The Challenge of Providing Secure Access to External Admins

Myron Helgering

Level: Intermediate

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

About me

- Solution Lead @ Pink Elephant
- Microsoft Security MVP
- Blogger and Speaker
- Fantasy geek

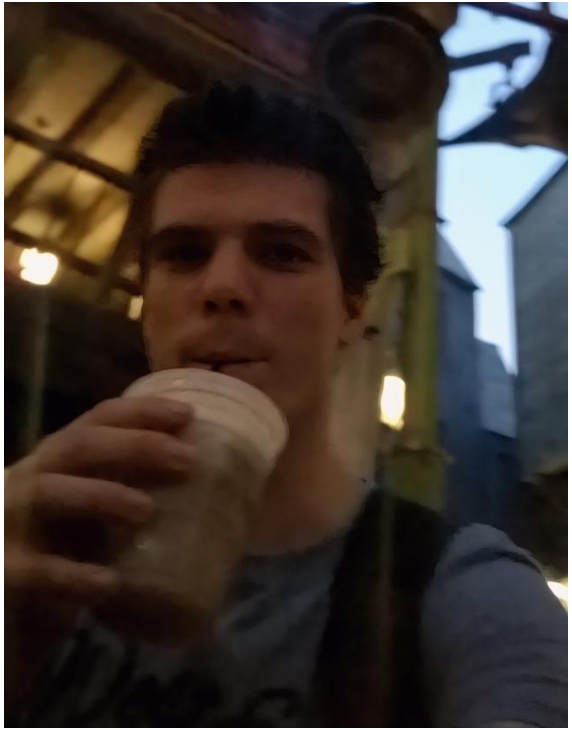
Myron Helgering

in/myronhelgering myronhelgering.com

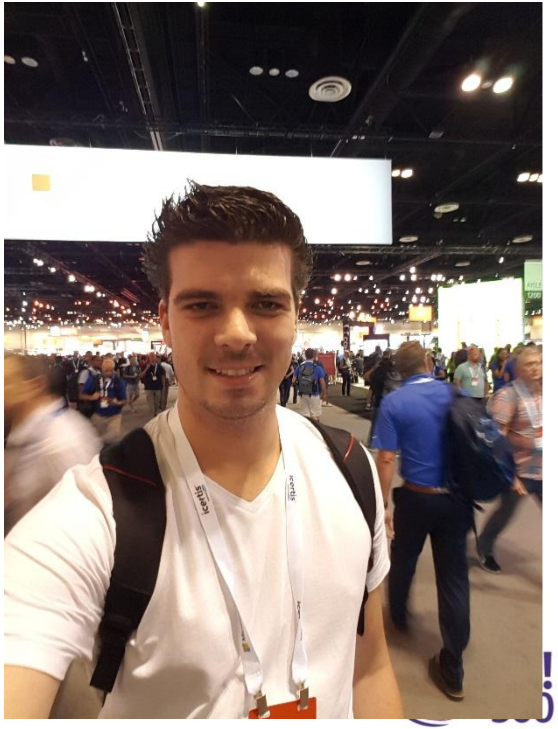
I 💘 Orlando

2007

2016



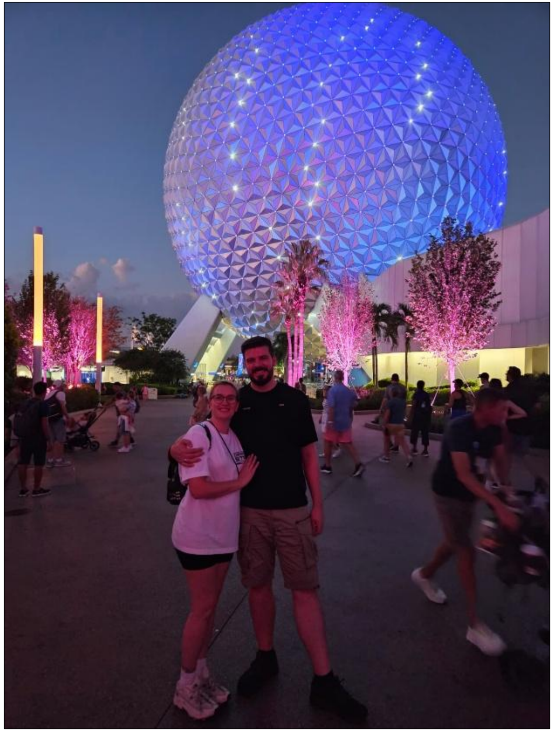
2018



I 💘 Orlando

2019

2024



2025

LIVE! 360 TECH CON 2025
ORLANDO
FLORIDA
Cybersecurity & Ransomware LIVE!
DEFENDING AGAINST RANSOMWARE AND OTHER ATTACKS
Banda Sea 2

Cybersecurity & Ransomware Live! Pre-Con Hands-On Lab: Sunday, Nov 16

9:00 AM - 6:00 PM CRHOL01 Hands-On Lab: Protect, Detect, Respond with Microsoft Defender XDR - Stefan Schörling & Mattias Borg

Cybersecurity & Ransomware Live! Pre-Con Workshops: Monday, Nov 17

8:30 AM - 5:30 PM CRM01 Workshop: Designing a Privileged Access Management Solution - Sami Laiho

Cybersecurity & Ransomware Live! Day 1: Tuesday, November 18

8:00 AM - 9:00 AM Cybersecurity & Ransomware Live! Keynote: 2026 Ransomware State of the Union - Sami Laiho, Chief Research Officer, Adminize

9:15 AM - 10:30 AM CRT02 Using Security Copilot and Defender XDR to Streamline Your SOC - John O'Neill Sr.

1:30 PM - 1:50 PM CRT04 Fast Focus: Connect Securely to Your Home Network Without a Single Firewall Port Open - Sami Laiho

2:00 PM - 2:20 PM CRT06 Fast Focus: Elevate to Admin on Demand - Sami Laiho

2:45 PM - 4:00 PM CRT08 When Hackers Collide – Unleashing Sticky Data Protection - Andy Malone

4:15 PM - 5:30 PM CRT10 Unlocking Next-Gen Cloud Security: What's New in Microsoft Defender for Cloud - Markus Lintuala

Cybersecurity & Ransomware Live! Day 2: Wednesday, November 19

8:00 AM - 9:15 AM CRW02 What Security Engineers and Developers Must Know About Azure AI Solutions - Markus Lintuala

9:30 AM - 10:45 AM CRW04 Automated Data Security: Identifying Sensitive Data with Microsoft Purview - Myron Helgering

2:00 PM - 3:15 PM CRW06 Improve Your Resilience with Cybersecurity Table-top Exercises - Stefan Schörling & Mattias Borg

4:00 PM - 5:15 PM CRW08 BYOAI: Bring Your Own AI to the Cybersecurity Fight - Michael Van Horenbeeck

Cybersecurity & Ransomware Live! Day 3: Thursday, November 20

8:00 AM - 9:15 AM CRH01 Securing, Managing and Hacking Microsoft Copilot - Stephen L. Rose

9:30 AM - 10:45 AM CRH03 Building a Resilient Incident Response Team: Beyond Playbooks and Tools - John O'Neill Sr.

11:00 AM - 12:00 PM Cybersecurity & Ransomware Live! Panel Discussion: How to Not Get Hacked in 2026 - Sami Laiho (moderator) Erica Burgess, Michael Niehaus, Stefan Schörling, & Michael Van Horenbeeck

1:00 PM - 2:15 PM CRH05 Six Methods to Protect Your Business From the Threat of Unmanaged Devices - Myron Helgering

2:30 PM - 3:45 PM CRH07 Why Domain Tiering is Critical to Prevent Ransomware - Sami Laiho

Agenda

01 | Introduction

02 | Access through User Account

03 | Access through Guest Account

04 | Access through GDAP

05 | Takeaways

06 | Q&A

Why this session?

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

What is the challenge?

- Organizations are not prepared for external admins
- Balancing security risks
- Option may result in bad user experience
- External admins work from their own device

Three options to grant access

1

Access through **User** Account

2

Access through **Guest** Account

3

Access through **GDAP**

Types of external admins

Consultant

MSP

Freelancer

MSSP

Four aspects to take into account

- User Experience
- Device Compliance
- Permissions
- Security

Three options to grant access

1

Access through **User** Account

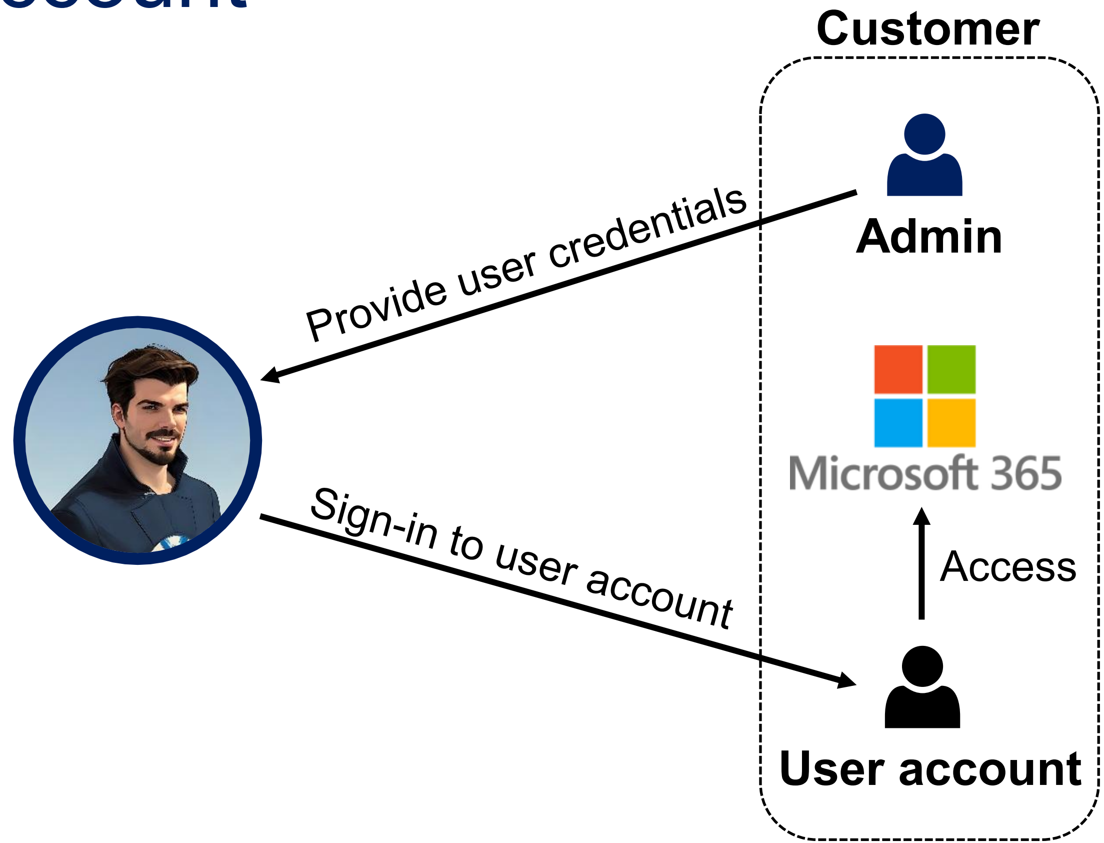
2

Access through **Guest** Account

3

Access through **GDAP**

User Account



Customer

Admin

Microsoft 365

Access

User account

Provide user credentials

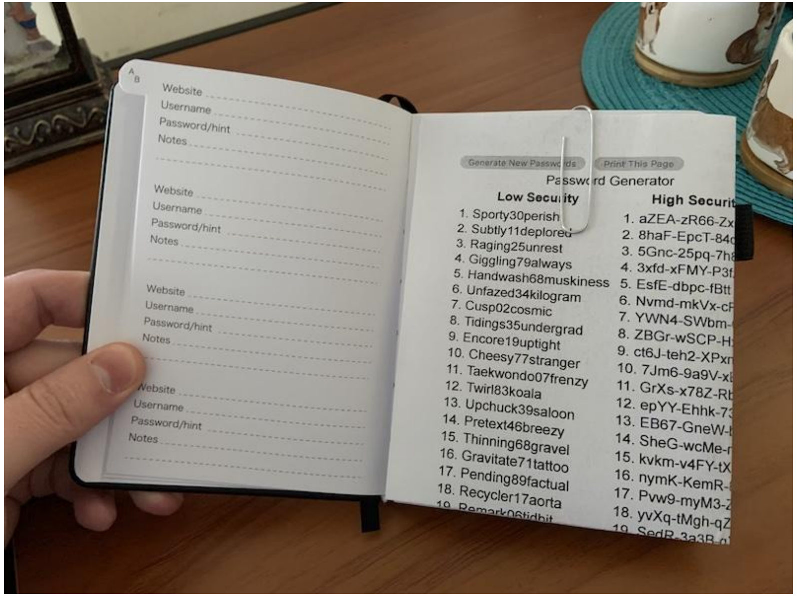
Sign-in to user account

Option 1: Access through User Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account				

