



M365 &
Productivity

Day 2 • Fri 12 June

09:00

Room 3 • 75 min

Solved: The challenge of onboarding and involving mobile first users.

Learn how to streamline onboarding, communication, security, and collaboration for mobile-first users with Microsoft 365, Teams, Copilot, Viva, Entra ID, and Intune—while reducing shadow IT and connecting frontline employees to the rest of the organization.

Ståle Hansen

Copilot MVP & RD

CloudWay

Simon Skotheimsvik

Intune MVP

CloudWay



www.expertslive.co.uk

#ELUK26

Experts Live UK 2026

WITH THANKS TO

Our sponsors.

HEADLINER



PLATINUM



GOLD



SUPPORTER



www.expertslive.co.uk

WELCOME TO THE STAGE

Simon Skotheimsvik

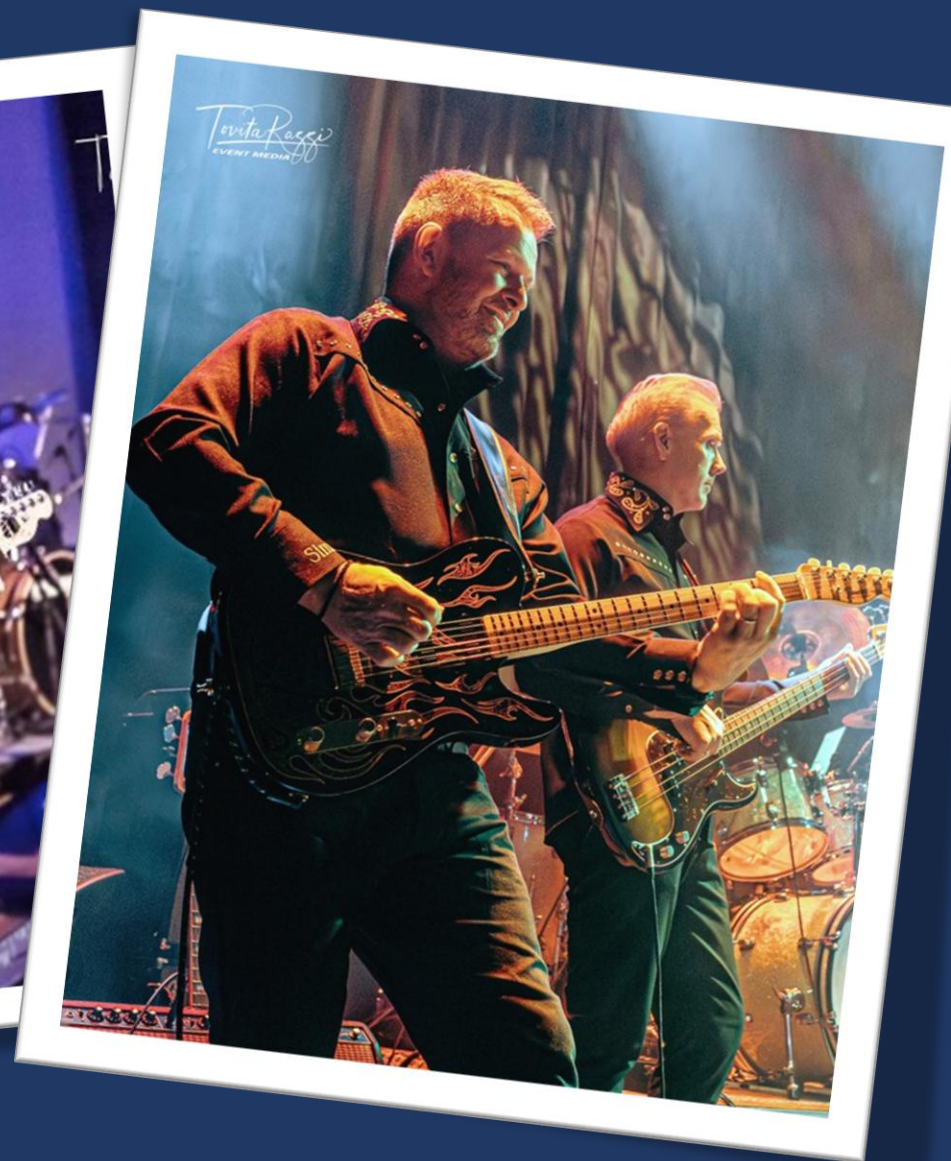
Senior Cloud Consultant, CloudWay, Norway

Microsoft MVP, Intune · keeps enterprises in tune on
identities, security and endpoint management

LinkedIn /in/simonskotheimsvik
Bluesky @skotheimsvik.no
Web linktr.ee/simonskotheimsvik



www.expertslive.co.uk



Experts  UK

www.expertslive.co.uk

UNITED STATES PATENT OFFICE

Application April 23, 1951, Serial No. 14,931

Aug. 14, 1951

Des. 164,227

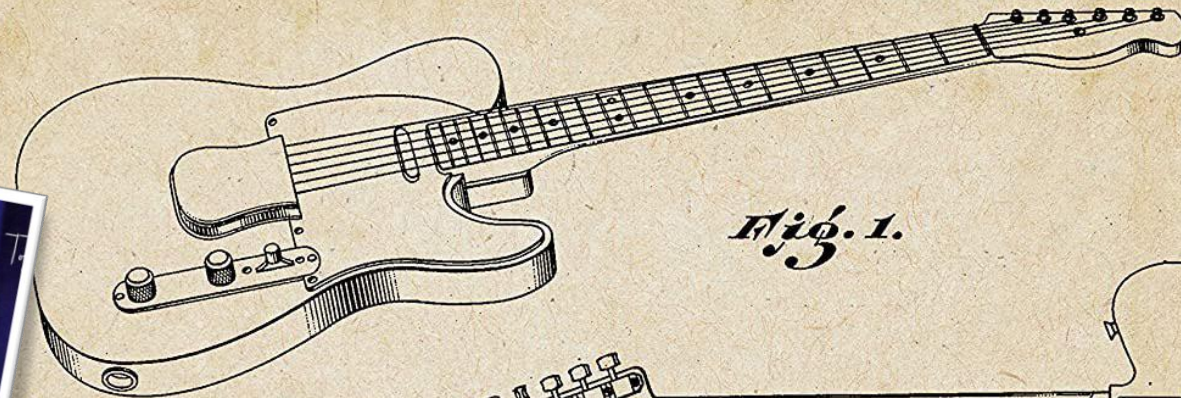


Fig. 1.

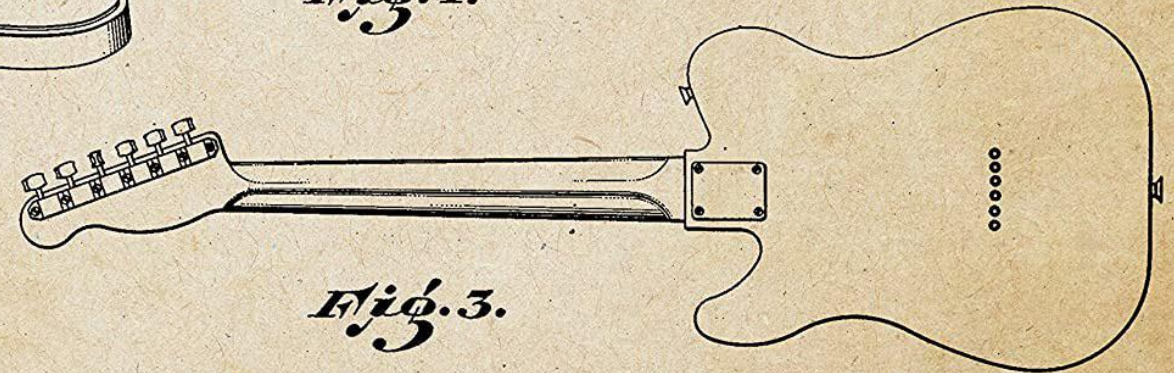


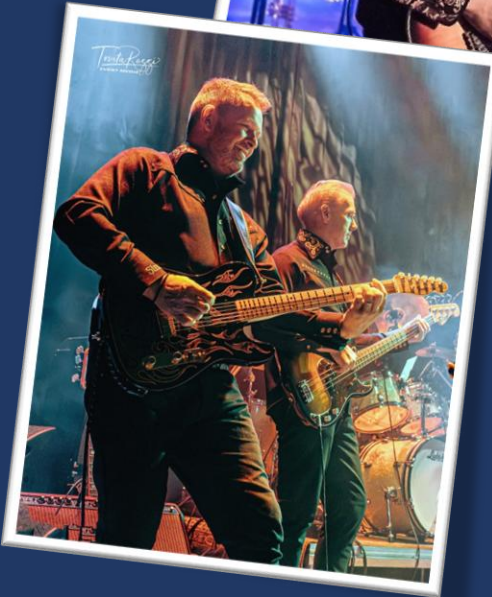
Fig. 3.

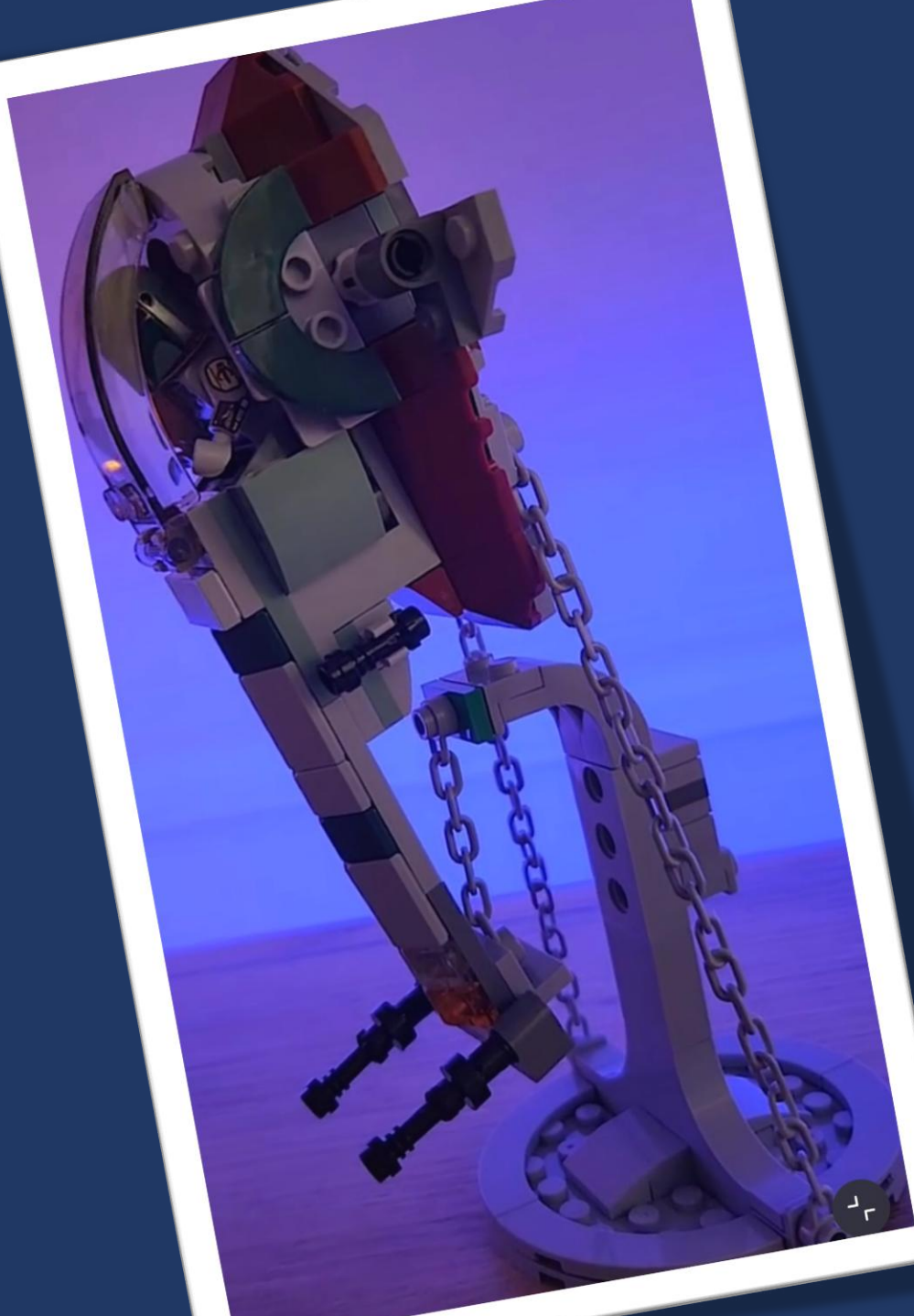


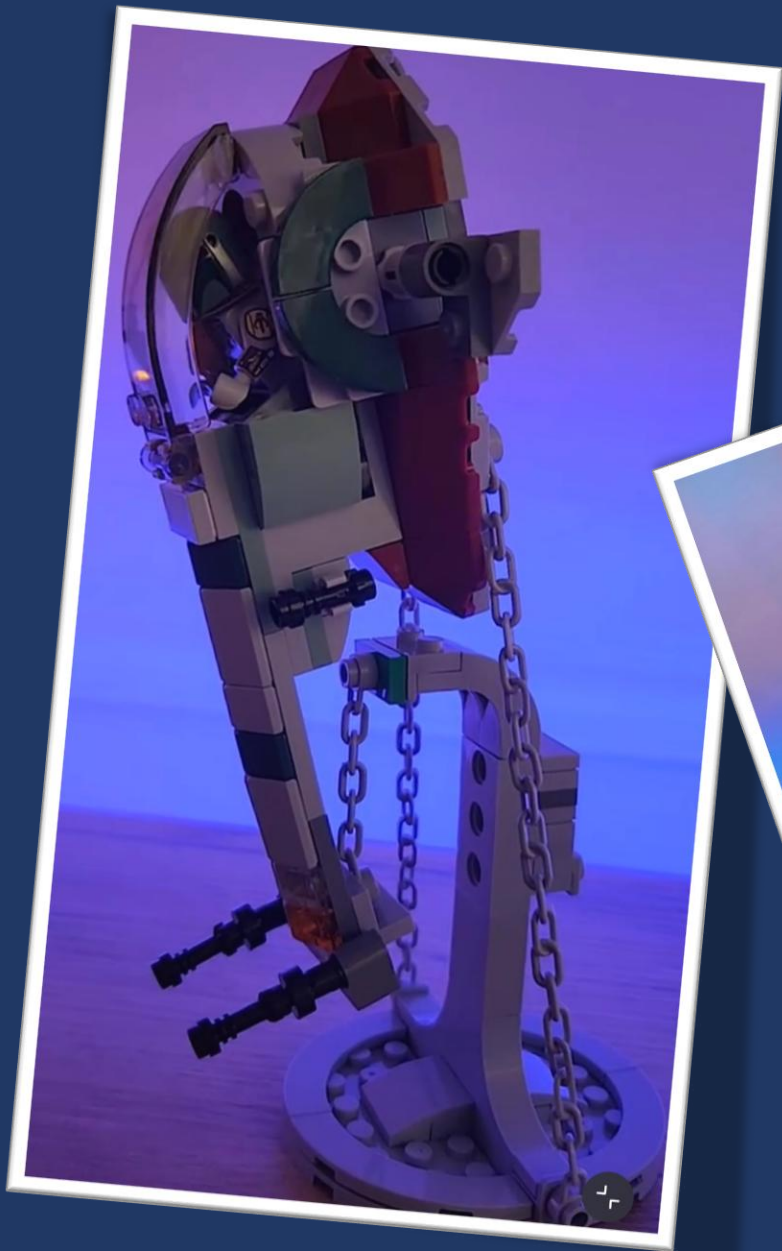
Fig. 2.

CLARENCE L. FENDER,
INVENTOR.

Lyons & Lyons
ATTORNEYS.







Experts  UK
www.expertslive.co.uk

G.K. CHRISTIANSEN

567913

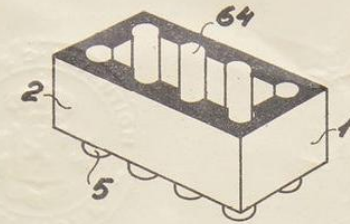


Fig. 9

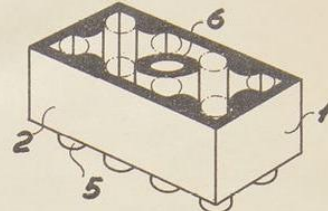


Fig. 10

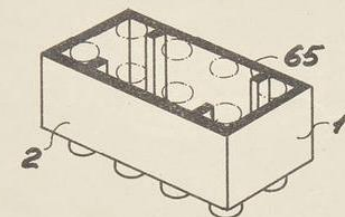


Fig. 11

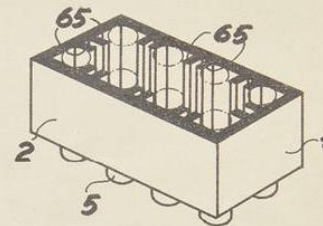


Fig. 12

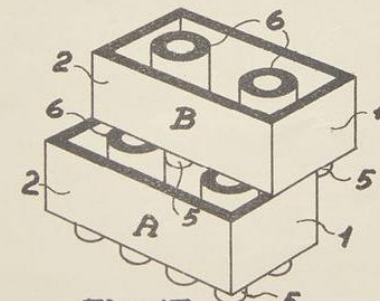


Fig. 13

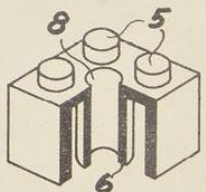


Fig. 14

Bruxelles, le 21 mai 1958
 P.Pon. de G.K. CHRISTIANSEN
 OFFICE KIRKPATRICK- C.T. PLUCKER
 25 IX 1958
 20F. 632640

WELCOME TO THE STAGE

Ståle Hansen

CEO, CloudWay, Norway

Microsoft RD & MVP, Copilot · Digital wellbeing
coach, Principal Cloud Architect

LinkedIn [/in/stalehansen/](#)
YouTube [@StaleHansen](#)
Web <https://msunified.net>



www.expertslive.co.uk

A man with glasses, wearing a dark suit, light blue shirt, and a red patterned tie, is holding a large white sign. He is looking down at the sign with a slight smile. The background is a solid dark blue.

The Challenge:

Onboard
and Involve
Mobile First Users

Mobile first user?

Communication

Communication



www.expertslive.co.uk

Communication





We are getting
Everyone on
Teams



Even the mobile
first users



They need their
Username
Password
And must set up
MFA



They need their
Username
Password
And must set up
MFA

- Get a corporate email address
- Learn your corporate email address
- Somehow, get hold of your temporary password

- Create a new password on first logon
- 15 letters
- 1 **capital** letter
- A number
- 1 **special** character
- But not that one

- ineedtoremember
- Ineedtoremember
- Ineedtoremember1
- Ineedtoremember1!

- I need to remember 2!
- But not too similar

- Now, set up twofactor authentication
 - Log on to <https://aka.ms/mfasetup>
 - Download the authenticator app
 - Set up and validate MFA

NOW you are ready

Download the Teams app

Remember your email address, remember your password, somehow get your authentication to work, oh, you need to download the company portal



www.expertslive.co.uk

- And sign in
- Reset your password every 3 month
- But you got a new phone
- Good luck

There has to be a simpler
way, Simon

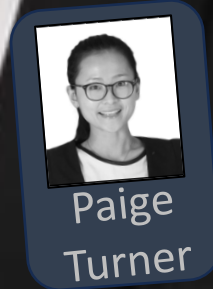
There has to be a simpler way, Simon

- BYOD
- Managed Device
- Shared Device



How Do I Sign In?

An employee have been
instructed to sign-in to Teams



Bring Your Own Device

You can sign in using your own
smartphone!

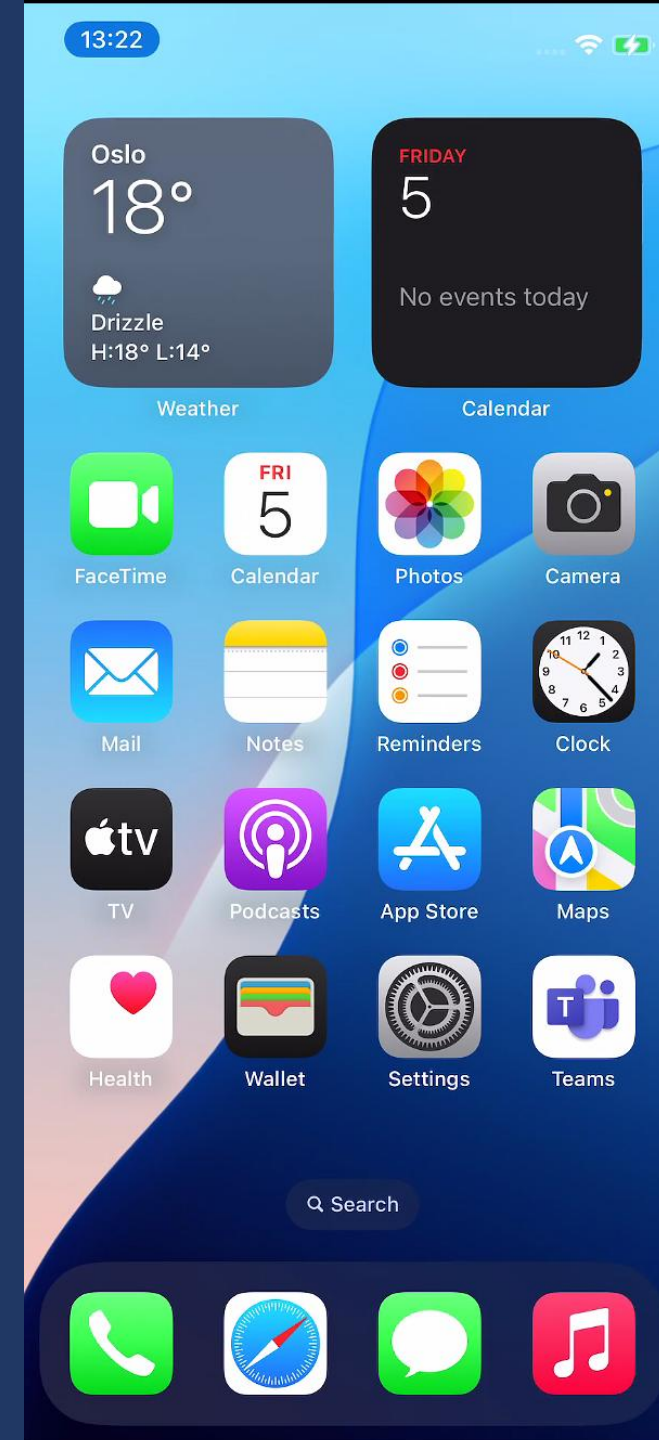


www.expertslive.co.uk

Bring Your Own Device

You can sign in using your own smartphone!

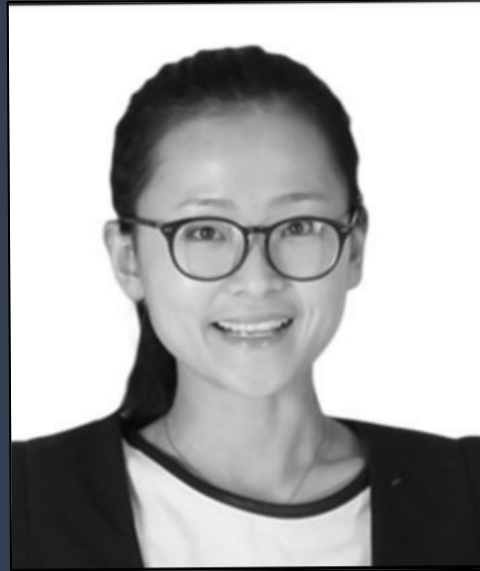
- Start Teams and sign in



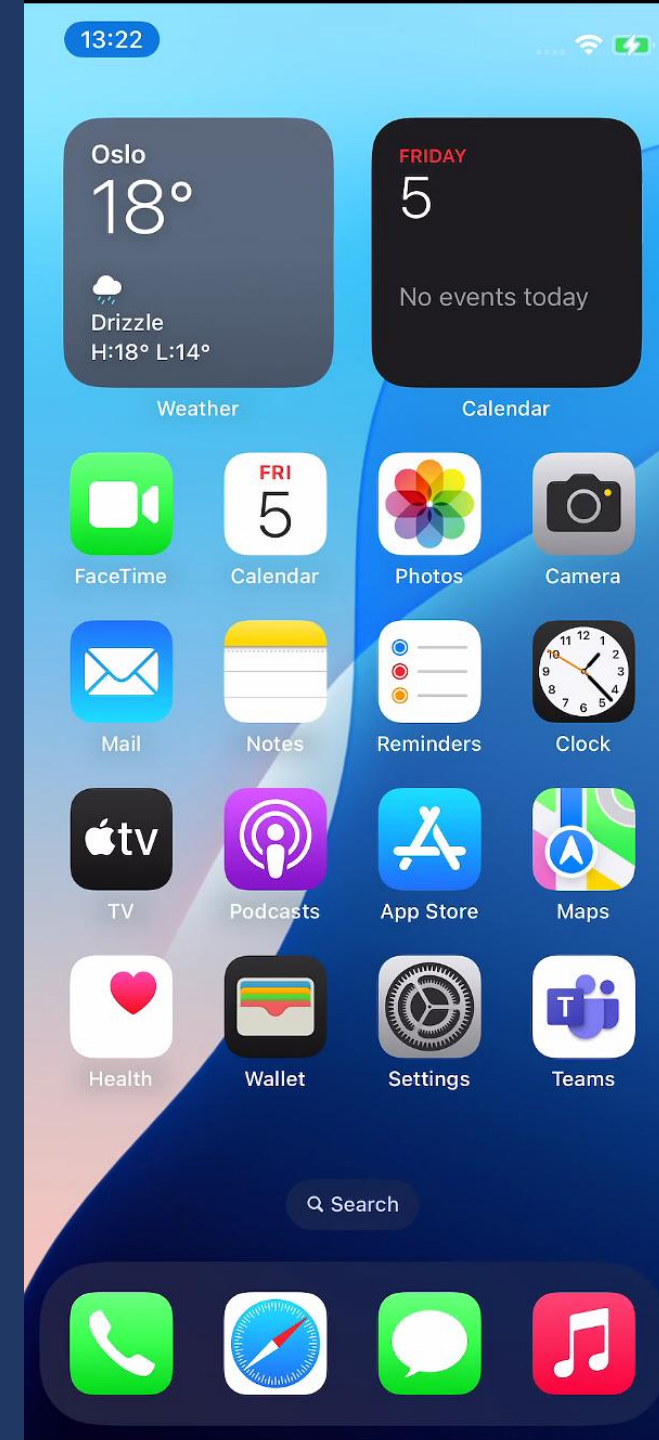
Bring Your Own Device

You can sign in using your own smartphone!

- Start Teams and sign in
- Use your badge



Paige
Turner



Bring Your Own Device

You can sign in using your own smartphone!

- Start Teams and sign in
- Use the back of your badge



Bring Your Own Device

You can sign in using your own smartphone!

- Start Teams and sign in
- Use the back of your badge



22:42



Intranet



Dashboard

News

Resources

Assigned Tasks

6 past due
Update
competency
credentials - Stål...

Add Task

Praise

Send praise to your
colleagues

Send praise

People

Find people

Enter a first or last name



Viva Learning

Keep learning, keep
growing

Open



Intranet

Chat

Engage

Calls

Activity

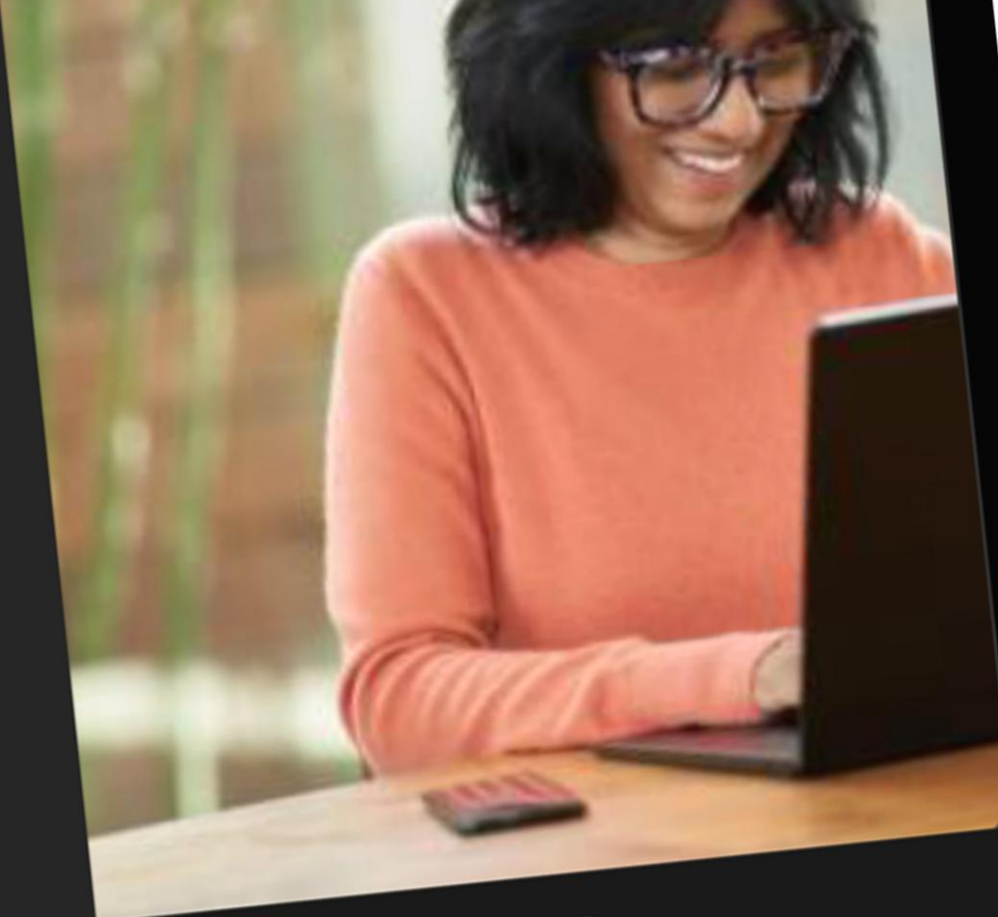
More



Viva Learning

Keep learning, keep
growing

Open



Intranet



Chat



Engage



Calls



Activity



More



Intranet

Dashboard

News

Resources



Assigned Tasks

6 past due

Update
competency
credentials - Stål...

