Microsoft

SC-300

Tag 4

Microsoft Identity and Access Administrator

Guten Morgen!

Microsoft

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
- Monitor and maintain Microsoft Entra ID

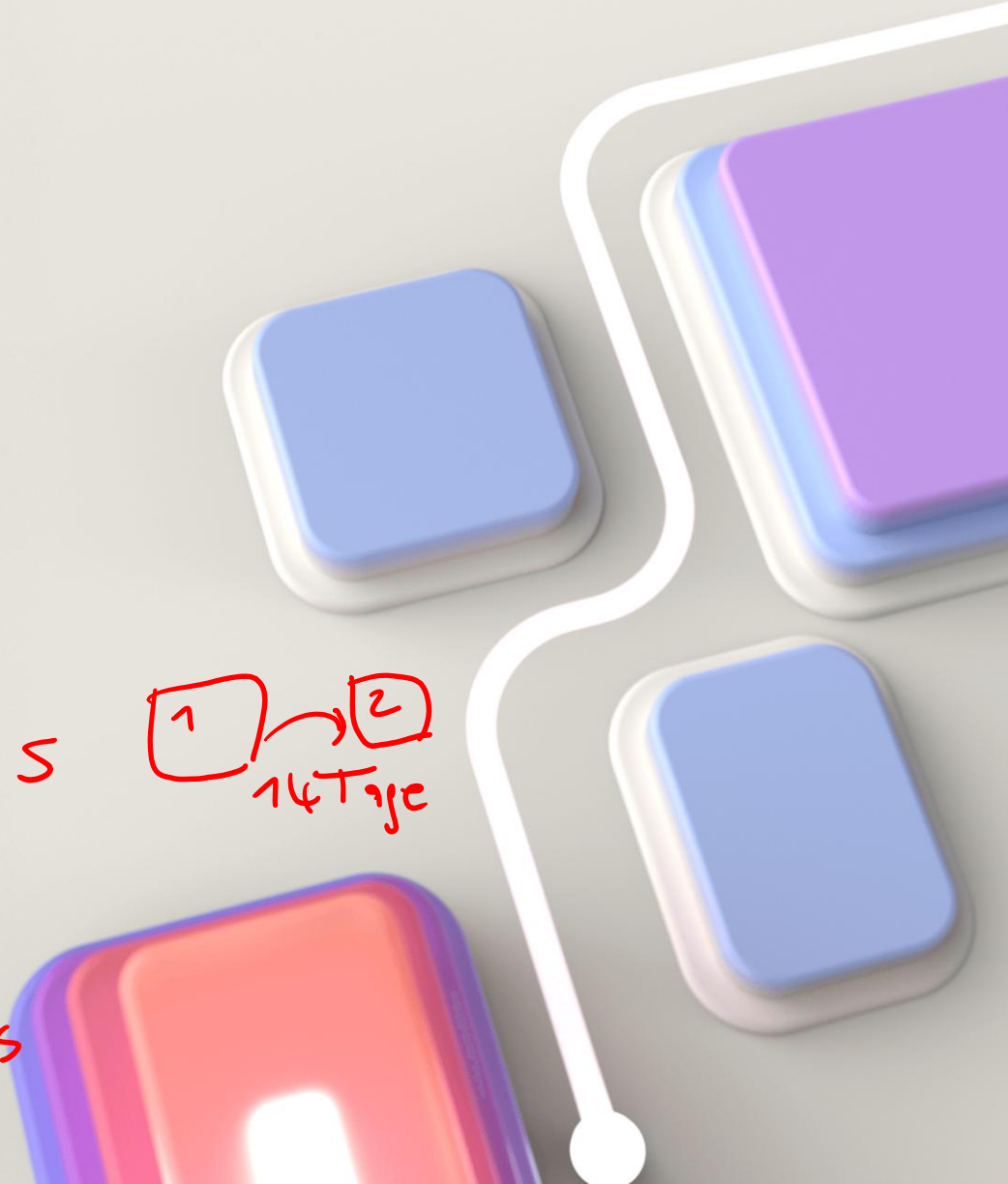
Learning objectives

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



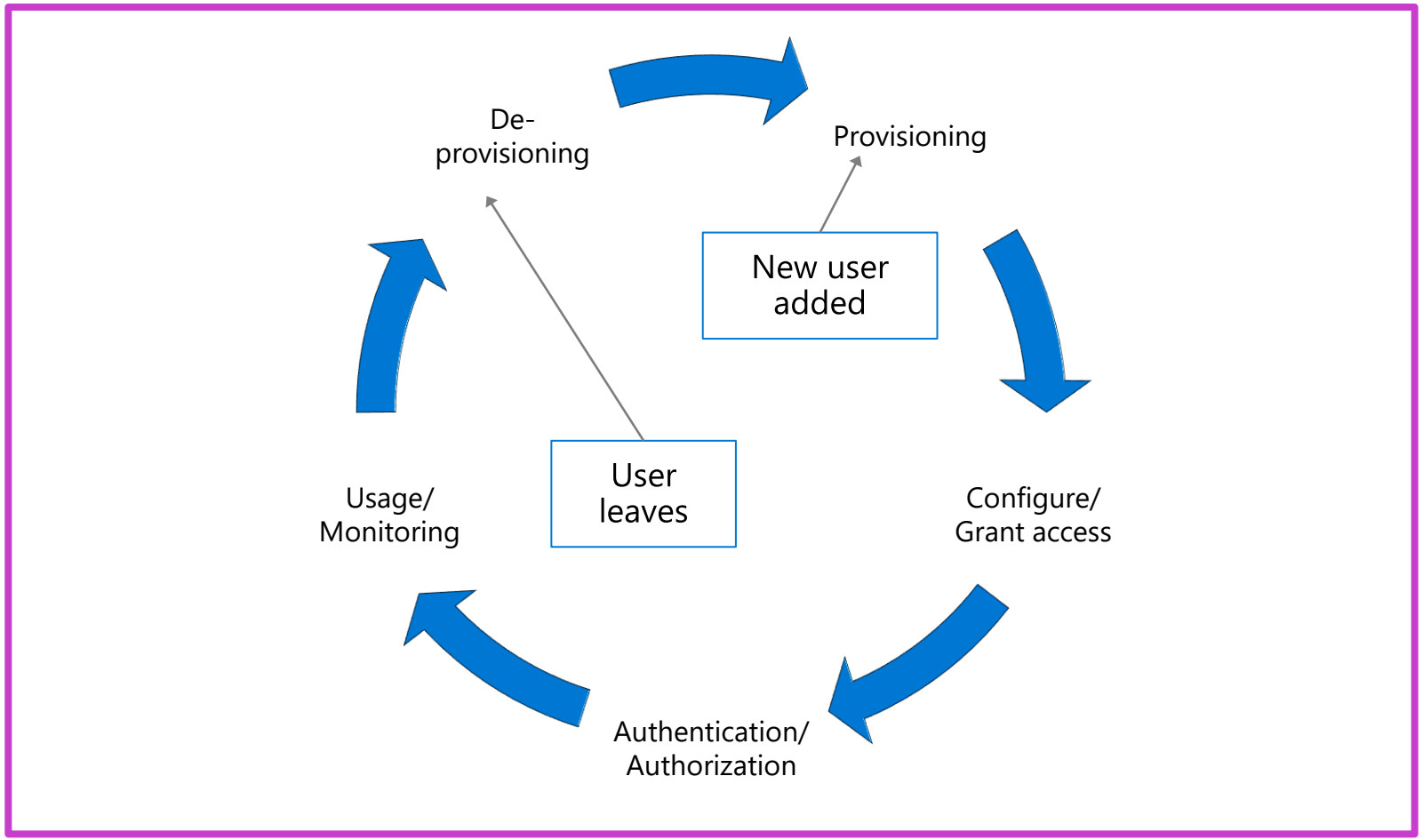
Objectives

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.



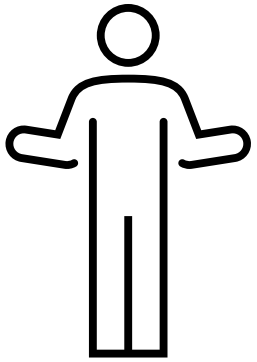
What is entitlement management?

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.

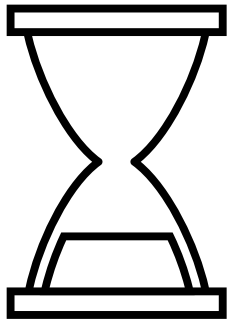
Microsoft Entra entitlement management can help you to more efficiently manage access to groups, applications, and SharePoint Online sites for internal users and for users outside your organization who need access to those resources.

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 lifecycle, such as how users get access, who can approve it, and how long users have access through an assignment. 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 policies. 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.

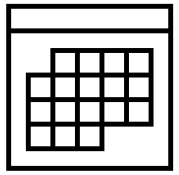
Define access packages

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.

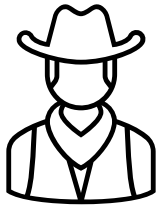
When should I use access packages?

Time-limited access

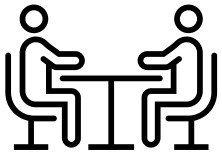


Manager approval or delegated role / identity

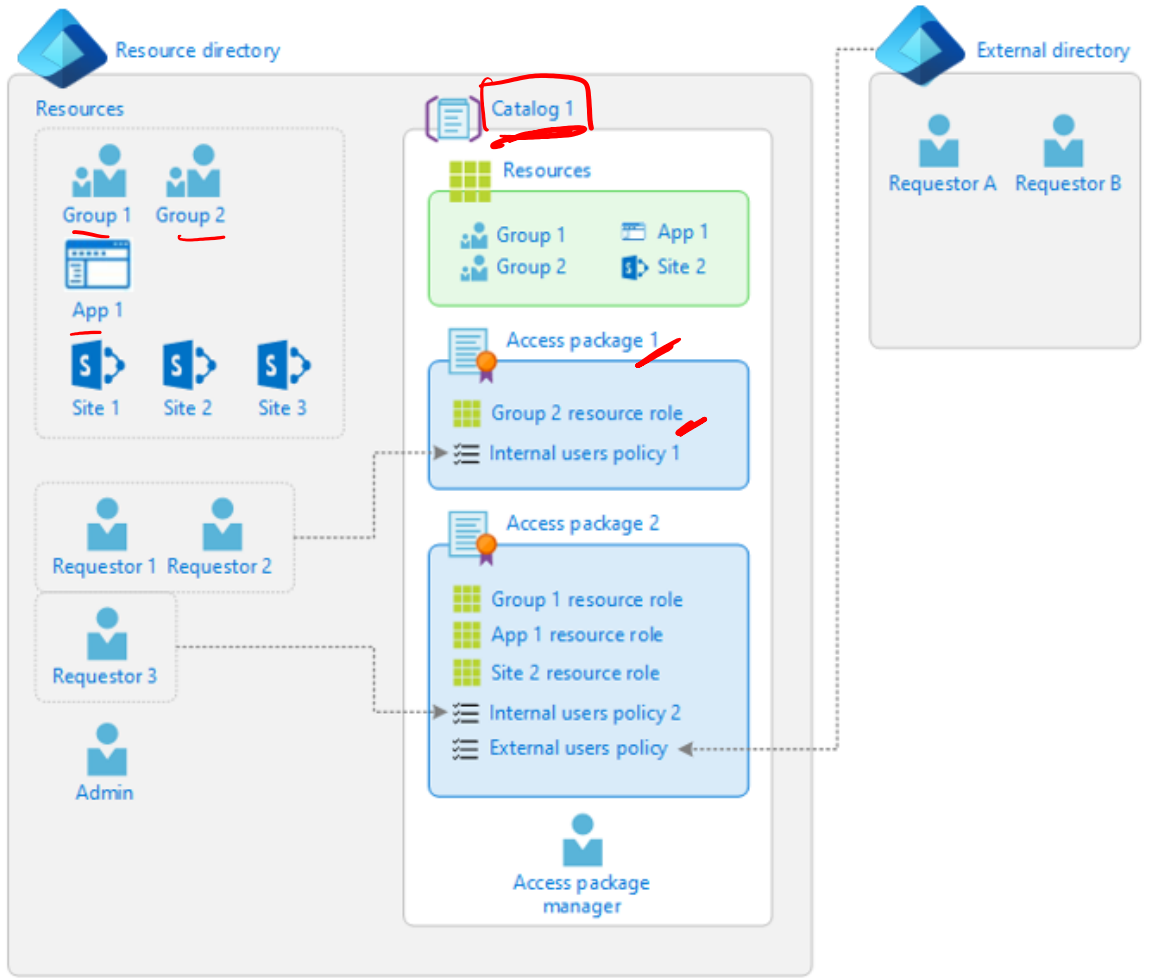
Manage access without IT involvement



Cross-organization collaboration

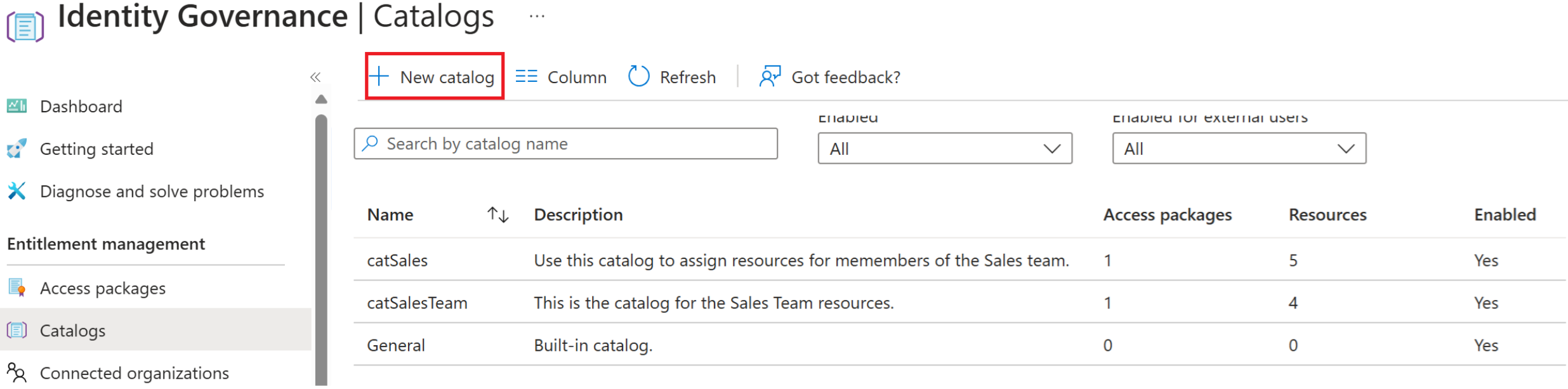


How do I control who gets access?



Define catalogs

What's a catalog?



A catalog is container of:

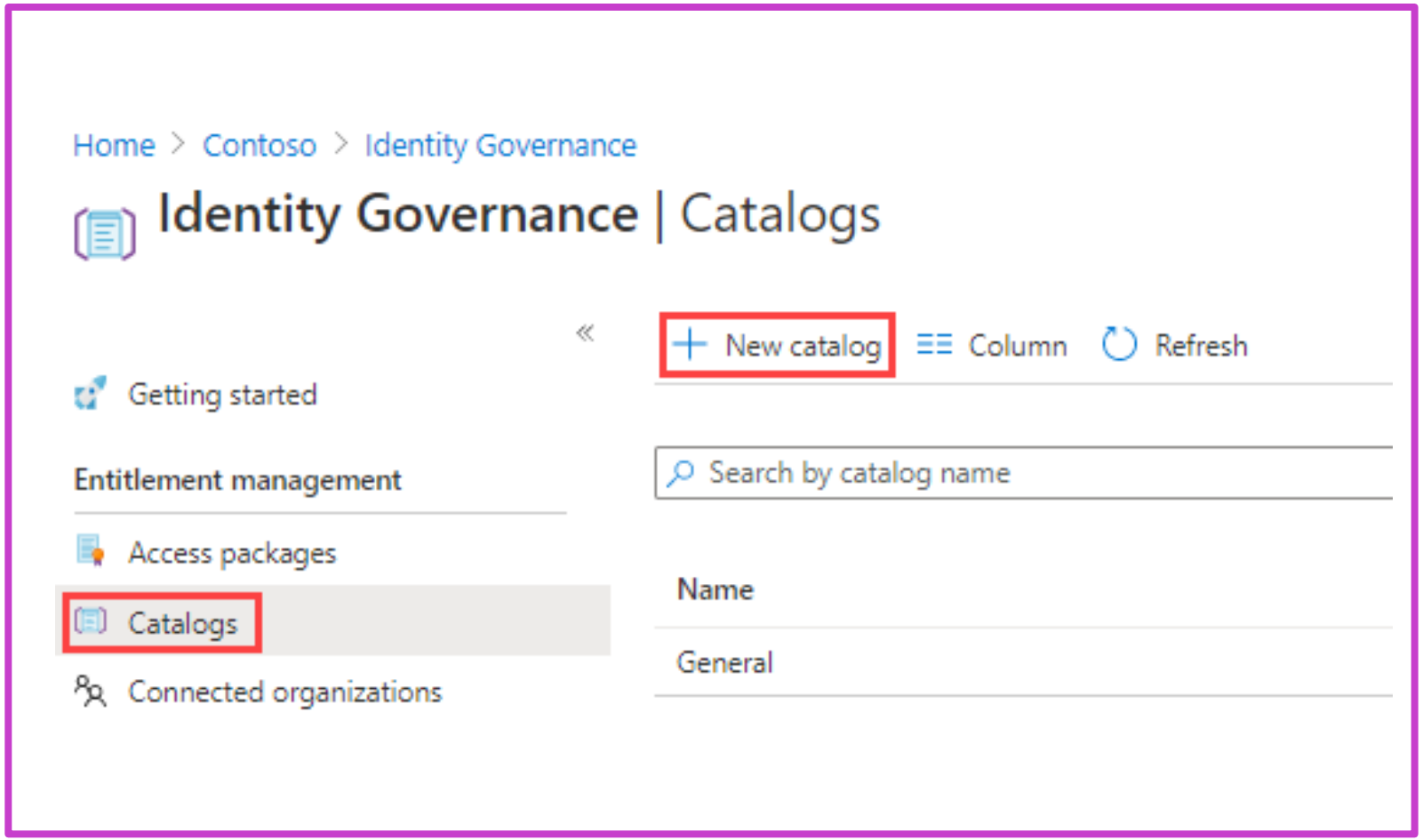
- Resources
- Access packages

It group related resources together.

