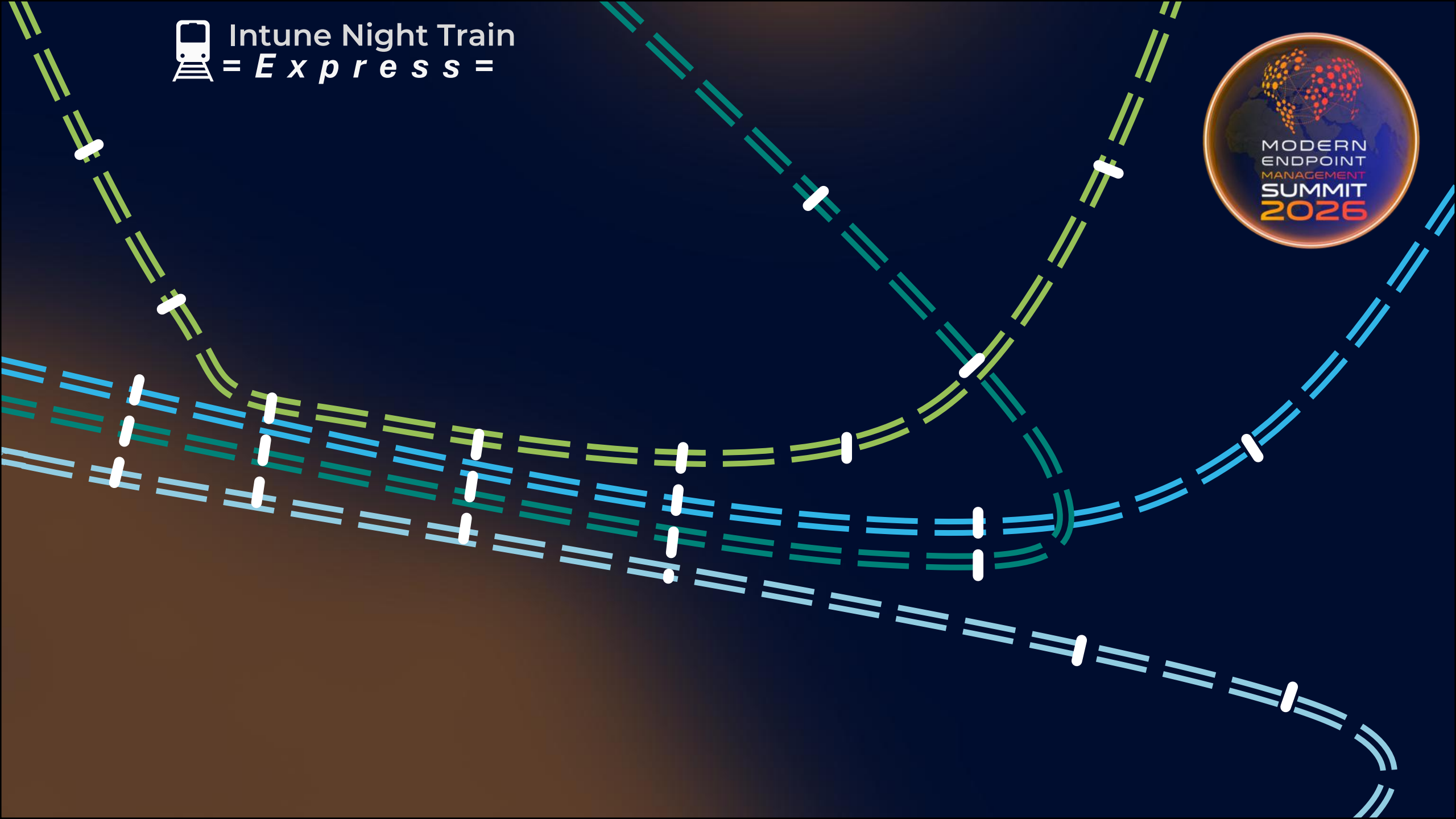
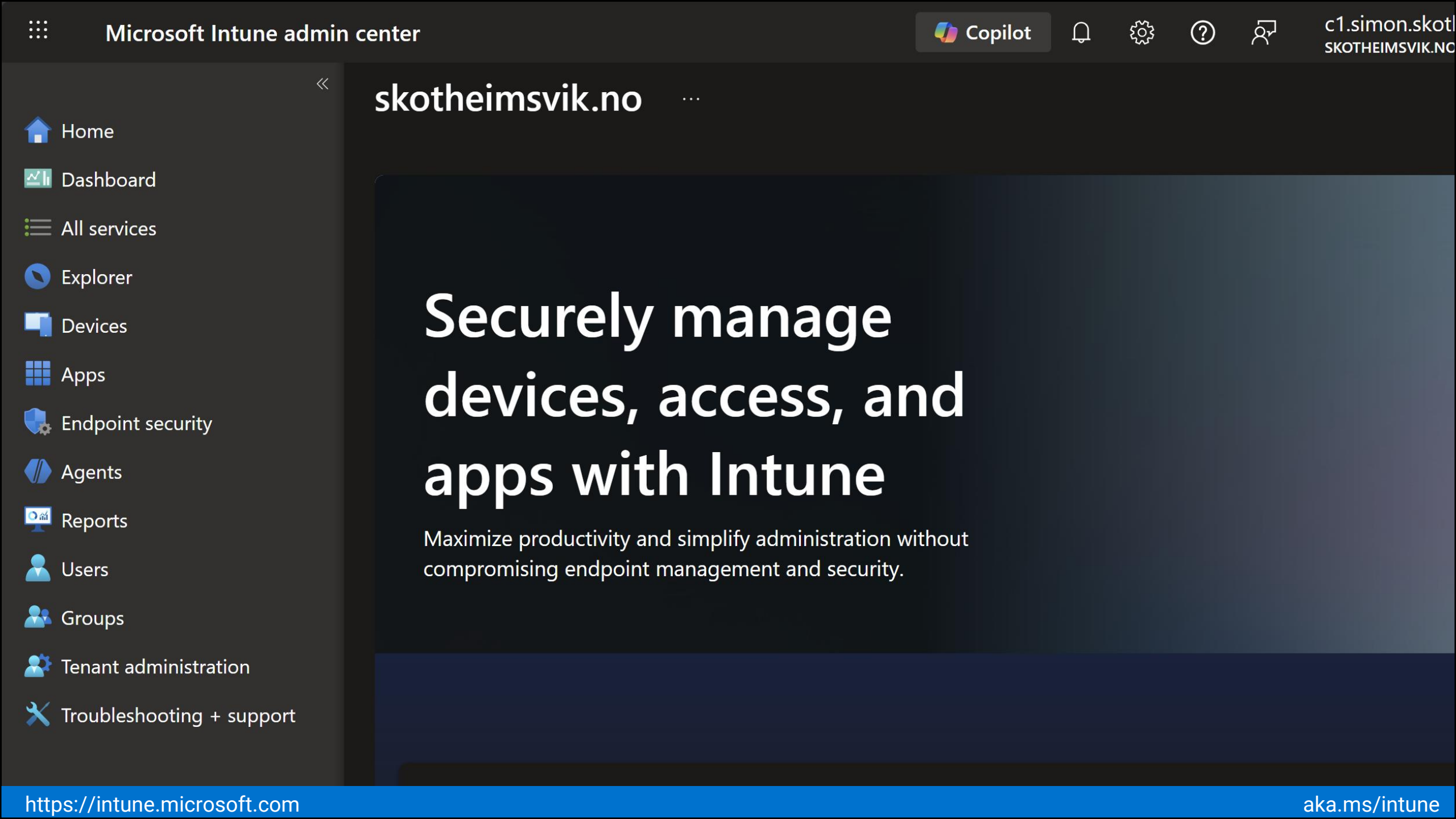
The 2026 Intune Night Train

Your Fast Track to the Future


Intune Night Train
= Express =
MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026


Microsoft Intune admin center
Copilot
c1.simon.skotl
SKOTHEIMSVIK.NO
skotheimsvik.no
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Securely manage devices, access, and apps with Intune
Maximize productivity and simplify administration without compromising endpoint management and security.
https://intune.microsoft.com
aka.ms/intune

But Hey,
I have already
configured Intune…

…during Covid

Copilot

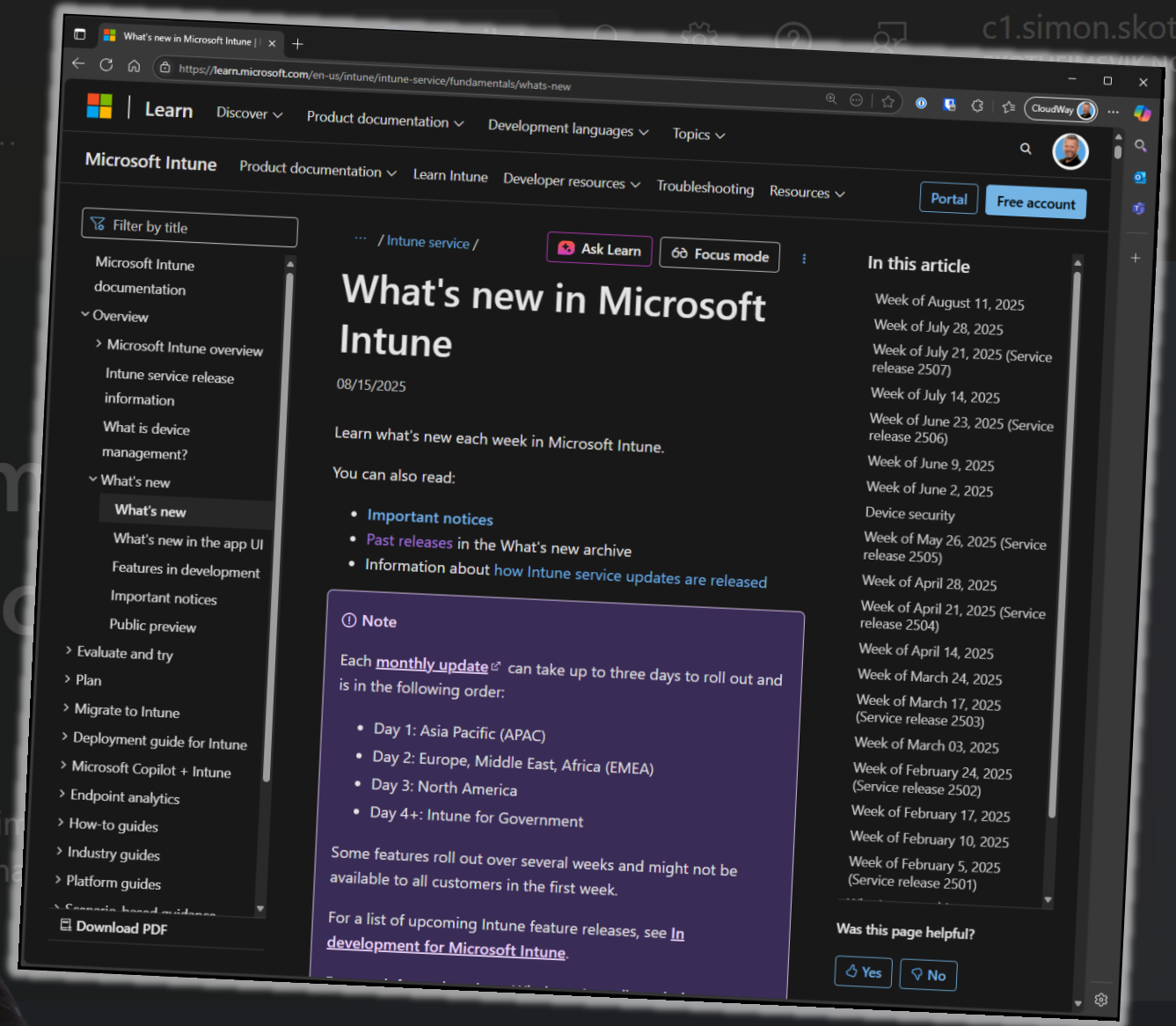
c1.simon.skot
SKOTHEIMSVIK.NO

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

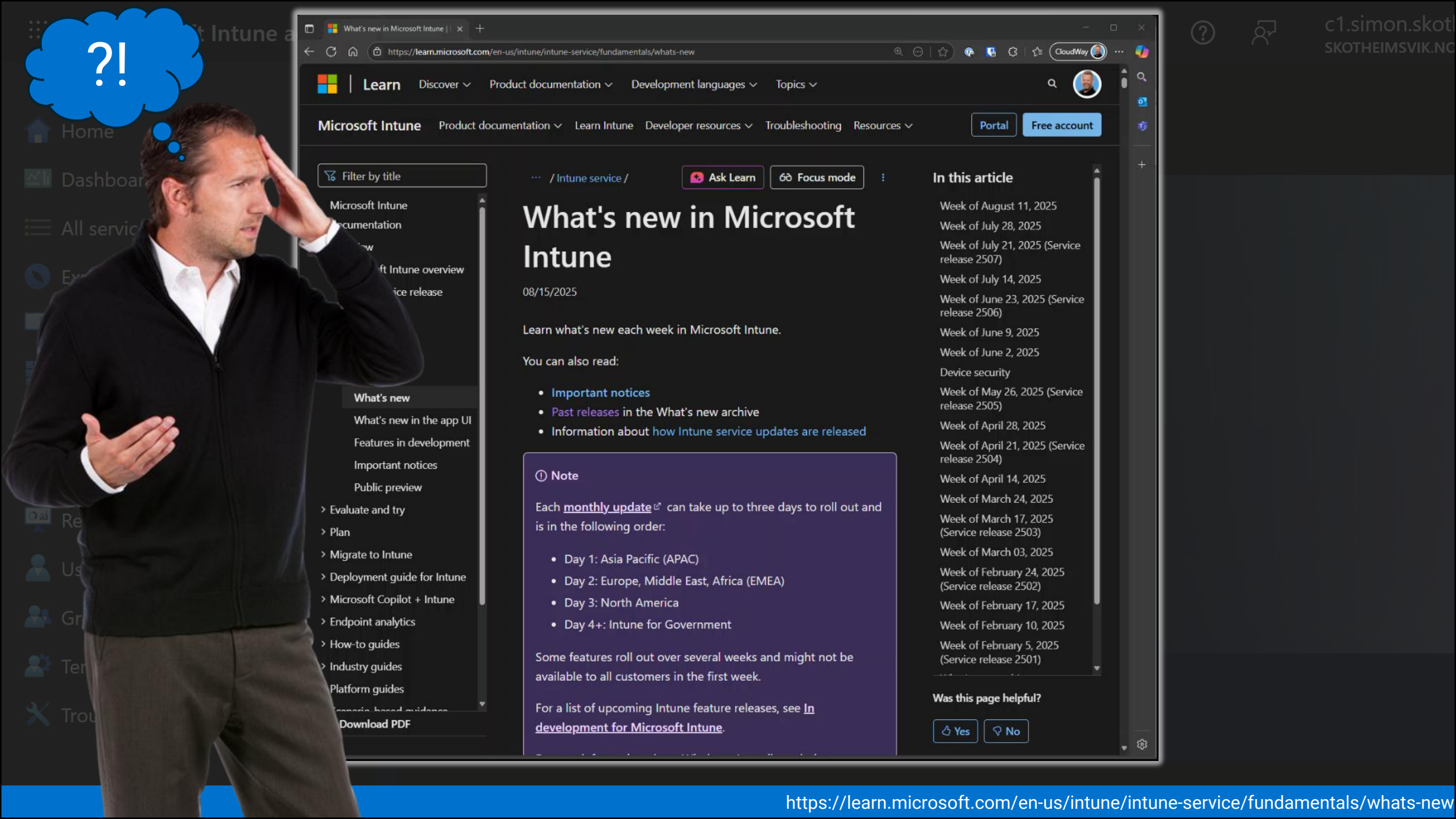
devices,
apps with

Maximize productivity and si
compromising endpoint mana

… and I am using the same licenses, what can have changed?

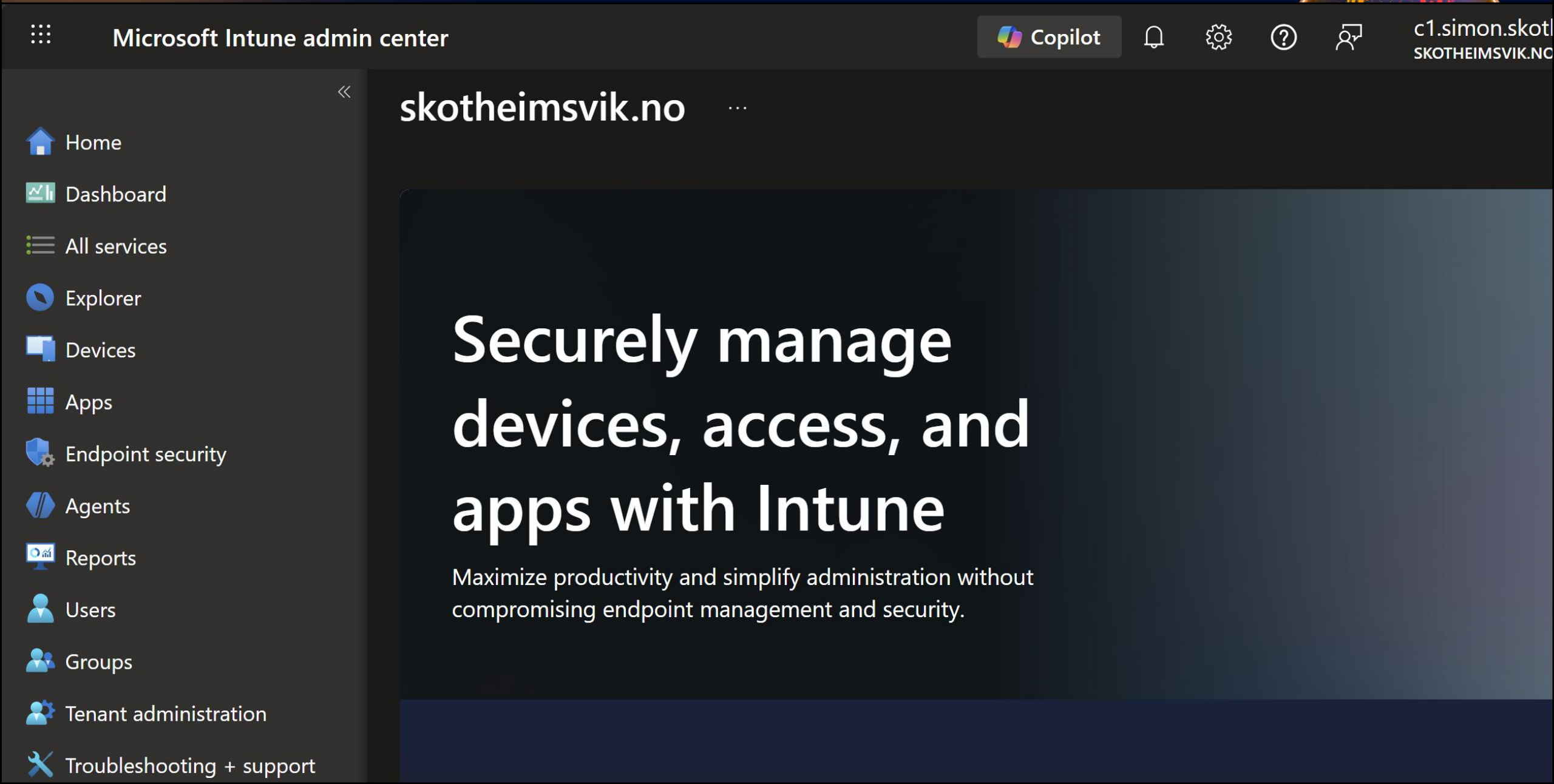


https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new

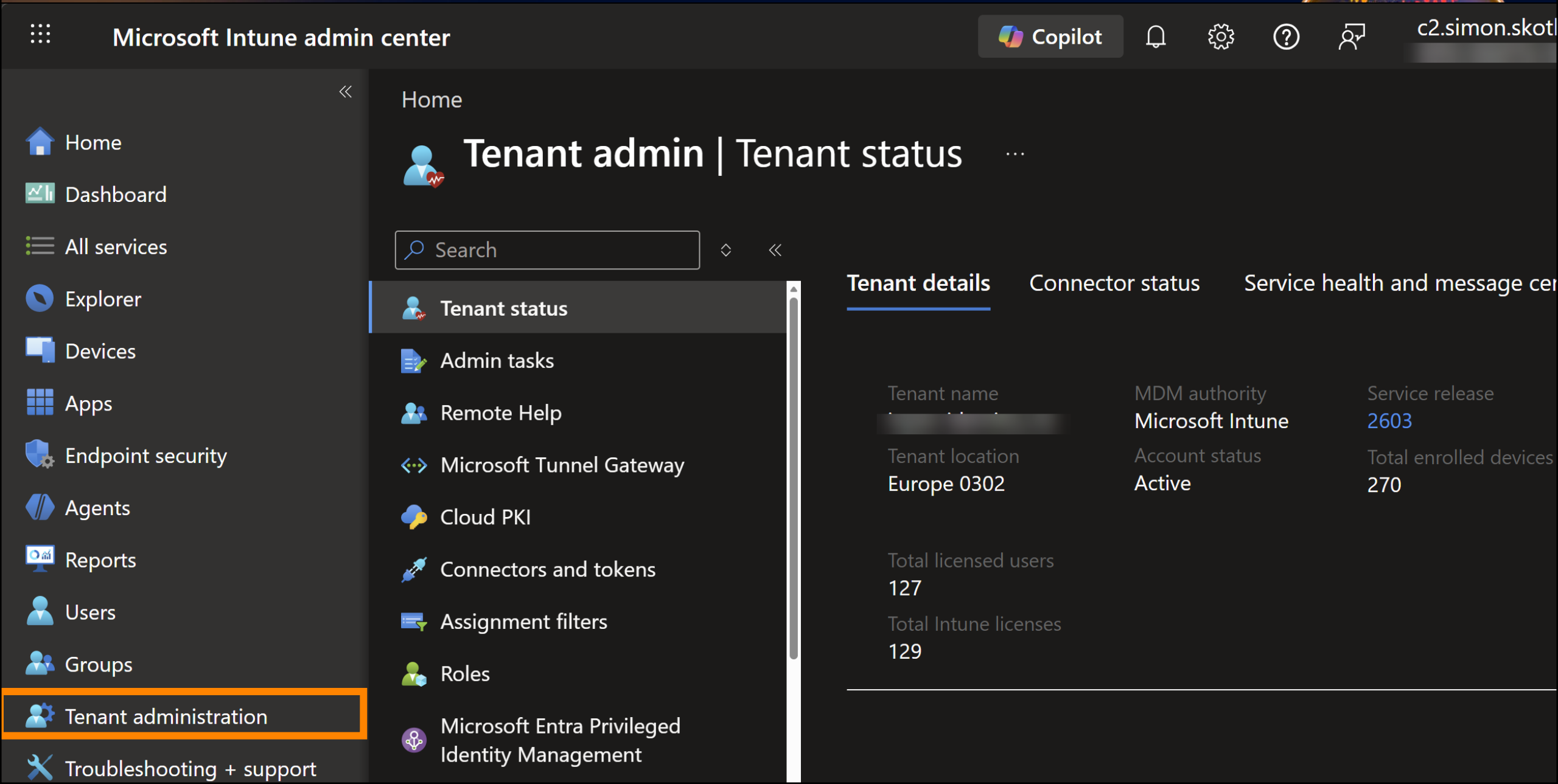


https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new

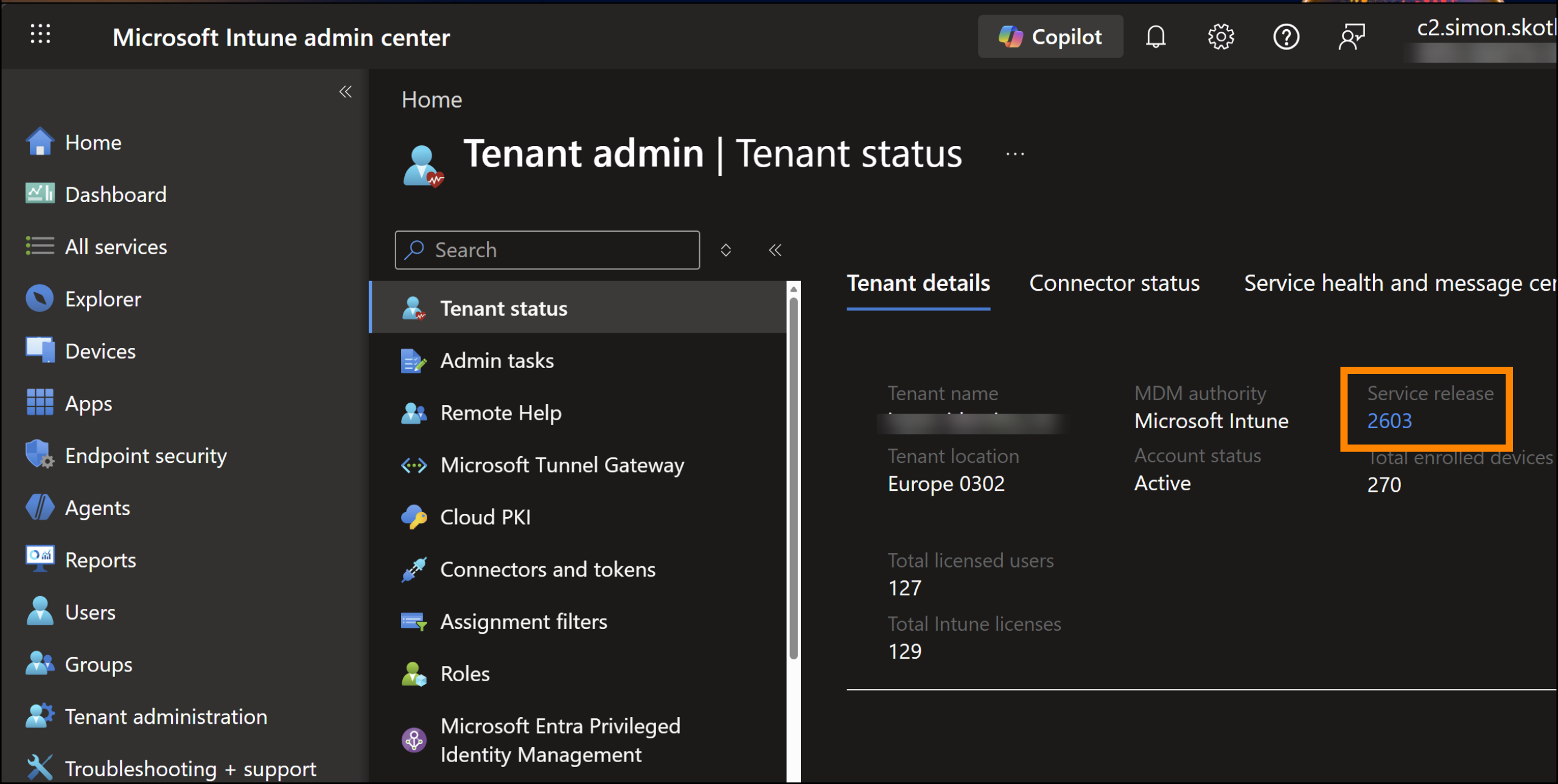
What Intune Version Am I Running?



What Intune Version Am I Running?



What Intune Version Am I Running?



The Locomotives

MODERN ENDPOINT MANAGEMENT

Simon Skotheimsvik
Microsoft MVP

Microsoft® Most Valuable Professional

Role
Senior Cloud Consultant
CloudWay, Norway

CloudWay

Focus
Intune · Entra ID · Security

Hobbies
Blogging, Speaking, Coding
Playing guitars
Three kids
One wife

Entra Cards
Intune Guardian
IntuneFans

linktr.ee/simonskotheimsvik

Jan Ketil Skanke
Microsoft MVP

Microsoft® Most Valuable Professional

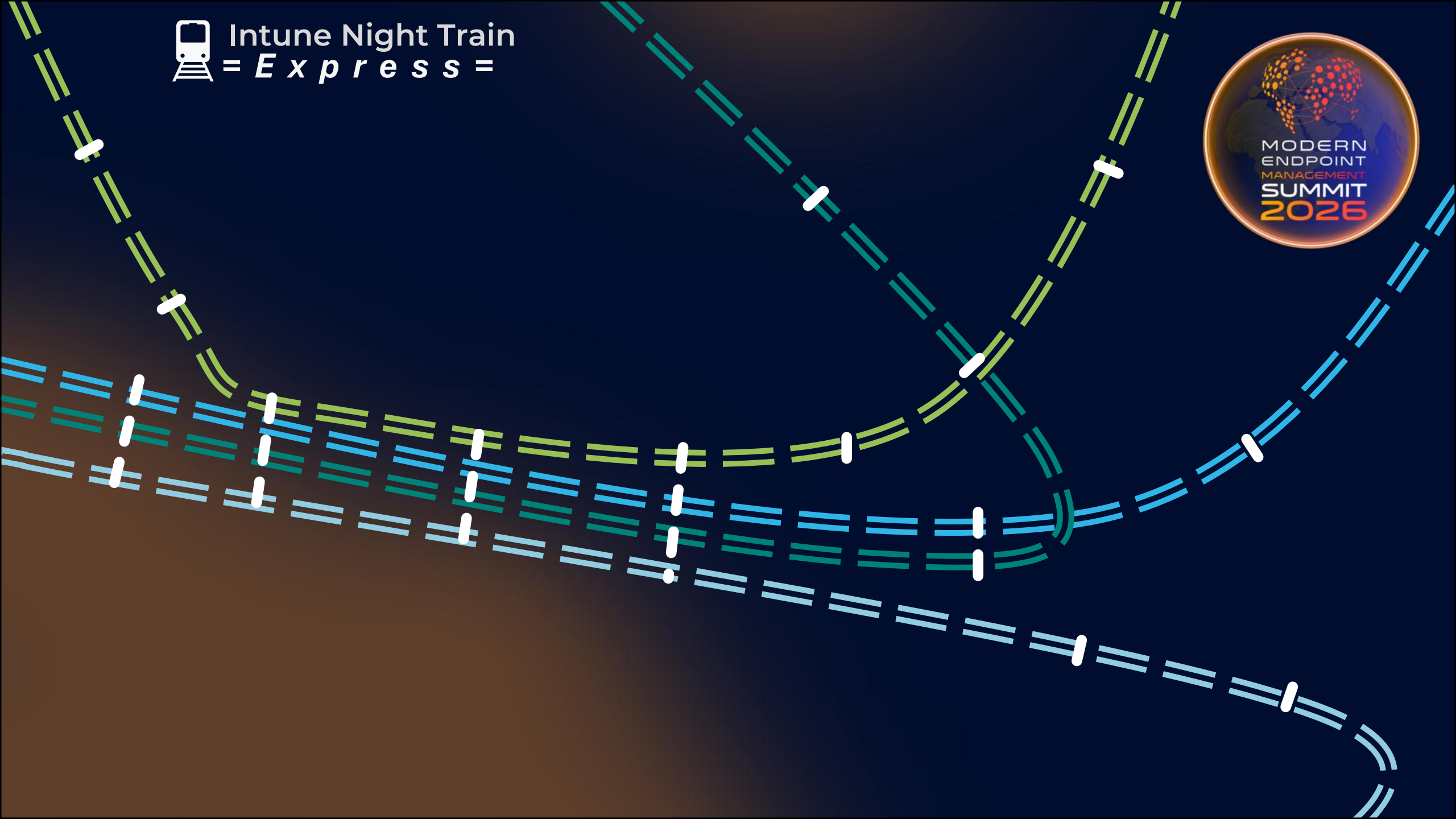
Role
Principal Cloud Architect
CloudWay, Norway

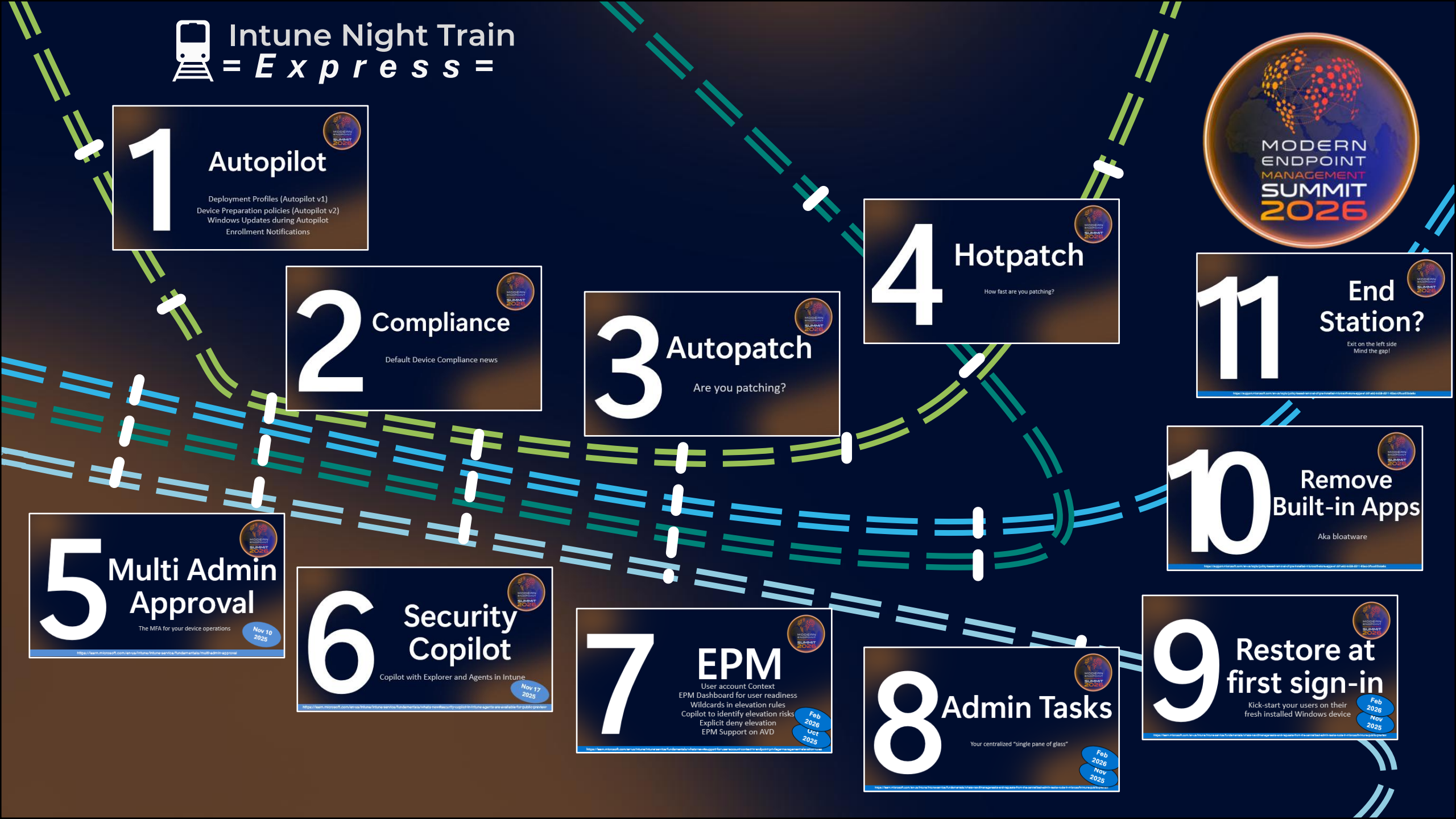
CloudWay

Focus
Intune · Entra ID · Security

Hobbies
Fotball, Formula1, Vibecoding,
Organizing community events

Intune Guardian
PIM Portal
Policy Management Tool


Intune Night Train
= Express =
MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026


Intune Night Train
= E x p r e s s =
MODERN ENDPOINT MANAGEMENT SUMMIT 2026
1
Autopilot
Deployment Profiles (Autopilot v1)
Device Preparation policies (Autopilot v2)
Windows Updates during Autopilot
Enrollment Notifications
2
Compliance
Default Device Compliance news
3
Autopatch
Are you patching?
4
Hotpatch
How fast are you patching?
11
End Station?
Exit on the left side
Mind the gap!
10
Remove Built-in Apps
Aka bloatware
5
Multi Admin Approval
The MFA for your device operations
Nov 10 2025
6
Security Copilot
Copilot with Explorer and Agents in Intune
Nov 17 2025
7
EPM
User account Context
EPM Dashboard for user readiness
Wildcards in elevation rules
Copilot to identify elevation risks
Explicit deny elevation
EPM Support on AVD
Feb 2026
Oct 2025
8
Admin Tasks
Your centralized "single pane of glass"
Feb 2026
Nov 2025
9
Restore at first sign-in
Kick-start your users on their fresh installed Windows device
Feb 2026
Nov 2025

1 Autopilot

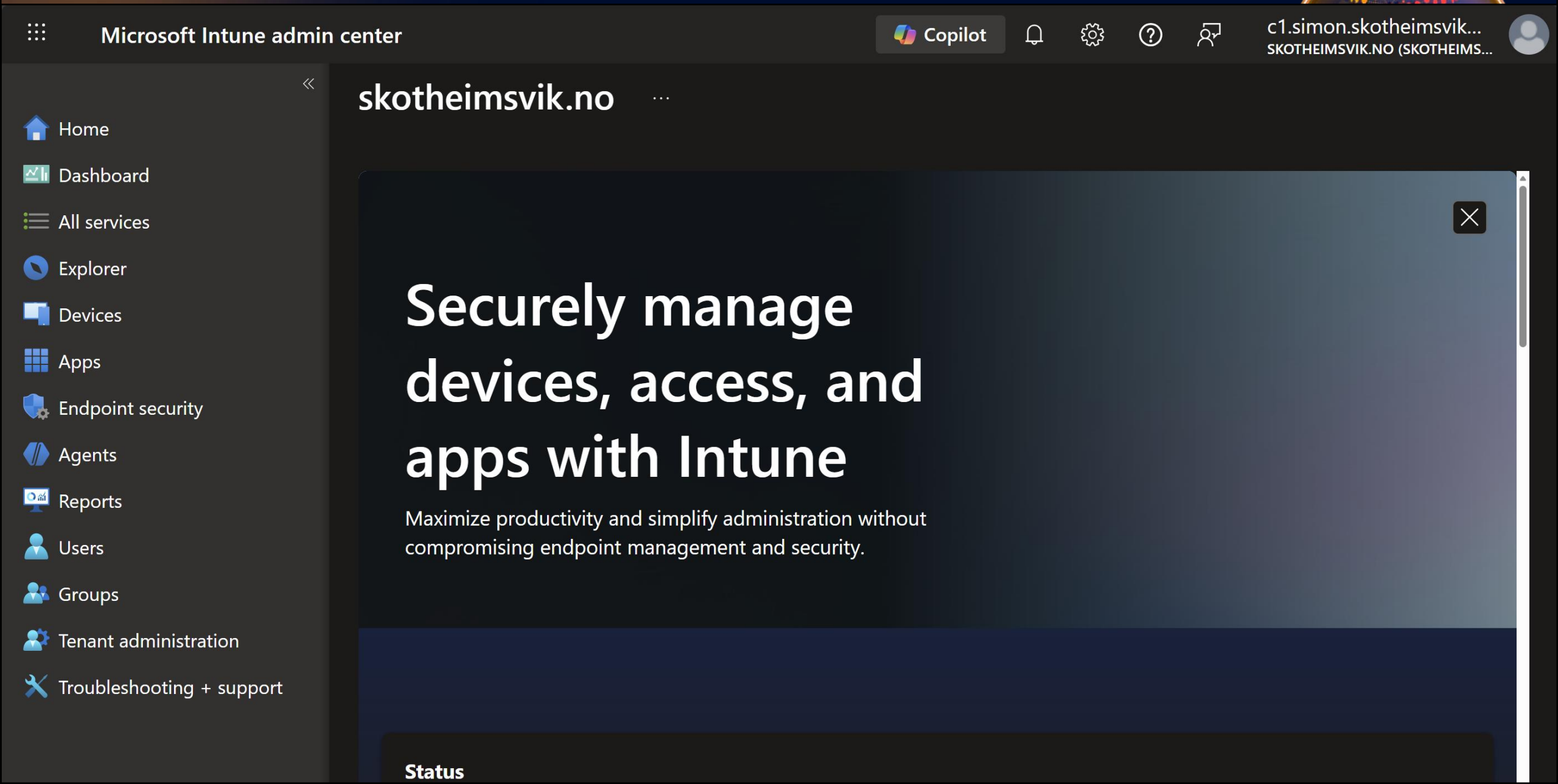
Deployment Profiles (Autopilot v1)

Device Preparation policies (Autopilot v2)

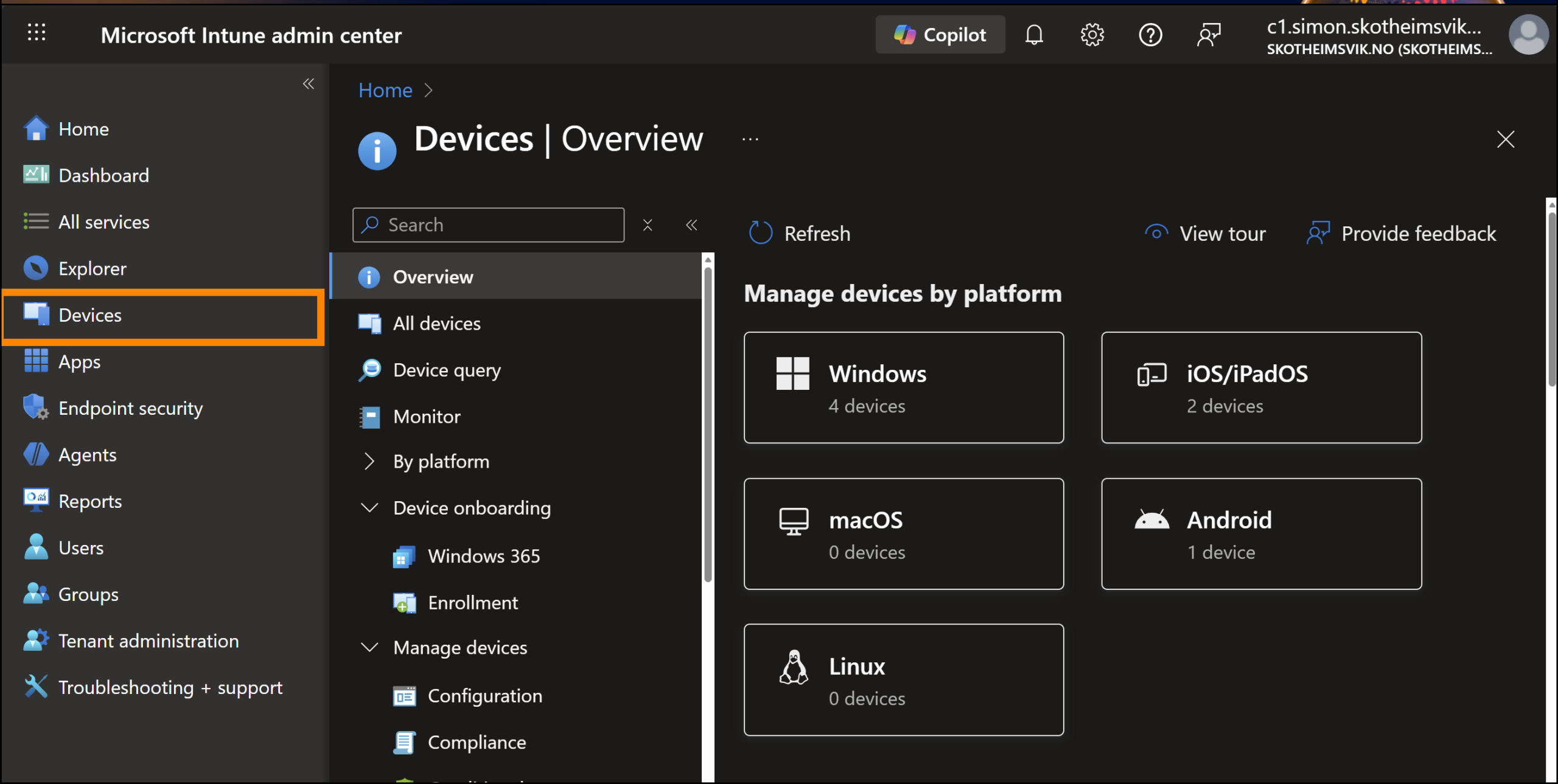
Windows Updates during Autopilot

Enrollment Notifications

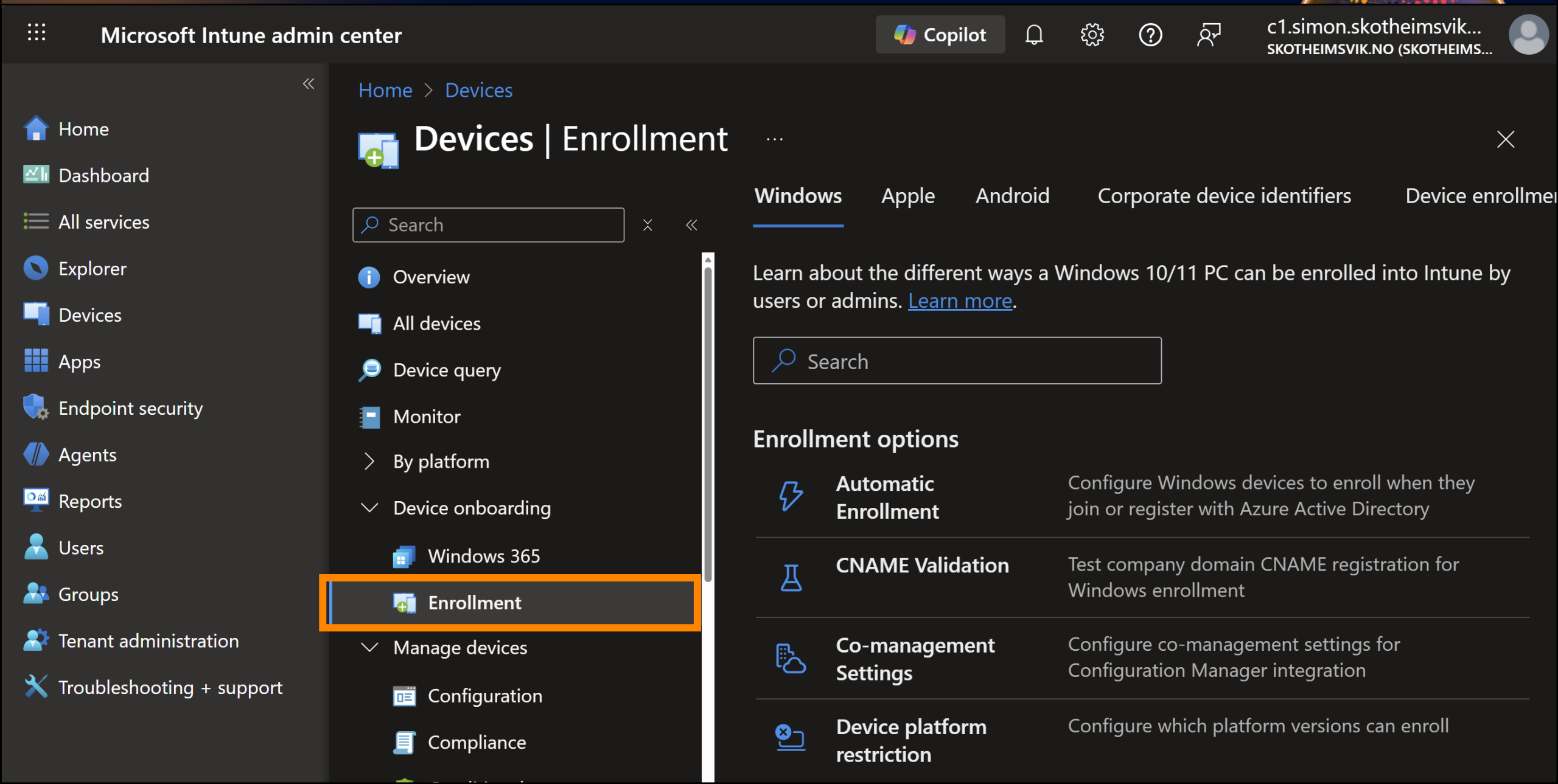
Autopilot Deployment Profiles



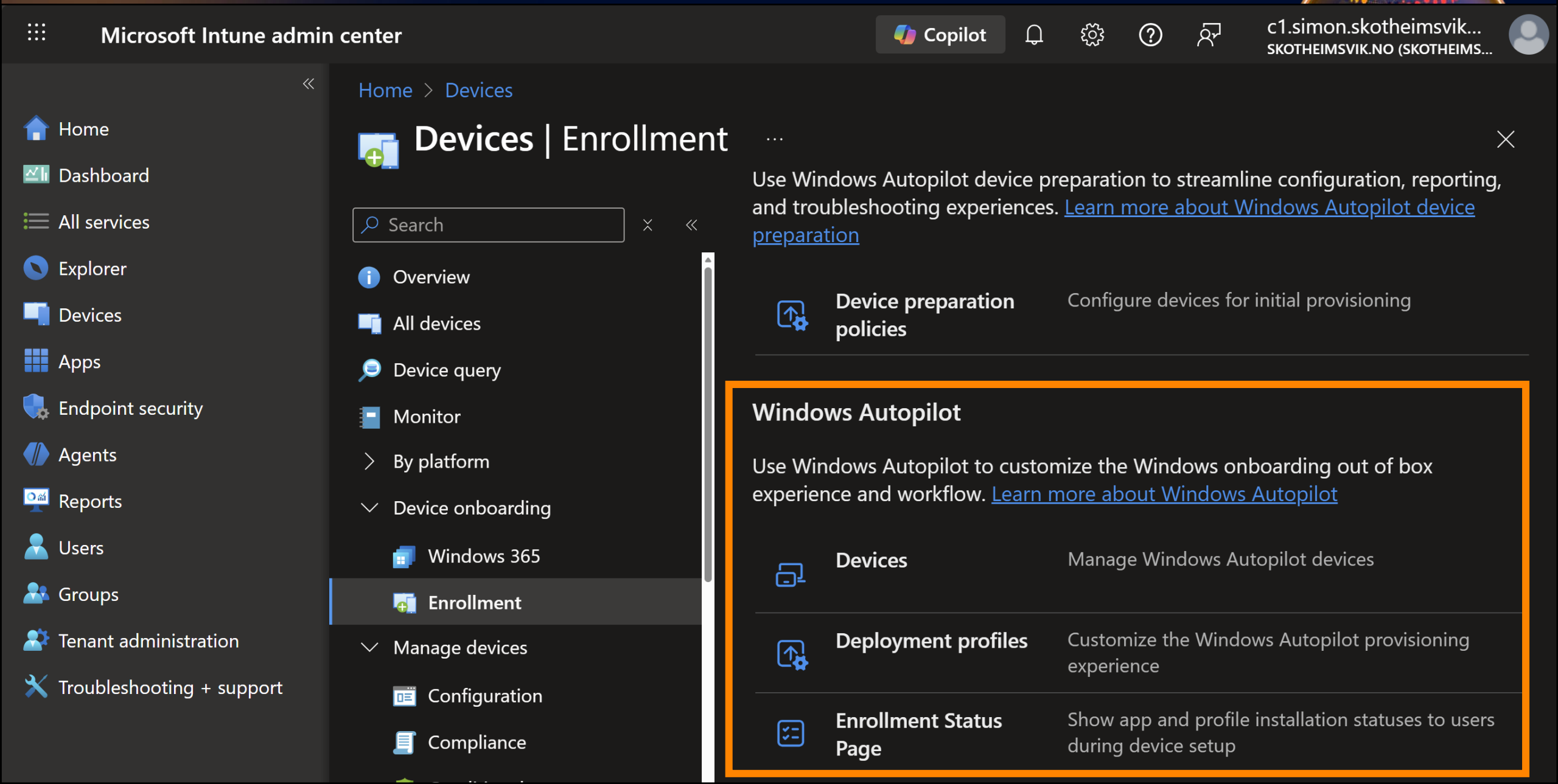
Autopilot Deployment Profiles



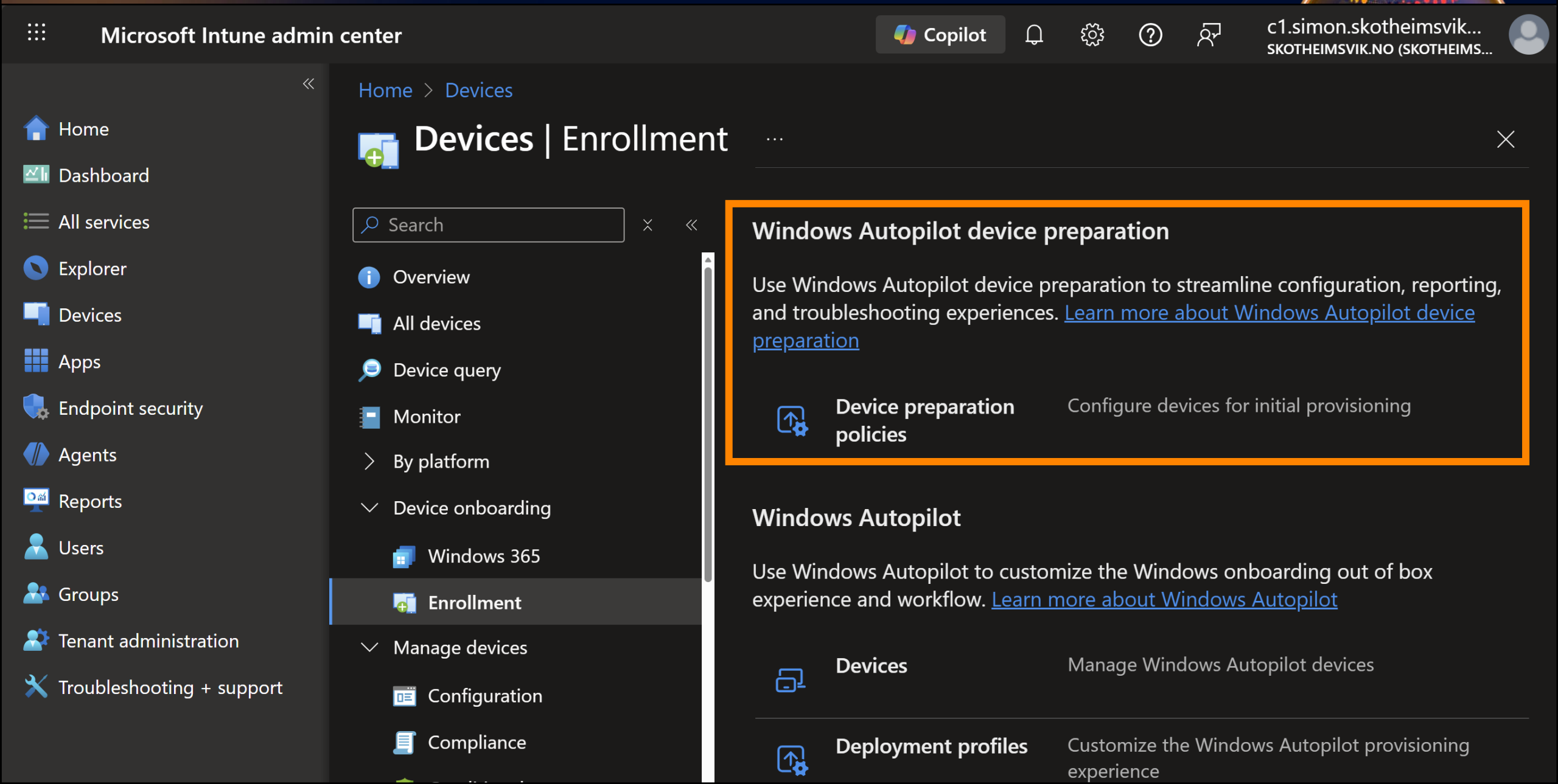
Autopilot Deployment Profiles



Autopilot Deployment Profiles

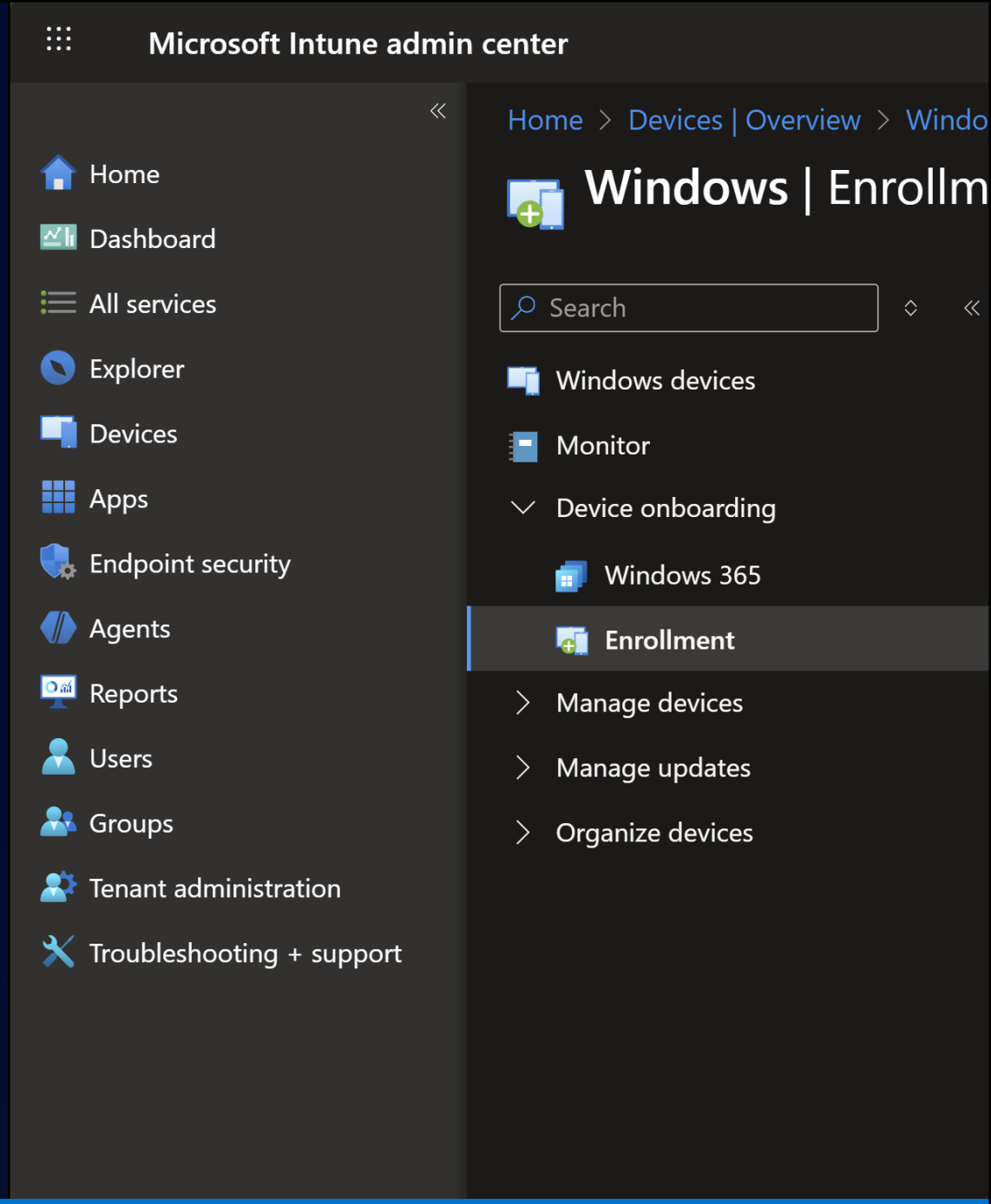


Autopilot Deployment Profiles



Security Updates during OOBE

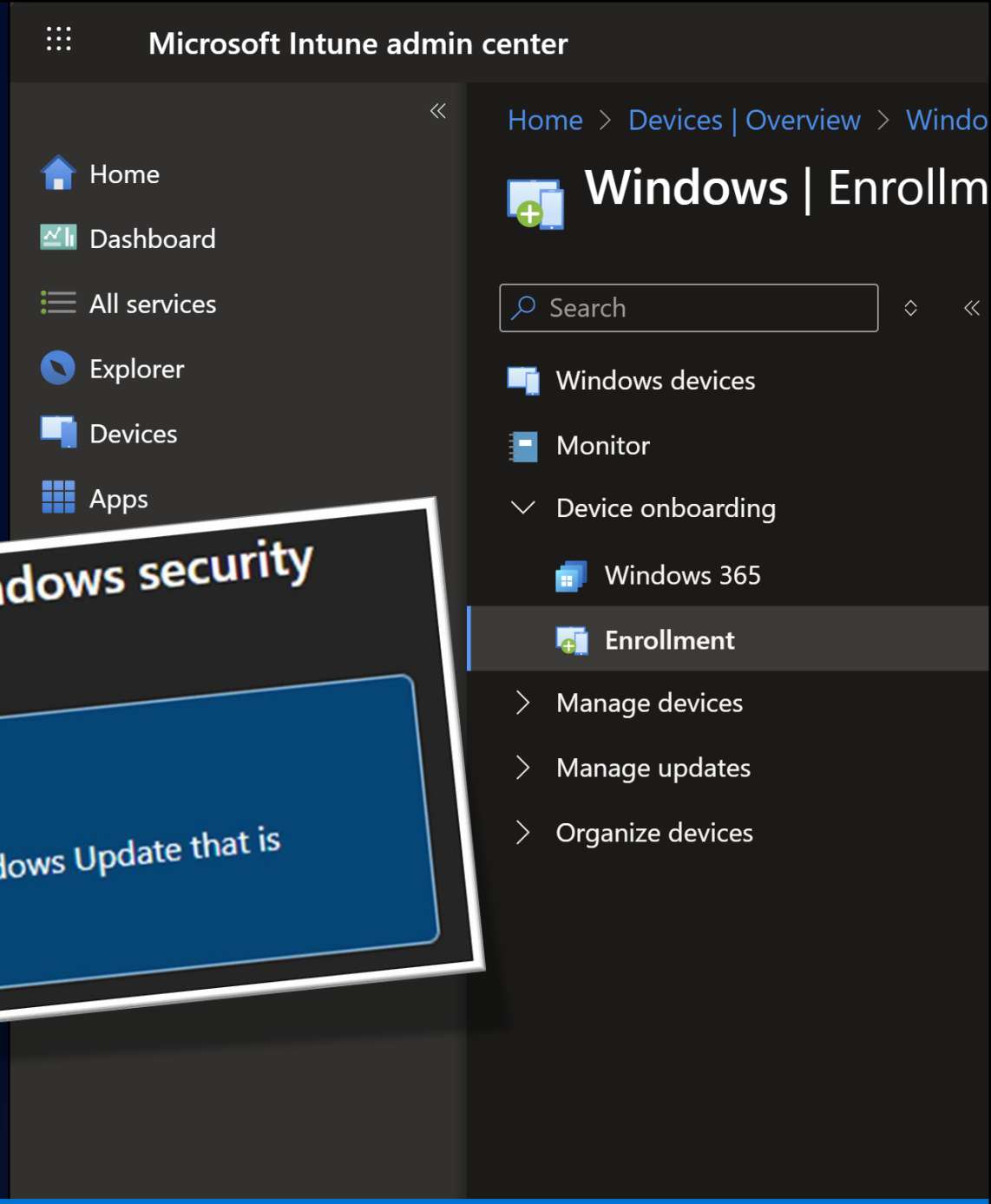
- **New setting** to allow or block automatic installation of Windows quality updates during OOBE



https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#enrollment-status-page-support-for-installing-windows-security-updates-during-windows-oobe-

Security Updates during OOBE

- **New setting** to allow or block automatic installation of Windows quality updates during OOBE



https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#enrollment-status-page-support-for-installing-windows-security-updates-during-windows-oobe-

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

Windows | Enrollment

Search
Windows devices
Monitor
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates
Organize devices

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

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

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

Edit profile

Turn on log collection and diagnostics page for end users	No / **Yes**
Only show page to devices provisioned by out-of-box experience (OOBE)	No / **Yes**
Install Windows updates (might restart the device)	**No** / Yes
Block device use until all apps and profiles are installed	No / **Yes**
Allow users to reset device if installation error occurs	No / **Yes**
Allow users to use device if installation error occurs	No / **Yes**
Block device use until required apps are installed if they are assigned to the user/device	All / **Selected**

Review + save

Cancel

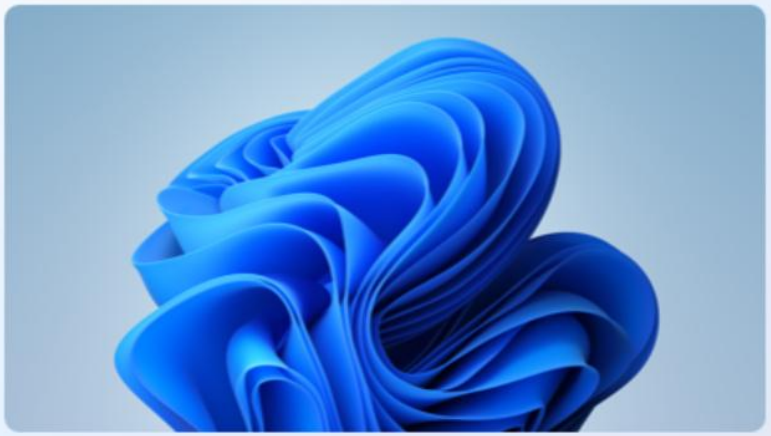
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Edit profile

Turn on log collection and diagnostics page for end users	No / Yes
Only show page to devices provisioned by out-of-box experience (OOBE)	No / Yes
Install Windows updates (might restart the device)	No / Yes
Block device use until all apps and profiles are installed	No / Yes
Allow users to reset device if installation error occurs	No / Yes
Allow users to use device if installation error occurs	No / Yes
Block device use until required apps are installed if they are assigned to the user/device	All / Selected

Review + save
Cancel

Checking for Windows updates

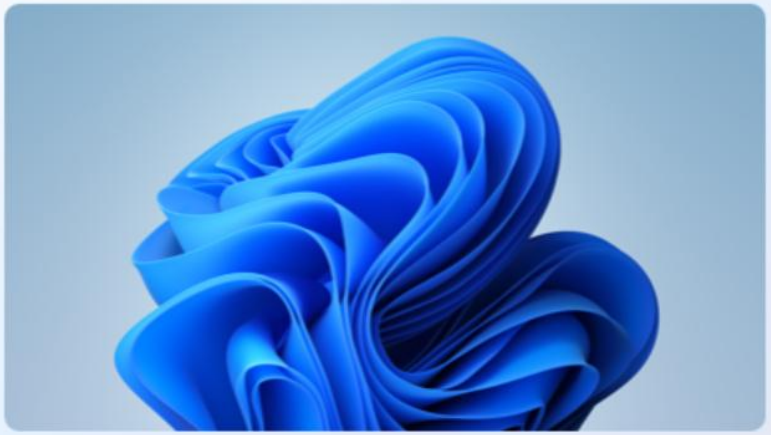


See you in a bit

If the update isn't done, it's OK to step away—we'll take care of the rest. Just be sure your PC is plugged in.

