Microsoft Security

SC-300

Tag 4

Microsoft Identity and Access Administrator

SC-300 Agenda

LP1: Implement an Identity Management Solution

LP2: Implement an Authentication and Access Management Solution

Hybrid ID

On Prem AD

AAD

Sync

Data Lake?

OAuth

LDAP

Kerberos

LP3: Implement Access Management for Apps

Access Packages

LP4: Plan and Implement an Identity Governance Strategy

PIM

Audit

Microsoft Security

Plan and Implement an Identity Governance Strategy

Outline

- Plan and implement entitlement management
- Plan, implement, and manage access reviews
- Plan and implement privileged access PIM
- Monitor and maintain Azure Active Directory

KQL
4 usto

LA

Microsoft Security

JIT

JEA

package
1 Woche

Plan and implement entitlement management

Objectives

- Entitlement Management
- Define catalogs
- Define access packages
- Plan, implement, and manage entitlements
- Implement and manage terms of use
- Manage the lifecycle of external users in Azure AD
- Configure and manage connected organization
- Review per-user entitlements

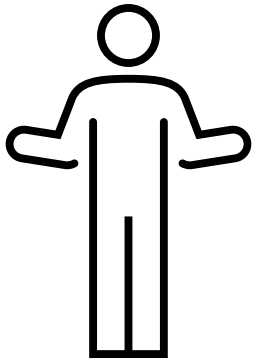
Entitlement management

What is entitlement management?

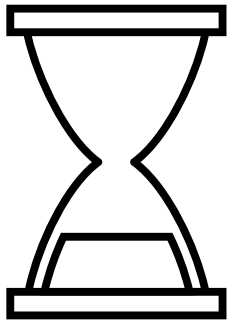
Azure Active Directory (Azure AD) entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

Azure AD entitlement management can help you more efficiently manage access to groups, applications, and SharePoint Online sites for internal users, and also 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

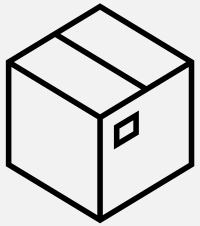


Users may hold on to access longer than needed

Summary of terminology

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, 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 is governed with policies. An access package is always contained in a catalog. You would create a new access package 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 non-administrators can create their own access packages. Catalog owners can add resources they own to a catalog.

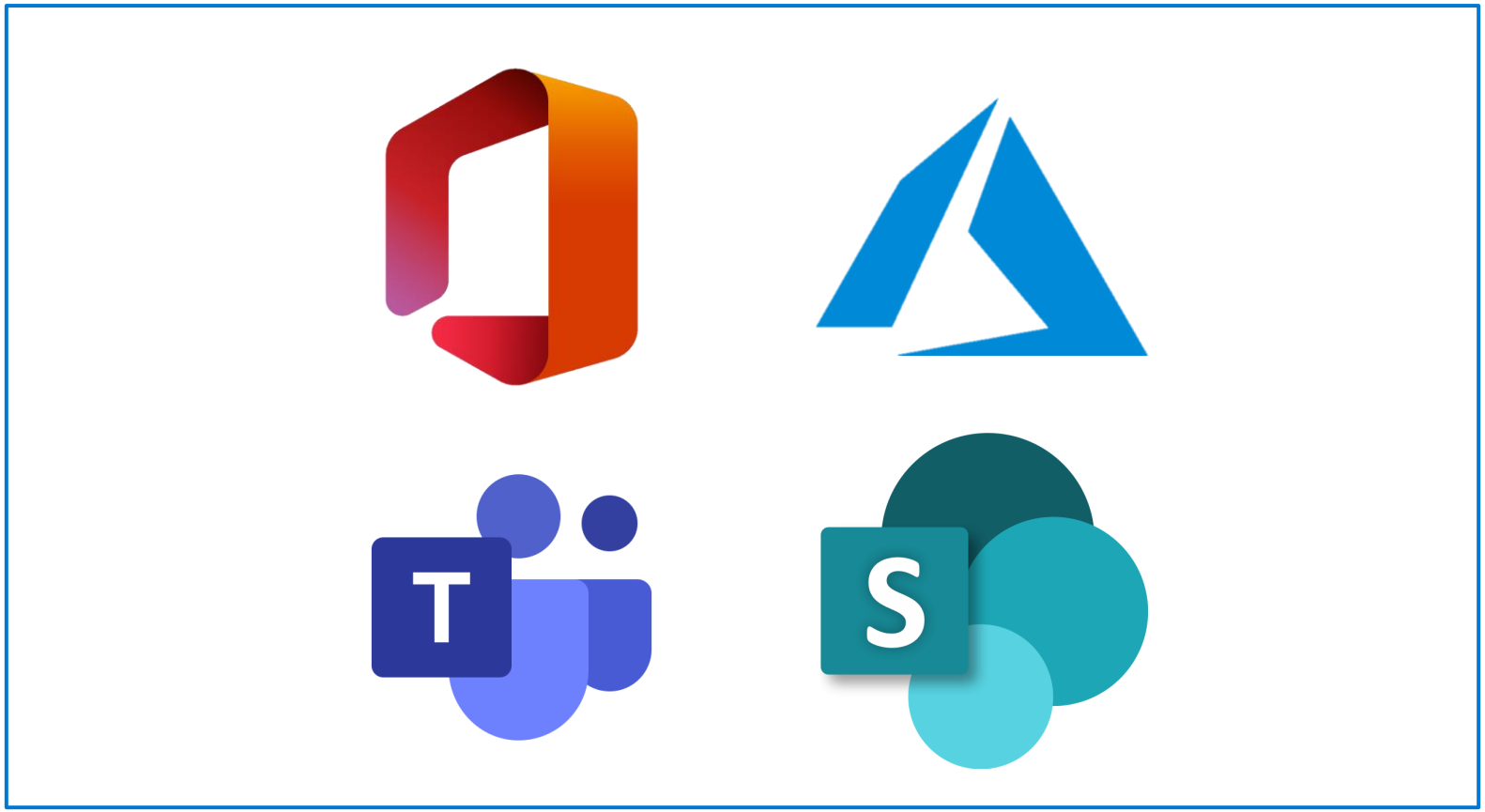
Define access packages



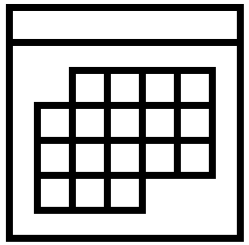
What are access packages? What can I manage with them?

An access package is list of resources like Groups, Apps, and Sites, along with the roles a user needs for those resources.

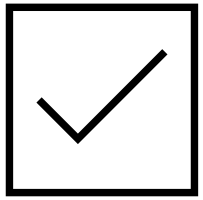
There is a policy included in the access package with rules for who can access the package.



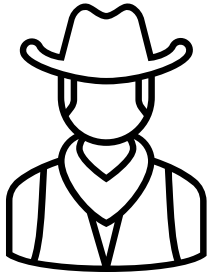
When should I use access packages?



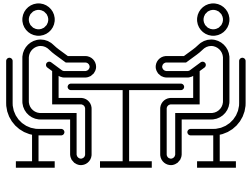
Time-limited access



Manager approval
-or-
Delegated Role / Identity

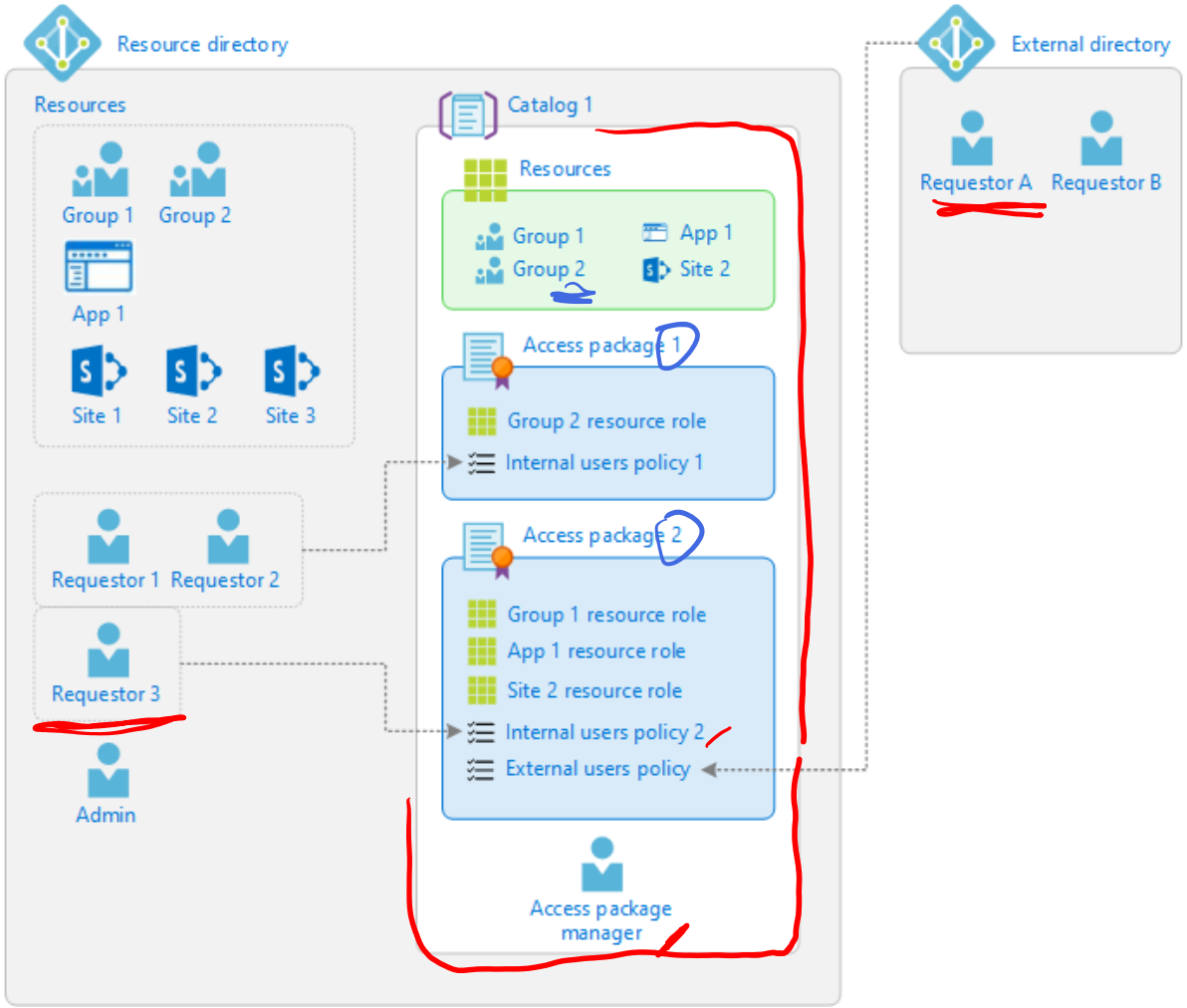


Manage access without IT

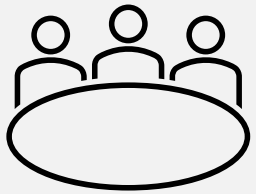


Cross organization collaboration

How do I control who gets access?



Define Catalogs



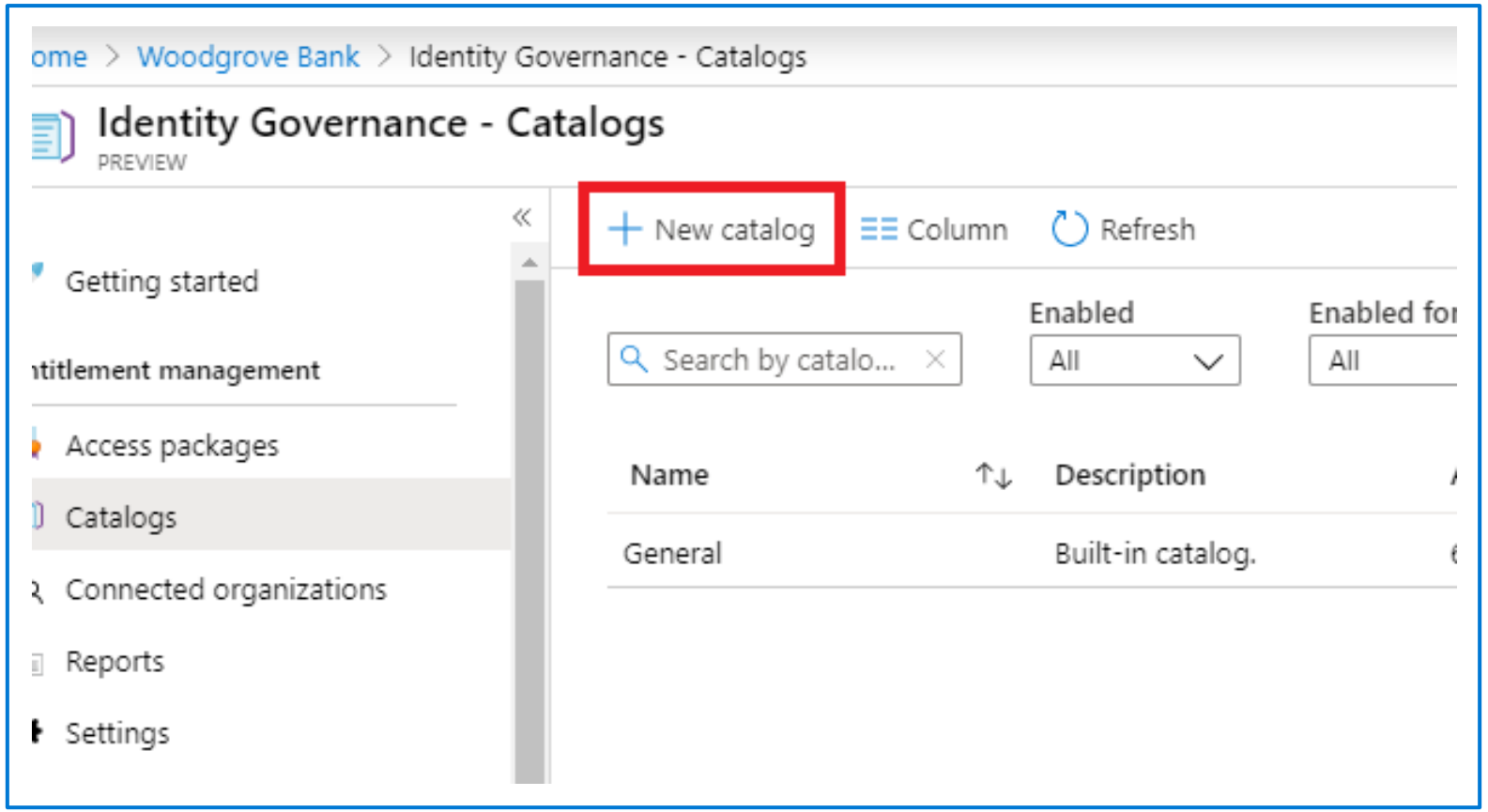
What is a catalog?

