SC-300 Notes (IAM) Identity & Access Admin Associate

MSFT Entra ID:

- Define common identity terms and explain how they're used in the Microsoft Cloud.
- Explore the common management tools and needs of an identity solution.
- Review the goal of Zero Trust and how it applies in the Microsoft Cloud.
- Explore the available identity services in the Microsoft Cloud.

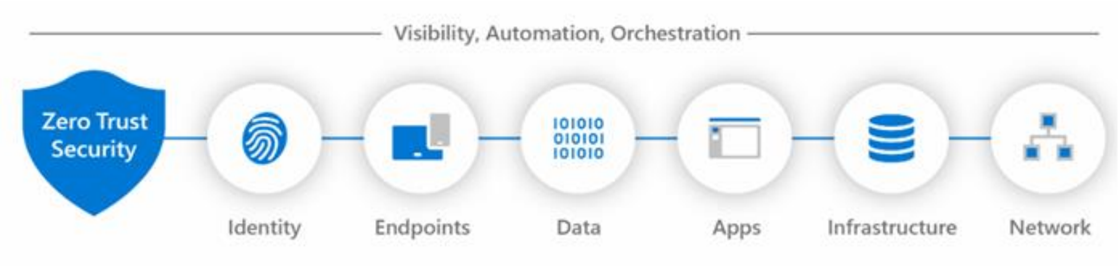
Zero Trust principles

Verify Explicitly	**Use least privilege access**	**Assume breach**
Always validate all available data points including:	To help secure both data and productivity, limit user access using:	Minimize blast radius for breaches and prevent lateral movement by:
User identity and location	Just-in-time (JIT)	Segmenting access by network, user, devices, and app awareness
Device health	Just-enough-access (JEA)	Encrypting all sessions end to end
Service or workload context	Risk-based adaptive policies	Use analytics for threat detection, posture visibility and improving defenses
Data classification	Data protection against out of band vectors	
Anomalies		

-

Deploying Zero trust solutions:

There are 6 pillars:



Verification is done with rich signal, stitching them together tells you what is most important, enabling you to respond fast with integrated remediation capabilities.

Control plane – routes network traffic around net arch, directing access to resources, user identity would be the place to check for access. Identity = CONTROL PLANE

IdP: - a sys that creates, manages, and stores digital identities

Most common components are

1. A repository of user identities
2. An authentication system
3. Security protocols that defend against intrusion
4. Someone we trust

-

Common identity protocols:

- OpenID provider (OIDC) - authen protocol based on (OAuth2 protocol which is used for authori). Uses message flows from OAuth2 to provide identity services via a RESTful HTTP API.
- SAML identity provider – open standard for exchanging authentication and authorization data between an identity/service provider.

-

Common identity admin tasks:

- **Identity proliferation** – deals with the storage of identity objects within the environment
- **Provision & Deprovision** – creation and removal of identities (deletion, disablement of security principle)
- **Identity updates** – how identity is updated, and move from a manual effort to an automated one
- **Synchronization** – ensures identity systems are up to date with latest identity info.
- **Password mgmt**. – where/how passwords are set through the infrastructure. Help desk resets pws usually.
- **Group mgmt**. – how orgs manage groups (like AD or LDAP) in environment, Most common but expensive.

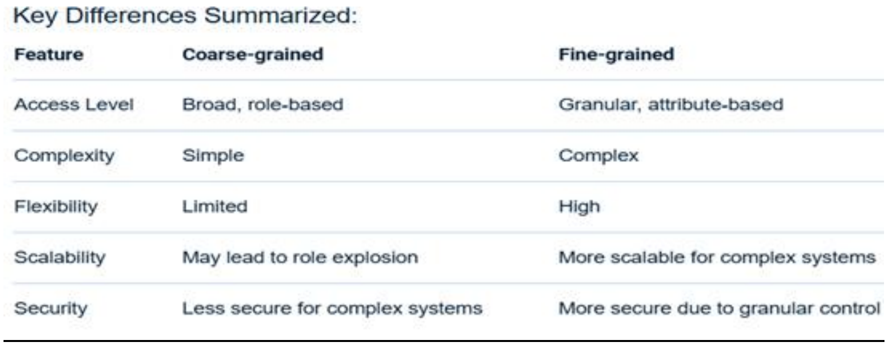
- **User Interface** – how user requests/make updates to their identity, usually through contacting Service desk

- **Change Control** – focus on how changes flow through the env. whether done by service desk, there can be automation w/wo workflow, which drives the change process

- **App Entitlement mgmt**. – how identities are granted to access to apps.

    - Focuses on coarse-grained app entitlements – which grants/denies access based on a single factor (often a user's role or group membership) – Implemented through RBAC

    - Fine-grained app entitlements – more granular, focuses more on control over access considering multiple attributes & conditions – Implemented through ABAC (attribute) or PBAC (policy-based)



Key Differences Summarized:

Feature	Coarse-grained	Fine-grained
Access Level	Broad, role-based	Granular, attribute-based
Complexity	Simple	Complex
Flexibility	Limited	High
Scalability	May lead to role explosion	More scalable for complex systems
Security	Less secure for complex systems	More secure due to granular control

Microsoft Graph:

- MSFT Graph API – use REST APIs or SDKs to access the endpoint https://graph.microsoft.com for insights into M365 Windows 10 and Enterprise Mobility + Security

- MSFT Graph Connectors – delivers data external to the M cloud into Graph services and apps to enhance M365 experiences

- MSFT Graph Data Connect -provide a set of tools to streamline scalable delivery of Graph data to popular Azure data stores

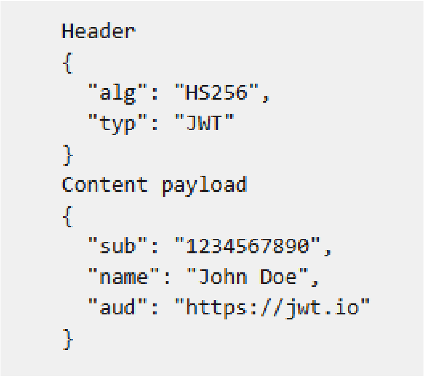
All 3 together power the MSFT cloud services platform.

-

B2C is a separate service from Entra ID, allow businesses to build customer facing apps & then anyone can sign up into those apps w/o restrictions on user acct.

Claims-based identity

- Claim - a value pair of data within a security token. There are multiple claims transferred within the token from the claim that defines the type of the token to the encryption method. Example:



```
Header
{
  "alg": "HS256",
  "typ": "JWT"
}
Content payload
{
  "sub": "1234567890",
  "name": "John Doe",
  "aud": "https://jwt.io"
}
```

- Assertion - a package of data, usually in the form of a token that shares the identity and security information about a user or account across security domains.
- Attribute - a value pair of data within a token.
- Augmentation - the process of adding other claims to the user token to provide extra detail about the user. This could include data from human resource (HR) systems, from an application like SharePoint, or other systems.

-

Auditing in identity

Event logs

Activity logs

Sign-in logs

Provisioning logs

Audit logs

Azure Monitor

MS Sentinel

-

Identity Lifecycle Management

- **Join** - when an individual comes into scope of needing access, an identity is needed by those applications, so a new digital identity might need to be created if one isn't already available.
- **Move** - when an individual moves between boundaries, extra access authorization is required to be added or removed to their digital identity.
- **Leave** - when an individual leaves the scope of needing access, access might need to be removed, and the identity is no longer be required by applications other than for audit or forensics purposes.

-

Monitoring tools:

- Azure Monitor
- Application Insights
- Azure Service Health
- Azure Resource Health
- Azure Resource Manager
- Azure Policy

Administrative Units

You can have users in the following roles to manage your administrative unit:

- Authentication administrator
- Helpdesk administrator
- License administrator
- Password administrator
- User administrator

Defining Roles

Each task should be evaluated for frequency, importance, and difficulty

Entra Security Defaults:

Requiring all users to register for multifactor authentication (MFA).

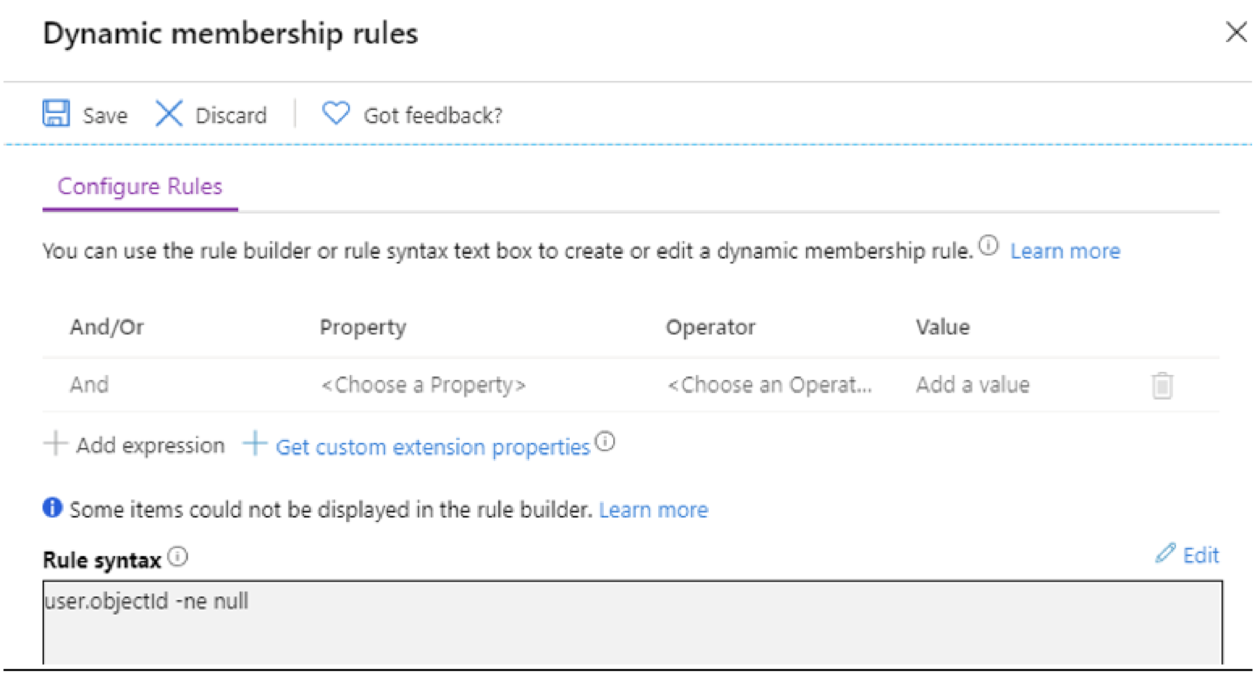
- Requiring administrators to perform multifactor authentication.
- Blocking legacy authentication protocols.
- Requiring users to perform multifactor authentication when necessary.
- Protecting privileged activities like access to the Azure portal.

Tenant ID settings

- Entra ID > Overview tab > Properties
- Is where Privacy Statement URL should go

Dynamic Groups

The final type of group is a dynamic group, which the name implies, the membership is generated by a formula each time the group is used. A dynamic group includes any recipient in Active Directory with attribute values that match its filter.



Dynamic membership rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

And/Or	Property	Operator	Value
And	<Choose a Property>	<Choose an Operat...	Add a value

Some items could not be displayed in the rule builder. Learn more

Rule syntax ⓘ

```
user.objectId -ne null
```

Consist of all valid members of the Entra ID

Hybrid entra joined devices

Typically, organizations with an on-premises footprint rely on imaging methods to configure devices, and they often use Configuration Manager or group policy (GP) to manage them

Usage Location Isn’t Allowed

When Microsoft Entra ID assigns group licenses, any users without a specified usage location inherit the location of the directory. We recommend that administrators set the correct usage location values on users before using group-based licensing to comply with local laws and regulations.

Dynamic groups

- **Automation** – No manual member updates.
- **Consistency** – Always up-to-date membership.
- **Licensing & Access Control** – Often paired with **group-based licensing**, Intune device policies, or application access assignments.
- **Security** – Auto-remove access when someone's role or department changes.

