



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

Pim Jacobs & Jan Bakker



**Microsoft®**  
Most Valuable  
Professional

# Pim Jacobs



Principal Consultant @ InSpark  
Microsoft MVP Security  
Let's connect!

Blog: <https://www.identity-man.eu/>  
Mail: pim.jacobs@inspark.nl





# Jan Bakker

Self-employed  
*aka.ms/janbakker*



Ramblings:  
**JANBAKKER.TECH**  
 sharing is caring



cegeka 

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

Always  
Verify

Use least-  
privilege  
access

Assume  
breach

A photograph of a modern city skyline at dusk or night, featuring several skyscrapers with illuminated windows against a dark sky.

We're no longer  
protecting  
office buildings

A photograph of a family in a modern kitchen. A woman is seated at a wooden table, working on a laptop. A man stands behind her, brushing the hair of a young girl who is sitting on his lap and looking at a tablet. The kitchen is well-lit with a large island and various items on the counter.

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



User Identity



Data classification



Device health

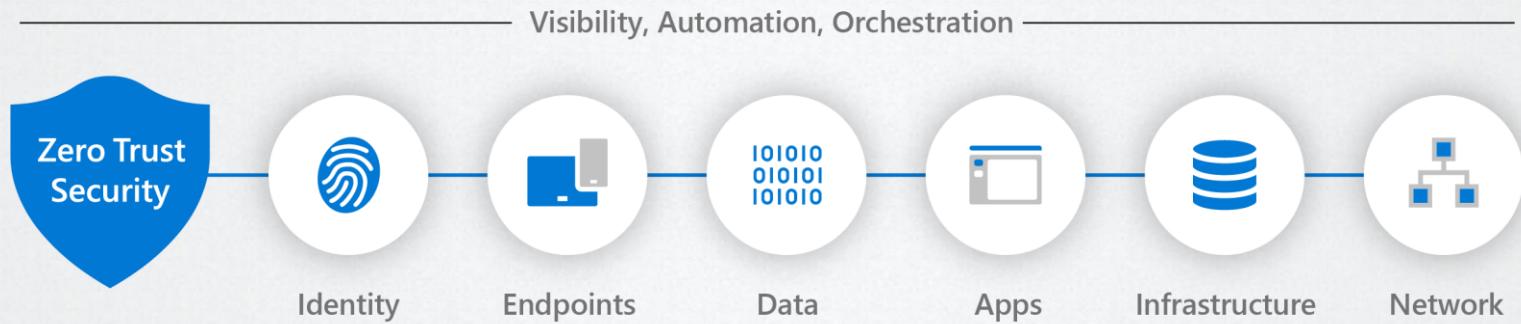


Location



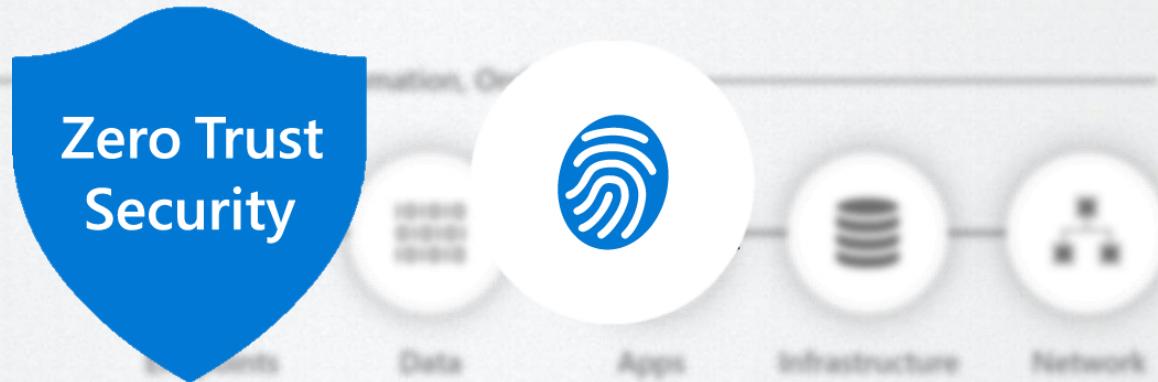
Risk

# Zero Trust across all workloads





# Identity to the next level!



# The 'Jungle' of authentication





# 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

<b>Method</b>	<b>Primary authentication</b>	<b>Secondary authentication</b>
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

## Tenant-wide MFA settings

Number of methods required to reset (i)

1

2

Methods available to users

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

verification options [\(learn more\)](#)

Methods available to users:

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

# Authentication methods policies

Authentication methods | Policies Contoso - Azure AD Security X

Search Got feedback? ...

