Take Zero Trust to the next level with Azure AD Authentication Methods, Strengths & Contexts!

Pim Jacobs & Jan Bakker

Experts Live Netherlands

Pim Jacobs

Principal Consultant @ InSpark

Microsoft MVP Security

Let's connect!

Blog: https://www.identity-man.eu/

Mail: pim.jacobs@inspark.nl

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Microsoft® Most Valuable Professional

Jan Bakker

Self-employed

aka.ms/janbakker

Ramblings:

JANBAKKER.TECH

sharing is caring

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Agenda

- Zero-trust is important
- Authentication Methods
- Authentication Strengths
- Authentication Context
- Next Steps & Key Take aways

Zero Trust is important

Zero Trust principles

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC


We’re no longer
protecting
office buildings

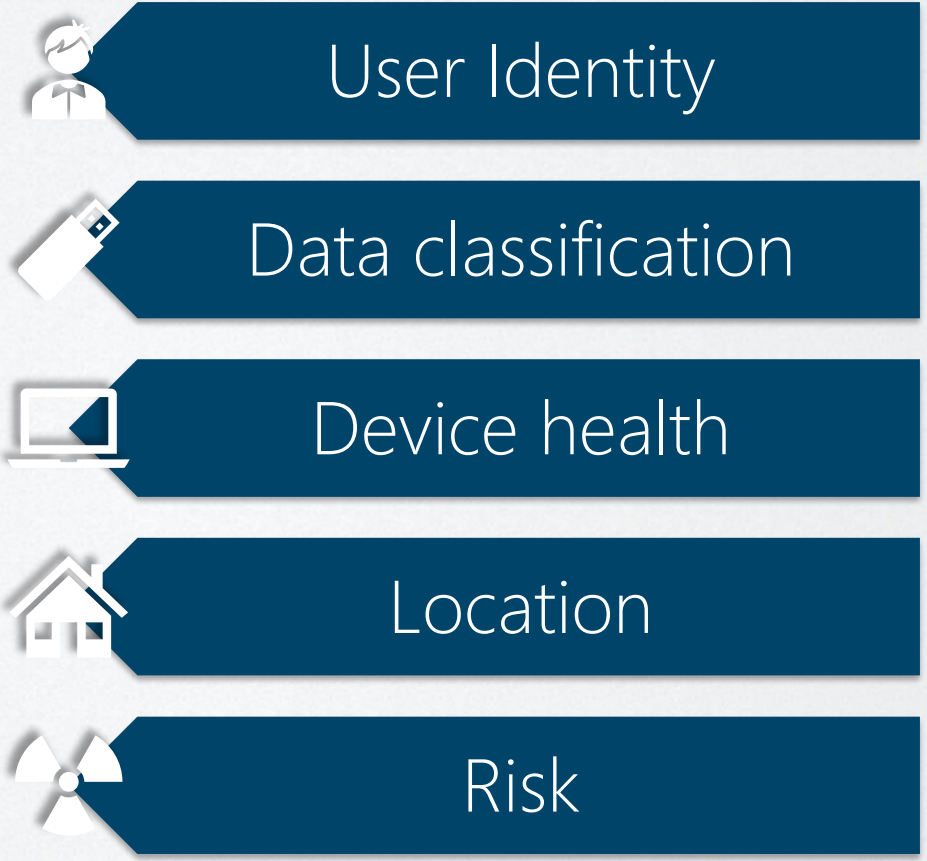

We’re protecting
everyone’s kitchens


And
beach
houses
in Hawaii

Everything behind the corporate firewall is safe.

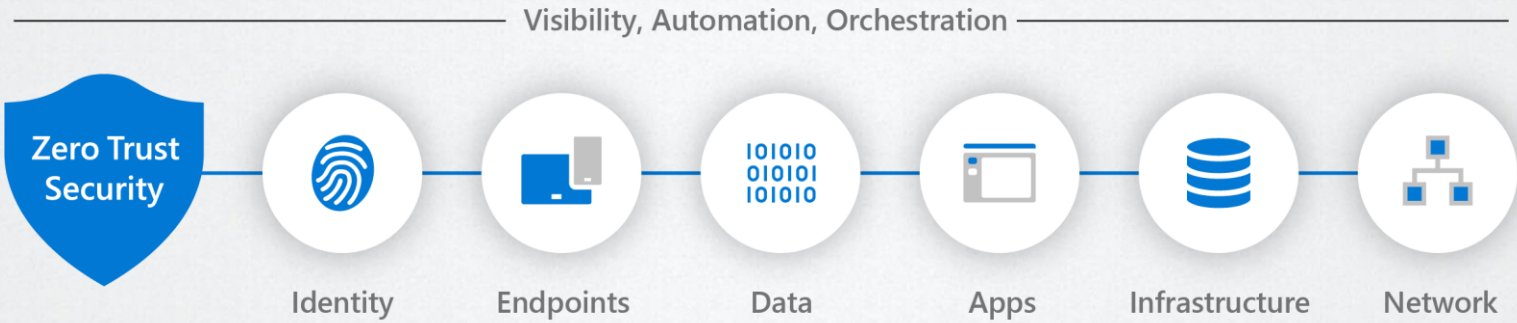
Everything behind the corporate firewall is no longer safe.

Always **verify** based on all available datapoints



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Zero Trust across all workloads



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Identity to the next level!

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

The 'Jungle' of authentication

- Allowed for registration
- Usable for authentication

Methods

- Limits the use of usable methods
- Dynamically targeted

Strengths

- Requires step-up authentication
- Dynamically targeted

Context

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Authentication Methods

Maturity Level 0

Security posture	None

Weak overall security posture

	Maturity Level 0	Maturity Level 1
Security posture	None	Low
	Weak overall security posture	Protect from opportunistic adversaries using commodity attacks

	Maturity Level 0	Maturity Level 1	Maturity Level 2
Security posture	None	Low	Medium
	Weak overall security posture	Protect from opportunistic adversaries using commodity attacks	Protect from targeted attackers using effective, well-known attacks

	Maturity Level 0	Maturity Level 1	Maturity Level 2	Maturity Level 3
Security posture	None	Low	Medium	High
	Weak overall security posture	Protect from opportunistic adversaries using commodity attacks	Protect from targeted attackers using effective, well-known attacks	Protect from targeted attackers using non-public tools and techniques

Strong authentication maturity levels

Maturity Level 0:
No MFA

qwerty123
Password

Email OTP

Maturity Level 1:
Password and…

Voice

SMS

Maturity Level 2:
Password and…

Microsoft Authenticator *

Hardware Tokens OTP

Software Tokens OTP

Maturity Level 3:
Phishing-resistant

Certificate-based authentication

FIDO2 security key

Windows Hello

* Includes Microsoft Authenticator Passwordless

Method	Primary authentication	Secondary authentication
Windows Hello for Business	Yes	MFA*
Microsoft Authenticator	Yes	MFA and SSPR
Authenticator Lite	No	MFA
FIDO2 security key	Yes	MFA
Certificate-based authentication	Yes	No
OATH hardware tokens (preview)	No	MFA and SSPR
OATH software tokens	No	MFA and SSPR
SMS	Yes	MFA and SSPR
Voice call	No	MFA and SSPR
Password	Yes	


TIME
FOR
CHANGE

SSPR Settings

Number of methods required to reset ⓘ

1 2

Methods available to users

- [ ] Mobile app notification
- [x] Mobile app code
- [x] Email
- [x] Mobile phone (SMS only)
- [ ] Office phone ⓘ
- [ ] Security questions

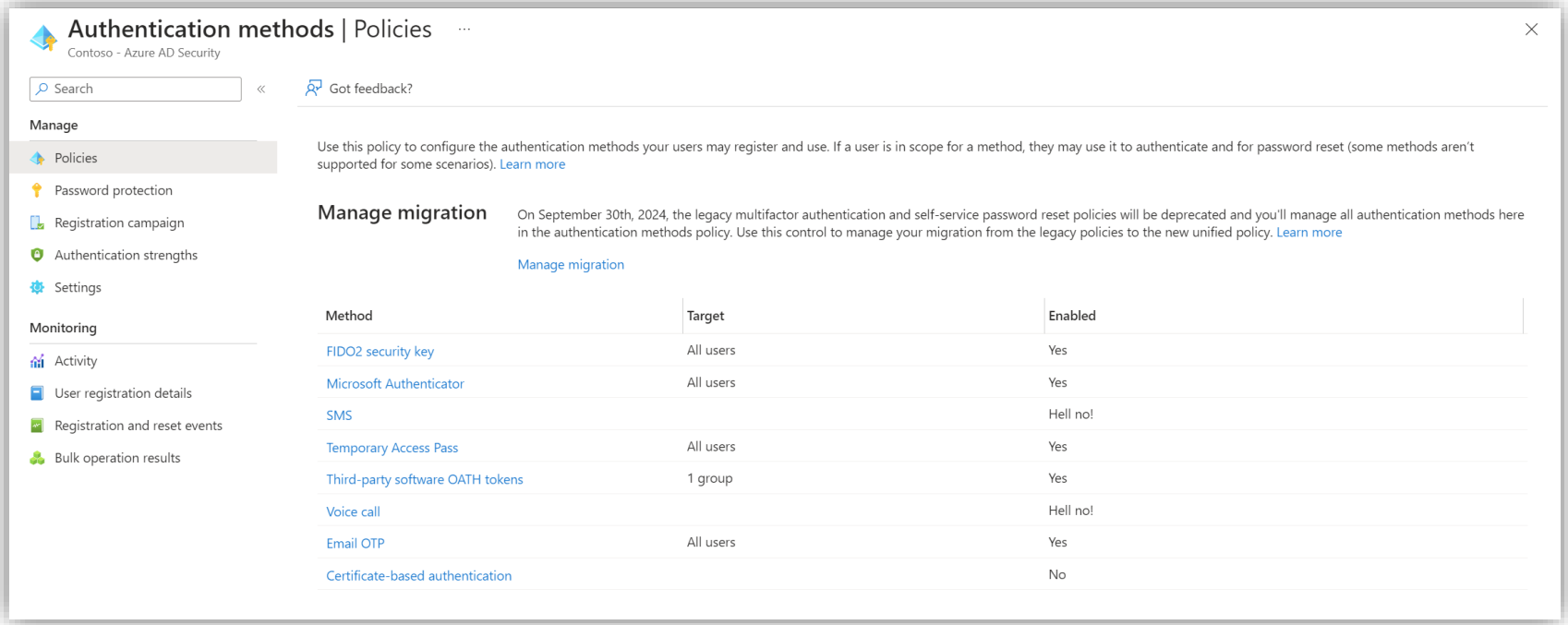
Tenant-wide MFA settings

verification options (learn more)

