

Fast Focus: Configuring Cross-Tenant Access for Secure Collaboration

Myron Helgering
Tech Lead Security
Pink Elephant

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!



Agenda

- Introduction
- Scenario
- Configuration demo's
- User experience demo's
- Considerations and takeaways



About me

- Technology Lead Security
- Microsoft Security MVP
- Blogger and Speaker
- Huge fantasy geek



Myron Helgering



in/myronhelgering



myronhelgering.com

TECHMENTOR
IN-DEPTH TRAINING FOR IT PROS

× **Cybersecurity** **LIVE!**
DEFENDING AGAINST RANSOMWARE AND OTHER ATTACKS

Scenario

- Guest user is coming from the **Pink Elephant** tenant.
- Our company tenant is the **Helgering** tenant.
- The guest user **has been invited** to our tenant.
- We want to **enforce MFA** and a **compliant device** on guest users coming from the Pink Elephant tenant.
- The guest user works on a **compliant device** managed by the Pink Elephant tenant and has **already signed in with MFA**.

Demo: Configuring Conditional Access policy for B2B guests in Microsoft Entra

Learn about upcoming depreciations, breaking, feature, and UX changes.

Demo: B2B Guest User Experience **without cross tenant access settings**

Azure services

Create a resource

Microsoft Entra Privileged...

Quickstart Center

Foundry

Kubernetes services

Virtual machines

App Services

Storage accounts

SQL databases

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

Conditional Access Policy details

↑ Previous ↓ Next

Policy: Require MFA and device compliance for B2B guests

Policy state: Enabled

Result: Failure

Assignments

User

Myron Helgering (Pink Elephant)

✓ Matched

Resource

Azure Resource Manager

✓ Matched

Conditions

Sign-in risk

None

● Not configured

Device platform

Windows10

● Not configured

Network (formerly location)

Utrecht, NL

2001:1c00:6094:2a00:e942:5667:b2ea:844f ⓘ

● Not configured

Client app

Browser

● Not configured

Device

{PII Removed}

● Not configured

User risk

● Not configured

Insider risk ⓘ

● Not configured

Authentication flows

● Not configured

Access controls

Grant Controls

✗ Not satisfied

Session Controls

● Not configured



Matched

B2B guest user assignment

Conditional access policy details



Not satisfied

Require multifactor authentication
Require compliant device

Demo: Configuring cross tenant access settings in Microsoft Entra

-  Home
-  Security Copilot agents
-  Security Copilot chat
-  Favorites

▼
-  Entra ID

^
-  Overview
-  Users
-  Groups
-  Devices
-  Agents
-  Enterprise apps
-  App registrations
-  Roles & admins
-  Delegated admin partners
-  Tenant governance (Preview)

Microsoft Entra

[Automate onboarding and manage user lifecycles with access to all applications](#)

[Secure internet access based on specific business needs](#)

Microsoft Entra plan

Entra Suite

[View licenses](#)

Knowledge center



Microsoft Learn for Entra
Build your skills for creating secure identities and access with the Microsoft Entra Family.



Microsoft Mechanics
The official Microsoft video series that shows you how to get the most from the software, service, and hardware built.



Support and troubleshooting
Tell us about your issue to get solutions and support.



Change announcements
Learn about upcoming depreciations, breaking, feature, and UX changes.

Demo: B2B Guest User Experience **with cross tenant access settings**

Azure services

Create a resource

Microsoft Entra Privileged...

Quickstart Center

Foundry

Kubernetes services

Virtual machines

App Services

Storage accounts

SQL databases

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

Conditional Access Policy details

↑ Previous ↓ Next

Policy: Require MFA and device compliance for B2B guests

Policy state: Enabled

Result: Success

Assignments

User

Myron Helgering (Pink Elephant)

✓ Matched

Resource

Azure Resource Manager

✓ Matched

Conditions

Sign-in risk

None

● Not configured

Device platform

Windows10

● Not configured

Network (formerly location)

Utrecht, NL

2001:1c00:6094:2a00:e942:5667:b2ea:844f ⓘ

● Not configured

Client app

Browser

● Not configured

Device

(PII Removed)

● Not configured

User risk

● Not configured

Insider risk ⓘ

● Not configured

Authentication flows

● Not configured

Access controls

Grant Controls

✓ Satisfied

Session Controls

● Not configured



Matched

B2B guest user assignment

Conditional access policy details



Satisfied

Require multifactor authentication
Require compliant device



The device compliant with
“our” policies, right?