Manage Policies

Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). [Learn more](#)

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](#)

Manage migration

Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		Hell no!
Temporary Access Pass	All users	Yes
Third-party software OATH tokens	1 group	Yes
Voice call		Hell no!
Email OTP	All users	Yes
Certificate-based authentication		No

# 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 the

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 authenticate users. Non-Microsoft software OATH tokens can also generate software OATH codes and is managed in the Microsoft Authenticator app. A 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

## 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 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.

[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



## Authentication methods | User registration details

Contoso - Azure AD Security

Search

Download

Refresh

Columns

Got feedback?

### Manage

Policies

Password protection

Registration campaign

Authentication strengths

Settings

### Monitoring

Activity

User registration details

Registration and reset events

Bulk operation results

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...
DebraB@M365x80658054.OnMicrosoft.com	Debra Berger	Not Capable	Not Capable	Not Capable	Mobile phone
JoniS@M365x80658054.OnMicrosoft.com	Joni Sherman	Not Capable	Not Capable	Not Capable	Mobile phone
NestorW@M365x80658054.OnMicrosoft.com	Nestor Wilke	Not Capable	Not Capable	Not Capable	Mobile phone

### Methods Registered

Mobile phone

Mobile phone

Mobile phone



Search



Got feedback?

## 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

 All users Select group

Target \*

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

IncludeExclude

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.

