

SC-300

Tag 4

Microsoft Identity and Access Administrator

Guten Morgen!



LP4

Plan and implement
an identity governance
strategy



Agenda

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

Skillable Labs
noch 176 Tage
(saved 7 Tage)

Outline

- Plan and implement entitlement management
- Plan, implement, and manage access reviews
- Plan and implement privileged access PIM
- Monitor and maintain Microsoft Entra ID

Learning objectives

After completing this module, you will be able to:

- 1** Establish and maintain an identity governance strategy for your solutions.
- 2** Implement privileged identity and access reviews to ensure Zero Trust.
- 3** Monitor and investigate the usage of your identity and access solutions.

RBAC

Plan and implement
entitlement management

Access Packages
Catalogs

Groups
Apps
SP Sites

1 → 2
14 Tage

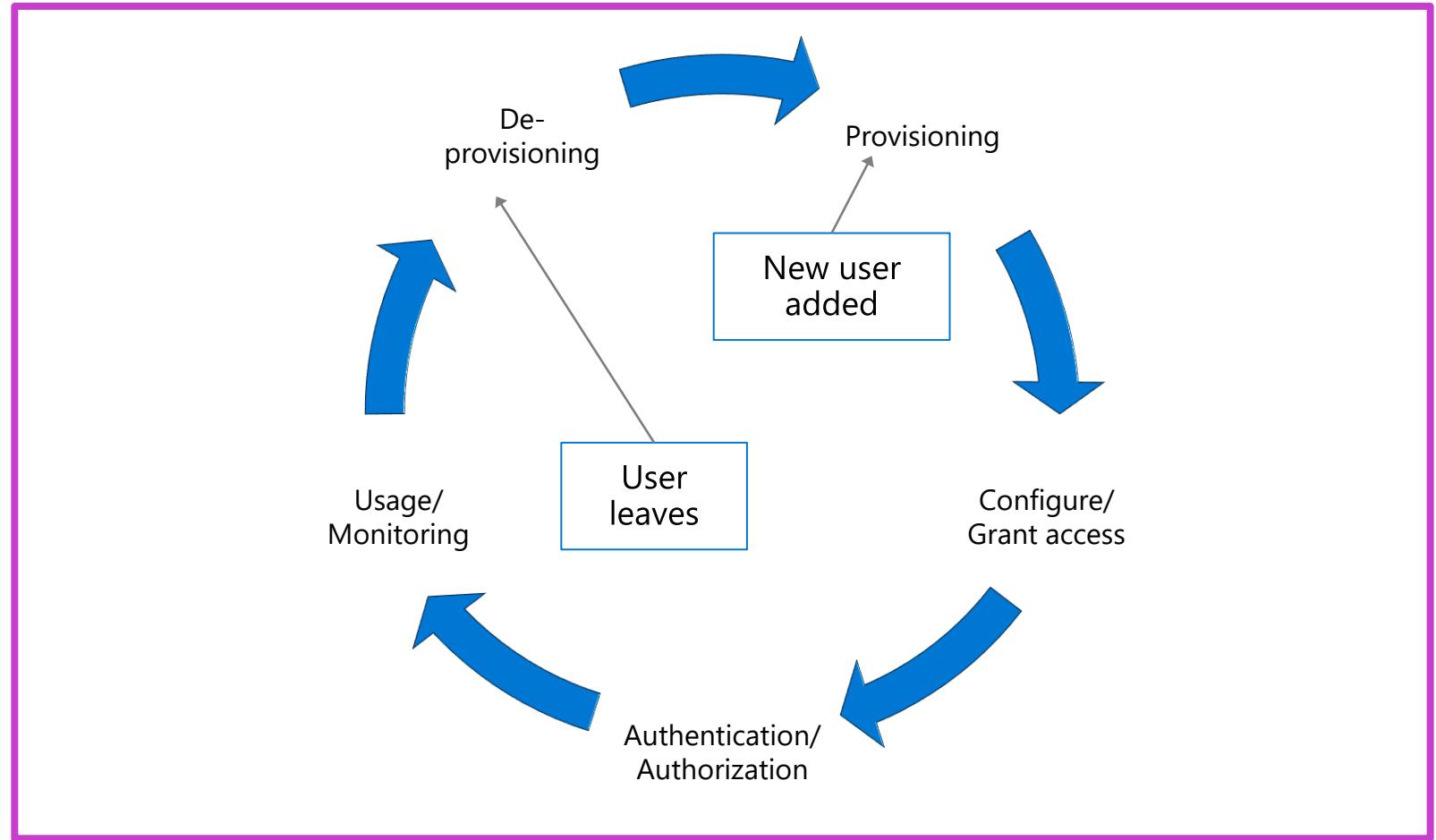
Objectives

- 1 Entitlement management
- 2 Define catalogs
- 3 Define access packages
- 4 Plan, implement, and manage entitlements
- 5 Implement and manage terms of use
- 6 Manage lifecycle of external users in Microsoft Entra ID
- 7 Configure and manage connected organization
- 8 Review per-user entitlements

Entitlement management

Governance and identity lifecycle management

- Governance is the process of overseeing and managing a system.
- Identity lifecycle management is the creation to deletion of accounts.



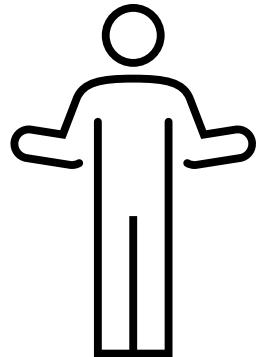
What is entitlement management?

Microsoft Entra entitlement management is an identity governance feature that enables organizations to manage the identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

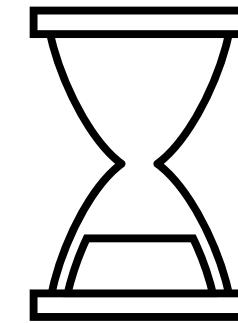
Microsoft Entra entitlement management can help you to more efficiently manage access to groups, applications, and SharePoint Online sites for internal users and for users outside your organization who need access to those resources.

Why is it important?

Users may not know what access they need or how to get it



Users may hold on to access longer than needed



Summary of terminology

My Account
My Apps
My Packages

Term	Description
Resource	An asset, such as a Microsoft 365 group, a security group, an application, or a SharePoint Online site, with a role that a user can be granted permissions to.
Policy	A set of rules that defines the access <u>lifecycle</u> , such as how <u>users</u> get access, who can approve it, and how long users have access through an <u>assignment</u> . A policy is linked to an access package. For example, an access package could have two policies: one for employees to request access and a second for external users to request access.
Access package	A bundle of resources that a team or project needs and that is governed with <u>policies</u> . An access package is always contained in a catalog. A new access package is created for a scenario in which users need to request access.
Catalog	A container of related resources and access packages. Catalogs are used for delegation so nonadministrators can create their own access packages. Catalog owners can add resources they own to a catalog.

Define access packages

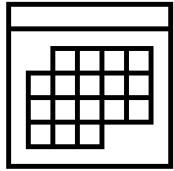
What are access packages? What can I manage with them?

- An access package is a list of resources such as groups, apps, and sites, along with the roles a user needs for those resources.
- There's a policy included in the access package with rules for who can access the package.



When should I use access packages?

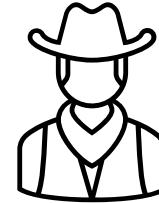
Time-limited
access



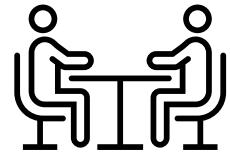
Manager approval
or delegated
role / identity



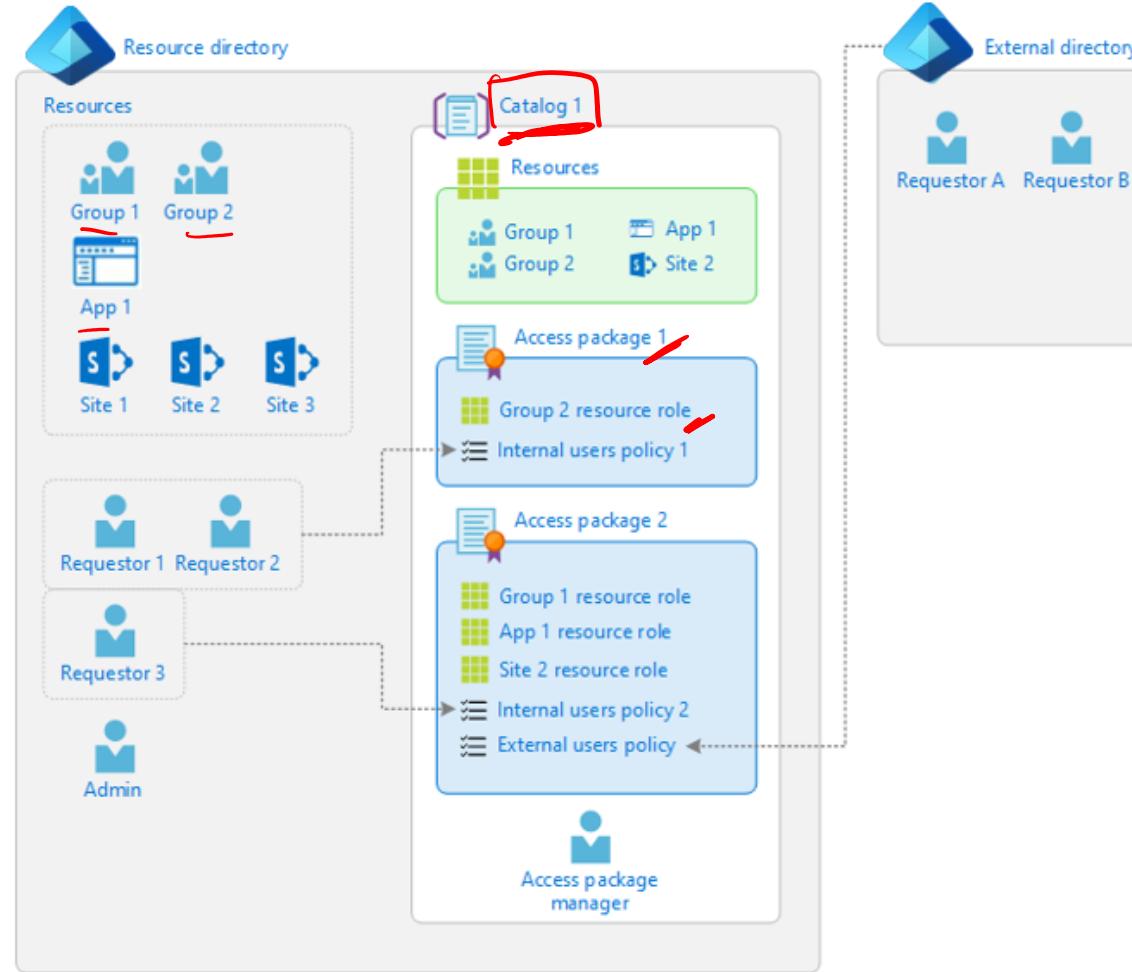
Manage access
without IT
involvement



Cross-organization
collaboration



How do I control who gets access?



Define catalogs

What's a catalog?

The screenshot shows the Microsoft Identity Governance interface for managing catalogs. On the left, there's a sidebar with links like Dashboard, Getting started, Diagnose and solve problems, Entitlement management (Access packages, Catalogs selected), and Connected organizations. The main area has a header with 'Identity Governance | Catalogs', a 'New catalog' button (which is highlighted with a red box), Column settings, Refresh, and Got feedback? link. Below the header is a search bar labeled 'Search by catalog name' and two dropdown filters: 'Enabled' (set to All) and 'Enabled for external users' (set to All). A table lists three catalogs: 'catSales' (description: 'Use this catalog to assign resources for members of the Sales team.', 1 access package, 5 resources, Enabled), 'catSalesTeam' (description: 'This is the catalog for the Sales Team resources.', 1 access package, 4 resources, Enabled), and 'General' (description: 'Built-in catalog.', 0 access packages, 0 resources, Enabled).