Task



Praise

Send praise to your
colleagues

Send praise

 People

Find people

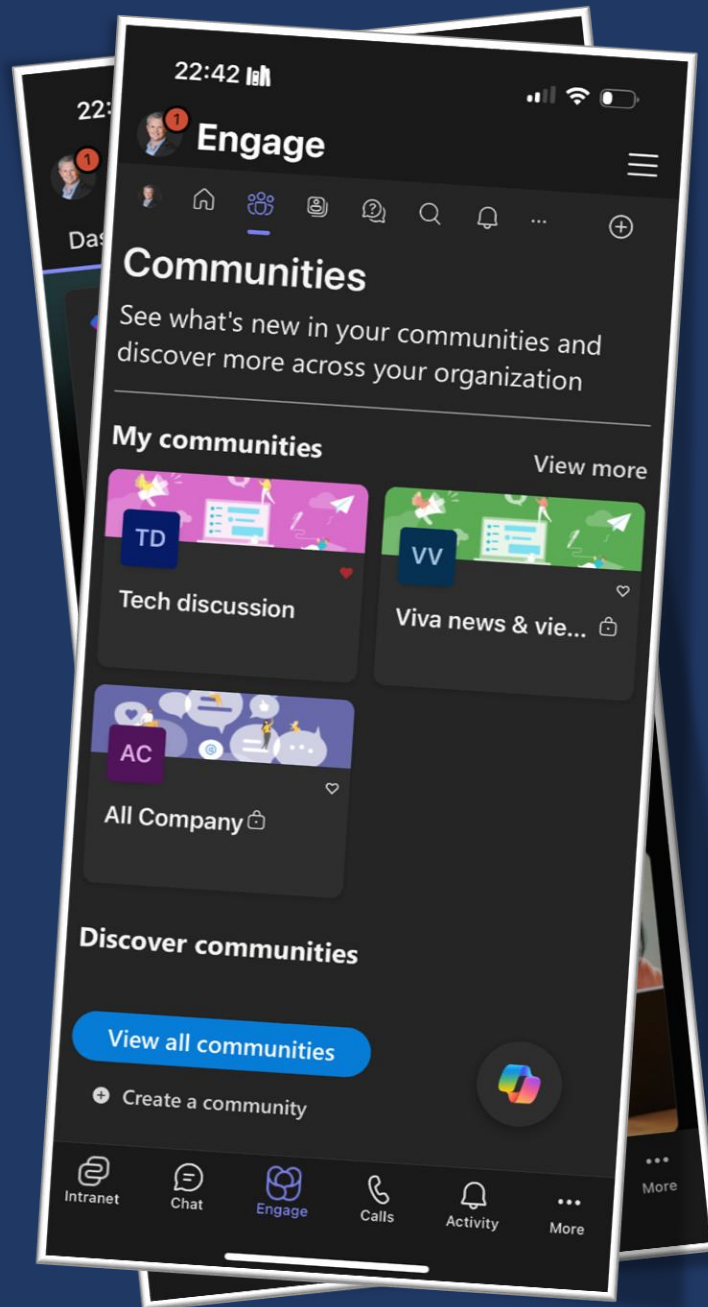
Enter a first or last name



 Viva Learning

Keep learning, keep
growing





07 Reports

08 Microsoft Global Collaboration

09 All What we do offers

10 New activities




Intranet


Chat


Engage


Calendar


Activity


More

22:45



Dashboard

Teams

Users

Teams devices

Teams apps

Manage apps

Permission policies

Setup policies

Customize store

Meetings

Messaging policies

Voice

Locations

Enhanced encryption p...

Policy packages

App setup policies

App setup policies control how apps are made available to a user with the Teams app. Use the Global (Org-wide default) policy and customize it or create custom policies and assign them to a set of users. [Learn more](#)

App setup policies summary

2

Default policies

0

Custom policies

Manage policies

Group policy assignment

+ Add

✎ Edit

📄 Duplicate

🗑 Delete

↺ Reset Global policy

👤 Assign users

🔍 Search



Name ↑

Global (Org-wide default)

FirstLineWorker

Description

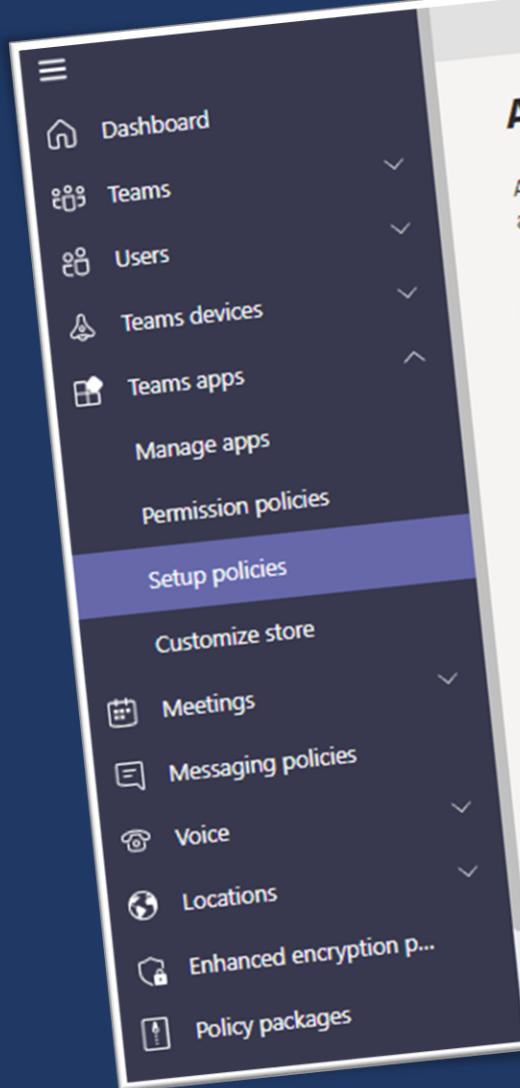
Custom policy

No

This is a default app setup ...

No





App setup po

App setup policies co
and customize it or c

App setu

2

Default

Mana

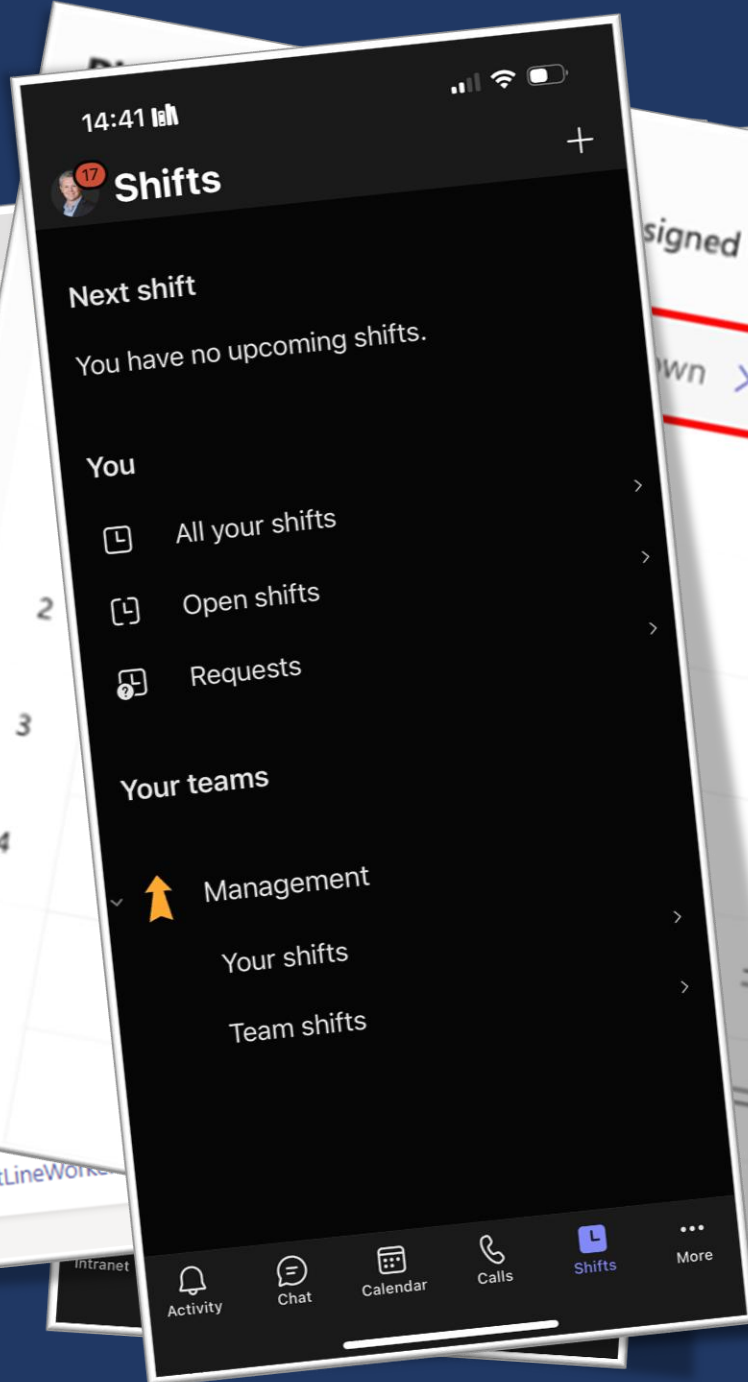
+

5

6

FirstLineWorks

Intranet



signed to this policy. S policy

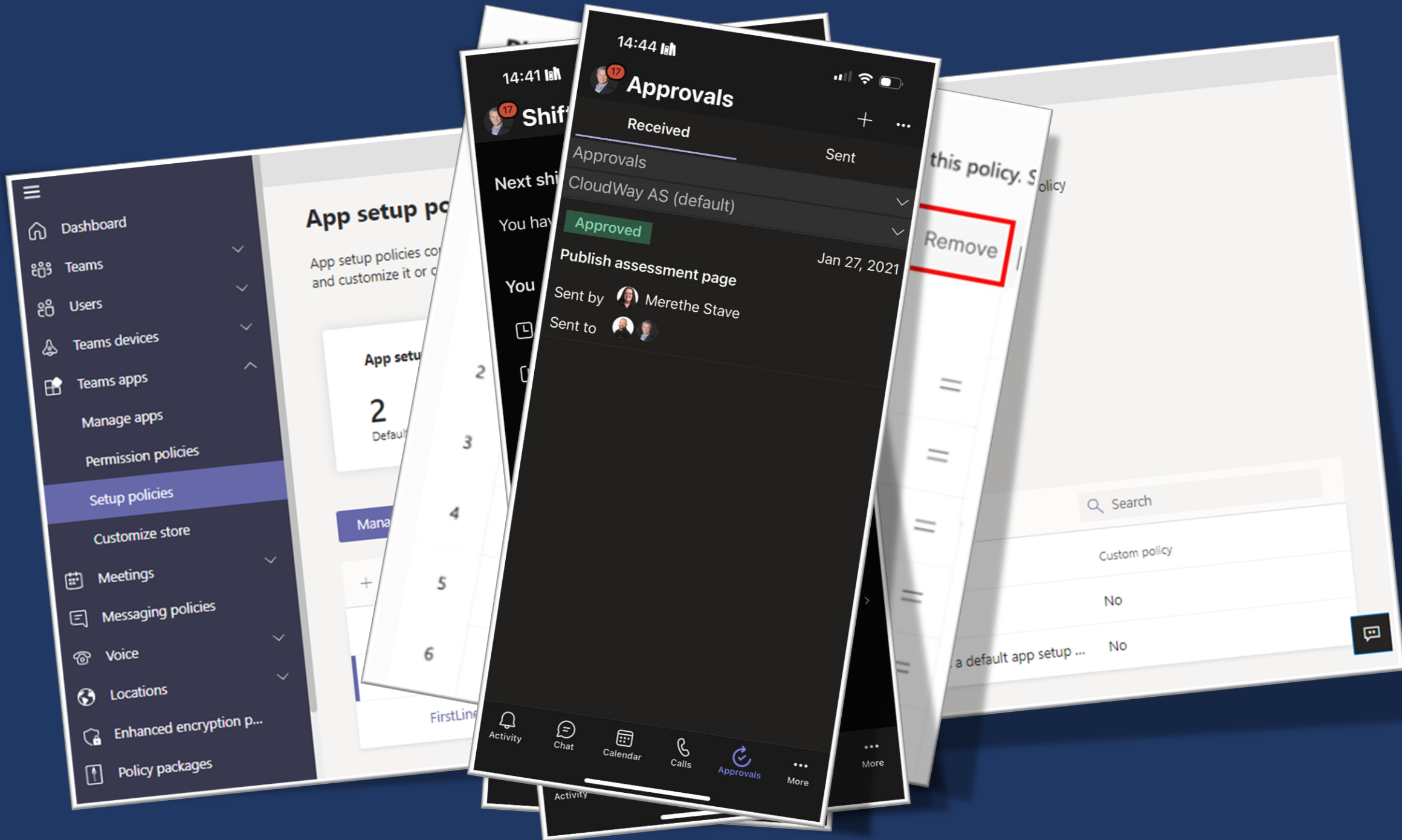
own X Remove

Search

Custom policy

No

a default app setup ... No



Communication



Communication



Communication



www.expertslive.co.uk

“

How Did You DO that?

The IT Manager wonders how this is possible!

How can I protect data on a personal device?





Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies

www.expertslive.co.uk



Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS

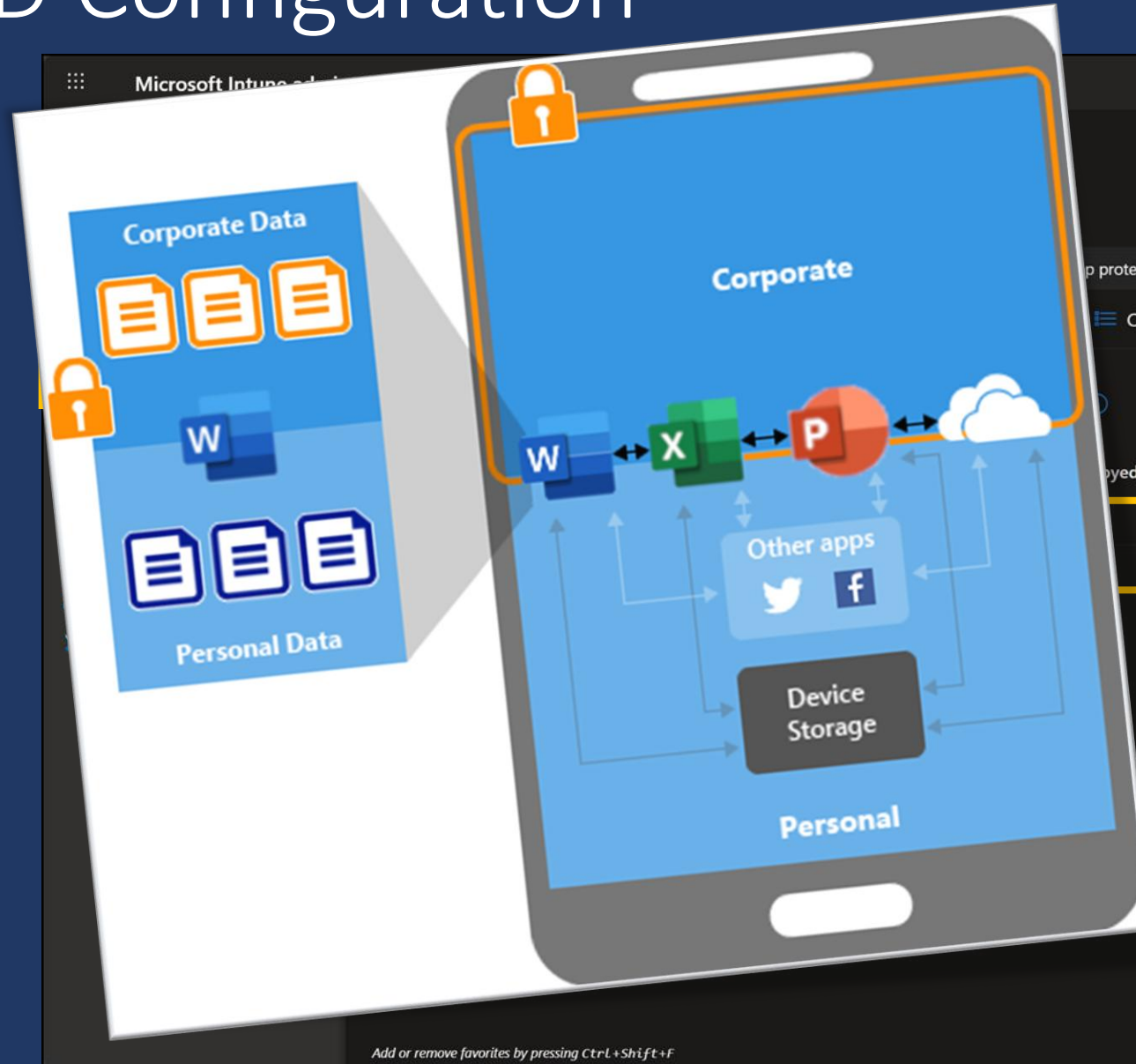
The screenshot shows the Microsoft Intune admin center interface. The left sidebar has the 'Apps' menu item highlighted with a yellow box. The main content area is titled 'Apps | Protection' and has the 'Protection' menu item highlighted with a yellow box. A table of App Protection Policies is displayed, with two policies highlighted by yellow boxes:

Policy name ↑	Deployed	Last modified	Platform
AAPP001 - All management type	Yes	10/09/2024, 09:43 AM	Android
IAPP001 - All management type	Yes	09/17/2024, 06:14 AM	iOS/iPadOS



Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS



Microsoft Intune

SKOTHEIMSVIK.NO (SKOTHEIMS...

App protection policies for Windows? [Learn more](#)

Columns ▾ App protection report: WIP via MDM 2 items

Add filters

Deployed	Last modified	Platform
	10/09/2024, 09:43 AM	Android
	09/17/2024, 06:14 AM	iOS/iPadOS

Add or remove favorites by pressing Ctrl+Shift+F

www.expertslive.co.uk

<https://learn.microsoft.com/en-us/intune/intune-service/apps/app-protection-policy>



Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS

Microsoft Intune admin center

Home > Apps

Apps | Protection

Search

Overview

All Apps

Monitor

Platforms

Manage apps

Configuration

Protection

iOS app provisioning profiles

S mode supplemental policies

Policies for Microsoft 365 apps

App selective wipe

Quiet time

Policy sets

Organize apps

Help and support

Did you know Microsoft Intune supports app protection policies for Windows? [Learn more](#)

Create Refresh Export Columns App protection report: WIP via MDM 2 items

Search Add filters

Policy name ↑	Deployed	Last modified	Platform
AAPP001 - All management type	Yes	10/09/2024, 09:43 AM	Android
IAPP001 - All management type	Yes	09/17/2024, 06:14 AM	iOS/iPadOS

Add or remove favorites by pressing Ctrl+Shift+F



Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS
 - Define for all apps
 - Store data only in managed locations

The screenshot displays the Microsoft Intune admin center interface. The left-hand navigation pane includes links to Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Intune App Protection | Properties' and shows details for a policy named 'IAPP001 - All management type'. The policy is configured for iOS/iPadOS and was created on 2023.07.17. The 'Basics' tab is active, showing the policy's name, description, and platform. The 'Apps' tab is also visible, showing settings for target apps, device types, and public apps. The 'Data protection' tab is highlighted with a yellow box, showing settings for preventing backups, sending org data to other apps, and saving copies of org data. The 'Data protection' settings are as follows:

Setting	Value
Prevent backups	Block
Send org data to other apps	Policy managed apps
Select apps to exempt	Default: skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
Select universal links to exempt	http://facetime.apple.com http://maps.apple.com
Save copies of org data	Block
Allow user to save copies to selected services	OneDrive for Business SharePoint
Transfer telecommunication data to	Any dialer app
Dialer App URL Scheme	No Dialer App URL Scheme

www.expertslive.co.uk

<https://learn.microsoft.com/en-us/intune/intune-service/apps/app-protection-policy>



Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS
 - Define for all apps
 - Store data only in managed locations
 - Control copy/paste
 - Encrypt corporate data
 - Block printing of org. data
 - Block screen capture
 - Set access requirements

The screenshot displays the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area shows the 'Camera' settings for an App Protection Policy. The settings are organized into two sections: 'Camera' and 'Access requirements'. The 'Camera' section includes settings for restricting cut, copy, and paste; cut and copy character limit; third party keyboards; encrypting org data; syncing policy managed app data; printing org data; restricting web content transfer; unmanaged browser protocol; org data notifications; Genmoji; screen capture; and writing tools. The 'Access requirements' section includes settings for PIN for access, PIN type, simple PIN, select minimum PIN length, touch ID instead of PIN for access (iOS 8+/iPadOS), override biometrics with PIN after timeout, timeout (minutes of inactivity), face ID instead of PIN for access (iOS 11+/iPadOS), and PIN reset after number of days. Several settings are highlighted with yellow boxes: 'Restrict cut, copy, and paste between other apps' (Policy managed apps with paste in other apps), 'Encrypt org data' (Require), 'Printing org data' (Block), 'Screen capture' (Block), 'PIN for access' (Require), 'PIN type' (Numeric), 'Simple PIN' (Block), 'Touch ID instead of PIN for access (iOS 8+/iPadOS)' (Allow), 'Face ID instead of PIN for access (iOS 11+/iPadOS)' (Allow), and 'Timeout (minutes of inactivity)' (0).

Setting	Value
Restrict cut, copy, and paste between other apps	Policy managed apps with paste in other apps
Cut and copy character limit for any app	0
Third party keyboards	Allow
Encrypt org data	Require
Sync policy managed app data with native apps or add-ins	Allow
Printing org data	Block
Restrict web content transfer with other apps	Microsoft Edge
Unmanaged browser protocol	No Unmanaged browser protocol
Org data notifications	Allow
Genmoji	Block
Screen capture	Block
Writing tools	Block

Access requirements [Edit](#)

Setting	Value
PIN for access	Require
PIN type	Numeric
Simple PIN	Block
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Not required
Timeout (minutes of inactivity)	0
Face ID instead of PIN for access (iOS 11+/iPadOS)	Allow
PIN reset after number of days	No

www.expertslive.co.uk

<https://learn.microsoft.com/en-us/intune/intune-service/apps/app-protection-policy>



Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS
 - Define for all apps
 - Store data only in managed locations
 - Control copy/paste
 - Encrypt corporate data
 - Block printing of org. data
 - Block screen capture
 - Set access requirements
 - Wipe corporate data, not device

Microsoft Intune admin center

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

Override biometrics with PIN after timeout Not required

Timeout (minutes of inactivity) 0

Face ID instead of PIN for access (iOS 11+/iPadOS) Allow

PIN reset after number of days No

Number of days 0

App PIN when device PIN is set Not required

Work or school account credentials for access Not required

Recheck the access requirements after (minutes of inactivity) 30

Conditional launch [Edit](#)

Setting	Value	Action
Max PIN attempts	10	Wipe data
Offline grace period	1440	Block access (minutes)
Offline grace period	60	Wipe data (days)
Disabled account		Wipe data
Jailbroken/rooted devices		Wipe data

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
All Users	None	None

www.expertslive.co.uk

<https://learn.microsoft.com/en-us/intune/intune-service/apps/app-protection-policy>

Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS
 - Define for all apps
 - Store data only in managed locations
 - Control copy/paste
 - Encrypt corporate data
 - Block printing of org. data
 - Block screen capture
 - Set access requirements
 - Wipe corporate data, not device

The screenshot shows the Microsoft Intune admin center interface. On the left is a navigation pane with options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Microsoft Intune admin center' and displays settings for 'Override biometrics with PIN after timeout'. The settings are as follows:

Setting	Value
Override biometrics with PIN after timeout	Not required
Timeout (minutes of inactivity)	0
Face ID instead of PIN for access (iOS 11+/iPadOS)	Allow
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Not required
Work or school account credentials for access	Not required
Recheck the access requirements after (minutes of inactivity)	30

Below these settings is a section for 'Conditional launch' with an 'Edit' link. It contains a table with the following settings:

Setting	Value
Max PIN attempts	10
Offline grace period	1440
Offline grace period	60
Disabled account	
Jailbroken/rooted devices	

At the bottom, there is an 'Assignments' section with an 'Edit' link, followed by an 'Included groups' section with a table:

Group	Filter
All Users	None

www.expertslive.co.uk

<https://learn.microsoft.com/en-us/intune/intune-service/apps/app-protection-policy>

13:42



Activity



Unread

@Mentions

Replies

Reactions



Your organization is now protecting its data in this app. Restart the app to continue.

OK

OK

Intune - BYOD Configuration

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS
 - Define for all apps
 - Store data only in managed locations
 - Control copy/paste
 - Encrypt corporate data
 - Block printing of org. data
 - Block screen capture
 - Set access requirements
 - Wipe corporate data, not device

Microsoft Intune admin center

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

Override biometrics with PIN after timeout Not required

Timeout (minutes of inactivity) 0

Face ID instead of PIN for access (iOS 11+ / iPadOS) Allow

PIN reset after number of days No

Number of days 0

App PIN when device PIN is set Not required

Work or school account credentials for access Not required

Recheck the access requirements after (minutes of inactivity) 30

Conditional launch Edit

Setting	Value
Max PIN attempts	10
Offline grace period	1440
Offline grace period	60
Disabled account	
Jailbroken/rooted devices	

Assignments Edit

Included groups

Group	Filter
All Users	None



Your organization requires this account's data to be protected with a PIN.



No repeats or sequences. Ex. 123 or 111

Intune - BYOD Configuration



Your organization doesn't allow screen capture or recording.

- Microsoft Intune
- BYOD is protected by App Protection Policies
- Build policies for Android and iOS
 - Define for all apps
 - Store data only in managed locations
 - Control copy/paste
 - Encrypt corporate data
 - Block printing of org. data
 - Block screen capture
 - Set access requirements
 - Wipe corporate data, not device

The screenshot displays the Microsoft Intune admin center interface. On the left is a navigation pane with options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Microsoft Intune admin center' and shows the configuration for an App Protection Policy. The 'Conditional launch' section is expanded, showing a table of settings:

Setting	Value
Override biometrics with PIN after timeout	Not required
Timeout (minutes of inactivity)	0
Face ID instead of PIN for access (iOS 11+/iPadOS)	Allow
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Not required
Work or school account credentials for access	Not required
Recheck the access requirements after (minutes of inactivity)	30

Below this, the 'Conditional launch' section is expanded, showing a table of settings:

Setting	Value
Max PIN attempts	10
Offline grace period	1440
Offline grace period	60
Disabled account	
Jailbroken/rooted devices	

At the bottom, the 'Assignments' section is expanded, showing a table of settings:

Group	Filter
All Users	None

www.expertslive.co.uk

<https://learn.microsoft.com/en-us/intune/intune-service/apps/app-protection-policy>

“

How Did You DO that?

The IT Manager wonders how this is possible!

What is QR Sign-In?

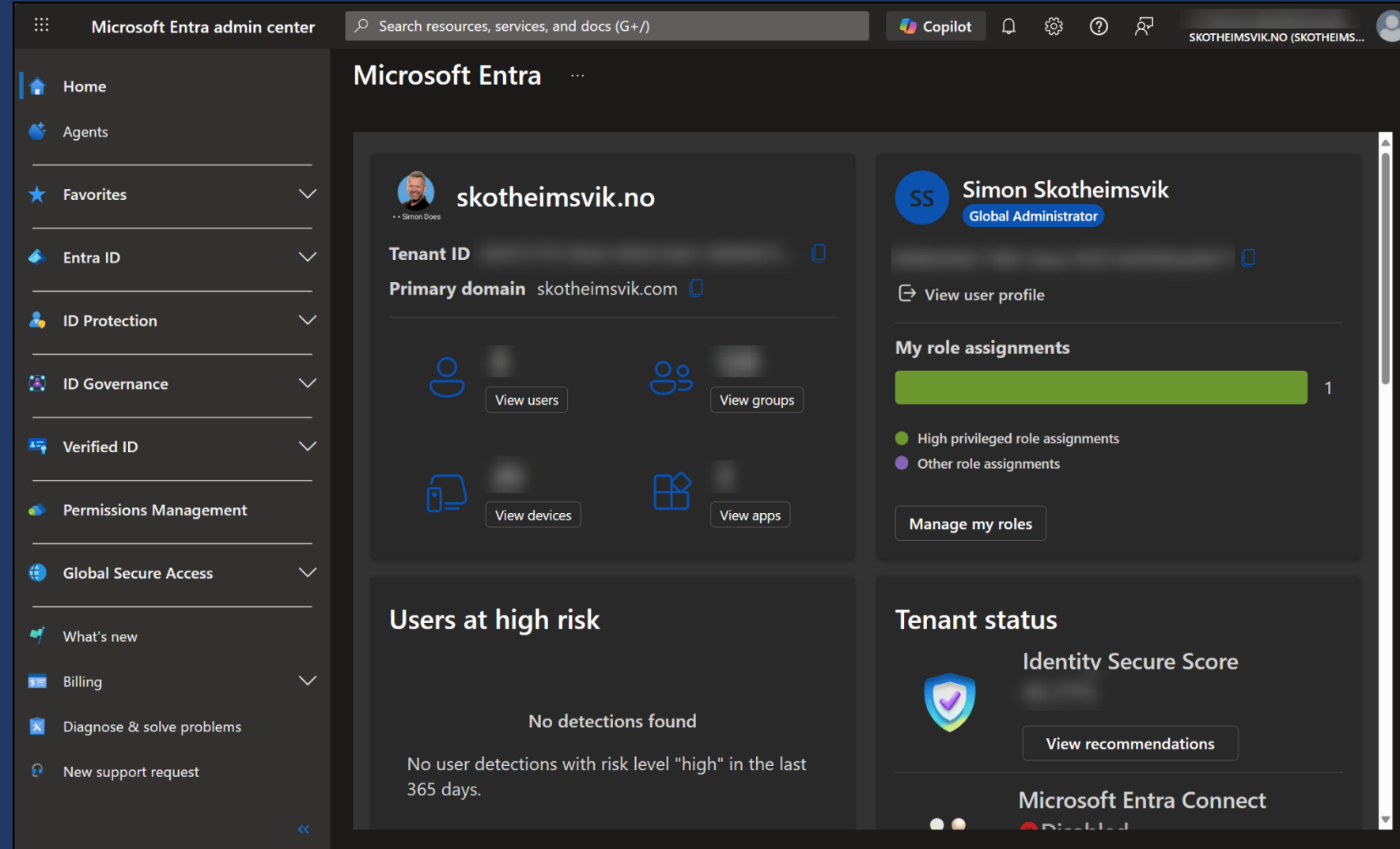




Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- A modern sign-in method
- Designed especially for frontline workers using shared devices.
- Simplifies and secures access by replacing traditional usernames and passwords with a QR code and PIN combo.

GA from June 24, 2025





Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Authentication methods
- Policies
- QR code

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > Authentication methods | Policies

skotheimsvik.no - Microsoft Entra ID Security

Search

+ Add external method (Preview) Refresh Got feedback?

Manage

- Policies
- Password protection
- Registration campaign
- Authentication strengths
- Settings

Monitoring

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Migration status: Complete (change)

Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens		No
Voice call		No
Email OTP		Yes
Certificate-based authentication		No
QR code	1 group	Yes



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Authentication methods
- Policies
- QR code
- Tune the settings

Home > Authentication methods | Policies >

QR code settings

QR code authentication is a simple and fast authentication method for frontline workers. To use it, you need both a QR code and PIN. [Learn more.](#)

Enable and Target Configure

Enable ☒

Include Exclude

Target ☐ All users ☒ Select groups

[Add groups](#)

Name	Type	Registration
AAD - Frontline Workers	Group	Optional



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Authentication methods
- Policies
- QR code
- Tune the settings
- Enable and scope

Home > Authentication methods | Policies >

QR code settings

QR code authentication is a simple and fast authentication method for frontline workers. To use it, you need both a QR code and PIN. [Learn more.](#)

Enable and Target Configure

Enable ☒

Include Exclude

Target ☐ All users ☒ Select groups

[Add groups](#)

Name	Type	Registration
AAD - Frontline Workers	Group	Optional



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Authentication methods
- Policies
- QR code
- Tune the settings
- Enable and scope

Home > Authentication methods | Policies >

QR code settings

QR code authentication is a simple and fast authentication method for frontline workers. To use it, you need both a QR code and PIN. [Learn more.](#)

Enable and Target Configure

Enable ☒

Include Exclude

Target ☐ All users ☒ Select groups

[Add groups](#)

Name	Type	Registration
AAD - Frontline Workers	Group	Optional



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Authentication methods
- Policies
- QR code
- Tune the settings
- Enable and scope

Home > Authentication methods | Policies >

QR code settings

QR code authentication is a simple and fast authentication method for frontline workers. To use it, you need both a QR code and PIN. [Learn more.](#)

Enable and Target Configure

Enable ☒

Include Exclude

Target ☐ All users ☒ Select groups

[Add groups](#)

Name	Type	Registration
AAD - Frontline Workers	Group	Optional



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Authentication methods
- Policies
- QR code
- Tune the settings
- Enable and scope
- QR quality and lifetime

Home > Authentication methods | Policies >

QR code settings

QR code authentication is a simple and fast authentication method for frontline workers. To use it, you need both a QR code and PIN. [Learn more.](#)

Enable and Target **Configure**

Defaults

QR PIN Length * ⓘ 8

Lifetime of standard QR code (days) * ⓘ 365



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Each user is assigned a unique QR code and numeric PIN

Microsoft Entra admin center

Search resources, services, and docs (G+/I)

Copilot

SKOTHEIMSVIK.NO (SKOTHEIMS...

