Microsoft Fabric documentation for admins

Learn about the Microsoft Fabric admin settings, options, and tools.

Fabric in your organization

OVERVIEW

What is Microsoft Fabric admin?

What is the admin portal?

GET STARTED

Enable Fabric for your organization

Region availability

Find your Fabric home region

HOW-TO GUIDE

Understand Fabric admin roles

REFERENCE

Governance documentation

Security documentation

Tools and settings

OVERVIEW

About tenant settings

HOW-TO GUIDE

Set up git integration

Set up item certification

Configure notifications

Set up metadata scanning

Enable content certification

Enable service principal authentication

Configure Multi-Geo support

Monitoring and management

OVERVIEW

What is the admin monitoring workspace?

CONCEPT

Feature usage and adoption report

HOW-TO GUIDE

Use the Monitoring hub

Workspace administration

CONCEPT

Manage workspaces

HOW-TO GUIDE

Workspace tenant settings

Administration overview

08/04/2024

Microsoft Fabric is a software as a service (SaaS) platform that lets users get, create, share, and visualize data. Fabric unified administration enables you to secure and govern data across the platform, and manage Fabric features. Controlling feature access and capabilities allow you to comply with company policies and external rules and regulations. Fabric also allows admins to delegate their responsibilities. Delegation lets you create different groups of admins for different tasks in your organization. Delegating admin responsibilities can reduce pressure that might cause one admin team to become a bottleneck for organizational processes.

This article uses the generic term "admin." For details about which types of admins can perform the tasks described here, visit these articles:

- Admin roles in Fabric.
- Microsoft Entra built-in roles
- Microsoft 365 admin roles

Manage

As an admin, you can manage many platform aspects for your organization. This section discusses the ability to manage some of Fabric's components, and the impact this has on your organization.

Grant and manage licenses

To access the Fabric SaaS platform, you need a license. Fabric has two type of licenses:

- Capacity license - An organizational license that provides a pool of resources for Fabric operations. Capacity licenses are divided into stock keeping units (SKUs). Each SKU provides a different number of capacity units (CUs) which are used to calculate the capacity's compute power.

- Per user license - Per user licenses allow users to work in Fabric.

To purchase licenses, you must be a Billing administrator. Billing administrators can buy licenses and control them with tools such as capacity pause and resume and scale.

After you purchase licenses, use the Microsoft 365 admin center, PowerShell, or the Azure portal to view and manage those licenses.

Turn off self-service

Self-service allows individuals to sign up, try, or purchase Fabric or Power BI on their own. You might not want users in your organization to use one or more forms of self-service. Perhaps all licensing is centralized and managed by an admin team or perhaps your organization doesn't permit trials. To learn how to turn off self-service, visit Enable or disable self-service.

Turning off self-service sign-up keeps users from exploring Fabric on their own. If you block individual sign-up, you might want to get Fabric (free) licenses for your organization and assign them to all users.

Take over a subscription

As an admin, you can't assign or unassign licenses for a self-service purchase subscription bought by a user in your organization. You can take over a purchase or trial subscription, and then assign or unassign licenses.

View your subscriptions

To see which subscriptions your organization has, follow these steps.

1. Sign in to the Microsoft 365 admin center.
2. In the navigation menu, select **Billing** > **Your products**.

Your active Fabric and Power BI subscriptions are listed along with any other subscriptions you have.

Assign admin roles

Admins can assign and manage Fabric admin roles. Admin roles allow users to buy licenses, and control organizational settings. For example, admins with certain roles can access the admin center and manage their organization's tenant settings.

Customize a Fabric tenant

Fabric is composed of tenants, capacities, and workspaces. Your organization might have one or more tenants, each with at least one capacity. Workspaces reside in capacities, and are where data is created, transformed, and consumed. Each organization can organize its tenants, capacities, and workspaces in accordance with their organizational structure. For example, in an organization with one tenant, capacities can be organized according to the organizational functions, and workspaces can be created according to each function's divisions.

Admins can control these processes throughout the organization. For example, being an admin allows you to create and delete workspaces, and to control workspace settings such as Azure connections, Git integration and OneLake.

To distribute management across the organization, you can also use domains. With a domain, you create a logical grouping of workspaces. For example, your organization can create domains according to functions such as sales and marketing. Designated users can become admins and oversee Fabric functions related to the data in each domain. Using domains allows your organization to appoint the right admins at the right level. You no longer need Fabric administrators with lots of permissions and responsibilities to manage every single area in your organization. Using domains, you can allocate some admin rights to users who are closer to the domain's subject matter. By doing that, you free Fabric administrators to concentrate on organizational processes, and allow experts to directly manage data in their fields.

Add and remove users

Admins can manage Fabric users by using the Microsoft 365 admin center. Managing users includes adding and deleting users, groups, and admins. You can also manage per user licenses and assign admin roles.

Govern and secure data

Fabric provides a set of tools that allow admins to manage and govern data across the organization. For example, you can use the information protection capabilities to protect sensitive information in your organization.

With a set of governance and security tools, you can make sure that your organization's data is secure, and that it complies to your organizational policies.

Data residency is also supported in Fabric. As an admin, by deciding where your tenants and capacities are created, you can specify your organization's data storage location.

You can also control your organization's disaster recovery capacity setting to make sure your data is safe if a disaster happens.

Control

Admins have control over Fabric settings and permissions across the platform. You can also delegate admin settings to other admins in your organization, to allow granular control across your organization.

