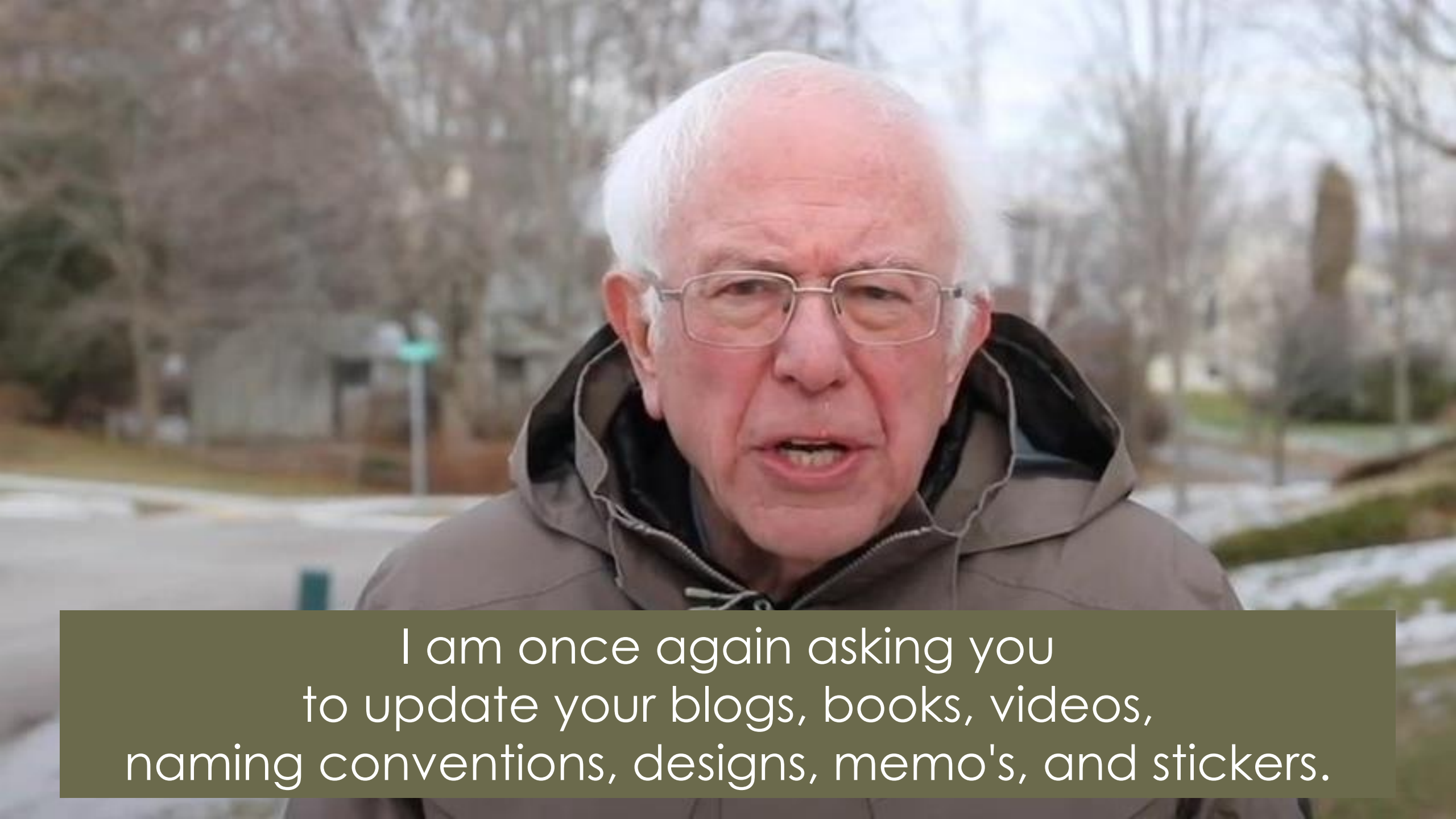

Identity Security
done right with
Microsoft Entra ID
(FORMERLY KNOWN AS
AZURE AD)

Microsoft® Most Valuable Professional

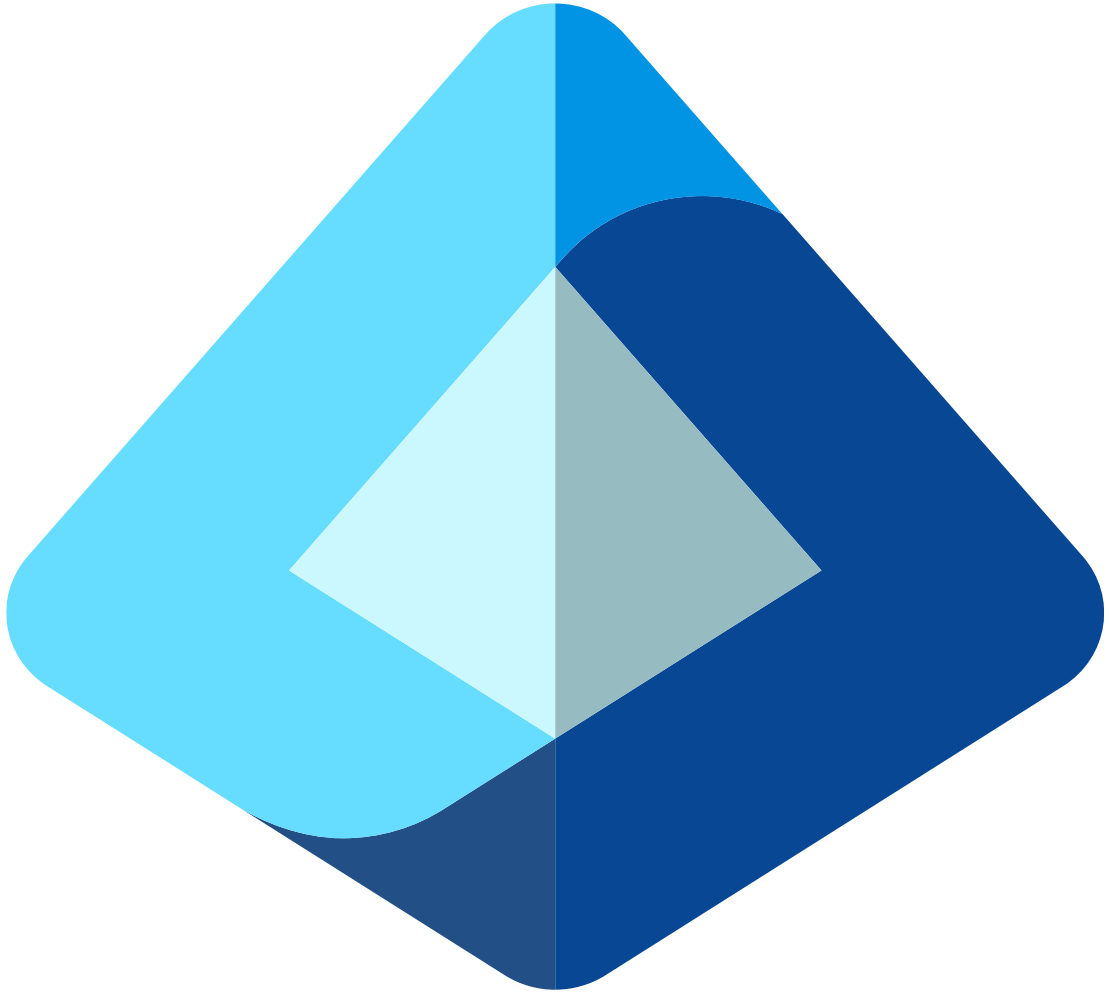
AKA.MS/JANBAKKER

SCAN ME


I am once again asking you
to update your blogs, books, videos,
naming conventions, designs, memo's, and stickers.

Azure Active Directory

Microsoft Entra ID



Microsoft Entra Naming Guide

Are you referring to the Azure AD product or a feature?

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

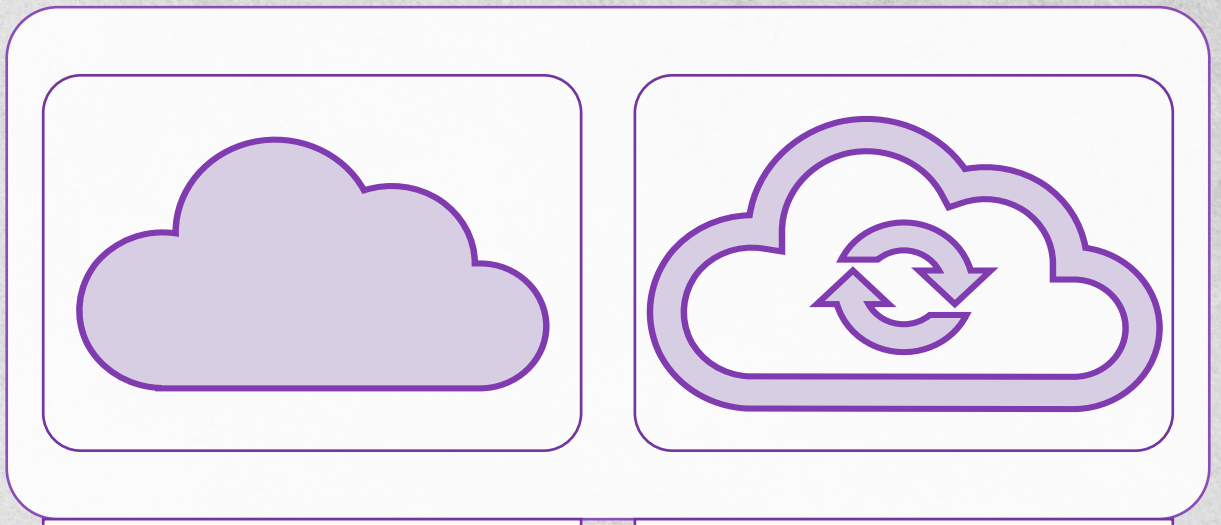
Windows Hello

* Includes Microsoft Authenticator Passwordless

How to improve your Identity security step by step?