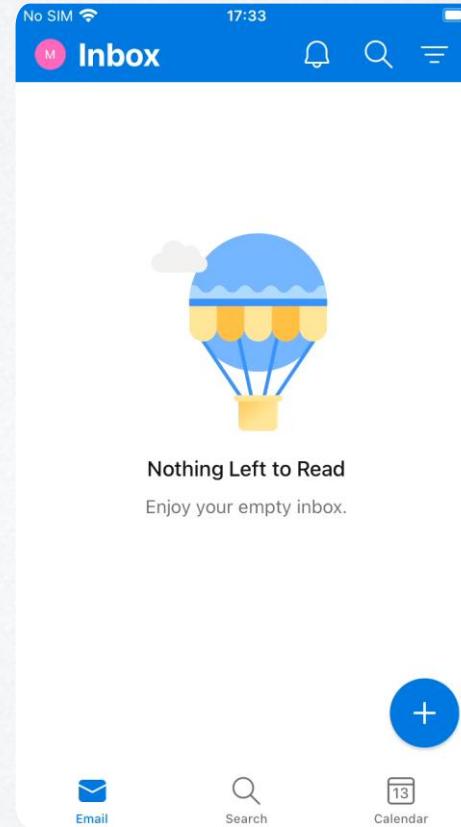


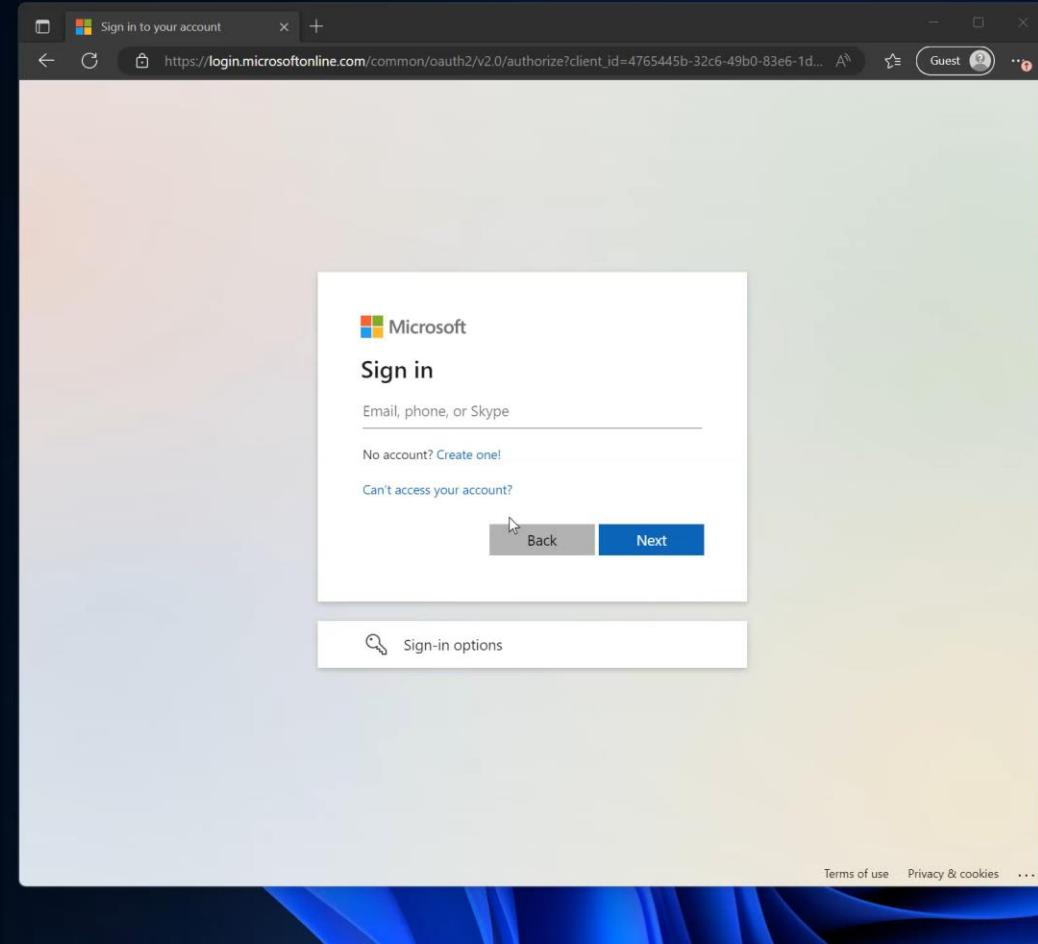
## AUTHENTICATOR LITE



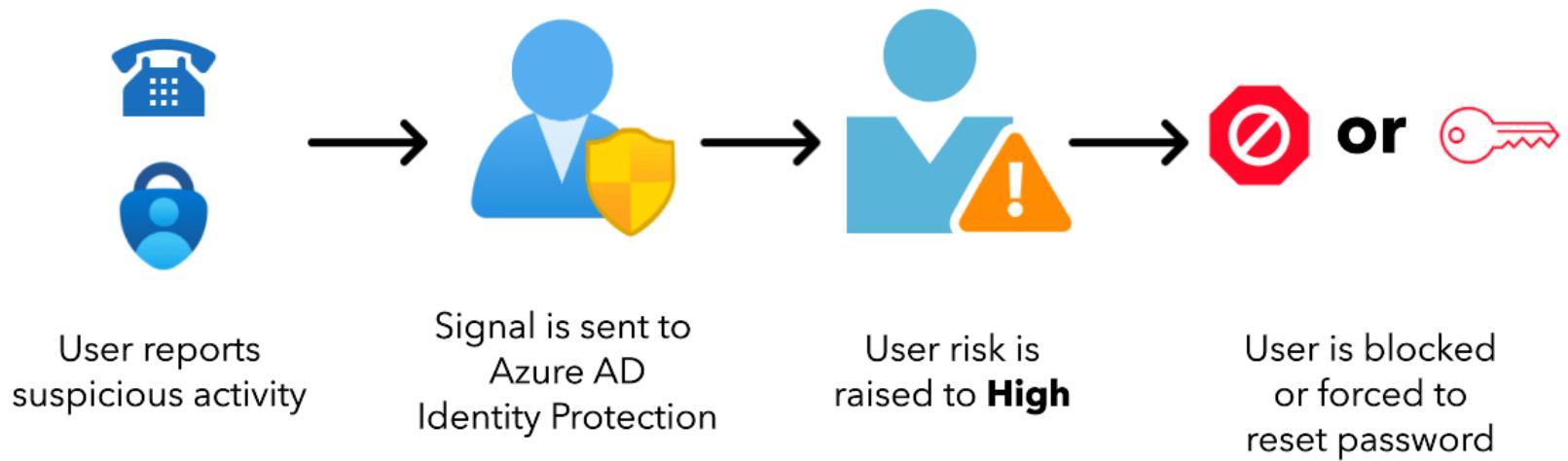


# Enrollment with Temporary Access Pass









## Authentication methods | Settings

Contoso - Azure AD Security



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



Home &gt; Adele Vance

## Adele Vance | Audit logs

User

Search



Download



Refresh



Columns



Got feedback

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

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

4/6/2023, 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[Learn more](#) [Download](#) [Select all](#) [Confirm user...](#)[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](#)

## 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	-
-----------------------	---------------------------------------	----------------	------------	---

<input type="checkbox"/> User ↑↓	Risk state
<input type="checkbox"/> Adele Vance	At risk
<input type="checkbox"/> Megan Bowen	At risk
<input type="checkbox"/> Debra Berger	At risk
<input type="checkbox"/> Miriam Graham	At risk
<input type="checkbox"/> Max Verstappen	At risk



# Dive into the Jungle of Authentication Methods

Demo



# Authentication Strengths



# Authentication Strengths

A screenshot of a Microsoft Edge browser window. The address bar shows the URL: <https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/authentication-strengths/mar>. The page content discusses the release of authentication strength in Azure AD, mentioning Pim Jacobs from InSpark. It quotes him as saying: "With the release of authentication strength in Azure AD we finally can ban the use of passwords for ourselves and the customers we support. The most heard feedback we got during workshops about passwordless was 'But that means I can still use my password to sign-in. With authentication strengths, that doesn't apply anymore!'". Below the quote, there are three items with the status 'yet'.

