

Microsoft Entra monitoring and health documentation

Learn how to access and use logs, reports, monitoring integrations, workbooks, and recommendations in Microsoft Entra ID.

About Identity monitoring and health

OVERVIEW

[What is Identity monitoring and health?](#)

[What are Identity Recommendations?](#)

[What are Identity Workbooks?](#)

CONCEPT

[Audit logs](#)

[Sign-in logs](#)

[Provisioning logs](#)

Identity logs and reports

CONCEPT

[Microsoft Entra Health](#)

[Usage and Insights report](#)

[Activity log schemas](#)

HOW-TO GUIDE

[Access activity logs in the Microsoft Entra admin center](#)

[Access logs with Microsoft Graph](#)

[Customize and filter logs](#)

[Download logs](#)

Identity logs and Azure Monitor logs



[Configure diagnostic settings](#)

[Integrate activity logs with Azure Monitor logs](#)

[Analyze activity logs in Azure Monitor logs](#)

[Stream logs to an event hub](#)

Common troubleshooting scenarios



[Common user sign-in errors](#)

[Manage inactive user accounts in Microsoft Entra ID](#)

[Troubleshoot sign-in errors](#)

[View Conditional Access details in the sign-in logs](#)

What is Microsoft Entra monitoring and health?

Article • 10/04/2024

The features of Microsoft Entra monitoring and health provide a comprehensive view of identity related activity in your environment. This data enables you to:

- Determine how your users utilize your apps and services.
- Detect potential risks affecting the health of your environment.
- Troubleshoot issues preventing your users from getting their work done.
- Gain insights by seeing audit events of changes to your Microsoft Entra directory.

Sign-in and audit logs comprise the activity logs behind many Microsoft Entra reports, which can be used to analyze, monitor, and troubleshoot activity in your tenant. Routing your activity logs to an analysis and monitoring solution provides greater insights into your tenant's health and security.

This article describes the types of activity logs available in Microsoft Entra ID, the reports that use the logs, and the monitoring services available to help you analyze the data.

Identity activity logs

Activity logs help you understand the behavior of users in your organization. There are three types of activity logs in Microsoft Entra ID:

- **Audit logs** include the history of every task performed in your tenant.
- **Sign-in logs** capture the sign-in attempts of your users and client applications.
- **Provisioning logs** provide information around users provisioned in your tenant through a third party service.

The activity logs can be viewed in the Azure portal or using the Microsoft Graph API. Activity logs can also be routed to various endpoints for storage or analysis. To learn about all of the options for viewing the activity logs, see [How to access activity logs](#).

Audit logs

Audit logs provide you with records of system activities for compliance. This data enables you to address common scenarios such as:

- Someone in my tenant got access to an admin group. Who gave them access?
- I want to know the list of users signing into a specific app because I recently onboarded the app and want to know if it's doing well.
- I want to know how many password resets are happening in my tenant.

Sign-in logs

The sign-in logs enable you to find answers to questions such as:

- 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?

Provisioning logs

You can use the provisioning logs to find answers to questions like:

- What groups were successfully created in ServiceNow?
- What users were successfully removed from Adobe?
- What users from Workday were successfully created in Active Directory?

Identity reports

Reviewing the data in the Microsoft Entra activity logs can provide helpful information for IT administrators. To streamline the process of reviewing data on key scenarios, we've created several reports on common scenarios that use the activity logs.

- [Identity Protection](#) uses sign-in data to create reports on risky users and sign-in activities.
- Activity related to your applications, such as service principal and app credential activity, are used to create reports in [Usage and insights](#).
- [Microsoft Entra workbooks](#) provide a customizable way to view and analyze the activity logs.
- Use [Microsoft Entra recommendations](#) to monitor and improve your tenant's security.
- [Microsoft Entra Health](#) capture global service level agreement attainment and health signals for several key scenarios.

Identity monitoring and tenant health

Reviewing Microsoft Entra activity logs is the first step in maintaining and improving the health and security of your tenant. You need to analyze the data, monitor on risky scenarios, and determine where you can make improvements. Microsoft Entra monitoring provides the necessary tools to help you make informed decisions.

Monitoring Microsoft Entra activity logs requires routing the log data to a monitoring and analysis solution. Endpoints include Azure Monitor logs, Microsoft Sentinel, or a third-party solution third-party Security Information and Event Management (SIEM) tool.

- Stream logs to an event hub to integrate with third-party SIEM tools.
- Integrate logs with Azure Monitor logs.
- Analyze logs with Azure Monitor logs and Log Analytics.

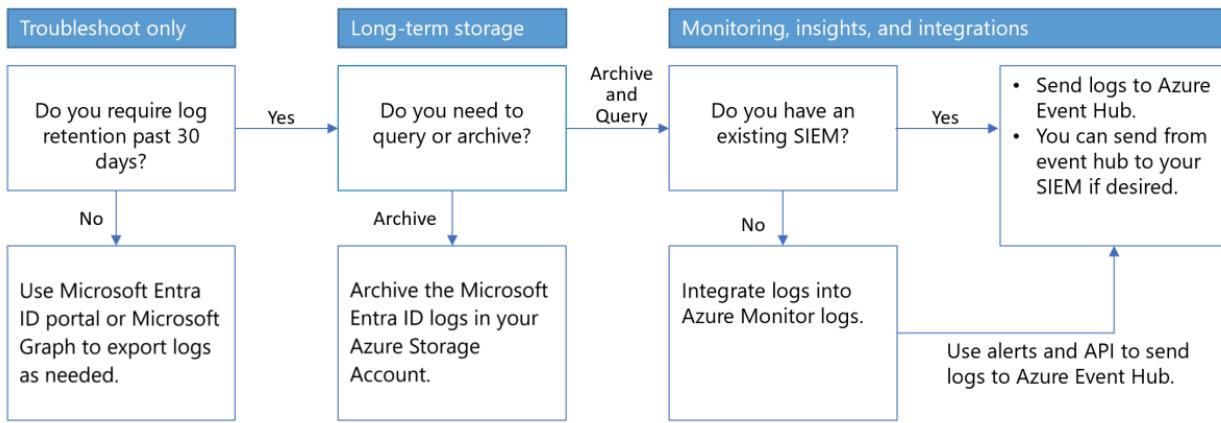
Use cases

How you use the logs, reports, and monitoring services available depends on your organization's needs. To better prioritize the use cases and solutions, it might help to see how these solutions are related to each other, how they differ, and how they can be used together.

Considerations

- **Retention** - Log retention: store audit logs and sign in logs of Microsoft Entra longer than 30 days
- **Analytics** - Logs are searchable with analytic tools
- **Operational and security insights** - Provide access to application usage, sign-in errors, self-service usage, trends, and so on.
- **SIEM integration** - Integrate and stream Microsoft Entra sign-in logs and audit logs to SIEM systems

With Microsoft Entra monitoring, you can route Microsoft Entra activity logs and retain them for long-term reporting and analysis to gain environment insights, and integrate it with SIEM tools. Use the following decision flow chart to help select an architecture.



For an overview of how to access, store, and analyze activity logs, see [How to access activity logs](#).

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)

What are Microsoft Entra recommendations?

Article • 04/15/2025

Keeping track of all the settings and resources in your tenant can be overwhelming. The Microsoft Entra recommendations feature helps monitor the status of your tenant so you don't have to. These recommendations help ensure your tenant is in a secure and healthy state while also helping you maximize the value of the features available in Microsoft Entra ID.

Microsoft Entra recommendations now include *Identity Secure Score* recommendations. These recommendations provide similar insights into the security of your tenant. For more information, see [What is Identity Secure Score](#).

All these Microsoft Entra recommendations provide you with personalized insights with actionable guidance to:

- Help you identify opportunities to implement best practices for Microsoft Entra related features.
- Improve the state of your Microsoft Entra tenant.
- Optimize the configurations for your scenarios.

This article gives you an overview of how you can use Microsoft Entra recommendations.

How does it work?

On a daily basis, Microsoft Entra ID analyzes the configuration of your tenant. During this analysis, Microsoft Entra ID compares the configuration of your tenant with security best practices and recommendation data. If a recommendation is flagged as applicable to your tenant, the recommendation appears in the **Recommendations** section of the Microsoft Entra identity overview area.

Each recommendation contains a description, a summary of the value of addressing the recommendation, and a step-by-step action plan. If applicable, impacted resources associated with the recommendation are listed, so you can resolve each affected area. If a recommendation doesn't have any associated resources, the impacted resource type is *Tenant level*, so your step-by-step action plan impacts the entire tenant and not just a specific resource.

Recommendations overview table

The recommendations listed in the following table are currently available in public preview or general availability the types of resources addressed by the recommendation, and more. The license requirements for recommendations in public preview are subject to change. The table provides links to available documentation for those recommendations that required separate guidance.

[Expand table](#)

Recommendation	Impacted resources	Availability	Identity Secure Score	Target roles for email notifications
AAD Connect Deprecated	Tenant	Preview	No	Hybrid Identity Administrator
Convert per-user MFA to Conditional Access MFA	Users	Generally available	No	Security Administrator

Recommendation	Impacted resources	Availability	Identity Secure Score	Target roles for email notifications
Designate more than one Global Administrator	Users	Generally available	Yes	Global Administrator
Do not allow users to grant consent to unreliable applications	Tenant	Generally available	Yes	Global Administrator
Do not expire passwords	Tenant	Generally available	Yes	Global Administrator
Enable password hash sync if hybrid	Tenant	Generally available	Yes	Hybrid Identity Administrator
Enable policy to block legacy authentication	Users	Generally available	Yes	Conditional Access Administrator, Security Administrator
Enable self-service password reset	Users	Generally available	Yes	Authentication Policy Administrator
Ensure all users can complete multifactor authentication	Users	Generally available	Yes	Conditional Access Administrator, Security Administrator
Migrate applications from AD FS to Microsoft Entra ID	Applications	Generally available	No	Application Administrator, Authentication Administrator Hybrid Identity Administrator
Migrate applications from the retiring Azure AD Graph APIs to Microsoft Graph	Applications	Preview	No	Application Administrator
Migrate from ADAL to MSAL	Applications	Generally available	No	Application Administrator
Migrate from MFA server to Microsoft Entra MFA	Tenant	Generally Available	No	Global Administrator
Migrate service principals from the retiring Azure AD Graph APIs to Microsoft Graph	Applications	Preview	No	Application Administrator
Migrate to Microsoft Authenticator	Users	Preview	No	Global Administrator

Recommendation	Impacted resources	Availability	Identity Secure Score	Target roles for email notifications
Minimize MFA prompts from known devices	Users	Generally available	No	Global Administrator
Protect all users with a sign-in risk policy	Users	Generally available	Yes	Conditional Access Administrator, Security Administrator
Protect all users with a user risk policy	Users	Generally available	Yes	Conditional Access Administrator, Security Administrator
Protect your tenant with Insider Risk Conditional Access policy	Users	Generally available	Yes	Conditional Access Administrator, Security Administrator
Remove unused applications	Applications	Preview	No	Application Administrator
Remove unused credentials from applications	Applications	Preview	No	Application Administrator
Renew expiring application credentials	Applications	Preview	No	Application Administrator
Renew expiring service principal credentials	Applications	Preview	No	Application Administrator
Require MFA for administrative roles	Users	Generally available	Yes	Conditional Access Administrator, Security Administrator
Review inactive users with Access Reviews	Users	Preview	No	Identity Governance Administrator
Secure and govern your apps with automatic user and group provisioning	Applications	Preview	No	Application Administrator, IT Governance Administrator
Use least privileged administrative roles	Users	Generally available	Yes	Privileged Role Administrator
Verify App Publisher	Applications	Preview	No	Global Administrator

Microsoft Entra only displays the recommendations that apply to your tenant, so you might not see all supported recommendations listed.

Identity Secure Score

Your Identity Secure Score, which appears at the top of the page, is a numerical representation of the health of your tenant. Recommendations that apply to the Identity Secure Score are given individual scores in the table at the bottom of the page. You can filter the list of recommendations to only the Identity Secure Score recommendations using the **Security** filter card. Identity Secure Score recommendations include *secure score points*, which are calculated as an overall score based on several security factors.

These scores add up to generate your Identity Secure Score. For more information, see [What is Identity Secure Score](#).

The screenshot shows the Microsoft Entra Recommendations interface. At the top, there are tabs for Overview, Monitoring, Properties, **Recommendations** (which is underlined), and Setup guides. Below the tabs, a message states: "Microsoft Entra ID recommendations identifies personalized opportunities for you to implement Microsoft Entra ID best practices. [Learn more](#)".

On the left, a box displays the **Identity Secure Score** as **80.48%**, with a note that it refreshes every 24 hours. A link to "View your Microsoft Secure Score" is provided. To the right is a "Score History" chart showing a steady score around 80% from December 2024 to January 2025.

Below these are three filter cards: "All" (14), "Security" (12, highlighted with a red box), and "Best practice" (2). A search bar and an "Add filter" button are also present.

The main area shows a table of 14 recommendations:

Priority	Recommendation	Required licenses	Release type	Secure Score points	Impacted resource type	Status
Medium	Protect your tenant with Inside...	Microsoft Entra ID P2	Generally available	0/5	Users	Active
High	Migrate Service Principals from...	Microsoft Entra ID Free	Preview	N/A	Applications	Active
High	Protect all users with a user risk...	Microsoft Entra ID P2	Preview	7/7	Users	Completed

Are Microsoft Entra recommendations related to Azure Advisor?

The Microsoft Entra recommendations feature is the Microsoft Entra specific implementation of [Azure Advisor](#), which is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. Azure Advisor analyzes your resource configuration and usage data to recommend solutions that can help you improve the cost effectiveness, performance, reliability, and security of your Azure resources.

Microsoft Entra recommendations use similar data to support you with the roll-out and management of Microsoft's best practices for Microsoft Entra tenants to keep your tenant in a secure and healthy state. The Microsoft Entra recommendations feature provides a holistic view into your tenant's security, health, and usage.

Email notifications (preview)

Microsoft Entra recommendations now generate email notifications when a new recommendation is generated. This new preview feature sends emails to a predetermined set of roles for each recommendation. For example, recommendations that are associated with the health of your tenant's applications are sent to users who have the Application Administrator role.

If your organization is using Privileged Identity Management (PIM), the recipients must be elevated to the role indicated in order to receive the email notification. If no one is actively assigned to the role, no emails are sent. For this reason, we recommend checking the recommendations regularly to ensure that you're aware of any new recommendations.

What are Microsoft Entra workbooks?

Article • 02/25/2025

As an IT admin, you might need to see your Microsoft Entra tenant data as a visual representation that enables you to understand how your identity management environment is doing. This article gives you an overview of how you can use Azure Workbooks for Microsoft Entra ID to analyze your Microsoft Entra tenant data.

With Azure Workbooks for Microsoft Entra ID, you can:

- Query data from multiple sources in Azure
- Visualize data for reporting and analysis
- Combine multiple elements into a single interactive experience

Workbooks are found in Microsoft Entra ID and in Azure Monitor. The concepts, processes, and best practices are the same for both types of workbooks. Workbooks for Microsoft Entra ID, however, cover only those identity management scenarios that are associated with Microsoft Entra ID. Sign-ins, Conditional Access, multifactor authentication, and Identity Protection are scenarios included in the Workbooks for Microsoft Entra ID.

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with various categories like Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, Monitoring & health, and Workbooks. The 'Monitoring & health' and 'Workbooks' items are highlighted with red boxes. The main content area is titled 'Gallery' under 'Azure Active Directory'. It shows a 'Quick start' section with an 'Empty' workbook (a completely empty workbook). Below it are sections for 'Recently modified workbooks (0)' (No items found) and 'Usage (11)' which includes tiles for Sign-ins using Legacy Auth..., Sign-ins, Access Package Activity, Application Role Assignment, App Consent Audit, SSPR Reset Funnel, Sign-In Analysis (Preview: ...), Identity Protection Risk An..., Authentication Prompts A..., Tenant restriction insights, Cross-tenant access activity, Conditional Access Insight..., Continuous access evaluat..., and Sign-ins by Conditional Ac... . At the bottom, there is a section for 'Conditional access (5)' with tiles for Conditional Access Insight..., Continuous access evaluat..., and Sign-ins by Conditional Ac... . The top navigation bar includes a search bar, a user profile icon, and various administrative icons.

For more information on workbooks for other Azure services, see [Azure Monitor workbooks](#).

How does it help me?

Workbooks are highly customizable, so you can make workbooks for any scenario. Public templates are added frequently, which provide a great starting point. Common scenarios for using workbooks include:

- Get shareable, at-a-glance summary reports about your Microsoft Entra tenant, and build your own custom reports.
- Find and diagnose sign-in failures, and get a trending view of your organization's sign-in health.
- Monitor Microsoft Entra logs for sign-ins, tenant administrator actions, provisioning, and risk together in a flexible, customizable format.
- Watch trends in your tenant's usage of Microsoft Entra features such as Conditional Access, self-service password reset, and more.
- Know who's using legacy authentications to sign in to your environment.
- Understand the effect of your Conditional Access policies on your users' sign-in experience.

Who should use it?

Because of the ability to customize workbooks, they can benefit many types of users. Typical personas that use workbooks are:

- **Reporting admin:** Someone who is responsible for creating reports on top of the available data and workbook templates
- **Tenant admins:** People who use the available reports to get insight and take action.
- **Workbook template builder:** Someone who "graduates" from the role of reporting admin by turning a workbook into a template for others with similar needs to use as a basis for creating their own workbooks.

Public workbook templates

Public workbook templates are built, updated, and deprecated to reflect the needs of customers and the current Microsoft Entra services. Detailed guidance is available for several Microsoft Entra public workbook templates.

- [Authentication prompts analysis](#)

- Conditional Access gap analyzer
- Cross-tenant access activity
- Multifactor authentication gaps
- Risk analysis
- Sensitive Operations Report
- Sign-ins using legacy authentication

Related content

- Learn how to use Azure Workbooks for Microsoft Entra ID
 - Create your own workbook
 - Create a Log Analytics workspace
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

What are Microsoft Entra audit logs?

Article • 01/31/2025

Microsoft Entra activity logs include audit logs, which is a comprehensive report on every logged event in Microsoft Entra ID. Changes to applications, groups, users, and licenses are all captured in the Microsoft Entra audit logs.

Two other activity logs are also available to help monitor the health of your tenant:

- [Sign-ins](#) – Information about sign-ins and how your resources are used by your users.
- [Provisioning](#) – Activities performed by the provisioning service, such as the creation of a group in ServiceNow or a user imported from Workday.

This article gives you an overview of the audit logs, such as the information they provide and what kinds of questions they can answer.

What can you do with audit logs?

Audit logs in Microsoft Entra ID provide access to system activity records, often needed for compliance. You can get answers to questions related to users, groups, and applications.

Users:

- What types of changes were recently applied to users?
- How many users were changed?
- How many passwords were changed?

Groups:

- What groups were recently added?
- Have the owners of group been changed?
- What licenses are to a group or a user?

Applications:

- What applications were, updated, or removed?
- Has a service principal for an application changed?
- Have the names of applications been changed?

Custom security attributes:

- What changes were made to [custom security attribute](#) definitions or assignments?
- What updates were made to attribute sets?
- What custom attribute values were assigned to a user?

ⓘ Note

Entries in the audit logs are system generated and can't be changed or deleted.

What do the logs show?

Audit logs display several valuable details on the activities in your tenant. For a full list of the available audit activities, see [Audit activity reference](#). The Microsoft Entra admin center defaults to the **Directory** tab, which displays the following information:

- 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)

A second tab for **Custom Security** displays audit logs for custom security attributes. To view data on this tab, you must have the [Attribute Log Administrator](#) or [Attribute Log Reader](#) role. This audit log shows all activities related to custom security attributes. For more information, see [What are custom security attributes](#).

Date	Service	Category	Activity
2/1/24, 10:30:57 AM	Account Provisioning	ProvisioningManagement	Import
2/1/24, 10:30:53 AM	PIM	RoleManagement	Add member to role complete...
2/1/24, 10:30:53 AM	Core Directory	RoleManagement	Add member to role
2/1/24, 10:30:52 AM	PIM	RoleManagement	Add member to role requested...
2/1/24, 10:30:02 AM	Account Provisioning	ProvisioningManagement	Import
2/1/24, 10:28:54 AM	Core Directory	UserManagement	Update user
2/1/24, 10:26:29 AM	Account Provisioning	ProvisioningManagement	Import

Microsoft 365 activity logs

You can view Microsoft 365 activity logs from the [Microsoft 365 admin center](#). Even though Microsoft 365 activity and Microsoft Entra activity logs share many directory resources, only the Microsoft 365 admin center provides a full view of the Microsoft 365 activity logs.

You can also access the Microsoft 365 activity logs programmatically by using the [Office 365 Management APIs](#).

Most standalone or bundled Microsoft 365 subscriptions have back-end dependencies on some subsystems within the Microsoft 365 datacenter boundary. The dependencies require some information write-back to keep directories in sync and essentially to help enable hassle-free onboarding in a subscription opt-in for Exchange Online. For these write-backs, audit log entries show actions taken by "Microsoft Substrate Management." These audit log entries refer to create/update/delete operations executed by Exchange Online to Microsoft Entra ID. The entries are informational and don't require any action.

Related content

- [Audit activity reference](#)
- [Access activity logs](#)
- [Customize and filter activity logs](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

What are Microsoft Entra sign-in logs?

Article • 11/11/2024

Microsoft Entra logs all sign-ins into a Microsoft Entra tenant, which includes your internal apps and resources. As an IT administrator, you need to know what the sign-in log details mean, so that you can interpret the log values correctly.

Reviewing sign-in errors and patterns provides valuable insight into how your users access applications and services. The sign-in logs provided by Microsoft Entra ID are a powerful type of [activity log](#) that you can analyze. This article describes several key aspects of the sign-in logs.

Two other activity logs are also available to help monitor the health of your tenant:

- **Audit** – Information about changes applied to your tenant, such as users and group management or updates applied to your tenant's resources.
- **Provisioning** – Activities performed by a provisioning service, such as the creation of a group in ServiceNow or a user imported from Workday.

What can you do with sign-in logs?

You can use the sign-in logs to answer questions such as:

- How many users signed into a particular application this week?
- How many failed sign-in attempts occurred in the last 24 hours?
- Are users signing in from specific browsers or operating systems?
- Which of my Azure resources were accessed by managed identities and service principals?

You can also describe the activity associated with a sign-in request by identifying the following details:

- **Who** – The identity (User) performing the sign-in.
- **How** – The client (Application) used for the sign-in.
- **What** – The target (Resource) accessed by the identity.

How do you access the sign-in logs?

There are several ways to access the logs, depending on your needs. For more information, see [How to access activity logs](#).

To view the sign-in logs from the Microsoft Entra admin center:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Sign-in logs**.

To more effectively use the sign-in logs in the Microsoft Entra admin center, adjust the filters to only view a specific set of logs. For more information, see [Filter sign-in logs](#).

What are the types of sign-in logs?

There are four types of logs in the sign-in logs preview:

- [Interactive user sign-ins](#)
- [Non-interactive user sign-ins](#)
- [Service principal sign-ins](#)
- [Managed identity sign-ins](#)

The classic sign-in logs only include interactive user sign-ins.

 **Note**

Entries in the sign-in logs are system generated and can't be changed or deleted.

Sign-in data used by other services

Sign-in data is used by several services in Azure and Microsoft Entra to monitor risky sign-ins, provide insight into application usage, and more.

Microsoft Entra ID Protection

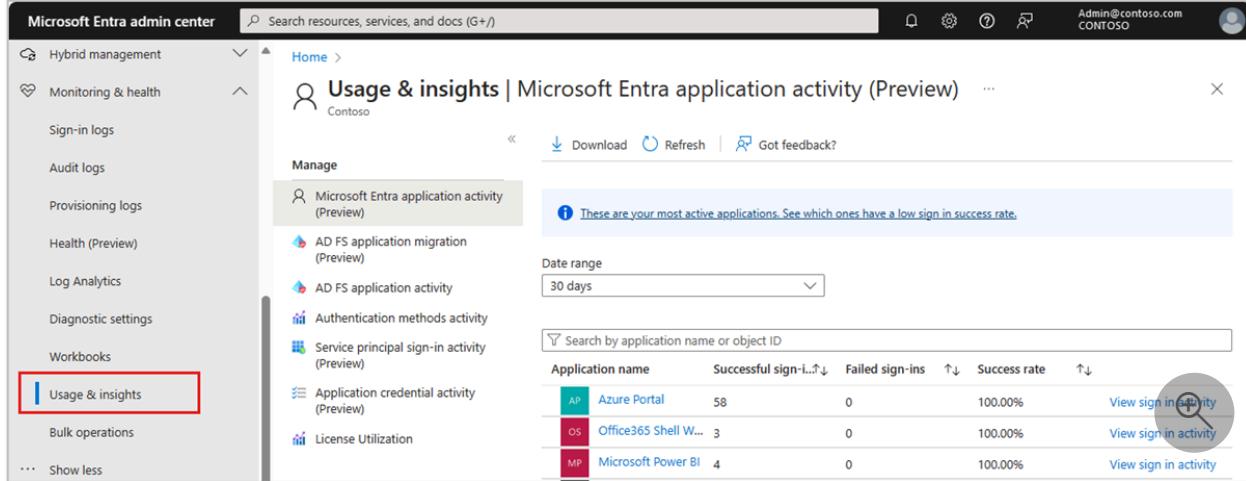
Sign-in log data visualization that relates to risky sign-ins is available in the [Microsoft Entra ID Protection](#) overview, which uses the following data:

- Risky users
- Risky user sign-ins
- Risky workload identities

For more information about the Microsoft Entra ID Protection tools, see the [Microsoft Entra ID Protection overview](#).

Microsoft Entra Usage and insights

To view application-specific sign-in data, browse to **Microsoft Entra ID > Monitoring & health > Usage & insights**. These reports provide a closer look at sign-ins for Microsoft Entra application activity and AD FS application activity. For more information, see [Microsoft Entra Usage & insights](#).



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with various management options like Hybrid management, Monitoring & health, and Usage & insights (which is highlighted with a red box). The main content area is titled "Usage & insights | Microsoft Entra application activity (Preview)". It includes a "Manage" section with a search bar and a list of activity types: Microsoft Entra application activity (Preview), AD FS application migration (Preview), AD FS application activity, Authentication methods activity, Service principal sign-in activity (Preview), Application credential activity (Preview), and License Utilization. Below this is a table showing application activity data:

Application name	Successful sign-ins	Failed sign-ins	Success rate	Action
Azure Portal	58	0	100.00%	View sign in activity
Office365 Shell W...	3	0	100.00%	View sign in activity
Microsoft Power BI	4	0	100.00%	View sign in activity

There are several reports available in **Usage & insights**. Some of these reports are in preview.

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

Microsoft 365 activity logs

You can view Microsoft 365 activity logs from the [Microsoft 365 admin center](#). Microsoft 365 activity and Microsoft Entra activity logs share a significant number of directory resources. Only the Microsoft 365 admin center provides a full view of the Microsoft 365 activity logs.

You can access the Microsoft 365 activity logs programmatically by using the [Office 365 Management APIs](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

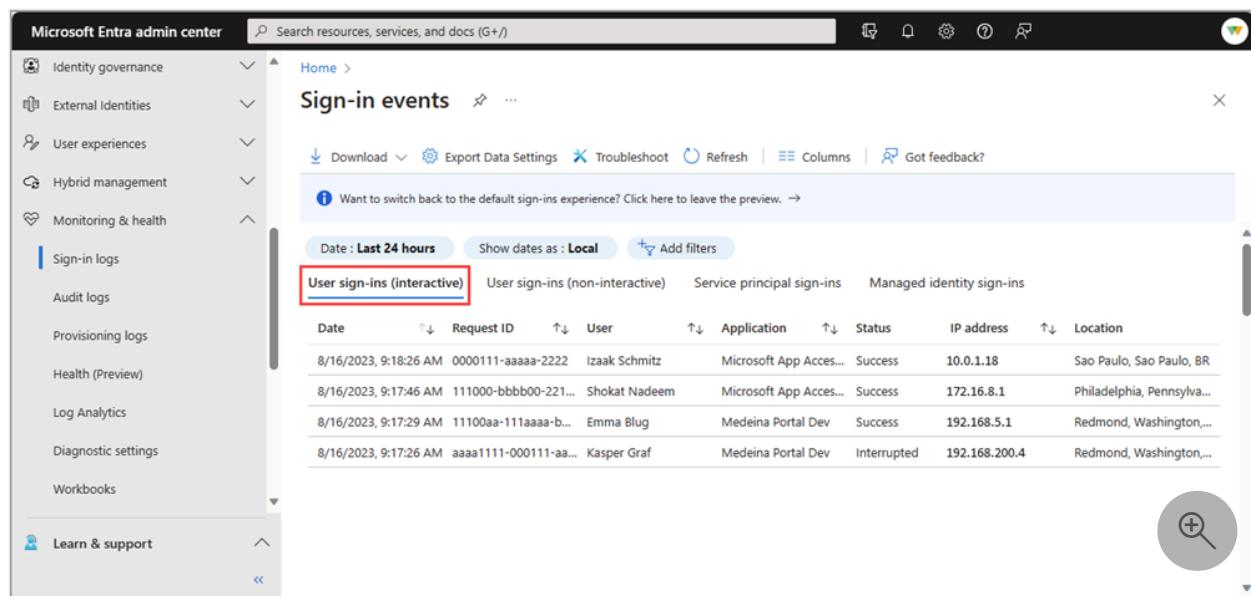
What are interactive user sign-ins in Microsoft Entra?

Article • 03/17/2025

Microsoft Entra monitoring and health provides several types of sign-in logs to help you monitor the health of your tenant. The interactive user sign-ins are the default view in the Microsoft Entra admin center.

What is an interactive user sign-in?

Interactive sign-ins are performed *by* a user. They provide an authentication factor to Microsoft Entra ID. That authentication factor could also interact with a helper app, such as the Microsoft Authenticator app. Users can provide passwords, responses to MFA challenges, biometric factors, or QR codes to Microsoft Entra ID or to a helper app. This log also includes federated sign-ins from identity providers that are federated to Microsoft Entra ID.



Date	Request ID	User	Application	Status	IP address	Location
8/16/2023, 9:18:26 AM	0000111-aaaa-2222	Izaak Schmitz	Microsoft App Acces...	Success	10.0.1.18	Sao Paulo, Sao Paulo, BR
8/16/2023, 9:17:46 AM	111000-bbbb00-221...	Shokat Nadeem	Microsoft App Acces...	Success	172.16.8.1	Philadelphia, Pennsylva...
8/16/2023, 9:17:29 AM	11100aa-111aaaa-b...	Emma Blug	Medeina Portal Dev	Success	192.168.5.1	Redmond, Washington,...
8/16/2023, 9:17:26 AM	aaaa1111-000111-aa...	Kasper Graf	Medeina Portal Dev	Interrupted	192.168.200.4	Redmond, Washington,...

Log details

The following examples show the type of information captured in the interactive user sign-in logs:

- A user provides username and password in the Microsoft Entra sign-in screen.
- A user passes an SMS MFA challenge.
- A user provides a biometric gesture to unlock their Windows PC with Windows Hello for Business.

- A user is federated to Microsoft Entra ID with an AD FS SAML assertion.

In addition to the default fields, the interactive sign-in logs also show:

- The sign-in location
- Whether Conditional Access was applied
- Cross-tenant access details, such as home and resource tenant IDs

 **Note**

Entries in the sign-in logs are system generated and can't be changed or deleted.

Special considerations

Partner access to downstream tenant resources

The interactive sign-in logs now include details about when a partner accesses a downstream tenant's resources. By looking at the **Cross tenant access type**, **Home tenant ID**, and **Resource tenant ID** columns, which are now visible by default, you can see when a partner logs into a downstream tenant resource.

- Filter on **Service Provider** in the **Cross tenant access type** column to isolate events related to partner sign-ins.
- Compare the details in the **Home tenant ID** and **Resource tenant ID** columns to identify sign-ins coming from your partner's tenant to the downstream tenant.

Non-interactive sign-ins on the interactive sign-in logs

Previously, some non-interactive sign-ins from Microsoft Exchange clients were included in the interactive user sign-in log for better visibility. This increased visibility was necessary before the non-interactive user sign-in logs were introduced in November 2020. However, it's important to note that some non-interactive sign-ins, such as those using FIDO2 keys, might still be marked as interactive due to the way the system was set up before the separate non-interactive logs were introduced. These sign-ins might display interactive details like client credential type and browser information, even though they're technically non-interactive sign-ins.

Passthrough sign-ins

Microsoft Entra ID issues tokens for authentication and authorization. In some situations, a user who is signed in to the Contoso tenant might try to access resources in the Fabrikam tenant, where they don't have access. A no-authorization token called a passthrough token, is issued to the Fabrikam tenant. The passthrough token doesn't allow the user to access any resources.

Previously, when reviewing the logs for this situation, the sign-in logs for the home tenant (in this scenario, Contoso) didn't show a sign-in attempt because *the token wasn't granting access to a resource with any claims*. The sign-in token was only used to display the appropriate failure message.

Passthrough sign-in attempts now appear in the home tenant sign-in logs and any relevant tenant restriction sign-in logs. This update provides more visibility into user sign-in attempts from your users and deeper insights into your tenant restriction policies.

The `crossTenantAccessType` property now shows `passthrough` to differentiate passthrough sign-ins and is available in the Microsoft Entra admin center and Microsoft Graph.

First-party, app-only service principal sign-ins

The service principal sign-in logs don't include first-party, app-only sign-in activity. This type of activity happens when first-party apps get tokens for an internal Microsoft job where there's no direction or context from a user. We exclude these logs so you're not paying for logs related to internal Microsoft tokens within your tenant.

You might identify Microsoft Graph events that don't correlate to a service principal sign-in if you're routing `MicrosoftGraphActivityLogs` with `SignInLogs` to the same Log Analytics workspace. This integration allows you to cross reference the token issued for the Microsoft Graph API call with the sign-in activity. The `UniqueTokenIdentifier` for sign-in logs and the `SignInActivityId` in the Microsoft Graph activity logs would be missing from the service principal sign-in logs.

Conditional Access

Sign-ins that show **Not applied** for Conditional Access can be difficult to interpret. If the sign-in is interrupted, the sign-in appears on the logs but shows **Not applied** for Conditional Access. Another common scenario is signing in to Windows Hello for Business. This sign-in doesn't have Conditional Access applied because the user is signing in to the device, not to cloud resources protected by Conditional Access.

TimeGenerated field

If you're integrating your sign-in logs with Azure Monitor logs and Log Analytics, you might notice that the `TimeGenerated` field in the logs doesn't match the time the sign-in occurred. This discrepancy is due to the way the logs are ingested into Azure Monitor. The `TimeGenerated` field is the time the entry was received and published by Log Analytics, not the time the sign-in occurred. The `CreatedDateTime` field in the logs shows the time the sign-in occurred.

Similarly, risky sign-in events also display `TimeGenerated` as the time when the risky event was detected, not when the sign-in occurred. To find the actual sign-in time, you can use the `CorrelationId` to find the sign-in event in the logs and locate the sign-in time.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

What are non-interactive user sign-ins in Microsoft Entra?

Article • 03/17/2025

Microsoft Entra monitoring and health provides several types of sign-in logs to help you monitor the health of your tenant. Non-interactive sign-ins are a subset of the user sign-in logs in the Microsoft Entra admin center.

What is a non-interactive user sign-in?

Non-interactive sign-ins are done *on behalf of a user*. These delegated sign-ins were performed by a client app or OS components on behalf of a user and don't require the user to provide an authentication factor. Instead, Microsoft Entra ID recognizes when the user's token needs to be refreshed and does so behind the scenes, without interrupting the user's session. In general, the user perceives these sign-ins as happening in the background.

Date	Request ID	Username	Application	Status	IP address	Resource	Resource ID	Condition...	# sign ins
9/18/2024, 5:00:00	7777cccc-88dd-eaaa	bsaparkzy@wood...	Medina PIM	Success	10.0.0.3	Microsoft Graph	a0a0a0-bbbb-cccc...	Success	1
9/19/2024, 9:0	2222bbbb-33cc-aaaa	bsaparkzy@wood...	Medina PIM	Success	10.0.0.3	Microsoft Graph	a0a0a0-bbbb-cccc...	Success	1
9/19/2024, 9:0	0000aaaa-11bb-cccc	bsaparkzy@wood...	Medina PIM	Success	10.0.0.3	Microsoft Graph	a0a0a0-bbbb-cccc...	Success	1
> 9/18/2024, 5:00:00	5555eeee-66ff-gggg	bsaparkzy@wood...	ADlbitzaUX	Success	10.0.0.3	Microsoft Graph	a0a0a0-bbbb-cccc...	Success	1
9/18/2024, 5:00:00	Aggregate	lwyn@woodgrove...	Medina PIM	Success	172.16.33.8	Microsoft Graph	d3d3d3d3-eeee-ffff...	Success	4
9/19/2024, 9:0	8888ddd9-99ee-ffff	lwyn@woodgrove...	Medina PIM	Success	172.16.33.8	Microsoft Graph	d3d3d3d3-eeee-ffff...	Success	1
9/19/2024, 9:0	1111bbbb-22cc-dddd	lwyn@woodgrove...	Medina PIM	Success	172.16.33.8	Microsoft Graph	d3d3d3d3-eeee-ffff...	Success	1
9/19/2024, 9:0	4444ffff-55aa-bbbb	lwyn@woodgrove...	Medina PIM	Success	172.16.33.8	Microsoft Graph	d3d3d3d3-eeee-ffff...	Success	1
9/19/2024, 9:0	7777cccc-88dd-eaaa	lwyn@woodgrove...	Medina PIM	Success	172.16.33.8	Microsoft Graph	d3d3d3d3-eeee-ffff...	Success	1

Log details

The following examples show the type of information captured in the non-interactive user sign-in logs:

- A client app uses an OAuth 2.0 refresh token to get an access token.
- A client uses an OAuth 2.0 authorization code to get an access token and refresh token.

- A user performs single sign-on (SSO) to a web or Windows app on a Microsoft Entra joined PC (without providing an authentication factor or interacting with a Microsoft Entra prompt).
- A user signs in to a second Microsoft Office app while they have a session on a mobile device using FOCI (Family of Client IDs).

In addition to the default fields, the non-interactive sign-in log also shows:

- Resource ID
- Number of grouped sign-ins

You can't customize the fields shown in this report.

 **Note**

Entries in the sign-in logs are system generated and can't be changed or deleted.

How does it work?

To make it easier to digest the data, non-interactive sign-in events are grouped. Clients often create many non-interactive sign-ins on behalf of the same user in a short time period. The non-interactive sign-ins share the same characteristics except for the time the sign-in was attempted. For example, a client might get an access token once per hour on behalf of a user. If the state of the user or client doesn't change, the IP address, resource, and all other information is the same for each access token request. The only state that does change is the date and time of the sign-in.

Date	Request ID	Username	Application	Status	IP Address	Resource	Resource ID	Conditional Acc...	# sign ins
✓ 9/4/2024, 5:00:00 PM	Aggregate	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	7
9/5/2024, 11:51:56 AM	0000aaaa-11bb-cccc-	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	1
9/5/2024, 11:51:55 AM	5555eeee-66ff-gggg-	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	1
9/5/2024, 11:51:55 AM	8888dddd-99ee-ffff-0	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	1
9/5/2024, 11:51:55 AM	1111bbbb-22cc-dddd	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	1
9/5/2024, 11:51:55 AM	4444ffff-55aa-bb bb-6	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	1
9/5/2024, 11:51:55 AM	7777cccc-88dd-eeee-	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	1
9/5/2024, 11:51:55 AM	2222bbbb-33cc-aaaa-	sdeol@woodgrove...	Medeina Service Dev	Success	192.0.2.9	Microsoft Graph	00000003-0000-0000...	Success	1



When Microsoft Entra logs multiple sign-ins that are identical other than time and date, those sign-ins are from the same entity and are aggregated into a single row. A row with multiple identical sign-ins (except for date and time issued) has a value greater than one in the *# sign-ins* column. These aggregated sign-ins might also appear to have the same time stamps. The **Time aggregate** filter can set to 1 hour, 6 hours, or 24 hours. You can expand the row to see all the different sign-ins and their different time stamps.

Sign-ins are aggregated in the non-interactive users when the following data matches:

- Application
- User
- IP address
- Status
- Resource ID

 Note

The IP address of non-interactive sign-ins performed by [confidential clients](#) doesn't match the actual source IP of where the refresh token request is coming from. Instead, it shows the original IP used for the original token issuance.

Feedback

Was this page helpful?

 Yes

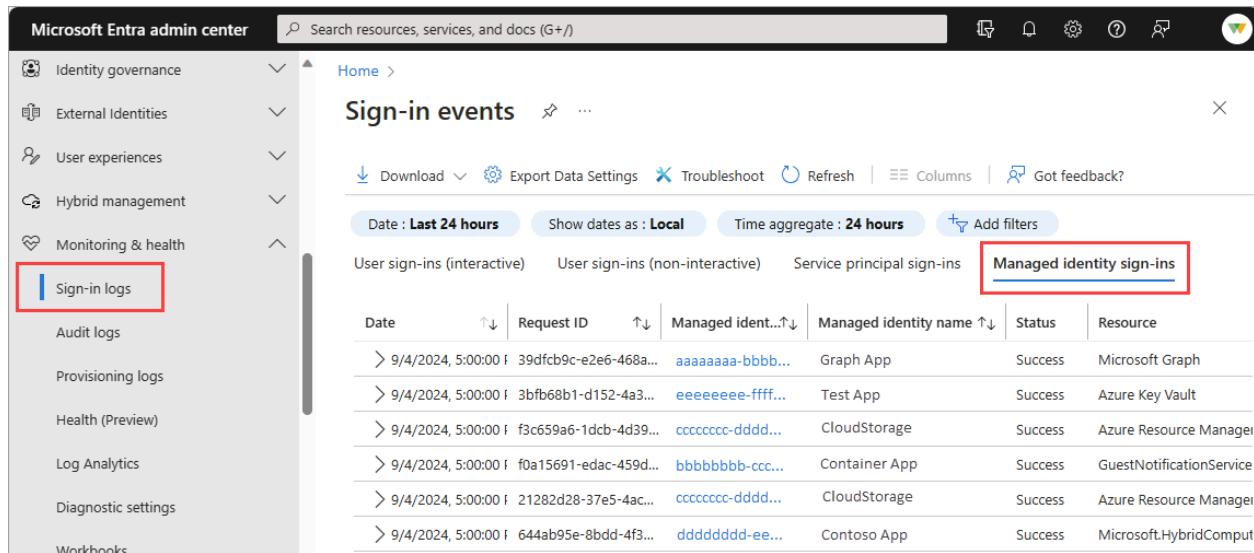
 No

[Provide product feedback ↗](#)

What are managed identity sign-ins in Microsoft Entra?

Article • 03/17/2025

Managed identities for Azure resources sign-ins are sign-ins that were performed by resources that have their secrets managed by Azure to simplify credential management. A VM with managed credentials uses Microsoft Entra ID to get an Access Token.



Date	Request ID	Managed ident...	Managed identity name	Status	Resource
> 9/4/2024, 5:00:00 I	39dfcb9c-e2e6-468a...	aaaaaaaa-bbbb...	Graph App	Success	Microsoft Graph
> 9/4/2024, 5:00:00 I	3bfb68b1-d152-4a3...	eeeeeeee-ffff...	Test App	Success	Azure Key Vault
> 9/4/2024, 5:00:00 I	f3c659a6-1dcb-4d39...	cccccccc-dddd...	CloudStorage	Success	Azure Resource Manager
> 9/4/2024, 5:00:00 I	f0a15691-edac-459d...	bbbbbbb-ccc...	Container App	Success	GuestNotificationService
> 9/4/2024, 5:00:00 I	21282d28-37e5-4ac...	ccccccc-ddd...	CloudStorage	Success	Azure Resource Manager
> 9/4/2024, 5:00:00 I	644ab95e-8bdd-4f3...	ddddddd-ee...	Contoso App	Success	Microsoft.HybridComput

You can't customize the fields shown in this report.

To make it easier to digest the data, these sign-in events are grouped together. Sign-ins from the same entity are aggregated into a single row. You can expand the row to see all the different sign-ins and their different time stamps. Sign-ins are aggregated in the managed identities report when all of the following data matches:

- Managed identity name or ID
- Status
- Resource name or ID

Select an item in the list view to display all sign-ins that are grouped under a node.

Select a grouped item to see all details of the sign-in.

ⓘ Note

Entries in the sign-in logs are system generated and can't be changed or deleted.

Feedback

Was this page helpful?

 Yes

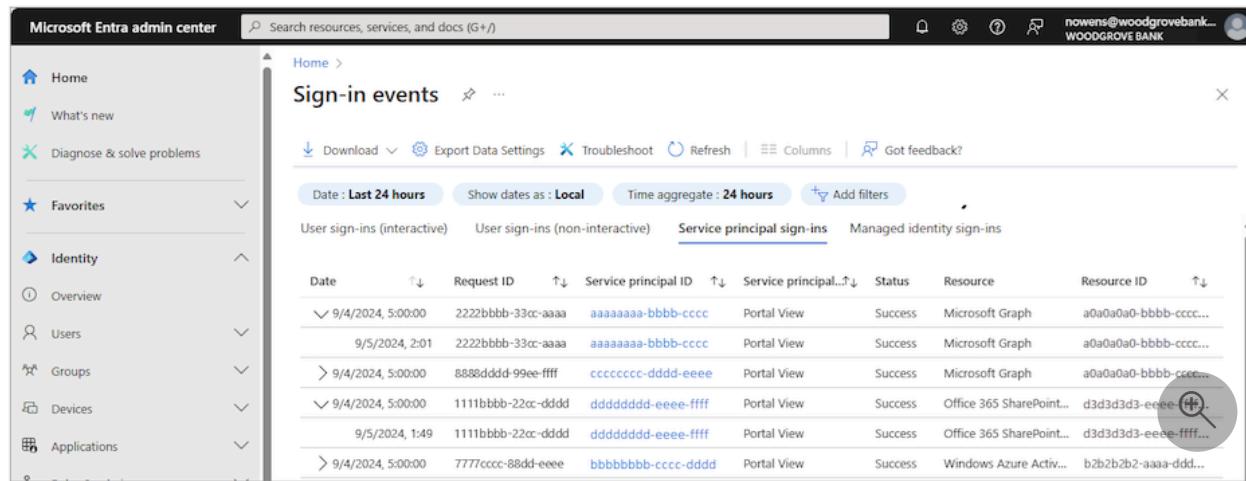
 No

Provide product feedback 

What are service principal sign-ins in Microsoft Entra?

Article • 03/17/2025

Unlike interactive and non-interactive user sign-ins, service principal sign-ins don't involve a user. Instead, they're sign-ins by any nonuser account, such as apps or service principals (except managed identity sign-in, which are included only in the managed identity sign-in log). In these sign-ins, the app or service provides its own credential, such as a certificate or app secret to authenticate or access resources.



Date	Request ID	Service principal ID	Status	Resource	Resource ID
9/4/2024, 5:00:00	2222bbbb-33cc-aaaa	aaaaaaaa-bbbb-cccc	Portal View	Microsoft Graph	a0a0a0a0-bbbb-cccc...
9/5/2024, 2:01	2222bbbb-33cc-aaaa	aaaaaaaa-bbbb-cccc	Portal View	Microsoft Graph	a0a0a0a0-bbbb-cccc...
9/4/2024, 5:00:00	8888dddd-99ee-ffff	cccccccc-dddd-eeee	Portal View	Microsoft Graph	a0a0a0a0-bbbb-cccc...
9/4/2024, 5:00:00	1111bbbb-22cc-dddd	ddddddd-eeee-ffff	Portal View	Office 365 SharePoint...	d3d3d3d3-eeee-ffff...
9/5/2024, 1:49	1111bbbb-22cc-dddd	ddddddd-eeee-ffff	Portal View	Office 365 SharePoint...	d3d3d3d3-eeee-ffff...
9/4/2024, 5:00:00	7777cccc-88dd-eeee	bbbbbbbb-cccc-dddd	Portal View	Windows Azure Activ...	b2b2b2b2-aaaa-ddd...

Log details

The following examples show the type of information captured in the service principal sign-in logs:

- A service principal uses a certificate to authenticate and access the Microsoft Graph.
- An application uses a client secret to authenticate in the OAuth Client Credentials flow.

You can't customize the fields shown in this report.

Note

Entries in the sign-in logs are system generated and can't be changed or deleted.

How does it work?

To make it easier to digest the data in the service principal sign-in logs, service principal sign-in events are grouped. Sign-ins from the same entity under the same conditions are aggregated into a single row. You can expand the row to see all the different sign-ins and their different time stamps. Sign-ins are aggregated in the service principal report when the following data matches:

- Service principal name or ID
 - Status
 - IP address
 - Resource name or ID
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Learn about the sign-in log activity details

Article • 02/25/2025

Microsoft Entra logs all sign-ins into an Azure tenant for compliance purposes. As an IT administrator, you need to know what the values in the sign-in logs mean, so that you can interpret the log values correctly.

- [Learn about the sign-in logs](#)
- [Customize and filter the sign-in logs](#)

This article explains the values found in the sign-in logs. These values provide valuable information for troubleshooting sign-in errors.

Sign-in activity components

In Microsoft Entra ID, a sign-in activity is made of three main components:

- **Who:** The identity (User) doing the sign-in.
- **How:** The client (Application) used for the access.
- **What:** The target (Resource) accessed by the identity.

Focus on those three components when investigating a sign-in to narrow your search so you're not looking at every detail. Within each of those three components, there are related identifiers that might provide more information. Each sign-in also contains unique identifiers that correlate the sign-in attempt to associated activities.

Who

The following details are associated with the user:

- User
- Username
- User ID
- Sign-in identifier
- User type

How

How the user signs in can be identified by looking at the following details:

- Authentication requirement
- Client app
- Client credential type
- Continuous access evaluation

What

You can identify the resource the user is attempting to access using the following details:

- Application
- Application ID
- Resource
- Resource ID
- Resource tenant ID
- Resource service principal ID

Unique identifiers

Sign-in logs also contain several unique identifiers that provide further insight into the sign-in attempt.

- **Correlation ID:** The correlation ID groups sign-ins from the same sign-in session. The value is based on parameters passed by a client, so Microsoft Entra ID can't guarantee its accuracy.
- **Request ID:** An identifier that corresponds to an issued token. If you're looking for sign-ins with a specific token, you need to extract the request ID from the token, first.
- **Unique token identifier:** A unique identifier for the token passed during the sign-in. This identifier is used to correlate the sign-in with the token request.

Sign-in activity details

Each sign-in attempt contains details associated with those three main components. The details are organized into several tabs, based on the type of sign-in.

Basic info

The Basic info tab contains the bulk of the details associated with a sign-in attempt. Take note of the unique identifiers, as they might be needed to troubleshoot sign-in issues. You can follow the *who, how, what* pattern using the details in the Basic info tab.

You can also launch the Sign-in Diagnostic from the Basic info tab. For more information, see [How to use the Sign-in Diagnostic](#).

Sign-in error codes

If a sign-in failed, you can get more information about the reason in the Basic info tab of the related log item. The error code and associated failure reason appear in the details. For more information, see [How to troubleshoot sign-in errors](#).

Activity Details: Sign-ins					
Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date		8/18/2023, 7:46:06 AM			
Request ID		1111aaa-000011-aabb-111bbbb000			
Correlation ID		00011aaa-bb00-111aa-1111aabbb00			
Authentication requirement		Multifactor authentication			
Status		Failure			
Continuous access evaluation		No			
Sign-in error code		500121			
Failure reason		Authentication failed during strong authentication request.			
Additional Details		The user didn't complete the MFA prompt. They may have decided not to authenticate, timed out while doing other work, or has an issue with their authentication setup.			
Follow these steps:					
Troubleshoot Event		Launch the Sign-in Diagnostic .			
		1. Review the diagnosis and act on suggested fixes.			
User		Semyon Maslov			
Username		semaslov@woodgrovegroceries.com			
User ID		0000111-0000			

Location and Device

The **Location** and **Device info** tabs display general information about the location and IP address of the user. The **Device info** tab provides details on the browser and operating system used to sign in. This tab also provides details on if the device is compliant, managed, or Microsoft Entra hybrid joined.

Authentication details

The **Authentication Details** tab in the details of a sign-in log provides the following information for each authentication attempt:

- A list of authentication policies applied, such as Conditional Access or Security Defaults.
- The sequence of authentication methods used to sign-in.
- If the authentication attempt was successful and the reason why.

This information allows you to troubleshoot each step in a user's sign-in. Use these details to track:

- The volume of sign-ins protected by MFA.
- Usage and success rates for each authentication method.
- Usage of passwordless authentication methods, such as Passwordless Phone Sign-in and FIDO2.
- How frequently authentication requirements are satisfied by token claims, such as when users aren't interactively prompted to enter a password or enter an SMS OTP.

Activity Details: Sign-ins						
Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
Authentication Policies Applied						
Conditional Access						
Date	Authentication met...	Authentication ...	Succeeded	Result detail	Requirement	
8/18/2023, 9:22:4...	Previously satisfied		true	First factor requirement ...	Phishing-resistant MFA	
8/18/2023, 9:22:4...	Previously satisfied		true	MFA requirement satisfi...	Phishing-resistant MFA	

Conditional Access

If Conditional Access policies are in use in your tenant, you can see if those policies were applied to the sign-in attempt. All policies that could be applied to the sign-in are listed. The end result of the policy appears so you can quickly see if the policy impacted the sign-in attempt.

- **Success:** The Conditional Access policy was applied successfully to the sign-in attempt.
- **Failure:** The Conditional Access policy was applied to the sign-in attempt, but the sign-in attempt failed.
- **Not Applied:** The sign-in didn't match the criteria for the policy to be applied.
 - There are specific scenarios that due to their nature, are required to be exempt from Conditional Access evaluation to prevent a circular dependency (chicken-

- and-egg scenario) that would not be possible to complete. These are considered "bootstrap scenarios" and might include sign-ins associated with device registration, device compliance, or Network Policy Server connectors.
- Windows Hello for Business sign-ins show as "Not Applied" because Conditional Access policies protect sign-in attempts to cloud resources, not the Windows sign-in process.
 - **Disabled:** The policy was disabled at the time of the sign-in attempt.

Report-only

Conditional Access policies can change the sign-in experience for your users and potentially disrupt their processes. We recommend configuring Conditional Access policies in **Report-only** mode for a period of time to make sure your policy is configured correctly. With **Report-only** mode, you can configure a policy and evaluate its potential effect before enabling the policy.

This tab of the sign-in logs displays the results of sign-in attempts that were in scope for the policy. For more information, see the [What is Conditional Access report-only mode?](#) article.

Sign-in details and considerations

The following scenarios are important to consider when you're reviewing sign-in logs.

- **IP address and location:** There's no definitive connection between an IP address and where the computer with that address is physically located. Mobile providers and VPNs issue IP addresses from central pools that are often far from where the client device is used. Currently, converting IP address to a physical location is a best effort based on traces, registry data, reverse lookups, and other information.
- **Date and time:** The date and time of a sign-in attempt is localized to the time zone for the person signed into the Microsoft Entra admin center, not the user who attempted the sign-in.
- **Conditional Access:**
 - **Not applied:** No policy applied to the user and application during sign-in.
Windows Hello for Business shows up as "Not Applied" because Conditional Access policies protect sign-in attempts to cloud resources, not the Windows sign-in process. Other sign-ins might get interrupted so a policy isn't applied.
 - **Success:** One or more Conditional Access policies applied to or were evaluated for the user and application (but not necessarily the other conditions) during

sign-in. Even though a Conditional Access policy might not apply, if it was evaluated, the Conditional Access status shows *Success*.

- **Failure**: The sign-in satisfied the user and application condition of at least one Conditional Access policy and grant controls are either not satisfied or set to block access.
- Conditional Access does not apply to Windows sign-in, such as Windows Hello for Business. Conditional Access protects sign-in attempts to cloud resources, not the device sign-in process.
- **Continuous access evaluation**: Shows whether continuous access evaluation (CAE) was applied to the sign-in event.
 - There are multiple sign-in requests for each authentication, which can appear on either the interactive or non-interactive tabs.
 - CAE is only displayed as true for one of the requests, and it can appear on the interactive tab or non-interactive tab.
 - For more information, see [Monitor and troubleshoot sign-ins with continuous access evaluation in Microsoft Entra ID](#).
- **Cross-tenant access type**: Describes the type of cross-tenant access used by the actor to access the resource. Possible values are:
 - **none** - A sign-in event that didn't cross a Microsoft Entra tenant's boundaries.
 - **b2bCollaboration** - A cross tenant sign-in performed by a guest user using B2B Collaboration.
 - **b2bDirectConnect** - A cross tenant sign-in performed by a B2B.
 - **microsoftSupport** - A cross tenant sign-in performed by a Microsoft support agent in a Microsoft external tenant.
 - **serviceProvider** - A cross-tenant sign-in performed by a Cloud Service Provider (CSP) or similar admin on behalf of that CSP's customer in a tenant.
 - **unknownFutureValue** - A sentinel value used by MS Graph to help clients handle changes in enum lists. For more information, see [Best practices for working with Microsoft Graph](#).
- **Tenant**: The sign-in log tracks two tenant identifiers that are relevant in cross-tenant scenarios:
 - **Home tenant** – The tenant that owns the user identity. Microsoft Entra ID tracks the ID and name.
 - **Resource tenant** – The tenant that owns the (target) resource.
 - Due to privacy commitments, Microsoft Entra ID doesn't populate the home tenant name during cross-tenant scenarios.
 - To find out how users outside your tenant are accessing your resources, select all entries where the home tenant doesn't match the resource tenant.

- **Multifactor authentication:** When a user signs in with MFA, several separate MFA events are actually taking place. For example, if a user enters the wrong validation code or doesn't respond in time, more MFA events are sent to reflect the latest status of the sign-in attempt. These sign-in events appear as one line item in the Microsoft Entra sign-in logs. That same sign-in event in Azure Monitor, however, appears as multiple line items. These events all have the same `correlationId`.
- **Authentication requirement:** Shows the highest level of authentication needed through all the sign-in steps for the sign-in to succeed.
 - Graph API supports `$filter` (`eq` and `startsWith` operators only).
- **Sign-in event types:** Indicates the category of the sign-in the event represents.
 - The user sign-ins category can be `interactiveUser` or `nonInteractiveUser` and corresponds to the value for the `isInteractive` property on the sign-in resource.
 - The managed identity category is `managedIdentity`.
 - The service principal category is `servicePrincipal`.
 - The Microsoft Graph API, supports: `$filter` (`eq` operator only).
 - The Azure portal doesn't show this value, but the sign-in event is placed in the tab that matches its sign-in event type. Possible values are:
 - `interactiveUser`
 - `nonInteractiveUser`
 - `servicePrincipal`
 - `managedIdentity`
 - `unknownFutureValue`
- **User type:** Examples include `member`, `guest`, or `external`.
- **Authentication details:**
 - **OATH verification code** is logged as the authentication method for both OATH hardware and software tokens (such as the Microsoft Authenticator app).
 - The **Authentication details** tab can initially show incomplete or inaccurate data until log information is fully aggregated. Known examples include:
 - A **satisfied by claim** in the **token** message is incorrectly displayed when sign-in events are initially logged.
 - The **Primary authentication** row isn't initially logged.
 - If you're unsure of a detail in the logs, gather the **Request ID** and **Correlation ID** to use for further analyzing or troubleshooting.
 - If Conditional Access policies for authentication or session lifetime are applied, they're listed above the sign-in attempts. If you don't see either of those options, those policies aren't currently applied. For more information, see [Conditional Access session controls](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Microsoft Entra flagged sign-ins

Article • 03/18/2025

As an IT admin, you want to resolve sign-in issues as soon as possible to unblock your users. Due to the amount of available data in the sign-in log, locating the right information can be a challenge.

This article gives you an overview of the flagged sign-ins feature that can significantly improve the time it takes to resolve user sign-in problems by making the related problems easier to find.

What are flagged sign-ins?

Microsoft Entra sign-in events are critical to understanding what happened with user sign-ins and the authentication configurations in your tenant. However, Microsoft Entra ID processes over 8 billion authentications a day, which can result in so many sign-in events that admins might find it difficult to find the ones that matter.

The flagged sign-ins feature is intended to improve the signal to noise ratio for user sign-ins that require your support. The feature allows users to raise awareness about sign-in errors they need help with. Admins and help desk workers also benefit from finding the right events more efficiently. Flagged sign-in events contain the same information as other sign-in events but they also indicate that a user flagged the event for review.

You can use flagged sign-ins to:

- **Empower** users to proactively indicate which sign-in errors require IT admin support.
- **Simplify** the process of locating sign-in errors.
- **Enable** help desk personnel to find sign-in errors without the end user having to do anything other than flag the event.

How it works

When users see a sign-in error, they can choose to enable flagging. For the next 20 minutes, any sign-in event from that user, on the same browser and client device or computer, displays *Flagged for Review: Yes* in the sign-in logs. After 20 minutes, the flagging automatically turns off.

- Any user signing into Microsoft Entra ID can flag sign-ins for review, including member and guest users.
- Reviewing flagged sign-in events requires permissions to read the sign-in logs. For more information, see [How to access activity logs](#).
- While the names are similar, **flagged sign-ins** and **risky sign-ins** are different capabilities:
 - Flagged sign-ins are sign-in error events users are asking assistance on.
 - A risky sign-in is a functionality of Microsoft Entra ID Protection. For more information, see [What is Microsoft Entra ID Protection](#).

How to flag an error

The user must complete this first step to enable flagging for sign-in errors.

1. The user receives an error during sign-in.
2. The user selects **View details** in the error message.
3. In the **Troubleshooting details** section of the error message, the user selects **Enable flagging**.
 - The text changes to **Disable Flagging** and flagging is now enabled.
 - The user must use the same browser and client or the events aren't flagged.



ivju37@woodgrove.ms

Request denied

We sent an identity verification request to your mobile device, but you denied it [View details](#)

[Send another request to my Microsoft Authenticator app](#)

Having trouble?

[Enter a security code](#) from your Microsoft account or authenticator app instead.

If you can't use an app right now [get a code a different way](#).

[More information](#)

[Cancel](#)

Hate typing your password? Go passwordless today
<https://aka.ms/passwordless> [Need Support?](#) [Email Woodgrove Support](#)

Troubleshooting details X

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Error Code: 500121

Request Id: 72d4d552-ea26-40b0-9e09-3304e19b2900

Correlation Id: cccc2222-dd33-4444-55ee-666666ffffff

Timestamp: 2024-10-01T18:48:50Z

Flag sign-in errors for review: [Enable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

4. Open a *new* browser window (in the same browser application) and attempt the same sign-in that failed.

If the sign-in error is reproduced, the flagged diagnostics are sent to the sign-in logs.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

What are the Microsoft Entra user provisioning logs?

Article • 03/17/2025

Microsoft Entra ID integrates with several non-Microsoft services to provision users into your tenant. If you need to troubleshoot an issue with a provisioned user, you can use the information captured in the Microsoft Entra provisioning logs to help find a solution.

Two other activity logs are also available to help monitor the health of your tenant:

- **Sign-ins** – Information about sign-ins and how your resources are used by your users.
- **Audit** – Information about changes applied to your tenant such as users and group management or updates applied to your tenant's resources.

This article gives you an overview of the logs that capture user provisioning through non-Microsoft services.

What can you do with the provisioning logs?

You can use the provisioning logs to find answers to questions like:

- What groups were successfully created in ServiceNow?
- What users were successfully removed from Adobe?
- What users from Workday were successfully created in Active Directory?

Note

Entries in the provisioning logs are system generated and can't be changed or deleted.

What do the logs show?

The logs display the identity, action taken, source system, target system, and the status of the provisioning event. Other columns can be added for further troubleshooting, but the following details are standard.

Date	Identity	Action	Source System	Target System	Status
11/4/2024, 12:55:06 PM	Source ID 9c2b93fe-12ec-46cf- Other	Update	salesforce.com	Microsoft Entra ID	Failure
11/4/2024, 12:53:55 PM	Display Name Purview Investigator Source ID: a0a0a0a0-bbbb-cc...	Update	Microsoft Entra ID	salesforce.com	Skipped
11/4/2024, 12:53:55 PM	Display Name Jonathan W Source ID: c2c2c2c2-dddd-ee...	Other	salesforce.com	Microsoft Entra ID	Skipped
11/4/2024, 12:53:55 PM	Display Name ZT MC Source ID: f5f5f5f5-aaaa-bbb...	Create	Microsoft Entra ID	salesforce.com	Skipped
11/4/2024, 12:53:55 PM	Display Name ProSales Source ID: bibibib1-cccc-dd...	Create	Microsoft Entra ID	Google Cloud / Workspace	Success
11/4/2024, 12:53:55 PM	Display Name LicM365 Source ID: d3d3d3d3-eeee-ffff...	Create	Microsoft Entra ID	Google Cloud / Workspace	Success
11/4/2024, 12:53:55 PM	Display Name Salesforce Admin Source ID: bibibib1-cccc-dd...	Create	Microsoft Entra ID	Google Cloud / Workspace	Success

- Identity:** The display name and source ID of the identity being provisioned appear in this column.
- Action:** Possible values include Create, Update, Delete, Disable, StagedDelete, and Other.
 - Examples of Other include if the source and target system details already match, so no change was made.
- Source System and Target System:** Paired together, these details show which system the identity is coming from and where it's being provisioned.
- Status:** Possible values include Success, Failure, Skipped, and Warning.
 - There are several scenarios that could trigger the Skipped status. For details on these scenarios, see [No users are being provisioned](#)

Select an item from the provisioning logs to see more details about this item, such as the steps taken to provision the user and tips for troubleshooting issues. The details are grouped into four tabs.

- Steps:** This tab outlines the steps taken to provision an object. Provisioning an object can include the following steps, but not all steps are applicable to all provisioning events.
 - Import the object.
 - Match the object between source and target.
 - Determine if the object is in scope.
 - Evaluate the object before synchronization.
 - Provision the object (create, update, delete, or disable).

Result	Success
Description	User 'cheryl@f128.info' was created in Box
ReportableIdentifier	cheryl@f128.info

- **Troubleshooting & Recommendations:** If there was an error, this tab provides the error code and reason. In many cases, a detailed description of the error is provided. Review this information to understand the issue and follow the guidance provided to resolve it. Review the following troubleshooting articles:
 - [Troubleshoot HR user creation issues](#)
 - [Troubleshoot HR user update issues](#)
 - [Troubleshoot insufficient access rights error](#)
- **Modified Properties:** If there were changes, this tab shows the old value and the new value.
- **Summary:** Provides an overview of what happened and identifiers for the object in the source and target systems.

Using provisioning logs workbooks and Log Analytics

With the querying and alerting capabilities of Log Analytics and workbooks, you can create custom reports and alerts. To get started, you need to [create a Log Analytics workspace](#). Once you have a workspace, you can stream your logs to that workspace, which allows you to query and analyze the data in Log Analytics and workbooks.

For more information, see [Integrating provisioning logs with Azure Monitor logs](#).

There are two workbook templates available for provisioning logs:

- **Provisioning Analysis** provides a high-level overview of the provisioning events in your tenant.
- **Provisioning Insights** provides details on events related to syncing users from other sources so you can see analyze these events in one place. For more

information, see [Provisioning insights workbook](#).

Related content

- [Integrating provisioning logs with Azure Monitor logs](#)
 - [Reporting on automatic user account provisioning](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Access Microsoft Graph activity logs

Article • 11/27/2024

Microsoft Graph activity logs are an audit trail of all HTTP requests that the Microsoft Graph service received and processed for a tenant. Tenant administrators can enable the collection and configure downstream destinations for these logs using diagnostic settings in Azure Monitor. The logs are stored in Log Analytics for analysis; you can export them to Azure Storage for long-term storage or stream with Azure Event Hubs to external SIEM tools for alerting, analysis, or archival.

All logs for API requests made from line of business applications, API clients, SDKs, and by Microsoft applications like Outlook, Microsoft Teams, or the Microsoft Entra admin center are available.

This service is available in the following [national cloud deployments](#).

[+] Expand table

Global service	US Government L4	US Government L5 (DOD)	China operated by 21Vianet
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Prerequisites

To access the Microsoft Graph activity logs, you need the following privileges.

- A Microsoft Entra ID P1 or P2 tenant license in your tenant.
- An administrator with a supported [Microsoft Entra administrator role](#). *Security Administrator* is the only least privileged admin role supported for configuring diagnostic settings.
- An Azure subscription with one of the following log destinations are configured, and permissions to access data in the corresponding log destinations.
 - An Azure Log Analytics workspace to send logs to Azure Monitor
 - An Azure Storage Account for which you have List Keys permissions
 - An Azure Event Hubs namespace to integrate with third-party solutions

What data is available in the Microsoft Graph activity logs?

The following data relating to API requests is available for Microsoft Graph activity logs on the Logs Analytics interface.

[Expand table](#)

Column	Type	Description
AadTenantId	string	The Azure AD tenant ID.
ApiVersion	string	The API version of the event.
AppId	string	The identifier for the application.
ATContent	string	Reserved for future use.
ATContentH	string	Reserved for future use.
ATContentP	string	Reserved for future use.
_BilledSize	real	The record size in bytes
ClientAuthMethod	int	Indicates how the client was authenticated. For a public client, the value is 0. If client ID and client secret are used, the value is 1. If a client certificate was used for authentication, the value is 2.
ClientRequestId	string	Optional. The client request identifier when sent. If no client request identifier is sent, the value will be equal to the operation identifier.
DurationMs	int	The duration of the request in milliseconds.
IdentityProvider	string	The identity provider that authenticated the subject of the token.
IPAddress	string	The IP address of the client from where the request occurred.
_IsBillable	string	Specifies whether ingesting the data is billable. When <code>_IsBillable</code> is <code>false</code> ingestion isn't billed to your Azure account
Location	string	The name of the region that served the request.
OperationId	string	The identifier for the batch. For non-batched requests, this will be unique per request. For batched requests, this will be the same for all requests in the batch.
RequestId	string	The identifier representing the request.
RequestMethod	string	The HTTP method of the event.
RequestUri	string	The URI of the request.

Column	Type	Description
ResponseSizeBytes	int	The size of the response in Bytes.
ResponseStatuscode	int	The HTTP response status code for the event.
Roles	string	The roles in token claims.
Scopes	string	The scopes in token claims.
ServicePrincipalId	string	The identifier of the servicePrincipal making the request.
SignInActivityId	string	The identifier representing the sign-in activity.
SourceSystem	string	The type of agent the event was collected by. For example, <code>OpsManager</code> for Windows agent, either direct connect or Operations Manager, <code>Linux</code> for all Linux agents, or <code>Azure</code> for Azure Diagnostics
TenantId	string	The Log Analytics workspace ID
TimeGenerated	datetime	The date and time the request was received.
TokenIssuedAt	datetime	The timestamp the token was issued at.
Type	string	The name of the table
UserAgent	string	The user agent information related to request.
UserId	string	The identifier of the user making the request.
Wids	string	Denotes the tenant-wide roles assigned to this user.

Common use cases for Microsoft Graph activity logs

- Get full visibility into the transactions made by applications and other API clients that you have consented to in the tenant.
- Identify the activities that a compromised user account conducted in your tenant.
- Build detections and behavioral analysis to identify suspicious or anomalous use of Microsoft Graph APIs.
- Investigate unexpected or suspicious privileged assignment of application permissions.
- Identify problematic or unexpected behaviors for client applications such as extreme call volumes.
- Correlate Microsoft Graph requests made by a user or app with sign-in information.

Configure to receive the Microsoft Graph activity logs

You can configure to stream the logs through the Diagnostic Setting in the Azure portal or through Azure Resource Manager APIs. For more information, see the guidance in the following articles:

- [Integrate activity logs with Azure Monitor logs](#)
- [Configure diagnosticSettings through the Azure Resource Manager API](#)

The following articles guide you to configure the storage destinations:

- [Azure Log Analytics Workspace](#)
- [Azure Storage](#)
- [Azure Event Hubs](#)

Cost planning estimates

If you already have a Microsoft Entra ID P1 license, you need an Azure subscription to set up the Log Analytics workspace, Storage account, or Event Hubs. The Azure subscription comes at no cost, but you have to pay to utilize Azure resources.

The amount of data logged and, thus, the cost incurred, can vary significantly depending on the tenant size and the applications in your tenant that interact with Microsoft Graph APIs. The following table provides some estimates for log data size to aid the price calculation. Use these estimations for general consideration only.

[+] [Expand table](#)

Users in tenant	Storage GiB/month	Event Hubs Messages/month	Azure Monitor Logs GiB/month
1000	14	62K	15
100000	1000	4.8M	1200

See the following pricing calculations for respective services:

- [Log Analytics pricing details](#)
- [Azure Storage pricing ↗](#)
- [Event Hubs pricing ↗](#)

Cost reduction for Log Analytics

If you're ingesting the logs to a Log Analytics Workspace but are only interested in logs filtered by a criteria, such as omitting certain columns or rows, you can partially reduce costs by applying a workspace transformation on the Microsoft Graph Activity Logs table. To find out more about workspace transformations, how it affects ingestion costs, and how to apply a transformation to your Microsoft Graph Activity Logs, see [Data collection transformations in Azure Monitor](#).

An alternative approach to reduce Log Analytics cost is to switch to the Basic log data plan which lowers the bills by providing reduced capabilities. For more information, see [Set a table's log data plan to Basic or Analytics](#).

Azure Monitor Logs query examples

If you send Microsoft Graph activity logs to a Log Analytics workspace, you can query the logs using Kusto Query Language (KQL). For more information about queries in Log Analytics Workspace, see [Analyze Microsoft Entra activity logs with Log Analytics](#). You can use these queries for data exploration, to build alert rules, build Azure dashboards, or integrate into your custom applications using the Azure Monitor Logs API or Query SDK.

The following Kusto query identifies the top 20 entities making requests to groups resources that are failing due to authorization:

```
Kusto

MicrosoftGraphActivityLogs
| where TimeGenerated >= ago(3d)
| where ResponseStatusCode == 401 or ResponseStatusCode == 403
| where RequestUri contains "/groups"
| summarize UniqueRequests=count_distinct(RequestId) by AppId,
ServicePrincipalId, UserId
| sort by UniqueRequests desc
| limit 20
```

The following Kusto query identifies resources queried or modified by potentially risky users:

```
Kusto

MicrosoftGraphActivityLogs
| where TimeGenerated > ago(30d)
| join AADRiskyUsers on $left.UserId == $right.Id
| extend resourcePath =
```

```
replace_string(replace_string(replace_regex(tostring(parse_url(RequestUri)).Path, @'(\+)/','/'), 'v1.0/',''), 'beta/','')
| summarize RequestCount=dcount(RequestId) by UserId, RiskState,
resourcePath, RequestMethod, ResponseStatusCode
```

The following Kusto query allows you to correlate the Microsoft Graph activity logs and sign-in logs. Activity logs from Microsoft applications may not all have matching sign-in log entries. For more information, see [Sign-in logs known limitations](#).