1. Pick the right **identity model** and **authentication type**

Microsoft cloud identity models



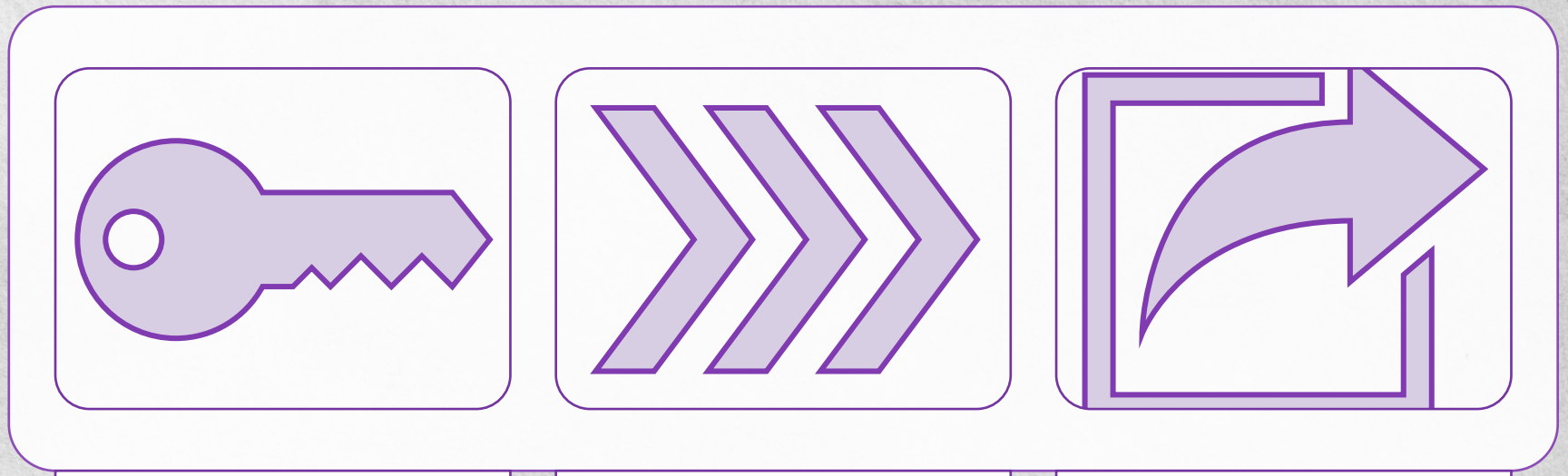
Cloud Identity

User accounts are managed in Microsoft Entra ID

Synchronized Identity

User accounts are managed in Active Directory and synced to Microsoft Entra ID

Microsoft authentication types



Password Hash Sync

Passthrough authentication

Federated authentication

Benefits Entra ID over ADFS

Identity Protection

Identity Governance

Brute force and DDoS mitigation

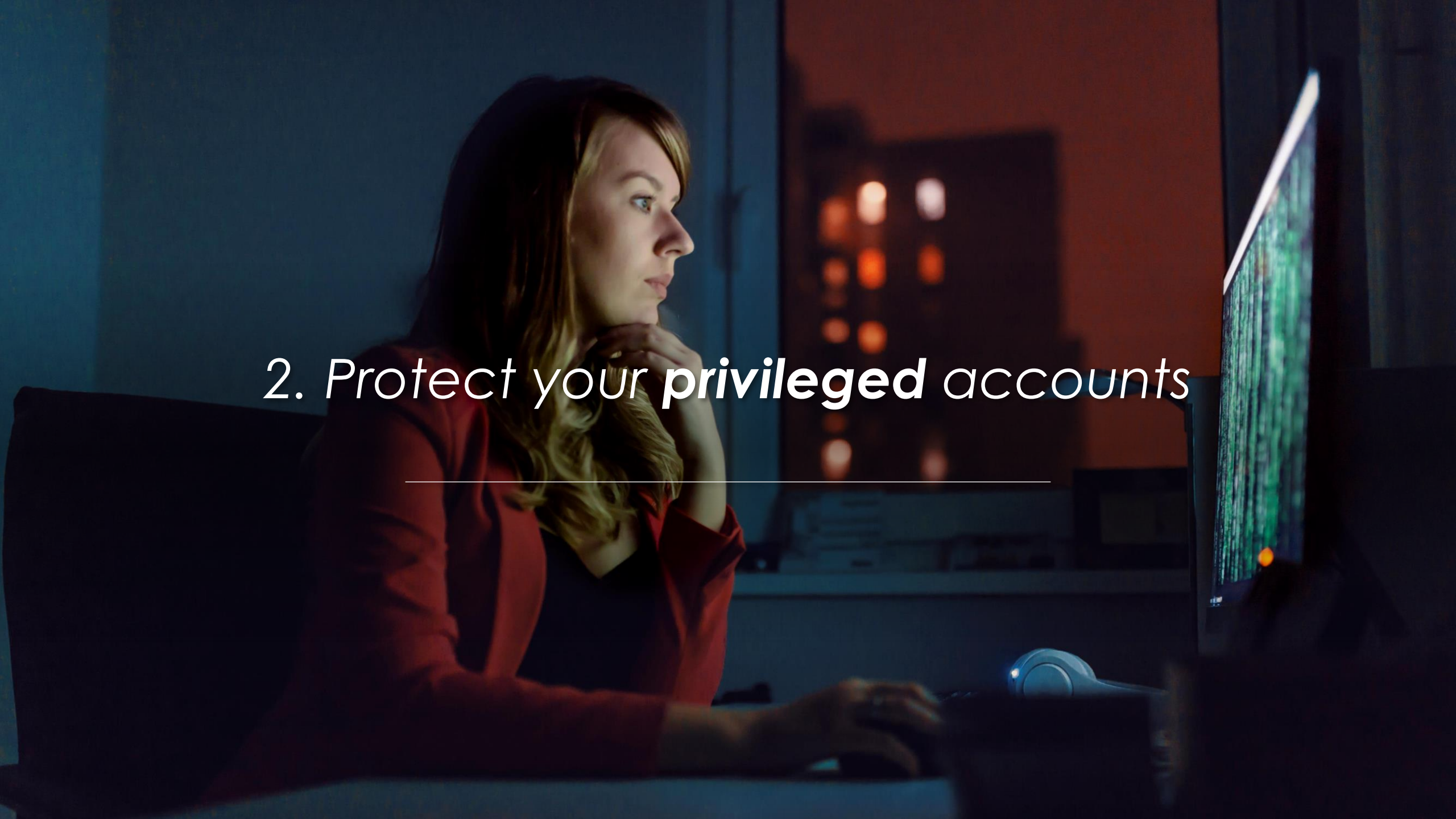
Mitigate on-premises outages

Conditional Access

Staged Rollout

Azure AD Connect: Cloud authentication via Staged Rollout - Microsoft Entra | Microsoft Learn


https://aka.ms/adfs2aad


2. Protect your **privileged** accounts


Use cloud-only accounts for privileged users to avoid lateral movement


Enable
MFA!


Not that one!


fido
CERTIFIED
FIDO2

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	☑		
Federated single-factor + something you have	☑		
Federated Multi-Factor	☑		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			


Manage
authentication
methods the
new way

SSPR Settings

Number of methods required to reset ⓘ

1 2

Methods available to users

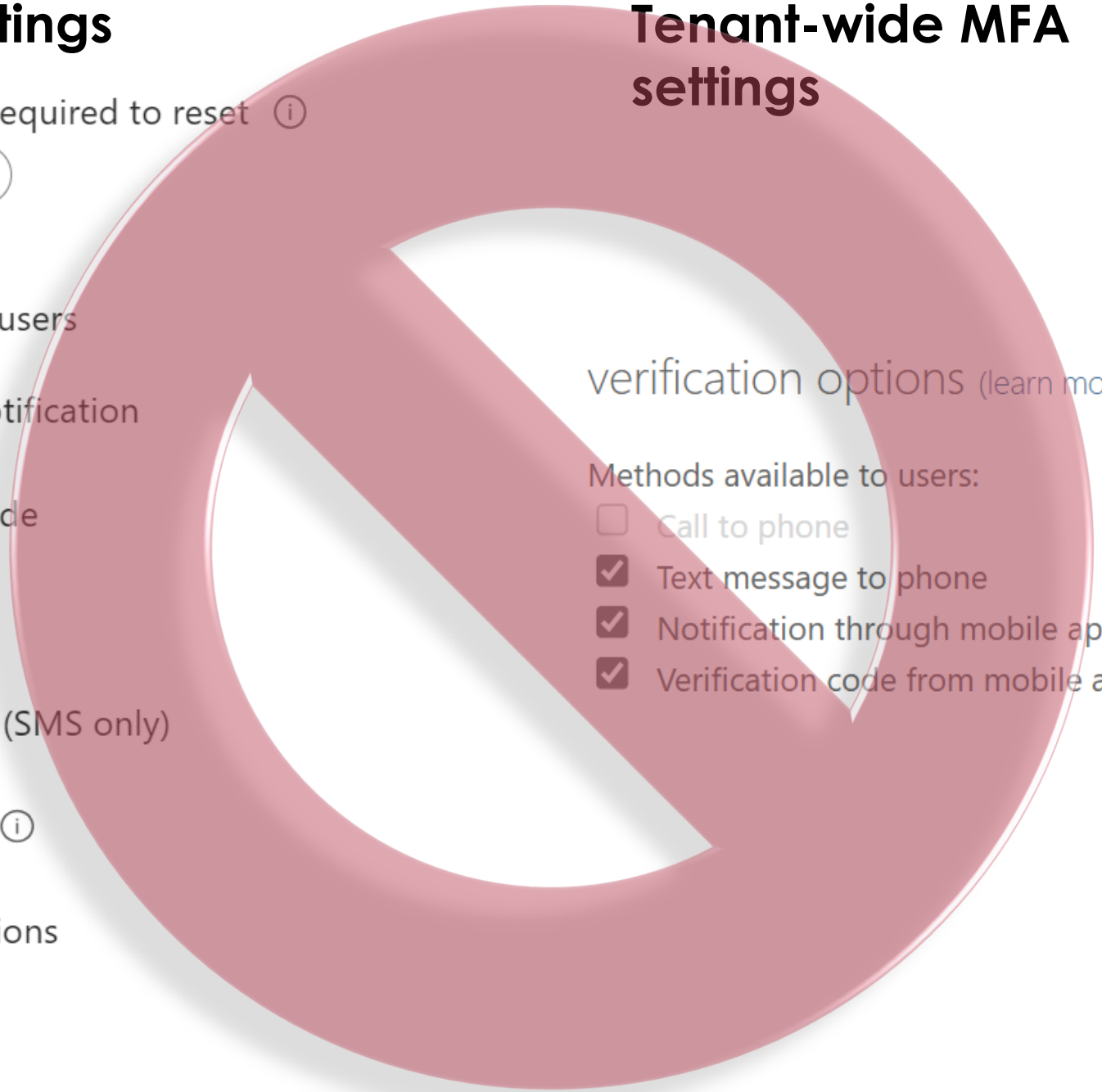
- [ ] Mobile app notification
- [x] Mobile app code
- [x] Email
- [x] Mobile phone (SMS only)
- [ ] Office phone ⓘ
- [ ] Security questions