Probably not

Encryption

Require encryption of data storage on device. ⓘ

Require

Not configured

Device Security

Firewall ⓘ

Require

Not configured

Trusted Platform Module (TPM) ⓘ

Require

Not configured

Antivirus ⓘ

Require

Not configured

Antispyware ⓘ

Require

Defender

Microsoft Defender Antimalware ⓘ

Require

Microsoft Defender Antimalware minimum version ⓘ

Not configured

Microsoft Defender Antimalware security intelligence up-to-date ⓘ

Require

Real-time protection ⓘ

Require



Devices | Compliance



Search



Overview



All devices



Device query



Monitor



By platform



Windows



Apple mobile



macOS



Android



Linux

Policies

Notifications

Retire noncompliant devices

Compliance settings



Save



Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

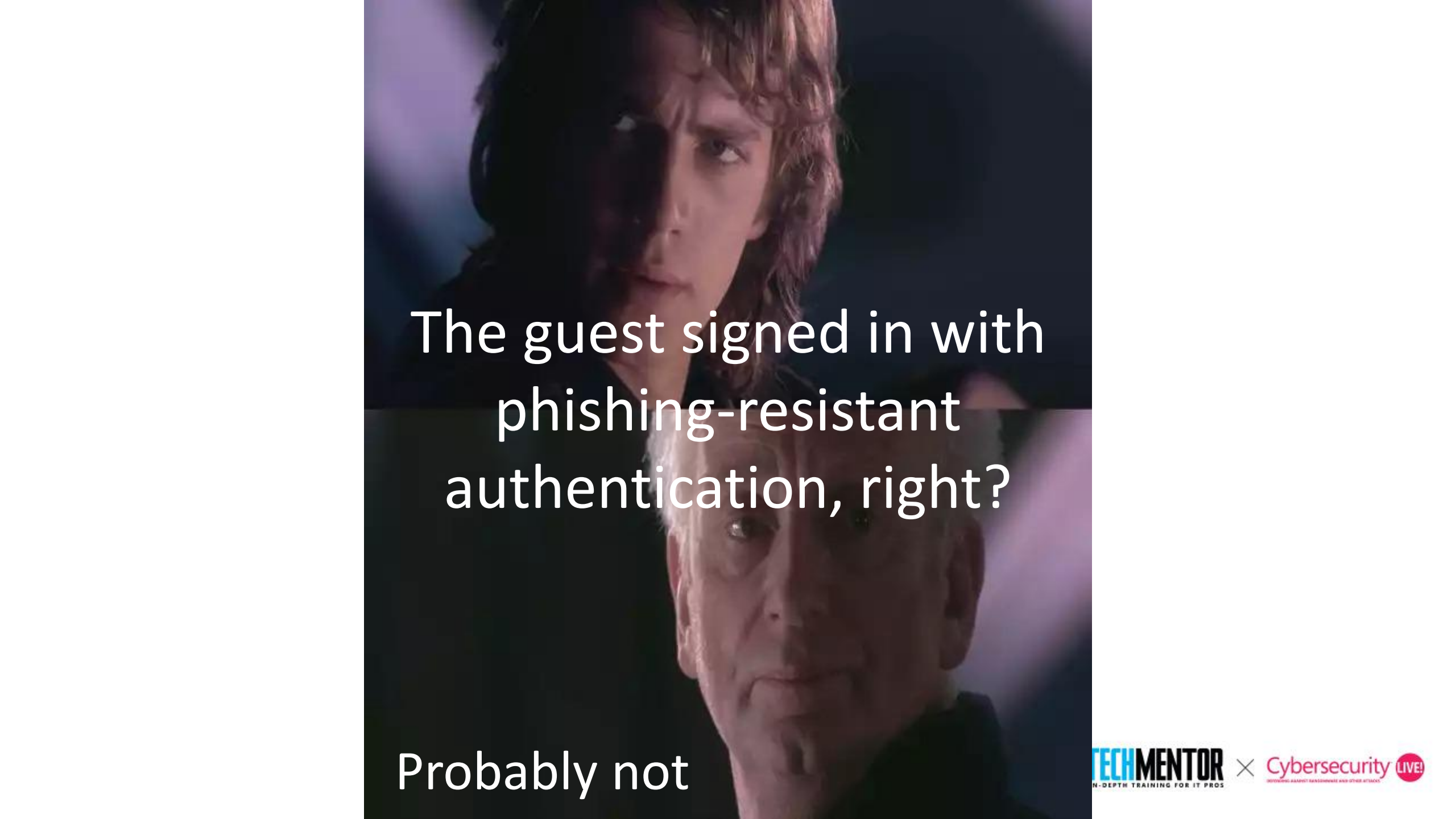
Mark devices with no compliance policy assigned as ⓘ