Home > Paige Turner >

Users skotheimsvik.no

All users

Audit logs

Sign-in logs

Diagnose and solve problems

Deleted users

Password reset

User settings

Bulk operation results

Bulk operation results (Preview)

New support request

+ New user Edit Delete Download users (Preview) Bulk operations

Azure Active Directory is now Microsoft Entra ID.

Search Add filter

9 users found

	Display name ↑	User principal name ↑↓	User type	On-premises
☐	[Redacted]	[Redacted]	Member	No
☐	[Redacted]	[Redacted]	Member	No
☐	Justin Time	justin.time@skoth...	Member	No
☐	Paige Turner	paige.turner@sko...	Member	No
☐	[Redacted]	[Redacted]	Member	No
☐	[Redacted]	[Redacted]	Guest	No
☐	[Redacted]	[Redacted]	Member	No
☐	[Redacted]	[Redacted]	Member	No
☐	Terry Bull	terry.bull@skothei...	Member	No



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Each user is assigned a unique QR code and numeric PIN
- Add authentication method

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane has the 'Authentication methods' option highlighted with a yellow box. The main content area is titled 'Paige Turner | Authentication methods' and includes a search bar and a '+ Add authentication method' button, which is also highlighted with a yellow box. Below this, there is a section for 'Usable authentication methods' with a table containing two rows of blurred information. Further down, there is a section for 'Non-usable authentication methods' which states 'No non-usable methods.' At the bottom, there is a section for 'System preferred multifactor authentication method' with a table containing two rows of blurred information.



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Each user is assigned a unique QR code and numeric PIN
- Add authentication method
 - QR code

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation pane has 'Authentication methods' highlighted. The main pane shows the 'Paige Turner | Authentication methods' page. On the right, the 'Add authentication method' dialog is open, displaying a 'Choose method' dropdown menu with options: Email, Phone number, Temporary Access Pass, and QR code. The 'QR code' option is selected and highlighted with a yellow border. Below the dropdown is an 'Add' button.



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Each user is assigned a unique QR code and numeric PIN
- Add authentication method
 - QR code
 - Expiration date
 - Activation time
 - PIN code

Microsoft Entra admin center

Home > Users > Paige Turner

Paige Turner | Authentication methods

Search

+ Add authentication method | Reset password

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Custom security attributes

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

New support request

Authentication methods are the ways users sign into Microsoft Entra ID. The user's default sign-in method is the one they are required to authenticate with a second factor - typically a registered, enabled authentication method to authenticate.

Default sign-in method (Preview) SMS (primary)

Usable authentication methods

Authentication method

Non-usable authentication methods

Authentication method

No non-usable methods.

System preferred multifactor authentication method

Feature status System preferred M

Add authentication method

Choose method

QR code

Standard QR code

This is the primary QR code associated with the authentication method. Once the standard QR code and PIN are generated, you can add a temporary QR code. [Learn more](#)

Expiration * ①

08/19/2026 11:59 PM

(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Activation time *

☒ Now

☐ Later

PIN

This PIN works for both standard and temporary QR codes. Users must change it when they first sign in.

PIN * ①

[Generate PIN](#)

Add



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Each user is assigned a unique QR code and numeric PIN
- Add authentication method
 - QR code
 - Expiration date
 - Activation time
 - PIN code
 - Download QR code

Microsoft Entra admin center

Home > Users > Paige Turner

Paige Turner | Authentication methods

Search

+ Add authentication method | Reset password

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Custom security attributes

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

New support request

Authentication methods are the ways users sign into Microsoft Entra ID. The user's default sign-in method is the one they are required to authenticate with a second factor - a registered, enabled authentication method to authenticate.

Default sign-in method (Preview) ⓘ SMS (primary)

Usable authentication methods

Authentication method
QR code

Non-usable authentication methods

Authentication method
No non-usable methods.

System preferred multifactor authentication method

Feature status	System preferred method

Download QR code Successfully added method

Successfully added QR code.

This QR code is only available for download right now. Download and save it in a secure place. If you need a QR code in future, simply delete this one and generate a new standard QR code.

COPY PIN

PIN

Standard QR code



QR code ID: [redacted]

Activation time: 8/20/2025, 12:37:56 PM

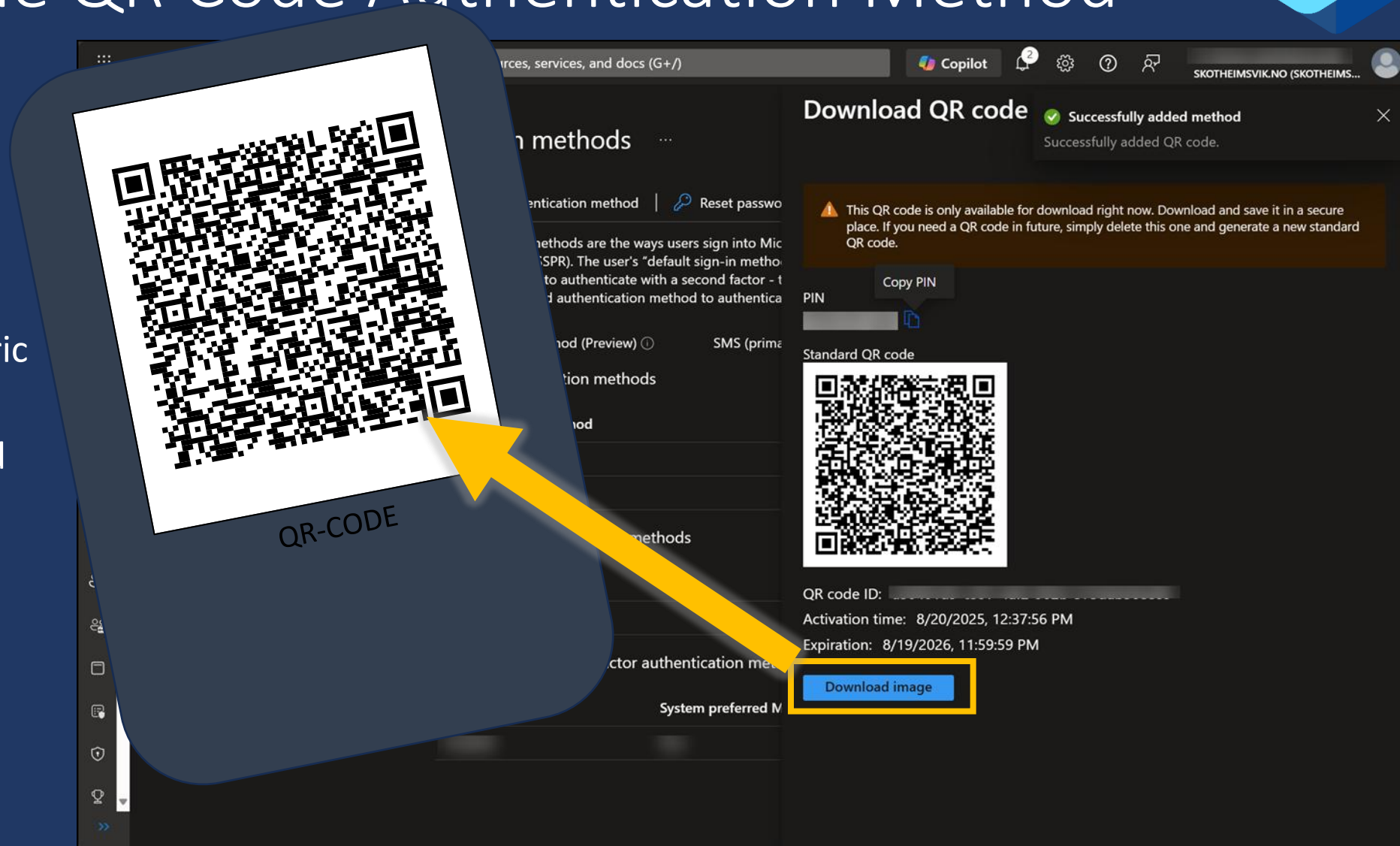
Expiration: 8/19/2026, 11:59:59 PM

Download image



Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Each user is assigned a unique QR code and numeric PIN
- Add authentication method
 - QR code
 - Expiration date
 - Activation time
 - PIN code
 - Download QR code
 - Apply it to the ID card



“

How Did You DO that?

The IT Manager wonders how this is possible!

Can we provision the QR code as part of onboarding process?





Entra ID – Enable QR Code Authentication Method

- Microsoft Entra ID QR Code Authentication
- Each user is assigned a unique QR code and numeric PIN
- Add authentication method
 - QR code
 - Expiration date
 - Activation time
 - PIN code
 - Download QR code
 - Apply it to the ID card
 - **PowerShell**

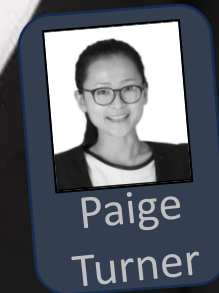
The screenshot shows a Visual Studio Code editor window with a PowerShell script titled 'EntraID-Add-QRCodeAuthenticationMethod.ps1'. The script includes a synopsis and a description. The synopsis states: 'Add QR code authentication method for a user using Microsoft Graph API'. The description states: 'This script demonstrates how to add a software OATH token (QR code) authentication method for a user in Entra ID (Azure AD) using Microsoft Graph REST API. The script will return the secret key and generate a QR code that can be scanned with an authenticator app.' The source is cited as: <https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-authentication-qr-code#add-qr-code>. Below the script, the 'TERMINAL' tab is active, showing a PowerShell prompt at 'C:\My Local Documents\GitHub\Community-By-SSkotheimsvik\Microsoft\AAD>'. The status bar at the bottom indicates the file is on 'main' branch, with 0 errors and 0 warnings. The user 'simon.skotheimsvik@gmail.com' is logged in, and the cursor is at line 21, column 1.

```
<#  
.SYNOPSIS  
    Add QR code authentication method for a user using Microsoft Graph API  
  
.DESCRIPTION  
    This script demonstrates how to add a software OATH token (QR code) authentication method  
    for a user in Entra ID (Azure AD) using Microsoft Graph REST API.  
    The script will return the secret key and generate a QR code that can be scanned with  
    an authenticator app.  
  
    Source: https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-authentication-qr-code#add-qr-code
```

PS C:\My Local Documents\GitHub\Community-By-SSkotheimsvik\Microsoft\AAD>

I Don't Like To Use My Private Phone for Work!

An employee have been instructed to sign-in to Teams



Shared Device

We have shared devices for you to use when needed

- Both Android and iOS

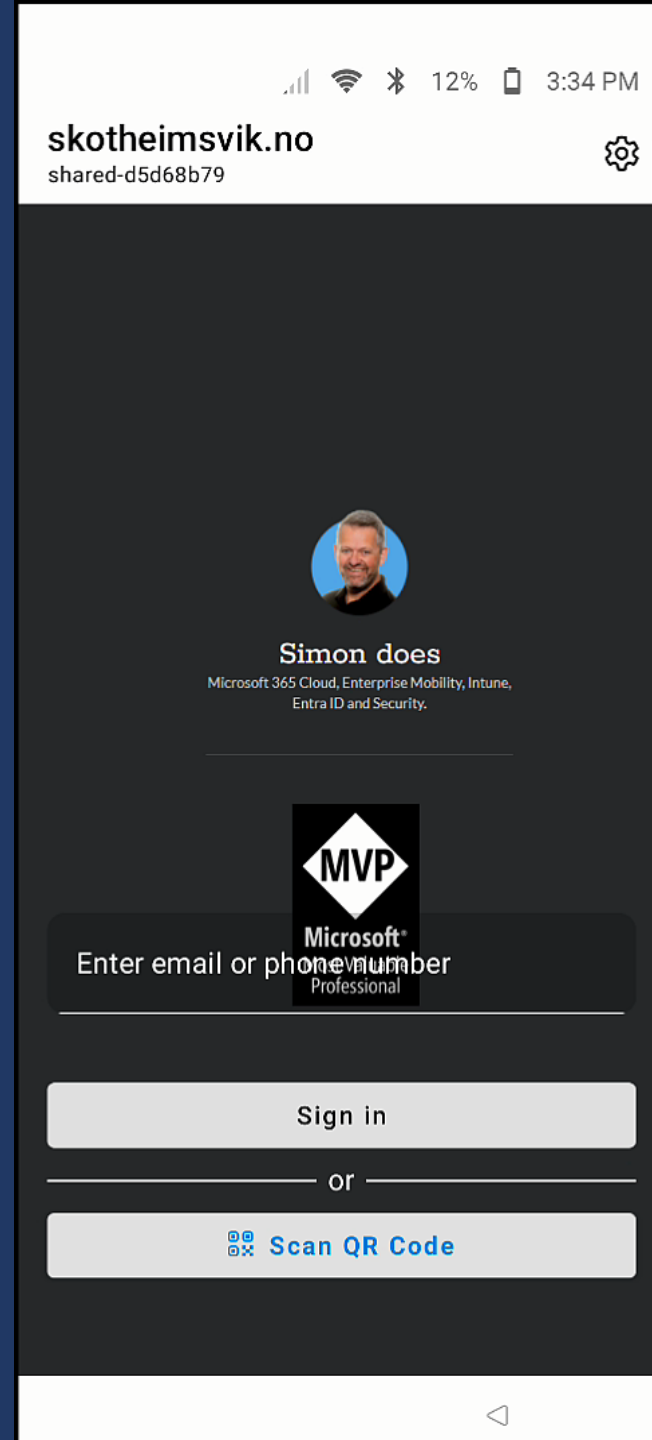
Shared Device

We have shared devices for you to use when needed

- Both Android and iOS
- Example: Android with Managed Home Screen

Email or Phone Number?

- Email and Password
 - A lot of typing
 - Big chance of typing wrong
 - Time-consuming
- Phone Number?
 - Need to bring your phone
 - Private?

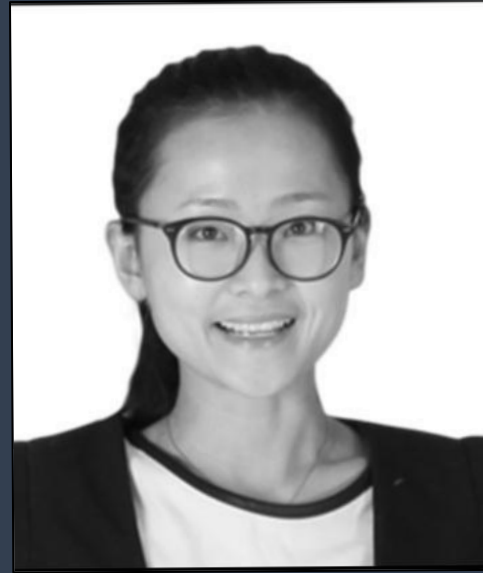


Shared Device

- Sign in with your employee card

Already used for other aspects:

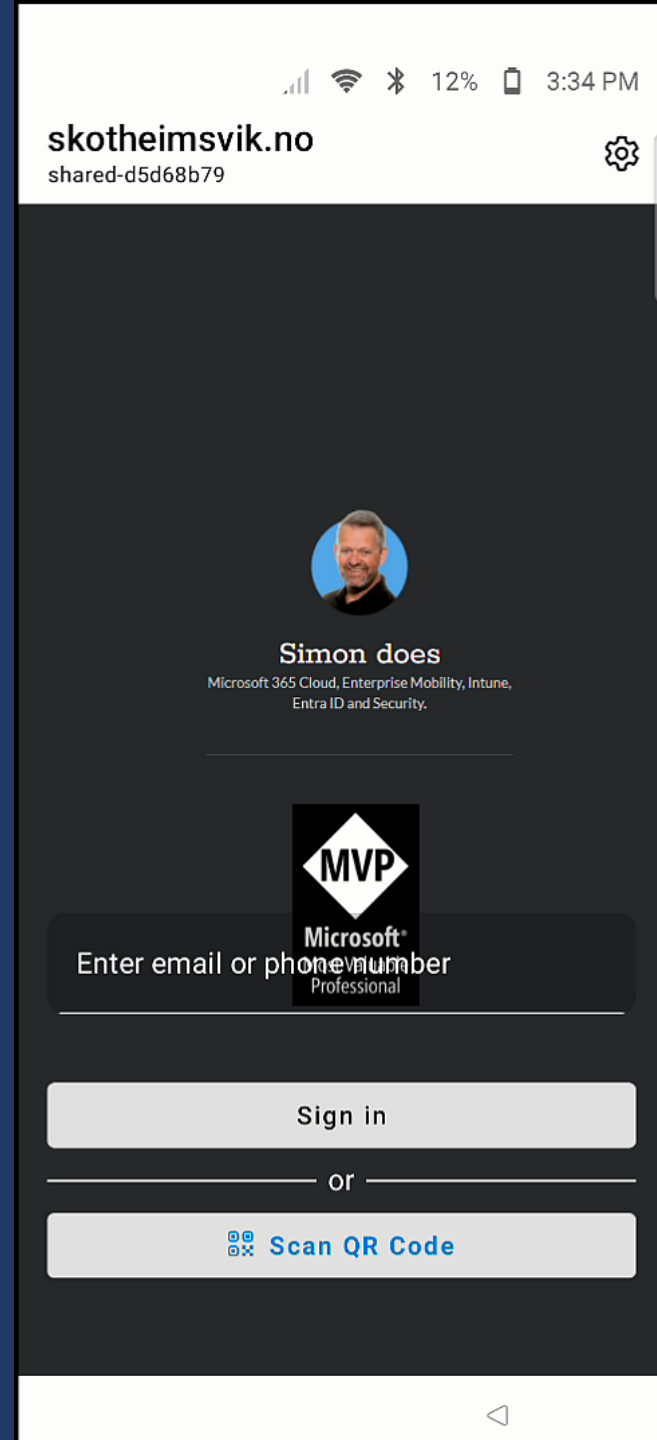
- Access to the buildings
- Physical identity
- Canteen
- Etc.



Paige
Turner



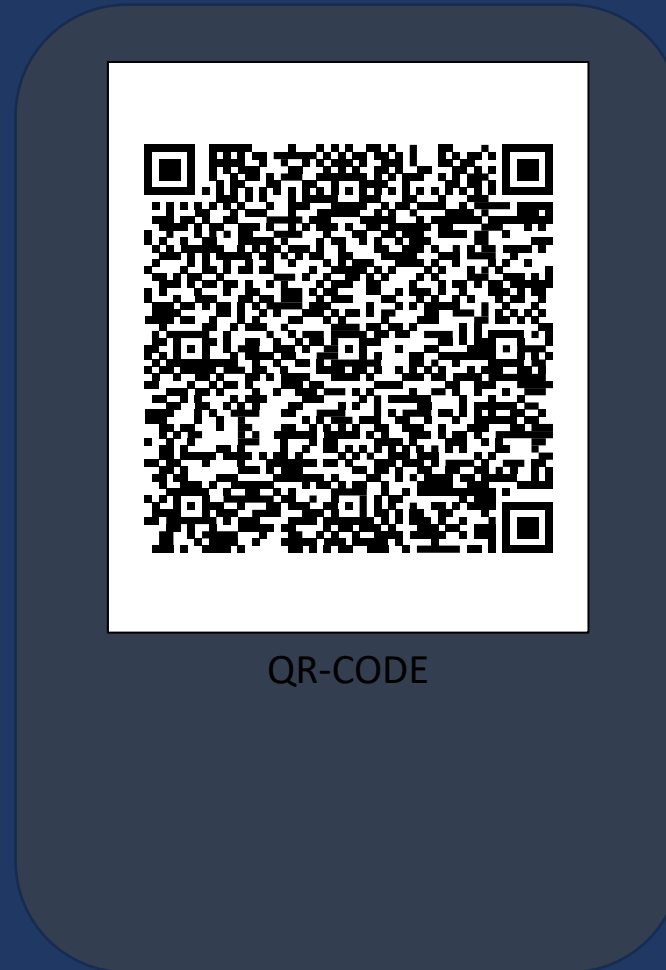
www.expertslive.co.uk



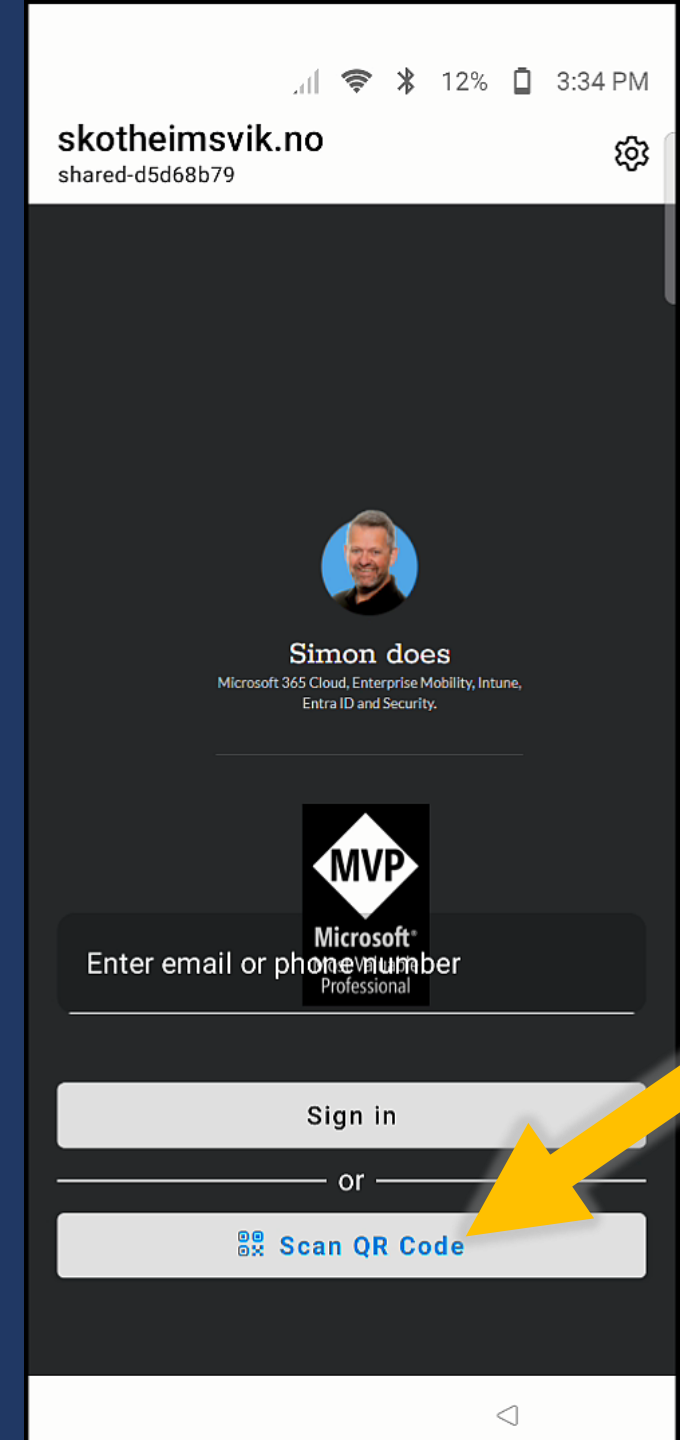
Shared Device

- Sign in with
the QR code on the back of
your employee card

Select “Scan QR Code” on the
shared device/phone



QR-CODE



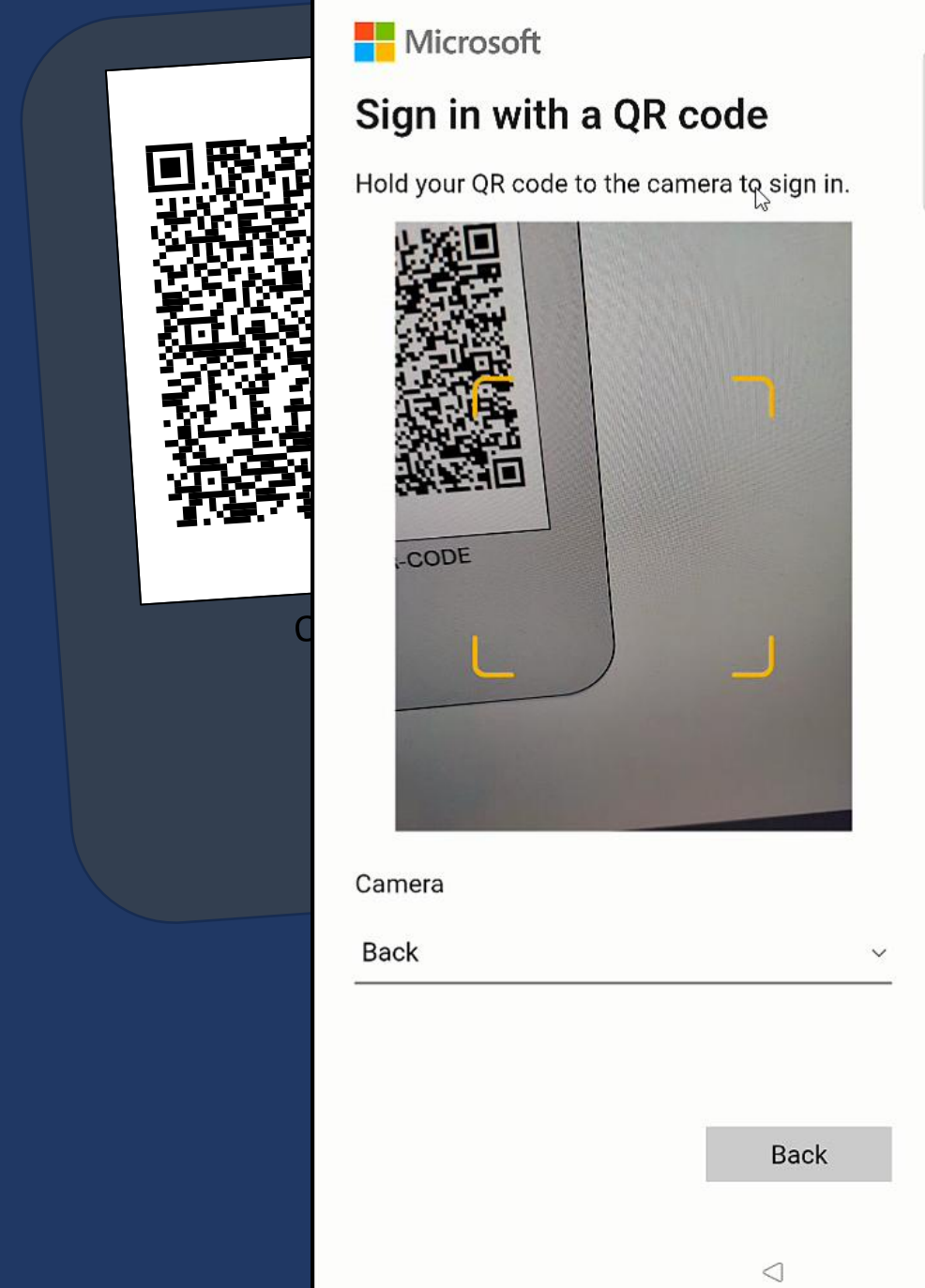
Shared Device

- Sign in with the QR code on the back of your employee card

Select "Scan QR Code" on the shared device/phone

Hold the QR code to the camera to sign in

(something you have)



Shared Device

- Sign in with
the QR code on the back of
your employee card

Select “Scan QR Code” on the
shared device/phone

Hold the QR code to the camera to
sign in

Type your personal PIN

(something you know)

• • Simon Does

← paige.turner@skotheimsvik.com

Enter your PIN

.....|

Forgot your PIN? Please contact your administrator.

Sign in

Sign-ins are monitored
 Caution:
Loose your credentials, and you might
have to write your apologies in binary!
Keep it safe, folks!

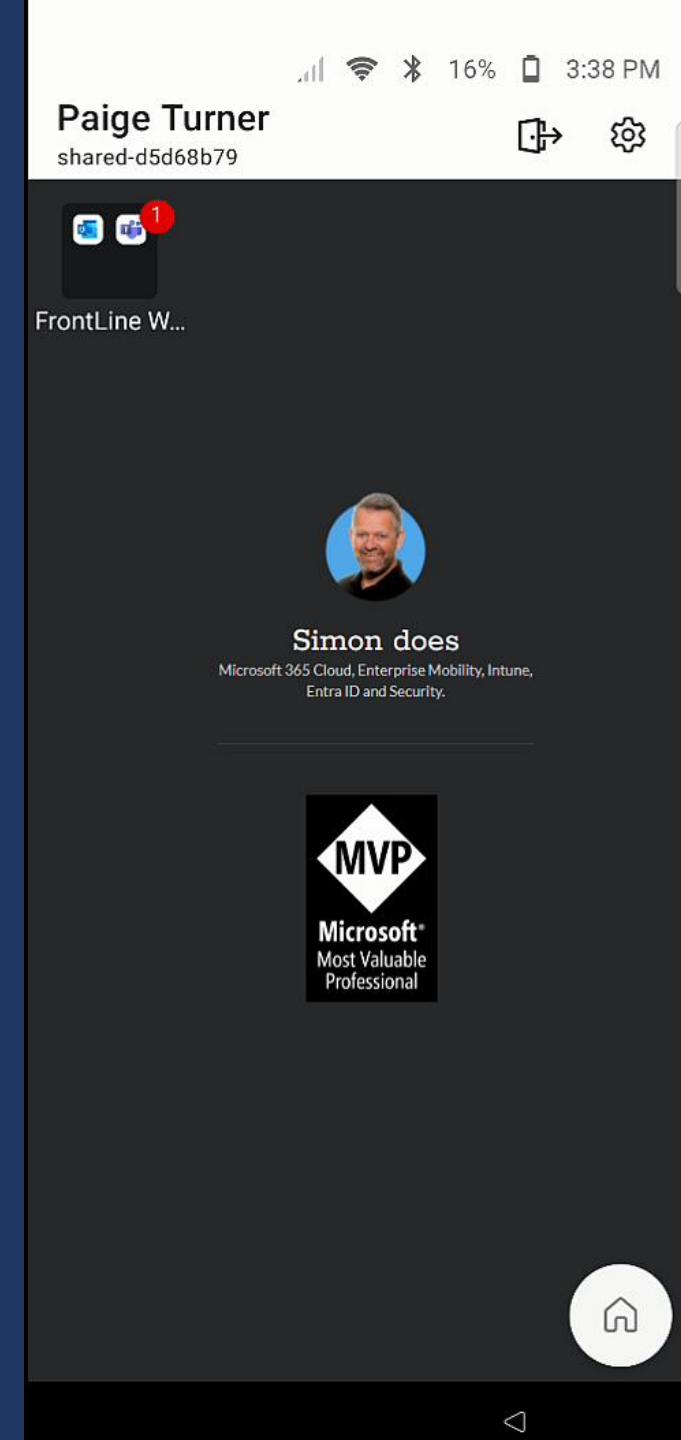
...

