

SC-300

Tag 2

Guten Morgen!

Microsoft Identity and Access Administrator



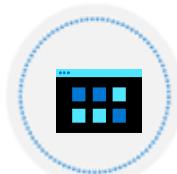
SC-300 Agenda



LP1: Implement an Identity Management Solution



LP2: Implement an Authentication and Access Management Solution



LP3: Implement Access Management for Apps



LP4: Plan and Implement an Identity Governance Strategy



gestern Lab Ø7

2 VM

DC1

AD &
on-prem

App1

Implement an Authentication and Access Management solution



Outline

LP 2



Plan and implement Azure Multifactor Authentication (MFA)

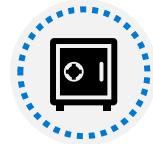


Manage user authentication



Plan, implement, and administer conditional access

CA



Manage Azure AD Identity Protection

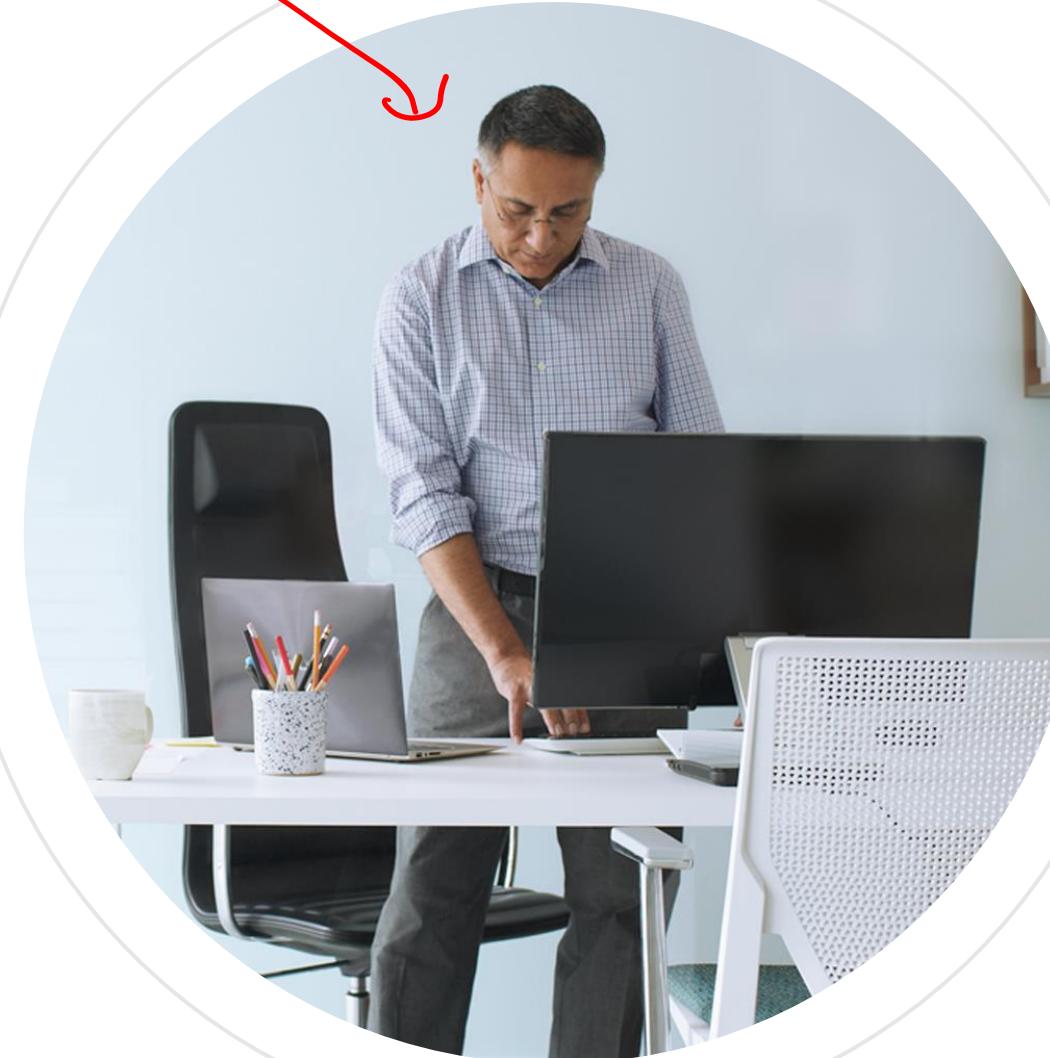


Implement access management for Azure resources



VAA
Managed ID

Secure Azure Active Directory users with multifactor Authentication



Objectives



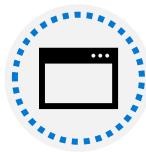
What is Azure AD multifactor Authentication?



Configure and deploy self-service password reset



Plan your multifactor authentication



Configure multifactor authentication methods

Azure AD Features to protect cloud assets

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

Always think **Zero Trust**

Always Verify – Use Least Privilege Access – Assume Breach

Identity ist der neue Perimeter! ?

What is Azure AD multifactor Authentication?



Value and Capabilities of Azure AD MFA

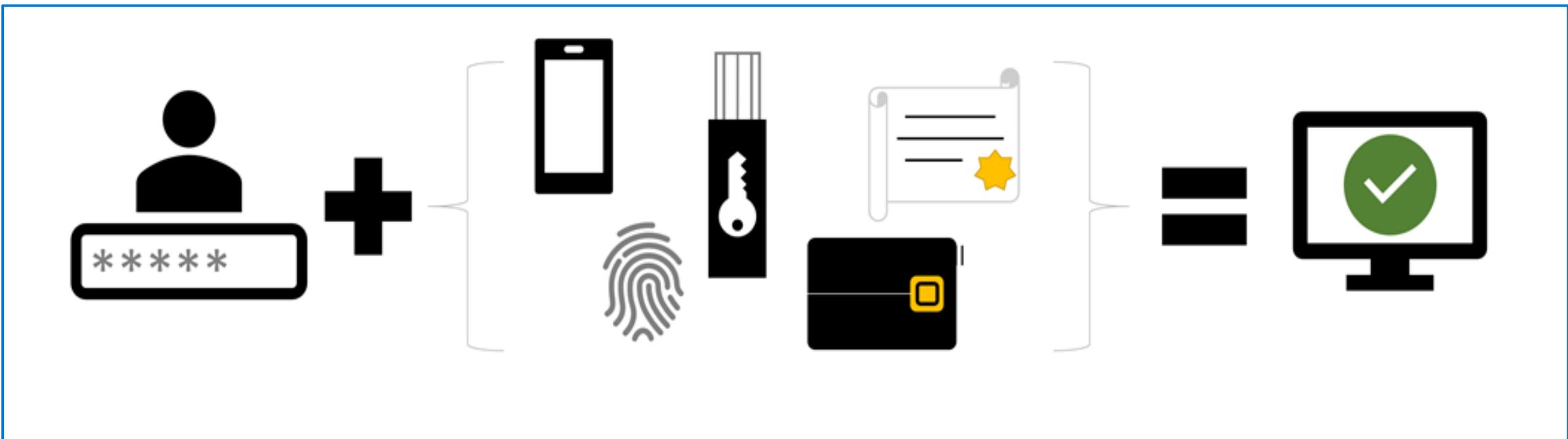
free "per user MFA"

Value

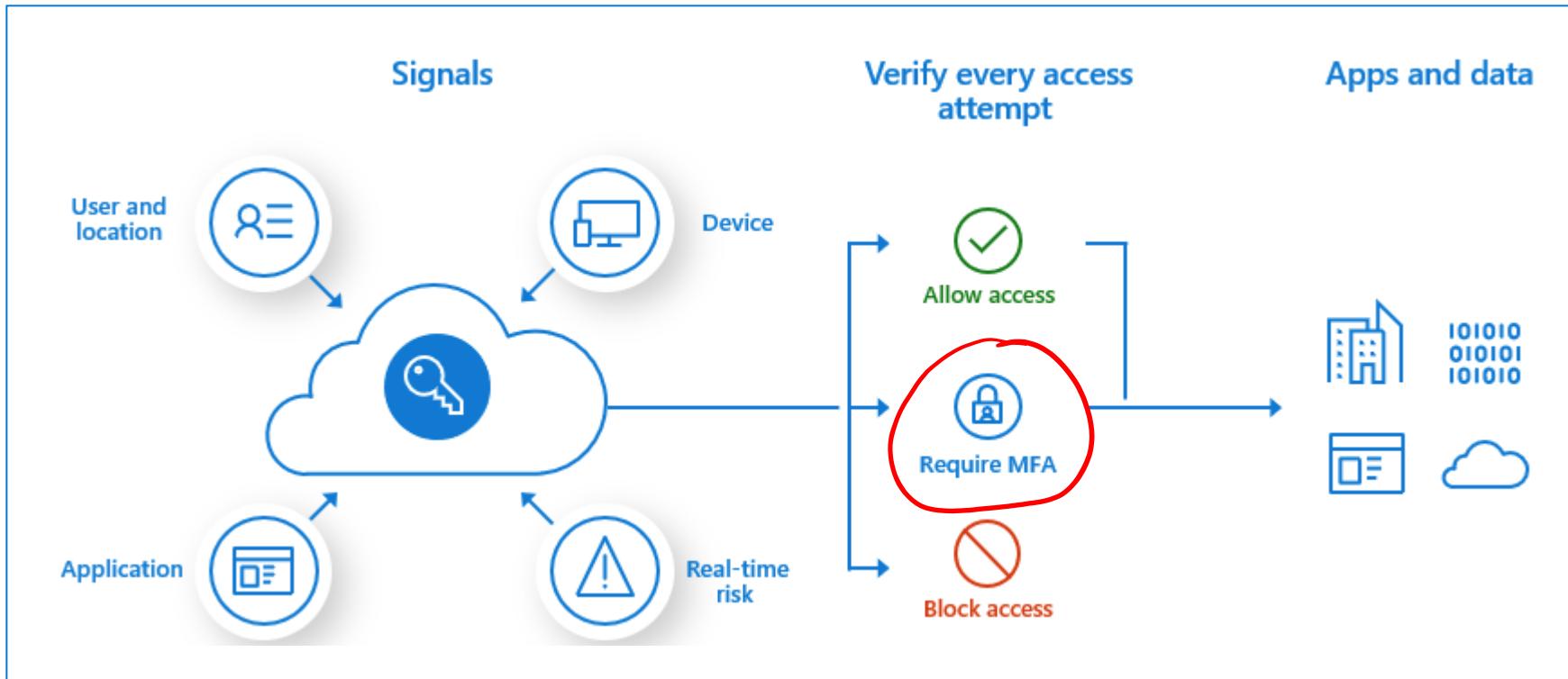
- More secure than passwords
- Quick and easy to setup and manage
- Strong Identity verification
- Stronger security
- Often support compliance goals
- Many different types of Authentication methods, with different levels of security

Categories of authentication factors

Something you know • Something you possess • Something you are



Enabling MFA with Conditional Access



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 Azure AD MFA based on the infrastructure

Cloud Only setup – Nothing additional required to set up Azure AD MFA

Hybrid Identity – Azure AD Connect must be deployed and synchronized / federated with your on-premises Active Directory Domain Services

Need on-premises legacy apps – Azure AD Proxy must be deployed.

Use Azure AD MFA with a RADIUS Authentication – A Network Policy Server (NPS) must be set up and configured

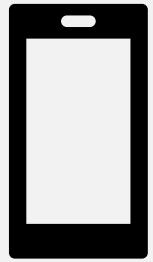
Plan your multifactor authentication deployment



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

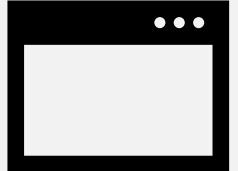


Call to a
phone



Text message
to a phone
SMS

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

The screenshot shows a Microsoft web page titled "Additional security verification". At the top, there's a Microsoft logo and a search bar. Below the title, a sub-header reads "Secure your account by adding phone verification to your password. View video to know how to secure your account". A section titled "Step 1: How should we contact you?" contains a dropdown menu set to "Authentication phone", a "Select your country or region" dropdown, and a "Method" section with two options: "Send me a code by text message" (unchecked) and "Call me" (checked). A note at the bottom states "Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply." A blue "Next" button is located on the right side.

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone ▾

Select your country or region ▾

Method

Send me a code by text message

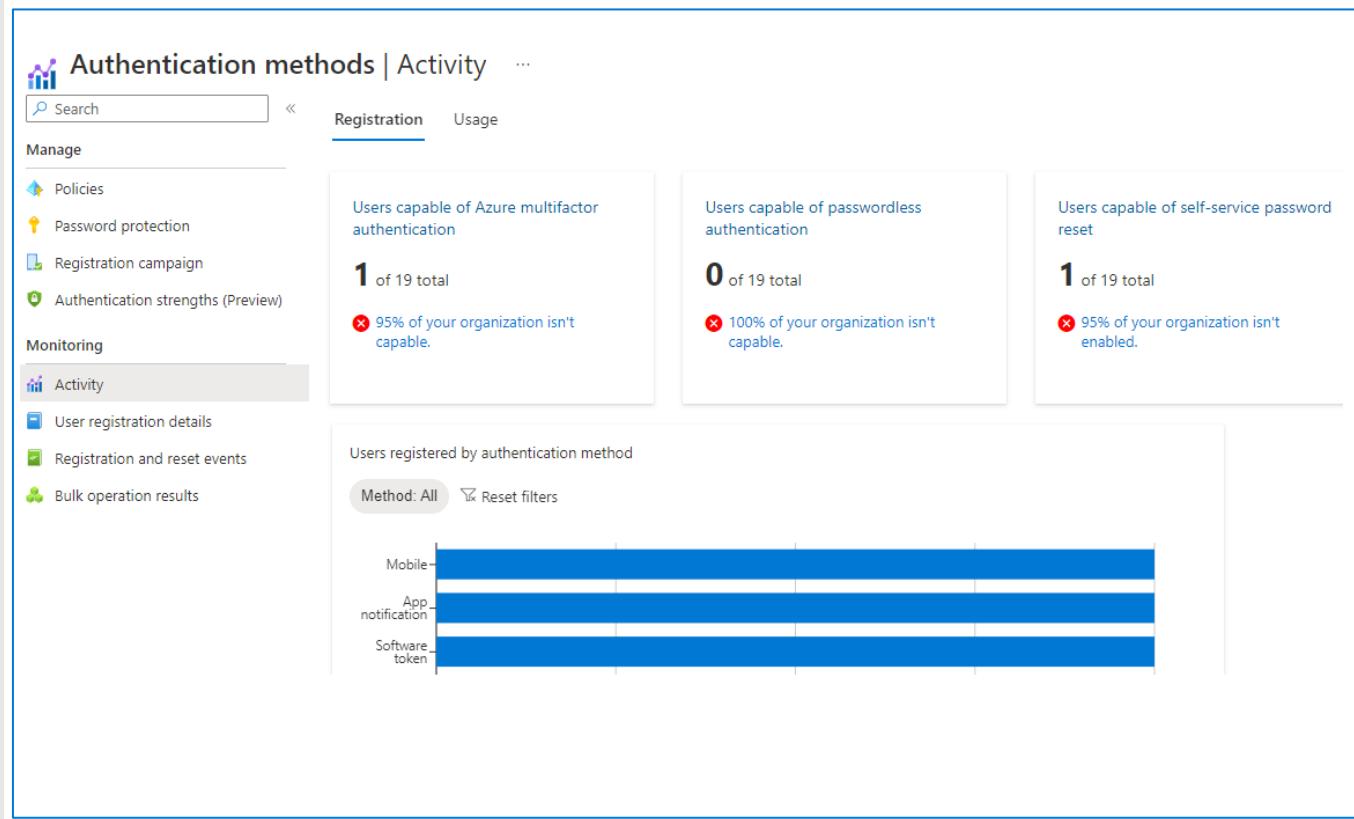
Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Next

Monitoring adoption

- Azure AD 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.

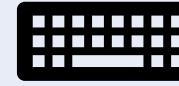


Configure and deploy self-service password reset



SSPR

Azure AD self-service password reset

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

Enabling SSPR

The screenshot shows the Azure Active Directory portal with the URL [https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/PasswordResetManagementBlade/Properties](#). The page title is "Contoso - Azure Active Directory". The left sidebar includes links for Home, Contoso, Password reset - Properties, Diagnose and solve problems, Manage (Properties selected), Authentication methods, Registration, Notifications, Customization, On-premises integration, Activity (Audit logs, Usage & insights), Troubleshooting + Support (New support request), and Help.

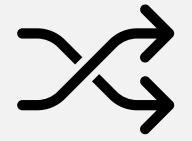
In the main content area, the "Password reset - Properties" blade is open. It shows the "Self service password reset enabled" setting is set to "Selected". A note below states: "These settings only apply to end users in your organization and are required to use two authentication methods to password policies."

A modal window titled "Default password reset policy" is displayed. It lists three groups: "SSPR-MFA-Converged-Registration" (disabled), "SSPR-Test-Group" (selected and highlighted with a red circle), and "Windows 10 Devices". The "Selected group" section shows "SSPR-Test-Group" with a "Remove" button. A "Select" button is at the bottom right of the modal.

SSPR Licensing options

Feature	Azure AD Free	Microsoft 365 Business Standard	Microsoft 365 Business Premium	Azure AD Premium P1 or P2
Cloud-only user password change When a user in Azure AD knows their password and wants to change it	•	•	•	•
Cloud-only user password reset When a user in Azure AD has forgotten their password		•	•	•
Hybrid user password change or reset with on-prem writeback When a user in Azure AD that's synchronized from an on-premises directory using Azure AD Connect			•	•

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 Windows Intune or Windows Intune Enrollment (seen in picture).
- 2) Policy within Intune device settings

The screenshot shows the 'New Conditional Access policy' page. The 'Cloud apps or actions' section is highlighted in grey. A callout box labeled 'Grant' details the configuration:

- Control access enforcement to block or grant access:** Grant access is selected.
- Require multifactor authentication:** Selected.
- For multiple controls:** Require all the selected controls is selected.

Other options like 'Require device to be marked as compliant' and 'Require password change' are not selected. The 'Access controls' section shows 'Grant' selected with 1 control selected. The 'Session' section shows 0 controls selected. The 'Enable policy' section has the toggle set to 'On'. The 'Create' button is at the bottom.

Protecting Azure AD from device attacks

Monitor the device:

- Device registration and Azure AD join
- Non-compliant devices accessing applications
- BitLocker key retrieval
- Device administrator roles
- Sign-ins to virtual machines

Logs with device data:

- Azure AD 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 Azure AD MFA activity

Use the Azure AD 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?

User – Sign-ins report

The screenshot shows the 'Users | Sign-ins' report in the Azure portal. The left sidebar has a red box around the 'Sign-ins' link under the 'Activity' section. The main area shows a table of sign-in logs for the last month. A second red box highlights the 'Authentication Details' tab in the event details section at the bottom.