Kusto

```
MicrosoftGraphActivityLogs
| where TimeGenerated > ago(7d)
| join kind=leftouter (union SigninLogs, AADNonInteractiveUserSignInLogs,
AADServicePrincipalSignInLogs, AADManagedIdentitySignInLogs, ADFSSignInLogs
| where TimeGenerated > ago(7d))
on $left.SignInActivityId == $right.UniqueTokenIdentifier
```

The following Kusto query identifies apps that are getting throttled:

Kusto

```
MicrosoftGraphActivityLogs
| where TimeGenerated > ago(3d)
| where ResponseStatusCode == 429
| extend path =
replace_string(replace_string(replace_regex(tostring(parse_url(RequestUri)).Path, @'(\+)/','/'), 'v1.0/',''), 'beta/','')
| extend UriSegments = extract_all(@"\/( [A-z2]+|\$batch)(\$|\V|\$| \$)", dynamic([1]), tolower(path))
| extend OperationResource = strcat_array(UriSegments, '/') | summarize
RateLimitedCount=count() by AppId, OperationResource, RequestMethod
| sort by RateLimitedCount desc
| limit 100
```

The following query allows you to render a time-series chart:

Kusto

```
MicrosoftGraphActivityLogs
| where TimeGenerated between (ago(3d) .. ago(1h))
| summarize EventCount = count() by bin(TimeGenerated, 10m)
| render timechart
with (
title="Recent traffic patterns",
xtitle="Time",
ytitle="Requests",
```

```
legend=hidden  
)
```

Limitations

- The Microsoft Graph activity logs feature allows the tenant administrators to collect logs for the resource tenant. This feature doesn't allow you to see the activities of a multitenant application in another tenant.
- You can't filter Microsoft Graph activity logs through diagnostic settings in Azure Monitor. However, options are available to reduce costs in Azure Log Analytics Workspace. For more information, see [Workspace transformation](#).
- In most regions, the events are available and delivered to the configuration destination within 30 minutes. In less common cases, some events might take up to 2 hours to be delivered to the destination.

Related content

- [Azure Monitor Reference: MicrosoftGraphActivityLogs](#)
- [Stream data from Azure Monitor to an event hub or external partner](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Microsoft Entra activity logs schema

Article • 10/04/2024

This article describes the information contained in the Microsoft Entra activity logs and how that schema is used by other services. This article covers the schemas from the Microsoft Entra admin center and Microsoft Graph. Descriptions of some key fields are provided.

Prerequisites

- For license and role requirements, see [Microsoft Entra monitoring and health licensing](#).
- The option to download logs is available in all editions of Microsoft Entra ID.
- Downloading logs programmatically with Microsoft Graph requires a [premium license](#).
- **Reports Reader** is the least privileged role required to view Microsoft Entra activity logs.
- Audit logs are available for features that you've licensed.
- The results of a downloaded log might show `hidden` for some properties if you don't have the required license.

What is a log schema?

Microsoft Entra monitoring and health offer logs, reports, and monitoring tools that can be integrated with Azure Monitor, Microsoft Sentinel, and other services. These services need to map the properties of the logs to their service's configurations. The schema is the map of the properties, the possible values, and how they're used by the service. Understanding the log schema is helpful for effective troubleshooting and data interpretation.

Microsoft Graph is the primary way to access Microsoft Entra logs programmatically. The response for a Microsoft Graph call is in JSON format and includes the properties and values of the log. The schema of the logs is defined in the [Microsoft Graph documentation](#).

There are two endpoints for the Microsoft Graph API. The V1.0 endpoint is the most stable and is commonly used for production environments. The beta version often contains more properties, but they're subject to change. For this reason, we don't recommend using the beta version of the schema in production environments.

Microsoft Entra customer can configure activity log streams to be sent to Azure Monitor storage accounts. This integration enables Security Information and Event Management (SIEM) connectivity, long-term storage, and improved querying capabilities with Log Analytics. The log schemas for Azure Monitor might differ from the Microsoft Graph schemas.

For full details on these schemas, see the following articles:

- [Azure Monitor audit logs](#)
- [Azure Monitor sign-in logs](#)
- [Azure Monitor provisioning logs](#)
- [Microsoft Graph audit logs](#)
- [Microsoft Graph sign-in logs](#)
- [Microsoft Graph provisioning logs](#)

How to interpret the schema

When looking up the definitions of a value, pay attention to the version you're using. There might be differences between the V1.0 and beta versions of the schema.

Values found in all log schemas

Some values are common across all log schemas.

- `correlationId`: This unique ID helps correlate activities that span across various services and is used for troubleshooting. This value's presence in multiple logs doesn't indicate the ability to join logs across services.
- `status` or `result`: This important value indicates the result of the activity. Possible values are: `success`, `failure`, `timeout`, `unknownFutureValue`.
- Date and time: The date and time when the activity occurred is in Coordinated Universal Time (UTC).
- Some reporting features require a Microsoft Entra ID P2 license. If you don't have the correct licenses, the value `hidden` is returned.

Audit logs

- `activityDisplayName`: Indicates the activity name or the operation name (examples: "Create User" and "Add member to group"). For more information, see [Audit log activities](#).
- `category`: Indicates which resource category that's targeted by the activity. For example: `UserManagement`, `GroupManagement`, `ApplicationManagement`,

`RoleManagement`. For more information, see [Audit log activities](#).

- `initiatedBy`: Indicates information about the user or app that initiated the activity.
- `targetResources`: Provides information on which resource was changed. Possible values include `User`, `Device`, `Directory`, `App`, `Role`, `Group`, `Policy` or `Other`.

Sign-in logs

- ID values: There are unique identifiers for users, tenants, applications, and resources. Examples include:
 - `resourceId`: The *resource* that the user signed into.
 - `resourceTenantId`: The tenant that owns the *resource* being accessed. Might be the same as the `homeTenantId`.
 - `homeTenantId`: The tenant that owns the user *account* that is signing in.
- Risk details: Provides the reason behind a specific state of a risky user, sign-in, or risk detection.
 - `riskState`: Reports status of the risky user, sign-in, or a risk event.
 - `riskDetail`: Provides the reason behind a specific state of a risky user, sign-in, or risk detection. The value `none` means that no action has been performed on the user or sign-in so far.
 - `riskEventTypes_v2`: Risk detection types associated with the sign-in.
 - `riskLevelAggregated`: Aggregated risk level. The value `hidden` means the user or sign-in wasn't enabled for Microsoft Entra ID Protection.
- `crossTenantAccessType`: Describes the type of cross-tenant access used to access the resource. For example, B2B, Microsoft Support, and passthrough sign-ins are captured here.
- `status`: The sign-in status that includes the error code and description of the error (if a sign-in failure occurs).

Applied Conditional Access policies

The `appliedConditionalAccessPolicies` subsection lists the Conditional Access policies related to that sign-in event. The section is called *applied* Conditional Access policies; however, policies that were *not* applied also appear in this section. A separate entry is created for each policy. For more information, see [conditionalAccessPolicy resource type](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

What is Microsoft Entra Health monitoring?

Article • 04/25/2025

Microsoft Entra Health provides you with observability of your Microsoft Entra tenant through continuous low-latency health monitoring and look-back reporting on [Service Level Agreements \(SLA\)](#). The low-latency health monitoring solution includes a set of health metric data streams, known as signals, with built-in alerts designed to help IT operations teams maintain high levels of uptime and service for common Microsoft Entra scenarios. The SLA Attainment is a monthly look-back solution that shows the core authentication availability of Microsoft Entra ID each month.

When these metrics and signals are paired together, you get a comprehensive view of the health of your Microsoft Entra tenant. Regularly monitoring the information provided in Microsoft Entra Health can help you identify trends, potential issues, and areas for improvement in your tenant's health. Email notifications can also be configured to alert you when the service identifies an anomaly in the pattern for your tenant. This article provides an overview of the Microsoft Entra Health monitoring features.

Important

Microsoft Entra Health scenario monitoring and alerts are currently in PREVIEW. This information relates to a prerelease product that might be substantially modified before release. Microsoft makes no warranties, expressed or implied, with respect to the information provided here.

Access Microsoft Entra Health

Scenario monitoring and SLA Attainment are available in the Microsoft Entra Health area of the Microsoft Entra admin center.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Entra ID > Monitoring & health > Health**.

The page opens to the SLA Attainment page.

Health Monitoring

SLA Attainment

SLA Attainment provides a report of Microsoft Entra ID's user authentication availability per month. When availability falls below the SLA threshold of 99.99%, the bar for that month in the chart turns from green to red. [Learn more](#). To browse incidents that may have impacted the SLA, see [Service Health | Health History](#).

Monthly authentication availability rate (%)

Month	Authentication availability rate
Jul 2024	99.999%
Aug 2024	99.999%

How Microsoft Entra Health monitoring (preview) works

Scenario Monitoring in Microsoft Entra Health is built on two key components: signals and alerts. Here's a high-level look at how they both work together:

1. Metrics and data are gathered, processed, and converted into meaningful signals displayed in Microsoft Entra Health monitoring.
2. These signals are fed into our anomaly detection service.
3. When the anomaly detection service identifies a significant change to a pattern in the signal, it triggers an alert.
4. When the alert is triggered, an email notification is sent to a set of users, preselected by the tenant admin. This email notification prompts recipients to investigate and determine if there's a problem.

5. After you see an alert, you need to research possible root causes, determine the next steps, and take action to mitigate the root cause. Each health alert contains an impact assessment and links to resources to help you through the process.

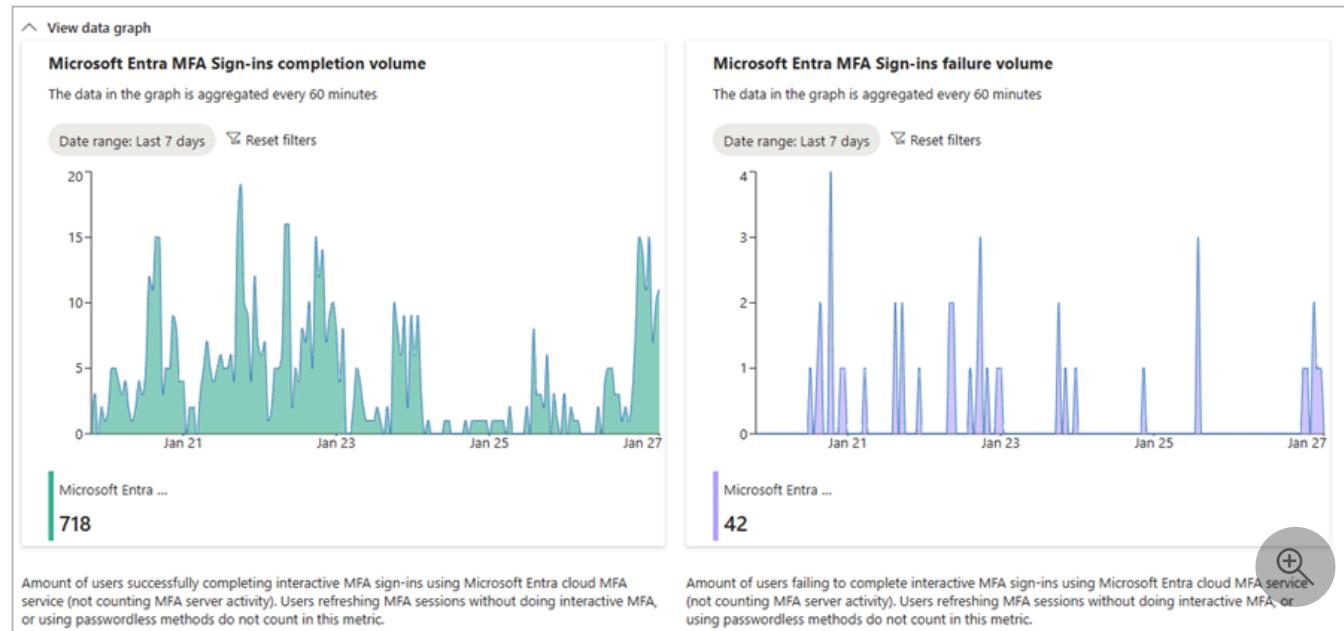
Signals

Many IT administrators spend a considerable amount of time investigating several key scenarios, such as sign-ins requiring multifactor authentication (MFA). Microsoft Entra Health provides a visualization of the data associated with these metrics, so you can quickly identify trends and potential issues.

The following key scenarios can be monitored in Microsoft Entra Health:

- Interactive user sign-in requests that require MFA.
- User sign-in requests that require a managed device through a Conditional Access policy.
- User sign-in requests that require a compliant device through a Conditional Access policy.
- User sign-in requests to applications using SAML authentication.

The data associated with each of these scenarios is aggregated into a view that's specific to that scenario. If you're only interested in sign-ins from compliant devices, you can dive into that scenario without noise from other sign-in activities.



Each scenario detail page provides trends and totals for that scenario for the last 30 days. This data is aggregated every 15 minutes, for low latency insights into your tenant's health.

Alerts

The anomaly detection service looks at the data and develops dynamic alerting thresholds based on a pattern specific to your tenant. When the service identifies a significant change to

that pattern at the tenant level, it triggers an alert. By regularly monitoring these scenarios and reviewing the alerts when they come in, you can more effectively monitor and improve the health of your tenant.

Alerts are specific to your tenant and to the scenario being monitored. Machine learning requires at least four weeks of data to establish a pattern for your tenant. The more data we collect on the signal, the more accurate the anomaly detection service becomes. The service looks back 25-30 minutes on the timeline and triggers an alert if the signal deviates from the pattern.

The service provides alerts for the following scenarios:

- [Sign-ins requiring a Conditional Access compliant device](#)
- [Sign-ins requiring a Conditional Access managed device](#)
- [Sign-ins requiring multifactor authentication \(MFA\)](#)
- [Conditional Access block policy](#)

Related content

- [Configure Health monitoring alerts](#)
- [Investigate Health monitoring alerts](#)
- [Service Level Agreement attainment for Microsoft Entra ID](#)

What are the identity logs you can stream to an endpoint?

Article • 04/16/2025

Using Microsoft Entra diagnostic settings, you can route activity logs to several endpoints for long term retention and data insights. You select the logs you want to route, then select the endpoint.

This article describes the logs that you can route to an endpoint with Microsoft Entra diagnostic settings. The logs are categorized into tiers based on their importance for security investigations.

Log streaming requirements and options

Setting up an endpoint, such as an event hub or storage account, might require different roles and licenses. To create or edit a new diagnostic setting, you need a user who's a **Security Administrator** for the Microsoft Entra tenant.

To help decide which log routing option is best for you, see [How to access activity logs](#). The overall process and requirements for each endpoint type are covered in the following articles:

- [Send logs to a Log Analytics workspace to integrate with Azure Monitor logs](#)
- [Archive logs to a storage account](#)
- [Stream logs to an event hub](#)
- [Send to a partner solution](#)

Activity log options

The following logs can be routed to an endpoint for storage, analysis, or monitoring.

Audit logs

The `AuditLogs` report capture changes to applications, groups, users, and licenses in your Microsoft Entra tenant. Once you routed your audit logs, you can filter or analyze by date/time, the service that logged the event, and who made the change. For more information, see [Audit logs](#).

Sign-in logs

The `SignInLogs` send the interactive sign-in logs, which are logs generated by your users signing in. Sign-in logs are generated when users provide their username and password on a Microsoft Entra sign-in screen or when they pass an MFA challenge. For more information, see [Interactive user sign-ins](#).

Non-interactive sign-in logs

The `NonInteractiveUserSignInLogs` are sign-ins done on behalf of a user, such as by a client app. The device or client uses a token or code to authenticate or access a resource on behalf of a user. For more information, see [Non-interactive user sign-ins](#).

Service principal sign-in logs

If you need to review sign-in activity for apps or service principals, the `ServicePrincipalSignInLogs` might be a good option. In these scenarios, certificates or client secrets are used for authentication. For more information, see [Service principal sign-ins](#).

Managed identity sign-in logs

The `ManagedIdentitySignInLogs` provide similar insights as the service principal sign-in logs, but for managed identities, where Azure manages the secrets. For more information, see [Managed identity sign-ins](#).

Provisioning logs

If your organization provisions users through a non-Microsoft application such as Workday or ServiceNow, you might want to export the `ProvisioningLogs` reports. For more information, see [Provisioning logs](#).

AD FS sign-in logs

Sign-in activity for Active Directory Federated Services (AD FS) applications are captured in this Usage and insight reports. You can export the `ADFSSignInLogs` report to monitor sign-in activity for AD FS applications. For more information, see [AD FS sign-in logs](#).

Risky users

The `RiskyUsers` logs identify users who are at risk based on their sign-in activity. This report is part of Microsoft Entra ID Protection and uses sign-in data from Microsoft Entra ID. For more

information, see [What is Microsoft Entra ID Protection?](#).

User risk events

The `UserRiskEvents` logs are part of Microsoft Entra ID Protection. These logs capture details about risky sign-in events. For more information, see [How to investigate risk](#).

Network access traffic logs

The `NetworkAccessTrafficLogs` are associated with Microsoft Entra Internet Access and Microsoft Entra Private Access. The logs are visible in Microsoft Entra ID, but selecting this option doesn't add new logs to your workspace unless your organization is using Microsoft Entra Internet Access and Microsoft Entra Private Access to secure access to your corporate resources. For more information, see [What is Global Secure Access?](#).

Risky service principals

The `RiskyServicePrincipals` logs provide information about service principals that Microsoft Entra ID Protection detected as risky. Service principal risk represents the probability that an identity or account is compromised. These risks are calculated asynchronously using data and patterns from Microsoft's internal and external threat intelligence sources. These sources might include security researchers, law enforcement professionals, and security teams at Microsoft. For more information, see [Securing workload identities](#).

Service principal risk events

The `ServicePrincipalRiskEvents` provide details around the risky sign-in events for service principals. These logs might include any identified suspicious events related to the service principal accounts. For more information, see [Securing workload identities](#).

Enriched Microsoft 365 audit logs

The `EnrichedOffice365AuditLogs` are associated with the enriched logs you can enable for Microsoft Entra Internet Access. Selecting this option doesn't add new logs to your workspace unless your organization is using Microsoft Entra Internet to secure access to your Microsoft 365 traffic *and* you enabled the enriched logs. For more information, see [How to use the Global Secure Access enriched Microsoft 365 logs](#).

Microsoft Graph activity logs

The `MicrosoftGraphActivityLogs` provide administrators full visibility into all HTTP requests accessing your tenant's resources through the Microsoft Graph API. You can use these logs to identify activities that a compromised user account conducted in your tenant or to investigate problematic or unexpected behaviors for client applications, such as extreme call volumes. Route these logs to the same Log Analytics workspace with `SignInLogs` to cross-reference details of token requests for sign-in logs. For more information, see [Access Microsoft Graph activity logs](#).

Remote network health logs

The `RemoteNetworkHealthLogs` provide insights into the health of your remote network configured through Global Secure Access. Selecting this option doesn't add new logs to your workspace unless your organization is using Microsoft Entra Internet Access and Microsoft Entra Private Access to secure access to your corporate resources. For more information, see [Remote network health logs](#).

Microsoft service principal sign-in logs (preview)

The `MicrosoftServicePrincipalSignInLogs` provides visibility into scenarios where Microsoft-owned (first-party) services authenticate to other Microsoft services within a tenant, such as when a user opens a Word document inside Microsoft Teams. These logs were released to provide greater transparency around service-to-service authentication but are not necessary for most customers as they are complex and generate a high volume of data. These applications are monitored by Microsoft security to ensure the security of the applications and follows principles of least privilege. We want to emphasize that this data is not essential for security investigations and we strongly advise against taking actions such as disabling applications based on this data, as doing so could cause misconfigurations and potential adverse effects such as tenant lock-out. This data is offered as an opt-in through diagnostic settings only and is currently in preview. For more information and commonly asked questions, please visit our [FAQ page](#).

Custom security attribute audit logs

The `CustomSecurityAttributeAuditLogs` are configured in the **Custom security attributes** section of diagnostic settings. These logs capture changes to custom security attributes in your Microsoft Entra tenant. To view these logs in the Microsoft Entra audit logs, you need the [Attribute Log Reader](#) role. To route these logs to an endpoint, you need the [Attribute Log Administrator](#) role and the [Security Administrator](#).

What are the Microsoft Entra activity log integration options?

Article • 11/21/2024

Using [Diagnostic settings](#) in Microsoft Entra ID, you can route activity logs to several endpoints for long term data retention and insights. You can archive logs for storage, route to Security Information and Event Management (SIEM) tools, and integrate logs with Azure Monitor logs.

With these integrations, you can enable rich visualizations, monitoring, and alerting on the connected data. This article describes the recommended uses for each integration type or access method. Cost considerations for sending Microsoft Entra activity logs to various endpoints are also covered.

Supported reports

The following logs can be integrated with one of many endpoints:

- The [audit logs activity report](#) gives you access to the history of every task performed in your tenant.
- With the [sign-in activity report](#), you can see when users attempt to sign in to your applications or troubleshoot sign-in errors.
- With the [provisioning logs](#), you can monitor which users were, updated, and deleted in all your non-Microsoft applications.
- The [risky users logs](#) helps you monitor changes in user risk level and remediation activity.
- With the [risk detections logs](#), you can monitor user's risk detections and analyze trends in risk activity detected in your organization.

Integration options

To help choose the right method for integrating Microsoft Entra activity logs for storage or analysis, think about the overall task you're trying to accomplish. The options are grouped into three main categories:

- Troubleshooting
- Long-term storage
- Analysis and monitoring

Basic troubleshooting

If you're performing basic troubleshooting tasks but you don't need to retain the logs for more than 30 days, we recommend using the Microsoft Entra admin center or the Microsoft Graph APIs to access the activity logs. You can filter the logs for your scenario and export or download them as needed.

If you're performing troubleshooting tasks *and* you need to retain the logs for more than 30 days, take a look at the long-term storage options.

Long-term storage

If you're performing troubleshooting tasks *and* you need to retain the logs for more than 30 days, you should export your logs to an Azure storage account. This option is ideal if you don't plan on querying that data often or you need to store the logs for compliance purposes.

If you need to query the data that you're retaining for more than 30 days, take a look at the analysis and monitoring options.

Analysis and monitoring

If your scenario requires that you retain data for more than 30 days *and* you plan on querying that data regularly, you've got a few options to integrate your data with SIEM tools for analysis and monitoring.

If you use a non-Microsoft SIEM tool, we recommend setting up an Event Hubs namespace and event hub where you can stream your data. With an event hub, you can stream logs to one of the supported SIEM tools.

If you don't plan on using a third-party SIEM tool, we recommend sending your Microsoft Entra activity logs to [Azure Monitor logs](#). With this integration, you can query your activity logs in a [Log Analytics workspace](#). Once your logs are integrated with Azure Monitor logs, you can query with Log Analytics and set up Workbooks for further analysis and alerting. We recommend setting up a workspace for storage of logs and a different workspace to integrate with Log Analytics and Workbooks.

In addition to Azure Monitor logs, [Microsoft Sentinel](#) provides near real-time security detection and threat hunting. If you decide to integrate with SIEM tools later, you can stream your Microsoft Entra activity logs along with your other Azure data through an event hub.

Cost considerations

There's a cost for sending data to a Log Analytics workspace, archiving data in a storage account, or streaming logs to an event hub. The amount of data and the cost incurred can vary significantly depending on the tenant size, the number of policies in use, and even the time of day. Changing an existing diagnostic setting might incur new charges.

Because the size and cost for sending logs to an endpoint is difficult to predict, the most accurate way to determine your expected costs is to route your logs to an endpoint for day or two. With this snapshot, you can get an accurate prediction for your expected costs. You can also get an estimate of your costs by downloading a sample of your logs and multiplying accordingly to get an estimate for one day.

Other considerations for sending Microsoft Entra logs to Azure Monitor logs are covered in the following Azure Monitor cost details articles:

- [Azure Monitor logs cost calculations and options](#)
- [Azure Monitor cost and usage](#)
- [Optimize costs in Azure Monitor](#)

Azure Monitor provides the option to exclude whole events, fields, or parts of fields when ingesting logs from Microsoft Entra ID. Learn more about this cost saving feature in [Data collection transformation in Azure Monitor](#).

Estimate your costs

To estimate the costs for your organization, you can estimate either the daily log size or the daily cost for integrating your logs with an endpoint.

The following factors could affect costs for your organization:

- Audit log events use around 2 KB of data storage
- Sign-in log events use on average 11.5 KB of data storage
- A tenant of about 100,000 users could incur about 1.5 million events per day
- Events are batched into about 5-minute intervals and sent as a single message that contains all the events within that time frame

Daily log size

To estimate the daily log size, gather a sample of your logs, adjust the sample to reflect your tenant size and settings, then apply that sample to the [Azure pricing calculator](#).

If you haven't downloaded logs from the Microsoft Entra admin center before, review the [How to download logs in Microsoft Entra ID](#) article. Depending on the size of your organization, you might need to choose a different sample size to start your estimation. The following sample sizes are a good place to start:

- 1,000 records
- For large tenants, 15 minutes of sign-ins
- For small to medium tenants, 1 hour of sign-ins

You should also consider the geographic distribution and peak hours of your users when you capture your data sample. If your organization is based in one region, it's likely that sign-ins peak around the same time. Adjust your sample size and when you capture the sample accordingly.

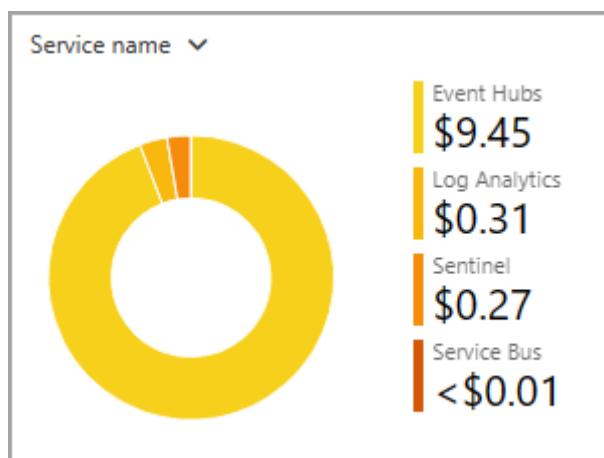
With the data sample captured, multiply accordingly to find out how large the file would be for one day.

Estimate the daily cost

To get an idea of how much a log integration could cost for your organization, you can enable an integration for a day or two. Use this option if your budget allows for the temporary increase.

To enable a log integration, follow the steps in the [Integrate activity logs with Azure Monitor logs](#) article. If possible, create a new resource group for the logs and endpoint you want to try out. Having a devoted resource group makes it easy to view the cost analysis and then delete it when you're done.

With the integration enabled, navigate to [Azure portal > Cost Management > Cost analysis](#). There are several ways to analyze costs. This [Cost Management quickstart](#) should help you get started. The figures in the following screenshot are used for example purposes and aren't intended to reflect actual amounts.



Make sure you're using your new resource group as the scope. Explore the daily costs and forecasts to get an idea of how much your log integration could cost.

Calculate estimated costs

From the [Azure pricing calculator ↗](#) landing page, you can estimate the costs for various products.

- [Azure Monitor ↗](#)
- [Azure storage ↗](#)
- [Azure Event Hubs ↗](#)
- [Microsoft Sentinel ↗](#)

Once you have an estimate for the GB/day that will be sent to an endpoint, enter that value in the [Azure pricing calculator ↗](#). The figures in the following screenshot are used for example purposes and aren't intended to reflect actual prices.

Azure Monitor

Region:

East US

Log Data Ingestion \$660.50

- i Daily log data ingested will depend on what you are monitoring with Log Analytics. [Learn more](#) about estimating data volumes.

Estimate Data Volume

- i Use the estimator to get the data ranges, and enter the amount in the box.

Estimate Data Volume For Monitoring VMs

Estimate Data Volume Using Container Insights

Estimate Data Volume Based On Application Activity

Analytics Logs

8 x 30 x \$2.30 = \$540.50
Daily logs ingested (GB/day) Days Per GB

- i This estimate is calculated using the most optimal pricing tier for the data ingestion. This calculation uses **Pay-As-You-Go tier**. [Learn more](#) about the pricing tiers

Basic Logs

8 x 30 x \$0.50 = \$120.00
Per day (GB) Days Per GB

Feedback

Was this page helpful?

 Yes

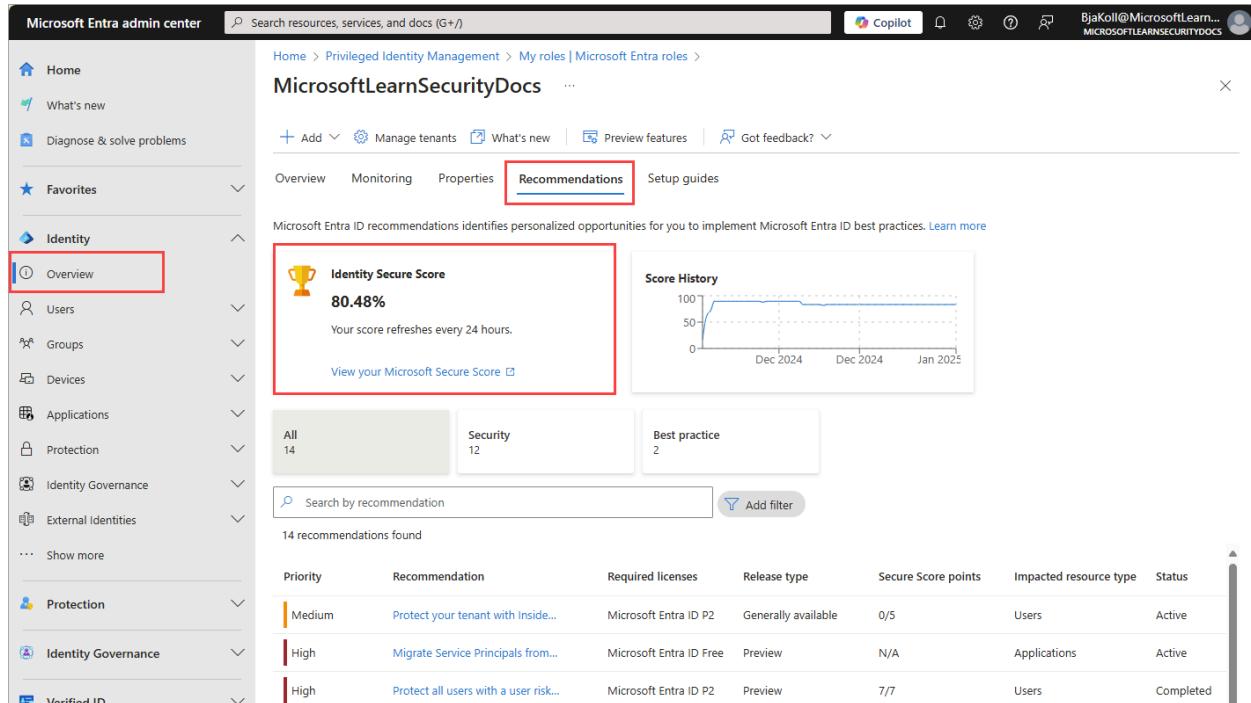
 No

Provide product feedback 

What is Identity Secure Score?

Article • 01/26/2025

The Identity Secure Score is shown as a percentage that functions as an indicator for how aligned you are with Microsoft's recommendations for security. Each improvement action in Identity Secure Score is tailored to your configuration. You can access the score and view individual recommendations related to your score in Microsoft Entra recommendations. You can also see how your score has changed over time.



The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with categories like Home, What's new, Diagnose & solve problems, Favorites, Identity (which is selected and highlighted with a red box), Protection, Identity Governance, and Verified ID. Under Identity, 'Overview' is also highlighted with a red box. The main content area shows the 'Privileged Identity Management' section with a sub-section for 'My roles | Microsoft Entra roles'. A card displays the 'Identity Secure Score' at 80.48%, with a note that it refreshes every 24 hours. To the right is a 'Score History' chart showing a steady increase from around 50% to 80% over the last few months. Below the chart, there are three tabs: All (14), Security (12), and Best practice (2). A search bar and a 'Add filter' button are also present. At the bottom, a table lists 14 recommendations, each with a priority level (Medium, High), a description, required licenses (e.g., Microsoft Entra ID P2, Free), release type (e.g., Generally available, Preview), secure score points (e.g., 0/5, N/A, 7/7), impacted resource type (e.g., Users, Applications), and status (e.g., Active, Completed).

The following recommendations are included in the Identity Secure Score:

- Require multifactor authentication (MFA) for administrative roles
- Ensure all users can complete MFA
- Enable policy to block legacy authentication
- Do not expire passwords
- Protect all users with a user risk policy
- Protect all users with a sign-in risk policy
- Enable password hash sync if hybrid
- Do not allow users to grant consent to unreliable applications
- Use least privileged administrative roles
- Designate more than one Global Administrator
- Enable self-service password reset

How does the Identity Secure Score benefit me?

This score helps to:

- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements

By following the improvement actions in the Microsoft Entra recommendations, you can:

- Improve your security posture and your score
- Take advantage the features available to your organization as part of your identity investments

How does it work?

Every 24 hours, we look at your security configuration and compare your settings with the recommended best practices. Based on the outcome of this evaluation, a new score is calculated for your directory. It's possible that your security configuration isn't fully aligned with the best practice guidance and the improvement actions are only partially met. In these scenarios, you're awarded a portion of the max score available for the control.

Prerequisites

- Identity Secure Score is available to free and paid customers.
- Some recommendations require a paid license to view and act on. For more information, see [What are Microsoft Entra recommendations](#).
- To update the status of an improvement action, you need to have [Security Administrator](#), [Exchange Administrator](#), or [SharePoint Administrator](#) permissions.
- To view the improvement action but not update, you need to have [Helpdesk Administrator](#), [User Administrator](#), [Service Support Administrator](#), [Security Reader](#), [Security Operator](#), or [Global Reader](#) permissions.

How do I use the Identity Secure Score?

To access the Identity Secure Score:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Global Reader](#).
2. Browse to **Protection > Identity Secure Score** to view the dashboard.

The score and related recommendations are also found at **Identity > Overview > Recommendations**.

Each recommendation is measured based on your configuration. If you're using non-Microsoft products to enable a best practice recommendation, you can indicate this configuration in the settings of an improvement action. You might set recommendations to be ignored if they don't apply to your environment. An ignored recommendation doesn't contribute to the calculation of your score.

Improvement action X

Use limited administrative roles

SCORE IMPACT ⓘ +1.79%

CURRENT SCORE ⓘ 1

MAX SCORE ⓘ 1

STATUS ⓘ

To address

To address

Risk accepted

Planned

Resolved through third party

Resolved through alternate mitigation

administrative privileged account being breached.

USER IMPACT ⓘ Low

IMPLEMENTATION COST ⓘ Low

WHAT AM I ABOUT TO CHANGE? ⓘ Reduce the number of persistent global administrator roles

Secure score updates can take up to 48 hours.

Save

- **To address** - You recognize that the improvement action is necessary and plan to address it at some point in the future. This state also applies to actions that are detected as partially, but not fully completed.
- **Risk accepted** - Security should always be balanced with usability, and not every recommendation works for everyone. When that is the case, you can choose to accept the risk, or the remaining risk, and not enact the improvement action. You aren't awarded any points, and the action isn't visible in the list of improvement actions. You can view this action in history or undo it at any time.
- **Planned** - There are concrete plans in place to complete the improvement action.
- **Resolved through third party** and **Resolved through alternate mitigation** - The improvement action was addressed by a non-Microsoft application or software, or an internal tool. You're awarded the points the action is worth, so your score better

reflects your overall security posture. If a non-Microsoft or internal tool no longer covers the control, you can choose another status. Keep in mind, Microsoft has no visibility into the completeness of implementation if the improvement action is marked as either of these statuses.

Frequently asked questions

Many factors can affect your score. Here are some frequently asked questions about the Identity Secure Score.

How are the recommendations scored?

Recommendations can be scored in two ways. Some are scored in a binary fashion, so 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, the recommendation states there's a maximum of 10.71% increase if you protect all your users with MFA. You have 5 of 100 total users protected, so you're given a partial score around 0.53% ($5 \text{ protected} / 100 \text{ total} * 10.71\% \text{ maximum} = 0.53\% \text{ partial score}$).

What does [Not Scored] mean?

Actions labeled as [Not Scored] are ones you can perform in your organization but aren't scored. So, you can still improve your security, but you aren't given credit for those actions right now.

My score changed. How do I figure out why?

The [Microsoft 365 Defender portal](#) shows your complete Microsoft secure score. You can easily see all the changes to your secure score by reviewing the in-depth changes on the history tab.

Does the score measure my risk of getting breached?

No, score doesn't express an absolute measure of how likely you're to get breached. It expresses the extent to which you adopted features that can *offset* risk. No service can guarantee protection, and the score shouldn't be interpreted as a guarantee in any way.

How should I interpret my 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 multifactor 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.

How does the Identity Secure Score relate to the Microsoft 365 secure score?

The [Microsoft secure score](#) contains five distinct control and score categories:

- Identity
- Data
- Devices
- Infrastructure
- Apps

The Identity Secure Score represents the identity part of the Microsoft secure score. This overlap means that your recommendations for the Identity Secure Score and the identity score in Microsoft are the same.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

What is the Usage and insights report in Microsoft Entra ID?

Article • 05/06/2025

With the Microsoft Entra **Usage and insights** reports, you can get an application-centric view of your sign-in data. Usage & insights includes a report on authentication methods, service principal sign-ins, and application credential activity. You can find answers to the following questions:

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

Prerequisites

To access the data from Usage and insights you must have:

- A Microsoft Entra tenant
- A Microsoft Entra ID P1 or P2 license to view the sign-in data
- A user in the Reports Reader, Security Reader, or Security Administrator role.

Access Usage and insights

You can access the Usage and insights reports from the Azure portal and using Microsoft Graph.

Microsoft Entra admin center

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to [Entra ID > Monitoring & health > Usage & insights](#).

The **Usage & insights** reports are also available from the **Enterprise applications** area of Microsoft Entra ID. All users can access their own sign-ins at the [My Sign-Ins portal](#).

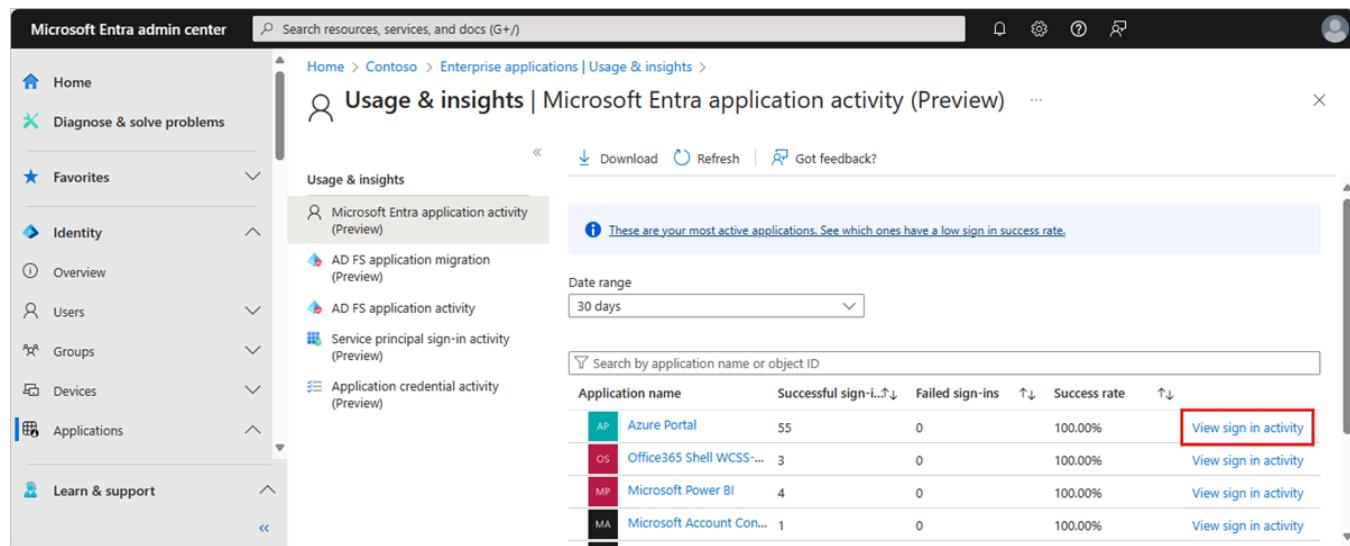
Microsoft Entra application activity (preview)

The **Microsoft Entra application activity (preview)** report shows the list of applications with one or more sign-in attempts. Any application activity during the selected date range appears

in the report. The report allows you to sort by the number of successful sign-ins, failed sign-ins, and the success rate.

It's possible that activity for a deleted application might appear in the report if the activity took place during the selected date range *and* before the application was deleted. Other scenarios could include a user attempting to sign in to an application that doesn't have a service principal associated with the app. For these types of scenarios, you might need to review the audit logs or sign-in logs to investigate further.

To view the details of the sign-in activity for an application, select the **View sign-in activity** link for the application.



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices, Applications, and Learn & support. The main content area is titled "Usage & insights | Microsoft Entra application activity (Preview)". It features a "Usage & insights" section with a message about active applications and a "Date range" dropdown set to "30 days". Below this is a search bar and a table of application activity. The table has columns for Application name, Successful sign-ins, Failed sign-ins, Success rate, and a "View sign in activity" link. The "View sign in activity" links for all five applications listed are highlighted with a red box.

Application name	Successful sign-ins	Failed sign-ins	Success rate	
AP Azure Portal	55	0	100.00%	View sign in activity
OS Office365 Shell WCSS...	3	0	100.00%	View sign in activity
MP Microsoft Power BI	4	0	100.00%	View sign in activity
MA Microsoft Account Con...	1	0	100.00%	View sign in activity

The sign-in activity graph uses interactive user sign-ins. Select a day in the application usage graph to see a detailed list of the sign-in activities for the application. This detailed list is actually the sign-in log with the filter set to the selected application and date. The details of any sign-in failures appear below the table.

Usage & insights - Microsoft Graph Command Line Tools

X

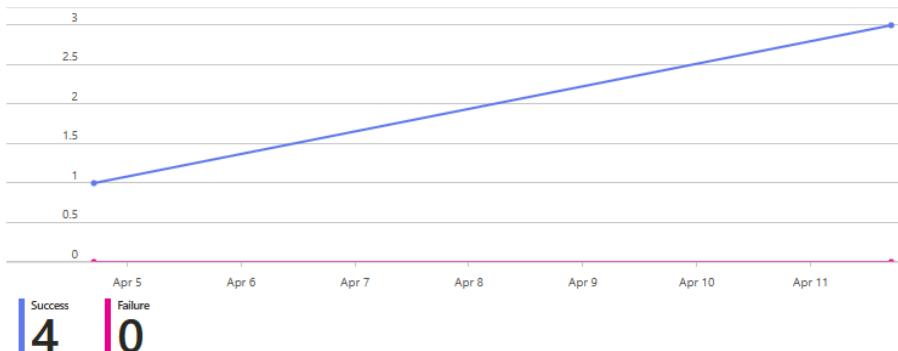
[Got feedback?](#)

Date

30 days

[Review inactive users](#)
[Start a new access review](#)

Sign-in activity



Sign-in failures

Error	Error code	Occurrences	Last seen
No results			

This report now includes applications owned by Microsoft Services that are instantiated in customer tenants. These applications can be involved in service-to-service authentications. When you select the applications from the **Usage and insights** report, the results say "Not found" because the application is not owned by your tenant, but is only instantiated in your tenant. To see the sign-in activity for these applications, select the **View sign-in activity** link.

Application activity using Microsoft Graph

You can view the `applicationSignInSummary` or `applicationSignInDetailedSummary` of Microsoft Entra application activity with Microsoft Graph.

Add the following query to view the **sign-in summary**, then select the **Run query** button.

HTTP

GET

```
https://graph.microsoft.com/beta/reports/getAzureADApplicationSignInSummary(period = '{period}')
```

Add the following query to view the **sign-in details**, then select the **Run query** button.

HTTP

```
GET https://graph.microsoft.com/beta/reports/applicationSignInDetailedSummary/{id}
```

For more information, see [Application sign-in in Microsoft Graph](#).

AD FS application activity

The AD FS application activity report in Usage & insights lists all Active Directory Federated Services (AD FS) applications in your organization that had an active user sign-in to authenticate in the last 30 days. These applications haven't been migrated to Microsoft Entra ID for authentication.

Viewing the AD FS application activity using Microsoft Graph retrieves a list of the `relyingPartyDetailedSummary` objects, which identifies the relying party to a particular Federation Service.

Add the following query, then select the Run query button.

```
HTTP
```

```
GET
```

```
https://graph.microsoft.com/beta/reports/getRelyingPartyDetailedSummary(period='{period}')
```

For more information, see [AD FS application activity in Microsoft Graph](#).

Authentication methods activity

The Authentication methods activity in Usage & insights displays visualizations of the different authentication methods used by your organization. The **Registration tab** displays statistics of users registered for each of your available authentication methods. Select the **Usage** tab at the top of the page to see actual usage for each authentication method.

You can also access several other reports and tools related to authentication.

Are you planning on running a registration campaign to nudge users to sign up for MFA? Use the **Registration campaign** option from the side menu to set up a registration campaign. For more information, see [Nudge users to set up Microsoft Authenticator](#).

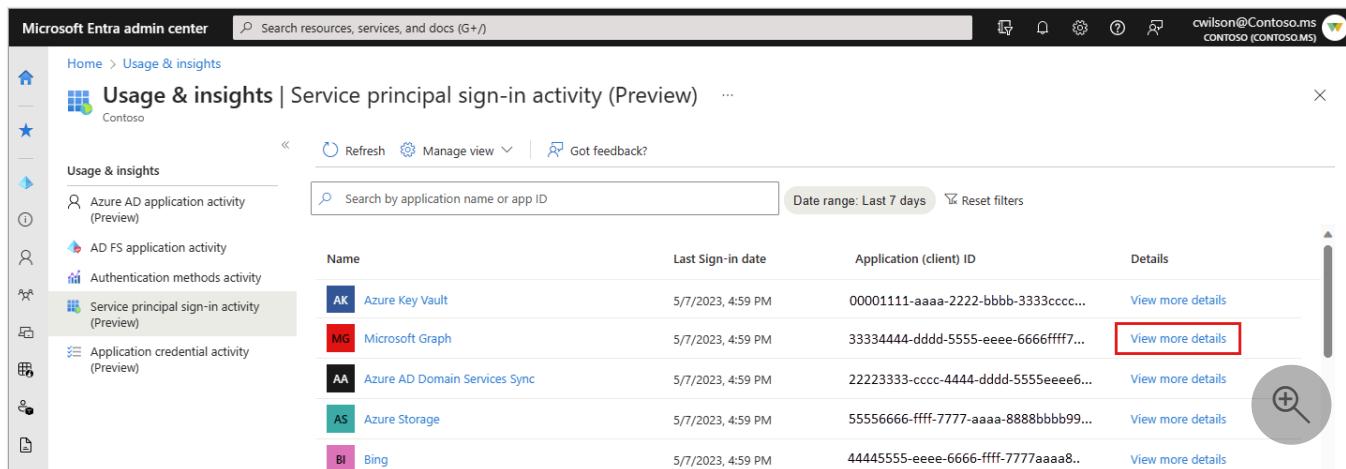
Looking for the details of a user and their authentication methods? Look at the **User registration details** report from the side menu and search for a name or UPN. The default MFA method and other methods registered are displayed. You can also see if the user is capable of registering for one of the authentication methods.

Looking for the status of an authentication registration or reset event of a user? Look at the **Registration and reset events** report from the side menu and then search for a name or UPN.

You can see the method used to attempt to register or reset an authentication method.

Service principal sign-in activity (preview)

The Service principal sign-in activity (preview) report provides the last activity date for every service principal. The report provides you with information on the usage of the service principal - whether it was used as a client or resource app and whether it was used in an app-only or delegated context. The report shows the last time the service principal was used.



The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a 'Usage & insights' section with several items: Azure AD application activity (Preview), AD FS application activity, Authentication methods activity, Service principal sign-in activity (Preview) (which is selected and highlighted in grey), and Application credential activity (Preview). The main content area is titled 'Usage & insights | Service principal sign-in activity (Preview)' and shows a table of activity. The table has columns for Name, Last Sign-in date, Application (client) ID, and Details. Five rows are listed: AK (Azure Key Vault), MG (Microsoft Graph), AA (Azure AD Domain Services Sync), AS (Azure Storage), and BI (Bing). The 'View more details' link for MG is highlighted with a red box. A magnifying glass icon is also present on the right side of the table.

Name	Last Sign-in date	Application (client) ID	Details
AK Azure Key Vault	5/7/2023, 4:59 PM	00001111-aaaa-2222-bbbb-3333cccc...	View more details
MG Microsoft Graph	5/7/2023, 4:59 PM	33334444-dddd-5555-eeee-6666ffff7...	View more details
AA Azure AD Domain Services Sync	5/7/2023, 4:59 PM	22223333-cccc-4444-dddd-5555eeee6...	View more details
AS Azure Storage	5/7/2023, 4:59 PM	55556666-ffff-7777-aaaa-8888bbbb99...	View more details
BI Bing	5/7/2023, 4:59 PM	44445555-eeee-6666-ffff-7777aaaa8..	View more details

Select the **View more details** link to locate the client and object IDs for the application and specific service principal sign-in activity.

Service principal sign-in activity

Microsoft Graph

App info

Application Client ID 44445555-eeee-6666-ffff-7777aaa... 

Application Object ID dddddddd-3333-4444-5555-eeeeeee... 

App only access

Authentication as client None

Authentication as resource 5/7/2023, 4:59 PM

Delegated access

Authentication as client 5/7/2023, 1:42 PM

Authentication as resource 5/7/2023, 4:47 PM 

Service principal sign-in activity using Microsoft Graph

The `servicePrincipalSignInActivity` reports can be viewed using Microsoft Graph.

Add the following query in Graph Explorer to retrieve the service principal sign-in activity, then select the **Run query** button.

HTTP

```
GET https://graph.microsoft.com/beta/reports/servicePrincipalSignInActivities/{id}
```

Example response:

JSON

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#reports/servicePrincipalSignInActivities",
```

```

"id": "A1bC2dE3fH4iJ5kL6mN7oP8qR9sT0u",
"appId": "00001111-aaaa-2222-bbbb-3333cccc4444",
"delegatedClientSignInActivity": {
    "lastSignInDateTime": "2021-01-01T00:00:00Z",
    "lastSignInRequestId": "2d245633-0f48-4b0e-8c04-546c2bcd61f5"
},
"delegatedResourceSignInActivity": {
    "lastSignInDateTime": "2021-02-01T00:00:00Z",
    "lastSignInRequestId": "d2b4c623-f930-42b5-9519-7851ca604b16"
},
"applicationAuthenticationClientSignInActivity": {
    "lastSignInDateTime": "2021-03-01T00:00:00Z",
    "lastSignInRequestId": "b71f24ec-f212-4306-b2ae-c229e15805ea"
},
"applicationAuthenticationResourceSignInActivity": {
    "lastSignInDateTime": "2021-04-01T00:00:00Z",
    "lastSignInRequestId": "53e6981f-2272-4deb-972c-c8272aca986d"
},
"lastSignInActivity": {
    "lastSignInDateTime": "2021-04-01T00:00:00Z",
    "lastSignInRequestId": "cd9733e8-d75a-468f-a63d-6e82bd48c05e"
}
}

```

For more information, see [List service principal activity in Microsoft Graph](#).

Application credential activity (preview)

The Application credential activity (preview) report provides the last credential activity date for every application credential. The report provides the credential type (certificate or client secret), the last used date, and the expiration date. With this report, you can view the expiration dates of all your applications in one place.

To view the details of the application credential activity, select the **View more details** link. These details include the application object, service principal, and resource IDs. You can also see if the credential origin is the application or the service principal.

Name	Application (client) ID	Credential ID	Credential type	Last used date	Expiration date	Details
WG App	00001111-aaaa-2222-bbbb-3333cccc4444	bbbbbbbb-1c1c-2d2d-3e3e	Unknown	8/8/2024, 3:24 PM	11/19/2024, 5:42 PM	View more details
Defender App	33334444-dddd-5555-eeee-6666	ddddddd-3e3e-4f4f-5a5a	Unknown	7/25/2024, 12:22 PM	11/17/2024, 8:56 PM	View more details
Portable ID card App	66667777-aaaa-8888-bbbb-9999	ffffffff-5a5a-6b6b-7c7c	Unknown	7/16/2024, 7:34 AM	11/14/2024, 8:15 AM	View more details

When you select the **View more details** link, you can see the application object ID and resource ID, in addition to the details visible in the report.

Application Credential activity

Silverfort Admin Console - Woodgrove

Key Usage	sign
Application Object ID	0000-1111-aa00 
Service principal ID	1100-00aa-11100 
Resource ID	00000002-0000-0000-c000-000000000000 
Credential Origin	application 

Application credential activity using Microsoft Graph

Application credential activity can be viewed and managed using Microsoft Graph on the `/beta` endpoint. You can get the application credential sign-in activity by entity `id`, `keyId`, and `appId`.

To get started, follow these instructions to work with `appCredentialSignInActivity` using Microsoft Graph in Graph Explorer.

1. Sign in to [Graph Explorer](#).
2. Select **GET** as the HTTP method from the dropdown.
3. Set the API version to **beta**.
4. Add the following query to retrieve recommendations, then select the **Run query** button.

HTTP

GET

`https://graph.microsoft.com/beta/reports/appCredentialSignInActivities/{id}`

Example response:

JSON

```
{  
  "@odata.type": "#microsoft.graph.appCredentialSignInActivity",  
  "id": "A1bC2dE3fH4iJ5kL6mN7oP8qR9sT0u",  
  "keyId": "aaaaaaaa-0b0b-1c1c-2d2d-333333333333",  
  "keyType": "certificate",  
  "keyUsage": "sign",  
  "lastModifiedDateTime": "2023-01-12T12:00:00Z",  
  "resourceId": "00000002-0000-0000-c000-000000000000",  
  "servicePrincipalId": "1100-00aa-11100",  
  "status": "Success",  
  "timeZone": "UTC",  
  "version": 1  
}
```

```
"appId": "11112222-bbbb-3333-cccc-4444dddd5555",
"appObjectId": "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb",
"servicePrincipalObjectId": "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb",
"resourceId": "a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1",
"credentialOrigin": "application",
"expirationDate": "2021-04-01T21:36:48-8:00",
"signInActivity": {
    "lastSignInDateTime": "2021-04-01T00:00:00-8:00",
    "lastSignInRequestId": "b0a282a3-68ec-4ec8-aef0-290ed4350271"
}
}
```

For more information, see [Application credential activity in Microsoft Graph](#).

Quickstart: Analyze sign-ins with the Microsoft Entra sign-in log

Article • 02/26/2025

With the information in the Microsoft Entra sign-in log, you can figure out what happened if a sign-in of a user failed. This quickstart shows how to locate failed sign-in using the sign-in log.

Prerequisites

To complete the scenario in this quickstart, you need:

- An Azure subscription. If you don't have one, create a [free account](#).
- A Microsoft Entra tenant with a [Premium P1 license](#).
- A user with the **Reports Reader**, **Security Reader**, or **Security Administrator** role for the tenant.
- A **test account called Isabella Simonsen** - If you don't know how to create a test account, see [Add cloud-based users](#).

Perform a failed sign-in

The goal of this step is to create a record of a failed sign-in in the Microsoft Entra sign-in log.

1. Sign in to the [Microsoft Entra admin center](#) as Isabella Simonsen using an incorrect password.
2. Wait for 5 minutes to ensure that you can find the event in the sign-in log.

Find the failed sign-in

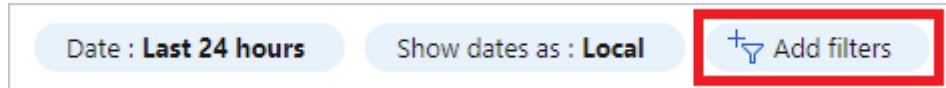
This section provides you with the steps to analyze a failed sign-in. Filter the sign-in log to remove all records that aren't relevant to your analysis. For example, set a filter to display only the records of a specific user. Then you can review the error details. The log details provide helpful information. You can also look up the error using the [sign-in error lookup tool](#). This tool might provide you with information to troubleshoot a sign-in error.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.

2. Browse to **Identity > Monitoring & health > Sign-in logs**.

3. Adjust the filter to view only the records for Isabella Simonsen:

- Open the **Add filters**, select **User**, and then select **Apply**.



- In the **User** textbox, type **Isabella Simonsen**, and then select **Apply**.

4. Select the failed sign-in attempt and view the details.

5. Copy the **Sign-in error code**.

Status	Failure
Sign-in error code	50126

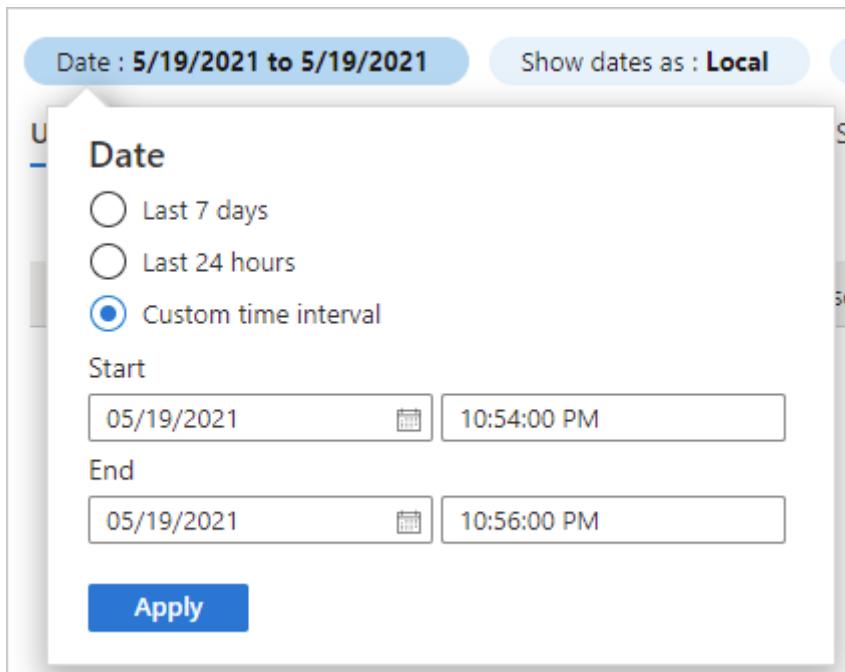
6. Paste the error code into the textbox of the [sign-in error lookup tool](#), and then select **Submit**.

Review the outcome of the tool and determine whether it provides you with additional information.

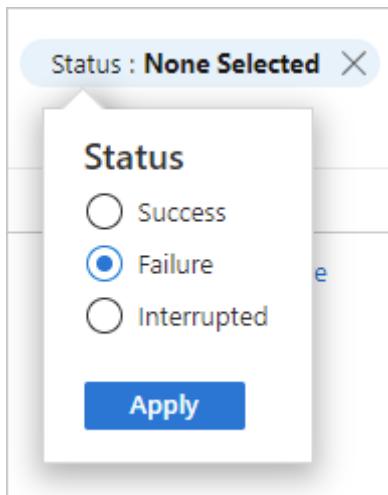
More tests

Now, that you know how to find an entry in the sign-in log by name, you should also try to find the record using the following filters:

- **Date** - Try to find Isabella using a **Start** and an **End**.



- Status - Try to find Isabella using **Status: Failure**.



Clean up resources

When no longer needed, delete the test user. If you don't know how to delete a Microsoft Entra user, see [Delete users from Microsoft Entra ID](#).

Related content

- Learn how to use the sign-in diagnostic

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Quickstart: Analyze a sign-in with the Microsoft Graph API

Article • 01/29/2025

In this Quickstart, you'll use the information in the Microsoft Entra sign-in logs to figure out what happened if a sign-in of a user failed. This quickstart shows you how to access the sign-in log using the Microsoft Graph API.

Prerequisites

To complete the scenario in this quickstart, you need:

- **Access to a Microsoft Entra tenant:** If you don't have access to a Microsoft Entra tenant, see [Create your Azure free account today](#).
- **A test account called Isabella Simonsen:** If you don't know how to create a test account, see [Add cloud-based users](#).
- **Access to the Microsoft Graph API:** If you don't have access yet, see [Microsoft Graph authentication and authorization basics](#).

Perform a failed sign-in

The goal of this step is to create a record of a failed sign-in in the Microsoft Entra sign-in log.

1. Sign in to the [Microsoft Entra admin center](#) as Isabella Simonsen using an incorrect password.
2. Wait for 5 minutes to ensure that you can find a record of the sign-in entry in the logs.

Find the failed sign-in

This section provides the steps to locate the failed sign-in attempt using the Microsoft Graph API.

1. Sign in to [Microsoft Graph Explorer](#) as a user with permissions to run a query.
2. Select **Modify permissions** to ensure you have the correct permissions.
3. Select **GET** as the HTTP method from the dropdown.

4. Set the API version to **beta**.
5. Enter the following query and select **Run query**:

```
https://graph.microsoft.com/beta/auditLogs/signIns?  
$top=10&$filter=userDisplayName eq 'Isabella Simonsen'
```
6. Review the query response and locate the **status** section of the response.

```
"mfaDetail": null,  
"authenticationAppDeviceDetails": null,  
"status": {  
    "errorCode": 50126,  
    "failureReason": "Error validating credentials due to invalid username or password.",  
    "additionalDetails": "The user didn't enter the right credentials. It's expected to  
    see some number of these errors in your logs due to users making mistakes."  
},  
"deviceDetail": {  
    "deviceId": "",  
    "displayName": "",  
    "operatingSystem": "Windows10",  
    "browser": "Edge 119.0.0",
```

Clean up resources

When no longer needed, delete the test user. If you don't know how to delete a Microsoft Entra user, see [Delete users from Microsoft Entra ID](#).

Next steps

[Analyze activity logs with Microsoft Graph](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

How to access activity logs in Microsoft Entra ID

Article • 11/11/2024

The data collected in your Microsoft Entra logs enables you to assess many aspects of your Microsoft Entra tenant. To cover a broad range of scenarios, Microsoft Entra ID provides you with several options to access your activity log data. As an IT administrator, you need to understand the intended uses cases for these options, so that you can select the right access method for your scenario.

You can access Microsoft Entra activity logs and reports using the following methods:

- Stream activity logs to an [event hub](#) to integrate with other tools
- Access activity logs through the [Microsoft Graph API](#)
- Integrate activity logs with [Azure Monitor logs](#)
- Monitor activity in real-time with [Microsoft Sentinel](#)
- View activity logs and reports in the [Azure portal](#)
- Export activity logs for [storage and queries](#)

Each of these methods provides you with capabilities that might align with certain scenarios. This article describes those scenarios, including recommendations and details about related reports that use the data in the activity logs. Explore the options in this article to learn about those scenarios so you can choose the right method.

Prerequisites

- A working Microsoft Entra tenant with the appropriate Microsoft Entra license associated with it.
 - For a full list of license requirements, see [Microsoft Entra monitoring and health licensing](#).
- Audit logs are available for features that you have licensed.
- [Reports Reader](#) is the least privileged role required to access the activity logs.
- [Security Administrator](#) is the least privileged role required to configure diagnostic settings.
- To consent to the required permissions to view logs with Microsoft Graph, you need the [Privileged Role Administrator](#).
- For a full list of roles, see [Least privileged role by task](#).

The required licenses vary based on the monitoring and health capability.

Capability	Microsoft Entra ID Free	Microsoft Entra ID P1 or P2 / Microsoft Entra Suite
Audit logs	Yes	Yes
Sign-in logs	Yes	Yes
Provisioning logs	No	Yes
Custom security attributes	Yes	Yes
Health	No	Yes
Microsoft Graph activity logs	No	Yes
Usage and insights	No	Yes

View logs through the Microsoft Entra admin center

For one-off investigations with a limited scope, the [Microsoft Entra admin center](#) is often the easiest way to find the data you need. The user interface for each of these reports provides you with filter options enabling you to find the entries you need to solve your scenario.

The data captured in the Microsoft Entra activity logs are used in many reports and services. You can review the sign-in, audit, and provisioning logs for one-off scenarios or use reports to look at patterns and trends. The data from the activity logs help populate the Identity Protection reports, which provide information security related risk detections that Microsoft Entra ID can detect and report on. Microsoft Entra activity logs also populate Usage and insights reports, which provide usage details for your tenant's applications.

Recommended uses

The reports available in the Azure portal provide a wide range of capabilities to monitor activities and usage in your tenant. The following list of uses and scenarios isn't exhaustive, so explore the reports for your needs.

- Research a user's sign-in activity or track an application's usage.

- Review details around group name changes, device registration, and password resets with audit logs.
- Use the Identity Protection reports for monitoring at risk users, risky workload identities, and risky sign-ins.
- Review the sign-in success rate in the Microsoft Entra application activity (preview) report from Usage and insights to ensure that your users can access the applications in use in your tenant.
- Compare the different authentication methods your users prefer with the Authentication methods report from Usage and insights.

Quick steps

Use the following basic steps to access the reports in the Microsoft Entra admin center.

Microsoft Entra activity logs

1. Browse to **Identity > Monitoring & health > Audit logs/Sign-in logs/Provisioning logs**.
2. Adjust the filter according to your needs.
 - [Learn how to filter activity logs](#)
 - [Explore the Microsoft Entra audit log categories and activities](#)
 - [Learn about basic info in the Microsoft Entra sign-in logs](#)

Audit logs can be accessed directly from the area of the Microsoft Entra admin center where you're working. For example, if you're in the **Groups or Licenses** section of Microsoft Entra ID, you can access the audit logs for those specific activities directly from that area. When you access the audit logs in this way, the filter categories are automatically set. If you're in **Groups**, the audit log filter category is set to **GroupManagement**.

Stream logs to an event hub to integrate with SIEM tools

Streaming your activity logs to an event hub is required to integrate your activity logs with Security Information and Event Management (SIEM) tools, such as Splunk and SumoLogic. Before you can stream logs to an event hub, you need to [set up an Event Hubs namespace and an event hub](#) in your Azure subscription.

Recommended uses

The SIEM tools you can integrate with your event hub can provide analysis and monitoring capabilities. If you're already using these tools to ingest data from other sources, you can stream your identity data for more comprehensive analysis and monitoring. We recommend streaming your activity logs to an event hub for the following types of scenarios:

- You need a big data streaming platform and event ingestion service to receive and process millions of events per second.
- You're looking to transform and store data by using a real-time analytics provider or batching/storage adapters.

Quick steps

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.
2. Create an Event Hubs namespace and event hub.
3. Browse to **Identity > Monitoring & health > Diagnostic settings**.
4. Choose the logs you want to stream, select the **Stream to an event hub** option, and complete the fields.
 - [Set up an Event Hubs namespace and an event hub](#)
 - [Learn more about streaming activity logs to an event hub](#)

Your independent security vendor should provide you with instructions on how to ingest data from Azure Event Hubs into their tool.

Access logs with the Microsoft Graph API

The Microsoft Graph API provides a unified programmability model that you can use to access data for your Microsoft Entra ID P1 or P2 tenants. It doesn't require an administrator or developer to set up extra infrastructure to support your script or app.

Tip

Steps in this article might vary slightly based on the portal you start from.

Recommended uses

Using Microsoft Graph explorer, you can run queries to help you with the following types of scenarios:

- View tenant activities such as who made a change to a group and when.
- Mark a Microsoft Entra sign-in event as safe or confirmed compromised.
- Retrieve a list of application sign-ins for the last 30 days.

Note

Microsoft Graph allows you to access data from multiple services that impose their own throttling limits. For more information on activity log throttling, see [Microsoft Graph service-specific throttling limits](#).

Quick steps

1. [Configure the prerequisites](#).
2. Sign in to [Graph Explorer](#).
3. Set the HTTP method and API version.
4. Add a query then select the **Run query** button.
 - [Familiarize yourself with the Microsoft Graph properties for directory audits](#)
 - [Complete the MS Graph Quickstart guide](#)

Integrate logs with Azure Monitor logs

With the Azure Monitor logs integration, you can enable rich visualizations, monitoring, and alerting on the connected data. Log Analytics provides enhanced query and analysis capabilities for Microsoft Entra activity logs. To integrate Microsoft Entra activity logs with Azure Monitor logs, you need a Log Analytics workspace. From there, you can run queries through Log Analytics.

Recommended uses

Integrating Microsoft Entra logs with Azure Monitor logs provides a centralized location for querying logs. We recommend integrating logs with Azure Monitor for the following types of scenarios:

- Compare Microsoft Entra sign-in logs with logs published by other Azure services.
- Correlate sign-in logs against Azure Application insights.
- Query logs using specific search parameters.

Quick steps

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Security Administrator**.
2. [Create a Log Analytics workspace](#).
3. Browse to **Identity > Monitoring & health > Diagnostic settings**.
4. Choose the logs you want to stream, select the **Send to Log Analytics workspace** option, and complete the fields.
5. Browse to **Identity > Monitoring & health > Log Analytics** and begin querying the data.
 - [Integrate Microsoft Entra logs with Azure Monitor logs](#)
 - [Learn how to query using Log Analytics](#)

Monitor events with Microsoft Sentinel

Sending sign-in and audit logs to Microsoft Sentinel provides your security operations center with near real-time security detection and threat hunting. The term *threat hunting* refers to a proactive approach to improve the security posture of your environment. As opposed to classic protection, threat hunting tries to proactively identify potential threats that might harm your system. Your activity log data might be part of your threat hunting solution.

Recommended uses

We recommend using the real-time security detection capabilities of Microsoft Sentinel if your organization needs security analytics and threat intelligence. Use Microsoft Sentinel if you need to:

- Collect security data across your enterprise.
- Detect threats with vast threat intelligence.
- Investigate critical incidents guided by AI.
- Respond rapidly and automate protection.

Quick steps

1. Learn about the [prerequisites, roles, and permissions](#).
2. [Estimate potential costs](#).
3. [Onboard to Microsoft Sentinel](#).
4. [Collect Microsoft Entra data](#).
5. [Begin hunting for threats](#).

Export logs for storage and queries

The right solution for your long-term storage depends on your budget and what you plan on doing with the data. You've got three options:

- Archive logs to Azure Storage
- Download logs for manual storage
- Integrate logs with Azure Monitor logs

[Azure Storage](#) is the right solution if you aren't planning on querying your data often. For more information, see [Archive directory logs to a storage account](#).

If you plan to query the logs often to run reports or perform analysis on the stored logs, you should [integrate your data with Azure Monitor logs](#).

If your budget is tight, and you need a cheap method to create a long-term backup of your activity logs, you can [manually download your logs](#). The user interface of the activity logs in the portal provides you with an option to download the data as **JSON** or **CSV**. One trade off of the manual download is that it requires more manual interaction. If you're looking for a more professional solution, use either Azure Storage or Azure Monitor.

Recommended uses

We recommend setting up a storage account to archive your activity logs for those governance and compliance scenarios where long-term storage is required.

If you want to long-term storage *and* you want to run queries against the data, review the section on [integrating your activity logs with Azure Monitor Logs](#).

We recommend manually downloading and storing your activity logs if you have budgetary constraints.

Quick steps

Use the following basic steps to archive or download your activity logs.

Archive activity logs to a storage account

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.
2. Create a storage account.
3. Browse to **Identity > Monitoring & health > Diagnostic settings**.
4. Choose the logs you want to stream, select the **Archive to a storage account** option, and complete the fields.

- Review the data retention policies

Next steps

- Stream logs to an event hub
- Archive logs to a storage account
- Integrate logs with Azure Monitor logs

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

How to download and analyze the Microsoft Entra provisioning logs

Article • 03/20/2025

The Microsoft Entra provisioning logs provide details about the provisioning events that occur in your tenant. You can use the information captured in the provisioning logs to help troubleshoot issues with a provisioned user.

This article describes the options for downloading the provisioning logs from the Microsoft Entra admin center and how to analyze the logs. Error codes and special considerations are also included.

Prerequisites

- A working Microsoft Entra tenant with a Microsoft Entra ID P1 or P2 license associated with it.
- [Reports Reader](#) is the least privileged role required to access the provisioning logs.
 - For a full list of roles, see [Least privileged role by task](#).

How to view the provisioning logs

There are several ways to view or analyze the Provisioning logs:

- View in the Microsoft Entra admin center.
- Stream logs to [Azure Monitor](#) through diagnostic settings.
- Analyze logs through [Workbook](#) templates.
- Access logs programmatically through the [Microsoft Graph API](#).
- [Download the logs](#) as a CSV or JSON file.

To access the logs in the Microsoft Entra admin center:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Provisioning logs**.

How to download the provisioning logs

To download the provisioning logs, select **Download** from the **Provisioning logs** page. Set the filters as specific as possible to reduce the size and time of the download.

Date	Identity	Action	Source System	Target System	Status
9/8/2023, 8:33:35 AM	Source ID 103009	Create	SuccessFactors	Microsoft Entra ID	Skipped

CSV format

The CSV download includes three files:

- **ProvisioningLogs**: Downloads all the logs, except the provisioning steps and modified properties.
- **ProvisioningLogs_ProvisioningSteps**: Contains the provisioning steps and the change ID. You can use the change ID to join the event with the other two files.
- **ProvisioningLogs_ModifiedProperties**: Contains the attributes that were changed and the change ID. You can use the change ID to join the event with the other two files.

JSON format

To open the JSON file, use a text editor such as [Microsoft Visual Studio Code](#). Visual Studio Code makes the file easier to read by providing syntax highlighting. You can also open the JSON file by using browsers in an uneditable format, such as [Microsoft Edge](#).

Prettify the JSON file

The JSON file is downloaded in a format to reduce the size of the download. This format can make the payload hard to read. To prettify the file, there are two options:

- Use [Visual Studio Code to format the JSON](#).
- Use PowerShell to format the JSON. This script produces a JSON output in a format that includes tabs and spaces:

```
$JSONContent = Get-Content -Path "<PATH TO THE PROVISIONING LOGS FILE>" |  
    ConvertFrom-JSON  
  