Accounts for multiple customers

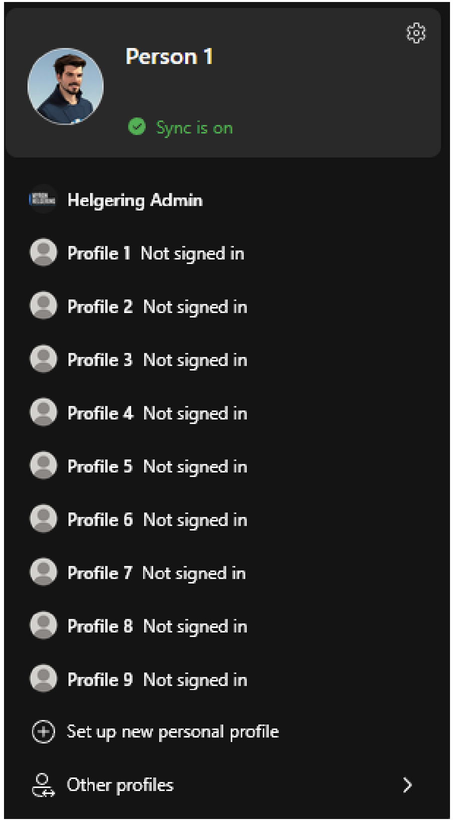
Accounts and passwords



Password Generator

Low Security	High Security
1. Sporty30perish	1. aZEA-zR66-Zx
2. Subtly11deplored	2. 8haF-EpcT-84
3. Raging25unrest	3. 5Gnc-25pq-7h
4. Giggling79always	4. 3xfd-xFMY-P3f
5. Handwash68muskiness	5. EsfE-dbpc-fBtt
6. Unfazed34kilogram	6. Nvmd-mkVx-cF
7. Cusp02cosmic	7. YWN4-SWbm-
8. Tidings35undergrad	8. ZBGr-wSCP-H
9. Encore19uptight	9. ct6J-teh2-XPxr
10. Cheesy77stranger	10. 7Jm6-9a9V-x
11. Taekwondo07frenzy	11. GrXs-x78Z-R
12. Twirl83koala	12. epYY-Ehhk-7
13. Upchuck39saloon	13. EB67-GneW-
14. Pretext46breezy	14. SheG-wcMe-
15. Thinning68gravel	15. kvkm-v4FY-tX
16. Gravitate71tattoo	16. nymK-KemR-
17. Pending89factual	17. Pvw9-myM3-
18. Recycler17aorta	18. yvXq-tMgh-qZ
19. Remark06tidbit	19. SedR-3a3B-q

Browser profiles



Person 1

Sync is on

Helgering Admin

Profile 1 Not signed in

Profile 2 Not signed in

Profile 3 Not signed in

Profile 4 Not signed in

Profile 5 Not signed in

Profile 6 Not signed in

Profile 7 Not signed in

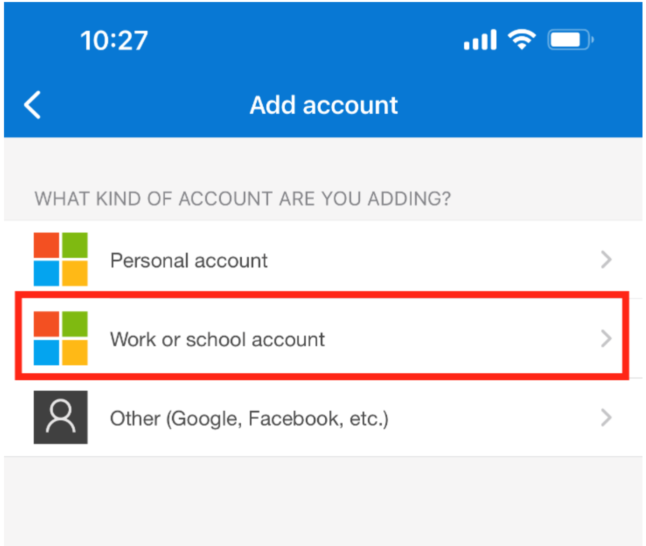
Profile 8 Not signed in

Profile 9 Not signed in

Set up new personal profile

Other profiles

MFA registrations



Add account

WHAT KIND OF ACCOUNT ARE YOU ADDING?

Personal account

Work or school account

Other (Google, Facebook, etc.)

User Experience after sign-in

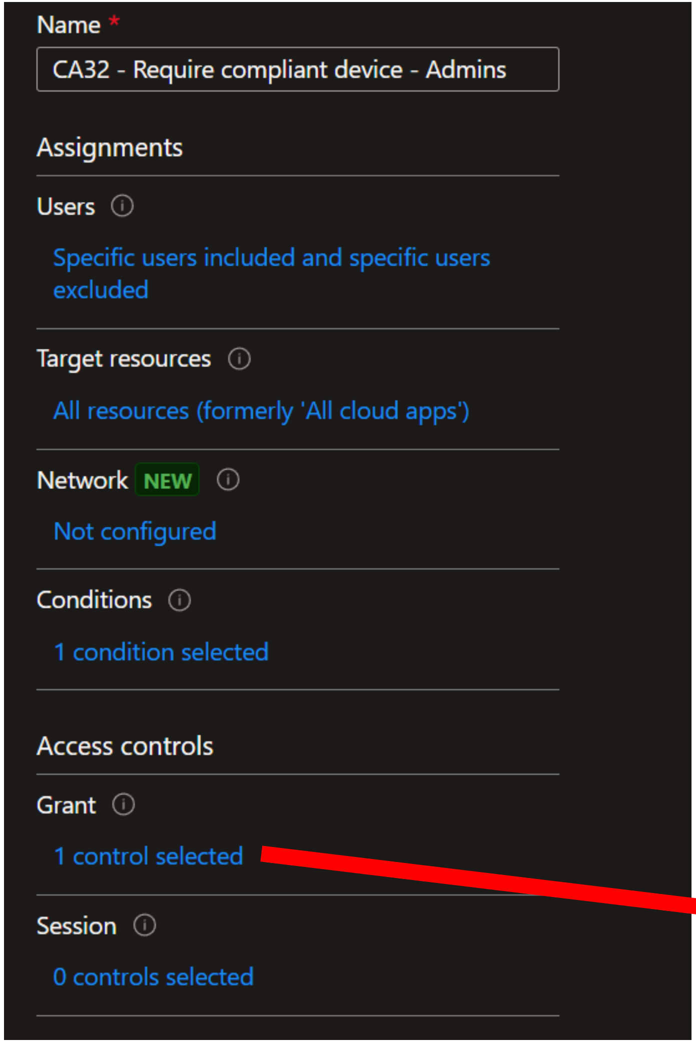
Option 1: Access through User Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	⭐⭐⭐			

Why managed and compliant device?

- Update OS and software and patch vulnerabilities
- Apply security configurations and policies
- Enable AV/EDR to protect against and detect threats
- Enable secure authentication methods
- Disable local admin rights
- Encrypt or fully wipe data on hard drive
- Restrict access whenever device is not compliant

Require compliant device with Conditional Access



Name *

CA32 - Require compliant device - Admins

Assignments

Users ⓘ

Specific users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Not configured

Conditions ⓘ

1 condition selected

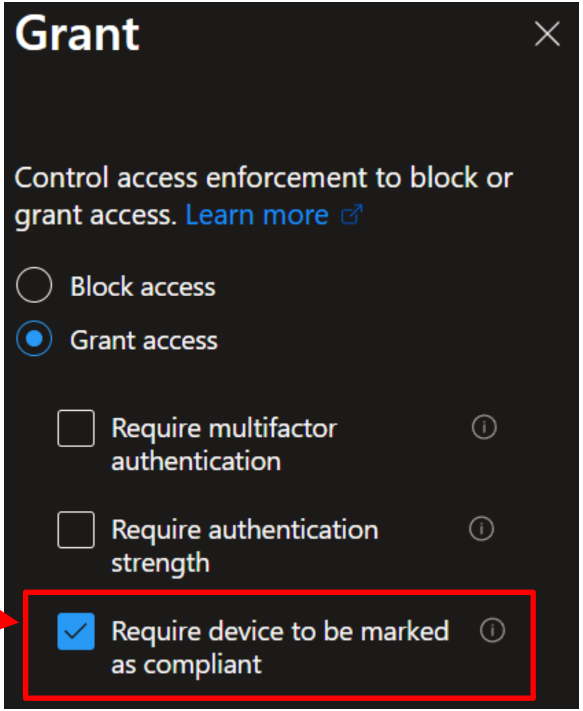
Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected



Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

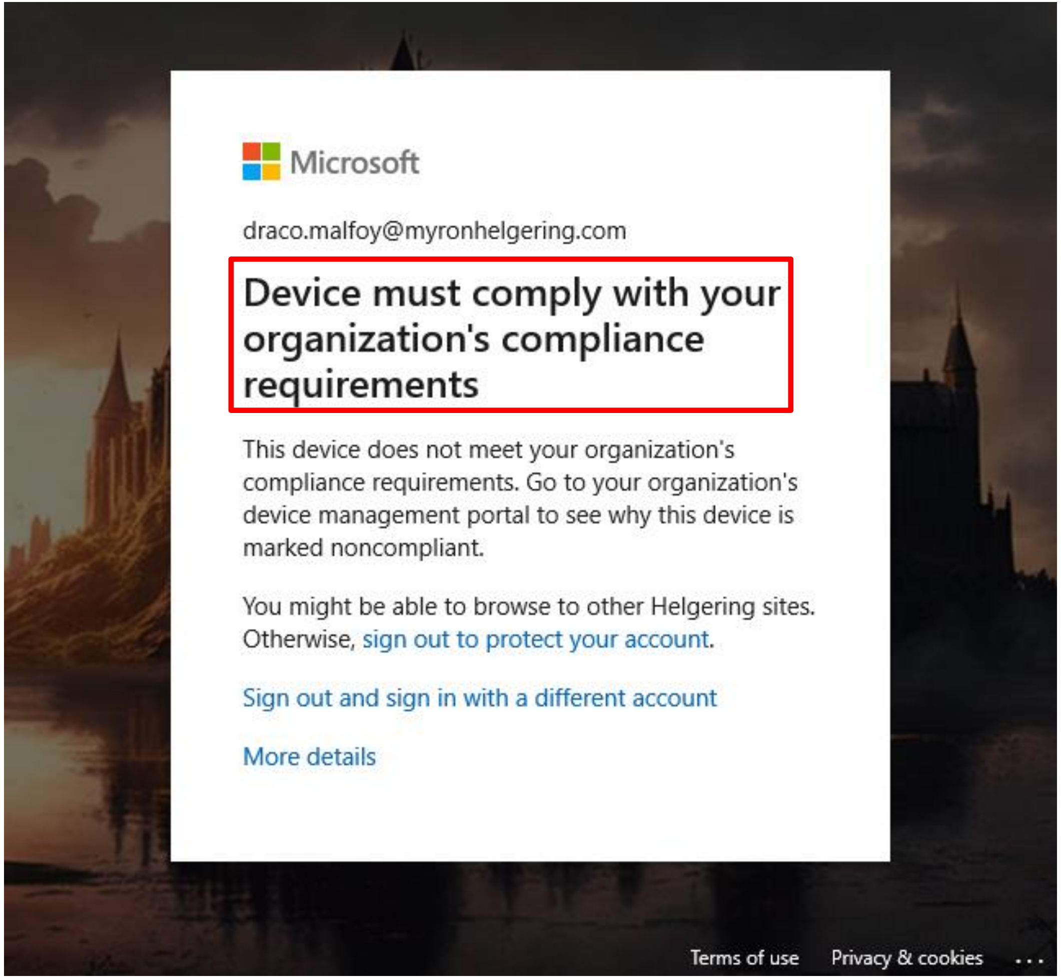
□ Require multifactor authentication ⓘ

□ Require authentication strength ⓘ

☑ Require device to be marked as compliant ⓘ

LIVE! 360

TECH EVENTS WITH PERSPECTIVE



Microsoft

draco.malfoy@myronhelgering.com

Device must comply with your organization's compliance requirements

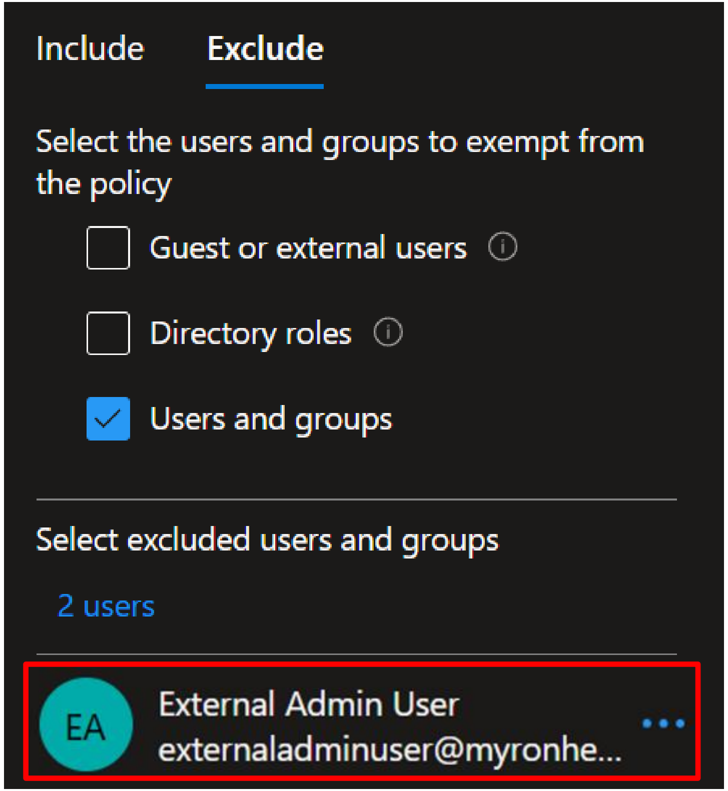
This device does not meet your organization's compliance requirements. Go to your organization's device management portal to see why this device is marked noncompliant.

You might be able to browse to other Helgering sites. Otherwise, sign out to protect your account.