Delegate admin rights

To avoid becoming a bottleneck for every single setting in your organization, you can delegate many of the controls to Capacity, Workspace, and Domain administrators. Delegating settings allows your organization to have several admins with different levels of admin rights in multiple logical locations within your organization. For example, you can have three admins with access to all the settings in your organization, and another admin for each team in your organization. The team admin can control settings and permissions relevant for the team, at the capacity, workspace, or domain level, depending on the way your organization is set up. You can also have multiple levels of admins in your organization, depending on your organization's needs.

Enable Fabric settings

Admins can enable and disable global platform settings by controlling the Tenant settings. If your organization has one tenant, you can enable and disable settings for the entire organization from that tenant. Organizations with multiple tenants require an admin for each tenant. If your organization has several tenants, it can opt for a centralized approach by appointing one admin (or a team of admins) to control the settings for all the organization's tenants.

Capacity and workspace settings allow you to be more specific when you control your Fabric platform, because they apply to a specific capacity or workspace. Most Fabric experiences and features, have their own settings, allowing control at an experience or feature level. For example, workspace administrators can customize Spark compute configuration settings.

Grant permissions

In Fabric, workspace roles allow workspace admins to manage who can access data. Some of the things workspace roles determine, are which users can view, create, share, and delete Fabric items. As an admin, you can grant and revoke workspace roles, using them to control access to data in your organization. You can also create security groups and use them to control workspace access.

Monitor

An important part of an admin's role is to monitor what's going on in the organization. Fabric has several tools for monitoring different aspects of the platform usage. Monitoring enables your organization to comply with internal policies and external rules and regulations. You can also use monitoring to review consumption and billing, so that you can establish the best way to use your organizational resources. By analyzing what's happening in your organization, you

can decide if you need to buy more resources, and potentially save money by using cheaper or fewer resources if that can be done.

Admin monitoring workspace

To view the usage of Fabric features in your organization, use the feature usage and adoption report in the admin monitoring workspace. The report allows you to gain insights into consumption across the organization. You can also use its semantic model to create a tailored report specific for your organization.

Monitoring hub

The monitoring hub lets you review Fabric activities per experience. Using the hub, you can spot failed activities and see who submitted the activity and how long it lasted. The hub can expose many other details regarding each activity, and you can also filter and search it as needed.

View audit logs

Audit logs allow you to track user activities in Fabric. You can search the logs and see which operations were performed in your organization. Reviewing the logs can have many uses in your organization, such as making sure policies are followed and debugging unexpected system behavior.

Understand consumption

Consumption in Fabric is measured using capacity units (CUs). Using the Capacity Metrics app admins can view consumption in their organization. This report enables you to make informed decisions regarding the use of your organizational resources. You can then take action by scaling a capacity up or down, pausing a capacity operation, optimizing query efficiency, or buying another capacity if needed. Understanding consumption makes your organization's Fabric operations run smoother, and might save your organization money.

Reviewing bills

Admins can view their organization's bills to understand what their organization is paying for. You can compare your bill with your consumption to understand if and where your organization can make savings.

Capabilities

This section provides a high level list of some of the admin capabilities mentioned in this article.

Expand table

Capability	Description
Capacity Metrics app	Monitor your organization's consumption
Feature usage and adoption report	Review the usage of Fabric features
Tenant settings	Control Fabric settings across your organization
Track user activities in Microsoft Fabric	Use log entries to view Fabric operations
workspace roles	Set up permissions for Fabric workspaces

Related content

- Admin roles
- Security overview
- Governance and compliance overview

What is Microsoft Fabric admin?

07/01/2024

Microsoft Fabric admin is the management of the organization-wide settings that control how Microsoft Fabric works. Users that are assigned to admin roles configure, monitor, and provision organizational resources. This article provides an overview of admin roles, tasks, and tools to help you get started.

Admin roles related to Microsoft Fabric

There are several roles that work together to administer Microsoft Fabric for your organization. Most admin roles are assigned in the Microsoft 365 admin portal or by using PowerShell. The capacity admin roles are assigned when the capacity is created. To learn more about each of the admin roles, see About admin roles. To learn how to assign admin roles, see Assign admin roles.

Microsoft 365 admin roles

This section lists the Microsoft 365 admin roles and the tasks they can perform.

- **Global administrator**
  - Unlimited access to all management features for the organization
  - Assign roles to other users
- **Billing administrator**
  - Manage subscriptions
  - Purchase licenses
- **License administrator**
  - Assign or remove licenses for users
- **User administrator**
  - Create and manage users and groups
  - Reset user passwords

Power Platform and Fabric admin roles

As a Power Platform or a Fabric admin, you have full access to all the Microsoft Fabric management tasks.

- **Power Platform administrator** or **Fabric administrator**

- Enable and disable Microsoft Fabric features
- Report on usage and performance
- Review and manage auditing

Capacity admin roles

As a capacity admin, you can perform these tasks on the capacity you're an admin of.

- **Capacity administrator**
  - Assign workspaces to the capacity
  - Manage user permission to the capacity
  - Manage workloads to configure memory usage

Admin tasks and tools

Microsoft Fabric admins work mostly in the Microsoft Fabric admin portal, but you should still be familiar with related admin tools. To find out which role is required to perform the tasks listed here, cross reference them with the admin roles listed in Admin roles related to Microsoft Fabric.