Name	Description	Access packages	Resources	Enabled
catSales	Use this catalog to assign resources for members of the Sales team.	1	5	Yes
catSalesTeam	This is the catalog for the Sales Team resources.	1	4	Yes
General	Built-in catalog.	0	0	Yes

A catalog is container of:

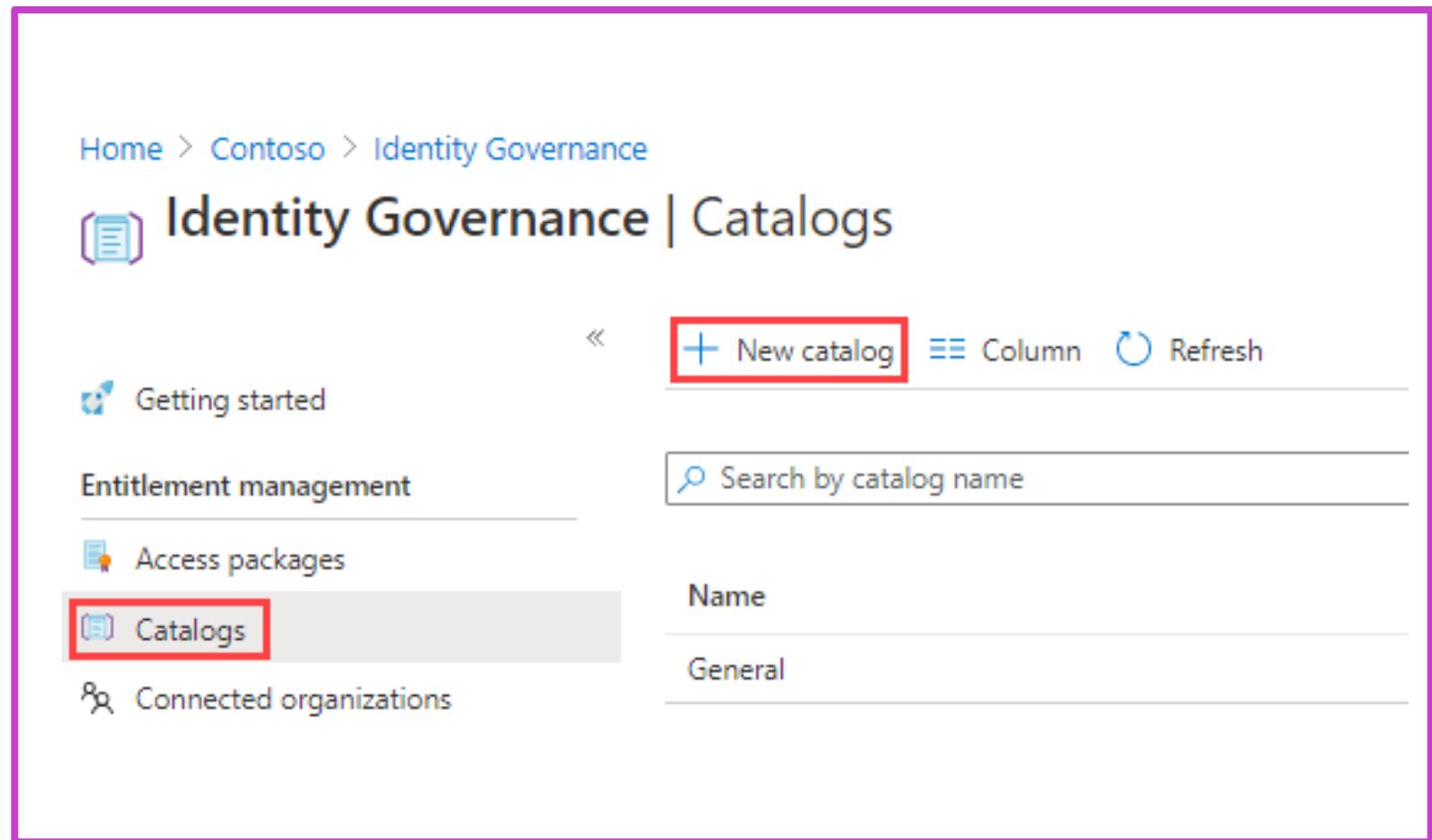
- Resources
- Access packages

It group related resources together.

The catalog creator is the default owner.

Creating a catalog

1. Log into Azure as global administrator
2. Open **Microsoft Entra ID** and then select **Identity Governance**, then **Entitlement Management**.
3. Select **Catalogs** and then **+ New Catalog**.
4. Enter a **Name** and **Description**.
5. Adjust the other settings as needed.
6. Select **Create**.



How do I add resources to a catalog?

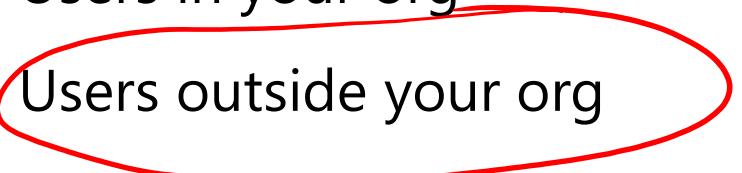
1. On the Identity Governance blade, if necessary, select **Catalogs**.
2. In the **Catalogs** list, select a catalog (**catSales** in example picture).
3. In the left navigation, under **Manage**, select **Resources**.
4. On the menu, select **+ Add resources**.
5. In the **Add resources to catalog**, review the available options.
6. When finished, click **Add**.

The screenshot shows the 'catSales | Resources' catalog page. The left sidebar has 'Overview' and 'Manage' sections; 'Manage' is selected and its sub-sections are 'Resources', 'Access packages', 'Roles and administrators', 'Custom extensions', and 'Reports'. The main area has a header with 'Add resources', 'Column', 'Remove', 'Require attributes', and 'Refresh' buttons. It includes a search bar and a dropdown for 'Type' set to 'All'. A table lists resources:

Resource	Type	Sub Type	Onboarded
<input type="checkbox"/> Demo App	Application	Application	Yes
<input type="checkbox"/> Sales and Marketing	Group and Team	Team	Yes
<input type="checkbox"/> Sales and Marketing	SharePoint Site	Site	Yes
<input type="checkbox"/> U.S. Sales	SharePoint Site	Site	Yes
<input type="checkbox"/> U.S. Sales	Group and Team	Team	Yes

Entitlement owners and process

- Delegate
- Users in your org
- **Users outside your org**
- Daily management
- Assignments and reports



?

Create a catalog of resources in Microsoft Entra ID

This exercise teaches students to create and manage catalogs for use with entitlement management in Microsoft Entra ID.

[Launch this exercise in GitHub](#)



Home > Identity Governance

Identity Governance | Terms of use

Terms of use

New terms Edit terms

Search for a terms of use

Name

Contoso Terms of Use

Activity

Audit logs

A screenshot of the Microsoft Entra ID Identity Governance Terms of use page. The page title is "Identity Governance | Terms of use". On the left, there's a sidebar with "Terms of use" selected. The main area shows a "Terms of use" card with a checkmark icon and the name "Contoso Terms of Use". There are buttons for "New terms" and "Edit terms", and a search bar. A vertical scrollbar is visible on the right side of the main content area.

Implement and manage terms of use

What are terms of use in entitlement management?

- Terms of use are stored as a PDF
- A PDF can contain any content, including contracts—End-User License Agreement (EULA)
- Can enforce compliance
- 24pt Font is recommended

New terms of use ...

Terms of use
Create and upload documents

Name * ⓘ Example: 'All users terms of use'

Terms of use document * ⓘ Upload required PDF Select default language

Display name + Add language

Require users to expand the terms of use ⓘ On Off

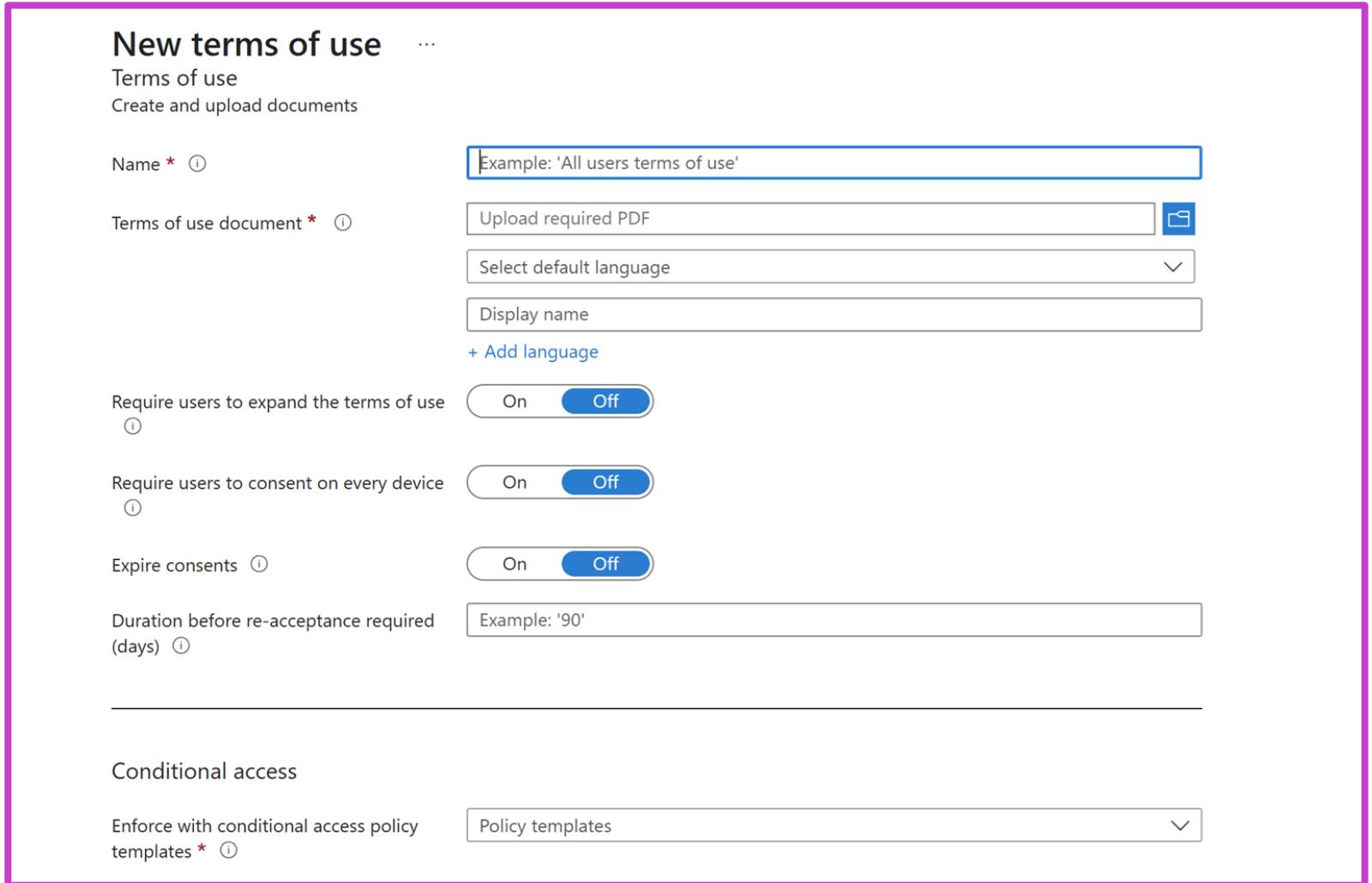
Require users to consent on every device ⓘ On Off

Expire consents ⓘ On Off

Duration before re-acceptance required (days) ⓘ Example: '90'

Conditional access

Enforce with conditional access policy templates * ⓘ Policy templates



Implement and manage terms of use



This exercise teaches students to create and manage terms of use for Microsoft Entra ID.

[Launch this exercise in GitHub](#)

A screenshot of the Microsoft Entra ID Terms of Use management interface. The title bar says "Identity Governance | Terms of use". Below the title are buttons for "New terms", "Edit terms", "Delete terms", "View audit logs", and "View selected". A search bar is labeled "Search for a terms of use". A table has one row with "Name" and "Contoso Terms of Use".