The catalog creator is the default owner.

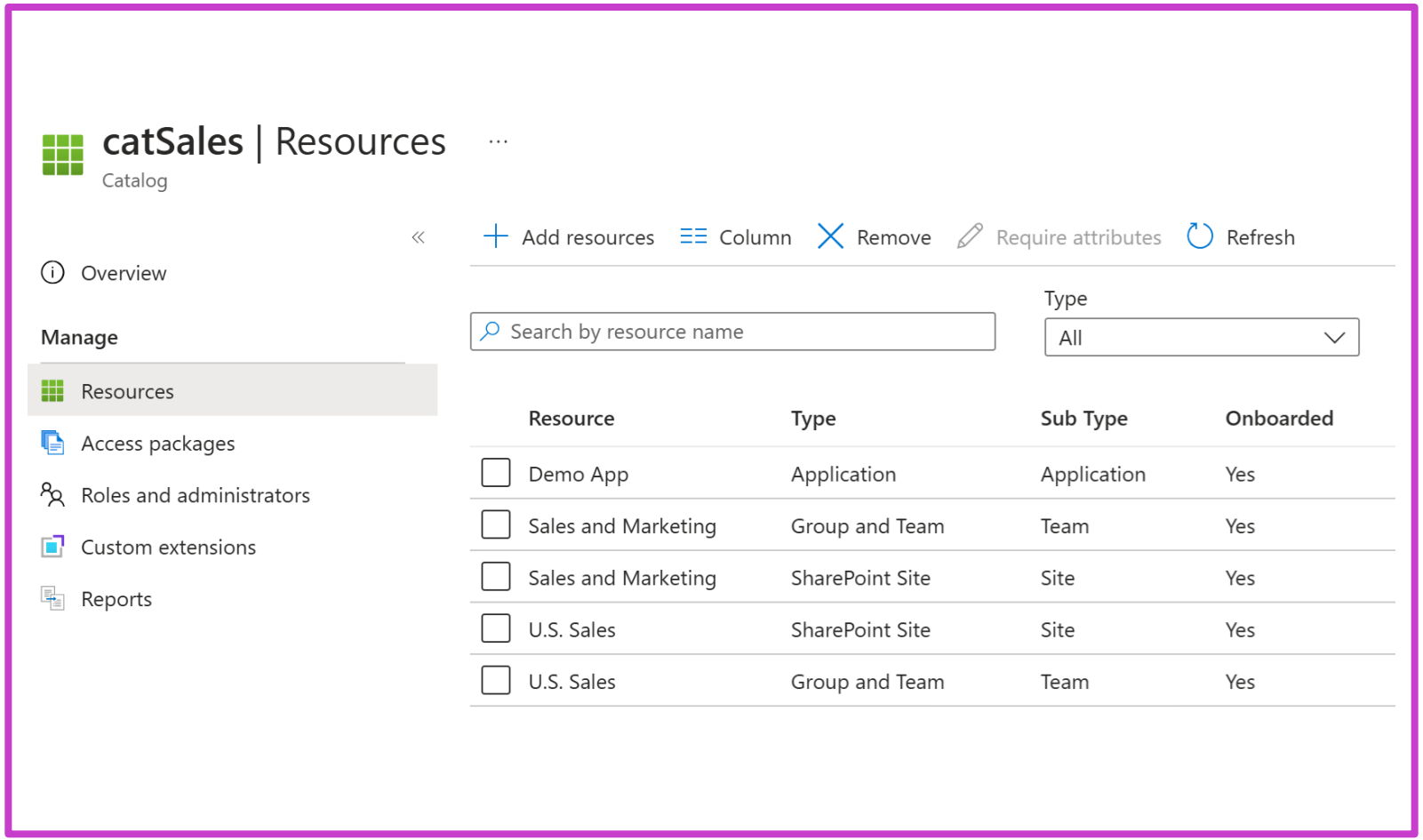
Creating a catalog

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**.



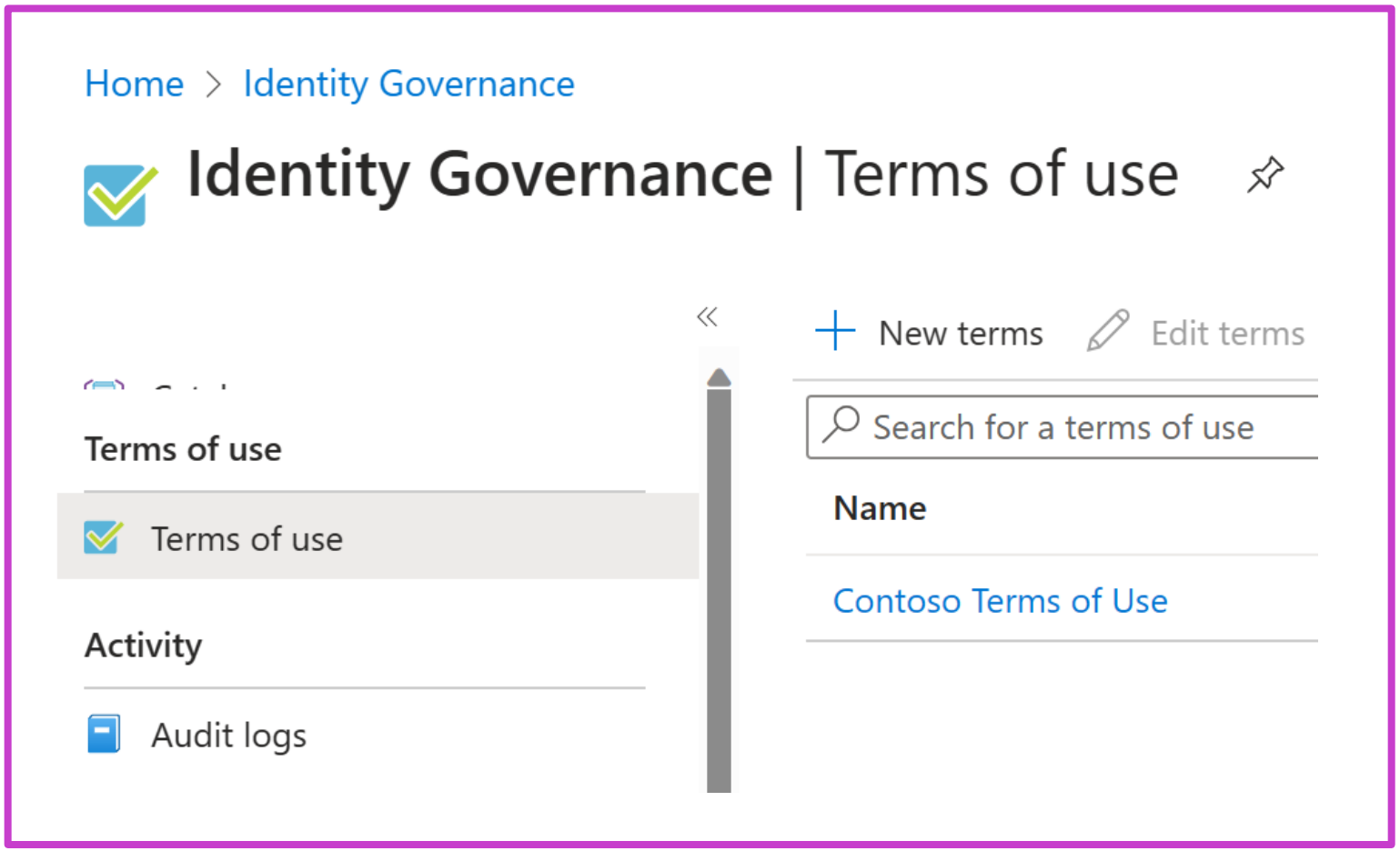
Entitlement owners and process

- 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.

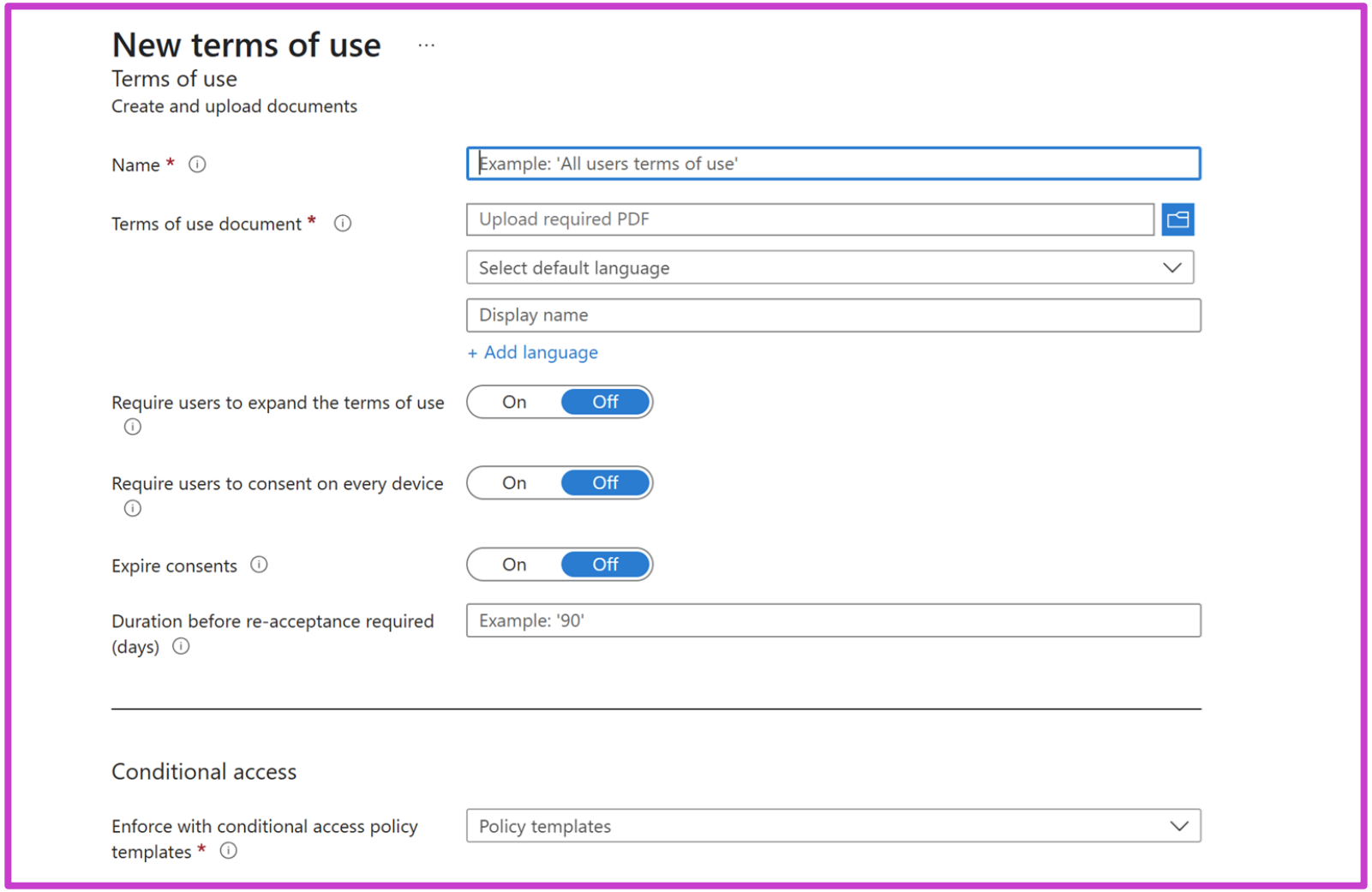
Launch this exercise in GitHub



Implement and manage terms of use

What are terms of use in entitlement management?

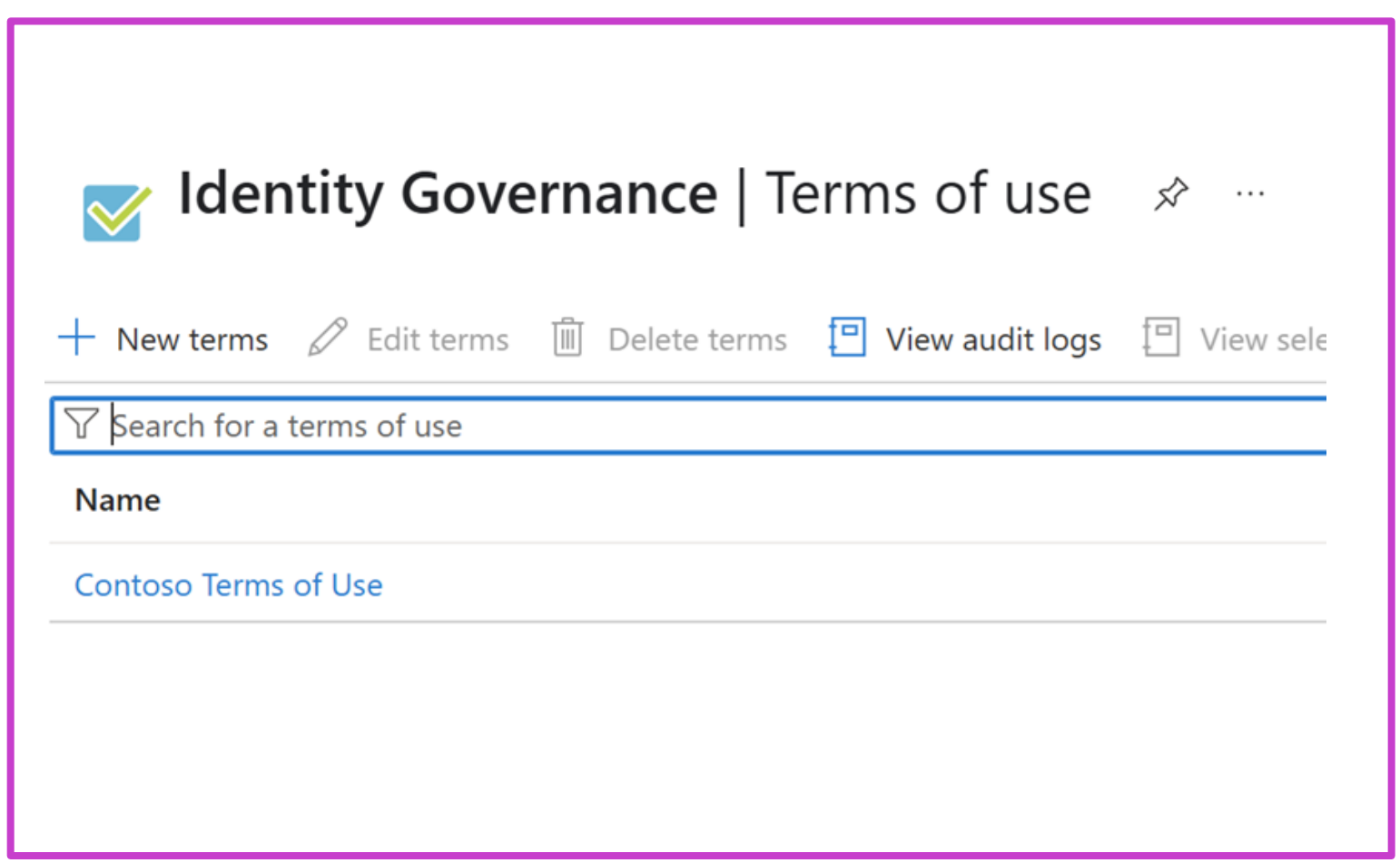
- Terms of use are stored as a PDF
- A PDF can contain any content, including contracts—End-User License Agreement (EULA)
- Can enforce compliance
- 24pt Font is recommended