1	2 ABC	3 DEF	—
4 GHI	5 JKL	6 MNO	↵
7 PQRS	8 TUV	9 WXYZ	⌫
* #	0 +	.	→



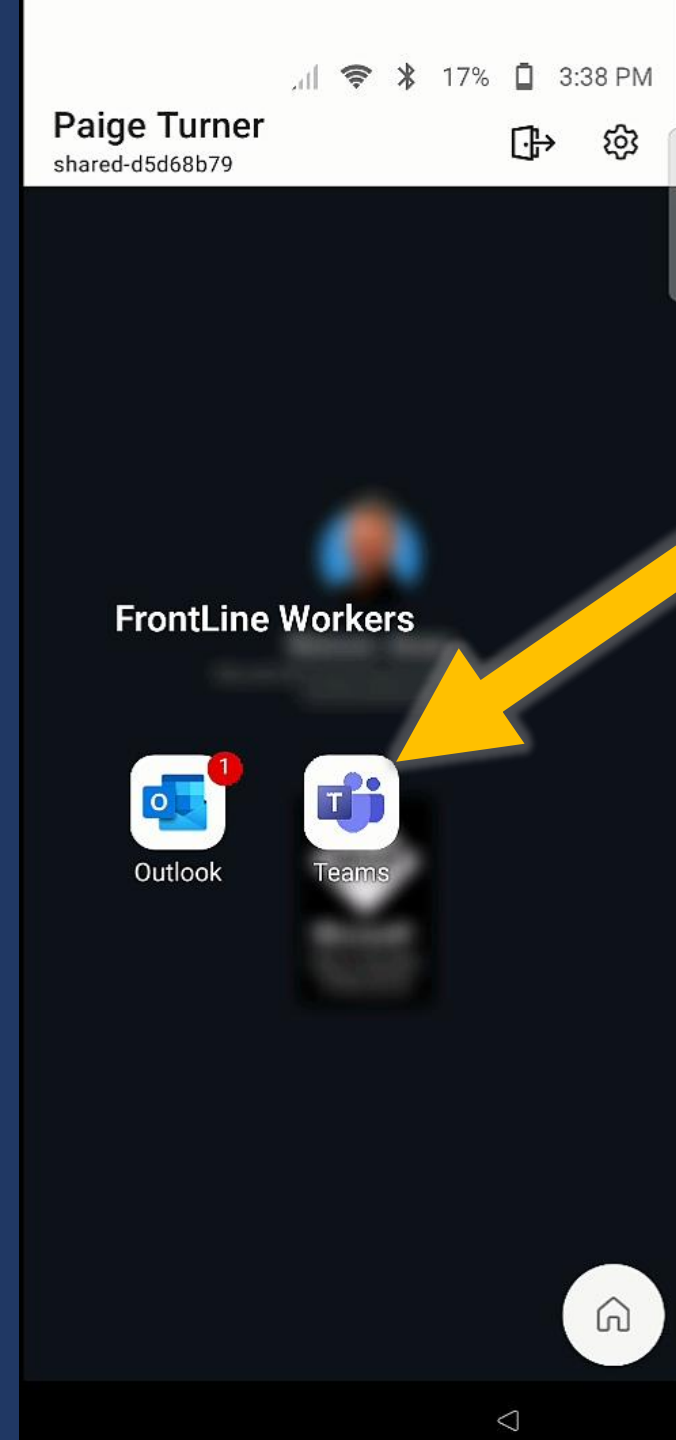
Shared Device

- You now have access to the company through Android Managed Home Screen
 - Branded
 - Structured
 - Uniform



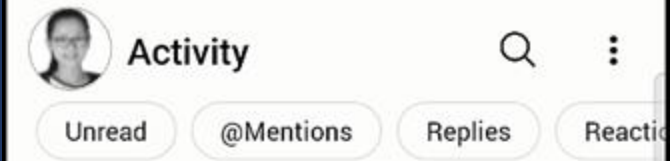
Shared Device

- Managed applications are available to the user
- Other things are hidden, making it easy for the Mobile First users.
- No permission requests, etc



Shared Device

- Single-Sign-On using the credentials from the QR-Code log in.



You'll find notifications here
Stay on top of relevant activity, such as mentions, likes, and replies.



Shared Dev

- Single-Sign-On using the credentials the QR-Code log in



JK



Activity



Unread

@Mentions

Replies

Reactions



You'll find notifications here

Stay on top of relevant activity, such as mentions, likes, and replies.



How Did You DO that?

The IT Manager wonders how this is possible!

How can I configure shared devices?





Intune - Shared Device Configuration

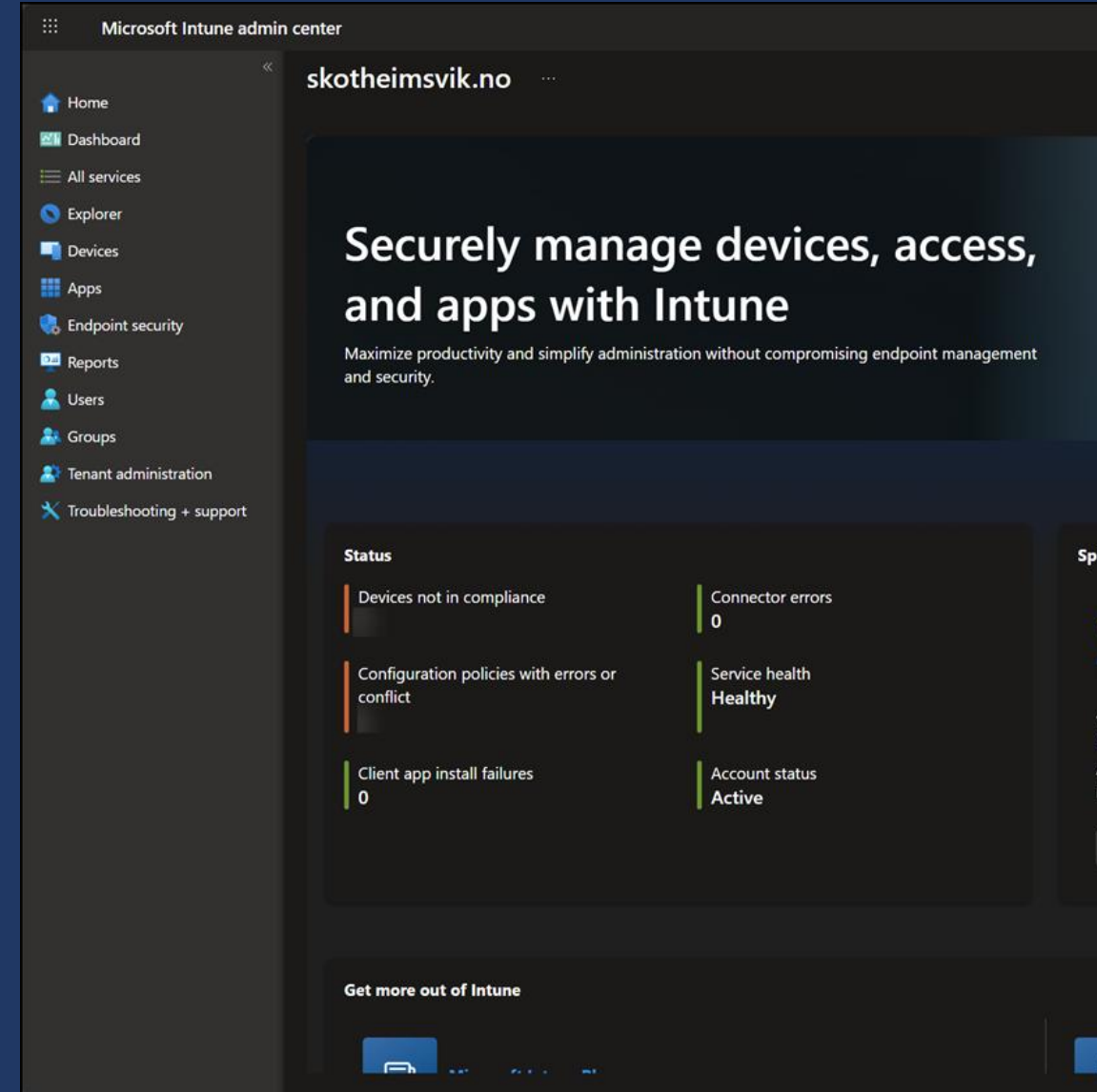
- Microsoft Intune Shared Device Mode

Shared device mode is a game-changer for operational efficiency and data protection in shift-based environments.

Shared device mode configures a mobile device (Android, iOS, iPadOS) so that:

- **Multiple users can sign in and out easily**
- **Apps support single sign-on (SSO)** across the device
- **User data is wiped upon sign-out**, prepping the device for the next shift

It's ideal for environments like retail, healthcare, manufacturing, and hospitality—where devices are passed between workers throughout the day.





Intune - Shared Device Configuration

- Microsoft Intune Shared Device Mode
- Enrollment Profile
- Android
- Corporate-owned dedicated devices

The screenshot displays the Microsoft Intune admin center. The left-hand navigation pane has the 'Devices' option highlighted with a yellow box. The main content area is titled 'Devices | Enrollment' and features tabs for 'Windows', 'Apple', and 'Android', with 'Android' being the active tab. Below the tabs, there is a search bar and a list of options: 'Overview', 'All devices', 'Device query', 'Monitor', 'By platform', and 'Device onboarding'. The 'Enrollment' option under 'Device onboarding' is highlighted with a yellow box. On the right side, the 'Android Enterprise' section is visible, containing 'Prerequisites' (Managed Google Play), 'Bulk enrollment methods' (Zero-touch enrollment), and 'Enrollment Profiles'. The 'Corporate-owned dedicated devices' profile is highlighted with a yellow box. The bottom of the screen shows a footer with the URL and the ExpertsLive UK logo.



Intune - Shared Device Configuration

- Microsoft Intune Shared Device Mode
- Enrollment Profile
- Android
- Corporate-owned dedicated devices

Microsoft Intune admin center

Home > Devices | Enrollment >

Corporate-owned dedicated devices

Android enrollment

Create an enrollment policy for Android Enterprise dedicated devices and send a token to who will be enrolling the device. [Learn more.](#)

+ Create policy Refresh Export Columns

Search

Policy state: Active Add filters

Name ↑	Token expiration date
Android FLW	01/02/2027, 12:00 AM



Intune - Shared Device Configuration

- Microsoft Intune Shared Device Mode
- Enrollment Profile
- Android
- Corporate-owned dedicated devices
- ...with Microsoft Entra shared mode and device name template

Microsoft Intune admin center

Home > Devices | Enrollment > Corporate-owned dedicated devices > Android FLW | Properties >

Edit profile

1 Basics 2 Review + save

Name * ⓘ Android FLW

Description Enrollment of Android for Frontline Workers

Token type ⓘ Corporate-owned dedicated device with Microsoft Entra shared mode

Token expiration date ⓘ 01/02/2027

Apply device name template ⓘ No Yes

Device name template * ⓘ shared-{{SERIAL}}

Review + save Cancel



Intune - Shared Device Configuration

- Microsoft Intune Shared Device Mode
- Enrollment Profile
- Android
- Corporate-owned dedicated devices
- ...with Microsoft Entra shared mode and device name template
- Token for onboarding
 - Alternatively, lock the device to the enrollment profile using OEM tools like Samsung Knox Mobile Enrollment (KME), Apple Business Manager (ABM), or other

Microsoft Intune admin center

Home > Devices | Enrollment > Corporate-owned dedicated devices > Android FLW

Android FLW | Token

Android enrollment

Search

Replace token Revoke token Export

Overview

Manage

Properties

Token

Android FLW

Use this token or QR code to enroll devices. [Learn more](#)

Token creation date
07/30/25, 3:30 PM

Token type
Corporate-owned dedicated device with Microsoft Entra shared mode

Token expiration date
01/02/27, 12:00 AM

Token

Token as QR code

Add or remove favorites by pressing Ctrl+Shift+F



Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune device configurations to tune and lock down the shared devices.

The screenshot shows the Microsoft Intune admin center interface. The left-hand navigation pane has the 'Devices' menu item highlighted with a yellow box. The main content area is titled 'Android | Configuration' and shows a list of configuration options. The 'Configuration' option is highlighted with a yellow box. On the right, the 'Policies' section is active, displaying a table of policies. The 'Android FLW Restrictions' policy is highlighted with a yellow box.

Policy name	Policy type	Last modified
Android FLW Restrictions	Device restrictions	7/31/2025, 9:17:13 AM



Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune device configurations to tune and lock down the shared devices.

- Kiosk mode, dedicated

Microsoft Intune admin center

Home > Devices | Overview > Android | Configuration > Android FLW Restrictions >

Device restrictions

Android Enterprise

Device experience

Device experience type [?] ¹ Kiosk mode (dedicated and fully managed) [▼]

Configure a kiosk-style experience on your dedicated devices. Prior to configuring these settings, go to Client apps and deploy any apps you want to the devices.

[Learn about Android Enterprise dedicated devices.](#)

Kiosk mode [?] Multi-app [▼]

i Multiple app kiosk mode – Locks the device to run multiple apps that are launched from the Managed Home Screen app. To use this mode, you must first approve and assign the Managed Home Screen app from the client apps workload.

Custom app layout [?] **Enable** Not configured

Grid size [?] 4 columns x 5 rows [▼]

Home Screen

FrontLine W...

Review + save Cancel



Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune device configurations to tune and lock down the shared devices.

- Kiosk mode, dedicated
- Multi-app

Microsoft Intune admin center

Home > Devices | Overview > Android | Configuration > Android FLW Restrictions >

Device restrictions

Android Enterprise

Device experience

Device experience type [?] ¹ Kiosk mode (dedicated and fully managed) [▼]

Configure a kiosk-style experience on your dedicated devices. Prior to configuring these settings, go to Client apps and deploy any apps you want to the devices.

[Learn about Android Enterprise dedicated devices.](#)

Kiosk mode [?] Multi-app [▼]

i Multiple app kiosk mode – Locks the device to run multiple apps that are launched from the Managed Home Screen app. To use this mode, you must first approve and assign the Managed Home Screen app from the client apps workload.

Custom app layout [?] **Enable** Not configured

Grid size [?] 4 columns x 5 rows [▼]

Home Screen

FrontLine W...

Review + save Cancel



Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune device configurations to tune and lock down the shared devices.

- Kiosk mode, dedicated
- Multi-app
- Custom MHS app layout

The screenshot displays the Microsoft Intune admin center interface. The left sidebar shows navigation options: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Device restrictions' and shows the configuration for 'Android Enterprise'. The 'Device experience type' is set to 'Kiosk mode (dedicated and fully managed)'. Below this, there is a section for 'Kiosk mode' set to 'Multi-app'. A blue information box states: 'Multiple app kiosk mode – Locks the device to run multiple apps that are launched from the Managed Home Screen app. To use this mode, you must first approve and assign the Managed Home Screen app from the client apps workload.' The 'Custom app layout' section is highlighted with a yellow box and shows a grid of 20 app icons arranged in 4 columns and 5 rows. The first icon in the top-left is labeled 'FrontLine W...'. The 'Grid size' is set to '4 columns x 5 rows'. At the bottom of the highlighted section, there are 'Review + save' and 'Cancel' buttons.

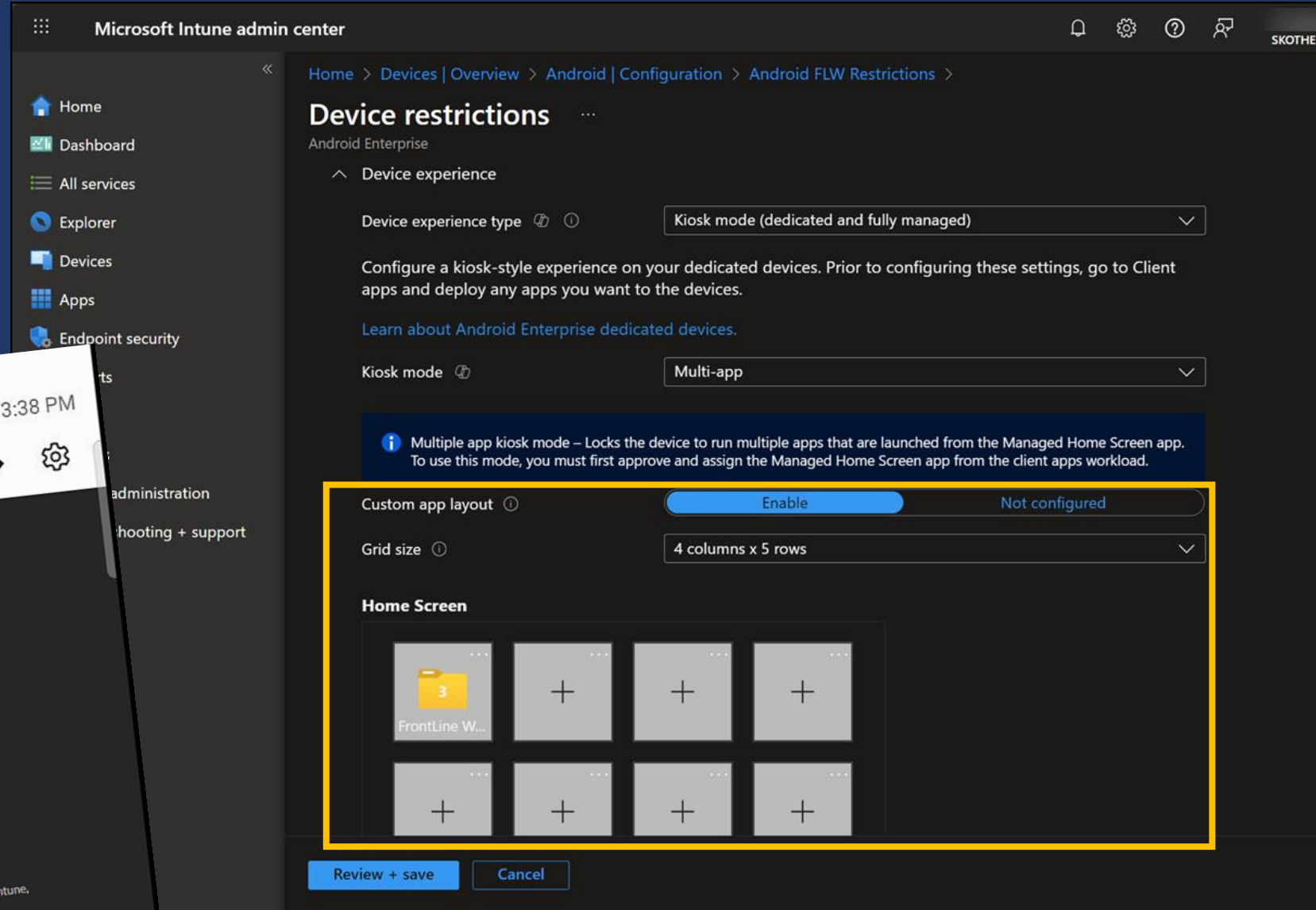
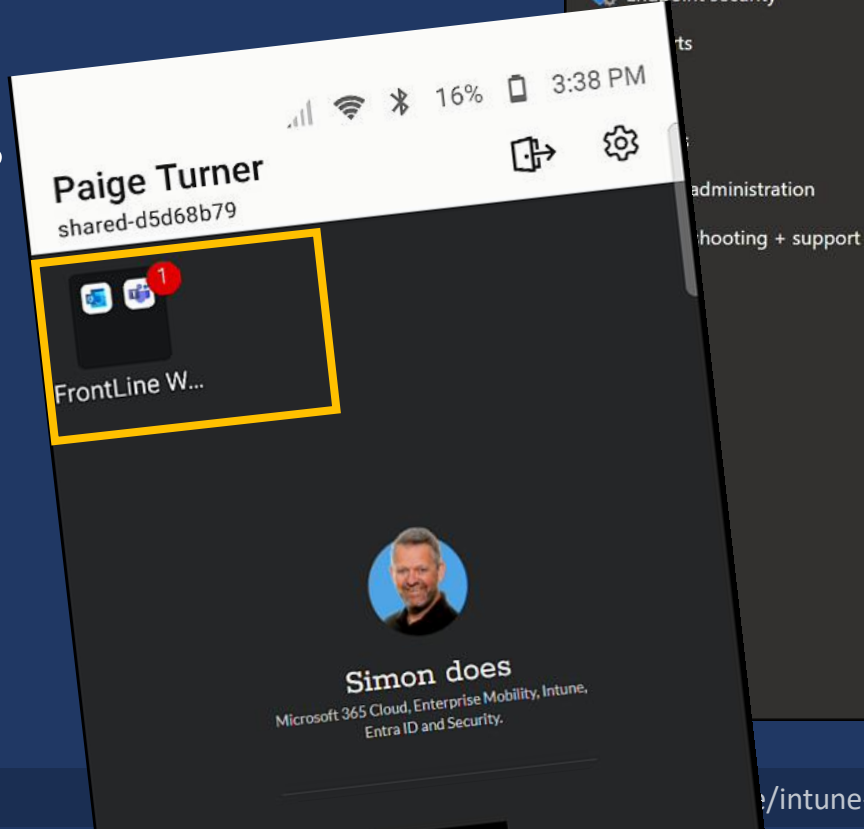


Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune device configurations to tune and lock down the shared devices.

- Kiosk mode, dedicated
- Multi-app
- Custom MHS





Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune device configurations to tune and lock down the shared devices.

- Kiosk mode, dedicated
- Multi-app
- Custom MHS app layout
- Customize MHS

Microsoft Intune admin center

Home > Devices | Overview > Android | Configuration > Android FLW Restrictions >

Device restrictions

Android Enterprise

Lock home screen ⓘ	Enable	Not configured
Folder icon ⓘ ⓘ	Dark theme rectangle	▼
App and folder icon size ⓘ ⓘ	Average	▼
Screen orientation ⓘ ⓘ	Not configured	▼
App notification badges ⓘ ⓘ	Enable	Not configured
Virtual home button ⓘ ⓘ	Floating	▼
Leave kiosk mode ⓘ ⓘ	Enable	Not configured
Leave kiosk mode code ⓘ ⓘ		
Set custom URL background ⓘ ⓘ	https://skotheimsvikintunefiles.blob.core.windows.net/intunepublicsour...	
Shortcut to settings menu ⓘ ⓘ	Disable	Not configured
Quick access to debug menu ⓘ ⓘ	Enable	Not configured
Wi-Fi configuration ⓘ ⓘ	Enable	Not configured
Wi-Fi allow-list ⓘ ⓘ		
SSID		

Import Export

Review + save Cancel

Intune - Share 15 duration, MHS

New remote actions to suspend and restore Managed Home Screen on Android devices

Intune has two new remote actions that allow admins to temporarily suspend and restore Managed Home Screen (MHS) on Android devices. These actions let users exit MHS and access the device's default launcher for a defined period, without removing policies or requiring a PIN.

When the specified duration expires, or when the *restore managed home screen* action is triggered, MHS automatically re-locks the device into the kiosk experience. This helps maintain security while reducing disruption during troubleshooting or short-term use outside of MHS.

To learn more, see:

- [Suspend Managed Home Screen](#)
- [Restore Managed Home Screen](#)

How to suspend the managed home screen from the Intune admin center

1. In the [Microsoft Intune admin center](#), select [Devices](#) > [All devices](#).
2. From the devices list, select a device.
3. At the top of the device overview pane, find the row of action icons. Select **Suspend Managed Home Screen**.

User experience

Once the Managed Home Screen is suspended, the device will no longer enforce the Managed Home Screen policies, and the user will have access to the standard home screen and apps.

Configuration page for a device in the Intune admin center. The 'Leave kiosk mode code' field is highlighted with a yellow box. Below it are settings for 'Set custom URL background', 'Shortcut to settings menu', 'Quick access to debug menu', and 'Wi-Fi configuration'. At the bottom are 'Review + save' and 'Cancel' buttons.

Setting	Value
Floating	Floating
Enable	Enable
Not configured	Not configured
Leave kiosk mode code	[Redacted]
Set custom URL background	https://skotheimsvikintunefiles.blob.core.windows.net/intunepublicresour...
Shortcut to settings menu	Disable
Quick access to debug menu	Enable
Wi-Fi configuration	Enable
Wi-Fi allow-list	Import
SSID	Export

Week of April 27, 2026
(Service release 2604)



Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune **app configurations** for even more options to tune and lock down the shared devices.

Microsoft Intune admin center

Home > Apps

Apps | Configuration

Search

Create Refresh Export Columns

Search

Platform: Android Add filter

Name ↑	Management type ⓘ
AMAP001 - FLW - QR Code Authentication - Microsoft Authenticat...	Managed devices
AMAP002 - FLW - Managed Home Screen	Managed devices

Configuration

Protection

iOS app provisioning profiles

S mode supplemental policies

Policies for Microsoft 365 apps

App selective wipe

Quiet time

Add or remove favorites by pressing Ctrl+Shift+F



Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune app configurations for even more options to tune and lock down the shared devices.

- Add configuration keys and values as seen in the Microsoft doc

- Show OS options in MHS
- Show user and device info

Microsoft Intune admin center

Home > Apps | Configuration > AMAP002 - FLW - Managed Home Screen

AMAP002 - FLW - Managed Home Screen | Properties

Search

Overview

Manage

Properties

Monitor

Device install status

Name: AMAP002 - FLW - Managed Home Screen

Description: Detailed configuration for the Managed Home Screen

Device enrollment type: Managed devices

Platform: Android Enterprise

Profile Type: Fully Managed, Dedicated, and Corporate-Owned Work

Targeted app: Managed Home Screen

Settings Edit

Permissions: Not configured

Configuration key	Value type	Configuration value
Show the brightness slider	bool	true
Show adaptive brightness toggle	bool	true
Top Bar User Name Style	choice	First Name, Last Name
Top Bar Secondary Element	choice	Device Name
Top Bar Primary Element	choice	Tenant Name
Battery and Signal Strength indicator bar	bool	true

Connected apps: Not configured

Add or remove favorites by pressing Ctrl+Shift+F



Intune - Shared Device Configuration, MHS

- Microsoft Intune Shared Device Mode

Use Intune app configurations for even more options to tune and lock down the shared devices.

- Add configuration keys and values as seen in the Microsoft doc
 - Show OS options in MHS
 - Show user and device info

Microsoft Intune admin center

Home > Apps | Configuration > AMAP002 - FLW - Managed Home Screen

AMAP002 - FLW - Managed Home Screen | Properties

Search

Overview

Name: AMAP002 - FLW - Managed Home Screen

Description: Detailed configuration for the Managed Home Screen

Device enrollment type: Managed devices

Platform: Android Enterprise

Profile Type: Fully Managed, Dedicated, and Corporate-Owned Work

Targeted app: Managed Home Screen

Settings Edit

Permissions: Not configured

Configuration key	Value type	Configuration value
Show the brightness slider	bool	true
Show adaptive brightness toggle	bool	true
Top Bar User Name Style	choice	First Name, Last Name
Top Bar Secondary Element	choice	Device Name
Top Bar Primary Element	choice	Tenant Name
Battery and Signal Strength indicator bar	bool	true

Connected apps: Not configured

Pressing Ctrl+Shift+F

skotheimsvik.no
shared-d5d68b79

Simon does
Microsoft 365 Cloud, Enterprise Mobility, Intune, Entra ID and Security.

MVP

ExpertsLiveUK

<https://learn.microsoft.com/en-us/intune/configuration-managed-home-screen-app>



Intune - Shared Device Configuration, QR for MHS

- Microsoft Intune Shared Device Mode

Use **Intune app configurations** to configure Microsoft Authenticator for **QR Code Authentication**

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains a navigation menu with the following items: Home, Dashboard, All services, Explorer, Devices, **Apps** (highlighted), Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Apps | Configuration' and includes a search bar, a 'Create' button, and a 'Refresh' button. Below these, there is a table of app configurations. The table has two columns: 'Name' and 'Management type'. The first row is highlighted and contains the text 'AMAP001 - FLW - QR Code Authentication - Microsoft Authenticat...' and 'Managed devices'. The second row contains 'AMAP002 - FLW - Managed Home Screen' and 'Managed devices'. The bottom of the screen shows a footer with the text 'Add or remove favorites by pressing Ctrl+Shift+F'.



Intune - Shared Device Configuration, QR for MHS

- Microsoft Intune Shared Device Mode

Use Intune app configurations to configure Microsoft Authenticator for QR Code Authentication

- Add configuration keys and values as seen in the Microsoft doc

- Support QR Sign In
- Suppress Camera Consent

Microsoft Intune admin center

Home > Apps | Configuration > AMAP001 - FLW - QR Code Authentication - Microsoft Authenticator

AMAP001 - FLW - QR Code Authentication - Microsoft Authenticator | Properties

Search

Overview

Manage

Properties

Monitor

Device install status

Basics Edit

Name: AMAP001 - FLW - QR Code Authentication - Microsoft Authenticator

Description: <https://learn.microsoft.com/en-us/entra/identity/authentication-qrcode#sign-in-to-microsoft-teams-or-managed-home-screen-mhs-with-qr-code>

Device enrollment type: Managed devices

Platform: Android Enterprise

Profile Type: Fully Managed, Dedicated, and Corporate-Owned Work

Targeted app: Microsoft Authenticator

Settings Edit

Permissions: Not configured

Configuration key	Value type	Configuration value
Suppress camera consent for QR code + PIN-based authentication.	bool	true
Preferred authentication configuration	string	qrpin

Connected apps: Not configured

Assignments Edit

Add or remove favorites by pressing Ctrl+Shift+F

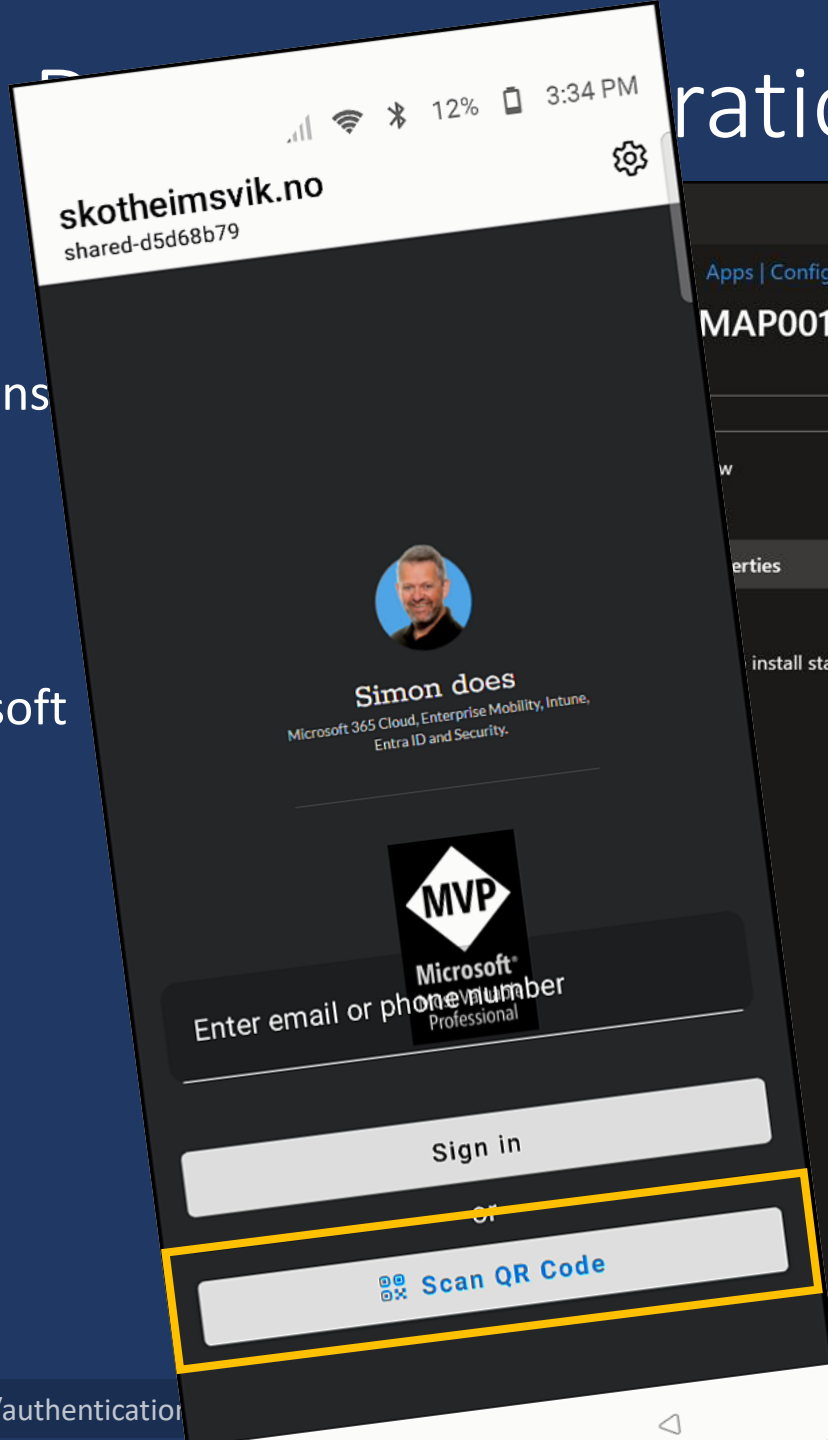


Intune - Shared Device Configuration, QR for MHS

- Microsoft Intune Shared Device Mode

Use Intune app configurations to configure Microsoft Authenticator for QR Code Authentication

- Add configuration keys and values as seen in the Microsoft doc
 - Support QR Sign In
 - Suppress Camera Consent



Apps | Configuration > AMAP001 - FLW - QR Code Authentication - Microsoft Authenticator

AMAP001 - FLW - QR Code Authentication - Microsoft Authenticator | Pro

Basics Edit

Name AMAP001 - FLW - QR Code Authentication - Microsoft A

Description <https://learn.microsoft.com/en-us/entra/identity/authen authentication-qr-code#sign-in-to-microsoft-teams-or-screen-mhs-with-qr-code>

Device enrollment type Managed devices

Platform Android Enterprise

Profile Type Fully Managed, Dedicated, and Corporate-Owned Work

Targeted app Microsoft Authenticator

Settings Edit

Permissions Not configured

Configuration Settings

Configuration key	Value type	Configu
Suppress camera consent for QR code + PIN-based authentication.	bool	true
Preferred authentication configuration	string	qrpin

Connected apps Not configured

Assignments Edit



Intune - Shared Device Configuration, Apps

- Microsoft Intune Shared Device Mode

Use Intune to assign managed applications to the shared devices.

