Enterprise

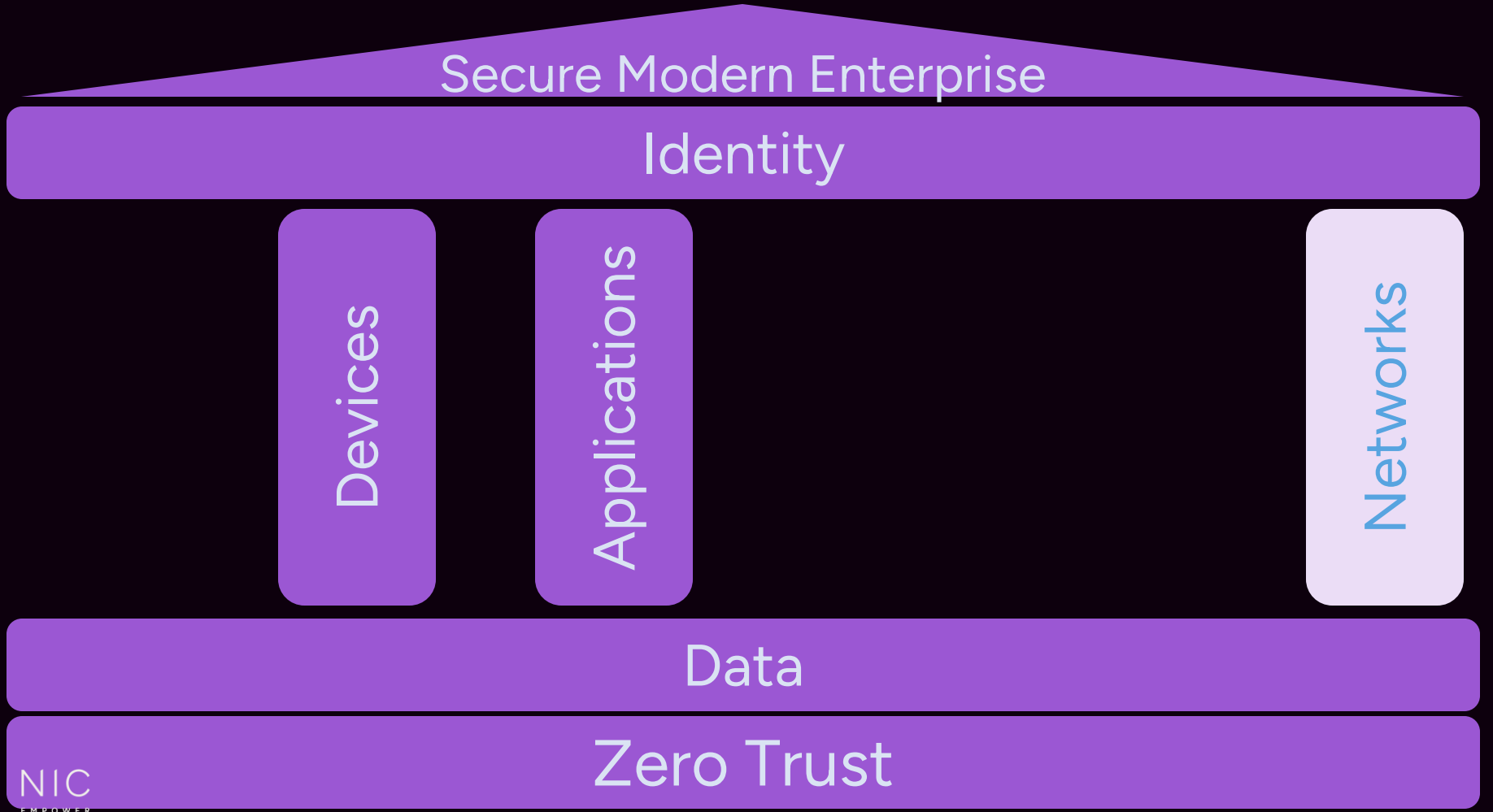


Infrastructure

Networks

Zero Trust

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility


Secure Modern Enterprise
Identity
Devices
Applications
Networks
Data
Zero Trust

Secure Mod

Ide

Devices

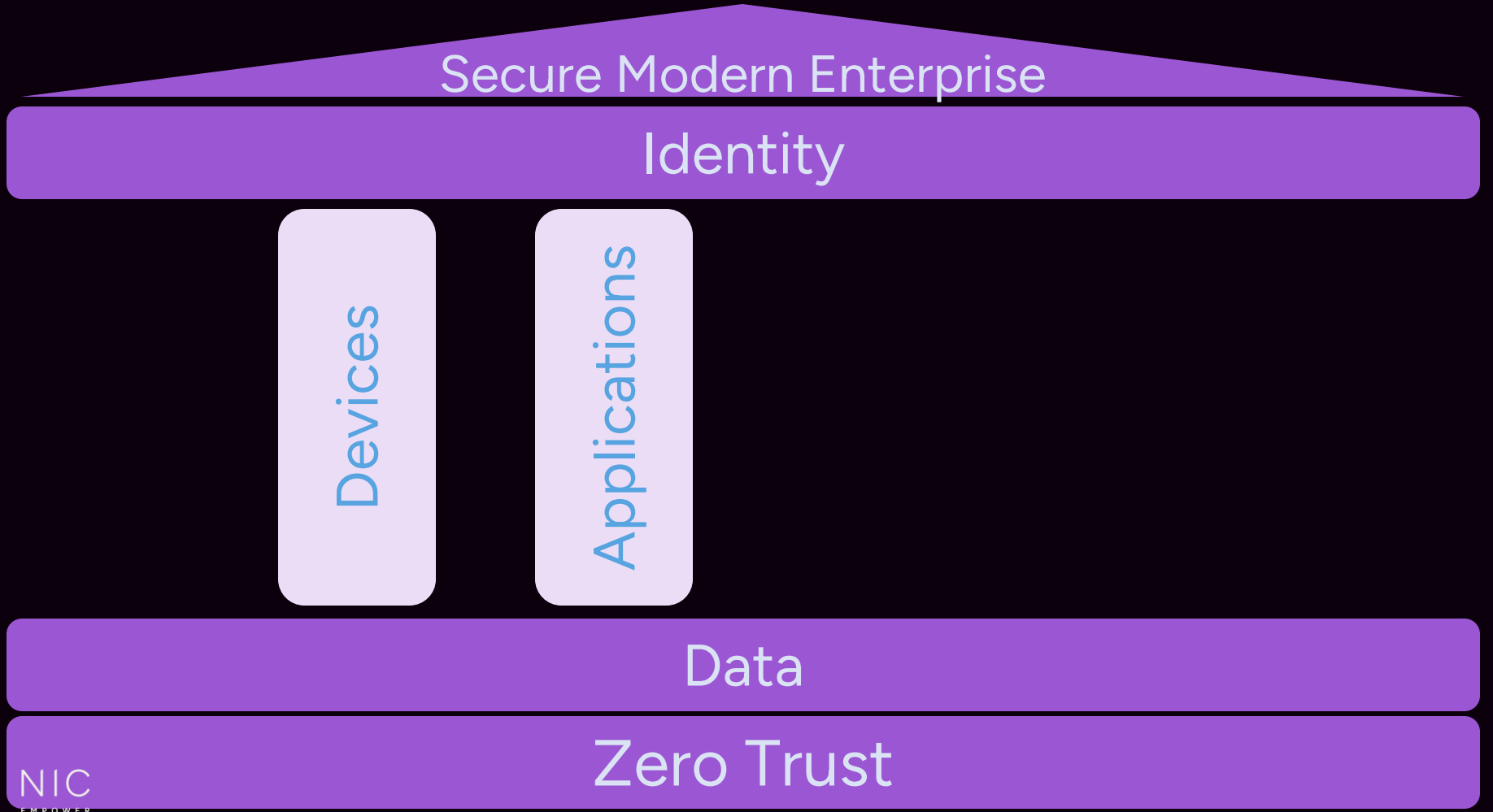
Applications

Networks

Dat

Zero T

NIC
EMPOWER


Secure Modern Enterprise
Identity
Devices
Applications
Data
Zero Trust

1 Why?

NIC
EMPOWER

2

Why?

We must know, and trust our devices!

NIC
EMPOWER

Is this the right country or region?

Norway

Afghanistan

Åland Islands

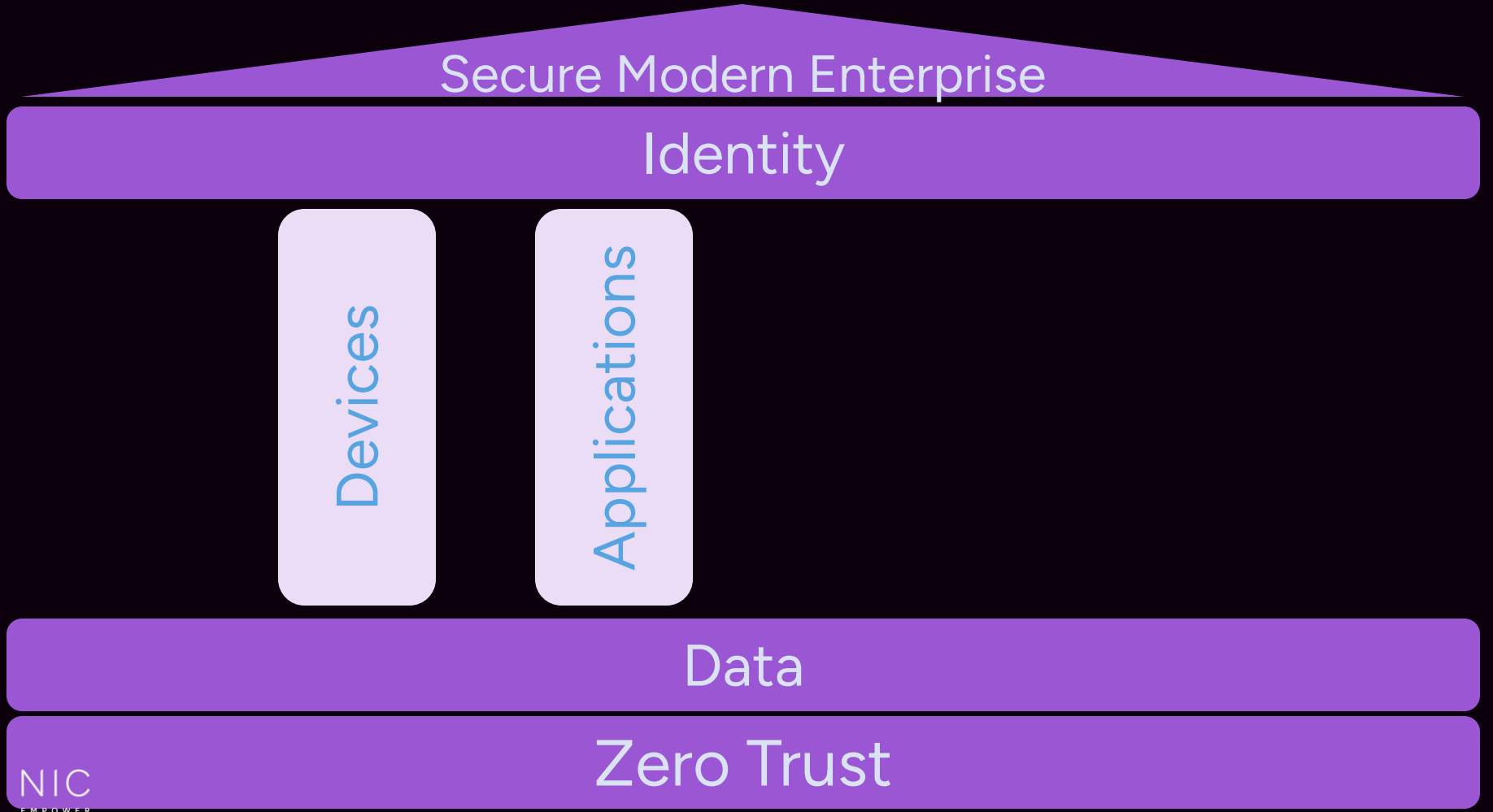
Albania

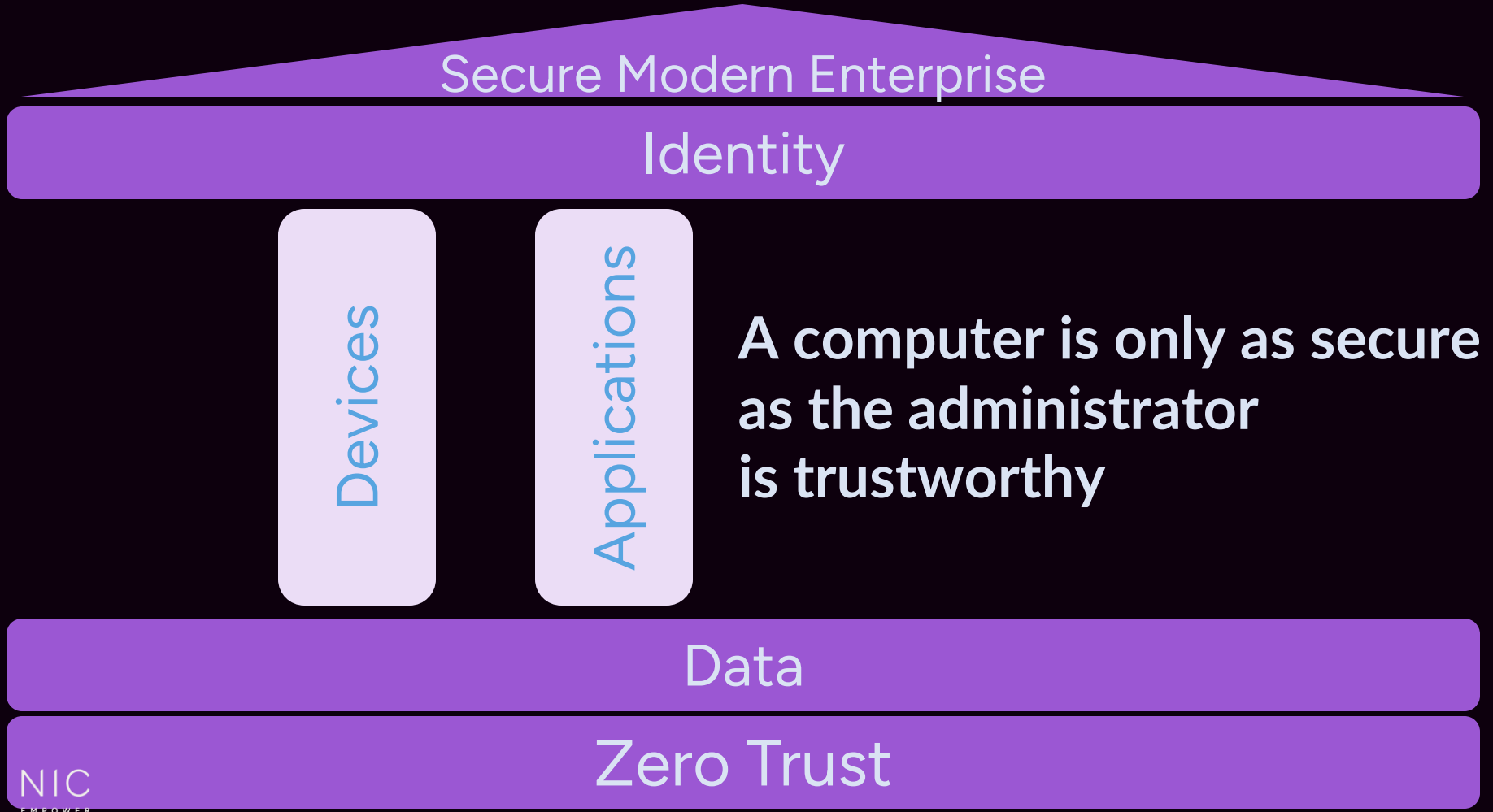
Algeria

American Samoa

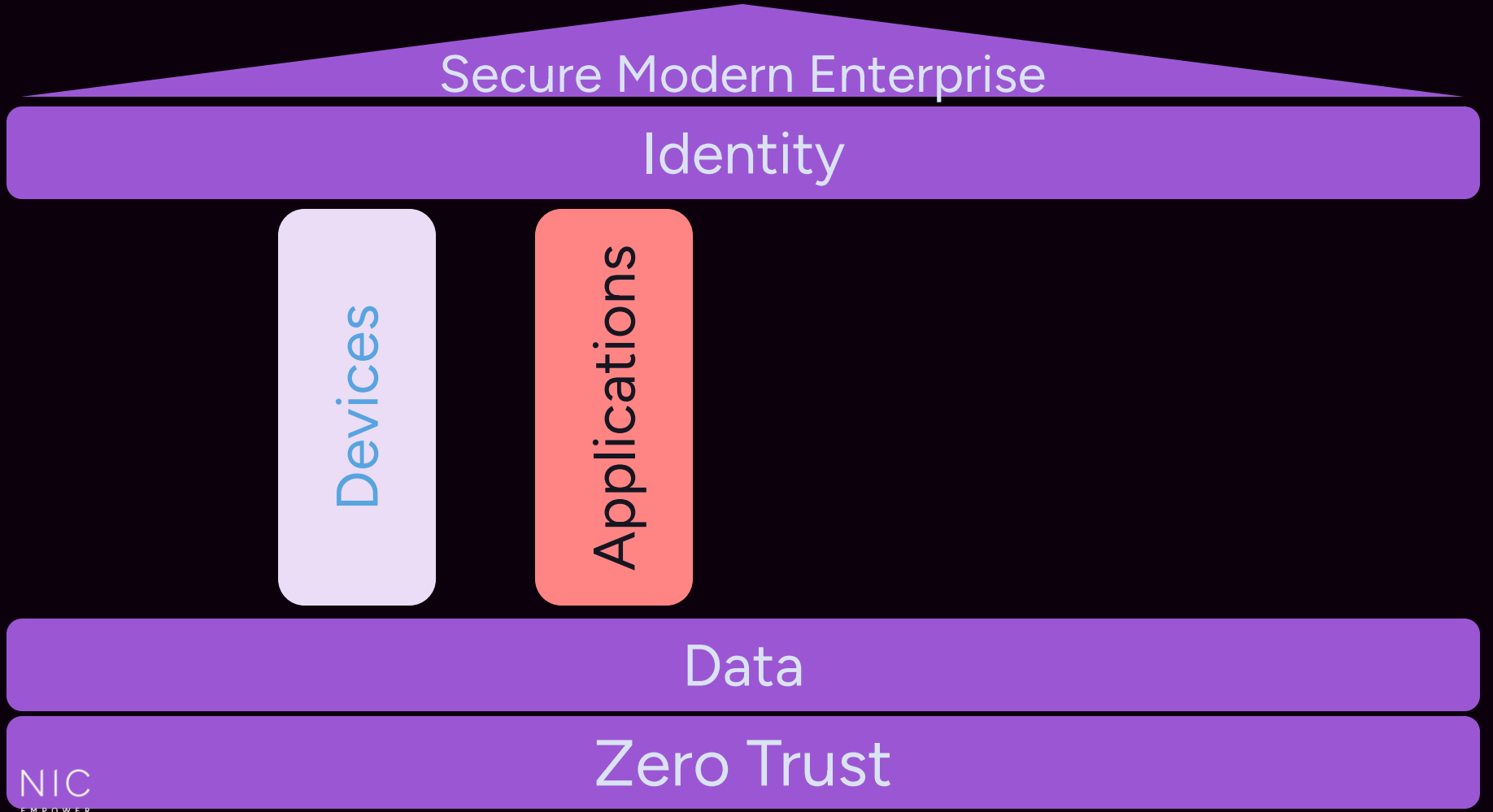
Andorra

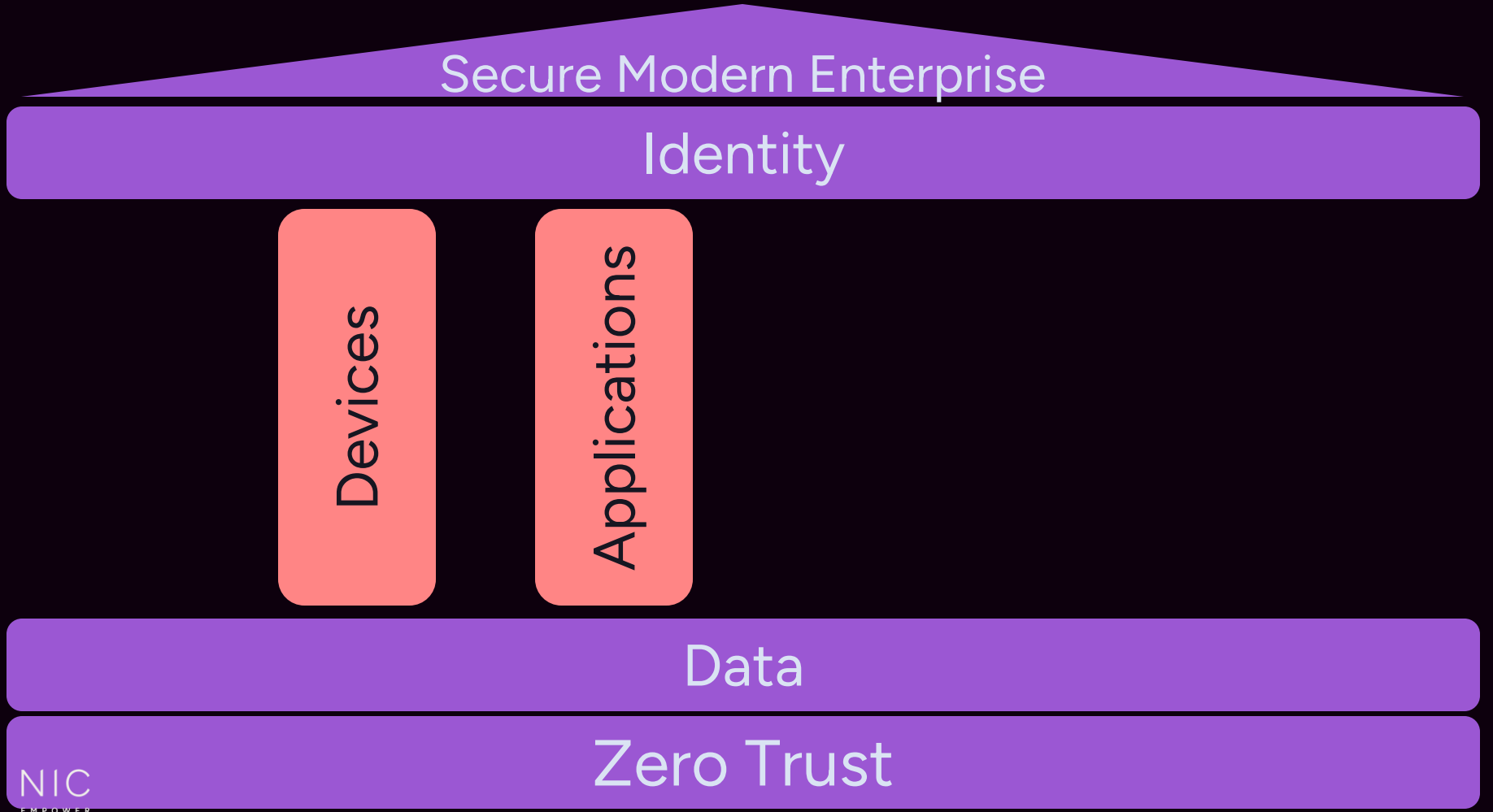
Yes

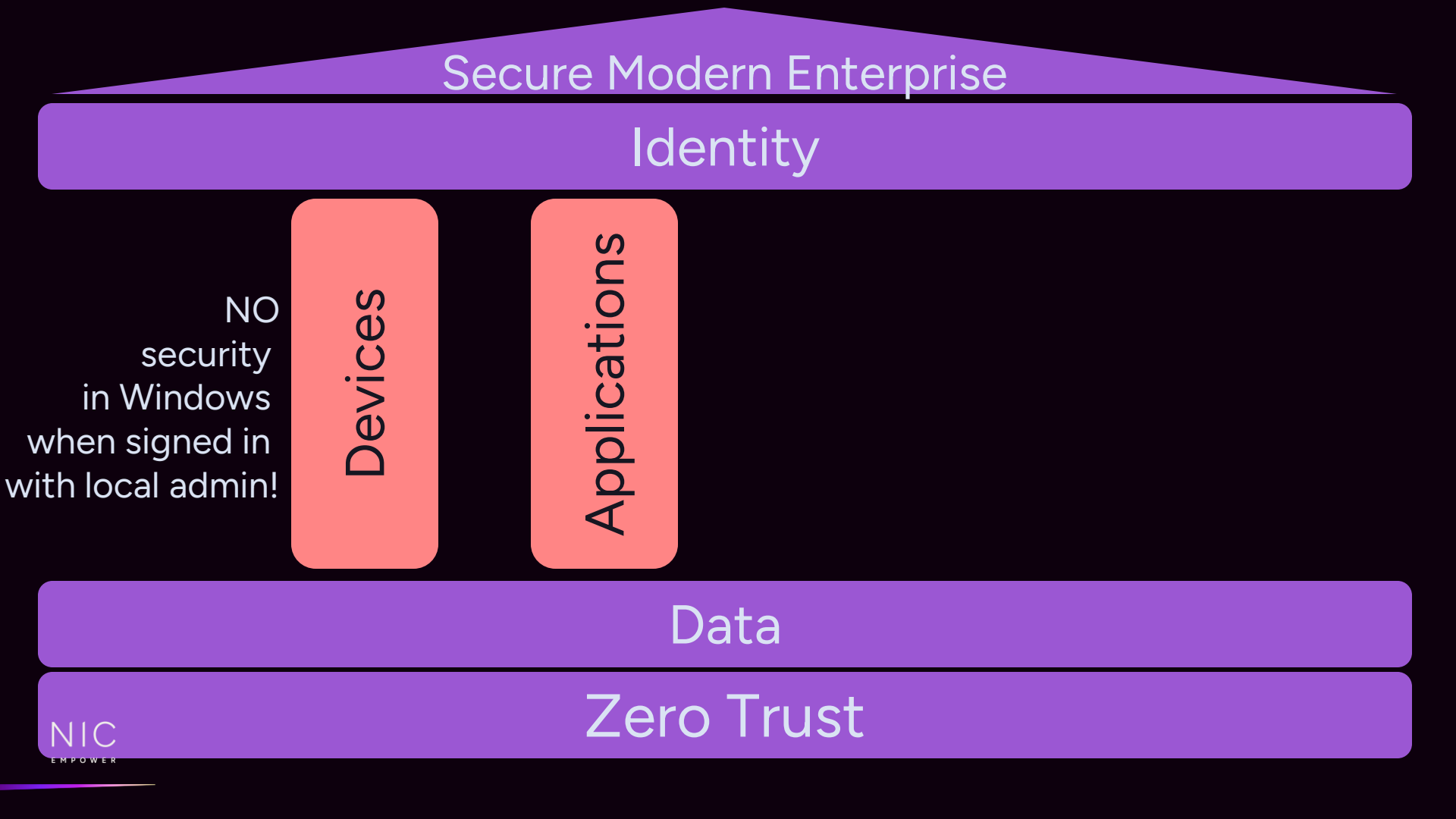

Secure Modern Enterprise
Identity
Devices
Applications
Data
Zero Trust



https://learn.microsoft.com/en-us/security/zero-trust/ten-laws-of-security#immutable-laws-of-security-v2


Secure Modern Enterprise
Identity
Devices
Applications
Data
Zero Trust


Secure Modern Enterprise
Identity
Devices
Applications
Data
Zero Trust


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

2

Why?

We must know, and trust our devices!

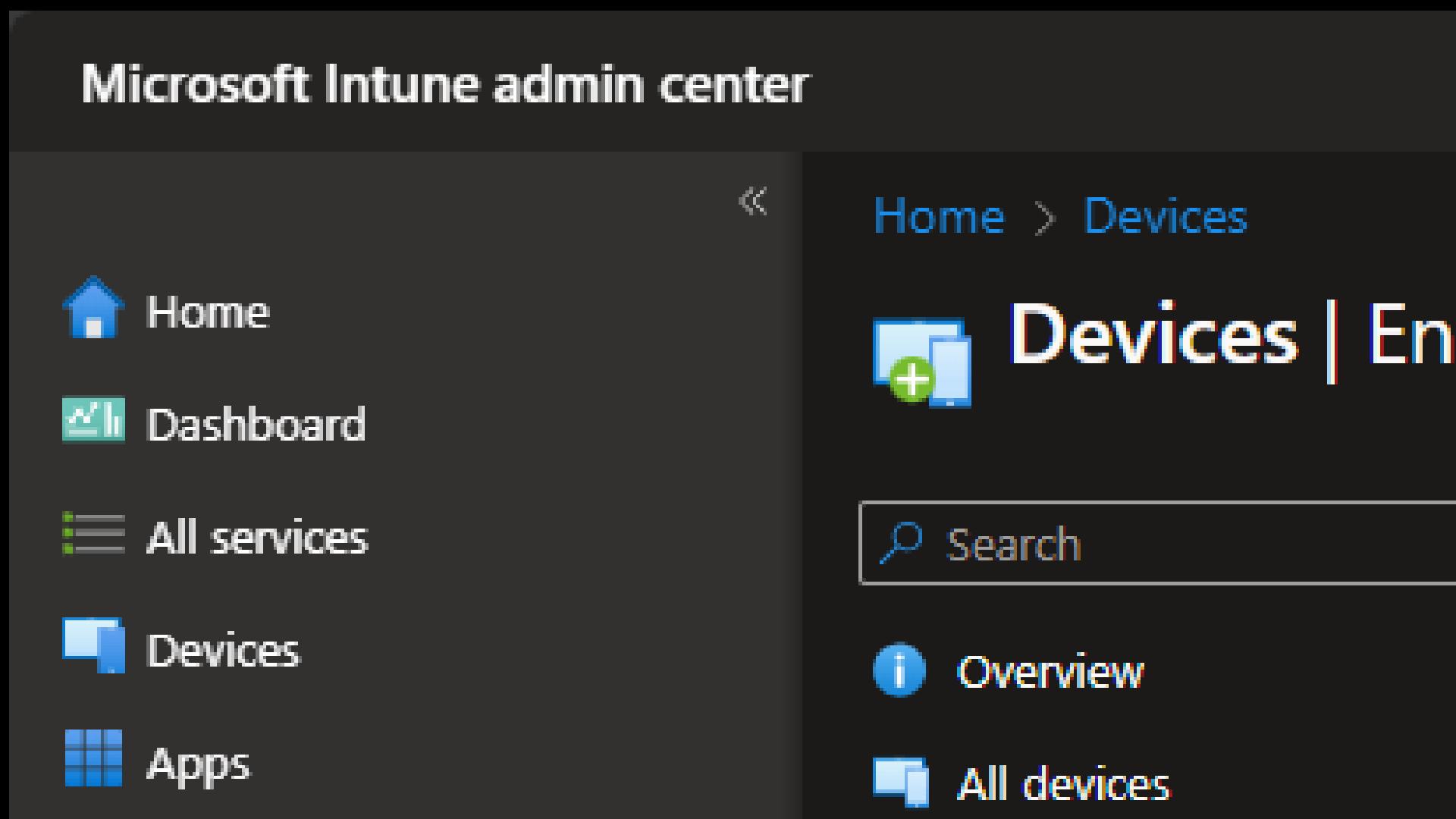
NIC
EMPOWER

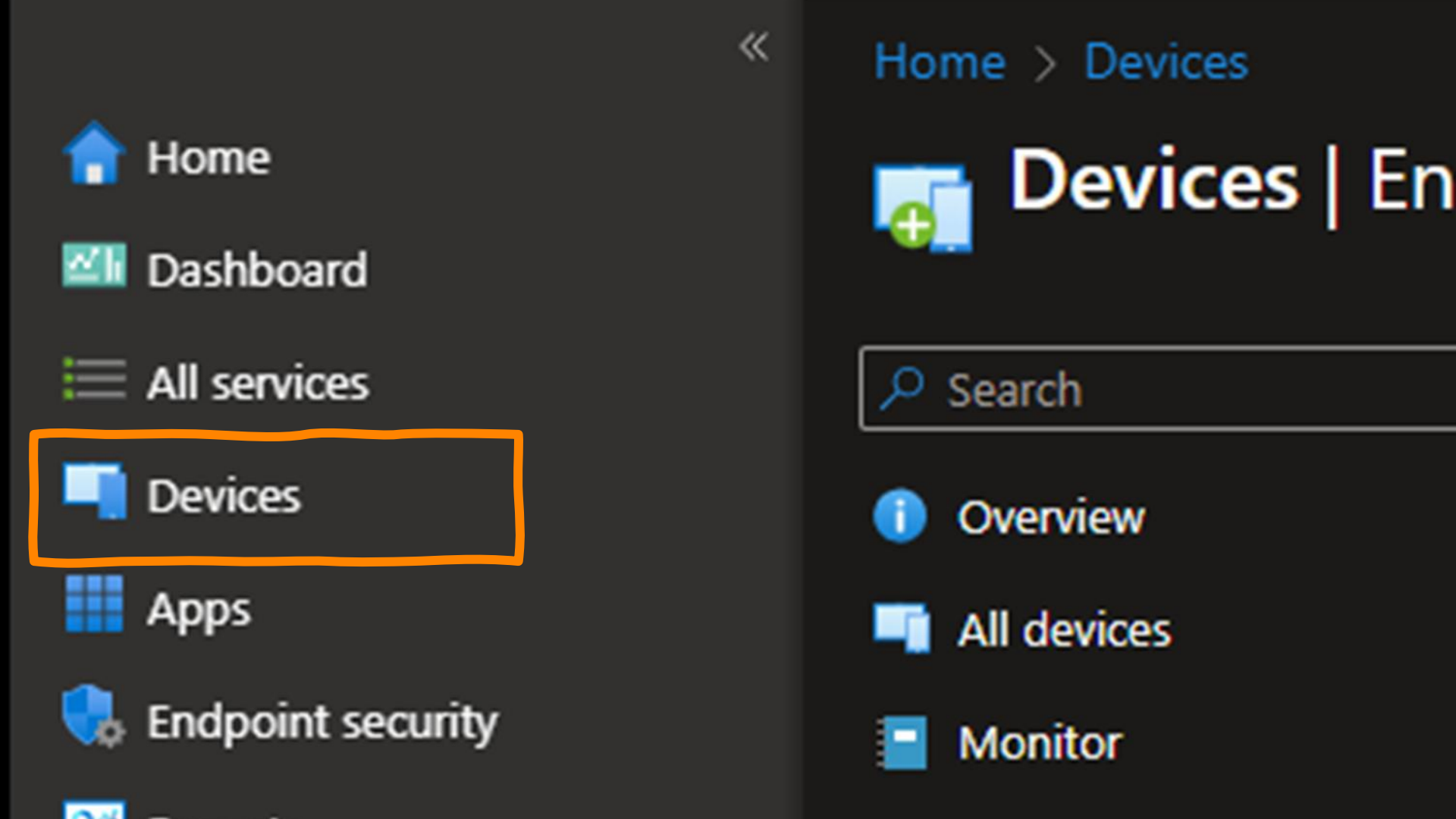
3

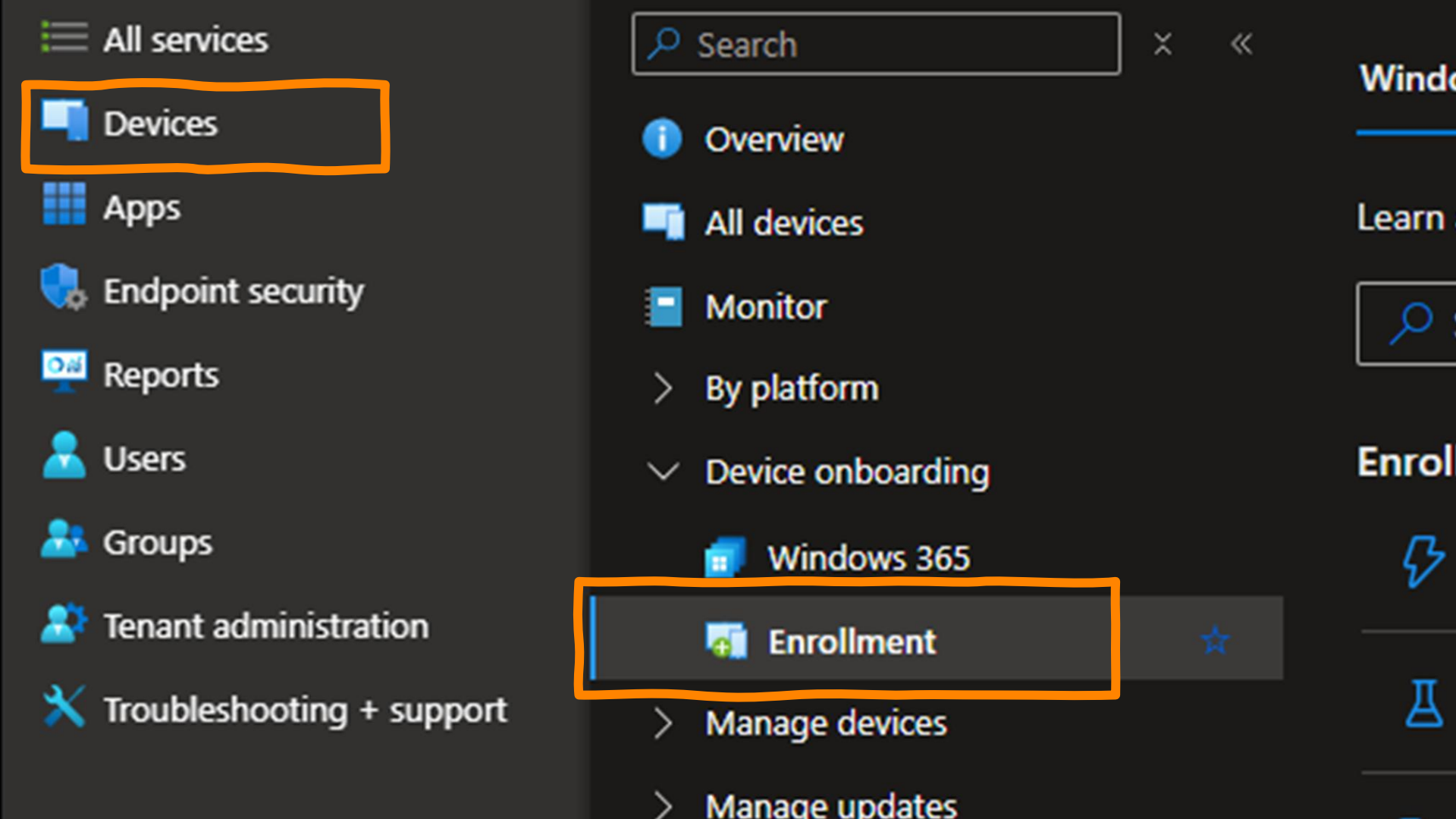
How?

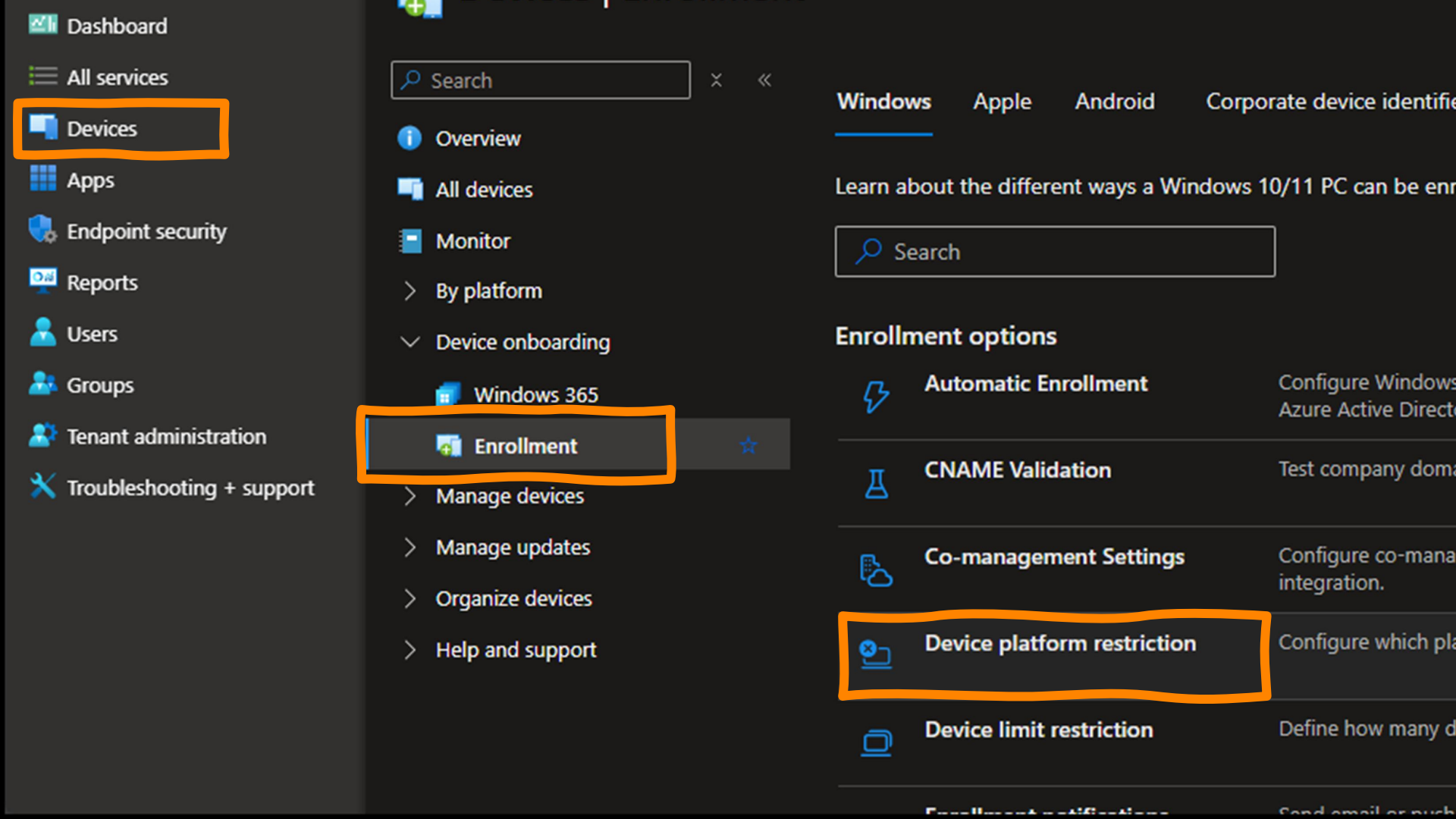
Can we know, and trust our devices?

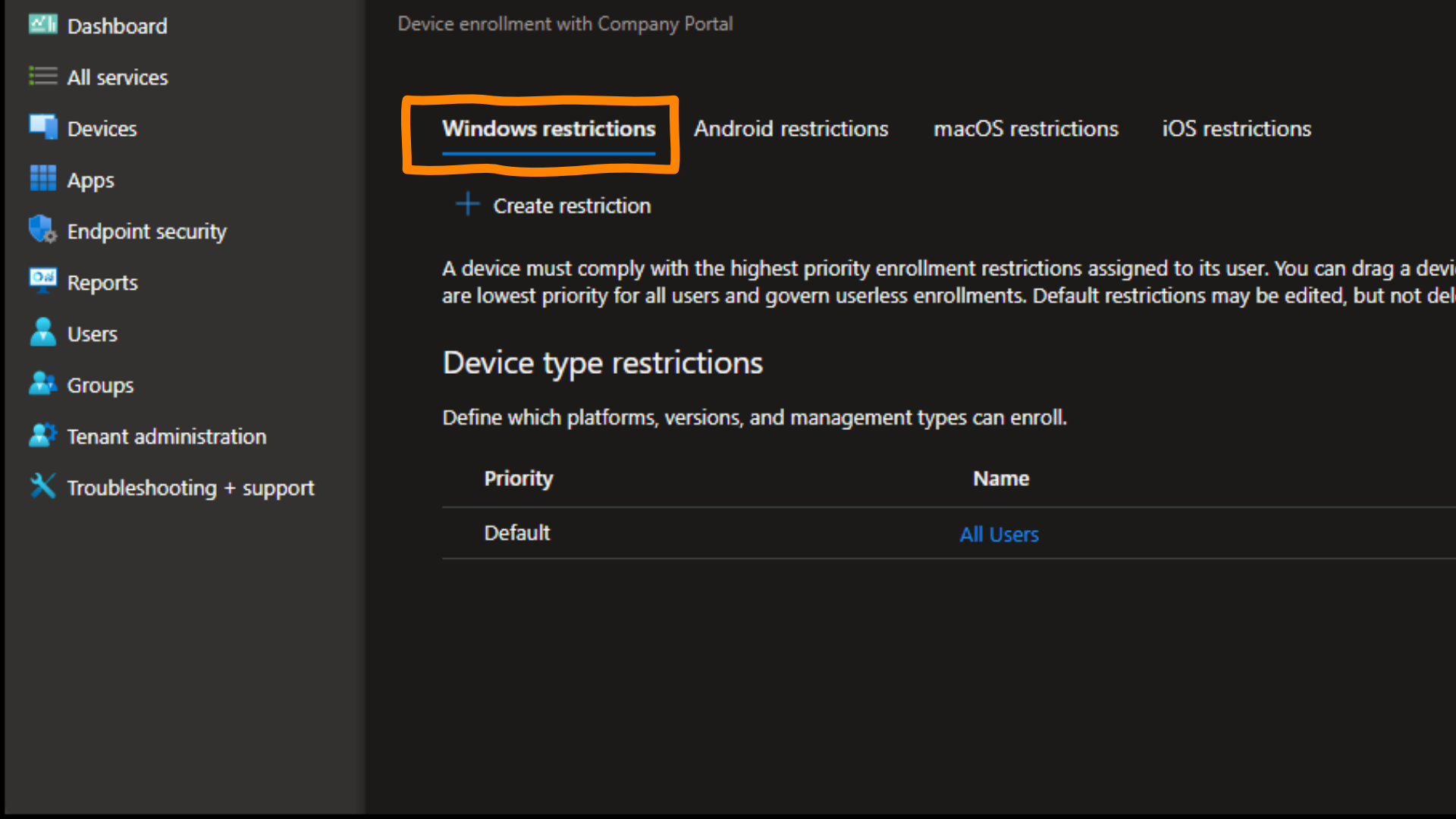
NIC
EMPOWER

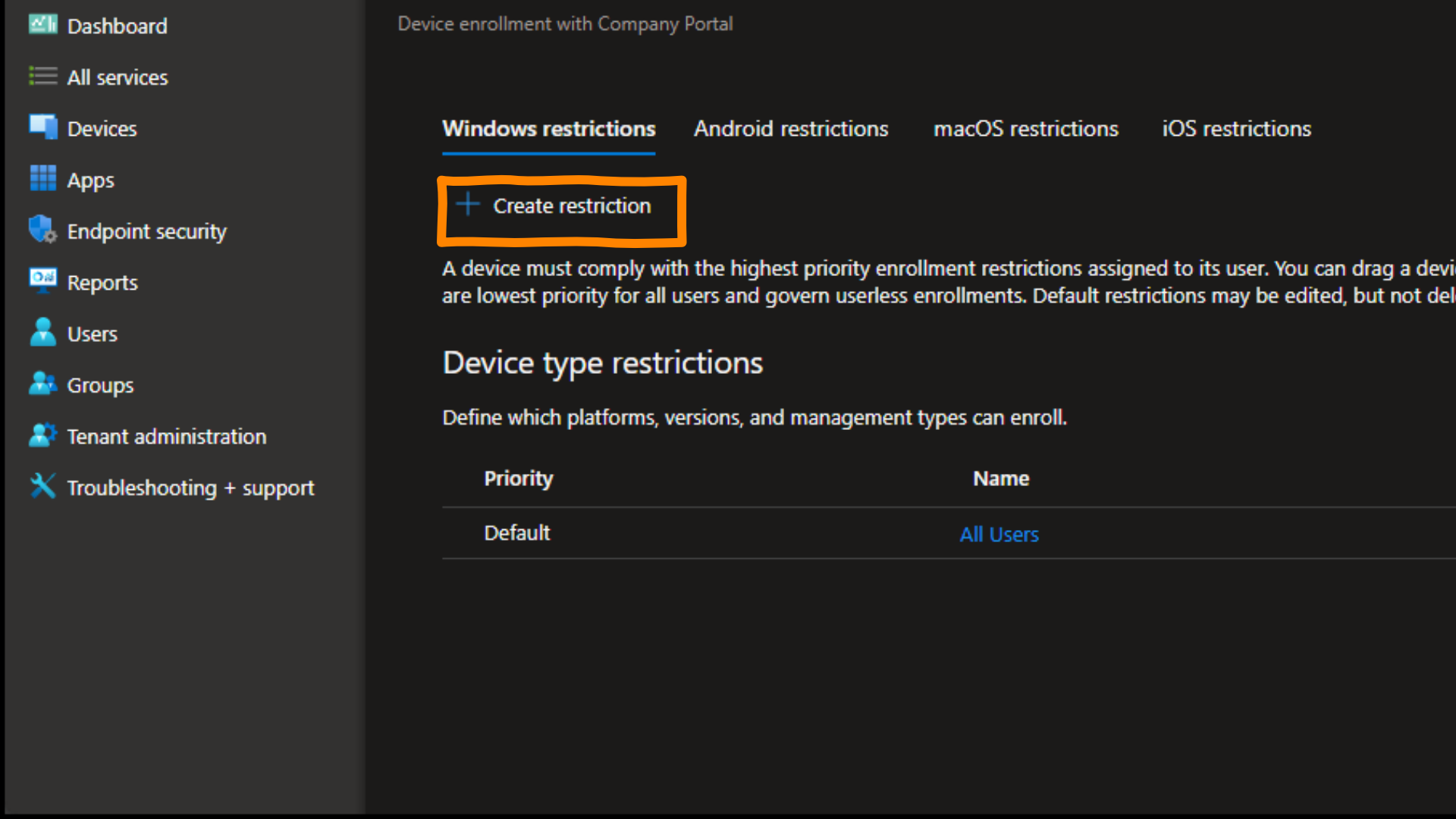

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Home > Devices
Devices | En
Search
Overview
All devices

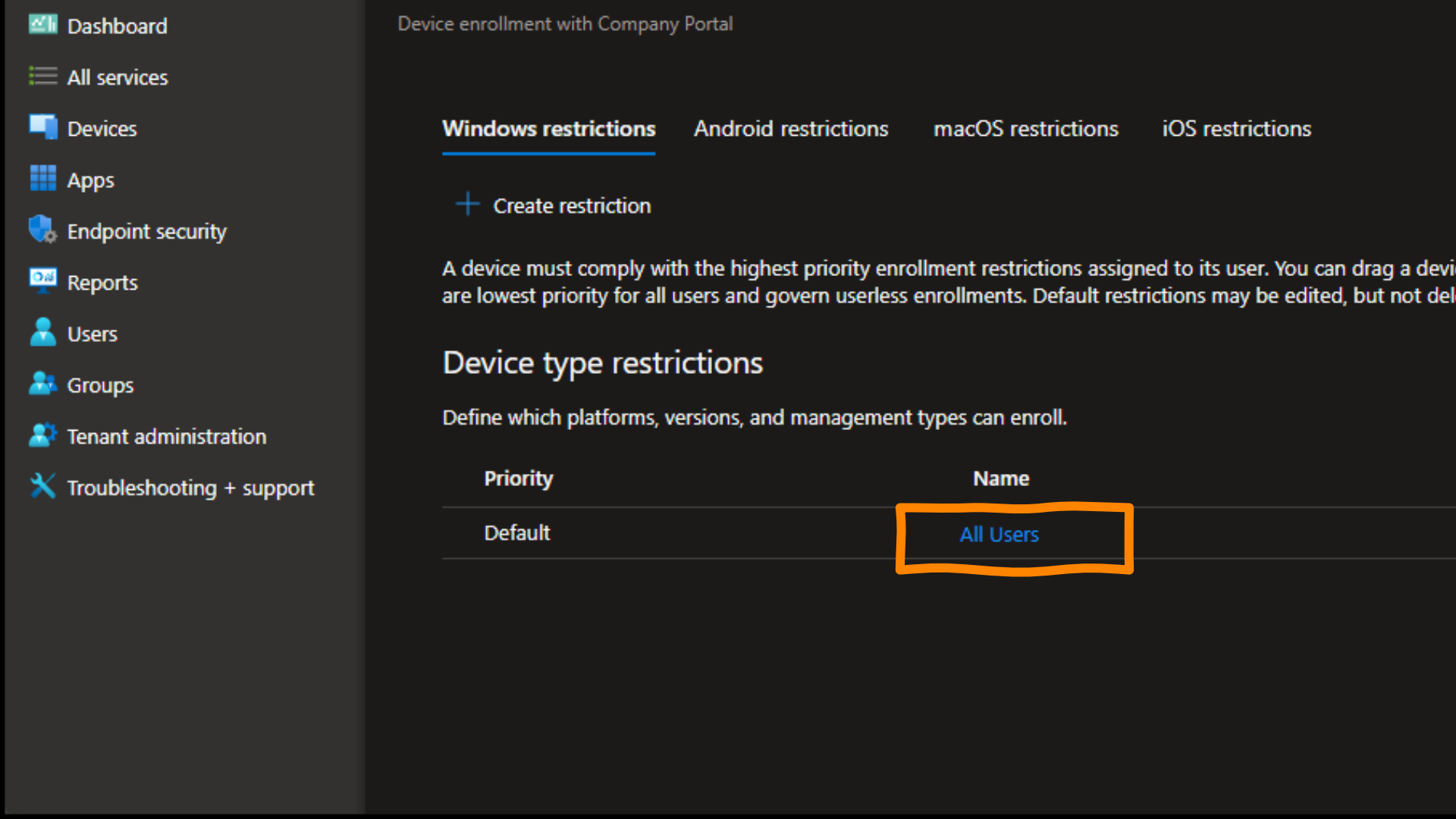

Home
Dashboard
All services
Devices
Apps
Endpoint security
Home > Devices
Devices | En
Search
Overview
All devices
Monitor

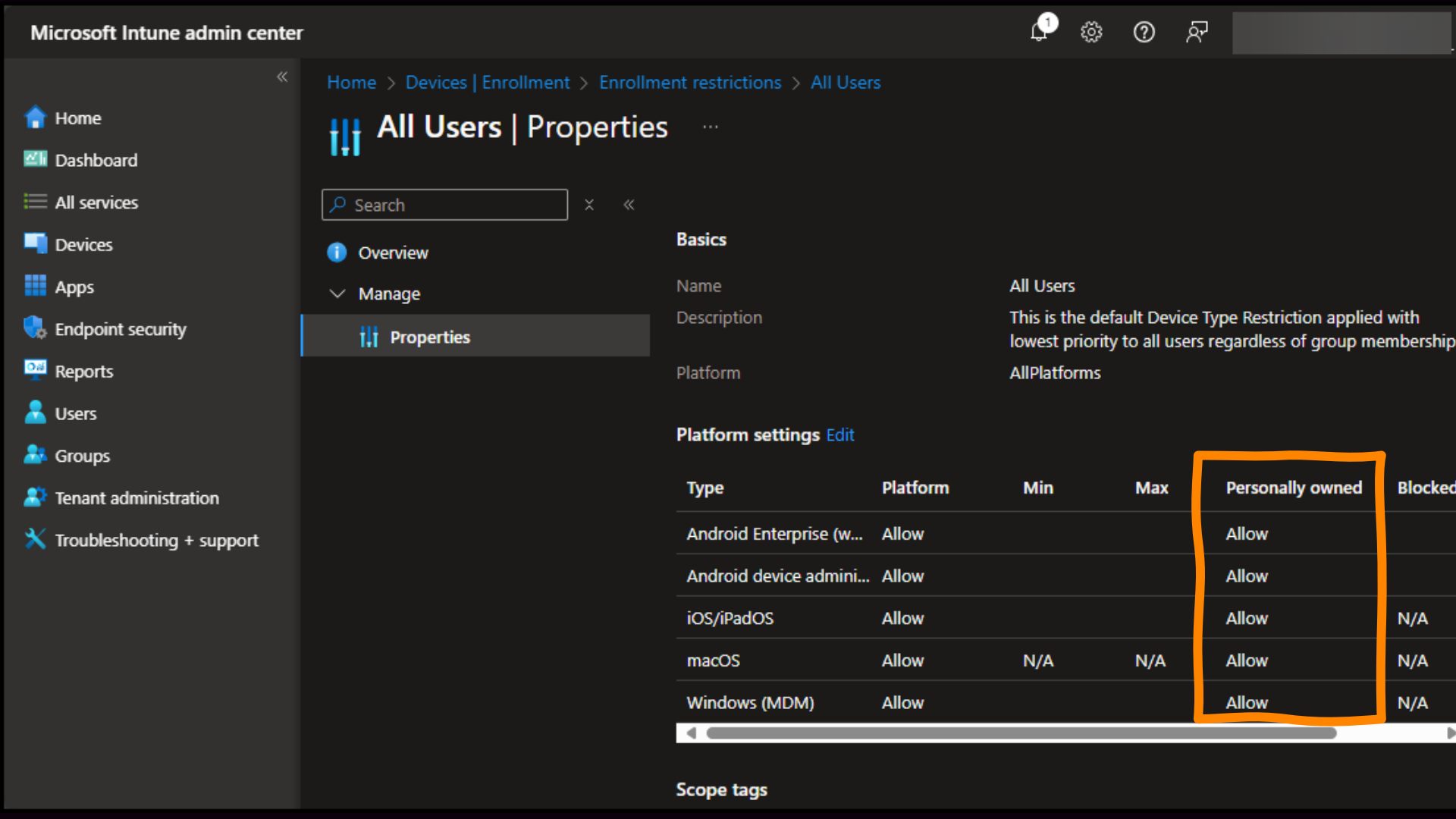

All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Search
Overview
All devices
Monitor
By platform
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates
Windo
Learn
Enrol

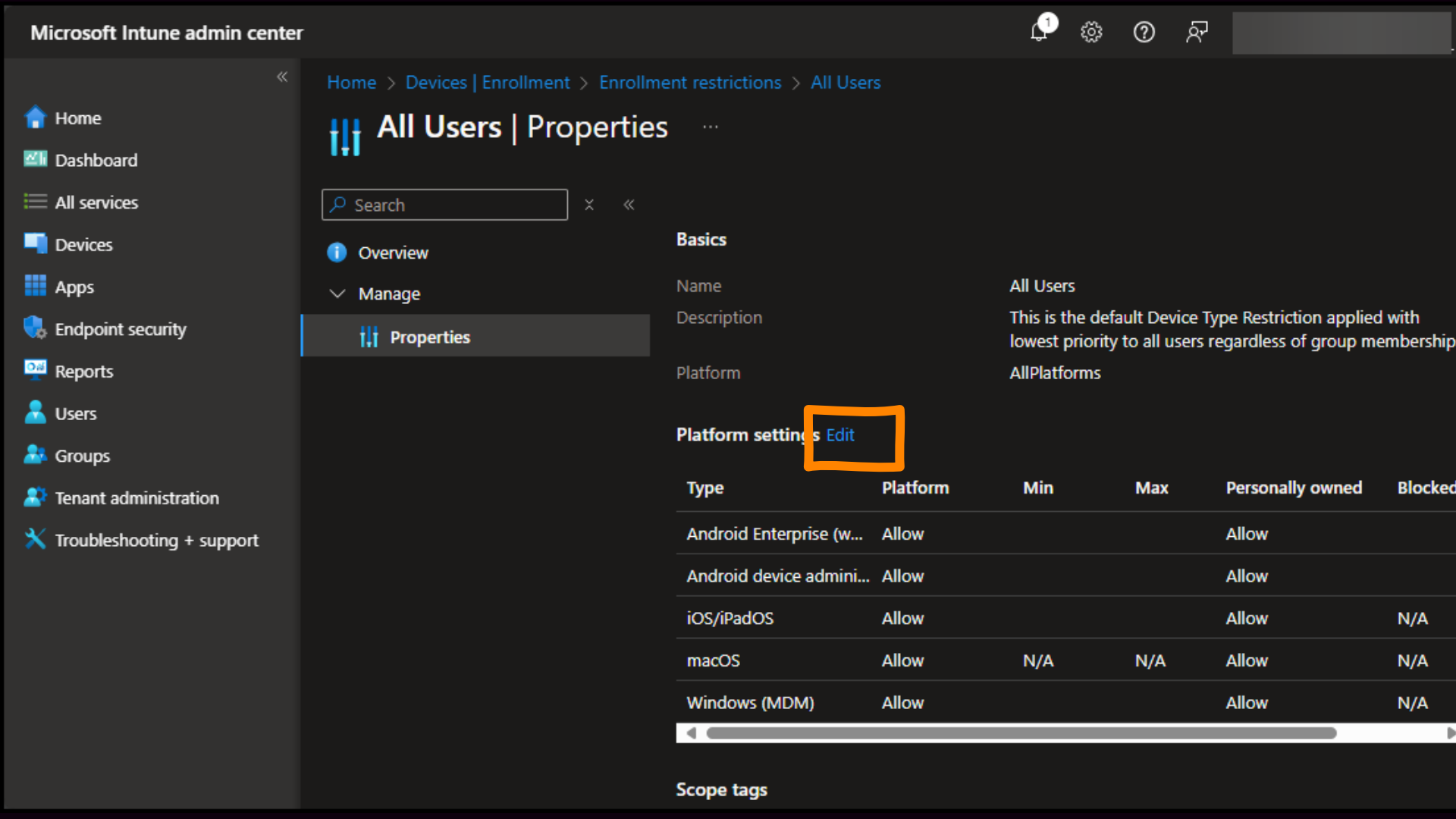

Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Search
Overview
All devices
Monitor
By platform
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates
Organize devices
Help and support
Windows
Apple
Android
Corporate device identifie
Learn about the different ways a Windows 10/11 PC can be enr
Search
Enrollment options
Automatic Enrollment
Configure Windows
Azure Active Direct
CNAME Validation
Test company doma
Co-management Settings
Configure co-mana
integration.
Device platform restriction
Configure which pla
Device limit restriction
Define how many d

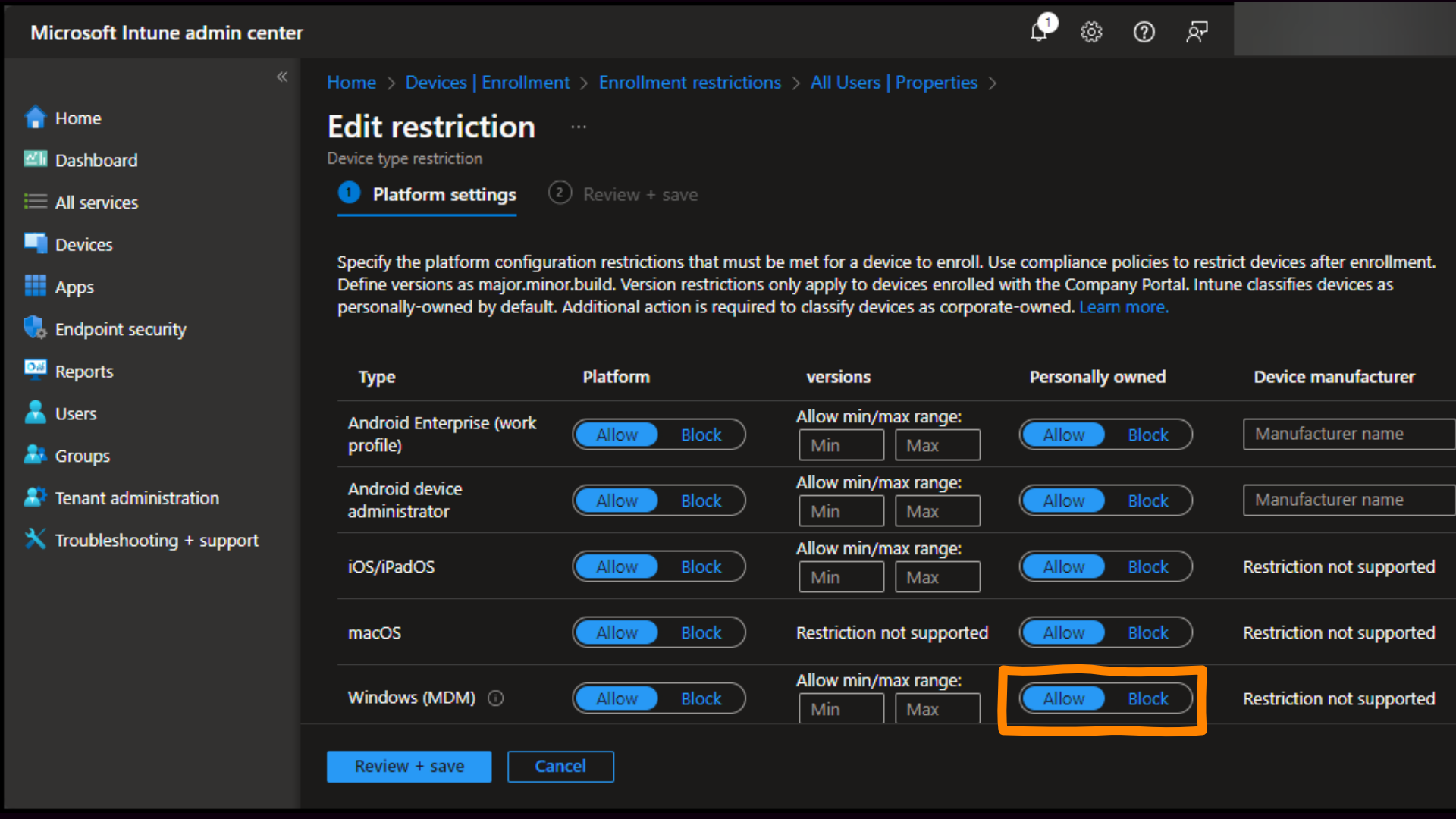

Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Device enrollment with Company Portal
Windows restrictions
Android restrictions
macOS restrictions
iOS restrictions
Create restriction
A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a devi
are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not del
Device type restrictions
Define which platforms, versions, and management types can enroll.
Priority
Name
Default
All Users

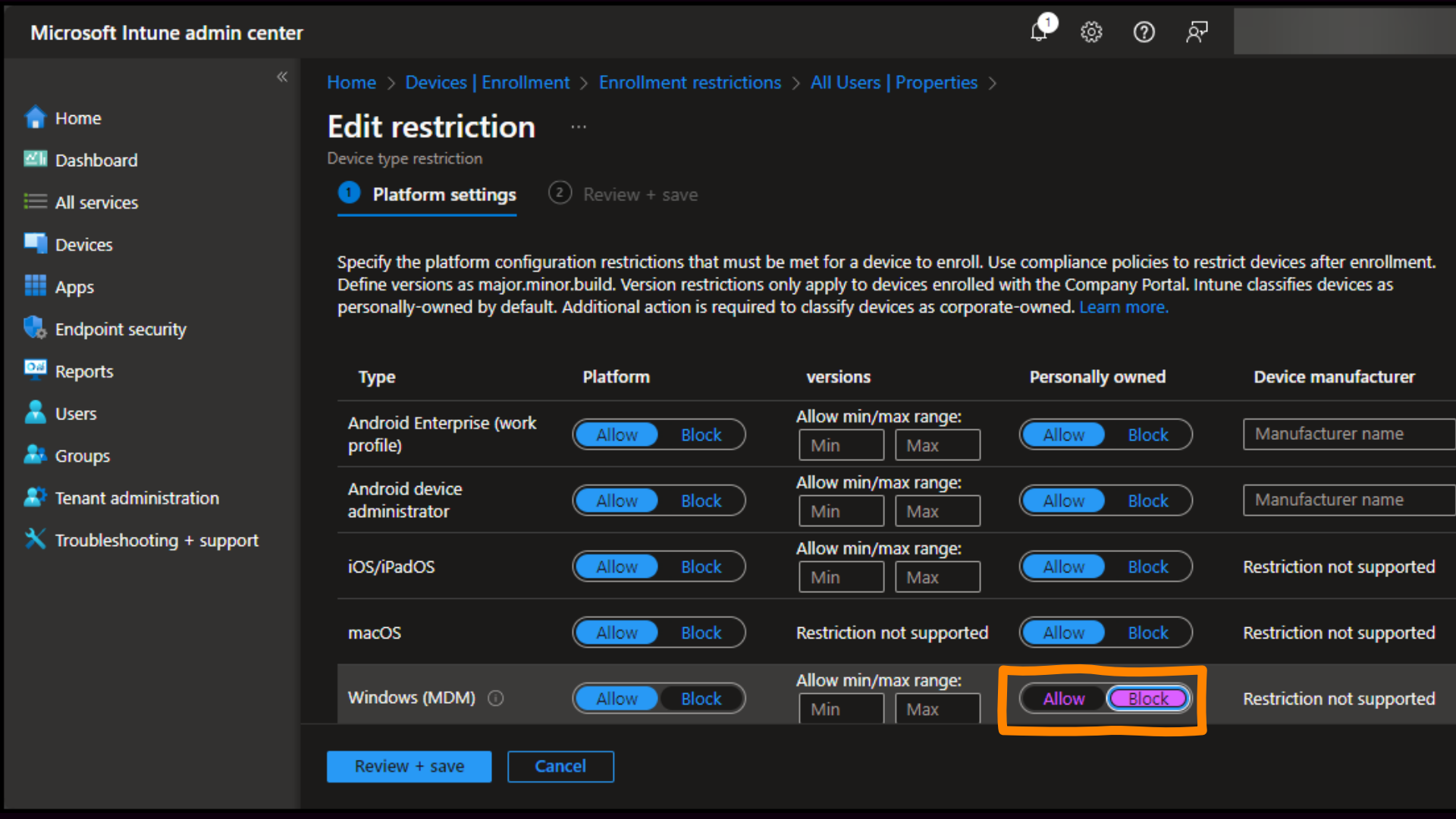

Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Device enrollment with Company Portal
Windows restrictions
Android restrictions
macOS restrictions
iOS restrictions
Create restriction
A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a devi
are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not del
Device type restrictions
Define which platforms, versions, and management types can enroll.
Priority
Name
Default
All Users

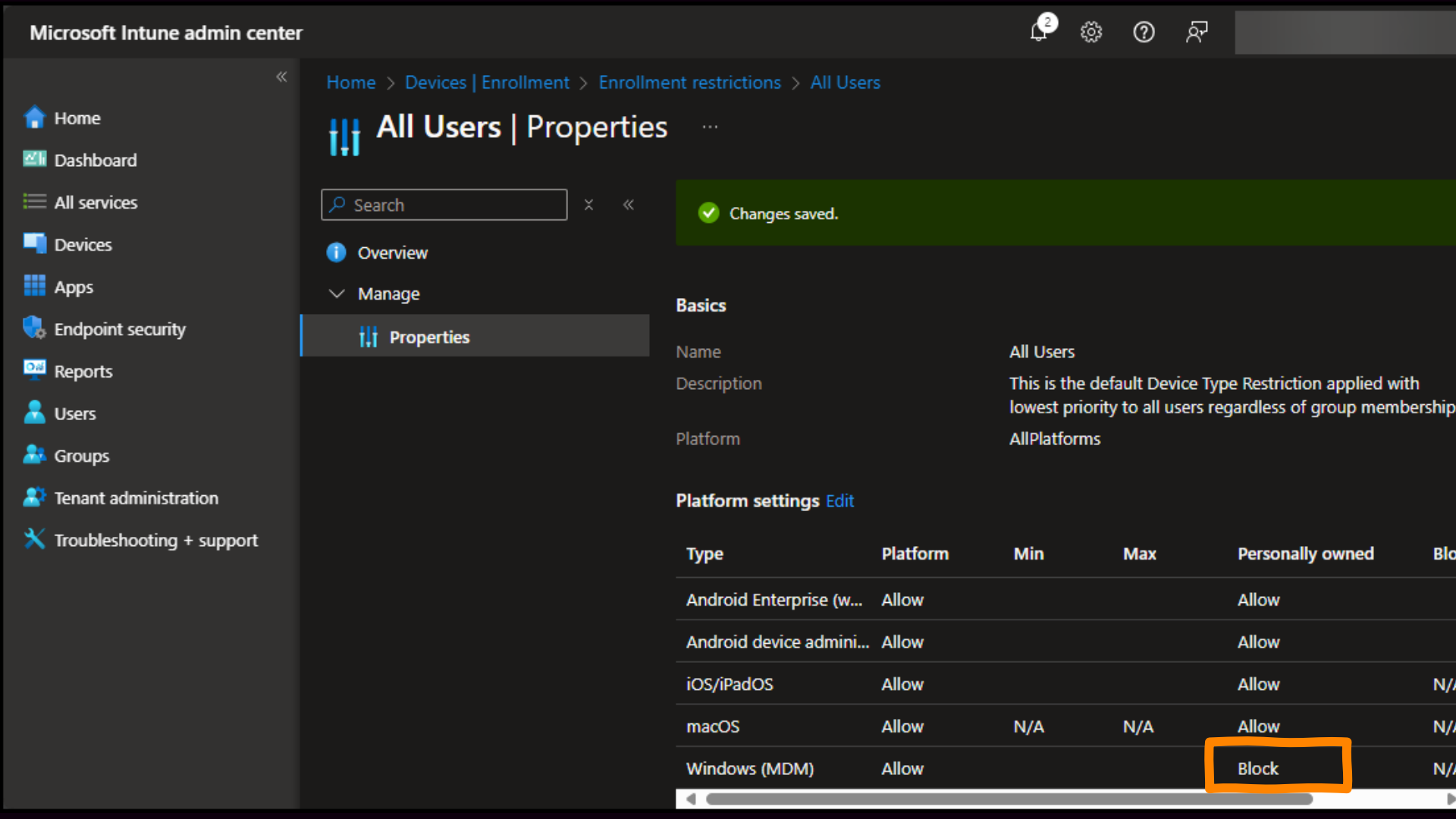

Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Device enrollment with Company Portal
Windows restrictions
Android restrictions
macOS restrictions
iOS restrictions
Create restriction
A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a devi
are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not del
Device type restrictions
Define which platforms, versions, and management types can enroll.
Priority
Name
Default
All Users


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Enrollment > Enrollment restrictions > All Users
All Users | Properties
Search
Overview
Manage
Properties
Basics
Name
All Users
Description
This is the default Device Type Restriction applied with lowest priority to all users regardless of group membership
Platform
AllPlatforms
Platform settings Edit
Type
Platform
Min
Max
Personally owned
Blocked
Android Enterprise (w...
Allow
Allow
Android device admini...
Allow
Allow
iOS/iPadOS
Allow
Allow
N/A
macOS
Allow
N/A
N/A
Allow
N/A
Windows (MDM)
Allow
Allow
N/A
Scope tags


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Enrollment > Enrollment restrictions > All Users
All Users | Properties
Search
Overview
Manage
Properties
Basics
Name
All Users
Description
This is the default Device Type Restriction applied with lowest priority to all users regardless of group membership
Platform
AllPlatforms
Platform settings Edit
Type
Platform
Min
Max
Personally owned
Blocked
Android Enterprise (w...
Allow
Allow
Android device admini...
Allow
Allow
iOS/iPadOS
Allow
Allow
N/A
macOS
Allow
N/A
N/A
Allow
N/A
Windows (MDM)
Allow
Allow
N/A
Scope tags


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Enrollment > Enrollment restrictions > All Users | Properties >
Edit restriction
Device type restriction
1 Platform settings
2 Review + save
Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more.
Type
Platform
versions
Personally owned
Device manufacturer
Android Enterprise (work profile)
Allow Block
Allow min/max range:
Min Max
Allow Block
Manufacturer name
Android device administrator
Allow Block
Allow min/max range:
Min Max
Allow Block
Manufacturer name
iOS/iPadOS
Allow Block
Allow min/max range:
Min Max
Allow Block
Restriction not supported
macOS
Allow Block
Restriction not supported
Allow Block
Restriction not supported
Windows (MDM)
Allow Block
Allow min/max range:
Min Max
Allow Block
Restriction not supported
Review + save
Cancel


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Enrollment > Enrollment restrictions > All Users | Properties >
Edit restriction
Device type restriction
1 Platform settings
2 Review + save
Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more.
Type
Platform
versions
Personally owned
Device manufacturer
Android Enterprise (work profile)
Allow Block
Allow min/max range:
Min Max
Allow Block
Manufacturer name
Android device administrator
Allow Block
Allow min/max range:
Min Max
Allow Block
Manufacturer name
iOS/iPadOS
Allow Block
Allow min/max range:
Min Max
Allow Block
Restriction not supported
macOS
Allow Block
Restriction not supported
Allow Block
Restriction not supported
Windows (MDM)
Allow Block
Allow min/max range:
Min Max
Allow Block
Restriction not supported
Review + save
Cancel


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Enrollment > Enrollment restrictions > All Users
All Users | Properties
Search
Overview
Manage
Properties
Changes saved.
Basics
Name
All Users
Description
This is the default Device Type Restriction applied with lowest priority to all users regardless of group membership
Platform
AllPlatforms
Platform settings Edit
Type
Platform
Min
Max
Personally owned
Android Enterprise (w...
Allow
Allow
Android device admini...
Allow
Allow
iOS/iPadOS
Allow
Allow
macOS
Allow
N/A
N/A
Allow
Windows (MDM)
Allow
Block

3

How?

