

SC-300

Tag 2

# Microsoft Identity and Access Administrator

Guten Morgen!



## LP 2

Implement an  
authentication and access  
management solution



# Agenda

---

①.

Q □ SP (APP) AI Agent  
Entra ID + Instance = Tenant  
+ Data

- LP 1 Implement an Identity Management Solution
- LP 2 Implement an Authentication and Access Management Solution
- LP 3 Implement Access Management for Apps
- LP 4 Plan and Implement an Identity Governance Strategy

A [Roles] = {Perm 1, 2, 27} . json  
Perm 1, 2

PIM Packages Policies

$12^{30} - 13^{30}$

# Outline

---

- Plan and implement Microsoft Entra multifactor authentication (MFA)
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra ID Protection
- Implement access management for Azure resources
- Configure and deploy Global Secure Access

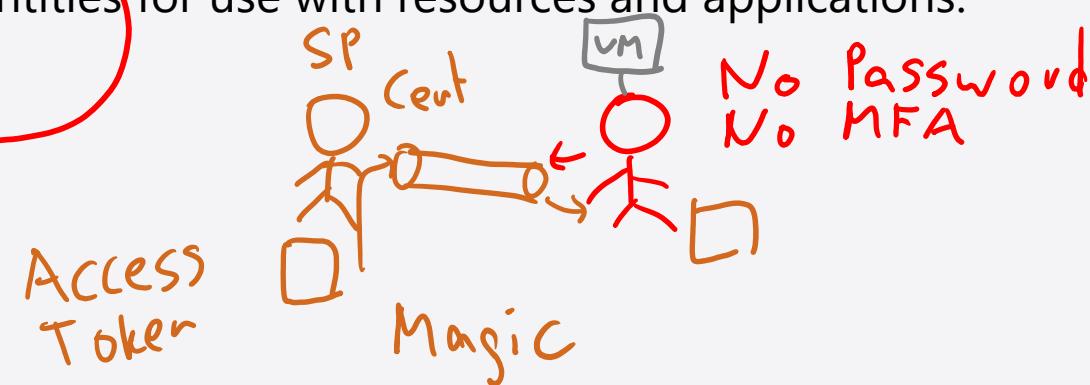
# Learning objectives

After completing this module, you will be able to:

1 Configure and manage authentication including MFA.

2 Implement Zero Trust using Conditional Access and other tools.

3 Create and manage identities for use with resources and applications.



# Secure Microsoft Entra users with multifactor authentication

# Objectives

- 1** Configure and deploy self-service password reset
- 2** What is Microsoft Entra multifactor authentication?
- 3** Plan your multifactor authentication
- 4** Configure multifactor authentication methods

# Microsoft Entra features to protect cloud assets



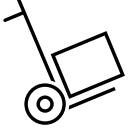
- Password complexity rules
- Password expiration rules
- Self-service password reset (SSPR)
- Microsoft Entra Identity Protection
- Microsoft Entra password protection
- Microsoft Entra smart lockout
- Microsoft Entra Application Proxy
- Single sign-on (SSO)
- Microsoft Entra Connect
- Microsoft Entra MFA and Conditional Access



# Configure and deploy self-service password reset

# Microsoft Entra self-service password reset

P1

Users can reset their own password	
	No admin/IT intervention
Reduces the loss of user productivity	
	Reduces helpdesk efforts
Users must be enrolled first	
	Requires an assigned license

MFA  
Questions

# Enabling SSPR

Home > Password reset

## Password reset | Properties

Microsoft Entra ID for workforce

«  Save  Discard

Diagnose and solve problems

Manage

-  Properties
-  Authentication methods
-  Registration
-  Notifications
-  Customization
-  On-premises integration
-  Administrator Policy

Self service password reset enabled 

 None  Selected  All

Select group 

Mark 8 Project Team

 These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

# SSPR Licensing options

Feature	Microsoft Entra ID Free	Microsoft 365 Business Standard	Microsoft 365 Business Premium	Microsoft Entra ID Premium P1 or P2
<b>Cloud-only user password change</b> When a user in Microsoft Entra ID knows their password and wants to change it	•	•	•	•
<b>Cloud-only user password reset</b> When a user in Microsoft Entra ID has forgotten their password		•	•	•
<b>Hybrid user password change or reset with on-premises writeback</b> When a user in Microsoft Entra ID is synchronized from an on-premises directory using Microsoft Entra Connect			•	•

# Exercise—Configure and deploy self-service password reset



Microsoft Entra self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or helpdesk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work. This ability reduces helpdesk calls and loss of productivity when a user can't sign in to their device or an application.

This exercise teaches the student to enable self-service password reset, register a cell phone number, and test self-service password reset.

[Launch this Exercise in GitHub](#)

## Password reset | Properties

Microsoft Entra ID for workforce

Save Discard

Self service password reset enabled

None Selected All

Select group

Mark 8 Project Team

# User—Sign-ins report

The screenshot shows two main sections: 'Sign-in events' and 'Activity Details: Sign-ins'.

**Sign-in events:** This section displays a table of sign-in logs for the last 24 hours. The columns are Date, Request ID, Application, and Status. One row, from Adele Vance, has its 'Status' field circled in red and contains the value 'Interrupted'.

Date	Request ID	Application	Status
4/29/2025, 11:00:01 A...	f3a68a2e-4da8-40a5...	Office365 Shell WCSS...	Success
4/29/2025, 11:00:01 A...	95b5d385-6820-48dc...	Office365 Shell WCSS...	Success
4/29/2025, 11:00:01 A...	997027ac-27cf-4dbb...	Office365 Shell WCSS...	Success
4/29/2025, 10:59:56 A...	0d09122f-d2a7-4a59...	Microsoft Office 365 ...	Success
4/29/2025, 10:59:47 A...	22683795-a4d0-4356...	Azure Portal	Success
4/29/2025, 10:35:47 A...	d4c2b8a2-c133-4b32...	Azure Portal	Success
4/29/2025, 10:35:43 A...	ab0f2fd3-f7e7-4416...	Azure Portal	Interrupted
4/28/2025, 3:45:14 PM	8f6b79c9-8867-4506...	Azure Portal	Success
4/28/2025, 3:42:21 PM	70272ee6-de2c-4f1e...	Azure Portal	Success
4/28/2025, 3:42:16 PM	08686a71-add5-4b6a...	Azure Portal	Interrupted

**Activity Details: Sign-ins:** This section provides detailed information about a specific sign-in event. It includes tabs for Basic info, Location, Device info, Authentication Details, Conditional Access, and Report-only. The Authentication Details tab is selected, showing the following data:

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date	4/29/2025, 10:35:43 AM		Multifactor authentication		
Request ID	ab0f2fc				
Correlation ID	fd7cc...				
Authentication requirement	Multifactor authentication				
Agent Type	Not Agentic				
Status	Interrupted				
Continuous access evaluation	No				

Below this, there is a note explaining the 'Interrupted' status: "This is an expected part of the login flow, where a user is asked if they want to remain signed into this browser to make further logins easier. For more details, see <https://techcommunity.microsoft.com/t5/microsoft-entra/the-new-azure-ad-sign-in-and-keep-me-signed-in-experiences/td-p/128267>".

The Troubleshoot Event section contains steps to follow:

- Launch the Sign-in Diagnostic.
- Review the diagnosis and act on suggested fixes.

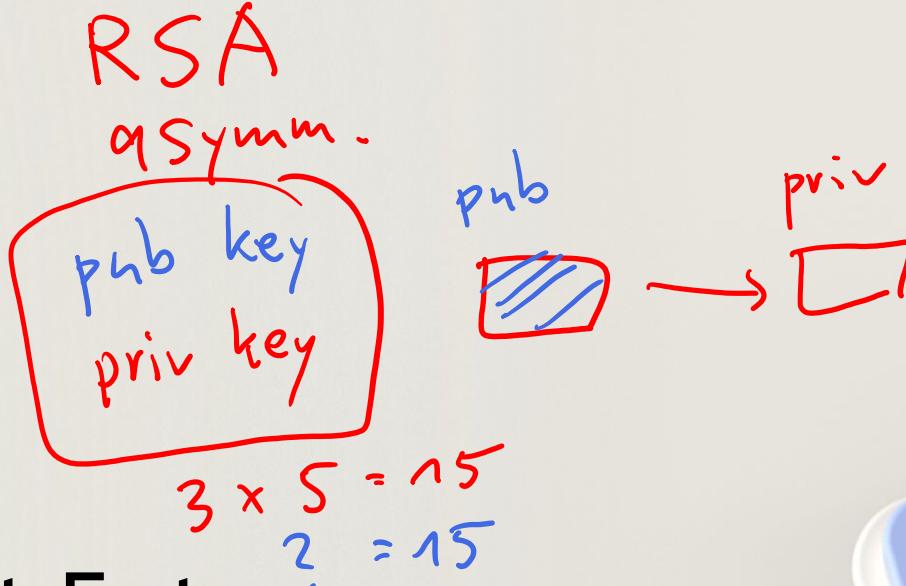
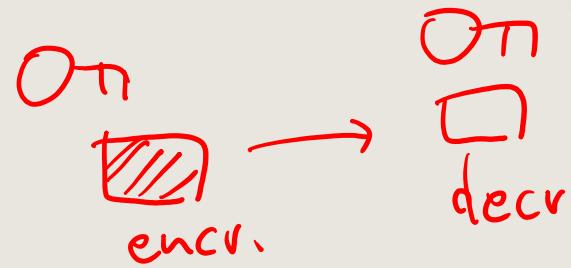
The User section shows Adele Vance with her email address adelev@contoso.com.

Handwritten annotations include:

- A blue box encloses the 'Authentication Details' tab.
- A red circle highlights the 'Status' column in the sign-in events table.
- A red circle highlights the 'User' and 'Username' fields in the activity details.
- A blue arrow points from the 'Authentication Details' tab to the handwritten text 'LLM'.
- A blue arrow points from the 'User' field to the handwritten text 'Vector 1'.
- A blue arrow points from the 'Username' field to the handwritten text 'Vector 2'.
- A blue arrow points from the 'Authentication Details' tab to the handwritten text 'semantic search'.

The **Authentication Details** or **Conditional Access** tab of the event details shows you the status code or which policy triggered the MFA prompt.

3DES  
Symm.



## What is Microsoft Entra multifactor authentication?

passkey  
priv key

public

A red arrow points from a box labeled "priv key" to a box labeled "passkey". A blue arrow points from a box labeled "public" to a box labeled "priv key".

WWW  
priv  
pub

Off

On

pub

A blue arrow points from a box labeled "priv" to a box labeled "WWW". A blue arrow points from a box labeled "pub" to a box labeled "Off". A red arrow points from a box labeled "On" to a box labeled "pub".

# Value and capabilities of Microsoft Entra MFA

## Value

- More secure than passwords
- Quick and easy to set up and manage
- Strong identity verification
- Stronger security
- Often supports compliance goals
- Many different types of authentication methods, with different levels of security

# Categories of authentication factors

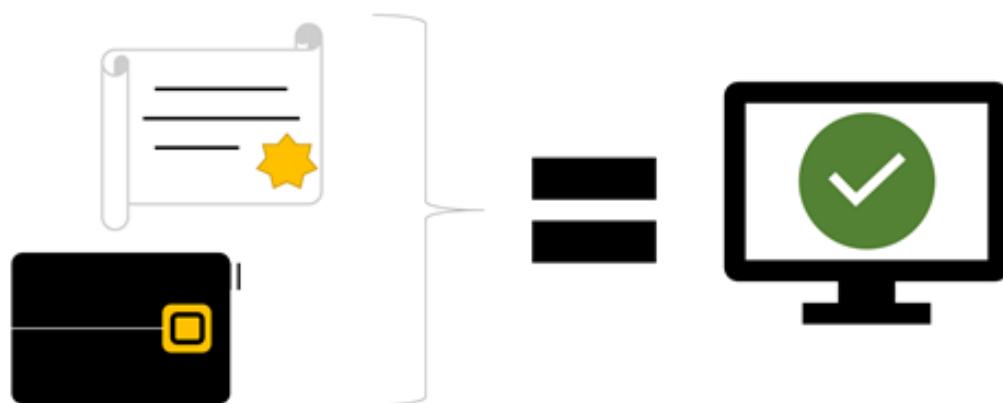
Something you know



Something you possess



Something you are

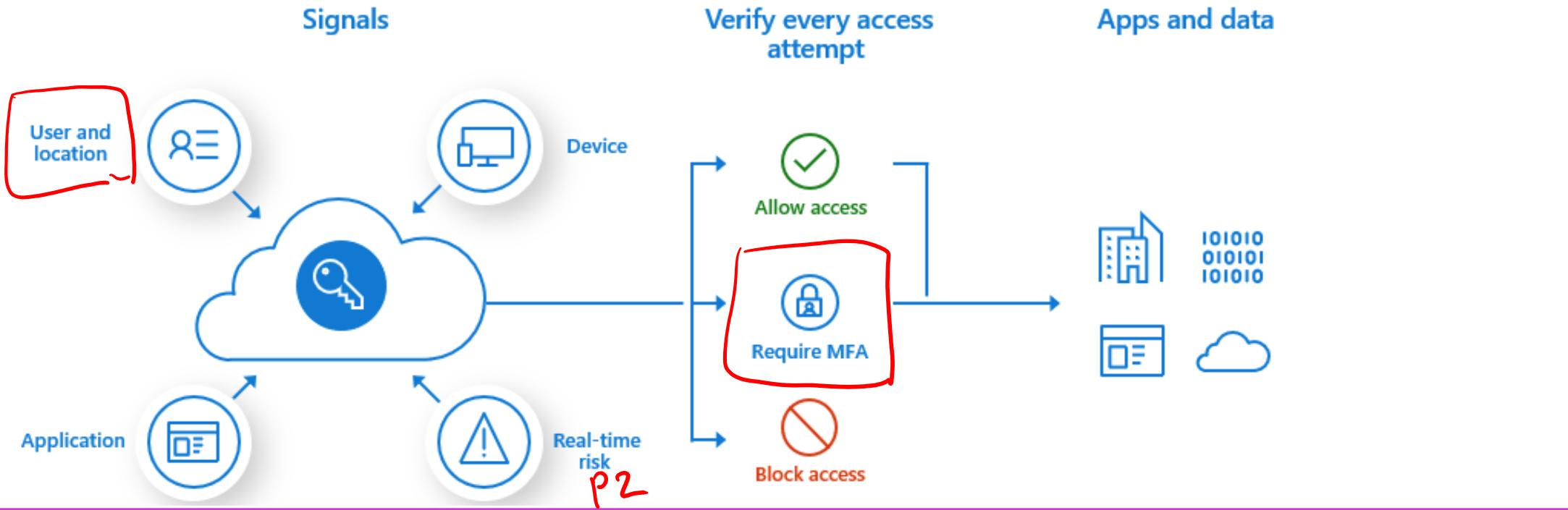


Free ✓  
Per User MFA

# Enabling MFA with Conditional Access

P1

All User  
exclude  
Paul  
Peter



Set up a Conditional Access policy that requires a user/group to have MFA required for access to specific resources.

# User states of MFA



Disabled—default state, user not enrolled in MFA.

---



Enabled—user is enrolled in MFA, but can still use their password. At each login they are prompted to register for an MFA authentication method.

---



Enforced—user is enrolled in MFA, and has either completed their MFA registration; or will be forced to complete it on their next login.

# Considerations for Microsoft Entra MFA based on the infrastructure



Cloud Only setup—nothing additional required to set up Microsoft Entra MFA

---



Hybrid Identity—Microsoft Entra Connect must be deployed and synchronized/federated with your on-premises Active Directory Domain Services

---



Need on-premises legacy apps—Microsoft Entra Application Proxy must be deployed

---



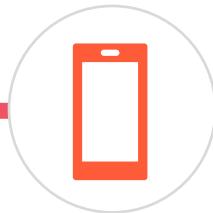
Use Microsoft Entra MFA with a RADIUS Authentication—a Network Policy Server (NPS) must be set up and configured

# Plan your multifactor authentication deployment

# Deployment considerations

- Get employee buy-in
  - User communications (posters, emails, and other support items)
- Consider rolling MFA out in waves
- Create a full communications plan
- Tie your MFA roll-out with Conditional Access compliance
  - Specific devices, working location, application or data access
- Select your authentication methods ✓
- Plan MFA registration process
- Add on-premises systems after MFA is established

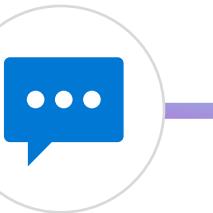
# Supported authentication methods



Mobile app verification



Call to a phone



Text message to a phone

# Exercise—enable Microsoft Entra multifactor authentication

This exercise teaches students how to configure multifactor authentication policies, set up Conditional Access rules, and configure Microsoft Entra MFA for passwords.



[Launch this Exercise in GitHub](#)

## Per-user multifactor authentication ...

Bulk update

Got feedback?

[Users](#)   [Service settings](#)

Use multifactor authentication (MFA) to protect your users and data. Our recommended

Before you begin, take a look at the [multifactor authentication deployment guide](#).

Enable MFA Disable MFA Enforce MFA User MFA settings

# Configure multifactor authentication methods

# Azure authentication methods

## AuthN methods when deploying MFA

- Microsoft Authenticator app
- Windows Hello for Business
- FIDO2 security key
- OATH hardware token (preview)
- OATH software token
- SMS
- Voice call

## Supplemental AuthN for niche use

- Security questions
  - Non-admins only
- Email address
  - Part of SSPR if enabled
- App passwords
  - For legacy apps that don't directly support Azure MFA

# Registering an authentication method

 Microsoft

lidiah

## Let's keep your account secure

We'll help you set up another way to verify it's you.

[Use a different account](#)

[Learn more about verifying your identity](#)

[Next](#)

## Microsoft Authenticator



Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

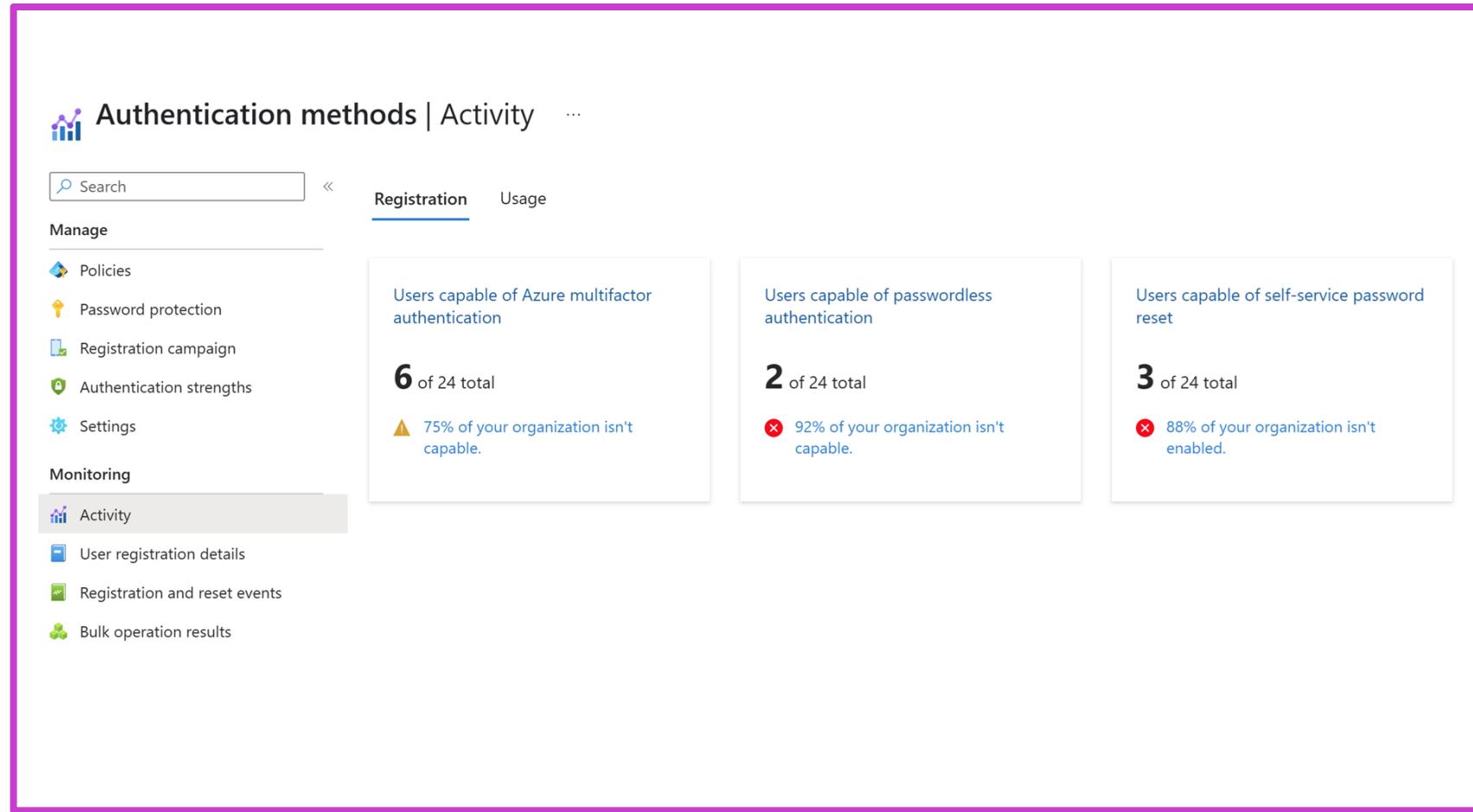
[Next](#)

I want to set up a different method

*Seed*

# Monitoring adoption

- Microsoft Entra ID includes a **Usage & insights** view in the **Monitoring** section where you can monitor the authentication methods activity. From here you can view the adoption of MFA.
- In addition to the overall registration numbers, you can also see the success and failure of registrations per authentication method.
- You can also learn more about MFA usage in your organization through the **Usage** tab on the main view.



# Extend MFA to devices

# Require MFA for devices

Use Conditional Access rules to extend MFA to devices and device enrollment.

Two methods:

- 1) Policy for Microsoft Intune or Microsoft Intune Enrollment (seen in picture).
- 2) Policy within Intune device settings.

The screenshot shows the 'New Conditional Access policy' page. A green arrow points from the 'Grant' section in the main panel to the expanded 'Grant' configuration box on the right.

