
The Challenge of Providing Secure Access to External Admins
WP Ninja Meetup #5 @ Interstellar
wpninjas.nl

About me

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

Myron Helgering

in/myronhelgering

myronhelgering.com

Why this session?

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

Access through **User** Account

Access through **Guest** Account

Access through **GDAP**

Types of external admins

Consultant

MSP

Freelancer

MSSP

Four aspects to take into account

- User Experience
- Device Compliance
- Permissions
- Overall Security

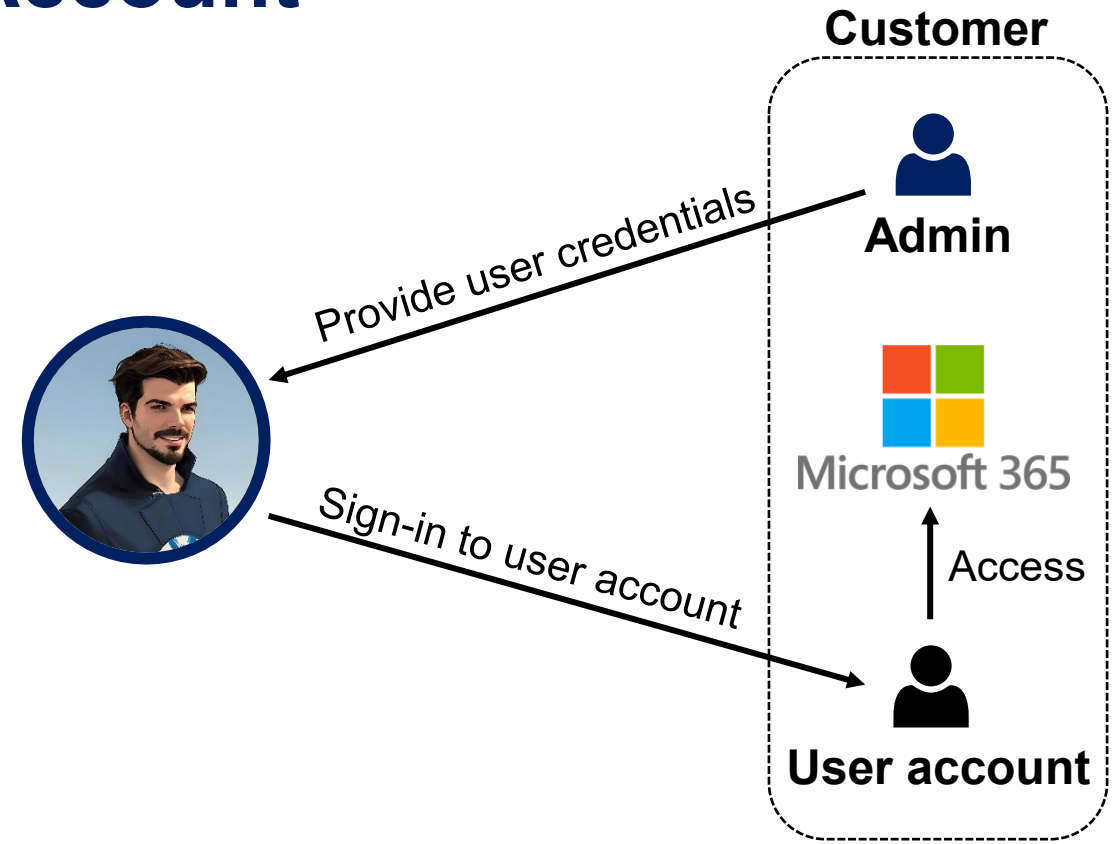
Three options to grant access

Access through **User** Account

Access through **Guest** Account

Access through **GDAP**

User Account

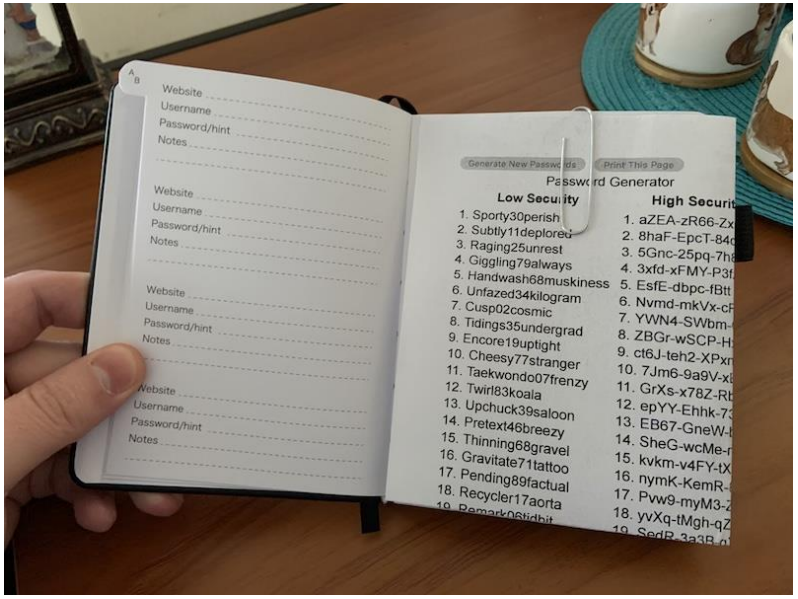


Option 1: Access through User Account

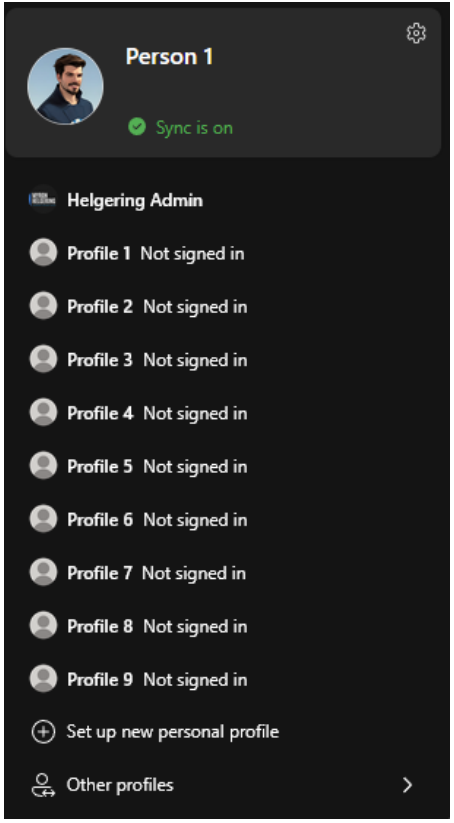
Scenario	User Experience	Device Compliance	Permissions	Overall Security
User Account				