Can we know,
and trust
our devices?

NIC
EMPOWER

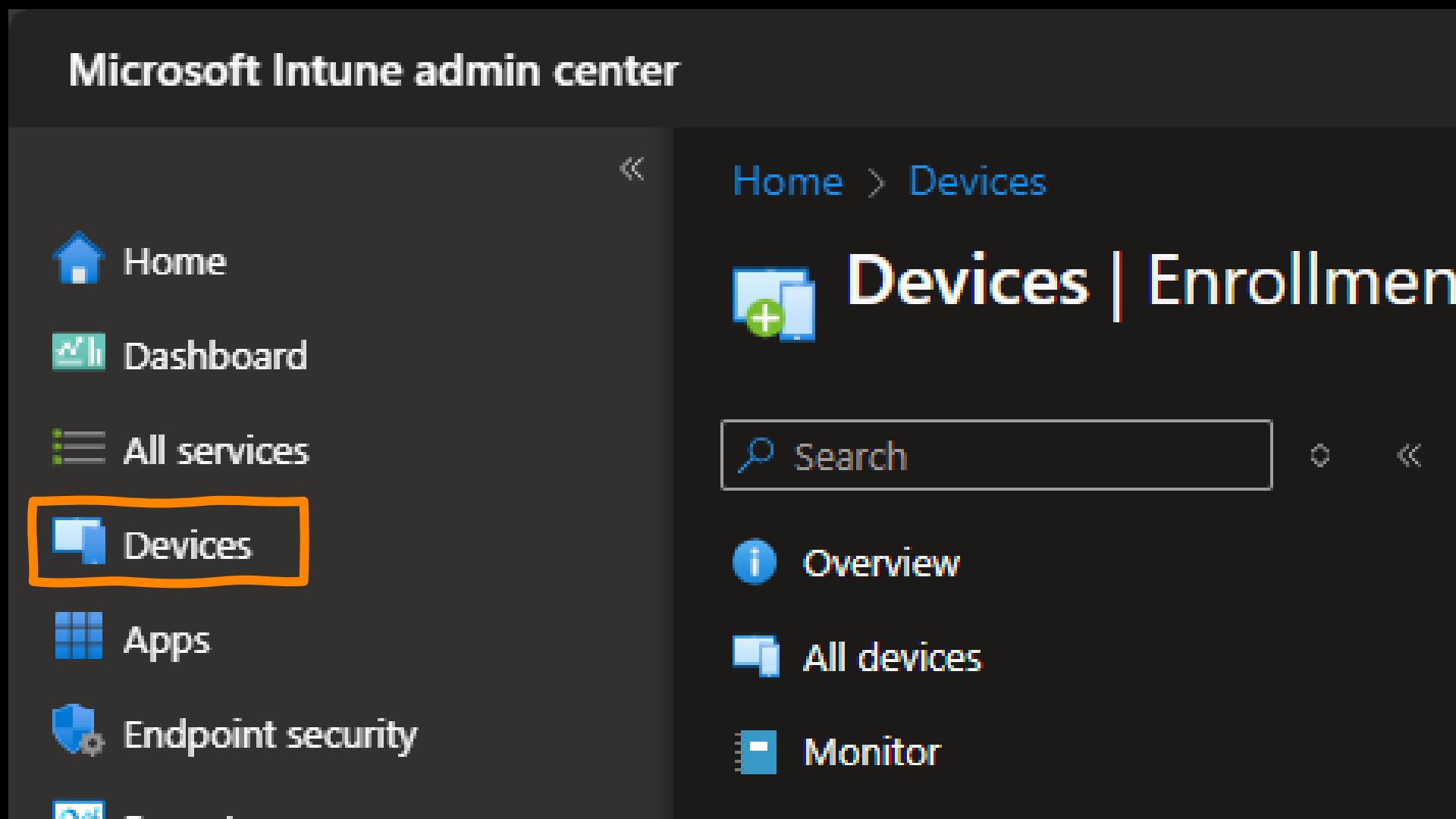
4

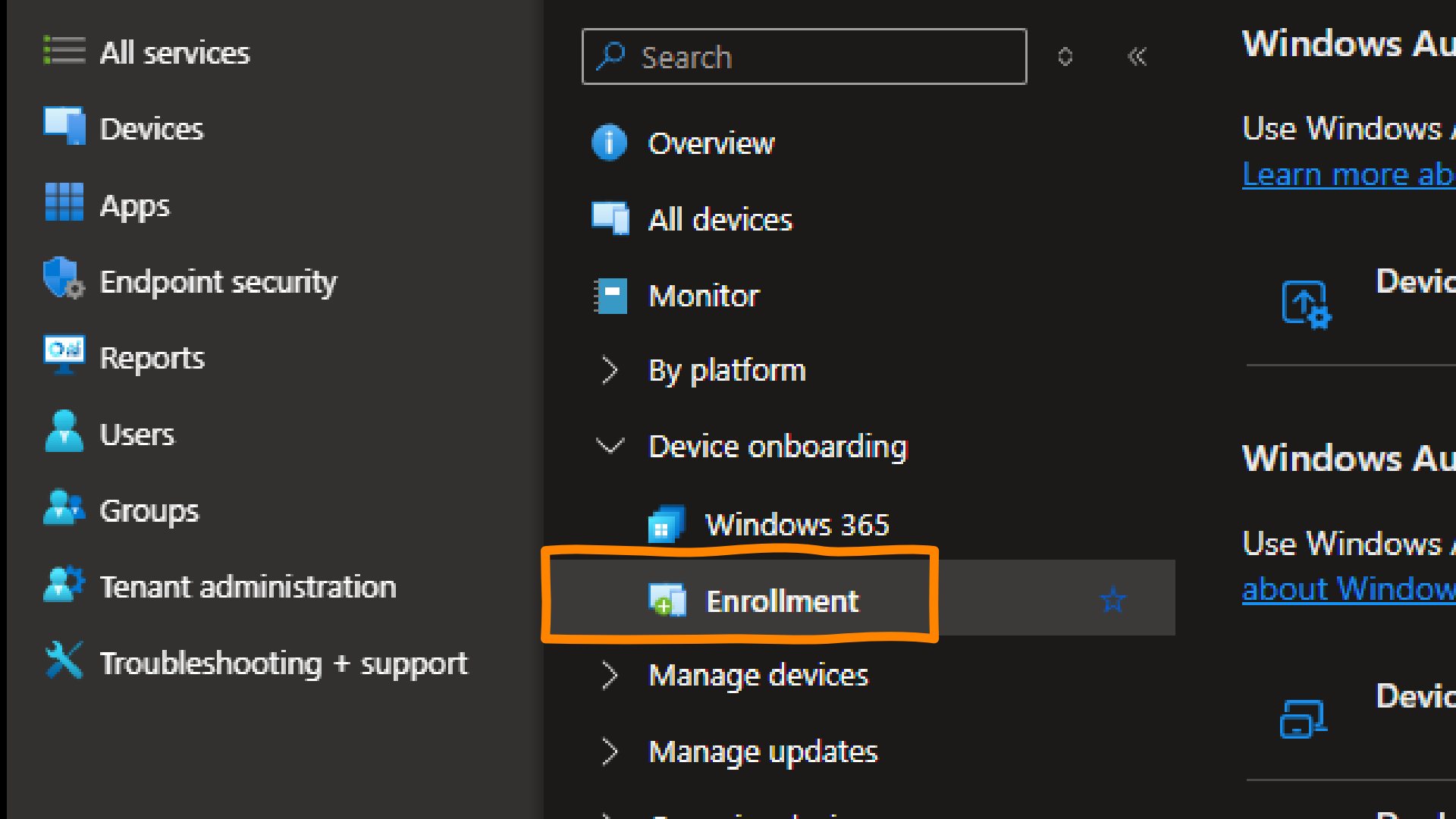
How?

Can we know,
and trust
our devices?

Windows Autopilot

NIC
EMPOWER


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Home > Devices
Devices | Enrollmen
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 Au
Use Windows
Learn more ab
Devic
Windows Au
Use Windows
about Windo
Devic

Windows Autopilot device preparation

Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting experience
Learn more about Windows Autopilot device preparation

Device preparation policies Configure devices for initial provisioning.

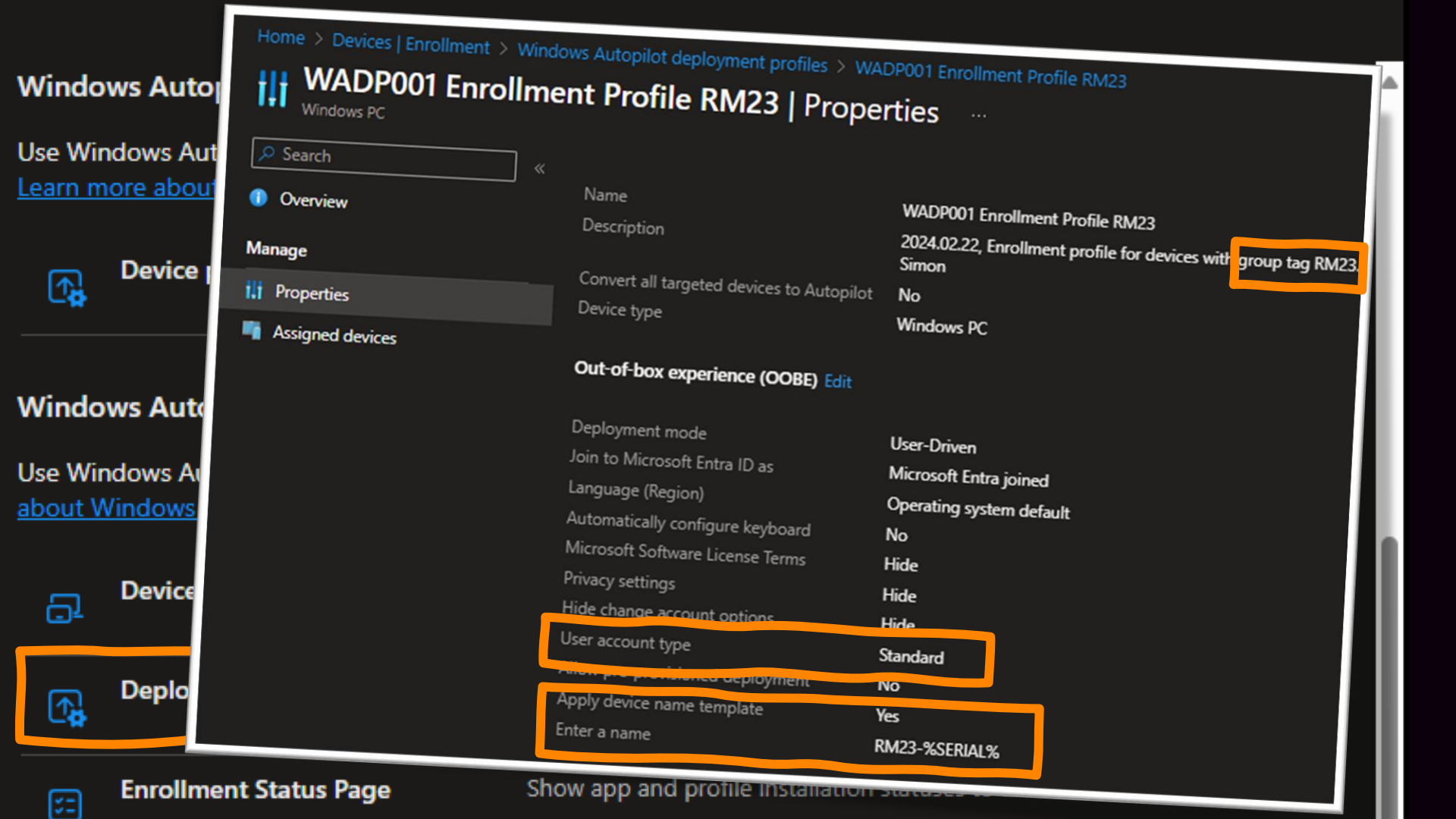
Windows Autopilot

Use Windows Autopilot to customize the Windows onboarding out of box experience and workflow. Learn more about Windows Autopilot

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 Autop
Use Windows Aut
Learn more about
Device
Windows Auto
Use Windows Au
about Windows
Device
Deplo
Enrollment Status Page
Show app and profile installation
Home > Devices | Enrollment > Windows Autopilot deployment profiles > WADP001 Enrollment Profile RM23
WADP001 Enrollment Profile RM23 | Properties
Windows PC
Search
Overview
Manage
Properties
Assigned devices
Name
WADP001 Enrollment Profile RM23
Description
2024.02.22, Enrollment profile for devices with group tag RM23.
Simon
Convert all targeted devices to Autopilot
No
Device type
Windows PC
Out-of-box experience (OOBE) Edit
Deployment mode
User-Driven
Join to Microsoft Entra ID as
Microsoft Entra joined
Language (Region)
Operating system default
Automatically configure keyboard
No
Microsoft Software License Terms
Hide
Privacy settings
Hide
Hide change account options
Hide
User account type
Standard
No
Apply device name template
Yes
Enter a name
RM23-%SERIAL%

Windows Autopilot device preparation

Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting experie
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. Learn mor
about Windows Autopilot

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

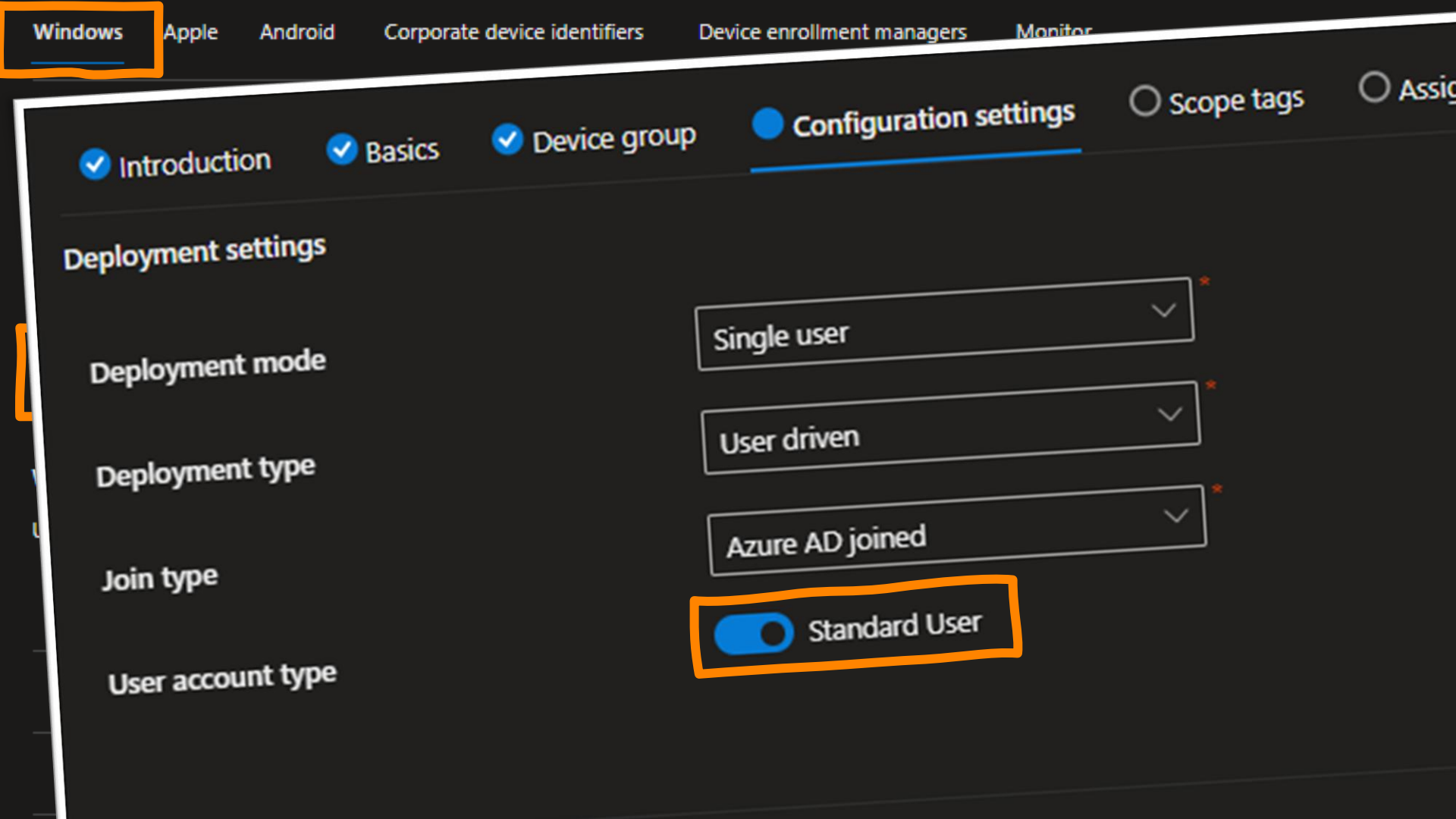
Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting experiences. Learn more about Windows Autopilot device preparation

Device preparation policies	Configure devices for initial provisioning.

Windows Autopilot

Use Windows Autopilot to customize the Windows onboarding out of box experience and workflow. Learn more about Windows Autopilot

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
Monitor
Introduction
Basics
Device group
Configuration settings
Scope tags
Assig
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
EMPOWER

4

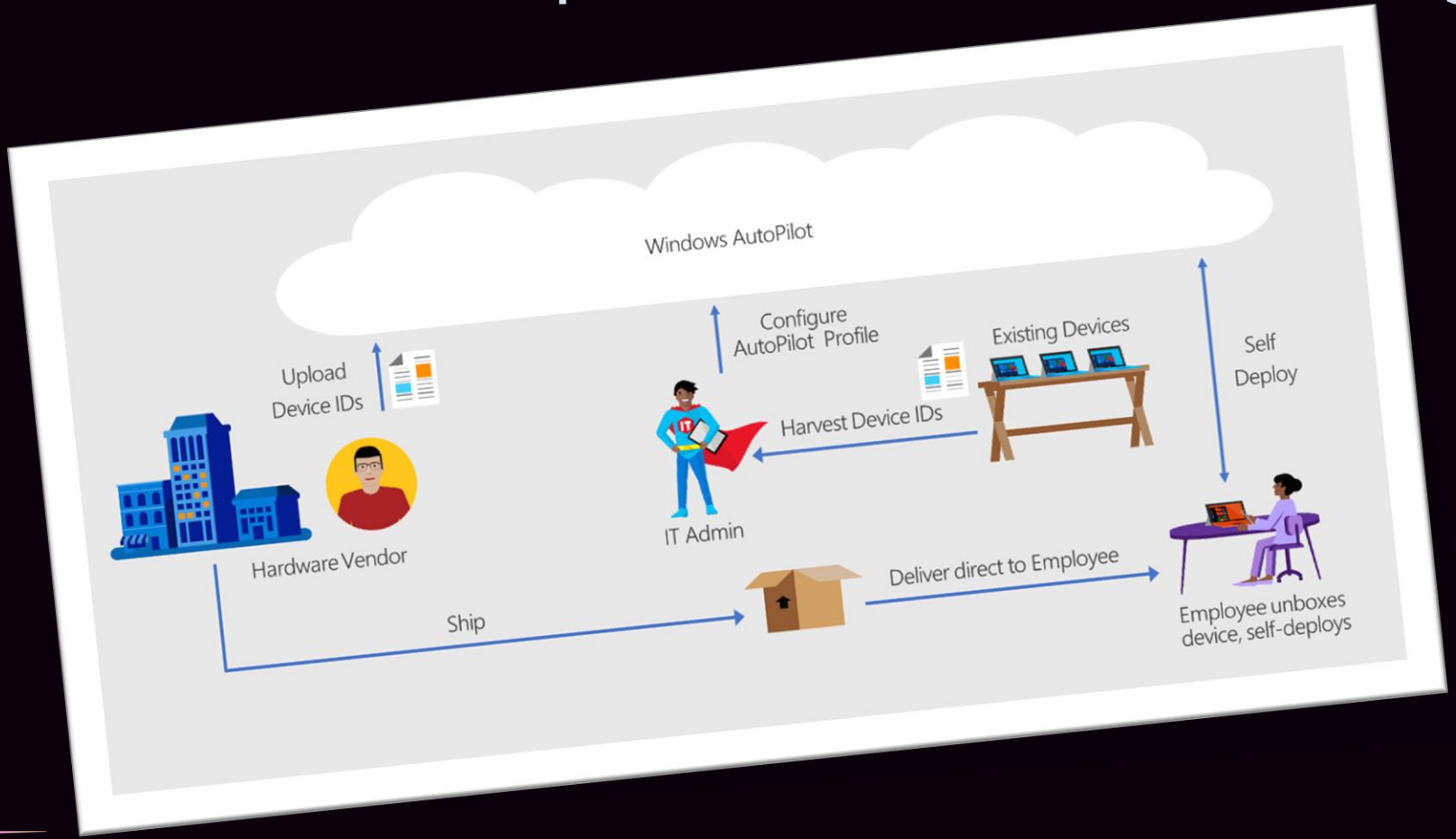
How?

Can we know,
and trust
our devices?

Windows Autopilot Device Onboarding

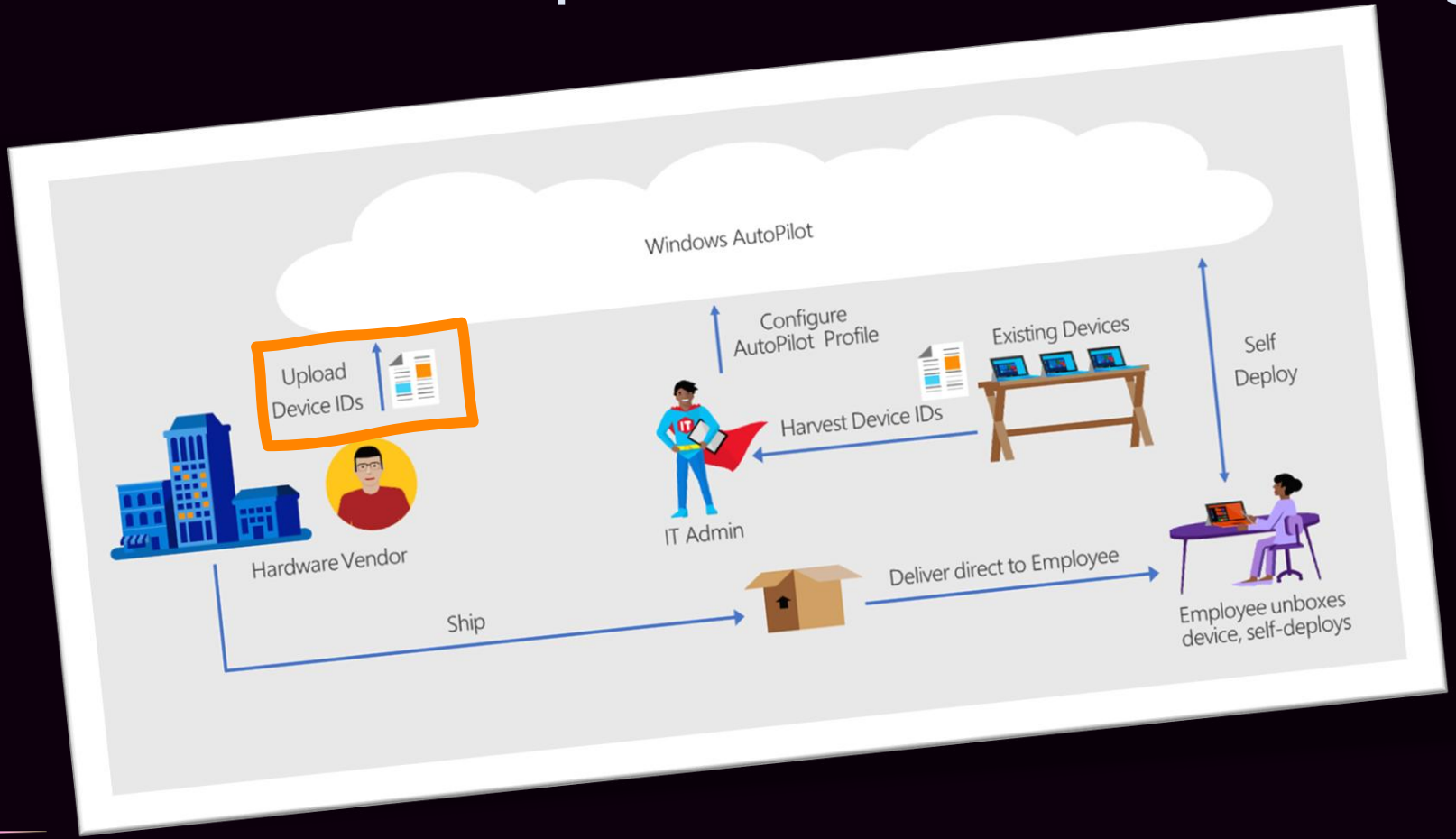
NIC
EMPOWER

Windows Autopilot Device Onboarding



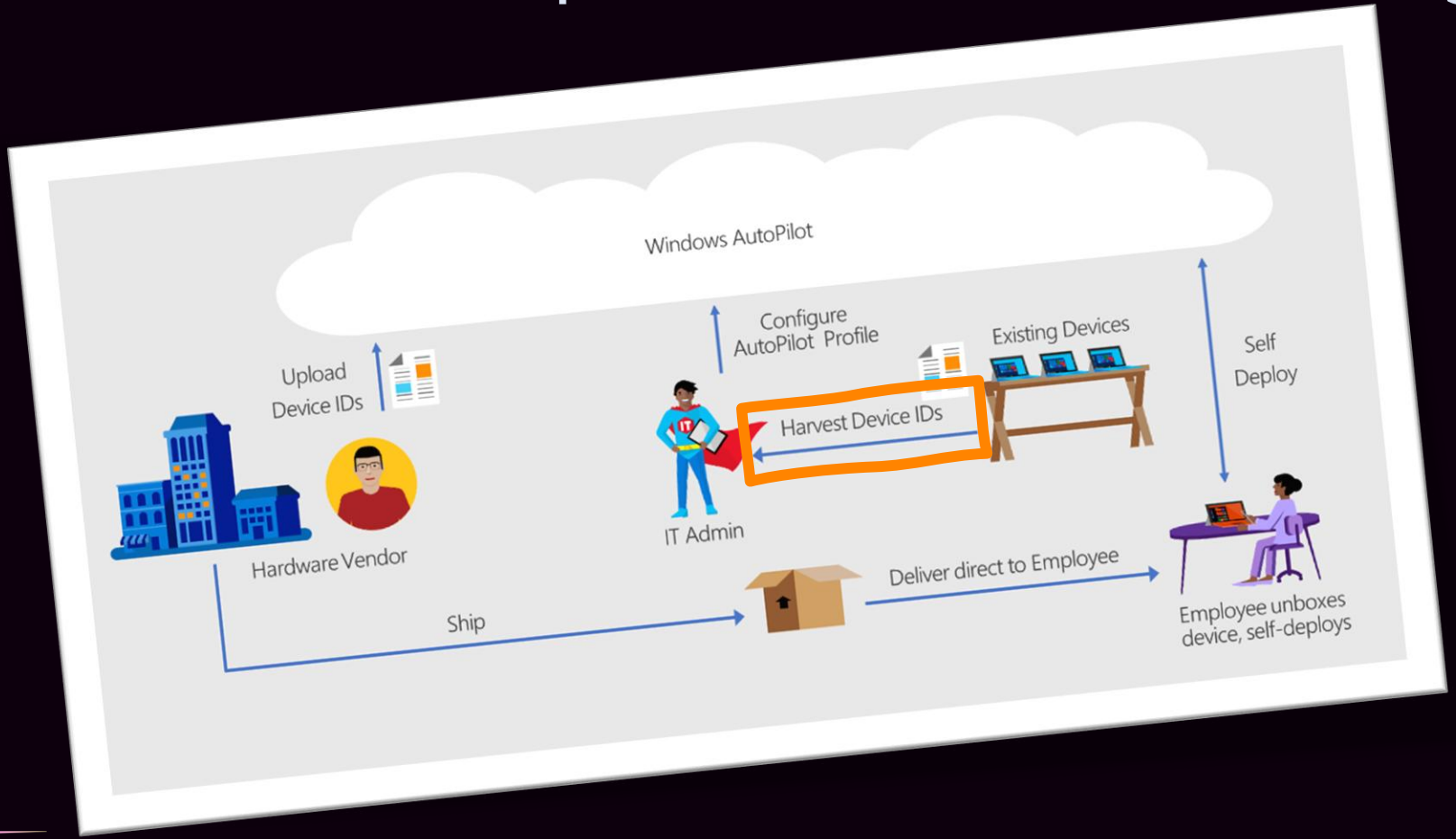
NIC
EMPOWER

Windows Autopilot Device Onboarding



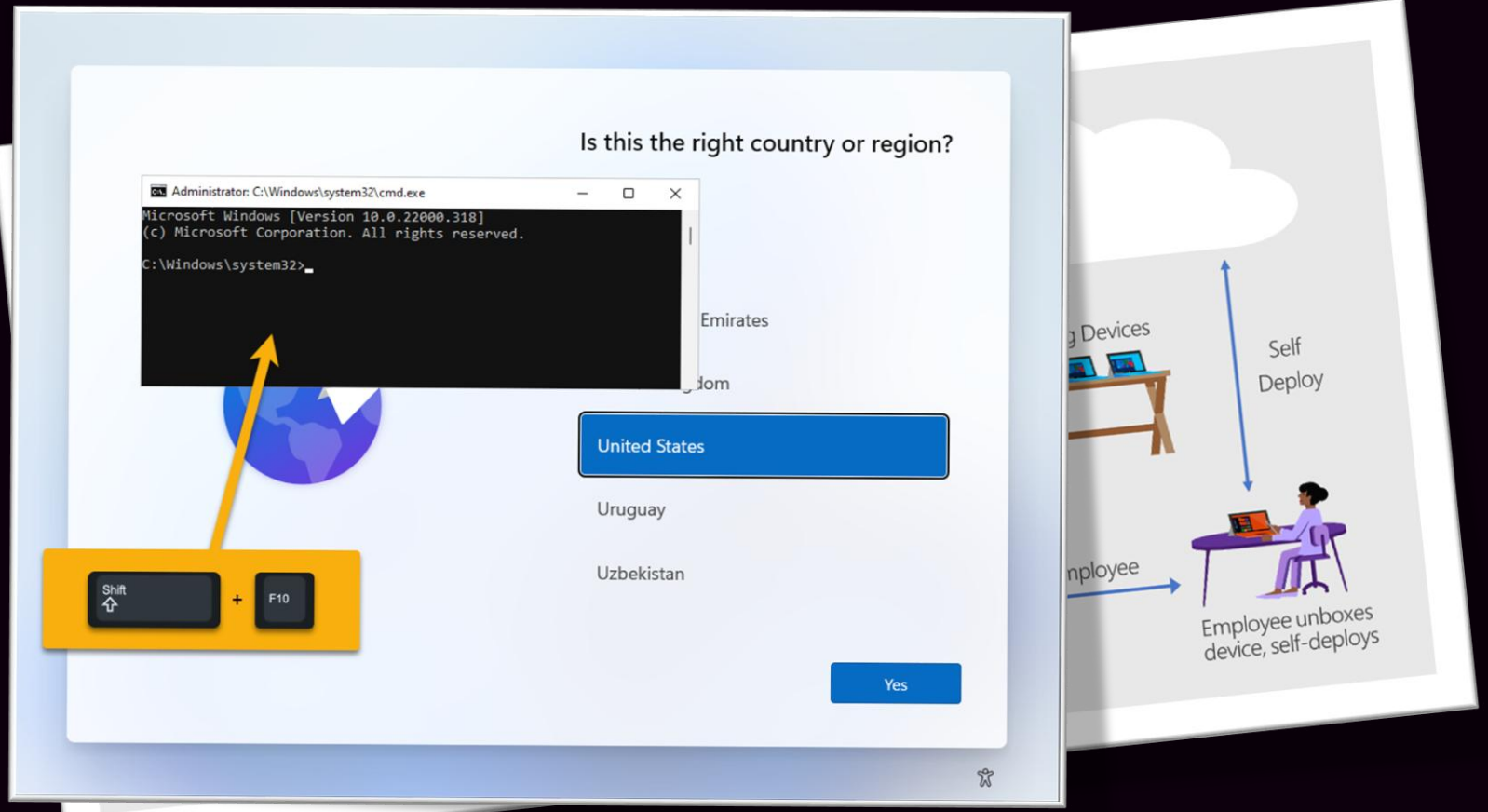
NIC
EMPOWER

Windows Autopilot Device Onboarding



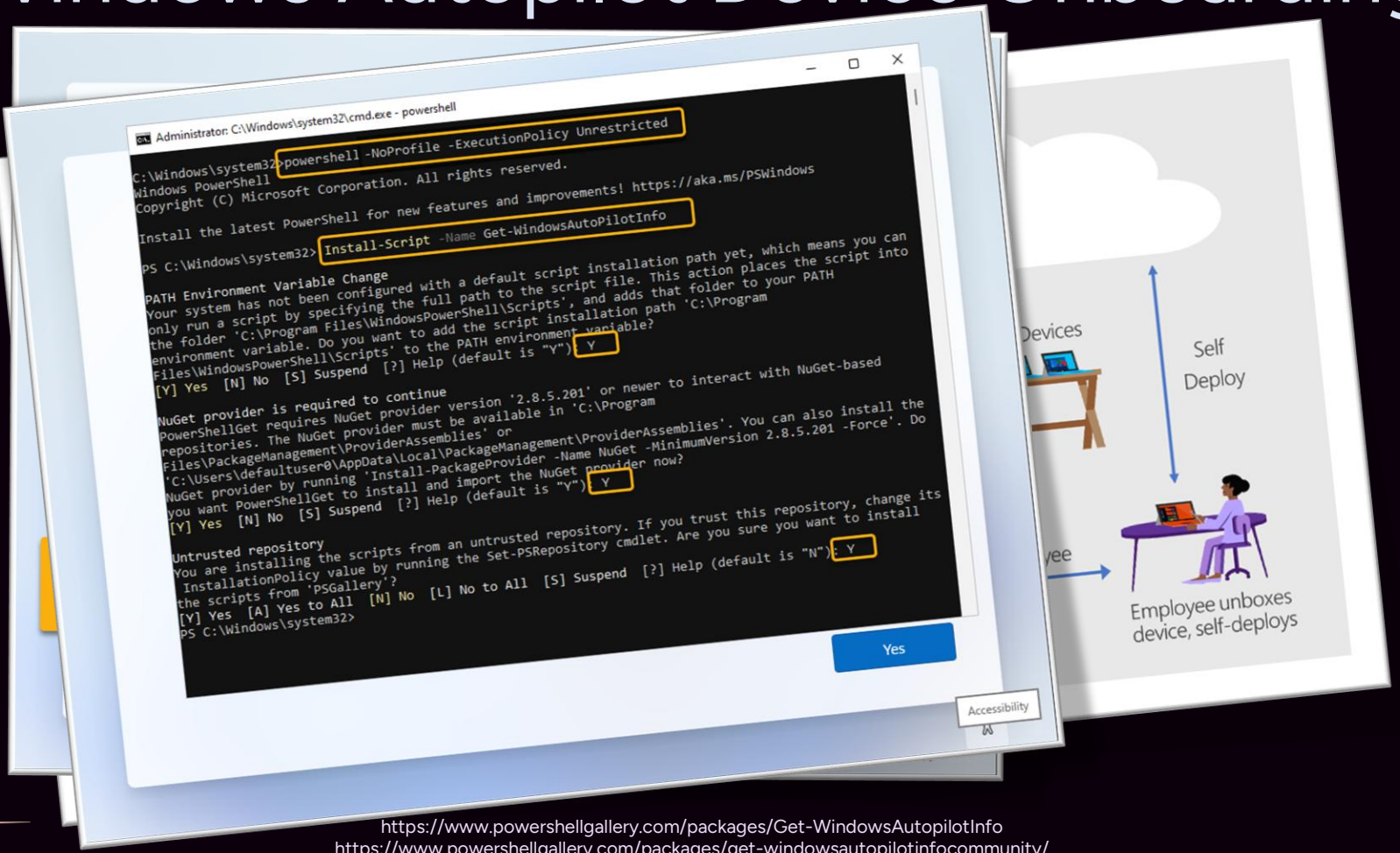
NIC
EMPOWER

Windows Autopilot Device Onboarding



NIC
EMPOWER

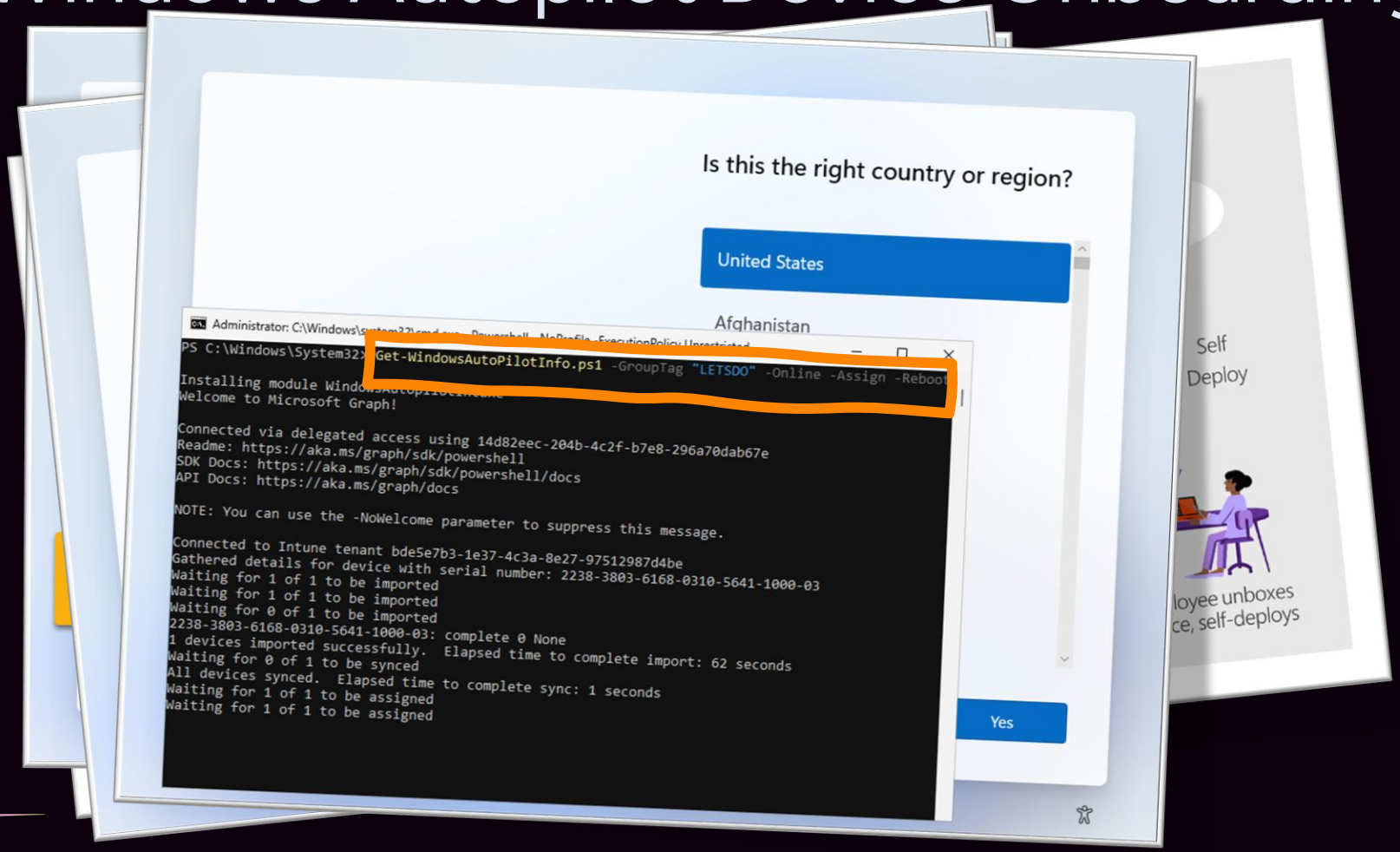
Windows Autopilot Device Onboarding



https://www.powershellgallery.com/packages/Get-WindowsAutopilotInfo
https://www.powershellgallery.com/packages/get-windowsautopilotinfocommunity/

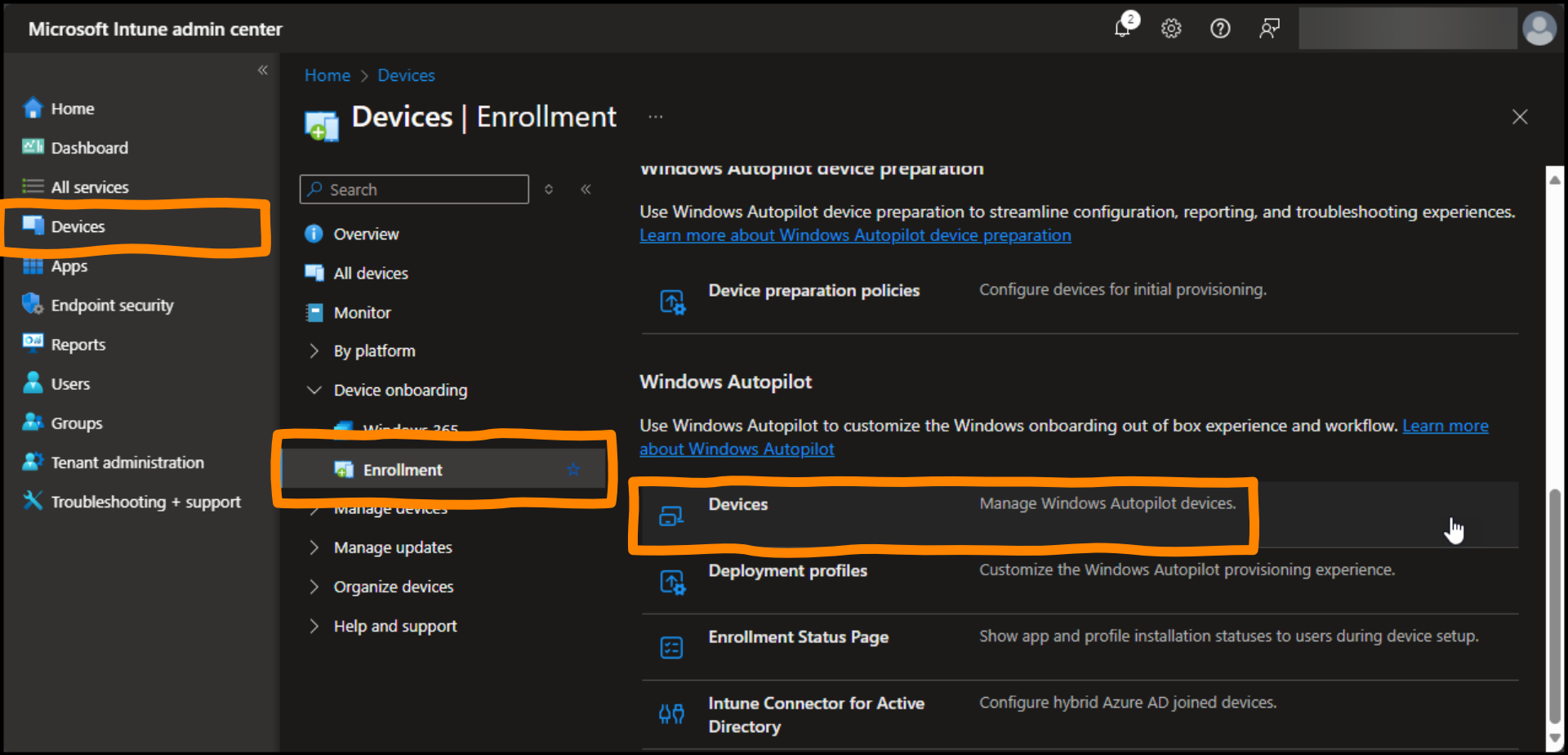
NIC EMPOWER

Windows Autopilot Device Onboarding

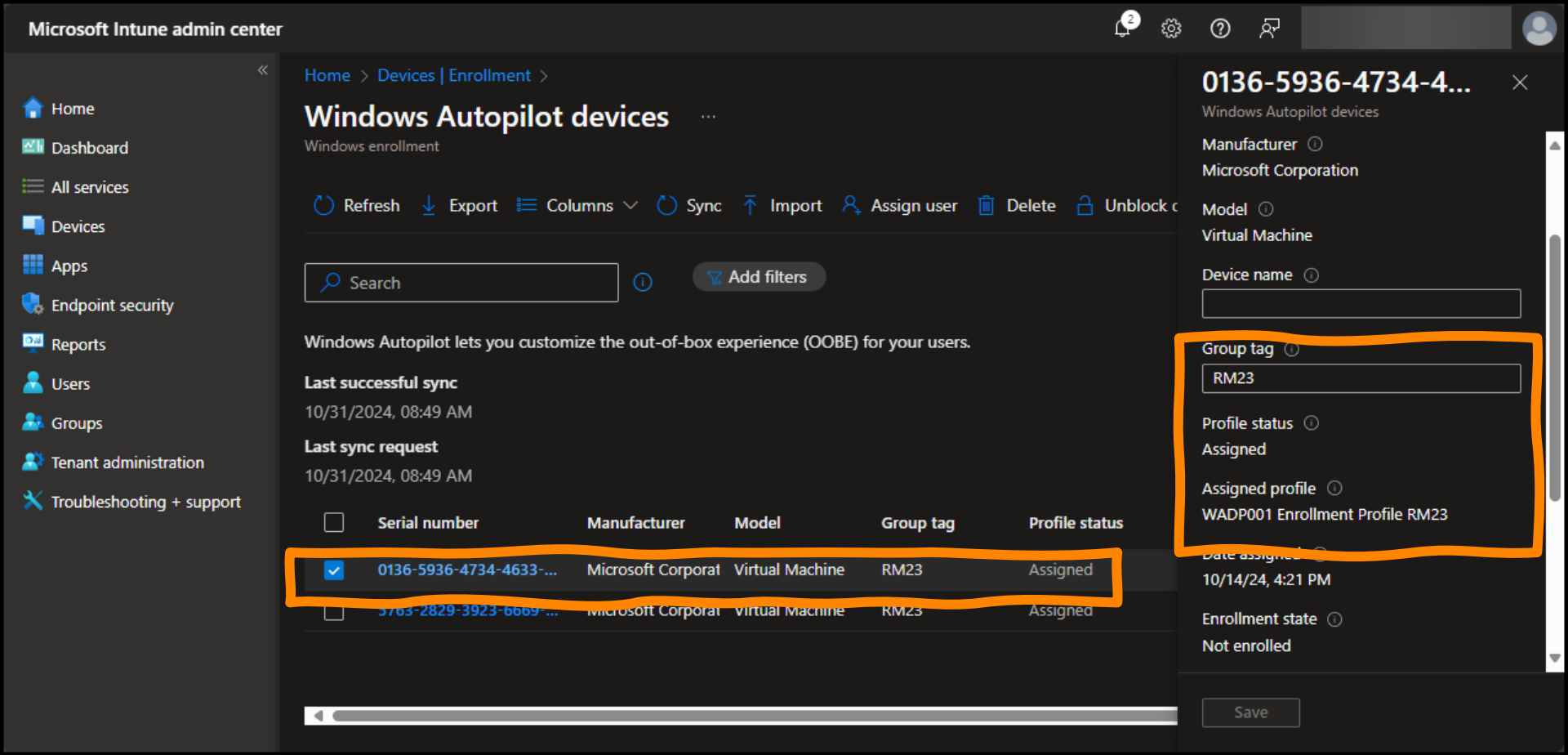


NIC
EMPOWER

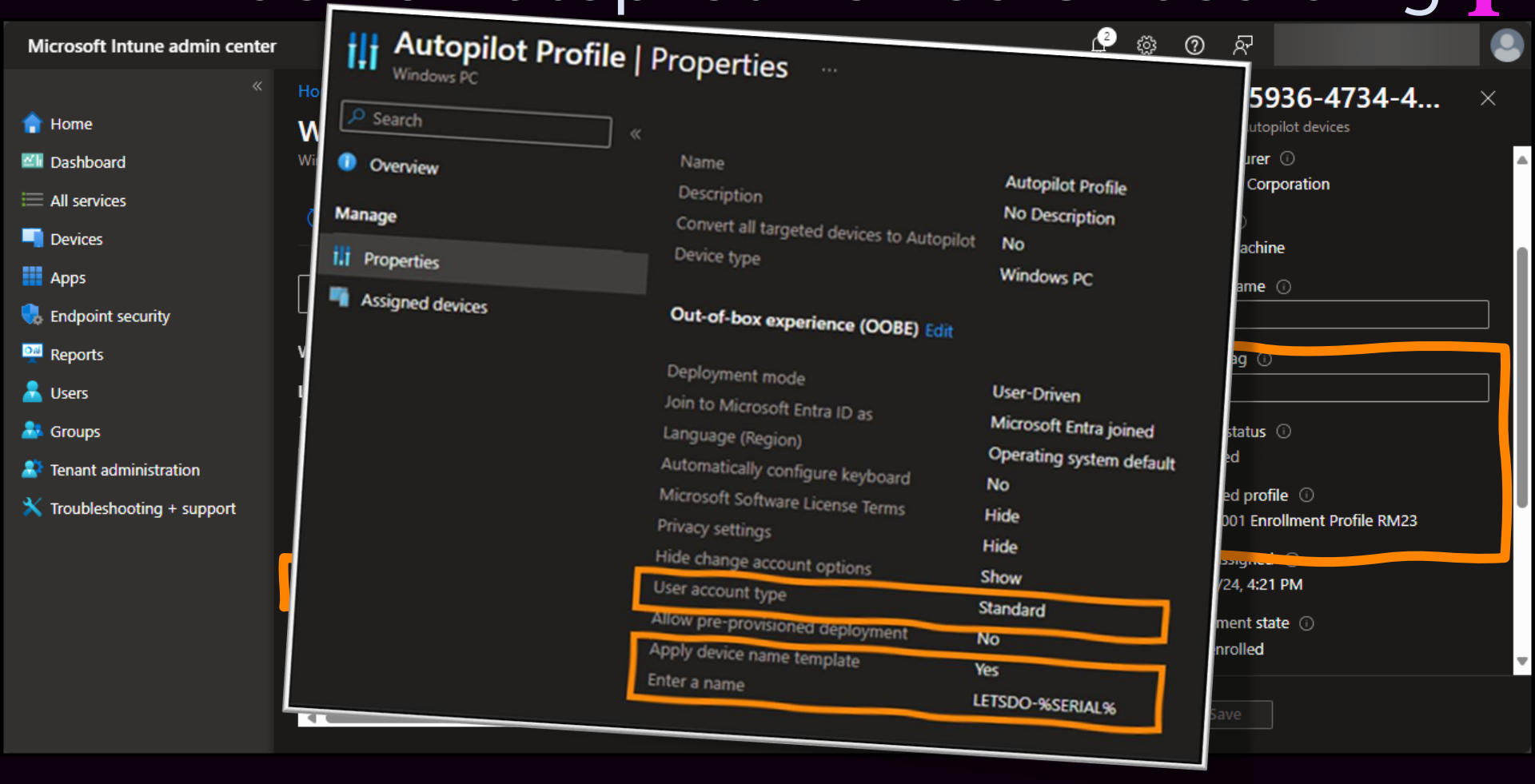
Windows Autopilot Device Onboarding I



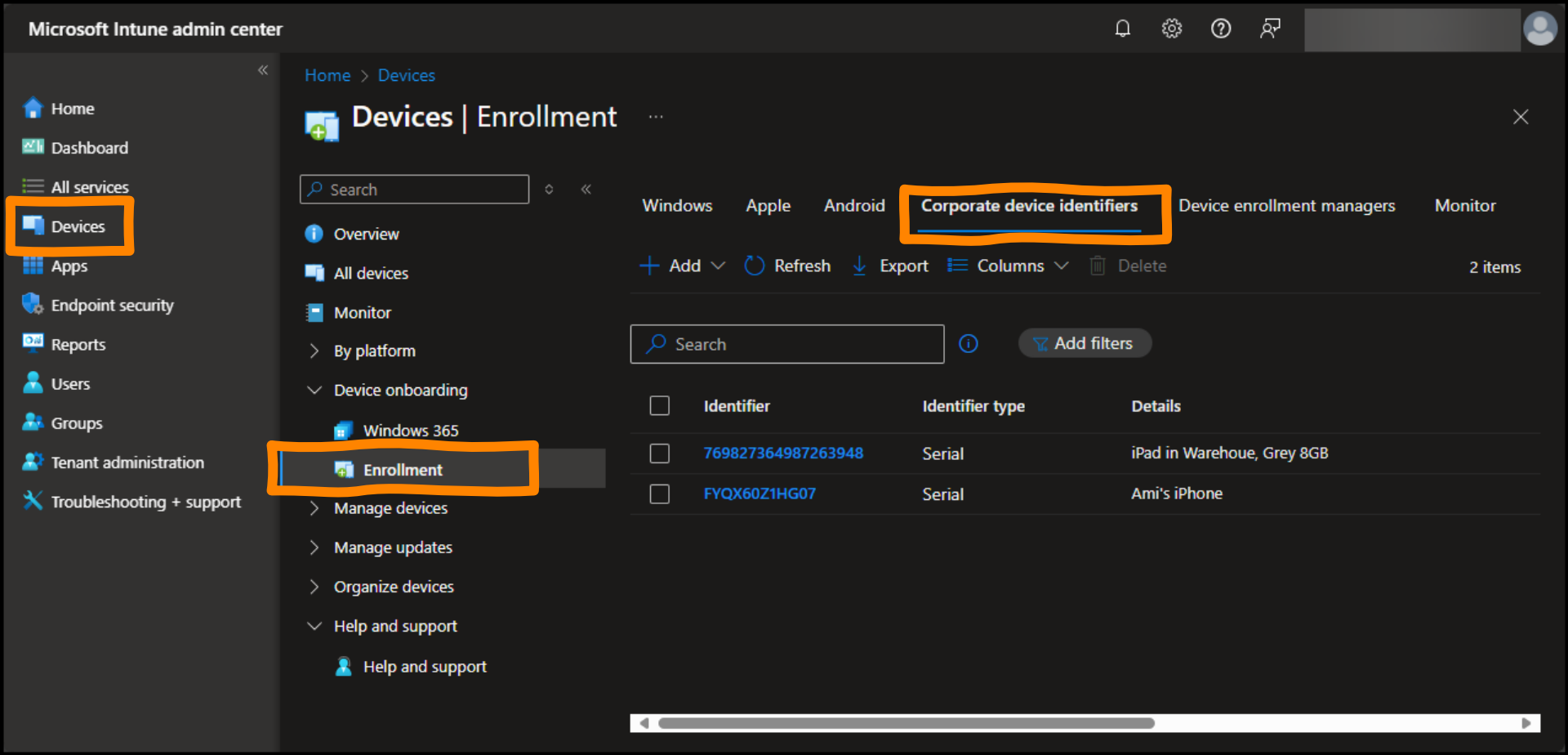
Windows Autopilot Device Onboarding I



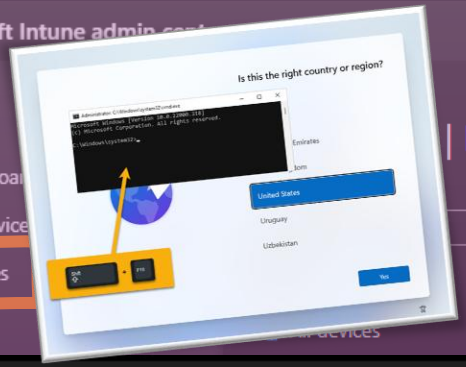
Windows Autopilot Device Onboarding I



Windows Autopilot Device Onboarding II



Windows Autopilot Device Onboarding II



Microsoft Intune admin

Home
Dashboard
All services
Devices
Apps

| Enrollment

Windows | Apple | Android | Corporate device identifiers | Device enrollment managers | Monitor

Add | Refresh | Export | Columns | Delete | 2 items

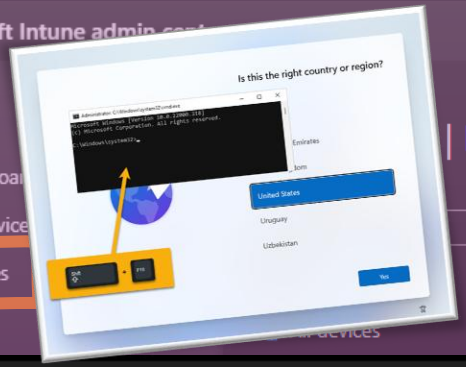
```
(Get-CimInstance Win32_ComputerSystem).Manufacturer+','+(Get-CimInstance Win32_ComputerSystem).Model+','+(Get-CimInstance Win32_BIOS).SerialNumber
```

Groups
Tenant administration
Troubleshooting + support

Windows 365
Enrollment
Manage devices
Manage updates
Organize devices
Help and support
Help and support

Identifier	Identifier type	Details
769827364987263948	Serial	iPad in Warehoue, Grey 8GB
FYQX60Z1HG07	Serial	Ami's iPhone

Windows Autopilot Device Onboarding II



Microsoft Intune admin

Home
Dashboard
All services
Devices
Apps

| Enrollment

Windows | Apple | Android | Corporate device identifiers | Device enrollment managers | Monitor

Add | Refresh | Export | Columns | Delete | 2 items

```
(Get-CimInstance Win32_ComputerSystem).Manufacturer+','+(Get-CimInstance Win32_ComputerSystem).Model+','+(Get-CimInstance Win32_BIOS).SerialNumber
```

Groups
Tenant administration
Troubleshooting + support

Windows 365
Enrollment
Manage devices
Manage updates
Organize devices
Help and support
Help and support

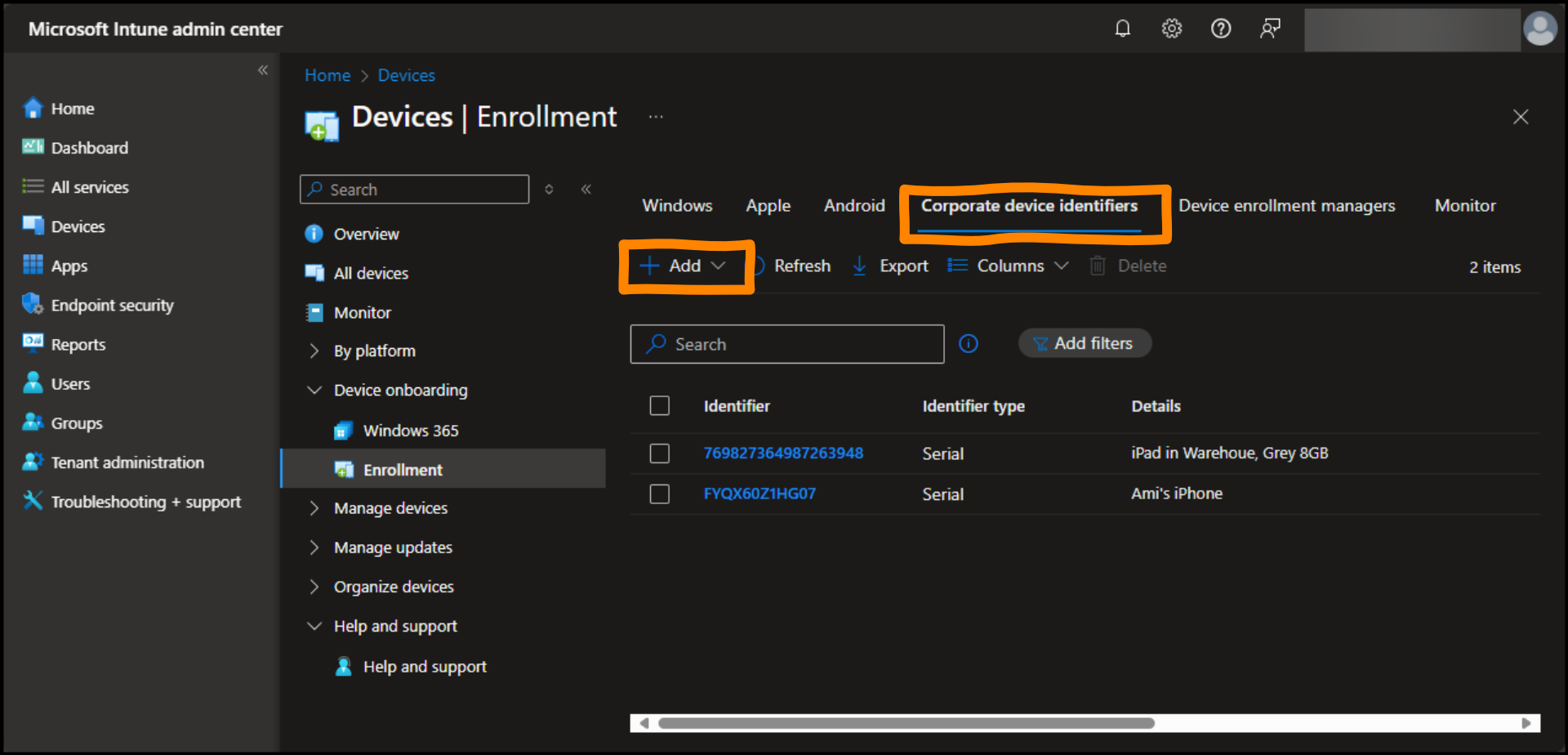
systeminfo.csv

File Edit View

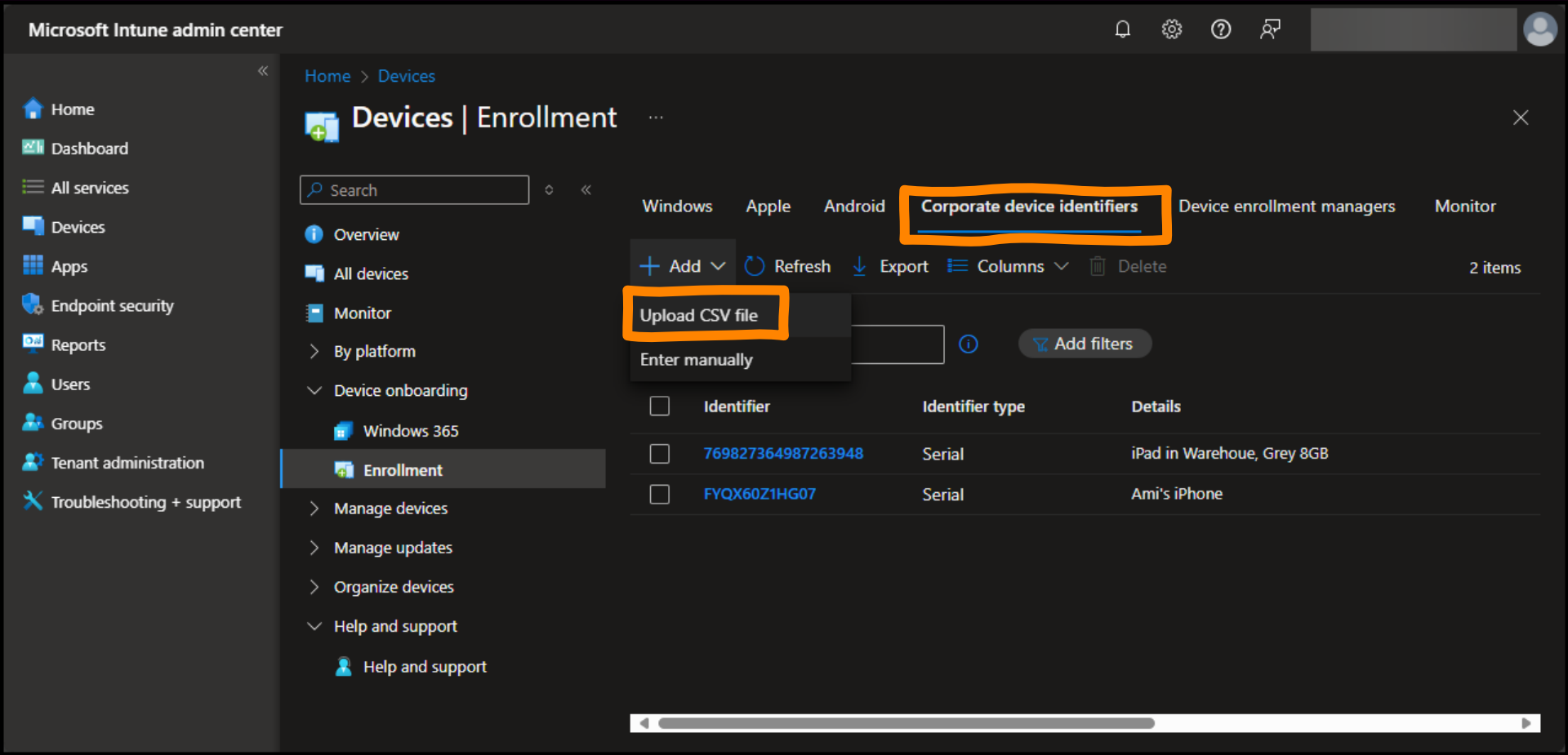
Microsoft Corporation,Surface Laptop Studio,0F[redacted]