Your update is in progress—this could take a while. Please keep your PC on and plugged in.

Step 1 of 3: Downloading - 13%



See you in a bit

If the update isn't done, it's OK to step away—we'll take care of the rest. Just be sure your PC is plugged in.

Your update is in progress—this could take a while. Please keep your PC on and plugged in.

Step 1 of 3: Downloading - 87%

Cancel feature and security updates

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

Edit profile

Turn on log collection and diagnostics page for end users	No / Yes
Only show page to devices provisioned by out-of-box experience (OOBE)	No / Yes
Install Windows updates (might restart the device)	No / Yes
Block device use until all apps and profiles are installed	No / Yes
Allow users to reset device if installation error occurs	No / Yes
Allow users to use device if installation error occurs	No / Yes
Block device use until required apps are installed if they are assigned to the user/device	All / Selected

Review + save
Cancel

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

Windows | Enrollment

Search

Windows devices
Monitor
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates
Organize devices

Windows | Corporate device identifiers | Device enrollment managers

Learn about the different ways a Windows 10/11 PC can be enrolled into Intune by users or admins. Learn more.

Search

Enrollment options

Automatic Enrollment	Configure Windows devices to enroll when they join or register with Azure Active Directory
CNAME Validation	Test company domain CNAME registration for Windows enrollment
Co-management Settings	Configure co-management settings for Configuration Manager integration
Device platform restriction	Configure which platform versions can enroll
Device limit restriction	Define how many devices each user can enroll

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

Microsoft Intune

MDM user scope

None Some All

MDM terms of use URL

https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL

https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc

Disable MDM enrollment when adding work or school account on Windows

No

MDM compliance URL

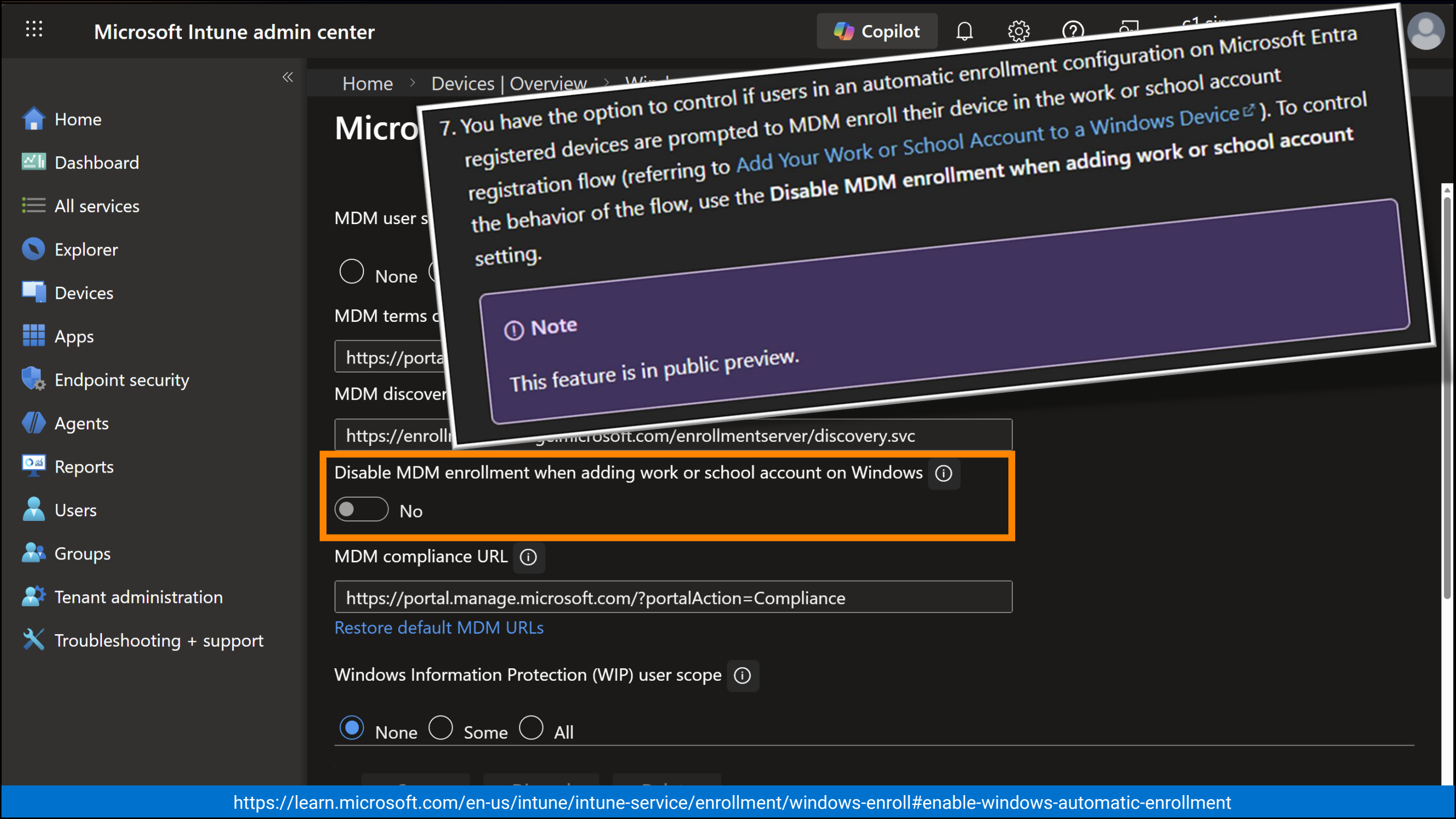
https://portal.manage.microsoft.com/?portalAction=Compliance

Restore default MDM URLs

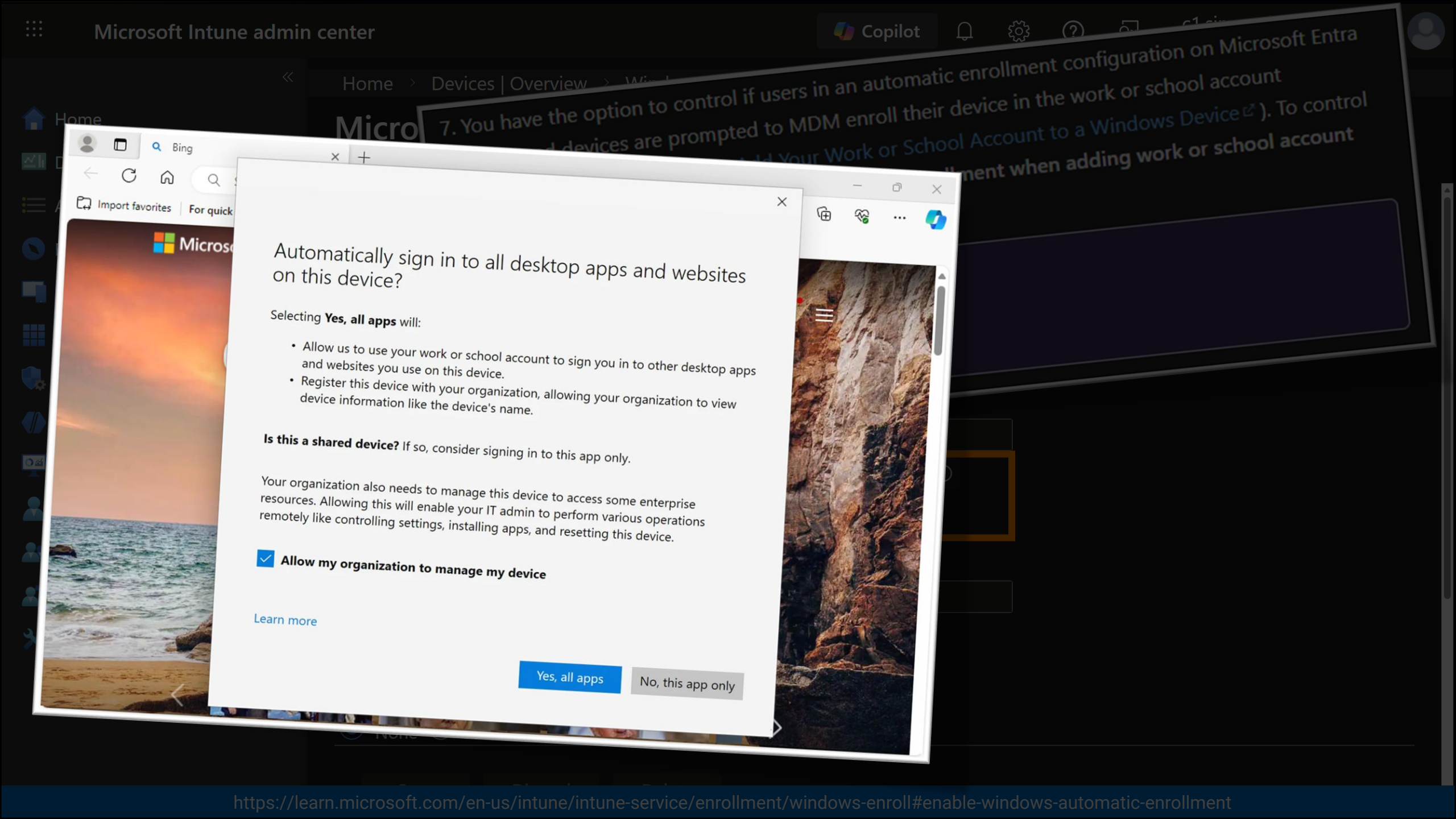
Windows Information Protection (WIP) user scope

None Some All

Save Discard Delete



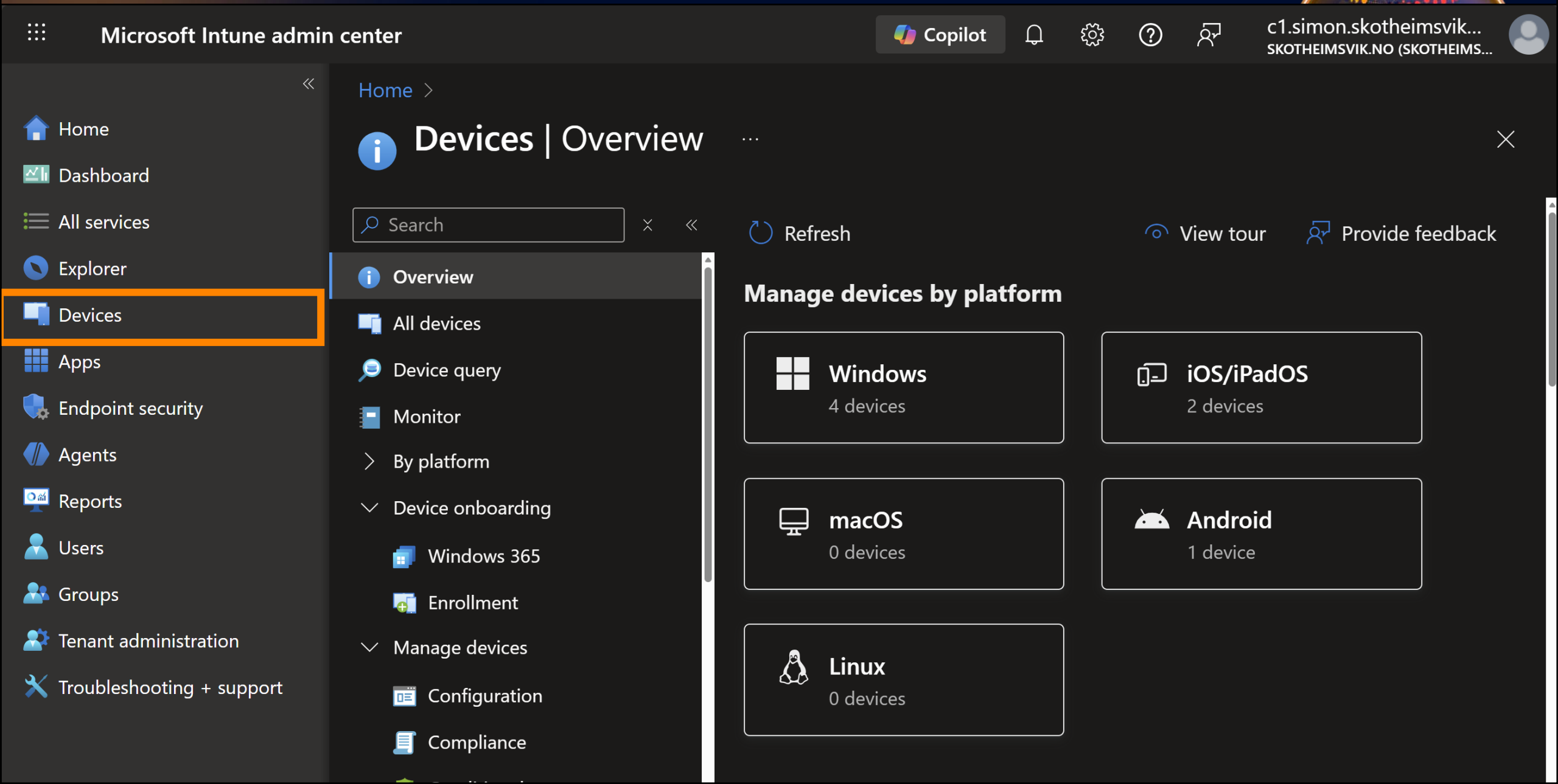
https://learn.microsoft.com/en-us/intune/intune-service/enrollment/windows-enroll#enable-windows-automatic-enrollment


Microsoft Intune admin center
Copilot
Home
Devices | Overview
7. You have the option to control if users in an automatic enrollment configuration on Microsoft Entra
devices are prompted to MDM enroll their device in the work or school account
Your Work or School Account to a Windows Device). To control
ment when adding work or school account
Bing
Import favorites
For quick
Automatically sign in to all desktop apps and websites on this device?
Selecting Yes, all apps will:
Allow us to use your work or school account to sign you in to other desktop apps and websites you use on this device.
Register this device with your organization, allowing your organization to view device information like the device's name.
Is this a shared device? If so, consider signing in to this app only.
Your organization also needs to manage this device to access some enterprise resources. Allowing this will enable your IT admin to perform various operations remotely like controlling settings, installing apps, and resetting this device.
Allow my organization to manage my device
Learn more
Yes, all apps
No, this app only
https://learn.microsoft.com/en-us/intune/intune-service/enrollment/windows-enroll#enable-windows-automatic-enrollment

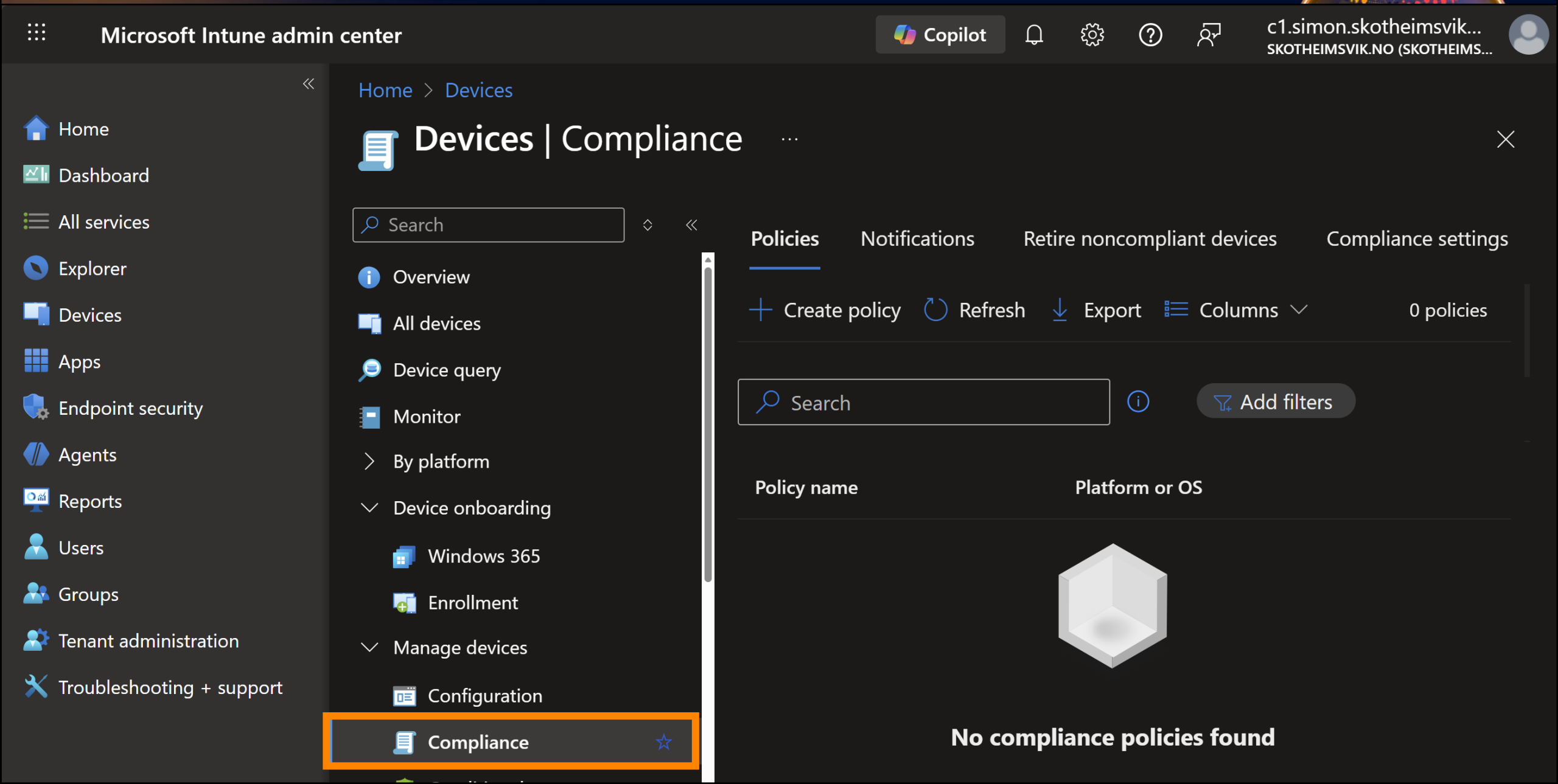
2 Compliance

Default Device Compliance news

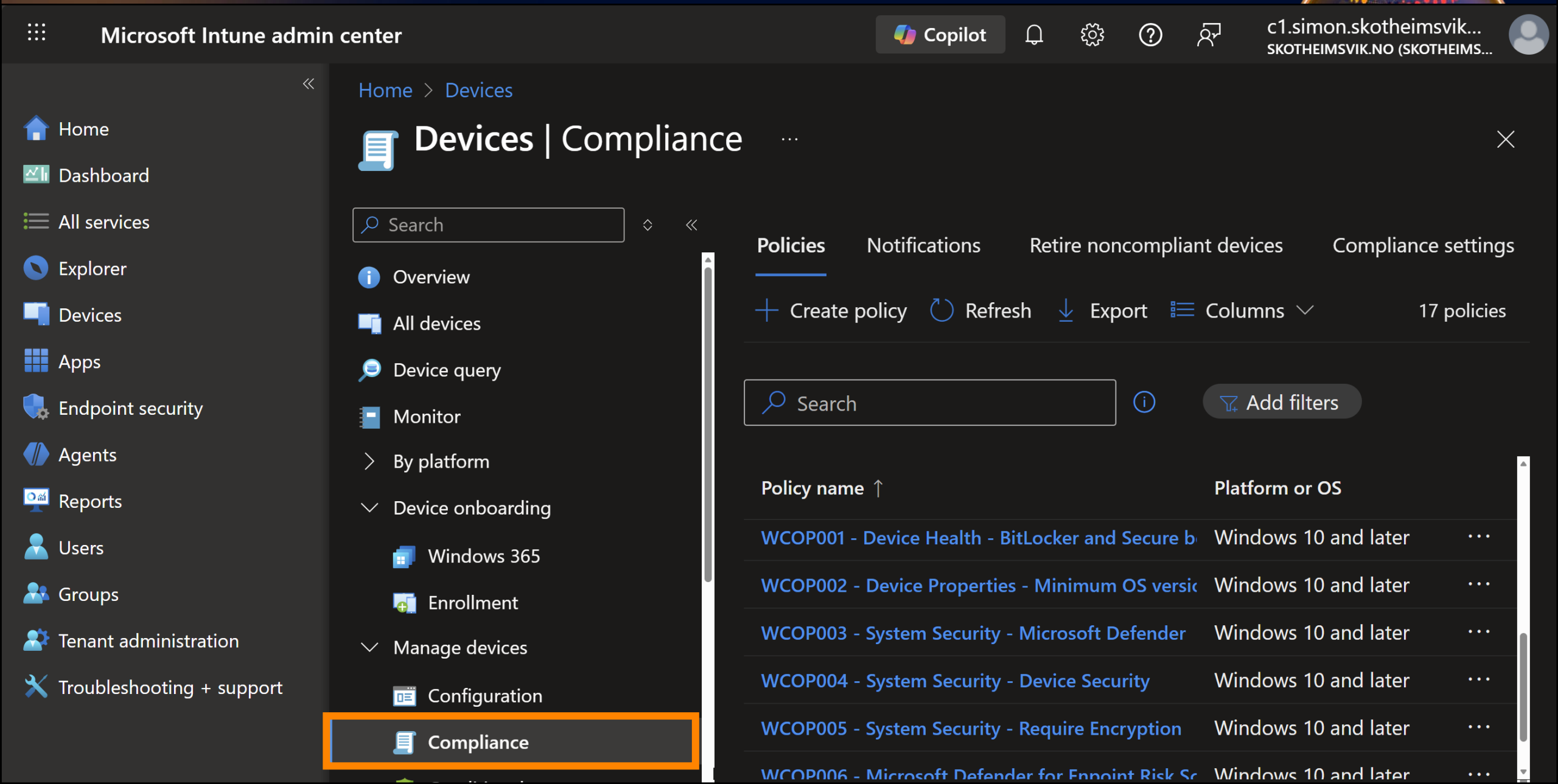
Intune Compliance Policies



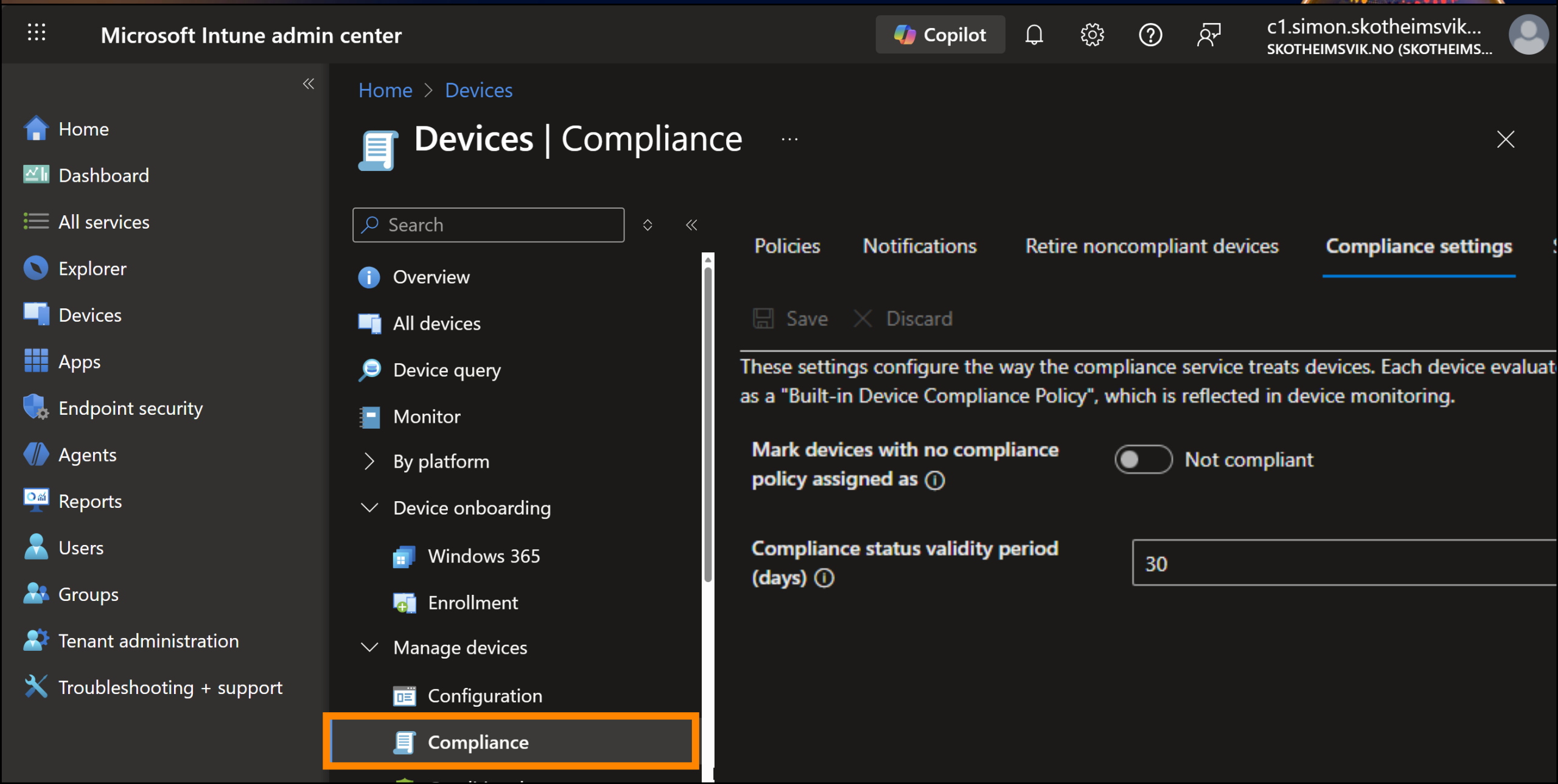
Intune Compliance Policies



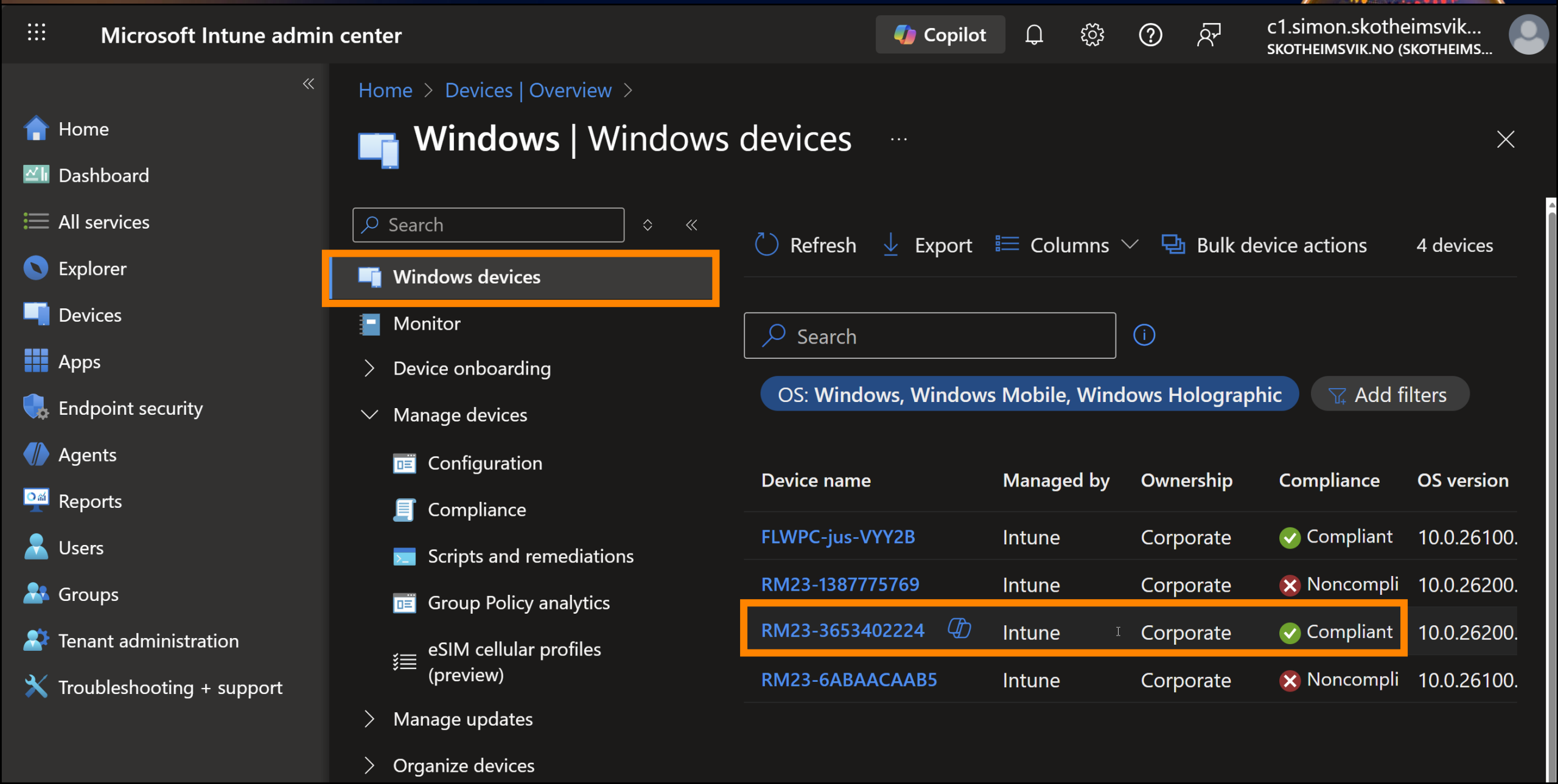
Intune Compliance Policies



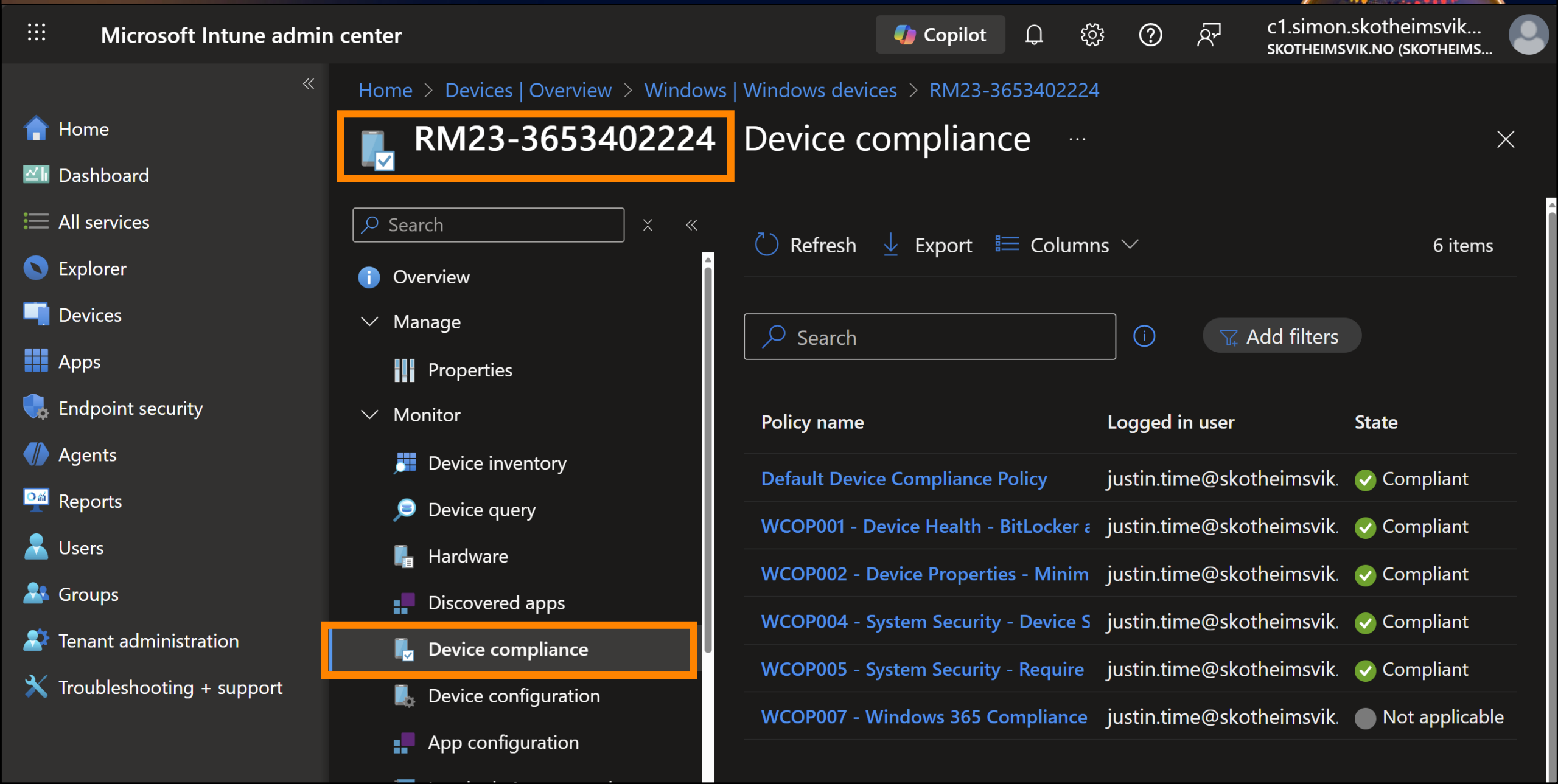
Intune Compliance Policies



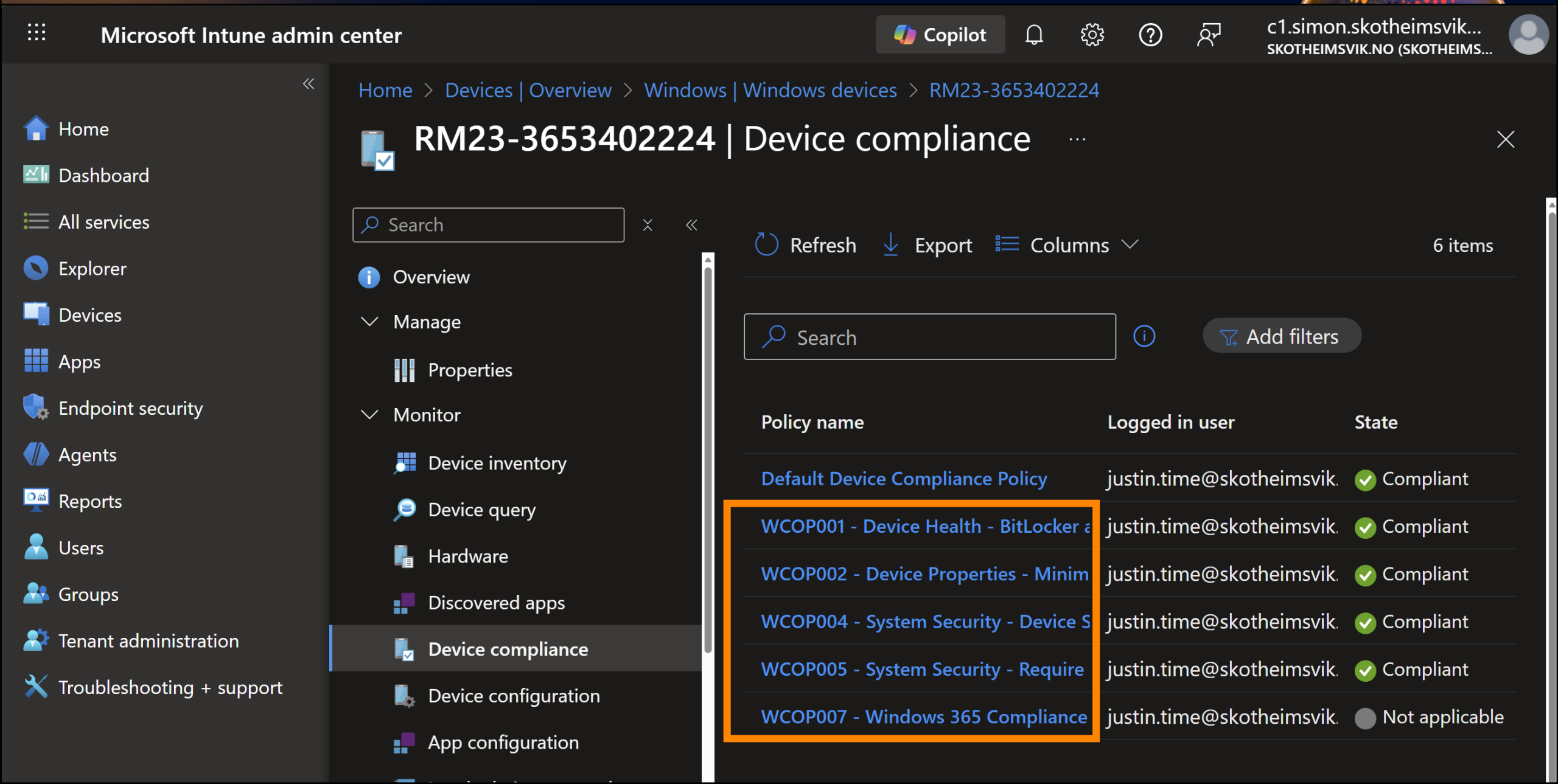
Intune Compliance Policies



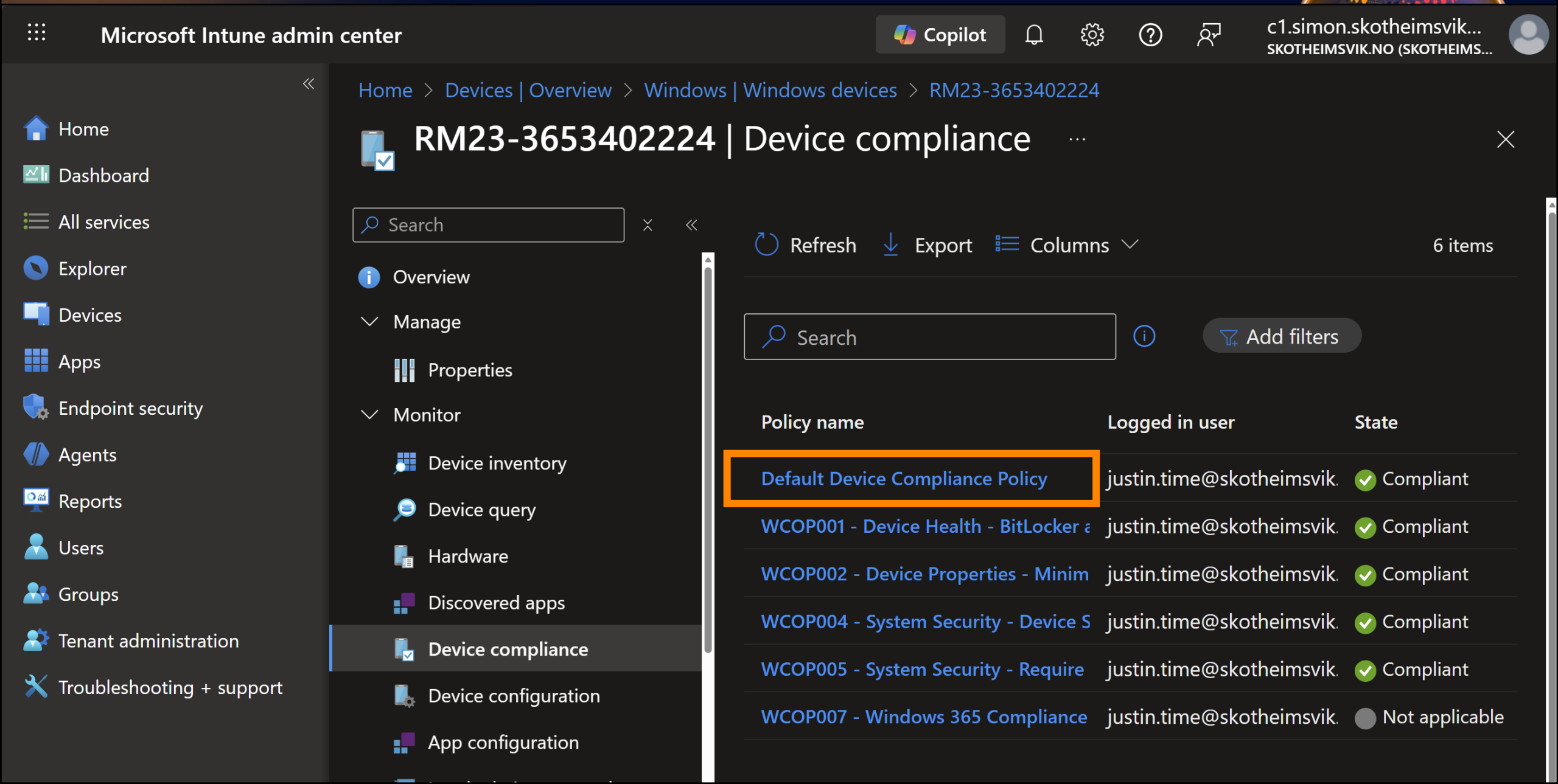
Intune Compliance Policies



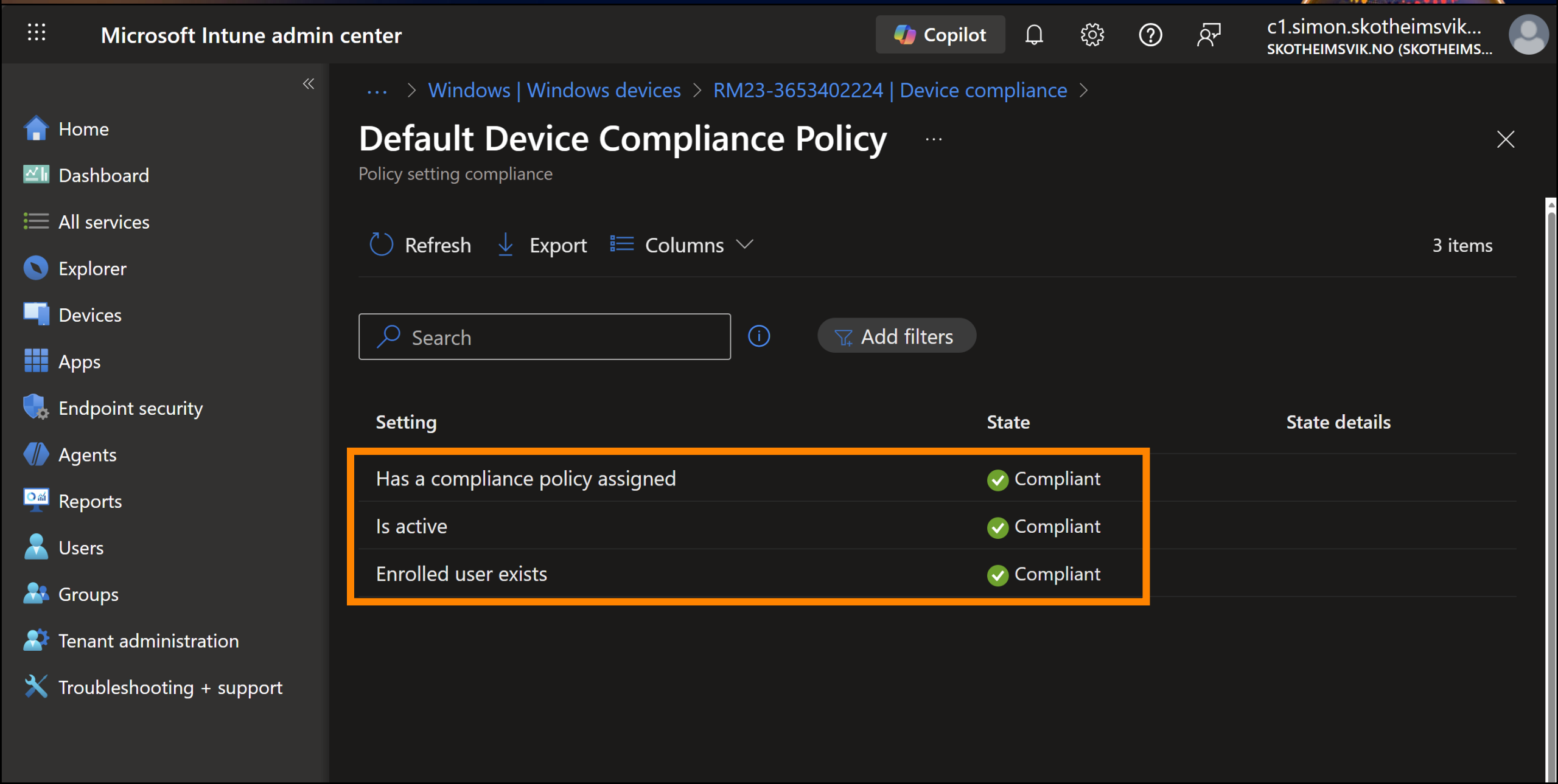
Intune Compliance Policies



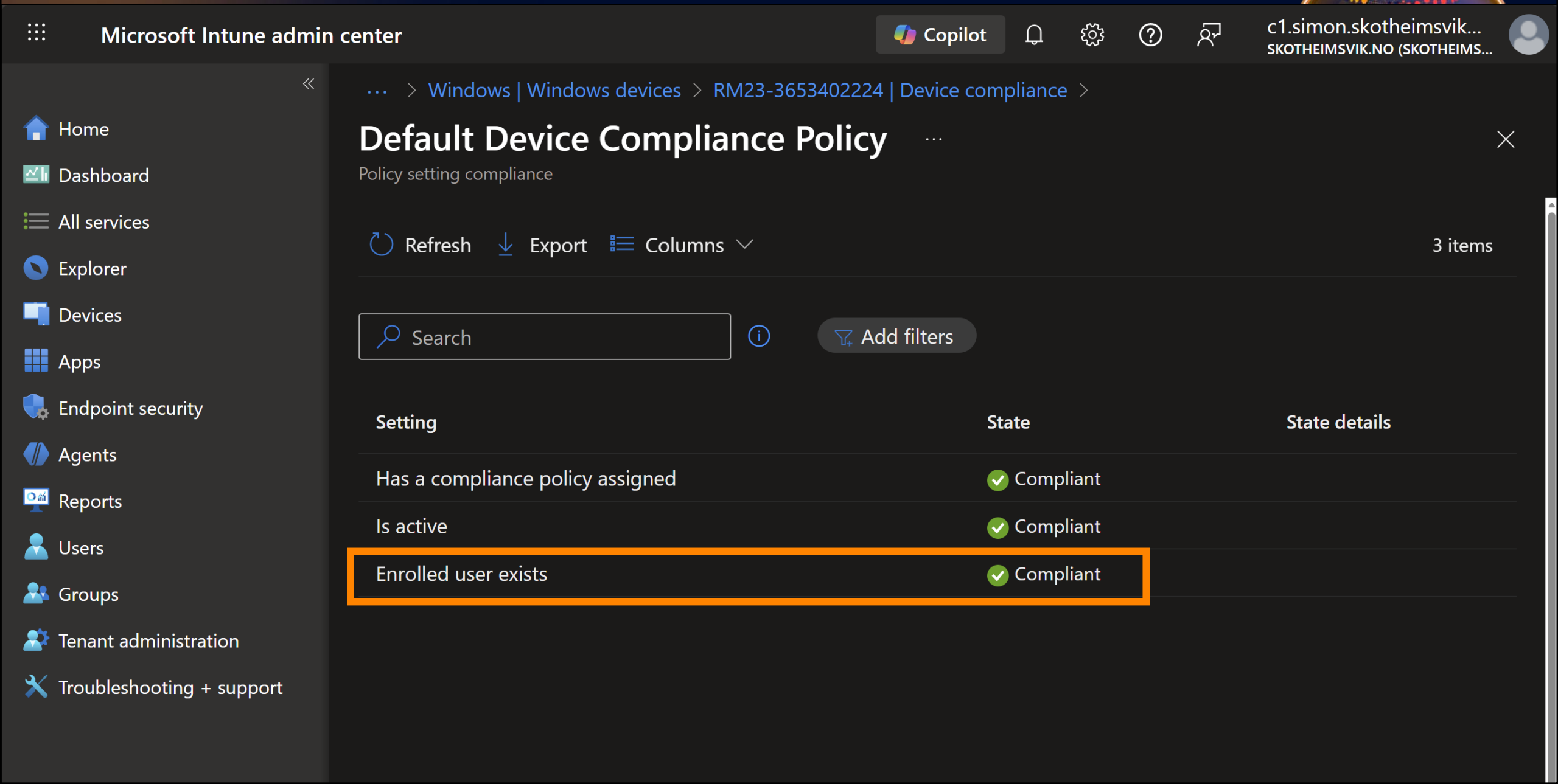
Intune Compliance Policies



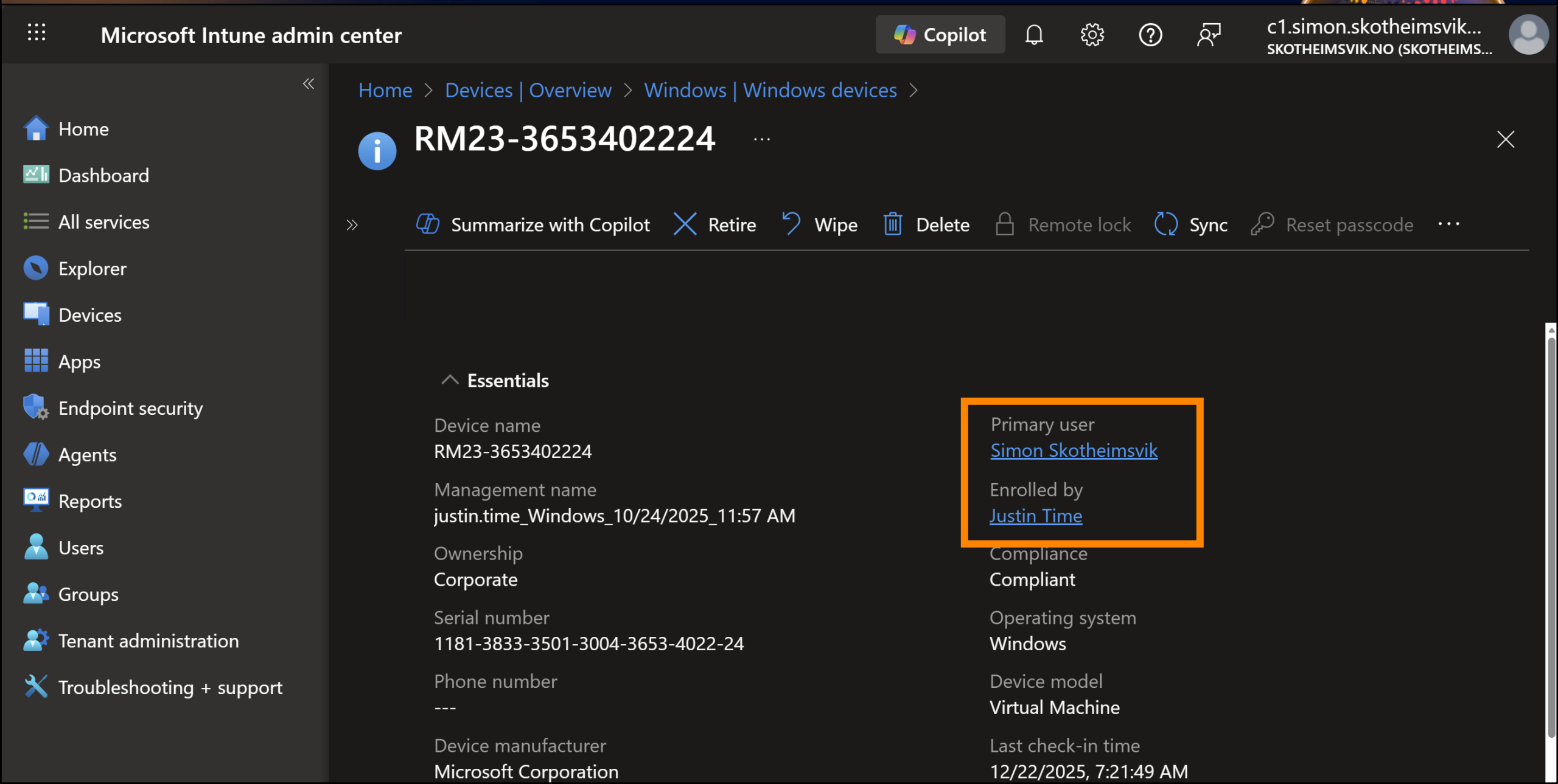
Intune Compliance Policies



Intune Compliance Policies



Intune Compliance Policies



Intune Compliance Policies

Microsoft Intune admin center

Copilot

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

Home > Devices | Overview > Windows | Windows devices >

RM23-3653402224

Retire | Wipe | Delete | Remote lock | Sync | Reset passcode

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

Microsoft Intune admin center

Default Device Compliance Policy

Setting	State
Has a compliance policy assigned	Compliant
Is active	Compliant
Enrolled user exists	Not compliant

Primary user
Simon Skotheimsvik

Enrolled by
Justin Time

Compliance
Compliant

Operating system
Windows

Device model
Virtual Machine

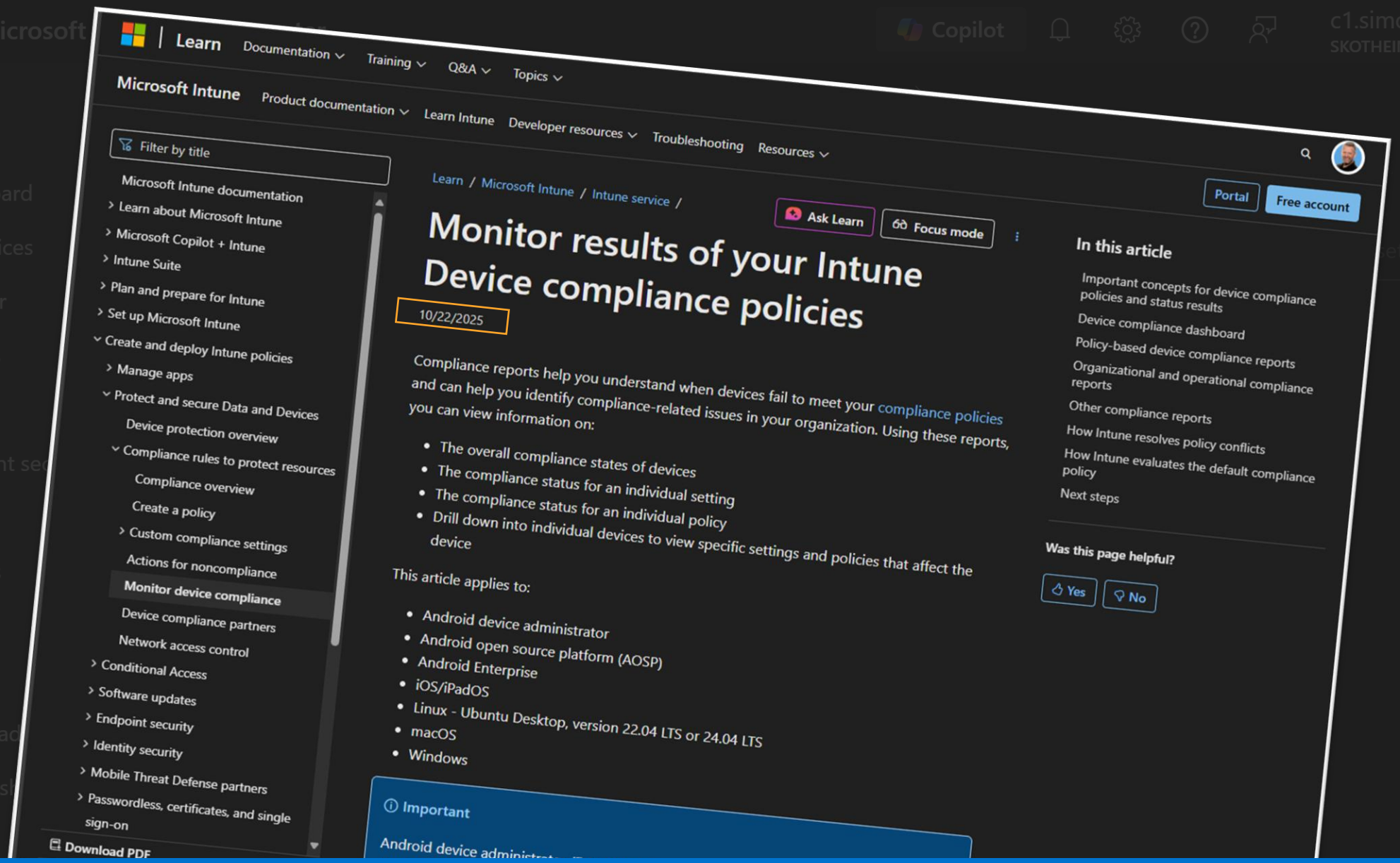
Last check-in time
12/22/2025, 7:21:49 AM

Serial number
1181-3833-3501-3004-3653-4022-24

Phone number

Device manufacturer
Microsoft Corporation

Intune Compliance Policies



Learn | Documentation | Training | Q&A | Topics

Microsoft Intune | Product documentation | Learn Intune | Developer resources | Troubleshooting | Resources

Filter by title

- Microsoft Intune documentation
- Learn about Microsoft Intune
- Microsoft Copilot + Intune
- Intune Suite
- Plan and prepare for Intune
- Set up Microsoft Intune
- Create and deploy Intune policies
  - Manage apps
  - Protect and secure Data and Devices
    - Device protection overview
    - Compliance rules to protect resources
      - Compliance overview
      - Create a policy
      - Custom compliance settings
      - Actions for noncompliance
      - Monitor device compliance
      - Device compliance partners
      - Network access control
    - Conditional Access
    - Software updates
    - Endpoint security
    - Identity security
    - Mobile Threat Defense partners
    - Passwordless, certificates, and single sign-on

Download PDF

Learn / Microsoft Intune / Intune service /

Ask Learn | Focus mode | Portal | Free account

Monitor results of your Intune Device compliance policies

10/22/2025

Compliance reports help you understand when devices fail to meet your compliance policies and can help you identify compliance-related issues in your organization. Using these reports, you can view information on:

- The overall compliance states of devices
- The compliance status for an individual setting
- The compliance status for an individual policy
- Drill down into individual devices to view specific settings and policies that affect the device

This article applies to:

- Android device administrator
- Android open source platform (AOSP)
- Android Enterprise
- iOS/iPadOS
- Linux - Ubuntu Desktop, version 22.04 LTS or 24.04 LTS
- macOS
- Windows

Important

Android device administ...

