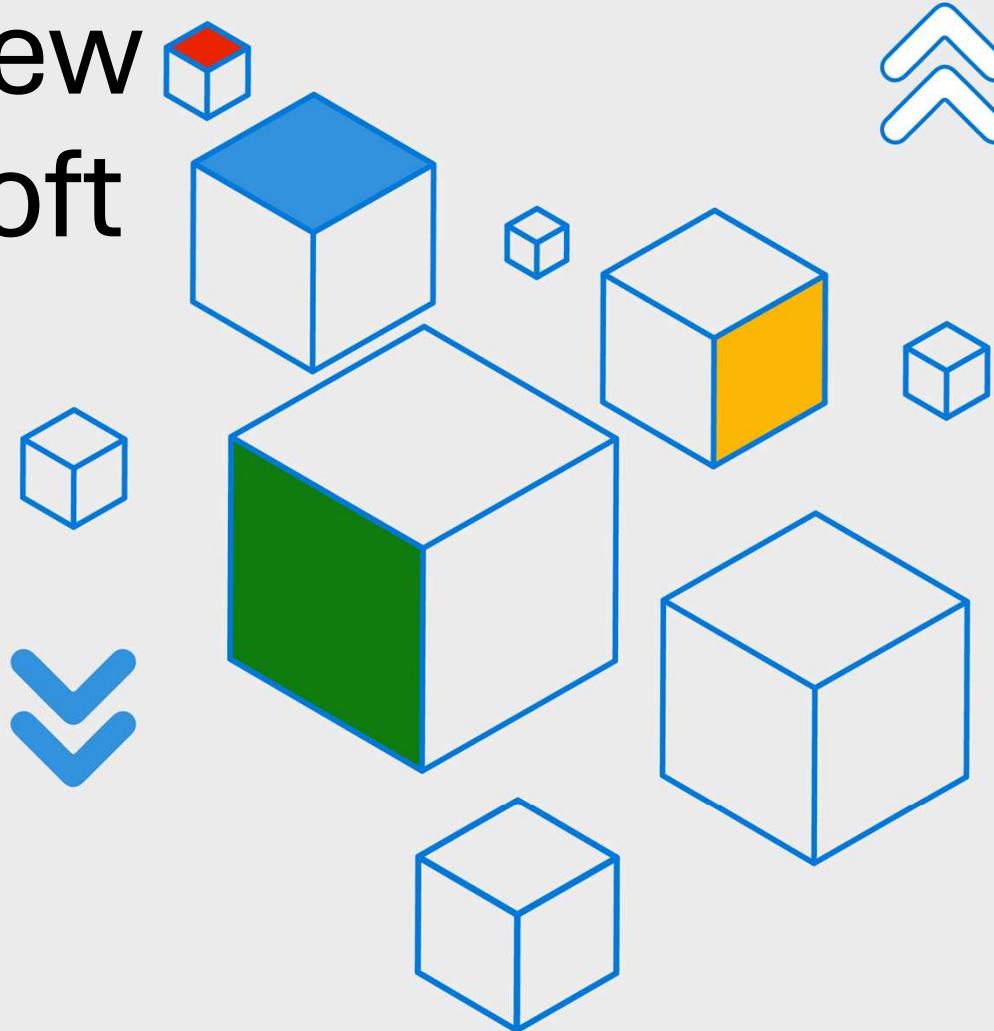


# What's New in Microsoft Entra ID

## August 2023



425Show



Grace Picking

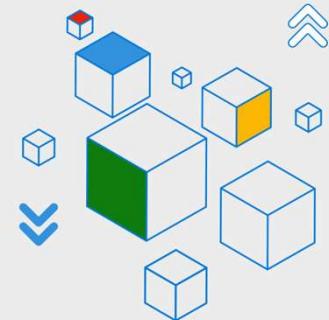


Jorge Lopez



425Show

# Azure AD is being renamed to Microsoft Entra ID



**Overview :** We are excited to inform you that Azure AD, which has been part of the Microsoft Entra product family since 2022, is becoming Microsoft Entra ID!

- **Microsoft Entra ID** (formerly Azure AD)
- **Microsoft Entra ID Protection**
- (formerly Identity Protection)
- **Microsoft Entra ID Governance**  
(formerly Identity Governance)
- **Microsoft Entra Workload ID**  
(formerly Workload Identities)
- **Microsoft Entra External ID** (formerly External Identities. Special note: Azure AD B2C will remain as is.)





425Show

# Microsoft Entra ID Governance

The following governance features went GA and are part of the Microsoft Entra ID Governance SKU

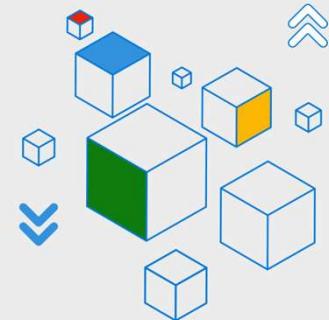


<a href="#">Identity Governance dashboard</a>	Discovers usage information about various Identity Governance & Administration (IGA) features configured in your tenant. It then gives you an at-a-glance view of your current state of Identity Governance, with actionable buttons and quickly accessible links to documentation.
<a href="#">Lifecycle workflows (LCW)</a>	Enables you to use custom workflows to automate identity lifecycle management tasks for your Microsoft Entra ID users by managing your joiner, mover, and leaver lifecycle processes. With LCW, you can leverage Microsoft Entra ID to confidently deploy workflows to configure out-of-the-box actions to onboard and offboard your employees.
<a href="#">Access reviews for inactive users</a>	Allows admins to review and address stale accounts that haven't been active for a specified period. Admins can set a specific duration to determine inactive accounts which were not used for either interactive or non-interactive sign-in activities. As part of the review process, stale accounts can automatically be removed.
<a href="#">Access reviews: Machine Learning (ML) based recommendation on User-to-Group Affiliation</a>	Provides ML-based recommendations to the reviewers of an access review, making the review experience easier and more accurate. This recommendation leverages a scoring mechanism and compares users' relative affiliation with other users in the group, based on the organization's reporting structure. Users who are very distant from other users in the group have low affiliation and our system then provides a Deny recommendation.
<a href="#">Entitlement management custom extensions to Logic Apps</a>	Extends the access lifecycle with specific processes and business logic when access is requested or about to expire. You can create tickets for manual access provisioning in disconnected systems, send custom notifications, automate additional access-related configuration in your business apps, or integrate complex governance, risk, and compliance (GRC) checks for more advanced scenarios.
<a href="#">Require Microsoft Entra Verified ID from specific issuer for entitlement management</a>	As an access package manager, you can require that requestors present a verified ID containing credentials from a trusted issuer. Approvers can then quickly view if a user's verifiable credentials were valid at the time that the user presented their credentials and submitted the access package request.
<a href="#">Assigning access automatically with no requests required</a>	Enables you to automate processes for access lifecycle management by assigning access to users based on their attributes coming from your HR system or other systems, without the need of access requests or administrative interaction.



425Show

# Identity Governance dashboard



**Stage : GA Product family :**  
Microsoft Entra ID Governance

**Overview :** Discovers usage information about various Identity Governance & Administration (IGA) features configured in your tenant. It then gives you an at-a-glance view of your current state of Identity Governance, with actionable buttons and quickly accessible links to documentation.

