



November 13-15, Oslo Spektrum

# Intune-Driven Approaches to Minimize Local Admin Risks

Simon Skotheimsvik

*Senior Cloud Consultant,  
CloudWay*



- [/in/simonskotheimsvik](https://www.linkedin.com/in/simonskotheimsvik)
- [@sskotheimsvik](https://twitter.com/sskotheimsvik)
- [@sskotheimsvik.bsky.social](https://bsky.social/@sskotheimsvik)
- [skotheimsvik.no](http://skotheimsvik.no)
- [linktr.ee/simonskotheimsvik](https://linktr.ee/simonskotheimsvik)

1 Why?

# Secure Modern Enterprise

## Zero Trust

# Secure Modern Enterprise

Identity

Devices

Applications

Data

Infrastructure

Networks

## Zero Trust

# Secure Modern Enterprise

## Identity

Devices

Applications

Data

Infrastructure

Networks

Zero Trust

# Secure Modern Enterprise

## Identity

Devices

Applications

Infrastructure

Networks

Data

Zero Trust

# Secure Modern Enterprise

## Identity

Devices

Applications

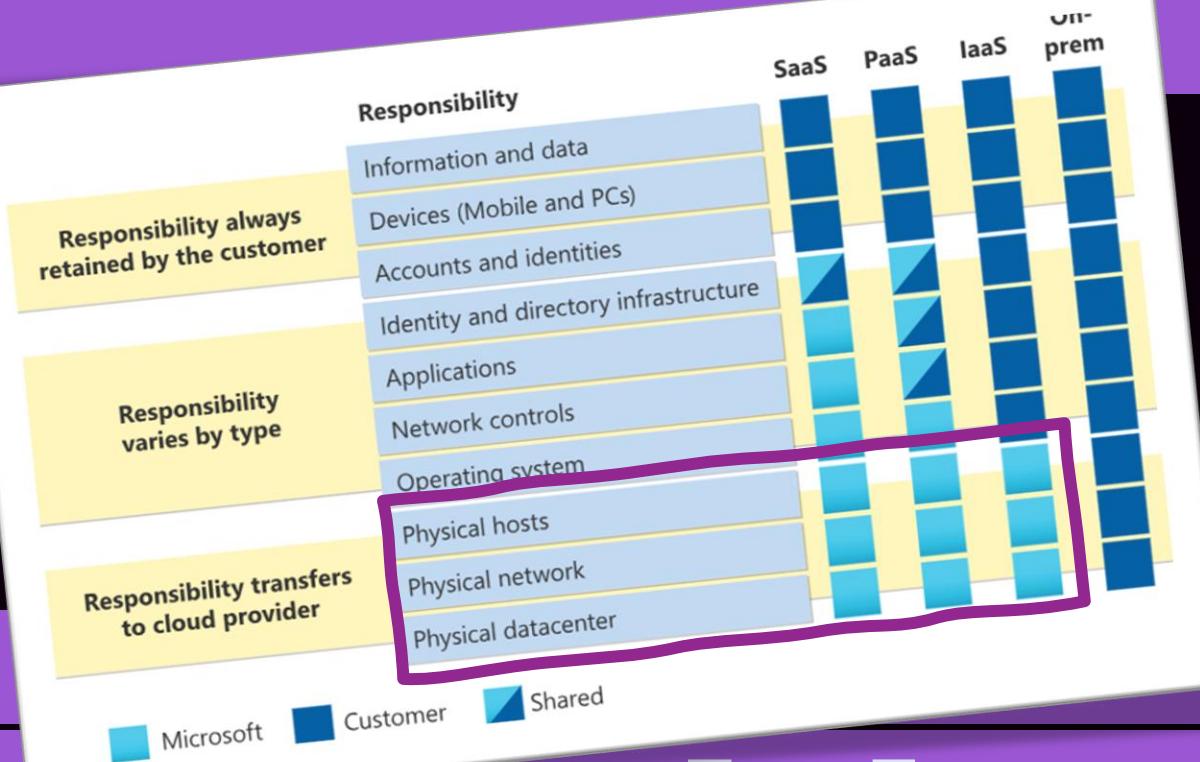
Infrastructure

Networks

Data

Zero Trust

# Secure Modern Enterprise



Infrastructure

Networks

# Zero Trust

# Secure Modern Enterprise

## Identity

Devices

Applications

Networks

Data

Zero Trust

Secure Mod

Ide

Devices

Applications

Data

Zero T



Networks

# Secure Modern Enterprise

## Identity

Devices

Applications

Data

Zero Trust

1 Why?

2

# Why?

We must know,  
and trust  
our devices!

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

# Secure Modern Enterprise

## Identity

Devices

Applications

A computer is only as secure  
as the administrator  
is trustworthy

Data

Zero Trust

# 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

2

# Why?

We must know,  
and trust  
our devices!

# 3

# How?

Can we know,  
and trust  
our devices?

# Microsoft Intune admin center



Home



Dashboard



All services



Devices



Apps



Home > Devices



## Devices | En



Search



Overview



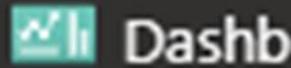
All devices



Home > Devices



Home



Dashboard



All services



Devices



Apps



Endpoint security



# 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

[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 identification](#)

Learn about the different ways a Windows 10/11 PC can be enrolled.

 Search

## Enrollment options

[Automatic Enrollment](#)

Configure Windows 10/11 PCs to automatically enroll in your organization using Azure Active Directory.

[CNAME Validation](#)

Test company domain names for enrollment.

[Co-management Settings](#)

Configure co-management integration.

[Device platform restriction](#)

Configure which platforms can be used.

[Device limit restriction](#)

Define how many devices can be used.

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

## 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 device to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not deleted.

## Device type restrictions

Define which platforms, versions, and management types can enroll.

Priority	Name
Default	All Users

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

**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 device to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not deleted.

**Device type restrictions**

Define which platforms, versions, and management types can enroll.

Priority	Name
Default	All Users

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

**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 device to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not deleted.

**Device type restrictions**

Define which platforms, versions, and management types can enroll.

Priority	Name
Default	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	All Platforms

### 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](#)

 All Users | Properties

...

 Search

X

&lt;&lt;

 Overview Manage Properties

## Basics

Name

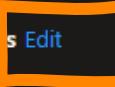
All Users

Description

This is the default Device Type Restriction applied with lowest priority to all users regardless of group membership

Platform

All Platforms

Platform settings 

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

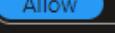
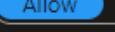
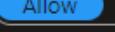
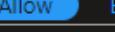
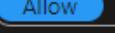
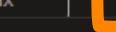
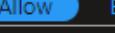
## Edit restriction

...

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 min/max range:  	 	Manufacturer name
Android device administrator	 	Allow min/max range:  	 	Manufacturer name
iOS/iPadOS	 	Allow min/max range:  	 	Restriction not supported
macOS	 	Restriction not supported	 	Restriction not supported
Windows (MDM) 	 	Allow min/max range:  	 	Restriction not supported

**Review + save****Cancel**

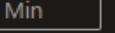
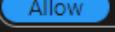
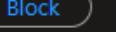
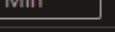
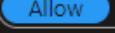
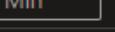
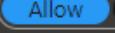
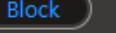
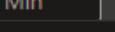
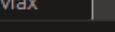
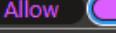
## Edit restriction

...

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 min/max range:  	 	Manufacturer name
Android device administrator	 	Allow min/max range:  	 	Manufacturer name
iOS/iPadOS	 	Allow min/max range:  	 	Restriction not supported
macOS	 	Restriction not supported	 	Restriction not supported
Windows (MDM) 	 	Allow min/max range:  	 	Restriction not supported

**Review + save****Cancel**

## All Users | Properties

 Search

Changes saved.

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	All Platforms

### Platform settings

Type	Platform	Min	Max	Personally owned	Block
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			Block	N/A

# 3

# How?

Can we know,  
and trust  
our devices?

# 4 HOW?

Can we know,  
and trust  
our devices?

## Windows Autopilot

# Microsoft Intune admin center



[Home](#) > [Devices](#)



Home



Dashboard



All services



Devices



Apps



Endpoint security



Feedback



## Devices | Enrollment



[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



Device

Windows Au

Use Windows /

about Window



Device

## 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.

## WADP001 Enrollment Profile RM23 | Properties ...

Search

Overview

Manage

Properties

Assigned devices

Name

Description

Convert all targeted devices to Autopilot

Device type

WADP001 Enrollment Profile RM23

2024.02.22, Enrollment profile for devices with group tag RM23.

No

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

Allow users to change deployment

No

Apply device name template

Yes

Enter a name

RM23-%SERIAL%

Windows Autopilot

Use Windows Autopilot

[Learn more about Windows Autopilot](#)

Device

Windows Autopilot

Use Windows Autopilot  
[Learn more about Windows Autopilot](#)

Device

Deployment

Enrollment Status Page

Show app and profile installation statuses

## 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 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.

Introduction Basics Device group Configuration settings Scope tags Assign

## 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?

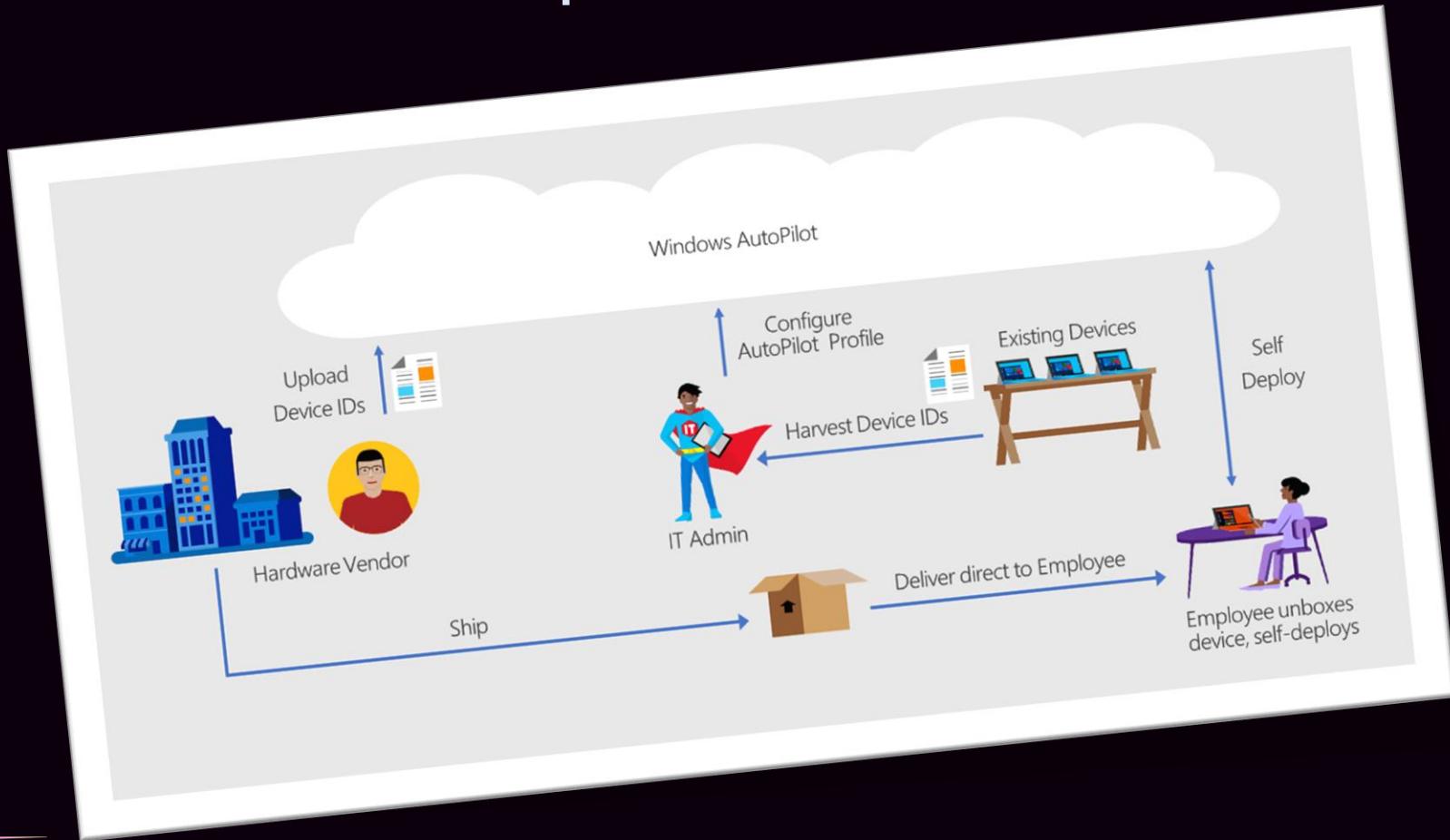
## Windows Autopilot

# 4 HOW?

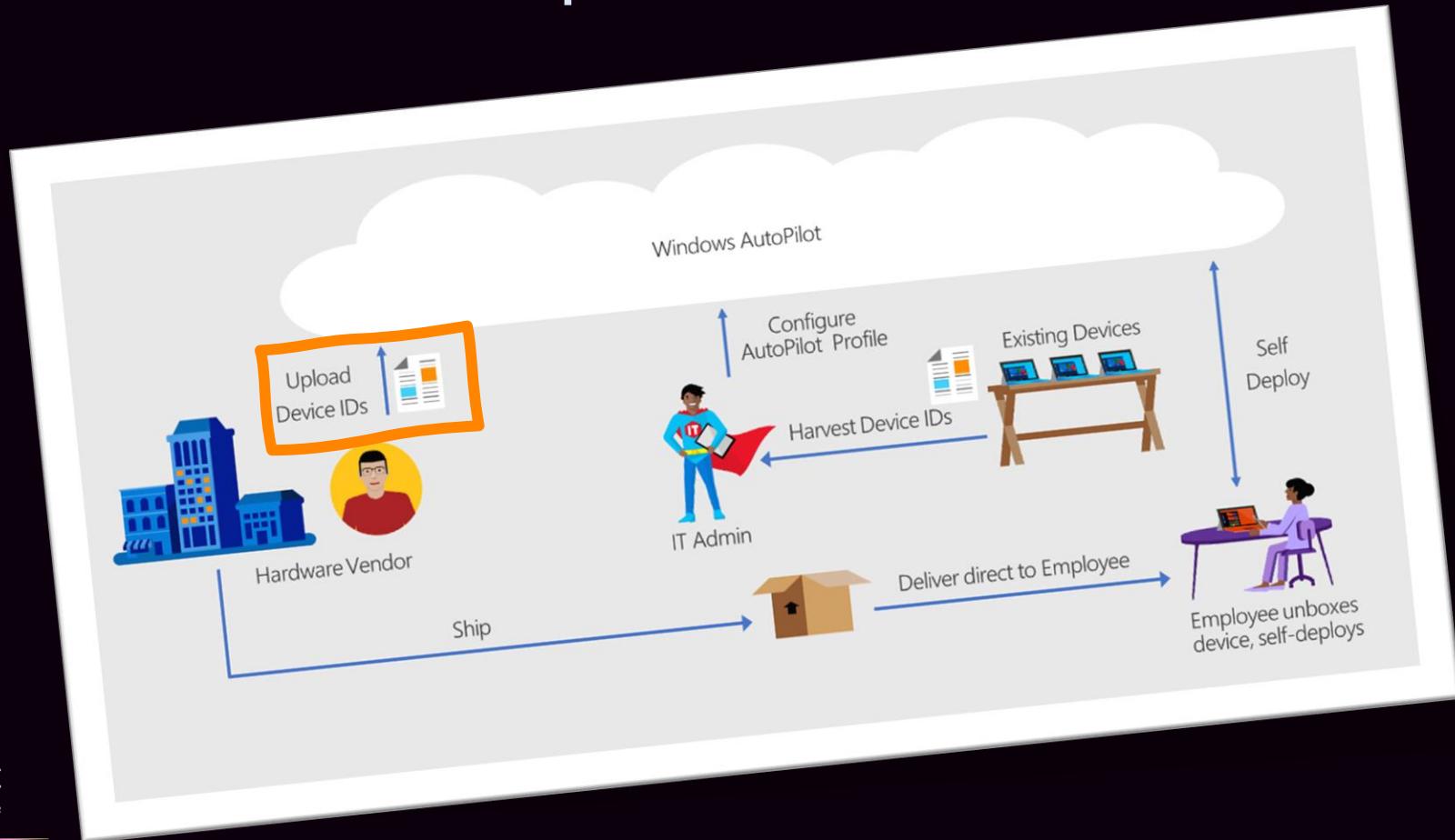
Can we know,  
and trust  
our devices?

Windows Autopilot  
Device Onboarding

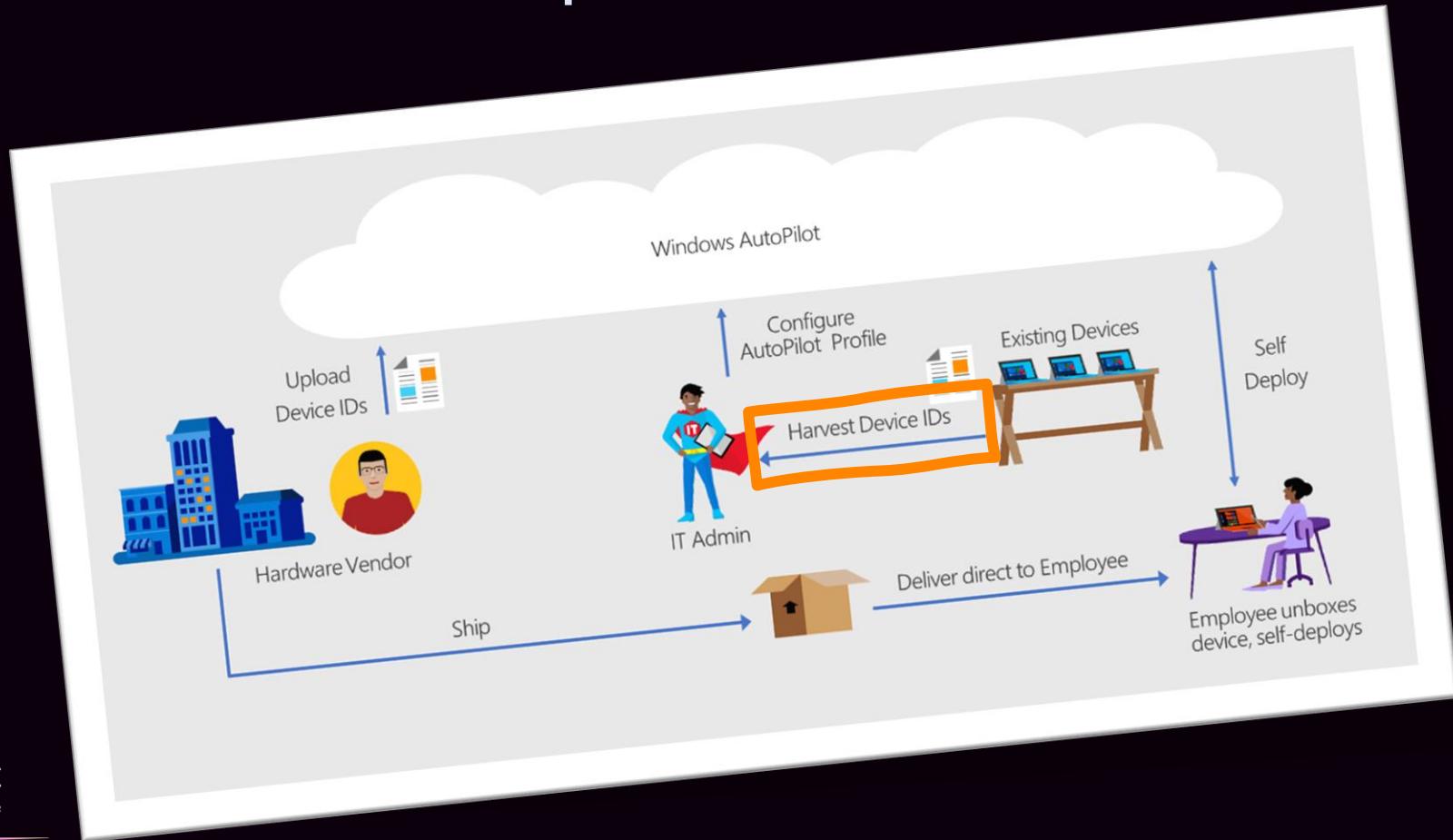
# Windows Autopilot Device Onboarding



# Windows Autopilot Device Onboarding



# Windows Autopilot Device Onboarding



# Windows Autopilot Device Onboarding I

Is this the right country or region?