Cloud Authentication

Password hash synch (PHS)- use same usrn & pw to login into on-prem AD to Entra Connect

1. Effortless to setup
2. SSO deployed
3. Suggest to deploy a 2nd Entra connect server in staging mode on standby configuration
4. Run new synch when updates are done to the on-prem AD - doesn't enforce changes

Pass through AuthN (PTA) - provides pw validation by using sw agent running on on-prem server, the server validates directly ensuring it doesn't happen in the clod

1. Need at least 3 lightweight agents installed on-prem servers, needing access to your AD DS and your AD domain controllers
2. SSO deployed
3. Suggests deploying 2 add'l agents for high availability,1 for mainten./failure, have another
4. Enforces your on-prem AD state/policies at time of login
5. Can use PHS if on-prem AD servers fail

Federated Authentication

Active Directory Federation Service (AD FS) - is when Entra ID uses a trusted external party to validate authentication on-prem

1. Org usually keep if invested on-prem already, company secures, more complex 2 operate
2. Can be configured to auto sign in users and devices, all based on company requirements
3. Needed when Entra doesn’t support a native authN requirement
4. Requires smartcards or certificates
5. Requires a load-balanced array of servers (farm) ensures availability of authN request

Why Organizations Use Federated Auth with AD FS

- **Password Stays On-Prem**: Cloud service never stores or validates the password — only AD FS talks to AD.
- **Custom Policies**: You can enforce conditional access rules in AD FS before issuing tokens.
- **Legacy Support**: AD FS can bridge to apps that use WS-Fed or SAML 1.1 that Entra ID might not natively support.
- **True SSO**: On corporate devices, users can log in without entering credentials again.

How to fix AttributeValueMustBeUnique error (errors during export to Entra)

- Identify the duplicated proxyAddresses, userPrincipalName or other attribute value that's causing the error. Also identify which two (or more) objects are involved in the conflict. The report generated by Microsoft Entra Connect Health for sync can help you identify the two objects.
- Identify which object should continue to have the duplicated value and which object shouldn't.
- Remove the duplicated value from the object that shouldn't have that value. You should make the change in the directory where the object is sourced from. In some cases, you need to delete one of the objects in conflict.
- If you made the change in the on premises AD, let Microsoft Entra Connect sync the change for the error to get fixed.

Admin role conflict

Description: An Existing Admin Role Conflict will occur on a user object during synchronization when that user object has:

- administrative permissions and
- the same UserPrincipalName as an existing Microsoft Entra object

How to fix

To resolve this issue do the following:

1. Remove the Microsoft Entra account (owner) from all admin roles.
2. Hard Delete the Quarantined object in the cloud.
3. The next sync cycle will take care of soft-matching the on-premises user to the cloud account (since the cloud user is now no longer a global GA).
4. Restore the role memberships for the owner.

MFA

- Should always support more than 1 method (mobile app verification, FIDO2, OATH token, etc)
- Use Entra ID Protection to register the employees/clients choice of MFA

Troubleshooting conditional access policies

- Get an interrupted sign-in- check monitoring and insights and filter to find the incident
- Click incident then go to CA tab, will show the exact policy that created the interruption
- Selecting the ellipsis on the right of a fail event will bring up the policy details

CA Optimization Agent

An AI-driven assistant for **Conditional Access (CA)** policy management, this agent **automatically scans your tenant** to identify gaps—such as users or apps not covered by policies—and proposes intelligent optimizations based on Zero Trust best practices

- **Gap detection**: Spots users/apps missing protections like MFA, device compliance, or app protection enforcement.
- **Policy consolidation**: Identifies redundant or overlapping CA policies and suggests combining them.
- **Legacy and risky sign-in control**: Recommends blocking legacy authentication and device code flow, and—if on P2—addresses risky users and sign-ins.

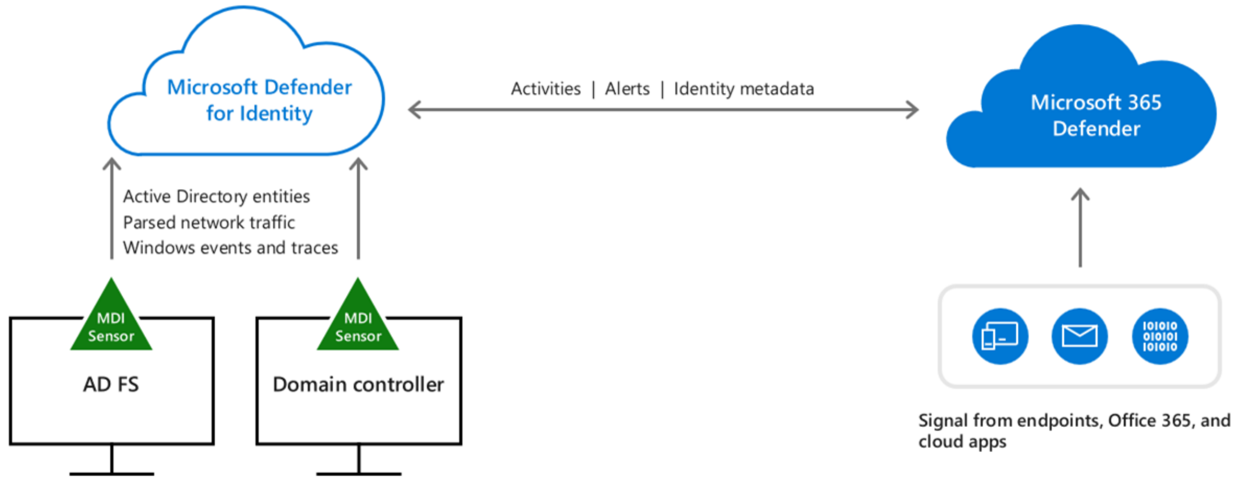
- **One-click suggestions**: Actions like adding users to policies or creating new (report-only) policies can be applied with a single click.
- **Reduces manual workload**—no more spreadsheets or PowerShell scripts to track coverage.
- **Enhances security posture**—helps close gaps swiftly and align with best practices.
- **Improves policy hygiene**—through consolidation and phased deployment, minimizing deployment risks.

Identity Protection - monitoring their usage and sign-in patterns helps ensure a secure cloud solution

**Do a stage roll out with these policies, start with a small group and test before full rollout

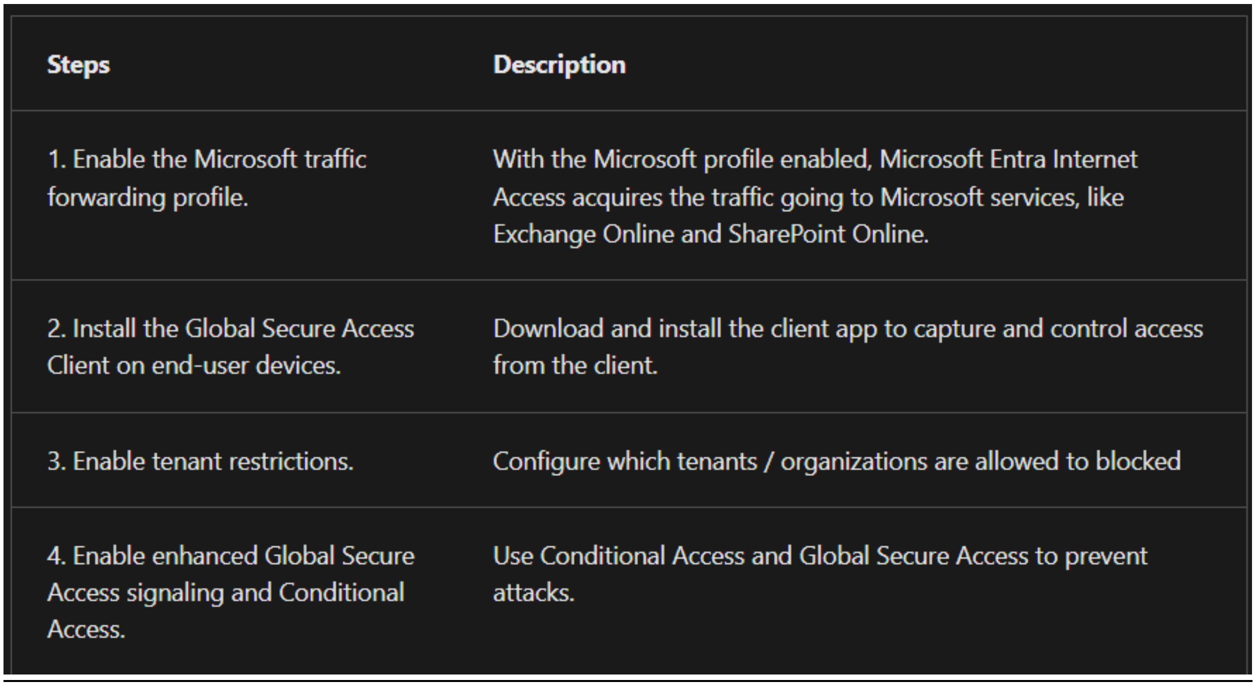
- Implement **User risk policy** - detects the probability that a user account has been compromised by detecting risk events that are atypical of a user's behavior -**set to HIGH**
- Implement **Sign-in risk policy** - detects suspicious actions that come along with the sign-in. It's focused on the sign-in activity itself and analyzes the probability that the sign-in was performed by some other than the user. -**set to MEDIUM**
- Implement **MFA registration policy**
- Monitor, investigate, remediate elevated risky users

Process flow for Defender for Identity


Microsoft Defender for Identity
Activities | Alerts | Identity metadata
Microsoft 365 Defender
Active Directory entities
Parsed network traffic
Windows events and traces
MDI Sensor
AD FS
MDI Sensor
Domain controller
Signal from endpoints, Office 365, and cloud apps

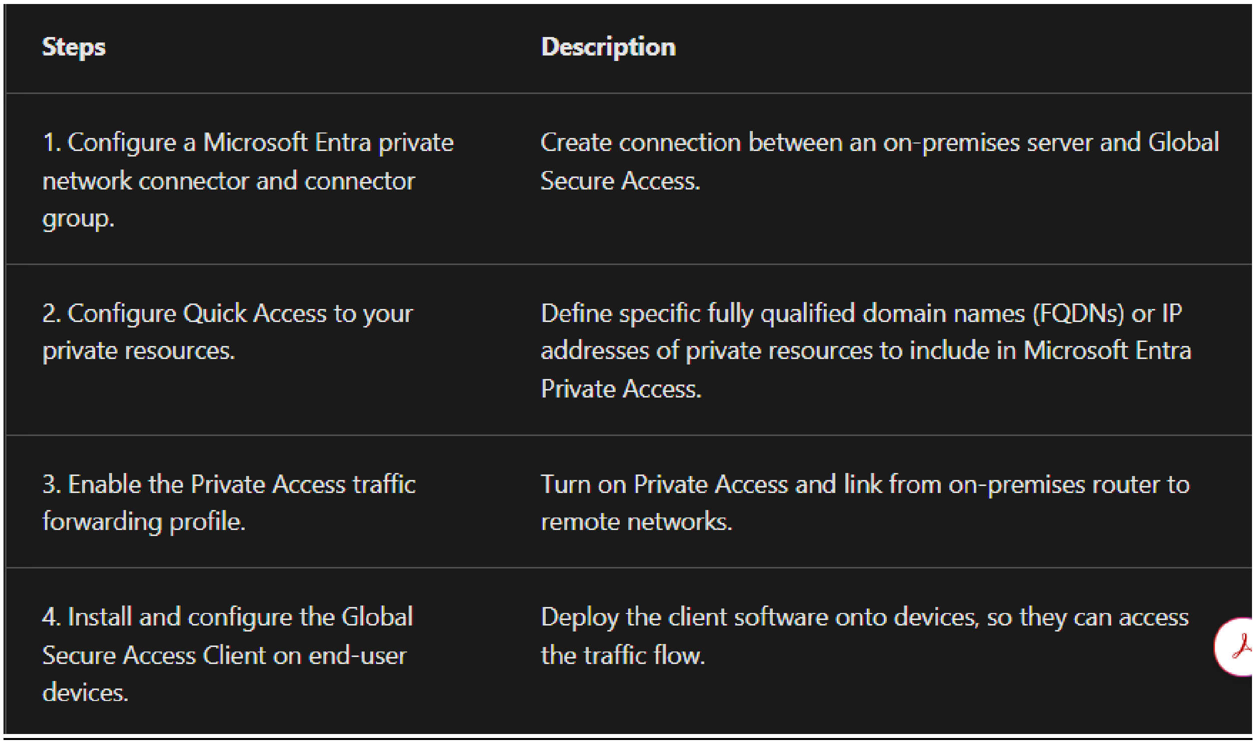
Global Secure Access (Entra Internet + Entra Private Access)

4 steps to deploy 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.