Date	Request ID	User	Application	Status	IP address	Location	Conditional access
5/15/2020, 10:44:55 AM	7172730c-ccfb-4576-8...	Bala Sandhu	Azure Portal	Success	73.254.185.87	Renton, Washington, US	Success
5/14/2020, 1:15:57 PM	57675637-14d5-4a03-a...	Bala Sandhu	Azure Portal	Success	73.254.185.87	Renton, Washington, US	Success
5/14/2020, 11:07:45 AM	dcf691d-7475-4005-9...	Alain Charon	Azure Portal	Success	74.42.13.223	Tacoma, Washington, US	Success
5/13/2020, 3:38:56 PM	0109afbc-2b48-4f8d-8c...	Bala Sandhu	Azure Portal	Success	73.254.185.87	Renton, Washington, US	Success
5/13/2020, 3:23:25 PM	bb641f5b-5559-4e91-9...	Tommy Weber	Azure Portal	Success	114.13.196.31	Redmond, Washington, US	Success

Details

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	Additional Details
Date	Authentication method	Authentication method...	Succeeded	Result detail	Requirement	
5/14/2020, 1:15:57 PM			false	MFA requirement satisfied by claim in the token	MultiConditionalAccess	

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

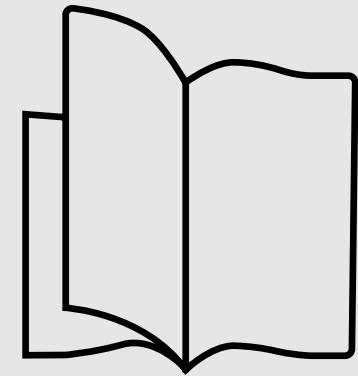
References

Planning a cloud-based Azure AD multifactor Authentication deployment

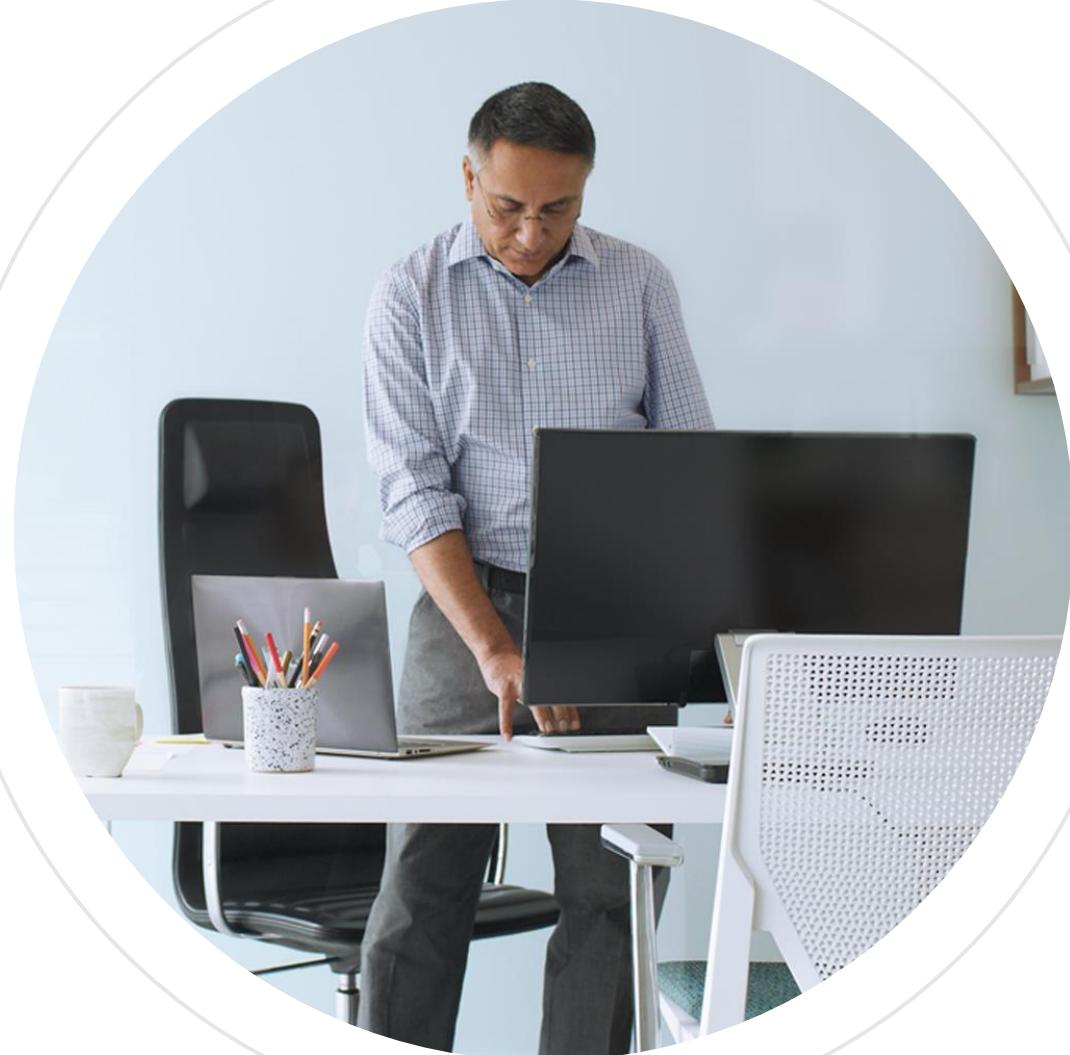
<https://docs.microsoft.com/azure/active-directory/authentication/howto-mfa-getstarted>

Deploy Azure AD self-service password reset

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



Manage user authentication



Objectives



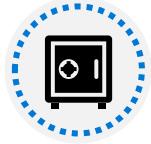
Administer authentication methods (FIDO2/Passwordless)



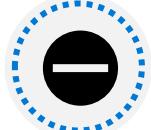
Implement an authentication solution based on Windows Hello for Business



Disable accounts and revoke sessions



Deploy and manage password protection



Configure smart lockout thresholds



Kerberos in Azure AD

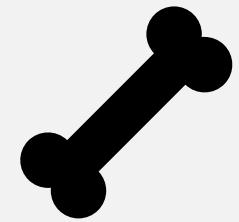


Certification based authentication

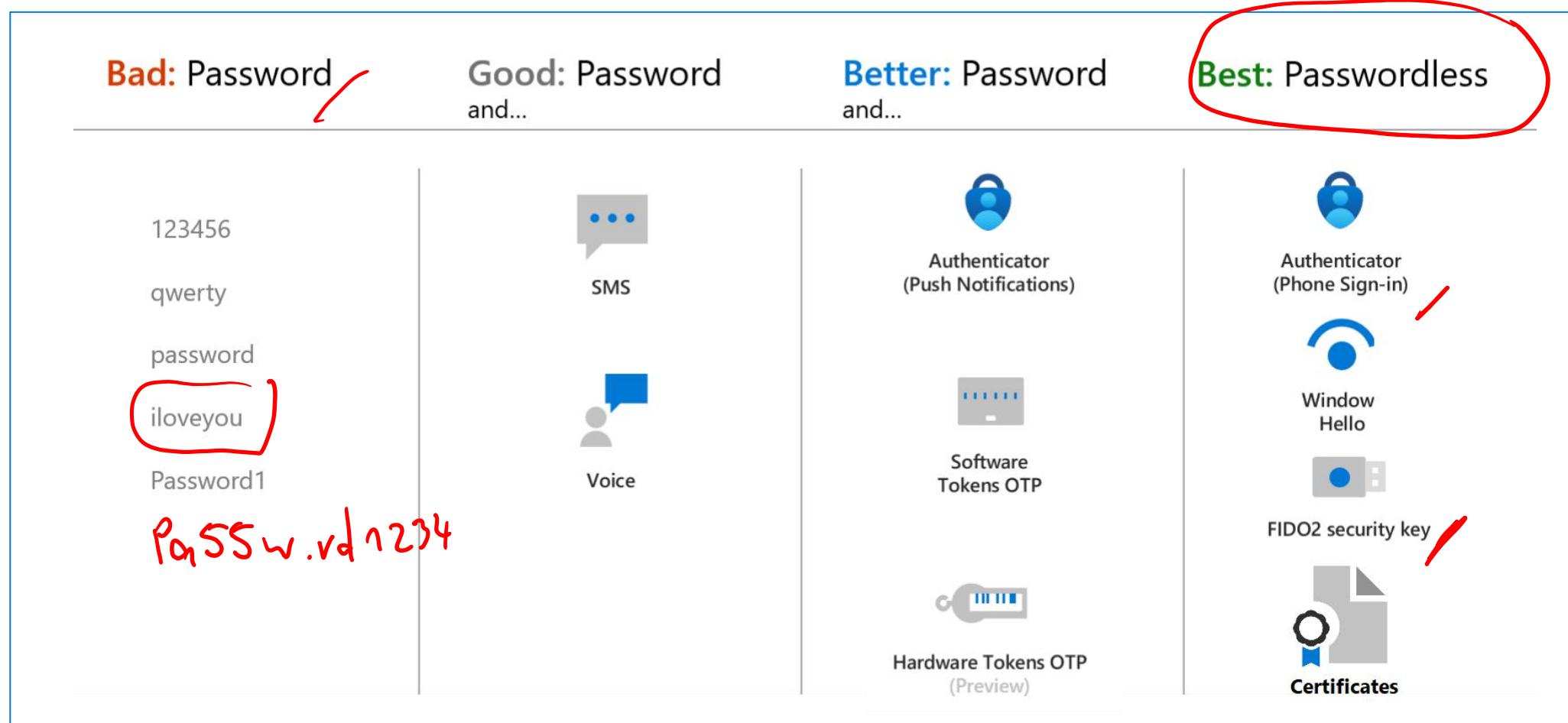


Azure AD user authentication in Virtual Machines (VMs)

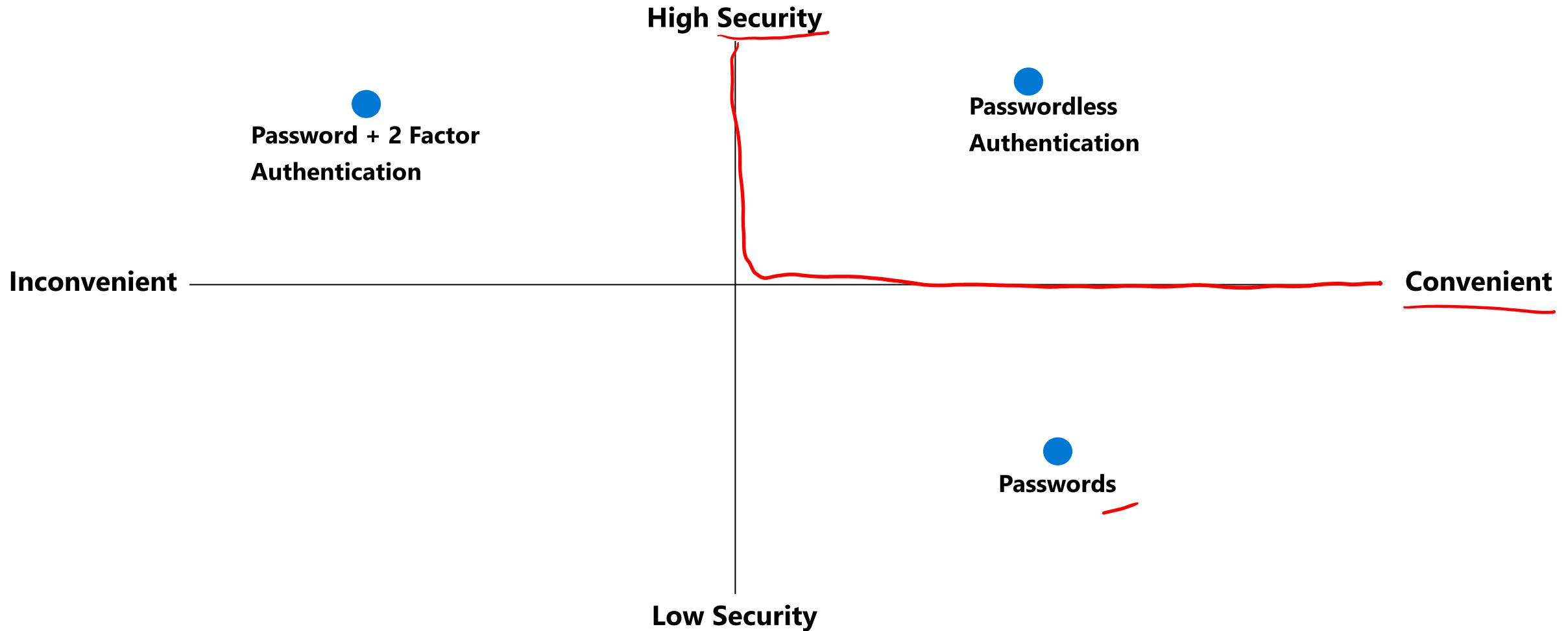
Administer authentication methods



Authentication methods

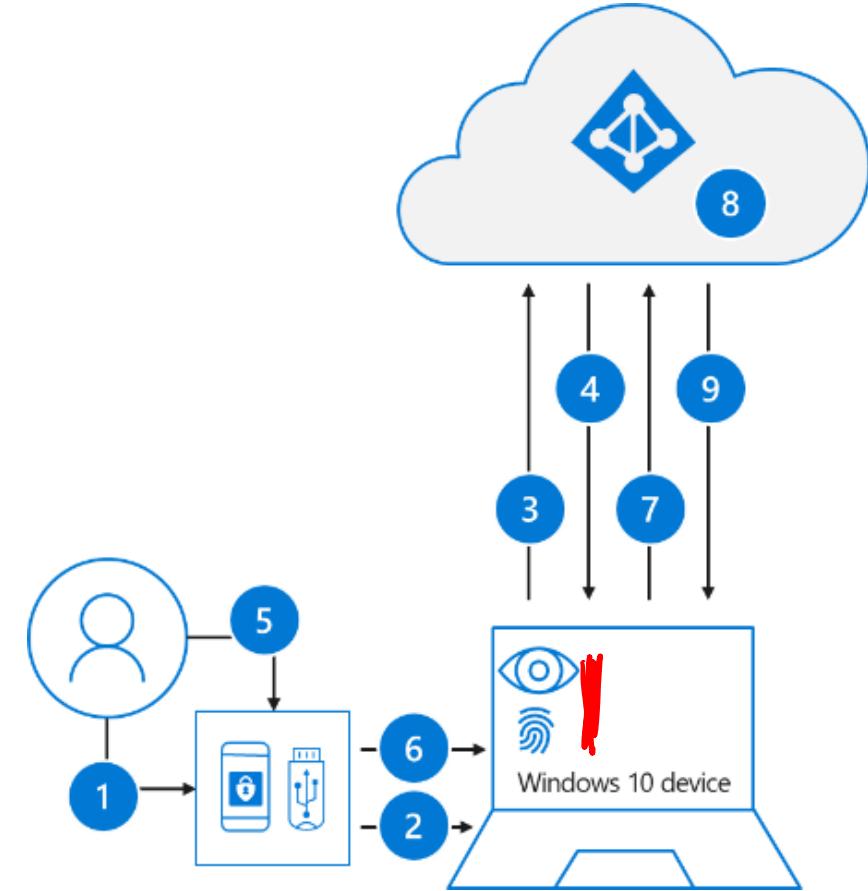


Authentication Method strength and security



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.

FIDO2 Security Key settings

Basics Configure

GENERAL

Allow self-service set up

Yes No

Enforce attestation

Yes No

KEY RESTRICTION POLICY

Enforce key restrictions

Yes No

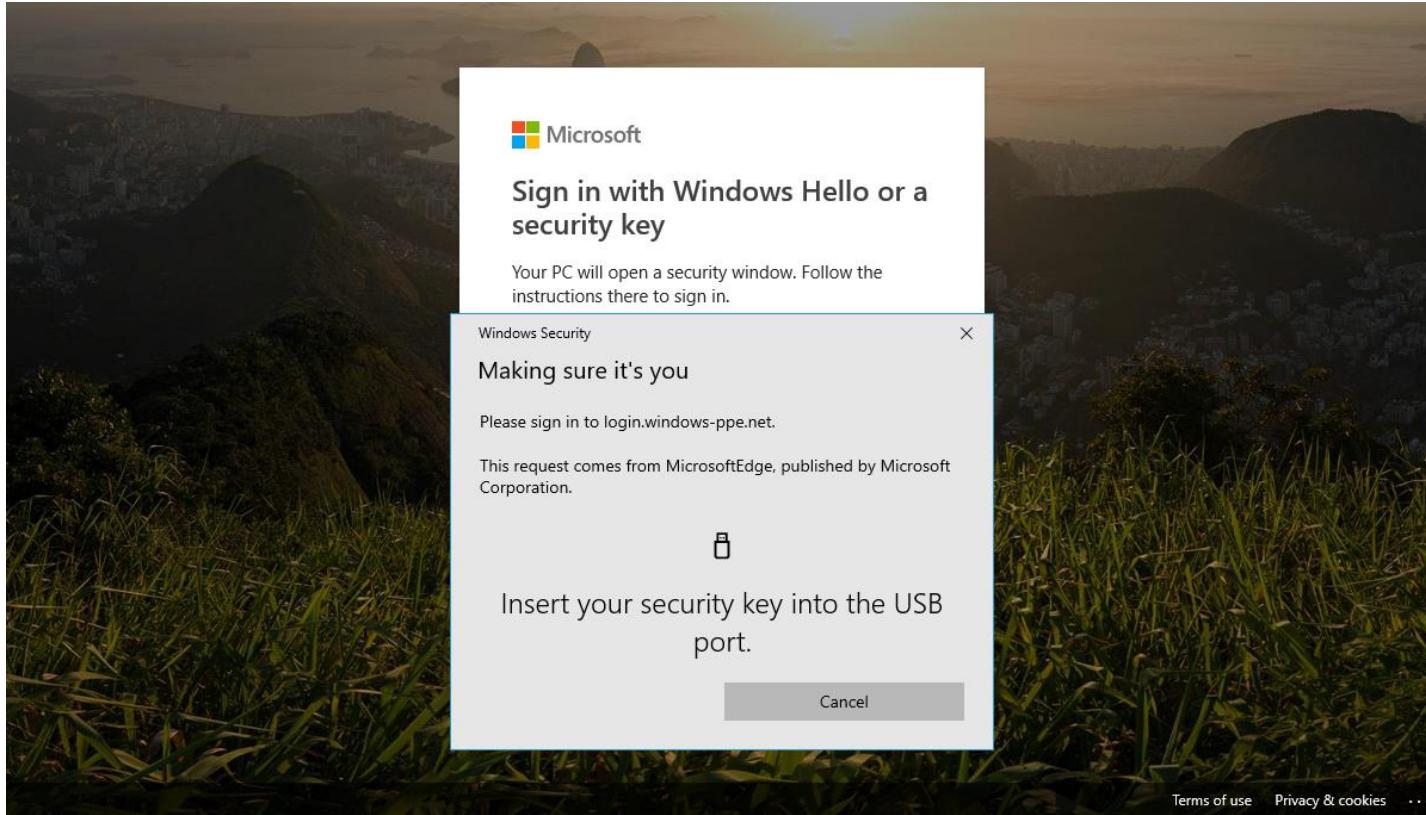
Restrict specific keys

Allow Block

[Add AAGUID](#)