Administrator: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.22000.318]  
(c) Microsoft Corporation. All rights reserved.  
C:\Windows\system32>



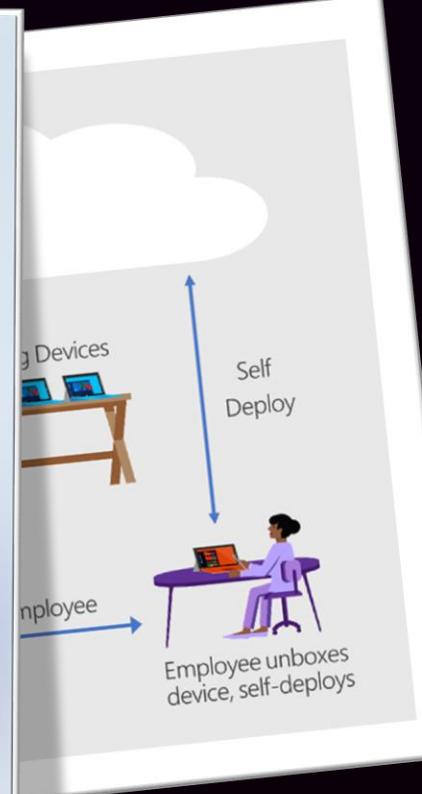
United States

Emirates

Uzbekistan

Uruguay

Yes



# Windows Autopilot Device Onboarding I

The image shows a stack of three cards. The top card is a screenshot of a Windows PowerShell window. It displays the command `Install-Script -Name Get-WindowsAutopilotInfo`. The output includes instructions about PATH Environment Variable Change and NuGet provider requirements. A yellow box highlights the command. The middle card is a diagram illustrating the 'Self Deploy' process. It shows a cloud icon above a desk with a laptop, labeled 'Devices'. An arrow points from the cloud to the laptop. Another arrow points from the laptop to a person sitting at a desk with a laptop, labeled 'Employee'. Below the person is the text 'Employee unboxes device, self-deploys'. The bottom card is a solid blue card.

```
C:\Windows\system32\cmd.exe - powershell
Administrator: C:\Windows\system32\powershell -NoProfile -ExecutionPolicy Unrestricted
C:\Windows\system32> Install-Script -Name Get-WindowsAutopilotInfo
PS C:\Windows\system32>
PATH Environment Variable Change
Your system has not been configured with a default script installation path yet, which means you can only run a script by specifying the full path to the script file. This action places the script into the folder 'C:\Program Files\WindowsPowerShell\Scripts', and adds that folder to your PATH environment variable. Do you want to add the script installation path 'C:\Program Files\WindowsPowerShell\Scripts' to the PATH environment variable? [Y] Yes [N] No [S] Suspend [?] Help (default is "Y") Y
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\defaultuser\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet provider now? [Y] Yes [N] No [S] Suspend [?] Help (default is "Y") Y
Untrusted repository
You are installing the scripts from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the scripts from ' PSGallery'? [Y] Yes to All [N] No [I] No to All [S] Suspend [?] Help (default is "N") Y
PS C:\Windows\system32>
```

Devices

Employee

Self Deploy

Employee unboxes device, self-deploys

# Windows Autopilot Device Onboarding I

Is this the right country or region?

United States

```
Administrator: C:\Windows\system32\cmd.exe - PowerShell - No-Profile, ExecutionPolicy Unrestricted
PS C:\Windows\System32> Get-WindowsAutoPilotInfo.ps1 -GroupTag "LETSOO" -Online -Assign -Reboot
Installing module WindowsAutopilot...
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

Connected to Intune tenant bdese7b3-1e37-4c3a-8e27-97512987d4be
Gathered details for device with serial number: 2238-3803-6168-0310-5641-1000-03
Waiting for 1 of 1 to be imported
Waiting for 1 of 1 to be imported
Waiting for 0 of 1 to be imported
2238-3803-6168-0310-5641-1000-03: complete 0 None
1 devices imported successfully. Elapsed time to complete import: 62 seconds
All devices synced. Elapsed time to complete sync: 1 seconds
Waiting for 1 of 1 to be assigned
Waiting for 1 of 1 to be assigned
```

Yes

Self Deploy



Employee unboxes  
device, self-deploys

# Windows Autopilot Device Onboarding I

Microsoft Intune admin center

Home > Devices

## Devices | Enrollment

Search

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](#)

Enrollment Manage Windows Autopilot devices.

Manage devices

Manage updates

Organize devices

Help and support

Devices Manage Windows Autopilot devices.

Deployment profiles Customize the Windows Autopilot provisioning experience.

Enrollment Status Page Show app and profile installation statuses to users during device setup.

Intune Connector for Active Directory Configure hybrid Azure AD joined devices.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar has a 'Devices' menu item highlighted with an orange box. Under the 'Devices' menu, the 'Enrollment' sub-item is also highlighted with an orange box. To the right, there's a main content area for 'Windows Autopilot device preparation' and 'Windows Autopilot'. The 'Devices' section under 'Windows Autopilot' is also highlighted with an orange box. Other items like 'Deployment profiles', 'Enrollment Status Page', and 'Intune Connector for Active Directory' are listed below it.

# Windows Autopilot Device Onboarding I

Microsoft Intune admin center

Home > Devices | Enrollment >

## Windows Autopilot devices

Windows enrollment

Refresh Export Columns Sync Import Assign user Delete Unblock

Search Add filters

Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.

Last successful sync  
10/31/2024, 08:49 AM

Last sync request  
10/31/2024, 08:49 AM

Serial number	Manufacturer	Model	Group tag	Profile status
0136-5936-4734-4633...	Microsoft Corporat	Virtual Machine	RM23	Assigned
3703-2829-3923-6669...	microsoft Corporat	virtual Machine	RM23	Assigned

0136-5936-4734-4... Windows Autopilot devices  
Manufacturer Microsoft Corporation  
Model Virtual Machine  
Device name  
Group tag RM23  
Profile status Assigned  
Assigned profile WADP001 Enrollment Profile RM23  
Date assigned 10/14/24, 4:21 PM  
Enrollment state Not enrolled

Save

# Windows Autopilot Device Onboarding I

## Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Autopilot Profile | Properties

Windows PC

Overview

Manage

Properties

Assigned devices

Name: Autopilot Profile

Description: No Description

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: Show

User account type: Standard

Allow pre-provisioned deployment: No

Apply device name template: Yes

Enter a name: LETSDO-%SERIAL%

5936-4734-4...  
Autopilot devices  
User  
Corporation  
Machine  
Name  
Tag  
status  
Created profile  
001 Enrollment Profile RM23  
Assigned  
2024-04-24, 4:21 PM  
Management state  
Enrolled  
Save

# Windows Autopilot Device Onboarding II

Microsoft Intune admin center

Home > Devices

## Devices | Enrollment

Search

Windows Apple Android Corporate device identifiers

Add Refresh Export Columns Delete

Device enrollment managers Monitor 2 items

Identifier Identifier type Details

<input type="checkbox"/>	769827364987263948	Serial	iPad in Warehoue, Grey 8GB
<input type="checkbox"/>	FYQX60Z1HG07	Serial	Ami's iPhone

Overview All devices Monitor Add filters

By platform Device onboarding Windows 365 Enrollment

- Manage devices
- Manage updates
- Organize devices

Help and support Help and support

Devices Apps Endpoint security Reports Users Groups Tenant administration Troubleshooting + support

The screenshot shows the Microsoft Intune admin center interface. The left sidebar has a 'Devices' section highlighted with an orange box. Under 'Devices', the 'Enrollment' option is also highlighted with an orange box. At the top, there are tabs for Windows, Apple, and Android, with 'Corporate device identifiers' being the active tab, also highlighted with an orange box. The main content area displays a table of device identifiers, showing two entries: one for an iPad and one for an iPhone. The table columns are 'Identifier', 'Identifier type', and 'Details'. The 'Identifier' column contains checkboxes. The 'Details' column provides specific information about each device. The overall theme is dark with blue and orange highlights for navigation.

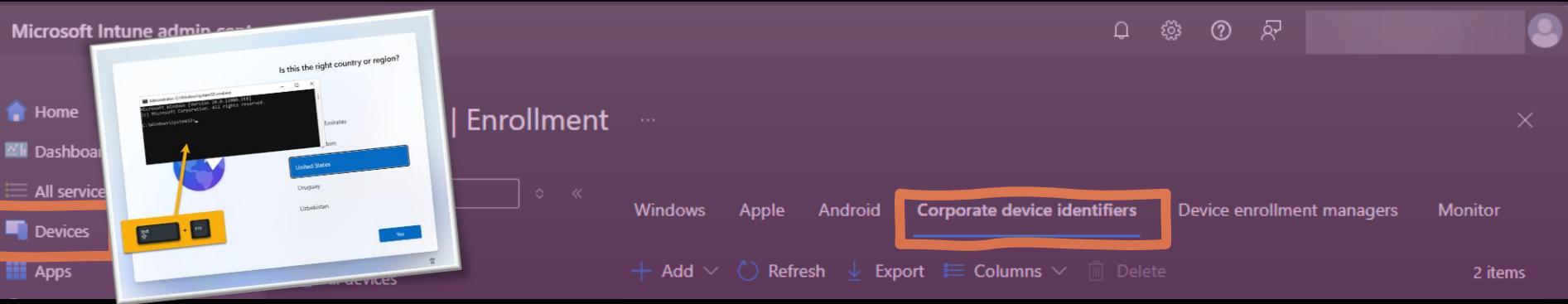
# Windows Autopilot Device Onboarding II

The screenshot shows the Microsoft Intune admin center interface. On the left, there's a navigation bar with Home, Dashboard, All services, Devices (which is selected and highlighted in orange), and Apps. In the center, the main content area has a title 'Enrollment' with tabs for Windows, Apple, and Android. Below the tabs, there's a sub-header 'Corporate device identifiers' which is also highlighted with an orange box. At the bottom of this section are buttons for Add, Refresh, Export, Columns, and Delete, along with a count of '2 items'. To the left of the main content, a modal window titled 'Is this the right country or region?' is open, showing a map of the world with various countries highlighted in blue. An orange arrow points from the 'Corporate device identifiers' tab on the main page down towards this modal window.

This screenshot shows a different part of the Microsoft Intune admin center. On the left, there's a sidebar with Groups, Tenant administration, and Troubleshooting + support. Under 'Device Onboarding', there are several options: Windows 365, Enrollment (which is selected and highlighted with an orange box), Manage devices, Manage updates, Organize devices, Help and support, and Help and support again. The main content area displays a table with two rows of data:

	Identifier	Identifier type	Details
<input type="checkbox"/>	769827364987263948	Serial	iPad in Warehouse, Grey 8GB
<input type="checkbox"/>	FYQX60Z1HG07	Serial	Ami's iPhone

# Windows Autopilot Device Onboarding II



Microsoft Intune admin center

## Enrollment

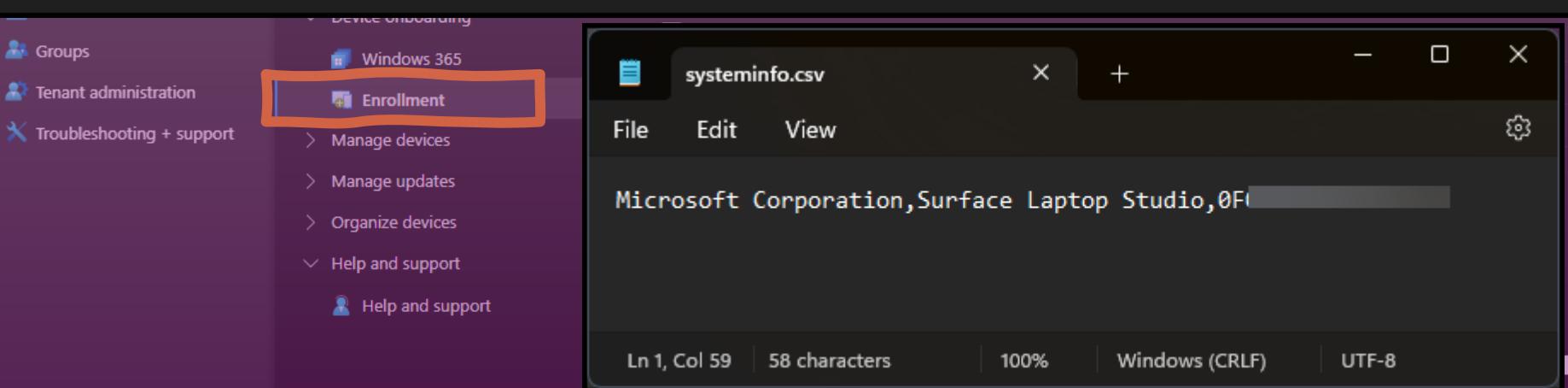
Windows Apple Android Corporate device identifiers

Add Refresh Export Columns Delete

Device enrollment managers Monitor

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, 0F1

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

# Windows Autopilot Device Onboarding II

Microsoft Intune admin center

Home > Devices

## Devices | Enrollment

Search Windows Apple Android Corporate device identifiers

Add Refresh Export Columns Delete

Overview All devices Monitor

By platform Device onboarding

- Windows 365
- Enrollment**

Manage devices Manage updates Organize devices Help and support

Help and support

2 items

<input type="checkbox"/>	Identifier	Identifier type	Details
<input type="checkbox"/>	769827364987263948	Serial	iPad in Warehoue, Grey 8GB
<input type="checkbox"/>	FYQX60Z1HG07	Serial	Ami's iPhone

# Windows Autopilot Device Onboarding II

Microsoft Intune admin center

Home > Devices

## Devices | Enrollment

Search

Windows Apple Android Corporate device identifiers

Add Refresh Export Columns Delete

Upload CSV file

Enter manually

Add filters

2 items

<input type="checkbox"/> Identifier	Identifier type	Details
<input type="checkbox"/> 769827364987263948	Serial	iPad in Warehoue, Grey 8GB
<input type="checkbox"/> FYQX60Z1HG07	Serial	Ami's iPhone

Overview All devices Monitor By platform Device onboarding Windows 365 Enrollment Manage devices Manage updates Organize devices Help and support Help and support

Device enrollment managers Monitor

Endpoint security Reports Users Groups Tenant administration Troubleshooting + support

The screenshot shows the Microsoft Intune admin center interface. The main title is "Windows Autopilot Device Onboarding II". The left sidebar includes links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The "Devices" link is selected and highlighted with a blue bar. Under "Devices", the "Enrollment" link is also highlighted with a blue bar. The top navigation bar has tabs for Windows, Apple, Android, and "Corporate device identifiers", with "Corporate device identifiers" being the active tab and highlighted with an orange box. Below the tabs is a toolbar with "Add", "Refresh", "Export", "Columns", and "Delete" buttons. A dropdown menu is open over the "Add" button, showing options "Upload CSV file" and "Enter manually", with "Upload CSV file" also highlighted with an orange box. The main content area displays a table of device identifiers, with two entries: "769827364987263948" (Serial, iPad in Warehoue, Grey 8GB) and "FYQX60Z1HG07" (Serial, Ami's iPhone). At the bottom of the page, there are links for "Help and support" under "Manage devices", "Manage updates", "Organize devices", and "Help and support".

# Windows Autopilot Device Onboarding II

## Microsoft Intune admin center



Home > Devices | Enrollment >

### Add identifiers

Corporate device identifiers

You can import a list to add device identifiers and details. Imported files can contain only one type of identifier. Identifiers can't be used with some platforms. [Learn more about platform limitations](#).

#### Select identifier type ⓘ

Manufacturer, model and serial number (Windows only)

⚠ Selecting identifier type "Manufacturer, model and serial number (Windows only)" means only devices matching this list will be defined as Corporate-owned. This means all other devices enrolling will be defined as Personal for Windows in your tenant. Click to learn more about this new corporate device identifier experience for Windows.

#### Import identifiers ⓘ

"systeminfo.csv"



Add

# Windows Autopilot Device Onboarding II

## Microsoft Intune admin center



Home > Devices | Enrollment >

### Add identifiers

Corporate device identifiers

Adding identifiers...

You can import a list to add device identifiers and details. Imported files can contain only one type of identifier. Identifiers can't be used with some platforms. [Learn more about platform limitations.](#)

Select identifier type

Manufacturer, model and serial number (Windows only)



Selecting identifier type "Manufacturer, model and serial number (Windows only)" means only devices matching this list will be defined as Corporate-owned. This means all other devices enrolling will be defined as Personal for Windows in your tenant. Click to learn more about this new corporate device identifier experience for Windows.

Import identifiers

"systeminfo.csv"



Add



### Notifications

More events in the activity log → [Dismiss all](#)

... Adding identifiers... Running

Adding 1 device identifiers...

a few seconds ago

# Windows Autopilot Device Onboarding II

Microsoft Intune admin center

Home > Devices

## Devices | Enrollment

Search

Windows Apple Android Corporate device identifiers Device enrollment managers Monitor

Add Refresh Export Columns Delete 3 items

Identifier Identifier type Detail

769827364987263948 Serial iPad ir

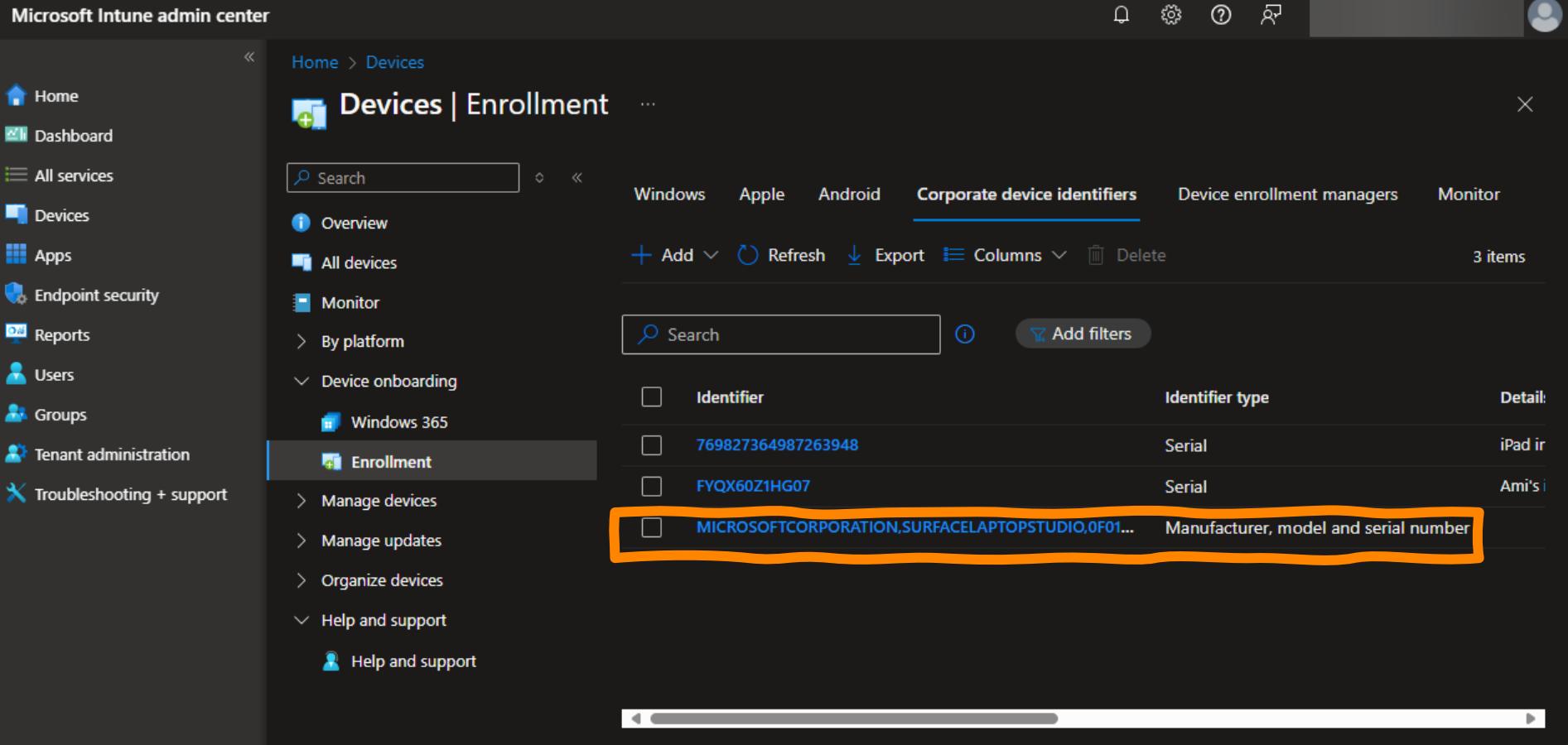
FYQX60Z1HG07 Serial Ami's i

MICROSOFTCORPORATION,SURFACELAPTOPSTUDIO,0F01... Manufacturer, model and serial number

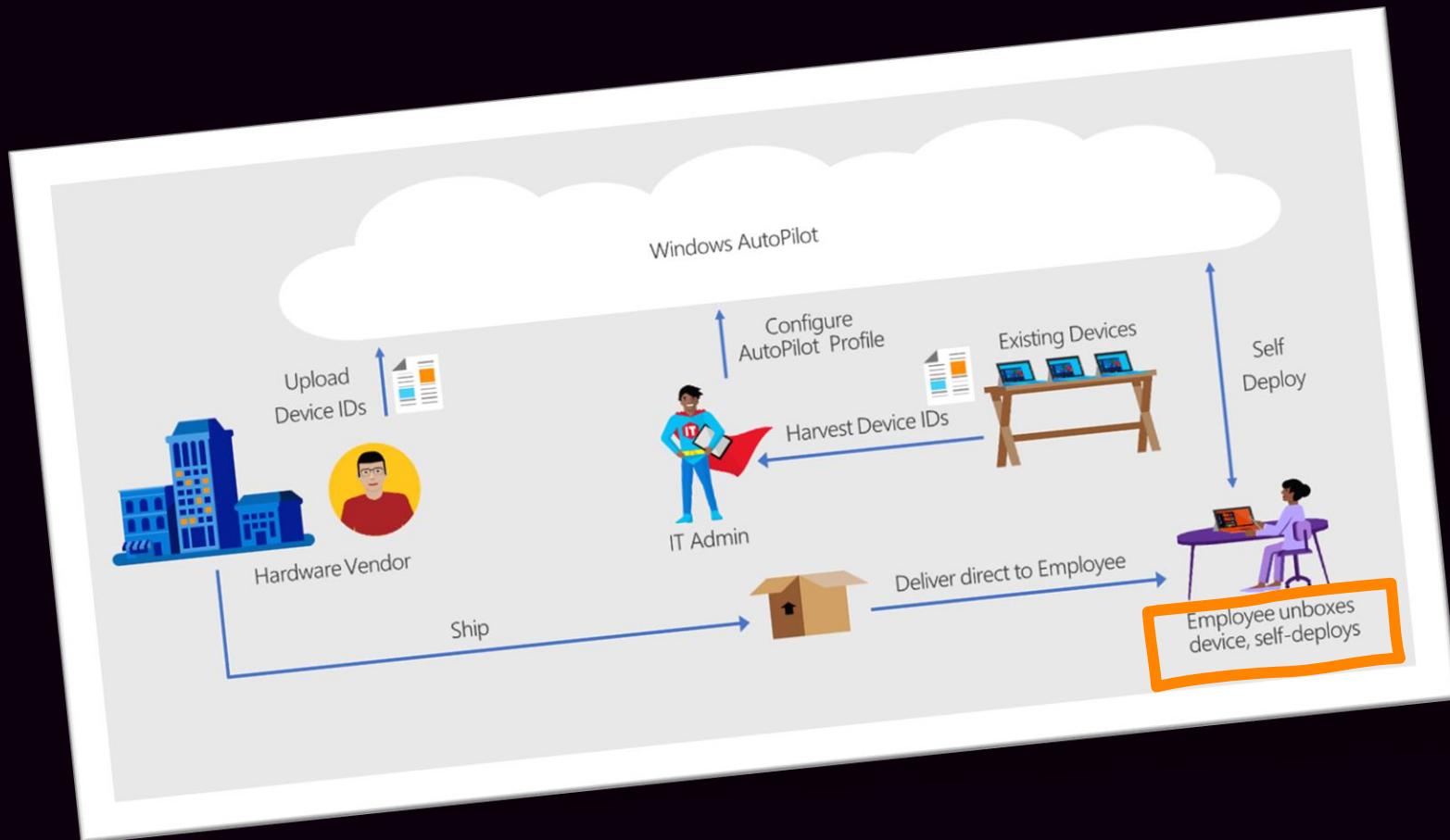
Overview All devices Monitor By platform Device onboarding Windows 365 Enrollment Manage devices Manage updates Organize devices Help and support Help and support

Search Add filters

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



# Windows Autopilot Device Onboarding II



## 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?

# 5 HOW?

## Can we do stuff?

### I NEED LOCAL ADMIN!

[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



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



Yes

No

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

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 &gt; 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 &gt; 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

[Got feedback?](#)[Diagnose and solve problems](#)

## Manage

[Assignments](#)[Description](#)

## Activity

[Bulk operation results](#)

## Troubleshooting + Support

[New support request](#)

## 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!

# 6 HOW?

Can we do stuff?