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]



Manage the lifecycle of external users in Microsoft Entra ID

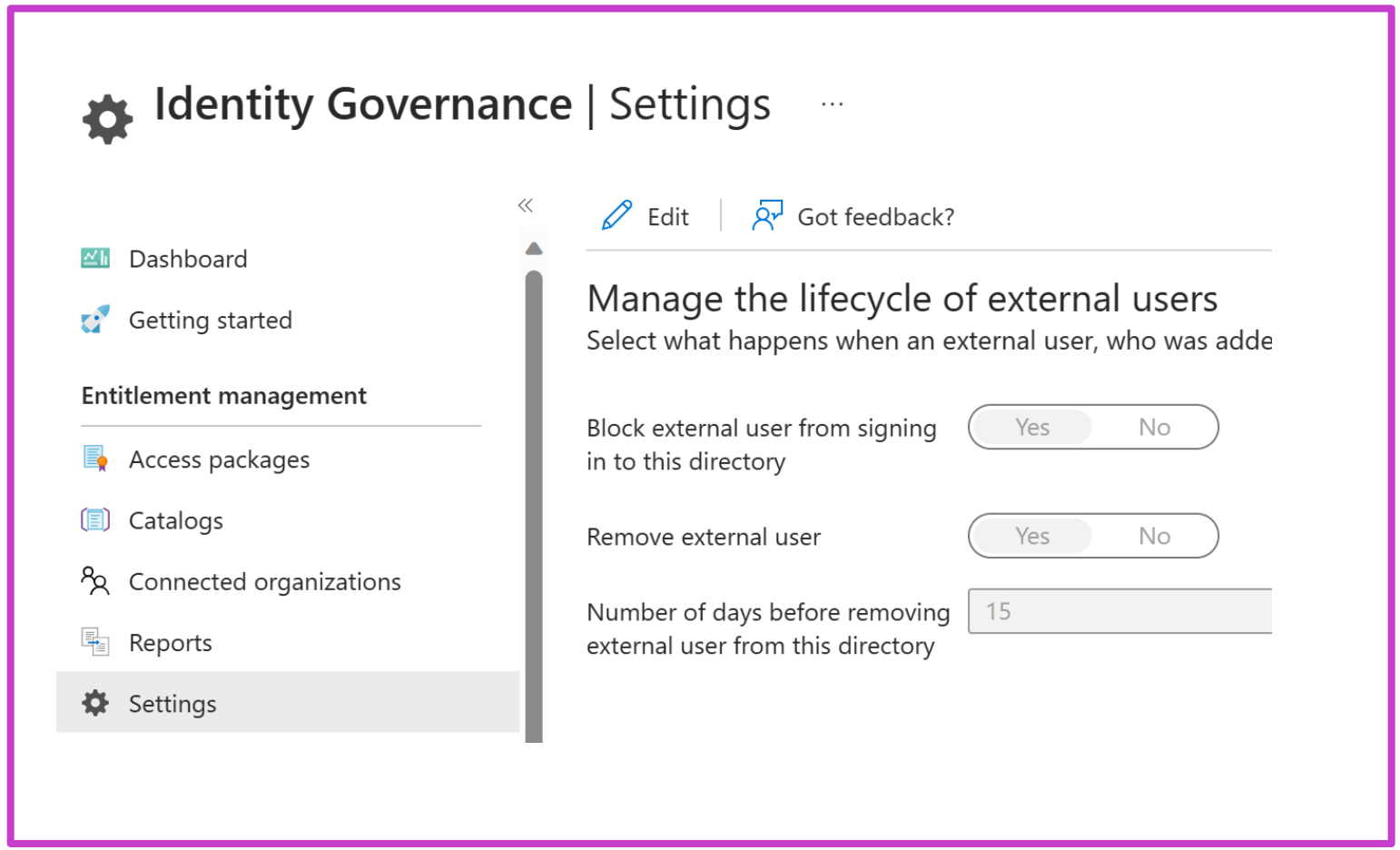
Manage the lifecycle of external users in Microsoft Entra ID Identity Governance settings

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]



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.

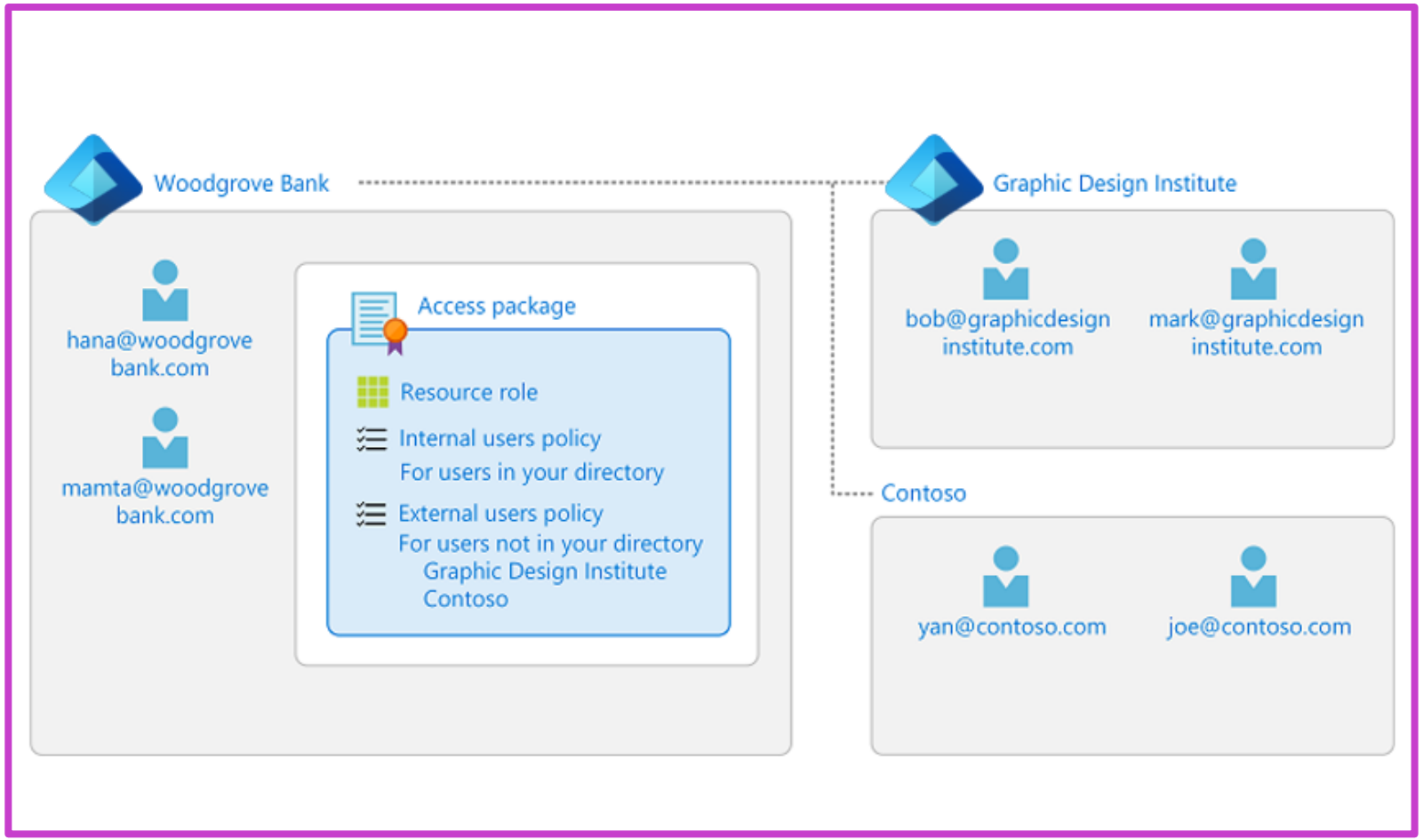
There are three ways that entitlement management lets you specify the users that form a connected organization:

- 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

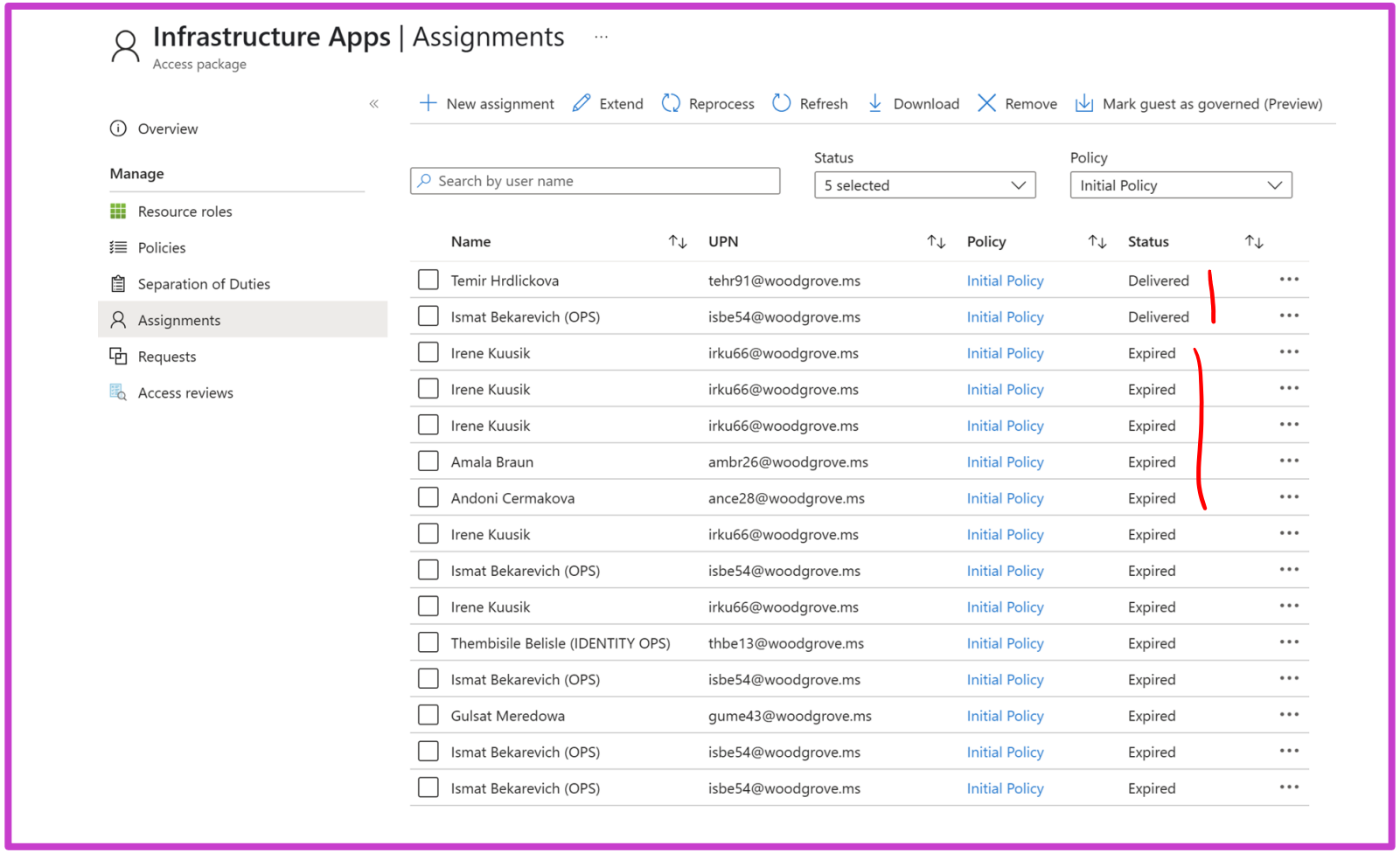
1. In the **Microsoft Entra admin center,** select **Identity Governance,** then **Entitlement Management**.
2. In the menu, select **Connected organizations,** and then select **+ Add connected organization**.
3. Select the **Basics** tab, and then enter a **display name** and **description** for the 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

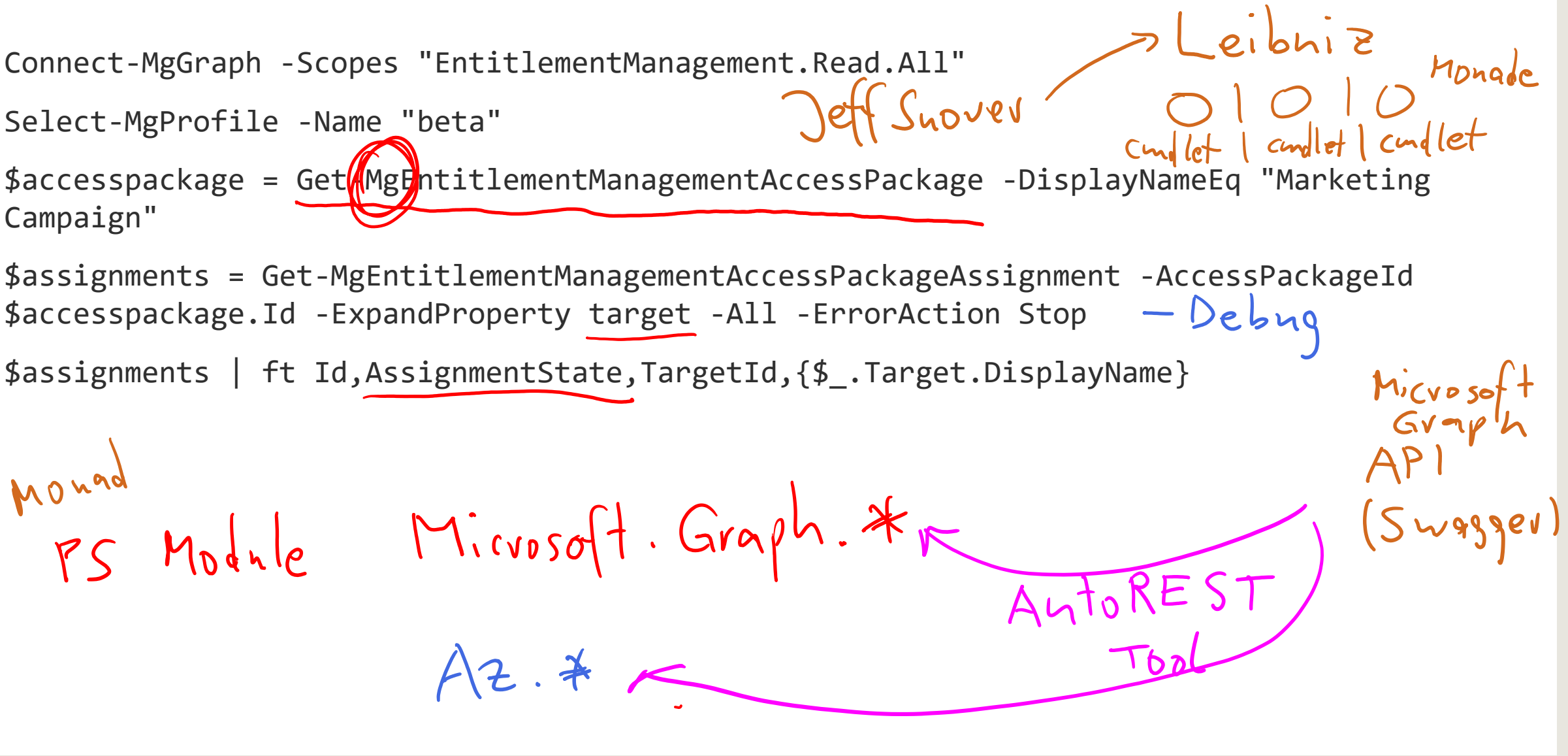
Following the rules of **Zero Trust**, you review your entitlement packages regularly.