Catalog is container of:

- Resources
- Access packages

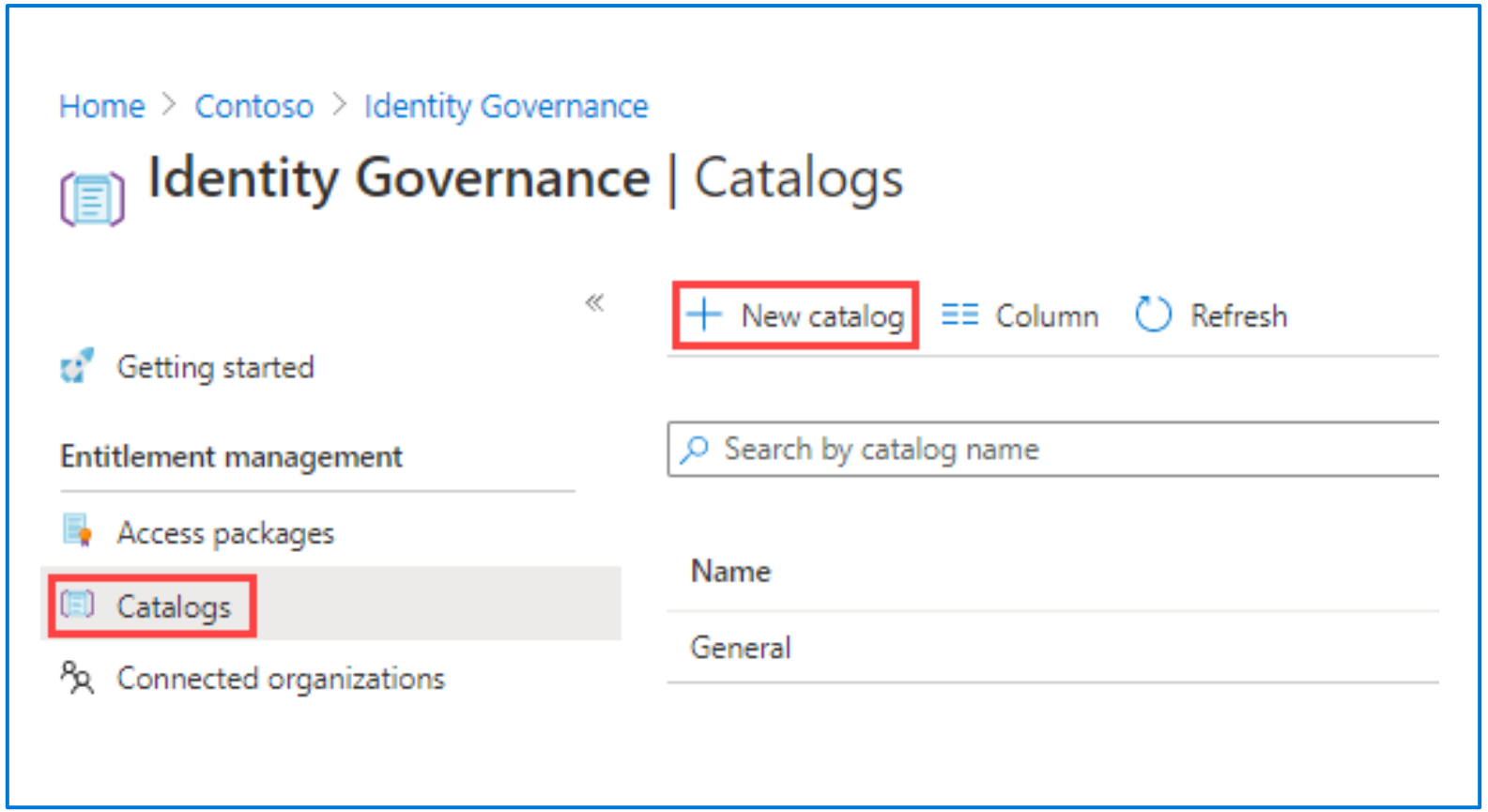
Group related resources together.

Catalog creator is the default owner.



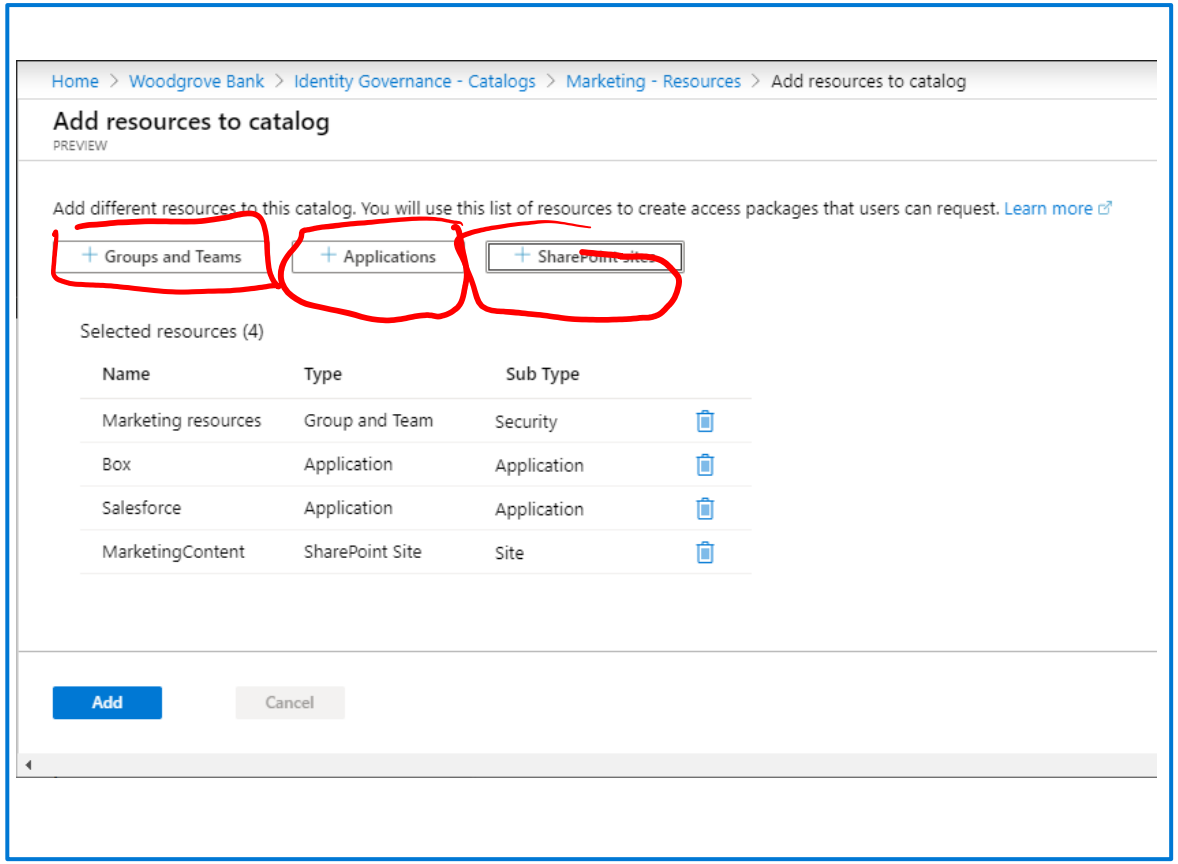
Creating a catalog

1. Log into Azure as Global administrator
2. Open **Azure Active Directory** and the select **Identity Governance**
3. Select **Catalogs** and then **+New Catalog**
4. Enter a **Name** and **Description**
5. Adjust 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 **Marketing**.
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**.

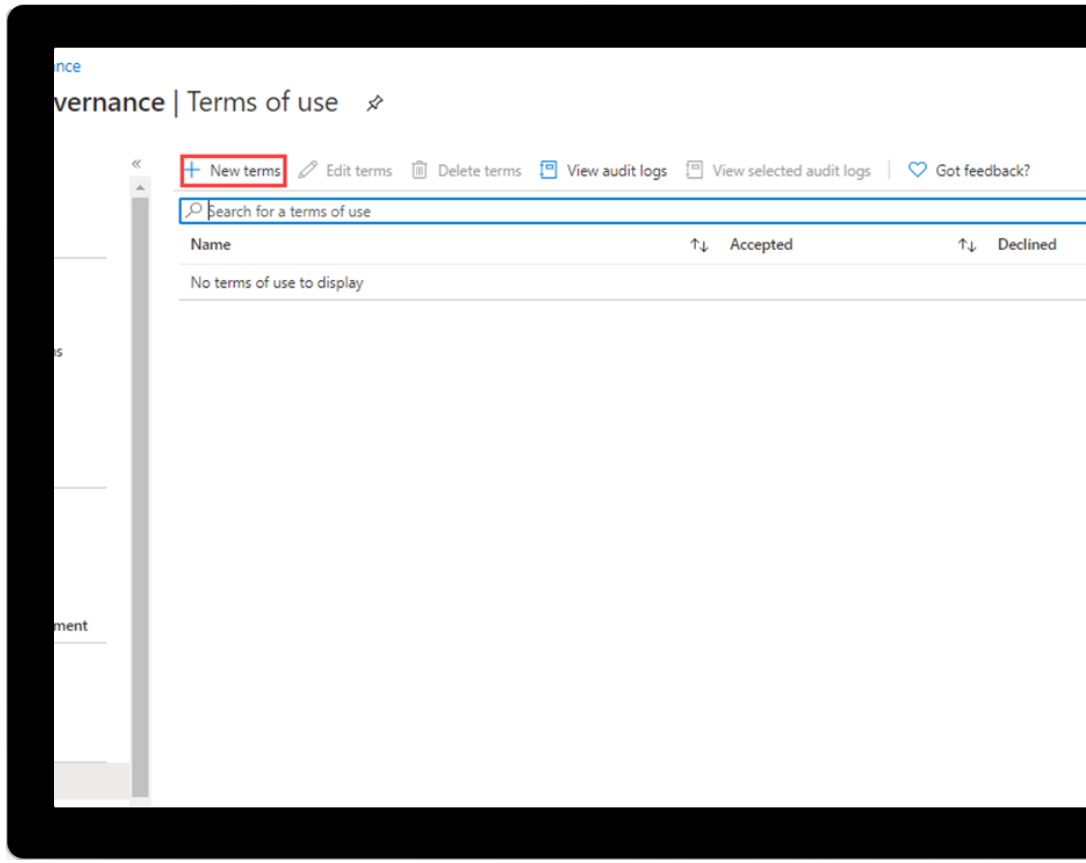


Entitlement Owners and Process

Create a catalog of resources in Azure AD

This exercise teaches students to create and manage catalogs for use with Entitlement Management in Azure AD.

[Launch this Exercise in GitHub]



Implement and manage terms of use

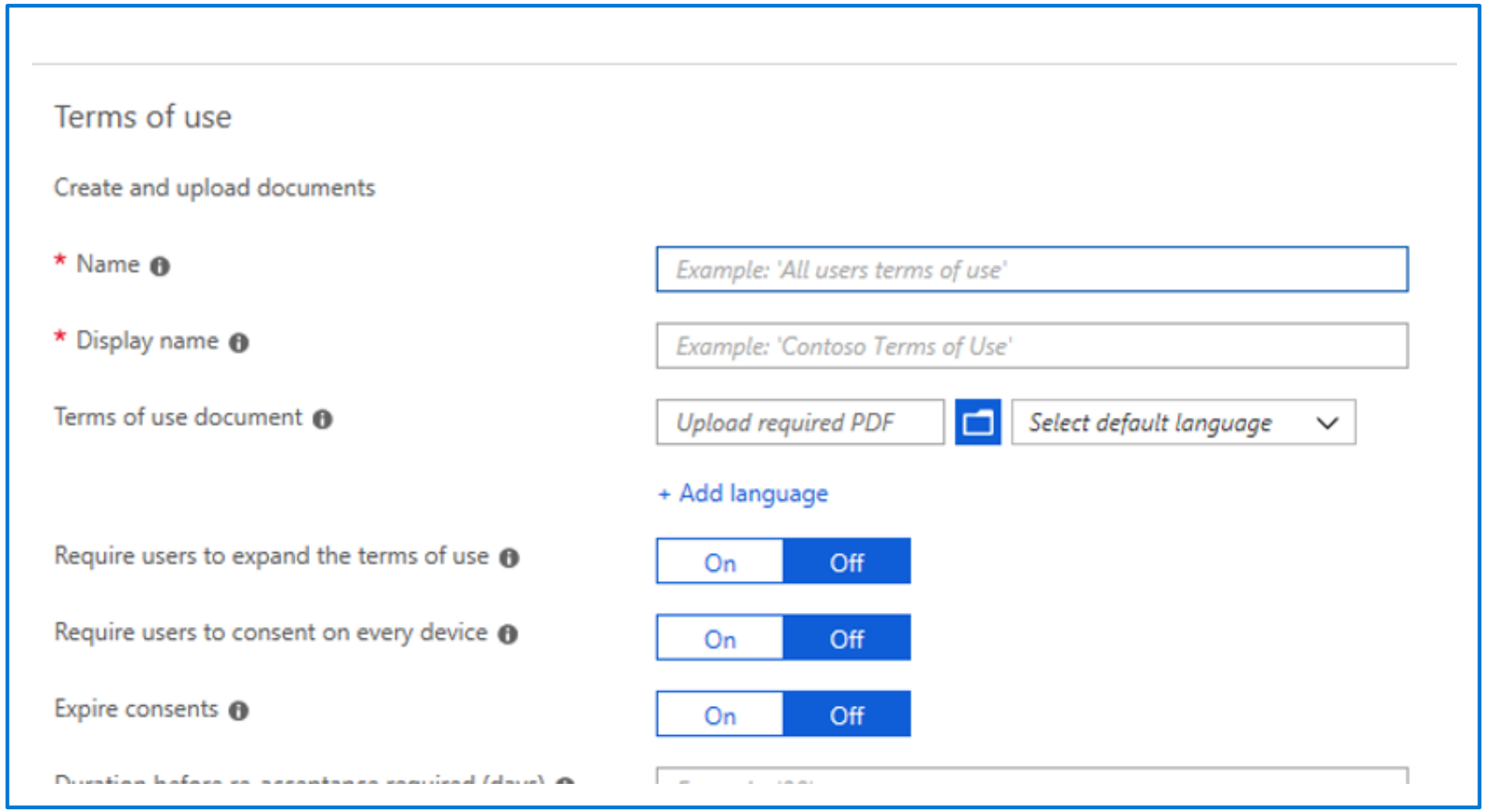
What are Terms of Use in Entitlement Management

Terms-of-use stored as a PDF

PDF can contain any content, including contracts - EULA

Can enforce compliance

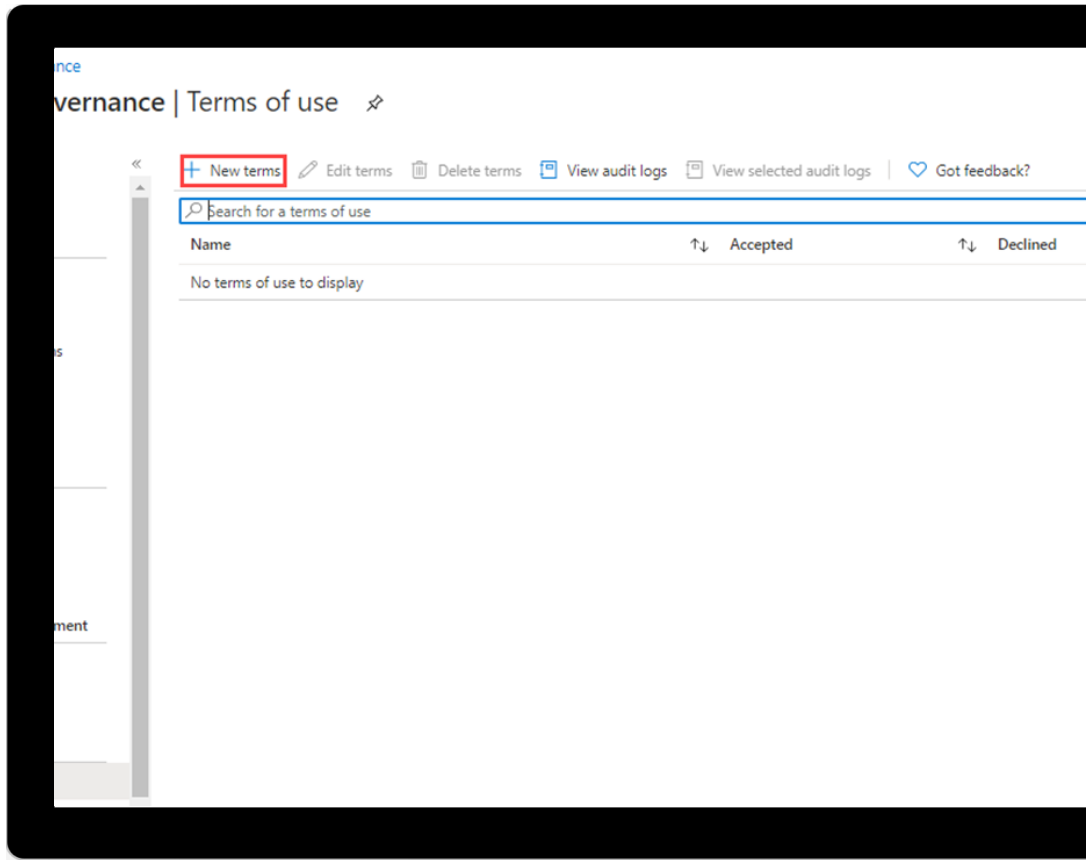
24pt Font recommended



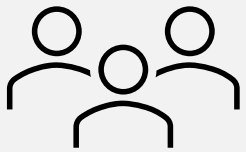
Implement and manage terms of use

This exercise teaches students to create and manage terms of use for Azure AD.