$JSONContent | ConvertTo-Json > <PATH TO OUTPUT THE JSON FILE>
```

Parse the JSON file

You can use any programming language that you're comfortable with. The following examples are in PowerShell.

- [Read the JSON file](#):

```
$JSONContent = Get-Content -Path "<PATH TO THE PROVISIONING LOGS FILE>" |  
ConvertFrom-JSON
```

Now you can parse the data according to your scenario. Here are a couple of examples:

- Output all job IDs in the JSON file:

```
foreach ($provitem in $JSONContent) { $provitem.jobId }
```

- Output all change IDs for events where the action was "create":

```
foreach ($provitem in $JSONContent) { if ($provItem.action -eq 'Create') {  
$provitem.changeId } }
```

What you should know

Here are some tips and considerations for analyzing the provisioning logs:

- The Microsoft Entra admin center stores reported provisioning data for 30 days if you have a premium edition and 7 days if you have a free edition. You can route the provisioning logs to [Azure Monitor logs](#) for retention beyond 30 days.
- You can use the change ID attribute as unique identifier, which can be helpful when you're interacting with product support, for example.
- You might see skipped events for users who aren't in scope.
 - Example 1: If the scope is set to `all users and groups` and setup scoping filters, you might see skipped logs for users that don't meet the scoping criteria.
 - Example 2: If the scope is set to `assigned users and groups`, you might continue to see users in the logs as skipped, even though they aren't assigned to the application. The way the provisioning service receives changes from the directory causes these users to appear.
- The provisioning logs don't show role imports (applies to Amazon Web Services, Salesforce, and Zendesk). You can find the logs for role imports in the audit logs.

- Some error codes contain `AzureActiveDirectory` in the name. These error codes refer to Microsoft Entra ID, but could not be rebranded from Azure Active Directory.

Error codes

Use the following table to better understand how to resolve errors that you find in the provisioning logs.

[] Expand table

Error code	Description
Conflict, EntryConflict	<p>Correct the conflicting attribute values in either Microsoft Entra ID or the application.</p> <p>Or, review your matching attribute configuration if the conflicting user account was supposed to be matched and taken over. For more information on configuring matching attributes, see Customize user provisioning attribute-mappings for SaaS applications in Microsoft Entra ID.</p>
TooManyRequests	<p>The target app rejected this attempt to update the user because the app is receiving too many requests. There's nothing to do. This attempt is automatically retried and Microsoft was notified of this issue.</p>
InternalServerError	<p>The target app returned an unexpected error. A service issue with the target application might be preventing it from working. This attempt is automatically retried in 40 minutes.</p>
InsufficientRights, MethodNotAllowed, NotPermitted, Unauthorized	<p>Microsoft Entra ID authenticated with the target application but wasn't authorized to perform the update. Review any instructions that the target application provided, along with the respective application. For more information, see Tutorials for integrating applications with Microsoft Entra ID.</p>
UnprocessableEntity	<p>The target application returned an unexpected response. The configuration of the target application might not be correct, or a service issue with the target application might be preventing it from working.</p>
WebExceptionProtocolError	<p>An HTTP protocol error occurred while connecting to the target application. There's nothing to do. This attempt is automatically retried in 40 minutes.</p>

Error code	Description
InvalidAnchor	<p>A user that was previously created or matched by the provisioning service no longer exists. Ensure that the user exists. To force a new matching of all users, use the Microsoft Graph API to restart the job.</p>
	<p>Restarting provisioning triggers an initial cycle, which can take time to complete. Restarting provisioning also deletes the cache that the provisioning service uses to operate. That means all users and groups in the tenant must be evaluated again, and certain provisioning events might be dropped.</p>
NotImplemented	<p>The target app returned an unexpected response. The configuration of the app might not be correct, or a service issue with the target app might be preventing it from working. Review any instructions that the target application provided, along with the respective application. For more information, see Tutorials for integrating applications with Microsoft Entra ID.</p>
MandatoryFieldsMissing, MissingValues	<p>The user couldn't be created because required values are missing. Correct the missing attribute values in the source record, or review your matching attribute configuration to ensure that the required fields aren't omitted. For more information, see Customize user provisioning attribute-mappings for SaaS applications in Microsoft Entra ID.</p>
SchemaAttributeNotFound	<p>The operation couldn't be performed because an attribute was specified that doesn't exist in the target application. Ensure that your configuration is correct by referring to Customize user provisioning attribute-mappings for SaaS applications in Microsoft Entra ID.</p>
InternalError	<p>An internal service error occurred within the Microsoft Entra provisioning service. There's nothing to do. This attempt is automatically retried in 40 minutes.</p>
InvalidDomain	<p>The operation couldn't be performed because an attribute value contains an invalid domain name. Update the domain name on the user or add it to the permitted list in the target application.</p>
Timeout	<p>The operation couldn't be completed because the target application took too long to respond. There's nothing to do. This attempt is automatically retried in 40 minutes.</p>

Error code	Description
LicenseLimitExceeded	<p>The user couldn't be created in the target application because there are no available licenses for this user. Procure more licenses for the target application.</p> <p>Or, review your user assignments and attribute mapping configuration to ensure that the correct users are assigned with the correct attributes.</p>
DuplicateTargetEntries	<p>The operation couldn't be completed because more than one user in the target application was found with the configured matching attributes. Remove the duplicate user from the target application, or reconfigure your attribute mappings. For more information, see Customize user provisioning attribute-mappings for SaaS applications in Microsoft Entra ID.</p>
DuplicateSourceEntries	<p>The operation couldn't be completed because more than one user was found with the configured matching attributes. Remove the duplicate user, or reconfigure your attribute mappings. For more information, see Customize user provisioning attribute-mappings for SaaS applications in Microsoft Entra ID.</p>
ImportSkipped	<p>When each user is evaluated, the system tries to import the user from the source system. This error commonly occurs when the user who's being imported is missing the matching property defined in your attribute mappings. Without a value present on the user object for the matching attribute, the system can't evaluate scoping, matching, or export changes. The presence of this error doesn't indicate that the user is in scope, because you haven't yet evaluated scoping for the user.</p>
EntrySynchronizationSkipped	<p>The provisioning service successfully queried the source system and identified the user. No further action was taken on the user and they were skipped. The user might have been out of scope or already existed in the target system with no further changes required.</p>
SystemForCrossDomainIdentity ManagementMultipleEntriesInResponse	<p>A GET request to retrieve a user or group received multiple users or groups in the response. The system expects to receive only one user or group in the response. For example, if you do a GET Group request to retrieve a group, provide a filter to exclude members, and your System for Cross-Domain Identity Management (SCIM) endpoint returns the members, this error appears.</p>

Error code	Description
SystemForCrossDomainIdentityManagementServiceIncompatible	The Microsoft Entra provisioning service is unable to parse the response from the non-Microsoft application. Work with the application developer to ensure that the SCIM server is compatible with the Microsoft Entra SCIM client .
SchemaPropertyCanOnlyAcceptValue	The property in the target system can only accept one value, but the property in the source system has multiple. Ensure that you either map a single-valued attribute to the property that is throwing an error, update the value in the source to be single-valued, or remove the attribute from the mappings.

Error codes for cross-tenant synchronization

Use the following table to better understand how to resolve errors that you find in the provisioning logs for [cross-tenant synchronization](#). Some error codes map to more than one cause, so there are multiple rows for the same error code.

[\[+\] Expand table](#)

Error code	Cause	Solution
AzureActiveDirectoryForbidden	The dirSync enabled property is set to true. As a result, the provisioning service cannot update user properties such as immutableId and extensionProperty1-15.	Remove the attribute from your attribute mappings to prevent failures.
AzureActiveDirectoryForbidden	External collaboration settings blocked invitations.	Navigate to user settings and ensure that external collaboration settings are permitted.
AzureActiveDirectoryCannotUpdateObjectsOriginatedInExternalService	The source of authority for the user is Exchange Online. The provisioning service can't update one or more exchange attributes on the user (ex: extensionAttribute 1	Update the attribute directly in the target tenant's exchange online . For example: <code>Set-MailUser -Identity CloudMailUser5 -</code>

Error code	Cause	Solution
	- 15). This impacts users that existed in the target tenant when the dirSyncEnabled property changed from "True" to "False."	CustomAttribute2 "Updated with EXO PowerShell"
AzureActiveDirectory CannotUpdateObjectsOriginated InExternalService	The synchronization engine couldn't update one or more user properties in the target tenant.	In some cases (for example when showInAddressList property is part of the user update), the synchronization engine might automatically retry the (user) update without the offending property. Otherwise, you need to update the property directly in the target tenant.
	The operation failed in Microsoft Graph API because of Source of Authority (SOA) enforcement. Currently, the following properties show up in the list: Mail showInAddressList	
AzureDirectory B2BManagementPolicy CheckFailure	The cross-tenant synchronization policy allowing automatic redemption failed. The synchronization engine checks to ensure that the administrator of the target tenant created an inbound cross-tenant synchronization policy allowing automatic redemption. The synchronization engine also checks if the administrator of the source tenant enabled an outbound policy for automatic redemption.	Ensure that the automatic redemption setting was enabled for both the source and target tenants. For more information, see Automatic redemption setting .
AzureActiveDirectory QuotaLimitExceeded	The number of objects in the tenant exceeds the directory limit.	Check whether the quota can be increased. For information about the

Error code	Cause	Solution
	Microsoft Entra ID has limits for the number of objects that can be created in a tenant.	directory limits and steps to increase the quota, see Microsoft Entra service limits and restrictions .
InvitationCreationFailure	The Microsoft Entra provisioning service attempted to invite the user in the target tenant. That invitation failed.	Further investigation likely requires contacting support.
InvitationCreationFailureUserAccountDisabled	The Microsoft Entra provisioning service attempted to invite the user in the target tenant. That invitation failed.	The user exists in the target tenant, but the account is disabled and invitation is pending. Enable the user account in the target tenant and attempt to provision the user again.
InvitationCreationFailureInvalidPropertyValue	Potential causes: * The Primary SMTP Address is an invalid value. * UserType isn't guest or member * Group email Address isn't supported	Potential solutions: * The Primary SMTP Address has an invalid value. Resolving this issue likely requires updating the mail property of the source user. For more information, see Prepare for directory synchronization to Microsoft 365 ↗ * Ensure that the userType property is provisioned as type guest or member. Check your attribute mappings to understand how the userType attribute is mapped. * The email address of the user matches with the email address of a group in the tenant.

Error code	Cause	Solution
		Update the email address for one of the two objects.
InvitationCreation FailureAmbiguousUser	The invited user has a proxy address that matches an internal user in the target tenant. The proxy address must be unique.	To resolve this error, delete the existing internal user in the target tenant or remove this user from sync scope.
AzureActiveDirectory CannotUpdateObjects MasteredOnPremises	If the user in the target tenant was originally synchronized from AD to Microsoft Entra ID and converted to an external user, the source of authority is still on-premises and the user can't be updated.	The user can't be updated with cross-tenant synchronization.
EntityTypeNotSupported	Groups can be used to determine what users are in scope for provisioning. Groups objects cannot be synchronized.	No customer action is required. This is a skipped event. If you are using the provisioning on-demand, ensure that you choose a user rather than a group to provision.

Related content

- [Check the status of user provisioning](#)
- [Problem configuring user provisioning to a Microsoft Entra Gallery application](#)
- [Graph API for provisioning logs](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

How to analyze activity logs with Microsoft Graph

Article • 11/11/2024

The Microsoft Entra [reporting APIs](#) provide you with programmatic access to the data through a set of REST APIs. You can call these APIs from many programming languages and tools.

This article describes how to analyze Microsoft Entra activity logs with Microsoft Graph Explorer and Microsoft Graph PowerShell.

Prerequisites

- A working Microsoft Entra tenant with a Microsoft Entra ID P1 or P2 license associated with it.
- To consent to the required permissions, you need the [Privileged Role Administrator](#).

Access reports using Microsoft Graph Explorer

With all the prerequisites configured, you can run activity log queries in Microsoft Graph. The Microsoft Graph API isn't designed for pulling large amounts of activity data. Pulling large amounts of activity data using the API might lead to issues with pagination and performance. For more information on Microsoft Graph queries for activity logs, see [Activity reports API overview](#).

1. Start [Microsoft Graph Explorer tool](#).

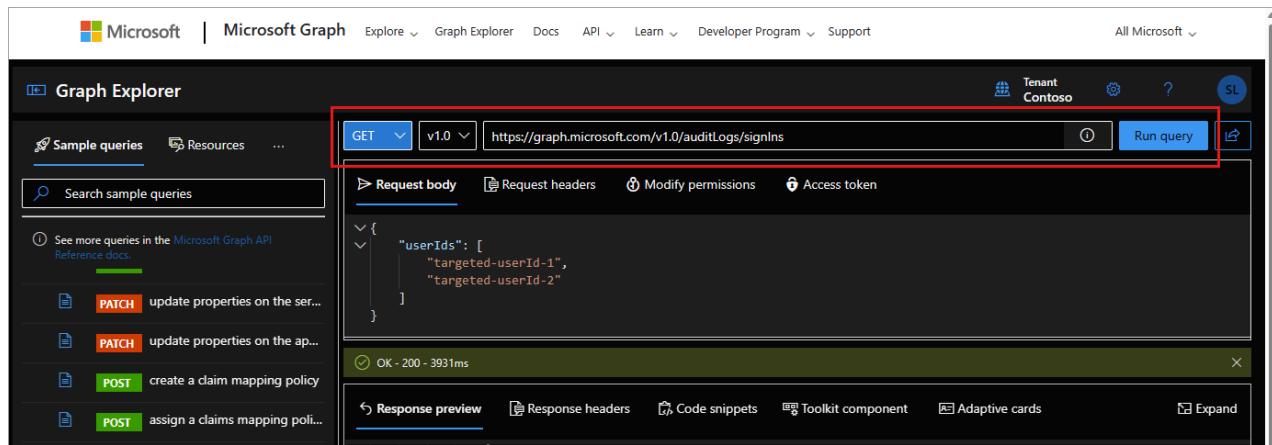
2. Select your profile and then select **Modify permissions**.

3. Consent to the following required permissions:

- `AuditLog.Read.All`
- `Directory.Read.All`

4. Use one of the following queries to start using Microsoft Graph for accessing activity logs:

- GET `https://graph.microsoft.com/v1.0/auditLogs/directoryAudits`
- GET `https://graph.microsoft.com/v1.0/auditLogs/signIns`
- GET `https://graph.microsoft.com/v1.0/auditLogs/provisioning`



Fine-tune your queries

To search for specific activity log entries, use the `$filter` and `createdDateTime` query parameters with one of the available properties. Some of the following queries use the `beta` endpoint. The `beta` endpoint is subject to change and isn't recommended for production use.

- [Sign-in log properties](#)
- [Audit log properties](#)

Try using the following queries:

- For sign-in attempts where Conditional Access failed:
 - GET `https://graph.microsoft.com/v1.0/auditLogs/signIns?$filter=conditionalAccessStatus eq 'failure'`
 - Consider using a date filter so the request doesn't time out.
- To find sign-ins to a specific application during a specific time frame:
 - GET `https://graph.microsoft.com/v1.0/auditLogs/signIns?$filter=(createdDateTime ge 2024-01-13T14:13:32Z and createdDateTime le 2024-01-14T17:43:26Z) and appId eq 'APP ID'`
- For non-interactive sign-ins:
 - GET `https://graph.microsoft.com/beta/auditLogs/signIns?$filter=(createdDateTime ge 2024-01-13T14:13:32Z and createdDateTime le 2024-01-14T17:43:26Z) and signInEventTypes/any(t: t eq 'nonInteractiveUser')`
- For service principal sign-ins:
 - GET `https://graph.microsoft.com/beta/auditLogs/signIns?$filter=(createdDateTime ge 2024-01-13T14:13:32Z and createdDateTime le 2024-01-14T17:43:26Z) and signInEventTypes/any(t: t eq 'servicePrincipal')`
- For managed identity sign-ins:

- GET `https://graph.microsoft.com/beta/auditLogs/signIns?$filter=(createdDateTime ge 2024-01-13T14:13:32Z and createdDateTime le 2024-01-14T17:43:26Z) and signInEventTypes/any(t: t eq 'managedIdentity')`
- To get the authentication method of a user:
 - GET `https://graph.microsoft.com/beta/users/{userObjectId}/authentication/methods`
 - Requires `UserAuthenticationMethod.Read.All` permission
- To see the user registration details report:
 - GET
`https://graph.microsoft.com/beta/reports/authenticationMethods/userRegistrationDetails`
 - Requires `UserAuthenticationMethod.Read.All` permission
- For the registration details of specific user:
 - GET
`https://graph.microsoft.com/beta/reports/authenticationMethods/userRegistrationDetails/{userId}`
 - Requires `UserAuthenticationMethod.Read.All` permission

Related APIs

Once you're familiar with the standard sign-in and audit logs, try exploring these other APIs:

- [Identity Protection APIs](#)
- [Provisioning logs API](#)

Access reports using Microsoft Graph PowerShell

You can use PowerShell to access the Microsoft Entra reporting API. For more information, see [Microsoft Graph PowerShell overview](#).

Microsoft Graph PowerShell cmdlets:

- **Audit logs:** `Get-MgAuditLogDirectoryAudit`
- **Sign-in logs:** `Get-MgAuditLogSignIn`
- **Provisioning logs:** `Get-MgAuditLogProvisioning`
- Explore the full list of [reporting-related Microsoft Graph PowerShell cmdlets](#).

Common errors

Error: Neither tenant is B2C or tenant doesn't have premium license: Accessing sign-in reports requires a Microsoft Entra ID P1 or P2 license. If you see this error message while accessing sign-ins, make sure that your tenant is licensed with a Microsoft Entra ID P1 license.

Error: User isn't in the allowed roles: If you see this error message while trying to access audit logs or sign-ins using the API, make sure that your account is part of the **Security Reader** or **Reports Reader** role in your Microsoft Entra tenant.

Error: Application missing Microsoft Entra ID 'Read directory data' or 'Read all audit log data' permission: The application must have either the `AuditLog.Read.All` or `Directory.Read.All` permission to access the activity logs with Microsoft Graph.

Related content

- [Get started with Microsoft Entra ID Protection and Microsoft Graph](#)
- [Audit API reference](#)
- [API signIn reference](#)

How to archive Microsoft Entra activity logs to an Azure storage account

Article • 03/10/2025

If you need to store Microsoft Entra activity logs for longer than the [default retention period](#), you can archive your logs to a storage account. We recommend that you use a general storage account and not a Blob storage account. For storage pricing information, see the [Azure Storage pricing calculator](#).

Prerequisites

To use this feature, you need:

- An Azure subscription. If you don't have an Azure subscription, you can [sign up for a free trial](#).
- An Azure storage account you have `ListKeys` permissions for. Learn how to [create a storage account](#).
- A user who's a [Security Administrator](#) for the Microsoft Entra tenant.

Archive logs to an Azure storage account

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Security Administrator](#).
2. Browse to **Entra ID > Monitoring & health > Diagnostic settings**. You can also select **Export Settings** from either the **Audit Logs** or **Sign-ins** page.
3. Select **+ Add diagnostic setting** to create a new integration or select **Edit setting** for an existing integration.
4. Enter a **Diagnostic setting name**. If you're editing an existing integration, you can't change the name.
5. Select the log categories that you want to stream.
6. Under **Destination Details** select the **Archive to a storage account** check box.
7. Select the appropriate **Subscription** and **Storage account** from the menus.

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name * Storage Account

Logs

Categories

- AuditLogs
- SignInLogs
- NonInteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSignInLogs
- RiskyUsers
- UserRiskEvents
- NetworkAccessTrafficLogs

Destination details

Send to Log Analytics workspace

Archive to a storage account

You'll be charged normal data rates for storage and transactions when you send diagnostics to a storage account.

Showing all storage accounts including classic storage accounts

Location All

Subscription Azure subscription 1

Storage account *

Stream to an event hub

Send to partner solution

(!) Note

The Diagnostic settings storage retention feature has been deprecated. If you're editing a diagnostic setting created when the retention option was available, those fields are still visible. For details on this change, see [Migrate from diagnostic settings storage retention to Azure Storage lifecycle management](#).

8. Select **Save** to save the setting.
9. Close the window to return to the diagnostic settings page.

Related content

- [Manually download activity logs](#)
- [Integrate activity logs with Azure Monitor logs](#)
- [Stream logs to an event hub](#)

How to customize and filter identity activity logs

Article • 11/11/2024

Sign-in logs are a commonly used tool to troubleshoot user access issues and investigate risky sign-in activity. Audit logs collect every logged event in Microsoft Entra ID and can be used to investigate changes to your environment. There are over 30 columns you can choose from to customize your view of the sign-in logs in the Microsoft Entra admin center. Audit logs and Provisioning logs can also be customized and filtered for your needs.

This article shows you how to customize the columns and then filter the logs to find the information you need more efficiently.

Prerequisites

- A working Microsoft Entra tenant with the appropriate Microsoft Entra license associated with it.
 - For a full list of license requirements, see [Microsoft Entra monitoring and health licensing](#).
- [Reports Reader](#) is the least privileged role required to access the activity logs.
 - For a full list of roles, see [Least privileged role by task](#).

How to access the activity logs in the Microsoft Entra admin center

You can always access your own sign-in history at <https://mysignins.microsoft.com>. You can also access the sign-in logs from **Users** and **Enterprise applications** in Microsoft Entra ID.

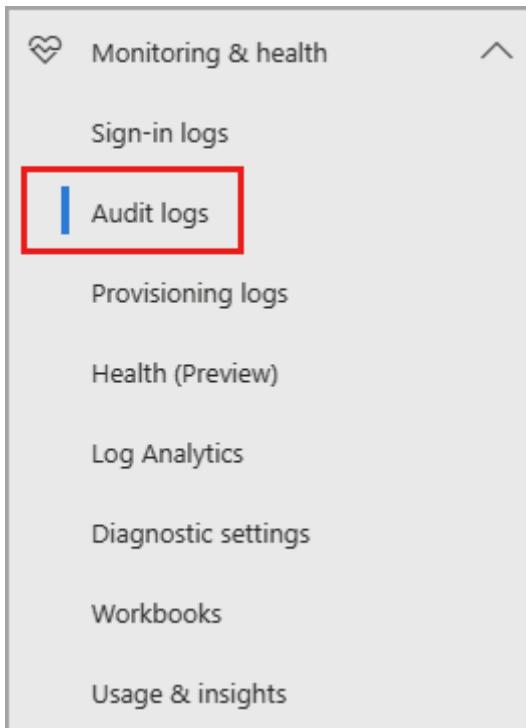
Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Audit logs/Sign-in logs/Provisioning logs**.

Audit logs

With the information in the Microsoft Entra audit logs, you can access all records of system activities for compliance purposes. Audit logs can be accessed from the **Monitoring and health** section of Microsoft Entra ID, where you can sort and filter on every category and activity. You can also access audit logs in the area of the admin center for the service you're investigating.



For example, if you're looking into changes to Microsoft Entra groups, you can access the Audit logs from **Microsoft Entra ID > Groups**. When you access the audit logs from the service, the filter is automatically adjusted according to the service.

The screenshot shows the 'Groups | All groups' page in the Microsoft Entra admin center. On the left, there's a sidebar with links like 'All groups', 'Deleted groups', and 'Diagnose and solve problems'. Below that are sections for 'Settings' (General, Expiration, Naming policy), 'Activity' (Privileged Identity Management, Access reviews, Audit logs, Bulk operation results), and 'Troubleshooting + Support' (New support request). The 'Audit logs' link under 'Activity' is highlighted with a red box.

Customize the layout of the audit logs

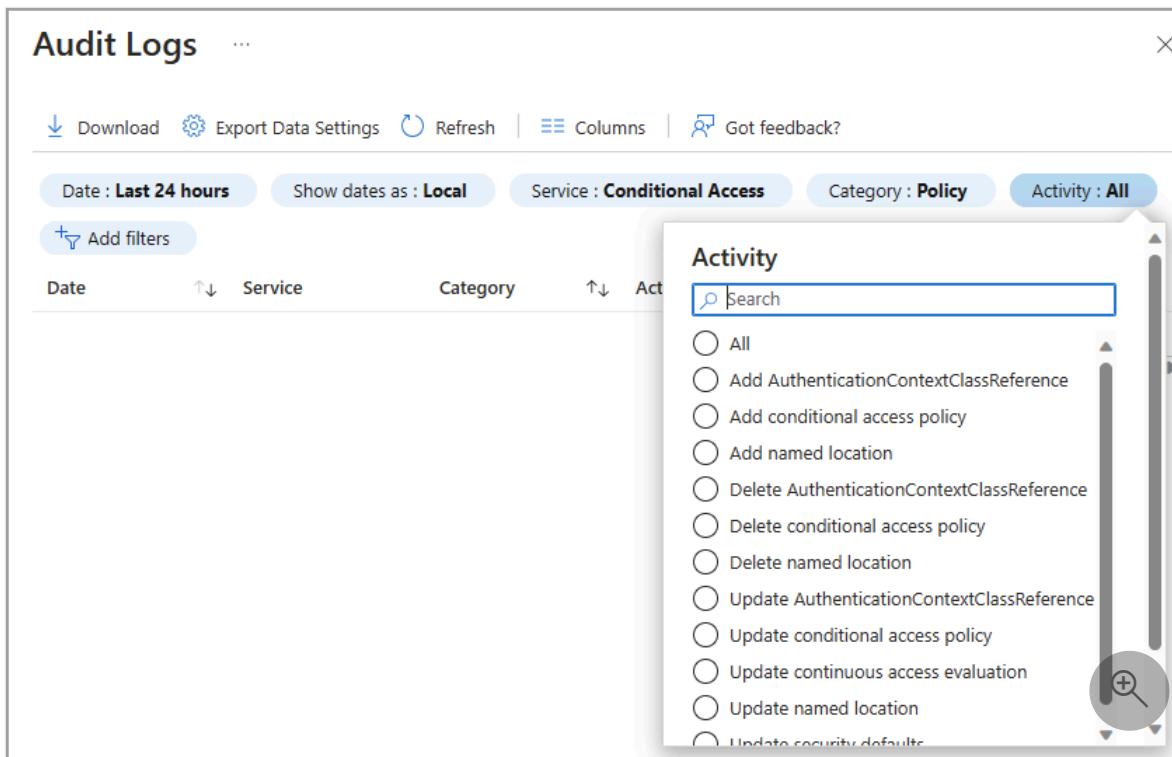
You can customize the columns in the audit logs to view only the information you need. The **Service**, **Category**, and **Activity** columns are related to each other, so these columns should always be visible.

The screenshot shows the 'Audit Logs' page in the Microsoft Entra admin center. The top navigation bar includes 'Home', 'Audit Logs', and a search bar. Below the navigation is a toolbar with 'Download', 'Export Data Settings', 'Refresh', 'Columns' (which is highlighted with a red box), and 'Got feedback?'. A filter bar allows setting the date range ('Last 24 hours'), service ('All'), category ('All'), activity ('All'), and adding filters. The main area displays a table of audit log entries with columns for Date, Service, Category, Activity, Status, Status reason, and Target(s). The first entry is for 'Core Directory' with 'UserManagement' category and 'Update user' activity.

Date	Service	Category	Activity	Status	Status reason	Target(s)
9/11/2023, 11:24:32 ...	Core Directory	UserManagement	Update user	Success		Weitao.Wang@w...
9/11/2023, 11:21:47 ...	Account Provisioning	ProvisioningManage...	Synchronization rule ...	Success	The Group 'Password V...	GitHub - Project'
9/11/2023, 11:21:47 ...	Account Provisioning	ProvisioningManage...	Synchronization rule ...	Success	The Group 'Compliance...	GitHub - Project'

Filter the audit logs

When you filter the logs by **Service**, the **Category**, and **Activity** details automatically change. In some cases, there might only be one Category or Activity. For a detailed table of all potential combinations of these details, see [Audit activities](#).



The screenshot shows the Microsoft Azure portal's Audit Logs page. At the top, there are filters for Date (Last 24 hours), Show dates as (Local), Service (Conditional Access), Category (Policy), and Activity (All). Below the filters is a table with columns: Date, Service, Category, and Activity. To the right of the table is a modal window titled "Activity" containing a search bar and a list of audit activity types. The list includes: All, Add AuthenticationContextClassReference, Add conditional access policy, Add named location, Delete AuthenticationContextClassReference, Delete conditional access policy, Delete named location, Update AuthenticationContextClassReference, Update conditional access policy, Update continuous access evaluation, Update named location, and Update security defaults. A magnifying glass icon is at the bottom right of the modal.

- **Service:** Defaults to all available services, but you can filter the list to one or more by selecting an option from the dropdown list.
- **Category:** Defaults to all categories, but can be filtered to view the category of activity, such as changing a policy or activating an eligible Microsoft Entra role.
- **Activity:** Based on the category and activity resource type selection you make. You can select a specific activity you want to see or choose all.

You can get the list of all Audit Activities using the Microsoft Graph API:

```
https://graph.windows.net/<tenantdomain>/activities/auditActivityTypesV2?  
api-version=beta
```

- **Status:** Allows you to look at result based on if the activity was a success or failure.
- **Target:** Allows you to search for the target or recipient of an activity. Search by the first few letters of a name or user principal name (UPN). The target name and UPN are case-sensitive.
- **Initiated by:** Allows you to search by who initiated the activity using the first few letters of their name or UPN. The name and UPN are case-sensitive.

- **Date range:** Enables to you to define a timeframe for the returned data. You can search the last 7 days, 24 hours, or a custom range. When you select a custom timeframe, you can configure a start time and an end time.

Related content

- [Analyze a sign-in error](#)
- [Troubleshoot sign-in errors](#)
- [Explore all audit log categories and activities](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

How to download logs in Microsoft Entra ID

Article • 04/25/2025

The Microsoft Entra admin center gives you access to three types of activity logs:

- **Sign-ins:** Information about sign-ins and how your resources are used by your users.
- **Audit:** Information about changes applied to your tenant such as users and group management or updates applied to your tenant's resources.
- **Provisioning:** Activities performed by a provisioning service, such as the creation of a group in ServiceNow or a user imported from Workday.

Microsoft Entra ID stores activity logs for a specific period, depending on your license. For more information, see [Microsoft Entra data retention](#). By downloading the logs, you can control how long logs are stored. This article explains how to download activity logs in Microsoft Entra ID.

Prerequisites

- A working Microsoft Entra tenant with the appropriate Microsoft Entra license associated with it.
 - For a full list of license requirements, see [Microsoft Entra monitoring and health licensing](#).
- The option to download logs is available in all editions of Microsoft Entra ID.
- Downloading logs programmatically with Microsoft Graph requires a [premium license](#).
- [Reports Reader](#) is the least privileged role required to view Microsoft Entra activity logs.

Log download considerations

Before you download logs, review the following considerations and tips:

- Microsoft Entra ID supports the following formats for your download:
 - CSV
 - JSON
- Timestamps in the downloaded files are based on UTC.
- You can download up to 100,000 sign-in or provisioning records per file.
- You can download up to 250,000 audit records per file.
- Set your filter before you download the logs to narrow the dataset.

Note

The Microsoft Entra admin center download service will time out if you attempt to download large data sets. Generally, data sets smaller than 250,000 for audit logs and 100,000 for sign-in and provisioning logs work well with the browser download feature.

If you face issues completing large downloads in the browser, use the [reporting API](#) to download the data or [send the logs to an endpoint through diagnostic settings](#).

! Note

The columns in the downloaded logs do not change. The output contains all details of the audit or sign-in log, *regardless of the columns you customized in the Microsoft Entra admin center*. If you set a custom filter, however, the output in the downloaded logs contain only the results that match the filter.

How to download activity logs

You can access the activity logs from the **Monitoring and health** section of Microsoft Entra ID or from the area of Microsoft Entra ID where you're working.

For example, if you're in the **Groups** or **Licenses** section of Microsoft Entra ID, you can access the audit logs for those specific activities directly from that area. When you access the audit logs in this way, the filter categories are automatically set. If you're in **Groups**, the audit log filter category is set to **GroupManagement**.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various sections like Devices, Applications, Roles & admins, Billing, and Licenses. The 'Licenses' section is currently selected and highlighted with a red box. Within the main content area, the 'Licenses | Overview' page is displayed. At the bottom of this page, under the 'Activity' section, there's a link labeled 'Audit logs' which is also highlighted with a red box. To the right of the main content, there's a sidebar titled 'Get started with license management' containing some text and a bulleted list of tasks. Further down, there's a 'Quick tasks' section with links to 'Get a free trial', 'See your bills', 'Manage your purchased licenses', and 'Manage your self-service subscriptions'.

Audit logs

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Entra ID > Monitoring & health > Audit logs**.
3. Select **Download**.
4. In the panel that opens, select the **Format**.
5. Optionally provide a unique file name.
6. Select the **Download** button. The download processes and sends the file to your default download location.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like Identity, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, and Monitoring & health. Under Monitoring & health, 'Audit logs' is selected. The main area displays 'Audit Logs' with a table of log entries. At the top right of this area are buttons for 'Download', 'Export Data Settings', and 'Refresh'. Below the table are filters for 'Add filter', 'Show dates as: Local', and 'Date range'. The table has columns for 'Date' and 'Service'. The log entries show various account provisioning activities. To the right of the table, a modal window titled 'Download Audit Logs' is open. It contains a note about downloading up to 250,000 records, a message about the download being based on filter selections, and a section for choosing 'Format' (CSV is selected) and 'File Name' ('AuditLogs_2024-03-20'). A large blue 'Download' button is at the bottom of this modal.

Sign-in logs

The options covered in this section align with the preview experience for sign-in logs.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Entra ID > Monitoring & health > Sign-in logs**.
3. Select the **Download** button and select either **JSON** or **CSV**.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like User experiences, Hybrid management, Monitoring & health, and Sign-in logs (which is currently selected). The main area is titled 'Sign-in events'. At the top right, there are various icons for search, refresh, and help. Below the title, there are download options ('Download JSON' and 'Download CSV') and filter settings ('Date: Last 24 hours', 'Show dates as: Local', 'Add filters'). The table below has columns for Date, Request ID, User, Application, Status, IP address, and Location. The first column, 'User sign-ins (interactive)', is underlined, indicating it's the active filter.

4. Optionally provide a unique file name for each file you need to download.
5. Select the **Download** button for one or more of the logs. The download processes and sends the file to your default download location.
 - Interactive sign-ins
 - Interactive sign-ins with only the [authentication details](#) included
 - Non-interactive sign-ins
 - Non-interactive sign-ins with only the [authentication details](#) included
 - Application sign-ins
 - Managed identity

Download Sign-ins in CSV format

X

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

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

File Name

InteractiveSignins_2024-03-19_2024-03-20

Download

File Name

InteractiveSignins_AuthDetails_2024-03-19_2024-03-20

Download

File Name

NonInteractiveSignins_2024-03-19_2024-03-20

Download

File Name

NonInteractiveSignins_AuthDetails_2024-03-19_2024-03-20

Download

File Name

ApplicationSignins_2024-03-19_2024-03-20

Download

File Name

MSISignins_2024-03-19_2024-03-20

Download

Provisioning logs

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Entra ID > Monitoring & health > Provisioning logs**.
3. Select the **Download** button and select either **JSON** or **CSV**.
4. Optionally provide a unique file name for each file you need to download.
5. Select the **Download** button for one or more of the logs. The download processes and sends the file to your default download location.
 - Provisioning logs
 - Provisioning logs with the provisioning steps
 - Provisioning logs with modified properties

Download provisioning logs in CSV format

i You can download up to 100,000 records. If you want to download more, use reporting APIs. [Click here to learn more.](#)

i Please use the filters to narrow the dataset, reduce the size of the download, and minimize the time it takes to download the logs. Your download will be based on the filter selections you have made.

File Name

ProvisioningLogs_03-19-2024_03-20-2024

Download

File Name

ProvisioningLogs_ProvisioningSteps_03-19-2024_03-20-2024

Download

File Name

ProvisioningLogs_ModifiedProperties_03-19-2024_03-20-2024

Download

How to detect and investigate inactive user accounts

Article • 02/23/2025

In large environments, user accounts aren't always deleted when employees leave an organization. As an IT administrator, you want to detect and resolve these obsolete user accounts because they represent a security risk.

This article explains a method to handle obsolete user accounts in Microsoft Entra ID.

ⓘ Note

This article applies only to finding inactive user accounts in Microsoft Entra ID. It doesn't apply to finding inactive accounts in [Azure AD B2C](#).

Prerequisites

- To access the `lastSuccessfulSignInDateTime` property using Microsoft Graph, you need a Microsoft Entra ID P1 or P2 license.
- You need to grant the app the following Microsoft Graph permissions:
 - AuditLog.Read.All
 - User.Read.All
- [Reports Reader](#) is the least privileged role required to access the activity logs.
 - For a full list of roles, see [Least privileged role by task](#).

What are inactive user accounts?

Inactive accounts are user accounts that aren't required anymore by members of your organization to gain access to your resources. One key identifier for inactive accounts is that they haven't been used *for a while* to sign in to your environment. Because inactive accounts are tied to the sign-in activity, you can use the timestamp of the last time an account attempted to sign in to detect inactive accounts.

The challenge of this method is to define what *for a while* means for your environment. For example, users might not sign in to an environment *for a while*, because they are on vacation. You need to consider all legitimate reasons for not signing in to your environment. In many organizations, a reasonable window for inactive user accounts is between 90 and 180 days.

The last sign-in date provides potential insights into a user's continued need for access to resources. It can help with determining if group membership or app access is still needed or could be removed. For external user management, you can determine if an external user is still active within the tenant or should be removed.

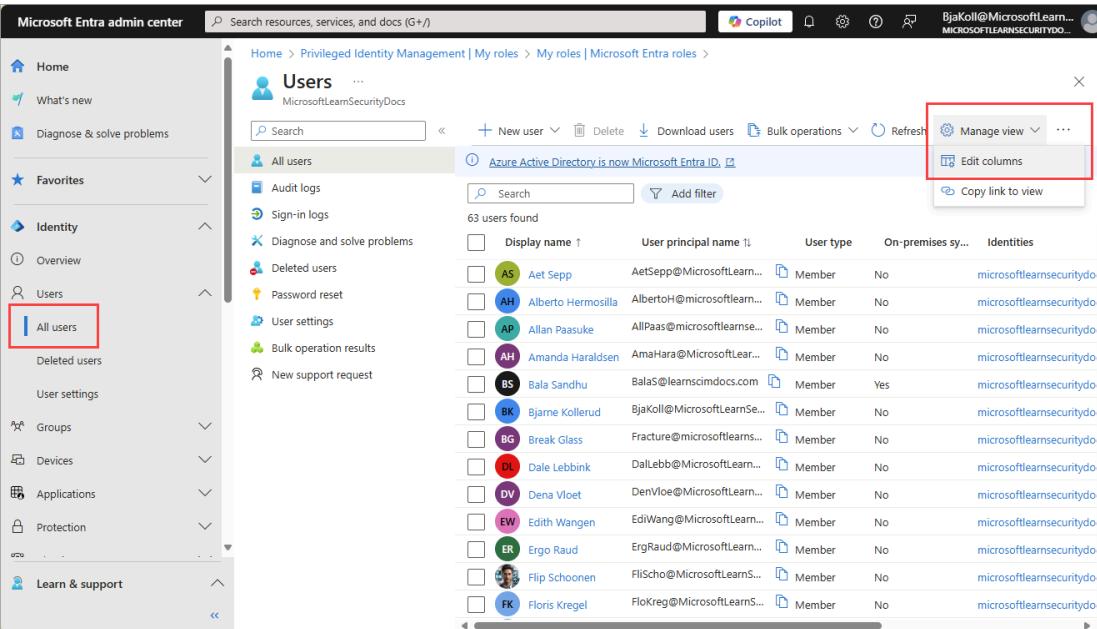
How to find and investigate inactive user accounts

You can use the Microsoft Entra admin center or the Microsoft Graph API to find inactive user accounts. While there isn't a built-in report for inactive user accounts, you can use the last sign-in date and time to determine if a user account is inactive.

To find the last sign-in time for a user, you can look at your user list in the Microsoft Entra admin center. While all users can see the list of users, some columns and details are only available to users with the appropriate permissions.

Find the last sign-in time for all users

1. Sign in to the [Microsoft Entra admin center](#) ↗ as at least a **Reports Reader**.
2. Browse to **Identity > Users > All users**.
3. Select **Manage view** and then **Edit columns**.



Display name	User principal name	User type	On-premises sync	Identities
AS	Aet Sepp	AetSepp@MicrosoftLearn...	Member	No
AH	Alberto Hermosilla	AlbertoH@microsoftlearn...	Member	No
AP	Allan Paasuke	AllPaas@microsoftlear...	Member	No
AH	Amanda Haraldsen	AmaHara@microsoftlear...	Member	No
BS	Bala Sandhu	BalaS@learnsimdocs.com	Member	Yes
BK	Bjarne Kollerud	BjaKoll@MicrosoftLearn...	Member	No
BG	Break Glass	Fracture@microsoftlear...	Member	No
DL	Dale Lebbink	DalLebb@microsoftlear...	Member	No
DV	Dena Vloe	DenVloe@microsoftlear...	Member	No
EW	Edith Wangen	EdiWang@microsoftlear...	Member	No
ER	Ergo Raud	ErgRaud@microsoftlear...	Member	No
FS	Flip Schoonen	FliScho@microsoftlear...	Member	No
FK	Floris Kregel	FloKreg@microsoftlear...	Member	No

4. From the list, select **+ Add column**, select **Last interactive sign-in time** from the list, then select **Save**.

Edit columns

X

↑ Move up ↓ Move down

Column Name

Display name



User principal name



User type



On-premises sync enabled



Identities



Company name



Creation type



Last interactive sign-in time



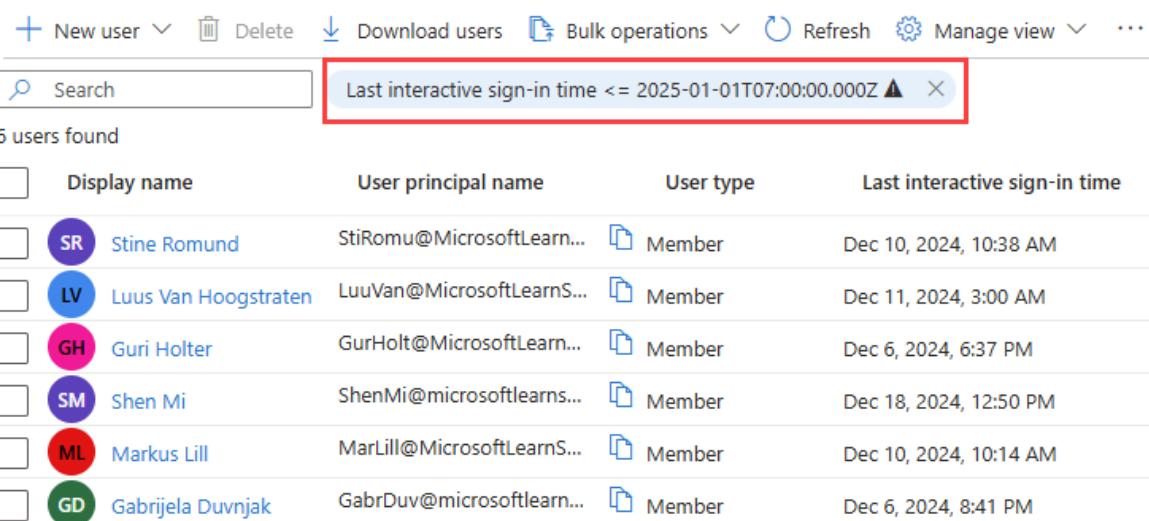
+ Add column

Save

Cancel

- With the column now visible in the all users list, select **Add filter** and set a time frame for your search using the filter options.

- Select \leq as the **Operator**, then select the date to find the last sign-in *before* that selected date.

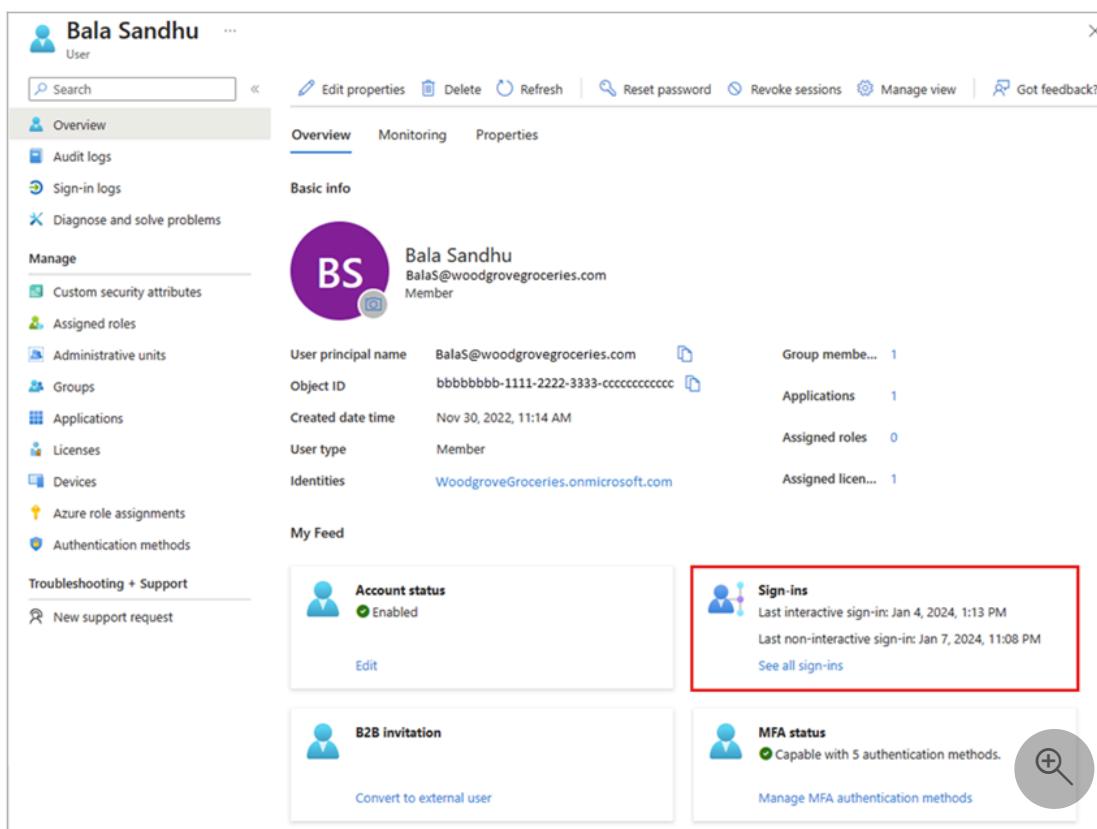


+ New user Delete Download users Bulk operations Refresh Manage view ...				
<input type="text"/> Search Last interactive sign-in time <= 2025-01-01T07:00:00.000Z ▲ X				
6 users found				
	Display name	User principal name	User type	Last interactive sign-in time
<input type="checkbox"/>	 Stine Romund	StiRomu@MicrosoftLearn...	Member	Dec 10, 2024, 10:38 AM
<input type="checkbox"/>	 Luus Van Hoogstraten	LuuVan@MicrosoftLearn...	Member	Dec 11, 2024, 3:00 AM
<input type="checkbox"/>	 Guri Holter	GurHolt@MicrosoftLearn...	Member	Dec 6, 2024, 6:37 PM
<input type="checkbox"/>	 Shen Mi	ShenMi@microsoftlearns...	Member	Dec 18, 2024, 12:50 PM
<input type="checkbox"/>	 Markus Lill	MarLill@MicrosoftLearnS...	Member	Dec 10, 2024, 10:14 AM
<input type="checkbox"/>	 Gabrijela Duvnjak	GabrDuv@microsoftlearn...	Member	Dec 6, 2024, 8:41 PM

Investigate a single user

If you need to view the latest sign-in activity for a user, you can view the user's sign-in details in Microsoft Entra ID. You can also use the Microsoft Graph API described in the [Users by name](#) section.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Identity > Users > All users**.
3. Select a user from the list.
4. In the **My Feed** area of the user's Overview, locate the **Sign-ins** tile.



The screenshot shows the Microsoft Entra admin center User Overview page for Bala Sandhu. The left sidebar contains navigation links like Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Manage, Troubleshooting + Support, and New support request. The main content area has tabs for Overview, Monitoring, and Properties. Under Basic info, it shows Bala Sandhu's profile picture (BS), name, email (BalaS@woodgrovegroceries.com), and member status. Below this, there are details for User principal name, Object ID, Created date time, User type, and Identities. The 'My Feed' section contains tiles for Account status (Enabled), Sign-ins, B2B invitation, and MFA status. The 'Sign-ins' tile is highlighted with a red box and displays the last interactive sign-in (Jan 4, 2024, 1:13 PM) and last non-interactive sign-in (Jan 7, 2024, 11:08 PM), with a 'See all sign-ins' link.

The last sign-in date and time shown on this tile might take up to 24 hours to update, which means the date and time might not be current. If you need to see the activity in near real time, select the **See all sign-ins** link on the **Sign-ins** tile to view all sign-in activity for that user.

How to address inactive users

After identifying inactive users, start by asking the following questions:

- Is the user still employed by the organization?
- Does the user still need access to the resources they have access to?
- Is the user account still needed for any other reason?

How you address inactive users depends on your scenario, but cleaning up unused accounts or over-privileged accounts should be your priority to reduce security risks. The following features and options are a great place to start, but note that some of these features might require additional licensing.

- [Clean up stale guest accounts](#)
- Consider dynamic membership group to automatically add or remove users from groups based on their user properties.
 - [Create a dynamic membership group](#)
- Use Microsoft Entra ID Governance access reviews to audit your users' access.
 - [What are access reviews?](#)
 - [Review recommendations for access reviews](#)

Related content

- [Audit API reference](#)
- [Sign-in activity report API reference](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Configure Microsoft Entra diagnostic settings for activity logs

Article • 02/26/2025

Using **diagnostic settings** in Microsoft Entra ID, you can integrate logs with Azure Monitor, stream logs to an event hub, or archive logs to a storage account. You can create multiple diagnostic settings to send activity logs to different destinations.

This article provides the steps to configure Microsoft Entra diagnostic settings for activity logs.

Prerequisites

To configure diagnostic settings, you need:

- An Azure subscription. If you don't have an Azure subscription, you can [sign up for a free trial](#).
- [Security Administrator](#) access to create general diagnostic settings for the Microsoft Entra tenant.
- [Attribute Log Administrator](#) access to create diagnostic settings for [custom security attribute](#) logs.
- A destination that is already set up. For example, if you want to stream logs to an event hub, you need to create the event hub before you can configure the diagnostic settings.

How to access diagnostic settings

This article provides the steps to access diagnostic settings for the Microsoft Entra logs. If you need to configure diagnostic settings for Azure Monitor or Azure resources outside of Microsoft Entra ID, see [Diagnostic settings in Azure Monitor](#).

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Security Administrator](#).
2. Browse to **Identity > Monitoring & health > Diagnostic settings**. The **General** settings appear by default.
3. Any existing diagnostic settings appear in the table. Select **edit settings** to change an existing setting, or select **Add diagnostic setting** to create a new setting.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like External Identities, User experiences, Hybrid management, Monitoring & health, Sign-in logs, Audit logs, Provisioning logs, Health (Preview), Log Analytics, and Diagnostic settings. The 'Diagnostic settings' link is highlighted with a red box. The main content area is titled 'Diagnostic settings | General'. It includes a 'Refresh' and 'Feedback' button, a brief description about diagnostic settings, and a table for managing diagnostic settings. The table has columns for Name, Storage account, Event hub, Log Analytics workspace, Partner solution, and Edit setting. A row shows 'No diagnostic settings defined' with a red box around the '+ Add diagnostic setting' button. Below this, instructions say 'Click 'Add Diagnostic setting' above to configure the collection of the following data:' followed by a list of log types.

Custom security attributes

The custom security attributes logs are a subset of the standard audit logs. You must have the **Attribute Log Administrator** role active to configure diagnostic settings for the custom security attributes. For more information, see [Custom security attributes overview](#).

To configure diagnostic settings for the custom security attribute audit logs, select **Custom security attributes**. The process to configure diagnostic settings is the same for both categories of logs.

This screenshot shows the 'Diagnostic settings | Custom security attributes' page. The left sidebar has a 'Diagnostic settings' section with 'General' and 'Custom security attributes' options, where 'Custom security attributes' is highlighted with a red box. The main content area is identical to the general logs page, featuring a 'Refresh' and 'Feedback' button, a description of diagnostic settings, a table for managing diagnostic settings (showing 'No diagnostic settings defined'), and a list of log types under the '+ Add diagnostic setting' button.

Tip

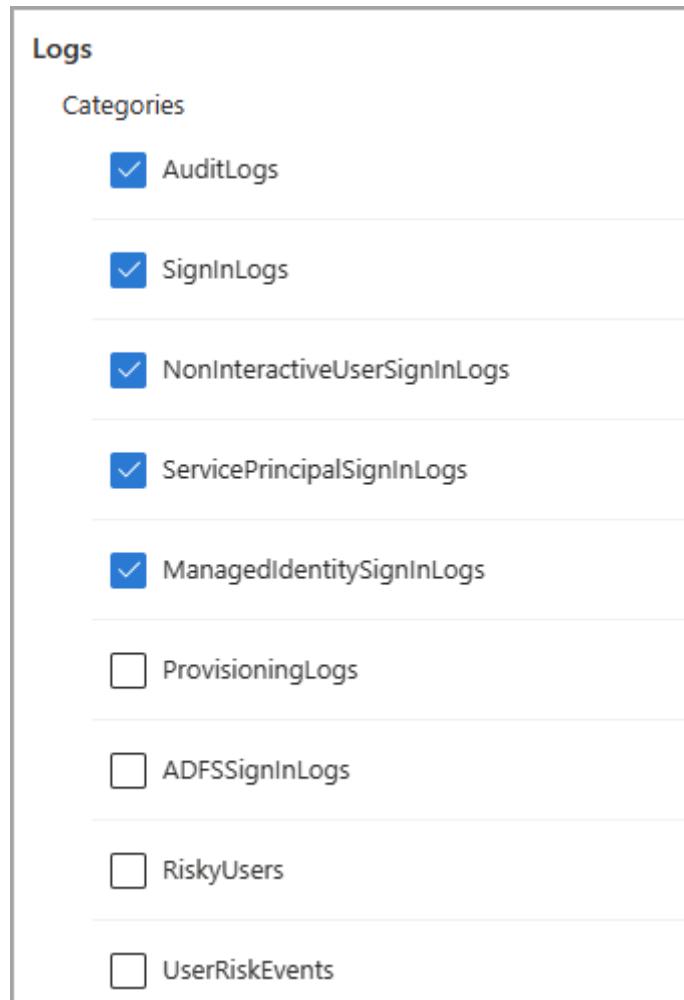
Microsoft recommends that you keep your custom security attribute audit logs separate from your directory audit logs so that attribute assignments are not revealed inadvertently.

Select the logs and destination

When you create or edit a diagnostic setting, you can choose which logs to include and where to send them.

Log categories

You can select one, some, or all of the available logs. Some logs might be part of a preview feature. Even if you select a log category, you might not see any data until the feature is generally available. For a description of the available logs, see [Log options for streaming to endpoints](#).



Destination details

You can send logs to a Log Analytics workspace, stream logs to an event hub, or archive logs to a storage account. Through Azure Native ISV services, you can send logs to services through the Azure Marketplace. For more information, see [Azure Native ISV services overview](#).

You must have a destination set up prior to configuring diagnostic settings.

- [Configure a Log Analytics workspace](#)
- [Create an event hub](#)
- [Create a storage account](#)

When you select a destination, more fields appear. Select the appropriate subscription and destination from the fields that appear.

Destination details

[Send to Log Analytics workspace](#)

Subscription [Visual Studio Enterprise](#) ▾

Log Analytics workspace [IdentityITPro \(eastus \)](#) ▾

[Archive to a storage account](#)

[Stream to an event hub](#)

[Send to partner solution](#)

For details on configuring diagnostic settings for a specific destination, see the following articles:

- [Integrate logs with Azure monitor logs](#)
- [Stream logs to an event hub](#)
- [Archive logs to an Azure storage account](#)

Basic process

The basic steps for configuring diagnostics settings are as follows:

1. To create a new diagnostic setting, select **Add diagnostic setting**.
2. Provide a name.
3. Select the logs you want to include.
4. Select the destination and subscription from the dropdown menus that appear.
5. Select the **Save** button.

Diagnostic setting

X

 Save

 Discard

 Delete

 Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

[JSON View](#)

Diagnostic setting name *

BasicLogs 

Logs

Categories

AuditLogs

SignInLogs

NonInteractiveUserSignInLogs

ServicePrincipalSignInLogs

ManagedIdentitySignInLogs

ProvisioningLogs

ADFSSignInLogs

RiskyUsers

UserRiskEvents

Destination details

Send to Log Analytics workspace

Subscription

Visual Studio Enterprise 

Log Analytics workspace

IdentityITPro (eastus) 

Archive to a storage account

Stream to an event hub

Send to partner solution

Note

It might take up to three days for the logs to start appearing in the destination.

How to stream activity logs to an event hub

Article • 01/29/2025

Your Microsoft Entra tenant produces large amounts of data every second. Sign-in activity and logs of changes made in your tenant add up to so much data that it can be hard to analyze. Integrating with Security Information and Event Management (SIEM) tools can help you gain insights into your environment.

This article shows how you can stream your logs to an event hub, to integrate with one of several SIEM tools.

Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can [sign up for a free trial ↗](#).
- An **Azure event hub** that is already set up. Learn how to [create an event hub](#).
- [Security Administrator](#) access to create general diagnostic settings for the Microsoft Entra tenant.
- [Attribute Log Administrator](#) access to create diagnostic settings for [custom security attribute logs](#).

Stream logs to an event hub

1. Sign in to the [Microsoft Entra admin center](#) ↗ as at least a [Security Administrator](#).
2. Browse to **Identity > Monitoring & health > Diagnostic settings**. You can also select **Export Settings** from either the **Audit Logs** or **Sign-ins** page.
3. Select **+ Add diagnostic setting** to create a new integration or select **Edit setting** for an existing integration.
4. Enter a **Diagnostic setting name**. If you're editing an existing integration, you can't change the name.
5. Select the log categories that you want to stream.
6. Select the **Stream to an event hub** check box.
7. Select the Azure subscription, Event Hubs namespace, and optional event hub where you want to route the logs.

The subscription and Event Hubs namespace must both be associated with the Microsoft Entra tenant from where you're streaming the logs.

Once you have the Azure event hub ready, navigate to the SIEM tool you want to integrate with the activity logs. The process is finished in the SIEM tool.

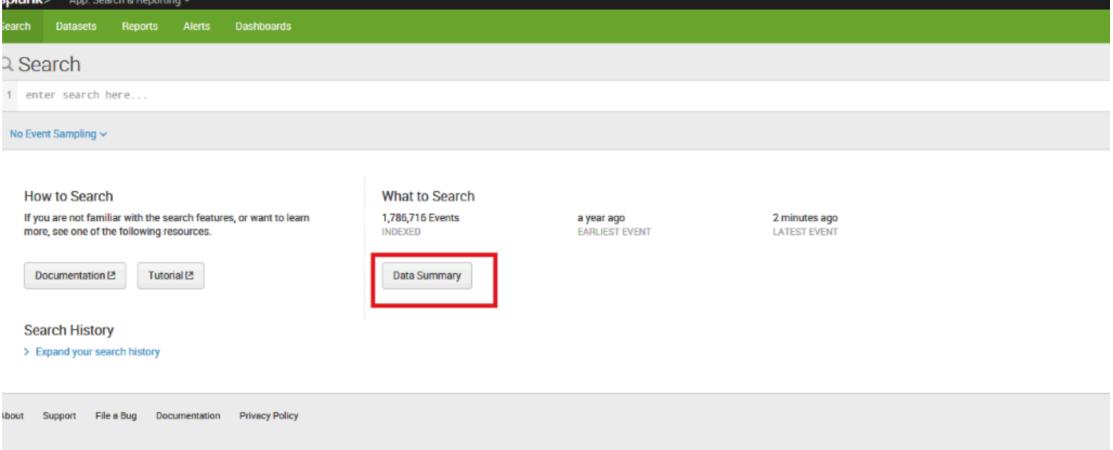
We currently support Splunk, SumoLogic, and ArcSight. Select a tab to get started. Refer to the tool's documentation.

Splunk

To use this feature, you need the [Splunk Add-on for Microsoft Cloud Services](#).

Integrate Microsoft Entra logs with Splunk

1. Open your Splunk instance and select **Data Summary**.



The screenshot shows the Splunk search interface. At the top, there is a navigation bar with links for 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. Below the navigation bar is a search bar with placeholder text 'enter search here...'. Underneath the search bar, a message says 'No Event Sampling'. On the left side, there is a 'How to Search' section with links to 'Documentation' and 'Tutorial'. On the right side, there is a 'What to Search' section showing statistics: '1,786,716 Events INDEXED', 'a year ago EARLIEST EVENT', and '2 minutes ago LATEST EVENT'. A red box highlights the 'Data Summary' button in the 'What to Search' section. At the bottom of the interface, there is a footer with links for 'About', 'Support', 'File a Bug', 'Documentation', and 'Privacy Policy'.

2. Select the **Sourcetypes** tab, and then select **mscs:azure:eventhub**

Data Summary				
Hosts (10)	Sources (23,993)	Sourcetypes (67)		
			filter	Q
			< Prev	1 2 Next >
Sourcetype		Count	Last Update	
o365:management:activity	109,297	8/3/21 10:07:28.000 PM		
mysourcetype	6	4/24/20 5:37:08.000 PM		
mscs:resource:virtualMachine	3,160	6/3/21 1:41:14.000 PM		
mscs:azure:eventhub	197	7/13/21 11:24:18.000 AM		
mscs:azure:audit	2,922	7/15/21 10:53:15.000 AM		
ms:defender:atp:alerts	13,800	7/26/21 5:52:40.000 AM		
m365:webhook	1	2/18/21 9:19:49.000 AM		
m365:teams:callRecord	1	8/20/20 11:12:33.000 AM		
m365:log:warn	4	10/14/20 4:04:16.000 PM		
m365:log:info	66	10/14/20 4:04:45.000 PM		

Append `body.records.category=AuditLogs` to the search. The Microsoft Entra activity logs are shown in the following figure:

New Search

sourcetype="mscs:azure:eventhub" body.records.category=AuditLogs

✓ 1 event (8/2/21 10:00:00.000 PM to 8/3/21 10:21:45.000 PM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 50 Per Page ▾

Time	Event
8/3/21 10:13:29.838 PM	<pre> > 8/3/21 { [[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[.. </pre>

SELECTED FIELDS
`a host 1`
`a source 1`
`a sourcetype 1`

INTERESTING FIELDS
`a body.records.callerIpAddress 1`
`a body.records.category 1`
`a body.records.correlationId 1`
`# body.records.durationMs 1`
`# body.records.Level 1`
`a body.records.operationName 1`
`# body.records.operationVersion 1`
`a body.records.properties.activityDateT`
`ime 1`
`a body.records.properties.activityDispl`
`ayName 1`
`a body.records.properties.additionalDe`
`tails[]key 1`
`a body.records.properties.additionalDe`
`tails[]value 1`
`a body.records.properties.category 1`

If you can't install an add-on in your Splunk instance (for example, if you're using a proxy or running on Splunk Cloud), you can forward these events to the Splunk HTTP Event Collector. To do so, use this [Azure function](#), which is triggered by new messages in the event hub.

Activity log integration options and considerations

If your current SIEM isn't supported in Azure Monitor diagnostics yet, you can set up **custom tooling** by using the Event Hubs API. To learn more, see the [Getting started receiving messages from an event hub](#).

IBM QRadar is another option for integrating with Microsoft Entra activity logs. The DSM and Azure Event Hubs Protocol are available for download at [IBM support](#). For more information about integration with Azure, go to the [IBM QRadar Security Intelligence Platform 7.3.0](#) site.

Some sign-in categories contain large amounts of log data, depending on your tenant's configuration. In general, the non-interactive user sign-ins and service principal sign-ins can be 5 to 10 times larger than the interactive user sign-ins.

Next steps

- [Analyze Microsoft Entra activity logs with Azure Monitor logs](#)
- [Use Microsoft Graph to access Microsoft Entra activity logs](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Tutorial: Create a Log Analytics workspace to analyze sign-in logs

Article • 04/14/2025

In this tutorial, you learn how to:

- ✓ Create a Log Analytics workspace
- ✓ Configure diagnostic settings to integrate sign-in logs with the Log Analytics workspace
- ✓ Run queries using the Kusto Query Language (KQL)

Prerequisites

To analyze activity logs with Log Analytics, you need the following roles and requirements:

- [Microsoft Entra monitoring and health licensing](#)
- [Access to create a Log Analytics workspace](#)
- The appropriate role for Azure Monitor:
 - Monitoring Reader
 - Log Analytics Reader
 - Monitoring Contributor
 - Log Analytics Contributor
- The appropriate role for Microsoft Entra ID:
 - Reports Reader
 - Security Reader
 - Global Reader
 - Security Administrator

Create a Log Analytics workspace

In this step, you create a Log Analytics workspace, which is where you eventually send your sign-in logs. Before you can create the workspace, you need an [Azure resource group](#).

1. Sign in to the [Azure portal](#) as at least a **Security Administrator** with **Log Analytics Contributor** permissions.
2. Browse to [Log Analytics workspaces](#).
3. Select **Create**.

The screenshot shows the Microsoft Azure Log Analytics workspaces page. At the top, there's a search bar and a Copilot button. Below the header, the page title is "Log Analytics workspaces". A red box highlights the "Create" button in the top navigation bar. Other buttons include "Open recycle bin", "Manage view", "Refresh", "Export to CSV", "Open query", and "Assign tags". Below the navigation are filter options: "Filter for any field...", "Subscription equals all", "Resource group equals all", "Add filter", and "More (1)".

4. On the **Create Log Analytics workspace** page, perform the following steps:

- Select your subscription.
- Select a resource group.
- Give your workspace a name.
- Select your region.

The screenshot shows the "Create Log Analytics workspace" page. The "Basics" tab is selected. A callout box provides information about what a Log Analytics workspace is and directs users to learn more. The "Project details" section allows users to select a subscription and resource group. The "Instance details" section lets users enter a workspace name and choose a region. Navigation buttons at the bottom include "Review + Create", "« Previous", and "Next : Tags >".

5. Select **Review + Create**.

6. Select **Create** and wait for the deployment. You might need to refresh the page to see the new workspace.

Configure diagnostic settings

To send your identity log information to your new workspace, you need to configure diagnostic settings. There are different diagnostic settings options for Azure and Microsoft Entra, so for the next set of steps let's switch to the Microsoft Entra admin center to make sure everything is identity related.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.

2. Browse to **Identity > Monitoring & health > Diagnostic settings**.

3. Select **Add diagnostic setting**.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a navigation menu with categories like External Identities, User experiences, Hybrid management, Monitoring & health, Log Analytics, and Protection. Under Monitoring & health, the 'Diagnostic settings' link is highlighted with a red box. The main content area is titled 'Diagnostic settings | General'. It shows a table with a single row: 'No diagnostic settings defined'. Below the table is a button labeled '+ Add diagnostic setting' with a red box around it. To the right of the table, there is a list of data collection options: AuditLogs, SignInLogs, NonInteractiveUserSignInLogs, ServicePrincipalSignInLogs, ManagedIdentitySignInLogs, ProvisioningLogs, ADFSsignInLogs, RiskyUsers, UserRiskEvents, NetworkAccessTrafficLogs, RiskyServicePrincipals, ServicePrincipalRiskEvents, EnrichedOffice365AuditLogs, MicrosoftGraphActivityLogs, and RemoteNetworkHealthLogs. At the top of the main content area, there is a note: 'Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations.' A 'Learn more about diagnostic settings' link is provided.

4. On the **Diagnostic setting** page, perform the following steps:

a. Provide a name for the diagnostic setting.

b. Under **Logs**, select **AuditLogs** and **SignInLogs**.

c. Under **Destination details**, select **Send to Log Analytics**, and then select your new log analytics workspace.

d. Select **Save**.

Diagnostic setting

Save  Discard  Delete  Feedback 

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name * 

Logs	Destination details
<p>Categories</p> <p><input checked="" type="checkbox"/> AuditLogs</p> <p><input checked="" type="checkbox"/> SignInLogs</p> <p><input checked="" type="checkbox"/> NonInteractiveUserSignInLogs</p> <p><input checked="" type="checkbox"/> ServicePrincipalSignInLogs</p> <p><input checked="" type="checkbox"/> ManagedIdentitySignInLogs</p> <p><input type="checkbox"/> ProvisioningLogs</p> <p><input type="checkbox"/> ADFSSignInLogs</p> <p><input type="checkbox"/> RiskyUsers</p> <p><input type="checkbox"/> UserRiskEvents</p>	<p><input checked="" type="checkbox"/> Send to Log Analytics workspace</p> <p>Subscription <input type="text" value="Visual Studio Enterprise"/></p> <p>Log Analytics workspace <input type="text" value="IdentityITPro (eastus)"/></p> <p><input type="checkbox"/> Archive to a storage account</p> <p><input type="checkbox"/> Stream to an event hub</p> <p><input type="checkbox"/> Send to partner solution</p>

Your selected logs might take up to 15 minutes for the logs to populate in your Log Analytics workspace.

Run queries in Log Analytics

With your logs streaming to your Log Analytics workspace, you can run queries using the **Kusto Query Language (KQL)**. The least privileged role to run queries is the **Reports Reader** role

1. Browse to Identity > Monitoring & health > Log Analytics.
2. In the **Search** textbox, type your query, and select Run.

Kusto query examples

Take 10 random entries from the input data:

- `SigninLogs | take 10`

Look at the sign-ins where the Conditional Access was a success:

- `SigninLogs | where ConditionalAccessStatus == "success" | project UserDisplayName, ConditionalAccessStatus`

Count number of successes:

- `SigninLogs | where ConditionalAccessStatus == "success" | project UserDisplayName, ConditionalAccessStatus | count`

Aggregate count of successful sign-ins by user by day:

- `SigninLogs | where ConditionalAccessStatus == "success" | summarize SuccessfulSignIns = count() by UserDisplayName, bin(TimeGenerated, 1d)`

View how many times a user does a certain operation in specific time period:

- `AuditLogs | where TimeGenerated > ago(30d) | where OperationName contains "Add member to role" | summarize count() by OperationName, Identity`

Pivot the results on operation name:

- `AuditLogs | where TimeGenerated > ago(30d) | where OperationName contains "Add member to role" | project OperationName, Identity | evaluate pivot(OperationName)`

Merge together Audit and Sign in Logs using an inner join:

- `AuditLogs | where OperationName contains "Add User" | extend UserPrincipalName = tostring(TargetResources[0].userPrincipalName) | project TimeGenerated, UserPrincipalName | join kind = inner (SigninLogs) on UserPrincipalName | summarize arg_min(TimeGenerated, *) by UserPrincipalName | extend SignInDate = TimeGenerated`

View number of signs ins by client app type:

- `SigninLogs | summarize count() by ClientAppUsed`

Count the sign ins by day:

- `SigninLogs | summarize NumberOfEntries=count() by bin(TimeGenerated, 1d)`

Take five random entries and project the columns you wish to see in the results:

- `SigninLogs | take 5 | project ClientAppUsed, Identity, ConditionalAccessStatus, Status, TimeGenerated`

Take the top 5 in descending order and project the columns you wish to see:

- `SigninLogs | take 5 | project ClientAppUsed, Identity, ConditionalAccessStatus, Status, TimeGenerated`

Create a new column by combining the values to two other columns:

- `SigninLogs | limit 10 | extend RiskUser = strcat(RiskDetail, "-", Identity) | project RiskUser, ClientAppUsed`

Next step

[Create a custom workbook](#)

Tutorial: Create a custom workbook for Microsoft Entra ID

Article • 04/14/2025

In this tutorial, you learn how to:

- ✓ Create a custom workbook
- ✓ Add a query to an existing workbook template

Prerequisites

To analyze activity logs with Log Analytics, you need the following roles and requirements:

- [Microsoft Entra monitoring and health licensing](#)
- [Access to create a Log Analytics workspace](#)
- The appropriate role for Azure Monitor:
 - Monitoring Reader
 - Log Analytics Reader
 - Monitoring Contributor
 - Log Analytics Contributor
- The appropriate role for Microsoft Entra ID:
 - Reports Reader
 - Security Reader
 - Global Reader
 - Security Administrator

If you haven't already created a Log Analytics workspace, complete the [Configure Log Analytics workspace](#) tutorial.

Create a custom workbook

In addition to querying the data with Kusto Query Language (KQL), you can create a custom workbook for further analysis and alerting. The least privileged role to create or update a workbook is the **Security Administrator** role.

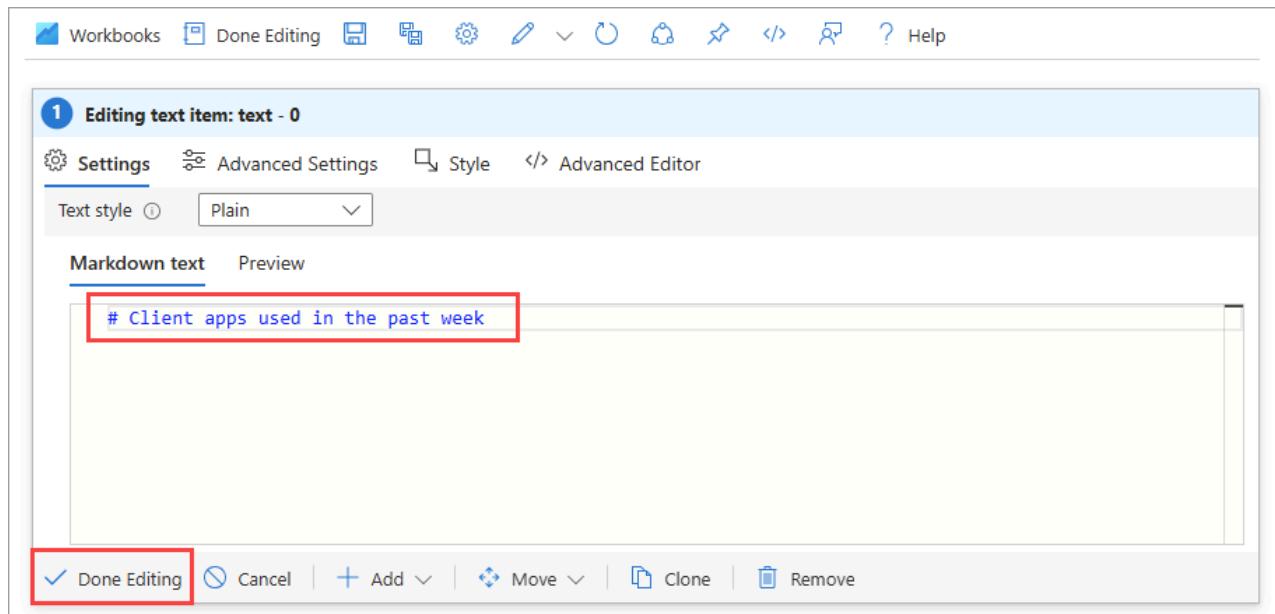
1. Browse to **Identity > Monitoring & health > Workbooks**.
2. In the **Quickstart** section, select **Empty**.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with various monitoring and health logs. The 'Workbooks' option is highlighted with a red box. The main area is titled 'Gallery' under 'Microsoft Entra ID'. It shows a list of workbooks, with the first one, 'Empty', highlighted by a red box. Below the list are sections for 'Recently modified workbooks (0)' and 'Usage (10)'. At the bottom, there are three cards: 'Sign-ins using Legacy Aut...', 'Sign-ins', and 'Access Package Activity'.

3. From the Add menu, select Add text.

The screenshot shows an 'Unsaved Workbook - 10/24/2024, 2:16 PM' window. The toolbar includes icons for Workbooks, Done Editing, and other editing tools. Below the toolbar, a message says 'This Workbook has no content.' An arrow points down to the 'Add' button, which is highlighted with a red box. A dropdown menu lists several options: 'Add text' (which is selected), 'Add parameters', 'Add links/tabs', 'Add query', 'Add metric', and 'Add group'. The 'Add text' option is currently selected.

4. In the textbox, enter # Client apps used in the past week and select Done Editing.



5. Below the text window, open the Add menu and select Add query.

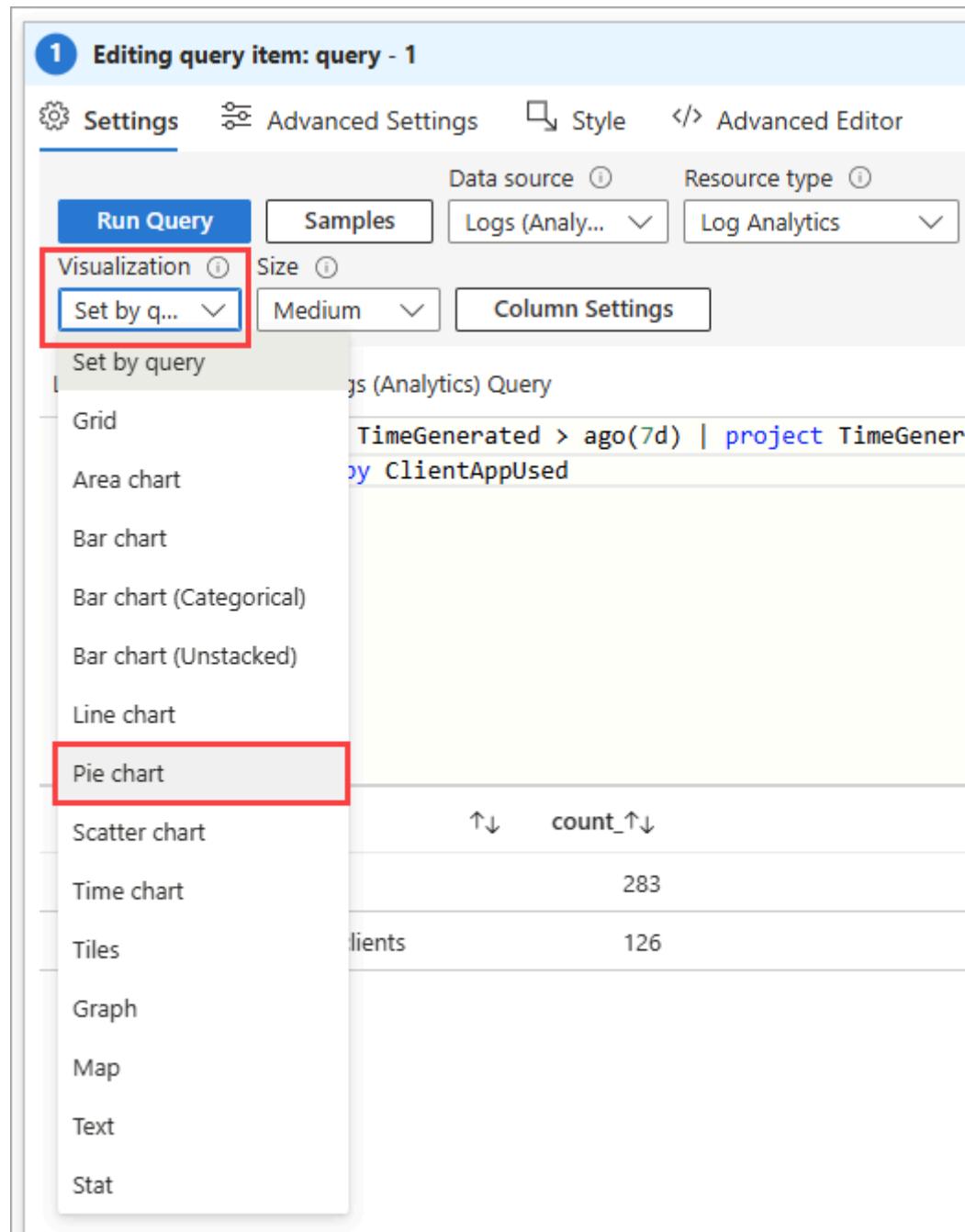
The screenshot shows the Log Analytics workspace with the title 'Client apps used in the past week'. At the top, there are navigation links: Workbooks, Done Editing, and several icons for search, refresh, and help. To the right of the title is an 'Edit' button. Below the title, there is a 'Add' dropdown menu with several options: 'Add text', 'Add parameters', 'Add links/tabs', 'Add query' (which is highlighted with a red box), 'Add metric', and 'Add group'. The 'Add' dropdown has a plus sign icon and a downward arrow.

6. In the query textbox, enter: `SigninLogs | where TimeGenerated > ago(7d) | project TimeGenerated, UserDisplayName, ClientAppUsed | summarize count() by ClientAppUsed`

7. Select Run Query.

The screenshot shows the Log Analytics workspace with the title 'Editing query item: query - 1'. At the top, there are navigation links: Workbooks, Done Editing, and several icons for search, refresh, and help. Below the header, a blue bar indicates 'Editing query item: query - 1'. The main area contains a 'Settings' tab, 'Advanced Settings' link, 'Style' tab, and 'Advanced Editor' link. Under 'Run Query', there are buttons for 'Run Query' (which is highlighted with a red box), 'Samples', 'Logs (Analytics)', 'Log Analytics', 'shlipsey-log-anal...', and 'Last 24 hours'. Below the toolbar, there are sections for 'Visualization' (with 'Set by q...' and 'Medium' buttons) and 'Log Analytics workspace Logs (Analytics) Query'. The query text is: `SigninLogs | where TimeGenerated > ago(7d) | project TimeGenerated, UserDisplayName, ClientAppUsed | summarize count() by ClientAppUsed`. To the right of the query text are 'Query help' and a gear icon.

8. In the toolbar, from the Visualization menu select Pie chart.



9. Select **Done Editing** at the top of the page.

10. Select the **Save** icon to save your workbook.

11. In the dialog box that appears, enter a title, select a Resource group, and select **Apply**.

Add a query to a workbook template

You can add Kusto queries to your workbook. The example is based on a query that shows the distribution of successful and failed sign-ins with applied Conditional Access policies. The least privileged role to create or update a workbook is the **Security Administrator** role.

1. Browse to Identity > Monitoring & health > Workbooks.

2. In the **Conditional Access** section, select **Conditional Access Insights and Reporting**.

The screenshot shows a dashboard titled 'Conditional Access Insights and Reporting' under 'Microsoft Entra ID'. It includes sections for 'Usage (10)' and 'Conditional access (5)'. The 'Conditional access' section contains five items: 'Conditional Access Insights...', 'Continuous access evaluat...', 'Sign-ins by Conditional Ac...', 'Sign-ins by Grant Controls...', and 'Conditional Access Gap A...'. The first item, 'Conditional Access Insights...', is highlighted with a red box.

3. In the toolbar, select **Edit**.

The screenshot shows the same dashboard as above, but the 'Edit' button in the toolbar is highlighted with a red box.

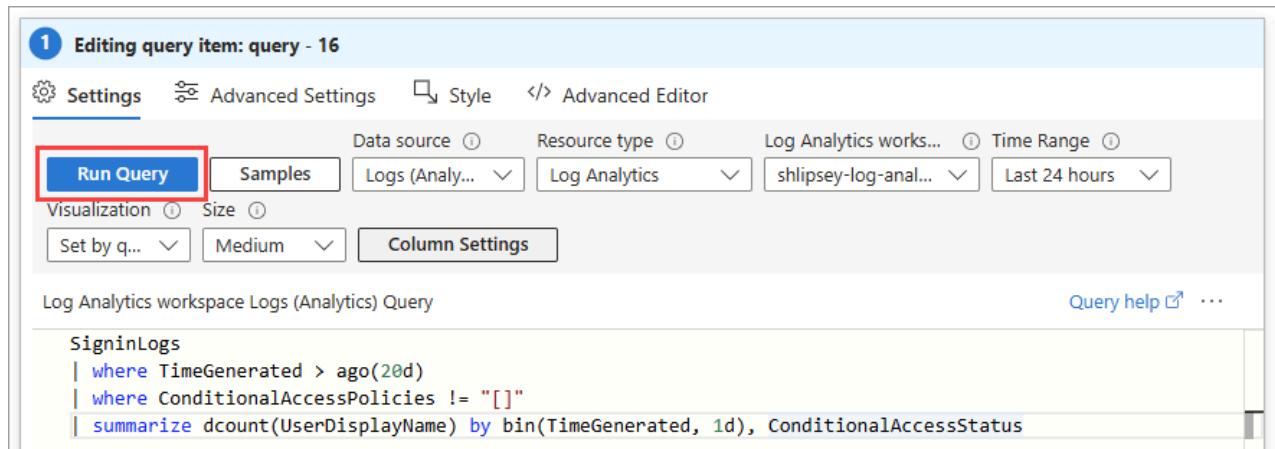
4. In the toolbar, select the three dots next to the **Edit** button, then **Add**, and then **Add query**.

The screenshot shows the dashboard with the 'Edit' button and its three-dot menu highlighted with red boxes. A context menu is open at the 'Add' option, with 'Add query' highlighted with a red box.

5. In the query textbox, enter: `SigninLogs | where TimeGenerated > ago(20d) | where ConditionalAccessPolicies != "[]" | summarize dcount(UserDisplayName) by`