**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 \*

Assignments

Users or workload identities [\(i\)](#)  
Specific users included

Cloud apps or actions [\(i\)](#)  
1 app included

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

Access controls

Grant [\(i\)](#)  
1 control selected

Session [\(i\)](#)  
0 controls selected

Enable policy  
 Report-only  On  Off

**Create**

**Control access based on all or specific cloud apps or actions. [Learn more](#)**

Select what this policy applies to

**Include** **Exclude**

None  
 All cloud apps  
 Select apps

Select  
[Microsoft Intune Enrollment](#)

**Grant**

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

Block access  
 Grant access

Require multifactor authentication  
 Require device to be marked as compliant  
 Require Hybrid Azure AD joined device  
 Require approved client app [See list of approved client apps](#)  
 Require app protection policy [See list of policy protected client apps](#)  
 Require password change

For multiple controls  
 Require all the selected controls  
 Require one of the selected controls

# Protecting Microsoft Entra ID from device attacks

## Monitor the device:

- Device registration and Microsoft Entra ID join
- Noncompliant devices accessing applications
- BitLocker key retrieval
- Device administrator roles
- Sign-ins to virtual machines

## Logs with device data:

- Microsoft Entra ID audit logs
- Sign-in logs
- Microsoft 365 audit logs
- Azure Key Vault logs

## Tools to use:

- Microsoft Sentinel
- Azure Monitor
- Azure Event Hubs

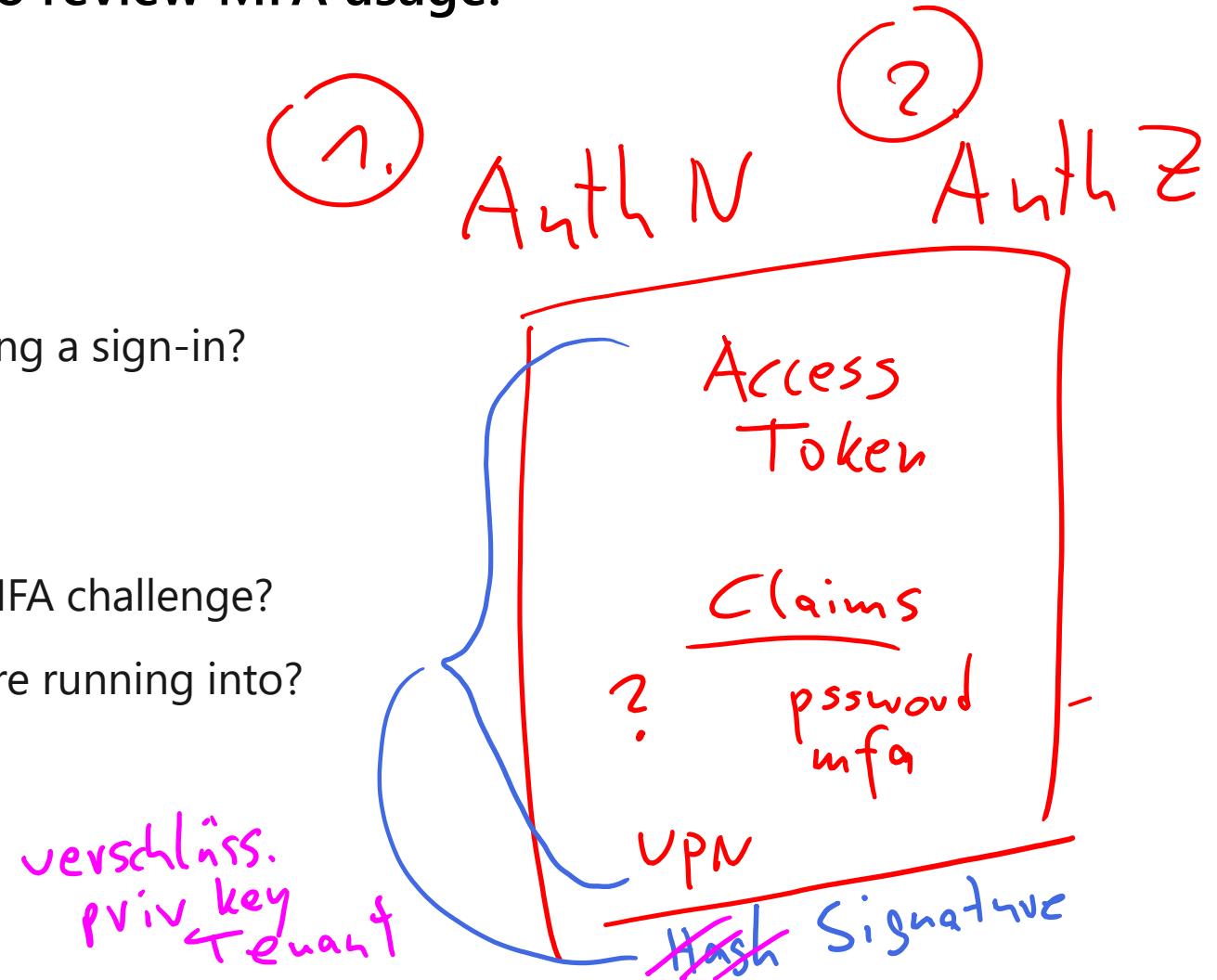
# Monitor MFA

# Monitor Microsoft Entra ID MFA activity

Use the Microsoft Entra sign-in report to review MFA usage.

Data available in the report:

- Was the sign-in challenged with MFA?
- How did the user complete MFA?
- Which authentication methods were used during a sign-in?
- Why was the user unable to complete MFA?
- How many users are challenged for MFA?
- How many users are unable to complete the MFA challenge?
- What are the common MFA issues end users are running into?



# References

## Planning a cloud-based Microsoft Entra multifactor authentication deployment

<https://learn.microsoft.com/azure/active-directory/authentication/howto-mfa-getstarted>

## Deploy Microsoft Entra self-service password reset

<https://learn.microsoft.com/azure/active-directory/authentication/howto-sspr-deployment>



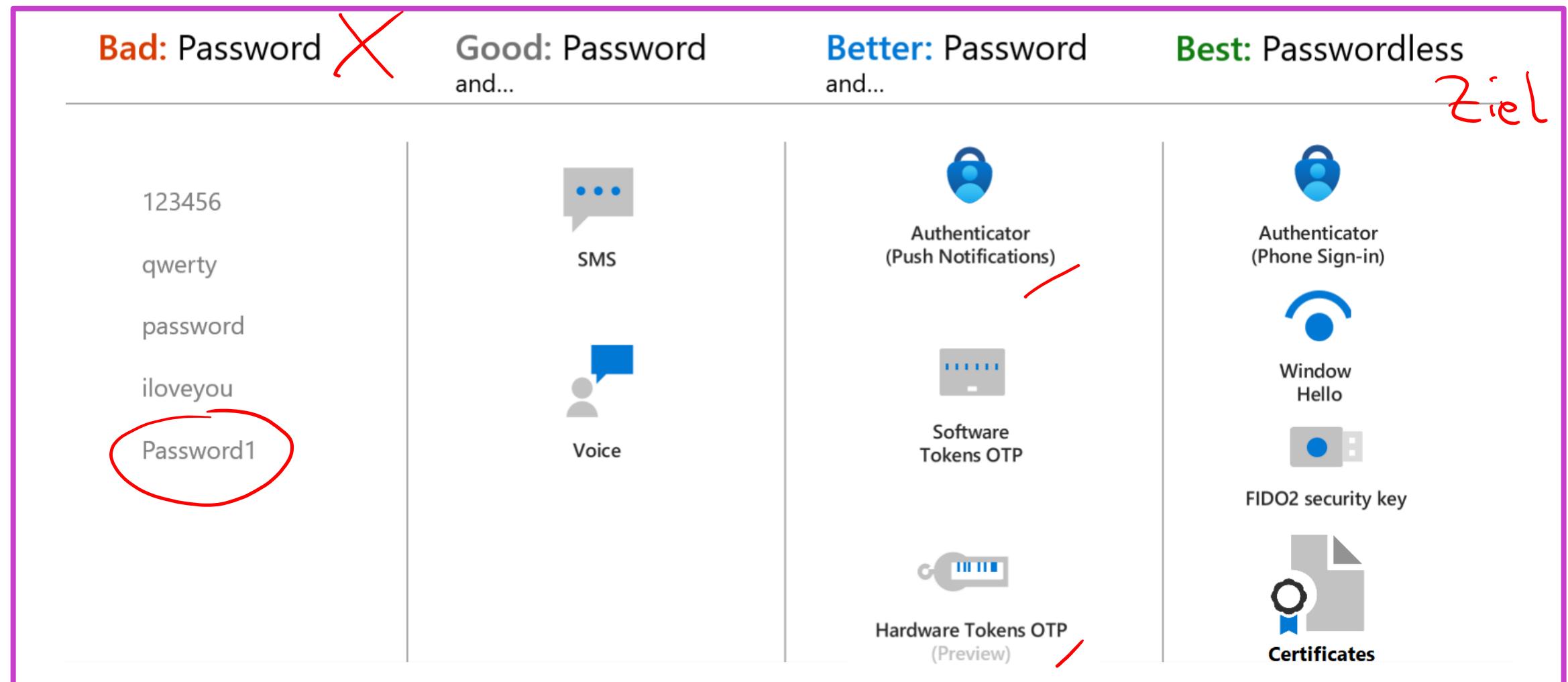
# Manage user authentication

# Objectives

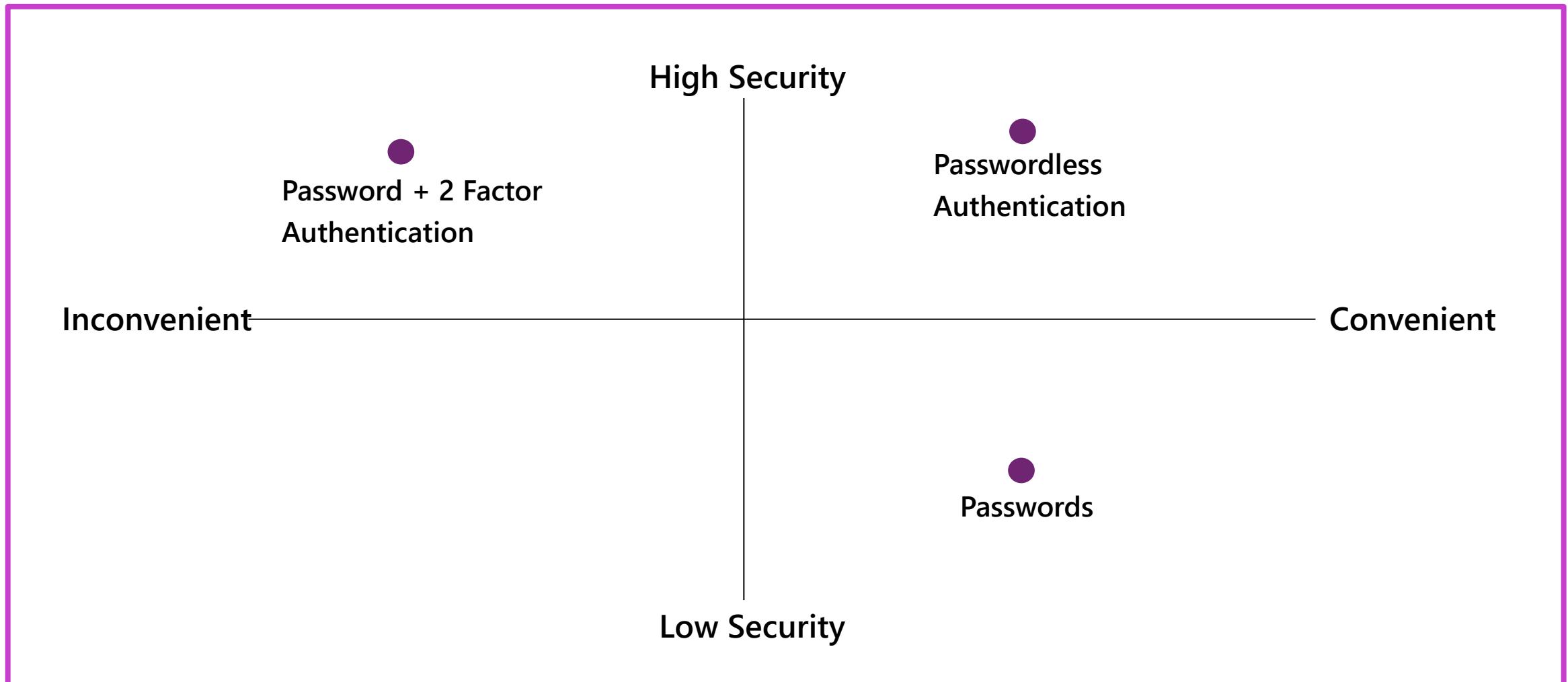
- 1** Administer authentication methods (FIDO2/Passwordless)
- 2** Implement an authentication solution based on Windows Hello for Business
- 3** Disable accounts and revoke sessions
- 4** Deploy and manage password protection
- 5** Configure smart lockout thresholds
- 6** Kerberos in Microsoft Entra ID
- 7** Certificate-based authentication
- 8** Microsoft Entra ID user authentication in Virtual Machines (VMs)

# Administer authentication methods

# Authentication methods



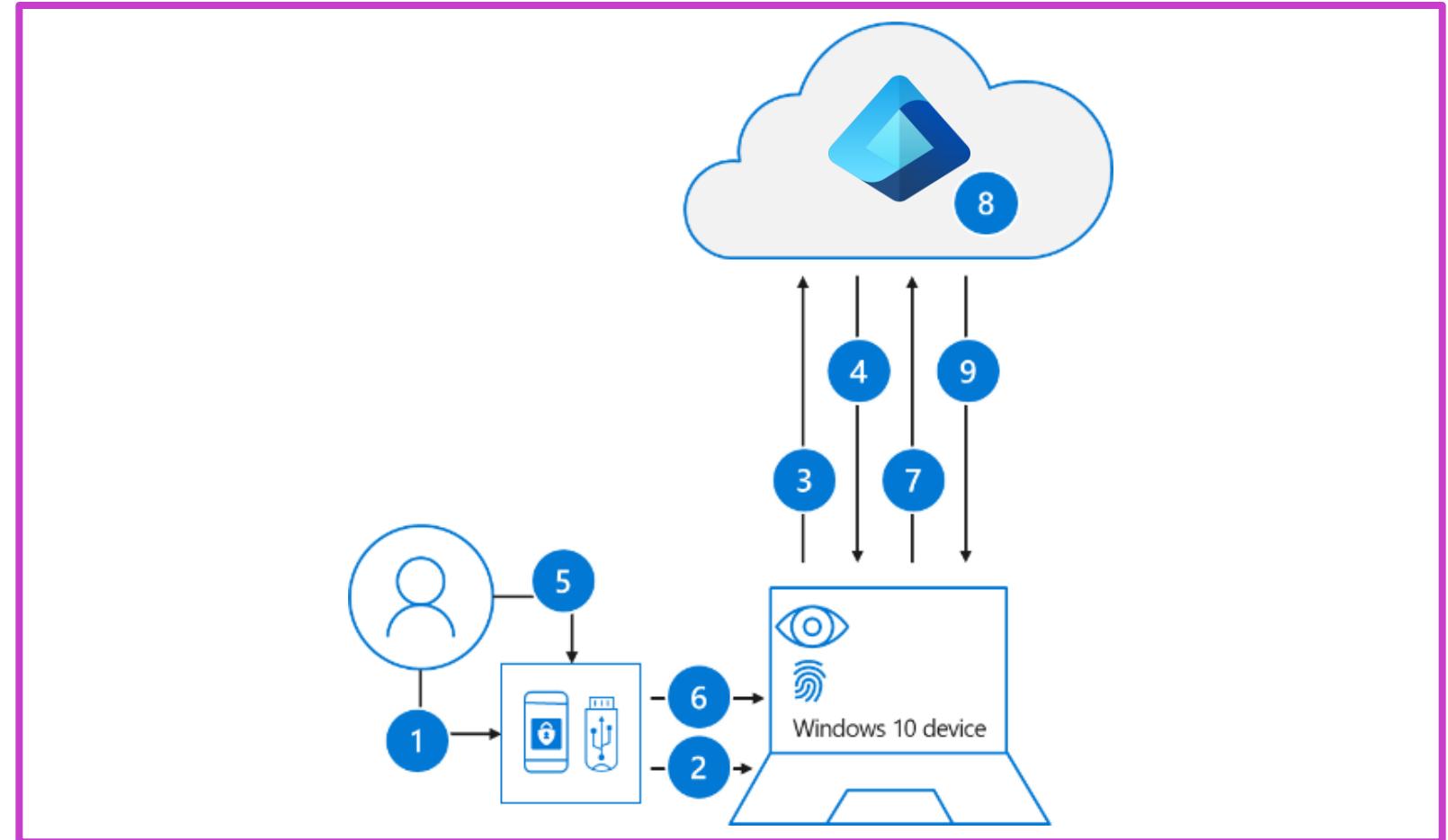
# Authentication method strength and security



TLA

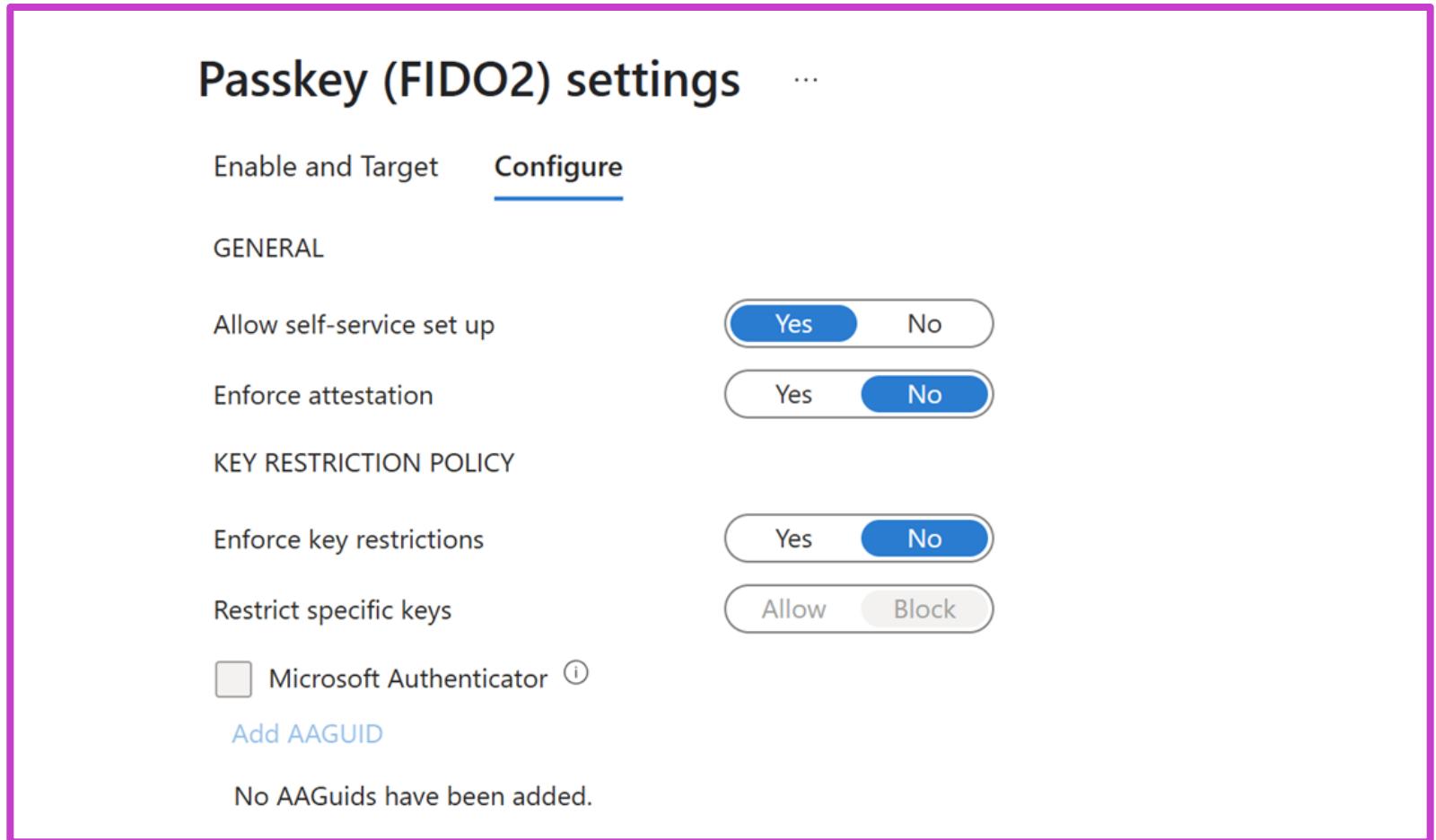
# What is FIDO2?

- FIDO2 security keys are an unphishable specification-based passwordless authentication method that can come in any form factor.
- Fast Identity Online (FIDO) is an open specification for passwordless authentication.
- FIDO allows users and organizations to leverage the specification to sign in to their resources without a username or password using an external security key or a platform key built into a device.

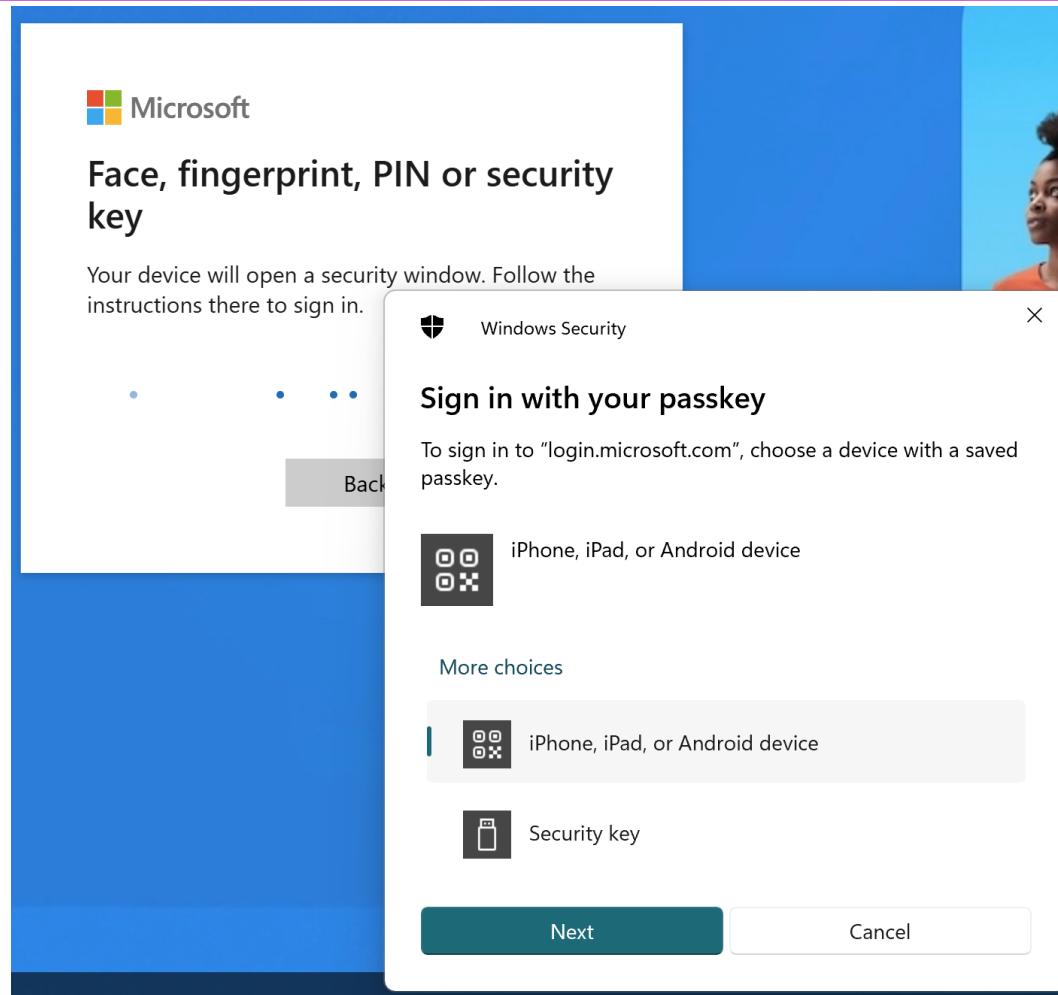


# Implement FIDO2 security keys

- **Allow self-service setup**—if set to NO, users cannot register a FIDO key.
- **Enforce attestation**—if set to YES, the FIDO key has to be published and verified with FIDO-Alliance.
- **Enforce key restrictions**—only set to YES if your organization wants to specify valid keys via AAGuids.