4 steps to deploy Entra Private Access



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

Integrating apps with older protocols

- Integrate apps using older protocols by using Application Proxy and/or Microsoft Entra Domain Services.

Configuring App Properties

- An app that uses SAML-based SSO will have fields such as *User access URL* whereas an app that uses OIDC-based SSO won't (within app properties).
- Apps added through Microsoft Entra ID - App registrations are by default OIDC-based apps
- Apps added through Microsoft Entra ID - Enterprise applications might use any SSO standard.

Comparisons of industry standard protocols

- OAuth vs. OpenID Connect: OAuth is used for authorization and OpenID Connect (OIDC) is used for authentication. OpenID Connect is built on top of OAuth 2.0, which means the terminology and flow are similar between the two. You can even authenticate a user using OpenID Connect and get authorization to access a protected resource that the user owns using OAuth 2.0 in one request.
- OAuth vs. SAML: OAuth is used for authorization and Security Assertion Markup Language (SAML) is used for authentication.
- OpenID Connect vs. SAML: Both OpenID Connect and SAML are used to authenticate a user and are used to enable single-sign-on. SAML authentication is commonly used with identity providers such as Active Directory Federation Services (ADFS) federated to Microsoft Entra ID and is therefore frequently used in enterprise applications. OpenID Connect is commonly used for apps that are purely in the cloud, such as mobile apps, web sites, and web APIs

SCIM

- **System for Cross-domain Identity Management** (SCIM) specification provides a common user schema to help users move into, out of, and around apps - *created to address the different methods/schema apps used to specify user information*

2 representations of applications in Microsoft Entra ID:

- **application objects (the blueprint, copy, recipe)** - define and describe the application to Microsoft Entra ID, enabling your identity provider to know how to issue tokens to the application based on its settings

- **service principals (the instance, cake)** - govern an application connecting to Microsoft Entra ID and can be considered.

Entitlement Management

When should I use access packages?

- Access packages don't replace other mechanisms for access assignment. They're most appropriate in situations such as when:
- Employees need time-limited access for a particular task. For example, you might use group-based licensing and a dynamic group to ensure all employees have an Exchange Online mailbox, and then use access packages for situations in which employees need additional access, such as to read departmental resources from another department.
- Access requires the approval of an employee's manager or other designated individuals.
- Departments wish to manage their own access policies for their resources without IT involvement.
- Two or more organizations are collaborating on a project, and as a result, multiple users from one organization will need to be brought in via Microsoft Entra B2B to access another organization's resources.the instance of the application in your directory.

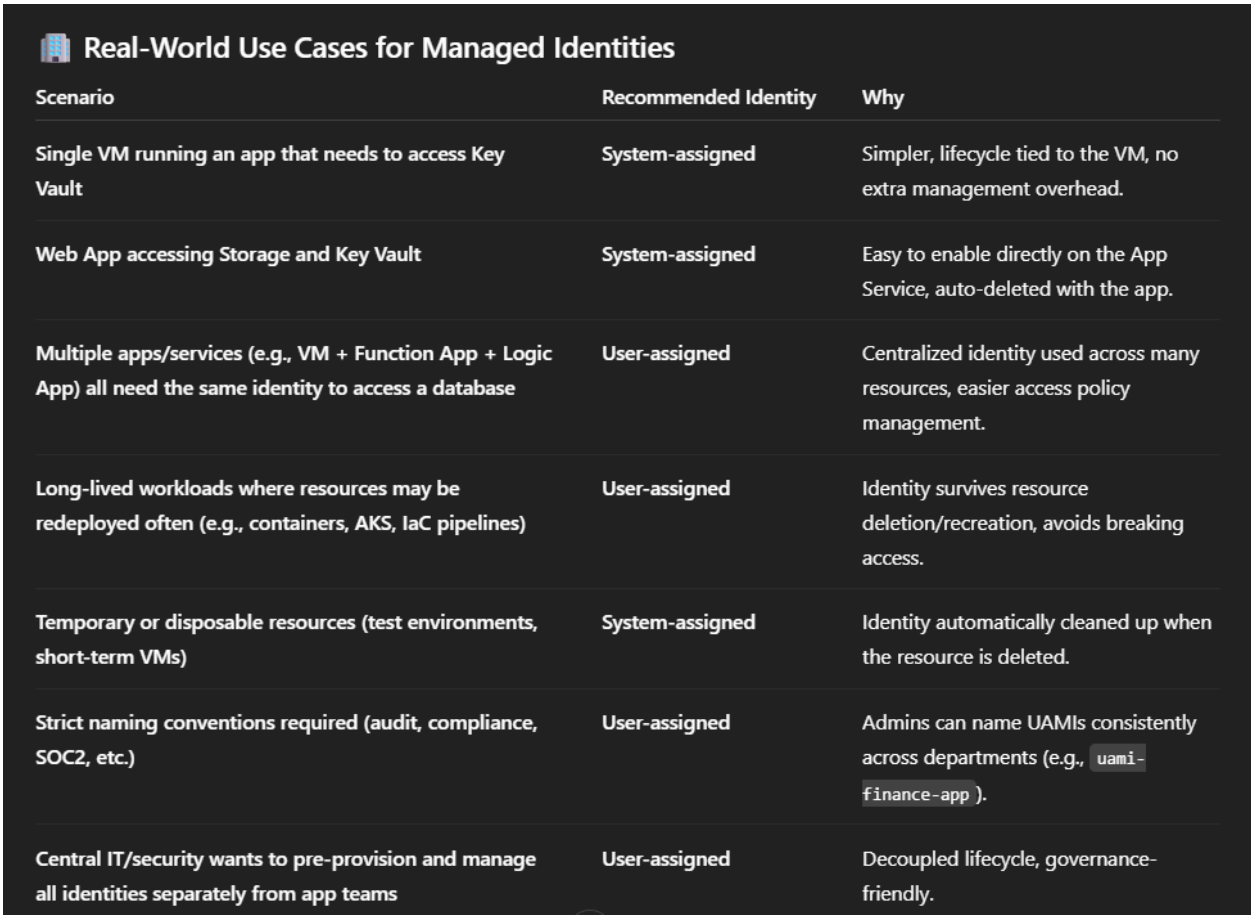
Catalog - is a container of resources and access packages.You create a catalog when you want to group related resources and access packages.

Access Review Policy Matrix

Group / Access Type	**Frequency**	**Reviewer**	**Duration**	**Upon Completion Setting**	**Notes / Best Practice**

Privileged Roles & Sensitive Groups *(Global Admins, Security Admins, Finance, HR, Compliance)*	Quarterly (every 3 months)	Group owner **+** Security/Compliance officer	14–30 days	**Remove access by default if not reviewed**	Strict governance; ensures least privilege; Microsoft recommended default
Business-Critical Apps & Departmental Groups *(Salesforce, SharePoint, Teams, Ops apps)*	Semi-annual (every 6 months)	Group owner or department manager	30 days	**Keep access by default if not reviewed**	Prevents accidental workflow disruption; non-reviewed accounts flagged for follow-up
General Access / Broad Groups *(All Employees, newsletters, collaboration)*	Annual (every 12 months)	Group owner	30 days	**Keep access by default** (system recommendation if enabled: remove if inactive 90+ days)	Light-touch governance; focus is on hygiene rather than strict removal
Dynamic Groups (automated by attributes)	Not applicable	Not applicable	Not applicable	Managed by automation	No manual review needed; relies on HR/attribute accuracy

Managed Identity SAMI v. UAMI:



🏢 Real-World Use Cases for Managed Identities

Scenario	Recommended Identity	Why
Single VM running an app that needs to access Key Vault	System-assigned	Simpler, lifecycle tied to the VM, no extra management overhead.
Web App accessing Storage and Key Vault	System-assigned	Easy to enable directly on the App Service, auto-deleted with the app.
Multiple apps/services (e.g., VM + Function App + Logic App) all need the same identity to access a database	User-assigned	Centralized identity used across many resources, easier access policy management.
Long-lived workloads where resources may be redeployed often (e.g., containers, AKS, IaC pipelines)	User-assigned	Identity survives resource deletion/recreation, avoids breaking access.
Temporary or disposable resources (test environments, short-term VMs)	System-assigned	Identity automatically cleaned up when the resource is deleted.
Strict naming conventions required (audit, compliance, SOC2, etc.)	User-assigned	Admins can name UAMIs consistently across departments (e.g., `uami-finance-app`).
Central IT/security wants to pre-provision and manage all identities separately from app teams	User-assigned	Decoupled lifecycle, governance-friendly.

Only 3 Azure roles can approve admin consent requests:

- Global Admin
- Cloud App Admin
- App Admin

You use a **Session Policy** in **Microsoft Defender for Cloud Apps (MDCA)** when you want to control **real-time user actions** in SaaS apps — such as **viewing, downloading, uploading, cutting, copying, or printing** files during an active session.

To manage policies, including access and session policies, you must have the **Global admin**, **Security admin**, or **Cloud App Security admin** role."

- If the question says "minimize administrative effort" → **Managed Identity**

- If the question says "non-Azure service or external system" → **Service Principal**

- If the question says "reuse one identity across several resources" → **User-assigned Managed Identity**

- If the question says "each resource should have its own" → **System-assigned Managed Identity**

ABAC in Azure is supported only for Azure Storage (specifically Blob and Queue data operations)

Only member users (like User1) can be made eligible for Azure AD roles in PIM; guest users and managed identities cannot.

User Admins can reset passwords only for users who are *non-admins* or have lower privilege.

A user can accept Terms of Use on any device, even if the device is not registered. Terms of Use enforcement occurs at sign-in, not based on device registration.

Managed identities can be added ONLY to:

- **Azure AD security groups**

- **Cloud-based groups**

- **Not Microsoft 365 groups**

- **Not dynamic groups**

- **Not Windows Server AD–synced groups**

- **Not distribution lists**

Azure AD cloud users can be added to:

- **Any assignable cloud group (security or M365)**

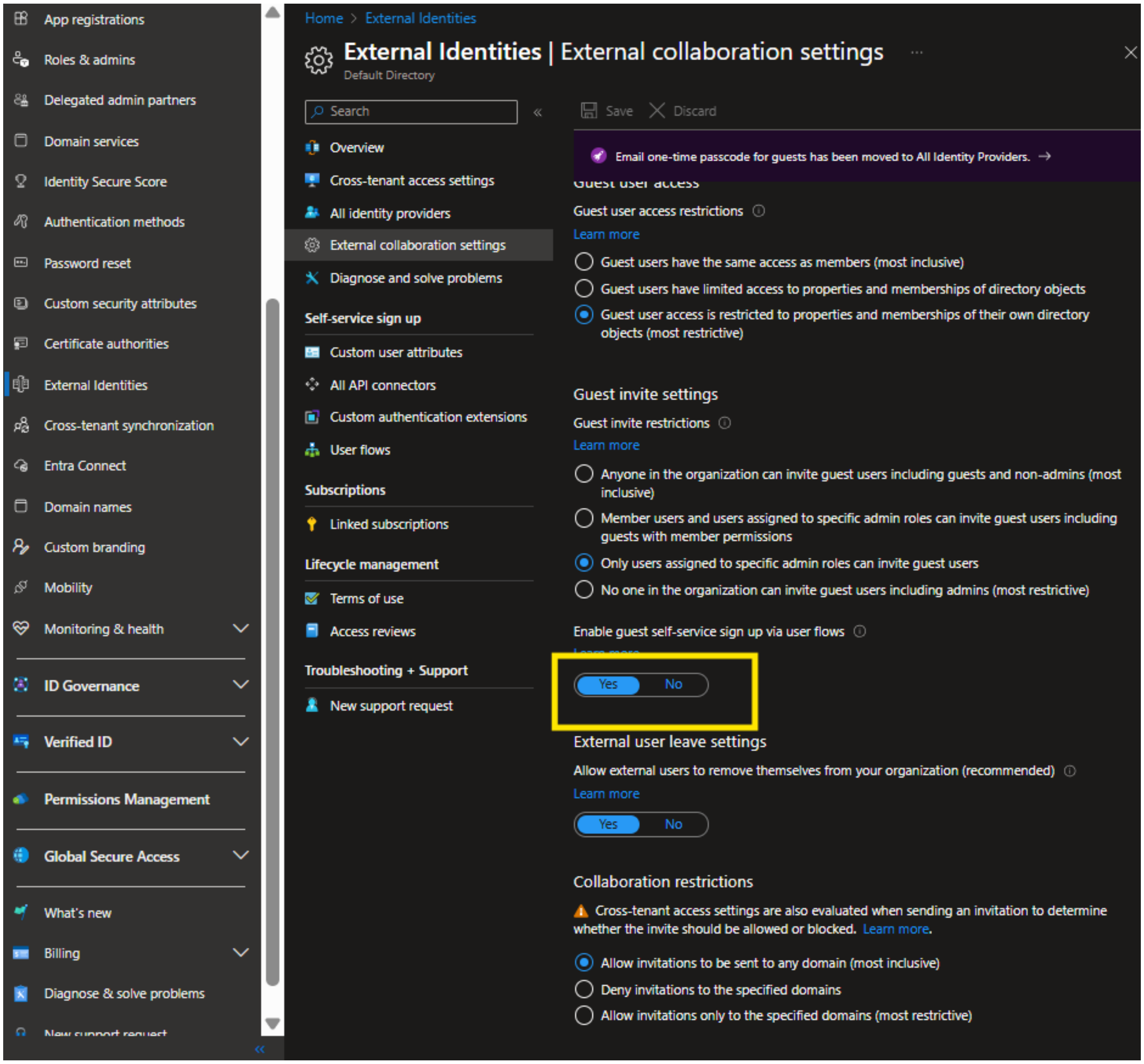
- **Not to dynamic membership groups**

- **Not to on-premises sync groups**

Configuring/managing a MS Entra tenant (labs)