Ln 1, Col 59 | 58 characters | 100% | Windows (CRLF) | UTF-8

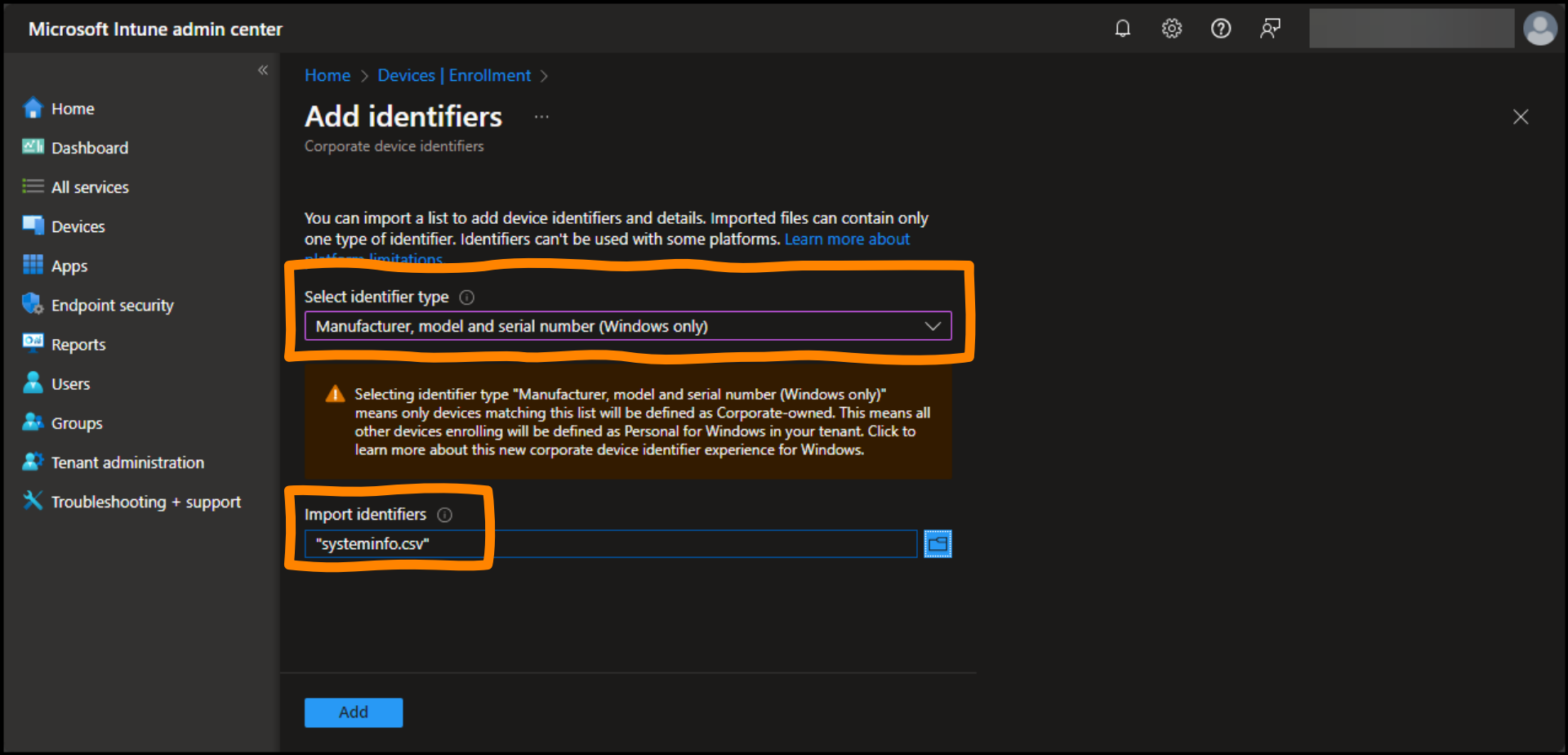
Windows Autopilot Device Onboarding II



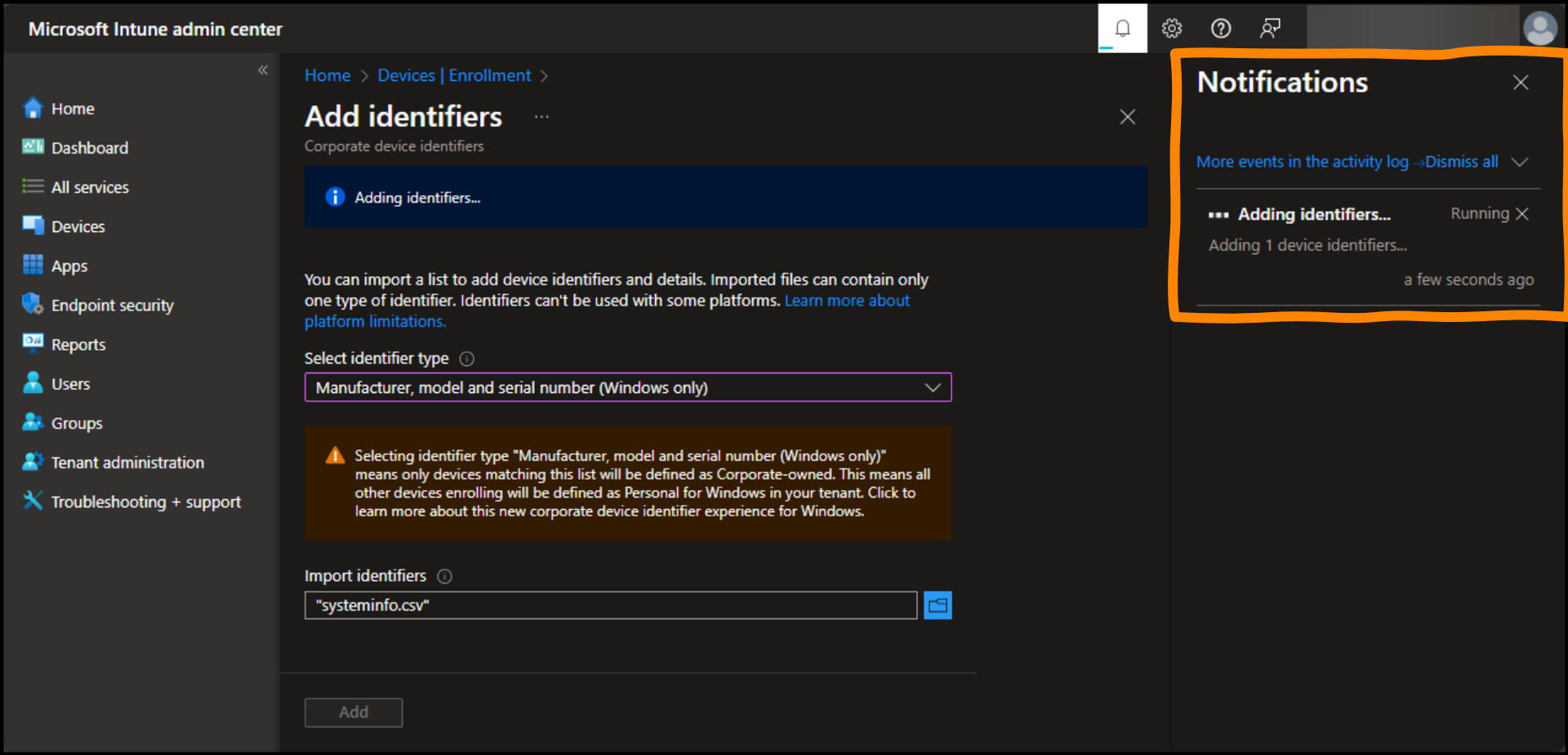
Windows Autopilot Device Onboarding II



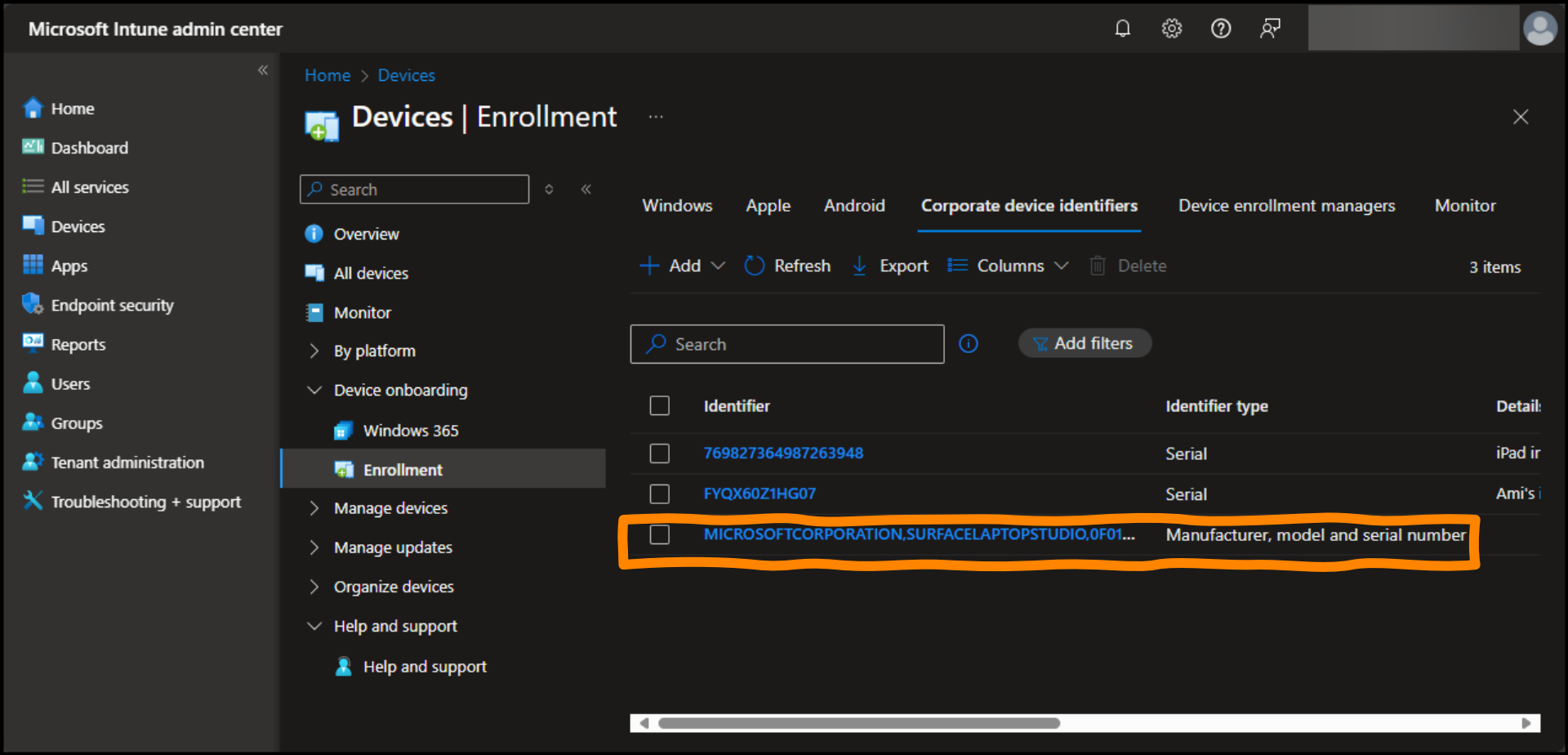
Windows Autopilot Device Onboarding II



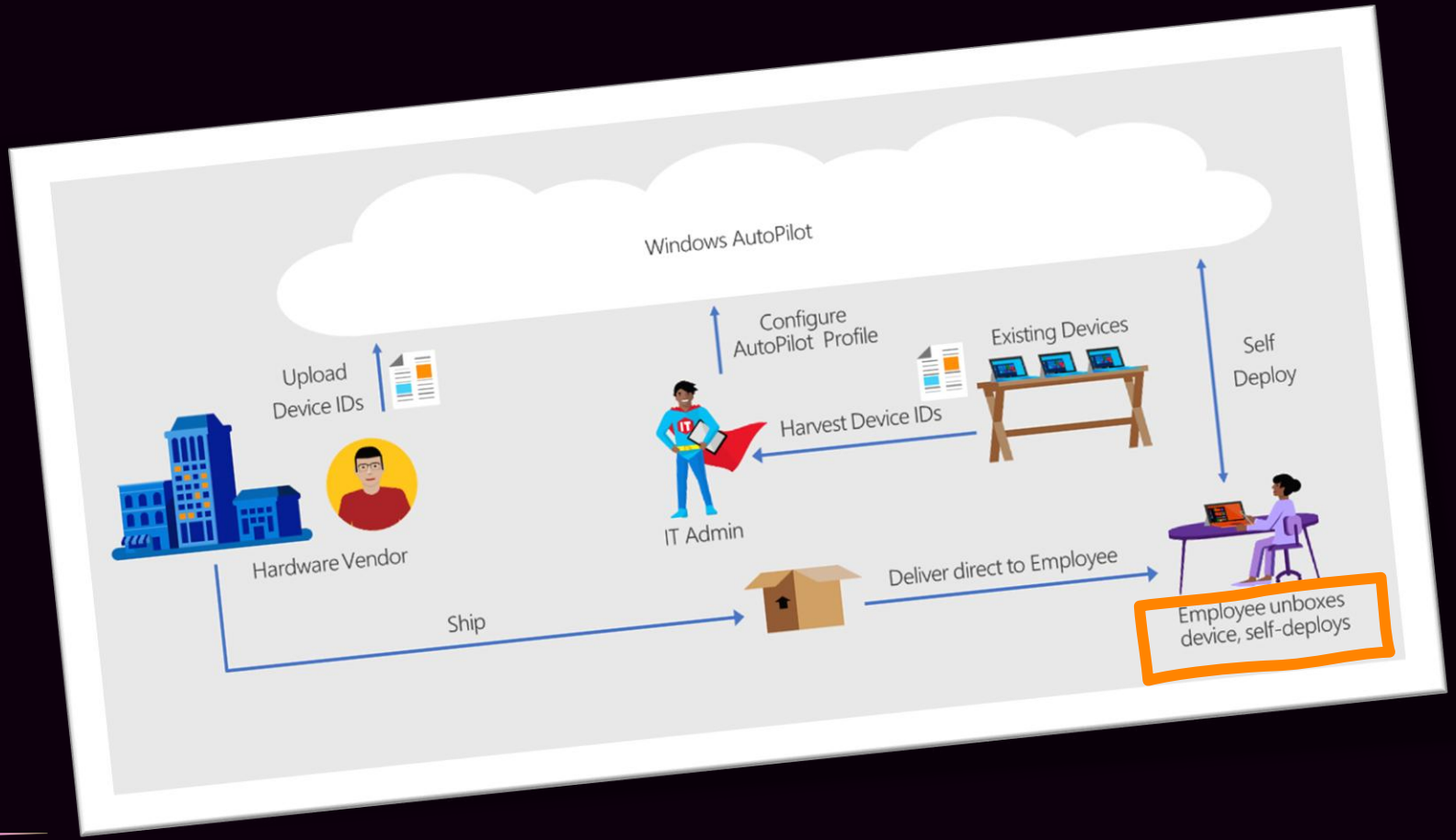
Windows Autopilot Device Onboarding II



Windows Autopilot Device Onboarding II



Windows Autopilot Device Onboarding II



NIC
EMPOWER

Is this the right keyboard layout or input method?

If you also use another keyboard layout, you can add that next.

US

Canadian Multilingual Standard

English (India)

Irish

NZ Aotearoa

Scottish Gaelic

Yes

5 How?

Can we do stuff?

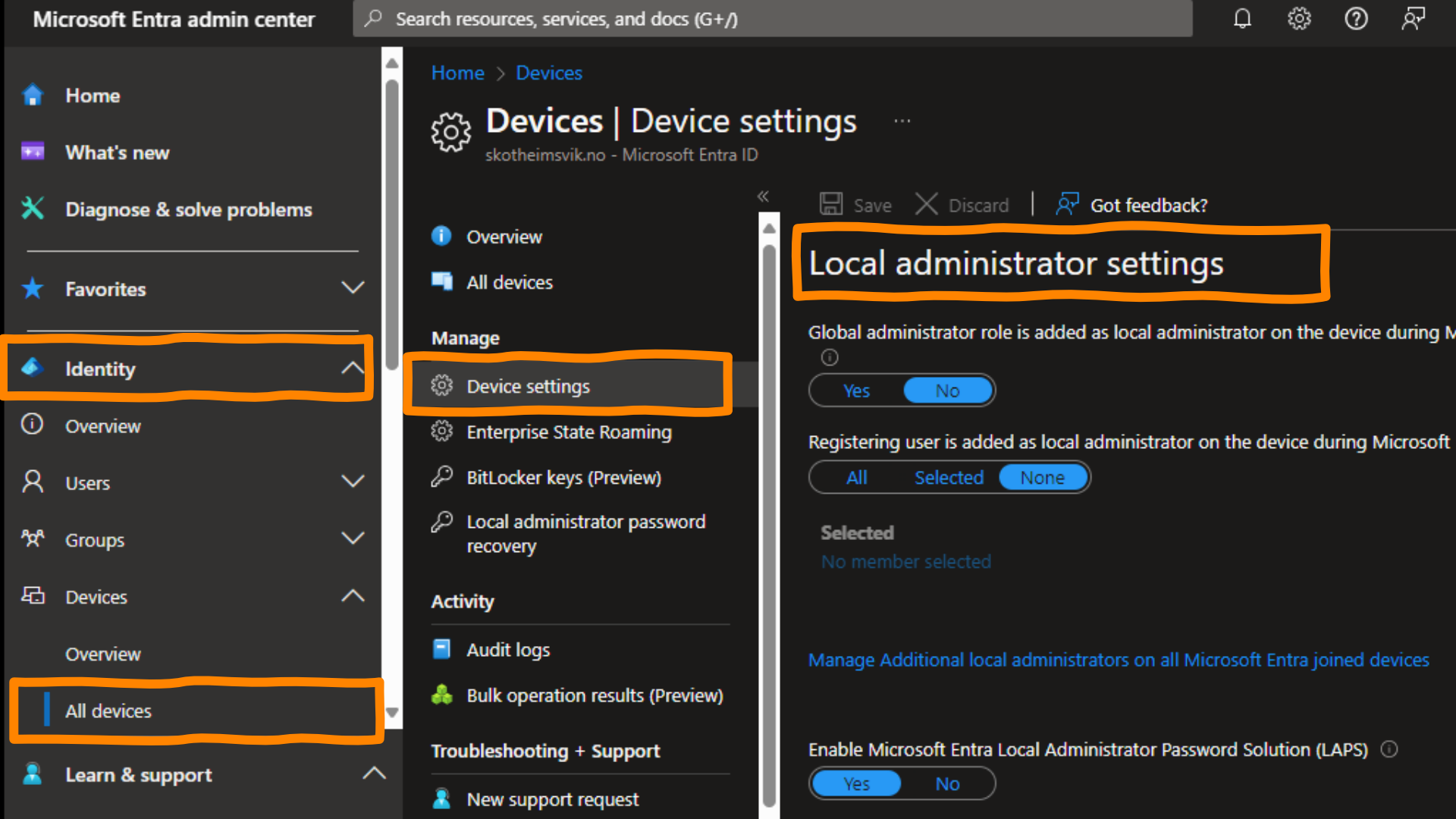
NIC
EMPOWER

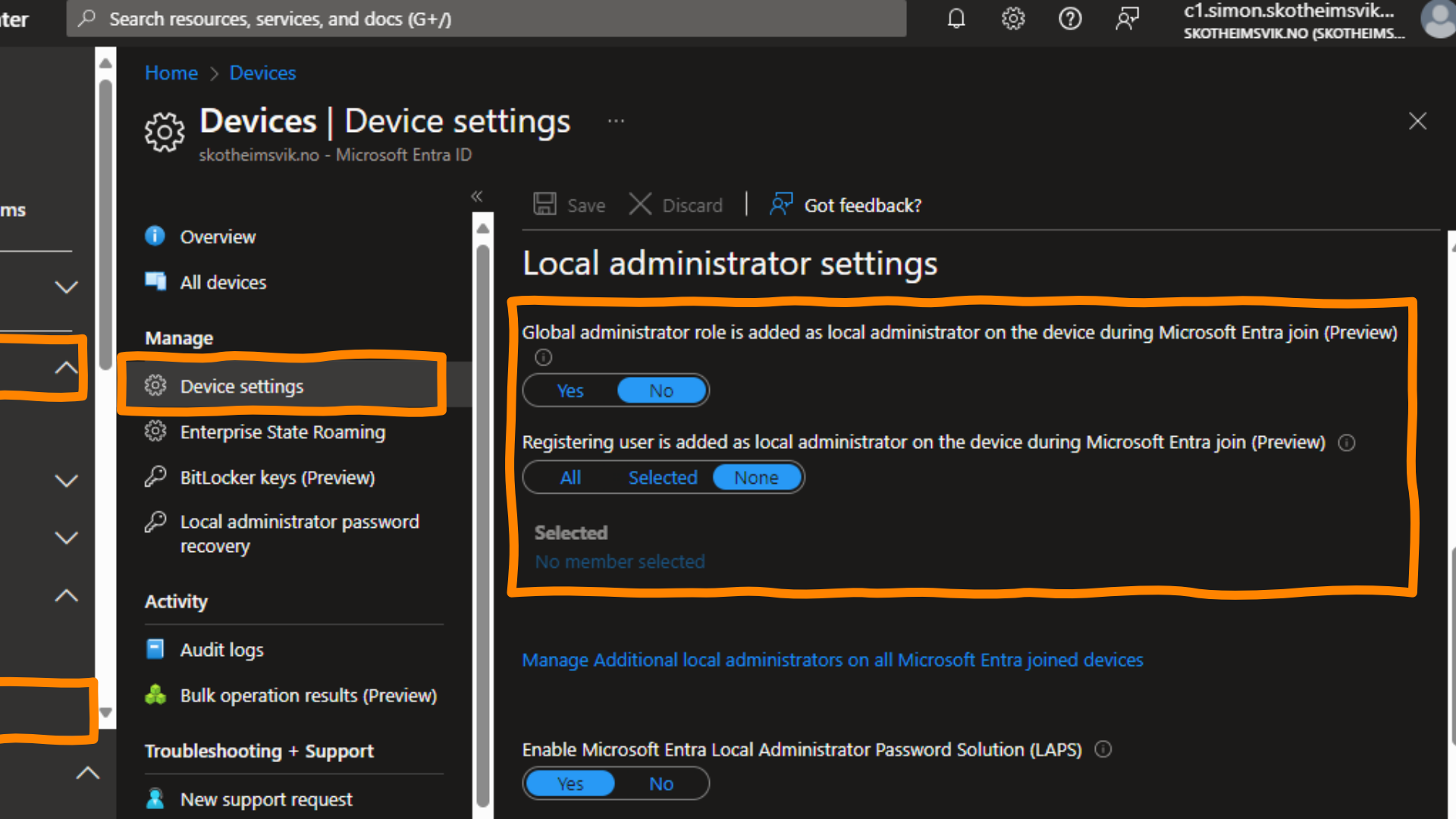
5 How?

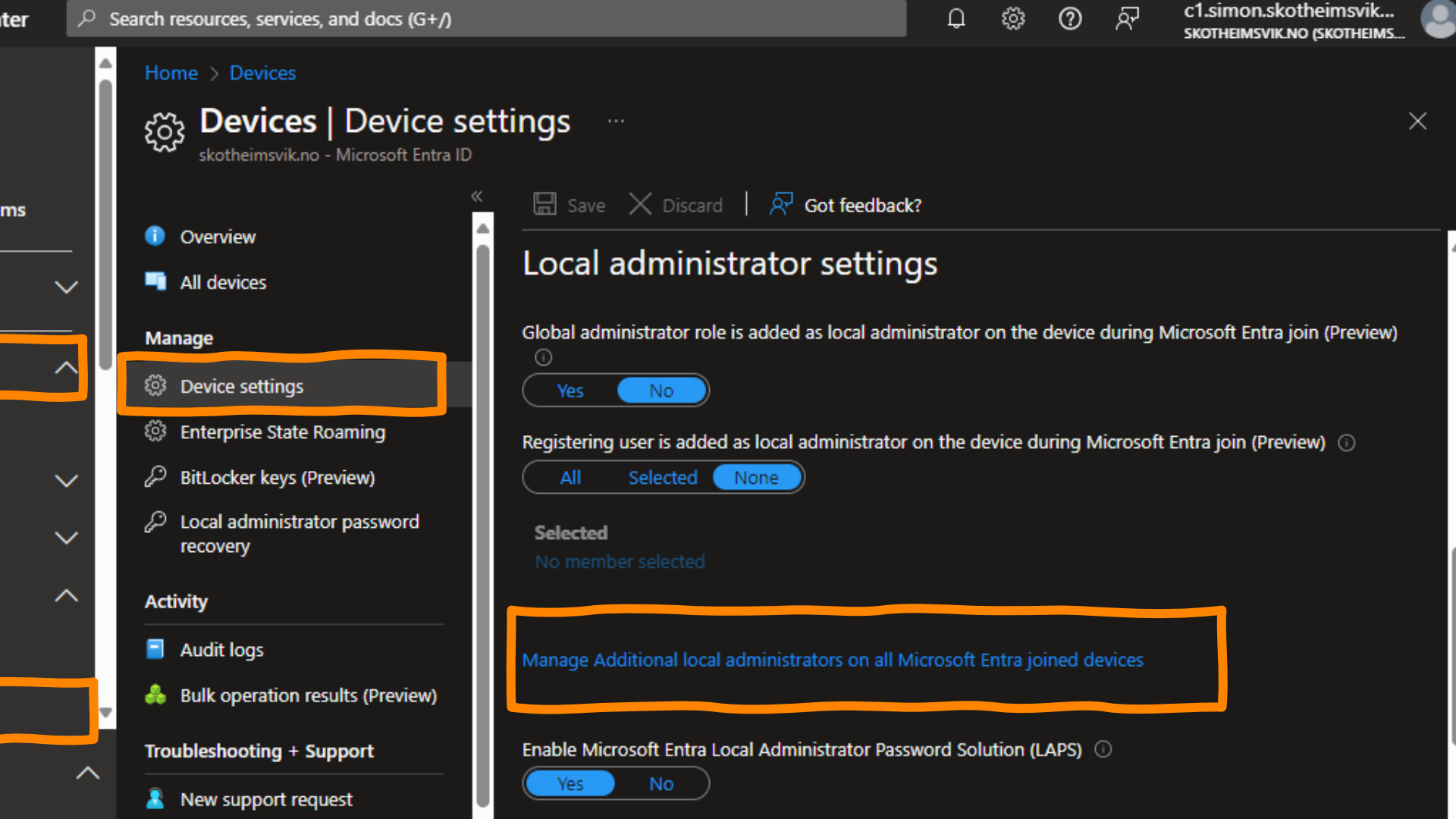
Can we do stuff?

I NEED LOCAL ADMIN!

NIC
EMPOWER


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Overview
All devices
Learn & support
Home > Devices
Devices | Device settings
skotheimsvik.no - Microsoft Entra ID
Overview
All devices
Manage
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Save
Discard
Got feedback?
Local administrator settings
Global administrator role is added as local administrator on the device during M
Yes
No
Registering user is added as local administrator on the device during Microsoft
All
Selected
None
Selected
No member selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Yes
No


Search resources, services, and docs (G+/)
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home > Devices
Devices | Device settings
skotheimsvik.no - Microsoft Entra ID
Save
Discard
Got feedback?
Overview
All devices
Manage
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Yes
No
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
All
Selected
None
Selected
No member selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Yes
No


Search resources, services, and docs (G+/)
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home > Devices
Devices | Device settings
skotheimsvik.no - Microsoft Entra ID
Save
Discard
Got feedback?
Overview
All devices
Manage
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Yes
No
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
All
Selected
None
Selected
No member selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Yes
No

Device Administrators | Description

All roles

Diagnose and solve problems

Manage

Assignments

Description

Activity

Bulk operation results

Troubleshooting + Support

New support request

Got feedback?

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

Role permissions

NIC
EMPOWER


NIC
EMPOWER


NIC
EMPOWER


NIC
EMPOWER


NIC
EMPOWER


NIC
EMPOWER

5 How?

Can we do stuff?

I NEED LOCAL ADMIN!

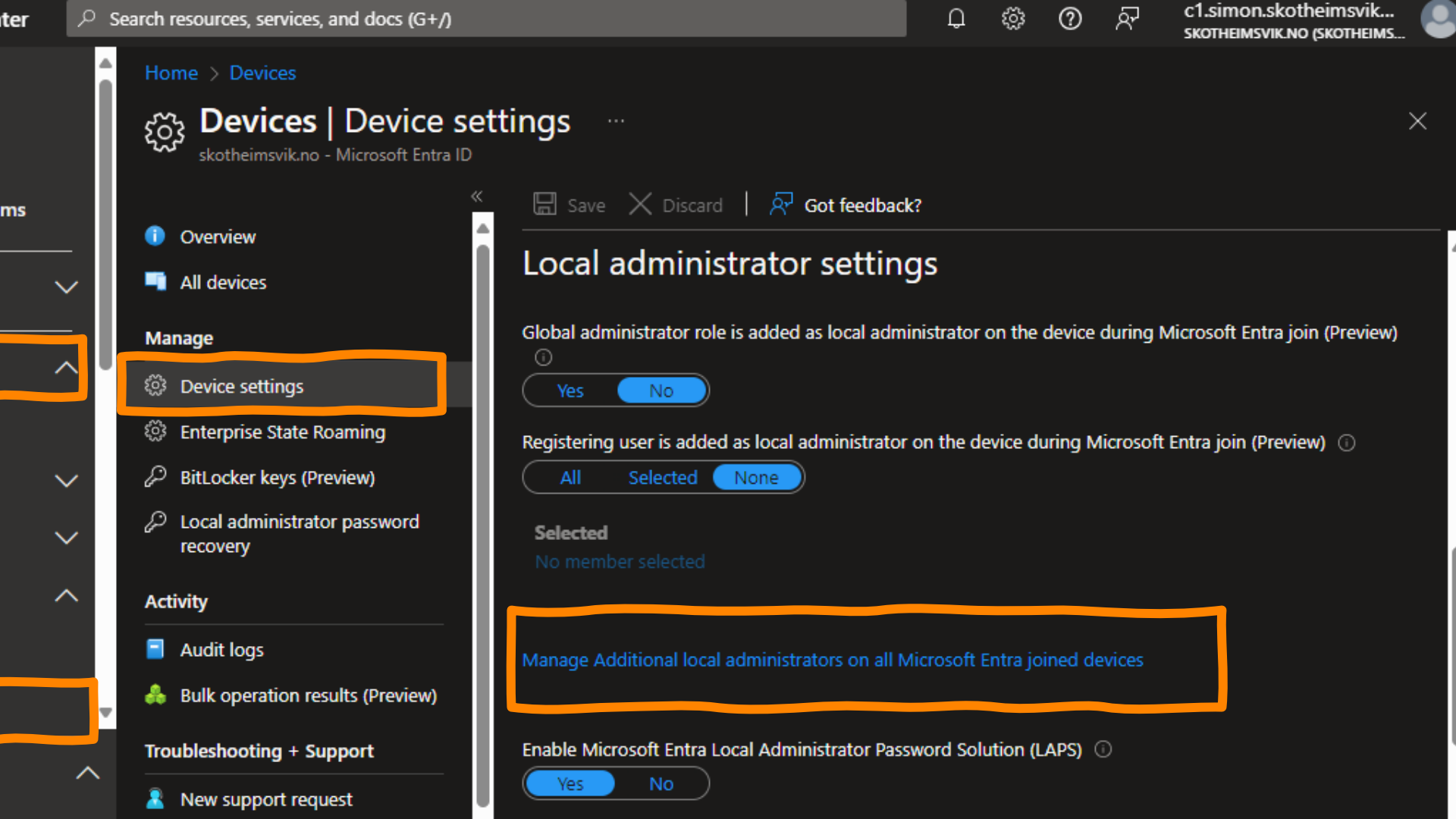
NIC
EMPOWER

6 How?

Can we do stuff?

I NEED LAPS!

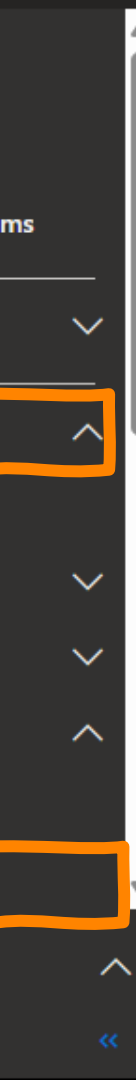
NIC
EMPOWER


Search resources, services, and docs (G+/)
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home > Devices
Devices | Device settings
skotheimsvik.no - Microsoft Entra ID
Save
Discard
Got feedback?
Overview
All devices
Manage
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Yes
No
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
All
Selected
None
Selected
No member selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Yes
No

Home > Devices

Devices | Device settings

skotheimsvik.no - Microsoft Entra ID



- Overview
- All devices

Manage

- Device settings
- Enterprise State Roaming
- BitLocker keys (Preview)
- Local administrator password recovery

Activity

- Audit logs
- Bulk operation results (Preview)

Troubleshooting + Support

- New support request
- Diagnose and solve problems

Save | Discard | Got feedback?

Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)

Yes | No

Registering user is added as local administrator on the device during Microsoft Entra join (Preview)

All | Selected | None

Selected

No member selected

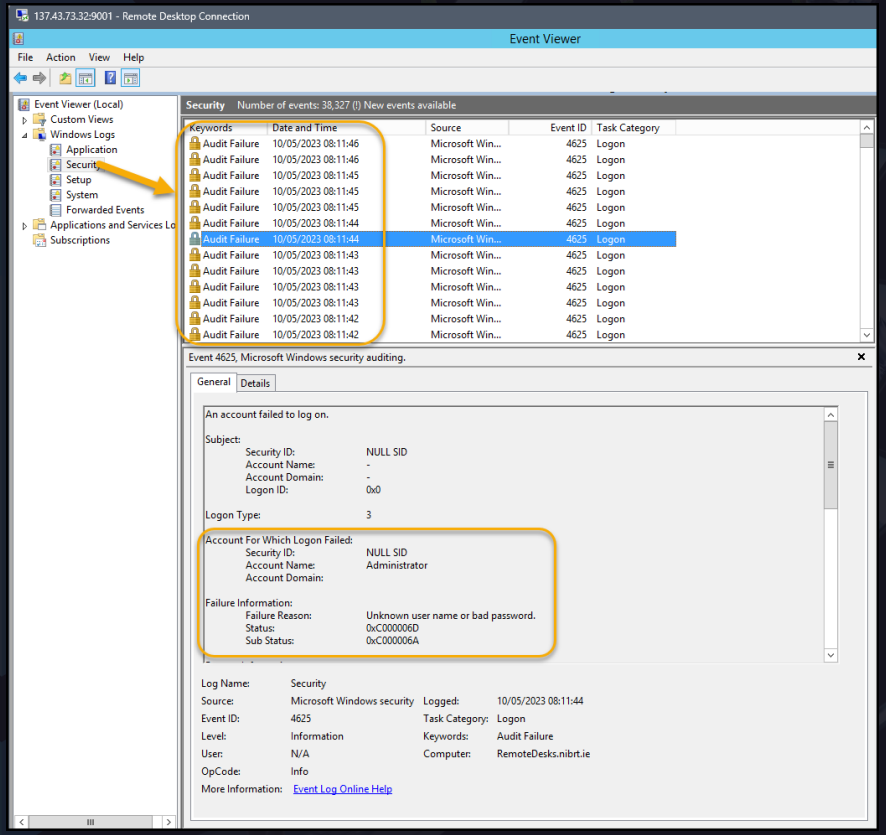
Manage Additional local administrators on all Microsoft Entra joined devices

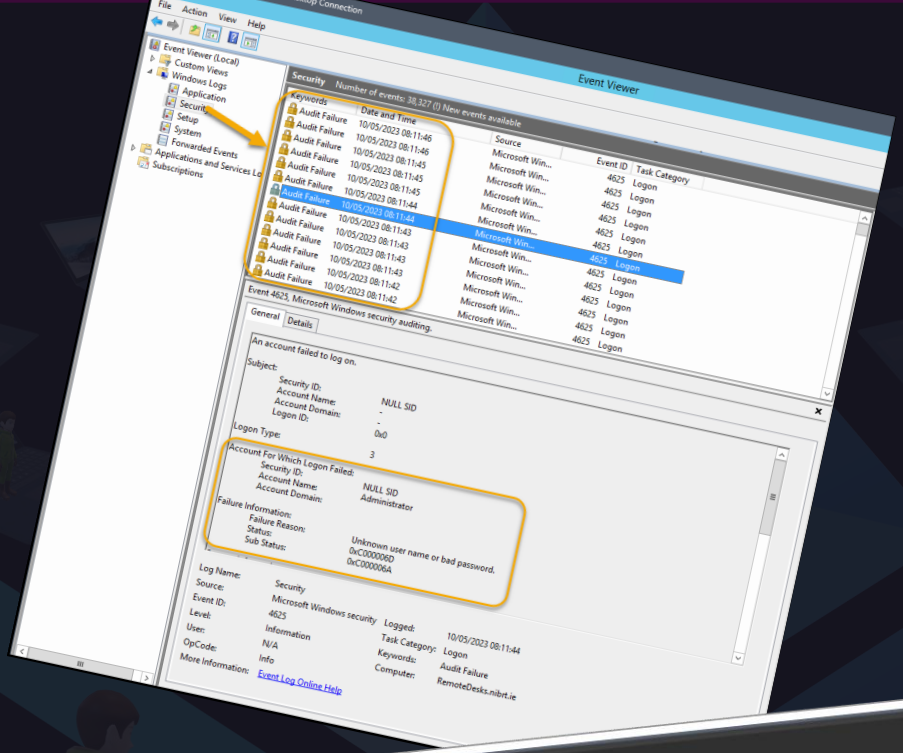
Enable Microsoft Entra Local Administrator Password Solution (LAPS)

Yes | No


NIC
EMPOWER


NIC
EMPOWER

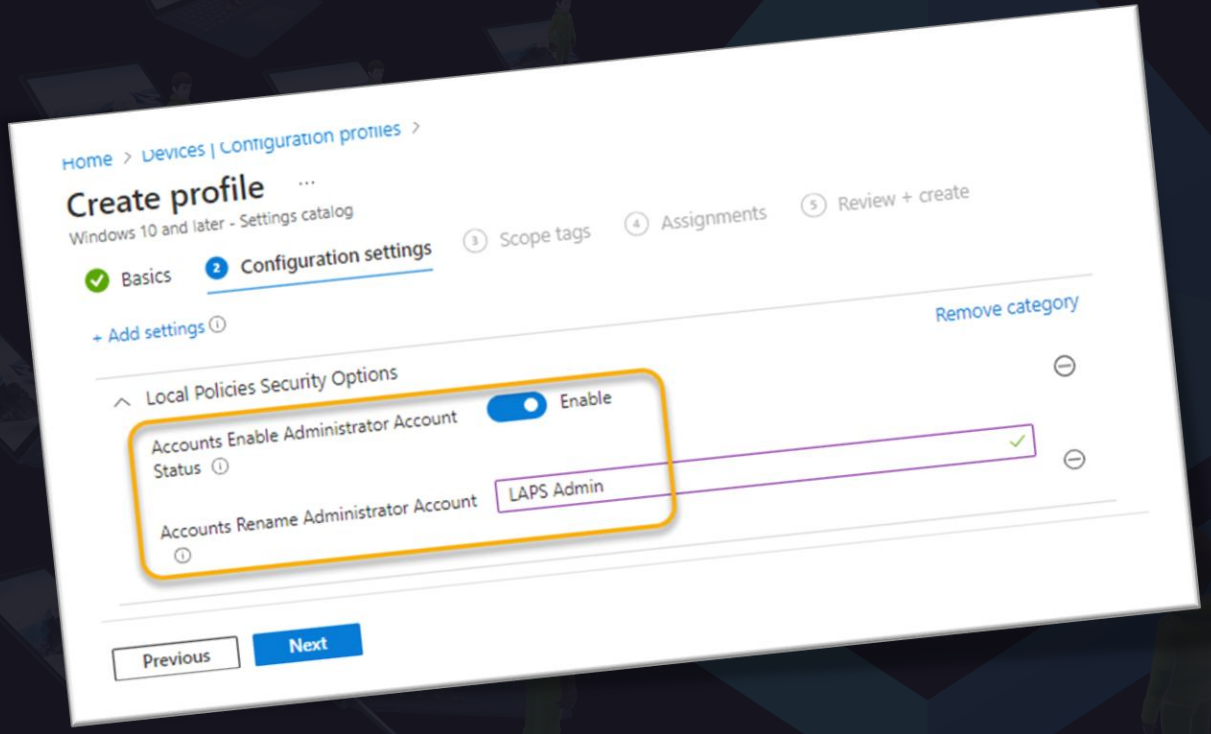

137.43.73.32:9001 - Remote Desktop Connection
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 38,327 (!) New events available
Keywords Date and Time Source Event ID Task Category
Audit Failure 10/05/2023 08:11:46 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:46 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:45 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:45 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:45 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:44 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:44 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:43 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:43 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:43 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:43 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:42 Microsoft Win... 4625 Logon
Audit Failure 10/05/2023 08:11:42 Microsoft Win... 4625 Logon
Event 4625, Microsoft Windows security auditing.
General Details
An account failed to log on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: Administrator
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Log Name: Security
Source: Microsoft Windows security
Logged: 10/05/2023 08:11:44
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: RemoteDesks.nibrt.ie
OpCode: Info
More Information: Event Log Online Help

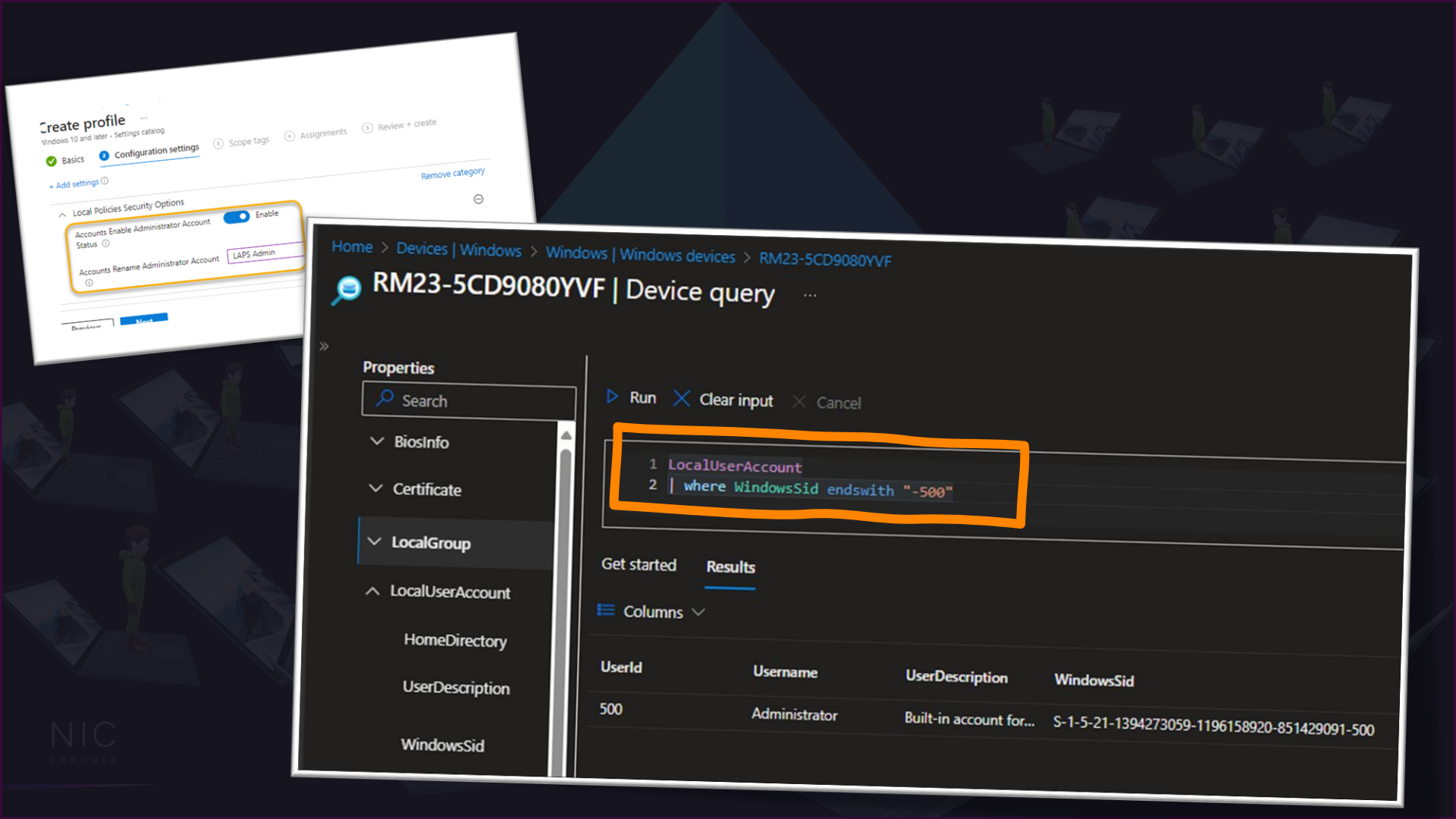


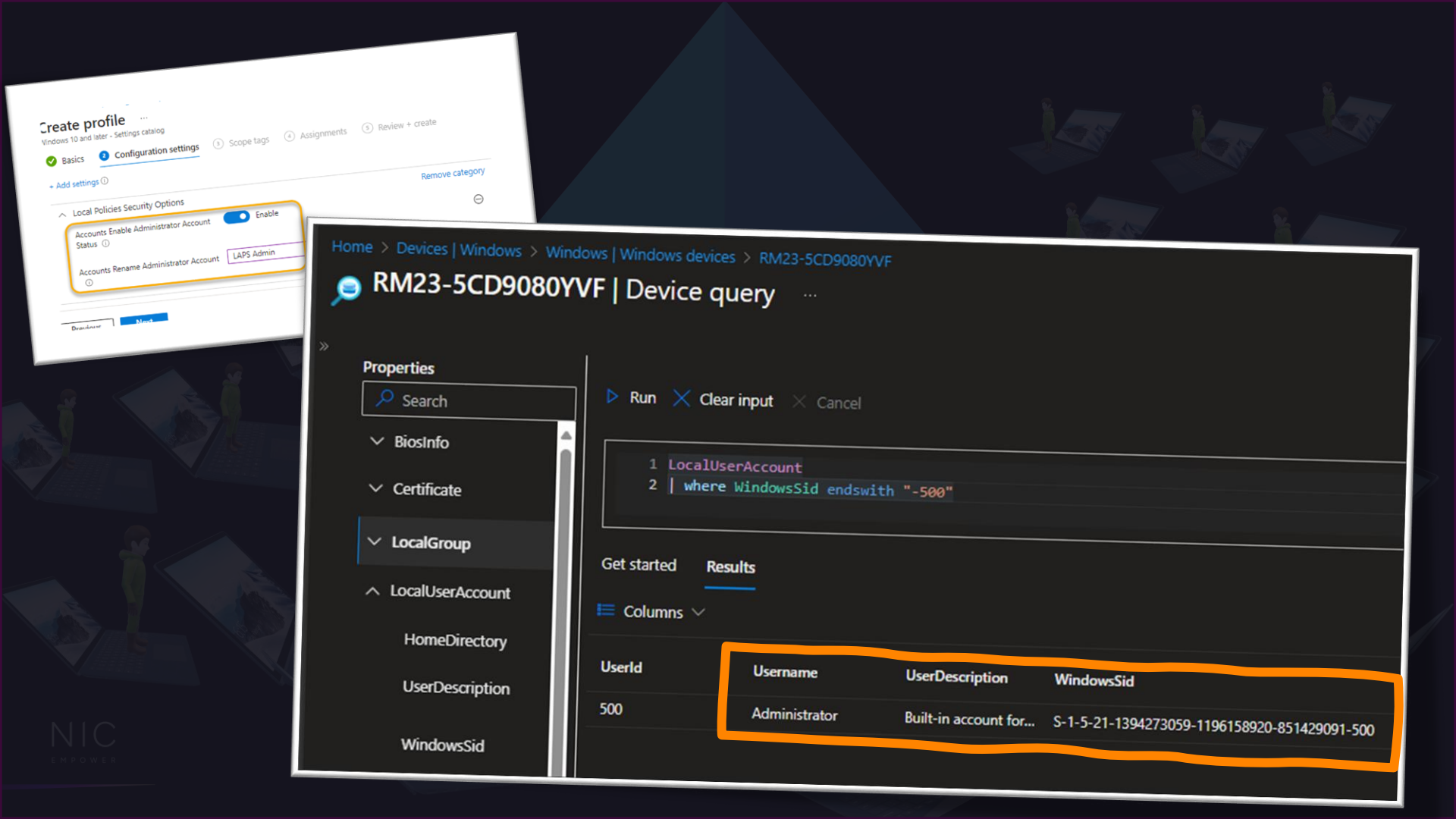
https://learn.microsoft.com/en-us/previous-versions/cc722488(v=technet.10)

10 Immutable Laws of Security Administration

Law #6: There really is someone out there trying to guess your passwords


Home > Devices | Configuration profiles >
Create profile
Windows 10 and later - Settings catalog
Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
+ Add settings
Remove category
Local Policies Security Options
Accounts Enable Administrator Account Status
Enable
Accounts Rename Administrator Account
LAPS Admin
Previous
Next

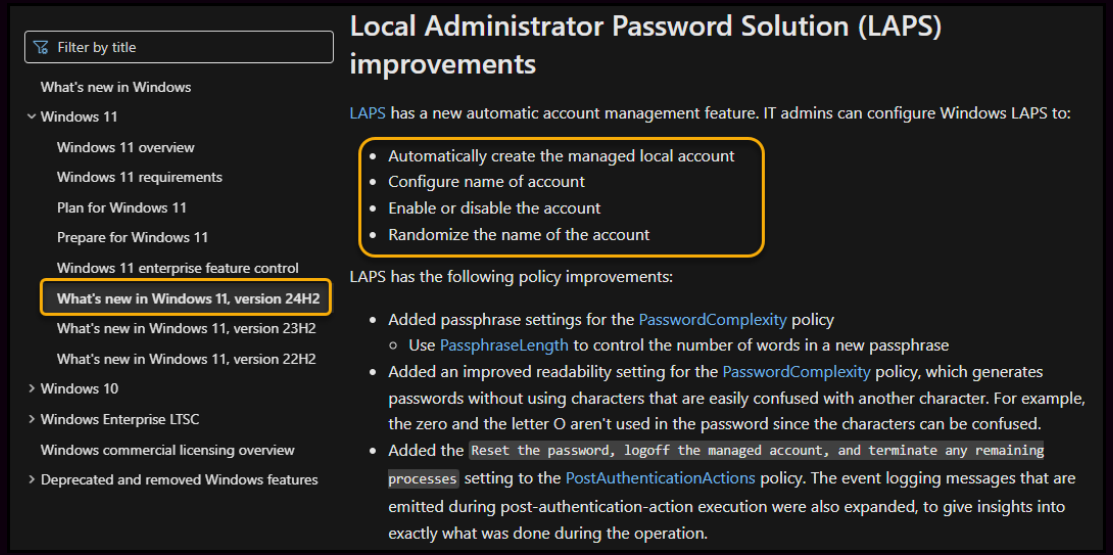

Create profile
Windows 10 and later - Settings catalog
Basics
Configuration settings
Scope tags
Assignments
Review + create
+ Add settings
Remove category
Local Policies Security Options
Accounts Enable Administrator Account Status
Enable
Accounts Rename Administrator Account
LAPS Admin
Home > Devices | Windows > Windows | Windows devices > RM23-5CD9080YVF
RM23-5CD9080YVF | Device query
Properties
Search
BiosInfo
Certificate
LocalGroup
LocalUserAccount
HomeDirectory
UserDescription
WindowsSid
Run
Clear input
Cancel
1 LocalUserAccount
2 | where WindowsSid endswith "-500"
Get started
Results
Columns
UserId
Username
UserDescription
WindowsSid
500
Administrator
Built-in account for...
S-1-5-21-1394273059-1196158920-851429091-500


Create profile
Windows 10 and later - Settings catalog
Basics
Configuration settings
Scope tags
Assignments
Review + create
+ Add settings
Remove category
Local Policies Security Options
Accounts Enable Administrator Account Status
Enable
Accounts Rename Administrator Account
LAPS Admin
Home > Devices | Windows > Windows | Windows devices > RM23-5CD9080YVF
RM23-5CD9080YVF | Device query
Properties
Search
BiosInfo
Certificate
LocalGroup
LocalUserAccount
HomeDirectory
UserDescription
WindowsSid
Run
Clear input
Cancel
1 LocalUserAccount
2 | where WindowsSid endswith "-500"
Get started
Results
Columns
UserId
Username
UserDescription
WindowsSid
500
Administrator
Built-in account for...
S-1-5-21-1394273059-1196158920-851429091-500

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



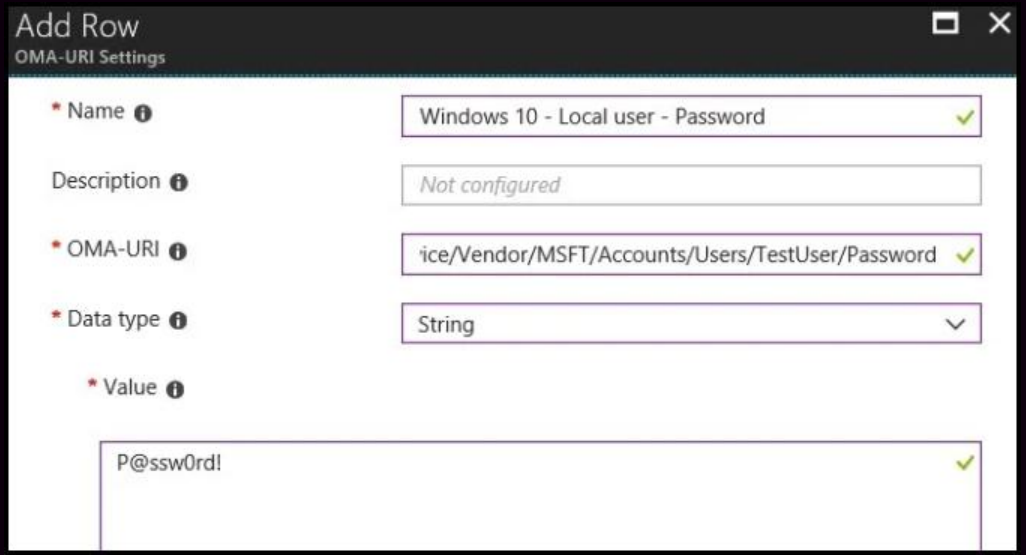
https://learn.microsoft.com/en-us/windows/whats-new/whats-new-windows-11-version-24h2#local-administrator-password-solution-laps-improvements

NIC EMPOWER

The LAPS Account

- Create a New Account Using a Policy?

- Same password on all devices
- Password in clear text



NIC
EMPOWER

The LAPS Account

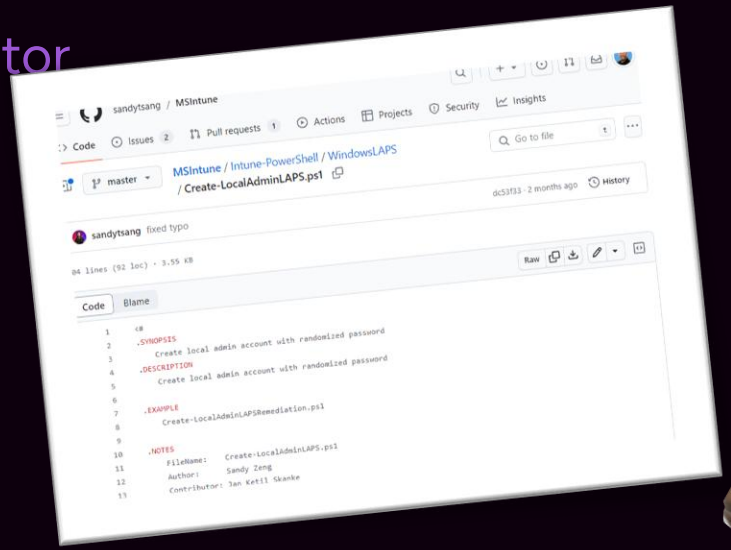
- Using a Script/Remediation!

- Random password for each device
- Will be managed with LAPS

The LAPS Account

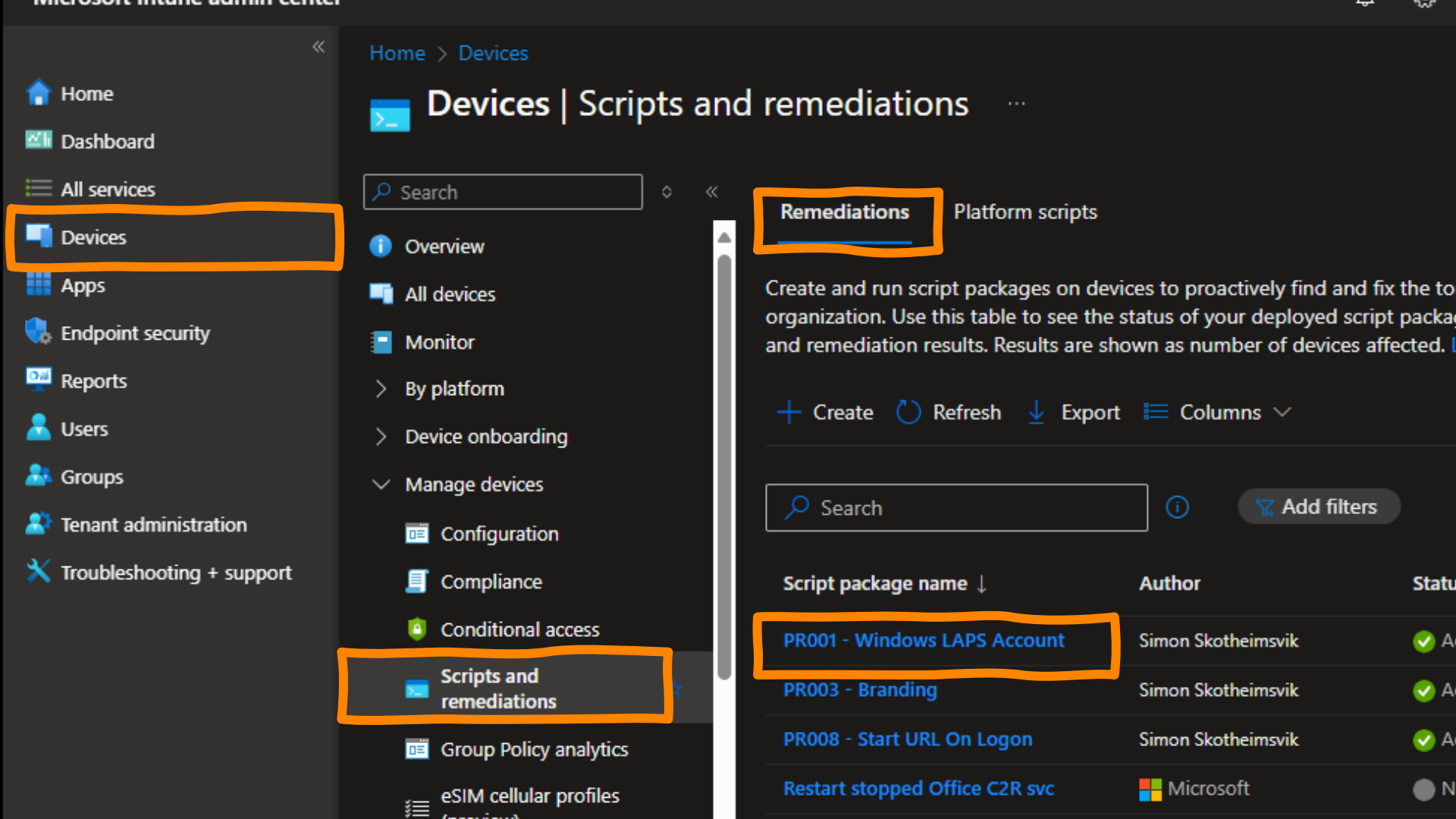
- Using a Script/Remediation!

- 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



https://github.com/sandytsang/MSIntune/tree/master/Intune-PowerShell/WindowsLAPS

NIC EMPOWER


Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices
Devices | Scripts and remediations
Search
Overview
All devices
Monitor
By platform
Device onboarding
Manage devices
Configuration
Compliance
Conditional access
Scripts and remediations
Group Policy analytics
eSIM cellular profiles
Remediations
Platform scripts
Create and run script packages on devices to proactively find and fix the to
organization. Use this table to see the status of your deployed script packa
and remediation results. Results are shown as number of devices affected.
Create
Refresh
Export
Columns
Search
Add filters
Script package name
Author
Statu
PR001 - Windows LAPS Account
Simon Skotheimsvik
PR003 - Branding
Simon Skotheimsvik
PR008 - Start URL On Logon
Simon Skotheimsvik
Restart stopped Office C2R svc
Microsoft

Microsoft Intune admin center

Edit - PR001 - Windows LAPS Account ...

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

1 Settings 2 Review + save

Create a custom script package from scripts you've written. By default, scripts will run on assigned devices every day.

Detection script file: Select a file

https://github.com/sandytsang/MSIntune/tree/master/Intune-PowerShell/WindowsLAPS

Detection script:

```
$localAdminName = "SimonDoesLocalAdmin"
#Get local admin group name by using known sid
$Localadmingroupname = $((Get-LocalGroup -SID "S-1-5-32-544").Name)

try {
    #Find the custom local admin account and check if it's a renamed built-in
account
```

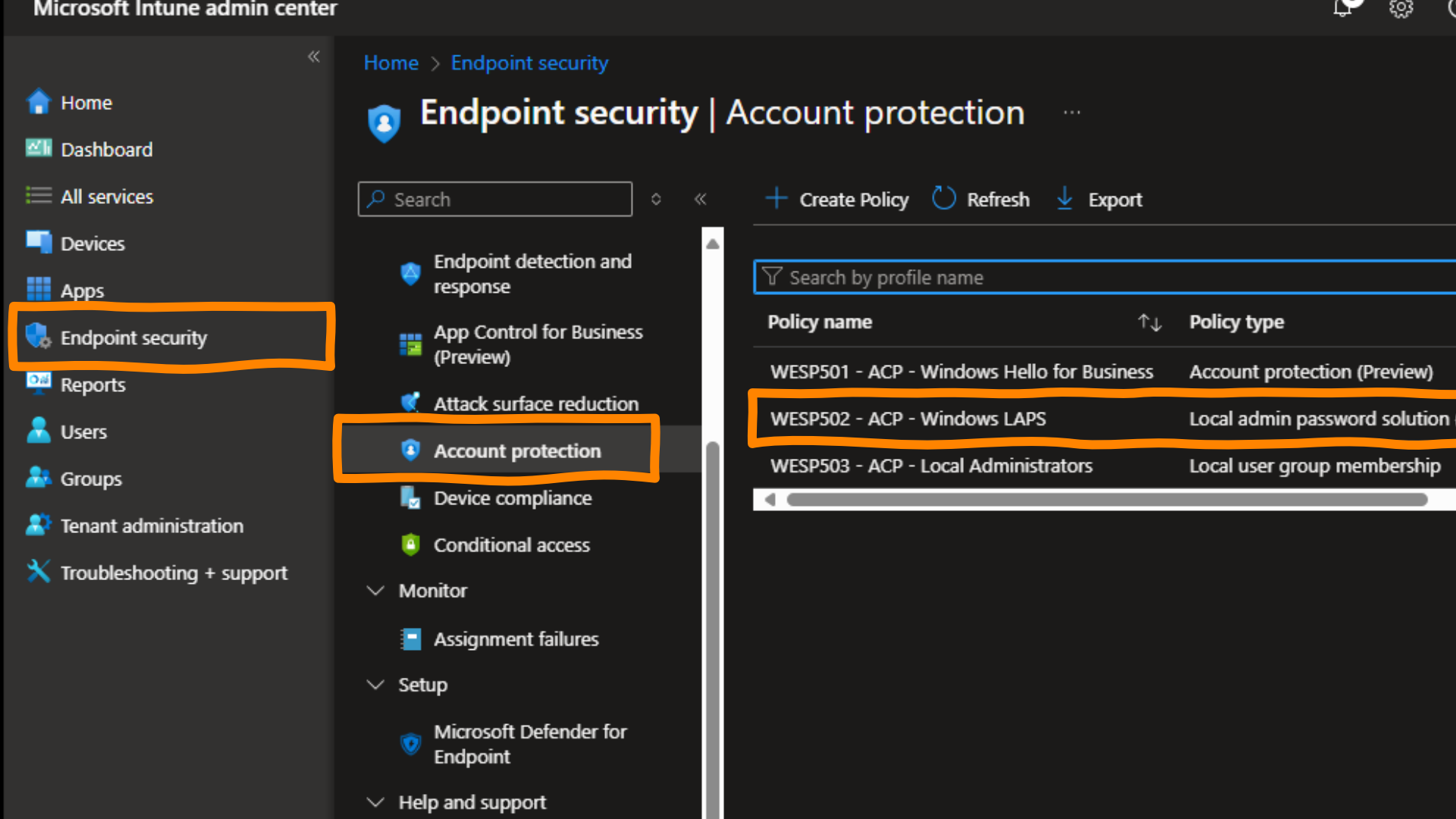
Remediation script file: Select a file

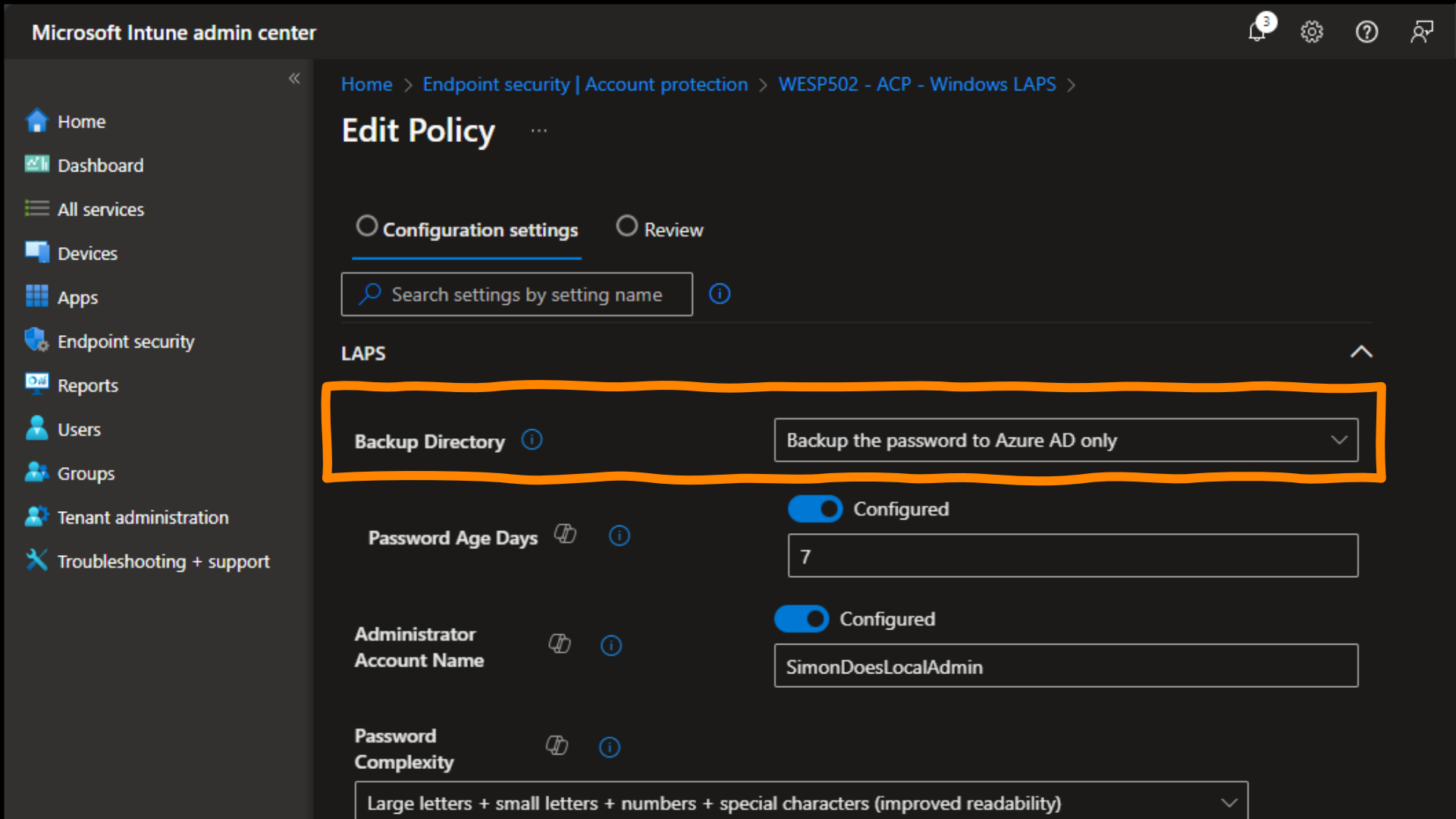
Remediation script:

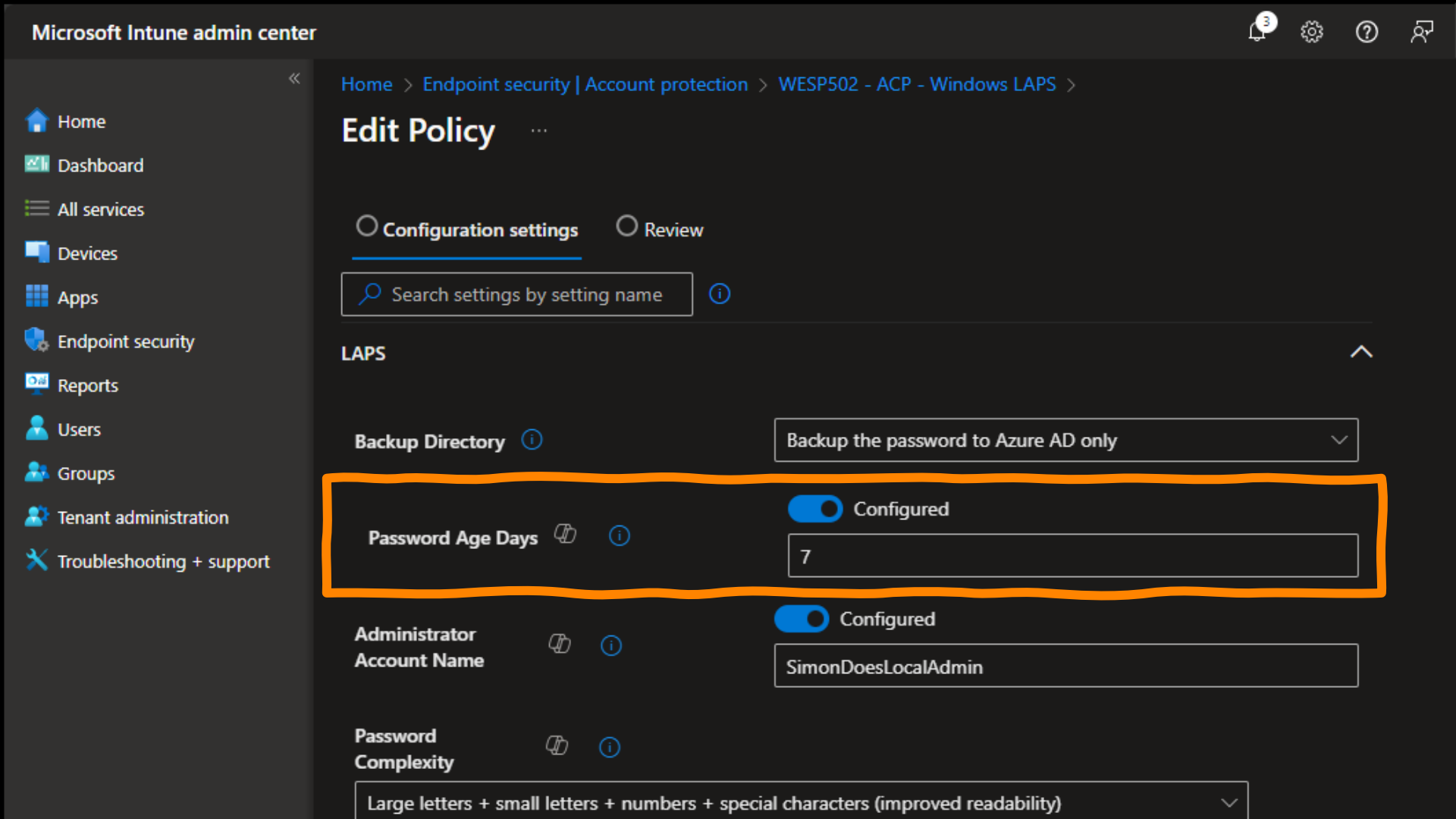
```
<#
.SYNOPSIS
    Create local admin account with randomized password
.DESCRIPTION
```

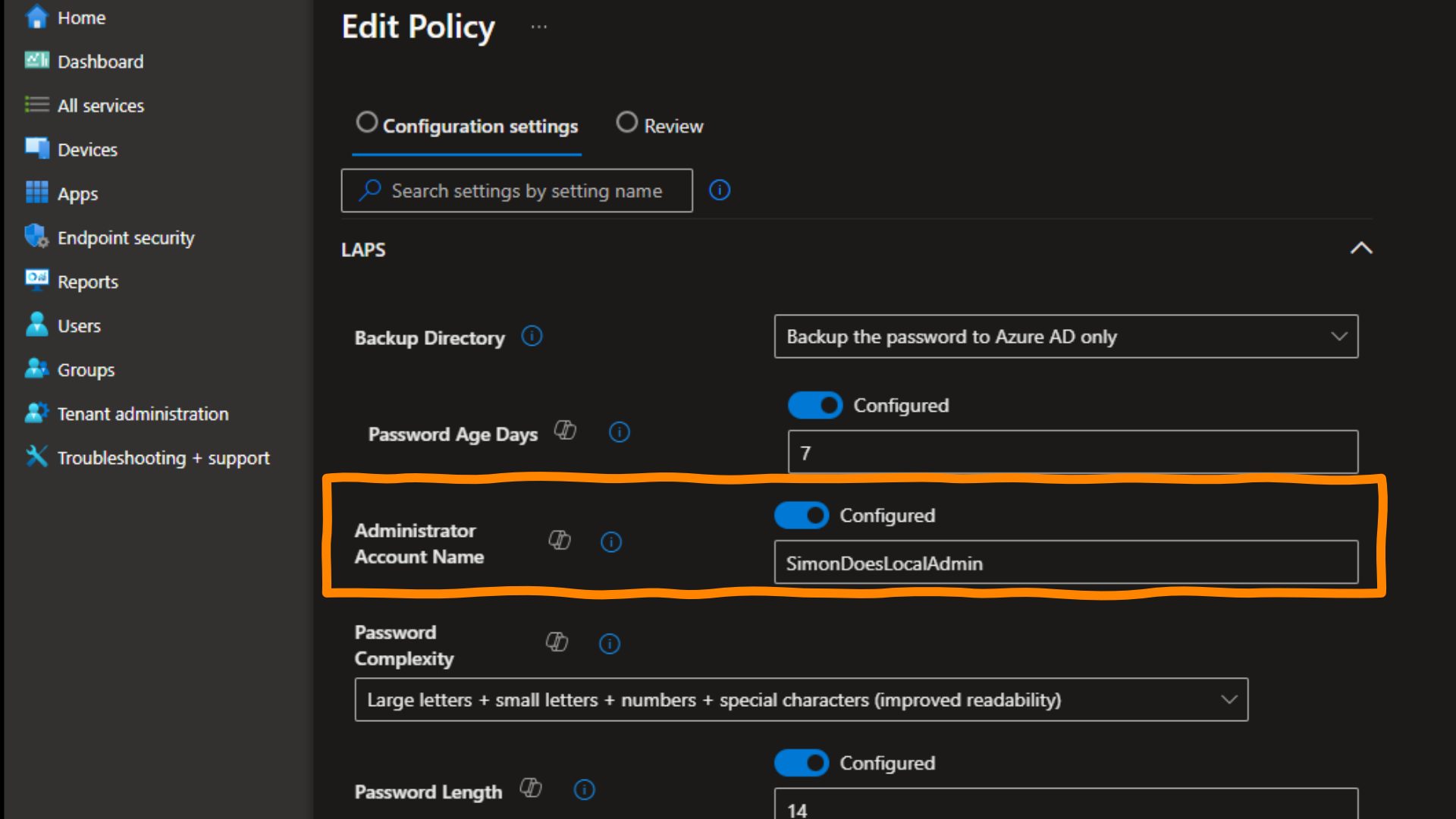

sjDF8sdfs/df#
#4f¤4#DS”e3f34
#4f¤4#DS”e3f34
sjDF8sdfs/df#
sjDF8sdfs/df#
4f¤4#DS”e3f34
sjDF8dfh7DF/df#
sdfssdf/df#
#4f¤4#DS”e3f34
sjDF8sdfs/df#
sdfssdf/df#
sjDF8sdfs/df
#4f¤4#DS”e3f34
ddfdssdfsd/df#
sdsjDFsdf8dfh7DF/df#

NIC
EMPOWER


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Account protection
Search
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Monitor
Assignment failures
Setup
Microsoft Defender for Endpoint
Help and support
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


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP502 - ACP - Windows LAPS >
Edit Policy
Configuration settings
Review
Search settings by setting name
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)


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP502 - ACP - Windows LAPS >
Edit Policy
Configuration settings
Review
Search settings by setting name
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)


Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Edit Policy
Configuration settings
Review
Search settings by setting name
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
14

Tenant administration

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

Tenant administration

Troubleshooting + support

Password Age Days

Microsoft | Windows Blogs Windows Experience Devices Windows Developer Microsoft Edge Windows Insider Microsoft 365

Announcing Windows 11 Insider Preview Build 26040 (Canary Channel)

Written By
Amanda Langowski
Brandon LeBlanc

published
January 26, 2024

Windows LAPS: improved readability password dictionary (and improved password font)

Windows Local Administrator Password Solution (LAPS) has been improved with a new PasswordComplexity setting. Using this feature, IT admins can now configure Windows LAPS to generate less confusing passwords. The new setting is similar to the existing complexity setting 4 in that all four character categories are used (upper case letters, lower case letters, numbers, and special characters). However when PasswordComplexity is configured with the new setting of 5, the most confusing characters are omitted to improve password readability and reduce confusion and wasted time. For example, the number "1" and the letter "l" are never used with the new setting.