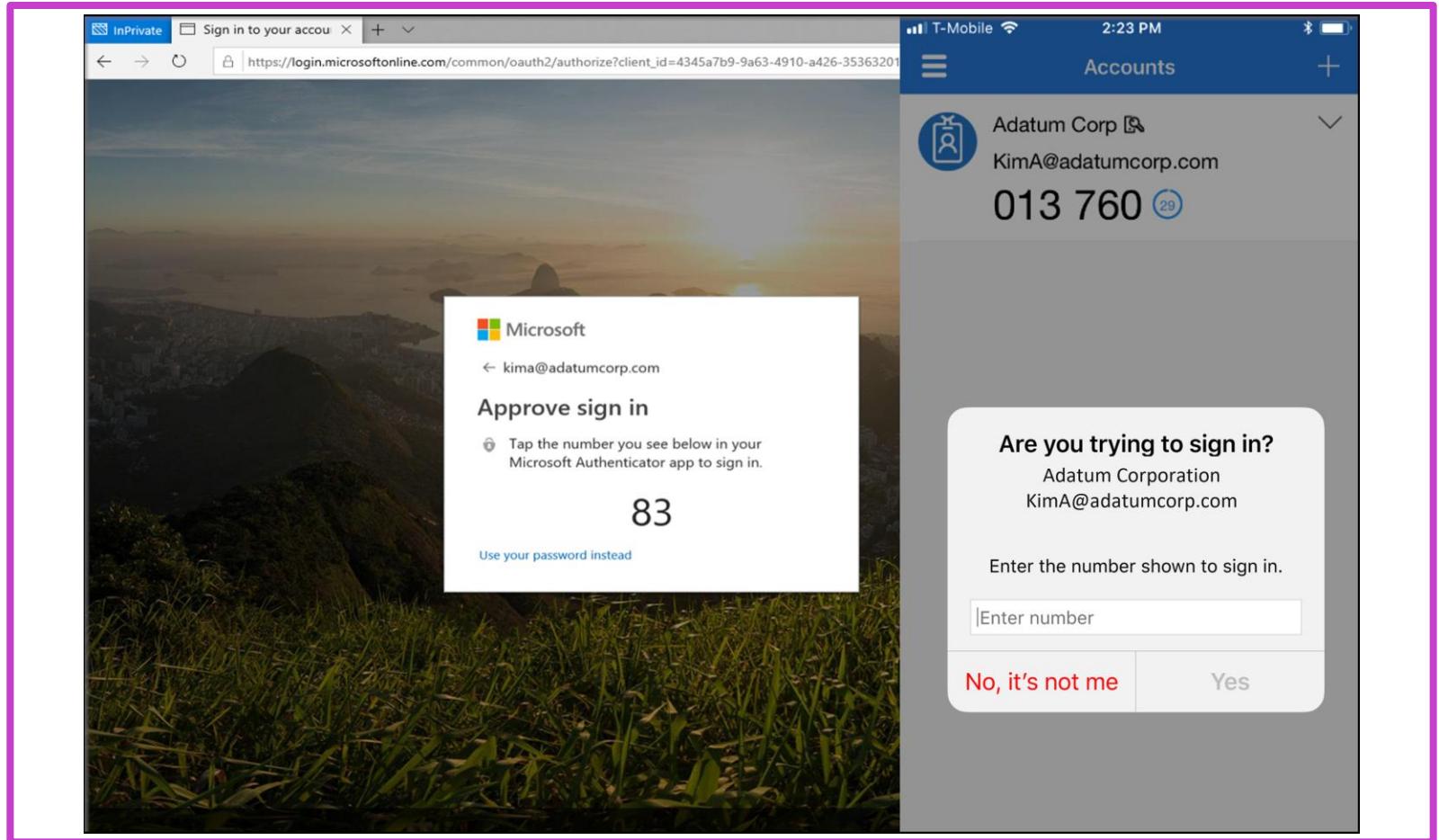


# Signing in with passwordless credential



# Microsoft Authenticator

- Approve through mobile app – Use a pin and or verify a number
- Generate an OATH verification code – One-time code entered into sign-in UI
- Enforce with policy and governance



# OATH tokens

 Multifactor authentication | OATH tokens (Preview) ...

«  Upload  Download  Delete  Refresh |  Documentation |  Columns |  Got feedback?

 Getting started  
 Diagnose and solve problems

**Settings**

 OATH tokens (Preview)

 Phone call settings

**Troubleshooting + Support**

 New support request

To get started, select the Upload button above and choose a .csv file. This file should contain the secret keys for the OATH tokens' manufacturer, model".  
For more information on available authentication and verification methods, view the public documentation.

Username  
Enter a user name

Show  
All

Name	Username	Serial Number	Model
No results			

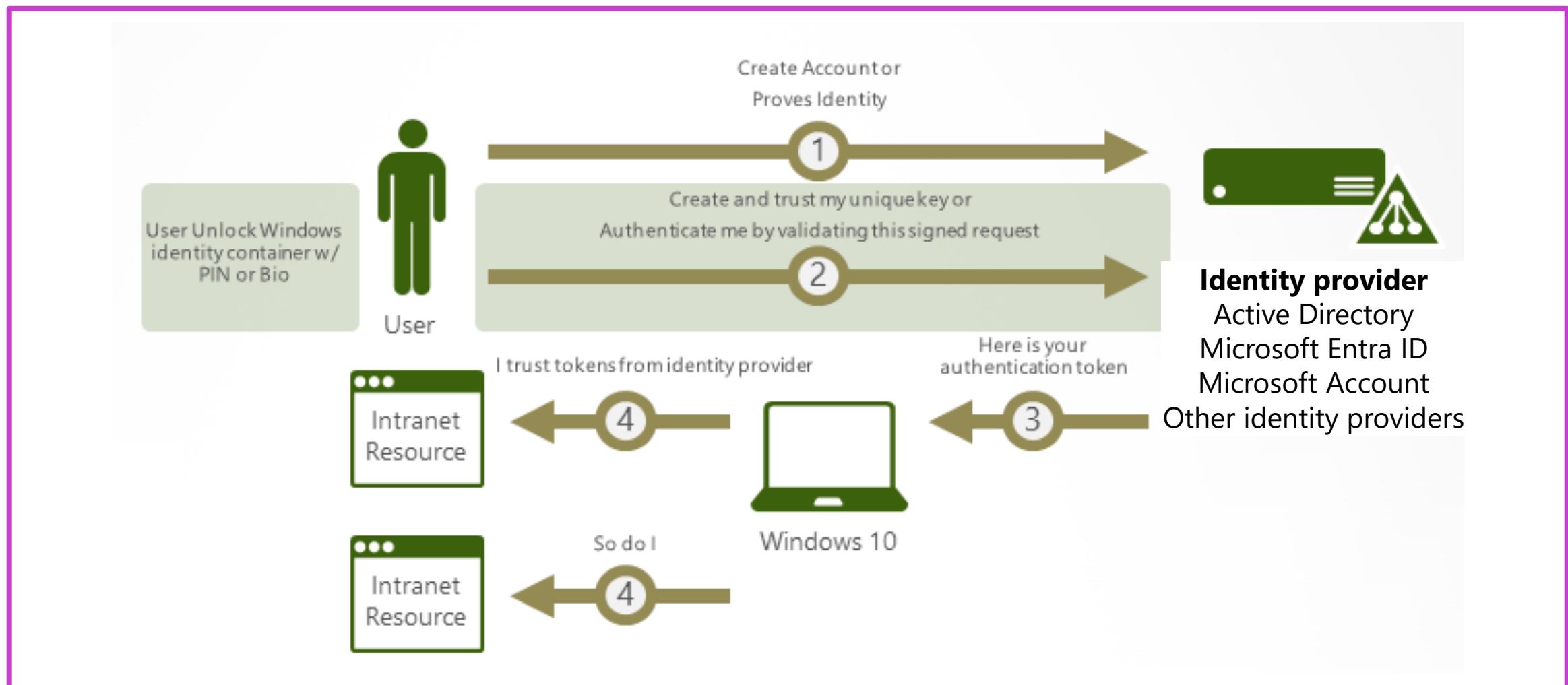
OATH—Open Authentication

TOTP—Time-based One Time Password

Software or hardware implementations available in Microsoft Entra ID

# Implement an authentication solution based on Windows Hello for Business

# Authentication in Windows Hello



# Windows Hello for Business—key points

## Key points

Credentials are based on certificate or asymmetrical key pair.

Credentials can be bound to the device, and the token that is obtained using the credential is also bound to the device.

Identity providers (such as Microsoft Entra ID, or a Microsoft account) validate user identity and maps the Windows Hello public key to a user account.

Keys can be generated in hardware (TPM 1.2 or 2.0 for enterprises, and TPM 2.0 for consumers) or software.

Two-factor authentication with the combination of a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (biometrics).

The private key never leaves a device when using TPM.

Personal (Microsoft account) and corporate (Active Directory or Microsoft Entra ID) accounts use a single container for keys.

# Disable accounts and revoke user sessions

# Describe how to disable accounts and revoke user sessions

There are occasions when you need to disable an account and/or revoke an existing user session.

- **Access tokens and refresh token**
  - When a user authenticates, they are issued an access token (Valid for one hour) and Refresh tokens.

Primary steps that you need to take:

- 1) Disable the account.
- 2) Reset the password.
- 3) Disable any devices, tokens, or other references.

# Disable accounts: On-premises and Microsoft Entra users

## Disabling and revoking access (PowerShell)

- **On-premises user**
  - Disable account → `Disable-ADAccount -Identity johndoe`
  - Reset password → `Set-ADAccountPassword -Identity johndoe -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "p@ssw0rd1" -Force)`
  - Recommended to run password reset twice to avoid pass-the-hash style attacks
- **Microsoft Entra user**
  - Disable account → `Set-AzureADUser -ObjectId johndoe@contoso.com -AccountEnabled $false`
  - Revoke refresh token → `Revoke-AzureADUserAllRefreshToken -ObjectId johndoe@contoso.com`
  - Disable user devices → `Get-AzureADUserRegisteredDevice -ObjectId johndoe@contoso.com | Set-AzureADDevice -AccountEnabled $false`

# Deploy and manage password protection

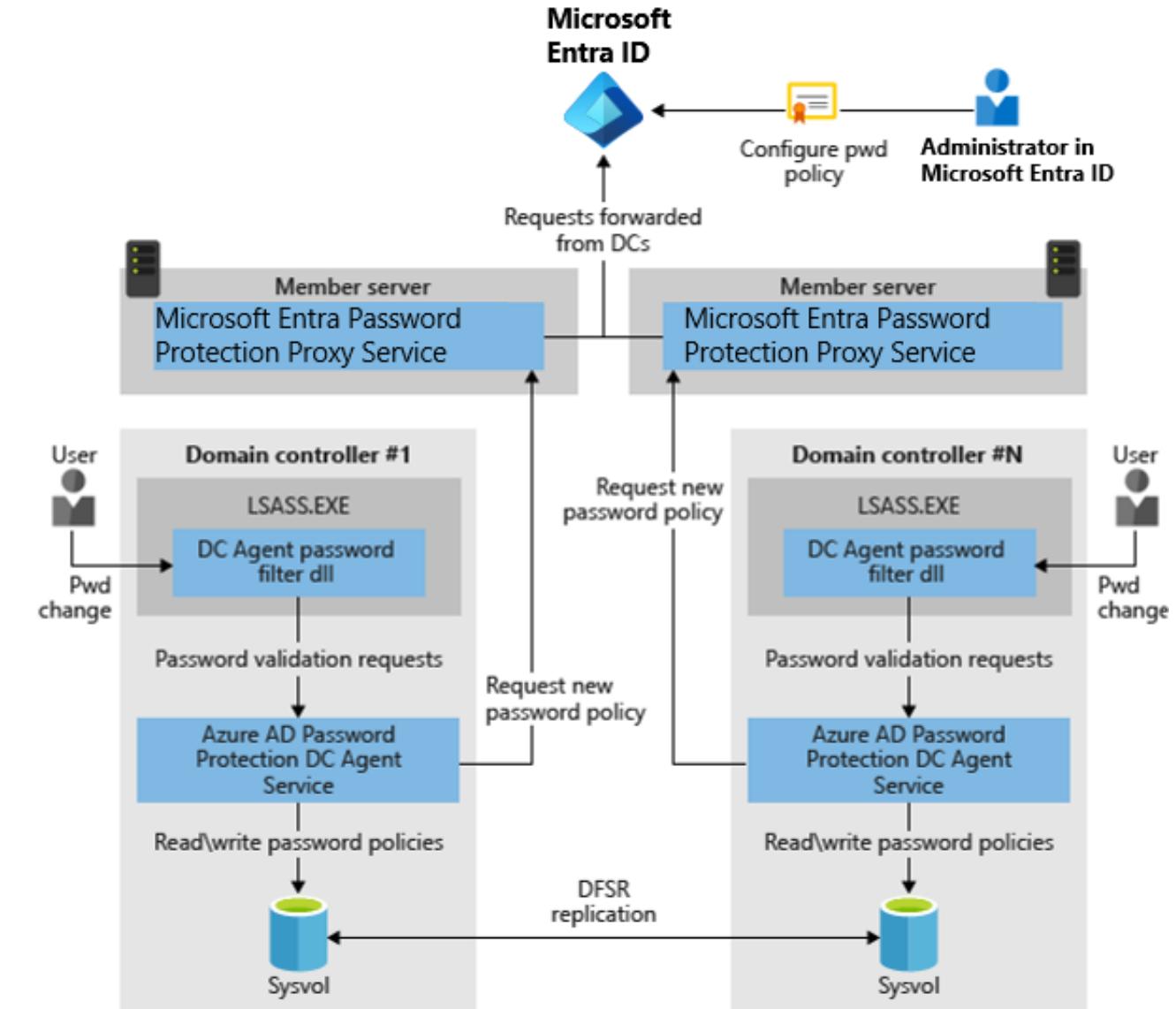
# Microsoft Entra password protection

Users often create easy to guess passwords that are weak against dictionary-based attacks. To help you enforce strong passwords, Microsoft Entra password protection provides a global and custom banned password list. Benefits include:

- Domain controllers (DCs) never have to communicate directly with the internet.
- No new network ports.
- No AD DS schema changes required.
- No minimum AD DS domain or forest functional level (DFL/FFL) required.
- The software doesn't create or require accounts in the AD DS domains that it protects.
- User clear-text passwords never leave the DC.
- The software isn't dependent on other Microsoft Entra features.
- Incremental deployment is supported.

# Deployment technology

How the basic components of Microsoft Entra password protection are configured and work together



# Deployment approach

## Strategy for rolling out password protection—don't just turn it on

### Audit mode

Audit mode is the default initial setting, where passwords can continue to be set. Passwords that would be blocked are recorded in the event log. After you deploy the proxy servers and DC agents in audit mode, monitor the impact that the password policy will have on users when the policy is enforced.

### Common findings

During the audit stage, many organizations find:

- They need to improve existing operational processes to use more secure passwords.
- Users often use unsecure passwords.
- Organizations need to inform users about the upcoming change in security enforcement, the possible impact on them, and how to choose more secure passwords.

# Considerations

- Multiple forest considerations
- Read-only domain controller considerations
- High availability considerations

# Configure smart lockout thresholds

# How smart lockout works

- By default, smart lockout locks the account for one minute after 10 failed attempts
- The account is locked again after subsequent attempts, for increasing periods
- Smart lockout is always on for all Microsoft Entra ID customers
- The default configuration can be customized
- Smart lockout doesn't guarantee that a genuine user is never locked out, but it is tailored to resisting bad actors
- Smart lockout can be integrated with hybrid deployments

# Exercise—manage Microsoft Entra smart lockout values

This exercise teaches students to customize the Microsoft Entra smart lockout values.

[Launch this Exercise in GitHub](#)



Home > Authentication methods

## Authentication methods | Password protection

Microsoft Entra ID Security

Search Save Discard Got feedback?

Manage

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

**Custom smart lockout**

Lockout threshold  10

Lockout duration in seconds  60

**Custom banned passwords**

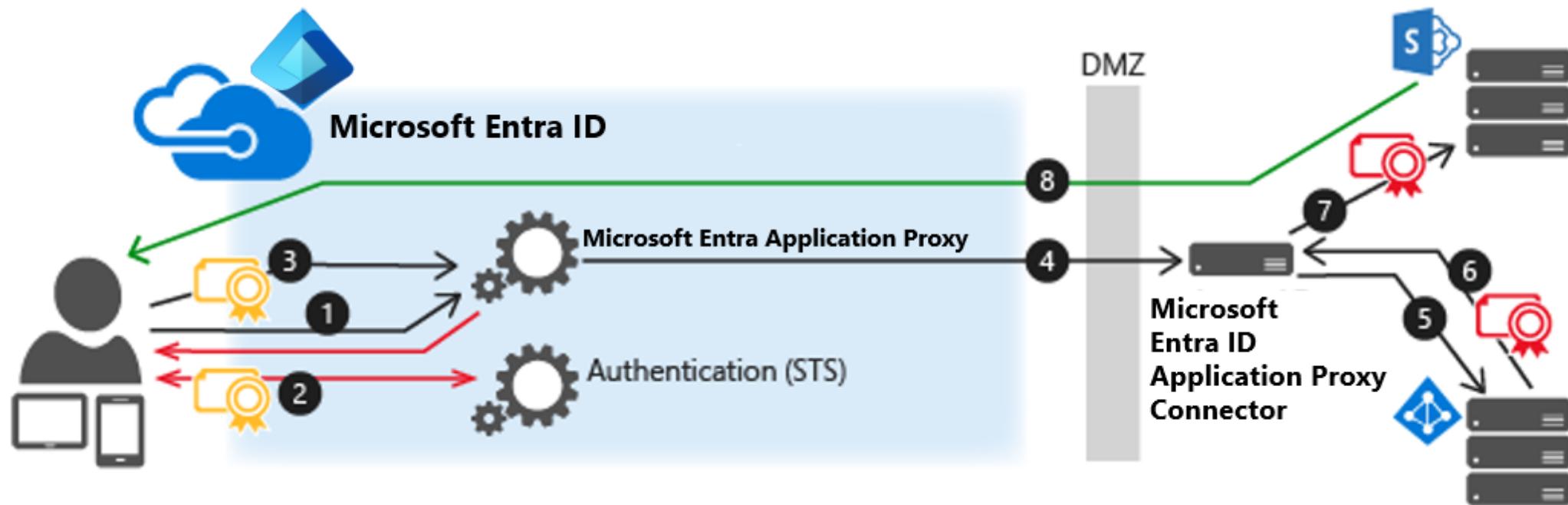
Enforce custom list  Yes  No

Custom banned password list

© Copyright Microsoft Corporation. All rights reserved.

# Kerberos in Microsoft Entra ID

# Configure Kerberos for use in Microsoft Entra ID



Environment setup needed:

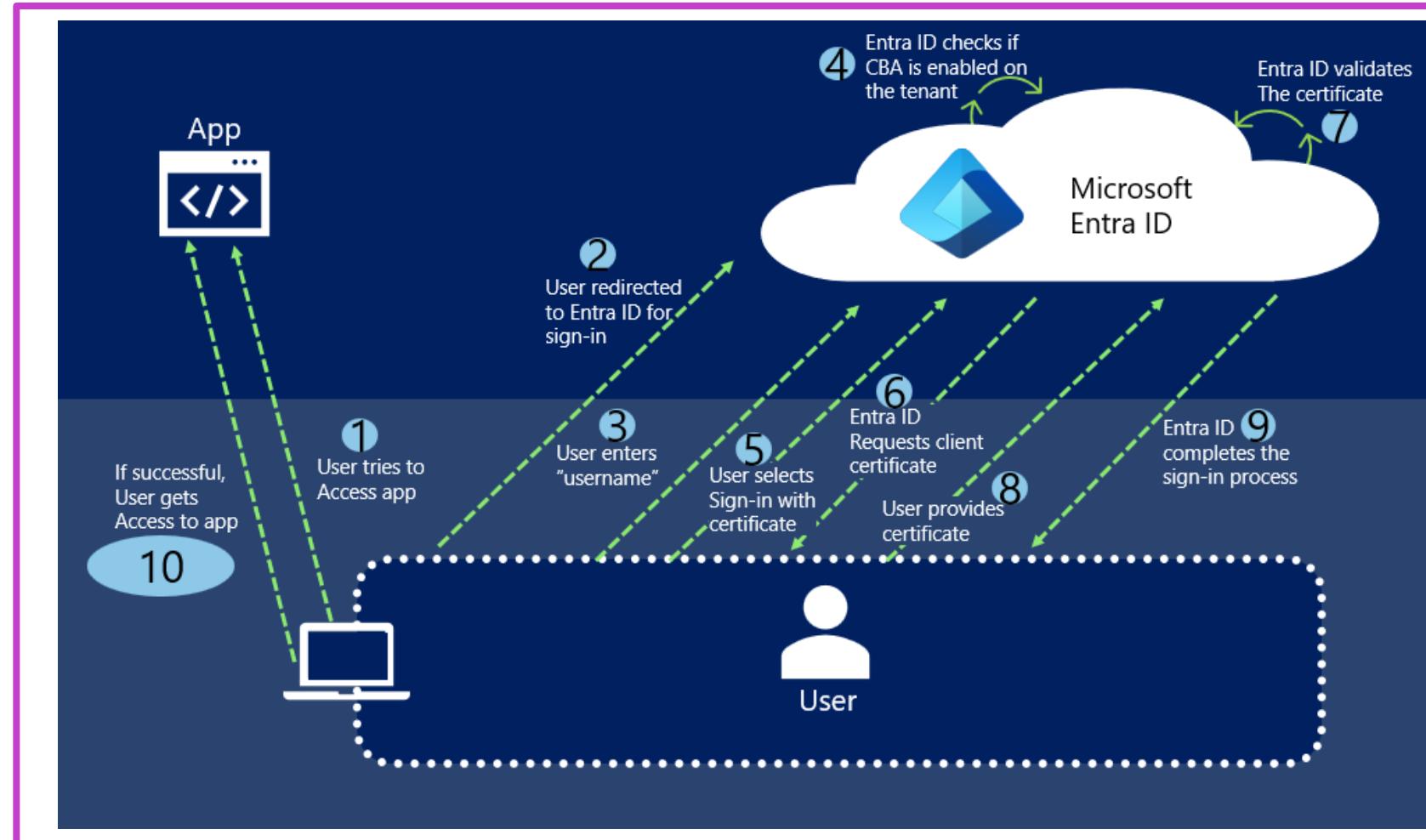
- Integrated Windows Authentication enabled on web apps
- All apps must have a service principal
- Server running the Kerberos connector must be in domain joined

# Certificate-based authentication

# Implement certificate-based authentication in Microsoft Entra ID

The following scenarios are supported:

- User sign-ins to web browser-based applications on all platforms.
- User sign-ins on mobile native browsers.
- Support for granular authentication rules for multifactor authentication by using the certificate issuer **Subject** and **policy OIDs**.
- Configuring certificate-to-user account bindings by using the certificate Subject Alternate Name (SAN) principal name and SAN RFC822 name.



# Enable certificate-based authentication

## Certificate-based authentication settings

Certificate-based authentication is a passwordless, phising-resistant authentication method that uses a certificate to verify user identity.

**Enable and Target** [Configure](#)

Enable

**Include** [Exclude](#)

Target  All users  Select groups

Name  
All users

## Certificate-based authentication settings

Certificate-based authentication is a passwordless, phising-resistant authentication method that uses a certificate to verify user identity.

[Enable and Target](#) [Configure](#)

**Certificate revocation list (CRL) validation**

This setting requires a CRL check for every certificate authority (CA). If the CRL distribution point is not found, the certificate is rejected.

Require CRL validation (recommended)

**Issuer Hints**

Enable issuer hints to show only the valid certificates in the certificate picker during authentication.

Issuer Hints

**Authentication binding**

The authentication binding policy helps determine the strength of your certificate-based authentication.

Protection Level [\(i\)](#)  Single-factor authentication  Multi-factor authentication

Required Affinity Binding [\(i\)](#)  Low  High

[+ Add rule](#)

Certificate issuer Policy OID

# Microsoft Entra ID user authentication for VMs

# Benefits of Microsoft Entra ID user authentication in VMs

## Benefits:

- Use Microsoft Entra credentials to sign in to Windows VMs in Azure.
- Reduce reliance on local administrator accounts.
- Password complexity and password lifetime policies configured for your Microsoft Entra ID.
- Configure Conditional Access policies to require multifactor authentication and other signals such as risky user or sign-in risk.

## Supported operation systems:

- Windows Server 2019 Datacenter edition and later.
- Windows 10 1809 and later.
- Windows 11.
- Linux virtual machine.

# Configure Windows VMs

## Identity

Enable system assigned managed identity  ⓘ



ⓘ System managed identity must be on to login with Microsoft Entra ID credentials. [Learn more ↗](#)

## Microsoft Entra ID

Login with Microsoft Entra ID  ⓘ



ⓘ RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Microsoft Entra ID login. [Learn more ↗](#)

To use Microsoft Entra sign-in for Windows VM in Azure, you must:

- First enable the Microsoft Entra sign-in option for your Windows VM.
- Then configure Azure role assignments for users who are authorized to sign into the VM.