```
bin(TimeGenerated, 1d), ConditionalAccessStatus
```

6. Select Run Query.



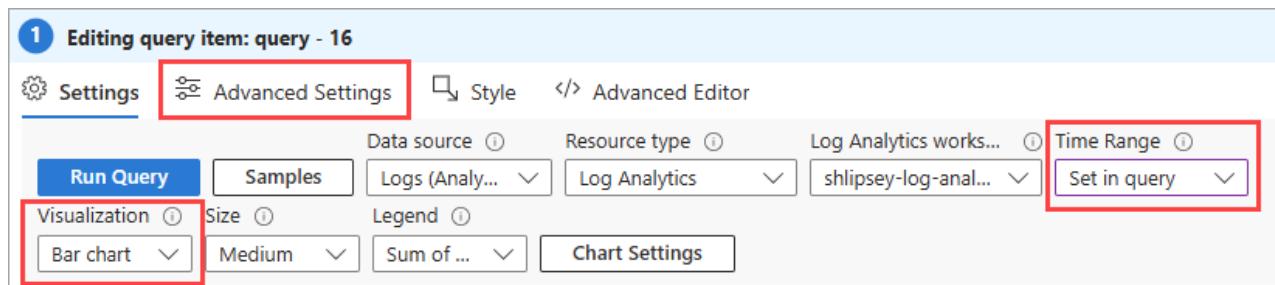
The screenshot shows the Log Analytics workspace interface. At the top, there's a navigation bar with 'Log Analytics workspace Logs (Analytics) Query'. Below it is a toolbar with tabs: 'Settings' (selected), 'Advanced Settings', 'Style', and 'Advanced Editor'. Under 'Advanced Settings', there are dropdowns for 'Data source' (Logs (Analytics)), 'Resource type' (Log Analytics), 'Log Analytics workspace...' (shlipsey-log-anal...), and 'Time Range' (Last 24 hours). The main area contains a query editor with the following DQL:

```
SigninLogs  
| where TimeGenerated > ago(20d)  
| where ConditionalAccessPolicies != "[]"  
| summarize dcount(UserDisplayName) by bin(TimeGenerated, 1d), ConditionalAccessStatus
```

7. From the Time Range menu, select Set in query.

8. From the Visualization menu, select Bar chart.

9. Select Advanced Settings.



This screenshot shows the same Log Analytics workspace interface as the previous one, but with different settings highlighted. The 'Advanced Settings' tab is now selected. In the 'Time Range' section, the 'Set in query' dropdown is highlighted with a red box. In the 'Visualization' section, the 'Bar chart' dropdown is also highlighted with a red box.

10. In the Chart title field, enter Conditional Access status over the last 20 days and select Done Editing.

1 Editing query item: query - 16

Settings Advanced Settings Style Advanced Editor

Step name ⓘ
query - 16

Make this item conditionally visible ⓘ
 Always show the pin icon on this step ⓘ
 When items are selected, export parameters ⓘ
 Show query when not editing
 Show open external query button when not editing
 Show refresh icon when not editing ⓘ
 Show Export to Excel button when not editing

Columns to Export
Visible Columns All Columns

Show annotations ⓘ
 Enable time range brushing ⓘ

Chart title ⓘ
Conditional Access status over the last 20 days

No data message ⓘ
The query returned no results.

No data message style ⓘ
Info

Done Editing Cancel | Add Move Clone Remove

Your Conditional Access success and failure chart displays a color-coded snapshot of your tenant.

Related content

- [Configure Log Analytics workspace](#)
- [Configure diagnostic settings](#)
- [Integrate activity logs with Log Analytics](#)

Analyze Microsoft Entra activity logs with Log Analytics

Article • 12/05/2024

After you [integrate Microsoft Entra activity logs with Azure Monitor logs](#), you can use the power of Log Analytics and Azure Monitor logs to gain insights into your environment.

- Compare your Microsoft Entra sign-in logs against security logs published by Microsoft Defender for Cloud.
- Troubleshoot performance bottlenecks on your application's sign-in page by correlating application performance data from Azure Application Insights.
- Analyze the Identity Protection risky users and risk detections logs to detect threats in your environment.

This article describes to analyze the Microsoft Entra activity logs in your Log Analytics workspace.

Prerequisites

To analyze activity logs with Log Analytics, you need:

- A working Microsoft Entra tenant with a Microsoft Entra ID P1 or P2 license associated with it.
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#). There are several factors that determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log

Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader
- **View and modify settings:**
 - Monitoring Contributor
 - Log Analytics Contributor

For more information on the Azure Monitor built-in roles, see [Roles, permissions, and security in Azure Monitor](#).

For more information on the Log Analytics roles, see [Azure built-in roles](#)

Microsoft Entra roles

Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

Access Log Analytics

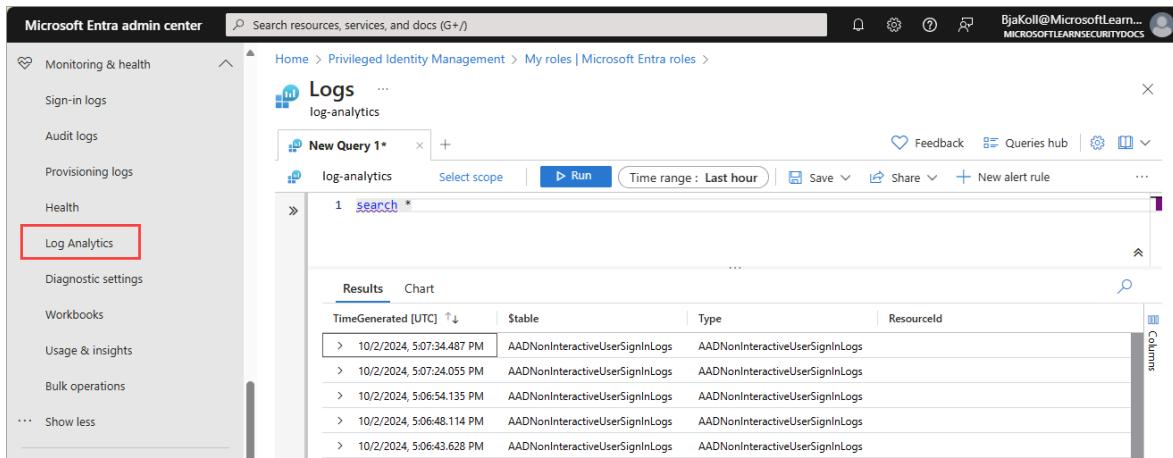
To view the Microsoft Entra ID Log Analytics, you must already be sending your activity logs from Microsoft Entra ID to a Log Analytics workspace. This process is covered in the [How to integrate activity logs with Azure Monitor](#) article.

💡 Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).

2. Browse to **Identity > Monitoring & health > Log Analytics**. A default search query runs.



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar under 'Monitoring & health' with options like Sign-in logs, Audit logs, Provisioning logs, Health, and Log Analytics (which is highlighted with a red box). The main area is titled 'Logs' and 'log-analytics'. It shows a 'New Query 1*' tab with a search bar containing 'search *'. Below it, there are tabs for 'Results' and 'Chart'. The results table has columns: TimeGenerated [UTC], \$Table, Type, and ResourceId. It lists five entries from 10/2/2024 at various times, all categorized as 'AADNonInteractiveUserSignInLogs'. At the top right of the main area, there are buttons for Feedback, Queries hub, Save, Share, New alert rule, and more.

3. Expand the **LogManagement** category to view the list of log related queries.
4. Select or hover over the name of a query to view a description and other useful details.
5. Expand a query from the list to view the schema.

The screenshot shows the Azure Log Analytics interface. At the top, there's a search bar and a 'Run' button. Below that is a navigation bar with 'Tables', 'Queries', 'Functions', and 'Filter'. A search bar and filter controls are also present. The main area displays a hierarchical list of tables under 'LogManagement'. The 'SigninLogs' table is highlighted with a red box. Below it is a list of columns: AADTenantId, AlternateSignInName, AppDisplayName, AppId, AppliedConditionalAccessPolicies, AppliedEventListeners, AuthenticationContextClassReferences, AuthenticationDetails, AuthenticationMethodsUsed, AuthenticationProcessingDetails, AuthenticationProtocol, AuthenticationRequirement, and AuthenticationRequirementPolicies.

Query activity logs

You can run queries against the activity logs being routed to a Log Analytics workspace. For example, to get a list of applications with the most sign-ins from last week, enter the following query and select the **Run** button.

```
Kusto

SigninLogs
| where CreatedDateTime >= ago(7d)
| summarize signInCount = count() by AppDisplayName
| sort by signInCount desc
```

To find risky sign-in events, use the following query:

```
Kusto
```

```
SigninLogs  
| where RiskState contains "atRisk"
```

To get the top audit events over the last week, use the following query:

Kusto

```
AuditLogs  
| where TimeGenerated >= ago(7d)  
| summarize auditCount = count() by OperationName  
| sort by auditCount desc
```

To summarize the count of provisioning events per day, by action:

Kusto

```
AADProvisioningLogs  
| where TimeGenerated > ago(7d)  
| summarize count() by Action, bin(TimeGenerated, 1d)
```

Take 100 provisioning events and project key properties:

Kusto

```
AADProvisioningLogs  
| extend SourceIdentity = parse_json(SourceIdentity)  
| extend TargetIdentity = parse_json(TargetIdentity)  
| extend ServicePrincipal = parse_json(ServicePrincipal)  
| where tostring(SourceIdentity.identityType) == "Group"  
| project tostring(ServicePrincipal.Id), tostring(ServicePrincipal.Name),  
ModifiedProperties, JobId, Id, CycleId, ChangeId, Action,  
SourceIdentity.identityType, SourceIdentity.details,  
TargetIdentity.identityType, TargetIdentity.details, ProvisioningSteps  
| take 100
```

Related content

- [Get started with queries in Azure Monitor logs](#)
- [Create and manage alert groups in the Azure portal](#)
- [Create a new alert rule](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

How to configure email notifications for Microsoft Entra Health monitoring alerts (preview)

Article • 02/10/2025

Microsoft Entra Health provides tenant-level metrics and health signals for several key identity scenarios. These signals are fed into an anomaly detection service, which triggers alerts when significant changes are detected. You can configure email notifications for when an alert is triggered.

This article describes how to configure email notifications for Microsoft Entra Health monitoring alerts.

ⓘ Important

Microsoft Entra Health scenario monitoring and alerts are currently in PREVIEW. This information relates to a prerelease product that might be substantially modified before release. Microsoft makes no warranties, expressed or implied, with respect to the information provided here. The Microsoft Entra admin center experience is being released to customers in phases, so you might not see all the features described in this article.

Prerequisites

There are different roles, permissions, and license requirements to view health monitoring signals and configure and receive alerts. We recommend using a role with least privilege access to align with the [Zero Trust guidance](#).

- A tenant with a [Microsoft Entra P1 or P2 license](#) is required to *view the Microsoft Entra health scenario monitoring signals*.
- A tenant with both a non-trial [Microsoft Entra P1 or P2 license](#) *and* at least 100 monthly active users is required to *view alerts* and *receive alert notifications*.
- The [Reports Reader](#) role is the least privileged role required to *view scenario monitoring signals, alerts, and alert configurations*.
- The [Helpdesk Administrator](#) is the least privileged role required to *update alerts* and *update alert notification configurations*.
- The `HealthMonitoringAlert.Read.All` permission is required to *view the alerts using the Microsoft Graph API*.

- The `HealthMonitoringAlert.ReadWrite.All` permission is required to *view and modify the alerts using the Microsoft Graph API*.
- For a full list of roles, see [Least privileged role by task](#).

ⓘ Note

Newly onboarded tenants might not have enough data to generate alerts for about 30 days.

Determine email notification recipients

We recommend daily review of the Microsoft Entra Health monitoring scenarios so you're familiar with the baseline metrics and so you can identify trends. It's important to also configure email notifications for when an alert is triggered.

Email notifications are sent to the [Microsoft Entra group](#) of your choice. We recommend sending alerts to users with the appropriate access to investigate and take action on the alerts. Not every role can take the same action, so consider including a group with the following roles:

- [Security Reader](#)
- [Security Administrator](#)
- [Intune Administrator](#)
- [Conditional Access Administrator](#)

Configure the email notifications

Email notification settings can be configured for each scenario in the Microsoft Entra admin center or using the Microsoft Graph API.

Microsoft Entra admin center

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Helpdesk Administrator](#).
2. Browse to **Identity > Monitoring & health > Health** and select the **Health monitoring** tab.
3. Select the scenario you want to configure email notifications for.

Keep track of your tenant's authentication procedures with low-latency monitoring and alerts for anomaly detection. Alerts last for 30 days.

All scenarios	Scenarios with active alerts
4	1

Scenario	Active alerts	Last alert received
Sign-ins requiring Entra ID MFA	1 alert	12/31/2024, 2:32:07 PM
Sign-ins requiring a managed device	No active alerts	
Sign-ins requiring a compliant device	No active alerts	
Sign-ins to applications using SAML authentication	Data only	

4. From the **Group alert notifications** section, select either the **+Select** or **Edit** button.

- If no group is selected, the **+Select** button is displayed.
- If a group is already selected, the **Edit** button is displayed.

This page helps you find potential multifactor authentication (MFA) sign-in health issues. Excludes refreshed sessions and passwordless methods.

Group alert notifications

Send an email to notify all members of a group each time there is an alert for this scenario.

Group to notify

AD Expense App **Edit**

View data graph

5. From the panel that opens, select the group you want to receive the alerts and select the **Select** button.

- Only one group can be selected.
- The group is updated in the **Group alert notifications** section of the scenario page.

Members of the selected group will receive an email notification the next time an alert is triggered for the scenario. Repeat this process for the other scenarios.

! Note

If the selected group has other groups added as members of that group, the notifications are sent to only the top three groups in the hierarchy.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback !\[\]\(2316339b7fcc7ac31f2aaab1990b3fd6_img.jpg\)](#)

How to investigate Microsoft Entra Health monitoring alerts (preview)

Article • 02/19/2025

Microsoft Entra Health monitoring helps you monitor the health of your Microsoft Entra tenant through a set of health metrics and intelligent alerts. Health metrics are fed into our anomaly detection service, which uses machine learning to understand the patterns for your tenant. When the anomaly detection service identifies a significant change in one of the tenant-level patterns, it triggers an alert.

The signals and alerts provided by Microsoft Entra Health provide you with the starting point for investigating potential issues in your tenant. Because there's a wide range of scenarios and even more data points to consider, it's important to understand how to investigate these alerts effectively. This article provides guidance on how to investigate alerts, in general. For scenario-specific guidance, see the related content at the end of this article.

ⓘ Important

Microsoft Entra Health scenario monitoring and alerts are currently in PREVIEW. This information relates to a prerelease product that might be substantially modified before release. Microsoft makes no warranties, expressed or implied, with respect to the information provided here.

Prerequisites

There are different roles, permissions, and license requirements to view health monitoring signals and configure and receive alerts. We recommend using a role with least privilege access to align with the [Zero Trust guidance](#).

- A tenant with a [Microsoft Entra P1 or P2 license](#) is required to *view* the Microsoft Entra health scenario monitoring signals.
- A tenant with both a non-trial [Microsoft Entra P1 or P2 license](#) and at least 100 monthly active users is required to *view alerts* and *receive alert notifications*.
- The [Reports Reader](#) role is the least privileged role required to *view scenario monitoring signals, alerts, and alert configurations*.
- The [Helpdesk Administrator](#) is the least privileged role required to *update alerts* and *update alert notification configurations*.

- The `HealthMonitoringAlert.Read.All` permission is required to *view the alerts using the Microsoft Graph API*.
- The `HealthMonitoringAlert.ReadWrite.All` permission is required to *view and modify the alerts using the Microsoft Graph API*.
- For a full list of roles, see [Least privileged role by task](#).

 **Note**

Newly onboarded tenants might not have enough data to generate alerts for about 30 days.

Investigate the signals and alerts

You can view the Microsoft Entra Health monitoring signals from the Microsoft Entra admin center. You can also view the properties of the signals and the public preview of health monitoring alerts, using [Microsoft Graph APIs](#).

When you receive an alert, you typically need to investigate the following data sets:

- **Metrics:** The data stream, or health signal, that caused the alert.
- **Affected entities:** Total number of affected entities. Could include users and applications.
- **Activity logs:** Sign-in logs provide details around affected users. Audit logs provide insights into application configuration changes.
- **Scenario-specific resources:** Depending on the scenario, you might need to investigate other sources of information from different services. For example, for device-related scenarios, you might need to review Intune device compliance policies.

 Admin center

The signals and alerts are available in the Microsoft Entra Health area of the Microsoft Entra admin center. Whether you're investigating an alert or just monitoring the health of your tenant, you can view the signals and alerts from the Microsoft Entra admin center.

View the signals

1. Sign into the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).

2. Browse to **Identity > Monitoring and health > Health**. The page opens to the Service Level Agreement (SLA) Attainment page.

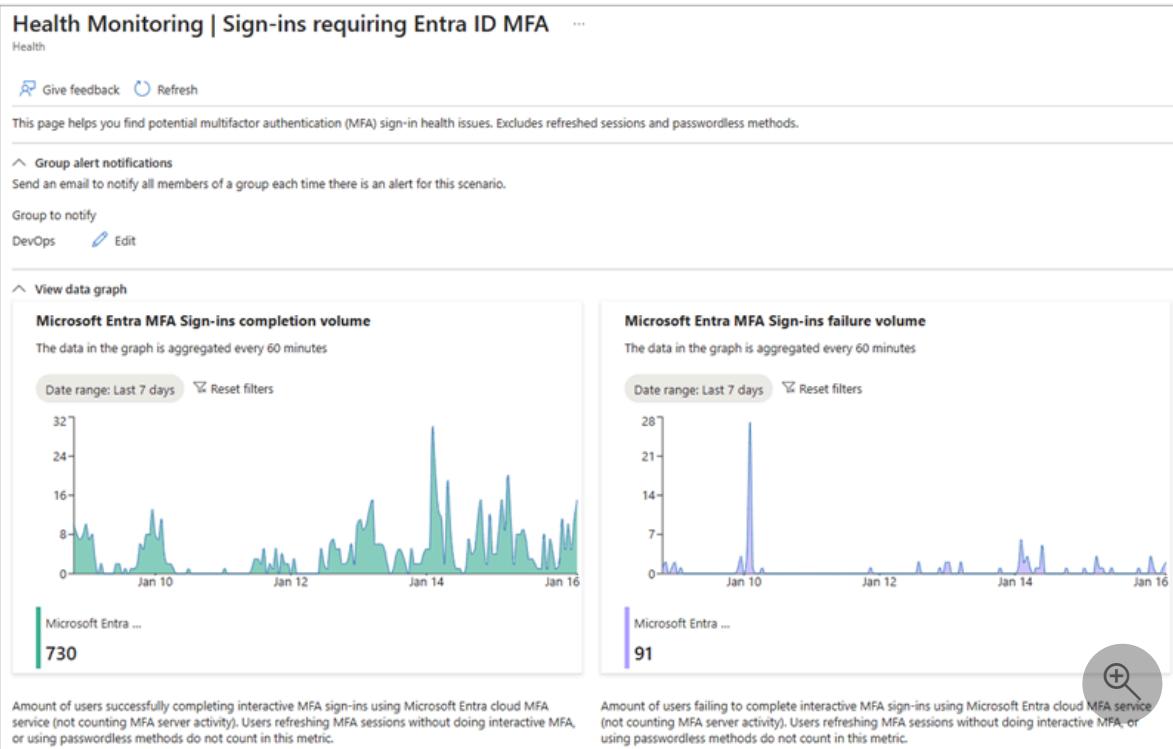
3. Select the **Health Monitoring** tab.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a tree view with categories like Identity Governance, External Identities, User experiences, Hybrid management, Monitoring & health, Sign-in logs, Audit logs, Provisioning logs, Log Analytics, Diagnostic settings, Workbooks, Usage & insights, and Learn & support. The 'Health' link under 'Monitoring & health' is highlighted with a red box. The main content area is titled 'Health' and contains a sub-header 'Health Monitoring'. It includes a brief description: 'Keep track of your tenant's authentication procedures with low-latency monitoring and alerts for anomaly detection. Alerts last for 30 days.' Below this are two buttons: 'All scenarios' (4) and 'Scenarios with active alerts' (1). A table lists four scenarios: 'Sign-ins requiring Entra ID MFA' (1 alert), 'Sign-ins requiring a managed device' (No active alerts), 'Sign-ins requiring a compliant device' (No active alerts), and 'Sign-ins to applications using SAML authentication' (Data only). A search icon is in the bottom right corner of the table area.

4. Select a scenario from the list. The page opens to the scenarios with active alerts, but if you want to view the signals for a different scenario, select the **All scenarios** filter button.

5. View the signal in the **View data graph** section. You might need to expand this section if you're viewing a scenario with an active alert.

- The date range can be changed to view the last 24 hours, seven days, or previous month.
- Hover your mouse over the graph to see the data points for a particular point in time.
- The value at the bottom of the graph is the total count for that scenario for the selected time frame.



Investigate the alerts

To view these details from the **Health monitoring** landing page:

1. Select the active alert you want to investigate.

The screenshot shows the 'Health Monitoring | Sign-ins requiring Entra ID MFA' page. It displays two boxes: 'All alerts' (2) and 'Active alerts' (1). The 'Active alerts' box is highlighted with a red border. Below the boxes are filters for 'Date range: Last 1 month' and 'Status: Needs attention'. A 'Mark alert as' dropdown is shown. At the bottom, there is a table with columns: Alert, Date created, Affected entities, and Status. The first row in the table is highlighted with a red border and contains the text 'Large increase in MFA sign-in failures'.

Alert	Date created	Affected entities	Status
<input type="checkbox"/> Large increase in MFA sign-in failures	1/10/2025, 4:59:41 PM	32	Needs attention

2. From the **Affected entities** section of the selected scenario, select **View** for the type of affected entity you want to investigate.

- Possible entities include users and applications.
- A link is provided to a scenario-specific article for more information on how to investigate the issue.

The screenshot shows a Microsoft Health Monitoring alert titled "Large increase in MFA sign-in failures". The alert status is "Needs attention" and it was created on "1/10/2025, 4:59:41 PM". It lists 31 affected users and 1 application. There are links to a troubleshooting guide and documentation.

Large increase in MFA sign-in failures ...

Health Monitoring

Mark alert as Give feedback Refresh

Status	Date created
Needs attention	1/10/2025, 4:59:41 PM

Affected entities

31 Users [View](#)
1 Application [View](#)

Documentation

[Troubleshooting guide](#)

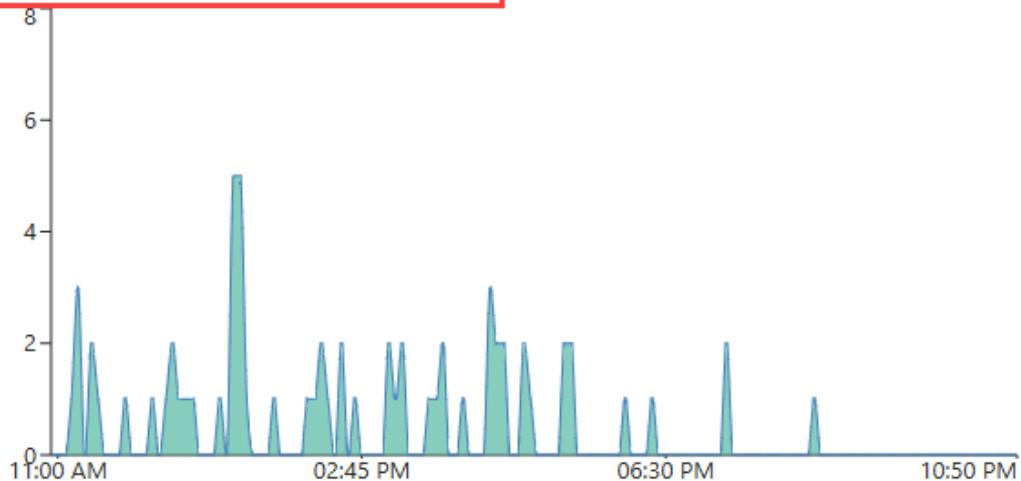
3. From the details that appear in the panel that opens, select an entity to explore further.
 - The top 10 most affected entities appear.
 - Selecting an item from the list navigates you to the user or application's profile page for further investigation.
4. The signal for the alert appears under the **Signals** section. Review the signal to understand the pattern and identify anomalies.
 - The time frame shows the time during which the anomaly occurred.

Signals

Microsoft Entra MFA Sign-ins completion volume

The data in the graph is aggregated every 10 minutes

Date range: 01/10 10:55 am - 01/10 10:50 pm



Microsoft Entra ...

65

5. After investigating and potentially resolving the root cause of the issue, you can dismiss the alert. From the active alert page, select the checkbox for that alert then select the **Mark alert as** menu and select **Dismissed**.

- The equivalent action using the Microsoft Graph API is to update the alert status to `resolved`.

Alert	Date created	Affected entities	Status
Large increase in MFA sign-in failures	1/10/2025, 4:59:41 PM	32	Needs attention

Related content

- [Sign-ins requiring a compliant or managed device](#)
- [Sign-ins requiring MFA](#)
- [Microsoft Graph Health monitoring alerts API documentation](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

How to investigate the Conditional Access block policy alert

Article • 04/25/2025

Microsoft Entra Health monitoring provides a set of tenant-level health metrics you can monitor and alerts for when a potential issue or failure condition is detected. There are multiple health scenarios that can be monitored, including Conditional Access block policies. To learn more about how Microsoft Entra Health works, see:

- [What is Microsoft Entra Health?](#)
- [How to use Microsoft Entra health monitoring signals and alerts](#)

This article describes the health metrics related to Conditional Access block policies, such as it unexpectedly blocking users from accessing resources or the policy not working as intended.

Important

Microsoft Entra Health scenario monitoring and alerts are currently in PREVIEW. This information relates to a prerelease product that might be substantially modified before release. Microsoft makes no warranties, expressed or implied, with respect to the information provided here.

Prerequisites

There are different roles, permissions, and license requirements to view health monitoring signals and configure and receive alerts. We recommend using a role with least privilege access to align with the [Zero Trust guidance](#).

- A tenant with a [Microsoft Entra P1 or P2 license](#) is required to *view* the Microsoft Entra health scenario monitoring signals.
- A tenant with both a [Microsoft Entra P1 or P2 license](#) *and* at least 100 monthly active users is required to *view alerts* and *receive alert notifications*.
- The [Reports Reader](#) role is the least privileged role required to *view scenario monitoring signals, alerts, and alert configurations*.
- The [Helpdesk Administrator](#) is the least privileged role required to *update alerts* and *update alert notification configurations*.
- The [Conditional Access Administrator](#) role is required to *view and modify Conditional Access policies*.
- The `HealthMonitoringAlert.Read.All` permission is required to *view the alerts using the Microsoft Graph API*.

- The `HealthMonitoringAlert.ReadWrite.All` permission is required to *view and modify the alerts using the Microsoft Graph API*.
- For a full list of roles, see [Least privileged role by task](#).

Investigate the alert and signal

Investigating an alert starts with gathering data. With Microsoft Entra Health in the Microsoft Entra admin center, you can view the signal and alert details in one place. You can also view the signals and alerts using the Microsoft Graph API. For more information, see [How to investigate health scenario alerts](#) for guidance on how to gather data using the Microsoft Graph API.

1. Sign into the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Identity > Monitoring and health > Health**. The page opens to the Service Level Agreement (SLA) Attainment page.
3. Select the **Health Monitoring** tab.
4. Select the **Conditional Access block policy** scenario and then select an active alert.
5. View the signal from the **View data graph** section to get familiar with the pattern and identify anomalies.
6. Investigate common Conditional Access issues.
 - [Troubleshoot Conditional Access sign-in problems](#).
 - [Block access example policy](#).
7. Review the sign-in logs.
 - [Review the sign-in log details](#).
 - Look for sign-ins where the Conditional Access status is "failure."
8. Check the audit logs for recent policy changes.
 - [Use the audit logs to troubleshoot Conditional Access policy changes](#).

Understand the signal

The Microsoft Entra Health signal for Conditional Access block policy could trigger an alert if there's a spike or dip in the number of users blocked from accessing resources due to a Conditional Access policy.

- A spike could mean a new policy was enabled or an existing policy was modified to target a broader set of users and resources.
- A dip could mean that a policy was disabled or modified to target a smaller set of users and resources.

These changes could be intentional or unintentional.

- If the change was intentional, no other action is likely needed.
- If the change is unintentional, you should review the modified Conditional Access policy in the audit logs.

Mitigate common issues

The following common issues could cause the Conditional Access block policy alert to trigger an alert. This list isn't exhaustive, but provides a starting point for your investigation.

Many users are receiving the "You can't get there from here" message

The Conditional Access block alert can trigger if there's an increase in the "You can't get there from here" error message during sign-in. This message appears if the application the user is trying to access can only be accessed from devices or client applications that meet the organization's mobile device management policy.

- A spike in a large number of users receiving this alert could indicate a change to the organization's mobile device management policy.
- A spike for a few users could indicate an issue with their specific device.

To investigate:

Go to the **Affected entities** section of the selected scenario and select **View** for users.

- If the issue is affecting a larger number of users, there might be a change to the mobile device management policy that you need to address.
- If the issue is affecting a few users, it could be related to their specific device. They might need to join their devices to the organization's network. Select a user to navigate directly to their profile.

To remediate issues affecting a large number of users:

1. Review the audit logs to see what changes were made to your Conditional Access policies.

- Filter to Category: Policy and look for the following events:
 - Add conditional access policy
 - Delete conditional access policy
 - Update conditional access policy

Audit Logs ...

Date ↓	Service	Category	Activity	Status
2/14/25, 3:46:46 PM	Core Directory	Policy	Update policy	Success
2/14/25, 9:14:50 AM	Conditional Access	Policy	Update conditional access policy	Success
2/14/25, 9:14:50 AM	Core Directory	Policy	Update policy	Success
2/14/25, 9:14:50 AM	Core Directory	Policy	Update policy	Success
2/14/25, 9:10:12 AM	Conditional Access	Policy	Add conditional access policy	Success
2/14/25, 9:10:12 AM	Core Directory	Policy	Update policy	Success
2/14/25, 9:10:11 AM	Core Directory	Policy	Add policy	Success
2/12/25, 3:28:33 PM	Conditional Access	Policy	Delete conditional access policy	Success

- You can also use the following Microsoft Graph API queries:
 - GET `https://graph.microsoft.com/beta/auditLogs/directoryAudits?`
`$filter=loggedByService eq 'Conditional Access'`
 - GET `https://graph.microsoft.com/beta/auditLogs/directoryAudits?`
`$filter=loggedByService eq 'Conditional Access' and operationType eq 'Update'`
 - GET `https://graph.microsoft.com/beta/auditLogs/directoryAudits?`
`$filter=loggedByService eq 'Conditional Access' and operationType eq 'Add'`
 - GET `https://graph.microsoft.com/beta/auditLogs/directoryAudits?`
`$filter=loggedByService eq 'Conditional Access' and operationType eq 'Delete'`
 - GET `https://graph.microsoft.com/beta/auditLogs/directoryAudits?`
`$filter=loggedByService eq 'Conditional Access' and activityDateTime ge 2024-12-04T22:03:57.2013763Z`

2. Review your mobile device management policies to ensure they're configured correctly.
 Sign in to the [Microsoft Intune admin center](#) as an **Intune Administrator** and browse to **Devices > Configuration** to review your policies.

To remediate issues affecting specific users:

- Join their work-owned device to the organization's network.
- Register their personal device with the organization's network.

Related content

- [Learn about Conditional Access and Intune](#)
- [How to investigate health scenario alerts](#)

How to investigate the sign-ins requiring a compliant or managed device alert

Article • 02/19/2025

Microsoft Entra Health monitoring provides a set of tenant-level health metrics you can monitor and alerts when a potential issue or failure condition is detected. There are multiple health scenarios that can be monitored, including two related to devices:

- Sign-ins requiring a Conditional Access compliant device
- Sign-ins requiring a Conditional Access managed device

This article describes the health metrics related to compliant and managed devices and how to troubleshoot a potential issue when you receive an alert. For details on how to interact with the Health Monitoring scenarios and how to investigate all alerts, see [How to investigate health scenario alerts](#).

ⓘ Important

Microsoft Entra Health scenario monitoring and alerts are currently in PREVIEW. This information relates to a prerelease product that might be substantially modified before release. Microsoft makes no warranties, expressed or implied, with respect to the information provided here.

Prerequisites

There are different roles, permissions, and license requirements to view health monitoring signals and configure and receive alerts. We recommend using a role with least privilege access to align with the [Zero Trust guidance](#).

- A tenant with a [Microsoft Entra P1 or P2 license](#) is required to *view* the Microsoft Entra health scenario monitoring signals.
- A tenant with both a non-trial [Microsoft Entra P1 or P2 license](#) *and* at least 100 monthly active users is required to *view alerts* and *receive alert notifications*.
- The [Reports Reader](#) role is the least privileged role required to *view scenario monitoring signals, alerts, and alert configurations*.
- The [Helpdesk Administrator](#) is the least privileged role required to *update alerts* and *update alert notification configurations*.

- The `HealthMonitoringAlert.Read.All` permission is required to view the alerts using the Microsoft Graph API.
- The `HealthMonitoringAlert.ReadWrite.All` permission is required to view and modify the alerts using the Microsoft Graph API.
- For a full list of roles, see [Least privileged role by task](#).

Investigate the signals and alerts

Investigating an alert starts with gathering data. With Microsoft Entra Health in the Microsoft Entra admin center, you can view the signal and alert details in one place. You can also view the signals and alerts using the Microsoft Graph API. For more information, see [How to investigate health scenario alerts](#) for guidance on how to gather data using the Microsoft Graph API.

1. Sign into the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Identity > Monitoring and health > Health**. The page opens to the Service Level Agreement (SLA) Attainment page.
3. Select the **Health Monitoring** tab.
4. Select the **Sign-ins requiring a compliant device** or **Sign-ins requiring a managed device** scenario and then select an active alert.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a tree view with categories like Identity Governance, External Identities, User experiences, Hybrid management, Monitoring & health, Sign-in logs, Audit logs, Provisioning logs, and Learn & support. The 'Health' category is expanded, and 'Health Monitoring' is selected, indicated by a red box. The main content area is titled 'Health' and shows a summary card with 'All scenarios' (4) and 'Scenarios with active alerts' (1). Below this, there are two sections: 'Sign-ins requiring Entra ID MFA' (No active alerts) and 'Sign-ins requiring a managed device' (No active alerts). At the bottom, the 'Sign-ins requiring a compliant device' section is highlighted with a red box, showing '1 alert' received '12/31/2024, 2:32:07 PM'. A search bar at the top and a navigation bar with icons are also visible.

5. View the signal from the **View data graph** section to get familiar with the pattern and identify anomalies.

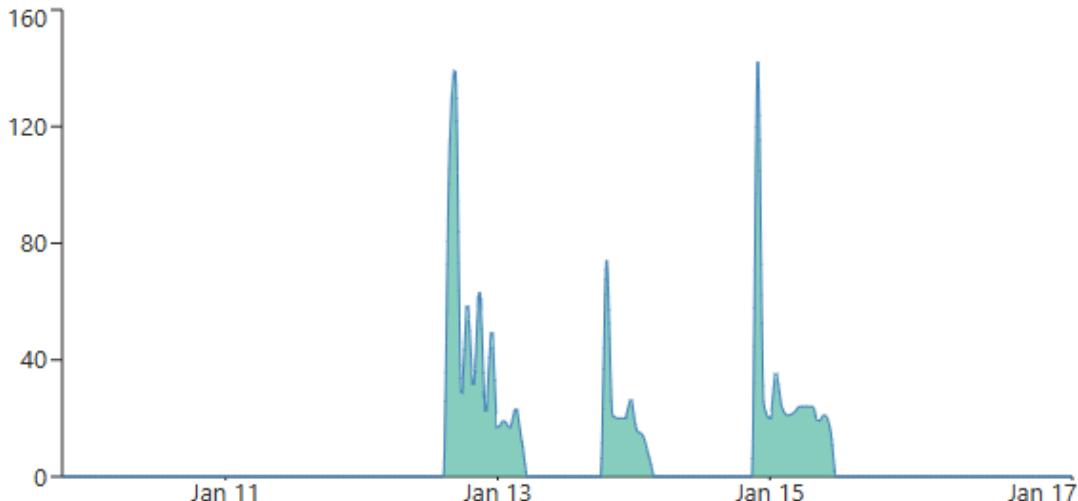
[View data graph](#)

Success count for sign-ins requiring a compliant device

The data in the graph is aggregated every 60 minutes

Date range: Last 7 days

Reset filters



Success count for...

1.2K

Number of user authentication requests that successfully satisfy a Conditional Access policy that requires devices compliance. Compliant devices are managed by Microsoft Intune and can be mobile iOS/Android devices, tablets, or cloud Microsoft Entra joined computers (not hybrid).

6. Review your Intune device compliance policies.

- For more information, see [Intune device compliance overview](#).
- Learn how to [Monitor device compliance policies](#).
- If you're not using Intune, review your device management solution's compliance policies.

7. Investigate common Conditional Access issues.

- [Troubleshoot Conditional Access device compliance policies](#).
- [Troubleshoot Conditional Access sign-in problems](#).

8. Review the sign-in logs.

- [Review the sign-in log details](#).
- Look for users being blocked from signing in *and* have a compliant device policy applied.

9. Check the audit logs for recent policy changes.

- [Use the audit logs to troubleshoot Conditional Access policy changes](#).

Mitigate common issues

The following common issues could cause a spike in sign-ins requiring a compliant or managed device. This list isn't exhaustive, but provides a starting point for your investigation.

Many users are blocked from signing in from known devices

If a large group of users are blocked from signing in to known devices, a spike could indicate that these devices have fallen out of compliance. If the number of affected users indicates a high percentage of your organization's users, you might be looking at a widespread issue.

To investigate:

1. From the **Affected entities** section of the selected scenario, select **View** for users.
 - A sample of affected users appears in a panel. Select a user to navigate directly to their profile where you can view their sign-in activity and other details.
 - With the Microsoft Graph API, look for the "user" `resourceType` and the `impactedCount` value in the impact summary.

The screenshot shows a card with two sections. The top section has 'Status' in blue and 'Needs attention' in bold black. To its right is 'Date created' in blue followed by the date '1/10/2025, 4:59:41 PM'. The bottom section is titled 'Affected entities' in blue, with '31 Users' and '1 Application' listed below it, each with a 'View' link. A red box highlights the 'Affected entities' section.

2. Check your [Intune device compliance policy](#).
3. Check your [Conditional Access device compliance policies](#).

User is blocked from signing in from an unknown device

If the increase in blocked sign-ins is coming from an unknown device, that spike could indicate that an attacker has acquired a user's credentials and is attempting to sign in from a device used for such attacks. If the number of affected users shows a small subset of users, the issue might be user-specific.

To investigate:

1. From the **Affected entities** section of the selected scenario, select **View for users**.
 - A list of affected users appears in a panel. Select a user to navigate directly to their profile where you can view their sign-in activity and other details.
 - With the Microsoft Graph API, look for the "user" `resourceType` and the `impactedCount` value in the impact summary.
2. [Review the sign-in logs](#).
3. [Investigate risk with Microsoft Entra ID Protection](#).

 **Note**

Microsoft Entra ID Protection requires a Microsoft Entra P2 license.

Network issues

There could be a regional system outage that required a large number of users to sign in at the same time.

To investigate:

1. From the **Affected entities** section of the selected scenario, select **View for users**.
 - A list of affected users appears in a panel. Select a user to navigate directly to their profile where you can view their sign-in activity and other details.
 - With the Microsoft Graph API, look for the "user" `resourceType` and the `impactedCount` value in the impact summary.
2. Check your system and network health to see if an outage or update matches the same timeframe as the anomaly.
3. [Review the sign-in logs](#).
 - Adjust your filter to show sign-ins from a region where an affected user is located.
4. If your organization is using Global Secure Access, review the [traffic logs](#).

Related content

- Learn about Conditional Access and Intune
 - Learn about Microsoft Entra hybrid joined devices
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

How to investigate sign-ins requiring Microsoft Entra multifactor authentication

Article • 02/19/2025

Microsoft Entra Health monitoring provides a set of tenant-level health metrics you can monitor and alerts when a potential issue or failure condition is detected. There are multiple health scenarios that can be monitored, including Microsoft Entra multifactor authentication (MFA).

This scenario:

- Aggregates the number of users who successfully completed an MFA sign-in using a Microsoft Entra cloud MFA service.
- Captures interactive sign-ins with Microsoft Entra MFA, aggregating both successes and failures.
- Excludes when a user refreshes the session without completing the interactive MFA or using passwordless sign-in methods.

This article describes these health metrics and how to troubleshoot a potential issue when you receive an alert. For details on how to interact with the Health Monitoring scenarios and how to investigate all alerts, see [How to investigate health scenario alerts](#).

ⓘ Important

Microsoft Entra Health scenario monitoring and alerts are currently in PREVIEW. This information relates to a prerelease product that might be substantially modified before release. Microsoft makes no warranties, expressed or implied, with respect to the information provided here.

Prerequisites

There are different roles, permissions, and license requirements to view health monitoring signals and configure and receive alerts. We recommend using a role with least privilege access to align with the [Zero Trust guidance](#).

- A tenant with a [Microsoft Entra P1 or P2 license](#) is required to view the Microsoft Entra health scenario monitoring signals.

- A tenant with both a non-trial Microsoft Entra P1 or P2 license *and* at least 100 monthly active users is required to *view alerts* and *receive alert notifications*.
- The [Reports Reader](#) role is the least privileged role required to *view scenario monitoring signals, alerts, and alert configurations*.
- The [Helpdesk Administrator](#) is the least privileged role required to *update alerts* and *update alert notification configurations*.
- The `HealthMonitoringAlert.Read.All` permission is required to *view the alerts using the Microsoft Graph API*.
- The `HealthMonitoringAlert.ReadWrite.All` permission is required to *view and modify the alerts using the Microsoft Graph API*.
- For a full list of roles, see [Least privileged role by task](#).

Investigate the signals and alerts

Investigating an alert starts with gathering data. With Microsoft Entra Health in the Microsoft Entra admin center, you can view the signal and alert details in one place. You can also view the signals and alerts using the Microsoft Graph API. For more information, see [How to investigate health scenario alerts](#) for guidance on how to gather data using the Microsoft Graph API.

1. Sign into the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring and health > Health**. The page opens to the Service Level Agreement (SLA) Attainment page.
3. Select the **Health Monitoring** tab.
4. Select the **Sign-ins requiring Entra ID MFA** scenario and then select an active alert.

Microsoft Entra admin center

Home > Health

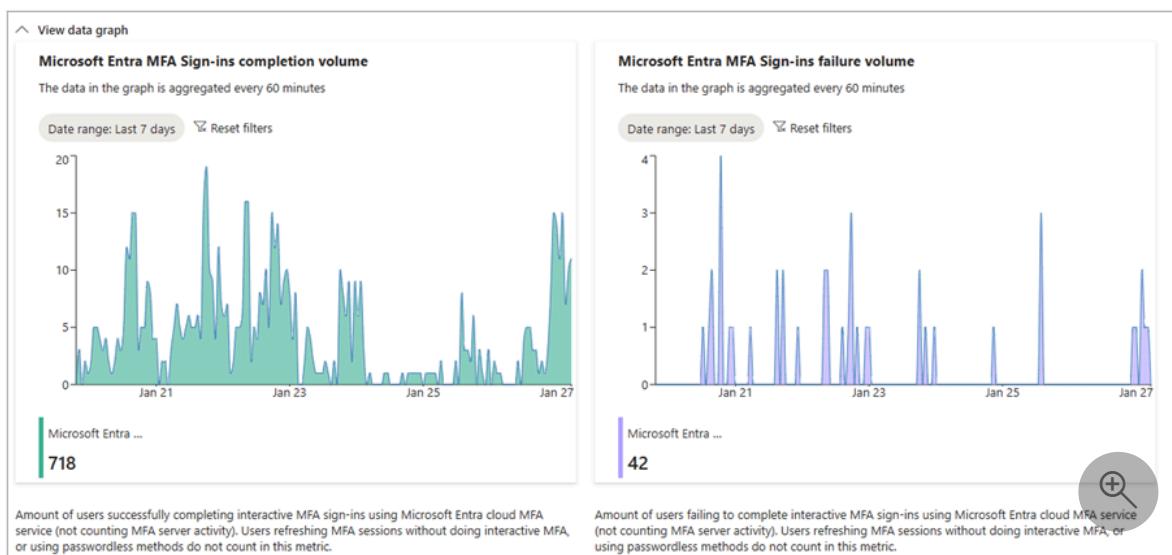
Health Monitoring SLA Attainment

Keep track of your tenant's authentication procedures with low-latency monitoring and alerts for anomaly detection. Alerts last for 30 days.

All scenarios	Scenarios with active alerts
4	1

Scenario	Active alerts	Last alert received
Sign-ins requiring Entra ID MFA	1 alert	12/31/2024, 2:32:07 PM
Sign-ins requiring a managed device	No active alerts	
Sign-ins requiring a compliant device	No active alerts	
Sign-ins to applications using SAML authentication	Data only	

- View the signal from the **View data graph** section to get familiar with the pattern and identify anomalies.



- Review the sign-in logs.

- Review the sign-in log details.
- Look for users being blocked from signing in *and* have a Conditional Access policy requiring MFA applied.

- Check the audit logs for recent policy changes.

- Use the audit logs to troubleshoot Conditional Access policy changes.

Mitigate common issues

The following common issues could cause a spike in MFA sign-ins. This list isn't exhaustive, but provides a starting point for your investigation.

Application configuration issues

An increase in sign-ins requiring MFA could indicate a policy change or new feature rollout potentially triggered a large number of users to sign in around the same time.

To investigate:

1. From the **Affected entities** section of the selected scenario, select **View** for applications.
 - A list of affected applications appears in a panel. Select the application to navigate directly to the application's details where you can view the audit logs and other details.
 - With the Microsoft Graph API, look for the "application" `resourceType` in the impact summary.
2. Review the audit logs for the application.
 - Determine if the application was recently added or reconfigured, which might trigger a large number of users signing in.
3. Review the sign-in logs.
 - Use the **Application** column to filter for the same application or date range to look for any other patterns.

User authentication issues

An increase in sign-ins requiring MFA could indicate a brute force attack, where multiple unauthorized sign-in attempts are made to a user's account.

To investigate:

1. From the **Affected entities** section of the selected scenario, select **View** for users.
 - A list of affected users appears in a panel. Select a user to navigate directly to their profile where you can view their sign-in activity and other details.
 - With the Microsoft Graph API, look for the "user" `resourceType` and the `impactedCount` value in the impact summary.
2. Review the sign-in logs.

- Use the following filters in the sign-in logs:
 - Status: Failure
 - Authentication requirement: Multifactor authentication
 - Adjust the date to match the timeframe indicated in the impact summary.
- Are the failed sign-in attempts coming from the same IP address?
- Are the failed sign-in attempts from the same user?
- Run the [sign-in diagnostic](#) to rule out standard user error issues or initial MFA setup issues.

Network issues

There could be a regional system outage that required a large number of users to sign in at the same time.

To investigate:

1. From the **Affected entities** section of the selected scenario, select **View** for users.
 - A list of affected users appears in a panel. Select a user to navigate directly to their profile where you can view their sign-in activity and other details.
 - With the Microsoft Graph API, look for the "user" `resourceType` and the `impactedCount` value in the impact summary.
2. Check your system and network health to see if an outage or update matches the same timeframe as the anomaly.
3. [Review the sign-in logs](#).
 - Adjust your filter to show sign-ins from a region where an affected user is located.
4. If your organization is using Global Secure Access, review the [traffic logs](#).

Related content

- [Configure Conditional Access for MFA for all users](#)
- [Troubleshoot common sign-in errors](#)
- [Learn about Conditional Access and Intune](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

How to investigate the sign-ins to applications using SAML authentication

Article • 04/25/2025

Microsoft Entra Health monitoring provides a set of tenant-level health metrics you can monitor to help improve the health of your tenant. The Security Assertion Markup Language (SAML) authentication scenario monitors SAML 2.0 authentication attempts that the Microsoft Entra cloud service for your tenant successfully processed.

- [Learn how the Microsoft Identity platform uses the SAML protocol](#)
- [Use a SAML 2.0 IdP for single sign on.](#)
- This metric currently excludes WS-FED/SAML 1.1 apps integrated with Microsoft Entra ID.
- Alerts are not available for this scenario.

Prerequisites

There are different roles, permissions, and license requirements to view health monitoring signals and configure and receive alerts. We recommend using a role with least privilege access to align with the [Zero Trust guidance](#).

- A tenant with a [Microsoft Entra P1 or P2 license](#) is required to view the Microsoft Entra health scenario monitoring signals.
- The [Reports Reader](#) role is the least privileged role required to view scenario monitoring signals.
- The `HealthMonitoringAlert.Read.All` permission is required to *view the alerts using the Microsoft Graph API*.
- For a full list of roles, see [Least privileged role by task](#).

Investigate the signals

You can view the signal using the Microsoft Entra admin center and the Microsoft Graph API. For more information, see [How to investigate health scenario alerts](#) for guidance on how to gather data using the Microsoft Graph API.

1. Sign into the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Entra ID > Monitoring & health > Health**. The page opens to the Service Level Agreement (SLA) Attainment page.
3. Select the **Health Monitoring** tab.

4. Select the Sign-ins to applications using SAML authentication scenario.

Health Monitoring | Sign-ins to applications using SAML authentication

Health

Give feedback Refresh

This page helps you find potential health issues with user authentications that use Security Assertion Markup Language (SAML) single sign-on (SSO).

View data graph

Sign-ins to applications using SAML authentication

The data in the graph is aggregated every 60 minutes

Date range: Last 7 days Reset filters

Date	Sign-ins to applic...
Jan 11	1
Jan 13	2
Jan 17	1

SAML 2.0 authentication successfully processed by the Microsoft Entra cloud service for your tenant. This health signal currently does not include WS-FED/SAML 1.1 apps integrated with Microsoft Entra ID.

+

How to use Microsoft Entra Recommendations

Article • 11/04/2024

The Microsoft Entra recommendations feature provides you with personalized insights with actionable guidance to:

- Help you identify opportunities to implement best practices for Microsoft Entra related features.
- Improve the state of your Microsoft Entra tenant.
- Optimize the configurations for your scenarios.

This article covers how to work with Microsoft Entra recommendations. Each Microsoft Entra recommendation contains similar details such as a description, the value of addressing the recommendation, and the steps to address the recommendation. Microsoft Graph API guidance is also provided in this article.

Prerequisites

There are different role requirements for viewing or updating a recommendation. Use the least-privileged role for the type of access needed. For a full list of roles, see [Least privileged roles by task](#).

 Expand table

Microsoft Entra role	Access type
Reports Reader	Read-only
Security Reader	Read-only
Global Reader	Read-only
Authentication Policy Administrator	Update and read
Exchange Administrator	Update and read
Security Administrator	Update and read
DirectoryRecommendations.Read.All	Read-only in Microsoft Graph
DirectoryRecommendations.ReadWrite.All	Update and read in Microsoft Graph

Some recommendations might require a P2 or other license. For more information, see [Recommendation availability and license requirements](#).

How to read a recommendation

Most recommendations follow the same pattern. You're provided information about how the recommendation works, its value, and some action steps to address the recommendation. This section provides an overview of the details provided in a recommendation, but aren't specific to one recommendation.

1. Sign in to the Microsoft Entra admin center [as at least a Reports Reader](#).
2. Browse to **Identity > Overview > Recommendations**.
3. Select a recommendation from the list.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, and Show more. The 'Identity' category is expanded. In the main content area, the 'Contoso, Ltd.' tenant is selected. The top navigation bar includes links for Add, Manage tenants, What's new, Preview features, and Got feedback. Below the navigation, tabs for Overview, Monitoring, Properties, Recommendations (which is underlined in red), and Tutorials are visible. A prominent section displays the 'Identity Secure Score' at 21.78%, with a note that it refreshes every 24 hours and a link to view the full score. Below this, a search bar and a filter button are shown. A table lists 12 recommendations, each with a priority (Medium, Medium, Low, High), a description (Remove unused credentials from applications, Remove unused applications, Use least privileged administrative roles, Protect all users with a user risk policy), a release type (Preview, Preview, Preview, Preview), and secure score points (N/A, N/A, 1/1, 0/7). The last four recommendations are highlighted with a red border.

Each recommendation provides the same set of details that explain what the recommendation is, why it's important, and how to fix it. The recommendation service runs every 24-48 hours, depending on the recommendation.

Protect your tenant with Insider Risk condition in Conditional Access policy

[Mark recommendation as](#) [Got feedback?](#)

Status	Priority	Points achieved	Impacted resource type
Active	Medium	0/5	Users

Status

The **Status** of a recommendation can be active, completed, dismissed, or postponed.

The recommendation service automatically marks a recommendation as completed when all impacted resources are addressed.

- **Active:** The recommendation has resources that need to be addressed. A dismissed, postponed, or completed recommendation can be manually changed back to active.
- **Completed:** All resources in the recommendation have been addressed. The status is updated automatically by the system when all resources are addressed according to the action plan. Recommendations can't be manually marked as completed.
- **Dismissed:** If the recommendation is irrelevant or the data is wrong, you can dismiss the recommendation. You must provide a reason for dismissing the recommendation.
- **Postponed:** If you want to address the recommendation at a later time, you can postpone it. The recommendation becomes active when the selected date occurs. You can postpone a recommendation for up to a year.

Priority

The **Priority** of a recommendation could be low, medium, or high. These values are determined by several factors, such as security implications, health concerns, or potential breaking changes.

- **High:** Must do. Not acting will result in severe security implications or potential downtime.
- **Medium:** Should do. No severe risk if action isn't taken.
- **Low:** Might do. No security risks or health concerns if action isn't taken.

Recommendation details

- The **Status description** tells you the date the recommendation status changed.
- The recommendation's **Value** is an explanation of why completing the recommendation benefits your organization and the value of the associated feature.
- The **Action plan** provides step-by-step instructions to implement a recommendation. The Action plan might include links to relevant documentation or direct you to other pages in the Azure portal.

- Some recommendations might include a **User impact** that describes the user experience when the recommendation is addressed.

Status description
Marked as active by system on 3/1/2023 at 5 PM MST.
Description
Your tenant has applications with credentials that will expire soon.

Impacted resources

The **Impacted resources** for a recommendation could be applications, users, or your full tenant. If the impacted resource is at the tenant level, you might need to make a global change. Not all recommendations populate the impacted resources table. For example, the "Remove unused applications" recommendation lists all applications that were identified by the recommendation service. Tenant-level recommendations, however, won't have any resources listed in the table.

For those recommendations where there are separate resources to address, the **Impacted resources** table contains a list of resources identified by the recommendation. The resource's name, ID, date it was first detected, and status are provided. The resource could be an application, user, or resource service principal, for example.

You can mark individual impacted resources as *dismissed* or *postponed*. The rules and functionality at the resource level are the same as at the recommendation level. In some recommendations, you can select the resource or the **More details** link to access the resource directly.

Remove unused credentials from applications

The screenshot shows the 'Impacted resources' section of the Microsoft Entra admin center. At the top, there are buttons for 'Mark recommendation as' and 'Got feedback?'. Below that is a section for 'Mark resource as' with a dropdown menu. A search bar labeled 'Search by ID' is present. Filter options include 'Show dates as: Local', 'Status : Active,Dismissed,Postponed' (with a close button), and 'Reset filters'. It displays '100 resources found'. A table lists three resources: 'Qmarkets' and 'SmartFile' are active and were first detected on Aug 28, 2024, at 3:01 AM; 'More details' links for both are highlighted with a red box. The third row is partially visible.

<input type="checkbox"/>	Resource	ID	First detected	Status	Actions
<input type="checkbox"/>	Qmarkets	11112222-bbbb-3333...	Aug 28, 2024, 3:01 AM	Active	More details
<input type="checkbox"/>	SmartFile	44445555-eeee-6666...	Aug 28, 2024, 3:01 AM	Active	More details

In the Microsoft Entra admin center, the impacted resources are limited to a maximum of 50 resources. To view all impacted resources for a recommendation, use the following Microsoft Graph API request: [GET](#)