Pim Jacobs, Principal Consultant at InSpark, who helps customers with their passwordless deployment, uses the authentication strength to enforce **passwordless MFA**:

*"With the release of authentication strength in Azure AD we finally can ban the use of passwords for ourselves and the customers we support. The most heard feedback we got during workshops about passwordless was 'But that means I can still use my password to sign-in. With authentication strengths, that doesn't apply anymore!'"*

yet  
yet  
yet

Authentication strengths

Classic policies

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



# Default authentication strengths

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows Hello for Business	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Certificate-based authentication (Multi-Factor)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Authenticator (Phone Sign-in)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Temporary Access Pass (One-time use AND Multi-use)	<input checked="" type="checkbox"/>		
Password + something you have <sup>1</sup>	<input checked="" type="checkbox"/>		
Federated single-factor + something you have <sup>1</sup>	<input checked="" type="checkbox"/>		
Federated Multi-Factor	<input checked="" type="checkbox"/>		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

<sup>1</sup> Something you have refers to one of the following methods: SMS, voice, push notification, software OATH token and Hardware OATH token.



# Custom authentication strengths

**Yubikey Bio**

Security key

Date registered  
7/8/2022, 2:36:05 PM

AAGUID  
d8522d9f-575b-4866-88a9-ba99fa02f35b

**FIDO2 security key settings**

FIDO2 security keys are a phishing-resistant, standards-based password. FIDO2 keys are not usable in the Self-Service Password Reset flow.