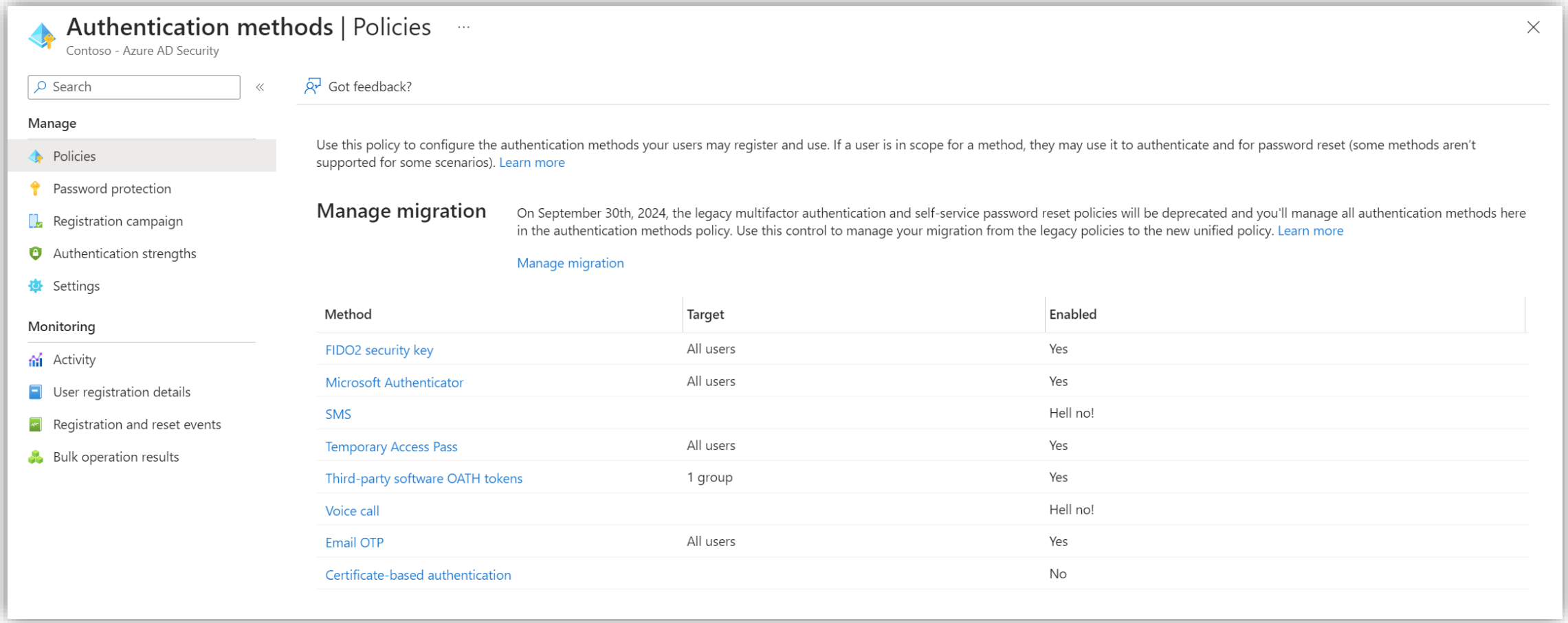
Tenant-wide MFA settings

verification options (learn more)

Methods available to users:

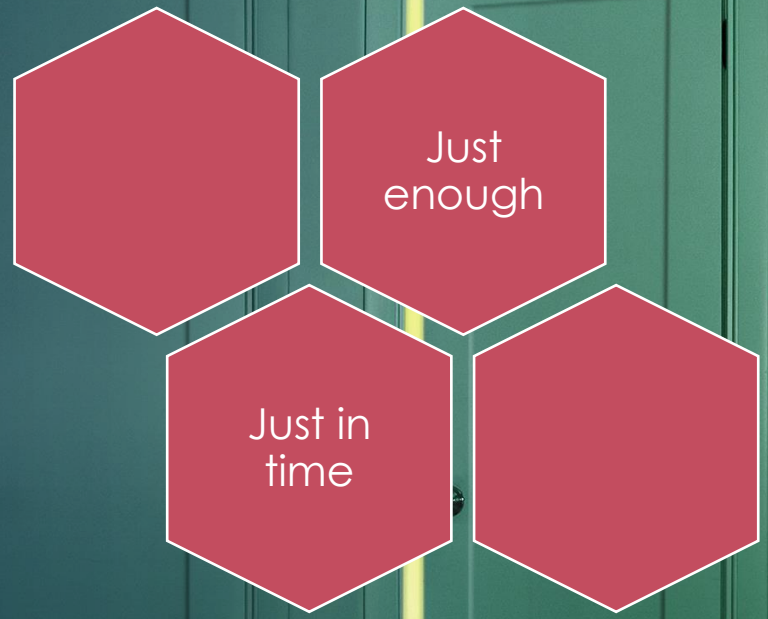
- [ ] Call to phone
- [x] Text message to phone
- [x] Notification through mobile app
- [x] Verification code from mobile app or hardware token




Authentication methods | Policies
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 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

Beginning **September 30, 2024**, authentication methods can't be managed in these legacy MFA and SSPR policies. We recommend customers use the manual migration control to migrate to the Authentication methods policy by the deprecation date.

Privileged Identity Management



Contoso | Quick start

Privileged Identity Management | Azure AD roles

Quick start
Overview

Tasks
My roles
Pending requests
Approve requests
Review access

Manage
Roles
Assignments
Alerts
Access reviews
Discovery and insights (Preview)
Settings

Activity
Resource audit
My audit

Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more

Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

Assign Eligibility

Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

Activate your role

Approve

View and approve all activation request for specific Azure AD roles that you are configured to approve

Approve requests

Audit

View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant

View your history

Contoso | Discovery and insights (Preview)

Privileged Identity Management | Azure AD roles

Quick start
Overview

Tasks
My roles
Pending requests
Approve requests
Review access

Manage
Roles
Assignments
Alerts
Access reviews
Discovery and insights (Preview)
Settings

Activity
Resource audit
My audit

Discovery and insights (Preview)

Discovery and insights find privileged role assignments across Azure AD, and then provides recommendations on how to secure them using Azure AD governance features like Privileged Identity Management (PIM).

Key Concepts

- What is PIM and how should I secure my role assignments?
- What are eligible role assignments and role activation?
- How can I use access reviews to make sure my people still need their role assignments?

Discovered assignments in Contoso

Refresh

5 permanent global administrator assignments

Microsoft recommends you to keep fewer than 5 standing global admins with 2 of them reserved for break glass scenarios

Reduce global administrators

0 accounts assigned to highly privileged roles

Microsoft recommends these as the top role assignments that you should change to eligible