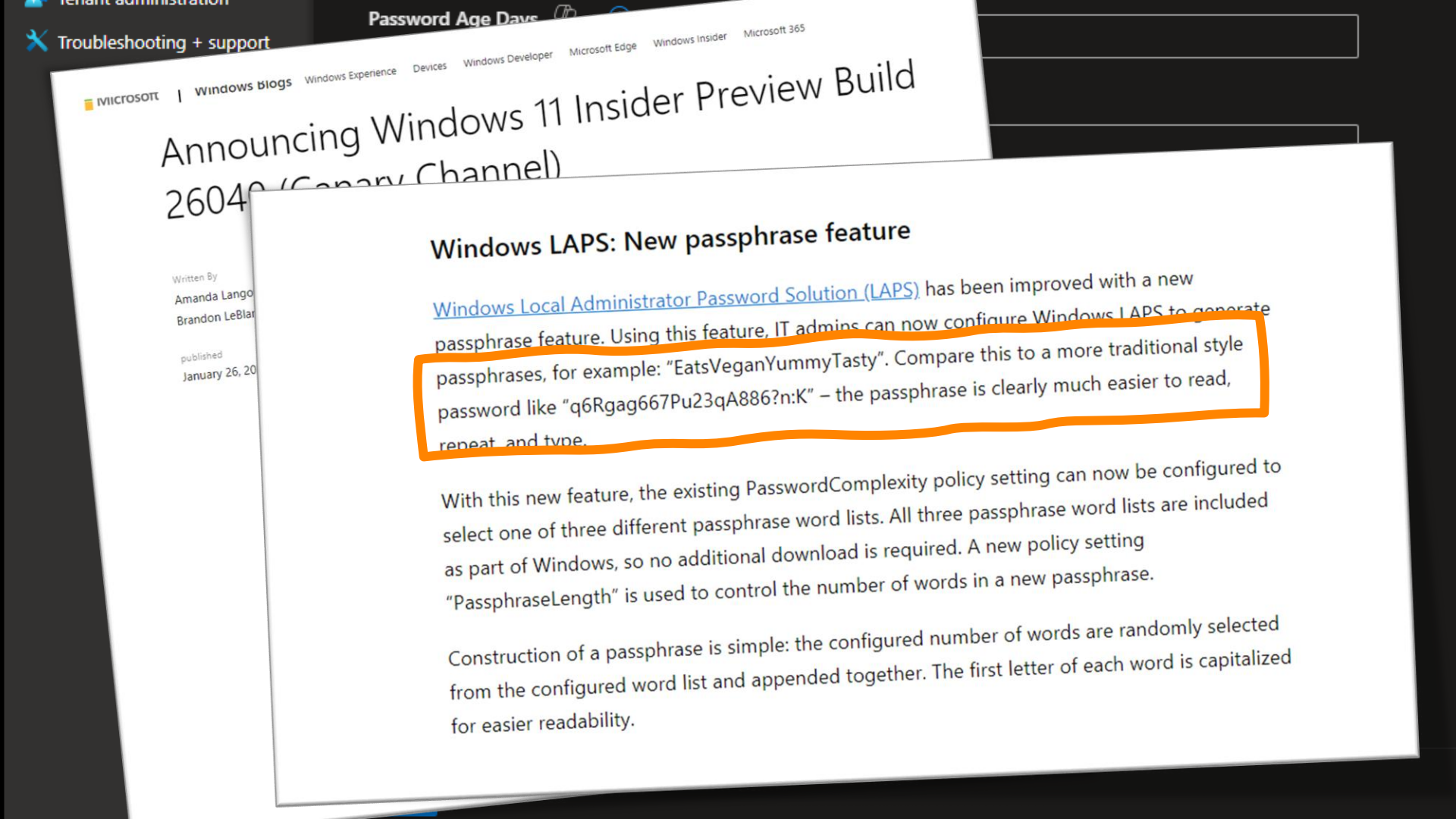
When PasswordComplexity is configured to 5, the following changes are made to the default password dictionary character set:

- Don't use these letters: 'I', 'O', 'Q', 'l', 'o'
- Don't use these numbers: '0', '1'
- Don't use these 'special' characters: ',', '.', '&', '{', '}', '[', ']', '(', ')', ';'
- Start using these 'special' characters: ':', '=', '?', '*'

The Windows LAPS tab in the Active Directory Users and Computers snap-in (via Microsoft Management Console) has also been improved. When the Windows LAPS password is displayed in the clear, the password now uses a new font for improving readability.

ability)

period, the manag...


Tenant administration
Troubleshooting + support
Password Age Days
Microsoft | Windows Blogs
Windows Experience
Devices
Windows Developer
Microsoft Edge
Windows Insider
Microsoft 365
Announcing Windows 11 Insider Preview Build
Written By
Amanda Langowski
Brandon LeBlanc
published
January 26, 2021
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?n:K" – 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.

Tenant administration

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

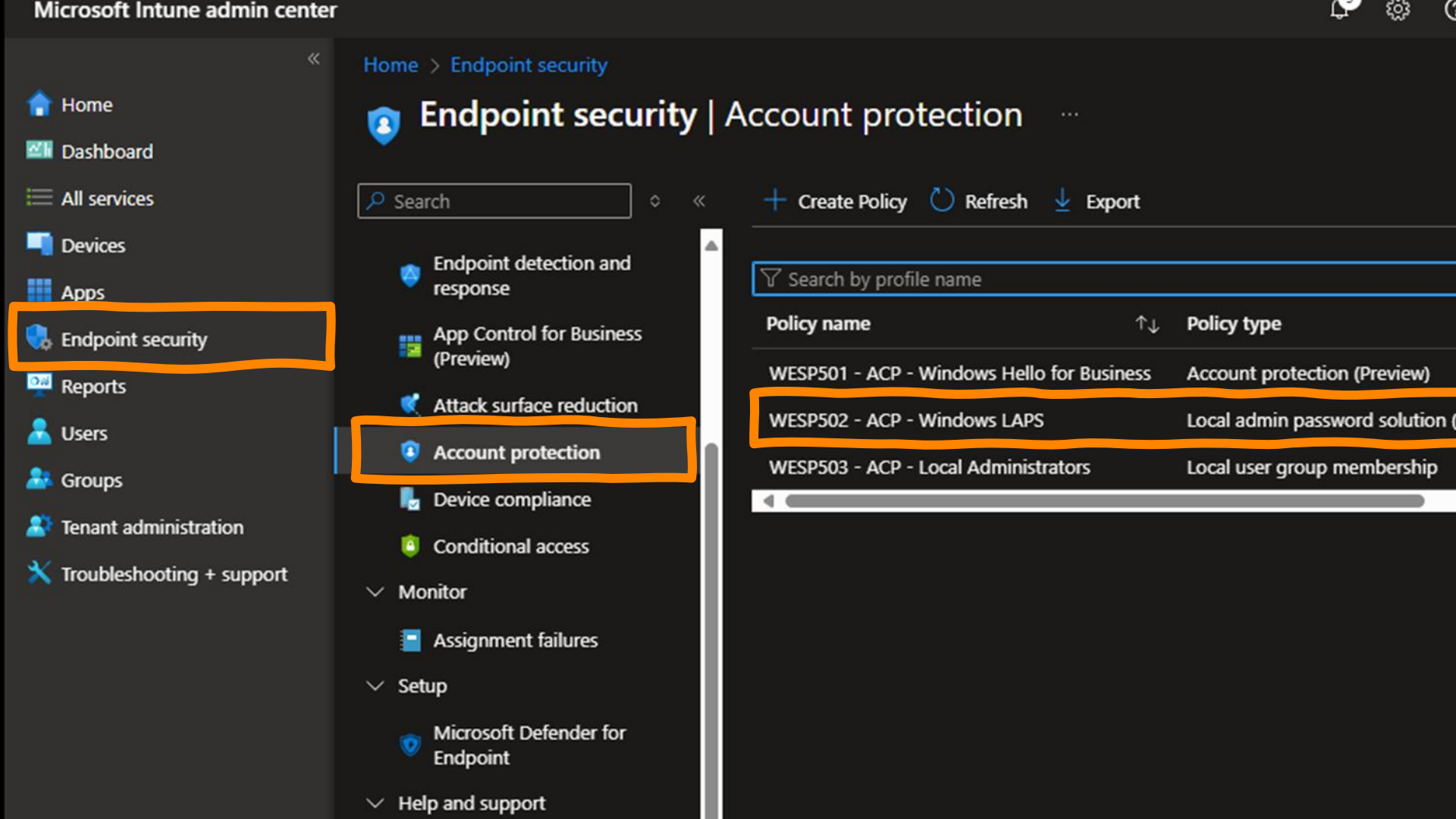
Reset the password and logoff the managed account: upon expiry of the grace period, the manag...

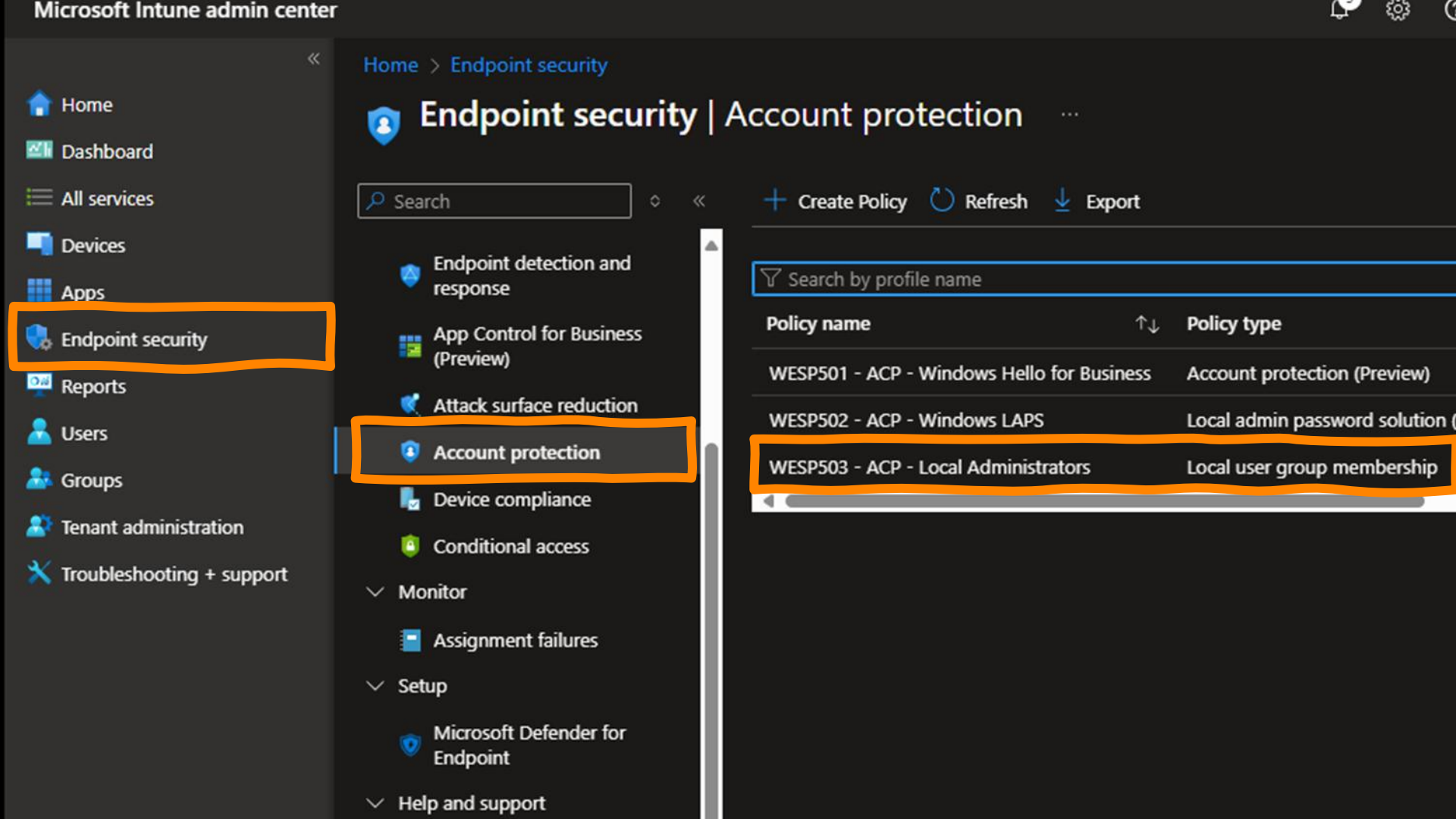
Post Authentication Reset Delay

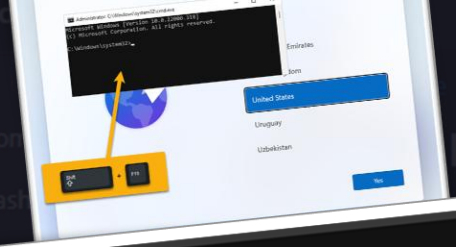
Configured

2

Next


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Account protection
Search
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Monitor
Assignment failures
Setup
Microsoft Defender for Endpoint
Help and support
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


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Account protection
Search
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Monitor
Assignment failures
Setup
Microsoft Defender for Endpoint
Help and support
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



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.
```

Endpoint security

Endpoint security | A

Account protection

Device compliance

Conditional access

Monitor

Assignment failures

Setup

Microsoft Defender for Endpoint

Help and support

Groups

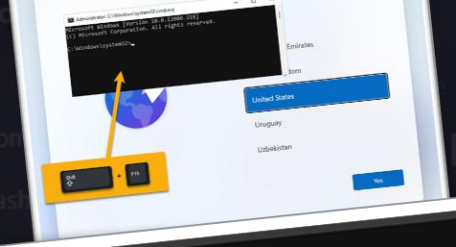
Tenant administration

Troubleshooting + support

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



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.
```

Endpoint security

Account protection

Device compliance

Conditional access

Monitor

Assignment failures

Setup

Microsoft Defender for Endpoint

Help and support

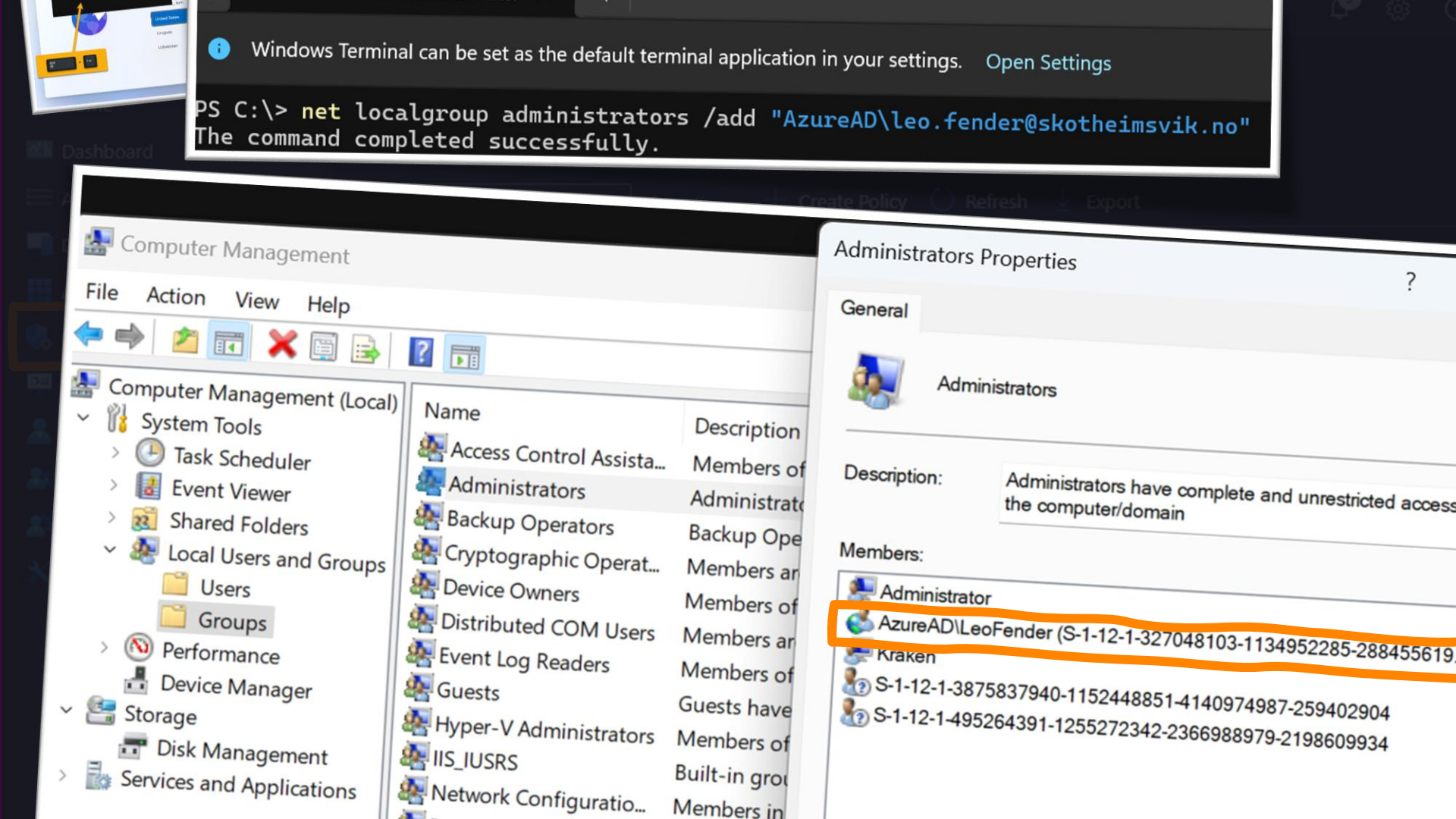
Groups

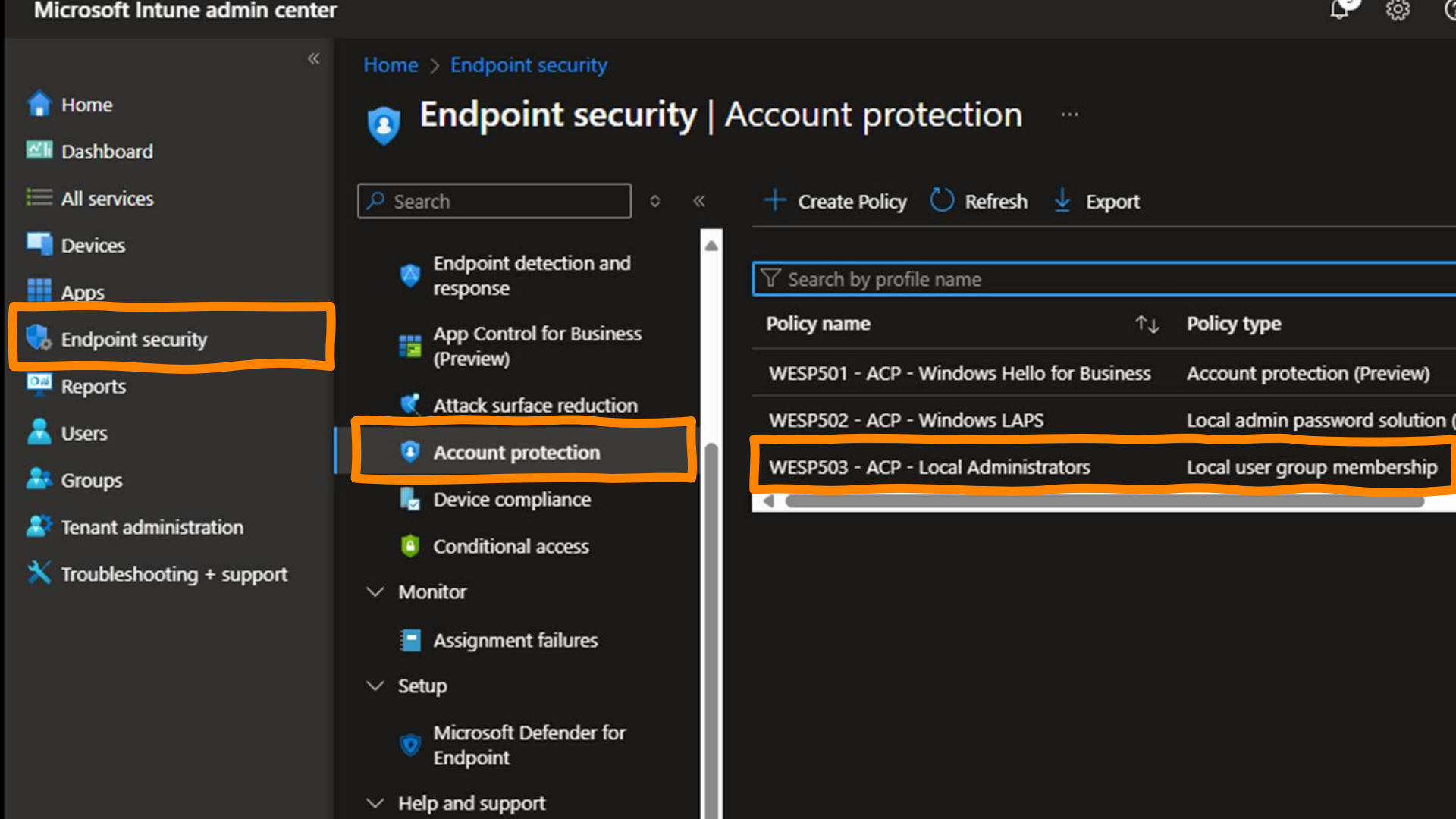
Tenant administration

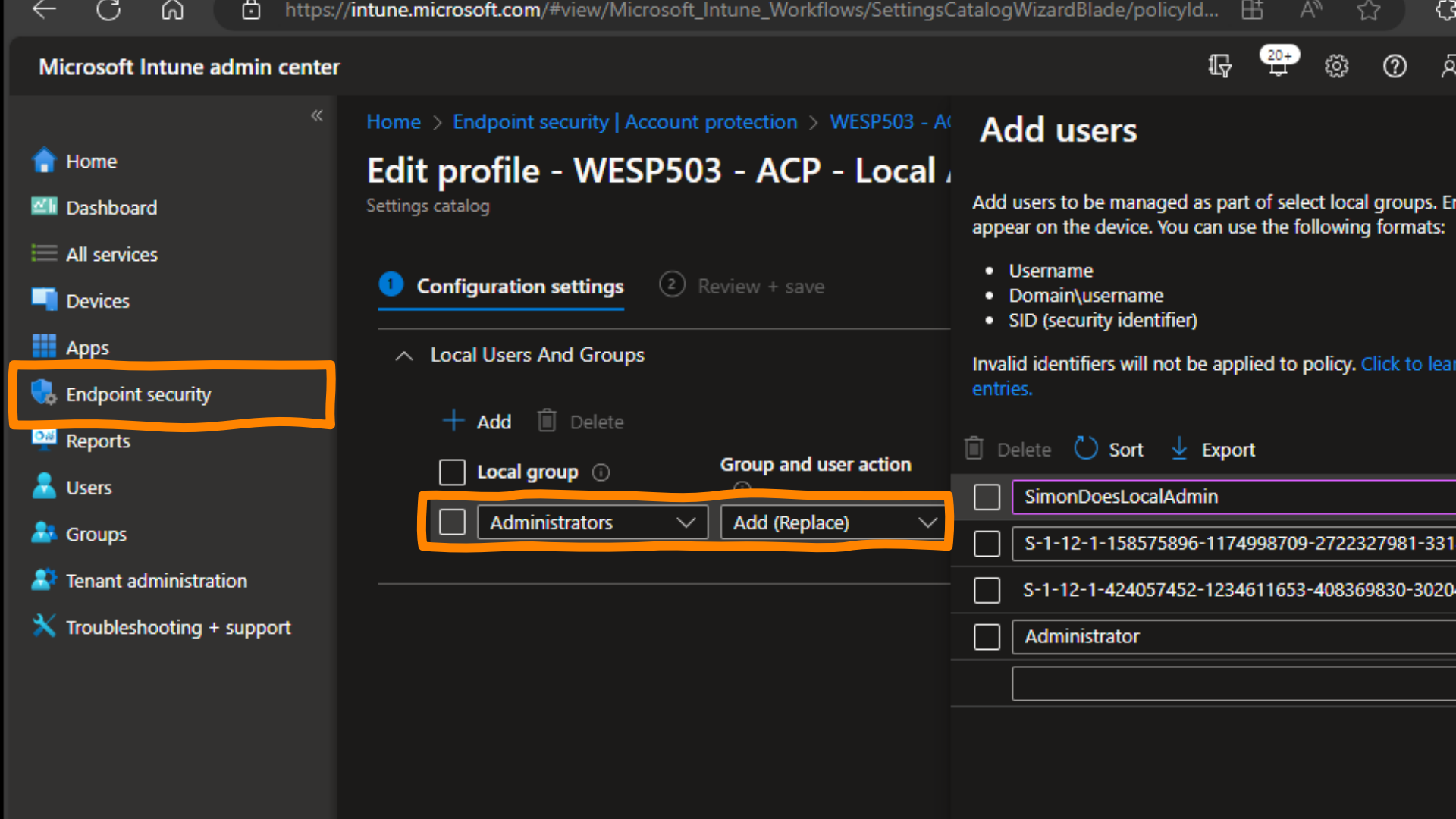
Troubleshooting + support

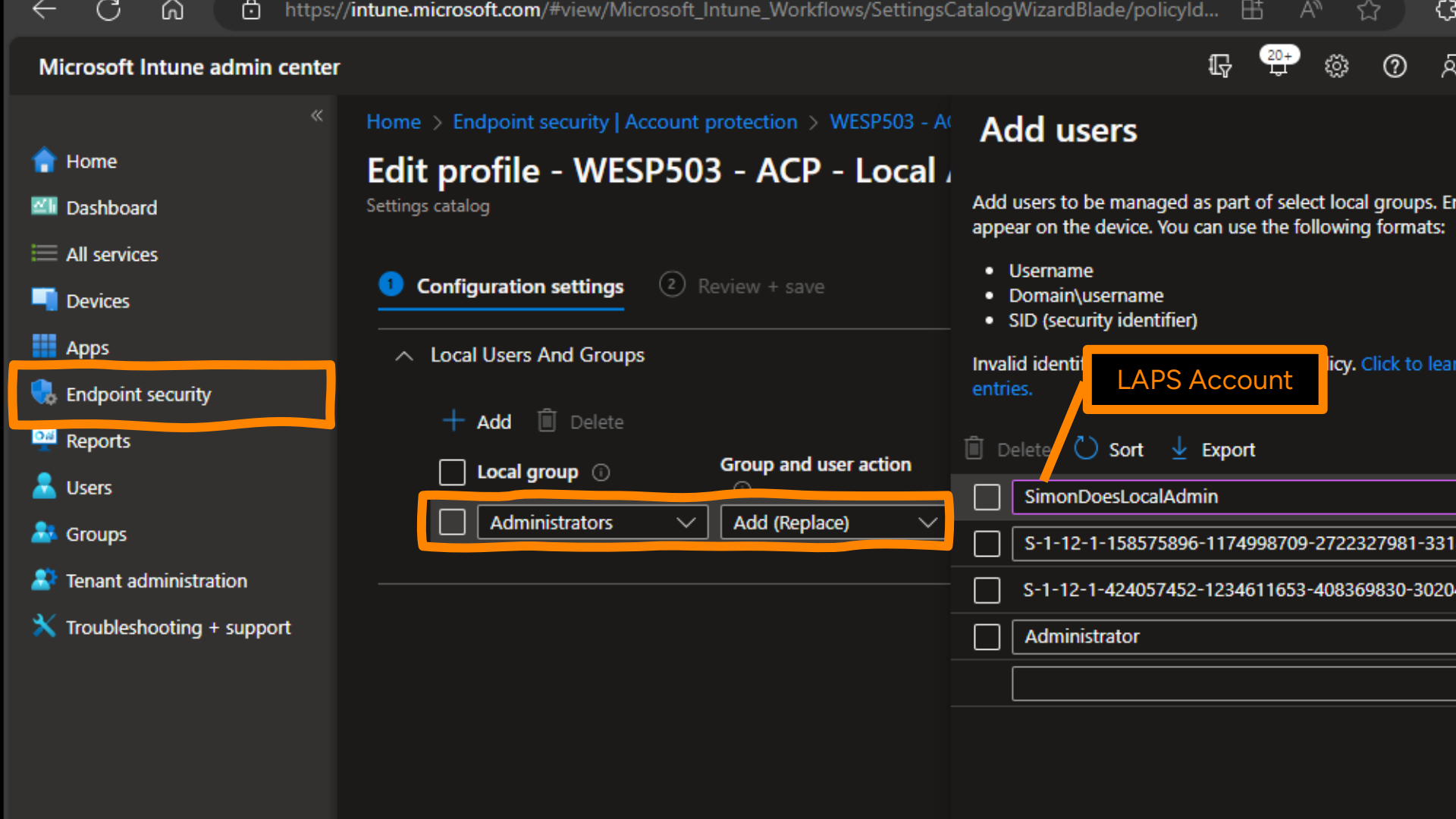
WESP502 - ACP - Windows LAPS — Local admin password solution

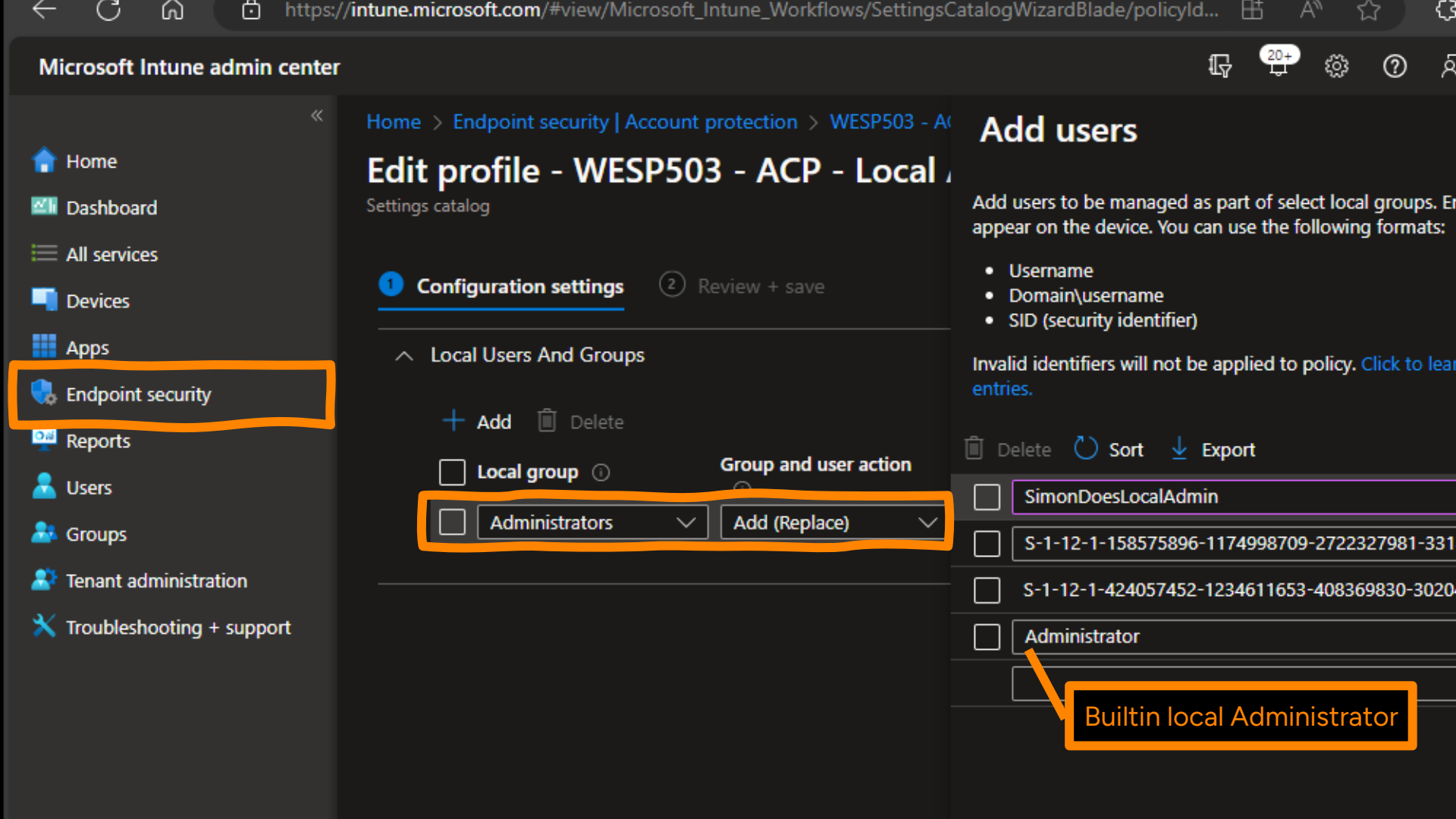
WESP503 - ACP - Local Administrators — Local user group membership

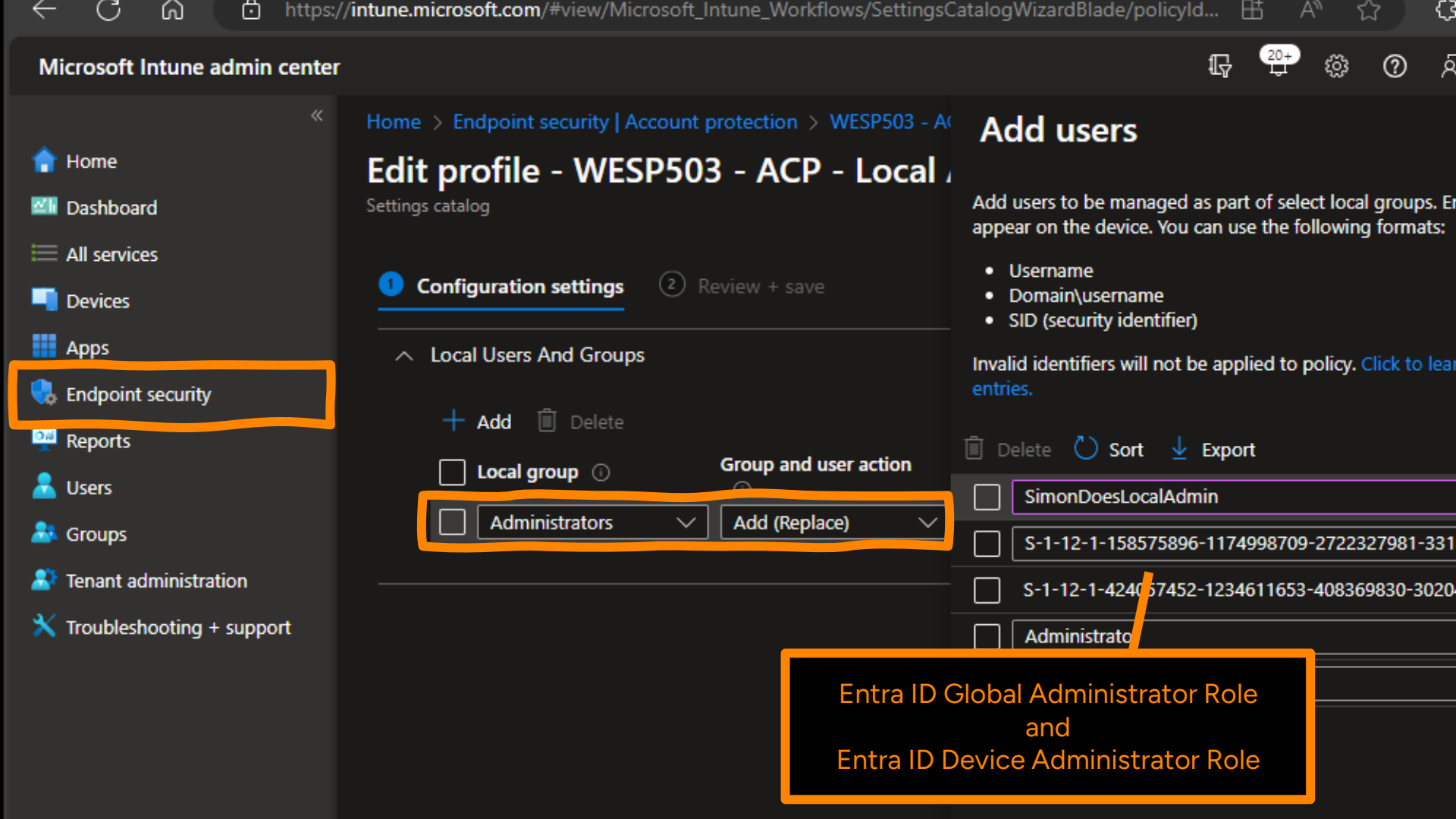

Windows Terminal can be set as the default terminal application in your settings. Open Settings
PS C:\> net localgroup administrators /add "AzureAD\leo.fender@skotheimsvik.no"
The command completed successfully.
Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Description
Access Control Assista...
Members of
Administrators
Administrato
Backup Operators
Backup Ope
Cryptographic Operat...
Members ar
Device Owners
Members of
Distributed COM Users
Members ar
Event Log Readers
Members of
Guests
Guests have
Hyper-V Administrators
Members of
IIS_IUSRS
Built-in grou
Network Configuratio...
Members in
Administrators Properties
General
Administrators
Description:
Administrators have complete and unrestricted access
the computer/domain
Members:
Administrator
AzureAD\LeoFender (S-1-12-1-327048103-1134952285-288455619
Kraken
S-1-12-1-3875837940-1152448851-4140974987-259402904
S-1-12-1-495264391-1255272342-2366988979-2198609934

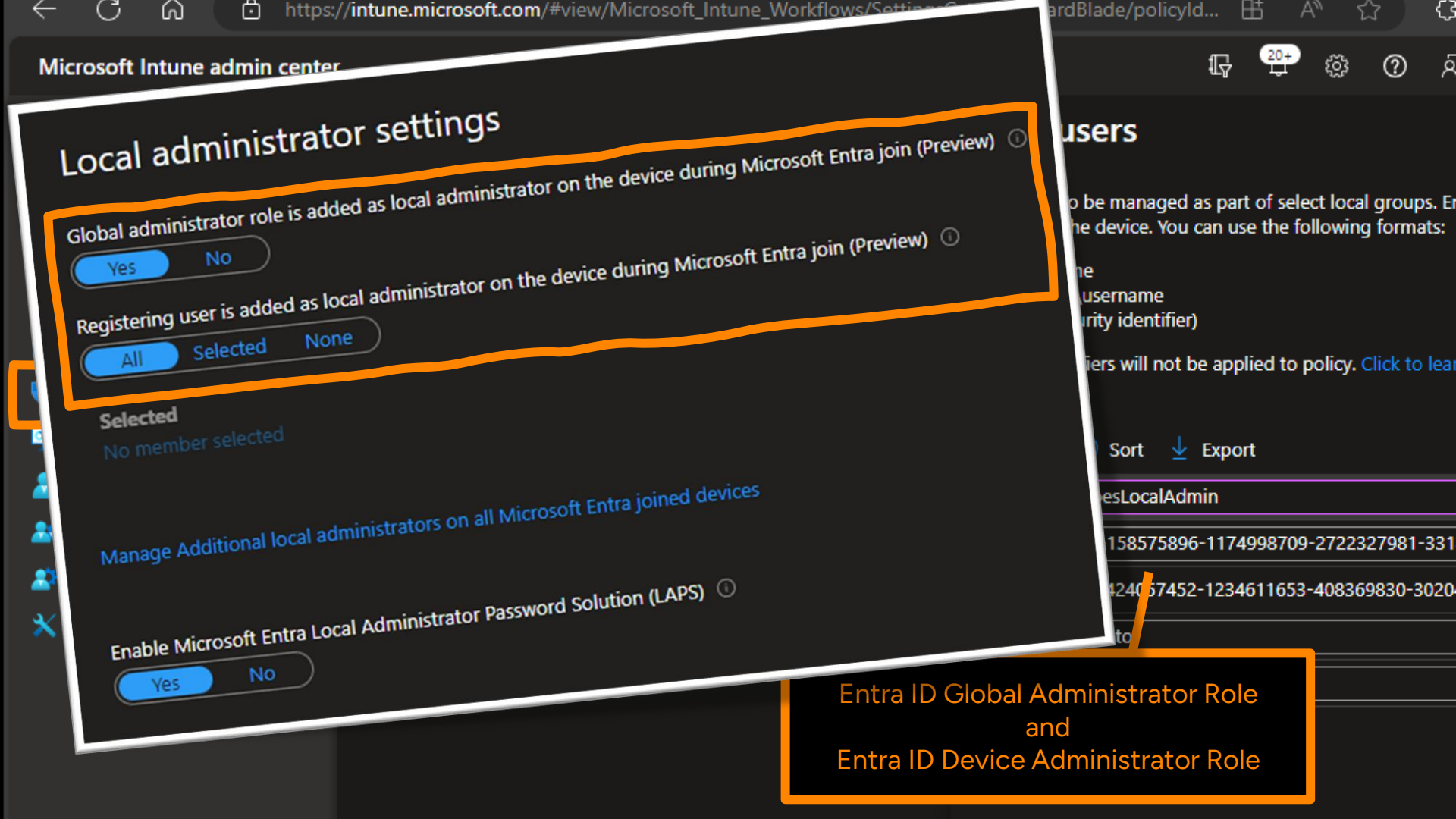

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Account protection
Search
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Monitor
Assignment failures
Setup
Microsoft Defender for Endpoint
Help and support
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

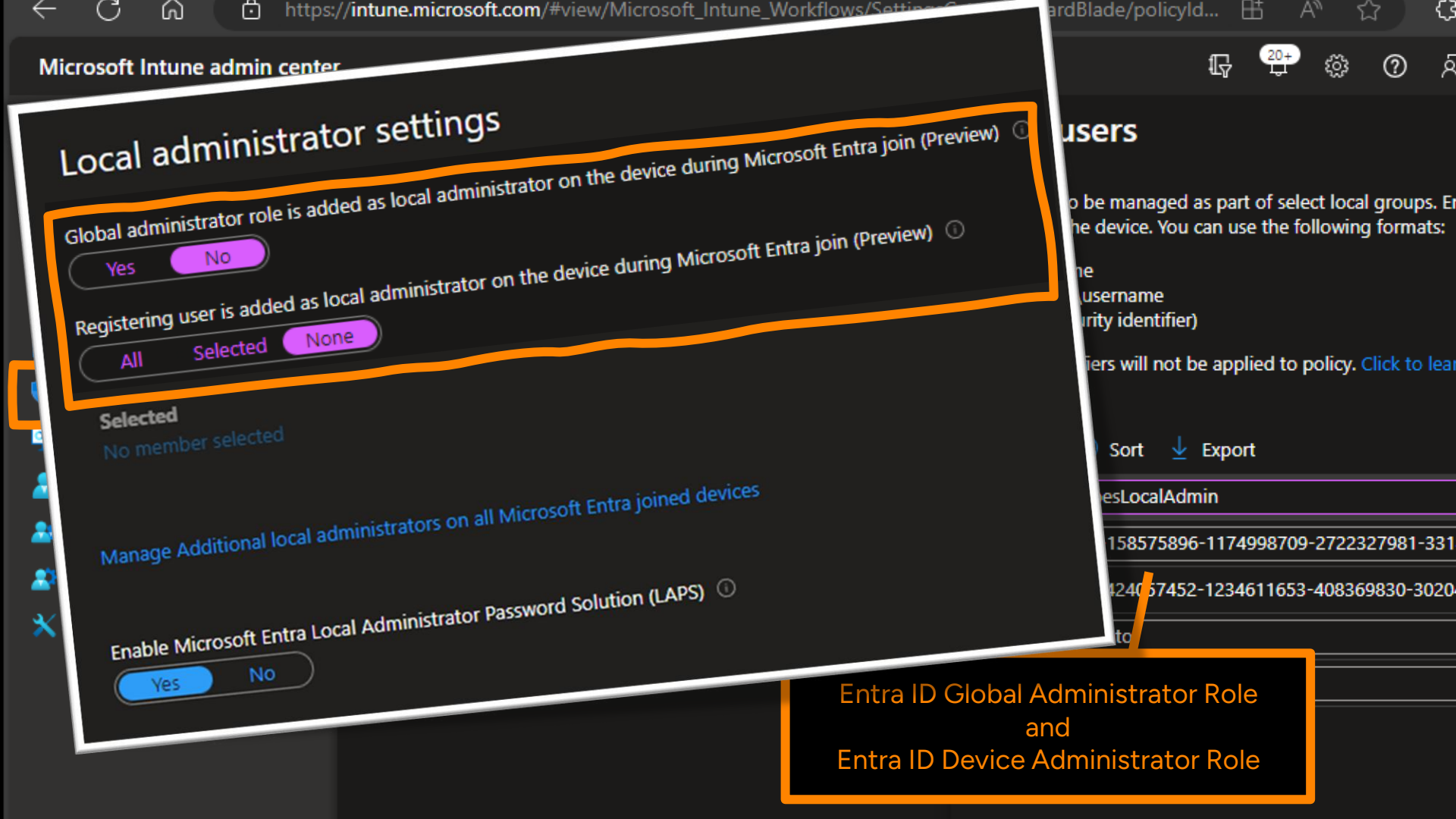

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SettingsCatalogWizardBlade/policyId...
Microsoft Intune admin center
20+
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP503 - A
Edit profile - WESP503 - ACP - Local
Settings catalog
1 Configuration settings
2 Review + save
Local Users And Groups
Add
Delete
Local group
Group and user action
Administrators
Add (Replace)
Add users
Add users to be managed as part of select local groups. E
appear on the device. You can use the following formats:
Username
Domain\username
SID (security identifier)
Invalid identifiers will not be applied to policy. Click to lea
entries.
Delete
Sort
Export
SimonDoesLocalAdmin
S-1-12-1-158575896-1174998709-2722327981-331
S-1-12-1-424057452-1234611653-408369830-3020
Administrator

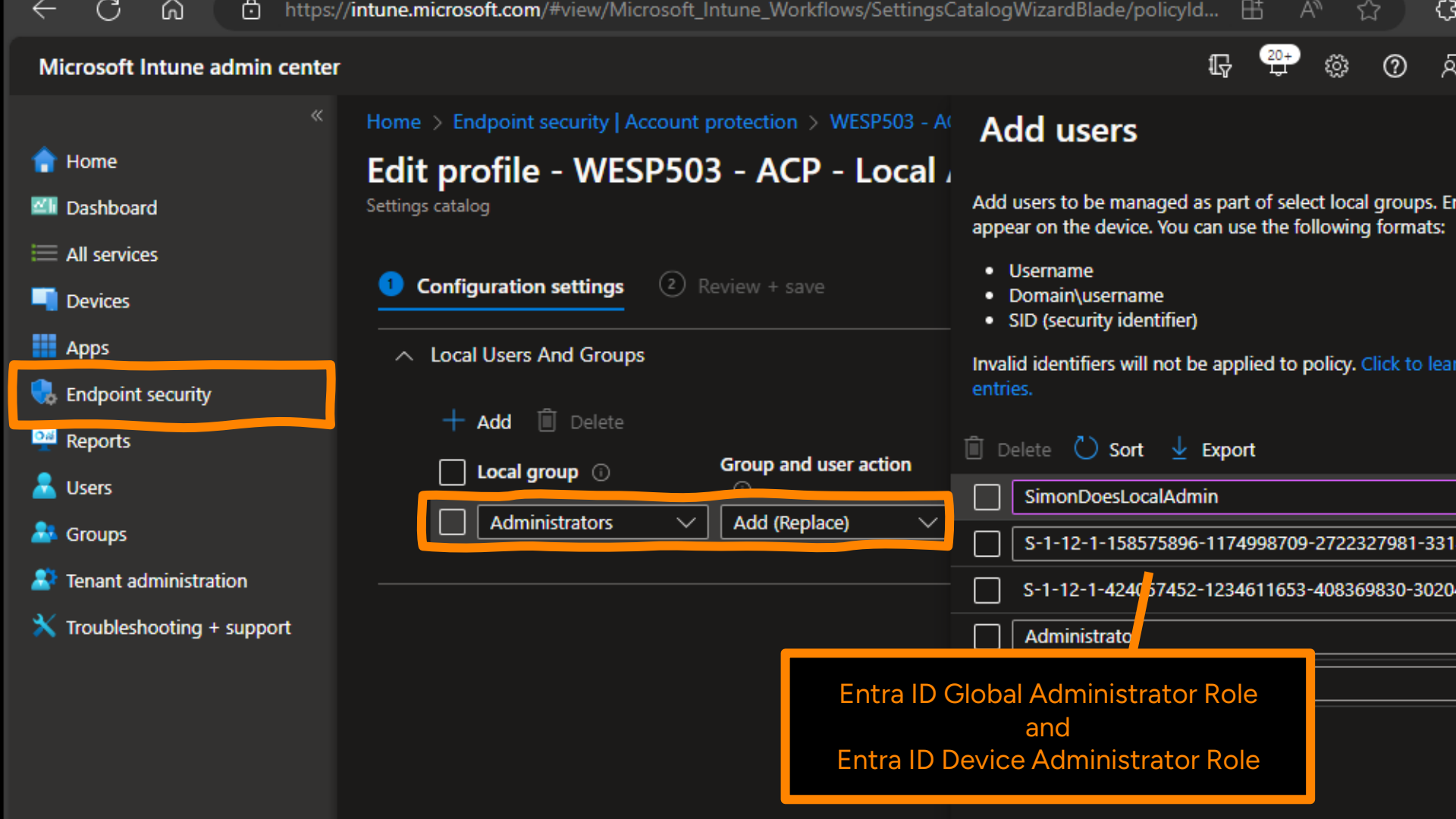

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SettingsCatalogWizardBlade/policyId...
Microsoft Intune admin center
20+
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP503 - A
Edit profile - WESP503 - ACP - Local
Settings catalog
1 Configuration settings
2 Review + save
Local Users And Groups
Add
Delete
Local group
Group and user action
Administrators
Add (Replace)
Add users
Add users to be managed as part of select local groups. E
appear on the device. You can use the following formats:
Username
Domain\username
SID (security identifier)
Invalid identi
icy. Click to lea
entries.
LAPS Account
Delete
Sort
Export
SimonDoesLocalAdmin
S-1-12-1-158575896-1174998709-2722327981-331
S-1-12-1-424057452-1234611653-408369830-3020
Administrator

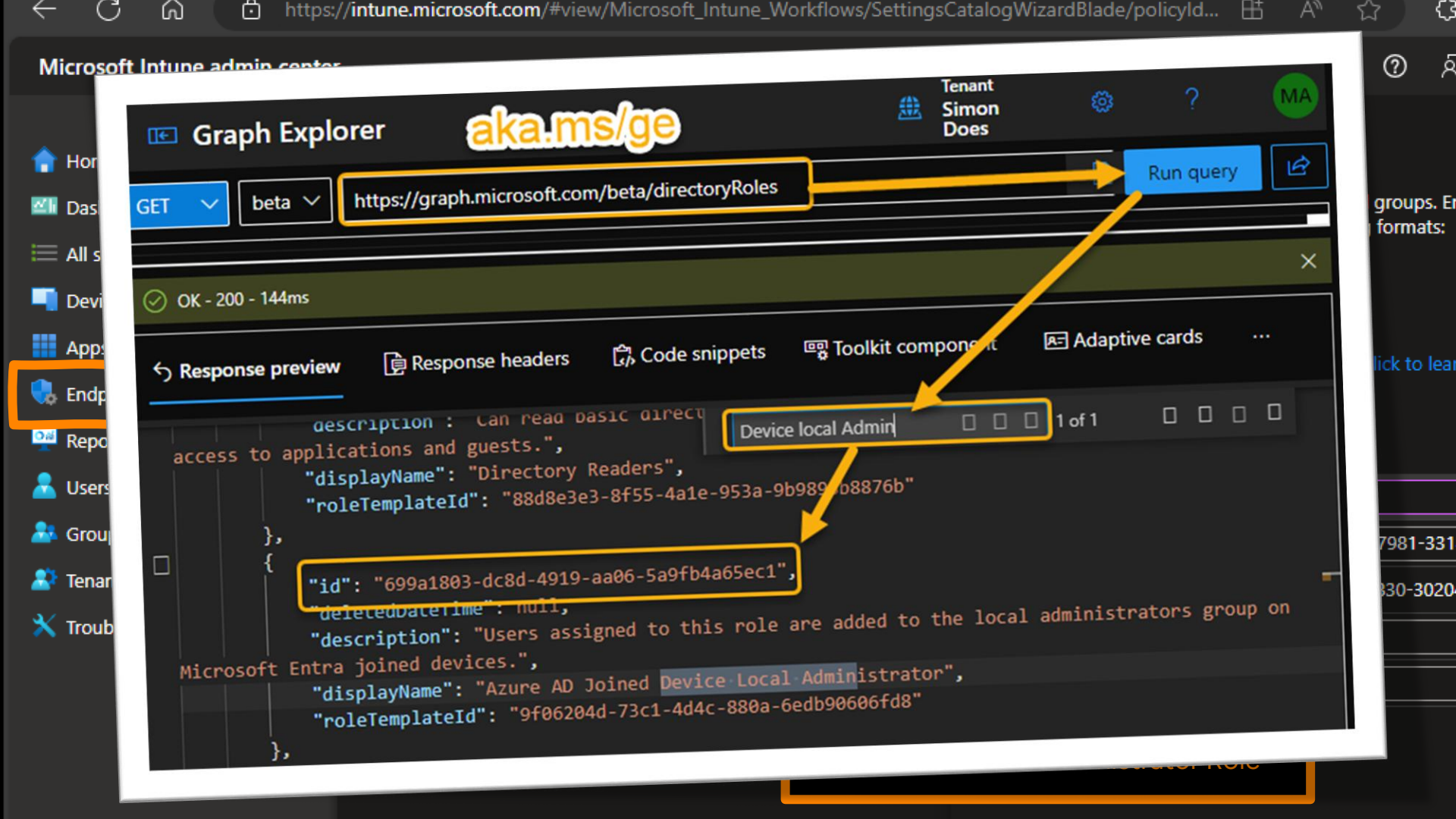

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SettingsCatalogWizardBlade/policyId...
Microsoft Intune admin center
20+
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP503 - A
Edit profile - WESP503 - ACP - Local
Settings catalog
1 Configuration settings
2 Review + save
Local Users And Groups
Add
Delete
Local group
Group and user action
Administrators
Add (Replace)
Add users
Add users to be managed as part of select local groups. E
appear on the device. You can use the following formats:
Username
Domain\username
SID (security identifier)
Invalid identifiers will not be applied to policy. Click to lea
entries.
Delete
Sort
Export
SimonDoesLocalAdmin
S-1-12-1-158575896-1174998709-2722327981-331
S-1-12-1-424057452-1234611653-408369830-3020
Administrator
Builtin local Administrator

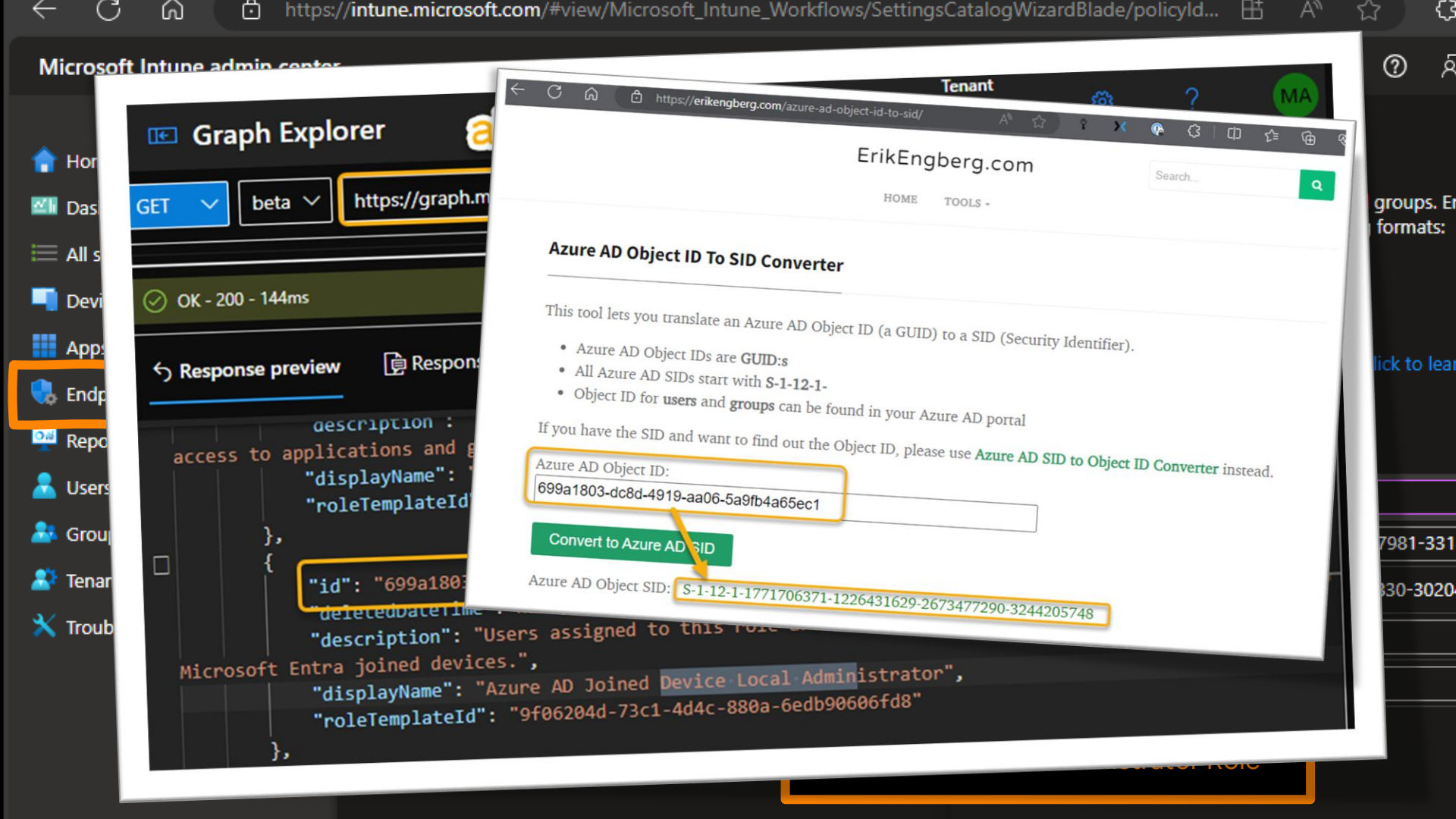

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SettingsCatalogWizardBlade/policyId...
Microsoft Intune admin center
20+
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP503 - A
Edit profile - WESP503 - ACP - Local
Settings catalog
1 Configuration settings
2 Review + save
Local Users And Groups
Add
Delete
Local group
Group and user action
Administrators
Add (Replace)
Add users
Add users to be managed as part of select local groups. E
appear on the device. You can use the following formats:
Username
Domain\username
SID (security identifier)
Invalid identifiers will not be applied to policy. Click to lea
entries.
Delete
Sort
Export
SimonDoesLocalAdmin
S-1-12-1-158575896-1174998709-2722327981-331
S-1-12-1-424
67452-1234611653-408369830-3020
Administrato
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

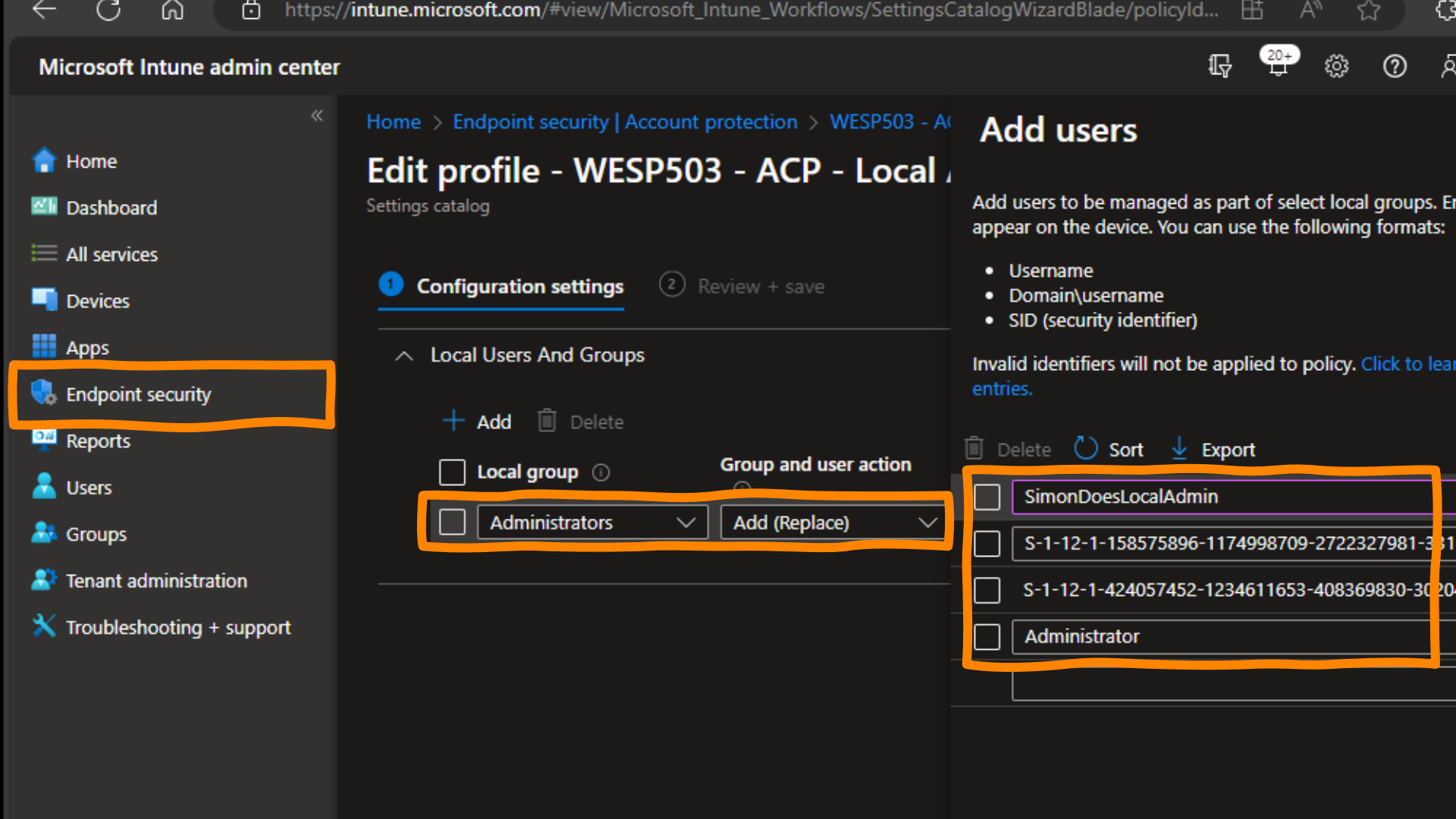

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/Setting
Microsoft Intune admin center
20+
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Yes
No
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
All
Selected
None
Selected
No member selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Yes
No
users
be managed as part of select local groups. En
he device. You can use the following formats:
ne
username
rity identifier)
iers will not be applied to policy. Click to lear
Sort
Export
esLocalAdmin
158575896-1174998709-2722327981-331
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

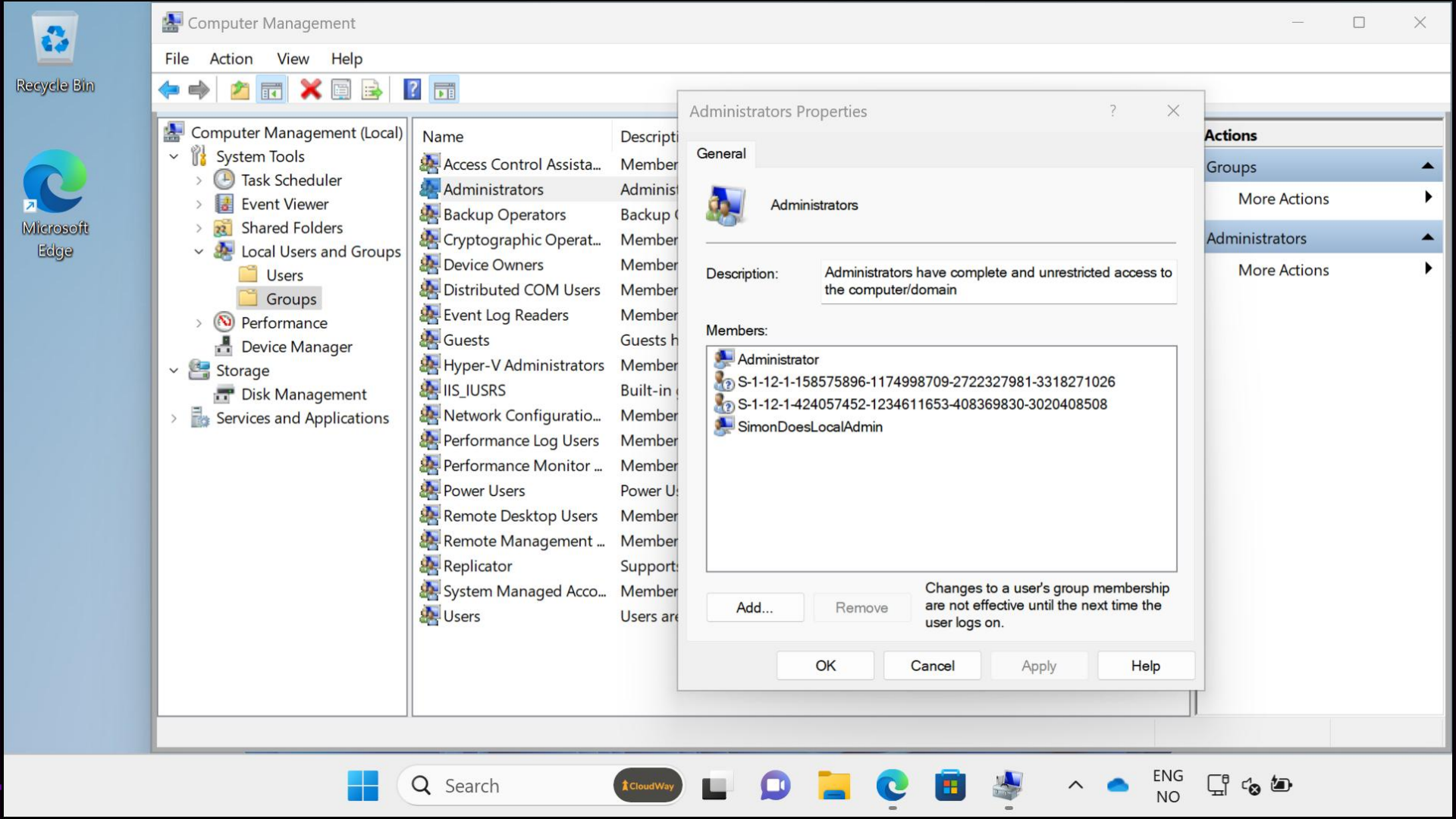

Microsoft Intune admin center
Local administrator settings
Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)
Yes
No
Registering user is added as local administrator on the device during Microsoft Entra join (Preview)
All
Selected
None
Selected
No member selected
Manage Additional local administrators on all Microsoft Entra joined devices
Enable Microsoft Entra Local Administrator Password Solution (LAPS)
Yes
No
Sort
Export
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

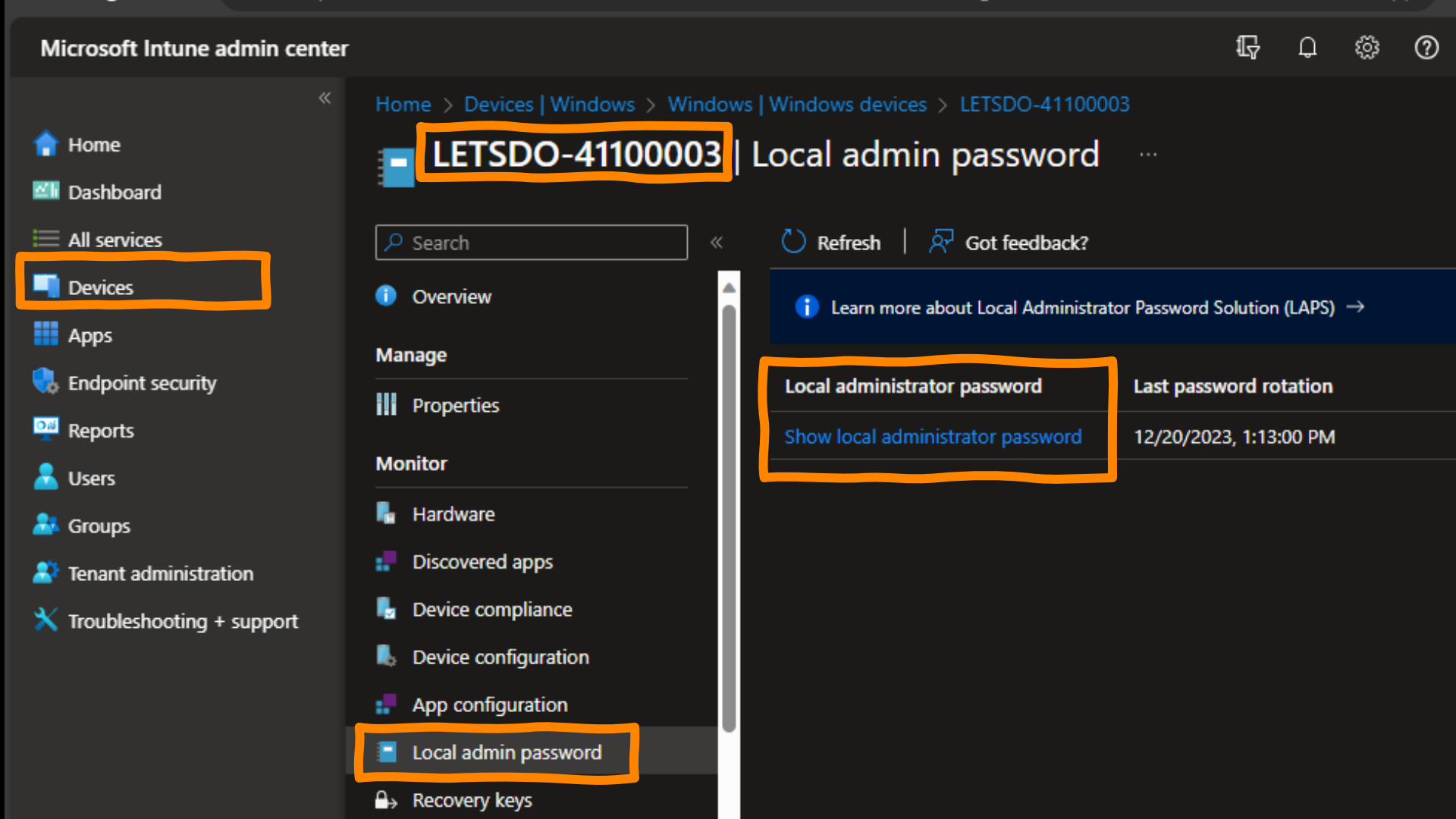

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SettingsCatalogWizardBlade/policyId...
Microsoft Intune admin center
20+
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP503 - A
Edit profile - WESP503 - ACP - Local
Settings catalog
1 Configuration settings
2 Review + save
Local Users And Groups
Add
Delete
Local group
Group and user action
Administrators
Add (Replace)
Add users
Add users to be managed as part of select local groups. E
appear on the device. You can use the following formats:
Username
Domain\username
SID (security identifier)
Invalid identifiers will not be applied to policy. Click to lea
entries.
Delete
Sort
Export
SimonDoesLocalAdmin
S-1-12-1-158575896-1174998709-2722327981-331
S-1-12-1-424
67452-1234611653-408369830-3020
Administrato
Entra ID Global Administrator Role
and
Entra ID Device Administrator Role