Methods available to users:

- [ ] Call to phone
- [x] Text message to phone
- [x] Notification through mobile app
- [x] Verification code from mobile app or hardware token

Authentication methods policies



Microsoft Authenticator settings ...

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or
devices. Learn more.

Enable and Target **Configure**

Note: Users must be included as part of the Microsoft Authenticator targeted groups under th

GENERAL

Allow use of Microsoft Authenticator OTP Yes **No**

Require number matching for push notifications

Third-party software OATH tokens settings ...

Software OATH tokens are applications that use the OATH TOTP standard and a secret key to generate 6-digit codes used to authe
non-Microsoft software OATH tokens. Microsoft Authenticator can also generate software OATH codes and is managed in the Micr
Software OATH token is not usable as a first-factor authentication method.

Enable and Target

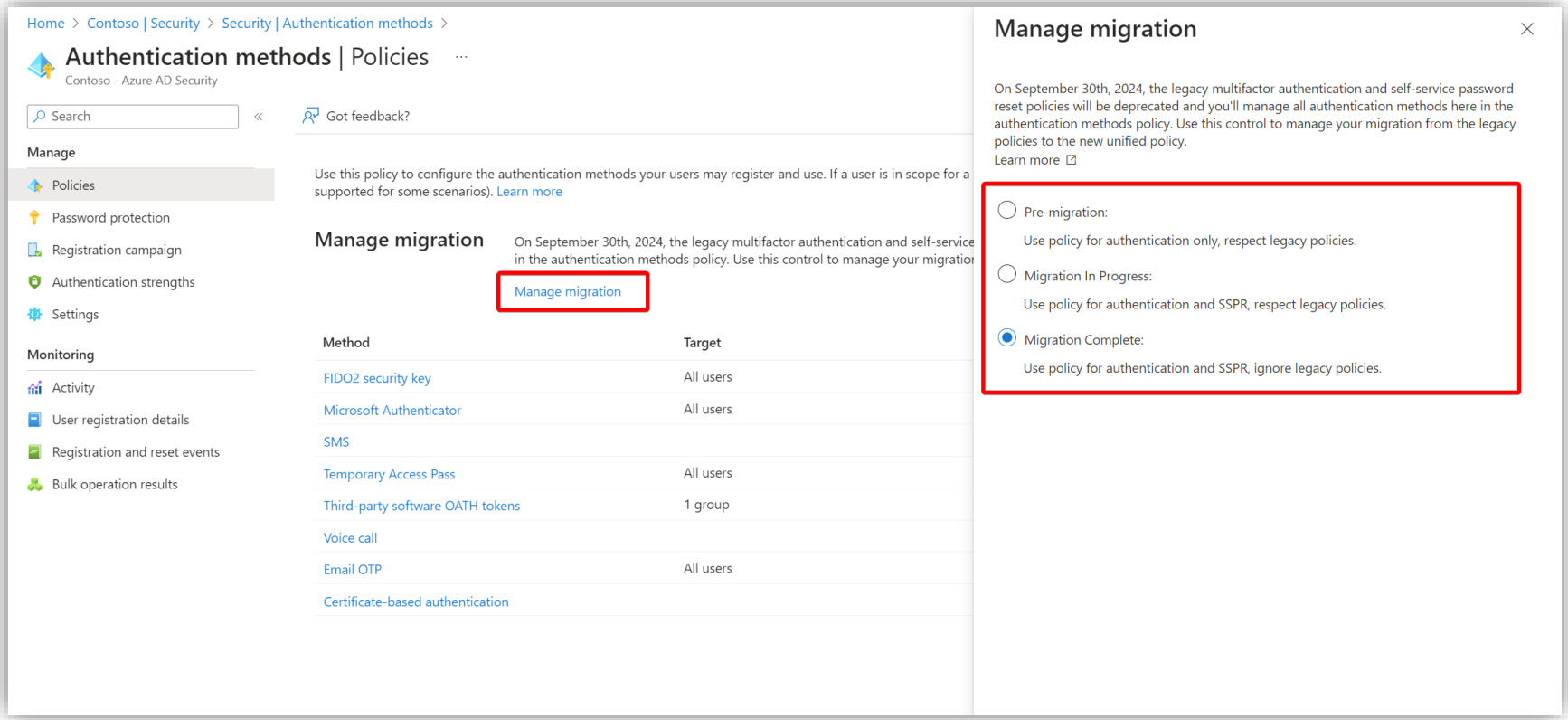
Enable

Include Exclude

Target All users Select groups

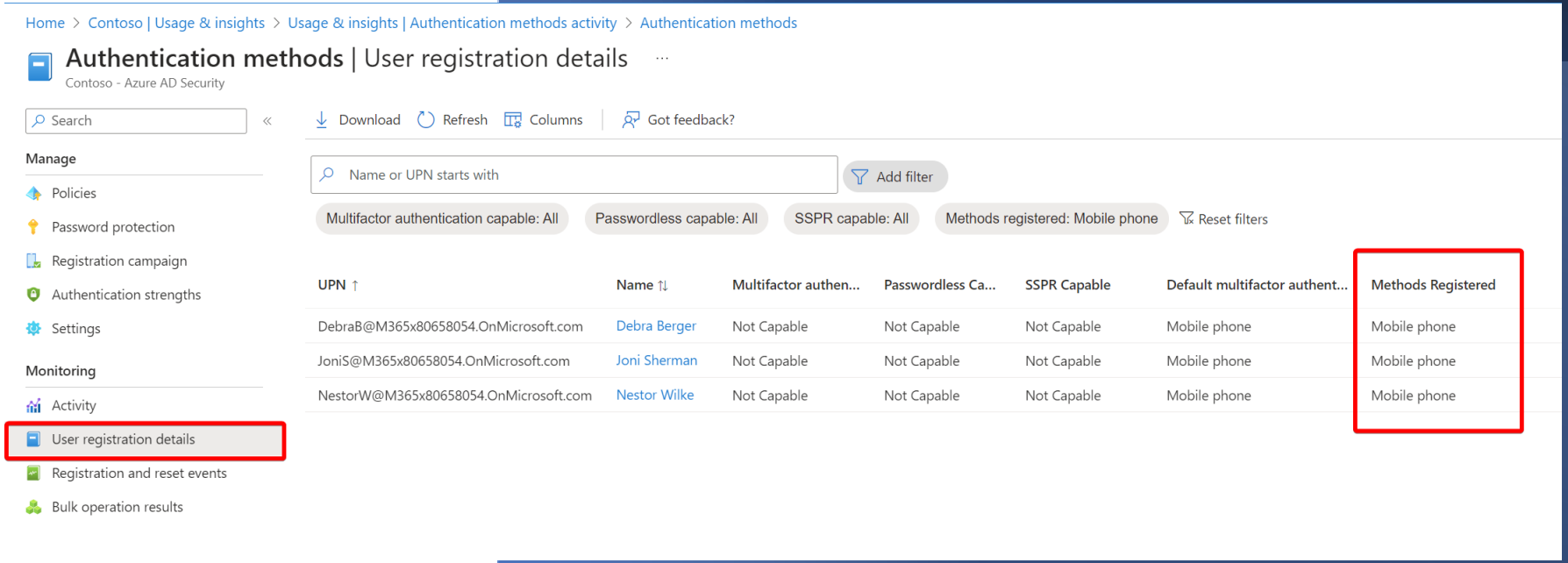
Add groups

Name	Type
AuthMethods-Allow3rdPartyApps	Group


Home > Contoso | Security > Security | Authentication methods >
Authentication methods | Policies
Contoso - Azure AD Security
Search
Got feedback?
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a
supported for some scenarios). Learn more
Manage migration
On September 30th, 2024, the legacy multifactor authentication and self-service
in the authentication methods policy. Use this control to manage your migratio
Manage migration
Method
Target
FIDO2 security key
All users
Microsoft Authenticator
All users
SMS
Temporary Access Pass
All users
Third-party software OATH tokens
1 group
Voice call
Email OTP
All users
Certificate-based authentication
Manage migration
On September 30th, 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy.
Learn more
Pre-migration:
Use policy for authentication only, respect legacy policies.
Migration In Progress:
Use policy for authentication and SSPR, respect legacy policies.
Migration Complete:
Use policy for authentication and SSPR, ignore legacy policies.