In this article

- Important concepts for device compliance policies and status results
- Device compliance dashboard
- Policy-based device compliance reports
- Organizational and operational compliance reports
- Other compliance reports
- How Intune resolves policy conflicts
- How Intune evaluates the default compliance policy
- Next steps

Was this page helpful?

Yes | No

https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-monitor#how-intune-evaluates-the-default-compliance-policy

Intune Compliance Policies

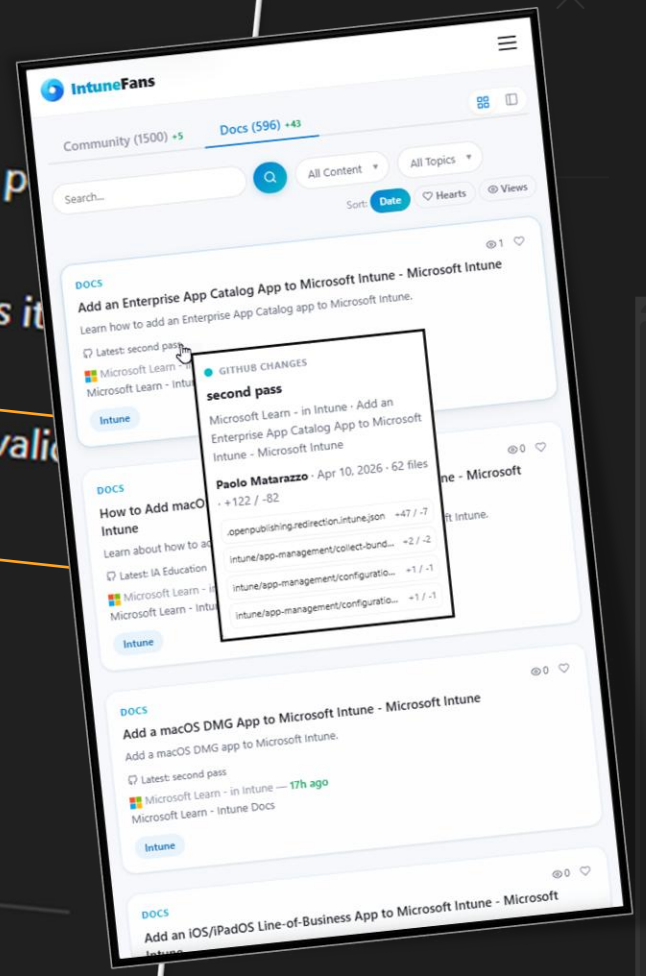
The evaluation process identifies the device as noncompliant if any of the following statements are false.

- The device has a compliance policy assigned: At least one applicable compliance p must be assigned to the device with an applicable setting.
- The device is active: The device should remain in contact with Intune. This requires it be turned on with an internet connection. The default grace period is 30 days.
- The enrolled user exists: The user that is actively using the device exists and has a vali Intune license.

Next steps

Compliance policies overview

Additional resources



https://learn.microsoft.com/en-us/intune/intune-service/protect/compliance-policy-monitor#how-intune-evaluates-the-default-compliance-policy

Intune Compliance Policies

Microsoft Intune admin center

Copilot

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

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

Home > Devices | Overview > Windows | Windows devices >

RM23-3653402224

Retire | Wipe | Delete | Remote lock | Sync | Reset passcode | ...

Microsoft Intune admin center

Default Device Compliance Policy

Setting	State
Has a compliance policy assigned	Compliant
Is active	Compliant
Enrolled user exists	Not compliant

Primary user
Simon Skotheimsvik

Enrolled by
Justin Time

Compliance
Compliant

Operating system
Windows

Device model
Virtual Machine

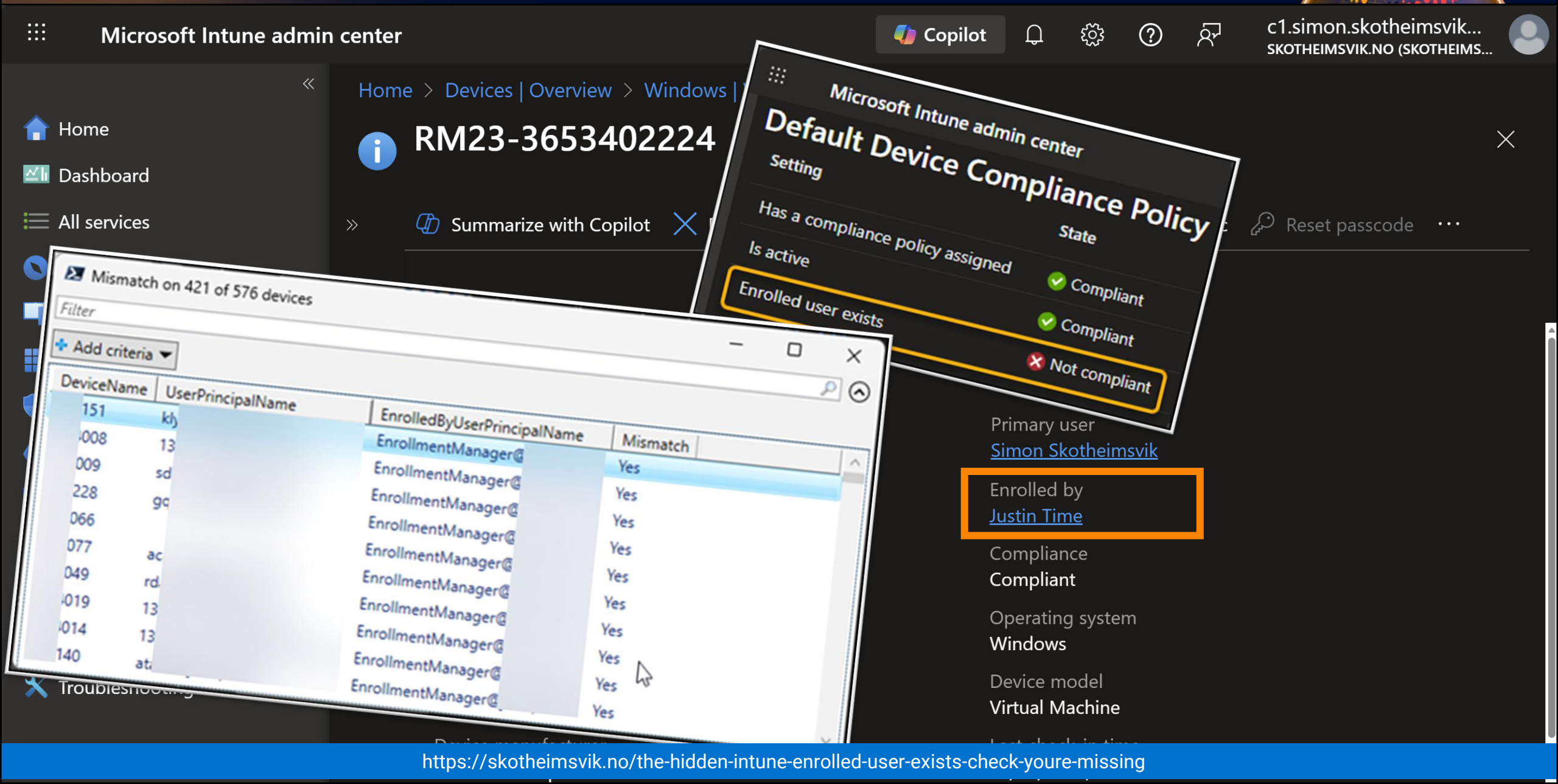
Last check-in time
12/22/2025, 7:21:49 AM

Serial number
1181-3833-3501-3004-3653-4022-24

Phone number

Device manufacturer
Microsoft Corporation

Intune Compliance Policies

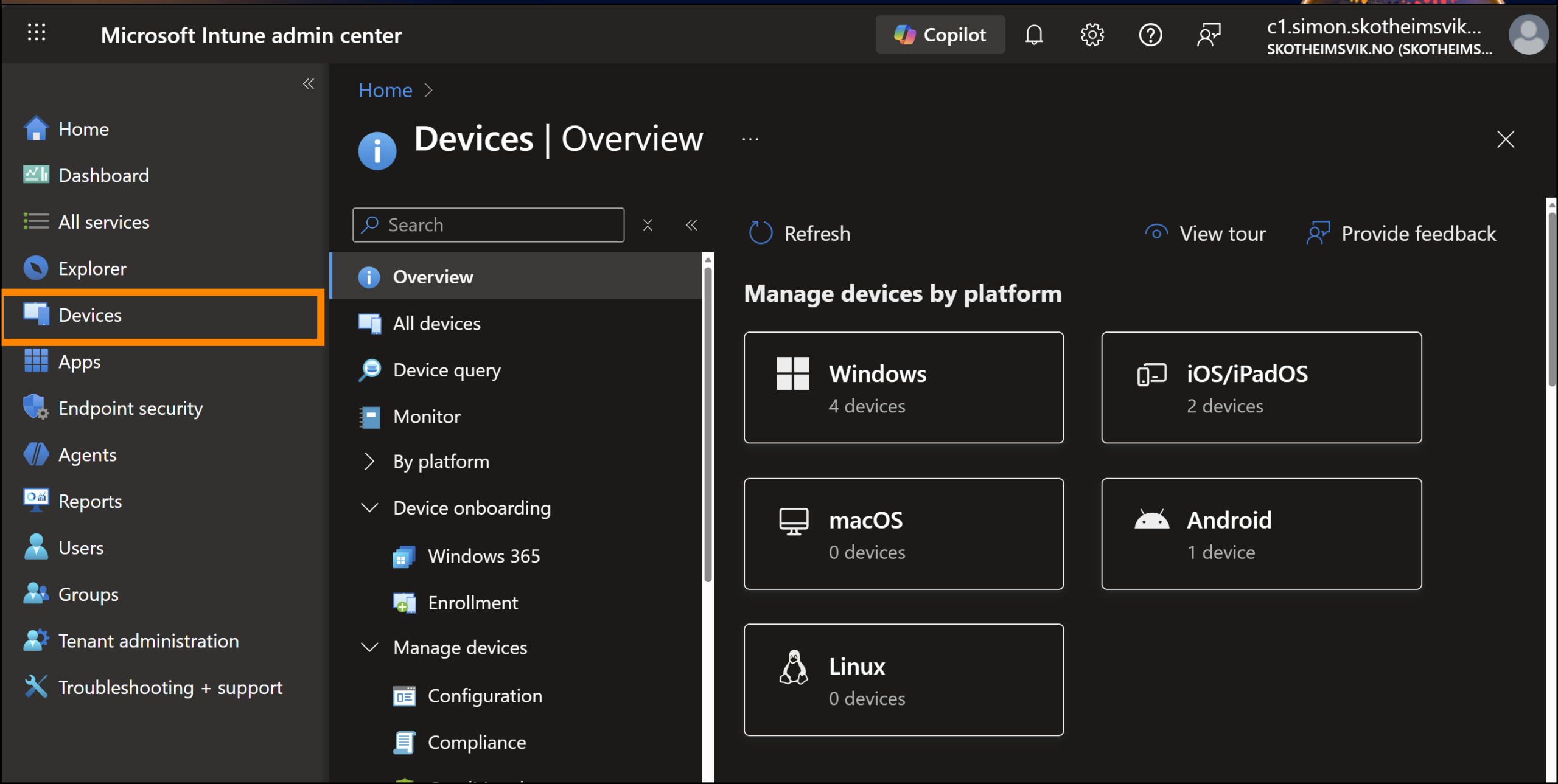


https://skotheimsvik.no/the-hidden-intune-enrolled-user-exists-check-youre-missing

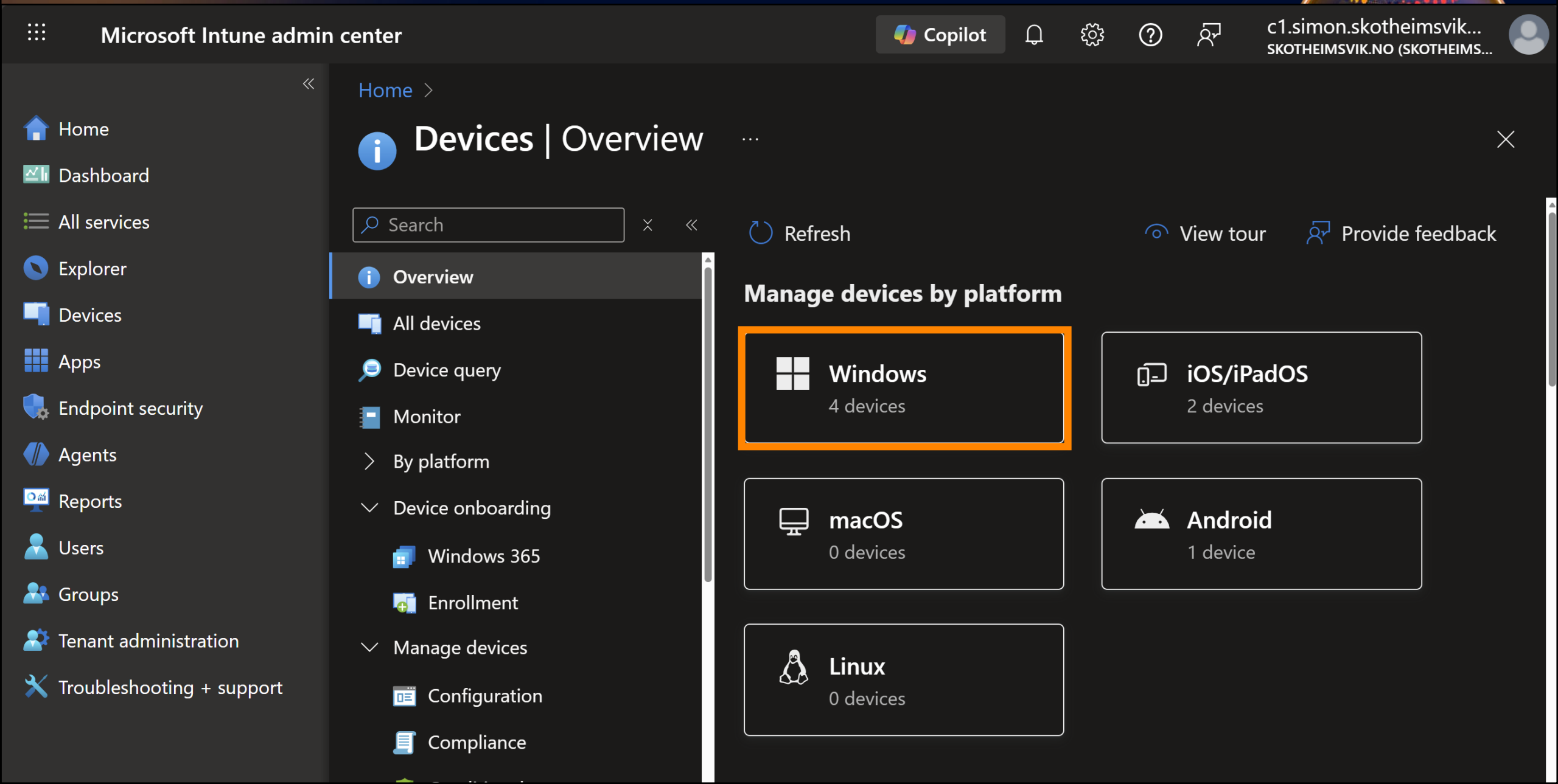
3 Autopatch

Are you patching?

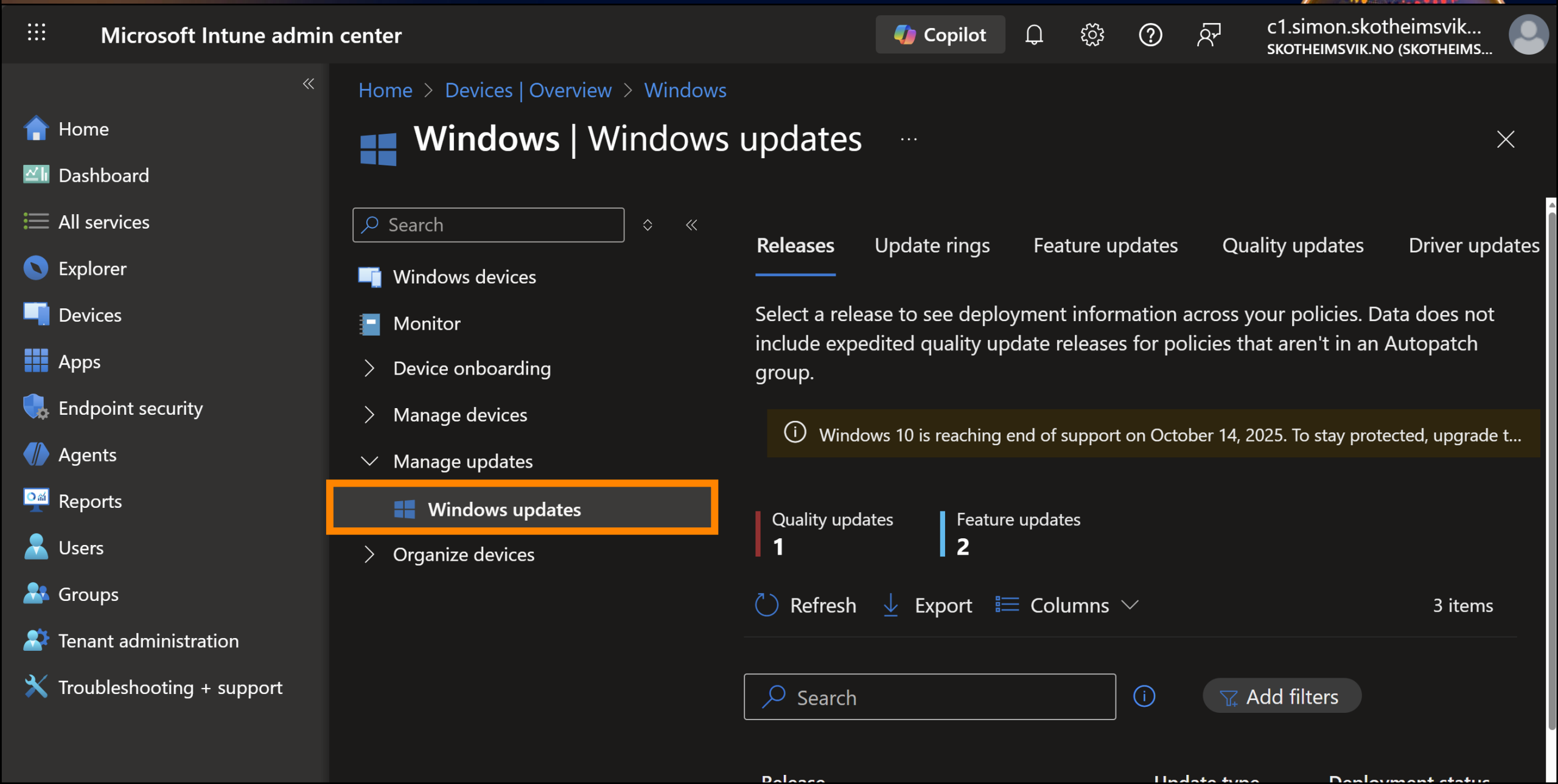
Windows Autopatch



Windows Autopatch



Windows Autopatch



Windows Autopatch

Microsoft Intune admin center

Copilot

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

Home > Devices | Overview > Windows

Windows | Windows updates

Search

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

- Windows devices
- Monitor
- Device onboarding
- Manage devices
- Manage updates
  - Windows updates
- Organize devices

Releases | Update rings | **Feature updates** | Quality updates | Driver updates

View your Windows feature update policy settings and create new feature update releases. Go to Tenant administration to manage your Autopatch groups.

Create | Refresh | Export | Columns | 0 policies

Create a feature update policy

Policies control how Windows updates are deployed to devices. Create a policy to deploy feature updates.

Learn more about managing policies through Autopatch

Windows Autopatch

endoflife.date
Operating Systems / Microsoft Windows

Microsoft Windows

Last updated on 03 October 2025

MICROSOFT OS WINDOWS

Release	Released	Active Support	Security Support	Extended Security Updates	Latest
11 25H2 (E)	1 month ago (30 Sep 2025)	Ends in 2 years and 11 months (10 Oct 2028)	Ends in 2 years and 11 months (10 Oct 2028)	Unavailable	10.0.26200
11 25H2 (W)	1 month ago (30 Sep 2025)	Ends in 1 year and 11 months (12 Oct 2027)	Ends in 1 year and 11 months (12 Oct 2027)	Unavailable	10.0.26200
11 24H2 IoT (LTS)	1 year ago (01 Oct 2024)	Ends in 3 years and 11 months (09 Oct 2029)	Ends in 8 years and 11 months (10 Oct 2034)	Unavailable	10.0.26100
11 24H2 (E) (LTS)	1 year ago (01 Oct 2024)	Ends in 3 years and 11 months (09 Oct 2029)	Ends in 3 years and 11 months (09 Oct 2029)	Unavailable	10.0.26100
11 24H2 (E)	1 year ago (01 Oct 2024)	Ends in 1 year and 11 months (12 Oct 2027)	Ends in 1 year and 11 months (12 Oct 2027)	Unavailable	10.0.26100
11 24H2 (W)	1 year ago (01 Oct 2024)	Ends in 11 months (13 Oct 2026)	Ends in 11 months (13 Oct 2026)	Unavailable	10.0.26100
11 23H2 (E)	2 years ago (31 Oct 2023)	Ends in 1 year (10 Nov 2026)	Ends in 1 year (10 Nov 2026)	Unavailable	10.0.22631
11 23H2 (W)	2 years ago (31 Oct 2023)	Ends in 1 week and 4 days (11 Nov 2025)	Ends in 1 week and 4 days (11 Nov 2025)	Unavailable	10.0.22631
~~10 22H2~~	3 years ago (18 Oct 2022)	Ended 2 weeks and 3 days ago (14 Oct 2025)	Ended 2 weeks and 3 days ago (14 Oct 2025)	Ends in 2 years and 11 months (10 Oct 2028)	~~10.0.19045~~
~~11 22H2 (E)~~	3 years ago (20 Sep 2022)	Ended 2 weeks and 3 days ago (14 Oct 2025)	Ended 2 weeks and 3 days ago (14 Oct 2025)	Unavailable	~~10.0.22621~~
~~11 22H2 (W)~~	3 years ago (20 Sep 2022)	Ended 1 year ago	Ended 1 year ago		

Copilot

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

Home
Dashboa
All servi
Explore
Device
Apps
Endpo
Agen
Repo
User
Gro
Ten
Tro

...ows

...ows updates ...

Releases | Update rings | **Feature updates** | Quality updates | Driver updates

View your Windows feature update policy settings and create new feature update releases. Go to Tenant administration to manage your Autopatch groups.

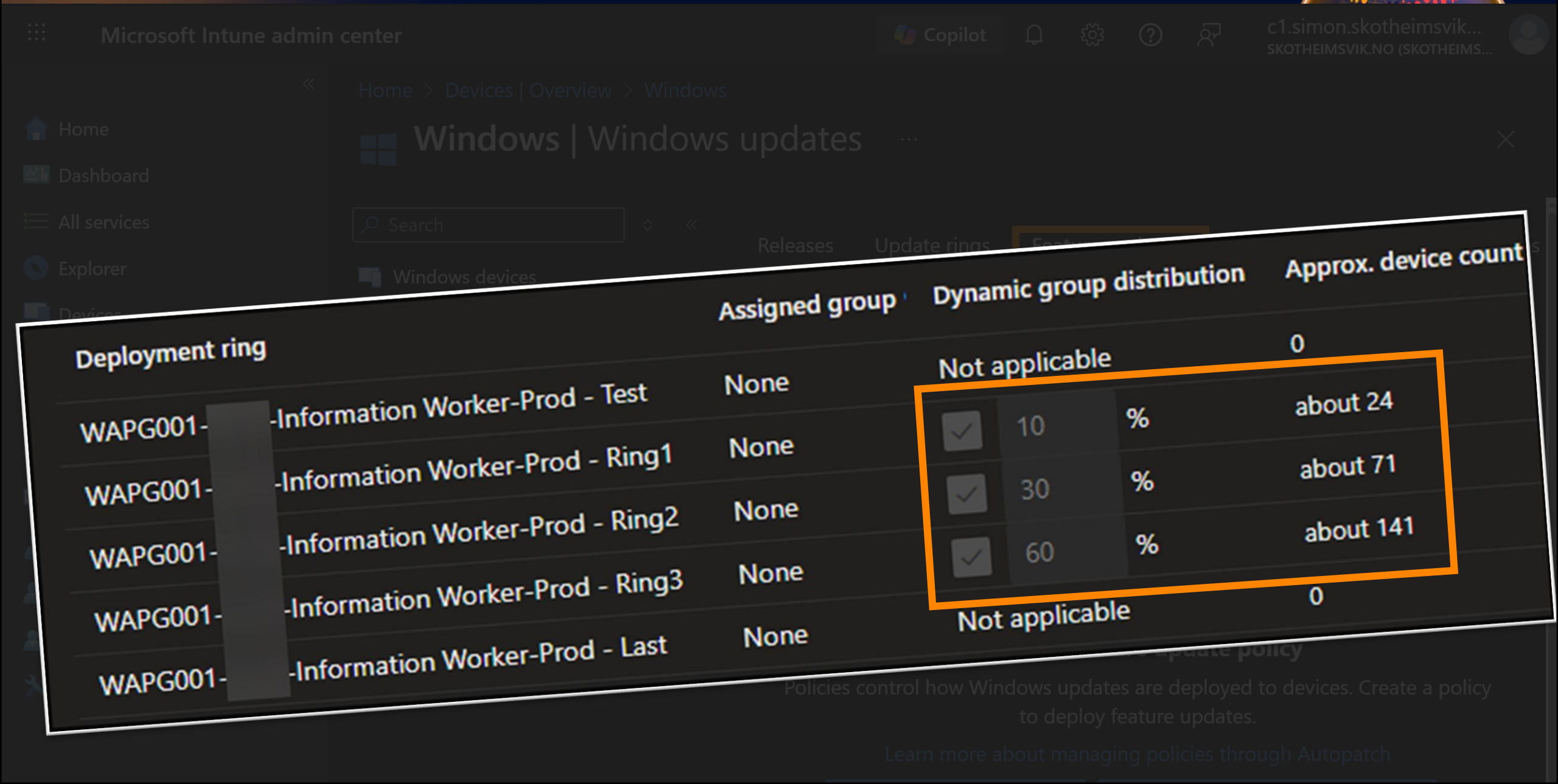
Create | Refresh | Export | Columns | 0 policies

Create a feature update policy

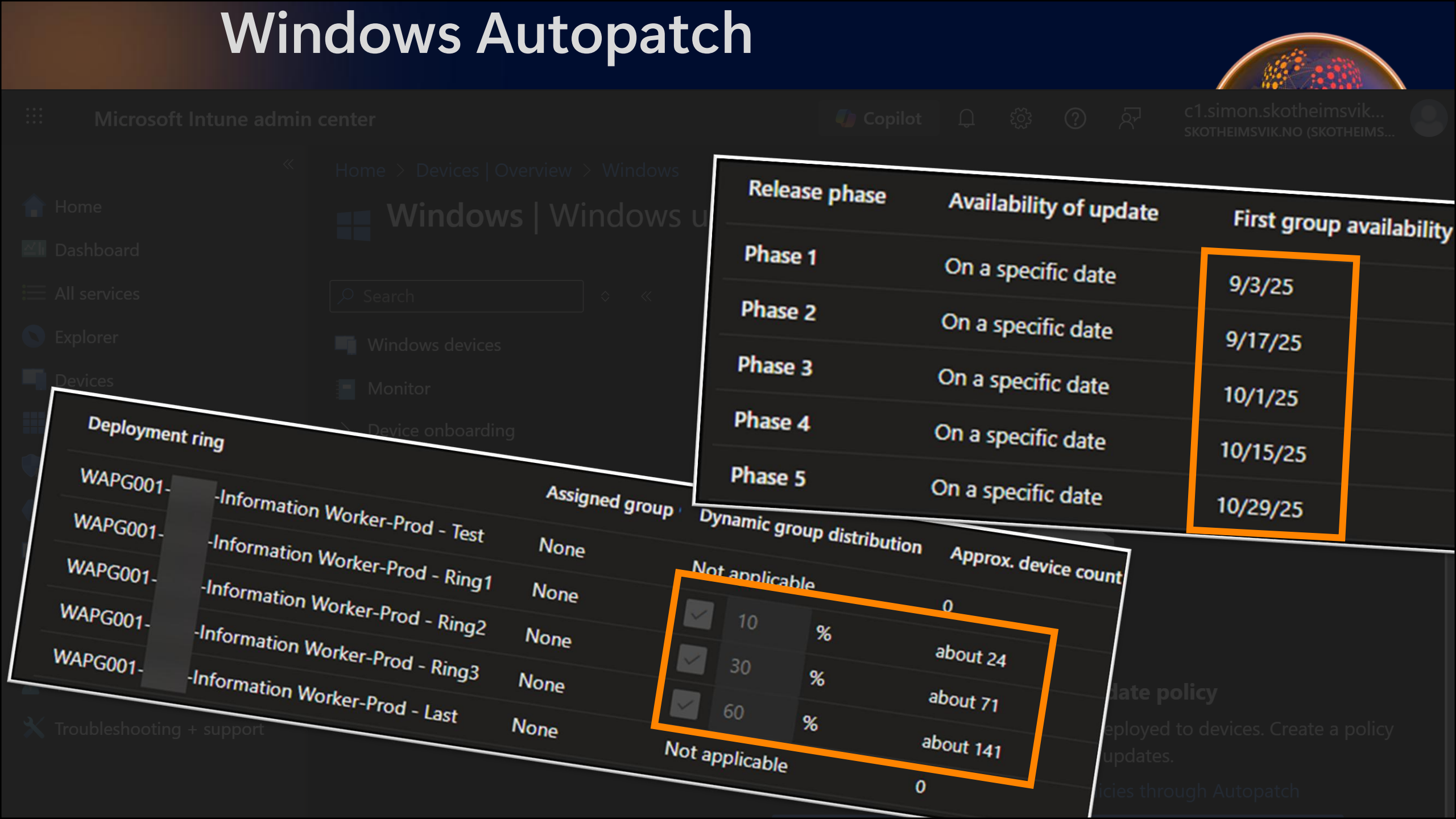
Policies control how Windows updates are deployed to devices. Create a policy to deploy feature updates.

Learn more about managing policies through Autopatch

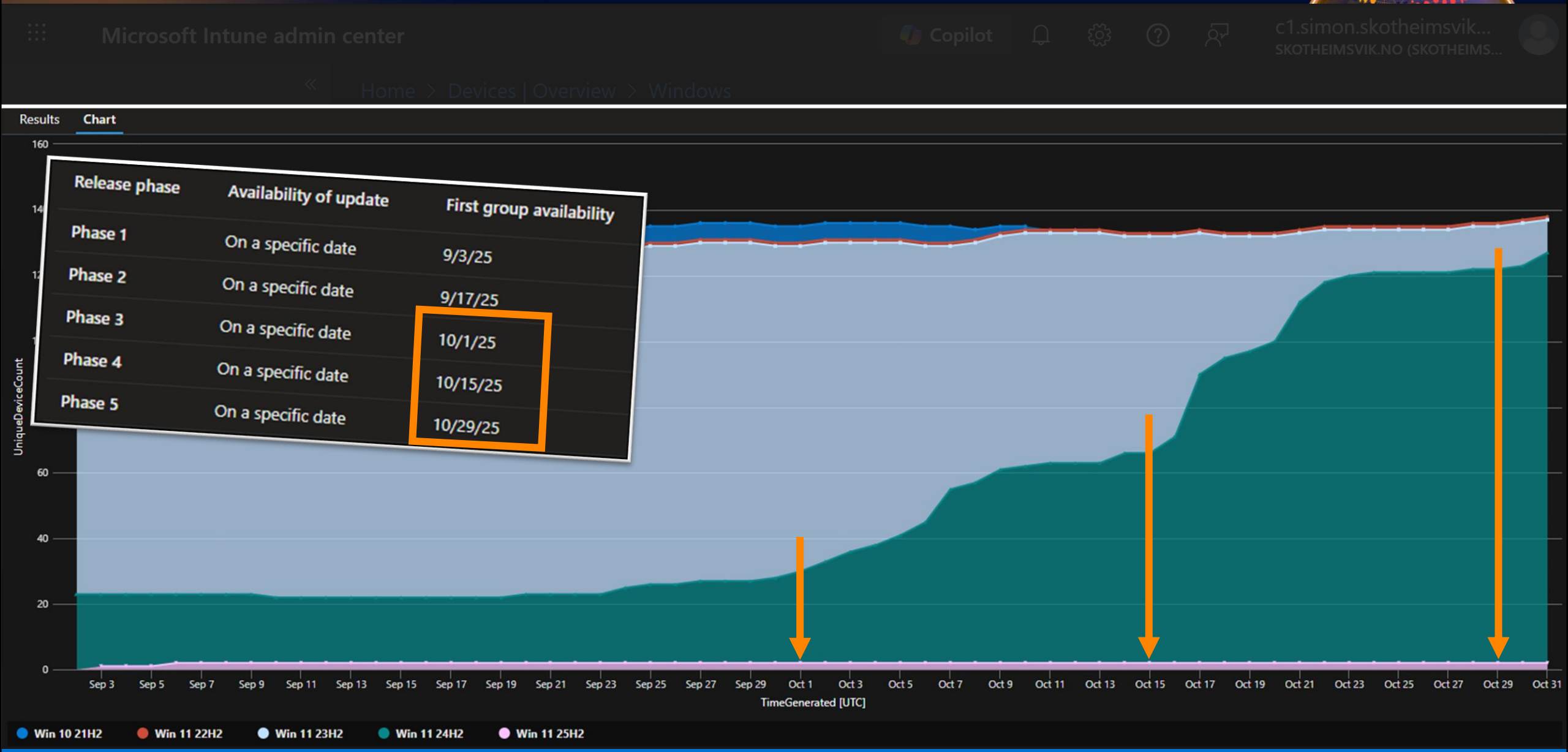
Windows Autopatch



Windows Autopatch



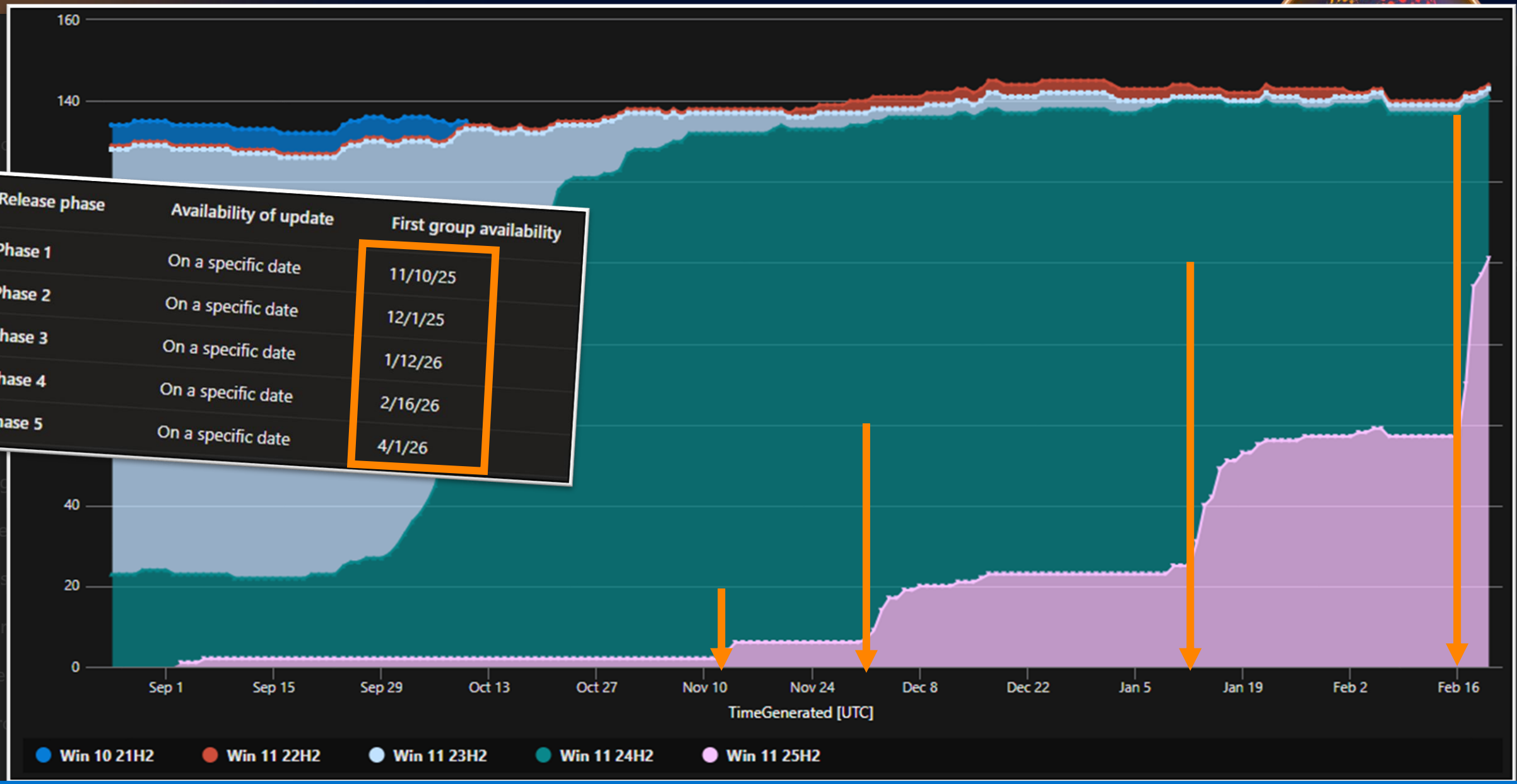
Windows Autopatch



Release phase	Availability of update	First group availability
Phase 1	On a specific date	9/3/25
Phase 2	On a specific date	9/17/25
Phase 3	On a specific date	10/1/25
Phase 4	On a specific date	10/15/25
Phase 5	On a specific date	10/29/25

https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/overview/windows-autopatch-overview

Windows Autopatch



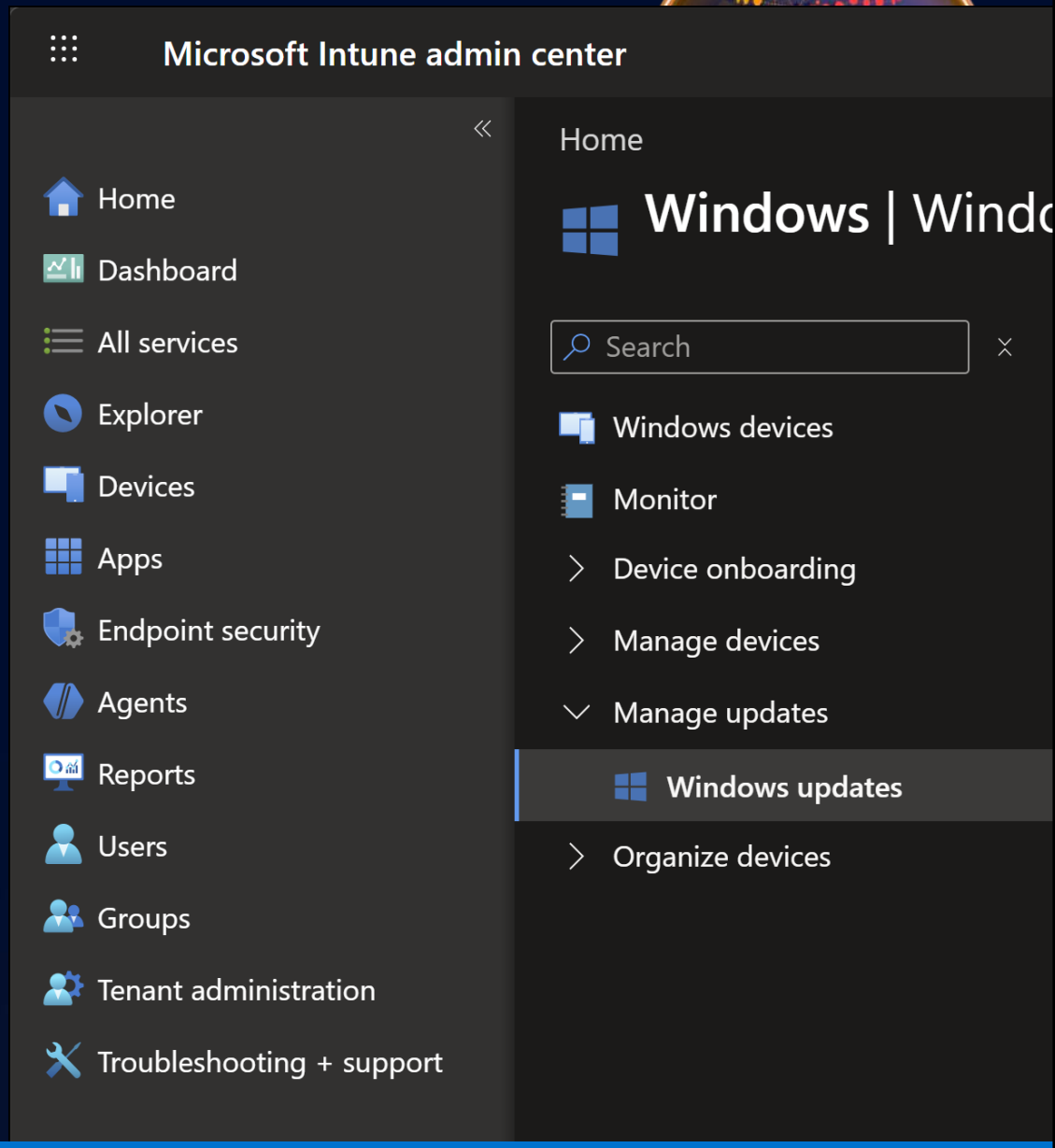
Release phase	Availability of update	First group availability
Phase 1	On a specific date	11/10/25
Phase 2	On a specific date	12/1/25
Phase 3	On a specific date	1/12/26
Phase 4	On a specific date	2/16/26
Phase 5	On a specific date	4/1/26

https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/overview/windows-autopatch-overview

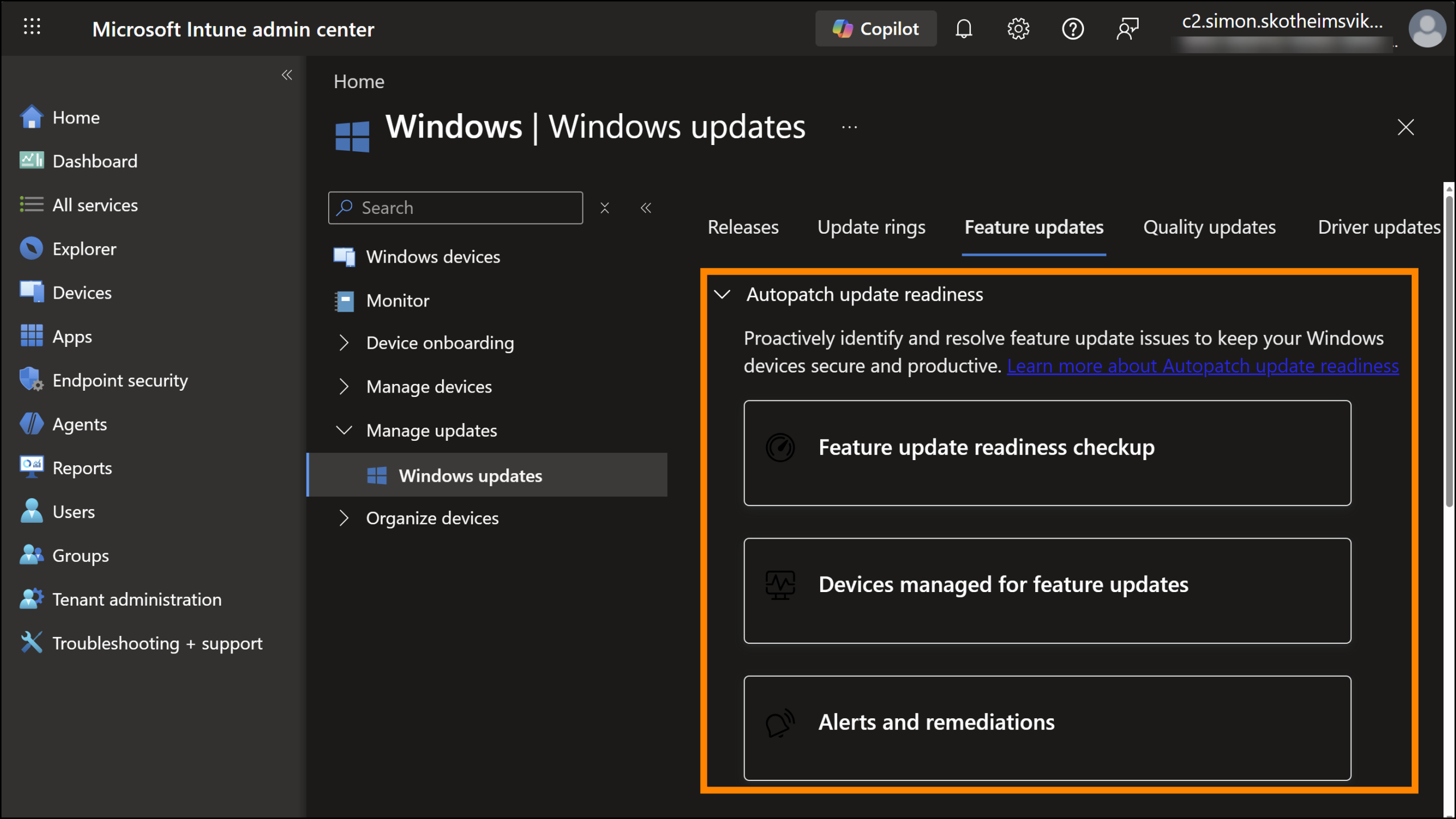
Windows Autopatch

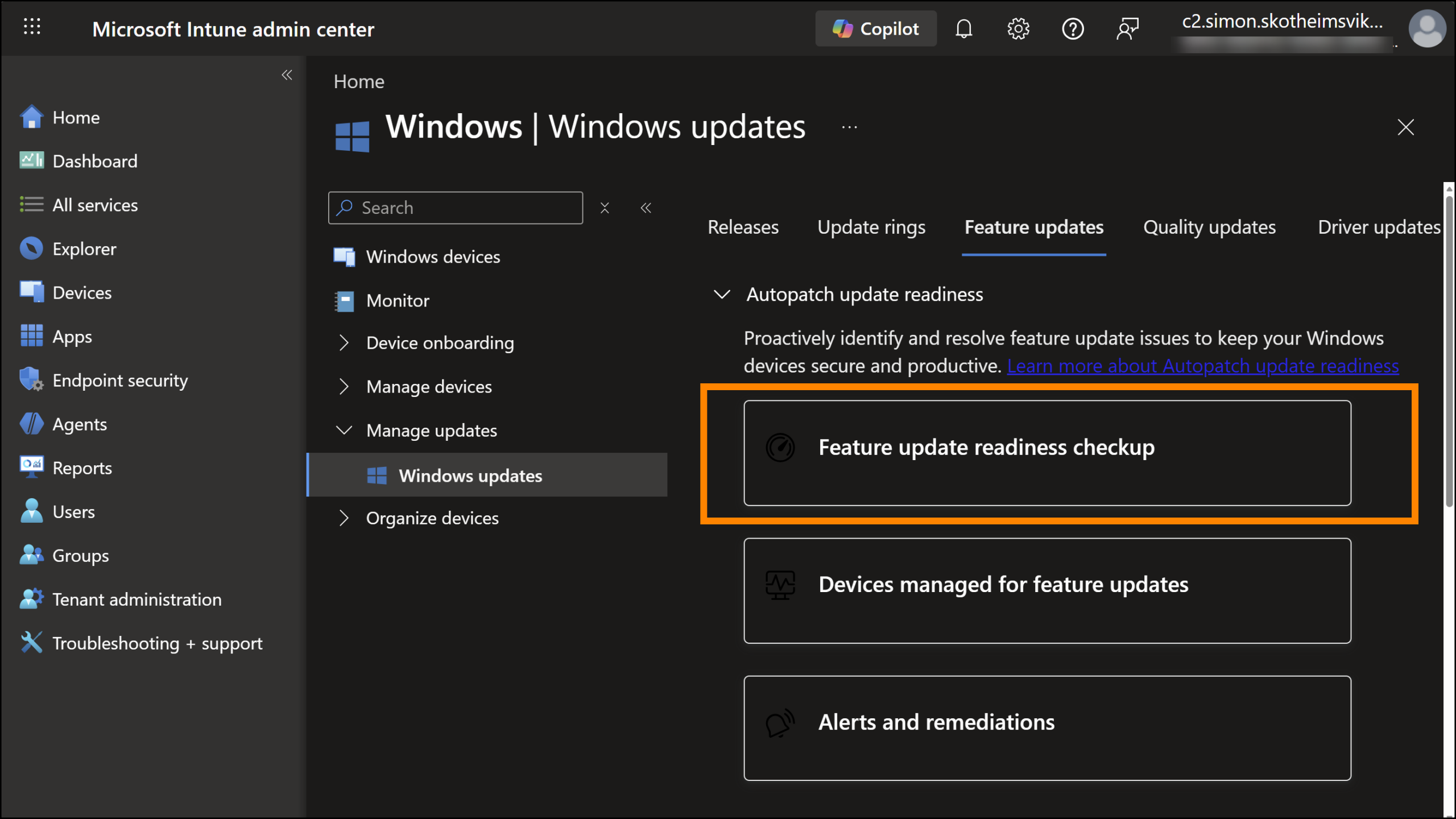
Ignite Announcements

- **Feature Update Readiness:** Automated checks ensure devices meet update prerequisites before rollout.
- **Clear Visibility:** Device journey maps provide step-by-step status updates, actionable alerts, and guided remediations.



https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-autopatch-%E2%80%94-elevate-your-update-experience-for-modern-work/4468111


Microsoft Intune admin center
Copilot
c2.simon.skotheimsvik...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home
Windows | Windows updates
Search
Windows devices
Monitor
Device onboarding
Manage devices
Manage updates
Windows updates
Organize devices
Releases
Update rings
Feature updates
Quality updates
Driver updates
Autopatch update readiness
Proactively identify and resolve feature update issues to keep your Windows devices secure and productive. Learn more about Autopatch update readiness
Feature update readiness checkup
Devices managed for feature updates
Alerts and remediations


Microsoft Intune admin center
Copilot
c2.simon.skotheimsvik...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home
Windows | Windows updates
Search
Windows devices
Monitor
Device onboarding
Manage devices
Manage updates
Windows updates
Organize devices
Releases
Update rings
Feature updates
Quality updates
Driver updates
Autopatch update readiness
Proactively identify and resolve feature update issues to keep your Windows devices secure and productive. Learn more about Autopatch update readiness
Feature update readiness checkup
Devices managed for feature updates
Alerts and remediations

Autopatch update readiness | Update readiness checkup

Update type: Feature update

Target release: Windows 11, version 25H2

Run checkup

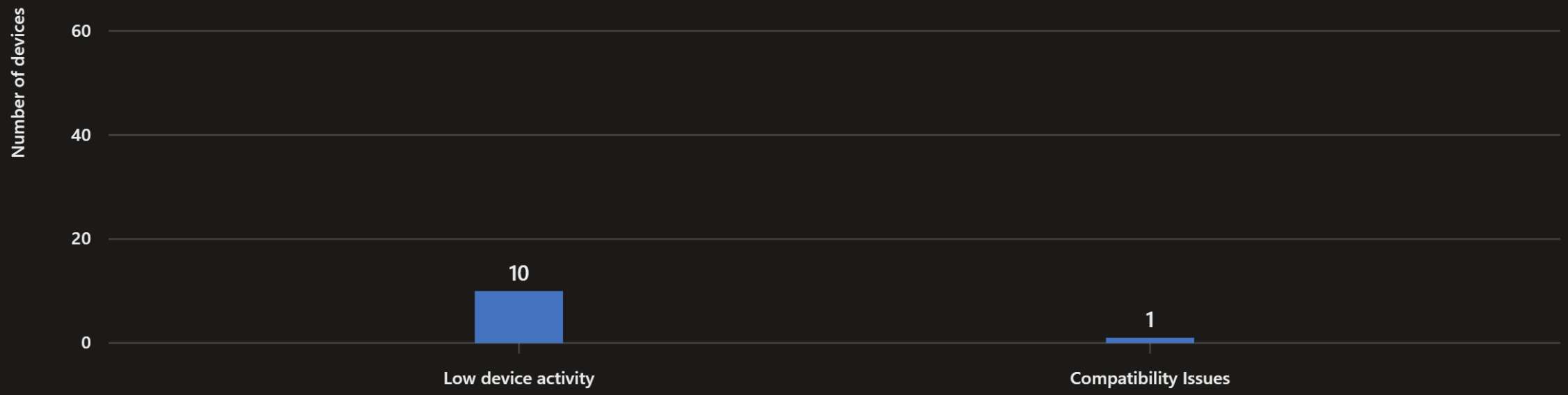
Readiness checkup overview

133
Checkup passed for feature update
View devices

10
Checkup failed for feature update
View devices

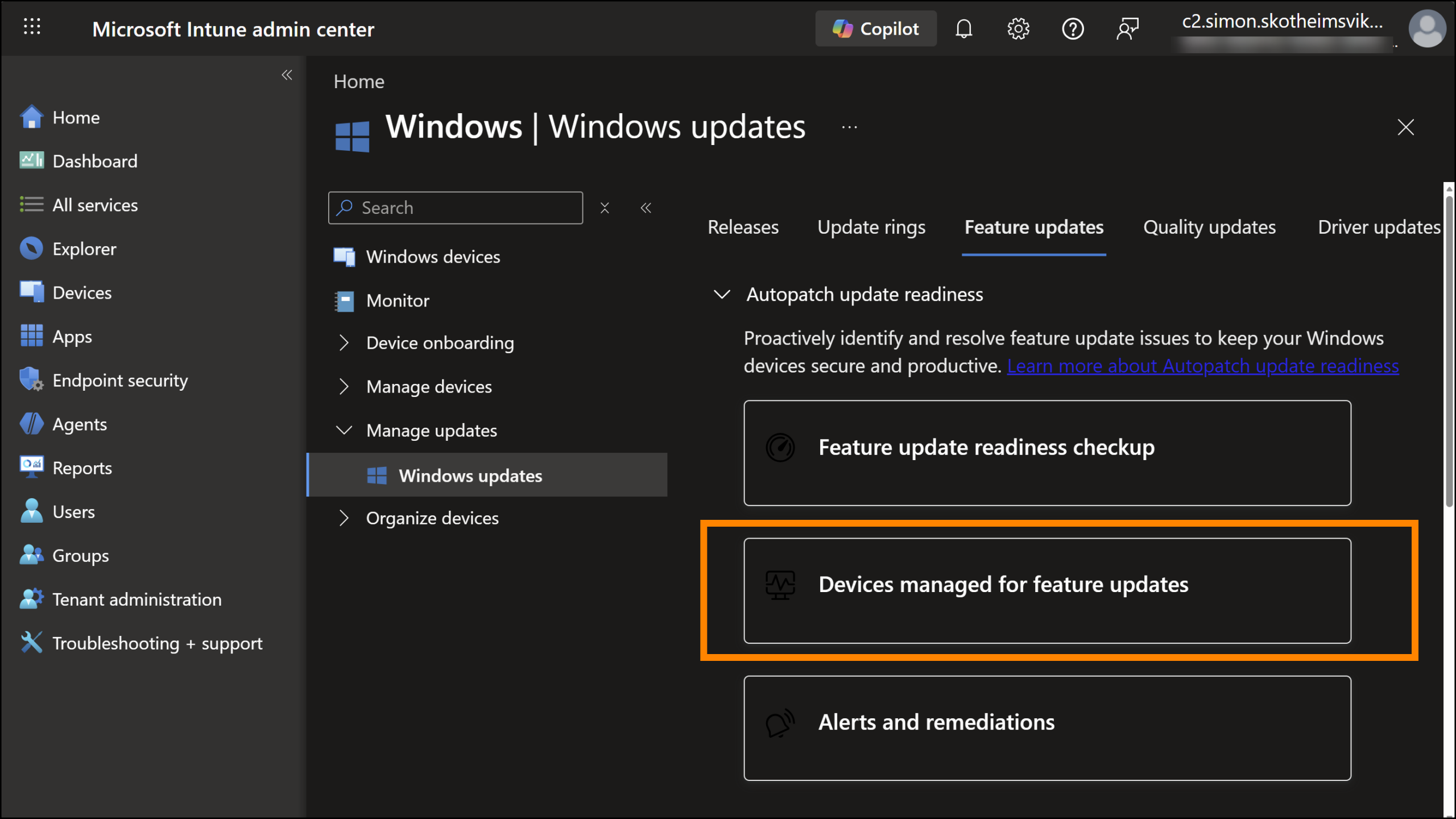
26
Target OS version already installed

169
Total number of devices assessed



Recommended Actions

Issue	Description	Affected Dev...	Recommended Actions
Low device activity	The affected devices have not checked in with Intune in the last 28 days and show minimal or no recent activity.	10	Check device usage and connectivity. If the devices are no longer in use, retire or update their records in Intune.
Compatibility Issues	Your device does not satisfy one or more of the minimum requirements needed to upgrade to the target Windows OS version.	1	Review the specific compatibility issues applicable to your devices here.