The screenshot shows the Microsoft Azure Identity Governance dashboard. On the left is a navigation sidebar with sections like Dashboard, Getting started, Entitlement management, Lifecycle workflows, Access reviews, Privileged Identity Management, Terms of use, Activity, and Audit logs. The main area has several cards:

- Welcome to Identity Governance**: Manage identity and access rights across multiple applications and services to meet security and regulatory compliance requirements. With Microsoft Entra ID Governance, balance security and productivity by ensuring that the right people have the right access to the right resources for the right amount of time. [Learn more](#)
- Member user lifecycle governance**: 129 member user accounts recently created. Improve operational efficiency, increase new hire productivity and reduce security risks by automating your employee onboarding and offboarding tasks. [Configure lifecycle workflows](#) | [Learn more](#)
- Application access governance**: 254 apps with direct user assignments. Manage how your employees and guests get access to business applications and maintain compliance by configuring request approval workflows and periodic access reviews and automatically revoke access when it is no longer necessary. [Create access package](#) | [Learn more](#)
- Guest access governance**: 5 guest user accounts recently created. Reduce security risk by monitoring inactive guest users at scale with intelligent insights, configure thresholds based on your compliance needs and perform periodic review of guest access to groups and business applications. [View inactive guests](#) | [Learn more](#)
- Privileged access governance**: 25 permanent global administrator assignments. Microsoft recommends you to keep fewer than 5 standing global admins with 2 of them reserved for break glass scenarios.
- Identity Governance status**: Your identity landscape (Member users: 1,262), Microsoft Entra ID Governance, and Your ID Governance configurations (Lifecycle workflows configured: 11, Access reviews configured: 201).



425Show

# Lifecycle workflows (LCW)

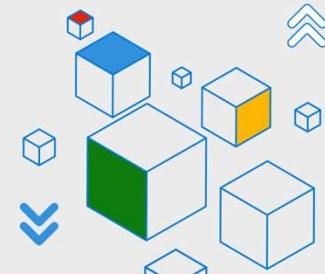
**Stage : GA Product**  
**family : Microsoft Entra**  
**ID Governance**

**Overview :** Enables you to use custom workflows to automate identity lifecycle management tasks for your Microsoft Entra ID users by managing your joiner, mover, and leaver lifecycle processes.  
With LCW, you can leverage Microsoft Entra ID to confidently deploy workflows to configure out-of-the-box actions to onboard and offboard your employees.

The screenshot shows the Microsoft Azure Identity Governance dashboard. On the left, a sidebar menu includes options like Dashboard, Getting started, Entitlement management, Access packages, Catalogs, Connected organizations, Reports, Settings, Lifecycle workflows (which is selected), Access reviews, Overview, Access reviews, Programs, Settings, Review History, Privileged Identity Management, Azure AD roles, Azure resources, Terms of use, Terms of use, Activity, and Audit logs. The main content area features several cards:

- Member user lifecycle governance:** Shows 131 member user accounts recently created. It includes a call-to-action button "Configure lifecycle workflows".
- Application access governance:** Shows 254 apps with direct user assignments. It includes a call-to-action button "Create access package".
- Guest access governance:** Shows 5 guest user accounts recently created. It includes a call-to-action button "View inactive guests".
- Privileged access governance:** Shows 25 permanent global administrator assignments. It includes a note from Microsoft about keeping global admins below 5.
- Identity Governance status:** Displays "Your Identity landscape" with 1,264 member users, "Microsoft Entra ID Governance", and "Your ID Governance configurations" showing 11 lifecycle workflows configured and 301 access reviews configured.

<https://aka.ms/425show/EntraIDG/Overview>





425Show

**Stage : GA Product**  
**family : Microsoft Entra**  
**ID Governance**

**Overview :** Allows admins to review and address stale accounts that haven't been active for a specified period. Admins can set a specific duration to determine inactive accounts which were not used for either interactive or non-interactive sign-in activities. As part of the review process, stale accounts can automatically be removed.

Home > Identity Governance | Access reviews >

## New access review ...

\*Review type \*Reviews Settings \*Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles. [Learn more](#)

Select what to review \* Teams + Groups

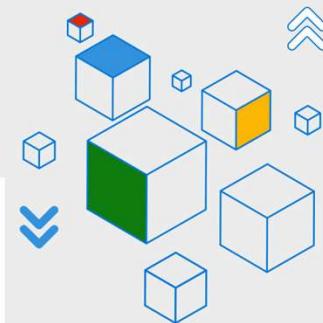
Review scope \*  All Microsoft 365 groups with guest users ⓘ  Select Teams + groups

Group \* Audit Team

Scope \*  Guest users only  All users ⓘ

**In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.**

Inactive users (on tenant level) only ⓘ Days inactive 30 ✓

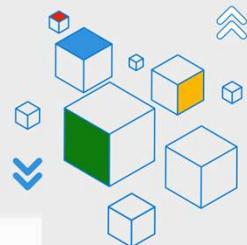


<https://aka.ms/425show/EntraIDG/Overview>



425Show

# Access reviews: Machine Learning (ML) based recommendation on User-to-Group Affiliation



**Stage : GA Product family :**  
Microsoft Entra ID Governance

**Overview** Provides ML-based recommendations to the reviewers of an access review, making the review experience easier and more accurate. This recommendation leverages a scoring mechanism and compares users' relative affiliation with other users in the group, based on the organization's reporting structure. Users who are very distant from other users in the group have low affiliation and our system then provides a Deny recommendation.

My Access ▾

Search users

← Access reviews

## User-to-Group Affiliation

Please review assignment to 'poltest1\_g01' [See details](#)

	Approve	Deny	Don't know	Reset decisions	Accept recommendations
<input type="radio"/> Name ↑					
<input type="radio"/> Sam Centrell sam.centrell@contoso.com					Approve
<input type="radio"/> Jessie Irwin jessie.irwin@contoso.com					Deny <small>Inactive user</small>
<input type="radio"/> Anthony Ivanov anthony.ivanov@contoso.com					Deny <small>Inactive user</small>
<input checked="" type="radio"/> Caleb Foster caleb.foster@contoso.com					Deny <small>Low Affiliation</small> <small>Inactive user</small>
<input type="radio"/> Olivia Wilson olivia.wilson@contoso.com					Deny <small>Low Affiliation</small> <small>Inactive user</small>

<https://aka.ms/425show/EntraIDG/Overview>



425Show

# Entitlement management custom extensions to Logic Apps

**Stage : GA Product family :**  
Microsoft Entra ID  
Governance

**Overview :** Extends the access lifecycle with specific processes and business logic when access is requested or about to expire. You can create tickets for manual access provisioning in disconnected systems, send custom notifications, automate additional access-related configuration in your business apps, or integrate complex governance, risk, and compliance (GRC) checks for more advanced scenarios.

Create a custom extension

Basics Extension Type Extension Configuration Details Review + create

Custom extensions are created to be paired to specific policy types within the access package governance workflow.

Select to which type of workflow you will be pairing this custom extension:

Request workflow (triggered when an access package is request, approved, granted or removed)

Pre-Expiration workflow (triggered when an access package assignment has 14 days till expiry or 1 day till expiry)

| Logic app designer ...