## I NEED LAPS!

Home &gt; 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



## 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

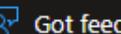
Diagnose and solve problems



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

137.43.73.32-9001 - Remote Desktop Connection

Event Viewer

File Action View Help

Event Viewer (Local)

Custom Views

Windows Logs

Application

Security (highlighted)

Setup

System

Forwarded Events

Applications and Services Log

Subscriptions

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 08:11:42 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

Event ID: 4625

Level: Information

User: N/A

OpCode: Info

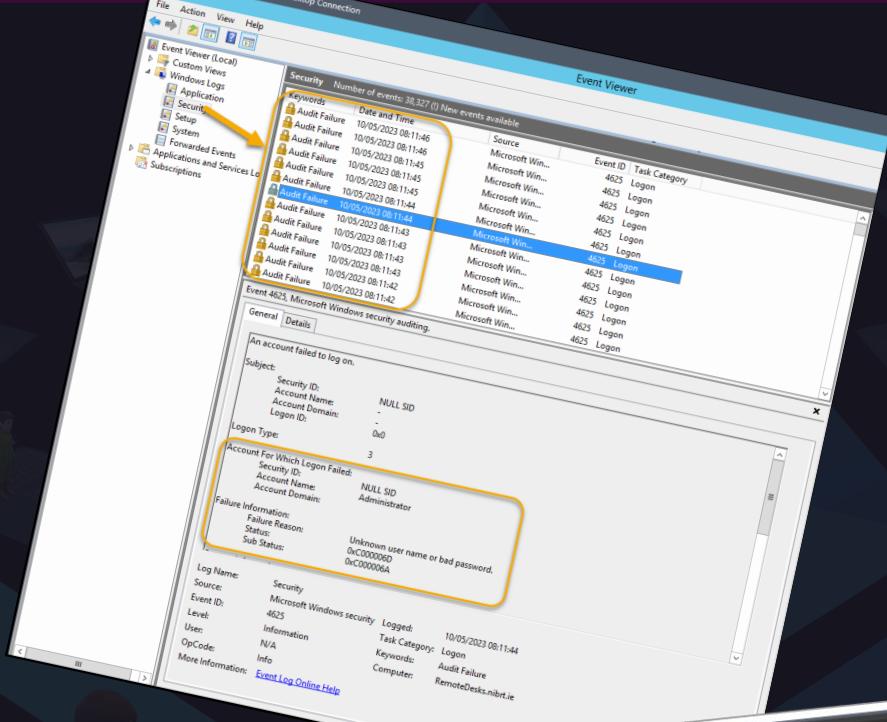
Keywords: Audit Failure

Logged: 10/05/2023 08:11:44

Task Category: Logon

Computer: RemoteDesks.nibr.ie

More information: [Event Log Online Help](#)



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 ①

### Local Policies Security Options

Accounts Enable Administrator Account

Enable

Status ①

Accounts Rename Administrator Account

LAPS Admin

Remove category



Previous

Next

NIC

EMPOWER

**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  Enable  
Status ⓘ Accounts Rename Administrator Account LAPS Admin

Download Next

Home > Devices | Windows > Windows | Windows devices > RM23-5CD9080YVF

## RM23-5CD9080YVF | Device query

Properties Search Run Clear input Cancel

1 LocalUserAccount  
2 | where WindowsSid endswith "-500"

Get started Results

Columns UserId Username UserDescription WindowsSid

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 ⚙️

Local Policies Security Options

Accounts Enable Administrator Account  Enable

Status ⓘ Accounts Rename Administrator Account LAPS Admin

Download Next

Home > Devices | Windows > Windows | Windows devices > RM23-5CD9080YVF

# RM23-5CD9080YVF | Device query

Properties

Search

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

NIC  
EMPOWER

# 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

Filter by title

## Local Administrator Password Solution (LAPS) improvements

LAPS has a new automatic account management feature. IT admins can configure Windows LAPS to:

- Automatically create the managed local account
- Configure name of account
- Enable or disable the account
- Randomize the name of the account

LAPS has the following policy improvements:

- Added passphrase settings for the [PasswordComplexity](#) policy
  - Use [PassphraseLength](#) to control the number of words in a new passphrase
- Added an improved readability setting for the [PasswordComplexity](#) policy, which generates passwords without using characters that are easily confused with another character. For example, the zero and the letter O aren't used in the password since the characters can be confused.
- Added the [Reset the password, logoff the managed account, and terminate any remaining processes](#) setting to the [PostAuthenticationActions](#) policy. The event logging messages that are emitted during post-authentication-action execution were also expanded, to give insights into exactly what was done during the operation.

What's new in Windows

Windows 11

- Windows 11 overview
- Windows 11 requirements
- Plan for Windows 11
- Prepare for Windows 11

Windows 11 enterprise feature control

What's new in Windows 11, version 24H2

- What's new in Windows 11, version 23H2
- What's new in Windows 11, version 22H2

Windows 10

Windows Enterprise LTSC

Windows commercial licensing overview

Deprecated and removed Windows features



# The LAPS Account

- Create a New Account Using a Policy?
- Same password on all devices
- Password in clear text

Add Row

OMA-URI Settings

* Name ⓘ	Windows 10 - Local user - Password
Description ⓘ	Not configured
* OMA-URI ⓘ	/ice/Vendor/MSFT/Accounts/Users/TestUser/Password
* Data type ⓘ	String
* Value ⓘ	P@ssw0rd!



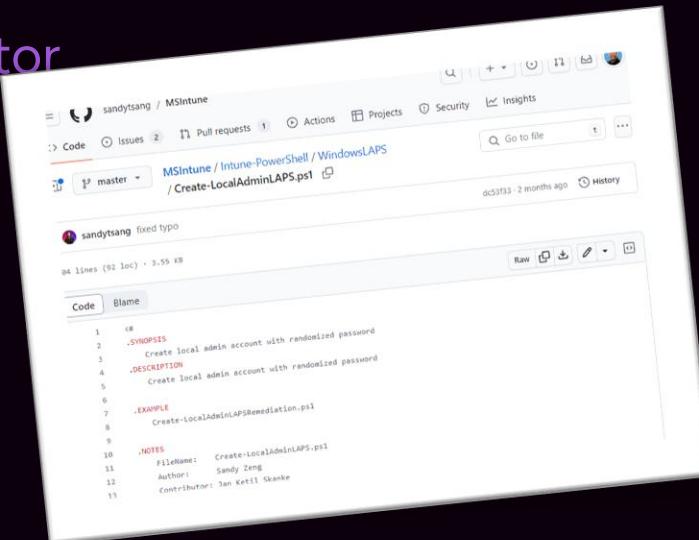
# The LAPS Account

- 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



A screenshot of a GitHub code editor displaying a PowerShell script named `Create-LocalAdminLAPS.ps1`. The script is intended to create a local admin account with a randomized password. It includes synopsis, description, example usage, and notes. The notes mention the file name, author (Sandy Zeng), and contributor (Jan Ketil Skanke).

```
1  #  
2  .SYNOPSIS  
3  Create local admin account with randomized password  
4  .DESCRIPTION  
5  Create local admin account with randomized password  
6  .EXAMPLE  
7  Create-LocalAdminLAPSRemediation.ps1  
8  .NOTES  
9  Filename: Create-LocalAdminLAPS.ps1  
10 Author: Sandy Zeng  
11 Contributor: Jan Ketil Skanke
```





# Devices | Scripts and remediations

 Search

## Remediations

Platform scripts

[Home](#)[Dashboard](#)[All services](#)[Devices](#)[Apps](#)[Endpoint security](#)[Reports](#)[Users](#)[Groups](#)[Tenant administration](#)[Troubleshooting + support](#)[Overview](#)[All devices](#)[Monitor](#)[By platform](#)[Device onboarding](#)[Manage devices](#)[Configuration](#)[Compliance](#)[Conditional access](#)[Scripts and remediations](#)[Group Policy analytics](#)[eSIM cellular profiles  
\(preview\)](#)

Create and run script packages on devices to proactively find and fix the issues in your organization. Use this table to see the status of your deployed script packages and remediation results. Results are shown as number of devices affected. [Learn more](#)

[Create](#)[Refresh](#)[Export](#)[Columns](#) Search[Add filters](#)[Script package name](#)

Script package name	Author	Status
PR001 - Windows LAPS Account	Simon Skotheimsvik	<span>✓ Active</span>
PR003 - Branding	Simon Skotheimsvik	<span>✓ Active</span>
PR008 - Start URL On Logon	Simon Skotheimsvik	<span>✓ Active</span>
Restart stopped Office C2R svc	Microsoft	<span>No activity</span>

## Edit - PR001 - Windows LAPS Account

### 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
```





Home &gt; Endpoint security



# Endpoint security | Account protection



Search



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

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

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

## Edit Policy

...

 Configuration settings  Review Search settings by setting name 

### LAPS

**Backup Directory**

Backup the password to Azure AD only

 Configured

7

**Password Age Days** **Administrator  
Account Name**  Configured

SimonDoesLocalAdmin

**Password  
Complexity**

Large letters + small letters + numbers + special characters (improved readability)

## 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

Password Age Days  

7

 ConfiguredAdministrator  
Account Name  

SimonDoesLocalAdmin

Password  
Complexity  Large letters + small letters + numbers + special characters (improved readability)  ConfiguredPassword Length  

14

Post Authentication  
Actions  Reset the password and logoff the managed account: upon expiry of the grace period, the manag...  ConfiguredPost Authentication  
Reset Delay  

2

 Next

# 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 of 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: '/', '.', '&', '!', 'Y', 'T', 'L', 'C', 'Y', '^', '\*, '=' , '?', '\*\*'
  - Start using 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.

# Announcing Windows 11 Insider Preview Build 2604 ( Canary Channel)

## Windows LAPS: New passphrase feature

Written By  
Amanda Lango  
Brandon LeBlanc  
  
published  
January 26, 2024

[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.

Password Age Days  

7

 ConfiguredAdministrator  
Account Name  

SimonDoesLocalAdmin

Password  
Complexity  Large letters + small letters + numbers + special characters (improved readability)  ConfiguredPassword Length  

14

Post Authentication  
Actions  Reset the password and logoff the managed account: upon expiry of the grace period, the manag...  ConfiguredPost Authentication  
Reset Delay  

2

 Next

Password Age Days  

7

 ConfiguredAdministrator Account Name  

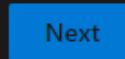
SimonDoesLocalAdmin

Password Complexity  Large letters + small letters + numbers + special characters (improved readability)  ConfiguredPassword Length  

14

Post Authentication Actions  Reset the password and logoff the managed account: upon expiry of the grace period, the manag...  ConfiguredPost Authentication Reset Delay  

2

 Next



# Endpoint security | Account protection



Search



Create Policy



Refresh



Export

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

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 (Preview)
WESP503 - ACP - Local Administrators		Local user group membership



# Endpoint security | Account protection



Search



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 (Preview)

WESP503 - ACP - Local Administrators

Local user group membership

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Endpoint detection and response

App Control for Business (Preview)

Attack surface reduction

Account protection

Device compliance

Conditional access

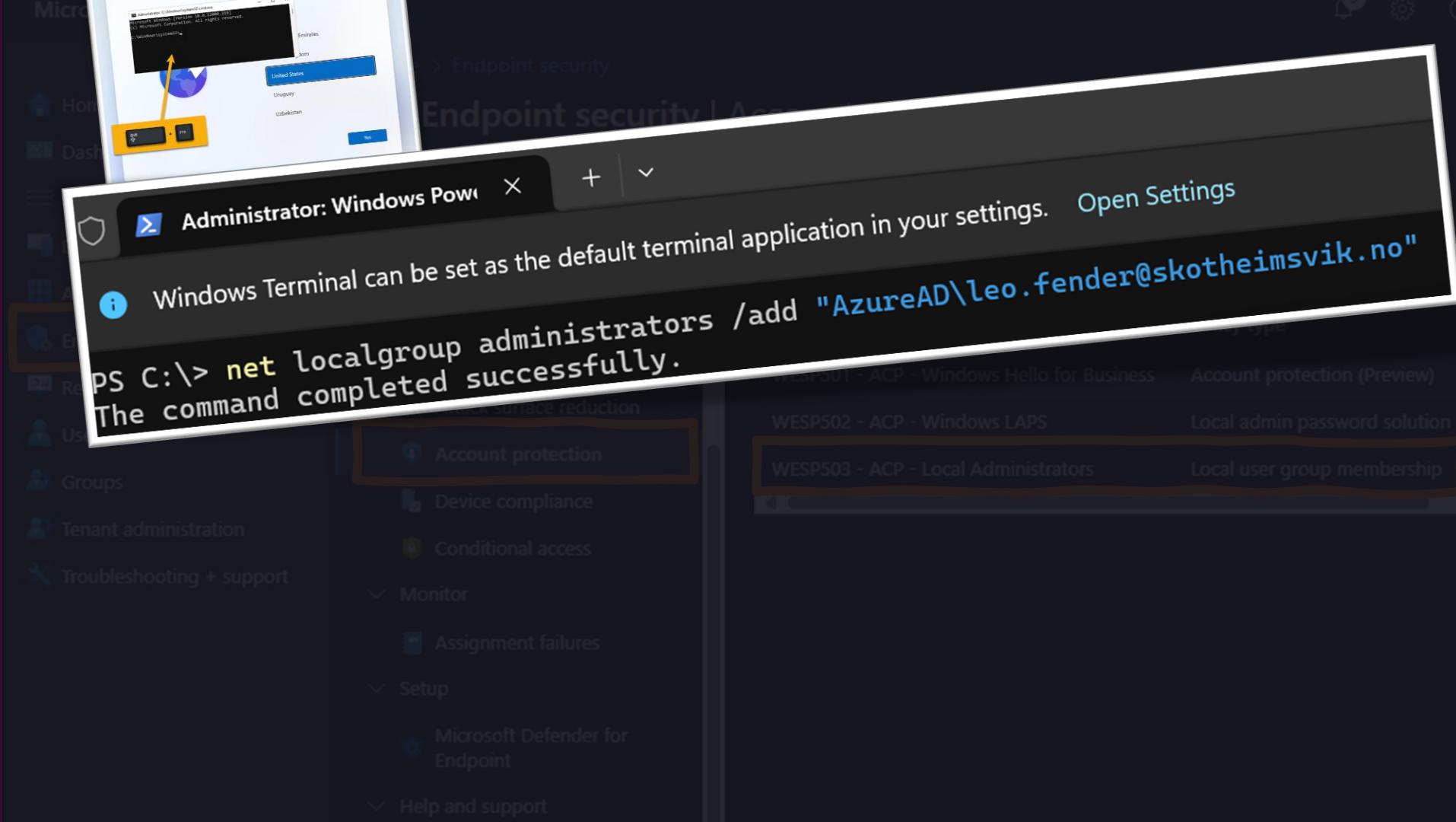
Monitor

Assignment failures

Setup

Microsoft Defender for Endpoint

Help and support





> Endpoint security

## Endpoint security | Advanced

Administrator: Windows PowerShell

PS C:\> net localgroup administrators /add "AzureAD\leo.fender@skotheimsvik.no"

The command completed successfully.

- Home
- Dashboards
- Activity
- Events
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

- Account protection
- Device compliance
- Conditional access
- Monitor
  - Assignment failures
- Setup
  - Microsoft Defender for Endpoint
- Help and support

- WESP501 - ACP - Windows Hello for Business
- WESP502 - ACP - Windows LAPS
- WESP503 - ACP - Local Administrators
- Account protection (Preview)
- Local admin password solution (Preview)
- Local user group membership

 i 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.
```

Dashboard Create Policy Refresh Export ?

## Computer Management

File Action View Help

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	Administrators
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 gro
Network Configuratio...	Members in

### Administrators Properties

#### General

 Administrators

Description: Administrators have complete and unrestricted access to 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



# Endpoint security | Account protection



Search



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 (Preview)

WESP503 - ACP - Local Administrators

Local user group membership

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

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

## Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Endpoint security | Account protection > WESP503 - ACP - Local

## 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. Entries will 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 learn more](#)

Delete Sort Export

SimonDoesLocalAdmin

S-1-12-1-158575896-1174998709-2722327981-331

S-1-12-1-424057452-1234611653-408369830-3020

Administrator

## Microsoft Intune admin center



Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

[Home](#) > [Endpoint security | Account protection](#) > [WESP503 - ACP - Local](#)

## 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. Enter the user names or SIDs of the users you want to add. User names appear on the device. You can use the following formats:

- Username
- Domain\username
- SID (security identifier)

Invalid identifier entries. [Learn more](#)

LAPS Account

Delete    Sort    Export

 SimonDoesLocalAdmin S-1-12-1-158575896-1174998709-2722327981-331 S-1-12-1-424057452-1234611653-408369830-3020 Administrator

## Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

[Home](#) > [Endpoint security | Account protection](#) > [WESP503 - ACP - Local Admin](#)

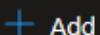
## Edit profile - WESP503 - ACP - Local Admin

Settings catalog

## ① Configuration settings

② Review + save

## ^ Local Users And Groups



Add



Delete

 Local group 

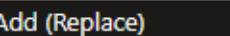
## Group and user action



Administrators



Add (Replace)



Delete



Sort



Export



SimonDoesLocalAdmin



S-1-12-1-158575896-1174998709-2722327981-331



S-1-12-1-424057452-1234611653-408369830-3020



Administrator

Builtin local Administrator

## Microsoft Intune admin center

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

Home > Endpoint security | Account protection > WESP503 - ACP - Local

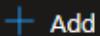
## Edit profile - WESP503 - ACP - Local

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. Entries will 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 learn more](#)

Delete ⏪ Sort ⏴ Export

SimonDoesLocalAdmin

S-1-12-1-158575896-1174998709-2722327981-331

S-1-12-1-424057452-1234611653-408369830-3020

Administrato

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

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

Entra ID Global Administrator Role  
and  
Entra ID Device Administrator Role

## Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Endpoint security | Account protection > WESP503 - ACP - Local

## 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. Entries will 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 learn more](#)

Delete ⏪ Sort ⏴ Export

SimonDoesLocalAdmin

S-1-12-1-158575896-1174998709-2722327981-331

S-1-12-1-424057452-1234611653-408369830-3020

Administrato

Entra ID Global Administrator Role  
and  
Entra ID Device Administrator Role

Microsoft Intune admin center

https://intune.microsoft.com/#view/Microsoft\_Intune\_Workflows/SettingsCatalogWizardBlade/policyId...