# Configure Microsoft Entra ID sign-in for Linux VMs

You can enable Microsoft Entra ID sign-in for any of the supported Linux distributions mentioned using the Azure portal. As an example, to create an Ubuntu Server 22.04 Long Term Support (LTS) VM in Azure with Microsoft Entra ID authentication:

1. Sign into the Azure portal, with an account that has access to create VMs, and select **+ Create** a resource.
2. Select **Create** under Ubuntu Server 18.04 LTS in the Popular view.
3. On the **Management** tab, Check the box to enable **Login with Microsoft Entra ID**.
4. Ensure **System assigned managed identity** is checked.
5. Complete the Linux virtual machine setup.

# References (1 of 2)

**Enable combined security information registration in Microsoft Entra ID**

<https://learn.microsoft.com/azure/active-directory/authentication/howto-registration-mfa-sspr-combined>

**Create a resilient access control management strategy with Microsoft Entra ID**

<https://learn.microsoft.com/azure/active-directory/authentication/concept-resilient-controls>

**Microsoft Entra authentication methods API overview**

<https://learn.microsoft.com/graph/api/resources/authenticationmethods-overview>

**Windows Hello for Business overview**

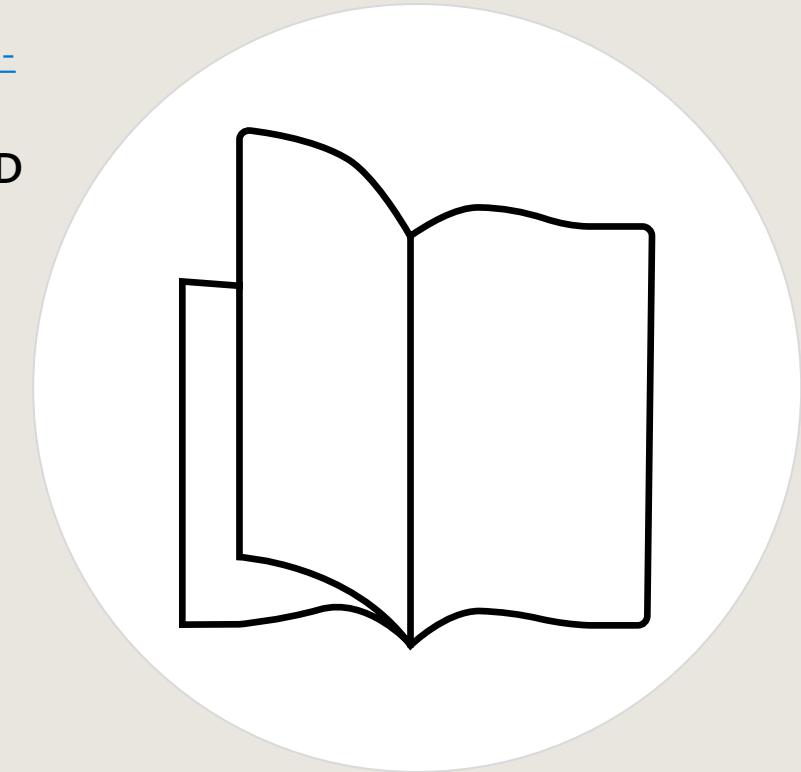
<https://learn.microsoft.com/windows/security/identity-protection/hello-for-business/hello-overview>

**Authentication methods in Microsoft Entra ID—Microsoft Authenticator app**

<https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-authenticator-app>

**Passwordless authentication options for Microsoft Entra ID**

<https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-passwordless>



# References (2 of 2)

**Authentication methods in Microsoft Entra ID—OATH tokens**

<https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-oath-tokens>

**Configure and enable users for SMS-based authentication using Microsoft Entra ID**

<https://learn.microsoft.com/azure/active-directory/authentication/howto-authentication-sms-signin>

**Authentication methods in Microsoft Entra ID—phone options**

<https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-phone-options>

**Enforce on-premises Microsoft Entra password protection for Active Directory Domain Services**

<https://learn.microsoft.com/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

**Enable on-premises Microsoft Entra password protection**

<https://learn.microsoft.com/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations>

**Step-by-step: Implementing Microsoft Entra password protection on-premises**

<https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-implementing-azure-ad-password-protection-on/ba-p/563342>



# Plan, implement, and administer Conditional Access

# Objectives

- 1 Plan and implement security defaults
- 2 Plan Conditional Access policies
- 3 Implement conditional access policy controls and assignments (targeting, applications, and conditions)
- 4 Template-based conditional access
- 5 Test and troubleshoot conditional access policies
- 6 Implement application controls and session management
- 7 Continuous Access Evaluation
- 8 Authentication context

# Explore security defaults

# Security defaults

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with a 'Favorites' section containing 'Identity' (which is highlighted with a red box), 'Overview', 'Users', 'Groups', 'Devices', 'Applications', 'Roles & admins', 'Billing', 'Settings', 'Protection', 'Identity governance', and 'External Identities'. At the top, there are links for 'Home', 'What's new', 'Diagnose & solve problems', 'Add', 'Manage tenants', 'What's new', 'Preview features', and 'Got feedback?'. Below the top navigation, tabs include 'Overview', 'Monitoring', 'Properties' (which is selected and highlighted with a red box), 'Recommendations', and 'Tutorials'. The main content area displays several configuration settings:

- Data location: United States datacenters
- Notification language: English
- Tenant ID: (empty input field)
- Technical contact: (empty input field)
- Global privacy contact: (empty input field)
- Privacy statement URL: (empty input field)
- Access management for Azure resources: Security defaults (highlighted with a red box)

Under 'Security defaults', the text reads: "Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks."

Two informational icons are present:

- An info icon: "Your organization is currently using Conditional Access policies which prevents you from enabling security defaults."
- A blue exclamation mark icon: "You can use Conditional Access to configure custom policies that enable the same behavior provided by security defaults."

# Who's it for?

## Who should use security defaults?

- Organizations that want to increase their security posture but don't know how or where to start
- Organizations utilizing the free tier of Microsoft Entra ID

## Who shouldn't use security defaults?

- Organizations currently using Conditional Access policies to bring signals together, make decisions, and enforce organizational policies
- Organizations with Microsoft Entra ID Premium licenses
- Organizations with complex security requirements that warrant using Conditional Access

# Exercise—work with security defaults



This exercise teaches the student how to enable security defaults in Microsoft Entra ID.

[Launch this Exercise in GitHub](#)

## Enable Security defaults ×

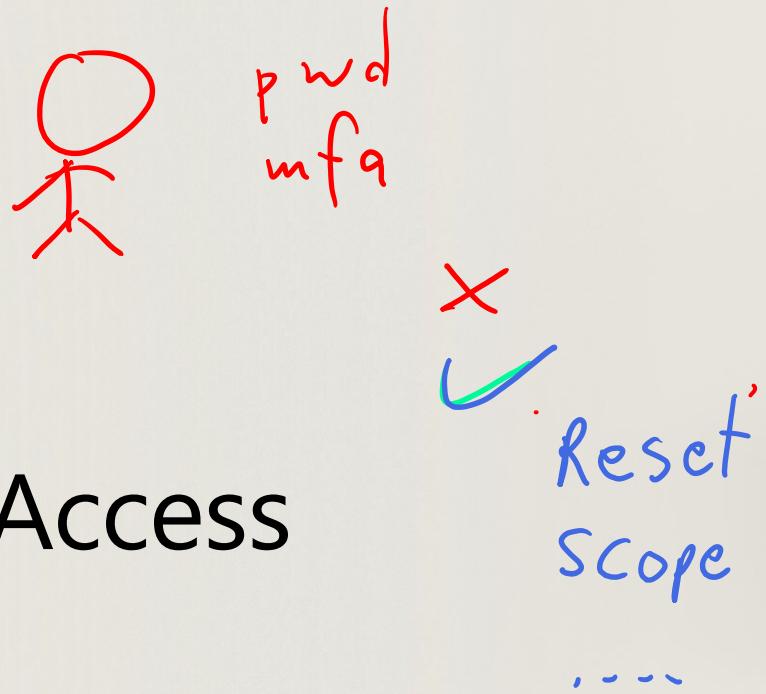
Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.

[Learn more](#)

Enable Security defaults

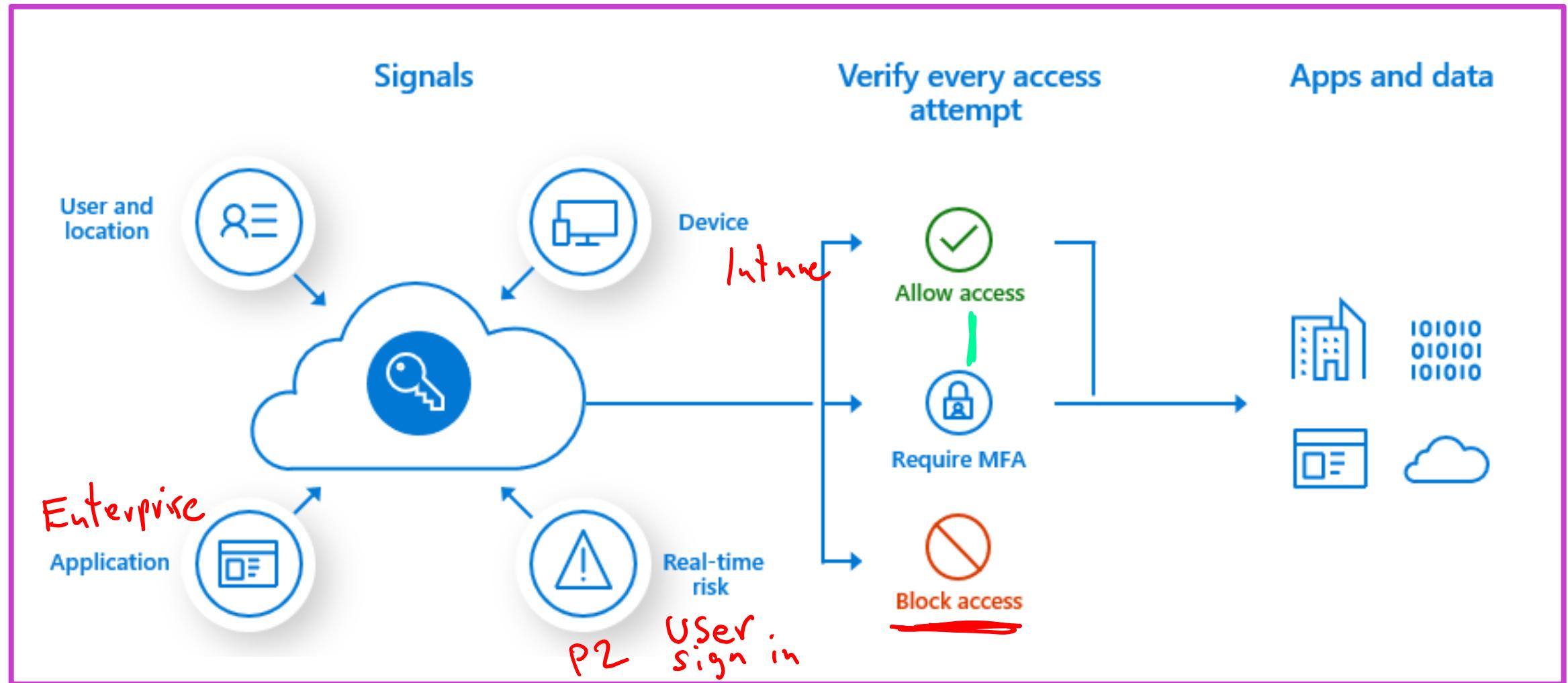
Yes No

# Plan Conditional Access policies



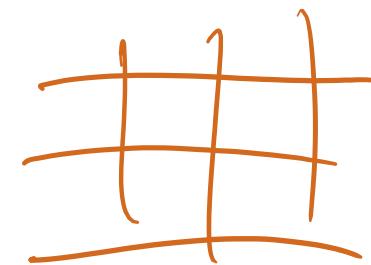
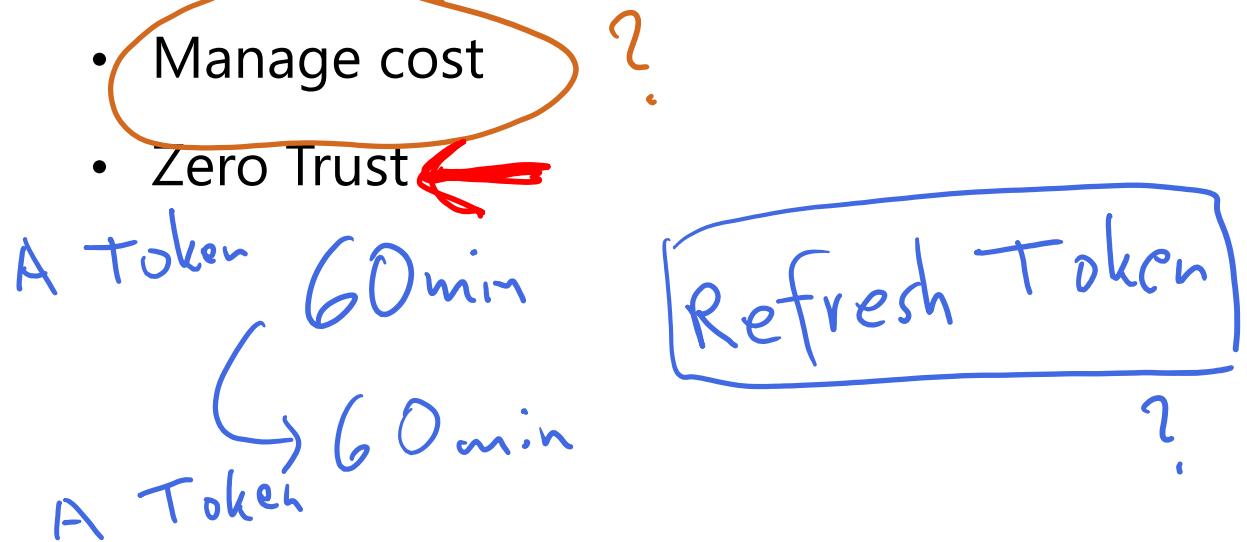
# About Conditional Access policies

P1 C E3



# Benefits of Conditional Access

- Increase productivity
- Manage risk
- Address compliance and governance
- Manage cost
- Zero Trust



m365maps.com

# Understanding Conditional Access policy components

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 \*

Example: 'Device compliance app policy'

Assignments

Users ⓘ 0 users and groups selected

Target resources ⓘ No target resources selected

Network **NEW** ⓘ Not configured

Conditions ⓘ 0 conditions selected

Access controls

Grant ⓘ 0 controls selected

Session ⓘ 0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ User risk level is the likelihood that the user account is compromised.  
Not configured

Sign-in risk ⓘ Sign-in risk level is the likelihood that the sign-in session is compromised.  
Not configured

Insider risk ⓘ Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.  
Not configured

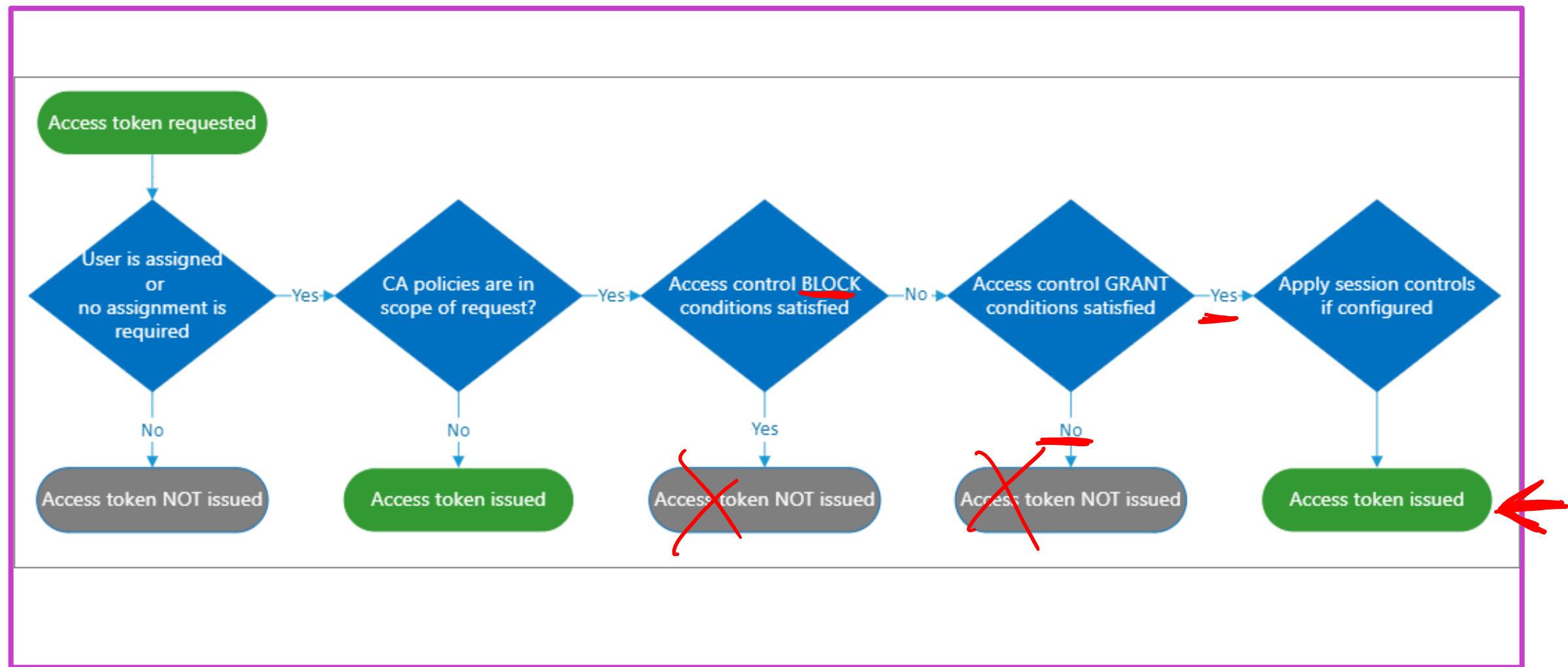
Device platforms ⓘ Not configured

Locations ⓘ Not configured

Client apps ⓘ Not configured

Filter for devices ⓘ Not configured

# Access token issuance



# Implement Conditional Access policies and assignments

# Setting up Conditional Access

The image shows two screenshots of the Microsoft Conditional Access interface. A red line connects the 'Create new policy' button on the left to the 'New Conditional Access policy' section on the right.

**Left Side: Conditional Access | Overview**

- Home >
- Conditional Access | Overview** (Microsoft Entra ID)
- Overview (highlighted)
- Policies
- Insights and reporting
- Diagnose and solve problems
- Manage
  - Named locations
  - Custom controls (Preview)
  - Terms of use
  - VPN connectivity
  - Authentication contexts
  - Authentication strengths
  - Classic policies
- Monitoring
  - Sign-in logs
  - Audit logs
- Troubleshooting + Support
  - New support request

**Right Side: New Conditional Access policy**

- Home > Conditional Access | Overview > 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 \* Example: 'Device compliance app policy'
- Select what this policy applies to: Cloud apps
- Include  Exclude
- None
- All cloud apps
- Select apps
- Edit filter (Preview)
  - None
  - Select
    - Office 365
- General Alerts
  - Named Locations**  
Microsoft Entra ID now supports IPv6! Update your Named locations with IPv6 ranges.  
[Learn more](#)
  - 0 policies have a Named Location condition
- Security Alerts (Preview)
- Enable policy
  - Report-only
  - On
  - Off
- Create

# Grant/block access controls

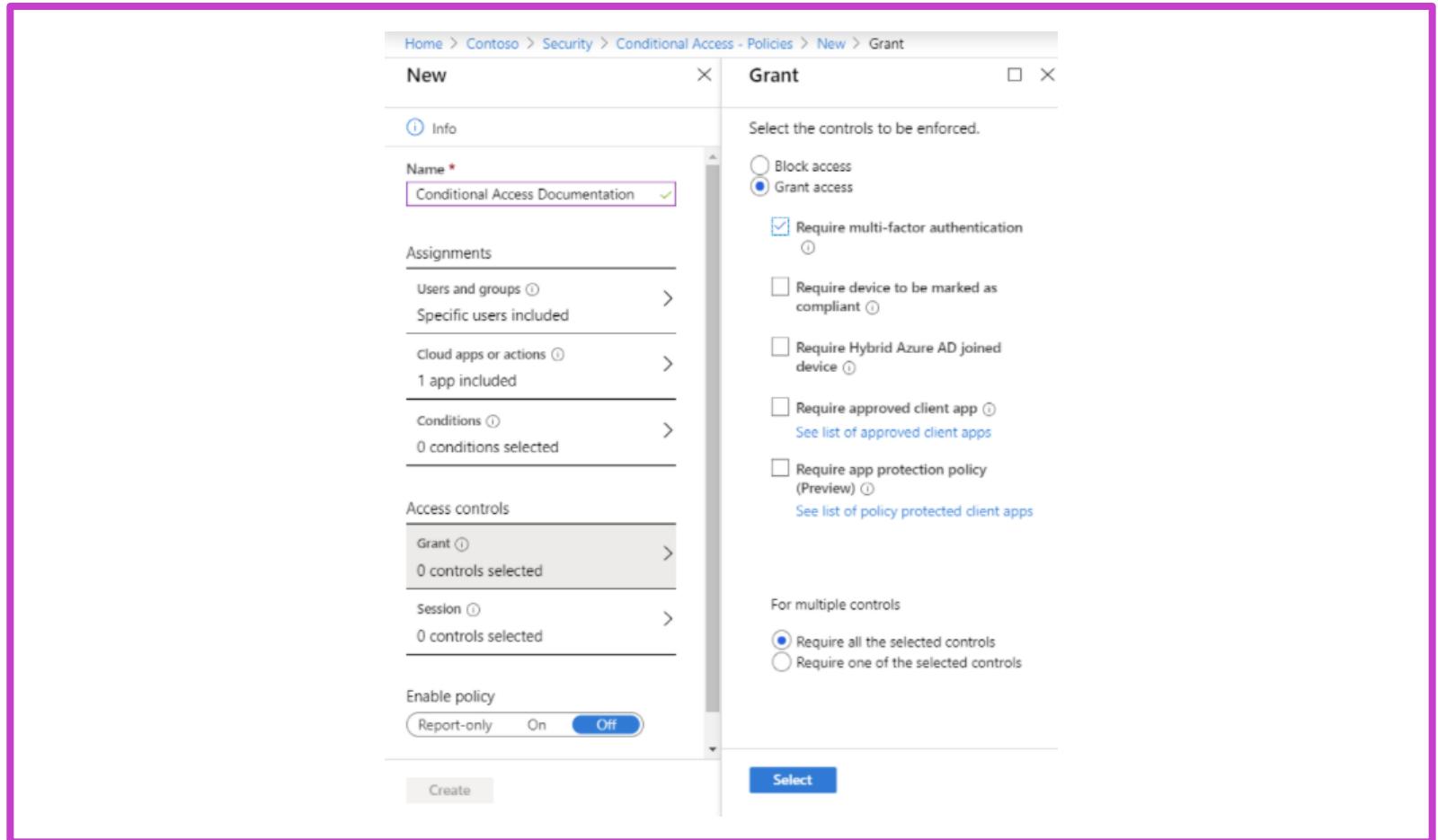
## Block access

- Use carefully or you could block your system
- Always test with What-if and Report-only mode

## Grant access

- Enforce several different controls before allowing access

**Note—require all/require one**



# Session access control

Limit the experience of the user/application within a specific cloud application.

Base the experience on specific conditions the user has met or failed to meet.