- **Microsoft Fabric admin portal**
  - Acquire and work with capacities
  - Ensure quality of service
  - Manage workspaces
  - Publish visuals
  - Verify codes used to embed Microsoft Fabric in other applications
  - Troubleshoot data access and other issues

- **Microsoft 365 admin portal**
  - Manage users and groups
  - Purchase and assign licenses
  - Block users from accessing Microsoft Fabric

- **Microsoft 365 Security & Microsoft Purview compliance portal**
  - Review and manage auditing
  - Data classification and tracking
  - Data loss prevention policies
  - Microsoft Purview Data Lifecycle Management

- **Microsoft Entra ID in the Azure portal**
  - Configure conditional access to Microsoft Fabric resources

- **PowerShell cmdlets**
  - Manage workspaces and other aspects of Microsoft Fabric using scripts
- **Administrative APIs and SDK**
  - Build custom admin tools.

Related content

- What is the admin portal?
- What is the admin monitoring workspace?
- Understand Microsoft Fabric admin roles

What is the admin portal?

The Microsoft Fabric admin portal includes settings that govern Microsoft Fabric. For example, you can make changes to tenant settings, access the Microsoft 365 admin portal, and control how users interact with Microsoft Fabric.

To access the admin portal, you need a Fabric license and the *Fabric administrator* role.

If you're not in one of these roles, you only see *Capacity settings* in the admin portal.

What can I do in the admin portal

The many controls in the admin portal are listed in the following table, with links to relevant documentation for each one.

Expand table

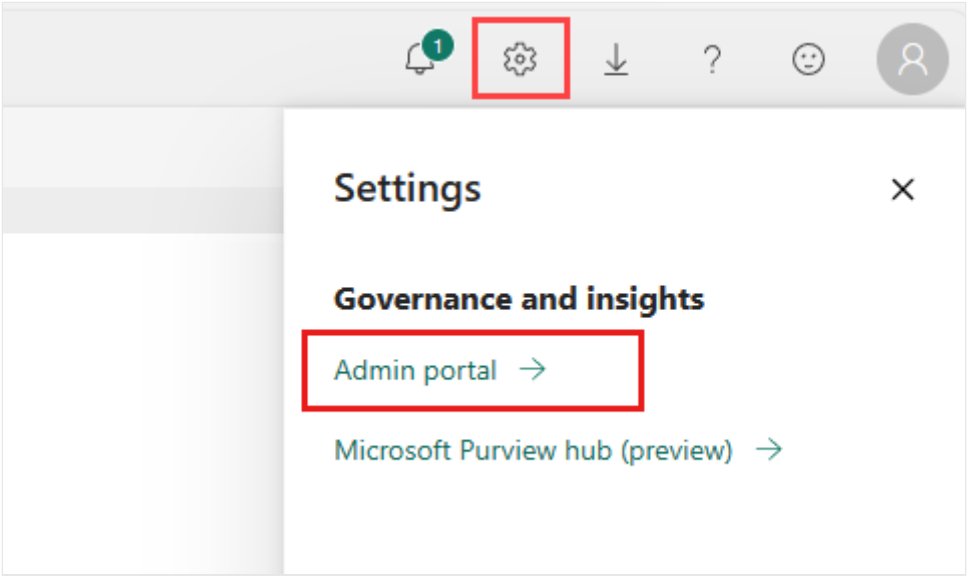
Feature	Description
Tenant settings	Enable, disable, and configure Microsoft Fabric.
Users	Manage users in the Microsoft 365 admin portal.
Premium Per User	Configure auto refresh and semantic model workload settings.
Audit logs	Audit Microsoft Fabric activities in the Microsoft Purview portal.
Domains	Manage and organize business data using custom domains in Fabric.
Workloads	Manage workloads and their settings.
Tags	Manage tags for organizing content.
Capacity settings	Manage Microsoft Fabric F, Power BI Premium P, and Power BI Embedded EM and A capacities.
Refresh summary	Schedule refresh on a capacity and view the details of refreshes that occurred.
Embed codes	View and manage the embed codes that have been generated for your organization to share reports publicly.
Organizational visuals	View, add, and manage which type of Power BI visuals users can access across the organization.
Organizational themes (preview)	Manage and distribute custom report themes across the organization.
Azure connections	Configure and manage connections to Azure resources.

Feature	Description
Workspaces	View and manage the workspaces that exist in your organization.
Custom branding	Change the look and feel of the Microsoft Fabric to match your organization's own branding.
Fabric identities	Govern the Fabric identities that exist in your organization.
Featured content	Manage the reports, dashboards, and apps that were promoted to the Featured section on your Home page.

How to get to the admin portal

To get to the admin portal, follow these steps:

1. Sign in to Microsoft Fabric using your admin account credentials.
2. Select the **Settings** (gear) icon, and then select **Admin portal**.



Related content

- What is the admin monitoring workspace?
- Workspace tenant settings
- Manage workspaces

Last updated on 10/30/2025

Microsoft Fabric governance documentation

Govern, manage, and protect all your data in Fabric.