Enable and Target    Configure

GENERAL

Allow self-service set up    Yes    No

Enforce attestation    Yes    No

KEY RESTRICTION POLICY

Enforce key restrictions    Yes    No

Restrict specific keys    Allow    Block

Add AAGUID

- cb69481e-8ff7-4039-93ec-0a2729a154a8
- f8a011f3-8c0a-4d15-8006-17111f9edc7d
- 2fc0579f-8113-47ea-b116-bb5a8db9202a
- 12ded745-4bed-47d4-abaa-e713f51d6393
- 77010bd7-212a-4fc9-b236-d2ca5e9d4084
- c39efba6-fcf4-4c3e-828b-fc4a6115a0ff
- ee041bce-25e5-4cdb-8f86-897fd6418464
- d8522d9f-575b-4866-88a9-ba99fa02f35b

**FIDO2 Key advanced options**

Enter a list of Authenticator Attestation GUIDs (AAGUIDs) that can be used to satisfy this authentication strength. Security keys with AAGUIDs not in this list will not be usable to satisfy this authentication strength.

Learn more

Allowed FIDO2 Keys

- d8522d9f-575b-4866-88a9-ba99fa02f35b
- Enter FIDO2 Key

**View authentication strength**

Custom

Configure    Review

Name \*  
Custom Passwordless

Description  
Add a description for your authentication strength

Search authentication combinations

Phishing-resistant MFA (3)

- Windows Hello For Business
- FIDO2 Security Key Advanced options

# Authentication Strengths in CA

Home > Contoso | Security > Security | Conditional Access > Conditional access policies

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \* Test-Authentication-Strengths ✓

Assignments

Users ⓘ All users

Cloud apps or actions ⓘ All cloud apps

Conditions ⓘ 0 conditions selected

Access controls

Grant ⓘ 0 controls selected

Enable policy

Report-only  On  Off

Create

Grant

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

Block access

Grant access

Require multifactor authentication ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require authentication strength ⓘ

Phishing-resistant MFA ⓘ

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Azure AD tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more](#)

Select

Phishing-resistant MFA ⓘ

Multifactor authentication

Combinations of methods that satisfy strong authentication, such as Password + SMS

Passwordless MFA

Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator

Phishing-resistant MFA ⓘ

Phishing-resistant

Passwordless methods for the strongest authentication, such as FIDO2 Security Key



# Why use authentication Strengths



Secure your admin accounts



Require Passwordless methods



Prevent insecure second factors



Protect sensitive resources



Secure auth based step-up authentication

# A few examples....

## Admins

Permitted Authenticator Types



## Passwordless users

Permitted Authenticator Types



## Guests

Permitted Authenticator Types



# 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



# Authentication Context



# Authentication Context

Conditional Access | Authentication context ...

Azure Active Directory

« + New authentication context Refresh Got feedback?

Overview (Preview) Policies Insights and reporting Diagnose and solve problems

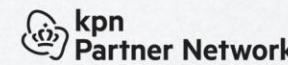
Manage

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

Get started **Authentication context**

Manage authentication context to protect data and actions in your apps. Authentication contexts cannot be deleted when they are referenced by Conditional Access policies. [Learn more](#)

Name	Description
Highly Sensitive Permissions	This context is used for highly sensitive permissions
Privileged Identity Management Activation Context	This context is used for PIM activations
Protected Permissions Context	This context is used for Protected Permissions
Step-up Auth	This label is used to perform step-up authentication



# Authentication Context in CA

Conditional Access | Authentication context ...  
Azure Active Directory

New authentication context Refresh Got feedback?

Overview (Preview) Policies Insights and reporting Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context

Get started Authentication context

Manage authentication context to protect data and actions in your apps. Authentication contexts cannot be deleted when they are referenced by Conditional Access policies. [Learn more](#)

Name	Description
Highly Sensitive Permissions	This context is used for highly sensit...

New ... Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Select what this policy applies to

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security. [Learn more](#)

Name \* Example: 'Device compliance app policy'

Assignments

Users [\(1\)](#) 0 users and groups selected

Cloud apps or actions [\(1\)](#) 1 authentication context included

Conditions [\(0\)](#) 0 conditions selected

Access controls

Grant [\(0\)](#) 0 controls selected

Enable policy [Report-only](#) On Off

Select the authentication contexts this policy will apply to  Highly Sensitive Permissions

# 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)

Edit role setting - Application Administrator ...