```
/directory/recommendations/{recommendationId}/impactedResources
```

How to update a recommendation and impacted resources

You can update the status of a recommendation and any related resource in the Microsoft Entra admin center or using Microsoft Graph.

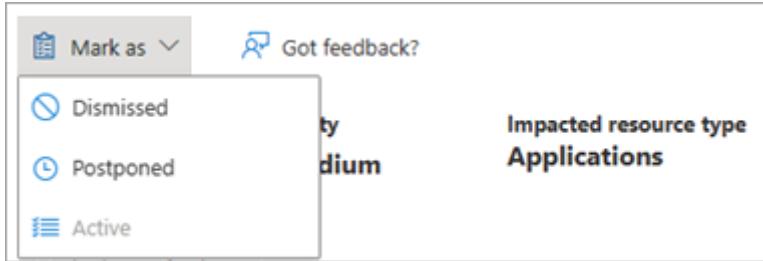
Microsoft Entra admin center

Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Overview > Recommendations**.
3. Select a recommendation from the list.
4. Follow the guidance in the **Action plan**.

5. If you need to manually change the status of a recommendation, select **Mark as** from the top of the page and select a status.



- Mark a recommendation as **Dismissed** if you think the recommendation is irrelevant or the data is wrong.
 - In the panel that opens, select a dismissed reason so we can improve the service.
- Mark a recommendation as **Postponed** if you want to address the recommendation at a later time.
 - In the panel that opens, select a date within the next year to postpone the recommendation.
 - The recommendation becomes active when the selected date occurs.
- Mark a dismissed, postponed, or completed recommendation as **Active** to reassess the resources and resolve the issue.
- Recommendations change to **Completed** when all impacted resources were addressed.
 - If the service identifies an active resource for a completed recommendation the next time the service runs, the recommendation automatically changes back to **Active**.
 - Completing a recommendation is the only action collected in the audit log. To view these logs, go to **Microsoft Entra ID > Audit logs** and filter the service to "Microsoft Entra recommendations."

6. If you need to manually change the status of an impacted resource, select the checkbox for that resource in the **Impacted resources** table and select the status from the menu.

7. Continue to monitor the recommendations in your tenant for changes.

① Note

You can't manually mark a recommendation as completed. The system automatically marks a recommendation as completed when all impacted

resources are addressed. When the service runs, if no active resources are found, the recommendation is marked as completed.

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn about Service Health notifications](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra recommendation: Protect your tenant with Insider Risk condition in Conditional Access policy

Article • 04/09/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to protect your tenant by enabling the Insider Risk condition in Conditional Access paired with Microsoft Purview Adaptive Protection. This recommendation is called `insiderRiskPolicy` in the recommendations API in Microsoft Graph.

Description

Adaptive protection dynamically assigns appropriate Data Loss Prevention (DLP) policies to users based on the risk levels defined and analyzed by the machine learning models in insider risk management. With this new capability, static DLP policies become adaptive based on user context. The most effective policy, such as blocking data sharing, is applied only to high-risk users while low-risk users can maintain productivity.

These risk signals, when integrated with Conditional Access policies, allow Administrators to take appropriate actions for each risk level. Configuring Conditional Access policies with insider risk allows organizations to respond effectively to changing threat landscapes.

Value

Implementing a Conditional Access policy that blocks access to resources for high-risk internal users is of high priority due to its critical role in proactively enhancing security, mitigating insider threats, and safeguarding sensitive data in real-time.

Action plan

1. Enable [Adaptive Protection](#) in Microsoft Purview.
 - You must be a member of the Insider Risk Management or Insider Risk Management Admins role group in Microsoft Purview to configure Adaptive Protection.
 - For information, see [Roles and role groups for Microsoft Purview](#)
2. Create a [Conditional Access policy](#) that includes the Insider Risk condition.

- You must be signed in as a [Conditional Access Administrator](#) to view this template.
- For more information, see [Conditional Access conditions: Insider Risk](#).

Next steps

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)

Microsoft Entra recommendation: Migrate from the Azure Active Directory Authentication Library to the Microsoft Authentication Libraries

Article • 04/09/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to migrate from the Azure Active Directory Authentication Library (ADAL) to the Microsoft Authentication Libraries (MSAL). This recommendation is called `adalToMsalMigration` in the recommendations API in Microsoft Graph.

Description

The **Migrate from ADAL to MSAL** recommendation is created to raise awareness and alert you about all applications using ADAL within your tenant. This recommendation is triggered for tenants with applications using ADAL. It labels any application that requests a token via ADAL as an "ADAL application," including those applications using both ADAL and MSAL.

Azure Active Directory Authentication Library (ADAL) has been deprecated. We strongly recommend migrating to the Microsoft Authentication Library (MSAL), which replaces ADAL. Microsoft **no longer releases new features and security fixes on ADAL**. Applications using ADAL won't be able to utilize the latest security features, leaving them vulnerable to future security threats. If you have existing applications that use ADAL, be sure to [migrate them to MSAL](#).

How it works

The system checks daily for new ADAL token requests over the past 30 days. If an application makes no new requests for 30 days, the recommendation status is marked as completed. The overall recommendation status updates to "completed" once all applications meet this criterion. If a new ADAL request is detected for a previously completed application, the status reverts back to "active."

Value

MSAL is designed to enable a secure solution without developers having to worry about the implementation details. MSAL simplifies how tokens are acquired, managed, cached, and refreshed. MSAL also uses best practices for resilience. For more information on MSAL supported scenarios, see [Migrate applications to MSAL](#).

Action plan

To identify and get details of all applications in your tenant that are currently using ADAL, you can use Sign-ins Workbook. To get the list of all apps programmatically, you can also use Microsoft Graph API or the Microsoft Graph PowerShell SDK.

Sign-ins Workbook

The sign-ins Workbook in the Microsoft Entra admin center consolidates logs from various types of sign-in events, including interactive, non-interactive, and service principal sign-ins. This aggregation offers detailed insights into the usage of ADAL applications across your tenant to help you fully understand and manage migration of your ADAL applications. For a more detailed analysis and deeper investigation of ADAL app sign-in data, you can enable the [Microsoft Entra sign-ins workbook](#) in your tenant. This tool supports the migration by providing comprehensive sign-in data insights.

Frequently asked questions

Review the following common questions as you work on ADAL to MSAL migration.

Why does it take 30 days to change the status to completed?

To reduce false positives, the service uses a 30 day window for ADAL requests. This way, the service can go several days without an ADAL request and not be falsely marked as completed.

How do I identify the owner of an application in my tenant?

You can locate the owner from the recommendation details. Select the resource, which takes you to the application details. Go to **Manage > Owners** to view the current owners. Viewing the owners requires at least the [Application Administrator](#) role.

Can the status change from *completed* to *active*?

Yes. If an application was marked as completed - so no ADAL requests were made during the 30 day window - that application would be marked as complete. If the service detects a new ADAL request, the status changes back to *active*. The system updates the status to *active* or *completed*. This status can't be manually changed.

How can I integrate Microsoft Entra sign-ins workbook?

You can find the detailed steps in the [Microsoft Entra sign-ins workbook](#).

Why is the number of ADAL applications different in the sign-ins workbook and the recommendation?

- **Aggregated Data vs. Transactional Data:** The recommendation aggregates data over the last 30 days, providing a summarized view of application activities. Conversely, the sign-ins workbook details each sign-in request as a transaction, which allows for a more detailed analysis.
- **Time Frame Flexibility:** The sign-ins workbook data can be filtered from as recently as the last 30 minutes to up to 30 days. This flexibility in selecting the time frame can lead to variations in the application count, potentially skewing the results.
- **Access to Historical Data:** Viewing data older than 7 days in the sign-ins workbook requires a Microsoft Entra ID P1 or P2 tenant subscription. This requirement affects the volume of historical data accessible compared to the aggregated data in the recommendation.

Related content

- [Get a list of apps using ADAL in your tenant](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)

Microsoft Entra recommendation: Migrate apps from ADFS to Microsoft Entra ID

Article • 04/09/2025

[Microsoft Entra recommendations](#) provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to migrate apps from Active Directory Federated Services (AD FS) to Microsoft Entra ID. This recommendation is called `adfsAppsMigration` in the recommendations API in Microsoft Graph.

Description

As an admin responsible for managing applications, you want your applications to use the security features of Microsoft Entra ID and maximize their value. This recommendation shows up if your tenant has apps on ADFS that can 100% be migrated to Microsoft Entra ID. For more information, see [Understand the stages of migrating application authentication from AD FS to Microsoft Entra ID](#).

Value

Using Microsoft Entra ID gives you granular per-application access controls to secure access to applications. With Microsoft Entra B2B collaboration, you can increase user productivity. Automated app provisioning automates the user identity lifecycle in cloud SaaS apps such as Dropbox, Salesforce, and more.

Action plan

1. [Install Microsoft Entra Connect](#) on your AD FS server.
2. [Review the AD FS application activity report](#) to get insights about your AD FS applications.
3. Read the solution guide for [migrating applications to Microsoft Entra ID](#).
4. Migrate applications to Microsoft Entra ID. For more information, see the article [Migrate from federation to cloud authentication](#).

Guided walkthrough

For a guided walkthrough of many of the recommendations in this article, see the migration guide [Migrate from AD FS to Microsoft Entra ID for identity management](#) when signed in to

the Microsoft 365 admin center. To review best practices without signing in and activating automated setup features, go to the [Microsoft 365 Setup portal](#).

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)

Microsoft Entra recommendation: Migrate from Azure AD Graph APIs to Microsoft Graph

Article • 04/09/2025

[Microsoft Entra recommendations](#) provide you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers two recommendations to migrate applications and service principals from Azure AD Graph APIs to Microsoft Graph. These recommendations are called `aadGraphDeprecationApplication` and `aadGraphDeprecationServicePrincipal` in the recommendations API in Microsoft Graph.

Description

The deprecation of Azure Active Directory (Azure AD) Graph APIs was announced in 2020 and are now in the retirement cycle. All applications and service principals need to migrate to the new Microsoft Graph APIs.

In general, applications and service principals that are still using Azure AD Graph APIs were developed by your organization or a vendor. These applications likely need to be updated by your developers or upgraded to a new version.

There are two recommendations associated with the deprecation of Azure AD Graph. One provides a list of applications and one provides a list of service principals. Both recommendations need to be addressed separately.

Applications and Service Principals

The Applications version of this recommendation details applications that are registered in your tenant and calling Azure AD Graph APIs. Think, app registrations in the Microsoft Entra admin center.

The Service Principals version of this recommendation details applications that are registered in another tenant, but consented for use in your tenant. Think, enterprise applications in the Microsoft Entra admin center. These applications could be supplied by a developer in your multitenant company or a software vendor. For Service Principals, you likely need to contact the vendor to identify how to get an update to a newer version of the application.

Value

Microsoft Graph offers a single unified endpoint to access Microsoft Entra and Microsoft 365 services. Microsoft Graph APIs have all the capabilities of Azure AD Graph APIs, plus many newer API features. The Microsoft Graph client libraries offer built-in support for features, such as retry handling, secure redirects, transparent authentication, and payload compression. These capabilities weren't available with Azure AD Graph.

Any applications or service principals still calling Azure AD Graph will be affected by future retirement activity. To prevent loss of functionality, we recommend migrating to Microsoft Graph.

Action plan

Both of the recommendations include a list of impacted resources. The process to review and update applications and service principals are similar.

1. Review the list of **applications** and **service principals** calling Azure AD Graph under **Impacted Resources** in the recommendations details.
2. Select the **More Details** link to view the following details about the Azure AD Graph API activity.

Impacted resources					
<input type="checkbox"/> Mark as ▼					
<input type="checkbox"/> Search by ID Show dates as: Local <input type="checkbox"/> Reset filters					
1 resource found					
<input type="checkbox"/> Resource	ID	First detected	Status	Actions	
<input type="checkbox"/> TestApp	000-11111-aaaaa-bbbb	Feb 6, 2024, 7:02 PM	Active	More Details	

- **Operation Name:** Description of the API operation, such as List Application, Create User, or Delete Group
- **Requests - 30 Days:** The number of requests made by this application in the last 30 days
- **Last Request Date:** The date and time the operation was last performed by the operation.

Additional Details

X

The list below provides information about the top Azure AD Graph operations that this application is using, including the number of successful requests for that operation in the past 30 days and the last time it performed that operation.

Resource

TestApp 

Operation Name	Requests - 30 Days	Last Request Date
List Application	1	Feb 4, 2024, 2:54 AM
List User	8	Feb 4, 2024, 2:54 AM
List Group	1	Feb 4, 2024, 2:54 AM

[Close](#)

3. Work with the owner or publisher of the corresponding application to identify the steps required to update the application.

These recommendations show as **Active** until there is no Azure AD Graph API activity for 30 days. After 30 days of no Azure AD Graph API activity, that application or service principal is marked as **Completed**. Once all resources are addressed, the recommendation is marked as **Completed**.

Related content

- [Migrate your apps](#)
- [Migration planning checklist](#)
- [Migration FAQs](#)

Microsoft Entra recommendation: Migrate from MFA server to Microsoft Entra multifactor authentication (MFA)

Article • 04/10/2025

[Microsoft Entra recommendations](#) provide you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to migrate from MFA server to Microsoft Entra MFA. This recommendation is called `mfaServerDeprecation` in the recommendations API in Microsoft Graph.

Description

Azure Multi-Factor Authentication Server (MFA Server) was scheduled for retirement on September 30th, 2024. To help organizations migrate to Microsoft Entra MFA, this Microsoft Entra recommendation identifies tenants with MFA server activity. This recommendation identifies tenants with active users and MFA attempts for MFA Server in the last seven days. MFA Server client integrations, including a list of affected clients are also surfaced as a part of this recommendation.

Value

MFA Server is a component for deploying and managing MFA on-premises. In 2019, Microsoft stopped allowing new deployments of MFA Server and investing in feature enhancements. In September 2022, [Microsoft formally announced the deprecation of MFA Server](#).

Cloud-based, Microsoft Entra multifactor authentication offers better resiliency, availability, and data compliancy. Migrating to Microsoft Entra MFA helps you improve your security posture by giving you access to the latest phishing-resistant authentication methods and more fine-grained access controls. It also helps reduce cost and deployment complexity by no longer having to maintain an on-premises component.

Action plan

1. [Learn how to migrate MFA Server to Microsoft Entra MFA](#).
2. Migrate MFA user information from on-premises to Microsoft Entra.

- You can either migrate this information manually or use the MFA Server Migration Utility (recommended).
- [How to use the MFA Server Migration Utility](#).

3. Use [Staged Rollout](#) to reroute users to authenticate against Microsoft Entra instead of MFA Server.
4. Identify and migrate any MFA Server dependencies, such as applications using [RADIUS](#) or [LDAP authentication](#).
5. Update domain federation settings and decommission MFA Server.

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)

Microsoft Entra recommendation: Migrate to Microsoft Authenticator (preview)

Article • 04/09/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to migrate users to the Microsoft Authenticator app, which is currently a preview recommendation. This recommendation is called `useAuthenticatorApp` in the recommendations API in Microsoft Graph.

Description

Multifactor authentication (MFA) is a key component to improve the security posture of your Microsoft Entra tenant. While SMS text and voice calls were once commonly used for multifactor authentication, they're becoming increasingly less secure. You also don't want to overwhelm your users with lots of MFA methods and messages.

One way to ease the burden on your users is to migrate anyone using SMS or voice call for MFA to use the Microsoft Authenticator app. This strategy also increases the security of their authentication methods.

This recommendation appears if Microsoft Entra ID detects that your tenant has users authenticating using SMS or voice instead of the Microsoft Authenticator app in the past week.

Value

Push notifications through the Microsoft Authenticator app provide the least intrusive MFA experience for users. This method is the most reliable and secure option because it relies on a data connection rather than telephony.

The verification code option enables MFA even in isolated environments without data or cellular signals, where SMS and Voice calls might not work.

The Microsoft Authenticator app is available for Android and iOS. Microsoft Authenticator can serve as a traditional MFA factor (one-time passcodes, push notification) and when your organization is ready for Password-less, the Microsoft Authenticator app can be used to sign in to Microsoft Entra ID without a password.

Action plan

1. Ensure that notification through mobile app and/or verification code from mobile app are available to users as authentication methods. How to Configure Verification Options
2. Educate users on how to add a work or school account.

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)

Microsoft Entra recommendation: Switch from per-user MFA to Conditional Access MFA

Article • 02/23/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to switch per-user multifactor authentication (MFA) accounts to Conditional Access MFA accounts. This recommendation is called `switchFromPerUserMFA` in the recommendations API in Microsoft Graph.

Description

As an admin, you want to maintain security for your company's resources, but you also want your employees to easily access resources as needed. MFA enables you to enhance the security posture of your tenant.

In your tenant, you can enable MFA on a per-user basis. In this scenario, your users perform MFA each time they sign in. There are some exceptions, such as when they sign in from trusted IP addresses or when the "remember MFA on trusted devices" feature is turned on. While enabling MFA is a good practice, switching per-user MFA to MFA based on [Conditional Access](#) can reduce the number of times your users are prompted for MFA.

This recommendation shows up if:

- You have per-user MFA configured for at least 5% of your users.
- Conditional Access policies are active for more than 1% of your users (indicating familiarity with Conditional Access policies).

Value

This recommendation improves your user's productivity and minimizes the sign-in time with fewer MFA prompts. Conditional Access and MFA used together help ensure that your most sensitive resources can have the tightest controls, while your least sensitive resources can be more freely accessible. For an overview of available functionality in Conditional Access, see [Building a Conditional Access policy](#).

Action plan

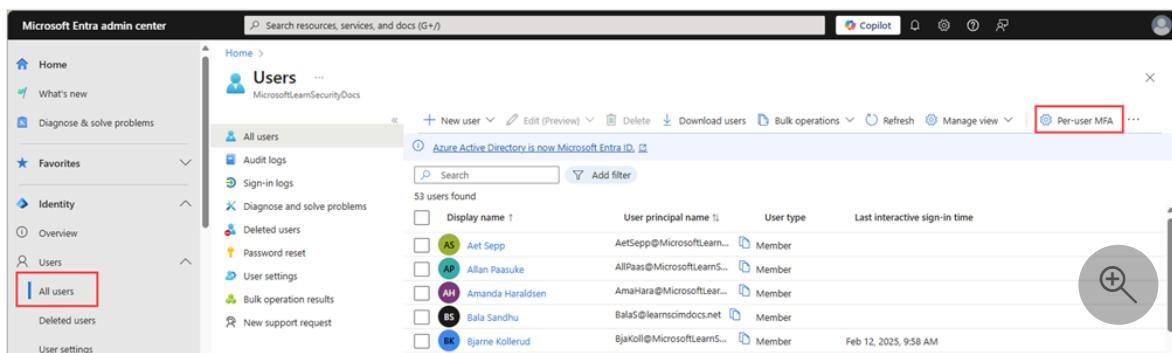
1. Require MFA using a Conditional Access policy.

- [Enable Microsoft Entra multifactor authentication with Conditional Access](#).
- Ensure that you're covering all resources and users you would like to secure with MFA.

2. Ensure that the per-user MFA configuration is turned off.

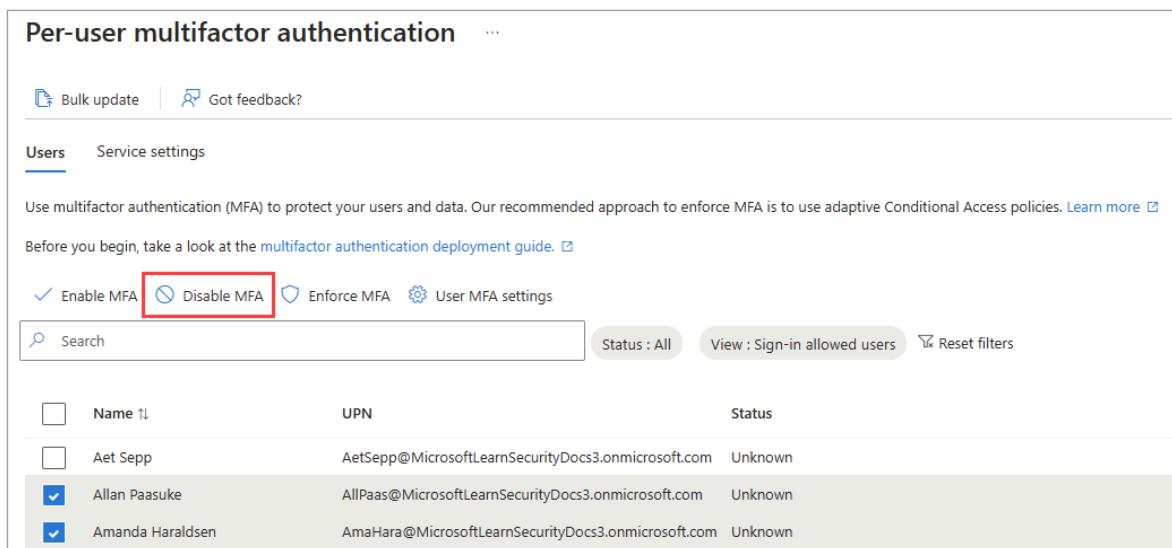
a. Sign in to the [Microsoft Entra admin center](#) as at least an [Authentication Policy Administrator](#).

b. Browse to **Users > All users** and select the **Per-user MFA** button.



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with options like Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users (with 'All users' selected), Deleted users, and User settings. The main area is titled 'Users' and shows a list of 53 users found. The columns include Display name, User principal name, User type, and Last interactive sign-in time. Each user entry has a small profile icon and a blue 'Member' badge. At the top right of the main area, there's a toolbar with various icons and a search bar. A red box highlights the 'Per-user MFA' button in the top right corner of the toolbar.

a. Select **Disable MFA** for all users who had this option enabled.



The screenshot shows the 'Per-user multifactor authentication' page. At the top, there are buttons for Bulk update and Got feedback?. Below that, there are tabs for Users (which is selected) and Service settings. A message encourages using multifactor authentication (MFA) to protect users and data, mentioning adaptive Conditional Access policies. It also links to a deployment guide. Below the message, there are four buttons: Enable MFA (checked), Disable MFA (highlighted with a red box), Enforce MFA, and User MFA settings. There are also filters for Search, Status (All), View (Sign-in allowed users), and Reset filters. The main table lists users with their names, UPN, and status. Three users have checkboxes next to their names: Aet Sepp, Allan Paasuke, and Amanda Haraldsen. Allan Paasuke and Amanda Haraldsen have checkboxes checked, while Aet Sepp does not.

Name	UPN	Status
Aet Sepp	AetSepp@MicrosoftLearnSecurityDocs3.onmicrosoft.com	Unknown
Allan Paasuke	AllPaas@MicrosoftLearnSecurityDocs3.onmicrosoft.com	Unknown
Amanda Haraldsen	AmaHara@MicrosoftLearnSecurityDocs3.onmicrosoft.com	Unknown

After all users are migrated to Conditional Access MFA accounts, the recommendation status automatically updates the next time the service runs. Continue to review your Conditional Access policies.

Related content

- [How to use Microsoft Entra recommendations](#)
- [Microsoft Graph API for recommendations](#)

- MFA and Conditional Access policy
 - MFA and Conditional Access policy tutorial
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Microsoft Entra recommendation: Minimize MFA prompts from known devices

Article • 04/10/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to minimize multifactor authentication prompts from known devices. This recommendation is called `tenantMFA` in the recommendations API in Microsoft Graph.

Description

As an admin, you want to maintain security for your company's resources, but you also want your employees to easily access resources as needed. While enabling MFA is a good practice, you should try to keep the number of MFA prompts your users have to go through at a minimum. One option you have to accomplish this goal is to **allow users to remember multifactor authentication on trusted devices**.

The *remember multifactor authentication on trusted device* feature sets a persistent cookie on the browser when a user selects the *Don't ask again for X days* option at sign-in. The user isn't prompted again for MFA from that browser until the cookie expires. If the user opens a different browser on the same device or clears the cookies, they're prompted again to verify.

For more information, see [Configure Microsoft Entra multifactor authentication settings](#).

This recommendation shows up if the **remember multifactor authentication** feature is set to less than 30 days.

Value

This recommendation improves your user's productivity and minimizes the sign-in time with fewer MFA prompts. Ensure that your most sensitive resources can have the tightest controls, while your least sensitive resources can be more freely accessible.

Action plan

1. Review the [How to configure Microsoft Entra multifactor authentication settings](#) article.
2. Sign in to the [Microsoft Entra admin center](#) as at least an [Authentication Policy Administrator](#).

3. Browse to Protection > Multifactor authentication.
4. Under the Configure heading, select the Additional cloud-based multifactor authentication settings link.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various categories like Home, What's new, Diagnose & solve problems, Favorites, Identity, Protection, and Multifactor authentication. The 'Multifactor authentication' item is selected and highlighted with a red box. The main content area is titled 'Multifactor authentication | Getting started'. It contains sections for 'Getting started', 'Configure', and 'Learn more'. The 'Configure' section specifically highlights the 'Additional cloud-based multifactor authentication settings' link, which is also enclosed in a red box.

5. Select the Service settings tab.

The screenshot shows the 'Per-user multifactor authentication' page in the Microsoft Entra admin center. The top navigation bar includes 'Multifactor authentication | Getting started'. The main content area is titled 'Per-user multifactor authentication'. It features tabs for 'Users' (selected) and 'Service settings' (highlighted with a red box). Below these tabs, there's a brief description about using MFA to protect users and data, followed by a link to the deployment guide. At the bottom, there are several configuration options: 'Enable MFA', 'Disable MFA', 'Enforce MFA', and 'User MFA settings'. A search bar and filter buttons for 'Status : All', 'View : Sign-in allowed users', and 'Reset filters' are also present.

6. Under the Remember multifactor authentication on trusted device heading, select the checkbox, and set the number of days to 90.

Per-user multifactor authentication

X

 Bulk update

 Got feedback?

Users **Service settings**

App passwords [Learn more](#)

- Allow users to create app passwords to sign in to non-browser apps
 Do not allow users to create app passwords to sign in to non-browser apps

Trusted IPs [Learn more](#)

Skip multifactor authentication for requests from federated users on my intranet

Skip multifactor authentication for requests from following range of IP address subnets:

Enter IP address

Verification options [Learn more](#)

-  These methods are now being managed in the authentication methods policy. Go there to manage methods used for authentication and password reset [authentication methods policy](#).

Remember multifactor authentication on trusted device [Learn more](#)

Allow users to remember multifactor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for

90

For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. [Learn more about reauthentication prompts](#).

Save

Discard

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)

Microsoft Entra recommendation: Remove unused applications (preview)

Article • 04/10/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to investigate unused applications. This recommendation is called `staleApps` in the recommendations API in Microsoft Graph.

ⓘ Note

With [Microsoft Security Copilot](#), you can use natural language prompts to get insights on unused applications. Learn more about how to [Assess application risks using Microsoft Security Copilot](#).

Prerequisites

There are different role requirements for viewing or updating a recommendation. Use the least-privileged role for the type of access needed. For a full list of roles, see [Least privileged roles by task](#).

[] Expand table

Microsoft Entra role	Access type
Reports Reader	Read-only
Security Reader	Read-only
Global Reader	Read-only
Authentication Policy Administrator	Update and read
Exchange Administrator	Update and read
Security Administrator	Update and read
DirectoryRecommendations.Read.All	Read-only in Microsoft Graph
DirectoryRecommendations.ReadWrite.All	Update and read in Microsoft Graph

Some recommendations might require a P2 or other license. For more information, see the [Recommendations overview table](#).

Description

This recommendation shows up if your tenant has applications that haven't been used for over 90 days. The following scenarios are included in this recommendation:

- The app was created but never used.
- The app isn't **soft deleted** from the application portfolio.
- The app isn't used by the tenant where it resides nor any of its instances (Service Principal) in other tenants.
- It's a client app that calls other resource apps, but hasn't been issued any tokens in the past 90 days.
- It's a resource app that doesn't have a record of any client apps requesting a token in the past 90 days.

The following apps are exempted from this recommendation:

- Apps that are managed by Microsoft, including anything created or modified by Microsoft-owned applications.
- Apps that work with other apps to obtain tokens or are used to enable scenarios that don't require tokens.
 - For example, [Peer-to-peer server](#), [Application proxy](#), [Microsoft Entra Cloud Sync](#), [linked single-sign-on](#), [password SSO](#), [Office add-ins](#), and [managed identities](#) are excluded from this recommendation.
- Apps that were created within the past 90 days.

Value

Removing unused applications helps reduce the attack surface area and helps clean up the app portfolio of a tenant.

Action plan

This recommendation is available in the Microsoft Entra admin center and using the Microsoft Graph API. Once you identify the applications that aren't being used, you can decide whether to remove them or keep them based on your organization's needs. The action plan is therefore broken down into two parts:

1. Review the applications that are flagged as unused.
2. Determine if the application is needed and how to address it.

Applications identified by the recommendation appear in the list of **Impacted resources** at the bottom of the recommendation.

Review the applications

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.
2. Browse to **Identity > Overview**.
3. Select the **Recommendations** tab and select the **Remove unused applications** recommendation.
4. From the **Impacted resources** table, select **More details** to view more details.
5. Select the **Resource** link to go directly to the app registration for the app.
 - Alternatively, you can browse to **Identity > Applications > App registrations** and locate the application that was surfaced as part of this recommendation.

Display name	Application (client) ID	Created on	Certificates & secrets
AN	00001111-aaaa-2222-bbbb-3333cccc4444	5/22/2024	-
CL	11112222-bbbb-3333-cccc-4444ddd5555	6/4/2023	Current
SA	55556666-ffff-7777-aaaa-8888bbbb9999	3/25/2023	-

Determine if the application is needed

There are many reasons why an app might be unused. Consider the app's usage scenario and business function. For example:

- Was the app deprecated?
- Is the app used for a business function that only happens at certain times of the year?

To remove the application:

1. [Soft delete](#) the app from your tenant.
2. Wait 15 days and then [permanently delete the app](#).

To indicate the application is still needed and skip the recommendation:

- [Update the recommendation status](#) to **dismissed** or **postponed**.
 - Use **dismissed** if determined that the app will remain inactive for the rest of its lifecycle.
 - Use **dismissed** if you think the app was included in the recommendation in error.
 - Use **postponed** if you need more time to review the app.

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)

Microsoft Entra recommendation: Remove unused credentials from apps (preview)

Article • 04/09/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to remove unused credentials from apps. This recommendation is called `staleAppCreds` in the recommendations API in Microsoft Graph.

Prerequisites

There are different role requirements for viewing or updating a recommendation. Use the least-privileged role for the type of access needed. For a full list of roles, see [Least privileged roles by task](#).

[] Expand table

Microsoft Entra role	Access type
Reports Reader	Read-only
Security Reader	Read-only
Global Reader	Read-only
Authentication Policy Administrator	Update and read
Exchange Administrator	Update and read
Security Administrator	Update and read
<code>DirectoryRecommendations.Read.All</code>	Read-only in Microsoft Graph
<code>DirectoryRecommendations.ReadWrite.All</code>	Update and read in Microsoft Graph

Some recommendations might require a P2 or other license. For more information, see the [Recommendations overview table](#).

Description

Application credentials can include certificates and other types of secrets that need to be registered with that application. These credentials are used to prove the identity of the

application. Only credentials actively in use by an application should remain registered with the application.

A credential is considered unused if:

- It has not been used in the past 30 days.
- It's a credential that was added to an application to be used for OAuth/OIDC flows or to the service principal for SAML flow.

The following credentials are exempted from the recommendation:

- Expired credentials do not show in the **Impacted resources** list.
- Credentials that were identified as unused but have expired since being flagged show as **Completed** in the **Impacted resources** list.

Value

Removing unused application credentials helps reduce the attack surface area and helps declutter the app portfolio of a tenant.

Action plan

This recommendation is available in the Microsoft Entra admin center and using the Microsoft Graph API.

Microsoft Entra admin center

Applications that the recommendation identified appear in the list of **Impacted resources** at the bottom of the recommendation.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.
2. Browse to **Identity > Overview**.
3. Select the **Recommendations** tab and select the **Remove unused credentials from applications** recommendation.
4. Take note of the following details from the **Impacted resources** table.
 - The **Resource** column displays the application name
 - The **ID** column displays the application ID
5. Select **More Details** from the **Actions** column to view more details.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has sections like Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Protection, Identity Governance, External Identities, Show more, Protection, Identity Governance, Verified ID, Permissions Management, and Global Secure Access. The main content area is titled "Remove unused credentials from applications". It shows a table with one row: Status (Active), Priority (Medium), and Impacted resource type (Applications). Below this is a "Status description" section stating "Marked as active by system on 7/22/2024 at 8 AM PDT." A "Description" section notes that the tenant has applications with credentials not used in over 30 days. A "Value" section explains the risk of compromised credentials. An "Action plan" section lists three steps: 1. Navigate to the app registration section. 2. Find the credential and remove it. 3. Use the MS Graph Service Principal API service action 'removePassword'. The "Impacted resources" section shows a table with three rows: Splunk (ID: 22223333-cccc-4444-dddd-5555eeee6666, First detected: Jul 22, 2024, 9:58 AM, Status: Active) and SharePoint Version Info App (ID: 44445555-eeee-6666-ffff-7777aaaa8888, First detected: Jul 22, 2024, 9:58 AM, Status: Active). The "Actions" column for the Splunk row has a "More Details" link, which is highlighted with a red box and a magnifying glass icon.

Status	Priority	Impacted resource type
Active	Medium	Applications

Status description
Marked as active by system on 7/22/2024 at 8 AM PDT.

Description
Your tenant has applications with credentials which have not been used in more than 30 days. Hence, they are flagged as unused.

Value
An application credential is used to get a token that grants access to a resource or another service. If an application credential is compromised, it could be used to access sensitive resources or allow a bad actor to move latterly depending on the access granted to the application. Removing credentials not actively used by applications improves security posture and promotes app hygiene. It reduces the risk of application compromise and improves the security posture of the application by reducing the attack surface for credential misuse by discovery.

Action plan

1. For application resources, navigate to the app registration section in your tenant.
2. In the 'Certificates and secrets' blade, find the credential and remove it.
3. To remove a credential from a service principal resource, use the MS Graph Service Principal API service action 'removePassword'

Impacted resources

Resource	ID	First detected	Status	Actions
Splunk	22223333-cccc-4444-dddd-5555eeee6666	Jul 22, 2024, 9:58 AM	Active	More Details
SharePoint Version Info App	44445555-eeee-6666-ffff-7777aaaa8888	Jul 22, 2024, 9:58 AM	Active	More Details

⚠ Note

If the origin of the credential is Service Principal, follow the guidance in the [Service principals](#) section.

- From the panel that opens, select **Update Credential** to navigate directly to the **Certificates & secrets** area of the app registration to remove the unused credential.
 - Alternatively, browse to **Identity > Applications > App registrations** and select the application that was surfaced as part of this recommendation.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various sections like Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices, and Applications. The 'Applications' section is highlighted with a red box. Under Applications, there are sub-sections for Enterprise applications, App registrations, Roles & admins, and Protection. The 'App registrations' section is also highlighted with a red box. The main content area is titled 'App registrations' and shows a list of 14 applications found. The columns are Display name, Application (client) ID, Created on, and Certificates & secrets. The applications listed are: AN (Android native), Cloudflare, and Salesforce.

Display name	Application (client) ID	Created on	Certificates & secrets
AN	00001111-aaaa-2222-bbbb-3333cccc4444	5/22/2024	-
Cloudflare	11112222-bbbb-3333-cccc-4444dddd5555	6/4/2023	Current
Salesforce	55556666-ffff-7777-aaaa-8888bbbb9999	3/25/2023	-

b. Then navigate to the Certificates & Secrets section of the app registration.

The screenshot shows the 'Application | Certificates & secrets' page. The left sidebar has sections for Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage (with sub-options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest), and a search bar. The 'Certificates & secrets' option is selected and highlighted with a red box. The main content area has a note: 'Some actions may be disabled due to your permissions. To request access, contact the application owner(s) or your administrator. View application owners or administrators.' Below this, it says: 'Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.' A callout box provides more details about Client secrets, stating: 'Application registration certificates, secrets and federated credentials can be found in the tabs below.' It shows a table for Client secrets with one entry: 'Secret for Application' (Description), '10/18/2025' (Expires), '*****' (Value), and 'ccccccc-2d2d-3e3e-4f4f...' (Secret ID).

Description	Expires	Value	Secret ID
Secret for Application	10/18/2025	*****	ccccccc-2d2d-3e3e-4f4f...

7. Locate the unused credential and remove it.

Service principals

If the origin of the credential is **service principal**, there are a few considerations and extra steps to follow.

Because there's often multiple service principals for a single application, it might be easier to navigate to Enterprise apps to view everything in one place.

1. In the [Microsoft Entra admin center](#), browse to **Identity > Applications > Enterprise applications**.
2. Search for and open the application that was surfaced as part of this recommendation.
3. Select **Single sign-on** from the side menu.

If the credential is a service principal but there are SAML certificates in use, you can identify the details of the credential using the Microsoft Graph API. To use the Microsoft Graph API, you need the `DirectoryRecommendations.Read.All` and `DirectoryRecommendations.ReadWrite.All` permissions. For more information, see [How to use Identity Recommendations](#).

4. Sign in to [Graph Explorer](#).
5. Select **GET** as the HTTP method from the dropdown.
6. Set the API version to **beta**.
7. Query the `keyCredential` and `passwordCredential` endpoints.
8. Use the `removePassword` or `removeKey` endpoints to remove the credential from the service principal.

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)
- [Learn about app and service principal objects in Microsoft Entra ID](#)

Microsoft Entra recommendation: Renew expiring application credentials (preview)

Article • 04/09/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to renew expiring application credentials. This recommendation is called `applicationCredentialExpiry` in the recommendations API in Microsoft Graph.

Prerequisites

There are different role requirements for viewing or updating a recommendation. Use the least-privileged role for the type of access needed. For a full list of roles, see [Least privileged roles by task](#).

 Expand table

Microsoft Entra role	Access type
Reports Reader	Read-only
Security Reader	Read-only
Global Reader	Read-only
Authentication Policy Administrator	Update and read
Exchange Administrator	Update and read
Security Administrator	Update and read
<code>DirectoryRecommendations.Read.All</code>	Read-only in Microsoft Graph
<code>DirectoryRecommendations.ReadWrite.All</code>	Update and read in Microsoft Graph

Some recommendations might require a P2 or other license. For more information, see the [Recommendations overview table](#).

Description

Application credentials can include certificates and other types of secrets that need to be registered with that application. These credentials are used to prove the identity of the

application.

This recommendation shows up if your tenant has application credentials that will expire soon.

An application credential is expiring if:

- It's on an application registration AND is expiring within the next 30 days.

The following credentials are exempted from this recommendation:

- Credentials that were identified as expiring but have since been removed from the app registration
- Credentials whose expiration date has lapsed show as **completed** in the list of **Impacted resources**.

Value

Renewing an application's credentials prior to their expiry date is crucial for maintaining uninterrupted operations and minimizing the risk of any downtime resulting from outdated credentials.

Action plan

This recommendation is available in the Microsoft Entra admin center and using the Microsoft Graph API.

Microsoft Entra admin center

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.
2. Browse to **Identity > Overview**.
3. Select the **Recommendations** tab and select the **Renew expiring application credentials** recommendation.
4. Take note of the following details from the **Impacted resources** table.
 - The **Resource** column displays the application name
 - The **ID** column displays the application ID

Microsoft Entra admin center

... > Woodgrove > Remove unused credentials from applications > App registrations > Splunk | Certificates & secrets > Woodgrove > Renew expiring application credentials ...

Value
Renewing the app credential(s) before its expiration ensures the application continues to function and reduces the possibility of downtime due to an expired credential.

Action plan
1. Navigate to the App registration section and locate the application for which the credential needs to be rotated.
2. Navigate to the "Certificates & Secrets" blade of the app registration.
3. Pick the credential type that you want to rotate and navigate to either "Certificates" or "Client Secret" tab and follow the prompts.
4. Once the certificate or secret is successfully added, update the service code to ensure it works with the new credential and has no negative customer impact. You should use Microsoft Entra ID's sign-in logs to validate that the thumbprint of the certificate matches the one that was just uploaded.
5. After validating the new credential, navigate back to the Certificates and Secrets blade for the app and remove the old credential.

Impacted resources

Resource	ID	First detected	Status
Contoso Chat Bot	aaaaaaaa-6666-7777-8888-bbbbbbb...	Aug 3, 2024, 5:04 AM	Active
Contoso Sales Tracker	ccccccc-8888-9999-0000-ddddd...	Aug 3, 2024, 5:04 AM	Active

Actions More Details

5. Select **More Details** from the **Actions** column.

6. From the panel that opens, select **Update Credential** to navigate directly to the **Certificates & secrets** area of the app registration to renew the expiring credential.
a. Alternatively, browse to **Identity > Applications > App registrations** and locate the application for which the credential needs to be rotated.

Microsoft Entra admin center

... > My roles | Microsoft Entra roles > Contoso > Remove unused credentials from applications > App registrations

New registration Endpoints Troubleshoot Refresh Download Preview features ...

All applications Owned applications Deleted applications

Start typing a display name or application (client) ID to filter these results Add filters

14 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
AN	00001111-aaaa-2222-bbbb-3333cccc4444	5/22/2024	-
cl	11112222-bbbb-3333-cccc-4444dddd5555	6/4/2023	Current
SA	55556666-ffff-7777-aaaa-8888bbbb9999	3/25/2023	-

Actions

a. Navigate to the **Certificates & Secrets** section of the app registration.

7. Pick the credential type that you want to rotate and navigate to either **Certificates** or **Client Secret** tab and follow the prompts.

The screenshot shows the Microsoft Entra ID portal with the URL: https://entra.microsoft.com/~/#/registrations/applications/Woodgrove/certificates-secrets. The left sidebar has a 'Manage' section with various options like Overview, Quickstart, Integration assistant, Diagnose and solve problems, and Certificates & secrets (which is selected). A message at the top right says: 'Some actions may be disabled due to your permissions. To request access, contact the application owner(s) or your administrator. View application owners or administrators.' Below this, a note about credentials is displayed. A modal window titled 'Client secrets (1)' is open, showing a table with one row: 'Secret for Application' (Description), '10/18/2025' (Expires), '*****' (Value), and 'ccccccc-2d2d-3e3e-4f4f...' (Secret ID). There is a '+' button to add a new secret.

8. Once the certificate or secret is successfully added, update the service code to ensure it works with the new credential and doesn't negatively affect customers.
9. Use the Microsoft Entra sign-in logs to validate that the Key ID of the credential matches the one that was recently added.
10. After validating the new credential, navigate back to **App registrations > Certificates and Secrets** for the app and remove the old credential.

Related content

- [Review the Microsoft Entra recommendations overview](#)
- [Learn how to use Microsoft Entra recommendations](#)
- [Explore the Microsoft Graph API properties for recommendations](#)
- [Learn about app and service principal objects in Microsoft Entra ID](#)

Microsoft Entra recommendation: Renew expiring service principal credentials (preview)

Article • 04/09/2025

[Microsoft Entra recommendations](#) is a feature that provides you with personalized insights and actionable guidance to align your tenant with recommended best practices.

This article covers the recommendation to renew expiring service principal credentials. This recommendation is called `servicePrincipalKeyExpiry` in the recommendations API in Microsoft Graph.

Prerequisites

There are different role requirements for viewing or updating a recommendation. Use the least-privileged role for the type of access needed. For a full list of roles, see [Least privileged roles by task](#).

[] Expand table

Microsoft Entra role	Access type
Reports Reader	Read-only
Security Reader	Read-only
Global Reader	Read-only
Authentication Policy Administrator	Update and read
Exchange Administrator	Update and read
Security Administrator	Update and read
<code>DirectoryRecommendations.Read.All</code>	Read-only in Microsoft Graph
<code>DirectoryRecommendations.ReadWrite.All</code>	Update and read in Microsoft Graph

Some recommendations might require a P2 or other license. For more information, see the [Recommendations overview table](#).

Description

Service principal credentials include certificates and client secrets added to a service principal. The credentials are used to prove the identity of that service principal. If the credentials expire, the service principal can't authenticate, which can cause downtime for your business scenario. This recommendation shows up if your tenant has service principals with credentials that are expiring soon.

A service principal credential is expiring if:

- It's on a service principal AND is expiring within the next 30 days.

The following credentials are exempted from this recommendation:

- Credentials that were identified as expiring but have since been removed from the application registration.
- Credentials whose expiration date has lapsed show as **completed** in the list of **Impacted resources**.

Value

Renewing a service principal's credentials prior to their expiry date is crucial for maintaining uninterrupted operations and minimizing the risk of any downtime resulting from outdated credentials.

Action plan

This recommendation is available in the Microsoft Entra admin center and using the Microsoft Graph API.

Microsoft Entra admin center

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.
2. Browse to **Identity > Overview**.
3. Select the **Recommendations** tab and select the **Renew expiring service principal credentials** recommendation.
4. Select **More Details** from the **Actions** column.
5. From the panel that opens, select **Update Credential** to navigate directly to the **Single sign-on** area of the app registration.

- a. Alternatively, browse to **Identity > Applications > App registrations** and locate the application for which the credential needs to be rotated.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, What's new, Diagnose & solve problems, Favorites, Identity (which is expanded), Overview, Users, Groups, Devices, Applications (which is selected and highlighted with a red box), Enterprise applications (which is collapsed), App registrations (which is selected and highlighted with a red box), Roles & admins, and Protection. The main content area is titled "App registrations" and shows a list of 14 applications found. The columns are Display name, Application (client) ID, Created on, and Certificates & secrets. The applications listed are: AN (Android native), CL (Cloudflare), and SA (Salesforce). The Cloudflare entry has a green checkmark next to "Certificates & secrets". A search bar at the top says "Start typing a display name or application (client) ID to filter these r..." and a "Add filters" button. There are also buttons for New registration, Endpoints, Troubleshoot, Refresh, Download, Preview features, and a three-dot menu.

Display name	Application (client) ID	Created on	Certificates & secrets
AN	00001111-aaaa-2222-bbbb-3333cccc4444	5/22/2024	-
CL	11112222-bbbb-3333-cccc-4444dddd5555	6/4/2023	Current
SA	55556666-ffff-7777-aaaa-8888bbbb9999	3/25/2023	-

- a. Navigate to the **Single sign-on** section of the app registration.
6. Edit the **SAML signing certificate** section and follow the prompts to add a new certificate.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is expanded to show the 'Applications' section under 'Identity'. Within 'Applications', 'Enterprise applications' is selected, and 'Single sign-on' is highlighted. The main content area displays the 'Zscaler | SAML-based Sign-on' configuration page. It includes sections for 'Basic SAML Configuration', 'Attributes & Claims', and 'SAML Certificates'. A numbered callout (1) points to the 'Basic SAML Configuration' section, (2) to the 'Attributes & Claims' section, and (3) to the 'SAML Certificates' section. The 'Edit' button for the certificate in the SAML Certificates section is highlighted with a red box.

7. Once the certificate or secret is successfully added, update the SAML signing certificate configuration to make the new cert active.

8. Verify that the application works as expected then remove the inactive SAML certificate from the SAML certificates collection.

! Note

If you don't have any SAML credentials configured but you received this recommendation, use the Microsoft Graph [ServicePrincipalAPI](#) endpoint to check the `keyCredentials` and `passwordCredentials` properties of the service principal object. Locate and rotate the credential.

We highly recommend changing your service so that it works with the credential defined on the backing application object instead of the service principal.

Related content

- Review the Microsoft Entra recommendations overview
- Learn how to use Microsoft Entra recommendations
- Explore the Microsoft Graph API properties for recommendations
- Learn about securing service principals

How to use Microsoft Entra Workbooks

Article • 04/25/2025

Workbooks are found in Microsoft Entra ID and in Azure Monitor. The concepts, processes, and best practices are the same for both types of workbooks, however, workbooks for Microsoft Entra ID cover only those identity management scenarios that are associated with Microsoft Entra ID.

When using workbooks, you can either start with an empty workbook, or use an existing template. Workbook templates enable you to quickly get started using workbooks without needing to build from scratch.

- **Public templates** published to a [gallery](#) are a good starting point when you're just getting started with workbooks.
- **Private templates** are helpful when you start building your own workbooks and want to save one as a template to serve as the foundation for multiple workbooks in your tenant.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader

- View and modify settings:
 - Monitoring Contributor
 - Log Analytics Contributor

Microsoft Entra roles

Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- Read:
 - Reports Reader
 - Security Reader
 - Global Reader
- Update:
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

Access Microsoft Entra workbooks

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Entra ID > Monitoring & health > Workbooks**.
 - **Workbooks:** All workbooks created in your tenant
 - **Public Templates:** Prebuilt workbooks for common or high priority scenarios
 - **My Templates:** Templates you created
3. Select a report or template from the list. Workbooks might take a few moments to populate.
 - Search for a template by name.
 - Select the **Browse across galleries** to view templates that aren't specific to Microsoft Entra ID.

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with various categories like Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, Monitoring & health, Sign-in logs, Audit logs, Provisioning logs, Health (Preview), Log Analytics, Diagnostic settings, and Workbooks. The 'Monitoring & health' and 'Workbooks' items are highlighted with red boxes. The main area is titled 'Gallery' under 'Azure Active Directory'. It includes a search bar, a 'Quick start' section with an 'Empty' template, a 'Recently modified workbooks (0)' section (No items found), and sections for 'Usage (11)' and 'Conditional access (5)'. Each item in these sections has a small icon and a brief description.

Create a new workbook

Workbooks can be created from scratch or from a template. When creating a new workbook, you can add elements as you go or use the **Advanced Editor** option to paste in the JSON representation of a workbook, copied from the [workbooks GitHub repository](#).

To create a new workbook from scratch:

1. Browse to Entra ID > **Monitoring & health** > **Workbooks**.
2. Select **+ New**.
3. Select an element from the **+ Add** menu.

For more information on the available elements, see [Creating an Azure Workbook](#).

This Workbook has no content.

Use the add button below to add items.

+ Add

- Add text
- Add parameters
- Add links/tabs
- Add query
- Add metric
- Add group

To create a new workbook from a template:

1. Browse to **Entra ID** > **Monitoring & health** > **Workbooks**.
 2. Select a workbook template from the **Gallery**.
 3. Select **Edit** from the top of the page.
 - Each element of the workbook has its own **Edit** button.
 - For more information on editing workbook elements, see [Azure Workbooks Templates](#)

Microsoft Entra admin center Search resources, services, and docs (G+/-) ...

Home > Sign-ins Azure Active Directory

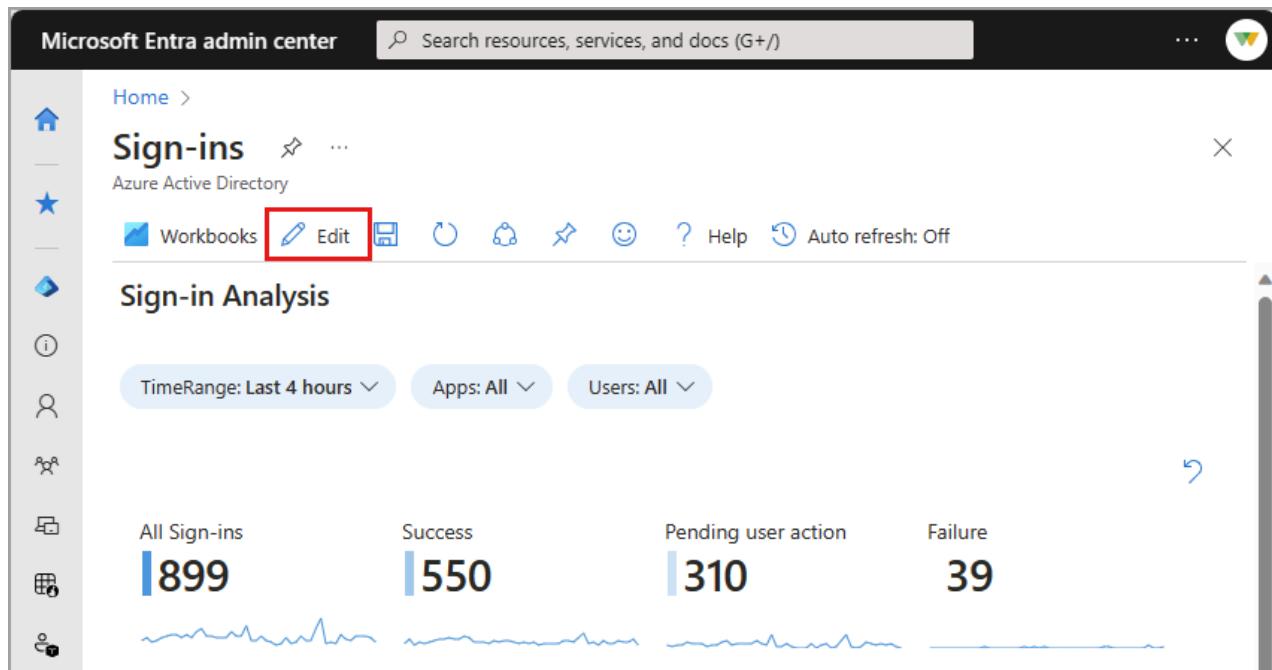
Workbooks **Edit**

Sign-in Analysis

TimeRange: Last 4 hours Apps: All Users: All

All Sign-ins Success Pending user action Failure

899 550 310 39



4. Select the **Edit** button for any element. Make your changes and select **Done editing**.

Microsoft Entra admin center Search resources, services, and docs (G+/-) ...

Home > Sign-ins Azure Active Directory

Workbooks **Done Editing**

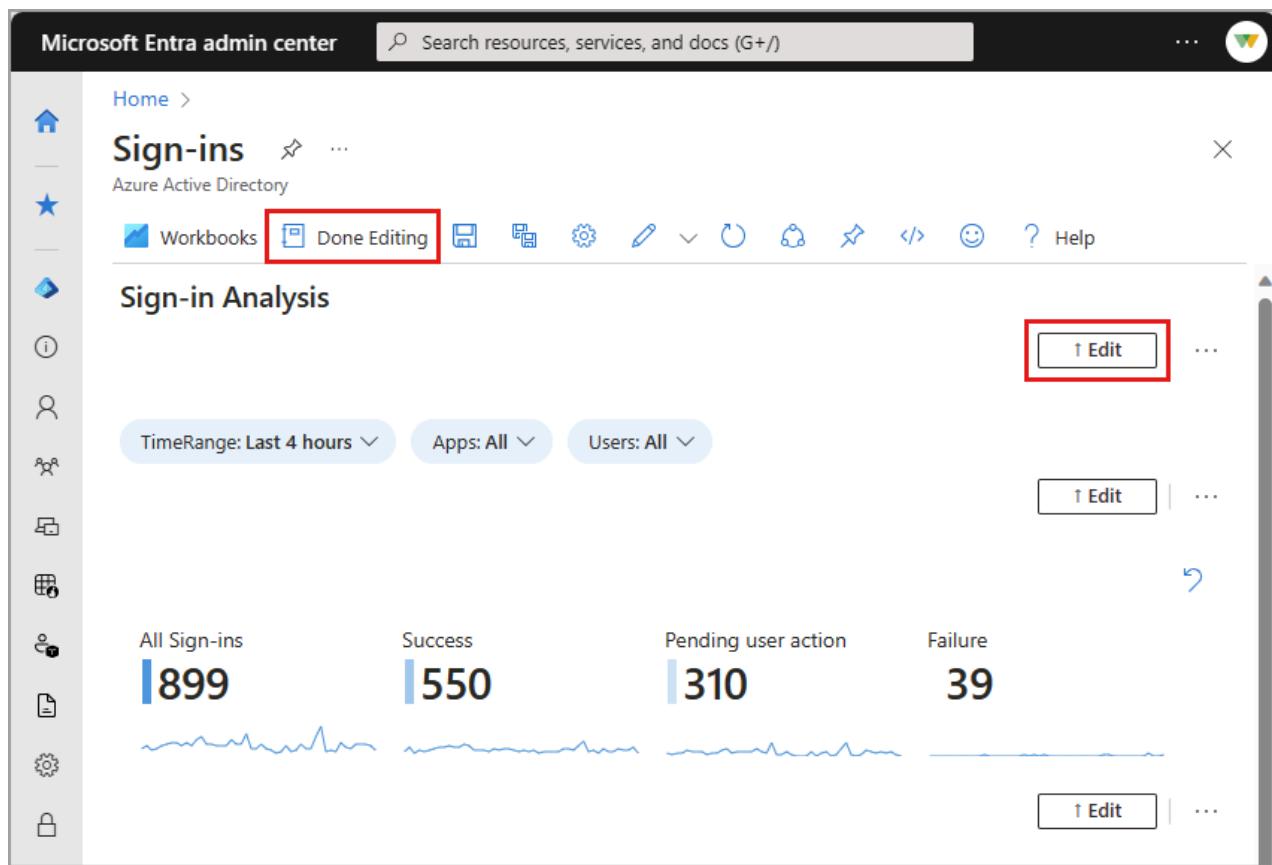
Sign-in Analysis

↑ Edit

TimeRange: Last 4 hours Apps: All Users: All

All Sign-ins Success Pending user action Failure

899 550 310 39



5. When you're done editing the workbook, select the **Save** button. The **Save as** window opens.

6. Provide a **Title**, **Subscription**, **Resource Group*** and **Location**

- You must have the ability to save a workbook for the selected Resource Group.
- Optionally choose to save your workbook content to an [Azure Storage Account](#).

7. Select the **Apply** button.

Next steps

- [Create interactive reports by using Monitor workbooks.](#)
- [Create custom Azure Monitor queries using Azure PowerShell.](#)

Authentication prompts analysis workbook

Article • 11/04/2024

As an IT Pro, you want the right information about authentication prompts in your environment so you can detect unexpected prompts and investigate further. Providing you with this type of information is the goal of the **Authentication Prompts Analysis** workbook.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader
- **View and modify settings:**
 - Monitoring Contributor
 - Log Analytics Contributor

Microsoft Entra roles

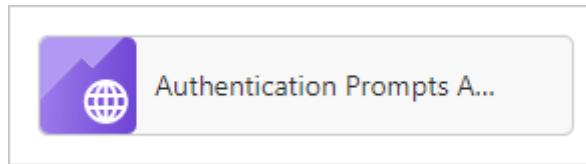
Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

Description



Have you recently received complaints from your users about getting too many authentication prompts?

Over-prompting users can affect productivity and can lead to users getting phished for multifactor authentication (MFA). To be clear, we aren't talking about *if* you should require MFA but *how frequently you should prompt your users*.

The following factors can cause over prompting:

- Misconfigured applications
- Over aggressive prompts policies
- Cyber-attacks

The authentication prompts analysis workbook identifies various types of authentication prompts. The types are based on different factors including users, applications, operating system, processes, and more.

You can use this workbook in the following scenarios:

- To research feedback of users getting too many prompts.
- To detect over-prompting attributed to one specific authentication method, policy application, or device.
- To view authentication prompt counts of high-profile users.
- To track legacy TLS and other authentication process details.

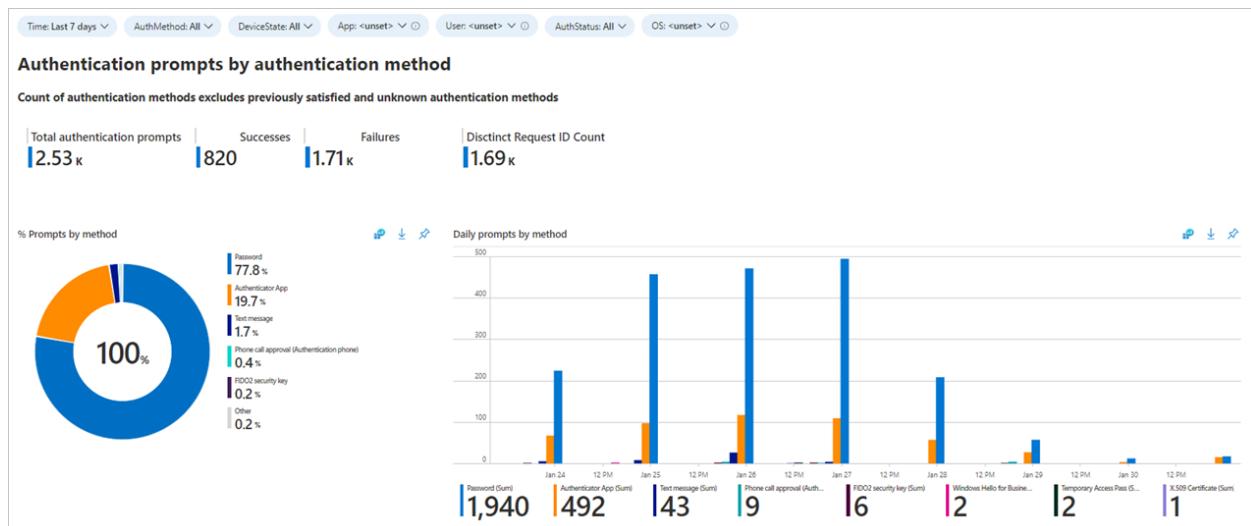
How to access the workbook

1. Sign in to the [Microsoft Entra admin center](#) using the appropriate combination of roles.
2. Browse to **Identity > Monitoring & health > Workbooks**.
3. Select the **Authentication Prompts Analysis** workbook from the **Usage** section.

Workbook sections

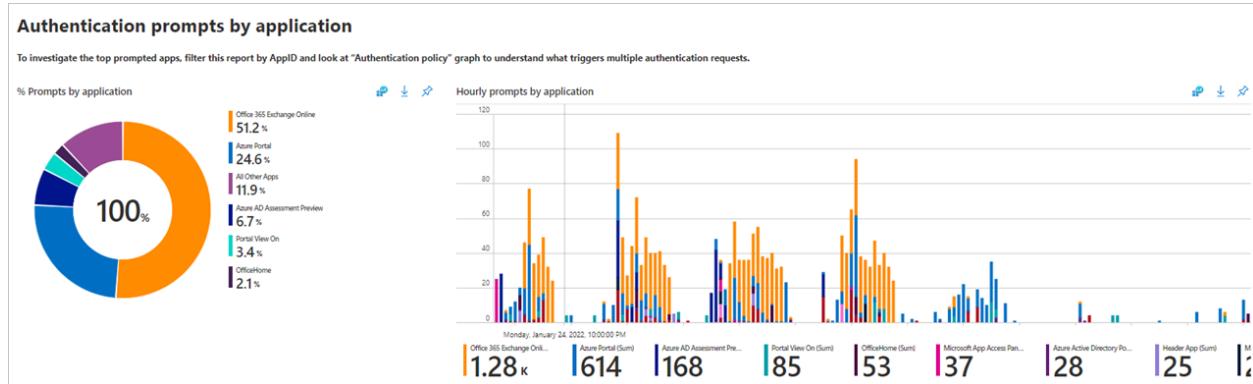
This workbook breaks down authentication prompts by:

- Method
- Device state
- Application
- User
- Status
- Operating System
- Process detail
- Policy



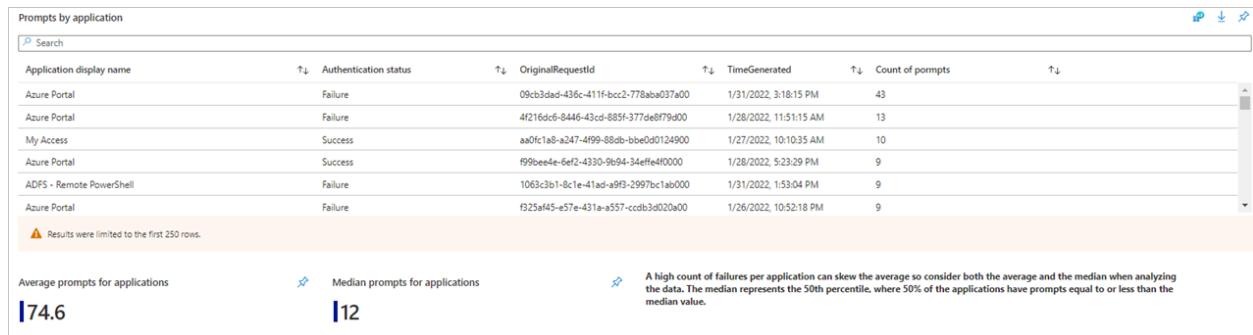
In many environments, the most used apps are business productivity apps. Anything that isn't expected should be investigated. The following charts show authentication

prompts by application.



The **prompts by application** list view shows additional information such as timestamps, and request IDs that help with investigations.

Additionally, you get a summary of the average and median prompts count for your tenant.



This workbook also helps track impactful ways to improve your users' experience and reduce prompts and the relative percentage.

Recommendations for reducing prompts and improving user experience		
Managed devices		
For improved user experience, we recommend enabling single sign-on using managed devices. Learn more: Plan your Azure Active Directory device deployment		
Windows Hello for Business		
To reduce authentication prompts and improve user experience on Windows 10 and above, we recommend using Windows Hello for Business. Learn more: Windows Hello for Business Overview - Microsoft 365 Security		
Android / iOS		
The Authenticator app serves as a token broker and can reduce authentication prompts. For improved user experience and reduce prompts on mobile devices, we recommend using the Microsoft Authenticator. Learn more: Microsoft Authenticator app authentication method - Azure Active Directory		
MacOS		
On MacOs we recommend the Microsoft Enterprise SSO plug-in for Apple devices. http://aka.ms/AADAppleSSO		
Managed Devices		
% Managed Devices		
0.90%	45	
WHFB authentications		
% WHFB		
0.13%	1569	
Authenticator app sign-ins on mobile		
% Authenticator App Sign-Ins		
90.44%		
MacOS user authentication prompts		
Avg Prompts for Mac Users		
5		

Filters

Take advantage of the filters for more granular views of the data:

Filters



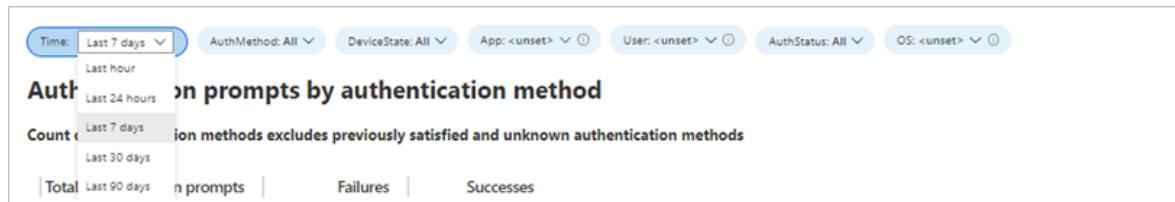
Filtering for a specific user that has many authentication requests or only showing applications with sign-in failures can also lead to interesting findings to continue to remediate.

Best practices

- If data isn't showing up or seems to be showing up incorrectly, confirm that you set the **Log Analytics Workspace** and **Subscriptions** on the proper resources.



- If the visuals are taking too much time to load, try reducing the Time filter to 24 hours or less.



- To understand more about the different policies that affect MFA prompts, see [Optimize reauthentication prompts and understand session lifetime for Microsoft Entra multifactor authentication](#).
- To learn how to move users from telecom-based methods to the Authenticator app, see [How to run a registration campaign to set up Microsoft Authenticator - Microsoft Authenticator app](#).

Related content

- [How to use the identity workbooks](#)
- [Manage the 'Stay signed in?' prompt](#)
- [How MFA works](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Conditional Access gap analyzer workbook

Article • 11/04/2024

In Microsoft Entra ID, you can protect access to your resources by configuring Conditional Access policies. As an IT administrator, you want to ensure that your Conditional Access policies work as expected to ensure that your resources are properly protected. With the Conditional Access gap analyzer workbook, you can detect gaps in your Conditional Access implementation.

This article provides you with an overview of the [Conditional Access gap analyzer](#) workbook.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) before you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader
- **View and modify settings:**

- Monitoring Contributor
- Log Analytics Contributor

Microsoft Entra roles

Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

Description

 Conditional access
 Conditional Access Gap Analyzer

As an IT administrator, you want to make sure that only the right people can access your resources. Microsoft Entra Conditional Access helps you to accomplish this goal.

The Conditional Access gap analyzer workbook helps you to verify that your Conditional Access policies work as expected.

This workbook:

- Highlights user sign-ins that have no Conditional Access policies applied to them.
- Allows you to ensure that there are no users, applications, or locations that were unintentionally excluded from Conditional Access policies.

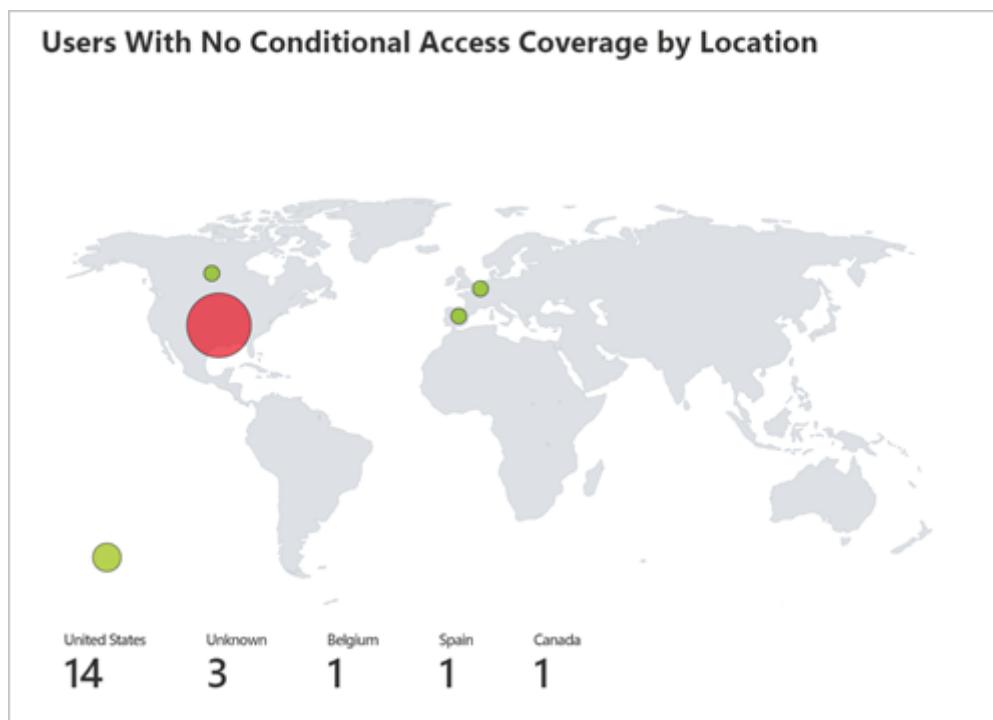
How to access the workbook

1. Sign in to the Microsoft Entra admin center [↗](#) using the appropriate combination of roles.
2. Browse to **Identity > Monitoring & health > Workbooks**.
3. Select the **Conditional Access Gap Analyzer** workbook from the **Conditional Access** section.

Workbook sections

The workbook has four sections:

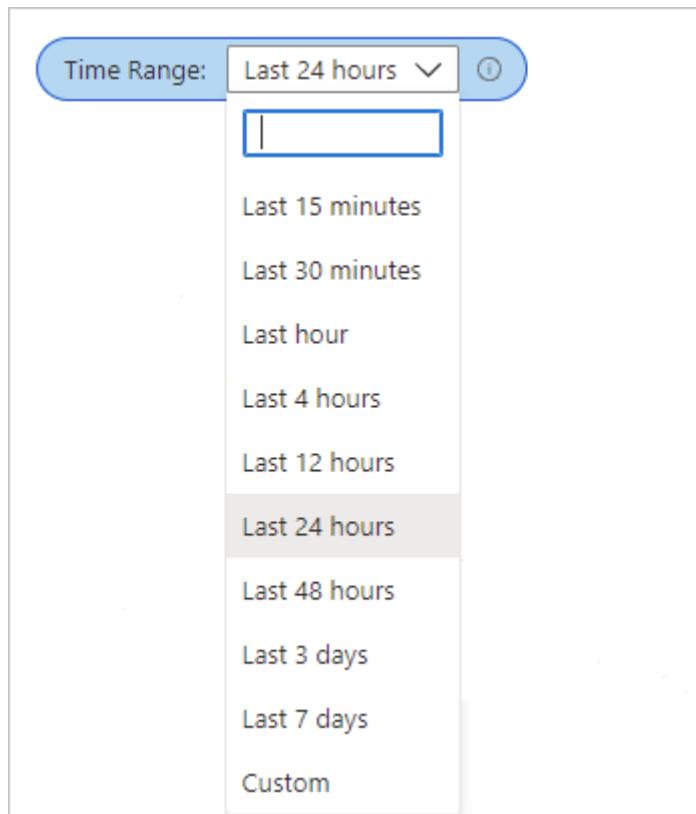
- Users signing in using legacy authentication
- Number of sign-ins by applications that aren't impacted by Conditional Access policies
- High risk sign-in events bypassing Conditional Access policies
- Number of sign-ins by location that weren't affected by Conditional Access policies



Each of these trends offers a breakdown of sign-ins to the user level, so that you can see which users per scenario are bypassing Conditional Access.

Filters

This workbook supports setting a time range filter.



Best practices

Use this workbook to ensure that your tenant is configured to the following Conditional Access best practices:

- Block all legacy authentication sign-ins
- Apply at least one Conditional Access Policy to every application
- Block all high risk sign-ins
- Block sign-ins from untrusted locations

Related content

- [How to use the identity workbooks](#)
- [What is Conditional Access?](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Cross-tenant access activity workbook

Article • 11/04/2024

As an IT administrator, you want insights into how your users are collaborating with other organizations. The cross-tenant access activity workbook helps you understand which external users are accessing resources in your organization, and which organizations' resources your users are accessing. This workbook combines all your organization's inbound and outbound collaboration into a single view.

This article provides you with an overview of the **Cross-tenant access activity** workbook.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader
- **View and modify settings:**
 - Monitoring Contributor
 - Log Analytics Contributor

Microsoft Entra roles

Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

Description



A screenshot of a Microsoft Power BI report titled "Usage". The report contains a single card with a purple icon featuring a globe and mountains, and the text "Cross-tenant access activity".

Tenant administrators who are making changes to policies governing cross-tenant access can use this workbook to visualize and review existing access activity patterns before making policy changes. For example, you can identify the applications your users are accessing in external organizations so that you don't inadvertently block critical business processes. Understanding how external users access resources in your tenant (inbound access) and how users in your tenant access resources in external tenants (outbound access) help ensure you have the right cross-tenant policies in place.

For more information, see the [Microsoft Entra External ID documentation](#).

How to access the workbook

1. Sign in to the [Microsoft Entra admin center](#) using the appropriate combination of roles.
2. Browse to **Identity > Monitoring & health > Workbooks**.

3. Select the **Cross-tenant access activity** workbook from the **Usage** section.

Workbook sections

This workbook has four sections:

- All inbound and outbound activity by tenant ID
- Sign-in status summary by tenant ID for inbound and outbound collaboration
- Applications accessed for inbound and outbound collaboration by tenant ID
- Individual users for inbound and outbound collaboration by tenant ID

The total number of external tenants that had cross-tenant access activity with your tenant is shown at the top of the workbook.

The **External Tenant** list shows all the tenants that had inbound or outbound activity with your tenant. When you select an external tenant in the table, the sections after the table display information about outbound and inbound activity for that tenant.

External Tenant	Outbound Sign-In	Outbound Sign-In	Outbound Users	Outbound Apps	Inbound Sign-In	Inbound Sign-In	Inbound Users
aaaaabbb-0000-c...	17	24	4	2	0	0	0
bbbbcccc-1111-d...	4	5	2	2	0	0	0
ccccdddd-2222-e...	4	2	1	1	0	0	0
dddeeeee-3333-f...	2	1	1	1	0	0	0
eeeeffff-4444-a...	12	0	2	4	0	0	0
eeeeffff-4444-a...	1	0	1	1	0	0	0
bbbbcccc-1111-d...	1	0	1	1	0	0	0
aaaaabbb-0000-c...	3	0	1	2	0	0	0
ccccdddd-2222-e...	0	0	0	0	4	0	1

When you select an external tenant from the list with outbound activity, associated details appear in the **Outbound activity** table. The same applies when you select an external tenant with inbound activity. Select the **Inbound activity** tab to view the details of an external tenant with inbound activity.

[Outbound activity](#)

[Inbound activity](#)

Outbound activity details for selected external tenant

Outbound sign-in status summary for selected external tenant

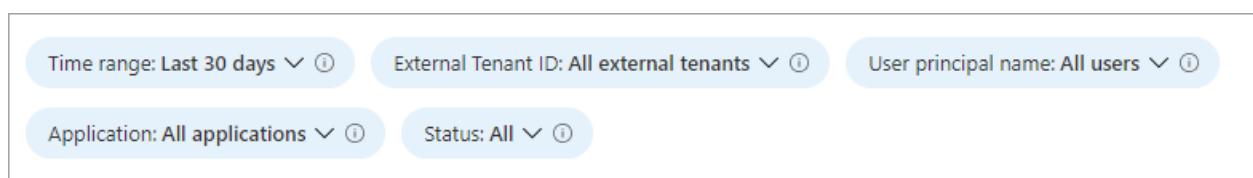
Status Count	↑↓	Status	↑↓	Status Code	↑↓	Status Reason
18		✖ Failure		50158		External security challenge was not satisfied.
1		✖ Failure		500212		Other
5		✖ Failure		50074		Strong Authentication is required.

When you're viewing external tenants with outbound activity, the subsequent two tables display details for the application, and user activity appear. When you're viewing external tenants with inbound activity, the same tables show inbound application and user activity. These tables are dynamic and based on what was previously selected, so make sure you're viewing the correct tenant and activity.

Filters

This workbook supports multiple filters:

- Time range (up to 90 days)
- External tenant ID
- User principal name
- Application
- Status of the sign-in (success or failure)



Best practices

Use this workbook to:

- Get the information you need to manage your cross-tenant access settings effectively, without breaking legitimate collaborations

- Identify all inbound sign-ins from external Microsoft Entra organizations
- Identify all outbound sign-ins by your users to external Microsoft Entra organizations

Related content

- [How to use the identity workbooks](#)
- [Introduction to Microsoft Entra External ID](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Multifactor Authentication Gaps workbook

Article • 11/04/2024

The Multifactor Authentication Gaps workbook helps with identifying user sign-ins and applications that aren't protected by multifactor authentication (MFA) requirements. This workbook:

- Identifies user sign-ins not protected by MFA requirements.
- Provides further drill down options using various pivots such as applications, operating systems, and location.
- Provides several filters such as trusted locations and device states to narrow down the users/applications.
- Provides filters to scope the workbook for a subset of users and applications.

This article gives you an overview of the **Multifactor authentication gaps** workbook.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**

- Monitoring Reader
- Log Analytics Reader
- **View and modify settings:**
 - Monitoring Contributor
 - Log Analytics Contributor

Microsoft Entra roles

Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

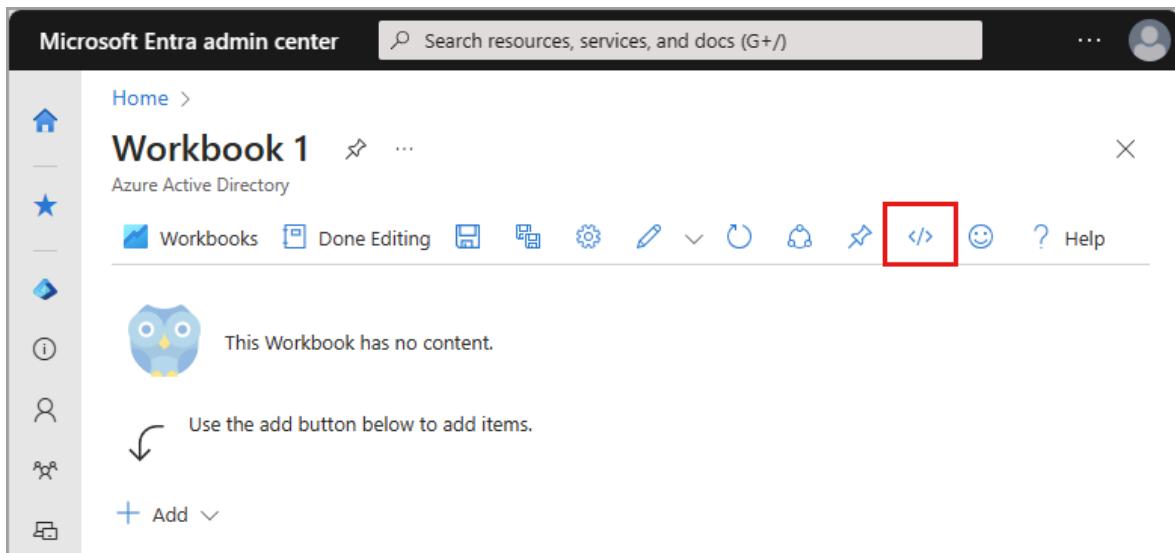
For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

How to import the workbook

The **MFA gaps** workbook is currently not available as a template, but you can import it from the Microsoft Entra workbooks GitHub repository.

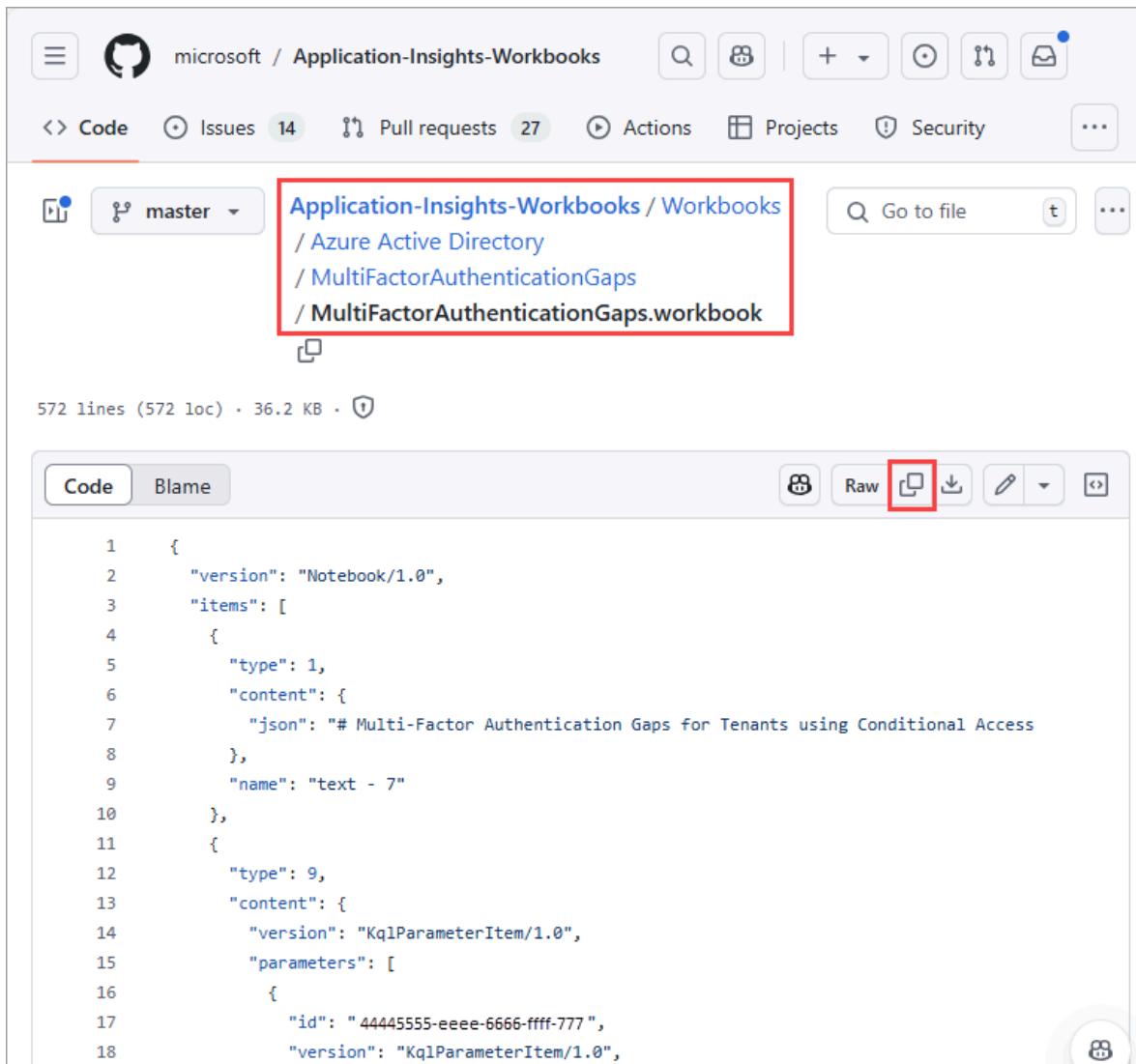
1. Sign in to the [Microsoft Entra admin center](#) using the appropriate combination of roles.
2. Browse to **Identity > Monitoring & health > Workbooks**.
3. Select **+ New**.
4. Select the **Advanced Editor** button from the top of the page. A JSON editor opens.



5. Use the following link to access the GitHub repository that contains the JSON file for the **Multifactor Authentication Gaps** workbook:

- Direct link to the Multifactor Authentication Gaps JSON file:
[https://github.com/microsoft/Application-Insights-Workbooks/blob/master/Workbooks/Azure%20Active%20Directory/MultiFactorAuthenticationGaps/MultiFactorAuthenticationGaps.workbook ↗](https://github.com/microsoft/Application-Insights-Workbooks/blob/master/Workbooks/Azure%20Active%20Directory/MultiFactorAuthenticationGaps/MultiFactorAuthenticationGaps.workbook)
- Make sure you're on the *MultiFactorAuthenticationGaps.workbook* file in the GitHub repository.

6. Copy the entire JSON file from the GitHub repository.



The screenshot shows a GitHub repository interface for the 'Application-Insights-Workbooks' repository. The path 'Application-Insights-Workbooks / Workbooks / Azure Active Directory / MultiFactorAuthenticationGaps / MultiFactorAuthenticationGaps.workbook' is highlighted with a red box. In the toolbar below the code editor, the 'Copy' button (represented by a clipboard icon) is also highlighted with a red box.