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

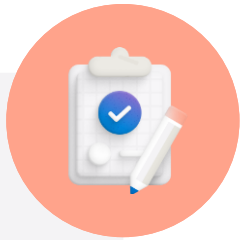


Review the assignments with PowerShell

```
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

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



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 considering 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

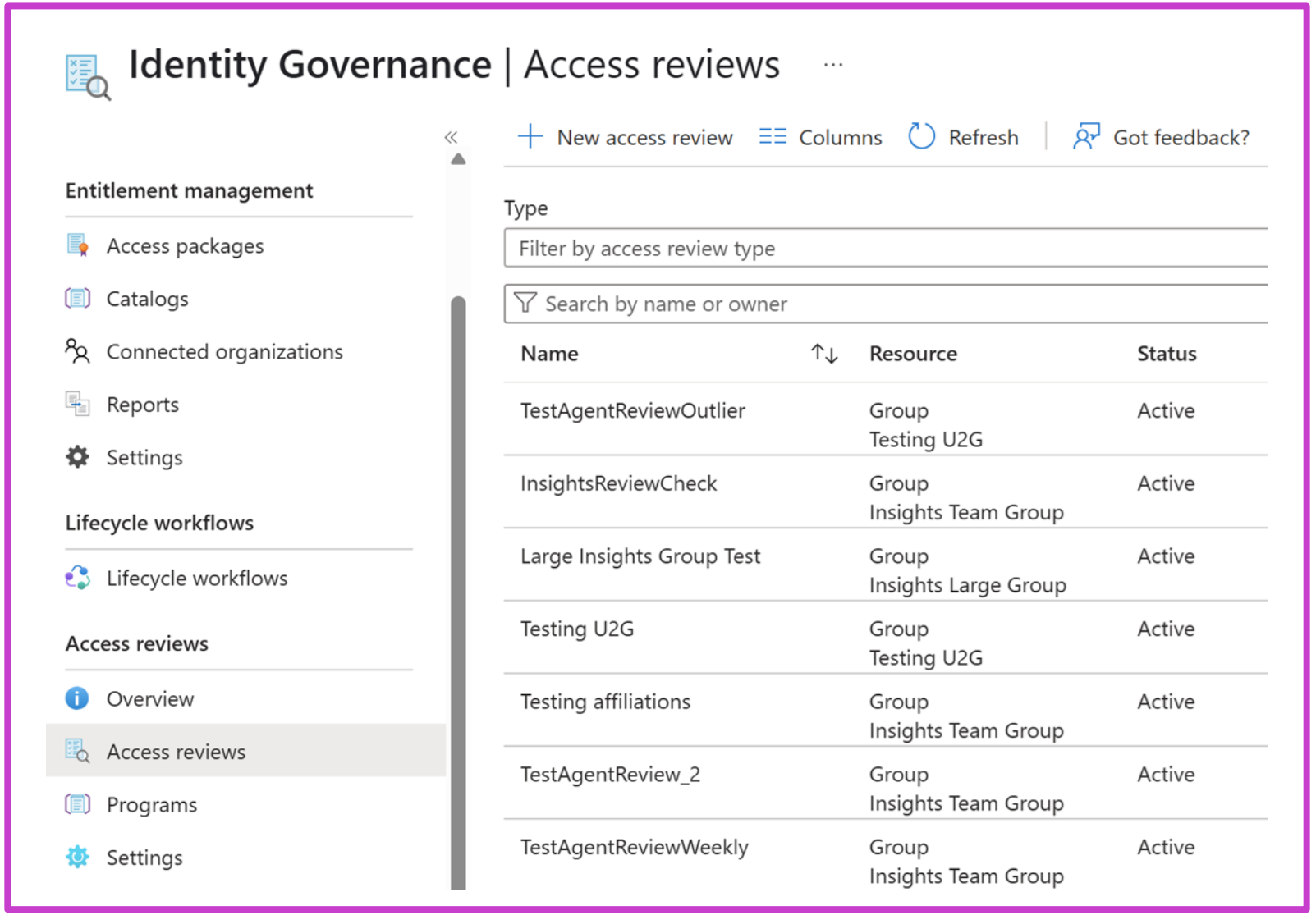
Customize email communication:

- 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

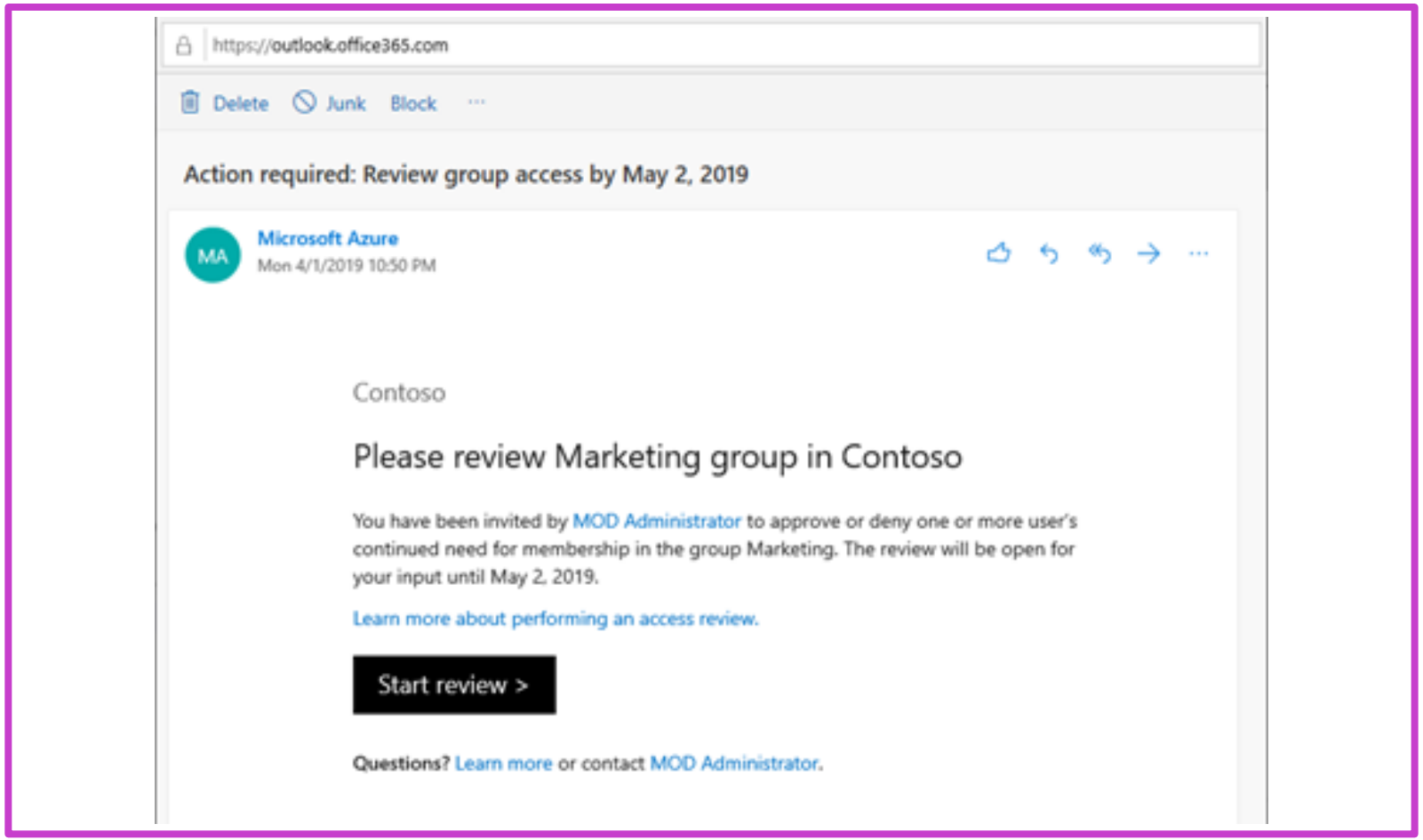
- Prevent stale access assignments by creating access reviews for group members or application access.
- If you need to review access routinely, you can also create recurring access reviews.



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 were'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

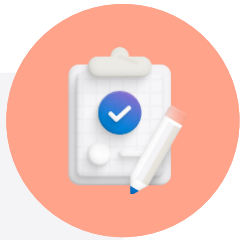
Configure recurring access reviews

- 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.

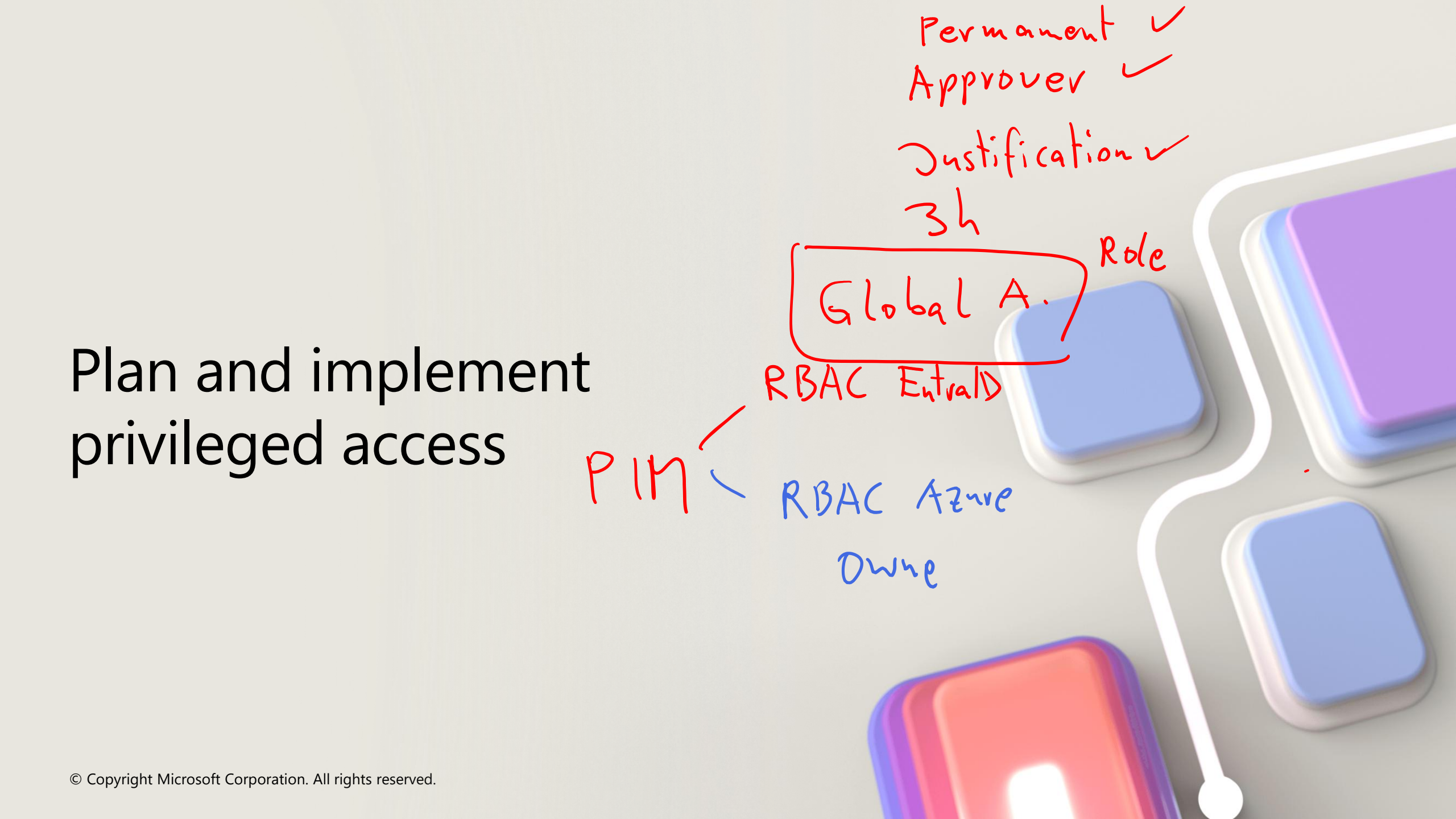
Summary



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



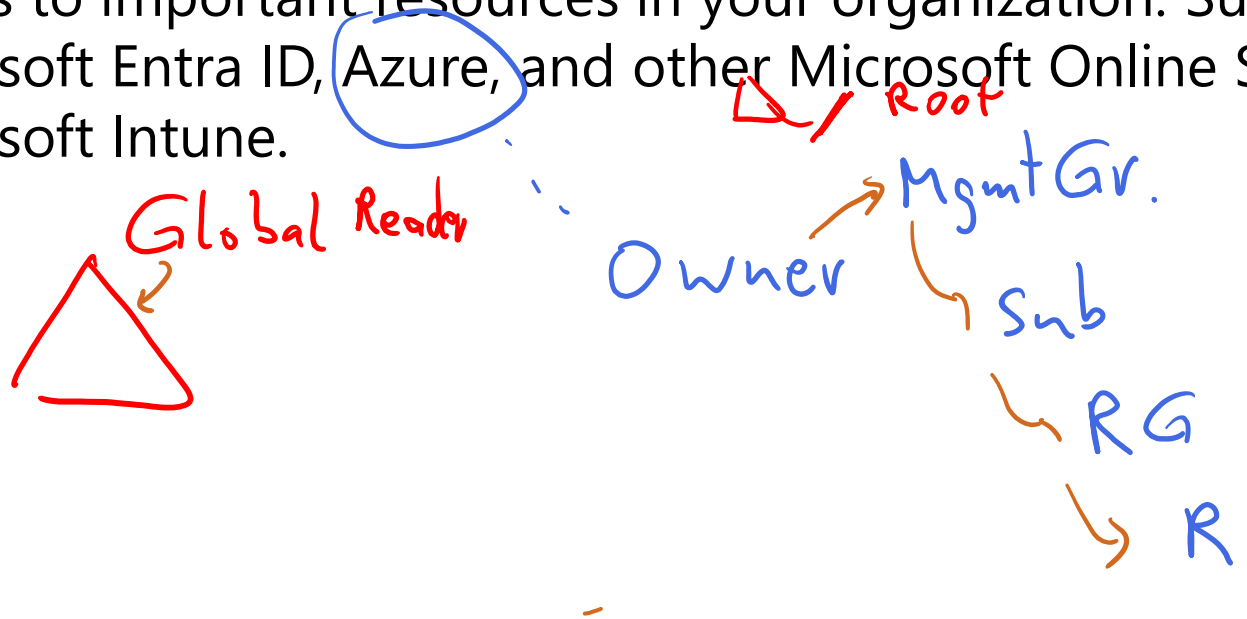
Objectives

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?

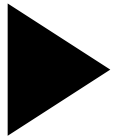
PIM provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources you care about. The key features of PIM include:

- 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

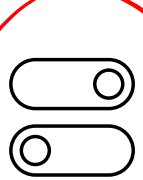


Enforce the principle of least privilege

Decide which roles to protect with PIM