[Launch this Exercise in GitHub]



Manage the lifecycle of external users in Azure AD



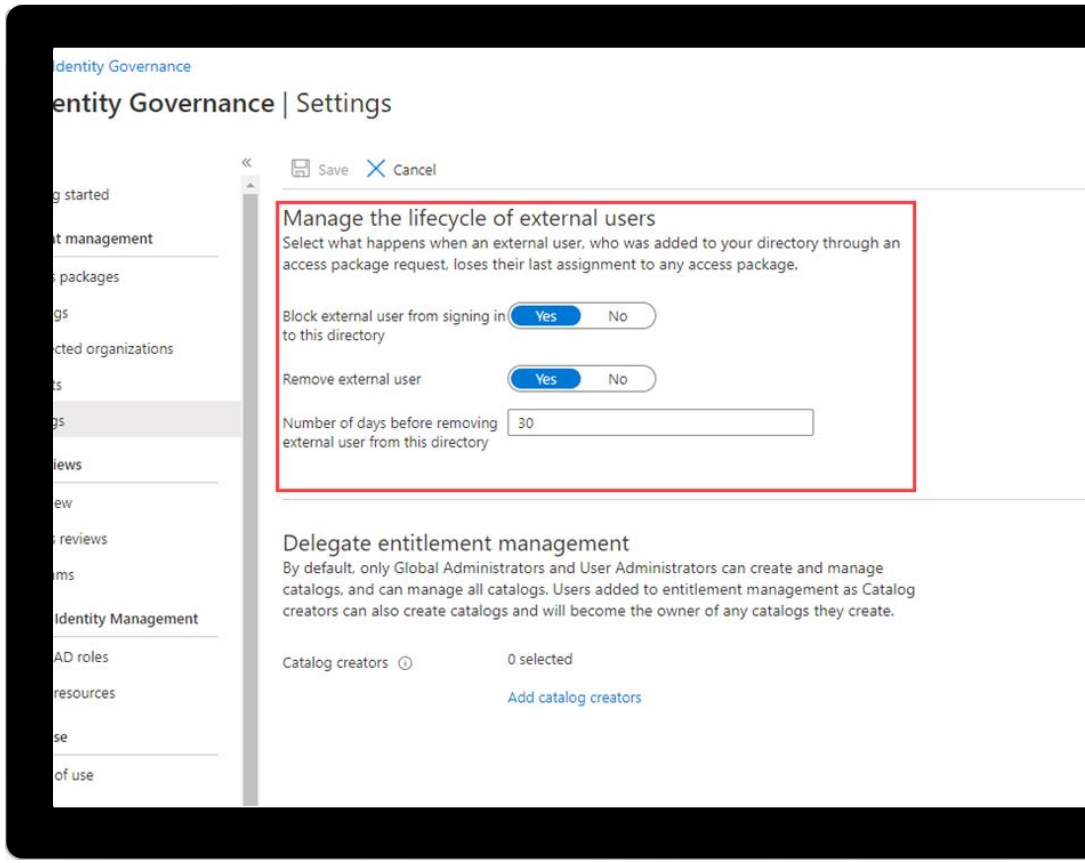
Manage the lifecycle of external users in Azure AD Identity Governance settings

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 are 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 Azure AD.

[Launch this Exercise in GitHub]



Configure and manage connected organizations

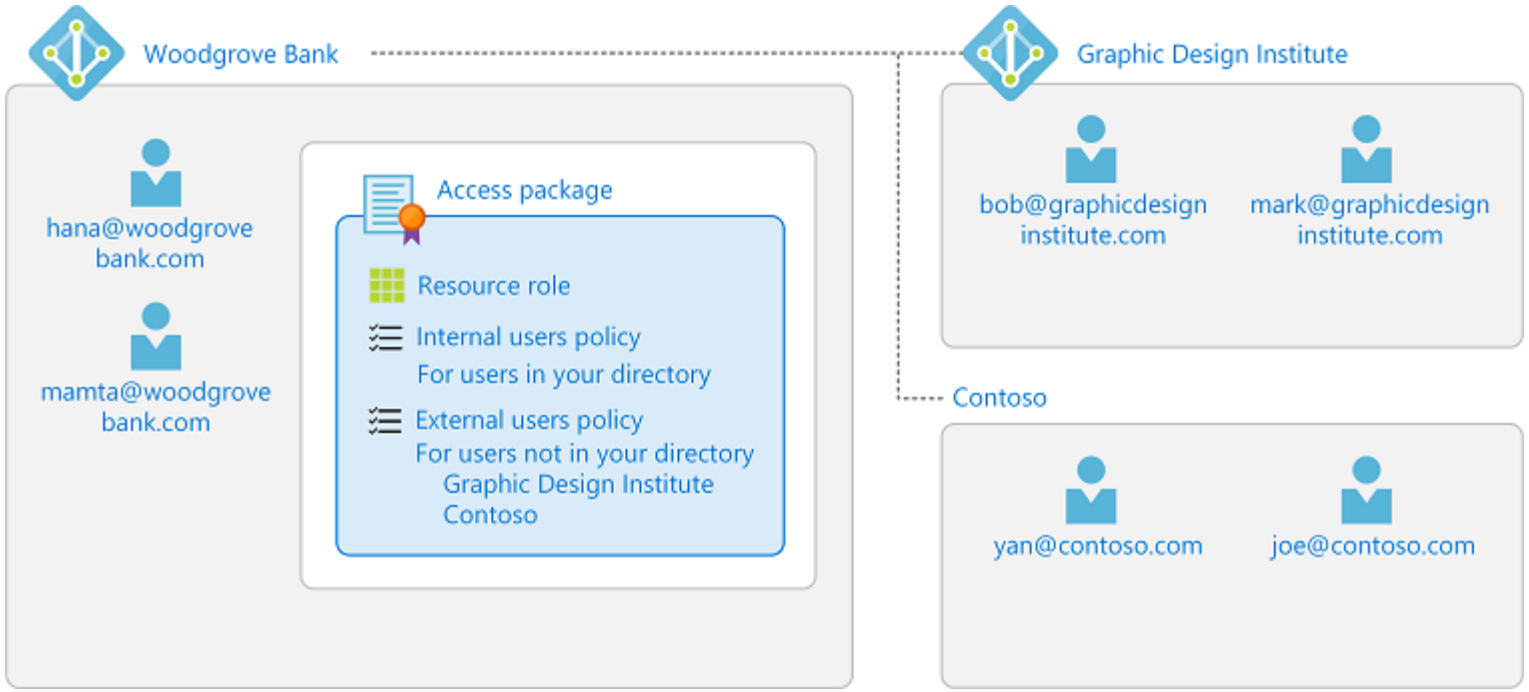
What is a connected organization

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 Azure AD directory, you can use entitlement management to bring them into your Azure AD directory as needed.

There are three ways that entitlement management lets you specify the users that form a connected organization. It could be

- users in another Azure AD directory (from any Microsoft cloud),
- users in another non-Azure AD directory that has been configured for direct federation, or
- users in another non-Azure AD 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 Azure AD, and their users have a user principal name that ends with *graphicdesigninstitute.com*.
- Contoso does not yet use Azure AD. Contoso users have a user principal name that ends with *contoso.com*.

Add a connected organization

1. In the **Azure portal**, select **Azure Active Directory**, and then select **Identity Governance**.
2. In the left pane, 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 Azure AD directory or domain. Be sure to enter the entire domain name.
6. Select Add to add the Azure AD directory or domain. Currently, you can add only one Azure AD directory or domain per connected organization.
7. After you've added the Azure AD 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.

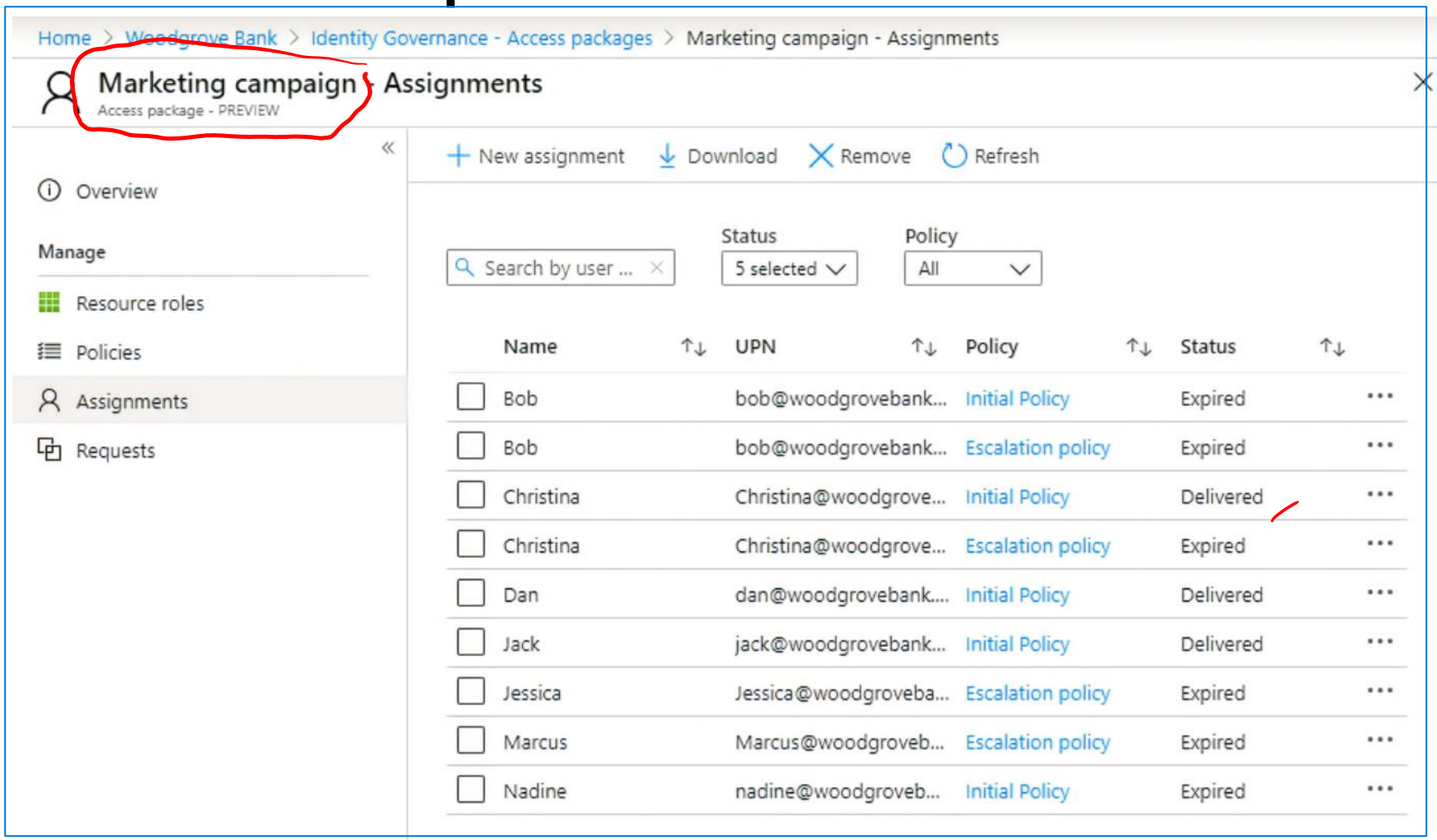
9. Select the Review + create tab, review your organization settings, and then select Create.

Review per-user Entitlements

Who has an entitlement – Azure portal

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

= APP

MS Graph
MSAL

```
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}
```

App Permission

var

alias
Format-Table

aktuelle Object

VS Code

Jeff Snover

Summary

In this section you learned how to:

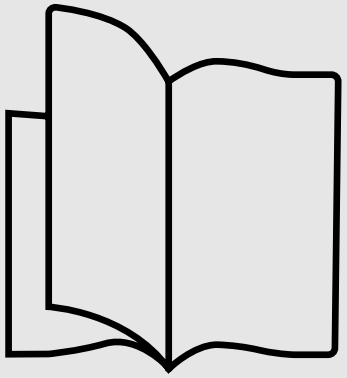
- Define catalogs
- Define access packages
- Plan, implement, and manage entitlements
- Implement and manage terms of use
- Manage the lifecycle of external users in Azure AD

References

Frequently Asked Questions

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use#frequently-asked-questions

Add a connected organization in Azure AD entitlement management - Azure Active Directory - Microsoft Entra | Microsoft Docs



Microsoft Security

Plan, implement, and manage access reviews

Objectives

- Plan for access reviews
- Create access reviews for groups and apps
- Create and configure access review programs
- Manage licenses for access reviews
- Automate access review management tasks
- Configure recurring access reviews

Plan for Access Review

What is an Access Review

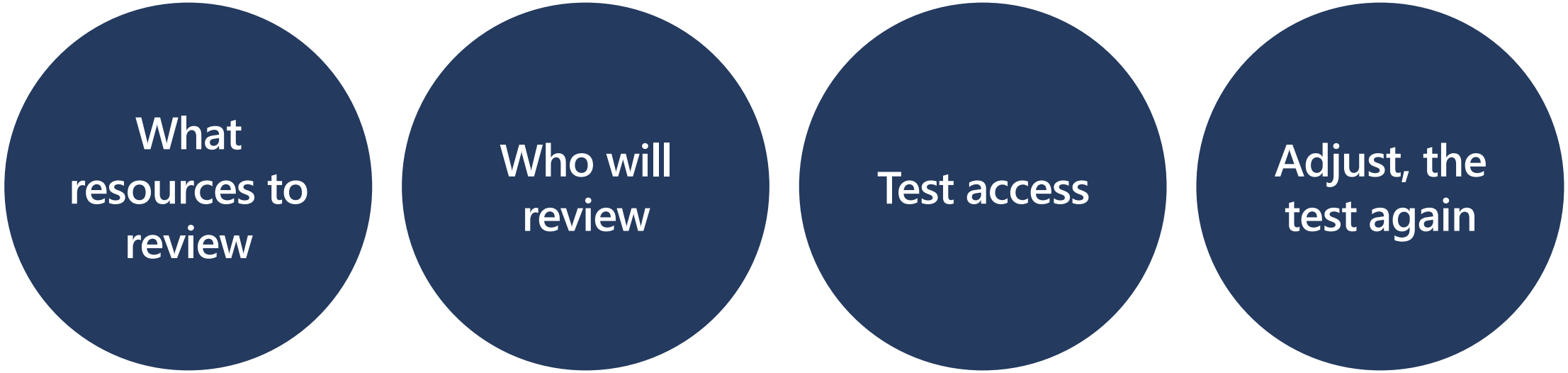
Access Reviews help users ensure that the right people have the right access to the right resources

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

Performed in Azure AD Identity Governance

Planning a pilot

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



Who will 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
Azure AD 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 will perform the review?
- How will they be notified to review?
- What are the timelines to be enforced for 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 as a result based on the review?
- What communications should be sent based on actions taken?