Save Discard Run Trigger Designer Code view Parameters Templates Connectors Help Info

100%

Condition

And

CatalogId is equal to fd1d07e2-a89f-4ecc-a128-59b877cfb110

True

Add an action

False

Add an action

<https://aka.ms/425show/EntraIDG/Overview>



425Show

# Require Microsoft Entra Verified ID from specific issuer for entitlement management

**Stage : GA Product**

**family : Microsoft Entra  
ID Governance**

**Overview :** As an access package manager, you can require that requestors present a verified ID containing credentials from a trusted issuer. Approvers can then quickly view if a user's verifiable credentials were valid at the time that the user presented their credentials and submitted the access package request.

The screenshot shows the Microsoft Entra ID Governance interface. On the left, there's a navigation bar with 'Access packages', 'Request history', 'Approvals', and 'Access reviews'. The main area is titled 'Access packages' with a sub-section 'product manager'. It lists one active access package: 'product manager resources', which is described as 'resources for new product managers' and associated with 'Salesforce, Project V'. To the right, a modal window titled 'product manager resources' displays a QR code with a red border. The text next to the QR code says 'This request is valid for 5 minutes and will automatically be refreshed. Refresh manually' and 'Can't scan image? Download Microsoft Authenticator on your phone'. At the bottom of the modal are 'Next' and 'Cancel' buttons.

<https://aka.ms/425show/EntraIDG/Overview>



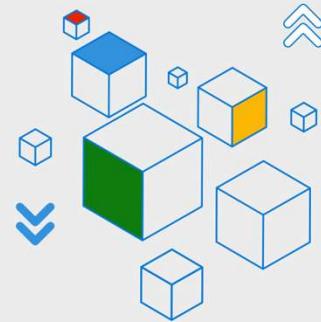
425Show

# Assigning access automatically with no requests required

**Stage : GA Product**

**family : Microsoft Entra  
ID Governance**

**Overview :** Enables you to automate processes for access lifecycle management by assigning access to users based on their attributes coming from your HR system or other systems, without the need of access requests or administrative interaction.



Home > Identity Governance | Access packages > Sales Team | Policies > Create a policy >

## Dynamic membership rules

Save Discard Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ① Learn more

And/Or	Property	Operator	Value
	department	Equals	Sales

+ Add expression + Get custom extension properties ①

Rule syntax Edit

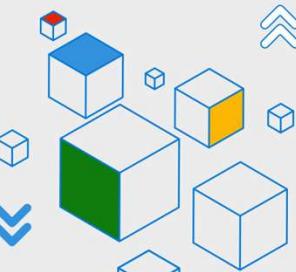
```
(user.department -eq "Sales")
```

<https://aka.ms/425show/EntraIDG/Overview>



425Show

# Enhanced company branding for sign-in experiences



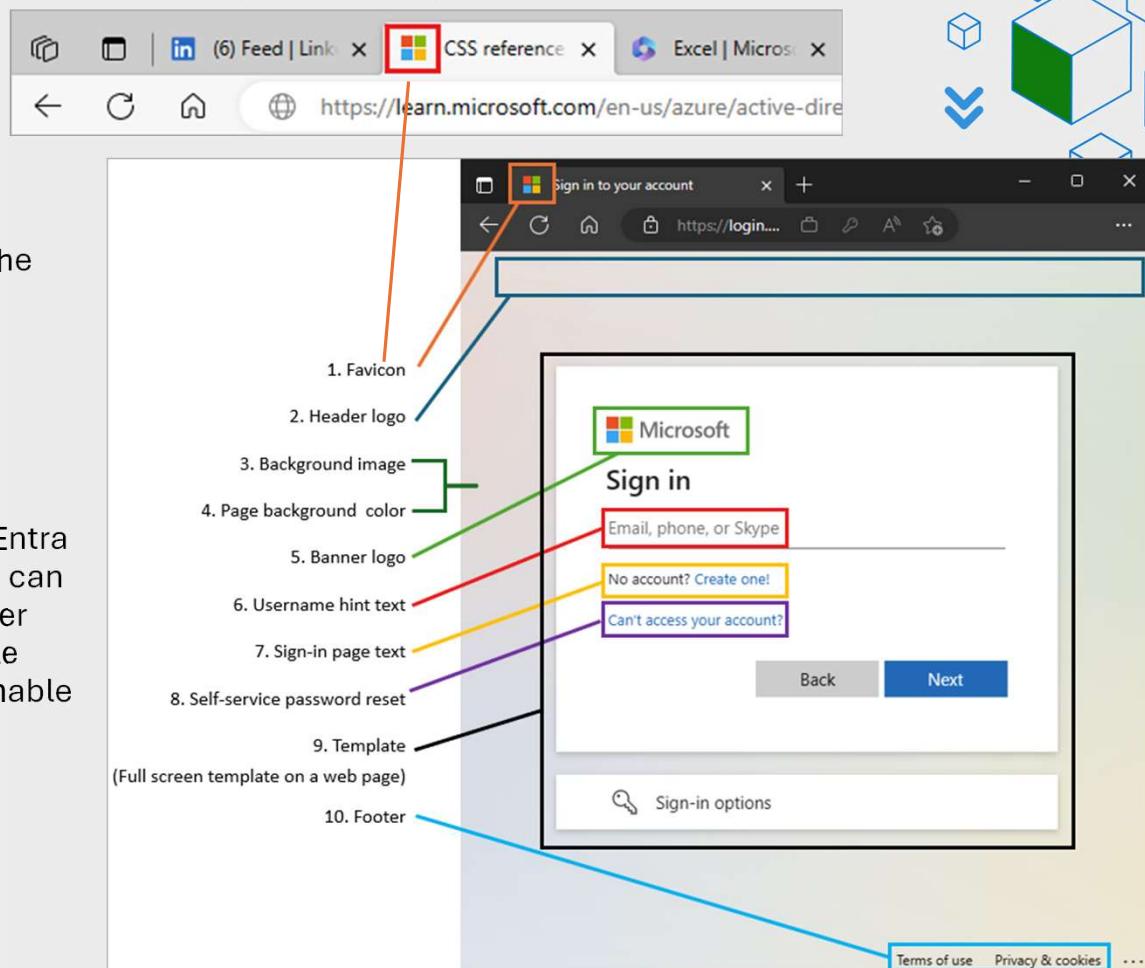
Stage : GA

Product family : Microsoft Entra ID

License : Adding custom branding requires one of the following licenses:

- Azure AD Premium 1
- Azure AD Premium 2
- Office 365 (for Office apps)

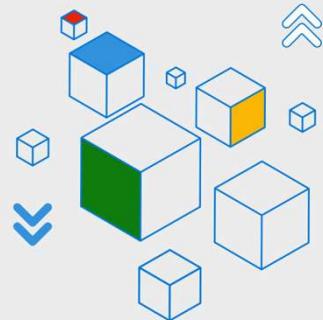
Create a custom look and feel for users' Microsoft Entra ID and Microsoft 365 sign-in experiences. Now, you can customize self-service password reset (SSPR), footer hyperlinks, and the browser icon. Also, you can style sign-in experiences by applying custom CSS and enable a header and footer by using one of the pre-defined templates.