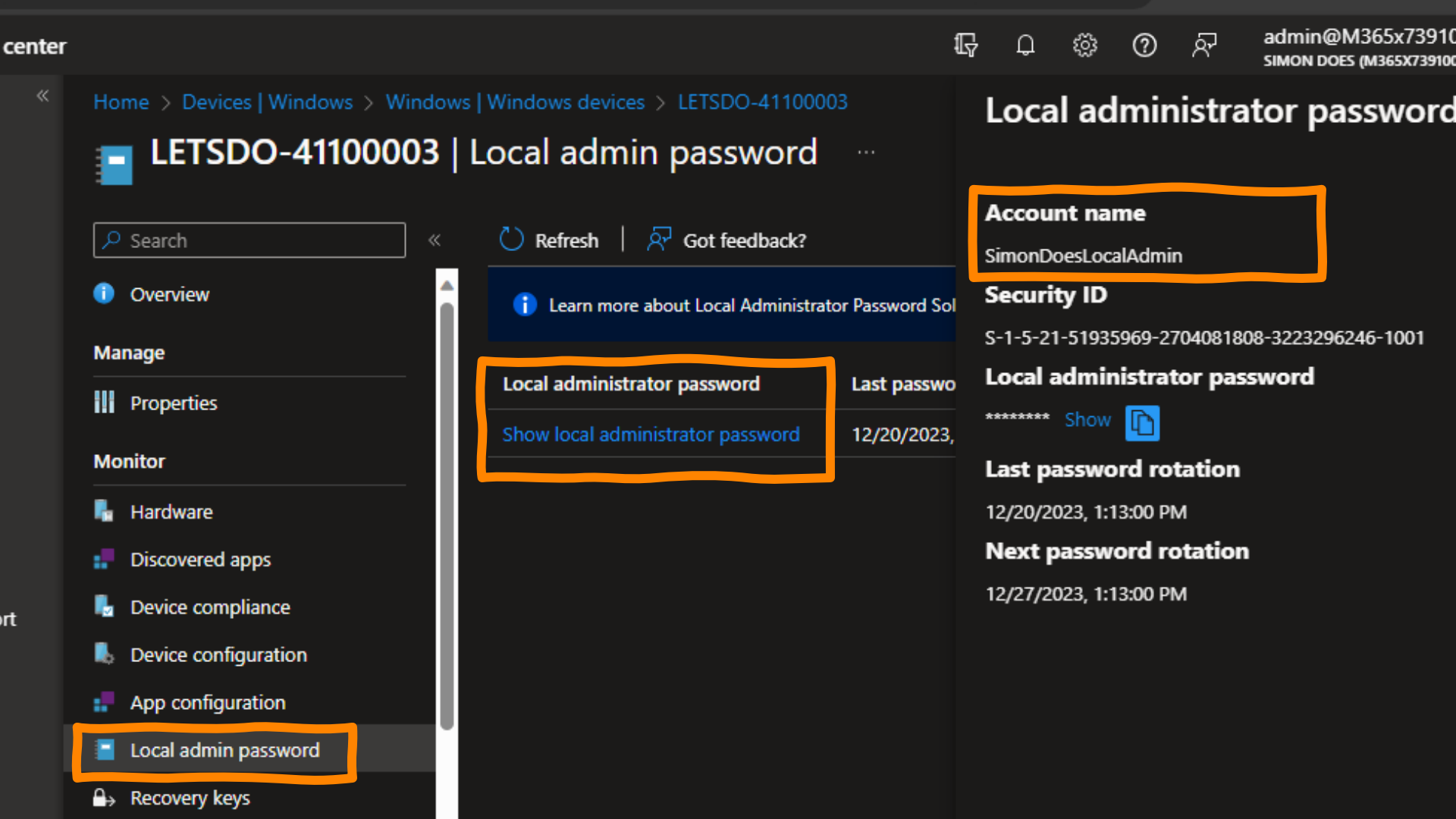

Graph Explorer
aka.ms/ge
Tenant
Simon
Does
MA
GET
beta
https://graph.microsoft.com/beta/directoryRoles
Run query
OK - 200 - 144ms
Response preview
Response headers
Code snippets
Toolkit component
Adaptive cards
Device local Admin
1 of 1
access to applications and guests.",
"displayName": "Directory Readers",
"roleTemplateId": "88d8e3e3-8f55-4a1e-953a-9b9898b8876b"
},
{
"id": "699a1803-dc8d-4919-aa06-5a9fb4a65ec1",
"description": "Users assigned to this role are added to the local administrators group on
Microsoft Entra joined devices.",
"displayName": "Azure AD Joined Device Local Administrator",
"roleTemplateId": "9f06204d-73c1-4d4c-880a-6edb90606fd8"
},

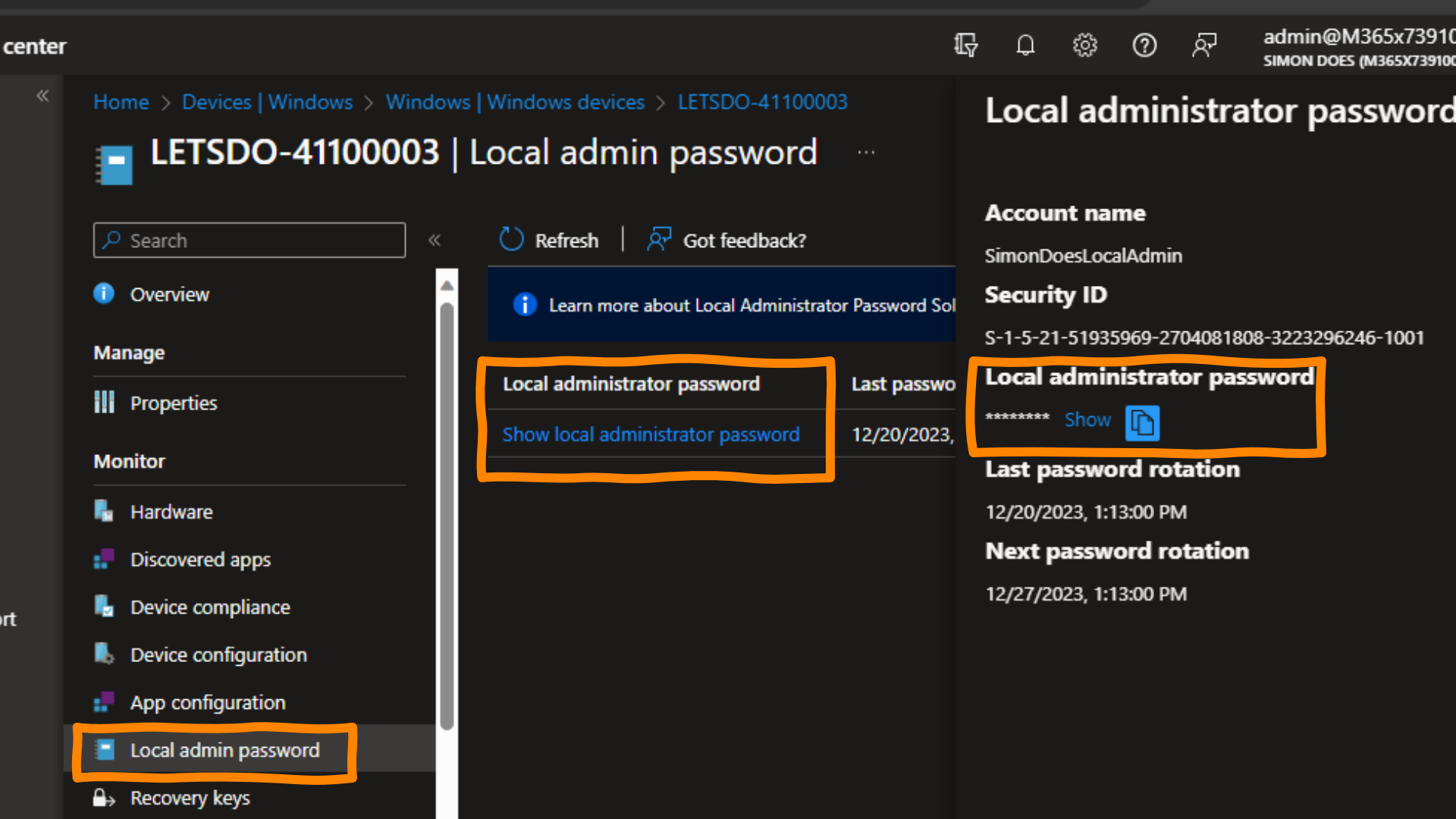

Graph Explorer
GET
beta
https://graph.m
OK - 200 - 144ms
Response preview
"description": "Users assigned to this role
Microsoft Entra joined devices.",
"displayName": "Azure AD Joined Device Local Administrator",
"roleTemplateId": "9f06204d-73c1-4d4c-880a-6edb90606fd8"
Tenant
https://erikengberg.com/azure-ad-object-id-to-sid/
ErikEngberg.com
HOME
TOOLS
Azure AD Object ID To SID Converter
This tool lets you translate an Azure AD Object ID (a GUID) to a SID (Security Identifier).
Azure AD Object IDs are GUID:s
All Azure AD SIDs start with S-1-12-1-
Object ID for users and groups can be found in your Azure AD portal
If you have the SID and want to find out the Object ID, please use Azure AD SID to Object ID Converter instead.
Azure AD Object ID:
699a1803-dc8d-4919-aa06-5a9fb4a65ec1
Convert to Azure AD SID
Azure AD Object SID:
S-1-12-1-1771706371-1226431629-2673477290-3244205748

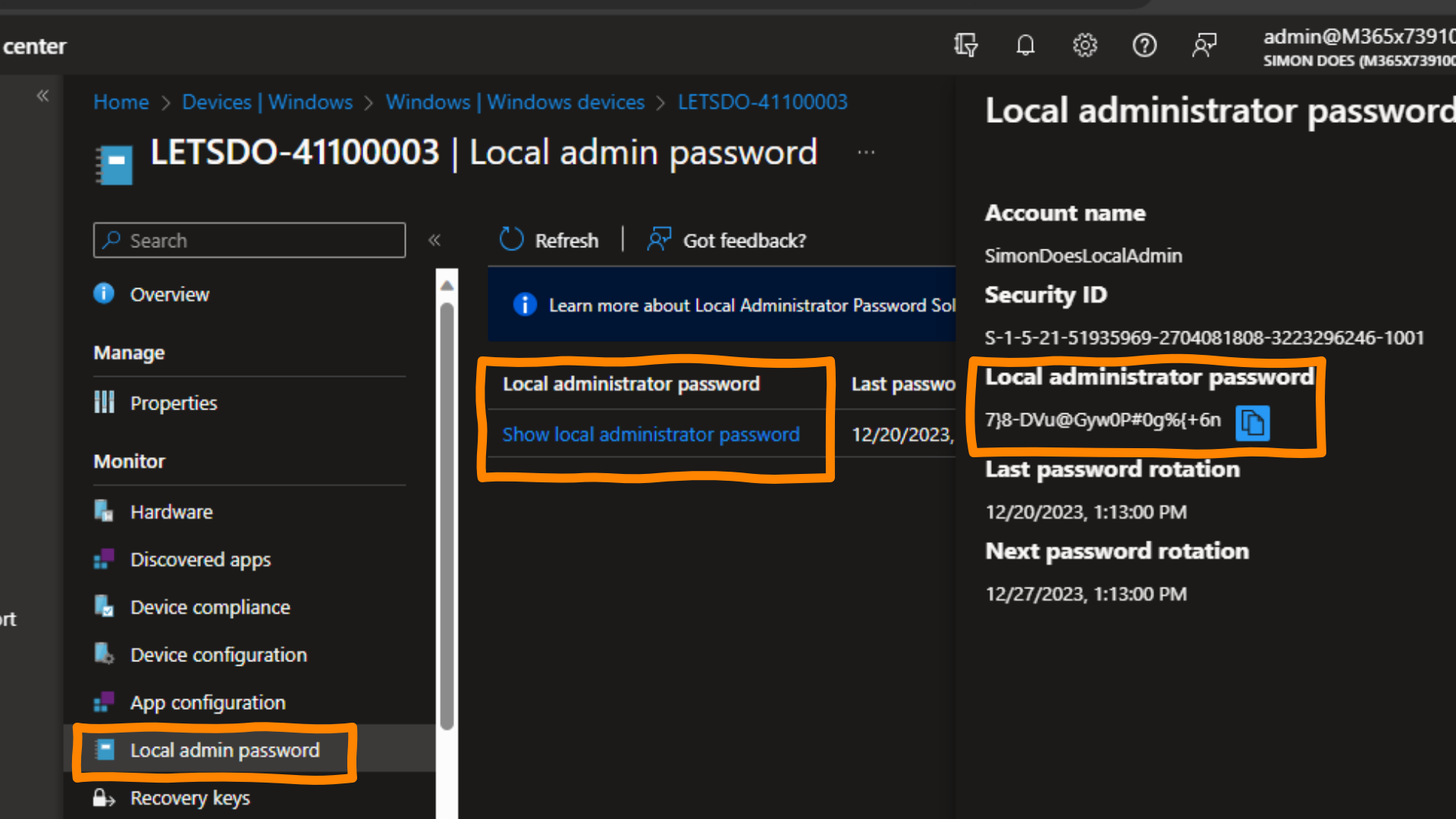

https://intune.microsoft.com/#view/Microsoft_Intune_Workflows/SettingsCatalogWizardBlade/policyId...
Microsoft Intune admin center
20+
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > WESP503 - A
Edit profile - WESP503 - ACP - Local
Settings catalog
1 Configuration settings
2 Review + save
Local Users And Groups
Add
Delete
Local group
Group and user action
Administrators
Add (Replace)
Add users
Add users to be managed as part of select local groups. E
appear on the device. You can use the following formats:
Username
Domain\username
SID (security identifier)
Invalid identifiers will not be applied to policy. Click to lea
entries.
Delete
Sort
Export
SimonDoesLocalAdmin
S-1-12-1-158575896-1174998709-2722327981-3
S-1-12-1-424057452-1234611653-408369830-30
Administrator

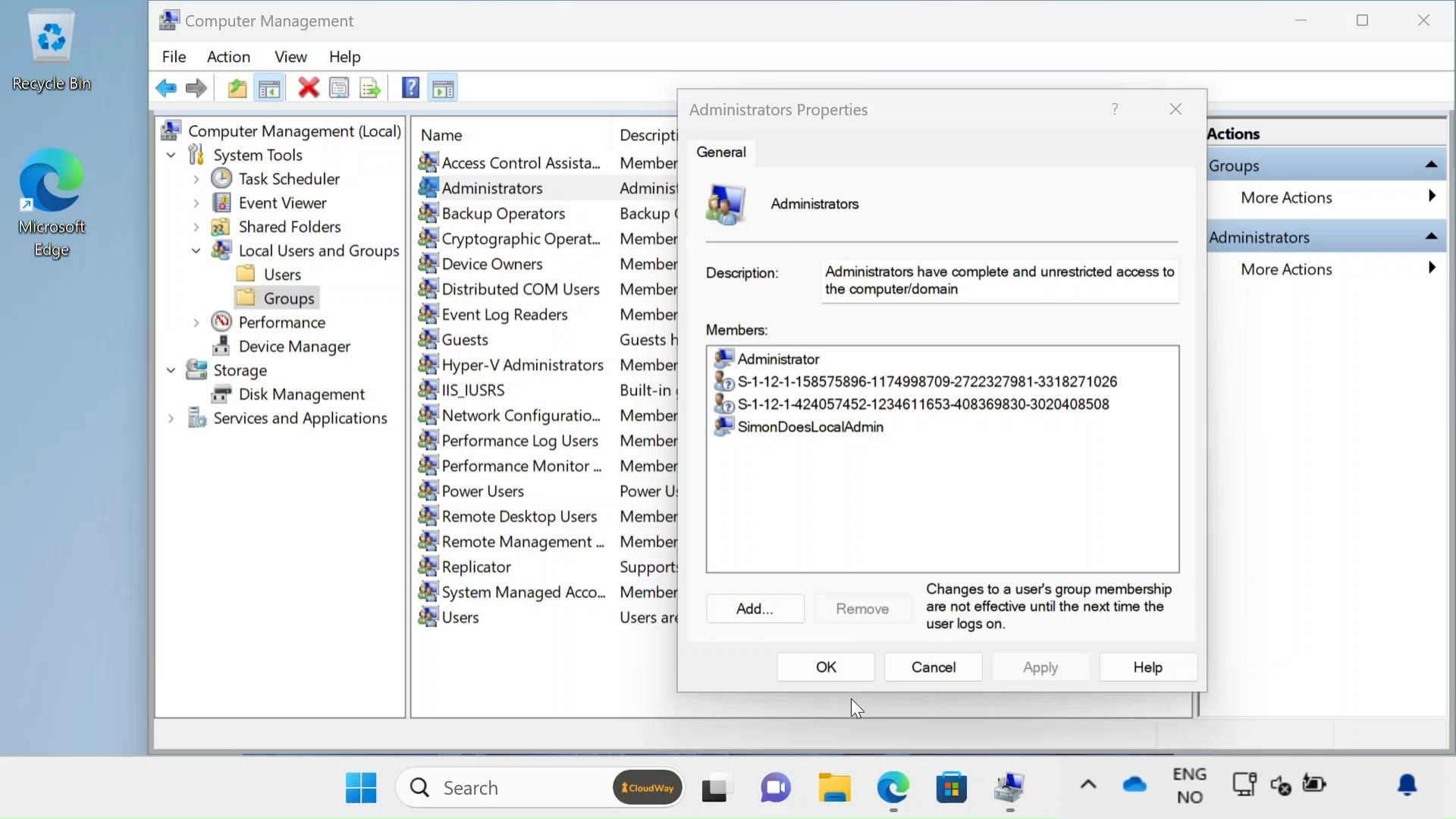

Recycle Bin
Microsoft Edge
Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Access Control Assista...
Administrators
Backup Operators
Cryptographic Operat...
Device Owners
Distributed COM Users
Event Log Readers
Guests
Hyper-V Administrators
IIS_IUSRS
Network Configuratio...
Performance Log Users
Performance Monitor ...
Power Users
Remote Desktop Users
Remote Management ...
Replicator
System Managed Acco...
Users
Actions
Groups
More Actions
Administrators
More Actions
Administrators Properties
General
Administrators
Description:
Administrators have complete and unrestricted access to the computer/domain
Members:
Administrator
S-1-12-1-158575896-1174998709-2722327981-3318271026
S-1-12-1-424057452-1234611653-408369830-3020408508
SimonDoesLocalAdmin
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help
Search
CloudWay
ENG
NO


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Windows > Windows | Windows devices > LETSDO-41100003
LETSDO-41100003 | Local admin password
Search
Overview
Manage
Properties
Monitor
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Local admin password
Recovery keys
Refresh
Got feedback?
Learn more about Local Administrator Password Solution (LAPS)
Local administrator password
Last password rotation
Show local administrator password
12/20/2023, 1:13:00 PM


center
admin@M365x73910
SIMON DOES (M365X739100
Home > Devices | Windows > Windows | Windows devices > LETSDO-41100003
LETSDO-41100003 | Local admin password
Search
Refresh
Got feedback?
Overview
Manage
Properties
Monitor
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Local admin password
Recovery keys
Learn more about Local Administrator Password Sol
Local administrator password
Last passwo
Show local administrator password
12/20/2023,
Local administrator password
Account name
SimonDoesLocalAdmin
Security ID
S-1-5-21-51935969-2704081808-3223296246-1001
Local administrator password
******** Show
Last password rotation
12/20/2023, 1:13:00 PM
Next password rotation
12/27/2023, 1:13:00 PM


center
admin@M365x73910
SIMON DOES (M365X739100
Home > Devices | Windows > Windows | Windows devices > LETSDO-41100003
LETSDO-41100003 | Local admin password
Search
Refresh
Got feedback?
Overview
Manage
Properties
Monitor
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Local admin password
Recovery keys
Learn more about Local Administrator Password Sol
Local administrator password
Last passwo
Show local administrator password
12/20/2023,
Local administrator password
******** Show
Last password rotation
12/20/2023, 1:13:00 PM
Next password rotation
12/27/2023, 1:13:00 PM
Local administrator password
Account name
SimonDoesLocalAdmin
Security ID
S-1-5-21-51935969-2704081808-3223296246-1001


center
admin@M365x73910
SIMON DOES (M365X739100
Home > Devices | Windows > Windows | Windows devices > LETSDO-41100003
LETSDO-41100003 | Local admin password
Search
Refresh
Got feedback?
Overview
Manage
Properties
Monitor
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Local admin password
Recovery keys
Learn more about Local Administrator Password Sol
Local administrator password
Last passwo
Show local administrator password
12/20/2023,
Local administrator password
Account name
SimonDoesLocalAdmin
Security ID
S-1-5-21-51935969-2704081808-3223296246-1001
Local administrator password
7}8-DVu@Gyw0P#0g%{+6n
Last password rotation
12/20/2023, 1:13:00 PM
Next password rotation
12/27/2023, 1:13:00 PM


Recycle Bin
Microsoft Edge
Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Access Control Assista...
Administrators
Backup Operators
Cryptographic Operat...
Device Owners
Distributed COM Users
Event Log Readers
Guests
Hyper-V Administrators
IIS_IUSRS
Network Configuratio...
Performance Log Users
Performance Monitor ...
Power Users
Remote Desktop Users
Remote Management ...
Replicator
System Managed Acco...
Users
Actions
Groups
More Actions
Administrators
More Actions
Administrators Properties
General
Administrators
Description:
Administrators have complete and unrestricted access to the computer/domain
Members:
Administrator
S-1-12-1-158575896-1174998709-2722327981-3318271026
S-1-12-1-424057452-1234611653-408369830-3020408508
SimonDoesLocalAdmin
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help
Search
CloudWay
ENG
NO

6

How?

Can we do stuff?

I NEED LAPS!

NIC
EMPOWER

6

How?

Can we do stuff?

I NEED LAPS!

Local Admin Access

NIC
EMPOWER

6

How?

Can we do stuff?

I NEED LAPS!

Local Admin Access

NIC
EMPOWER

Local Admin Access

NIC
EMPOWER

Local Admin Access

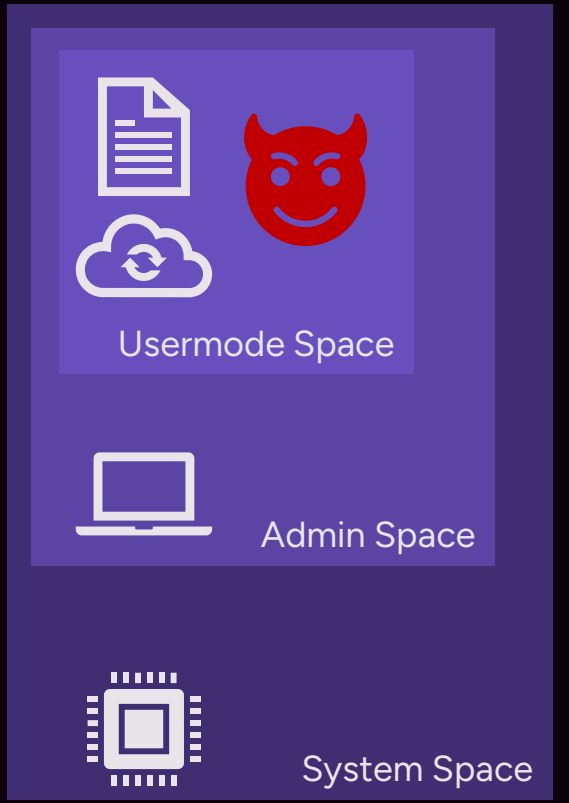
Usermode Space

Admin Space

System Space

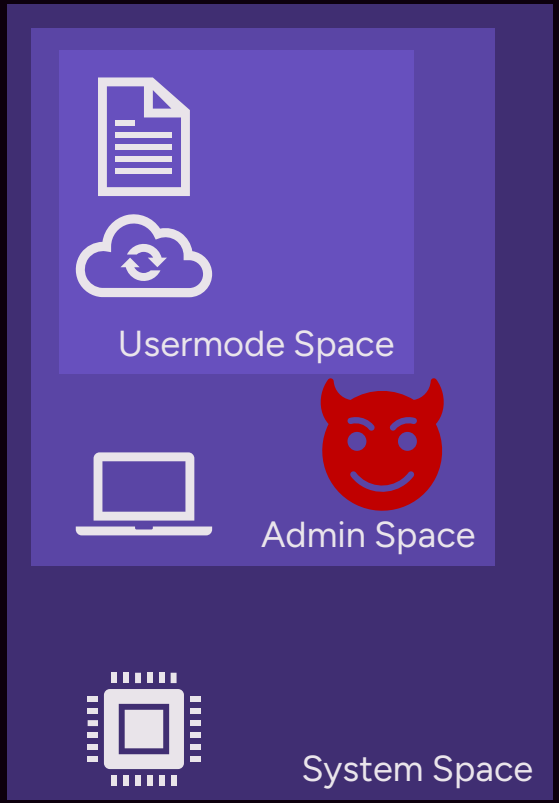
NIC
EMPOWER

Local Admin Access



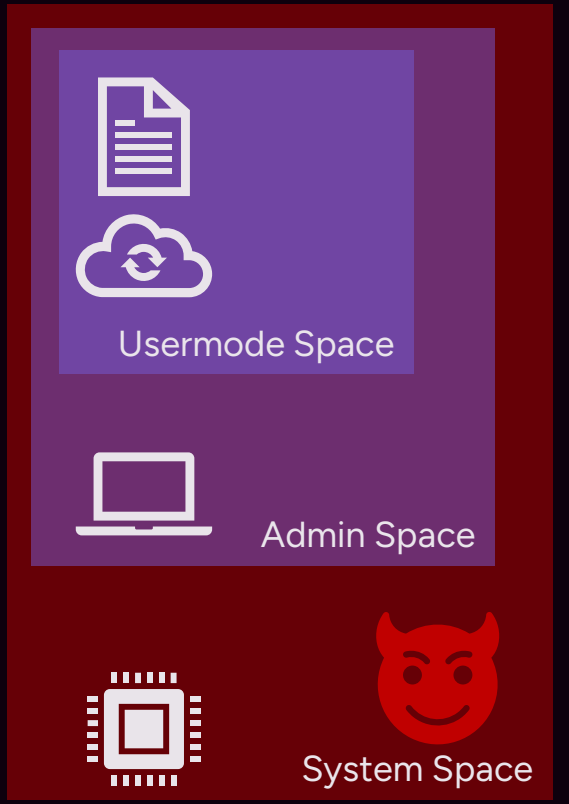
NIC
EMPOWER

Local Admin Access



NIC
EMPOWER

Local Admin Access



NIC
EMPOWER

6

How?

Can we do stuff?

I NEED LAPS!

Local Admin Access

NIC
EMPOWER

7

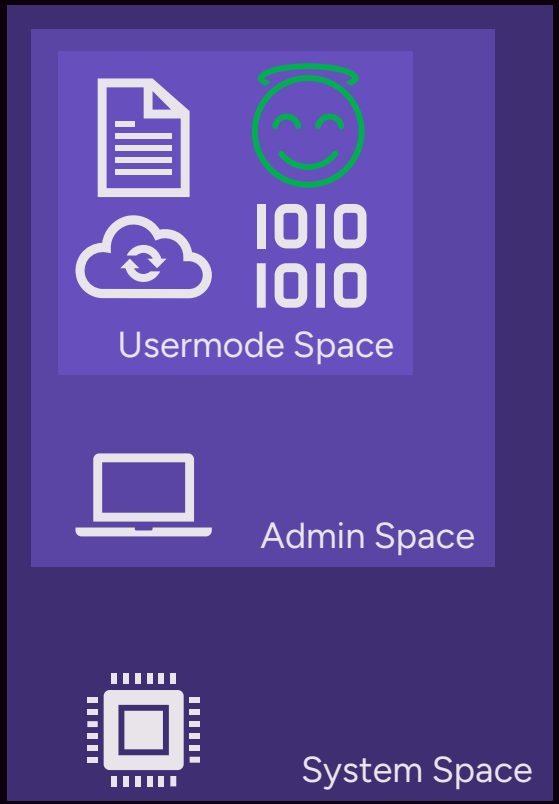
How?

Can we do stuff?

I NEED EPM!

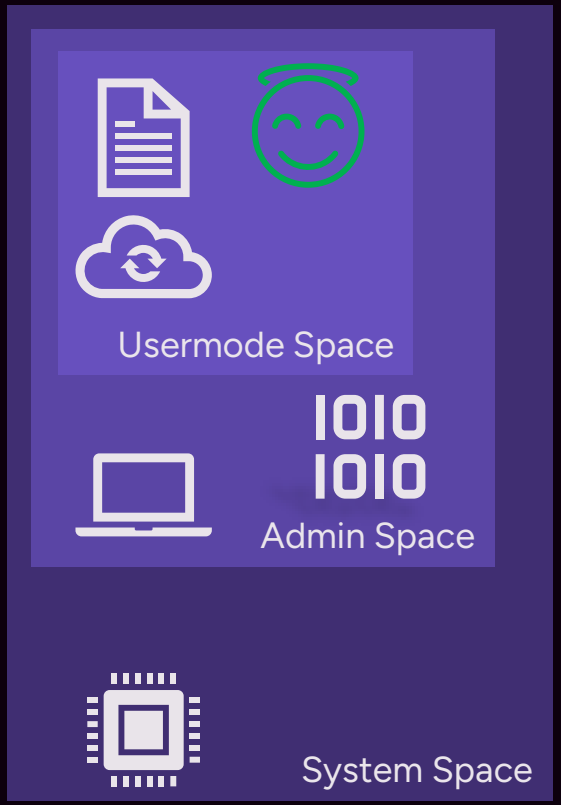
NIC
EMPOWER

Endpoint Privilege Management



NIC
EMPOWER

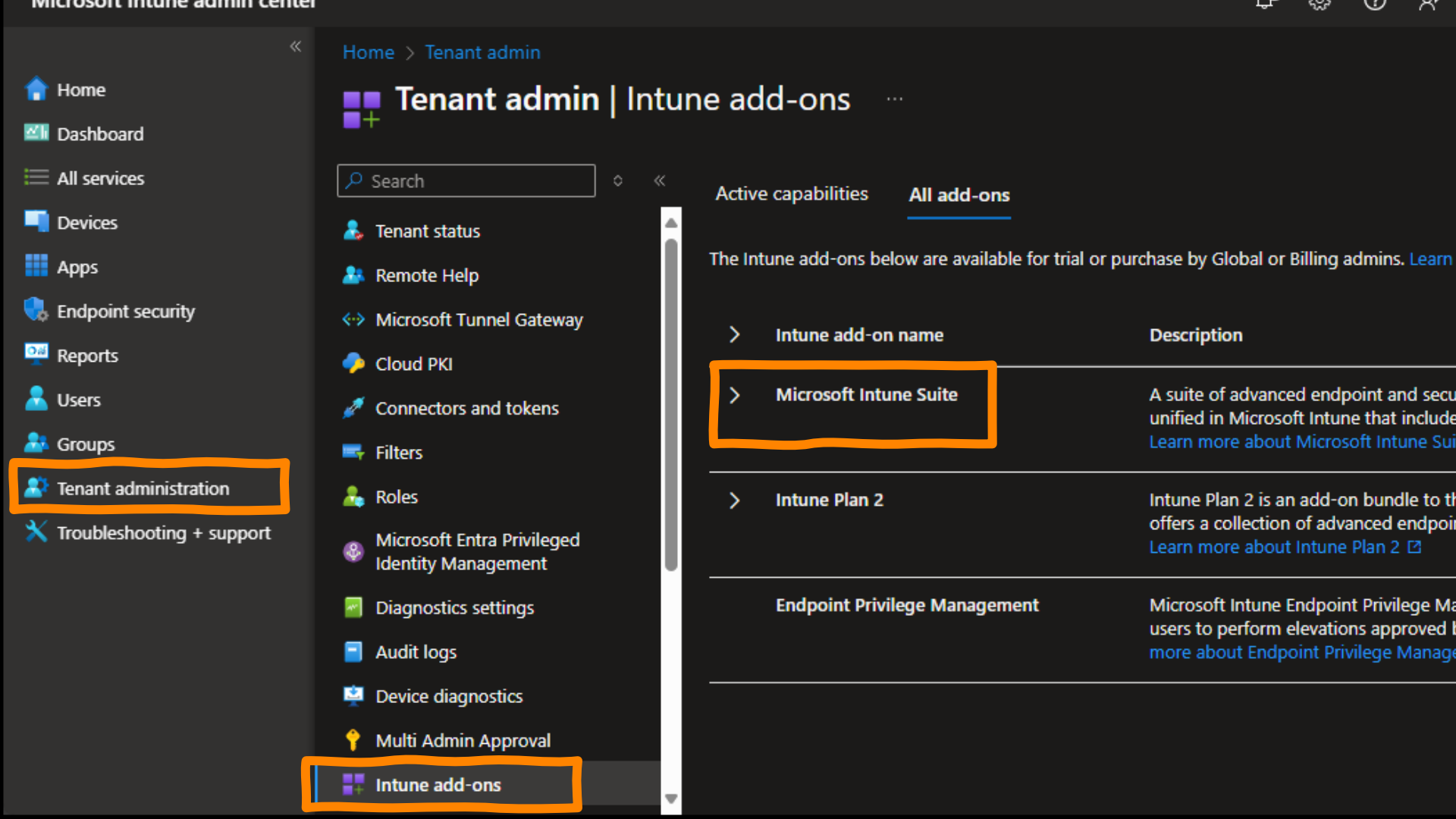
Endpoint Privilege Management

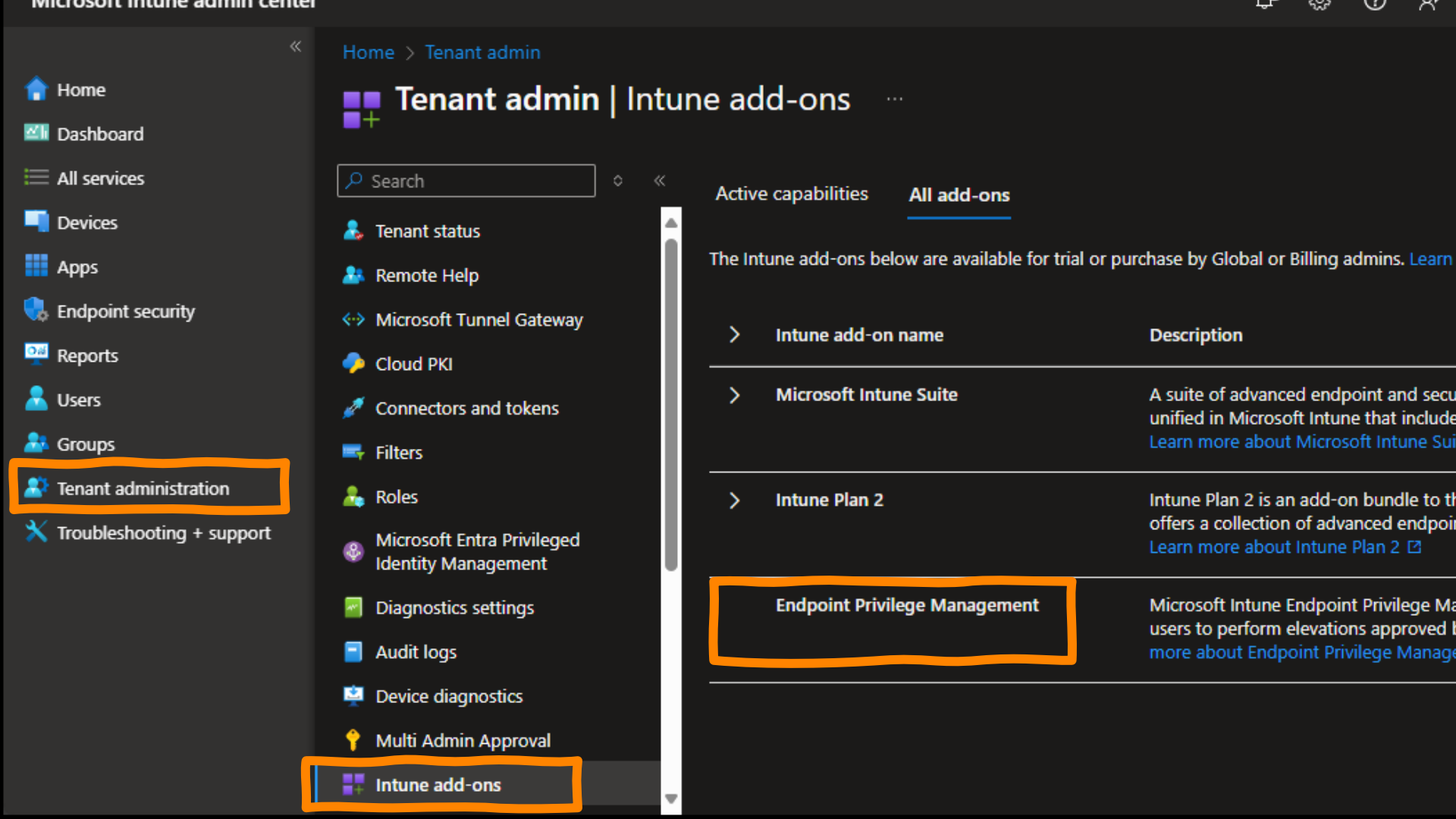


NIC
EMPOWER

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		✓	✓


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Intune add-ons
Search
Tenant status
Remote Help
Microsoft Tunnel Gateway
Cloud PKI
Connectors and tokens
Filters
Roles
Microsoft Entra Privileged Identity Management
Diagnostics settings
Audit logs
Device diagnostics
Multi Admin Approval
Intune add-ons
Active capabilities
All add-ons
The Intune add-ons below are available for trial or purchase by Global or Billing admins. Learn
Intune add-on name
Description
Microsoft Intune Suite
A suite of advanced endpoint and secu
unified in Microsoft Intune that include
Learn more about Microsoft Intune Sui
Intune Plan 2
Intune Plan 2 is an add-on bundle to th
offers a collection of advanced endpoi
Learn more about Intune Plan 2
Endpoint Privilege Management
Microsoft Intune Endpoint Privilege Ma
users to perform elevations approved b
more about Endpoint Privilege Manage


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Intune add-ons
Search
Tenant status
Remote Help
Microsoft Tunnel Gateway
Cloud PKI
Connectors and tokens
Filters
Roles
Microsoft Entra Privileged Identity Management
Diagnostics settings
Audit logs
Device diagnostics
Multi Admin Approval
Intune add-ons
Active capabilities
All add-ons
The Intune add-ons below are available for trial or purchase by Global or Billing admins. Learn
Intune add-on name
Description
Microsoft Intune Suite
A suite of advanced endpoint and secu
unified in Microsoft Intune that include
Learn more about Microsoft Intune Sui
Intune Plan 2
Intune Plan 2 is an add-on bundle to th
offers a collection of advanced endpoi
Learn more about Intune Plan 2
Endpoint Privilege Management
Microsoft Intune Endpoint Privilege Ma
users to perform elevations approved b
more about Endpoint Privilege Manage

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
EMPOWER

Endpoint Privilege Management (EPM)

- Trigger detection

🔎 EPM identifies a process

- Based on rules

👨‍💻 User selects ‘Run Elevated’

- Right click menu

Endpoint Privilege Management (EPM)

- Elevation Actions

🪄 Automatic

- Every time a binary launches, it is elevated

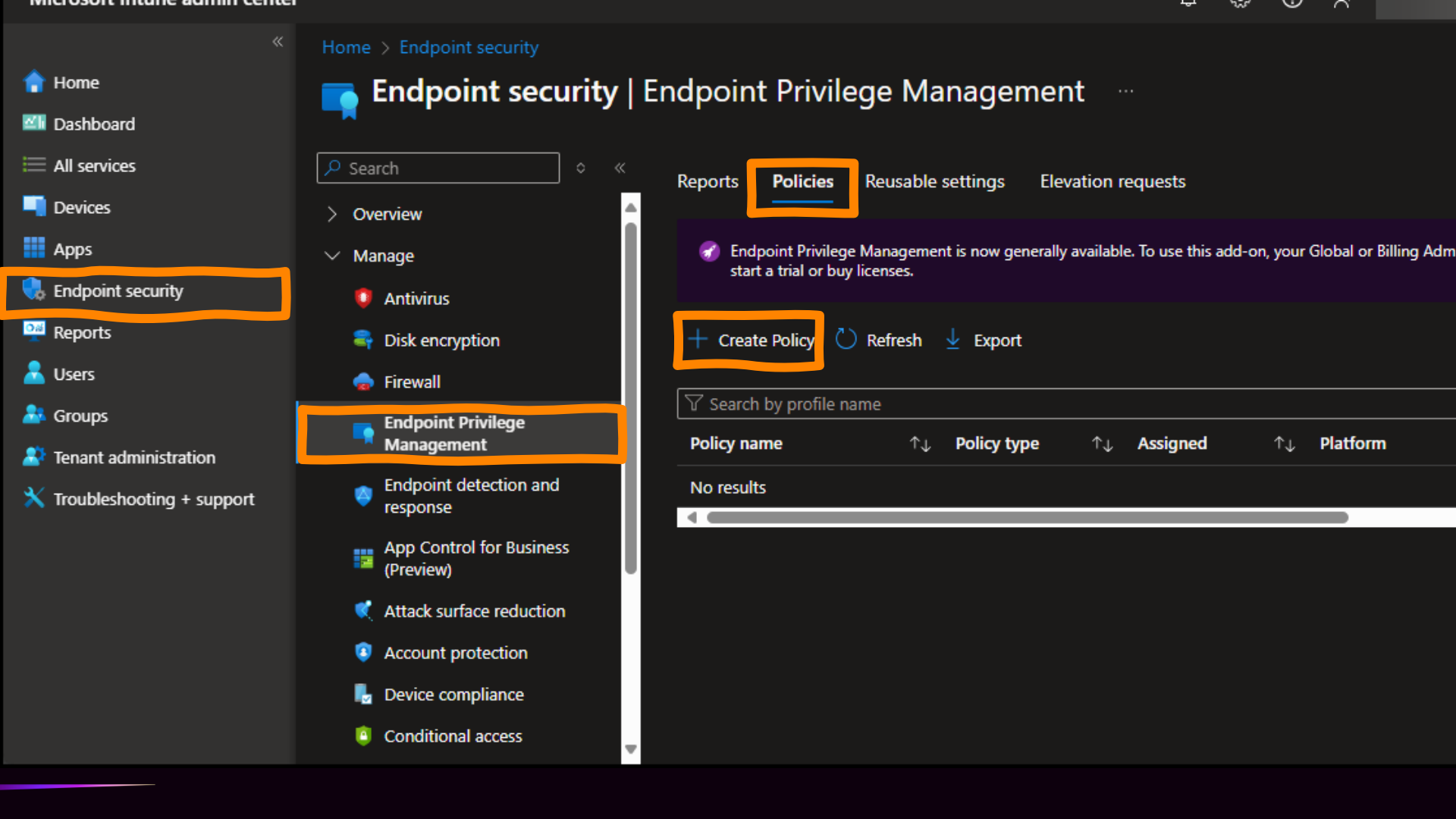
👩‍💻 User confirmed

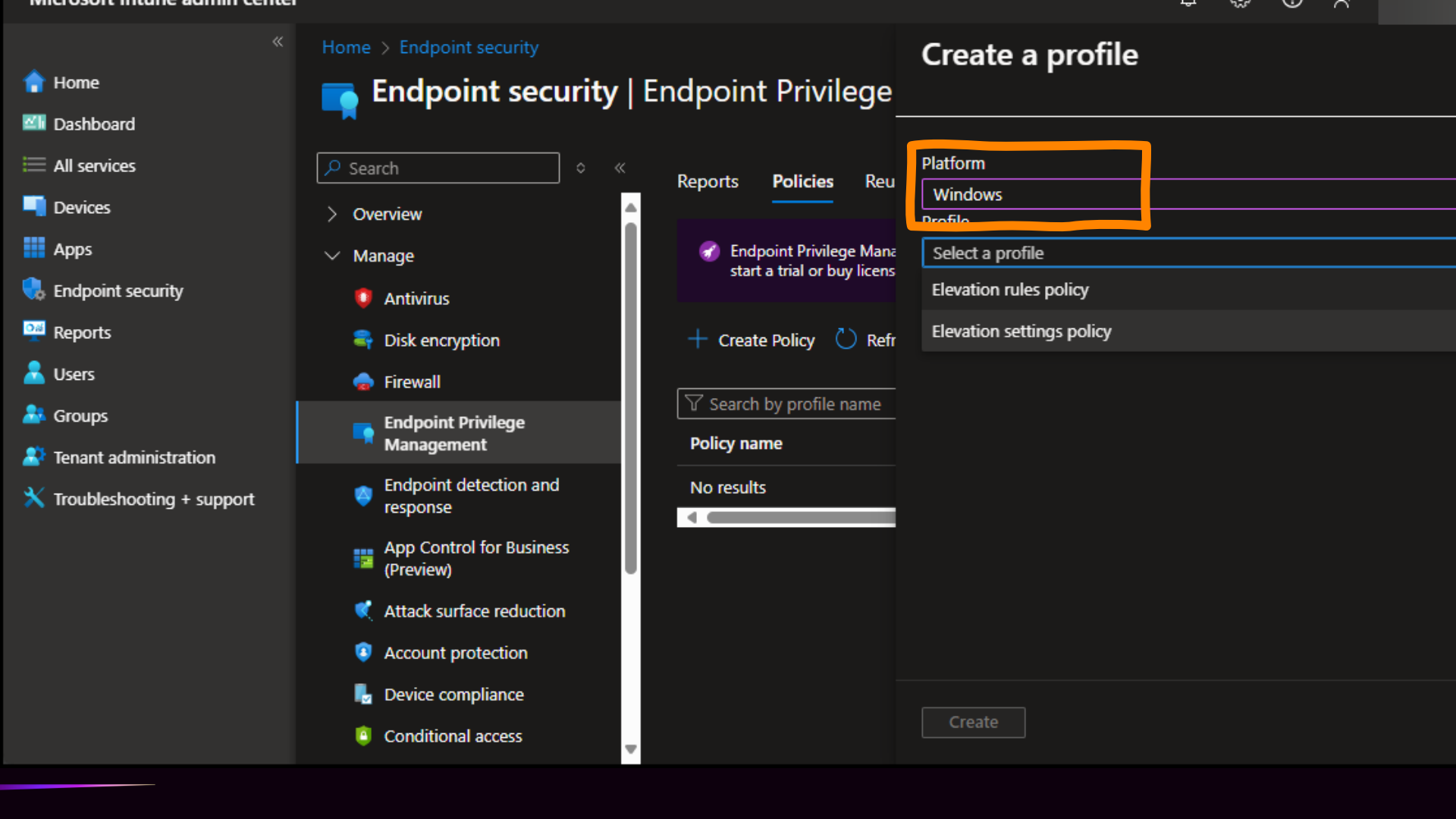
- On request from user

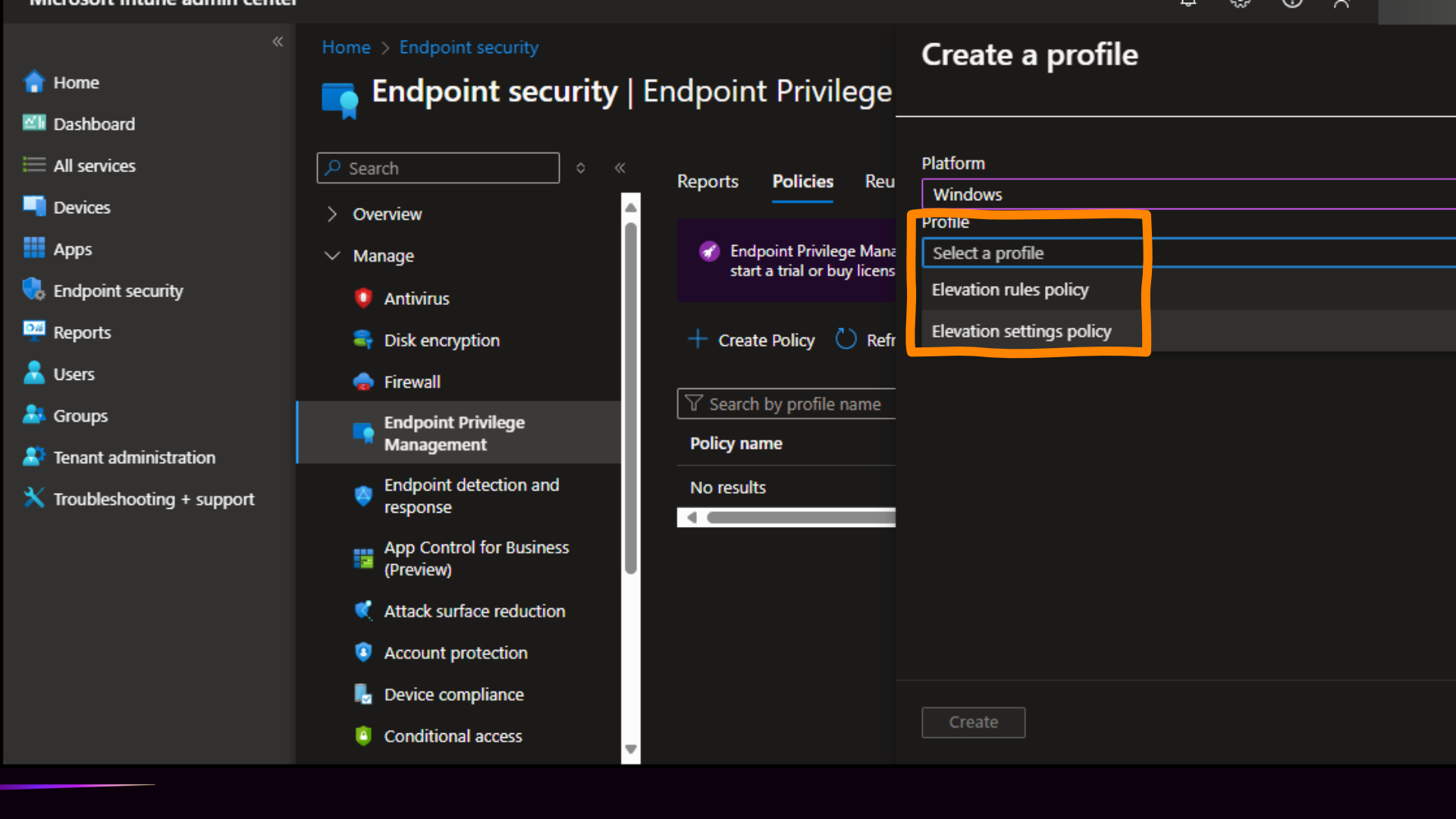
👮 Support approved

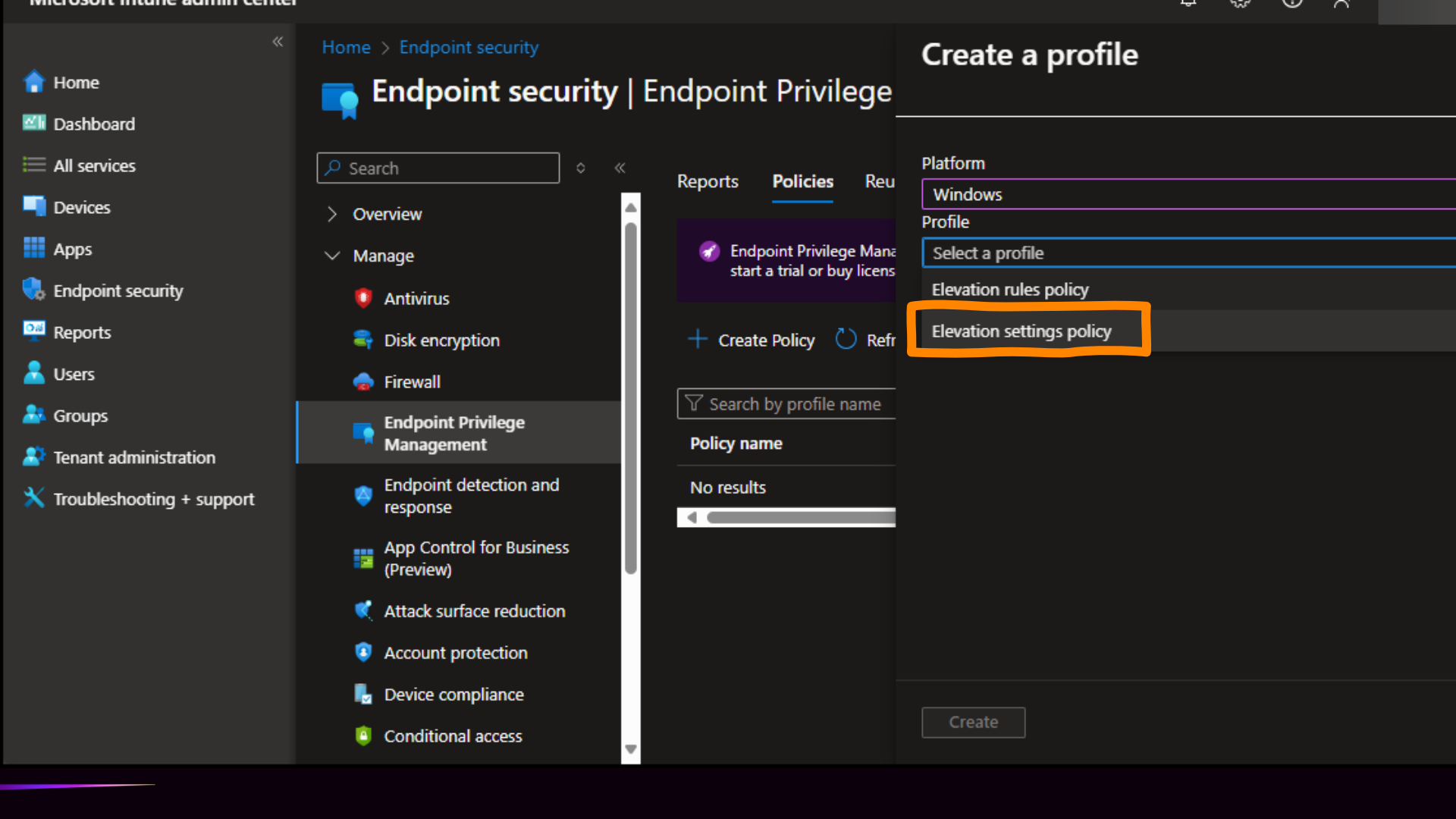
- IT must approve the request

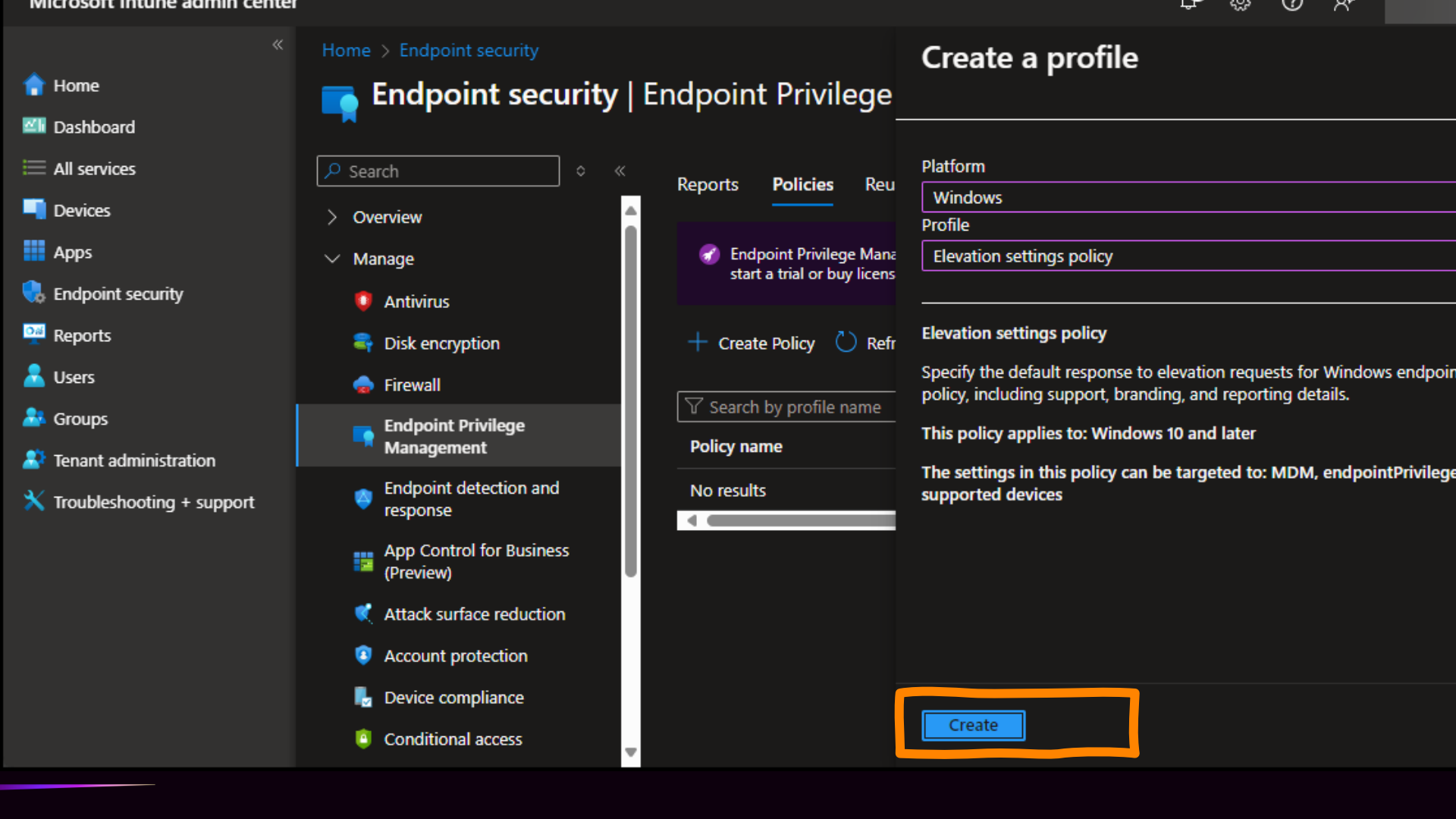
NIC
EMPOWER

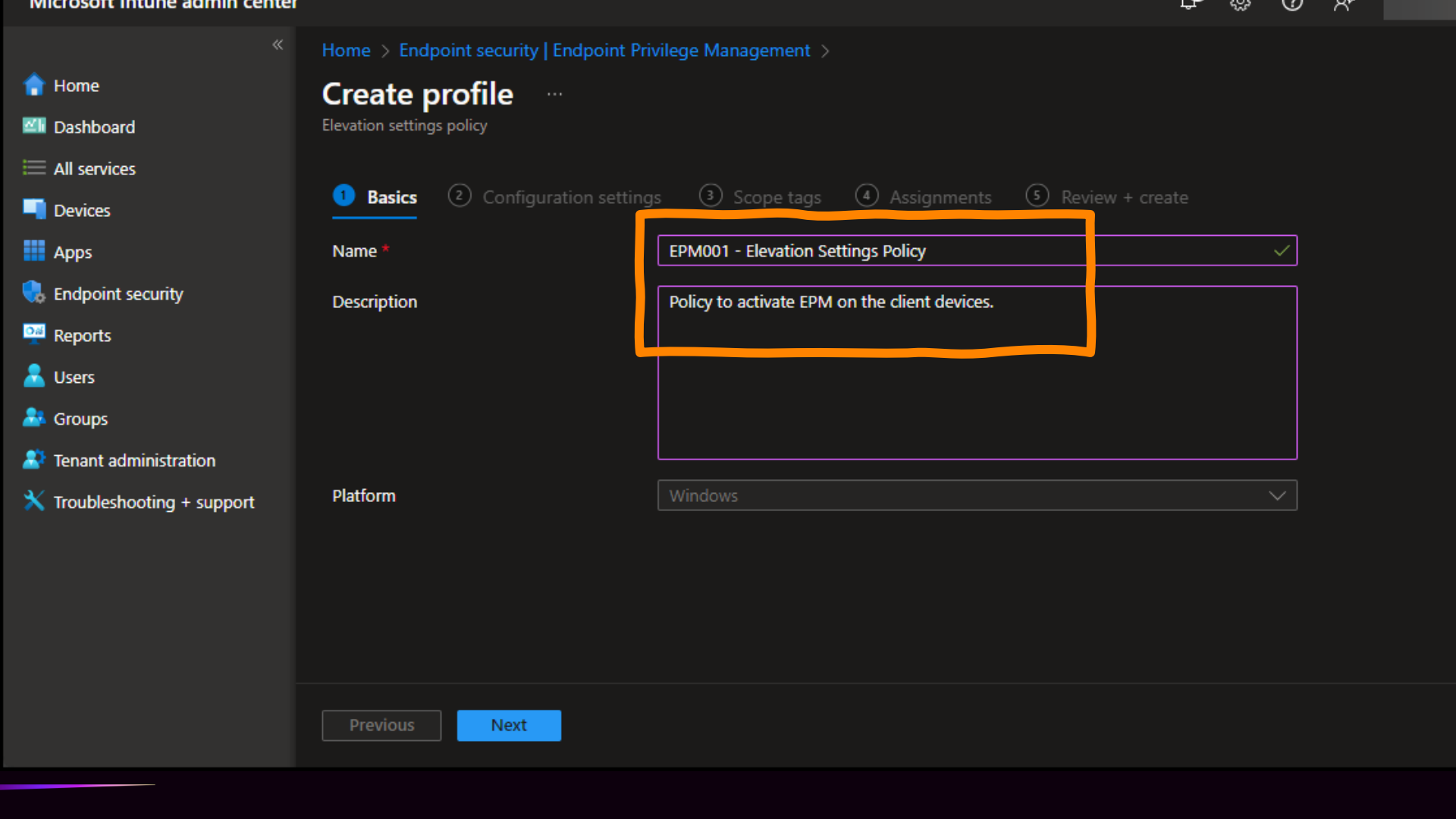

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Reports
Policies
Reusable settings
Elevation requests
Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Adm
start a trial or buy licenses.
Create Policy
Refresh
Export
Search by profile name
Policy name
Policy type
Assigned
Platform
No results

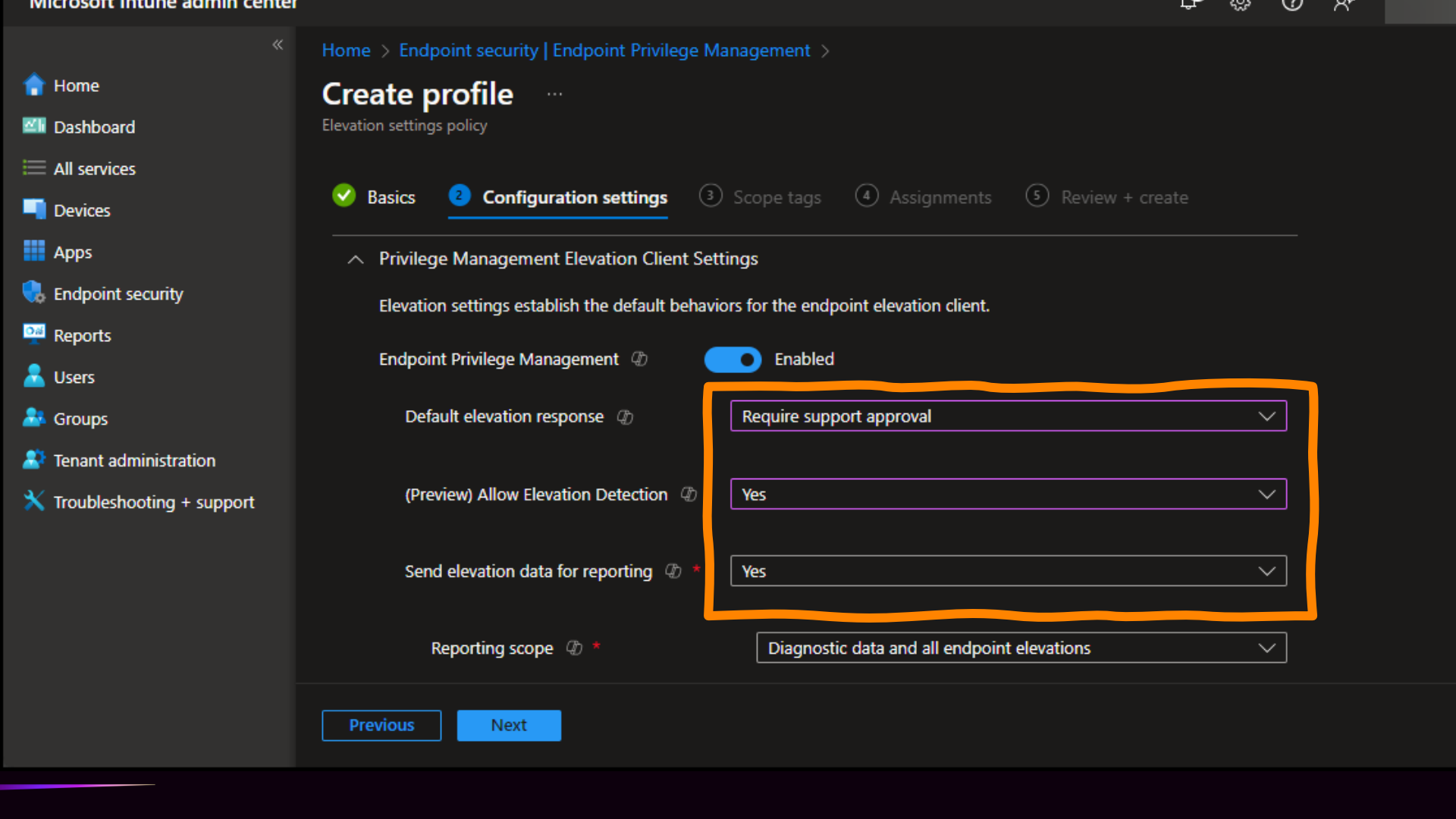

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Reports
Policies
Reu
Endpoint Privilege Mana
start a trial or buy licens
Create Policy
Refr
Search by profile name
Policy name
No results
Create a profile
Platform
Windows
Profile
Select a profile
Elevation rules policy
Elevation settings policy
Create

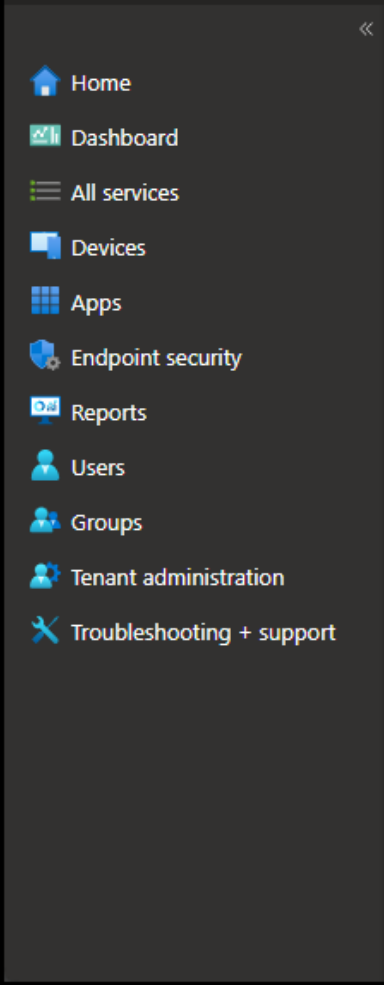

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Reports
Policies
Endpoint Privilege Mana
start a trial or buy licens
Create Policy
Search by profile name
Policy name
No results
Create a profile
Platform
Windows
Profile
Select a profile
Elevation rules policy
Elevation settings policy
Create


Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege
Search
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
Reports
Policies
Endpoint Privilege Mana
start a trial or buy licens
Create Policy
Refr
Search by profile name
Policy name
No results
Create a profile
Platform
Windows
Profile
Select a profile
Elevation rules policy
Elevation settings policy
Create


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege
Search
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
Reports
Policies
Endpoint Privilege Mana
start a trial or buy licens
Create Policy
Search by profile name
Policy name
No results
Create a profile
Platform
Windows
Profile
Elevation settings policy
Elevation settings policy
Specify the default response to elevation requests for Windows endpoin
policy, including support, branding, and reporting details.
This policy applies to: Windows 10 and later
The settings in this policy can be targeted to: MDM, endpointPrivilege
supported devices
Create


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation settings policy
1 Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Name *
EPM001 - Elevation Settings Policy
Description
Policy to activate EPM on the client devices.
Platform
Windows
Previous
Next


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation settings policy
Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Privilege Management Elevation Client Settings
Elevation settings establish the default behaviors for the endpoint elevation client.
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

Elevation settings policy

Basics | Configuration settings | Scope tags | 4 Assignments | 5 Review + create

Included groups

Add groups | Add all users | Add all devices

Groups	Group Members	Filter	Filter mode	Edit filter
All devices		None	None	Edit filter

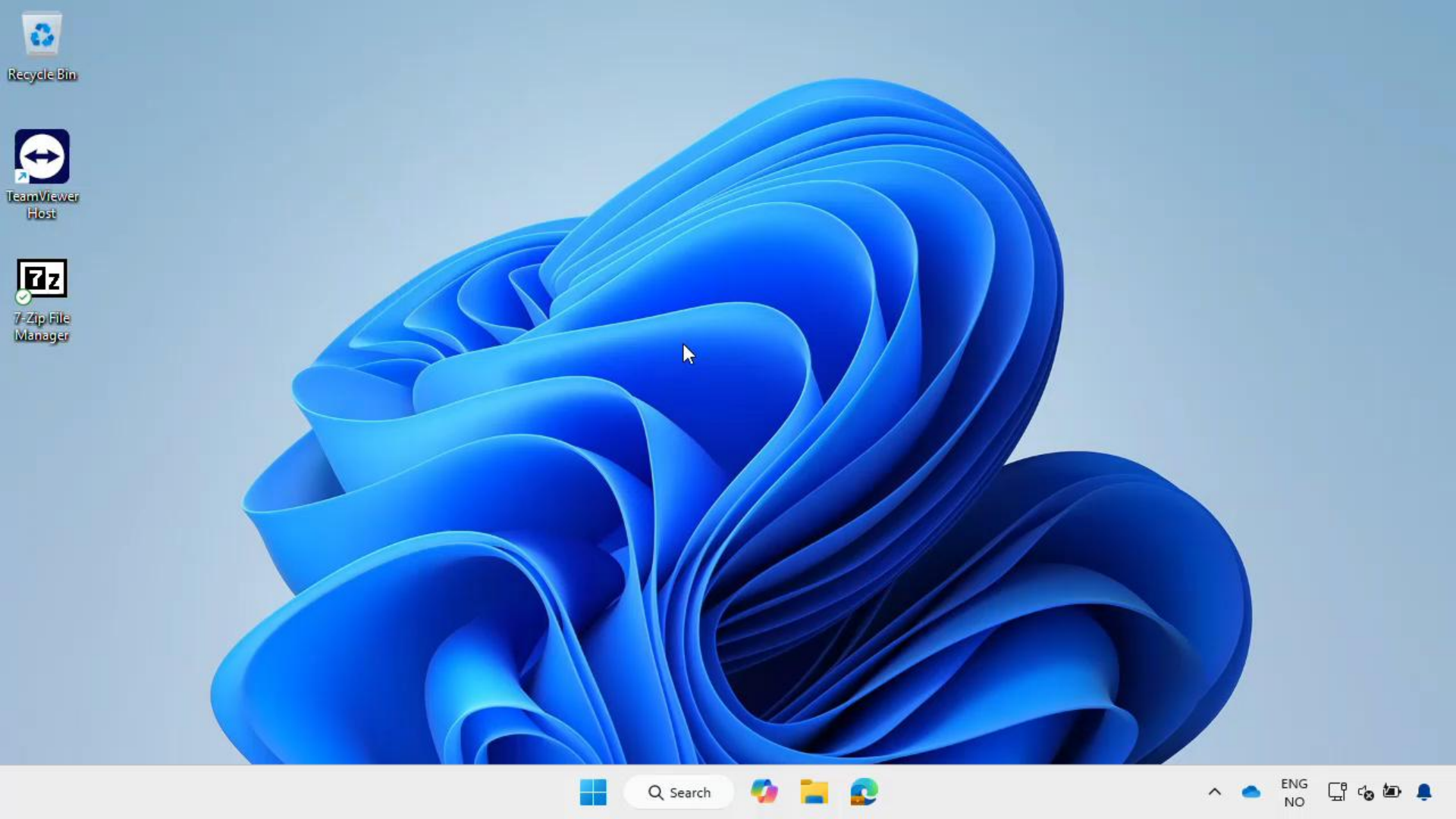
Excluded groups

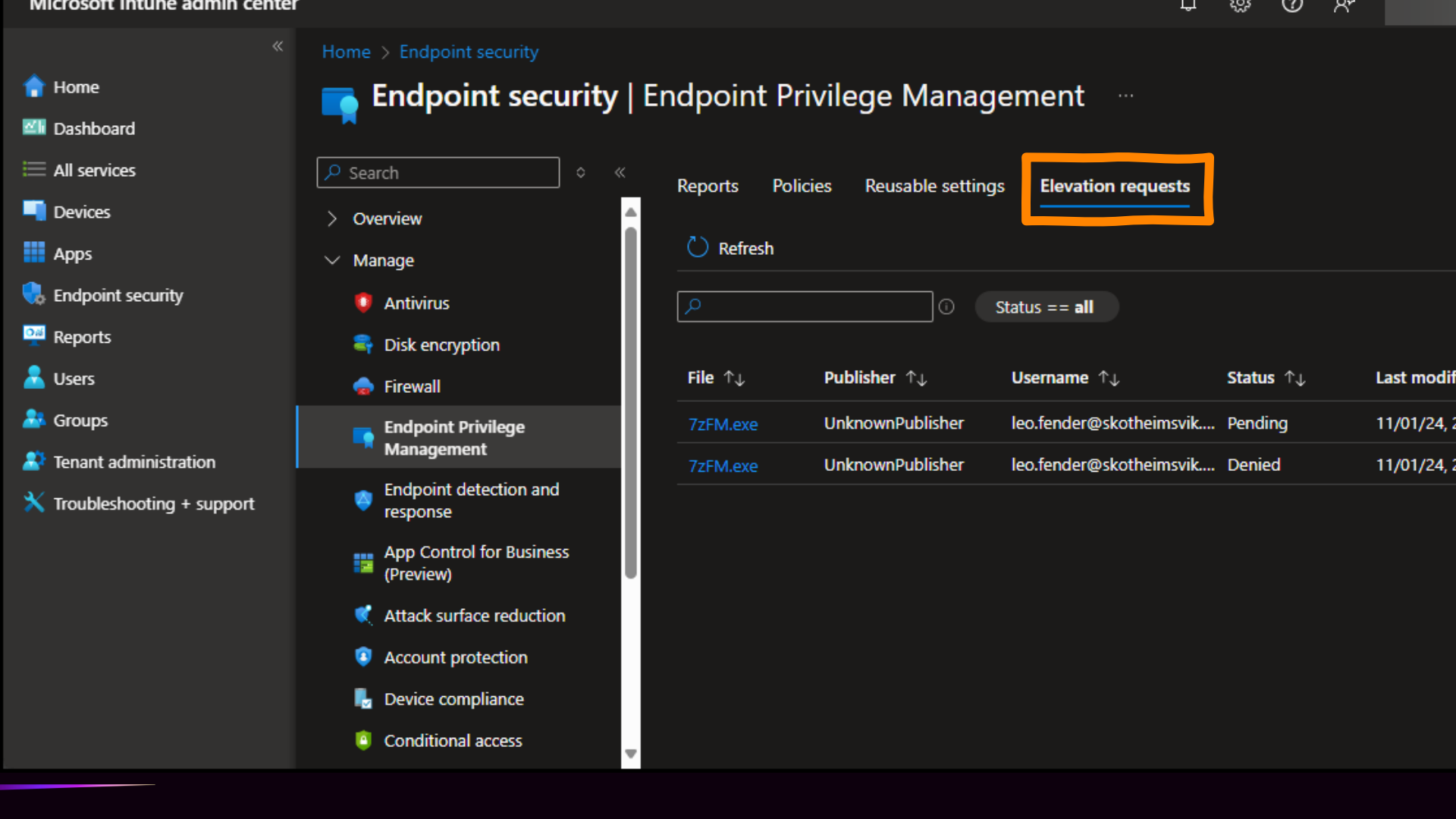
When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