Privileged Identity Management | Azure AD roles

Activation   Assignment   Notification

Activation maximum duration (hours)

On activation, require

None  
 Azure MFA  
 Azure AD Conditional Access authentication context (Preview)

[Learn more](#)

High-Impact Permissions

This Authentication Context is used within Conditional Access and Protected Permissions.



# Authentication Context



Sensitivity labels (E5)



# Sensitivity Labels & Authentication Context





## Demo ExpertsLive 2023 | Properties

Group



Save



Discard



Got feedback?

[Overview](#)[Diagnose and solve problems](#)

### Manage

[Properties](#)[Members](#)[Owners](#)[Roles and administrators](#)[Administrative units](#)[Group memberships](#)[Applications](#)[Azure role assignments](#)

### Activity

[Privileged Identity Management \(Preview\)](#)[Access reviews](#)[Audit logs](#)[Bulk operation results](#)

Save



Discard



Got feedback?

### General settings

Group name \*

Demo ExpertsLive 2023



Group description

Demo ExpertsLive 2023



Group type

Microsoft 365

Membership type \*

Assigned



Sensitivity label

High Sensitive Data

Remove

Object Id

97f21137-ec80-4534-87ee-6d6618d285fc



Azure AD roles can be assigned to the group

 Yes  No

Group writeback state

No writeback

**INSPARK****Partner Network****YDENTIC**



# Authentication Context



Defender for Cloud Apps (E5)



# Defender for Cloud Apps & Step-up auth





## Advanced Settings

## Actions

Select an action to be applied when user activity matches the policy.

**Test**

Monitor login activities

**Block**

A default block message is displayed when possible

**Require step-up authentication**PREVIEW FEATURE

Re-evaluate Azure AD Conditional Access policies based on the authentication context.

Unpublished authentication context will not be enforced

[Configure authentication context](#)