Decide whether to use a group to assign roles

Decide which users should be permanent or eligible

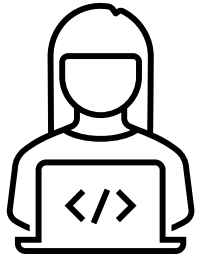


Draft your PIM settings

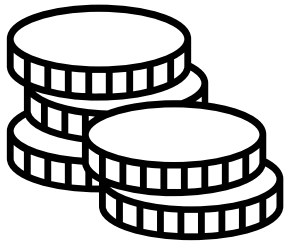
Principle of least privilege

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

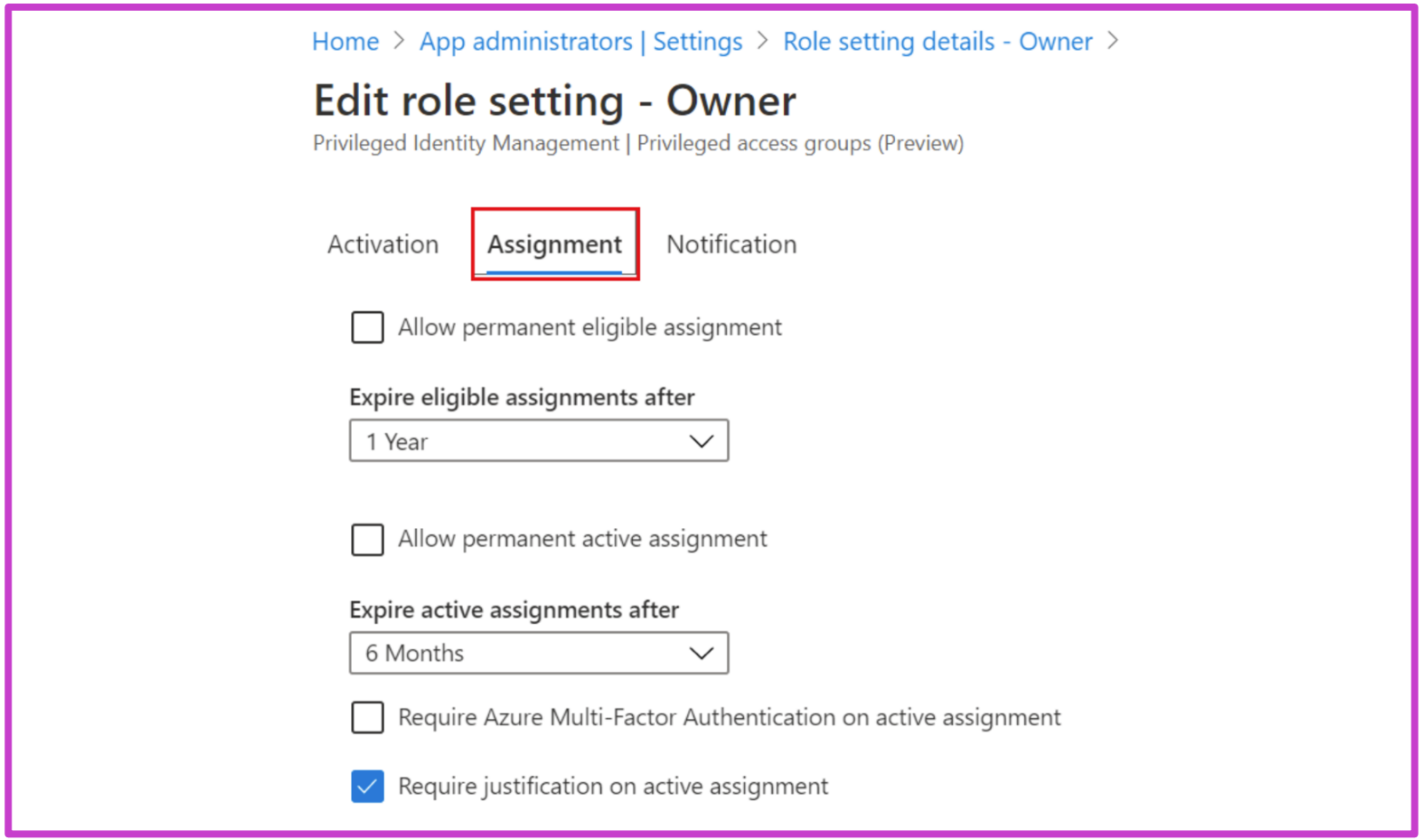
In PIM, you can now assign eligibility for the membership or ownership of privileged access groups. You can assign Microsoft Entra built-in roles to cloud groups and use PIM to manage group member and owner eligibility and activation. With the privileged access groups preview, you can give workload-specific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



Configure Privileged Identity Management (PIM) for Azure resource roles

Assign Azure resource roles

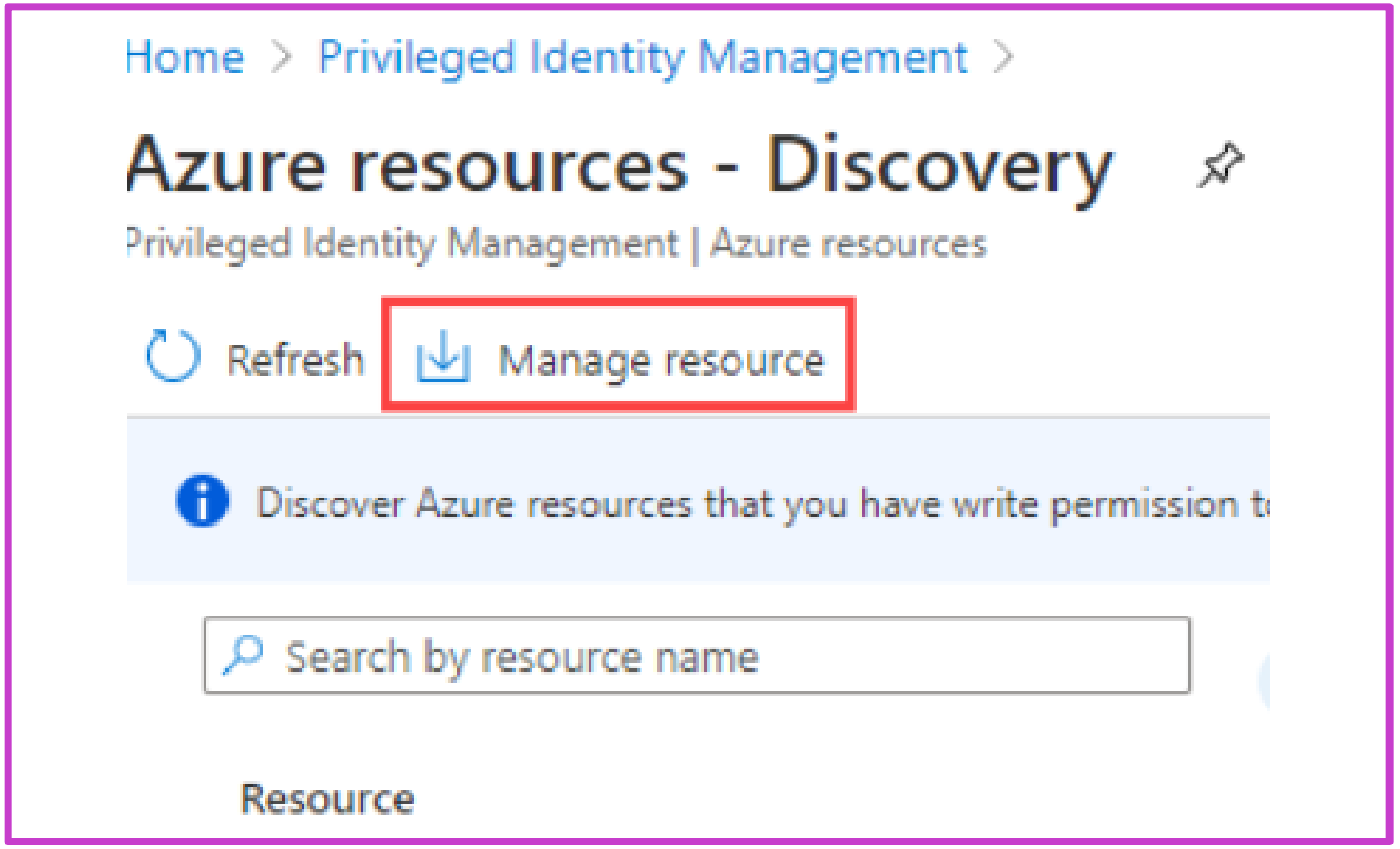
PIM can manage the built-in Azure resource roles, as well as custom roles, including (but not limited to) the following:

- 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.

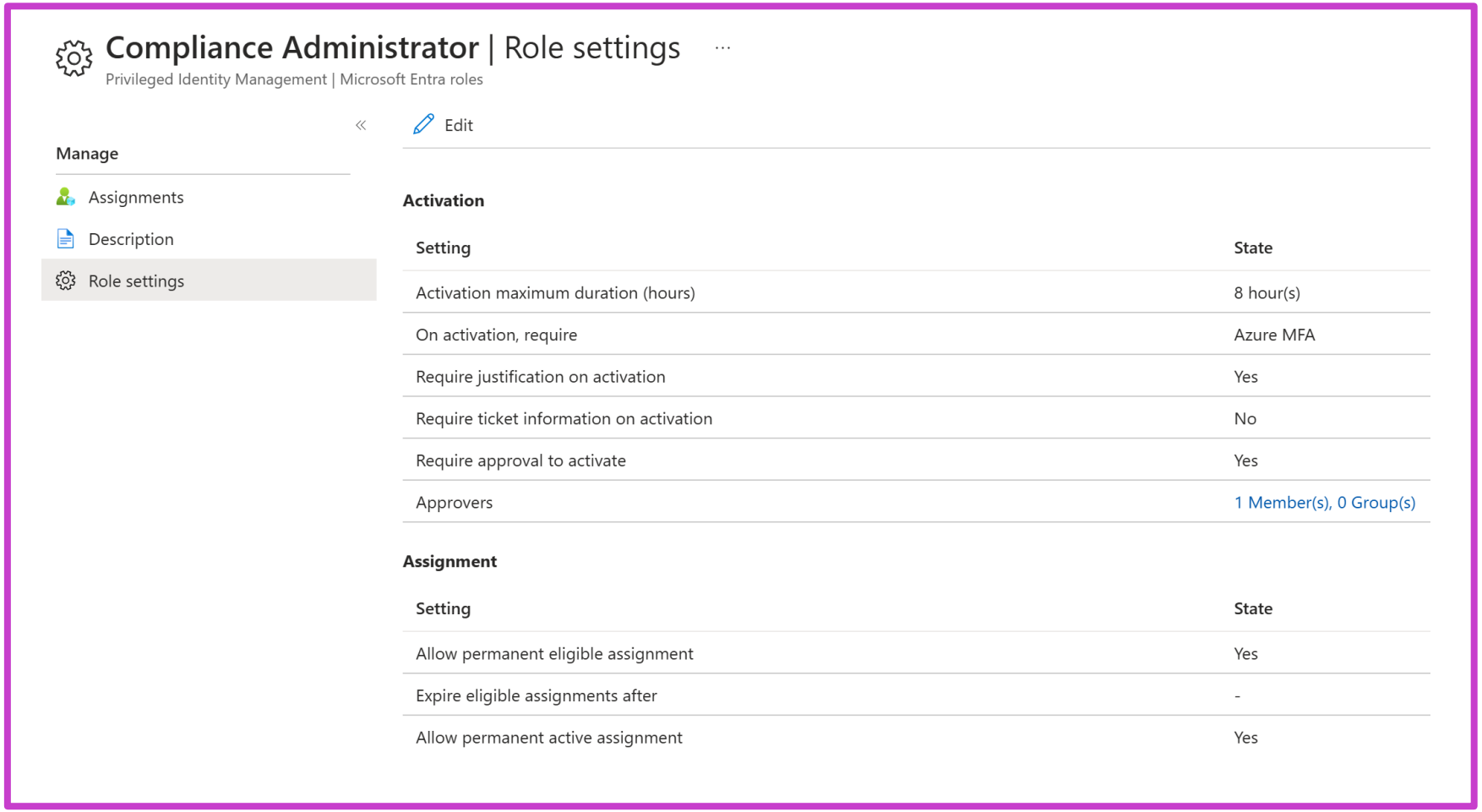
[Launch this exercise in GitHub]



Configure Privileged Identity Management (PIM) for Microsoft Entra roles

Configure PIM for Microsoft Entra roles

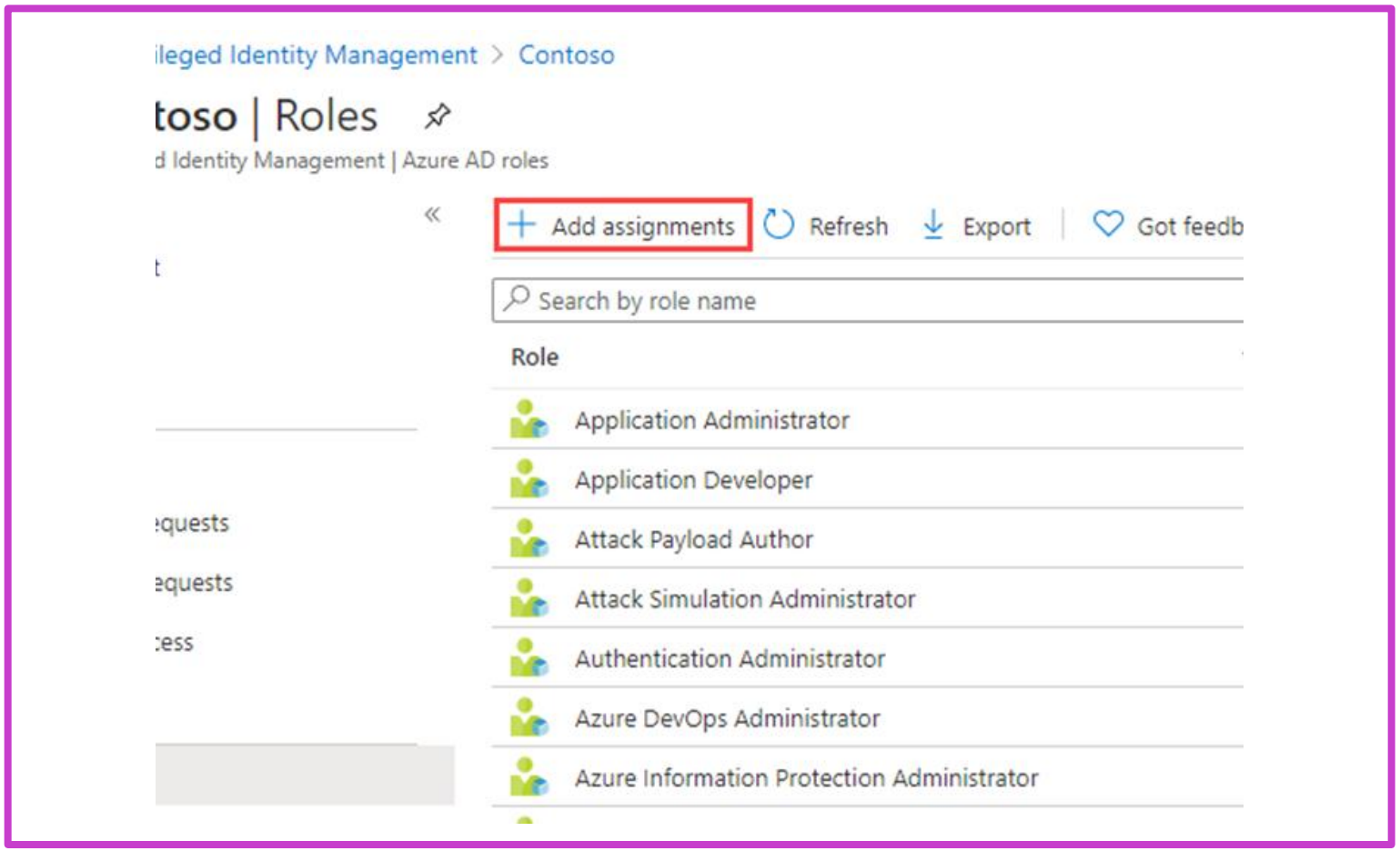
A Privileged Role Administrator can customize PIM in their Microsoft Entra organization, including changing the experience for a user who's activating an eligible role assignment.



Exercise: Configure PIM for Microsoft Entra roles

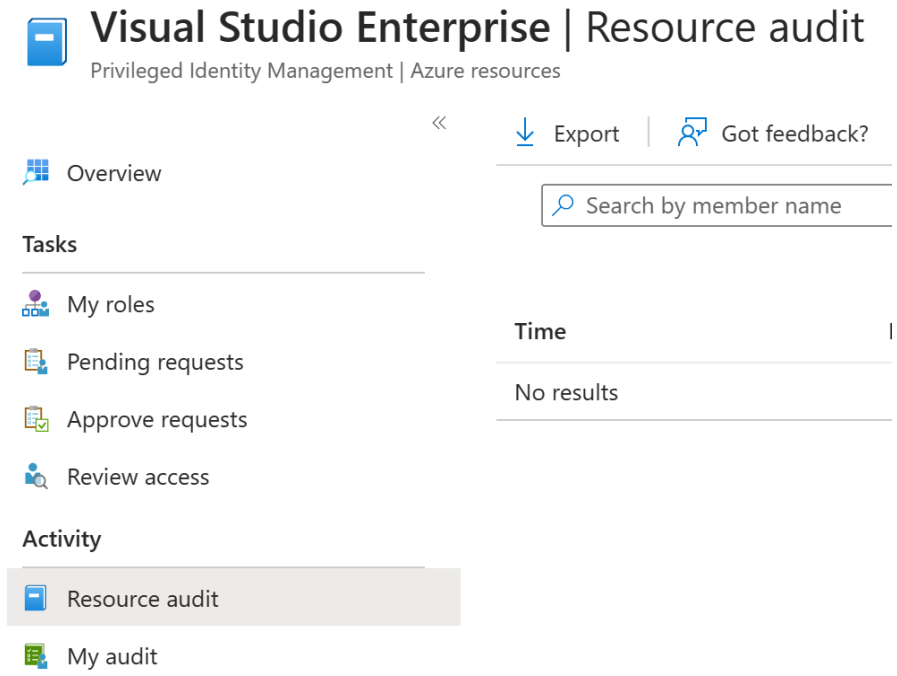