Graph Explorer aka.ms/ge

Tenant Simon Does

Run query

GET beta https://graph.microsoft.com/beta/directoryRoles

OK - 200 - 144ms

Response preview

Response headers

Code snippets

Toolkit component

Adaptive cards

Device local Admin

1 of 1

description : Can read basic directory information and has full access to applications and guests.",  
access to applications and guests.",  
"displayName": "Directory Readers",  
"roleTemplateId": "88d8e3e3-8f55-4a1e-953a-9b989b8876b"  
,  
{  
"id": "699a1803-dc8d-4919-aa06-5a9fb4a65ec1",  
"deletedDateTime": null,  
"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"  
,

Microsoft Intune admin center

https://intune.microsoft.com/#view/Microsoft\_Intune\_Workflows/SettingsCatalogWizardBlade/policyId...

Graph Explorer

GET beta https://graph.m...

OK - 200 - 144ms

Response preview

```
description : "access to applications and groups", "displayName": "Azure AD Joined Device Local Administrator", "roleTemplateId": "9f06204d-73c1-4d4c-880a-6edb90606fd8", "id": "699a1803-dc8d-4919-aa06-5a9fb4a65ec1", "deletedDateTime": null, "description": "Users assigned to this role can manage Microsoft Entra joined devices.", "displayName": "Azure AD Joined Device Local Administrator", "roleTemplateId": "9f06204d-73c1-4d4c-880a-6edb90606fd8"}, {
```

Tenant 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

## Microsoft Intune admin center



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

Home > Endpoint security | Account protection > WESP503 - ACP - Local

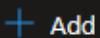
## Edit profile - WESP503 - ACP - Local

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. Entries will 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 learn more](#)

Delete Sort Export

<input type="checkbox"/>	SimonDoesLocalAdmin
<input type="checkbox"/>	S-1-12-1-158575896-1174998709-2722327981-3181
<input type="checkbox"/>	S-1-12-1-424057452-1234611653-408369830-3020
<input type="checkbox"/>	Administrator



- 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...	Member
Administrators	Administrators
Backup Operators	Backup Operators
Cryptographic Operat...	Member
Device Owners	Member
Distributed COM Users	Member
Event Log Readers	Member
Guests	Guests have limited access to the computer.
Hyper-V Administrators	Member
IIS_IUSRS	Built-in group for IIS users.
Network Configuration...	Member
Performance Log Users	Member
Performance Monitor ...	Member
Power Users	Power Users
Remote Desktop Users	Member
Remote Management ...	Member
Replicator	Support Replicator
System Managed Acco...	Member
Users	Users are part of the local group.

## 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

Changes to a user's group membership are not effective until the next time the user logs on.

Add...

Remove

OK

Cancel

Apply

Help

## Actions

## Groups

More Actions

## Administrators

More Actions



Search

CloudWay



ENG NO

&lt;

Home &gt; Devices | Windows &gt; Windows | Windows devices &gt; LETSDO-41100003



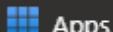
Home



All services



Devices



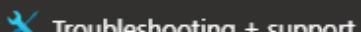
Endpoint security



Users



Tenant administration



LETSDO-41100003



Search

&lt;&lt;



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 Solution (LAPS) →

Local administrator password

Show local administrator password

Last password rotation

12/20/2023, 1:13:00 PM

&lt;

Home &gt; Devices | Windows &gt; Windows | Windows devices &gt; 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

[Show local administrator password](#)

Last passwo

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

&lt;

Home &gt; Devices | Windows &gt; Windows | Windows devices &gt; LETSDO-41100003

## LETSDO-41100003 | Local admin password



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

&lt;

Home &gt; Devices | Windows &gt; Windows | Windows devices &gt; LETSDO-41100003

## LETSDO-41100003 | Local admin password



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@GywOP#0g%{+6n



### Last password rotation

12/20/2023, 1:13:00 PM

### Next password rotation

12/27/2023, 1:13:00 PM



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...	Member
Administrators	Administrators
Backup Operators	Backup Operators
Cryptographic Operat...	Member
Device Owners	Member
Distributed COM Users	Member
Event Log Readers	Member
Guests	Guests have limited access to the computer.
Hyper-V Administrators	Member
IIS_IUSRS	Built-in group for IIS users.
Network Configuration...	Member
Performance Log Users	Member
Performance Monitor ...	Member
Power Users	Power Users have increased access to system resources.
Remote Desktop Users	Member
Remote Management ...	Member
Replicator	Supports replication between servers.
System Managed Acco...	Member
Users	Users are part of the local group.

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

Changes to a user's group membership are not effective until the next time the user logs on.

Add... Remove OK Cancel Apply Help

Actions
Groups More Actions
Administrators More Actions



# 6 HOW? Can we do stuff? I NEED LAPS!

# 6 HOW?

Can we do stuff?  
I NEED LAPS!

## Local Admin Access

# 6 HOW?

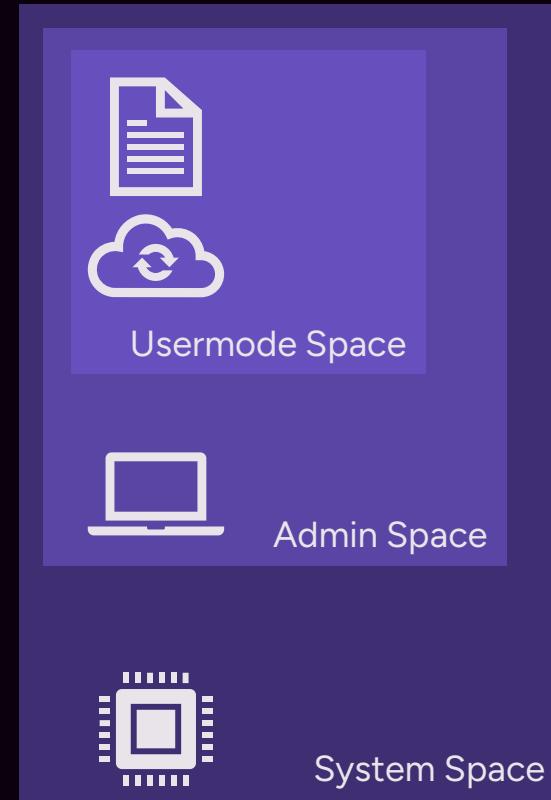
## Can we do stuff? I NEED LAPS!

### Local Admin Access

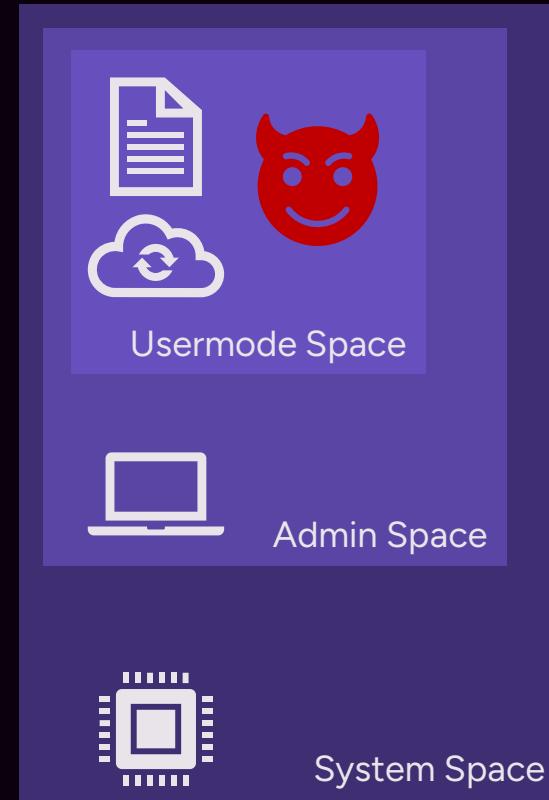
# Local Admin Access



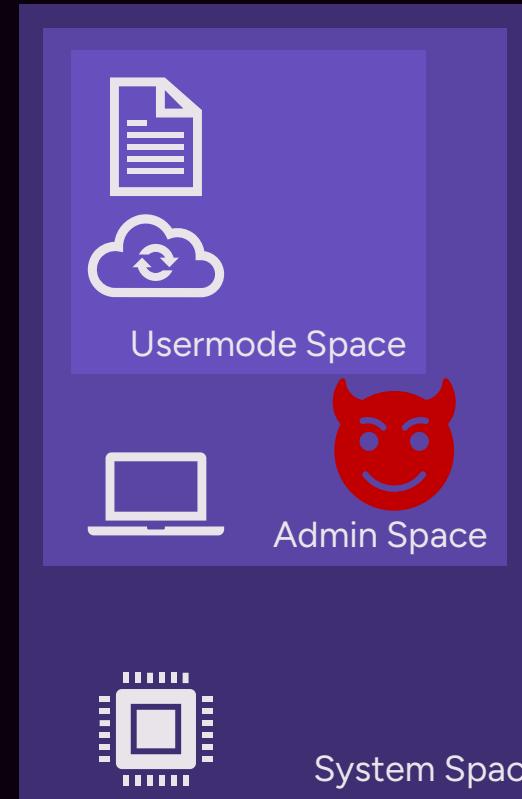
# Local Admin Access



# Local Admin Access



# Local Admin Access



# Local Admin Access



Usermode Space



Admin Space



System Space

# 6 HOW?

Can we do stuff?  
I NEED LAPS!

## Local Admin Access



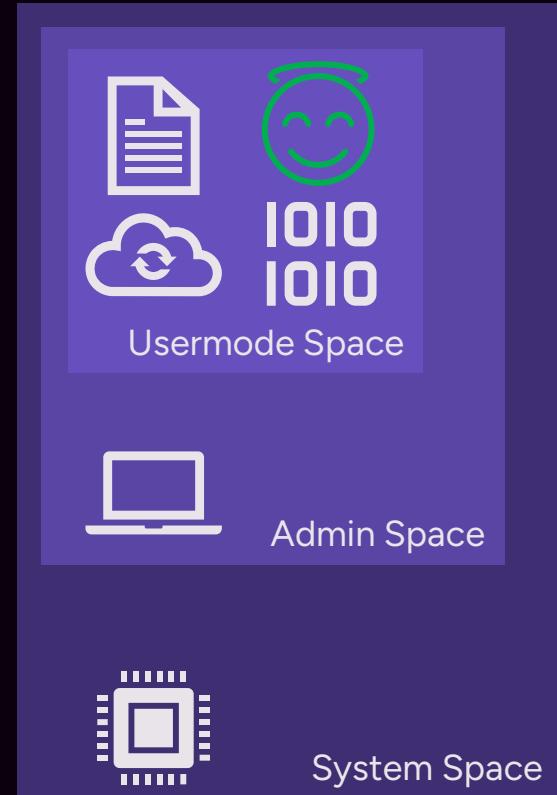
NIC  
EMPOWER

# 7 HOW? Can we do stuff?

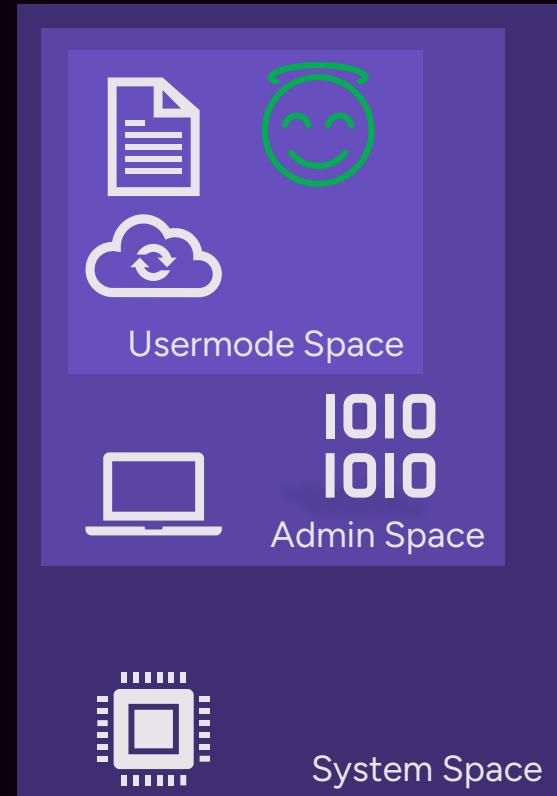
I NEED EPM!



# Endpoint Privilege Management



# Endpoint Privilege Management



# 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		✓	✓

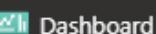




Home &gt; Tenant admin



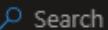
Home



Home &gt; 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 more](#)

Intune add-on name	Description
Microsoft Intune Suite	A suite of advanced endpoint and security features unified in Microsoft Intune that include... <a href="#">Learn more about Microsoft Intune Suite</a>
Intune Plan 2	Intune Plan 2 is an add-on bundle to the Microsoft Intune service that offers a collection of advanced endpoint management features... <a href="#">Learn more about Intune Plan 2</a>
Endpoint Privilege Management	Microsoft Intune Endpoint Privilege Management allows users to perform elevations approved by their administrator... <a href="#">Learn more about Endpoint Privilege Management</a>



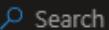
Home &gt; Tenant admin



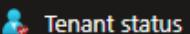
Home



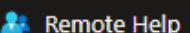
## Tenant admin | Intune add-ons



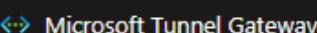
Search



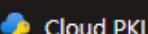
Tenant status



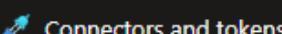
Remote Help



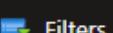
Microsoft Tunnel Gateway



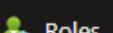
Cloud PKI



Connectors and tokens



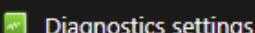
Filters



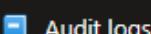
Roles



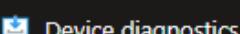
Microsoft Entra Privileged Identity Management



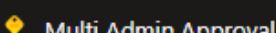
Diagnostics settings



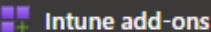
Audit logs



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 more](#)

Intune add-on name	Description
Microsoft Intune Suite	A suite of advanced endpoint and security management tools unified in Microsoft Intune that include... <a href="#">Learn more about Microsoft Intune Suite</a>
Intune Plan 2	Intune Plan 2 is an add-on bundle to the Microsoft Intune Suite that offers a collection of advanced endpoint management features... <a href="#">Learn more about Intune Plan 2</a>
Endpoint Privilege Management	Microsoft Intune Endpoint Privilege Management allows users to perform elevations approved by their administrator... <a href="#">Learn more about Endpoint Privilege Management</a>

# 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

# 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

Microsoft Intune admin center

Home > Endpoint security

## Endpoint security | Endpoint Privilege Management

Search Reports Policies Reusable settings Elevation requests

Overview Manage

- Antivirus
- Disk encryption
- Firewall

Create Policy Refresh Export

Search by profile name

Policy name	Policy type	Assigned	Platform
No results			

Endpoint Privilege Management

- Endpoint detection and response
- App Control for Business (Preview)
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

The screenshot shows the Microsoft Intune admin center interface. The left sidebar has a dark theme with orange highlights around the 'Endpoint security' and 'Endpoint Privilege Management' sections. The main content area shows the 'Endpoint security | Endpoint Privilege Management' page. At the top, there are tabs for 'Reports', 'Policies' (which is selected and highlighted with an orange box), 'Reusable settings', and 'Elevation requests'. Below the tabs, a message states: 'Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Admin start a trial or buy licenses.' There are buttons for 'Create Policy', 'Refresh', and 'Export'. A search bar is labeled 'Search by profile name'. A table below shows columns for 'Policy name', 'Policy type', 'Assigned', and 'Platform', with a note 'No results'. The 'Endpoint Privilege Management' section in the main content area is also highlighted with an orange box.



Home &gt; Endpoint security

## Endpoint security | Endpoint Privilege

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Search



&gt; 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

Re

 Endpoint Privilege Management  
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

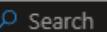
Elevation settings policy

Create



Home &gt; Endpoint security

## Endpoint security | Endpoint Privilege



Search



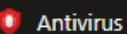
Reports

Policies

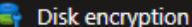
Re

&gt; Overview

Manage



Antivirus



Disk encryption



Firewall

**Endpoint Privilege Management**

Endpoint detection and response

App Control for Business (Preview)

Attack surface reduction

Account protection

Device compliance

Conditional access

Endpoint Privilege Management  
start a trial or buy licenses

Create Policy



Search by profile name

Policy name

No results

## Create a profile

Platform

Windows

Profile

Select a profile

Elevation rules policy

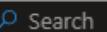
Elevation settings policy

Create



Home &gt; Endpoint security

## Endpoint security | Endpoint Privilege



Search



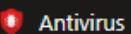
Reports

Policies

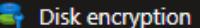
Re

&gt; Overview

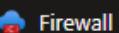
Manage



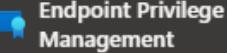
Antivirus



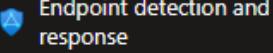
Disk encryption



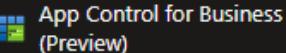
Firewall



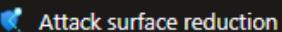
Endpoint Privilege Management



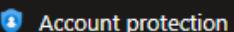
Endpoint detection and response



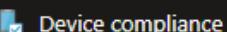
App Control for Business (Preview)



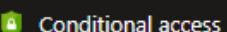
Attack surface reduction



Account protection



Device compliance



Conditional access

## Create a profile

Platform

Windows

Profile

Select a profile

Elevation rules policy

Elevation settings policy

Search by profile name

Policy name

No results

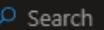
Create



Home &gt; Endpoint security



## Endpoint security | Endpoint Privilege

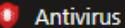


Search

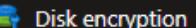


&gt; Overview

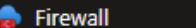
Manage



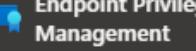
Antivirus



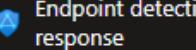
Disk encryption



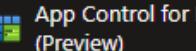
Firewall



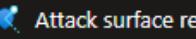
Endpoint Privilege Management



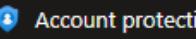
Endpoint detection and response



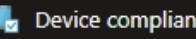
App Control for Business (Preview)



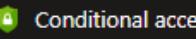
Attack surface reduction



Account protection



Device compliance

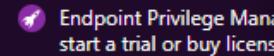
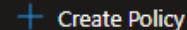


Conditional access

Reports

Policies

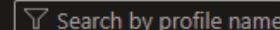
Re

Endpoint Privilege Management  
start a trial or buy licens

Create Policy



Ref



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 endpoint 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, endpointPrivileged supported devices

  
Create



## 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

# Create profile

Elevation settings policy

Basics

Configuration settings

Scope tags

Assignments

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 \*

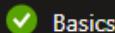
Diagnostic data and all endpoint elevations

[Previous](#)[Next](#)

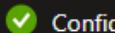
# Create profile

...