Microsoft Intune admin center
Copilot
c2.simon.skotheimsvik...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home
Windows | Windows updates
Search
Windows devices
Monitor
Device onboarding
Manage devices
Manage updates
Windows updates
Organize devices
Releases
Update rings
Feature updates
Quality updates
Driver updates
Autopatch update readiness
Proactively identify and resolve feature update issues to keep your Windows devices secure and productive. Learn more about Autopatch update readiness
Feature update readiness checkup
Devices managed for feature updates
Alerts and remediations

Feature update journey

View feature update trending and point in time update state. Learn more about Windows feature updates

Target release: Windows 11, version 25H2

Policy: Windows Autopatch - DSS policy - Windows 11 25H2 - P...

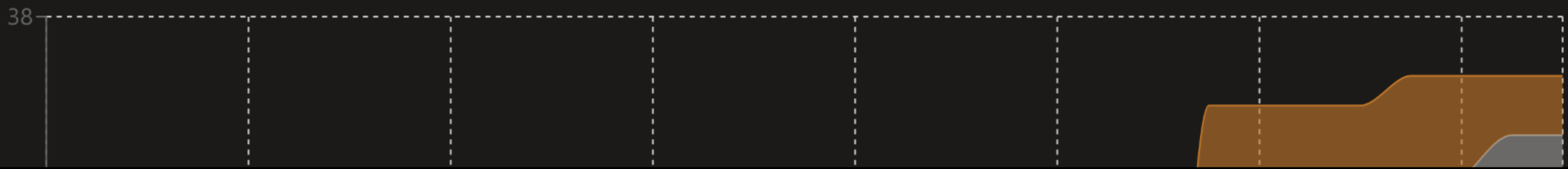
Generate

Status breakdown

Request Received	In Progress	Installed	Failed	Cancelled	No Data	Total Devices
17	1	8	0	4	4	17

State trending

Time range: Last 30 days



Request Received	In Progress	Installed	Failed	Cancelled	No Data	Total Devices
17	1	8	0	4	4	17

State trending

Time range: **Last 30 days**

Microsoft Intune admin center

Copilot

c2.simon.skotheimsvik...

State point in time

Showing today's state breakdown of devices for each stage in the deployment process.

Request Received	Download Start	Install Start	Restart Required	Installed	Failed Download	Failed Install	Failed Reboot	Client C
17	1	6	10	8	0	0	0	4

Update timeline |

Device details

Device name

OS version
10.0.26200.8037

Model
21QL0040MX

OS build
26200.8037

Serial number
PF5X6055

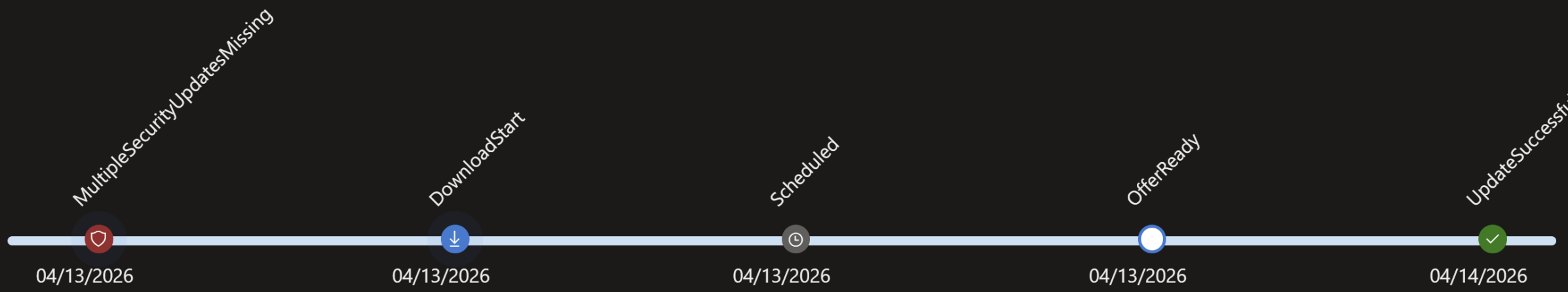
Target version
Windows 11, version 25H2

Last sync time
4/16/2026, 8:17:43 AM

Device timeline

Time: 04/13/2026 - 04/14/2026

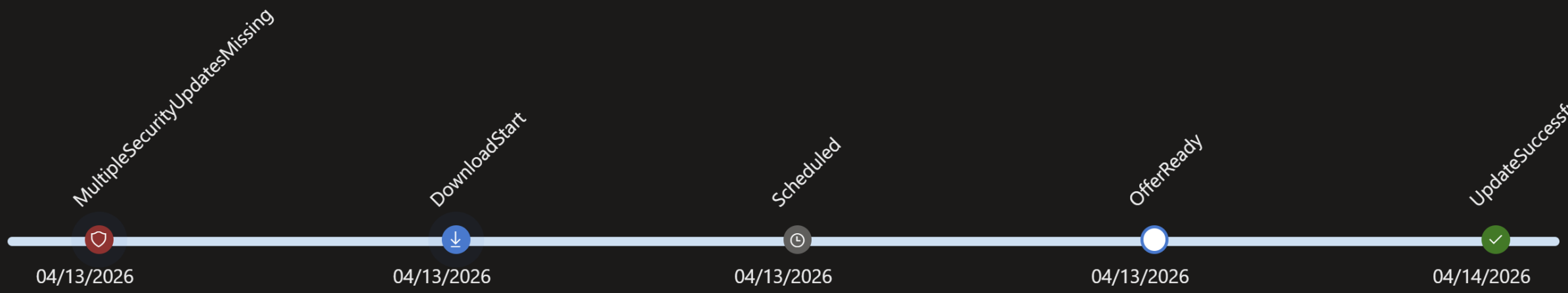
Add filters



04/13/2026, 4:00 PM

Device timeline

Time: 04/13/2026 - 04/14/2026
Add filters



04/13/2026, 4:00 PM

Alert

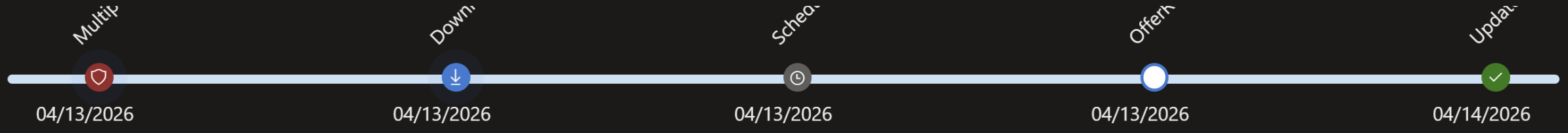
installed a Windows cumulative update in more than 60 days and are missing important security updates.

less

5 events

Refresh Export Columns

5 events



04/13/2026, 4:00 PM

Alert

installed a Windows cumulative update in more than 60 days and are missing important security updates.

less

5 events

Refresh Export Columns 5 events

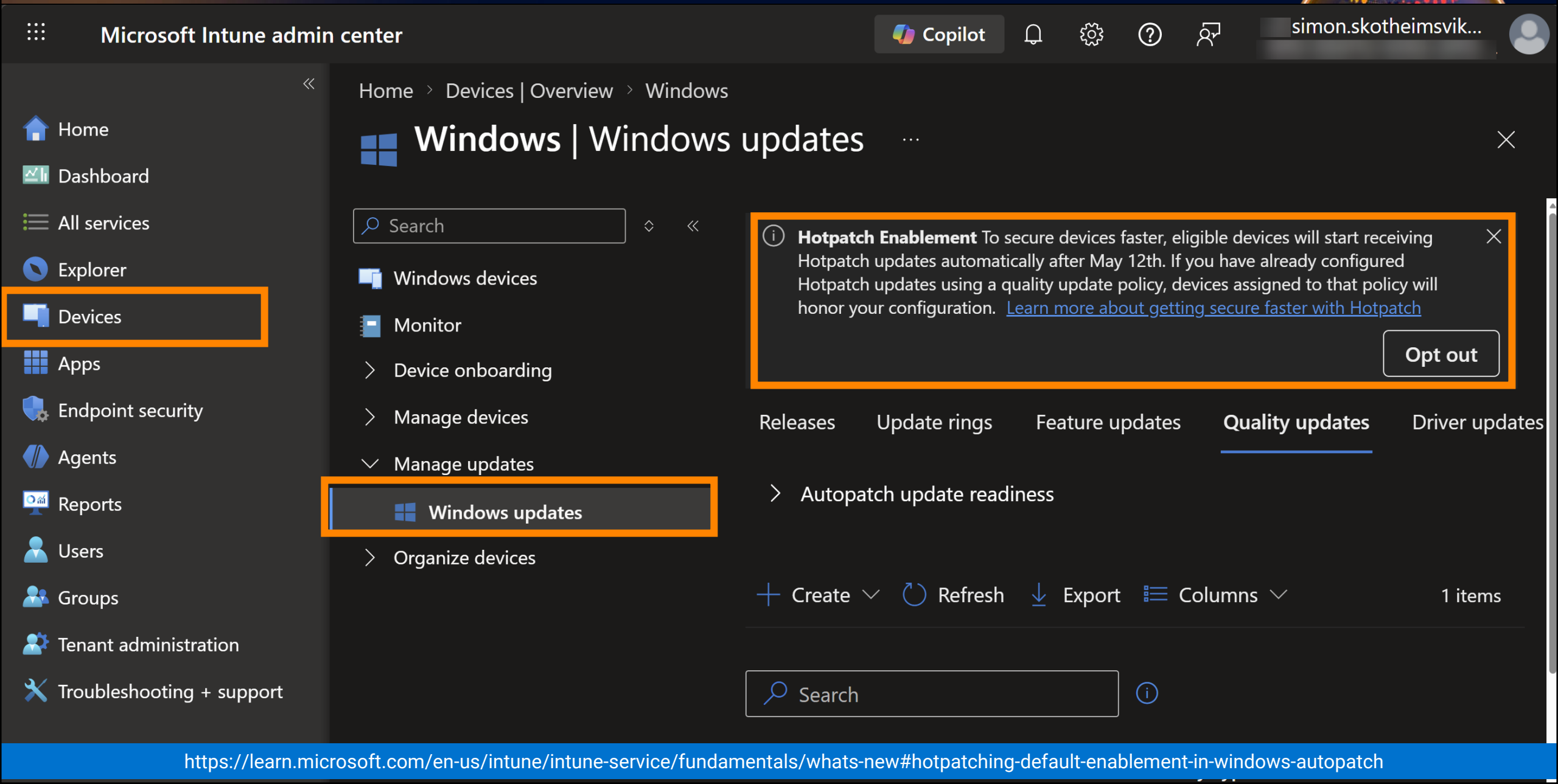
Event Time	Event Type	Status
4/13/2026 4:00:00 PM	Alert	MultipleSecurityUpdatesMissing
4/13/2026 4:54:43 PM	ClientEvent	DownloadStart
4/13/2026 5:16:53 PM	ServiceState	Scheduled
4/13/2026 5:16:54 PM	ServiceState	OfferReady
4/14/2026 12:39:29 PM	ClientEvent	UpdateSuccessful

4

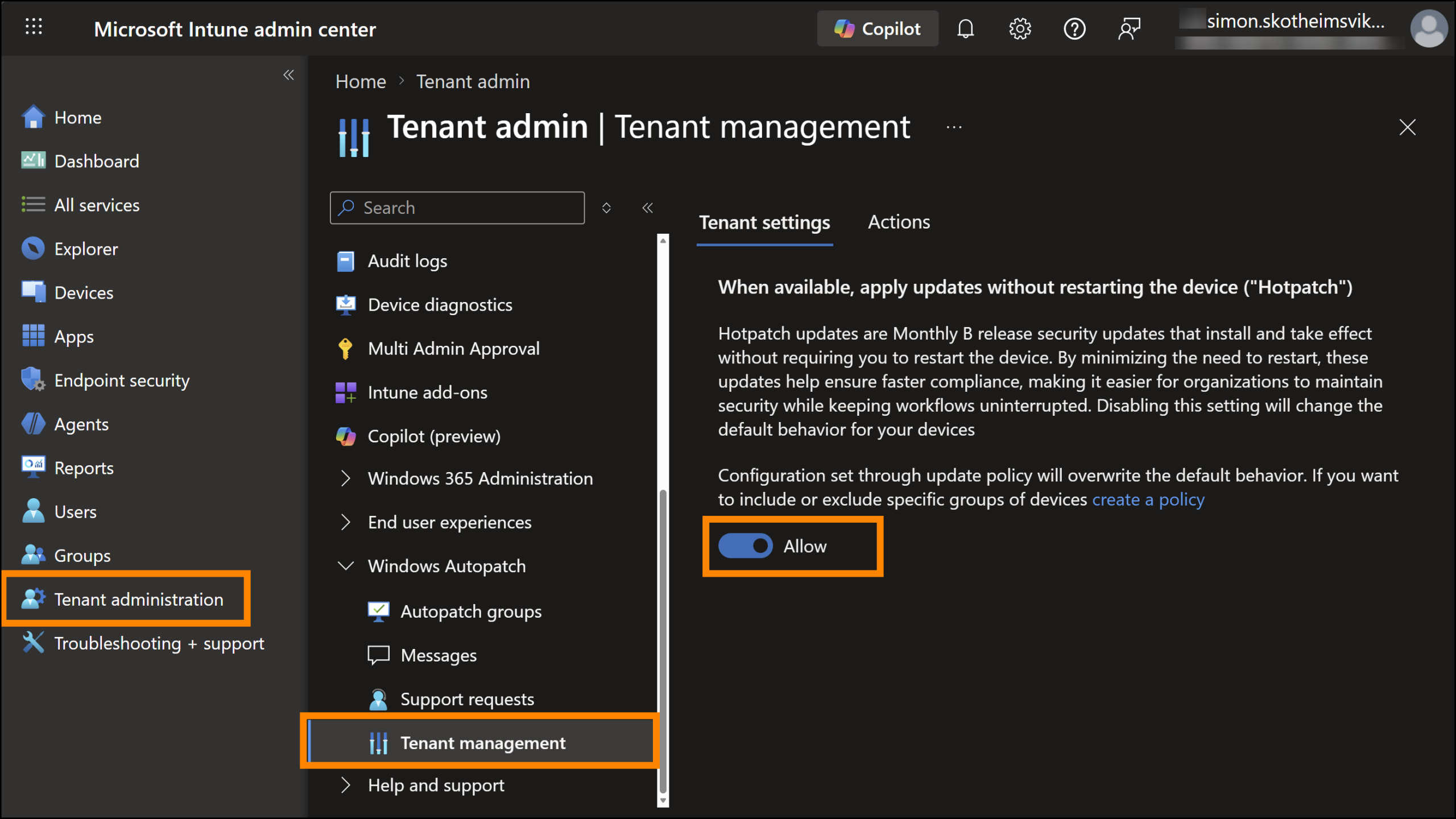
Hotpatch

How fast are you patching?

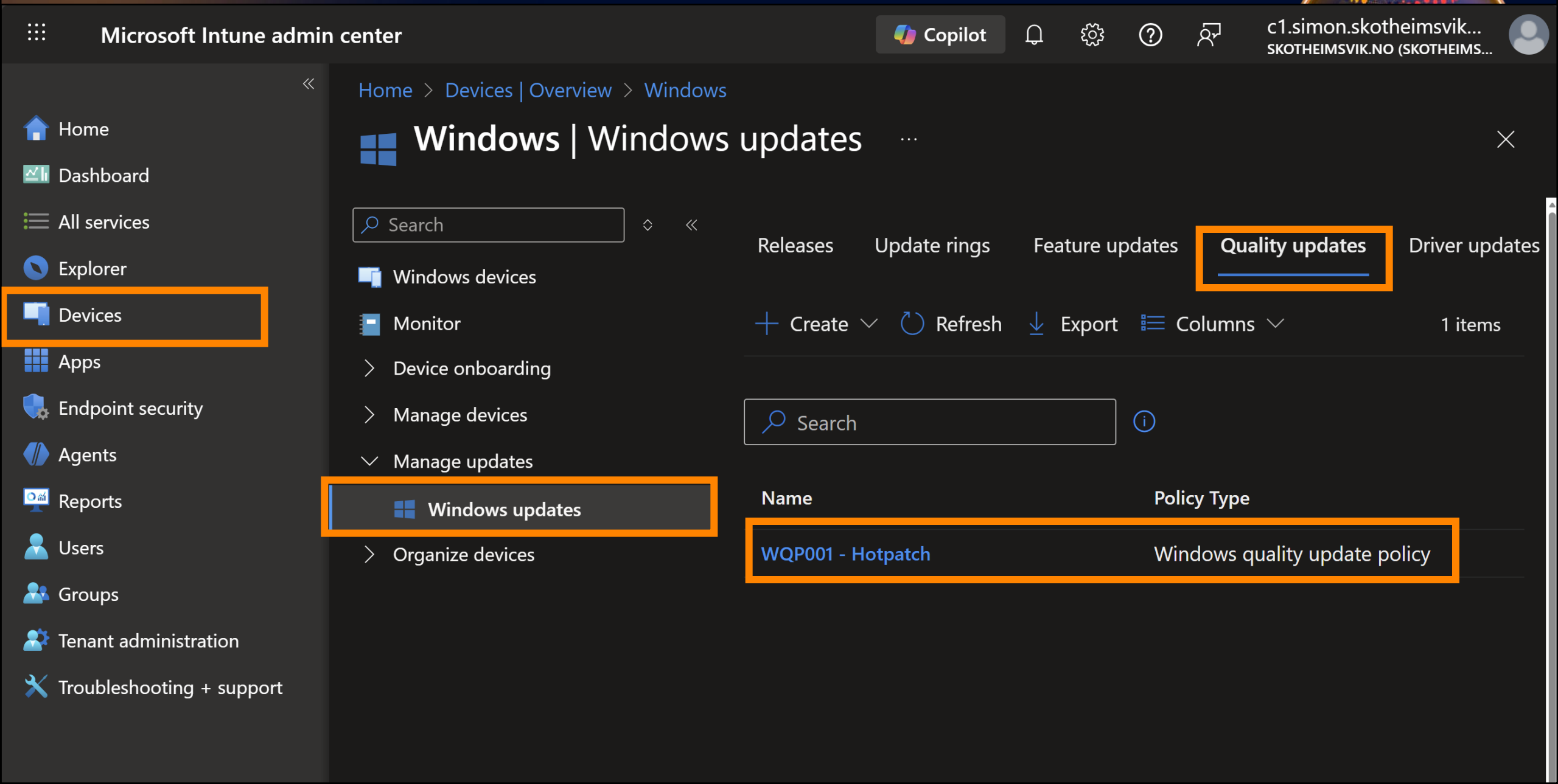
Windows Hotpatch



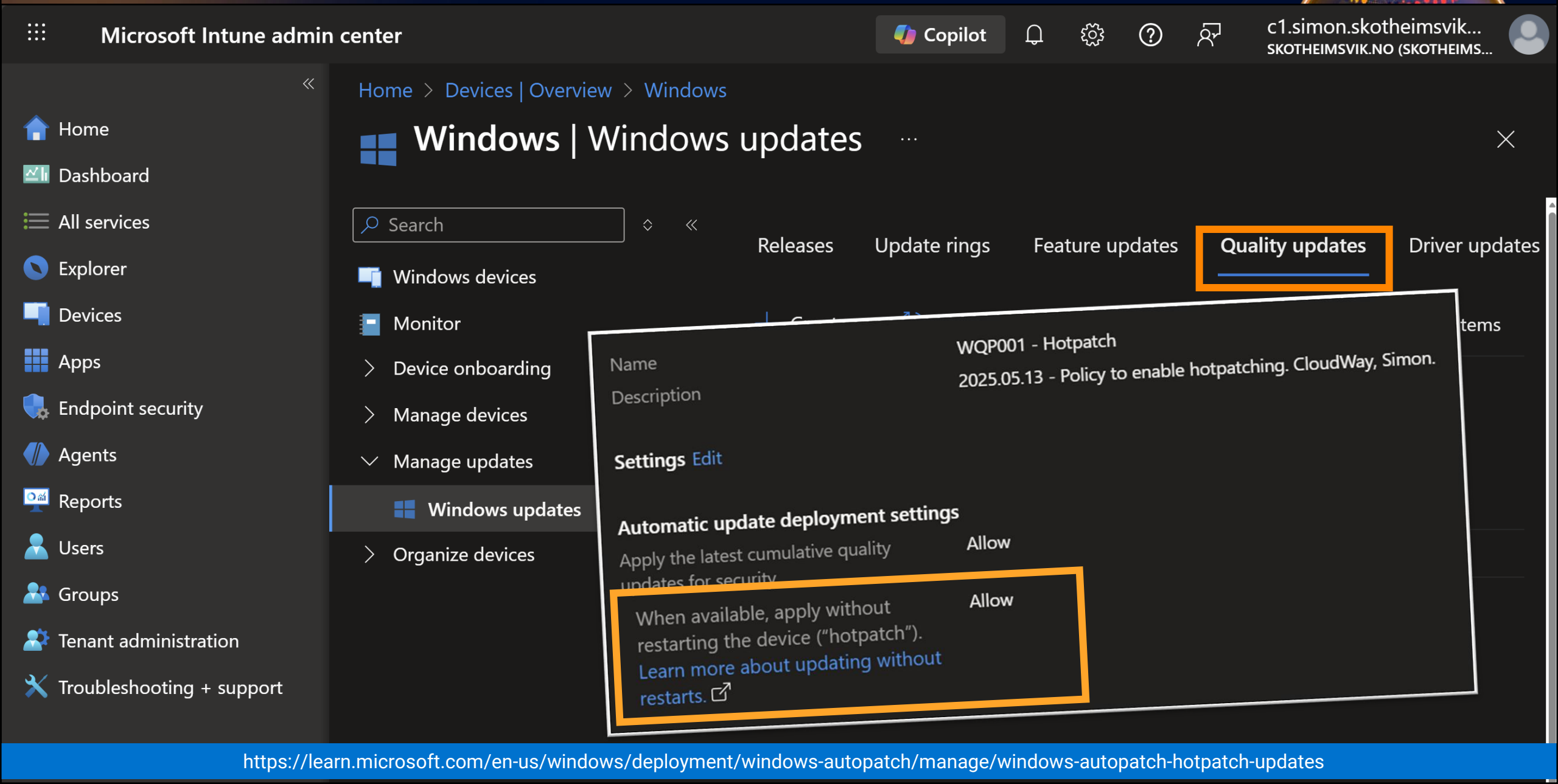
https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#hotpatching-default-enablement-in-windows-autopatch


Microsoft Intune admin center
Copilot
simon.skotheimsvik...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Tenant management
Search
Audit logs
Device diagnostics
Multi Admin Approval
Intune add-ons
Copilot (preview)
Windows 365 Administration
End user experiences
Windows Autopatch
Autopatch groups
Messages
Support requests
Tenant management
Help and support
Tenant settings
Actions
When available, apply updates without restarting the device ("Hotpatch")
Hotpatch updates are Monthly B release security updates that install and take effect without requiring you to restart the device. By minimizing the need to restart, these updates help ensure faster compliance, making it easier for organizations to maintain security while keeping workflows uninterrupted. Disabling this setting will change the default behavior for your devices
Configuration set through update policy will overwrite the default behavior. If you want to include or exclude specific groups of devices create a policy
Allow

Windows Hotpatch



Windows Hotpatch



https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/manage/windows-autopatch-hotpatch-updates

Windows Hotp

Microsoft Intune admin center

Home > Devices | Overview >

Windows | Wi

Home
Dashboard
All services
Explorer
Devices
Apps

Search

Windows devices
Monitor

Name
Description
WQP001 - Hotpatch
2025.05.13 - Policy to enable hotpatching. CloudWay, Simon.

Settings Edit

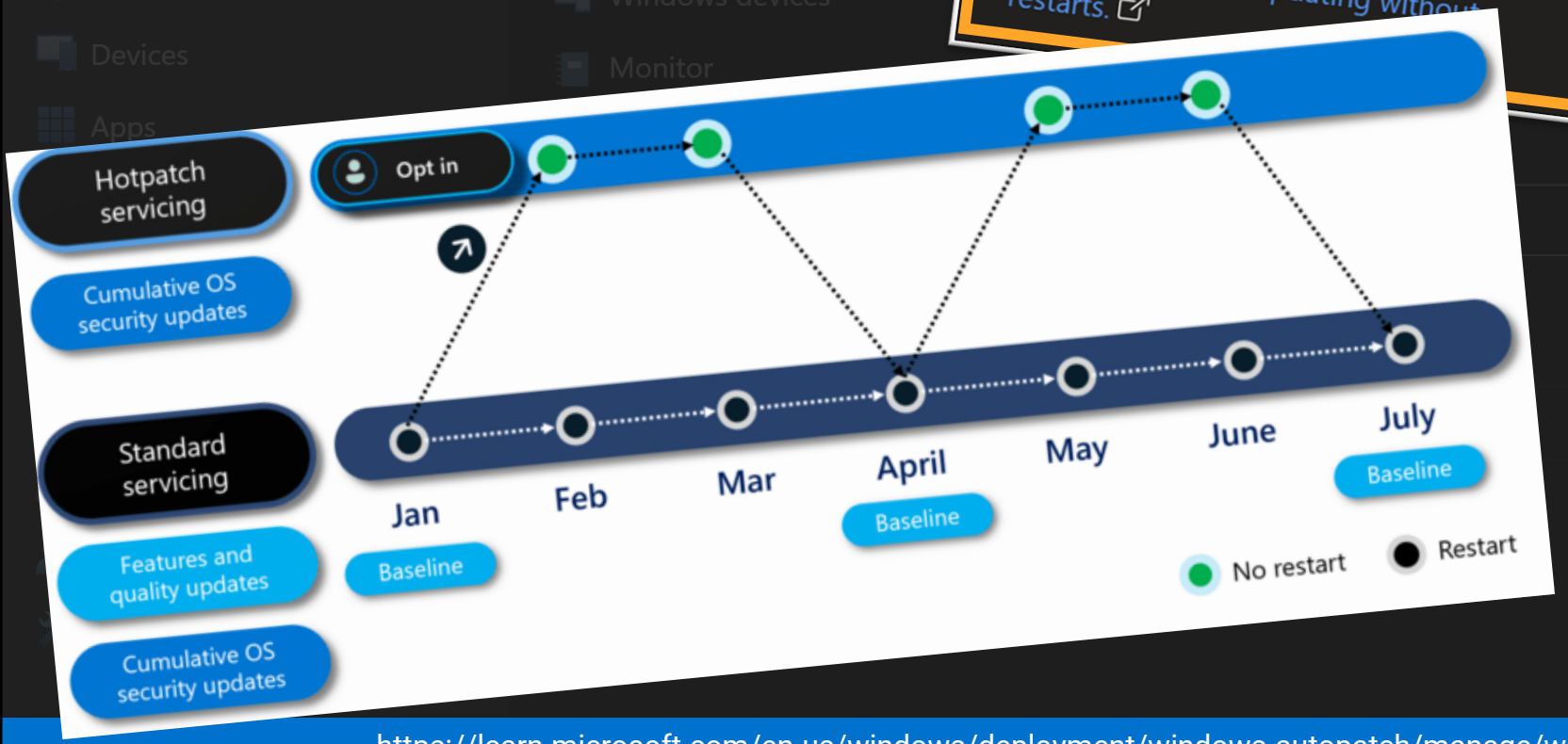
Automatic update deployment settings

Apply the latest cumulative quality updates for security — Allow

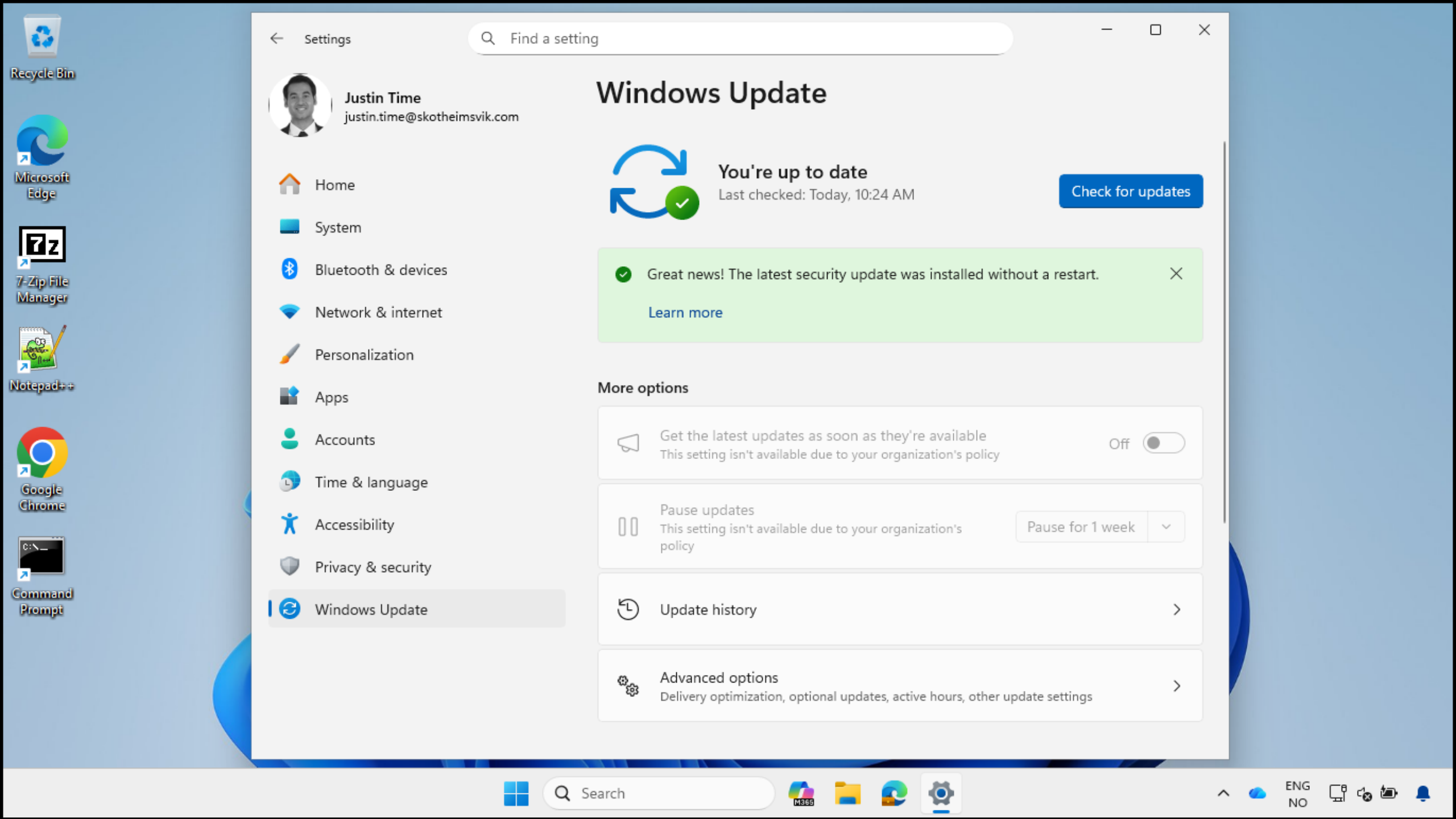
When available, apply without restarting the device ("hotpatch"). Learn more about updating without restarts. — Allow

Policy Type

Windows quality update policy



https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/manage/windows-autopatch-hotpatch-updates


Recycle Bin
Microsoft Edge
7-Zip File Manager
Notepad++
Google Chrome
Command Prompt
Settings
Find a setting
Justin Time
justin.time@skotheimsvik.com
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Accessibility
Privacy & security
Windows Update
Windows Update
You're up to date
Last checked: Today, 10:24 AM
Check for updates
Great news! The latest security update was installed without a restart.
Learn more
More options
Get the latest updates as soon as they're available
This setting isn't available due to your organization's policy
Off
Pause updates
This setting isn't available due to your organization's policy
Pause for 1 week
Update history
Advanced options
Delivery optimization, optional updates, active hours, other update settings
Search
ENG
NO

Windows Hotp

Microsoft Intune admin center

Home > Devices | Overview >

Windows | Wi

Home
Dashboard
All services
Explorer
Devices
Apps

Search

Windows devices
Monitor

Name
Description
WQP001 - Hotpatch
2025.05.13 - Policy to enable hotpatching. CloudWay, Simon.

Settings Edit

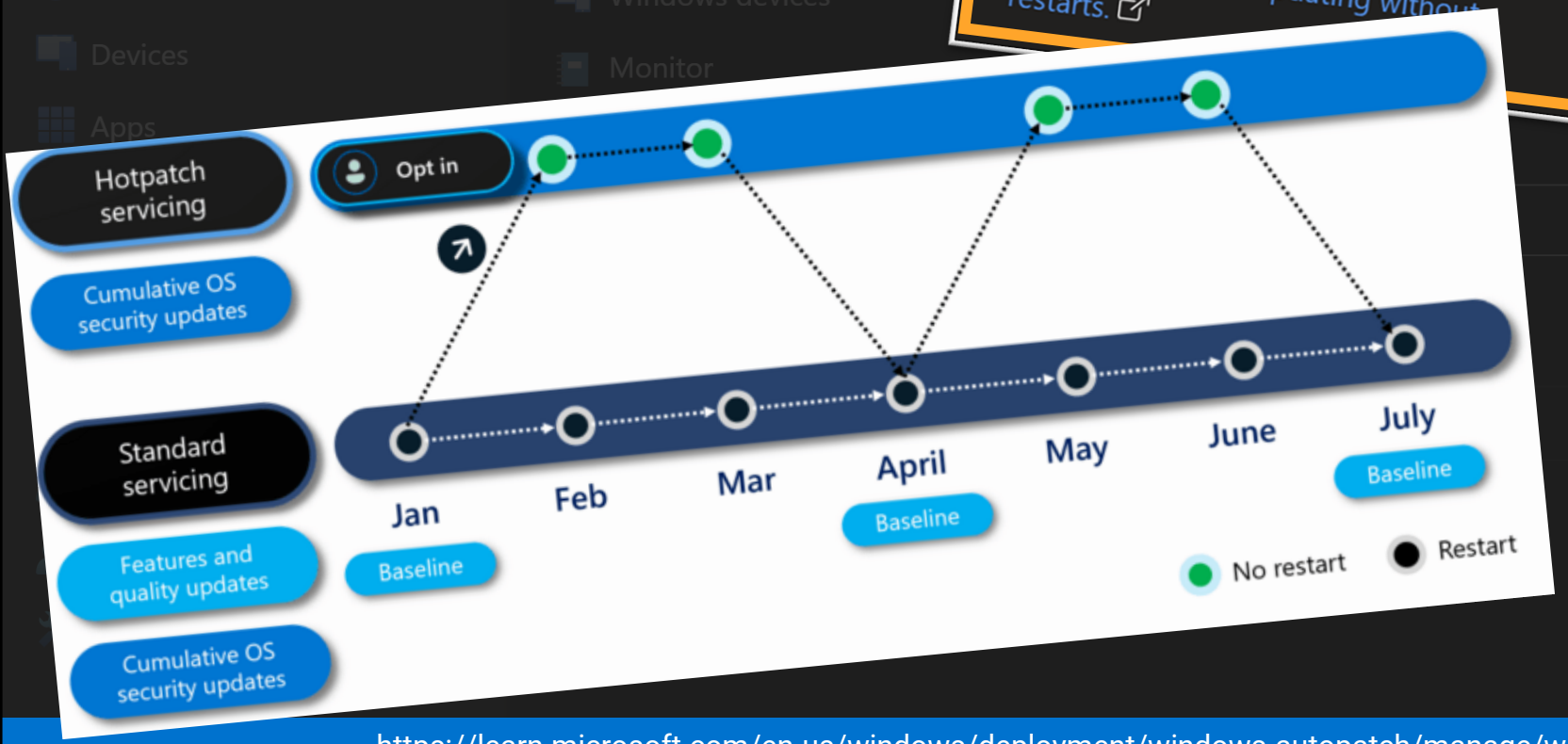
Automatic update deployment settings

Apply the latest cumulative quality updates for security — Allow

When available, apply without restarting the device ("hotpatch"). Learn more about updating without restarts. — Allow

Policy Type

Windows quality update policy



https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/manage/windows-autopatch-hotpatch-updates

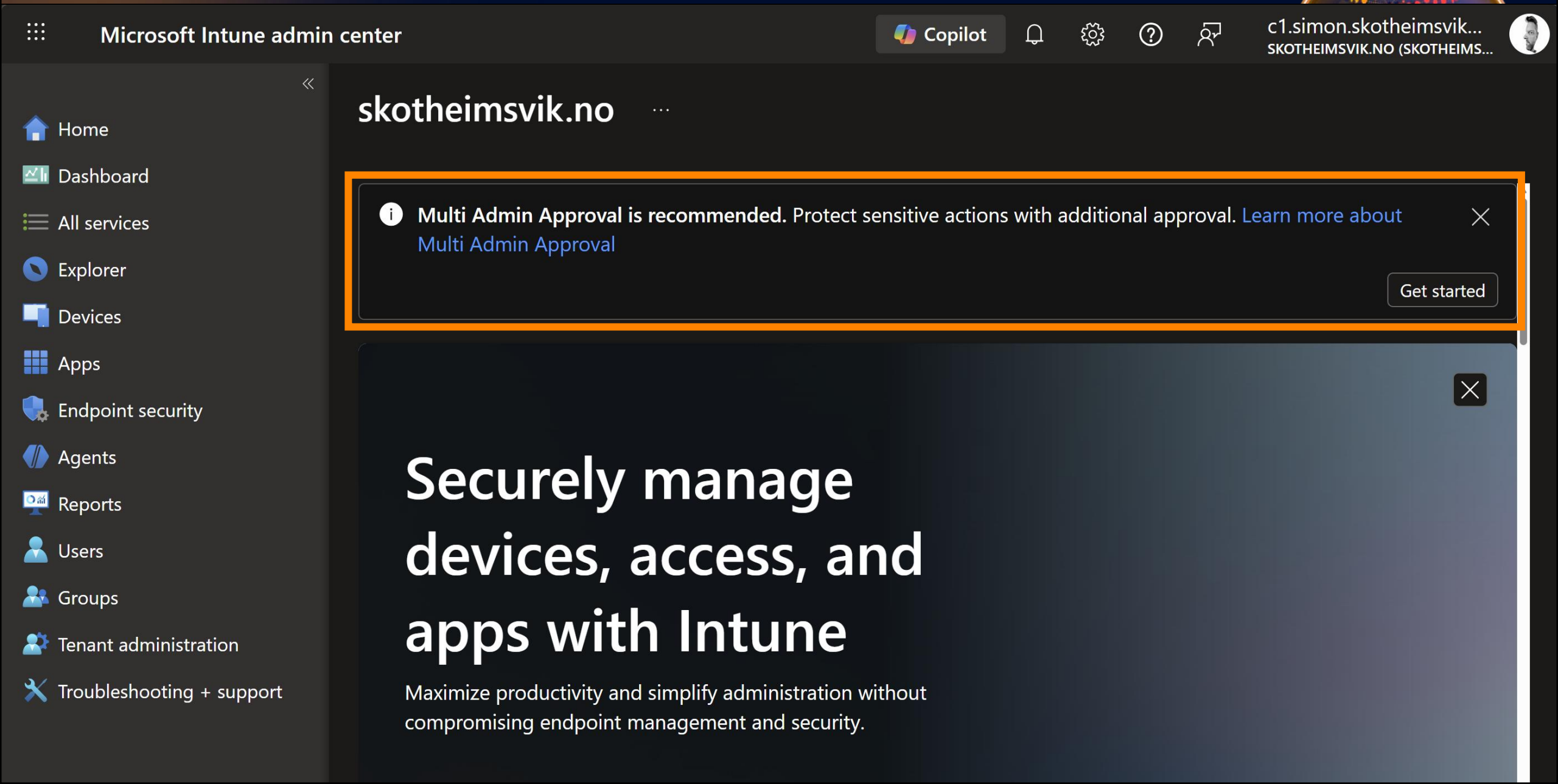
5 Multi Admin Approval

The MFA for your device operations

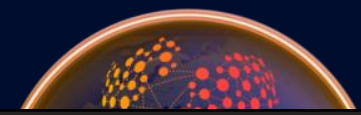
Nov 10 2025

https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/multi-admin-approval

Multi Admin Approval



Multi Admin Approval



Microsoft Intune admin center

Copilot

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

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

Home > Tenant admin

Tenant admin | Multi Admin Approval

Search

- Connectors and tokens
- Assignment filters
- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings
- Audit logs
- Device diagnostics
- Multi Admin Approval
- Alerts
- Intune add-ons
- Cloud PC encryption type

All requests | My requests | Access policies

Access policies allow you to control which tasks and actions need approval along with the specific approval groups

Create | Refresh

Search by name | Add filter

Showing 0 to 0 of 0 records | < Previous | Page 0 of 0 | Next >

Name	Policy type	Policy platform
There are no policies to view		

Multi Admin Approval

Microsoft Intune admin center

Copilot

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

Create an access policy

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

1 Basics 2 Approvers 3 R...

Name *

Description

Policy type * ⓘ

App
Device delete
Device retire
Device wipe
Role
Script
Tenant configuration

Device wipe

A remote device action policy will limit actions on specific action like delete, retire or wipe for single device or bulk devices in admin portal or Graph APIs.

Multi Admin Approval

Microsoft Intune admin center

Copilot

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

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

Home > Tenant admin | Multi Admin Approval >

Create an access policy

Basics | 2 Approvers | 3 Review + submit for approval

Members of groups you add here can approve requests that need more than one admin to approve

Included groups

Add groups

Groups	Status	Remove
AZ-Intune-Multi Admin Approval	Active	Remove

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

Create an access policy

Basics ✓ Approvers ✓ 3 Review + submit for approval

Summary

⚠ Before this resource can be created, it must be approved by another admin. Before you can submit this request, you must enter your business justification.

Basics

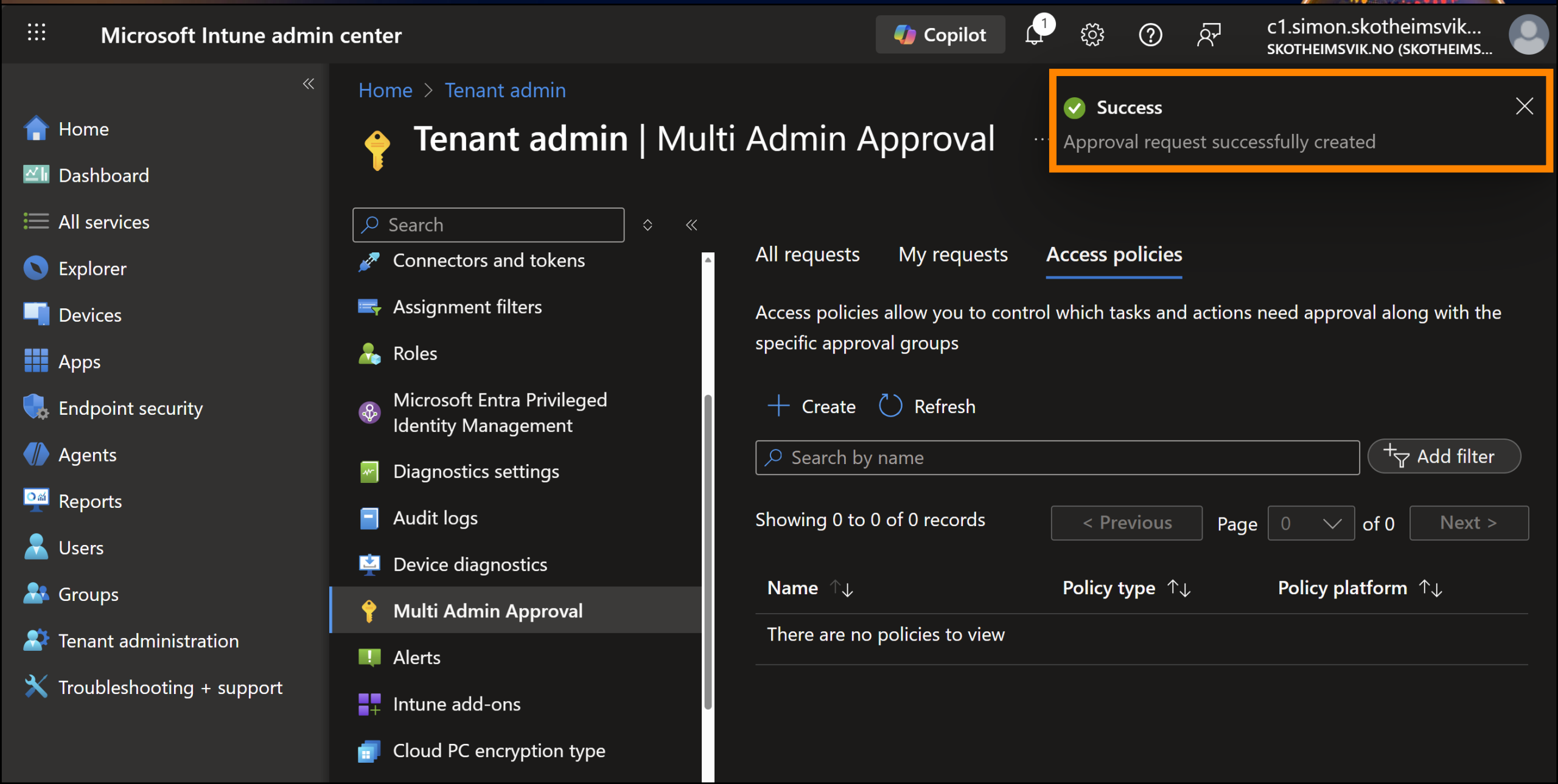
Name	MAA001 - Device Wipe
Description	Multi Admin Approval required for wiping devices.
Policy type	Device wipe
Policy platform	All platforms

Business justification *

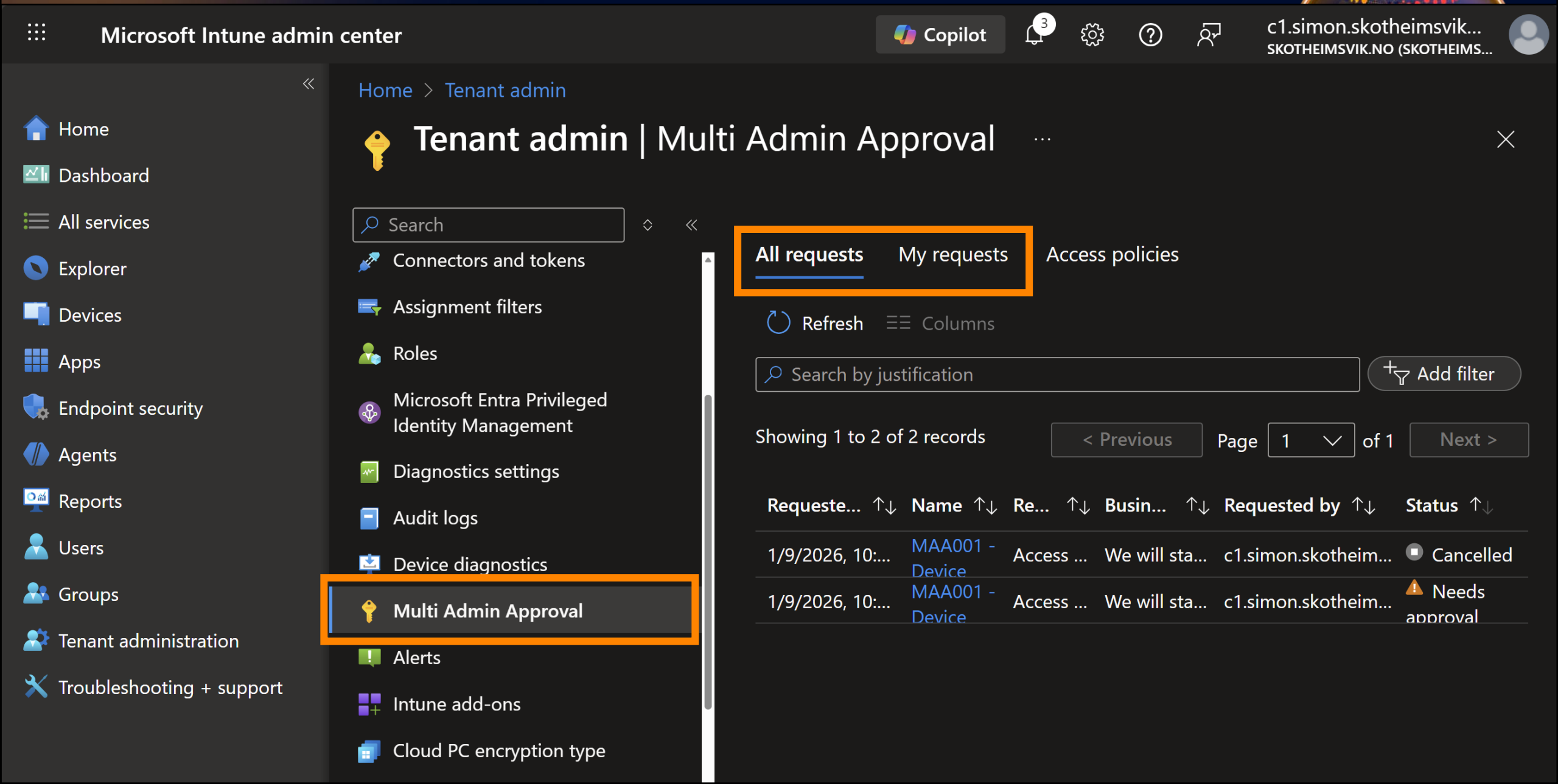
We will start with multi admin approval for device wipes after last weeks incident of accidental CEO wipe

Previous | Submit for approval

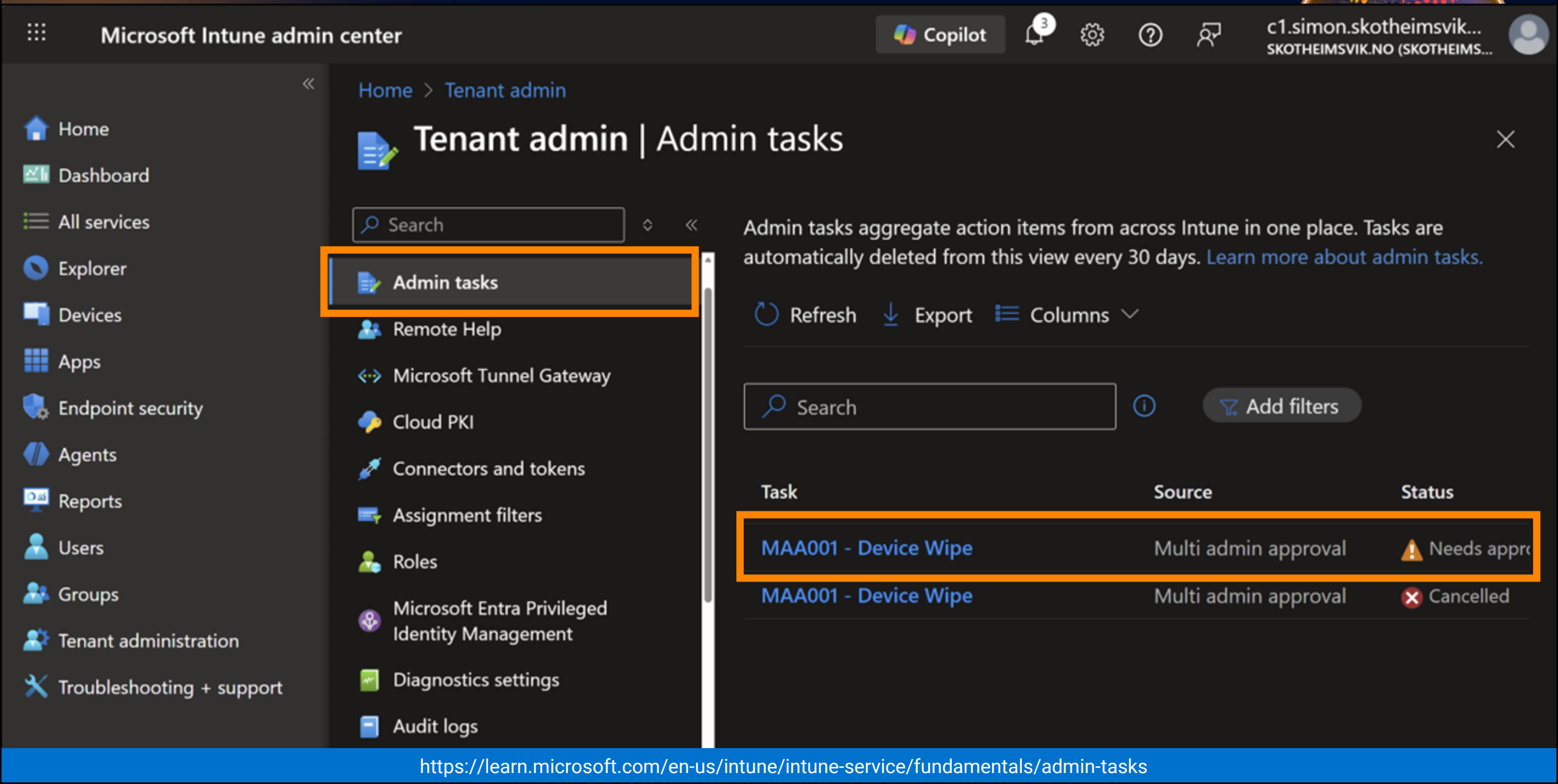
Multi Admin Approval



Multi Admin Approval

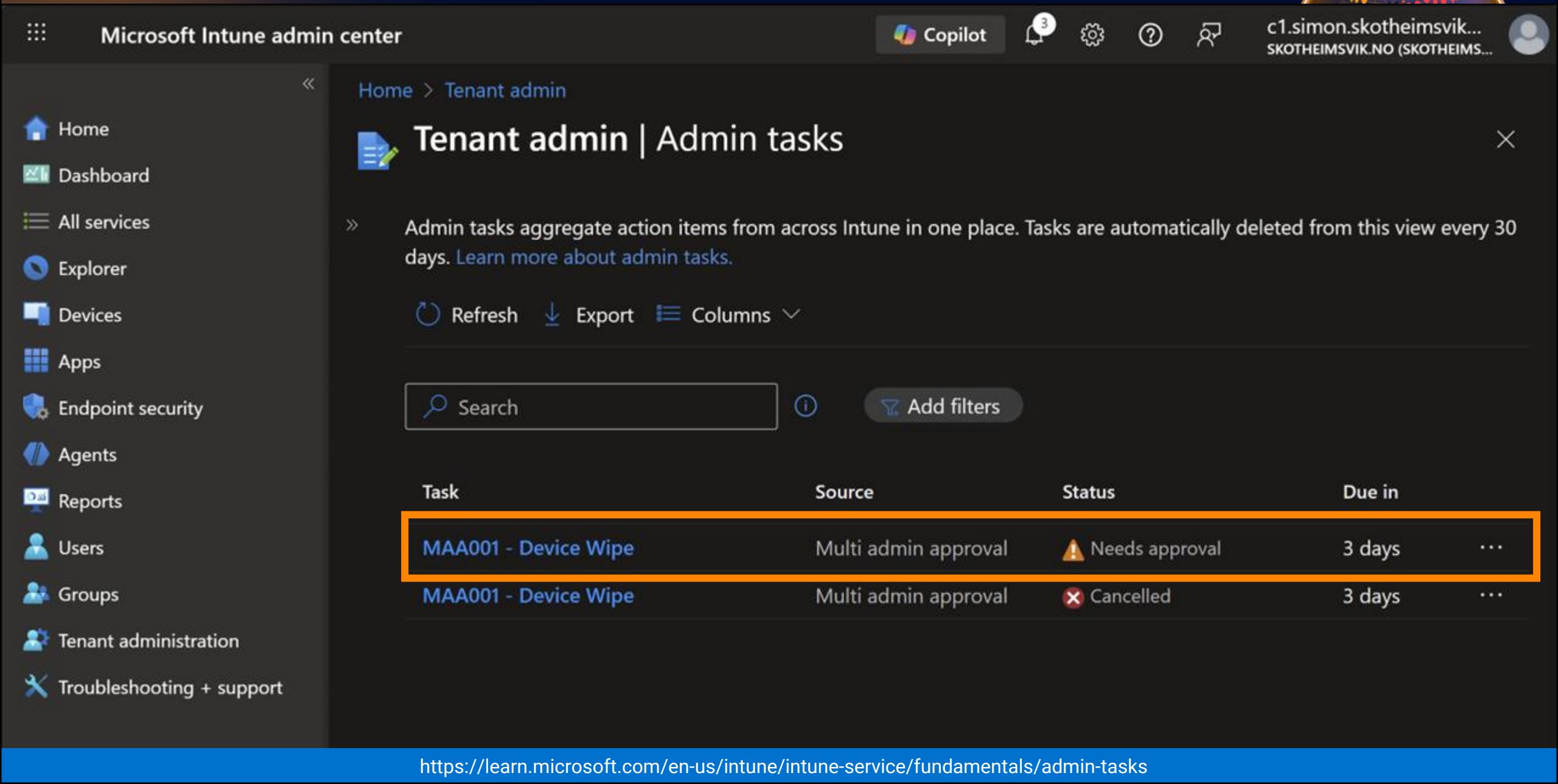


Multi Admin Approval



https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/admin-tasks

Multi Admin Approval



https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/admin-tasks

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

MAA001 - Device Wipe - Create

Multi admin approval request

Review the changes below and take the appropriate action.