Accounts for multiple customers

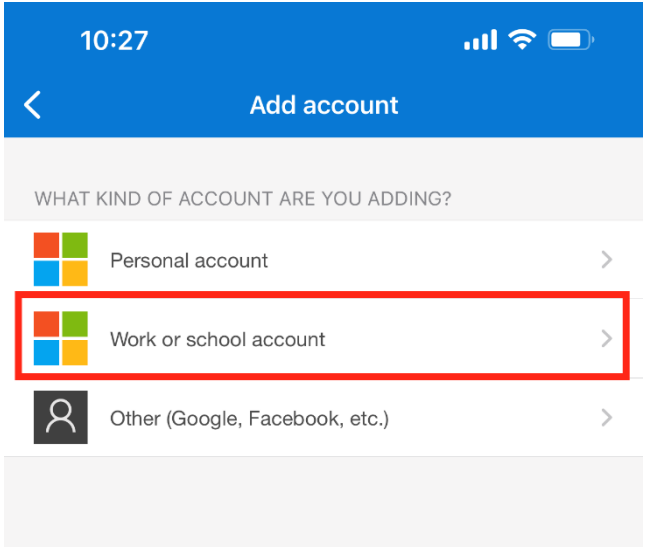
Accounts and passwords



Browser profiles



MFA registrations



User Experience after sign-in

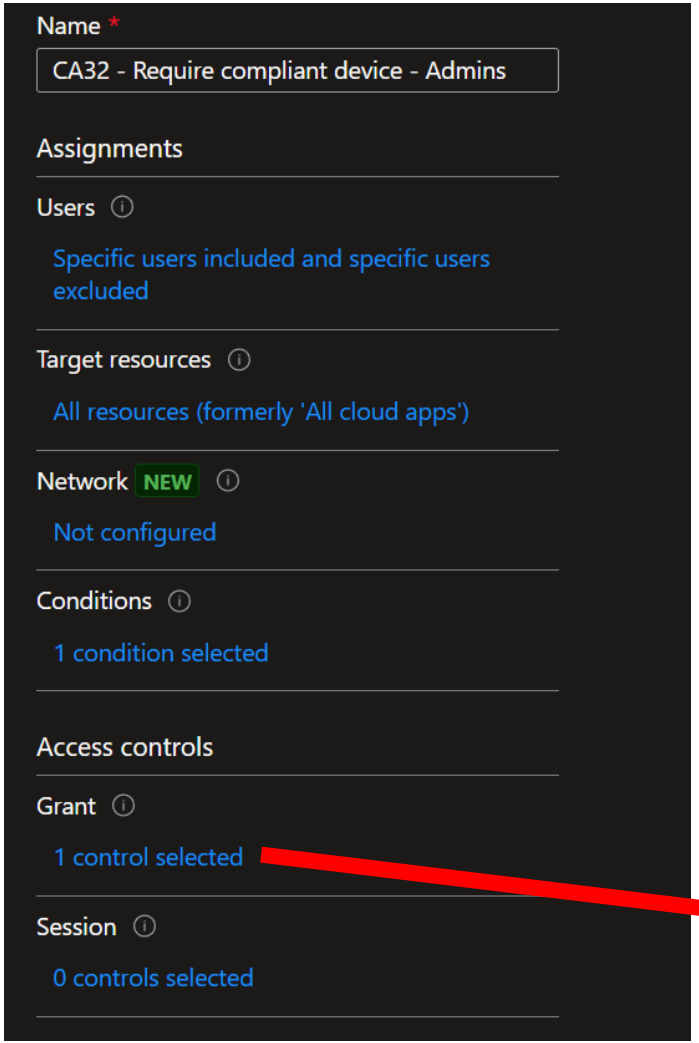
Option 1: Access through User Account

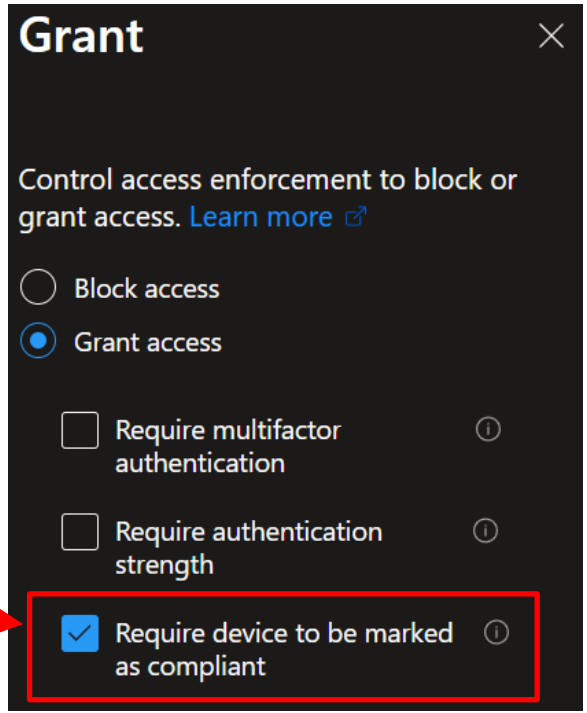
Scenario	User Experience	Device Compliance	Permissions	Overall Security
User Account				

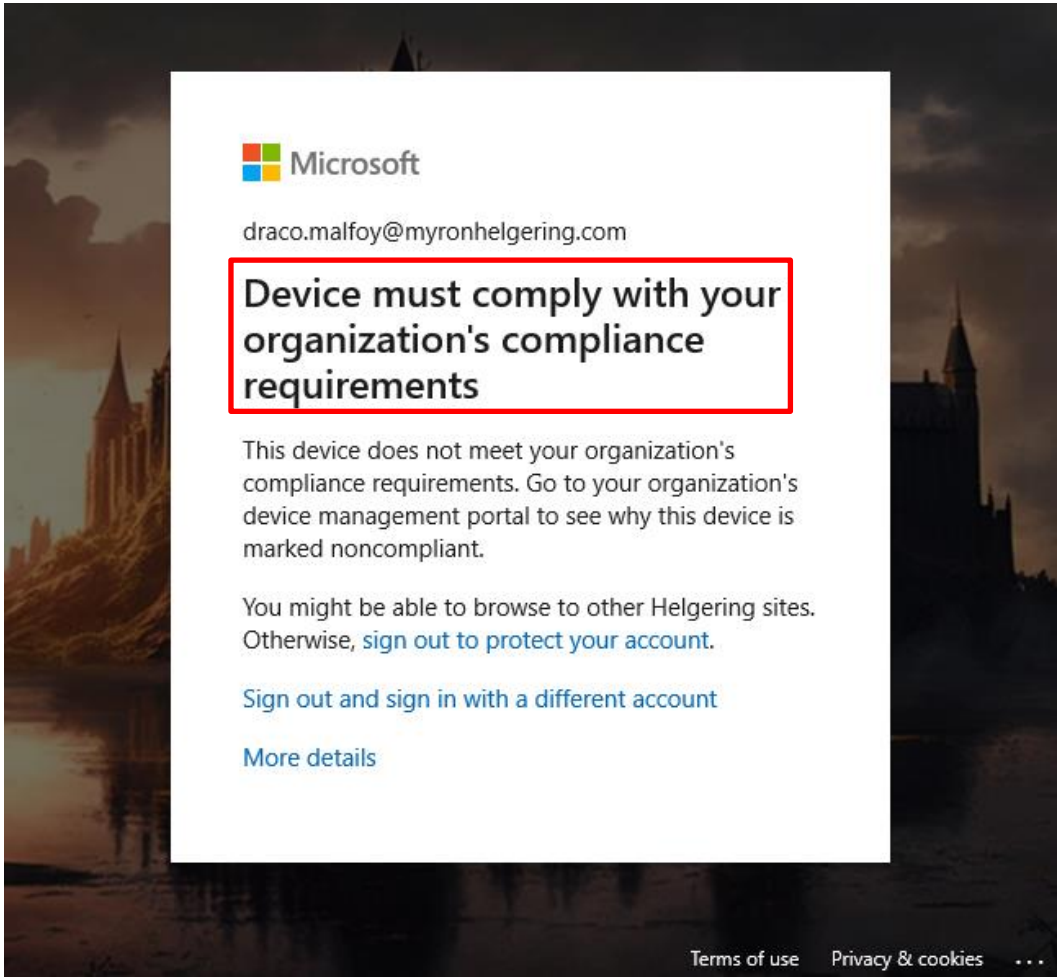
Why managed and compliant device?

- 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

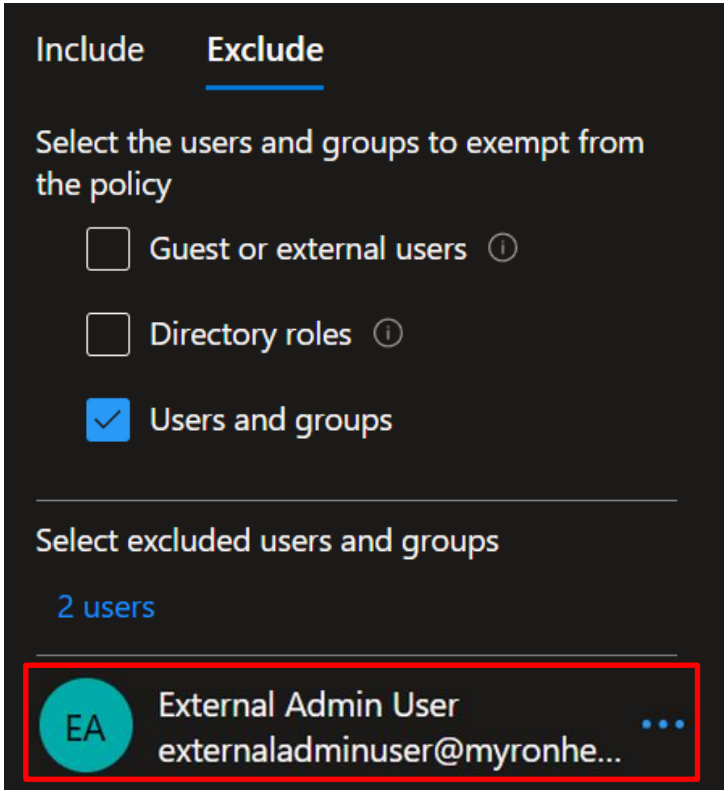
Require compliant device with Conditional Access