- Managed Google Play Store adds Android apps to Intune.

- Managed Home Screen
- Microsoft Authenticator
- Microsoft Intune
- Microsoft Teams
- ...

Microsoft Intune admin center

Home > Apps | Overview >

Android | Android apps

Search

Android apps

Monitor

Manage apps

- Configuration
- Protection
- App selective wipe
- Quiet time

Organize apps

- Assignment filters
- App categories

Create Refresh Export Columns

Search

Platform: Android Type: Android Enterprise system app, Android line-of-busine...

Add filters

Name ↑	Platform	Type
Managed Home Screen	Android	Managed Google Play store ap
Microsoft Authenticator	Android	Managed Google Play store ap
Microsoft Intune	Android	Managed Google Play store ap
Microsoft Outlook	Android	Managed Google Play store ap
Microsoft Teams	Android	Managed Google Play store ap

Add or remove favorites by pressing Ctrl+Shift+F

Intune - Shared Device Configuration, Assignments



- Microsoft Intune Shared Device Mode

Assignments using Intune native technology to ensure speed.

- Virtual group “All Devices”
- Assignment filters

Microsoft Intune admin center

Home > Apps | Overview > Android | Android apps > Managed Home Screen

Managed Home Screen | Properties

Client Apps

Search

Overview

Manage

Properties

Monitor

- Device install status
- User install status

App information Edit

Name	Managed Home Screen
Description	A Microsoft Intune managed, multi App Kiosk mode launcher
Publisher	Microsoft Corporation
Appstore URL	https://play.google.com/store/apps/details?id=com.microsoft.launcher.enterprise&hl=nb-NO
Logo	

Available licenses: 0

Total licenses: 0

Assignments Edit

Group mode	Group	Filter mode	Filter
Required			
Included	All devices	Include	AFLT001 - Android FLW

Available for enrolled devices

Available with or without enrollment

Intune - Shared Device Configuration, Assignments



- Microsoft Intune Shared Device Mode

Assignments using Intune native technology to ensure speed.

- Virtual group “All Devices”
- Assignment filters

Microsoft Intune admin center

Home > Devices

Devices | Assignment filters

Search

+ Create Refresh Export Columns

Overview

All devices

Device query

Monitor

> By platform

> Device onboarding

> Manage devices

> Manage updates

> Organize devices

Device clean-up rules

Assignment filters

> Help and support

Search

Platform: Android Enterprise

Filter name ↑	Platform	Filter type
AFLT001 - Android FLW	Android Enterprise	Managed devices

Add or remove favorites by pressing Ctrl+Shift+F

Intune - Shared Device Configuration, Assignments



- Microsoft Intune Shared Device Mode

Assignments using Intune native technology to ensure speed.

- Virtual group “All Devices”
- Assignment filters

The screenshot displays the Microsoft Intune admin center interface. The left-hand navigation pane includes links to Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'AFLT001 - Android FLW' and features two tabs: 'Properties' (which is highlighted with a yellow box) and 'Associated assignments'. Under the 'Properties' tab, there are sections for 'Summary', 'Basics' (with an 'Edit' link), and 'Rules' (with an 'Edit' link). The 'Basics' section shows the filter name as 'AFLT001 - Android FLW', the description as 'Android Frontline Workers devices', and the platform as 'Android Enterprise'. The 'Rules' section contains a 'Rule syntax' field, also highlighted with a yellow box, which contains the expression '(device.deviceName -startsWith "shared-")'.

Intune - Shared Device Configuration, Assignments



- Microsoft Intune Shared Device Mode

Assignments using Intune technology to ensure sp

- Virtual group “All Device
- Assignment filters

Microsoft Intune admin center

Home > Devices | Overview > Android | Assignment filters > AFLT001 - Android FLW

Edit AFLT001 - Android FLW

1 Rules 2 Review + save

You can use the rule builder or rule syntax text box to create or edit the filter rule. [Learn more about creating filters](#)

And/Or	Property	Operator	Value
	enrollmentProf...	Equals	Android FLW

+ Add expression

Rule syntax Edit

(device.enrollmentProfileName -eq "Android FLW")

Filter preview

You can see the devices that match the filter rules.

Preview

Preview devices

Refresh Columns

Search

Device name ↓

shared-d5d68b79

Intune - Shared Device Configuration, Assignments



- Microsoft Intune Shared Device Mode

Assignments using Intune native technology to ensure speed.

- Virtual group “All Devices”
- Assignment filters

Microsoft Intune admin center

Home > Devices | Assignment filters >

AFLT001 - Android FLW

Properties **Associated assignments**

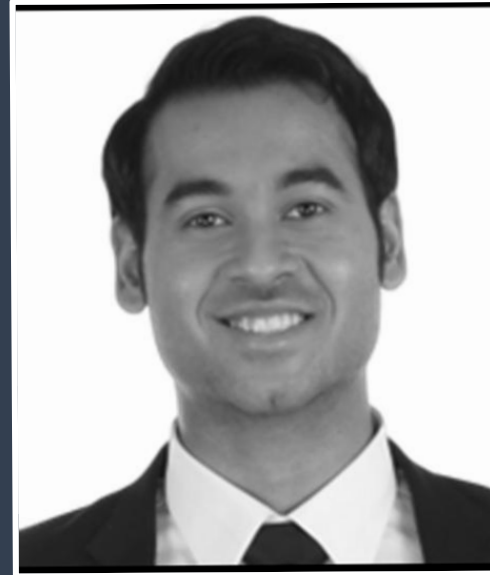
See the policy, profile and application assignments that use this filter. [Learn more](#)

Name	Resource type	Group	Filter mode
AMAP002 - FLW - Managed Home Screen	App Configuration (Android)	All devices	Include
AMAP001 - FLW - QR Code Authentication - Microsoft Aut...	App Configuration (Android)	All devices	Include
Managed Home Screen	Managed Google Play store app	All devices	Include
Microsoft Teams	Managed Google Play store app	All devices	Include
Android FLW Restrictions	Device restrictions	All devices	Include
ACOP001 - FLW - Device Health - Rooted Device	Fully managed, dedicated, and corporate-ow...	All devices	Include
Microsoft Outlook	Managed Google Play store app	All devices	Include
Microsoft Authenticator	Managed Google Play store app	All devices	Include
Microsoft Intune	Managed Google Play store app	All devices	Include

Whats in it for me?

The Team Manager wonders how we get the most out of all users in Teams

How can I communicate most effectively?



Justin
Time



Ståle Hansen



Nikki Chapple

Copilot

Content isn't available after the meeting
You won't have access to Copilot or any content it generates once the meeting ends.

Let AI handle the busywork
Copilot can generate notes, list tasks, and much more-so you don't have to.

Check the facts
A response could be inaccurate or incomplete. Share feedback to help Copilot improve.

It's your Copilot
Other people in the meeting can't see this conversation.

Ask me anything about this meeting

More prompts

Weekly sales meeting



View



Notes



Rooms



Copilot



Apps



Copilot



Content isn't available after the meeting
You won't have access to Copilot or any content it generates once the meeting ends.



Let AI handle the busywork

Copilot can generate notes, list tasks, and much more-so you don't have to.



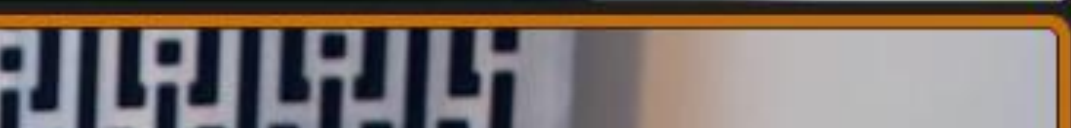
Check the facts

A response could be inaccurate or incomplete. Share feedback to help Copilot improve.



It's your Copilot

Other people in the meeting can't see this conversation.





Ståle Hansen



Nikki Chapple

Copilot

Content isn't available after the meeting
You won't have access to Copilot or any content it generates once the meeting ends.

Let AI handle the busywork
Copilot can generate notes, list tasks, and much more-so you don't have to.

Check the facts
A response could be inaccurate or incomplete. Share feedback to help Copilot improve.

It's your Copilot
Other people in the meeting can't see this conversation.

Ask me anything about this meeting

More prompts



Ståle Hansen



Nikki Chapple

Copilot

Content isn't available after the meeting
You won't have access to Copilot or any content it generates once the meeting ends.

- Let AI handle the busywork**
Copilot can generate notes, list tasks, and much more-so you don't have to.
- Check the facts**
A response could be inaccurate or incomplete. Share feedback to help Copilot improve.
- It's your Copilot**
Other people in the meeting can't see this conversation.

Prompt suggestions

- Recap meeting so far
- List action items
- Suggest follow-up questions
- What questions are unresolved?
- List different perspectives by topic
- List main ideas we discussed
- Generate meeting notes

Prompt suggestions

Recap meeting so far

List action items

Suggest follow-up questions

What questions are unresolved?

List different perspectives by topic

List main ideas we discussed

Generate meeting notes



More prompts





Ståle Hansen



Nikki Chapple

Copilot

Content isn't available after the meeting
You won't have access to Copilot or any content it generates once the meeting ends.

Let AI handle the busywork
Copilot can generate notes, list tasks, and much more-so you don't have to.

Check the facts
A response could be inaccurate or incomplete. Share feedback to help Copilot improve.

It's your Copilot
Other people in the meeting can't see this conversation.

Generate meeting notes

Generating a response

Ask me anything about this meeting

More prompts



Ståle Hansen



Nikki Chapple

Copilot

Content isn't available after the meeting
You won't have access to Copilot or any content it generates once the meeting ends.

Key Topics:

- **Marketing activities:** Nikki reported on the email campaigns and the clickthrough rates, and planned to improve the low-performing ones and use social media platforms, especially LinkedIn. ¹
- **Webinars:** Ståle reminded the team to check the registration list and encourage their customers to join the webinars, which will inform about important news and new routines. ²
- **Year end and pipeline:** Ståle urged the team to update their leads, projects and pipeline, and identify the high value targets, to prepare for the budget and the marketing activities for the next year. ³

Recap meeting so far

List action items

Ask me anything about this meeting

More prompts



Key Topics:

- **Marketing activities:** Nikki reported on the email campaigns and the clickthrough rates, and planned to improve the low-performing ones and use social media platforms, especially LinkedIn. [1](#)
- **Webinars:** Ståle reminded the team to check the registration list and encourage their customers to join the webinars, which will inform about important news and new routines. [2](#)
- **Year end and pipeline:** Ståle urged the team to update their leads, projects and pipeline, and identify the high value targets, to prepare for the budget and the marketing activities for the next year. [3](#)

Recap meeting so far

List action items



Action Items:

Marketing activities:

- Analyze the click through rates of the email campaigns and adjust the tactics for the next wave. (Nikki) 1
- Check the registration list for the webinars and follow up with the customers to ensure their attendance. (All team members) 2

Sales pipeline:

- Update the pipeline with the current status of the leads and projects and identify the high value targets. (All team members) 3

Fundraising success:

- Share the positive news of fund X with the team and target potential

Recap meeting so far

List action items

NEW

Activity

Copilot

Chat

Teams

Calendar

Calls

Tasks by Pla...

OneDrive

Topics

Intranet

Viva Engage

...

Apps

0 - Announcements

Posts

Files

Porteføljeplan for hav

Ståle Hansen

13:44

Minutes from this weeks status meeting

Thank you everyone for a good meeting today, here are the minutes from the meeting

Key Topics:

• **Marketing activities:** Nikki reported on the email campaigns and the clickthrough rates, and planned to improve the low-performing ones and use social media platforms, especially LinkedIn. 1

• **Webinars:** Ståle reminded the team to check the registration list and encourage their customers to join the webinars, which will inform about important news and new routines. 2

• **Year end and pipeline:** Ståle urged the team to update their leads, projects and pipeline, and identify the high value targets, to prepare for the budget and the marketing activities for the next year. 3

• **Fundraising success:** Nikki announced that they have raised 500,000 for fund X, and asked the team to share the positive news and keep up the momentum, and to analyze the key success criteria that made people invest. 4

• **Sales pitch guidelines:** Ståle informed the team about the new templates and the new guidelines for the sales pitch, and emphasized the importance of using them and not the old ones. 5

Action Items:

Marketing activities:

• Analyze the click through rates of the email campaigns and adjust the tactics for the next wave. (Ståle) 1

• Check the registration list for the webinars and follow up with the customers to

Start a post



Action Items:

Marketing activities:

- Analyze the click through rates of the email campaigns and adjust the tactics for the next wave. (Ståle) 1
- Check the registration list for the webinars and follow up with the customers to ensure their attendance. (All team members) 2

Sales pipeline:

- Update the pipeline with the current status of the leads and projects and identify the high value targets. (All team members) 3

Fundraising success:

- Share the positive news of fund X with the team and target potential investors with the key reasons to invest. (Nikki) 4

Meeting summary:

- Use the new templates for the offers and follow the sales pitch guidelines. (All team members) 5

[see less](#)



Loved the flow in the meeting. I got inspired and I have already done my activities, asked our colleague if it could be done, which it can and I have updated our tasks in Planner 👍



Action Items:

Marketing activities:

- Analyze the click through rates of the email campaigns and adjust the tactics for the next wave. (Ståle) 1
- Check the registration list for the webinars and follow up with the customers to ensure their attendance. (All team members) 2

Sales pipeline:

- Update the pipeline with the current status of the leads and projects and identify the high value targets. (All team members) 3

Fundraising success:

- Share the positive news of fund X with the team and target potential investors with the key reasons to invest. (Nikki) 4

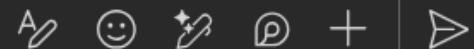
Meeting summary:

- Use the new templates for the offers and follow the sales pitch guidelines. (All team members) 5

[see less](#)



Loved the flow in the meeting. I got inspired and I have already done my activities, asked our colluegue if it could be done, which it can and I have updated our tasks in Planner 👍



Action Items:

Marketing activities:

- Analyze the click through rates of the email campaigns and adjust the tactics for the next wave. (Ståle) 1
- Check the registration list for the webinars and follow up with the customers to ensure their attendance. (All team members) 2

Sales pipeline:

- Update the pipeline with the current status of the leads and projects and identify the high value targets. (All team members) 3

Fundraising success:

- Share the positive news of fund X with the team and target potential investors with the key reasons to invest. (Nikki) 4

Meeting summary:

- Use the new templates for the offers and follow the sales pitch guidelines. (All team members) 5

[see less](#)



Loved the flow in the meeting. I got inspired and I have already done my activities, asked our colluegue if it could be done, which it can and I have updated our tasks in Planner 👍



How to survive a large Team?

▼  Project X

General

0 - Announcements

1 - Business Case

2 - Deployment

3 - Adoption

4 - Operations

5 - Change Management

6 - Endpoint Managemet

IT 

See all channels

...

Hide all channels

Add member

Add channel

Manage team

Manage tags

Copy link

Archive

Leave team

Delete team

Create a new tag

Tag name *

Copilot Experts

Tag description

Use this tag to mention Copilot Experts

Enter name of a member *

Enter name



Merethe Stave

merethe.stave@cloudway.com



Ståle Hansen

stale.hansen@cloudway.com



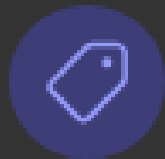
Cancel

Create

see more



Suggestions



Technical Experts
1 person



Share someone's contact info



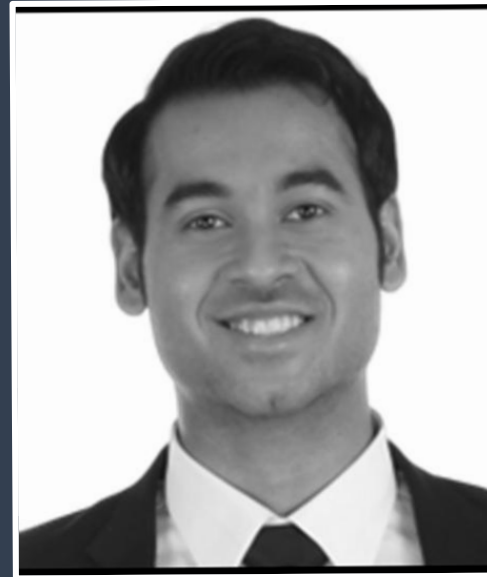
@tech

have already

Whats in it for me?

The Team Manager wonders
how we get the most out of all
users in Teams

How can I get on top of status?



Justin
Time



 **New chat**

 Search

 Library

 Create

Agents

 Researcher

 Analyst

 PowerPoint

 Cowork (Frontier)

 New agent

... All agents

 Apps

1

 Ståle Hansen



Work

Web

Auto



Hi, what can I help you with?

Message Copilot



Files

Emails

People

Meetings



Copilot Prompt Gallery

Search for prompts

Suggested

Your prompts

Team prompts

Created by



Task



Job type



Copilot agent



Speaker and Community

for this conversation please look at the past 30 days in the channel Speaking and Community , no...



You created this



Please roast my week as a...

Please summarize my week in the style of a comedy roast



You created this





New chat

Search

Library

Create

Agents

Researcher

Analyst

PowerPoint

Cowork (Frontier)

New agent

All agents

Apps

1

Ståle Hansen

...

Work

Web

Auto



for this conversation please look at the past 30 days in the channel / , no other channels, look at the threads, are there any events that are not published yet, are there any upcoming events where call for speakers are still open? Give me an executive summary at the end



All

People

Files

Meetings

Channels

4 More

search speak



Speaking and Community
CloudWay



New chat

Search

Library

Create

Agents

Researcher

Analyst

PowerPoint

Cowork (Frontier)

New agent

All agents

Apps

1

Ståle Hansen

...

Today

Work

Web

Auto



for this conversation please look at the past 30 days in the channel [Speaking and Community](#), no other channels, look at the threads, are there any events that are not published yet, are there any upcoming events where call for speakers are still open? Give me an executive summary at the end

Copilot

Lining things up...



Message Copilot



AI-generated content may be incorrect





Upcoming Events and Speaker Calls Summary

Work

Web



Auto



New chat

Search

Library

Create

Agents

Researcher

Analyst

PowerPoint

Cowork (Frontier)

New agent

All agents

Apps

1

Ståle Hansen



1. Events Mentioned but Not Yet Published (or explicitly stated as missing from agendas)

◆ Experts Live UK 2026 – missing agenda items

- Nikki Chapple explicitly states that:
 - A 30-minute lightning talk (topic TBA) and
 - Participation in the Women in IT panelhave not yet appeared on the agenda Speaking and Commu...
- These are confirmed acceptances, but not publicly visible yet.

✓ **Status:** Event is published, but some accepted sessions are still unpublished.

Message Copilot



AI-generated content may be incorrect





Upcoming Events and Speaker Calls Summary

Work

Web



Auto



New chat

Search

Library

Create

Agents

Researcher

Analyst

PowerPoint

Cowork (Frontier)

New agent

All agents

Apps

1

Ståle Hansen



◆ Techorama Netherlands 2026 – CFP open, no publication yet

- Techorama Netherlands 2026 is announced with:
 - CFP open
 - Submission deadline **May 29, 2026**
 - Event dates **Oct 26–28, 2026** Speaking and Commu...
- No indication of CloudWay sessions submitted or published yet.

✓ **Status: Not published (for CloudWay), CFP still open.**

2. Events with Call for Speakers Still Open

Message Copilot



AI-generated content may be incorrect





Upcoming Events and Speaker Calls Summary

Work

Web



Auto



New chat

Search

Library

Create

Agents

Researcher

Analyst

PowerPoint

Cowork (Frontier)

New agent

All agents

Apps

1

Ståle Hansen

 **Workplace-focused event (May 27, Oslo – day before CloudWay gathering)**

- Described by [Ståle Hansen](#) as:
 - Looking for speakers across Identity, Security, Endpoint, Copilot, Sentinel, Purview, AVD, etc.
 - Clearly framed as an **open speaker request**, not yet finalized  Speaking and Commu...
- No confirmation that:
 - Sessions are finalized
 - Event is publicly published

 **Status: Speaker selection ongoing, effectively still open.**

Message Copilot



AI-generated content may be incorrect





Upcoming Events and Speaker Calls Summary

Work

Web



Auto ▾



New chat

Search

Library

Create

Agents

Researcher

Analyst

PowerPoint

Cowork (Frontier)

New agent

All agents

Apps

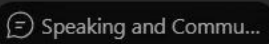
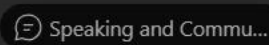
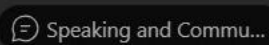
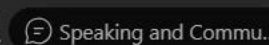
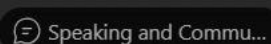
1

Ståle Hansen



3. Events That Are Published / Closed (for completeness, not action)

These are **already published or CFP-closed**, included here just to prevent false positives:

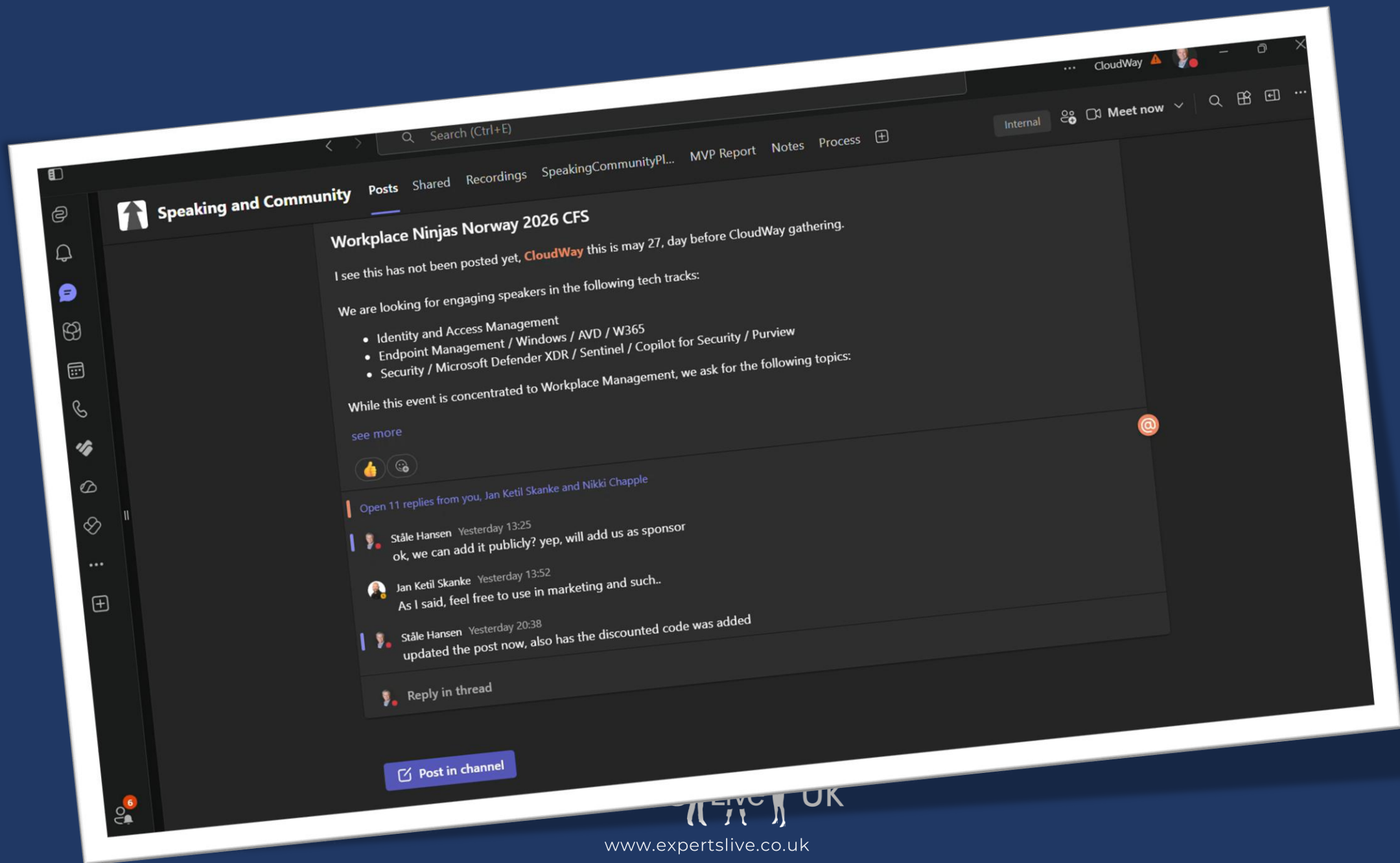
- Commsverse 2026 – The Microsoft Teams Conference
 - ✓ Published, schedule live 
- Workplace Ninjas Norway 2026
 - ✓ Accepted and published 
- ESPC 2026
 - ✗ CFP closed April 2 
- Teamsdagen 2026
 - ✗ CFP closed April 12 
- Experts Live Sweden 2026
 - ✗ CFP closed April 30 (noted retrospectively) 

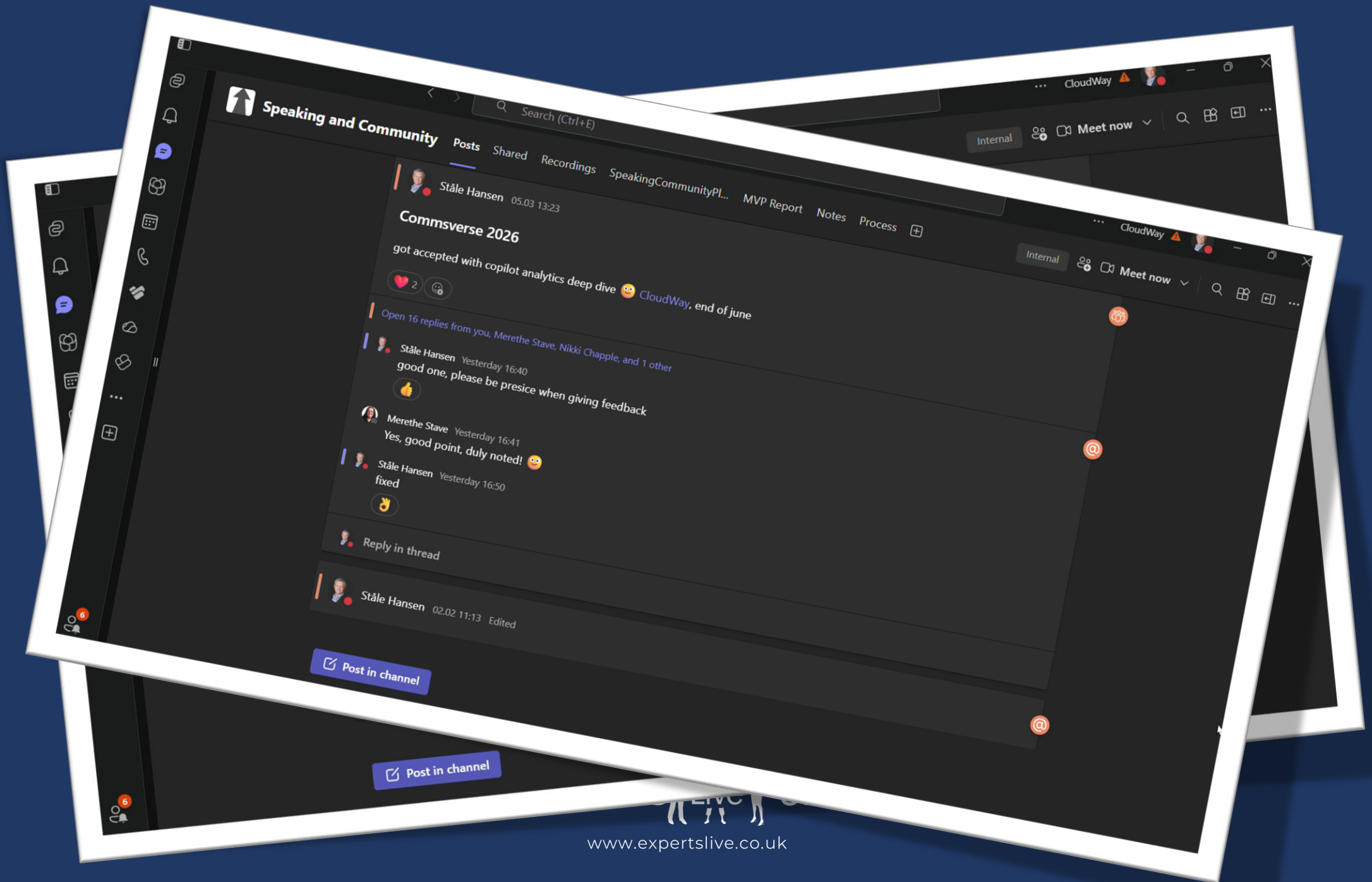
Message Copilot

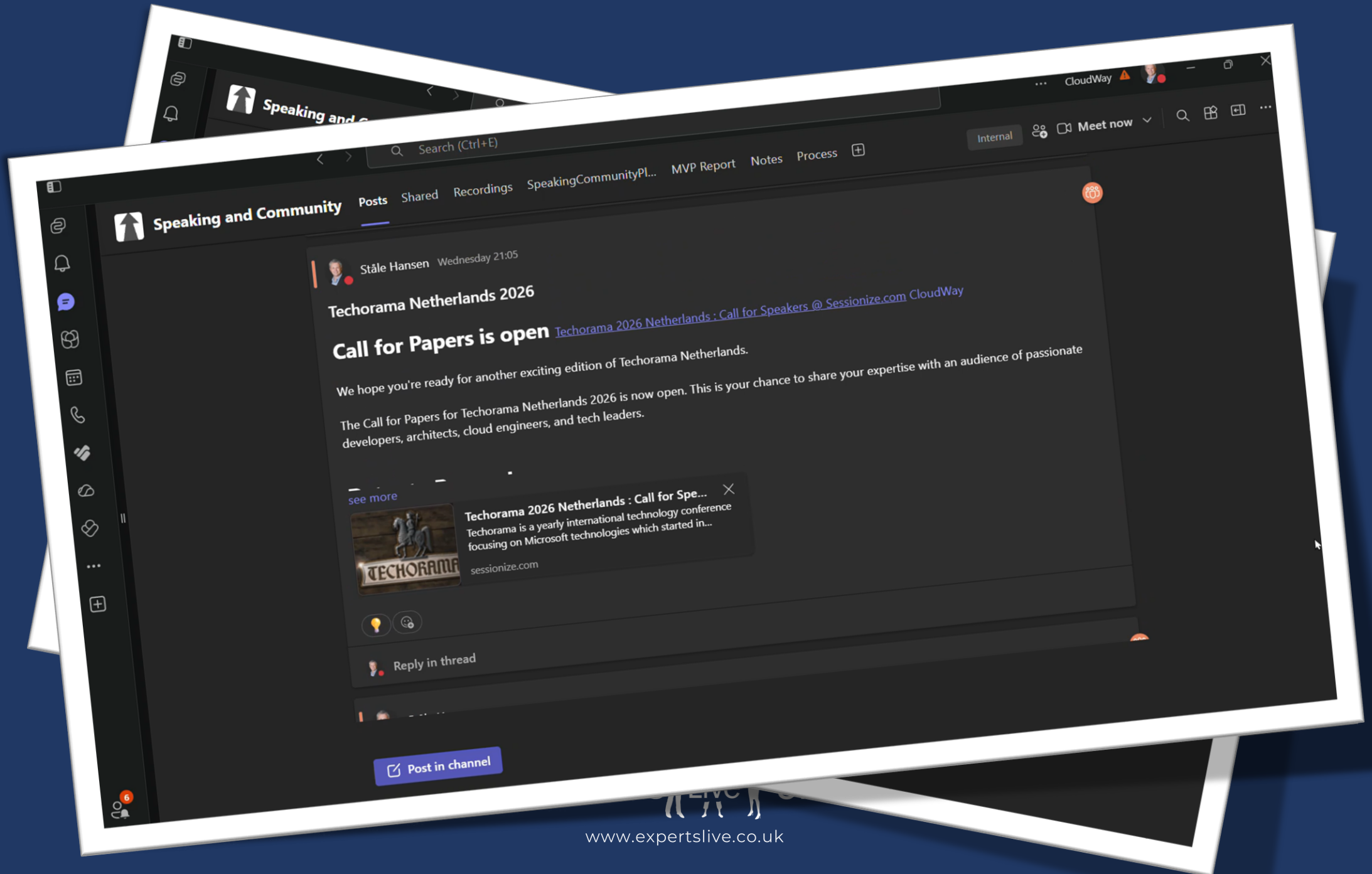


AI-generated content may be incorrect









I Have Forgot My Badge, How Do I Sign In?