Request information

Resource type	Access policy
Operation	Create
Requested by	c1.simon.skotheimsvik@skotheimsvikno.onmicrosoft.com
Requested on	1/9/2026, 10:30:31 AM
Request expires on	1/12/2026, 10:30:31 AM
Business justification	We will start with multi admin approval for device wipes after last weeks incident of accidental CEO wipe
Status	Needs approval

Property	Previous version	Requested changes
ID	-	-
Display name	-	MAA001 - Device Wipe
Description	-	Multi Admin Approval required for wiping devices.

The request needs approval from another administrator with appropriate permissions before the request can be completed.

Complete request | Cancel request

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

MAA001 - Device Wipe - Create

Multi admin approval request

Resource type	Access policy
Operation	Create
Requested by	c1.simon.skotheimsvik@skotheimsvikno.onmicrosoft.com
Requested on	1/9/2026, 10:30:31 AM
Request expires on	1/12/2026, 10:30:31 AM
Business justification	We will start with multi admin approval for device wipes after last weeks incident of accidental CEO wipe
Status	Needs approval

Property	Previous version	Requested changes
ID	-	-
Display name	-	MAA001 - Device Wipe
Description	-	Multi Admin Approval required for wiping devices.
Policy type	-	Device wipe
Policy platform	-	All platforms
Approver groups	-	AZ-Intune-Multi Admin Approval

The request needs approval from another administrator with appropriate permissions before the request can be completed.

Complete request | Cancel request

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

MAA001 - Device Wipe - Create

Multi admin approval request

Review the changes below and take the appropriate action.

Request information

Resource type	Access policy
Operation	Create
Requested by	c1.simon.skotheimsvik@skotheimsvikno.onmicrosoft.com
Requested on	1/9/2026, 10:30:31 AM
Request expires on	1/12/2026, 10:30:31 AM
Business justification	We will start with multi admin approval for device wipes after last weeks incident of accidental CEO wipe
Status	Needs approval

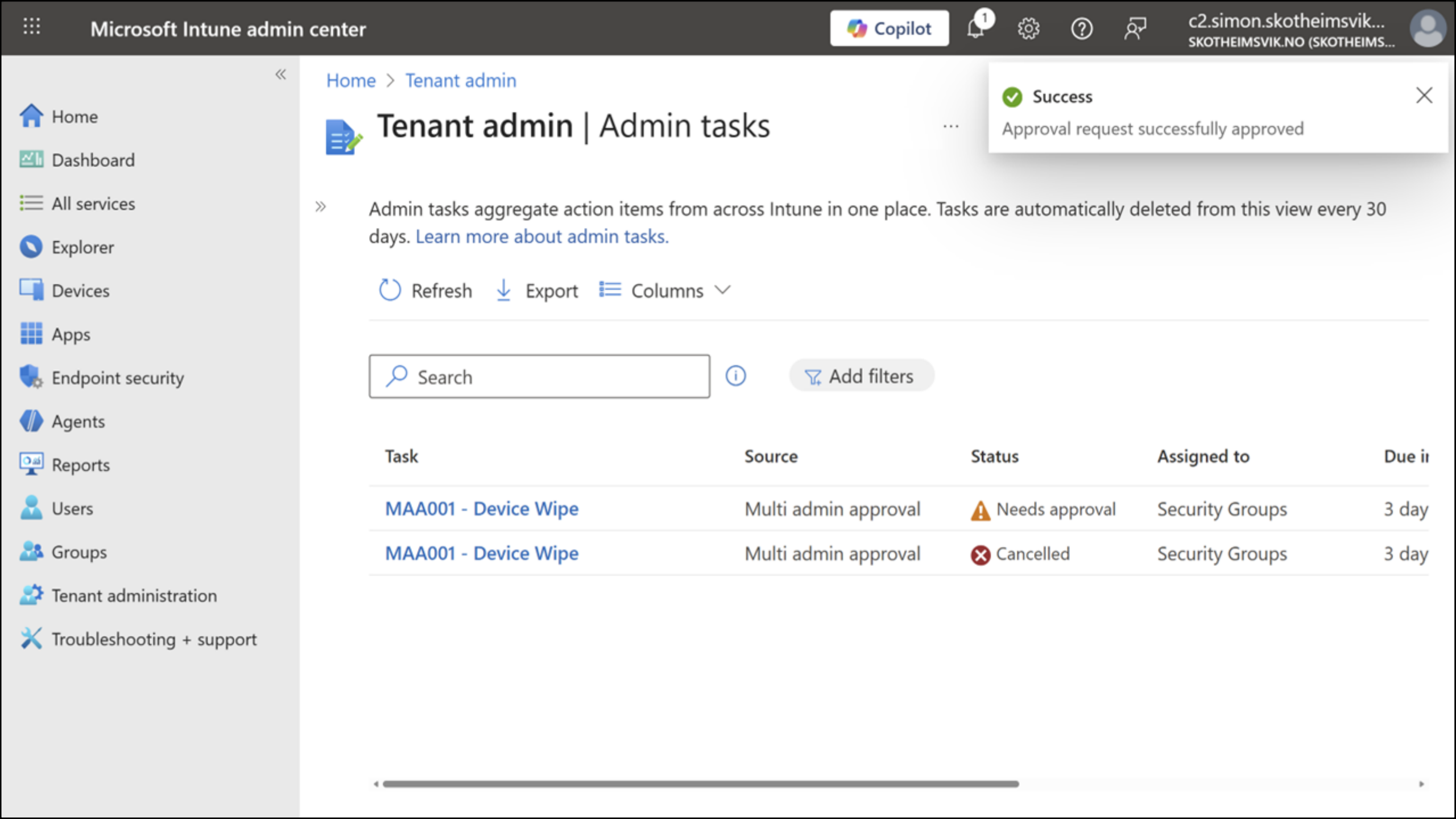
Property	Previous version	Requested changes

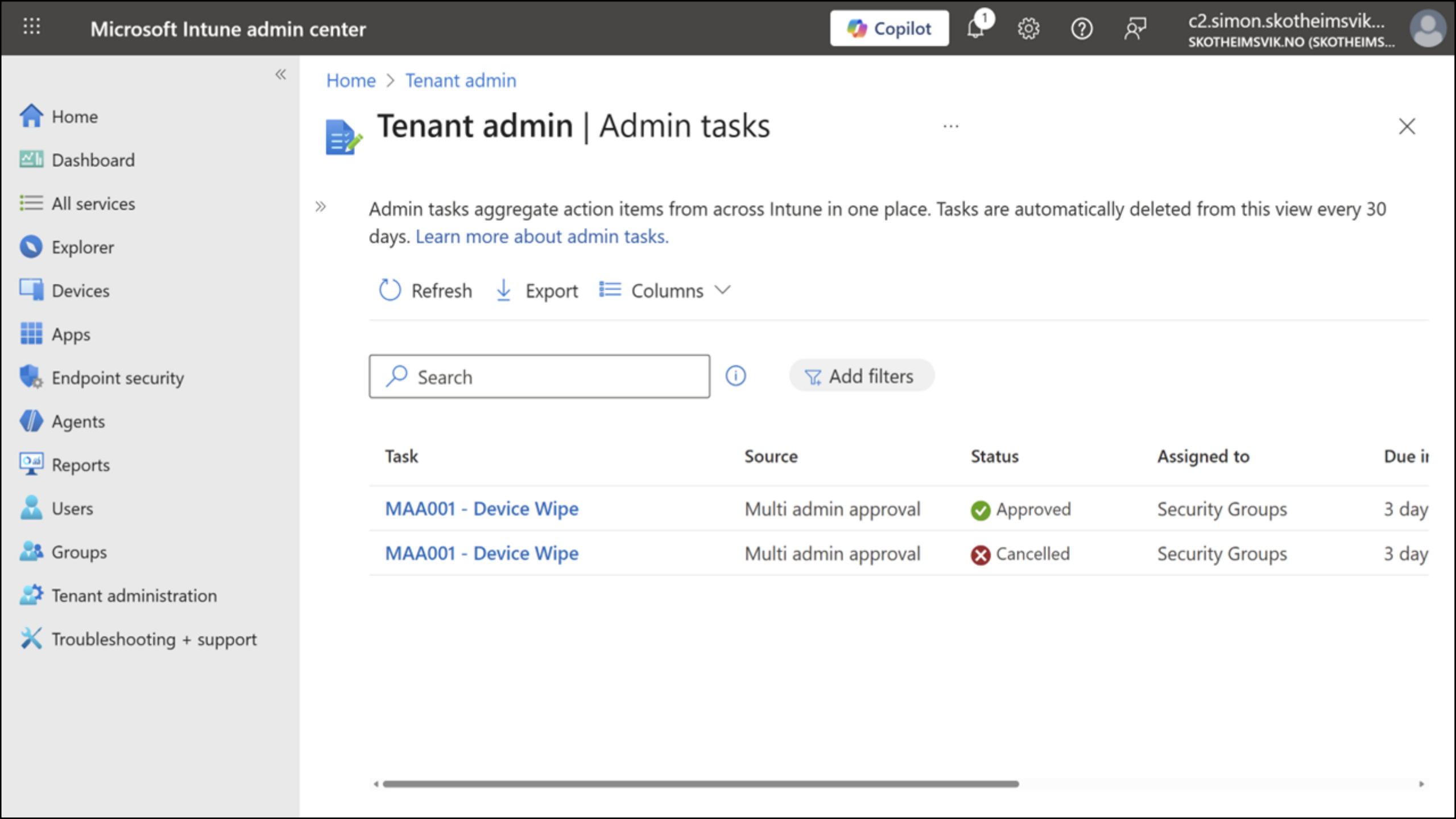
Approver notes

This is an extremely good idea to implement.

You may approve or reject this request if you have approver permission.

Approve request | Reject request


Microsoft Intune admin center
Copilot
c2.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Admin tasks
Success
Approval request successfully approved
Admin tasks aggregate action items from across Intune in one place. Tasks are automatically deleted from this view every 30 days. Learn more about admin tasks.
Refresh
Export
Columns
Search
Add filters
Task
Source
Status
Assigned to
Due i
MAA001 - Device Wipe
Multi admin approval
Needs approval
Security Groups
3 day
MAA001 - Device Wipe
Multi admin approval
Cancelled
Security Groups
3 day


Microsoft Intune admin center
Copilot
1
c2.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Admin tasks
Admin tasks aggregate action items from across Intune in one place. Tasks are automatically deleted from this view every 30 days. Learn more about admin tasks.
Refresh
Export
Columns
Search
Add filters
Task
Source
Status
Assigned to
Due i
MAA001 - Device Wipe
Multi admin approval
Approved
Security Groups
3 day
MAA001 - Device Wipe
Multi admin approval
Cancelled
Security Groups
3 day

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

Tenant admin | Multi Admin Approval

All requests | My requests | Access policies

Refresh | Columns

Search by justification | Add filter

Showing 1 to 2 of 2 records

< Previous | Page 1 of 1 | Next >

Requested on	Name	Resource type	Business justi...	Requested by	Status
1/9/2026, 10:30:31 AM	MAA001 - Device Wipe - Create	Access policy	We will start with ...	c1.simon.skothei...	Approved
1/9/2026, 10:28:00 AM	MAA001 - Device Wipe - Create	Access policy	We will start with ...	c1.simon.skothei...	Cancelled

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

Tenant admin | Multi Admin Approval

All requests | My requests | Access policies

Access policies allow you to control which tasks and actions need approval along with the specific approval groups

+ Create | Refresh

Search by name | Add filter

Showing 0 to 0 of 0 records

< Previous | Page 0 of 0 | Next >

Name	Policy type	Policy platform
There are no policies to view		

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

Tenant admin | Multi Admin Approval

All requests | My requests | Access policies

Refresh | Columns

Search by justification | Add filter

Showing 1 to 2 of 2 records

< Previous | Page 1 of 1 | Next >

Requested on	Name	Resource type	Business justi...	Requested by	Status
1/9/2026, 10:30:31 AM	MAA001 - Device Wipe - Create	Access policy	We will start with ...	c1.simon.skothei...	Approved
1/9/2026, 10:28:00 AM	MAA001 - Device Wipe - Create	Access policy	We will start with ...	c1.simon.skothei...	Cancelled

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

MAA001 - Device Wipe - Create

Multi admin approval request

Review the changes below and take the appropriate action.

Request information

Resource type	Access policy
Operation	Create
Requested by	c1.simon.skotheimsvik@skotheimsvikno.onmicrosoft.com
Requested on	1/9/2026, 10:30:31 AM
Request expires on	1/12/2026, 10:30:31 AM
Business justification	We will start with multi admin approval for device wipes after last weeks incident of accidental CEO wipe
Status	Approved

Property	Previous version	Requested changes

Approver notes

This is an extremely good idea to implement.

The request is approved and can be completed.

Complete request | Cancel request

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

Tenant admin | Multi Admin Approval

Access policy created
Access policy MAA001 - Device Wipe created

Success
Approval request successfully completed

All requests | My requests | Access policies

Refresh | Columns

Search by justification | Add filter

Showing 1 to 2 of 2 records

< Previous | Page 1 of 1 | Next >

Requested on	Name	Resource type	Business justi...	Requested by	Status
1/9/2026, 10:30:31 AM	MAA001 - Device Wipe - Create	Access policy	We will start with ...	c1.simon.skothei...	Approved
1/9/2026, 10:28:00 AM	MAA001 - Device Wipe - Create	Access policy	We will start with ...	c1.simon.skothei...	Cancelled

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

Tenant admin | Multi Admin Approval

All requests | My requests | Access policies

Access policies allow you to control which tasks and actions need approval along with the specific approval groups

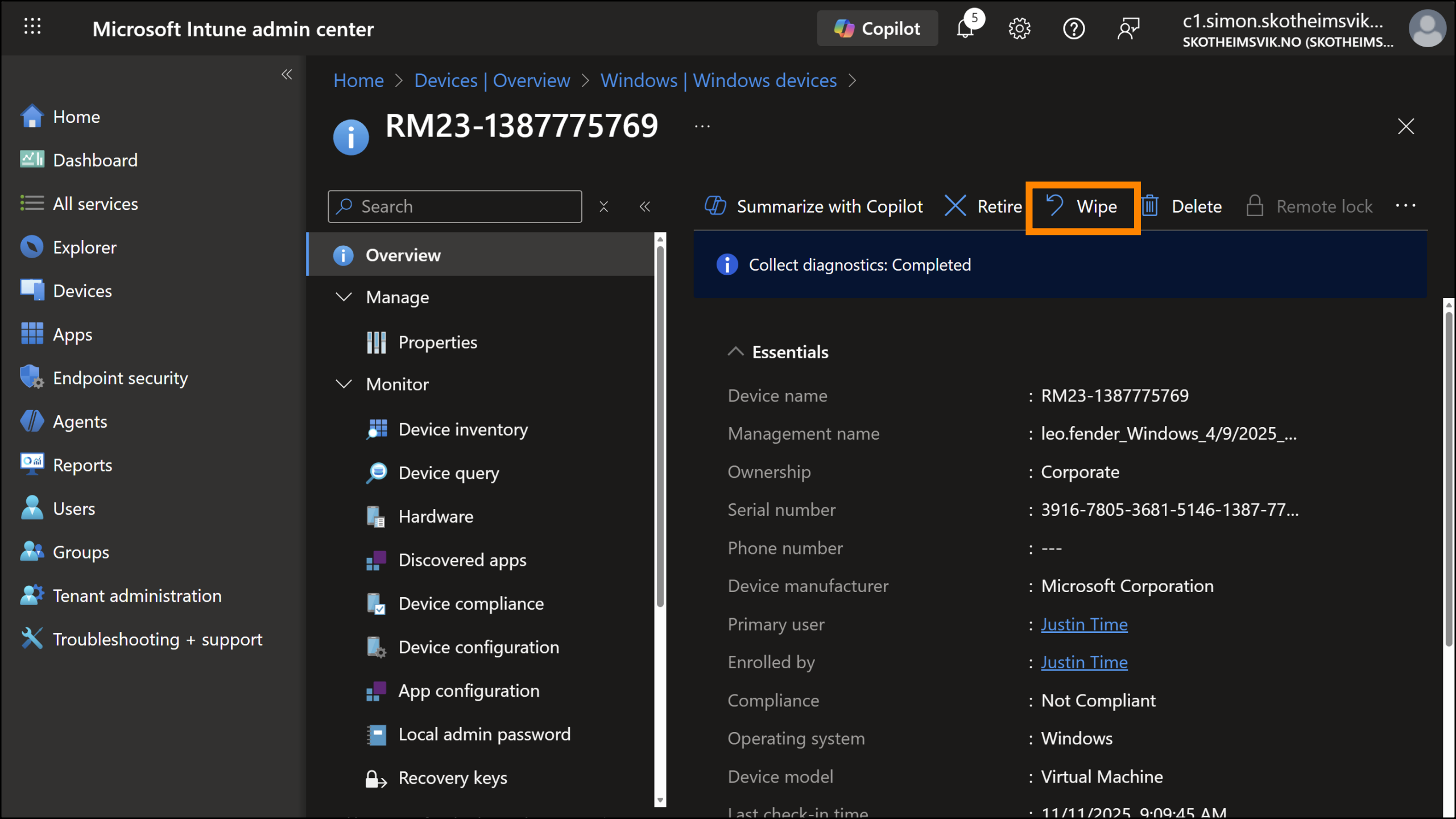
Create | Refresh

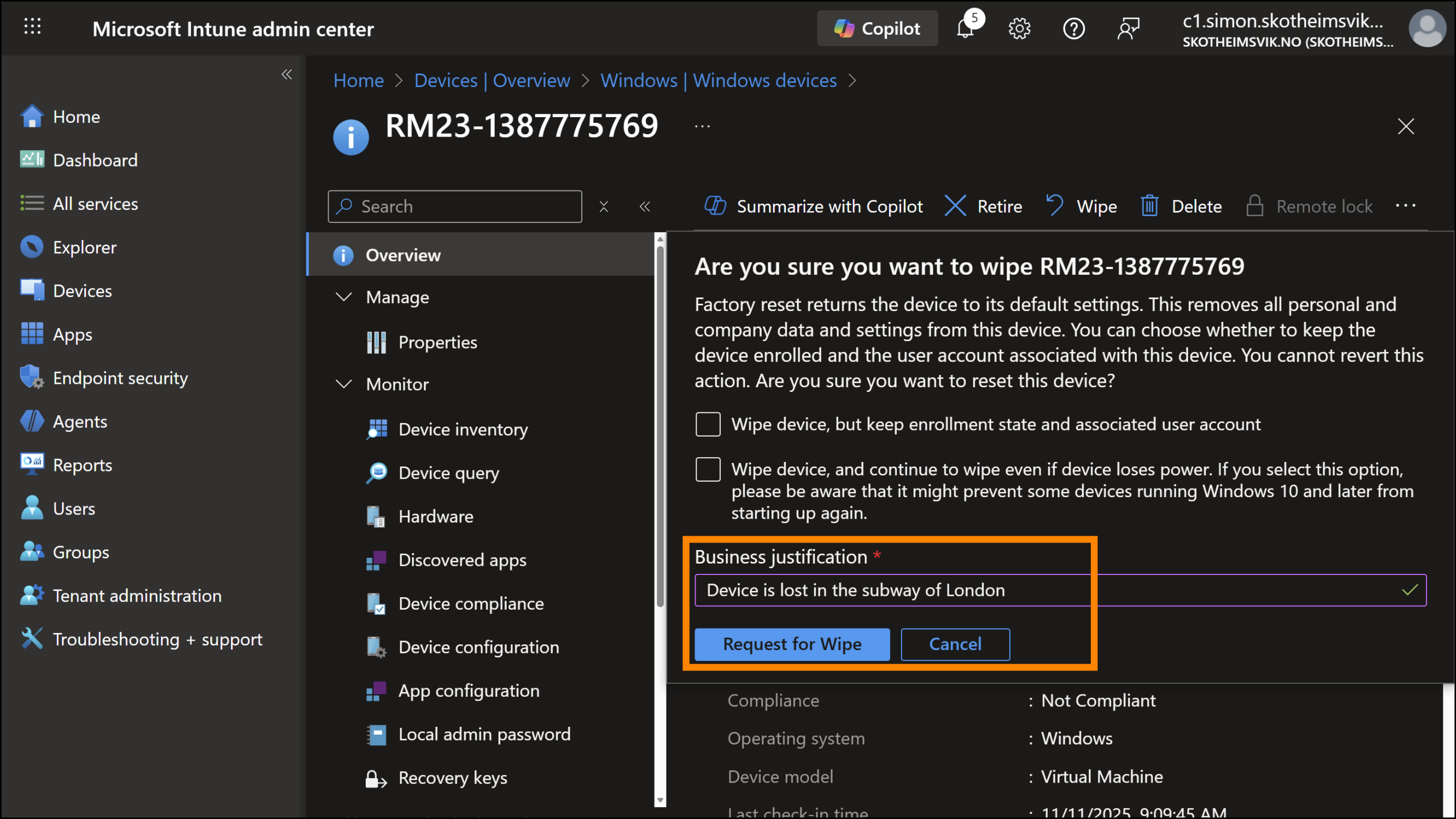
Search by name | Add filter

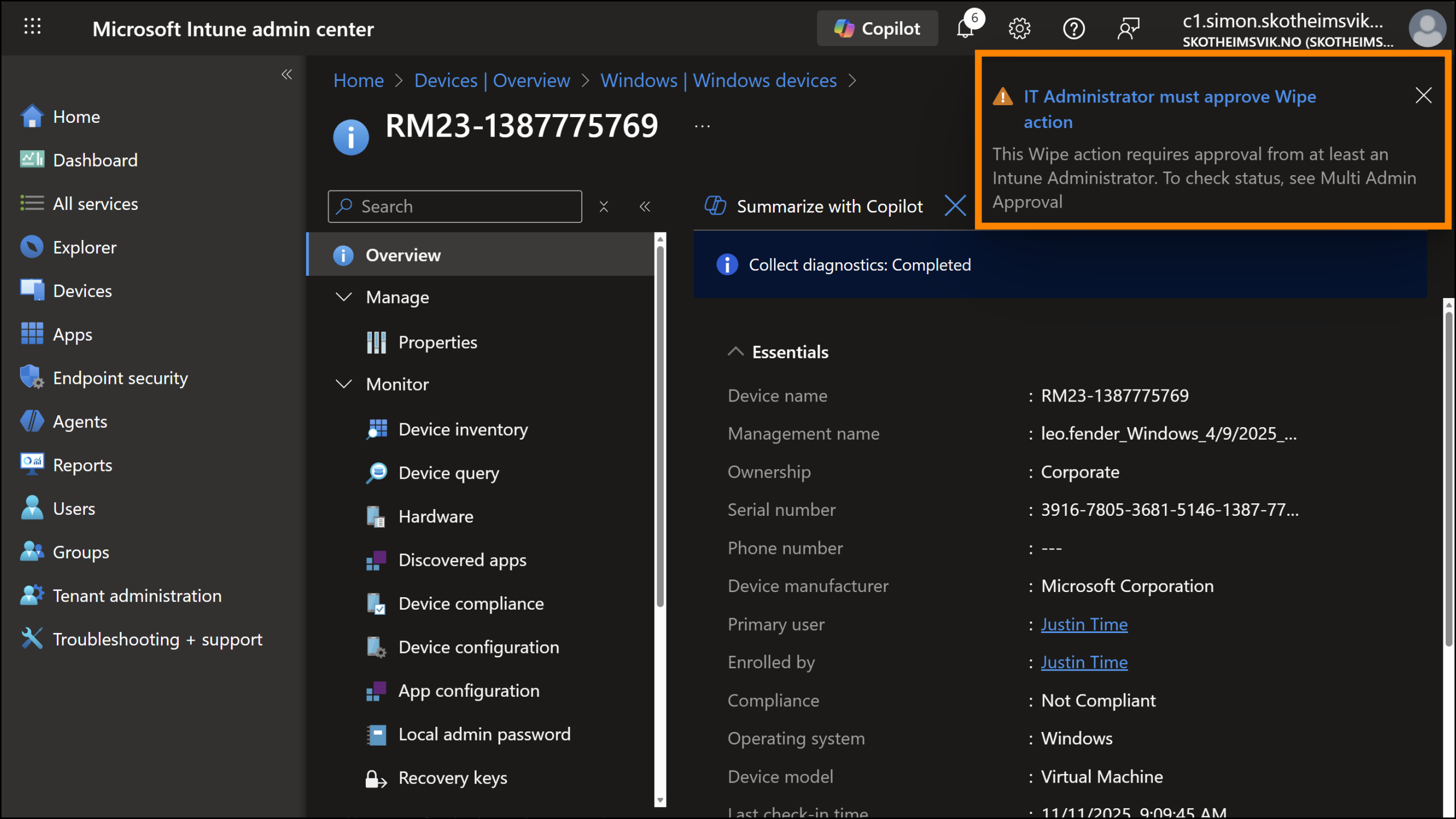
Showing 1 to 1 of 1 records

< Previous | Page 1 of 1 | Next >

Name	Policy type	Policy platform
MAA001 - Device Wipe	Device wipe	All platforms


Microsoft Intune admin center
Copilot
5
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Overview > Windows | Windows devices >
RM23-1387775769
Search
Overview
Manage
Properties
Monitor
Device inventory
Device query
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Local admin password
Recovery keys
Summarize with Copilot
Retire
Wipe
Delete
Remote lock
Collect diagnostics: Completed
Essentials
Device name : RM23-1387775769
Management name : leo.fender_Windows_4/9/2025_...
Ownership : Corporate
Serial number : 3916-7805-3681-5146-1387-77...
Phone number : ---
Device manufacturer : Microsoft Corporation
Primary user : Justin Time
Enrolled by : Justin Time
Compliance : Not Compliant
Operating system : Windows
Device model : Virtual Machine
Last check-in time : 11/11/2025, 9:09:45 AM


Microsoft Intune admin center
Copilot
5
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Overview > Windows | Windows devices >
RM23-1387775769
Search
Summarize with Copilot
Retire
Wipe
Delete
Remote lock
Overview
Manage
Properties
Monitor
Device inventory
Device query
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Local admin password
Recovery keys
Are you sure you want to wipe RM23-1387775769
Factory reset returns the device to its default settings. This removes all personal and company data and settings from this device. You can choose whether to keep the device enrolled and the user account associated with this device. You cannot revert this action. Are you sure you want to reset this device?
Wipe device, but keep enrollment state and associated user account
Wipe device, and continue to wipe even if device loses power. If you select this option, please be aware that it might prevent some devices running Windows 10 and later from starting up again.
Business justification *
Device is lost in the subway of London
Request for Wipe
Cancel
Compliance : Not Compliant
Operating system : Windows
Device model : Virtual Machine
Last check-in time : 11/11/2025, 9:09:45 AM


Microsoft Intune admin center
Copilot
6
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Overview > Windows | Windows devices >
RM23-1387775769
IT Administrator must approve Wipe action
This Wipe action requires approval from at least an Intune Administrator. To check status, see Multi Admin Approval
Search
Summarize with Copilot
Overview
Manage
Properties
Monitor
Device inventory
Device query
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Local admin password
Recovery keys
Collect diagnostics: Completed
Essentials
Device name : RM23-1387775769
Management name : leo.fender_Windows_4/9/2025_...
Ownership : Corporate
Serial number : 3916-7805-3681-5146-1387-77...
Phone number : ---
Device manufacturer : Microsoft Corporation
Primary user : Justin Time
Enrolled by : Justin Time
Compliance : Not Compliant
Operating system : Windows
Device model : Virtual Machine
Last check-in time : 11/11/2025, 9:09:45 AM

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

Tenant admin | Admin tasks

Admin tasks aggregate action items from across Intune in one place. Tasks are automatically deleted from this view every 30 days. Learn more about admin tasks.

Refresh Export Columns

Search Add filters

Task	Source	Status	Assigned to	Due i
RM23-1387775769	Multi admin approval	Needs approval	Security Groups	3 day
MAA001 - Device Wipe	Multi admin approval	Completed	Security Groups	3 day
MAA001 - Device Wipe	Multi admin approval	Cancelled	Security Groups	3 day

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

RM23-1387775769 - Action

Multi admin approval request

Wipe device action changes

```
1 -
1+[
2+  {
3+    "deviceId": "a3ce66f1-0879-4262-a0ea-c131959c31f9",
4+    "deviceName": "RM23-1387775769",
5+    "serialNumber": "3916-7805-3681-5146-1387-7757-69",
6+    "primaryUser": "137e5ba7-ff5d-43a5-a2d5-eeabd4422367",
7+    "primaryUserEmail": "justin.time@skotheimsvik.com",
8+    "actionName": "Wipe",
9+    "notFound": false,
10+   "notInScope": false,
11+   "@odata.type": "microsoft.graph.MAADeviceAction.ManagedDeviceMAAPayload"
12+ }
13+]
```

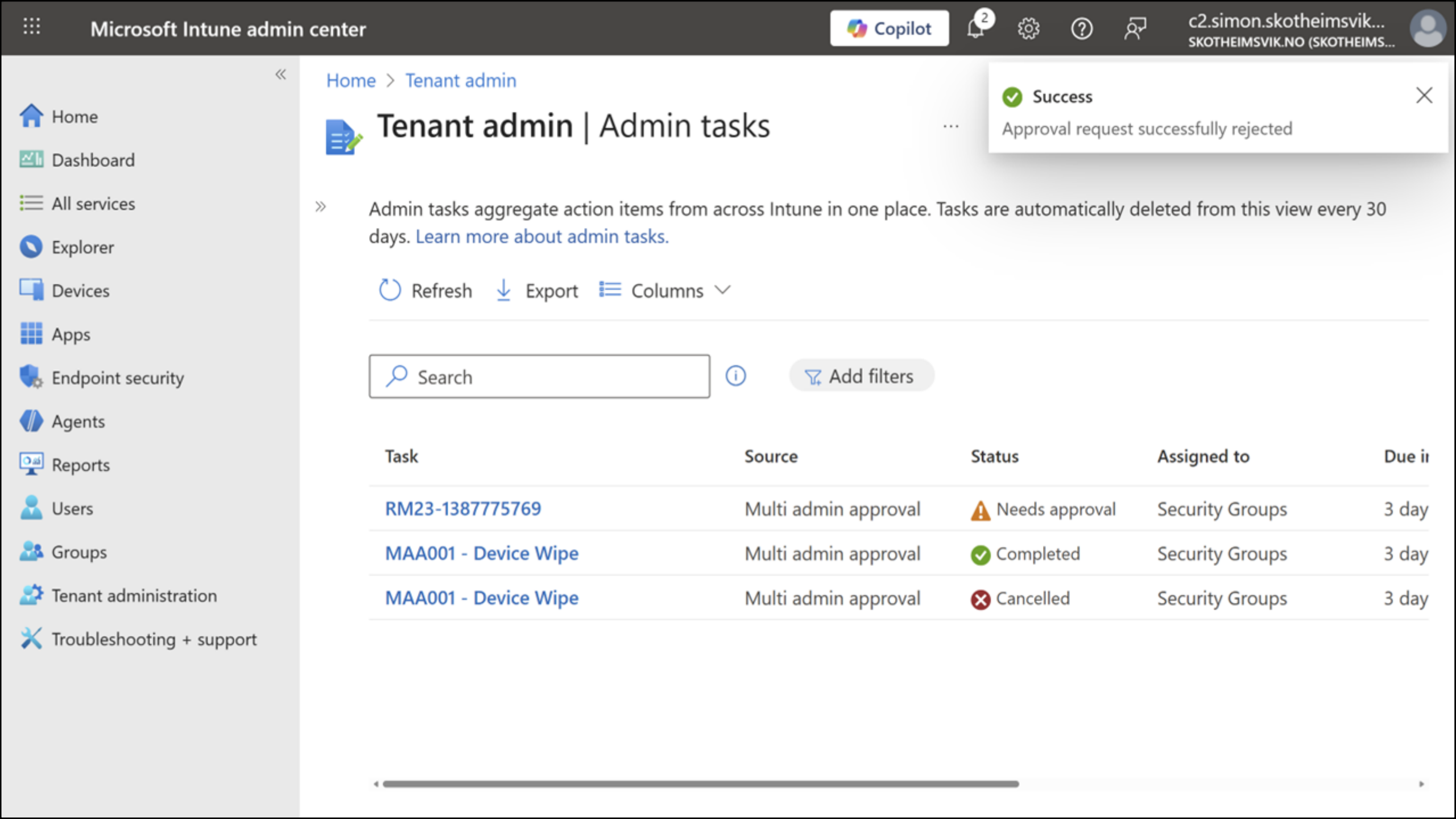
Approver notes

I heard he found his device in the car

You may approve or reject this request if you have approver permission.

Approve request | Reject request

Reject request


Microsoft Intune admin center
Copilot
2
c2.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Admin tasks
Success
Approval request successfully rejected
Admin tasks aggregate action items from across Intune in one place. Tasks are automatically deleted from this view every 30 days. Learn more about admin tasks.
Refresh
Export
Columns
Search
Add filters
Task
Source
Status
Assigned to
Due i
RM23-1387775769
Multi admin approval
Needs approval
Security Groups
3 day
MAA001 - Device Wipe
Multi admin approval
Completed
Security Groups
3 day
MAA001 - Device Wipe
Multi admin approval
Cancelled
Security Groups
3 day

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

Tenant admin | Admin tasks

Admin tasks aggregate action items from across Intune in one place. Tasks are automatically deleted from this view every 30 days. Learn more about admin tasks.

Refresh Export Columns

Search Add filters

Task	Source	Status	Assigned to	Due i
RM23-1387775769	Multi admin approval	Rejected	Security Groups	3 day
MAA001 - Device Wipe	Multi admin approval	Completed	Security Groups	3 day
MAA001 - Device Wipe	Multi admin approval	Cancelled	Security Groups	3 day

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

Tenant admin | Multi Admin Approval

All requests | My requests | Access policies

Refresh | Columns

Search by justification | Add filter

Showing 1 to 3 of 3 records

< Previous | Page 1 of 1 | Next >

Requested on	Name	Resource t...	Business justification	Req...	Status
1/9/2026, 11:55:01 AM	RM23-1387775769 - Action	Device action	Device is lost in the subway ...	c1.simon....	Rejected
1/9/2026, 10:30:31 AM	MAA001 - Device Wipe - Create	Access policy	We will start with multi adm...	c1.simon....	Completed
1/9/2026, 10:28:00 AM	MAA001 - Device Wipe - Create	Access policy	We will start with multi adm...	c1.simon....	Cancelled

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

RM23-1387775769 - Action

Multi admin approval request

Review the changes below and take the appropriate action.

Request information

Resource type	Device action
Operation	Action
Requested by	c1.simon.skotheimsvik@skotheimsvikno.onmicrosoft.com
Requested on	1/9/2026, 11:55:01 AM
Request expires on	1/12/2026, 11:55:01 AM
Business justification	Device is lost in the subway of London
Status	Rejected

Wipe device action changes

```
1  -
1 +[
```

Approver notes

I heard he found his device in the car

The request was rejected.

Complete request Cancel request

Intune Guardian

Simon Skotheimsvik (C2) SS

Audit Events

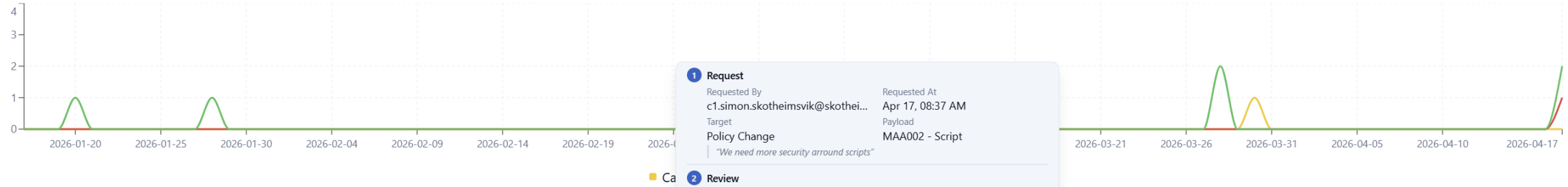
Updated 1:37:45 PM | Last 90 days

Total Events	Unique Applications	Devices Retired	Devices Wiped
1,037 ↗1%	2 ↗3%	0	2 ↘100%

Welcome | Summary | Device Actions | Target Actions | Admin Actions | App Actions | Autopilot | **Multi Admin Approval** | Anomaly Detection | Audit Log

Total	Completed	Pending	Awaiting Execution	Rejected	Cancelled	Avg Review	Avg Total
8	6	0	0	1	1	13m 15s	25m 10s

Activity Trend



1 **Request**
Requested By: c1.simon.skotheimsvik@skothei...
Requested At: Apr 17, 08:37 AM
Target: Policy Change
Payload: MAA002 - Script
"We need more security arround scripts"

2 **Review**
Reviewed By: c2.simon.skotheimsvik@skothei...
Reviewed At: Apr 17, 08:43 AM
Decision: Approved
Duration: 5m 40s
"Good idea."

3 **Execution**
Executed By: c1.simon.skotheimsvik@skothei...
Executed At: Apr 17, 08:50 AM
Policy: MAA002 - Script
Total Duration: 12m 40s

MAA002 - Script | Details

Search requestor, reviewer, targ | All statuses | All targets

8 of 8 requests

Status	Payload	Request	Review	Execution	Total
Rejected	— DeviceManagementScript	c1.simon.skotheimsvik... Apr 17, 09:00 AM *"Some incoming verry needed securi..."*	43m 18s	—	43m 18s
Completed	MAA002 - Script Policy Change	c1.simon.skotheimsvik... Apr 17, 08:37 AM *"We need more security arround scri..."*	5m 40s	c1.simon.skotheimsvik... Apr 17, 08:50 AM	12m 40s
Completed	MAA001 - Configuration Policy Policy Change	c1.simon.skotheimsvik... Apr 17, 08:36 AM *"Tuning the namings"*	6m 38s	c1.simon.skotheimsvik... Apr 17, 08:49 AM	13m 55s
Cancelled	— IDeviceManagementPolicy	c1.simon.skotheimsvik... Mar 30, 07:52 AM	39m 13s	—	39m 13s

Apr 17, 08:43 AM *"Good idea."*
c2.simon.skotheimsv... Apr 17, 08:42 AM *"Good naming convention."*
c1.simon.skotheimsv... Mar 30, 08:31 AM

6 Security Copilot

Copilot with Explorer and Agents in Intune

Nov 17 2025

https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#security-copilot-in-intune-agents-are-available-for-public-preview-

Security Copilot

Microsoft Intune admin center

Copilot 7

c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...

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

skotheimsvik.no

Securely manage devices, access, and apps with Intune

Maximize productivity and simplify administration without compromising endpoint management and security.

Status

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

Explorer ...

Show examples
Provide feedback

Explore data in your tenant based on device, app, and management properties. Learn more about exploring data, including what's coming soon

Query your data

Start typing to search your Intune data, or see below for examples

Find the Intune data you're looking for

Search your tenant for info about devices, users, apps, compliance, or updates. Copilot can also help you understand what kind of questions you can ask and how to ask them.

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

Explorer ...

Show examples
Provide feedback

Explore data in your tenant based on device, app, and management properties. Learn more about exploring data, including what's coming soon

Query your data

Start typing to search your Intune data, or see below for examples

Find the Intune data you're looking for

Search your tenant for info about devices, users, apps, compliance, or updates. Copilot can also help you understand what kind of questions you can ask and how to ask them.

Security Copilot

Microsoft Security Copilot / Usage monitoring

default | Export

- Home
- Agents
- Promptbooks
- Build Preview
- History
- Owner
  - Owner settings
  - Plugin settings
  - Role assignment
  - Manage workspaces
  - Usage monitoring

SecurityCopilot | + New capacity

Change units | View billing in Azure

Provisioned units used

0 of 0 units

in the last hour

Overage units used

0 of 4 units

in the last hour

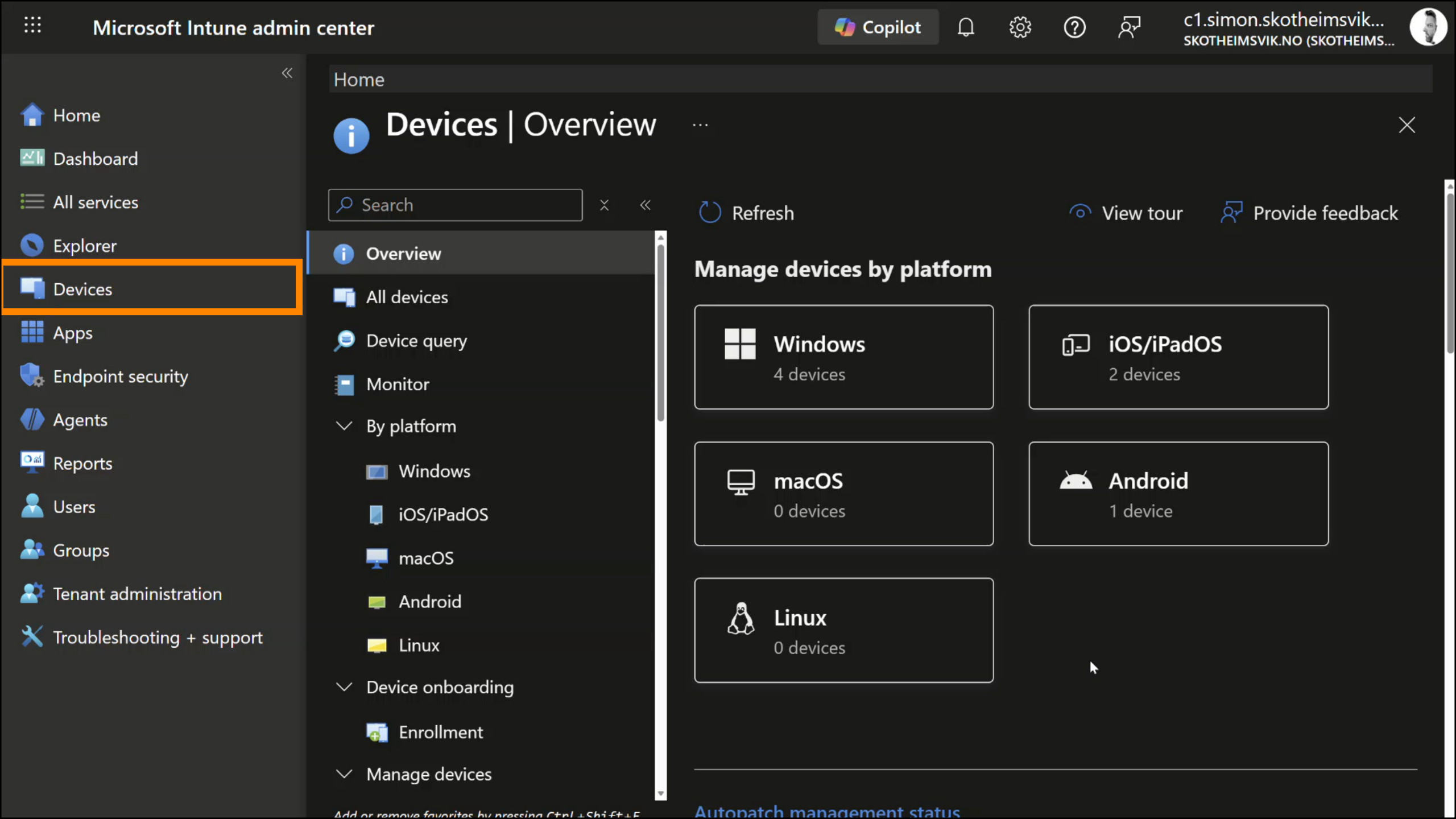
Workspace using this capacity

default

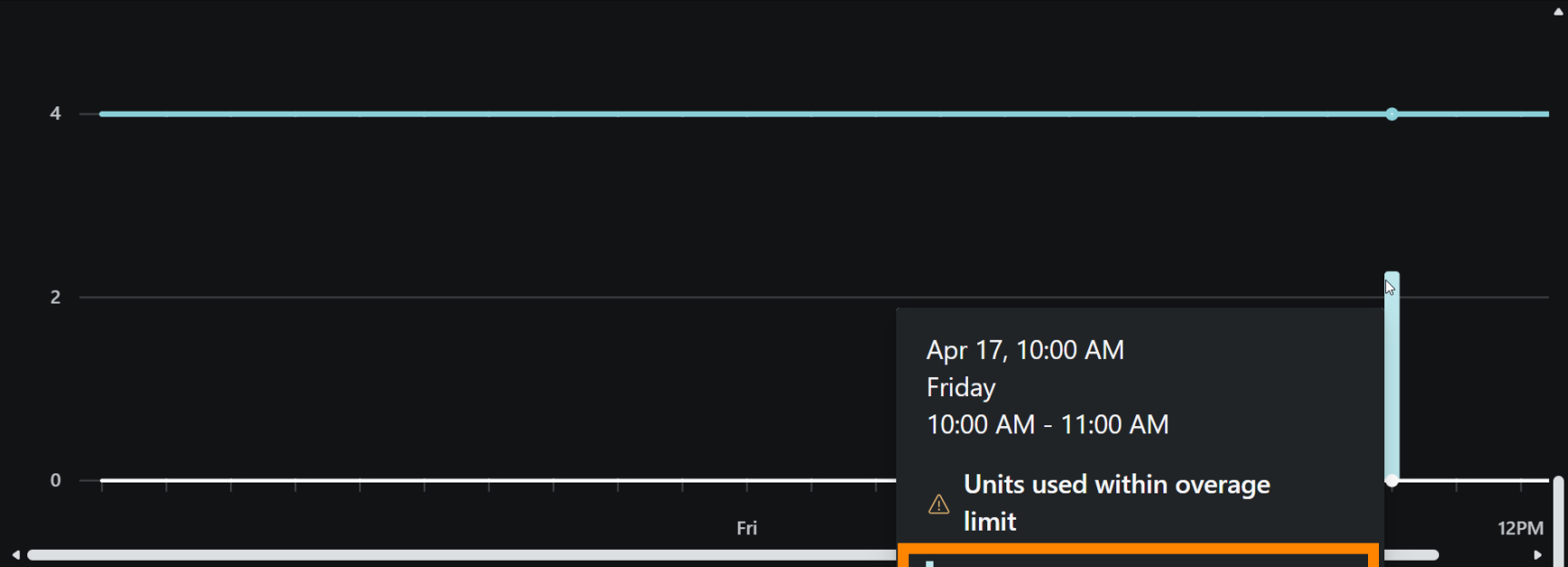
Manage workspaces

Date: Last 24 hours

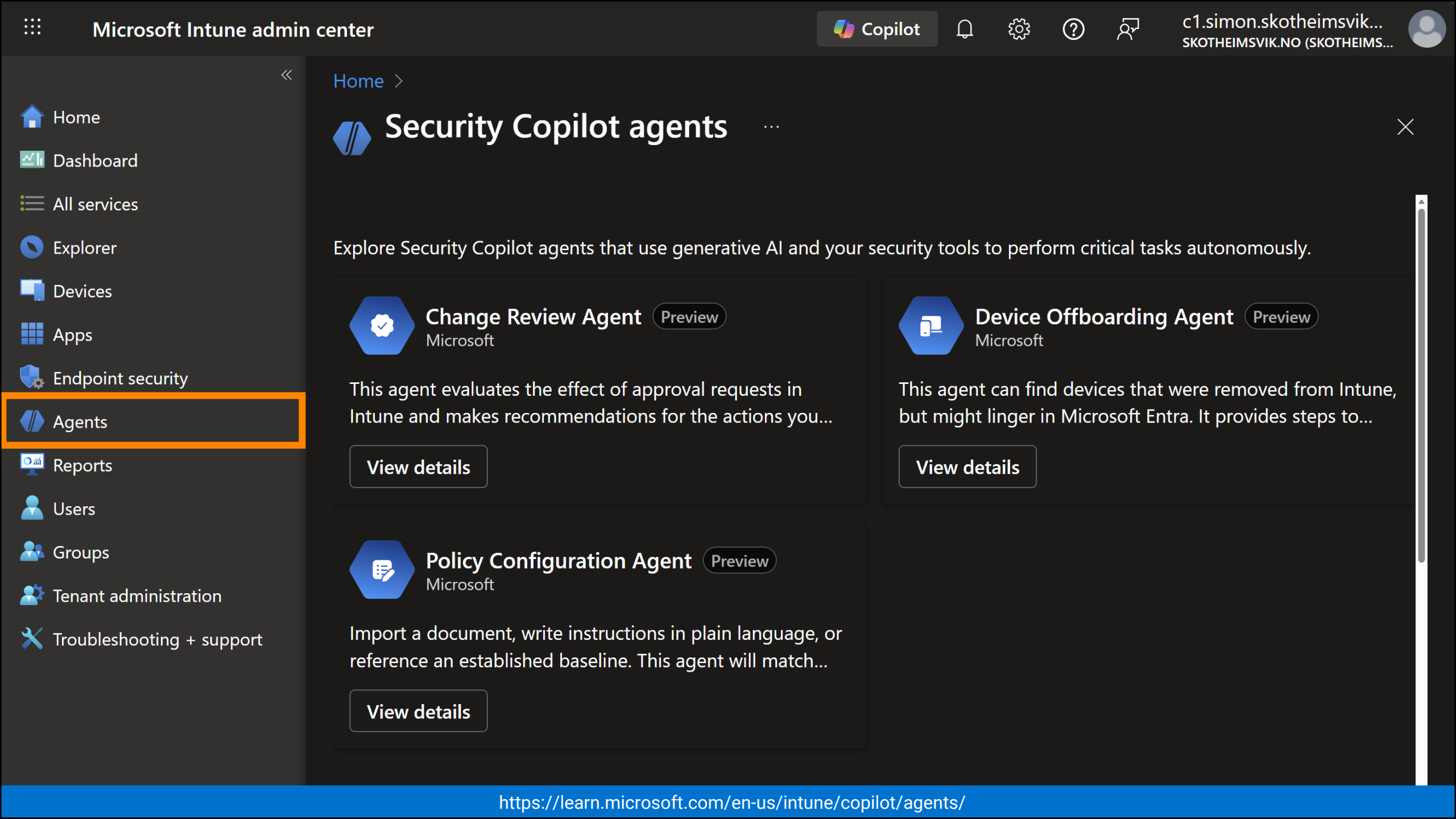
https://securitycopilot.microsoft.com/usage-monitoring


Microsoft Intune admin center
Copilot
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home
Devices | Overview
Search
Overview
All devices
Device query
Monitor
By platform
Windows
iOS/iPadOS
macOS
Android
Linux
Device onboarding
Enrollment
Manage devices
Refresh
View tour
Provide feedback
Manage devices by platform
Windows
4 devices
iOS/iPadOS
2 devices
macOS
0 devices
Android
1 device
Linux
0 devices
Autopatch management status

Home
Agents
Promptbooks
Build Preview
History
Owner
Owner settings
Plugin settings
Role assignment
Manage workspaces
Usage monitoring
Security Store



Session ID	Date	Units used	Initiated by			Cop exp
73b54f85-b852-4fa7-9ff1-e62c7c734cfe	Apr 17, 10:55 AM	1.3	SS Simon Skotheimsvik (C1)	User prompt	Automated	Unk
c233ab6f-57e2-431a-bf72-7aaf7788fb0d	Apr 17, 10:51 AM	0.7	SS Simon Skotheimsvik (C1)	User prompt	Automated	Unk
4e84b003-3d7f-411a-b507-	Apr 17, 10:46 AM	0.3	SS Simon Skotheims	User prompt	Automated	Unk



https://learn.microsoft.com/en-us/intune/copilot/agents/

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

MAA002 - Script

Access policy

Basics Edit

Name	MAA002 - Script
Description	Multi Admin Approval for scripts, such as PowerShell scripts or remediation scripts. This could include create, edit, assign, and delete. Script policies apply to all platforms.
Policy type	Script
Policy platform	All platforms

Approver groups Edit

Included groups

Group	Status
AZ-Intune-Multi Admin Approval	Active

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

Add PowerShell script ...

Basics
Script settings
3 Review + submit for approval

Summary

Before this resource can be created, it must be approved by another admin. Before you can submit this request, you must enter your business justification.

Basics

Name	WPS666 - My Personal Local Admin
Description	A script to add my own personal local admin on all Windows devices.

Script settings

Business justification *

Some incoming verry needed security tunings

Previous
Submit for approval

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

Tenant admin | Multi Admin Approval

All requests | My requests | Access policies

Refresh | Columns

Search by justification | Add filter

Showing 1 to 6 of 6 records

< Previous | Page 1 of 1 | Next >

Reque...	Name	Resource...	Business justificati...	Reque...	Status
4/17/2026, ...	WPS666 - My Personal Local Admin - Create	PowerShell scr...	Some incoming verry n...	c1.simon.sk...	Needs approval
4/17/2026, ...	MAA002 - Script - Create	Access policy	We need more security...	c1.simon.sk...	Completed
4/17/2026, ...	MAA for Configuration Policy - Update	Access policy	Tuning the namings	c1.simon.sk...	Completed
3/30/2026, ...	WDCP205 - APP - Microsoft Edge Managed Bookmarks	Configuration ...	Adjusted some texts in ...	c1.simon.sk...	Cancelled
3/28/2026, ...	WDCP205 - APP - Microsoft Edge Managed Bookmarks	Configuration ...	Updated with new URL...	c1.simon.sk...	Completed
3/28/2026, ...	MAA for Configuration Policy - Create	Access policy	I want to apply MAA fo...	c1.simon.sk...	Completed

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

Tenant admin | Admin tasks

Admin tasks aggregate action items from across Intune in one place. Multi-admin approval and EPM elevation request tasks are automatically deleted from this view after 30 days. Learn more about admin tasks.

Refresh Export Columns

Search Add filters

Task	Source	Status	Assigned to	Due
WPS666 - My Personal Local Admin	Multi admin approval	Needs approval	Security Groups	3 da
MAA002 - Script	Multi admin approval	Completed	Security Groups	3 da
MAA for Configuration Policy	Multi admin approval	Completed	Security Groups	3 da
WDCP205 - APP - Microsoft Edge Managed Bookmarks (User)	Multi admin approval	Cancelled	Security Groups	Ove
WDCP205 - APP - Microsoft Edge Managed Bookmarks (User)	Multi admin approval	Completed	Security Groups	Ove
MAA for Configuration Policy	Multi admin approval	Completed	Security Groups	Ove

Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents

WPS666 - My Personal Local Admin - Create

Multi admin approval request

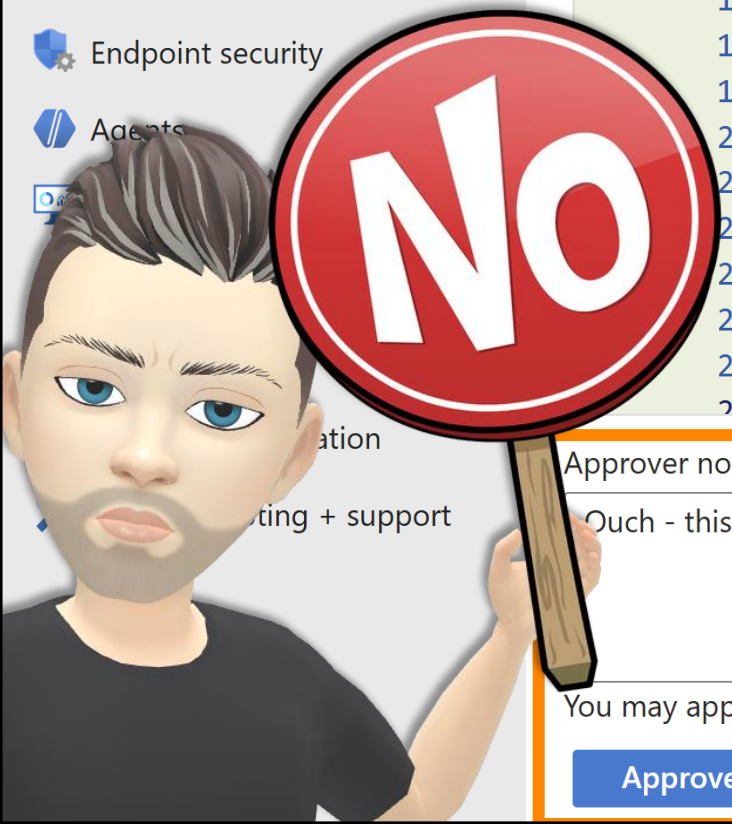
```
    Remove-LocalUser -Name $UserName
}

# Create and enable local user
New-LocalUser -Name $UserName `
              -Password $securePassword `
              -FullName "Super Local Admin" `
              -Description "Created for Intune multi-admin approval testing"

Enable-LocalUser -Name $UserName

# Add user to local Administrators group
Add-LocalGroupMember -Group "Administrators" -Member $UserName

Write-Output "Created and enabled user: $UserName"
Write-Output "Added $UserName to local Administrators group."
```



Approver notes

Ouch - this was a long script - I trust you, mate ✌️

You may approve or reject this request if you have approver permission.

Approve request | Reject request

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

Security Copilot agents

Explore Security Copilot agents that use generative AI and your security tools to perform critical tasks autonomously.

Change Review Agent Preview
Microsoft

This agent evaluates the effect of approval requests in Intune and makes recommendations for the actions you can take.

View details

Device Offboarding Agent Preview
Microsoft

This agent can find devices that were removed from Intune, but might linger in Microsoft Entra. It provides steps to...

View details

Policy Configuration Agent Preview
Microsoft

Import a document, write instructions in plain language, or reference an established baseline. This agent will match...

View details

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

Change Review Agent (Preview)

Run | Refresh | Remove Agent

Updated as of 4/17/2026, 9:22:02 AM

Overview | Suggestions | Settings

No agent activity yet

Your organization will be able to monitor and manage the agent. You should check its output to make sure it's correct and give feedback to help the agent learn and improve. Like all AI, an agent might be wrong sometimes.