Sign out and sign in with a different account

More details

Sign in with unmanaged device



Include Exclude

Select the users and groups to exempt from the policy

□ Guest or external users ⓘ

□ Directory roles ⓘ

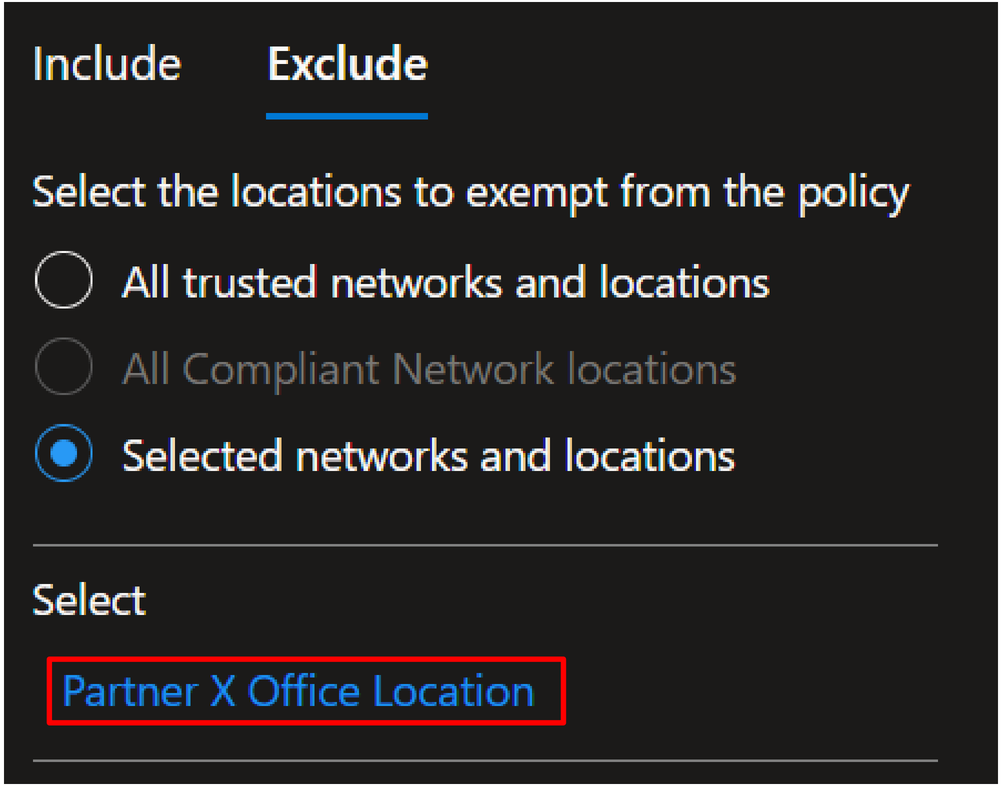
☑ Users and groups

Select excluded users and groups

2 users

EA External Admin User
externaladminuser@myronhe... •••

Exclude external admin user



Include Exclude

Select the locations to exempt from the policy

○ All trusted networks and locations

○ All Compliant Network locations

● Selected networks and locations

Select

Partner X Office Location

Exclude external admin location

Is the device compliant?
Probably not

THIS IS FINE

Actual solutions

- **Give external admins managed device**

Give external admins a device

LIVE! 360

TECH EVENTS WITH PERSPECTIVE

General

Other solutions

- Give external admins managed device
- **Windows 365 Cloud PC or Azure Virtual Desktop**

Windows 365 Cloud PC

- Easy to setup
- Fixed monthly cost
- Desktop per user

Azure Virtual Desktop

- Complex setup
- Pay-as-you-go
- Supports multi-session

Other solutions

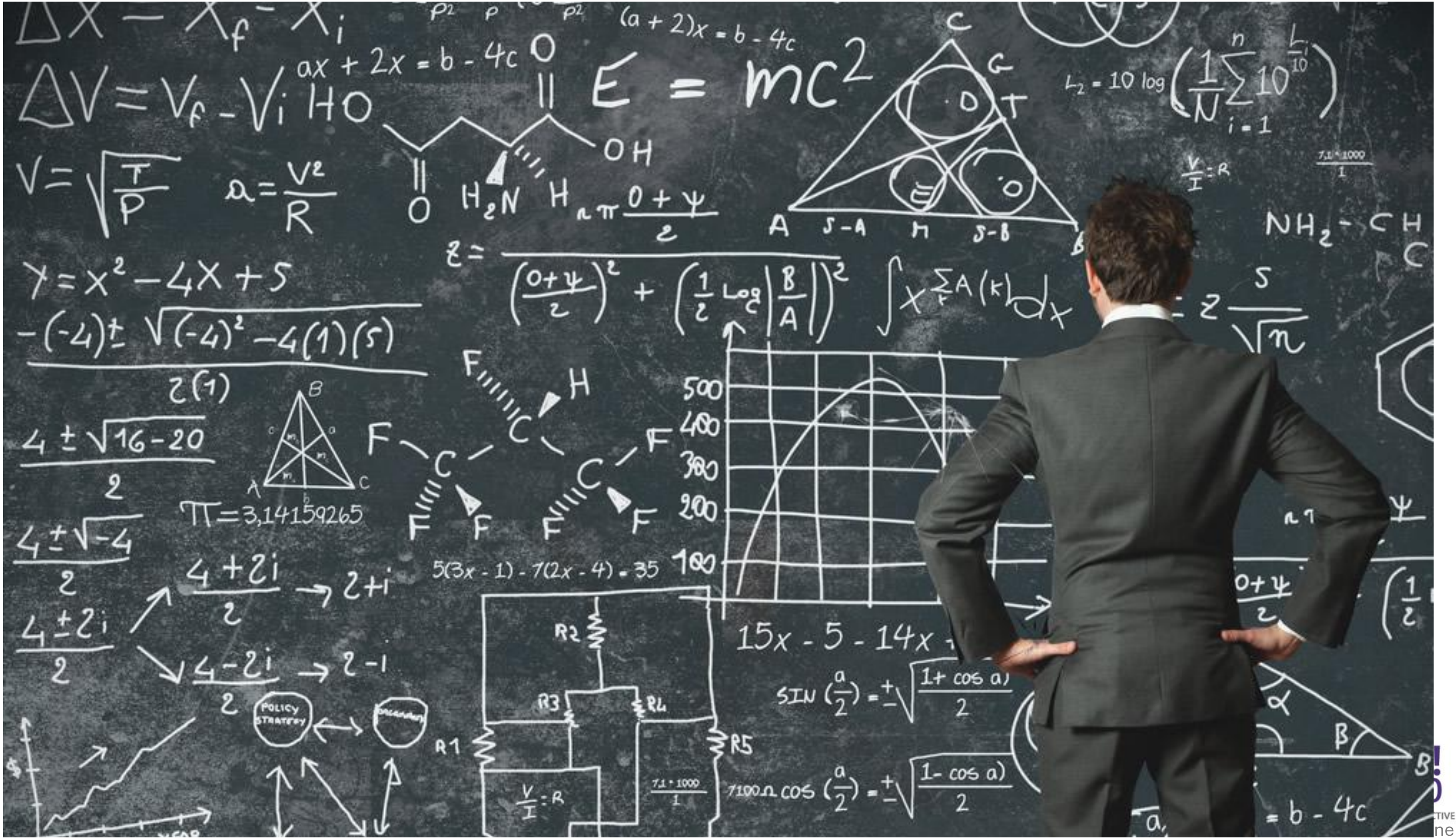
- Give external admins managed device
- Windows 365 Cloud PC or Azure Virtual Desktop
- **Privileged Access Workstation (PAW)**

Privileged Access Workstation (PAW)

- Can be physical or virtual
- Used only for administrative tasks
- Smaller attack surface
- Configuration hardening

PAW Configuration Hardening

- Restrict the use of applications
- Restrict web browsing
- No local admin rights
- Onboard and enable AV/EDR
- Deny BYOD device enrollment
- Strict security policies & configurations
- Only allow admin access from PAW


ΔX = X_f - X_i
(a + 2)x = b - 4c
ax + 2x = b - 4c
ΔV = V_f - V_i
HO
E = mc²
OH
O
H₂N
H
V = √(T/P)
a = V²/R
L₂ = 10 log (1/N Σ 10^(Lᵢ/10))
i = 1
n
V/I = R
7,1 * 1000 / 1
C
G
D
T
A
S-A
M
S-B
B
NH₂ - CH
z = (0+ψ)/2
Y = x² - 4X + 5
-(-4) ± √((-4)² - 4(1)(5))
2(1)
4 ± √(16-20)
2
4 ± √-4
2
4 + 2i
2
2 + i
4 ± 2i
2
4 - 2i
2
2 - i
π = 3,14159265
F
H
C
5(3x - 1) - 7(2x - 4) = 35
500
400
300
200
100
15x - 5 - 14x
SIN (a/2) = ± √((1 + cos a)/2)
7100Ω cos (a/2) = ± √((1 - cos a)/2)
R1
R2
R3
R4
R5
V/I = R
7,1 * 1000 / 1
POLICY STRATEGY
α
β
= b - 4c
$
YEAR

TIVE
neral

Option 1: Access through User Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	⭐⭐⭐	⭐		

Permissions

- Privileged Identity Management (PIM) ✅
- Role Based Access Control (RBAC) ✅
- Access Packages & Reviews ✅

Option 1: Access through User Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	

MSP perspective

Security

- Upsides
  - Permissions (PIM, Access Packages & Reviews) ✅
  - Device compliance is possible ✅
  - Full visibility in sign-in and audit logs ✅
- Downsides
  - Device compliance can be hard to achieve ⚠️
  - MSP managing account security is (almost) impossible ⛔

Option 1: Access through User Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	★★★	★	★★★	★★★

Three options to grant access

1

Access through **User** Account

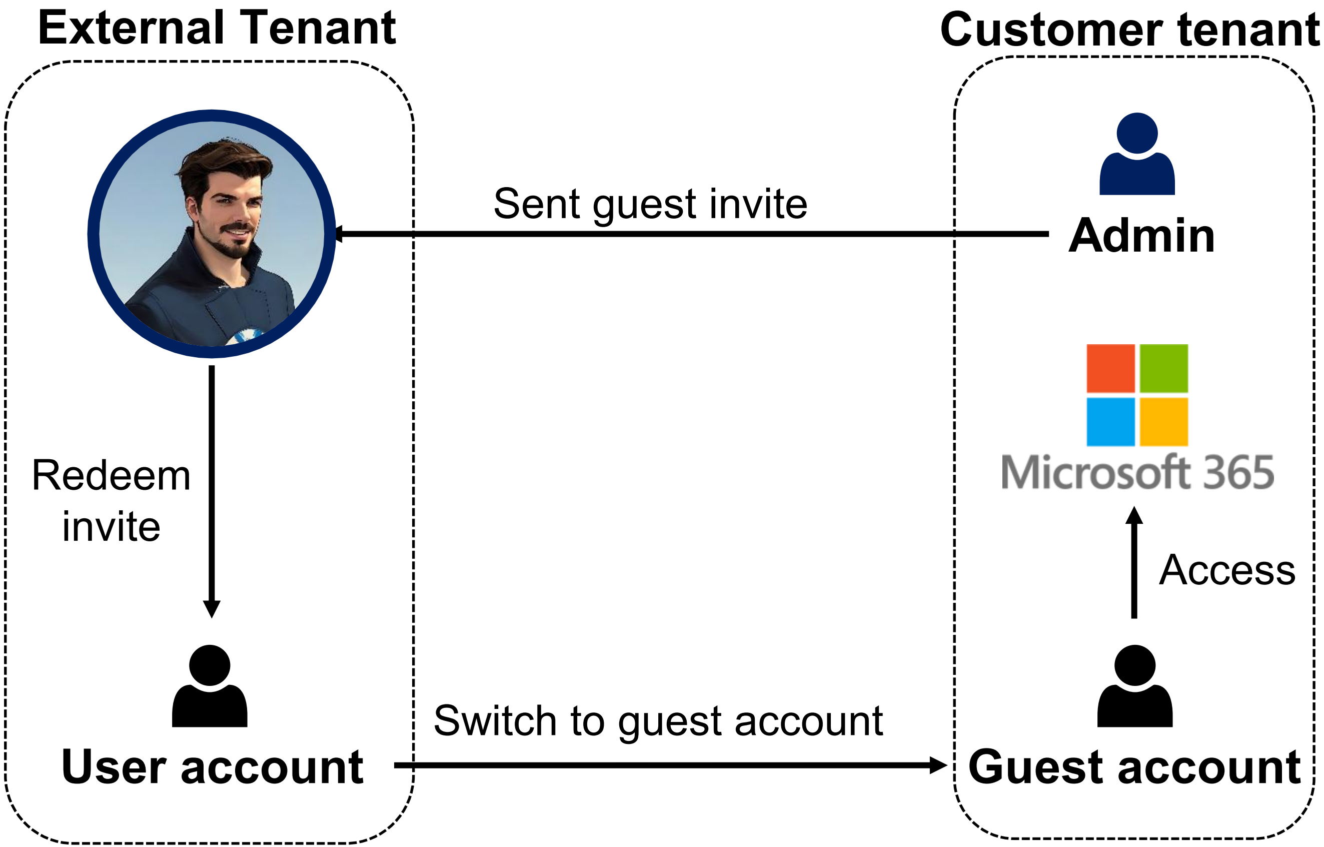
2

Access through **Guest** Account

3

Access through **GDAP**

Guest account



External Tenant

Customer tenant

Sent guest invite

Admin

Redeem invite

Microsoft 365

Access

User account

Switch to guest account

Guest account

Option 2: Access through Guest Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	★ ★ ★	★	★ ★ ★	★ ★ ★
Guest Account				