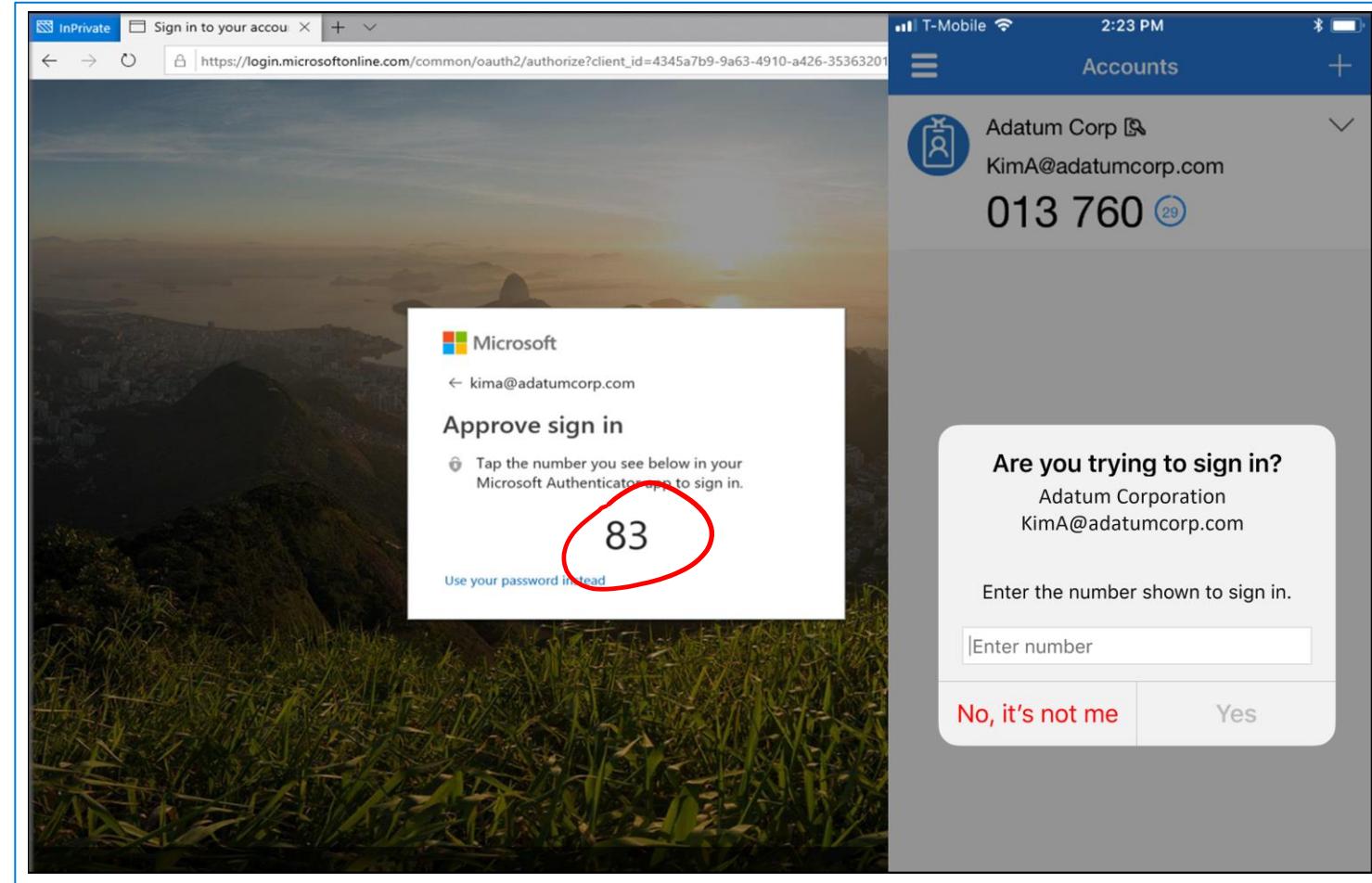
No AAGuids have been added.

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

The screenshot shows the 'Multi-Factor Authentication | OATH tokens' page in the Azure portal. The left sidebar has a 'Getting started' link, a 'Diagnose and solve problems' link, a 'Settings' section with 'Account lockout', 'Block/unblock users', 'Fraud alert', 'Notifications' (which is highlighted with a red box), and 'OATH tokens' (which is also highlighted with a red box). Below these are 'Phone call settings' and 'Providers'. The main content area has a header with 'Upload', 'Download', 'Delete', 'Refresh', 'Documentation', 'Columns', and 'Got feedback?'. It includes instructions for uploading a .csv file with columns: 'upn, serial number, secret key, time interval, manufacturer, model'. A 'Show' dropdown is set to 'All'. A table lists one OATH token entry:

Name	Username	Serial Number	Model	Manufacturer	Activated
Bala Sandhu	bala@contoso.com	1234567	HardwareKey	Contoso	Activate

OATH - Open Authentication

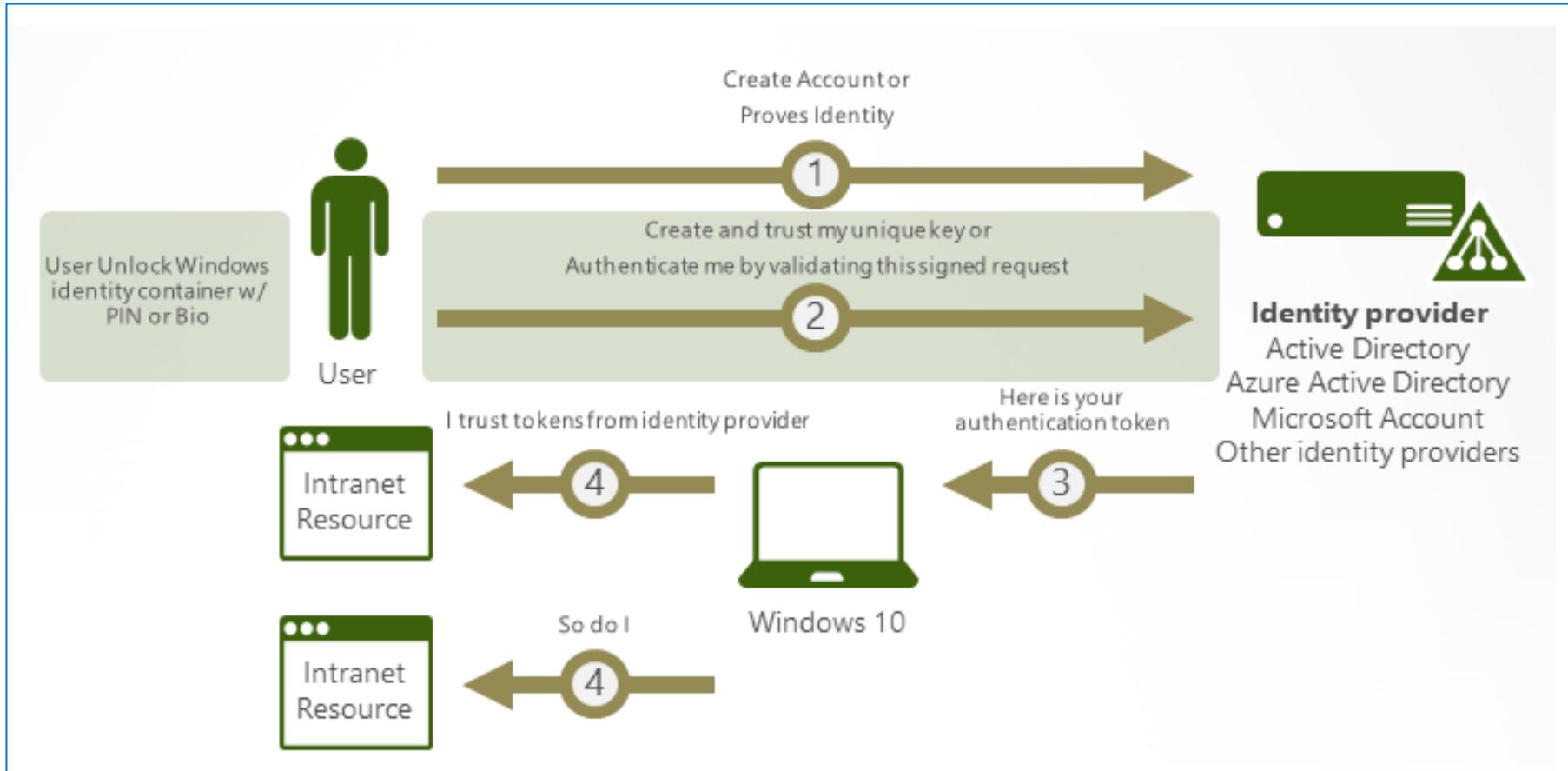
TOTP – Time-based One Time Password

Software or hardware implementations available in Azure AD

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 Active Directory, Azure AD, 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 Azure AD) 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 (Valid for 1 hour) and Refresh tokens.

Primary steps that you need to take:

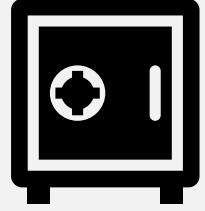
- 1) Disable the account
- 2) Reset the password
- 3) Disable any devices, tokens, or other references

Disable accounts: On-premises and Azure AD 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@sswOrd1" -Force)`
 - Recommended to run password reset twice to avoid pass-the-hash style attacks
- Azure AD 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



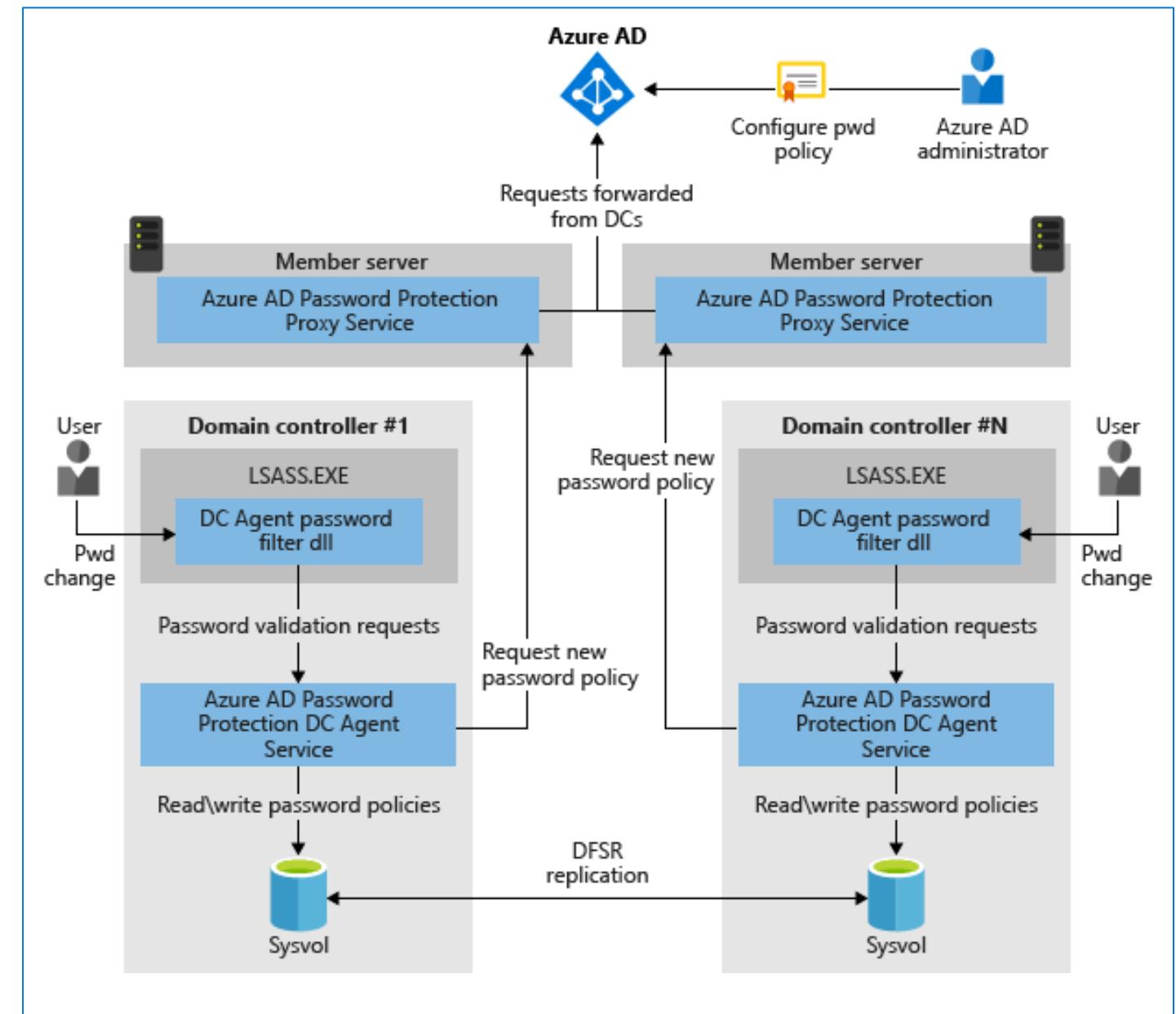
Azure AD Password Protection

Users often create easy to guess passwords that are weak against dictionary-based attacks. To help you enforce strong passwords, Azure AD 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 Azure AD features
- Incremental deployment is supported

Deployment technology

How the basic components of Azure AD 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.
- They need to inform users about the upcoming change in security enforcement, 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



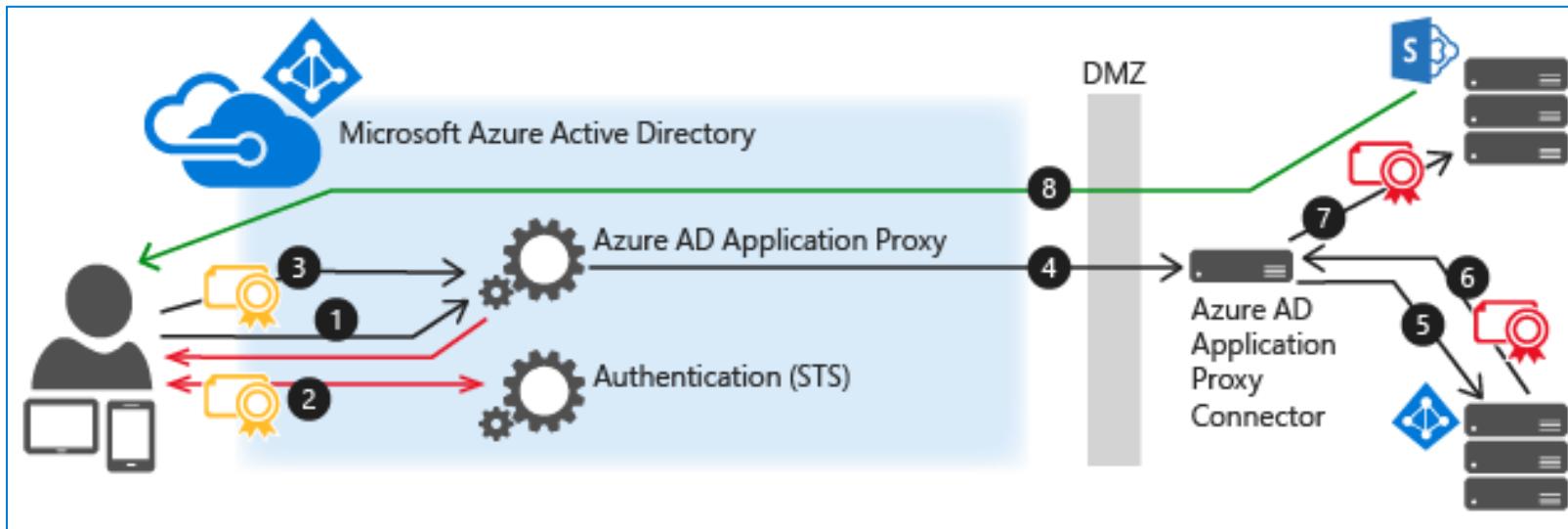
How smart lockout works

- 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 Azure AD 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

Kerberos in Azure AD



Configure Kerberos for use in Azure AD



Environment setup needed:

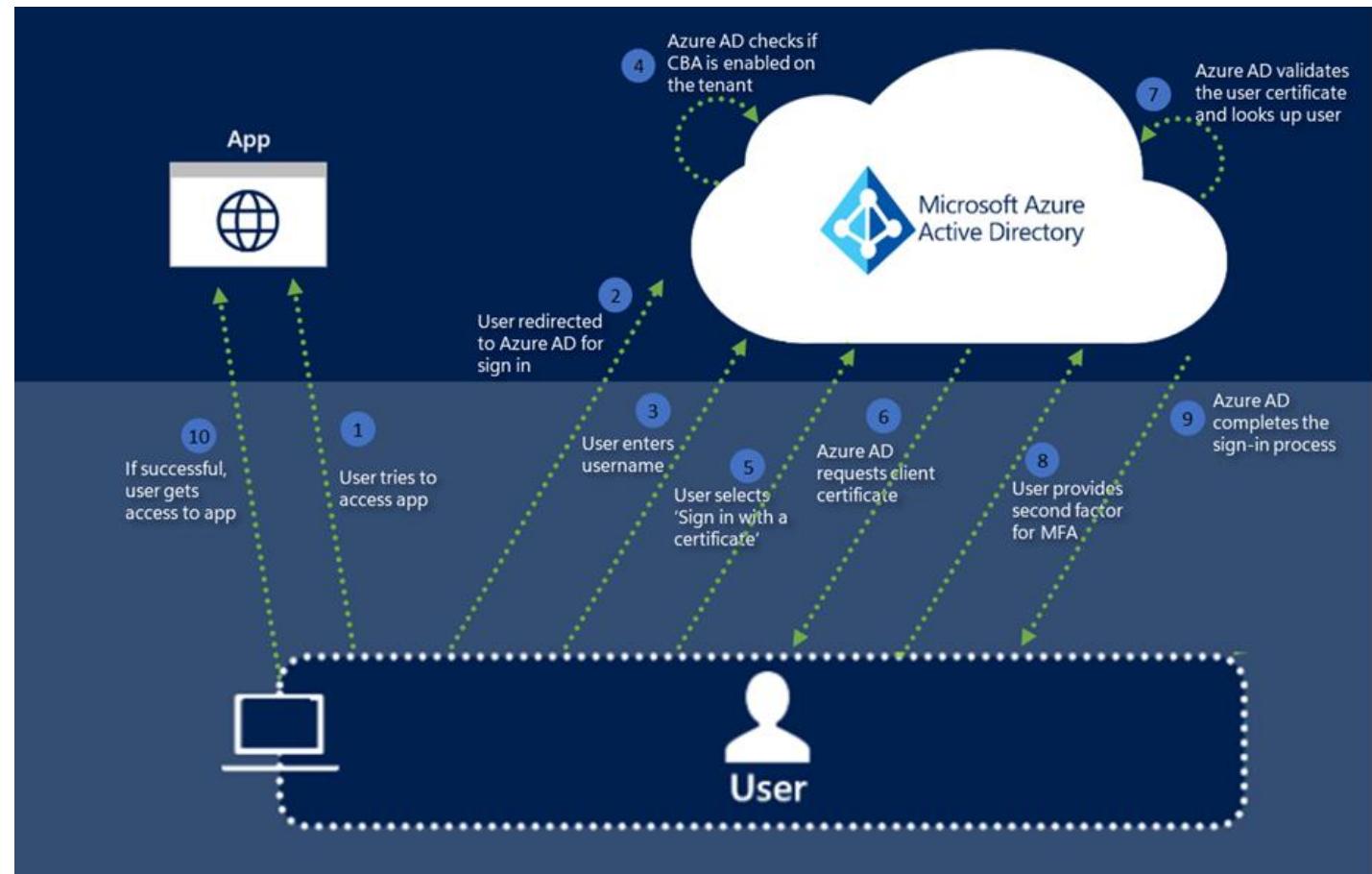
- Integrated Windows Authentication enabled on web apps
- All apps must have a Service Principal
- Server running the Kerberos connector must be in domain joined

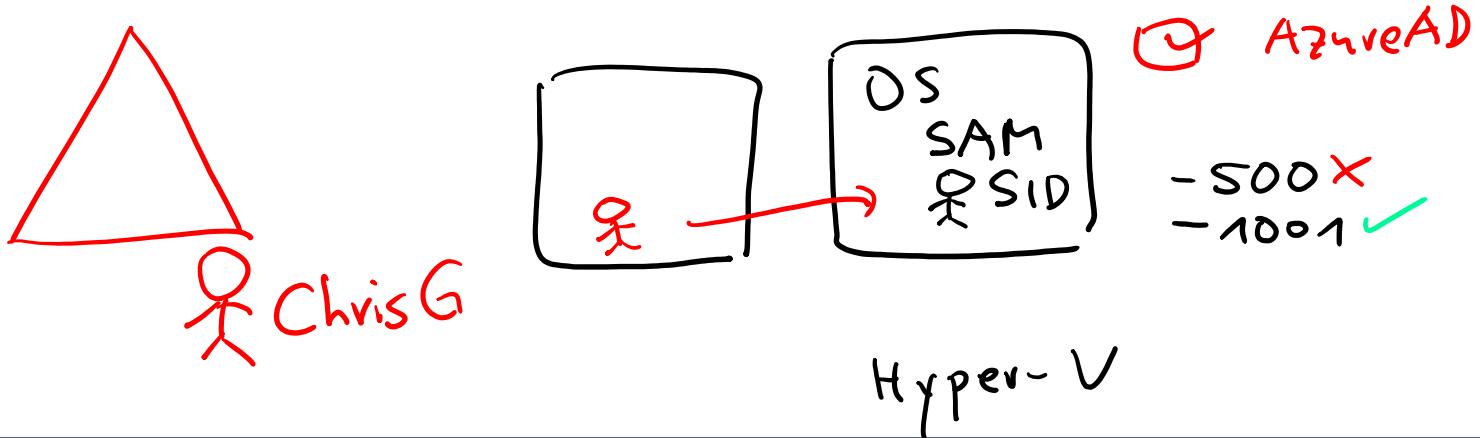
Certificate based authentication

Implement certificate-based authentication in Azure AD

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.