The screenshot shows the 'New Conditional Access policy' page. A red box highlights the 'Session' tab at the top right. A red circle highlights the 'Grant' radio button under 'Access controls'. A red arrow points to the 'Enable policy' section, which includes a 'Report-only' button, an 'On' switch, and an 'Off' switch. A red arrow also points to the 'Persistent browser session' option, which is crossed out with a large red X. A red arrow points to the 'Sign-in frequency' option, which is preceded by a question mark icon. A red box highlights the note: 'This option only works with Global Secure Access resources.'

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 \*

Assignments

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

Target resources [\(1\)](#)  
No target resources selected

Network [\(1\)](#)  
Not configured

Conditions [\(1\)](#)  
0 conditions selected

Access controls

Grant   
0 controls selected

Session [\(1\)](#)  
0 controls selected

Enable policy  
 Report-only  On  Off

[Create](#) [Select](#)

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

Use app enforced restrictions [\(1\)](#)

**This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. [Learn more](#)**

Use Conditional Access App Control [\(1\)](#)

Sign-in frequency [\(1\)](#) ←

Persistent browser session [\(1\)](#) X

Customize continuous access evaluation

Disable resilience defaults [\(1\)](#)

Require token protection for sign-in sessions (Preview) [\(1\)](#)

Use Global Secure Access security profile [\(1\)](#)

**This option only works with Global Secure Access resources.**

# Template-based Conditional Access

export ?.  
json

# Conditional Access templates

There are 14 policy templates available:

1. Open Microsoft admin center.
2. View the Identity menu.
3. Open the Protection section.
4. Choose Conditional Access.
5. Create new policy from template.

The screenshot displays the 'Create new policy from templates' interface. At the top, there's a search bar and navigation tabs for 'Secure foundation', 'Zero Trust', 'Remote work', 'Protect administrator', 'Emerging threats', and 'All'. Below these are four rows of policy templates:

- Require multifactor authentication for admins**: Secure privileged administrative accounts. Description: 'Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.' [Learn more](#)
- Securing security info registration**: Secure user registration for multifactor authentication. Description: 'Secure when and how users register for Azure AD multifactor authentication and self-service password reset.' [Learn more](#)
- Block legacy authentication**: Block bypass of multifactor authentication. Description: 'Block legacy authentication endpoints that can be used to bypass multifactor authentication.' [Learn more](#)
- Require multifactor authentication for Azure management**: Protect access to Azure management. Description: 'Require multifactor authentication to protect privileged access to Azure management.' [Learn more](#)
- Require compliant or hybrid Azure AD joined device or multifactor authentication for all users**: Protect company resources. Description: 'Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.' [Learn more](#)
- Require MDM-enrolled and compliant device to access cloud apps for all users (Preview)**: Require MDM enrollment and compliance. Description: 'Require devices to be enrolled in mobile device management (MDM) and be compliant for all users and devices accessing company resources. This improves data security by reducing risks of breaches, malware, and unauthorized access. Directory Synchronization Accounts are excluded for on-premise' [Learn more](#)

# Examples of Conditional Access scenarios

- Require registration from a trusted location
- Block access by location
- Require compliant devices
- Exclude access from emergency and service accounts

# Conditional Access terms of use (TOU)

## New terms of use ...

### Terms of use

Create and upload documents

Name \* ⓘ

Example: 'All users terms of use'

Terms of use document \* ⓘ

Upload required PDF



Select default language



Display name

+ Add language

Require users to expand the terms of use

On Off

Require users to consent on every device

On Off

Expire consents ⓘ

On Off

Duration before re-acceptance required  
(days) ⓘ

Example: '90'

### Conditional access

Enforce with conditional access policy  
templates \* ⓘ

Policy templates



# Exercise—implement conditional access policies, roles, and assignments



**Microsoft Entra Conditional Access** is an advanced feature of Microsoft Entra ID that allows you to specify detailed policies that control who can access your resources. This exercise teaches students how to create and test a Conditional Access policy.

[Launch this Exercise in GitHub](#)

Name **\***  
Example: 'Device compliance app policy'

Assignments

Users ⓘ  
0 users and groups selected

Target resources ⓘ  
No target resources selected

Network **NEW** ⓘ  
Not configured

Conditions ⓘ  
0 conditions selected

# Test and troubleshoot Conditional Access policies

# Configurations to avoid

## For all users, all cloud apps:

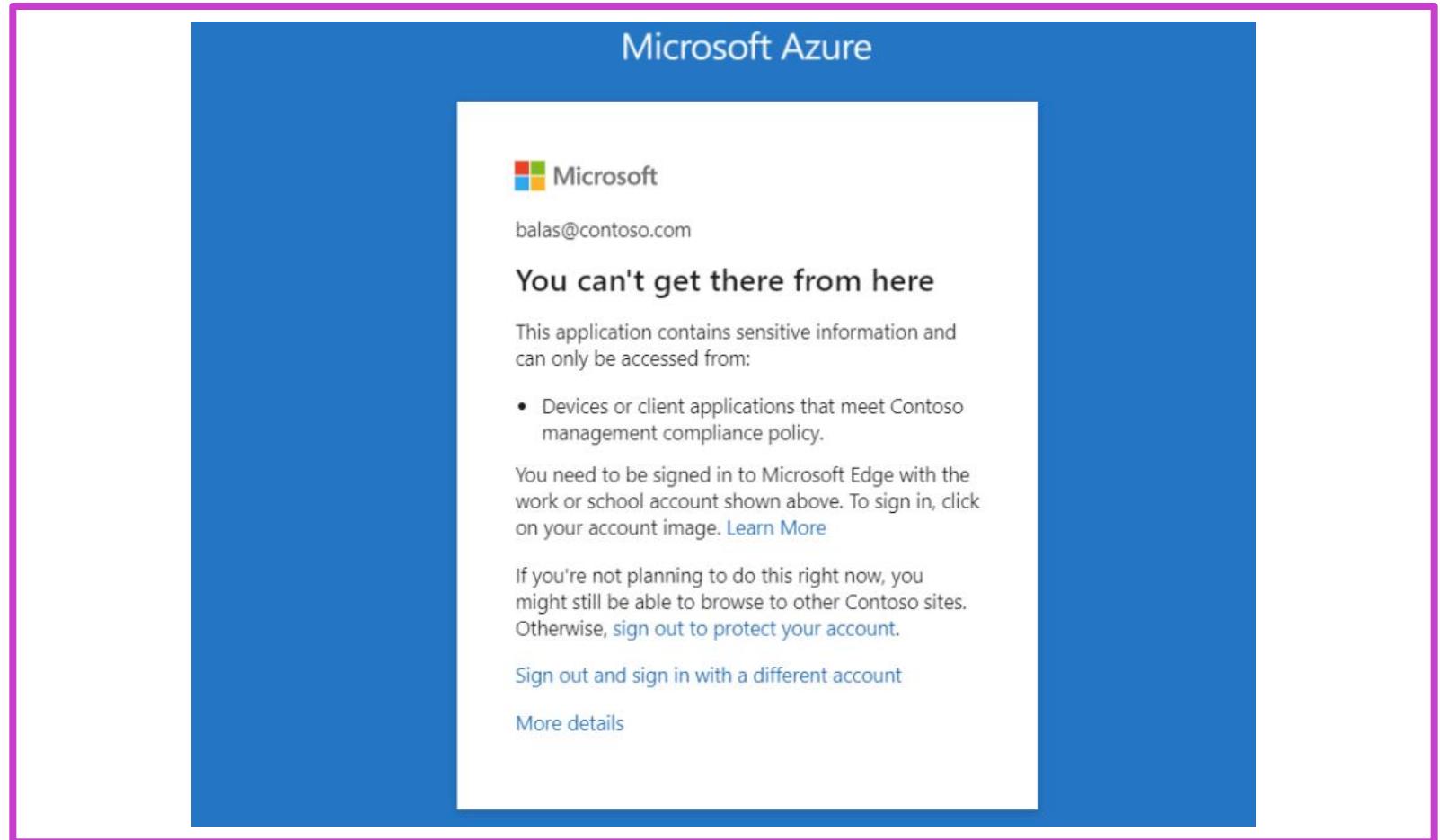
- Block access
- Require device to be marked as compliant
- Require Hybrid Microsoft Entra ID domain-joined device
- Require app protection policy

## For all users, all cloud apps, all platforms:

- Block access

# Troubleshooting sign-in interrupts

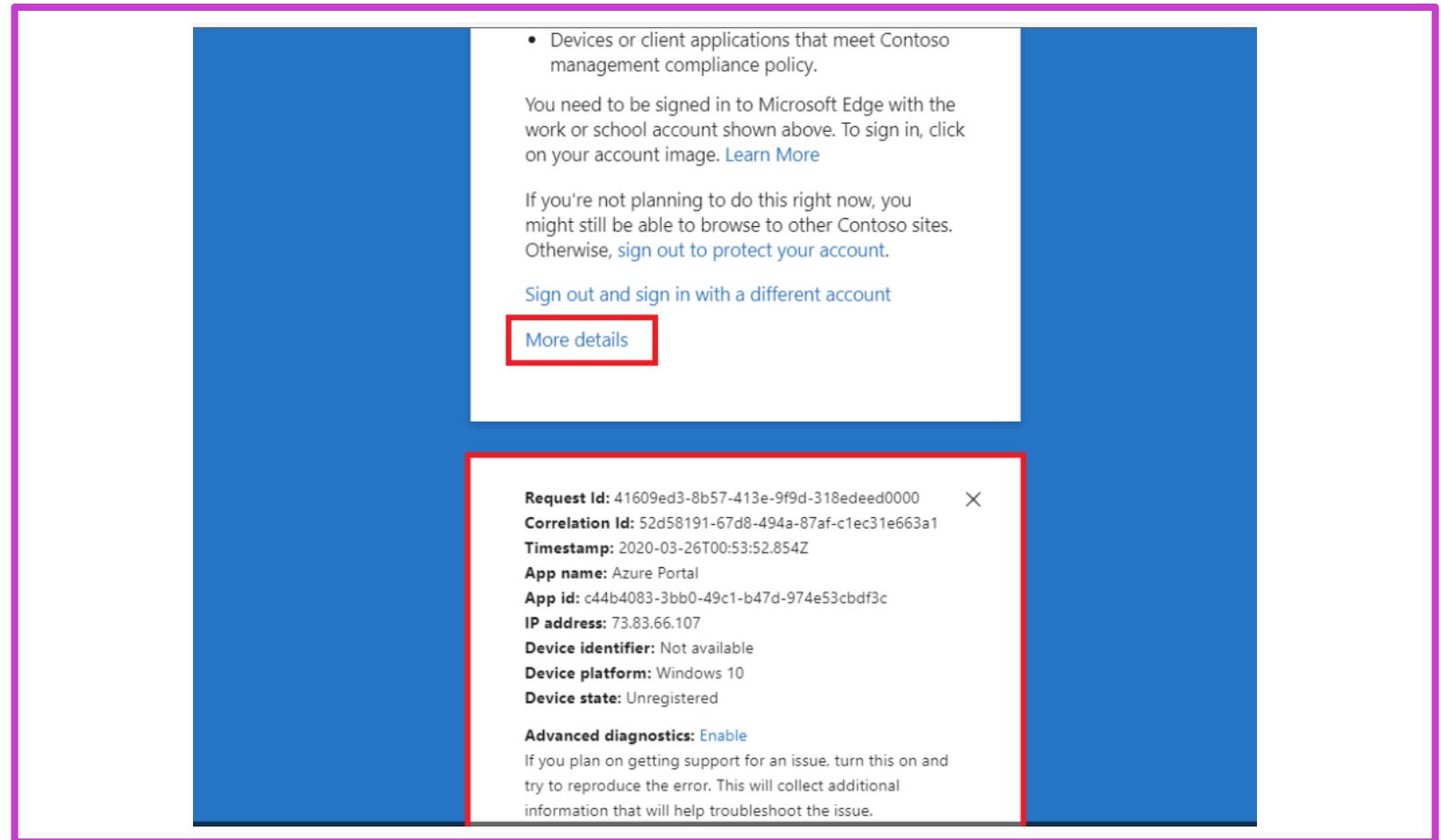
In this error, the message states that the application can only be accessed from devices or client applications that meet the company's mobile device management policy. In this case, the application and device do not meet that policy.



# Troubleshooting directory sign-in events

Find more information about the problem by clicking **More Details** in the initial error page.

Clicking **More Details** will reveal troubleshooting information that is helpful when searching the Microsoft Entra sign-in events for the specific failure event the user saw, or when opening a support incident with Microsoft.



# Implement application controls

# Conditional Access App Control

- Block download, cut, copy and print
- Enforce document labeling with Azure Information Protection
- Prevent file uploads
- Monitor/log sessions for compliance
- Block app access based on risk factors

The screenshot shows the 'New Conditional Access policy' page. Under the 'Session' tab, there are several options:

- Use app enforced restrictions
- Use Conditional Access App Control (highlighted with a red box)
- Sign-in frequency
- Persistent browser session
- Customize continuous access evaluation
- Disable resilience defaults
- Require token protection for sign-in sessions (Preview)

Handwritten annotations include:

- A large yellow bracket on the right labeled "Security Copilot" spans multiple sections.
- A red bracket labeled "Security Portal" covers the "Session" and "Access controls" tabs.
- A red bracket labeled "SIEA" points to the "Session" tab.
- Red arrows point from the bottom labels "Defender Cloud", "Def EP", and "Def User" up towards the "Session" tab.
- A large red bracket at the bottom points to the text "CA-App Control works with Microsoft Defender for Cloud Apps".

Text at the bottom of the slide:

CA-App Control works with Microsoft Defender for Cloud Apps

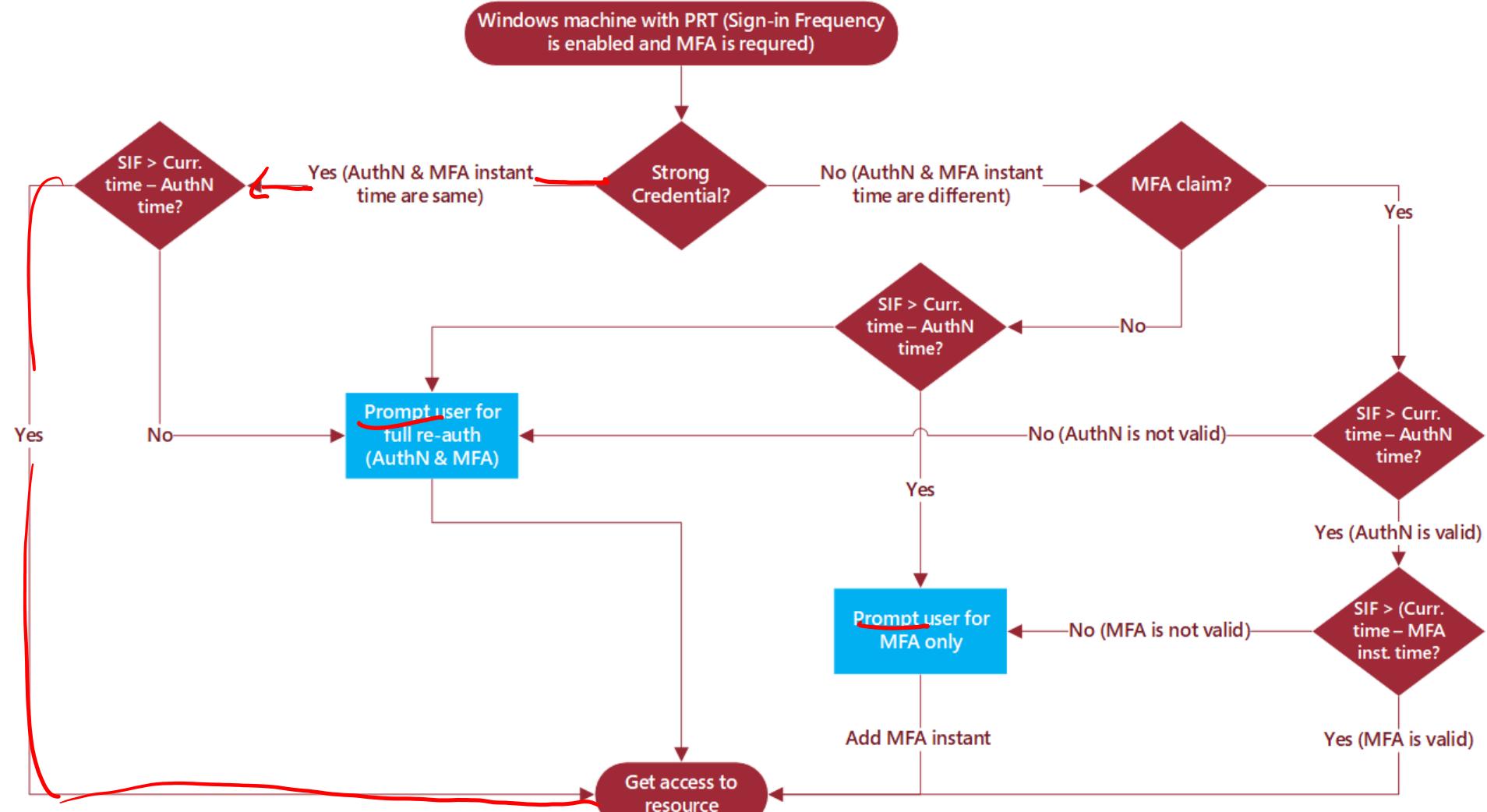
© Copyright Microsoft Corporation. All rights reserved.

# Benefits of using app protection policies (MDM/MAM)

- Protecting your company data at the app level
- End-user productivity isn't affected, and policies don't apply when using the app in a personal context
- App protection policies ensure that the app-layer protections are in place
- MDM, in addition to MAM, ensures that the device is protected

# Implement session management

# User sign-in frequency and multifactor authentication



# Validation

## Use the What If tool:

- Simulate a login from the user to the target application
- Select other conditions based on how you configured your policy.

The authentication session management controls show up in the result of the tool.

**What If** ...

Policies

[Info](#) | [Got feedback?](#)

Test the impact of Conditional Access on a user when signing in under certain conditions. [Learn more](#)

User or Workload identity [i](#)  
Patti Fernandez

Cloud apps, actions, or authentication context [i](#)  
1 app selected

IP address [i](#)  
Enter IP address (ex: 40.77.182.32)

Country [i](#)  
Select country...

Device platform [i](#)  
Select device platform...

Client apps [i](#)  
Select a client app...

Device state (deprecated) [i](#)  
Select device state...

Sign-in risk [i](#)  
Select sign-in risk...

User risk [i](#)  
Select user risk...

Service principal risk [i](#)  
Select service principal risk...

Select what this policy applies to

Any cloud app

Select apps

Select

[Microsoft Admin Portals \(Preview\)](#)

 Microsoft Admin Portals (Preview... [\\*\\*\\*](#)

# Exercise—configure authentication session controls

This exercise teaches the student to configure sign-in frequency controls using a conditional access policy.

[Launch this Exercise in GitHub](#)



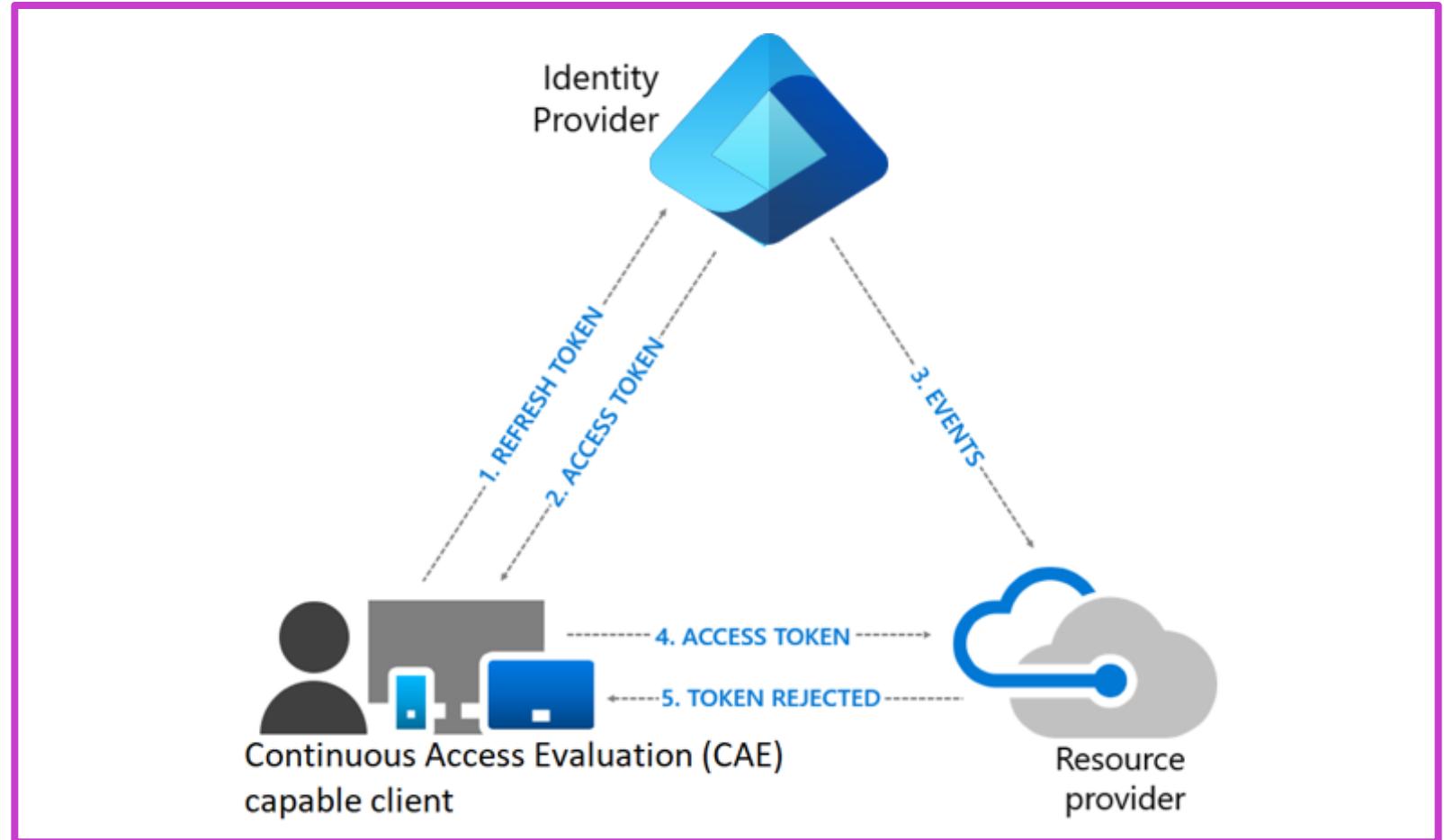
The screenshot shows the Conditional Access | Overview page in the Microsoft Entra ID portal. The page has a navigation bar with links for Overview, Policies, Insights and reporting, Diagnose and solve problems, Getting started, Coverage, Monitoring (Preview), and Tutorials. The Overview tab is selected. Below the navigation is a Policy Summary section with a Policy Snapshot card showing 5 Enabled, 1 Report-only, and 0 Off policies, and a link to View all policies. To the right is a Users section showing 2 users signed in during the last 7 days without any policy coverage, with a link to See all unprotected sign-ins.