Plan for 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.

Plan for access reviews

Review access packages

Review groups and apps

Review Azure AD roles

Review Azure resource roles

Plan communications

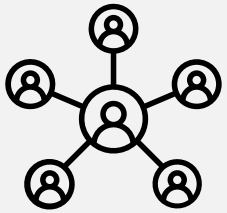
Communication is critical to the success of any new business process. Proactively communicate to users how and when their experience will change and how to gain support if they experience issues.

Communicate changes in accountability

Customize email communication:

- Include a personal message to reviewers, so they understand it is 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.

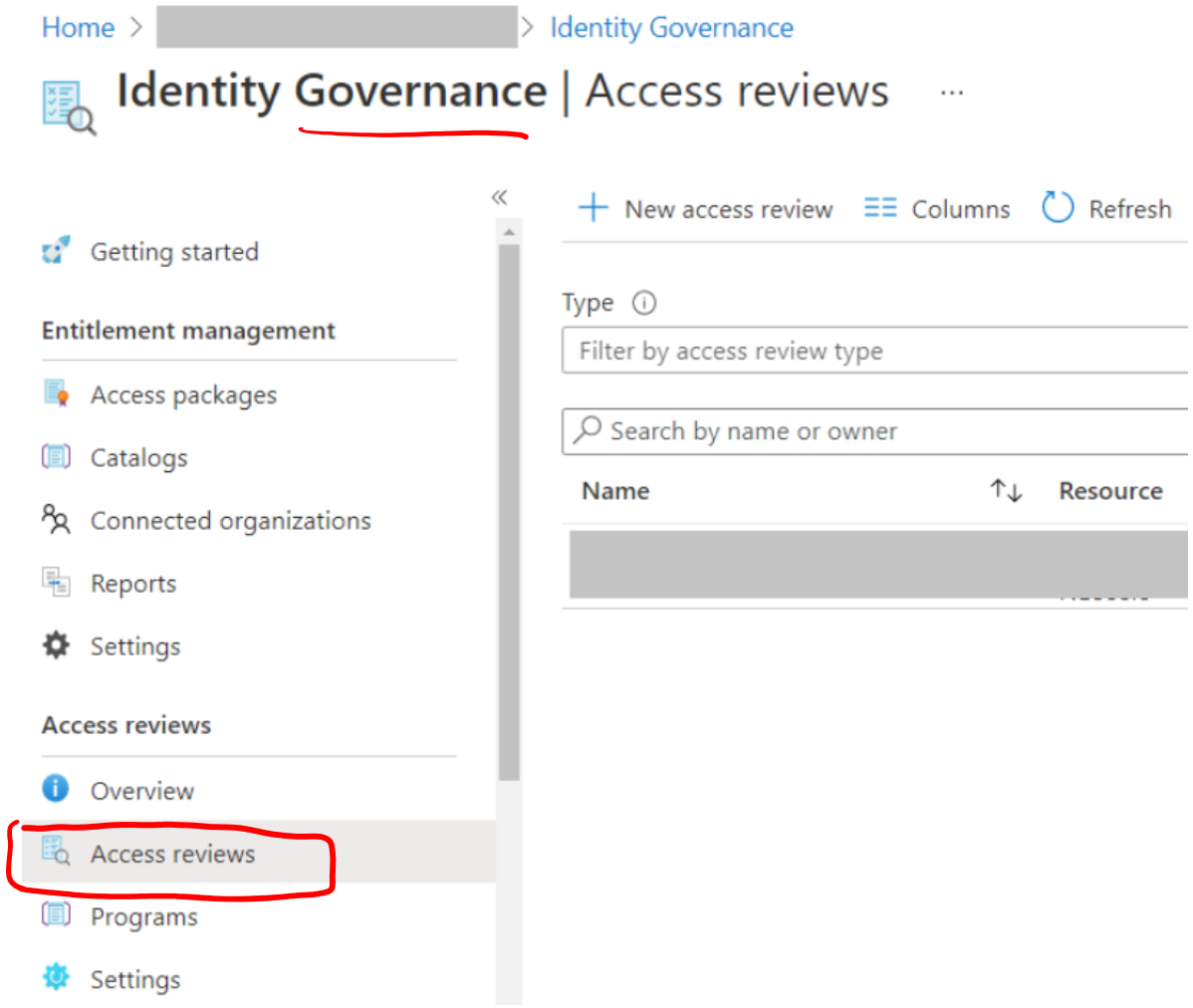
Create access reviews for groups and apps



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 routinely review access, you can also create recurring access reviews

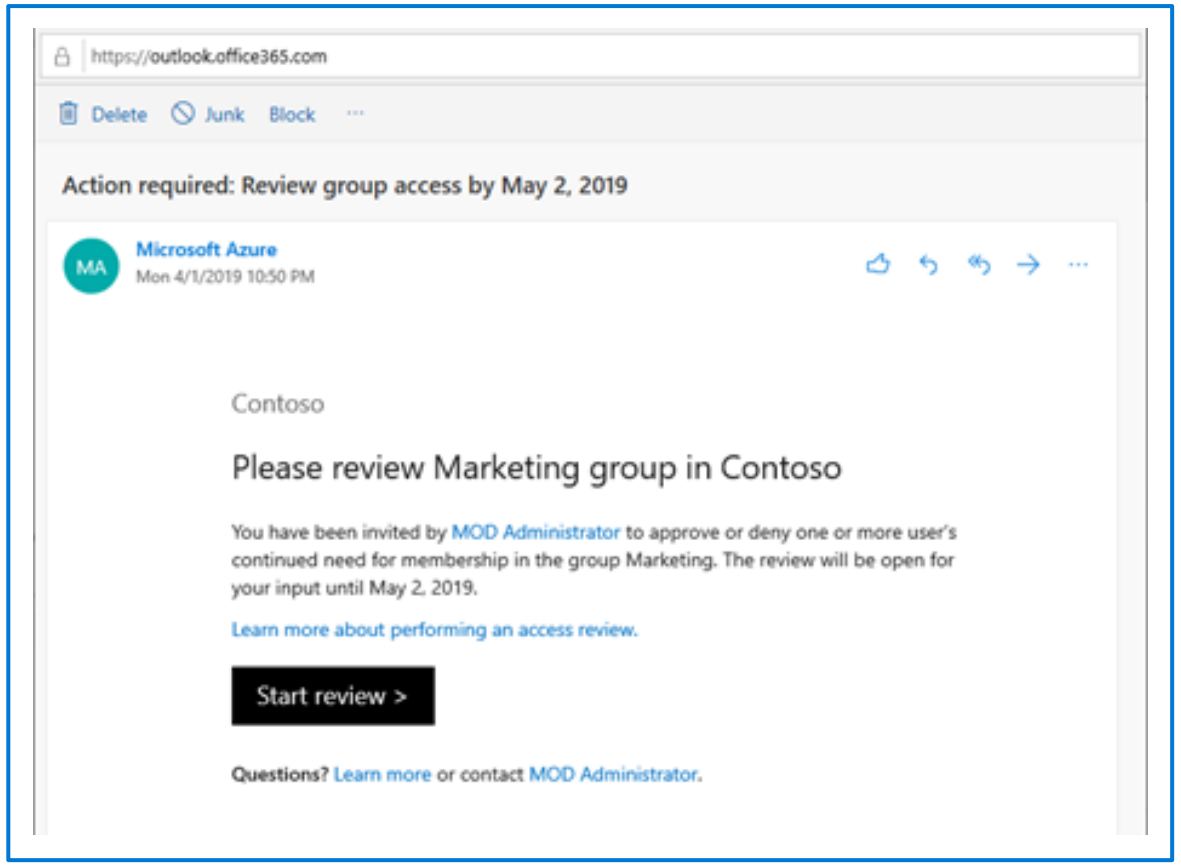


Monitor access review findings

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 see a summary of the recommended actions.
2. Click Ok to accept the recommendations.

Create and configure access review programs

Programs for Access Review

Azure Active Directory (Azure AD) access reviews is a feature of Azure AD 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.

Azure AD access review resource types:

- accessReview – container for the access review
- businessFlowTemplate – defines the resources on which an access review can be performed
- program – defines an access review program
- programControl – links access review to a program
- programControlType – type of access review being performed

Register Azure AD application to call Microsoft Graph API

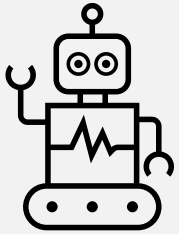
1. Navigate to the Azure AD extension, and select App registrations in the Manage section, to land at the page register apps
2. Select the New application registration button at the top of the page.
3. Provide a name for the application that is different from any other application in your tenant's directory (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. Put a check in the box by those two permissions, and choose Select.
10. Select "Done".

Azure AD 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 not 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 elevate 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, end date, and you're ready to go. Reviewers will be notified at the start of each review
- Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations

Why Recurring Access Reviews?

Doing an Access Review once and never again, there is no value. So set up reviews to occur on a regular schedule.

Summary

In this section you learned how to:

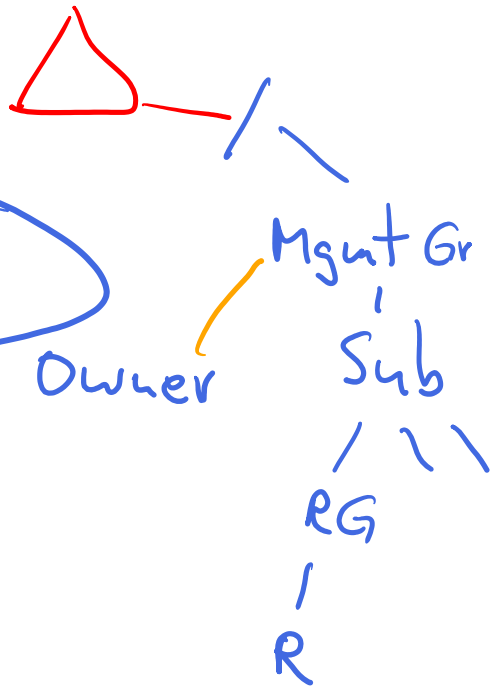
- Plan for access reviews
- Create access reviews for groups and apps
- Monitor access review findings
- Manage licenses for access reviews
- Automate access review management tasks
- Configure recurring access reviews

Microsoft Security

Plan and implement privileged access

Objectives

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



Define a privileged access strategy for administrative users

What is Privileged identity management?

PIM is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. Such resources include those in Azure AD, 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 that you care about. Key features of PIM include:

- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multifactor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit

JIT
4h
1 Jahr
Request Time
Bestätigung
MFA
Begründung

Define a privileged access strategy for administrative users

Identify stakeholders

Start using PIM

Enforce principle of least privilege

Decide which roles to protect with PIM

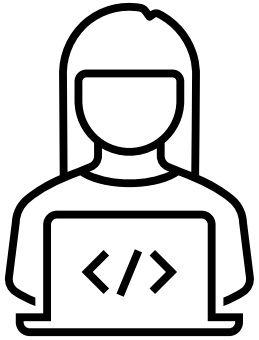
Decide whether to use a group to assign roles

Decide which should be permanent or eligible

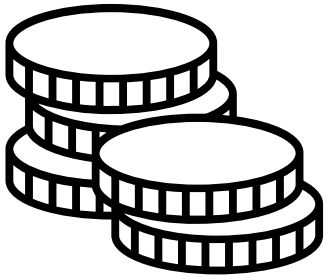
Draft your PIM settings

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



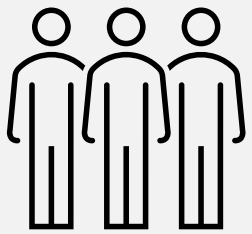
Developer



Financial analyst

Just enough access – Just in time

Plan and configure Privileged Access Groups



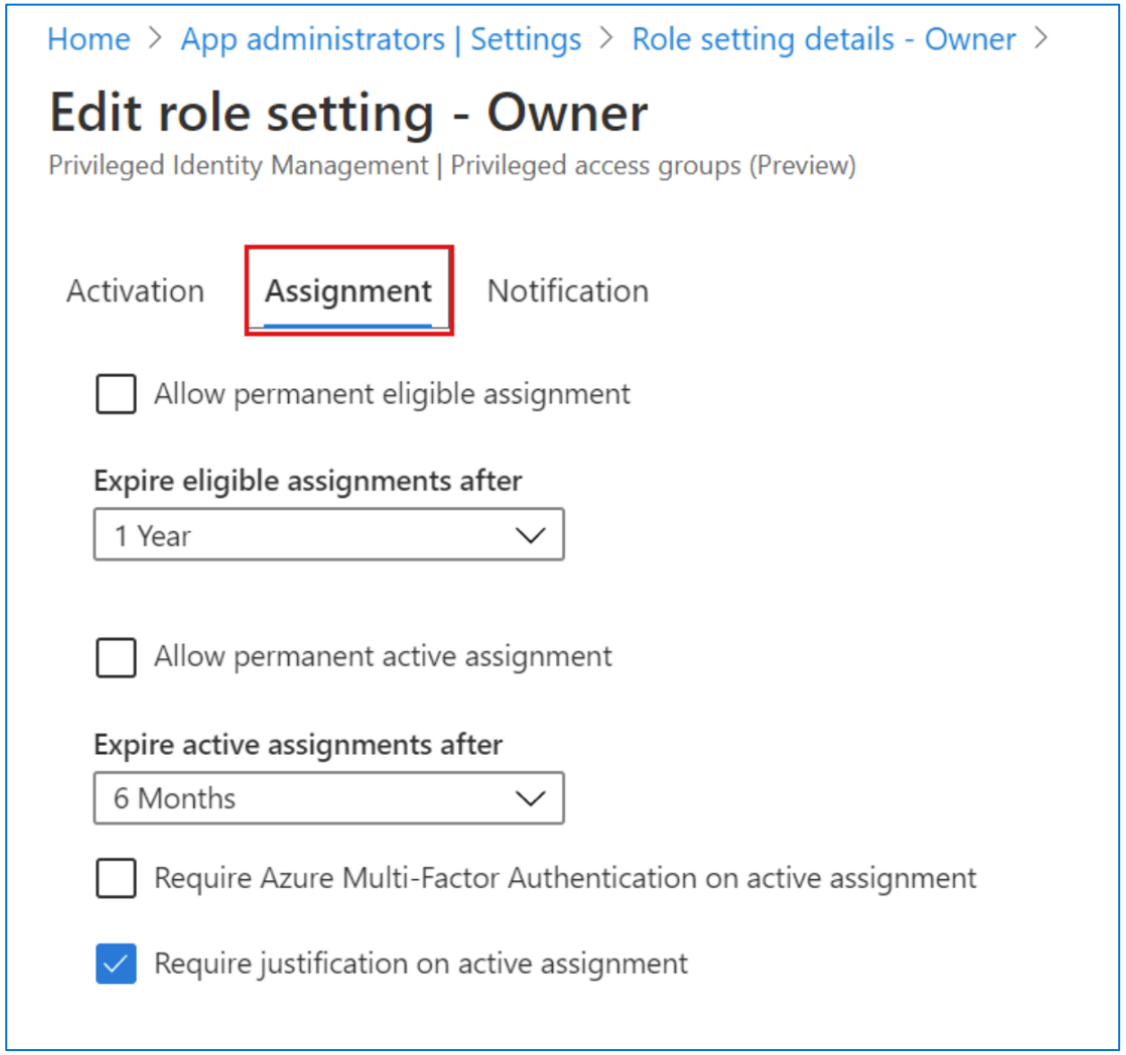
Management for Privileged Access Groups

In Privileged Identity Management (PIM), you can now assign eligibility for membership or ownership of privileged access groups. You can assign Azure Active Directory (Azure AD) 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.