An employee have been
instructed to sign-in to Teams
for information,
but the badge is left at home...



I Have Forgot My Badge, How Do I Sign In?

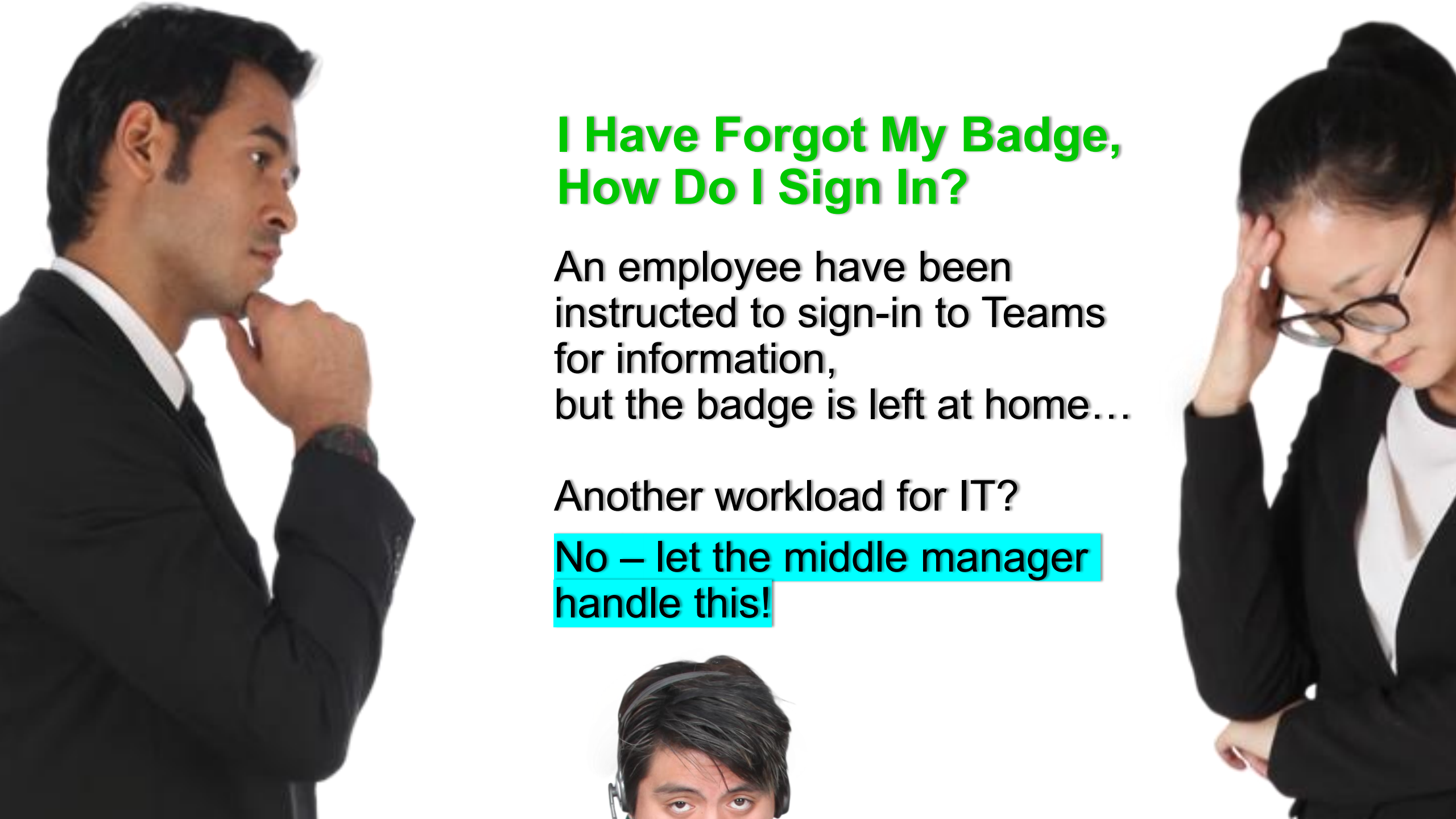
An employee have been instructed to sign-in to Teams for information, but the badge is left at home...

Another workload for IT?



Max
Kernel





I Have Forgot My Badge, How Do I Sign In?

An employee have been instructed to sign-in to Teams for information, but the badge is left at home...

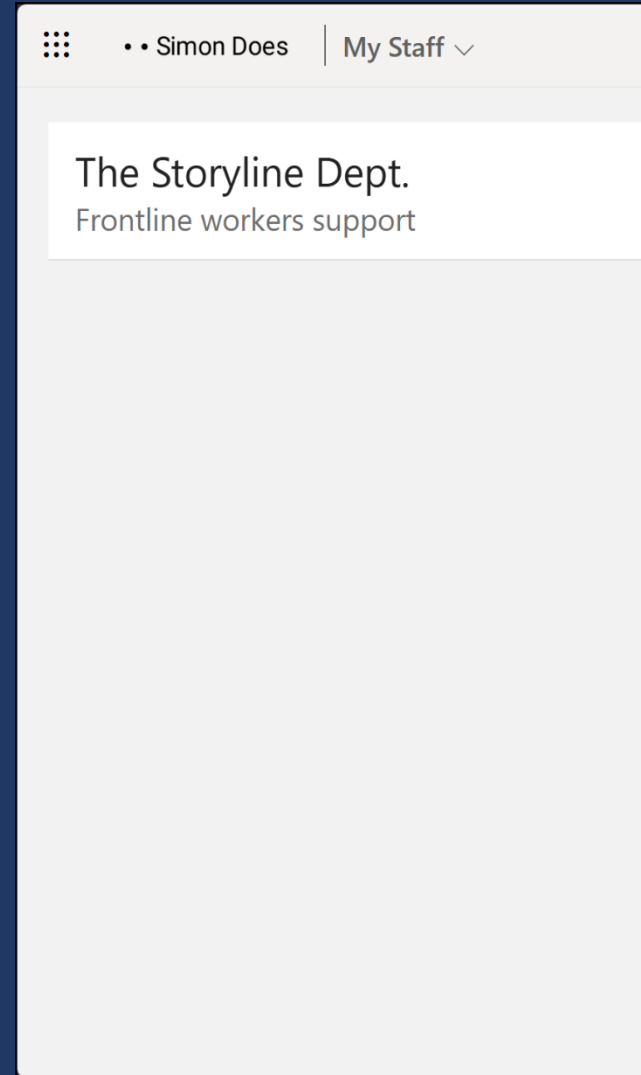
Another workload for IT?

No – let the middle manager handle this!

Entra ID – My Staff

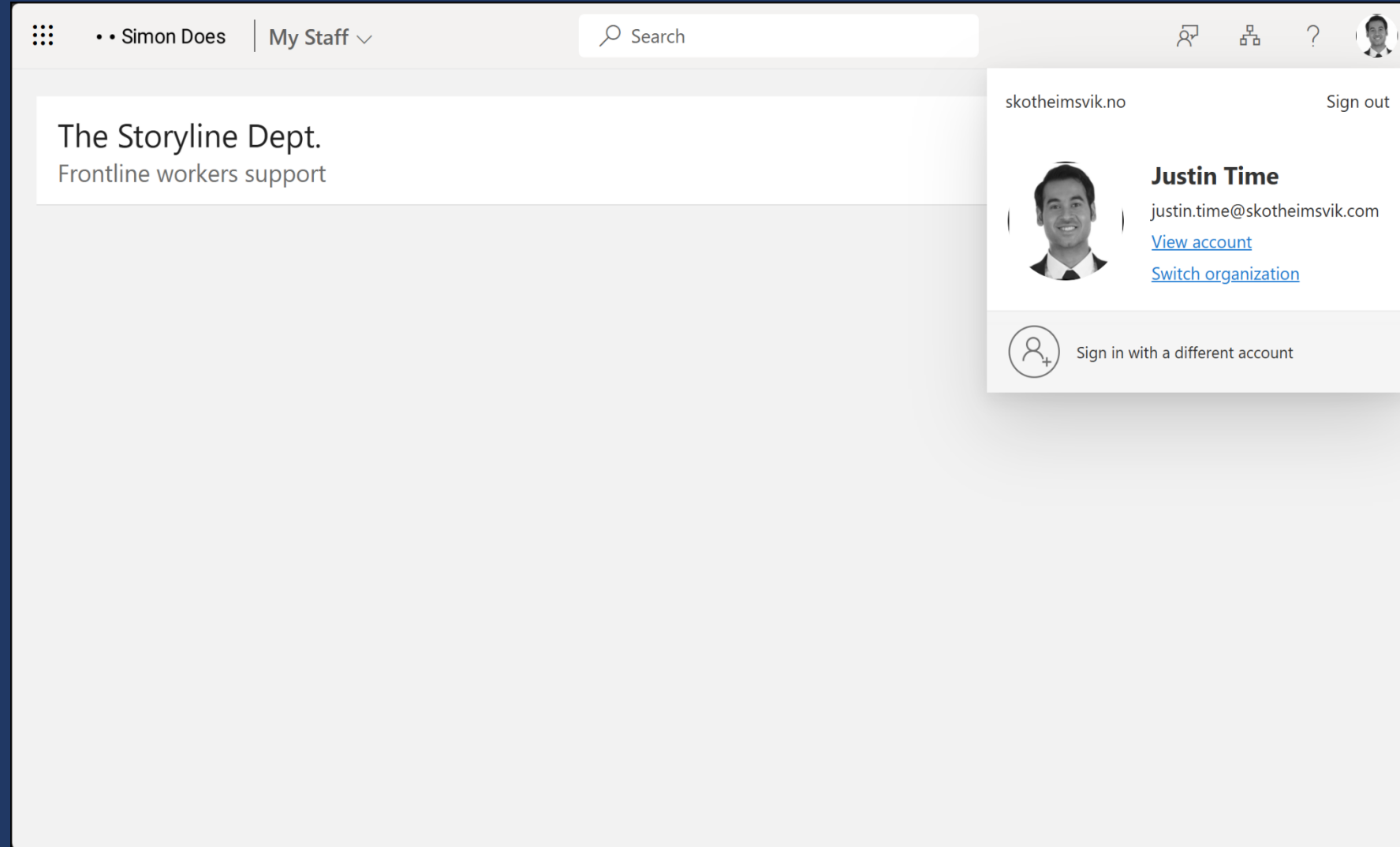


- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems



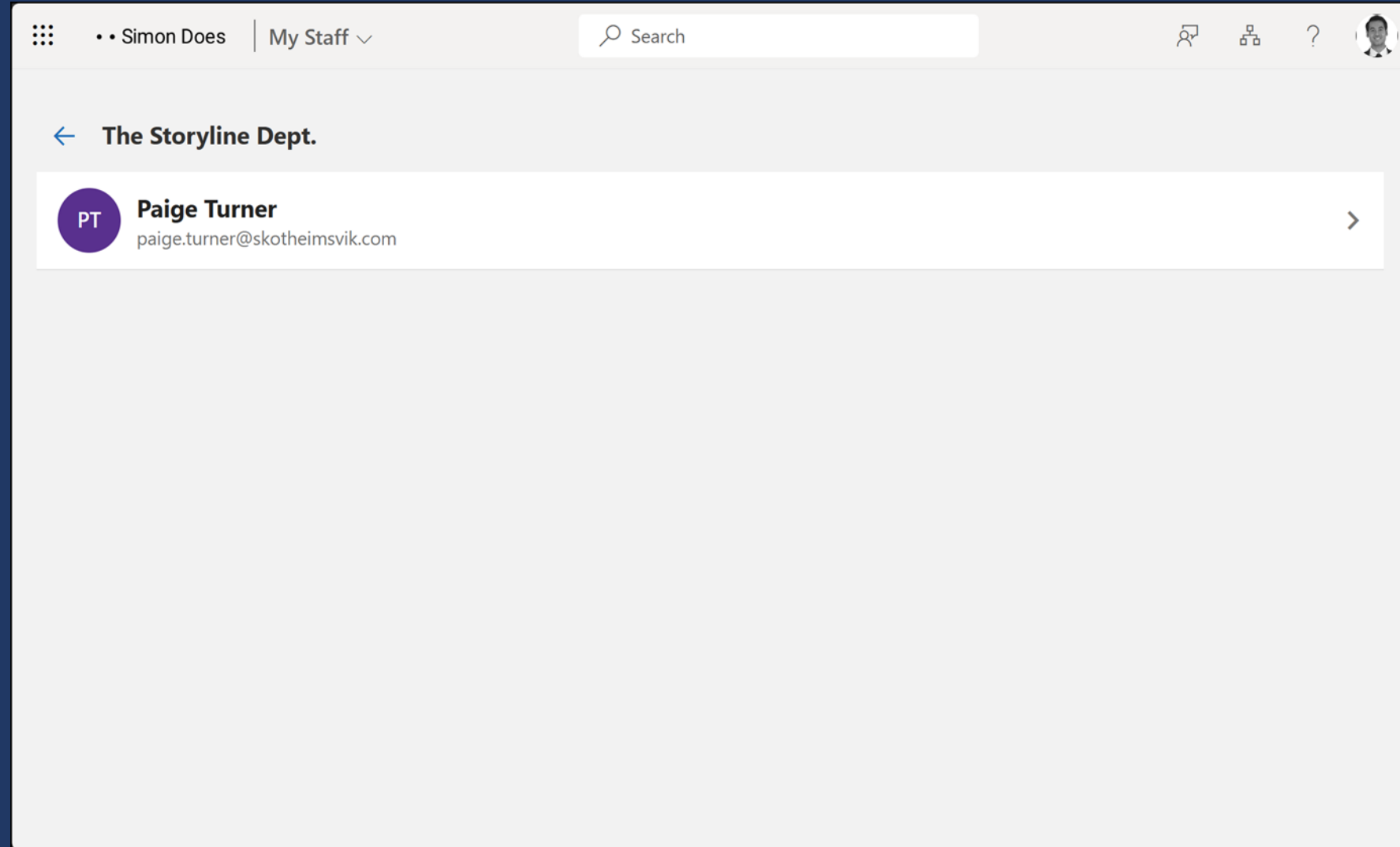
Entra ID – My Staff

- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems



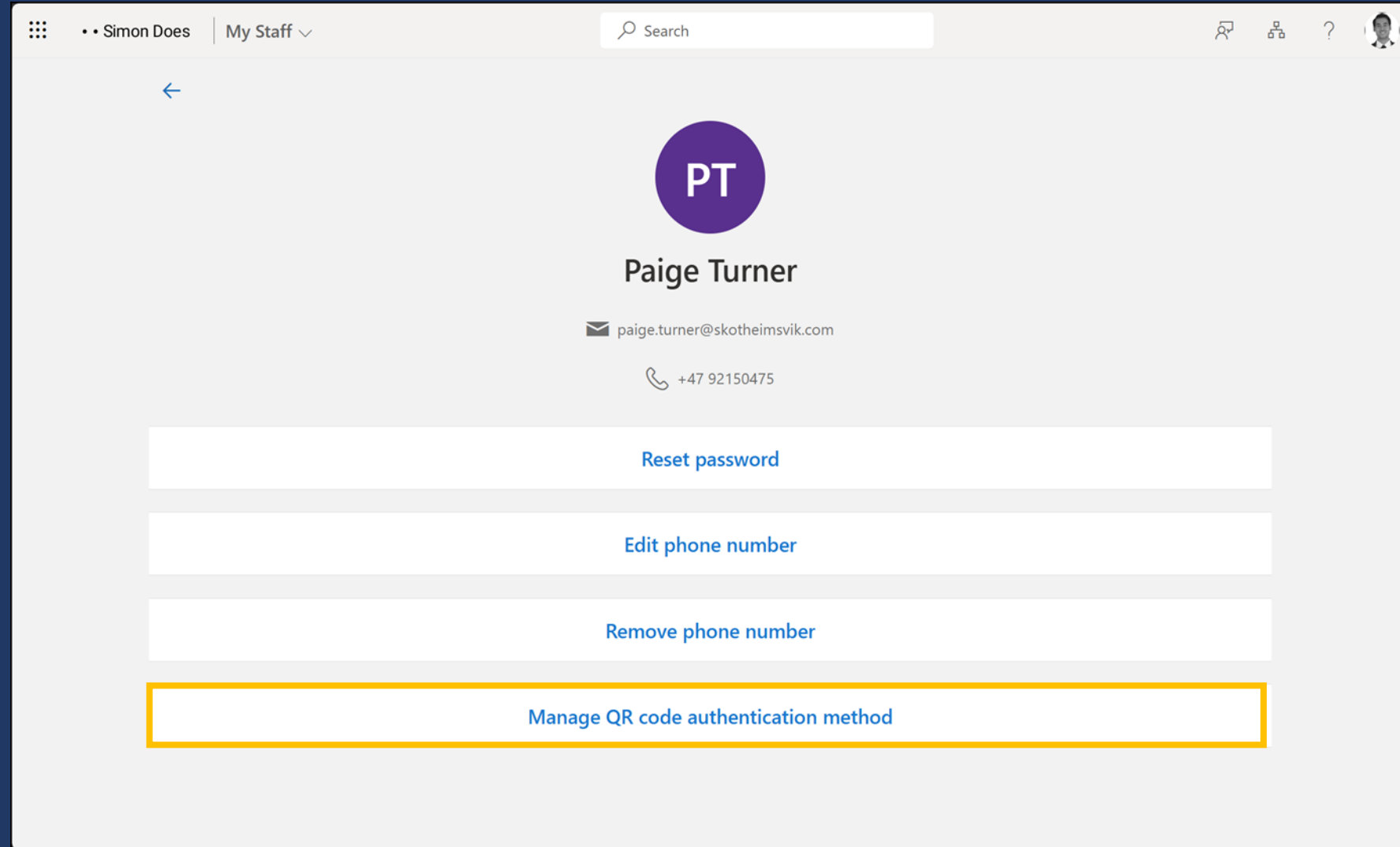
Entra ID – My Staff

- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems



Entra ID – My Staff

- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems



Entra ID – My Staff

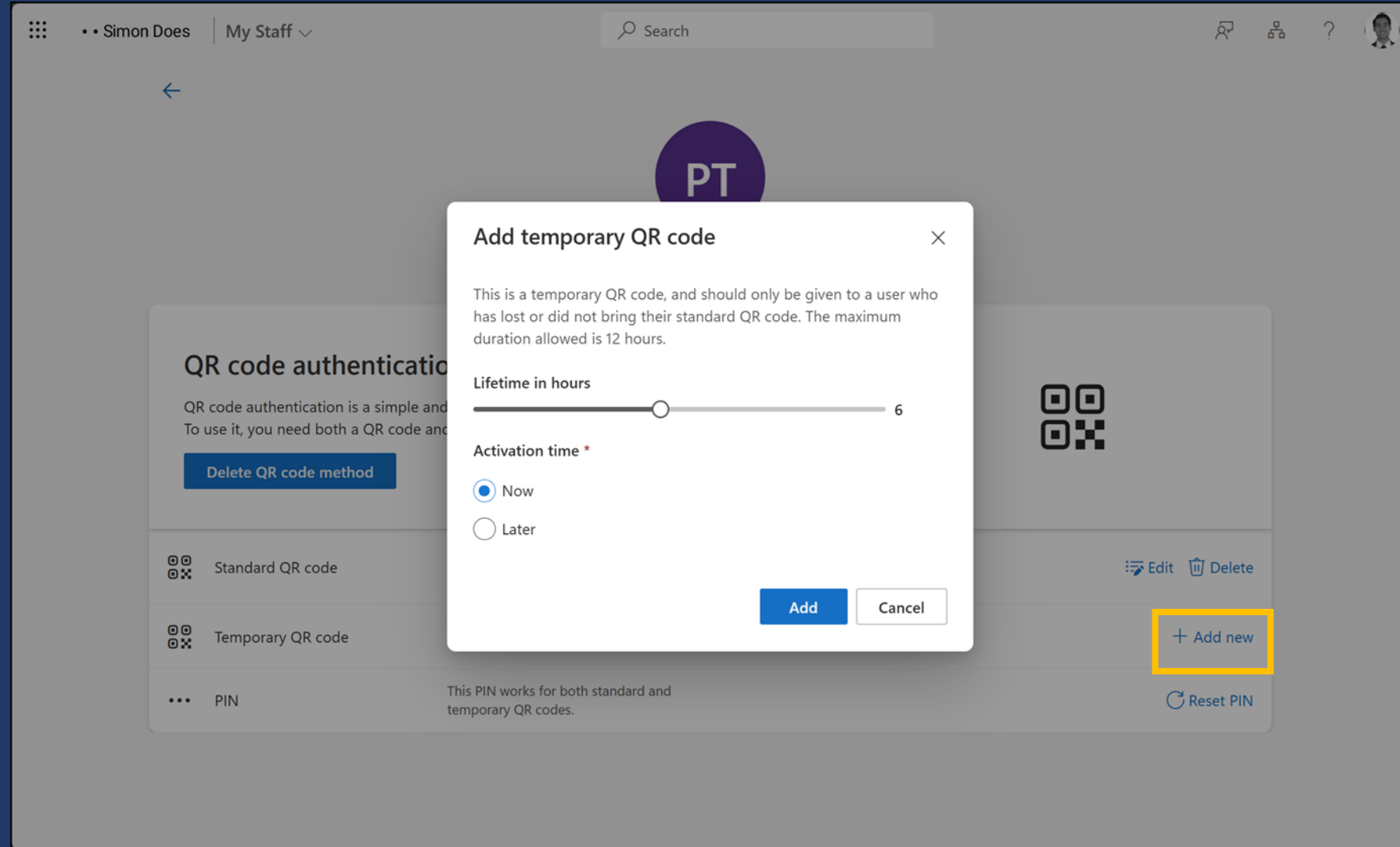
- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems

The screenshot shows the 'My Staff' portal for a user named Paige Turner. The interface includes a top navigation bar with the user's name 'Simon Does' and a search bar. Below the navigation bar, there is a back arrow and a profile card for Paige Turner with a purple circle containing 'PT'. The main content area is titled 'QR code authentication Method' and includes a description: 'QR code authentication is a simple and fast authentication method for frontline workers. To use it, you need both a QR code and PIN.' There is a blue button labeled 'Delete QR code method'. Below this, there is a table with three rows: 'Standard QR code', 'Temporary QR code', and 'PIN'. The 'Temporary QR code' row is highlighted with a yellow border and has a '+ Add new' button. The 'PIN' row has a 'Reset PIN' button.

Method	Details	Actions
Standard QR code	Activated on Wed Aug 20 2025 12:37:56 GMT+0200 (Central European Summer Time) Expires on Wed Aug 19 2026 23:59:59 GMT+0200 (Central European Summer Time)	Edit Delete
Temporary QR code	Not Added	+ Add new
PIN	This PIN works for both standard and temporary QR codes.	Reset PIN

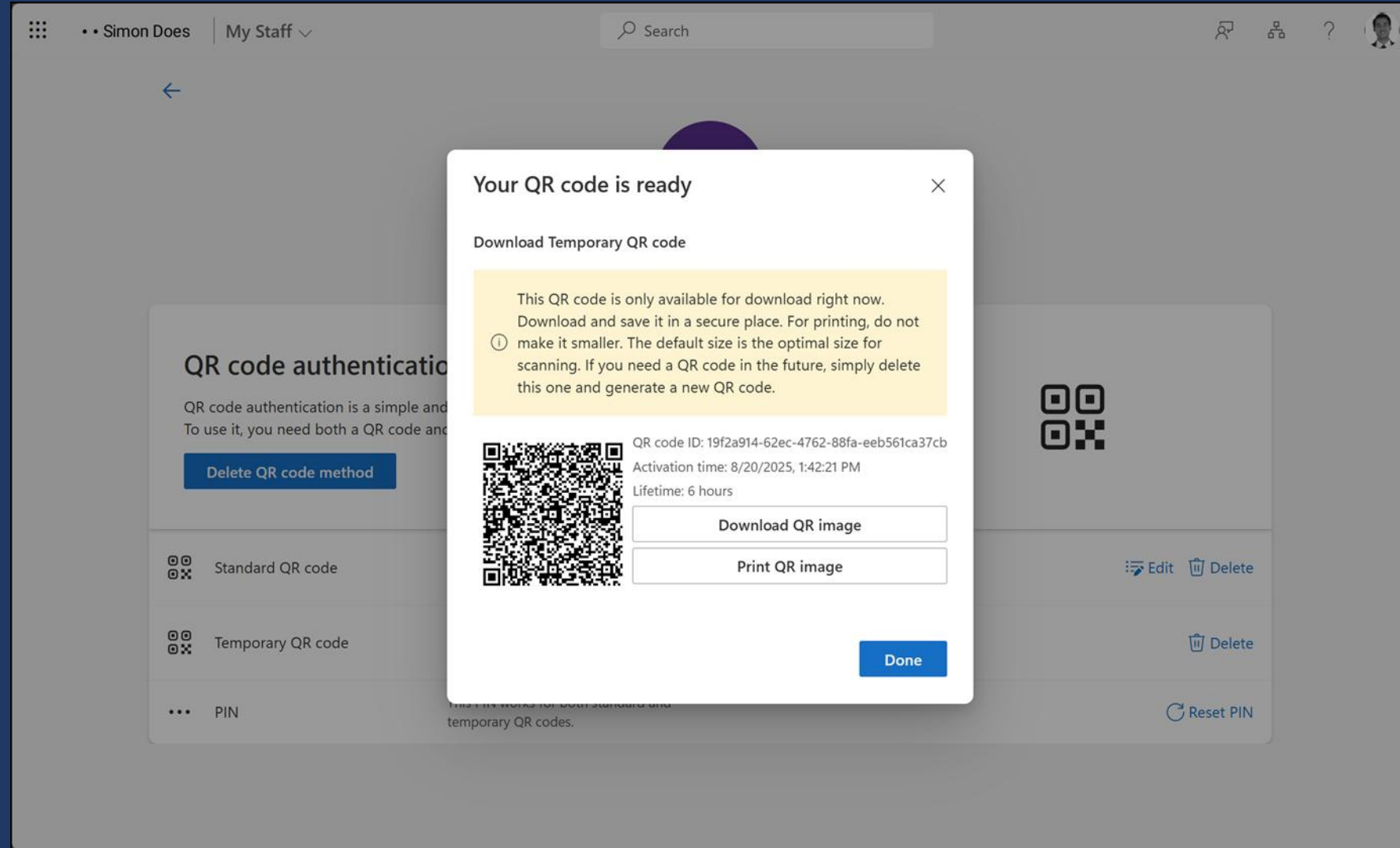
Entra ID – My Staff

- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems



Entra ID – My Staff

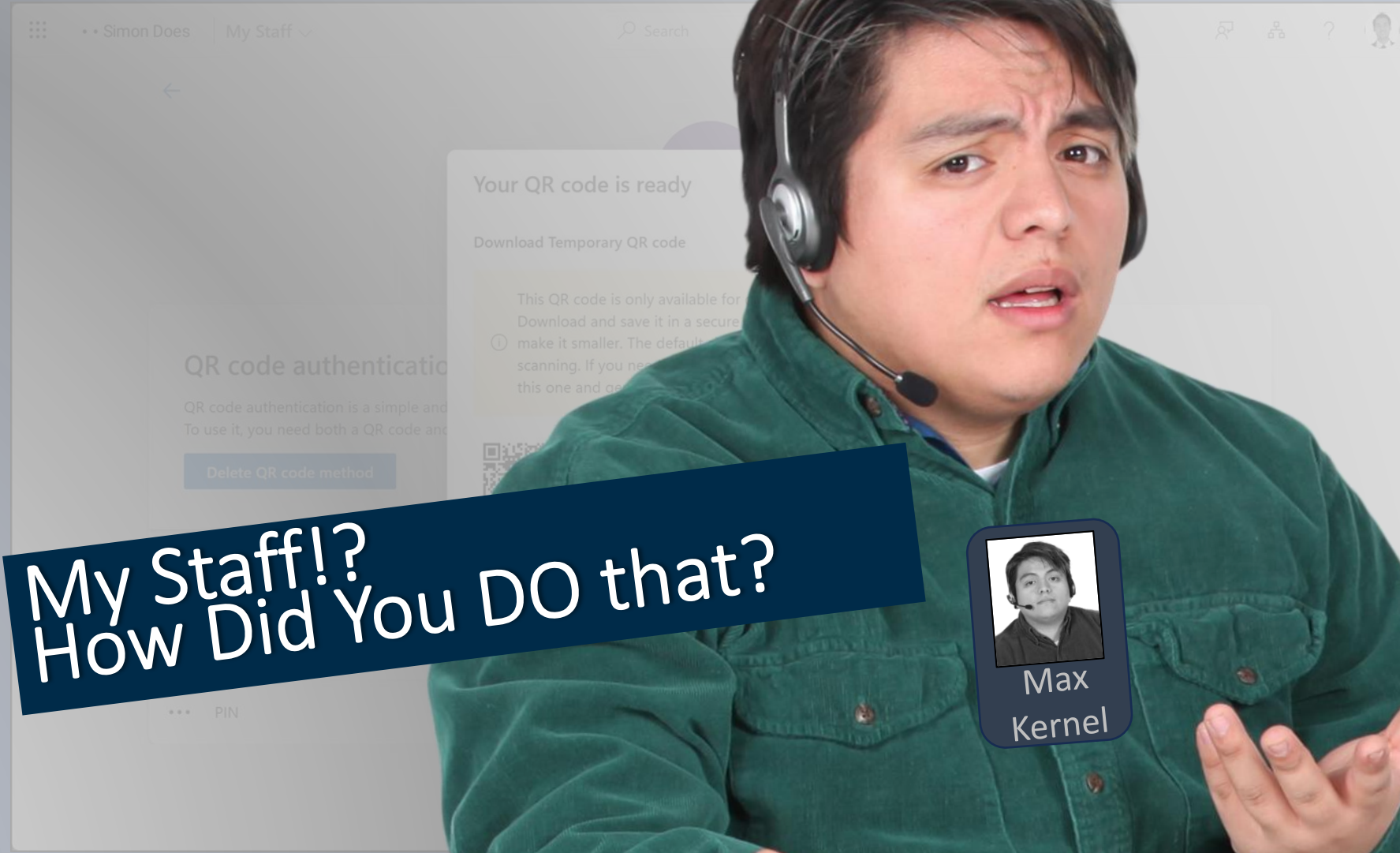
- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems



Entra ID – My Staff

- My Staff portal empowers frontline managers, like store leads or shift supervisors, to handle basic identity tasks for their team without needing IT support.
- Manage their users
- Register users for QR Code
- Assist with access problems

My Staff!?
How Did You DO that?