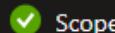
Elevation settings policy



Basics



Configuration settings



Scope tags



Assignments



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

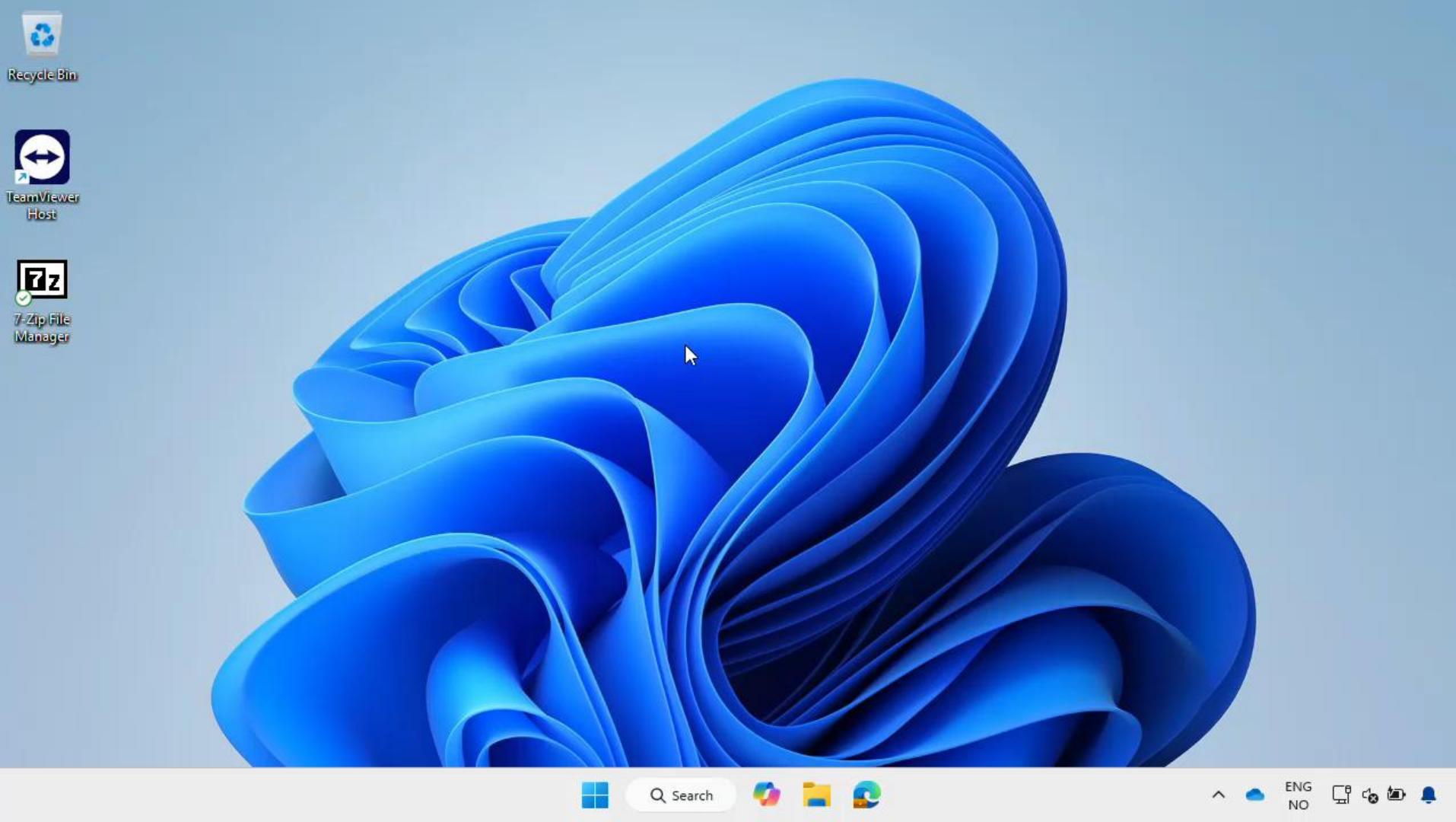
Group Members ⓘ

Remove

No groups selected

Previous

Next



Recycle Bin



TeamViewer  
Host



7-Zip File  
Manager



Search



ENG  
NO



Home &gt; Endpoint security



# Endpoint security | Endpoint Privilege Management

 Search

Reports

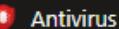
Policies

Reusable settings

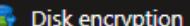
Elevation requests

&gt; Overview

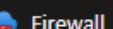
Manage



Antivirus



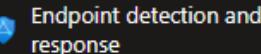
Disk encryption



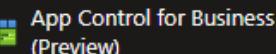
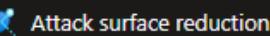
Firewall



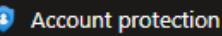
Endpoint Privilege Management



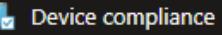
Endpoint detection and response

App Control for Business  
(Preview)

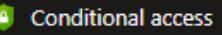
Attack surface reduction



Account protection



Device compliance



Conditional access



Status == all

File ↑↓	Publisher ↑↓	Username ↑↓	Status ↑↓	Last modified
7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Pending	11/01/24, 2
7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Denied	11/01/24, 2



Home &gt; Endpoint security

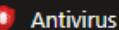


# Endpoint security | Endpoint Privilege Management

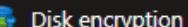
 Search

&gt; Overview

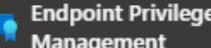
Manage



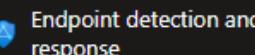
Antivirus



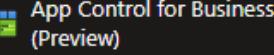
Firewall



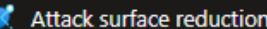
Endpoint Privilege Management



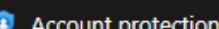
Endpoint detection and response



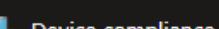
(Preview)



Attack surface reduction



Account protection



Device compliance



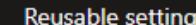
Conditional access



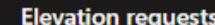
Reports



Policies



Reusable settings



Elevation requests



Refresh



Search

Status == all

File ↑↓

Publisher ↑↓

Username ↑↓

Status ↑↓

Last modified

7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Pending	11/01/24, 2024
7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Denied	11/01/24, 2024

Home &gt; Endpoint security

# Endpoint security | Endpoint

Search

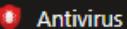
Search

...

&lt;

&gt; Overview

Manage



Antivirus



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

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

## 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
-----------	------------------------



# Endpoint security | Endpoint

Reports



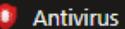
File ↑↓

7zFM.exe

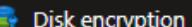
7zFM.exe

&gt; Overview

Manage



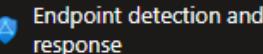
Antivirus



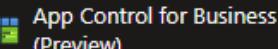
Firewall



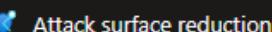
Endpoint Privilege Management



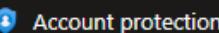
Endpoint detection and response



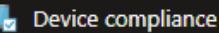
App Control for Business (Preview)



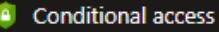
Attack surface reduction



Account protection



Device compliance



Conditional access

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

028CF2158DF45889E9A565C9CE3C6048FB05C286B97F39

Version

24.8.0.0

File description

7-Zip File Manager

Product name

7-Zip

Internal name

7zFM

Approve

Deny



Home &gt; Endpoint security

# Endpoint security | Endpoint

Reports



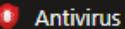
File ↑↓

7zFM.exe

7zFM.exe

&gt; Overview

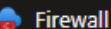
Manage



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

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 028CF2158DF45889E9A565C9CE3C6648FB05C286B97F39

Version 24.8.0.0

File description 7-Zip File Manager

Product name 7-Zip

Internal name 7zFM

Approve

Deny

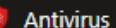


## Endpoint security | Endpoint

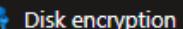
 Search

&gt; Overview

Manage



Antivirus



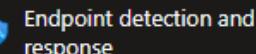
Disk encryption



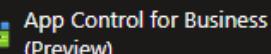
Firewall



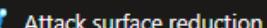
Endpoint Privilege Management



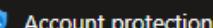
Endpoint detection and response



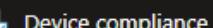
App Control for Business (Preview)



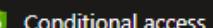
Attack surface reduction



Account protection

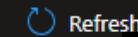


Device compliance



Conditional access

Reports



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



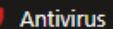
Home &gt; Endpoint security

# Endpoint security | Endpoint

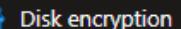
 Search

&gt; Overview

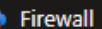
Manage



Antivirus



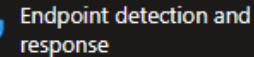
Disk encryption



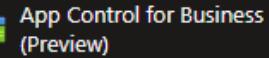
Firewall



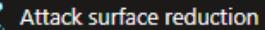
Endpoint Privilege Management



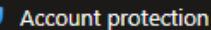
Endpoint detection and response



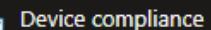
App Control for Business (Preview)



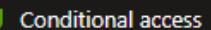
Attack surface reduction



Account protection

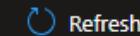


Device compliance



Conditional access

Reports



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

Behave!

Yes

No

File description

7-Zip File Manager

Product name

7-Zip

Internal name

7zFM

Approve

Deny

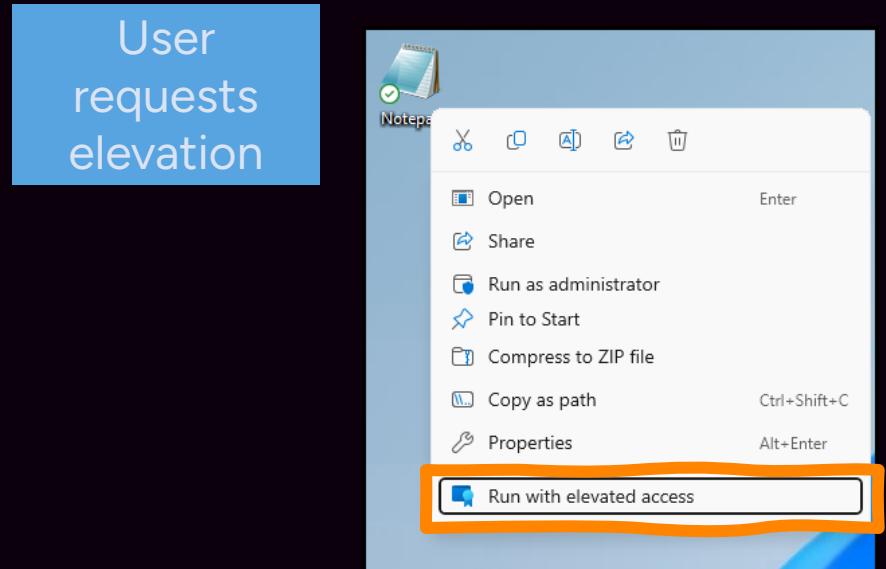
# Endpoint Privilege Management (EPM)

- Support Approved workflow

User  
requests  
elevation

# Endpoint Privilege Management (EPM)

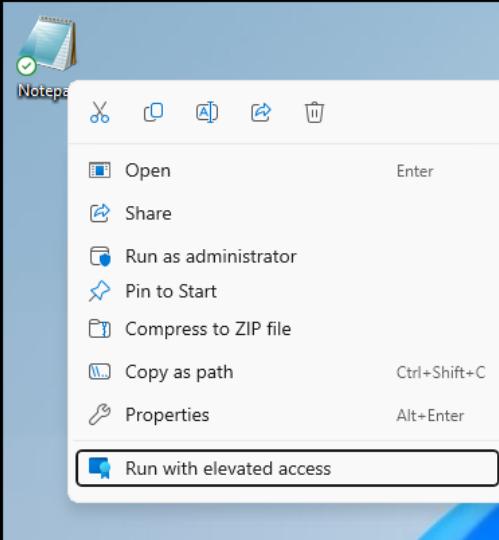
- Support Approved workflow



# Endpoint Privilege Management (EPM)

- Support Approved workflow

User requests elevation



Endpoint Privilege Management

Request to open this app as administrator?

notepad  
Verified publisher: Microsoft Windows

Enter business justification

I need to take notes  
20/280

You'll be asked to verify your identity. Once verified, your request will be sent.

This information will be sent to your organization's IT admin. [Privacy info](#)

Cancel Send

The image shows two screenshots illustrating the Endpoint Privilege Management (EPM) process. On the left, a blue callout box labeled 'User requests elevation' points to a Windows context menu for the 'Notepad' application. The menu items include 'Open', 'Share', 'Run as administrator' (which is highlighted with a red box), 'Pin to Start', 'Compress to ZIP file', 'Copy as path', 'Properties', and 'Run with elevated access'. On the right, a window titled 'Endpoint Privilege Management' displays a request to open 'notepad' as an administrator. It asks for a 'business justification' (with 'I need to take notes' entered) and states that verification will be required. A red box highlights the 'Enter business justification' field. At the bottom, there are 'Cancel' and 'Send' buttons.

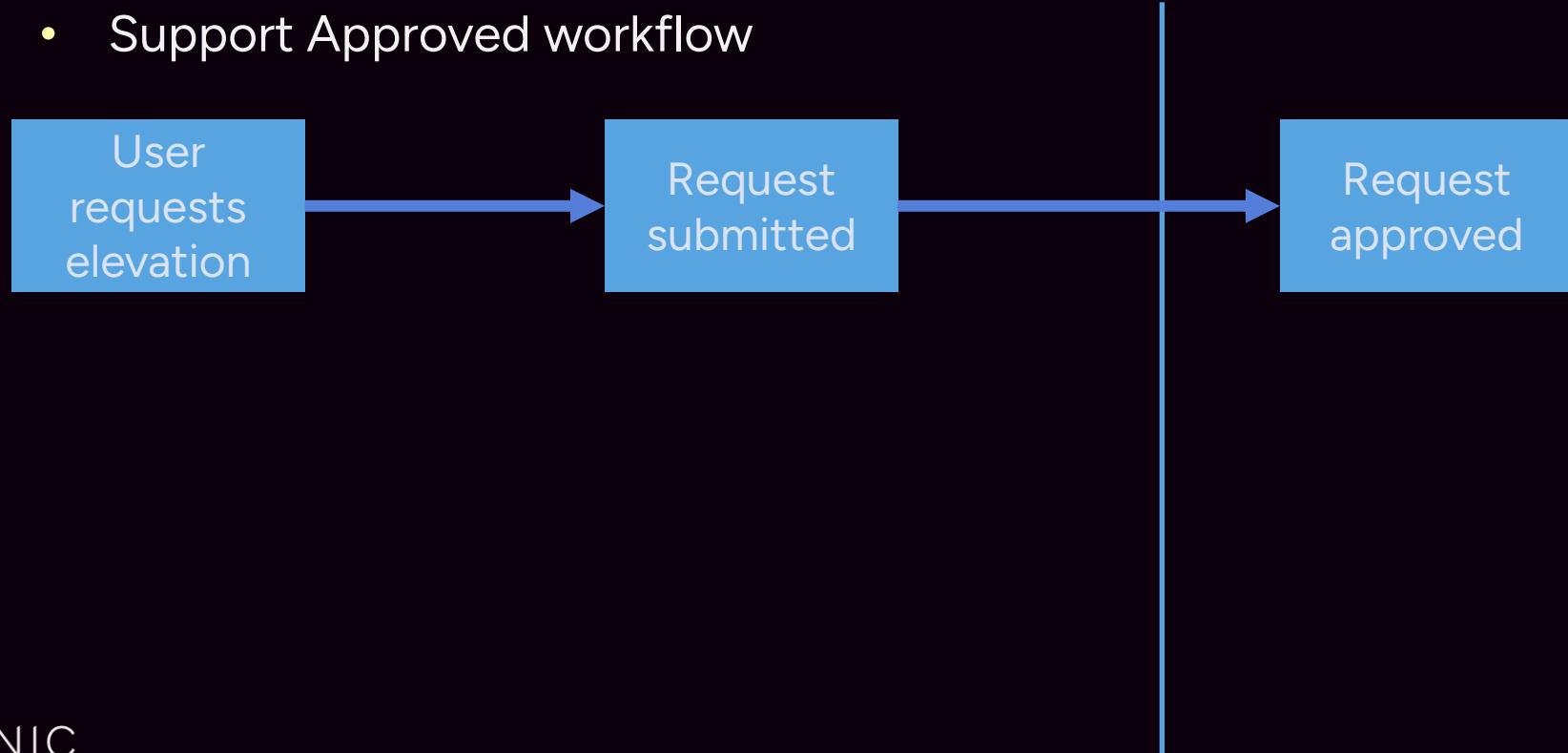
# Endpoint Privilege Management (EPM)

- Support Approved workflow



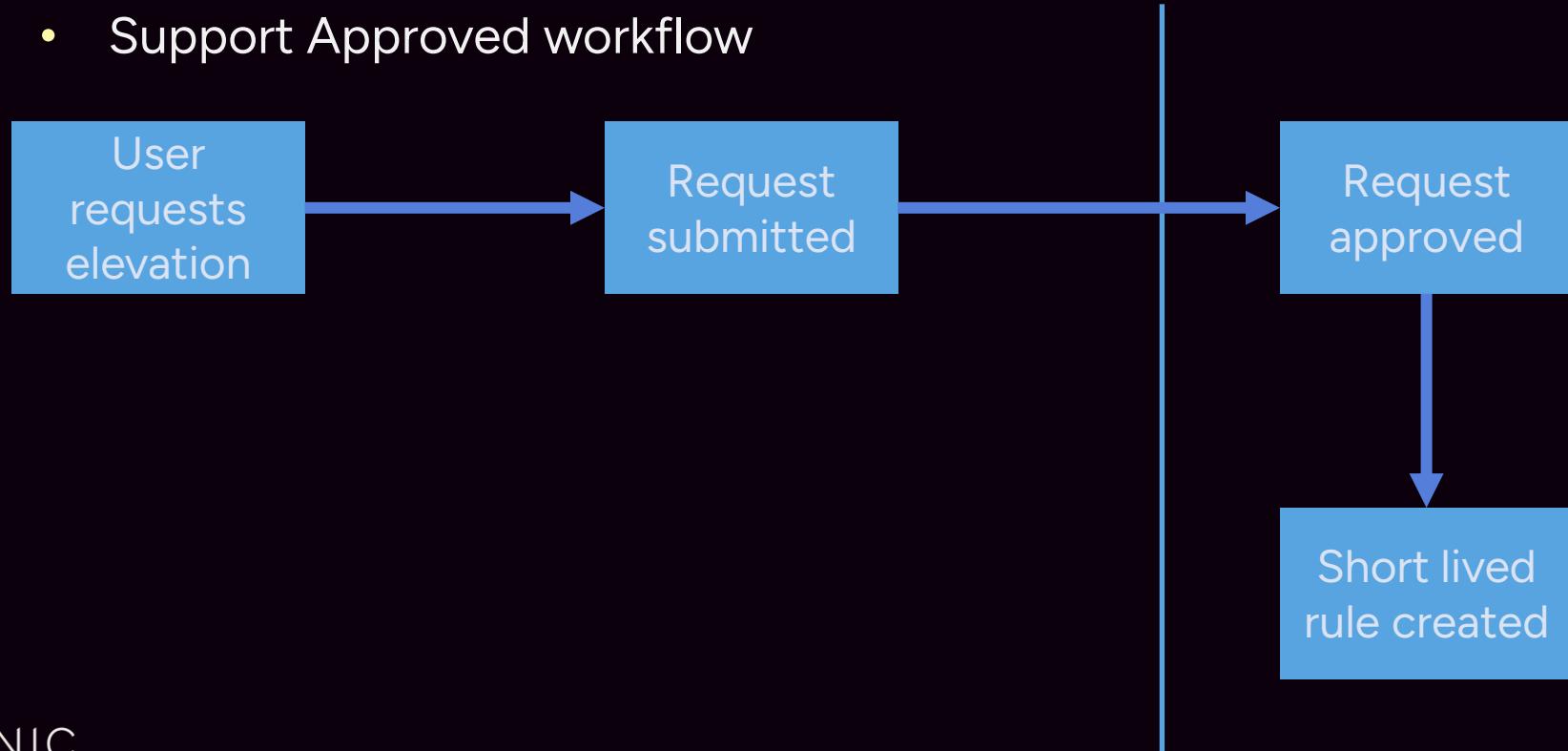
# Endpoint Privilege Management (EPM)

- Support Approved workflow



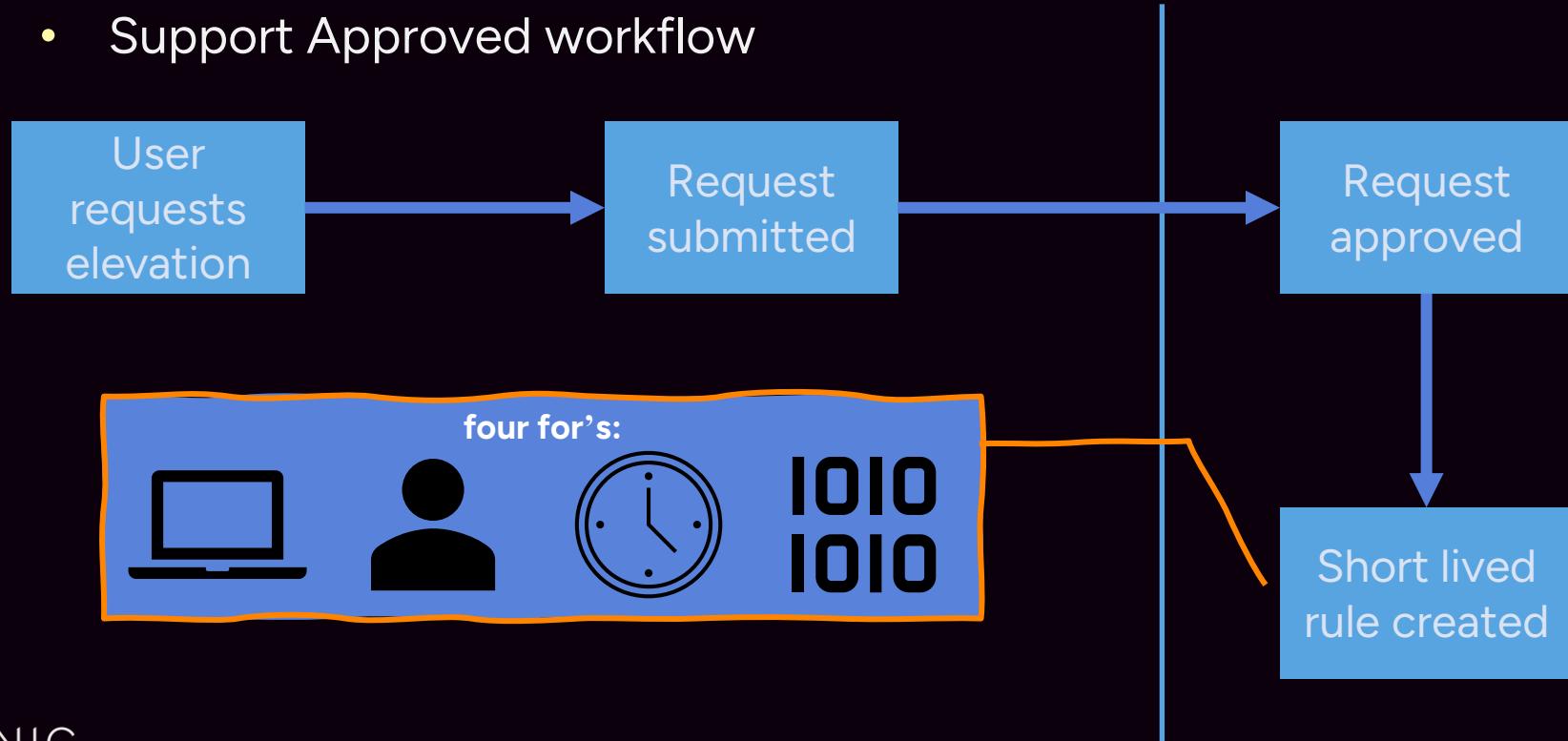
# Endpoint Privilege Management (EPM)