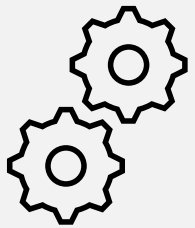
Example:
Your **Tier 0 Office Admins** might need just-in-time access to the **Exchange Admin**, **Office Apps Admin**, **Teams Admin**, and **Search Admin** roles to thoroughly investigate incidents daily.

Example – How to implement

1. Create a new group
2. Check the role-assignable box.
3. Add the 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 for Azure resources



Assign Azure resource roles

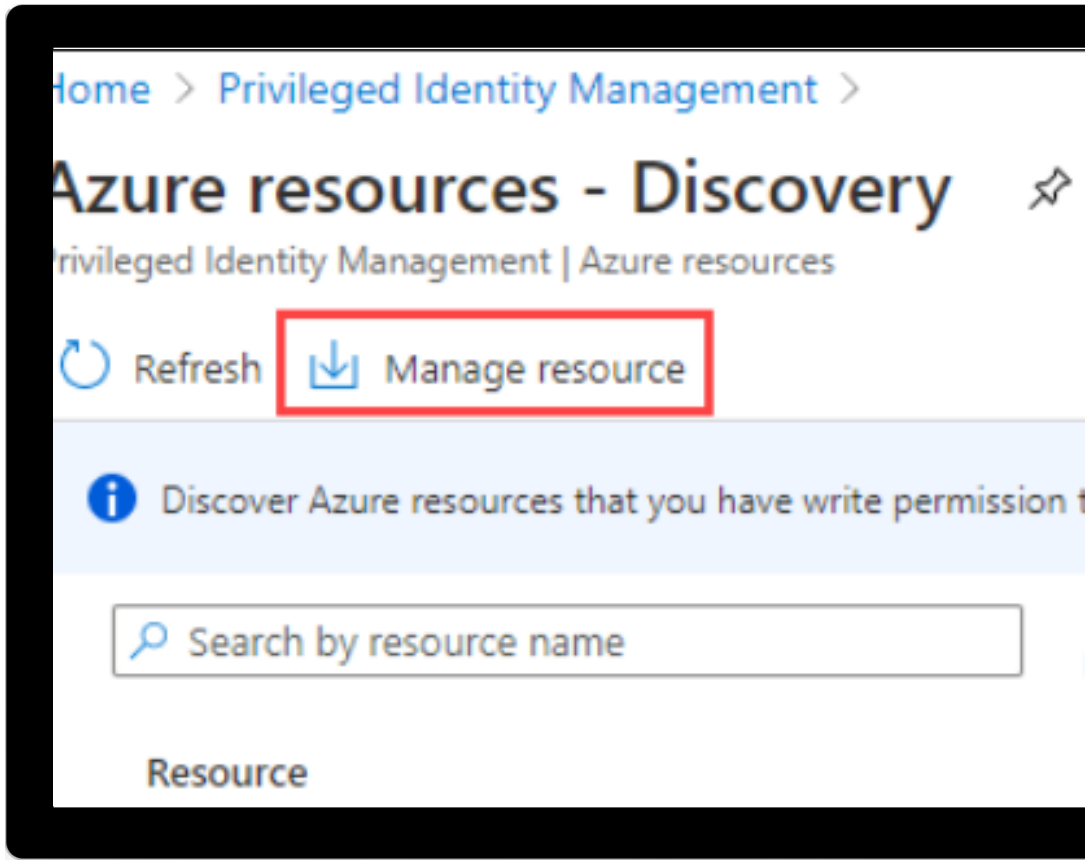
Azure Active Directory (Azure AD) Privileged Identity Management (PIM) can manage the built-in Azure resource roles, as well as custom roles, including (but not limited to):

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

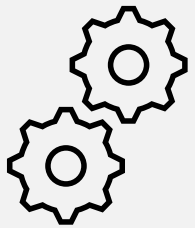
Exercise: Assign Azure resource roles in PIM

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 for Azure AD roles



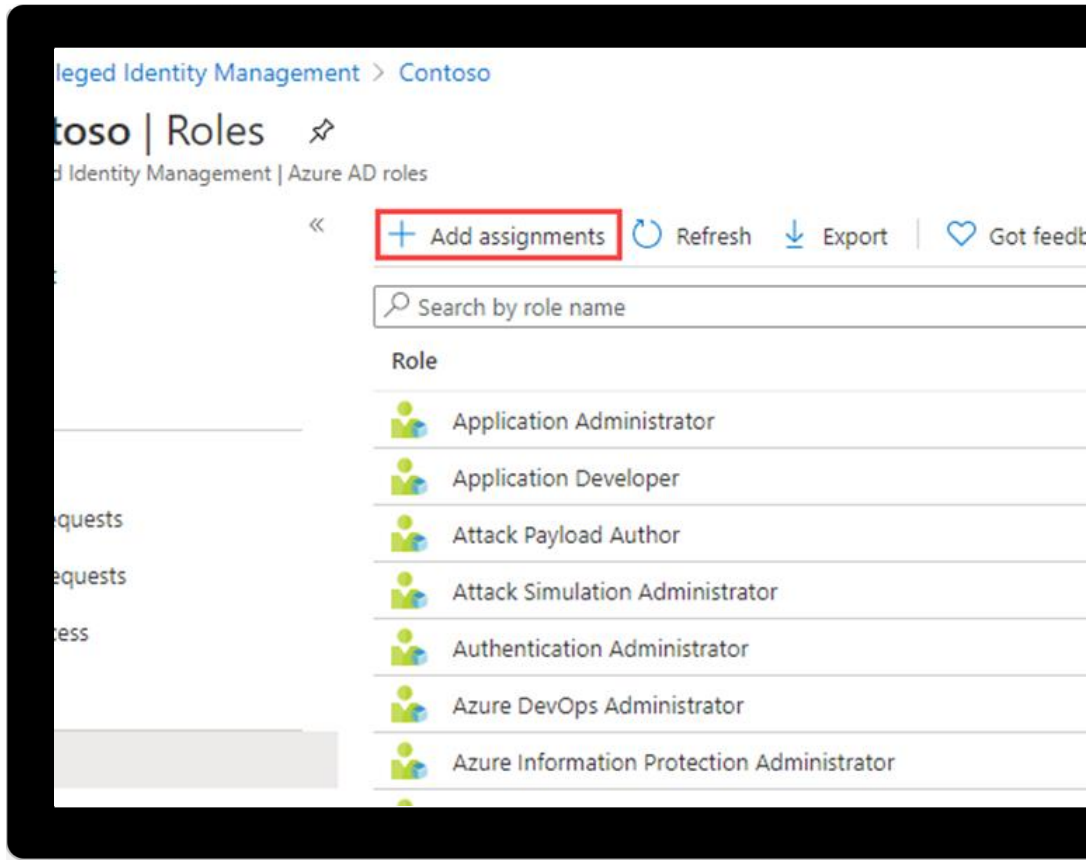
Configure PIM for Azure AD roles

A Privileged role administrator can customize Privileged Identity Management (PIM) in their Azure Active Directory (Azure AD) organization, including changing the experience for a user who is activating an eligible role assignment

Exercise: Configure PIM for Azure AD roles

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

[Launch this Exercise in GitHub]



Analyze PIM audit history and reports

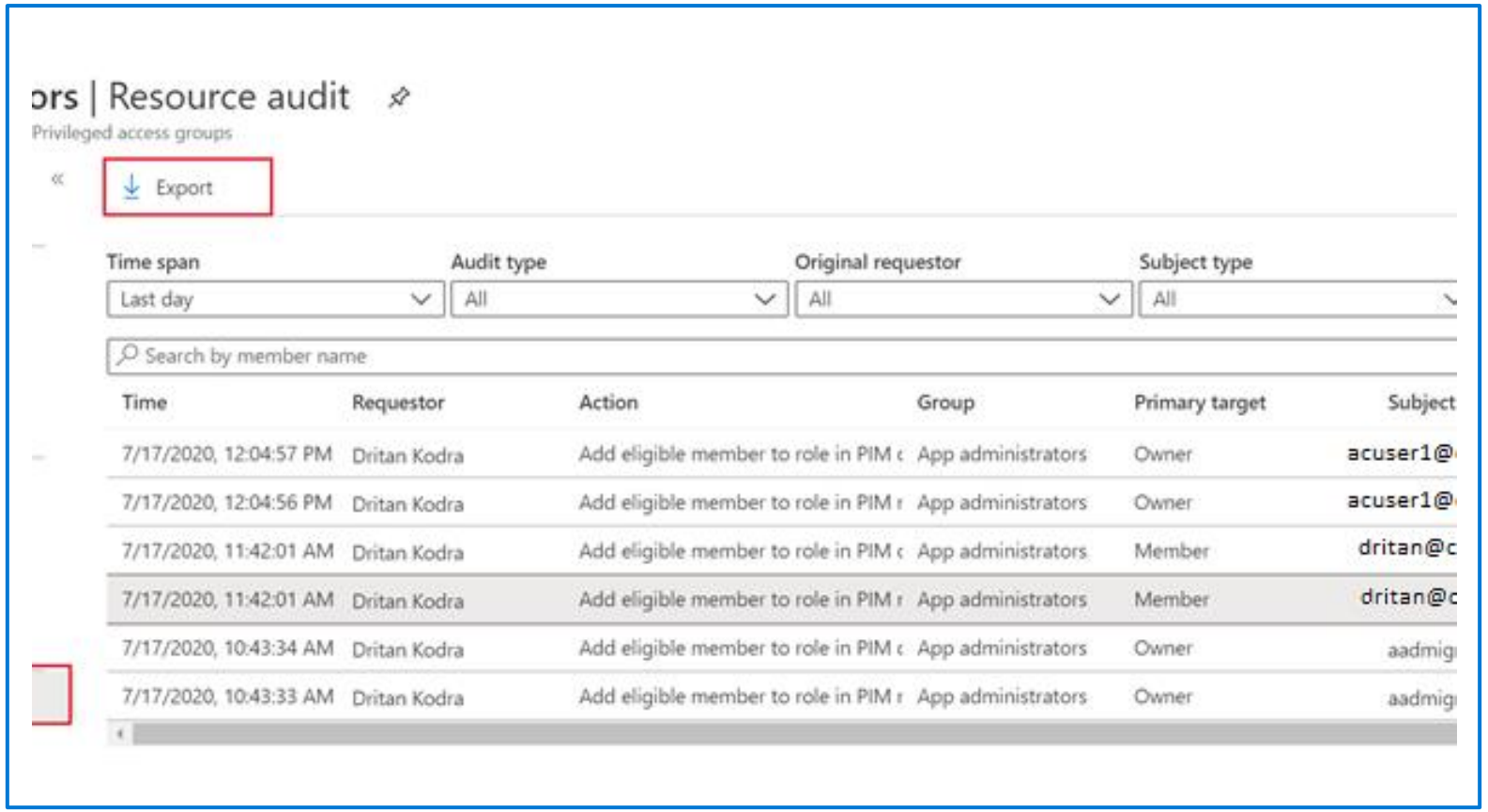
Analyze PIM audit history and reports

Reasons to use

Minimize access to secure information or resources and give users just-in-time privileged access to Azure resources and Azure AD, 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 that you care about.



Create and manage break-glass accounts

What is a Break-Glass Account and Why use?

Prevent being accidentally locked out of your Azure AD 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 that you maintain a goal of restricting emergency account use to only the times when it is absolutely 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 are not federated or synchronized from an on-premises environment.

Exclude Multi-factor authentication

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

Exclude from Conditional Access

During an emergency, you do not 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, at minimum do the following steps at regular intervals:

- Notify of the account-check
- Ensure accounts are documented and current
- Train security officers who might need emergency are trained on the process
- Update the account credentials, in particular any passwords
- Then validate that the emergency access accounts can sign-in and perform administrative tasks
- Ensure that multifactor authentication or self-service password reset (SSPR) is not 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 Azure AD subscriptions in the organization have changed

Summary

→ Feedback MTM

→ Badges 4xLP + 1xSeminar Code

In this section you learned how to:

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

Microsoft Security

Monitor and maintain Azure Active Directory

Objectives

- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Azure AD audit logs
- Enable and integrate Azure AD diagnostic logs with Log Analytics/Microsoft Sentinel

  LA

  Data Lake

  Kusto
- Export sign-in and audit logs to a third-party SIEM
- Review Azure AD activity by using Log Analytics/Microsoft Sentinel, excluding KQL use
- Analyze Azure Active Directory workbooks/reporting
- Monitor security posture with Identity Secure Score in Azure AD

  CSPM

  Free

Analyze and investigate sign-in logs to troubleshoot access issues

Troubleshoot access issues

Id Protection

Activity

- **Sign-ins:** review sign-in activities
- **Audit logs:** review system activity
- **Provisioning logs:** monitor activity by the provisioning service

Security

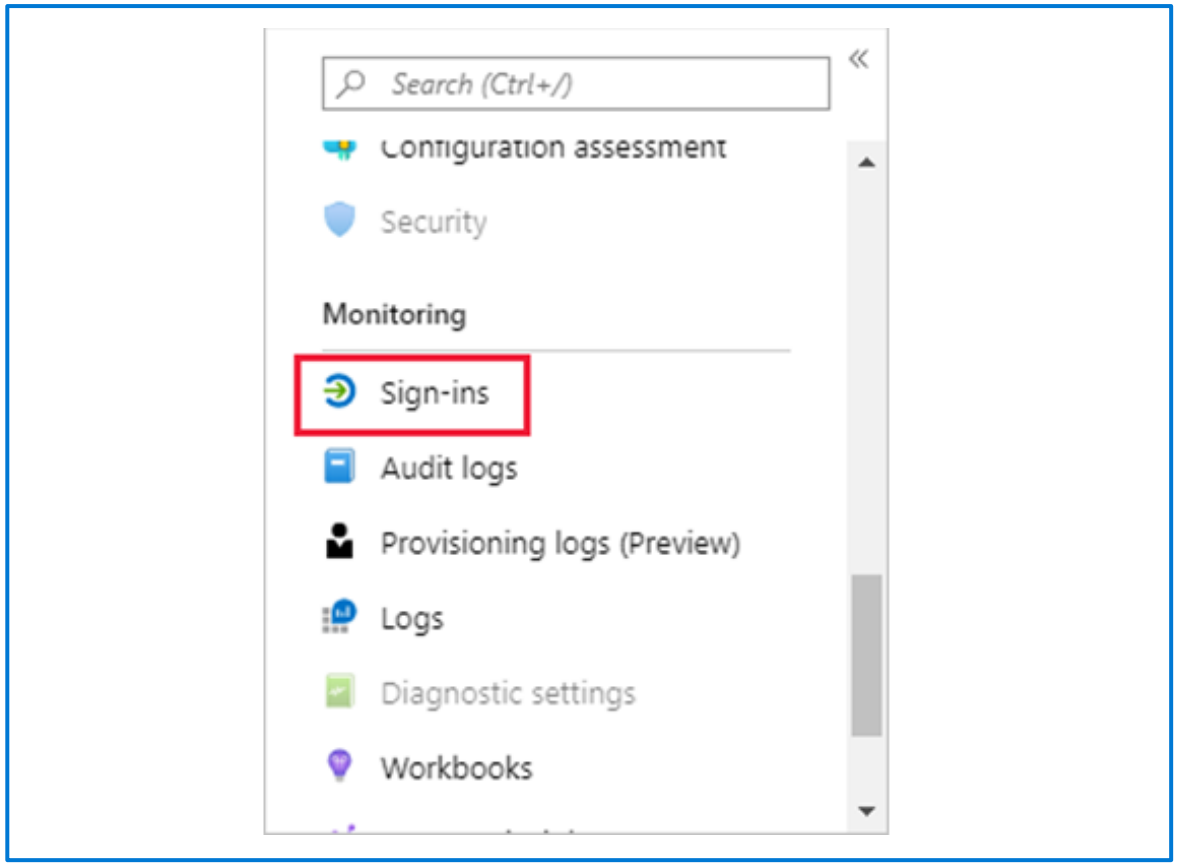
- **Risky sign-ins:** indicator of odd sign-in behavior
- **Users flagged for risk:** indicator an account might be compromised

Access this information by going to:

Azure Portal → Azure AD → Monitoring menu

Sign-ins report

First, narrow down the reported data to a level that works for you. Second, filter sign-in data using date field as default filter.