Entra ID – My Staff Configuration

- My Staff need to be enabled in Entra ID
- User Settings – User Features

Microsoft Entra admin center

Search resources, services, and docs (G+/I)

Copilot

Home > Users > Justin Time | Authentication methods > Roles and administrators | Admin units > Users

Users | User settings

skotheimsvik.no

Refresh | Got feedback?

All users

Audit logs

Sign-in logs

Diagnose and solve problems

Deleted users

Password reset

User settings

Bulk operation results

New support request

Administration center

Learn more

Restrict access to Microsoft Entra admin center ☒ Yes

LinkedIn account connections

Learn more

Allow users to connect their work or school account with LinkedIn ☒ Yes ☐ Selected group ☐ No

Show keep user signed in

Show keep user signed in ☐ No

External users

Manage external collaboration settings

User features

Manage user feature settings

Save Cancel



Entra ID – My Staff Configuration

- My Staff need to be enabled in Entra ID
- User Settings – User Features
- My Staff
 - Assignment

The screenshot displays the Microsoft Entra admin center interface. The left-hand navigation pane includes links for Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, and Identity Secure Score. The main content area is titled 'User features' and shows configuration options for 'My Apps' and 'My Staff'. The 'Administrators can access My Staff' toggle is currently set to 'Selected' and is highlighted with a yellow rectangular box. Below this toggle, a 'Select a group' dropdown menu is visible, with 'Managers' selected. The top of the interface features a search bar and various utility icons.



Entra ID – Administrative Units

- Administrative units restrict permissions in a role to any portion of your organization that you define.
- Create one Admin Unit

The screenshot shows the Microsoft Entra admin center interface. On the left, the 'Roles & admins' menu item is highlighted. The main content area shows the 'Roles and administrators | Admin units' page. The 'Admin units' tab is selected, displaying a table of administrative units. The table has columns for 'Name', 'Description', and 'Restricted manage...'. One unit is listed: 'The Storyline Dept.' with the description 'Frontline workers supp...' and 'Restricted manage...' set to 'No'.

Name	Description	Restricted manage...
The Storyline Dept.	Frontline workers supp...	No



Entra ID – Administrative Units

- Administrative units restrict permissions in a role to any portion of your organization that you define.
- Create one Admin Unit

The screenshot displays the Microsoft Entra admin center interface. The left-hand navigation pane shows the 'Roles & admins' section highlighted. The main content area is titled 'Roles and administrators | Admin units'. Below this, there is a search bar for administrative units and a table listing them. The table has columns for 'Name', 'Description', and 'Restricted manage...'. One entry, 'The Storyline Dept.', is highlighted. An inset window shows a preview of this unit with the name 'The Storyline Dept.' and the description 'Frontline workers support'.

Name	Description	Restricted manage...
The Storyline Dept.	Frontline workers supp...	No



Entra ID – Administrative Units

- Administrative units restrict permissions in a role to any portion of your organization that you define.
- Create one Admin Unit
- Add assets (users)

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane has the 'Roles & admins' option highlighted with a yellow box. The main content area shows the breadcrumb path 'Home > Paige Turner > Roles and administrators > Admin units > The Storyline Dept.' with the last two segments highlighted in yellow. Below the breadcrumb, the title 'The Storyline Dept. | Users' is displayed. A yellow box highlights the 'Users' option in the 'Manage' section. To the right, a table lists users, with the first row highlighted in yellow:

	Display name ↑	User principal name ↑↓	User ty
☐	Paige Turner	paige.turner@sko...	Membe



Entra ID – Administrative Units

- Administrative units restrict permissions in a role to any portion of your organization that you define.
- Create one Admin Unit
- Add assets (users)
- Give scoped assigned roles to the managers

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane has a yellow box around the 'Users' link. The main content area shows the profile for 'Justin Time', with a yellow box around the 'Assigned roles' link in the left sub-menu. The 'Assigned roles' page displays a table of roles assigned to the user. A yellow box highlights the table headers and the first two rows of data.

Role	Principal na...	Scope
User Administrator	justin.time@skot...	The Storyline Dept. (Administrative unit)
Privileged Authentication Administrator	justin.time@skot...	The Storyline Dept. (Administrative unit)

Is This Even Secure?

The management is nervous

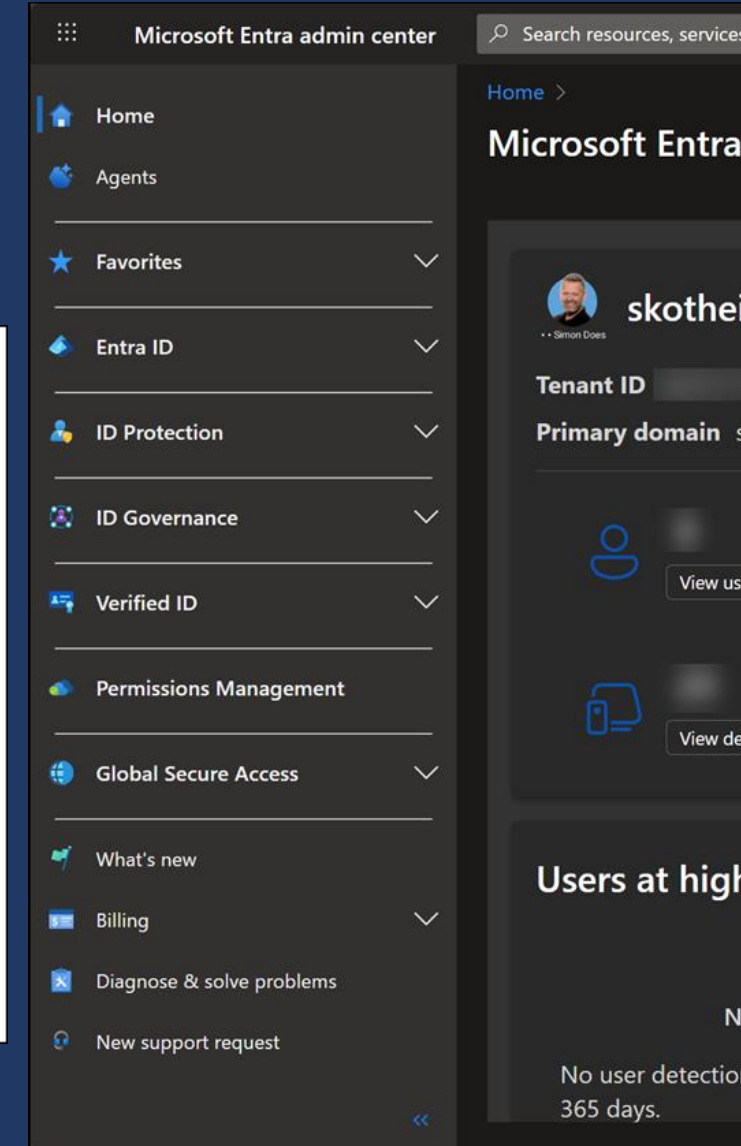
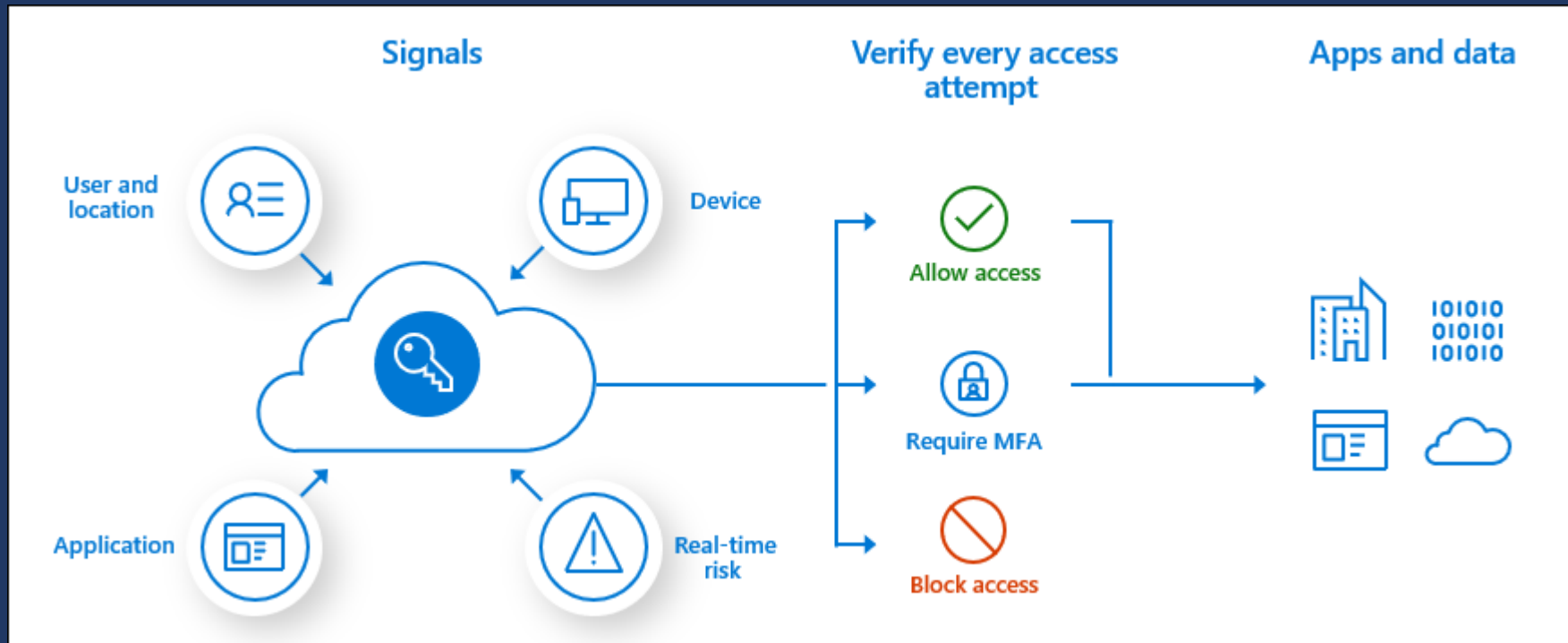
QR code and a PIN code?
That's it? No MFA!?





Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.





Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

Microsoft Entra admin center

Search resources, services, and docs (G+/I)

Copilot

Home > Microsoft Entra > Conditional Access

Conditional Access | Policies

Microsoft Entra ID

- Overview
- Policies**
- Insights and reporting
- Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication contexts
- Authentication strengths
- Classic policies

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

- New support request

User created policies

Policies created ⓘ

45

ca6

6 out of 45 policies found

Policy name
CA600 - Frontline - Office365 - Browser - Block
CA601 - Frontline - AllApps - iOSorAndroid - Compliant - Grant
CA602 - Frontline - AllApps - UnknownLocation - Block
CA603 - Frontline - AllApps - AnyPlatform - Signinfrequency - 4 hours - Session
CA604 - Frontline - AllApps - HighUserRisk - Block
CA605 - Frontline - AllApps - AnyPlatform - HighSignInRisk - Block



Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

Policy name

CA600 - Frontline - Office365 - Browser - Block

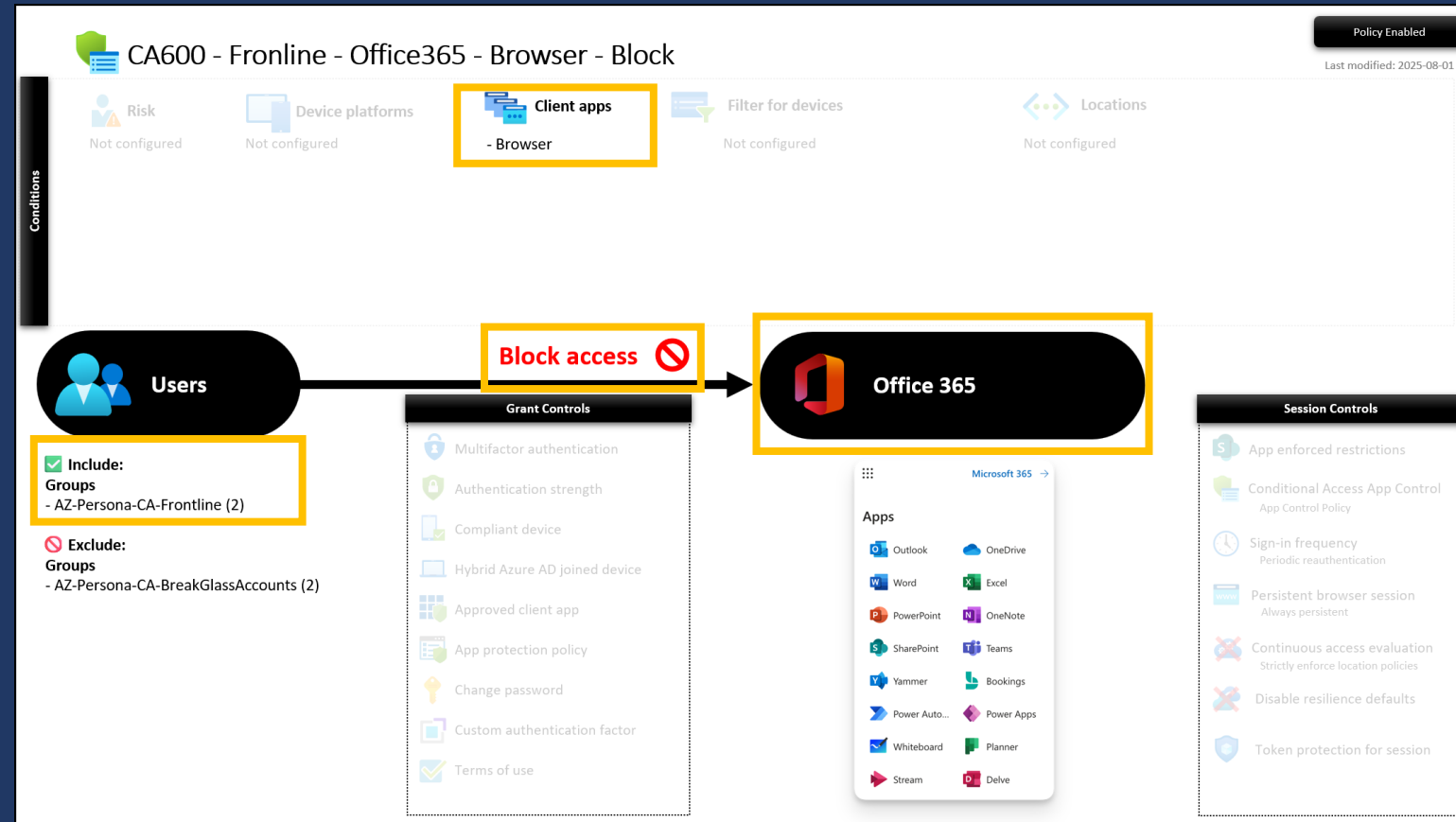
CA601 - Frontline - AllApps - iOSorAndroid - Compliant - Grant

CA602 - Frontline - AllApps - UnknownLocation - Block

CA603 - Frontline - AllApps - AnyPlatform - Signinfrequency - 4 hours - Session

CA604 - Frontline - AllApps - HighUserRisk - Block

CA605 - Frontline - AllApps - AnyPlatform - HighSignInRisk - Block





Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

Policy name

CA600 - Frontline - Office365 - Browser - Block

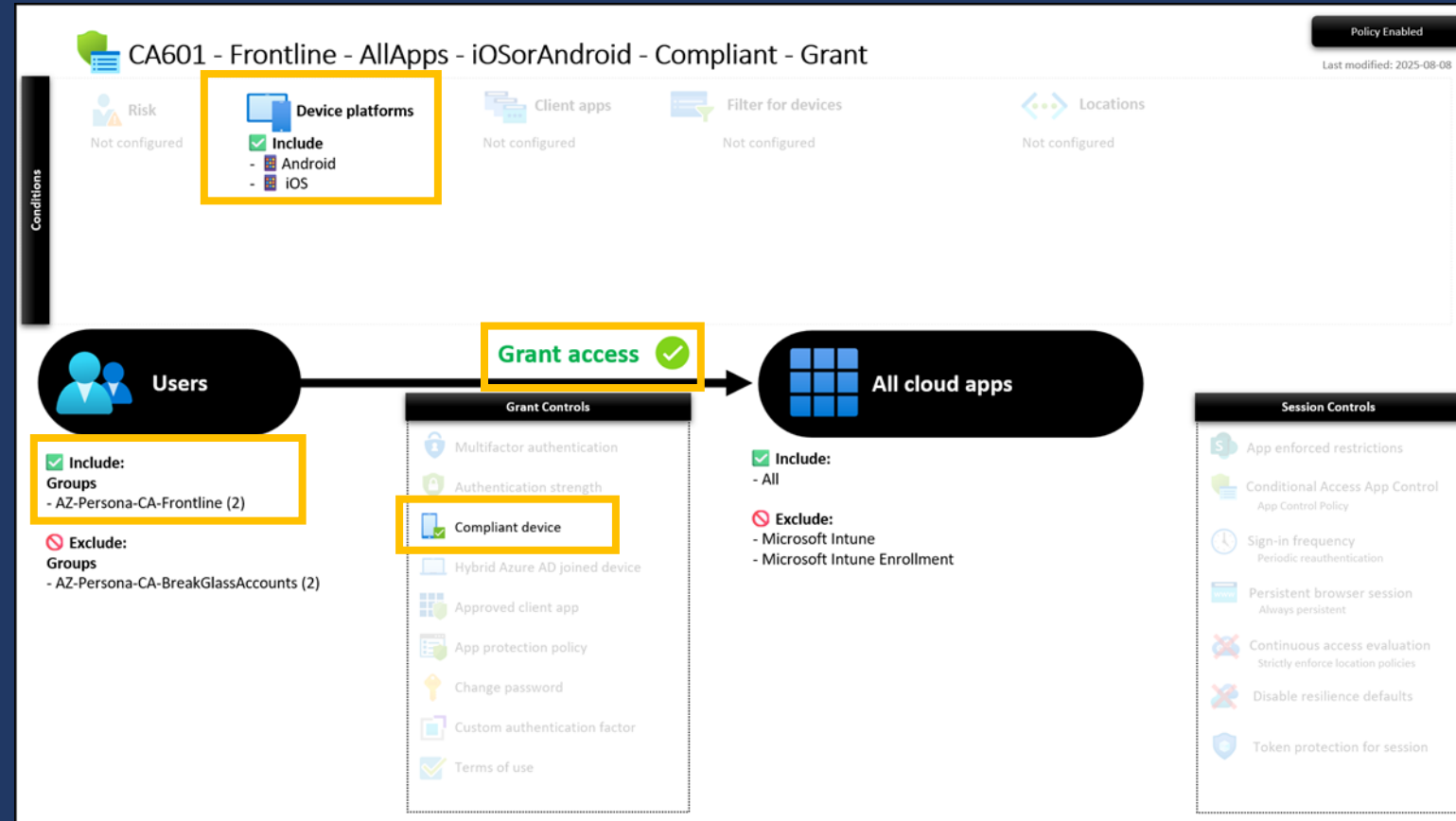
CA601 - Frontline - AllApps - iOSorAndroid - Compliant - Grant

CA602 - Frontline - AllApps - UnknownLocation - Block

CA603 - Frontline - AllApps - AnyPlatform - Signinfrequency - 4 hours - Session

CA604 - Frontline - AllApps - HighUserRisk - Block

CA605 - Frontline - AllApps - AnyPlatform - HighSignInRisk - Block





Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

Policy name

CA600 - Frontline - Office365 - Browser - Block

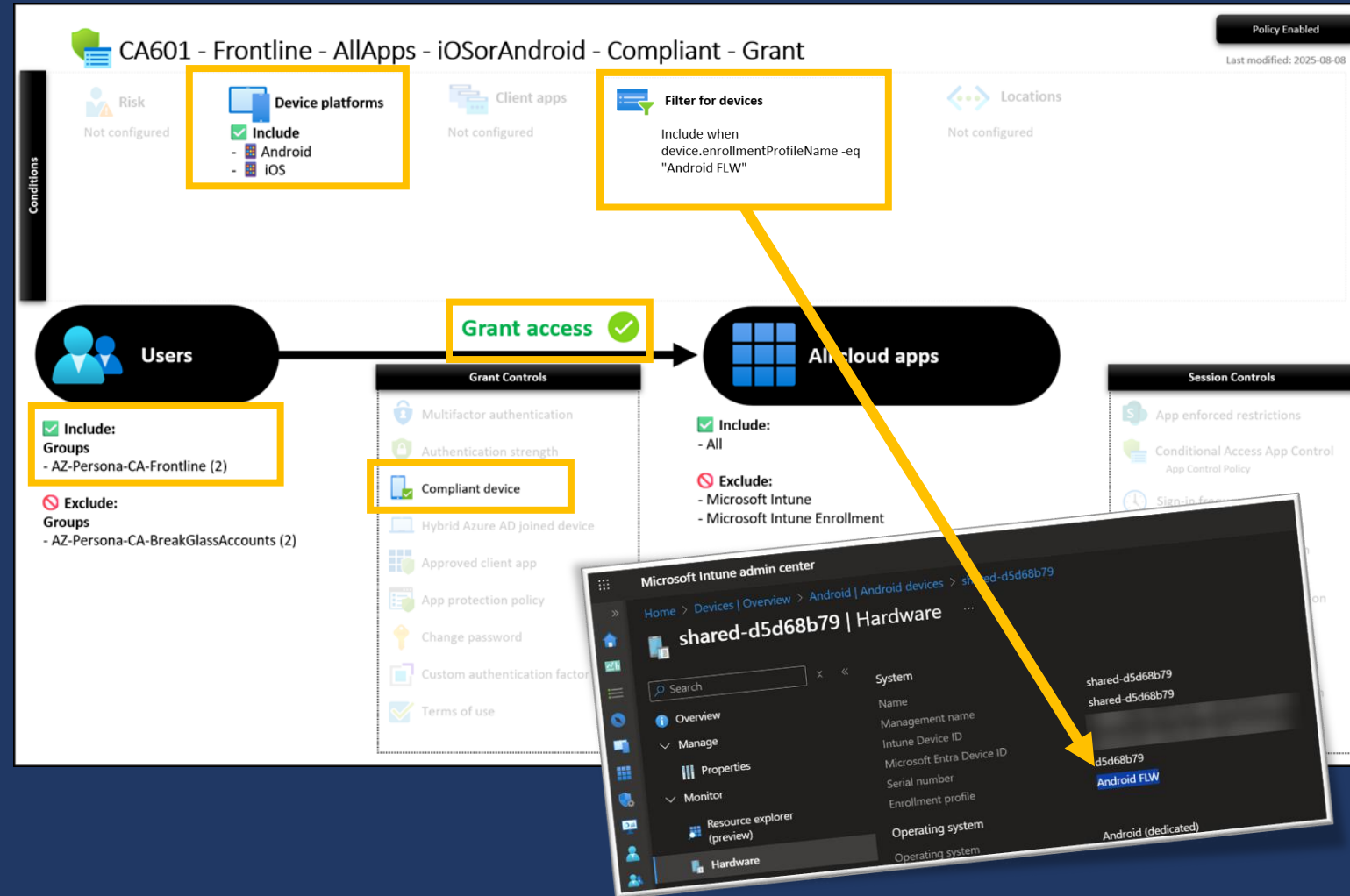
CA601 - Frontline - AllApps - iOSorAndroid - Compliant - Grant

CA602 - Frontline - AllApps - UnknownLocation - Block

CA603 - Frontline - AllApps - AnyPlatform - Signinfrequency - 4 hours - Session

CA604 - Frontline - AllApps - HighUserRisk - Block

CA605 - Frontline - AllApps - AnyPlatform - HighSignInRisk - Block





Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

Policy name

CA600 - Frontline - Office365 - Browser - Block

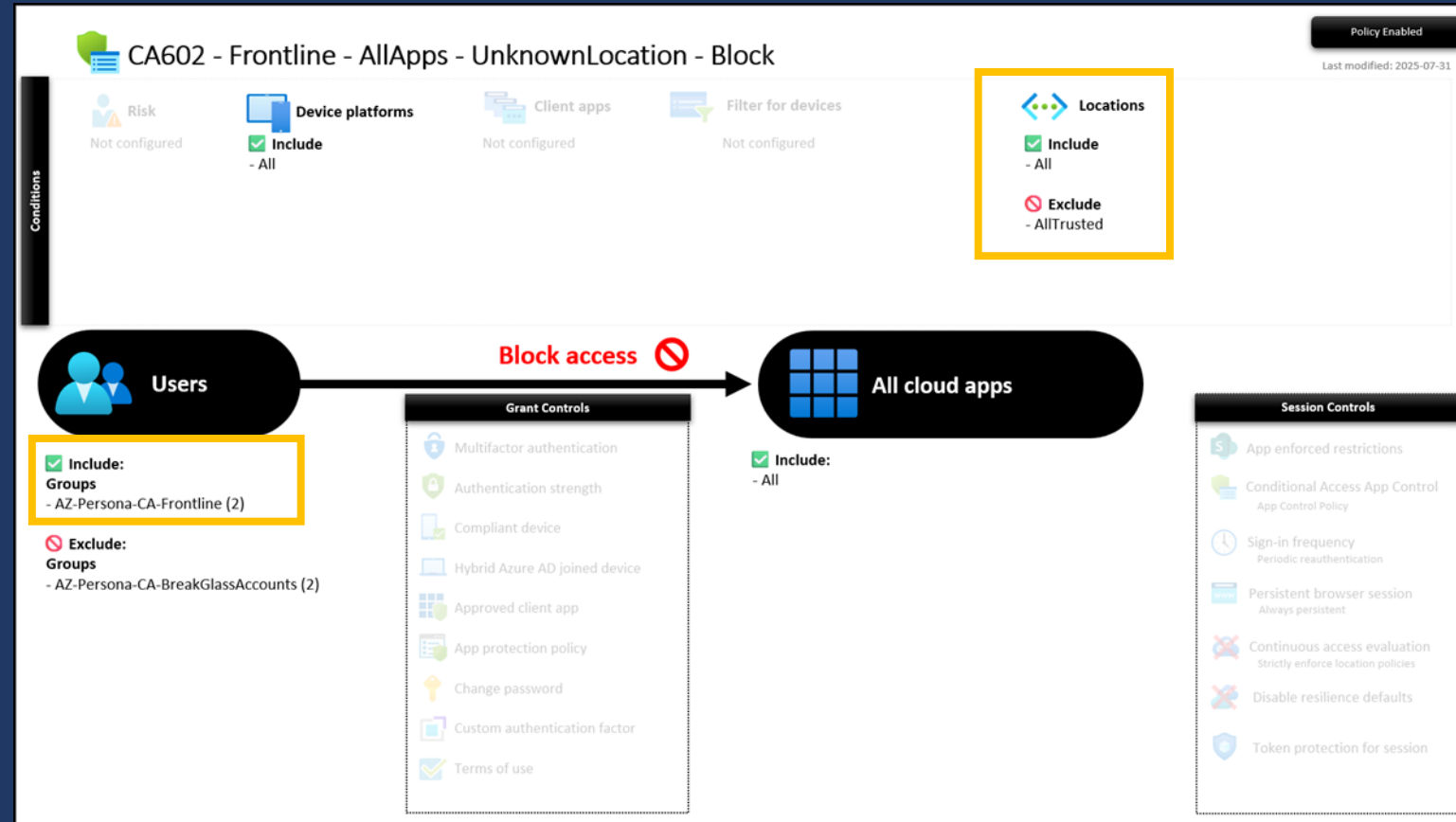
CA601 - Frontline - AllApps - iOSorAndroid - Compliant - Grant

CA602 - Frontline - AllApps - UnknownLocation - Block

CA603 - Frontline - AllApps - AnyPlatform - Signinfrequency - 4 hours - Session

CA604 - Frontline - AllApps - HighUserRisk - Block

CA605 - Frontline - AllApps - AnyPlatform - HighSignInRisk - Block





Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

Policy name

CA600 - Frontline - Office365 - Browser - Block

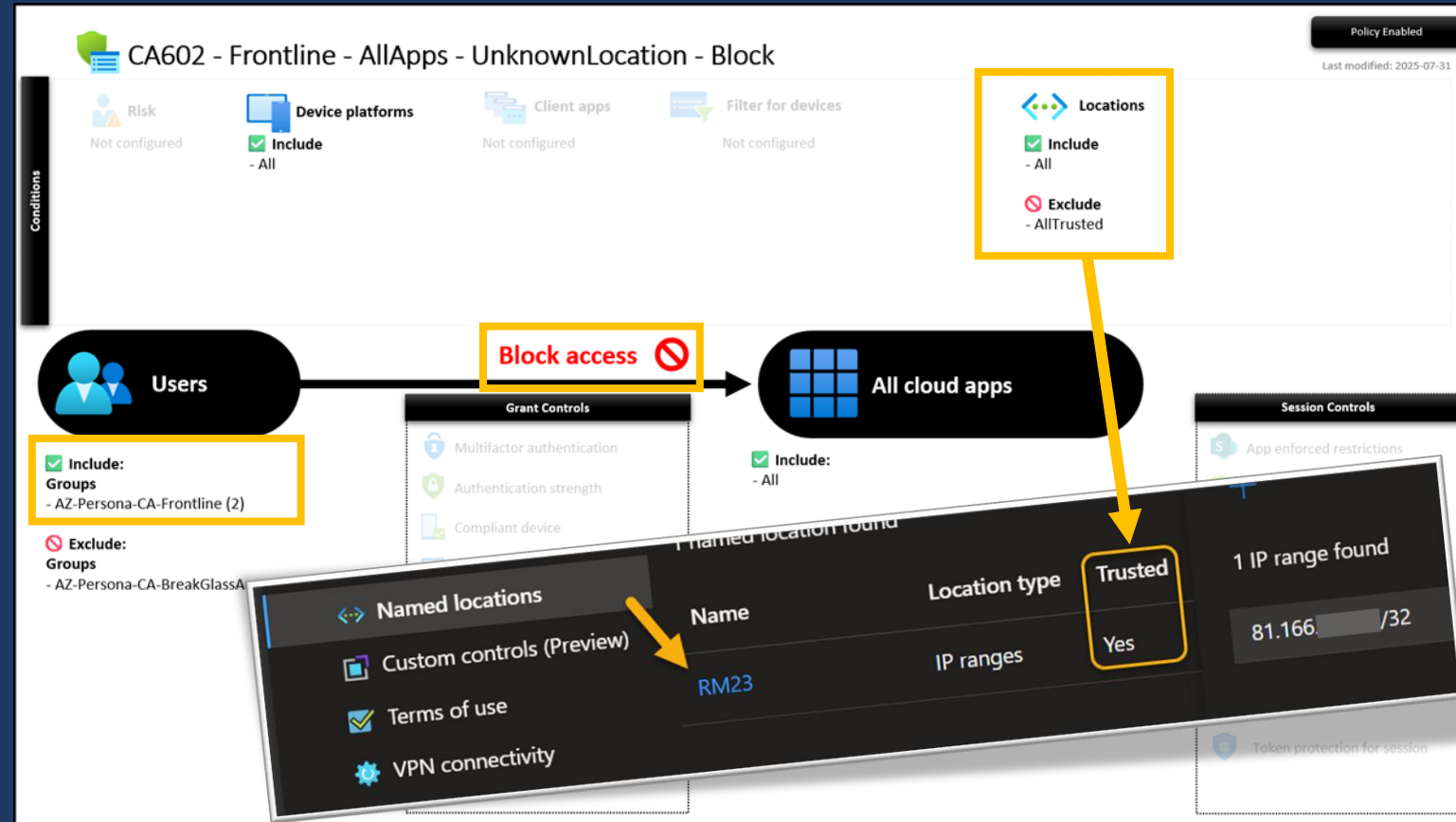
CA601 - Frontline - AllApps - iOSorAndroid - Compliant - Grant