Secure, protect and comply

OVERVIEW

Governance and compliance in Fabric

Security overview

HOW-TO GUIDE

Manage access

Audit

DEPLOY

Information protection

Data loss prevention in Power BI

REFERENCE

Security documentation

Admin documentation

Manage your data estate

REFERENCE

Tenant settings and control

CONCEPT

Optimize business on domains

HOW-TO GUIDE

Workspace management

Govern capacity resources

Tenant multicloud abilities

Encourage data discovery, trust, and use

HOW-TO GUIDE

Discover

Track lineage

Analyze impact

OVERVIEW

Endorse and trust

Curate

Monitor, uncover insights and act

CONCEPT

Monitor

Data insights for admins

Data insights for creators

OVERVIEW

Automate

Microsoft Fabric security

Microsoft Fabric is a software as a service (SaaS) platform that offers a complete security package. Fabric removes the cost and responsibility of maintaining your security solution and transfers it to the cloud. With Fabric, you can use the expertise and resources of Microsoft to keep your data secure, patch vulnerabilities, monitor threats, and comply with regulations.

Fabric security fundamentals

OVERVIEW

Security in Microsoft Fabric

Microsoft Fabric security fundamentals

CONCEPT

Fabric and OneLake security

HOW-TO GUIDE

Configure Multi-Geo support for Fabric

Inbound network security

OVERVIEW

Microsoft Entra ID

Zero Trust

Conditional Access

HOW-TO GUIDE

Conditional access in Fabric

Outbound network security

CONCEPT

On-premises data gateway with Dataflow Gen 2

Integration runtime in Azure Data Factory

Integration runtime in Azure Data Factory

Azure Data Factory managed virtual network

Lakehouse SQL analytics endpoints

Direct lake

REFERENCE

Azure service tags

Service tags on-premises

Governance and compliance

GET STARTED

Governance and compliance documentation

OVERVIEW

Governance and compliance in Microsoft Fabric

CONCEPT

Microsoft Purview

Microsoft Purview hub

Enable Microsoft Fabric for your organization

10/17/2025

The Microsoft Fabric admin switch lets organizations that use Power BI enable Microsoft Fabric.

> **Note**
>
> - Power BI is part of Microsoft Fabric. The Power BI portal mentioned in this article is now the Microsoft Fabric portal.
> - Microsoft Fabric availability is restricted in some regions. For more information, see Fabric region availability.

You can enable Microsoft Fabric for:

- **Your tenant** - Use this option to enable Microsoft Fabric for everyone in the tenant.
- **A specific capacity** - Use this option if you want to enable Microsoft Fabric for users in a specific capacity.

In both cases, you can use security groups to provide Microsoft Fabric access to a specified list of users.

Prerequisites

To enable Microsoft Fabric, you need to have the *Fabric administrator* role.

Enable for your tenant

When you enable Microsoft Fabric using the tenant setting, users can create Fabric items in that tenant, unless capacity admins turned it off for a specific capacity. Depending on the configuration you select, Microsoft Fabric becomes available for everyone in the tenant, or to a selected group of users.

> **Note**
>
> - You, or other admins, can override the Microsoft Fabric setting at the capacity level.
> - The Microsoft Fabric trial capacity gives you free access for 60 days to explore most features across data engineering, data science, real-time analytics, business

intelligence, and more.

In your tenant, you can enable Microsoft Fabric for:

- **The entire organization** - In most cases your organization has one tenant, so selecting this option enables it for the entire organization. In organizations that have several tenants, if you want to enable Microsoft Fabric for the entire organization, you need to enable it in each tenant.
- **Specific security groups** - Use this option to enable Microsoft Fabric for specific users. You can either specify the security groups that Microsoft Fabric will be enabled for, or the security groups that Microsoft Fabric won't be available for.

Follow these steps to enable Microsoft Fabric for your tenant.

1. In the Power BI portal, navigate to the tenant settings in the admin portal and in *Microsoft Fabric*, expand **Users can create Fabric items**.
2. Enable the **Users can create Fabric items** switch.
3. (Optional) Use the **Specific security groups** option to enable Microsoft Fabric for specific users. You can also use the **Except specific security groups** option, to exclude specific users.
4. Select **Apply**.

> **Note**
>
> The *Delegate settings to other admins* option, isn't available because it's automatically delegated to capacity admins.

Enable for a capacity

Consider the Microsoft Fabric setting at the tenant level a recommendation for the entire organization. Capacity admins can override this setting, depending on their needs. For example, Fabric can be enabled for all the users in your organization. However, for security reasons your organization decided to disable Fabric for a specific capacity. In such cases, Microsoft Fabric can be disabled for that capacity.

Follow these steps to enable Microsoft Fabric for a specific capacity.

1. Navigate to the capacity settings in the admin portal.

2. Select the capacity you want to enable Microsoft Fabric for.
3. Select the **Delegate tenant settings** tab, and under **Microsoft Fabric**, expand the **Users can create Fabric items** setting.
4. Check the **Override tenant admin selection** checkbox and verify that the **Users can create Fabric items** setting is enabled.
5. (Optional) Use the **Specific security groups** option to enable Microsoft Fabric for specific users. You can also use the **Except specific security groups** option, to enable Microsoft Fabric for the capacity, and exclude specific users.
6. Select **Apply**.

Can I disable Microsoft Fabric?

To disable Microsoft Fabric, you can turn off the *Microsoft Fabric* admin switch. After disabling Microsoft Fabric, users will have view permissions for Microsoft Fabric items. If you disable Microsoft Fabric for a specific capacity while Microsoft Fabric is available in your organization, your selection will only affect that capacity.

Considerations

In some cases, users that don't have Microsoft Fabric enabled will be able to view Microsoft Fabric items and icons.

Users that don't have Microsoft Fabric enabled, can:

- View Microsoft Fabric items created by other users in the same workspace, as long as they have at least read-only access to that workspace.
- View Microsoft Fabric icons in capacities where other users have Microsoft Fabric enabled, as long as they have at least read-only access to that capacity.