Move to strong authentication methods

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC


Home > Contoso | Usage & insights > Usage & insights | Authentication methods activity > Authentication methods
Authentication methods | User registration details
Contoso - Azure AD Security
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Download
Refresh
Columns
Got feedback?
Name or UPN starts with
Add filter
Multifactor authentication capable: All
Passwordless capable: All
SSPR capable: All
Methods registered: Mobile phone
Reset filters
UPN
Name
Multifactor authen...
Passwordless Ca...
SSPR Capable
Default multifactor authent...
Methods Registered
DebraB@M365x80658054.OnMicrosoft.com
Debra Berger
Not Capable
Not Capable
Not Capable
Mobile phone
Mobile phone
JoniS@M365x80658054.OnMicrosoft.com
Joni Sherman
Not Capable
Not Capable
Not Capable
Mobile phone
Mobile phone
NestorW@M365x80658054.OnMicrosoft.com
Nestor Wilke
Not Capable
Not Capable
Not Capable
Mobile phone
Mobile phone

Authentication methods | Settings

Contoso - Azure AD Security

Manage

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

Monitoring

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

Report suspicious activity (Preview)

Allows users to report suspicious activities if they receive an authentication request that they did not initiate. This control is available when using the Microsoft Authenticator app and voice calls. Reporting suspicious activity will set the user's risk to high. If the user is subject to risk-based Conditional Access policies, they may be blocked.
Learn more

State * Microsoft managed

Target * All users / Select group

Reporting code * 0

System-preferred multifactor authentication

This setting designates whether the most secure multifactor authentication method is presented to users. Learn more
Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time. Learn more

State Microsoft managed

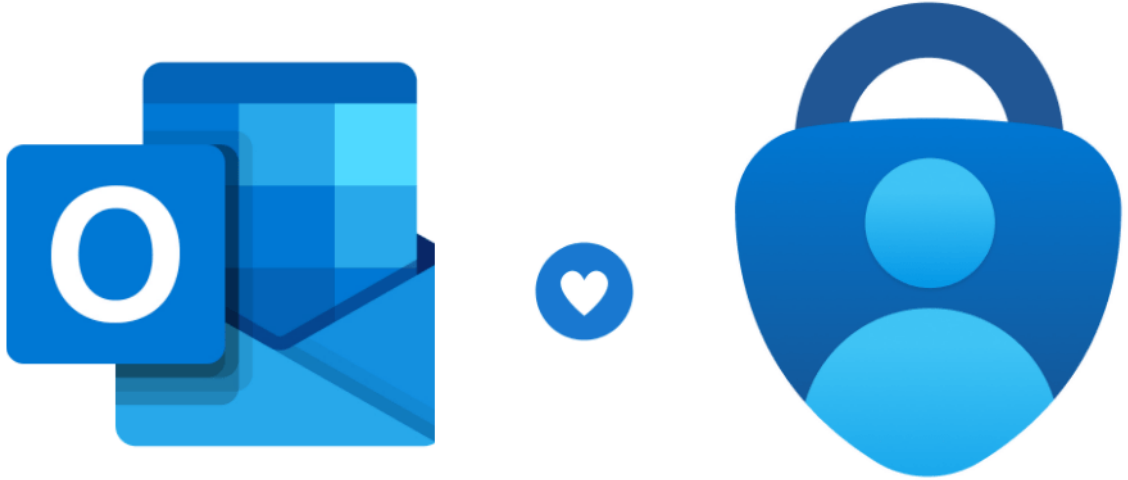
Include | Exclude

Target * All users / Select group

Save | Discard

1. Temporary Access Pass
2. Certificate-based authentication
3. FIDO2 security key
4. Microsoft Authenticator notification
5. Companion app notification
6. Microsoft Authenticator time-based one-time password (TOTP)
7. Companion app TOTP
8. Hardware token based TOTP
9. Software token based TOTP
10. SMS over mobile
11. OnewayVoiceMobileOTP
12. OnewayVoiceAlternateMobileOTP
13. OnewayVoiceOfficeOTP
14. TwowayVoiceMobile
15. TwowayVoiceAlternateMobile
16. TwowayVoiceOffice
17. TwowaySMSOverMobile

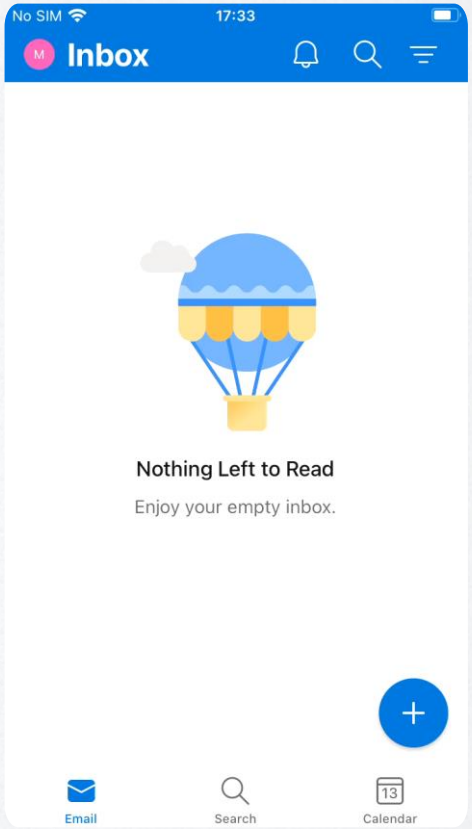
The user is prompted to sign-in with the most secure method according to the following order.