1 service principals with privileged role assignments

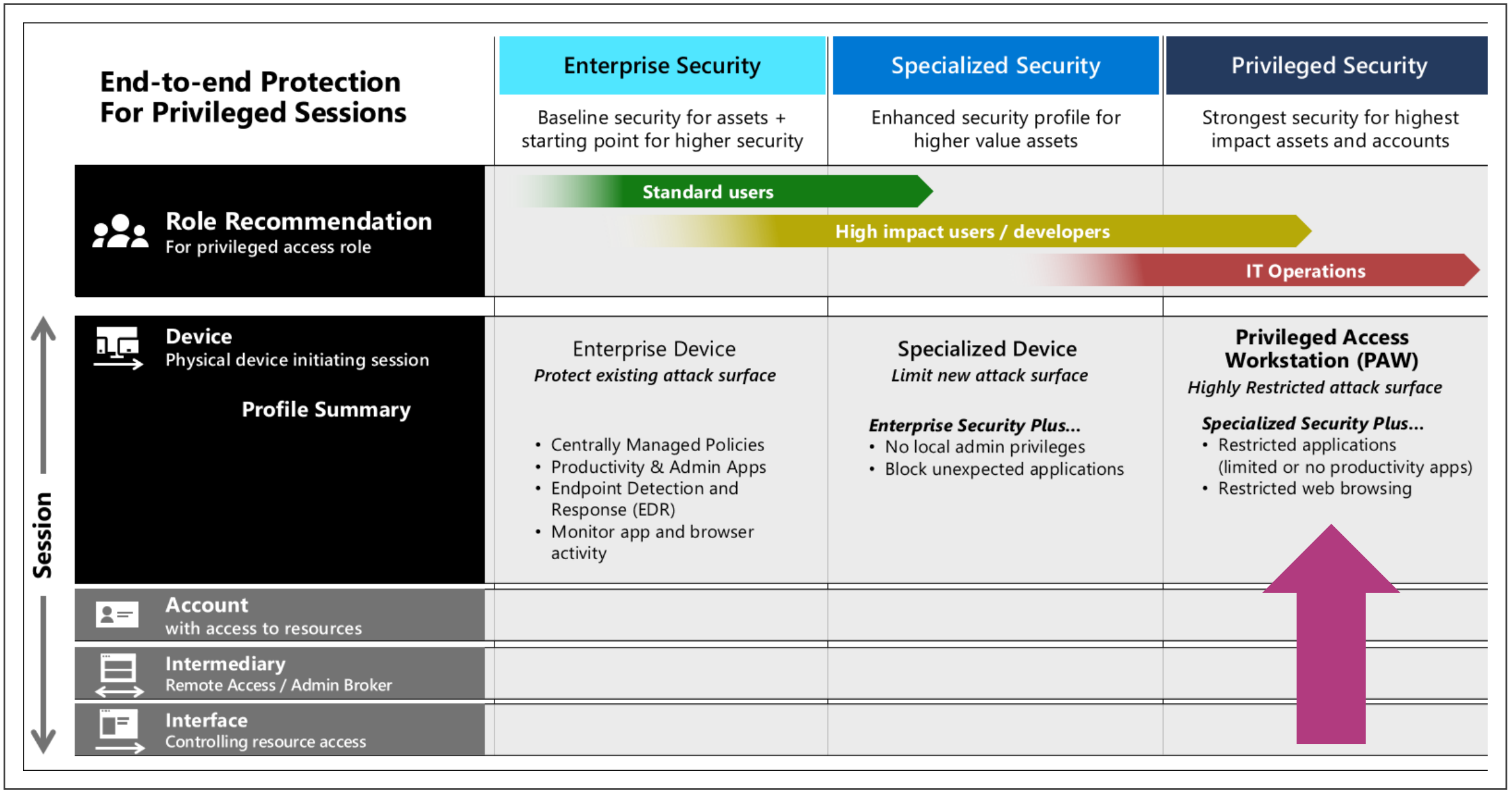
Microsoft recommends you to review all service principals assigned to privileged roles and remove all unnecessary access

Review service principals

A few tips for Privileged Identity Management

- No more standing access
- Protect your Global admin role with approval
- Use Role Assignable Groups
- Keep reviewing access
- Act on alerts
- Start small
- Can be used for both roles and resources

Privileged Access Workstation


End-to-end Protection For Privileged Sessions
Enterprise Security
Baseline security for assets + starting point for higher security
Specialized Security
Enhanced security profile for higher value assets
Privileged Security
Strongest security for highest impact assets and accounts
Role Recommendation
For privileged access role
Standard users
High impact users / developers
IT Operations
Session
Device
Physical device initiating session
Profile Summary
Enterprise Device
Protect existing attack surface
• Centrally Managed Policies
• Productivity & Admin Apps
• Endpoint Detection and Response (EDR)
• Monitor app and browser activity
Specialized Device
Limit new attack surface
Enterprise Security Plus...
• No local admin privileges
• Block unexpected applications
Privileged Access Workstation (PAW)
Highly Restricted attack surface
Specialized Security Plus...
• Restricted applications (limited or no productivity apps)
• Restricted web browsing
Account
with access to resources
Intermediary
Remote Access / Admin Broker
Interface
Controlling resource access

Home
Favorites
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity governance
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

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 *

Require PAW for administrators

Assignments

Users

0 users and groups selected

Target resources

No target resources selected

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Control access based on like risk, device platform, device state. Learn more

User risk

Not configured

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps

Not configured

Filter for devices

Exclude filtered devices

Enable policy

Report-only | On | Off

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure

Yes | No

Devices matching the rule:

- Include filtered devices in policy
- Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	deviceId	Equals	000005c3-b7a6-4c61-89fc-80bf5ccfc366
Or	enrollmentProfileName	Equals	Privileged Access Workstation

Add expression

Rule syntax

Edit

```
device.deviceId -eq "000005c3-b7a6-4c61-89fc-80bf5ccfc366" -or device.enrollmentProfileName -eq "Privileged Access Workstation"
```

3. Protect your **users**


You all will get MFA!!

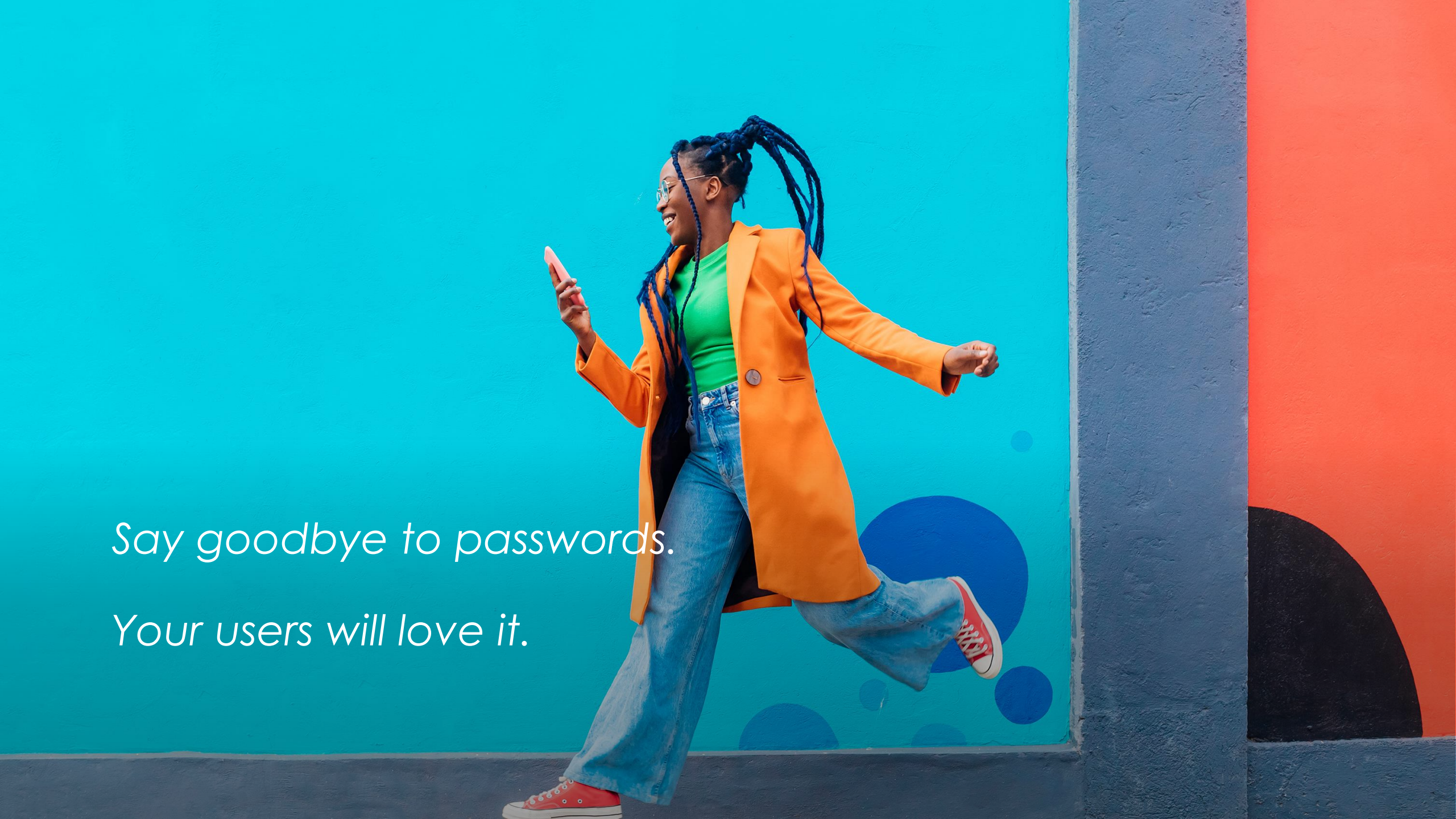
How to enable MFA?

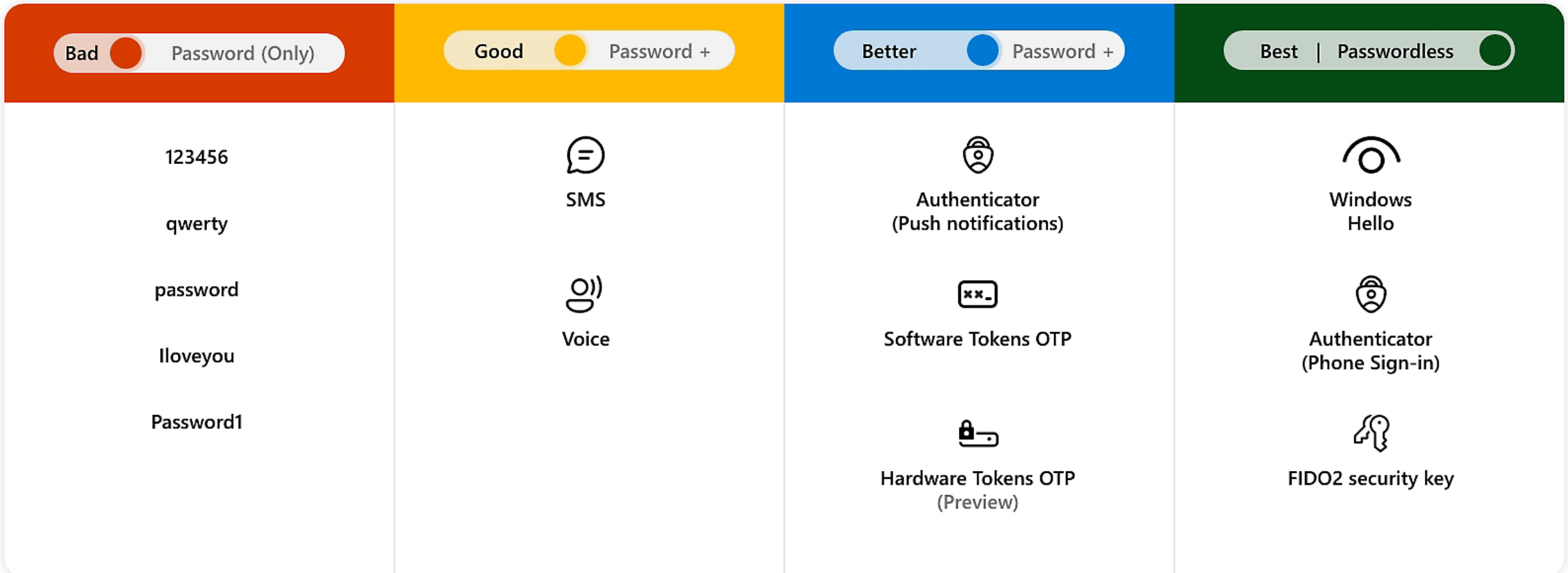
Per user MFA	• Free. Horrible user experience
Security Defaults	• Also free. Easiest way to get secure with the click of a button
Conditional Access	• P1. Very flexible. Works for most organizations
Conditional Access + Identity Protection	• P2. Supports risk-based MFA.