Step-up Auth



Always apply the selected action even if data cannot be scanned



# 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

# 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



# Dive into the Jungle of Authentication Strengths and Contexts

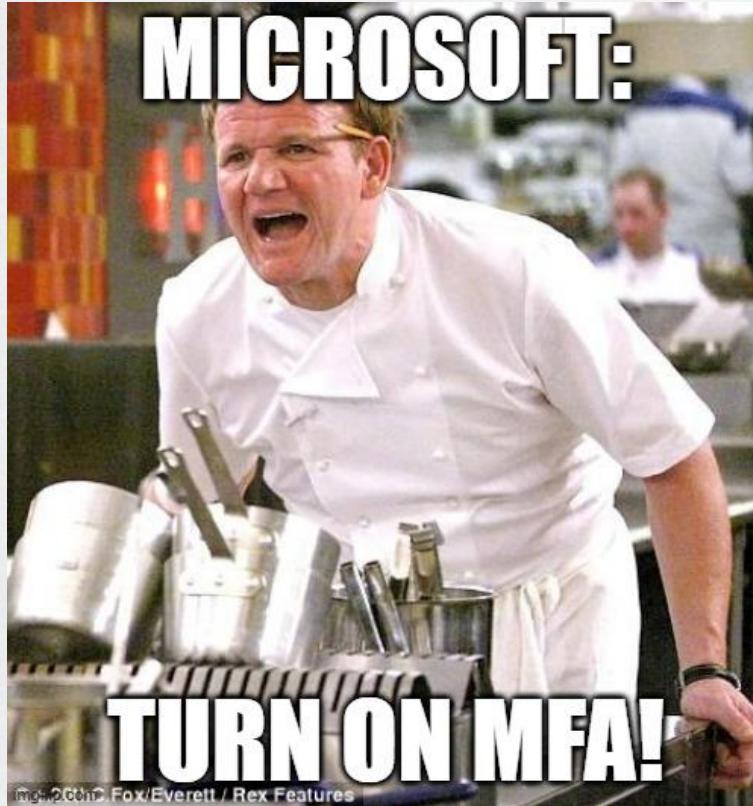
Demo



# Next steps & Key Takeaways





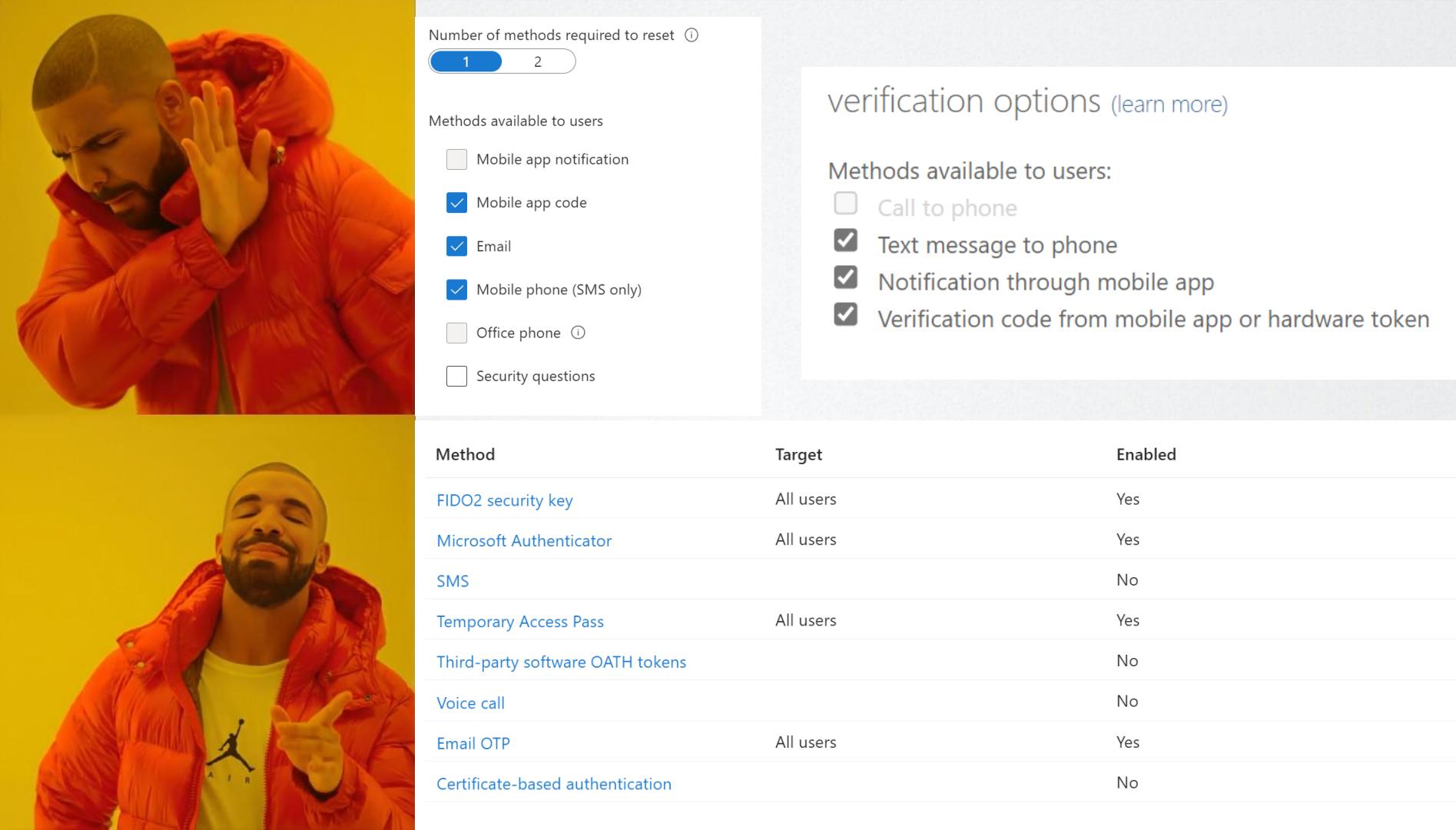


imgflip.com Fox/Everett / Rex Features



imgflip.com





Number of methods required to reset ⓘ

1 2

Methods available to users

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

verification options (learn more)

Methods available to users:

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

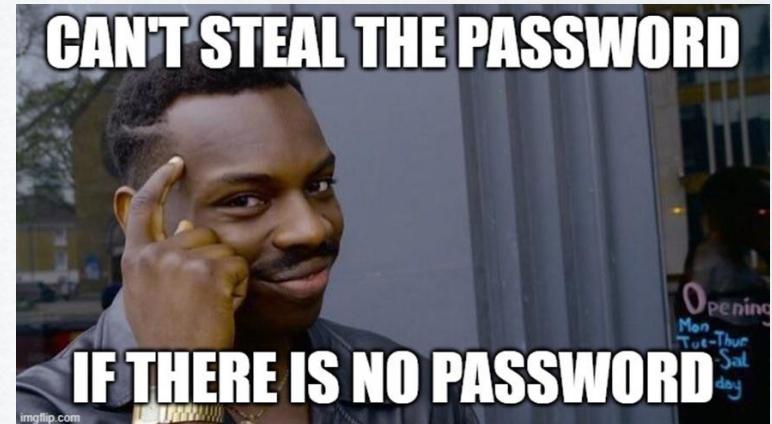
Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Third-party software OATH tokens		No
Voice call		No
Email OTP	All users	Yes
Certificate-based authentication		No

# Move from 'Require MFA' to 'Require Authentication Strength'



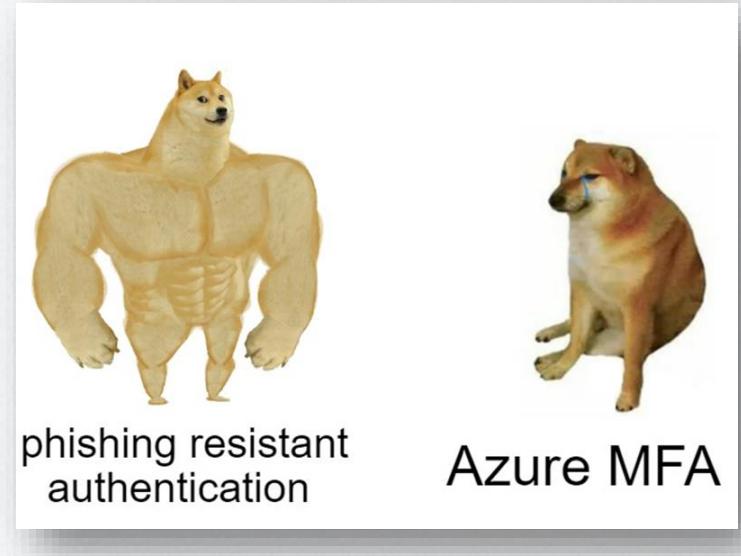


# Continue your passwordless journey with authentication strengths





# Require phishing resistant auth for admins with auth context





# Protect your sensitive resources using sensitivity labels

**SENSITIVITY  
LABELS**



**SENSITIVITY  
LABELS  
ON GROUPS**



**AUTHENTICATION  
CONTEXT  
BASED ON LABELS**



**STEP-UP AUTH  
IN DEFENDER  
FOR CLOUD APPS**



imgflip.com





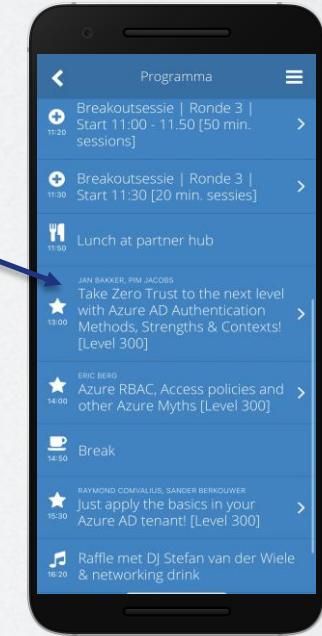
# Questions?





Please rate our session!

# Thank you!



**Pim Jacobs**



pim.jacobs@inspark.nl



**Jan Bakker**



jan@janbakkerconsulting.nl





Next session: 14:00 – 14:50

# Unleashing the Power of Microsoft Intune Community Tools

Jörgen Nilsson