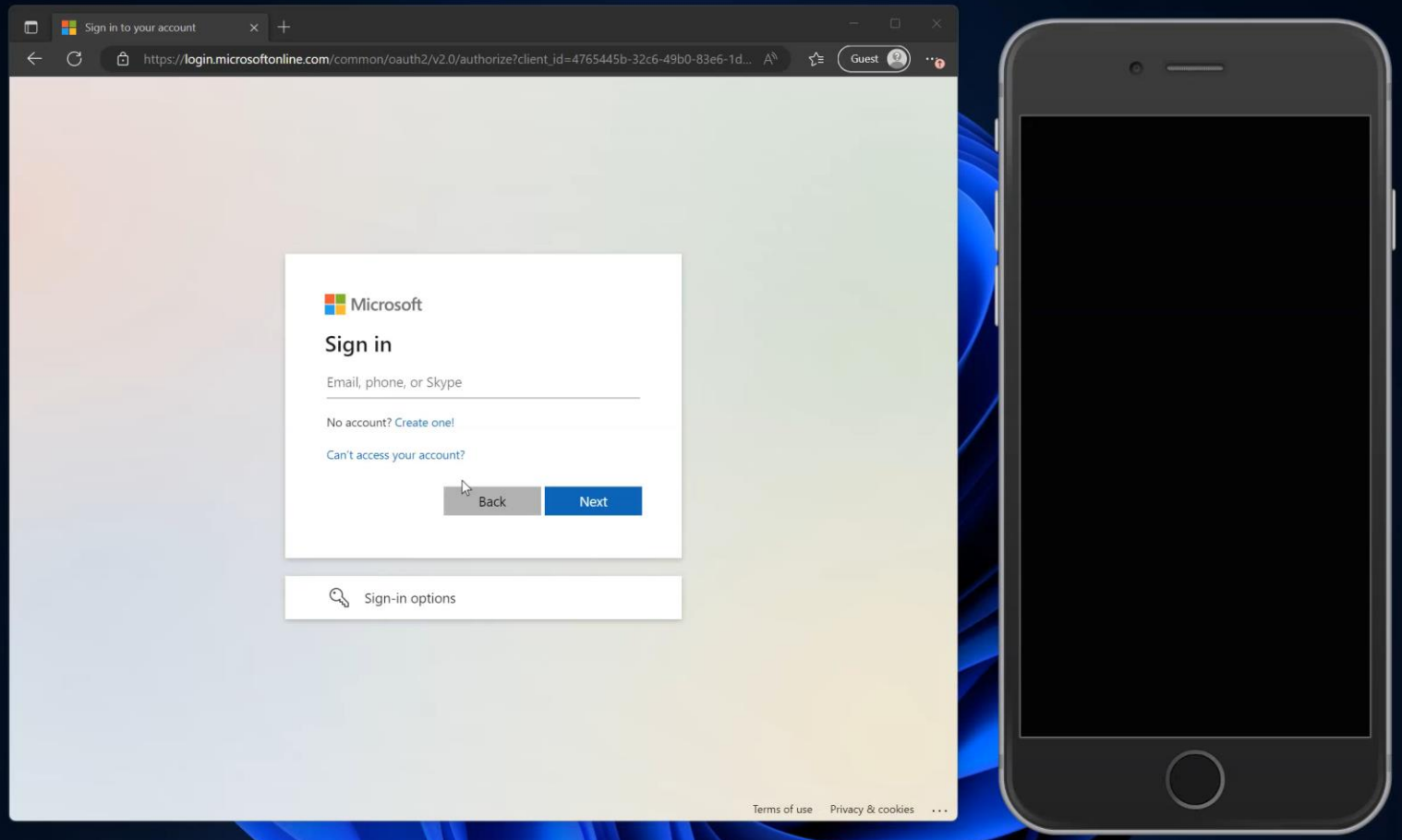
AUTHENTICATOR LITE

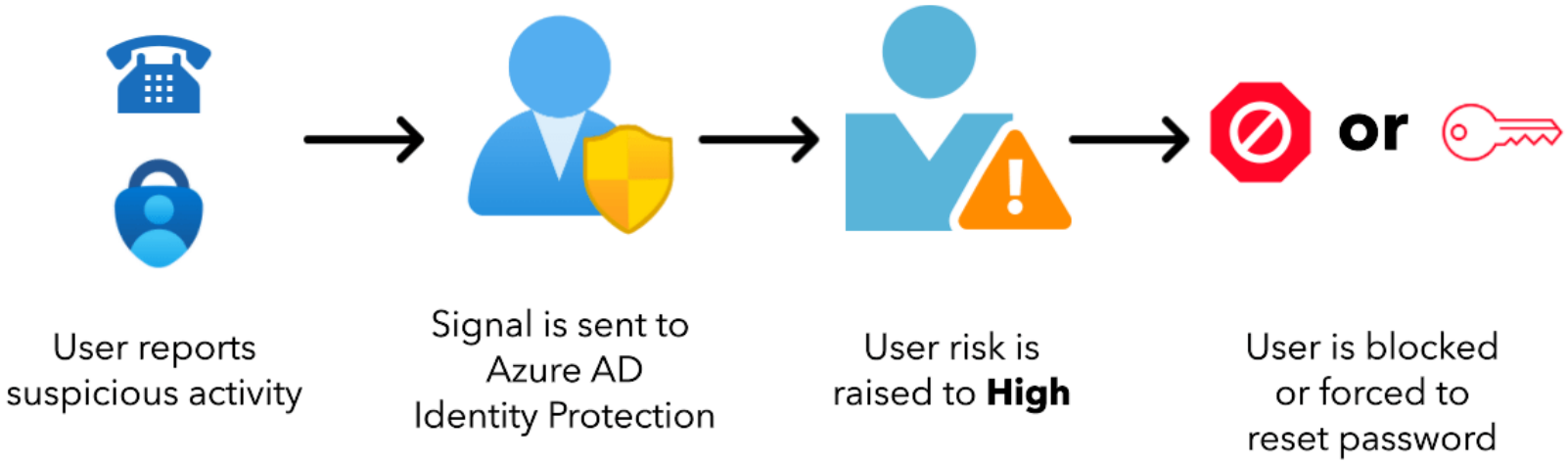
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

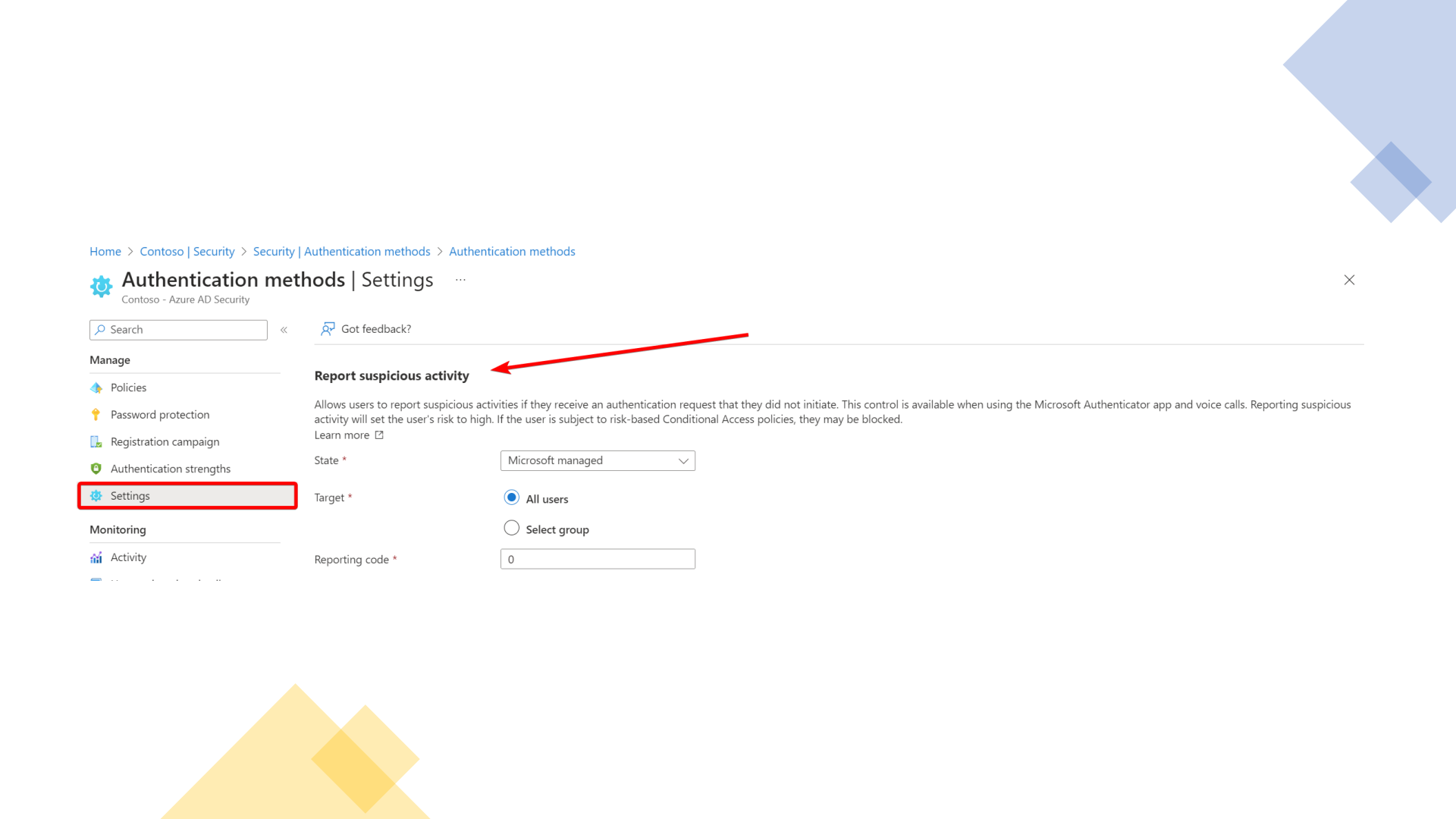
Enrollment with Temporary Access Pass



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC


Sign in to your account
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d...
Guest
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Sign-in options
Terms of use
Privacy & cookies


or
User reports suspicious activity
Signal is sent to Azure AD Identity Protection
User risk is raised to **High**
User is blocked or forced to reset password


Home > Contoso | Security > Security | Authentication methods > Authentication methods
Authentication methods | Settings
Contoso - Azure AD Security
Search
Got feedback?
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
Report suspicious activity
Allows users to report suspicious activities if they receive an authentication request that they did not initiate. This control is available when using the Microsoft Authenticator app and voice calls. Reporting suspicious activity will set the user's risk to high. If the user is subject to risk-based Conditional Access policies, they may be blocked.
Learn more
State *
Microsoft managed
Target *
All users
Select group
Reporting code *
0

Adele Vance | Audit logs

User

Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage
Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods

Troubleshooting + Support
New support request

Download | Refresh | Columns | Got feedback

Date : **Last 1 month** | Show dates as : **Local** | Service :

Date	Activity
5/4/2023, 2:28:06 PM	Fraud reported
5/4/2023, 2:28:06 PM	Suspicious acti
4/17/2023, 4:50:25 PM	Update user
4/17/2023, 4:50:25 PM	Update user
4/17/2023, 4:50:25 PM	Update user
4/17/2023, 4:50:25 PM	Update user
4/17/2023, 4:50:25 PM	Update user
4/6/2023, 11:33:22 AM	Update user

Audit Log Details

Activity | Target(s) | Modified Properties

Activity

Date	5/4/2023, 2:28 PM
Activity Type	Suspicious activity reported
Correlation ID	3101ebdb-fb63-4e5f-8a77-aad719f2ebbf
Category	UserManagement
Status	success
Status reason	Successfully reported suspicious activity
User Agent	

Initiated by (actor)

Type	User
Display Name	
Object ID	4c188483-1ac1-4593-a684-dd4e4986d8e2
User Principal Name	AdeleV@M365x341716.OnMicrosoft.com

Additional Details

AuthenticationMet...	Mobile app notification

Identity Protection | Risky users

Search

Overview
Tutorials
Diagnose and solve problems

Protect
User risk policy
Sign-in risk policy
Multifactor authentication registration policy

Report
Risky users
Risky workload identities
Risky sign-ins
Risk detections

Settings
Users at risk detected alerts
Weekly digest

Troubleshooting + Support
Troubleshoot
New support request

Learn more | Download | Select all | Confirm user(

Want to allow automatic risk remediation? Setup risk policies in Cond

Auto refresh : **Off** | Show dates as : **Local** | Risk stat

User	Risk state
Adele Vance	At risk
Megan Bowen	At risk
Debra Berger	At risk
Miriam Graham	At risk
Max Verstappen	At risk

Risky User Details

User's sign-ins | User's risky sign-ins | User's risk detections | Reset password | Confirm user compromised