Demo
4 ways to enable MFA

Do's and don'ts for MFA

Do this	MFA on all apps. Exclusions where needed
	Risk-based prompts
	Use Windows Hello for Business
Don't do this	Exclude trusted locations
	Prompt on specific intervals
	Per-user MFA
	Per-user MFA


Say goodbye to passwords.
Your users will love it.


Bad
Password (Only)
123456
qwerty
password
Iloveyou
Password1
Good
Password +
SMS
Voice
Better
Password +
Authenticator
(Push notifications)
Software Tokens OTP
Hardware Tokens OTP
(Preview)
Best | Passwordless
Windows
Hello
Authenticator
(Phone Sign-in)
FIDO2 security key

Windows Hello for Business	• Best option for Windows devices with 1:1 relation to a single user. • Multi-factor unlock • PIN is better than password
FIDO 2 security key	• Shared or roaming devices • BYOD scenarios • Many formfactors
Authenticator phone sign-in	• Can cover many use cases • User friendly • Multi-account support for iOS

Passwordless methods must be bootstrapped using existing MFA method or Temporary Access Pass

It's time to rethink your onboarding strategy

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

Select a template to get started

Got feedback?

Create custom workflows by selecting a built-in template, then modify the tas

Choose a template | Basics | Configure scope | Review tasks | R

Choose a workflow

Choose a workflow template to start creating your custom workflow. Learn mo

Joiner

Onboard pre-hire employee

Configure pre-hire tasks for onboarding employees before their first day

Select | Details

Joine

Onboard

Configure employee

Select | D

Mover | On-demand

Real-time employee change

Execute real-time tasks for employee job changes

Leave

Real-time

Execute re on their la

Template summary

Onboard pre-hire employee

Basics

Name	Onboard pre-hire employee
Description	Configure pre-hire tasks for onboarding employees before their first day
Category	Joiner
Trigger type	Trigger and scope based
Days from event	7
Event timing	Before
Event user attribute	employeeHireDate

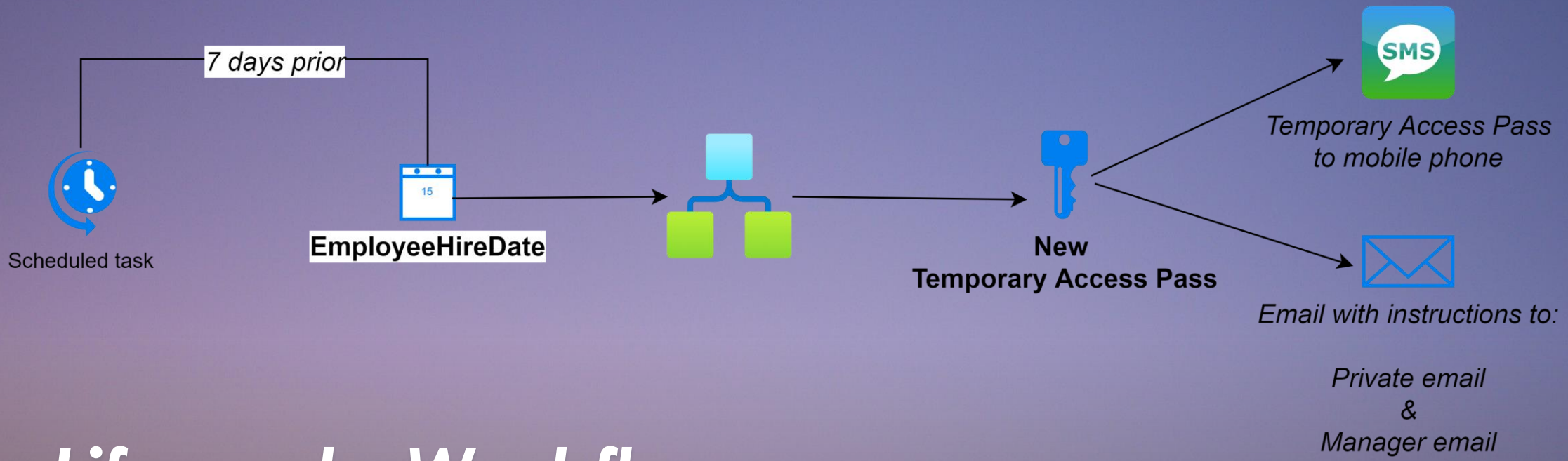
Configure

Scope type	Rule based
Rule	(department eq 'Marketing')

Review tasks

Generate TAP and Send Email	Enabled

Lifecycle Workflows



Lifecycle Workflows + Logic Apps

Automate issuing Temporary Access Pass for joiners with LifeCycle Workflows - JanBakker.tech

Temporary Access Pass Manager

JANBAKKER.TECH
sharing is caring

Search User | Adele Vance | Clear

Create Temporary Access Pass

List/Get Temporary Access Pass

Delete Temporary Access Pass

Send Temporary Access Pass to mobile phone

Temporary Access Pass **A&Unj$#m**

ID	aa77cce2-98ca-420d-add5-488573a3dd01
Lifetime (minutes)	60
is Usable	true
is Usable Once	false
Created	Monday, August 9, 2021 10:10:40
Usability	EnabledByPolicy

+31643941043

AdeleV@M365x583104.OnMicrosoft.com

Bellevue

Power apps + Power Automate

Graph Explorer

Tenant Contoso

MA

Sample queries | Resources | History

Search sample queries

See more queries in the Microsoft Graph API Reference docs.

- Getting Started (8)
  - GET my profile
  - GET my profile (beta)
  - GET my photo
  - GET my mail
  - GET list items in my drive
  - GET items trending around me
  - GET my manager
  - GET my To Do task lists
- Applications (8)
- Batching (2)
- Compliance (beta) (10)
- Edge (4)
- Excel (7)

POST v1.0 https://graph.microsoft.com/v1.0/users/DeliaD@M365x80658054.OnMicrosoft.com/authentication/temporaryAccessPassMethods

Run query

Request body | Request headers | Modify permissions | Access token

```
{}
```

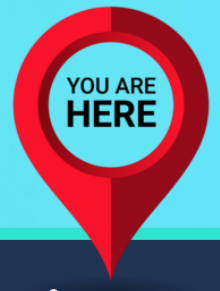
Created - 201 - 3108ms

Response preview | Response headers | Code snippets | Toolkit component | Adaptive cards | Expand


```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users('DeliaD%40M365x80658054.OnMicrosoft.com')/authentication/temporaryAccessPassMethods/$entity",
    "id": "9fc4635f-cc21-4209-9bf2-a3388d465e84",
    "isUsable": true,
    "methodUsabilityReason": "EnabledByPolicy",
    "temporaryAccessPass": "=KE*$P5G",
    "createdDateTime": "2023-09-10T13:14:05.4630766Z",
    "startDateTime": "2023-09-10T13:14:03.8359833Z",
    "lifetimeInMinutes": 60,
    "isUsableOnce": false
}
```


Integrate with any app using Graph API

Not ready for passwordless yet?



