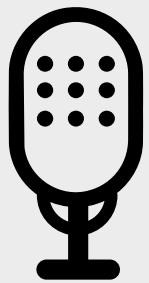
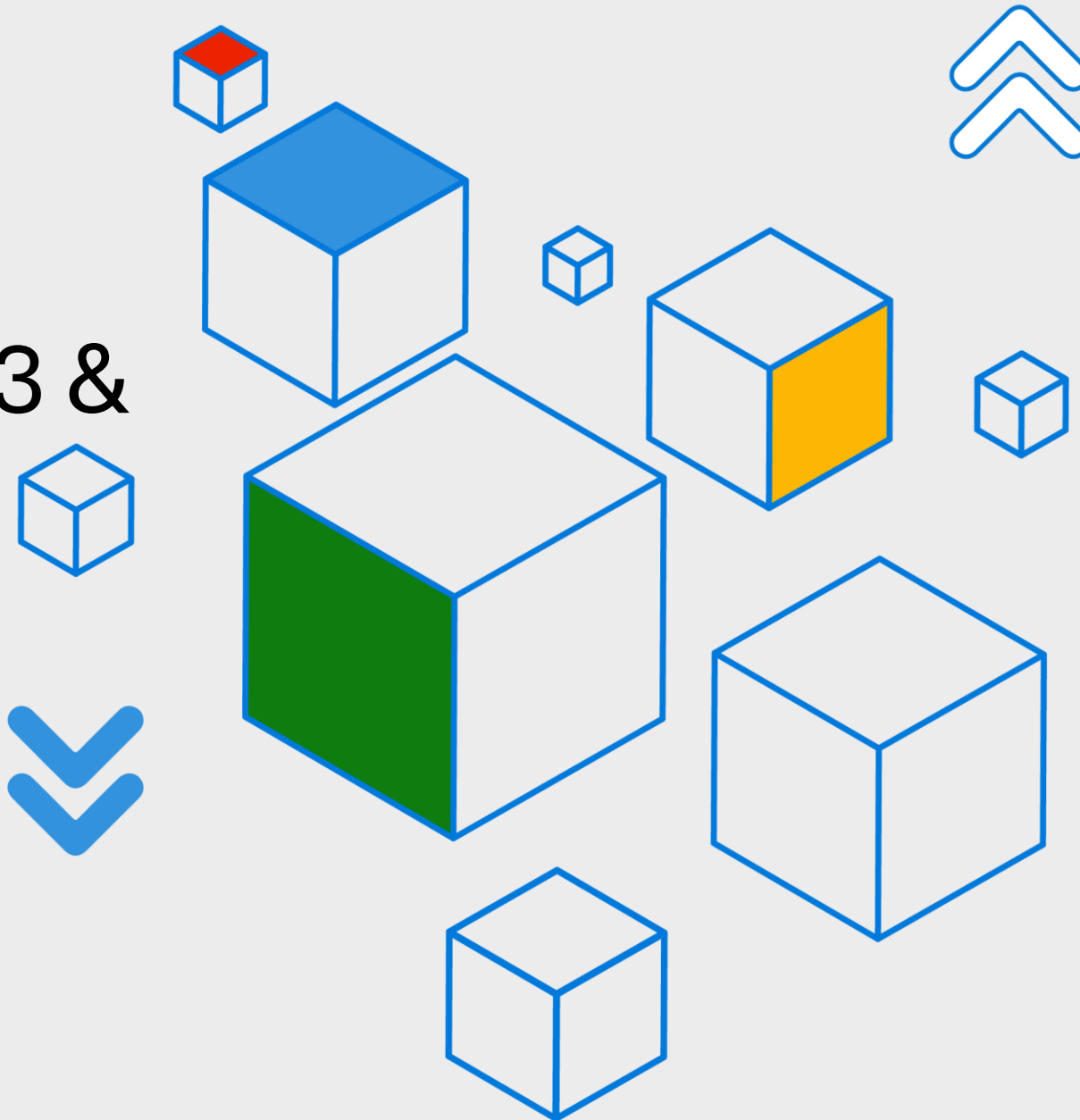


# What's New in Microsoft Entra ID December '23 & January '24



**425**Show



Grace Picking



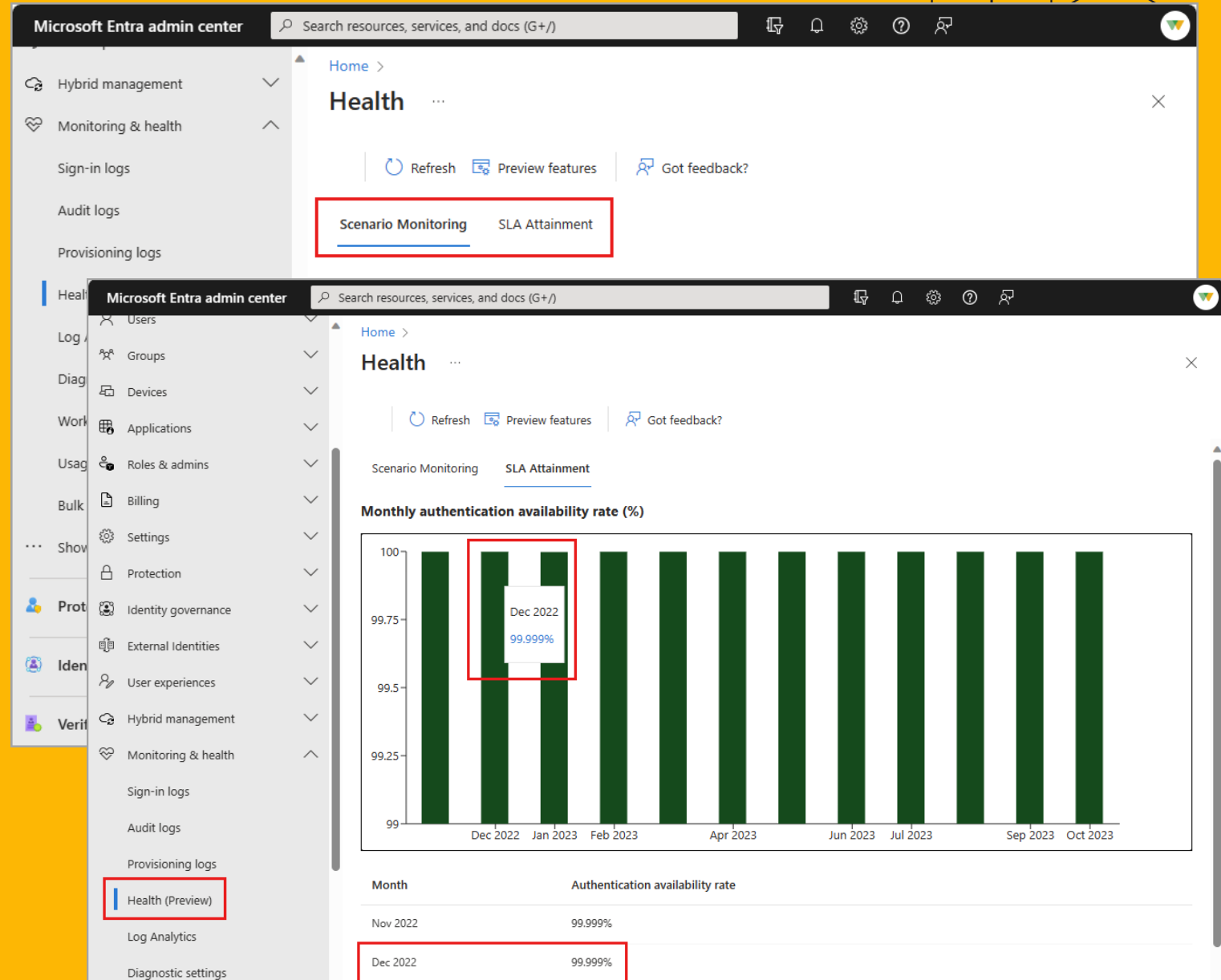
Jorge Lopez



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

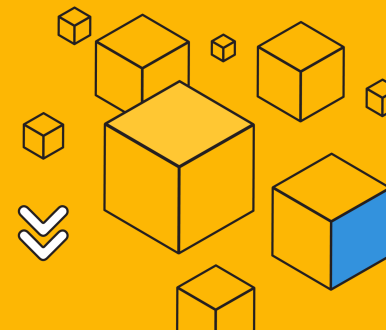
**Overview:** Provides you with the ability to view the health of your Microsoft Entra tenant through a report of service level agreement (SLA) attainment and a data stream of health metrics you can use to monitor key Microsoft Entra ID authentication scenarios.





425Show

# Last successful sign-in date for users



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** Additional property added to the signInActivity API to display the last successful sign-in time for a specific user, regardless if the sign-in was interactive or non-interactive.

GET beta https://graph.microsoft.com/beta/me?\$select=signInActivity

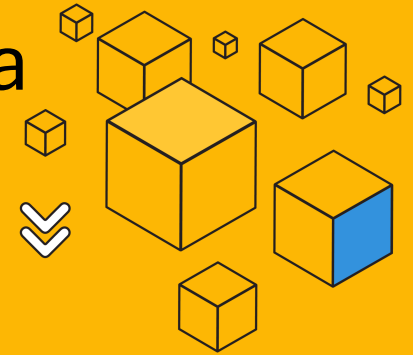
Request body Request headers Modify permissions Access token