Configuring external B2B collab settings in Entra ID (Least privilege access)

Enabled guest self-service sign up as well



External Identities | External collaboration settings

Default Directory

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions

Learn more

○ Guest users have the same access as members (most inclusive)

○ Guest users have limited access to properties and memberships of directory objects

● Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions

Learn more

○ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

○ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

● Only users assigned to specific admin roles can invite guest users

○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows

Learn more

[✓ Yes] No

External user leave settings

Allow external users to remove themselves from your organization (recommended)

Learn more

[✓ Yes] No

Collaboration restrictions

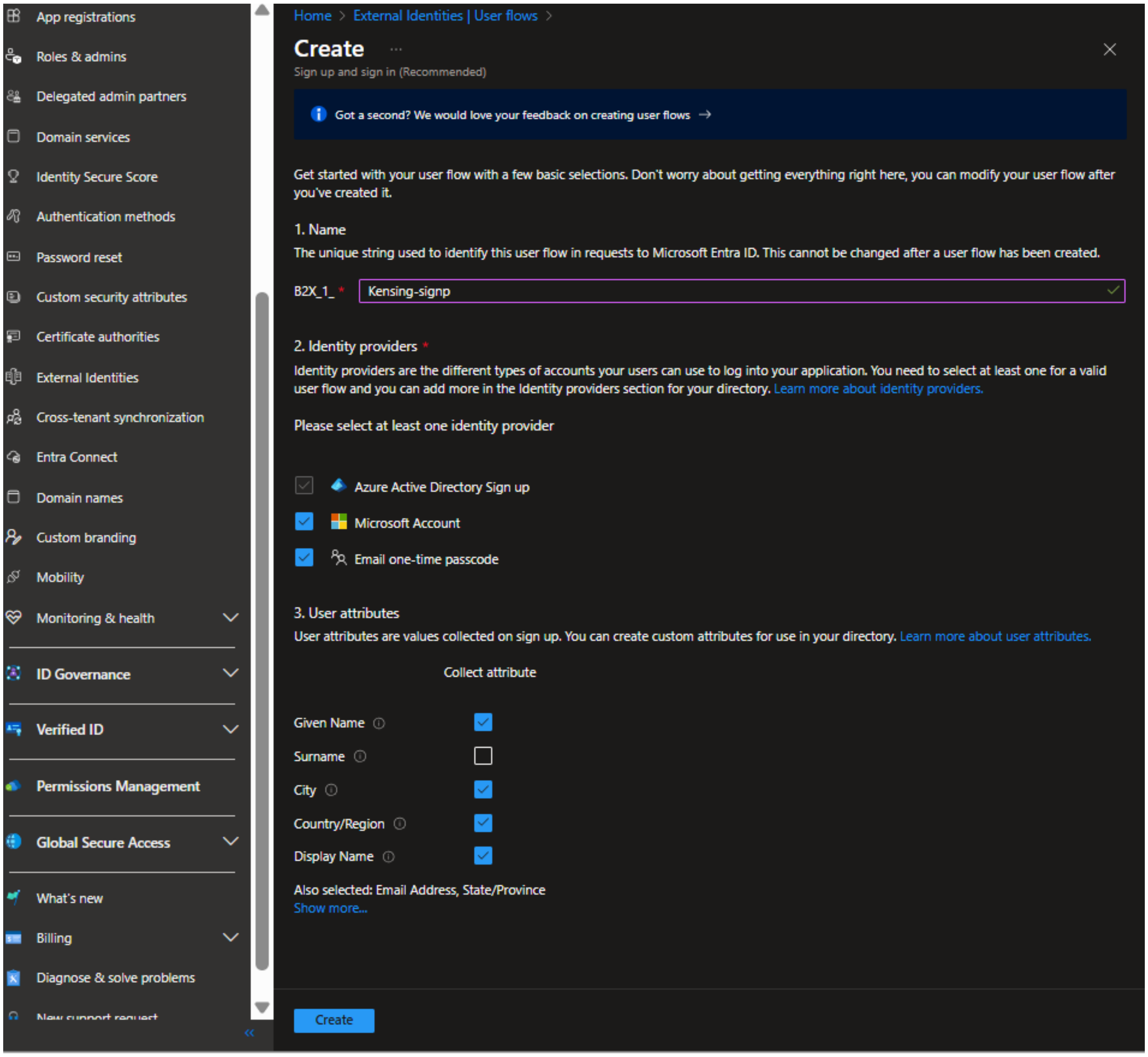
⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. Learn more.

● Allow invitations to be sent to any domain (most inclusive)

○ Deny invitations to the specified domains

○ Allow invitations only to the specified domains (most restrictive)

Created a new user flow for the self service sign up



Create

Sign up and sign in (Recommended)

Got a second? We would love your feedback on creating user flows →

Get started with your user flow with a few basic selections. Don't worry about getting everything right here, you can modify your user flow after you've created it.

1. Name

The unique string used to identify this user flow in requests to Microsoft Entra ID. This cannot be changed after a user flow has been created.

B2X_1_ * Kensing-signp

2. Identity providers *

Identity providers are the different types of accounts your users can use to log into your application. You need to select at least one for a valid user flow and you can add more in the Identity providers section for your directory. Learn more about identity providers.

Please select at least one identity provider

☑ Azure Active Directory Sign up

☑ Microsoft Account

☑ Email one-time passcode

3. User attributes

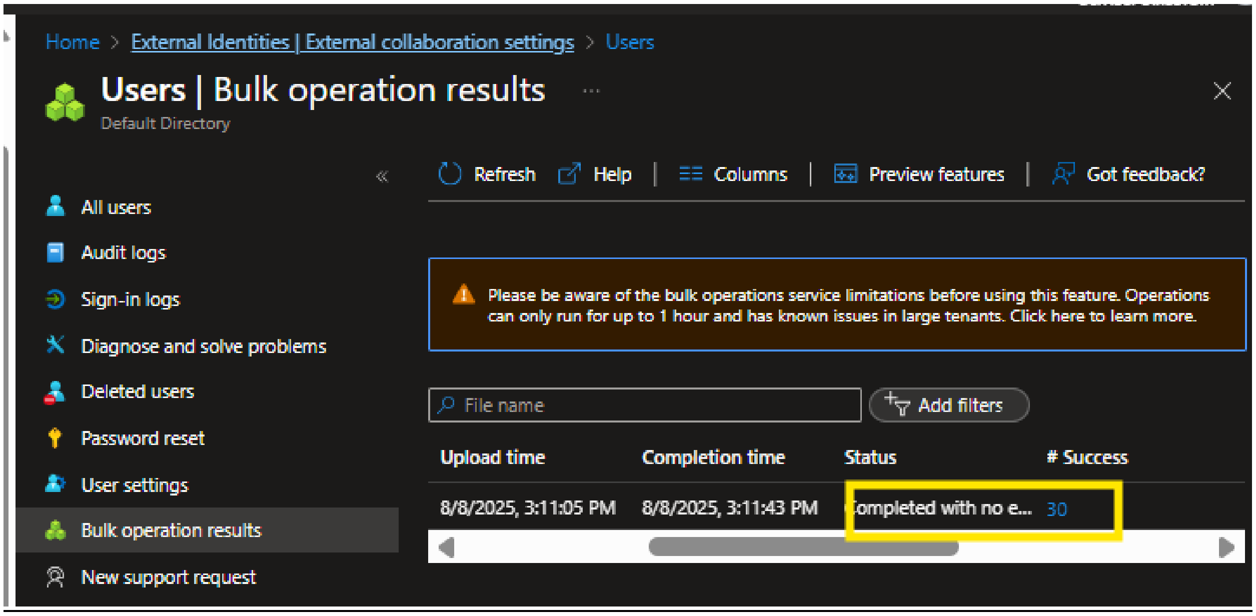
User attributes are values collected on sign up. You can create custom attributes for use in your directory. Learn more about user attributes.

	Collect attribute
Given Name ⓘ	☑
Surname ⓘ	□
City ⓘ	☑
Country/Region ⓘ	☑
Display Name ⓘ	☑

Also selected: Email Address, State/Province

Show more...

Bulk invited 30 guest users using .csv template



Home > External Identities | External collaboration settings > Users

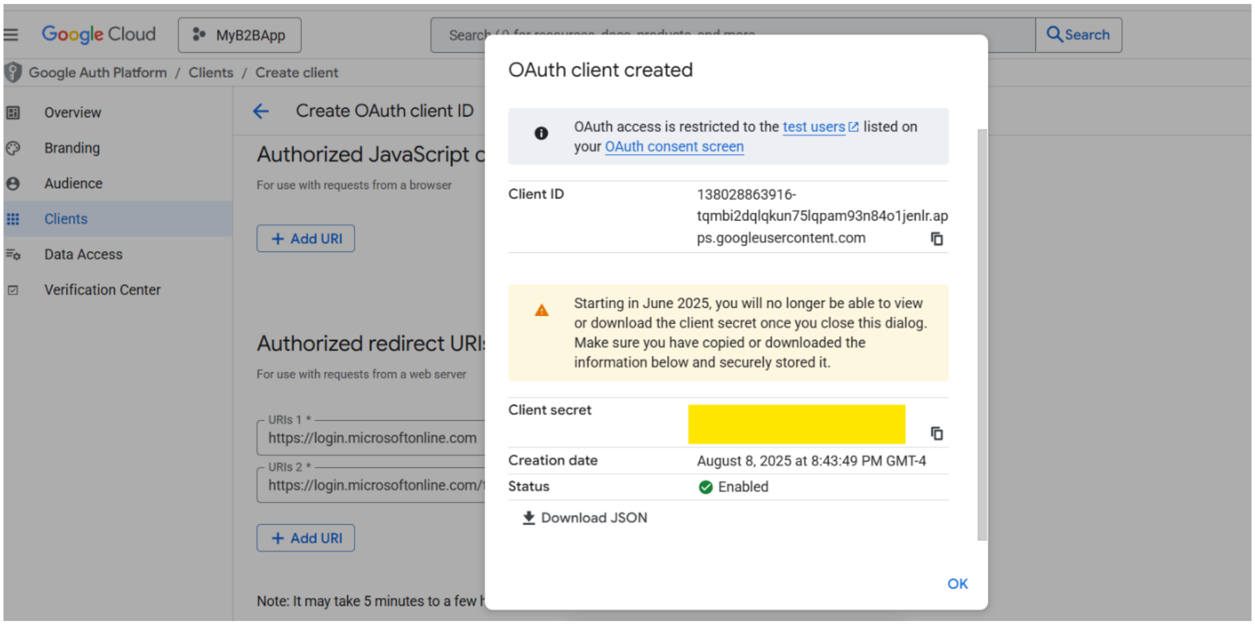
Users | Bulk operation results

Default Directory

Please be aware of the bulk operations service limitations before using this feature. Operations can only run for up to 1 hour and has known issues in large tenants. Click here to learn more.