- Support Approved workflow



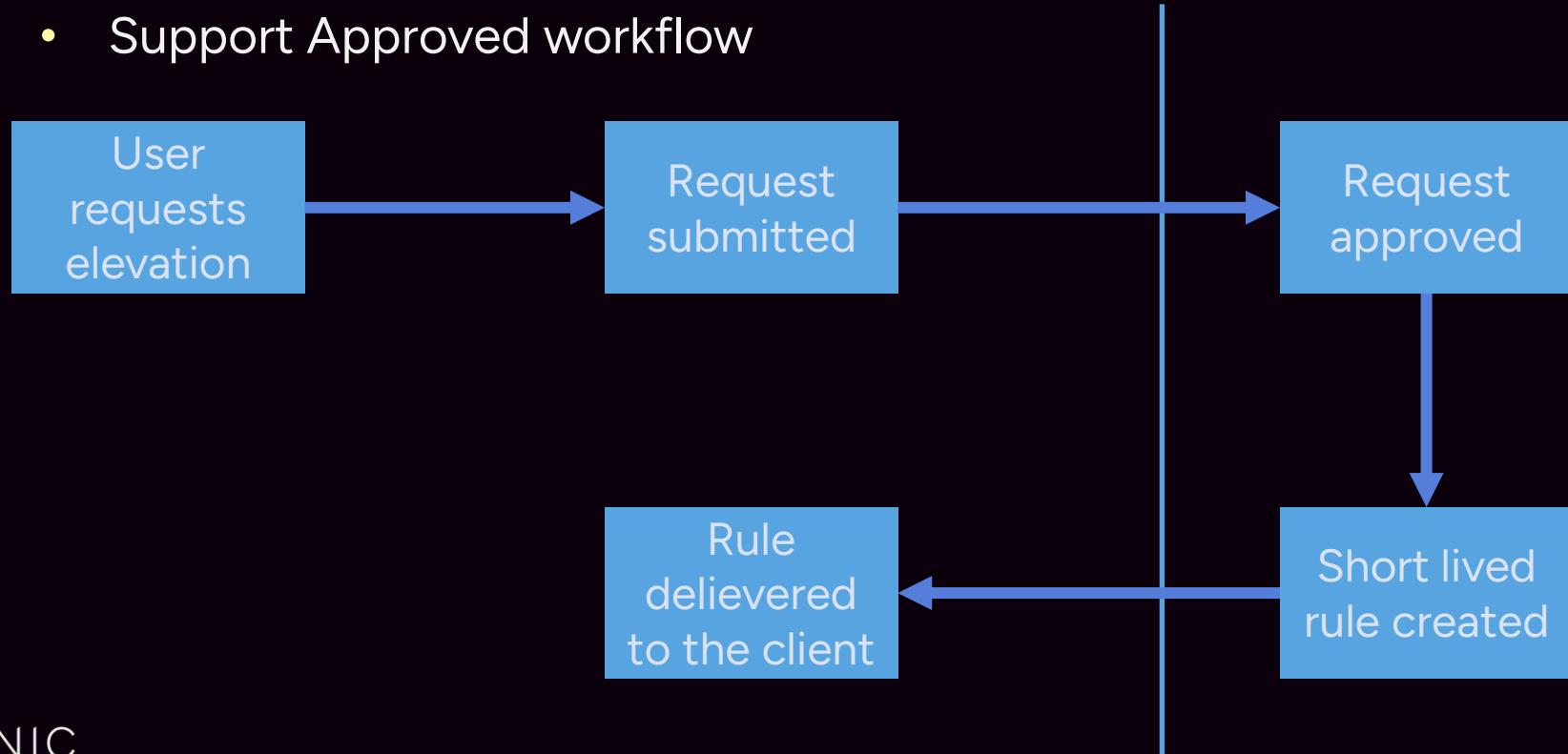
# Endpoint Privilege Management (EPM)

- Support Approved workflow



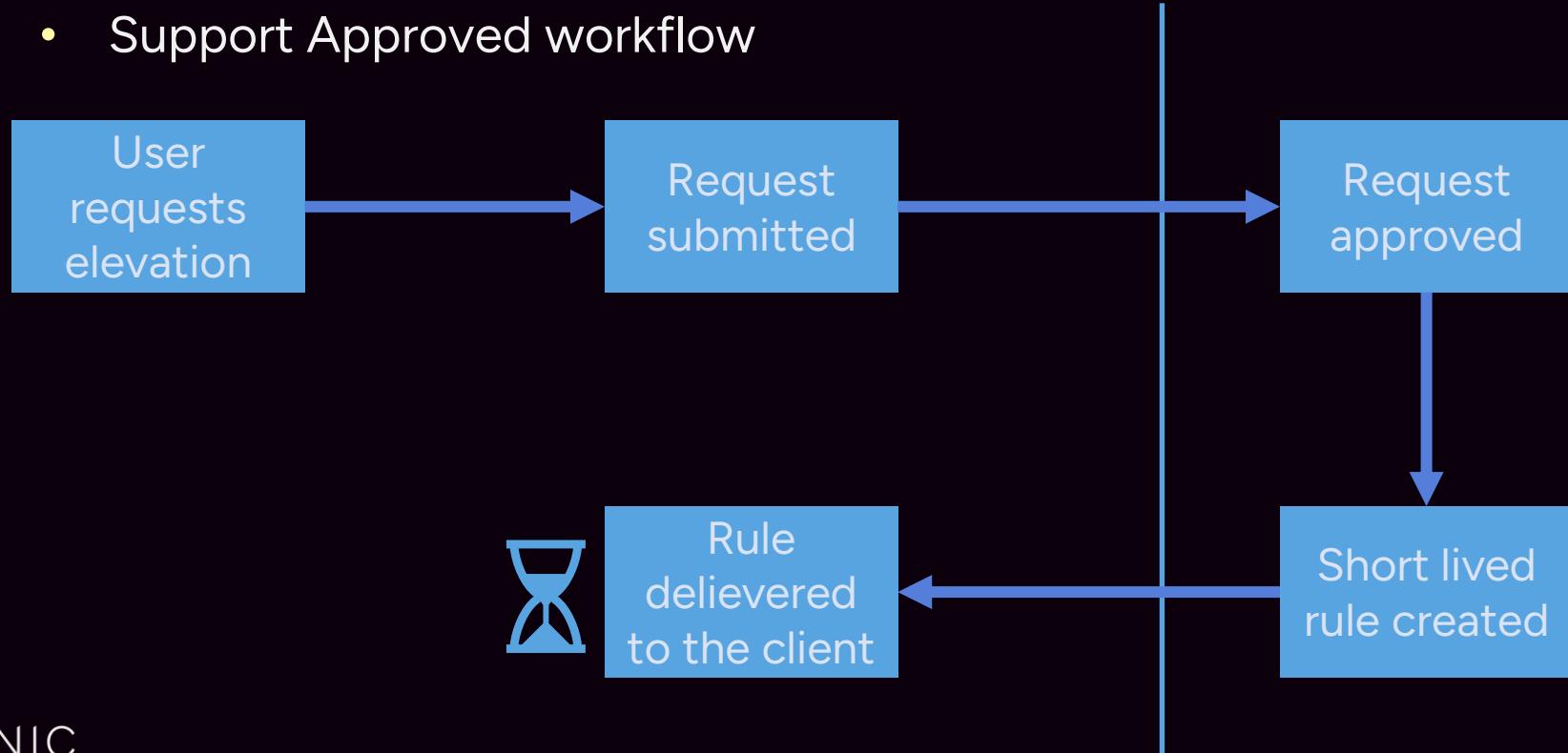
# Endpoint Privilege Management (EPM)

- Support Approved workflow



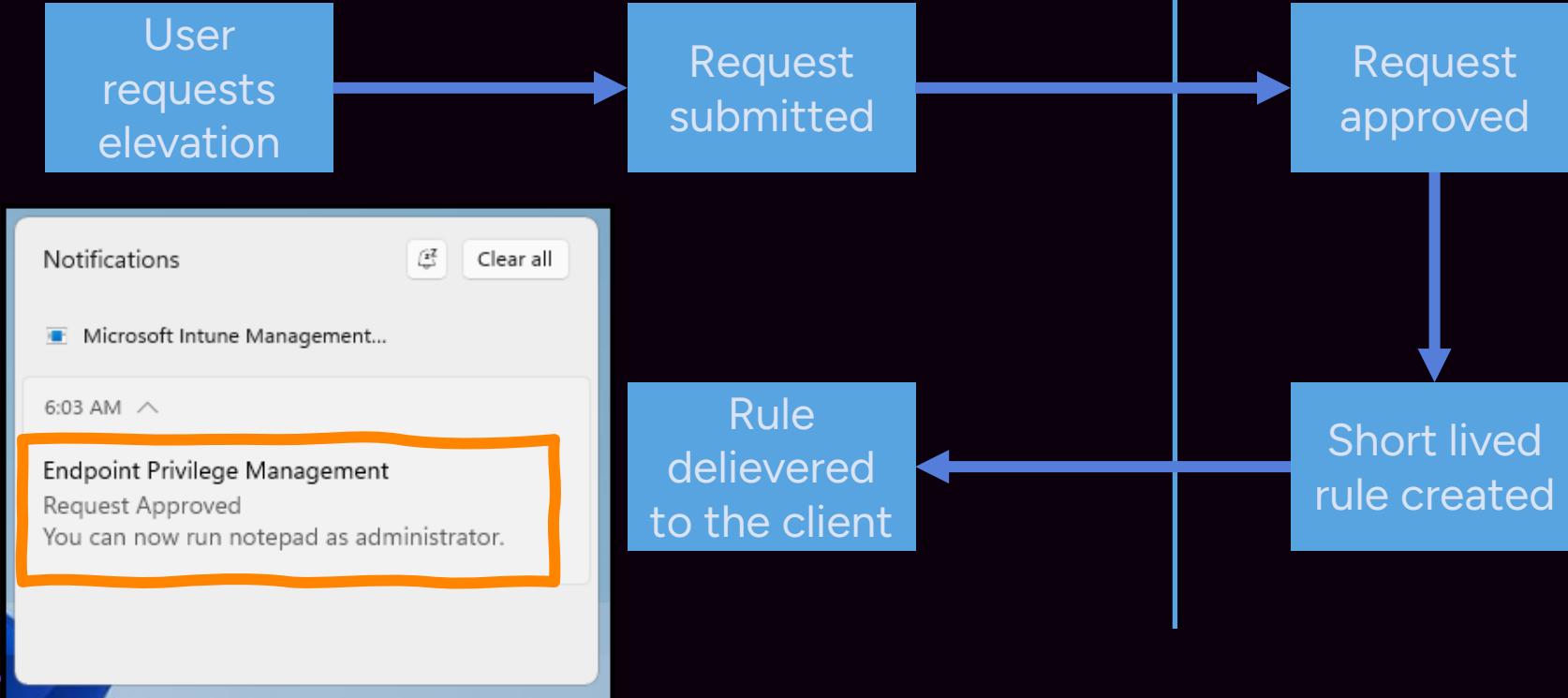
# Endpoint Privilege Management (EPM)

- Support Approved workflow



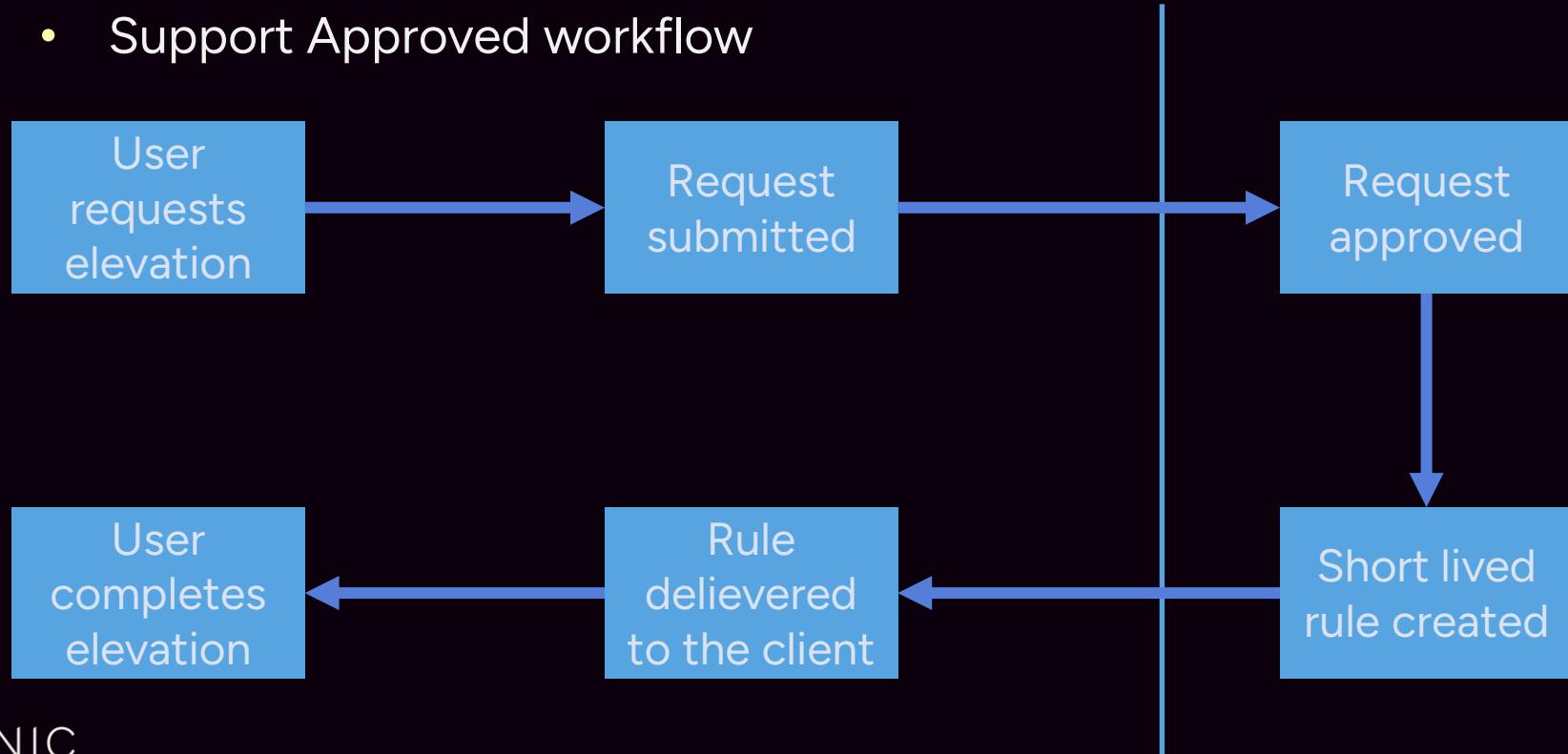
# Endpoint Privilege Management (EPM)

- Support Approved workflow



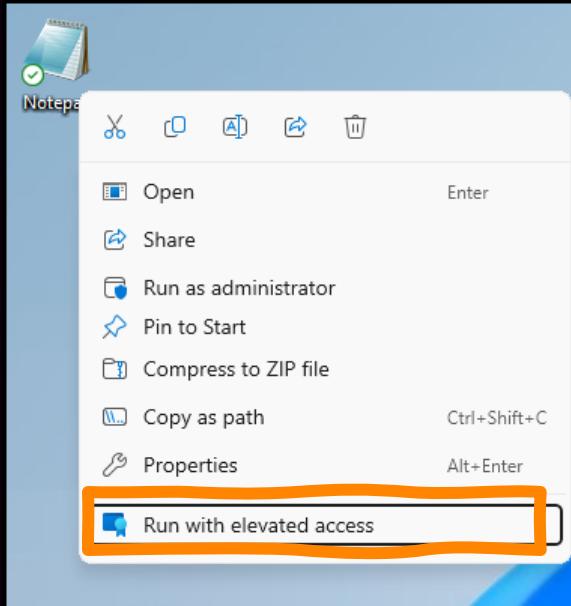
# Endpoint Privilege Management (EPM)

- Support Approved workflow



# Endpoint Privilege Management (EPM)

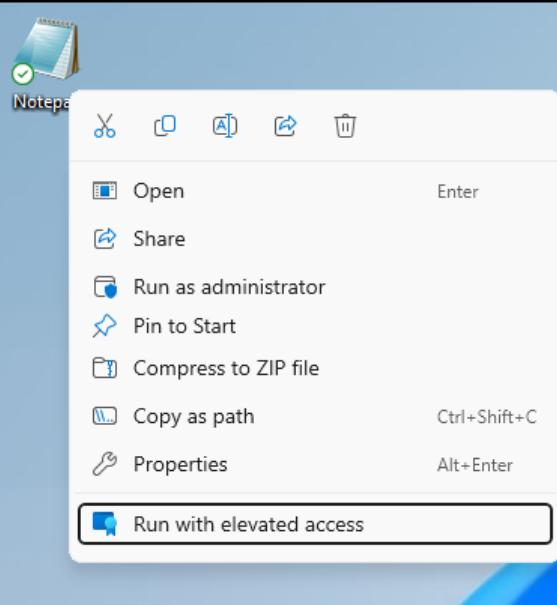
- Support Approved workflow



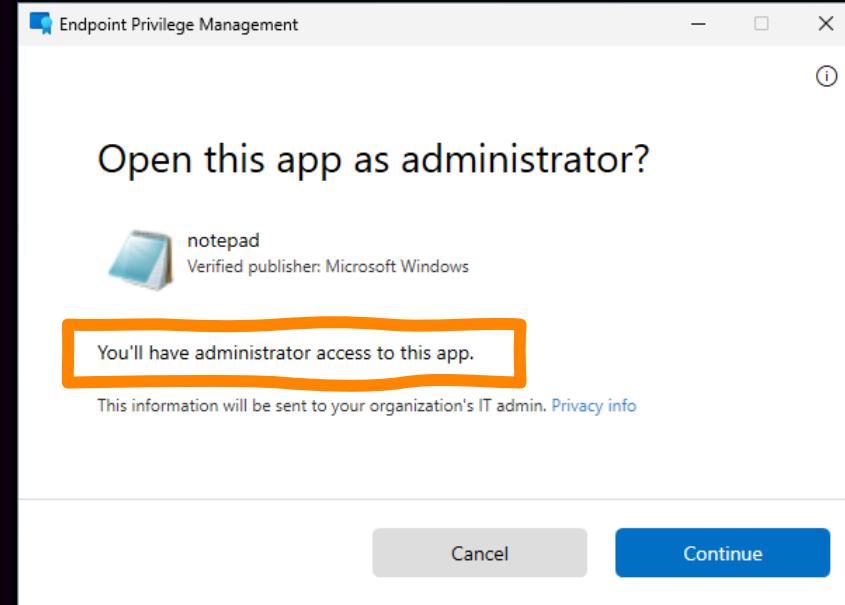
User completes elevation

# Endpoint Privilege Management (EPM)

- Support Approved workflow



User completes elevation



Open this app as administrator?

notepad  
Verified publisher: Microsoft Windows

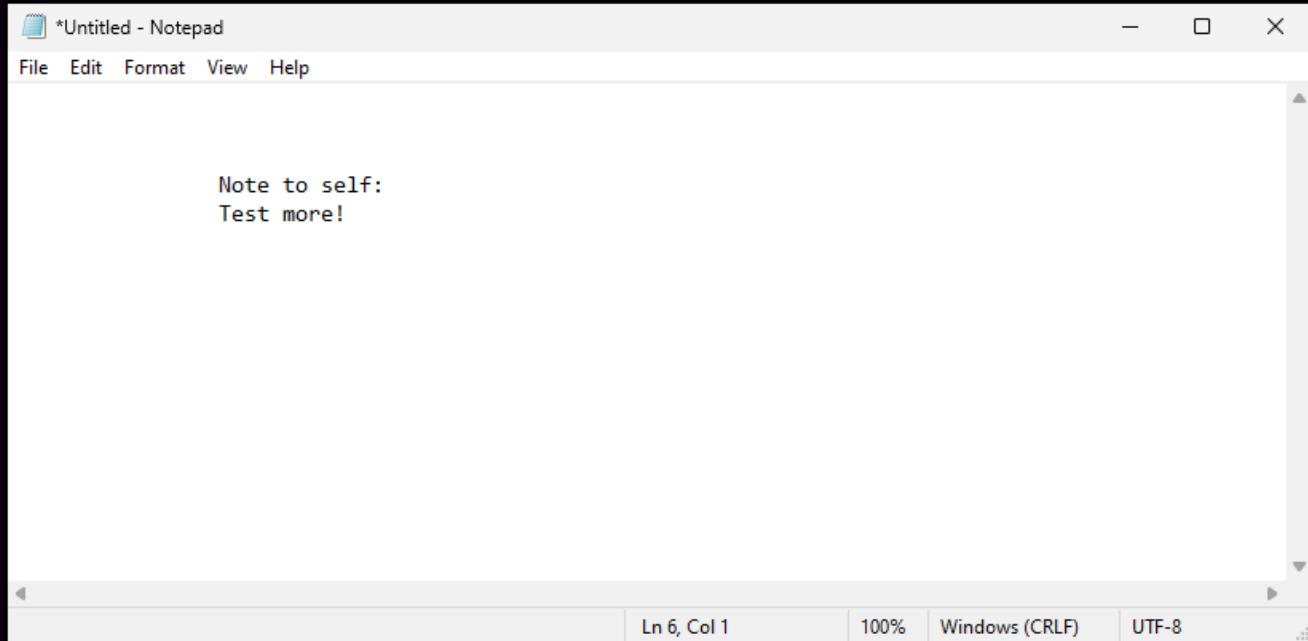
You'll have administrator access to this app.