# Continuous access evaluation

# Continuous access evaluation

## Benefits

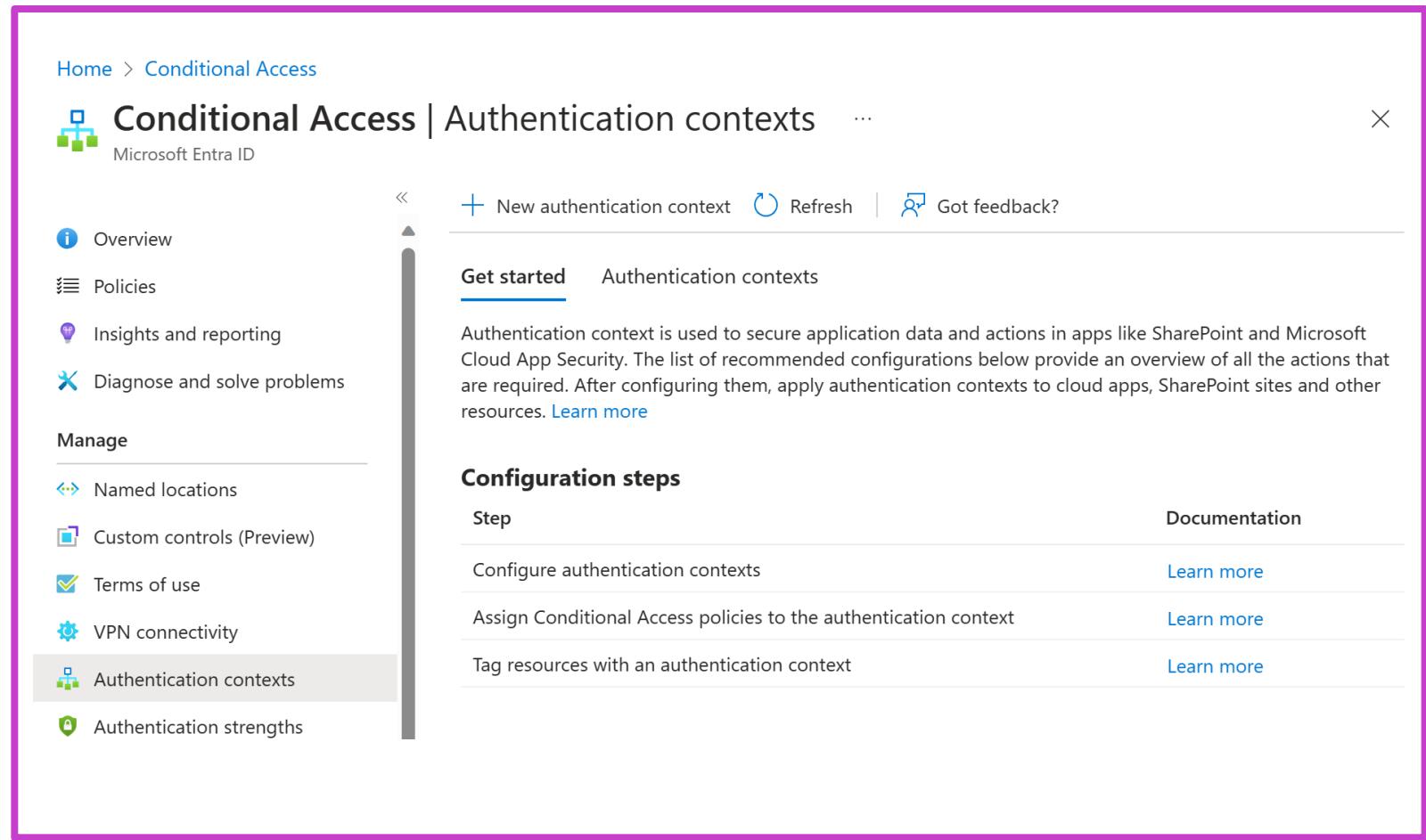
- There are several key benefits to continuous access evaluation.
- User termination or password change/reset: User session revocation will be enforced in near real time.
- Network location change: Conditional Access location policies will be enforced in near real time.
- Token export to a machine outside of a trusted network can be prevented with Conditional Access location policies.



# Authentication context

# Configure authentication context—Conditional Access

Authentication context can be used to further secure data and actions in applications. These applications can be your own custom applications, custom line-of-business (LOB) applications, applications like SharePoint, or applications protected by Microsoft Defender for Cloud Apps.



The screenshot shows the Microsoft Entra ID Conditional Access interface. The left sidebar has a tree view with nodes: Overview, Policies, Insights and reporting, Diagnose and solve problems, Manage, Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication contexts (which is selected and highlighted in grey), and Authentication strengths. The main content area has a title 'Conditional Access | Authentication contexts' and a sub-section 'Get started'. It includes a brief description of what authentication context is used for, followed by a 'Configuration steps' section with four items: 'Configure authentication contexts', 'Assign Conditional Access policies to the authentication context', and 'Tag resources with an authentication context', each with a 'Learn more' link. At the top right, there are 'New authentication context', 'Refresh', and 'Got feedback?' buttons.

# References (1 of 2)

**What is Conditional Access?**

<https://www.youtube.com/watch?v=ffMAw2IVO7A>

**How to deploy Conditional Access**

[https://www.youtube.com/watch?v=c\\_izIRNJNuk](https://www.youtube.com/watch?v=c_izIRNJNuk)

**How to roll out CA policies to end users**

[https://www.youtube.com/watch?v=0\\_Fze7Zpyvc](https://www.youtube.com/watch?v=0_Fze7Zpyvc)

**Conditional Access with device controls**

<https://www.youtube.com/watch?v=NcONUf-jeS4>

**Conditional Access with Microsoft Entra MFA**

<https://www.youtube.com/watch?v=Tbc-SU97G-w>



# References (2 of 2)

**Conditional Access in Enterprise Mobility and Security**

<https://www.youtube.com/watch?v=A7IrxAH87wc>

**Using the location condition in a Conditional Access policy**

<https://learn.microsoft.com/azure/active-directory/conditional-access/location-condition>

**Use compliance policies to set rules for devices you manage with Intune**

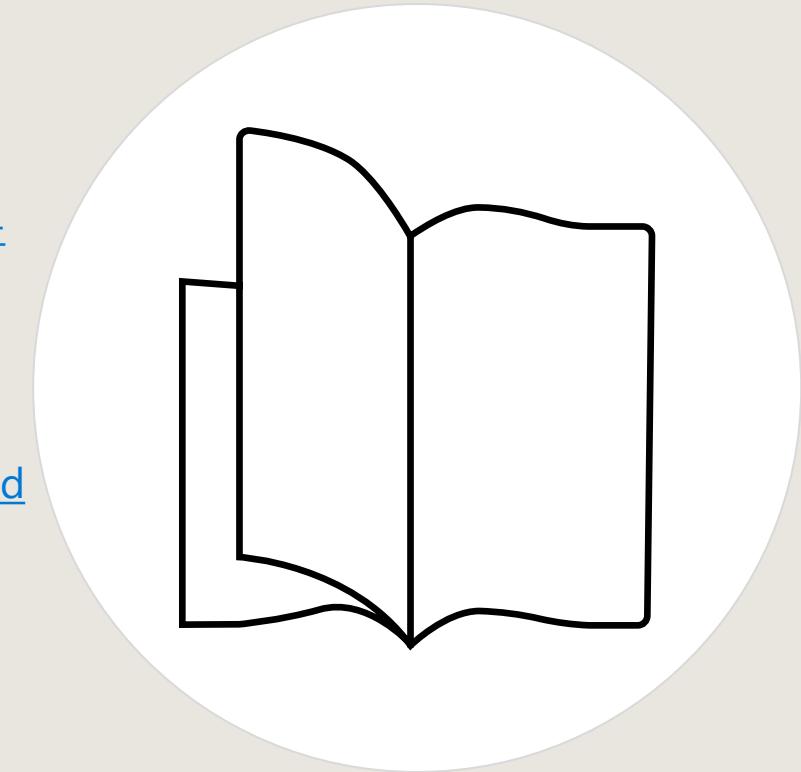
<https://learn.microsoft.com/mem/intune/protect/device-compliance-get-started>

**Introducing security defaults**

<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414>

**Plan a Conditional Access deployment**

<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414>



# Manage Microsoft Entra Identity Protection

# Objectives

- 1** Review identity protection basics
- 2** Implement and manage user risk policy
- 3** Implement MFA registration policy
- 4** Monitor, investigate, and remediate elevated risky users
- 5** Security for workload identities
- 6** Microsoft Defender for Identity

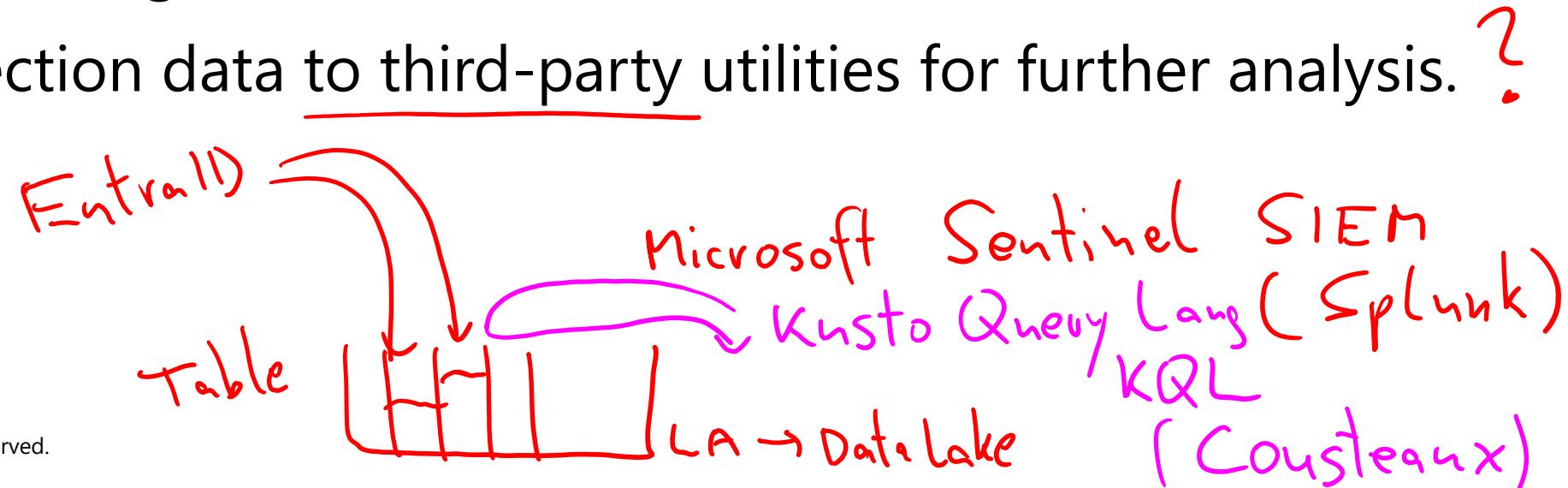
# Review identity protection basics

# Identity protection basics

Identity protection is a service that enables organizations to view the security posture of any account.

Key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the Microsoft Entra admin center.
- Export risk detection data to third-party utilities for further analysis. ?



# Risk detection, remediation, and investigation

## Common risks detected and remediated

- Anonymous IP address/atypical travel
- Malware-linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray
- Microsoft Entra threat intelligence
- New country
- Suspicious inbox forwarding

Medium

## Risk investigation

### Reports:

- Risky users
- Risky sign-ins
- Risk detections

### Risk levels—low/medium/high

- Each level represents a higher likelihood that a user or sign-in is compromised

# Licensing for Identity Protection

ES

Capability	Microsoft Entra ID Free/ Microsoft 365 Apps	Microsoft Entra ID Premium P1	Microsoft Entra ID Premium P2
User risk policy (via Identity Protection)	No	No	Yes
Sign-in risk policy (via identity protection)	No	No	Yes
Security reports	Overview	No	Yes
	Risky users	Limited Information.*	Limited Information.*
	Risky sign-ins	Limited Information.*	Limited Information.*
	Risk detection	No	Limited Information.*
Notifications	User at risk alert	No	Yes
	Weekly digest	No	Yes
MFA registration policy	No	No	Yes

\* See notes or student materials for details.

# Identity Protection permissions

Password Admin

Role	Can do	Cannot do
Global Administrator	Full access to Identity Protection	
Security Administrator	Full access to Identity Protection CA	Reset password for a user
Security Operator	View all Identity Protection reports and Overview blade  Dismiss user risk, confirm safe sign-in, confirm compromise	Configure or change policies  Reset password for a user  Configure alerts
Security Reader	View all Identity Protection reports and Overview blade	Configure or change policies  Reset password for a user  Configure alerts  Give feedback on detections

Microsoft Entra ID P2 license required

© Copyright Microsoft Corporation. All rights reserved.

# Implement and manage user risk policy

# User risk policies

- Both sign-in risk policies and user risk policies can be enabled to automate the response to risk detections and allow users to self-remediate.
- Organizations must decide the level of risk they are willing to accept, balancing user experience and security posture.

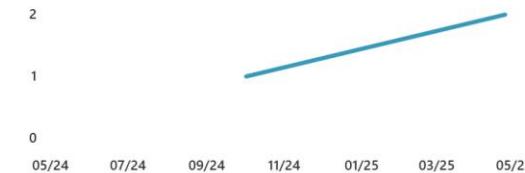
Microsoft Entra ID admin center → Identity → Protection → Identity Protection

Play tour Export dashboard Share

## Number of attacks blocked

3 Past 2 months ▲ Up 100% in the last 30 days

Number of attacks blocked by ID Protection.



[View attacks](#)

## Number of users protected

0 Past 12 months

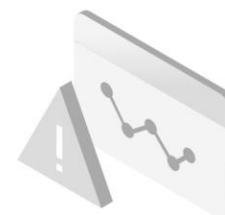


No data available.

[View users protected](#)

## Mean time to remediate high risk users

0 hours Past 12 months



No data available.

[Enable risk policy](#)

## Number of high risk users

0 Past 12 months



No data available.

[View high risk users](#)

# Exercise—enable sign-in risk policy

This exercise teaches students to enable a user risk policy and a sign-in risk policy.

[Launch this Exercise in GitHub](#)



Identity Protection | Sign-in risk policy

Search

Dashboard (Preview)

Overview

Tutorials

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky users

Risky workload identities

We recommend migrating sign-in risk policy to

Policy Name  
Sign-in risk remediation policy

Assignments

Users  
All users

Sign-in risk  
Medium and above

Controls

Access  
Require multifactor authentication

# Implement MFA registration policy

# What is MFA registration policy?

Microsoft Entra multifactor authentication provides a means to verify who you are using more than just a username and password. It provides a second layer of security to user sign-ins. For users to be able to respond to MFA prompts, they must first register for Microsoft Entra multifactor authentication.

We recommend that you require Microsoft Entra multifactor authentication for user sign-ins because it:

- Delivers strong authentication through a range of verification options.
- Plays a key role in preparing your organization to self-remediate from risk detections in Identity Protection.

# Demo—configure Microsoft Entra multifactor authentication registration policy

Microsoft Entra multifactor authentication provides a means to verify who you are using more than just a username and password. It provides a second layer of security to user sign-ins. This exercise teaches students to configure a registration policy.



[Launch this Exercise in GitHub](#)

Home > Identity Protection

## Identity Protection | Multifactor authentication registration policy

Search

- Dashboard (Preview)
- Overview
- Tutorials
- Diagnose and solve problems

Policy Name  
Multifactor authentication registration policy

Assignments

Users  
All users

Protect

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

Controls

Require Microsoft Entra ID multifactor authentication registration

Monitor, investigate,  
and remediate elevated  
risky users

# Risk reports

Each report launches with a list of all detections for the period shown at the top of the report. Each report allows for the addition or removal of columns based on administrator preference. Administrators can choose to download the data in .CSV or .JSON format. Reports can be filtered using the filters across the top of the report

## Identity Protection | Risky sign-ins

Download Learn more Export Data Settings Configure trusted IPs Troubleshoot Select all ...

We recommend migrating Identity Protection policies to Conditional Access for more conditions and controls. [Learn more →](#)

Auto refresh : Off Date : Last 1 month Show dates as : Local Risk state : 2 selected

Risk level (real-time) : None Selected Risk level (aggregate) : None Selected Detection type(s) : None Selected

Sign-in Type : 2 selected [+ Add filters](#)

Date ↑↓	User ↑↓	IP address	Location	Risk state ↑↓
8/8/2024, 4:28:24 PM	Iker Grgic	2806:2f0:9380:f019:2d...	MX	At risk
8/8/2024, 10:55:13 AM	Nikolajs Lusis	192.0.2.30	Bengaluru, Karnataka, IN	At risk
8/8/2024, 2:09:19 AM	Shanequa Gihon (Corp M)	223.233.80.8	Pune, Maharashtra, IN	At risk
8/7/2024, 12:34:34 PM	Shanequa Gihon (Corp M)	203.0.113..144	Chas, Jharkhand, IN	At risk
8/7/2024, 4:07:15 AM	Nikolajs Lusis	192.0.2.30	Bengaluru, Karnataka, IN	At risk
8/5/2024, 5:22:41 AM	Shanequa Gihon (Corp M)	198.51.100.143	Hyderabad, Telangana, IN	At risk
8/2/2024, 5:28:54 AM	Shanequa Gihon (Corp M)	198.51.100.28	Hyderabad, Telangana, IN	At risk
8/2/2024, 3:02:46 AM	Shanequa Gihon (Corp M)	192.0.2.119	Ranchi, Jharkhand, IN	At risk
8/2/2024, 3:00:39 AM	Shanequa Gihon (Corp M)	192.0.2.119	Ranchi, Jharkhand, IN	At risk
8/2/2024, 2:59:50 AM	Shanequa Gihon (Corp M)	192.0.2.119	Ranchi, Jharkhand, IN	At risk
8/2/2024, 2:58:19 AM	Shanequa Gihon (Corp M)	192.0.2.119	Ranchi, Jharkhand, IN	At risk
8/2/2024, 2:57:11 AM	Shanequa Gihon (Corp M)	192.0.2.119	Ranchi, Jharkhand, IN	At risk
8/2/2024, 2:42:08 AM	Shanequa Gihon (Corp M)	198.51.100.81	Hyderabad, Telangana, IN	At risk
8/1/2024, 1:30:23 AM	Shanequa Gihon (Corp M)	198.51.100.30	Hyderabad, Telangana, IN	At risk

# Report details—example Risky Users Report

Risky users ⚙ ...

Learn more Download Unselect all Confirm user(s) compromised Confirm user(s) safe Dismiss user(s) risk Refresh

Want to allow automatic risk remediation? Setup risk policies in Conditional Access. Learn more →

Get help investigating a risky user with Copilot. Select a user to get started.

Auto refresh : Off Show dates as : Local Risk level : High Add filters

User ↑↓	Risk state ↑↓	Risk last updated ↑↓
<input type="checkbox"/> Michael G Scott	At risk	7/23/2024, 8:06:02 PM
<input type="checkbox"/> Toby Adeniyi	At risk	6/7/2024, 4:09:40 PM
<input type="checkbox"/> Lee Gu	At risk	5/23/2024, 1:36:46 AM
<input type="checkbox"/> Oksana Avira	At risk	4/17/2024, 10:36:10 AM
<input type="checkbox"/> Cameron Potter	At risk	4/11/2024, 12:07:11 PM
<input type="checkbox"/> Garima Maheshwari	At risk	4/1/2024, 2:24:08 PM
<input type="checkbox"/> Admin Lab	At risk	2/29/2024, 3:59:46 AM
<input type="checkbox"/> Jonathan Wolcott	At risk	2/26/2024, 6:03:15 AM
<input type="checkbox"/> Cam Morales	At risk	9/18/2023, 7:53:06 AM
<input type="checkbox"/> Malka Bunnell (Corp)	At risk	8/30/2023, 4:17:02 PM
<input type="checkbox"/> -	At risk	9/28/2022, 3:53:58 PM
<input type="checkbox"/> -	At risk	2/22/2022, 7:17:56 PM
<input type="checkbox"/> -	At risk	2/22/2022, 7:17:56 PM
<input type="checkbox"/> -	At risk	2/22/2022, 7:17:55 PM
<input type="checkbox"/> -	At risk	2/22/2022, 7:17:55 PM

# Remediate risks and unblock users

**Administrators have the following options to remediate:**

- Self-remediation with risk policy
- Manual password reset
- Dismiss user risk
- Close individual risk detections manually

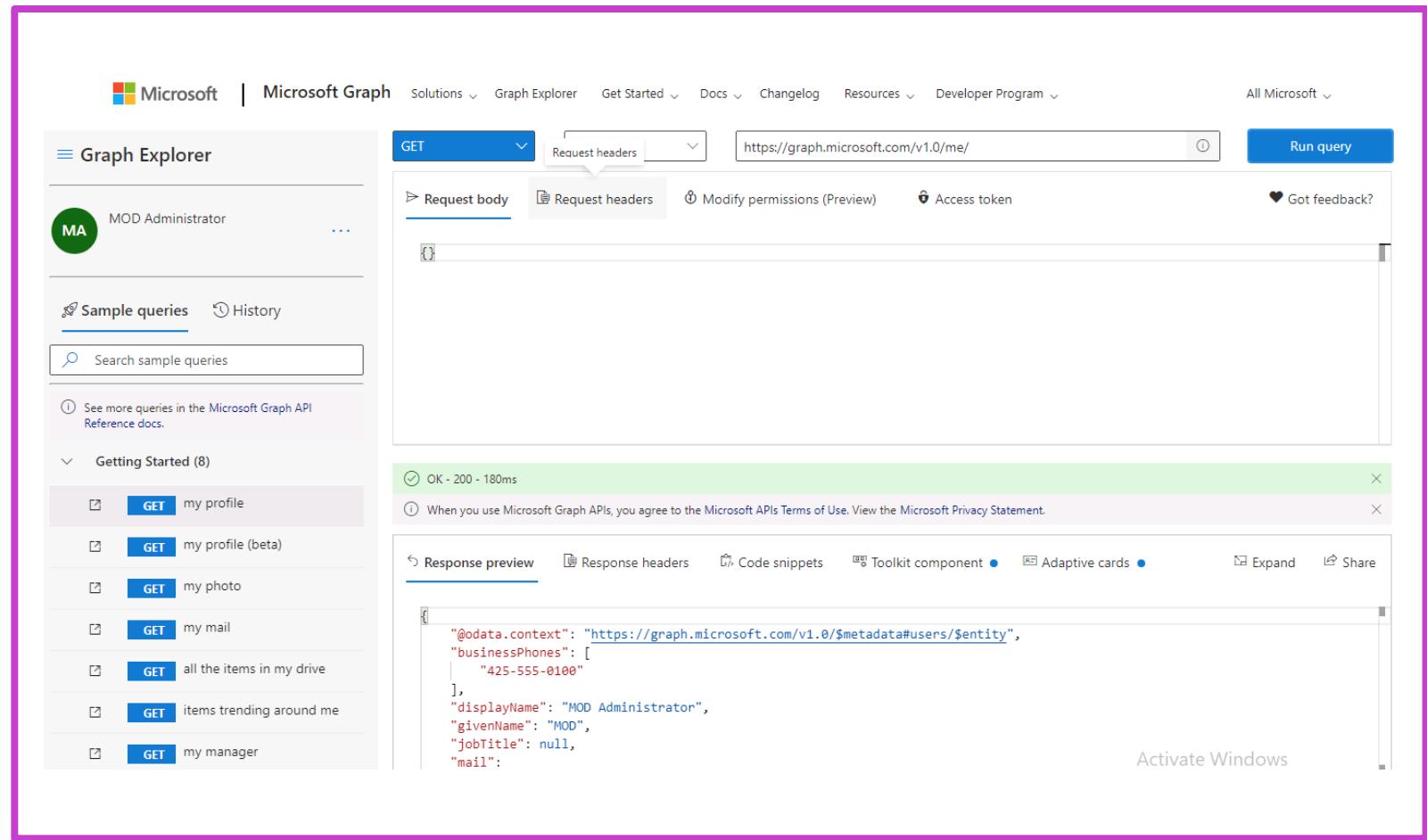
# Copilot for Security + Microsoft Entra – Risky Users

The screenshot shows the Microsoft Entra Identity Protection Risky users interface. On the left, a navigation sidebar under the 'Identity' section has 'Identity Protection' and 'Risky users' highlighted with red boxes. The main content area displays a search bar, navigation links (Learn more, Download, Select all, Confirm user(s) compromised, Dismiss user(s) risk), and a recommendation to migrate policies to Conditional Access. It also features a Copilot help card. The central part of the screen shows a table of risky users with columns for User, Risk state, and Risk last updated. The first user, Giovanna Costa, is highlighted with a red box.