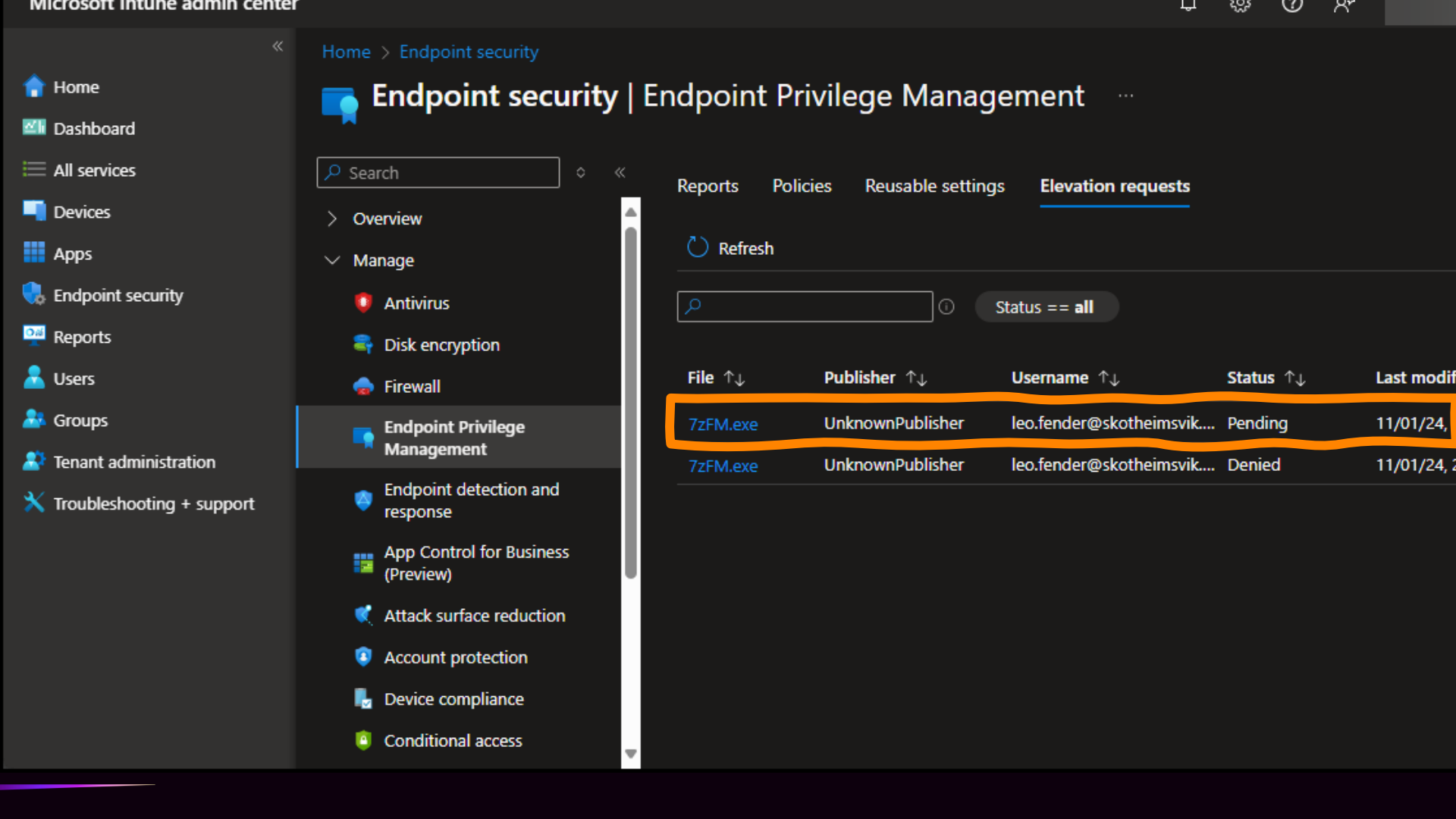
Add groups

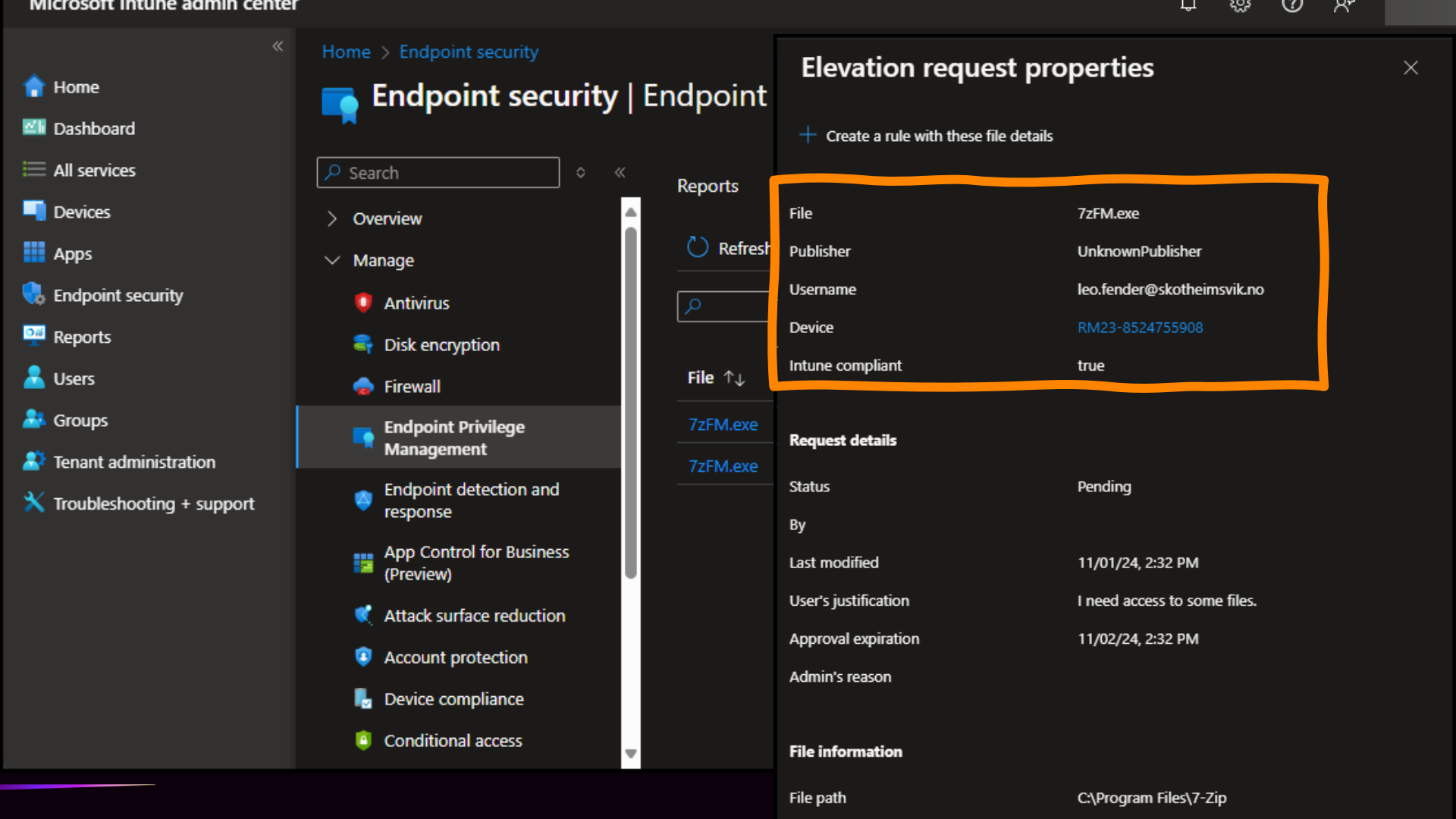
Groups	Group Members	Remove
No groups selected		

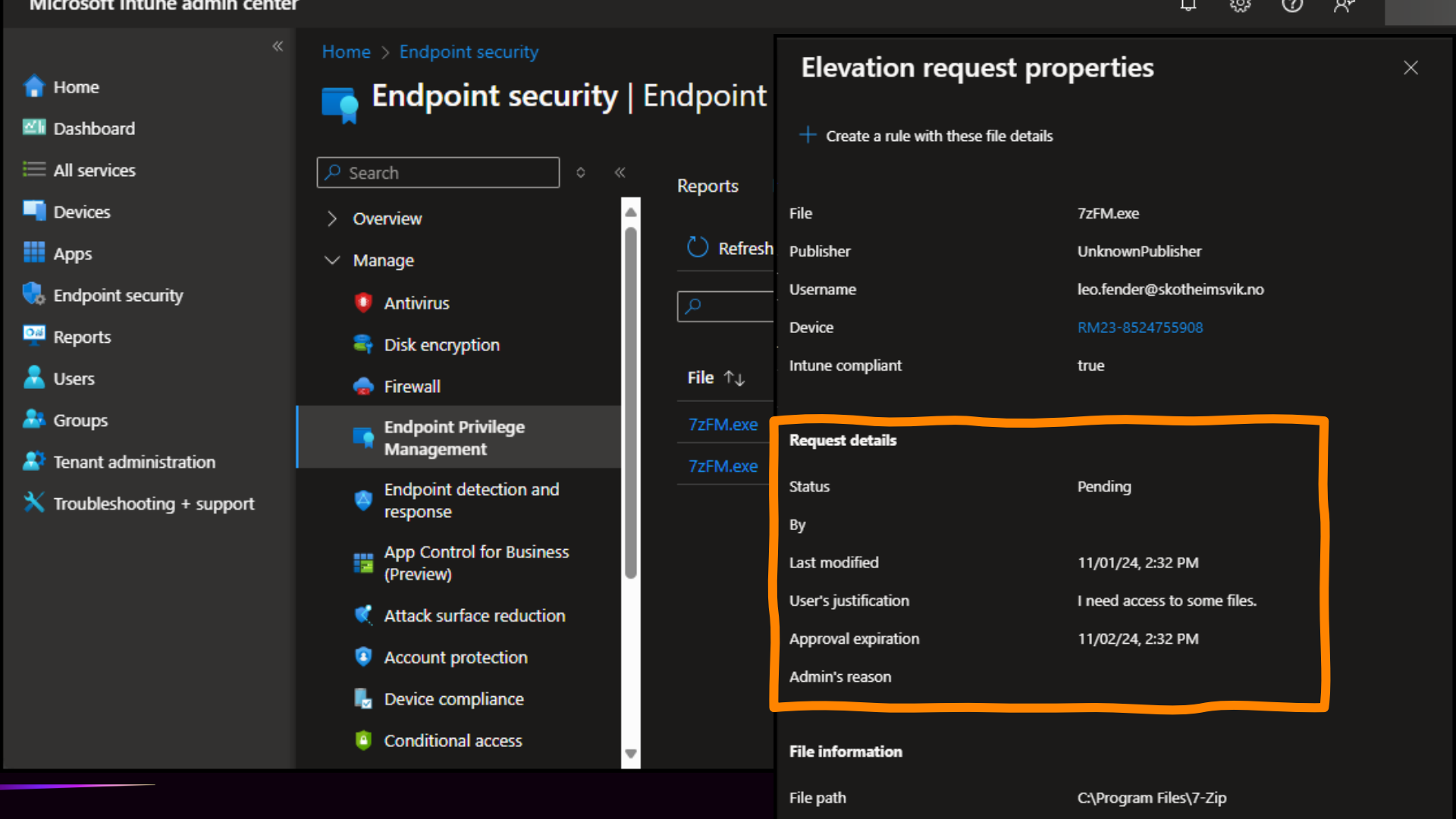
Previous | Next

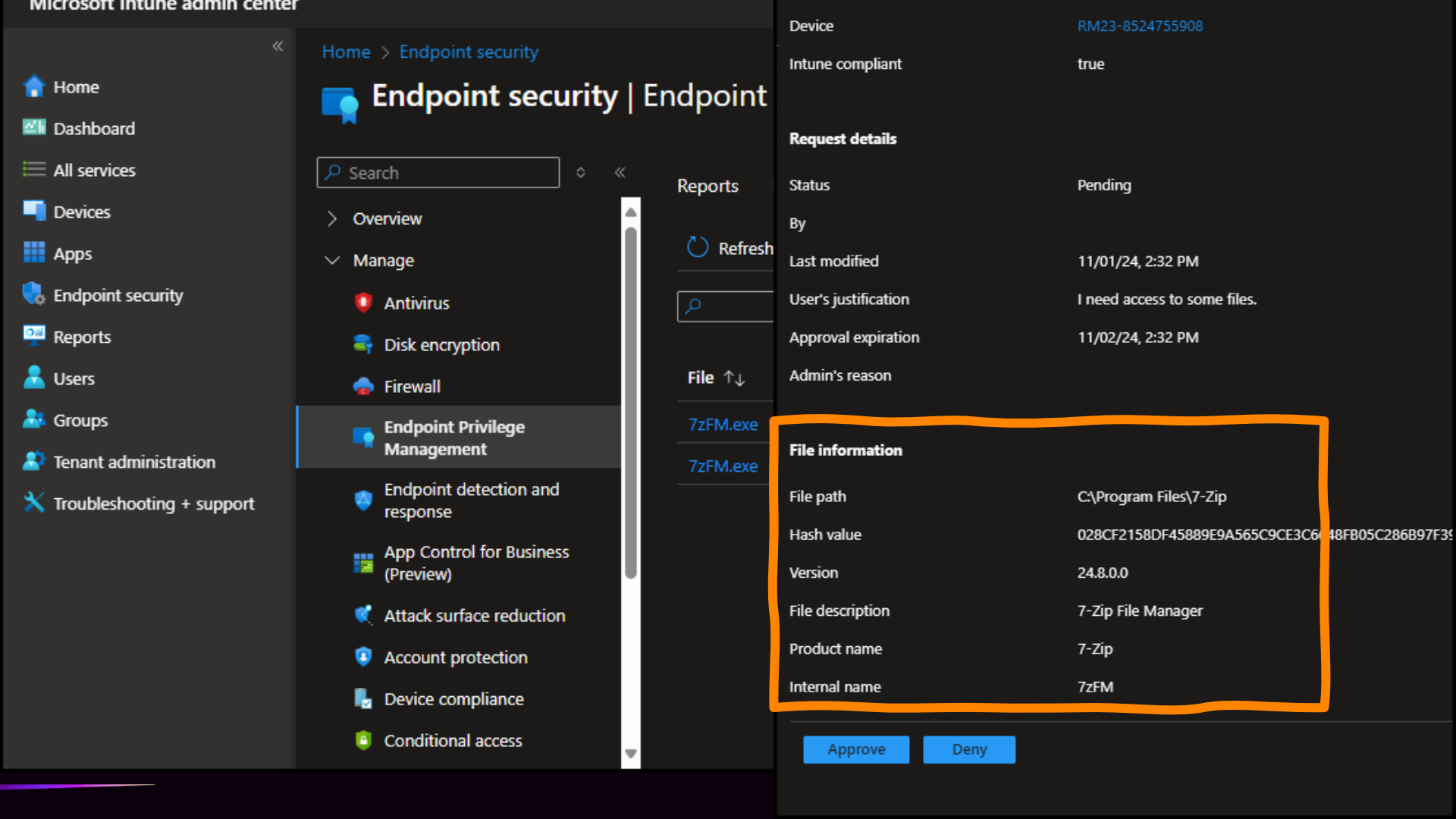

Recycle Bin
TeamViewer Host
7-Zip File Manager
Search
ENG
NO

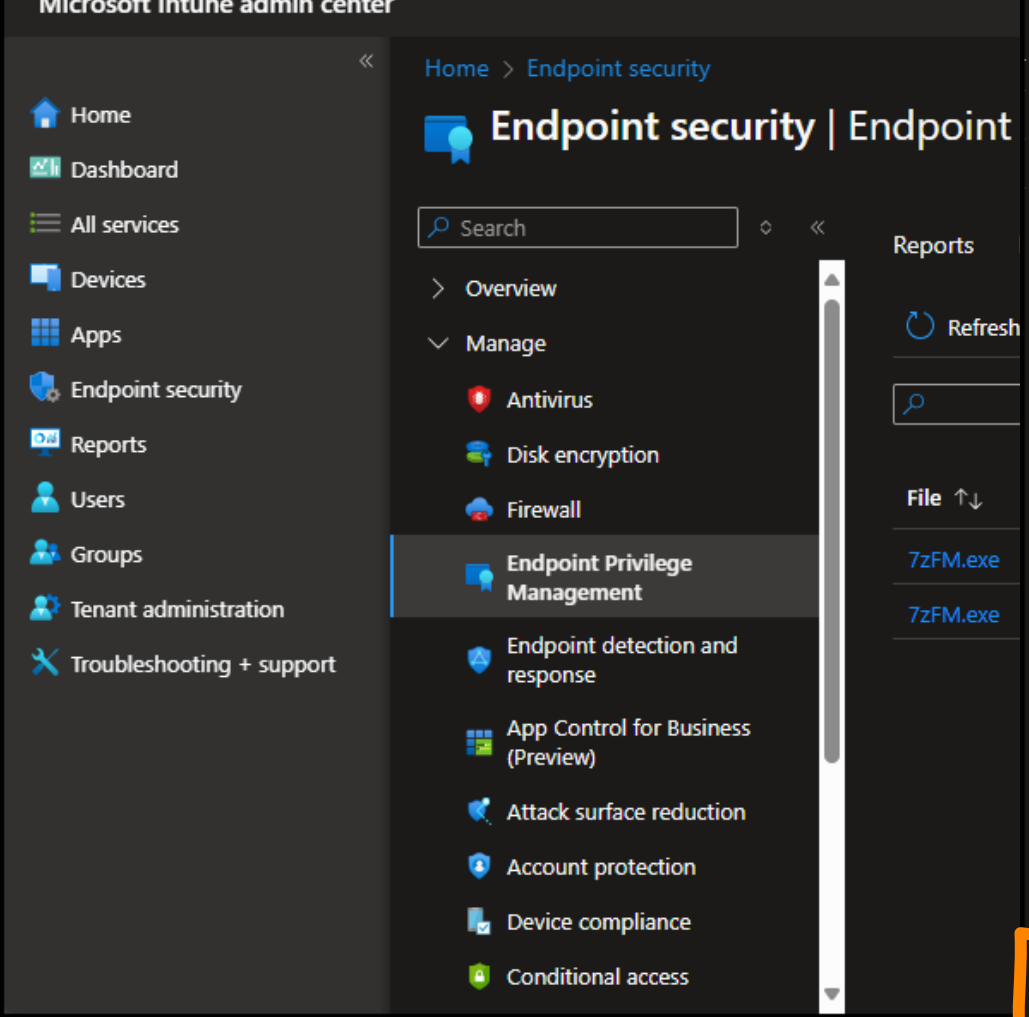

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Reports
Policies
Reusable settings
Elevation requests
Refresh
Status == all
File
Publisher
Username
Status
Last modif
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Pending
11/01/24,
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Denied
11/01/24,


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
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
Reports
Policies
Reusable settings
Elevation requests
Refresh
Status == all
File
Publisher
Username
Status
Last modif
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Pending
11/01/24,
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Denied
11/01/24,


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
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
Reports
Refresh
File
7zFM.exe
7zFM.exe
Elevation request properties
Create a rule with these file details
File 7zFM.exe
Publisher UnknownPublisher
Username leo.fender@skotheimsvik.no
Device RM23-8524755908
Intune compliant true
Request details
Status Pending
By
Last modified 11/01/24, 2:32 PM
User's justification I need access to some files.
Approval expiration 11/02/24, 2:32 PM
Admin's reason
File information
File path C:\Program Files\7-Zip


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
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
Reports
Refresh
File
7zFM.exe
7zFM.exe
Elevation request properties
Create a rule with these file details
File 7zFM.exe
Publisher UnknownPublisher
Username leo.fender@skotheimsvik.no
Device RM23-8524755908
Intune compliant true
Request details
Status Pending
By
Last modified 11/01/24, 2:32 PM
User's justification I need access to some files.
Approval expiration 11/02/24, 2:32 PM
Admin's reason
File information
File path C:\Program Files\7-Zip


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
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
Reports
Refresh
File
7zFM.exe
7zFM.exe
Device
RM23-8524755908
Intune compliant
true
Request details
Status
Pending
By
Last modified
11/01/24, 2:32 PM
User's justification
I need access to some files.
Approval expiration
11/02/24, 2:32 PM
Admin's reason
File information
File path
C:\Program Files\7-Zip
Hash value
028CF2158DF45889E9A565C9CE3C6
48FB05C286B97F3
Version
24.8.0.0
File description
7-Zip File Manager
Product name
7-Zip
Internal name
7zFM
Approve
Deny



Device	RM23-8524755908
Intune compliant	true

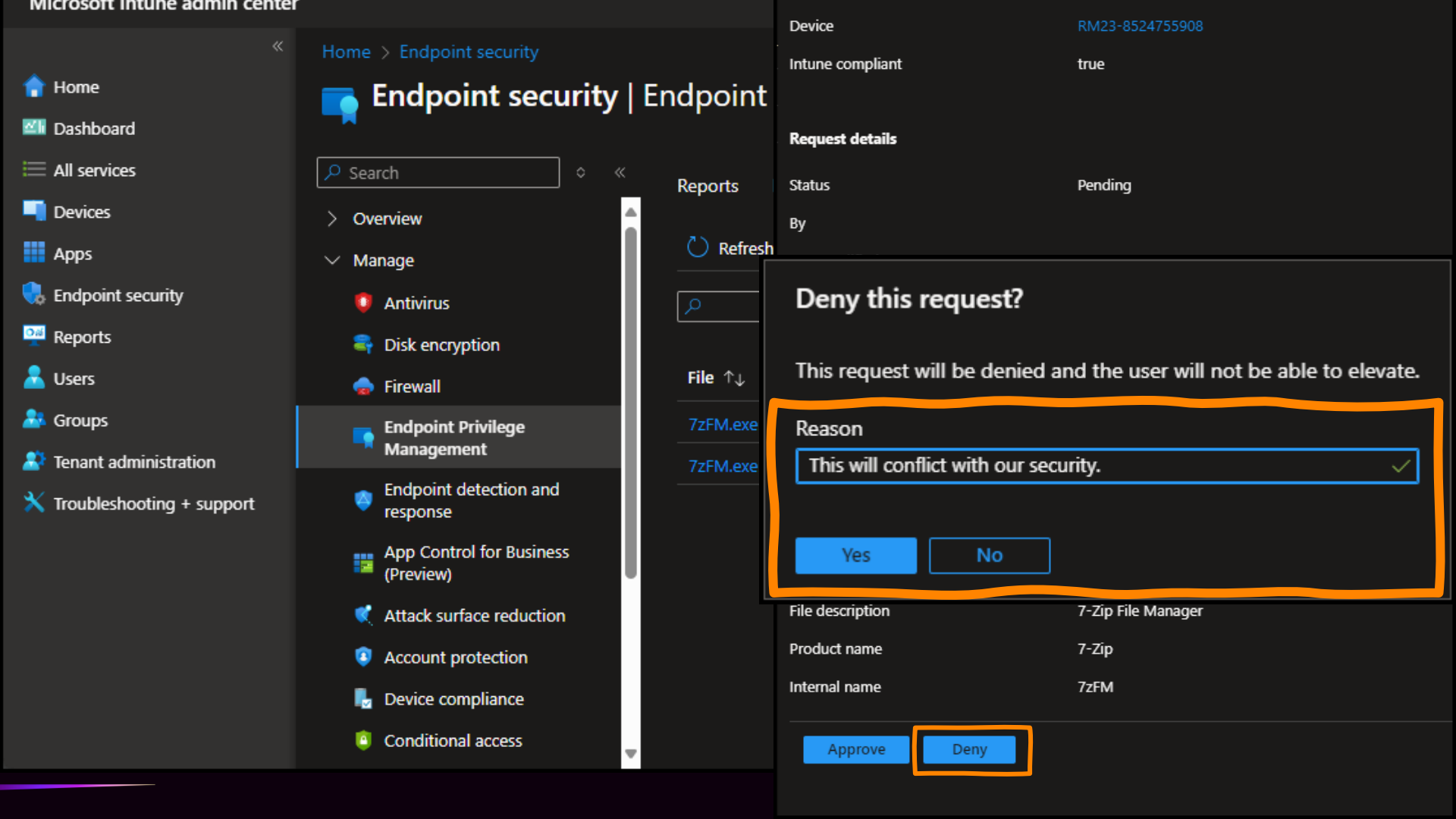
Request details

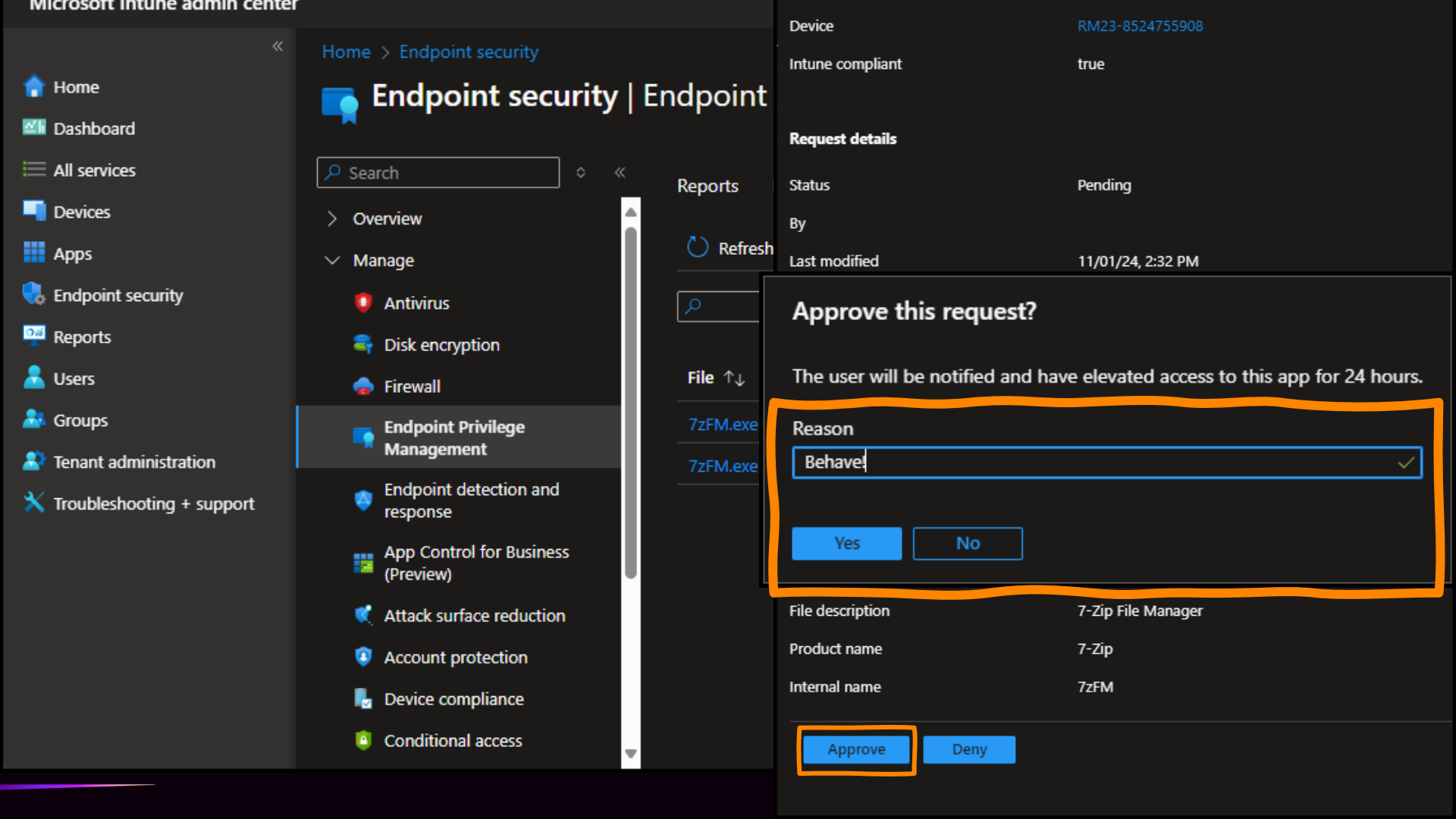
Status	Pending
By	
Last modified	11/01/24, 2:32 PM
User's justification	I need access to some files.
Approval expiration	11/02/24, 2:32 PM
Admin's reason	

File information

File path	C:\Program Files\7-Zip
Hash value	028CF2158DF45889E9A565C9CE3C6648FB05C286B97F3
Version	24.8.0.0
File description	7-Zip File Manager
Product name	7-Zip
Internal name	7zFM

Approve Deny


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
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
Reports
Refresh
File
7zFM.exe
7zFM.exe
Device
RM23-8524755908
Intune compliant
true
Request details
Status
Pending
By
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
File description
7-Zip File Manager
Product name
7-Zip
Internal name
7zFM
Approve
Deny


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
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
Reports
Refresh
File
7zFM.exe
7zFM.exe
Device
RM23-8524755908
Intune compliant
true
Request details
Status
Pending
By
Last modified
11/01/24, 2:32 PM
Approve this request?
The user will be notified and have elevated access to this app for 24 hours.
Reason
Behavel
Yes
No
File description
7-Zip File Manager
Product name
7-Zip
Internal name
7zFM
Approve
Deny

Endpoint Privilege Management (EPM)

- Support Approved workflow

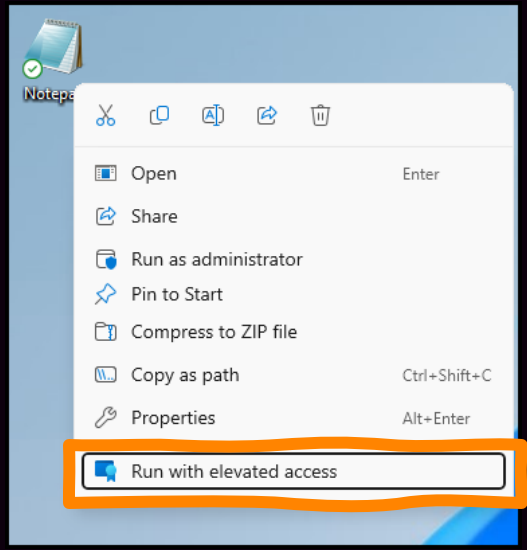
User requests elevation

NIC
EMPOWER

Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation

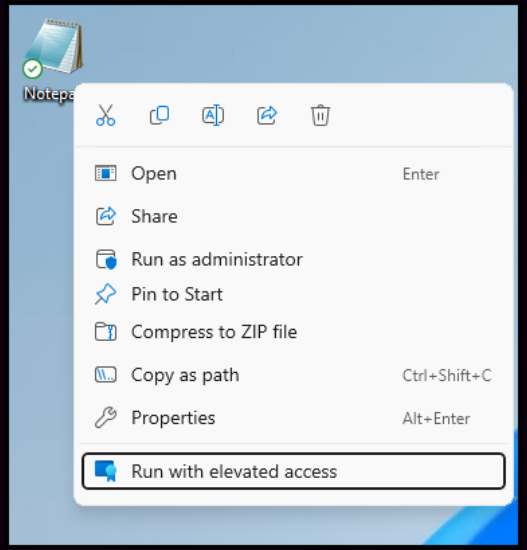


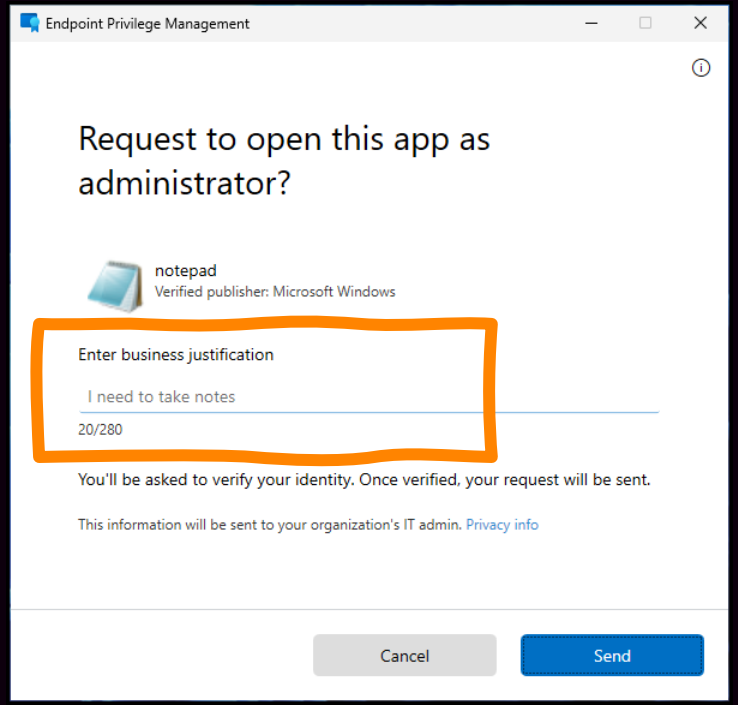
NIC EMPOWER

Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation





NIC EMPOWER

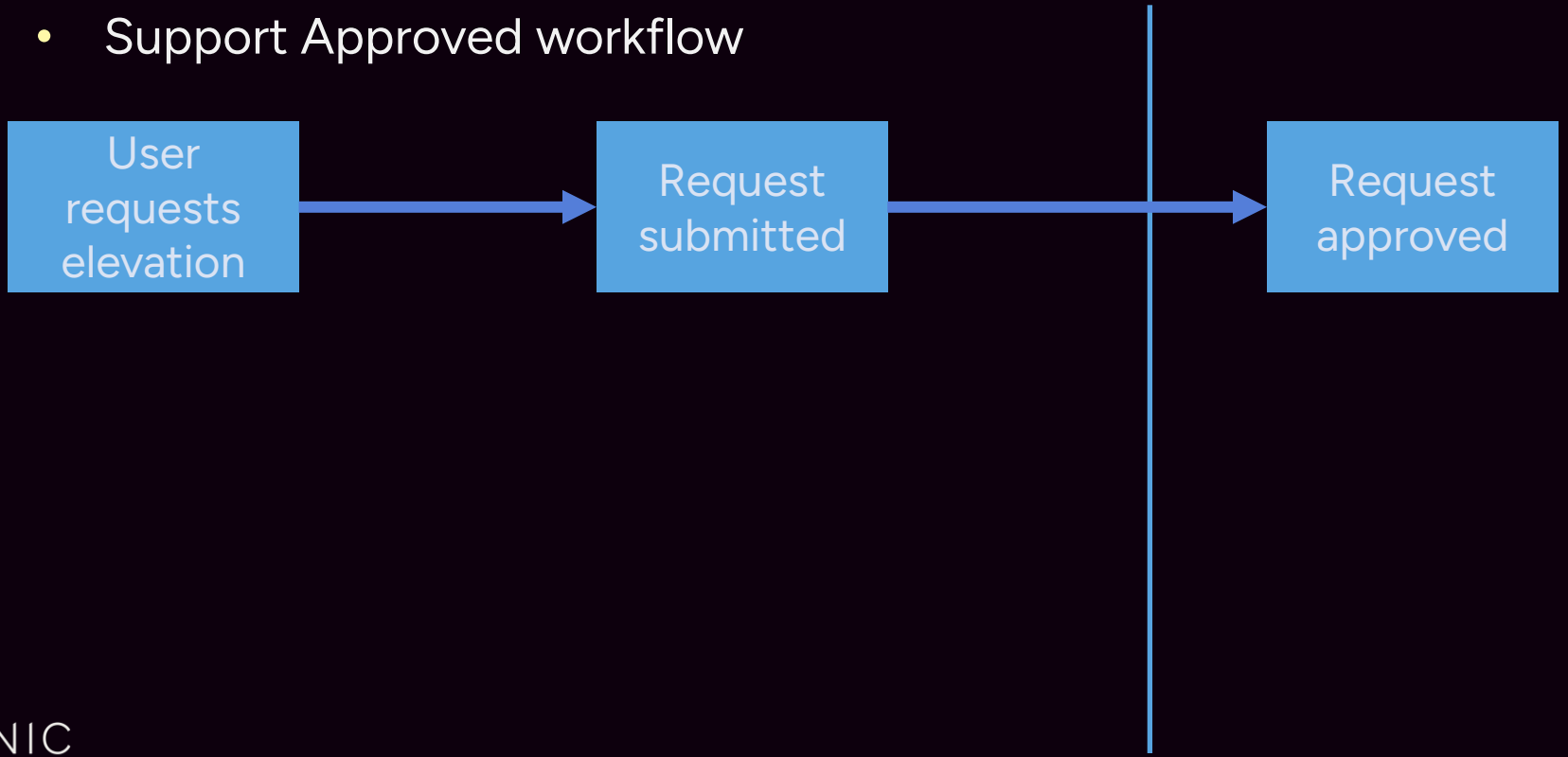
Endpoint Privilege Management (EPM)

- Support Approved workflow

NIC
EMPOWER

Endpoint Privilege Management (EPM)

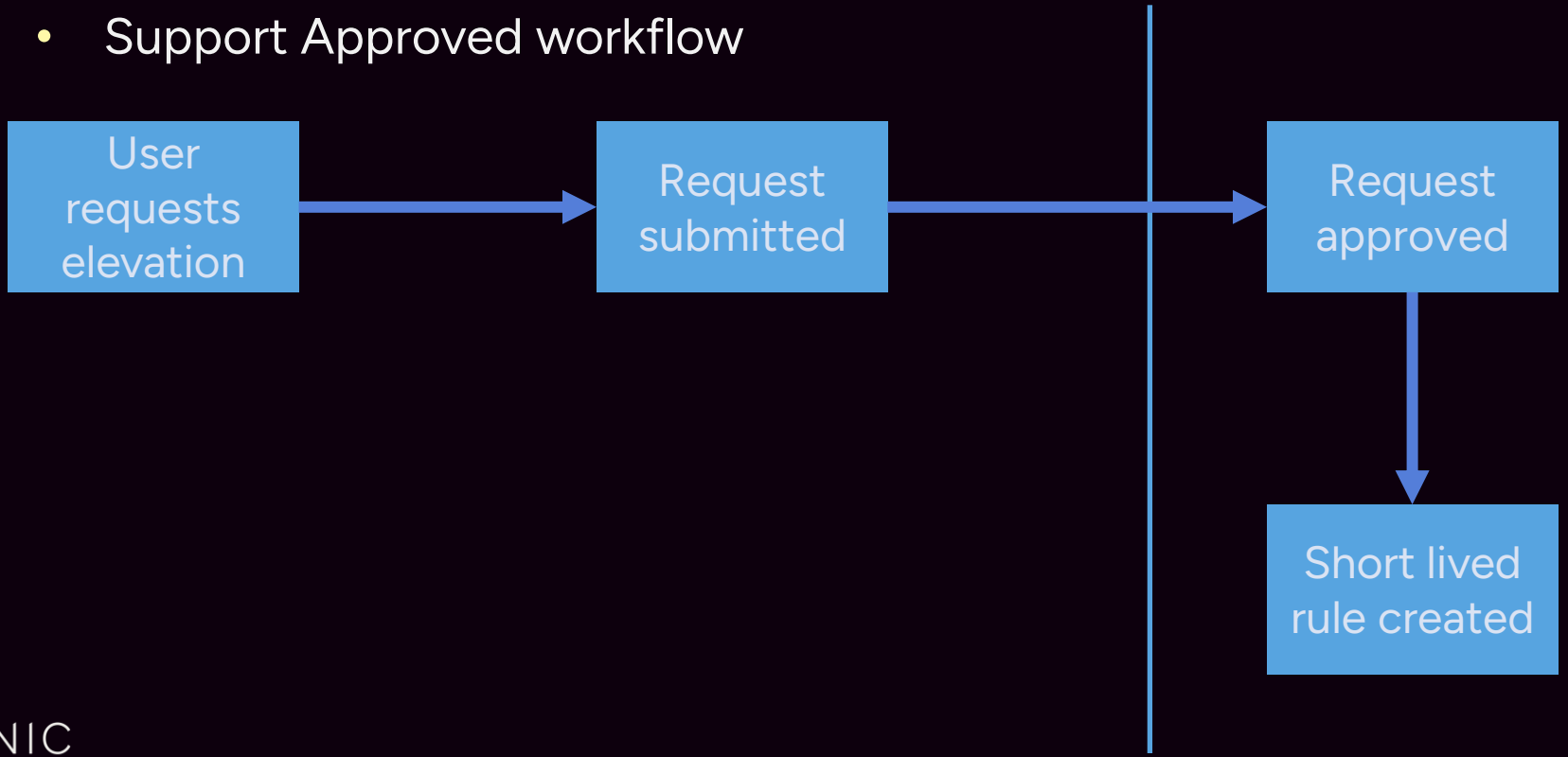
- Support Approved workflow



NIC
EMPOWER

Endpoint Privilege Management (EPM)

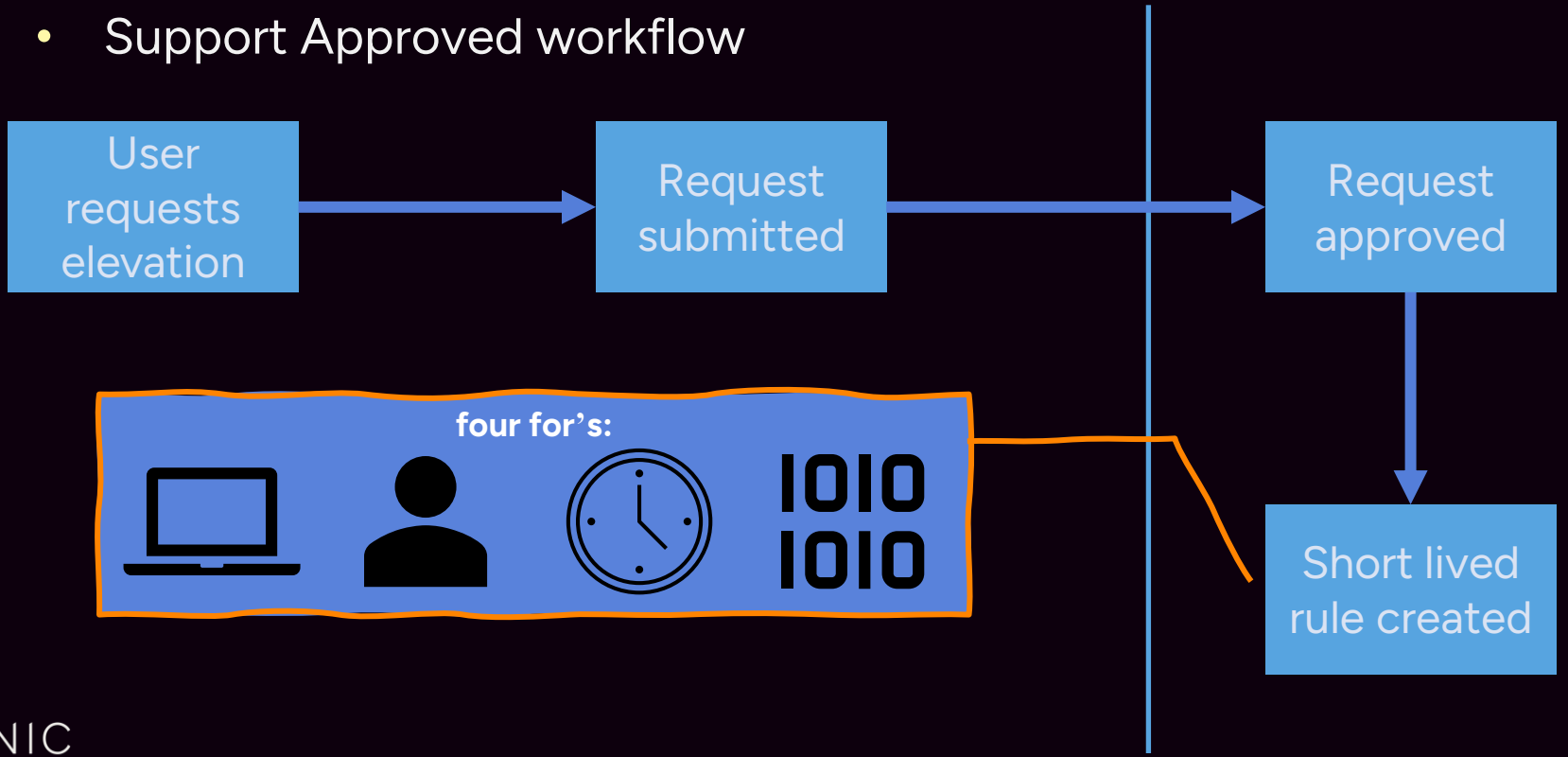
- Support Approved workflow



NIC
EMPOWER

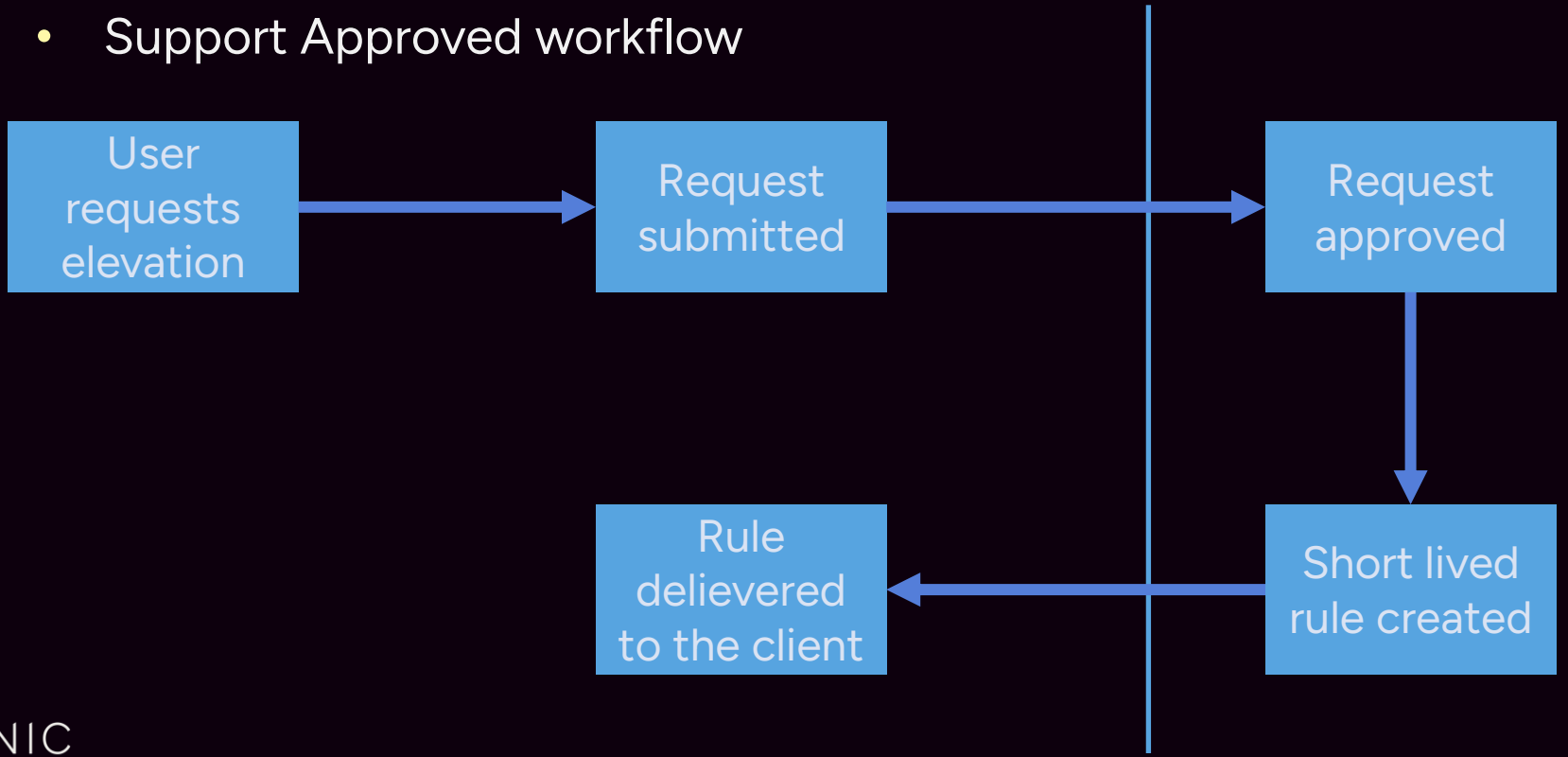
Endpoint Privilege Management (EPM)

- Support Approved workflow



Endpoint Privilege Management (EPM)

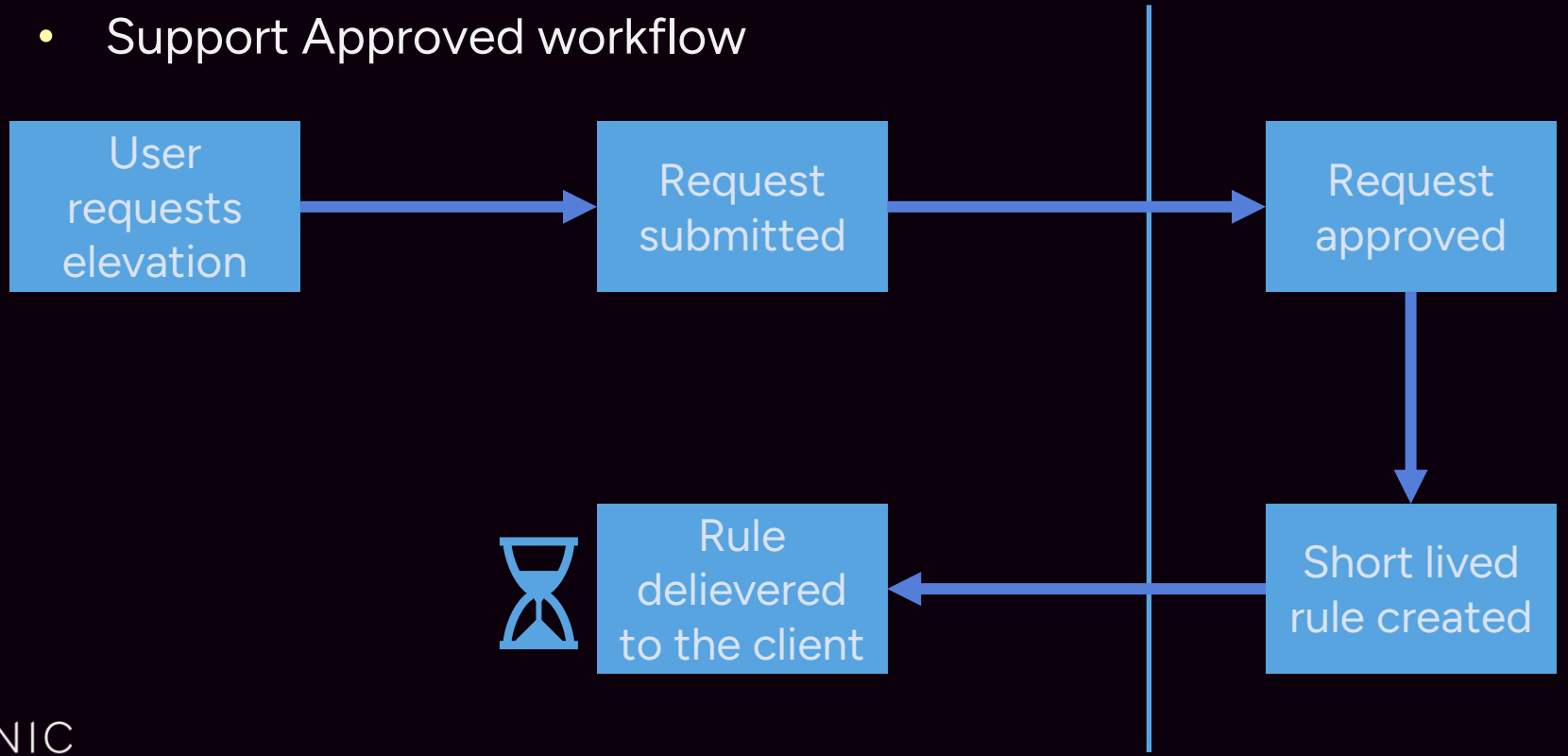
- Support Approved workflow



NIC
EMPOWER

Endpoint Privilege Management (EPM)

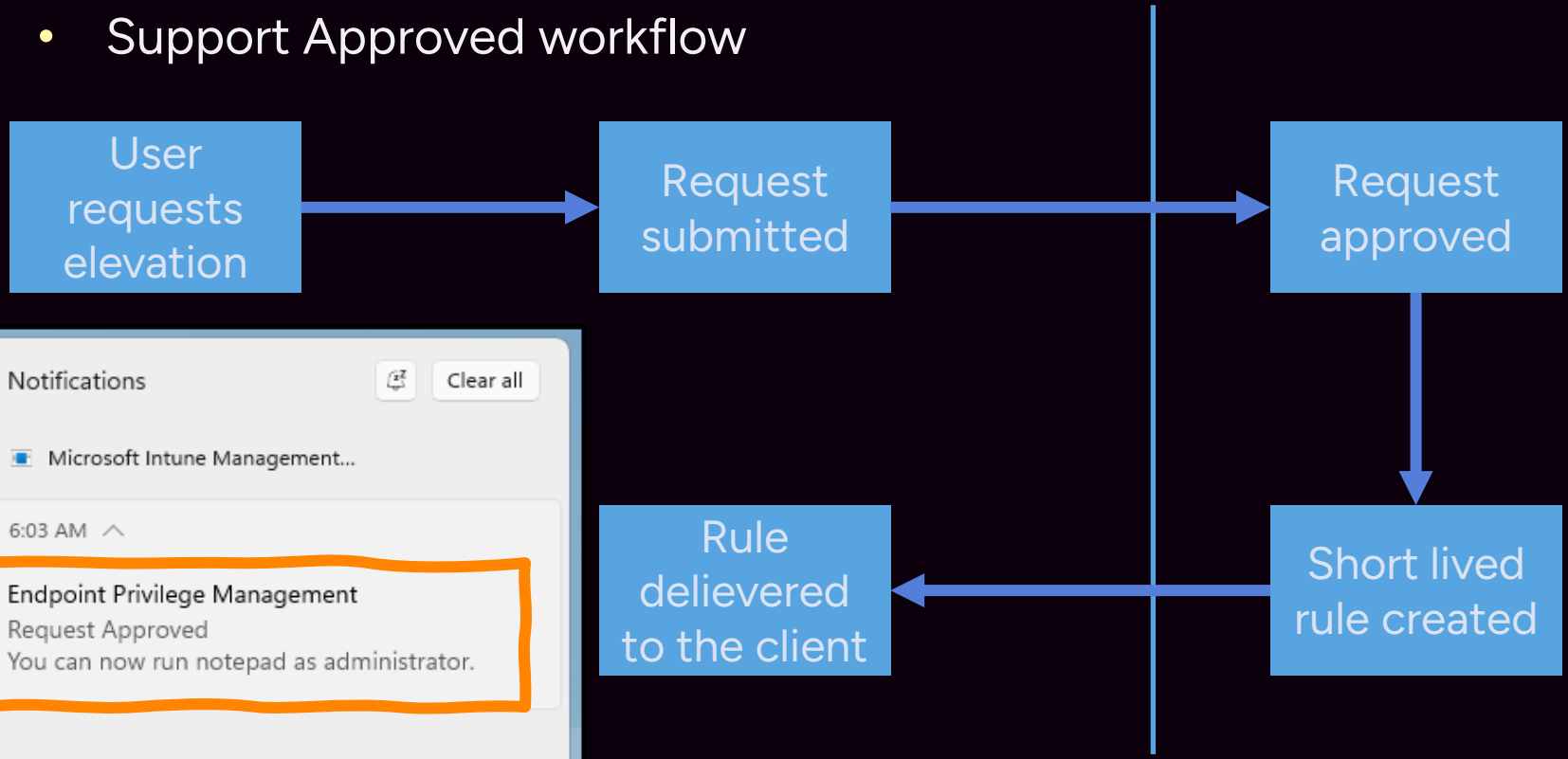
- Support Approved workflow



NIC
EMPOWER

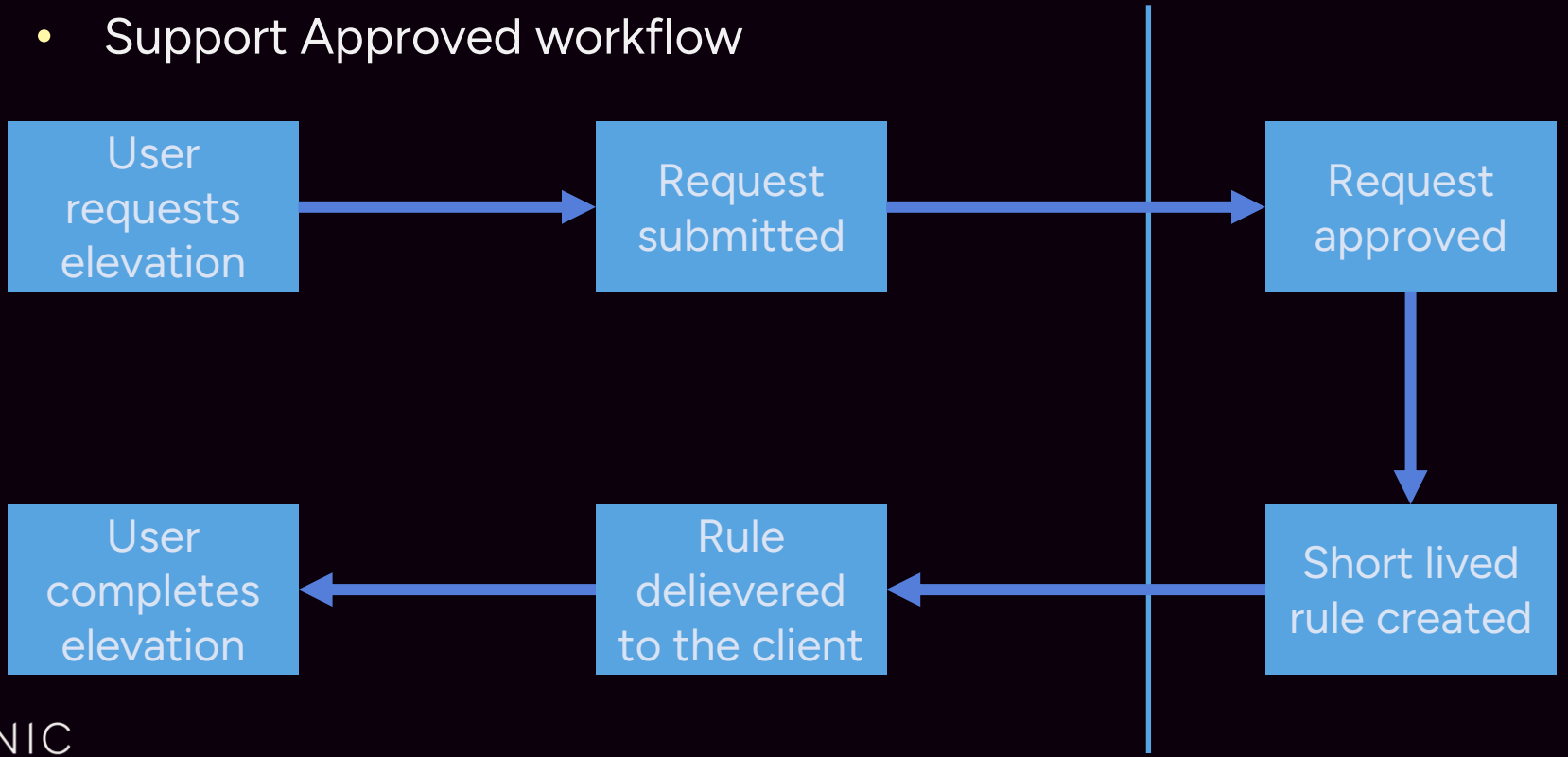
Endpoint Privilege Management (EPM)

- Support Approved workflow



Endpoint Privilege Management (EPM)

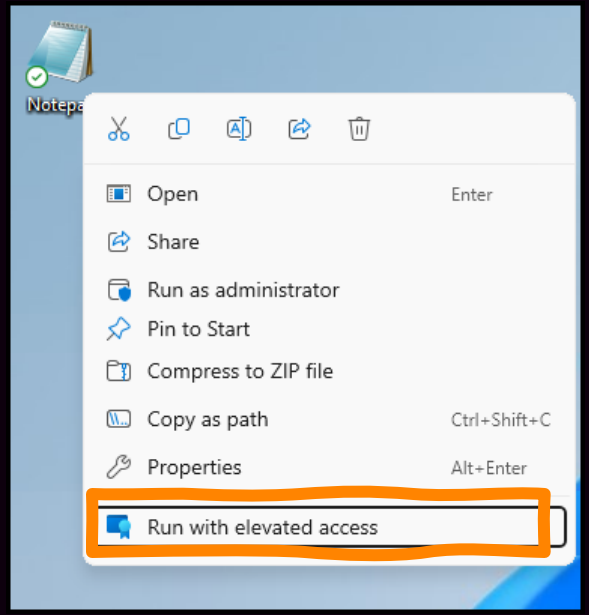
- Support Approved workflow



NIC
EMPOWER

Endpoint Privilege Management (EPM)

- Support Approved workflow

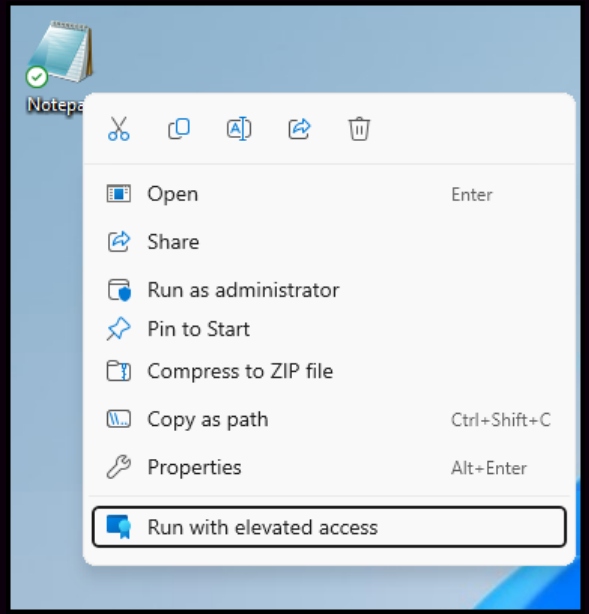


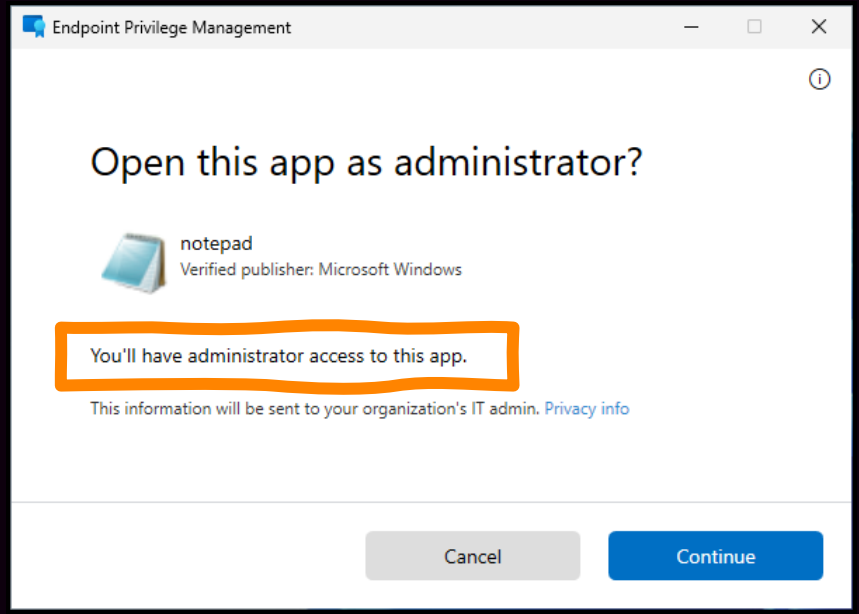
User completes elevation

NIC EMPOWER

Endpoint Privilege Management (EPM)

- Support Approved workflow



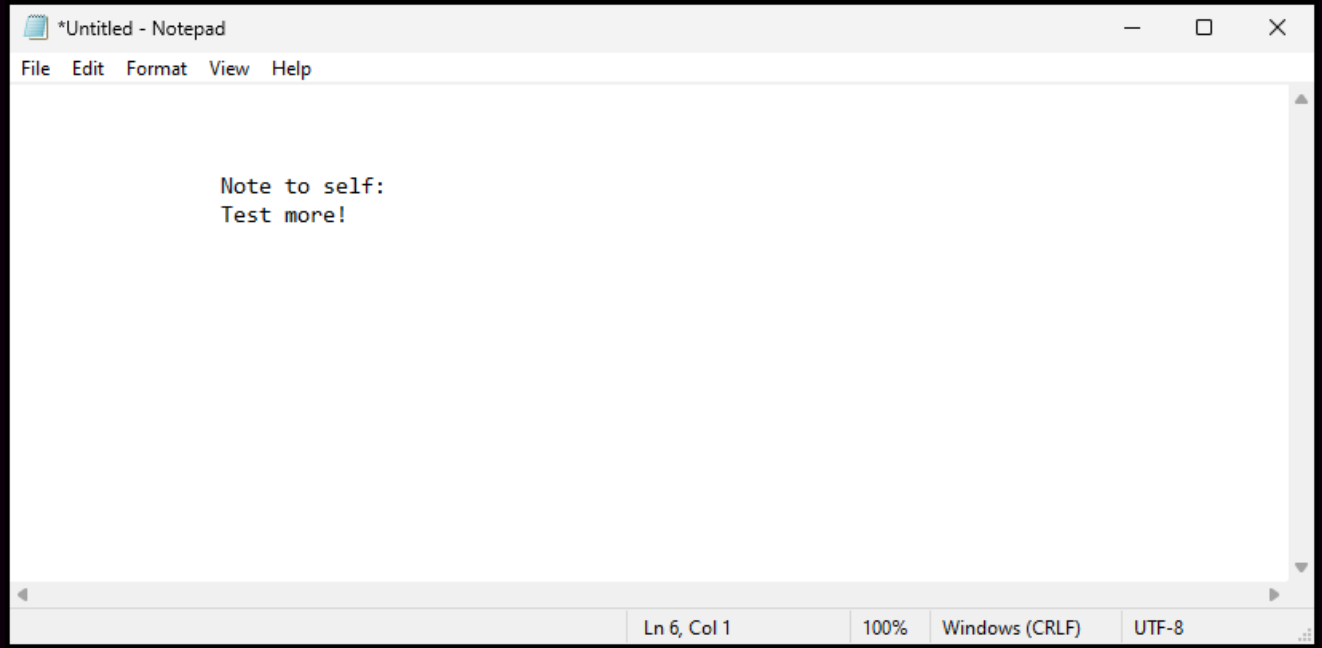


User completes elevation

NIC EMPOWER

Endpoint Privilege Management (EPM)