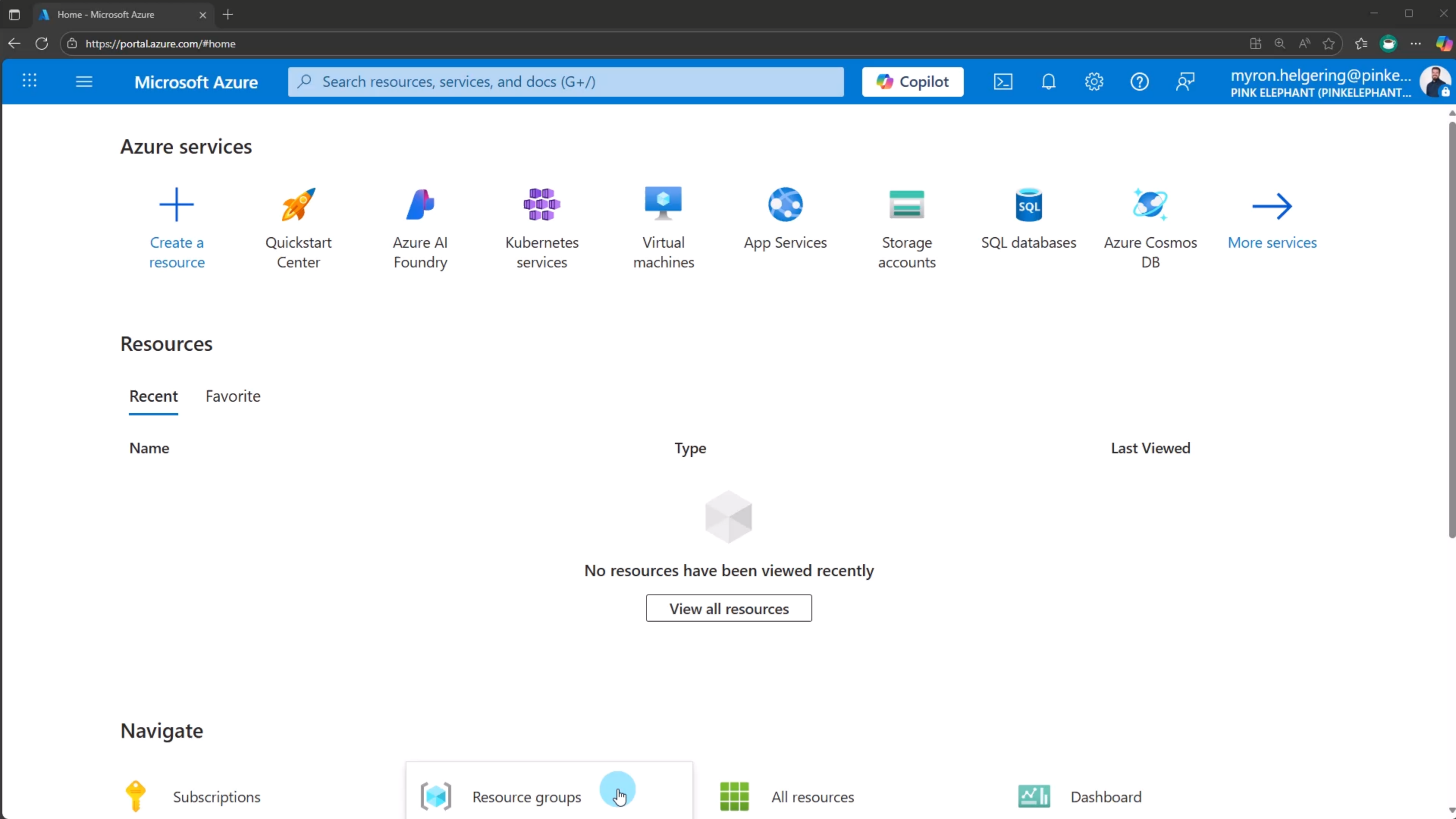
Four jobs to do

- Start a virtual machine in **Azure management portal**
- View message center in **M365 admin center**
- View onboarded devices in **Defender admin center**
- Close an eDiscovery case in **Purview admin center**

Preparation before demo

- Invite guest user to the Helgering tenant
- Gave access to **Global Administrator** role through PIM
- Gave access to the **Azure Subscription** through PIM
- Redeem the guest user invitation
- Register and authenticate with MFA

Demo: Admin Portals access with Guest Account



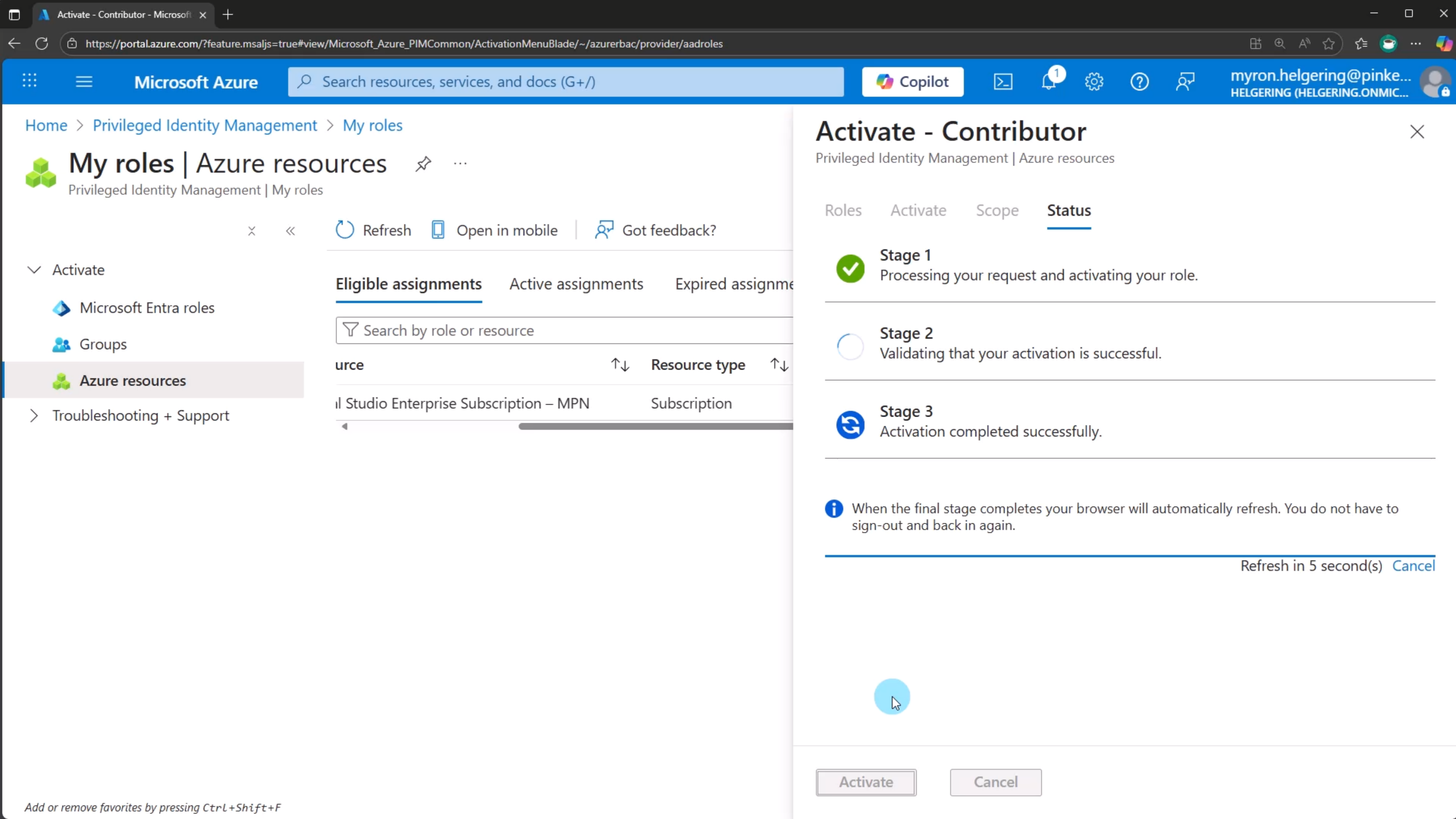
Azure services

Resources

Name	Type	Last Viewed

No resources have been viewed recently

Navigate


Activate - Contributor - Microsoft
https://portal.azure.com/?feature.msaljs=true#view/Microsoft_Azure_PIMCommon/ActivationMenuBlade/~/azurerbac/provider/aadroles
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
1
myron.helgering@pinke...
HELGERING (HELGERING.ONMIC...
Home > Privileged Identity Management > My roles
My roles | Azure resources
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 assignme
Search by role or resource
urce
Resource type
ıl Studio Enterprise Subscription – MPN
Subscription
Add or remove favorites by pressing Ctrl+Shift+F
Roles
Activate
Scope
Status
Activate
Cancel

Activate - Contributor

Privileged Identity Management | Azure resources

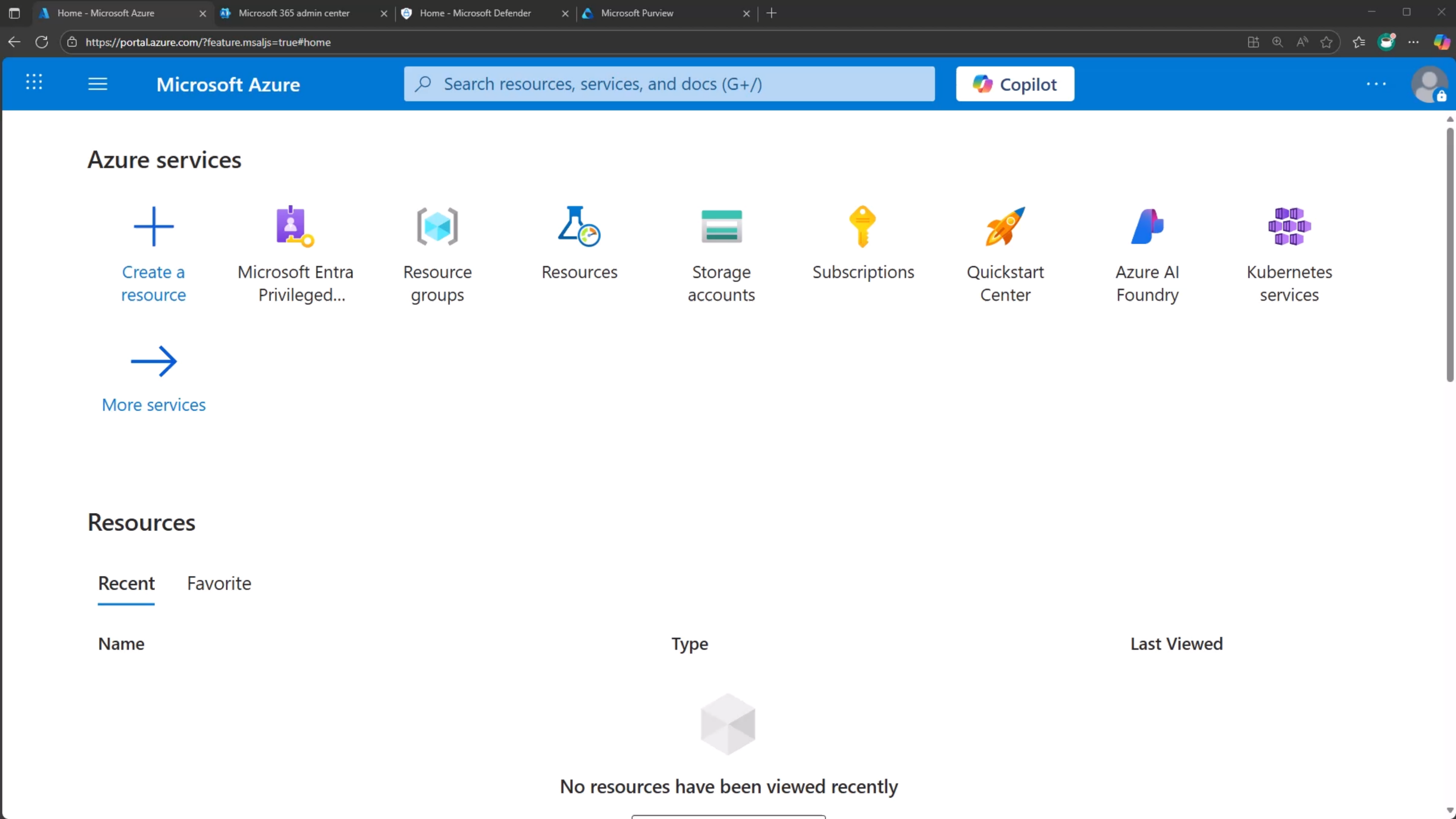
Stage 1
Processing your request and activating your role.

Stage 2
Validating that your activation is successful.

Stage 3
Activation completed successfully.

When the final stage completes your browser will automatically refresh. You do not have to sign-out and back in again.

Refresh in 5 second(s) Cancel



https://portal.azure.com/?feature.msaljs=true#home

Azure services

Resources

Name	Type	Last Viewed

No resources have been viewed recently

Admin Portal Access

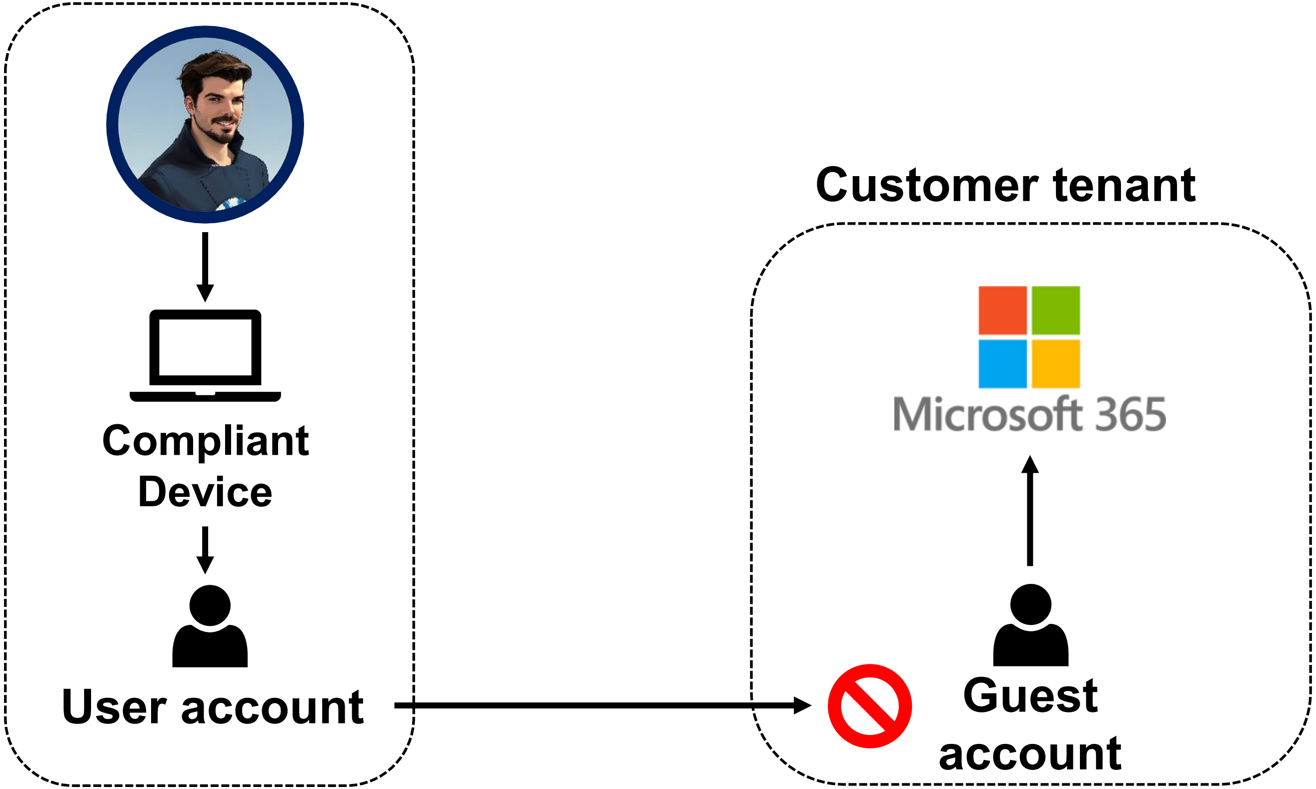
- Access ✅
  - **Azure Management** portal
  - **Entra** admin center
  - **Intune** admin center
  - **Defender** admin center (through MTO switch button)
- No access ⛔
  - **M365** admin center
  - **Exchange** admin center
  - **SharePoint Online** admin center
  - **Teams** admin center
  - **Power platform** admin center
- Access by pasting tenant ID 😅
  - **Purview** admin center