OK - 200 - 873ms

Response preview Response headers Code snippets Toolkit component Adaptive cards

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#users(signInActivity)/$entity",
  "id": "41901d28-c724-42ed-a3f5-14a3201ddd32",
  "signInActivity": {
    "lastSignInDateTime": "2024-01-03T16:06:45Z",
    "lastSignInRequestId": "a42fa4c4-18ee-4f6d-8a94-477ac9da7305",
    "lastNonInteractiveSignInDateTime": "2024-01-03T16:07:05Z",
    "lastNonInteractiveSignInRequestId": "9b1b5743-dba8-4947-8bc6-277182e4f703",
    "lastSuccessfulSignInDateTime": "2024-01-03T16:07:05Z",
    "lastSuccessfulSignInRequestId": "9b1b5743-dba8-4947-8bc6-277182e4f703"
  }
}
```

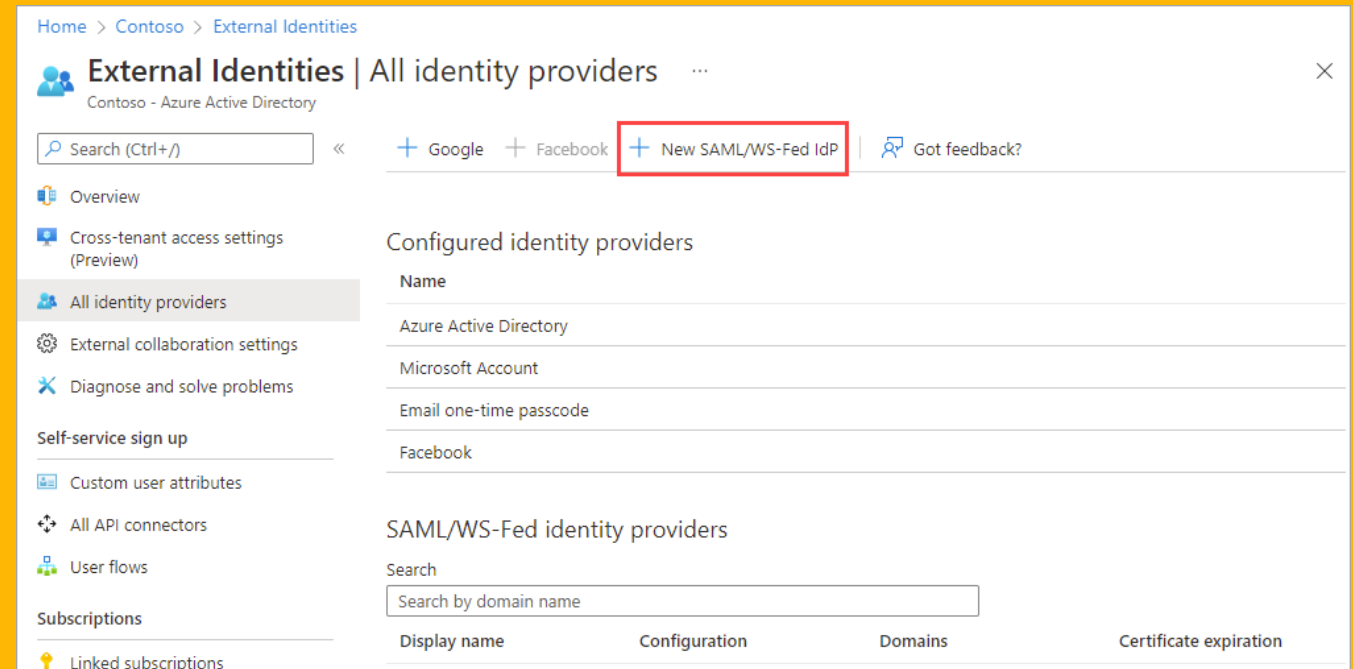
# SAML/WS-Fed identity provider for Microsoft Entra ID verified domains



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** Enables admins to invite Microsoft Entra ID guests with Microsoft Entra ID verified domains to redeem with a SAML/WS-Fed identity provider.



# Configurable redemption for B2B collaboration



**Stage :** Public Preview

**Product family:** Microsoft  
Entra ID

**Overview:** Provides you the ability to configure the redemption precedence order instead of using the one preset by Microsoft

Home > Inbound access settings - Default settings ...

B2B collaboration B2B direct connect Trust settings

B2B collaboration inbound access settings lets you collaborate with people outside of your organization by allowing them to sign in using their own identities. These users become guests in your Azure AD organization. You can invite external users directly or you can set up self-service sign-up so they can request access to your resources.  
[Learn more](#)

External users and groups Applications **Redemption order**

**Primary identity providers**

Users will redeem their invitations using the default order set by Microsoft. You can enable and specify the order of identity providers that your guest users can sign in with when they redeem their invitation.  
[Learn more](#)

↑ Move up ↓ Move down ↺ Reset to default

Identity provider	Enable provider
<input type="checkbox"/> Azure Active Directory	<input checked="" type="checkbox"/> Enabled
<input checked="" type="checkbox"/> SAML/WS-Fed Identity Providers	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/> Social providers (Google, Facebook)	<input checked="" type="checkbox"/> Enabled

**Fallback identity providers**

① Fallback identity providers are used when none of the primary identity providers are applicable. You must always have at least one fallback provider set to prevent users from being blocked while redeeming an invitation.

Identity provider	Enable provider
-------------------	-----------------

# Configurable Microsoft accounts in External Identities



**Stage :** Public Preview

**Product family:** Microsoft Entra ID

**Overview:** Provides you with the ability to remove consumer Microsoft accounts as an option for Microsoft Entra ID B2B guests. This feature prevents invited guests from using personal accounts and instead requires an account managed by an external organization

Home > Inbound access settings - Default settings ...

B2B collaboration B2B direct connect Trust settings

B2B collaboration inbound access settings lets you collaborate with people outside of your organization by allowing them to sign in using their own identities. These users become guests in your Azure AD organization. You can invite external users directly or you can set up self-service sign-up so they can request access to your resources. [Learn more](#)

External users and groups Applications **Redemption order**

**Primary identity providers**

Users will redeem their invitations using the default order set by Microsoft. You can enable and specify the order of identity providers that your guest users can sign in with when they redeem their invitation. [Learn more](#)

↑ Move up ↓ Move down ↺ Reset to default

Identity provider	Enable provider
<input type="checkbox"/> Azure Active Directory	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/> SAML/WS-Fed Identity Providers	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/> Social providers (Google, Facebook)	<input checked="" type="checkbox"/> Enabled

**Fallback identity providers**

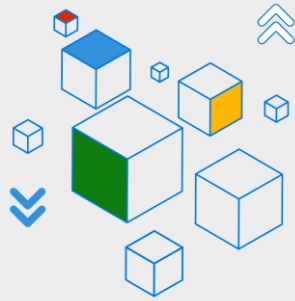
ⓘ Fallback identity providers are used when none of the primary identity providers are applicable. You must always have at least one fallback provider set to prevent users from being blocked while redeeming an invitation.

Identity provider	Enable provider
<input checked="" type="checkbox"/> Microsoft service account (MSA)	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/> Email one-time passcode	<input checked="" type="checkbox"/> Enabled



425Show

# Rich notifications in Microsoft Graph



**Stage : GA**

**Overview:** Allows you to subscribe to changes in your data and to receive notifications via webhooks and other methods. This feature supports various resources, such as messages, events, and contacts. Benefits include supplying richer information such as resource data and change type.

The encrypted notifications enhance security and privacy.