Learn more about agents

Set up agent

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

Tenant admin | Multi Admin Approval

Use the Change Review Agent from Security Copilot to evaluate the effect of approval requests in Intune. Set up agent

All requests | My requests | Access policies

Refresh | Columns

Search by justification | Add filter

Showing 1 to 6 of 6 records

< Previous | Page 1 of 1 | Next >

Requested on	Name	Resource...	Business justification	Requeste...	Status
4/17/2026, 9:00:09 AM	WPS666 - My Personal Local Admin	PowerShell scr...	Some incoming verry nee...	c1.simon.skot...	Rejected
4/17/2026, 8:37:23 AM	MAA002 - Script - Create	Access policy	We need more security arr...	c1.simon.skot...	Completed
4/17/2026, 8:36:02 AM	MAA for Configuration Policy	Access policy	Tuning the namings	c1.simon.skot...	Completed
3/30/2026, 7:52:33 AM	WDCP205 - APP - Microsoft Edge	Configuration ...	Adjusted some texts in th...	c1.simon.skot...	Cancelled
3/28/2026, 6:18:03 PM	WDCP205 - APP -	Configuration ...	Updated with new URL for...	c1.simon.skot...	Completed

Home
Agents
Promptbooks
Build Preview
History
Embedded Copilot Session - ...
Session: f3aedbef-f1fe-4755-...
97c1282b-ff6c-46aa-bbd7-1...
Embedded Copilot Session - ...
All history
Owner
Owner settings
Plugin settings
Role assignment
Manage workspaces
Usage monitoring
Security Store

by the number of provisioned units you've purchased, and any added overage units. Learn more about usage

SecurityCopilot | New capacity

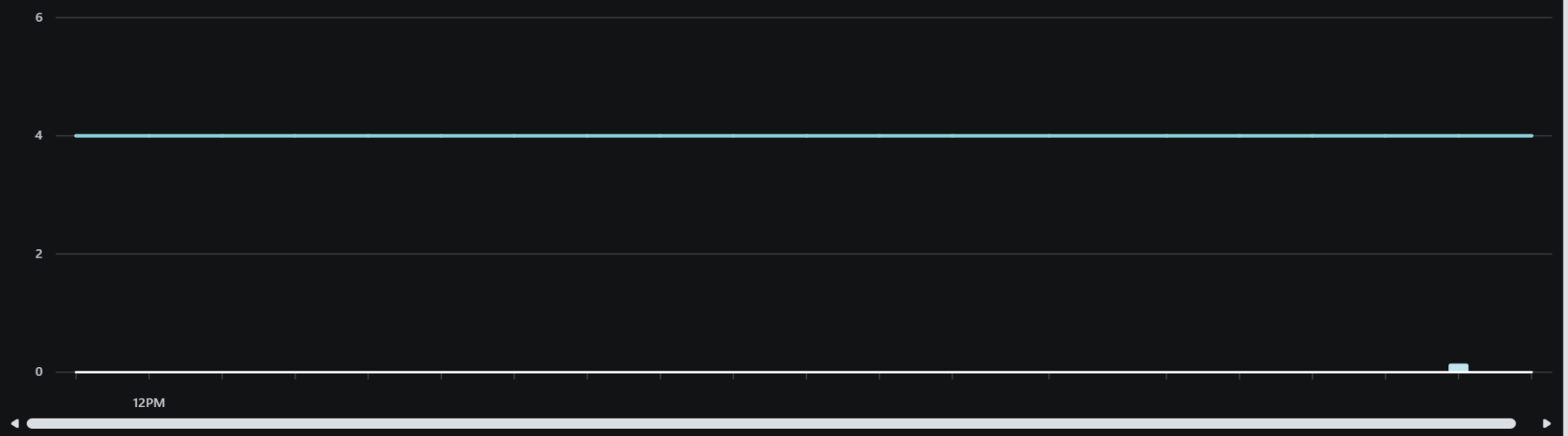
Change units | View billing in Azure

Provisioned units used
0 of 0 units
in the last hour

Overage units used
0 of 4 units
in the last hour

Workspace using this capacity
default
Manage workspaces

Date: Last 24 hours



Session ID	Date ↓	Units used	Initiated by	Category	Type	Copilot experience	Plugins used
9c4a2cbd-f49d-4fb0-954f-37ef4c8bb12b	Apr 17, 09:40 AM	0.1	SS Simon Skotheimsvik (C2)	Agent	Manual	Unknown	Global.Intune.ChangeReviewAgent

1

Learn about Security Copilot inclusion in Microsoft 365 E5 subscription

At Ignite 2025, Microsoft is announcing that Security Copilot agents will be directly built into the flow of work for security teams using Microsoft Defender, Microsoft Entra, Microsoft Intune, and Microsoft Purview.

When will Security Copilot inclusion in Microsoft 365 E5 be available?

Security Copilot will be included for all Microsoft 365 E5 customers in the upcoming months - bringing agentic AI in the daily workflow. Customers receive a 30-day advanced notification before activation. If you're already a Microsoft 365 E5 customer using Security Copilot, you can access this benefit at no additional cost.

What capacity is included?

Customers with Microsoft 365 E5 will have 400 Security Compute Units (SCU) each month for every 1,000 paid user license, up to 10,000 SCUs each month at no additional cost.

This amount scales by user license count, including for customers with fewer than 1,000 user licenses. This included capacity is expected to support typical scenarios as mentioned.

- Example 1: An organization with 400 user licenses gets 160 SCUs/month.
- Example 2: An organization with 4,000 user licenses gets 1,600 SCUs/month.

https://learn.microsoft.com/en-us/copilot/security/security-copilot-inclusion#do-customers-need-to-take-any-steps-to-configure-security-copilot-when-theyre-enabled-through-microsoft-365-e5

7 EPM

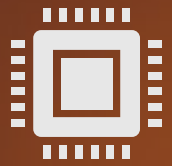
User account Context
EPM Dashboard for user readiness
Wildcards in elevation rules
Copilot to identify elevation risks
Explicit deny elevation
EPM Support on AVD

Feb 2026

Oct 2025

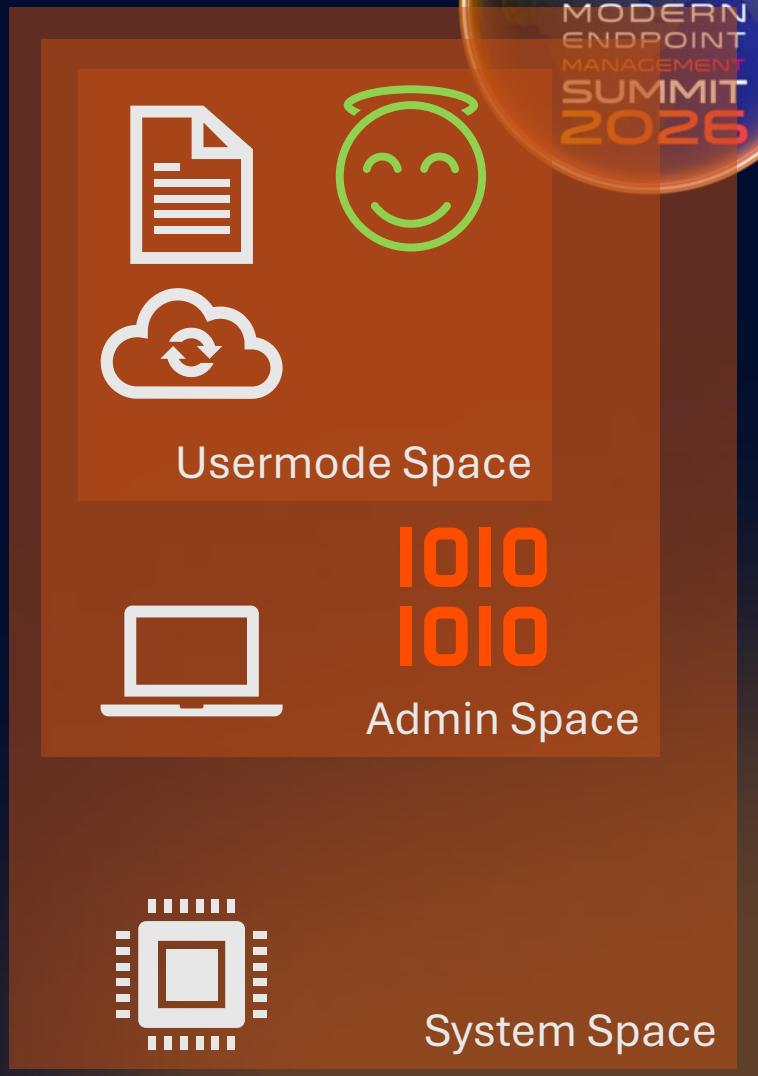
https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#support-for-user-account-context-in-endpoint-privilege-management-elevation-rules

Endpoint Privilege Management

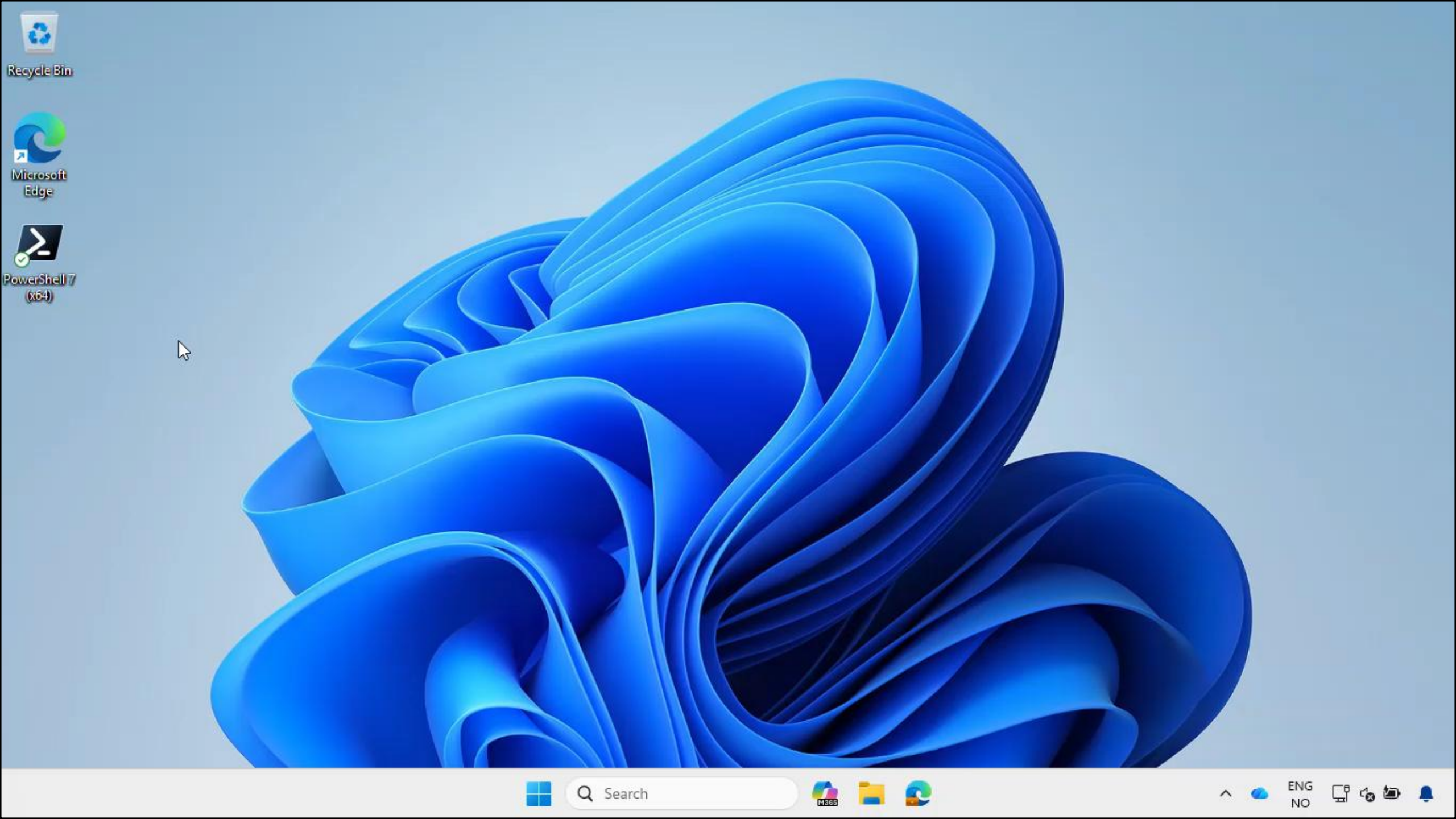


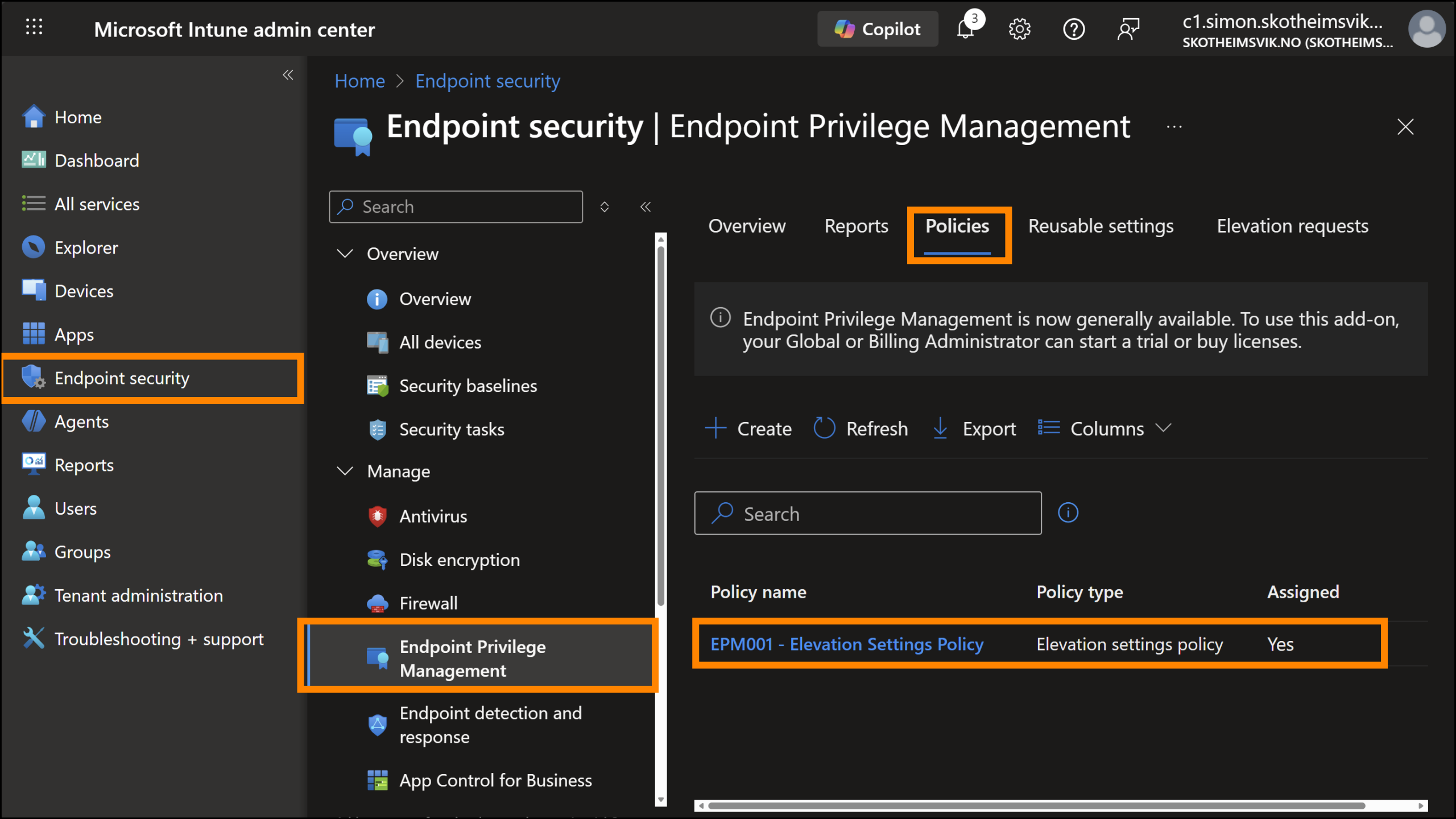
https://learn.microsoft.com/en-us/intune/intune-service/protect/epm-overview

Endpoint Privilege Management



https://learn.microsoft.com/en-us/intune/intune-service/protect/epm-overview


Recycle Bin
Microsoft Edge
PowerShell 7 (x64)
Search
M365
ENG
NO


Microsoft Intune admin center
Copilot
3
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
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
Overview
Reports
Policies
Reusable settings
Elevation requests
Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Administrator can start a trial or buy licenses.
Create
Refresh
Export
Columns
Search
Policy name
Policy type
Assigned
EPM001 - Elevation Settings Policy
Elevation settings policy
Yes

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

EPM001 - Elevation Settings Policy

Elevation settings policy

Summarize with Copilot Delete

Configuration settings Edit

Privilege management elevation client settings

Endpoint Privilege Management	Enabled
Default elevation response	Require user confirmation
Validation	Business justification, Windows authentication
Send elevation data for reporting	Yes
Reporting scope	Diagnostic data and all endpoint elevations

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

EPM001 - Elevation Settings Policy

Elevation settings policy

Summarize with Copilot Delete

Configuration settings Edit

Privilege management elevation client settings

Endpoint Privilege Management	Enabled
Default elevation response	Require user confirmation
Validation	Business justification, Windows authentication
Send elevation data for reporting	Yes
Reporting scope	Diagnostic data and all endpoint elevations

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

EPM001 - Elevation Settings Policy

Elevation settings policy

Summarize with Copilot Delete

Configuration settings Edit

Privilege management elevation client settings

Endpoint Privilege Management	Enabled
Default elevation response	Require user confirmation
Validation	Business justification, Windows authentication
Send elevation data for reporting	Yes
Reporting scope	Diagnostic data and all endpoint elevations

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

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

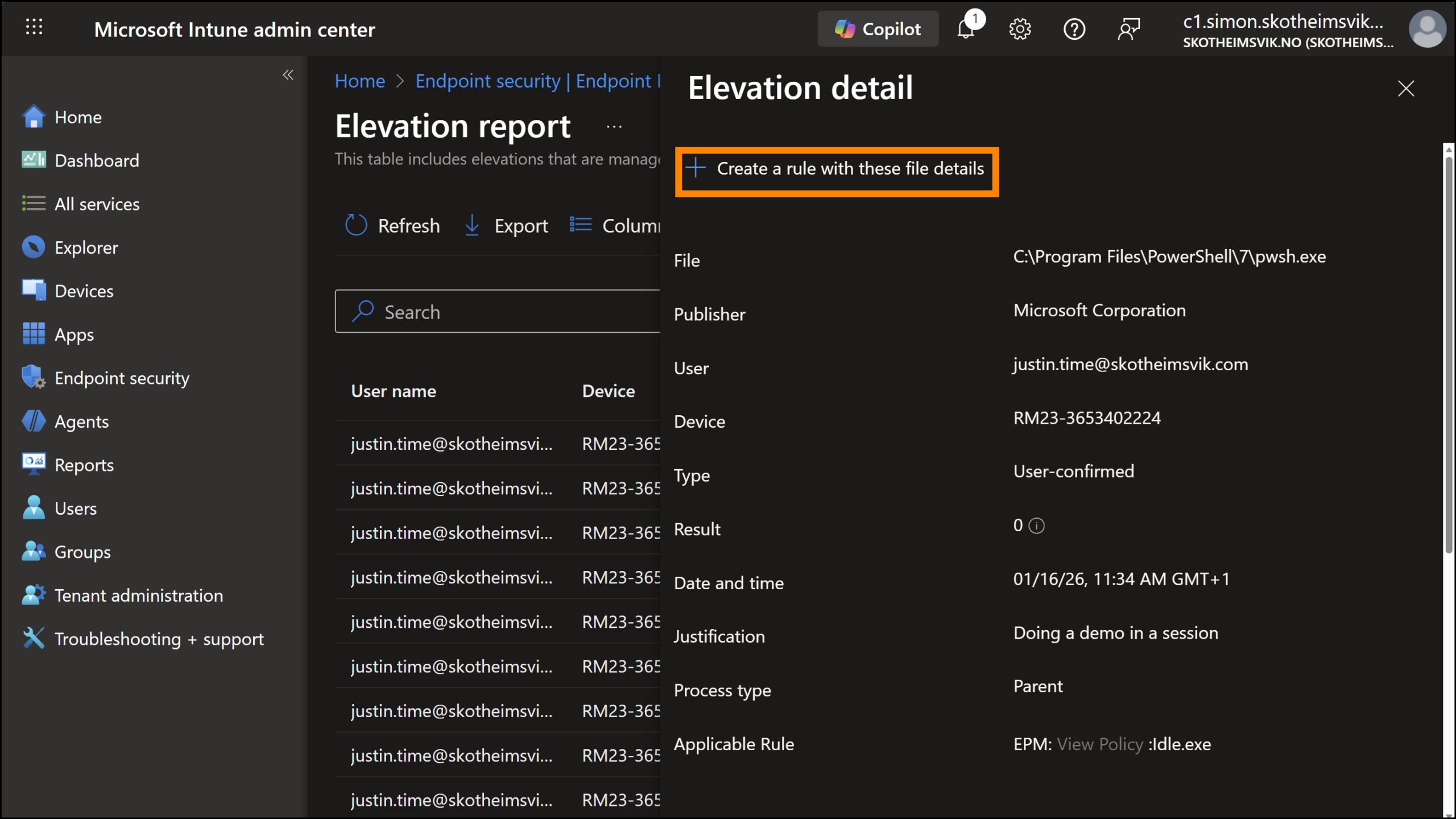
Overview | Reports | Policies | Reusable settings | Elevation requests

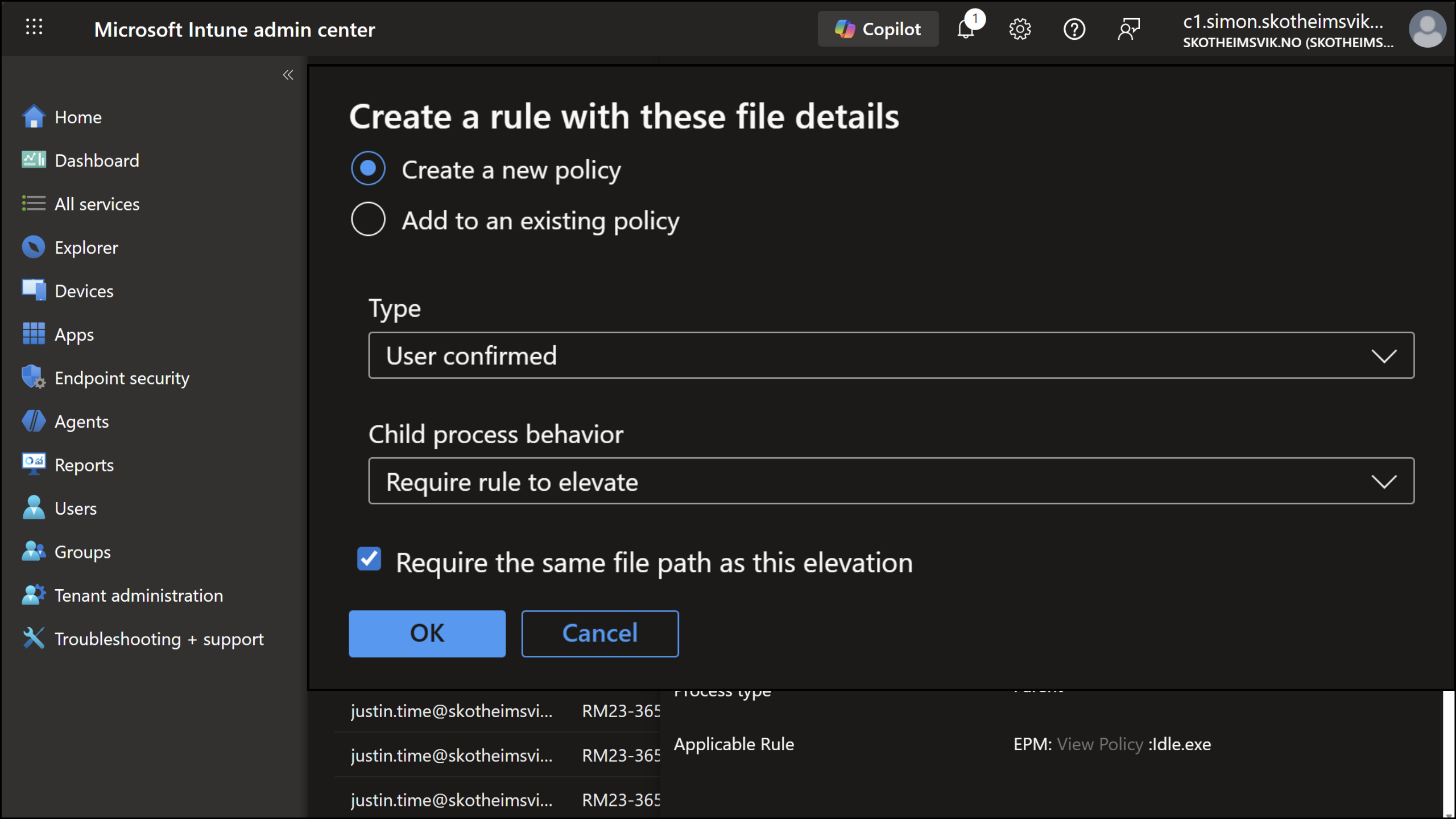
Elevation report
See all elevations, both managed and unmanaged by elevation policies.

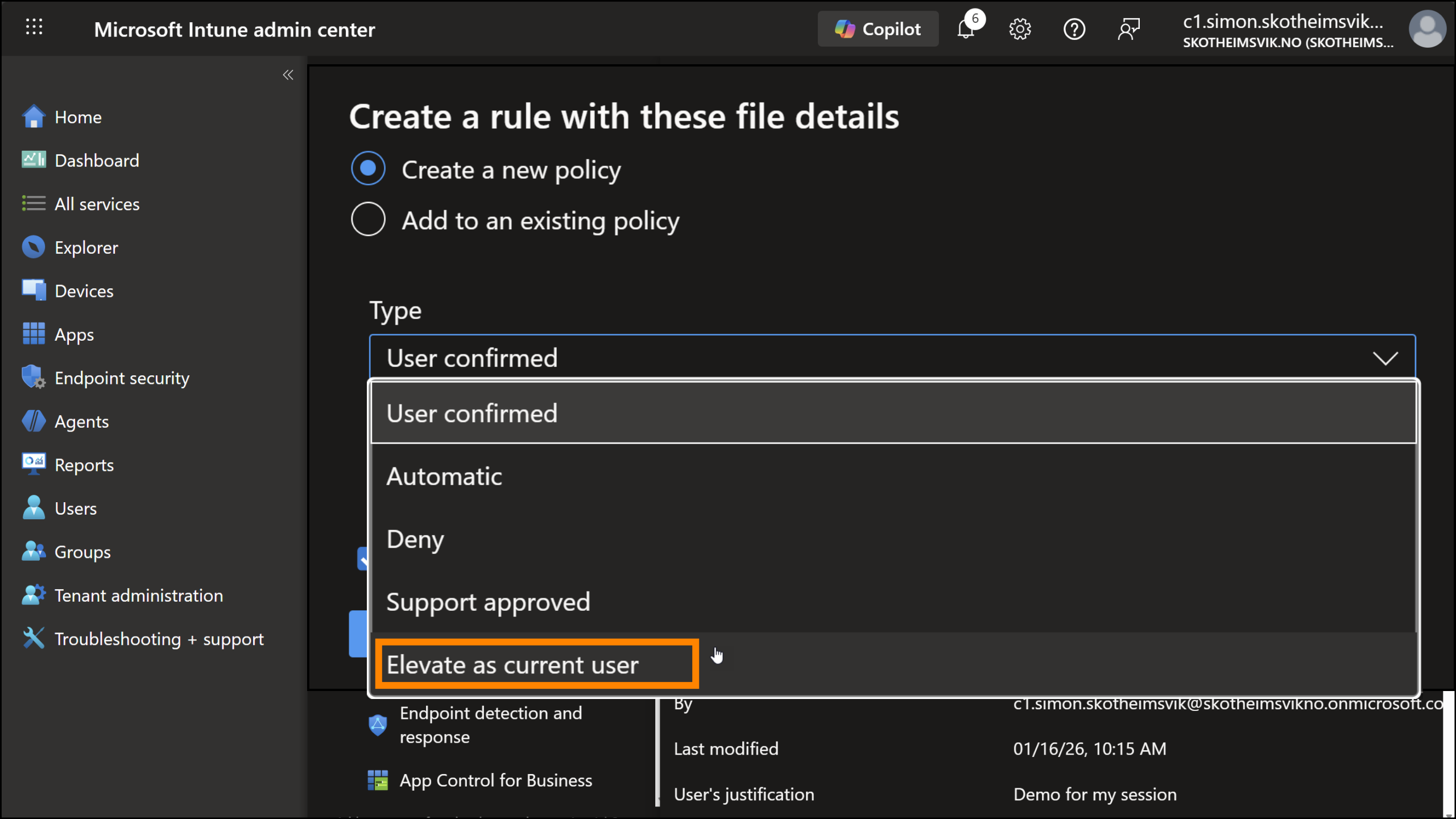
Managed elevation report
See the status of elevations that occurred inside the elevation management policies.

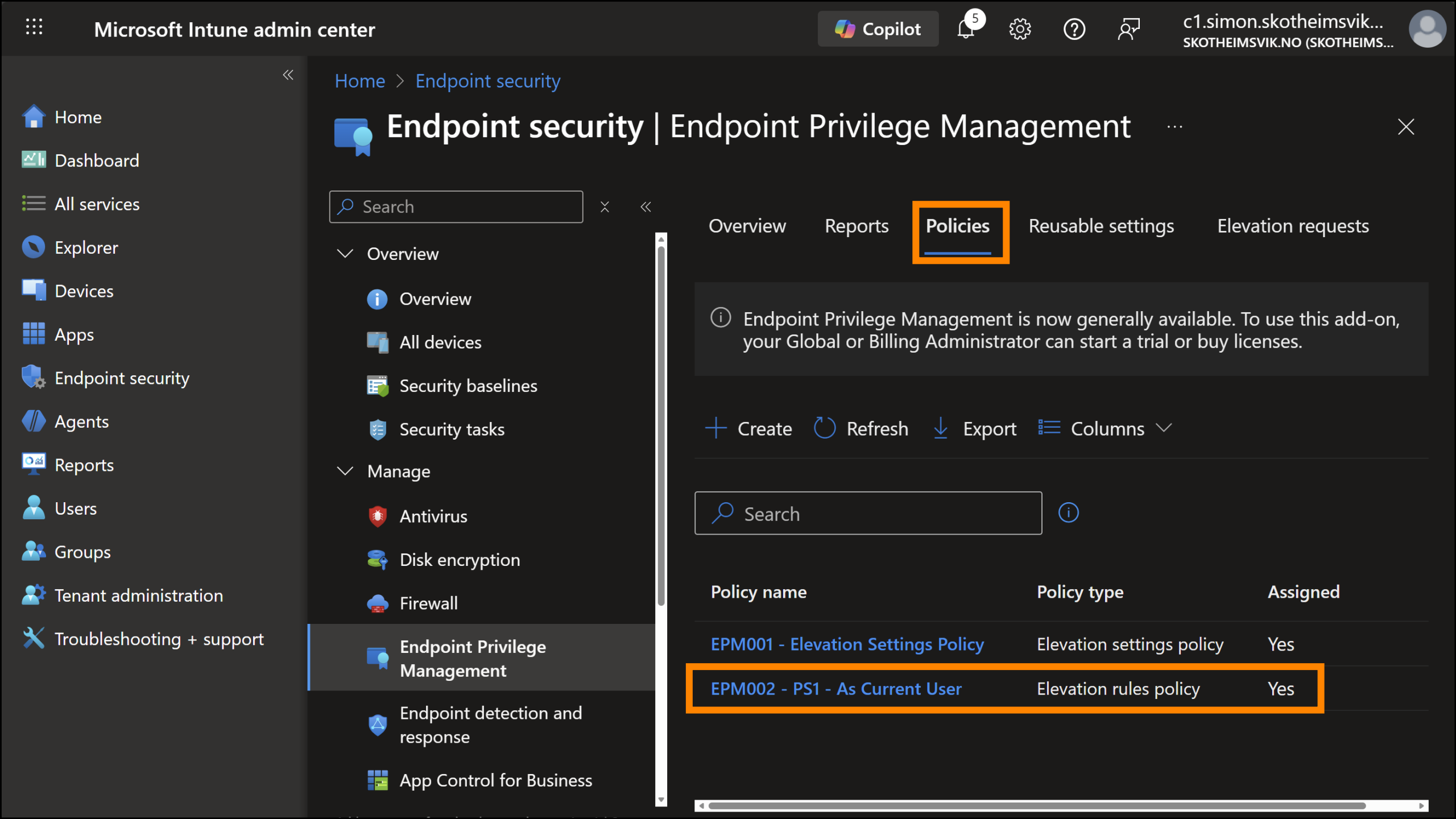
Elevation report by applications
See all elevations, both managed and unmanaged by application.

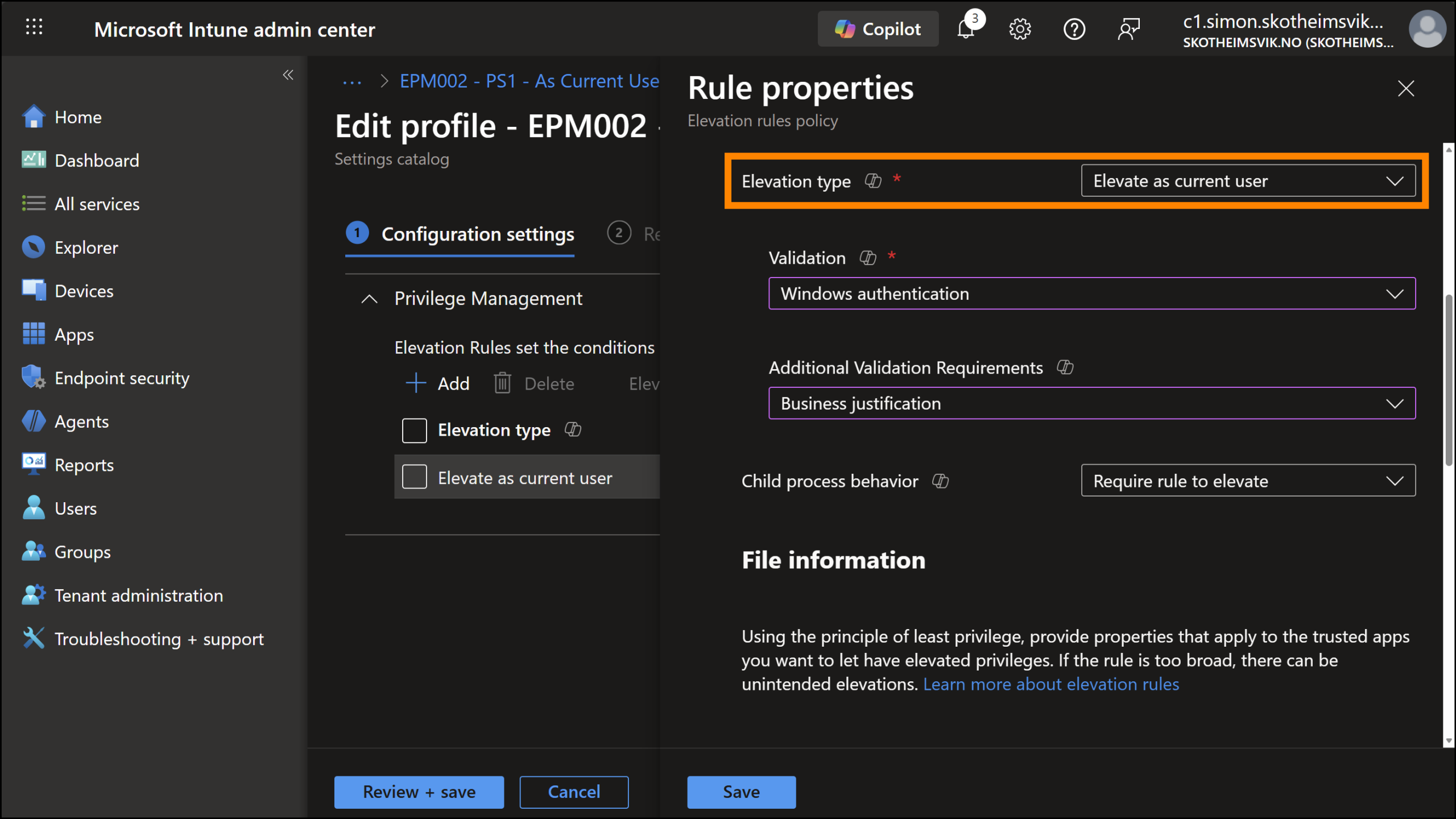
Elevation report by publisher
See number of elevations by each publisher.

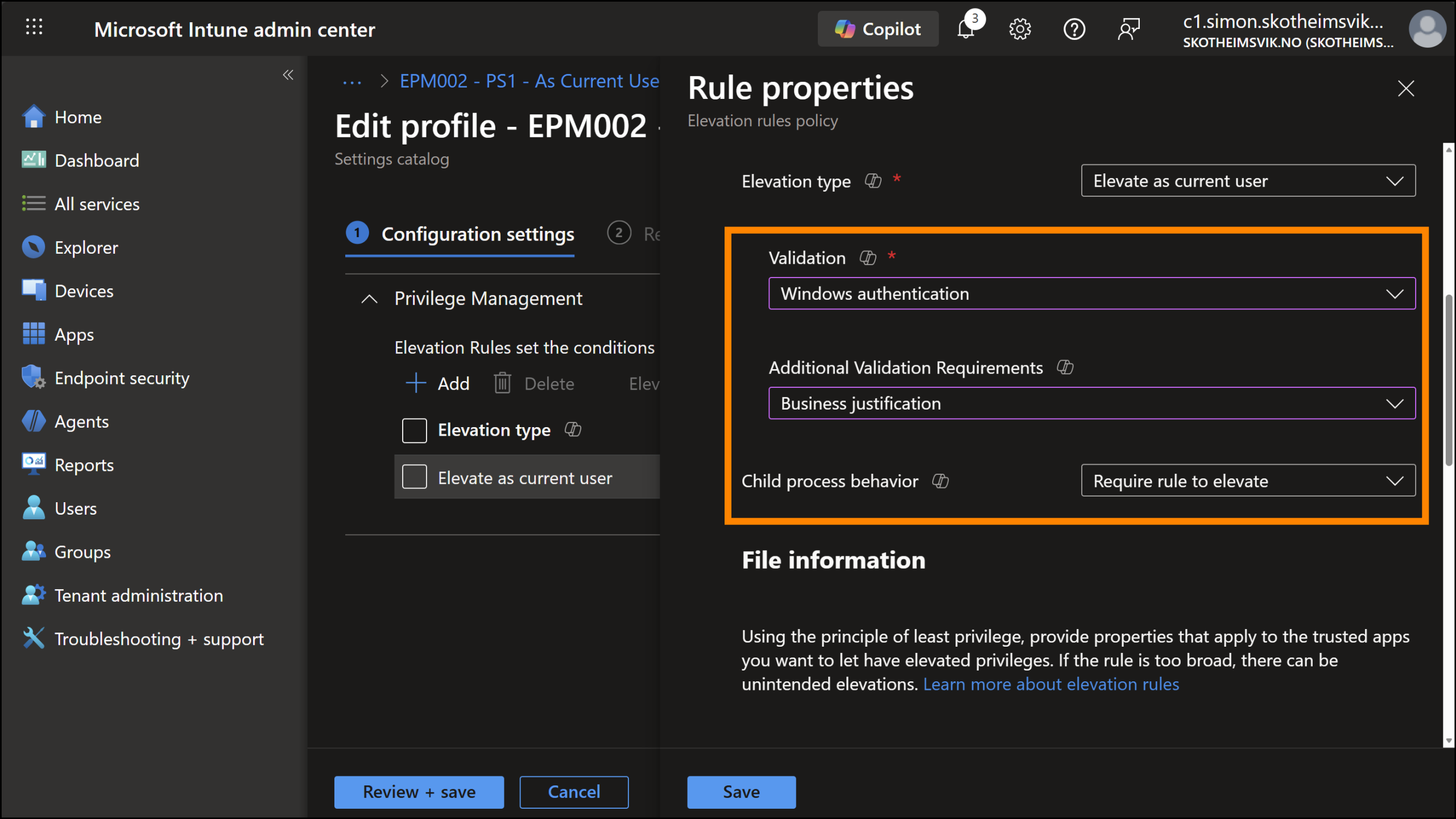

Microsoft Intune admin center
Copilot
1
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint I
Elevation report
This table includes elevations that are manag
Refresh
Export
Colum
Search
User name
Device
justin.time@skotheimsvi...
RM23-365
Elevation detail
Create a rule with these file details
File
C:\Program Files\PowerShell\7\pwsh.exe
Publisher
Microsoft Corporation
User
justin.time@skotheimsvik.com
Device
RM23-3653402224
Type
User-confirmed
Result
0
Date and time
01/16/26, 11:34 AM GMT+1
Justification
Doing a demo in a session
Process type
Parent
Applicable Rule
EPM: View Policy :Idle.exe

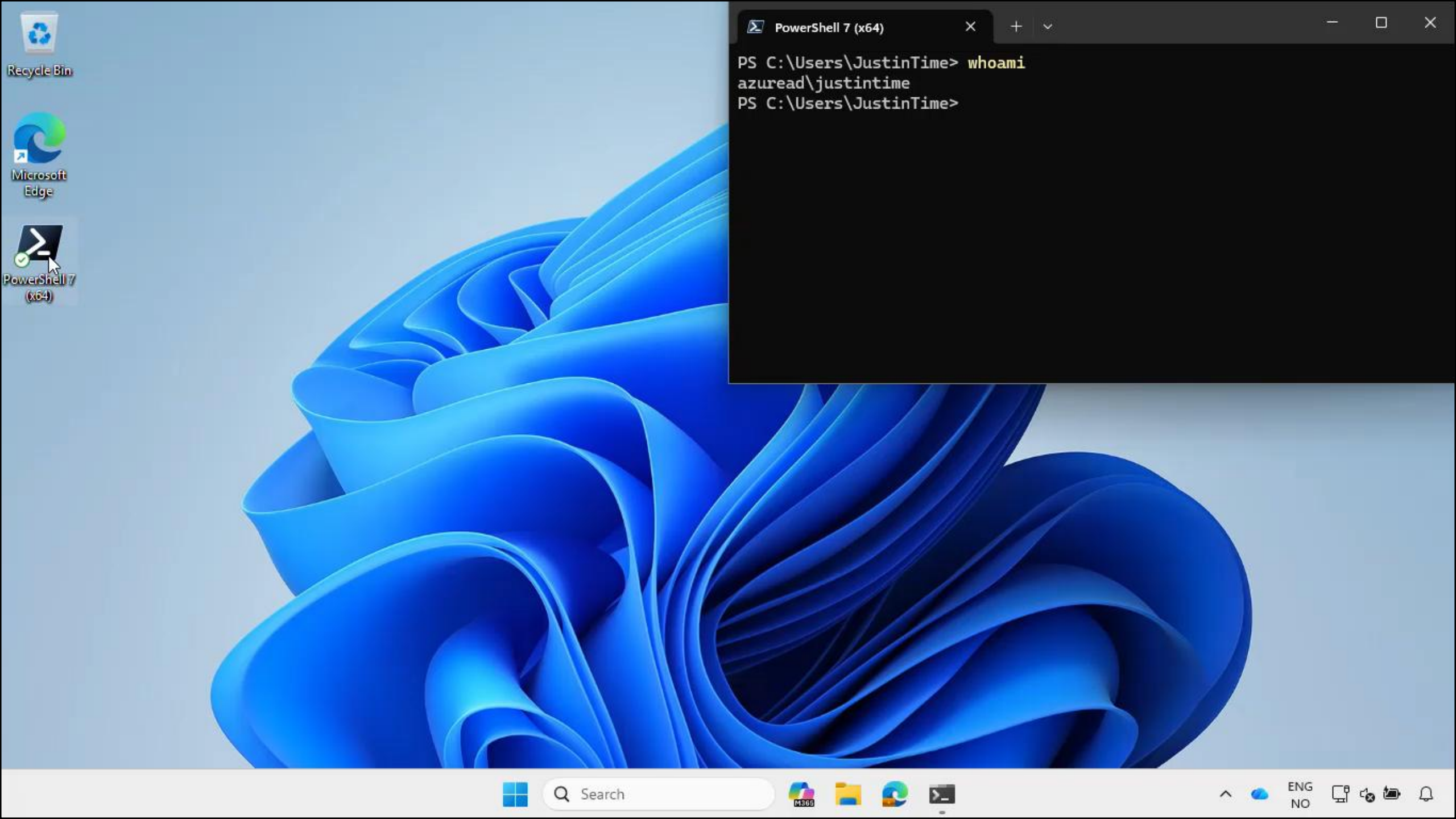

Microsoft Intune admin center
Copilot
1
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Create a rule with these file details
Create a new policy
Add to an existing policy
Type
User confirmed
Child process behavior
Require rule to elevate
Require the same file path as this elevation
OK
Cancel
justin.time@skotheimsvi... RM23-365
justin.time@skotheimsvi... RM23-365
justin.time@skotheimsvi... RM23-365
Applicable Rule
EPM: View Policy :Idle.exe


Microsoft Intune admin center
Copilot
6
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Create a rule with these file details
Create a new policy
Add to an existing policy
Type
User confirmed
User confirmed
Automatic
Deny
Support approved
Elevate as current user
Endpoint detection and response
App Control for Business
By
c1.simon.skotheimsvik@skotheimsvikno.onmicrosoft.co
Last modified
01/16/26, 10:15 AM
User's justification
Demo for my session


Microsoft Intune admin center
Copilot
5
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
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
Overview
Reports
Policies
Reusable settings
Elevation requests
Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Administrator can start a trial or buy licenses.
Create
Refresh
Export
Columns
Search
Policy name
Policy type
Assigned
EPM001 - Elevation Settings Policy
Elevation settings policy
Yes
EPM002 - PS1 - As Current User
Elevation rules policy
Yes


Microsoft Intune admin center
Copilot
3
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
EPM002 - PS1 - As Current Use
Edit profile - EPM002
Settings catalog
1 Configuration settings
2 Re
Privilege Management
Elevation Rules set the conditions
Add
Delete
Elev
Elevation type
Elevate as current user
Review + save
Cancel
Rule properties
Elevation rules policy
Elevation type * Elevate as current user
Validation * Windows authentication
Additional Validation Requirements Business justification
Child process behavior Require rule to elevate
File information
Using the principle of least privilege, provide properties that apply to the trusted apps you want to let have elevated privileges. If the rule is too broad, there can be unintended elevations. Learn more about elevation rules
Save


Microsoft Intune admin center
Copilot
3
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
EPM002 - PS1 - As Current Use
Edit profile - EPM002
Settings catalog
1 Configuration settings
2 Re
Privilege Management
Elevation Rules set the conditions
Add
Delete
Elev
Elevation type
Elevate as current user
Review + save
Cancel
Rule properties
Elevation rules policy
Elevation type *
Elevate as current user
Validation *
Windows authentication
Additional Validation Requirements
Business justification
Child process behavior
Require rule to elevate
File information
Using the principle of least privilege, provide properties that apply to the trusted apps you want to let have elevated privileges. If the rule is too broad, there can be unintended elevations. Learn more about elevation rules
Save


Recycle Bin
Microsoft Edge
PowerShell 7 (x64)
PowerShell 7 (x64)
PS C:\Users\JustinTime> whoami
azuread\justintime
PS C:\Users\JustinTime>
Search
ENG
NO

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

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...

Refresh Export Columns 11 items

Search

Date: After 01/12/2026, 03:26 PM

Add filters

User name	Device	File	Result
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\system32\whoami.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Program Files\PowerShell\7\pwsh.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\system32\whoami.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Program Files\PowerShell\7\pwsh.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\System32\cmd.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\System32\cmd.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\System32\cmd.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\system32\whoami.exe	Completed
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\System32\cmd.exe	Completed

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

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...

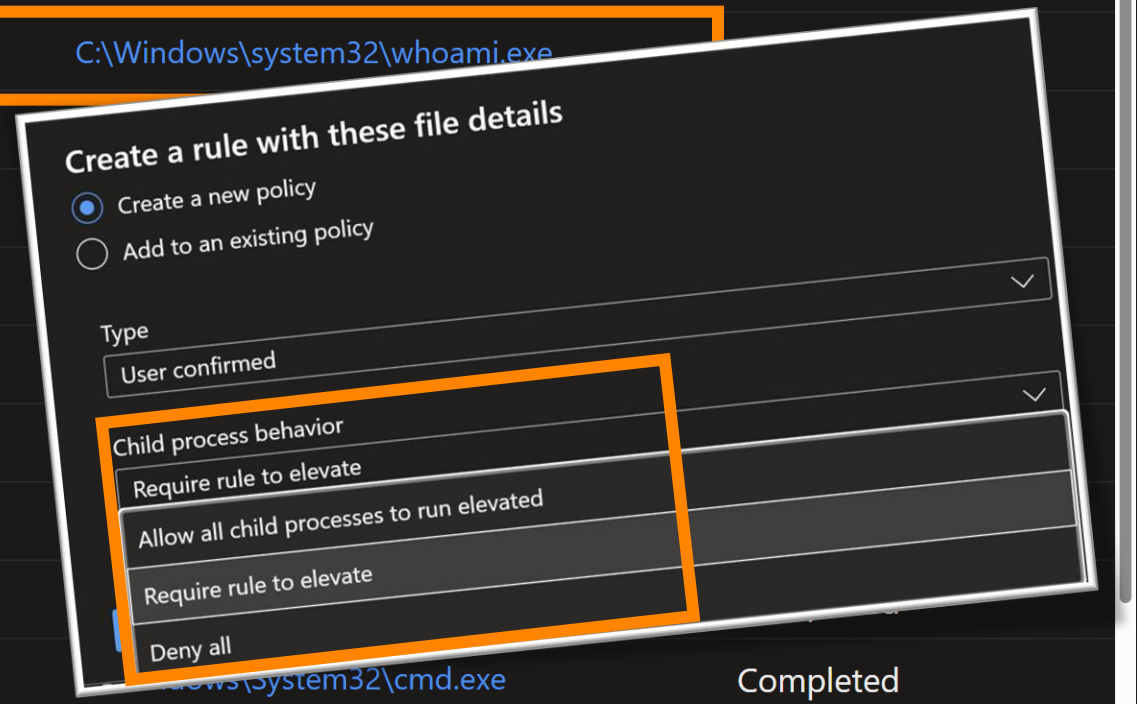
Refresh Export Columns 11 items

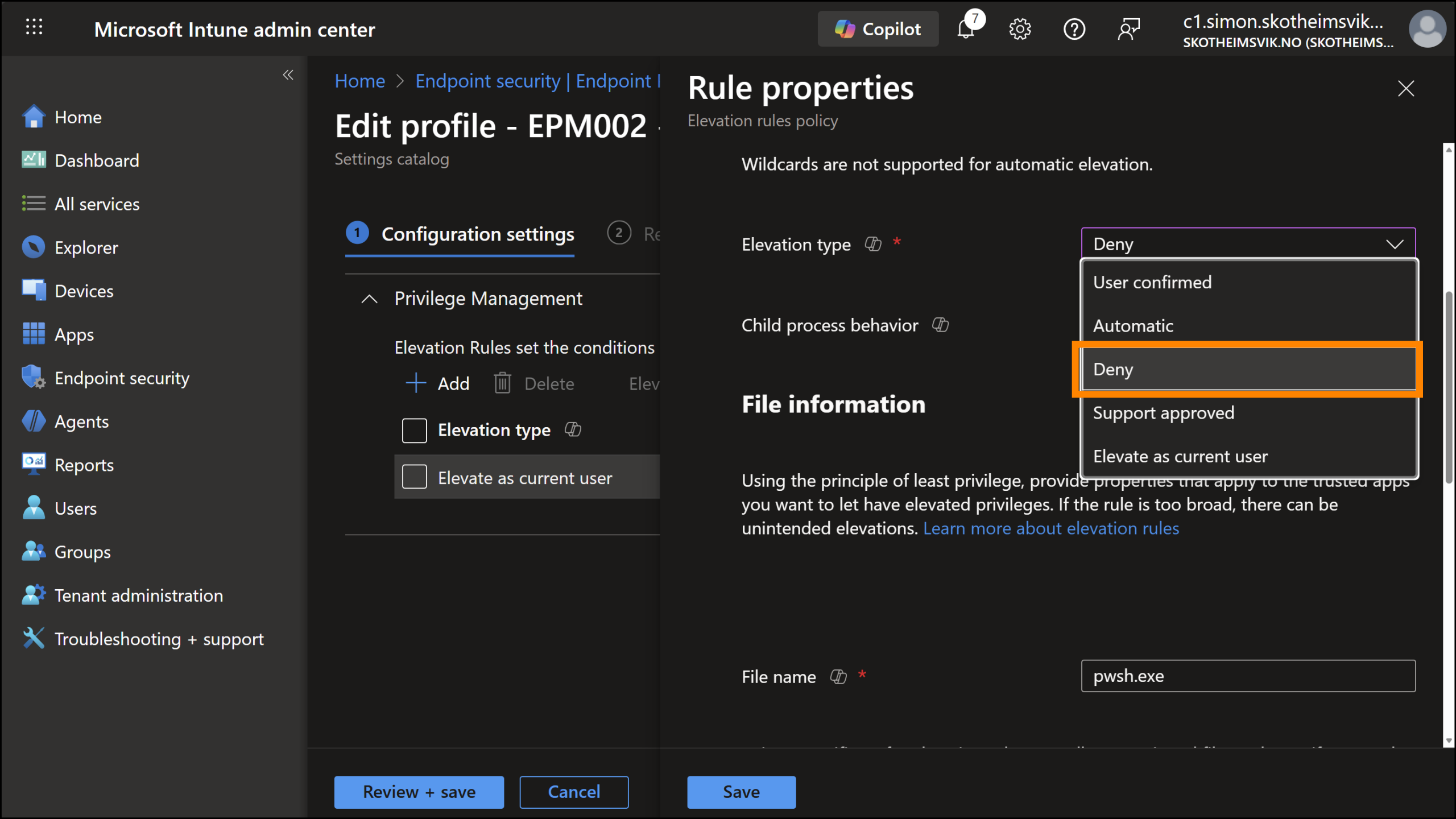
Search

Date: After 01/12/2026, 03:26 PM

Add filters

User name	Device	File	Result
justin.time@skotheimsvi...	RM23-3653402224	C:\Windows\system32\whoami.exe	
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224		
justin.time@skotheimsvi...	RM23-3653402224	System32\cmd.exe	Completed




Microsoft Intune admin center
Copilot
7
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Endpoint I
Edit profile - EPM002
Settings catalog
1 Configuration settings
2 Re
Privilege Management
Elevation Rules set the conditions
Add
Delete
Elev
Elevation type
Elevate as current user
Review + save
Cancel
Save
Rule properties
Elevation rules policy
Wildcards are not supported for automatic elevation.
Elevation type *
Deny
User confirmed
Automatic
Deny
Support approved
Elevate as current user
Child process behavior
File information
Using the principle of least privilege, provide properties that apply to the trusted apps you want to let have elevated privileges. If the rule is too broad, there can be unintended elevations. Learn more about elevation rules
File name *
pwsh.exe

8 Admin Tasks

Your centralized “single pane of glass”

Feb 2026

Nov 2025

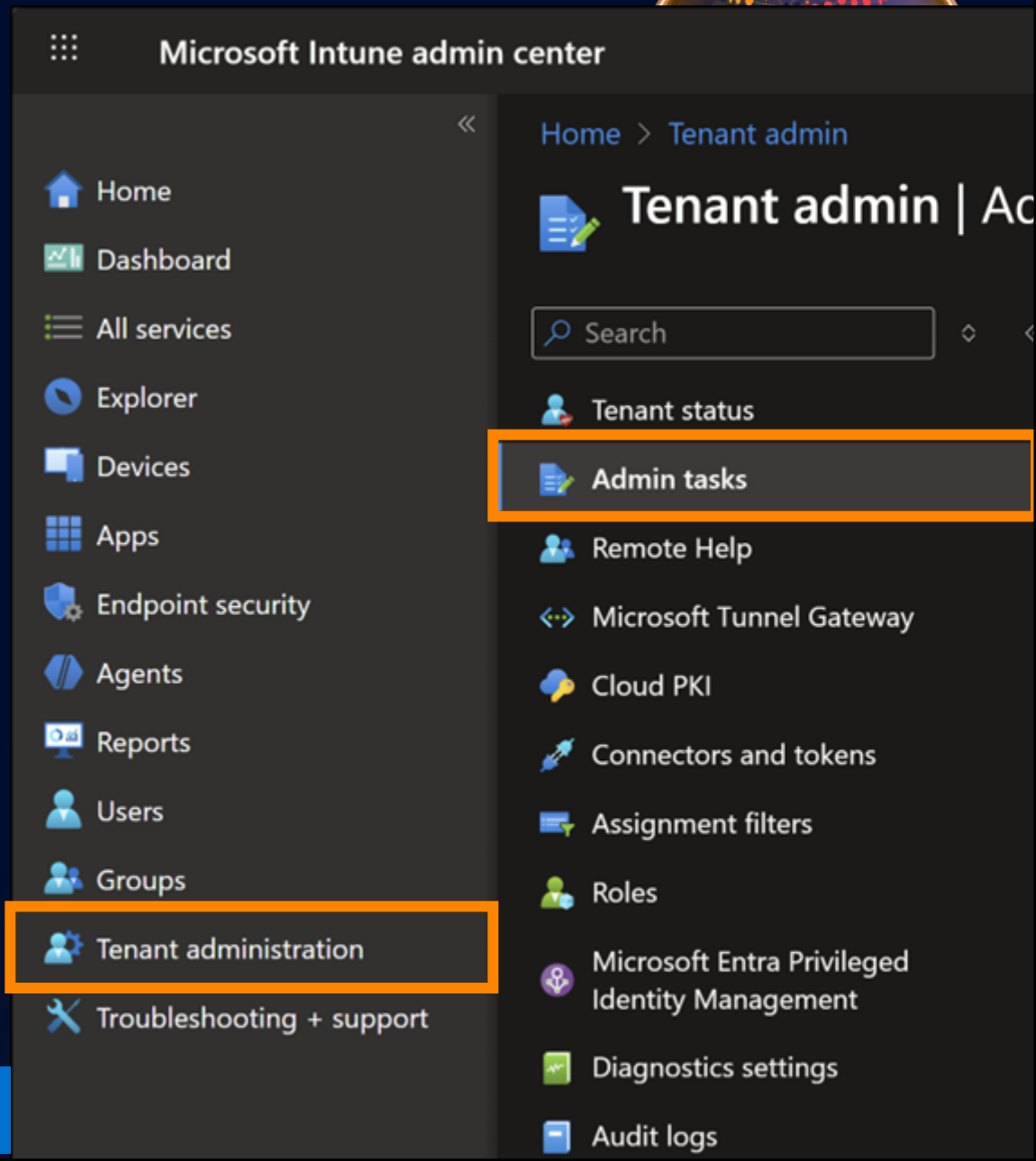
https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#manage-tasks-and-requests-from-the-centralized-admin-tasks-node-in-microsoft-intune-public-preview