Option 2: Access through Guest Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	⭐⭐⭐
Guest Account	⭐			

Device Compliance as a Guest User

External tenant



Compliant Device

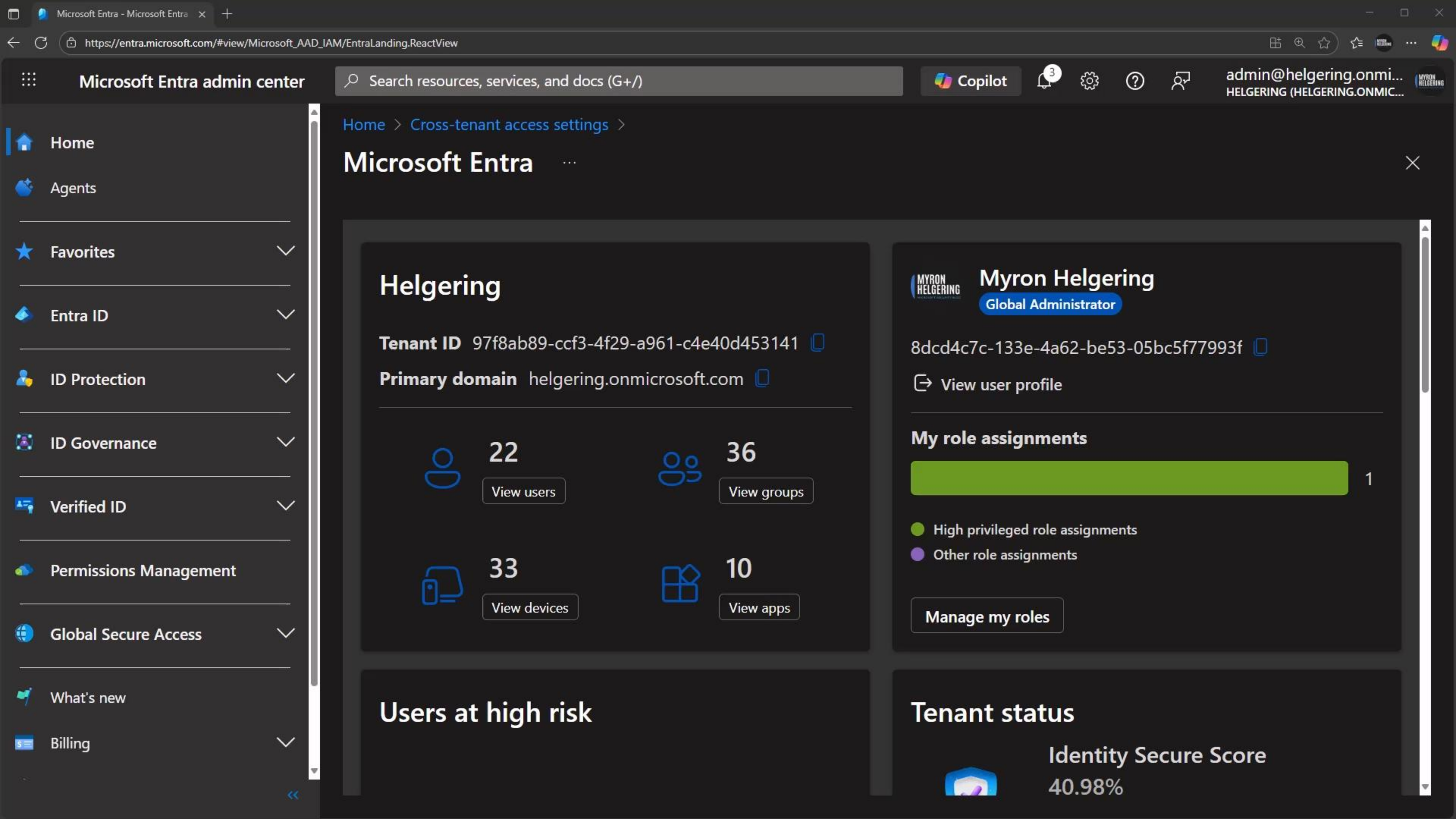
User account

Customer tenant

Microsoft 365

Guest account

Demo: Configuring cross tenant access settings in Microsoft Entra


Microsoft Entra - Microsoft Entra
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/EntraLanding.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
3
admin@helgering.onmi...
HELGERING (HELGERING.ONMIC...
Home
Agents
Favorites
Entra ID
ID Protection
ID Governance
Verified ID
Permissions Management
Global Secure Access
What's new
Billing
Home > Cross-tenant access settings >
View users
View groups
View devices
View apps
View user profile
Manage my roles

Microsoft Entra

Helgering

Tenant ID 97f8ab89-ccf3-4f29-a961-c4e40d453141

Primary domain helgering.onmicrosoft.com

22 View users

36 View groups

33 View devices

10 View apps

Myron Helgering

Global Administrator

8dcd4c7c-133e-4a62-be53-05bc5f77993f

My role assignments

1

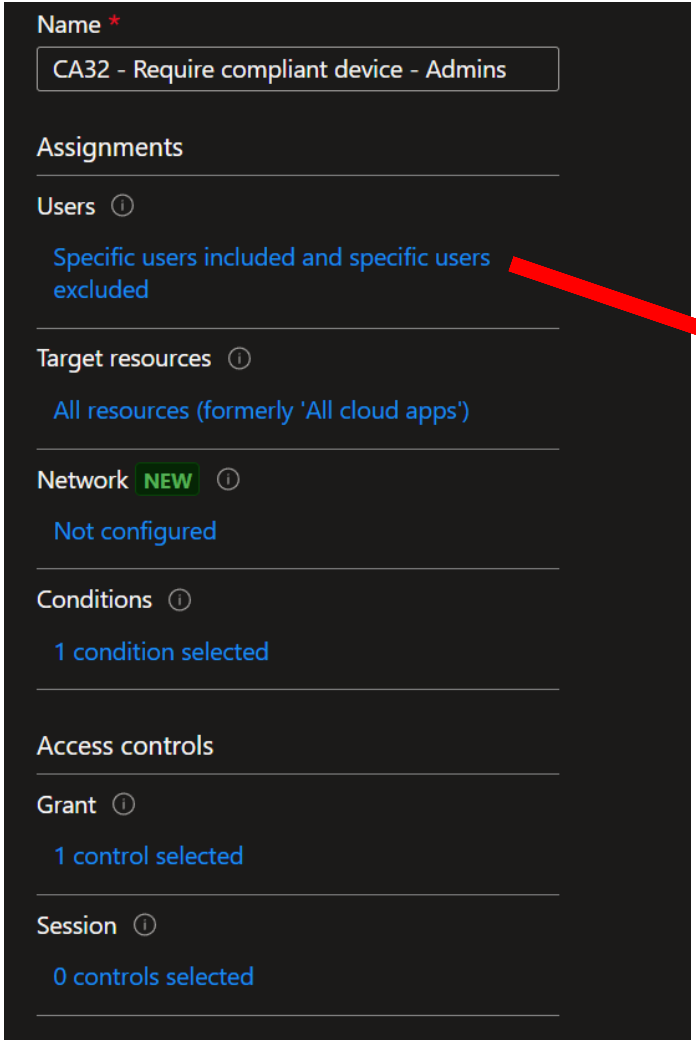
- 🟢 High privileged role assignments
- 🟣 Other role assignments

Users at high risk

Tenant status

Identity Secure Score

40.98%



Name *

CA32 - Require compliant device - Admins

Assignments

Users ⓘ

Specific users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Not configured

Conditions ⓘ

1 condition selected

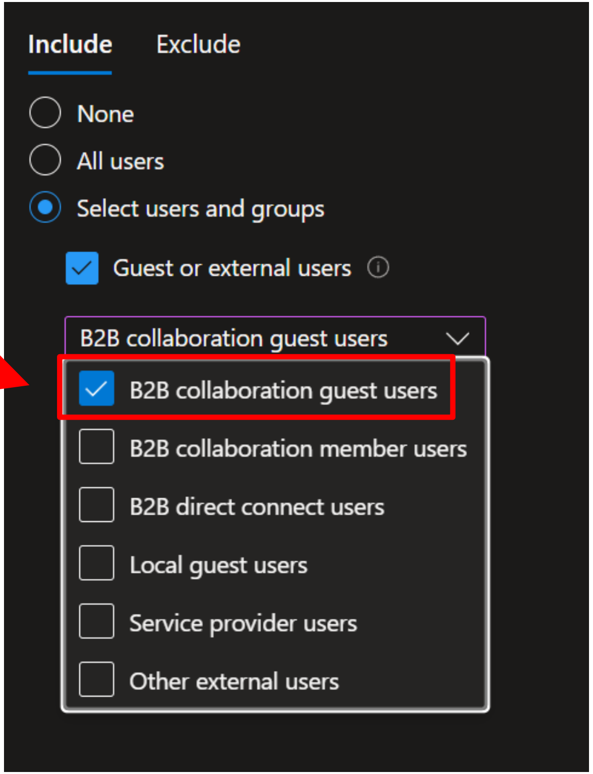
Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected



Include | Exclude

○ None

○ All users

● Select users and groups

☑ Guest or external users ⓘ

B2B collaboration guest users

☑ B2B collaboration guest users

☐ B2B collaboration member users

☐ B2B direct connect users

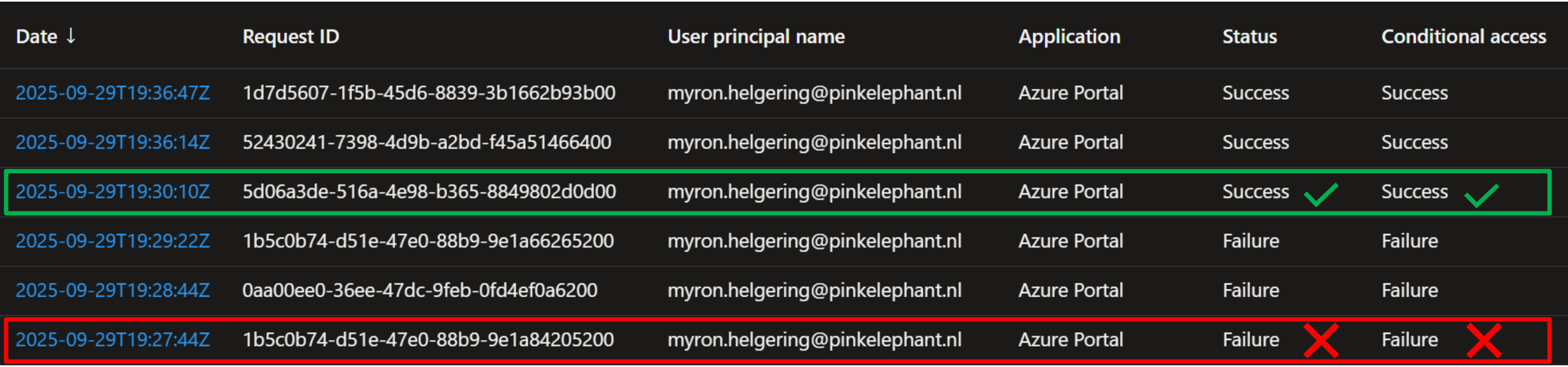
☐ Local guest users

☐ Service provider users

☐ Other external users

Include B2B guest users

Sign-in as a guest user

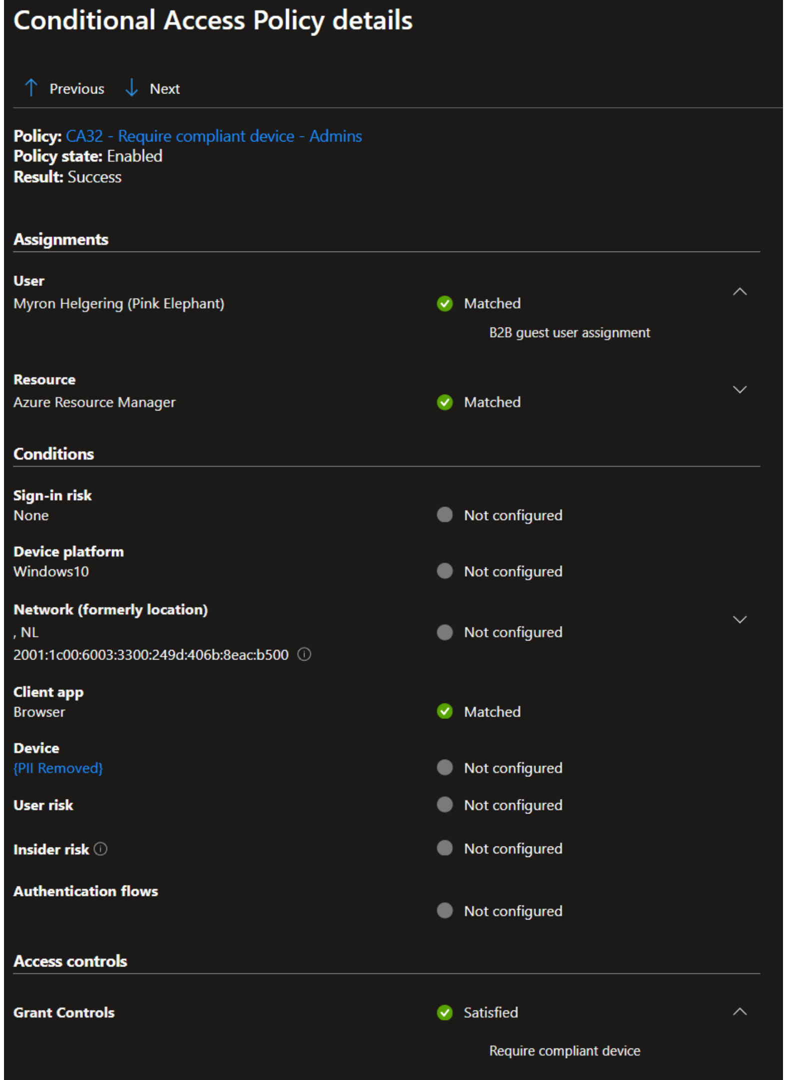


Date ↓	Request ID	User principal name	Application	Status	Conditional access
2025-09-29T19:36:47Z	1d7d5607-1f5b-45d6-8839-3b1662b93b00	myron.helgering@pinkelephant.nl	Azure Portal	Success	Success
2025-09-29T19:36:14Z	52430241-7398-4d9b-a2bd-f45a51466400	myron.helgering@pinkelephant.nl	Azure Portal	Success	Success
2025-09-29T19:30:10Z	5d06a3de-516a-4e98-b365-8849802d0d00	myron.helgering@pinkelephant.nl	Azure Portal	Success ✓	Success ✓
2025-09-29T19:29:22Z	1b5c0b74-d51e-47e0-88b9-9e1a66265200	myron.helgering@pinkelephant.nl	Azure Portal	Failure	Failure
2025-09-29T19:28:44Z	0aa00ee0-36ee-47dc-9feb-0fd4ef0a6200	myron.helgering@pinkelephant.nl	Azure Portal	Failure	Failure
2025-09-29T19:27:44Z	1b5c0b74-d51e-47e0-88b9-9e1a84205200	myron.helgering@pinkelephant.nl	Azure Portal	Failure ✗	Failure ✗

- Sign-in with **non-compliant** and a **compliant** device

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

Conditional Access Policy details



Conditional Access Policy details

Policy: CA32 - Require compliant device - Admins
Policy state: Enabled
Result: Success

Assignments

User
Myron Helgering (Pink Elephant) — ✓ Matched
B2B guest user assignment

Resource
Azure Resource Manager — ✓ Matched

Conditions

Sign-in risk
None — ● Not configured

Device platform
Windows10 — ● Not configured

Network (formerly location)
, NL
2001:1c00:6003:3300:249d:406b:8eac:b500 — ● Not configured

Client app
Browser — ✓ Matched

Device
{PII Removed} — ● Not configured

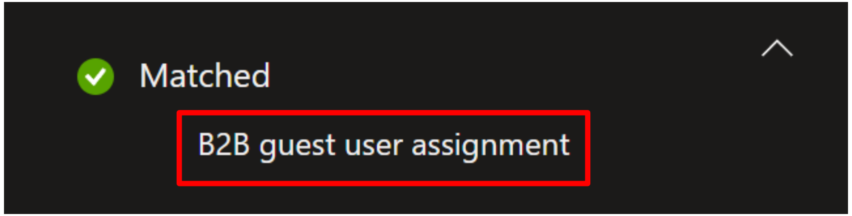
User risk — ● Not configured

Insider risk — ● Not configured

Authentication flows — ● Not configured

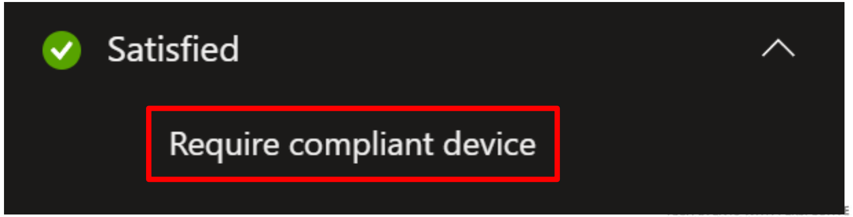
Access controls

Grant Controls — ✓ Satisfied
Require compliant device



✓ Matched

B2B guest user assignment



✓ Satisfied

Require compliant device

Is the device compliant with “our” policies?
Probably not

Option 2: Access through Guest Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	★★★	★	★★★	★★★
Guest Account	★	★★		

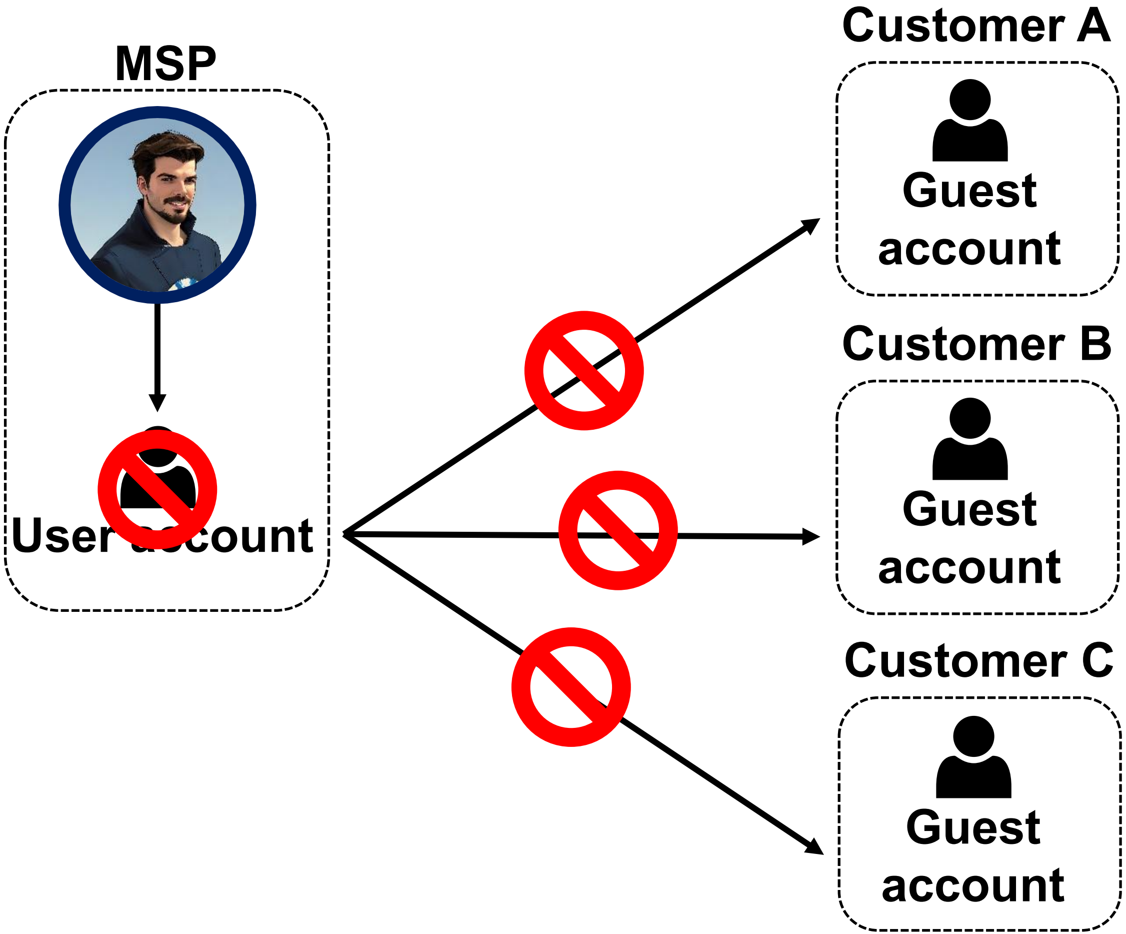
Permissions

- Privileged Identity Management (PIM) ✅
- Role Based Access Control (RBAC) ✅
- Access Packages & Reviews ✅

Option 2: Access through Guest Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	★★★	★	★★★	★★★
Guest Account	★	★★	★★★	

MSP perspective



Security

- Upsides
  - Permissions (PIM, Access Packages & Reviews) ✅
  - Device compliance with trust settings for guests works ✅
  - Guest access is disabled when (MSP) account is disabled ✅
  - Full visibility in sign-in and audit logs ✅
- Downsides
  - Real device compliance can’t be achieved ⛔

Option 2: Access through Guest Account

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	⭐⭐⭐
Guest User Account	⭐	⭐⭐	⭐⭐⭐	⭐⭐

Three options to grant access

1

Access through **User** Account

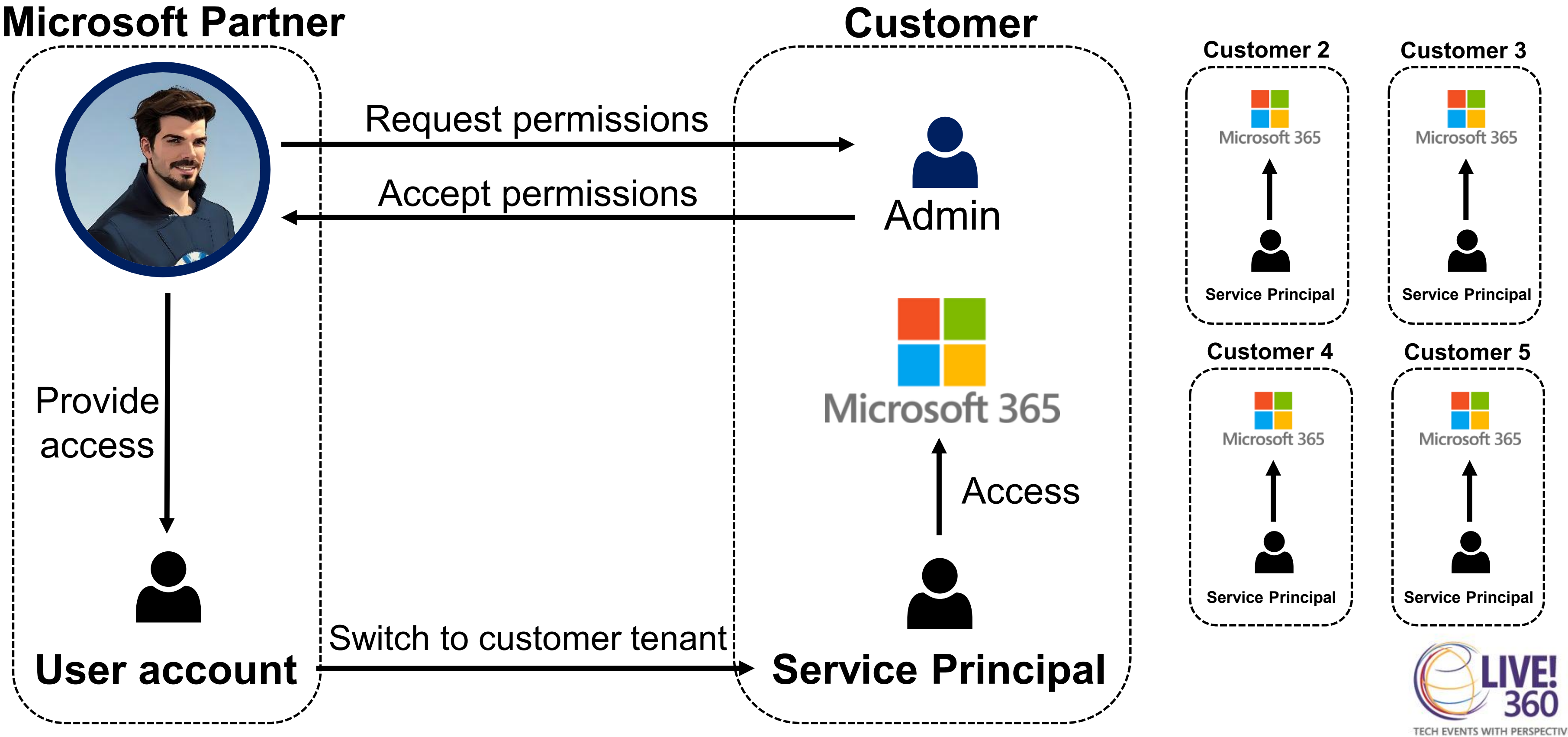
2

Access through **Guest** Account

3

Access through **GDAP**

Granular Delegated Admin Permissions (GDAP)