Azure AD user auth for VMs

Benefits of Azure AD user authentication in VMs

Benefits:

- Use Azure AD credentials to sign into Windows VMs in Azure.
- Reduce reliance on local administrator accounts.
- Password complexity and password lifetime policies configured for your Azure AD.
- 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

Azure AD

Login with Azure AD ⓘ



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

[Review + create](#)

[< Previous](#)

[Next : Advanced >](#)

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

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

Configure Azure AD sign-in for Linux VMs

You can enable Azure AD sign-in for any of the supported Linux distributions mentioned using the Azure portal. As an example, to create an Ubuntu Server 18.04 Long Term Support (LTS) VM in Azure with Azure AD 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 Azure Active Directory (Preview)**.
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 Azure Active Directory

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

Create a resilient access control management strategy with Azure Active Directory

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

Azure AD authentication methods API overview

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

Windows Hello for Business Overview

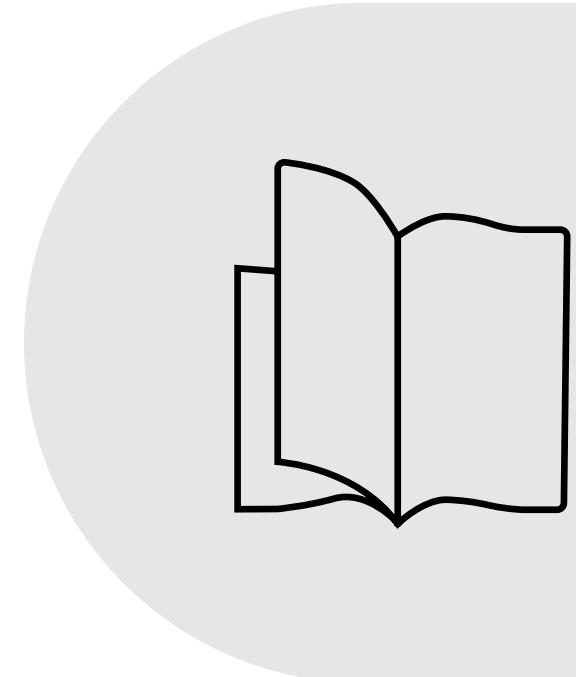
<https://docs.microsoft.com/windows/security/identity-protection/hello-for-business/hello-overview>

Authentication methods in Azure Active Directory - Microsoft Authenticator app

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

Passwordless authentication options for Azure Active Directory

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



References (2 of 2)

Authentication methods in Azure Active Directory - OATH tokens

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

Configure and enable users for SMS-based authentication using Azure Active Directory

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

Authentication methods in Azure Active Directory - phone options

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

Enforce on-premises Azure AD Password Protection for Active Directory Domain Services

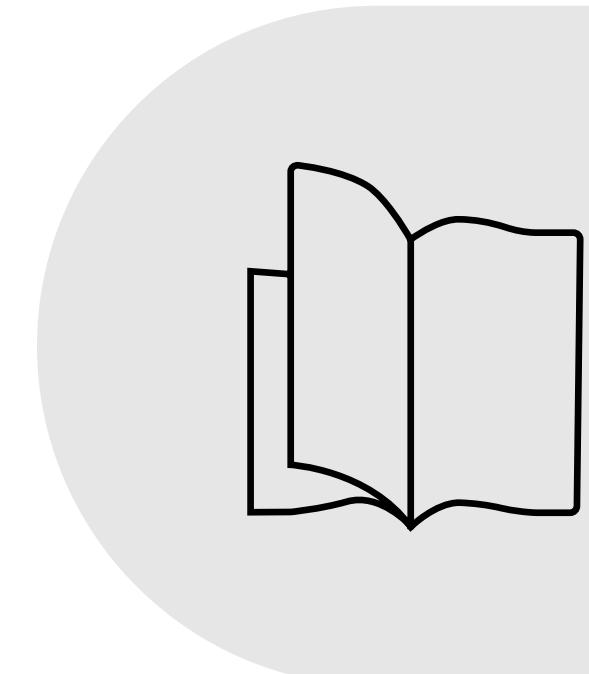
<https://docs.microsoft.com/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

Enable on-premises Azure Active Directory Password Protection

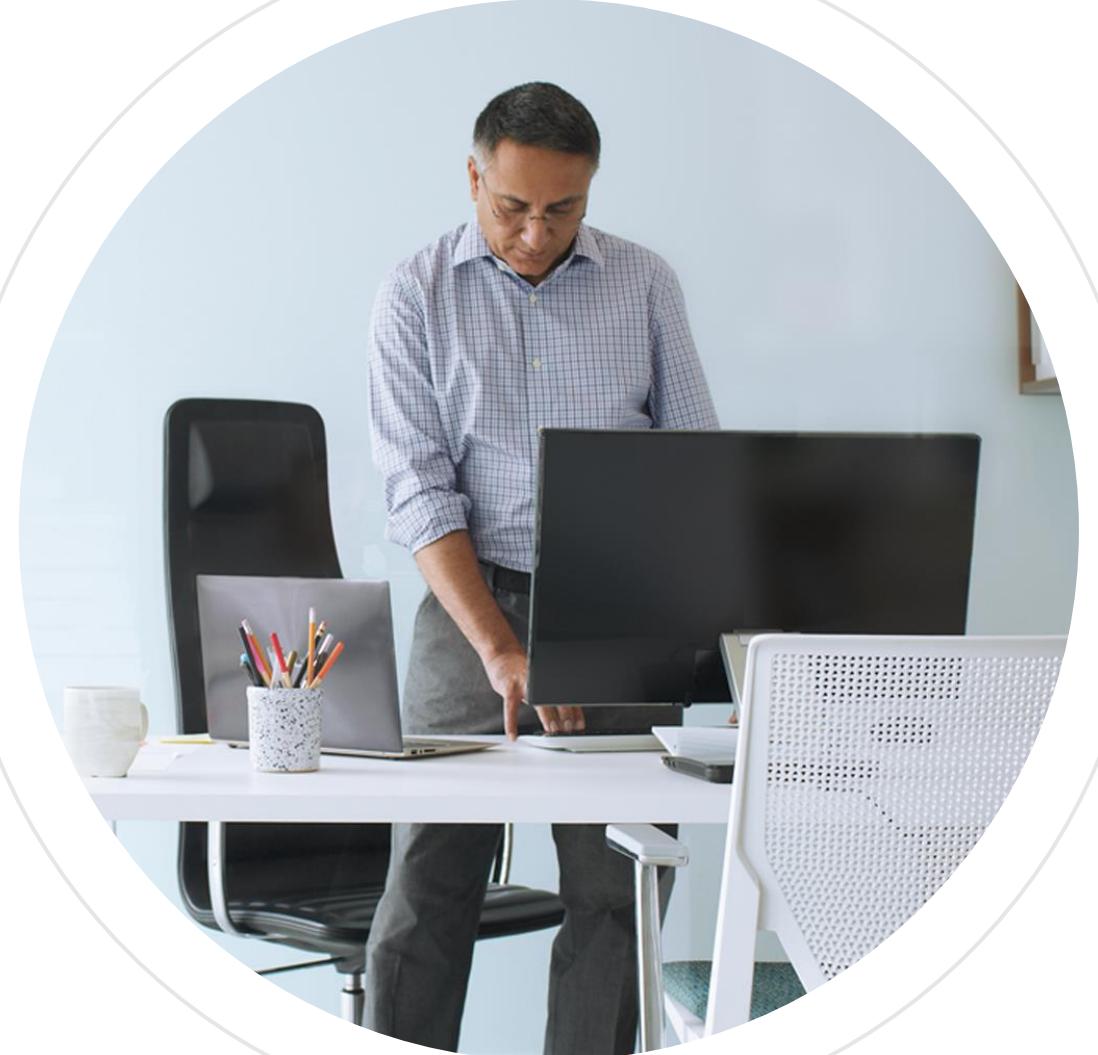
<https://docs.microsoft.com/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations>

Step-By-Step: Implementing Azure AD 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



Plan and implement security defaults



Plan conditional access policies



Implement conditional access policy controls and assignments (targeting, applications, and conditions)



Template based conditional access



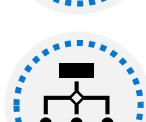
Test and troubleshoot conditional access policies



Implement application controls and session management



Continuous Access Evaluation



Authentication Context

Explore security defaults



Security defaults

The screenshot shows the Microsoft Azure Active Directory Properties page for the 'Contoso' tenant. The left sidebar lists various management options like Users, Groups, and Enterprise applications. The 'Properties' option is highlighted with a red box. The main pane displays 'Directory properties' with fields for Name (Contoso), Country or region (United States), Location (United States datacenters), and Notification language (English). A modal dialog titled 'Enable Security defaults' is open over the properties pane. This dialog contains a descriptive text about security defaults and two buttons: 'Yes' (highlighted with a red box) and 'No'. Below the modal, there's a section for 'Access management for Azure resources' where the user 'balas@contoso.com' is granted access to management groups, with 'Yes' selected. A 'Save' button is visible at the bottom right of the properties pane.

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 Azure Active Directory Licensing

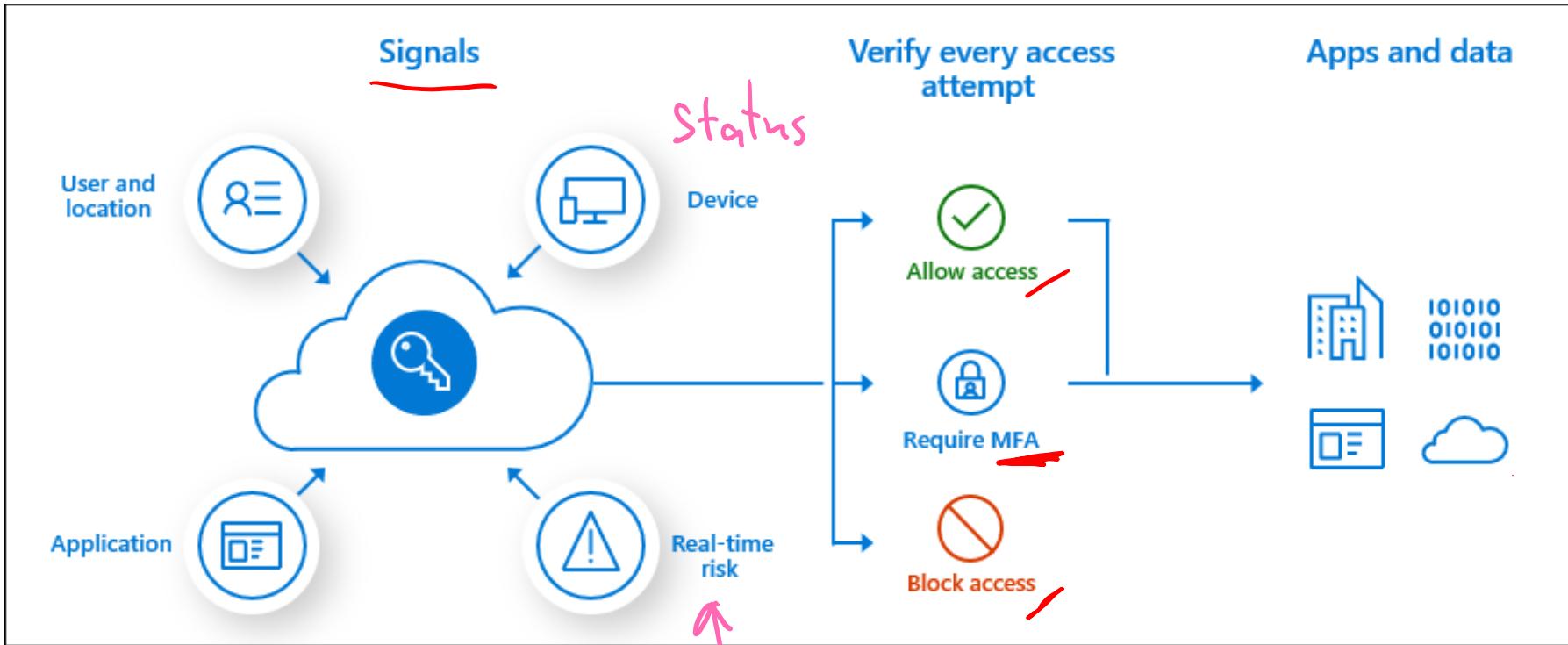
Who shouldn't use security defaults?

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

Plan conditional access policies



About conditional access policies



ID Protection

High
Medium
Low
None

Benefits of Conditional Access

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

Understanding Conditional Access policy components

New

Info

Want to switch back to the previous configuration experience? Click to leave the preview. →

Name *

Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ >
0 users and groups selected

Cloud apps or actions ⓘ >
No cloud apps or actions selected

Conditions ⓘ >
0 conditions selected

Device platforms ⓘ >
Not configured

Locations ⓘ >
Not configured

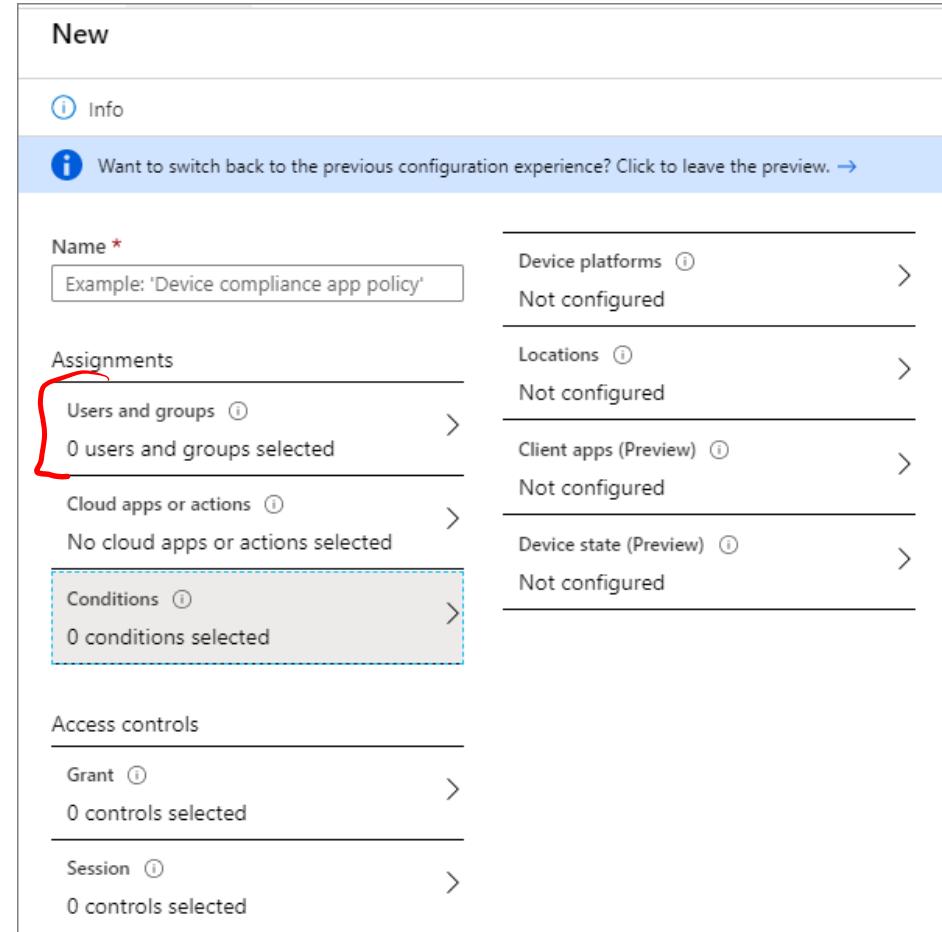
Client apps (Preview) ⓘ >
Not configured

Device state (Preview) ⓘ >
Not configured

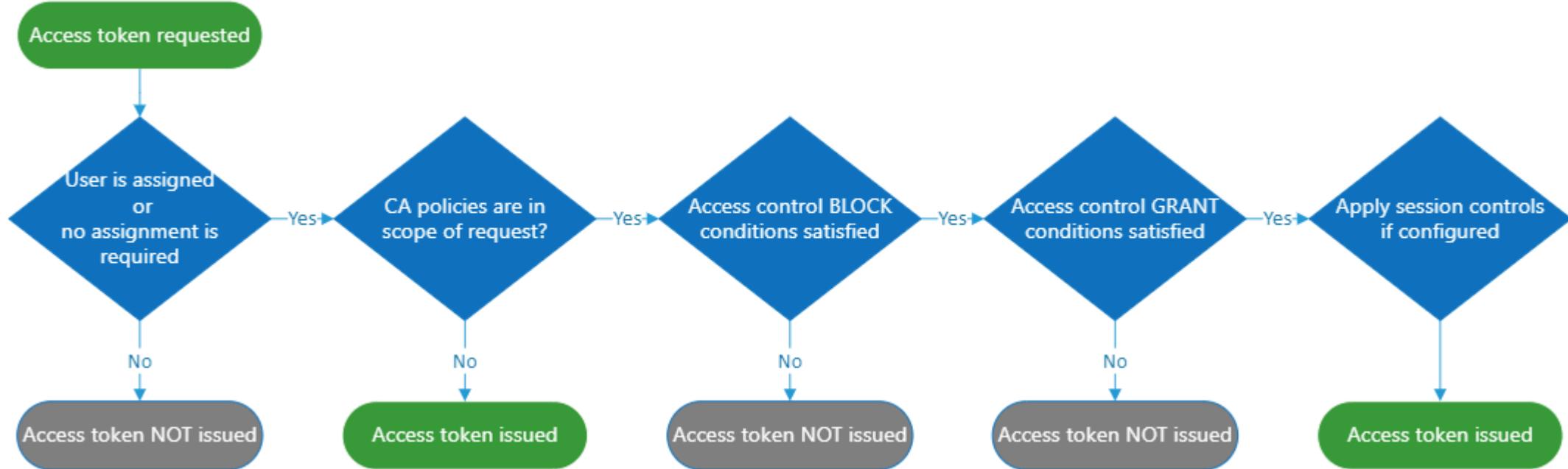
Access controls

Grant ⓘ >
0 controls selected

Session ⓘ >
0 controls selected



Access token issuance



Implement conditional access policies and assignments



Setting up Conditional Access

The screenshot displays the Microsoft Azure Conditional Access - Policies interface. On the left, a navigation sidebar under the 'Security' section includes links for 'Getting started', 'Protect' (with 'Conditional Access' selected), 'Identity Protection', 'Security Center', 'Manage' (with 'Identity Secure Score', 'Named locations', 'Authentication methods', and 'MFA'), 'Troubleshooting + Support' (with 'Troubleshoot' and 'New support request'), and 'Cloud apps or actions'. The main area shows a 'Conditional Access - Policies' page with a 'Policies' list containing four baseline policies: 'Baseline policy: Require MFA for admins (Preview)', 'Baseline policy: End user protection (Preview)', 'Baseline policy: Block legacy authentication (Preview)', and 'Baseline policy: Require MFA for Service Management (Preview)'. A prominent yellow box highlights the '+ New policy' button. To the right, a 'New' dialog box is open, allowing the creation of a new policy. It includes fields for 'Name' (example: 'Device compliance app policy'), 'Assignments' (Users and groups, Specific users included), 'Cloud apps or actions' (1 app included), 'Conditions' (1 condition selected), 'Access controls' (Grant, 1 control selected), and 'Session' (0 controls selected). The 'Enable policy' switch is set to 'On'. The 'Done' button at the bottom right of the dialog is highlighted.