Admin Tasks

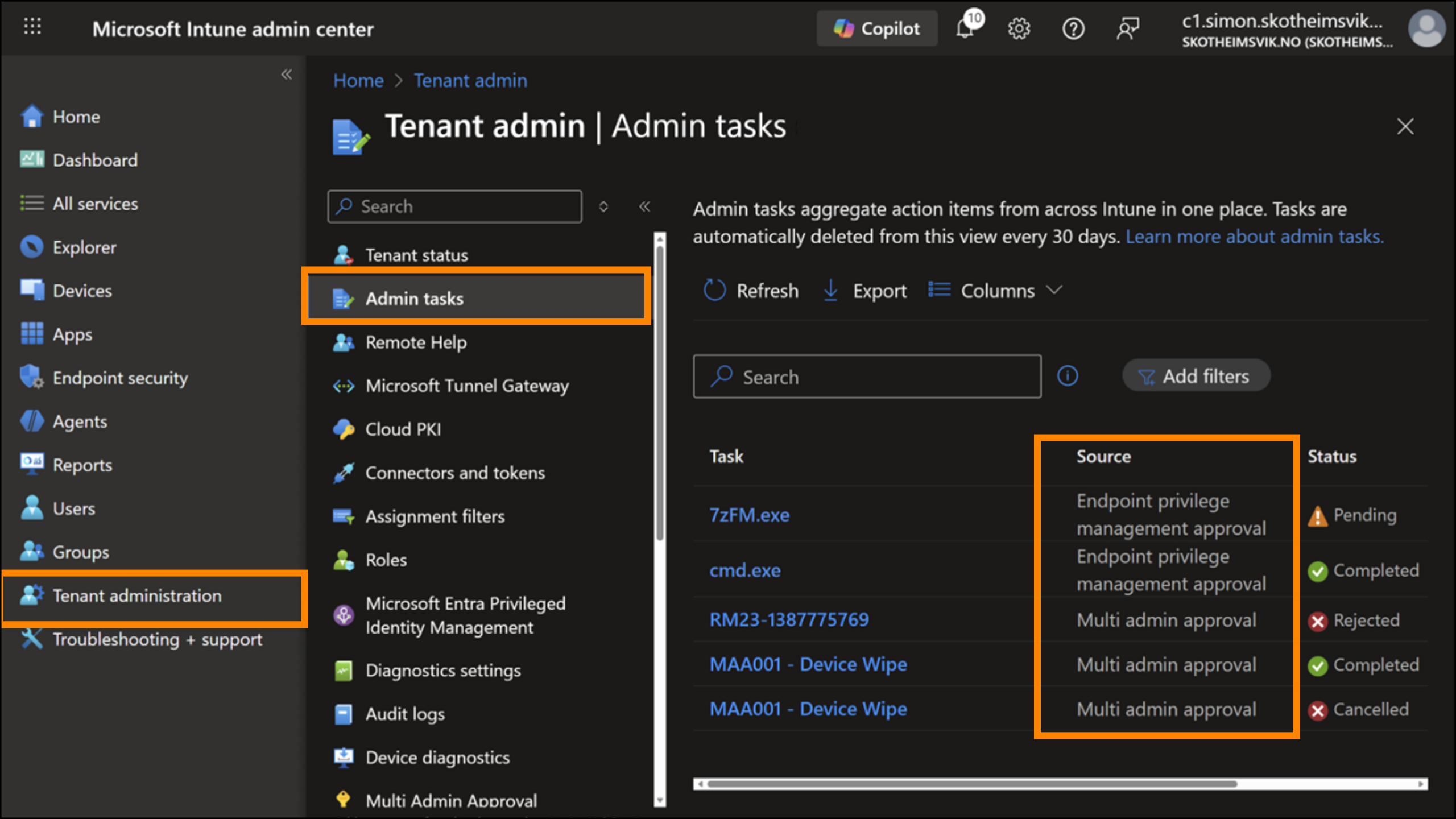
Centralized view to discover, organize, and act on security tasks and user elevation requests

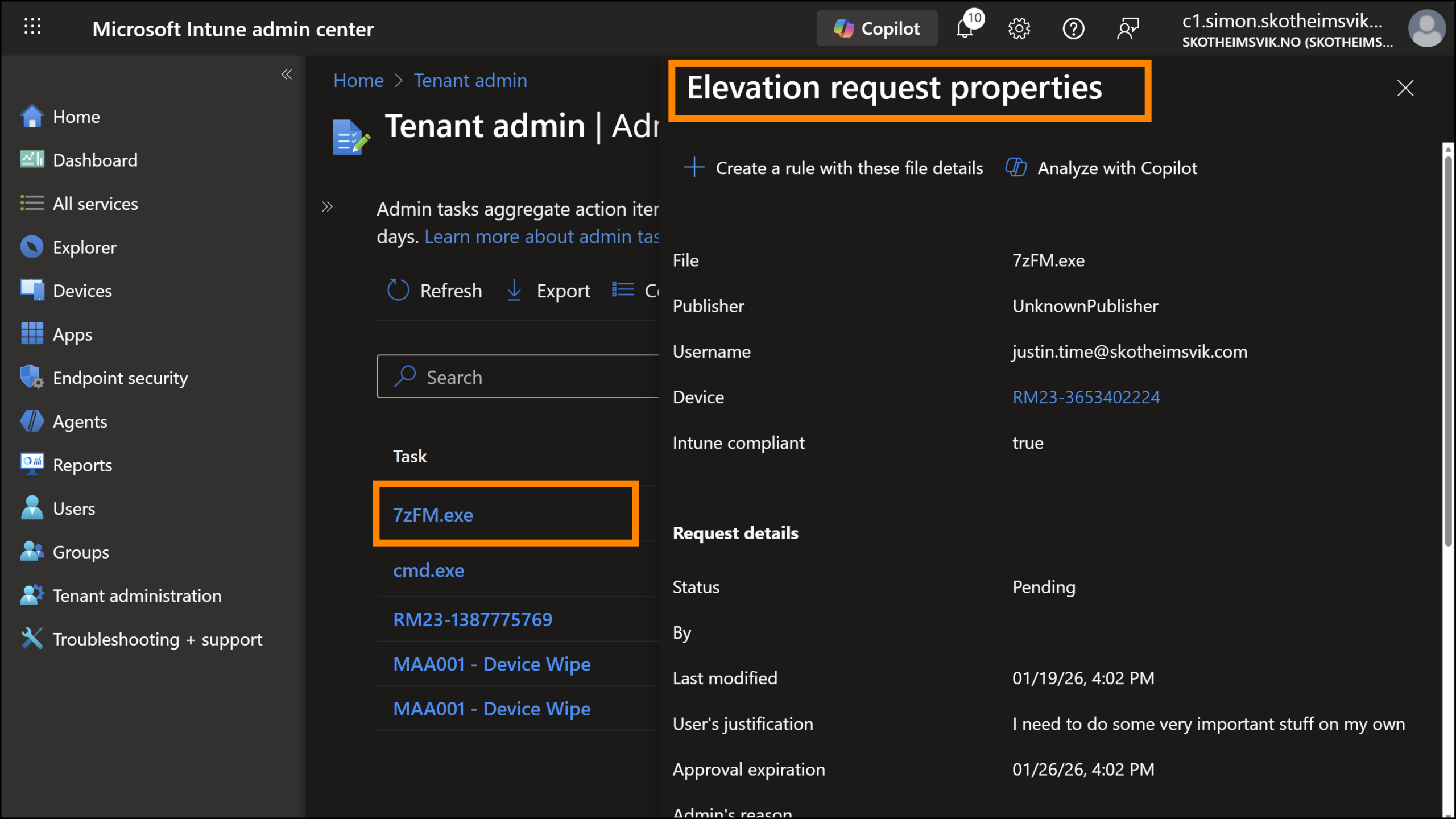
The following task types are supported:

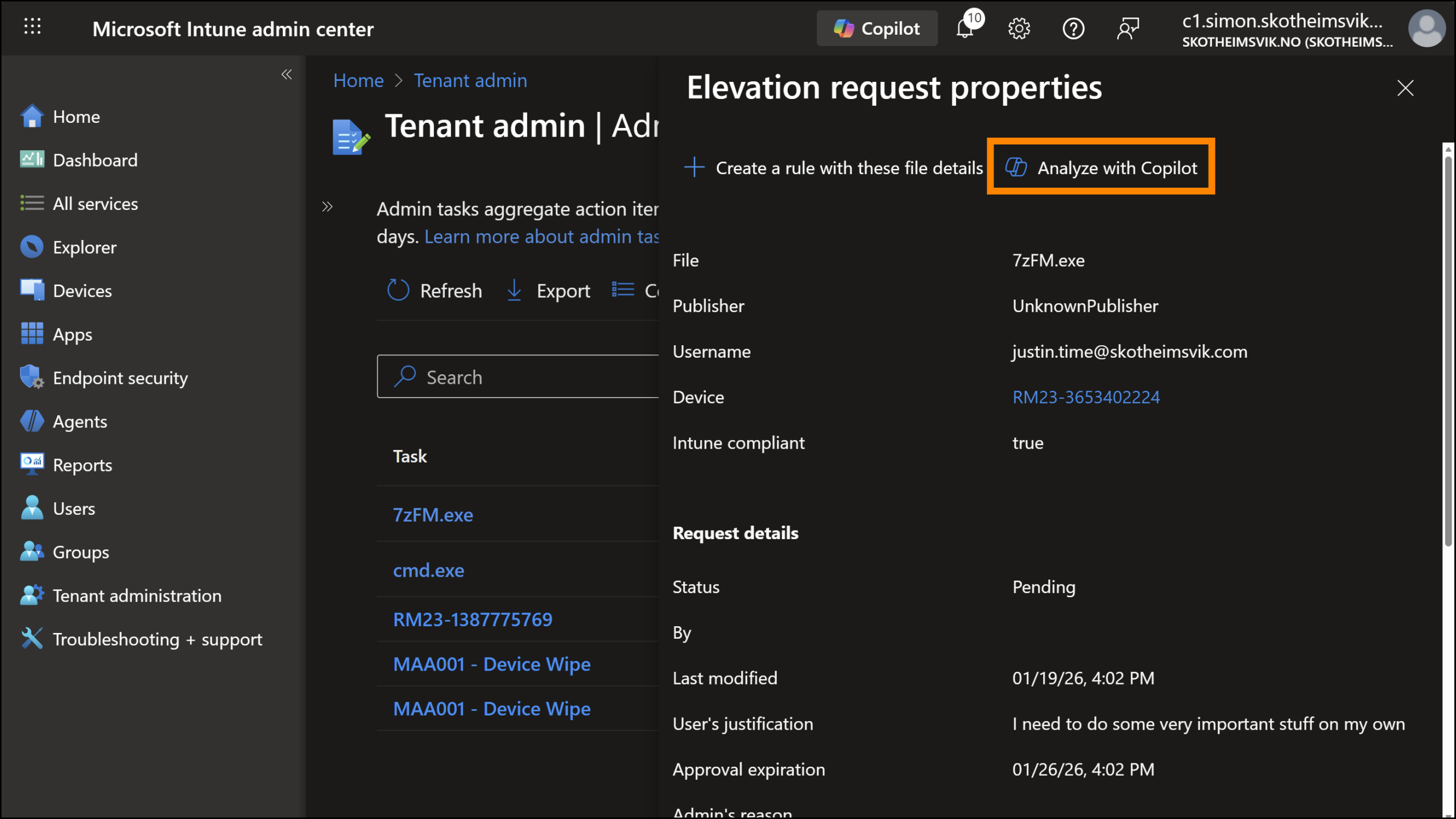
- Endpoint Privilege Management requests
- Microsoft Defender security tasks
- Multi Admin Approval requests

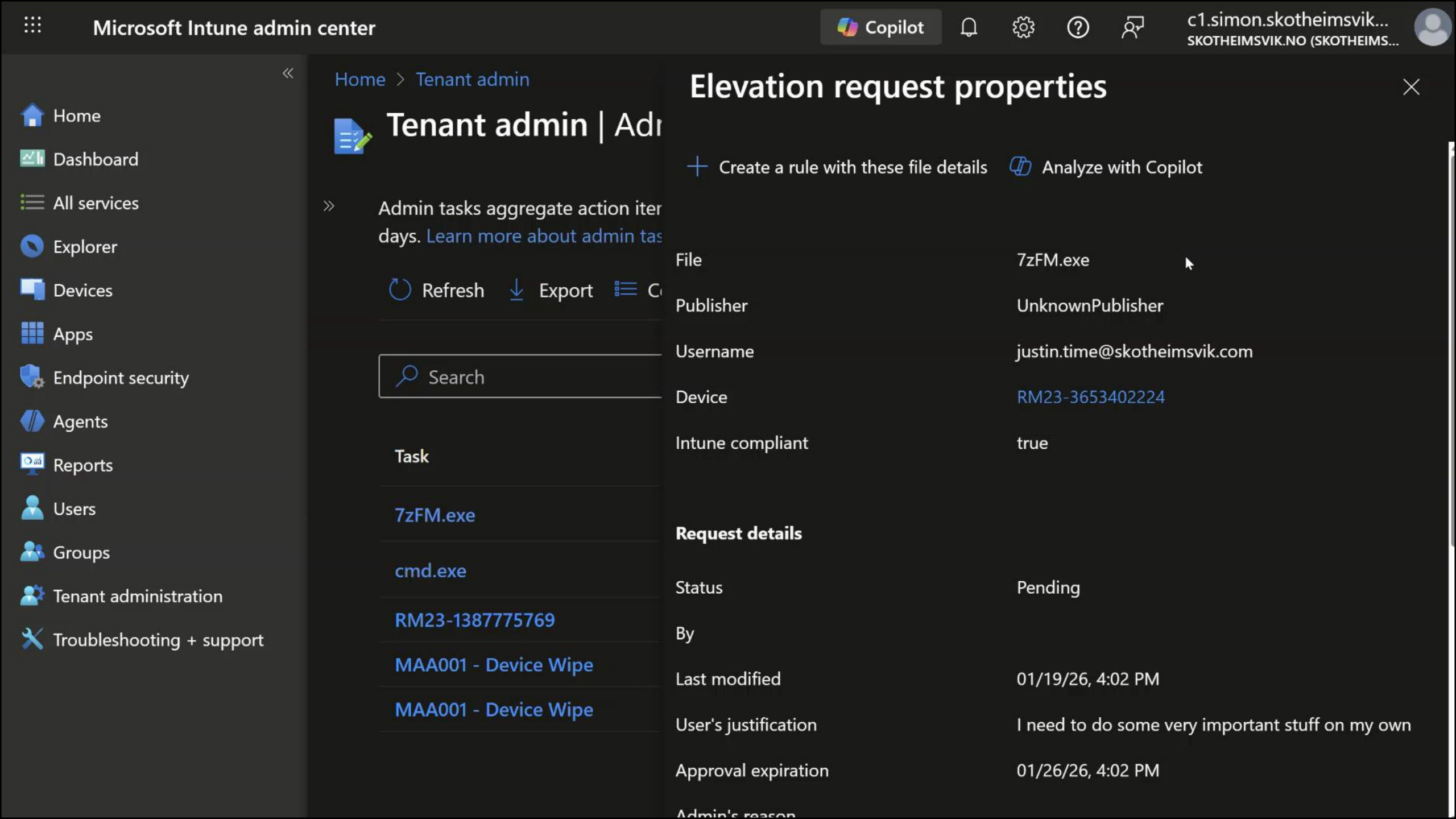


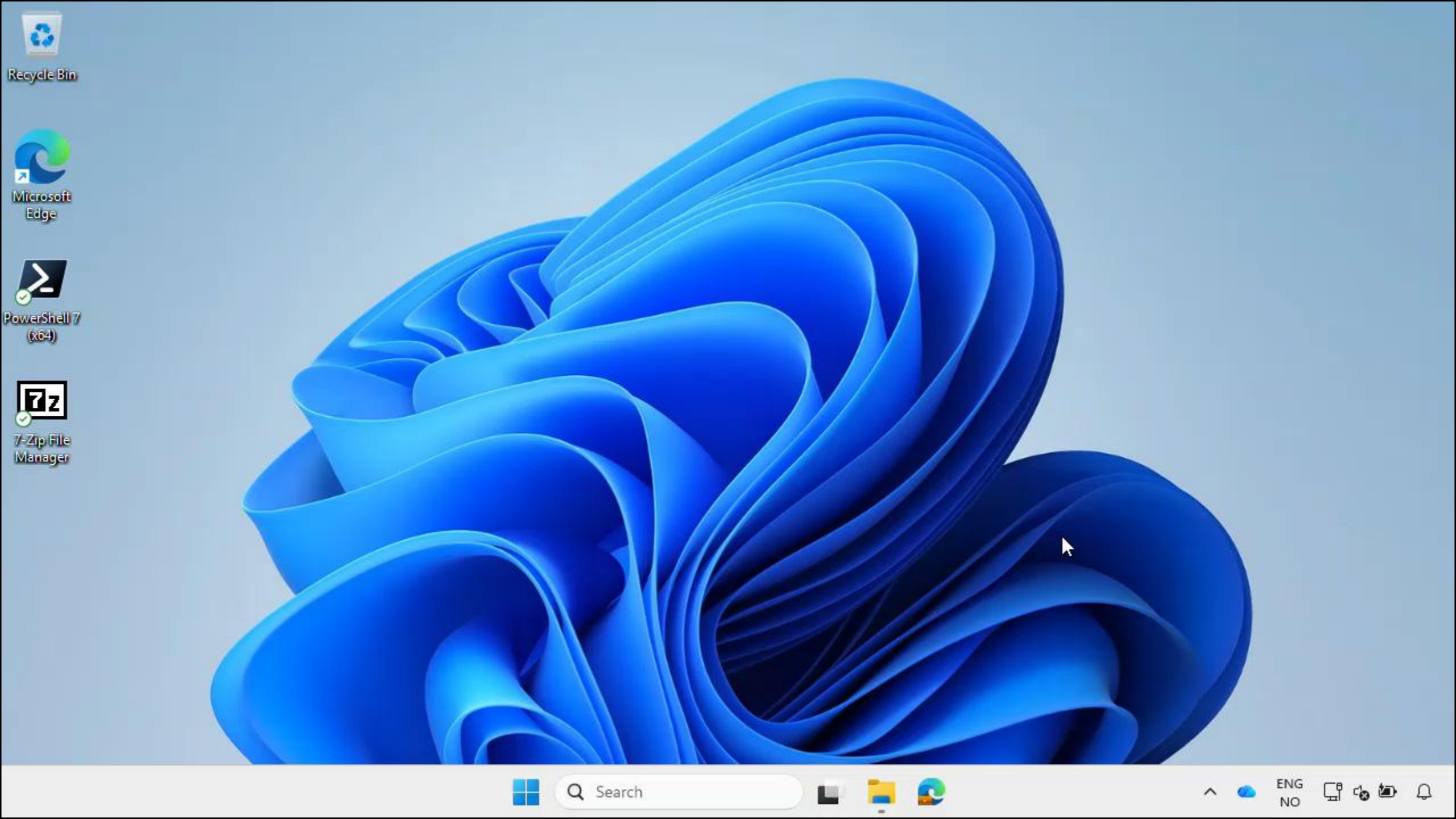
https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#manage-tasks-and-requests-from-the-centralized-admin-tasks-node-in-microsoft-intune-public-preview

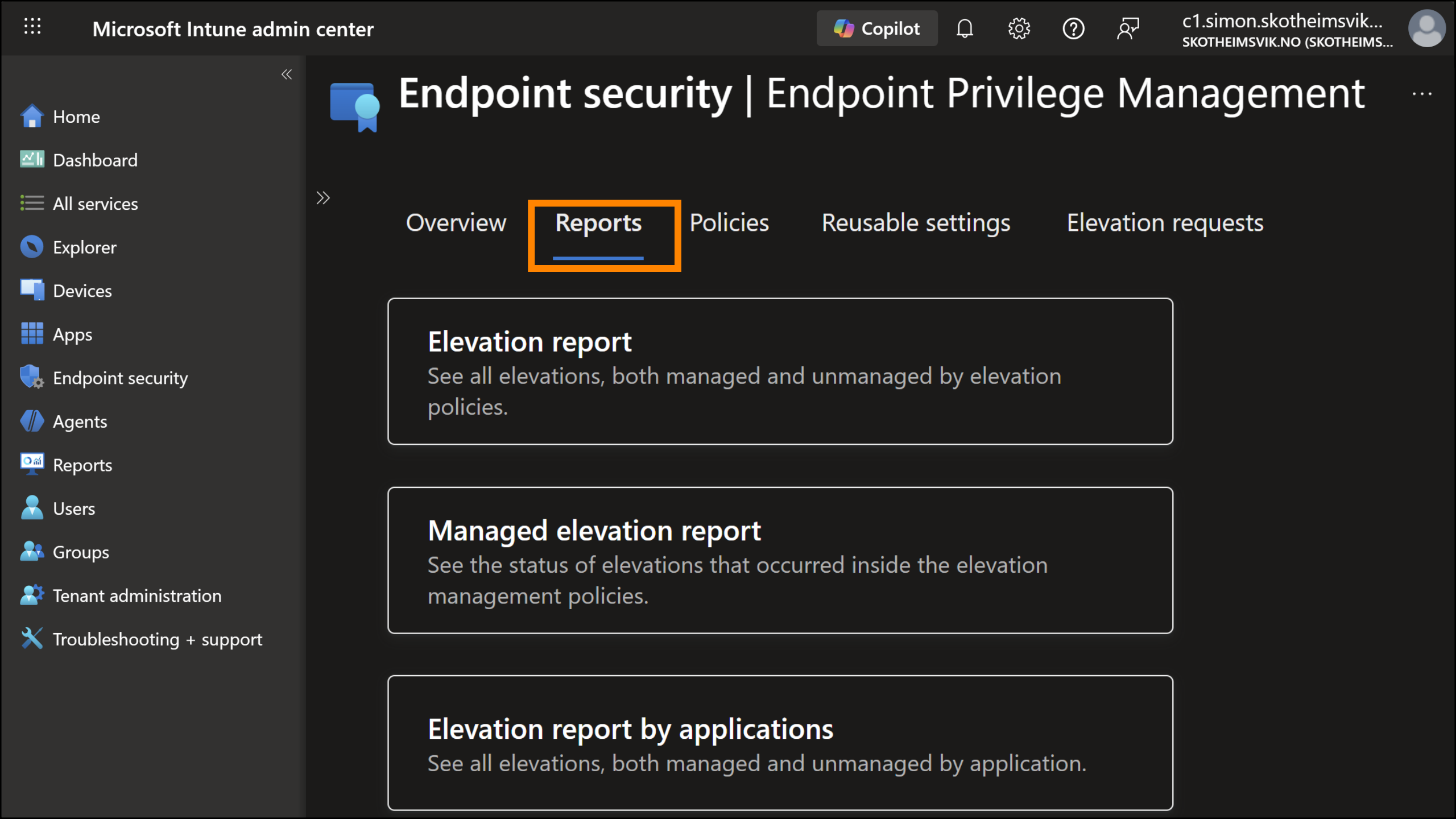

Microsoft Intune admin center
Copilot
10
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Admin tasks
Search
Tenant status
Admin tasks
Remote Help
Microsoft Tunnel Gateway
Cloud PKI
Connectors and tokens
Assignment filters
Roles
Microsoft Entra Privileged Identity Management
Diagnostics settings
Audit logs
Device diagnostics
Multi Admin Approval
Admin tasks aggregate action items from across Intune in one place. Tasks are automatically deleted from this view every 30 days. Learn more about admin tasks.
Refresh
Export
Columns
Search
Add filters
Task
Source
Status
7zFM.exe
Endpoint privilege management approval
Pending
cmd.exe
Endpoint privilege management approval
Completed
RM23-1387775769
Multi admin approval
Rejected
MAA001 - Device Wipe
Multi admin approval
Completed
MAA001 - Device Wipe
Multi admin approval
Cancelled


Microsoft Intune admin center
Copilot
10
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Adr
Admin tasks aggregate action iter
days. Learn more about admin tas
Refresh
Export
Search
Task
7zFM.exe
cmd.exe
RM23-1387775769
MAA001 - Device Wipe
MAA001 - Device Wipe
Elevation request properties
Create a rule with these file details
Analyze with Copilot
File
7zFM.exe
Publisher
UnknownPublisher
Username
justin.time@skotheimsvik.com
Device
RM23-3653402224
Intune compliant
true
Request details
Status
Pending
By
Last modified
01/19/26, 4:02 PM
User's justification
I need to do some very important stuff on my own
Approval expiration
01/26/26, 4:02 PM
Admin's reason


Microsoft Intune admin center
Copilot
10
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Adr
Admin tasks aggregate action iter
days. Learn more about admin tas
Refresh
Export
Search
Task
7zFM.exe
cmd.exe
RM23-1387775769
MAA001 - Device Wipe
MAA001 - Device Wipe
Elevation request properties
Create a rule with these file details
Analyze with Copilot
File
7zFM.exe
Publisher
UnknownPublisher
Username
justin.time@skotheimsvik.com
Device
RM23-3653402224
Intune compliant
true
Request details
Status
Pending
By
Last modified
01/19/26, 4:02 PM
User's justification
I need to do some very important stuff on my own
Approval expiration
01/26/26, 4:02 PM
Admin's reason


Microsoft Intune admin center
Copilot
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Tenant admin
Tenant admin | Adı
Admin tasks aggregate action iter
days. Learn more about admin tas
Refresh
Export
Search
Task
7zFM.exe
cmd.exe
RM23-1387775769
MAA001 - Device Wipe
MAA001 - Device Wipe
Elevation request properties
Create a rule with these file details
Analyze with Copilot
File
7zFM.exe
Publisher
UnknownPublisher
Username
justin.time@skotheimsvik.com
Device
RM23-3653402224
Intune compliant
true
Request details
Status
Pending
By
Last modified
01/19/26, 4:02 PM
User's justification
I need to do some very important stuff on my own
Approval expiration
01/26/26, 4:02 PM


Recycle Bin
Microsoft Edge
PowerShell 7 (x64)
7-Zip File Manager
Search
ENG
NO


Microsoft Intune admin center
Copilot
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Endpoint security | Endpoint Privilege Management
Overview
Reports
Policies
Reusable settings
Elevation requests
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.

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

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.

Elevation report by user
See number of elevations by each user.

Denied elevation report
See number of denied elevations by each user.

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

Elevation report by User

See number of elevations by each User

Due to the amount of data, this report might take some time to generate and will expire after 72 hours.

Generate again | Cancel | Report generated 02/13/2026, 10:18 AM

Columns | 1 item

Search

User name	Managed elevations	Unmanaged elevations	Total elevations
justin.time@skotheimsvik.com	16	0	16

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

Elevation report by Application for a month

See number of elevations for a month

Refresh Columns

Search

User name	Device	File	Type	Monthly Elevations
justin.time@skotheimsvik.com	RM23-3653402224	whoami.exe	Automatic	5
justin.time@skotheimsvik.com	RM23-3653402224	pwsh.exe	User-confirmed	3
justin.time@skotheimsvik.com	RM23-3653402224	cmd.exe	User-confirmed	3
justin.time@skotheimsvik.com	RM23-3653402224	cmd.exe	Support-approved	2
justin.time@skotheimsvik.com	RM23-3653402224	7zFM.exe	Support-approved	1
justin.time@skotheimsvik.com	RM23-3653402224	7zFM.exe	User-confirmed	1
justin.time@skotheimsvik.com	RM23-3653402224	shutdown.exe	Automatic	1

9 Restore at first sign-in

Kick-start your users on their fresh installed Windows device

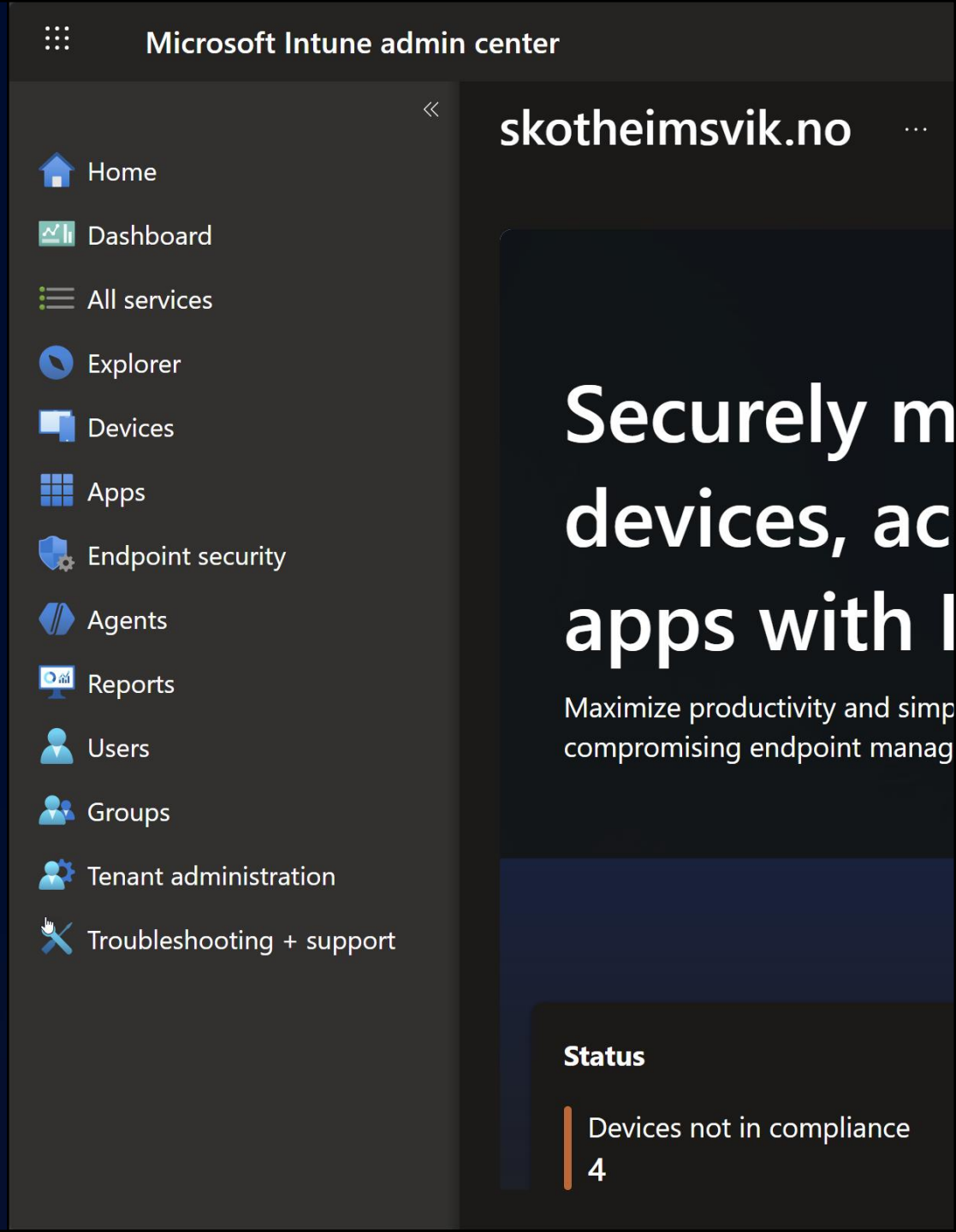
Feb 2026

Nov 2025

https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/whats-new#manage-tasks-and-requests-from-the-centralized-admin-tasks-node-in-microsoft-intune-public-preview

Restore at First Sign-in

- OneDrive for Business Known Folder Move
- Enterprise State Roaming in Entra ID
- Backup Windows settings
- Restore Windows settings



Restore at First Sign-in

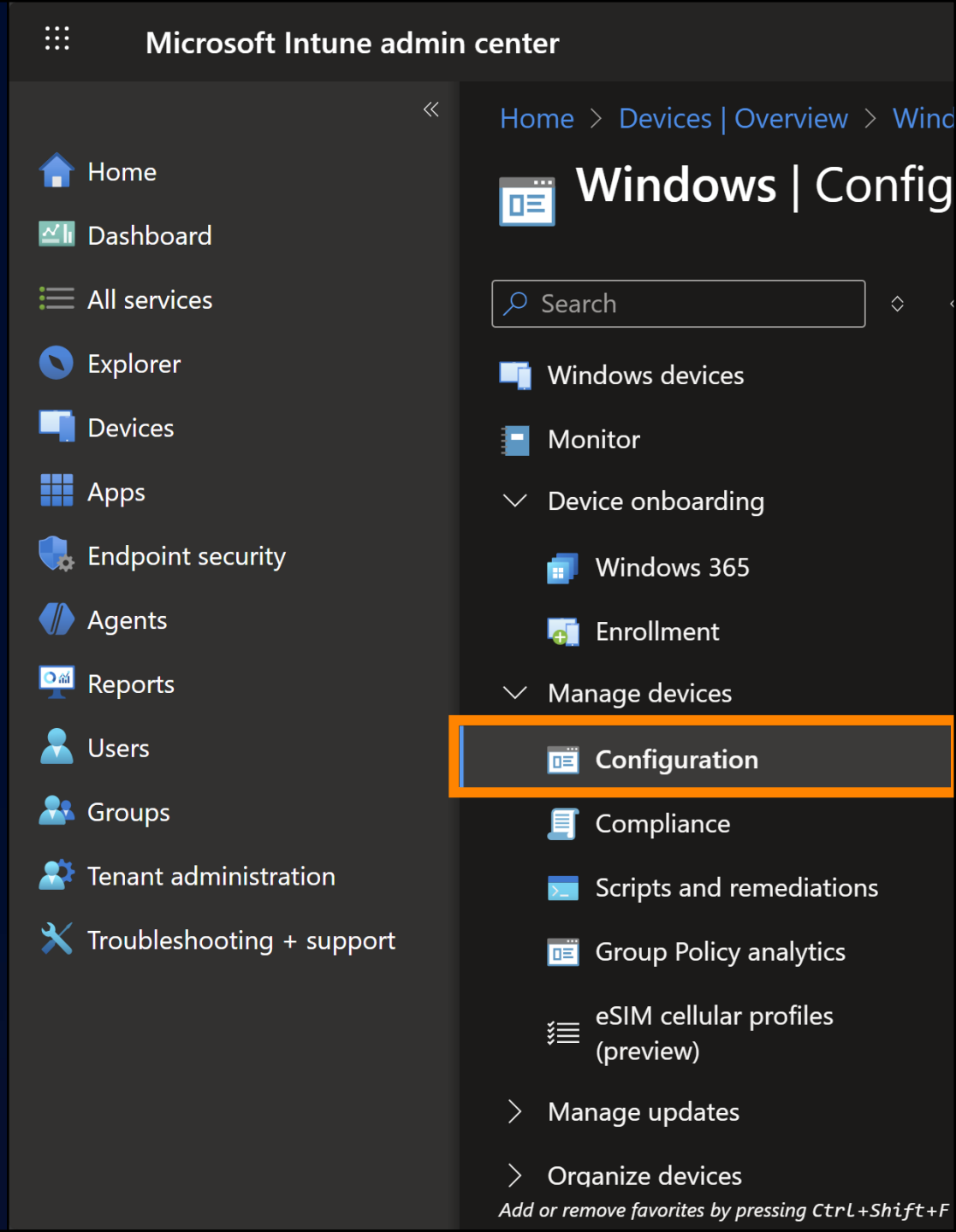
- OneDrive for Business Known Folder M
- Enterprise State Roaming in Entra ID
- Backup Windows settings
- Restore Windows settings

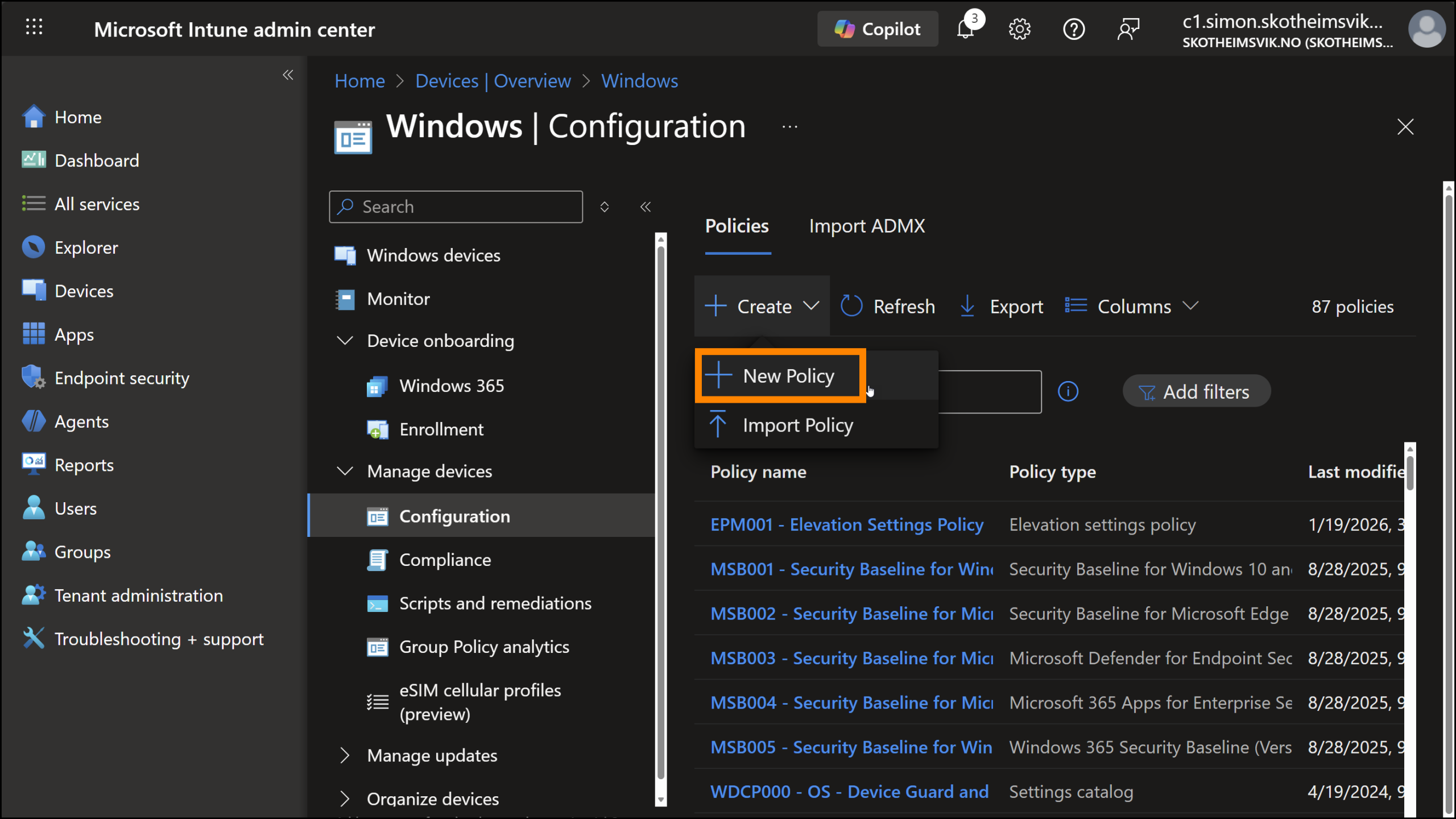
https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-first-sign-in-restore-experience-now-available/4495551

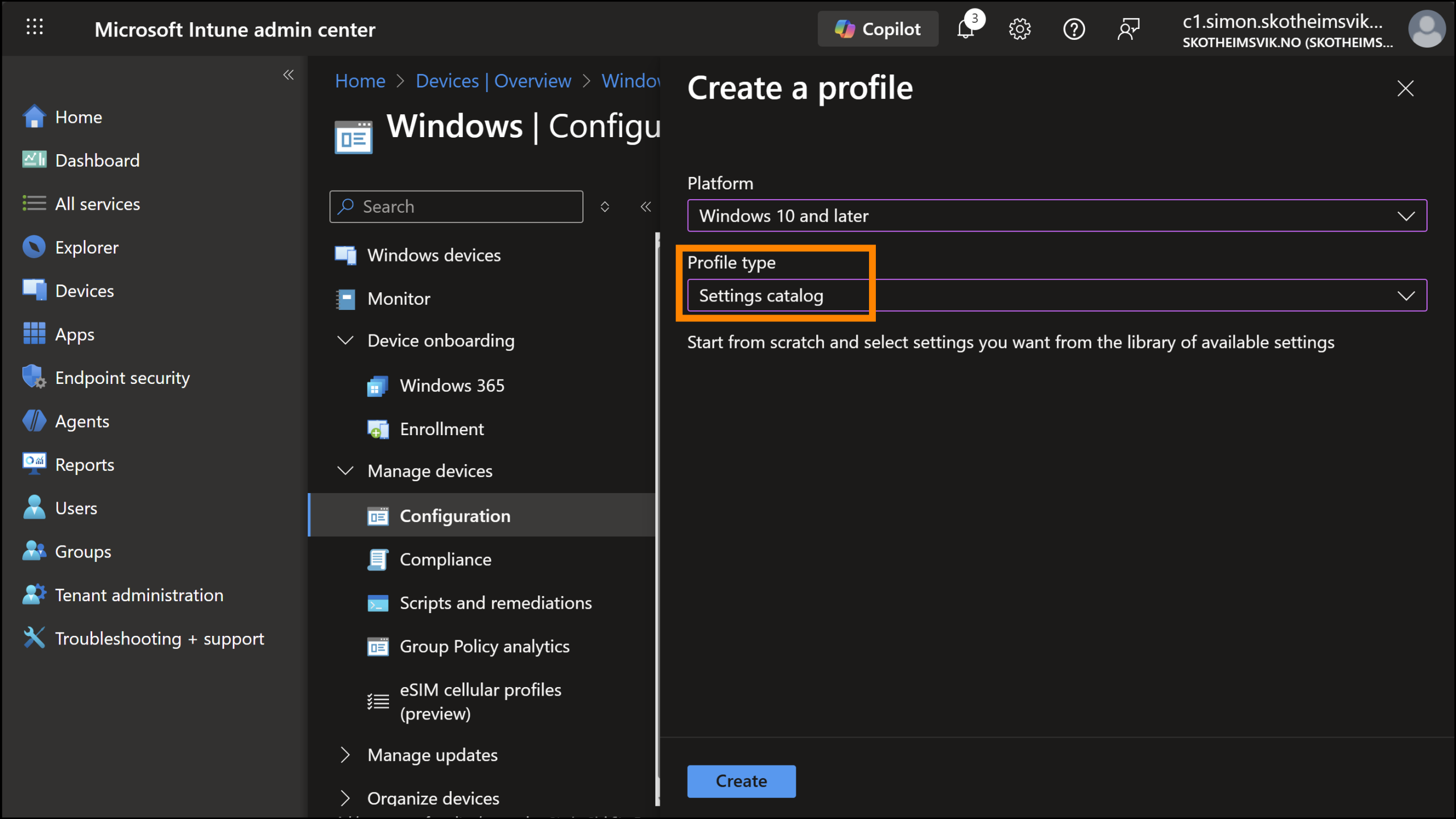
Restore at First Sign-in

- OneDrive for Business Known Folder Move
- Enterprise State Roaming in Entra ID
- Backup Windows settings
- Restore Windows settings

- Reduce migration overhead
- Minimize user disruption
- Strengthen device resilience against incidents
- Simplify transition to new devices
- Reduce troubleshooting




Microsoft Intune admin center
Copilot
3
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Overview > Windows
Windows | Configuration
Search
Windows devices
Monitor
Device onboarding
Windows 365
Enrollment
Manage devices
Configuration
Compliance
Scripts and remediations
Group Policy analytics
eSIM cellular profiles (preview)
Manage updates
Organize devices
Policies
Import ADMX
Create
Refresh
Export
Columns
87 policies
New Policy
Import Policy
Add filters
Policy name
Policy type
Last modifie
EPM001 - Elevation Settings Policy
Elevation settings policy
1/19/2026, 3
MSB001 - Security Baseline for Win
Security Baseline for Windows 10 an
8/28/2025, 9
MSB002 - Security Baseline for Mici
Security Baseline for Microsoft Edge
8/28/2025, 9
MSB003 - Security Baseline for Mici
Microsoft Defender for Endpoint Sec
8/28/2025, 9
MSB004 - Security Baseline for Mici
Microsoft 365 Apps for Enterprise Se
8/28/2025, 9
MSB005 - Security Baseline for Win
Windows 365 Security Baseline (Vers
8/28/2025, 9
WDCP000 - OS - Device Guard and
Settings catalog
4/19/2024, 9


Microsoft Intune admin center
Copilot
3
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Overview > Windo
Windows | Configu
Search
Windows devices
Monitor
Device onboarding
Windows 365
Enrollment
Manage devices
Configuration
Compliance
Scripts and remediations
Group Policy analytics
eSIM cellular profiles (preview)
Manage updates
Organize devices
Create a profile
Platform
Windows 10 and later
Profile type
Settings catalog
Start from scratch and select settings you want from the library of available settings
Create

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

WDCP027 - OS - Windows Backup

Device configuration profile

Summarize with Copilot Delete

No results.

Scope tags Edit

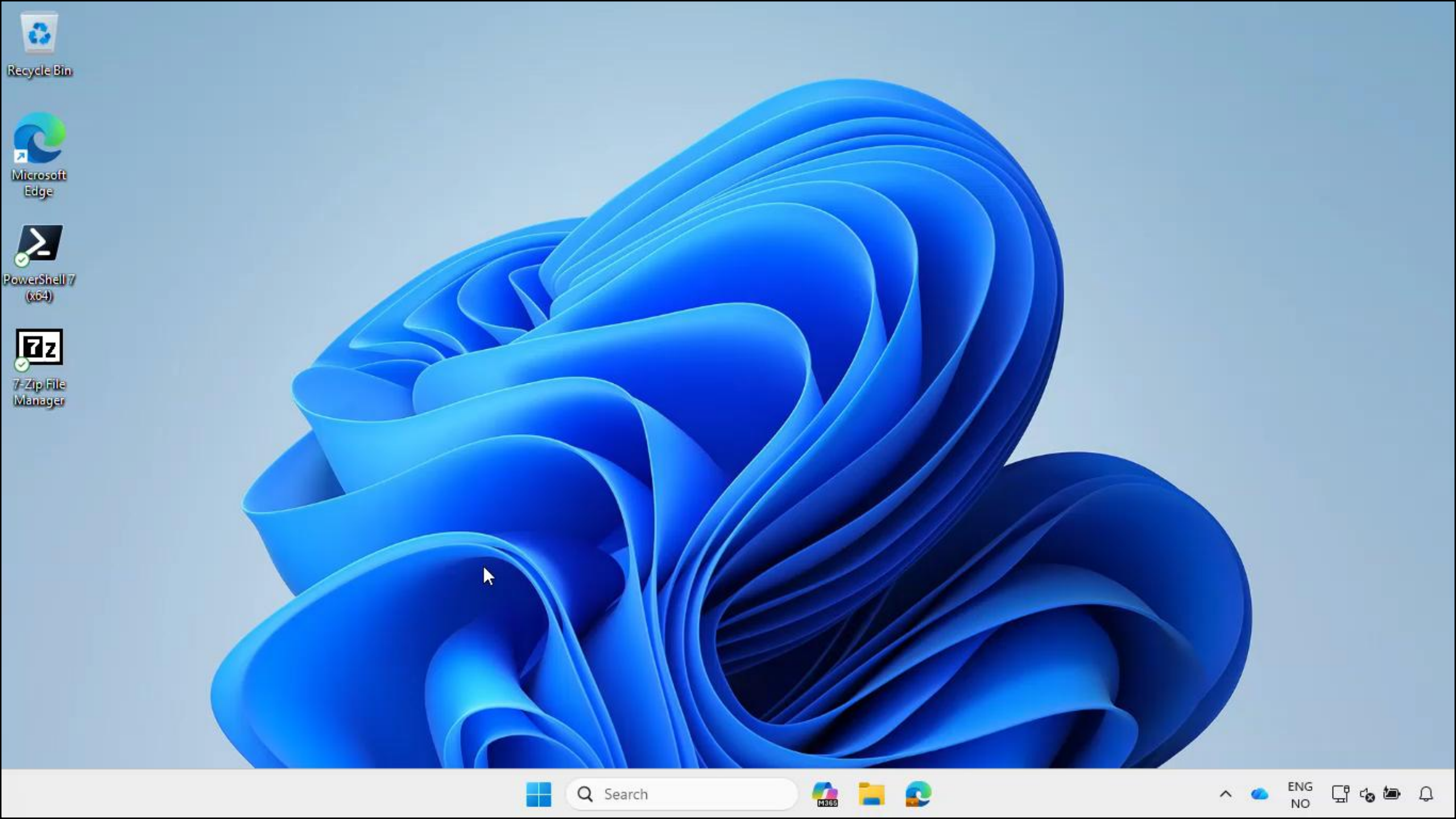
Selected tags Default

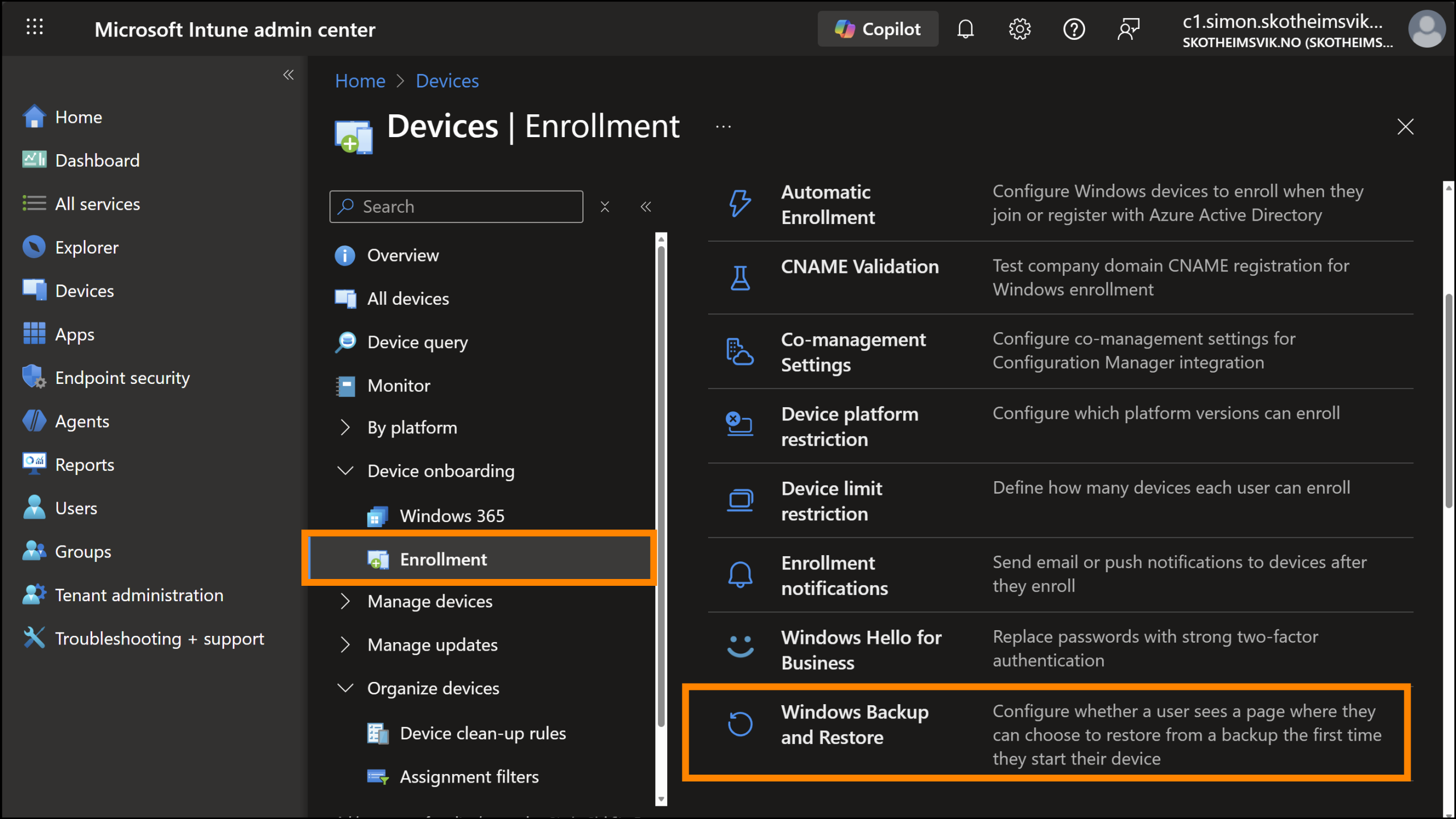
Configuration settings Edit

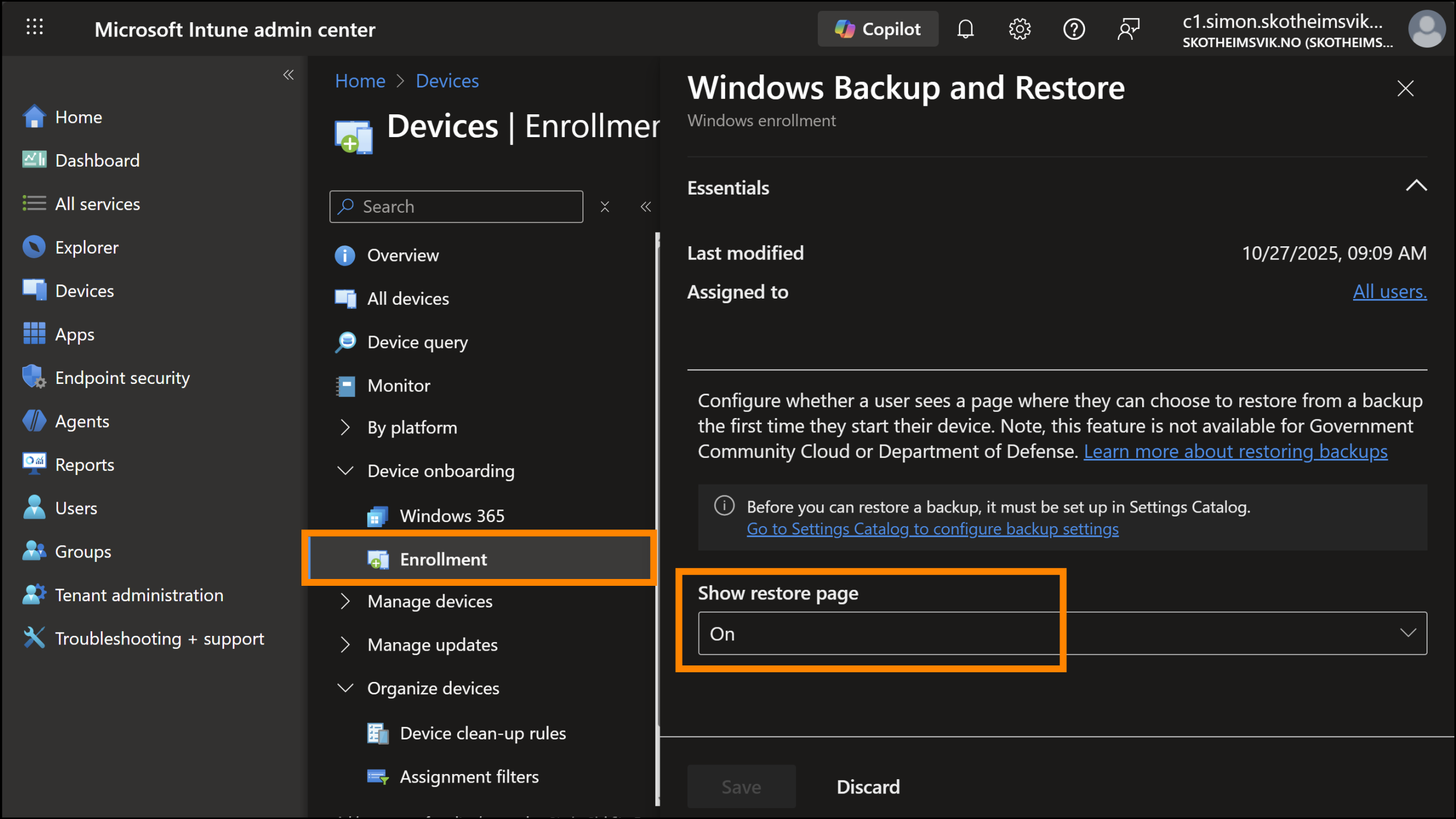
Administrative Templates

Windows Components > Sync your settings

Enable Windows Backup Enabled


Recycle Bin
Microsoft Edge
PowerShell 7 (x64)
7-Zip File Manager
Search
ENG
NO


Microsoft Intune admin center
Copilot
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices
Devices | Enrollment
Search
Overview
All devices
Device query
Monitor
By platform
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates
Organize devices
Device clean-up rules
Assignment filters
Automatic Enrollment
Configure Windows devices to enroll when they join or register with Azure Active Directory
CNAME Validation
Test company domain CNAME registration for Windows enrollment
Co-management Settings
Configure co-management settings for Configuration Manager integration
Device platform restriction
Configure which platform versions can enroll
Device limit restriction
Define how many devices each user can enroll
Enrollment notifications
Send email or push notifications to devices after they enroll
Windows Hello for Business
Replace passwords with strong two-factor authentication
Windows Backup and Restore
Configure whether a user sees a page where they can choose to restore from a backup the first time they start their device


Microsoft Intune admin center
Copilot
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices
Devices | Enrollmer
Search
Overview
All devices
Device query
Monitor
By platform
Device onboarding
Windows 365
Enrollment
Manage devices
Manage updates
Organize devices
Device clean-up rules
Assignment filters
Windows Backup and Restore
Windows enrollment
Essentials
Last modified
10/27/2025, 09:09 AM
Assigned to
All users.
Configure whether a user sees a page where they can choose to restore from a backup the first time they start their device. Note, this feature is not available for Government Community Cloud or Department of Defense. Learn more about restoring backups
Before you can restore a backup, it must be set up in Settings Catalog.
Go to Settings Catalog to configure backup settings
Show restore page
On
Save
Discard

Let's set things up for your work or school

You'll use this info to sign in to your devices.

simon.skotheimsvik@

You can't get there from here

This application contains sensitive information and can only be accessed from:

Devices or client applications that meet management compliance policy.

If this is a personal device you can choose to let manage your device by going to Settings > Accounts > Access work or school and clicking in "Connect". When you're done come back and try again.

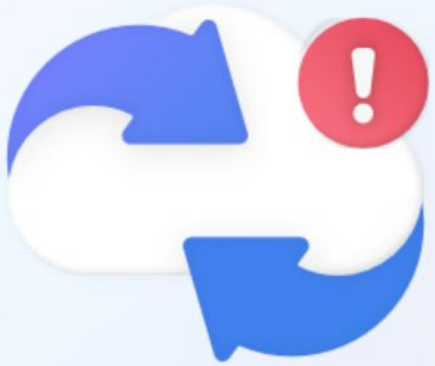
OK

Something went wrong

We encountered an error while checking for backups. Privacy Statement

Set up as a new PC

Try again



You can't restore this PC later

If you restore your PC, we'll bring this device up-to-date with your latest backup. If you don't, you can't restore your previous settings or Microsoft Store apps later.

Try again

Set up as a new PC

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID (Preview)
Enterprise apps
App registrations
Roles & admins

Simon Skotheimsvik | Sign-in logs

User

Download | Export Data Settings | Troubleshoot | Refresh | Columns

This view will soon be replaced with a view that includes more filters infinite scrolling, and column reordering. Try out our new signIns preview.