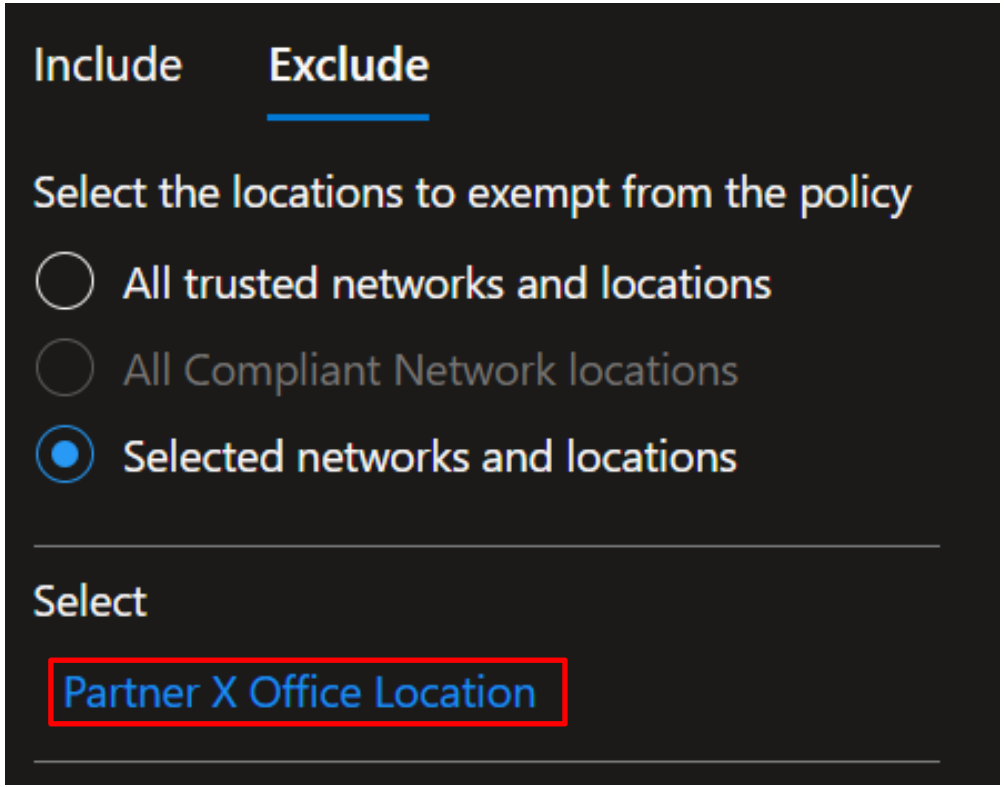




Sign in with unmanaged device



Exclude external admin user



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

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

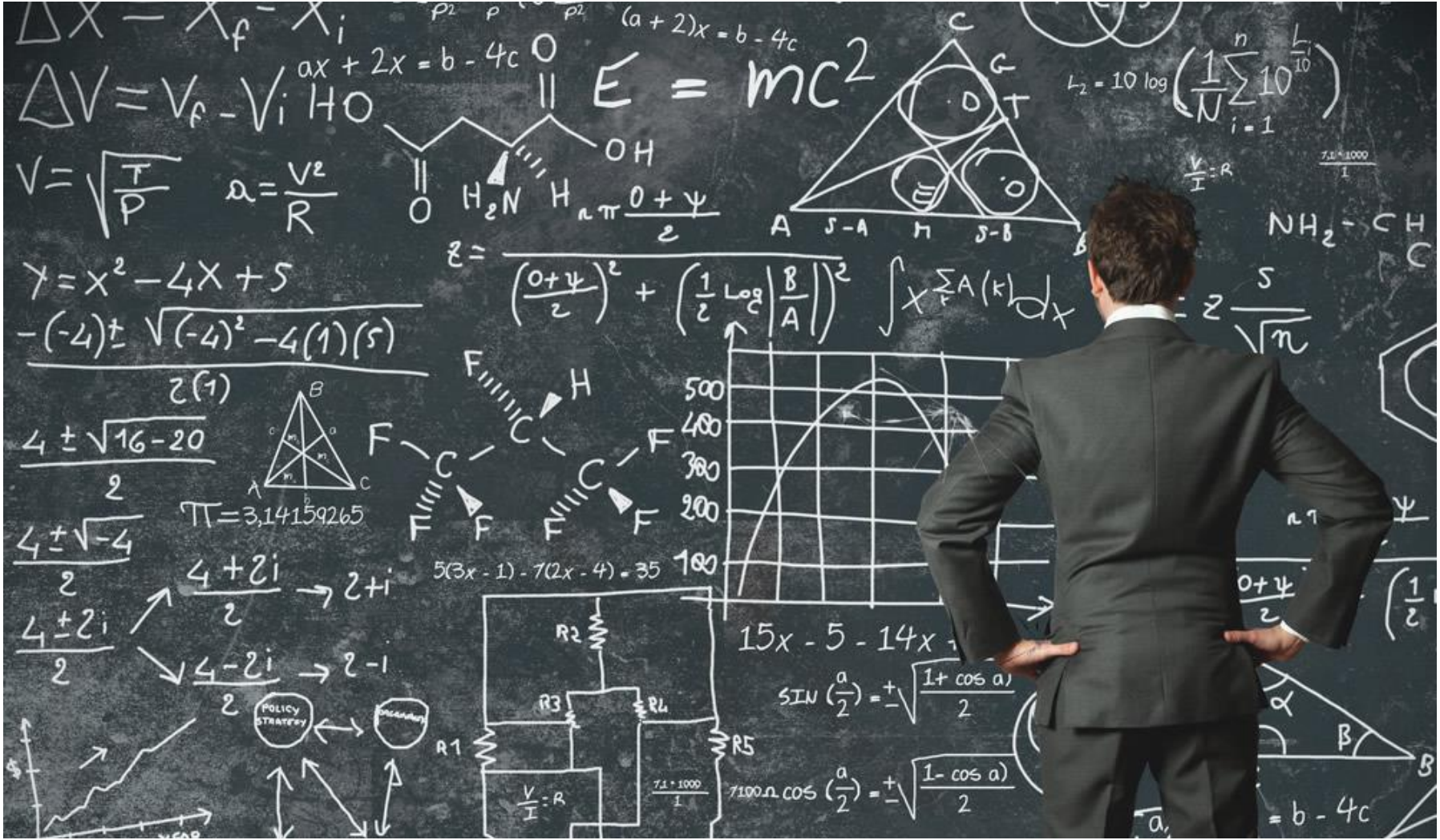
- Give external admins managed device
- Windows 365 Cloud PC or Azure Virtual Desktop
- **Privileged Access Workstation (PAW)**

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


E = mc²
ax + 2x = b - 4c
(a + 2)x = b - 4c
ΔV = V_f - V_i
V = √(T/P)
a = V²/R
y = x² - 4x + 5
π = 3,14159265
5(3x - 1) - 7(2x - 4) = 35
15x - 5 - 14x
NH₂ - CH
POLICY
STRATEGY
R1
R2
R3
R4
R5

Option 1: Access through User Account

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

Permissions

- Privileged Identity Management (PIM) ✅
- Access Packages & Reviews ✅

Option 1: Access through User Account

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

MSP trying to keep track

Overall 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	Overall Security
User Account	⭐ ⭐ ⭐	⭐	⭐ ⭐ ⭐	⭐ ⭐ ⭐