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

The screenshot shows the 'Conditional Access - Policies' section in the Microsoft Azure portal. A new policy is being created with the name 'Conditional Access Documentation'. The 'Grant' access type is selected. Under 'Access controls', the 'Grant' section is expanded, showing 0 controls selected. The 'Session' section is also expanded, showing 0 controls selected. At the bottom, the 'Enable policy' switch is set to 'Off'. On the right, a sidebar titled 'Select the controls to be enforced' lists several options: 'Require multi-factor authentication' (checked), 'Require device to be marked as compliant' (unchecked and highlighted with a red box), 'Require Hybrid Azure AD joined device' (unchecked), 'Require approved client app' (unchecked), and 'Require app protection policy (Preview)' (unchecked). Below these, it says 'For multiple controls' with radio buttons for 'Require all the selected controls' (selected) and 'Require one of the selected controls'. Red handwritten annotations 'AND' and 'OR' are placed next to the respective radio buttons. A 'Create' button is at the bottom left, and a 'Select' button is at the bottom right.

Session Access control

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

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

The screenshot shows the Microsoft Conditional Access - Policies interface. A new policy named "Conditional Access Documentation" is being created under the "Session" category. The "Info" section includes a note about session controls enabling limited experiences within a cloud app, with a link to learn more. The "Assignments" section lists "Specific users included" and "1 app included". The "Conditions" section shows "0 conditions selected". The "Access controls" section shows "1 control selected" under "Grant" and "0 controls selected" under "Session". The "Enable policy" section has a switch set to "Off". At the bottom are "Create" and "Select" buttons.

Types of Conditional Access policies

- Sign-in risk-based Conditional Access
- User risk-based Conditional Access

Template based Conditional Access

Conditional Access Templates

14 policy templates:

1. Azure portal
2. Azure Active Directory
3. Security
4. Conditional Access
5. Create new policy from template

Home > Conditional Access >

Create new policy from templates ...

Customize your build Select template Review + create

We recommend the following templates based on your response

<input checked="" type="radio"/> Require multi-factor authentication for admins Require multi-factor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default. View policy summary	<input type="radio"/> Securing security info registration Secure when and how users register for Azure AD Multi-Factor Authentication and self-service password. View policy summary	<input type="radio"/> Block legacy authentication Block legacy authentication endpoints that can be used to bypass multi-factor authentication. View policy summary
<input type="radio"/> Require multi-factor authentication for guest access Require guest users perform multi-factor authentication when accessing your company resources. View policy summary	<input type="radio"/> Require multi-factor authentication for Azure management Require multi-factor authentication to protect privileged access to Azure resources. (Requires an Azure AD Premium 2 License) View policy summary	<input type="radio"/> Require multi-factor authentication for risky sign-in Require multi-factor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)

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)

Require TOU

Info Delete

* Name
Require TOU for Isabella

Assignments

Users and groups ⓘ Specific users included >

Cloud apps ⓘ 1 app included >

Conditions ⓘ 0 conditions selected >

Access controls

Grant ⓘ 1 control selected >

Session ⓘ 0 controls selected >

Enable policy

On Off

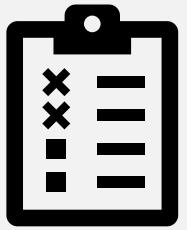
<<Select User or Group>> ...

MA Microsoft Azure Managem... ...

Grant access

My TOU

Test and troubleshoot conditional access policies



Configurations to avoid

For all users, all cloud apps:

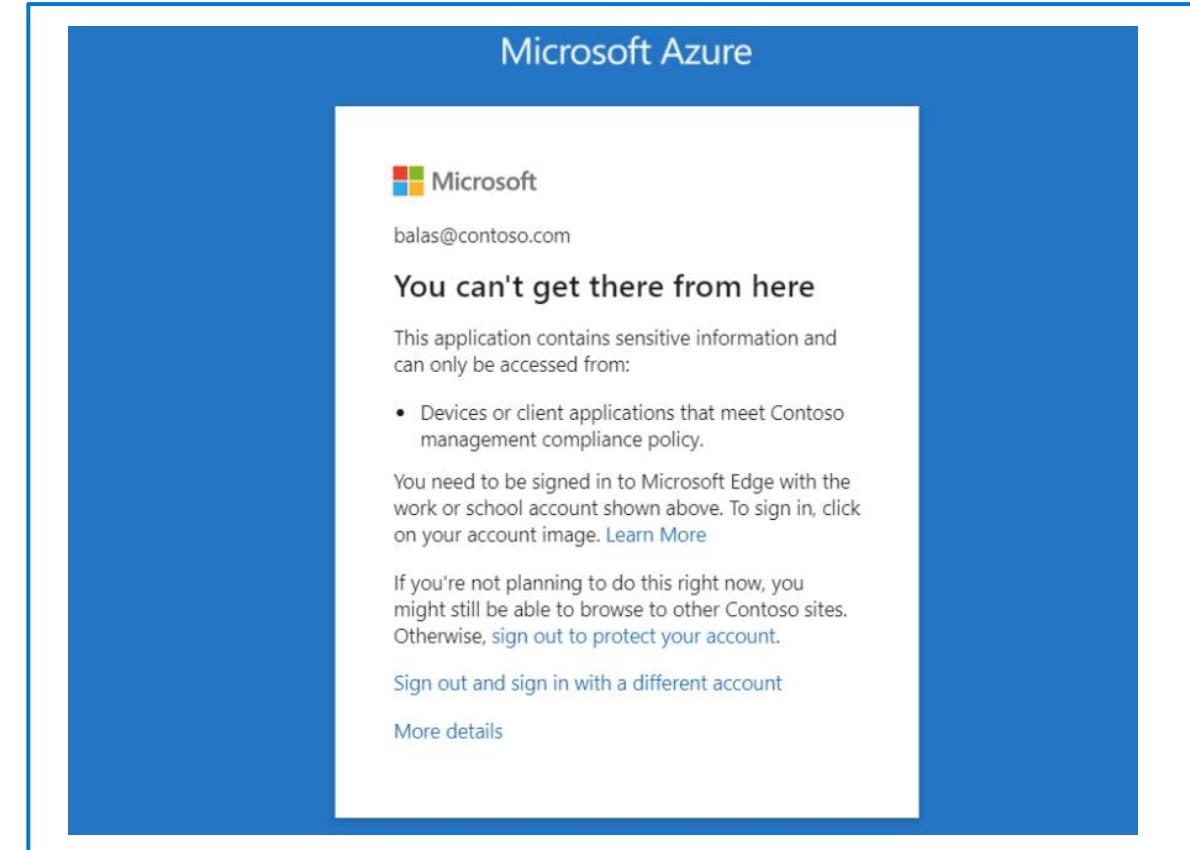
- Block access
- Require device to be marked as compliant
- Require Hybrid Azure AD domain joined device
- Require app protection policy

For all users, all cloud apps, all platforms:

- Block access

Troubleshooting sign-in interrupts

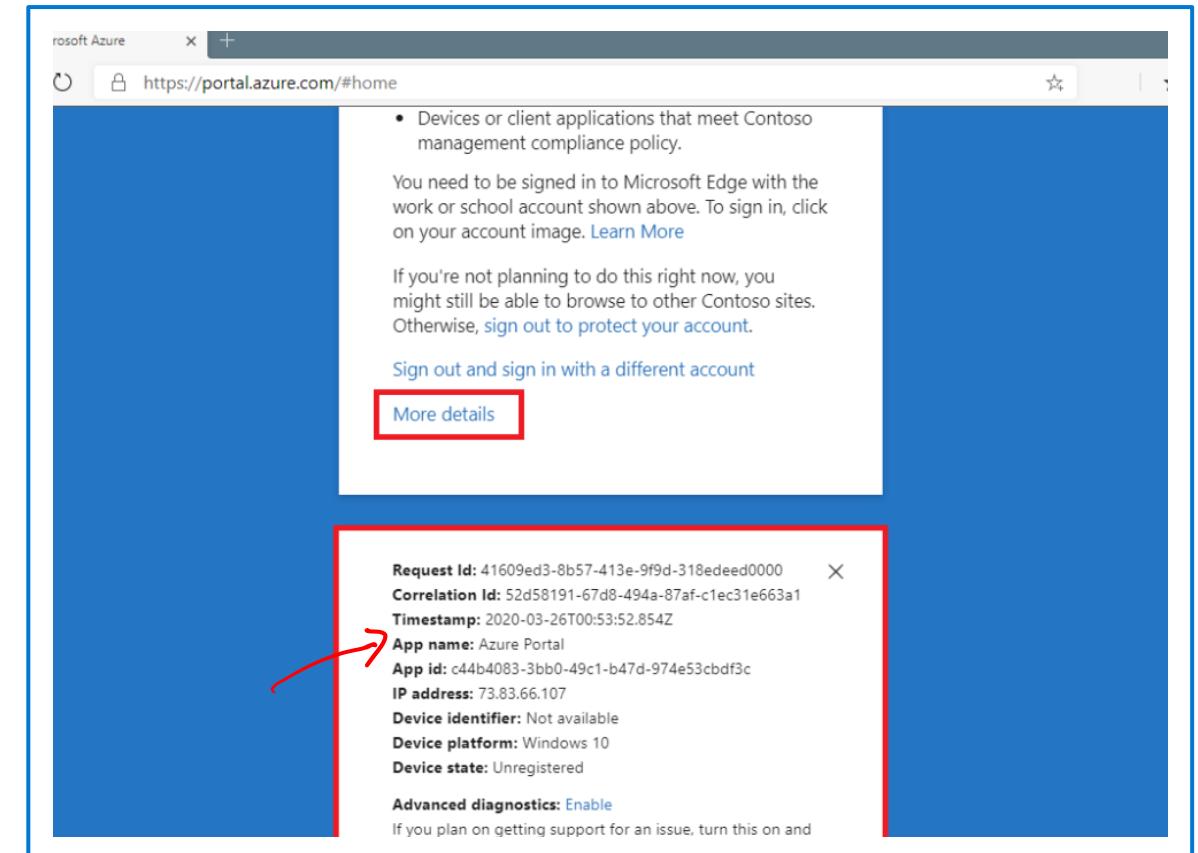
In this error, the message states that the application can only be accessed from devices or client applications that meet the company's mobile device management policy. In this case, the application and device do not meet that policy.



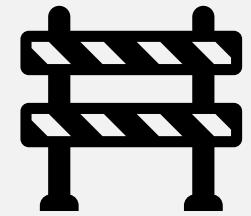
Troubleshooting Active Directory sign-in events

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 Azure AD 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

The screenshot shows the 'Session' configuration page within the Conditional Access Policies interface. A green box highlights the 'Use Conditional Access App Control' checkbox under the 'Session controls' section.

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

CA-App Control works with Microsoft Defender for Cloud Apps

Defender for Cloud
(ASC)

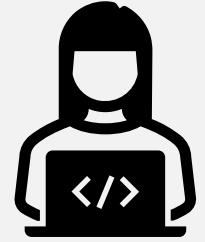
Defender M365

Cloud Id
Endpoints

Benefits of using app protection policies (MDM/MAM)

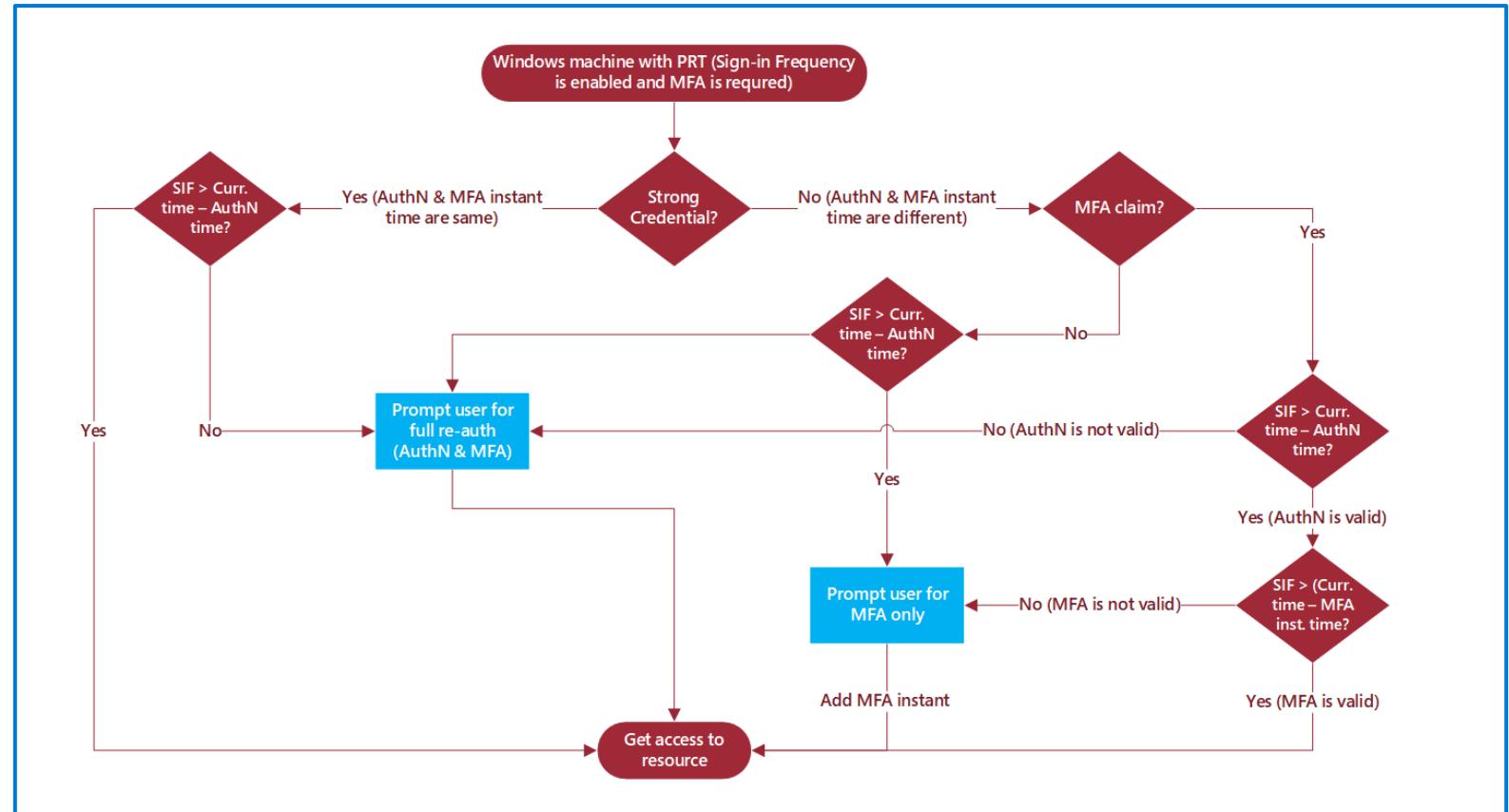
- Protecting your company data at the app level
- End-user productivity isn't affected, and policies don't apply when using the app in a personal context
- App protection policies ensure that the app-layer protections are in place
- MDM, in addition to MAM, ensures that the device is protected

Implement session management



User sign-in frequency and multifactor authentication

Sign-in frequency previously applied only to the first factor authentication on devices that were Azure AD joined, Hybrid Azure AD joined, and Azure AD registered. There was no easy way for our customers to reinforce multifactor authentication (MFA) on those devices. Based on customer feedback, sign-in frequency will apply for MFA as well



Validation

Use the What-If tool to simulate a login from the user to the target application and 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

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

* User [i](#)
bala@contoso.com

Cloud apps [i](#)
1 apps selected

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

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

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

Client apps (preview) [i](#)
Mobile apps and desktop clients - Modern authentication clients

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

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

What If **Reset**

Evaluation result

Policies that will apply Policies that will not apply

POLICY NAME	GRANT CONTROLS
Sign-in frequency	

SESSION CONTROLS

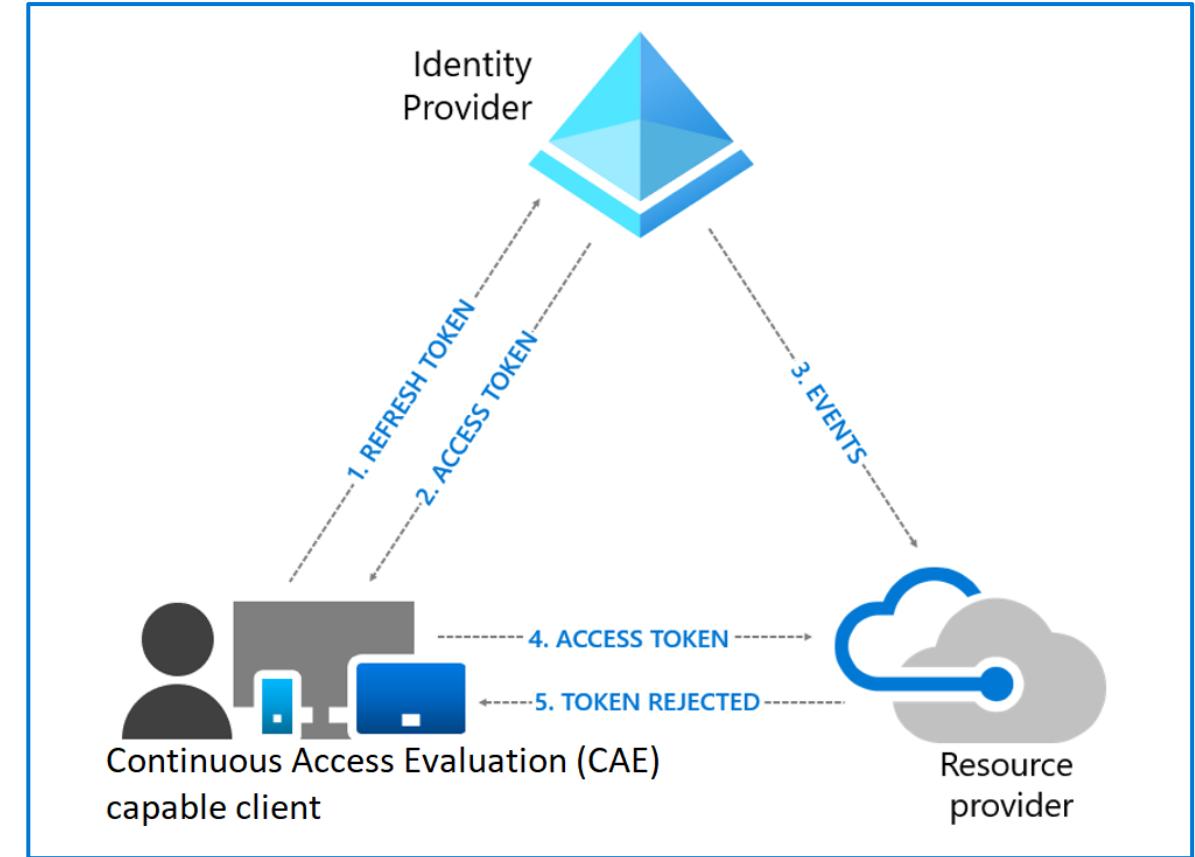
Persistent browser session (preview) - N... [...](#)

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.