Name	
Contoso Terms of Use	

Manage the lifecycle of external users in Microsoft Entra ID

Manage the lifecycle of external users in Microsoft Entra ID Identity Governance settings

You can select what happens when an external user, who was invited to your directory through an access package request being approved, no longer has any access package assignments. This can happen if the user relinquishes all their access package assignments, or their last access package assignment expires. By default, when an external user no longer has any access package assignments, they're blocked from signing into your directory. After 30 days, their guest user account is removed from your directory.

Manage the lifecycle of external users

This exercise teaches students how to manage the lifecycle of external users in Microsoft Entra ID.

[Launch this exercise in GitHub](#)



Identity Governance | Settings ...

Dashboard Getting started

Entitlement management

- Access packages
- Catalogs
- Connected organizations
- Reports

Settings

Edit Got feedback?

Manage the lifecycle of external users
Select what happens when an external user, who was added to this directory

Block external user from signing in to this directory Yes No

Remove external user Yes No

Number of days before removing external user from this directory

Configure and manage connected organizations

What's a connected organization?

(No WS-Fed)

A connected organization is another organization that you have a relationship with. In order for the users in that organization to be able to access your resources, such as your SharePoint Online sites or apps, you'll need a representation of that organization's users in that directory. Because, in most cases, the users in that organization aren't already in your Microsoft Entra directory, you can use entitlement management to bring them into your Microsoft Entra directory as needed.

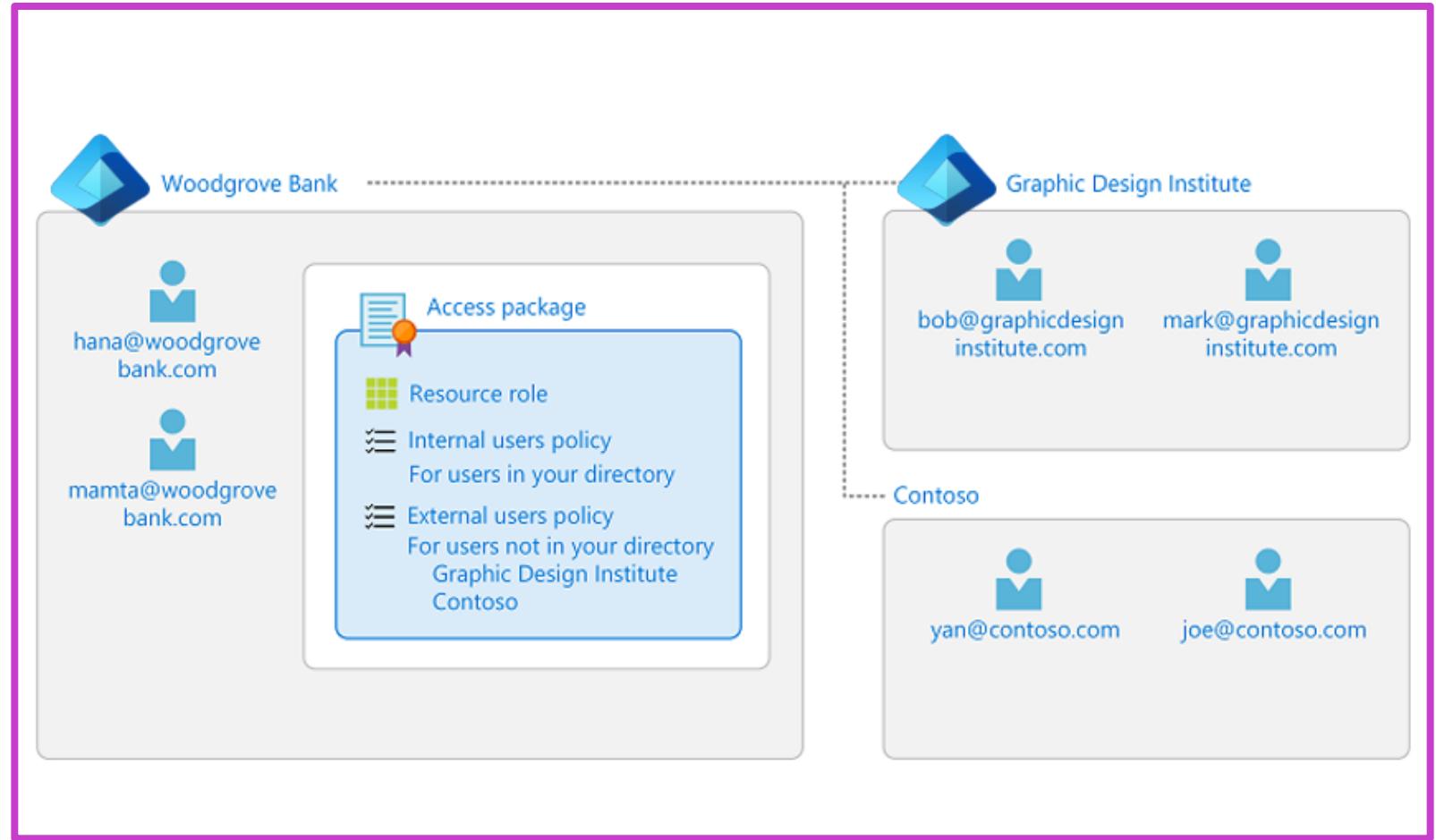
There are three ways that entitlement management lets you specify the users that form a connected organization:

- Users in another Microsoft Entra directory (from any Microsoft cloud).
- Users in another non-Microsoft Entra directory that's been configured for direct federation.
- Users in another non-Microsoft Entra directory, whose email addresses all have the same domain name in common.

Scenario: Woodgrove Bank and Contoso

For example, suppose you work at Woodgrove Bank and you want to collaborate with two external organizations. These two organizations have different configurations:

- Graphic Design Institute uses Microsoft Entra ID, and its users have a user principal name that ends with *graphicdesigninstitute.com*.
- Contoso does not yet use Microsoft Entra ID. Its users have a user principal name that ends with *contoso.com*.



Add a connected organization

- 1 In the **Microsoft Entra admin center**, select **Identity Governance**, then **Entitlement Management**.
- 2 In the menu, select **Connected organizations**, and then select **+ Add connected organization**.
- 3 Select the **Basics** tab, and then enter a **display name** and **description** for the organization.
- 4 Select the **Directory + domain** tab, and then select **Add directory + domain**.
- 5 In the **search** box, enter a domain name to search for the Microsoft Entra directory or domain. Be sure to enter the entire domain name.
- 6 Select **Add** to add the Microsoft Entra directory or domain. Currently, you can add only one Microsoft Entra directory or domain per connected organization.
- 7 After you've added the Microsoft Entra directory or domain, select **Select**.
- 8 Select the **Sponsors** tab, and then add optional sponsors for this connected organization.
 - Sponsors are internal or external users already in your directory. Sponsors are the point of contact for the relationship with this connected organization.
- 9 Select the **Review + create** tab, review your organization settings, and then select **Create**.

Review per-user entitlements

Who has an entitlement? Microsoft Entra admin center

Following the rules
of **Zero Trust**, you review
your entitlement
packages regularly.

There are tools built into
the system to support
this review.

The screenshot shows the Microsoft Entra admin center interface for managing access packages. The title bar reads "Infrastructure Apps | Assignments" under "Access package". The left sidebar, titled "Manage", includes options for "Resource roles", "Policies", "Separation of Duties", and "Assignments" (which is selected and highlighted with a grey background). The main area displays a table of assignments with columns for Name, UPN, Policy, and Status. A search bar at the top allows filtering by user name. The "Status" column shows various states like "Delivered" and "Expired". A red box highlights the "Assignments" option in the sidebar, and a red arrow points from the "Status" column header to the "Status" column itself, suggesting a filtering or sorting function.

Name	UPN	Policy	Status
Temir Hrdlickova	tehr91@woodgrove.ms	Initial Policy	Delivered
Ismat Bekarevich (OPS)	isbe54@woodgrove.ms	Initial Policy	Delivered
Irene Kuusik	irku66@woodgrove.ms	Initial Policy	Expired
Irene Kuusik	irku66@woodgrove.ms	Initial Policy	Expired
Irene Kuusik	irku66@woodgrove.ms	Initial Policy	Expired
Amala Braun	ambr26@woodgrove.ms	Initial Policy	Expired
Andoni Cermakova	ance28@woodgrove.ms	Initial Policy	Expired
Irene Kuusik	irku66@woodgrove.ms	Initial Policy	Expired
Ismat Bekarevich (OPS)	isbe54@woodgrove.ms	Initial Policy	Expired
Irene Kuusik	irku66@woodgrove.ms	Initial Policy	Expired
Thembisile Belisle (IDENTITY OPS)	thbe13@woodgrove.ms	Initial Policy	Expired
Ismat Bekarevich (OPS)	isbe54@woodgrove.ms	Initial Policy	Expired
Gulsat Meredowa	gume43@woodgrove.ms	Initial Policy	Expired
Ismat Bekarevich (OPS)	isbe54@woodgrove.ms	Initial Policy	Expired
Ismat Bekarevich (OPS)	isbe54@woodgrove.ms	Initial Policy	Expired

Review the assignments with PowerShell

```
Connect-MgGraph -Scopes "EntitlementManagement.Read.All"
```

```
Select-MgProfile -Name "beta"
```

```
$accesspackage = Get-MgEntitlementManagementAccessPackage -DisplayNameEq "Marketing Campaign"
```

```
$assignments = Get-MgEntitlementManagementAccessPackageAssignment -AccessPackageId $accesspackage.Id -ExpandProperty target -All -ErrorAction Stop -Debug
```

```
$assignments | ft Id,AssignmentState,TargetId,{$_.Target.DisplayName}
```

monad

PS Module

Microsoft.Graph.*

Az.*

Leibniz
Jeff Snover
0 1 0 1 0
cmdlet cmdlet cmdlet cmdlet
Monade

Microsoft
Graph
API
(Swagger)

AutoREST

Tool

Summary



In this section, you learned how to:

- Define catalogs.
- Define access packages.
- Plan, implement, and manage entitlements.
- Implement and manage terms of use.
- Manage the lifecycle of external users in Microsoft Entra ID.

References

Frequently asked questions

- <https://learn.microsoft.com/entra/identity/conditional-access/terms-of-use#frequently-asked-questions>
- Add a connected organization in Microsoft Entra entitlement management – Microsoft Entra | Microsoft Docs --
<https://learn.microsoft.com/entra/id-governance/entitlement-management-organization>



Plan, implement, and manage access reviews

Objectives

- 1** Plan for access reviews
- 2** Create access reviews for groups and apps
- 3** Create and configure access review programs
- 4** Manage licenses for access reviews
- 5** Automate access review management tasks
- 6** Configure recurring access reviews

Plan for access reviews

What's an access review?

Access reviews help users ensure that the right people have the right access to the right resources.

They mitigate access risk by protecting, monitoring, and auditing access to critical assets—while ensuring employee and business partner productivity.

They are done in Microsoft Entra ID Governance.

Planning a pilot

Pilot access reviews with a small group and targets noncritical resources. Piloting can help you adjust processes and increase users' and reviewers' ability to meet security and compliance requirements.

Things to consider when planning an access review pilot:

- What resources to review
- Who will review — Owner
- Test access
- Adjust, then test again

-

Who'll create and manage access reviews?

Resource type	Create and manage access reviews (Creators)	Read access review results
Group or application	Global Administrator User Administrator Identity Governance Administrator	Global administrator/reader User administrator Identity Governance administrator
Microsoft Entra roles	Global Administrator Privileged Role Administrator	Global administrator Global reader User administrator
Azure Resources (privileged roles)	Global Administrator User Administrator Resource Owner	User Access Administrator Resource Owner
Access package	Global Administrator User Administrator	Global Administrator Global Reader

Subset listed. See notes or content page.

Components of an access review

Before implementing your access reviews, you should plan the types of reviews relevant to your organization. To create an access review policy, you must have the following information:

- What resource(s) must be reviewed?
- Whose access is being reviewed?
- How often should the review occur?
- Who'll perform the review?
- How will they be notified to do the review?
- What are the timelines to be enforced for the review?
- What automatic actions should be enforced based on the review?
- What happens if the reviewer doesn't respond in time?
- What manual actions will be taken based on the review results?
- What communications should be sent based on the actions taken?