Download sign-in activities

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

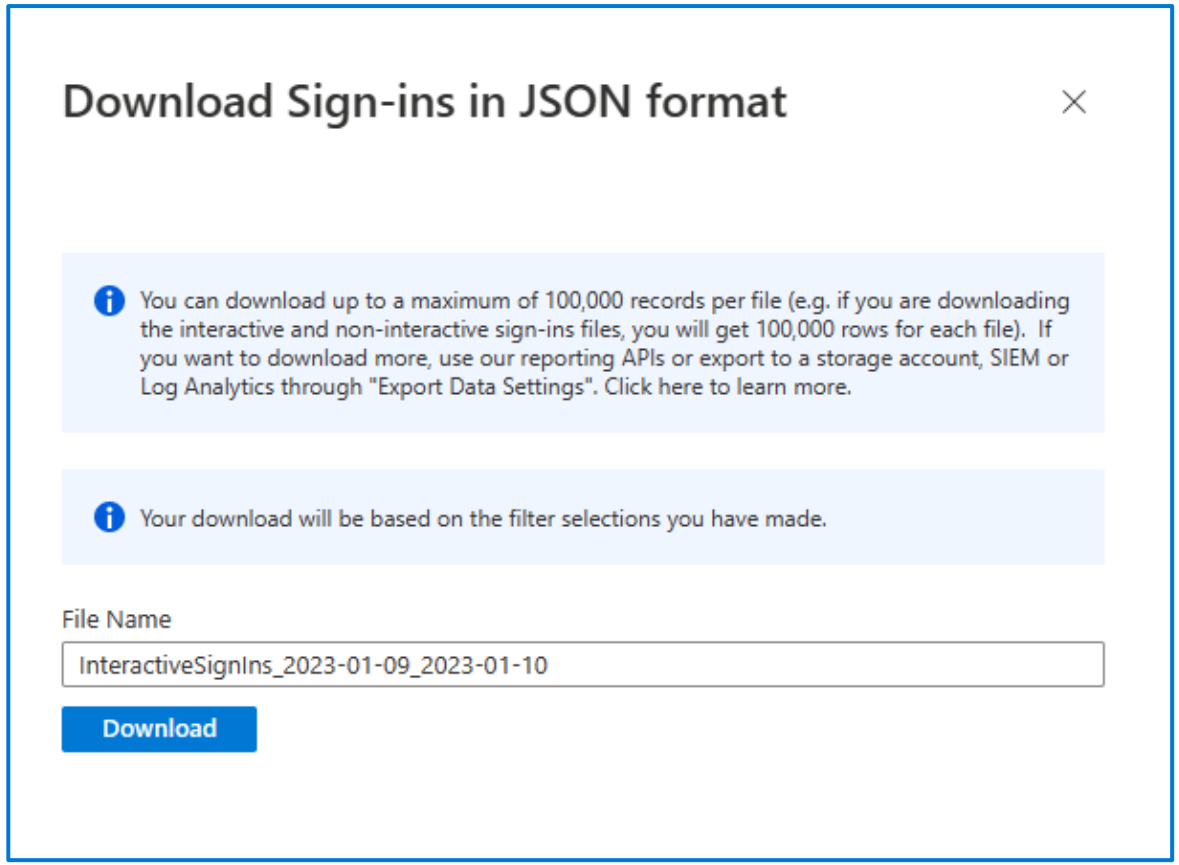
- What is the sign-in pattern of a user?
- How many users have signed in over a week?
- What's the status of these sign-ins?

File formats available:

- CSV or JSON

Available records:

- 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

LA

Azure

VM

AMA

LA

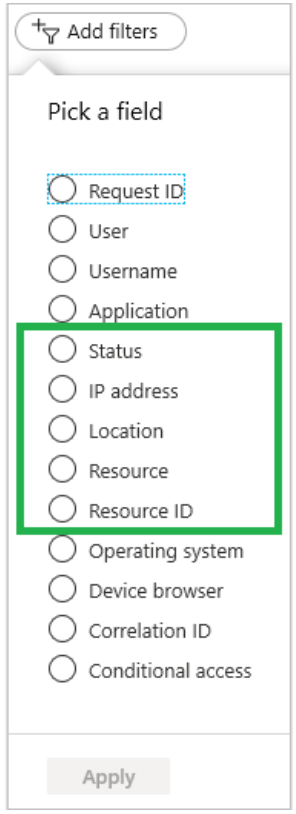
Connector

Sentinel

LA

SC-200!

KQL

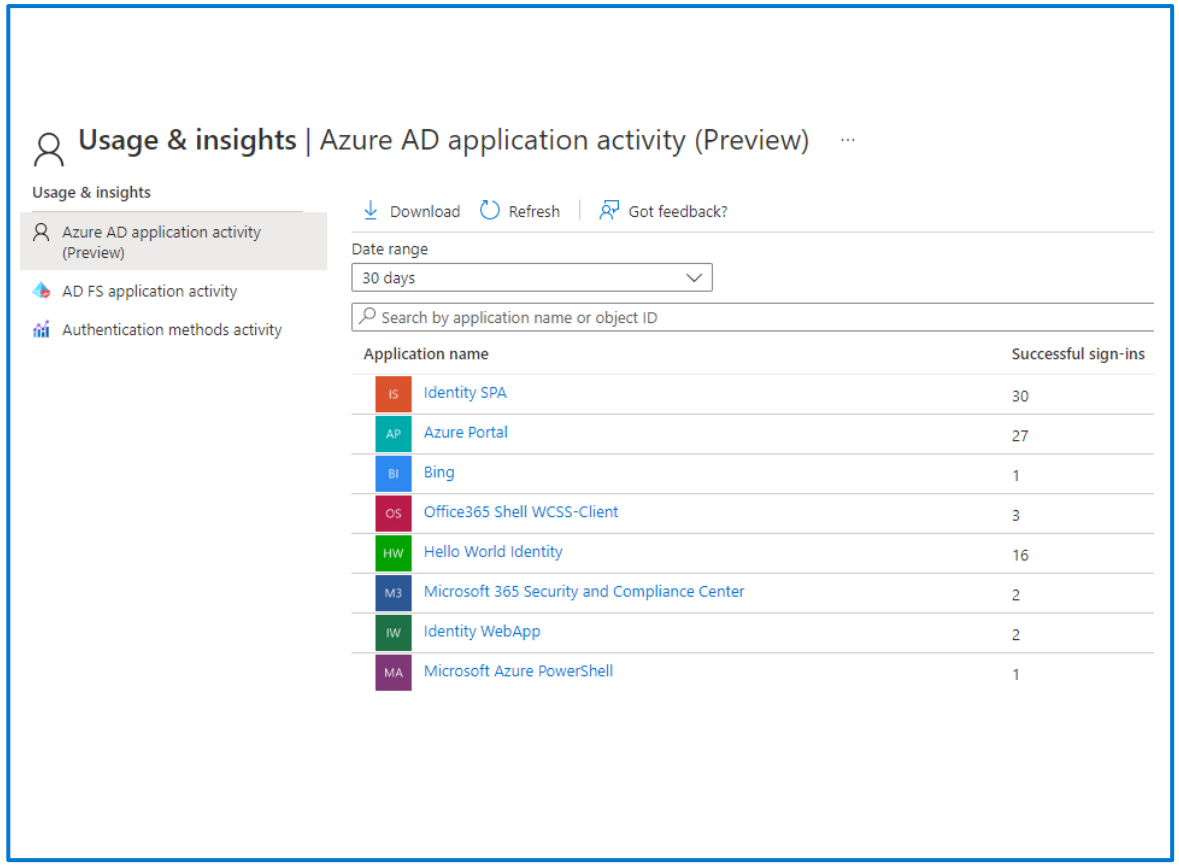


Sign-In Activity for Managed Applications

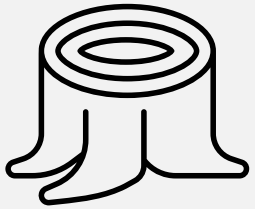
With an application-centric view of your sign-in data, you can answer questions such as:

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

The entry point to this data is the top three applications in your organization. The data is contained within the last 30 days report in the **Overview** section under **Enterprise applications**



Review and monitor Azure AD audit logs



Audit logs

The Azure AD audit logs provide records of system activities for compliance. To access the audit report, select **Audit logs** in the **Monitoring** section of **Azure Active Directory**

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

- 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 an activity

Filtering audit-logs

Service filter

- AAD Management UX
- Access Reviews
- Account Provisioning
- Application Proxy
- Authentication Methods
- B2C
- 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…

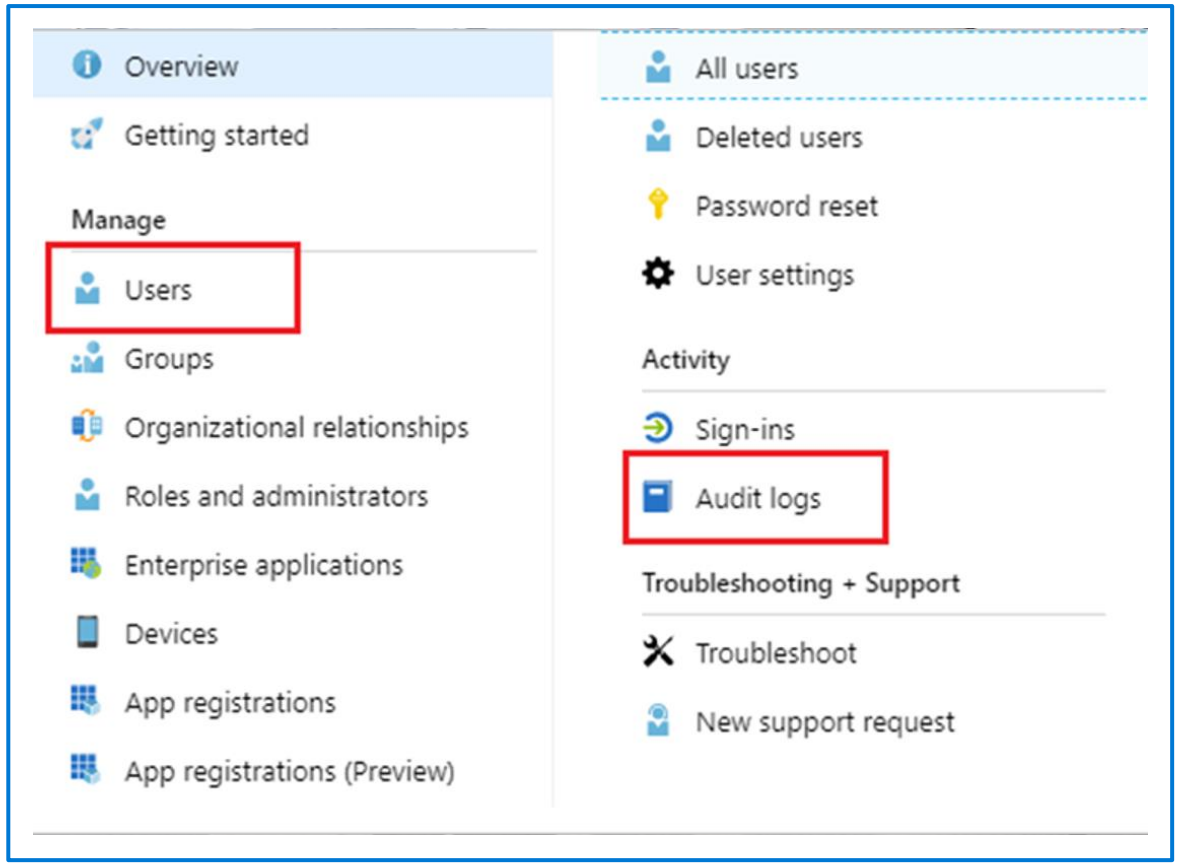
Activity filter

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:

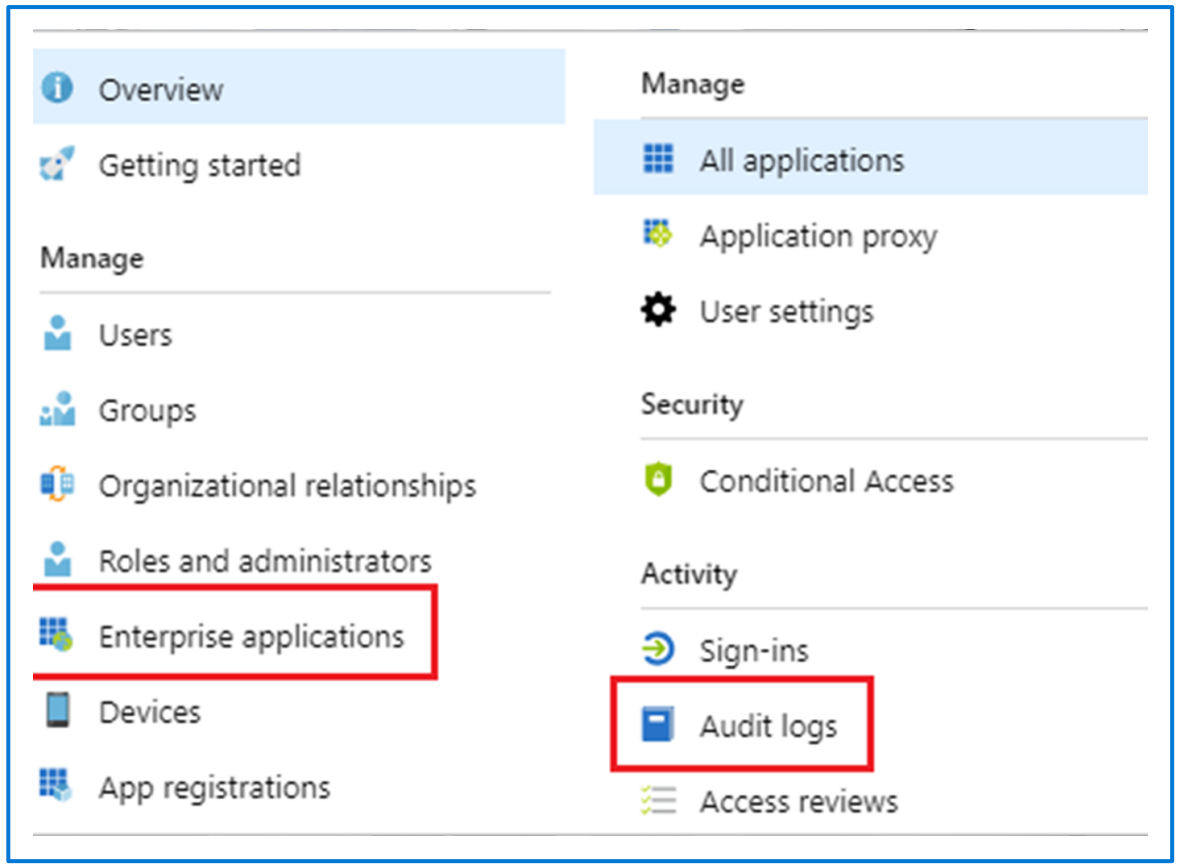
- What types of updates have been applied to users?
- How many users were changed?
- How many passwords were changed?
- What has an administrator done in a directory?
- What are the groups that have been added?
- Are there groups with membership changes?
- Have the owners of a group been changed?
- What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

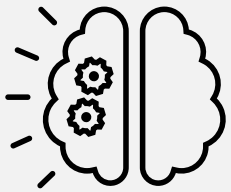
- What applications have been added or updated?
- What applications have been removed?
- Has a service principal for an application changed?
- Have the names of applications been changed?
- Who gave consent to an application?



Microsoft 365 activity logs

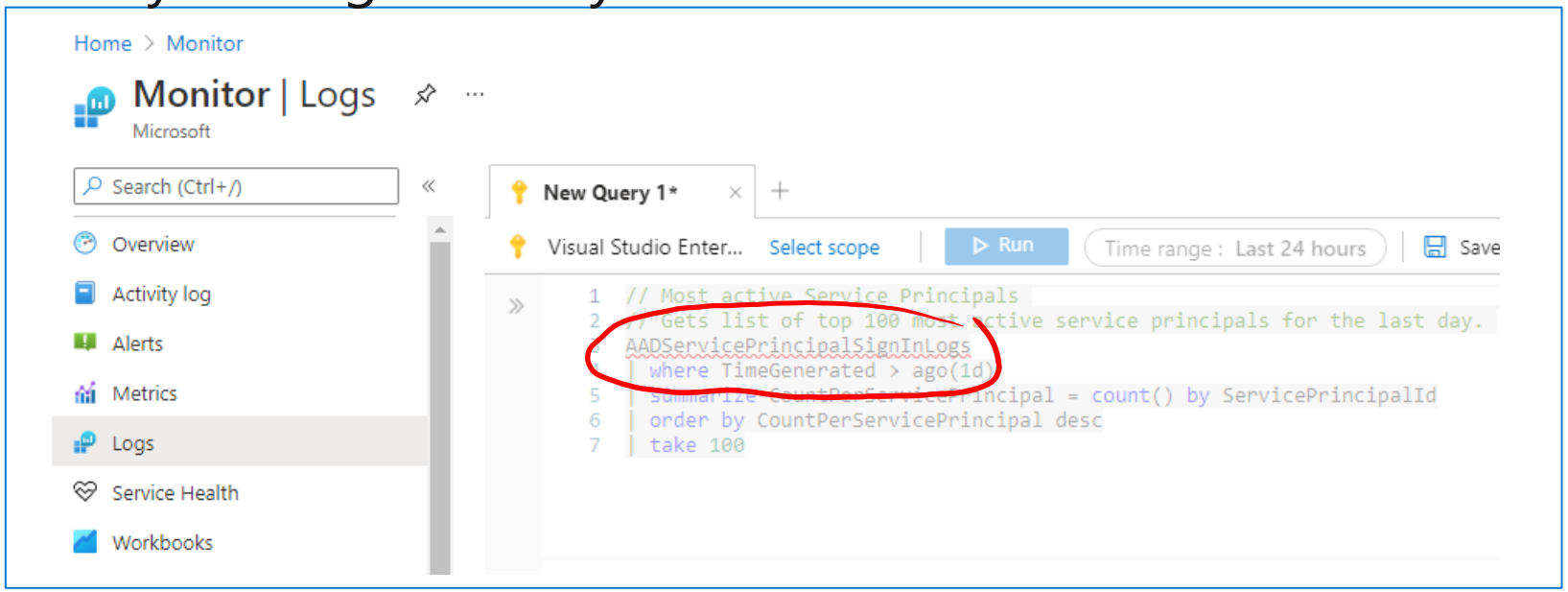
Logs can be viewed from the Microsoft 365 admin center. Only the Microsoft 365 admin center provides a full view of the Microsoft 365 activity logs

Enable and integrate Azure AD diagnostic logs with Log Analytics / Microsoft Sentinel

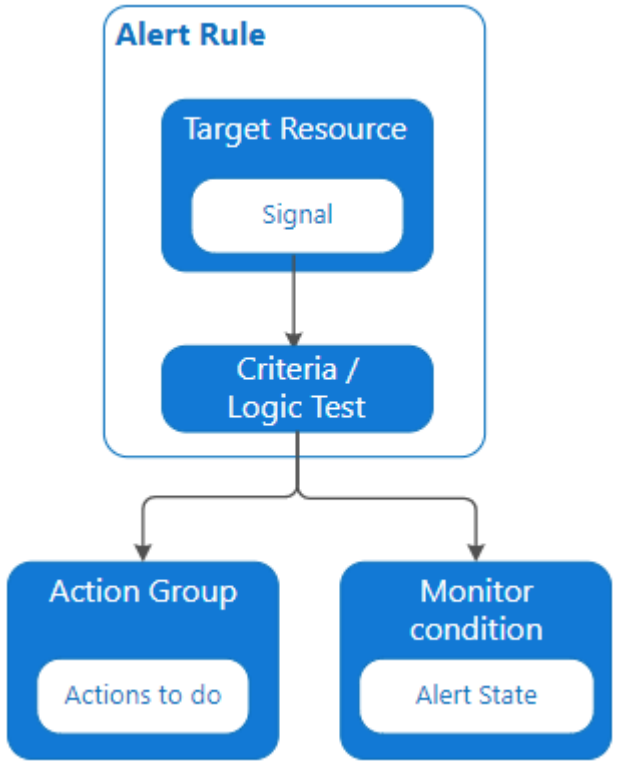


What is Log Analytics

Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor Logs and interactively analyze their results. 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

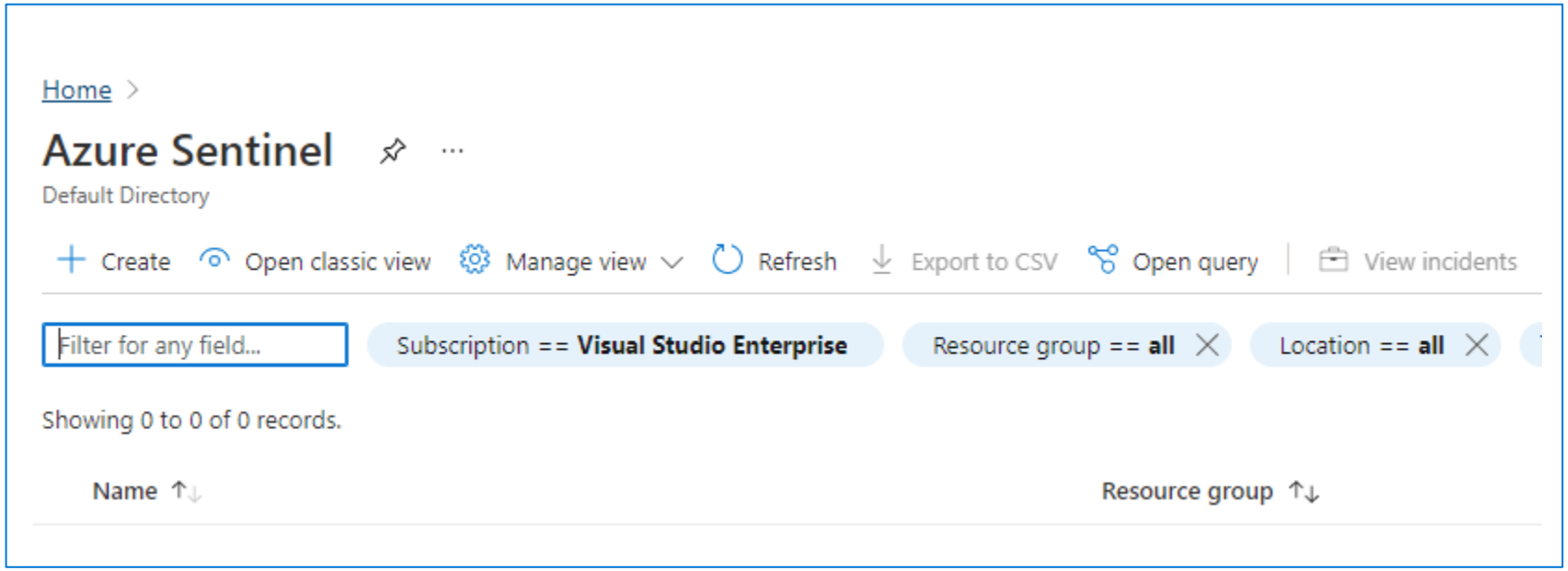


Alerts proactively notify you when issues are found with your infrastructure or application using your monitoring data in Azure Monitor.

- Watch virtual machines, storage accounts, and other sources for events or thresholds.
  - Possible early warning of an attack
- Set actions and alert 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.



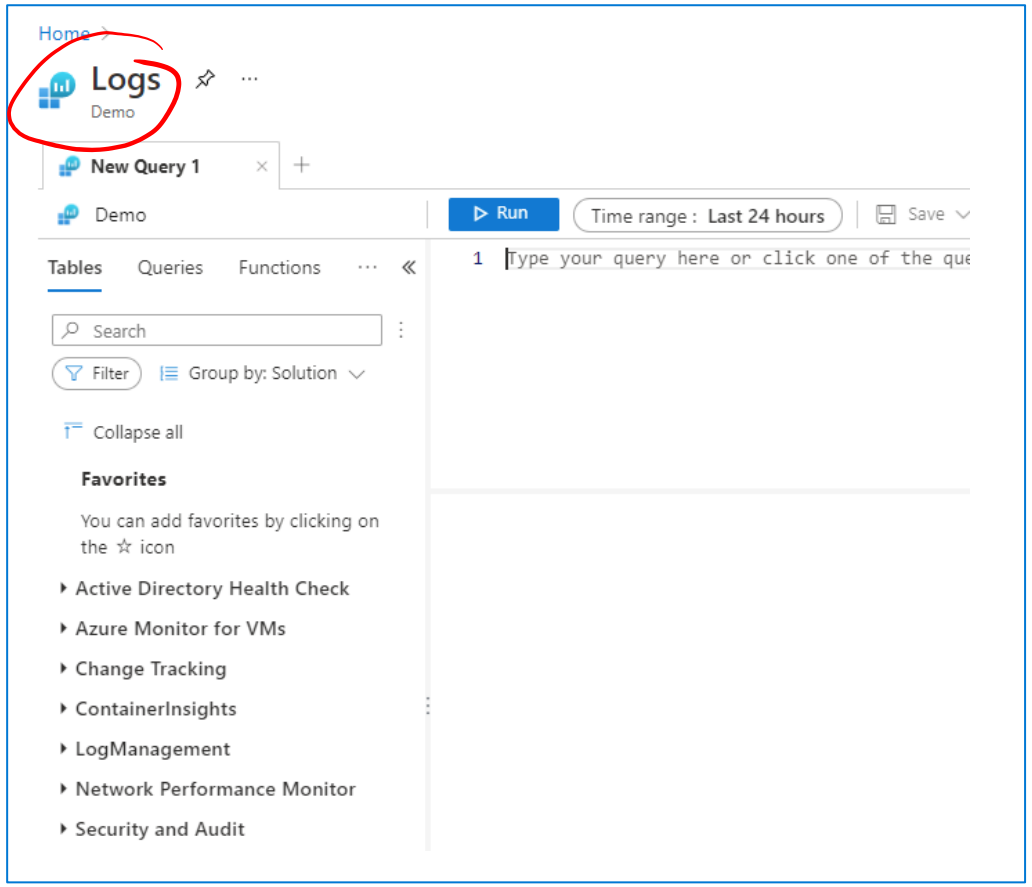
Connecting Azure AD logs into Log Analytics

Azure Monitor → Logs → Queries

Select your Subscription

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

AAD license required



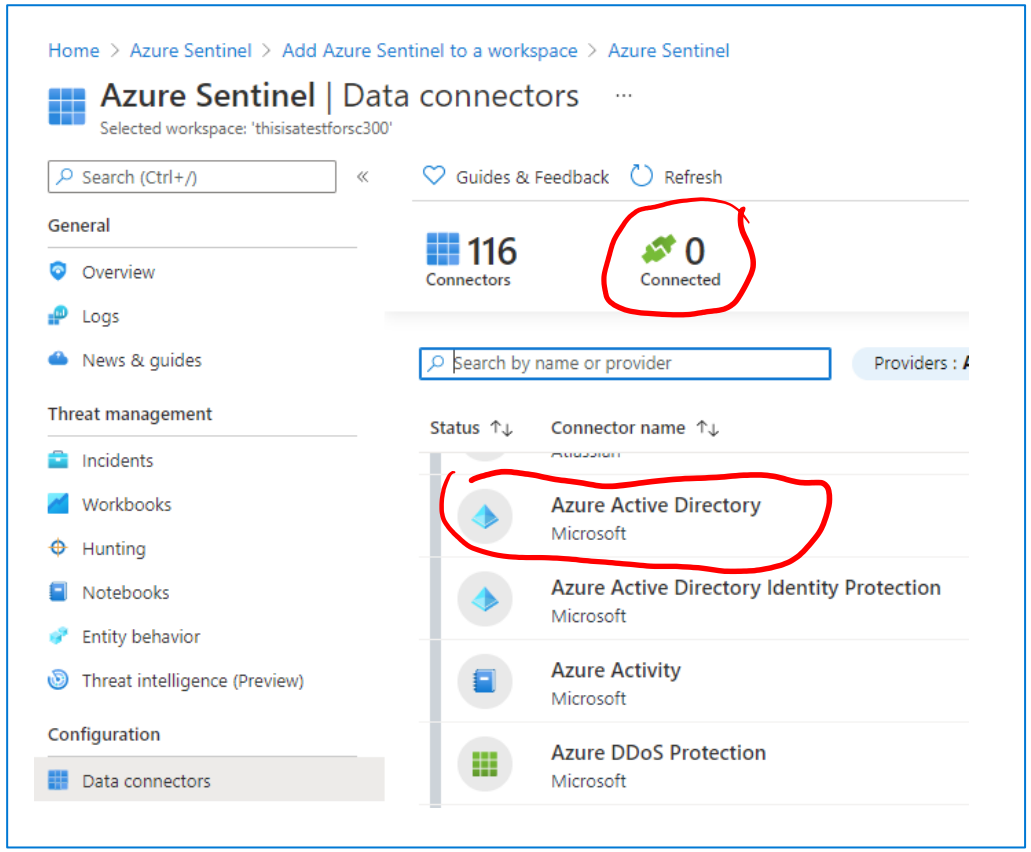
Connecting Azure AD logs into Microsoft Sentinel