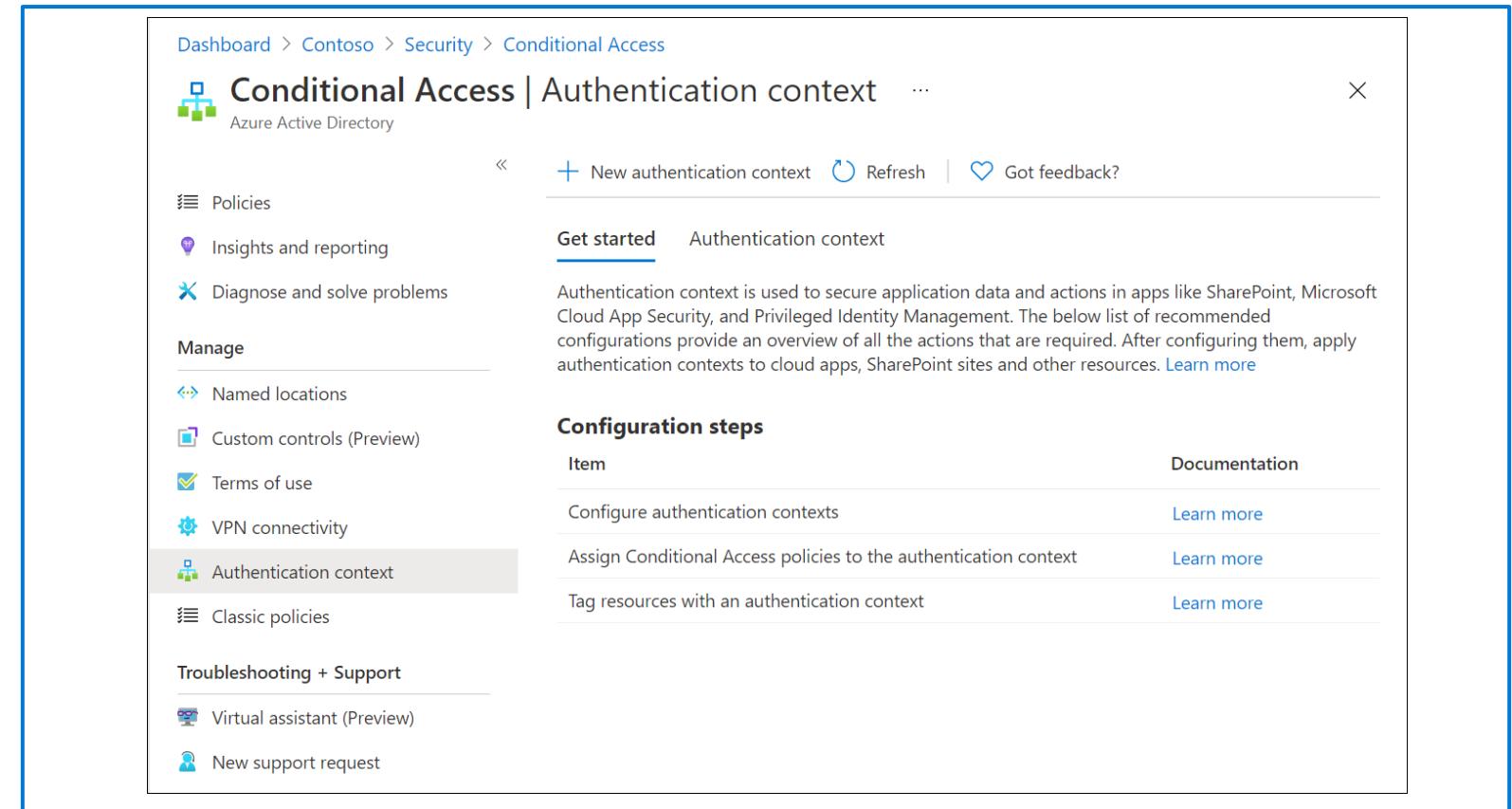


Authentication context



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 'Conditional Access | Authentication context' page in the Azure Active Directory portal. The left sidebar includes links for Policies, Insights and reporting, Diagnose and solve problems, Manage (with sub-links for Named locations, Custom controls (Preview), Terms of use, VPN connectivity, and Authentication context), Classic policies, Troubleshooting + Support (with sub-links for Virtual assistant (Preview) and New support request), and a navigation bar with Dashboard, Contoso, Security, and Conditional Access. The main content area displays the 'Get started' section, which explains that authentication context is used to secure application data and actions in apps like SharePoint, Microsoft Cloud App Security, and Privileged Identity Management. It lists recommended configurations: 'Configure authentication contexts', 'Assign Conditional Access policies to the authentication context', and 'Tag resources with an authentication context'. Each item has a 'Learn more' link and a 'Documentation' column.

Dashboard > Contoso > Security > Conditional Access

Conditional Access | Authentication context

Azure Active Directory

Policies

- Insights and reporting
- Diagnose and solve problems

Manage

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

Classic policies

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

« + New authentication context Refresh Got feedback? X

Get started Authentication context

Authentication context is used to secure application data and actions in apps like SharePoint, Microsoft Cloud App Security, and Privileged Identity Management. The below list of recommended configurations provide an overview of all the actions that are required. After configuring them, apply authentication contexts to cloud apps, SharePoint sites and other resources. [Learn more](#)

Configuration steps

Item	Documentation
Configure authentication contexts	Learn more
Assign Conditional Access policies to the authentication context	Learn more
Tag resources with an authentication context	Learn more

References (1 of 2)

What is Conditional Access?

<https://www.youtube.com/watch?v=ffMAw2IV07A>

How to deploy Conditional Access

https://www.youtube.com/watch?v=c_izIRNJNuk

How to roll out CA policies to end users

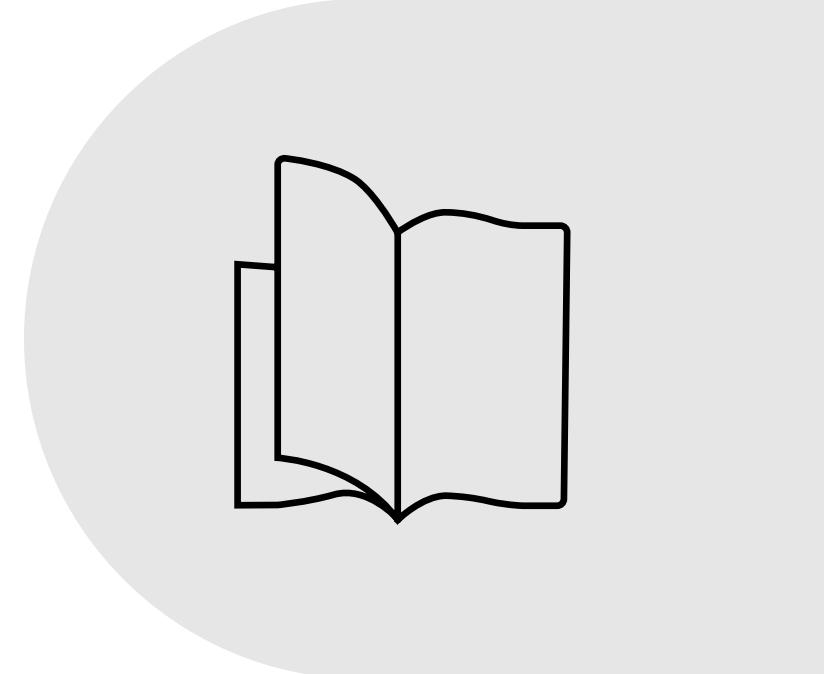
https://www.youtube.com/watch?v=0_Fze7Zpyvc

Conditional Access with device controls

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

Conditional Access with Azure AD MFA

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



References (2 of 2)

Conditional Access in Enterprise Mobility + Security

<https://www.youtube.com/watch?v=A7lrxAH87wc>

Using the location condition in a Conditional Access policy

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

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

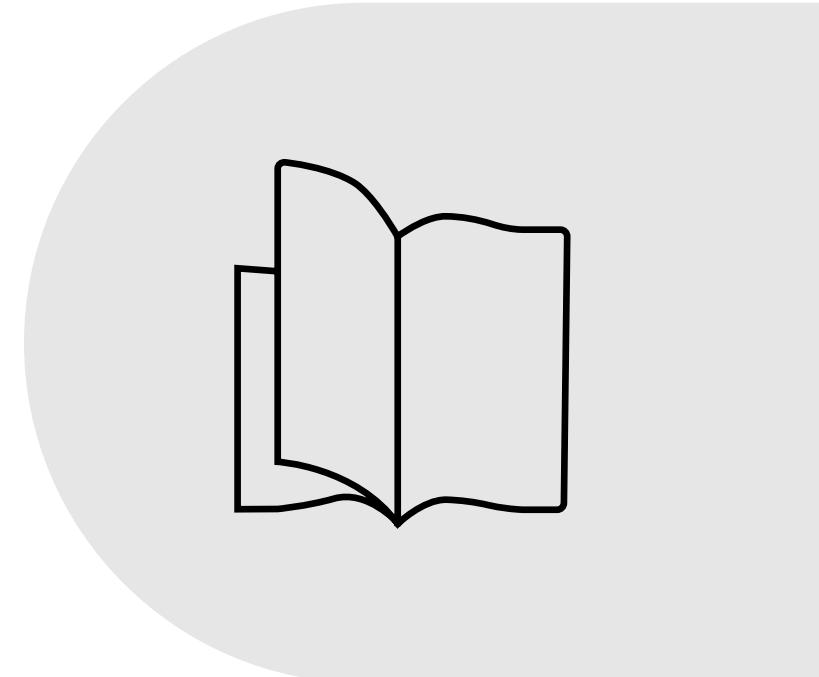
<https://docs.microsoft.com/mem/intune/protect/device-compliance-get-started>

Introducing security defaults

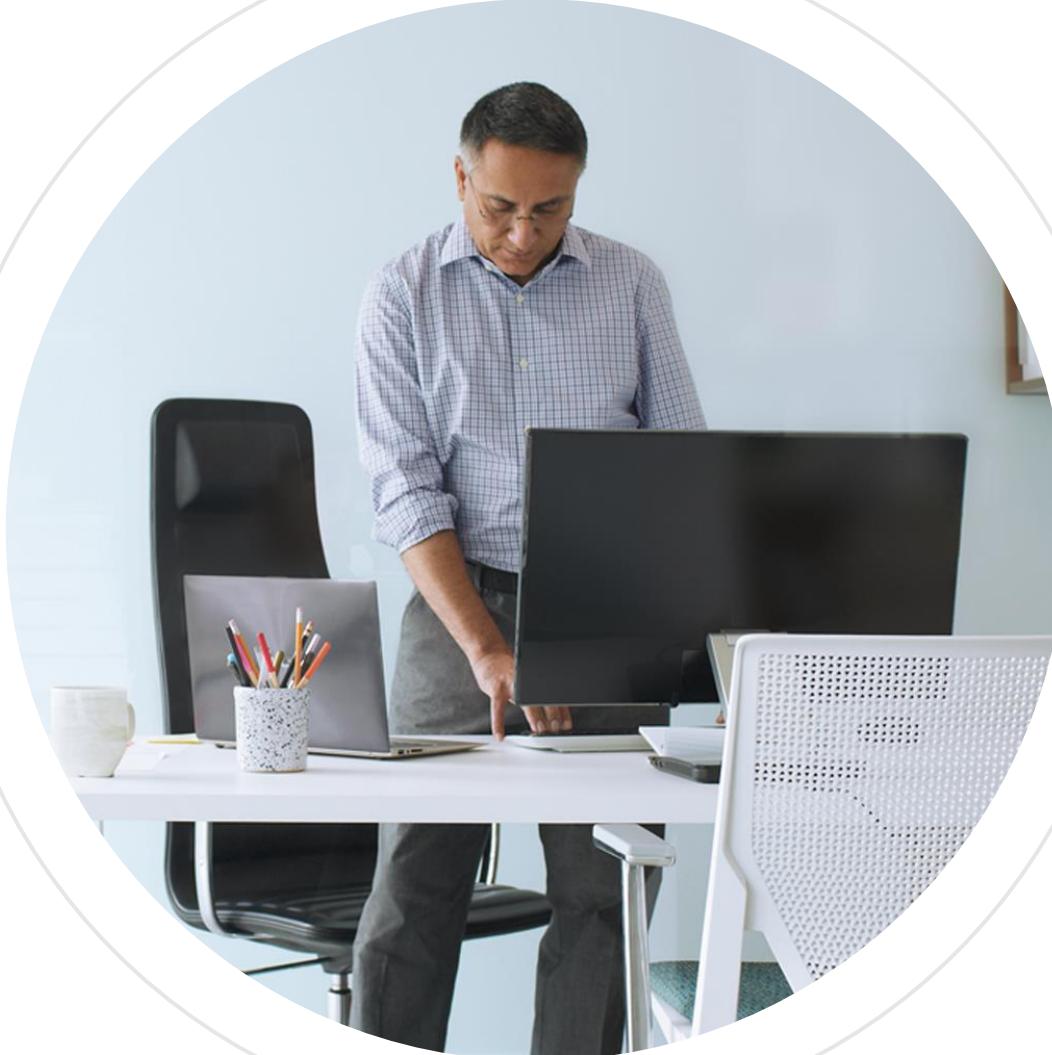
<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414>

Plan a Conditional Access deployment

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



Manage Azure AD Identity Protection



Objectives



Review identity protection basics



Implement and manage user risk policy



Implement MFA registration policy



Monitor, investigate, and remediate elevated risky users

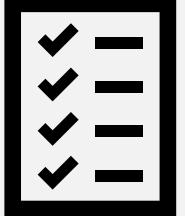


Security for Workload Identities



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 portal.
- 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
- Azure AD threat intelligence
- New country
- Suspicious inbox forwarding

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

Capability	Azure AD Free / Microsoft 365 Apps	Azure AD Premium P1	Azure AD 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	No	Yes
	Risky users	Limited Information.*	Limited Information.*	Full access
	Risky sign-ins	Limited Information.*	Limited Information.*	Full access
	Risk detection	No	Limited Information.*	Full access
Notifications	User at risk alert	No	No	Yes
	Weekly digest	No	No	Yes
MFA registration policy	No	No	Yes	

* See notes or student materials for details.

Identity Protection permissions

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

Azure AD P2 license required

Implement and manage user risk policy

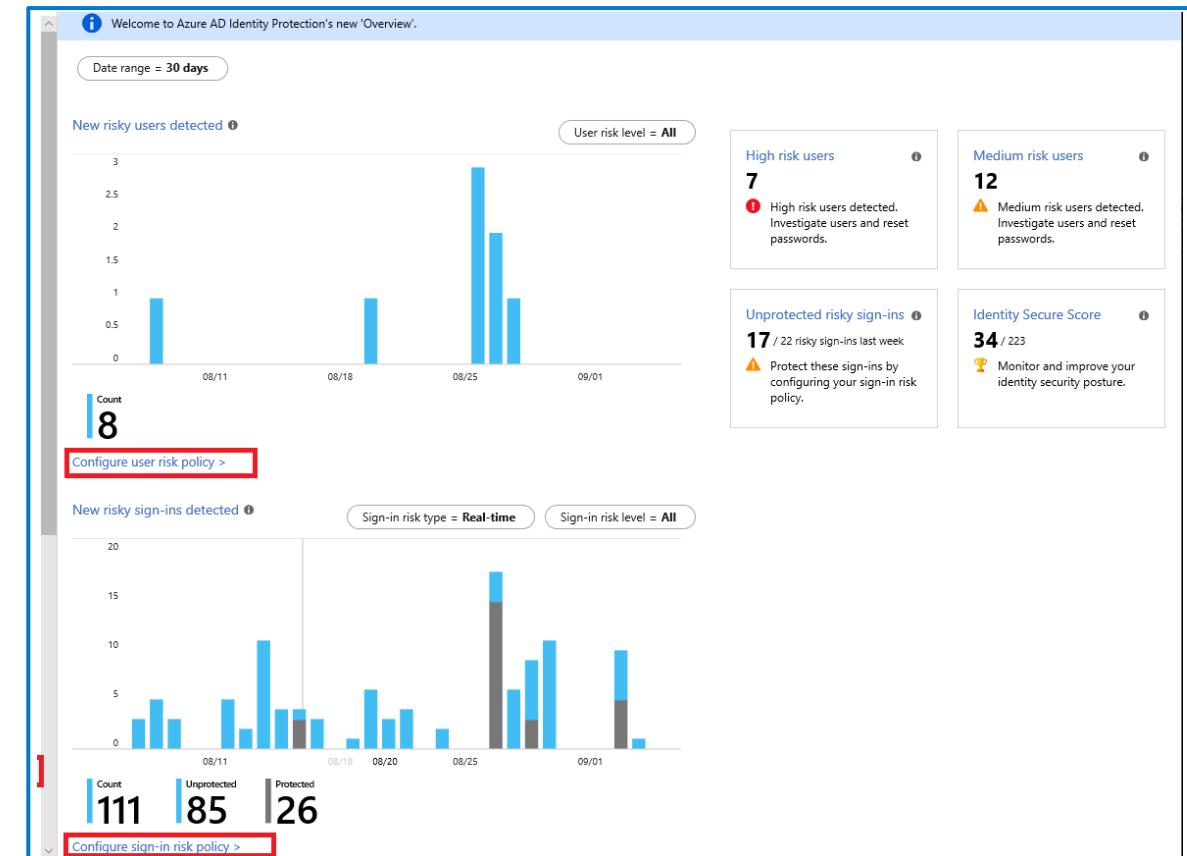


User risk policies

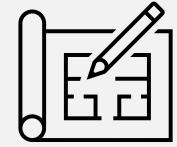
Both sign-in risk policies and user risk policies can be enabled to automate the response to risk detections and allow users to self-remediate

Organizations must decide the level of risk they are willing to accept, balancing user experience and security posture

Azure Portal → Azure AD → Security → Identity Protection



Implement MFA registration policy



What is MFA registration policy

Azure AD Multi-Factor 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. In order for users to be able to respond to MFA prompts, they must first register for Azure AD Multi-Factor Authentication.