Related content

- Admin overview

Fabric region availability

This article lists the region availability of the Microsoft Fabric F SKUs, which are available in the Azure public cloud regions. Some of the Fabric workloads might not be immediately available in new regions, or regions where data centers become constrained.

For details about purchasing a Fabric subscription, see Buy a Microsoft Fabric subscription.

Home region

Your home region is associated with your tenant. If your home region doesn't reside in the following regions, you won't be able to access all the Fabric functionalities. In such cases, to access all the Fabric features, you can create a capacity in a region where Fabric is available. For more information, see Multi-Geo support for Fabric.

Workload and feature availability

The following tables list the availability of Fabric workloads according to the region of your tenant.

All workloads

This table lists regions where all Fabric workloads are available.

Expand table

Americas	Europe	Middle East	Africa	Asia Pacific
Brazil South	North Europe [4]	UAE North	South Africa North	Australia East
Canada Central	West Europe			Australia Southeast
Canada East [3]	France Central			Central India
Central US	Germany West Central			East Asia
East US [5]	Italy North			Indonesia Central [6]
East US 2	Norway East			Israel Central [4, 6]
Mexico Central [6]	Poland Central			Japan East

Americas	Europe	Middle East	Africa	Asia Pacific
North Central US	Spain Central [6]			Japan West [4, 6]
South Central US [2, 4, 5, 6]	Sweden Central			Korea Central
West US	Switzerland North			New Zealand North [6]
West US 2	Switzerland West			Southeast Asia
West US 3	UK South			South India
	UK West [1]			

[1] Fabric SQL database isn't available in this region. [2] Healthcare Solutions isn't available in this region. [3] Fabric User Data Functions isn't available in these regions. [4] Digital twin builder (preview) isn't available in these regions. [5] Operations agent (preview) isn't available in these regions. [6] Ontology (preview) isn't available in these regions.

Power BI

This table lists regions where the only available Fabric workload is Power BI.

Expand table

Americas	Europe	Middle East	Africa	Asia Pacific
Chile Central	Austria East	Qatar Central	South Africa West	India West
	France South	UAE Central		Korea South
	Germany North			Taiwan North
	Norway West			Taiwan Northwest
				Malaysia West

** Copilot is not supported for regions listed in this section.

Public preview

This table lists regions where public preview features are available, according to workload.

Expand table

Region	Copilot**	Retail Solutions	Dataflow Gen2 with CI/CD
Australia East	• Dataflows • Synapse Notebook	✅	✅
Australia Southeast	• Dataflows • Exploration • Synapse Notebook	✅	✅
Brazil South	• Dataflows • Exploration • Synapse Notebook	✅	✅
Canada Central	• Dataflows • Synapse Notebook	✅	✅
Canada East	Synapse Notebook	❌	✅
Central India	• Dataflows • Synapse Notebook	✅	✅
Central US	❌	❌	✅
East Asia	Synapse Notebook	✅	✅
East US	• Dataflows • Exploration • Synapse Notebook	✅	✅
East US2	• Dataflows • Exploration • Synapse Notebook	✅	✅
France Central	• Dataflows • Exploration • Synapse Notebook	❌	✅
Germany West Central	• Dataflows • Synapse Notebook	❌	✅
Italy North	❌	❌	✅
Japan East	• Dataflows • Exploration • Synapse Notebook	✅	✅
Korea Central	• Dataflows • Synapse Notebook	❌	✅
North Central US	• Dataflows	✅	✅

Region	Copilot**	Retail Solutions	Dataflow Gen2 with CI/CD
	• Exploration • Synapse Notebook		
North Europe	• Dataflows • Exploration • Synapse Notebook	✅	✅
Norway East	❌	❌	✅
Poland Central	❌	❌	✅
South Africa North	Synapse Notebook	✅	✅
South Africa West	❌	❌	✅
South Central US	• Dataflows • Exploration • Synapse Notebook	✅	❌
Southeast Asia	• Dataflows • Synapse Notebook	✅	✅
South India	• Dataflows • Exploration	❌	✅
Sweden Central	Synapse Notebook	❌	✅
Switzerland North	Synapse Notebook	❌	✅
Switzerland West	❌	❌	✅
UAE North	• Dataflows • Exploration • Synapse Notebook		✅
West Europe	• Dataflows • Exploration • Synapse Notebook	✅	✅
West US	• Dataflows • Exploration • Synapse Notebook	✅	✅
West US2	• Dataflows • Exploration • Synapse Notebook	✅	✅
West US3	• Dataflows • Synapse Notebook	✅	✅

** Only the workloads listed in the table are available in each region. If no workloads are listed, Copilot isn't available in that region.