Microsoft Partner

Request permissions

Accept permissions

Provide access

User account

Switch to customer tenant

Customer

Admin

Microsoft 365

Access

Service Principal

Customer 2

Microsoft 365

Service Principal

Customer 3

Microsoft 365

Service Principal

Customer 4

Microsoft 365

Service Principal

Customer 5

Microsoft 365

Service Principal

LIVE! 360 TECH EVENTS WITH PERSPECTIVE

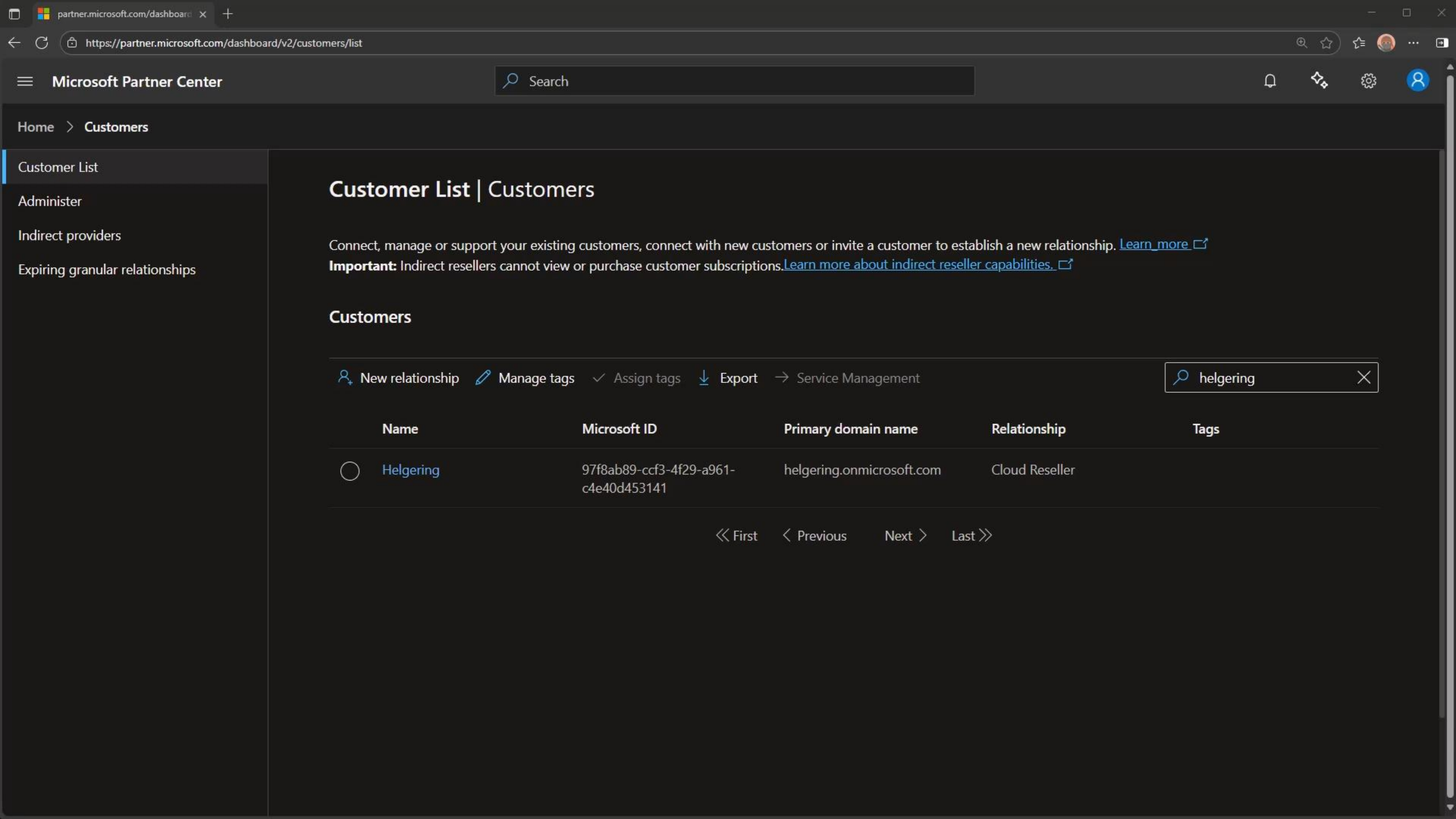
Option 3: Access through GDAP

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	★★★	★	★★★	★★★
Guest User Account	★	★★	★★★	★★
GDAP Access				

Three jobs to do

- Troubleshoot enrollment failures
- Assign authentication method policies
- Change SharePoint library settings

Demo: Using GDAP access



Customer List | Customers

Connect, manage or support your existing customers, connect with new customers or invite a customer to establish a new relationship. Learn more
Important: Indirect resellers cannot view or purchase customer subscriptions.Learn more about indirect reseller capabilities.

Customers

	Name	Microsoft ID	Primary domain name	Relationship	Tags
○	Helgering	97f8ab89-ccf3-4f29-a961-c4e40d453141	helgering.onmicrosoft.com	Cloud Reseller	

Access through GDAP

- Admin features are not working
- Limited SPO & Teams access
- Tenant switching
  - Button only available in M365
  - Arrive in the wrong tenant
- Bugs, bugs & more bugs

LIVE! 360 TECH EVENTS WITH PERSPECTIVE

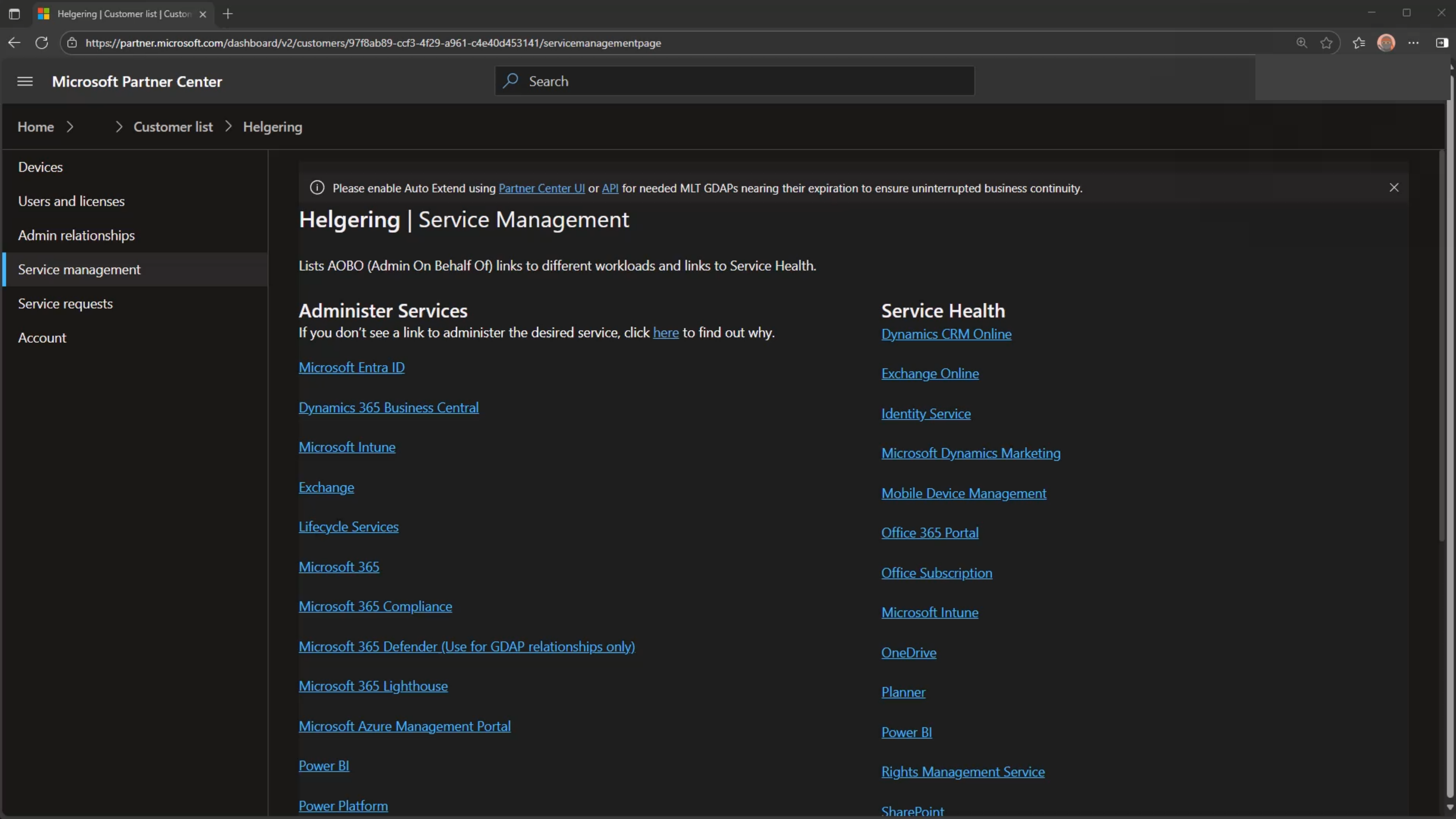
M365 Lighthouse

- Central Management for all your customers
- Account Management
- Device Security
- Audit Logs
- Role Management
- Baseline Deployment
- Message Quarantine Management

Demo: M365 Lighthouse

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

General



Helgering | Customer list | Custon
https://partner.microsoft.com/dashboard/v2/customers/97f8ab89-ccf3-4f29-a961-c4e40d453141/servicemanagementpage
Microsoft Partner Center
Search
Home > > Customer list > Helgering
Devices
Users and licenses
Admin relationships
Service management
Service requests
Account

Please enable Auto Extend using Partner Center UI or API for needed MLT GDAPs nearing their expiration to ensure uninterrupted business continuity.

Helgering | Service Management

Lists AOBO (Admin On Behalf Of) links to different workloads and links to Service Health.

Administer Services

If you don't see a link to administer the desired service, click here to find out why.

Microsoft Entra ID

Dynamics 365 Business Central

Microsoft Intune

Exchange

Lifecycle Services

Microsoft 365

Microsoft 365 Compliance

Microsoft 365 Defender (Use for GDAP relationships only)

Microsoft 365 Lighthouse

Microsoft Azure Management Portal

Power BI

Power Platform

Service Health

Dynamics CRM Online

Exchange Online

Identity Service

Microsoft Dynamics Marketing

Mobile Device Management

Office 365 Portal

Office Subscription

Microsoft Intune

OneDrive

Planner

Power BI

Rights Management Service

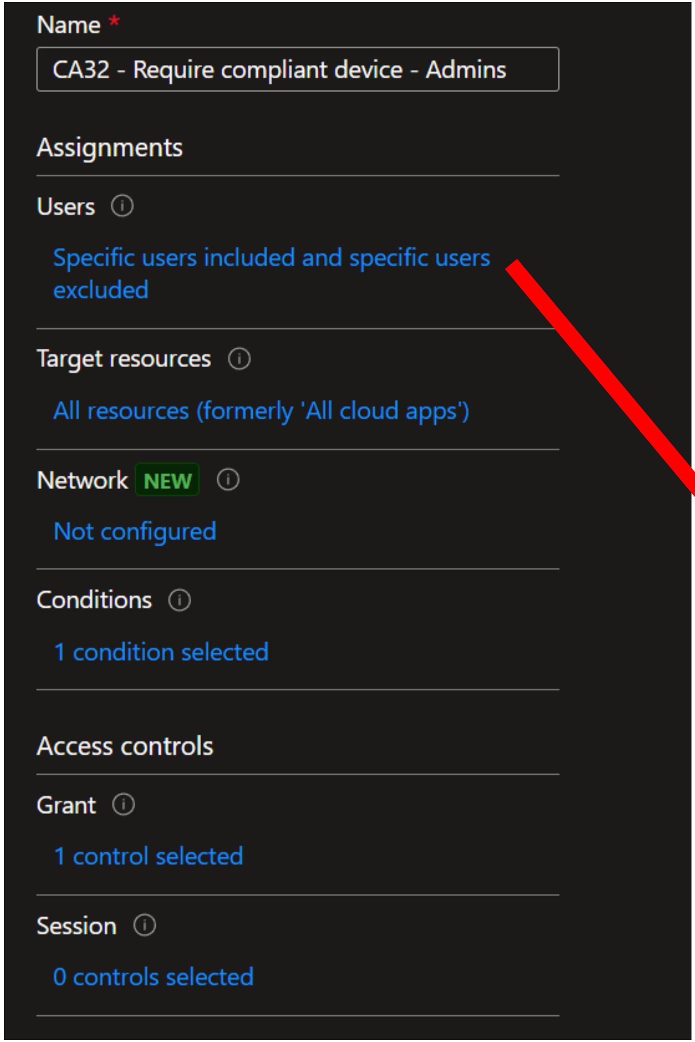
SharePoint

Option 3: Access through GDAP

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	⭐⭐⭐
Guest User Account	⭐	⭐⭐	⭐⭐⭐	⭐⭐
GDAP Access	⭐⭐			

Device Compliance

- Cross-tenant access settings work the same as “Option 2: Guest Account.” ✅



Name *

CA32 - Require compliant device - Admins

Assignments

Users ⓘ

Specific users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Not configured

Conditions ⓘ

1 condition selected

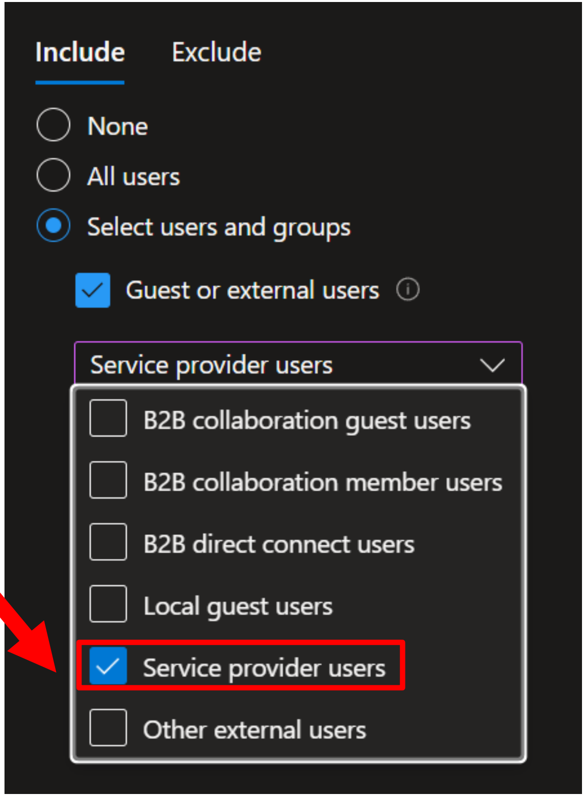
Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected



○ None

○ All users

● Select users and groups

☑ Guest or external users ⓘ

Service provider users

- ☐ B2B collaboration guest users
- ☐ B2B collaboration member users
- ☐ B2B direct connect users
- ☐ Local guest users
- ☑ Service provider users
- ☐ Other external users

Include service provider users

Option 3: Access through GDAP

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	★★★	★	★★★	★★★
Guest User Account	★	★★	★★★	★★
GDAP Access	★★	★★		

Delegated Admin Permissions (DAP)