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

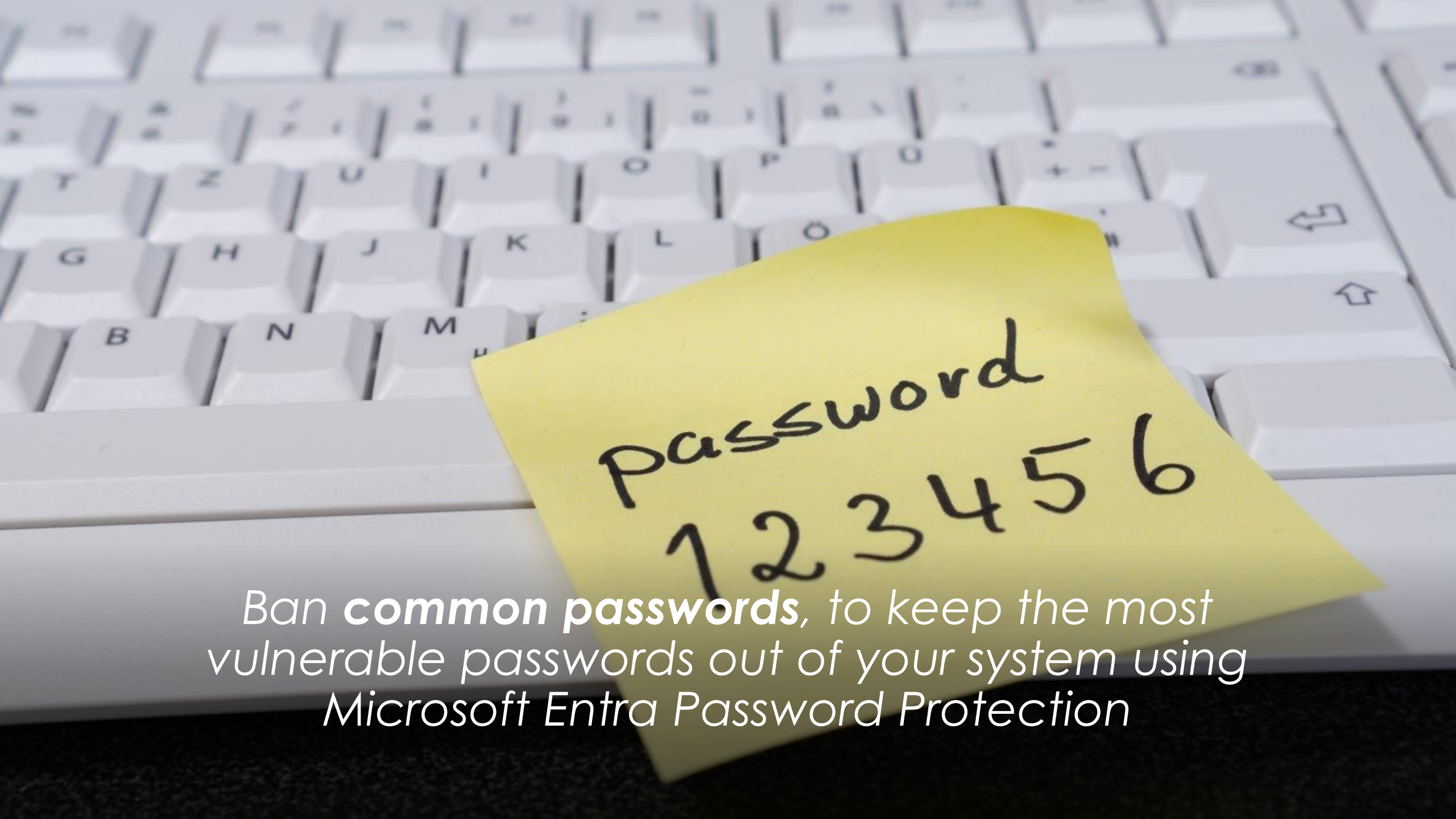

Let's talk about
passwords

What about them?

- We need to memorize them, so we:
  - Make them weak
  - Reuse passwords

- (outdated) IT principals force us to:
  - Create long, complex passwords
  - Reset them every x days


What can we do
about it?

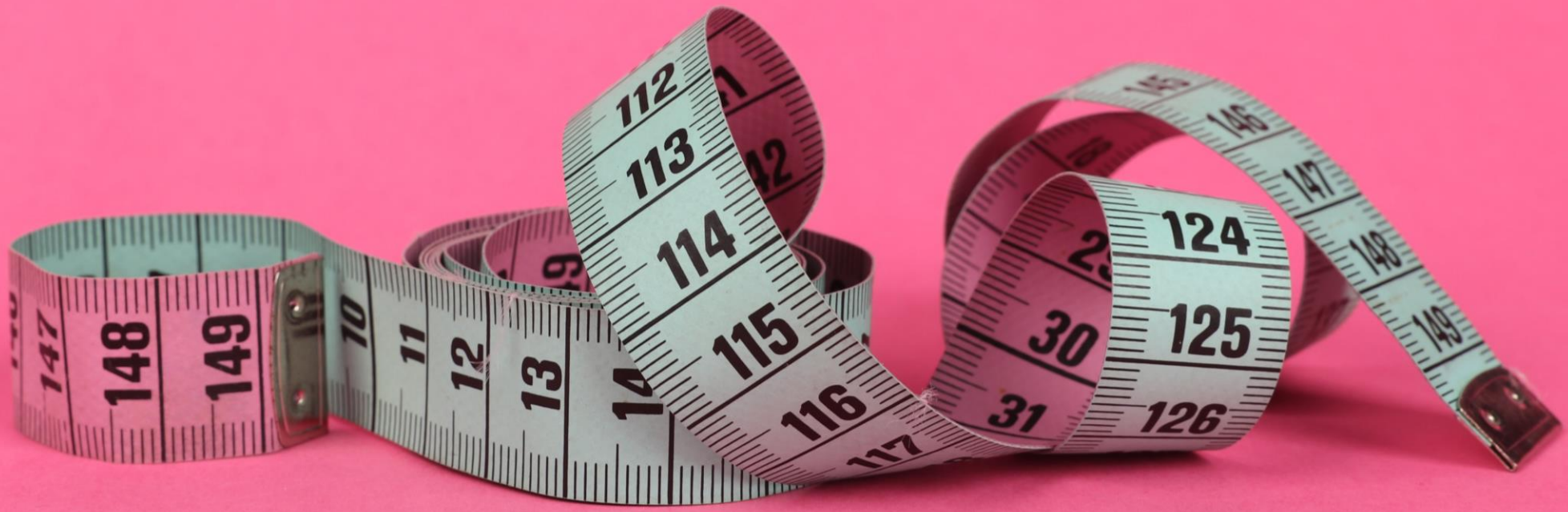


*Ban **common passwords**, to keep the most vulnerable passwords out of your system using Microsoft Entra Password Protection*


Don't require character composition requirements. For example, *&(^%$


Don't require mandatory periodic password resets for user accounts

To encourage users to think about a unique password, we recommend keeping a reasonable **14-character** minimum length requirement.



Flower-country

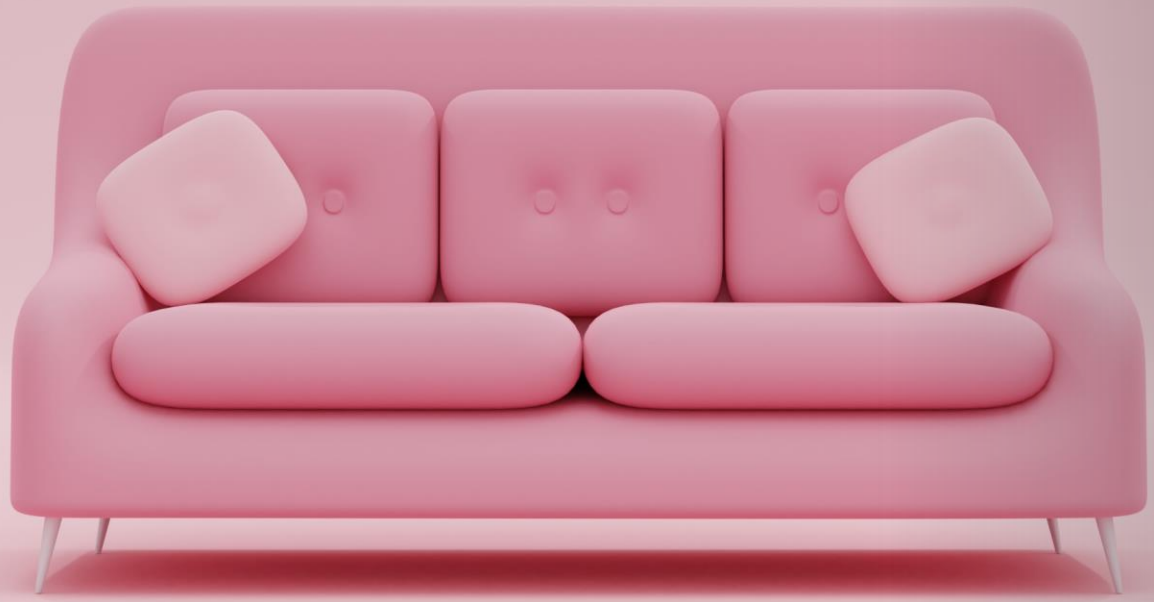

bus-Corn-fleet


emploY-shallow-Truth


Password Hash Sync also enables **leaked credential detection** for your hybrid accounts.

4. Management & Governance

Keep things simple




Targeted vs Zero Trust
approach


User personas or existing license groups for Conditional Access

Suggested Personas for Conditional Access

- Internals
- Externals
- Guests
- Admins
- Developers
- Service Accounts
- Workload Identities

Make use of the Conditional Access templates

Always start with report-only!

Home
Favorites
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity governance
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

Create new policy from templates

Select a template | Review + Create

Search

Secure foundation | Zero Trust | Remote work | Protect administrator | Emerging threats | All

Require multifactor authentication for admins

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.
Learn more

View | Download JSON file

Securing security info registration

Secure when and how users register for Azure AD multifactor authentication and self-service password reset.
Learn more

View | Download JSON file

Block legacy authentication

Block legacy authentication endpoints that can be used to bypass multifactor authentication.
Learn more

View | Download JSON file

Require multifactor authentication for all users

Require multifactor authentication for all user accounts to reduce risk of compromise.
Learn more

View | Download JSON file

Require multifactor authentication for Azure management

Require multifactor authentication to protect privileged access to Azure management.
Learn more

View | Download JSON file

Require compliant or hybrid Azure AD joined device or multifactor authentication for all users

Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. (macOS or Windows only)
Learn more