```
HTTP Copy

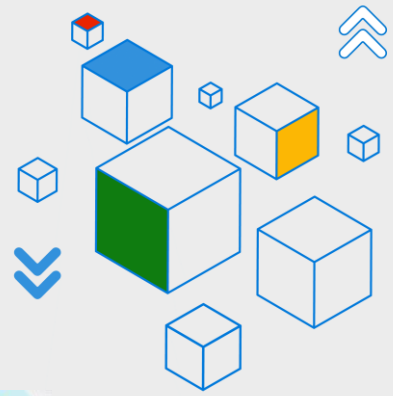
POST https://graph.microsoft.com/v1.0/subscriptions
Content-Type: application/json
{
  "changeType": "created,updated",
  "notificationUrl": "https://webhook.azurewebsites.net/api/resourceNotification",
  "resource": "/teams/{id}/channels/{id}/messages",
  "includeResourceData": true,
  "encryptionCertificate": "{base64encodedCertificate}",
  "encryptionCertificateId": "{customId}",
  "expirationDateTime": "2019-09-19T11:00:00.0000000Z",
  "clientState": "{secretClientState}"
}
```

[aka.ms/425show/RichNotifications](https://aka.ms/425show/RichNotifications)





# Single sign-on (SSO) and passwordless authentication for Azure Virtual Desktop and Windows 365



**Stage :** GA

**Product family :** Microsoft Entra ID

**Overview :** Provides passwordless SSO with Microsoft Entra ID authentication and WebAuthn redirection for in session passwordless authentication for Azure Virtual Desktop and Windows 365. It helps bring not only a better end-user experience, but also a more secure one with support for phish resistant credentials that satisfies Executive Order requirements in the United States



425 Show : <https://aka.ms/425Show/AVDSSO>





425Show

# Custom Security Attributes



Stage : GA

Product family : Microsoft Entra ID

**Overview:** Business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra objects.

These attributes can be used to store information, categorize objects, or enforce fine-grained access control over specific Azure resources.

Home > Users > Joe

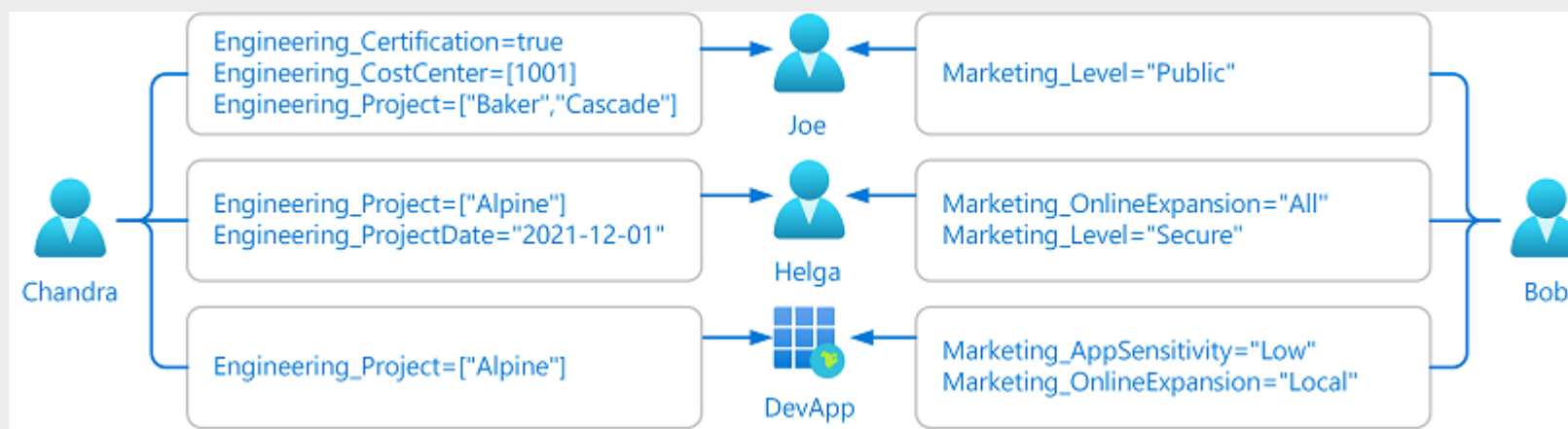
Joe | Custom security attributes

Search

Save Discard Add assignment Remove assignment Got feedback?

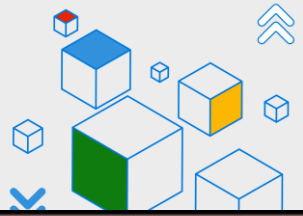
Search attribute names or values Add filters

<input type="checkbox"/>	Attribute set	Attribute name	Attribute description	Data type	Multi-valued	Assigned values	
<input type="checkbox"/>	Engineering	Certification	Certification status	Boolean	No	true	
<input type="checkbox"/>	Engineering	CostCenter	Project cost center	Integer	Yes	2 values	
<input type="checkbox"/>	Engineering	Project	Active projects for user	String	Yes	2 values	
<input type="checkbox"/>	Engineering	NumVendors	Number of vendors	Integer	No	8	
<input type="checkbox"/>	Marketing	EmployeeId	Employee identification	String	No	GS45897	
<input type="checkbox"/>	Engineering	ProjectDate	Target completion dat...	String	No	2023-11-15	



[aka.ms/425show/customsecurityattributes](https://aka.ms/425show/customsecurityattributes)

# Filter for applications in Conditional Access (CA)

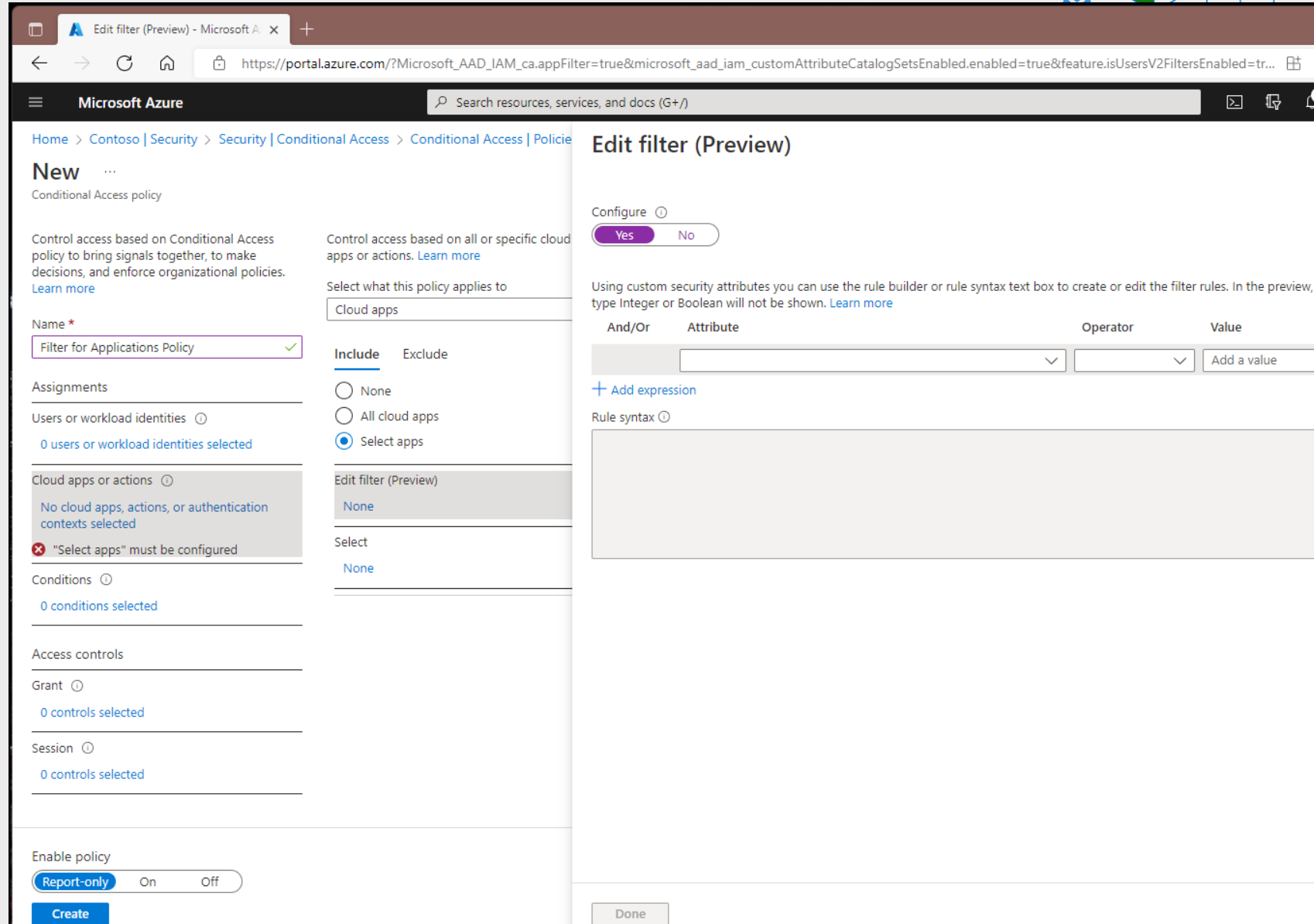


**Stage :** GA

**Product family :** Microsoft Entra ID

**Overview:** – Filters for apps in CA simplify policy management by allowing admins to tag apps with custom security attributes and target them in CA policies, instead of using direct assignments. With this feature you can scale up your policies and protect any number of apps, as the policy size won't increase when more apps are added. Workload identities can also be targeted with the new filter capability.

aka.ms/425show/CAfilterforapps



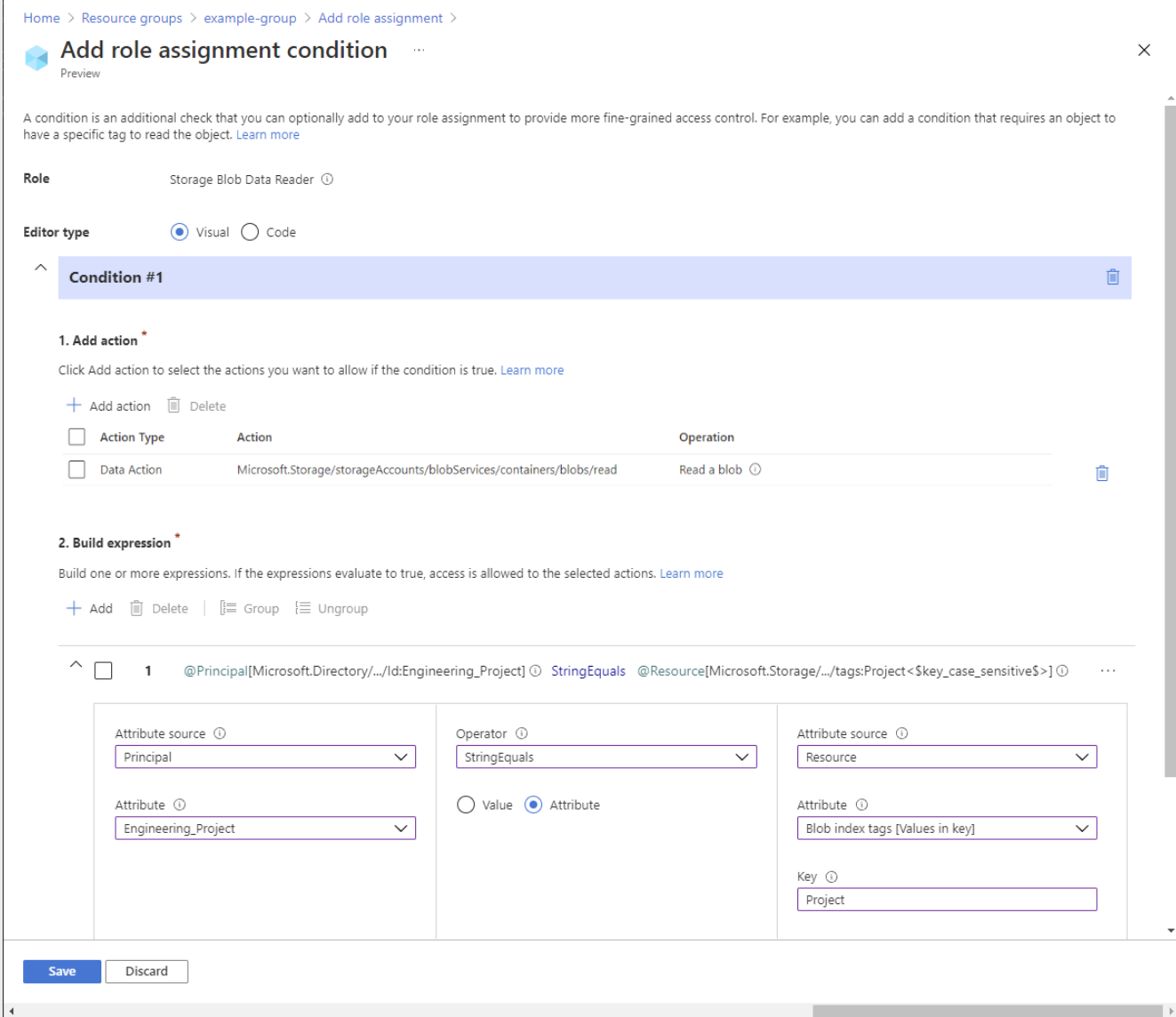
The screenshot displays the 'Edit filter (Preview)' page in the Microsoft Azure portal. The breadcrumb navigation shows the path: Home > Contoso | Security > Security | Conditional Access > Conditional Access | Policies. The page title is 'Edit filter (Preview)'. The 'Configure' section has a 'Yes' button selected. Below this, a table for building filter rules is visible with columns: And/Or, Attribute, Operator, and Value. The 'Rule syntax' section is currently empty. On the left sidebar, the 'Name' field is 'Filter for Applications Policy'. Under 'Assignments', 'Users or workload identities' is selected with '0 users or workload identities selected'. Under 'Cloud apps or actions', it shows 'No cloud apps, actions, or authentication contexts selected' and an error message: 'Select apps must be configured'. The 'Enable policy' section at the bottom has 'Report-only' selected, with 'On' and 'Off' options. A 'Create' button is at the bottom left, and a 'Done' button is at the bottom right.