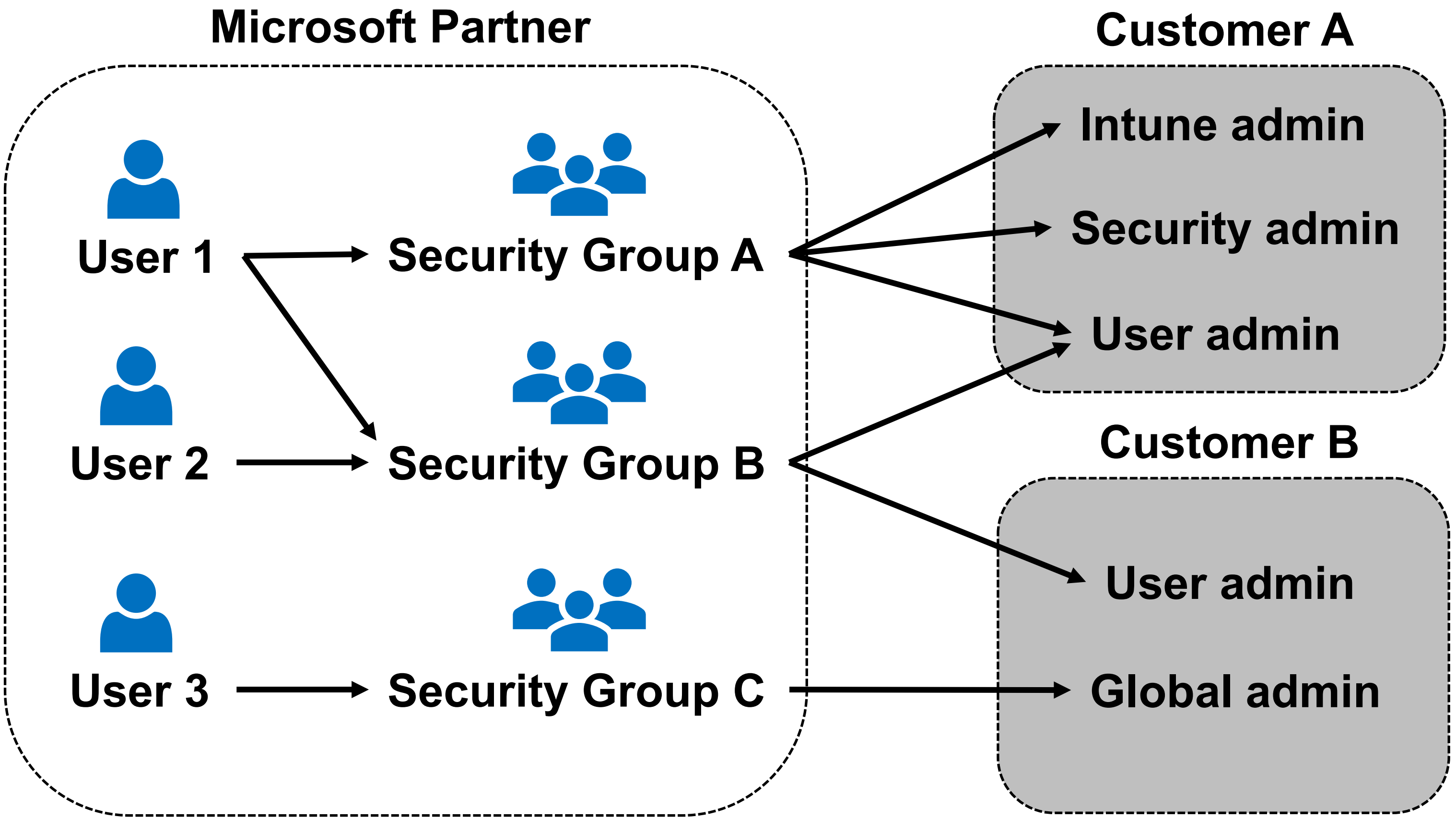
- Overprivileged access
- Indefinite access
- Limited audit logging
- Vulnerable to threat actors

Granular Delegated Admin Permissions (GDAP)

- Granular access
- Timebound access
- Full audit logging
- Less vulnerable to threat actors

Customer
You realize you’re not in control anymore

Granting Permissions through GDAP



Microsoft Partner

User 1

User 2

User 3

Security Group A

Security Group B

Security Group C

Customer A

Intune admin

Security admin

User admin

Customer B

User admin

Global admin

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

General

GDAP + PIM (role-based)

Customer	Sec Group	Roles	PIM
Customer A Customer B Customer C	Service desk	Global reader Helpdesk admin	Permanent
Customer A Customer B Customer C	Engineers	Intune administrator Exchange administrator	Eligible
Customer A Customer B Customer C	Global admins	Global administrator	Approval

Don’t do this please!

GDAP + PIM (customer-based)

Customer	Sec Group	Roles	PIM
Customer A	CustomerA_T1	Global reader Helpdesk admin	Permanent
Customer A	CustomerA_T2	Intune administrator Exchange administrator	Eligible
Customer A	CustomerA_T3	Global administrator	Approval
Customer B	CustomerB_T1	Global reader Helpdesk admin	Permanent
Customer B	CustomerB_T2	Intune administrator Exchange administrator	Eligible

GDAP + PIM (customer + role based)

Customer	Sec Group	Roles	PIM
Customer A Customer B Customer C	Service desk	Global reader Helpdesk admin	Permanent
Customer A	CustomerA_T2	Intune administrator Exchange administrator	Eligible
Customer A	CustomerA_T3	Global administrator	Approval
Customer B	CustomerB_T2	Intune administrator Exchange administrator	Eligible
Customer B	CustomerB_T3	Global administrator	Approval

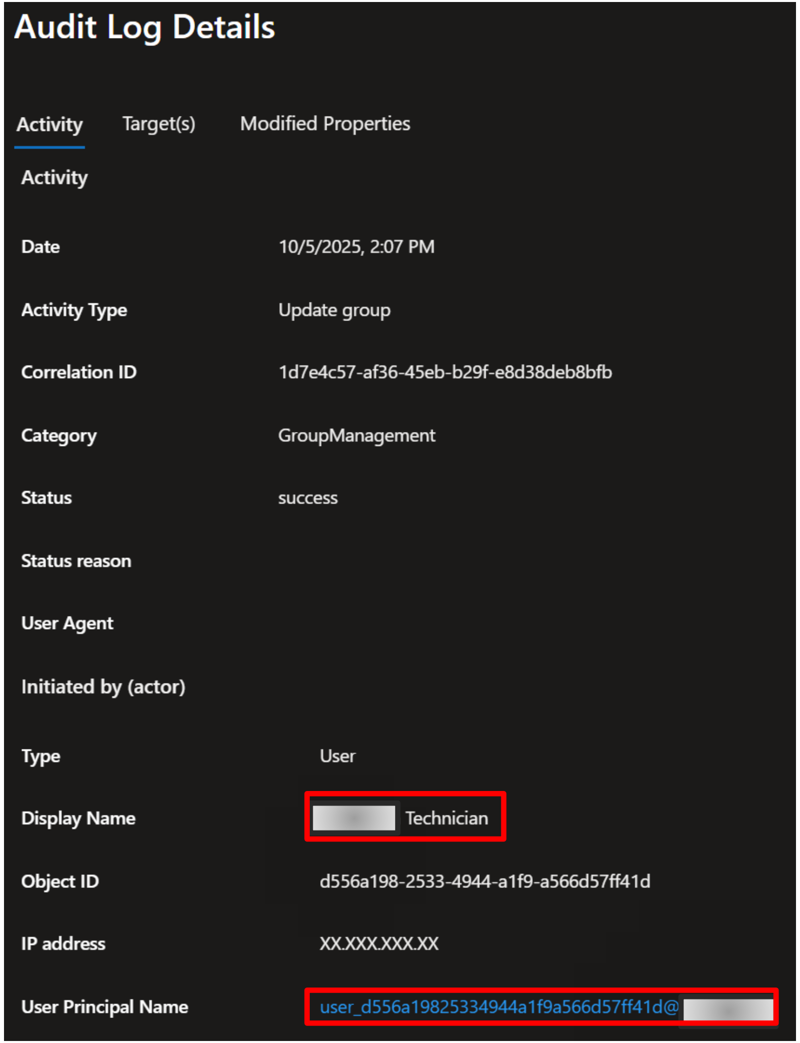
Permissions available through GDAP

- 20 out of 118 Entra roles are missing
- Custom roles are not supported
- Admin portal specific RBAC roles are not supported
  - Defender
  - Purview
  - Intune

Option 3: Access through GDAP

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	⭐⭐⭐
Guest User Account	⭐	⭐⭐	⭐⭐⭐	⭐⭐
GDAP Access	⭐⭐	⭐⭐	⭐⭐	

Audit logs from Customer Perspective



Audit Log Details

Activity

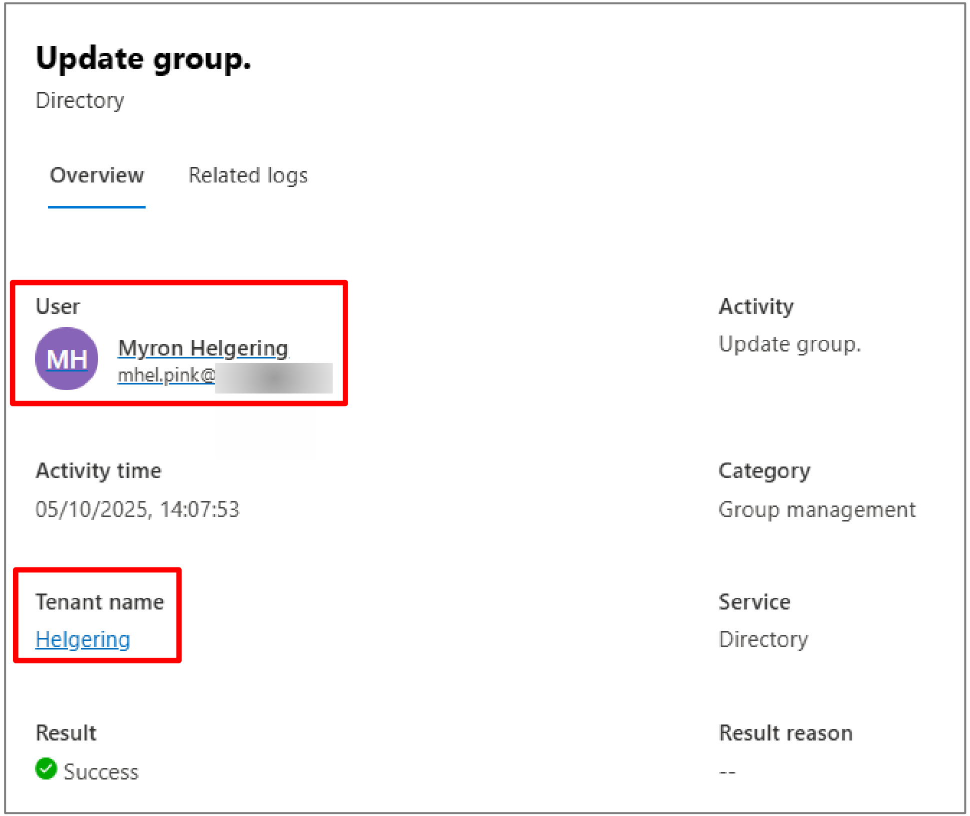
Date	10/5/2025, 2:07 PM
Activity Type	Update group
Correlation ID	1d7e4c57-af36-45eb-b29f-e8d38deb8bfb
Category	GroupManagement
Status	success
Status reason	
User Agent	

Initiated by (actor)

Type	User
Display Name	[redacted] Technician
Object ID	d556a198-2533-4944-a1f9-a566d57ff41d
IP address	XX.XXX.XXX.XX
User Principal Name	user_d556a19825334944a1f9a566d57ff41d@[redacted]

- UPN = user_XX@partner.com
- DN = “Partner” Technician

Audit logs from MSP Perspective



Update group.

Directory

Overview | Related logs

User
MH Myron Helgering
mhel.pink@[redacted]

Activity
Update group.

Activity time
05/10/2025, 14:07:53

Category
Group management

Tenant name
Helgering

Service
Directory

Result
✓ Success

Result reason
--

- UPN visible
- Display Name visible

Overall Security

- Upsides
  - Microsoft Partner can combine GDAP with PIM ✅
  - Device compliance with trust settings for guests works ✅
  - Guest access is disabled when (MSP) account is disabled ✅
- Downsides
  - GDAP supports only a limited amount of roles ⚠️
  - Customer has little control over permission governance ⛔
  - Real device compliance can’t be achieved ⛔
  - Customer has limited insights in sign-in and audit logs ⚠️

Option 3: Access through GDAP

Scenario	User Experience	Device Compliance	Permissions	Security
User Account	★★★	★	★★★	★★★
Guest User Account	★	★★	★★★	★★
GDAP Access	★★	★★	★★	★

General

When to choose which option

- Option 1: User account
  - If you want to be in control of your own environment and want to maintain a high security level.
- Option 2: Guest account
  - If external admins only need access to specific accessible admin portals.
- Option 3: GDAP
  - If you delegate most of your IT business to an MSP partner.

Takeaways

- Prepare your organization for external admins.
- Don’t simply exclude external admins from your Conditional Access policies.
- If possible, give your external admins access through a (virtual) managed device, such as a PAW.
- Configure cross-tenant access settings for external GDAP and B2B guest admins.
- Always combine PIM with GDAP permissions and create security groups for each customer.

Time for questions!

LIVE! 360

TECH EVENTS WITH PERSPECTIVE

Other sessions @ Live! 360

- Wednesday, November 19, 2025
  - Automated Data Security: Identifying Sensitive Data with Microsoft Purview **(9:30am – 10:45am)**
- Thursday, November 20, 2025
  - Six Methods to Protect your Business from the Threat of Unmanaged Devices **(1:00pm – 2:15pm)**
  - The Challenge of Providing Secure Access to External Admins **(2:30pm – 3:45pm)**

LIVE! 360

TECH EVENTS WITH PERSPECTIVE

General

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

LIVE! 360

TECH EVENTS WITH PERSPECTIVE

Thank you!