This exercise teaches the student how to configure PIM for Microsoft Entra and for Azure roles.

[Launch this exercise in GitHub]



Analyze Privileged Identity Management (PIM) audit history and reports

Analyze PIM audit history and reports



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:

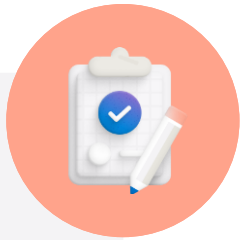
- Define which account to check.
- Ensure the accounts are documented and current.
- Ensure security officers who might need emergency accounts are trained on the process.
- Update the account credentials—in particular, any passwords.
- Validate that the emergency access accounts can sign in and perform 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.

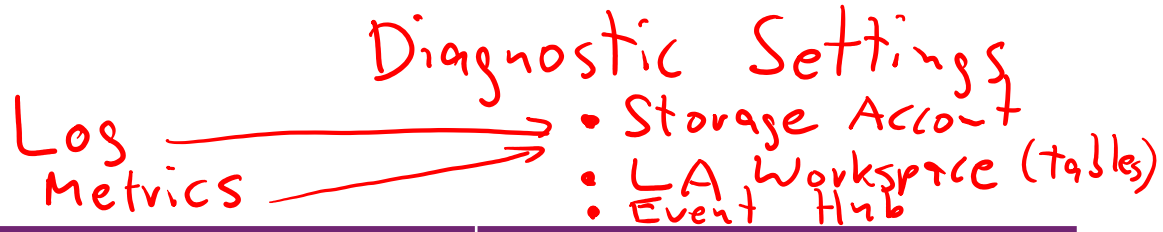
Security

- **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?

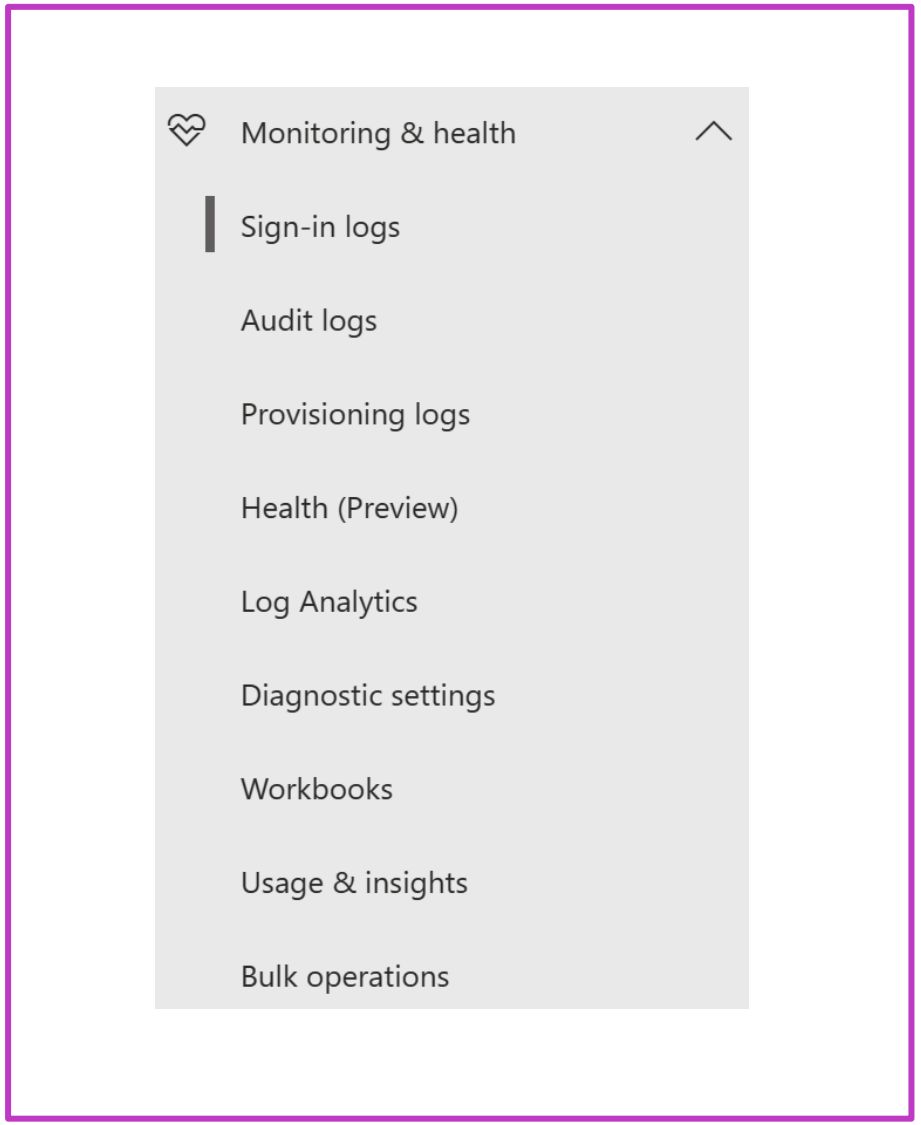


Report	Free Microsoft Entra ID	Microsoft Entra ID P1	Microsoft Entra ID P2
Audit Logs	7 days	30 days	30 days
Sign-ins	7 days	30 days	30 days
Multifactor authentication usage	30 days	30 days	30 days
Microsoft Graph activity logs	N/A	Must be stored in a storage account	Must be stored in a storage account

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.



Download sign-in activities

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

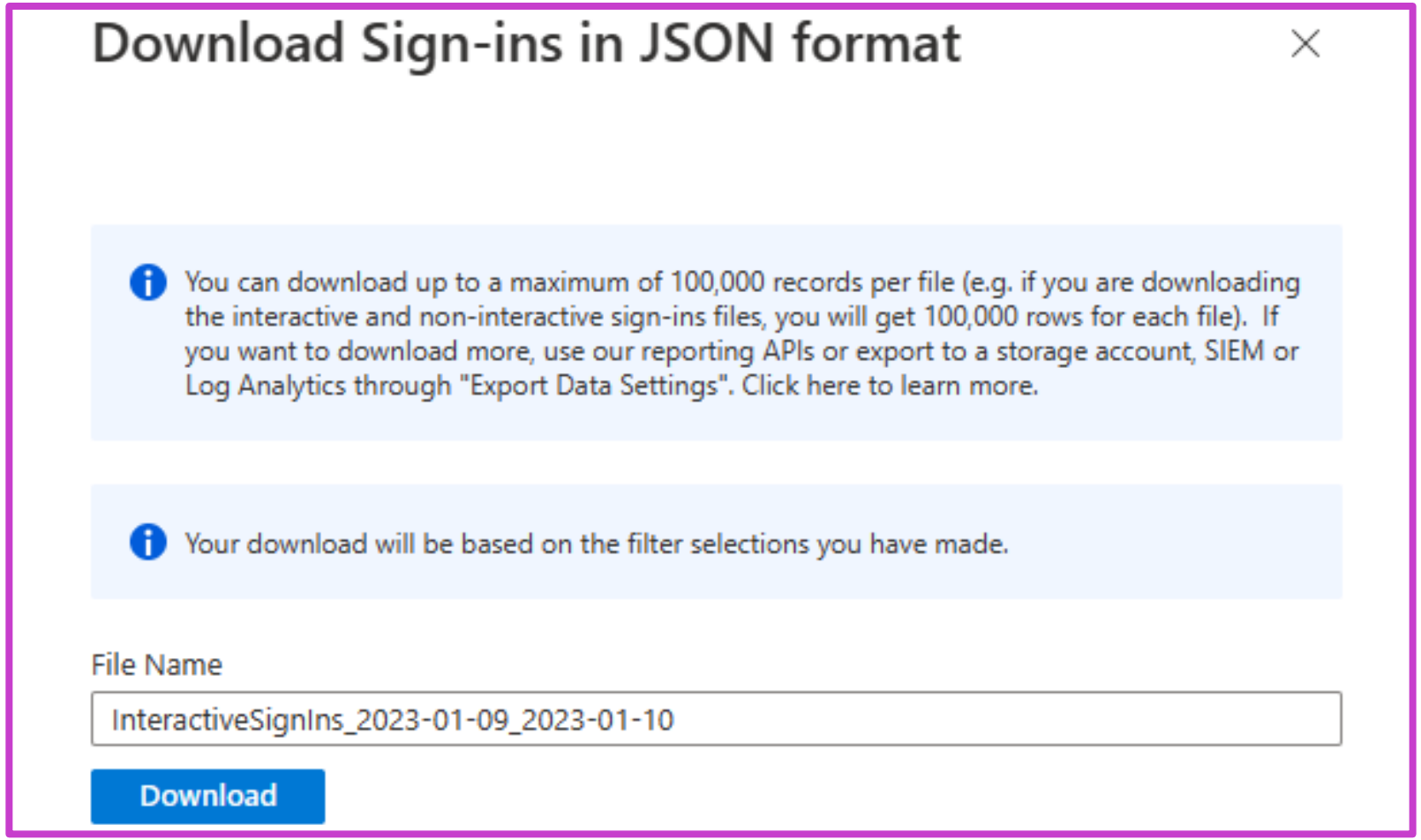
- What's the sign-in pattern of a user?
- How many users have signed in over a week?
- What's the status of these sign-ins?

File formats available:

- CSV or JSON.

Available records:

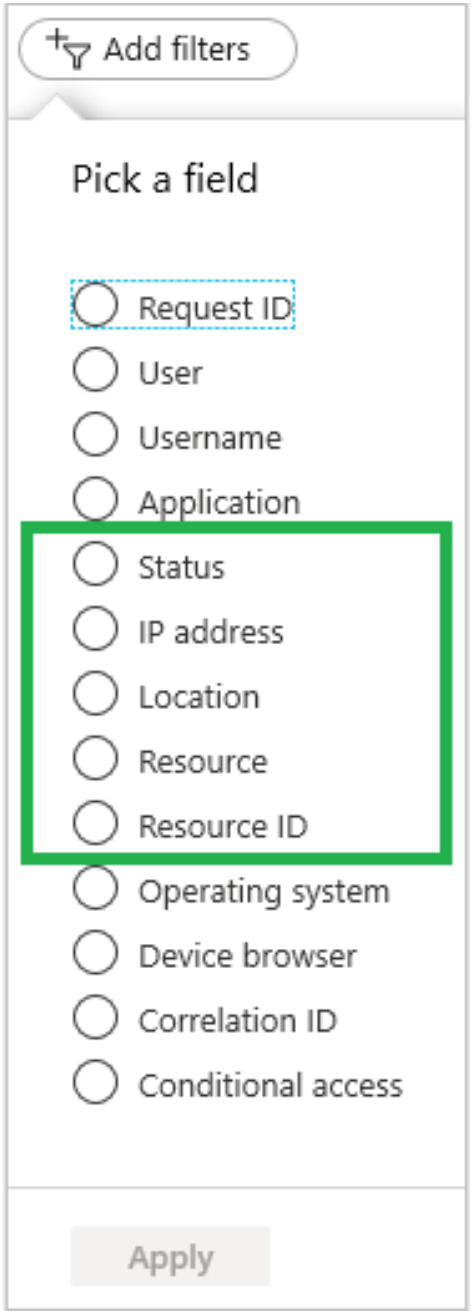