Compliant

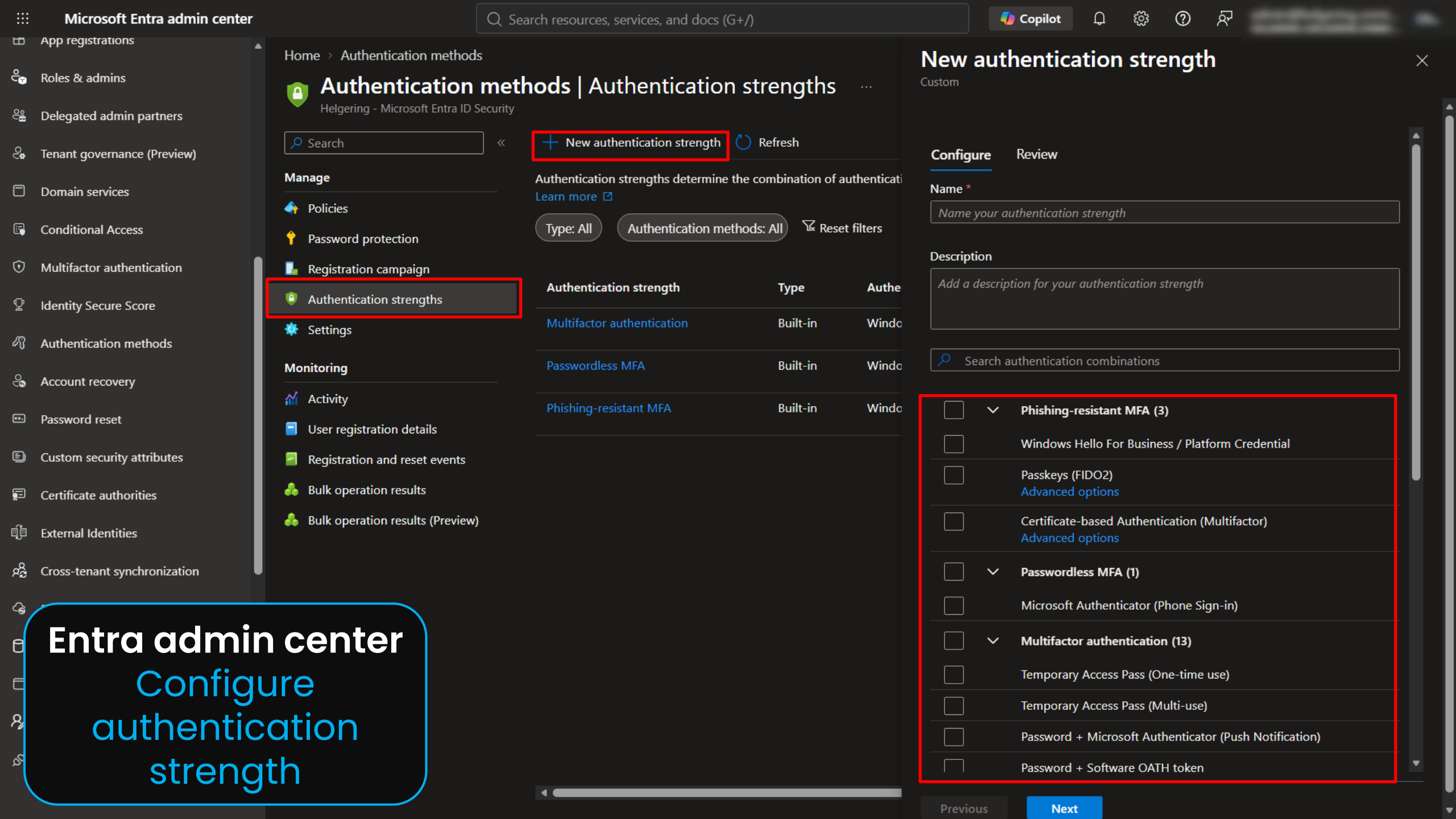
Compliance status validity period (days) ⓘ