425 Show

# Authentication methods reporting API



## Stage : GA

## **Product family : Microsoft Entra ID**

## /Internet Access /Private Access

**License : An Azure AD Premium P1 or P2 license is required to access usage and insights.**

# Azure AD Multi-Factor Authentication and self-service password reset (SSPR)

**Overview :** The new authentication methods activity dashboard enables admins to monitor authentication method registration and usage across their organization. This reporting capability provides your organization with the means to understand what methods are being registered and how they're being used.

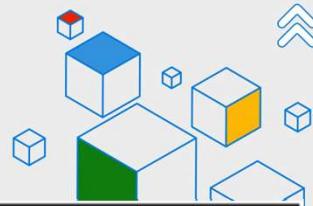
HTTP/1.1 200 OK  
Content-Type: application/json

```
{  
    "@odata.context":  
    "https://graph.microsoft.com/v1.0/$metadata#reports/authenticationMethods/userRegistratio  
ns",  
    "value": [  
        {  
            "id": "86462606-fde0-4fc4-9e0c-a20eb73e54c6",  
            "userPrincipalName": "AlexW@Contoso.com",  
            "userDisplayName": "Alex Wilber",  
            "isAdmin": false,  
            "isSsprRegistered": false,  
            "isSsprEnabled": false,  
            "isSsprCapable": false,  
            "isMfaRegistered": true,  
            "isMfaEnabled": false  
        }  
    ]  
}
```



425Show

# FIDO2 support on iOS and macOS browsers



The screenshots illustrate the Microsoft sign-in flow on mobile devices:

- Sign-in Step:** The user enters their email or phone number. A red box highlights the "Sign-in options" link at the bottom left.
- Sign-in Options Step:** The "Sign in with a security key" option is highlighted with a red box. It instructs the user to choose this only if they have enabled a security key for their account.
- Sign-in with a Security Key Step:** The user is prompted to open a security window on their device to follow instructions for signing in.
- Sign In Step (iPhone):** The user selects "Security key" as the method to sign in to [login.microsoftonline.com](https://login.microsoftonline.com). The "Security key" option is checked with a blue checkmark.
- Use Security Key Step (iPhone):** Instructions are provided to insert and activate the security key. It notes that if an NFC key is available, it should be brought near the top of the iPhone screen.



425Show

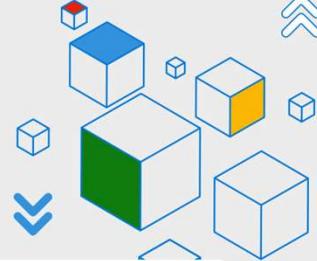
Stage : GA

# Entitlement management support in Conditional Access (CA)

**Product family :** Microsoft Entra ID Governance

**License :** Microsoft Entra ID Governance, You can set up a trial of Microsoft Entra ID Governance at <https://aka.ms/EntraIDGovTrial>.

**Overview :** Enables you to include or exclude entitlement management in CA policies, better setting up your organization for self-service onboarding and CA policy exception management scenarios. The Entitlement Management service is now targetable in the conditional access policy for inclusion or exclusion of applications. By enabling the inclusion or exclusion of Entitlement Management and/or My Access in conditional access policies, your organization is better set up for self-service onboarding and conditional access policy exception management scenarios.



Home > Conditional Access | Overview >

## New

Conditional Access policy

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

Name \*  ✓

Assignments

Users or workload identities [\(1\)](#)  
0 users or workload identities selected

Target resources [\(1\)](#)  
1 app included

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

Select what this policy applies to  ▼

Include  Exclude

None  
 All cloud apps  
 Select apps

Edit filter (Preview)  
None

Select  
 Azure AD Identity Governance - Entitlement Management



425Show

# Recommendation to migrate ADAL apps to MSAL



Stage : GA

Product family : Microsoft Entra ID

**Overview :** With Azure Active Directory Authentication Library (ADAL) having been retired on June 30th, this recommendation helps you identify apps using the legacy ADAL via the Azure portal, Microsoft Graph API and PowerShell.

## Deployment Steps:

The first step to migrating your apps from ADAL to MSAL is to identify all applications in your tenant that are currently using ADAL. You can identify your apps in the Azure portal or programmatically.

### Migrate your applications that use the ADAL Library to the MSAL Library

Mark as | Got feedback?

Status Active	Priority Medium	Impacted resource type Applications
------------------	--------------------	--

**Status description**  
Marked as active by system on 7/23/2023 at 1 AM GMT+1.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Woodgrove | Overview >

### Migrate your applications that use the ADAL Library to the MSAL Library

Mark as | Got feedback?

Status Active	Priority Medium	Impacted resource type Applications
------------------	--------------------	--

**Status description**  
Marked as active by system on 7/23/2023 at 1 AM GMT+1.

**Description**  
Your tenant has 1 applications that use the Azure Active Directory Library (ADAL). ADAL support ends on June 30, 2023. Existing apps using ADAL will continue to work after the end-of-support date, but Microsoft will no longer release security fixes for ADAL putting these apps at risk.

**Action plan**

1. Open PowerShell as an administrator
2. Connect to Microsoft Graph by running command "Connect-MgGraph -Tenant <YOUR\_TENANT\_ID>"
3. Select your profile by running the command "Select-MgProfile beta"
4. Get a list of your recommendations by running the command "Get-MgDirectoryRecommendation | Format-List"
5. Migrate your ADAL applications to MSAL by following the steps outlined [here](#).

**Impacted resources**

Resource	ID	First detected
Portal View	e924cd3e-3db4-4b8a-a623-285738a...	Jul 23, 2023, 4:07 AM

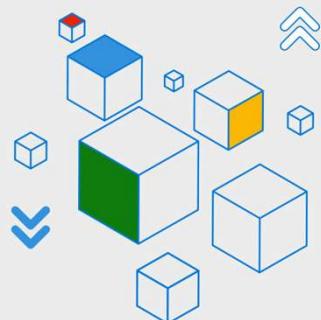


425Show

Stage : GA

Product family : Microsoft Entra ID

**Overview :** Enables you to revoke an application's permissions that have been granted for the entire organization through admin consent.



# Revoke previously granted tenant-wide permissions

Dashboard > Enterprise applications - All applications

**Graph Explorer - Permissions** Enterprise Application

Overview Getting started

Manage

- Properties
- Owners
- Users and groups
- Provisioning
- Self-service

Security

- Conditional Access
- Permissions**
- Token encryption (Preview)

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs
- Access reviews

Review permissions

Why do you want to review permissions for this application?

- I want to control access to this application
- This application has more permissions than I want
- This application is suspicious and I want to investigate before allowing users to access
- This application is malicious and I'm compromised

RECOMMENDATION

- From Properties, require User assignment to access the application
- From User and Groups, remove unwanted users assigned to the application
- From User and Groups, assign user(s) or group(s) to the application

OPTIONAL

- Using PowerShell, remove all users assigned to stop access to the application

PowerShell script

```
Remove all users assigned to the application
Connect-AzureAD

# Get Service Principal using objectId
$sp = Get-AzureADServicePrincipal -ObjectId "f0b75bca-b8cb-4049-86e3-2cf39c9ffbf"

# Get Azure AD App role assignments using objectId of the Service Principal
$assignments = Get-AzureADServiceAppRoleAssignment -ObjectId $sp.ObjectId -All $true

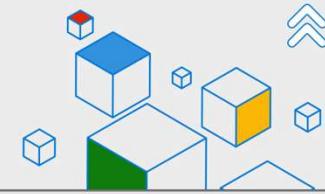
# Remove all users and groups assigned to the application
$assignments | ForEach-Object {
```

Visit here to learn more about permissions and consent grants



425Show

# Revoke previously granted tenant-wide permissions



To revoke an application's permissions that have been granted for the entire organization:

1. Sign in to the Azure portal using one of the roles listed in the prerequisites section.
2. Select Azure Active Directory, and then select Enterprise applications.
3. Select the application that you want to restrict access to.
4. Select Permissions.
5. The permissions listed in the Admin consent tab apply to your entire organization. Choose the permission you would like to remove, select the ... control for that permission, and then choose Revoke permission.