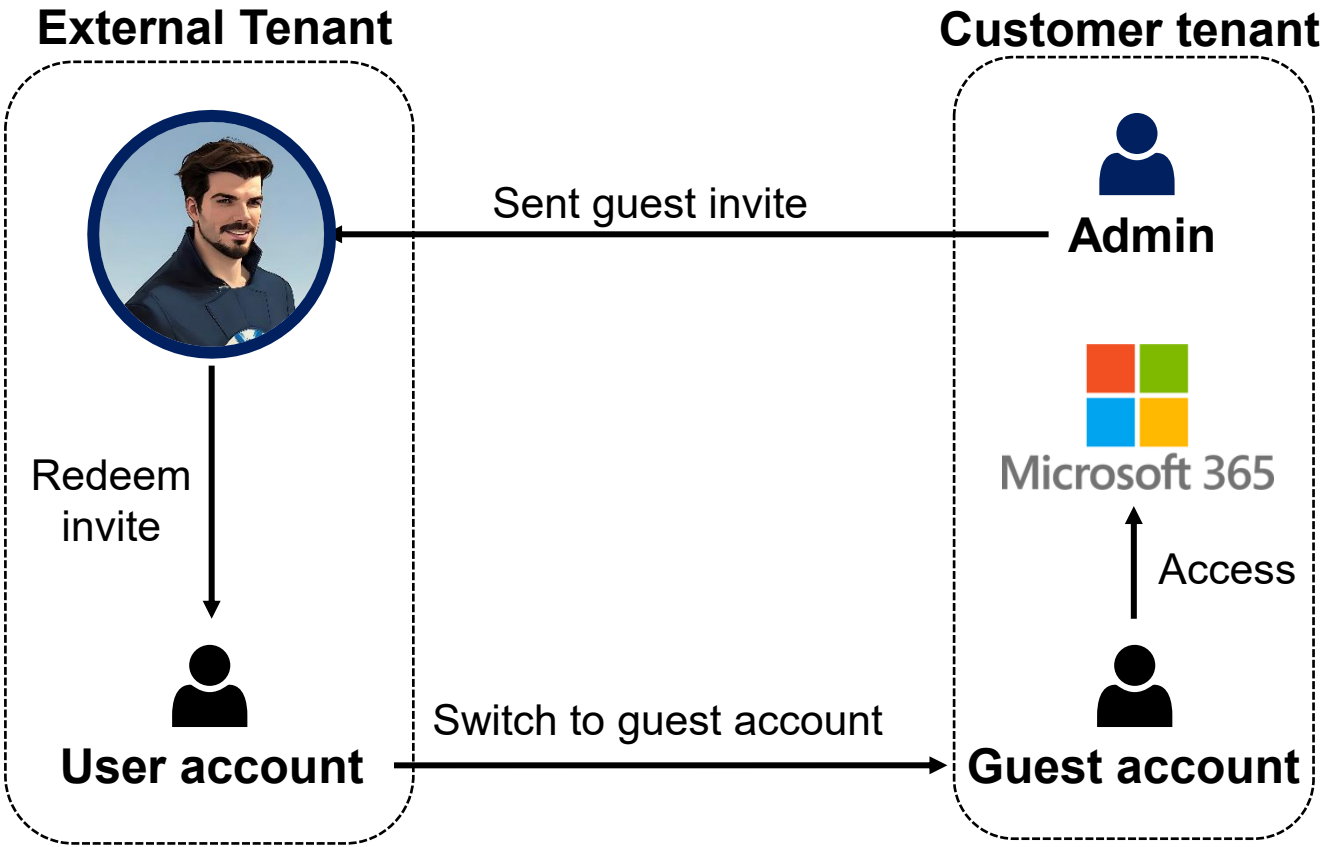
Three options to grant access

Access through **User** Account

Access through **Guest** Account

Access through **GDAP**

Guest account



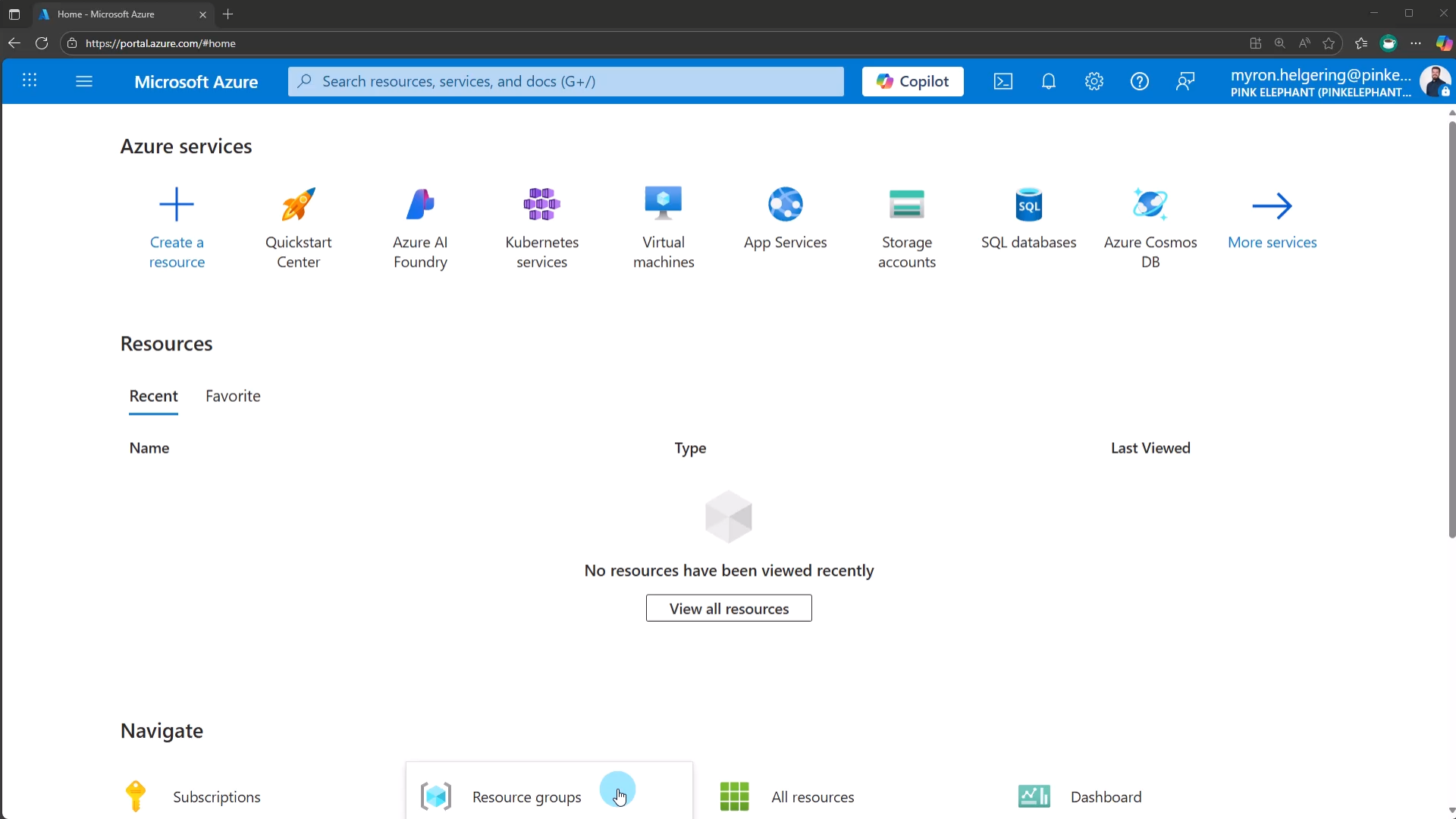
Option 2: Access through Guest Account

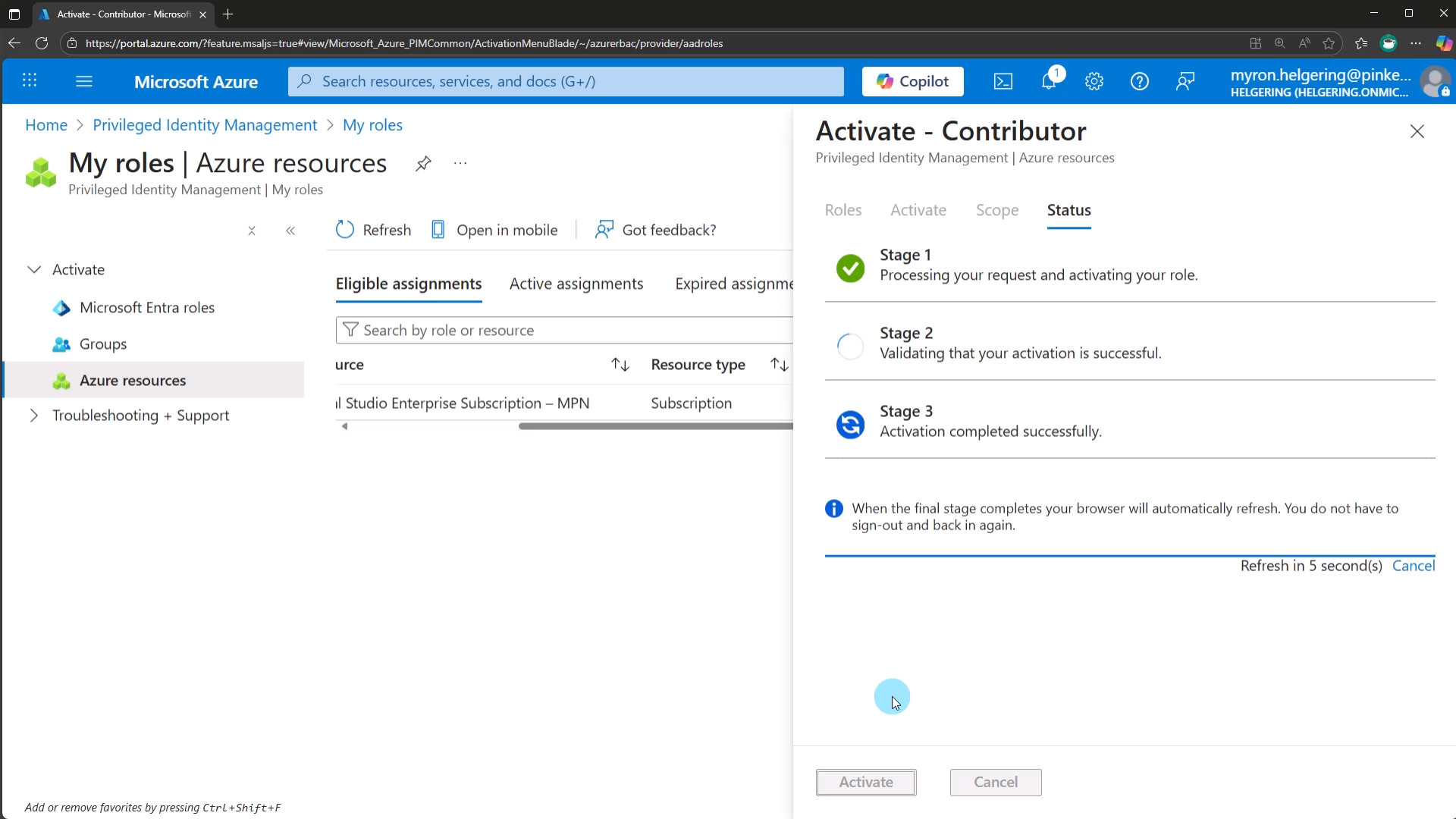
Scenario	User Experience	Device Compliance	Permissions	Overall Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	⭐⭐⭐
Guest Account				

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 with Guest Account


Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
myron.helgering@pinke...
PINK ELEPHANT (PINKELEPHANT...
Azure services
Create a resource
Quickstart Center
Azure AI Foundry
Kubernetes services
Virtual machines
App Services
Storage accounts
SQL databases
Azure Cosmos DB
More services
Resources
Recent
Favorite
Name
Type
Last Viewed
No resources have been viewed recently
View all resources
Navigate
Subscriptions
Resource groups
All resources
Dashboard


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
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
l Studio Enterprise Subscription – MPN
Subscription
Activate - Contributor
Privileged Identity Management | Azure resources
Roles
Activate
Scope
Status
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
Activate
Cancel
Add or remove favorites by pressing Ctrl+Shift+F