# Azure ABAC conditions using principal attributes for Azure Storage

**Stage : GA**

**Product family :  
Microsoft Entra ID**

**Overview:** Authorize access to Azure Blob Storage based on blob index tags and custom security attributes assigned to users or applications.



Home > Resource groups > example-group > Add role assignment >

### Add role assignment condition

Preview

A condition is an additional check that you can optionally add to your role assignment to provide more fine-grained access control. For example, you can add a condition that requires an object to have a specific tag to read the object. [Learn more](#)

**Role** Storage Blob Data Reader ⓘ

**Editor type** ☒ Visual ☐ Code

**Condition #1** ⓘ

**1. Add action \***

Click Add action to select the actions you want to allow if the condition is true. [Learn more](#)

+ Add action ⓘ Delete ⓘ

<input type="checkbox"/> Action Type	Action	Operation
<input type="checkbox"/> Data Action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read	Read a blob ⓘ

**2. Build expression \***

Build one or more expressions. If the expressions evaluate to true, access is allowed to the selected actions. [Learn more](#)

+ Add ⓘ Delete ⓘ | [Group] ⓘ [Ungroup] ⓘ

1 @Principal[Microsoft.Directory/.../Id:Engineering\_Project] ⓘ StringEquals ⓘ @Resource[Microsoft.Storage/.../tags:Project<\$key\_case\_sensitive\$>] ⓘ ...

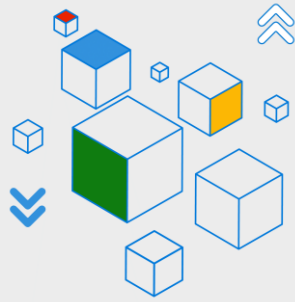
Attribute source ⓘ Principal ⓘ	Operator ⓘ StringEquals ⓘ <input type="radio"/> Value <input checked="" type="radio"/> Attribute	Attribute source ⓘ Resource ⓘ Attribute ⓘ Blob index tags [Values in key] ⓘ Key ⓘ Project ⓘ
-----------------------------------	--	--

Save Discard



425Show

# FIPS 140-3 enterprise compliance for Microsoft Authenticator app on Android



**Stage :** GA

**Product family :** Microsoft Entra ID

**Overview:** Beginning with version 6.2310.7174, Microsoft Authenticator for Android is compliant with Federal Information Processing Standard (FIPS 140-3) for all Microsoft Entra authentications, including phishing-resistant device-bound passkeys, push multi-factor authentication (MFA), passwordless phone sign-in (PSI) and time-based one-time passcodes (TOTP)





# Microsoft Entra CBA as Most Recently Used (MRU) method

**Stage : GA**

**Product family : Microsoft Entra ID**

**Overview:** Set once a user authenticates successfully using Microsoft Entra CBA, and the user's MRU authentication method is set to CBA. Next time, when the user enters their UPN and clicks Next, the user is taken to the CBA method directly and need not select Use the certificate or smart card.

**Select a certificate for authentication**

Site certauth.login.windows:443 needs your credentials:

mfauser	WoodgroveCA	9/21/2022
vance	WoodgroveCA	9/12/2022
vancede	WoodgroveCA	9/9/2022

[Certificate information](#) **OK** **Cancel**

← mfauser@woodgroveorg.net

**Enter password**

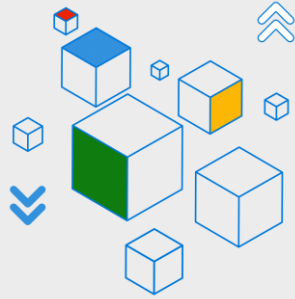
Password

[Forgot my password](#)

[Use a certificate or smart card](#)

**Sign in**

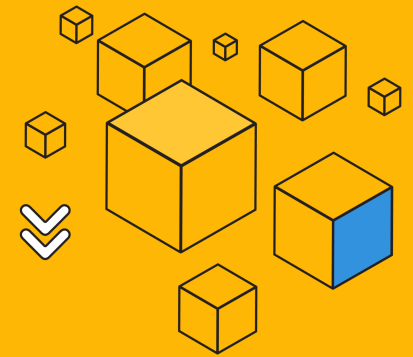
aka.ms/425show/CBA





425Show

# Microsoft Entra CBA: support for additional username bindings



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** Adds three additional bindings, including subject, issuer+subject and issuer+serial number.

Add username binding policy rule

Certificate field \*

Select certificate field

High affinity

Issuer and serial number

SKI (already configured)

SHA1PublicKey (already configured)

Low affinity

PrincipalName (already configured)

RFC822Name (already configured)

Issuer and subject

Subject

[aka.ms/425show/CBA](https://aka.ms/425show/CBA)

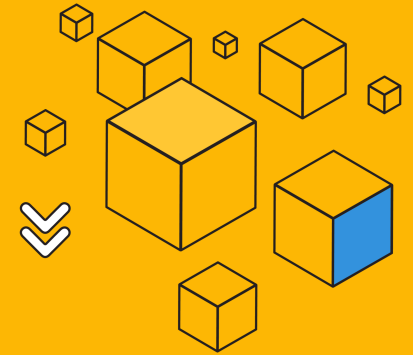