To review an application's permissions:

1. Sign in to the Azure portal using one of the roles listed in the prerequisites section.
2. Select Azure Active Directory, and then select Enterprise applications.
3. Select the application that you want to restrict access to.
4. Select Permissions. In the command bar, select Review permissions. Screenshot of the review permissions window.
5. Give a reason for why you want to review permissions for the application by selecting any of the options listed after the question, Why do you want to review permissions for this application?

**Graph Explorer - Permissions**

Enterprise Application

Dashboard > Enterprise applications - All applications

Overview Getting started Manage Properties Owners Users and groups Provisioning Self-service Security Conditional Access Permissions Token encryption (Preview) Activity Sign-ins Usage & insights (Preview) Audit logs Access reviews Troubleshooting + Support Virtual assistant (Preview) Troubleshoot New support request

Grant a permission

API NAME

WINDOWS

Windows PowerShell

RECOMMENDATION

Why do you want to review permissions for this application?

I want to control access to this application  
 This application has more permissions than I want  
 This application is suspicious and I want to investigate before allowing users to access it  
 This application is malicious and I'm compromised

OPTIONAL

From Properties, require User assignment to access the application  
From User and Groups, remove unwanted users assigned to the application  
From User and Groups, assign user(s) or group(s) to the application

Using PowerShell, remove all users assigned to stop access to the application

PowerShell script

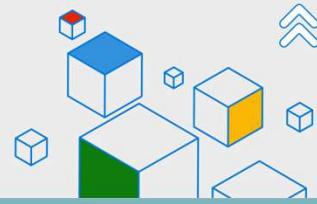
```
Remove all users assigned to the application
Connect-AzureAD
# Get Service Principal using objectId
$sp = Get-AzureADServicePrincipal -ObjectId "f0b75bca-b8cb-4049-86e3-2cf39c9ffbc"
# Get Azure AD App role assignments using objectId of the Service Principal
$assignments = Get-AzureADServiceAppRoleAssignment -ObjectId $sp.ObjectId -All $true
# Remove all users and groups assigned to the application
$assignments |ForEach-Object {
```

Visit here to learn more about permissions and consent grants



425Show

# Microsoft Entra ID Protection: Unfamiliar sign-in properties



**Stage : GA**

**Product family : Microsoft Entra ID Protection**

**License : Azure AD Premium P2**

**Overview :** The Unfamiliar sign-in properties detection shows which properties are unfamiliar in the Additional Info field in the Risk detection report details.

## Deployment Steps:

Step 1: Review existing reports

Step 2: Plan for Conditional Access risk policies

Step 3: Configure your policies

Step 4: Monitoring and continuous operational need

The screenshot shows the 'Risk Detection Details' page in the Microsoft Azure portal. The main content area displays a 'Risk Detection Details' card with the following information:

Property	Value
Detection type	Unfriendly sign-in properties
Risk state	At risk
Risk level	Low
Risk detail	-
Source	Identity Protection
Detection timing	Real-time
Activity	Sign-in
Detection time	6/13/2023, 12:35 AM
Detection last updated	6/13/2023, 12:37 AM
Token issuer type	Azure AD

Below this card, there is a section titled 'Additional Info' which contains the following text:

The following properties of this sign-in are unfamiliar for the given user: browser, device, IP, location, Exchange Active Sync ID, tenant IP subnet.

On the left side of the page, there is a sidebar with various navigation links under categories like 'Protect', 'Detect', and 'Manage'.



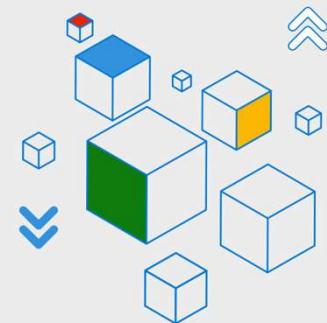
425Show

# Integration of Microsoft Entra ID Protection with Microsoft 365 Defender

Stage : GA

Product family : Microsoft Entra ID Protection

**Overview :** Microsoft Entra ID Protection alerts are correlated into related incidents along with alerts from the other security domains and can be reviewed directly in Microsoft 365 Defender for a holistic view of an end-to-end attack. Organizations who have deployed Microsoft 365 Defender and Microsoft Defender for Identity gain extra value from Identity Protection signals. This value comes in the form of enhanced correlation with other data from other parts of the organization and extra automated investigation and response.



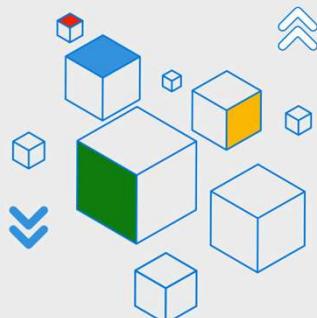
The screenshot shows the Microsoft 365 Defender web interface. On the left is a navigation sidebar with options like Home, Incidents & alerts (which is selected and highlighted with a red box), Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, and Devices. The main content area displays a user profile for "Bala Sandhu" (Senior Talent Sourcing | Woodgrove). Below the profile, there are tabs for Overview, Alerts (3), Observed in organization, and Timeline. The "Alerts" tab is active and highlighted with a red box. A table below shows three alerts, each with a red box highlighting the "Alert name" column. The table columns are Alert name, Severity, and Time generated.

Alert name	Severity	Time generated
Azure AD threat intelligence	High	Jun 30, 2023 7:59 PM
Azure AD threat intelligence	High	Jun 30, 2023 3:50 PM
Azure AD threat intelligence	High	Jun 22, 2023 3:49 PM



425Show

# New My Groups experience



Stage : GA

**Overview :** My Groups is an end-user group management experience that empowers admins to delegate group management to end users so they can manage their group membership and group lifecycle by themselves. The new My Groups experience improves navigation for end users, addresses limitations My Groups has today, and aligns with other end user experiences.

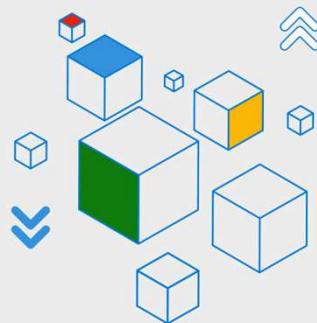
<https://myaccount.microsoft.com/groups/>

The screenshot shows the Microsoft My Groups interface. At the top, there's a navigation bar with the Microsoft logo, a search bar, and a user profile icon. On the left, a sidebar menu includes 'Overview' (which is selected and highlighted in blue), 'Groups I own (7)', 'Groups I am in (237)', and 'Requests (0)'. The main content area is titled 'Overview' and features a 'Collaborate' section with a 'Create M365 Group' button and an icon showing overlapping documents. Below this is a 'Requests to join your groups' section which currently displays 'No new requests.'