```
1  {
2    "version": "Notebook/1.0",
3    "items": [
4      {
5        "type": 1,
6        "content": {
7          "json": "# Multi-Factor Authentication Gaps for Tenants using Conditional Access
8        },
9        "name": "text - 7"
10       },
11      {
12        "type": 9,
13        "content": {
14          "version": "KqlParameterItem/1.0",
15          "parameters": [
16            {
17              "id": "44445555-eeee-6666-ffff-777",
18              "version": "KqlParameterItem/1.0",

```

7. Return to the workbook Advanced Editor window and paste the JSON file over the existing text.
8. Select the **Apply** button. The workbook might take a few moments to populate.
9. Select **Done Editing** and then select the **Save** button and provide the required information.
 - Provide a **Title**, **Subscription**, **Resource Group** (you must have the ability to save a workbook for the selected Resource Group), and **Location**.
 - Optionally choose to save your workbook content to an [Azure Storage Account](#).
10. Select the **Apply** button.

Summary

The summary widget provides a detailed look at sign-ins related to multifactor authentication.

Sign-ins not protected by MFA requirement by applications

- **Number of users signing-in not protected by multi-factor authentication requirement by application:** This widget provides a time based bar-graph representation of the number of user sign-ins not protected by MFA requirement by applications.
- **Percent of users signing-in not protected by multi-factor authentication requirement by application:** This widget provides a time based bar-graph representation of the percentage of user sign-ins not protected by MFA requirement by applications.
- **Select an application and user to learn more:** This widget groups the top users signed in without MFA requirement by application. Select the application to see a list of the user names and the count of sign-ins without MFA.

Sign-ins not protected by MFA requirement by users

- **Sign-ins not protected by multi-factor auth requirement by user:** This widget shows top user and the count of sign-ins not protected by MFA requirement.
- **Top users with high percentage of authentications not protected by multi-factor authentication requirements:** This widget shows users with top percentage of authentications that aren't protected by MFA requirements.

Sign-ins not protected by MFA requirement by Operating Systems

- **Number of sign-ins not protected by multi-factor authentication requirement by operating system:** This widget provides time based bar graph of sign-in counts that aren't protected by MFA by operating system of the devices.
- **Percent of sign-ins not protected by multi-factor authentication requirement by operating system:** This widget provides time based bar graph of sign-in percentages that aren't protected by MFA by operating system of the devices.

Sign-ins not protected by MFA requirement by locations

- **Number of sign-ins not protected by multi-factor authentication requirement by location:** This widget shows the sign-ins counts that aren't protected by MFA requirement in map bubble chart on the world map.

Related content

- [How to use the identity workbooks](#)
 - [Conditional Access gap analyzer workbook](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Understand how provisioning integrates with Azure Monitor logs

Article • 03/04/2025

Provisioning integrates with Azure Monitor logs and Log Analytics. With Azure monitoring you can do things like create workbooks, also known as dashboards, store provisioning logs for 30+ days, and create custom queries and alerts. This article discusses how provisioning logs integrate with Azure Monitor logs. To learn more about how provisioning logs work in general, see [provisioning logs](#).

Enabling provisioning logs integration

If you're not already familiar with Azure Monitor and Log Analytics, explore the following resources and then come back to learn about integrating application provisioning logs with Azure Monitor logs.

- [Azure Monitor overview](#)
- [Configure a Log Analytics workspace](#)
- [Integrate activity logs with Azure Monitor logs](#)

To integrate provisioning logs with Azure Monitor logs:

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a [Security Administrator](#).
2. [Create a Log Analytics workspace](#).
3. Browse to **Identity > Monitoring & health > Diagnostic settings**.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a 'Diagnostic settings' link highlighted with a red box. The main content area is titled 'Diagnostic settings | General' and shows a table with one row for 'Woodgrove'. A red box highlights the '+ Add diagnostic setting' button. Below the table, a list of log types is provided, and a magnifying glass icon is in the bottom right corner.

Name	Storage account	Event hub	Log Analytics works...	Partner solution	Edit setting
Woodgrove			woodgrove		Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditLogs
- SignInLogs
- NoninteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSignInLogs
- RiskyUsers
- UserRiskEvents
- NetworkAccessTrafficLogs
- RiskyServicePrincipals
- ServicePrincipalRiskEvents
- EnrichedOffice365AuditLogs
- MicrosoftGraphActivityLogs
- RemoteNetworkHealthLogs
- NetworkAccessAlerts

- Choose the logs you want to stream, select the **Send to Log Analytics workspace** option, and complete the fields.

- Browse to **Identity > Monitoring & health > Log Analytics** and begin querying the data.

! Note

It can take some time before logs appear in Log Analytics after first enabling the integration. If you receive an error that the subscription is not registered to use `microsoft.insights` then check back after a few minutes.

Understanding the data

The underlying data stream that Provisioning sends log viewers is almost identical. Azure Monitor logs gets nearly the same stream as the Microsoft Entra admin center and the Microsoft Graph API. There are a few differences in the log fields as outlined in the following table. Log Analytics might display more events than the logs in the Microsoft Entra admin center. To learn more about these fields, see [List provisioningObjectSummary](#).

[Expand table](#)

Azure Monitor logs	Azure portal UI	Azure API
errorDescription	reason	resultDescription

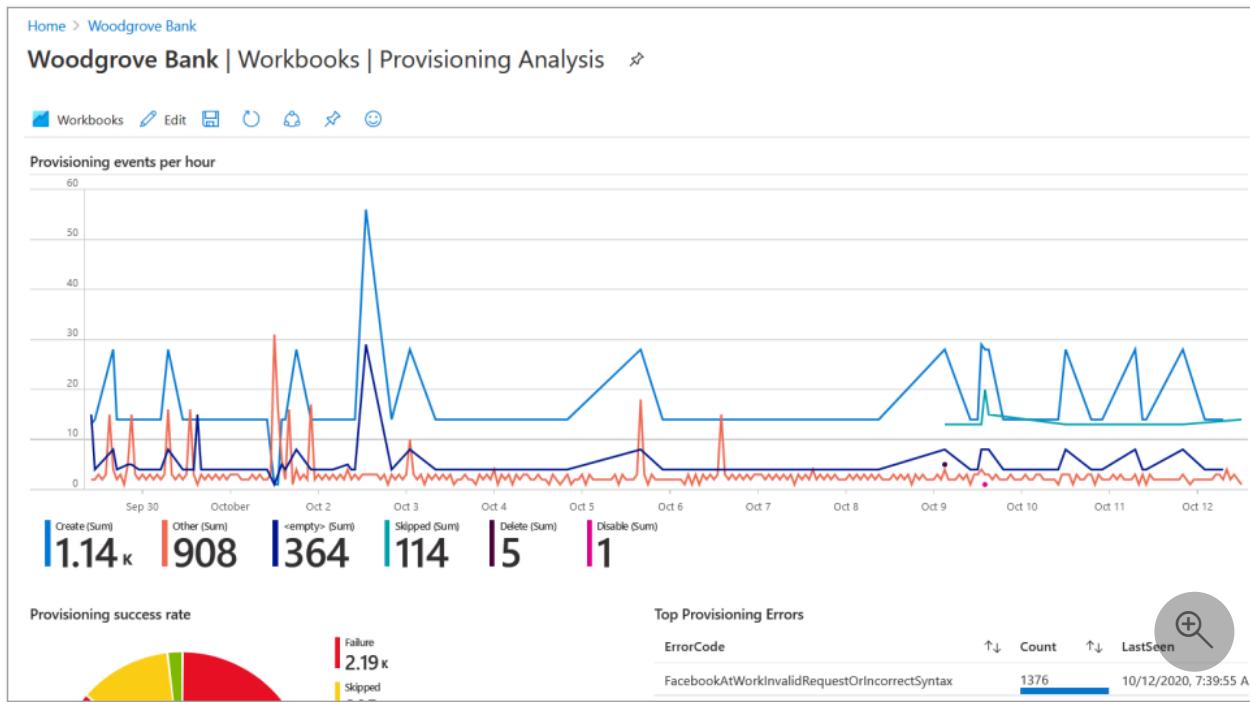
Azure Monitor logs	Azure portal UI	Azure API
status	resultType	resultType
activityDateTime	TimeGenerated	TimeGenerated

Microsoft Entra workbooks

Microsoft Entra identity workbooks provide a flexible canvas for data analysis. They also provide for the creation of rich visual reports within the Azure portal. To learn more, see [Microsoft Entra workbooks](#).

The **Provisioning Analysis** and **Provisioning Insights** are two of the prebuilt workbooks available. To view the data, ensure that all the filters (timeRange, jobID, appName) are populated. Also confirm the app was provisioned, otherwise there isn't any data in the logs.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like External Identities, User experiences, Hybrid management, Monitoring & health, Log Analytics, Diagnostic settings, Protection, Identity Protection, Conditional Access, and Learn & support. Under 'Diagnostic settings', the 'Workbooks' option is selected and highlighted with a red box. The main area is titled 'Gallery' under 'Conditional access'. It lists several workbooks: 'Conditional Access Insight...', 'Continuous access evaluat...', 'Sign-ins by Conditional Ac...', 'Sign-ins by Grant Controls...', 'Conditional Access Gap A...', 'ID Protection Risk Analysis', 'Impact analysis of risk-bas...', 'Sensitive Operations Report', 'Sign-ins Failure Analysis', 'Archived Log Date Range', 'Provisioning Insights' (which is also highlighted with a red box), and 'Provisioning Analysis' (which is also highlighted with a red box). At the bottom right of the main area, there's a search icon.



Custom queries

You can create custom queries and show the data in your workbooks. To learn how, see [Get started with log queries in Azure Monitor](#) and [Log queries in Azure Monitor](#).

Here are some samples to get started with application provisioning log queries.

Query the logs for a user a based on their ID in the source system:

```
Kusto

AADProvisioningLogs
| extend SourceIdentity = parse_json(SourceIdentity)
| where tostring(SourceIdentity.Id) == "49a4974bb-5011-415d-b9b8-
78caa7024f9a"
```

Summarize count per ErrorCode:

```
Kusto

AADProvisioningLogs
| summarize count() by ErrorCode = ResultSignature
```

Summarize count of events per day by action:

```
Kusto

AADProvisioningLogs
| where TimeGenerated > ago(7d)
```

```
| summarize count() by Action, bin(TimeGenerated, 1d)
```

Take 100 events and project key properties:

Kusto

```
AADProvisioningLogs
| extend SourceIdentity = parse_json(SourceIdentity)
| extend TargetIdentity = parse_json(TargetIdentity)
| extend ServicePrincipal = parse_json(ServicePrincipal)
| where tostring(SourceIdentity.identityType) == "Group"
| project tostring(ServicePrincipal.Id), tostring(ServicePrincipal.Name),
ModifiedProperties, JobId, Id, CycleId, ChangeId, Action,
SourceIdentity.identityType, SourceIdentity.details,
TargetIdentity.identityType, TargetIdentity.details, ProvisioningSteps
| take 100
```

Retrieve groups with skipped members due to problems resolving references.

Kusto

```
AADProvisioningLogs
| where TimeGenerated >= ago(10d)
| where JobId == "Azure2Azure.73f0883f-d67d-4af1-ac8a-45367f8982e0.5ef3be57-
f45f-451g-88c4-68a7fda680bb" // Customize by adding a specific app JobId
| extend SourceIdentity = parse_json(SourceIdentity)
| extend ProvisioningSteps = parse_json(ProvisioningSteps)
| where tostring(SourceIdentity.identityType) == "Group"
| where ProvisioningSteps matches regex
"UnableToResolveReferenceAttributeValue"
| parse tostring(ProvisioningSteps.[2].description) with "We were unable to
assign " userObjectId " as the members of " groupDisplayName "."
| project groupDisplayName, userObjectId, JobId
| take 100
```

Summarize actions by application.

Kusto

```
AADProvisioningLogs
| where TimeGenerated > ago(30d)
| where JobId == "Azure2Azure.73f0883f-d67d-4af1-ac8a-45367f8982e0.5ef3be57-
f45f-451g-88c4-68a7fda680bb" // Customize by adding a specific app JobId
| extend ProvisioningSteps = parse_json(ProvisioningSteps)
| extend eventName = tostring(ProvisioningSteps.[ -1 ].name)
| summarize count() by eventName, JobId
| order by JobId asc
| take 5
```

Identify spikes in specific operations.

Kusto

```
AADProvisioningLogs
| where TimeGenerated > ago(30d)
| where JobId == "scim.73f0883f-d67d-4af1-ac8a-45367f8982e0.5ef3be57-f45f-
451g-88c4-68a7fda680bb" // Customize by adding a specific app JobId
| extend ProvisioningSteps = parse_json(ProvisioningSteps)
| extend eventName = tostring(ProvisioningSteps.[ -1].name)
| summarize count() by eventName, bin(TimeGenerated, 1d)
| render timechart
```

Custom alerts

Azure Monitor lets you configure custom alerts so that you can get notified about key events related to Provisioning. For example, you might want to receive an alert on spikes in failures spikes in disables or deletes. You might also want to be alerted if there's a lack of any provisioning, which indicates something is wrong.

To learn more about alerts, see [Azure Monitor Log Alerts](#). There are many options and configurations, so review the full documentation. But at a high-level, here's how you can create an alert:

1. From Log Analytics, select **+ New alert rule**.
2. On the **Condition** tab, select the **View result and edit query in Logs** link.
3. Enter a query you want to alert on, and complete the necessary fields to create the alert.

To create an alert when there's a spike in failures:

Kusto

```
AADProvisioningLogs
| where JobId == "string" // Customize by adding a specific app JobId
| where ResultType == "Failure"
```

There might be an issue that caused the provisioning service to stop running. Use the following query to detect when there are no provisioning events during a given time interval.

Kusto

```
AADProvisioningLogs
```

| take 1

To create an alert when there's a spike in disables or deletes:

Kusto

```
AADProvisioningLogs  
| where Action in ("Disable", "Delete")
```

Community contributions

We're taking an open source and community-based approach to application provisioning queries and dashboards. Build a query, alert, or workbook that you think is useful to others, then publish it to the [AzureMonitorCommunity GitHub repo](#). Shoot us an email with a link. We review and publish queries and dashboards to the service so others benefit too. Contact us at provisioningfeedback@microsoft.com.

Next steps

- [Integrate Microsoft Entra logs with Azure Monitor logs](#)
- [Get started with queries in Azure Monitor logs](#)
- [Create and manage alert groups in the Azure portal](#)
- [Provisioning logs API](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Identity protection risk analysis workbook

Article • 11/04/2024

Microsoft Entra ID Protection detects, remediates, and prevents compromised identities. As an IT administrator, you want to understand risk trends in your organizations and opportunities for better policy configuration. With the Identity Protection Risky Analysis Workbook, you can answer common questions about your Identity Protection implementation.

This article provides you with an overview of the [Identity Protection Risk Analysis](#) workbook.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader
- **View and modify settings:**

- Monitoring Contributor
- Log Analytics Contributor

Microsoft Entra roles

Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

Description



As an IT administrator, you need to understand trends in identity risks and gaps in your policy implementations, to ensure you're best protecting your organizations from identity compromise. The identity protection risk analysis workbook helps you analyze the state of risk in your organization.

This workbook:

- Provides visualizations of where in the world risk is being detected.
- Allows you to understand the trends in real time vs. offline risk detections.
- Provides insight into how effective you are at responding to risky users.

How to access the workbook

1. Sign in to the [Microsoft Entra admin center](#) using the appropriate combination of roles.

2. Browse to **Identity > Monitoring & health > Workbooks**.

3. Select the **Identity Protection Risk Analysis** workbook from the **Usage** section.

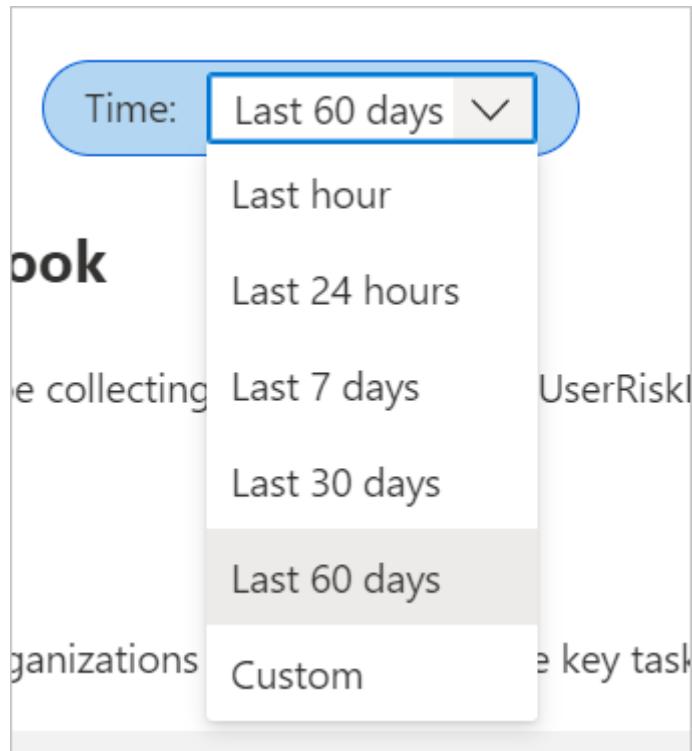
Workbook sections

This workbook has five sections:

- Heatmap of risk detections
- Offline vs real-time risk detections
- Risk detection trends
- Risky users
- Summary

Filters

This workbook supports setting a time range filter.



There are more filters in the risk detection trends and risky users sections.

Risk Detection Trends:

- Detection timing type (real-time or offline)
- Risk level (low, medium, high, or none)

Risky Users:

- Risk detail (which indicates what changed a user's risk level)
- Risk level (low, medium, high, or none)

Best practices

- **Enable risky sign-in policies** - To prompt for multifactor authentication (MFA) on medium risk or higher. Enabling the policy reduces the proportion of active real-time risk detections by allowing legitimate users to self-remediate the risk detections with MFA.
- **Enable a risky user policy** - To enable users to securely remediate their accounts when they're considered high risk. Enabling the policy reduces the number of active at-risk users in your organization by returning the user's credentials to a safe state.
- To learn more about identity protection, see [What is identity protection](#).
- For more information about Microsoft Entra workbooks, see [How to use Microsoft Entra workbooks](#).

Related content

- [How to use the identity workbooks](#)
- [What is Microsoft Entra ID Protection?](#)
- [What are risk detections?](#)

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Sensitive operations report workbook

Article • 11/04/2024

The sensitive operations report workbook is intended to help identify suspicious application and service principal activity that might indicate compromises in your environment.

This article provides you with an overview of the [Sensitive Operations Report](#) workbook.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader
- **View and modify settings:**
 - Monitoring Contributor
 - Log Analytics Contributor

Microsoft Entra roles

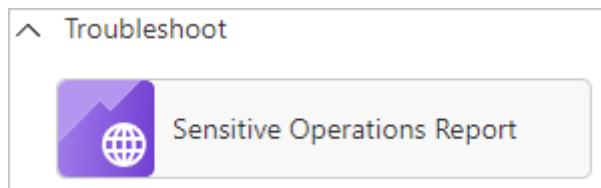
Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

Description



This workbook identifies recent sensitive operations performed in your tenant.

If your organization is new to Azure monitor workbooks, you need to integrate your Microsoft Entra sign-in and audit logs with Azure Monitor before accessing the workbook. This integration allows you to store, query, and visualize your logs using workbooks for up to two years. Only sign-in and audit events created after Azure Monitor integration are stored, so the workbook won't contain insights before that date. For more information, see [Integrate Microsoft Entra logs with Azure Monitor](#).

How to access the workbook

1. Sign in to the [Microsoft Entra admin center](#) using the appropriate combination of roles.
2. Browse to **Identity > Monitoring & health > Workbooks**.
3. Select the **Sensitive Operations Report** workbook from the **Troubleshoot** section.

Sections

This workbook is split into four sections:

- ✓ Modified application and service principal credentials/authentication methods
- ✓ New permissions granted to service principals
- ✓ Directory role and group membership updates to service principals
- ✓ Modified federation settings

- **Modified application and service principal credentials/authentication methods** - This report flags actors who recently changed many service principal credentials, and how many of each type of service principal credentials changed.
- **New permissions granted to service principals** - This workbook also highlights recently granted OAuth 2.0 permissions to service principals.
- **Directory role and group membership updates for service principals**
- **Modified federation settings** - This report highlights when a user or application modifies federation settings on a domain. For example, it reports when a new Active Directory Federated Service (ADFS) TrustedRealm object, such as a signing certificate, is added to the domain. Modification to domain federation settings should be rare.

Modified application and service principal credentials/authentication methods

One of the most common ways for attackers to gain access in the environment is by adding new credentials to existing applications and service principals. The credentials allow the attacker to authenticate as the target application or service principal, granting them access to all resources to which it has permissions.

This section includes the following data to help you detect:

- All new credentials added to apps and service principals, including the credential type
- Top actors and the number of credentials modifications they performed

- A timeline for all credential changes

New permissions granted to service principals

Attackers often attempt to add permissions to another service principal or application if they can't find a service principal or application with a high privilege set of permissions through which to gain access.

This section includes a breakdown of the AppOnly permissions grants to existing service principals. Admins should investigate any instances of excessive high permissions being granted, including, but not limited to, Exchange Online, and Microsoft Graph.

Directory role and group membership updates for service principals

Following the logic of the attacker adding new permissions to existing service principals and applications, another approach is adding them to existing directory roles or groups.

This section includes an overview of all changes made to service principal memberships and should be reviewed for any additions to high privilege roles and groups.

Modified federation settings

Another common approach to gain a long-term foothold in the environment is to:

- Modify the tenant's federated domain trusts.
- Add another SAML IDP that the attacker controls as a trusted authentication source.

This section includes the following data:

- Changes performed to existing domain federation trusts
- Addition of new domains and trusts

Filters

This paragraph lists the supported filters for each section.

Modified Application and Service Principal Credentials/Authentication Methods

- Time range
- Operation name
- Credential
- Actor
- Exclude actor

New permissions granted to service principals

- Time range
- Client app
- Resource

Directory role and group membership updates to service principals

- Time range
- Operation
- Initiating user or app

Modified federation settings

- Time range
- Operation
- Initiating user or app

Best practices

- **Use modified application and service principal credentials** to look out for credentials being added to service principals that aren't frequently used in your organization. Use the filters present in this section to further investigate any of the suspicious actors or service principals that were modified.
- **Use new permissions granted to service principals** to look out for broad or excessive permissions being added to service principals by actors that might be compromised.
- **Use modified federation settings** section to confirm that the added or modified target domain/URL is a legitimate admin behavior. Actions that modify or add domain federation trusts are rare and should be treated as high fidelity to be investigated as soon as possible.

Related content

- [How to use the identity workbooks](#)
 - [Service principal sign-in logs](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Sign-ins using legacy authentication workbook

Article • 11/04/2024

Have you ever wondered how you can determine whether it's safe to turn off legacy authentication in your tenant? The sign-ins using legacy authentication workbook helps you to answer this question.

This article gives you an overview of the [Sign-ins using legacy authentication](#) workbook.

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

- A Microsoft Entra tenant with a [Premium P1 license](#)
- A Log Analytics workspace *and* access to that workspace
- The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. Several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

Azure Monitor roles

Azure Monitor provides [two built-in roles](#) for viewing monitoring data and editing monitoring settings. Azure role-based access control (RBAC) also provides two Log Analytics built-in roles that grant similar access.

- **View:**
 - Monitoring Reader
 - Log Analytics Reader
- **View and modify settings:**
 - Monitoring Contributor
 - Log Analytics Contributor

Microsoft Entra roles

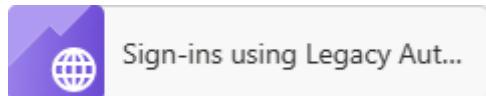
Read only access allows you to view Microsoft Entra ID log data inside a workbook, query data from Log Analytics, or read logs in the Microsoft Entra admin center. Update access adds the ability to create and edit diagnostic settings to send Microsoft Entra data to a Log Analytics workspace.

- **Read:**
 - Reports Reader
 - Security Reader
 - Global Reader
- **Update:**
 - Security Administrator

For more information on Microsoft Entra built-in roles, see [Microsoft Entra built-in roles](#).

For more information on the Log Analytics RBAC roles, see [Azure built-in roles](#).

Description



Microsoft Entra ID supports several of the most widely used authentication and authorization protocols including legacy authentication. Legacy authentication refers to basic authentication, which was once a widely used industry-standard method for passing user name and password information through a client to an identity provider.

Examples of applications that commonly or only use legacy authentication are:

- Microsoft Office 2013 or older.
- Apps using legacy auth with mail protocols like POP, IMAP, and SMTP AUTH.

Single-factor authentication (for example, username and password) doesn't provide the required level of protection for today's computing environments. Passwords are bad as they're easy to guess and humans are bad at choosing good passwords.

Unfortunately, legacy authentication:

- Doesn't support multifactor authentication (MFA) or other strong authentication methods.
- Makes it impossible for your organization to move to passwordless authentication.

To improve the security of your Microsoft Entra tenant and experience of your users, you should disable legacy authentication. However, important user experiences in your tenant might depend on legacy authentication. Before shutting off legacy authentication, you might want to find those cases so you can migrate them to more secure authentication.

The **Sign-ins using legacy authentication** workbook lets you see all legacy authentication sign-ins in your environment. This workbook helps you find and migrate critical workflows to more secure authentication methods before you shut off legacy authentication.

How to access the workbook

1. Sign in to the [Microsoft Entra admin center](#) using the appropriate combination of roles.
2. Browse to **Identity > Monitoring & health > Workbooks**.
3. Select the **Sign-ins using legacy authentication** workbook from the **Usage** section.

Workbook sections

With this workbook, you can distinguish between interactive and non-interactive sign-ins. This workbook highlights which legacy authentication protocols are used throughout your tenant.

The data collection consists of three steps:

1. Select a legacy authentication protocol, and then select an application to filter by users accessing that application.
2. Select a user to see all their legacy authentication sign-ins to the selected app.
3. View all legacy authentication sign-ins for the user to understand how legacy authentication is being used.

Filters

This workbook supports multiple filters:

- Time range (up to 90 days)
- User principal name

- Application
- Status of the sign-in (success or failure)

The screenshot shows a search interface with four dropdown filters. From left to right: 'Time range: Last 24 hours', 'User principal name: All users', 'Application: All applications', and 'Status: Success'. Each filter has a small downward arrow indicating it can be expanded.

Best practices

- For guidance on blocking legacy authentication in your environment, see [Block legacy authentication to Microsoft Entra ID with Conditional Access](#).
- Many email protocols that once relied on legacy authentication now support more secure modern authentication methods. If you see legacy email authentication protocols in this workbook, consider migrating to modern authentication for email instead. For more information, see [Deprecation of Basic authentication in Exchange Online](#).
- Some clients can use both legacy authentication or modern authentication depending on client configuration. If you see "modern mobile/desktop client" or "browser" for a client in the Microsoft Entra logs, it's using modern authentication. If it has a specific client or protocol name, such as "Exchange ActiveSync," it's using legacy authentication to connect to Microsoft Entra ID. The client types in Conditional Access, and the Microsoft Entra reporting page in the Microsoft Entra admin center demarcate modern authentication clients and legacy authentication clients for you, and only legacy authentication is captured in this workbook.
- To learn more about identity protection, see [What is identity protection](#).
- For more information about Microsoft Entra workbooks, see [How to use Microsoft Entra workbooks](#).

Related content

- [How to use the identity workbooks](#)
- [Authentication methods overview](#)

Feedback

Was this page helpful?



Yes



No

Provide product feedback ↗

How to troubleshoot Microsoft Entra sign-in errors

Article • 04/25/2025

The Microsoft Entra sign-in logs enable you to find answers to questions around managing access to the applications in your organization, including:

- 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?

In addition, the sign-in logs can also help you troubleshoot sign-in failures for users in your organization. In this guide, you learn how to isolate a sign-in failure in the sign-ins report, and use it to understand the root cause of the failure. Some common sign-in errors are also described.

Prerequisites

You need:

- A working Microsoft Entra tenant with the appropriate Microsoft Entra license associated with it.
 - For a full list of license requirements, see [Microsoft Entra monitoring and health licensing](#).
- [Reports Reader](#) is the least privileged role required to access the activity logs.
- In addition, any user can access their own sign-ins from <https://mysignins.microsoft.com>.

Gather sign-in details

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Entra ID > Monitoring & health > Sign-in logs**.
3. Use the filters to narrow down the results
 - Search by username if you're troubleshooting a specific user.
 - Search by application if you're troubleshooting issues with a specific app.
 - Select **Failure** from the **Status** menu to display only failed sign-ins.
4. Select the failed sign-in you want to investigate to open the details window.

5. Explore the details on each tab. You might want to save a few details for further troubleshooting. These details are highlighted in the screenshot following the list.

- Correlation ID
- Sign-in error code
- Failure reason
- Username, User ID, and Sign-in identifier

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date	8/18/2023, 7:46:06 AM				
Request ID	1111aaa-000011-aabb-111bbbb000				
Correlation ID	cccc2222-dd33-4444-55ee-666666ffffff				
Authentication requirement	Multifactor authentication				
Status	Failure				
Continuous access evaluation	No				
Sign-in error code	500121				
Failure reason	Authentication failed during strong authentication request.				
Additional Details	The user didn't complete the MFA prompt. They may have decided not to authenticate, timed out while doing other work, or has an issue with their authentication setup.				
Follow these steps:					
Troubleshoot Event	Launch the Sign-in Diagnostic.				
1. Review the diagnosis and act on suggested fixes.					
User	Semyon Maslov				
Username	semaslov@woodgrovegroceries.com				
User ID	44ee44ee-ff55-aa66-bb77-88cc88cc88cc				

Troubleshoot sign-in errors

With sign-in details gathered, you should explore the results and troubleshoot the issue.

Failure reason and additional details

The **Failure reason** and **Additional Details** might provide you with the details and next steps to resolve the issue. The Failure reason describes the error. The Additional Details provides more details and often tells you how to resolve the issue.

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date	8/18/2023, 7:46:06 AM				
Request ID	1111aaa-000011-aabb-111bbbb000				
Correlation ID	cccc2222-dd33-4444-55ee-666666fffff				
Authentication requirement	Multifactor authentication				
Status	Failure				
Continuous access evaluation	No				
Sign-in error code	500121				
Failure reason	Authentication failed during strong authentication request.				
Additional Details	The user didn't complete the MFA prompt. They may have decided not to authenticate, timed out while doing other work, or has an issue with their authentication setup.				
Follow these steps:					
Troubleshoot Event	Launch the Sign-in Diagnostic.				
1. Review the diagnosis and act on suggested fixes.					

The following failure reasons and details are common:

- The failure reason **Authentication failed during the strong authentication request** doesn't provide much to troubleshoot, but the additional details field says the user didn't complete the MFA prompt. Have the user sign-in again and complete the MFA prompts.
- The failure reason **The Federation Service failed to issue an OAuth Primary Refresh Token** provides a good starting point, but the additional details briefly explain how authentication works in this scenario and tell you to make sure that device sync is enabled.
- A common failure reason is **Error validating credentials due to invalid username or password**. The user entered something incorrectly and needs to try again.

Sign-in error codes

If you need more specifics to research, you can use the [sign-in error code](#) for further research.

- Enter the error code into the [Error code lookup tool](#) to get the error code description and remediation information.
- Search for an error code in the [sign-ins error codes reference](#).

The following error codes are associated with sign-in events, but this list isn't exhaustive:

- **50058:** User is authenticated but not yet signed in.

- This error code appears for sign-in attempts when the user didn't complete the sign-in process.
 - Because the user didn't sign-in completely, the User field might display an Object ID or a globally unique identifier (GUID) instead of a username.
 - In some of these situations, the User ID shows up like "00000000-0000-0000".
- **90025:** An internal Microsoft Entra service hit its retry allowance to sign the user in.
 - This error often happens without the user noticing and is usually resolved automatically.
 - If it persists, have the user sign in again.
- **500121:** User didn't complete the MFA prompt.
 - This error often appears if the user hasn't completed setting up MFA.
 - Instruct the user to complete the setup process through to sign-in.
- **70046:** Session expired or reauthentication check failed.
 - This error can occur if a session token expired or if a reauthentication check failed.
 - A reauthentication check can happen if a Conditional Access policy is enabled to require reauthentication for various sign-in risk levels.

If all else fails, or the issue persists despite taking the recommended course of action, open a support request. For more information, see [how to get support for Microsoft Entra ID](#).

Next steps

- [Sign-ins error codes reference](#)
- [Sign-ins report overview](#)
- [How to use the Sign-in diagnostics](#)

What is the Sign-in diagnostic in Microsoft Entra ID?

Article • 02/26/2025

Determining the reason for a failed sign-in can quickly become a challenging task. You need to analyze what happened during the sign-in attempt, and research the available recommendations to resolve the issue. Ideally, you want to resolve the issue without involving others, such as Microsoft support. If you are in a situation like this, you can use the Sign-in diagnostic in Microsoft Entra ID, a tool that helps you investigate sign-ins in Microsoft Entra ID.

This article gives you an overview of what the Sign-in diagnostic is and how you can use it to troubleshoot sign-in related errors.

Prerequisites

- The least privileged role to use the sign-in diagnostic *from a support request or Diagnose and solve problems* is [Billing Administrator](#).
- To use the sign-in diagnostic *from the sign-in logs*, you ALSO need [Reports Reader](#).
- For a full list of roles, see [Least privileged role by task](#).
- Flagged sign-in events can also be reviewed from the Sign-in diagnostic.
 - Flagged sign-in events are captured *after* a user enabled flagging during their sign-in experience.
 - For more information, see [flagged sign-ins](#).

How does it work?

In Microsoft Entra ID, sign-in attempts are controlled by:

- Who performed a sign-in attempt.
- How a sign-in attempt was performed.

For example, you can configure Conditional Access policies that enable administrators to configure all aspects of the tenant when they sign in from the corporate network. But the same user might be blocked when they sign in to the same account from an untrusted network.

Due to the greater flexibility of the system to respond to a sign-in attempt, you might end up in scenarios where you need to troubleshoot sign-ins. The Sign-in diagnostic tool enables diagnosis of sign-in issues by:

- Analyzing data from sign-in events and flagged sign-ins.
- Displaying information about what happened.

- Providing recommendations to resolve problems.

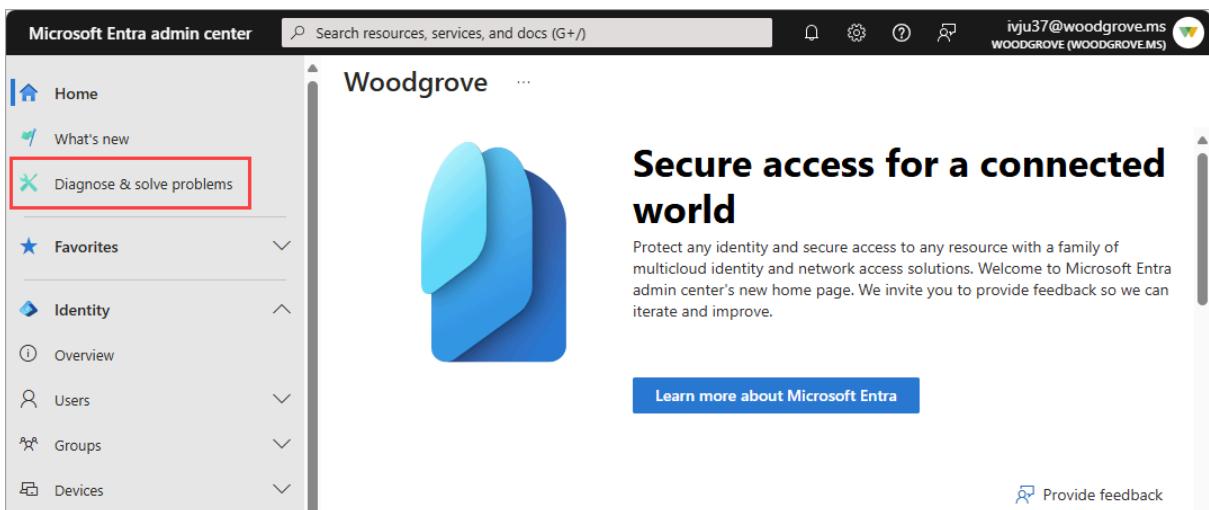
How to access the Sign-in diagnostic

There are three ways to access the Sign-in diagnostic in Microsoft Entra ID. Select a tab to learn about each method.

From Diagnose and Solve Problems

You can start the Sign-in diagnostic from the **Diagnose and Solve Problems** area of Microsoft Entra ID. From Diagnose and Solve Problems you can review any flagged sign-in events or search for a specific sign-in event. You can also start this process from the Conditional Access Diagnose and Solve Problems area.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Global Reader**.
2. Browse to **Diagnose & solve problems** at the top of the left-hand navigation.



The screenshot shows the Microsoft Entra admin center homepage. On the left, there is a navigation sidebar with links like Home, What's new, and a prominent 'Diagnose & solve problems' link, which is highlighted with a red box. To the right, there is a large blue graphic of overlapping shapes and the text 'Woodgrove'. Below the graphic, the heading 'Secure access for a connected world' is displayed, followed by a brief description and a 'Learn more about Microsoft Entra' button. At the bottom right of the page, there is a 'Provide feedback' link.

- You can also access **Diagnose & solve problems** from Conditional Access, Users, Groups, Identity Protection, and Multifactor authentication.

3. Select the **Troubleshoot** link on the **Sign-in Diagnostic** tile.



Sign-in Diagnostic

Use the diagnostic to analyze what happened during a sign-in and what actions you can take to resolve problems.

[Troubleshoot](#)

4. Select the **All Sign-In Events** tab to start a search.

- In some cases, the system automatically starts looking for flagged sign-in events. If nothing is found, you're redirected to the **All Sign-In Events** tab.

5. Enter as many details as possible into the search fields.

- **User:** Provide the name or email address of who made the sign-in attempt.
- **Application:** Provide the application display name or application ID.
- **correlationId** or **requestId**: These details can be found in the error report or the sign-in log details.
- **Date and time:** Provide a date and time to find sign-in events that occurred within 48 hours.

6. Select the **Next** button.

7. Explore the results and take action as necessary.

How to use the diagnostic results

After the Sign-in diagnostic completes its search, a few things appear on the screen.

The **Authentication summary** lists all of the events that match the details you provided. Select the **View Columns** option in the upper-right corner of the summary to change the columns that appear.

Diagnose and solve problems ...

| Start Over | New Support Request | Got feedback?

Sign-in Diagnostic: Review Sign-ins

Flagged Sign-In Events All Sign-In Events

Authentication summary			
createdDateTime	userDisplayName	userPrincipalName	appDisplayName
<input checked="" type="checkbox"/> 2024-09-19T18:39:13Z	Bjarne Kollerud	bjakoll@microsoftlearnsecuritydocs.onmicrosoft.com	Azure Portal

The **Diagnostic results** describe what happened during the sign-in events.

- Scenarios could include MFA requirements from a Conditional Access policy, sign-in events that might need to have a Conditional Access policy applied, or a large number of failed sign-in attempts over the past 48 hours.
- Related content and links to troubleshooting tools might be provided.
- Read through the results to identify any actions that you can take.
- Because it's not always possible to resolve issues without more help, a recommended step might be to open a support ticket.



Based on the information you provided the user Anika Markunaite was trying to sign into My Profile but the user sign-in was interrupted for required setup of Multi-Factor Authentication (MFA).

The MFA requirement was from Conditional Access policy. If the MFA requirement is unexpected or the client cannot use MFA for some reason you may edit the policy or policies. Microsoft recommends MFA be used for all user sign-ins.

The setup requirement can happen when the user is required to set MFA up for the first time or when an admin has set their account to require a new proofup for some reason.

This interrupt can be avoided next time by having the user finish the MFA setup in the next sign in attempt (also known as "proofup"). If the user has not finished the MFA setup you can direct them to <https://mysignins.microsoft.com/security-info>. This means the user would simply configure and verify the additional authentication methods for MFA. For example, if texting is the method the user would have to get the code on their phone and then enter it into the setup page.

After proofup is done the user will be able to sign-in for the application they were trying to use.

In this case we did not see any successful sign-ins into My Profile from the user thereafter.

Common scenarios

Review the tips in the following section for some common scenarios where the sign-in diagnostic can provide helpful troubleshooting information.

Conditional Access

Conditional Access policies are used to apply the right access controls when needed to keep your organization secure. Because Conditional Access policies can be used to grant or block access to resources, they often show up in the sign-in diagnostic.

- **Blocked by Conditional Access:** Your Conditional Access policies prevented the user from signing in.
- **Failed Conditional Access:** It's possible your Conditional Access policies are too strict. Review your configurations for complete sets of users, groups, and apps. Make sure you understand the implications of restricting access from certain types of devices.
- **Multifactor authentication (MFA) from Conditional Access:** Your Conditional Access policies triggered the MFA process for the user.
- **B2B blocked sign-in due to Conditional Access:** You have a Conditional Access policy in place to block external identities from signing in.

Multifactor authentication

There are several multifactor authentication (MFA) related events that you can troubleshoot using the sign-in diagnostic tool.

- **MFA from other requirements:** If the results showed MFA from a requirement other than Conditional Access, you might have MFA enabled on a per-user basis. We [recommend converting per-user MFA to Conditional Access](#). The sign-in diagnostic provides details around the source of the MFA interruption and the result of the interaction.
- **MFA "proofup":** MFA interrupted the sign-in attempt, so information about "proofup" is provided in the diagnostic results. This error appears when users are setting up MFA for the first time and don't complete the setup or their configuration wasn't set up ahead of time.

The screenshot shows a 'Diagnostic Results' page with a purple header bar containing a wrench icon and the text 'Diagnostic Results'. Below the header, the main content area contains the following text:

Based on the information you provided the user Anika Markunaite was trying to sign into My Profile but the user sign-in was interrupted for required setup of Multi-Factor Authentication (MFA).

The MFA requirement was from Conditional Access policy. If the MFA requirement is unexpected or the client cannot use MFA for some reason you may edit the policy or policies. Microsoft recommends MFA be used for all user sign-ins.

The setup requirement can happen when the user is required to set MFA up for the first time or when an admin has set their account to require a new proofup for some reason.

This interrupt can be avoided next time by having the user finish the MFA setup in the next sign in attempt (also known as "proofup"). If the user has not finished the MFA setup you can direct them to <https://mysignins.microsoft.com/security-info>. This means the user would simply configure and verify the additional authentication methods for MFA. For example, if texting is the method the user would have to get the code on their phone and then enter it into the setup page.

After proofup is done the user will be able to sign-in for the application they were trying to use.

In this case we did not see any successful sign-ins into My Profile from the user thereafter.

- **Correct & incorrect credentials:** Sometimes users just enter the wrong credentials. The sign-in diagnostic tool can help distinguish between human error and other issues.
- **Successful sign-in:** In some cases, you want to know if sign-in events *aren't* interrupted by Conditional Access or MFA, but they *should* be. The sign-in diagnostic tool provides details about sign-in events that should be interrupted, but aren't.
- **Account locked:** A user attempted to sign in with incorrect credentials too many times. The diagnostic results help determine where the attempts are coming from and if they're legitimate user sign-in attempts or not. Details about the apps, the number of attempts, the device used, the operating system, and the IP address are provided. For more information, see [Microsoft Entra Smart Lockout](#).

- **Invalid username or password:** When a user attempts to sign in using an invalid username or password, the sign-in diagnostic provides details about the apps, the number of attempts, the device used, the operating system, and the IP address. This information helps determine if the user entered incorrect credentials or if the application cached an old password and is resubmitting it.

Enterprise apps

In enterprise applications, problems might occur with the identity provider (Microsoft Entra ID) application configuration or the service provider (application service, also known as SaaS application) configuration

- **Enterprise apps service provider:** If the sign-in failed due to a problem with the service provider (application) side of the sign-in flow, the issue is resolved by fixing problems on the application service. You need to sign into the other service and change some configuration per the diagnostic guidance.
- **Enterprise apps configuration:** If the sign-in failed due to a configuration issue on the Microsoft Entra ID side of the application, you need to review and update the configuration of the application in Enterprise Applications.

Security defaults

Sign-in events can be interrupted due to security defaults settings. Security defaults enforce best practice security for your organization. One best practice is to require MFA to be configured and used to prevent password sprays, replay attacks, and phishing attempts from being successful.

For more information, see [What are security defaults?](#).

Error code insights

When an event doesn't have a contextual analysis in the sign-in diagnostic, an updated error code explanation and relevant content might be shown. The error code insights contain detailed text about the scenario, how to remediate the problem, and any content to read regarding the problem.

Legacy authentication

This scenario involves a sign-in event that was blocked or interrupted because the client was attempting to use Legacy (or Basic) Authentication.

Preventing legacy authentication sign-in is recommended as the best practice for security. Legacy authentication protocols like POP, SMTP, IMAP, and MAPI can't enforce MFA, which makes them preferred entry points for adversaries to attack your organization.

For more information, see [How to block legacy authentication to Microsoft Entra ID with Conditional Access](#).

B2B blocked sign-in due to Conditional Access

This diagnostic scenario detects a blocked or interrupted sign-in due to the user being from another organization. For example, a B2B sign-in, where a Conditional Access policy requires that the client's device is joined to the resource tenant.

For more information, see [Conditional Access for B2B collaboration users](#).

Blocked by risk policy

This scenario is where risk-based Conditional Access policies block a sign-in attempt because the sign-in attempt was identified as risky.

For more information, see [How to configure and enable risk policies](#).

Pass through authentication

Because pass through authentication is an integration of on premises and cloud authentication technologies, it can be difficult to determine where the problem lies. This diagnostic is intended to make these scenarios easier to diagnose and resolve.

This diagnostic scenario identifies user specific sign-in issues when the authentication method being used is pass through authentication (PTA) and there's a PTA specific error. Errors due to other problems—even when PTA authentication is being used—will still be diagnosed correctly.

The diagnostic results show contextual information about the failure and the user signing in. The results could show other reasons why the sign-in failed, and recommended actions the admin can take to resolve the problem. For more information, see [Microsoft Entra Connect: Troubleshoot Pass-through Authentication](#).

Seamless single sign-on

Seamless single sign-on integrates Kerberos authentication with cloud authentication. Because this scenario involves two authentication protocols, it can be difficult to understand where a

failure point lies when sign-in problems occur. This diagnostic is intended to make these scenarios easier to diagnose and resolve.

This diagnostic scenario examines the context of the sign-in failure and specific failure cause. The diagnostic results could include contextual information on the sign-in attempt, and suggested actions the admin can take. For more information, see [Troubleshoot Microsoft Entra seamless single sign-on](#).

Related content

- [Sign in diagnostics for Microsoft Entra scenarios](#)
- [Learn about flagged sign-ins](#)
- [Troubleshoot sign-in errors](#)

What is the Sign-in diagnostic in Microsoft Entra ID?

Article • 02/26/2025

Determining the reason for a failed sign-in can quickly become a challenging task. You need to analyze what happened during the sign-in attempt, and research the available recommendations to resolve the issue. Ideally, you want to resolve the issue without involving others, such as Microsoft support. If you are in a situation like this, you can use the Sign-in diagnostic in Microsoft Entra ID, a tool that helps you investigate sign-ins in Microsoft Entra ID.

This article gives you an overview of what the Sign-in diagnostic is and how you can use it to troubleshoot sign-in related errors.

Prerequisites

- The least privileged role to use the sign-in diagnostic *from a support request or Diagnose and solve problems* is [Billing Administrator](#).
- To use the sign-in diagnostic *from the sign-in logs*, you ALSO need [Reports Reader](#).
- For a full list of roles, see [Least privileged role by task](#).
- Flagged sign-in events can also be reviewed from the Sign-in diagnostic.
 - Flagged sign-in events are captured *after* a user enabled flagging during their sign-in experience.
 - For more information, see [flagged sign-ins](#).

How does it work?

In Microsoft Entra ID, sign-in attempts are controlled by:

- Who performed a sign-in attempt.
- How a sign-in attempt was performed.

For example, you can configure Conditional Access policies that enable administrators to configure all aspects of the tenant when they sign in from the corporate network. But the same user might be blocked when they sign in to the same account from an untrusted network.

Due to the greater flexibility of the system to respond to a sign-in attempt, you might end up in scenarios where you need to troubleshoot sign-ins. The Sign-in diagnostic tool enables diagnosis of sign-in issues by:

- Analyzing data from sign-in events and flagged sign-ins.
- Displaying information about what happened.

- Providing recommendations to resolve problems.

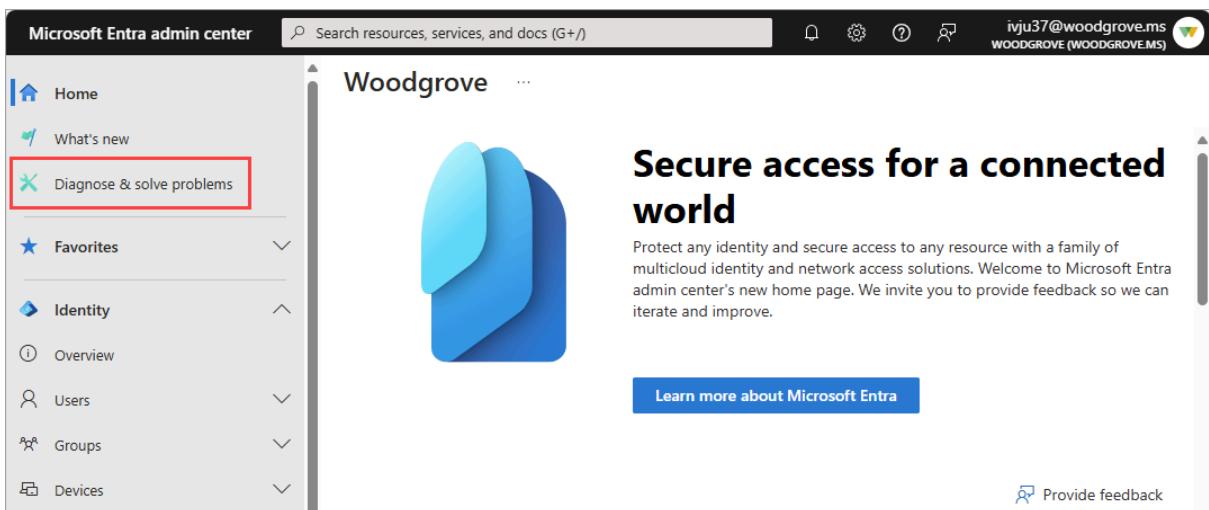
How to access the Sign-in diagnostic

There are three ways to access the Sign-in diagnostic in Microsoft Entra ID. Select a tab to learn about each method.

From Diagnose and Solve Problems

You can start the Sign-in diagnostic from the **Diagnose and Solve Problems** area of Microsoft Entra ID. From Diagnose and Solve Problems you can review any flagged sign-in events or search for a specific sign-in event. You can also start this process from the Conditional Access Diagnose and Solve Problems area.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Global Reader**.
2. Browse to **Diagnose & solve problems** at the top of the left-hand navigation.



The screenshot shows the Microsoft Entra admin center homepage. On the left, there is a navigation sidebar with links like Home, What's new, and a prominent 'Diagnose & solve problems' link, which is highlighted with a red box. To the right, there is a large blue graphic of overlapping shapes and the text 'Woodgrove'. Below the graphic, the heading 'Secure access for a connected world' is displayed, followed by a brief description and a 'Learn more about Microsoft Entra' button. At the bottom right of the page, there is a 'Provide feedback' link.

- You can also access **Diagnose & solve problems** from Conditional Access, Users, Groups, Identity Protection, and Multifactor authentication.

3. Select the **Troubleshoot** link on the **Sign-in Diagnostic** tile.



Sign-in Diagnostic

Use the diagnostic to analyze what happened during a sign-in and what actions you can take to resolve problems.

[Troubleshoot](#)

4. Select the **All Sign-In Events** tab to start a search.

- In some cases, the system automatically starts looking for flagged sign-in events. If nothing is found, you're redirected to the **All Sign-In Events** tab.

5. Enter as many details as possible into the search fields.

- **User:** Provide the name or email address of who made the sign-in attempt.
- **Application:** Provide the application display name or application ID.
- **correlationId** or **requestId**: These details can be found in the error report or the sign-in log details.
- **Date and time:** Provide a date and time to find sign-in events that occurred within 48 hours.

6. Select the **Next** button.

7. Explore the results and take action as necessary.

How to use the diagnostic results

After the Sign-in diagnostic completes its search, a few things appear on the screen.

The **Authentication summary** lists all of the events that match the details you provided. Select the **View Columns** option in the upper-right corner of the summary to change the columns that appear.

Diagnose and solve problems ...

| Start Over | New Support Request | Got feedback?

Sign-in Diagnostic: Review Sign-ins

Flagged Sign-In Events All Sign-In Events

Authentication summary			
createdDateTime	userDisplayName	userPrincipalName	appDisplayName
<input checked="" type="checkbox"/> 2024-09-19T18:39:13Z	Bjarne Kollerud	bjakoll@microsoftlearnsecuritydocs.onmicrosoft.com	Azure Portal

The **Diagnostic results** describe what happened during the sign-in events.

- Scenarios could include MFA requirements from a Conditional Access policy, sign-in events that might need to have a Conditional Access policy applied, or a large number of failed sign-in attempts over the past 48 hours.
- Related content and links to troubleshooting tools might be provided.
- Read through the results to identify any actions that you can take.
- Because it's not always possible to resolve issues without more help, a recommended step might be to open a support ticket.



Based on the information you provided the user Anika Markunaite was trying to sign into My Profile but the user sign-in was interrupted for required setup of Multi-Factor Authentication (MFA).

The MFA requirement was from Conditional Access policy. If the MFA requirement is unexpected or the client cannot use MFA for some reason you may edit the policy or policies. Microsoft recommends MFA be used for all user sign-ins.

The setup requirement can happen when the user is required to set MFA up for the first time or when an admin has set their account to require a new proofup for some reason.

This interrupt can be avoided next time by having the user finish the MFA setup in the next sign in attempt (also known as "proofup"). If the user has not finished the MFA setup you can direct them to <https://mysignins.microsoft.com/security-info>. This means the user would simply configure and verify the additional authentication methods for MFA. For example, if texting is the method the user would have to get the code on their phone and then enter it into the setup page.

After proofup is done the user will be able to sign-in for the application they were trying to use.

In this case we did not see any successful sign-ins into My Profile from the user thereafter.

Common scenarios

Review the tips in the following section for some common scenarios where the sign-in diagnostic can provide helpful troubleshooting information.

Conditional Access

Conditional Access policies are used to apply the right access controls when needed to keep your organization secure. Because Conditional Access policies can be used to grant or block access to resources, they often show up in the sign-in diagnostic.

- **Blocked by Conditional Access:** Your Conditional Access policies prevented the user from signing in.
- **Failed Conditional Access:** It's possible your Conditional Access policies are too strict. Review your configurations for complete sets of users, groups, and apps. Make sure you understand the implications of restricting access from certain types of devices.
- **Multifactor authentication (MFA) from Conditional Access:** Your Conditional Access policies triggered the MFA process for the user.
- **B2B blocked sign-in due to Conditional Access:** You have a Conditional Access policy in place to block external identities from signing in.

Multifactor authentication

There are several multifactor authentication (MFA) related events that you can troubleshoot using the sign-in diagnostic tool.

- **MFA from other requirements:** If the results showed MFA from a requirement other than Conditional Access, you might have MFA enabled on a per-user basis. We [recommend converting per-user MFA to Conditional Access](#). The sign-in diagnostic provides details around the source of the MFA interruption and the result of the interaction.
- **MFA "proofup":** MFA interrupted the sign-in attempt, so information about "proofup" is provided in the diagnostic results. This error appears when users are setting up MFA for the first time and don't complete the setup or their configuration wasn't set up ahead of time.

The screenshot shows a 'Diagnostic Results' page with a purple header bar containing a wrench icon and the text 'Diagnostic Results'. Below the header, the main content area contains the following text:

Based on the information you provided the user Anika Markunaite was trying to sign into My Profile but the user sign-in was interrupted for required setup of Multi-Factor Authentication (MFA).

The MFA requirement was from Conditional Access policy. If the MFA requirement is unexpected or the client cannot use MFA for some reason you may edit the policy or policies. Microsoft recommends MFA be used for all user sign-ins.

The setup requirement can happen when the user is required to set MFA up for the first time or when an admin has set their account to require a new proofup for some reason.

This interrupt can be avoided next time by having the user finish the MFA setup in the next sign in attempt (also known as "proofup"). If the user has not finished the MFA setup you can direct them to <https://mysignins.microsoft.com/security-info>. This means the user would simply configure and verify the additional authentication methods for MFA. For example, if texting is the method the user would have to get the code on their phone and then enter it into the setup page.

After proofup is done the user will be able to sign-in for the application they were trying to use.

In this case we did not see any successful sign-ins into My Profile from the user thereafter.

- **Correct & incorrect credentials:** Sometimes users just enter the wrong credentials. The sign-in diagnostic tool can help distinguish between human error and other issues.
- **Successful sign-in:** In some cases, you want to know if sign-in events *aren't* interrupted by Conditional Access or MFA, but they *should* be. The sign-in diagnostic tool provides details about sign-in events that should be interrupted, but aren't.
- **Account locked:** A user attempted to sign in with incorrect credentials too many times. The diagnostic results help determine where the attempts are coming from and if they're legitimate user sign-in attempts or not. Details about the apps, the number of attempts, the device used, the operating system, and the IP address are provided. For more information, see [Microsoft Entra Smart Lockout](#).

- **Invalid username or password:** When a user attempts to sign in using an invalid username or password, the sign-in diagnostic provides details about the apps, the number of attempts, the device used, the operating system, and the IP address. This information helps determine if the user entered incorrect credentials or if the application cached an old password and is resubmitting it.

Enterprise apps

In enterprise applications, problems might occur with the identity provider (Microsoft Entra ID) application configuration or the service provider (application service, also known as SaaS application) configuration

- **Enterprise apps service provider:** If the sign-in failed due to a problem with the service provider (application) side of the sign-in flow, the issue is resolved by fixing problems on the application service. You need to sign into the other service and change some configuration per the diagnostic guidance.
- **Enterprise apps configuration:** If the sign-in failed due to a configuration issue on the Microsoft Entra ID side of the application, you need to review and update the configuration of the application in Enterprise Applications.

Security defaults

Sign-in events can be interrupted due to security defaults settings. Security defaults enforce best practice security for your organization. One best practice is to require MFA to be configured and used to prevent password sprays, replay attacks, and phishing attempts from being successful.

For more information, see [What are security defaults?](#).

Error code insights

When an event doesn't have a contextual analysis in the sign-in diagnostic, an updated error code explanation and relevant content might be shown. The error code insights contain detailed text about the scenario, how to remediate the problem, and any content to read regarding the problem.

Legacy authentication

This scenario involves a sign-in event that was blocked or interrupted because the client was attempting to use Legacy (or Basic) Authentication.

Preventing legacy authentication sign-in is recommended as the best practice for security. Legacy authentication protocols like POP, SMTP, IMAP, and MAPI can't enforce MFA, which makes them preferred entry points for adversaries to attack your organization.

For more information, see [How to block legacy authentication to Microsoft Entra ID with Conditional Access](#).

B2B blocked sign-in due to Conditional Access

This diagnostic scenario detects a blocked or interrupted sign-in due to the user being from another organization. For example, a B2B sign-in, where a Conditional Access policy requires that the client's device is joined to the resource tenant.

For more information, see [Conditional Access for B2B collaboration users](#).

Blocked by risk policy

This scenario is where risk-based Conditional Access policies block a sign-in attempt because the sign-in attempt was identified as risky.

For more information, see [How to configure and enable risk policies](#).

Pass through authentication

Because pass through authentication is an integration of on premises and cloud authentication technologies, it can be difficult to determine where the problem lies. This diagnostic is intended to make these scenarios easier to diagnose and resolve.

This diagnostic scenario identifies user specific sign-in issues when the authentication method being used is pass through authentication (PTA) and there's a PTA specific error. Errors due to other problems—even when PTA authentication is being used—will still be diagnosed correctly.

The diagnostic results show contextual information about the failure and the user signing in. The results could show other reasons why the sign-in failed, and recommended actions the admin can take to resolve the problem. For more information, see [Microsoft Entra Connect: Troubleshoot Pass-through Authentication](#).

Seamless single sign-on

Seamless single sign-on integrates Kerberos authentication with cloud authentication. Because this scenario involves two authentication protocols, it can be difficult to understand where a

failure point lies when sign-in problems occur. This diagnostic is intended to make these scenarios easier to diagnose and resolve.

This diagnostic scenario examines the context of the sign-in failure and specific failure cause. The diagnostic results could include contextual information on the sign-in attempt, and suggested actions the admin can take. For more information, see [Troubleshoot Microsoft Entra seamless single sign-on](#).

Related content

- [Sign in diagnostics for Microsoft Entra scenarios](#)
- [Learn about flagged sign-ins](#)
- [Troubleshoot sign-in errors](#)

View applied Conditional Access details in the Microsoft Entra activity logs

Article • 11/21/2024

With Conditional Access policies, you can control how your users get access to your Azure and Microsoft Entra resources. As a tenant admin, you need to be able to determine what effect your Conditional Access policies have on sign-ins to your tenant, so that you can take action if necessary. You might also need to view audit logs for recent changes to Conditional Access policies.

This article explains how to view applied Conditional Access policies in the Microsoft Entra activity logs.

Prerequisites

To see applied Conditional Access policies in the logs, administrators must have permissions to view *both* the logs and the policies. The least privileged built-in role that grants *both* permissions is *Security Reader*. As a best practice, you should add the Security Reader role to the related administrator accounts.

The following built-in roles grant permissions to *read Conditional Access policies*:

- Security Reader
- Security Administrator
- Conditional Access Administrator

The following built-in roles grant permission to *view activity logs*:

- Reports Reader
- Security Reader
- Security Administrator

Permissions

If you use a client app or the Microsoft Graph PowerShell module to pull logs from Microsoft Graph, your app needs permissions to receive the `AppliedConditionalAccessPolicy` resource from Microsoft Graph. As a best practice, assign `Policy.Read.ConditionalAccess` because it's the least privileged permission.

The following permissions allow a client app to access the activity logs and any applied Conditional Access policies in the logs through Microsoft Graph:

- `Policy.Read.ConditionalAccess`
- `Policy.ReadWrite.ConditionalAccess`
- `Policy.Read.All`
- `AuditLog.Read.All`
- `Directory.Read.All`

To use the Microsoft Graph PowerShell module, you also need the following least privileged permissions with the necessary access:

- To consent to the necessary permissions: `Connect-MgGraph -Scopes Policy.Read.ConditionalAccess, AuditLog.Read.All, Directory.Read.All`
- To view the sign-in logs: `Get-MgAuditLogSignIn`
- To view the audit logs: `Get-MgAuditLogDirectoryAudit`

For more information, see [Get-MgAuditLogSignIn](#) and [Get-MgAuditLogDirectoryAudit](#).

Conditional Access and sign-in log scenarios

As a Microsoft Entra administrator, you can use the sign-in logs to:

- Troubleshoot sign-in problems.
- Check on feature performance.
- Evaluate the security of a tenant.

Some scenarios require you to get an understanding of how your Conditional Access policies were applied to a sign-in event. Common examples include:

- Helpdesk administrators who need to look at applied Conditional Access policies to understand if a policy is the root cause of a ticket that a user opened.
- Tenant administrators who need to verify that Conditional Access policies have the intended effect on the users of a tenant.

You can access the sign-in logs by using the Microsoft Entra admin center, the Azure portal, Microsoft Graph, and PowerShell.

How to view Conditional Access policies

💡 Tip

Steps in this article might vary slightly based on the portal you start from.

The activity details of sign-in logs contain several tabs. The **Conditional Access** tab lists the Conditional Access policies applied to that sign-in event.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Sign-in logs**.
3. Select a sign-in item from the table to view the sign-in details pane.
4. Select the **Conditional Access** tab.

If you don't see the Conditional Access policies, confirm you're using a role that provides access to both the sign-in logs and the Conditional Access policies.

Conditional Access and audit log scenarios

The Microsoft Entra audit logs contain information about changes to Conditional Access policies. You can use the audit logs to find out when a policy was created, updated, or deleted.

To see when an existing Conditional Access policy was updated:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Audit logs**.
3. Set **Service** filter to **Conditional Access**.
4. Set the **Category** filter to **Policy**.
5. Set the **Activity** filter to **Update conditional access policy**.

You might need to adjust the date to see the changes you're looking for. The **Target** column shows the name of the Conditional Access policy that was updated.

To compare the current policy with the previous policy, select the audit log entry and then select the **Modified properties** tab.

Related content

- [Troubleshoot Conditional Access related sign-in problems](#)
- [Review the Conditional Access sign-in logs FAQs](#)
- [Learn about the sign-in logs](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Use audit logs to troubleshoot Conditional Access policy changes

Article • 04/25/2025

The Microsoft Entra audit log is a valuable source of information when troubleshooting why and how Conditional Access policy changes happened in your environment.

Audit log data is only kept for 30 days by default, which might not be long enough for every organization. Organizations can store data for longer periods by changing diagnostic settings in Microsoft Entra ID to:

- Send data to a Log Analytics workspace
- Archive data to a storage account
- Stream data to Event Hubs
- Send data to a partner solution

Find these options under **Entra ID > Monitoring & health > Diagnostic settings > Edit setting**. If you don't have a diagnostic setting, follow the instructions in the article [Create diagnostic settings to send platform logs and metrics to different destinations](#) to create one.

Use the audit log

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Entra ID > Monitoring & health > Audit logs**.
3. Select the **Date** range you want to query.
4. From the **Service** filter, select **Conditional Access** and select the **Apply** button.

The audit logs display all activities, by default. Open the **Activity** filter to narrow down the activities. For a full list of the audit log activities for Conditional Access, see the [Audit log activities](#).

5. To view the details, select a row. The **Modified Properties** tab lists the modified JSON values for the selected audit activity.

Searched for "Audit Log Details" in Microsoft Entra admin center.

The screenshot shows the Audit Log Details page with the following details:

- Audit Logs** section is selected.
- Modified Properties** tab is selected in the top navigation bar.
- Target**: access pol... (ConditionalAccess)
- Property Name**: ConditionalAcc...
- Old Value**: A complex JSON object representing a Conditional Access policy.
- New Value**: A complex JSON object representing a modified Conditional Access policy, showing changes like adding "mfa" as a grant control.

The table below lists audit log entries:

Date	Service
3/22/24, 12:18:28 PM	Conditional Access
3/22/24, 12:07:09 PM	Conditional Access

Use Log Analytics

Log Analytics allows organizations to query data using built in queries or custom created Kusto queries, for more information, see [Get started with log queries in Azure Monitor](#).

The screenshot shows the Microsoft Azure Log Analytics interface. The left sidebar navigation bar includes links for Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Security, Monitoring, Sign-in logs, Audit logs, Provisioning logs, and Log Analytics (which is highlighted with a red box). The main content area displays a query editor with the following query:

```
1 AuditLogs  
2 | where OperationName == "Update conditional access policy"
```

The results pane shows a table with the following data:

TimeGenerated [Local Time]	ResourceId
2023-10-12T12:00:00Z	IPCGraph_f5afdf5ee-0e51-409f-829f-46b25bb6006a_YA45U_6628328
2023-10-12T12:00:00Z	InitiatedBy
2023-10-12T12:00:00Z	LoggedByService
2023-10-12T12:00:00Z	Result
2023-10-12T12:00:00Z	ResultReason
2023-10-12T12:00:00Z	TargetResources
2023-10-12T12:00:00Z	0
2023-10-12T12:00:00Z	administrativeUnits
2023-10-12T12:00:00Z	displayName
2023-10-12T12:00:00Z	id
2023-10-12T12:00:00Z	modifiedProperties
2023-10-12T12:00:00Z	0
2023-10-12T12:00:00Z	displayName
2023-10-12T12:00:00Z	newValue
2023-10-12T12:00:00Z	oldValue

The results table shows two rows of data. The first row corresponds to the 'TargetResources' field in the query, and the second row corresponds to the 'modifiedProperties' field.

Once enabled find access to Log Analytics in the **Entra ID > Monitoring & health > Log Analytics**. The table of most interest to Conditional Access Administrators is **AuditLogs**.

Kusto

AuditLogs

```
| where OperationName == "Update Conditional Access policy"
```

Changes can be found under **TargetResources > modifiedProperties**.

Reading the values

The old and new values from the audit log and Log Analytics are in JSON format. Compare the two values to see the changes to the policy.

Old policy example:

JSON

```
{
  "conditions": {
    "applications": {
      "applicationFilter": null,
      "excludeApplications": [
      ],
      "includeApplications": [
        "797f4846-ba00-4fd7-ba43-dac1f8f63013"
      ],
      "includeAuthenticationContextClassReferences": [
      ],
      "includeUserActions": [
      ]
    },
    "clientAppTypes": [
      "browser",
      "mobileAppsAndDesktopClients"
    ],
    "servicePrincipalRiskLevels": [
    ],
    "signInRiskLevels": [
    ],
    "userRiskLevels": [
    ],
    "users": {
      "excludeGroups": [
        "eedad040-3722-4bcb-bde5-bc7c857f4983"
      ],
      "excludeRoles": [
      ],
      "excludeUsers": [
      ]
    }
  }
}
```

```

        ],
        "includeGroups": [
        ],
        "includeRoles": [
        ],
        "includeUsers": [
            "All"
        ]
    }
},
"displayName": "Common Policy - Require MFA for Azure management",
"grantControls": {
    "builtInControls": [
        "mfa"
    ],
    "customAuthenticationFactors": [
    ],
    "operator": "OR",
    "termsOfUse": [
        "a0d3eb5b-6cbe-472b-a960-0baacbd02b51"
    ]
},
"id": "334e26e9-9622-4e0a-a424-102ed4b185b3",
"modifiedDateTime": "2021-08-09T17:52:40.781994+00:00",
"state": "enabled"
}

```

Updated policy example:

JSON

```
{
    "conditions": {
        "applications": {
            "applicationFilter": null,
            "excludeApplications": [
            ],
            "includeApplications": [
                "797f4846-ba00-4fd7-ba43-dac1f8f63013"
            ],
            "includeAuthenticationContextClassReferences": [
            ],
            "includeUserActions": [
            ]
        },
        "clientAppTypes": [
            "browser",
            "mobileAppsAndDesktopClients"
        ],
        "servicePrincipalRiskLevels": [
        ],
        "signInRiskLevels": [

```