# Microsoft Entra certificate-based authentication (CBA) as second factor

**Stage :** Public Preview

**Product family:** Microsoft Entra ID

**Overview:** Microsoft Entra CBA can be used as a second factor to meet MFA requirements with single-factor certificates



**Add authentication binding policy rule**

Certificate attribute

☒ Certificate issuer

☐ Policy OID

Certificate issuer identifier ⓘ

CN=CBATestRootProd ▼ \*

Authentication strength \*

☐ Single-factor authentication

☒ Multi-factor authentication

Affinity binding \*

☒ Low

☐ High

**Add** Cancel

[aka.ms/425show/CBA](https://aka.ms/425show/CBA)





# Microsoft Entra certificate-based authentication (CBA): issuer and OID support on the authentication method policy

**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** Admins can now configure certificate strength as well as the username binding used to authenticate a certificate by issuer and Policy OID values.

aka.ms/425show/CBA

Search resources, services, and docs (G+)

Home > Authentication methods | Policies >

Certificate-based authentication settings

Certificate-based authentication is a passwordless, phishing-resistant authentication method that uses x.509 certificates and an enterprise public key infrastructure (PKI) for authentication. [Learn more.](#)

Enable and TargetConfigure

Authentication binding

The authentication binding policy helps determine the strength of your certificate-based authentication method policy as single-factor or multi-factor and low affinity or high affinity. Override default settings with special rules. [Learn more](#)

Protection Level ⓘ

Single-factor authentication

Multi-factor authentication

Required Affinity Binding ⓘ

Low

High

+ Add rule

Certificate issuer	Policy OID	Authentication strength	Affinity binding	
CN=WOODGROVECA	N/A	Single-factor	Low	...
N/A	1.2.3.4	Multi-factor	Low	...

Username binding

Select one of the X.509 certificates fields to bind with one of the user attributes in the cloud. [Learn more](#)

+ Add rule

Certificate field	Affinity binding	User attribute	
PrincipalName	Low	userPrincipalName	...
Issuer and serial number	High	CertificateUserIDs	...
SKI	High	CertificateUserIDs	...
RFC822Name	Low	userPrincipalName	...

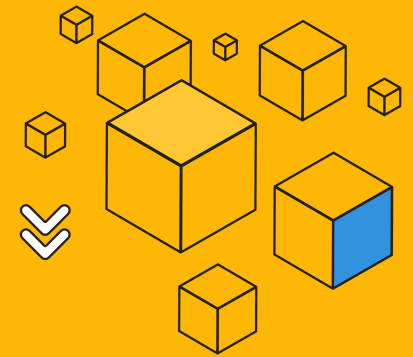
Save

Discard



425Show

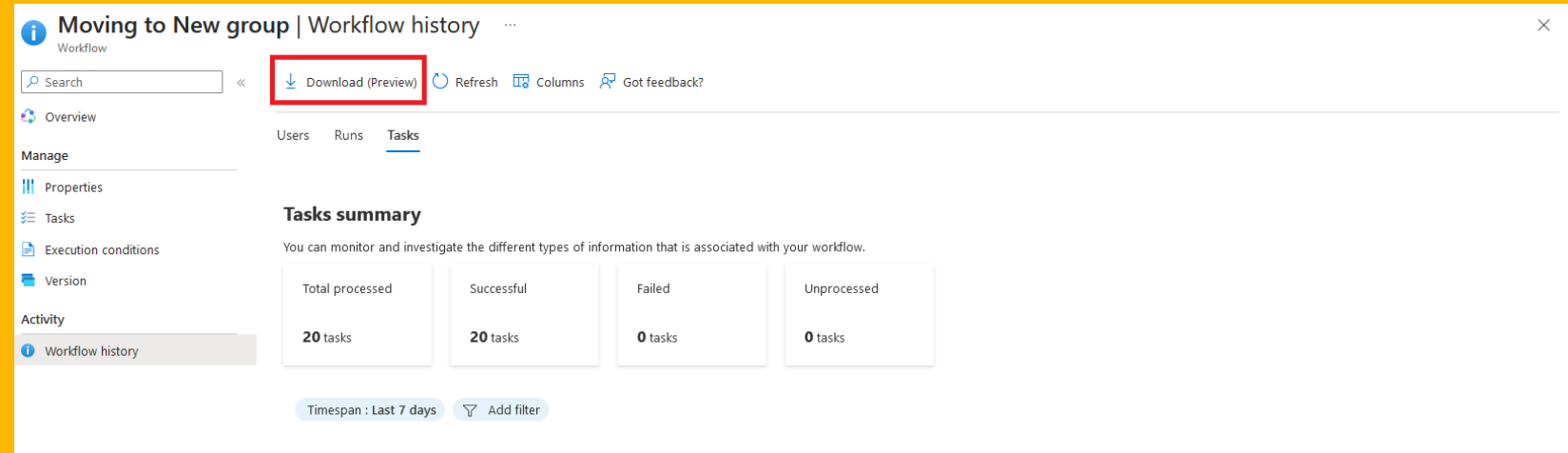
# Lifecycle workflows: Download workflow history reports



**Stage :** Public Preview

**Product family:** Microsoft Entra ID

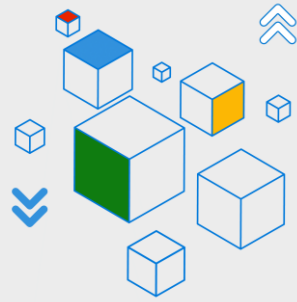
**Overview:** Allows you to download Lifecycle Workflows' existing workflow history reports as comma-separated values (CSV) file via the Microsoft Entra admin center.



[aka.ms/425show/LCWHistory](https://aka.ms/425show/LCWHistory)



# Microsoft Entra ID Governance: inactive guest insights



Stage : GA

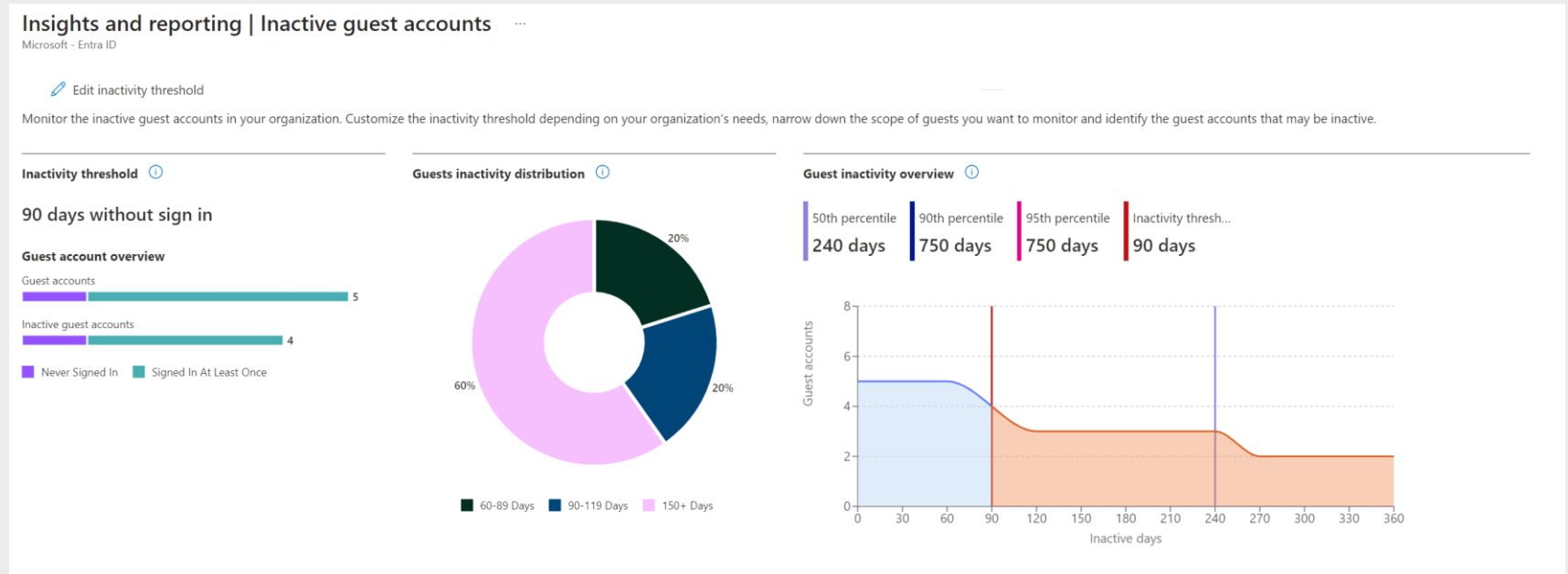
**Product family :**  
Microsoft Entra ID  
Governance

**Overview:** Allows you to monitor guest accounts at scale

with intelligent insights into inactive guest users in your organization. You can customize the inactivity

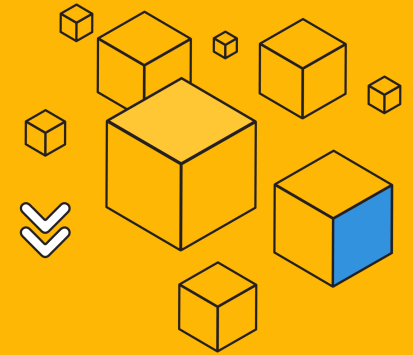
threshold depending on your organization's needs, narrow down the scope of guest users you want to

monitor and identify the guest users that may be inactive.



[aka.ms/425show/IDGInactiveGuests](https://aka.ms/425show/IDGInactiveGuests)

# AD FS to Microsoft Entra ID application migration wizard



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview:** Analyzes an AD FS environment to identify compatible applications ready to migrate to Microsoft Entra ID and provides step-by-step guidance

Dashboard > ADFS Ogma Team PPE | Usage & insights >

## Usage & insights | Application Migration (Preview)

ADFS Ogma Team PPE

Manage

- Application Migration (Preview)

Usage & insights

- Azure AD application activity (Preview)
- AD FS application activity
- Authentication methods activity
- Service principal sign-in activity (Preview)
- Application credential activity (Preview)
- License Utilization

Refresh