425Show

# New search experience in My Access



Stage : GA

Product family : Microsoft Entra ID Governance

Overview : Enables search of access packages based on keywords in access package names, descriptions, or resource names.

The screenshot shows the Microsoft Entra ID Governance interface. On the left, there's a sidebar with icons for 'Access packages' (selected), 'Request history', 'Approvals', and 'Access reviews'. The main area has a header with a search bar labeled 'Search packages by name, description or resources'. Below the header, the title 'Access packages' is displayed, followed by a sub-instruction: 'Access groups and teams, SharePoint sites, applications, and more in a single package. Select from the following packages, or search to find what you're looking for.' Underneath, there are three tabs: 'Available (28)', 'Active (0)', and 'Expired (0)'. The 'Available' tab is selected. The main content area is a table with columns: 'Name ↑', 'Description', 'Resources', and 'Actions'. The 'Actions' column contains a 'Request' button for each row. A red box highlights the search bar and the first four rows of the table. The table data is as follows:

Name ↑	Description	Resources	Actions
Access for on-premises apps	For header-based and apps requiring provisioning Leave...	Woodgrove_IT-Admins, Header App	Request
Approver flow	testing approver flow	Azure AD Power BI Content Pack App, AIPClient, Asana	Request
Azure Active Directory and Graph PowerShell	This access package grants you access for 30 days to Azure...	Azure Active Directory PowerShell, Microsoft Graph...	Request
Azure Lighthouse Administration	Access to Azure Lighthouse for administration of customer...	Lighthouse Administrators	Request



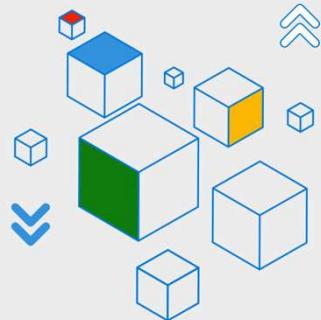
425Show

# Azure Key Vault: configure key rotation policy governance

Stage : GA

**License :** There's an additional cost per scheduled key rotation.

**Overview :** Using the Azure Policy service you can govern the key lifecycle and ensure that all cryptographic software and Hardware Security Module (HSM) keys within your Azure Key Vault are configured to undergo regular rotation, adhering to your organization's specific security standards.



**Rotation policy**

testkey

Expiry time: 2 years

Rotation:

Enable auto rotation:  Enabled  Disabled

Rotation option:  Automatically renew at a given time after ...

Rotation time: 18 months

Notification:

Notification option:  Notify at a given time before expiry

Notification time: 30 days



425Show

# Microsoft Entra Internet Access

**Stage :** Public Preview

**Product family :** Microsoft Entra Internet Access

**License :**

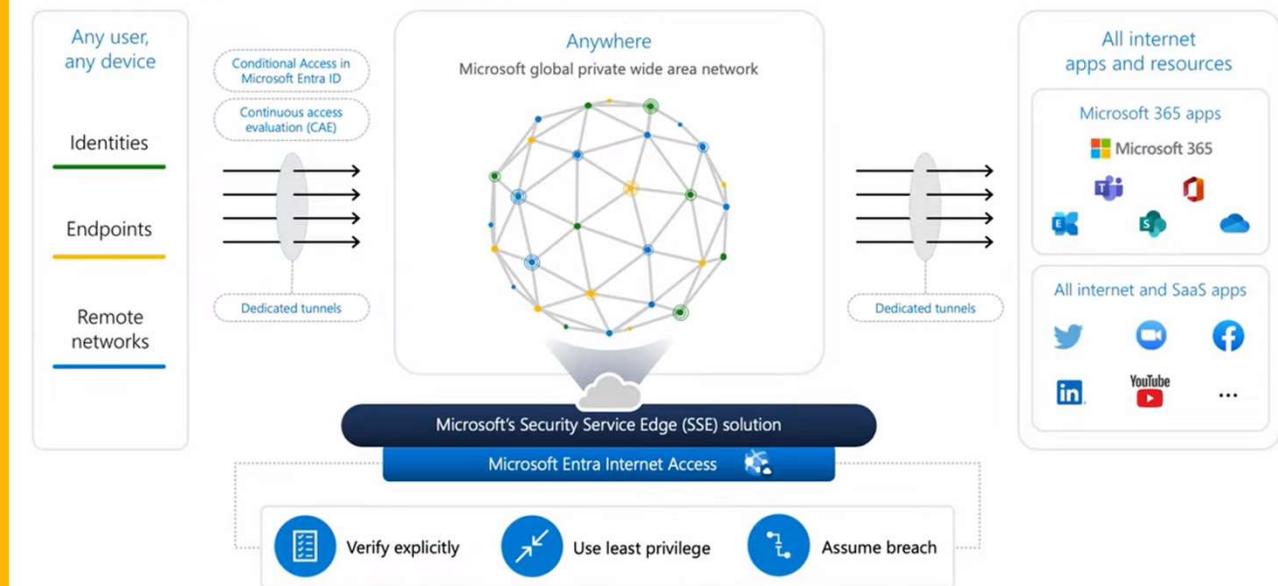
**Overview :** This identity-centric Secure Web Gateway (SWG) protects access to Microsoft 365 apps and enables best-in-class security and visibility, along with faster and more seamless access to Microsoft 365 apps. You can also leverage the extended Conditional Access capabilities and protect your organization against data exfiltration and token theft. Also, you gain detailed insights into your network traffic, including the original user source IP.

**Stakeholders to engage:** Networks, SecOps, helpdesk & end user compute



## Microsoft Entra Internet Access

An identity-centric Secure Web Gateway (SWG)





## Microsoft Entra Private Access



# Microsoft's Identity-centric SSE solution

### Microsoft Entra Internet Access

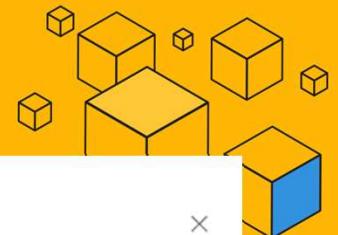
Secure access to all internet, SaaS, and Microsoft 365 apps and protect against malicious internet traffic with an **identity-centric Secure Web Gateway (SWG)**.





425Show

# Sponsors field for B2B users



**Stage :** Preview

**Overview :** The Sponsor refers to the person who invited the user to the organization to track who invited them and assign accountability.

**Deployment Steps:**  
to have the Global administrator direct User Administrators

1. Sign in to the Azure portal
2. Navigate to Azure Active Directory
3. Select Invite external users
4. Enter the details  
Next: Properties
5. You can add sponsors in the Properties
6. Select the Review + Create process.

Home > Ellis Turner >

## Ellis Turner ...

Properties

Refresh Got feedback?