30



The guest signed in with
phishing-resistant
authentication, right?

Probably not



- App registrations
- Roles & admins
- Delegated admin partners
- Tenant governance (Preview)
- Domain services
- Conditional Access
- Multifactor authentication
- Identity Secure Score
- Authentication methods
- Account recovery
- Password reset
- Custom security attributes
- Certificate authorities
- External Identities
- Cross-tenant synchronization

Home > Authentication methods



Authentication methods | Authentication strengths

Helgering - Microsoft Entra ID Security

Search

+ New authentication strength

Refresh

Manage

🏠 Policies

🔑 Password protection

📄 Registration campaign

🛡️ Authentication strengths

⚙️ Settings

Monitoring

📊 Activity

📄 User registration details

📄 Registration and reset events

👥 Bulk operation results

👥 Bulk operation results (Preview)

Authentication strengths determine the combination of authentication
[Learn more](#)

Type: All

Authentication methods: All

🗑️ Reset filters

Authentication strength	Type	Authen
Multifactor authentication	Built-in	Windo
Passwordless MFA	Built-in	Windo
Phishing-resistant MFA	Built-in	Windo

New authentication strength

Custom

Configure

Review

Name *

Name your authentication strength

Description

Add a description for your authentication strength

Search authentication combinations

- ☐ ☒ Phishing-resistant MFA (3)
 - ☐ Windows Hello For Business / Platform Credential
 - ☐ Passkeys (FIDO2)
[Advanced options](#)
 - ☐ Certificate-based Authentication (Multifactor)
[Advanced options](#)
- ☐ ☒ Passwordless MFA (1)
 - ☐ Microsoft Authenticator (Phone Sign-in)
- ☐ ☒ Multifactor authentication (13)
 - ☐ Temporary Access Pass (One-time use)
 - ☐ Temporary Access Pass (Multi-use)
 - ☐ Password + Microsoft Authenticator (Push Notification)
 - ☐ Password + Software OATH token

Previous

Next

Entra admin center
Configure
authentication
strength

Change the MFA requirement

Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multifactor authentication ⓘ

☐ Require authentication strength ⓘ



Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication ⓘ

☒ Require authentication strength ⓘ
Strong authentication ▼

Authentication methods support for registration

Authentication method	Home tenant	Resource tenant
Text message as second factor	✓	✓
Voice call	✓	✓
Microsoft Authenticator push notification	✓	✓
Microsoft Authenticator phone sign-in	✓	
OATH software token	✓	✓
OATH hardware token	✓	
FIDO2 security key	✓	
Windows Hello for Business	✓	
Certificate-based authentication	✓	

Passkey registration

- **Passkey registration** for guest users is currently **not supported** (it will be supported by the end of 2026).
- Guest users need to have **their passkey registered previously** in their home tenant.

Takeaways

- Use **cross-tenant access settings** to reduce friction and enable collaboration.
- Trust **compliant device claims**, but only from trusted partners.
- Only enforce **authentication methods** that guest users can register or have registered.

Time for questions!

Other sessions @ Cybersecurity Live!

- Tuesday, August 4, 2026
 - Creating Classifiers from Scratch to Identify Sensitive Data with Microsoft Purview **(1:15pm – 2:30pm)**
- Wednesday, August 5, 2026
 - Edge for Business in 2026: Is the Browser Becoming the New Security Perimeter? **(8:00am – 9:15am)**
 - Configuring Cross-Tenant Access for Secure Collaboration **(1:15pm – 1:40pm)**
 - How to Protect Your Business from the Threat of Unmanaged Devices **(2:30pm – 3:45pm)**

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!