Azure services

- Create a resource
- Resource groups
- Microsoft Entra Privileged...
- Resources
- Storage accounts
- Subscriptions
- Quickstart Center
- Azure AI Foundry
- Kubernetes services
- More services

Resources

Recent | Favorite

Name	Type	Last Viewed
Servers_MyronHelgering.com	Resource group	an hour ago

See all

Navigate

- Subscriptions
- Resource groups
- All resources
- Dashboard

Tools

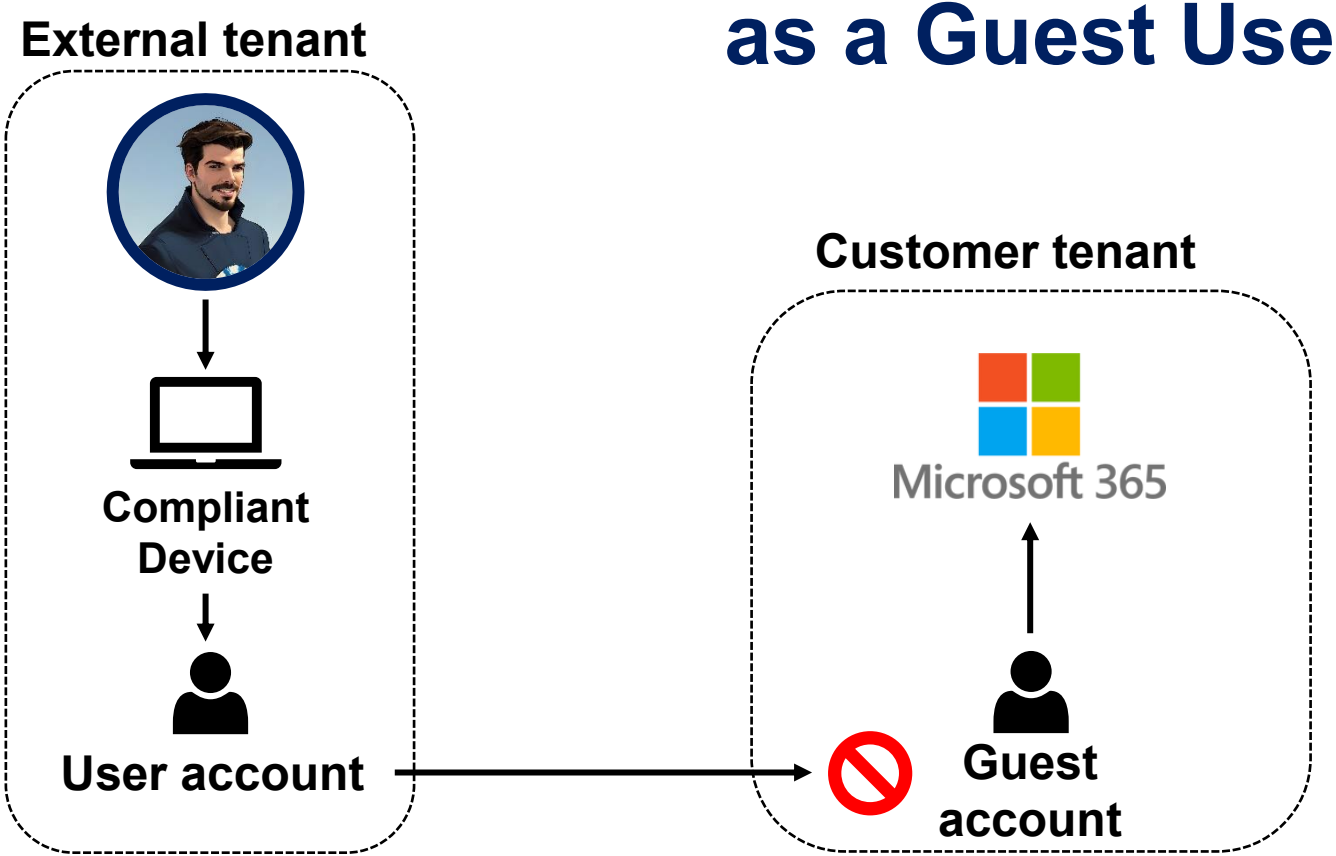
Admin Portal Access

- Access ✅
  - **Azure Management** portal
  - **Entra** admin center
  - **Intune** admin center
- No access ⛔
  - **M365** admin center
  - **Exchange** admin center
  - **SharePoint Online** admin center
  - **Teams** admin center
  - **Power platform** admin center
- Access by copy/pasting tenant ID 😅
  - **Purview** admin center
  - **Defender** admin center

Option 2: Access through Guest Account

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

Device Compliance as a Guest User



Demo: Device compliance through cross tenant access settings

Home
Agents
Favorites
Entra ID
ID Protection
ID Governance
Verified ID
Permissions Management
Global Secure Access
What's new
Billing