This information will be sent to your organization's IT admin. [Privacy info](#)

Cancel Continue

# Endpoint Privilege Management (EPM)

- Support Approved workflow



User  
completes  
elevation

# Endpoint Privilege Management (EPM)

- Support Approved workflow



# Endpoint Privilege Management (EPM)

- Support Approved

Rudyooms · 50 min. ago

When you are elevating a process with epm, the process is launched in a different context and am account. This is a virtual account which isn't the same user ...

<https://call4cloud.nl/2023/05/the-virtual-account-that-rocks-the-epm/>

3

Reply Share ...

Note to self:  
Test more!

r/MSIntune · Posted by u/tariklehaine 1 hour ago

Testing Endpoint Privilege Management and allot of problems with VS Code and CMD?

Issues & Bugs

Hi all, we recently started implementing EPM within our own company. Everything went pretty well while testing, however now we have deployed EPM also to our developers they started having allot of problems

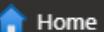
Windows (CRLF) UTF-8



Home &gt; Endpoint security



# Endpoint security | Endpoint Privilege Management



Home



Dashboard



All services



Devices



Apps



Endpoint security



Reports



Users



Groups



Tenant administration



Troubleshooting + support

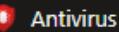


Search

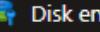


&gt; Overview

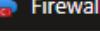
Manage



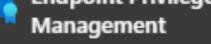
Antivirus



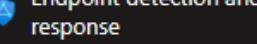
Disk encryption



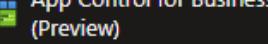
Firewall



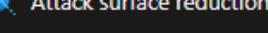
Endpoint Privilege Management



Endpoint detection and response



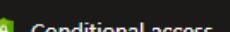
(Preview)



Attack surface reduction



Account protection



Device compliance



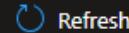
Conditional access

Reports

Policies

Reusable settings

Elevation requests



Search

Status == all

File ↑↓

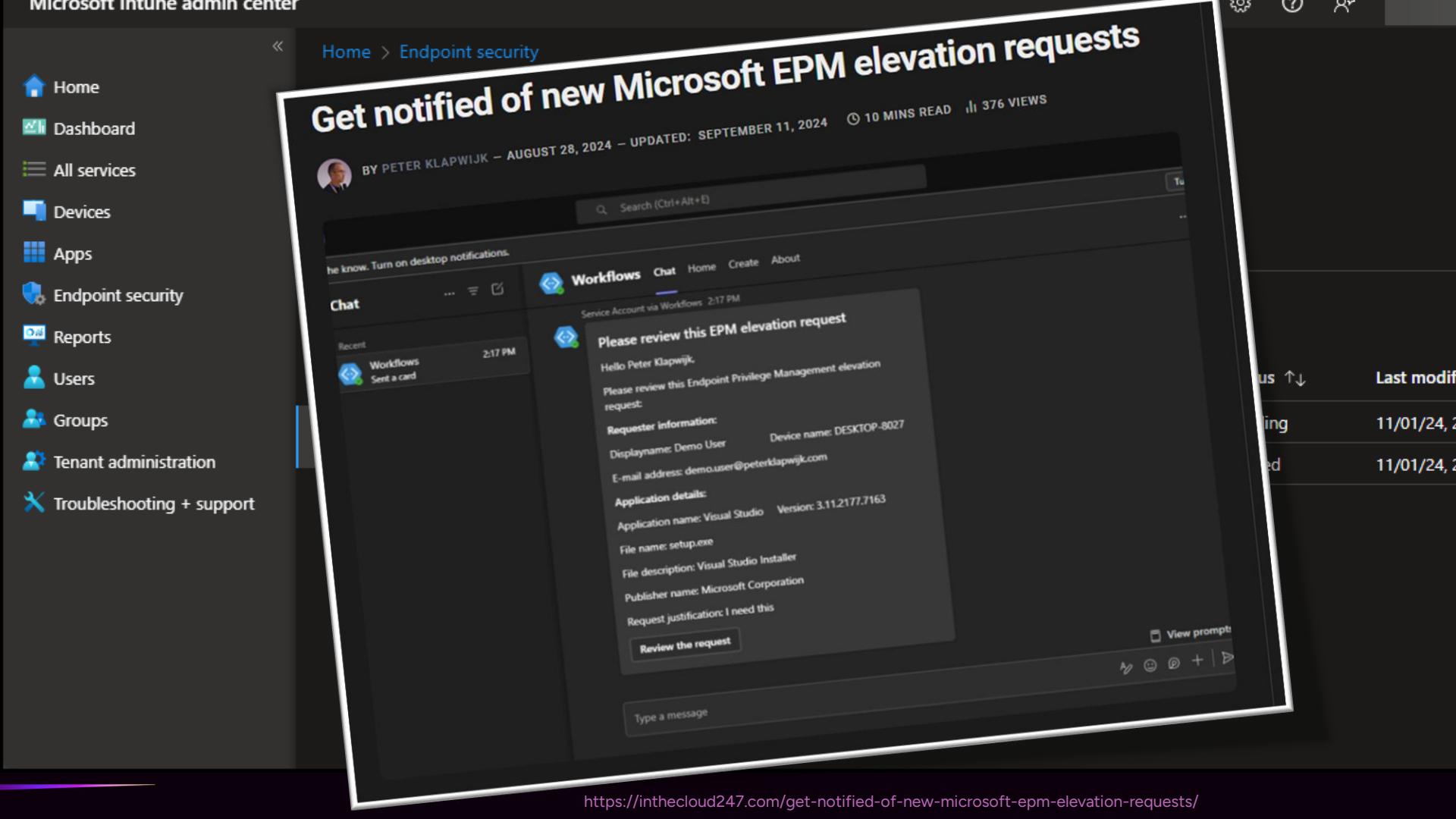
Publisher ↑↓

Username ↑↓

Status ↑↓

Last modified

7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Pending	11/01/24, 2
7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Denied	11/01/24, 2





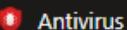
Home &gt; Endpoint security

## Endpoint security | Endpoint Privilege

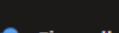
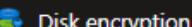
 Search

&gt; Overview

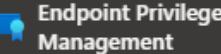
Manage



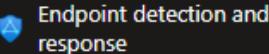
Antivirus



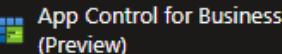
Firewall



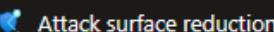
Endpoint Privilege Management



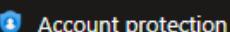
Endpoint detection and response



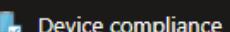
App Control for Business (Preview)



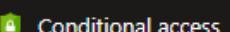
Attack surface reduction



Account protection



Device compliance

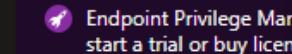


Conditional access

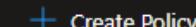
Reports

Policies

Re



start a trial or buy licens



Create Policy



Ref



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: endpointPrivilegeManagement devices

Create



# 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

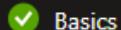
Windows

[Previous](#)[Next](#)

[Home](#) > [Endpoint security | Endpoint Privilege Management](#) >

## Create profile

Elevation rules policy



Basics



Configuration settings



Scope tags



Assignments



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.

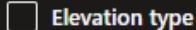


Add



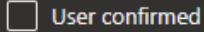
Delete

Elevation Rule Name



Elevation type

Rule name



User confirmed

Configure settings

[+ Edit instance](#)[Previous](#)[Next](#)

## 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 + E

The field for Rule name is required.

## 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](#)

[Previous](#)[Next](#)[Save](#)

## Create profile

Elevation rules policy

✖ Please review policy.✓ Basics✖ Configuration settings③ Scope tags④ 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.

## 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

Require rule to elevate

Child process behavior \*

### File information

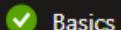
Using the principle of least privilege, provide properties that apply to apps you want to let have elevated privileges. If the rule is too broad, unintended elevations. [Learn more about elevation rules](#)

PreviousNextSave

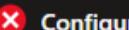
## Create profile

Elevation rules policy

Please review policy.



Basics



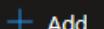
Configuration settings



Scope tags

### Privilege Management

Elevation Rules set the conditions for allowing users to get just

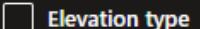


Add



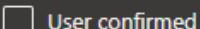
Delete

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

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

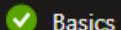
Tenant administration

Troubleshooting + support

## Create profile

Elevation rules policy

Please review policy.



Basics



Configuration settings



Scope tags

### Privilege Management

Elevation Rules set the conditions for allowing users to get just

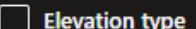


Add



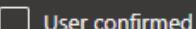
Delete

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 the apps you want to let have elevated privileges. If the rule is too broad, the unintended elevations. [Learn more about elevation rules](#)

File name

File path

Signature source

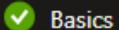
Upload a certificate file

Save

## Create profile

Elevation rules policy

Please review policy.



Basics



Configuration settings



Scope tags

### Privilege Management

Elevation Rules set the conditions for allowing users to get just

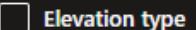


Add



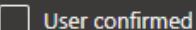
Delete

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 the apps you want to let have elevated privileges. If the rule is too broad, the unintended elevations. [Learn more about elevation rules](#)

File name

File path

Signature source

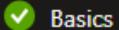
Upload a certificate file

Save

## Create profile

Elevation rules policy

Please review policy.



Basics



Configuration settings



Scope tags

### Privilege Management

Elevation Rules set the conditions for allowing users to get just

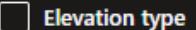


Add



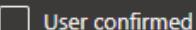
Delete

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 the apps you want to let have elevated privileges. If the rule is too broad, the unintended elevations. [Learn more about elevation rules](#)

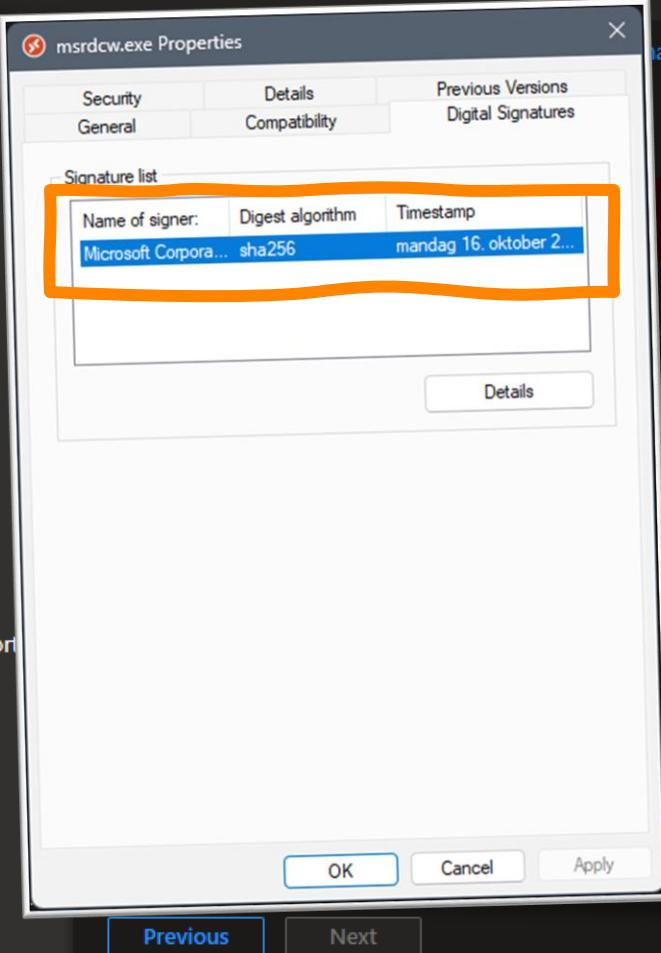
File name

File path

Signature source

Upload a certificate file

Save



## Rule properties

Elevation rules policy

Child process behavior

Deny all

### File information

Using the principle of least privilege, provide properties that apply to the apps you want to let have elevated privileges. If the rule is too broad, the unintended elevations. [Learn more about elevation rules](#)

Scope tags

ers to get just

name

File name

File path

Signature source

Upload a certificate file

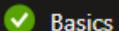
Save

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

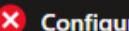
## Create profile

Elevation rules policy

Please review policy.



Basics



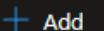
Configuration settings



Scope tags

### Privilege Management

Elevation Rules set the conditions for allowing users to get just

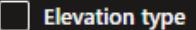


Add



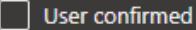
Delete

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

https://intune.microsoft.com/..VIEW/microsoft\_intune\_Workflows/SettingCatalog...      

One admin center 

Home > Endpoint security | Endpoint Privilege Management <

## Create profile

Elevation rules policy

 Please review policy.

 Basics  Configuration settings 

 Privilege Management

Elevation Rules set the conditions for allowing users to get just

 Add  Delete Elevation Rule Name

<input type="checkbox"/> Elevation type	Rule name
<input type="checkbox"/> User confirmed	<input type="text" value=""/>

The field for Rule name is required.

Previous  Save

## 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

https://intune.microsoft.com/.. VIEW/microsoft\_intune\_Workflows/SettingCatalog...

ne admin center

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

<input type="checkbox"/> Elevation type	Rule name
<input type="checkbox"/> User confirmed	<input type="text"/>

The field for Rule name is required.

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

Previous Next Save



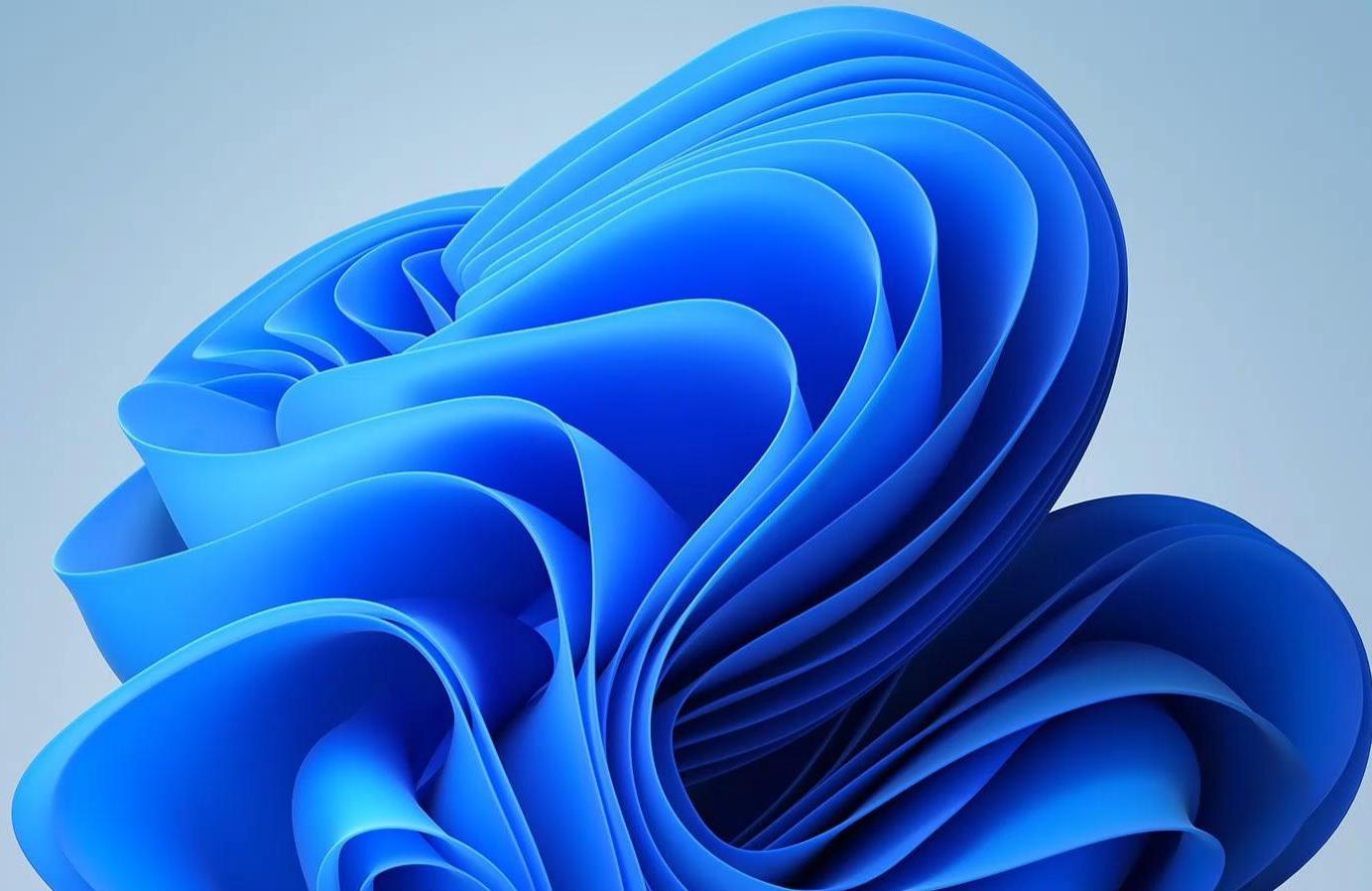
Recycle Bin



Microsoft  
Edge



7-Zip File  
Manager



Search

Simon Does



ENG  
NO



https://intune.microsoft.com/.. View/microsoft\_intune\_Workflows/SettingCatalog...

One admin center

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

<input type="checkbox"/> Elevation type	Rule name
<input type="checkbox"/> User confirmed	<input type="text"/>

The field for Rule name is required.

File name \* 7zFM.exe

File path

Signature source Not configured

File hash \* 1EA0839C8DC95AD2C060AF7D042C✓

Minimum version

File description

Product name

Internal name

Previous Next Save

https://intune.microsoft.com/.. VIEW/microsoft\_intune\_Workflows/SettingCatalog...

One admin center

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

Home > Endpoint security | Endpoint Privilege Management <

## Create profile

Elevation rules policy

Basics Configuration settings Scope tags Assignments 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 Elevation Rule Name

<input type="checkbox"/> Elevation type	Rule name	Configure settings
<input type="checkbox"/> User confirmed	7Zip	+ Edit instance

Previous Next

https://intune.microsoft.com/#/VIEW/microsoft\_intune\_Workflows/SettingCatalog...      

One admin center 

Home > Endpoint security | Endpoint Privilege Management

## Create profile

Elevation rules policy

Basics Configuration settings Scope tags Assignments 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

https://intune.microsoft.com/..VIEW/microsoft\_intune\_Workflows\_SecurityManage...

ne admin center

Home > Endpoint security

## Endpoint security | Endpoint Privilege Management

Search

Reports Policies Reusable settings

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Create Policy Refresh Export

Search by profile name

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

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

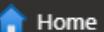
admin@M365x7391006... SIMON DOES (M365X73910067.O...)



Home &gt; Endpoint security



# Endpoint security | Endpoint Privilege Management



Home



Dashboard



All services



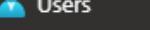
Devices



Apps



Endpoint security



Reports



Users



Groups



Tenant administration



Troubleshooting + support

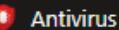


Search

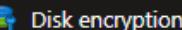


&gt; Overview

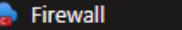
Manage



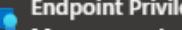
Antivirus



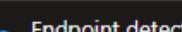
Disk encryption



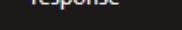
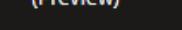
Firewall



Endpoint Privilege Management



Endpoint detection and response

(Preview)  
App Control for Business

Attack surface reduction



Account protection



Device compliance



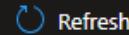
Conditional access

Reports

Policies

Reusable settings

Elevation requests



Search

Status == all

File ↑↓

Publisher ↑↓

Username ↑↓

Status ↑↓

Last modified

7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Approved	11/01/24, 2024
7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Denied	11/01/24, 2024

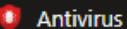
Home &gt; Endpoint security

# Endpoint security | Endpoint

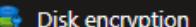
 Search

&gt; Overview

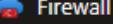
Manage



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
-----------	------------------------

Home &gt; Endpoint security

# Endpoint security | Endpoint

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

Search

&gt; 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

## 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

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home &gt; Endpoint security

# Endpoint security | Endpoint

Search

Reports

&gt; 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

## 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



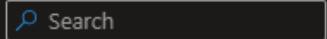
Home &gt; Endpoint security



# Endpoint security | Endpoint Privilege Management

Policy created

Policy "EPM002 - 7ZIP File Manager Elevation Rule" created successfully



Reports

Policies

Reusable settings

Elevation requests



Status == all

File ↑↓	Publisher ↑↓	Username ↑↓	Status ↑↓	Last modified
7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Approved	11/01/24, 2024
7zFM.exe	UnknownPublisher	leo.fender@skotheimsvik....	Denied	11/01/24, 2024

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



Home &gt; Endpoint security



# Endpoint security | Endpoint Privilege Management

 Search

Reports

**Policies**

Reusable settings

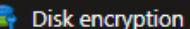
Elevation requests

&gt; Overview

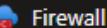
Manage



Antivirus



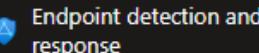
Disk encryption



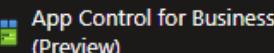
Firewall



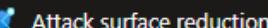
Endpoint Privilege Management



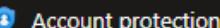
Endpoint detection and response



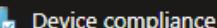
App Control for Business (Preview)



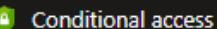
Attack surface reduction



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 Admin can start a trial or buy licenses.