Plan access reviews for applications

When you review access to an application, you're reviewing the access for employees and external identities to the information and data within the application. Choose to review an application when you need to know who has access to a specific application, instead of an access package or a group.

Establish a plan for access reviews

- Review access packages
- Review groups and apps
- Review Microsoft Entra roles
- Review Azure resource roles

Plan communications

Communication is critical to the success of any new business process. Communicate to user proactively how and when their experience will change and how to gain support if they have issues.

Communicate changes in accountability

Customize email communication:

- Include a personal message to reviewers, so they understand it's sent by your compliance or IT department.
- Include a hyperlink or reference to internal information on what the expectations of the review are and additional reference or training material.
- Include a link to instructions on how to perform a self-review of access.

Create access reviews for groups and apps

Create access reviews for groups and apps

- Prevent stale access assignments by creating access reviews for group members or application access.
- If you need to review access routinely, you can also create recurring access reviews.

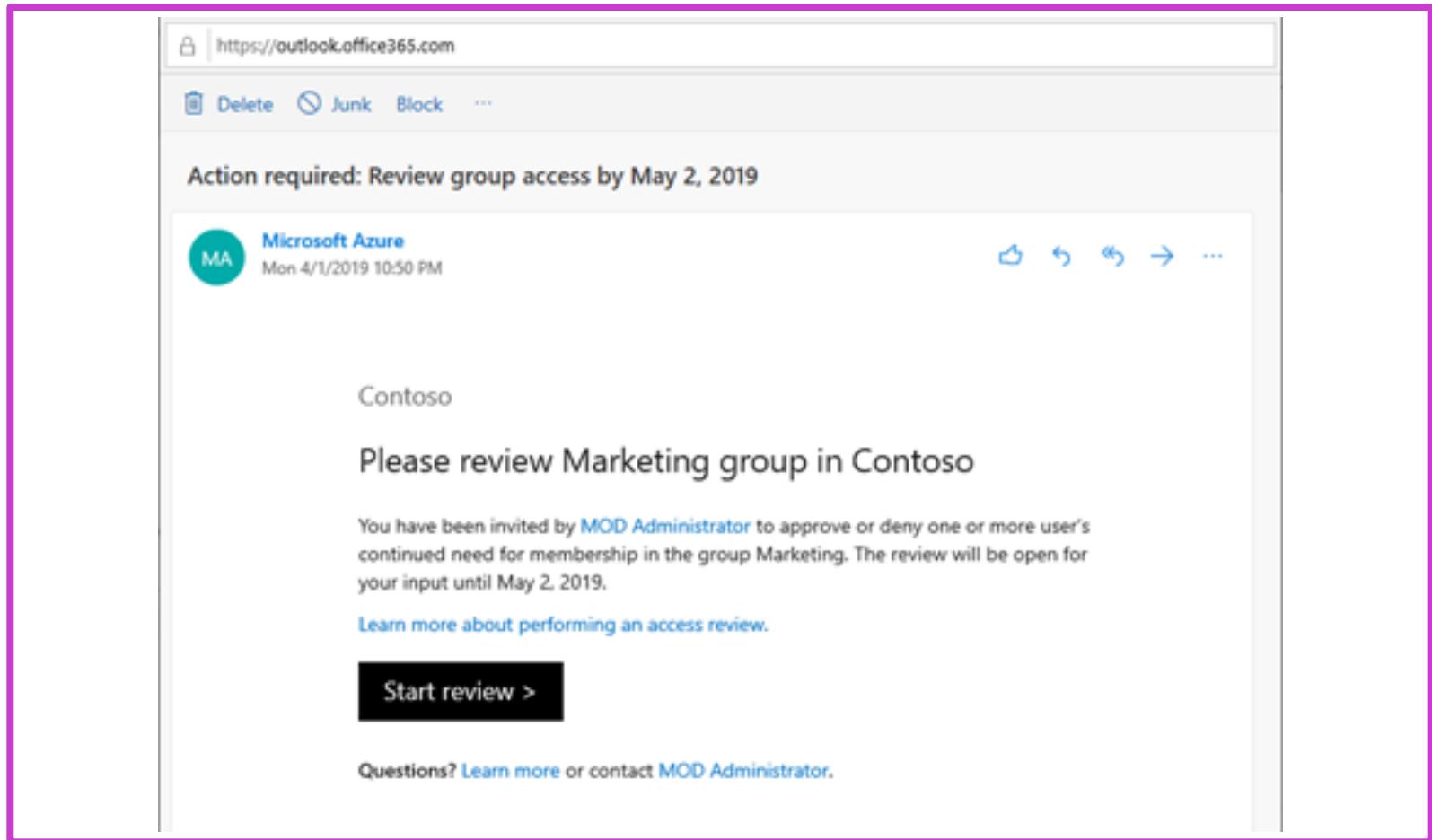
The screenshot shows the 'Identity Governance | Access reviews' page. On the left, there's a sidebar with navigation links: Entitlement management (Access packages, Catalogs, Connected organizations, Reports, Settings), Lifecycle workflows (Lifecycle workflows), Access reviews (Overview, Access reviews, Programs, Settings). The 'Access reviews' link under 'Access reviews' is highlighted with a grey background. The main area displays a table of access reviews with columns: Name, Resource, and Status. There are seven entries listed:

Name	Resource	Status
TestAgentReviewOutlier	Group Testing U2G	Active
InsightsReviewCheck	Group Insights Team Group	Active
Large Insights Group Test	Group Insights Large Group	Active
Testing U2G	Group Testing U2G	Active
Testing affiliations	Group Insights Team Group	Active
TestAgentReview_2	Group Insights Team Group	Active
TestAgentReviewWeekly	Group Insights Team Group	Active

Monitor access review findings

View an access review

- The reviewer is notified when a review is ready to perform.
- To check out the access review findings, follow the link in the email.



Review the access review findings

Perform access reviews manually

- 1 Review the list of users and decide whether to approve or deny their continued access.
- 2 Click **Approve** or **Deny**.
- 3 If required, provide a reason for the decision.
- 4 Once you have specified the action to take, click **Save**.

Recommendations are generated based on the user's sign-in activity

- 1 In the blue bar at the bottom of the page, click **Accept recommendations**. You'll see a summary of the recommended actions.
- 2 Click **OK** to accept the recommendations

Create and configure access review programs

Programs for access review

In Microsoft Entra ID, the access review is a feature of Microsoft Entra Identity Governance. Access reviews help to ensure that the right identities have the right access to the right resources in the organization. Access reviews can be implemented programmatically using the access reviews API in Microsoft Graph.

Microsoft Entra access review resource types:

- AccessReview—container for the access review.
- BusinessFlowTemplate—defines the resources on which an access review can be done.
- Program—defines an access review program.
- ProgramControl—links access review to a program.
- ProgramControlType—type of access review being done.

Register Microsoft Entra application to call Microsoft Graph API

- 1 Go to the Microsoft Entra ID screen, and select **App registrations** in the Manage section, to land at the page register apps
- 2 Select the **New application registration** button at the top of the page.
- 3 Provide a name for the application that's different from any other application in your tenant's directory (example = graphsample).
- 4 Change the Application type to **Native**, and provide the following as the Redirect URI:
urn:ietf:wg:oauth:2.0:oob
- 5 Select **Create**.
- 6 When the application is registered, copy the Application ID value, and save the value for later.
- 7 Select **Settings**, then select **Required permissions**.
- 8 Select **Add**. Choose **Select an API**, select **Microsoft Graph**, and then choose **Select**.
- 9 Check the box by those two permissions and choose **Select**.
- 10 Select **Done**.

Microsoft Entra access-reviews uses the following delegated permissions:

- Read all access reviews that user can access
- Manage all access reviews that user can access
- Read all programs that user can access
- Manage all programs that user can access.

This example application requires only the permissions:
Read all access reviews that user can access and **Read all programs that user can access**

Automate access review management tasks

Automate access review management tasks

Take recommendations

Recommendations can be created to suggest changing permissions based on user behavior. For example, if a user is inactive for 30 days, it will recommend that the user be removed.

Review guest user access

Review and clean up collaboration partners' access.

You can choose to have access removal automated by setting the **Auto apply results to resource option** to **Enable**. Once the review is completed and has ended, users who weren't approved by the reviewer will automatically be removed from the resource—or kept with continued access. This could mean removing their group membership, their application assignment, or revoking their right to be elevated to a privileged role.

Configure recurring access reviews

Configure recurring access reviews

- Access reviews can be set to occur on a recurring basis.
- Name your access review, select a start date, frequency, duration, and end date, then you're ready to go. Reviewers will be notified at the start of each review.
- Reviewers can approve or deny access with a user-friendly interface and with the help of smart recommendations.

Why have recurring access reviews?

By doing an access review once and never again, there's limited value. So set up reviews to occur on a regular schedule.

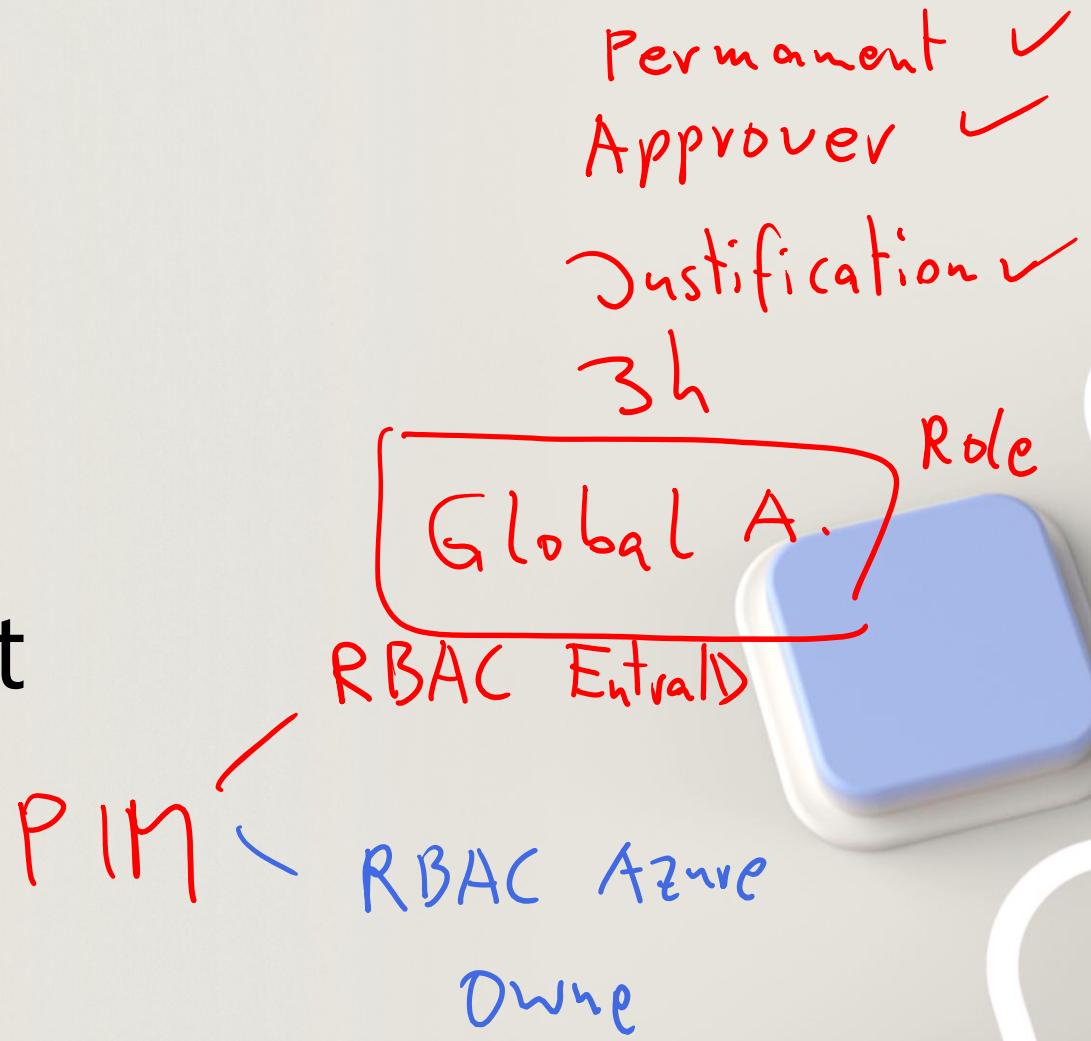
Summary



In this section you learned how to:

- Plan for access reviews.
- Create access reviews for groups and apps
- Monitor access review findings
- Manage licenses for access reviews
- Automate access review management tasks
- Configure recurring access reviews

Plan and implement privileged access



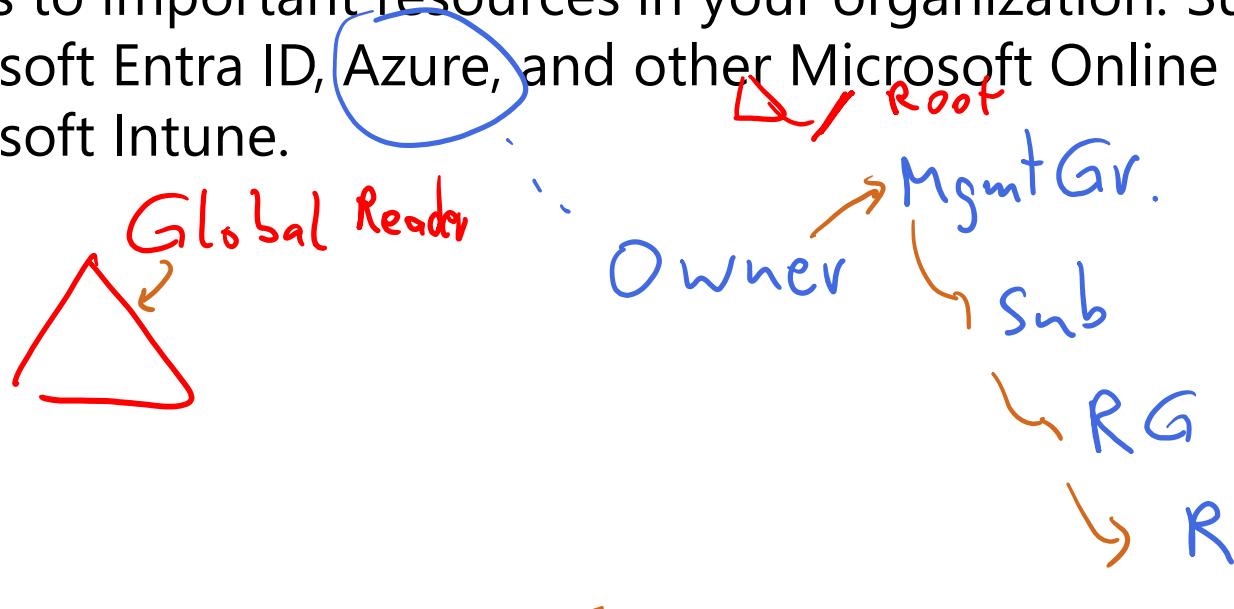
Objectives

- 1** Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds)
- 2** Configure Privileged Identity Management (PIM) for Azure Roles
- 3** Configure PIM for Azure resources
- 4** Assign roles
- 5** Manage PIM requests
- 6** Analyze PIM audit history and reports
- 7** Create and manage break-glass accounts

Define a privileged access strategy for administrative users

What's Privileged Identity Management (PIM)?

PIM is a service in Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization. Such resources include those in Microsoft Entra ID, Azure, and other Microsoft Online Services, such as Microsoft 365 or Microsoft Intune.



What does PIM do?

PIM provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources you care about.
The key features of PIM include:

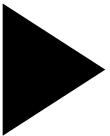
- Provide just-in-time privileged access to Microsoft Entra ID and Azure resources.
- Assign time-bound access to resources using start and end dates.
- Require approval to activate privileged roles.
- Collect justification to understand why users activate.
- Get notifications when privileged roles are activated.
- Conduct access reviews to ensure users still need the roles.
- Download audit history for internal or external audit.

Define a privileged access strategy for administrative users

Identify stakeholders



Start using PIM



Enforce the principle of least privilege



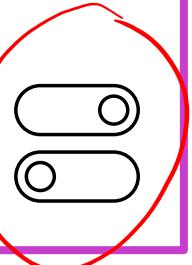
Decide which roles to protect with PIM



Decide whether to use a group to assign roles



Decide which users should be permanent or eligible



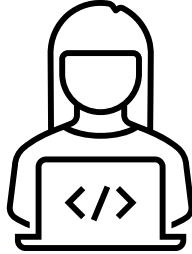
Draft your PIM settings



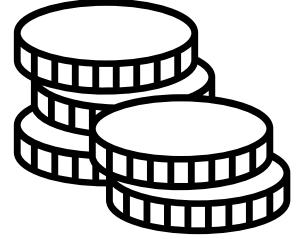
Principle of least privilege

The principle of least privilege states that every process, user, or program should only be able to access the information and resources necessary for its legitimate purpose.

Developer



Financial analyst



Just enough access — Just in time

Plan and configure privileged access groups

Management for privileged access groups

In PIM, you can now assign eligibility for the membership or ownership of privileged access groups. You can assign Microsoft Entra built-in roles to cloud groups and use PIM to manage group member and owner eligibility and activation. With the privileged access groups preview, you can give workload-specific administrators quick access to multiple roles with a single just-in-time request.

Example:

Your **Tier-0 Office Admins** might need just-in-time access to the **Exchange Admin, Office Apps Admin, Teams Admin, and Search Admin** roles to thoroughly investigate incidents thoroughly daily.

Example: How to implement

1. Create a new group.
2. Check the role-assignable box.
3. Add these roles:
 - Exchange Admin
 - Office Apps Admin
 - Teams Admin
 - Search Admin
4. Add the members and owners of the group.
5. Using PIM, make eligible for assignment.
6. Set the duration.

Home > App administrators | Settings > Role setting details - Owner >

Edit role setting - Owner

Privileged Identity Management | Privileged access groups (Preview)

Activation **Assignment** Notification

Allow permanent eligible assignment

Expire eligible assignments after
1 Year

Allow permanent active assignment

Expire active assignments after
6 Months

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment

Configure Privileged Identity Management (PIM) for Azure resource roles

Assign Azure resource roles

PIM can manage the built-in Azure resource roles, as well as custom roles, including (but not limited to) the following:

- Owner
- User Access Administrator
- Contributor
- Security Admin
- Security Manager

Exercise: Assign Azure resource roles in PIM

This exercise teaches the student how to manage the built-in Azure resource roles, as well as custom roles.

[Launch this exercise in GitHub](#)



Home > Privileged Identity Management >

Azure resources - Discovery ✖

Privileged Identity Management | Azure resources

Refresh Manage resource

Discover Azure resources that you have write permission to

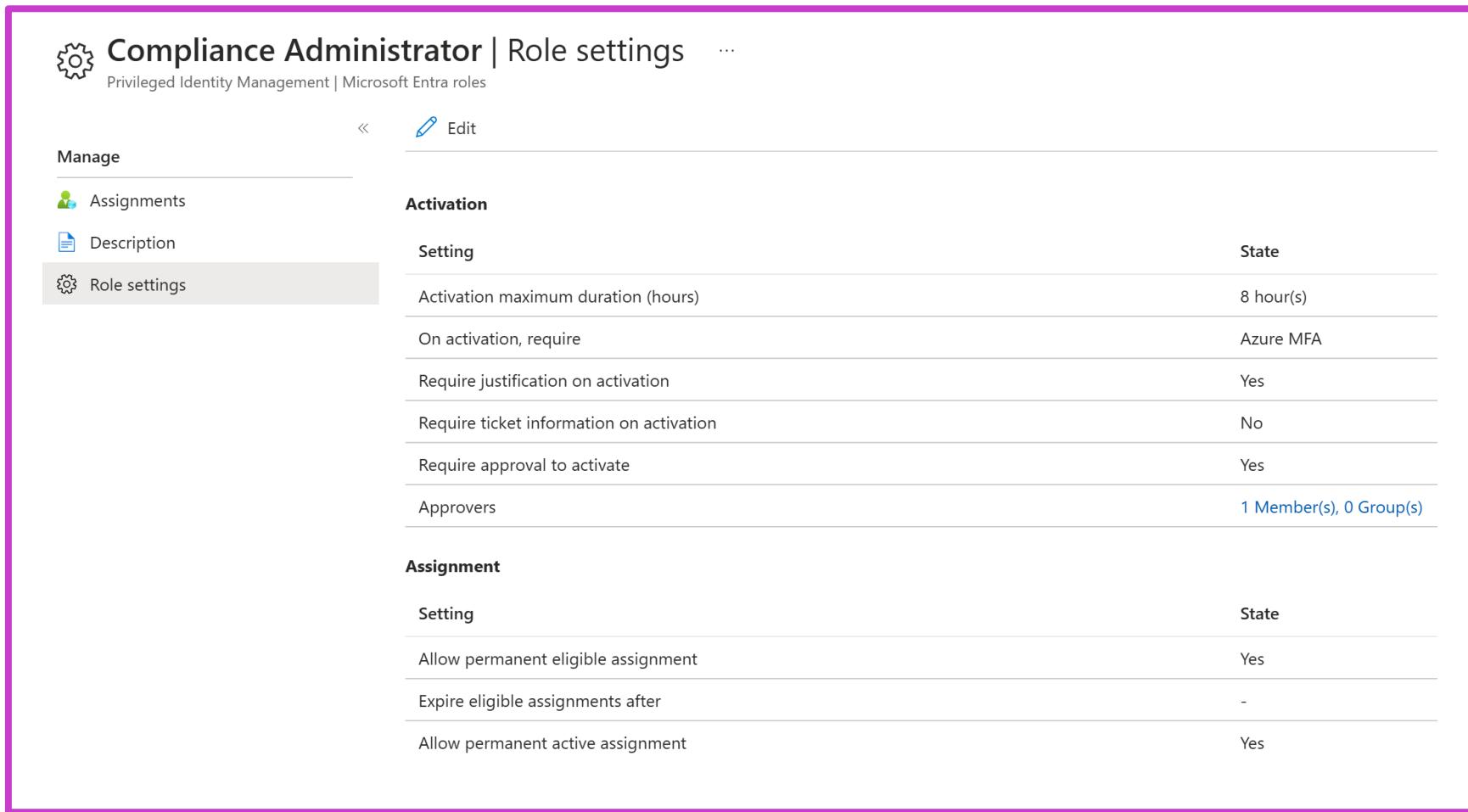
Search by resource name

Resource

Configure Privileged Identity Management (PIM) for Microsoft Entra roles

Configure PIM for Microsoft Entra roles

A Privileged Role Administrator can customize PIM in their Microsoft Entra organization, including changing the experience for a user who's activating an eligible role assignment.



The screenshot shows the 'Role settings' page for a 'Compliance Administrator' role in Microsoft Entra. The left sidebar has 'Manage' navigation with 'Assignments', 'Description', and 'Role settings' (selected). The main area is titled 'Activation' with sections for 'Setting' (Activation maximum duration: 8 hour(s), State: 8 hour(s)), 'On activation, require' (Azure MFA), 'Require justification on activation' (Yes), 'Require ticket information on activation' (No), and 'Require approval to activate' (Yes). It also lists 'Approvers' (1 Member(s), 0 Group(s)). The 'Assignment' section includes 'Setting' (Allow permanent eligible assignment: Yes, State: Yes), 'Expire eligible assignments after' (No value listed), and 'Allow permanent active assignment' (Yes).

Exercise: Configure PIM for Microsoft Entra roles

This exercise teaches the student how to configure PIM for Microsoft Entra and for Azure roles.