All Identity Job Information Contact Information Parental controls Settings On-premises

Search

Showing 9 results

Manage	Job title
Company name	
Department	
Employee ID	
Employee type	
Employee hire date	
Office location	
Manager	+ Add manager
Sponsors (preview)	Elizabeth Moore  Edit

Troubleshoot New support



425Show

# Mobile Application Management (MAM) for Windows using Microsoft Edge

**Stage :** Preview

**Product family :** Microsoft Entra ID

**Overview :** Windows MAM extends MAM application configuration and protection capabilities to Edge on Windows including admin experience, policy lifecycle management, client for applications, and Windows Defender health checks. MAM is enforced via CA before allowing resource access on Windows which ensures only MAM protected Edge can access CA-protected resources.

## Deployment Steps:

Customers interested in the public preview will need to opt-in using the MAM for Windows Public Preview Sign Up Form.



Sign in to Outlook

https://login.microsoftonline.com/common/login

Outlook

Microsoft  
balas@contoso.com

Sign in with your work account

To access your service, app, or website, you may need to sign in to Microsoft Edge browser profile using [balas@contoso.com](#) or register your device with Contoso if you are already signed in. [Learn More](#)

[Sign out and sign in with a different account](#)

[More details](#)

[Switch Edge profile](#)



425Show

# Strictly enforce location policies using continuous access evaluation (CAE)



**Stage :** Preview

**Product family :** Microsoft Entra ID

**Overview :** Allows tenant admins to investigate IP addresses, seen by resource providers, to utilize CAE to promptly invalidate tokens that violate location policies.

Step 1 - Configure a Conditional Access location base policy for your target users

Step 2 - Test policy on a small subset of users

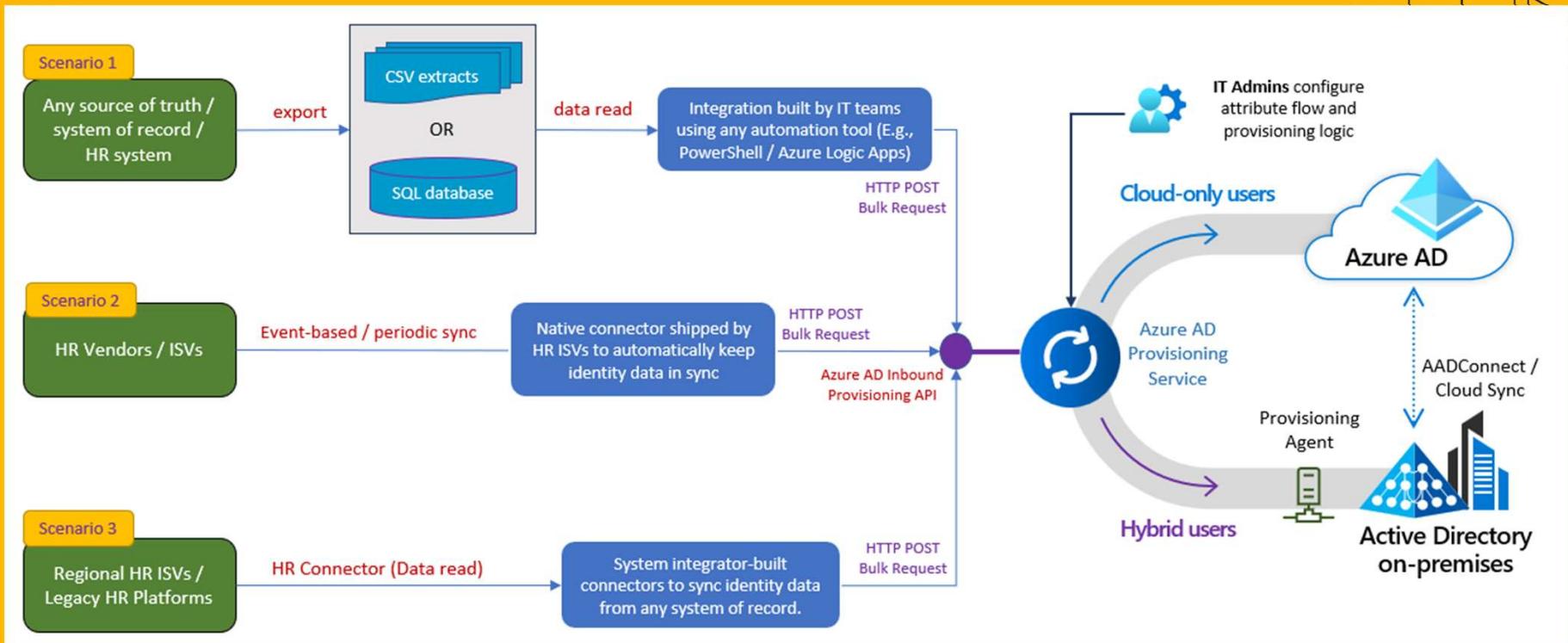
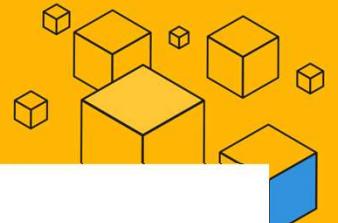
Step 3 - Use the CAE Workbook to Identify IP addresses that should be added to your named locations

Step 4 - Continue deployment - Repeat steps 2 and 3 with expanding groups of users until Strictly Enforce Location Policies are applied across your target user base. Roll out carefully to avoid impacting user experience.

The screenshot shows the Microsoft Azure portal interface for configuring a Conditional Access policy. The main pane displays the 'Conditional Access policy' settings, including assignments, target resources, conditions, and access controls. The 'Session' tab is active, showing options for controlling access based on session controls. A red box highlights the 'Customize continuous access evaluation' section, specifically the radio button for 'Strictly enforce location policies (Preview)'. Below this, another red box highlights the 'Session' section under 'Access controls', which contains the message 'Use continuous access evaluation - Strict location'. To the right, a separate window shows a Microsoft sign-in error message: 'You cannot access this right now' with the sub-message 'Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.'



# API-driven inbound provisioning



**Stage :** Preview **Product family :** Microsoft Entra ID

**Overview :** Enables you to use any automation tool of your choice to retrieve workforce data from any system of record for provisioning into Microsoft Entra ID and connected on-premises Active Directory domains. IT admins have full control on how the data is processed and transformed with attribute mappings. Once the workforce data is available in Microsoft Entra ID, IT admins can configure appropriate joiner-mover-leaver business processes using Microsoft Entra ID Governance Lifecycle Workflows.



425Show

# Microsoft Entra ID Protection: new landing page



Stage : Preview

Product family : Microsoft Entra ID Governance

License : Microsoft Entra ID Governance

**Overview :** The brand-new Microsoft Entra ID Protection dashboard is designed as a central hub to empower IT admins and SOC teams with rich insights and actionable recommendations tailored to your tenant. By providing a deeper view into the security posture of your organization, the dashboard enables you to implement effective protections accordingly.

The screenshot shows the Microsoft Entra ID Protection Dashboard (Preview) on a Microsoft Azure portal. The dashboard features a central illustration of a blue padlock on a network of clouds. Below the illustration are several data cards:

- Number of attacks blocked:** 18 (Past 3 months) - No change in the last 30 days. Number of attacks blocked by Identity Protection: 4. View attacks.
- Number of users protected:** 7 (Past 3 months) - No change in the last 30 days. Number of users in this tenant whose risk state is "Remediated" or "Dismissed": 1. View users protected.
- Mean time to remediate user risk:** 923 hours (Past 2 months) - Up 1044% in the last 30 days. Average time for the users' risk state to change from "At risk" to "Remediated". View remediated users.
- Number of high risk users:** 189 (Past 12 months) - No change in the last 30 days. Number of risky users with risk level "High". View high risk users.