Related content

- Buy a Microsoft Fabric subscription
- Find your Fabric home region

Last updated on 12/01/2025

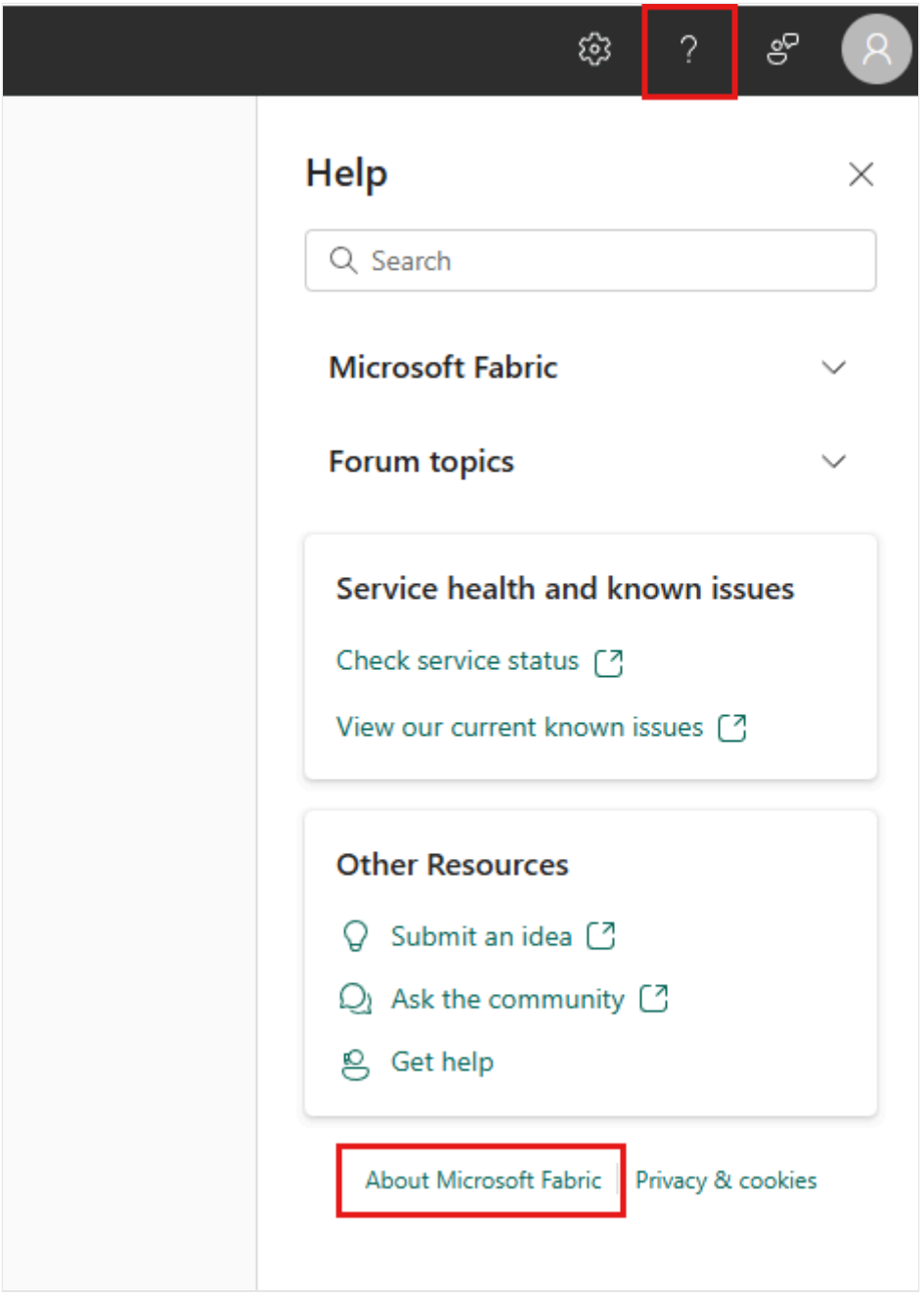
Find your Fabric home region

08/04/2025

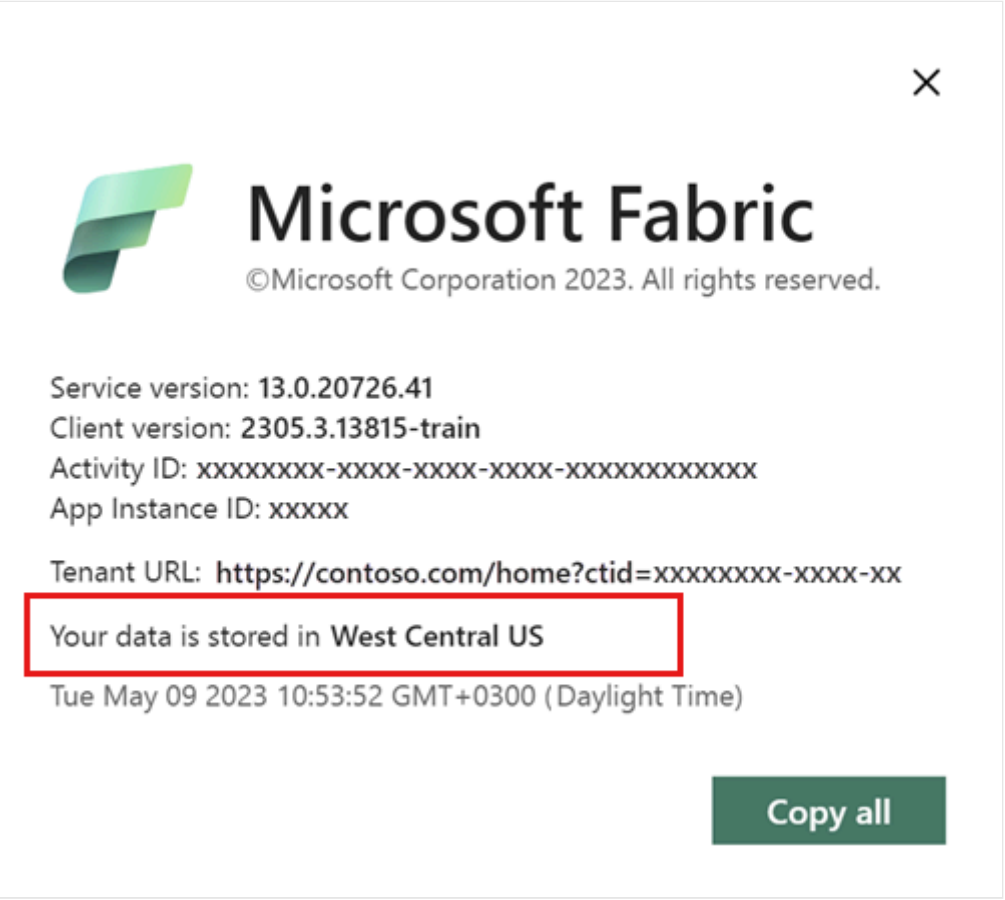
A Fabric home region is the Azure datacenter region linked to your Fabric tenant, chosen when your tenant was created. Knowing your home region is important for understanding workload and feature availability, as well as data residency, performance, and compliance.