We recommend that you require Azure AD Multi-Factor 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.

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

The screenshot shows the 'Contoso - Risky sign-ins' blade in the Microsoft Azure portal. The URL is https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RiskySignins. The page title is 'Wingtip Toys - Risky sig'. The top navigation bar includes 'Home', 'Contoso - Risky sign-ins', 'Azure Active Directory', and user information 'Bala.sandhu@contoso... CONTOSO'. The main content area displays a table of risky sign-in detections for the 'Last 1 month'. The table has columns: DATE, USER, APPLICATION, STATUS, IP ADDRESS, LOCATION, RISK STATE, REQUEST ID, and CONDITIONAL ACCE...'. The first row shows a success sign-in from Alain Charon via the Azure Portal. The second row shows an interrupted sign-in from Alain Charon via the Azure Portal. The third row is selected, showing an interrupted sign-in from Alain Charon via Microsoft Office 365. The fourth row shows an interrupted sign-in from Alain Charon via the Azure Portal. The fifth row shows an interrupted sign-in from Alain Charon via the Azure Portal. Below the table, there is a 'Details' section with tabs for 'Basic info', 'Risk info', 'Device info', 'MFA info', and 'Conditional Access'. The 'Basic info' tab is selected, displaying details for the selected row: Request ID 29e08ac8-xxxx-xxxx-4a65c26bab00, Correlation ID 44ff76a8-xxxx-xxxx-41bea9d6be5d, User Alain Charon, Username alain.charon@contoso.com, User ID bab8aed7-xxxx-xxxx-49c36888f05e, Application Microsoft Office 365 Portal, Application ID 00000006-0000-0ff1-ce00-000000000000, Resource Windows Azure Active Directory, Resource ID 00000002-0000-0000-c000-000000000000, IP address 131.107.159.177, Location Redmond, Washington, US, Date 9/10/2019, 9:15:42 AM, Status Interrupted, Sign-in error code 50140, Failure reason This error occurred due to 'Keep me signed in' interrupt when the user was signing-in, Client app Browser.

Report details – example Risky Users Report

Home > Default Directory > Security

Security | Risky users

Search (Ctrl+ /)

Learn more

Download

Select all

X Confirm user(s) compromised

✓ Dismiss user(s) risk

↻ Reset password

- Block user

⟳ Refresh

Getting started

Protect

Conditional Access

Identity Protection

Security Center

Verifiable credentials (Preview)

Manage

Identity Secure Score

Named locations

Authentication methods

MFA

Report

Risky users

Risky sign-ins

Auto refresh : Off

Show dates as : Local

Risk state : 2 selected

Status : Active

+ Add filters

User	Risk state	Risk level	Risk last updated	⋮
<input type="checkbox"/> unknown	Remediated	-	8/25/2020, 1:03:07 PM	⋮
<input type="checkbox"/> Sarah	Dismissed	-	8/7/2020, 1:30:13 PM	⋮
<input type="checkbox"/> Jose	At risk	Medium	7/31/2020, 2:11:54 PM	⋮
<input type="checkbox"/> Charlie Cummings	At risk	Medium	7/30/2020, 6:55:25 PM	⋮
<input type="checkbox"/> Flash Threetoe	At risk	High	7/30/2020, 4:26:42 PM	⋮
<input type="checkbox"/> Bob Brown	At risk	High	7/22/2020, 10:00:11 AM	⋮
<input type="checkbox"/> Sarah Handler	Dismissed	-	6/11/2020, 6:10:07 PM	⋮
<input type="checkbox"/> Anthony Ames	At risk	High	11/7/2019, 9:56:41 AM	⋮
<input type="checkbox"/> BadUser	At risk	High	10/9/2019, 10:34:39 AM	⋮
<input type="checkbox"/> Admin Demo	Remediated	-	1/9/2019, 5:29:02 PM	⋮
<input type="checkbox"/> R	Remediated	-	1/9/2019, 1:27:32 PM	⋮
<input type="checkbox"/> Rohit Prasad	Remediated	-	12/13/2018, 1:31:33 PM	⋮
<input type="checkbox"/> Admin Kloud	At risk	Medium	11/10/2018, 9:50:02 PM	⋮
<input type="checkbox"/> Joe	Remediated	-	10/28/2018, 3:18:42 PM	⋮
<input type="checkbox"/> James Romanoski	Remediated	-	10/25/2018, 10:56:00 PM	⋮

Load more

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

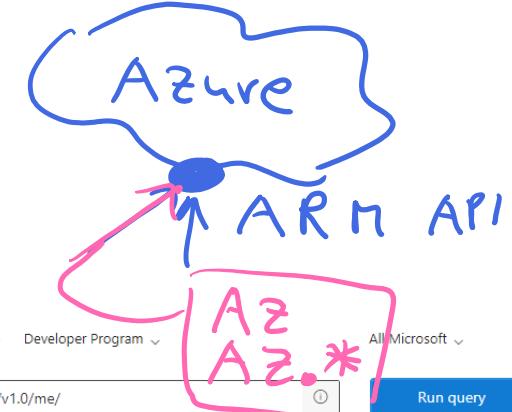
PowerShell Module ~~AzureAD~~ ADAL (old)

Use the Microsoft Graph API

~~nsGraph~~

nsAL (new)

- Microsoft Graph - unified API endpoint and the home of Azure Active Directory Identity Protection APIs
- Three Microsoft Graph APIs expose information about risky users and sign-ins:
 - riskDetection
 - riskyUsers
 - signIn



The screenshot shows the Microsoft Graph Explorer interface. At the top, there's a navigation bar with links like 'Solutions', 'Graph Explorer', 'Get Started', 'Docs', 'Changelog', 'Resources', 'Developer Program', and 'All Microsoft'. Below the navigation bar, there's a search bar with the URL 'https://graph.microsoft.com/v1.0/me/'. The main area has tabs for 'Request body', 'Request headers', 'Modify permissions (Preview)', 'Access token', and 'Run query'. On the left, there's a sidebar with sections like 'Getting Started (8)' and a list of sample queries with 'GET' buttons. On the right, there's a 'Response preview' section showing JSON data for a user profile. The JSON output includes fields like '@odata.context', 'businessPhones', 'displayName', 'givenName', 'jobTitle', and 'mail'.

Security for Workload identities

Workload identities risk

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

These workload identities differ from traditional user accounts as they:

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

The screenshot shows the 'Security | Risk detections' page. On the left, there's a sidebar with links like 'Getting started', 'Manage' (with 'Identity Secure Score', 'Named locations', 'Authentication methods', and 'MFA'), 'Report' (with 'Risky users', 'Risky workload identities (preview)', 'Risky sign-ins', and 'Risk detections'), and a search bar. The main area has filters at the top: 'Auto refresh: Off', 'Detection time: Last 90 days', 'Show dates as: Local', 'Detection type: None Selected', 'Risk state: 2 selected', 'Risk level: None Selected', and 'Add filters'. Below these, there are two tabs: 'User detections' and 'Workload identity detections', with 'Workload identity detections' highlighted by a red box. A table follows, with columns: 'Detection time ↑↓', 'Service principal ... ↑↓', 'Detection type ↑↓', 'Risk state ↑↓', and 'Risk level ↑↓'. The table contains six rows of data, each with a timestamp, a service principal name, a risk status, and a risk level. The last row is highlighted with a grey background.

Detection time ↑↓	Service principal ... ↑↓	Detection type ↑↓	Risk state ↑↓	Risk level ↑↓
10/31/2021, 11:40:48 P...	Risky Test App 2	Risk detected	Confirmed compromis...	High
10/27/2021, 12:13:00 ...	Risky Test App 3	Risk detected	Confirmed compromis...	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

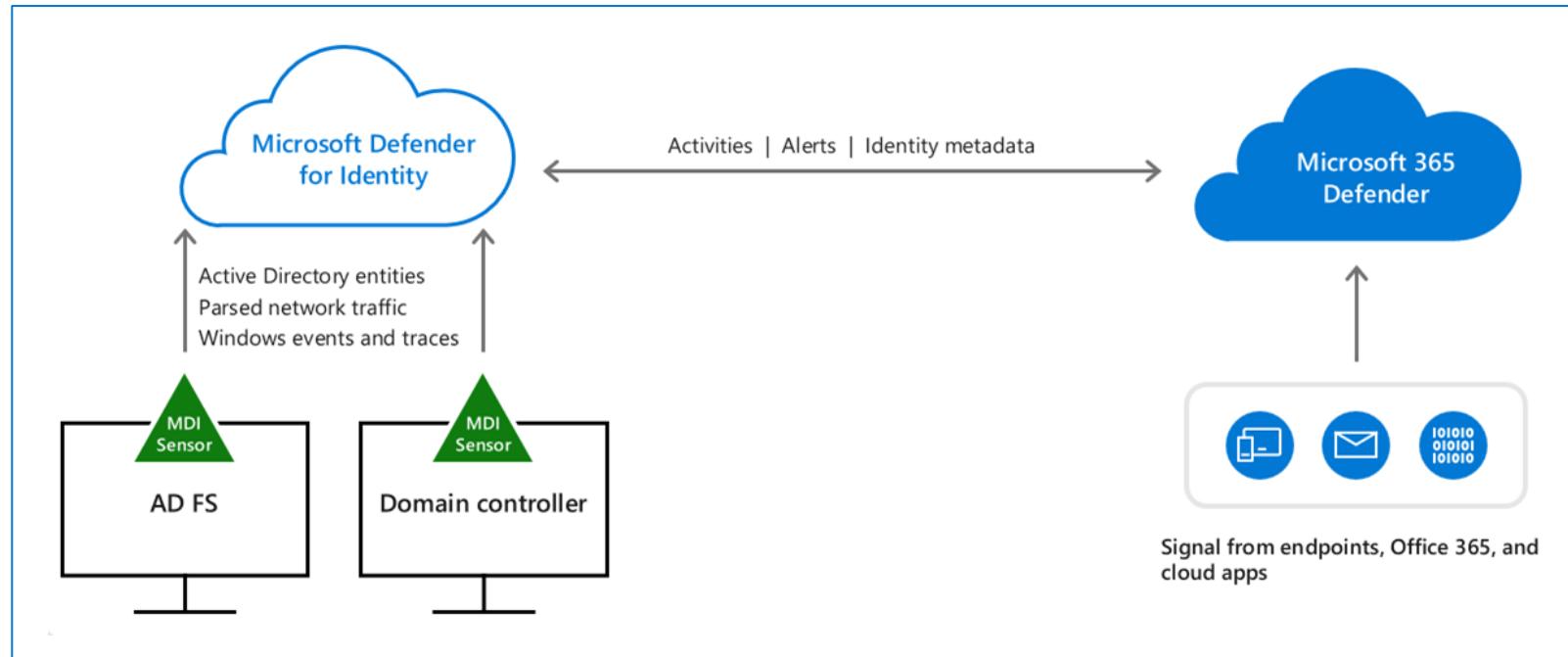
Detection Name	Description
Azure AD threat intelligence	This risk detection indicates some activity that is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.
Suspicious Sign-ins	This risk detection indicates sign-in properties or patterns that 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 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>
- Formerly - <https://portal.atp.azure.com/>

References

Conditional Access for workloads

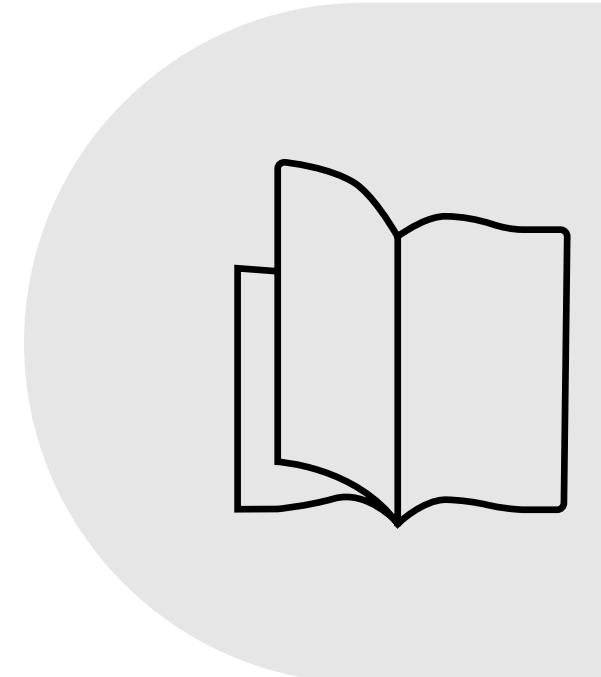
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/workload-identity>

Require MFA for all users

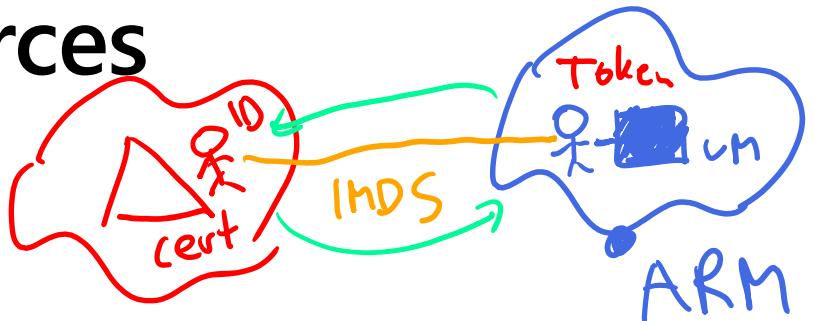
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

Defender for Identity

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



Implement access management for Azure resources



Objectives



Assign Azure roles



Configure a custom Azure role



Create and configure Managed Identities



Access Azure resources with Managed Identities



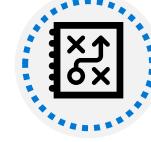
Analyze Azure role permissions

UAA

Owner



Configure Azure Key Vault policies and access objects



Explore Microsoft Entra Permissions Management

Assign Azure roles

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">• User• Group• Service Principal• Managed Identity	Built-in Azure roles <ul style="list-style-type: none">• Owner - full access to all resources.• Contributor - Can create and manage all types of Azure resources, but can't grant access.• Reader - Can view the available Azure resources.• User Access Administrator - Assign access to Azure resources.• Other task specific roles, like Virtual Machine Contributor, can be assigned.
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 managing access control (IAM) in a resource group named "example-group".

Left sidebar:

- Home > Resource groups > example-group
- example-group | Access control (IAM)
- Resource group
- Search (Ctrl+ /)
- Overview
- Activity log
- Access control (IAM)** (highlighted with a red box)
- Tags
- Events
- Settings
- Deployments
- Policies
- Properties
- Locks
- Cost Management
- Cost analysis
- Cost alerts (preview)
- Budgets
- Advisor recommendations

Top navigation bar:

- Add
- Download role assignments
- Edit columns
- Refresh
- Remove
- Got feedback?

Check access tab:

- My access**: View my level of access to this resource. Includes a "View my access" button.
- Check access**: Review the level of access a user, group, service principal, or managed identity has to this resource. Includes a "Find" input field for "User, group, or service principal" and a search bar.

Actions:

- Grant access to this resource**: Grant access to resources by assigning a role. Includes a "Add role assignments" button and a "Learn more" link.
- View access to this resource**: View the role assignments that grant access to this and other resources. Includes a "View" button and a "Learn more" link.
- View deny assignments**: View deny assignments.

Assign a role using script

PowerShell

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

CLI scripting

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

Configure a Custom Azure Role

Create a custom role

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

To create the custom role:

1. Open Azure AD in the Azure portal.
2. Select **Roles and administration**.
3. Select + **New custom role**.
4. Then name and assign the capabilities needed.

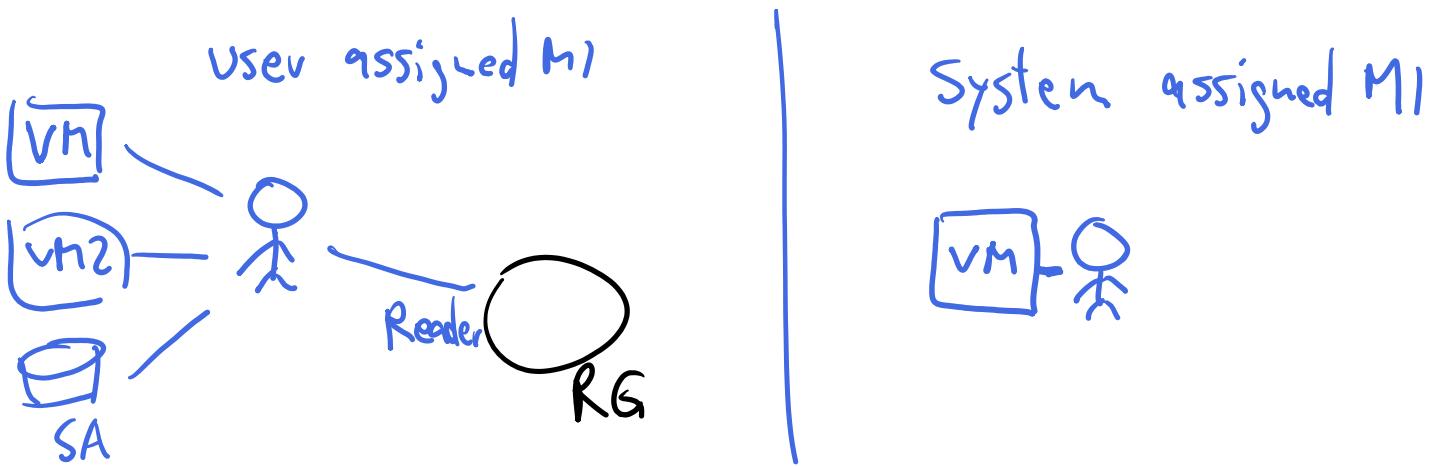
The screenshot shows the 'New custom role' page in the Azure portal. The URL is 'Home > Contoso > Roles and administrators > New custom role'. The page has tabs for 'Basics', 'Permissions' (which is selected), and 'Review + create'. A note says 'Add permissions for this custom role. Currently, permissions for Application registrations and Enterprise applications are supported in custom roles.' A 'Search by permission name or description' input field is present. Below it is a table of permissions with columns for 'Permission' (checkbox), 'Description', and 'Type'. The permissions listed are:

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

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 that use this command Microsoft/Billing/*/read. The wildcard can exist at any level.

```
{  
    "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": []  
            }  
        ]  
    }  
}
```



Create and configure Managed Identities

Types of Managed Identities

Identity type	Description and usage
System-assigned	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 Azure AD. 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 Azure AD.
User-assigned	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 Azure AD 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 the Azure portal interface for managing identities of an App Service named "userassigned-windows".