Basic info | Recent risky sign-ins | Detections not linked to a sign-in | **Risk history**

Date	Activity	Actor	Risk state	Risk level
5/4/2023, 2:30:46 PM	User reported suspicious activity	Azure AD	At risk	High
2/27/2023, 8:44:01 PM	User performed secured password reset	Max Verstappen	Remediated	-

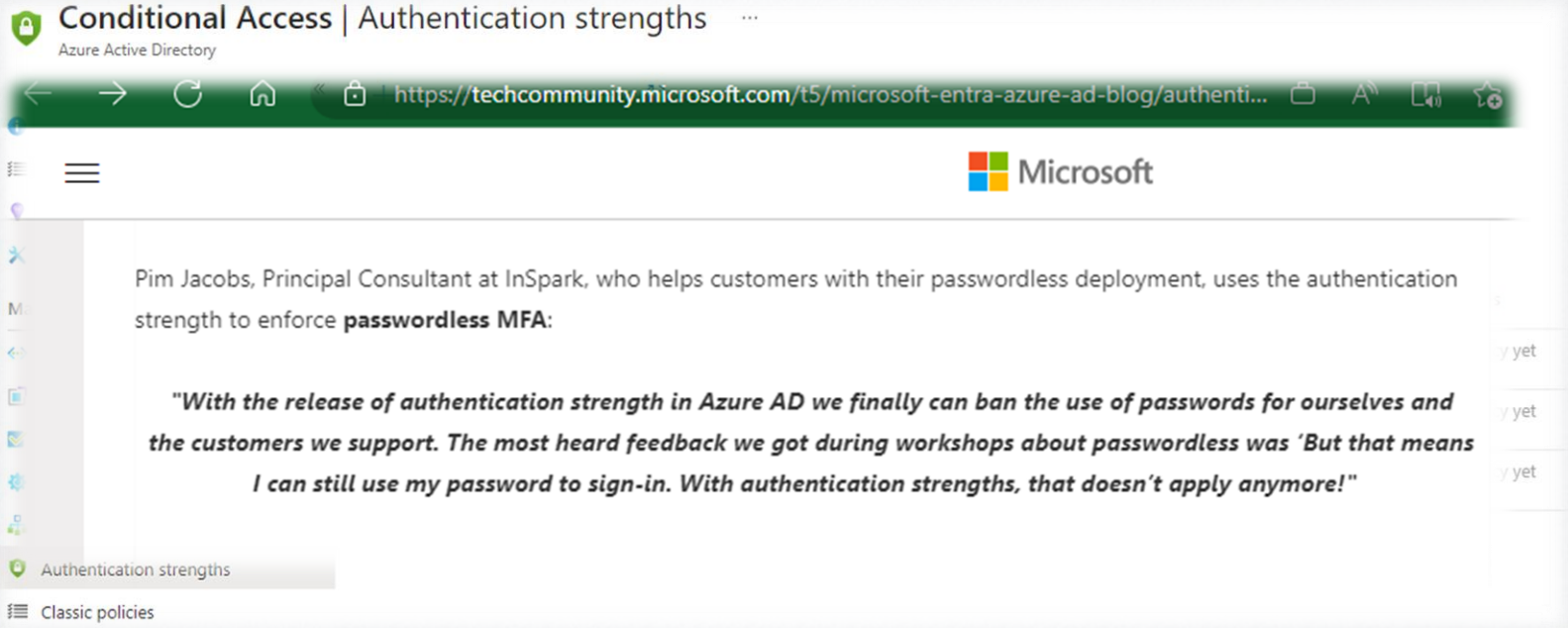
Dive into the Jungle of Authentication Methods

Demo

Experts Live Netherlands

Authentication Strengths

Authentication Strengths



[Authentication strength – choose the right auth method for your scenario! - Microsoft Community Hub]

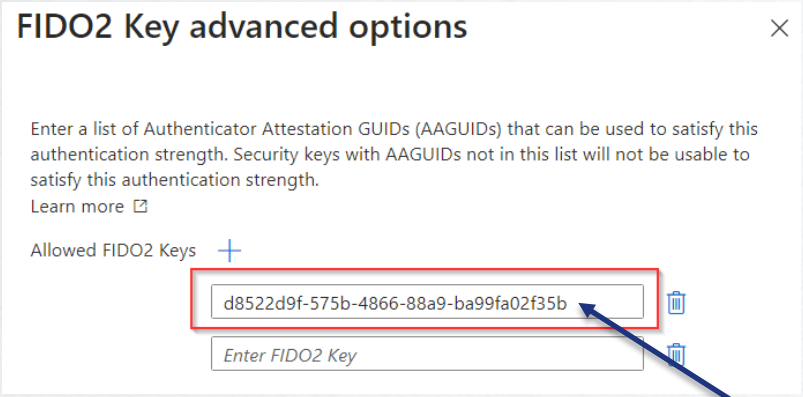
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

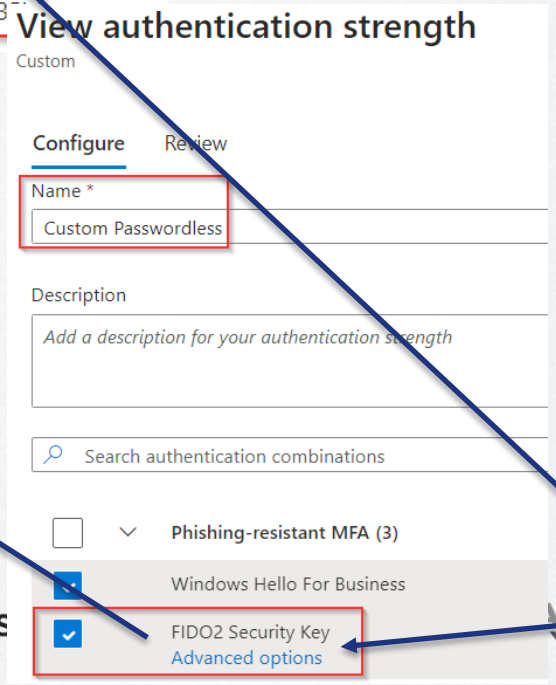
Default authentication strengths

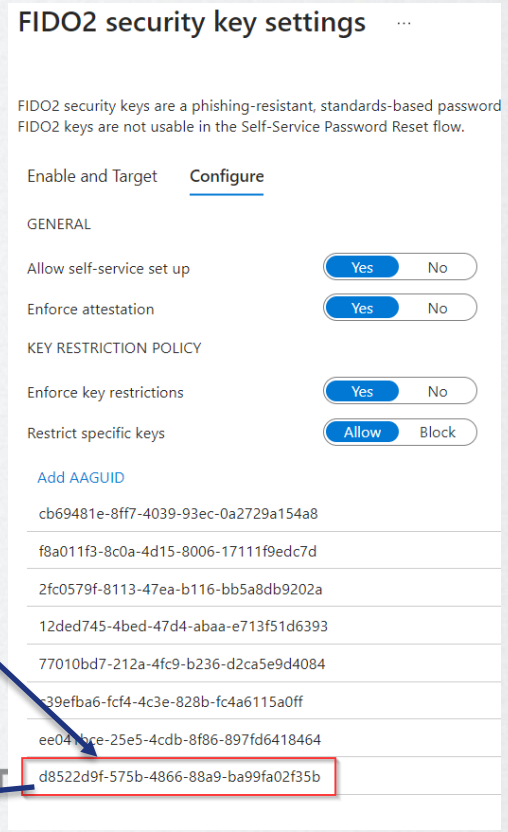
Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	☑	☑	☑
Windows Hello for Business	☑	☑	☑
Certificate-based authentication (Multi-Factor)	☑	☑	☑
Microsoft Authenticator (Phone Sign-in)	☑	☑	
Temporary Access Pass (One-time use AND Multi-use)	☑		
Password + something you have[1]	☑		
Federated single-factor + something you have[1]	☑		
Federated Multi-Factor	☑		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

[1] *Something you have refers to one of the following methods: SMS, voice, push notification, software OATH token and Hardware OATH token.*