[Launch this exercise in GitHub](#)



Prohibited Identity Management > Contoso

Contoso | Roles

Identity Management | Azure AD roles

Add assignments Refresh Export Got feedback

Search by role name

Role
Application Administrator
Application Developer
Attack Payload Author
Attack Simulation Administrator
Authentication Administrator
Azure DevOps Administrator
Azure Information Protection Administrator

Analyze Privileged Identity Management (PIM) audit history and reports

Analyze PIM audit history and reports

The screenshot shows the 'Visual Studio Enterprise | Resource audit' interface. At the top, there's a logo and the text 'Visual Studio Enterprise | Resource audit' followed by 'Privileged Identity Management | Azure resources'. Below this is a navigation bar with 'Overview' (selected), 'Export', and 'Got feedback?'. A search bar says 'Search by member name'. On the left, there's a sidebar with 'Tasks' (My roles, Pending requests, Approve requests, Review access) and 'Activity' (Resource audit, My audit). The 'Resource audit' item is highlighted with a grey background. The main area is titled 'Time' and shows 'No results'.

Reasons to use PIM

Minimize access to secure information or resources and give users just-in-time privileged access to Azure resources and Microsoft Entra ID, while maintaining oversight of admin privileges.

What does it do?

PIM provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources you care about.

Create and manage break-glass accounts

What's a *break-glass account* and why use one?

Prevent being accidentally locked out of your Microsoft Entra organization because you can't sign in or activate another user's account as an administrator.

Emergency access accounts are limited to emergency or "break glass" scenarios where normal administrative accounts can't be used. We recommend you maintain a goal of restricting emergency account use to only the times when it's necessary.

Implement strict security controls—always

Considerations for creating break-glass accounts

Create emergency accounts

Create two or more emergency access accounts. These accounts should be cloud-only accounts that use the *.onmicrosoft.com domain and that aren't federated or synchronized from an on-premises environment.

Exclude multifactor authentication

At least one of your emergency access accounts should not have the same multifactor authentication mechanism as your other non-emergency accounts.

Exclude from Conditional Access

During an emergency, you don't want a policy to potentially block your access to fix an issue. At least one emergency access account should be excluded from all Conditional Access policies.

Validate break-glass accounts

When you train staff members to use emergency access accounts and validate the emergency access accounts, as a minimum, do the following steps at regular intervals:

- Define which account to check.
- Ensure the accounts are documented and current.
- Ensure security officers who might need emergency accounts are trained on the process.
- Update the account credentials—in particular, any passwords.
- Validate that the emergency access accounts can sign in and perform administrative tasks.
- Ensure that multifactor authentication or self-service password reset (SSPR) isn't registered to any individual user's device or details.

Frequency of break-glass accounts verification

Account verifications should be performed at regular intervals and for key changes:

- At least every 90 days.
- When there has been a recent change in IT staff, such as a job change, a departure, or a new hire.
- When the Microsoft Entra subscriptions in the organization have changed.

Summary



In this section you learned how to:

- Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds).
- Configure Privileged Identity Management (PIM) for Microsoft Entra roles.
- Configure PIM for Azure resources.
- Assign roles.
- Manage PIM requests.
- Analyze PIM audit history and reports.
- Create and manage break-glass accounts.

Monitor and maintain Microsoft Entra ID

Objectives

- 1 Analyze and investigate sign-in logs to troubleshoot access issues
- 2 Review and monitor Microsoft Entra audit logs
- 3 Enable and integrate Microsoft Entra diagnostic logs with Log Analytics/
Microsoft Sentinel
- 4 Export sign-in and audit logs to a third-party SIEM
- 5 Review Microsoft Entra activity by using Log Analytics/Microsoft Sentinel,
excluding KQL use
- 6 Analyze Microsoft Entra ID workbooks/reporting
- 7 Monitor security posture with Identity Secure Score in Microsoft Entra ID

Analyze and investigate sign-in logs to troubleshoot access issues

Troubleshoot access issues

Activity

- **Sign-ins:** Review sign-in activities.
- **Audit logs:** Review system activity.
- **Provisioning logs:** Monitor activity by the provisioning service.

Security

- **Risky sign-ins:** Indicator of odd sign-in behavior.
- **Users flagged for risk:** Indicator than an account might be compromised.

Access this information by going to:

Microsoft Entra admin center → Identity → Monitoring & Health

How long are logs available?

Diagnostic Settings
Log Metrics →
• Storage Account
• Log Analytics Workspace (tables)
• Event Hub

Report	Free Microsoft Entra ID	Microsoft Entra ID P1	Microsoft Entra ID P2
Audit Logs	7 days	30 days	30 days
Sign-ins	7 days	30 days	30 days
Multifactor authentication usage	30 days	30 days	30 days
Microsoft Graph activity logs	N/A	Must be stored in a storage account	Must be stored in a storage account

Security Signals	Free Microsoft Entra ID	Microsoft Entra ID P1	Microsoft Entra ID P2
Risky users	Unlimited	Unlimited	Unlimited
Risky sign-ins	7 days	30 days	90 days

Sign-ins report

First, narrow down the reported data to a level that works for you.

Second, filter sign-in data using the date field as the default filter.

 Monitoring & health



Sign-in logs

Audit logs

Provisioning logs

Health (Preview)

Log Analytics

Diagnostic settings

Workbooks

Usage & insights

Bulk operations

Download sign-in activities

The user sign-ins report provides answers to the following questions:

- What's the sign-in pattern of a user?
- How many users have signed in over a week?
- What's the status of these sign-ins?

File formats available:

- CSV or JSON.

Available records:

- The most recent 100,000 records.

Download Sign-ins in JSON format

X

i You can download up to a maximum of 100,000 records per file (e.g. if you are downloading the interactive and non-interactive sign-ins files, you will get 100,000 rows for each file). If you want to download more, use our reporting APIs or export to a storage account, SIEM or Log Analytics through "Export Data Settings". Click here to learn more.

i Your download will be based on the filter selections you have made.

File Name

InteractiveSignInIns_2023-01-09_2023-01-10

Download

Filter sign-in activities

Get more targeted data:

- Filter content specific to your needs.
- Reporting APIs.
- Export data to storage account or SIEM or Log Analytics.

The screenshot shows a user interface for filtering sign-in activities. At the top right is a button labeled "Add filters". Below it is a section titled "Pick a field" containing a list of filter options. The "Request ID" option is selected (indicated by a blue border around the input field). A green rectangular box highlights a group of five options: "Status", "IP address", "Location", "Resource", and "Resource ID". Other options shown include "User", "Username", "Application", "Operating system", "Device browser", "Correlation ID", and "Conditional access". At the bottom right is a "Apply" button.

+ Add filters

Pick a field

Request ID

User

Username

Application

Status

IP address

Location

Resource

Resource ID

Operating system

Device browser

Correlation ID

Conditional access

Apply

Sign-in activity for managed applications

With an application-centric view of your sign-in data, you can answer questions such as these:

- Who's using my applications?
- What are the top three applications in my organization?
- How's my newest application doing?

The screenshot shows the 'Usage & insights | Microsoft Entra application activity (Preview)' dashboard. A red oval highlights the title bar. On the left, a sidebar titled 'Manage' lists several options: 'Microsoft Entra application activity (Preview)' (selected), 'AD FS application migration', 'Authentication methods activity', 'Service principal sign-in activity (Preview)', 'Application credential activity (Preview)', and 'License Utilization'. The main area displays a message: 'These are your most active applications. See which ones have a low sign in success rate.' Below this is a 'Date range' dropdown set to '30 days'. A search bar allows searching by application name or object ID. A table titled 'Successful sign-ins' lists the top applications with their names and counts: Microsoft_AAD_UsersAndTenants (2), Microsoft 365 Support Service (1), Azure Portal (63), Office365 Shell WCSS-Client (9), Microsoft 365 Security and Compliance Center (2), ADlbizaUX (9), Best Practices Demo (3), Microsoft Office 365 Portal (1), and Office 365 Exchange Online (1).

Application name	Successful sign-ins
Microsoft_AAD_UsersAndTenants	2
Microsoft 365 Support Service	1
Azure Portal	63
Office365 Shell WCSS-Client	9
Microsoft 365 Security and Compliance Center	2
ADlbizaUX	9
Best Practices Demo	3
Microsoft Office 365 Portal	1
Office 365 Exchange Online	1

Review and monitor Microsoft Entra audit logs

Audit logs

The Microsoft Entra audit logs provide records of system activities for compliance. To access the audit report, select **Audit logs** in the **Monitoring** section of **Microsoft Entra ID**.

An audit log has a default list view that shows the following:

- Date and time of the occurrence.
- Service that logged the occurrence.
- Category and name of the activity (what).
- Status of the activity (success or failure).
- Target.
- Initiator/actor (who) of the activity.

Filtering audit logs

Service filter

- Microsoft Entra ID Management UX
- Access Reviews
- Account Provisioning
- Application Proxy
- Authentication Methods
- B2C (Business to Customer)
- Conditional Access
- Core Directory
- Entitlement Management
- Hybrid Authentication
- Identity Protection
- Invited Users
- And more...

Category filter

- AdministrativeUnit
- ApplicationManagement
- Authentication
- Authorization
- Contact
- Device
- DeviceConfiguration
- DirectoryManagement
- EntitlementManagement
- GroupManagement
- KerberosDomain
- KeyManagement
- And more...

Activity filter

- You can select a specific activity you want to see or choose all.

User and group audit logs

With user and group-based audit reports, you can get answers to questions such as:

- What types of updates have been applied to users?
- How many users were changed?
- How many passwords were changed?
- What has an administrator done in a directory?
- What groups have been added?
- Are there groups with membership changes?
- Have the owners of a group been changed?
- What licenses have been assigned to a group or a user?

The screenshot shows the Microsoft Azure portal interface. On the left, there's a navigation pane with 'Identity' selected, which further branches into 'Overview', 'Users', 'Groups', and 'Overview'. Under 'Users', 'Audit logs' is highlighted. The main content area is titled 'Users | Audit logs' and lists several audit log categories: 'All users', 'Audit logs' (which is also highlighted), 'Sign-in logs', 'Diagnose and solve problems', 'Deleted users', 'Password reset', 'User settings', 'Bulk operation results', and 'New support request'. The 'Audit logs' item has a blue square icon next to it.

Enterprise application audit logs

With application-based audit reports, you can get answers to questions such as these:

- What applications have been added or updated?
- What applications have been removed?
- Has a service principal for an application changed?
- Have the names of applications been changed?
- Who gave consent to an application?

The screenshot shows the Microsoft Azure portal interface. On the left, there is a navigation pane with the following structure:

- Identity
 - Overview
 - Devices
- Applications
 - Enterprise applications
 - App registrations
 - Roles & admins
 - Roles & admins
 - Admin units
 - Delegated admin partners
- Learn & support

On the right, the main content area is titled "Enterprise applications | Audit logs". It contains the following sections:

- Overview
- Diagnose and solve problems
- Manage
 - All applications
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews
 - Admin consent requests
 - Bulk operation results

The "Audit logs" item under the Activity section is highlighted with a gray background.

Microsoft 365 activity logs

Logs can be viewed from the Microsoft 365 admin center. Only the Microsoft 365 admin center provides a full view of the Microsoft 365 activity logs.

Enable and integrate
Microsoft Entra diagnostic
logs with Log Analytics/
Microsoft Sentinel

What's Log Analytics?