Date : **Last 24 hours** | Show dates as : **Local**

User contains | Add filters

User sign-ins (interactive) | User sign-ins (non-interactive)

Date	Request ID	User	Application	Status
2/23/2026, 12:15:16 ...	4df8d067-9872-440...	Simon Skotheimsvik ...	Windows Backup an...	Failure
2/23/2026, 12:15:14 ...	9ed142c6-b552-406...	Simon Skotheimsvik ...	Windows Backup an...	Failure
2/23/2026, 12:14:48 ...	2535b71c-843d-4aef...	Simon Skotheimsvik ...	Microsoft Authentica...	Success
2/23/2026, 12:14:46 ...	4076f35d-06d3-466...	Simon Skotheimsvik ...	Microsoft Authentica...	Success
2/23/2026, 8:58:18 AM	3a7f9c94-f1dd-4008...	Simon Skotheimsvik ...	Windows Sign In	Success

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID (Preview)
Enterprise apps
App registrations
Roles & admins

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

Date	2/23/2026, 12:15:14 PM
Request ID	[redacted]
Correlation ID	[redacted]
Authentication requirement	Single-factor authentication
Agent Type	Not Agentic
Status	Failure
Continuous access evaluation	No
Sign-in error code	53000
Failure reason	Device is not in required device state: {state}. Conditional Access policy requires a compliant device, and the device is not compliant. The user must enroll their device with an approved MDM provider like Intune.
Additional Details	Your administrator might have configured a conditional access policy that allows access to your organization's resources only from compliant devices. To be compliant, your device must be either joined to your on-premises Active Directory or joined to your Azure Active Directory. More details available at https://support.microsoft.com/account-billing/troubleshooting-compliance-error-messages-for-a-work-or-school-account-479a9c42-d9d1-4e44-9e90-24bbad96c251

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID (Preview)
Enterprise apps
App registrations
Roles & admins

Directory. More details available at https://support.microsoft.com/account-billing/troubleshooting-compliance-error-messages-for-a-work-or-school-account-479a9c42-d9d1-4e44-9e90-24bbad96c251

1. Review the diagnosis and act on suggested fixes.

User	Simon Skotheimsvik
Username	simon.skotheimsvik@
User ID	
Sign-in identifier	
Session ID	
App owner tenant ID	
Resource owner tenant ID	
User type	Member
Cross tenant access type	None
Application	Windows Backup and Restore
Application ID	74d197dc-b84d-4d43-a1b2-b5bf3bb91c11
Resource	Microsoft Activity Feed Service
Resource ID	d32c68ad-72d2-4acb-a0c7-46bb2cf93873
Resource tenant ID	256fe0b9-baf7-42a5-95b6-c7902f95bcb5

Home
Entra agents
Favorites
Entra ID
Overview
Users
Groups
Devices
Agent ID (Preview)
Enterprise apps
App registrations
Roles & admins

Directory. More details available at https://support.microsoft.com/acc...
billing/troubleshooting-compliance-error-messages-for-a-...
479a9c42-d9d1-4e44-9e90-24bbad96c251

1. Review the diag...

User	Simon Skotheimsvik...
Username	simon.skotheimsvik@...
User ID	[redacted]
Sign-in identifier	
Session ID	[redacted]
App owner tenant ID	[redacted]
Resource owner tenant ID	[redacted]
User type	Member
Cross tenant access type	None
Application	Windows Backup and Restore
Application ID	74d197dc-b84d-4d43-a1b2-b5bf3bb91c11
Resource	Microsoft Activity Feed Service
Resource ID	d32c68ad-72d2-4acb-a0c7-46bb2cf93873
Resource tenant ID	256fe0b9-baf7-42a5-95b6-c7902f95bcb5

Policy conflicts from multiple policy sources

Windows Backup for Organizations can be configured by GPO or CSP, but not a combination of both. Avoid mixing GPO and CSP policy settings for Windows Backup for Organizations, as it can lead to unexpected results.

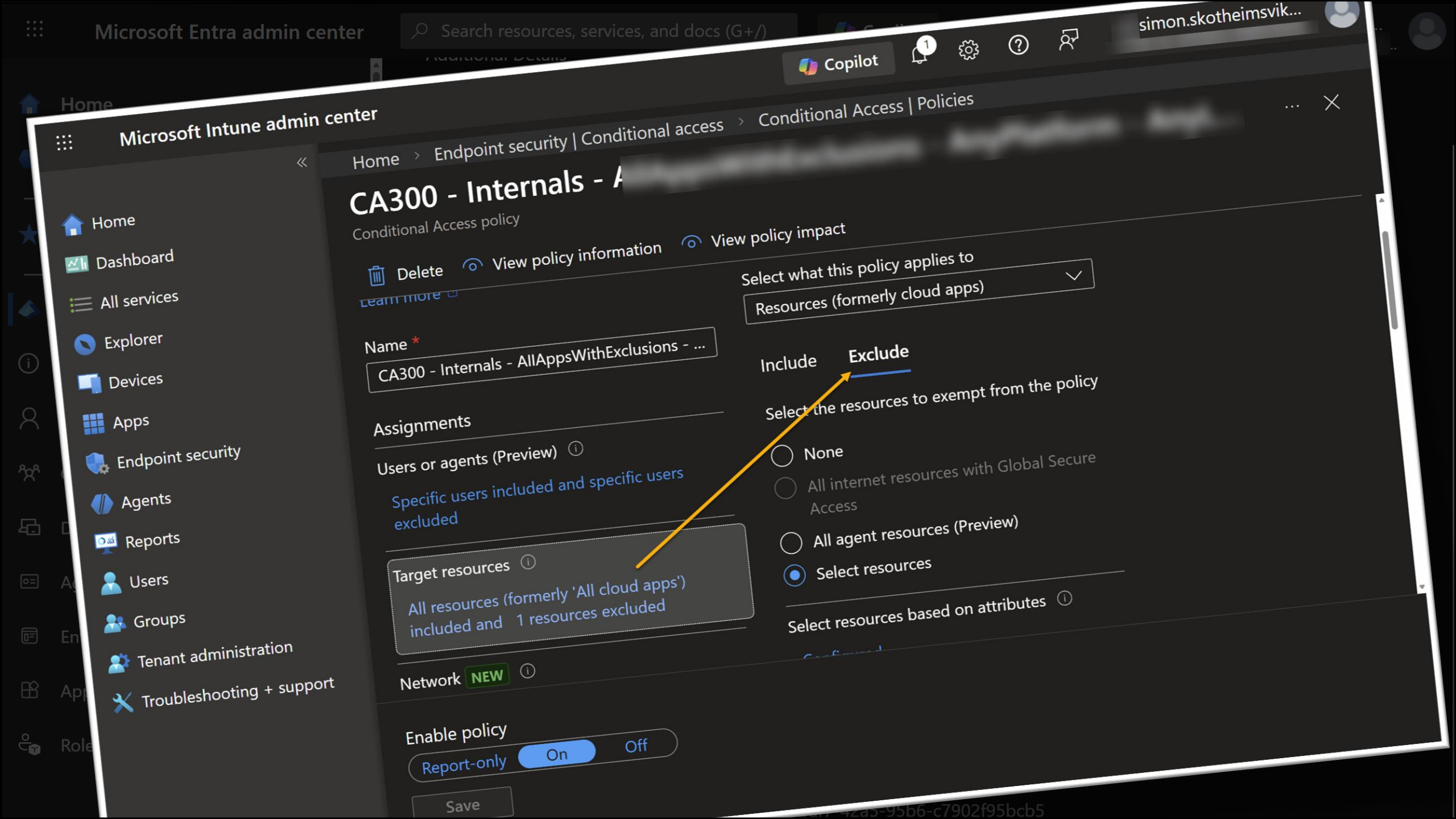
Conditional Access policy interference

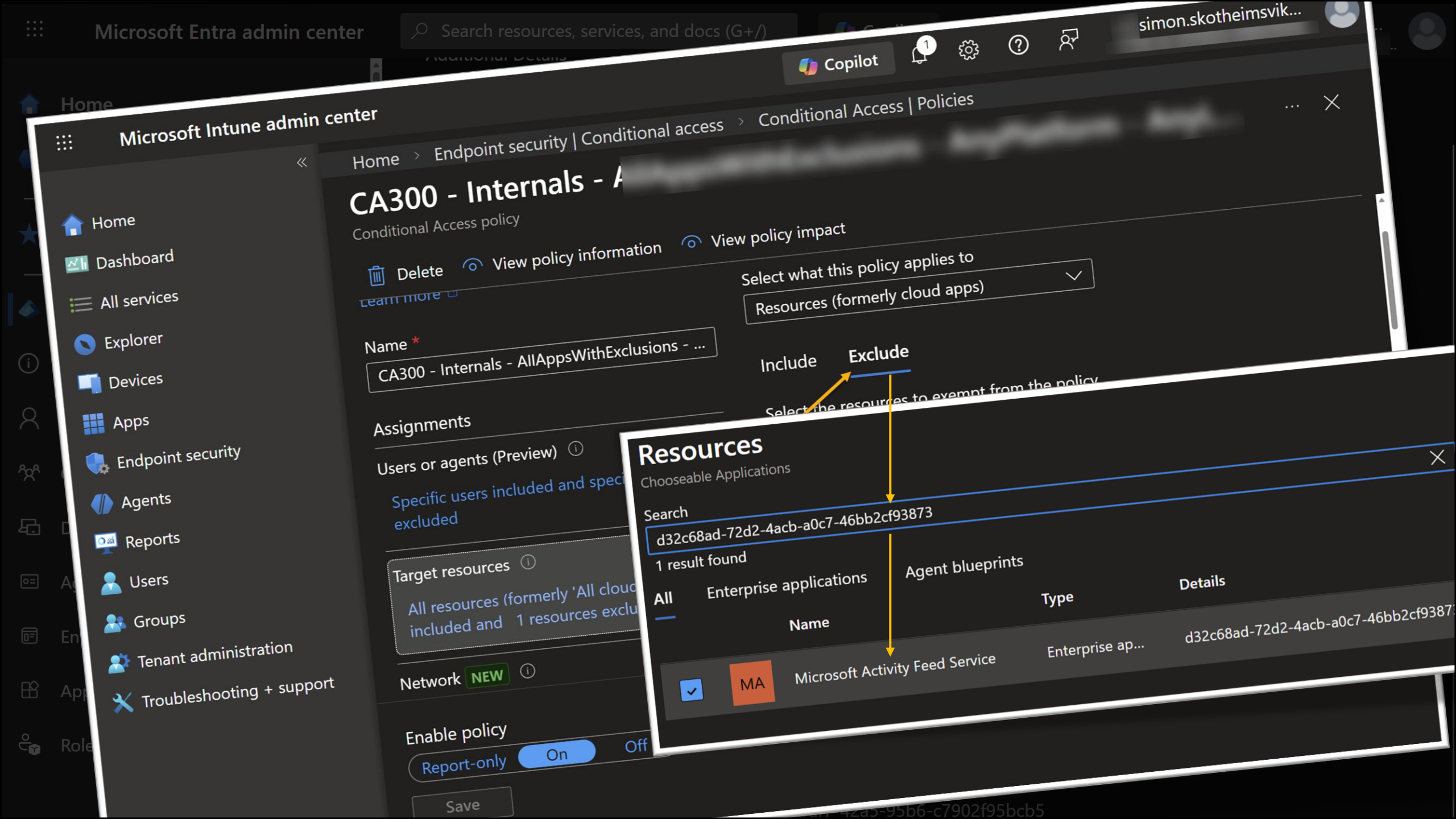
If conditional access is enabled for cloud applications, it might prevent the Microsoft Entra user from obtaining an access token, resulting in the following error.

Expand table

Error title	Error description
You don't have access to this	Your sign-in was successful but you don't have the permissions to access this resource.
You can't get there from here	This application contains sensitive information and can only be accessed from: Devices or client applications that meet Contoso engagement compliance policy. If this is a personal device, you can choose to let Contoso manage your device by going to **Settings** > **Accounts** > **Access work or school** and clicking on **Connect**. When you're done come back and try again.

To fix this error, you'll need to create a custom policy that allows the Microsoft service (app id: d32c68ad-72d2-4acb-a0c7-46bb2cf93873) to enable the restore flow to proceed. Verify that the app id is listed in the custom policy before you proceed further.

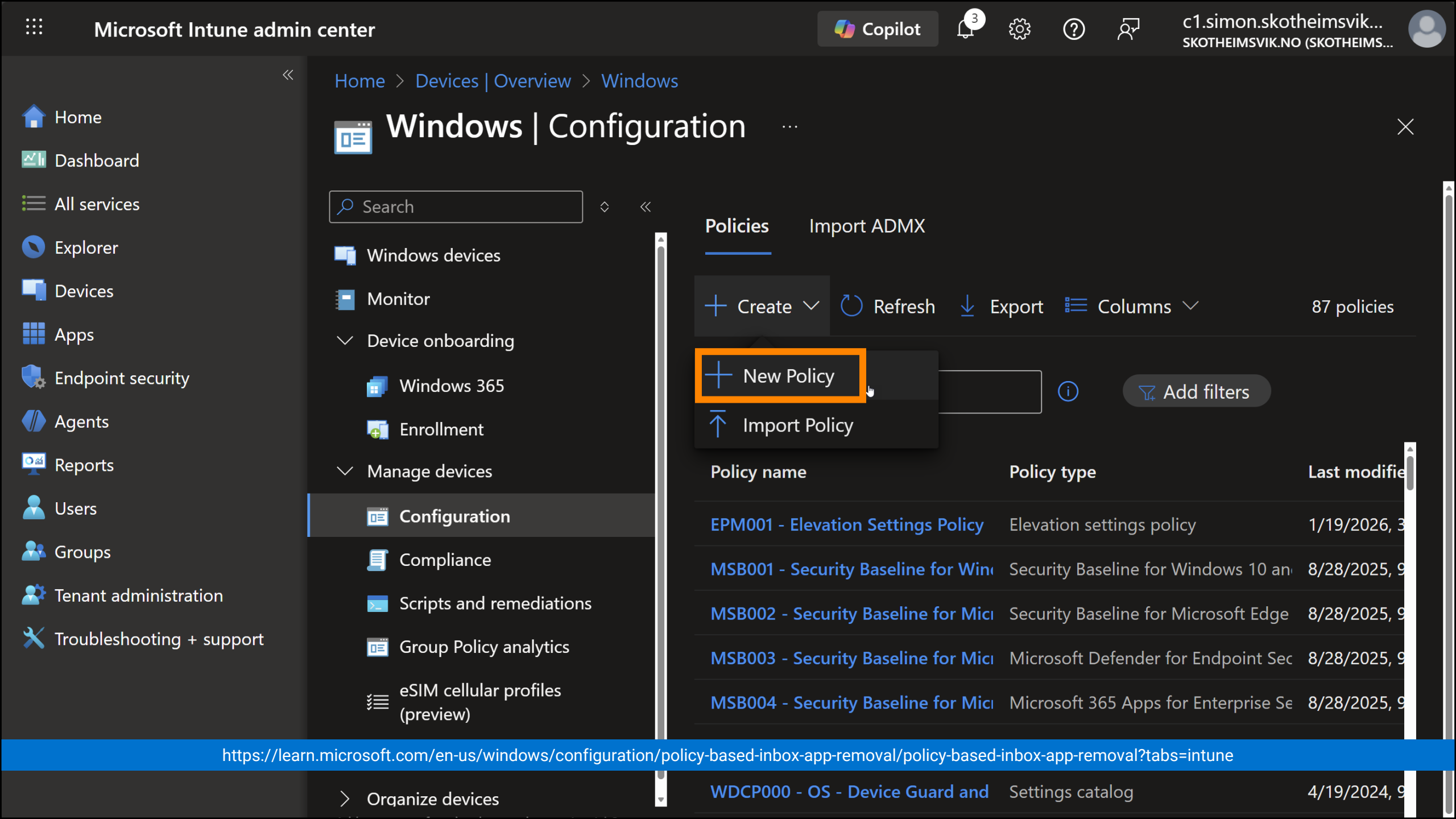

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Microsoft Intune admin center
Copilot
simon.skotheimsvik...
Home
Endpoint security | Conditional access
Conditional Access | Policies
CA300 - Internals - A
Conditional Access policy
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Delete
View policy information
View policy impact
Learn more
Name *
CA300 - Internals - AllAppsWithExclusions - ...
Assignments
Users or agents (Preview)
Specific users included and specific users excluded
Target resources
All resources (formerly 'All cloud apps') included and 1 resources excluded
Network NEW
Enable policy
Report-only
On
Off
Save
Select what this policy applies to
Resources (formerly cloud apps)
Include
Exclude
Select the resources to exempt from the policy
None
All internet resources with Global Secure Access
All agent resources (Preview)
Select resources
Select resources based on attributes


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Microsoft Intune admin center
Copilot
simon.skotheimsvik...
Home
Endpoint security | Conditional access
Conditional Access | Policies
CA300 - Internals - A
Conditional Access policy
Delete
View policy information
View policy impact
Learn more
Name *
CA300 - Internals - AllAppsWithExclusions - ...
Select what this policy applies to
Resources (formerly cloud apps)
Include
Exclude
Assignments
Users or agents (Preview)
Specific users included and specified excluded
Target resources
All resources (formerly 'All cloud apps') included and 1 resources excluded
Network NEW
Enable policy
Report-only
On
Off
Save
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Resources
Chooseable Applications
Search
d32c68ad-72d2-4acb-a0c7-46bb2cf93873
1 result found
All
Enterprise applications
Agent blueprints
Name
Type
Details
MA
Microsoft Activity Feed Service
Enterprise ap...
d32c68ad-72d2-4acb-a0c7-46bb2cf93873

10 Remove Built-in Apps

Aka bloatware

https://support.microsoft.com/en-us/topic/policy-based-removal-of-pre-installed-microsoft-store-apps-e1d41a92-b658-4511-95a6-0fbcc02b4e9c


Microsoft Intune admin center
Copilot
3
c1.simon.skotheimsvik...
SKOTHEIMSVIK.NO (SKOTHEIMS...
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Overview > Windows
Windows | Configuration
Search
Windows devices
Monitor
Device onboarding
Windows 365
Enrollment
Manage devices
Configuration
Compliance
Scripts and remediations
Group Policy analytics
eSIM cellular profiles (preview)
Organize devices
Policies
Import ADMX
Create
Refresh
Export
Columns
87 policies
New Policy
Import Policy
Add filters
Policy name
Policy type
Last modifie
EPM001 - Elevation Settings Policy
Elevation settings policy
1/19/2026, 3
MSB001 - Security Baseline for Win
Security Baseline for Windows 10 an
8/28/2025, 9
MSB002 - Security Baseline for Mici
Security Baseline for Microsoft Edge
8/28/2025, 9
MSB003 - Security Baseline for Mici
Microsoft Defender for Endpoint Sec
8/28/2025, 9
MSB004 - Security Baseline for Mici
Microsoft 365 Apps for Enterprise Se
8/28/2025, 9
https://learn.microsoft.com/en-us/windows/configuration/policy-based-inbox-app-removal/policy-based-inbox-app-removal?tabs=intune
WDCP000 - OS - Device Guard and
Settings catalog
4/19/2024, 9

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

Edit profile - WDCP026 - OS - Remove Bloatware

Settings catalog

1 Configuration settings 2 Review + save

+ Add settings

Administrative Templates

Remove category

Windows Components > App Package Deployment

Remove subcategory

1 of 27 settings in this subcategory are not configured

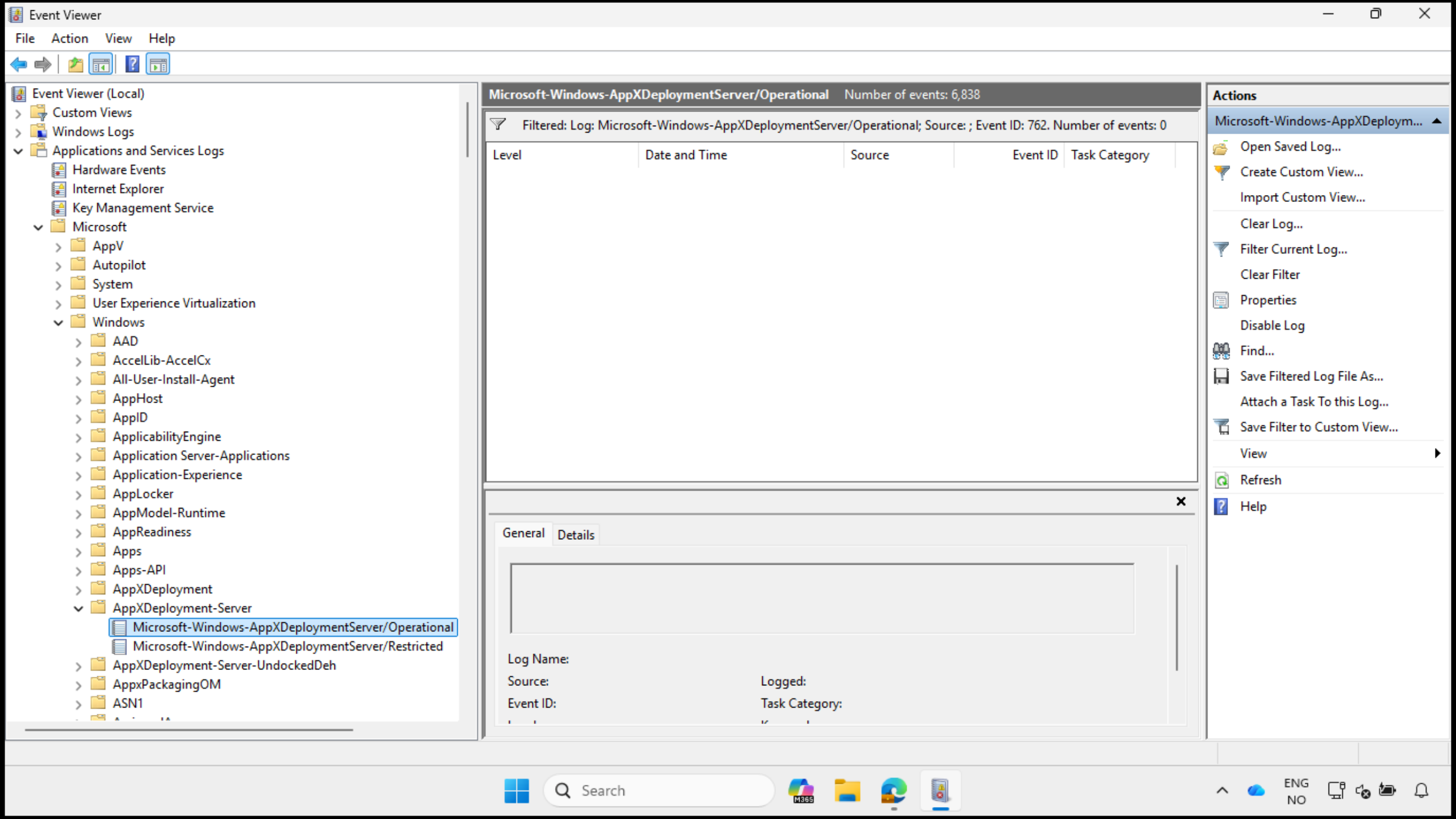
Feedback Hub (Device)	True
Microsoft 365 Copilot (Device)	False
Microsoft Clipchamp (Device)	False
Microsoft Copilot (Device)	False

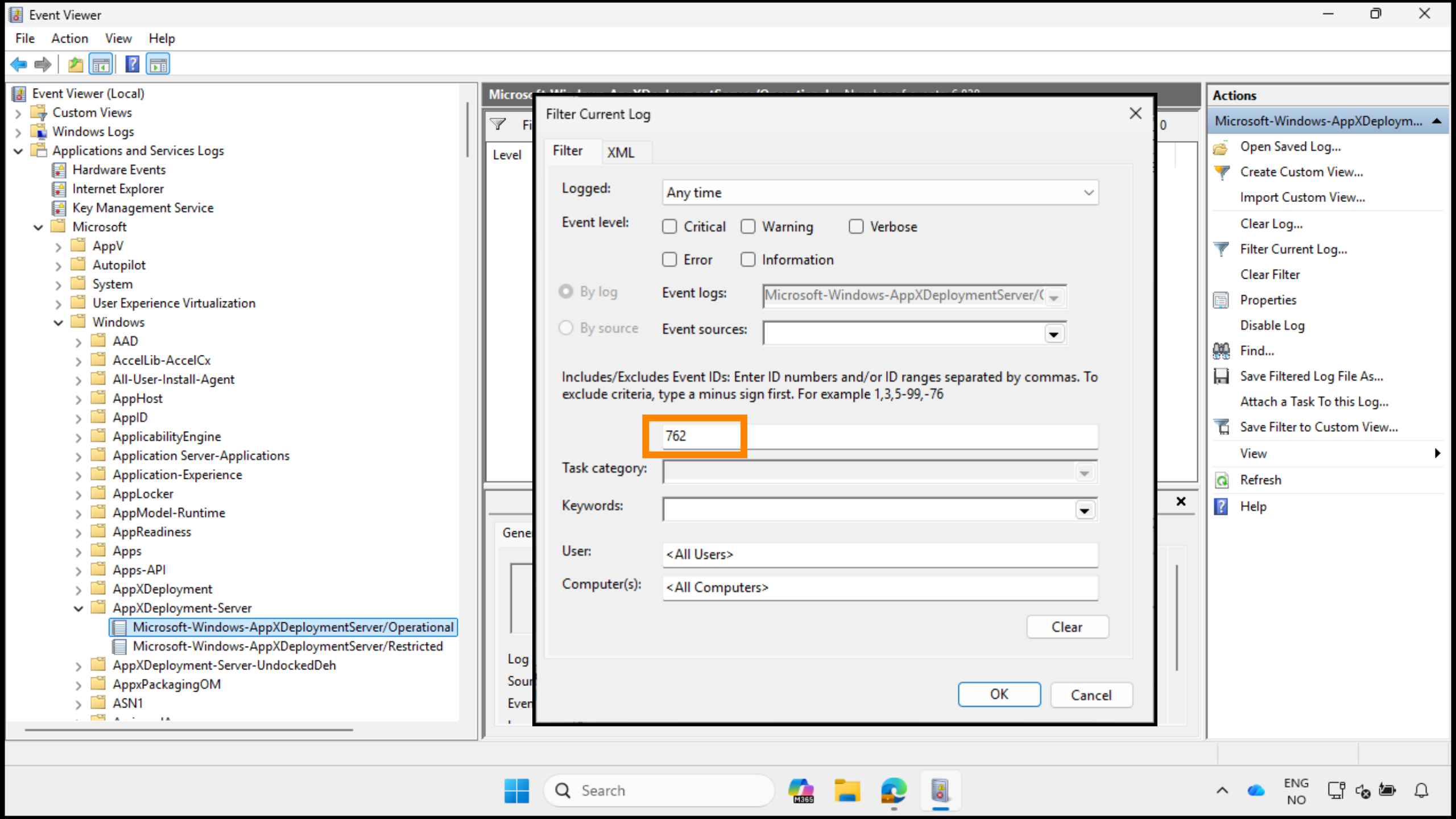
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

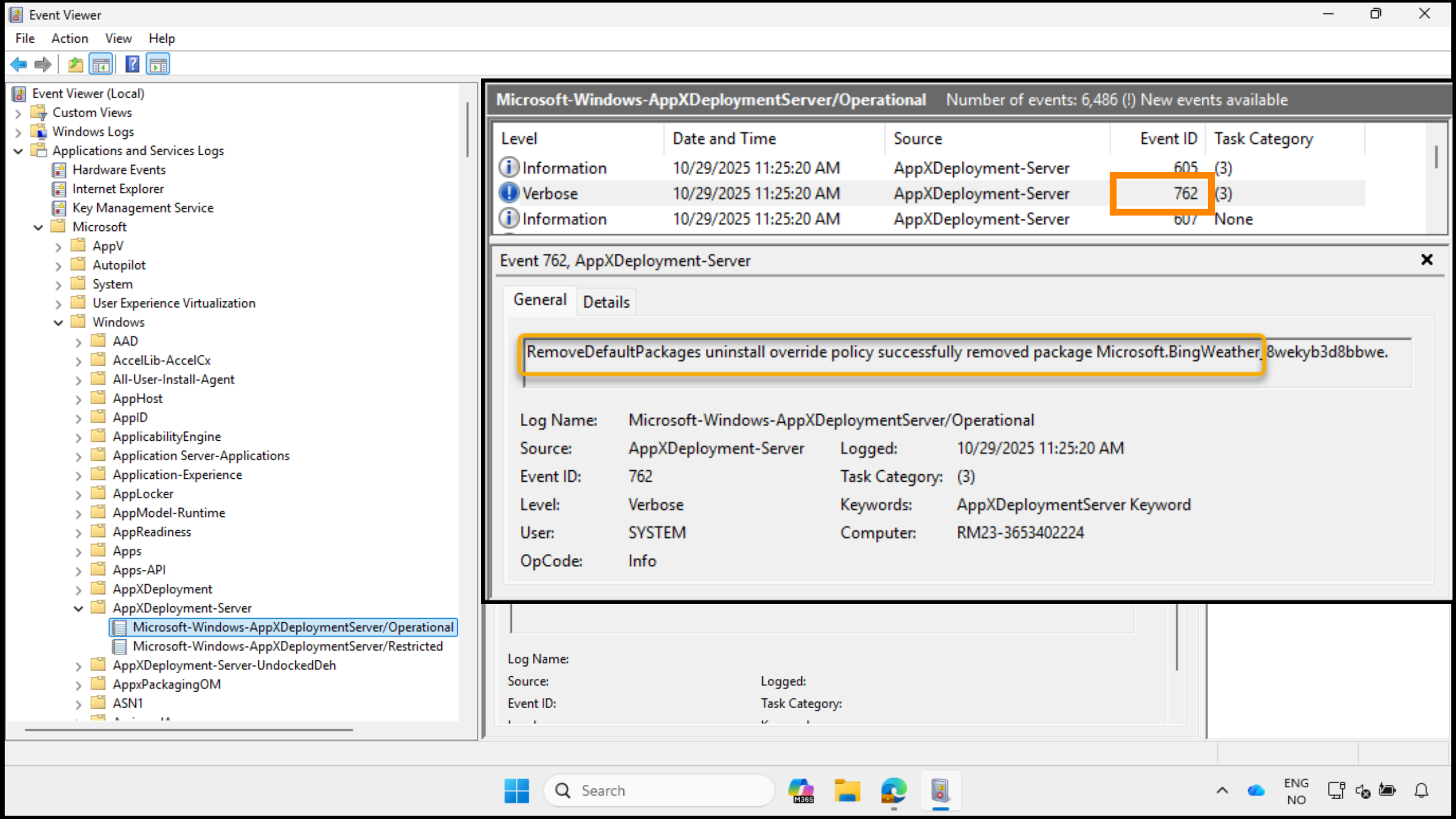
Microsoft News (Device)	True
Microsoft Photos ** (Device)	True
Microsoft Solitaire Collection (Device)	True
Microsoft Sticky Notes (Device)	False
Microsoft Teams (Device)	False
Microsoft To Do (Device)	False
MSN Weather (Device)	True
Outlook for Windows (Device)	False
Paint (Device)	False
Quick Assist (Device)	True
Snipping Tool (Device)	False
Windows Calculator (Device)	False

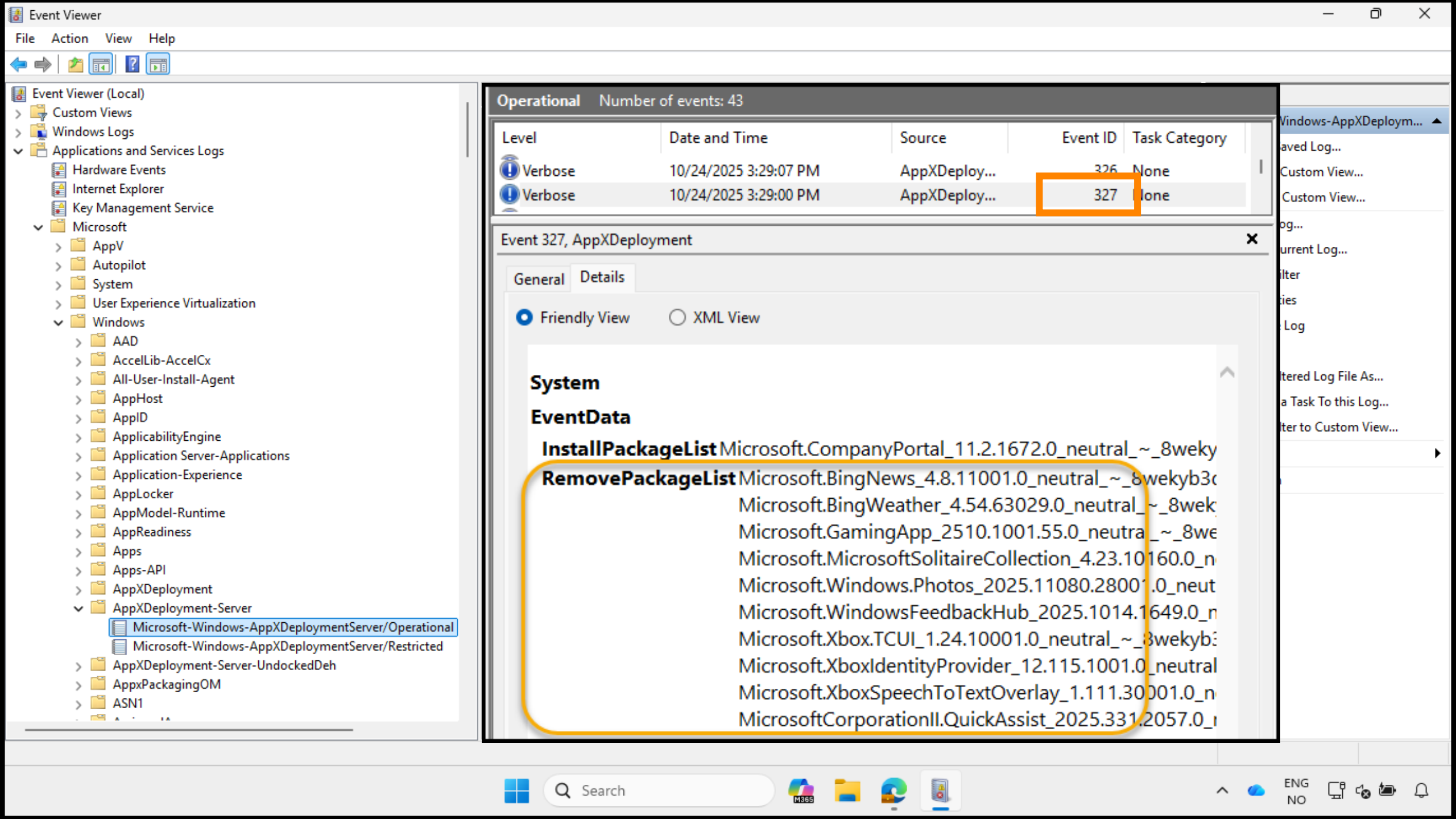
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Windows Camera ** (Device)	False
Windows Media Player ** (Device)	False
Windows Notepad ** (Device)	False
Windows Sound Recorder (Device)	False
Windows Terminal (Device)	False
Xbox Gaming App (Device)	True
Xbox Identity Provider * (Device)	True
Xbox Speech To Text Overlay * (Device)	True
Xbox TCUI * (Device)	True
Remove Default Microsoft Store packages from the system.	Enabled


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Hardware Events
Internet Explorer
Key Management Service
Microsoft
AppV
Autopilot
System
User Experience Virtualization
Windows
AAD
AccelLib-AccelCx
All-User-Install-Agent
AppHost
AppID
ApplicabilityEngine
Application Server-Applications
Application-Experience
AppLocker
AppModel-Runtime
AppReadiness
Apps
Apps-API
AppXDeployment
AppXDeployment-Server
Microsoft-Windows-AppXDeploymentServer/Operational
Microsoft-Windows-AppXDeploymentServer/Restricted
AppXDeployment-Server-UndockedDeh
AppxPackagingOM
ASN1
Microsoft-Windows-AppXDeploymentServer/Operational Number of events: 6,838
Filtered: Log: Microsoft-Windows-AppXDeploymentServer/Operational; Source: ; Event ID: 762. Number of events: 0
Level
Date and Time
Source
Event ID
Task Category
General
Details
Log Name:
Source:
Logged:
Event ID:
Task Category:
Actions
Microsoft-Windows-AppXDeploym...
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Disable Log
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help
Search
ENG
NO

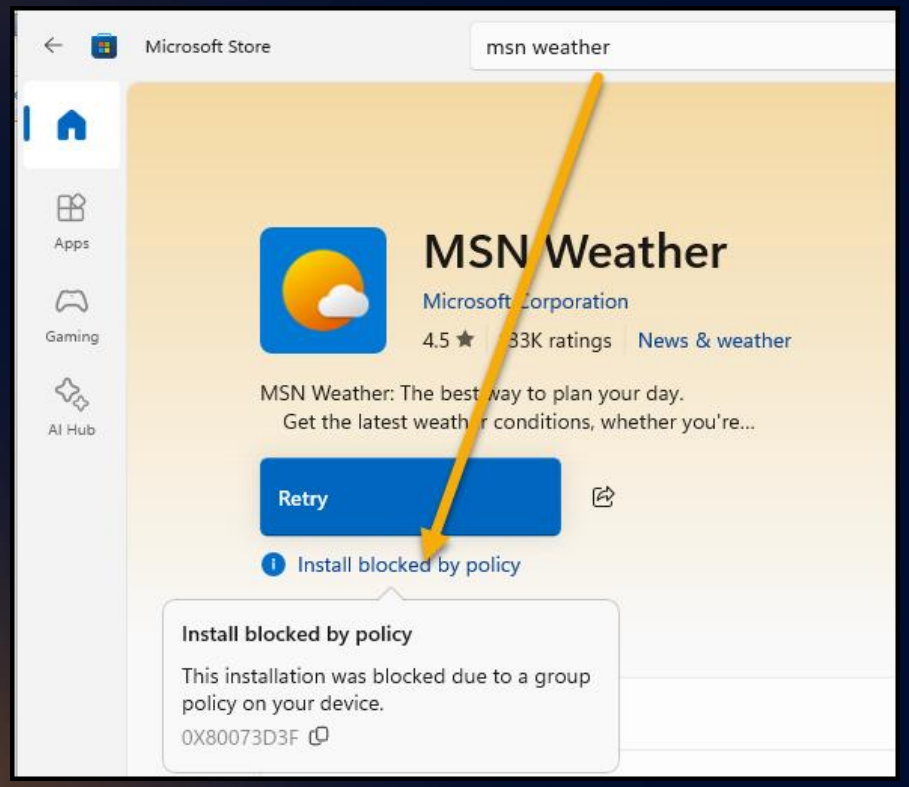

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Hardware Events
Internet Explorer
Key Management Service
Microsoft
AppV
Autopilot
System
User Experience Virtualization
Windows
AAD
AccelLib-AccelCx
All-User-Install-Agent
AppHost
AppID
ApplicabilityEngine
Application Server-Applications
Application-Experience
AppLocker
AppModel-Runtime
AppReadiness
Apps
Apps-API
AppXDeployment
AppXDeployment-Server
Microsoft-Windows-AppXDeploymentServer/Operational
Microsoft-Windows-AppXDeploymentServer/Restricted
AppXDeployment-Server-UndockedDeh
AppxPackagingOM
ASN1
Level
Filter Current Log
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Microsoft-Windows-AppXDeploymentServer/(
By source
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
762
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel
Actions
Microsoft-Windows-AppXDeploym...
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Disable Log
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help
Search
ENG
NO

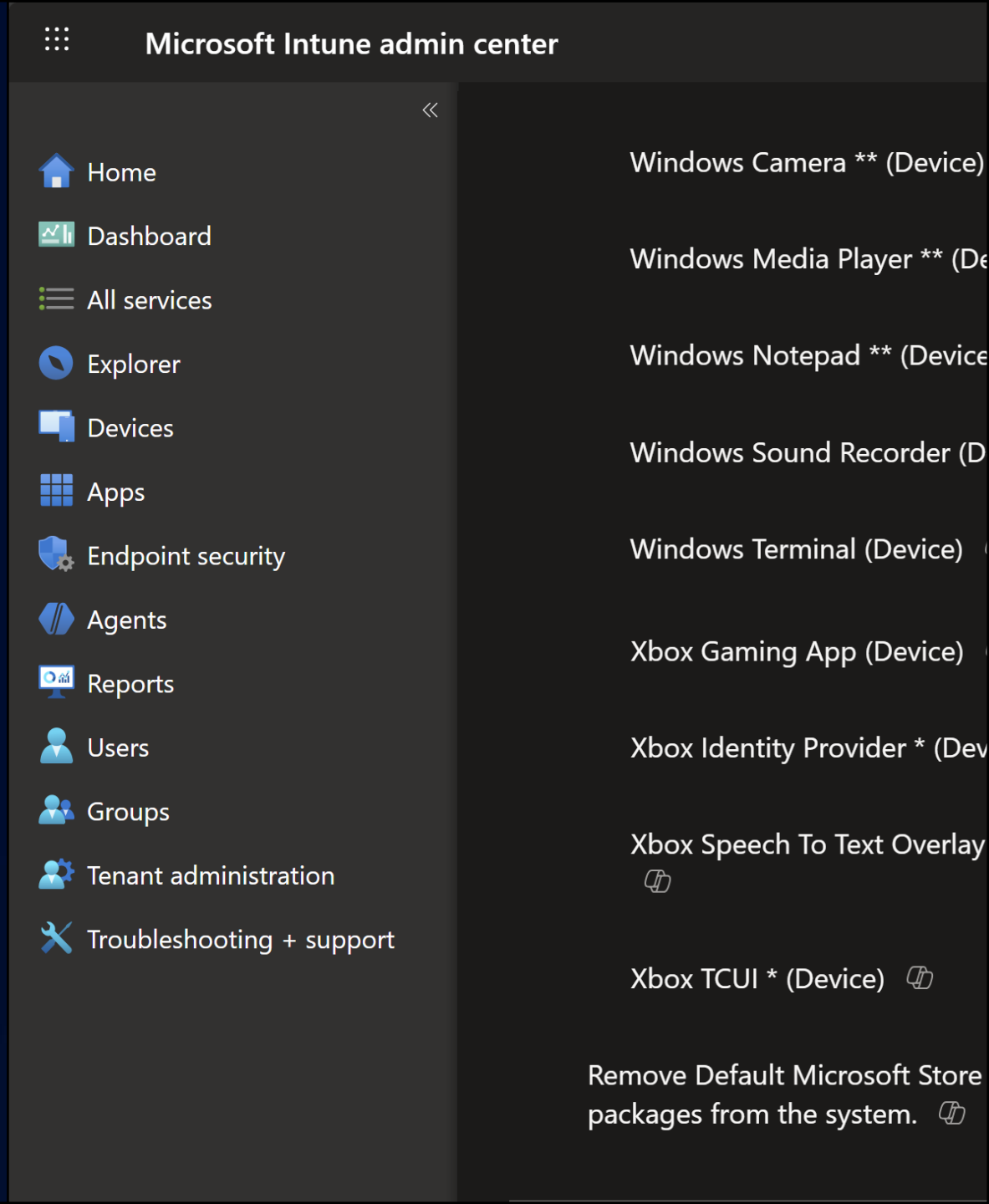

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Hardware Events
Internet Explorer
Key Management Service
Microsoft
AppV
Autopilot
System
User Experience Virtualization
Windows
AAD
AccelLib-AccelCx
All-User-Install-Agent
AppHost
AppID
ApplicabilityEngine
Application Server-Applications
Application-Experience
AppLocker
AppModel-Runtime
AppReadiness
Apps
Apps-API
AppXDeployment
AppXDeployment-Server
Microsoft-Windows-AppXDeploymentServer/Operational
Microsoft-Windows-AppXDeploymentServer/Restricted
AppXDeployment-Server-UndockedDeh
AppxPackagingOM
ASN1
Microsoft-Windows-AppXDeploymentServer/Operational Number of events: 6,486 (!) New events available
Level Date and Time Source Event ID Task Category
Information 10/29/2025 11:25:20 AM AppXDeployment-Server 605 (3)
Verbose 10/29/2025 11:25:20 AM AppXDeployment-Server 762 (3)
Information 10/29/2025 11:25:20 AM AppXDeployment-Server 607 None
Event 762, AppXDeployment-Server
General Details
RemoveDefaultPackages uninstall override policy successfully removed package Microsoft.BingWeather_8wekyb3d8bbwe.
Log Name: Microsoft-Windows-AppXDeploymentServer/Operational
Source: AppXDeployment-Server Logged: 10/29/2025 11:25:20 AM
Event ID: 762 Task Category: (3)
Level: Verbose Keywords: AppXDeploymentServer Keyword
User: SYSTEM Computer: RM23-3653402224
OpCode: Info
Log Name:
Source: Logged:
Event ID: Task Category:
Search
ENG
NO


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Hardware Events
Internet Explorer
Key Management Service
Microsoft
AppV
Autopilot
System
User Experience Virtualization
Windows
AAD
AccelLib-AccelCx
All-User-Install-Agent
AppHost
AppID
ApplicabilityEngine
Application Server-Applications
Application-Experience
AppLocker
AppModel-Runtime
AppReadiness
Apps
Apps-API
AppXDeployment
AppXDeployment-Server
Microsoft-Windows-AppXDeploymentServer/Operational
Microsoft-Windows-AppXDeploymentServer/Restricted
AppXDeployment-Server-UndockedDeh
AppxPackagingOM
ASN1
Operational Number of events: 43
Level Date and Time Source Event ID Task Category
Verbose 10/24/2025 3:29:07 PM AppXDeploy... 326 None
Verbose 10/24/2025 3:29:00 PM AppXDeploy... 327 None
Event 327, AppXDeployment
General Details
Friendly View XML View
System
EventData
InstallPackageList Microsoft.CompanyPortal_11.2.1672.0_neutral_~_8weky
RemovePackageList Microsoft.BingNews_4.8.11001.0_neutral_~_8wekyb3
Microsoft.BingWeather_4.54.63029.0_neutral_~_8wek
Microsoft.GamingApp_2510.1001.55.0_neutra_~_8we
Microsoft.MicrosoftSolitaireCollection_4.23.10160.0_n
Microsoft.Windows.Photos_2025.11080.2800.0_neut
Microsoft.WindowsFeedbackHub_2025.1014.1649.0_n
Microsoft.Xbox.TCUI_1.24.10001.0_neutral_~_8wekyb3
Microsoft.XboxIdentityProvider_12.115.1001.0_neutral
Microsoft.XboxSpeechToTextOverlay_1.111.30001.0_n
MicrosoftCorporationII.QuickAssist_2025.331.2057.0_
Windows-AppXDeploym...
aved Log...
Custom View...
Custom View...
og...
urrent Log...
lter
ies
Log
tered Log File As...
a Task To this Log...
ter to Custom View...
Search
ENG
NO

Microsoft Store Apps

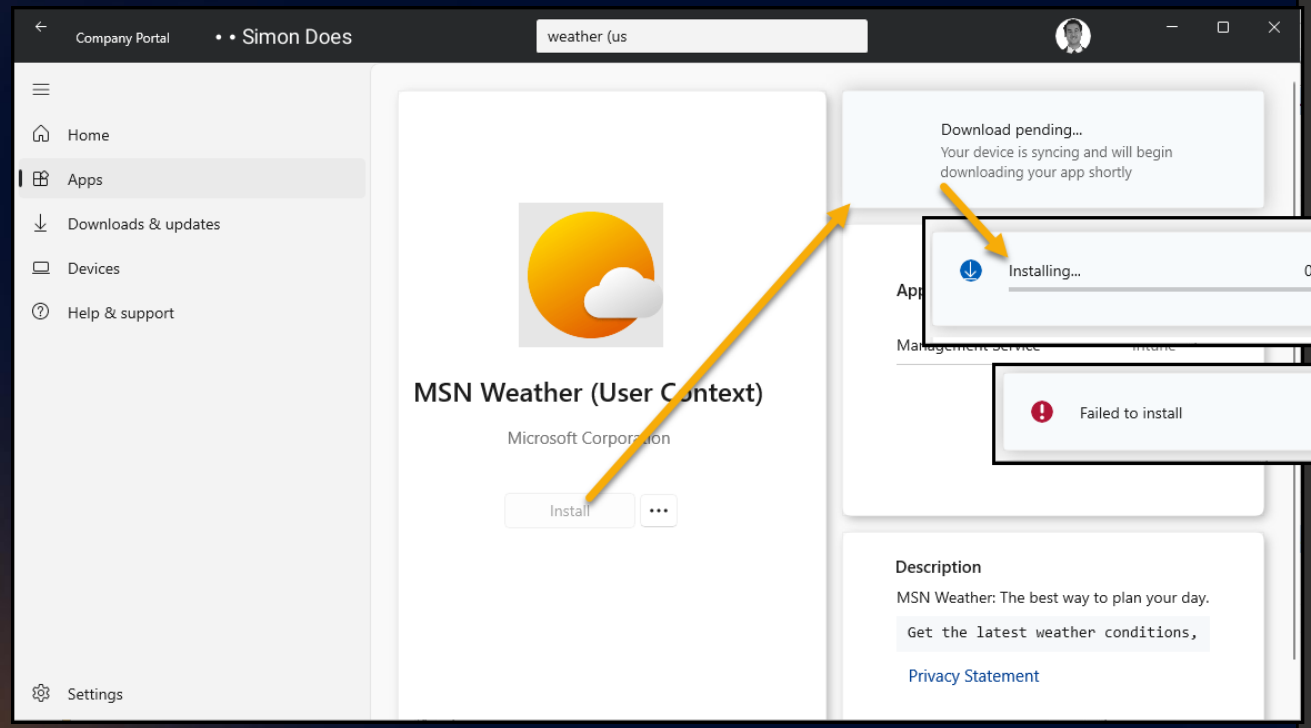
- Users can’t reinstall apps

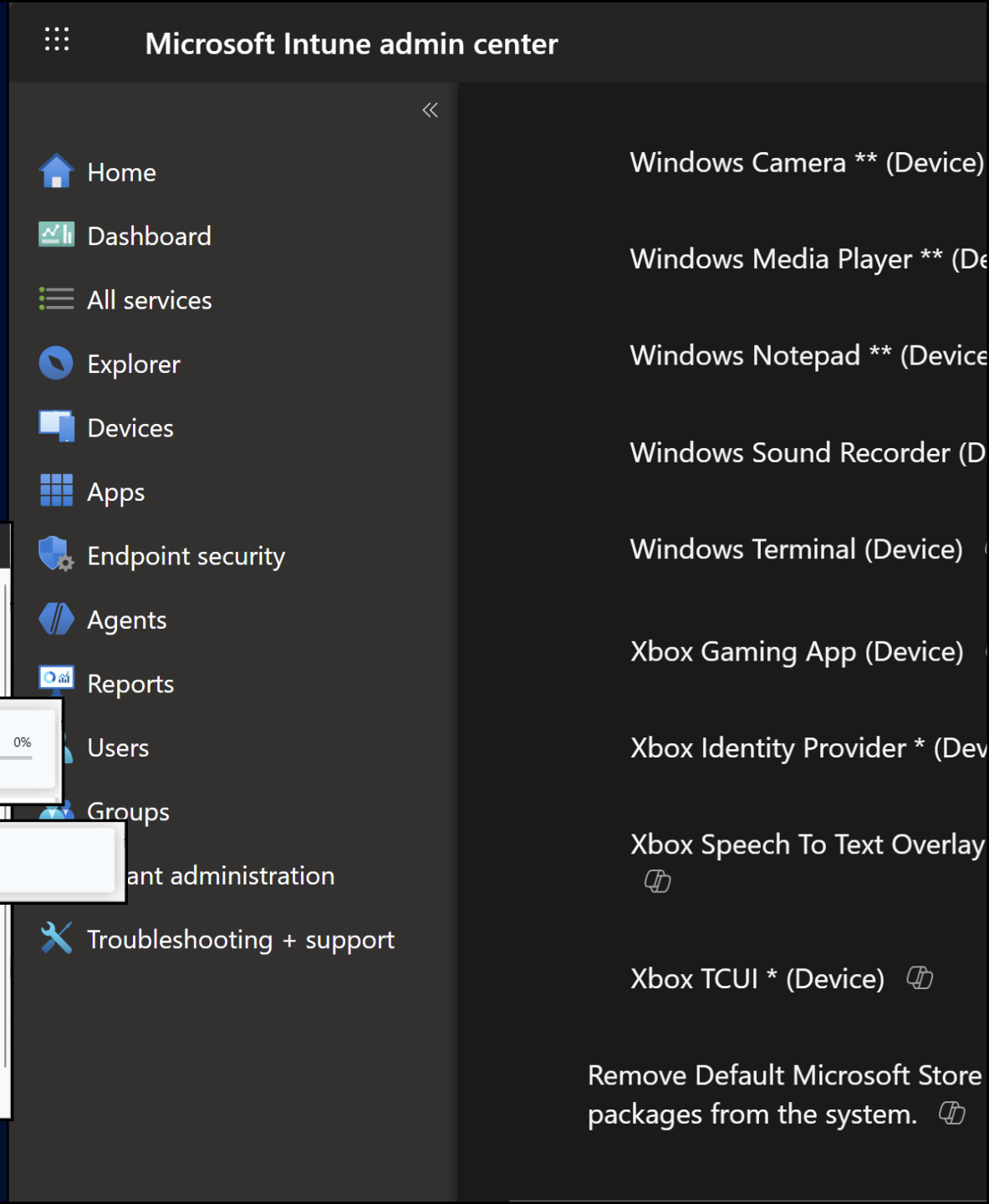




Microsoft Store Apps

- Users can’t reinstall apps
- Intune can’t install apps

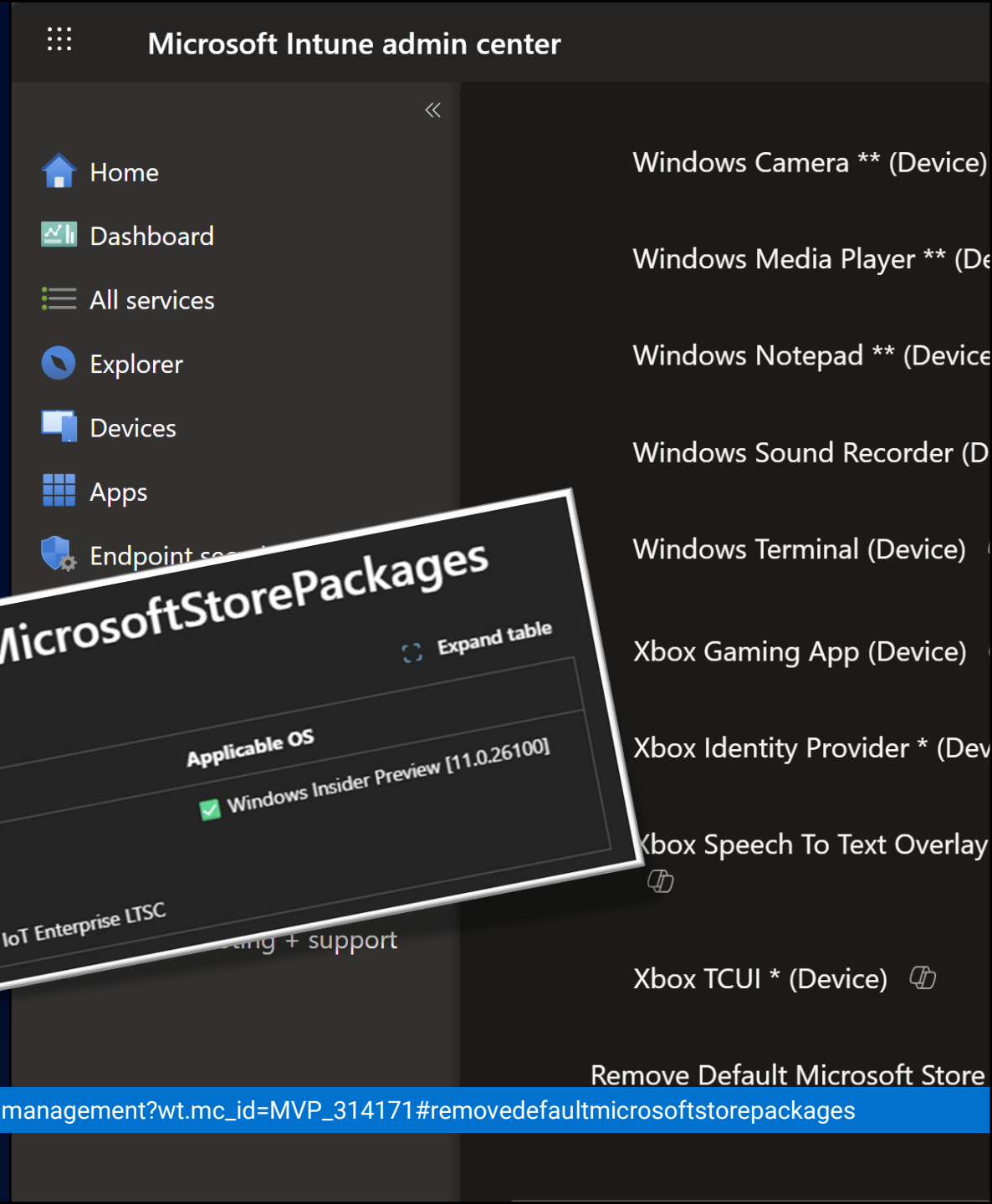




Microsoft Store Apps

- Users can’t reinstall apps
- Intune can’t install apps

- Only available for Enterprise
- Only available for Win 25H2



https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-applicationmanagement?wt.mc_id=MVP_314171#removedefaultmicrosoftstorepackages

Microsoft Store Apps

- Users can't reinstall apps
- Intune can't install apps

- Only available for Enterprise
- Only available for Win 25H2

https://msendpointmgr.com/2025/10/29/how-to-remove-built-in-apps-for-windows-11-25h2/

End Station?

Exit on the left side
Mind the gap!

https://support.microsoft.com/en-us/topic/policy-based-removal-of-pre-installed-microsoft-store-apps-e1d41a92-b658-4511-95a6-0fbcc02b4e9c


MIND THE GAP
MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026
Intune is a cloud service
Change is constant
Keep moving forward
Keep evergreen

Until your next Intune Night Train(ing)

Community

MEMSummit	https://www.endpointsummit.com/
WPNinjas	https://www.wpninjas.ch/, https://www.wpninjas.no/…
Experts Live	https://www.expertslive.org/
CTTT	https://cloudtechtallinn.com/
MMS	https://mmsmoa.com/
MSEndpointMGR	https://msendpointmgr.com/, https://www.youtube.com/@MSEndpointMgr/videos
Intune Newsletter	https://andrewstaylor.com/category/newsletter/
Reddit	https://www.reddit.com/r/MSIntune/ , https://www.reddit.com/r/Intune/
Bluesky	https://bsky.app/profile/did:plc:jsd42mucvn26b666i4g2yrjg/lists/3laeau7ntjc2n
LinkedIn MEM Group	https://www.linkedin.com/company/modern-endpoint-security

Official

MS Intune Blog	https://techcommunity.microsoft.com/t5/microsoft-intune-blog/bg-p/MicrosoftEndpointManagerBlog
What's New	https://learn.microsoft.com/en-us/mem/intune/fundamentals/whats-new
In Development	https://aka.ms/IntuneID
Message Center	https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/TenantAdminMenu/~/tenantStatus
Roadmap	https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=&searchterms=Intune
CCP	https://aka.ms/JoinMMCCP
Intune Doc	https://learn.microsoft.com/en-us/mem/intune/

IntuneFans

Give two hands to the Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

robopack

numecent

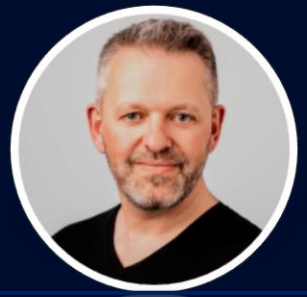
Microsoft

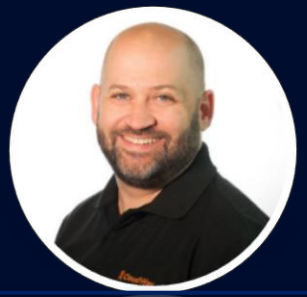
eido

Rimo3

THANK YOU!

Simon Skotheimsvik





Jan Ketil Skanke

Please rate this session on Sched.com

We would love to hear what you liked
and how we could improve!