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

View user profile

My role assignments

1

High privileged role assignments

Other role assignments

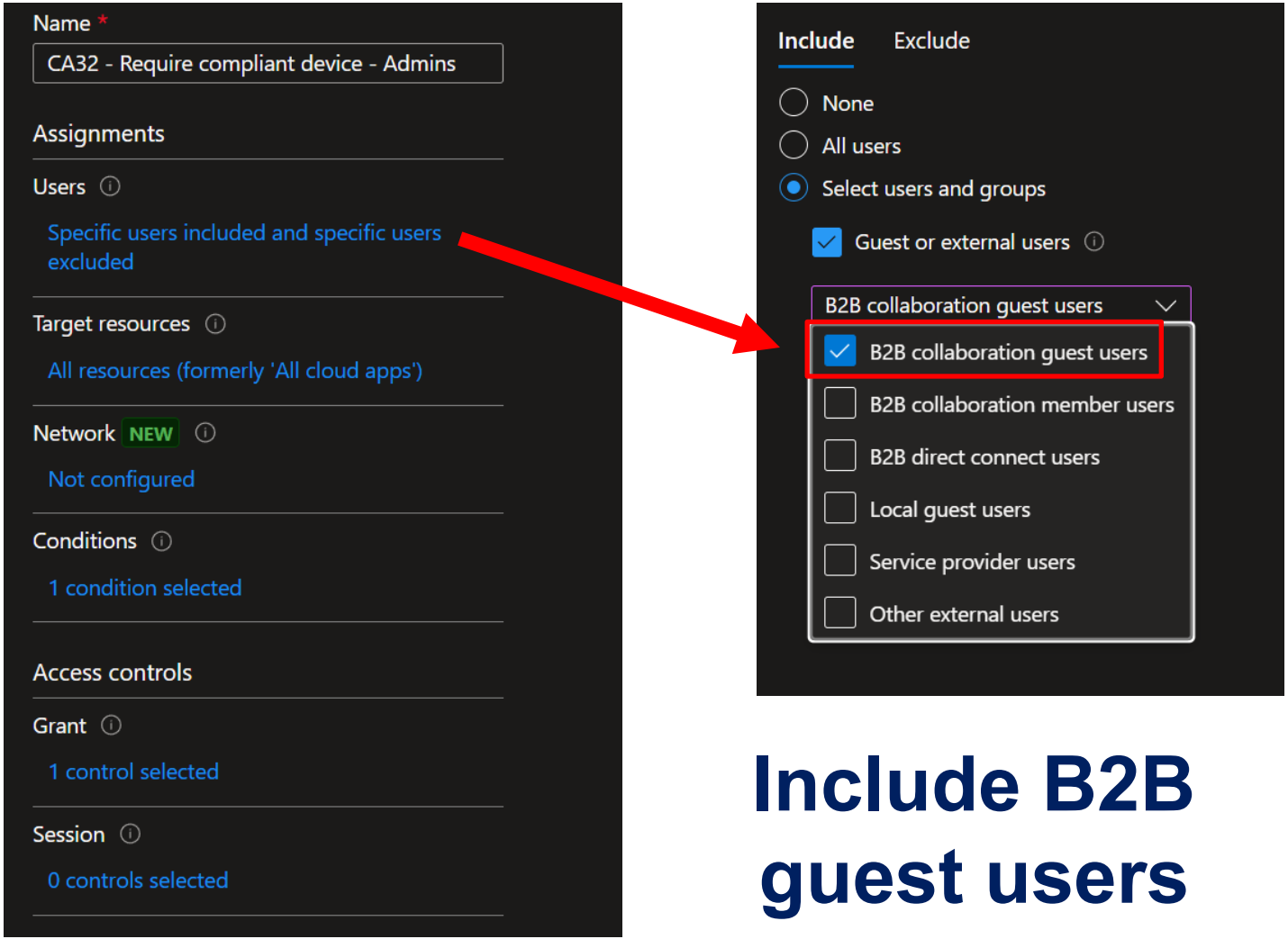
Manage my roles

Users at high risk

Tenant status

Identity Secure Score

40.98%

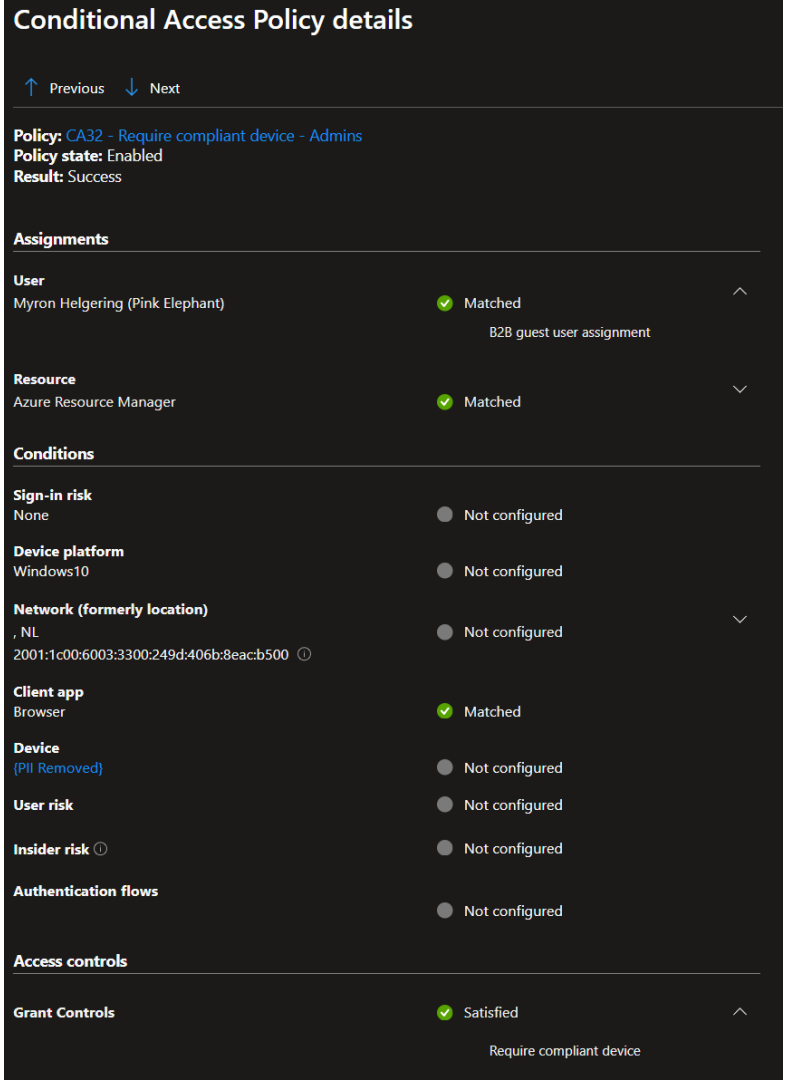


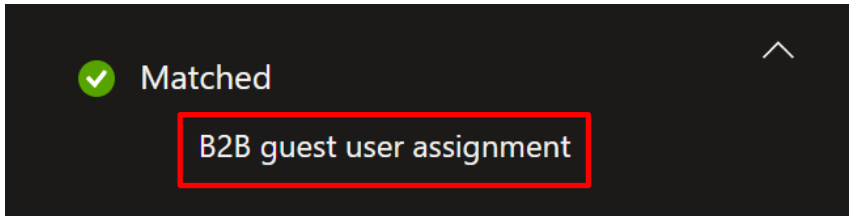
Include B2B guest users

Sign-in as a guest user

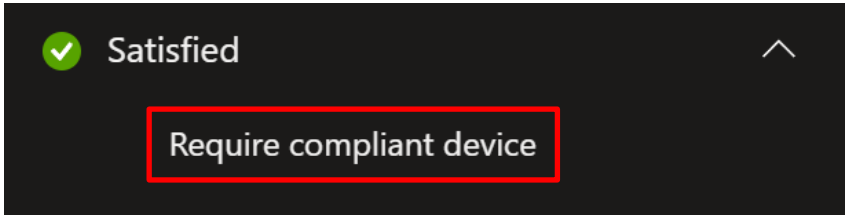
Date ↓	Request ID	User principal name	Application	Status	Conditional access
2025-09-29T19:36:47Z	1d7d5607-1f5b-45d6-8839-3b1662b93b00	myron.helgering@pinkelephant.nl	Azure Portal	Success	Success
2025-09-29T19:36:14Z	52430241-7398-4d9b-a2bd-f45a51466400	myron.helgering@pinkelephant.nl	Azure Portal	Success	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





Conditional Access Policy details




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

Option 2: Access through Guest Account

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

Permissions

- Privileged Identity Management (PIM) ✅
- Access Packages & Reviews ✅

Option 2: Access through Guest Account

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

Overall 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	Overall Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	⭐⭐⭐
Guest Account	⭐	⭐⭐	⭐⭐⭐	⭐⭐