Home > Monitor

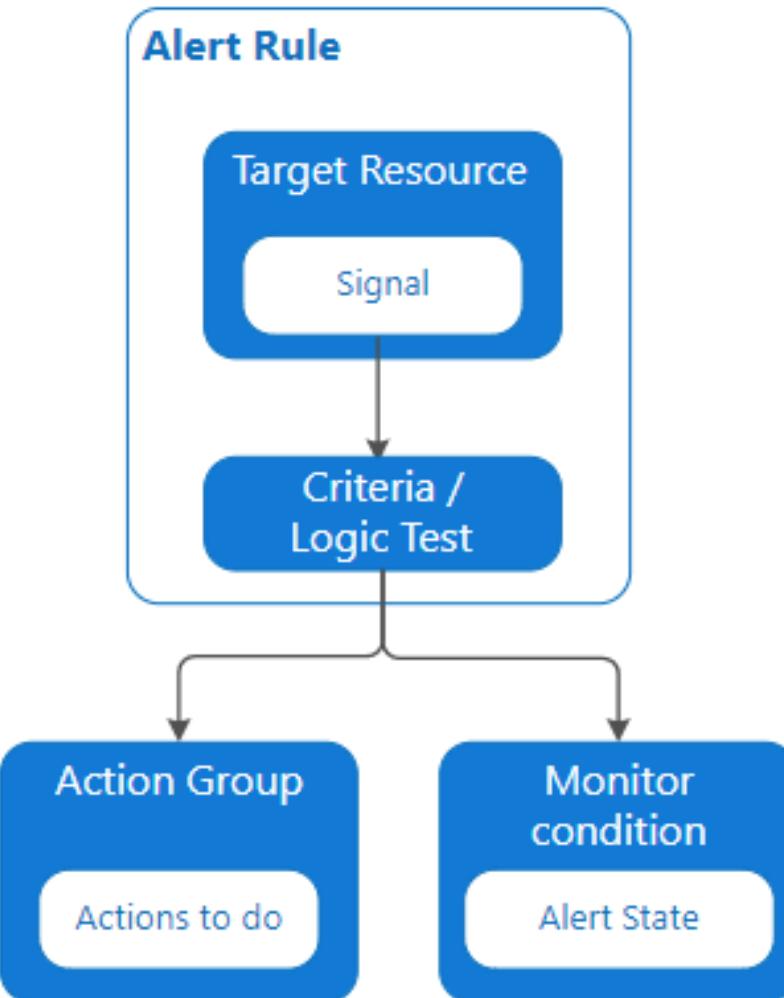
The screenshot shows the Microsoft Azure Monitor Logs interface. At the top, there is a navigation bar with 'Home' and 'Monitor'. Below it is a header with 'Monitor | Logs' and a Microsoft logo. A search bar is on the left. In the center, there is a 'New Query 1' card with a close button and a plus sign. To its right are buttons for 'ContosoResource...', 'Select scope', 'Run' (which is highlighted in blue), and 'Save'. A time range selector shows 'Last 24 hours'. Below these controls is a text input field containing the placeholder 'Type your query here or click one of the queries to start'. A red handwritten mark 'KQL' is overlaid on this input field. On the far left, a sidebar lists several options: Overview, Activity log, Alerts, Metrics, Logs (which is selected and highlighted in grey), and Change Analysis.

Log Analytics is a tool in the Azure portal used to edit and run log queries from data collected by Azure Monitor Logs and to interactively analyze their results interactively. You can use Log Analytics queries to retrieve records matching criteria, identify trends, analyze patterns, and provide a variety of insights into your data.

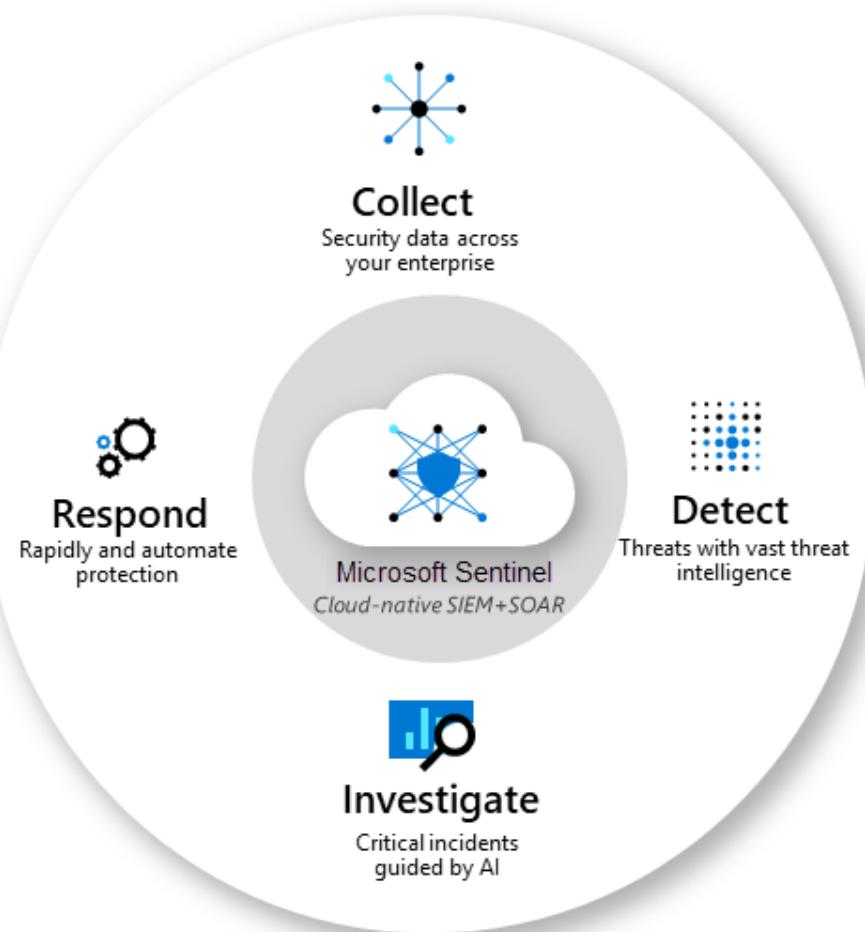
Azure Monitor alerts

Alerts proactively notify you when issues are found with your infrastructure or application using your monitoring data in Azure Monitor.

- Watch virtual machines, storage accounts, and other sources for events or thresholds.
 - Possible early warning of an attack.
- Set actions and alerts to trigger when conditions are met.



What is Microsoft Sentinel?



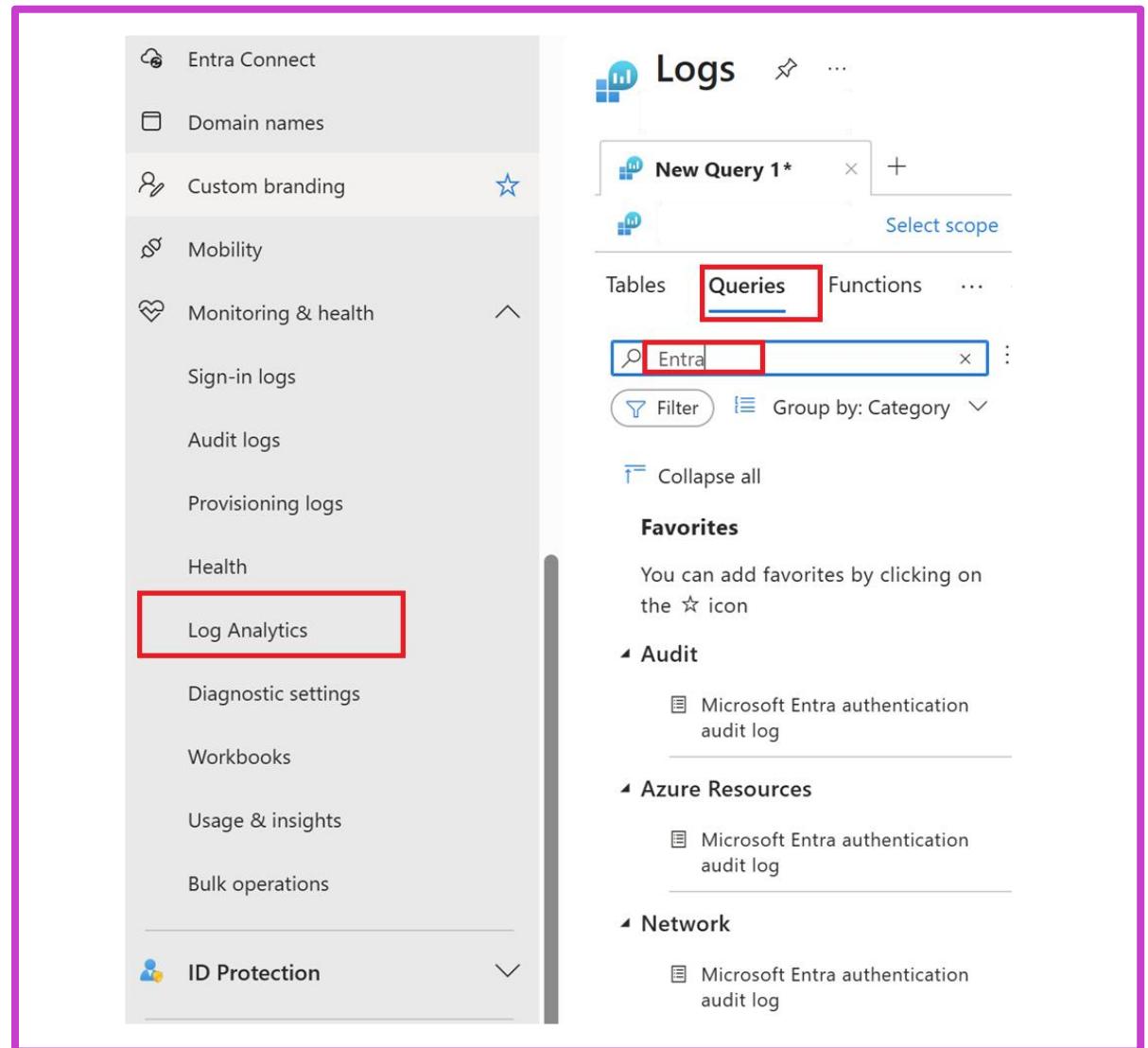
Microsoft Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

Connecting Microsoft Entra logs into Log Analytics

Azure Monitor → Logs → Queries hub

- Use an existing query.
- Build your own in the query window.

A Microsoft Entra ID license is required.



Connecting Microsoft Entra ID logs into Microsoft Sentinel

**Microsoft Sentinel →
Data Connectors
(Content Hub)**

Set up or use a Workspace.

Microsoft Entra ID

- Sign-in logs and audit logs.

Microsoft Entra ID license required.

The screenshot shows the Microsoft Sentinel Content hub interface. At the top, there's a navigation bar with 'Home > Microsoft Sentinel workspaces > Microsoft Sentinel'. Below it is the title 'Microsoft Sentinel | Content hub' with a sub-header 'Selected workspace: 'sentinelloganalytics''. On the left, a sidebar lists categories like General, Threat management, and Content management. The main area displays various connectors: 'Solutions' (358), 'Standalone contents' (276), 'Installed' (1), and 'Updates' (1). A search bar and filters for 'Status : All' and 'Content type : All' are also present. A table lists the connectors, with the 'Microsoft Entra ID' row highlighted by a red box. This row shows the connector name, a 'FEATURED' badge, an 'Installed' status with a green checkmark, and an 'Updates' link. Other connectors listed include Microsoft Defender for... (Not installed), Microsoft Defender XDR (Not installed), Network... (Not installed), SAP applications (Not installed), Security Threat Essenti... (Not installed), and Sentinel SOAR Essentials (Not installed).

Content title	Status
Microsoft Defender for...	FEATURED Not installed
Microsoft Defender XDR	FEATURED Not installed
Microsoft Entra ID	FEATURED Installed Updates
Network ...	FEATURED PREVIEW Not installed
SAP applications	FEATURED Not installed
Security Threat Essenti...	FEATURED Not installed
Sentinel SOAR Essentials	FEATURED Not installed

Exercise: Connect data from Microsoft Entra ID to Microsoft Sentinel



This exercise teaches the student how to connect Microsoft Entra ID and Microsoft Sentinel.

[Launch this exercise in GitHub](#)

Azure Sentinel

data connectors

Guides & Feedback Refresh

68 Connectors 0 Connected 0 Coming soon

Azure

Connector name

- Azure Active Directory Microsoft
- Azure Active Directory Identity Protection Microsoft
- Azure Activity Microsoft
- Azure Advanced Threat Protection (Preview) Microsoft
- Azure DDoS Protection Microsoft
- Azure Firewall Microsoft
- Azure Information Protection (Preview) Microsoft
- Azure SQL Database Microsoft
- Azure Security Center

Azure Active Directory

Not connected Status

Description Gain insights into Azure Active Directory logs to Azure Sentinel. Active Directory scenarios, conditional access policies, Sign-in logs. You can get info on Reset (SPR) usage, Azure AD-like user, group, role, app info.

Last data received ...