Upload time	Completion time	Status	# Success
8/8/2025, 3:11:05 PM	8/8/2025, 3:11:43 PM	ompleted with no e...	30

Configured Google IdP via Drive API with OAuth client



Authorized JavaScript c

For use with requests from a browser

Authorized redirect URI

For use with requests from a web server

URIs 1 * https://login.microsoftonline.com

URIs 2 * https://login.microsoftonline.com/

Note: It may take 5 minutes to a few h

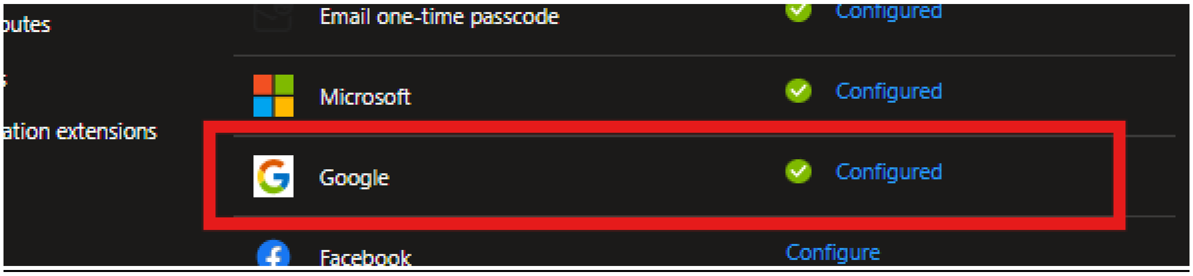
OAuth client created

OAuth access is restricted to the test users listed on your OAuth consent screen

Client ID	138028863916-tqmbi2dqlqkun75lqpam93n84o1jenlr.apps.googleusercontent.com

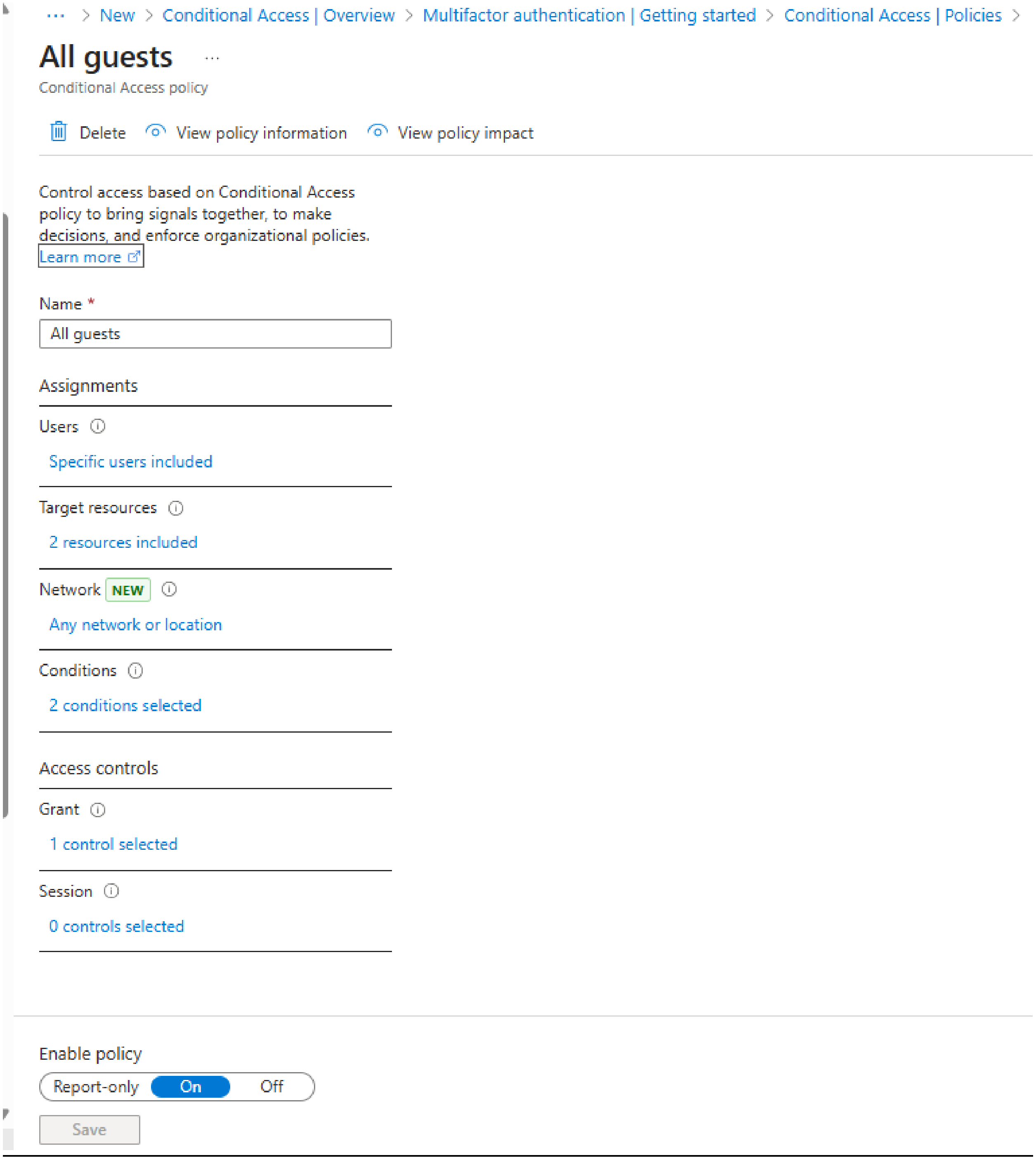
Starting in June 2025, you will no longer be able to view or download the client secret once you close this dialog. Make sure you have copied or downloaded the information below and securely stored it.

Client secret	[redacted]
Creation date	August 8, 2025 at 8:43:49 PM GMT-4
Status	✓ Enabled



Email one-time passcode	✓ Configured
Microsoft	✓ Configured
Google	✓ Configured
Facebook	Configure

Created Conditional Access policy to enforce MFA, by user/location/device



··· > New > Conditional Access | Overview > Multifactor authentication | Getting started > Conditional Access | Policies >

All guests ···

Conditional Access policy

Delete
View policy information
View policy impact

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

Name *

All guests

Assignments

Users ⓘ

Specific users included

Target resources ⓘ

2 resources included

Network NEW ⓘ

Any network or location

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

1 control selected

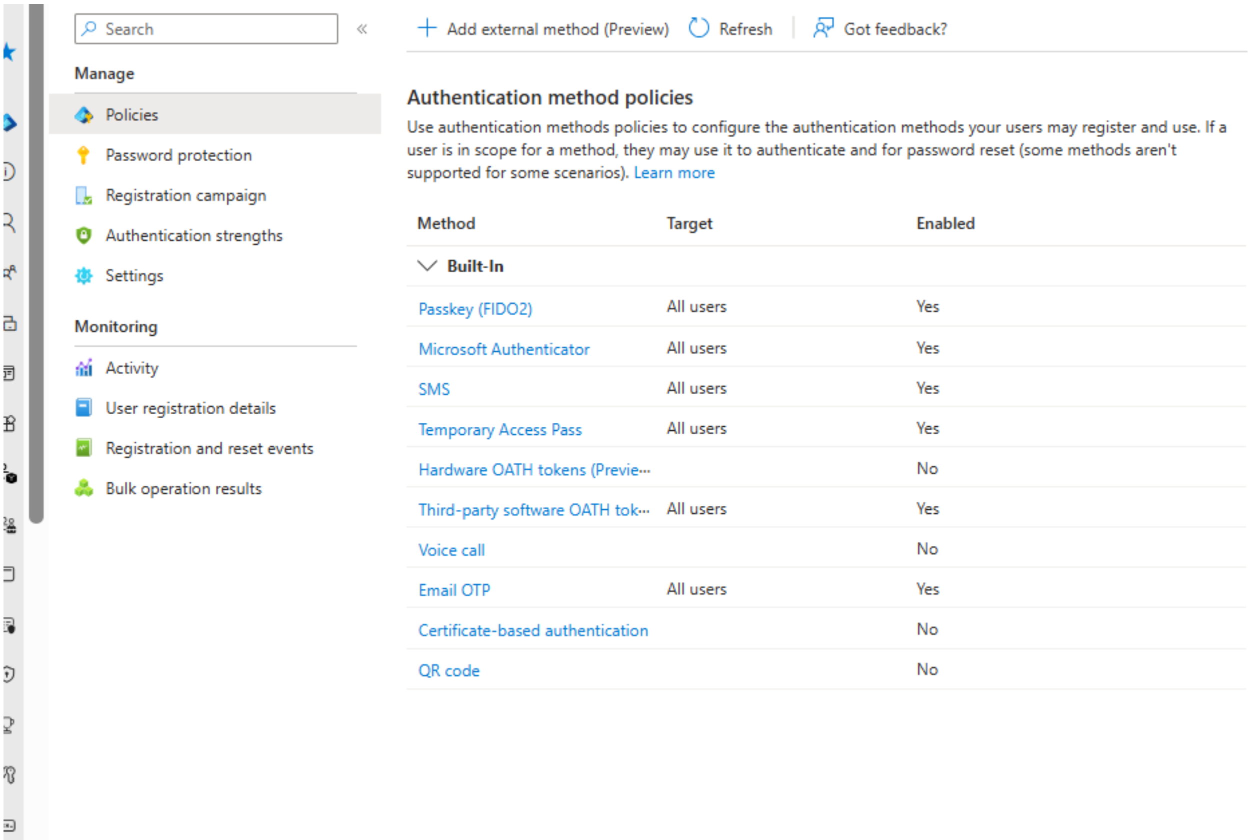
Session ⓘ

0 controls selected

Enable policy

Report-only [✓ On] Off

Enable multiple authN methods targeting All users (FIDO2, MSFT authenticator, etc.)

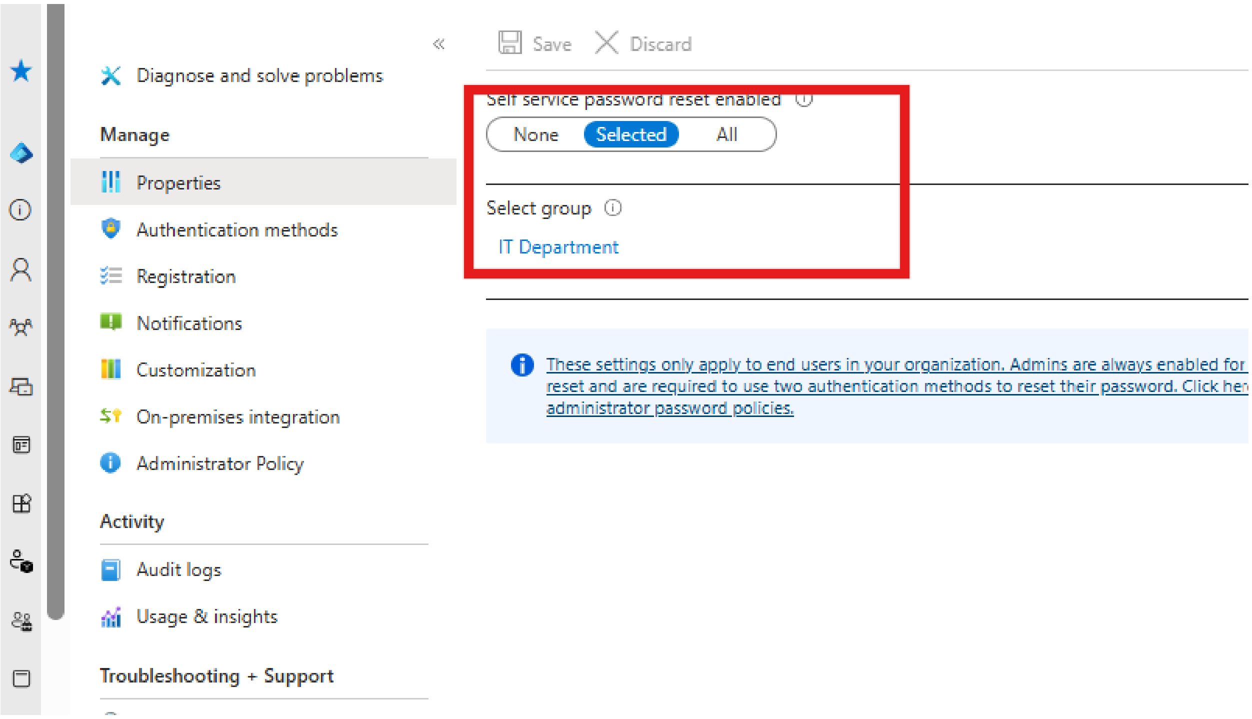


Authentication method policies

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

Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Previe...		No
Third-party software OATH tok...	All users	Yes
Voice call		No
Email OTP	All users	Yes
Certificate-based authentication		No
QR code		No