Improve your organizations security by migrating your applications to Azure AD.

- Read our quick migration guide
- Add your application to Azure AD using this quick migration flow.
- If necessary, adjust the configuration in Azure AD.
- Configure the AD FS application to point to Azure AD.

All apps  
24 of 24  
Application report

Ready to migrate  
16 of 24  
Assisted migration

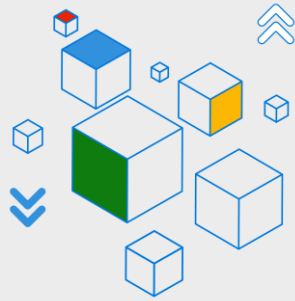
Migrated apps  
4 of 24  
Ready to configure

Name	Application identifier	Unique user count	Successful sign-ins	Failed sign-ins	Next Steps
AW Adventure Works	https://customer.demo.com/adventureworks	1	201	0	Ready
AW Amazon Web Services	urn:amazon:webservices	1	325	0	Additional steps required
BL Blackboard	https://customer.blackboard.com/mgmt	1	515	0	Ready
BO BOX	https://box.net	1	115	0	Ready
CL ClaimsXray	urn:microsoft:adfs:claimsxray	1	260	0	Additional steps required
CO Concur	https://concur.com	1	0	216	Ready
CO Contoso	https://customer.demo.com/contoso	1	141	0	Ready

aka.ms/425show/ADFSStoEntraID



# Support for hybrid Exchange Server deployments with Microsoft Entra Connect cloud sync



**Stage : GA**

**Product family :** Microsoft Entra ID

**Overview:** Ensures Active Directory user attributes are up to date for those on-premises users in disconnected forests who have their mailbox managed by Exchange Online.

### Basics

Enable password hash sync ... ☒

Exchange hybrid writeback ... ☒

### Notifications

One notification will be sent within 24 hours of quarantine.

Notification email

### Accidental deletions

Protect your configuration from accidental changes that can affect many users and groups and result in quarantine. Set the threshold for the number of objects that, if deleted, synchronization should stop and a notification will be sent to the email that is specified. This threshold should be between 1 and 250,000.

[Learn more](#)

Prevent accidental deletion ☒

Accidental deletion threshold

aka.ms/425show/ExchangeHybridWB



# Centralized view of Permissions Management risk recommendations as part of Microsoft Defender for Cloud



**Stage :** Public Preview

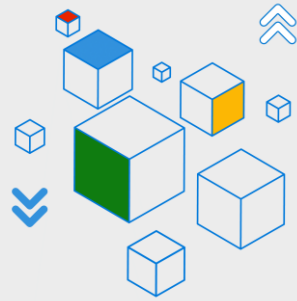
**Product family :** Microsoft Entra Permissions Management

**Overview:** Security admins can now get a centralized view of the unused or excessive access permissions within Microsoft Defender for Cloud. This capability enables teams to drive the least privilege access controls for cloud resources and receive actionable recommendations for resolving permissions risks across Microsoft Azure, AWS, and GCP – as part of Microsoft Defender Cloud Security Posture Management (CSPM).

Category	Capabilities	Defender for Cloud	Permissions Management
Discover	Permissions discovery for high-risk identities (including unused identities, overprovisioned active identities, unused super identities) in Azure, AWS, and GCP	✓	✓
	Permissions Creep Index (PCI) for multicloud environments (Azure, AWS, GCP) and all identities	✓	✓
	Permissions discovery for all identities, groups in Azure, AWS, and GCP	X	✓
	Permissions usage analytics, role/policy assignments in Azure, AWS, and GCP	X	✓
	Support for Identity Providers (including AWS IAM Identity Center, Okta, Google Workspace)	X	✓
Remediate	Automated deletion of permissions	X	✓
	Remediate identities by attaching/detaching the permissions	X	✓
	Custom role/AWS Policy generation based on activities of identities, groups, and users.	X	✓
	Permissions on demand (time-bound access) for human and workload identities via Microsoft Entra Admin Center, APIs, ServiceNow app.	X	✓
Monitor	Machine Learning-powered anomaly detections	X	✓
	Activity based, rule-based alerts	X	✓
	Context-rich forensic reports (for example, PCI history report, user entitlement and usage report)	X	✓

aka.ms/425show/MEPMDefenderForCloud

# Microsoft Entra Permissions Management: Permissions Analytics Report (PAR) PDF

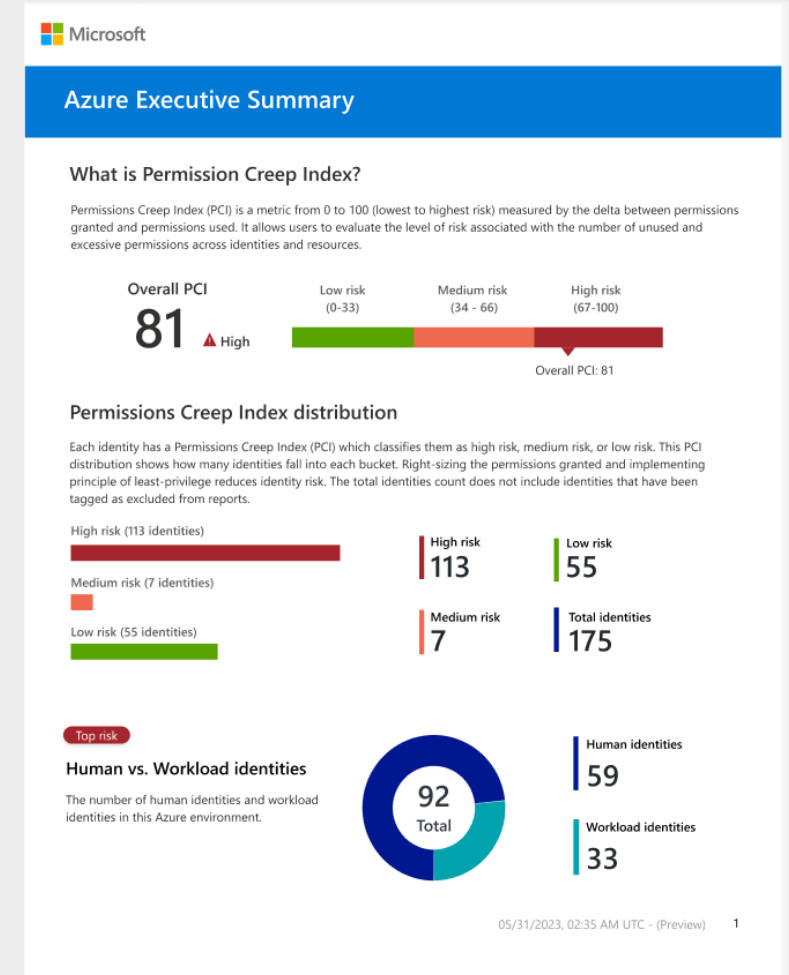
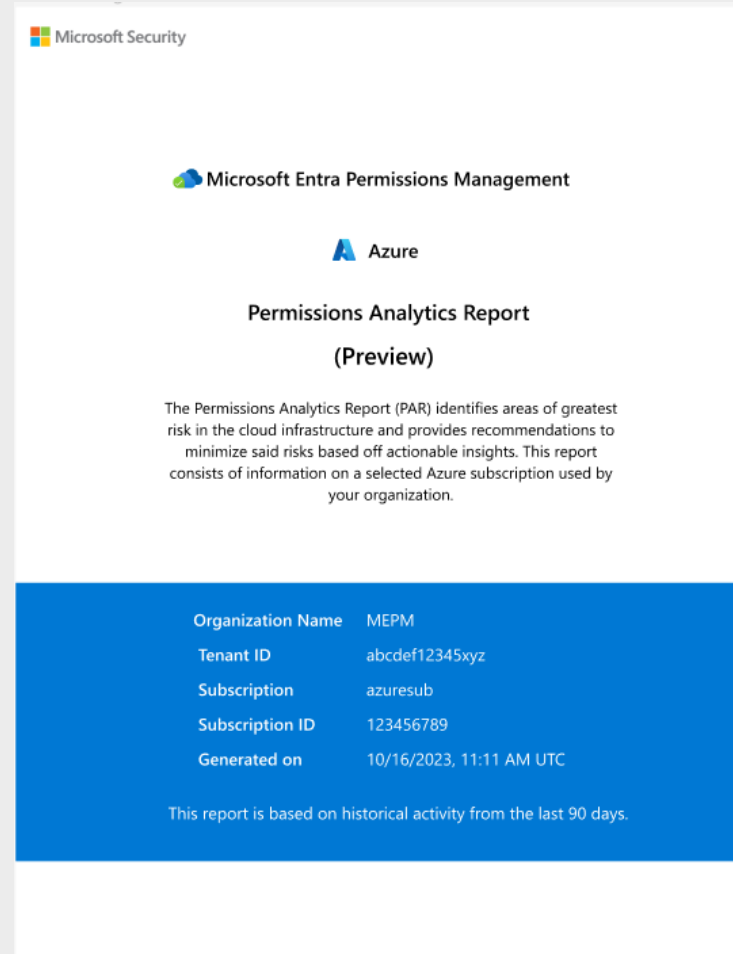