User	Risk state	Risk last updated
Giovanna Costa	At risk	3/26/2024, 4:06:02 PM
Ratih Winata	At risk	3/26/2024, 11:31:01 AM
Sascha Lange	At risk	3/26/2024, 7:21:32 AM

# Use the Microsoft Graph API

- Microsoft Graph—unified API endpoint and the home of Microsoft Entra Identity Protection APIs
- Three Microsoft Graph APIs expose information about risky users and sign-ins:
  - RiskDetection
  - RiskyUsers
  - SignIn



# Security for workload identities

# Workload identities risk

A workload identity allows an application or service principal access to resources.

These workload identities differ from traditional user accounts as they:

- Can't perform multifactor authentication.
- Often have no formal lifecycle process.
- Need to store their credentials or secrets.

The screenshot shows the Microsoft Identity Protection Risk detections interface. The left sidebar includes links for Dashboard, Risk policy impact analysis, Tutorials, Diagnose and solve problems, Protect (Conditional Access, User risk policy, Sign-in risk policy, Multifactor authentication registration policy), Report (Risky users, Risky workload identities, Risky sign-ins, Risk detections), and a search bar. The main area has tabs for User detections and Workload identity detections, with 'Workload identity detections' highlighted by a red box. The table lists risk detections with columns for Detection time, Service principal name, Detection type, Risk state, and Risk level. The first two rows show 'Risky Test App 2' and 'Risky Test App 3' with 'Risk detected' status and 'High' risk level. The third row for 'AADIP-SP-Risk-Test-App' is highlighted in grey. The last two rows show 'Risky Test App 3' and 'Risky Test App 2' again, both with 'At risk' status and 'High' risk level.

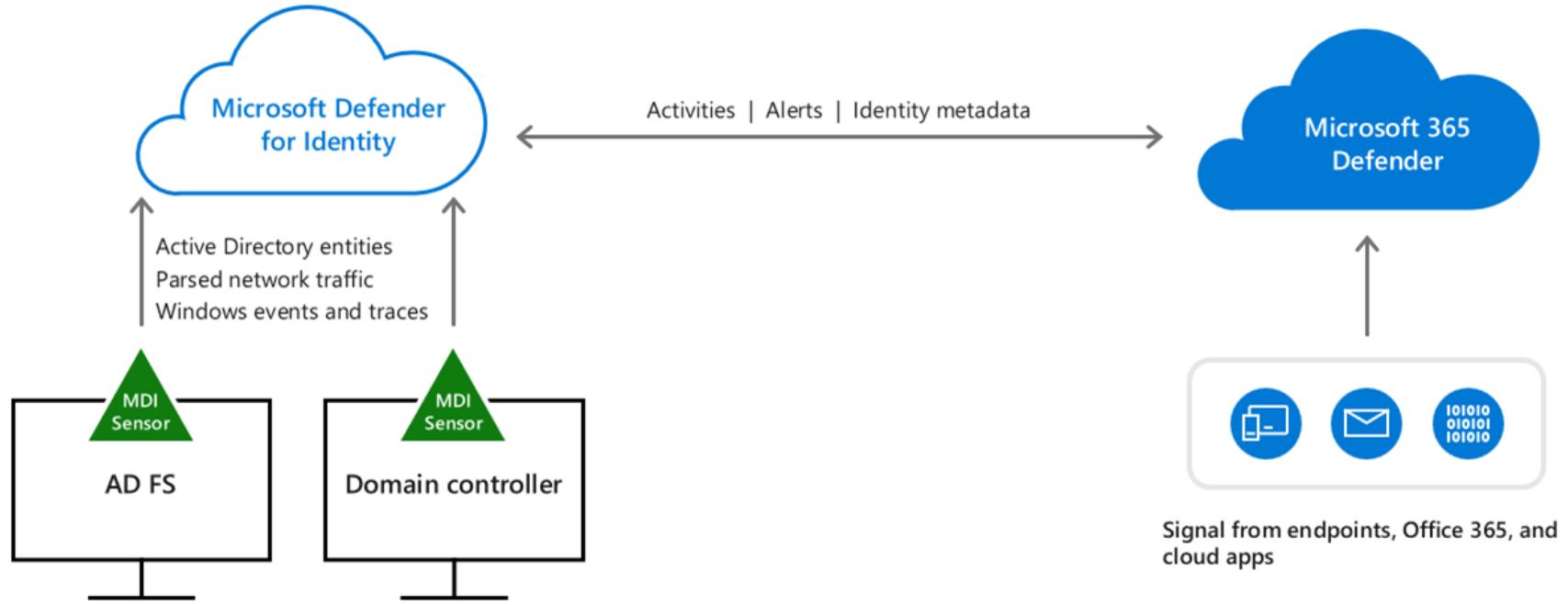
Detection time	Service principal name	Detection type	Risk state	Risk level
10/31/2021, 11:40:48 PM	Risky Test App 2	Risk detected	Confirmed compromised	High
10/27/2021, 12:13:00 PM	Risky Test App 3	Risk detected	Confirmed compromised	High
10/19/2021, 8:53:56 PM	AADIP-SP-Risk-Test-App	Azure AD threat intellig...	At risk	High
10/19/2021, 8:00:00 PM	Risky Test App 3	Risk detected	At risk	High
10/19/2021, 8:00:00 PM	Risky Test App 2	Risk detected	At risk	High
10/19/2021, 8:00:00 PM	Risky Test App 5	Risk detected	At risk	High

# Workload identity risks detected

Detection name	Description
Microsoft Entra threat intelligence	This risk detection indicates some activity that is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.
Suspicious sign-ins	This risk detection indicates sign-in properties or patterns that are unusual for this service principal.
Unusual addition of credentials to an OAuth app	This detection identifies the suspicious addition of privileged credentials to an OAuth app. This can indicate that an attacker has compromised the app, and is using it for malicious activity.
Admin confirmed account compromised	This detection indicates an admin has selected 'Confirm compromised' in the Risky Workload Identities UI or using the riskyServicePrincipals API.

# Microsoft Defender for Identity

# Microsoft Defender for Identity



- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

## Log into Defender for Identity:

- <https://security.microsoft.com/settings/identities>

# What Microsoft Defender for Identity does

- **Monitors**
  - AD on-premises and hybrid signals
  - Uses behavioral analytics
  - Finds identity-based attacks
  - Surfaces risk in the identity usage
- **Detects**
  - Credential theft
  - Golden ticket / silver ticket attacks
  - DCSync and DCShadow
  - Reconnaissance
  - Lateral movement
- **Signals sent to Sentinel / XDR**
  - Endpoint activity
  - Email signals
  - Unusual cloud app behavior
- **Signals for Microsoft Identity Threat Detection and Response (ITDR)**
  - On-prem AD activity
  - Lateral movement
  - Kerberos abuse
  - Domain dominance attempts

# References

## Conditional Access for workloads

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/workload-identity>

## Require MFA for all users

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

## Defender for Identity

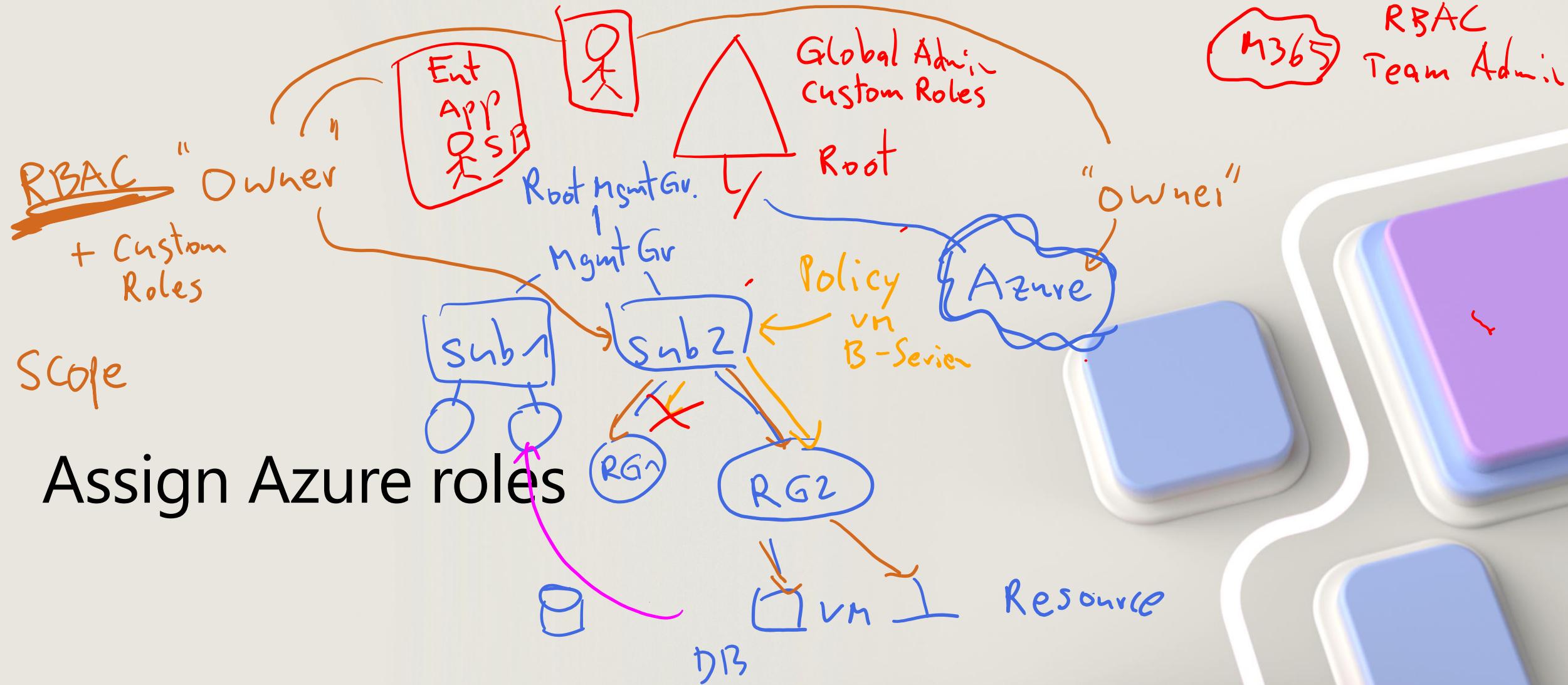
<https://learn.microsoft.com/en-us/defender-for-identity/>



# Implement access management for Azure resources

# Objectives

- 1 Assign Azure roles
- 2 Configure a custom Azure role
- 3 Create and configure managed identities
- 4 Access Azure resources with managed identities
- 5 Analyze Azure role permissions
- 6 Configure Azure Key Vault policies and access objects



# Identities and roles

Azure role-based access control (Azure RBAC) is the authorization system to manage access to Azure resources. Assign roles to users, groups, service principals, or managed identities at a particular scope.

Who needs access	What role to assign
Identities <ul style="list-style-type: none"><li>User ✓</li><li>Group ✓</li><li>Service Principal ✓</li><li>Managed Identity ✓</li></ul>	Built-in Azure roles <ul style="list-style-type: none"><li><u>Owner</u> – Full access to all resources.</li><li><u>Contributor</u> – Can create and manage all types of Azure resources, but can't grant access.</li><li><u>Reader</u> – Can view the available Azure resources.</li><li><u>User Access Administrator</u> – Assign access to Azure resources.</li><li>Other task specific roles, like Virtual Machine Contributor, can be assigned. ✓ ✓ ✓</li></ul>

What scope to assign?

Management Group – Subscription – Resource Group - Resource

# Assign a role in the Azure portal

The screenshot shows the Azure portal interface for the 'rgBuild' resource group. A red box highlights the 'Access control (IAM)' section in the left sidebar. A red arrow points from the text 'Access control (IAM)' in the heading to the 'Access control (IAM)' link in the sidebar. Another red box highlights the 'Active' tab under 'Current User Assignments', which shows a value of 1. A red arrow points from the text 'Active' to the number 1.

rgBuild | Access control (IAM) ...

Resource group

Search X « » Add Download role assignments Edit columns Refresh Delete Feedback

Overview Activity log Access control (IAM) Tags Resource visualizer Events Settings Cost Management Monitoring Automation Help

Action required: 1 user has elevated access in your tenant. You should take immediate action and remove all role assignments

Check access Role assignments Roles Deny assignments Classic administrators

Looking for the previous check access view? [Click here](#).

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Check access

Current User Assignments

Active ⓘ	Eligible ⓘ	Deny ⓘ
1	0	0

Search by role name or membership

Role Name ↑ Scope ↑ Membership ↑

Active permanent assignments (1)

User Access Administrator	Root (Inherited)
---------------------------	------------------

Active time-bound assignments (0)

Eligible permanent assignments (0)

Eligible time-bound assignments (0)

# Assign a role using script

PS7  
Windows PS 5.1  
Monad

Module Az

Az. Account  
Az. Storage

## PowerShell

```
New-AzRoleAssignment -ObjectId <objectId>  
-RoleDefinitionName <roleName>  
-Scope  
/subscriptions/<subscriptionId>/resourcegroups/<resourceGroupName>/providers/<providerName>/<res  
ourceType>/<resourceSubType>/<resourceName>
```

Jeff Snover

## CLI scripting

```
az role assignment create --assignee "{assignee}" \  
--role "{roleNameOrId}" \  
--resource-group "{resourceGroupName}"
```



User



# Configure a custom Azure role

Entra

# Create a custom role

The principle of least privilege lets you pick just the capabilities you need.

To create the custom role:

1. Open Microsoft Entra admin center then open Identity.
2. Select Roles and administration.
3. Select + New custom role.
4. Then name and assign the capabilities needed.

The screenshot shows the 'New custom role' interface in the Microsoft Entra admin center. The top navigation bar includes 'Home', 'Contoso', 'Roles and administrators', and a feedback link. Below the navigation is a breadcrumb trail: 'All roles' > 'New custom role'. A 'Got feedback?' button is present. The main content area has tabs for 'Basics' (selected) and 'Permissions' (underlined), with a 'Review + create' button. A note states: 'Add permissions for this custom role. Currently, permissions for Application registrations and Enterprise applications are supported in custom roles.' A 'Learn more' link is provided. A search bar labeled 'Search by permission name or description' is at the top of the permissions list. The permissions table has columns for 'Permission' (checkboxes) and 'Description'. The table lists 15 permissions related to application policies and organization applications, such as 'microsoft.directory/applicationPolicies/allProperties/read' (Read all properties of application policies) and 'microsoft.directory/applications/myOrganization/allProperties/update' (Update all properties on single-directory applications).

Permission	Description
<input type="checkbox"/> microsoft.directory/applicationPolicies/allProperties/read	Read all properties of application policies.
<input type="checkbox"/> microsoft.directory/applicationPolicies/allProperties/update	Update all properties of application policies.
<input type="checkbox"/> microsoft.directory/applicationPolicies/basic/update	Update standard properties of application policies.
<input type="checkbox"/> microsoft.directory/applicationPolicies/create	Create application policies.
<input type="checkbox"/> microsoft.directory/applicationPolicies/createAsOwner	Create application policies. Creator is added as first owner.
<input type="checkbox"/> microsoft.directory/applicationPolicies/delete	Delete application policies.
<input type="checkbox"/> microsoft.directory/applicationPolicies/owners/read	Read owners on application policies.
<input type="checkbox"/> microsoft.directory/applicationPolicies/owners/update	Update the owner property of application policies.
<input type="checkbox"/> microsoft.directory/applicationPolicies/policyAppliedTo/read	Read application policies applied to objects list.
<input type="checkbox"/> microsoft.directory/applicationPolicies/standard/read	Read standard properties of application policies.
<input type="checkbox"/> microsoft.directory/applications/myOrganization/allProperties/read	Read all properties of single-directory applications.
<input type="checkbox"/> microsoft.directory/applications/myOrganization/allProperties/update	Update all properties on single-directory applications

# Create a custom role using JSON

The asterisk (\*) is used as a wildcard. If you need to assign all of the read permissions from the Billing resource, use this command:

*Microsoft/Billing/\*/read.*

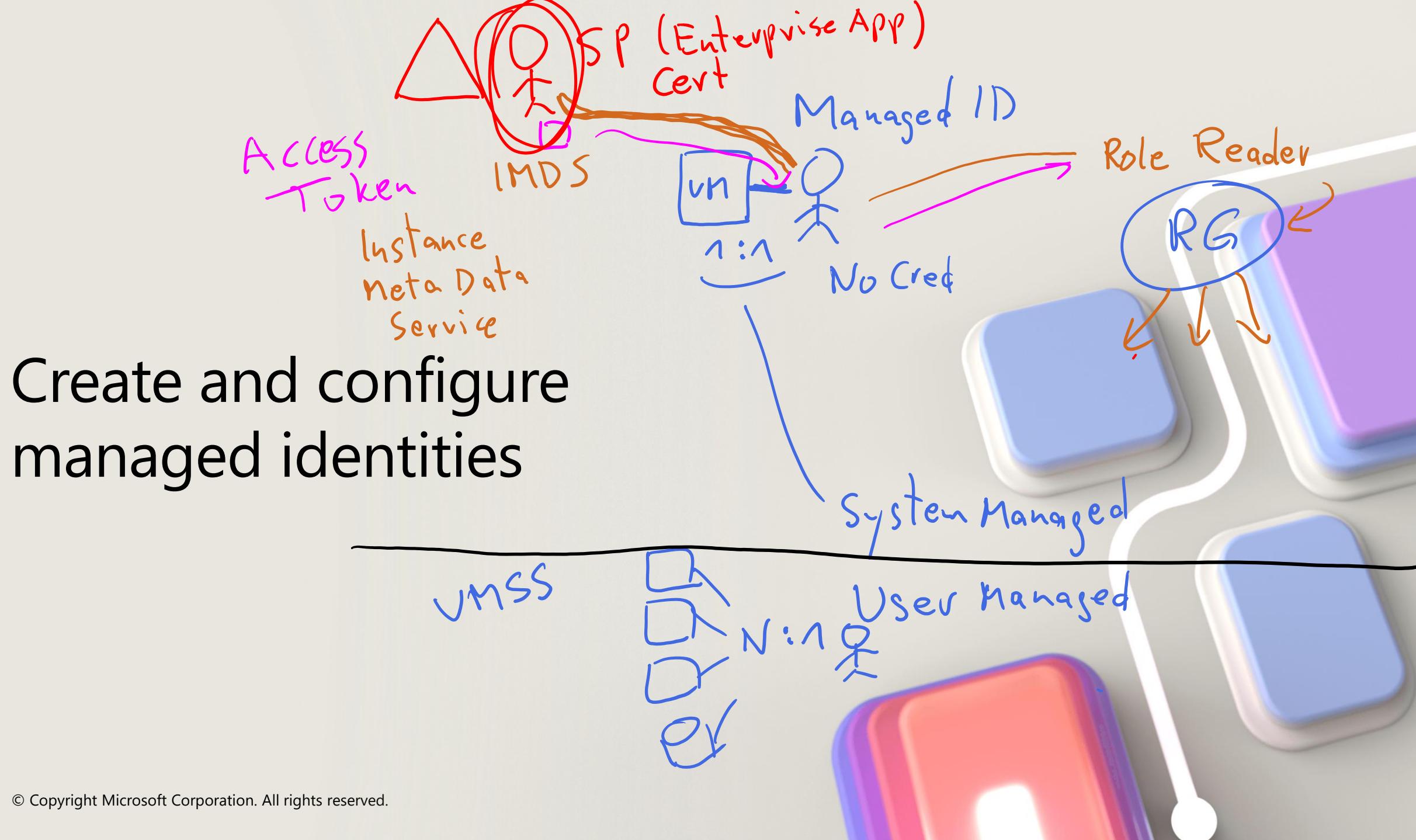
The wildcard can exist at any level.

A screenshot of a JSON object representing a custom role. The JSON structure is as follows:

```
{  
  "properties": {  
    "roleName": "Billing Reader Plus",  
    "description": "Read billing data and download invoices",  
    "assignableScopes": [  
      "/subscriptions/your-subscription-number"  
    ],  
    "permissions": [  
      {  
        "actions": [  
          "Microsoft.Authorization/*/read",  
          "Microsoft.Billing/*/read",  
          "Microsoft.Commerce/*/read",  
          "Microsoft.Consumption/*/read",  
          "Microsoft.Management/managementGroups/read",  
          "Microsoft.CostManagement/*/read",  
          "Microsoft.Support/*"  
        ],  
        "notActions": [],  
        "dataActions": [],  
        "notDataActions": []  
      }  
    ]  
  }  
}
```

Annotations on the JSON:

- A red circle highlights the `roleName` field with the value `"Billing Reader Plus"`.
- A blue oval encloses the entire `permissions` array.
- Blue arrows point from the `actions` array within the `permissions` block to the following actions:
  - `Microsoft.Authorization/*/read`
  - `Microsoft.Billing/*/read`
  - `Microsoft.Commerce/*/read`
  - `Microsoft.Consumption/*/read`
  - `Microsoft.Management/managementGroups/read`
  - `Microsoft.CostManagement/*/read`
  - `Microsoft.Support/*`
- A blue arrow points from the `notActions` array to the text **Azure Provider**.
- A red arrow points from the `Data` label to the `dataActions` and `notDataActions` arrays.



# Types of Managed Identities

Identity type	Description and usage
System-assigned  1 : 1	Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity, an identity is created in Microsoft Entra ID. The identity is tied to the lifecycle of that service instance. When the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Microsoft Entra ID.
User-assigned  Portal N : 1 ID Resources	You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more instances of an Azure service. For user-assigned managed identities, the identity is managed separately from the resources that use it.

## Benefits of using managed identities

- You don't need to manage credentials. Credentials aren't even accessible to you.
- You can use managed identities to authenticate to any resource that supports Microsoft Entra authentication, including your own applications. Managed identities can be used without any extra cost.

# Use a managed identity in the Azure portal

The screenshot shows two windows from the Azure portal. On the left is the main 'TestManagedIdentities | Managed identities' blade, and on the right is a modal dialog titled 'Add user assigned managed identity'.

**Main Blade (Left):**

- Subscription: TestManagedIdentities | API Management service
- Search bar
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Events
- Settings
- APIs
- Developer portal
- Monitoring
- Deployment + infrastructure
- Security
  - Defender for Cloud
  - Managed identities** (highlighted with a red box)
  - Certificates
  - Protocols + ciphers

**Modal Dialog (Right):**

### Add user assigned managed identity

Select a subscription \*

Visual Studio Enterprise Subscription

User assigned managed identities

Filter by identity name and/or resource group name

No user assigned managed identities found based on the search term.

Selected identities:

No user assigned managed identities selected. Select one or more user assigned managed identities you want to assign to this resource.

**Blade Headers:**

- System assigned
- User assigned (highlighted with a red box)

**Blade Buttons:**

- + Add (highlighted with a red box)
- Remove
- Refresh

**Blade Tables:**

Name
No results

# Assign a managed identity in script

## CLI

```
az webapp identity assign --resource-group <group-name> --name <app-name> --identities <identity-name>
```

## PowerShell

```
Update-AzFunctionApp -Name <app-name> -ResourceGroupName <group-name> -IdentityType UserAssigned -IdentityId $userAssignedIdentity.Id
```

## Within a template ARM (json)

```
"identity": {  
    "type": "UserAssigned",  
    "userAssignedIdentities": {  
        "<RESOURCEID>": {}  
    }  
}
```



# Access Azure resources with managed identities

# Managed identities and Azure resources

## Scenario:

- Application needs to access outside resources like a database or storage account
- How can a developer do this securely?
- You don't want to embed an account/password into the application.