View | Download JSON file

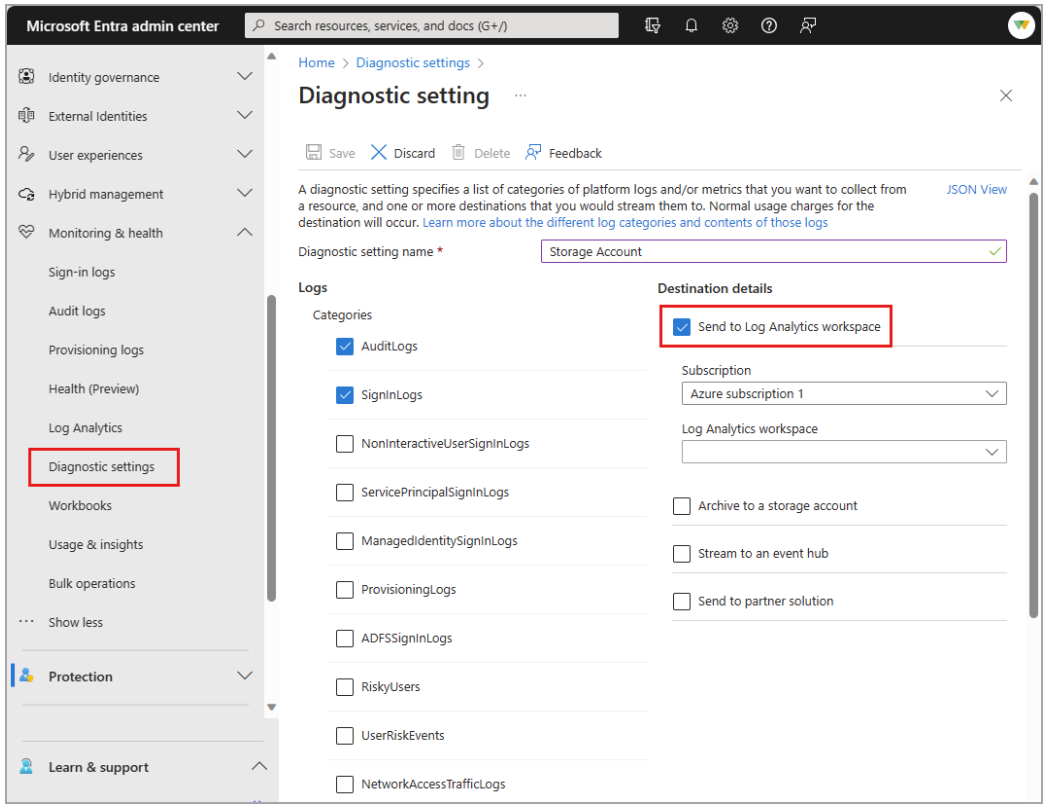
Keep reviewing your exclusion groups!

- Access reviews
- PIM for groups

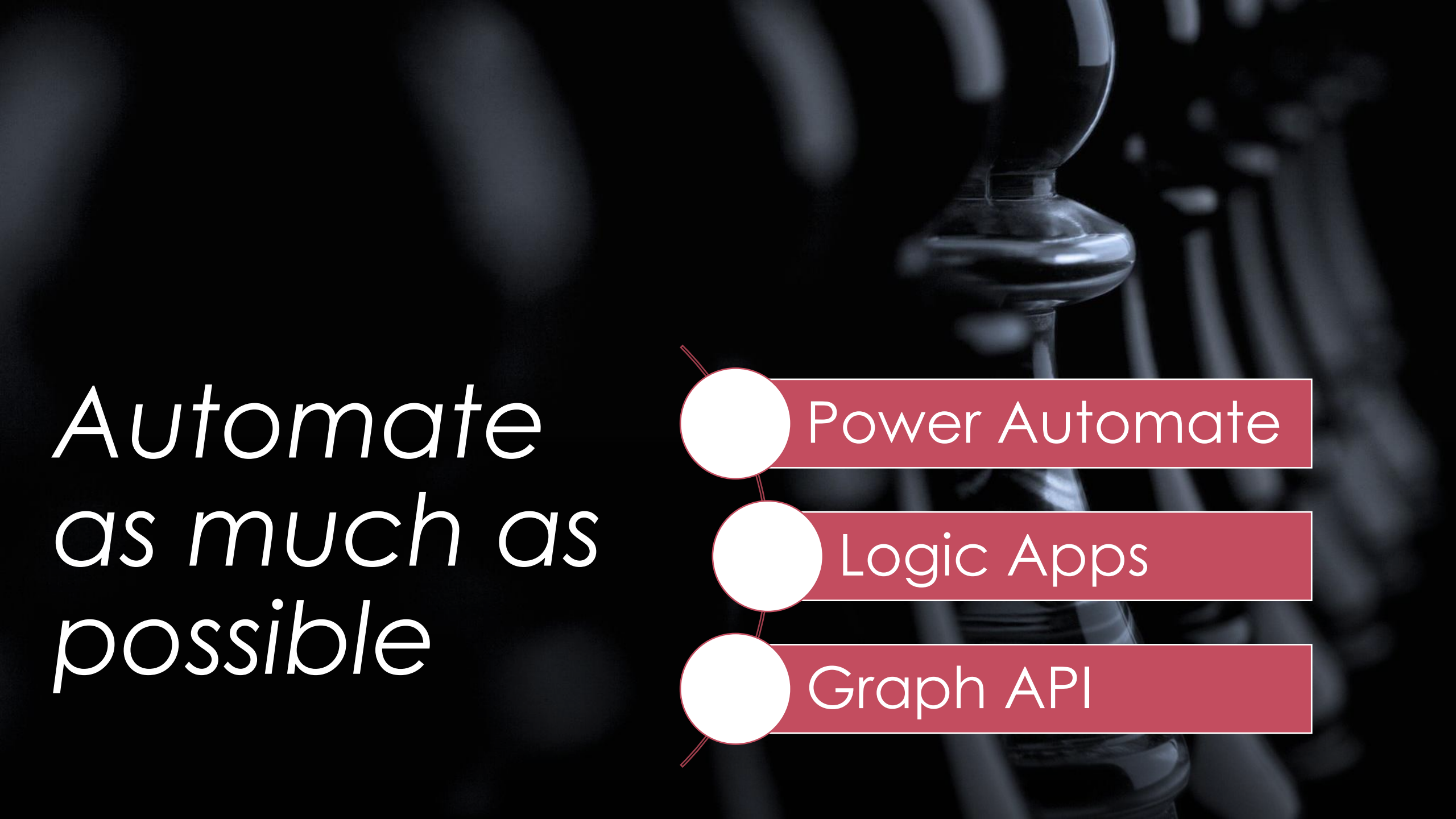
Don't forget about your ***break-glass*** *emergency accounts*

Tip: FIDO2 keys make great break-glass methods!

Send logs to Log Analytics



[Integrate Azure Active Directory logs with Azure Monitor logs - Microsoft Entra | Microsoft Learn]


Automate as much as possible
Power Automate
Logic Apps
Graph API


Embrace self-service

Demo: My Groups & My Access in Microsoft 365


Request group membership using My Groups

CONTOSO demo | My Groups

AV
Adele Vance
AdeleV@M365x80658054.On...

- Overview
- Groups I own (0)
- Groups I am in (16)
- Requests (0)

Overview

Join a group
Search groups around you

Collaborate

Use Microsoft 365 Groups to send email to a group of users, establish a team in Teams, or create a SharePoint site.

Create M365 Group

Control Access

Security groups are used to secure resources. Resource permissions assigned to a SG apply to all its members.

Create Security Group

Requests to join your groups

Requested by	Group
No new requests.	

Adele requests access to a group

CONTOSO demo | My Groups

MA

MOD Administrator
admin@M365x80658054.onm..

- Overview
- Groups I own (19)
- Groups I am in (13)
- Requests (0)

Overview

Join a group
Search groups around you

Collaborate

Use Microsoft 365 Groups to send email to a group of users, establish a team in Teams, or create a SharePoint site.

Create M365 Group

Control Access

Security groups are used to secure resources. Resource permissions assigned to a SG apply to all its members.

Create Security Group

Requests to join your groups

Requested by	Group
No new requests.	

Group owner approves the request

CONTOSO demo | My Groups

AV
Adele Vance
AdeleV@M365x80658054.On...

- Overview
- Groups I own (0)
- Groups I am in (17)
- Requests (0)

Overview

Join a group
Search groups around you

Collaborate

Use Microsoft 365 Groups to send email to a group of users, establish a team in Teams, or create a SharePoint site.

Create M365 Group

Control Access

Security groups are used to secure resources. Resource permissions assigned to a SG apply to all its members.