Enabled SSPR for a selected group

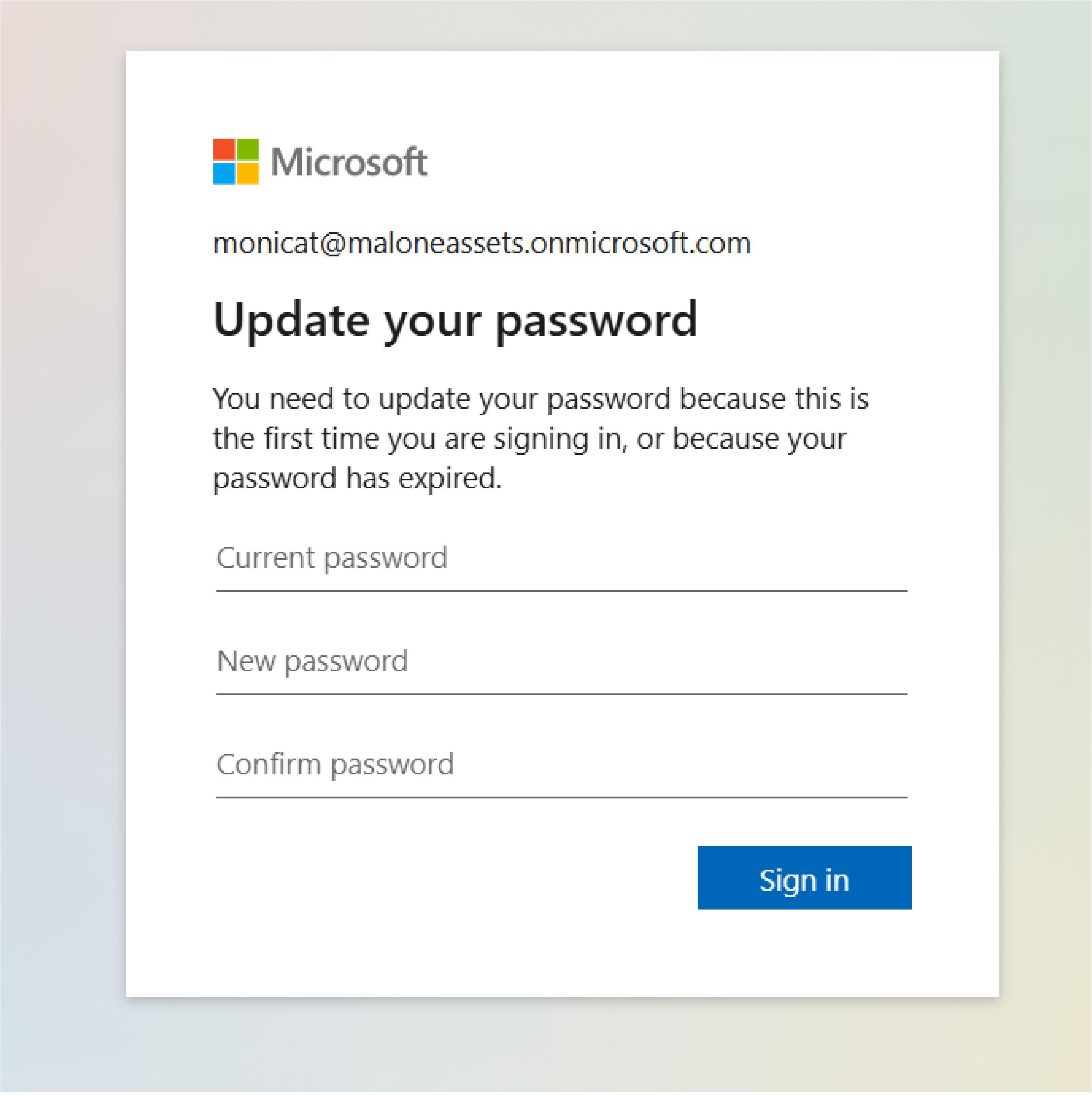


Self service password reset enabled: None [✓ Selected] All

Select group: IT Department

These settings only apply to end users in your organization. Admins are always enabled for reset and are required to use two authentication methods to reset their password. Click her administrator password policies.

Tested using credentials from a user in the group

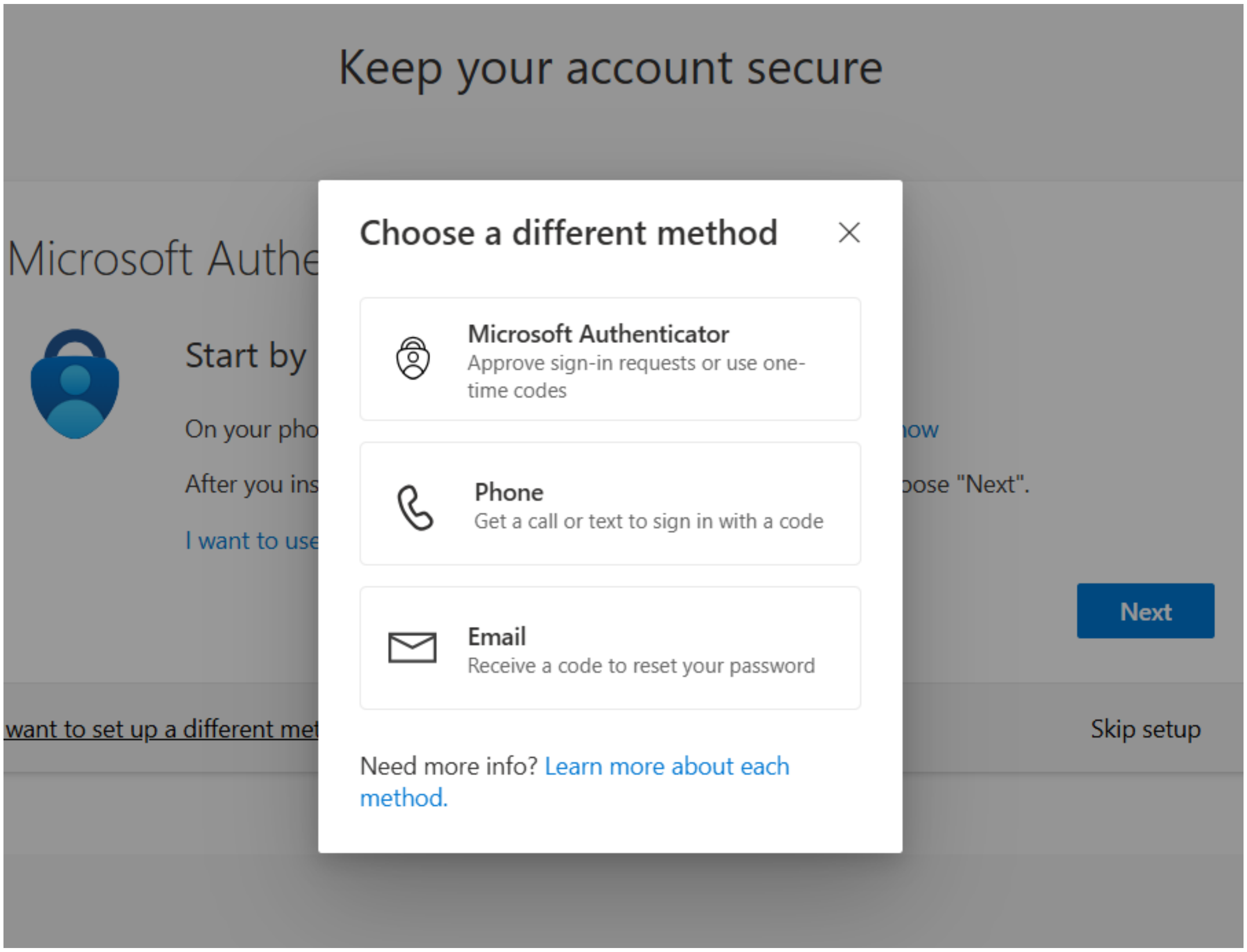


monicat@maloneassets.onmicrosoft.com

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Ensured multiple auth methods were available



Keep your account secure

Microsoft Authe

Start by

On your pho ow

After you ins ose "Next".

I want to use

Choose a different method

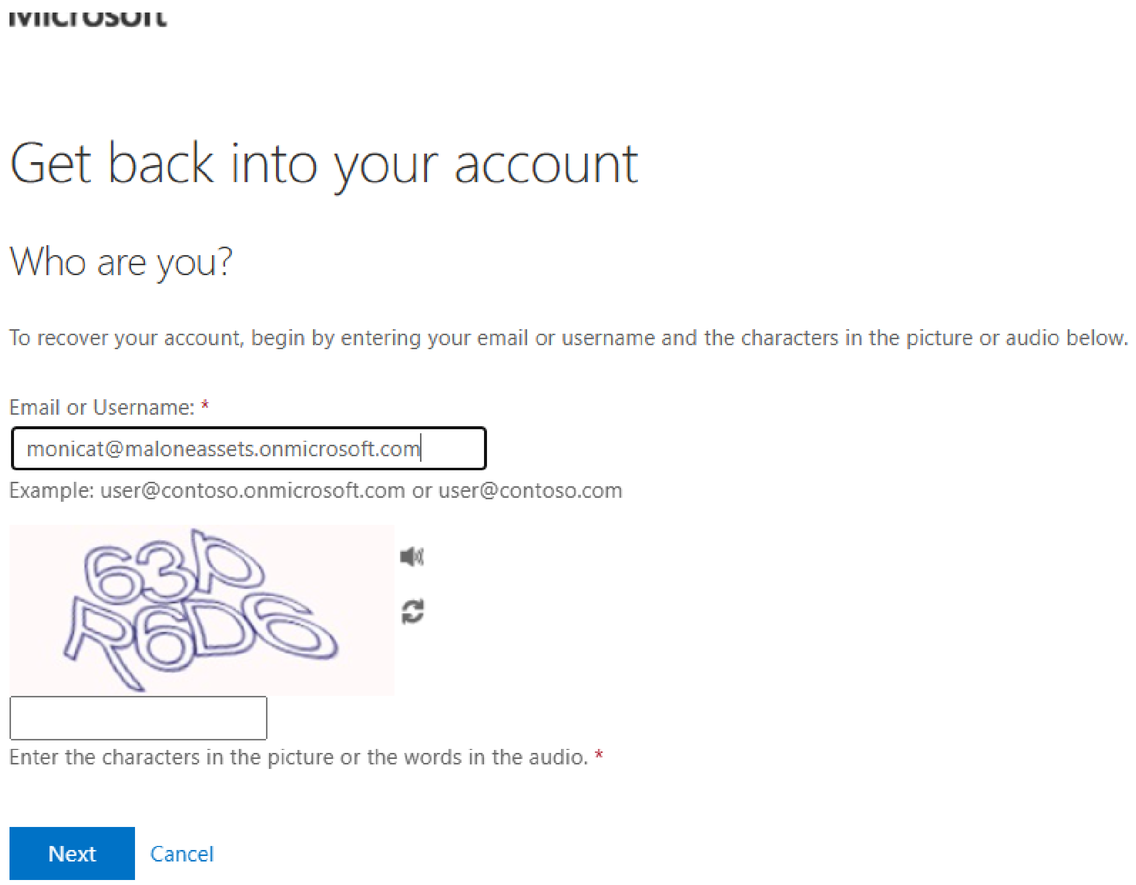
Microsoft Authenticator
Approve sign-in requests or use one-time codes

Phone
Get a call or text to sign in with a code

Email
Receive a code to reset your password

Need more info? Learn more about each method.