**Stage : GA**

**Product family :** Microsoft Entra Permissions Management

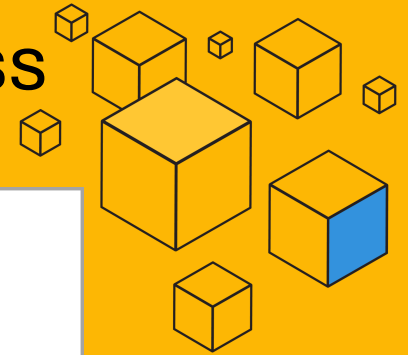
**Overview:** The PAR lists findings across identities and resources in Microsoft Entra Permissions Management and can be directly viewed in the UI, downloaded in an Excel format, and exported as a PDF. The report is available for all supported cloud environments: AWS, Microsoft Azure, and GCP, and can be downloaded for up to 10 authorization systems with one click.

[aka.ms/425show/MEPMPAR](https://aka.ms/425show/MEPMPAR)





# Microsoft Entra Private Access: Conditional Access and modern authentication methods



**Stage :** Public Preview

**Product family :** Microsoft Global Secure Access

**Overview:** Enables you to use Conditional Access controls and modern authentication methods, such as multifactor authentication (MFA), to secure access to all private applications and resources for remote and on-premises users.

Home > Enterprise applications > QuickAccess | Conditional Access >

## New

Conditional Access policy

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

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

Select what this policy applies to

Cloud apps

**Include** Exclude

☐ None

☐ All cloud apps


☒ Select apps

Edit filter (Preview)

None

Select

QuickAccess

 QuickAccess  
313ec331-3318-48a1-a9fe-96c4480861d1

**Target resources** ⓘ

1 app included

**Assignments**

**Users** ⓘ

0 users and groups selected

**Conditions** ⓘ

0 conditions selected

**Access controls**

**Grant** ⓘ

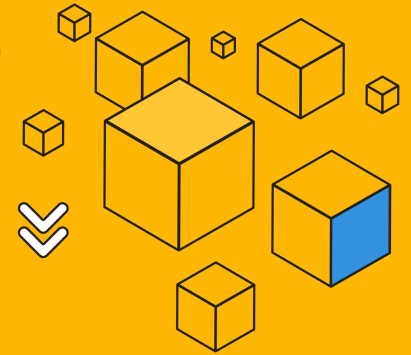
0 controls selected

**Session** ⓘ

0 controls selected



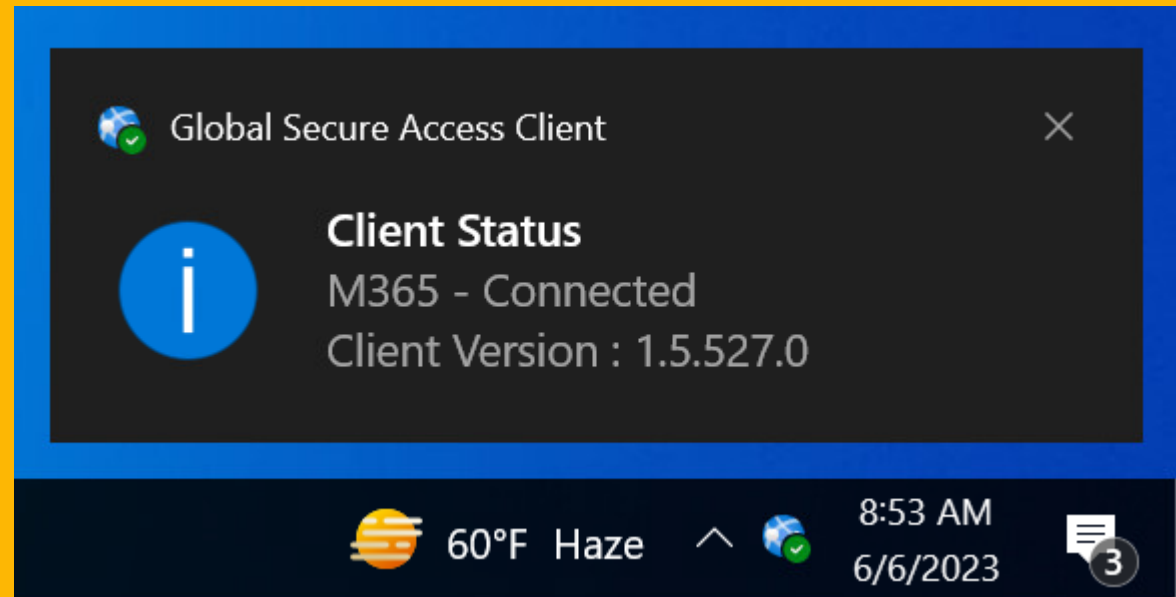
# Microsoft Security Service Edge: client support for Windows



**Stage :** Public Preview

**Product family :** Microsoft Entra Global Secure Access

**Overview:** For both Microsoft Entra Internet Access and Microsoft Entra Private Access, we now support a client for Windows.



[aka.ms/425show/MicrosoftEntraSSE](https://aka.ms/425show/MicrosoftEntraSSE)




# Update: Microsoft Security Service Edge: increase of points of presence coverage –



**Stage :** Public Preview

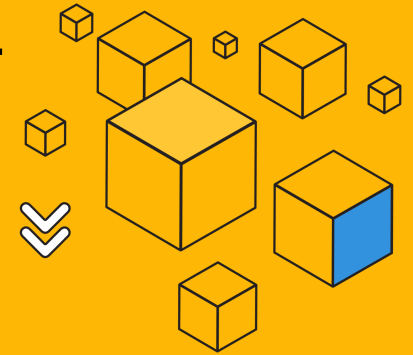
**Product family :** Microsoft Global Secure Access

**Overview:** Microsoft Security Service Edge is now available globally (except in China and Russia) with more points of presence added in the future.

Microsoft Entra Internet Access and Microsoft Entra Private Access			
 Expand table			
Europe Middle East Africa (EMEA)	Asia Pacific (APAC)	Latin America (LATAM)	North America (NA)
Amsterdam, Netherlands	Busan, South Korea	Rio de Janeiro, Brazil	Boydton, Virginia, USA
Berlin, Germany	Chennai, India		Cheyenne, Wyoming, USA
Cape Town, South Africa	Melbourne, Australia		Chicago, Illinois, USA
Dubai, UAE	Osaka, Japan		Des Moines, Iowa, USA
Dublin, Ireland	Pune, India		Manassas, Virginia, USA
Frankfurt, Germany	Seoul, South Korea		Montreal, Quebec, Canada
Gavle, Sweden	Singapore, Singapore		Phoenix, Arizona, USA
Johannesburg, South Africa	Sydney, Australia		Queretaro, Mexico
London, UK	Taipei, Taiwan		Quincy, Washington, USA
Milan, Italy	Tokyo, Japan		San Antonio, Texas, USA
Paris, France			San Jose, California, USA
Tel Aviv, Israel			Toronto, Ontario, Canada
Warsaw, Poland			
Zurich, Switzerland			

aka.ms/425show/MicrosoftEntraSSE

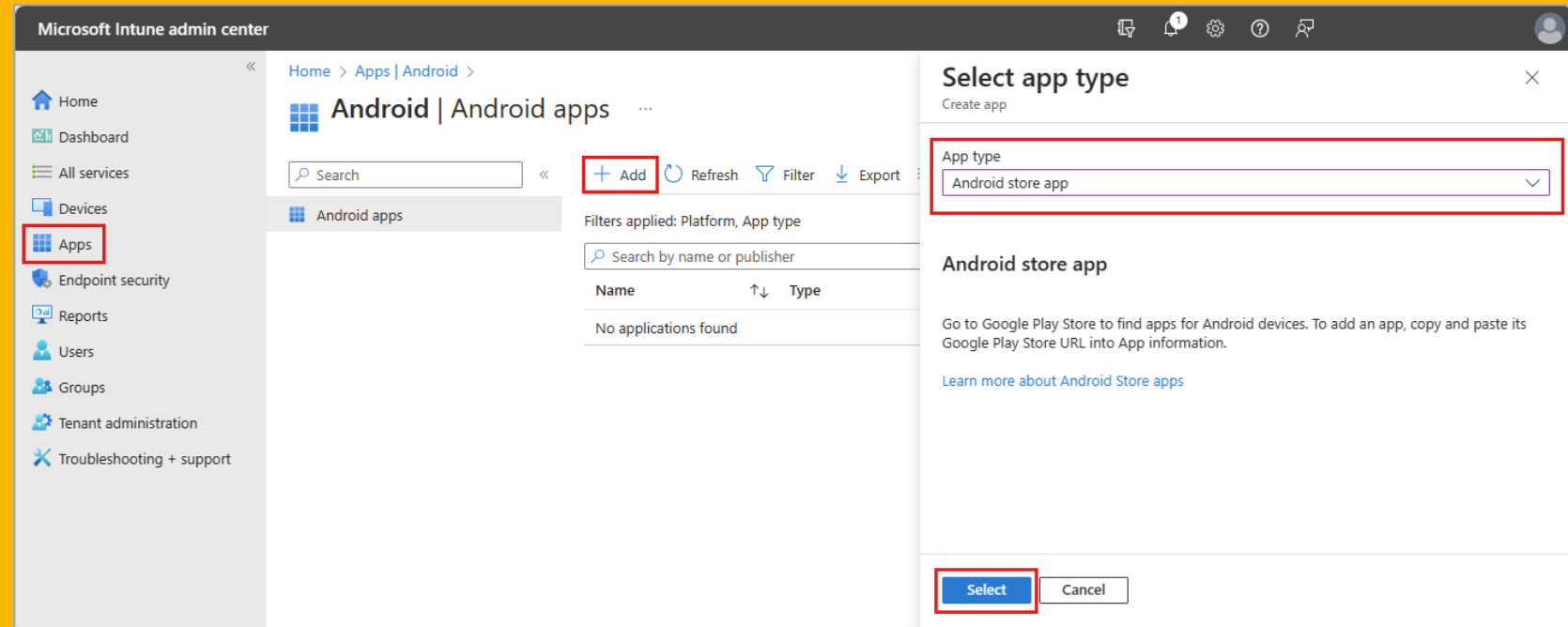
# Microsoft Security Service Edge: client support for Android



**Stage :** Public Preview

**Product family :**  
Microsoft Global Secure  
Access

**Overview:** For both  
Microsoft Entra Internet  
Access and Microsoft  
Entra Private Access, we  
now add a client  
supporting Android.

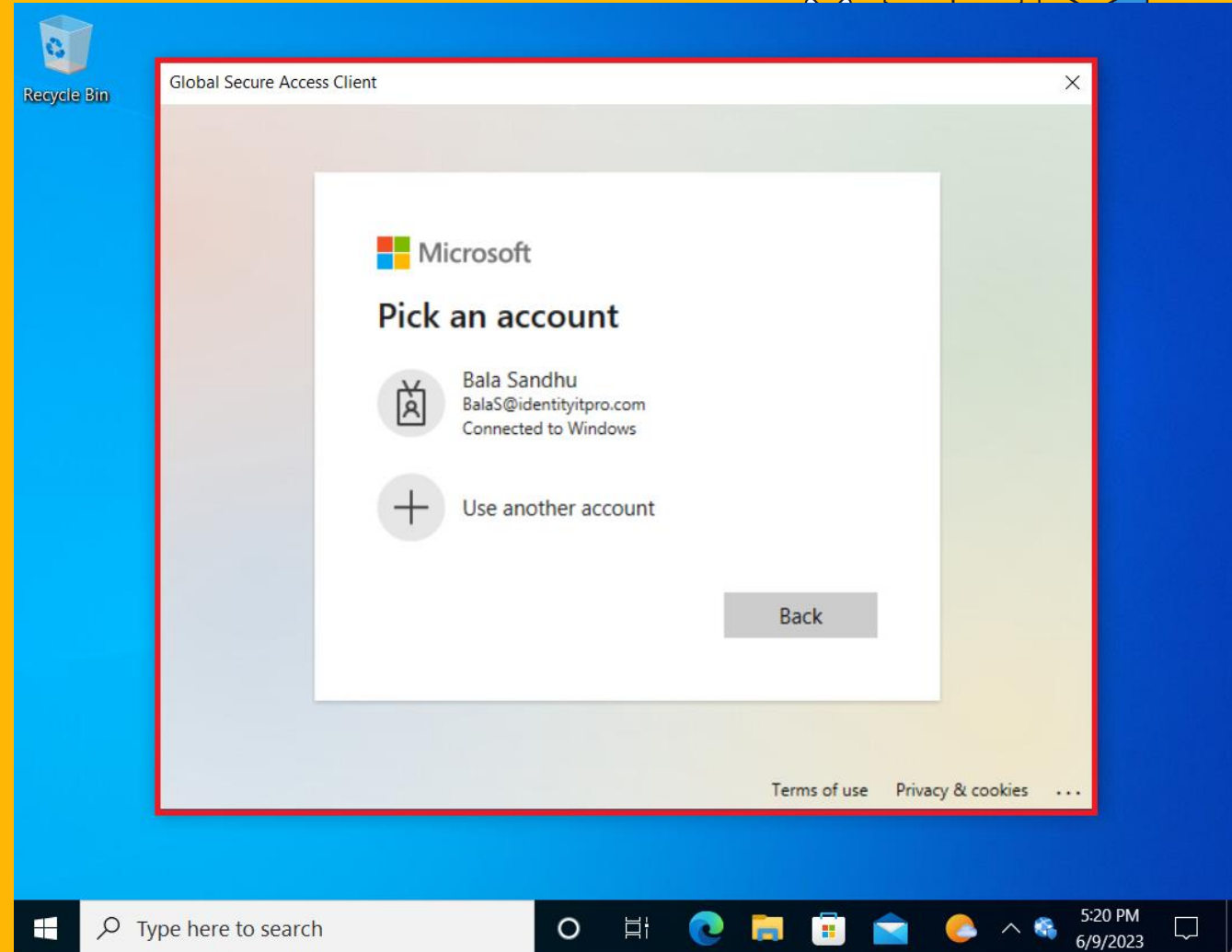


# Microsoft Entra Internet Access: Universal Conditional Access

**Stage :** Public Preview

**Product family :** Microsoft Global Secure Access

**Overview:** Extends adaptive access controls to any network destination, such as an external website or a non-federated SaaS application.

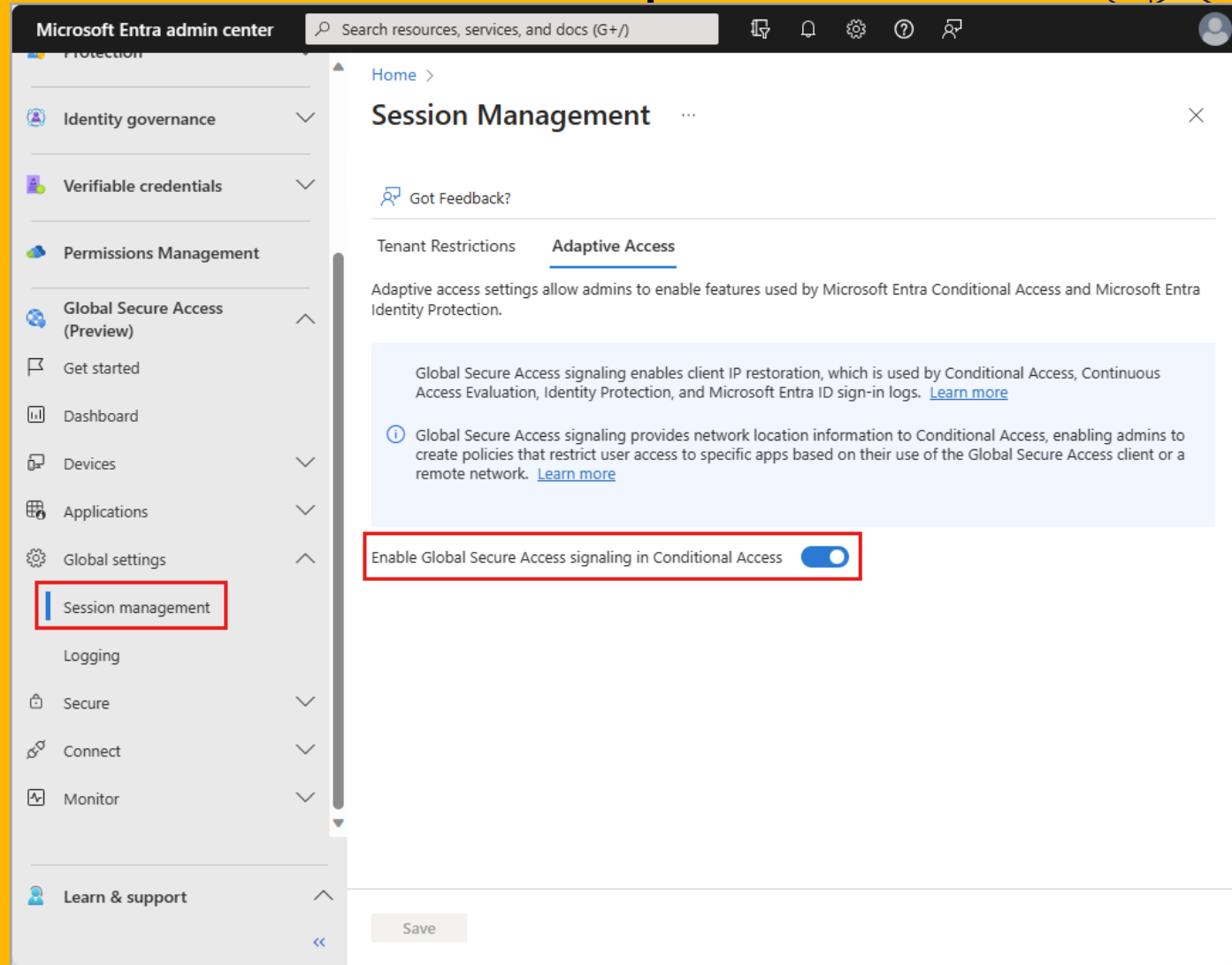