To find your Fabric home region, follow these steps:

1. Sign in to Fabric.
2. Open the Help pane and choose the **About** link (the text of the link varies depending on which workload is selected).



3. Look for the value next to **Your data is stored in**. The location shown is the default region where your data is stored. You might also be using capacities in different regions for your workspaces.



Related content

- Buy a Microsoft Fabric subscription
- Region availability
- Azure public cloud geographies and regions

Manage your Fabric capacity

09/02/2025

This article describes the Microsoft Fabric capacity settings. The article is aimed at admins who want to understand how to manage their Microsoft Fabric capacities.

Get to the capacity settings

To get to the capacity settings, follow these steps:

1. In Microsoft Fabric, select the gear icon (⚙), and then select **Admin portal**.
2. In the Admin portal, select **Capacity settings**.

View your capacity

The capacity settings page shows a list of all the capacities in your tenant. At the top of the page you can see a list of the different Fabric capacity types. Select a capacity type to view all the capacities of that type in your tenant.

- **Power BI Premium** - A capacity that was bought as part of a Power BI Premium subscription. These capacities use P SKUs.

  > ⓘ **Note**
  >
  > Power BI capacities are transitioning to Fabric. For more information, see Power BI Premium transition to Microsoft Fabric.

- **Power BI Embedded** - A capacity that was bought as part of a Power BI Embedded subscription. These capacities use A or EM SKUs.
- **Trial** - A Microsoft Fabric trial capacity. These capacities use Trial SKUs.
- **Fabric capacity** - A Microsoft Fabric capacity. These capacities use F SKUs.

The rest of this article is divided to sections based on the different capacity types. To view the settings of your capacity, select the tab that matches your capacity type. If there's no tab to select, the section applies to all capacity types.

Manage your capacity

This section lists basic capacity management tasks, such as creating a new capacity, changing a capacity's name and deleting a capacity.

Create a new capacity

To create a new capacity you need to be a Microsoft Fabric admin.

Power BI Premium

To create a new Power BI Premium capacity, follow these steps:

1. On the **Capacity settings** page, select **Power BI Premium**.
2. Select **Set up new capacity**.
3. On the **Set up a new capacity** page, enter the following information:
    - **Capacity name** - Give your capacity a name.
    - **Capacity admins** - Add capacity admins.
    - **Region** - Select the region you want to create the capacity in.
    - **Available v-cores** - Select the number of v-cores you want to use for the capacity.
    - **Capacity size** - Select the size of the capacity.

      > ⓘ **Note**
      >
      > If you select an EM size, you'll create a Power BI Embedded capacity.
4. Select **Create**.

Change the name of your capacity

To change the name of your capacity, you need to be a capacity admin. To become a capacity admin, you need to be assigned the capacity admin role in the capacity settings. For more information, see Add and remove admins.

Power BI Premium

To change the name of your Power BI Premium capacity, follow these steps:

1. On the **Capacity settings** page, select **Power BI Premium**.
2. From the list of capacities, select the gear icon (⚙) next to the capacity you want to change.
3. Select the pencil icon next to the **Capacity name** field.
4. Enter the new name for the capacity, and then select the checkmark icon (✓).

Add and remove admins

To add and remove admins from your capacity, you need to be a capacity admin. Only users that belong to the tenant the capacity is part of, can be added as admins to the capacity.

Power BI Premium

To add or remove admins in a Power BI Premium capacity, follow these steps:

1. On the **Capacity settings** page, select **Power BI Premium**.
2. From the list of capacities, select the capacity you want to make changes to.
3. From the *Details* tab, select expand **Admin permissions**.
4. Add or remove admins from the text box.
5. Select **Apply**.

Resize a capacity

To resize your capacity, you need to be a capacity admin. To become a capacity admin, you need to be assigned the capacity admin role in the capacity settings. For more information, see Add and remove admins.

Power BI Premium

To resize a Power BI Premium capacity, follow these steps:

1. On the **Capacity settings** page, select **Power BI Premium**.
2. Select the capacity you want to resize.
3. Select **Change size**.
4. In the *Change size* window, from the **Capacity size** dropdown, select the new size for the capacity.

5. Select **Apply**.

Delete a capacity

To delete a capacity you need to be a Microsoft Fabric admin.