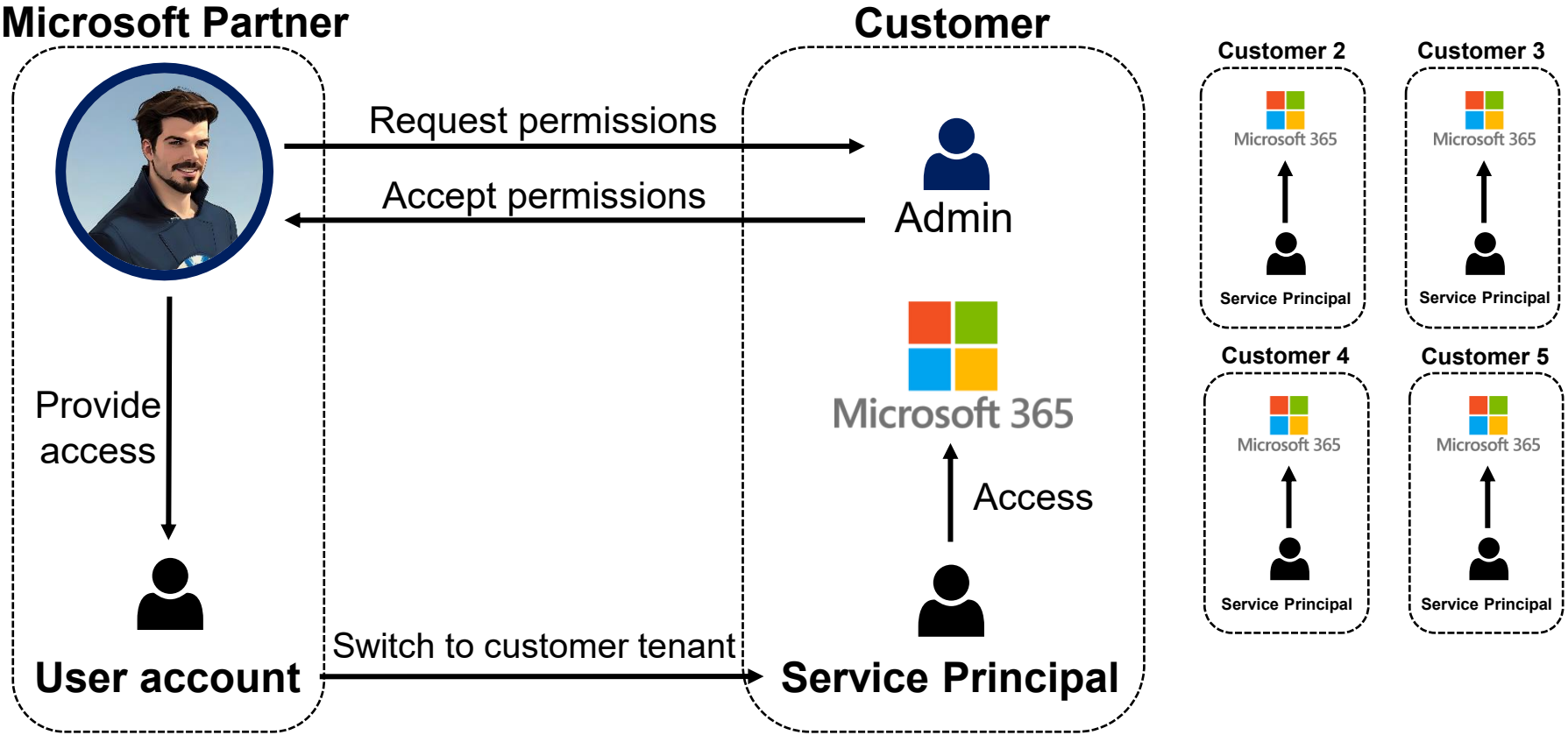
Three options to grant access

Access through **User** Account

Access through **Guest** Account

Access through **GDAP**

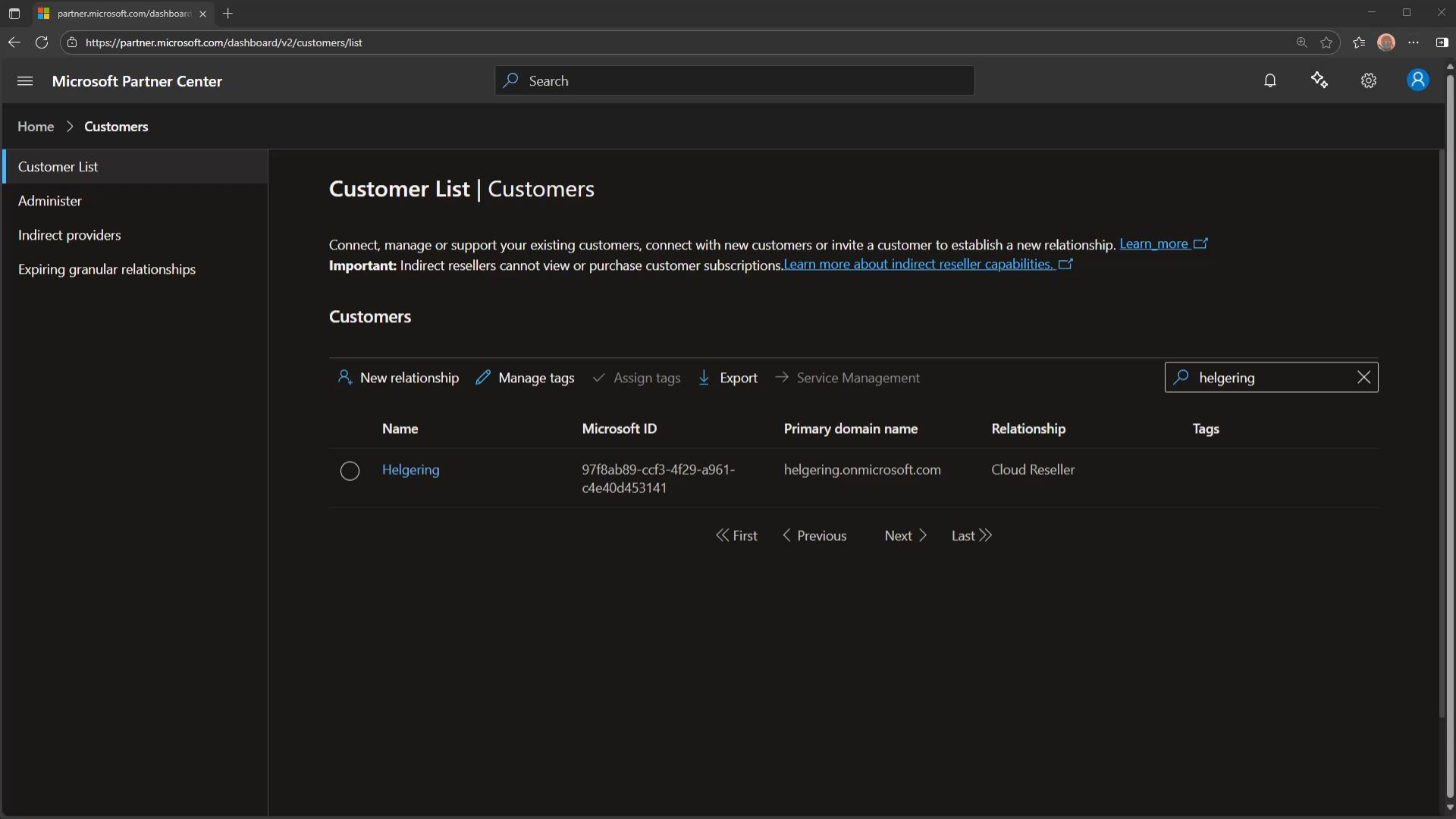
Granular Delegated Admin Permissions (GDAP)



Option 3: Access through GDAP

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

Demo: Access through GDAP


partner.microsoft.com/dashboard
https://partner.microsoft.com/dashboard/v2/customers/list
Microsoft Partner Center
Search
Home
Customers
Customer List
Administer
Indirect providers
Expiring granular relationships
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
New relationship
Manage tags
Assign tags
Export
Service Management
helgering
Name
Microsoft ID
Primary domain name
Relationship
Tags
Helgering
97f8ab89-ccf3-4f29-a961-c4e40d453141
helgering.onmicrosoft.com
Cloud Reseller
First
Previous
Next
Last

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

M365 Lighthouse

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

Demo: M365 Lighthouse

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

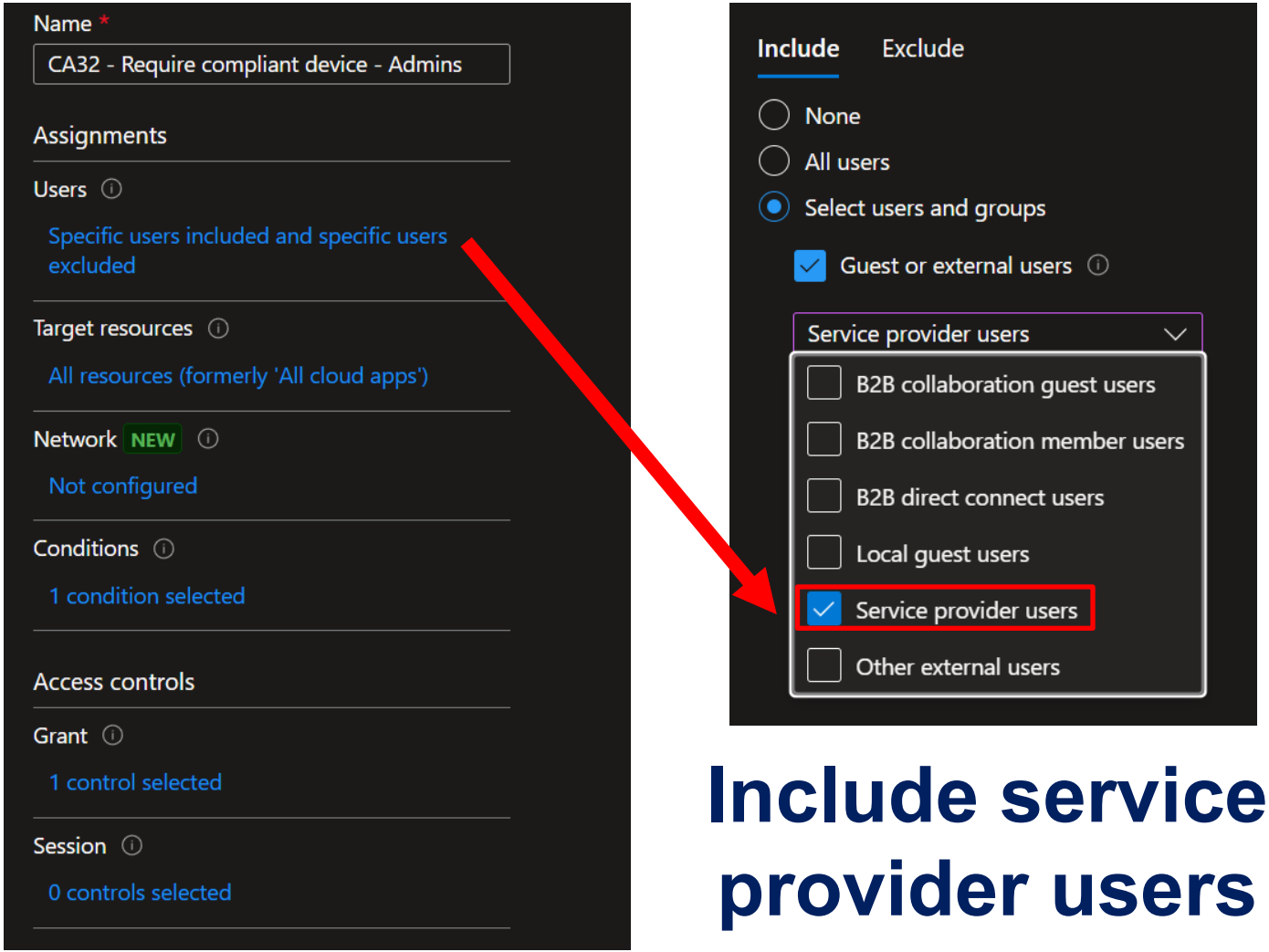
SharePoint

Option 3: Access through GDAP

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

Device Compliance

- Works the same as “Option 2: Guest Account” ✅
- Make sure you include the service provider users in your conditional access policy



Include service provider users

Option 3: Access through GDAP

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

Delegated Admin Permissions (DAP)