Related content

6 Workbooks 2 Queries

Data received

100
80
60
40

Open connector page

Export sign-in and audit logs to a third-party SIEM

Introduction to SIEM

Security information and event management (SIEM) is a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Most of the top Azure services can be accessed through a single logging pipeline, including Azure Resource Manager and Microsoft Defender for Cloud. These services have onboarded to Azure Monitor and produce relevant security logs to ease the setup and management of log routing across large Azure environments.

Example of a few third-party SIEM tools

SIEM tool	Currently using log integrator
Splunk	Begin migrating to the Azure Monitor Add-On for Splunk.
IBM QRadar	Begin migrating to the Microsoft Azure DSM and Microsoft Azure Event Hub Protocol, available from the IBM support website.
ArcSight	The ArcSight Azure Event Hub smart connector is available as part of the ArcSight smart connector collection.

Analyze Microsoft Entra ID workbooks/reporting

Analyze Microsoft Entra ID with usage and insights

- Explore the effects of Conditional Access policies on your users' sign-in.
- Troubleshoot sign-in issues and check sign-in health.
- Find legacy authentication sign-in attempts.
- Many other items.

Microsoft Entra admin center

Home > Usage & insights

Usage & insights

- Microsoft Entra application activity (Preview)
- AD FS application activity
- Authentication methods activity
- Service principal sign-in activity (Preview)
- Application credential activity (Preview)

Identity governance

External Identities

User experiences

Hybrid management

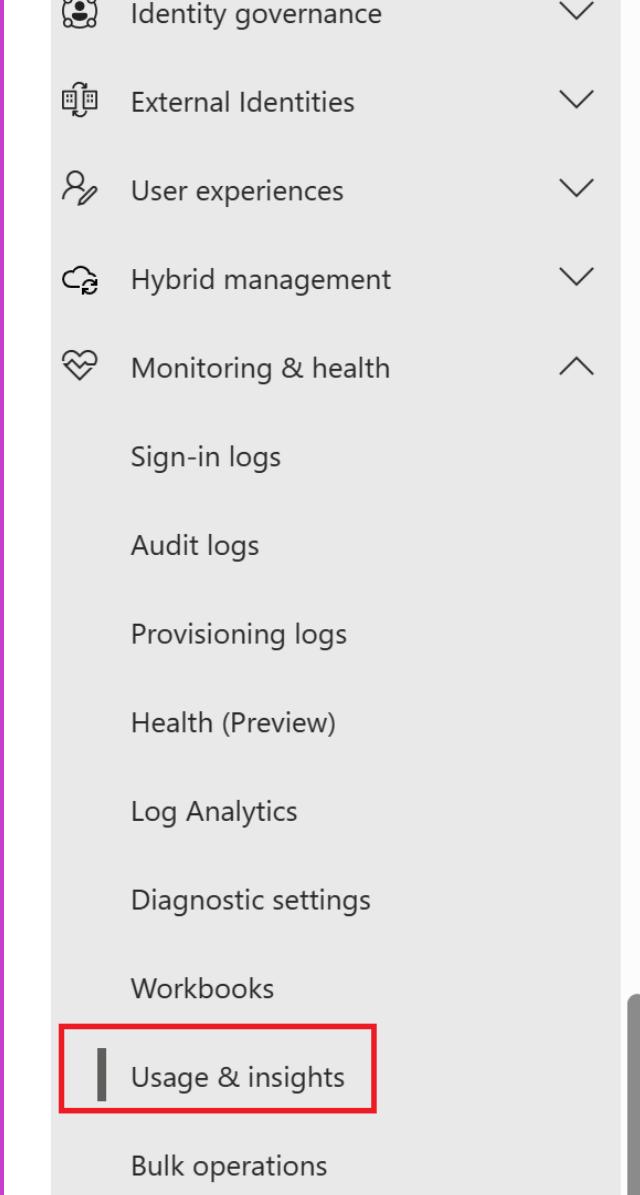
Monitoring & health

- Sign-in logs
- Audit logs
- Provisioning logs
- Health (Preview)
- Log Analytics
- Diagnostic settings

Workbooks

Usage & insights

Bulk operations

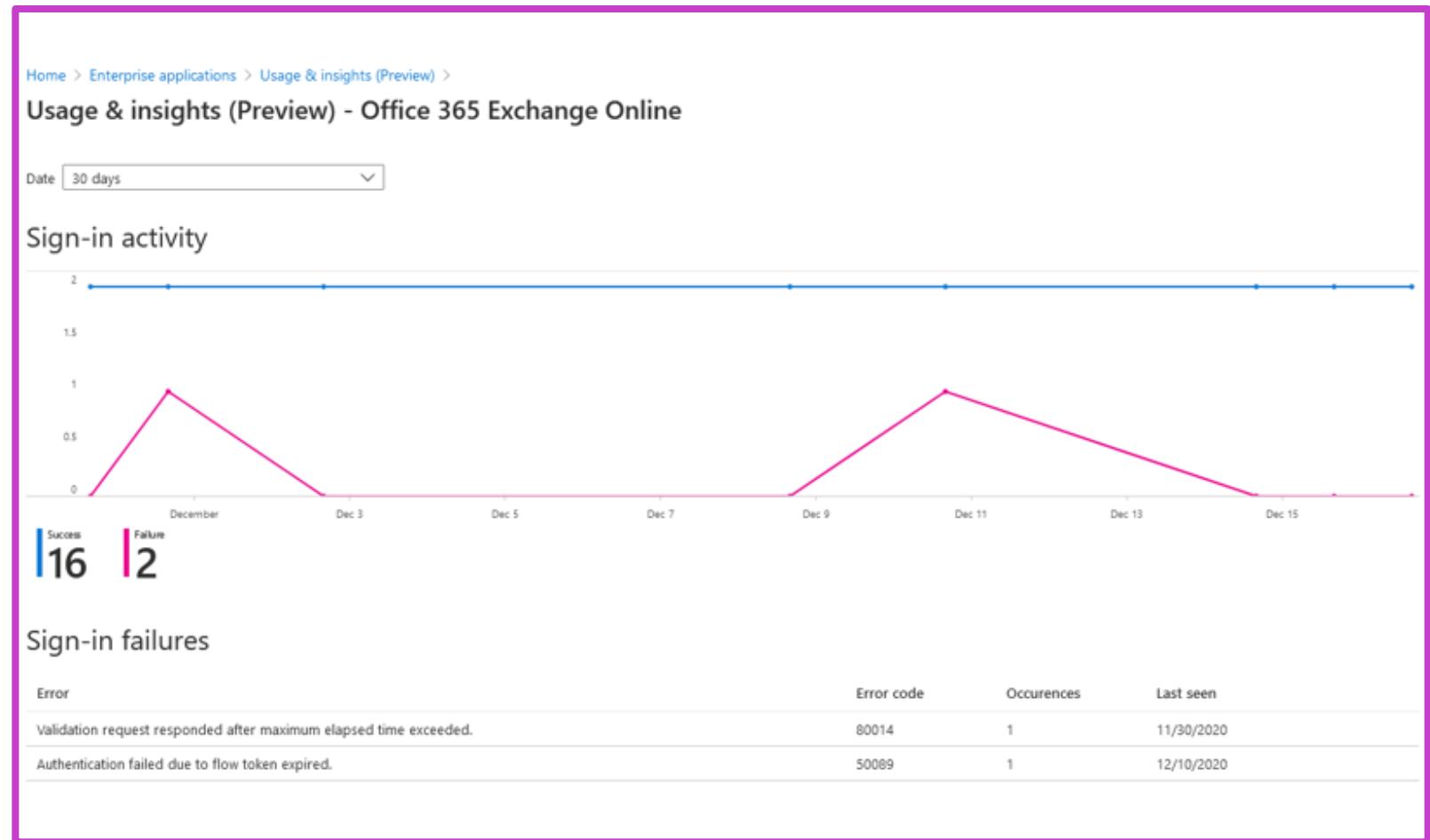


Usage report

Usage and insights report:

Shows the number of sign-in attempts and the success rate.

Clicking **Load more** at the bottom of the list allows you to view additional applications on the page. You can select the date range to view all applications that have been used within the range.



Monitor your security posture with Identity Secure Score

What's Identity Secure Score in Microsoft Entra ID?

Security | Identity Secure Score

Search | Learn more | Got feedback?

Getting started | Diagnose and solve problems

A new Secure Score experience is available, check it out here.

Microsoft Secure Score for Identity is a representation of your organization's security posture and your opportunity to improve it. [Learn more](#).

Secure Score for Identity

88.60%

Last updated 5/5/2025, 5:00:00 PM [View your Microsoft Secure Score](#).

Comparison

Organization	Score (%)
Woodgrove	88.60%
Typical 1001-10000 person company	52.02%

Score history

Score history chart showing the trend of the secure score over the last 7 days. The score has been increasing from approximately 88.60% on April 29 to a peak of about 94% on May 3, before starting to decline towards 90% by May 5.

Date	Score (%)
April 29	88.60%
May 1	91.00%
May 3	94.00%
May 5	90.00%

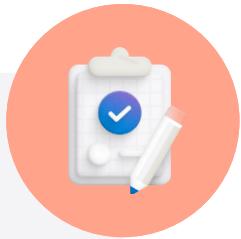
Improvement actions

Name ↑↓	Score Impact ↑↓	User Impact ↑↓	Implementation Cost ↑↓
Stop clear text credentials exposure	1.83%	Low	Low
Remove dormant accounts from sensitive groups	1.83%	Low	Low
Modify unsecure Kerberos delegations to prevent imp...	1.83%	Low	Low
Set a honeypot account	0.37%	Low	Low
Reduce lateral movement path risk to sensitive entities	1.83%	Low	Low
Disable Print spooler service on domain controllers	1.83%	Low	Low

Using Identity Secure Score

How are controls scored?	How should I interpret my score?
<p>Controls can be scored in two ways. Some are scored in a binary fashion; you get 100% of the score if you have the feature or setting configured based on our recommendation. Other scores are calculated as a percentage of the total configuration. For example, if the improvement recommendation states you'll get a maximum of 10.71% if you protect all your users with MFA and you only have 5 of 100 total users protected, you would be given a partial score around 0.53% ($5 \text{ protected}/100 \text{ total} * 10.71\% \text{ maximum} = 0.53\% \text{ partial score}$).</p>	<p>Your score improves for configuring recommended security features or performing security-related tasks (such as reading reports). Some actions are scored for partial completion, such as enabling MFA for your users. Your identity secure score is directly representative of the Microsoft security services you use. Remember that security must be balanced with usability. All security controls have a user impact component. Controls with low user impact should have little to no effect on your users' day-to-day operations.</p>

Summary



Entitlement management

- Catalogs
- Access packages
- Assign entitlements
- Manage entitlements using Identity Governance

Manage access reviews

- Design an access review plan
- Access reviews for groups and apps
- Monitor access review findings
- Remediate and automate access review issues

Privileged access management

- Define privileged access strategy
- Configure PIM for roles and resources
- Audit and manage PIM
- Break-glass accounts

Monitor and maintain Microsoft Entra ID

- Use sign-in logs
- Monitor Azure audit logs
- Configure Log Analytics and Microsoft Sentinel
- Configure alerts

Labs



Lab	Brief description	Length
22. Create and manage catalogs	Create and manage catalogs for use with entitlement management in Microsoft Entra ID.	15 minutes
23. Implement terms of use	Create and manage terms of use for Microsoft Entra ID.	5 minutes
24. Manage external user lifecycle	Manage the lifecycle of external users in Microsoft Entra ID.	5 minutes
25. Access Reviews	Create and access for internal and external users.	15 minutes
26. Enable and Configure PIM	Configure PIM for Microsoft Entra ID and for Azure roles.	5 minutes
27. Kusto Query <i>KQL</i>	Use a simple Kusto query in Microsoft Sentinel to review Microsoft Entra data sources.	15 minutes
28. Identity Secure Score	Monitor and manage your security posture with Identity Secure Score.	10 minutes

Learning path recap

In this learning path, we've done the following:

Established and maintained an identity governance strategy for your solutions.

Implemented privileged identity and access reviews to ensure Zero Trust.

Monitored and investigated the usage of your identity and access solutions.

End of presentation