CA602 - Frontline - AllApps - UnknownLocation - Block

CA603 - Frontline - AllApps - AnyPlatform - Signinfrequency - 4 hours - Session

CA604 - Frontline - AllApps - HighUserRisk - Block

CA605 - Frontline - AllApps - AnyPlatform - HighSignInRisk - Block





Entra ID – Conditional Access

- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

Policy name

CA600 - Frontline - Office365 - Browser - Block

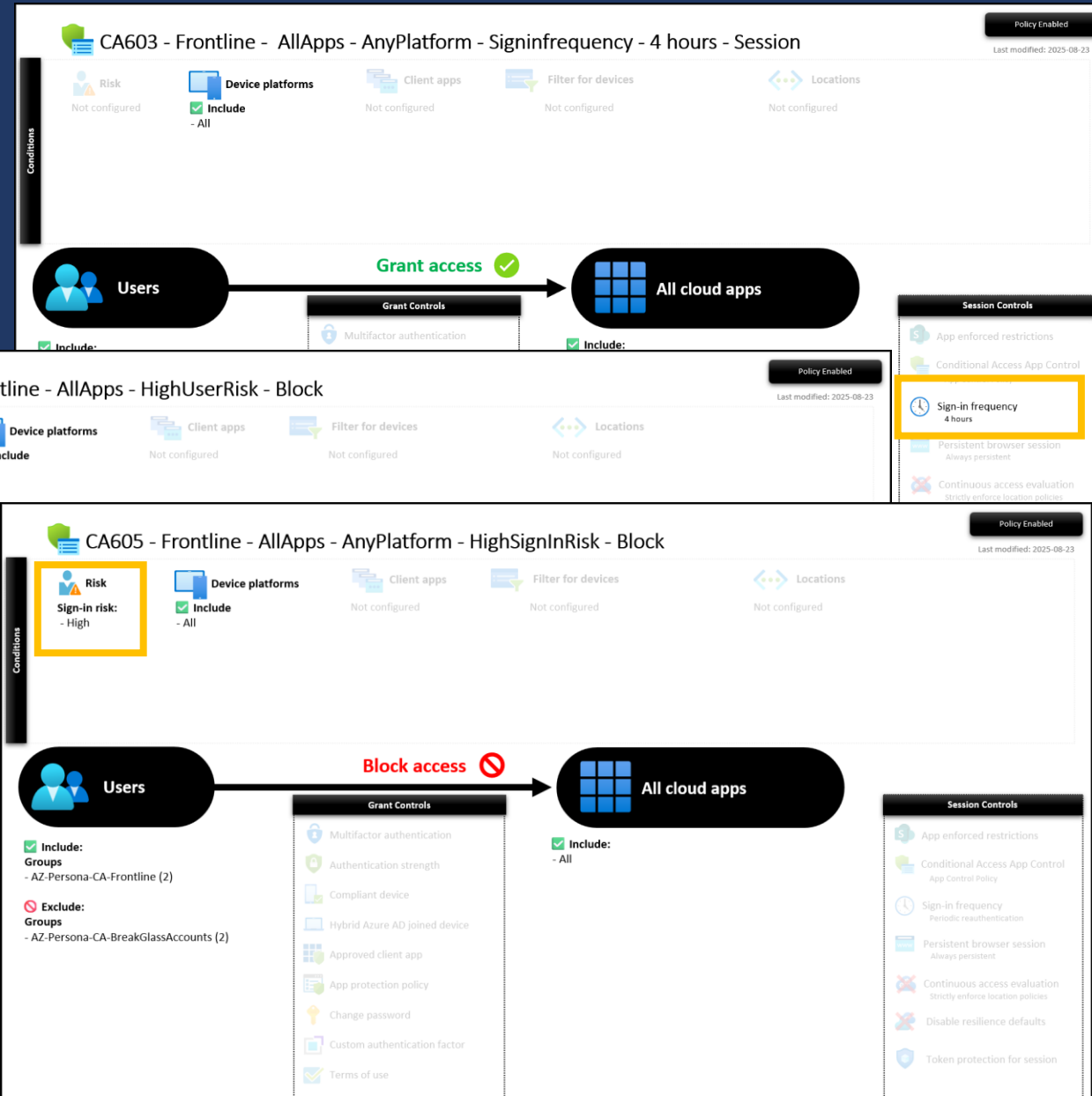
CA601 - Frontline - AllApps - iOSorAndroid - Compliant - Grant

CA602 - Frontline - AllApps - UnknownLocation - Block

CA603 - Frontline - AllApps - AnyPlatform - Signinfrequency - 4 hours - Session

CA604 - Frontline - AllApps - HighUserRisk - Block

CA605 - Frontline - AllApps - AnyPlatform - HighSignInRisk - Block





Entra ID – Conditional Access, My Staff

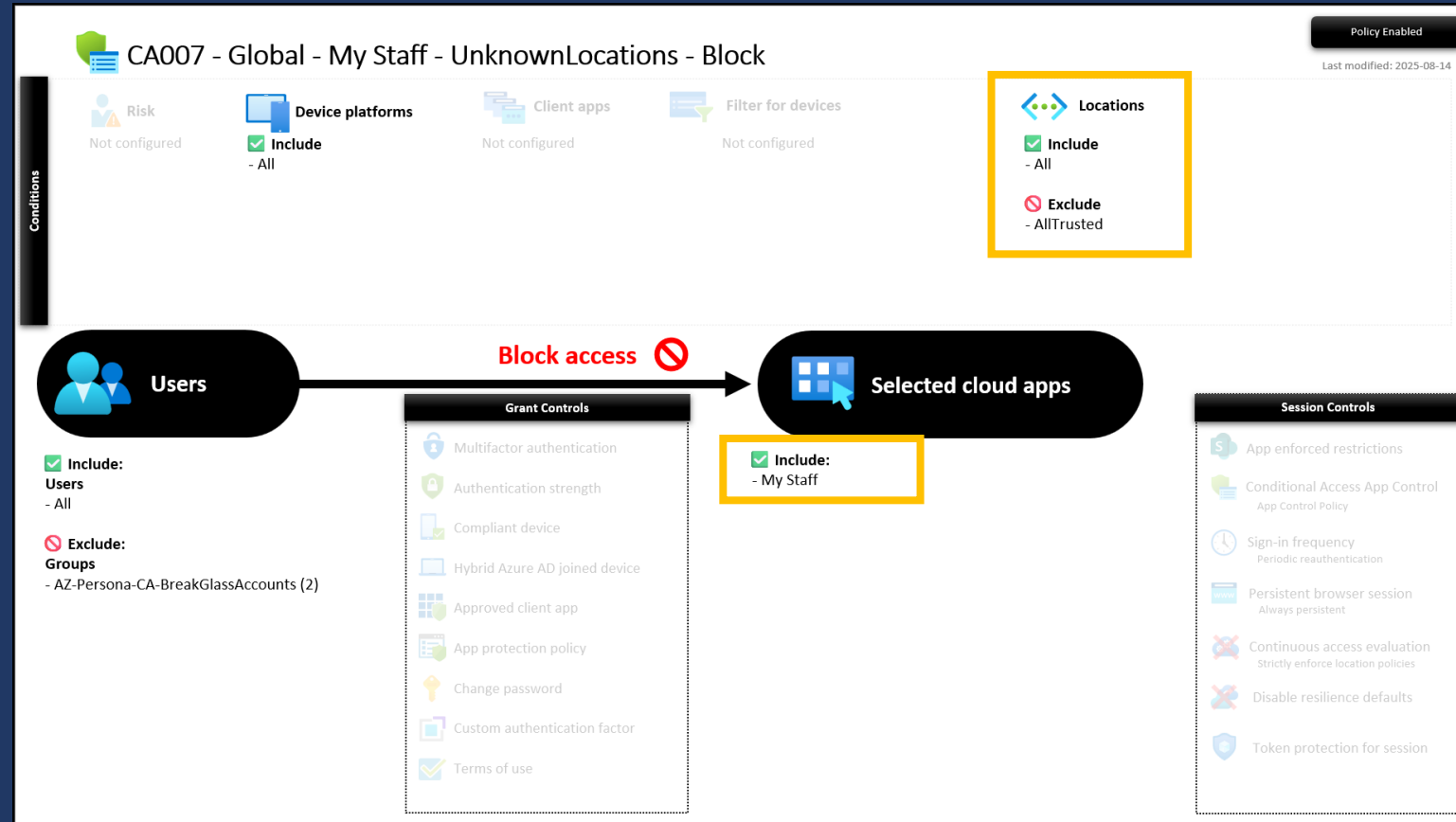
- Conditional Access Policies is Microsoft's Zero Trust policy engine, the Firewall of Cloud Identity.

ca0

7 out of 46 policies found

Policy name

CA007 - Global - My Staff - UnknownLocations - Block





Entra ID – Privileged Identity Management, My Staff

- Avoid standing permissions using PIM.

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

Home > Conditional Access | Policies > Roles and administrators | All roles > Users > Justin Time

Justin Time | Assigned roles

User

Search

+ Add assignments Refresh Got feedback?

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal na...	Scope
User Administrator	justin.time@skot...	The Storyline Dept. (Administrators)
Privileged Authentication Administrator	justin.time@skot...	The Storyline Dept. (Administrators)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

New support request

Entra ID – Privileged Identity Management, My Staff



- Avoid standing permissions using PIM.
 - Remove active assignments

The screenshot shows the Microsoft Entra admin center interface. The left navigation pane has 'Assigned roles' highlighted. The main content area shows the 'Assigned roles' page for the user 'Justin Time'. The 'Active assignments' tab is highlighted with a yellow box. Below the tabs, there is a search bar and a table with columns 'Role', 'Principal na...', and 'Scope'. The table currently shows 'No results'.

Entra ID – Privileged Identity Management, My Staff



- Avoid standing permissions using PIM.
 - Remove active assignments
 - Use eligible assignments

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links for Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, and Identity Secure Score. The main content area displays the 'Assigned roles' page for the user 'Justin Time'. The 'Eligible assignments' tab is highlighted, showing a table of roles assigned to the user.

Role	Principal name	Scope
User Administrator	justin.time@skothei...	The Storyline Dept. (Admi...
Privileged Authentication Administrator	justin.time@skothei...	The Storyline Dept. (Admi...

Entra ID – Privileged Identity Management Staff

- Avoid standing PIM.
 - Remove act
 - Use eligible

Edit role setting - Privileged Authentication Administrator

Privileged Identity Management | Microsoft Entra roles

Activation Assignment Notification

Activation maximum duration (hours)

On activation, require

☐ None

☐ Azure MFA

☒ Microsoft Entra Conditional Access authentication context

Learn more

☒ Require justification on activation

☐ Require ticket information on activation

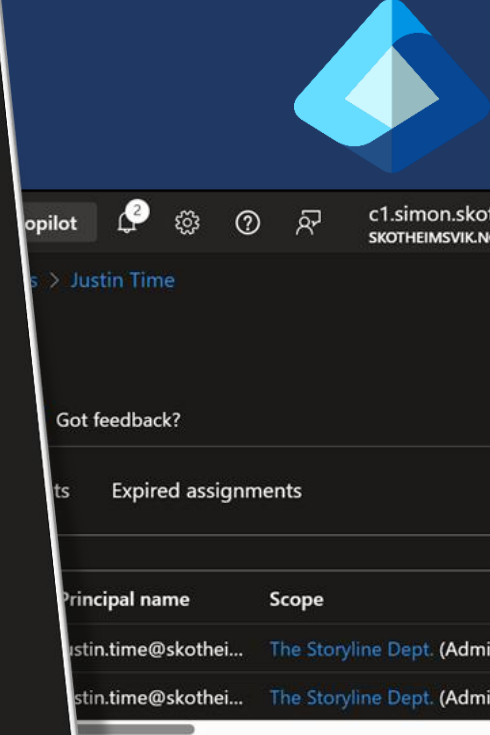
☐ Require approval to activate

1

Select

Require Reauth

Require Strong Auth



Entra ID – Privileged Identity Management, My Staff



- Avoid standing permissions using PIM.
 - Remove active assignments
 - Use eligible assignments
 - The manager must “PIM” into roles

The screenshot shows the 'My roles' page in the Microsoft Azure portal. The page title is 'My roles | Microsoft Entra roles' with the subtitle 'Privileged Identity Management | My roles'. The user is logged in as 'justin.time@skotheimsvik.com'. The page has tabs for 'Eligible assignments', 'Active assignments', and 'Expired assignments'. The 'Eligible assignments' tab is selected, showing a table of roles. The table has columns for 'Role', 'Scope', and 'Action'. The 'Action' column contains 'Per...' and 'Activate' links. The 'Activate' links for the 'User Administrator' and 'Privileged Authentication Administrator' roles are highlighted in a yellow box.

Role	Scope	Action
User Administrator	The Storyline Dept. (Administrative Direct	Per... Activate
Privileged Authentication Administrator	The Storyline Dept. (Administrative Direct	Per... Activate

Entra ID – Privileged Identity Management, My Staff



- Avoid standing permissions using PIM.
 - Remove active assignments
 - Use eligible assignments
 - The manager must “PIM” into roles
 - Length and justification

The screenshot displays the Microsoft Azure Privileged Identity Management (PIM) 'Activate' interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. The main content area is titled 'Activate - Privileged Authentication Admini...' and shows the 'Activate' tab for a role. The 'Duration (hours)' slider is set to 1, and the 'Reason (max 500 characters)' text box contains the justification: 'I must help Paige Turner getting access.' The 'Activate' button is highlighted in blue.



Entra ID – Privileged Identity Management, My Staff

- Avoid standing permissions using PIM.
 - Remove active assignments
 - Use eligible assignments
 - The manager must “PIM” into roles
 - Length and justification
 - Role activation
 - Role is active

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Privileged Identity Management >

My roles | Microsoft Entra roles

Privileged Identity Management | My roles

Refresh Open in mobile Got feedback?

Activate

Microsoft Entra roles

Groups

Azure resources

Troubleshooting + Support

Your active assignments have changed. Click here to view your active assignments →

Eligible assignments Active assignments Expired assignments

Search by role

Role	Scope	Membership	End time	Action
User Administrator	The Storyline Dept. (Ad Direct)	Permanent	Activate	
Privileged Authentic...	The Storyline Dept. (Ad Direct)	Permanent	Activate	

Add or remove favorites by pressing Ctrl+Shift+F

Entra ID – Privileged Identity Management, My Staff



- Avoid standing permissions using PIM.
 - Remove active assignments
 - Use eligible assignments
 - The manager must “PIM” into roles
 - Length and justification
 - Role activation
 - Role is active
 - Active assignments

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > Privileged Identity Management >

My roles | Microsoft Entra roles

Privileged Identity Management | My roles

Refresh Open in mobile Got feedback?

Activate

- Microsoft Entra roles
- Groups
- Azure resources
- Troubleshooting + Support

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Scope	Member...	State	End time	Action
Privileged Authentication A...	The Storyline	Direct	Activated	8/29/2025, 3:10:38 PM	Deactivate

Add or remove favorites by pressing Ctrl+Shift+F

PIM Require EntraID P2

My Workers Need PC

Mobile phone only!?
Give us access to Windows...



Windows 365 - Cloud PC

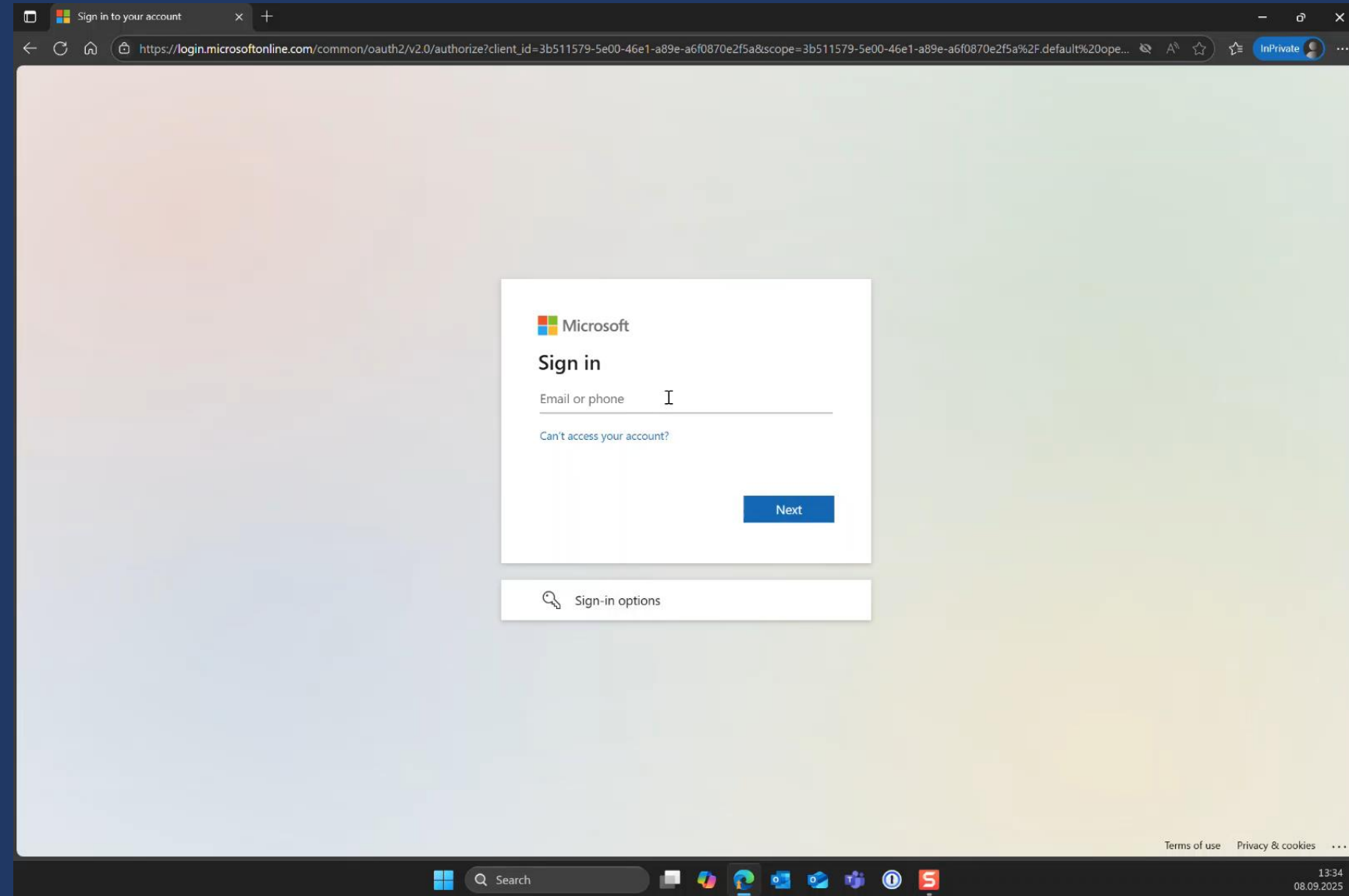
- Modern Windows experience from the cloud to shared devices
- 1:3 ratio of license and frontline workers



Windows 365 - Cloud PC



- Modern Windows experience from the cloud to shared devices
- 1:3 ratio of license and frontline workers
- FLW logs in



Windows 365 - Cloud PC

- Windows 365 Cloud PC
 - Windows 365 App
 - Windows 365 Web
 - Windows 365 Boot
 - Windows 365 Link

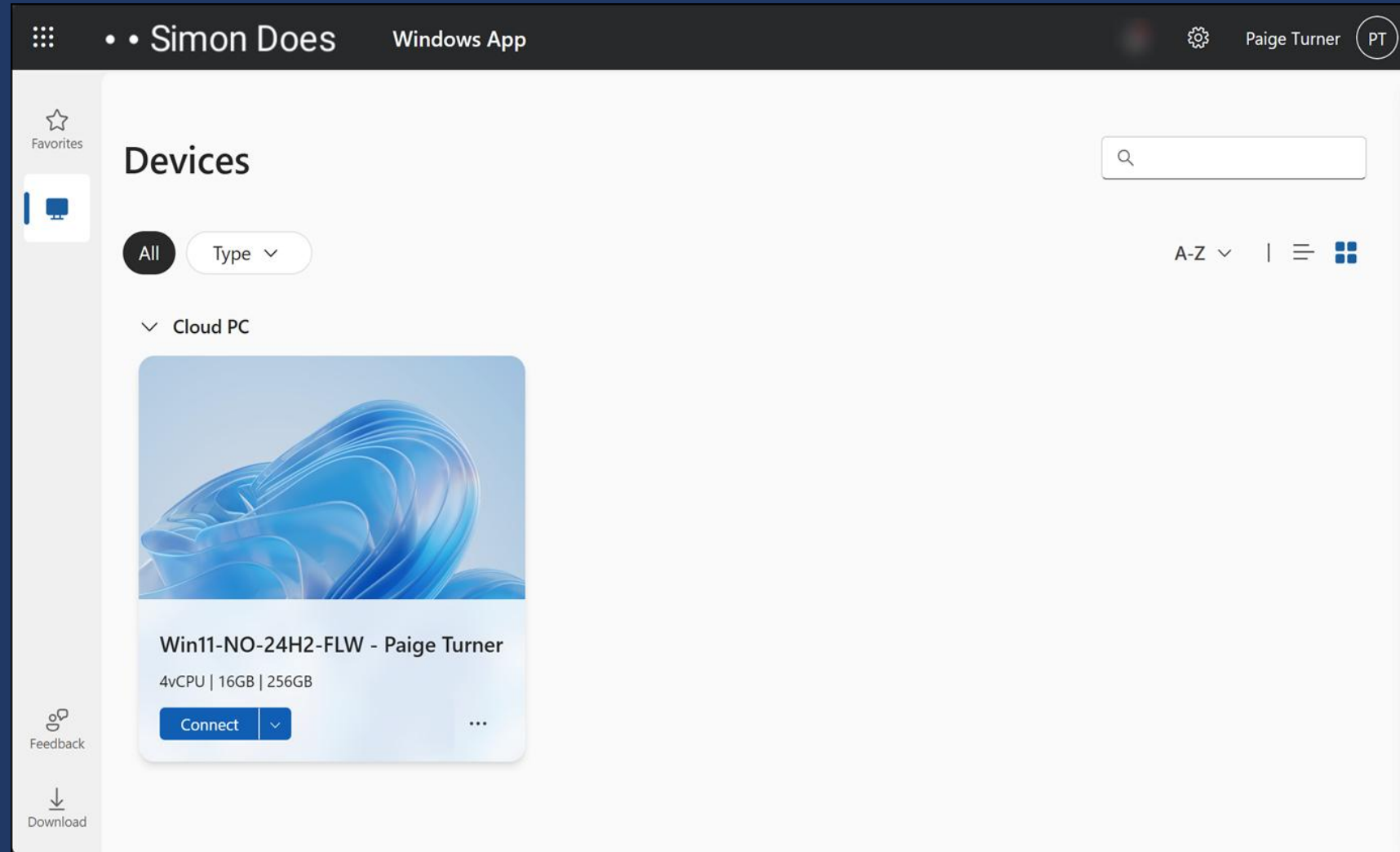
Windows App is the recommended application to connect to Windows 365 Cloud PCs and can be used on any device (Windows, macOS, iOS, iPadOS, Android, Chrome OS, Web browsers, Meta Quest VR headset (preview)).



Windows 365 - Cloud PC

- Windows 365 Cloud PC
 - Windows 365 App
 - Windows 365 Web
 - Windows 365 Boot
 - Windows 365 Link

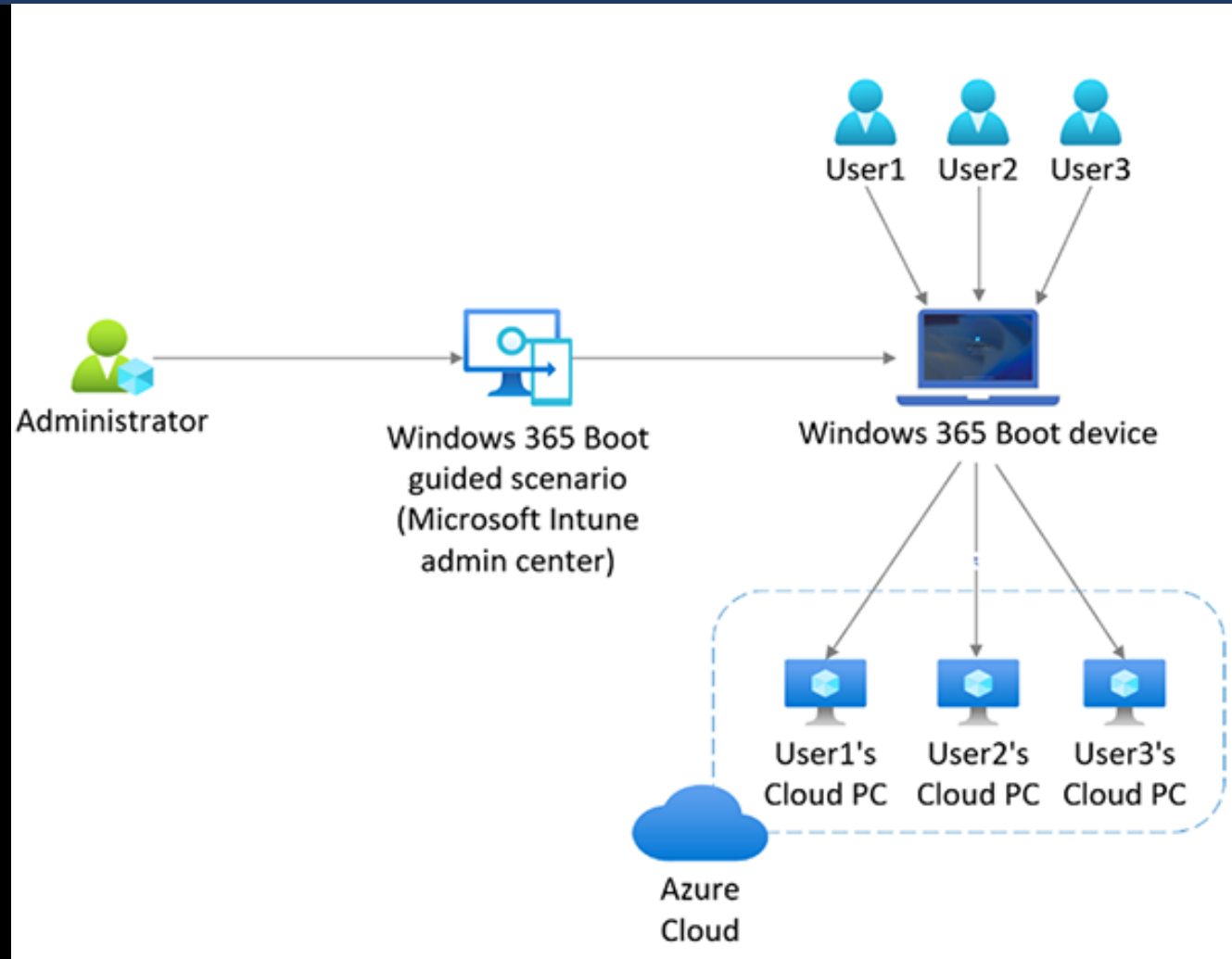
Users can access their Cloud PC from a website if they are on a supported operating system (Windows, macOS, ChromeOS, Linux) and using a modern browser like Edge, Chrome, Safari, Firefox, or LG webOS 23.



Windows 365 - Cloud PC

- Windows 365 Cloud PC
 - Windows 365 App
 - Windows 365 Web
 - Windows 365 Boot
 - Windows 365 Link

Windows 365 Boot allows administrators to configure Windows 11 physical devices so that when a user turns on the physical device and signs in, Windows 365 Boot signs them in directly to their Cloud PC, bypassing the physical device.



GA 16.09.2025!

Windows 365 - Cloud PC

- Windows 365 Cloud PC
 - Windows 365 App
 - Windows 365 Web
 - Windows 365 Boot
 - Windows 365 Link

Maximize productivity with Cloud PC devices that connect in seconds to Windows 365 and offer responsive, high-fidelity experiences.

Reduce your attack surface with Cloud PC devices that have no local data, adminless users, and passwordless authentication using Microsoft Entra ID



This Smells Expensive!

We need to be aware of the cost, while keeping everything easy and secure



Microsoft 365 Licensing

- **BYOD Scenario**
 - **Microsoft 365 F1 (\$2.25)**
 - Basic access to Teams, SharePoint, and Yammer; no email or desktop apps, Conditional Access
- **F5 Security Addon**
 - Risk-based Conditional Access, PIM, Defender for Office, ++

Microsoft 365 Licensing

- **BYOD Scenario**

- **Microsoft 365 F1 (\$2.25)**

- Basic access to Teams, SharePoint, and Yammer; no email or desktop apps, Conditional Access

- **F5 Security Addon**

- Risk-based Conditional Access, PIM, Defender for Office, ++

Shared Device Scenario

- **Microsoft 365 F3 (\$8)**

- Includes Teams, email, Office apps (web/mobile), and security features, Conditional Access

- **F5 Security Addon**

- Risk-based Conditional Access, PIM, Defender for Office, ++

Microsoft 365 Licensing

• BYOD Scenario

- Microsoft 365 F1 (\$2.25)
 - Basic access to Teams, SharePoint, and Yammer; no email or desktop apps, Conditional Access
- F5 Security Addon
 - Risk-based Conditional Access, PIM, Defender for Office, ++

Shared Device Scenario

- Microsoft 365 F3 (\$8)
 - Includes Teams, email, Office apps (web/mobile), and security features, Conditional Access
- F5 Security Addon
 - Risk-based Conditional Access, PIM, Defender for Office, ++

Cloud PC Scenario

- Microsoft 365 F3 (\$8)
 - Basic access to Teams, SharePoint, and Yammer; no email or desktop apps
 - Conditional Access
- F5 Security Addon
 - Defender for Office, ++
- Windows 365 Frontend (\$50/3)
 - Windows Cloud PC

Hardware Options

Shared Mobile/Tablet

- Android Phone (\$500)
- Android Tablet (\$500)
- iPhone (\$700)
- iPad (\$500)



Windows 365 Boot

- Windows Desktop (\$500)
- Windows Laptop (\$600)



Windows 365 Link (\$349)

Not yet available in my region, what about yours?



QR Alternative

- Fido Key (\$40+)



Communication



Communication



Communication



www.expertslive.co.uk



The Challenge:

Onboard
and Involve
Mobile First Users

Thank you!

Please remember to **rate our session.**



Ståle



Simon