Tested Self Service Password Reset



Get back into your account

Who are you?

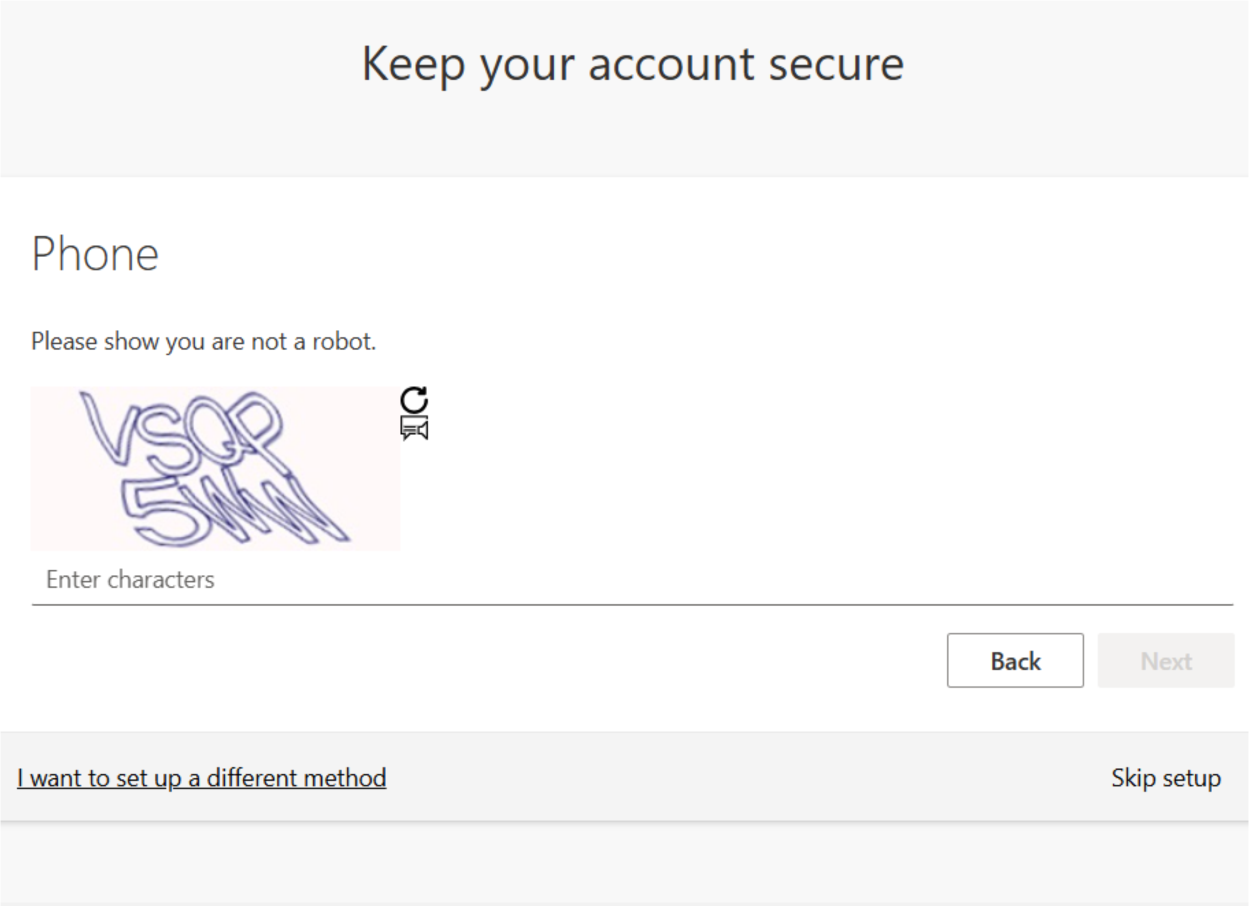
To recover your account, begin by entering your email or username and the characters in the picture or audio below.

Email or Username: *
monicat@maloneassets.onmicrosoft.com

Example: user@contoso.onmicrosoft.com or user@contoso.com

Enter the characters in the picture or the words in the audio. *

Met with a captcha



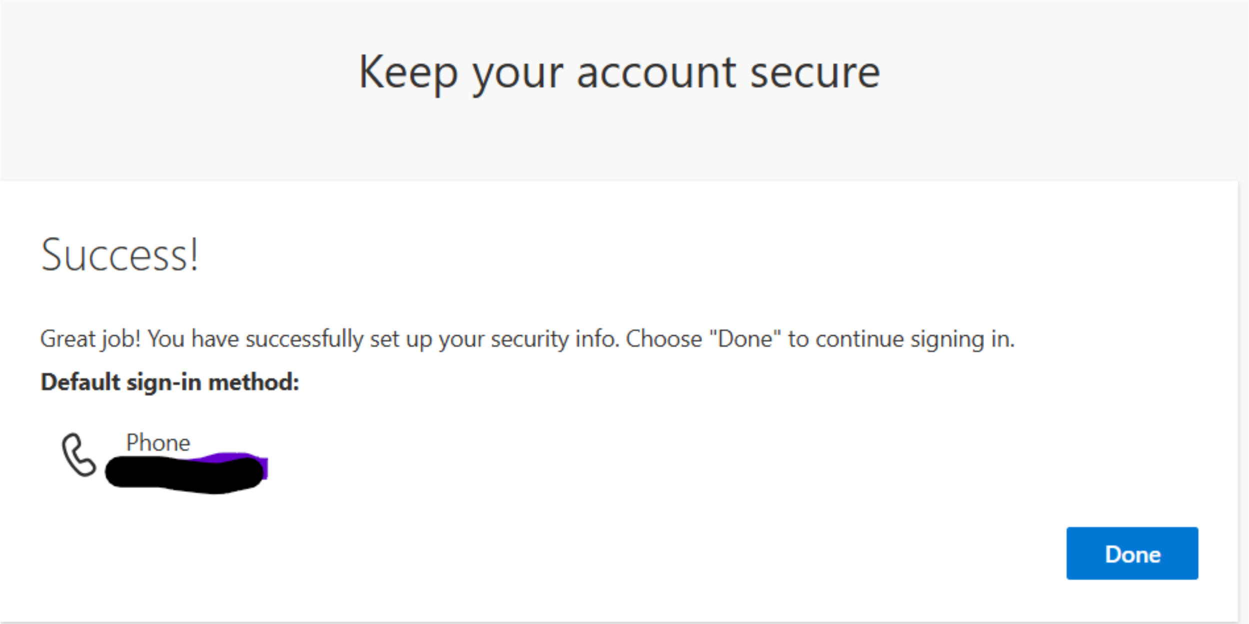
Keep your account secure

Phone

Please show you are not a robot.

Enter characters

Password reset successful



Keep your account secure

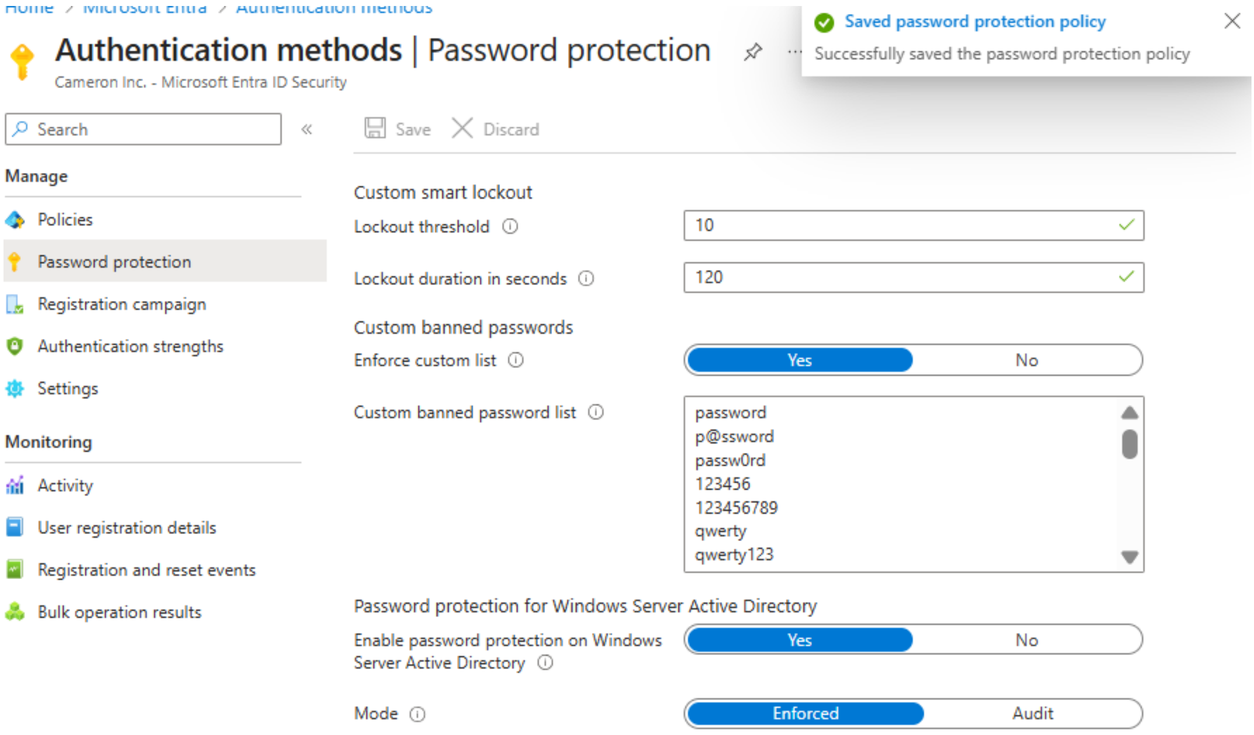
Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Phone
[redacted]

Managed smart lockouts by enforcing password protection



Home > Microsoft Entra > Authentication methods

Authentication methods | Password protection

Cameron Inc. - Microsoft Entra ID Security

Saved password protection policy

Successfully saved the password protection policy

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 120

Custom banned passwords

Enforce custom list: Yes

Custom banned password list:

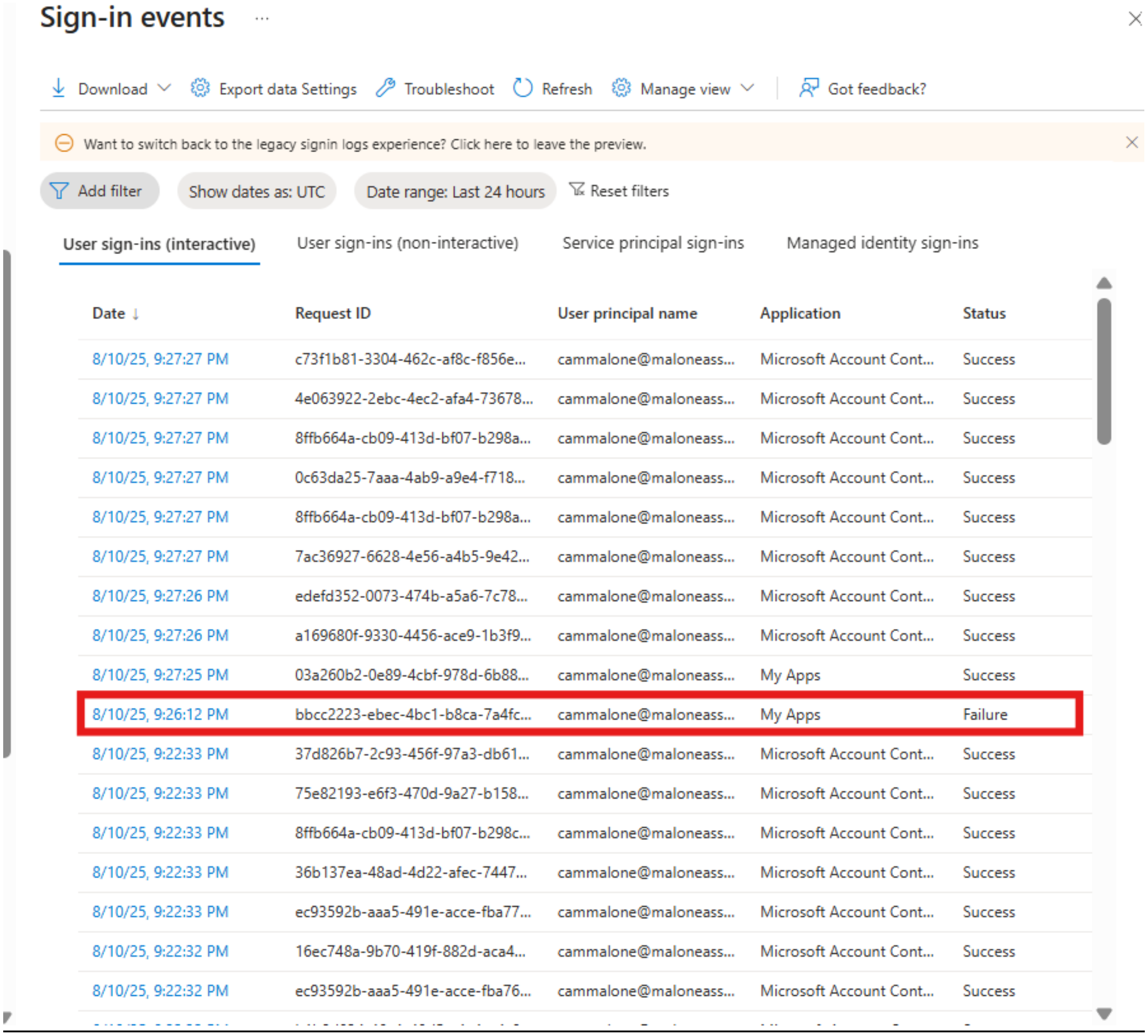
```
password
p@ssword
passw0rd
123456
123456789
qwerty
qwerty123
```