- The most recent 100,000 records.



Filter sign-in activities

Get more targeted data:

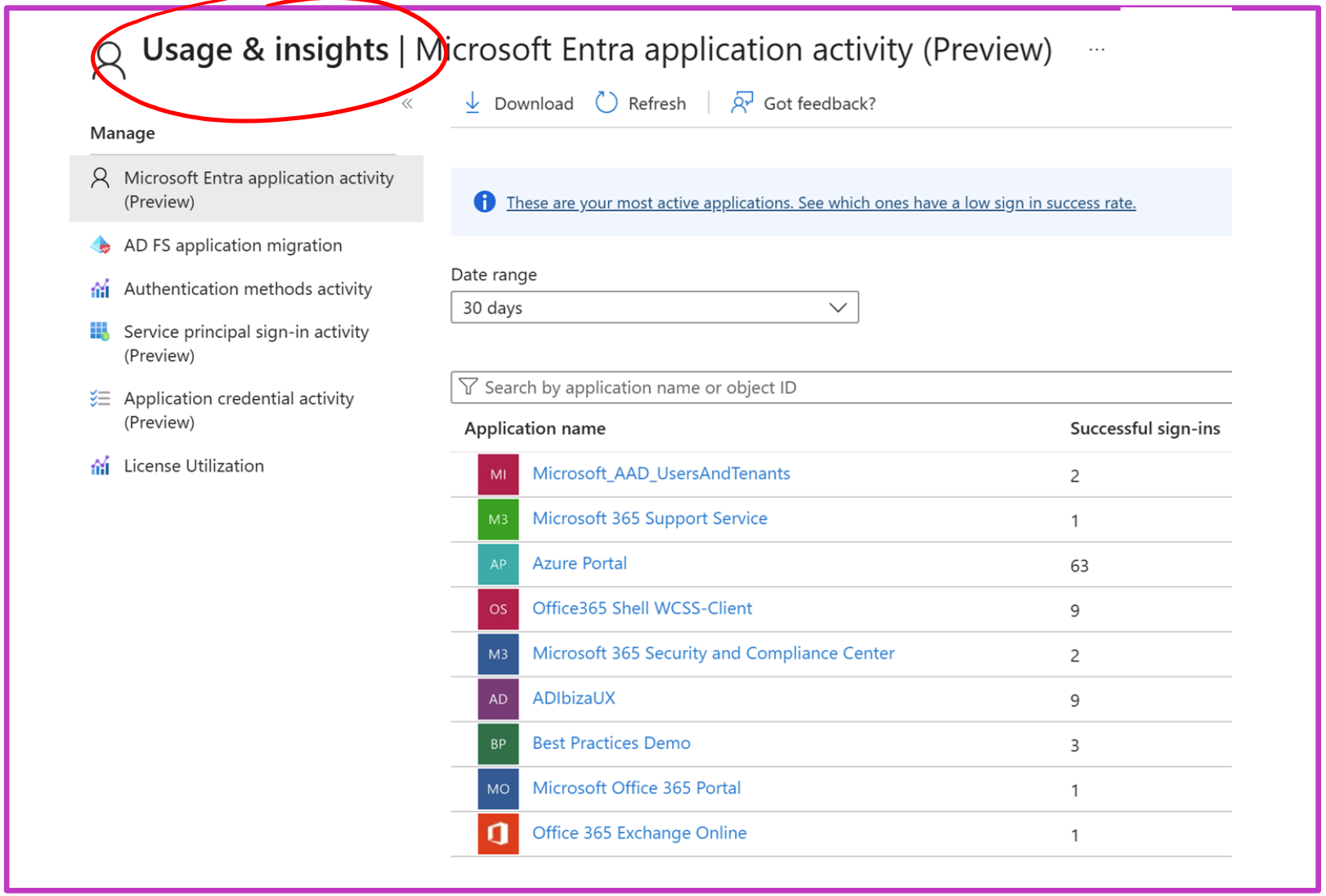
- Filter content specific to your needs.
- Reporting APIs.
- Export data to storage account or SIEM or Log Analytics.



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?



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…

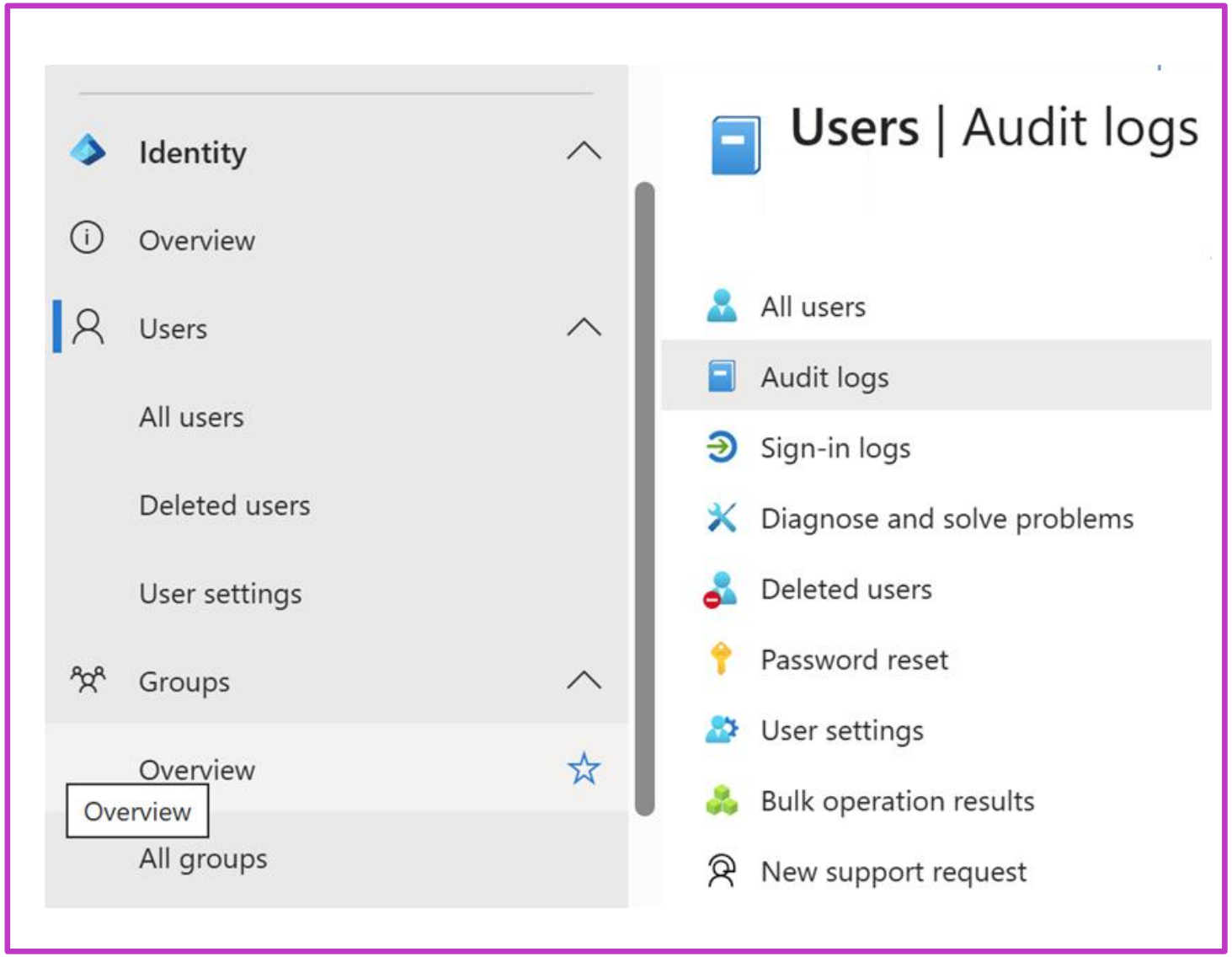
Activity filter

- 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:

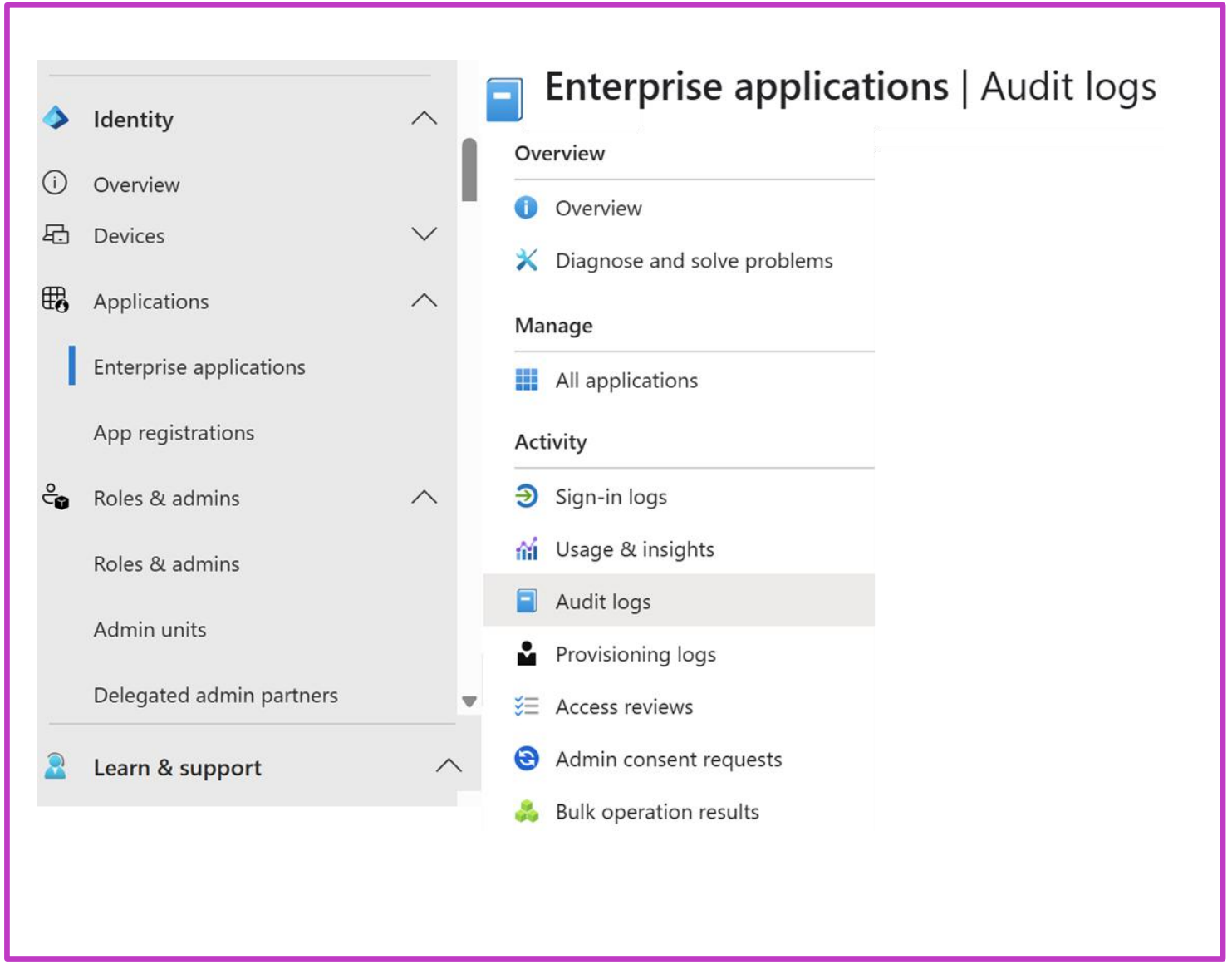
- What types of updates have been applied to users?
- How many users were changed?
- How many passwords were changed?
- What has an administrator done in a directory?
- What groups have been added?
- Are there groups with membership changes?
- Have the owners of a group been changed?
- What licenses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



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?

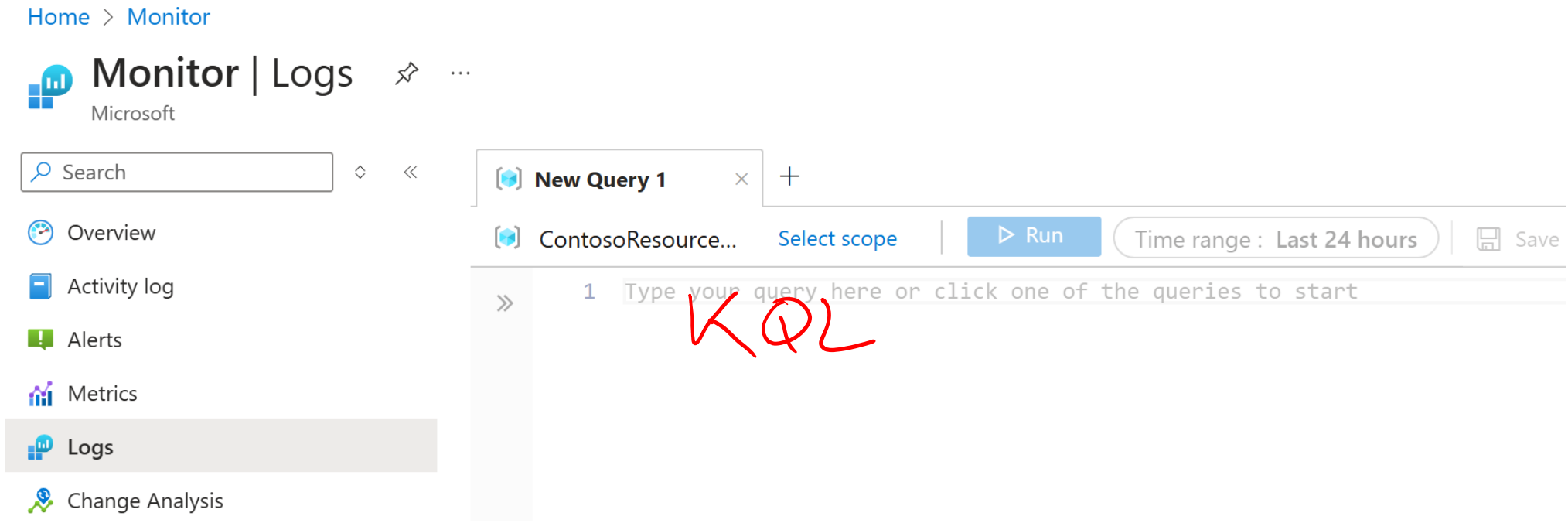


Microsoft 365 activity logs

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?

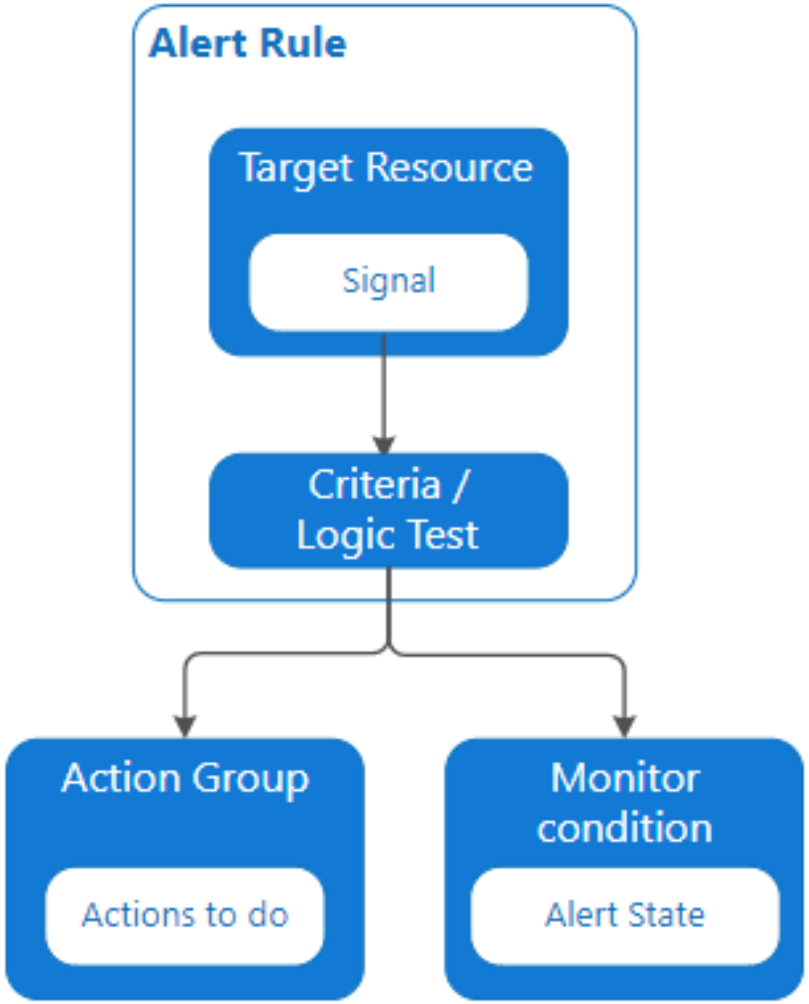


Log Analytics is a tool in the Azure portal used to edit and run log queries from data collected by Azure Monitor Logs and to interactively analyze their results interactively. You can use Log Analytics queries to retrieve records matching criteria, identify trends, analyze patterns, and provide a variety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

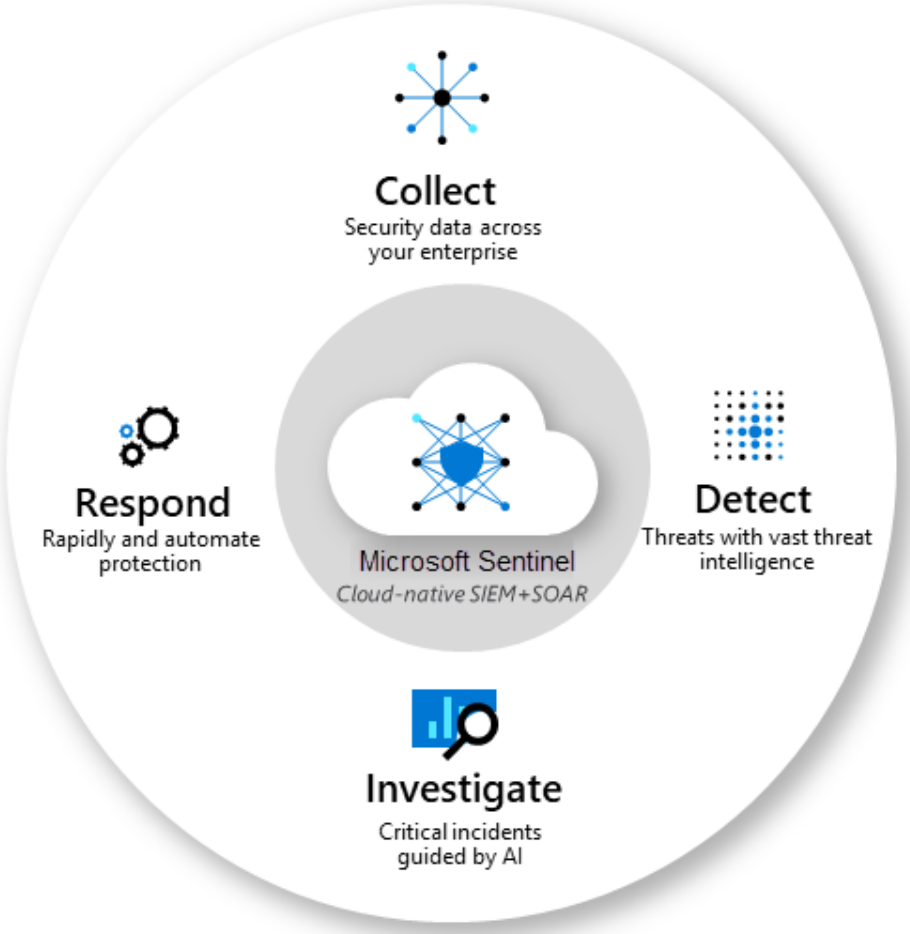
Azure Monitor alerts