Left Panel (App Service Identity Settings):

- Subscription: Home > App Services > userassigned-windows - Identity
- App Service: userassigned-windows - Identity
- Search bar: Search (Ctrl+ /)
- Settings menu:
 - System assigned
 - User assigned
- Description: User assigned managed identities enable Azure resources to aut...
User assigned managed identities are created by associating an Azure resource (e.g. Virtual Machine) with a managed identity. A managed identity can be shared across multiple resources (e.g. Virtual Machines, Functions, and Storage Accounts).
- Action buttons: + Add, Remove, Refresh, Got feedback?
- No results listed.

Right Panel (Add user assigned managed identity):

- Subscription: APEX C+L - Aquent Vendor Subscriptions
- User assigned managed identities search bar: userassig... (highlighted with a red box)
- Result list:
 - userassignedmanagedidentity (Resource Group: appRG)
- Selected identities: (empty)
- Add button (highlighted with a red box)

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 *A&h (Bicep)*

```
"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 assigning a role. On the left, the 'Add role assignment' dialog is open, showing the 'Members' tab selected. The 'Selected role' is set to 'Owner'. Under 'Assign access to', the 'Managed identity' option is selected, highlighted with a red box. The 'Members' section shows 'No members selected'. A 'Description' field is present with the placeholder 'Optional'. On the right, a 'Select managed identities' modal is displayed. It includes fields for 'Subscription' (selected) and 'Managed identity' (set to 'Select', also highlighted with a red box). A search bar labeled 'Search by name' is provided. At the bottom of the modal are 'Select' and 'Close' buttons.

Home > sc300strgacnt >

Add role assignment

Got feedback?

Role Members • Review + assign

Selected role Owner

Assign access to User, group, or service principal Managed identity

Members [Select members](#)

Name	Object ID
No members selected	

Description [Optional](#)

Select managed identities

Got feedback?

Subscription *

Managed identity

Select

Search by name

Select Close

Analyze Azure AD role permissions

What is a permission?

The dictionary definition of permission is the **consent or authorization to perform a specific action**.

In Azure Active Directory:

- Permissions for each of the operations you're able to do.
- Permission can range from viewing your settings:
 - Ability to change your setting.
 - All the way up to granting permission to add or remove users and beyond.

There are two primary places where permission can be assigned, at a user or group level.

Default user permissions

Member Users	Guest Users
Enumerate list of users and their contacts	Read own properties
Invite guest users	Invite guest users
Can create Security and Microsoft 365 Groups	Can search for non-hidden groups by name
Register new applications	Read properties of registered and enterprise applications

Add or restrict permissions

 **Users | User settings**
Default Directory - Azure Active Directory

Enterprise applications
[Manage how end users launch and view their applications](#)

App registrations

Users can register applications ⓘ
 Yes No

Administration portal

Restrict access to Azure AD administration portal ⓘ
 Yes No

LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users consent to connect their Microsoft work or school account with their LinkedIn account.

[Learn more about LinkedIn account connections ⓘ](#)

Yes Selected group No

External users
[Manage external collaboration settings](#)

User features
[Manage user feature settings](#)

 **Roles and administrators | All roles**
Default Directory - Azure Active Directory

Administrative roles
Administrative roles are used for granting access for privilege application configuration. [Learn more](#).

[Learn more about Azure AD role-based access control](#)

 Search by name or description

Role

<input type="checkbox"/>	Application administrator
<input type="checkbox"/>	Application developer
<input type="checkbox"/>	Attack payload author
<input type="checkbox"/>	Attack simulation administrator
<input type="checkbox"/>	Attribute assignment administrator 
<input type="checkbox"/>	Attribute assignment reader 
<input type="checkbox"/>	Attribute definition administrator 
<input type="checkbox"/>	Attribute definition reader 

Exploring available permissions

Application administrator | Description ...

All roles

« Got feedback?

Diagnose and solve problems

Manage

Assignments

Description

Activity

Bulk operation results

Troubleshooting + Support

New support request

Summary

Name: Application administrator

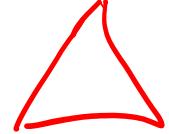
Description: Users in this role can add, manage, and configure enterprise applications, app registrations and manage on-premises like app proxy.

Template ID:

Related articles: [Assigning administrator roles in Azure Active Directory](#)

Role permissions

microsoft.directory/adminConsentRequestPolicy/allProperties/allTasks	Manage admin consent request policies in Azure AD
microsoft.directory/appConsent/appConsentRequests/allProperties/read	Read all properties of consent requests for applications registered with Azure AD
microsoft.directory/applications/create	Create all types of applications
microsoft.directory/applications/delete	Delete all types of applications
microsoft.directory/applications/applicationProxy/read	Read all application proxy properties
microsoft.directory/applications/applicationProxy/update	Update all application proxy properties



MFA ← Fido
SMS on
off

ID Protection ← User Risk Policy
Sign In Risk

CA Policies

Configure Azure Key Vault RBAC policy



Role

Owner
Contributor
Reader
UAA

MI

KV

Key Vault Access Policy

- You can grant access to Azure Key Vault using either role-based access control (RBAC) or using 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

Add access policy

Configure from template (optional)

Key permissions

Secret permissions

Certificate permissions

Select principal *

Authorized application ⓘ

Add

0 selected

Select all

Key Management Operations

Get

List

Update

Create

Import

Delete

Recover

Backup

Restore

Cryptographic Operations

Decrypt

Encrypt

Unwrap Key

Wrap Key

Verify

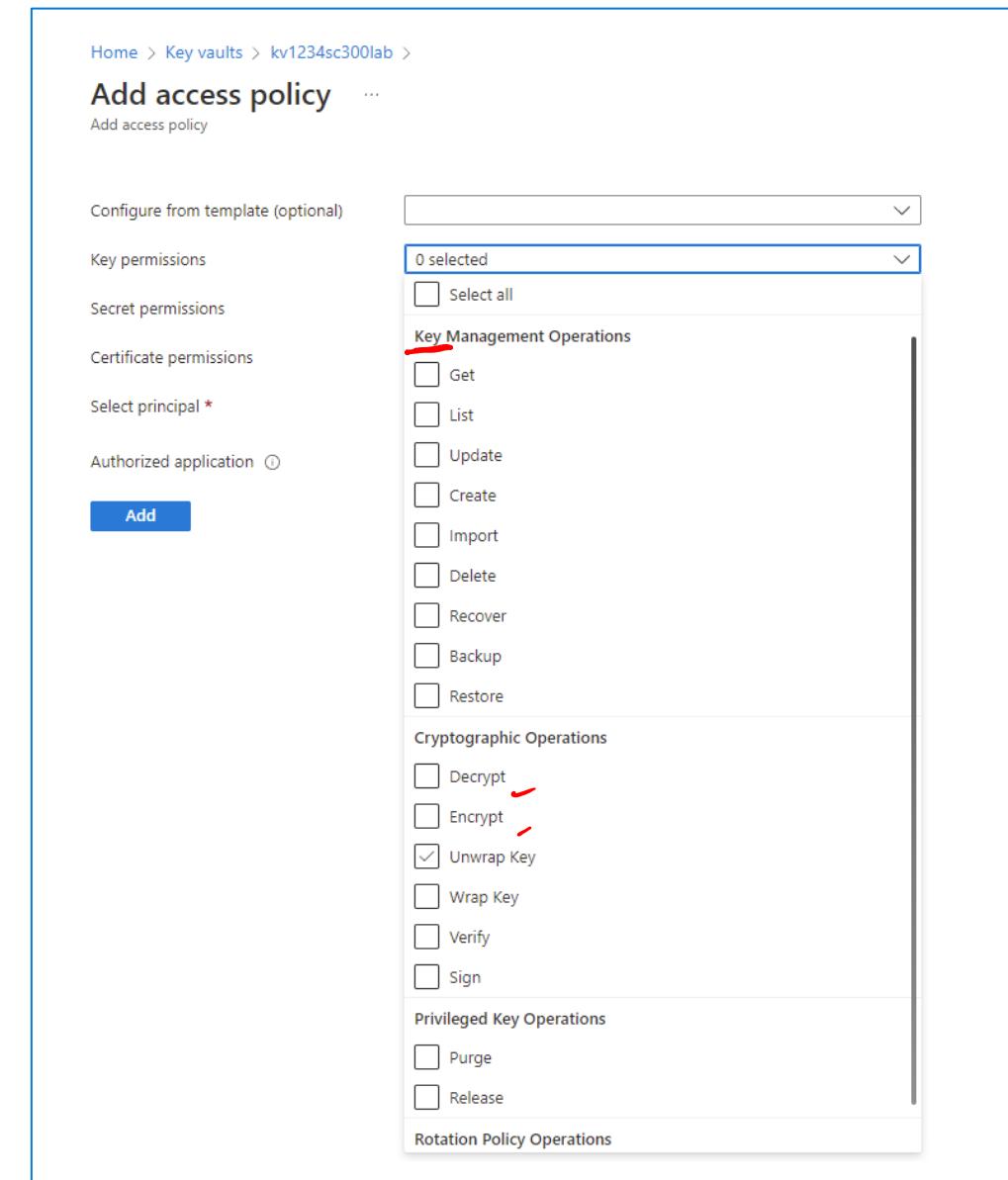
Sign

Privileged Key Operations

Purge

Release

Rotation Policy Operations



Key Vault and RBAC policies

The screenshot shows the 'kv1234sc300lab | Access policies' page in the Azure portal. The left sidebar lists several 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 has a search bar, Save, Discard, and Refresh buttons, and 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', there are two radio buttons: 'Vault access policy' (unchecked) and 'Azure role-based access control' (checked). A blue bracket labeled 'Policy' points to the 'Vault access policy' button, and a red box surrounds the 'Azure role-based access control' button, with the word 'RBAC' written in red next to it.

Assign access with RBAC to Key Vault

kv1234sc300lab | Access control (IAM) ...

Key vault

Search (Ctrl+ /) Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Events Settings Keys Secrets Certificates Access policies Networking Security Properties Locks Monitoring Alerts Metrics Diagnostic settings Logs

Check access Role assignments Roles Deny assignments Classic administrators

My access
View my level of access to this resource.
[View my access](#)

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

Find User, group, or service principal Managed identity

Search by name or email address

Grant access to this resource
Grant access to resources by assigning a role.

[Add role assignment](#) Learn more

View access to this resource
View the role assignments that grant access to this and other resources.

[View](#) Learn more

View deny assignments
View the role assignments that have been denied access to specific actions at this scope.

[View](#) Learn more

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 Crypto Officer	Perform any action on the keys 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 using from Key Vault in the Azure portal

- Azure Key Vault is a secure tool for storing secrets, keys, and certificate.
- 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

The screenshot shows the Azure Key Vault interface for managing a secret. At the top, the path is Home > Key vaults > kv1234sc300lab > mySC300keyvaultSecret >. Below this, the secret identifier is ba6102eeaf724b23bdea13e835260de6. There are 'Save' and 'Discard changes' buttons. The 'Properties' section shows 'Created' at 6/19/2022, 3:37:12 PM and 'Updated' at 6/19/2022, 3:37:12 PM. Under 'Settings', 'Set activation date' and 'Set expiration date' have checkboxes next to them, both of which are unchecked. The 'Enabled' setting has a 'Yes' button highlighted in blue and a 'No' button. The 'Tags' section shows '0 tags'. In the 'Secret' section, there is a 'Content type (optional)' field with an empty input box and a 'Hide Secret Value' button with a red border. At the bottom, the 'Secret value' is displayed as a greyed-out box containing the text 'This is my secret'.

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"
```

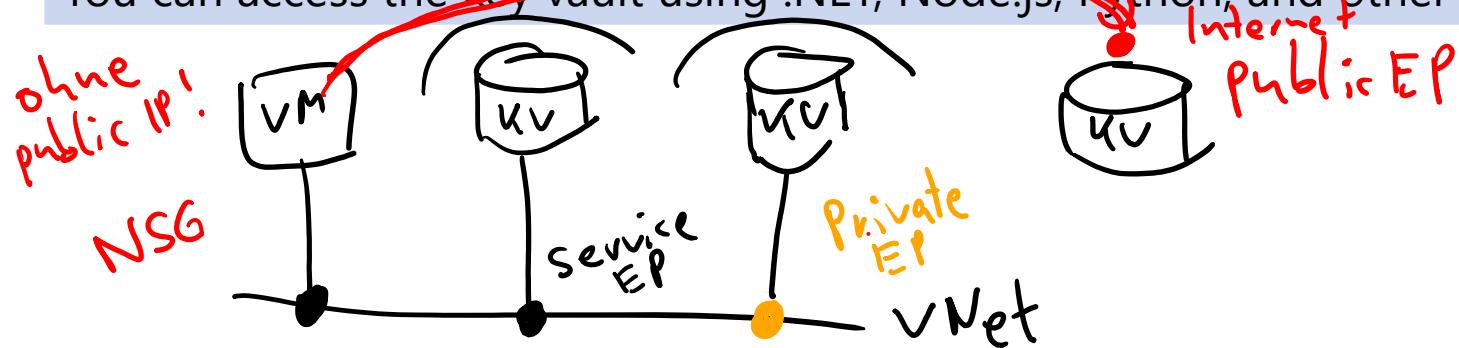
PowerShell

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

- Debug

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. **SDK**



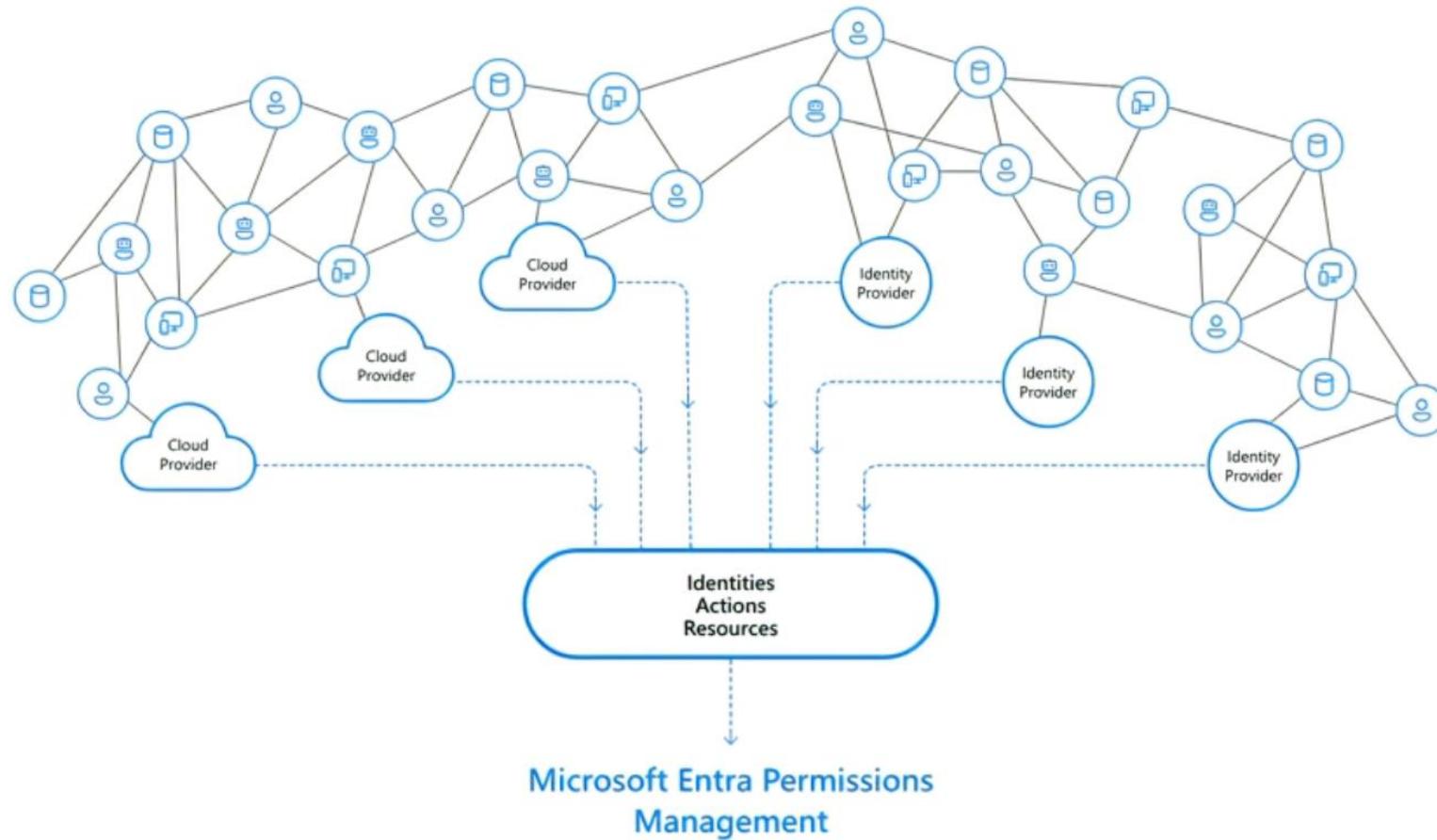
Explore Microsoft Entra Permissions Management (formerly Cloudknox)



Key use cases for Permissions Management

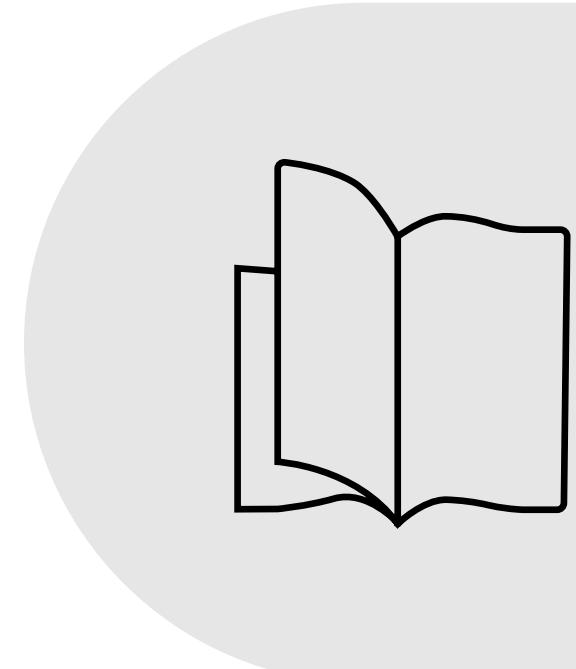
Use case	Description
Discover	Customers can assess permission risks by evaluating the gap between permissions granted and permissions used.
Remediate	Customers can right-size permissions based on usage, grant new permissions on-demand, and automate just-in-time access for cloud resources.
Monitor	Customers can detect anomalous activities with machine language-powered (ML-powered) alerts and generate detailed forensic reports.

Permissions Management process flow



References

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



Summary

LP2

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
- **Entra Permissions Management**

Labs

Lab	Brief description	Length
8. Enable MFA	Configure Multifactor Authentication policies, set up conditional access rules, and configure Azure AD MFA for passwords.	10 minutes
9. Configure and deploy SSPR	Enable self-service password reset, register a mobile phone number, and test self-service password reset.	15 minutes
10. Azure AD Authentication for Windows and Linux VMs	Configure Azure AD 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 Azure AD smart lockout values.	Customize the Azure AD 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

End of presentation