The left sidebar contains navigation links for Dashboard (Preview), Overview, Tutorials, Diagnose and solve problems, Protect (User risk policy, Sign-in risk policy, Multifactor authentication registration policy), Report (Risky users, Risky workload identities, Risky sign-ins, Risk detections), Settings (Users at risk detected alerts, Weekly digest), Troubleshooting + Support (Troubleshoot, New support request), and Help.

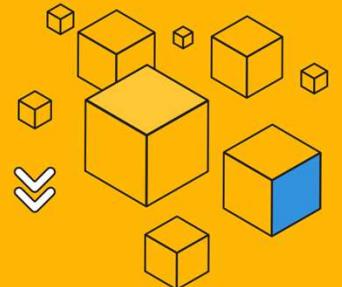
**Welcome to Microsoft Entra ID Protection**

Welcome to the new Microsoft Entra ID Protection home. Microsoft analyzes trillions of signals per day to prevent customers from identity compromise. Learn more about Microsoft Entra ID Protection.



425Show

# Microsoft Entra ID Governance: Sponsors as approvers in entitlement management



**Stage :** Preview

**Product family :** Microsoft Entra ID Governance

**License :** Microsoft Entra ID Governance

**Overview :** Sponsors for guest users can be approvers for access packages which were requested by a guest user.

## First Approver

**Sponsors as approvers (Preview)**

Manager as approver

Choose specific approvers

Sponsors as approvers (Preview)

### First Approver

! Sponsors as approvers requires a Microsoft Entra ID Governance subscription. [Learn more](#)

Manager as approver

Manager as approver

Choose specific approvers

Sponsors as approvers (Preview)

Decision must be made in how many days? !

14

Maximum 14

Require approver justification !

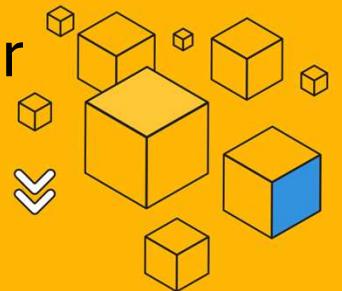
Yes     No

[Show advanced request settings](#)



425Show

# Microsoft Entra ID Governance: manage guest user lifecycle



**Stage :** Preview

**Product family :** Microsoft Entra ID Governance

**Overview :** Entitlement management (ELM) allows you to govern the state of a guest user's lifecycle. When a guest user is set as Governed, based on ELM tenant settings, their account will be deleted or disabled in specified days after their last access package assignment expires.

## Deployment Steps:

1. In the Azure portal, select Azure Active Directory and then select Identity Governance.
2. In the left menu, select Access packages and then open the access package.
3. In the left menu, select Assignments.
4. On the assignments screen, select the user you want to manage the lifecycle for, and then select Mark guest as governed (Preview).
5. Select save.

The screenshot shows the 'Assignments' screen for the 'Sales and Marketing' access package. The top navigation bar includes 'New assignment', 'Extend (Preview)', 'Reprocess (Preview)', 'Refresh', 'Download (Preview)', 'Remove', and 'Mark guest as governed (Preview)'. The left sidebar has sections for 'Overview', 'Manage' (with 'Resource roles', 'Policies', and 'Separation of Duties'), and a search bar. The main table lists assignments for 'Brian Johnson (TAILSPIN)'. The columns are 'Name', 'UPN', 'Policy', 'Status', and 'End date'. A new column 'User lifecycle (Preview)' is shown at the bottom right of the table. The 'Mark guest as governed (Preview)' button and the 'User lifecycle (Preview)' column are both highlighted with red boxes.

Name	UPN	Policy	Status	End date	User lifecycle (Preview)
Brian Johnson (TAILSPIN)	BrianJ@M365x41594852.OnMicro...	Initial Policy	Delivered	6/26/2024, 2:13:34 PM	



425Show

# Microsoft Entra ID Governance: inactive guest insights



**Stage :** Preview **Product family :** Microsoft Entra ID Governance **License :** 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.

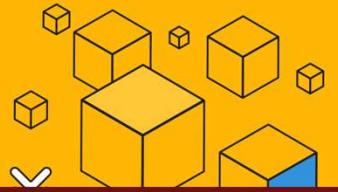
## Deployment Steps:

1. Sign in to the Azure portal and open the Identity Governance page.
2. Access the inactive guest account report by navigating to "Guest access governance" card and click on "View inactive guests"
3. You will see the inactive guest report which will provide insights about inactive guest users based on 90 days of inactivity. The threshold is set to 90 days by default but can be configured using "Edit inactivity threshold" based on your organization's needs.
4. The following insights are provided as part of this report:
  - Guest account overview (total guests and inactive guests with further categorization of guests who have never signed in or signed in at least once)
  - Guest inactivity distribution (Percentage distribution of guest users based on days since last sign in)
  - Guest inactivity overview (Guest inactivity guidance to configure inactivity threshold)
  - Guest accounts summary (A tabular view with details of all guest accounts with insights into their activity state. The Activity state could be active or inactive based on the configured inactivity threshold)
5. The inactive days are calculated based on last sign in date if the user has signed in atleast once. For users who have never signed in, the inactive days are calculated based on creation date.



425Show

# Microsoft Entra ID Governance: inactive guest insights



A Identity Governance - Microsoft ... +

portal.azure.com/#view/Microsoft\_AAD\_ERM/DashboardBlade/~/Dashboard

Microsoft Azure Search resources, services, and docs (G+/)

grpickin@woodgrove.ms WOODGROVE (WOODGROVE.MS)

Home > Identity Governance

Dashboard

Getting started

Entitlement management

Access packages

Catalogs

Connected organizations

Reports

Settings

Lifecycle workflows

Lifecycle workflows

Access reviews

Overview

Access reviews

Programs

Settings

Review History

Privileged Identity Management

Azure AD roles

Azure resources

Member user lifecycle governance

**129 member user accounts recently created**

Improve operational efficiency, increase new hire productivity and reduce security risks by automating your employee onboarding and offboarding tasks.

Configure lifecycle workflows Learn more

Application access governance

**254 apps with direct user assignments**

Manage how your employees and guests get access to business applications and maintain compliance by configuring request approval workflows and periodic access reviews, and automatically revoke access when it is no longer necessary.

Create access package Learn more

Guest access governance

**5 guest user accounts recently created**

Reduce security risk by monitoring inactive guest users at scale with intelligent insights, configure thresholds based on your compliance needs and perform periodic review of guest access to groups and business applications.

View inactive guests Learn more

Privileged access governance

Identity Governance status

## Welcome to Identity Governance

Manage identity and access rights across multiple applications and services to meet security and regulatory compliance requirements. With Microsoft Entra ID Governance, balance security and productivity by ensuring that the right people have the right access to the right resources for the right amount of time.

Learn more

Thank you for  
tuning in!

Don't forget to  
tune in again for  
the September  
updates on  
6<sup>th</sup> September  
2023



425Show



Grace Picking



Jorge Lopez