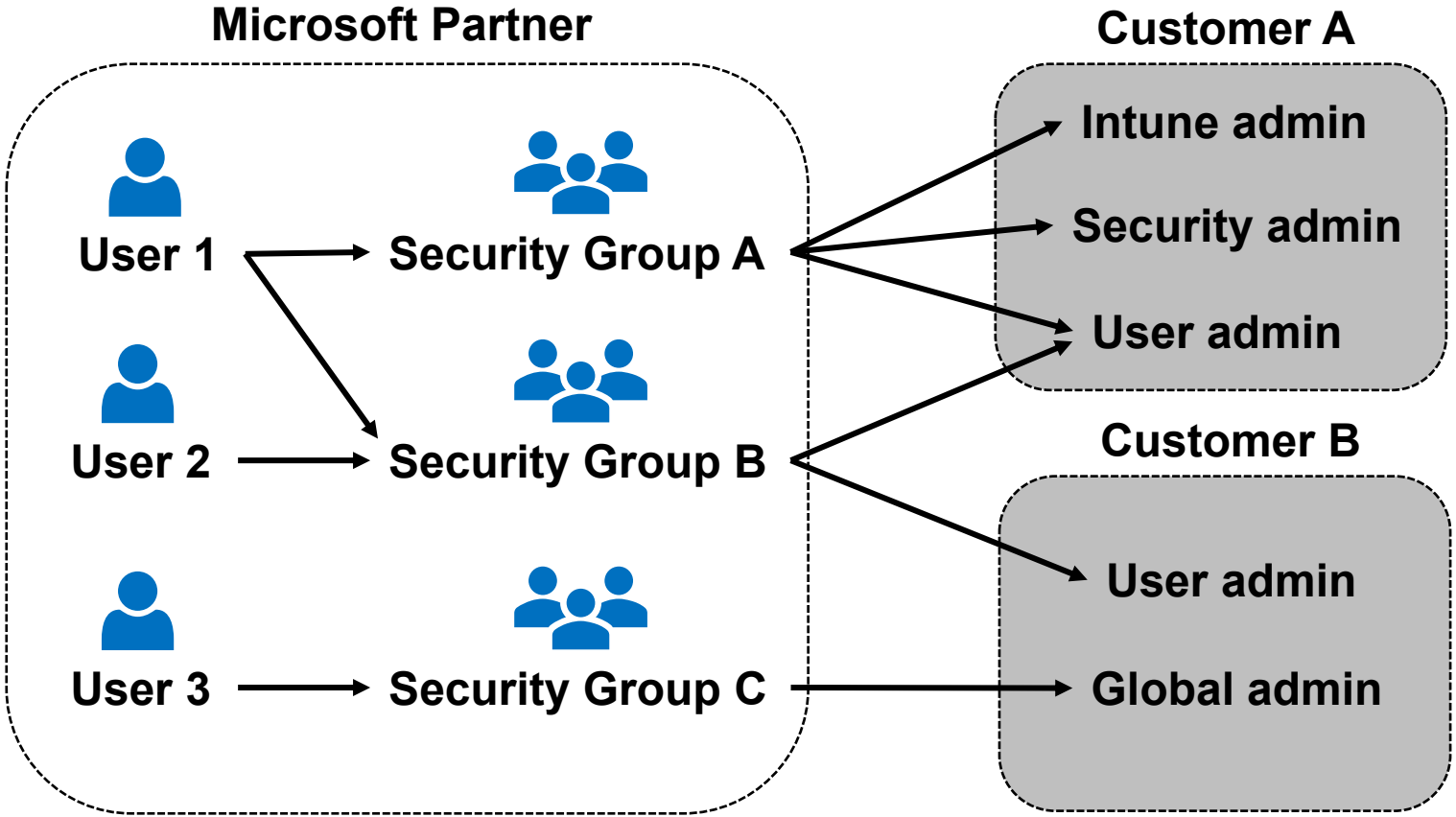
- Overprivileged access
- Indefinite access
- Limited audit logging
- Vulnerable to threat actors

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




NO, GOD! NO, GOD, PLEASE NO! NO! NO!
NOOOOOOOOOOOO!

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	Eligible
Customer B	CustomerB_T2	Intune administrator Exchange administrator	Eligible

GDAP + PIM (customer + role based)

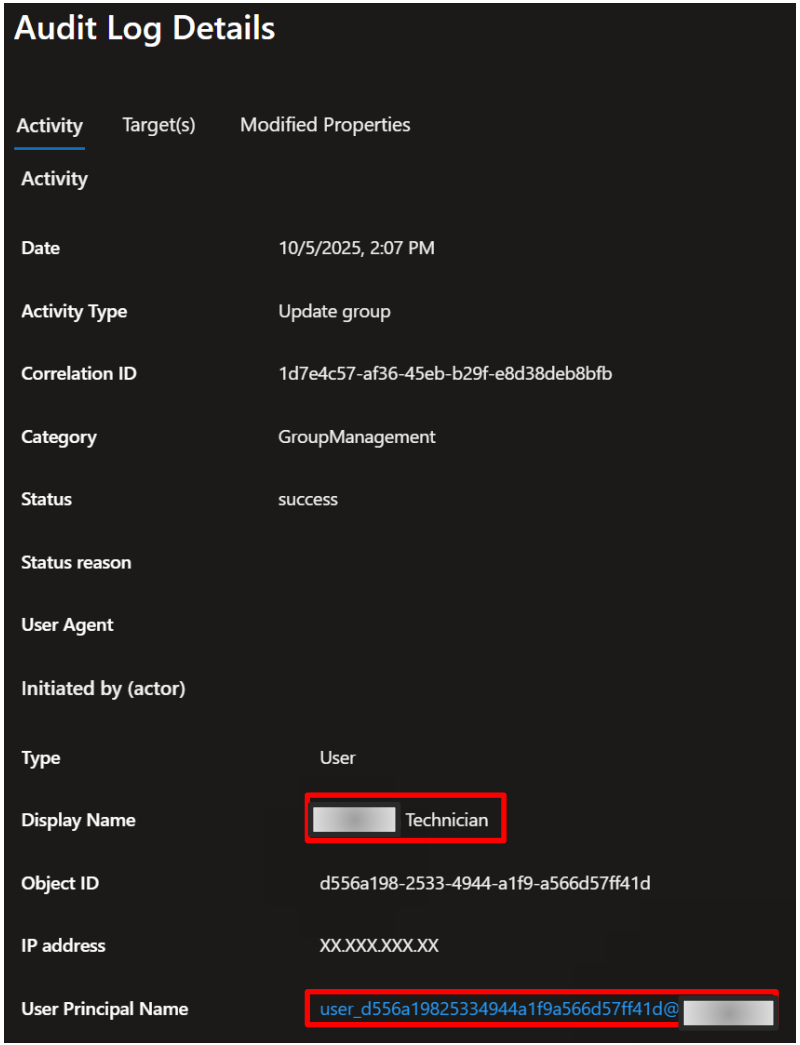
Customer	Sec Group	Roles	PIM
Customer A Customer B Customer C	Service desk	Global reader Helpdesk admin	Permanent
Customer A	CustomerA_T2	Intune administrator Exchange administrator	Eligible
Customer A	CustomerA_T3	Global administrator	Approval
Customer B	CustomerB_T2	Intune administrator Exchange administrator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

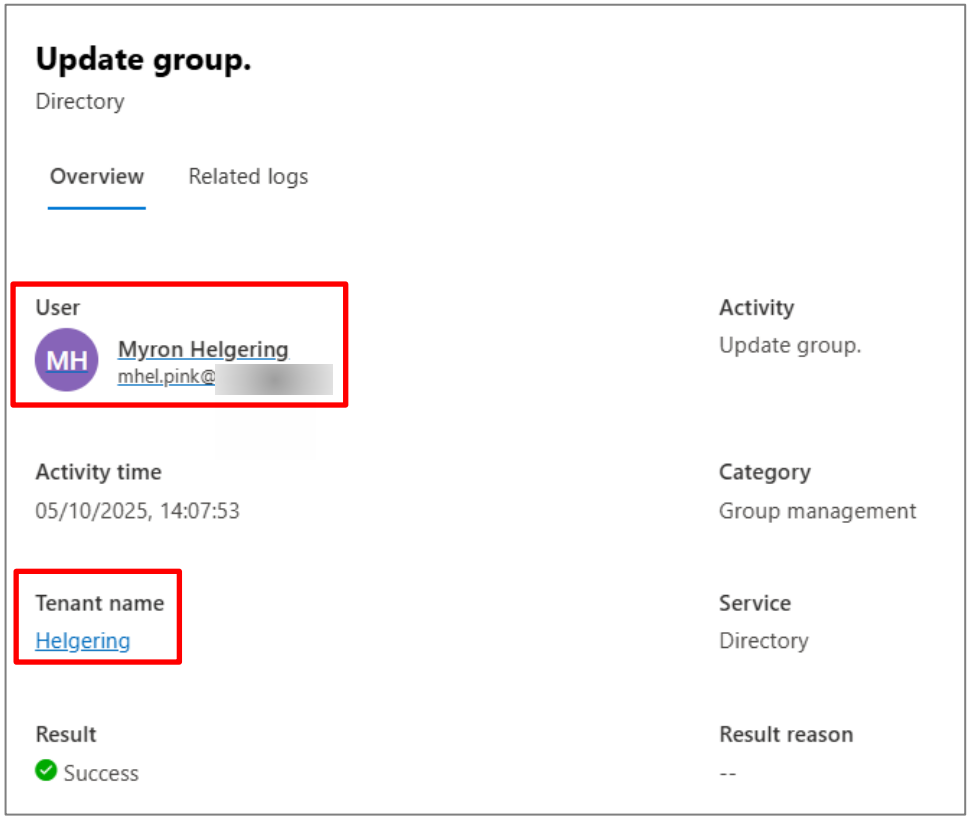
Scenario	User Experience	Device Compliance	Permissions	Overall Security
User Account	★★★	★	★★★	★★★
Guest Account	★	★★	★★★	★★
GDAP Access	★★	★★	★★	



Audit logs from Customer Perspective

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

Audit logs from MSP Perspective



- 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	Overall Security
User Account	⭐⭐⭐	⭐	⭐⭐⭐	⭐⭐⭐
Guest Account	⭐	⭐⭐	⭐⭐⭐	⭐⭐
GDAP Access	⭐⭐	⭐⭐	⭐⭐	⭐

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 your external admins only need access to specific admin portals that are accessible.
- 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!

Thank you!