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?



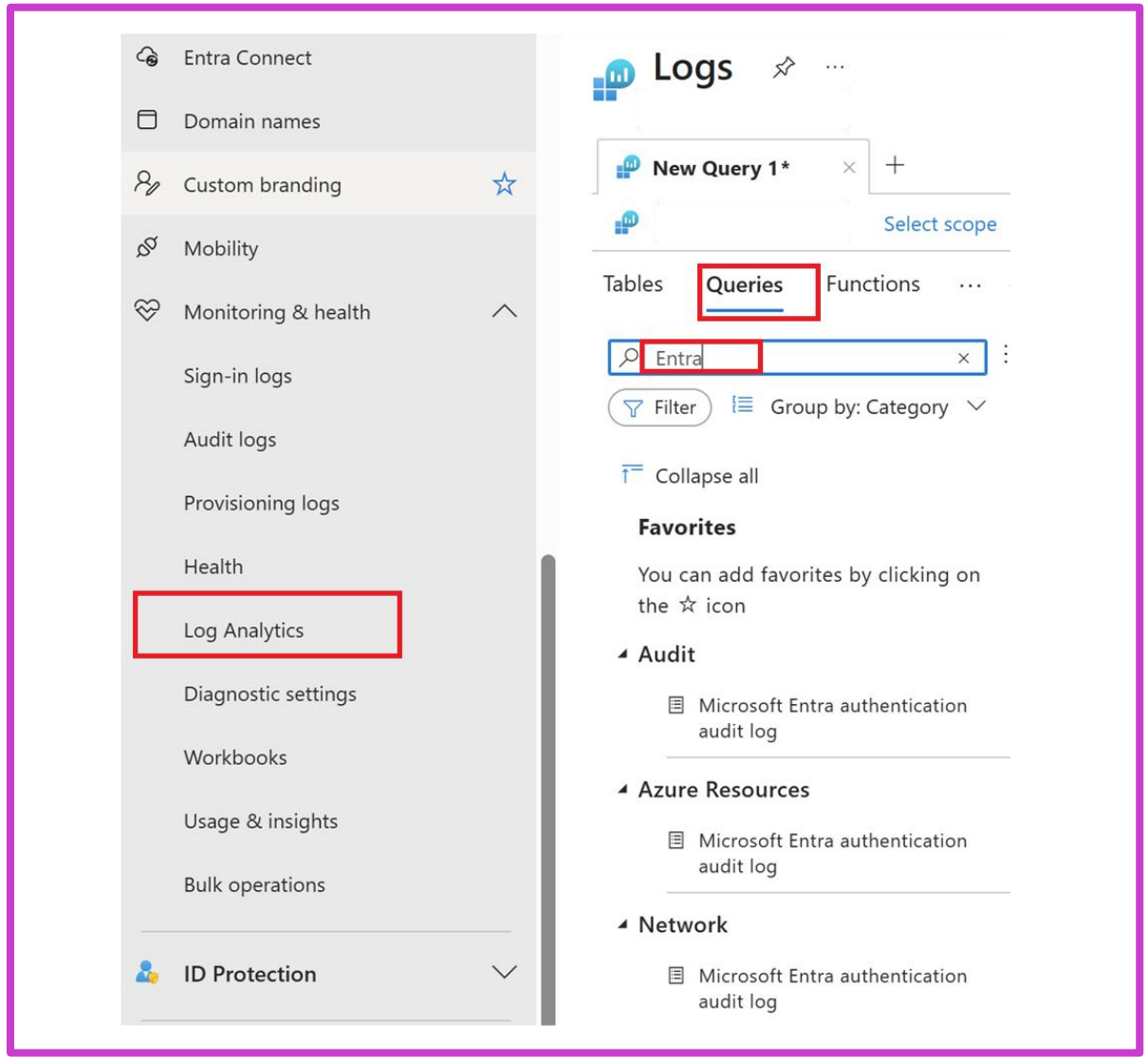
Microsoft Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes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

Connecting Microsoft Entra logs into Log Analytics

Azure Monitor → Logs → Queries hub

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

A Microsoft Entra ID license is required.



Connecting Microsoft Entra ID logs into Microsoft Sentinel

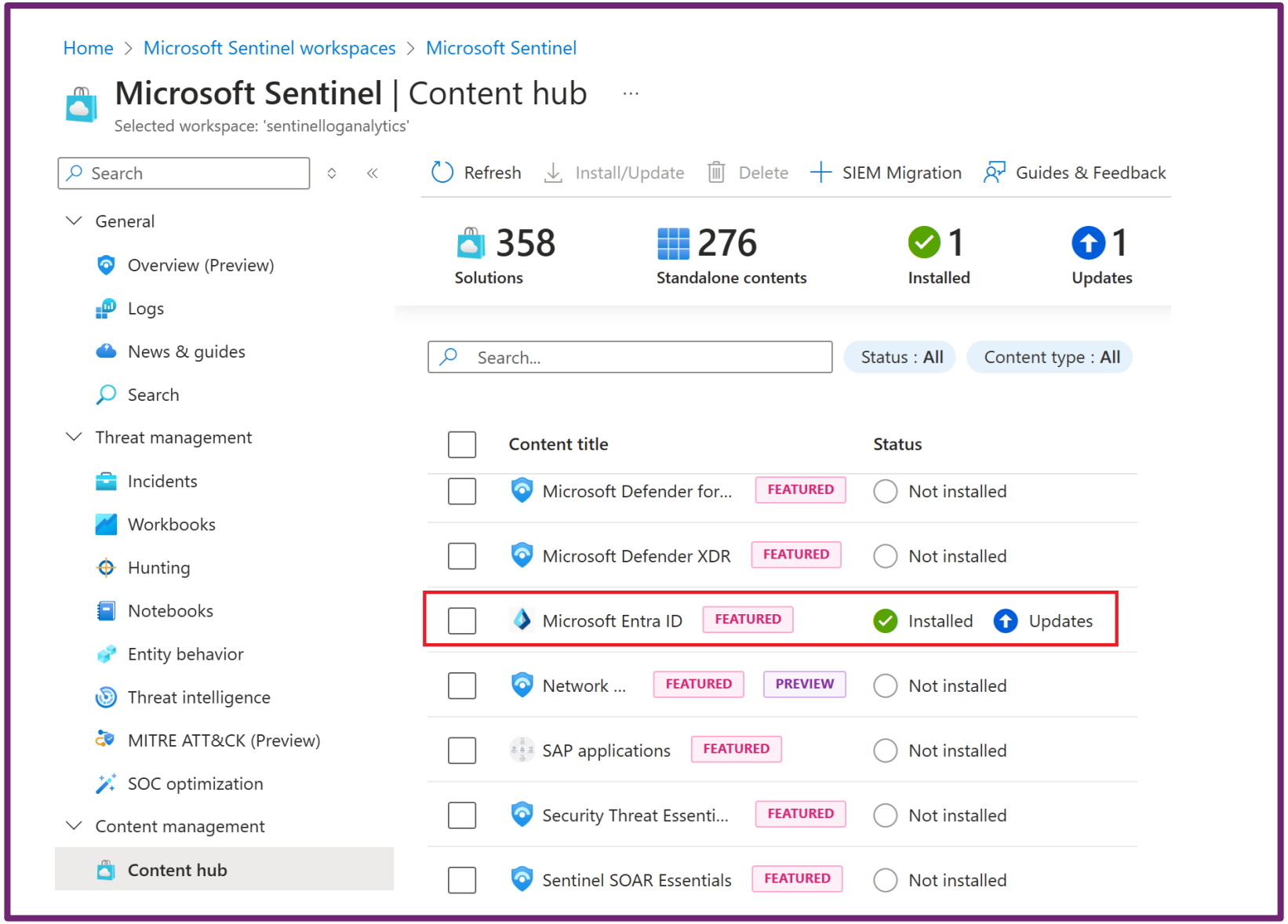
Microsoft Sentinel → Data Connectors (Content Hub)

Set up or use a Workspace.

Microsoft Entra ID

- Sign-in logs and audit logs.

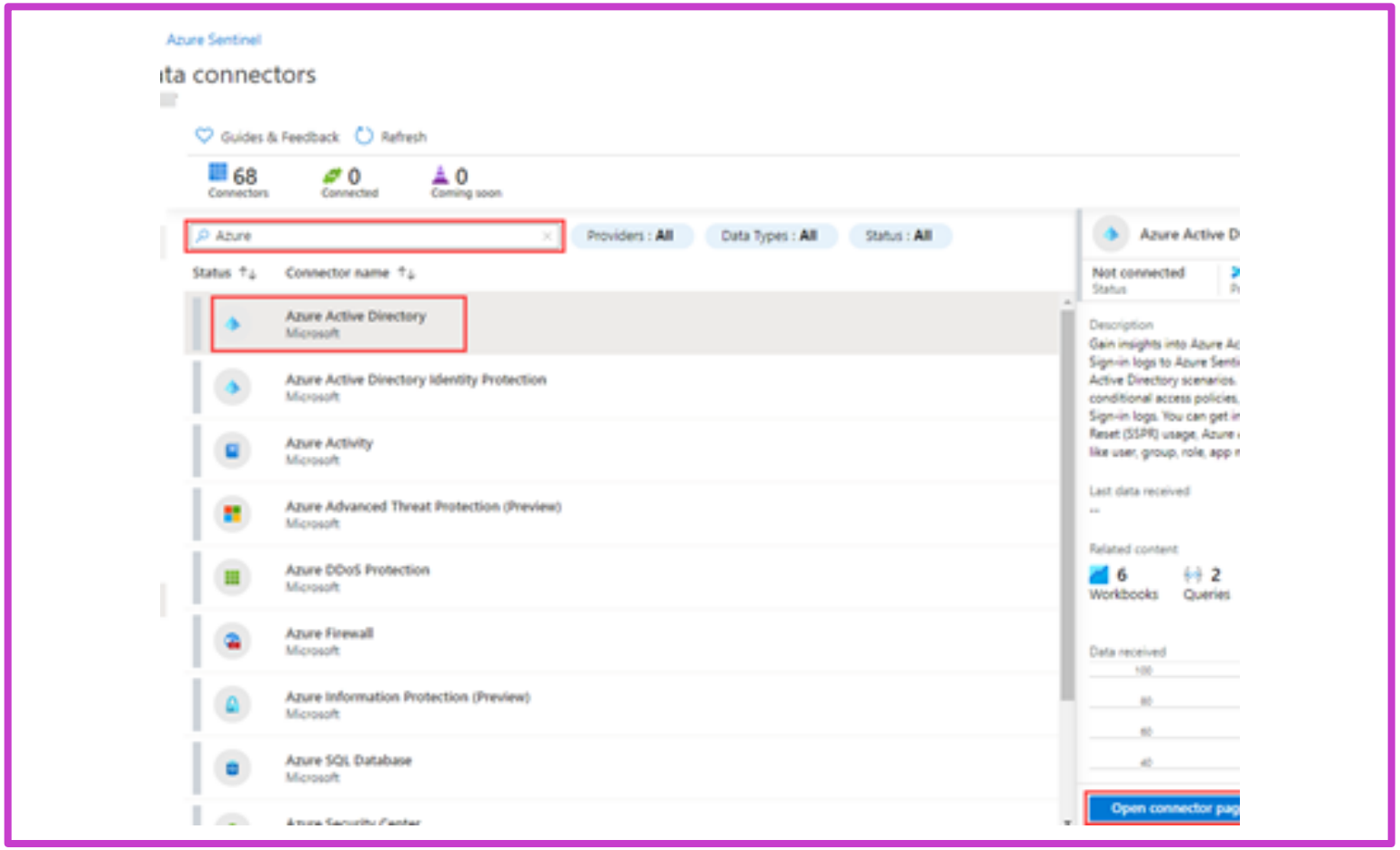
Microsoft Entra ID license required.



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]



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.

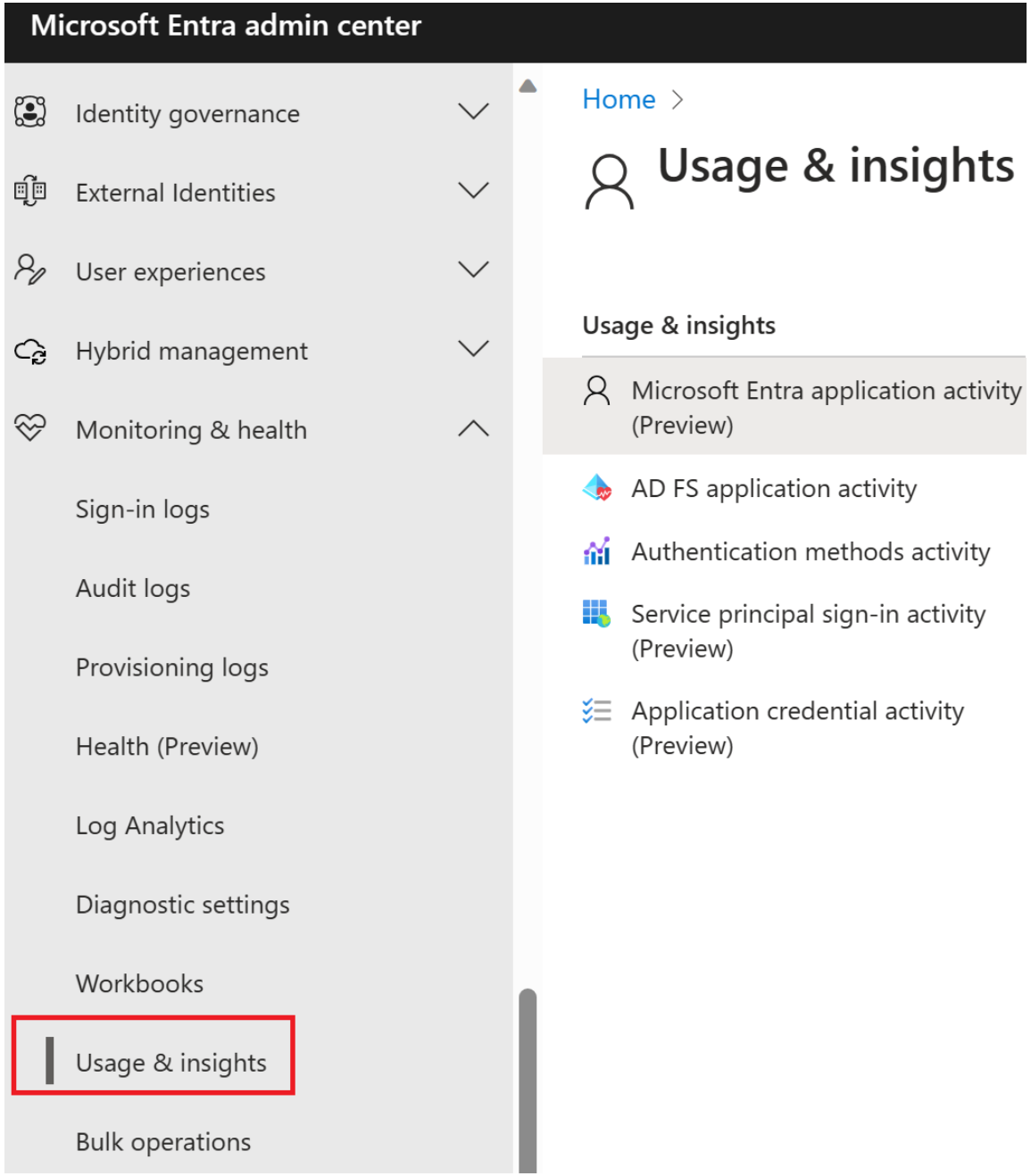
Example of a few third-party SIEM tools

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.



Usage report

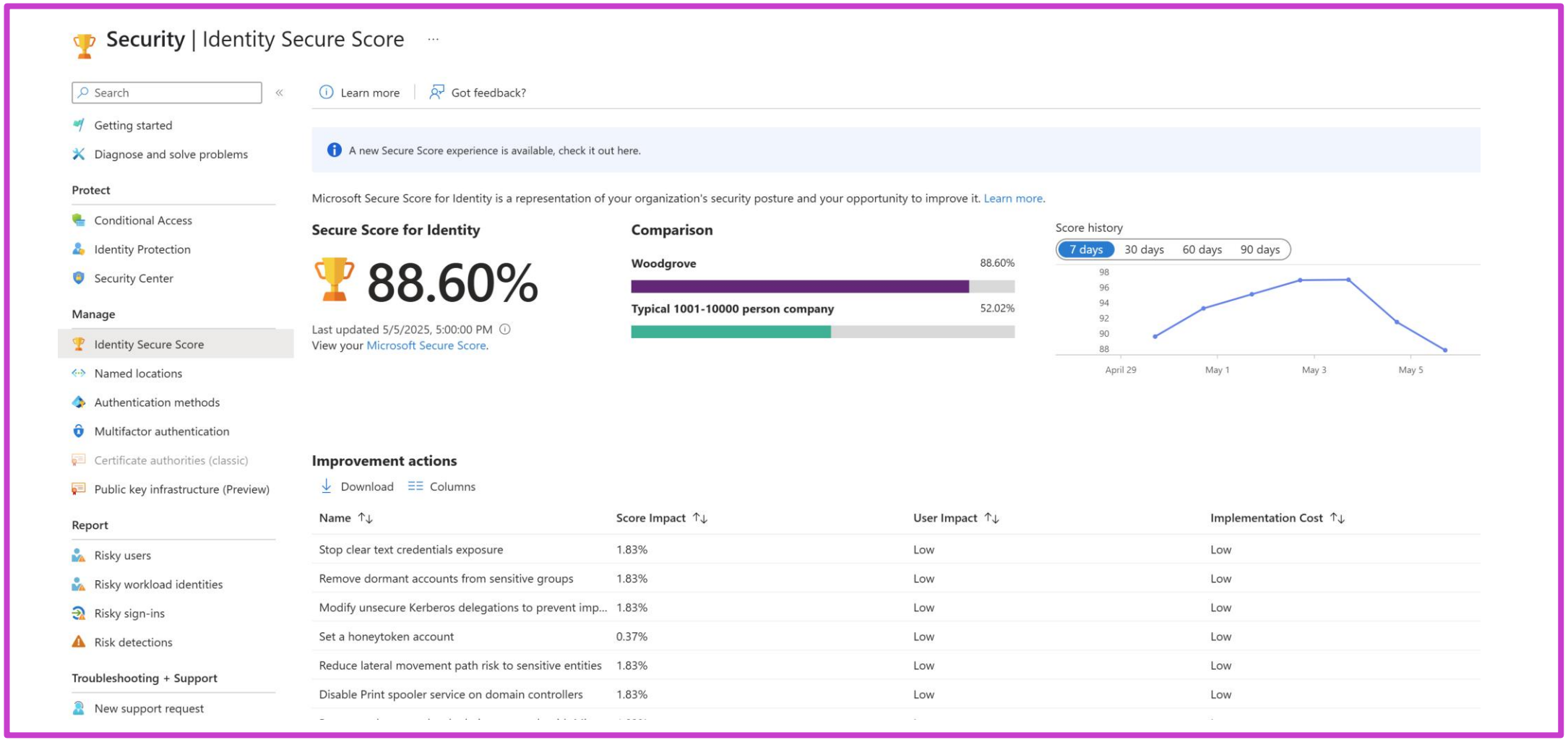
Usage and insights report:

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

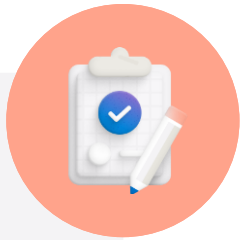
What's Identity Secure Score in Microsoft Entra ID?



Using Identity Secure Score

How are controls scored?	How should I interpret my score?
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 protected/100 total * 10.71% maximum = 0.53% partial score).	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.

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	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