- Support Approved workflow

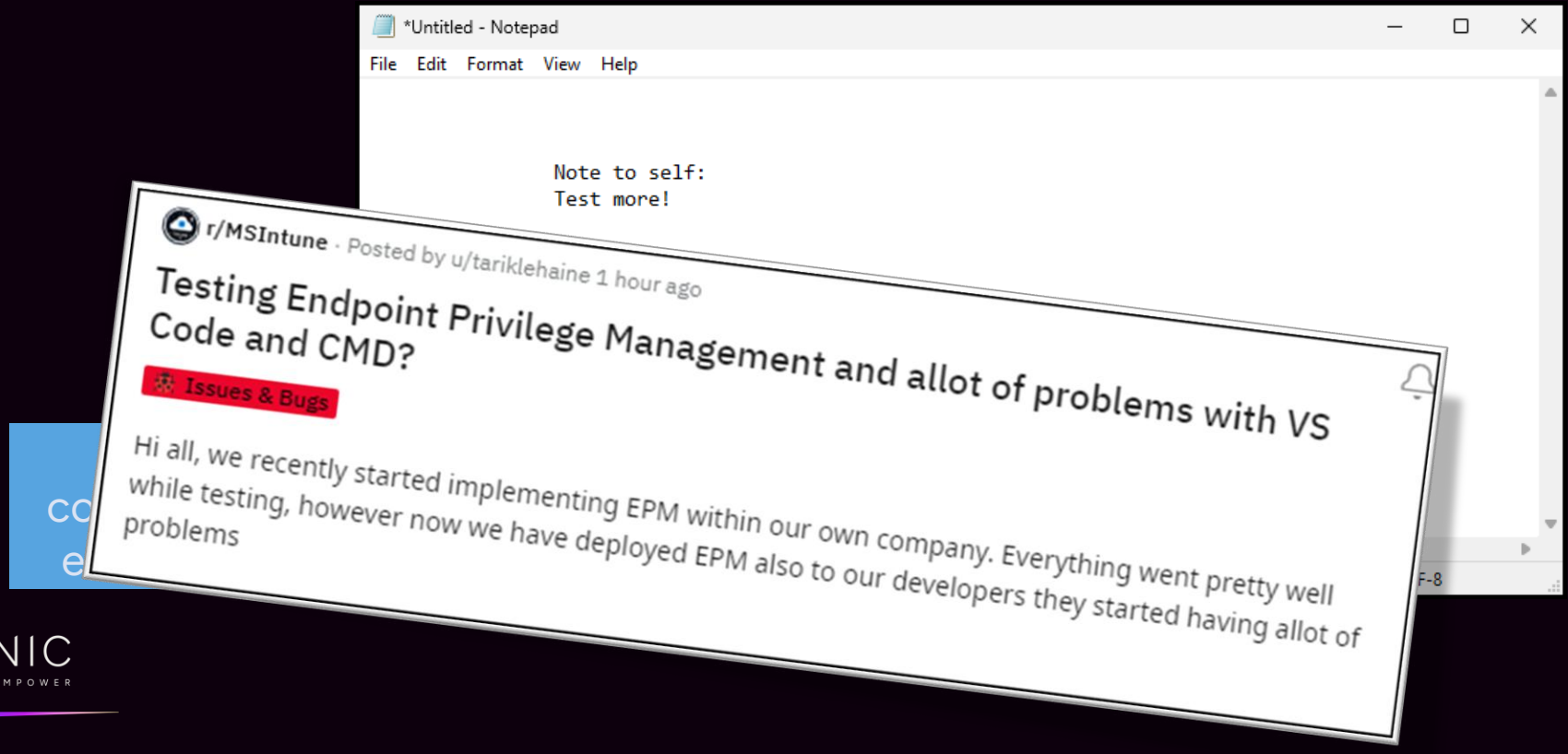


User completes elevation

NIC EMPOWER

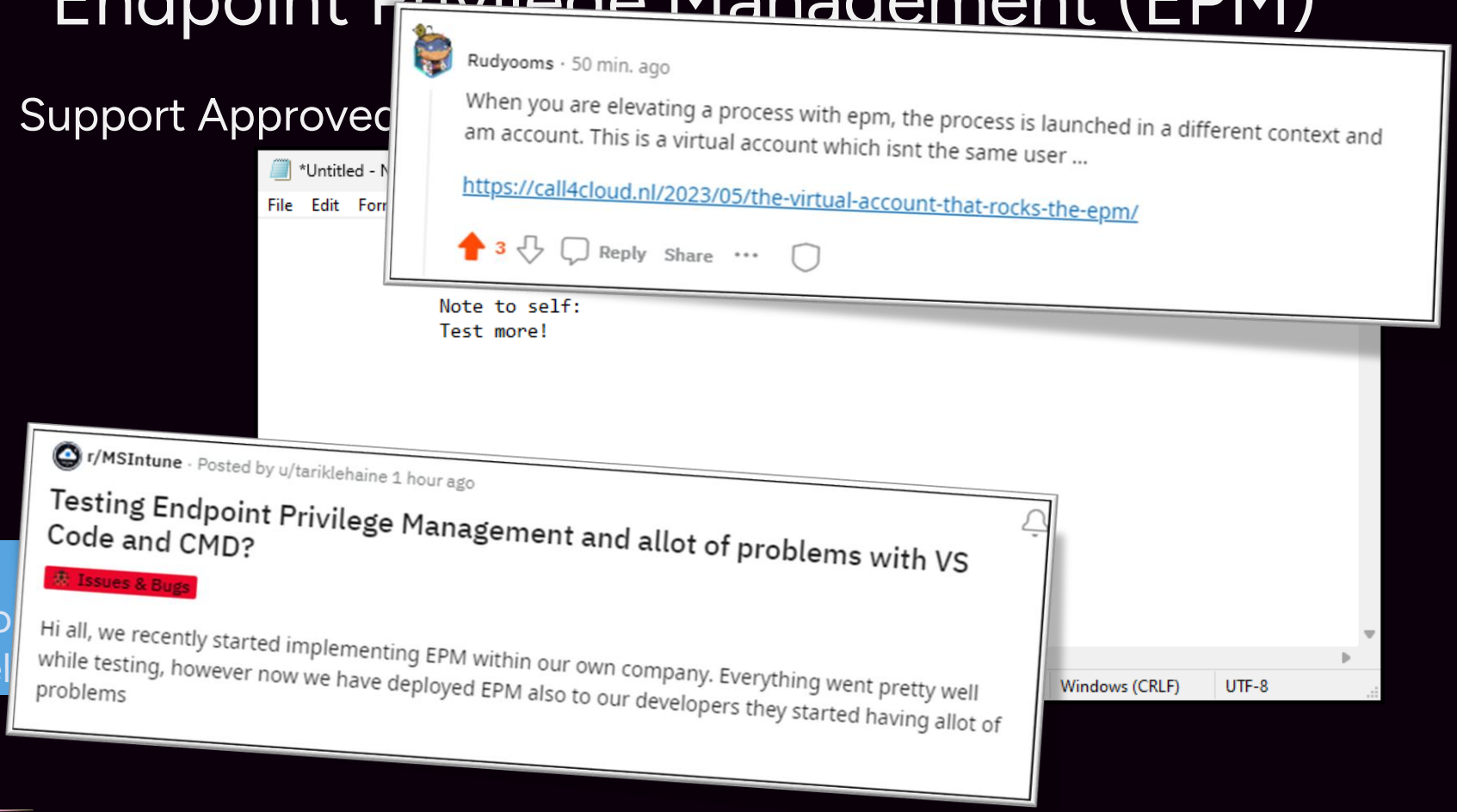
Endpoint Privilege Management (EPM)

- Support Approved workflow

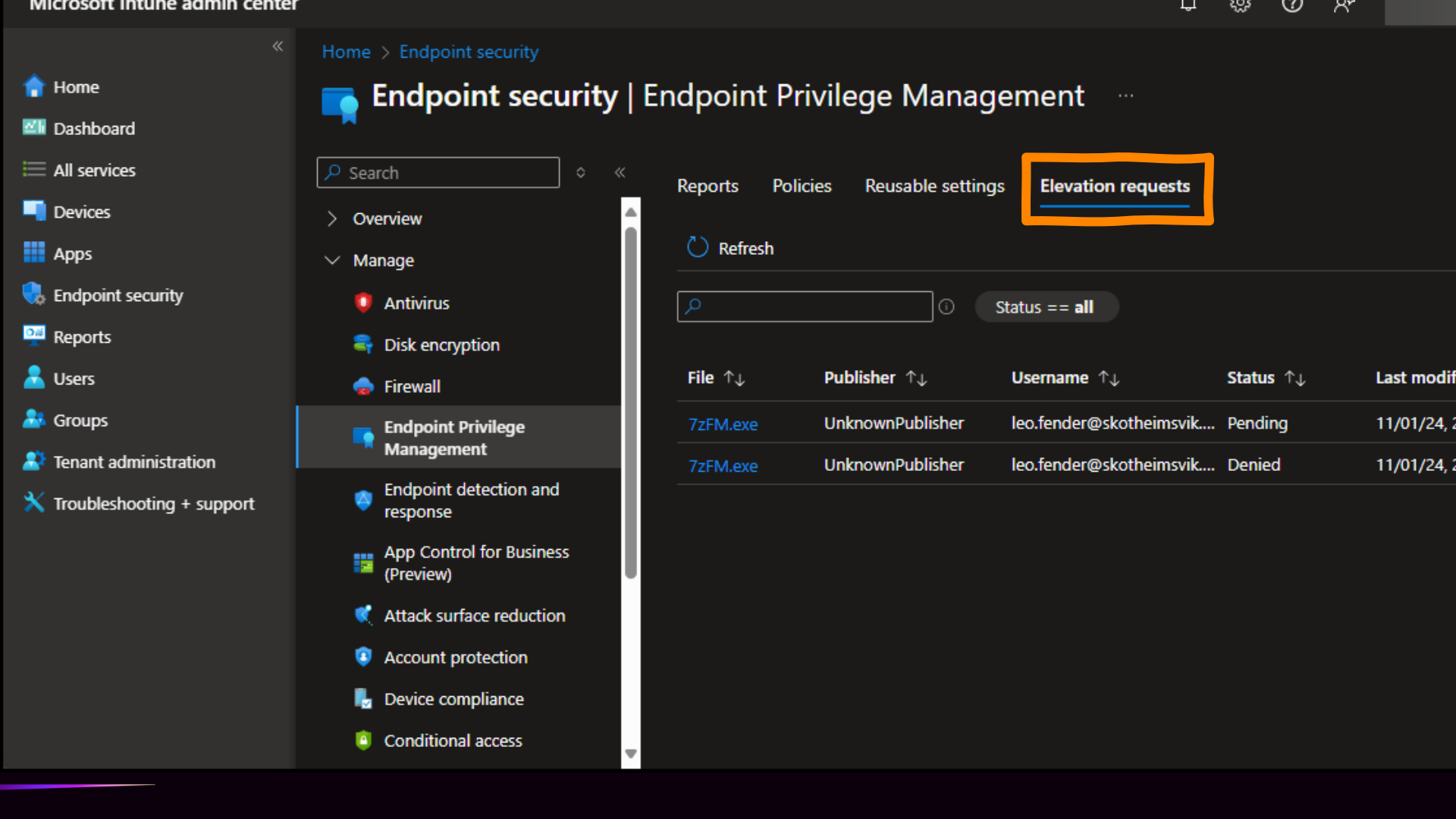


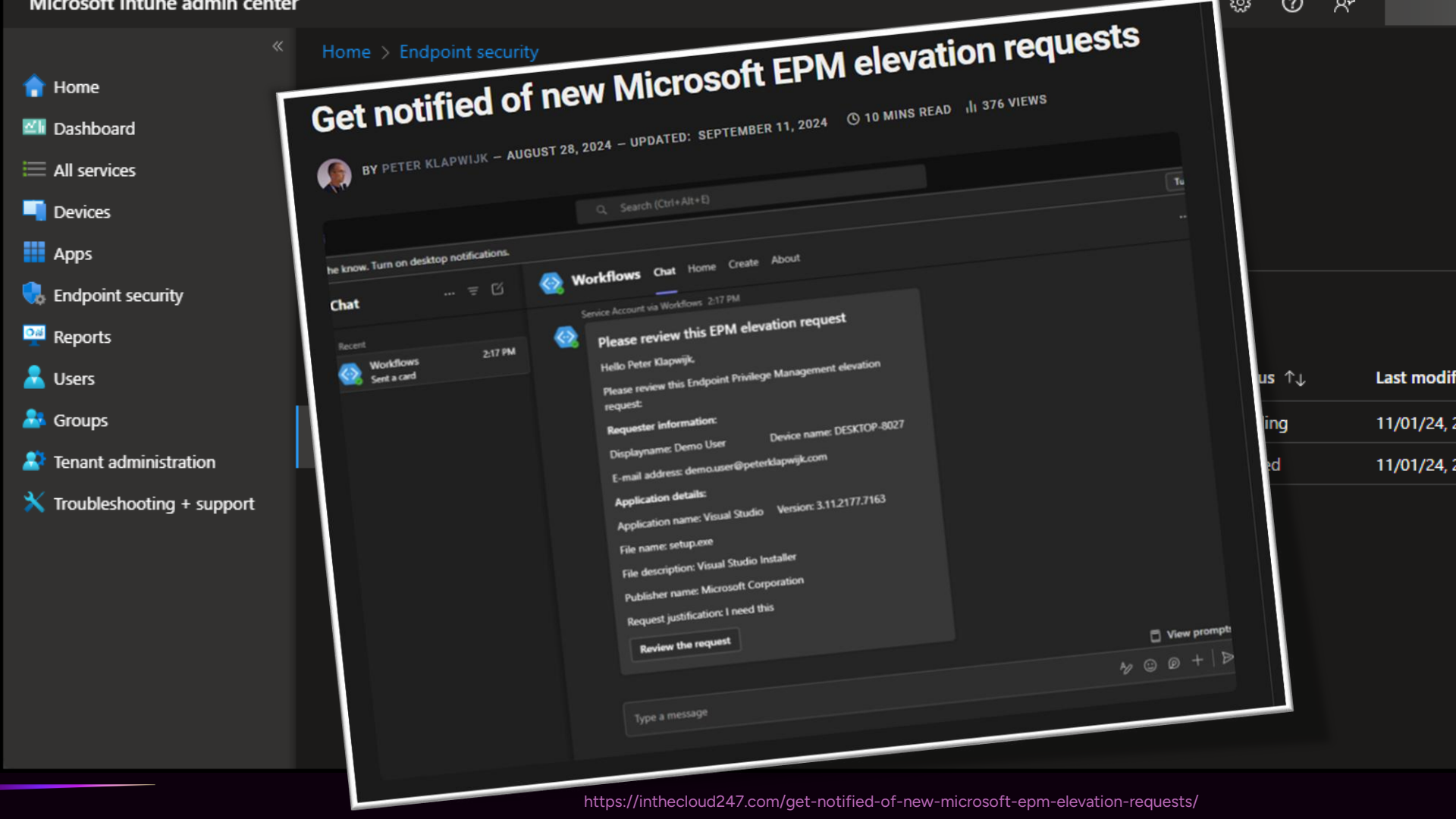
Endpoint Privilege Management (EPM)

- Support Approved

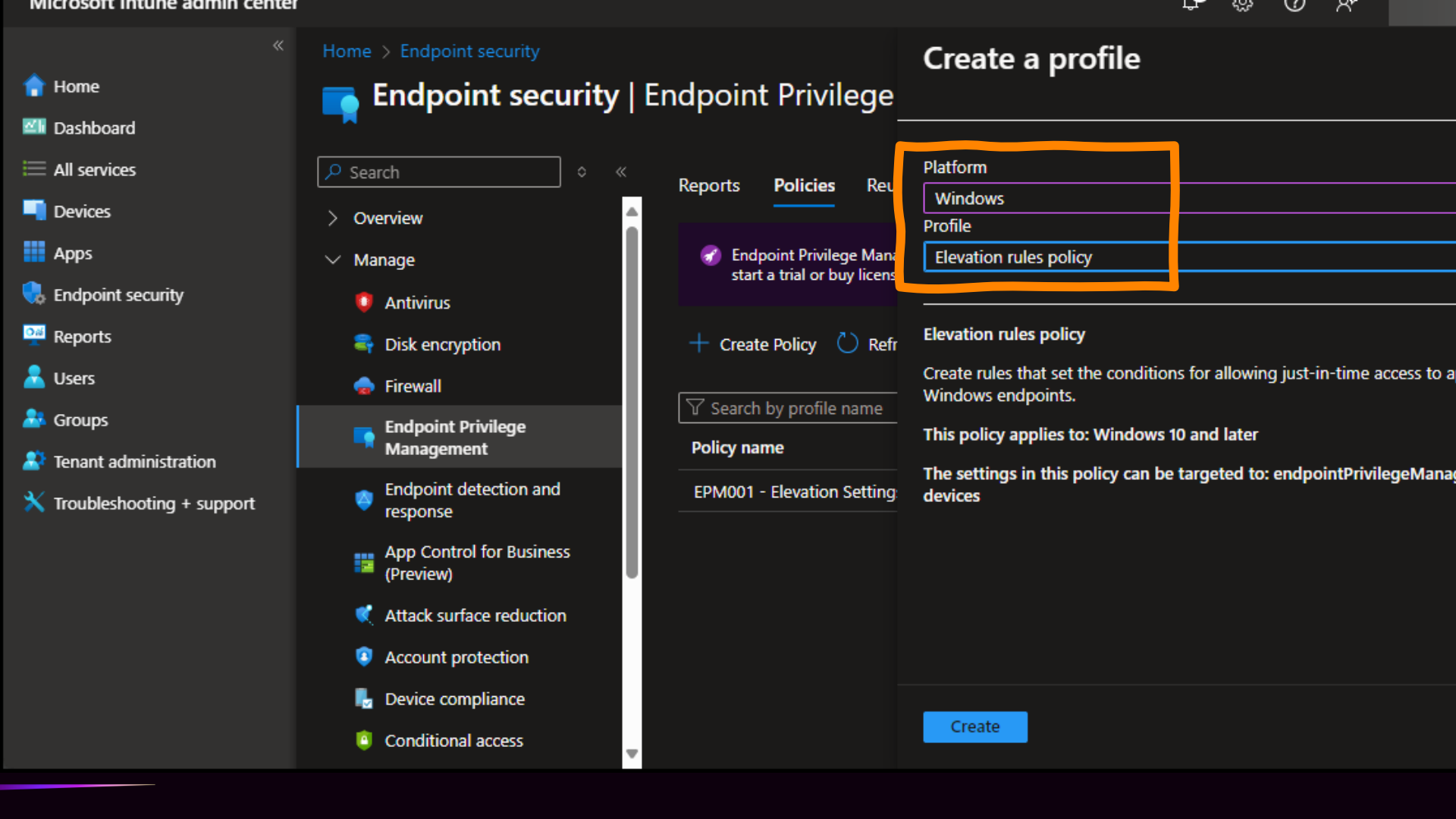


NIC
EMPOWER


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
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
Reports
Policies
Reusable settings
Elevation requests
Refresh
Status == all
File
Publisher
Username
Status
Last modif
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Pending
11/01/24,
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Denied
11/01/24,



https://inthecloud247.com/get-notified-of-new-microsoft-epm-elevation-requests/


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege
Search
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
Reports
Policies
Endpoint Privilege Mana
start a trial or buy licens
Create Policy
Refr
Search by profile name
Policy name
EPM001 - Elevation Setting
Create a profile
Platform
Windows
Profile
Elevation rules policy
Elevation rules policy
Create rules that set the conditions for allowing just-in-time access to a
Windows endpoints.
This policy applies to: Windows 10 and later
The settings in this policy can be targeted to: endpointPrivilegeManag
devices
Create

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Create profile

Elevation rules policy

1 Basics | 2 Configuration settings | 3 Scope tags | 4 Assignments | 5 Review + create

Name * EPM002 - 7ZIP File Manager Elevation Rule

Description Elevation Rule to allow 7ZIP File Manager

Platform Windows

Previous Next

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Create profile

Elevation rules policy

Basics | 2 Configuration settings | 3 Scope tags | 4 Assignments | 5 Review + create

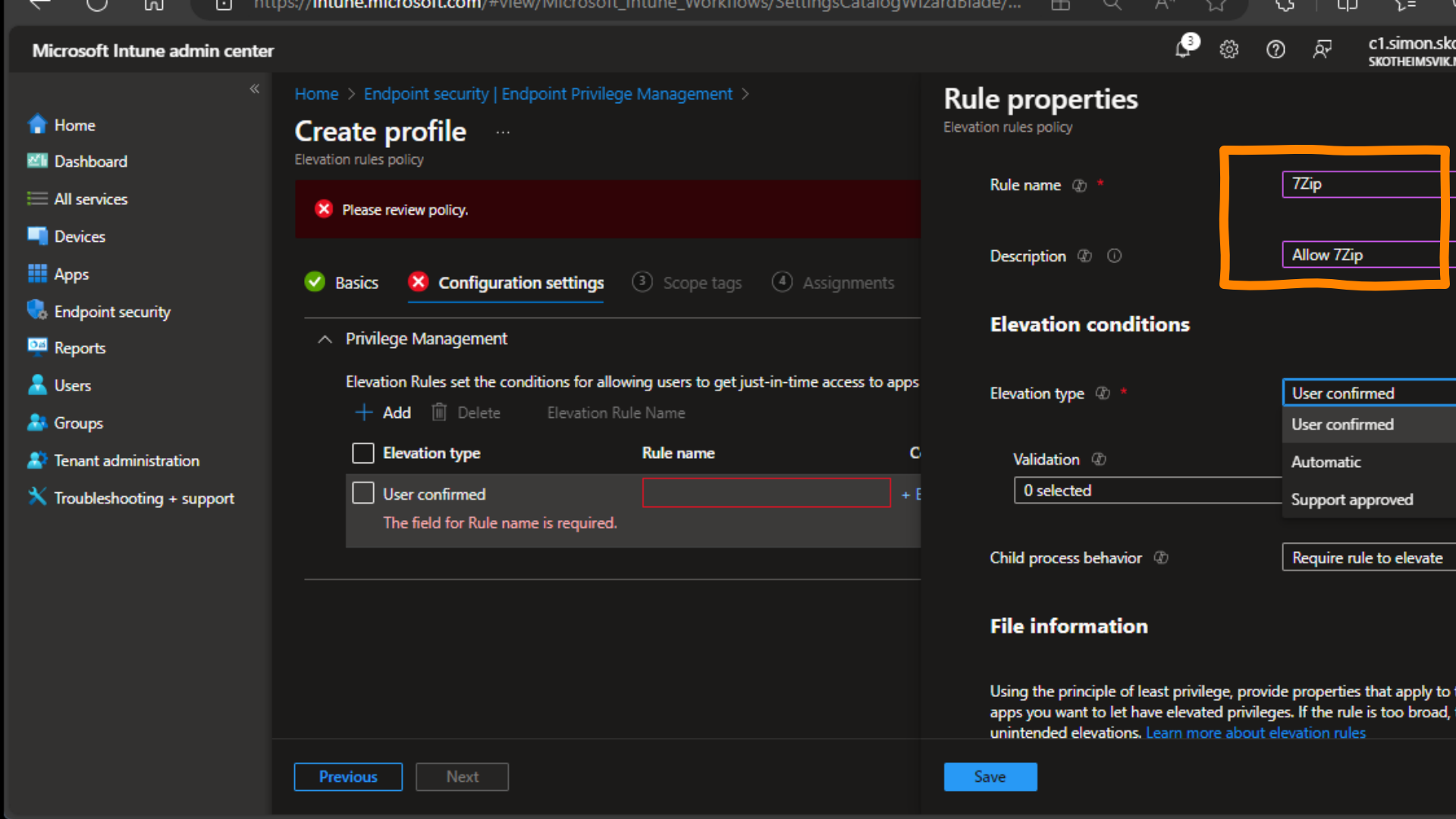
Privilege Management

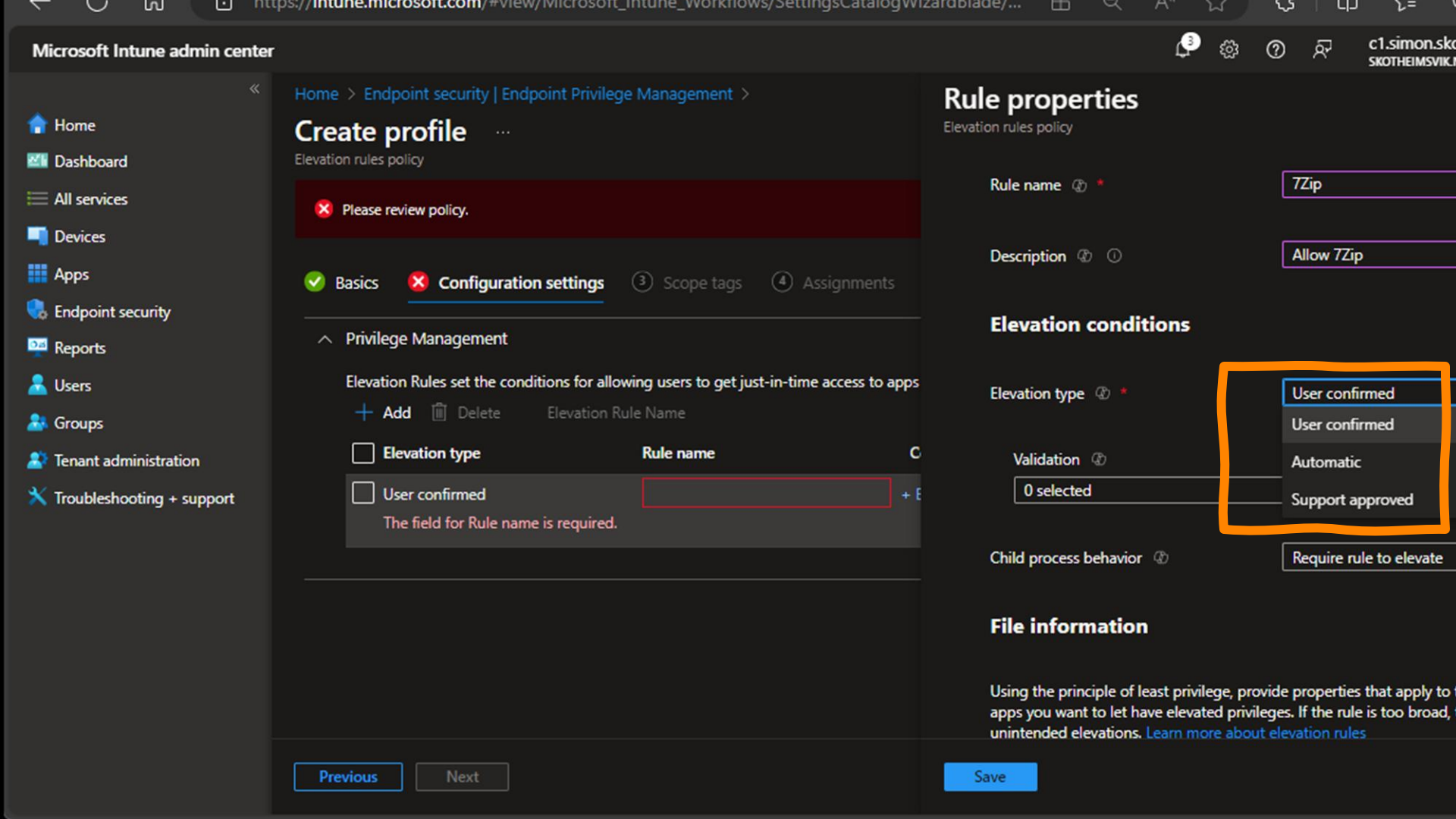
Elevation Rules set the conditions for allowing users to get just-in-time access to apps and files on their devices.

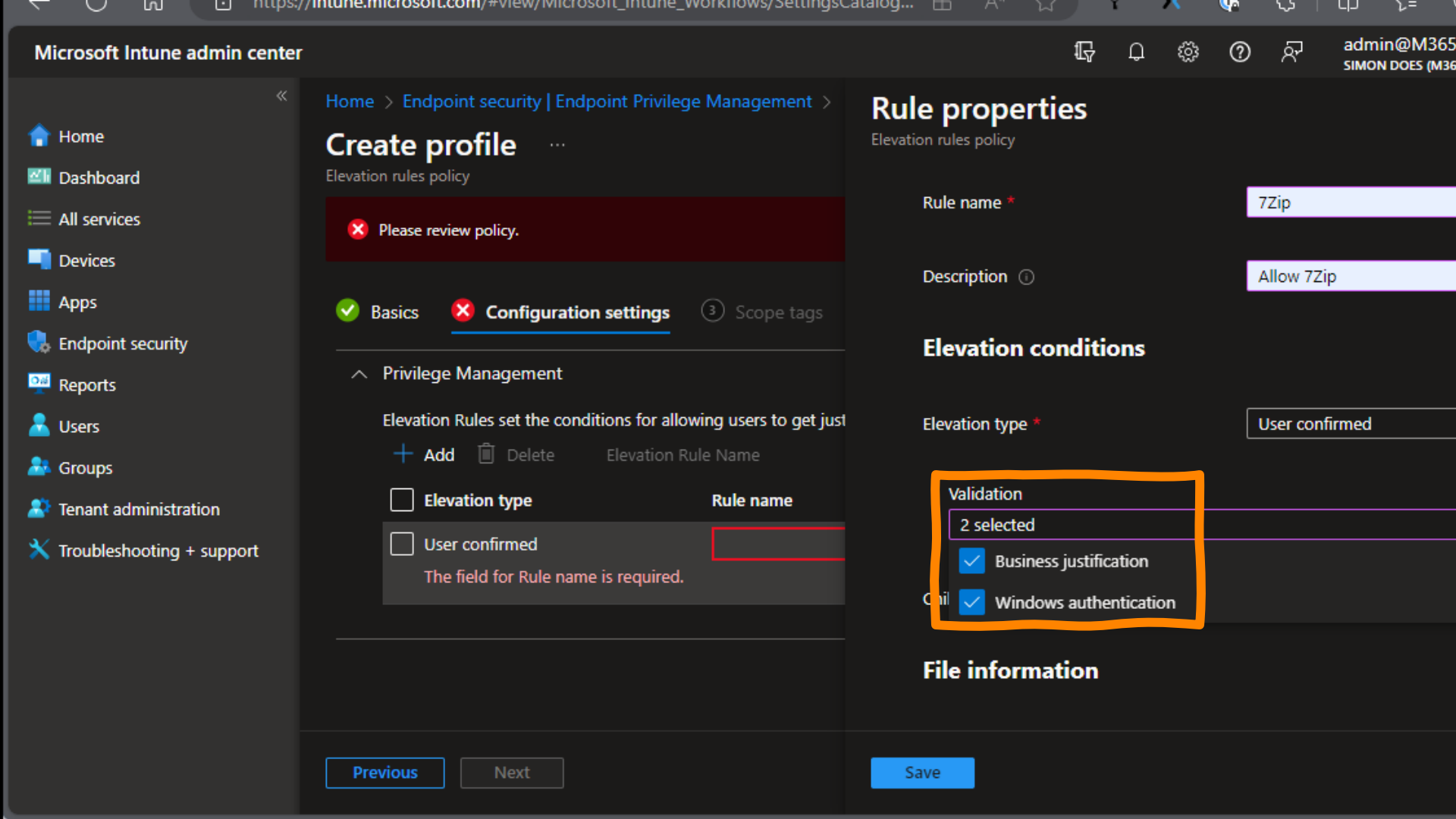
+ Add | Delete | Elevation Rule Name

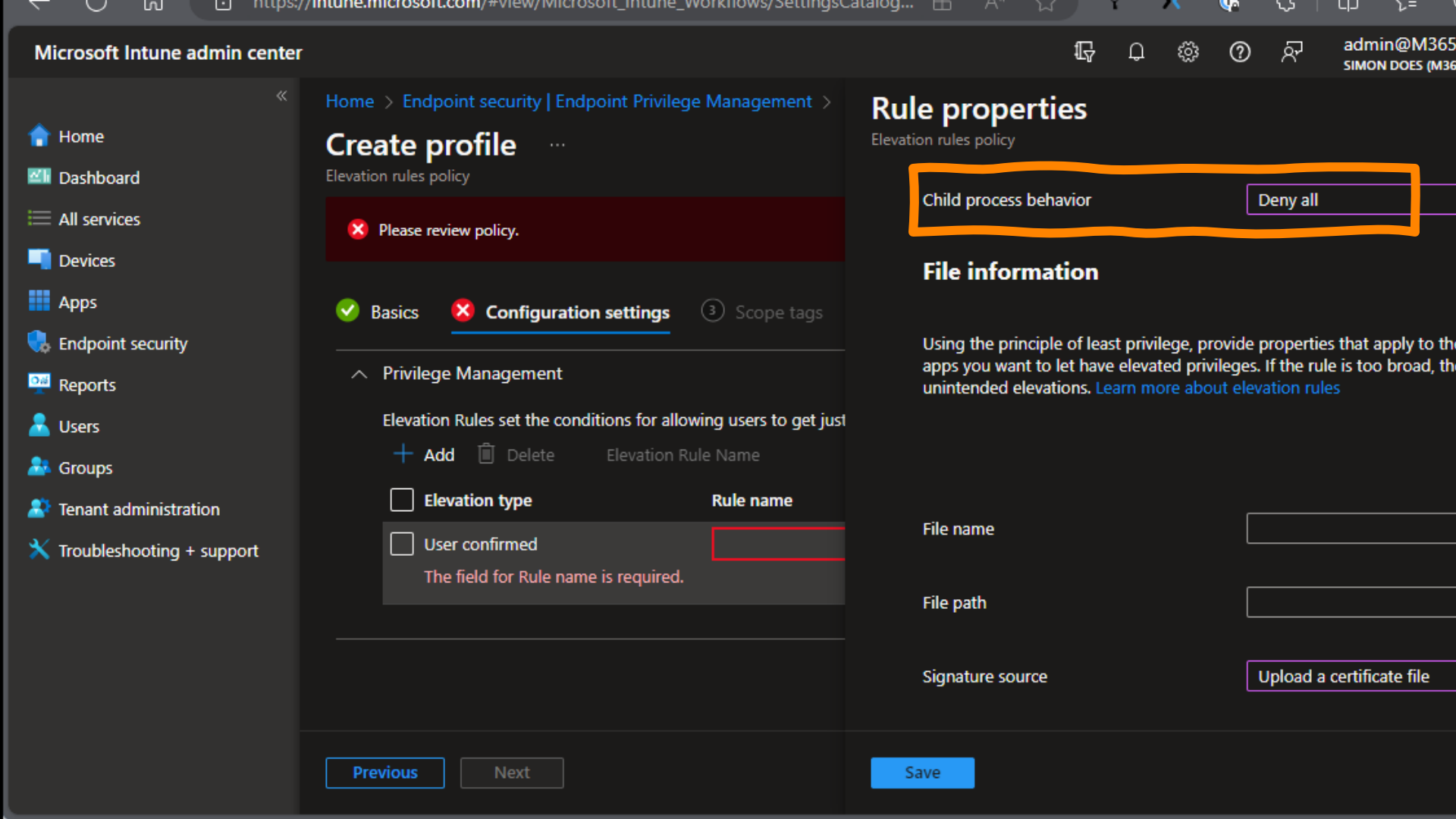
Elevation type	Rule name	Configure settings
User confirmed		+ Edit instance

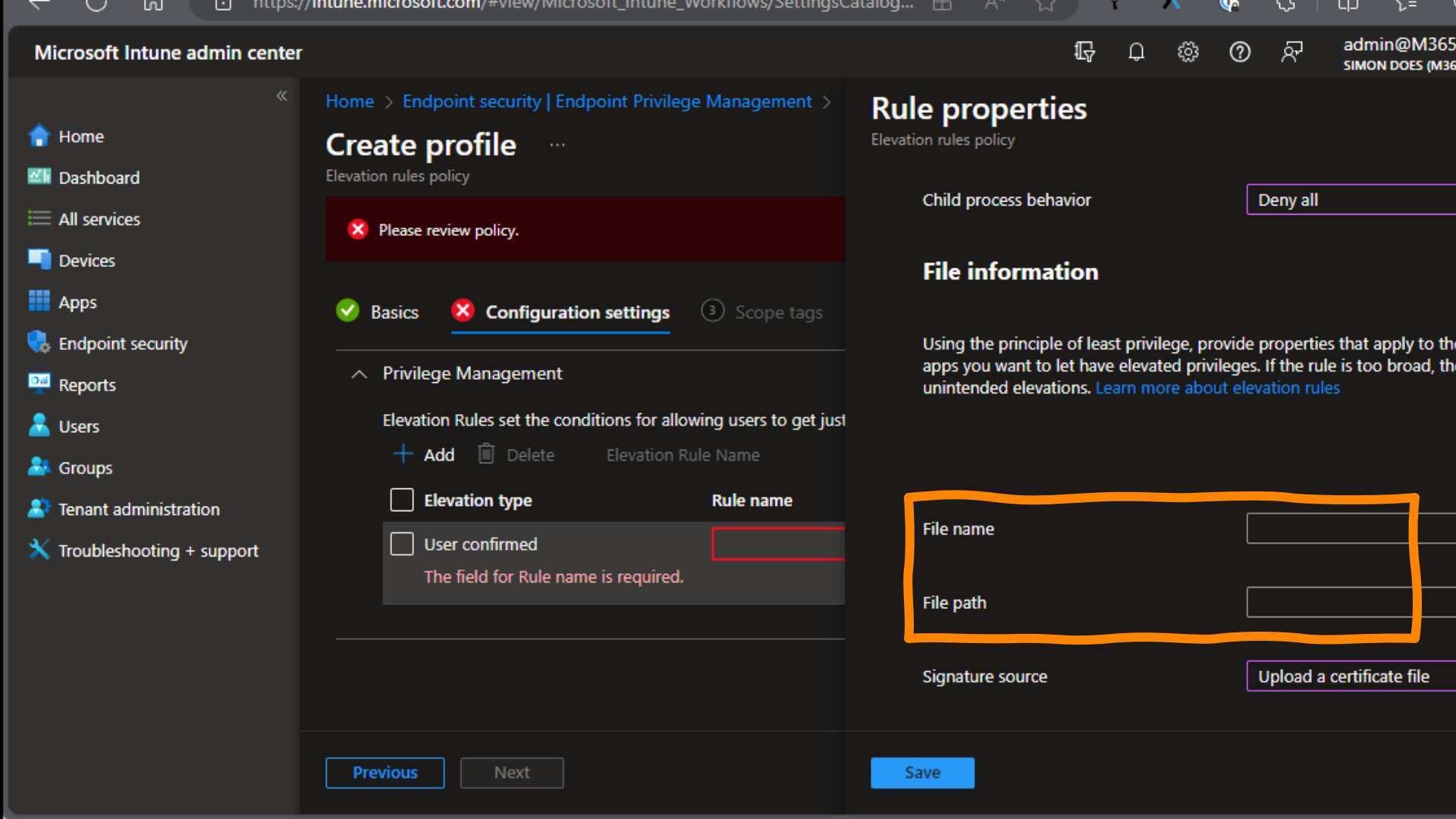
Previous | Next

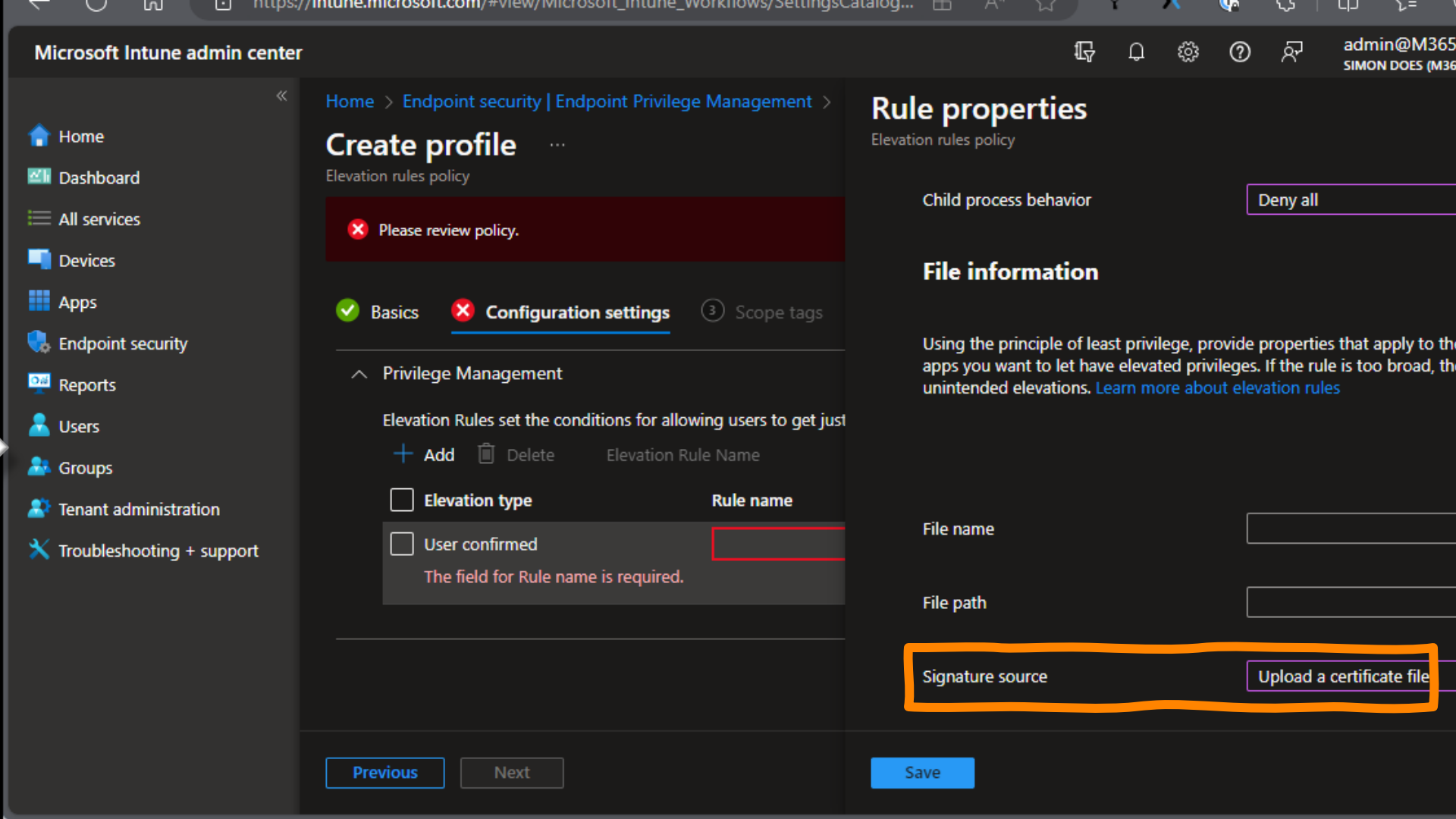

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
4 Assignments
Privilege Management
Elevation Rules set the conditions for allowing users to get just-in-time access to apps
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
Rule name *
7Zip
Description
Allow 7Zip
Elevation conditions
Elevation type *
User confirmed
User confirmed
Automatic
Support approved
Validation
0 selected
Child process behavior
Require rule to elevate
File information
Using the principle of least privilege, provide properties that apply to
apps you want to let have elevated privileges. If the rule is too broad,
unintended elevations. Learn more about elevation rules
Save

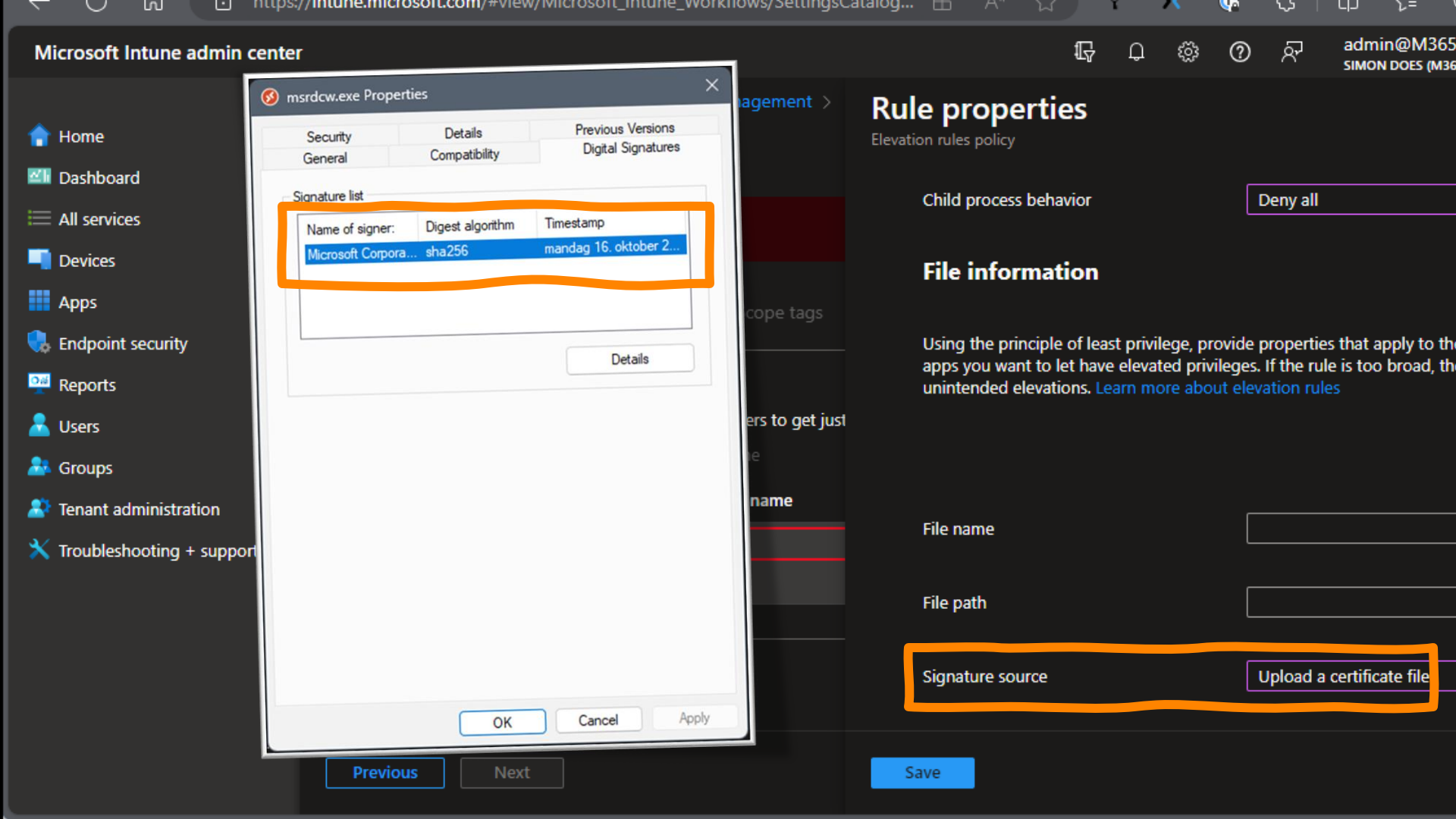

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
Scope tags
Assignments
Privilege Management
Elevation Rules set the conditions for allowing users to get just-in-time access to apps
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
Rule name
7Zip
Description
Allow 7Zip
Elevation conditions
Elevation type
User confirmed
User confirmed
Automatic
Support approved
Validation
0 selected
Child process behavior
Require rule to elevate
File information
Using the principle of least privilege, provide properties that apply to
apps you want to let have elevated privileges. If the rule is too broad,
unintended elevations. Learn more about elevation rules
Save

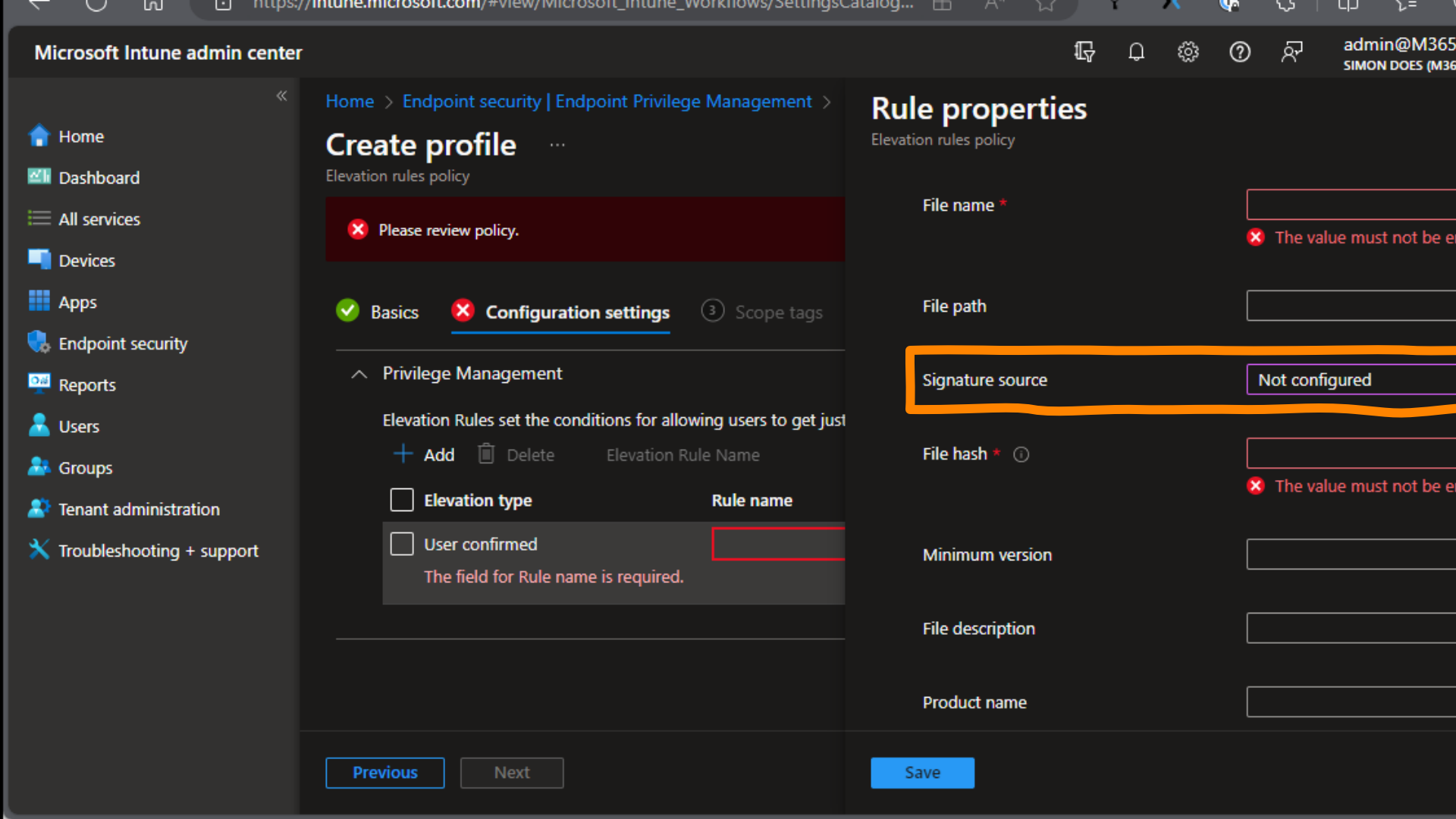

Microsoft Intune admin center
admin@M365
SIMON DOES (M36
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
Rule name *
7Zip
Description
Allow 7Zip
Elevation conditions
Elevation type *
User confirmed
Validation
2 selected
Business justification
Windows authentication
File information
Save

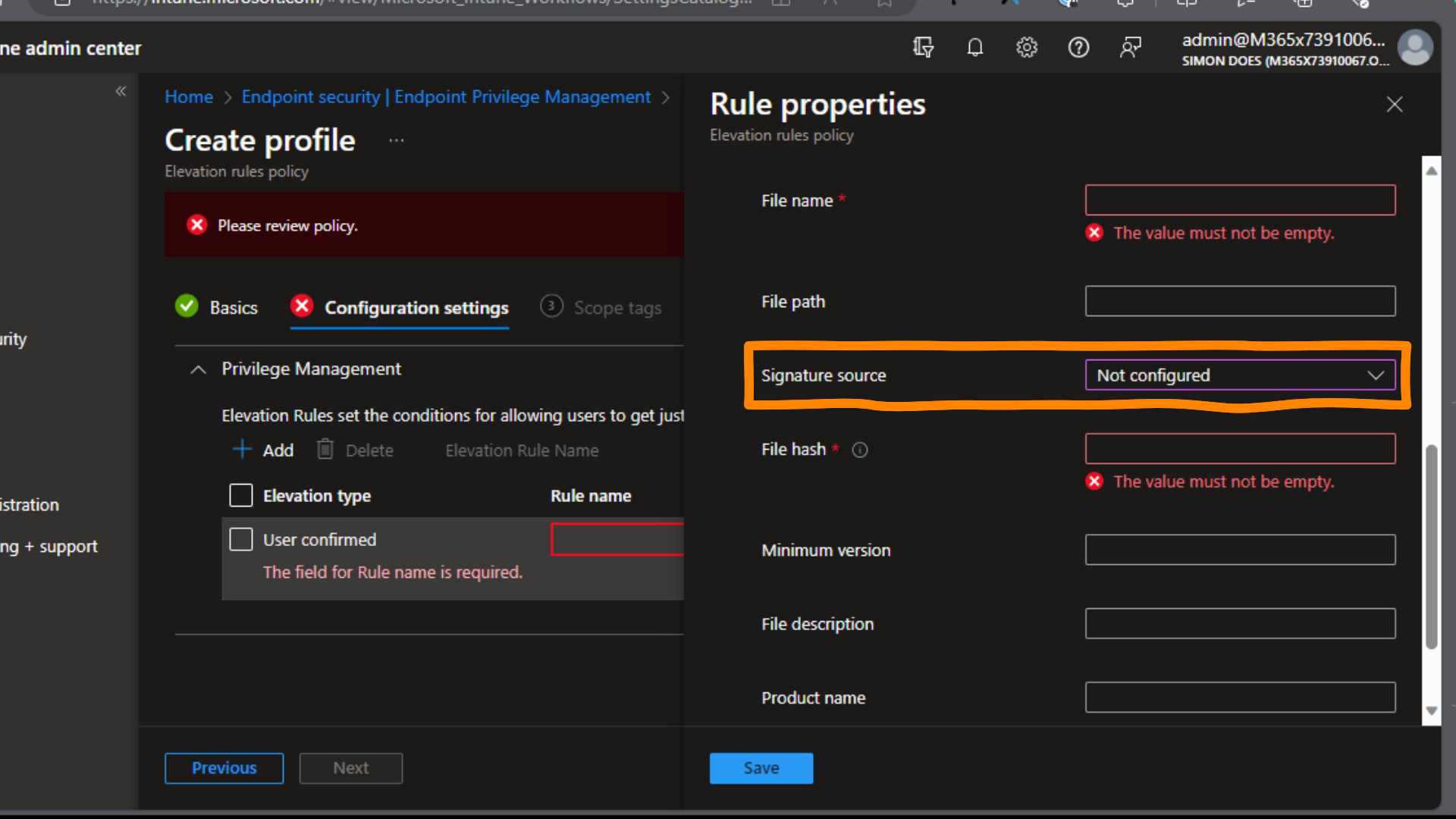

Microsoft Intune admin center
admin@M365
SIMON DOES (M36
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
Child process behavior
Deny all
File information
Using the principle of least privilege, provide properties that apply to th
apps you want to let have elevated privileges. If the rule is too broad, th
unintended elevations. Learn more about elevation rules
File name
File path
Signature source
Upload a certificate file
Save

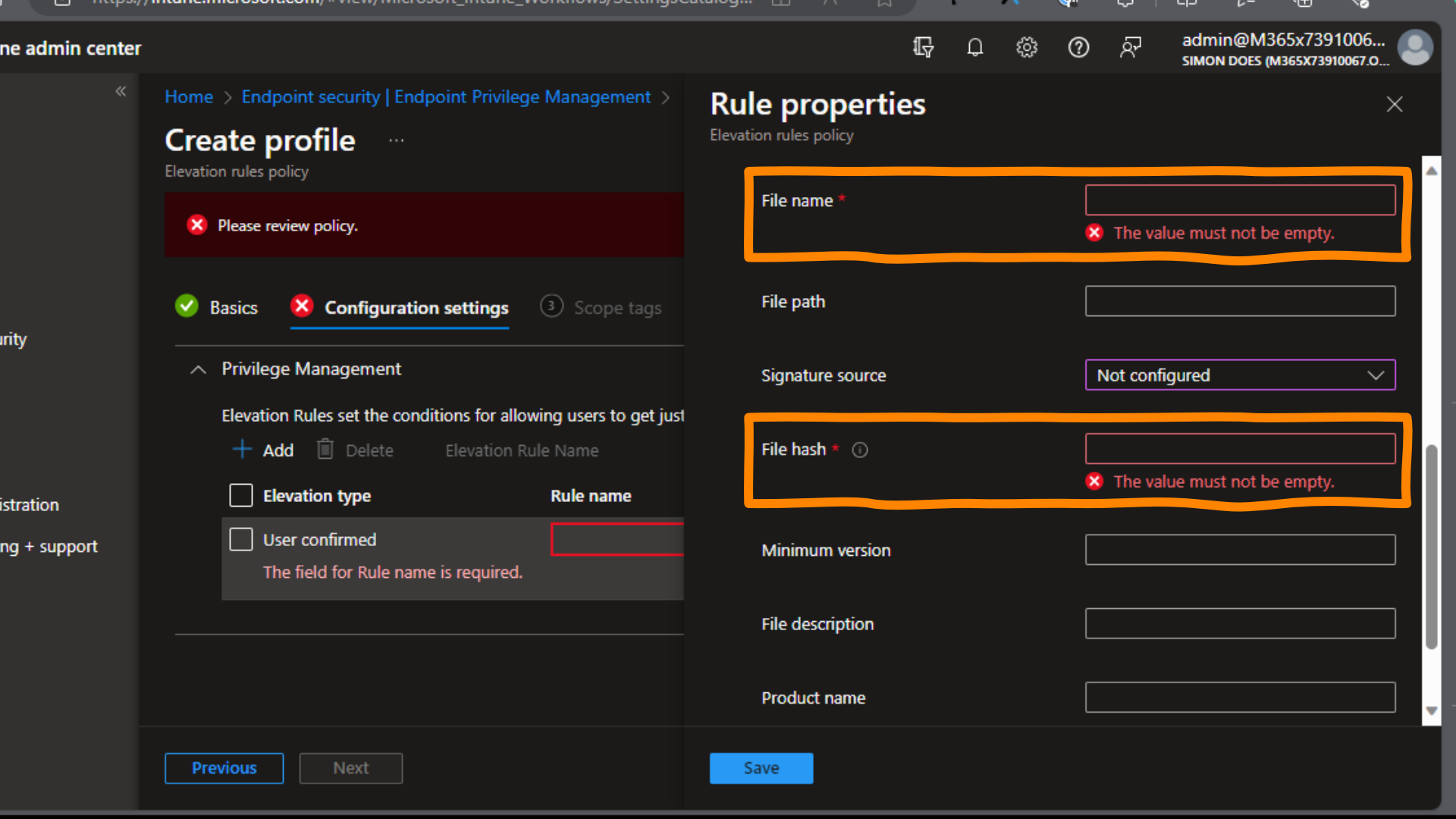

Microsoft Intune admin center
admin@M365
SIMON DOES (M36
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
Child process behavior
Deny all
File information
Using the principle of least privilege, provide properties that apply to th
apps you want to let have elevated privileges. If the rule is too broad, th
unintended elevations. Learn more about elevation rules
File name
File path
Signature source
Upload a certificate file
Save

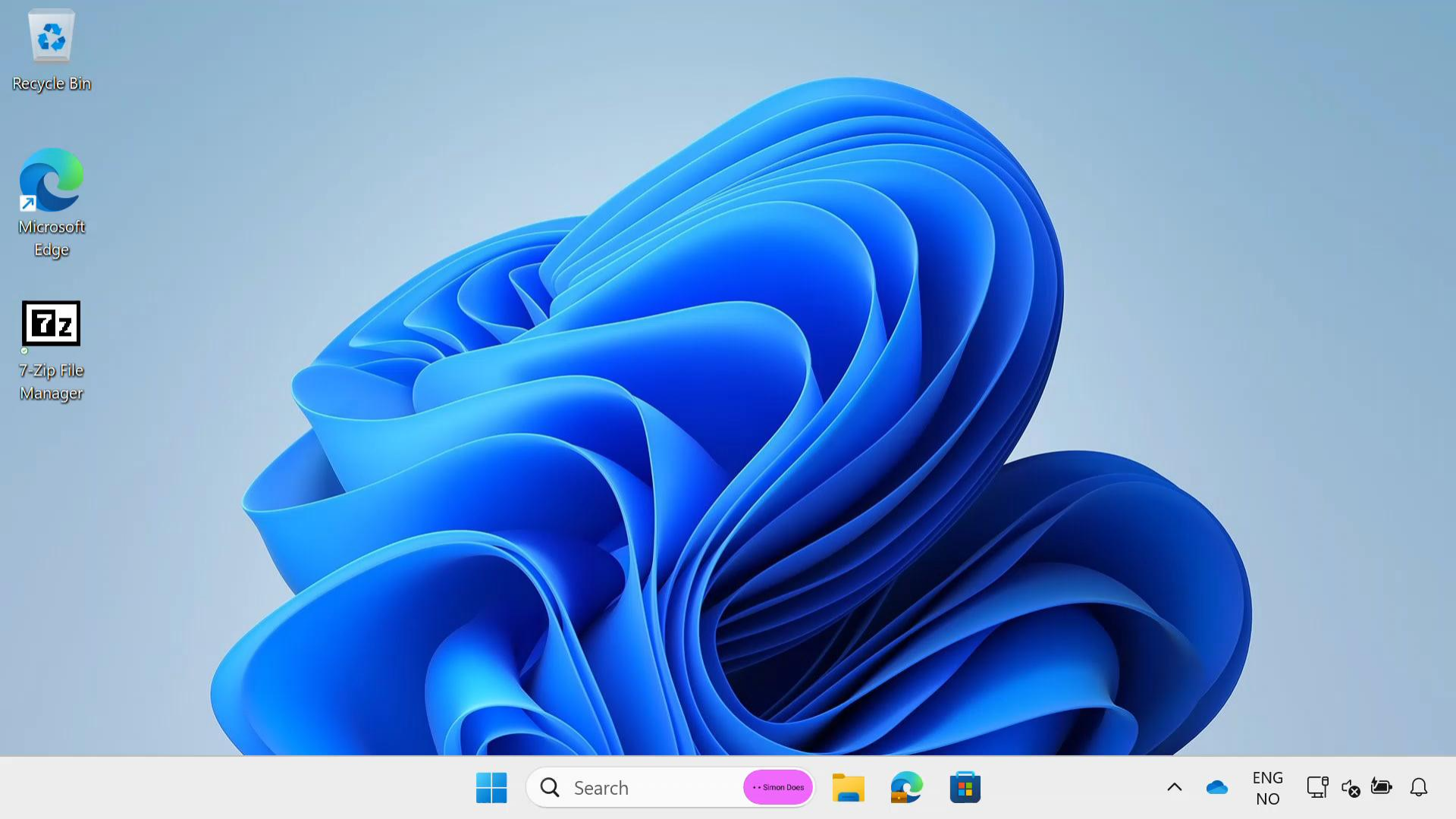

Microsoft Intune admin center
admin@M365
SIMON DOES (M36
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
Child process behavior
Deny all
File information
Using the principle of least privilege, provide properties that apply to th
apps you want to let have elevated privileges. If the rule is too broad, th
unintended elevations. Learn more about elevation rules
File name
File path
Signature source
Upload a certificate file
Save

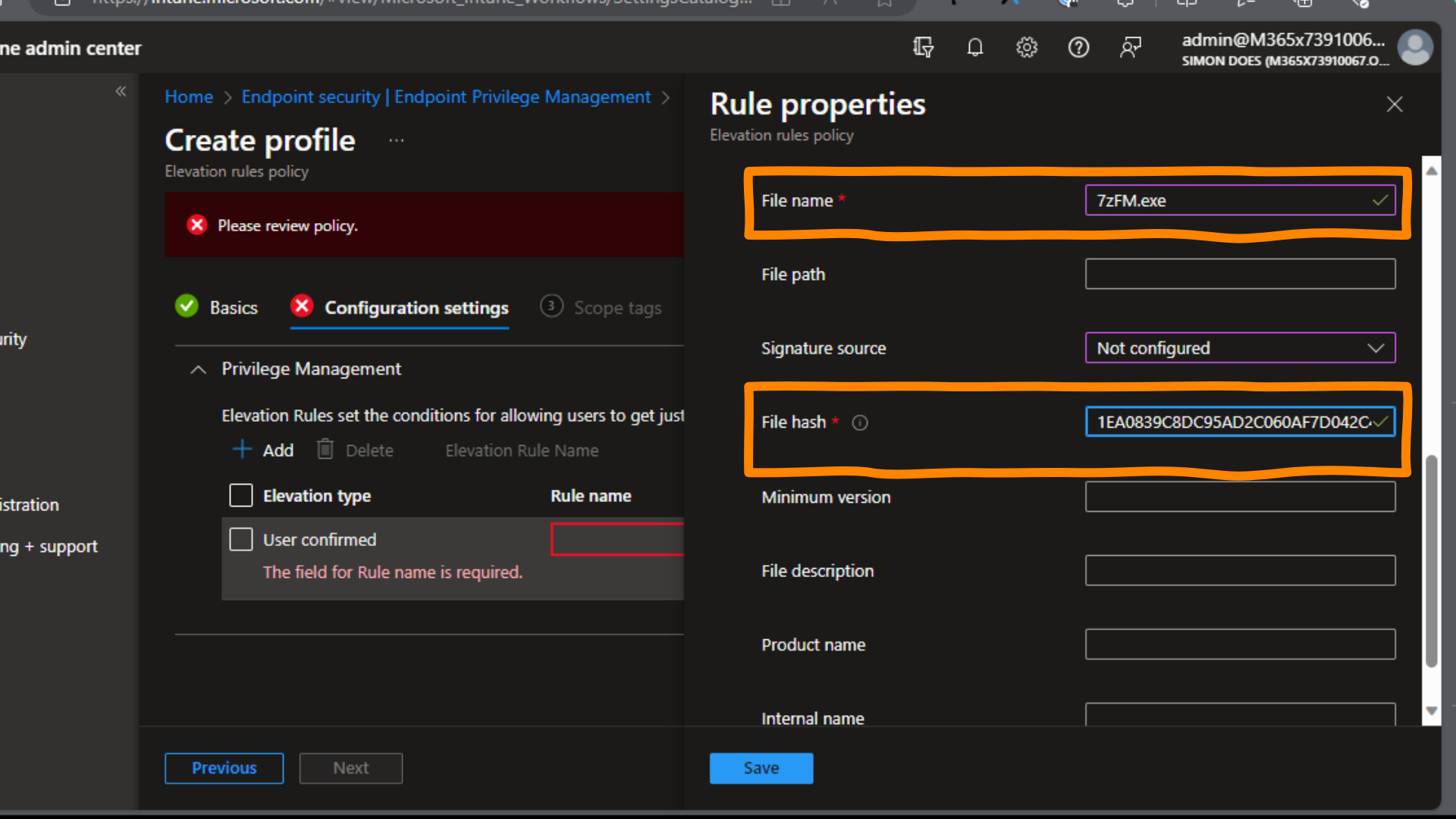

Microsoft Intune admin center
admin@M365
SIMON DOES (M36
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
msrdcw.exe Properties
Security
Details
Previous Versions
General
Compatibility
Digital Signatures
Signature list
Name of signer:
Digest algorithm
Timestamp
Microsoft Corpora...
sha256
mandag 16. oktober 2...
Details
OK
Cancel
Apply
Rule properties
Elevation rules policy
Child process behavior
Deny all
File information
Using the principle of least privilege, provide properties that apply to th
apps you want to let have elevated privileges. If the rule is too broad, th
unintended elevations. Learn more about elevation rules
File name
File path
Signature source
Upload a certificate file
Previous
Next
Save


Microsoft Intune admin center
admin@M365
SIMON DOES (M36
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
File name *
The value must not be e
File path
Signature source
Not configured
File hash *
The value must not be e
Minimum version
File description
Product name
Save


ne admin center
admin@M365x7391006...
SIMON DOES (M365X73910067.O...
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
File name *
The value must not be empty.
File path
Signature source
Not configured
File hash *
The value must not be empty.
Minimum version
File description
Product name
Save


ne admin center
admin@M365x7391006...
SIMON DOES (M365X73910067.O...
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
File name *
The value must not be empty.
File path
Signature source
Not configured
File hash *
The value must not be empty.
Minimum version
File description
Product name
Save


Recycle Bin
Microsoft Edge
7-Zip File Manager
Search
Simon Does
ENG
NO


ne admin center
admin@M365x7391006...
SIMON DOES (M365X73910067.O...
Home > Endpoint security | Endpoint Privilege Management >
Create profile
Elevation rules policy
Please review policy.
Basics
Configuration settings
3 Scope tags
Privilege Management
Elevation Rules set the conditions for allowing users to get just
Add
Delete
Elevation Rule Name
Elevation type
Rule name
User confirmed
The field for Rule name is required.
Previous
Next
Rule properties
Elevation rules policy
File name *
7zFM.exe
File path
Signature source
Not configured
File hash *
1EA0839C8DC95AD2C060AF7D042C
Minimum version
File description
Product name
Internal name
Save

Create profile

Elevation rules policy

Basics | 2 Configuration settings | 3 Scope tags | 4 Assignments | 5 Review + create

Privilege Management

Elevation Rules set the conditions for allowing users to get just-in-time access to apps and files on their devices.

+ Add | Delete | Elevation Rule Name

Elevation type	Rule name	Configure settings
User confirmed	7Zip	+ Edit instance

Previous | Next

Create profile

Elevation rules policy

Basics | Configuration settings | Scope tags | 4 Assignments | 5 Review + create

Included groups

Add groups | Add all users | Add all devices

Groups	Group Members	Remove
All devices		Remove

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Add groups

Groups	Group Members	Remove
No groups selected		

Previous | Next

Endpoint security | Endpoint Privilege Management

Search

Overview

Overview
All devices
Security baselines
Security tasks

Manage

Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)

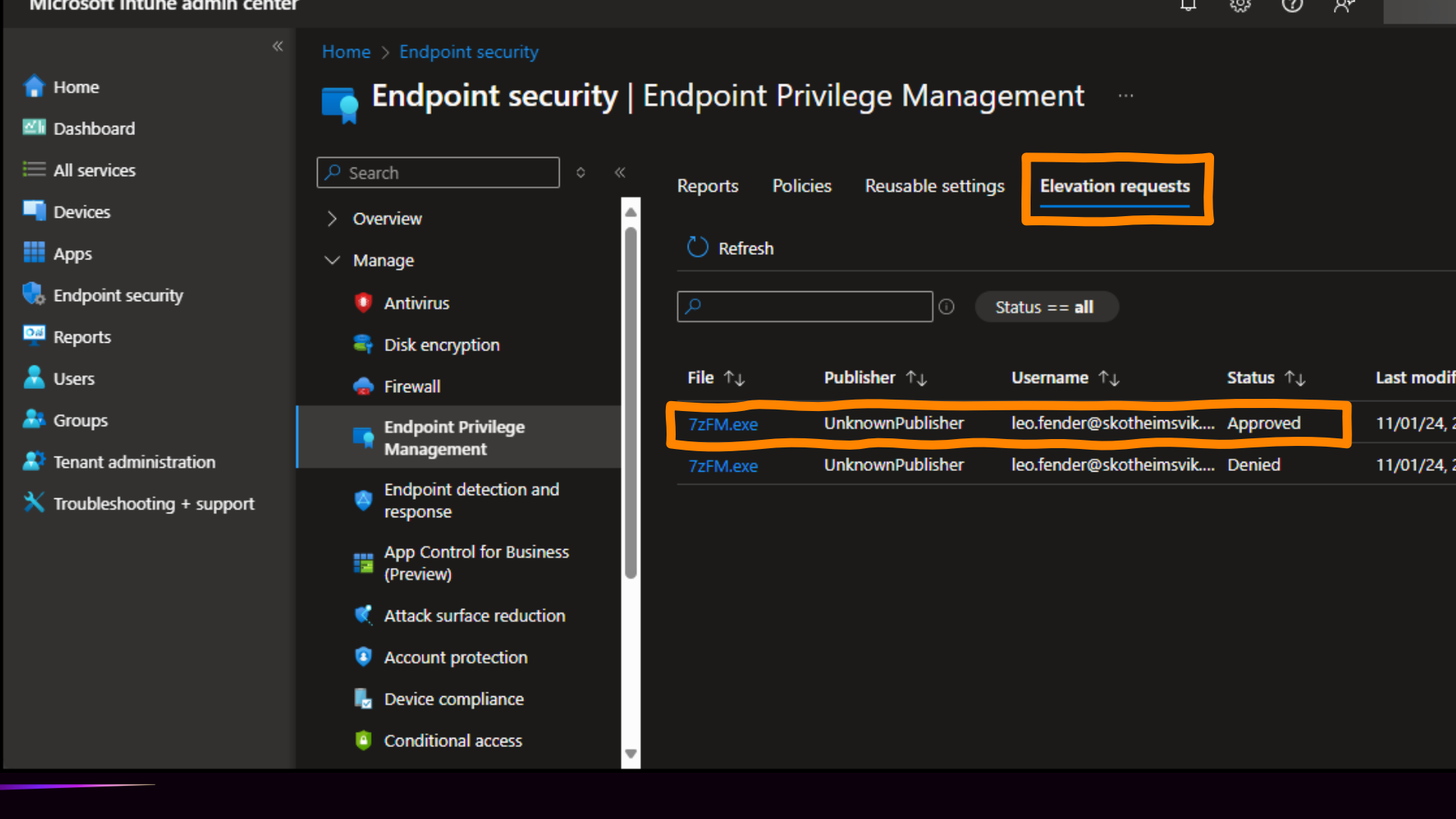
Reports | Policies | Reusable settings

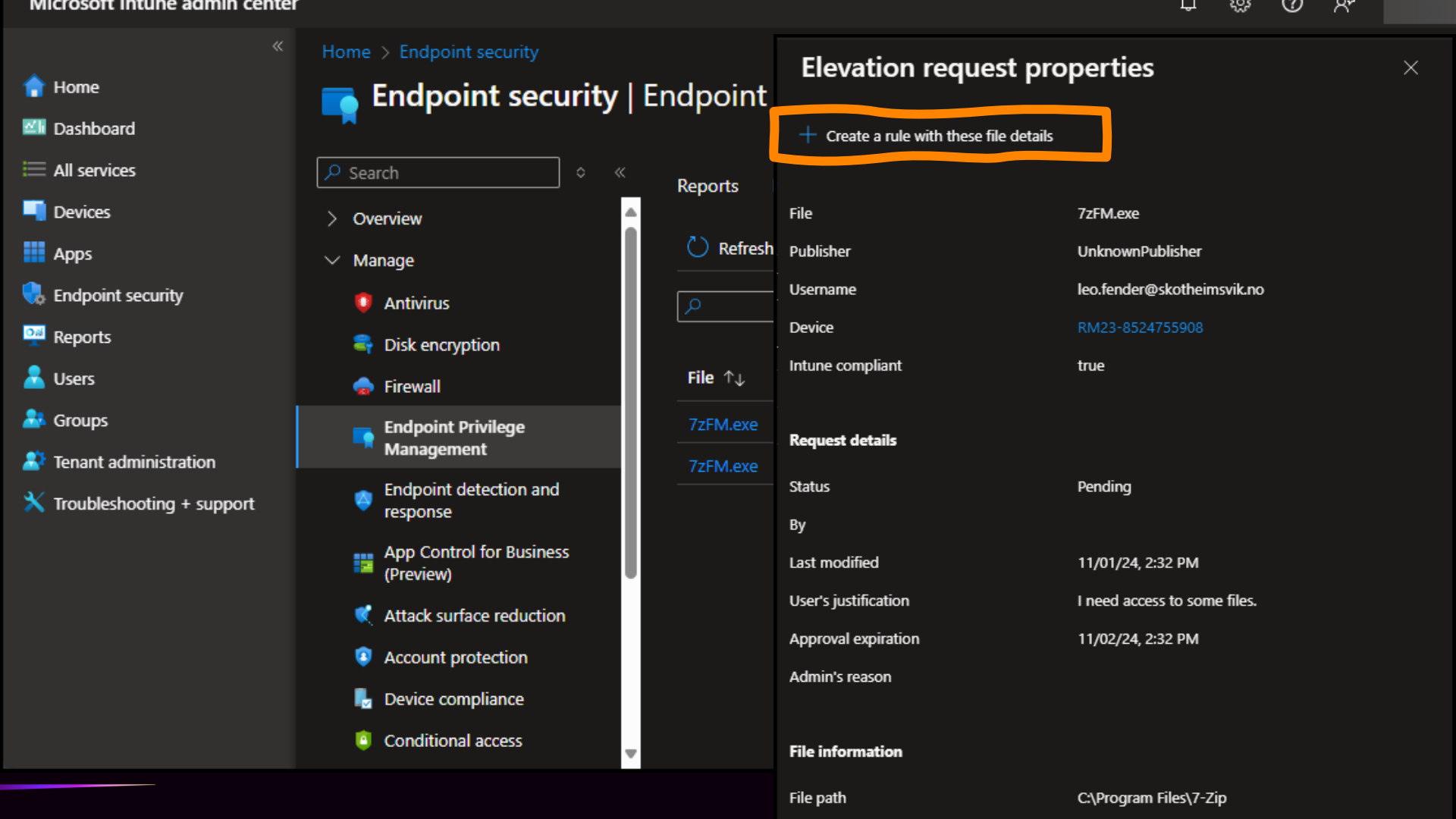
90 days left in trial - to keep using Endpoint Privilege Management after the trial ends, you will need to buy licenses.