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes

Mode: Enforced

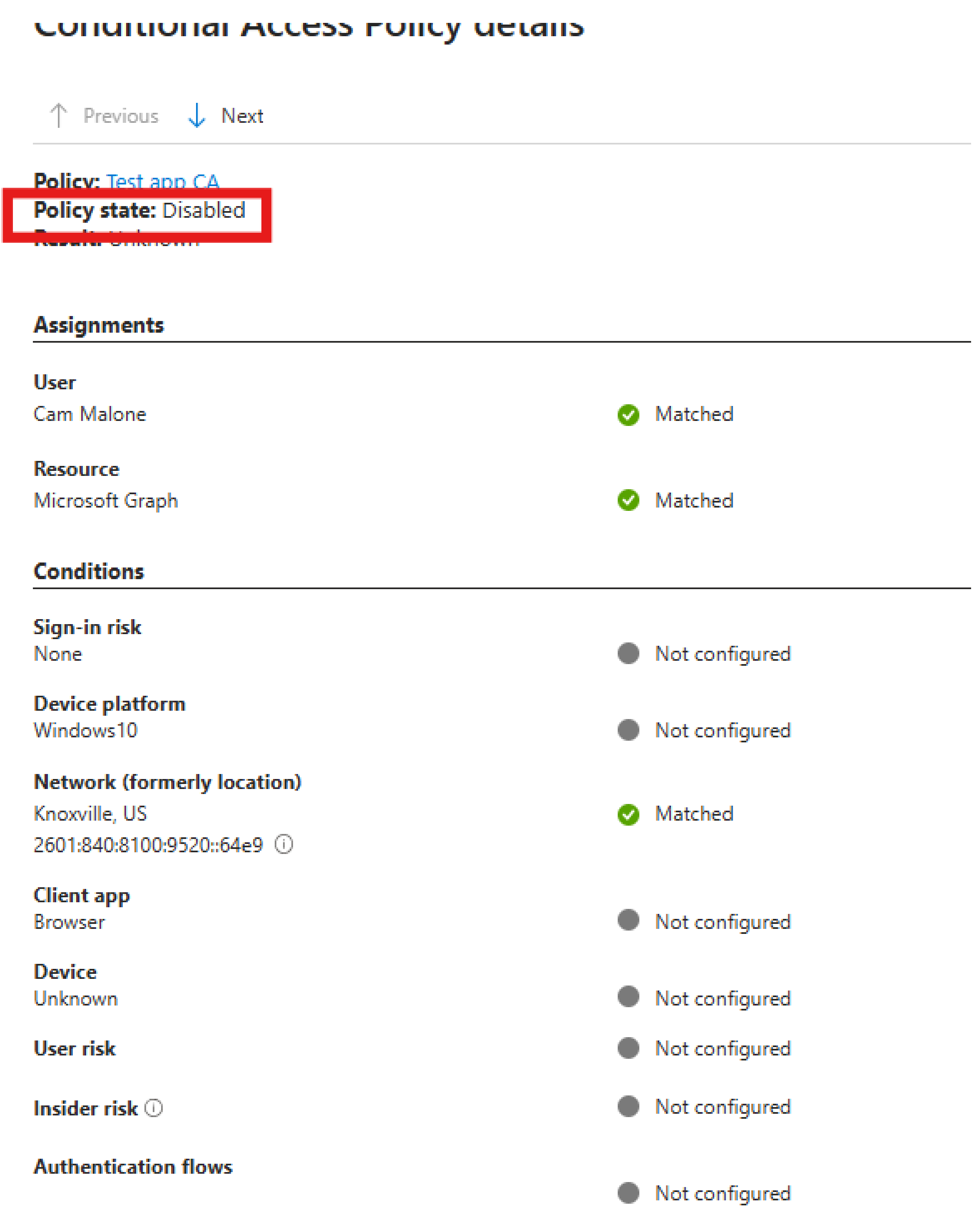
Reviewing CA logs to identify if any policies failed, and why



Sign-in events
Download
Export data Settings
Troubleshoot
Refresh
Manage view
Got feedback?
Want to switch back to the legacy signin logs experience? Click here to leave the preview.
Add filter
Show dates as: UTC
Date range: Last 24 hours
Reset filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

Date ↓	Request ID	User principal name	Application	Status
8/10/25, 9:27:27 PM	c73f1b81-3304-462c-af8c-f856e...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:27 PM	4e063922-2ebc-4ec2-afa4-73678...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:27 PM	8ffb664a-cb09-413d-bf07-b298a...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:27 PM	0c63da25-7aaa-4ab9-a9e4-f718...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:27 PM	8ffb664a-cb09-413d-bf07-b298a...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:27 PM	7ac36927-6628-4e56-a4b5-9e42...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:26 PM	edefd352-0073-474b-a5a6-7c78...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:26 PM	a169680f-9330-4456-ace9-1b3f9...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:27:25 PM	03a260b2-0e89-4cbf-978d-6b88...	cammalone@maloneass...	My Apps	Success
8/10/25, 9:26:12 PM	bbcc2223-ebec-4bc1-b8ca-7a4fc...	cammalone@maloneass...	My Apps	Failure
8/10/25, 9:22:33 PM	37d826b7-2c93-456f-97a3-db61...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:22:33 PM	75e82193-e6f3-470d-9a27-b158...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:22:33 PM	8ffb664a-cb09-413d-bf07-b298c...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:22:33 PM	36b137ea-48ad-4d22-afec-7447...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:22:33 PM	ec93592b-aaa5-491e-acce-fba77...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:22:32 PM	16ec748a-9b70-419f-882d-aca4...	cammalone@maloneass...	Microsoft Account Cont...	Success
8/10/25, 9:22:32 PM	ec93592b-aaa5-491e-acce-fba76...	cammalone@maloneass...	Microsoft Account Cont...	Success

The policy was disabled, resulting in a failure



Conditional Access Policy details

Policy: Test app CA

Policy state: Disabled

Result: Unknown

Assignments

User
Cam Malone
● Matched

Resource
Microsoft Graph
● Matched

Conditions

Sign-in risk
None
● Not configured

Device platform
Windows10
● Not configured

Network (formerly location)
Knoxville, US
2601:840:8100:9520::64e9 ⓘ
● Matched

Client app
Browser
● Not configured

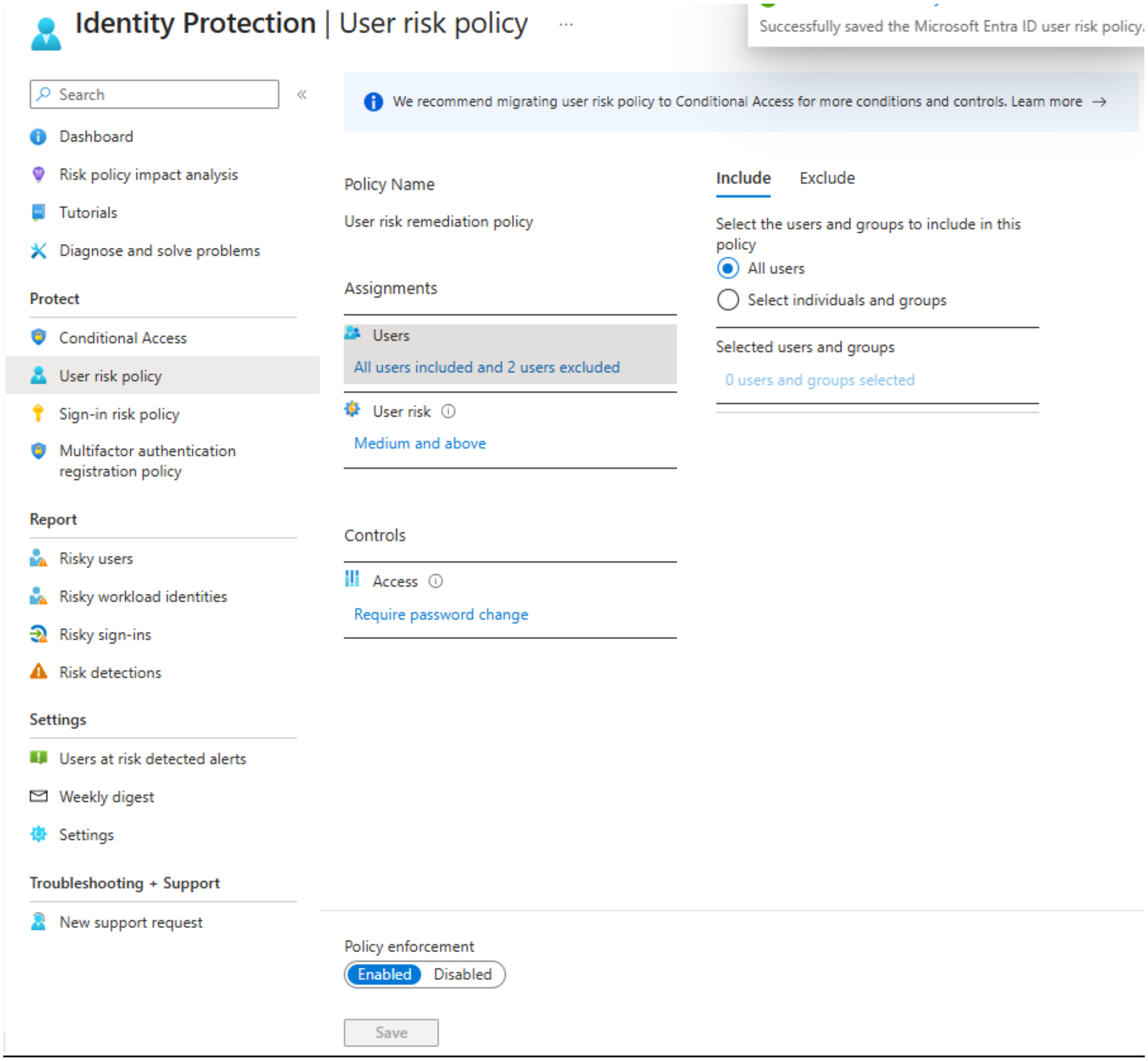
Device
Unknown
● Not configured

User risk
● Not configured

Insider risk ⓘ
● Not configured

Authentication flows
● Not configured

Implemented User risk & Sign-risk policies for all users, excluding emergency accounts



Identity Protection | User risk policy ...

Successfully saved the Microsoft Entra ID user risk policy.

We recommend migrating user risk policy to Conditional Access for more conditions and controls. Learn more →

Policy Name

User risk remediation policy

Assignments

Users

All users included and 2 users excluded

User risk ⓘ

Medium and above

Controls

Access ⓘ

Require password change

Select the users and groups to include in this policy

● All users

○ Select individuals and groups

Selected users and groups

0 users and groups selected

Policy enforcement

[✓ Enabled] Disabled

Configured Global Secure Access