Custom authentication strengths

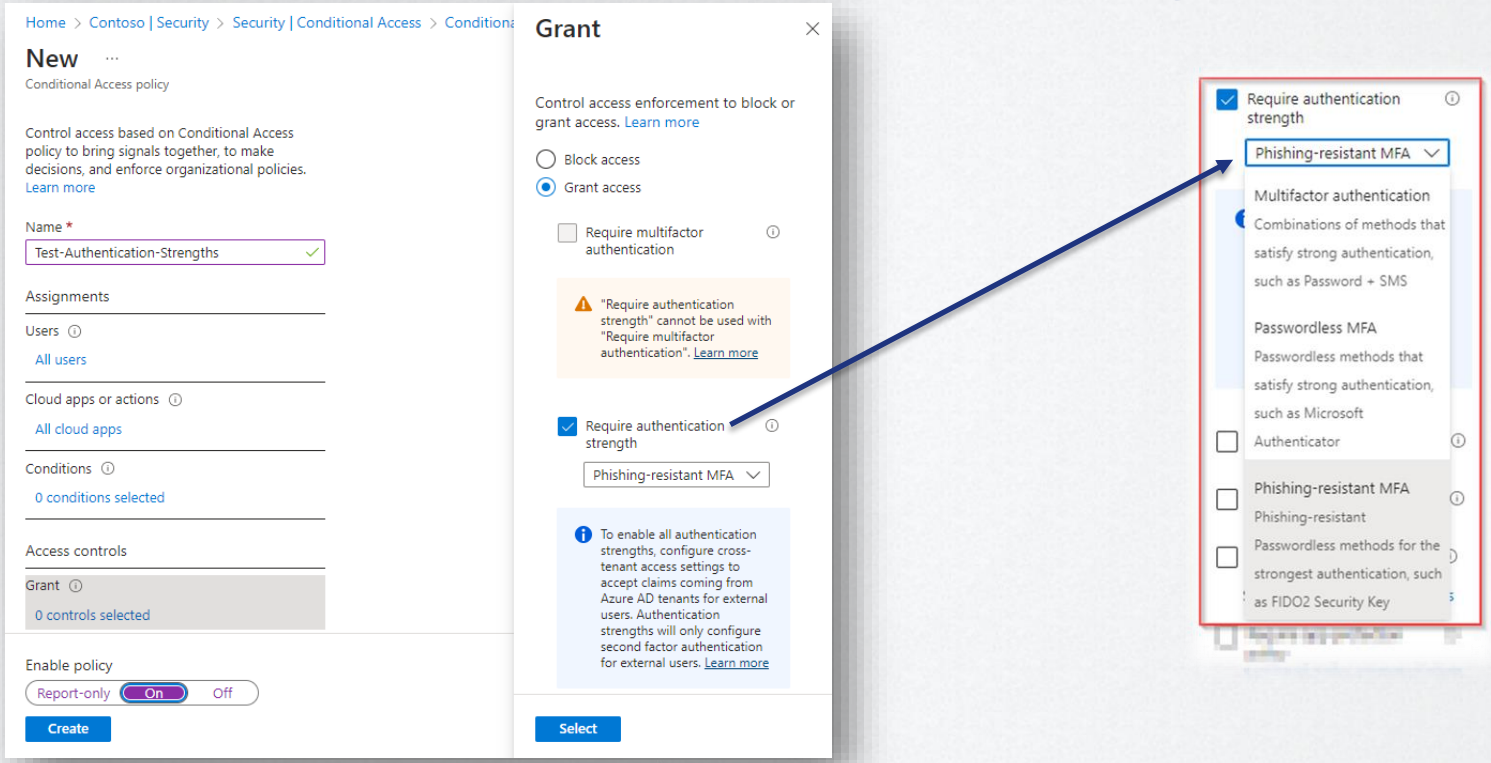






cegeka

Authentication Strengths in CA



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

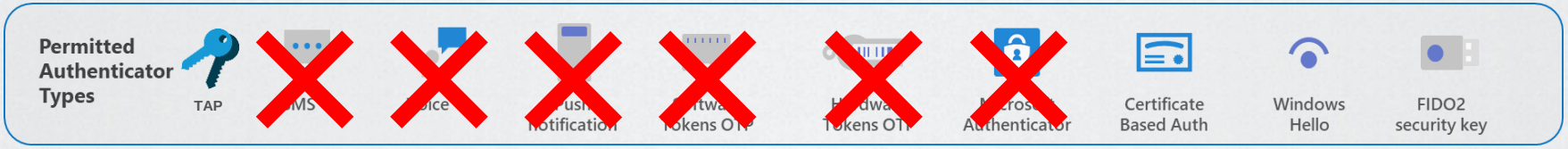
Why use authentication Strengths

- Secure your admin accounts
- Require Passwordless methods
- Prevent insecure second factors
- Protect sensitive resources
- Secure auth based step-up authentication

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

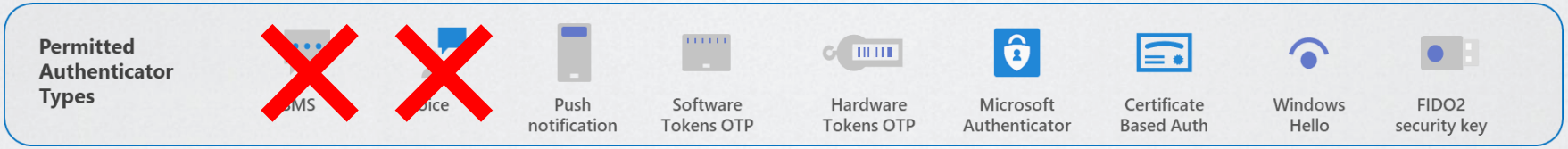
A few examples….

Admins



Passwordless users

Guests



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Authentication strengths limitations

Don't lock yourself out!

Evaluated **after** initial authentication

MFA & Auth Strengths can't be used in the same policy

Email OTP for guests isn't supported

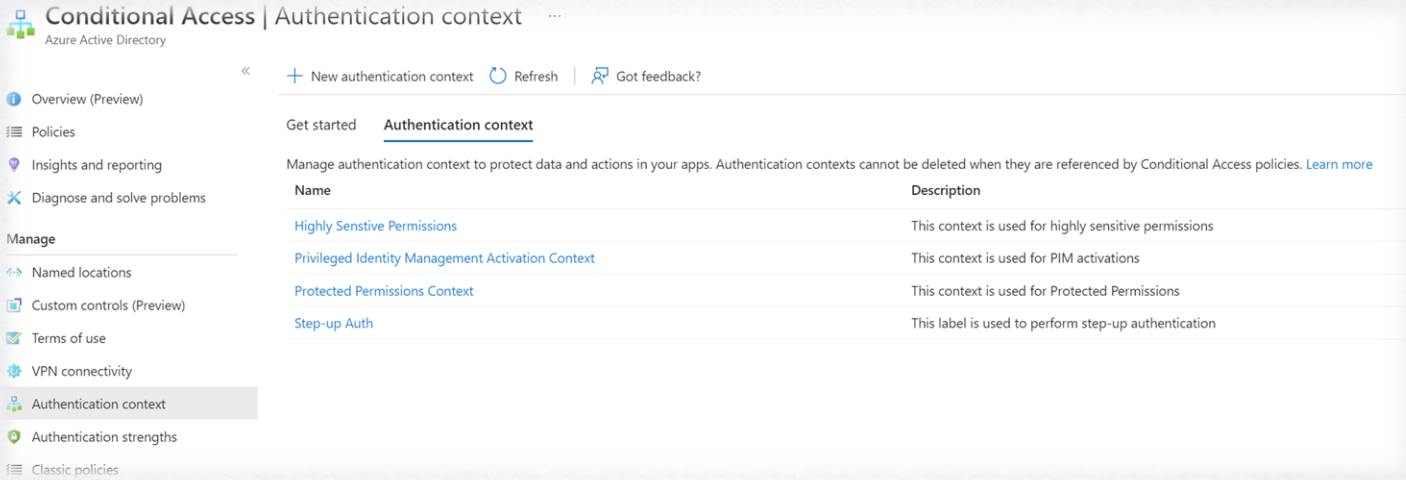
Default Passwordless option doesn’t contain TAP

Additional configuration can be required for guests

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

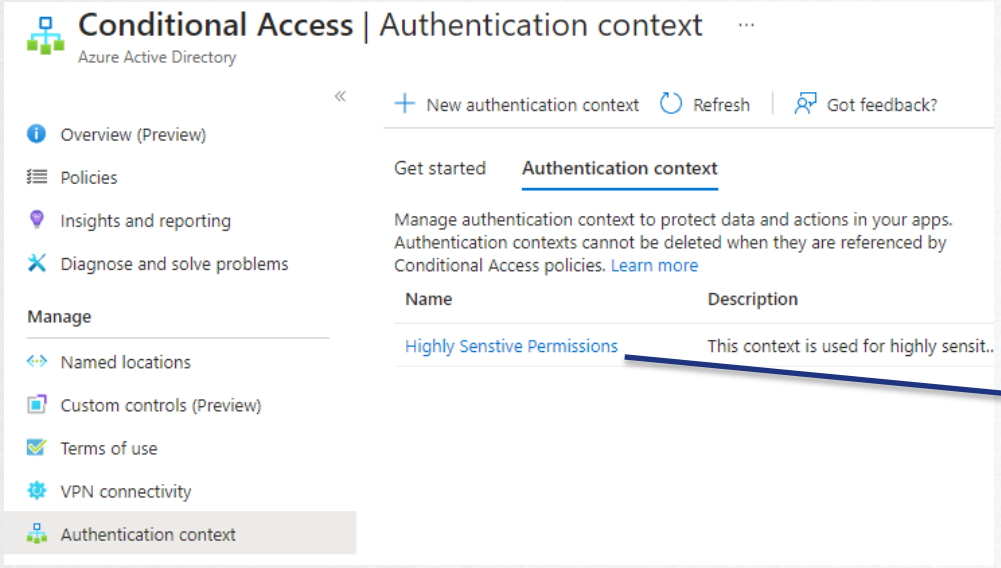
Authentication Context

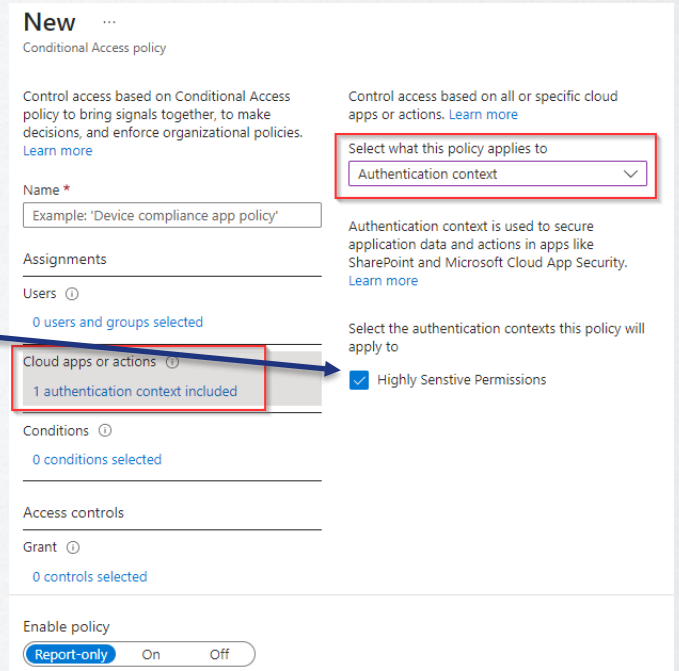
Authentication Context



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Authentication Context in CA





cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

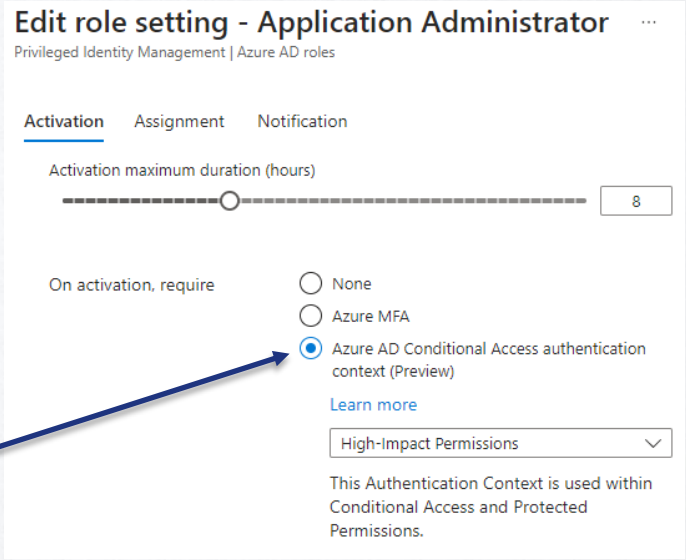
Using authentication Context

Protected Actions (P1)

Permission	Conditional Access authentication context
microsoft.directory/conditionalAccessPolicies/basic/update	High-Impact Permissions
microsoft.directory/conditionalAccessPolicies/delete	High-Impact Permissions
microsoft.directory/namedLocations/basic/update	High-Impact Permissions
microsoft.directory/namedLocations/delete	High-Impact Permissions

Apply Authentication Context

Privileged Identity Management (P2)

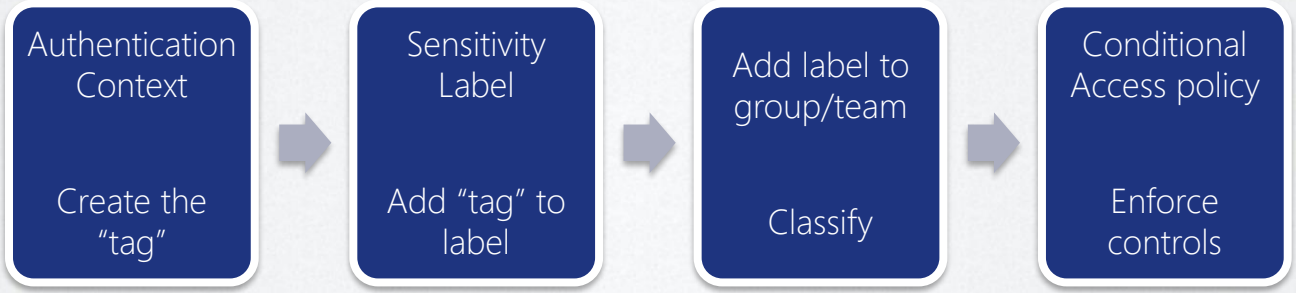


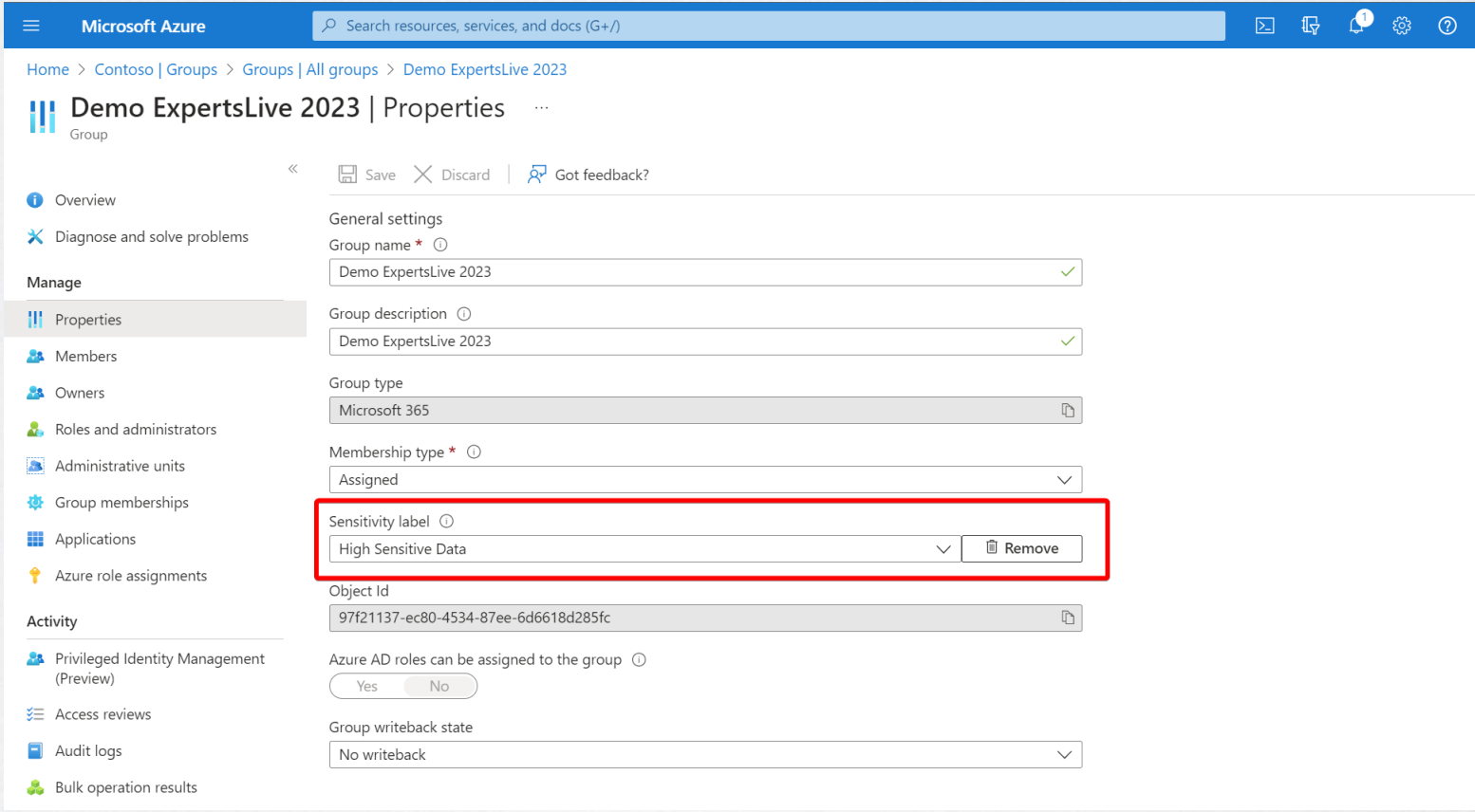
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Authentication Context

Sensitivity labels (E5)