# Microsoft Entra Internet Access: compliant network check

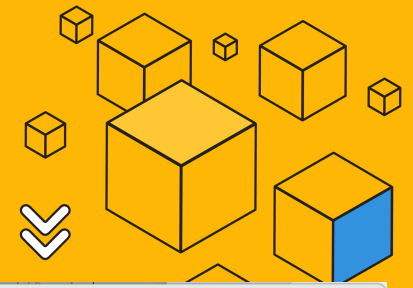
**Stage :** Public Preview

**Product family :** Microsoft Global Secure Access

**Overview:** Compliant Network Check, an easy-to-manage construct within Conditional Access, allows you to protect Microsoft Entra integrated cloud applications against token theft and ensures users do not bypass network security policies specific to their tenant while accessing critical cloud services.



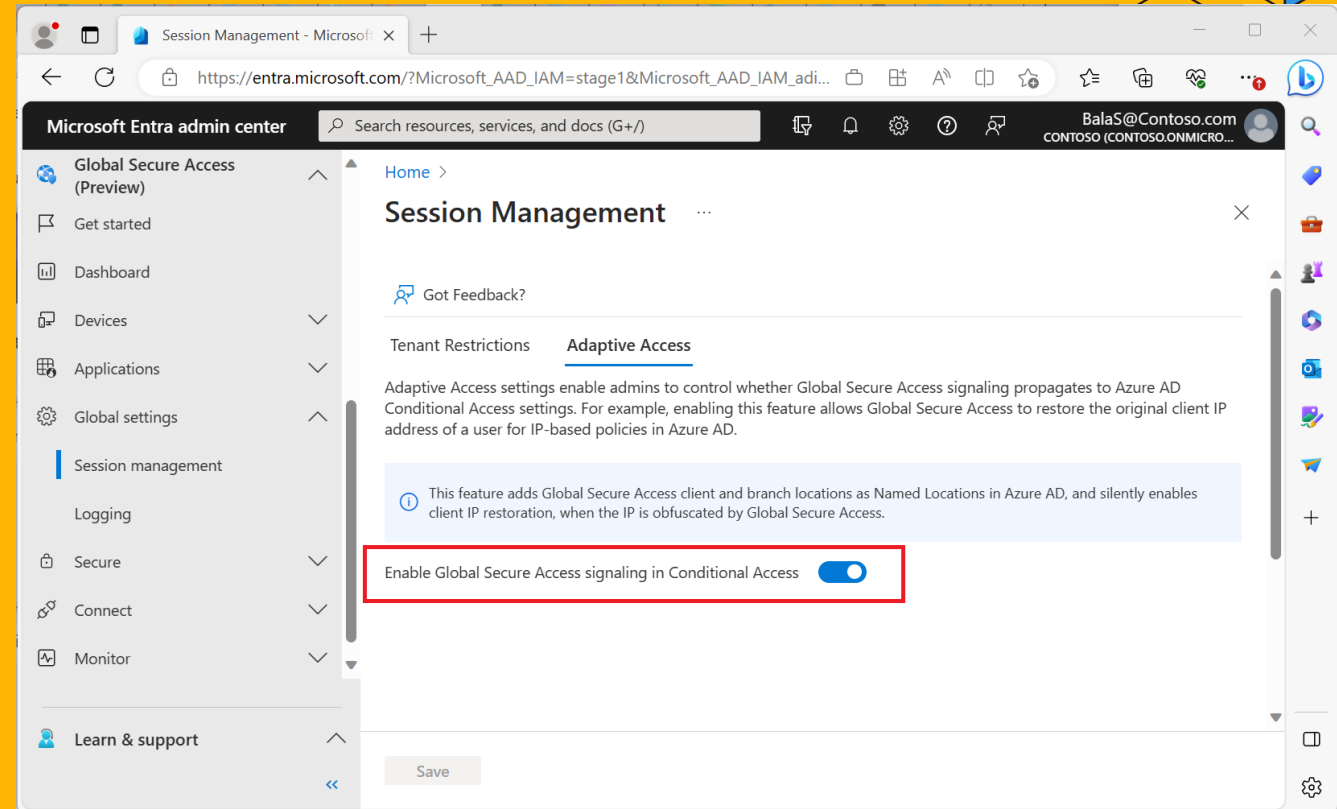
# Microsoft Entra Internet Access: Source IP restoration



**Stage :** Public Preview

**Product family :** Microsoft Global Secure Access

**Overview:** Compliant Network Check, an easy-to-manage construct within Conditional Access, allows you to protect Microsoft Entra integrated cloud applications against token theft and ensures users do not bypass network security policies specific to their tenant while accessing critical cloud services.





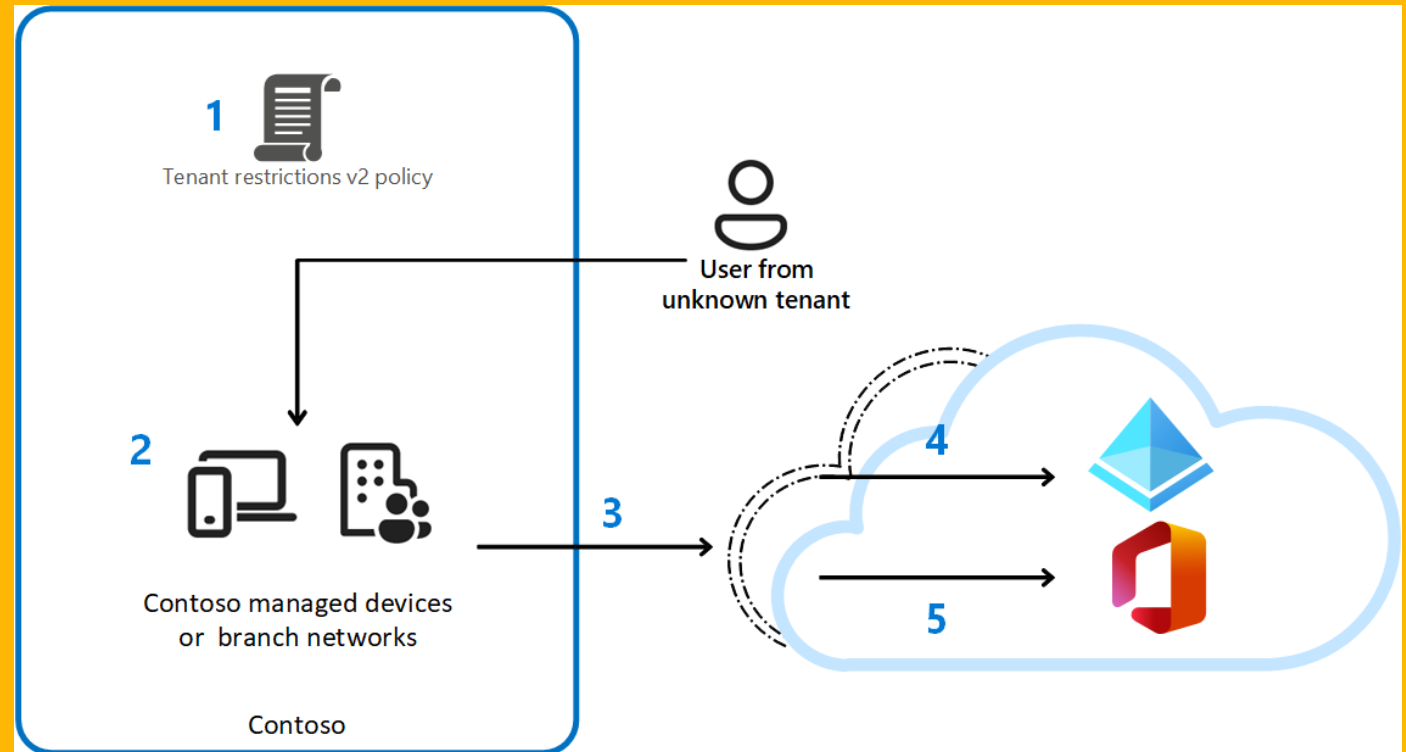
# Microsoft Entra Internet Access: Universal tenant restrictions



**Stage :** Public Preview

**Product family :** Microsoft Global Secure Access

**Overview:** Enhance the functionality of tenant restriction v2 using Global Secure Access to tag all traffic no matter the operating system, browser, or device form factor. It allows support for both client and remote network connectivity. Administrators no longer have to manage proxy server configurations or complex network configurations



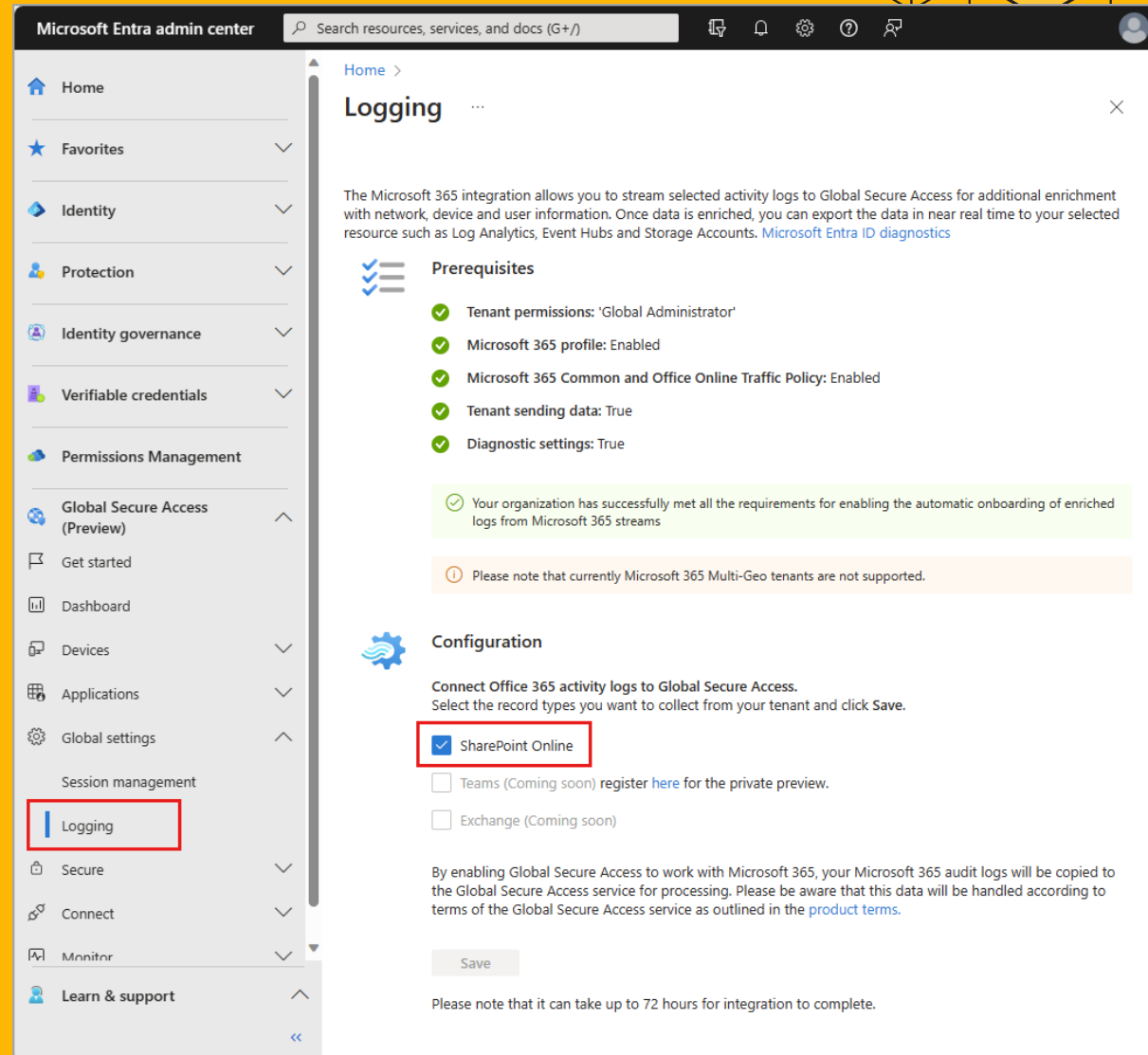
[aka.ms/425show/MicrosoftEntraSSE](https://aka.ms/425show/MicrosoftEntraSSE)

# Microsoft Entra Internet Access: enriched Microsoft 365 logs

**Stage :** Public Preview

**Product family :** Microsoft Global Secure Access

**Overview:** Gain insights into the performance, experience, and availability of the Microsoft 365 apps your organization uses





# Microsoft Entra Internet Access: remote network health logs



**Stage :** Public Preview

**Product family :**  
Microsoft Global Secure Access

**Overview:** Provides visibility into the health of the IPSec tunnel and the Border Gateway Protocol route advertisement. This long-running tunnel and routing information are the keys to your remote network health

Microsoft Entra admin center									
Search resources, services, and docs (G+/)									
Home >									
Remote network health logs									
Download Refresh Columns Got feedback?									
Timespan : Last 24 hours Add filter									
Created date time ↓	Source IP	Destination IP	Status	Description	BGP routes ad...	Sent bytes	Received bytes	Remote network ID	
10/11/2023, 03:41 PM	10.0.0.0	192.0.2.0	Alive	N/A	89	27.19 KB	1.87 KB	c6941c04-36b4-3655	
10/11/2023, 03:41 PM	172.16.0.0	203.0.113.0	Alive	N/A	89	2.15 KB	1.64 KB	48867b0d-2b0b-c470	
10/11/2023, 03:26 PM	10.0.0.0	192.0.2.0	Tunnel connect...	ConnectReason...	0	23.27 KB	1.97 KB	c6941c04-36b4-3655	
10/11/2023, 03:26 PM	172.16.0.0	203.0.113.0	Alive	N/A	89	7.43 KB	11.95 KB	48867b0d-2b0b-c470	



425Show

# Microsoft Entra Internet Access for all apps



**Stage :** Public Preview

**Product family :** Microsoft  
Global Secure Access

**Overview:** Provides an identity-centric Secure Web Gateway (SWG) solution for Software as a Service (SaaS) applications and other Internet traffic. It protects users, devices, and data from the Internet's wide threat landscape with best-in-class security controls and visibility through Traffic Logs.

```
"Security Profile for Angie"    <---- the security profile
    Allow msn.com at priority 100 <---- higher priority filtering policies
    Block News at priority 200  <---- lower priority filtering policy
```

[aka.ms/425show/MicrosoftEntraSSE](https://aka.ms/425show/MicrosoftEntraSSE)

Thank you for  
tuning in!

Don't forget to  
tune in again for  
the October  
updates in  
November!



**425**Show



Grace Picking



Jorge Lopez