## Use a managed identity:

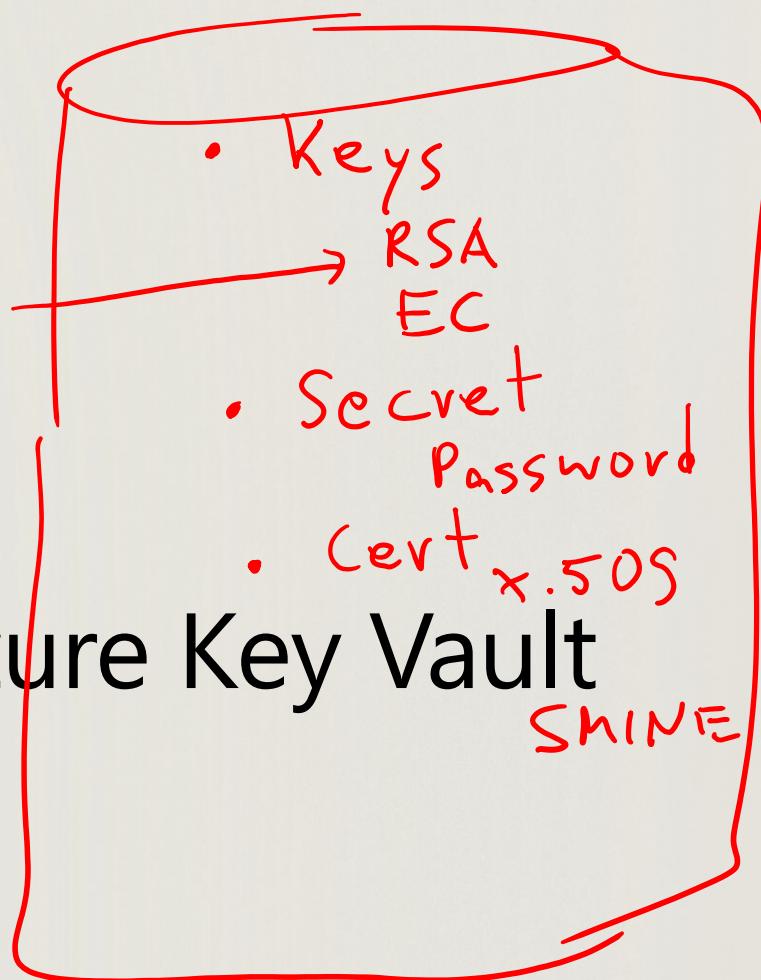
- Assign a managed identity to an application or virtual machine.
- Open the applications properties.
- Launch the Access Control (IAM).
- Add a role assignment to grant the needed access and resource.

# Assigning a resource and managed identity

The screenshot shows the Azure portal interface for adding a role assignment. The main page has a navigation bar at the top: Home > vmBuild | Access control (IAM) > Add role assignment. Below this, there are tabs: Role, Members\*, Conditions, and Review + assign. The Members tab is selected, indicated by a blue underline and a red dot. The 'Selected role' is set to 'Avere Operator'. Under 'Assign access to', the 'Managed identity' option is selected (radio button is blue). A red box highlights the 'Select members' button. The 'Members' section shows a table with columns: Name, Object ID, and Type. The message 'No members selected' is displayed. The 'Description' section is labeled 'Optional'. To the right, a modal window titled 'Select managed identities' is open. It contains a warning message: '⚠ Some results might be hidden due to your ABAC condition.' Below this, there are dropdown menus for 'Subscription' (set to 'Visual Studio Enterprise Subscription') and 'Managed identity' (with a 'Select' button highlighted by a red box). A search bar labeled 'Search by resource type' is also present. At the bottom of the modal are 'Select' and 'Close' buttons, with a 'Feedback' link on the far right.

Data  
Role  
oder  
KV Access Policy

## Configure Azure Key Vault RBAC policy



msmt  
Role

# Key Vault Access policy

- You can grant access to Azure Key Vault using either role-based access control (RBAC) or Key Vault access policies.
- Either method works to protect your secrets, certificates, and keys.
- Access policies give you a little more granular control, but can be harder to manage.
- Choose the best option based on your security posture needs.

Home > Key vaults > kv1234sc300lab >  
**Add access policy** ...

Configure from template (optional)

Key permissions

0 selected

Select all

Key Management Operations

Get

List

Update

Create

Import

Delete

Recover

Backup

Restore

Secret permissions

Certificate permissions

Select principal \*

Authorized application ⓘ

Add

Key Management Operations

Decrypt

Encrypt

Unwrap Key

Wrap Key

Verify

Sign

Cryptographic Operations

Purge

Privileged Key Operations

Release

Rotation Policy Operations

besser: RBAC

# Key Vault and RBAC policies

The screenshot shows the 'Access policies' page for a Key Vault named 'kv1234sc300lab'. The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Settings, Keys, Secrets, Certificates, **Access policies** (which is highlighted with a red box), and Networking. The main area displays a message: 'Please click the 'Save' button to commit your changes.' Below this, under 'Enable Access to:', there are three checkboxes: 'Azure Virtual Machines for deployment', 'Azure Resource Manager for template deployment', and 'Azure Disk Encryption for volume encryption'. Under 'Permission model', two radio buttons are shown: 'Vault access policy' (unselected) and 'Azure role-based access control' (selected, and it is also highlighted with a red box). The top right of the page has Save, Discard, and Refresh buttons.

# Assign access with RBAC to Key Vault

The screenshot shows the 'kvBuild04242025 | Access control (IAM)' blade in the Azure portal. A red circle highlights the 'Access control (IAM)' link in the left sidebar. The main content area displays a warning message: 'Action required: 1 user has elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access.' Below this, there are tabs for 'Check access', 'Role assignments', 'Roles', 'Deny assignments', and 'Classic administrators'. The 'Check access' tab is selected. Under 'My access', there is a 'View my access' button. The 'Check access' section allows reviewing access levels for users, groups, service principals, or managed identities. It includes a 'Check access' button and a 'Learn more' link. The page also features three cards: 'Grant access to this resource' (with 'Add role assignment' button), 'View access to this resource' (with 'View' button), and 'View deny assignments' (with 'View' button).

# Built-in Azure Key Vault roles

Built-in role	Description
Key Vault Administrator	Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. Can't manage key vault resources or manage role assignments.
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except manage permissions.
Key Vault <u>Crypto Officer</u>	Perform any action on the <u>keys</u> of a key vault, except manage permissions.
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations.
Key Vault Crypto User	Perform cryptographic operations using keys.
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets. Can't read sensitive values such as secret contents or key material.
Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage permissions.
Key Vault Secrets User	Read secret contents.

# Retrieve objects from Azure Key Vault

# Retrieve a secret from Key Vault in the Azure portal

- Azure Key Vault is a secure tool for storing secrets, keys, and certificates.
- Once stored, these items can be used by users and applications to perform actions and operations in a secure method.

## Retrieval methods:

- Key Vault UI
- Scripting/code

Home > Key vaults > kv1234sc300lab > mySC300keyvaultSecret >

 ba6102eeaf724b23bdea13e835260de6  
Secret Version

 Save  Discard changes

### Properties

Created 6/19/2022, 3:37:12 PM

Updated 6/19/2022, 3:37:12 PM

### Secret Identifier

### Settings

Set activation date ⓘ

Set expiration date ⓘ

### Enabled

Yes  No

Tags 0 tags

### Secret

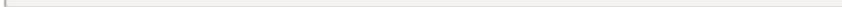
#### Content type (optional)

 Hide Secret Value



#### Secret value

This is my secret



 Key, Cert X

# Retrieve a secret from Key Vault in code/script

## Azure CLI

```
az keyvault secret show --name "mySC300keyvaultSecret" --vault-name "<your-unique-keyvault-name>" --query "value"
```

## PowerShell

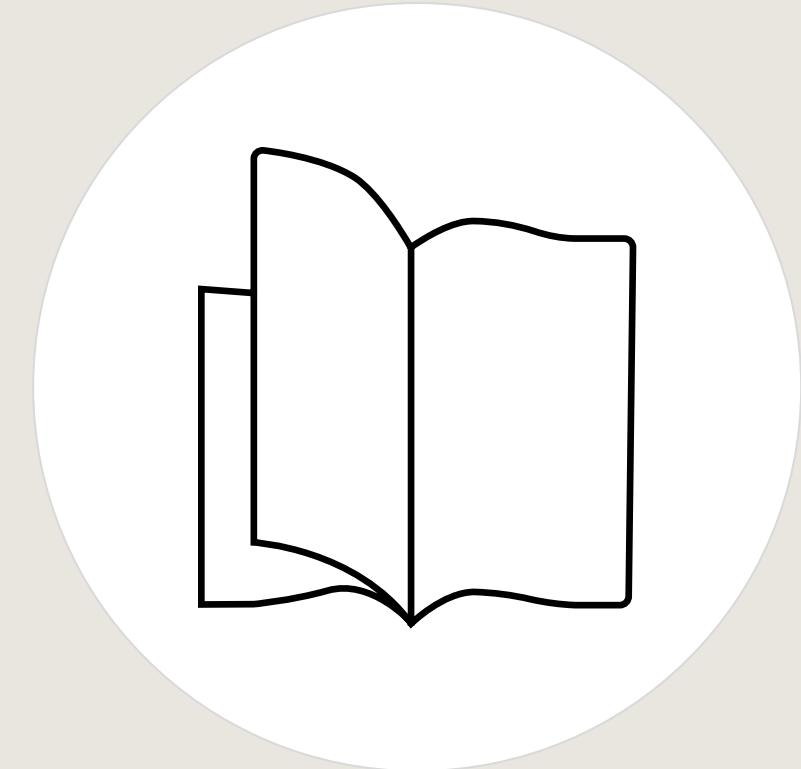
```
$secret = Get-AzKeyVaultSecret -VaultName "<your-unique-keyvault-name>" -Name "mySC300keyvaultSecret" -AsPlainText
```

## Application code

If you're building an application that needs access to your key vault secrets, certificates, and keys that can be done. You can access the key vault using .NET, Node.js, Python, and other languages.

# References

- [Assign Azure roles using the Azure portal – Azure RBAC](#)
- [Create or update Azure custom roles using the Azure portal – Azure RBAC](#)
- [Configure managed identities using the Azure portal – Microsoft Entra ID](#)
- [Assign a managed identity access to a resource using the Azure portal – Microsoft Entra ID](#)
- [Understand Azure role definitions – Azure RBAC](#)
- [Grant permission to applications to access an Azure key vault using Azure RBAC](#)
- [Create and access a secret in Azure Key Vault](#)



# Deploy and configure Global Secure Access with Microsoft Entra

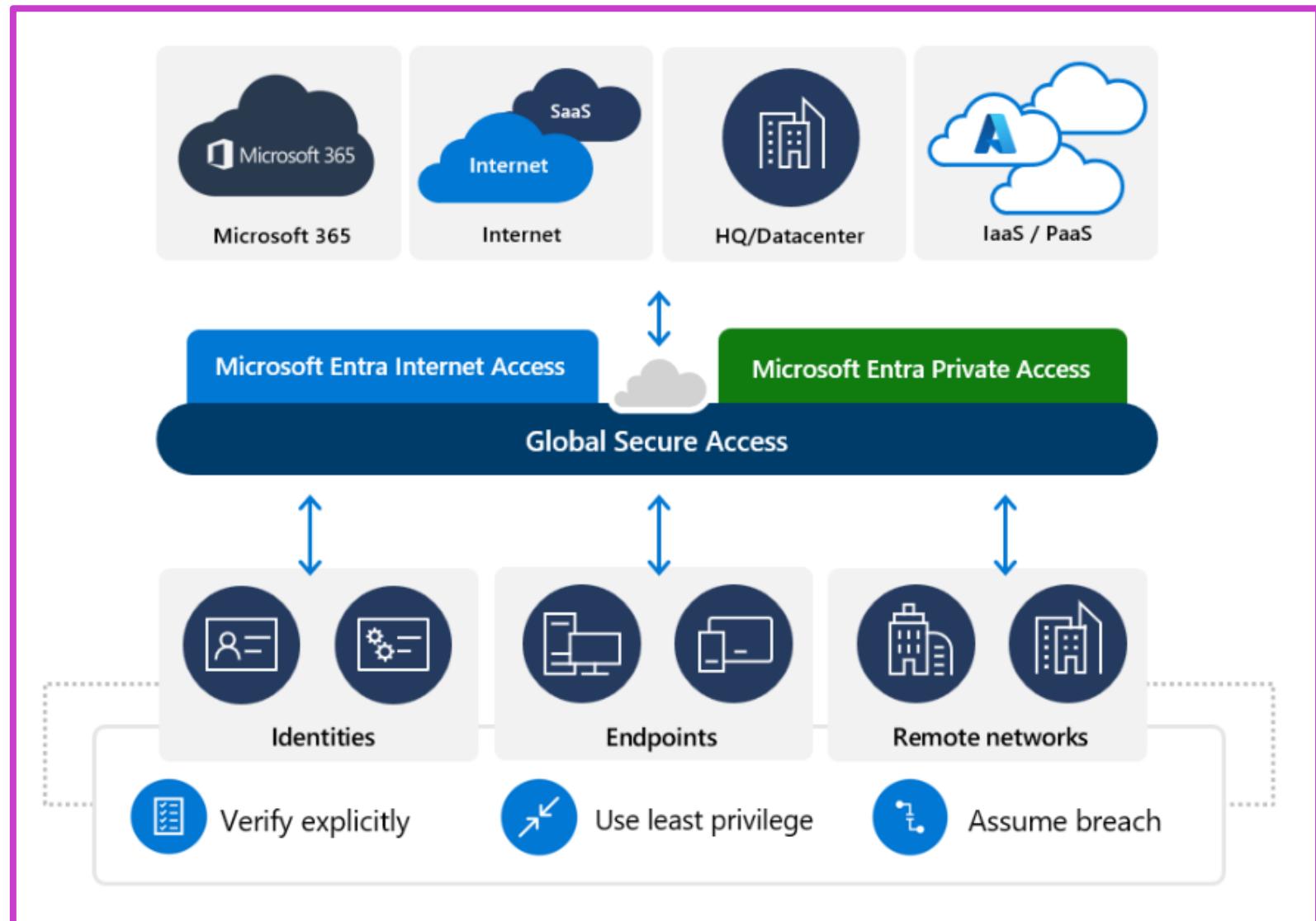
# Objectives

- 1** Define Global Secure Access and its components
- 2** Explore deployment and configuration of Microsoft Entra Internet Access
- 3** Explore deployment and configuration of Microsoft Entra Private Access
- 4** Use the Global Secure Access Dashboard to monitor your systems
- 5** Configure Remote Networks
- 6** Create Conditional Access based on Global Secure Access

# What is Global Secure Access?

## Microsoft Security Service Edge (SSE)

- Microsoft Entra Internet Access
  - Secure access to Microsoft services, SaaS apps, and public internet apps
- Microsoft Entra Private Access
  - Secure access to private corporate resources.



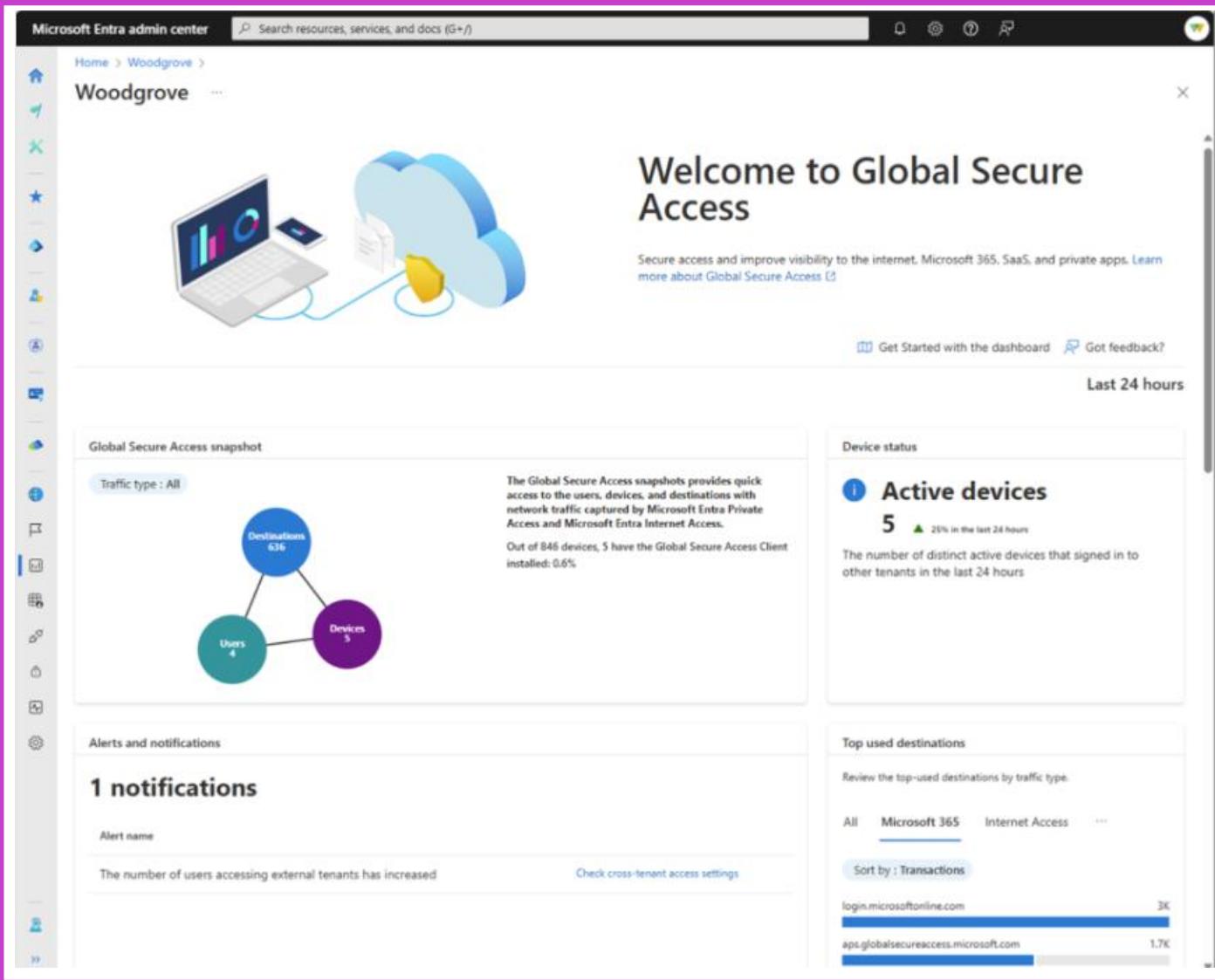
# Deploy and configure Microsoft Entra Internet Access

Steps	Description
1. Enable the Microsoft traffic forwarding profile.	With the Microsoft profile enabled, Microsoft Entra Internet Access acquires the traffic going to Microsoft services, like Exchange Online and SharePoint Online.
2. Install the Global Secure Access Client on end-user devices.	Download and install the client app to capture and control access from the client.
3. Enable tenant restrictions.	Configure which tenants / organizations are allowed to blocked.
4. Enable enhanced Global Secure Access signaling and Conditional Access.	Use Conditional Access and Global Secure Access to prevent attacks.

# Deploy and configure Microsoft Entra Private Access

Steps	Description
<b>1. Configure a Microsoft Entra private network connector and connector group.</b>	Create connection between an on-premises server and Global Secure Access.
<b>2. Configure Quick Access to your private resources.</b>	Define specific fully qualified domain names (FQDNs) or IP addresses of private resources to include in Microsoft Entra Private Access.
<b>3. Enable the Private Access traffic forwarding profile.</b>	Turn on Private Access and link from on-premises router to remote networks.
<b>4. Install and configure the Global Secure Access Client on end-user devices.</b>	Deploy the client software onto devices, so they can access the traffic flow.

# Global Secure Access Dashboard



## Reporting widgets and deeper details:

- Global Secure Access snapshot
- Alerts and notifications
- Usage profiling
- Top used destinations
- Cross-tenant access
- Web category filtering
- Device status

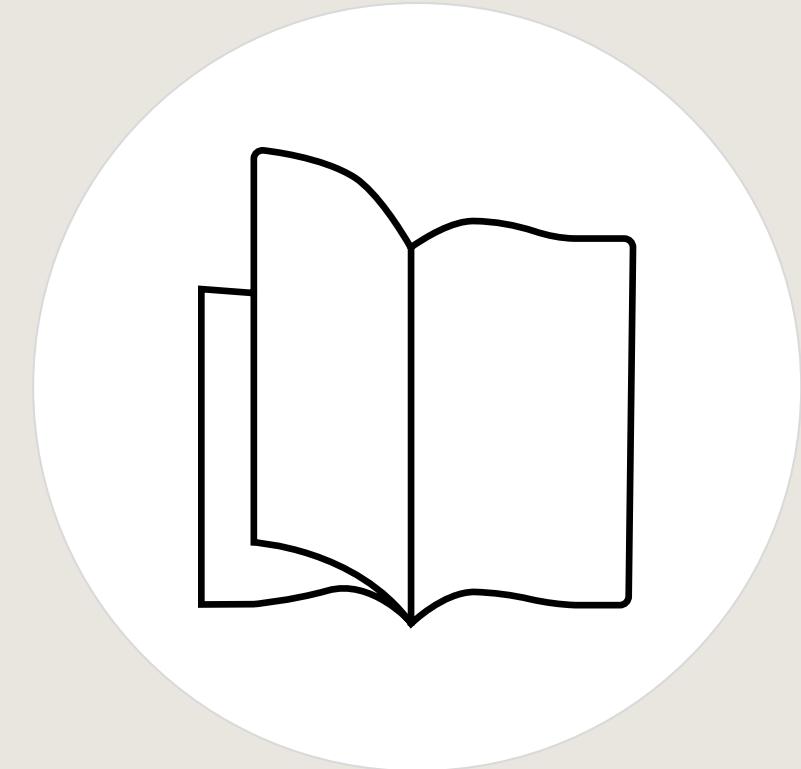
# Conditional Access updates with Global Secure Access

New Conditional Access check	What it does
Compliant network check	Ensures users connect from a verified network connectivity model for their specific tenant and are compliant with security policies enforced by administrators.
Private Access apps	Microsoft Entra Private Access apps is a powerful way to enforce security policies for your internal, private resources.
Source IP restoration	Source IP restoration in Global Secure Access allows backward compatibility for Microsoft Entra customers to continue using original user Source IP.

- 
- Always remember to protect your break-glass accounts.
  - You can combine new and existing conditions for more security.

# References

- [Global Secure Access documentation - Global Secure Access](#)
- [Learn about Microsoft Entra Private Access - Global Secure Access](#)
- [Learn about Microsoft Entra Internet Access - Global Secure Access](#)
- [Learn about Universal Conditional Access through Global Secure Access - Global Secure Access](#)



# Summary



## Plan and implement MFA

- Plan your MFA deployment
- Configure and manage MFA settings
- Manage MFA for users
- Core piece of Zero Trust

## Conditional Access

- Conditional Access policies
- Testing and troubleshooting CA
- Implement application controls
- Session management

## Manage user authentication

- Configure authentication methods (passwords to passwordless)
- Windows Hello for Business
- Use Password Protection and Smart Lockout
- Implement tenant restrictions

## Identity Protection

- Implement user risk policy
- Configure sign-in risk policies
- Manage MFA registration policy
- Remediate elevated risky users

## Access Azure resources

- Built-in and custom roles
- Managed identities
- Key Vault identity level access

# Labs



Lab	Brief description	Length
8. Enable MFA ✓	Configure multifactor authentication policies, set up Conditional Access rules, and configure Microsoft Entra MFA for passwords.	10 minutes
9. Configure and deploy SSPR ✓	Enable self-service password reset, register a cell phone number, and test self-service password reset.	15 minutes
10. Microsoft Entra ID Authentication for Windows and Linux VMs	Configure Microsoft Entra ID authentication on a virtual machine running Windows or Linux.	15 minutes
11. Assign Azure resources	Use PIM to assign Azure resource roles	10 minutes
12. Manage Microsoft Entra smart lockout values.	Customize the Microsoft Entra smart lockout values.	5 minutes
13. Implement Conditional Access ✓	Create and test a Conditional Access policy.	10 minutes
14. Enable sign-in risk policy	Enable a user risk policy and a sign-in risk policy.	10 minutes
15. Configure MFA registration policy	Configure a multifactor authentication registration policy.	5 minutes
16. Key Vault and managed identities	Configure an Azure Key Vault for access from a managed identity	10 minutes

# Learning path recap

In this learning path, we learned how to:

Configure and manage authentication including MFA.

Implement Zero Trust using Conditional Access and other tools.

Create and manage identities for use with resources and applications.