Sensitivity Labels & Authentication Context

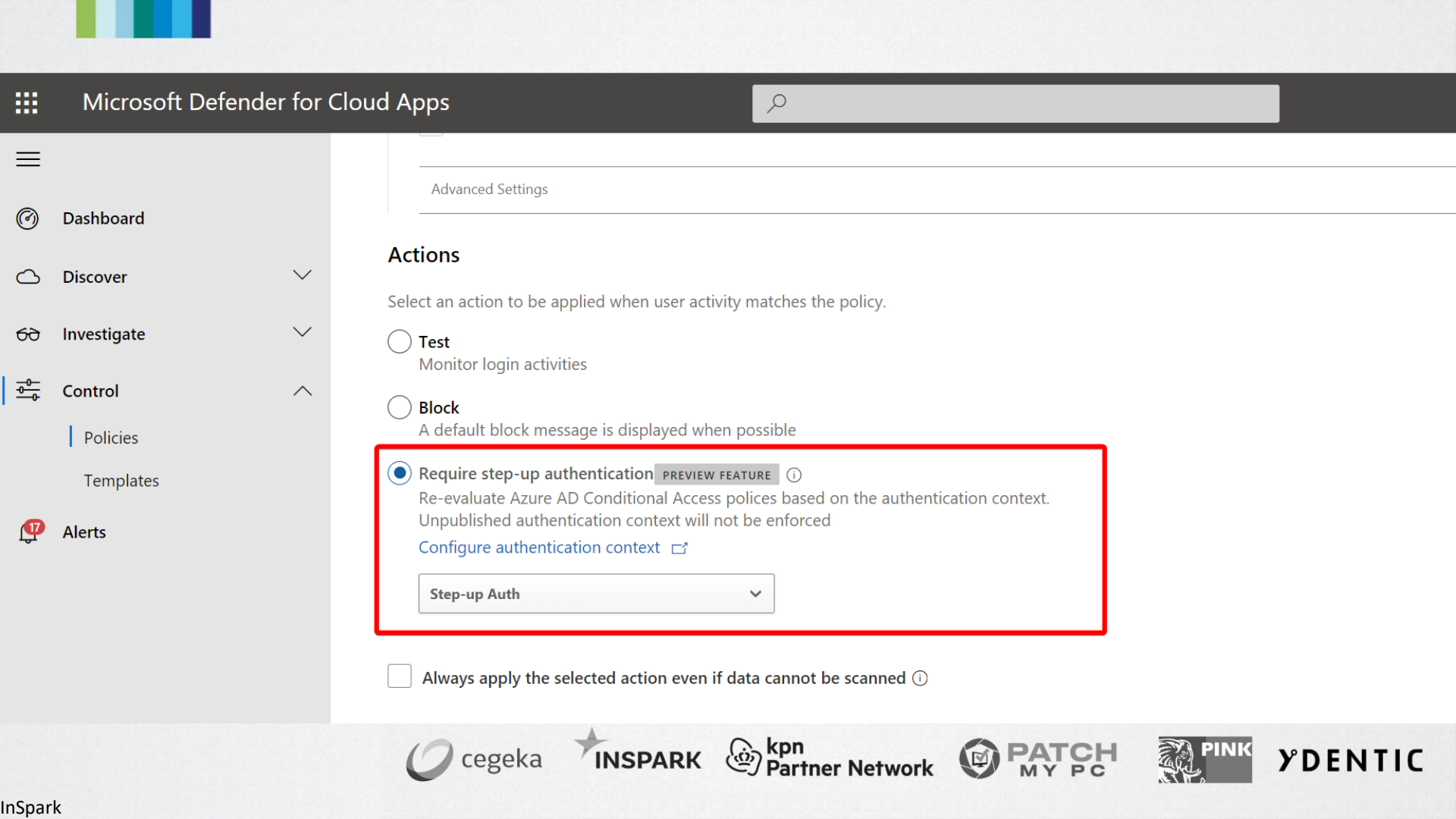




Authentication Context

Defender for Cloud Apps (E5)

Defender for Cloud Apps & Step-up auth



Why use authentication Context

Authentication Context is a zero-trust enabler

Require step-up authentication

Require more secure authentication

Show additional Terms of Use

More granular security controls

Not app bound but resource bound

To ‘tag’ resources

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Authentication Context Limitations

Maximum of 25 authentication contexts

Deleting an authentication context only blocked when in use by CA

References are always made to the authentication context ID

Not available in all services

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

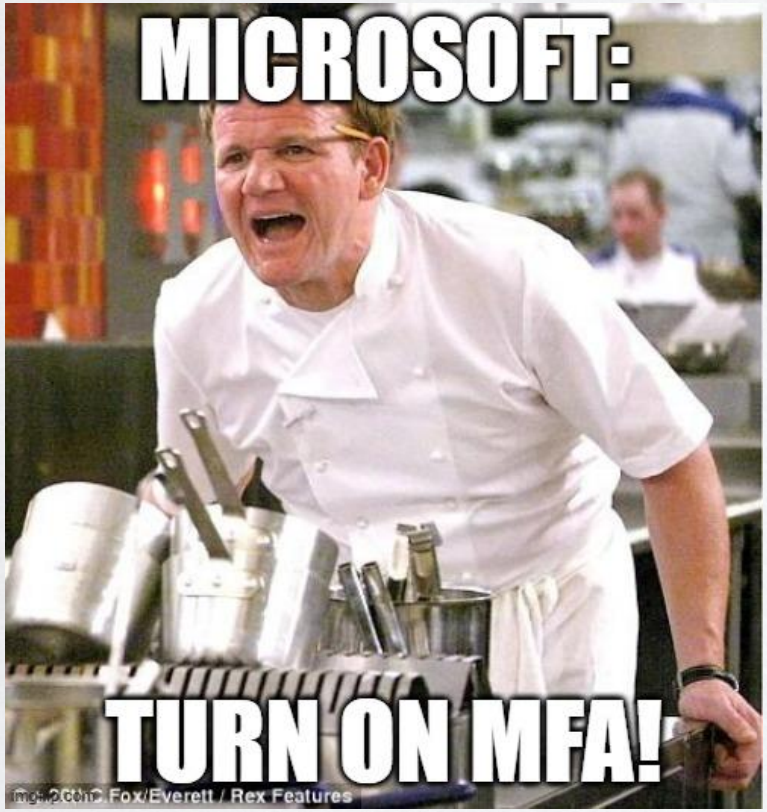
Dive into the Jungle of Authentication Strengths and Contexts

Demo

Experts Live Netherlands

Next steps & Key Takeaways

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC



Number of methods required to reset

1 2

Methods available to users

- [ ] Mobile app notification
- [x] Mobile app code
- [x] Email
- [x] Mobile phone (SMS only)
- [ ] Office phone
- [ ] Security questions

verification options (learn more)

Methods available to users:

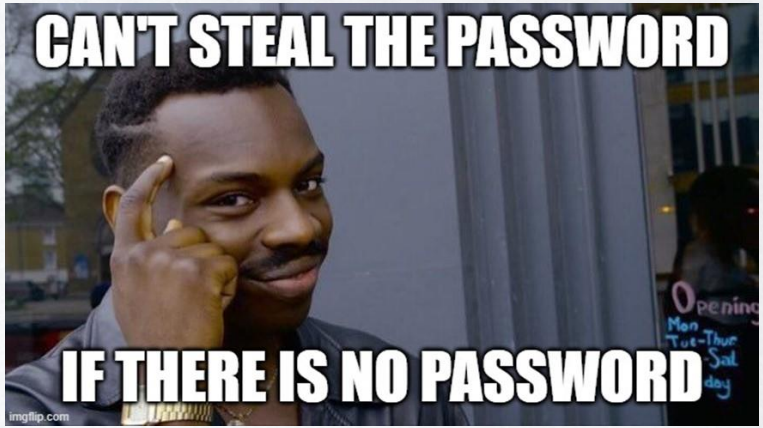
- [ ] Call to phone
- [x] Text message to phone
- [x] Notification through mobile app
- [x] Verification code from mobile app or hardware token

Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Third-party software OATH tokens		No
Voice call		No
Email OTP	All users	Yes
Certificate-based authentication		No

Move from ‘Require MFA’ to ‘Require Authentication Strength’

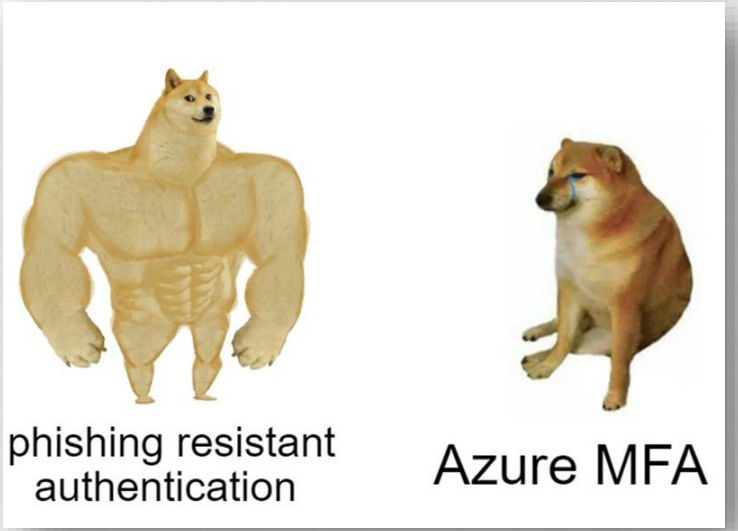
cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Continue your passwordless journey with authentication strengths



cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Require phishing resistant auth for admins with auth context

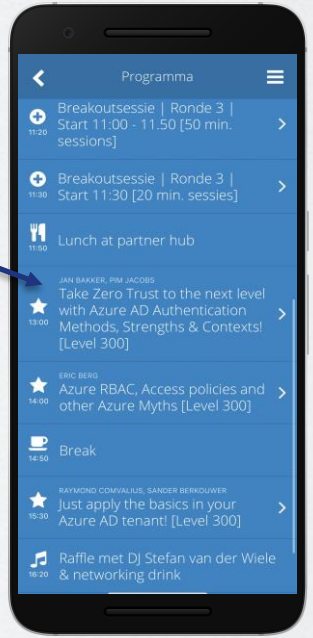


Protect your sensitive resources using sensitivity labels

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Questions?

Please rate our session!



Thank you!

Pim Jacobs
pim.jacobs@inspark.nl

Jan Bakker
jan@janbakkerconsulting.nl

cegeka INSPARK kpn Partner Network PATCH MY PC PINK YDENTIC

Next session: 14:00 – 14:50

Unleashing the Power of Microsoft Intune Community Tools

Jörgen Nilsson

Experts Live Netherlands