[Create Policy](#) [Refresh](#) [Export](#) Search by profile name

Policy name	Policy type	Assign...	Platform	Target
EPM001 - Elevation Settings Policy	Elevation settings po...	Yes	Windows	MDM
EPM002 - 7ZIP File Manager Elevation I	Elevation rules policy	No	Windows	endpo



Home &gt; Endpoint security



## Endpoint security | Endpoint Privilege Management



Home



Dashboard



All services



Devices



Apps



Endpoint security



Reports



Users



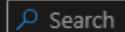
Groups



Tenant administration



Troubleshooting + support

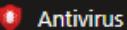


Search

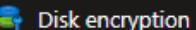


&gt; Overview

Manage



Antivirus



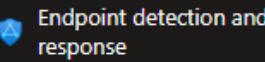
Disk encryption



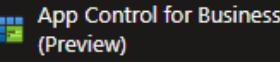
Firewall



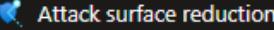
Endpoint Privilege Management



Endpoint detection and response



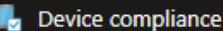
App Control for Business (Preview)



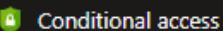
Attack surface reduction



Account protection



Device compliance



Conditional access

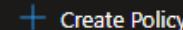
Reports

Policies

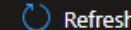
Reusable settings

Elevation requests

Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Admin can start a trial or buy licenses.



Create Policy



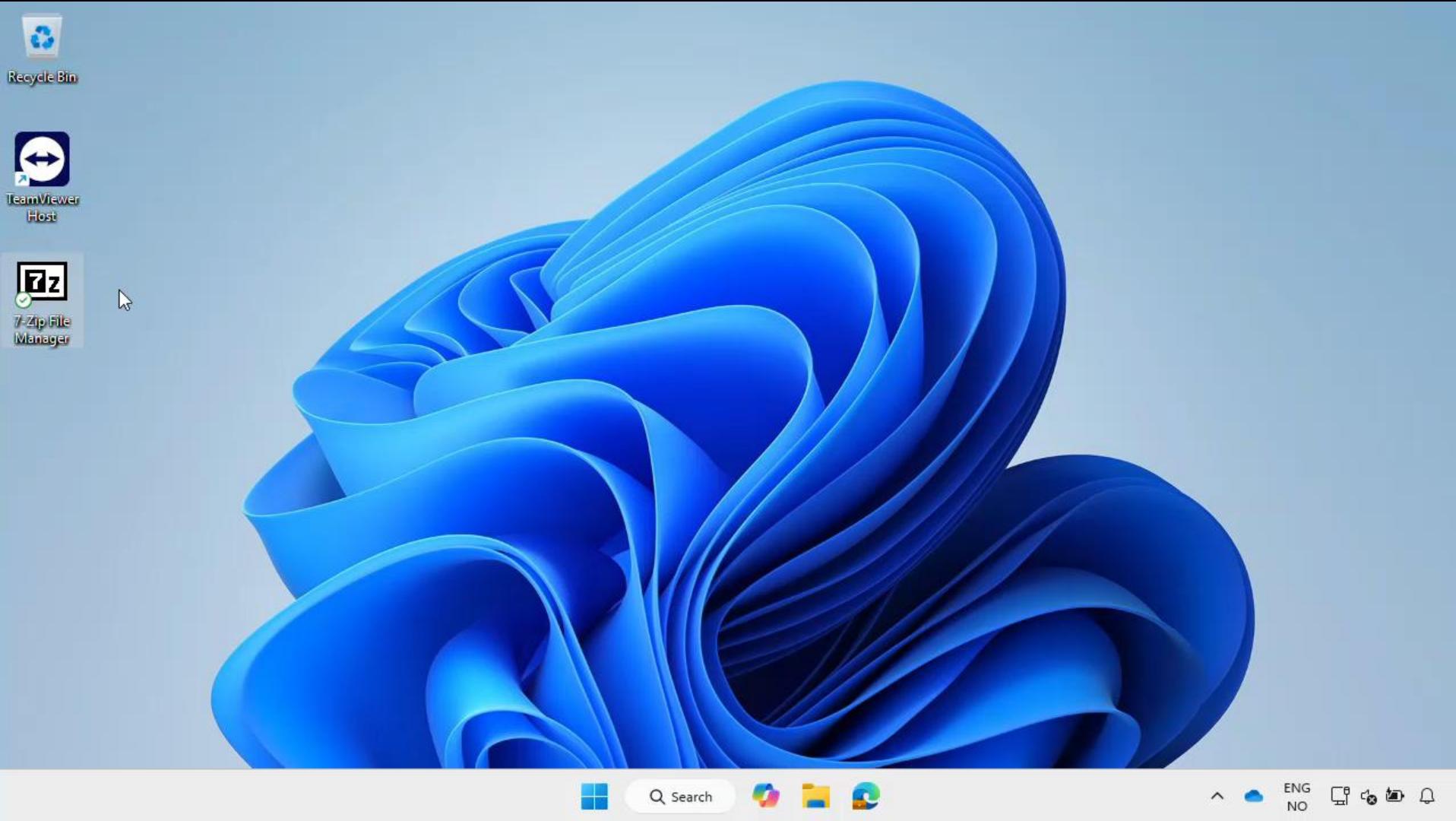
Refresh



Export

Search by profile name

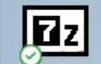
Policy name	Policy type	Assign...	Platform	Target
FPM001 - Elevation Settings Policy	Elevation settings policy	Yes	Windows	MDM
EPM002 - 7ZIP File Manager Elevation	Elevation rules policy	No	Windows	endpoint



Recycle Bin



TeamViewer  
Host



7-Zip File  
Manager



Search



ENG  
NO



https://intune.microsoft.com/..VIEW/microsoft\_intune\_Workflows\_SecurityManage...

ne admin center

Home > Endpoint security

## Endpoint security | Endpoint Privilege Management

Search

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	Platform
EPM001 - Elevation Settings Policy	Elevation settings policy	Yes	Windows
EPM002 - 7Zip File Manager Elevation Rule	Elevation rules policy	Yes	Windows

Navigation sidebar:

- Overview
- All devices
- Security baselines
- Security tasks
- Manage
- Antivirus
- Disk encryption
- Firewall
- Endpoint Privilege Management
- Endpoint detection and response
- App Control for Business (Preview)



## Endpoint security | Endpoint Privilege Management



Reports

Policies

Reusable settings

### 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

### 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



«

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

One admin center

https://intune.microsoft.com/... View / Microsoft Intune Workbooks / Privileged Elevation

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

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
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe	Igor Pavlov	User-confirmed	Completed

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

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

One admin center

https://intune.microsoft.com/... View | Microsoft Intune Workbooks / Privileged Elevation

Home > Endpoint security | Endpoint Privilege Management > Endpoint elevation report

## Endpoint elevation report

This table includes elevations that are managed by specific rules and those that are triggered by user actions.

Refresh Columns Export

Search Type == all Date > 2024-03-01

User name	Device	File name
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe

## 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

One admin center

https://intune.microsoft.com/ /view/Microsoft\_Intune\_Worksheets/PrivilegeManagement...     

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

Home > Endpoint security | Endpoint Privilege Management > **Elevation detail**

## Endpoint elevation report

This table includes elevations that are managed by specific rules and those that are triggered by specific processes.

Refresh Columns Export

Search Type == all Date > 2023-01-01

User name	Device	File name
AzureAD\SimonSkotheimsvik	LETSDO-41100003	C:\Program Files\7-Zip\7zFM.exe

**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

Search Add filter

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	Microsoft Corporation	Unmanaged	30

Load more

Internal name

7zFM

7-Zip

391006...  
3910067.O...

https://intune.microsoft.com //view/Microsoft\_Intune\_Workflows/Privilegemanag... 891006... 3910067.O...

Microsoft Intune admin center

Microsoft Intune admin center

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
	64	194	194
	0	0	64
	0	20	20

VMConnect.exe 10.0.22621.2500  
pnputil.exe

Internal name 7zFM

# 7 HOW? Can we do stuff?

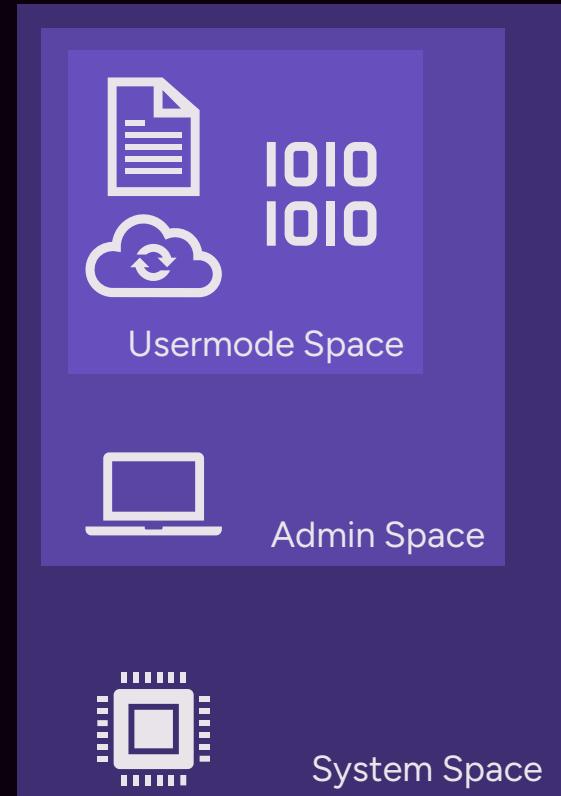
8

HOW?

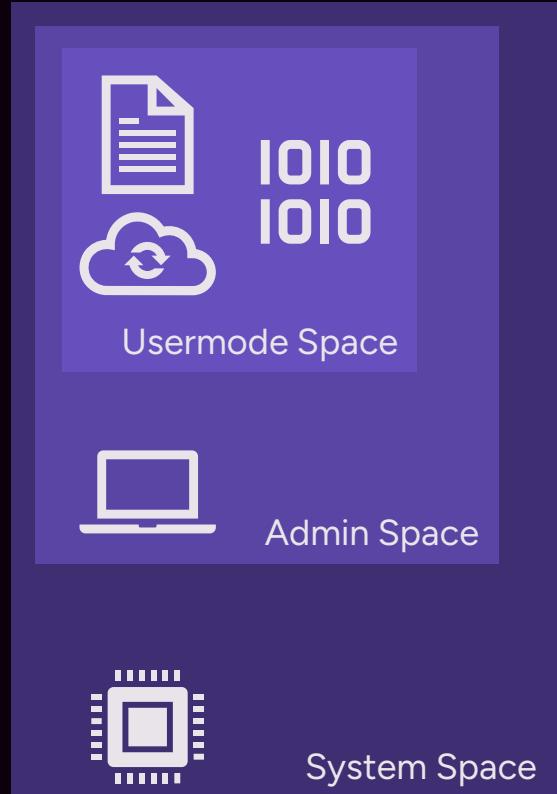
Can we do stuff?

Embrace Modern

# Embrace Modern



# Embrace Modern



8

How?

Can we do stuff?

9

How?

Can we do stuff?

BYODers



9

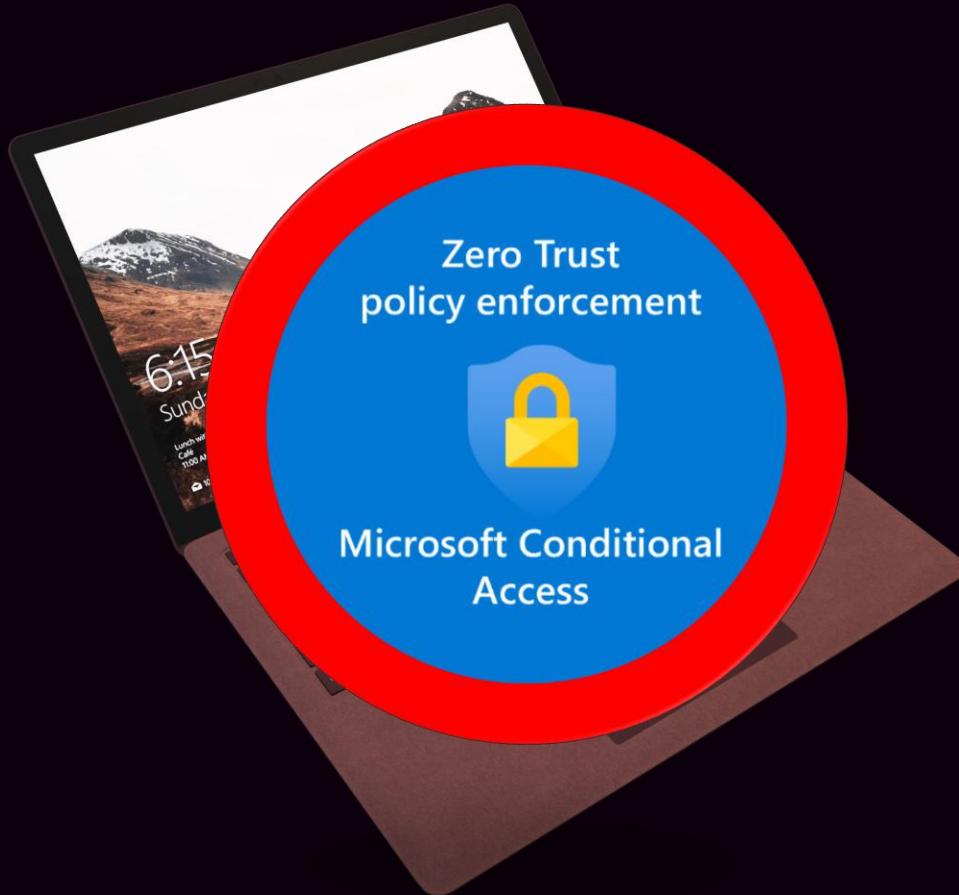
# How?

Can we do stuff?

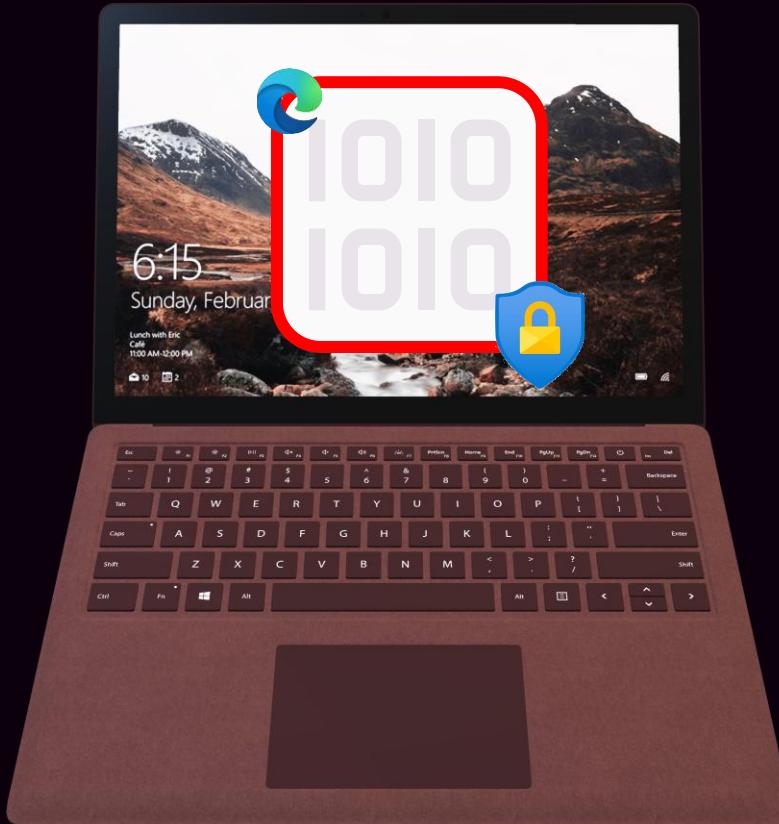
BYODers



# No Access for BYODers?



# MAM Access for BYODers?



# MAM Access for BYODers?

Florian Salzmann Jannik Reinhard

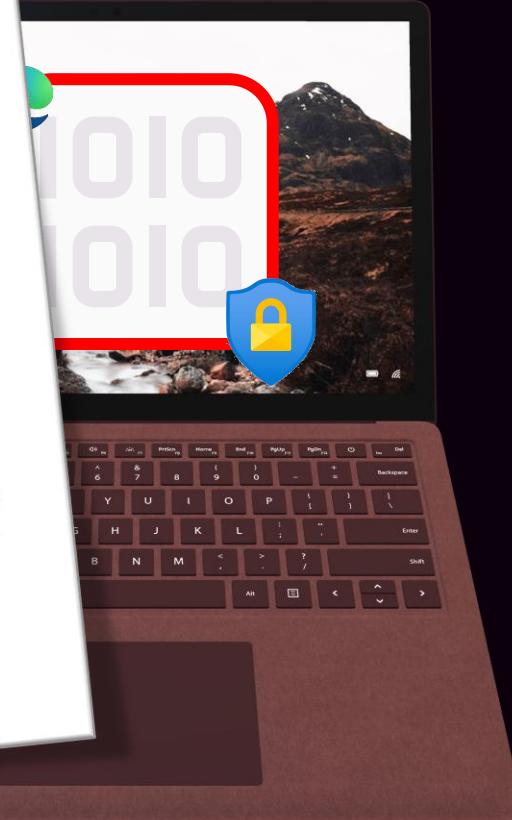
### BYOD Lockdown with MAM & co.

This session will explore securing corporate data on personal devices with a multi-layered approach using Microsoft Intune, Conditional Access, and App-Enforced Restrictions for SharePoint and Exchange Online.

We'll cover:

- Application Protection Policies (MAM): Configure granular security policies for specific applications that access corporate data, such as data encryption, copy/paste control, and selective wiping. Those with a focus on mobile devices.
- App Enforced Restrictions: Block offline access to SharePoint and Exchange Online on your Windows and MacOS devices.
- Conditional Access: Enforce these protection and restriction policies to cover any access to your corporate data.

**SERVER & CLIENT** | Fri 11:10 am - 12:10 pm



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

# Cloud PC for BYODers?



# Cloud PC for BYODers?



Army University continues innovation with mass adoption of remote desktop  
[army.mil](http://army.mil) • 4 min read

NIC  
EMPOWER

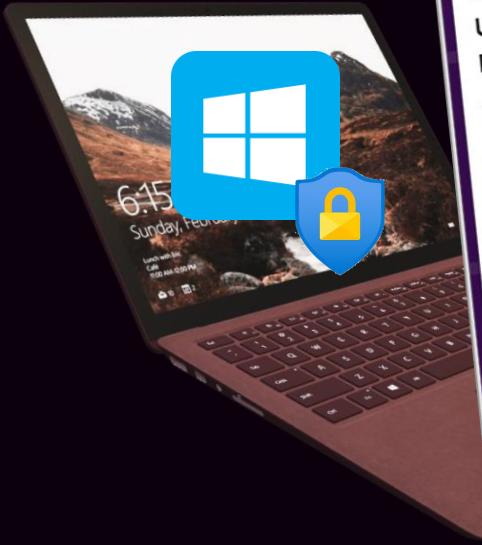
<https://www.azure.microsoft.com/en-us/windows-365>

Now?  
Can we know,  
and trust  
our devices?

# Cloud PC for BYODers?



# 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

Can we know,  
and trust  
our devices?

# CA for BYODers



# CA for BYODers



Conditions!



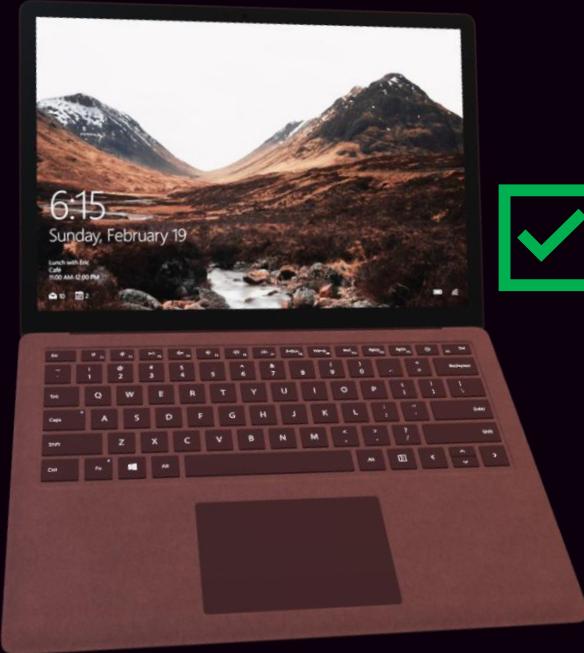
# CA for BYODers



Conditions!



# CA for BYODers



Conditions!



# 10 DON'T BE The Hackers Dream Customer



# 10

# DON'T BE

The Hackers  
Dream Customer

Remove  
LOCAL ADMIN!



# 10

# DON'T BE

The Hackers  
Dream Customer

Remove 

# LOCAL ADMIN!



# Simon Says



Remove  
**LOCAL ADMIN!**



# Thanks for attending!



NIC

E M P O W E R



Secure productivity happens in the cloud

We will help you on your way

website

me

**Simon.Skotheimsvik@TeamCloudWay.com**

twitter (x)

email