```
        ],
        "userRiskLevels": [
        ],
        "users": {
            "excludeGroups": [
                "eedad040-3722-4bcb-bde5-bc7c857f4983"
            ],
            "excludeRoles": [
            ],
            "excludeUsers": [
            ],
            "includeGroups": [
            ],
            "includeRoles": [
            ],
            "includeUsers": [
                "All"
            ]
        }
    },
    "displayName": "Common Policy - Require MFA for Azure management",
    "grantControls": {
        "builtInControls": [
            "mfa"
        ],
        "customAuthenticationFactors": [
        ],
        "operator": "OR",
        "termsOfUse": [
        ]
    },
    "id": "334e26e9-9622-4e0a-a424-102ed4b185b3",
    "modifiedDateTime": "2021-08-09T17:52:54.9739405+00:00",
    "state": "enabled"
}
```

In the previous example, the updated policy doesn't include terms of use in grant controls.

Related content

- [What is Microsoft Entra monitoring?](#)
- [Install and use the log analytics views for Microsoft Entra ID](#)

Troubleshooting sign-in problems with Conditional Access

Article • 03/04/2025

Use this article to troubleshoot unexpected sign-in outcomes related to Conditional Access using error messages and Microsoft Entra sign-in logs.

Select "all" consequences

The Conditional Access framework provides great configuration flexibility. However, great flexibility also means that you should carefully review each configuration policy before releasing it to avoid undesirable results. In this context, pay special attention to assignments affecting complete sets such as **all users / groups / cloud apps**.

Organizations should avoid the following configurations:

For all users, all resources:

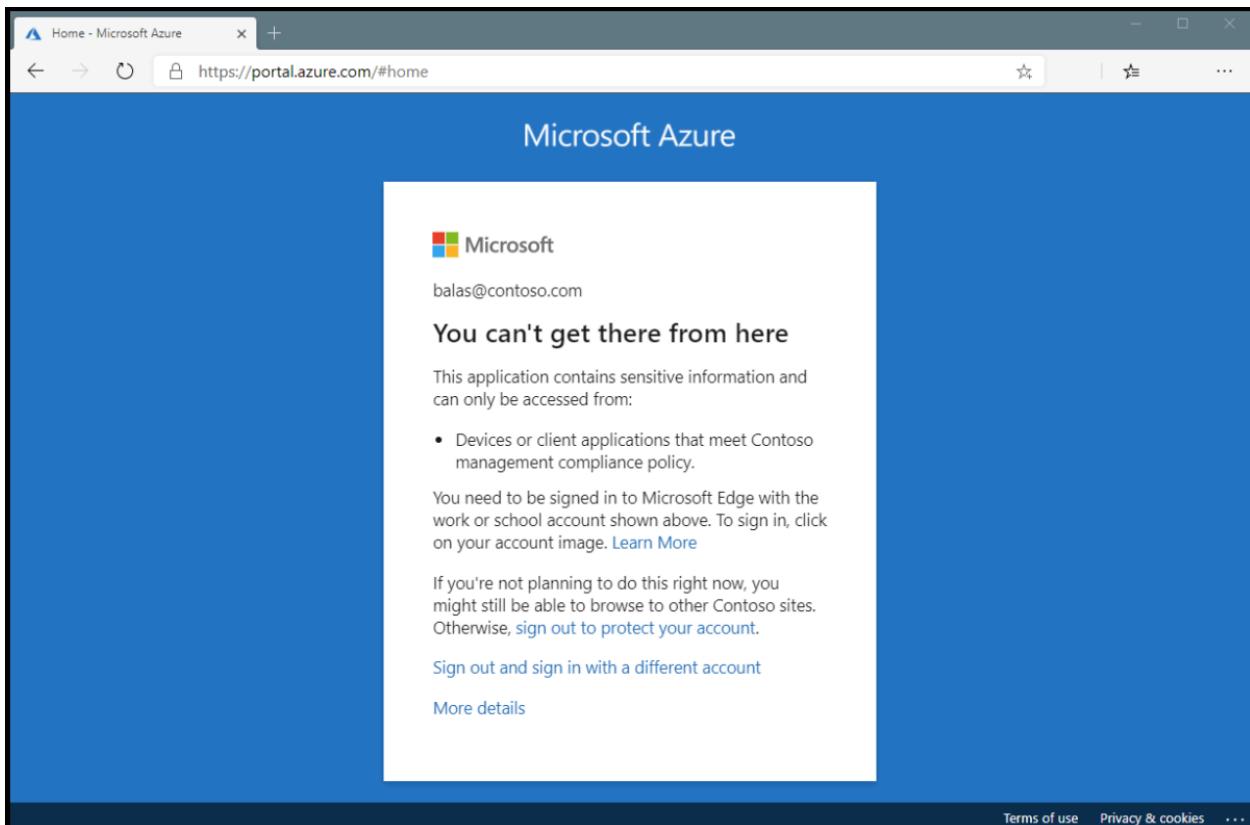
- **Block access** - This configuration blocks the entire organization.
- **Require device to be marked as compliant** - For users that haven't enrolled their devices yet, this policy blocks all access including access to the Intune portal. If you're an administrator without an enrolled device, this policy blocks you from getting back in to change the policy.
- **Require Hybrid Microsoft Entra domain joined device** - This policy also has the potential to block access for all users in your organization if they don't have a Microsoft Entra hybrid joined device.
- **Require app protection policy** - This policy also has the potential to block access for all users in your organization if you don't have an Intune policy. If you're an administrator without a client application that has an Intune app protection policy, this policy blocks you from getting back into portals such as Intune and Azure.

For all users, all resources, all device platforms:

- **Block access** - This configuration blocks your entire organization.

Conditional Access sign-in interrupt

Review the error message that appears. For problems signing in when using a web browser, the error page itself has detailed information. This information alone might describe the problem and suggest a solution.

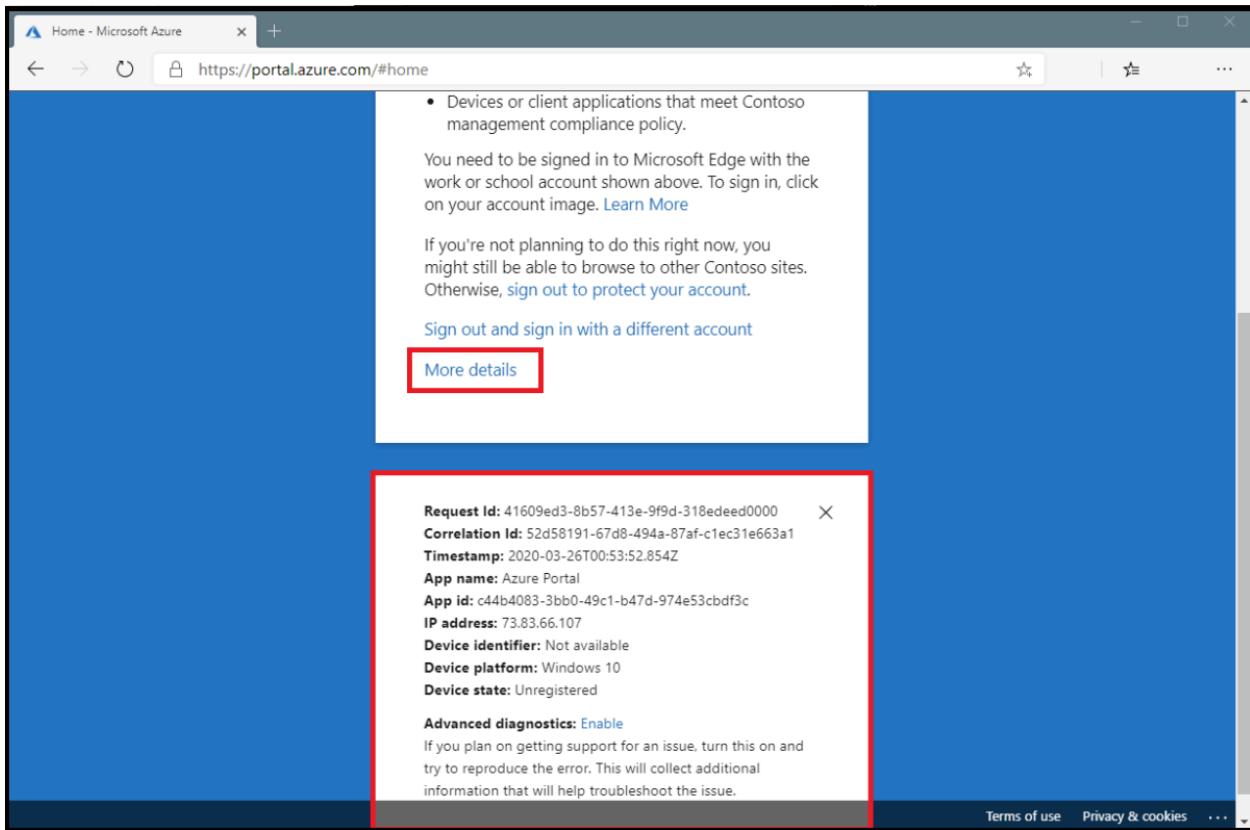


In the above error, the message states that the application can only be accessed from devices or client applications that meet the company's mobile device management policy. In this case, the application and device don't meet the policy.

Microsoft Entra sign-in events

The second method to get detailed information about the sign-in interruption is to review the Microsoft Entra sign-in events to see which Conditional Access policy or policies were applied and why.

More information can be found about the problem by clicking **More Details** in the initial error page. Clicking **More Details** reveals troubleshooting information that is helpful when searching the Microsoft Entra sign-in events for the specific failure event the user saw or when opening a support incident with Microsoft.



To find out which Conditional Access policy or policies applied and why, follow these steps.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Identity > Monitoring & health > Sign-in logs**.
3. Find the event for the sign-in to review. Add or remove filters and columns to filter out unnecessary information.
 - a. Narrow the scope by adding filters like:
 - i. **Correlation ID** when you have a specific event to investigate.
 - ii. **Conditional Access** to see policy failure and success. Scope your filter to show only failures to limit results.
 - iii. **Username** to see information related to specific users.
 - iv. **Date** scoped to the time frame in question.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is collapsed, and the main area is titled "Sign-in events". At the top right, there are download, export, troubleshoot, refresh, column settings, and feedback links. A message box says "Want to switch back to the default sign-ins experience? Click here to leave the preview." Below this, there are filter buttons for date (Last 24 hours), show dates as (Local), status (Failure, highlighted with a red box), and add filters. The table below has tabs for User sign-ins (interactive), User sign-ins (non-interactive), Service principal sign-ins, and Managed identity. The "User sign-ins (interactive)" tab is selected. The columns are Date, Request ID, User, Application, and Status. One row is shown: Date 3/21/2024, 1:01:18 PM, Request ID a0a0a0a0-bbbb-ccc..., User MOD Administrator, Application Microsoft App Acces..., Status Failure.

4. After finding the sign-in event that corresponds to the user's sign-in failure, select the **Conditional Access** tab. The Conditional Access tab shows the specific policy or policies that resulted in the sign-in interruption.
 - a. Information in the **Troubleshooting and support** tab might provide a clear reason as to why a sign-in failed such as a device that didn't meet compliance requirements.
 - b. To investigate further, drill down into the configuration of the policies by clicking on the **Policy Name**. Clicking the **Policy Name** shows the policy configuration user interface for the selected policy for review and editing.
 - c. The **client user** and **device details** that were used for the Conditional Access policy assessment are also available in the **Basic Info**, **Location**, **Device Info**, **Authentication Details**, and **Additional Details** tabs of the sign-in event.

Policy not working as intended

Selecting the ellipsis on the right side of the policy in a sign-in event brings up policy details. This option gives administrators additional information about why a policy was successfully applied or not.

The left side provides details collected at sign-in and the right side provides details of whether those details satisfy the requirements of the applied Conditional Access policies. Conditional Access policies only apply when all conditions are satisfied or not configured.

If the information in the event isn't enough to understand the sign-in results or adjust the policy to get desired results, use the sign-in diagnostic tool. The sign-in diagnostic is under **Basic info > Troubleshoot Event**. For more information about the sign-in diagnostic, see [What is the sign-in diagnostic in Microsoft Entra ID](#). You can also [use the What If tool to troubleshoot Conditional Access policies](#).

If you need to submit a support incident, provide the request ID and time and date from the sign-in event in the incident submission details. This information allows Microsoft support to find the specific event you're concerned about.

Common Conditional Access error codes

[Expand table](#)

Sign-in Error Code	Error String
53000	DeviceNotCompliant
53001	DeviceNotDomainJoined
53002	ApplicationUsedIsNotAnApprovedApp
53003	BlockedByConditionalAccess

Sign-in Error Code	Error String
53004	ProofUpBlockedDueToRisk
53009	Application needs to enforce Intune protection policies

More information about error codes can be found in the article [Microsoft Entra authentication and authorization error codes](#). Error codes in the list appear with a prefix of `AADSTS` followed by the code seen in the browser, for example `AADSTS53002`.

Service dependencies

In some scenarios, users are blocked because cloud apps depend on resources blocked by Conditional Access policy.

To determine the service dependency, check the sign-in log for the application and resource called by the sign-in. In the following screenshot, the application called is **Azure Portal** but the resource called is **Windows Azure Service Management API**. To target this scenario appropriately all the applications and resources should be similarly combined in Conditional Access policy.

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date	3/22/2024, 11:56:26 AM				
Request ID	0x00000-0000-0000-x00x-0xxx0x00x0				
Correlation ID	0x00000-0000-0000-x00x-0xxx0x00x0				
Authentication requirement	Single-factor authentication				
Status	Success				
Continuous access evaluation	No				

Follow these steps:

Troubleshoot Event [Launch the Sign-in Diagnostic](#).
1. Review the diagnosis and act on suggested fixes.

User	MOD Administrator
Username	admin@contoso.com
User ID	0x00000-0000-0000-x00x-0xxx0x00x0
Sign-in identifier	admin@contoso.com
User type	Member
Cross tenant access type	None

Application	Azure Portal
Application ID	0x00000-0000-0000-x00x-0xxx0x00x0
Resource	Windows Azure Service Management API
Resource ID	0x00000-0000-0000-x00x-0xxx0x00x0

Resource tenant ID: 0x00000-0000-0000-x00x-0xxx0x00x0
Home tenant ID: 0x00000-0000-0000-x00x-0xxx0x00x0
Home tenant name:

What to do if you're locked out

If you're locked out due to an incorrect setting in a Conditional Access policy:

- Check if there are other administrators in your organization who aren't blocked yet. An administrator with access can disable the policy that is impacting your sign-in.
- If none of the administrators in your organization can update the policy, submit a support request. Microsoft support can review and upon confirmation update the Conditional Access policies that are preventing access.

Next steps

- [Use the What If tool to troubleshoot Conditional Access policies](#)
 - [Sign-in activity reports](#)
 - [Troubleshooting Conditional Access using the What If tool](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Understanding bulk user updates during verified domain changes

Article • 02/25/2025

This article describes a common scenario where the audit logs display many `UserPrincipalName` updates triggered by a verified domain change. This article explains the causes and considerations for UserManagement updates in the audit logs that occur during verified domain changes. The article provides a deep dive into the backend operation that triggers mass object changes in Microsoft Entra ID.

Symptoms

The Microsoft Entra audit logs show multiple user updates occurred in my Microsoft Entra tenant. The **Actor** information for these events is empty or shows N/A.

The bulk updates involve changing the domain for the `UserPrincipalName` changed from the organization's preferred domain to the default `*.onmicrosoft.com` domain suffix.

Sample audit log details

Activity Date (UTC): 2022-01-27 07:44:05

Activity: Update user

Actor Type: Other

Actor UPN: N/A

Status: success

Category: UserManagement

Service: Core Directory

Target Id: aaaaaaaaaa-bbbb-0000-1111-bbbbbbbbbbbb

Target Name: user@contoso.com

Target Type: User

Within the full details of the audit log entry, look for the `modifiedProperties` section. This section shows the changes made to the user object. The `oldValue` and `newValue`

fields show the domain change.

JSON

```
"modifiedProperties":  
  "displayName": "UserPrincipalName",  
  "oldValue": "[\"user@contoso.onmicrosoft.com\"]",  
  "newValue": "[\"user@contoso.com\"]"
```

Causes

One common reason behind mass object changes is due to a nonsynchronous backend operation. This operation determines the appropriate `UserPrincipalName` and `proxyAddresses` that are updated in Microsoft Entra users, groups, or contacts.

The purpose of this backend operation ensures that `UserPrincipalName` and `proxyAddresses` are consistent in Microsoft Entra ID at any time. An explicit change, such as a verified domain change, triggers this operation.

For example, if you add a verified domain Fabrikam.com to your Contoso.onmicrosoft.com tenant, this action triggers the backend operation on *all* objects in the tenant. This event is captured in the Microsoft Entra audit logs as **Update User** events preceded by an **Add verified domain** event.

If Fabrikam.com was removed from the Contoso.onmicrosoft.com tenant, then all the **Update User** events are preceded by a **Remove verified domain** event.

Resolution

If you encountered this issue, you might benefit from using Microsoft Entra Connect to sync data between your on-premises directory and Microsoft Entra ID. This action ensures that the `UserPrincipalName` and `proxyAddresses` are consistent in both environments.

When you try to manually add or maintain these objects, you run the risk of another backend operation triggering a bulk change.

Review the following articles to become familiar with these concepts:

- [Microsoft Entra UserPrincipalName population](#)
- [How the proxyAddresses attribute is populated in Microsoft Entra ID](#)

Considerations

This backend operation doesn't cause changes to certain objects that:

- don't have an active Microsoft Exchange license
- have `MSEchRemoteRecipientType` set to Null
- aren't considered a shared resource

A shared resource is when `CloudMSEchRecipientDisplayType` contains one of the following values:

- `MailboxUser` (shared)
- `PublicFolder`
- `ConferenceRoomMailbox`
- `EquipmentMailbox`
- `ArbitrationMailbox`
- `RoomList`
- `TeamMailboxUser`
- `GroupMailbox`
- `SchedulingMailbox`
- `ACLableMailboxUser`
- `ACLableTeamMailboxUser`

To build more correlation between these two disparate events, Microsoft is working on updating the **Actor** info in the audit logs to identify these changes as triggered by a verified domain change. This action helps check when the verified domain change event took place and started to mass update the objects in the tenant.

In most cases, there are no changes to users as their `UserPrincipalName` and `proxyAddresses` are consistent, so we're working to only display in the audit logs those updates that caused an actual change to the object. This action prevents noise in the audit logs and help admins correlate the remaining user changes to verified domain change events.

Deep dive

Want to learn more about what's happening behind the scenes? Here's a deep dive into the backend operation that triggers mass object changes in Microsoft Entra ID. Before you dive in, check out the [Microsoft Entra Connect Sync service shadow attributes](#) article to understand the shadow attributes.

UserPrincipalName

For cloud-only users, the UserPrincipalName is set to a verified domain suffix. When an inconsistent UserPrincipalName is processed, the operation converts it to the default `onmicrosoft.com` suffix, for example: `username@Contoso.onmicrosoft.com`.

For synchronized users, the UserPrincipalName is set to a verified domain suffix and matches the on-premises value, `ShadowUserPrincipalName`. When an inconsistent UserPrincipalName is processed, the operation reverts to the same value as the `ShadowUserPrincipalName` or, in the case that domain suffix was removed from the tenant, converts it to the default `*.onmicrosoft.com` domain suffix.

ProxyAddresses

For cloud-only users, consistency means that the `proxyAddresses` match a verified domain suffix. When an inconsistent proxyAddresses is processed, the backend operation converts it to the default `*.onmicrosoft.com` domain suffix, for example:

`SMTP:username@Contoso.onmicrosoft.com`.

For synchronized users, consistency means that the proxyAddresses match the on-premises proxyAddresses value (that is, `ShadowProxyAddresses`). The proxyAddresses are expected to be in sync with `ShadowProxyAddresses`. If the synchronized user has an Exchange license assigned, then the cloud and on-premises values must match. These values must also match a verified domain suffix.

In this scenario, the backend operation sanitizes the inconsistent proxyAddresses with an unverified domain suffix and is removed from the object in Microsoft Entra ID. If that unverified domain is verified later, the backend operation recomputes and adds the proxyAddresses from `ShadowProxyAddresses` back to the object in Microsoft Entra ID.

Note

For synchronized objects, to avoid the backend operation logic from calculating unexpected results, it's best to set proxyAddresses to a Microsoft Entra verified domain on the on-premises object.

Related content

[Microsoft Entra Connect Sync service shadow attributes](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra audit log categories and activities

Article • 10/04/2024

Microsoft Entra audit logs collect all traceable activities within your Microsoft Entra tenant. Audit logs can be used to determine who made a change to service, user, group, or other item.

This article provides a comprehensive list of the audit categories and their related activities. To jump to a specific audit category, use the "In this article" section.

Audit log activities and categories change periodically. The tables are updated regularly, but might not be in sync with what is available in Microsoft Entra ID. Provide us with feedback if you think there's a missing audit category or activity.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Audit logs**.
3. Adjust the filters accordingly.
4. To view the details, select a row from the resulting table.

Microsoft Entra (AAD) Management UX

⋮⋮ Expand table

Audit Category	Activity
AdministrativeUnit	Bulk add members to administrative unit - finished (bulk)
AdministrativeUnit	Bulk remove members to administrative unit - finished (bulk)
AdministrativeUnit	started (bulk)
DeviceManagement	Bulk add authentication devices - finished (bulk)
DeviceManagement	Download devices - finished (bulk)
DeviceManagement	started (bulk)
DirectoryManagement	Bulk download hardware tokens - finished (bulk)
DirectoryManagement	Download registration and reset events - finished (bulk)
DirectoryManagement	Download role assignments - finished (bulk)

Audit Category	Activity
DirectoryManagement	Download service principals - finished (bulk)
DirectoryManagement	Download user registration details - finished (bulk)
DirectoryManagement	Download users - finished (bulk)
DirectoryManagement	Export summary data - finished (bulk)
DirectoryManagement	Export summary data new - finished (bulk)
DirectoryManagement	started (bulk)
GroupManagement	Bulk import group members - finished (bulk)
GroupManagement	Bulk remove group members - finished (bulk)
GroupManagement	Download group members - finished (bulk)
GroupManagement	Download groups - finished (bulk)
GroupManagement	started (bulk)
Policy	Add blocked user
Policy	Add bypass user
Policy	Clear block on user
Policy	Remove bypassed user
Policy	Update Sign-In Risk Policy
Policy	Update User Risk and MFA Registration Policy
UserManagement	Bulk create users - finished (bulk)
UserManagement	Bulk delete users - finished (bulk)
UserManagement	Bulk invite users - finished (bulk)
UserManagement	Bulk restore deleted users - finished (bulk)
UserManagement	Download users - finished (bulk)
UserManagement	started (bulk)

Access reviews

With [Microsoft Entra ID Governance access reviews](#), you can ensure users have the appropriate access. Access review audit logs can tell you who initiated or ended an

access review. These logs can also tell you if any access review settings were changed.

 Expand table

Audit Category	Activity
DirectoryManagement	Create program
DirectoryManagement	Link program control
DirectoryManagement	Unlink program control
DirectoryManagement	Update program
Policy	Access review ended
Policy	Apply decision
Policy	Approve decision
Policy	Bulk Approve decisions
Policy	Bulk Deny decisions
Policy	Bulk Reset decisions
Policy	Bulk mark decisions as don't know
Policy	Cancel request
Policy	Create access review
Policy	Create request
Policy	Delete access review
Policy	Delete approvals
Policy	Deny decision
Policy	Don't know decision
Policy	Request expired
Policy	Reset decision
Policy	Update access review
Policy	Update partner directory settings
Policy	Update request
UserManagement	Apply review

Audit Category	Activity
UserManagement	Approve all requests in business flow
UserManagement	Auto review
UserManagement	Auto apply review
UserManagement	Create business flow
UserManagement	Create governance policy template
UserManagement	Delete access review
UserManagement	Delete business flow
UserManagement	Delete governance policy template
UserManagement	Deny all decisions
UserManagement	Deny all requests in business flow
UserManagement	Request approved
UserManagement	Request denied
UserManagement	Update business flow
UserManagement	Update governance policy template

Account provisioning

Configuration changes for application provisioning, HR provisioning, cross-tenant synchronization, and [Microsoft Entra Connect cloud sync](#), are found in this log. The provisioning service only has one audit category in the logs. For actions that the provisioning service performs such as creating users, updating users, and deleting users we recommend using the [provisioning logs](#). For monitoring changes to your provisioning configuration, we recommend using the [audit logs](#).

[] Expand table

Audit Category	Activity	Description
ProvisioningManagement	Add provisioning configuration	A new provisioning configuration has been created.
ProvisioningManagement	Delete provisioning configuration	The provisioning configuration has been deleted.

Audit Category	Activity	Description
ProvisioningManagement	Disable/pause provisioning configuration	The provisioning job has been disabled / paused.
ProvisioningManagement	Enable/restart provisioning configuration	The provisioning job has been restarted.
ProvisioningManagement	Enable/start provisioning configuration	The provisioning job has been started.
ProvisioningManagement	Export	The provisioning job has exported a change to the target system (ex: create a user).
ProvisioningManagement	Import	The provisioning job imported the object from the source system (ex: import the user properties in Entra before provisioning the account into Salesforce).
ProvisioningManagement	Other	
ProvisioningManagement	Process escrow	The provisioning service was unable to export a change to the target application and is retrying the operation.
ProvisioningManagement	Quarantine	The provisioning job is executing at a reduced frequency due to issues such as a lack of connectivity to the target application. Learn more
ProvisioningManagement	Synchronization rule action	The provisioning service evaluated the object and did not export a change to the target system. This even is most often emitted when a user is skipped due to being out of scope for provisioning.
ProvisioningManagement	Update attribute mappings or scope	The attribute mappings or scoping rules for the provisioning job have been updated.
ProvisioningManagement	Update provisioning setting or credentials	The settings on your provisioning job (ex: notification email change, sync all vs. sync assigned users and groups, accidental deletions prevention) have been updated. The credentials for your provisioning job (ex: add a new bearer token) have been updated.
ProvisioningManagement	User Provisioning	The schema for the provisioning job has been restored to the default.

Application proxy

If you're utilizing [Application Proxy](#) to provide your users with remote access to internal apps, the Application Proxy audit logs can help you keep track of changes to available applications or [Connector groups](#).

[+] Expand table

Audit Category	Activity
Application Management	Add application
Application Management	Delete application
Application Management	Update application
Authentication	Add a group to feature rollout
Authentication	Create rollout policy for feature
Authentication	Delete rollout policy of feature
Authentication	Remove a group from feature rollout
Authentication	Remove user from feature rollout
Authentication	Update rollout policy of feature
Authorization	User authorization for application access
DirectoryManagement	Disable Desktop Sso
DirectoryManagement	Disable Desktop Sso for a specific domain
DirectoryManagement	Disable application proxy
DirectoryManagement	Disable passthrough authentication
DirectoryManagement	Enable Desktop Sso
DirectoryManagement	Enable Desktop Sso for a specific domain
DirectoryManagement	Enable application proxy
DirectoryManagement	Enable passthrough authentication
ResourceManagement	Add connector Group
ResourceManagement	Add a Connector to Connector Group
ResourceManagement	Add application SSL certificate

Audit Category	Activity
ResourceManagement	Delete Connector Group
ResourceManagement	Delete SSL binding
ResourceManagement	Register connector
ResourceManagement	Update Connector Group

Authentication Methods

The Audit logs for Authentication Methods can be used to make sure that your users have registered their mobile device properly to enable multifactor authentication.

[\[\] Expand table](#)

Audit Category	Activity
ApplicationManagement	Assign Hardware Oath Token
ApplicationManagement	Authentication Methods Policy Reset
ApplicationManagement	Authentication Methods Policy Update
ApplicationManagement	Authentication Strength Combination Configuration Create
ApplicationManagement	Authentication Strength Combination Configuration Delete
ApplicationManagement	Authentication Strength Combination Configuration Update
ApplicationManagement	Authentication Strength Policy Create
ApplicationManagement	Authentication Strength Policy Delete
ApplicationManagement	Authentication Strength Policy Update
ApplicationManagement	Bulk upload Hardware Oath Token
ApplicationManagement	Create Hardware Oath Token
ApplicationManagement	Delete Hardware Oath Token
ApplicationManagement	MFA Service Policy Update
ApplicationManagement	PATCH UserAuthMethod.PatchSignInPreferencesAsync
ApplicationManagement	PATCH UserAuthMethod.ResetQRPinAsync
ApplicationManagement	PATCH UserAuthMethod.UpdateQRPinAsync

Audit Category	Activity
ApplicationManagement	POST UserAuthMethod.SecurityInfoRegistrationCallback
ApplicationManagement	POST UserAuthMethod.SoftwareOathProofupRegistration
ApplicationManagement	Update Hardware Oath Token
DirectoryManagement	DELETE Subscription.DeleteProviders
DirectoryManagement	DELETE Tenant.DeleteAgentStatuses
DirectoryManagement	DELETE Tenant.DeleteCaches
DirectoryManagement	DELETE Tenant.DeleteGreetings
DirectoryManagement	PATCH Tenant.Patch
DirectoryManagement	PATCH Tenant.PatchCaches
DirectoryManagement	POST SoundFile.Post
DirectoryManagement	POST Subscription.CreateProvider
DirectoryManagement	POST Subscription.CreateSubscription
DirectoryManagement	POST Tenant.CreateBlockedUser
DirectoryManagement	POST Tenant.CreateBypassedUser
DirectoryManagement	POST Tenant.CreateCacheConfig
DirectoryManagement	POST Tenant.CreateGreeting
DirectoryManagement	POST Tenant.CreateTenant
DirectoryManagement	POST Tenant.GenerateNewActivationCredentials
DirectoryManagement	POST Tenant.RemoveBlockedUser
DirectoryManagement	POST Tenant.RemoveBypassedUser
UserManagement	Admin deleted security info
UserManagement	Admin registered security info
UserManagement	Admin started password reset
UserManagement	Admin updated security info
UserManagement	Get passkey creation options
UserManagement	Restore multifactor authentication on all remembered devices

Audit Category	Activity
UserManagement	Update per-user multifactor authentication state
UserManagement	User canceled security info registration
UserManagement	User changed default security info
UserManagement	User deleted security info
UserManagement	User registered all required security info
UserManagement	User registered security info
UserManagement	User reviewed security info
UserManagement	User started password change
UserManagement	user started password reset
UserManagement	User started security info registration
UserManagement	User updated security info

Microsoft Entra (Azure AD) Recommendations

[Microsoft Entra Recommendations](#) monitors your Microsoft Entra tenant and provides personalized insights and actionable guidance to implement best practices for Microsoft Entra features and optimize your tenant configurations. These logs provide a history of the changes made to the status of a recommendation.

[] [Expand table](#)

Audit Category	Activity
DirectoryManagement	Dismiss recommendation
DirectoryManagement	Mark recommendation as complete
DirectoryManagement	Postpone recommendation

Microsoft Entra (Azure MFA) multifactor authentication

The Microsoft Entra multifactor authentication audit logs can help you track trends in suspicious activity or when fraud was reported. Use the [Microsoft Entra sign-in logs](#) to

see each time a user signs in when MFA is required.

[\[+\] Expand table](#)

Audit Category	Activity
DirectoryManagement	DeleteDataFromBackend
DirectoryManagement	DeleteDataFromCosmosDb
DirectoryManagement	ExportDataFromBackend
DirectoryManagement	ExportDataFromCosmosDb
UserManagement	Fraud reported - no action taken
UserManagement	Fraud reported - user is blocked for MFA
UserManagement	Suspicious activity reported
UserManagement	User registered security info

Azure RBAC (Elevated Access)

[\[+\] Expand table](#)

Audit Category	Activity
AzureRBACRoleManagementElevateAccess	The role assignment of User Access Administrator has been removed from the user
AzureRBACRoleManagementElevateAccess	User has elevated their access to User Access Administrator for their Azure Resources

B2B Auth

[\[+\] Expand table](#)

Audit Category	Activity
UserManagement	Redeem extern user invite

B2C

This set of audit logs is related to [B2C](#). Due to the number of connected resources and potential external accounts, this service has a large set of categories and activities. Audit categories include ApplicationManagement, Authentication, Authorization, DirectoryManagement, IdentityProtection, KeyManagement, PolicyManagement, and ResourceManagement. Logs related to one-time passwords are found in the Other category.

[+] Expand table

Audit Category	Activity
Authentication	A self-service sign-up request was completed
Authentication	An API was called as part of a user flow
Authentication	Delete all available strong authentication devices
Authentication	Evaluate Conditional Access policies
Authentication	Exchange token
Authentication	Federate with an identity provider
Authentication	Get available strong authentication devices
Authentication	Issue a SAML assertion to the application
Authentication	Issue an access token to the application
Authentication	Issue an authorization code to the application
Authentication	Issue an id_token to the application
Authentication	Make phone call to verify phone number
Authentication	Register TOTP secret
Authentication	Remediate user
Authentication	Send SMS to verify phone number
Authentication	Send verification email
Authentication	Validate Client Credentials
Authentication	Validate local account credentials
Authentication	Validate user authentication
Authentication	Verify email address

Audit Category	Activity
Authentication	verify one time password
Authentication	Verify phone number
Authorization	Add v2 application permissions
Authorization	Check whether the resource name is available
Authorization	Create API connector
Authorization	Create Identity Provider
Authorization	Create authenticationEventListener
Authorization	Create authenticationEventsFlow
Authorization	Create custom identity provider
Authorization	Create custom policy
Authorization	Create customAuthenticationExtension
Authorization	Create or update a B2C directory resource
Authorization	Create or update a B2C directory tenant and resource
Authorization	Create or update a CIAM directory tenant and resource
Authorization	Create or update a Guest Usages resource
Authorization	Create or update localized resource
Authorization	Create policy key
Authorization	Create starter pack
Authorization	Create user attribute
Authorization	Create user flow
Authorization	Create v2 application
Authorization	Delete API connector
Authorization	Delete B2C Tenant where the caller is an administrator
Authorization	Delete B2C directory resource
Authorization	Delete CIAM directory resource
Authorization	Delete Guest Usages resource

Audit Category	Activity
Authorization	Delete Identity Provider
Authorization	Delete authenticationEventlistener
Authorization	Delete authenticationEventsFlow
Authorization	Delete custom policy
Authorization	Delete customAuthenticationExtension
Authorization	Delete localized resource
Authorization	Delete policy key
Authorization	Delete user attribute
Authorization	Delete user flow
Authorization	Delete v2 application
Authorization	Delete v2 application permission grant
Authorization	Generate key
Authorization	Get API connector
Authorization	Get API connectors
Authorization	Get B2C Tenants where the caller is an administrator
Authorization	Get B2C directory resource
Authorization	Get B2C directory resources in a resource group
Authorization	Get B2C directory resources in a subscription
Authorization	Get CIAM directory resource
Authorization	Get CIAM directory resources in a resource group
Authorization	Get CIAM directory resources in a subscription
Authorization	Get Guest Usages resources
Authorization	Get Guest Usages resources in a subscription
Authorization	Get Identity Provider
Authorization	Get Identity Providers
Authorization	Get OnAttributeCollectionStartCustomExtension

Audit Category	Activity
Authorization	Get OnAttributeCollectionSubmitCustomExtension
Authorization	Get OnPageRenderStartCustomExtension
Authorization	Get active key metadata from policy key
Authorization	Get age gating configuration
Authorization	Get authentication flows policy
Authorization	Get authenticationEventListener
Authorization	Get authenticationEventsFlow
Authorization	Get authenticationEventsFlows
Authorization	Get available output claims
Authorization	Get configured custom identity providers
Authorization	Get configured identity providers
Authorization	Get configured local identity providers
Authorization	Get custom domains
Authorization	Get custom identity provider
Authorization	Get custom policies
Authorization	Get custom policy
Authorization	Get custom policy metadata
Authorization	Get customAuthenticationExtension
Authorization	Get customAuthenticationExtensions
Authorization	Get identity provider types
Authorization	Get list of tenants
Authorization	Get localized resource
Authorization	Get operation status for an async operation
Authorization	Get operations of Microsoft.AzureActiveDirectory resource provider
Authorization	Get policy key
Authorization	Get policy keys

Audit Category	Activity
Authorization	Get resource properties of a tenant
Authorization	Get supported cultures
Authorization	Get supported identity providers
Authorization	Get supported page contracts
Authorization	Get tenant details
Authorization	Get tenant domains
Authorization	Get the authenticationEventsPolicy
Authorization	Get user attribute
Authorization	Get user attributes
Authorization	Get user flow
Authorization	Get user flows
Authorization	Get v1 and v2 applications
Authorization	Get v1 applications
Authorization	Get v2 application
Authorization	Initialize tenant
Authorization	Move resources
Authorization	Restore policy key
Authorization	Retrieve v2 application permissions grants
Authorization	Retrieve v2 application service principals
Authorization	Update API connector
Authorization	Update Identity Provider
Authorization	Update OnAttributeCollectionStartCustomExtension
Authorization	Update OnAttributeCollectionSubmitCustomExtension
Authorization	Update OnPageRenderStartCustomExtension
Authorization	Update a B2C directory resource
Authorization	Update a CIAM directory resource

Audit Category	Activity
Authorization	Update a Guest Usages resource
Authorization	Update age gating configuration
Authorization	Update authentication flows policy
Authorization	Update authenticationEventListener
Authorization	Update authenticationEventsFlow
Authorization	Update authenticationEventsPolicy
Authorization	Update custom identity provider
Authorization	Update custom policy
Authorization	Update customAuthenticationExtension
Authorization	Update identity provider
Authorization	Update local identity provider
Authorization	Update policy key
Authorization	Update subscription status
Authorization	Update tenant metadata
Authorization	Update user attribute
Authorization	Update user flow
Authorization	Upload certificate to policy key
Authorization	Upload key to policy key
Authorization	Upload secret into policy key
Authorization	Validate customExtension authenticationConfiguration
Authorization	Validate move resources
Authorization	Verify if tenant is B2C
Device	Delete pre-created device
Device	Pre-create device
Device	Recover device local administrator password
Device	Register device

Audit Category	Activity
Device	Unregister device
Device	Update device local administrator password
Directory Management	Get age gating configuration
Directory Management	Get list of tenants
Directory Management	Get resources properties of a tenant
Directory Management	Get tenant details
Directory Management	Get tenant domains
Directory Management	Initialize tenant
Directory Management	Update age gating configuration
Directory Management	Update tenant metadata
Directory Management	Verify if tenant is B2C
IdentityProtection	Evaluate Conditional Access policies
IdentityProtection	Remediate user
KeyManagement	Add BitLocker key
KeyManagement	Create policy key
KeyManagement	Delete BitLocker key
KeyManagement	Delete policy key
KeyManagement	Get active key metadata from policy key
KeyManagement	Get policy key
KeyManagement	Get policy keys
KeyManagement	Read BitLocker key
KeyManagement	Restore policy key
KeyManagement	Update policy key
KeyManagement	Upload key to policy key
KeyManagement	Upload secret into policy key
Other	Generate one time password

Audit Category	Activity
Other	Verify one time password
PolicyManagement	Create authenticationEventListener
PolicyManagement	Create authenticationEventsFlow
PolicyManagement	Create customAuthenticationExtension
PolicyManagement	Delete authenticationEventListener
PolicyManagement	Delete authenticationEventsFlow
PolicyManagement	Delete customAuthenticationExtension
PolicyManagement	Get OnAttributeCollectionStartCustomExtension
PolicyManagement	Get OnAttributeCollectionSubmitCustomExtension
PolicyManagement	Get OnPageRenderStartCustomExtension
PolicyManagement	Get authenticationEventListener
PolicyManagement	Get authenticationEventListeners
PolicyManagement	Get authenticationEventsFlow
PolicyManagement	Get authenticationEventsFlows
PolicyManagement	Get customAuthenticationExtension
PolicyManagement	Get customAuthenticationExtensions
PolicyManagement	Get the authenticationEventsPolicy
PolicyManagement	Update OnAttributeCollectionStartCustomExtension
PolicyManagement	Update OnAttributeCollectionSubmitCustomExtension
PolicyManagement	Update OnPageRenderStartCustomExtension
PolicyManagement	Update authenticationEventListener
PolicyManagement	Update authenticationEventsFlow
PolicyManagement	Update authenticationEventsPolicy
PolicyManagement	Update customAuthenticationExtension
PolicyManagement	Validate customExtension authenticationConfiguration
ResourceManagement	Check whether the resource name is available

Audit Category	Activity
ResourceManagement	Create API connector
ResourceManagement	Create Identity Provider
ResourceManagement	Create custom identity provider
ResourceManagement	Create custom policy
ResourceManagement	Create or update a B2C directory resource
ResourceManagement	Create or update a B2C directory tenant and resource
ResourceManagement	Create or update a CIAM directory tenant and resource
ResourceManagement	Create or update a Guest Usages resource
ResourceManagement	Create or update a localized resource
ResourceManagement	Create policy key
ResourceManagement	Create user attribute
ResourceManagement	Create user flow
ResourceManagement	Delete API connector
ResourceManagement	Delete B2C Tenant where the caller is an administrator
ResourceManagement	Delete B2C directory resource
ResourceManagement	Delete CIAM directory resource
ResourceManagement	Delete Guest Usages resource
ResourceManagement	Delete Identity Provider
ResourceManagement	Delete custom policy
ResourceManagement	Delete localized resource
ResourceManagement	Delete policy key
ResourceManagement	Delete user attribute
ResourceManagement	Delete user flow
ResourceManagement	Generate key
ResourceManagement	Get API connector
ResourceManagement	Get API connectors

Audit Category	Activity
ResourceManagement	Get B2C Tenant where the caller is an administrator
ResourceManagement	Get B2C directory resource
ResourceManagement	Get B2C directory resources in a resource group
ResourceManagement	Get B2C directory resources in a subscription
ResourceManagement	Get CIAM directory resource
ResourceManagement	Get CIAM directory resources in a resource group
ResourceManagement	Get CIAM directory resources in a subscription
ResourceManagement	Get Guest Usages resource
ResourceManagement	Get Guest Usages directory resources in a resource group
ResourceManagement	Get Guest Usages directory resources in a subscription
ResourceManagement	Get Identity Provider
ResourceManagement	Get Identity Providers
ResourceManagement	Get active key metadata from policy key
ResourceManagement	Get authentication flows policy
ResourceManagement	Get available output claims
ResourceManagement	Get configured custom identity providers
ResourceManagement	Get configured identity providers
ResourceManagement	Get configured local identity providers
ResourceManagement	Get custom identity provider
ResourceManagement	Get custom policies
ResourceManagement	Get custom policy
ResourceManagement	Get custom policy metadata
ResourceManagement	Get identity provider
ResourceManagement	Get identity provider types
ResourceManagement	Get identity providers
ResourceManagement	Get localized resource

Audit Category	Activity
ResourceManagement	Get operation status of an async operation
ResourceManagement	Get operations of Microsoft.AzureActiveDirectory resource provider
ResourceManagement	Get policy key
ResourceManagement	Get policy keys
ResourceManagement	Get supported cultures
ResourceManagement	Get supported identity providers
ResourceManagement	Get supported page contracts
ResourceManagement	Get user attribute
ResourceManagement	Get user attributes
ResourceManagement	Get user flow
ResourceManagement	Get user flows
ResourceManagement	Move resources
ResourceManagement	Update API connector
ResourceManagement	Identity Provider
ResourceManagement	Update B2C directory resource
ResourceManagement	Update CIAM directory resource
ResourceManagement	Update Guest Usages resource
ResourceManagement	Update authentication flows policy
ResourceManagement	Update custom identity provider
ResourceManagement	Update custom policy
ResourceManagement	Update identity provider
ResourceManagement	Update local identity provider
ResourceManagement	Update policy key
ResourceManagement	Update subscription status
ResourceManagement	Update user attribute
ResourceManagement	Update user flow

Audit Category	Activity
ResourceManagement	Update certificate to policy key
ResourceManagement	Update secret into policy key
ResourceManagement	Validate move resources
UserManagement	Add Windows Hello for Business credential
UserManagement	Add passwordless phone sign-in credential
UserManagement	Delete Windows Hello for Business credential
UserManagement	Delete passwordless phone sign-in credential

Conditional Access

Use these logs to see when changes were made to your [Conditional Access policies](#).

[] Expand table

Audit Category	Activity
Policy	Add AuthenticationContextClassReference
Policy	Add Conditional Access policy
Policy	Add named location
Policy	Delete AuthenticationContextClassReference
Policy	Delete Conditional Access policy
Policy	Delete named location
Policy	Update AuthenticationContextClassReference
Policy	Update Conditional Access policy
Policy	Update continuous access evaluation
Policy	Update named location
Policy	Update security defaults

Core Directory

Logs captured in the Core Directory service cover a wide variety of scenarios. Changes to service principals and applications, updates to company settings, and many other directory related details are captured here. Because so many logs are included in this service, utilize the filter options and date ranges to narrow down the results.

[] [Expand table](#)

Audit Category	Activity
AdministrativeUnit	Add administrative unit
AdministrativeUnit	Add member to administrative unit
AdministrativeUnit	Add member to restricted management administrative unit
AdministrativeUnit	Delete administrative unit
AdministrativeUnit	Hard Delete administrative unit
AdministrativeUnit	Remove member from administrative unit
AdministrativeUnit	Remove member from restricted management administrative unit
AdministrativeUnit	Restore administrative unit
AdministrativeUnit	Update administrative unit
Agreement	Add agreement
Agreement	Delete agreement
Agreement	Hard delete agreement
Agreement	Update agreement
ApplicationManagement	Add app role assignment to service principal
ApplicationManagement	Add application
ApplicationManagement	Add delegated permission grant
ApplicationManagement	Add owner to application
ApplicationManagement	Add owner to service principal
ApplicationManagement	Add policy to application
ApplicationManagement	Add policy to service principal
ApplicationManagement	Add service principal

Audit Category	Activity
ApplicationManagement	Add service principal credentials
ApplicationManagement	Cancel application update with safe rollout
ApplicationManagement	Complete application update after safe rollout
ApplicationManagement	Consent to application
ApplicationManagement	Delete application
ApplicationManagement	Hard Delete application
ApplicationManagement	Hard delete service principal
ApplicationManagement	Remove app role assignment from service principal
ApplicationManagement	Remove delegated permission grant
ApplicationManagement	Remove owner from application
ApplicationManagement	Remove owner from service principal
ApplicationManagement	Remove policy from application
ApplicationManagement	Remove policy from service principal
ApplicationManagement	Remove service principal
ApplicationManagement	Remove service principal credentials
ApplicationManagement	Restore application
ApplicationManagement	Restore service principal
ApplicationManagement	Restore consent
ApplicationManagement	Set verified publisher
ApplicationManagement	Unset verified publisher
ApplicationManagement	Update application
ApplicationManagement	Update application with safe rollout
ApplicationManagement	Update application - Certificates and secrets management
ApplicationManagement	Update external secrets
ApplicationManagement	Update service principal

Audit Category	Activity
Authentication	Test audit log
AuthorizationPolicy	Update authorization policy
CertBasedConfiguration	Add CertBasedAuthConfiguration
CertBasedConfiguration	Hard delete CertificationBasedAuthConfiguration
CertificateAuthorityEntity	Create CertificateAuthorityEntity
CertificateAuthorityEntity	Delete CertificateAuthorityEntity
CertificateAuthorityEntity	Hard Delete CertificateAuthorityEntity
CertificateAuthorityEntity	Restore CertificateAuthorityEntity
CertificateAuthorityEntity	Update CertificateAuthorityEntity
CertificateBasedAuthConfiguration	Add CertificateBasedAuthConfiguration
CertificateBasedAuthConfiguration	Delete CertificateBasedAuthConfiguration
CertificateBasedAuthConfiguration	Update CertificateBasedAuthConfiguration
CompanyBranding	Create Branding Theme
CompanyBranding	Delete Branding Theme
CompanyBranding	Hard Delete Branding Theme
CompanyBranding	Update Branding Theme
CompanyBrandingLocale	Create Branding Theme Localization
CompanyBrandingLocale	Delete Branding Theme Localization
CompanyBrandingLocale	Hard Delete Branding Theme Localization
CompanyBrandingLocale	Update Branding Theme Localization
Contact	Add contact
Contact	Delete contact
Contact	Update contact
CrossTenantAccessSettings	Add a domain-based partner to cross-tenant access setting
CrossTenantAccessSettings	Add a partner to cross-tenant access setting

Audit Category	Activity
CrossTenantAccessSettings	Delete a domain-based partner to cross-tenant access setting
CrossTenantAccessSettings	Delete partner specific cross-tenant access setting
CrossTenantAccessSettings	Migrated partner cross-tenant access settings to the scalable model
CrossTenantAccessSettings	Reset the cross-tenant access default setting
CrossTenantAccessSettings	Update a domain-based partner to cross-tenant access setting
CrossTenantAccessSettings	Update a partner cross-tenant access setting
CrossTenantAccessSettings	Update the company default cross-tenant access setting
CrossTenantIdentitySyncSettings	Create a partner cross-tenant identity sync setting
CrossTenantIdentitySyncSettings	Delete a partner cross-tenant identity sync setting
CrossTenantIdentitySyncSettings	Update a partner cross-tenant identity sync setting
DelegatedAdminServiceProviderConstraints	Adding allowed assignable roles
DelegatedAdminServiceProviderConstraints	Updating allowed assignable roles
Device	Add device
Device	Add registered owner to device
Device	Add registered users to device
Device	Delete device
Device	Device no longer compliant
Device	Device no longer managed
Device	Hard Delete device
Device	Remove registered owner from device
Device	Remove registered users from device
Device	Restore device

Audit Category	Activity
Device	Update device
DeviceConfiguration	Add device configuration
DeviceConfiguration	Delete device configuration
DeviceConfiguration	Update device configuration
DeviceTemplate	Add device from DeviceTemplate
DeviceTemplate	Add DeviceTemplate
DeviceTemplate	Add owner to DeviceTemplate
DeviceTemplate	Delete DeviceTemplate
DirectoryManagement	Add partner to company
DirectoryManagement	Add sharedEmailDomainInvitation
DirectoryManagement	Add unverified domain
DirectoryManagement	Add verified domain
DirectoryManagement	Create Company
DirectoryManagement	Create company settings
DirectoryManagement	Delete company allowed data location
DirectoryManagement	Delete company settings
DirectoryManagement	Delete subscription
DirectoryManagement	Deleting Source Tenant subscriptions
DirectoryManagement	Demote partner
DirectoryManagement	Directory deleted
DirectoryManagement	Directory deleted permanently
DirectoryManagement	Directory scheduled for deletion (Lifecycle)
DirectoryManagement	Directory scheduled for deletion (UserRequest)
DirectoryManagement	Get cross-cloud verification code for domain
DirectoryManagement	Hard Delete Domain
DirectoryManagement	Promote company to partner

Audit Category	Activity
DirectoryManagement	Promote sub domain to root domain
DirectoryManagement	Remove partner from company
DirectoryManagement	Remove unverified domain
DirectoryManagement	Remove verified domain
DirectoryManagement	Schedule Add sharedEmailDomain
DirectoryManagement	Schedule Remove sharedEmailDomain
DirectoryManagement	Set Company Information
DirectoryManagement	Set DirSync feature
DirectoryManagement	Set DirSyncEnabled flag
DirectoryManagement	Set Partnership
DirectoryManagement	Set accidental deletion threshold
DirectoryManagement	Set company allowed data location
DirectoryManagement	Set company multinational feature enabled
DirectoryManagement	Set directory feature on tenant
DirectoryManagement	Set domain authentication
DirectoryManagement	Set federation settings on domain
DirectoryManagement	Set password policy
DirectoryManagement	Soft Delete Domain
DirectoryManagement	Suspending Source Tenant Subscriptions
DirectoryManagement	Update Domain
DirectoryManagement	Update company
DirectoryManagement	Update company settings
DirectoryManagement	Update domain
DirectoryManagement	Update sharedEmailDomain
DirectoryManagement	Update sharedEmailDomainInvitation
DirectoryManagement	Verify domain

Audit Category	Activity
DirectoryManagement	Verify email verified domain
GroupManagement	Add app role assignment to group
GroupManagement	Add group
GroupManagement	Add member to group
GroupManagement	Add owner to group
GroupManagement	Assign label to group
GroupManagement	Create group settings
GroupManagement	Delete group
GroupManagement	Delete group settings
GroupManagement	Finish applying group based license to user
GroupManagement	Grant contextual consent to application
GroupManagement	Hard Delete group
GroupManagement	Remove app role assignment from group
GroupManagement	Remove eligible member from group
GroupManagement	Remove eligible owner from group
GroupManagement	Remove label from group
GroupManagement	Remove member from group
GroupManagement	Remove owner from group
GroupManagement	Restore group
GroupManagement	Set group license
GroupManagement	Set group to be managed by user
GroupManagement	Start applying group based license to users
GroupManagement	Trigger group license recalculation
GroupManagement	Update group
GroupManagement	Update group settings
KerberosDomain	Add kerberos domain

Audit Category	Activity
KerberosDomain	Delete kerberos domain
KerberosDomain	Restore kerberos domain
KerberosDomain	Update kerberos domain
Label	Add label
Label	Delete label
Label	Update label
MicrosoftSupportAccessManagement	Access approved
MicrosoftSupportAccessManagement	Access removed
MicrosoftSupportAccessManagement	Request approved
MicrosoftSupportAccessManagement	Request canceled
MicrosoftSupportAccessManagement	Request created
MicrosoftSupportAccessManagement	Request rejected
MultiTenantOrg	Create a MultiTenantOrg
MultiTenantOrg	Hard Delete MultiTenantOrg
MultiTenantOrg	Update a MultiTenantOrg
MultiTenantOrgIdentitySyncPolicyUpdate	Reset a multi tenant org identity sync policy template
MultiTenantOrgIdentitySyncPolicyUpdate	Update a multi tenant org identity sync policy template
MultiTenantOrgPartnerConfigurationTemplate	Reset a multi tenant org partner configuration template
MultiTenantOrgPartnerConfigurationTemplate	Update a multi tenant org partner configuration template
MultiTenantOrgTenant	Add MultiTenantOrg tenant
MultiTenantOrgTenant	Delete MultiTenantOrg tenant
MultiTenantOrgTenant	Hard Delete MultiTenantOrg tenant
MultiTenantOrgTenant	Tenant joining MultiTenantOrg tenant
MultiTenantOrgTenant	Update MultiTenantOrg tenant

Audit Category	Activity
OrganizationalUnitContainer	Create OrganizationalUnit
OrganizationalUnitContainer	Delete OrganizationalUnit
OrganizationalUnitContainer	Update OrganizationalUnit
PendingExternalUserProfile	Create PendingExternalUserProfile
PendingExternalUserProfile	Delete PendingExternalUserProfile
PendingExternalUserProfile	Hard Delete PendingExternalUserProfile
PermissionGrantPolicy	Add permission grant policy
PermissionGrantPolicy	Delete permission grant policy
PermissionGrantPolicy	Update permission grant policy
Policy	Add owner to policy
Policy	Add policy
Policy	Delete policy
Policy	Hard Delete policy
Policy	Remove owner from policy
Policy	Remove policy credentials
Policy	Restore policy
Policy	Update policy
PublicKeyInfrastructure	Create PublicKeyInfrastructure
PublicKeyInfrastructure	Delete PublicKeyInfrastructure
PublicKeyInfrastructure	Hard Delete PublicKeyInfrastructure
PublicKeyInfrastructure	Initiate PublicKeyInfrastructure
PublicKeyInfrastructure	Restore PublicKeyInfrastructure
PublicKeyInfrastructure	Update PublicKeyInfrastructure
RoleManagement	Add EligibleRoleAssignment to RoleDefinition
RoleManagement	Add eligible member to role
RoleManagement	Add member to role

Audit Category	Activity
RoleManagement	Add member to role scoped over Restricted Management Administrative Unit
RoleManagement	Add role assignment to role definition
RoleManagement	Add role definition
RoleManagement	Add role from template
RoleManagement	Add scoped member to role
RoleManagement	Delete role definition
RoleManagement	Remove EligibleRoleAssignment from RoleDefinition
RoleManagement	Remove eligible member from role
RoleManagement	Remove member from role
RoleManagement	Remove member from role scoped over Restricted Management Administrative Unit
RoleManagement	Remove role assignment from role definition
RoleManagement	Remove scoped member from role
RoleManagement	Update role
RoleManagement	Update role definition
UserManagement	Add app role assignment to group
UserManagement	Add user
UserManagement	Add user sponsor
UserManagement	Change user license
UserManagement	Change user password
UserManagement	Convert federated user to managed
UserManagement	Create application password for user
UserManagement	Delete application password for user
UserManagement	Delete user
UserManagement	Disable Strong Authentication

Audit Category	Activity
UserManagement	Disable account
UserManagement	Enable Strong Authentication
UserManagement	Enable account
UserManagement	Hard Delete user
UserManagement	Remove OrganizationalUnit assigned to a user
UserManagement	Remove app role assignment from user
UserManagement	Remove user sponsor
UserManagement	Reset password
UserManagement	Restore user
UserManagement	Set force change user password
UserManagement	Set user manager
UserManagement	Takeover user cloned
UserManagement	Update OrganizationalUnit assigned to a user
UserManagement	Update StsRefreshTokenValidFrom Timestamp
UserManagement	Update external secrets
UserManagement	Update user

Device Registration Service

If you need to manage [Microsoft Entra ID](#) and [Microsoft Entra hybrid joined devices](#), use the logs captured in the Device Registration Service to review changes to devices.

[] [Expand table](#)

Audit Category	Activity
Device	Delete pre-created device
Device	Pre-create device
Device	Recover device local administrator password
Device	Register device

Audit Category	Activity
Device	Unregister device
Device	Update local administrator password
KeyManagement	Add BitLocker key
KeyManagement	Delete BitLocker key
KeyManagement	Read BitLocker key
Policy	Set device registration policies
UserManagement	Add Passkey (device-bound)
UserManagement	Add Windows Hello for Business credential
UserManagement	Add passwordless phone sign-in credential
UserManagement	Add platform credential
UserManagement	Delete Passkey (device-bound)
UserManagement	Delete Windows Hello for Business credential
UserManagement	Delete passwordless phone sign-in credential
UserManagement	Delete platform credential

Entitlement Management

Use these logs to monitor changes to Entitlement Management settings. Entitlement Management can be used to streamline how you assign members of Microsoft Entra security groups, grant licenses for Microsoft 365, or provide access to applications. [Access reviews](#) and [Lifecycle workflows](#) have separate logs.

[] [Expand table](#)

Audit Category	Activity
EntitlementManagement	Add Entitlement Management role assignment
EntitlementManagement	Administrator directly assigns user to access package
EntitlementManagement	Administrator directly removes user access package assignment
EntitlementManagement	Approval stage completed for access package assignment request

Audit Category	Activity
EntitlementManagement	Approve access package assignment request
EntitlementManagement	Assign user as external sponsor
EntitlementManagement	Assign user as internal sponsor
EntitlementManagement	Auto approve access package assignment request
EntitlementManagement	Cancel access package assignment request
EntitlementManagement	Create access package
EntitlementManagement	Create access package assignment policy
EntitlementManagement	Create access package assignment user update request
EntitlementManagement	Create access package catalog
EntitlementManagement	Create connected organization
EntitlementManagement	Create custom extension
EntitlementManagement	Create incompatible access package
EntitlementManagement	Create incompatible group
EntitlementManagement	Create resource environment
EntitlementManagement	Create resource remove request
EntitlementManagement	Create resource request
EntitlementManagement	Delete access package
EntitlementManagement	Delete access package assignment policy
EntitlementManagement	Delete access package assignment request
EntitlementManagement	Delete access package assignment policy for a deleted user
EntitlementManagement	Delete access package catalog
EntitlementManagement	Delete connected organization
EntitlementManagement	Delete custom extension
EntitlementManagement	Delete incompatible access package
EntitlementManagement	Delete incompatible group
EntitlementManagement	Deny access package assignment request

Audit Category	Activity
EntitlementManagement	Entitlement Management creates access package assignment request for user
EntitlementManagement	Entitlement Management removes access package assignment request for user
EntitlementManagement	Execute custom extension
EntitlementManagement	Extend access package assignment
EntitlementManagement	Failed access package assignment request
EntitlementManagement	Fulfill access package assignment request
EntitlementManagement	Fulfill access package resource assignment
EntitlementManagement	Partially fulfill access package assignment request
EntitlementManagement	Ready to fulfill access package assignment request
EntitlementManagement	Remove Entitlement Management role assignment
EntitlementManagement	Remove access package resource assignment
EntitlementManagement	Remove user as external sponsor
EntitlementManagement	Remove user as internal sponsor
EntitlementManagement	Schedule a future access package assignment
EntitlementManagement	Update access package
EntitlementManagement	Update access package assignment policy
EntitlementManagement	Update access package assignment request
EntitlementManagement	Update access package catalog
EntitlementManagement	Update access package catalog resource
EntitlementManagement	Update connected organization
EntitlementManagement	Update custom extension
EntitlementManagement	Update request answers by approver
EntitlementManagement	Update tenant setting
EntitlementManagement	User requests access package assignment
EntitlementManagement	User requests an access package assignment on behalf of service

Audit Category	Activity
	principal
EntitlementManagement	User requests to extend access package assignment
EntitlementManagement	User requests to remove access package assignment

Global Secure Access

If you're using Microsoft Entra Internet Access or Microsoft Entra Private Access to acquire and secure network traffic to your corporate resources, these logs can help identify when changes were made to your network policies. These logs capture changes to traffic forwarding policies and remote networks, such as branch office locations. For more information, see [What is Global Secure Access](#).

[] [Expand table](#)

Audit Category	Activity
ApplicationManagement	Create Certificate
ApplicationManagement	Delete Certificate
ApplicationManagement	Update Certificate
ObjectManagement	Offboarding Process Started
ObjectManagement	Onboarding Process Started
ObjectManagement	Update Adaptive Access Policy
ObjectManagement	Update Enriched Audit Logs Settings
ObjectManagement	Update Forwarding Options Policy
PolicyManagement	Create Filtering Policy
PolicyManagement	Create Filtering Policy Profile
PolicyManagement	Create Remote Network
PolicyManagement	Create Security Provider Policy
PolicyManagement	Delete Filtering Policy
PolicyManagement	Delete Filtering Policy Profile
PolicyManagement	Delete Forwarding Policy

Audit Category	Activity
PolicyManagement	Delete Private Access Policy
PolicyManagement	Delete Remote Network
PolicyManagement	Delete Security Provider Policy
PolicyManagement	Update Filtering Policy
PolicyManagement	Update Filtering Policy Profile
PolicyManagement	Update Filtering Profile
PolicyManagement	Update Forwarding Options Policy
PolicyManagement	Update Forwarding Policy
PolicyManagement	Update Forwarding Profile
PolicyManagement	Update Forwarding Rule
PolicyManagement	Update Private Access Policy
PolicyManagement	Update Remote Network
PolicyManagement	Update Security Provider Policy
ResourceManagement	Create Registration of Security Provider

Hybrid Authentication

[\[+\] Expand table](#)

Audit Category	Activity
Authentication	Add user to feature rollout
Authentication	Remove user from feature rollout

Microsoft Entra ID Protection (Identity Protection)

[\[+\] Expand table](#)

Audit Category	Activity
IdentityProtection	Update IdentityProtectionPolicy

Audit Category	Activity
IdentityProtection	Update NotificationSettings
Other	ConfirmAccountCompromised
Other	ConfirmAccountSafe
Other	ConfirmCompromised
Other	ConfirmSafe
Other	DismissRisk
Other	DismissUser
Other	confirmServicePrincipalCompromised
Other	DismissServicePrincipal

Invited users

Use the Invited users logs to help you manage the status of users who were invited to collaborate as guests in your tenant. These logs can help troubleshoot issues with invitations sent to external users.

[Expand table](#)

Audit Category	Activity
UserManagement	Delete external user
UserManagement	Email not sent, user unsubscribed
UserManagement	Invitation Email
UserManagement	Invite external user
UserManagement	Invite external user with reset invitation status
UserManagement	Invite internal user to B2B collaboration
UserManagement	Redeem external user invite

Lifecycle Workflows

[Lifecycle Workflows](#)(preview) are a great way to automate identity related processes for joiners, movers, and leavers so you don't have to. For more information, see [Lifecycle](#)

Workflows audits.

[+] Expand table

Audit Category	Activity
Other	Create custom task extension
Other	Delete custom task extension
Other	Update custom task extension
TaskManagement	Add task to workflow
TaskManagement	Disable task
TaskManagement	Enable task
TaskManagement	Remove task from workflow
TaskManagement	Update task
WorkflowManagement	Add execution conditions
WorkflowManagement	Add workflow version
WorkflowManagement	Create workflow
WorkflowManagement	Delete workflow
WorkflowManagement	Disable workflow
WorkflowManagement	Disable workflow schedule
WorkflowManagement	Enable workflow
WorkflowManagement	Enable workflow schedule
WorkflowManagement	Hard delete workflow
WorkflowManagement	On-demand workflow execution completed
WorkflowManagement	Restore workflow
WorkflowManagement	Schedule workflow execution completed
WorkflowManagement	Schedule workflow execution started
WorkflowManagement	Set workflow for on-demand execution
WorkflowManagement	Update execution conditions
WorkflowManagement	Update tenant settings

Audit Category	Activity
WorkflowManagement	Update workflow

Microsoft Identity Manager (MIM) Service

If you're using [MIM](#) to automate identity and group provisioning based on business policy and workflow, these audit logs can help track when changes were made to groups and members through the MIM service.

[\[+\] Expand table](#)

Audit Category	Activity
GroupManagement	Add group
GroupManagement	Add member to group
GroupManagement	Add owner to group
GroupManagement	Delete group
GroupManagement	Remove member from group
GroupManagement	Remove owner from group
GroupManagement	Update group
UserManagement	User Password Registration
UserManagement	User Password Reset

Mobility Management

[\[+\] Expand table](#)

Audit Category	Activity
Authentication	User confirmed unusual sign-in event as legitimate
Authentication	User reported unusual sign-in event as not legitimate
UserManagement	User changed default security info
UserManagement	User deleted security info
UserManagement	User registered security info

Audit Category	Activity
UserManagement	User started security info registration

MyAccess

 [Expand table](#)

Audit Category	Activity
ApplicationManagement	Create application collection

MyApps

Use the [MyApps](#) audit logs to identify when an application was added to a collection for your MyApp portal.

 [Expand table](#)

Audit Category	Activity
ApplicationManagement	Create application collection
ApplicationManagement	Delete application collection
ApplicationManagement	Update application collection
ApplicationManagement	Update application collection order
ApplicationManagement	Update preview settings

Privileged Identity Management (PIM)

Many of the activities captured in the PIM audit logs are similar, so take note of details like *renew*, *timebound*, and *permanent*. PIM activities can generate many logs in a 24 hour period, so utilize the filters to narrow things down. For more information on the audit capabilities within the PIM service, see [View audit history for Microsoft Entra roles in PIM](#).

 [Expand table](#)

Audit Category	Activity
ApplicationManagement	Add member to role approval requested (PIM activation)
ApplicationManagement	Add member to role in PIM completed (timebound)
ApplicationManagement	Add member to role in PIM requested (timebound)
ApplicationManagement	Approve request - direct role assignment
ApplicationManagement	PIM activation request expired
ApplicationManagement	PIM policy removed
ApplicationManagement	Remove member from role in PIM completed (timebound)
ApplicationManagement	Remove request
ApplicationManagement	Role definition created
ApplicationManagement	Update role setting in PIM
GroupManagement	Add eligible member to role in PIM canceled (renew)
GroupManagement	Add eligible member to role in PIM canceled (timebound)
GroupManagement	Add eligible member to role in PIM completed (permanent)
GroupManagement	Add eligible member to role in PIM completed (timebound)
GroupManagement	Add eligible member to role in PIM requested (permanent)
GroupManagement	Add eligible member to role in PIM requested (renew)
GroupManagement	Add eligible member to role in PIM requested (timebound)
GroupManagement	Add member to role approval requested (PIM activation)
GroupManagement	Add member to role canceled (PIM activation)
GroupManagement	Add member to role completed (PIM activation)
GroupManagement	Add member to role in PIM canceled (permanent)
GroupManagement	Add member to role in PIM canceled (renew)
GroupManagement	Add member to role in PIM canceled (timebound)
GroupManagement	Add member to role in PIM completed (permanent)
GroupManagement	Add member to role in PIM completed (timebound)
GroupManagement	Add member to role in PIM requested (permanent)

Audit Category	Activity
GroupManagement	Add member to role in PIM requested (renew)
GroupManagement	Add member to role in PIM requested (timebound)
GroupManagement	Add member to role request approved (PIM activation)
GroupManagement	Add member to role request denied (PIM activation)
GroupManagement	Add member to role requested (PIM activation)
GroupManagement	Cancel request
GroupManagement	Cancel request for role removal
GroupManagement	Cancel request for role update
GroupManagement	Offboarded resource from PIM
GroupManagement	Onboarded resource to PIM
GroupManagement	PIM activation request expired
GroupManagement	PIM policy removed
GroupManagement	Process request
GroupManagement	Process role removal request
GroupManagement	Remove eligible member from role in PIM completed (permanent)
GroupManagement	Remove eligible member from role in PIM completed (timebound)
GroupManagement	Remove eligible member from role in PIM requested (permanent)
GroupManagement	Remove eligible member from role in PIM requested (timebound)
GroupManagement	Remove member from role (PIM activation expired)
GroupManagement	Remove member from role completed (PIM deactivate)
GroupManagement	Remove member from role in PIM completed (permanent)
GroupManagement	Remove member from role in PIM completed (timebound)
GroupManagement	Remove member from role in PIM requested (permanent)
GroupManagement	Remove member from role in PIM requested (timebound)
GroupManagement	Remove member from role requested (PIM deactivate)
GroupManagement	Remove permanent direct role assignment

Audit Category	Activity
GroupManagement	Remove permanent eligible role assignment
GroupManagement	Remove request
GroupManagement	Resource updated
GroupManagement	Restore eligible member from role in PIM completed
GroupManagement	Restore member from role
GroupManagement	Restore member from role in PIM completed
GroupManagement	Restore permanent direct role assignment
GroupManagement	Update eligible member in PIM canceled (extend)
GroupManagement	Update eligible member in PIM requested (extend)
GroupManagement	Update member in PIM approved by admin (extend/renew)
GroupManagement	Update member in PIM canceled (extend)
GroupManagement	Update member in PIM denied by admin (extend/renew)
GroupManagement	Update member in PIM requested (extend)
GroupManagement	Update role setting in PIM
ResourceManagement	Add eligible member to role in PIM canceled (permanent)
ResourceManagement	Add eligible member to role in PIM canceled (renew)
ResourceManagement	Add eligible member to role in PIM canceled (timebound)
ResourceManagement	Add eligible member to role in PIM completed (permanent)
ResourceManagement	Add eligible member to role in PIM completed (timebound)
ResourceManagement	Add eligible member to role in PIM requested (permanent)
ResourceManagement	Add eligible member to role in PIM requested (renew)
ResourceManagement	Add eligible member to role in PIM requested (timebound)
ResourceManagement	Add member to role approval requested (PIM activation)
ResourceManagement	Add member to role canceled (PIM activation)
ResourceManagement	Add member to role completed (PIM activation)
ResourceManagement	Add member to role in PIM canceled (renew)

Audit Category	Activity
ResourceManagement	Add member to role in PIM canceled (timebound)
ResourceManagement	Add member to role in PIM completed (permanent)
ResourceManagement	Add member to role in PIM completed (timebound)
ResourceManagement	Add member to role in PIM requested (permanent)
ResourceManagement	Add member to role in PIM requested (renew)
ResourceManagement	Add member to role in PIM requested (timebound)
ResourceManagement	Add member to role outside of PIM (permanent)
ResourceManagement	Add member to role request approved (PIM activation)
ResourceManagement	Add member to role request denied (PIM activation)
ResourceManagement	Add member to role requested (PIM activation)
ResourceManagement	Cancel request
ResourceManagement	Cancel request for role removal
ResourceManagement	Cancel request for role update
ResourceManagement	Deactivate PIM alert
ResourceManagement	Disable PIM alert
ResourceManagement	Enable PIM alert
ResourceManagement	Offboarded resource from PIM
ResourceManagement	Onboarded resource from PIM
ResourceManagement	PIM activation request expired
ResourceManagement	PIM policy removed
ResourceManagement	Process request
ResourceManagement	Process role removal request
ResourceManagement	Process role update request
ResourceManagement	Remove eligible member from role in PIM completed (permanent)
ResourceManagement	Remove eligible member from role in PIM completed (timebound)
ResourceManagement	Remove eligible member from role in PIM requested (permanent)

Audit Category	Activity
ResourceManagement	Remove eligible member from role in PIM requested (timebound)
ResourceManagement	Remove member from role (PIM activation expired)
ResourceManagement	Remove member from role completed (PIM deactivate)
ResourceManagement	Remove member from role in PIM completed (permanent)
ResourceManagement	Remove member from role in PIM completed (timebound)
ResourceManagement	Remove member from role in PIM requested (permanent)
ResourceManagement	Remove member from role in PIM requested (timebound)
ResourceManagement	Remove member from role requested (PIM deactivate)
ResourceManagement	Remove permanent direct role assignment
ResourceManagement	Remove permanent eligible role assignment
ResourceManagement	Remove request
ResourceManagement	Resolve PIM alert
ResourceManagement	Resource updated
ResourceManagement	Restore eligible member from role in PIM completed
ResourceManagement	Restore member from role
ResourceManagement	Restore member from role in PIM completed
ResourceManagement	Restore permanent direct role assignment
ResourceManagement	Restore permanent eligible role assignment
ResourceManagement	Tenant offboarded from PIM
ResourceManagement	Triggered PIM alert
ResourceManagement	Update eligible member in PIM canceled (extend)
ResourceManagement	Update eligible member in PIM requested (extend)
ResourceManagement	Update member in PIM approved by admin (extend/renew)
ResourceManagement	Update member in PIM canceled (extend)
ResourceManagement	Update member in PIM denied by admin (extend/renew)
ResourceManagement	Update member in PIM requested (extend)

Audit Category	Activity
ResourceManagement	Update role setting in PIM
RoleManagement	Add eligible member to role in PIM canceled (permanent)
RoleManagement	Add eligible member to role in PIM canceled (renew)
RoleManagement	Add eligible member to role in PIM canceled (timebound)
RoleManagement	Add eligible member to role in PIM completed (permanent)
RoleManagement	Add eligible member to role in PIM completed (timebound)
RoleManagement	Add eligible member to role in PIM requested (permanent)
RoleManagement	Add eligible member to role in PIM requested (renew)
RoleManagement	Add eligible member to role in PIM requested (timebound)
RoleManagement	Add member to role approval requested (PIM activation)
RoleManagement	Add member to role canceled (PIM activation)
RoleManagement	Add member to role completed (PIM activation)
RoleManagement	Add member to role in PIM canceled (renew)
RoleManagement	Add member to role in PIM canceled (timebound)
RoleManagement	Add member to role in PIM completed (permanent)
RoleManagement	Add member to role in PIM completed (timebound)
RoleManagement	Add member to role in PIM requested (permanent)
RoleManagement	Add member to role in PIM requested (renew)
RoleManagement	Add member to role in PIM requested (timebound)
RoleManagement	Add member to role outside of PIM (permanent)
RoleManagement	Add member to role request approved (PIM activation)
RoleManagement	Add member to role request denied (PIM activation)
RoleManagement	Add member to role requested (PIM activation)
RoleManagement	Cancel request for role removal
RoleManagement	Cancel request for role update
RoleManagement	Deactivate PIM alert

Audit Category	Activity
RoleManagement	Disable PIM alert
RoleManagement	Enable PIM alert
RoleManagement	Offboarded resource from PIM
RoleManagement	Onboarded resource from PIM
RoleManagement	PIM activation request expired
RoleManagement	PIM policy removed
RoleManagement	Process request
RoleManagement	Process role removal request
RoleManagement	Process role update request
RoleManagement	Refresh PIM alert
RoleManagement	Remove eligible member from role in PIM completed (permanent)
RoleManagement	Remove eligible member from role in PIM completed (timebound)
RoleManagement	Remove eligible member from role in PIM requested (permanent)
RoleManagement	Remove eligible member from role in PIM requested (timebound)
RoleManagement	Remove member from role (PIM activation expired)
RoleManagement	Remove member from role completed (PIM deactivate)
RoleManagement	Remove member from role in PIM completed (permanent)
RoleManagement	Remove member from role in PIM completed (timebound)
RoleManagement	Remove member from role in PIM requested (permanent)
RoleManagement	Remove member from role in PIM requested (timebound)
RoleManagement	Remove member from role requested (PIM deactivate)
RoleManagement	Remove permanent direct role assignment
RoleManagement	Remove permanent eligible role assignment
RoleManagement	Remove request
RoleManagement	Resolve PIM alert
RoleManagement	Restore eligible member from role in PIM completed

Audit Category	Activity
RoleManagement	Restore member from role
RoleManagement	Restore member from role in PIM completed
RoleManagement	Restore permanent direct role assignment
RoleManagement	Restore permanent eligible role assignment
RoleManagement	Tenant offboarded from PIM
RoleManagement	Triggered PIM alert
RoleManagement	Update PIM alert setting
RoleManagement	Update eligible member in PIM canceled (extend)
RoleManagement	Update eligible member in PIM requested (extend)
RoleManagement	Update member in PIM approved by admin (extend/renew)
RoleManagement	Update member in PIM canceled (extend)
RoleManagement	Update member in PIM denied by admin (extend/renew)
RoleManagement	Update member in PIM requested (extend)
RoleManagement	Update role setting in PIM

Self-service group management

Users in your tenant can manage many aspects of their group memberships on their own. Use the Self-service group management logs to help troubleshoot issues with these scenarios.

Many of the activities in this group are associated with background processes related to a user's activity. For example, you might see multiple `Features_GetFeaturesAsync` instances in your logs when a user accesses the MyApps or MyGroups portal. This activity doesn't indicate if the user made any changes. Other activities such as `GroupsODataV4_Get` often occur in groups for similar user actions.

[\[+\] Expand table](#)

Audit Category	Activity
GroupManagement	ApprovalNotification_Create

Audit Category	Activity
GroupManagement	Approval_Act
GroupManagement	Approval_Get
GroupManagement	Approval_GetAll
GroupManagement	Approvals_Post
GroupManagement	Approve a pending request to join a group
GroupManagement	Cancel a pending request to join a group
GroupManagement	Create lifecycle management policy
GroupManagement	Delete a pending request to join a group
GroupManagement	Delete lifecycle management policy
GroupManagement	Device_Create
GroupManagement	Device_Delete
GroupManagement	Device_Get
GroupManagement	Device_GetAll
GroupManagement	Features_GetFeaturesAsync
GroupManagement	Features_IsFeatureEnabledAsync
GroupManagement	Features_UpdateFeaturesAsync
GroupManagement	GroupLifecyclePolicies_Get
GroupManagement	GroupLifecyclePolicies_addGroup
GroupManagement	GroupLifecyclePolicies_removeGroup
GroupManagement	Group_AddMember
GroupManagement	Group_AddOwner
GroupManagement	Group_BatchValidateDynamicMembership
GroupManagement	Group_Create
GroupManagement	Group_Delete
GroupManagement	Group_Get
GroupManagement	Group_GetAll

Audit Category	Activity
GroupManagement	Group_GetDynamicGroupProperties
GroupManagement	Group_GetDynamicMembershipDeviceAttributes
GroupManagement	Group_GetDynamicMembershipOperators
GroupManagement	Group_GetDynamicMembershipUserBaseAttributes
GroupManagement	Group_GetExpiryNotificationDate
GroupManagement	Group_GetMembers
GroupManagement	Group_GetOwners
GroupManagement	Group_RemoveMember
GroupManagement	Group_RemoveOwner
GroupManagement	Group_Restore
GroupManagement	Group_Update
GroupManagement	Group_ValidateDynamicMembership
GroupManagement	GroupsODataV4_Get
GroupManagement	GroupsODataV4_GetgroupLifecyclePolicies
GroupManagement	GroupsODataV4_evaluateDynamicMembership
GroupManagement	Groups_CreateLink
GroupManagement	Groups_Get
GroupManagement	LcmPolicy_Get
GroupManagement	LcmPolicy_RenewGroup
GroupManagement	Reject a pending request to join a group
GroupManagement	Renew group
GroupManagement	Request to join a group
GroupManagement	set dynamic group properties
GroupManagement	Settings_GetSettingsAsync
GroupManagement	Update lifecycle management policy
GroupManagement	User_Create

Audit Category	Activity
GroupManagement	User_Delete
GroupManagement	User_Get
GroupManagement	User_GetAll
GroupManagement	User_GetMemberOf
GroupManagement	User_GetOwnedObjects
Other	ApprovalNotification_Create
UserManagement	Updated ConvergedUXV2 feature value
UserManagement	Updated MyApp feature value
UserManagement	Update MyStaff feature value
UserManagement	Updated SSPRConvergence feature value
UserManagement	Updated SignInReports feature value

Self-service password management

The Self-service password management logs provide insight into changes made to passwords by users and admins or when users register for self-service password reset.

[\[+\] Expand table](#)

Audit Category	Activity
DirectoryManagement	Disable password writeback for directory
DirectoryManagement	Enable password writeback for directory
UserManagement	Blocked from self-service password reset
UserManagement	Change password (self-service)
UserManagement	Reset password (by admin)
UserManagement	Reset password (self-service)
UserManagement	Security info saved for self-service password reset
UserManagement	Self-service password reset flow activity progress
UserManagement	Unlock user account (self-service)

Terms of use

[\[+\] Expand table](#)

Audit Category	Activity
Policy	Accept Terms Of Use
Policy	Create Terms Of Use
Policy	Decline Terms Of Use
Policy	Delete Consent
Policy	Delete Terms Of Use
Policy	Edit Terms Of Use
Policy	Publish Terms Of Use

Verified ID

[\[+\] Expand table](#)

Audit Category	Activity
ResourceManagement	Create authority
ResourceManagement	Create authorization policy
ResourceManagement	Create contract
ResourceManagement	Create issuance policy
ResourceManagement	Delete issuance policy
ResourceManagement	Process POST /authorities/:issuerId/didInfo/signingKeys/rotate request
ResourceManagement	Process POST /authorities/:issuerId/didInfo/signingKeys/synchronizeWithDidDocument request
ResourceManagement	Revoke credential
ResourceManagement	Rotate signing key
ResourceManagement	Tenant onboarding
ResourceManagement	Tenant opt-out

Audit Category	Activity
ResourceManagement	Update MyAccount settings
ResourceManagement	Update authority
ResourceManagement	Update contract
ResourceManagement	Update issuance policy
ResourceManagement	Update linked domains

Next steps

- Microsoft Entra monitoring and health overview.
- Audit logs report
- Programmatic access to Microsoft Entra reports

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra data retention

Article • 12/05/2023

In this article, you learn about the data retention policies for the different activity reports in Microsoft Entra ID.

When does Microsoft Entra ID start collecting data?

 Expand table

Microsoft Entra Edition	Collection Start
Microsoft Entra ID P1	When you sign up for a subscription
Microsoft Entra ID P2	
Microsoft Entra Workload ID	
Premium	
Microsoft Entra ID Free	The first time you open Microsoft Entra ID or use the reporting APIs

If you already have activities data with your free license, then you can see it immediately on upgrade. If you don't have any data, then it will take up to three days for the data to show up in the reports after you upgrade to a premium license.

- For security signals, the collection process starts when you opt in to use the [Identity Protection Center](#).
- For Microsoft Graph activity logs, the collection process starts when the [log category is enabled in diagnostic settings](#).

How long does Microsoft Entra ID store the data?

Log storage within Microsoft Entra varies by report type and license type. You can retain the audit and sign-in activity data for longer than the default retention period outlined in the previous table by routing it to an Azure storage account using Azure Monitor. For more information, see [Archive Microsoft Entra logs to an Azure storage account](#).

Activity reports

[+] Expand table

Report	Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2
Audit logs	Seven days	30 days	30 days
Sign-ins	Seven days	30 days	30 days
Microsoft Entra multifactor authentication usage	30 days	30 days	30 days
Microsoft Graph activity logs*	NA	Must be integrated with storage or analytics tools	Must be integrated with storage or analytics tools

*Microsoft Graph activity logs are only available for Microsoft Entra ID P1 and P2 licenses. Data is not retained unless it's archived to a storage account or integrated with analytics tools.

Security signals

[+] Expand table

Report	Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2
Risky users	No limit	No limit	No limit
Risky sign-ins	7 days	30 days	90 days

! Note

Risky users and workload identities are not deleted until the risk has been remediated.

Can I see last month's data after getting a premium license?

No, you can't. Azure stores up to seven days of activity data for a free version. When you switch from a free to a premium version, you can only see up to 7 days of data.

Next steps

- Stream logs to an event hub
- Learn how to download Microsoft Entra logs

Log latency in Microsoft Entra ID

Article • 09/27/2024

Latency is the amount of time it takes for Microsoft Entra ID reporting data to appear in the Monitoring and health logs. This article describes the factors that can affect latency.

Latency and first-time setup

When you upgrade from a free version of Microsoft Entra Premium P1 or P2, you should expect a delay of roughly 24 hours from when you upgrade your tenant before all premium reporting features show data. Many premium reporting features only begin retaining data after this 24-hour period following your upgrade.

When setting up a new storage account or security information and event management (SIEM) tool, you should also expect a delay of 24 hours before reporting data appears in those tools.

When routing activity logs to a Log Analytics workspace for analysis with Azure Monitor logs, you should expect a delay of up to three days before the logs appear in the workspace.

Reporting latency factors

Many factors influence the latency of reporting data. The type of data, the amount of data, and the infrastructure that the reporting tools are built on can all influence latency. If there's a delay in the underlying infrastructure, Microsoft Entra reports might experience a delay in reporting data.

One key factor in log latency is the path that the data travels from the source event to the logs in the Microsoft Entra admin center. Log data travels through the following systems before it appears in the logs.

1. Customer signs in to a service that uses Microsoft Entra ID as the identity and access service.
2. Log processors read the event metadata and publish it to the Azure storage queue.
3. Event metadata is processed and reviewed for success or failure.
4. Successful events are published to partner services, such as Azure Monitor and Microsoft Graph.
5. IT admin views the data in the Microsoft Entra admin center, or their SIEM tool of choice.

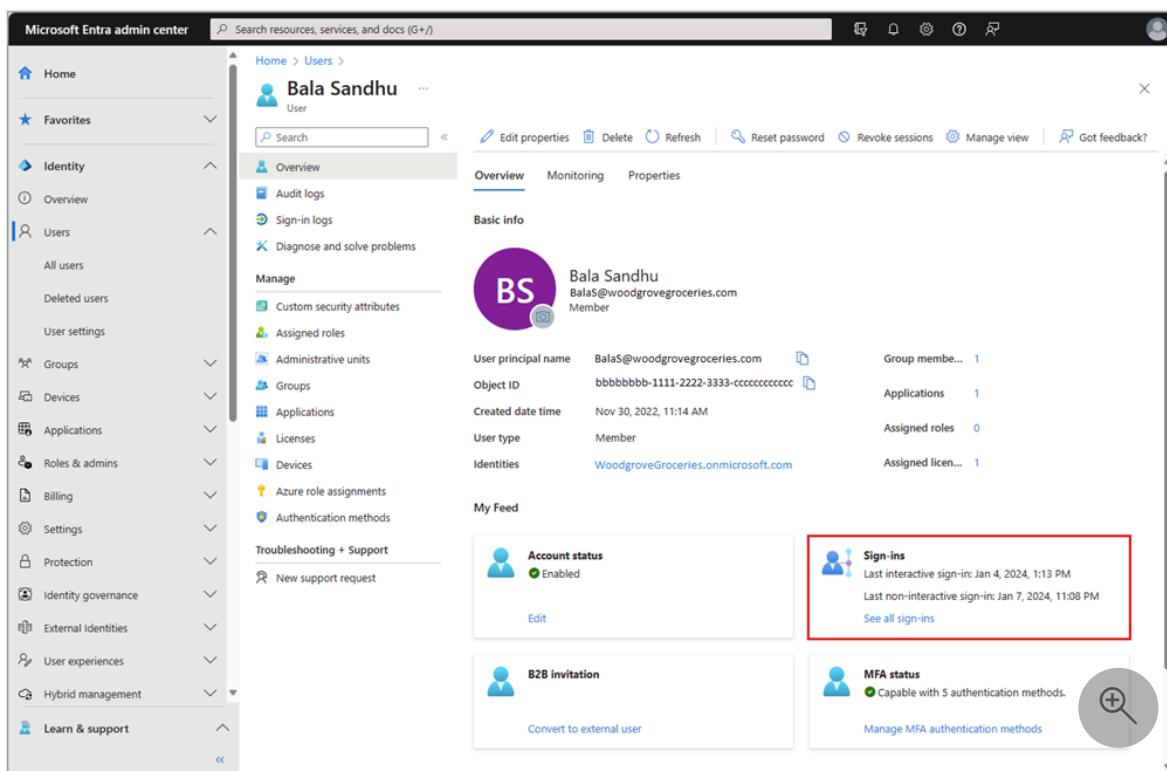
There are many more steps in this process that aren't reflected here. Even with these summarized steps, it's easy to see how latency can be introduced into the system.

Last sign-in

The last sign-in of a user is one of the most common questions related to log latency. This information is provided by the `signInActivity` property in Microsoft Graph. The `signInActivity` property provides the last interactive and non-interactive sign-in *attempt* for a user. This property might take up to 24 hours to update. For more information, see [signInActivity resource type](#).

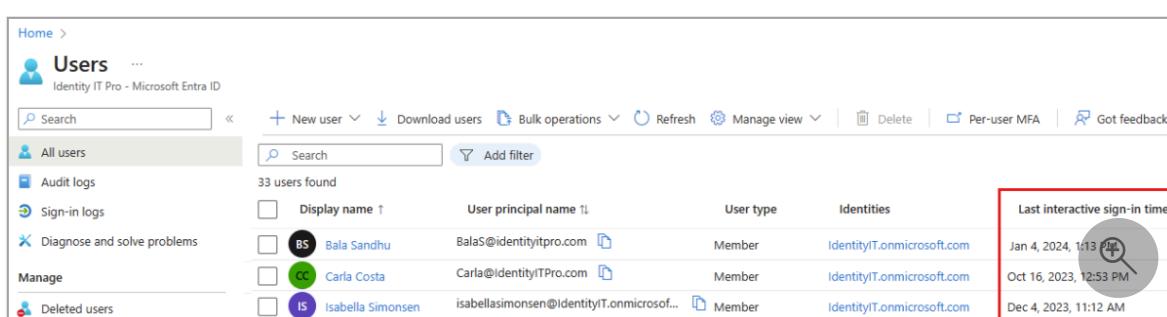
You must be using a [Microsoft Entra role](#) that grants access to the sign-in logs to see this detail, which is found in several places:

- The **Sign-ins** tile in the **My Feed** section of the user's profile.



The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation sidebar with various categories like Home, Favorites, Identity, Users, Groups, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, and Learn & support. The main area shows the user profile for "Bala Sandhu". The "Overview" tab is selected. Below the overview, there's a "Basic info" section with a purple circular profile picture labeled "BS". It lists the user's principal name (BalaS@woodgrovegroceries.com), object ID (bbbbbbb-111-2222-3333-ccccccccccc), created date (Nov 30, 2022, 11:14 AM), user type (Member), identities (WoodgroveGroceries.onmicrosoft.com), and group membership (1). In the "My Feed" section, there are four tiles: "Account status" (Enabled), "Sign-ins" (highlighted with a red box), "B2B invitation" (Convert to external user), and "MFA status" (Capable with 5 authentication methods). The "Sign-ins" tile displays the last interactive sign-in (Jan 4, 2024, 1:13 PM) and the last non-interactive sign-in (Jan 7, 2024, 11:08 PM).

- The **Last interactive sign-in** and **Last non-interactive sign-in** columns in the **Users** list.



The screenshot shows the "Users" list page in the Microsoft Entra admin center. The top navigation bar includes "Home", "Users", "Identity IT Pro - Microsoft Entra ID", and search/filter options. The main table lists 33 users found, with columns for "Display name", "User principal name", "User type", "Identities", and "Last interactive sign-in time". The "Last interactive sign-in time" column for user "Bala Sandhu" is highlighted with a red box and shows the value "Jan 4, 2024, 1:13 PM". Other users listed include "Carla Costa" and "Isabella Simonsen".

Display name	User principal name	User type	Identities	Last interactive sign-in time
Bala Sandhu	BalaS@identityitpro.com	Member	IdentityIT.onmicrosoft.com	Jan 4, 2024, 1:13 PM
Carla Costa	Carla@identityITPro.com	Member	IdentityIT.onmicrosoft.com	Oct 16, 2023, 12:53 PM
Isabella Simonsen	isbellasimonsen@IdentityIT.onmicrosoft.com	Member	IdentityIT.onmicrosoft.com	Dec 4, 2023, 11:12 AM

- The sign-in logs filtered for a particular user.

Bala Sandhu | Sign-in logs

Date : Last 7 days Show dates as : Local User contains Add filters

Date	Request ID	Application	Status	Correlation ID	Conditional Access	Authentication requi...
1/8/2024, 9:39:20 AM	b6730eaa-9e3e-42d2-bd...	Azure Portal	Success	dddd3333-ee44-5555-6...	Success	Multifactor authentication
1/8/2024, 9:32:55 AM	70584d8b-7255-4cfa-b1...	Azure Portal	Success	dddd3333-ee44-5555-6...	Success	Multifactor authentication
1/8/2024, 9:29:01 AM	b78523ed-eabf-44b0-af5...	Azure Portal	Success	dddd3333-ee44-5555-6...	Success	Multifactor authentication
1/4/2024, 1:19:23 PM	cbbc54f-49d5-4234-89b...	Azure Portal	Success	aaaa6666-bb77-8888-9...	Success	Multifactor authentication
1/4/2024, 9:08:43 AM	0d3ed0ac-97e1-4cd7-be...	Azure Portal	Success	aaaa6666-bb77-8888-9...	Success	Multifactor authentication
1/3/2024, 2:15:31 PM	b1f10ba5-6ed1-4d51-aa...	Azure Portal	Success	aaaa6666-bb77-8888-9...	Success	Multifactor authentication
1/3/2024, 2:14:32 PM	7c4bc5a0-c47c-4a8c-beb...	Azure Portal	Success	aaaa6666-bb77-8888-9...	Success	Multifactor authentication

The last sign-in details that appear on the **Sign-ins** tile on the user profile and the **Last interactive sign-in** and **Last non-interactive sign-in** columns in the **Users** list are *not* real-time.

If you need to see the most recent sign-in date and time for a user, go to the sign-in logs and filter for that user.

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)

Microsoft Graph PowerShell cmdlets for Microsoft Entra monitoring and health

Article • 02/09/2024

With Microsoft Entra monitoring and health, you can get details on activities around all the write operations in your directory (audit logs) and authentication data (sign-in logs). Although the information is available by using the Microsoft Graph API, now you can retrieve the same data by using the Microsoft Graph PowerShell cmdlets for Identity monitoring and health.

This article gives you an overview of the Microsoft Graph PowerShell cmdlets to use for audit logs and sign-in logs. [Get started with Microsoft Graph PowerShell](#).

Audit logs

[Audit logs](#) provide traceability through logs for all changes done by various features within Microsoft Entra ID. Examples of audit logs include changes made to any resources within Microsoft Entra ID like adding or removing users, apps, groups, roles, and policies.

You get access to the audit logs using the `Get-MgAuditLogDirectoryAudit` cmdlet.

[] Expand table

Scenario	PowerShell command
Application Display Name	<code>Get-MgAuditLogDirectoryAudit -Filter "initiatedBy/app/displayName eq 'Azure AD Cloud Sync'"</code>
Category	<code>Get-MgAuditLogDirectoryAudit -Filter "category eq 'ApplicationManagement'"</code>
Activity Date Time	<code>Get-MgAuditLogDirectoryAudit -Filter "activityDateTime gt 2019-04-18"</code>
All of the above	<code>Get-MgAuditLogDirectoryAudit -Filter "initiatedBy/app/displayName eq 'Azure AD Cloud Sync' and category eq 'ApplicationManagement' and activityDateTime gt 2019-04-18"</code>

Sign-in logs

The [sign-ins](#) logs provide information about the usage of managed applications and user sign-in activities.

You get access to the sign-in logs using the `Get-MgAuditLogSignIn` cmdlet. Use the following table for more scenarios.

[\[+\] Expand table](#)

Scenario	Microsoft Graph PowerShell command
User Display Name	<code>Get-MgAuditLogSignIn -Filter "userDisplayName eq 'Timothy Perkins'"</code>
Create Date Time	<code>Get-MgAuditLogSignIn -Filter "createdDateTime gt 2023-04-18T17:30:00.0Z"</code> (Everything since 5:30 pm on 4/18)
Status	<code>Get-MgAuditLogSignIn -Filter "status/errorCode eq 50105"</code>
Application Display Name	<code>Get-MgAuditLogSignIn -Filter "appDisplayName eq 'StoreFrontStudio [wsfed enabled]'"</code>
All of the above	<code>Get-MgAuditLogSignIn -Filter "userDisplayName eq 'Timothy Perkins' and status/errorCode ne 0 and appDisplayName eq 'StoreFrontStudio [wsfed enabled]'"</code>

Next steps

- [Analyze activity logs with Microsoft Graph](#)

Microsoft service principal sign-in logs table

Article • 05/06/2025

The Microsoft service principal sign-in logs capture service-to-service authentication events for Microsoft services in your tenant. While not necessary for security investigations, the information can be useful for understanding how your services are interacting with each other.

How to access the logs

These logs are only available by configuring diagnostic settings in Microsoft Entra to route the logs to an endpoint of your choice. For full guidance on this process, see [Configure diagnostic settings](#).

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Administrator**.
2. Browse to **Entra ID > Monitoring & health > Diagnostics**.
3. Adjust the filters accordingly.
4. Select **+ Add diagnostic setting**.
5. Select the **MicrosoftServicePrincipalSignInLogs**.
6. Select the destination and subscription from the dropdown menus that appear.
7. Select the **Save** button.

Microsoft service principal sign-in logs

This table maps application IDs from the logs to the application name and a brief description of the application. This table is not exhaustive and will grow over time. Applications currently listed here illustrate the variety of applications that can be found in the logs.

Some application display names might include acronyms or abbreviations from previous application names. For example, some services still retain "AAD" (Azure Active Directory) in their display name, even though the service was rebranded to Microsoft Entra ID.

[] Expand table

Application display name	Application ID	Description
AAD App Management	f0ae4899-d877-4d3c-ae25-679e38eea492	Provides a single sign-on experience with access management to line of business applications, such as Salesforce or ServiceNow.
AAD Applications ARM RP	c8e14c19-0ae6-4966-bd07-	Creates and manages first party and non-Microsoft apps in internal Microsoft Services and

Application display name	Application ID	Description
	17e5ffa8e4ce	infrastructure tenants only. This app doesn't work outside of allowlisted tenants.
App Protection	c6e44401-4d0a-4542-ab22-ecd4c90d28d7	Automatically disables applications based on user-defined and predefined policies. This app doesn't create app registrations or service principals in your tenant but can disable a service principal associated with a suspicious application.
Azure AD Application Proxy	47ee738b-3f1a-4fc7-ab11-37e4822b007e	Provides ability to publish applications inside your private network and provides access to users outside your network. This app is used as part of workflows for both Microsoft Entra Private Access and Microsoft Entra Application Proxy.
Azure ESTS Service	fc03f97a-9db0-4627-a216-ec98ce54e018	Standards compliant authentication service for Microsoft Entra.
Azure HDInsight Cluster API	fc03f97a-9db0-4627-a216-ec98ce54e018	Big data analytics service that includes the Apache Hadoop and Apache Spark ecosystems, which enables the processing of massive amounts of data.
Azure Machine Learning	0736f41a-0425-4b46-bdb5-1563eff02385	Cloud service for accelerating and managing the machine learning project lifecycle.
Azure Security Insights	98785600-1bb7-4fb9-b9fa-19afe2c8a360	Cloud-native solution that provides Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) functionality.
Azure SQL Managed Instance to Azure AD Resource Provider	913c6de4-2a4a-4a61-a9ce-945d2b2ce2e0	Platform as a service (PaaS) that offers cloud-enhanced SQL Server within an isolated private virtual network environment.
Bot Framework Dev Portal	f3723d34-6ff5-4ceb-a148-d99dcd2511fc	Creates an app registration on behalf of the user when the Azure Bot Service (ABS) is asked to create a new app registration during the ABS resource creation process.
CPIM Service	bb2a2e3a-c5e7-4f0a-88e0-8e01fd3fc1f4	The Customer and Partner Identity Management (CPIM) service provides a solution for customers to create user directories for external identities to authenticate to apps registered in their tenant.

Application display name	Application ID	Description
		These external identity features can include social identity providers, such as Google or Facebook, self-service sign-up, and API connectors in the self-service sign-up flow.
Dynamics Lifecycle services	bb2a2e3a-c5e7-4f0a-88e0-8e01fd3fc1f4	An Azure-based portal that provides a unifying, collaborative environment for customers and partners to manage the application lifecycle of their Microsoft Dynamics implementations.
Fabric Identity Management	c0be6b4c-212d-4ca9-8a35-fd260fe22342	Creates and manages Fabric Workspace Identities.
MDATPNetworkScanAgent	04687a56-4fc2-4e36-b274-b862fb649733	Creates non-Microsoft apps within the customer tenant for each NetworkScan agent registered at customer sites.
Microsoft Rights Management Services	00000012-0000-0000-c000-000000000000	Also known as the Azure Rights Management Service, this app applies encryption via Purview labels and other encryption related tasks.
Microsoft Volume Licensing	3ab9b3bc-762f-4d62-82f7-7e1d653ce29f	Commerce platform that supports the Microsoft Product and Services Agreement (MPSA), which is a transactional licensing agreement for commercial, government, and academic organizations with 250 or more users/devices.
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000	This app represents the first-party instance of OneDrive and SharePoint apps.
Partner Customer Delegated Admin Migration	39d63e7-7fa3-4b2b-94ea-ee256fdb8c2f	Granular Delegated Admin Privileges (GDAP) uses Extended Tools and Production (XTAP) to grant a partner's access to a customer tenant.
Power Virtual Agents Service 9d8f559b-5984-46a4-902a-ad4271e83efa	9d8f559b-5984-46a4-902a-ad4271e83efa 9d8f559b-5984-46a4-902a-ad4271e83efa	Power Virtual Agents is the former name for Microsoft Copilot Studio. Both instances of this app allow the service to manage the applications and service principals created for each agent.
Storage Resource Provider	a6aa9161-5291-40bb-8c5c-923b567bee3b	Enables customers to manage storage accounts and keys programmatically.
SubstrateActionService	06dd8193-75af-46d0-84bb-	Assists non-Microsoft app developers to build customized MessageExtension apps like Poll and

Application display name	Application ID	Description
	9b9bcaa89e8b	Survey for use in Microsoft Teams.
ZTNA Network Access Control Plane	9d4afbbc-06a4-49e0-8005-4e5afd1d4fec	A feature of Global Secure Access, this app allows admins to control their network change's effect and try new features without affecting their onboarded environments.

SLA performance for Microsoft Entra ID

Article • 05/02/2025

As an identity admin, you might need to track the Microsoft Entra service-level agreement (SLA) performance to make sure Microsoft Entra ID can support your vital apps. This article shows how the Microsoft Entra service has performed according to the [SLA for Microsoft Entra ID](#).

You can use this article in discussions with app or business owners to help them understand the performance they can expect from Microsoft Entra ID.

!**Note**

This article applies to both workforce and external tenants. (Learn more about [tenant configurations](#)).

How is SLA measured for Microsoft Entra ID?

Details on how downtime is defined and how uptime percentage is calculated are provided in the [SLA for Microsoft Entra ID](#).

Performance is measured in a way that reflects customer authentication experience, rather than simply reporting on whether the system is available to outside connections. This distinction means that the calculation is based on if:

- Users can authenticate
- Microsoft Entra ID successfully issues tokens for target apps after authentication

No planned downtime

You rely on Microsoft Entra ID to provide identity and access management for your vital systems. To ensure Microsoft Entra ID is available when business operations require it, Microsoft doesn't plan downtime for Microsoft Entra system maintenance. Instead, maintenance is performed as the service runs, without customer impact.

Recent worldwide SLA performance

To help you plan for moving workloads to Microsoft Entra ID, we publish past SLA performance. These numbers show the level at which Microsoft Entra ID met the requirements in the [SLA for Microsoft Entra ID](#), for all tenants.

The numbers in the table are a global total of Microsoft Entra authentications across all customers and geographies. The number is truncated at three places after the decimal. Numbers aren't rounded up, so actual SLA attainment is higher than indicated.

 Expand table

Month	2021	2022	2023	2024	2025
January		99.998%	99.998%	99.999%	99.998%
February	99.999%	99.999%	99.999%	99.999%	99.998%
March	99.568%	99.998%	99.999%	99.999%	99.996%
April	99.999%	99.999%	99.999%	99.999%	99.999%*
May	99.999%	99.999%	99.999%	99.999%	
June	99.999%	99.999%	99.999%	99.999%	
July	99.999%	99.999%	99.999%	99.999%	
August	99.999%	99.999%	99.999%	99.999%	
September	99.999%	99.998%	99.999%	99.999%	
October	99.999%	99.999%	99.999%	99.998%	
November	99.998%	99.999%	99.999%	99.998%	
December	99.978%	99.999%	99.999%	99.998%	

*Starting in April 2025, we updated our SLA performance calculations to provide a more complete view of the user experience with authentication availability. The new calculation includes authentication successes from Microsoft Entra's resilient infrastructure, such as when the [backup authentication system](#) succeeds on retry. Prior to April 2025, these successful sign-ins were not included in the SLA calculation. With the addition of this new calculation, the SLA performance percentages will increase. For example, the April 2025 number using the previous calculation logic would have been 99.998%. With new logic, it's 99.999%.

Incident history

All incidents that seriously affect Microsoft Entra performance are documented in the [Azure status history](#). Not all events documented in Azure status history are serious enough to cause Microsoft Entra ID to go below its SLA. You can view information about the impact of incidents, and a root cause analysis of what caused the incident and what steps Microsoft took to prevent future incidents.

SLA attainment

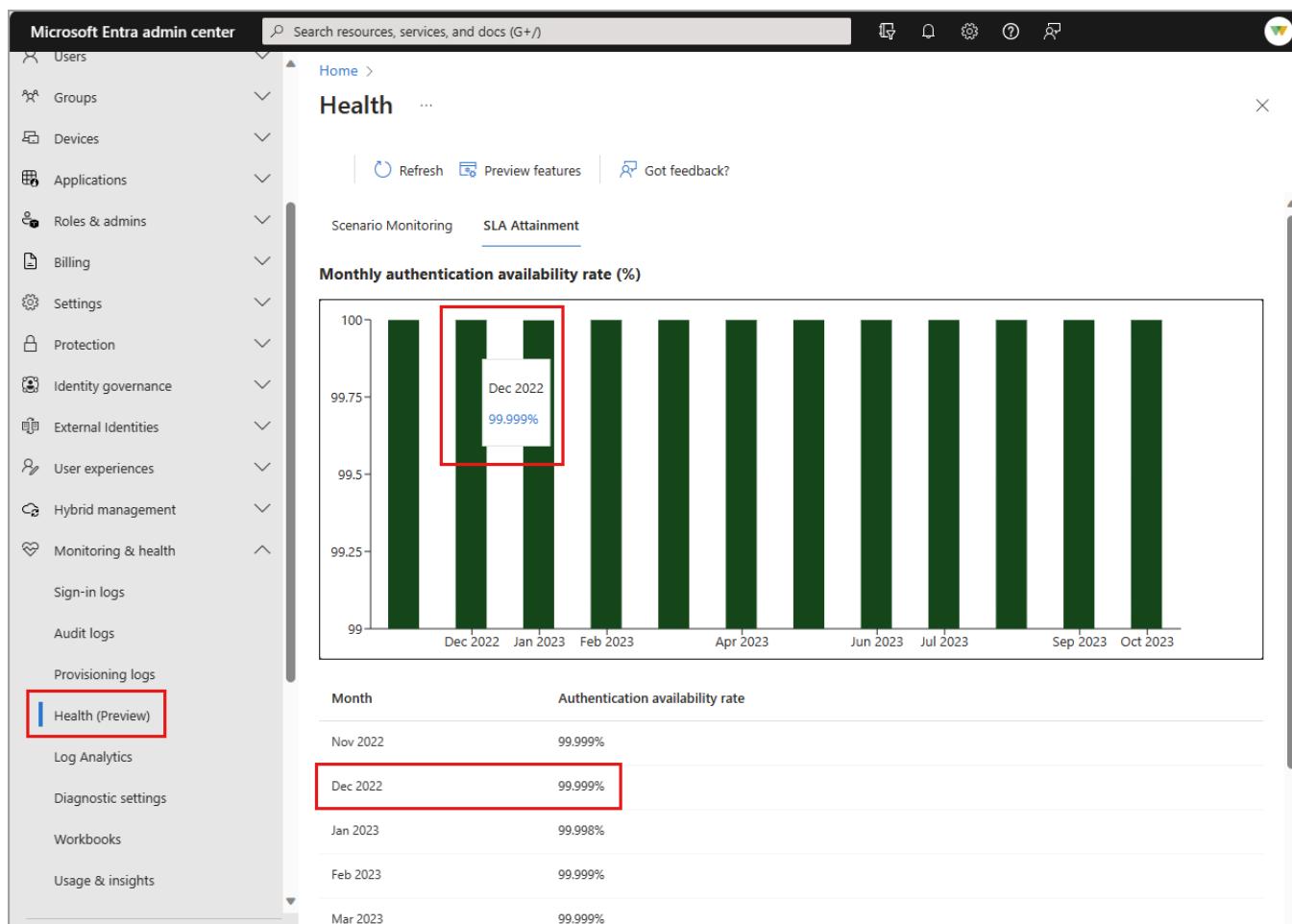
In addition to publicly reporting global SLA performance, Microsoft Entra ID provides tenant-level SLA performance for organizations with at least 5000 monthly active users. The Service Level Agreement (SLA) attainment is the user authentication availability for Microsoft Entra ID. For the current availability target and details on how SLA is calculated, see [SLA for Microsoft Entra ID](#).

To see the tenant-level SLA:

1. Sign in to the [Microsoft Entra admin center](#).
2. Browse to **Entra ID > Monitoring & health > Health**.

Hover your mouse over the bar for a month to view the percentage for that month. A table with the same details appears below the graph.

You can also view SLA attainment using [Microsoft Graph APIs](#).



Related content

- [Microsoft Entra monitoring and health overview](#)
- [Programmatic access to Microsoft Entra reports](#)

- Microsoft Entra risk detections

Frequently asked questions around Microsoft Entra monitoring and health

FAQ

This article includes answers to frequently asked questions about Microsoft Entra monitoring and health. For more information, see [Microsoft Entra monitoring and health overview](#).

Licensing

How do I get a premium license?

See [Microsoft Entra ID licensing](#) to upgrade your Microsoft Entra edition.

How soon should I see activity log data after getting a premium license?

If you already have activity log data with a free license, you can see it immediately. If you don't have any data, it can take up to three days for the data to show up in the reports.

Can I see last month's data after getting a Microsoft Entra ID P1 or P2 license?

If you recently switched to a Premium version (including a trial version), you can see data up to seven days initially. When data accumulates, you can see data for the past 30 days.

Activity logs and reports

What role do I need to see the activity logs in the Microsoft Entra admin center?

The [least privileged role](#) to view audit and sign-in logs is **Reports Reader**. Other roles include **Security Reader** and **Security Administrator**.

What logs can I integrate with Azure Monitor?

Sign-in, audit, provisioning, ID Protection, network access, and many other logs can be integrated with Azure Monitor and other monitoring and alerting tools. B2C-related audit

events are currently not included. For a complete list of the Microsoft Entra logs that can be integrated with other endpoints, see [Log options for streaming to endpoints](#).

Can I get Microsoft 365 activity log information through the Microsoft Entra admin center or the Azure portal?

Microsoft 365 and Microsoft Entra activity logs share many directory resources. If you want a full view of the Microsoft 365 activity logs, you should go to the [Microsoft 365 admin center](#) to get Office 365 Activity log information. The APIs for Microsoft 365 are described in the [Microsoft 365 Management APIs](#) article.

How many records I can download from the Microsoft Entra admin center?

Several factors determine the number of logs you can download from the Microsoft Entra admin center, such as browser memory size, network speeds, and Microsoft Entra reporting APIs loads. Generally, data sets smaller than 250,000 for audit logs and 100,000 for sign-in and provisioning logs work well with the browser download feature. Depending on the number of fields you included, this number could vary. If you face issues completing large downloads in the browser, use the [reporting API](#) to download the data or [send the logs to an endpoint through diagnostic settings](#).

The active filters in the Microsoft Entra admin center when you begin the download determine the specific set of logs you can download. For example, filtering to a specific user in the Microsoft Entra admin center mean your download pulls logs for that specific user. The columns in the downloaded logs do *not* change. The output contains all details of the audit or sign-in log, *regardless of the columns you customized in the Microsoft Entra admin center*.

How long does Microsoft Entra ID store activity logs? What is the data retention?

Depending on your license, Microsoft Entra ID stores activity logs for between 7 and 30 days. For more information, see [Microsoft Entra report retention policies](#).

Why do I see "Not found" when I select an app from the **Usage and Insights** report?

The **Usage and Insights** report now includes service-to-service authentication for Microsoft Cloud Services applications. If an application appears in this list, it likely means that it authenticated to or from an application that is homed in your tenant. But the application in the list is not homed in your tenant, only an instance of it appears in the report to show the authentication.

Audit logs

How can I find out if a user purchased a license or enabled a trial license for my tenant? I don't see this activity in the audit logs.

At this time, there isn't a specific activity in the audit logs for license purchases or enablement. However, you might be able to correlate the "Onboard resource to PIM" activity from the "Resource Management" category to the purchase or enablement of a license. This activity might not always be available or provide the exact details.

Sign-in logs

I used the signInActivity resource to look up a user's last sign-in time, but it hasn't updated after a few hours. When will it be updated with the latest sign in time?

The signInActivity resource is used to find inactive [users who haven't signed in for some time](#). It doesn't update in near real time. If you need to find the user's last sign-in activity more quickly, you can use the Microsoft Entra sign-in logs to see near real time sign-in activity for all your users.

What data is included in the CSV file I can download from the Microsoft Entra sign-in logs?

The CSV includes sign-in logs for the type of sign-ins you selected. Data that is represented as a nested array in the Microsoft Graph API for sign-in logs is *not* included. For example, Conditional Access policies and report-only information aren't included. If you need to export all the information contained in your sign-in logs, use the **Export Data Settings** feature.

It's also important to note the columns included in the downloaded logs don't change, even if you customized the columns in the Microsoft Entra admin center.

I see .XXX in part of the IP address or "PII Removed" in the Device Details of a user in my sign-in logs. Why is that happening?

Microsoft Entra ID might redact part of a sign-in log to protect user privacy in the following scenarios:

- During cross-tenant sign ins, such as when a CSP technician signs into a tenant that CSP manages.
- When our service wasn't able to determine the user's identity with sufficient confidence to be sure the user belongs to the tenant viewing the logs.
- Microsoft Entra ID redacts Personally Identifiable Information (PII) generated by devices that don't belong to your tenant to ensure customer data. PII doesn't spread beyond tenant boundaries without user and data owner consent.

I see duplicate sign-in entries / multiple sign-in events per requestId. Why is that happening?

There are several reasons sign-in entries might be duplicated in your logs.

- If a risk is identified on a sign-in, another nearly identical event is published immediately after with risk included.
- If MFA events related to a sign-in are received, all related events are aggregated to the original sign-in.
- If partner publishing for a sign-in event fails, such as publishing to Kusto, an entire batch of events is retried and published again, which might result in duplicates.
- Sign-in events that involve multiple Conditional Access policies might be split into multiple events, which can result in at least two events per sign-in event.

I'm investigating a sign-in event using Log Analytics, but the TimeGenerated time doesn't match the actual time of the sign-in. Why is that happening?

The TimeGenerated field in Log Analytics is the time the entry was received and published by Log Analytics. Remember, in order for your logs to appear in Log Analytics, you have to

configure diagnostics settings to *send* the logs to the Log Analytics workspace. That process takes time, so the TimeGenerated field might not match the actual time of the sign-in.

To confirm the date and time match the sign-in, look for the `CreatedDateTime` field a little further down in the Log Analytics results. The `AuthenticationDetails` fields can also be expanded to see the exact time of the sign-in. The time in Log Analytics appears in UTC, but the time in the sign-in logs in the Microsoft Entra admin center appears in local time, so you might need to adjust.

Risky sign-in events also have a different TimeGenerated time than the actual sign-in time. The TimeGenerated time for risky sign-ins is the time the risk was detected, not the time of the sign-in. Check the risky sign-in event itself for the activity time, which is the actual time of the sign-in.

Why do my non-interactive sign-ins appear to have the same time stamp?

Non-interactive sign-ins can trigger a large volume of events every hour, so they're grouped together in the logs.

In many cases, non-interactive sign-ins have all the same characteristics, except for the date and time of the sign-in. If the time aggregate is set to 24 hours, the logs appear to show the sign-ins at the same time. Each of these grouped rows can be expanded to view the exact time stamp.

I'm seeing User IDs / Object IDs / GUIDs in the username field of my sign-in log. Why is this happening?

There are several reasons why sign-in entries might display User IDs, Object IDs, or GUIDs in the username field.

- With passwordless authentication, User IDs appear as the username. To confirm this scenario, look at the details of the sign-in event in question. The *authenticationDetail* field says *passwordless*.
- The user authenticated but has not yet signed in. To confirm, there's an *error code 50058* that correlates with an interrupt.
- If the username field shows *000000-0000-0000-0000* or something similar, there could be tenant restrictions in place, preventing the user from signing in to the selected tenant.
- Multifactor authentication sign-in attempts are aggregated with multiple data entries, which might take longer to display properly. Data might take up to two hours to fully

aggregate, but rarely takes that long.

I see a 90025 error in the sign in logs. Does this mean my user failed to sign in? Has my tenant hit a throttling limit?

No, in general 90025 errors are resolved by an automatic retry without the user noticing the error. This error can occur when an internal Microsoft Entra subservice hits its retry allowance and doesn't indicate your tenant is being throttled. These errors are usually resolved by Microsoft Entra ID internally. If the user is unable to sign in due to this error, manually trying again should resolve the issue.

In the Service Principal sign-in logs, what does it mean if I see "00000000-0000-0000-0000-000000000000" or " " for Service Principal ID or Resource Service Principal ID in my sign-in logs?

If the Service Principal ID has the value "00000000-0000-0000-0000-000000000000" there's no Service Principal for the client application in that instance of authentication. Microsoft Entra no longer issues access tokens without a client Service Principal, except for a few Microsoft and non-Microsoft applications.

If the Resource Service Principal ID has the value "00000000-0000-0000-0000-000000000000," there's no Service Principal for the resource application in that instance of authentication.

This behavior is currently allowed only for a limited number of resource apps.

You can query for instances of authentication without a client or resource Service Principal in your tenant.

- To find instances of sign-in logs for your tenant where a client Service Principal is missing, use the following query:

```
https://graph.microsoft.com/beta/auditLogs/signIns?  
$filter=signInEventTypes/any(t: t eq 'servicePrincipal') and  
servicePrincipalId eq '00000000-0000-0000-0000-000000000000'
```

- To find instances of sign-in logs for your tenant where a resource Service Principal is missing, use the following query:

```
https://graph.microsoft.com/beta/auditLogs/signIns?  
$filter=signInEventTypes/any(t: t eq 'servicePrincipal') and  
resourceServicePrincipalId eq '00000000-0000-0000-0000-000000000000'
```

You can also find these sign-in logs in Microsoft Entra admin center.

- Sign in to the [Microsoft Entra admin center](#).
- Browse to **Entra ID > Monitoring & health > Sign-in logs**.
- Select **Service Principal Sign-ins**.
- Select an appropriate time frame in the Date field (last 24 hours, 7 days, and so on).
- Add a filter and select **Service Principal ID** and provide the value '00000000-0000-0000-0000-000000000000' to get instances of authentication with no client Service Principal.

How can I restrict sign-in (authentication) for various apps that I see in the Service Principal sign-in logs?

If you wish to control how authentication works in your tenant for specific client or resource apps, follow instructions in the [Restrict Microsoft Entra app to a set of users](#) article.

Why do sign-ins that are technically non-interactive show up on my interactive sign-in logs?

Some non-interactive sign-ins were made available before the non-interactive sign-in logs were available in public preview. These non-interactive sign-ins were included in the interactive sign-in logs and remained in the interactive sign-in logs after the non-interactive logs became available. Sign-ins using the FIDO2 keys are an example of non-interactive sign-ins that show up in the interactive sign-in logs. At this time, these non-interactive logs are always included in the interactive sign-in log.

What reporting API should I use for Identity Protection risk detections, such as leaked credentials or sign-ins from anonymous IP addresses?

You can use the [Identity Protection risk detections API](#) to access security detections through Microsoft Graph. This API includes advanced filtering and field selection and standardizes risk detections into one type for easier integration into SIEMs and other data collection tools.

Conditional Access

What Conditional Access details can I see in the sign-in logs?

You can troubleshoot Conditional Access policies through all sign-in logs. Review the Conditional Access status and dive into the details of the policies that applied to the sign-in and the result for each policy.

To get started:

- Sign in to the [Microsoft Entra admin center](#).
- Browse to **Entra ID > Monitoring & health > Sign-in logs**.
- Select the sign-in that you want to troubleshoot.
- Select the **Conditional Access** tab to view all the policies that impacted the sign-in and the result for each policy.

What are all possible values for the Conditional Access status?

Conditional Access status can have the following values:

- **Not Applied:** There was no Conditional Access policy with the user and app in scope.
- **Success:** There was a Conditional Access policy with the user and app in scope and Conditional Access policies were successfully satisfied.
- **Failure:** The sign-in satisfied the user and application condition of at least one Conditional Access policy and grant controls are either not satisfied or set to block access.

What are all possible values for the Conditional Access policy result?

A Conditional Access policy can have the following results:

- **Success:** The policy was successfully satisfied.
- **Failure:** The policy wasn't satisfied.
- **Not applied:** The policy conditions might not have been met.
- **Not enabled:** The policy might be in a disabled state.

The policy name in the sign-in log doesn't match the policy name in Conditional Access. Why?

The policy name in the sign-in log is based on the Conditional Access policy name at the time of the sign-in. The name can be inconsistent with the policy name in Conditional Access if you updated the policy name after the sign-in.

My sign-in was blocked due to a Conditional Access policy, but the sign-in log shows that the sign-in succeeded. Why?

Currently the sign-in log might not show accurate results for Exchange ActiveSync scenarios when Conditional Access is applied. There can be cases when the sign-in result in the report shows a successful sign-in, but the sign-in actually failed due to a policy.

Why does Windows Sign-in or Windows Hello for Business show as "out of scope" or "not applicable" on the Conditional Access tab in the sign-in log details?

Conditional Access policies don't apply to Windows Sign-in or Windows Hello for Business. Conditional Access policies protect sign-in attempts to cloud resources, not the Windows sign-in process.

Microsoft Graph APIs

I currently use the ``https://graph.windows.net/<tenant-name>/reports/`` endpoint APIs to pull Microsoft Entra audit and integrated application usage reports into our reporting systems programmatically. What should I switch to?

Look up the [API reference](#) to see how you can use the APIs to access activity logs. This endpoint has two reports (**Audit** and **Sign-ins**) which provide all the data you got in the old API endpoint. This new endpoint also has a sign-ins report with the Microsoft Entra ID P1 or P2 license that you can use to get app usage, device usage, and user sign-in information.

I currently use the `https://graph.windows.net/<tenant-name>/reports/` endpoint APIs to pull Microsoft Entra security reports (specific types of detections, such as leaked credentials or sign-ins from anonymous IP addresses) into our reporting systems programmatically. What should I switch to?

You can use the [Identity Protection risk detections API](#) to access security detections through Microsoft Graph. This new format gives greater flexibility in how you can query data. The format provides advanced filtering, field selection, and standardizes risk detections into one type for easier integration into SIEMs and other data collection tools. Because the data is in a different format, you can't substitute a new query for your old queries. However, [the new API uses Microsoft Graph](#), which is the Microsoft standard for such APIs as Microsoft 365 or Microsoft Entra ID. So the work required can either extend your current Microsoft Graph investments or help you begin your transition to this new standard platform.

I keep getting permissions errors when running queries. I thought I had the appropriate role.

You might need to sign in to Microsoft Graph separately from the Microsoft Entra admin center. Select your profile icon on the upper-right corner and sign in to the right directory. You might be trying to run a query that you don't have permissions for. Select **Modify Permissions** and select the **Consent** button. Follow the sign-in prompts.

Why are there `MicrosoftGraphActivityLogs` events that don't correlate to a Service Principal sign-in?

Every time a token is used to call a Microsoft Graph endpoint, the `MicrosoftGraphActivityLogs` are updated with that call. Some of those calls are first-party, app-only calls, which aren't published to the Service Principal sign-in logs. When a `MicrosoftGraphActivityLogs` shows a `uniqueTokenIdentifier` that you can't locate in the sign-in logs, the token identifier is referencing a first-party app-only token.

Recommendations

Why did a recommendation that was "completed" change back to "active"?

If the service detects activity related to that recommendation for something marked as "completed" it changes automatically back to "active."

Microsoft service principal sign-in logs (preview)

I've enabled the `'MicrosoftServicePrincipalSignInLogs'` through diagnostic settings, but I'm unsure what to do with this data.

This log is in preview and might not be available for all customers. These logs provide visibility into service-to-service authentication, specifically for Microsoft-owned applications to keep token issuance authentications to customer-owned resources transparent.

In the unlikely scenario where an application is used to gain access into other resources, these logs could provide the information needed to pinpoint the source of the compromise.

Where can I learn more about why these calls are happening?

The specific reasons behind Microsoft-owned applications requesting or issuing tokens are part of our system's design and can't be shared publicly. The logs are shared to maintain transparency and provide visibility into authentications that are occurring within the boundaries of our customers' tenants.

Is this data essential for security investigations?

We have categorized datasets from our Microsoft Entra log streams based on their importance for security investigations. This particular dataset is considered a much lower priority compared to others. While having this data is beneficial, not enabling it should not negatively impact your security posture.

What actions can I take on this data?

We recommend being very cautious before making any changes to Microsoft-owned applications. These applications often have essential settings, like token issuance for billing applications. Disabling them could result in losing access to your account. Our internal security teams have implemented extensive security controls and access policies to keep these applications secure. We are confident in their security, and we strongly advise against making any additional changes to them.

If you choose to block or control these applications, it might lead to unexpected issues, and unfortunately, we won't be able to support or take responsibility for those problems.

appCredentialSignInActivity resource type

Article • 07/31/2024

Namespace: microsoft.graph

ⓘ Important

APIs under the `/beta` version in Microsoft Graph are subject to change. Use of these APIs in production applications is not supported. To determine whether an API is available in v1.0, use the **Version** selector.

Represents an application credential activity in a given tenant. This resource contains information about the last usage time of an application credential.

For more information about this report, see [Usage and insights report: Microsoft Entra application activity \(preview\)](#)

Methods

Expand table

Method	Return Type	Description
List	appCredentialSignInActivity collection	Get a list of appCredentialSignInActivity objects that contains recent activity of application credentials.
Get	appCredentialSignInActivity	Get an appCredentialSignInActivity object that contains recent activity of an application credential.

Properties

Expand table

Property	Type	Description
appId	String	The globally unique appId (also called <i>client ID</i> on the Microsoft Entra admin center) of the credentialed application.
appObjectId	String	The ID of the credential application instance.
createdDateTime	DateTimeOffset	The date and time when the credential was created. The Timestamp type represents date and time information

Property	Type	Description
		using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> .
credentialOrigin	applicationKeyOrigin	The type the key credential originated from. Possible values are: <code>application</code> , <code>servicePrincipal</code> , <code>unknownFutureValue</code> .
expirationDateTime	DateTimeOffset	The date and time when the credential is set to expire. The <code>Timestamp</code> type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> .
id	String	The unique identifier of the <code>appCredentialSignInActivity</code> instance in the response.
keyId	String	The key ID of the credential.
keyType	applicationKeyType	Specifies the key type. The possible values are: <code>clientSecret</code> , <code>certificate</code> , <code>unknownFutureValue</code> .
keyUsage	applicationKeyUsage	Specifies what the key was used for. The possible values are: <code>sign</code> , <code>verify</code> , <code>unknownFutureValue</code> .
resourceId	String	The ID of the accessed resource.
servicePrincipalObjectId	String	The ID of the service principal.
signInActivity	signInActivity	The sign-in activity of the credential across all flows.

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

JSON

```
{
  "@odata.type": "#microsoft.graph.appCredentialSignInActivity",
  "appId": "String",
  "appObjectId": "String",
  "createdDateTime": "String (timestamp)",
  "credentialOrigin": "String",
```

```
"expirationDateTime": "String (timestamp)",
"id": "String (identifier)",
"keyId": "String",
"keyType": "String",
"keyUsage": "String",
"resourceId": "String",
"servicePrincipalObjectId": "String",
"signInActivity": {"@odata.type": "microsoft.graph.signInActivity"}  
}
```

directoryAudit resource type

Article • 05/24/2024

Namespace: microsoft.graph

Represents the directory audit items and its collection.

Methods

[] Expand table

Method	Return Type	Description
List	directoryAudit	List the directory audit items in the collection and their properties.
Get	directoryAudit	Get a specific directory audit item and its properties.

Properties

[] Expand table

Property	Type	Description
activityDateTime	DateTimeOffset	Indicates the date and time the activity was performed. The Timestamp type is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Supports <code>\$filter (eq, ge, le)</code> and <code>\$orderby</code> .
activityDisplayName	String	Indicates the activity name or the operation name (examples: "Create User" and "Add member to group"). For a list of activities logged, refer to Microsoft Entra audit log categories and activities . Supports <code>\$filter (eq, startswith)</code> .
additionalDetails	keyValue collection	Indicates additional details on the activity.
category	String	Indicates which resource category that's targeted by the activity. For example: <code>UserManagement</code> , <code>GroupManagement</code> , <code>ApplicationManagement</code> , <code>RoleManagement</code> . For a list of categories for activities logged, refer to Microsoft Entra audit log categories and activities .
correlationId	Guid	Indicates a unique ID that helps correlate activities that span across various services. Can be used to trace logs across services. Supports <code>\$filter (eq)</code> .

Property	Type	Description
id	String	Indicates the unique ID for the activity. This is a GUID. Supports <code>\$filter (eq)</code> .
initiatedBy	auditActivityInitiator	Indicates information about the user or app initiated the activity. Supports <code>\$filter (eq)</code> for <code>user/id</code> , <code>user/displayName</code> , <code>user/userPrincipalName</code> , <code>app/appId</code> , <code>app/displayName</code> ; and <code>\$filter (startswith)</code> for <code>user/userPrincipalName</code> .
loggedByService	String	Indicates information on which service initiated the activity (For example: <code>Self-service Password Management</code> , <code>Core Directory</code> , <code>B2C</code> , <code>Invited Users</code> , <code>Microsoft Identity Manager</code> , <code>Privileged Identity Management</code> . Supports <code>\$filter (eq)</code>).
operationType	String	Indicates the type of operation that was performed. The possible values include but are not limited to the following: <code>Add</code> , <code>Assign</code> , <code>Update</code> , <code>Unassign</code> , and <code>Delete</code> .
result	<code>operationResult</code>	Indicates the result of the activity. Possible values are: <code>success</code> , <code>failure</code> , <code>timeout</code> , <code>unknownFutureValue</code> .
resultReason	String	Indicates the reason for failure if the <code>result</code> is <code>failure</code> or <code>timeout</code> .
targetResources	targetResource collection	Indicates information on which resource was changed due to the activity. Target Resource Type can be <code>User</code> , <code>Device</code> , <code>Directory</code> , <code>App</code> , <code>Role</code> , <code>Group</code> , <code>Policy</code> or <code>Other</code> . Supports <code>\$filter (eq)</code> for <code>id</code> and <code>displayName</code> ; and <code>\$filter (startswith)</code> for <code>displayName</code> .

Relationships

None

JSON representation

The following JSON representation shows the resource type.

JSON

```
{
  "activityDateTime": "String (timestamp)",
  "activityDisplayName": "String",
  "additionalDetails": [{"@odata.type": "microsoft.graph.keyValue"}],
```

```
"category": "String",
"correlationId": "Guid",
"id": "String (identifier)",
"initiatedBy": {"@odata.type": "microsoft.graph.auditActivityInitiator"},
"loggedByService": "String",
"operationType": "String",
"result": "String",
"resultReason": "String",
"targetResources": [{"@odata.type": "microsoft.graph.targetResource"}]
}
```

Use the Microsoft Entra recommendations API to implement Microsoft Entra ID best practices for your tenant

Article • 06/13/2024

Microsoft Entra recommendations are personalized and actionable insights for you to implement Microsoft Entra ID best practices in your tenant. The Microsoft Entra recommendation service runs daily to check your tenant against predefined conditions for every recommendation. If the service detects that a recommendation applies to your tenant, the corresponding recommendation object is generated and its status is set to active.

Use the recommendations API in Microsoft Graph to identify and track the insights, assess and apply the guidance provided for implementing the best practices, and keep your tenant healthy, secure, and optimized.

Manage recommendations

Microsoft Entra recommendations are made up of two building blocks: **recommendations** and **the Microsoft Entra resources they apply to**.

A single recommendation can apply to one or more Microsoft Entra resource instances. For example, a recommendation relating to expiring application credentials referencing all apps in your tenant that have expiring application credentials.

For each recommendation, you have the following data:

- The type of recommendation. A limited number is currently supported. For more information, see [Types of recommendations](#).
- The Microsoft Entra resources to which the recommendation applies. These include users, groups, and applications.
- The recommended action plan to address the recommendation.
- Where applicable, when Microsoft Entra ID recommends the recommendation to have been completed before it impacts the associated service.
- The impact of the recommendation, which can be tenant-wide or resource-specific.
- A Microsoft-assigned priority ranking for the recommendation.
- The status of the recommendation such as whether it's still active or has been completed, dismissed, or postponed to a future date.

Types of recommendations

Eight types of recommendations are currently available in Microsoft Entra recommendations. These recommendations are identified in a **recommendationType** property that's part of the [recommendation resource type](#) in Microsoft Graph.

The following table lists the recommendation types that are available, and maps the Microsoft Graph values to the user-friendly names that are used on the Microsoft Entra admin center.

[+] [Expand table](#)

recommendationType	Friendly name in the Microsoft Entra admin center	Comments
adfsAppsMigration	Migrate your eligible applications from AD FS to Microsoft Entra ID for more security, productivity and automation	For more information, see Migrate apps from ADFS to Microsoft Entra ID
aadGraphDeprecationApplication, aadGraphDeprecationServicePrincipal	Migrate from Azure AD Graph APIs to Microsoft Graph	For more information, see Migrate from Azure AD Graph APIs to Microsoft Graph
adalToMsalMigration	Migrate from the Azure Active Directory Authentication Library to the Microsoft Authentication Libraries	For more information, see Migrate from the Azure Active Directory Authentication Library to the Microsoft Authentication Libraries
applicationCredentialExpiry	Renew expiring application credentials	For more information, see Renew expiring application credentials
mfaServerDeprecation	Migrate from MFA server to Microsoft Entra multifactor authentication (MFA)	For more information, see Migrate from MFA server to Microsoft Entra multifactor authentication (MFA)
servicePrincipalKeyExpiry	Renew expiring service principal credentials	For more information, see Renew expiring service principal credentials
staleApps	Remove unused applications	For more information, see Remove unused applications
staleAppCreds	Remove unused credentials from applications	For more information, see Remove unused credentials from apps

recommendationType	Friendly name in the Microsoft Entra admin center	Comments
switchFromPerUserMFA	Convert per-user MFA to Conditional Access MFA	For more information, see Convert per-user MFA to Conditional Access MFA
tenantMFA	Minimize MFA prompts for your users signing in from known devices	For more information, see Minimize MFA prompts from known devices
useAuthenticatorApp	Migrate eligible users from SMS and voice call to Microsoft Authenticator App for a better MFA user experience	For more information, see Migrate to Microsoft authenticator

API scenarios

You manage recommendations through the [recommendation resource type](#) and its associated methods. This resource type exposes the **impactedResources** relationship that you use to query the Microsoft Entra resource to which the recommendations apply.

The following are some of the most popular requests for working with the Microsoft Graph recommendations API:

[] [Expand table](#)

Scenarios	API
Retrieve all recommendations and their associated data, including the impacted resources.	List recommendations
Retrieve a recommendation and its associated data, including the impacted resources.	Get recommendation
Act on a recommendation	Dismiss Postpone Complete Reactivate
Retrieve details of all impacted resources for a recommendation.	List impactedResources
Retrieve details of an impacted resource for a recommendation.	Get impactedResource

Scenarios	API
Act on a recommendation for an impacted resource	Dismiss Postpone Complete Reactivate
Get the historical Secure Score data for your tenant.	Get tenantSecureScores

License requirements

The various recommendations have different license requirements. For more information about licenses for each type of recommendation, see [Microsoft Entra recommendations: Roles and licenses](#).

Related content

- [What is Microsoft Entra recommendations \(preview\)](#)

servicePrincipalSignInActivity resource type

Article • 07/31/2024

Namespace: microsoft.graph

ⓘ Important

APIs under the `/beta` version in Microsoft Graph are subject to change. Use of these APIs in production applications is not supported. To determine whether an API is available in v1.0, use the **Version** selector.

Represents the service principal sign-in activity usage in a given tenant. This resource contains information about the last usage time of a service principal.

For more information about this report, see [Usage and insights report: Service principal sign-in activity \(preview\)](#)

Methods

[] [Expand table](#)

Method	Return Type	Description
List	servicePrincipalSignInActivity collection	Get a list of servicePrincipalSignInActivity objects that contains sign-in activity information for service principals in a Microsoft Entra tenant.
Get	servicePrincipalSignInActivity	Get a servicePrincipalSignInActivity object that contains sign-in activity information for a service principal in a Microsoft Entra tenant.

Properties

[] [Expand table](#)

Property	Type	Description
appId	String	The globally unique appId (also called <i>client ID</i> on the Microsoft Entra admin center) of the credentialed resource application.

Property	Type	Description
applicationAuthenticationClientSignInActivity	signInActivity	The sign-in activity of the application in a app-only authentication flow (app-to-app tokens) where the application acts like a client.
applicationAuthenticationResourceSignInActivity	signInActivity	The sign-in activity of the application in a app-only authentication flow (app-to-app tokens) where the application acts like a resource.
delegatedClientSignInActivity	signInActivity	The sign-in activity of the application in a delegated flow (user sign-in) where the application acts like a client.
delegatedResourceSignInActivity	signInActivity	The sign-in activity of the application in a delegated flow (user sign-in) where the application acts like a resource.
id	String	The unique ID for each service principal sign-in event.
lastSignInActivity	signInActivity	The most recent sign-in activity of the application across delegated or app-only flows where the application is used either as a client or resource.

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

JSON
<pre>{ "@odata.type": "#microsoft.graph.servicePrincipalSignInActivity", "appId": "String", "applicationAuthenticationClientSignInActivity": {"@odata.type": "microsoft.graph.signInActivity"}, "applicationAuthenticationResourceSignInActivity": {"@odata.type": "microsoft.graph.signInActivity"}, "delegatedClientSignInActivity": {"@odata.type": "microsoft.graph.signInActivity"},</pre>

```
"delegatedResourceSignInActivity": {"@odata.type":  
"microsoft.graph.signInActivity"},  
"id": "String (identifier)",  
"lastSignInActivity": {"@odata.type": "microsoft.graph.signInActivity"}  
}
```

signIn resource type

Article • 08/29/2024

Namespace: microsoft.graph

Details user and application sign-in activity for a tenant (directory). You must have a Microsoft Entra ID P1 or P2 license to download sign-in logs by using the Microsoft Graph API.

The [Microsoft Entra data retention policies](#) govern the availability of sign-in logs.

Methods

[+] [Expand table](#)

Method	Return Type	Description
List	signIn	Read the properties and relationships of <code>signIn</code> objects.
Get	signIn	Read the properties and relationships of <code>signIn</code> object.

Properties

[+] [Expand table](#)

Property	Type	Description
appDisplayName	String	App name displayed in the Microsoft Entra admin center. Supports <code>\$filter</code> (<code>eq</code> , <code>startsWith</code>).
appId	String	Unique GUID that represents the app ID in the Microsoft Entra ID. Supports <code>\$filter</code> (<code>eq</code>).
appliedConditionalAccessPolicies	appliedConditionalAccessPolicy collection	Provides a list of conditional access policies that the corresponding sign-in activity triggers. Apps need more Conditional Access-related privileges to read the details of this property. For more information, see Permissions for viewing applied conditional access (CA) policies in sign-ins .
clientAppUsed	String	Identifies the client used for the sign-in activity. Modern authentication clients include <code>Browser</code> , <code>modern clients</code> . Legacy

Property	Type	Description
		authentication clients include Exchange ActiveSync, IMAP, MAPI, SMTP, POP, and other clients.
		Supports <code>\$filter</code> (eq).
conditionalAccessStatus	conditionalAccessStatus	Reports status of an activated conditional access policy. Possible values are: <code>success</code> , <code>failure</code> , <code>notApplied</code> , and <code>unknownFutureValue</code> .
		Supports <code>\$filter</code> (eq).
correlationId	String	The request ID sent from the client when the sign-in is initiated. Used to troubleshoot sign-in activity.
		Supports <code>\$filter</code> (eq).
createdDateTime	DateTimeOffset	Date and time (UTC) the sign-in was initiated. Example: midnight on Jan 1, 2014 is reported as <code>2014-01-01T00:00:00Z</code> .
		Supports <code>\$orderby</code> , <code>\$filter</code> (eq, le, and ge).
deviceDetail	deviceDetail	Device information from where the sign-in occurred; includes device ID, operating system, and browser.
		Supports <code>\$filter</code> (eq, <code>startsWith</code>) on <code>browser</code> and <code>operatingSystem</code> properties.
id	String	Unique ID representing the sign-in activity.
		Supports <code>\$filter</code> (eq).
ipAddress	String	IP address of the client used to sign in.
		Supports <code>\$filter</code> (eq, <code>startsWith</code>).
isInteractive	Boolean	Indicates whether a sign-in is interactive.
location	signInLocation	Provides the city, state, and country code where the sign-in originated.
		Supports <code>\$filter</code> (eq, <code>startsWith</code>) on <code>city</code> , <code>state</code> , and <code>countryOrRegion</code> properties.
resourceDisplayName	String	Name of the resource the user signed into.

Property	Type	Description
		Supports <code>\$filter</code> (eq).
resourceId	String	ID of the resource that the user signed into. Supports <code>\$filter</code> (eq).
riskDetail	riskDetail	The reason behind a specific state of a risky user, sign-in, or a risk event. The possible values are <code>none</code> , <code>adminGeneratedTemporaryPassword</code> , <code>userPerformedSecuredPasswordChange</code> , <code>userPerformedSecuredPasswordReset</code> , <code>adminConfirmedSigninSafe</code> , <code>aiConfirmedSigninSafe</code> , <code>userPassedMFADrivenByRiskBasedPolicy</code> , <code>adminDismissedAllRiskForUser</code> , <code>adminConfirmedSigninCompromised</code> , <code>hidden</code> , <code>adminConfirmedUserCompromised</code> , <code>unknownFutureValue</code> , <code>adminConfirmedServicePrincipalCompromised</code> , <code>adminDismissedAllRiskForServicePrincipal</code> , <code>m365DAdminDismissedDetection</code> , <code>userChangedPasswordOnPremises</code> , <code>adminDismissedRiskForSignIn</code> , <code>adminConfirmedAccountSafe</code> . Use the <code>Prefer: include-unknown-enum-members</code> request header to get the following value or values in this evolvable enum : <code>adminConfirmedServicePrincipalCompromised</code> , <code>adminDismissedAllRiskForServicePrincipal</code> , <code>m365DAdminDismissedDetection</code> , <code>userChangedPasswordOnPremises</code> , <code>adminDismissedRiskForSignIn</code> , <code>adminConfirmedAccountSafe</code> . The value <code>none</code> means that Microsoft Entra risk detection did not flag the user or the sign-in as a risky event so far.
riskEventTypes_v2	String collection	Supports <code>\$filter</code> (eq). Note: Details for this property are only available for Microsoft Entra ID P2 customers. All other customers are returned <code>hidden</code> .
		The list of risk event types associated with the sign-in. Possible values: <code>unlikelyTravel</code> , <code>anonymizedIPAddress</code> , <code>maliciousIPAddress</code> , <code>unfamiliarFeatures</code> , <code>malwareInfectedIPAddress</code> ,

Property	Type	Description
		<p><code>suspiciousIPAddress</code>, <code>leakedCredentials</code>, <code>investigationsThreatIntelligence</code>, <code>generic</code>, or <code>unknownFutureValue</code>.</p> <p>Supports <code>\$filter</code> (<code>eq</code>, <code>startsWith</code>).</p>
riskLevelAggregated	riskLevel	<p>Aggregated risk level. The possible values are: <code>none</code>, <code>low</code>, <code>medium</code>, <code>high</code>, <code>hidden</code>, and <code>unknownFutureValue</code>. The value <code>hidden</code> means the user or sign-in wasn't enabled for Microsoft Entra ID Protection.</p> <p>Supports <code>\$filter</code> (<code>eq</code>).</p> <p>Note: Details for this property are only available for Microsoft Entra ID P2 customers. All other customers are returned <code>hidden</code>.</p>
riskLevelDuringSignIn	riskLevel	<p>Risk level during sign-in. The possible values are: <code>none</code>, <code>low</code>, <code>medium</code>, <code>high</code>, <code>hidden</code>, and <code>unknownFutureValue</code>. The value <code>hidden</code> means the user or sign-in wasn't enabled for Microsoft Entra ID Protection.</p> <p>Supports <code>\$filter</code> (<code>eq</code>).</p> <p>Note: Details for this property are only available for Microsoft Entra ID P2 customers. All other customers are returned <code>hidden</code>.</p>
riskState	riskState	<p>Reports status of the risky user, sign-in, or a risk event. The possible values are: <code>none</code>, <code>confirmedSafe</code>, <code>remediated</code>, <code>dismissed</code>, <code>atRisk</code>, <code>confirmedCompromised</code>, <code>unknownFutureValue</code>.</p> <p>Supports <code>\$filter</code> (<code>eq</code>).</p>
status	<code>signInStatus</code>	<p>Sign-in status. Includes the error code and description of the error (if a sign-in failure occurs).</p> <p>Supports <code>\$filter</code> (<code>eq</code>) on <code>errorCode</code> property.</p>
userDisplayName	String	<p>Display name of the user that initiated the sign-in.</p> <p>Supports <code>\$filter</code> (<code>eq</code>, <code>startsWith</code>).</p>

Property	Type	Description
userId	String	ID of the user that initiated the sign-in. Supports <code>\$filter (eq)</code> .
userPrincipalName	String	User principal name of the user that initiated the sign-in. This value is always in lowercase. For guest users whose values in the user object typically contain #EXT# before the domain part, this property stores the value in both lowercase and the "true" format. For example, while the user object stores <code>AdeleVance_fabrikam.com#EXT#@contoso.com</code> , the sign-in logs store <code>adelevance@fabrikam.com</code> . Supports <code>\$filter (eq, startsWith)</code> .

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

```
JSON
{
  "id": "String (identifier)",
  "createdDateTime": "String (timestamp)",
  "appDisplayName": "String",
  "appId": "String",
  "ipAddress": "String",
  "clientAppUsed": "String",
  "correlationId": "String",
  "conditionalAccessStatus": "string",
  "appliedConditionalAccessPolicies": [{"@odata.type": "microsoft.graph.appliedConditionalAccessPolicy"}],
  "isInteractive": true,
  "deviceDetail": {"@odata.type": "microsoft.graph.deviceDetail"},
  "location": {"@odata.type": "microsoft.graph.signInLocation"},
  "riskDetail": "string",
  "riskLevelAggregated": "string",
  "riskLevelDuringSignIn": "string",
  "riskState": "string",
  "riskEventTypes": ["string"],
  "riskEventTypes_v2": ["String"],
  "resourceDisplayName": "string",
```

```
"resourceId": "string",
"status": {"@odata.type": "microsoft.graph.signInStatus"},
"userDisplayName": "string",
"userId": "string",
"userPrincipalName": "string"
}
```