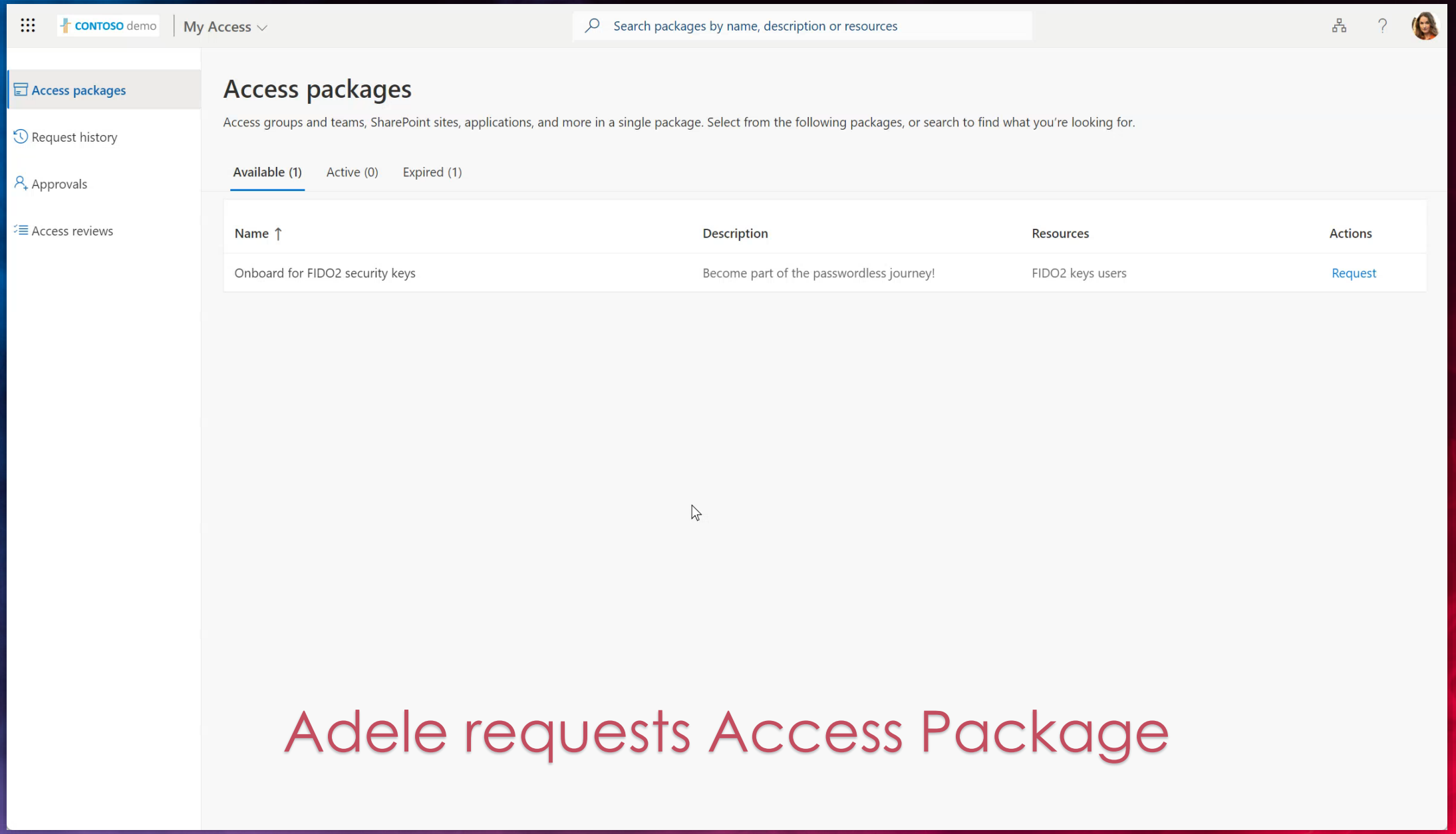
Create Security Group

Requests to join your groups

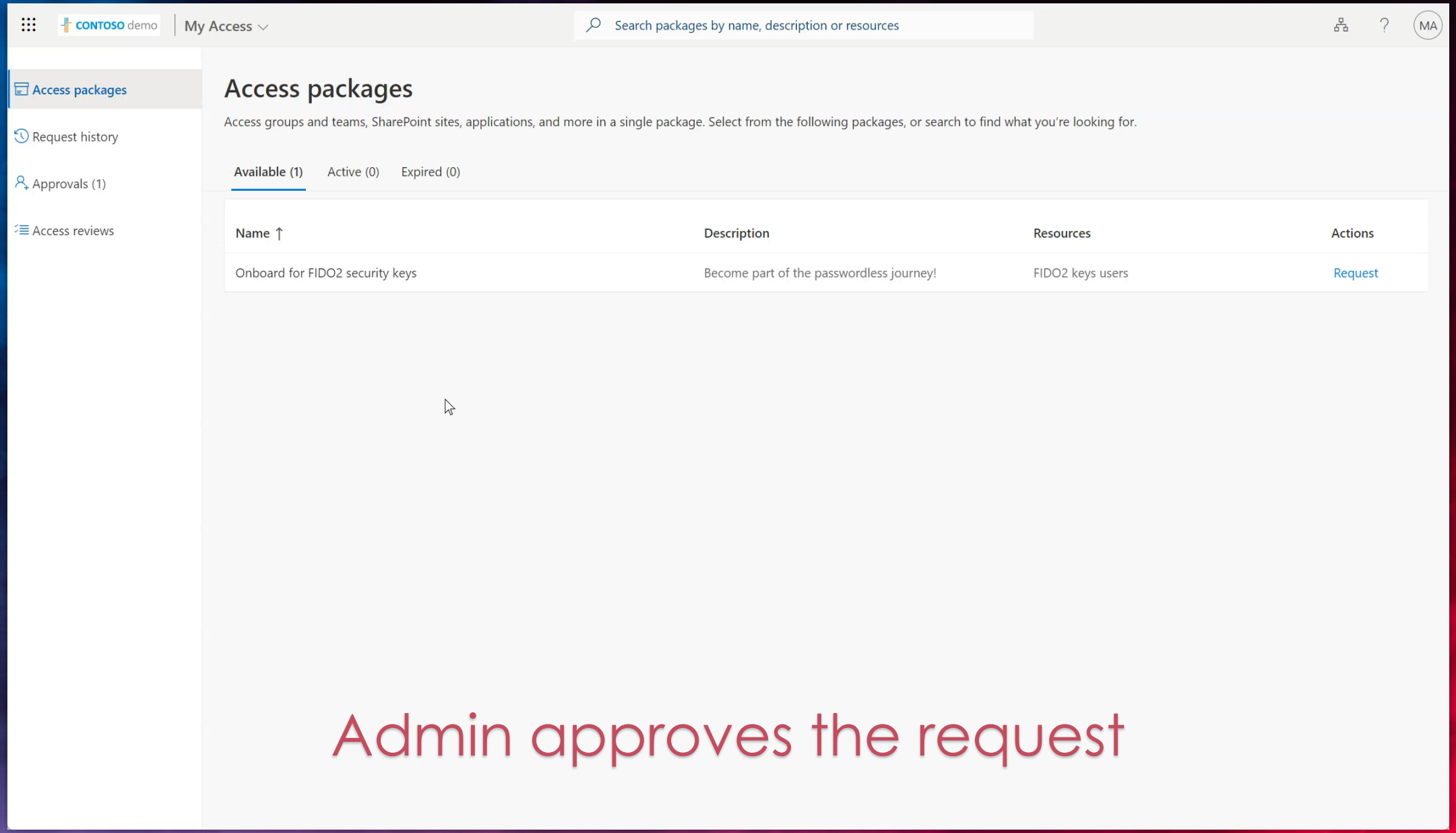
Requested by	Group
No new requests.	

Adele is now a member of the group

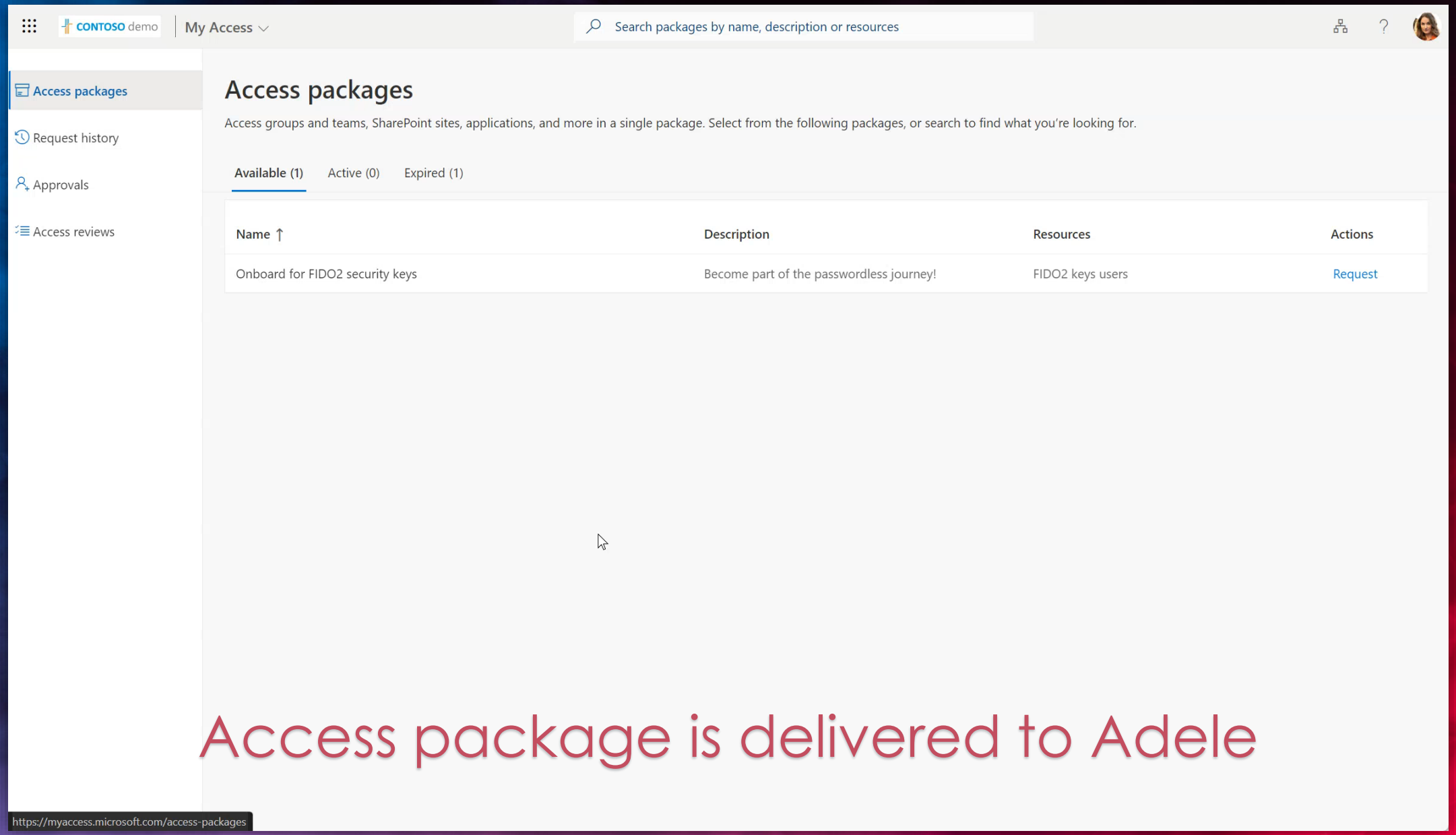

Request access
package using
My Access



Adele requests Access Package



Admin approves the request



Access package is delivered to Adele

To sum up…..

Enable MFA for admins and users

Use PIM and PAW for admins

Pick the right identity model & authentication type

Stop the password nightmare

Keep things simple

Automate

Embrace Self-Service!


Questions?

Thank you & stay safe!