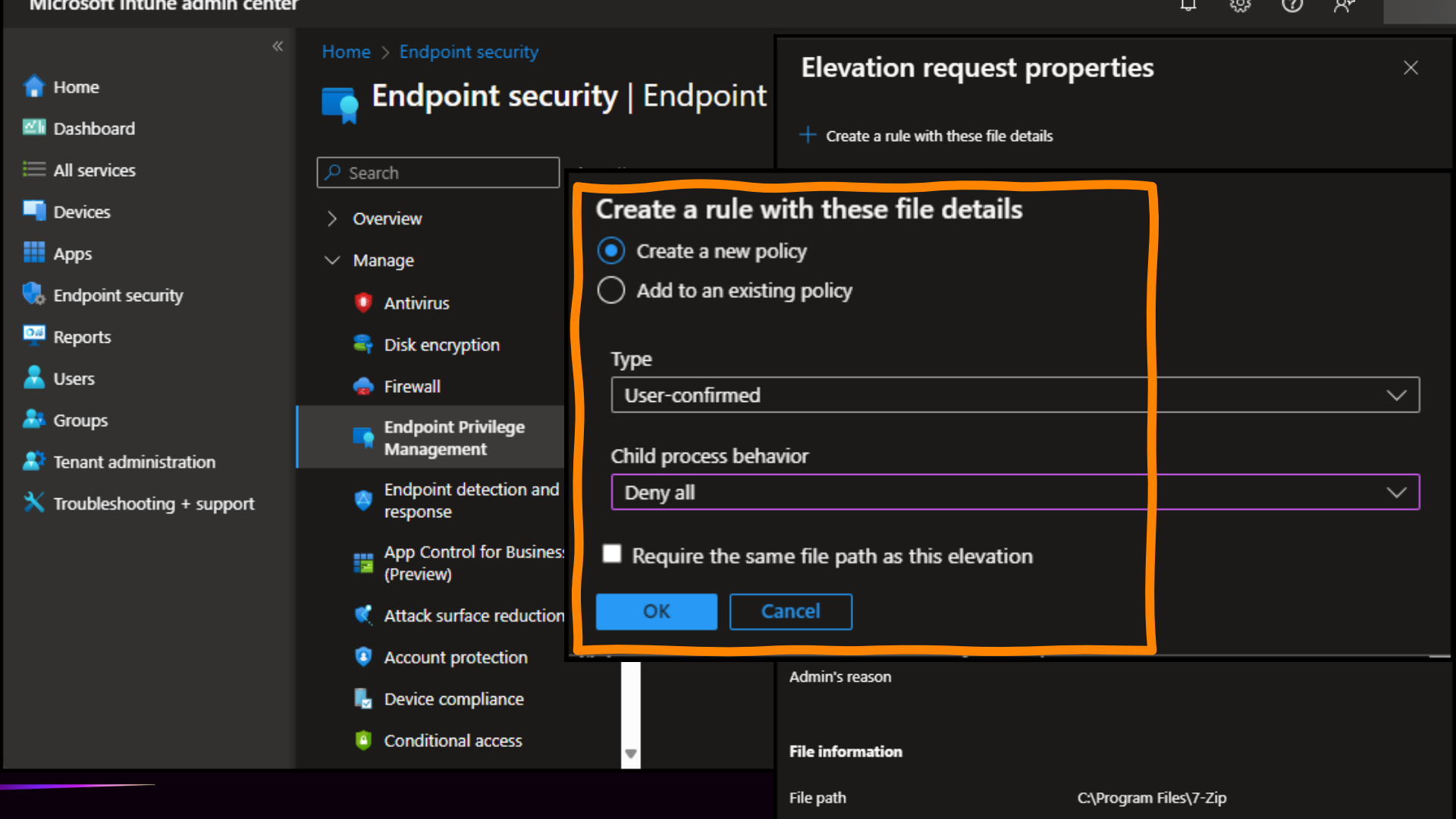
+ Create Policy | Refresh | Export

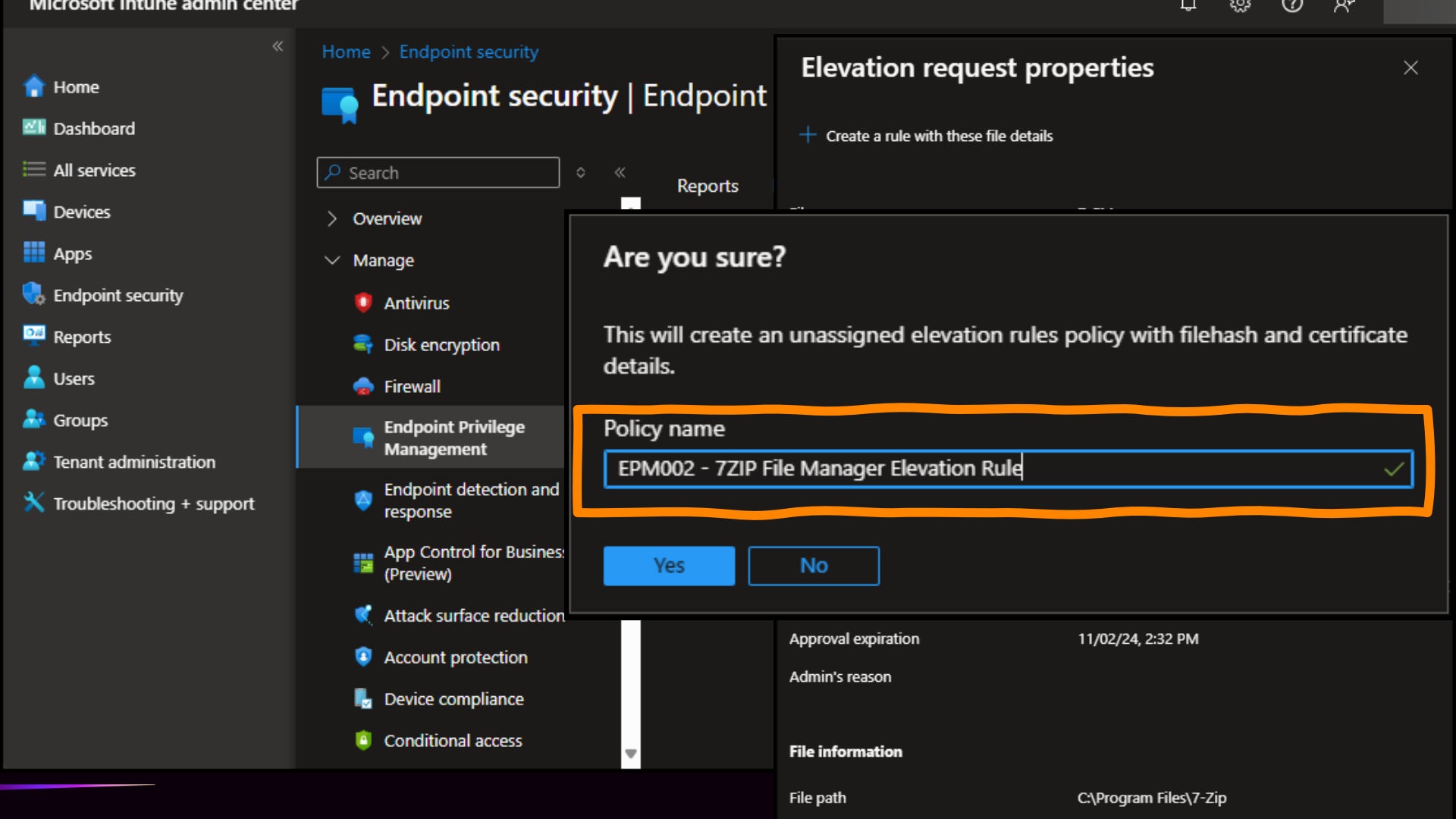
Search by profile name

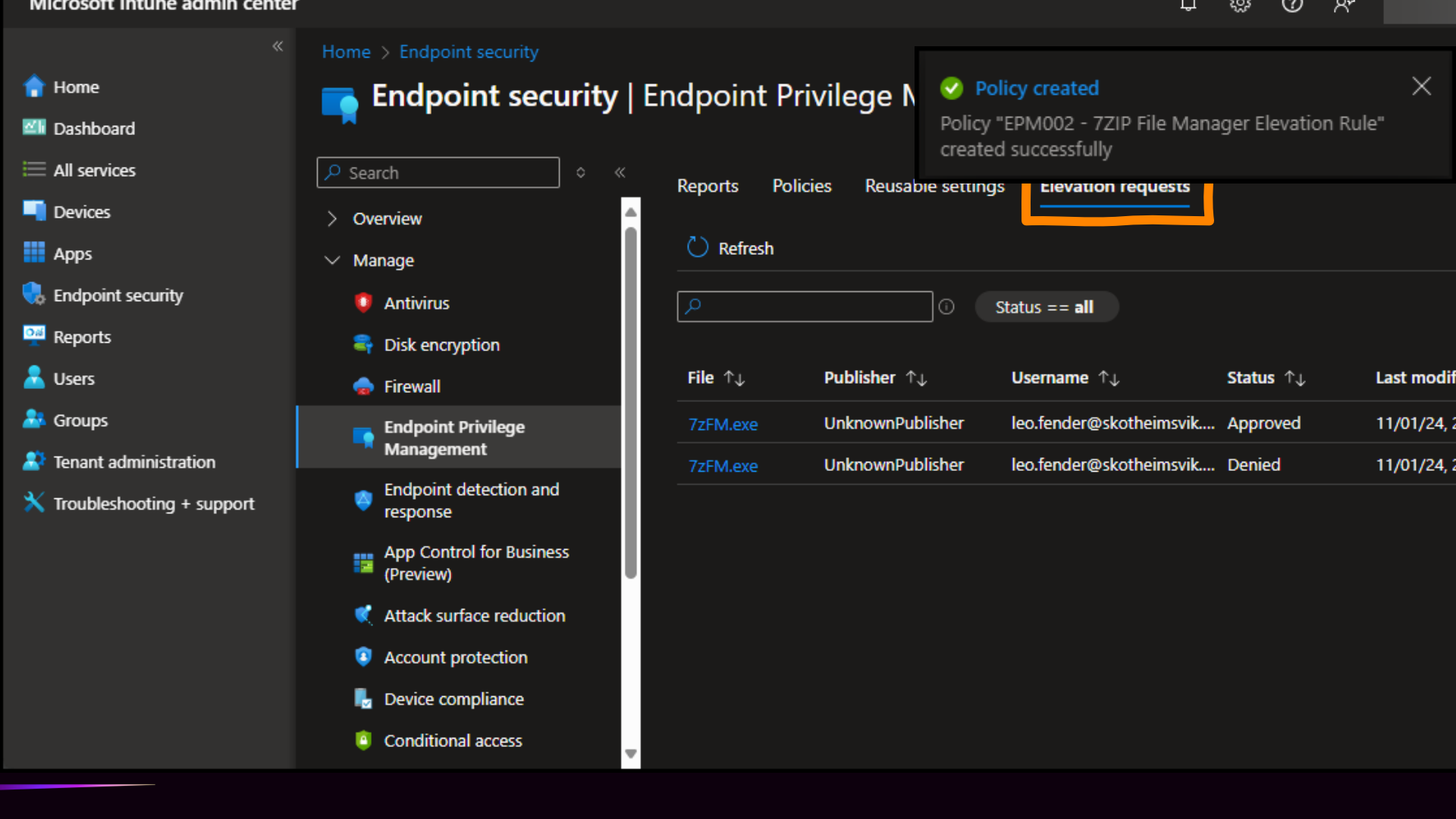
Policy name	Policy type	Assigned	Platfor
EPM001 - Elevation Settings Policy	Elevation settings policy	Yes	Windov
EPM002 - 7Zip File Manager Elevation Rule	Elevation rules policy	Yes	Windov

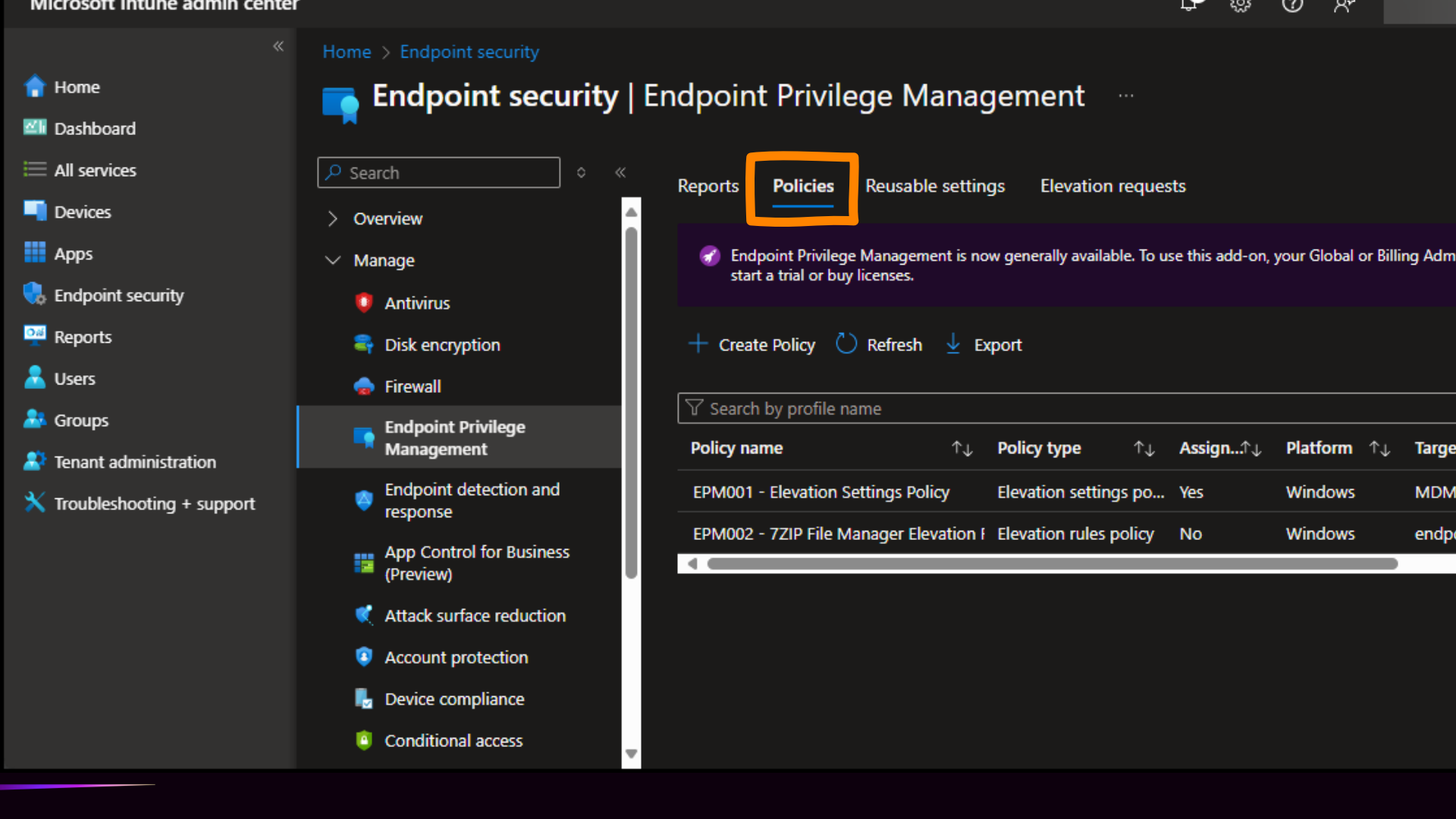

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Reports
Policies
Reusable settings
Elevation requests
Refresh
Status == all
File
Publisher
Username
Status
Last modif
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Approved
11/01/24,
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Denied
11/01/24,

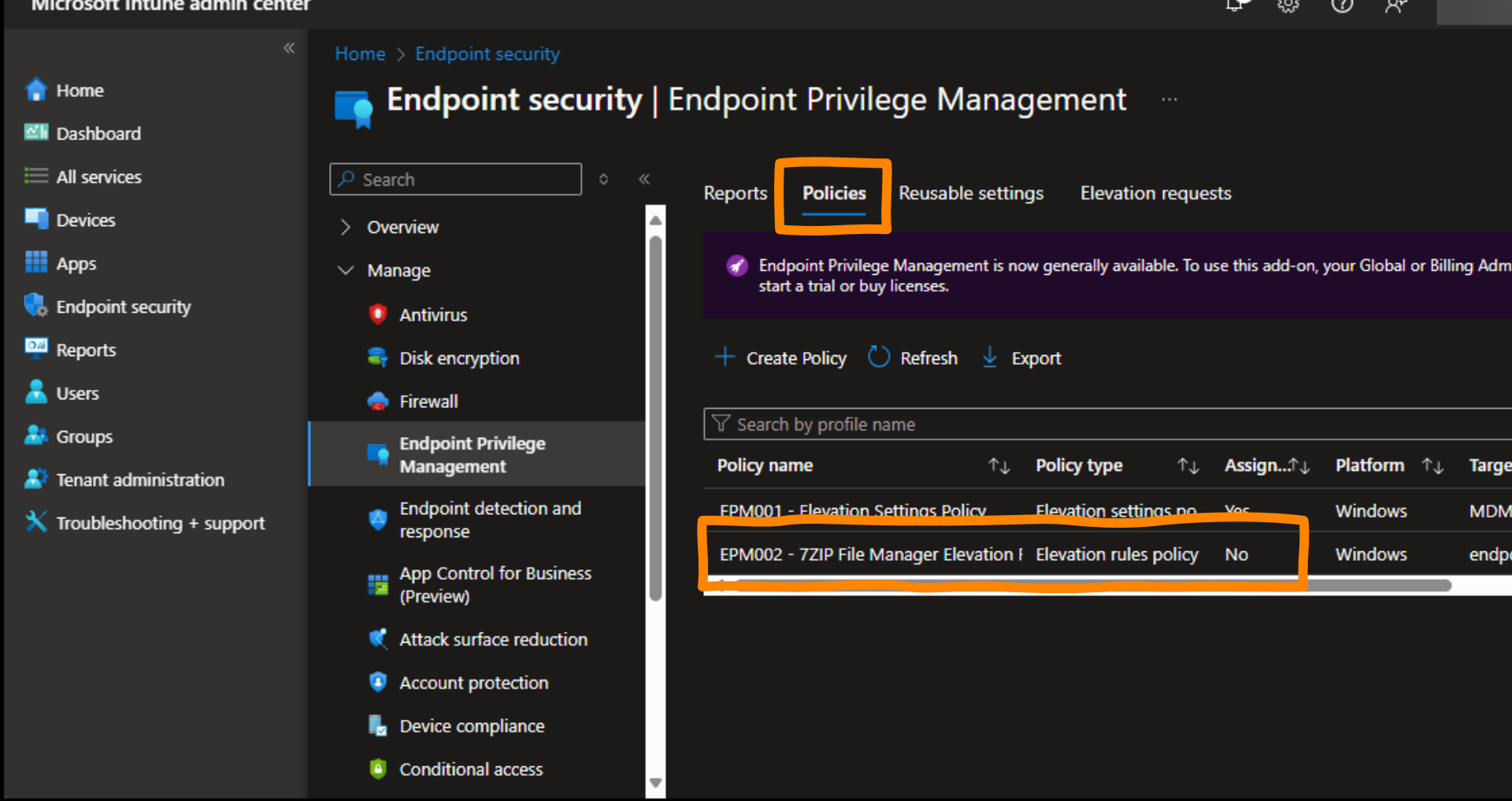

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Reports
Refresh
File
7zFM.exe
7zFM.exe
Elevation request properties
Create a rule with these file details
File 7zFM.exe
Publisher UnknownPublisher
Username leo.fender@skotheimsvik.no
Device RM23-8524755908
Intune compliant true
Request details
Status Pending
By
Last modified 11/01/24, 2:32 PM
User's justification I need access to some files.
Approval expiration 11/02/24, 2:32 PM
Admin's reason
File information
File path C:\Program Files\7-Zip

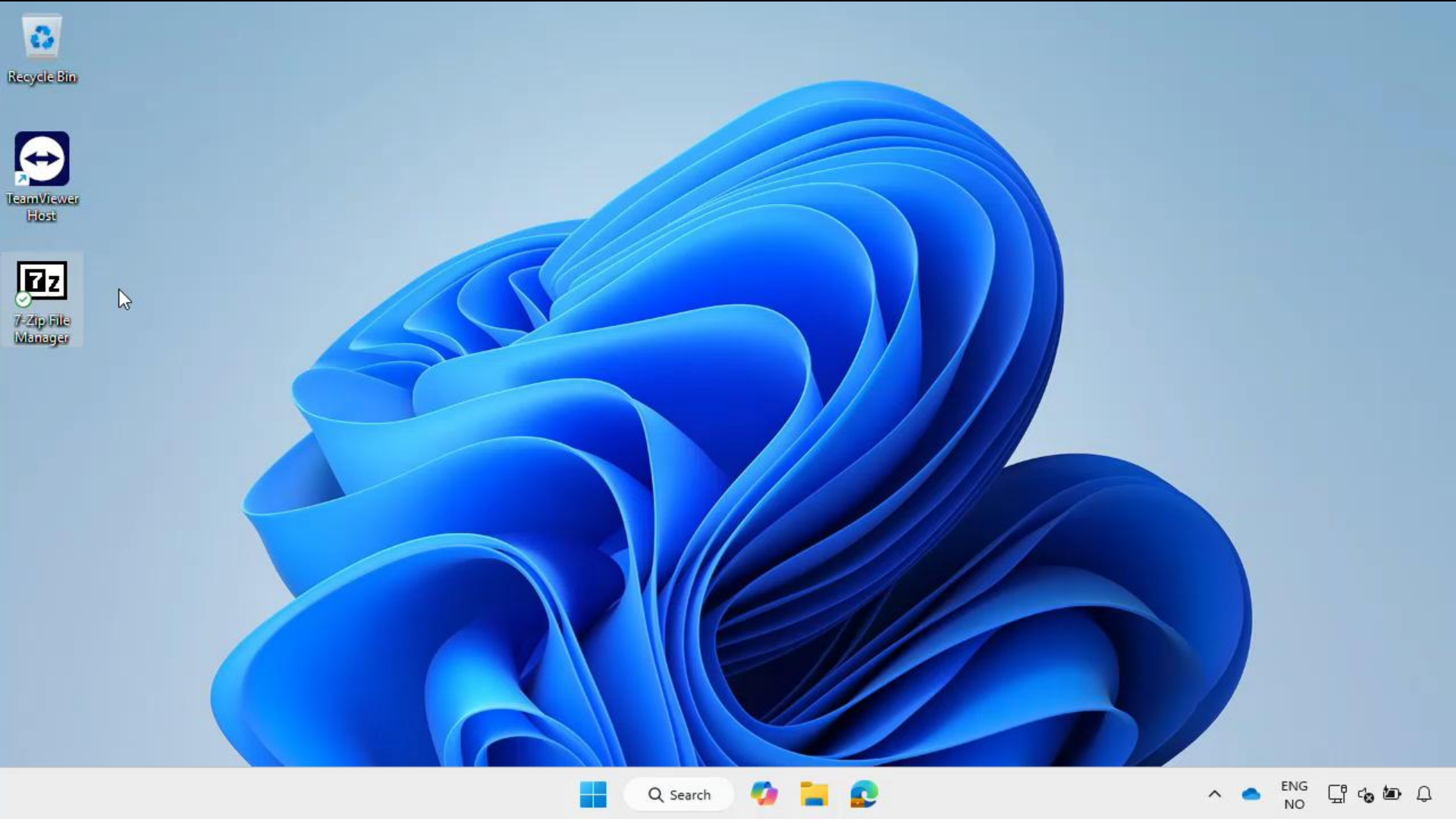

Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Busines (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Elevation request properties
Create a rule with these file details
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
Admin's reason
File information
File path
C:\Program Files\7-Zip


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint
Search
Overview
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Busines (Preview)
Attack surface reduction
Account protection
Device compliance
Conditional access
Reports
Elevation request properties
Create a rule with these file details
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
Approval expiration
11/02/24, 2:32 PM
Admin's reason
File information
File path
C:\Program Files\7-Zip


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege M
Policy created
Policy "EPM002 - 7ZIP File Manager Elevation Rule" created successfully
Search
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
Reports
Policies
Reusable settings
Elevation requests
Refresh
Status == all
File
Publisher
Username
Status
Last modif
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Approved
11/01/24,
7zFM.exe
UnknownPublisher
leo.fender@skotheimsvik....
Denied
11/01/24,


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
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
Reports
Policies
Reusable settings
Elevation requests
Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Adm
start a trial or buy licenses.
Create Policy
Refresh
Export
Search by profile name
Policy name
Policy type
Assign...
Platform
Targe
EPM001 - Elevation Settings Policy
Elevation settings po...
Yes
Windows
MDM
EPM002 - 7ZIP File Manager Elevation F
Elevation rules policy
No
Windows
endp


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
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
Reports
Policies
Reusable settings
Elevation requests
Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Adm
start a trial or buy licenses.
Create Policy
Refresh
Export
Search by profile name
Policy name
Policy type
Assign...
Platform
Targe
EPM001 - Elevation Settings Policy
Elevation settings po
Yes
Windows
MDM
EPM002 - 7ZIP File Manager Elevation F
Elevation rules policy
No
Windows
endp


Recycle Bin
TeamViewer Host
7-Zip File Manager
Search
ENG
NO

Endpoint security | Endpoint Privilege Management

Search

Overview

Overview
All devices
Security baselines
Security tasks

Manage

Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)

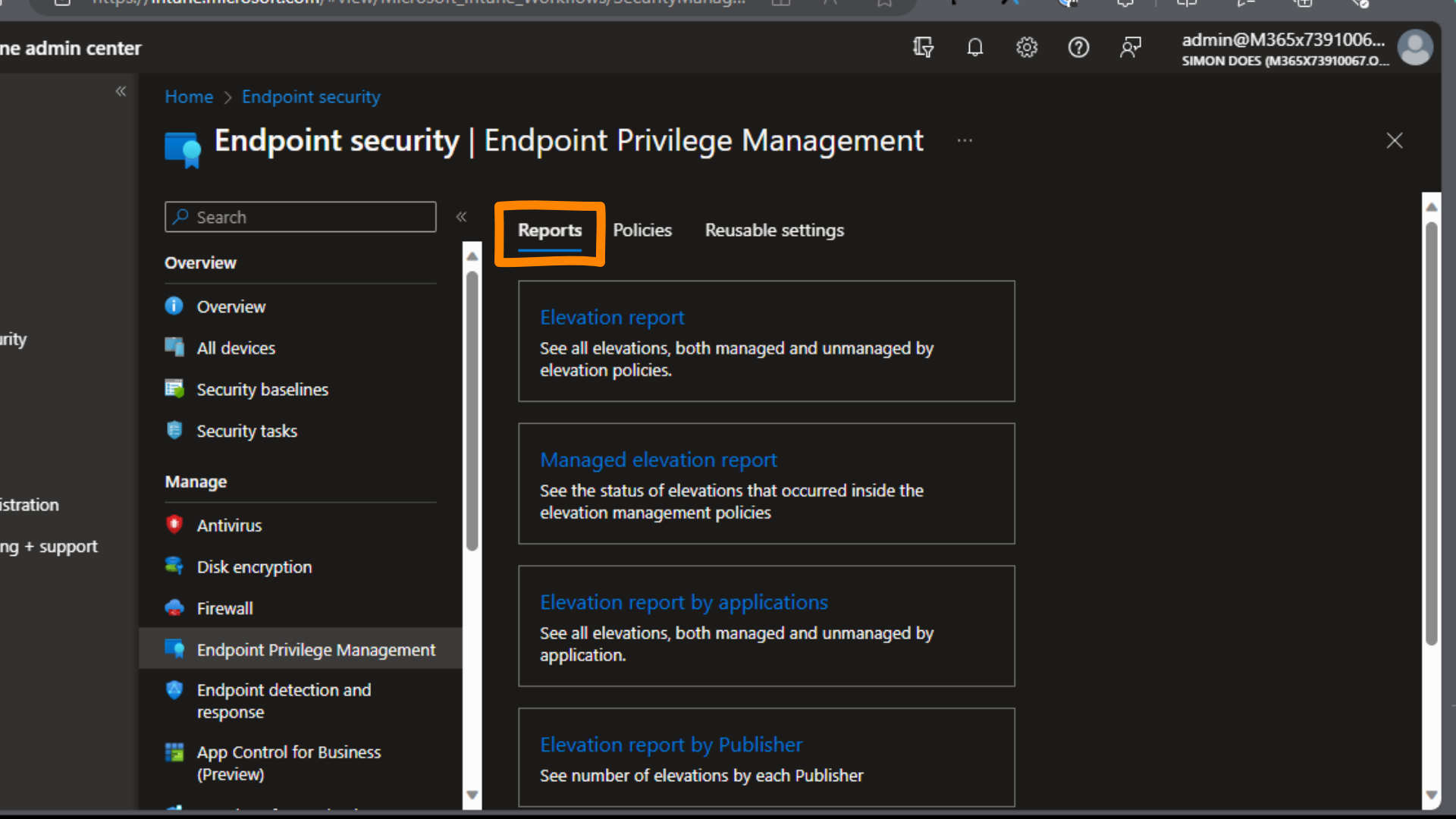
Reports | Policies | Reusable settings

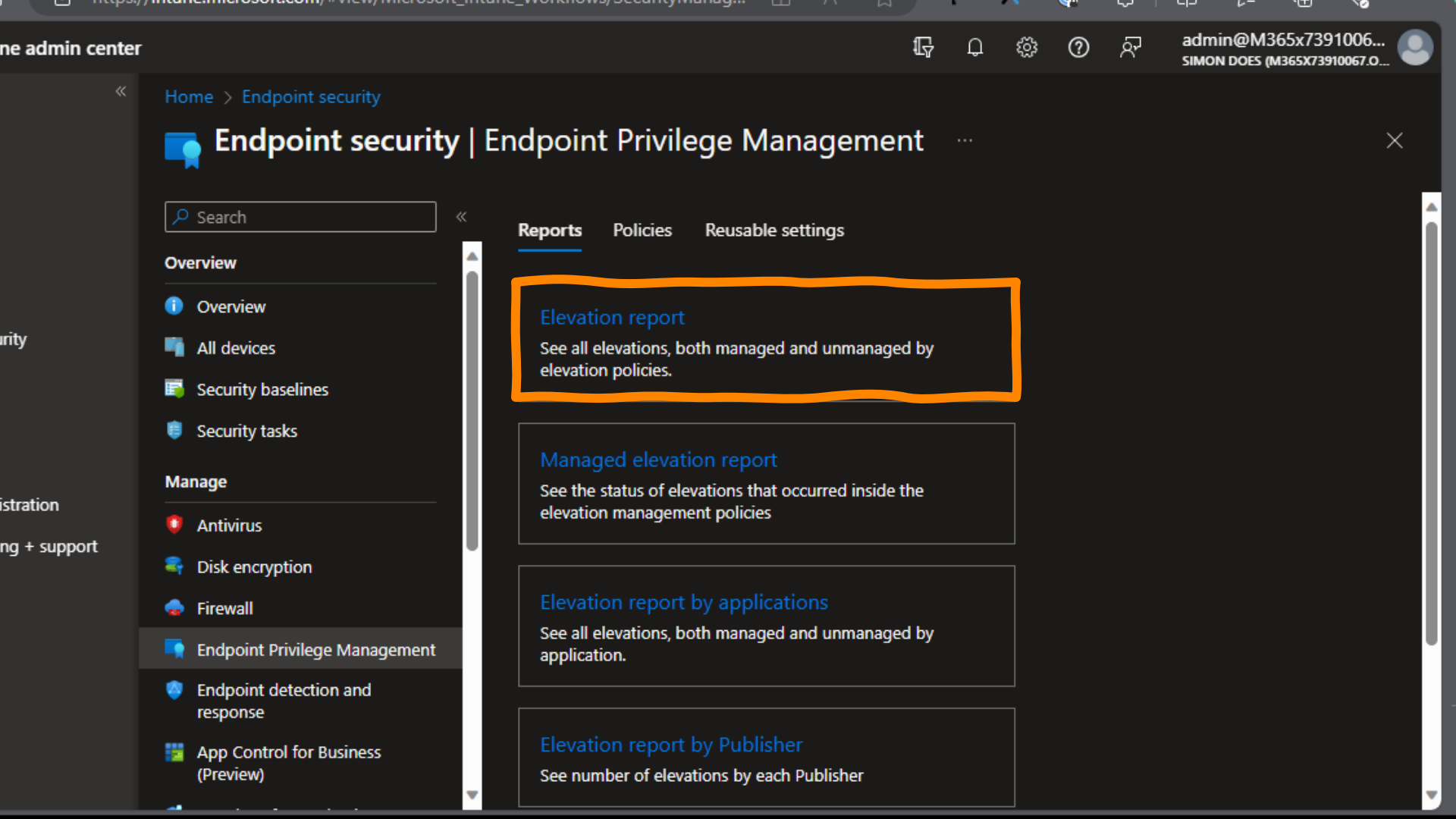
90 days left in trial - to keep using Endpoint Privilege Management after the trial ends, you will need to buy licenses.

+ Create Policy | Refresh | Export

Search by profile name

Policy name	Policy type	Assigned	Platfor
EPM001 - Elevation Settings Policy	Elevation settings policy	Yes	Windov
EPM002 - 7Zip File Manager Elevation Rule	Elevation rules policy	Yes	Windov


ne admin center
admin@M365x7391006...
SIMON DOES (M365X73910067.O...
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
Overview
Overview
All devices
Security baselines
Security tasks
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
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


ne admin center
admin@M365x7391006...
SIMON DOES (M365X73910067.O...
Home > Endpoint security
Endpoint security | Endpoint Privilege Management
Search
Overview
Overview
All devices
Security baselines
Security tasks
Manage
Antivirus
Disk encryption
Firewall
Endpoint Privilege Management
Endpoint detection and response
App Control for Business (Preview)
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

ne admin center

admin@M365x7391006...
SIMON DOES (M365X73910067.O...

Home > Endpoint security | Endpoint Privilege Management >

Endpoint elevation report

This table includes elevations that are managed by specific rules and those that were not defined by rules but are captured by default elevation setting policies

Refresh   Columns   Export

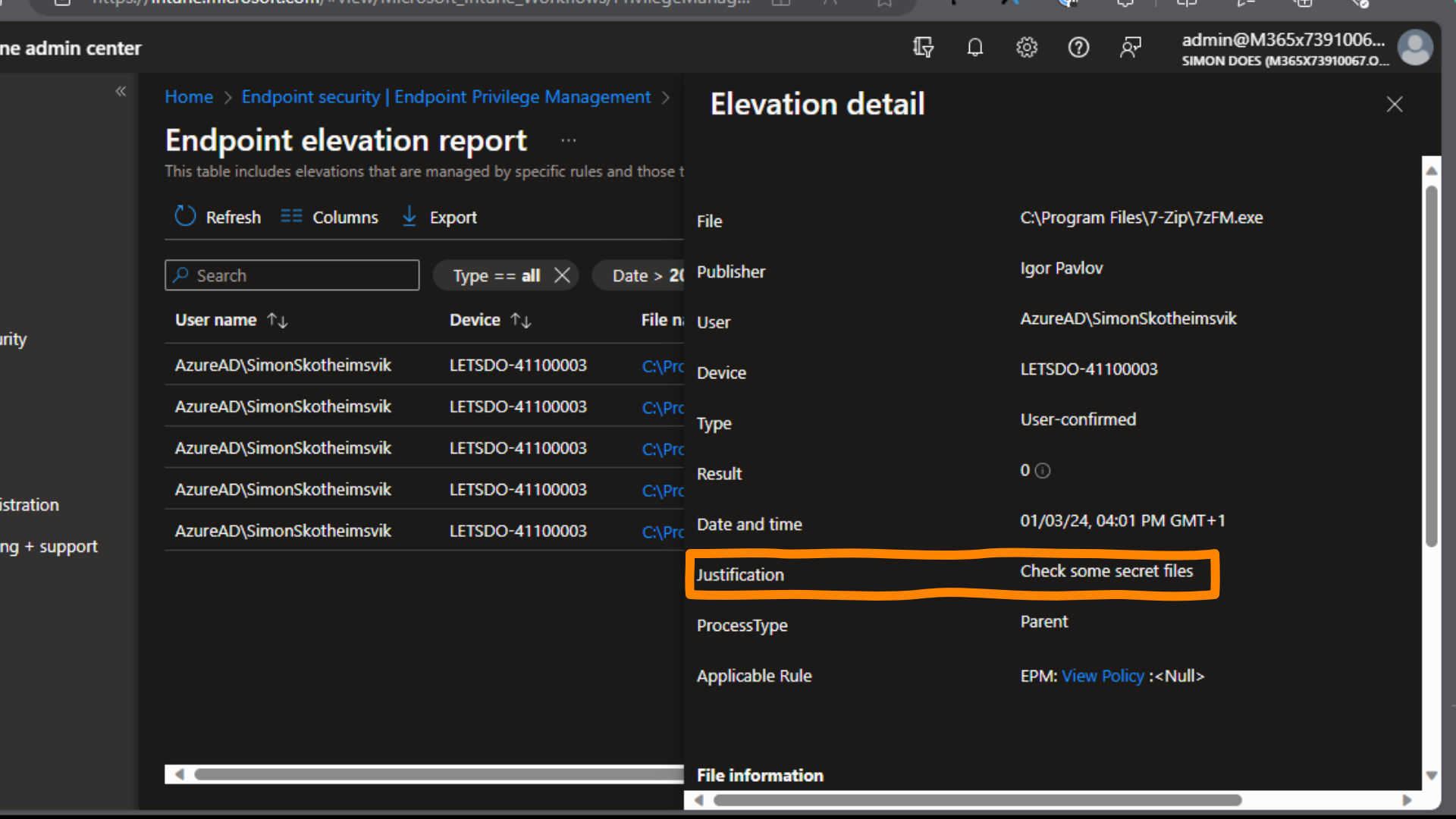
Search   Type == all   Date > 2024-01-02T09:39:25.135Z   Add filter

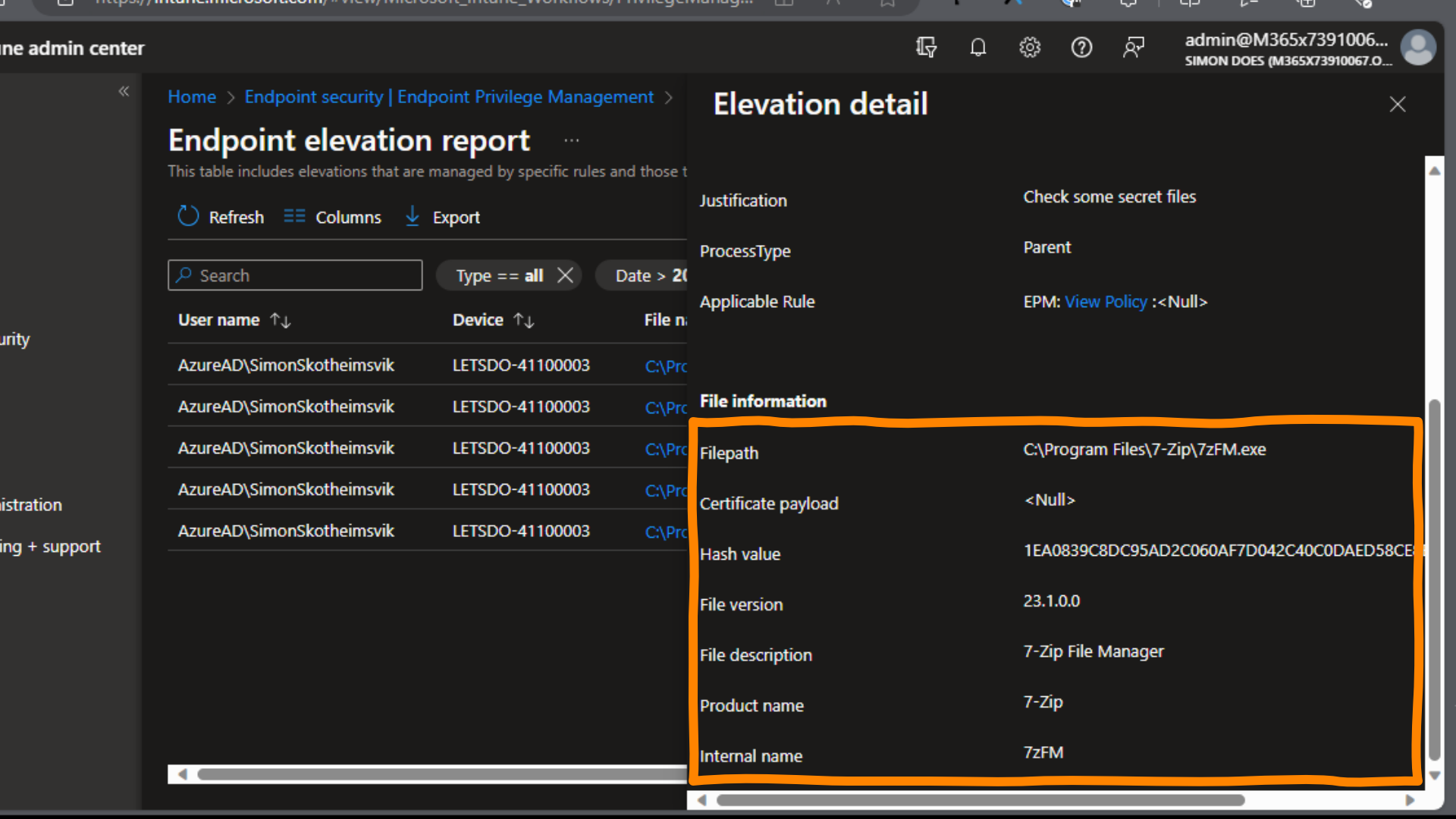
User name	Device	File name	Publisher	Type	Result
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe	Igor Pavlov	User-confirmed	Completed
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe	Igor Pavlov	User-confirmed	Completed
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe	Igor Pavlov	User-confirmed	Completed
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe	Igor Pavlov	User-confirmed	Completed
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe	Igor Pavlov	User-confirmed	Completed

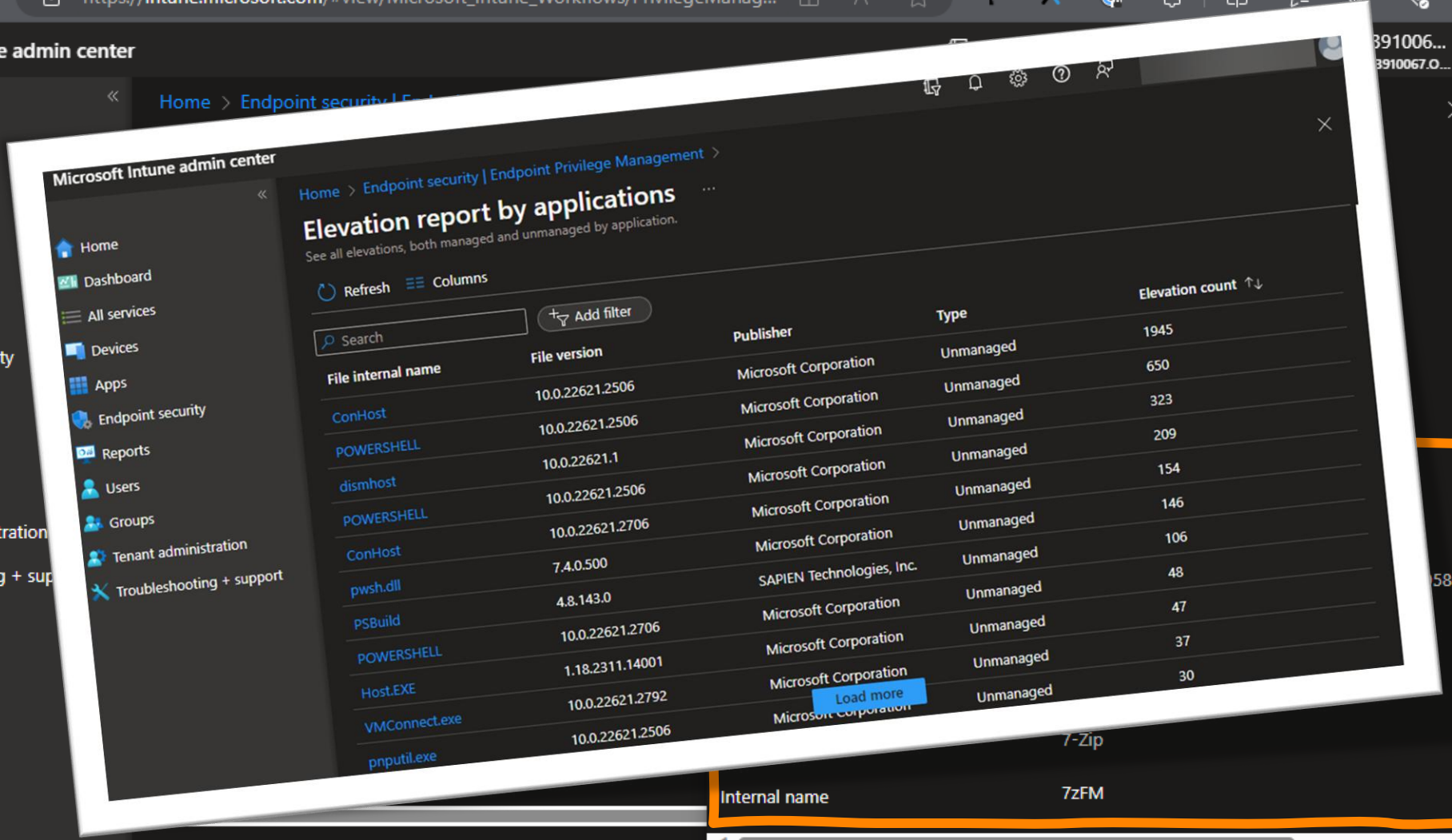
urity

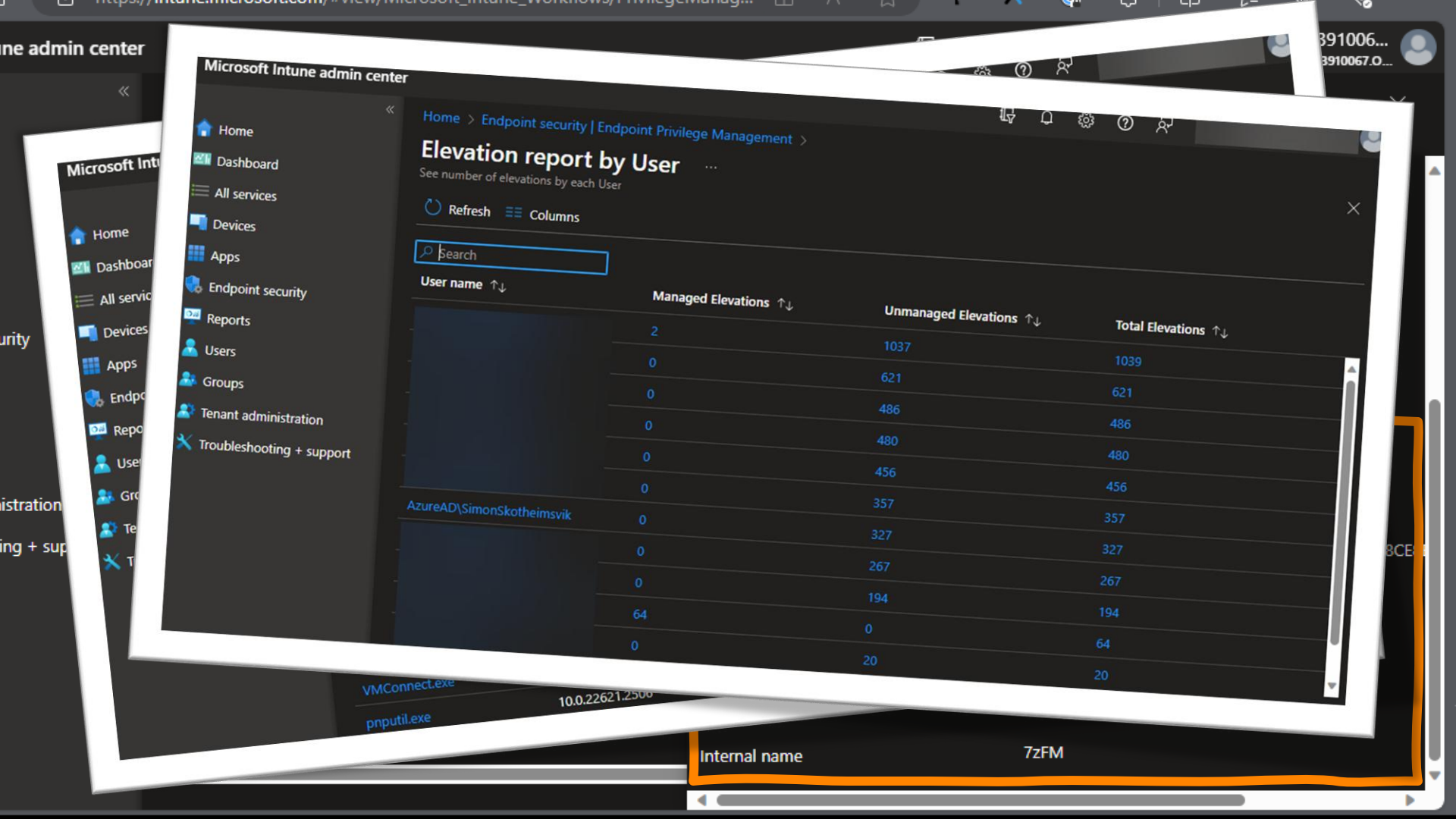
istration

ng + support


ne admin center
admin@M365x7391006...
SIMON DOES (M365X73910067.O...
Home > Endpoint security | Endpoint Privilege Management >
Endpoint elevation report
This table includes elevations that are managed by specific rules and those t
Refresh
Columns
Export
Search
Type == all
Date > 2(
User name
Device
File n
AzureAD\SimonSkotheimsvik LETSDO-41100003 C:\Pro
AzureAD\SimonSkotheimsvik LETSDO-41100003 C:\Pro
AzureAD\SimonSkotheimsvik LETSDO-41100003 C:\Pro
AzureAD\SimonSkotheimsvik LETSDO-41100003 C:\Pro
AzureAD\SimonSkotheimsvik LETSDO-41100003 C:\Pro
Elevation detail
File C:\Program Files\7-Zip\7zFM.exe
Publisher Igor Pavlov
User AzureAD\SimonSkotheimsvik
Device LETSDO-41100003
Type User-confirmed
Result 0
Date and time 01/03/24, 04:01 PM GMT+1
Justification Check some secret files
ProcessType Parent
Applicable Rule EPM: View Policy :<Null>
File information


ne admin center
admin@M365x7391006...
SIMON DOES (M365X73910067.O...
Home > Endpoint security | Endpoint Privilege Management >
Endpoint elevation report
This table includes elevations that are managed by specific rules and those t
Refresh
Columns
Export
Search
Type == all
Date > 2(
User name
Device
File n
AzureAD\SimonSkotheimsvik
LETSDO-41100003
C:\Pro
AzureAD\SimonSkotheimsvik
LETSDO-41100003
C:\Pro
AzureAD\SimonSkotheimsvik
LETSDO-41100003
C:\Pro
AzureAD\SimonSkotheimsvik
LETSDO-41100003
C:\Pro
AzureAD\SimonSkotheimsvik
LETSDO-41100003
C:\Pro
Elevation detail
Justification
Check some secret files
ProcessType
Parent
Applicable Rule
EPM: View Policy :<Null>
File information
Filepath
C:\Program Files\7-Zip\7zFM.exe
Certificate payload
<Null>
Hash value
1EA0839C8DC95AD2C060AF7D042C40C0DAED58CE
File version
23.1.0.0
File description
7-Zip File Manager
Product name
7-Zip
Internal name
7zFM


Microsoft Intune admin center
Home > Endpoint security | Endpoint Privilege Management
Elevation report by applications
See all elevations, both managed and unmanaged by application.
Refresh
Columns
Add filter
Search
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
File internal name
File version
Publisher
Type
Elevation count
ConHost 10.0.22621.2506 Microsoft Corporation Unmanaged 1945
POWERSHELL 10.0.22621.2506 Microsoft Corporation Unmanaged 650
dismhost 10.0.22621.1 Microsoft Corporation Unmanaged 323
POWERSHELL 10.0.22621.2506 Microsoft Corporation Unmanaged 209
ConHost 10.0.22621.2706 Microsoft Corporation Unmanaged 154
pwsh.dll 7.4.0.500 SAPIEN Technologies, Inc. Unmanaged 146
PSBuild 4.8.143.0 Microsoft Corporation Unmanaged 106
POWERSHELL 10.0.22621.2706 Microsoft Corporation Unmanaged 48
Host.EXE 1.18.2311.14001 Microsoft Corporation Unmanaged 47
VMConnect.exe 10.0.22621.2792 Microsoft Corporation Unmanaged 37
pnputil.exe 10.0.22621.2506 Load more Unmanaged 30
7-Zip
Internal name 7zFM


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint Privilege Management >
Elevation report by User
See number of elevations by each User
Refresh
Columns
Search
User name
Managed Elevations
Unmanaged Elevations
Total Elevations
AzureAD\SimonSkotheimsvik
2 1037 1039
0 621 621
0 486 486
0 480 480
0 456 456
0 357 357
0 327 327
0 267 267
0 194 194
64 0 64
0 20 20
VMConnect.exe
pnputil.exe
10.0.22621.2506
Internal name
7zFM

7

How?

Can we do stuff?

NIC
EMPOWER

8

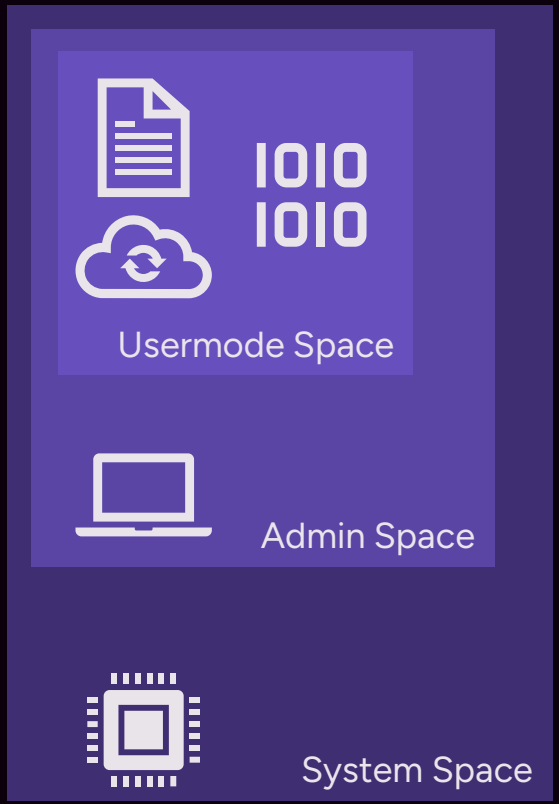
How?

Can we do stuff?

Embrace Modern

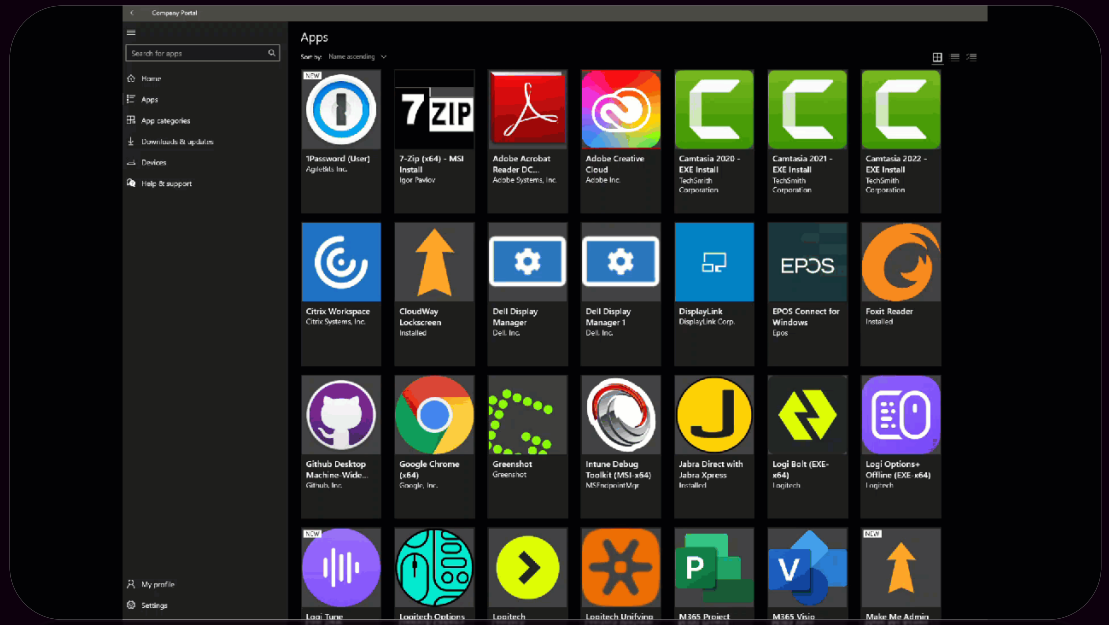
NIC
EMPOWER

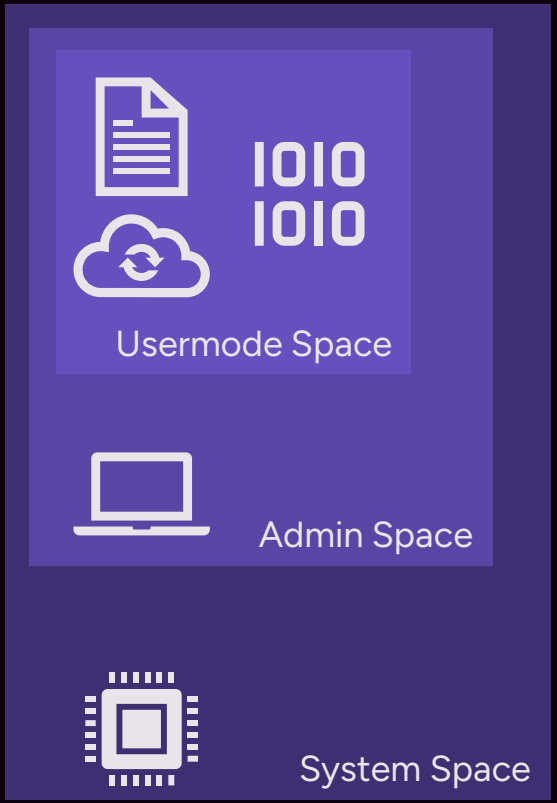
Embrace Modern



NIC
EMPOWER

Embrace Modern





8

How?

Can we do stuff?

NIC
EMPOWER

9

How?

Can we do stuff?

BYODers

NIC
EMPOWER

9 How?

Can we do stuff?

BYODers

NIC
EMPOWER

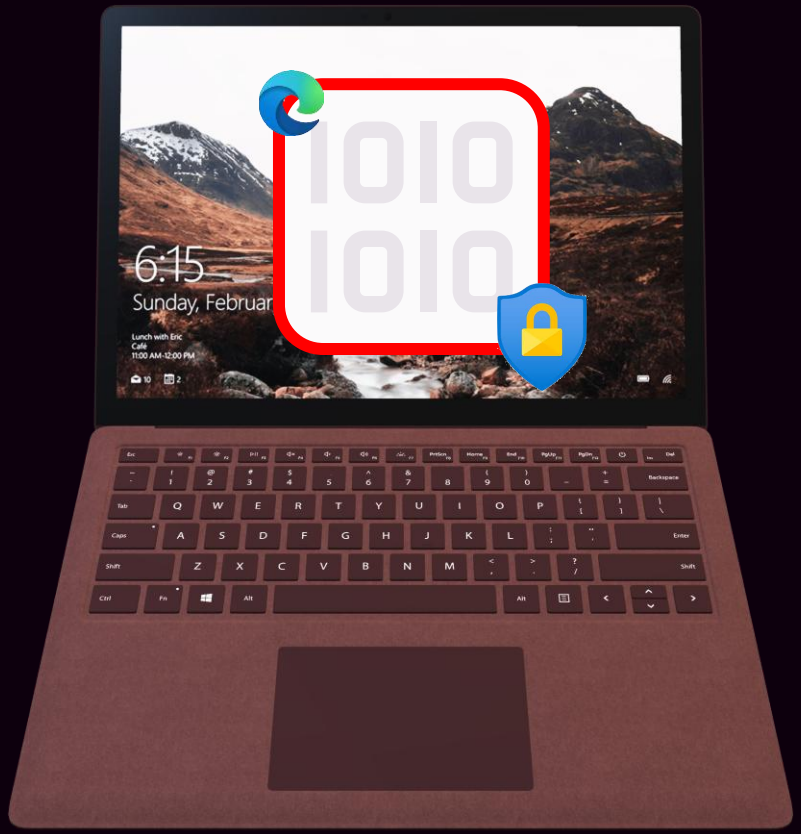
No Access for BYODers?

3 How?

Can we know, and trust our devices?

NIC
EMPOWER

MAM Access for BYODers?



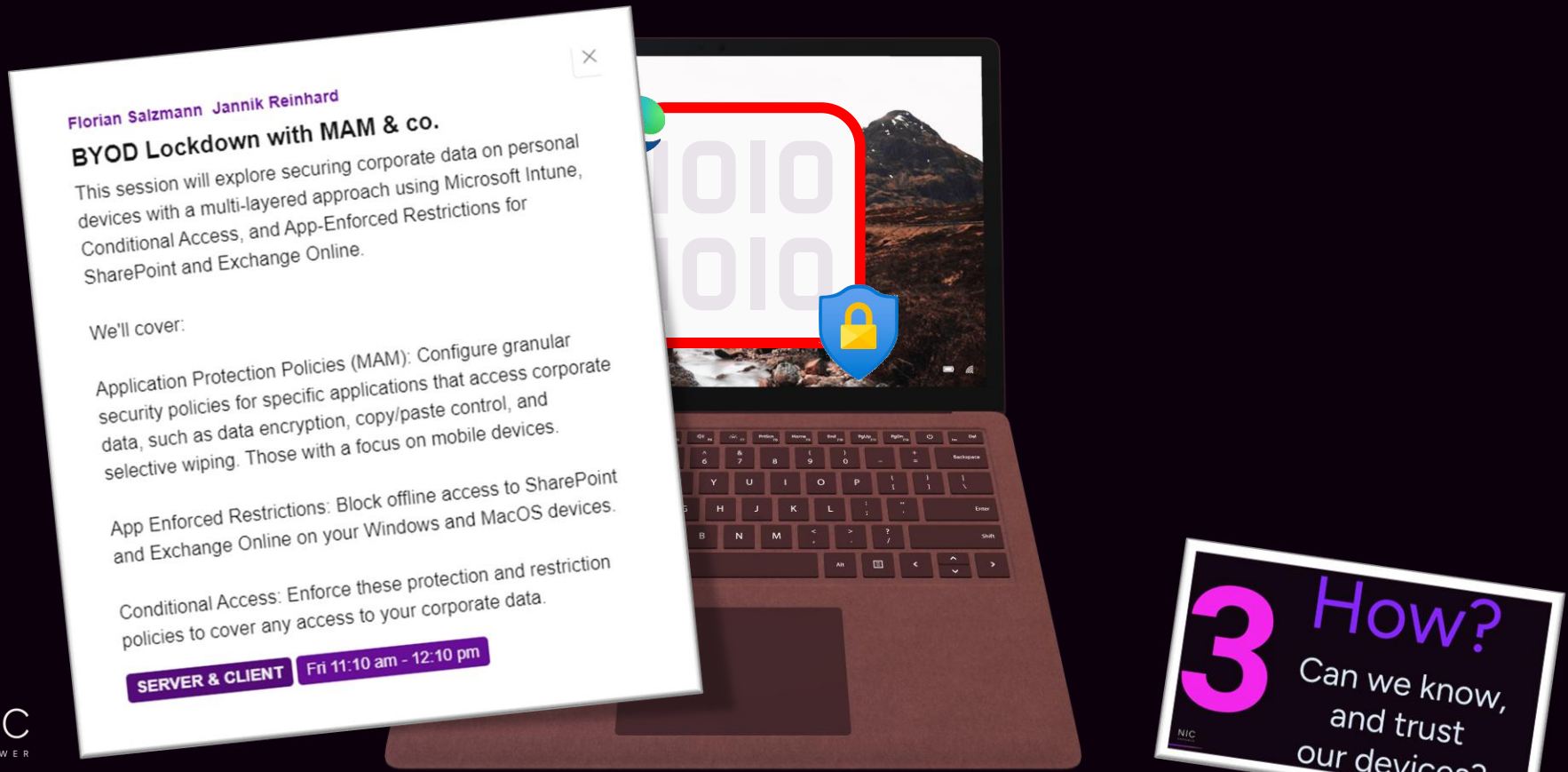
3 How?

Can we know, and trust our devices?

NIC EMPOWER

https://learn.microsoft.com/en-us/mem/intune/apps/protect-mam-windows

MAM Access for BYODers?



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

NIC EMPOWER

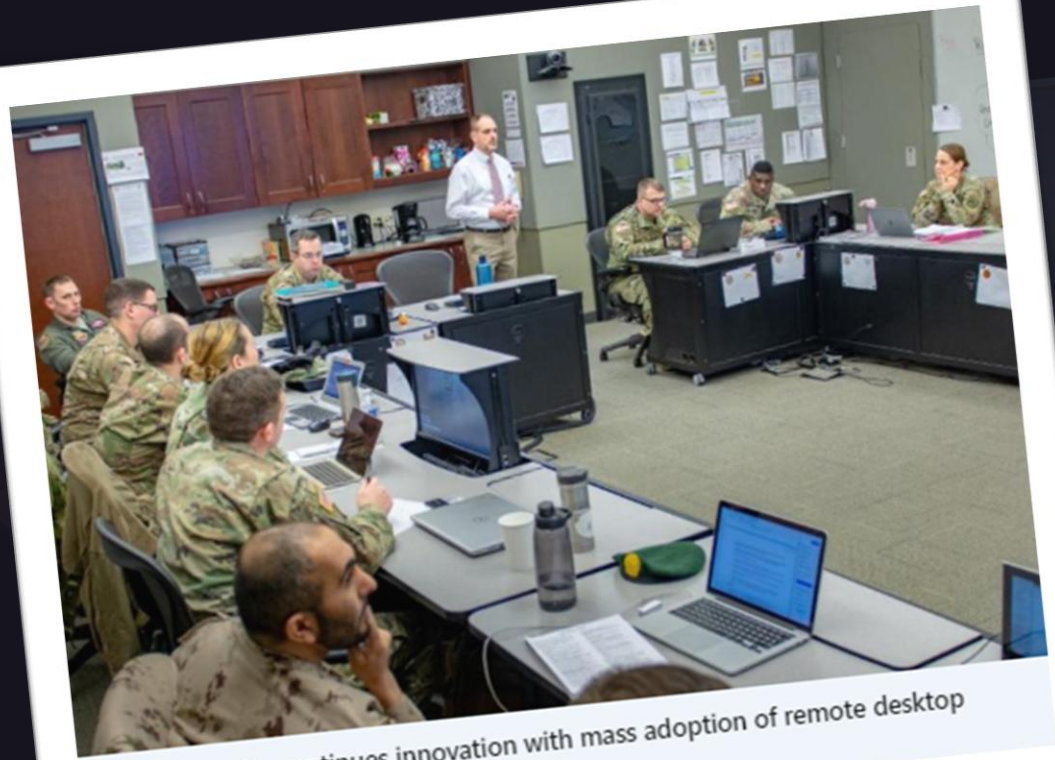
https://learn.microsoft.com/en-us/mem/intune/apps/protect-mam-windows

Cloud PC for BYODers?

https://www.microsoft.com/en-us/windows-365
https://azure.microsoft.com/en-us/products/virtual-desktop

NIC
EMPOWER

Cloud PC for BYODers?



Army University continues innovation with mass adoption of remote desktop

army.mil • 4 min read

Can we know, and trust our devices?

NIC EMPOWER

/en-us/windows-365

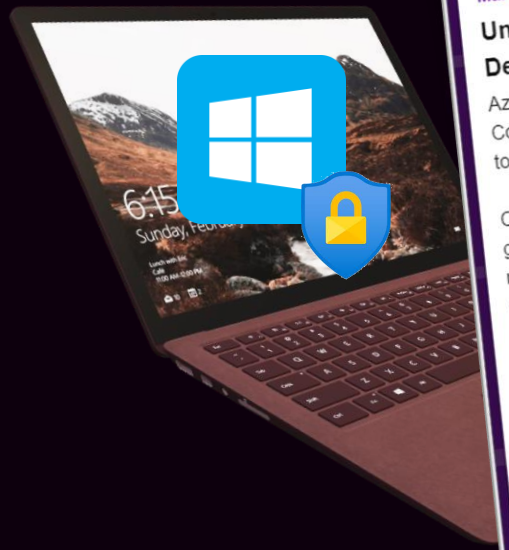
azure.microsoft.com/en-us/products/virtual-desktop

Cloud PC for BYODers?

https://www.microsoft.com/en-us/windows-365
https://azure.microsoft.com/en-us/products/virtual-desktop

NIC
EMPOWER

Cloud PC for BYODers?



Marcel Meurer

Unleash the power of Intune and Azure Virtual Desktop

Azure Virtual Desktop extends the possibilities of End-User-Computing in the Microsoft Azure cloud. There are many ways to manage desktops and handle the application life cycle.

Combined with Intune, we unleash the true power: Creating a golden Master with Intune to deploy win32 and package manager apps. Additionally, Intune policies are used to configure Azure Virtual Desktop session hosts. But using Intune with AVD contains some pitfalls - let us start doing that and avoid some of the classic mistakes.

Using Intune, PowerShell, and some tools allows us to build AVD environments integrated into AD, AAD&AD, or AAD-only. Even AAD-only is becoming more and more popular. An easier integration, fewer dependencies, and, at the same time, new challenges: How to store FSLogix profiles with cloud-only users, accessing on-premises resources, etc.

Finally, session attendees can deploy and configure AVD with Intune and make the right decision about where to deploy AVD and how to work in an AAD-only environment like a charm.

SERVER & CLIENT | Fri 3:20 pm - 4:20 pm

Marcel Meurer

Reach out to the sky with Azure Virtual Desktop

AVD has been on the market for a few years and is becoming increasingly important for End-User-Computing. In recent months, it has brought excellent features to level up the user and admin experience. Don't miss this session. Learn how to use hibernation from custom images to save money and raise the UX, enable SSO (where it is possible), roll out AVD cloud-native, and much more. Attendees will get a lot of live demos, scripts, and tools to master the daily work.

CLOUD | Fri 12:40 pm - 1:40 pm

3 Can we know, and trust our devices?

https://www.microsoft.com/en-us/windows-365

https://azure.microsoft.com/en-us/products/virtual-desktop

NIC EMPOWER

CA for BYODers

3 How?

Can we know, and trust our devices?

NIC
EMPOWER

CA for BYODers

Conditions!

NIC
EMPOWER

CA for BYODers

Conditions!

3 How?

Can we know, and trust our devices?

NIC
EMPOWER

CA for BYODers

Conditions!

3 How?

Can we know, and trust our devices?

NIC
EMPOWER

10 DON'T BE

The Hackers Dream Customer

NIC
EMPOWER

10 DON'T BE

The Hackers Dream Customer

Remove LOCAL ADMIN!

NIC
EMPOWER

10 DON'T BE

The Hackers Dream Customer

Remove

LOCAL ADMIN!

NIC
EMPOWER

Simon Says

Remove LOCAL ADMIN!

NIC
EMPOWER

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