Microsoft Sentinel → Data Connectors

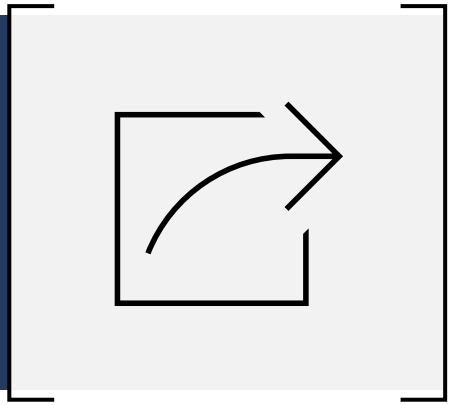
Set up or use a Workspace

Azure Active Directory
- Sign-in Logs and Audit Logs

Azure AD license required



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



Introduction to SIEM

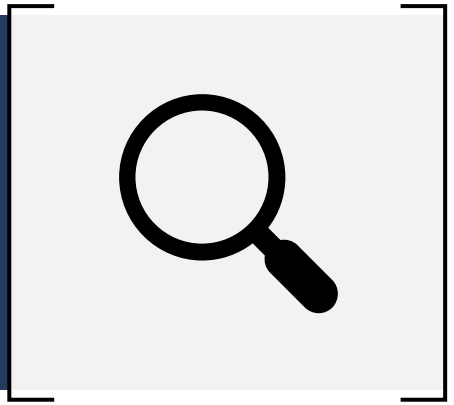
Security information and event management (SIEM) is a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications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

Example of a few 3rd 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 Azure Active Directory workbooks / reporting



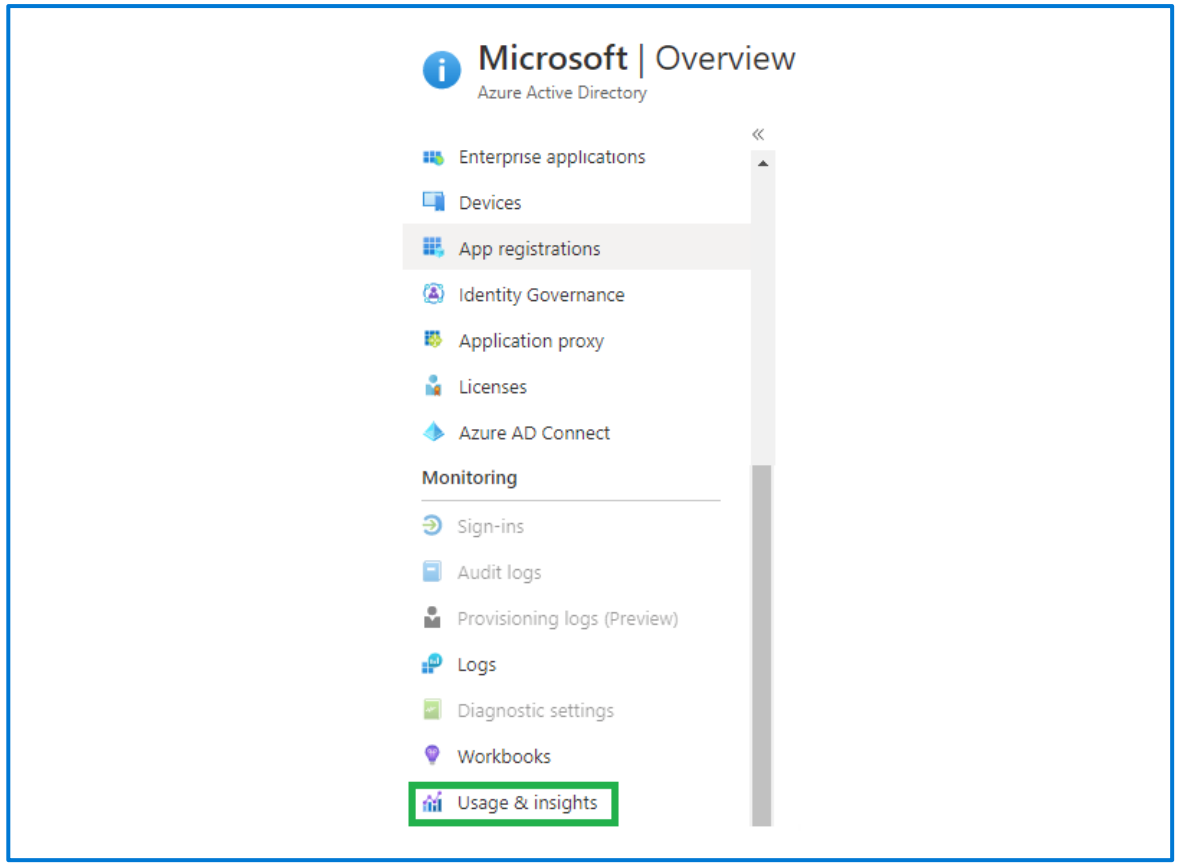
Analyze Azure AD with Usage and Insights

Explore 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

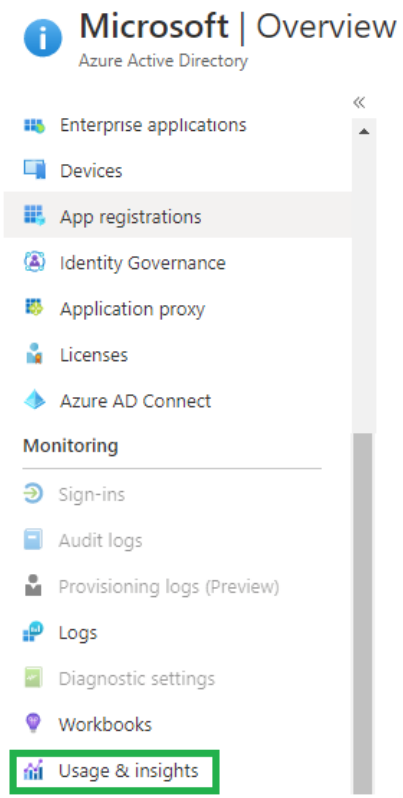
Many other items



Analyze Azure Active Directory usage and insights reporting

With the usage and insights report, you can get an application-centric view of your sign-in data. You can find answers to the following questions:

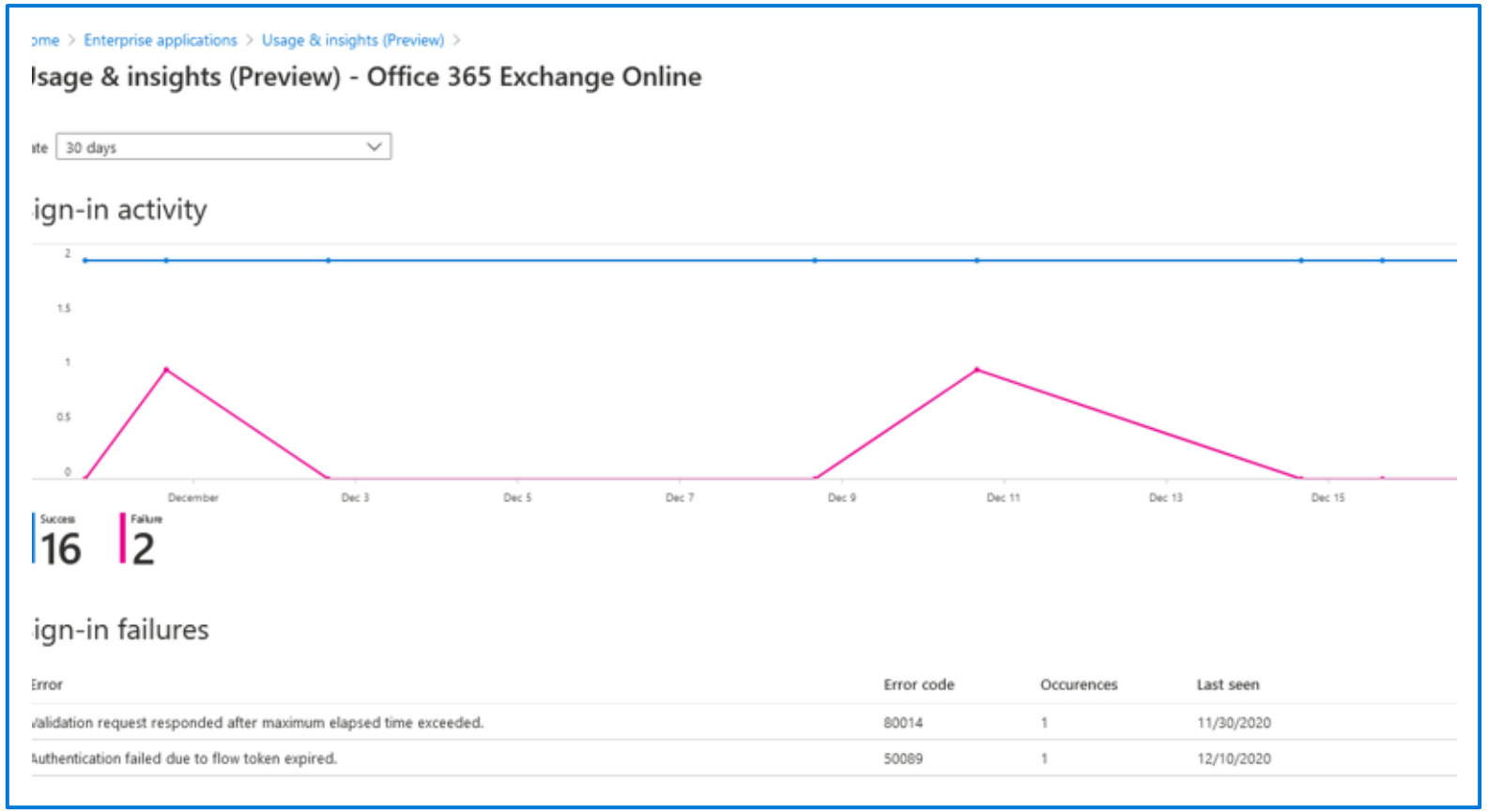
- What are the most used applications in my organization?
- What applications have the most failed sign-ins?
- What are the top sign-in errors for each application?



Usage report

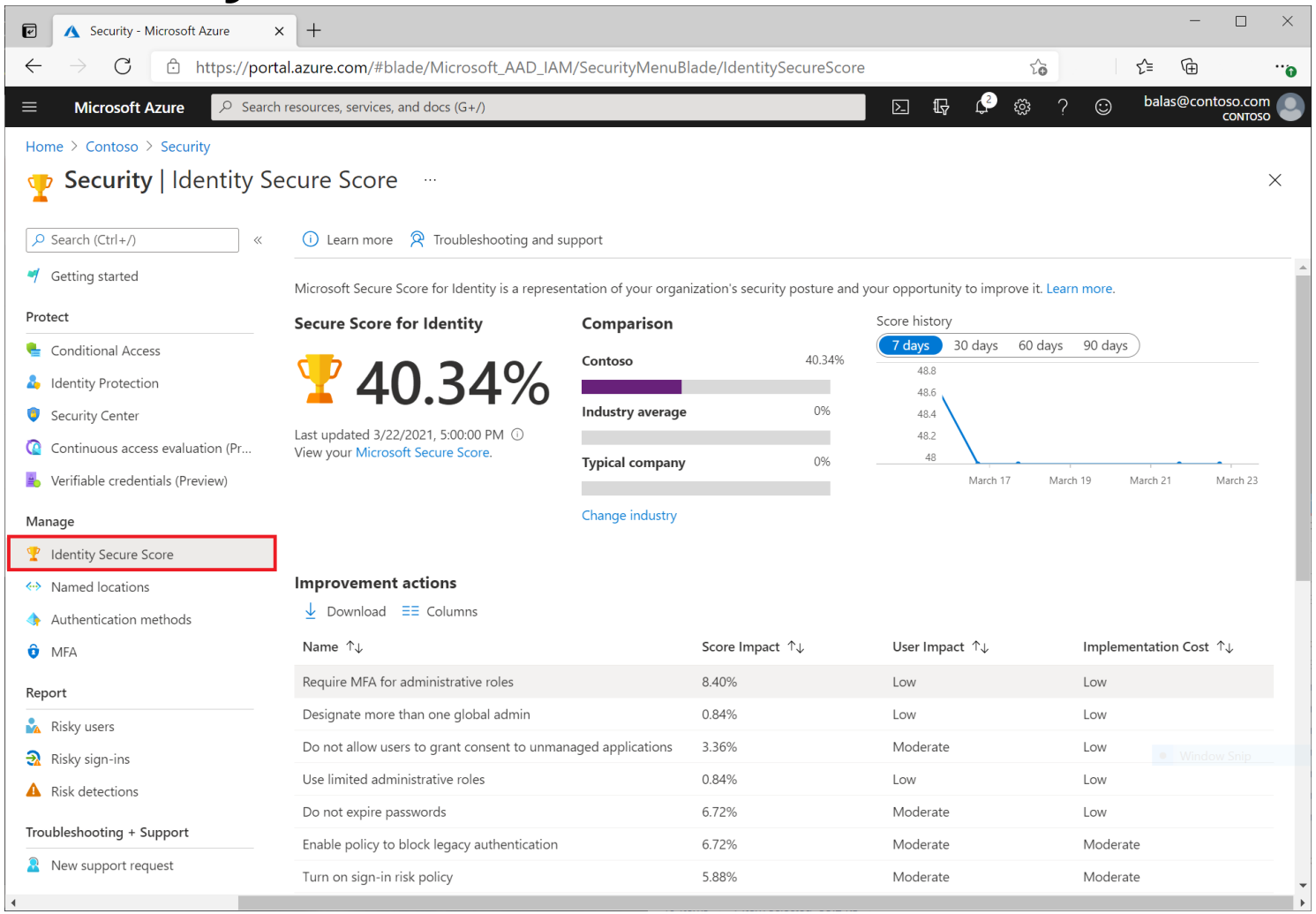
Usage and insights report:
Shows the number of sign-in attempts and the success rate

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 is Identity Secure Score in Azure AD



Using the 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 (like reading reports). Some actions are scored for partial completion, like enabling multi-factor authentication (MFA) for your users. Your 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

In this section you learned how to:

- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Azure AD audit logs
- Enable and integrate Azure AD diagnostic logs with Log Analytics/Microsoft Sentinel
- Export sign-in and audit logs to a third-party SIEM
- Review Azure AD activity by using Log Analytics/Microsoft Sentinel, excluding KQL use
- Analyze Azure Active Directory workbooks/reporting

Summary

Entitlement Management

- Catalogs
- Access Packages
- Assign entitlements
- Manage 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
- Configure PIM for resources
- Audit and manage PIM
- Break-glass accounts

Monitor and maintain Azure AD

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

Labs

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

End of presentation