When you delete a Power BI Premium, Trial or Fabric Capacity, non-Power BI Fabric items in workspaces assigned to the capacity are soft deleted. These Fabric items can still be seen in OneLake Data Hub and in the workspace list, but can't be opened or used. If the workspace that holds these items is associated to a capacity (other than Power BI Embedded) from the same region as the deleted capacity within seven days, the deleted items are restored. This seven-day period is separate from the workspace retention policy.

Power BI Premium

To delete a Power BI Premium capacity, follow these steps:

1. On the **Capacity settings** page, select **Power BI Premium**.
2. From the list of *Power BI Premium* capacities, select the gear icon (⚙) next to the capacity you want to delete.
3. Select **Delete capacity**.
4. From the confirmation dialog, select **Delete**.

Autoscale

Power BI Premium

To enable autoscale on a Power BI Premium capacity, see Using Autoscale with Power BI Premium.

Capacity settings

After selecting a capacity, you can control its settings from these two tabs:

- **Details** - Capacity details are settings that are specific to the capacity.
- **Delegated tenant settings** - Tenant settings are delegated by Fabric admins to be managed by capacity admins. Changes to these settings only affect the capacity the

changes are made in.

> **Note**
>
> Delegated tenant settings are available for Power BI Premium and Fabric capacities.

To view the settings of a specific capacity, follow these steps:

1. Go to the **Capacity settings** page.
2. Select the capacity type your capacity belongs to.
3. From the list, select the capacity you want to view.

Details

This table summarizes the actions you can take in the details section.

> **Note**
>
> - Some of the features in the table are only available if they are enabled in the tenant.
> - Trail capacities only have some of the settings listed in the table

Expand table

Details setting name	Description
Disaster Recovery	Enable disaster recovery for the capacity
Capacity usage report	The usage report is replaced with the capacity metrics app
Notifications	Enable notification for your capacity
Copilot capacity	Designate this capacity as a Fabric Copilot capacity
Contributor permissions	Set up the ability to add workspaces to the capacity. Select one of these two options: • The entire organization • Specific users or security groups
Admin permissions	Give specific users the ability to do the following: • Change capacity settings • Add contributors to the capacity • Add or remove workspaces from the capacity
Power BI workloads	Configure Power BI workloads for: • Semantic models

Details setting name	Description
	• Paginated reports • AI
Preferred capacity for My workspace	Designate the capacity as the default capacity for My workspaces
Data Engineering/Science Settings	Allow workspace admins to set the size of their spark pools
Workspaces assigned to this capacity	*Add or remove workspaces assigned to the capacity

* To assign a workspace to a Fabric capacity or a capacity with an A SKU, you need to have a capacity **contributor** role, and a workspace admin role. A **contributor** on a capacity can assign workspaces to that capacity but can't modify capacity settings or delete the capacity. This role is typically used to allow workspace admins to move their workspaces into a managed capacity without giving them full administrative control.

Delegated tenant settings

Delegating admin settings can be used to grant granular access to features in the capacity. The delegated tenant settings section lists these tenant settings:

- Workload management tenant settings that are automatically delegated to the capacity.
- Tenant settings delegated by the Fabric Admin.

By default, delegated tenant settings inherit their configuration from the tenant. To override this configuration, follow the steps below. When the tenant setting delegation is enabled, you can disable delegation by clearing the *Override tenant admin selection* checkbox.

1. From the **Delegate tenant setting** list, open the setting you want to delegate permissions for.

2. Select the **Override tenant admin selection** checkbox.

3. Select **Enabled**

4. In the *Apply to* section, select one of the following options:

    - **All the users in capacity** - Delegate the setting to all the users in the capacity.
    - **Specific security groups** - Apply the setting to specific security groups. Enter the security groups you want to apply the setting to.

To exclude specific security groups from the setting, select **Except specific security groups** and enter the security groups you want to exclude. This setting is optional and can be used with together with the *Apply to* setting.

5. Select **Apply**.

Manage max memory for semantic models

To optimize performance and prevent memory-related errors, administrators can adjust the **Max memory (%)** setting for semantic models within the Power BI Premium and Power BI Embedded capacity settings.

1. Go to the **Admin portal**.
2. Select **Capacity settings**.
3. Choose the relevant capacity and click on the **Workloads** tab.
4. Locate the **Semantic models** section.
5. Adjust the **Max memory (%)** slider to allocate more memory as needed.

> [NOTE] Increasing memory allocation may help resolve issues such as model loading failures or performance bottlenecks. For more context on SKU limitations, see Semantic model SKU limitation.

Related content

- Microsoft Fabric licenses
- About tenant settings

ⓘ **Note:** The author created this article with assistance from AI. Learn more

Understand Microsoft Fabric admin roles

08/12/2025

Microsoft Fabric administration involves managing organization-wide settings that control how Microsoft Fabric operates. To be a Microsoft Fabric admin for an organization, a user must be assigned one of the following roles:

- Power Platform administrator
- Fabric administrator

These roles provide access the admin portal and control over organization-wide Fabric settings, usage metrics, and admin features, except for licensing. See Microsoft 365 admin roles for details about these roles and the tasks they can perform. Assigning users to dedicated Fabric admin roles allows organizations to grant the permissions needed to administer Fabric without granting full Microsoft 365 admin rights.

Assign users to Fabric admin roles

Microsoft 365 user admins assign users to the Fabric administrator or Power Platform administrator roles in the Microsoft 365 admin portal, or by using a PowerShell script.

Microsoft 365 admin portal

To assign users to an admin role in the Microsoft 365 admin portal, follow the instructions in Add an admin.

PowerShell

You can also assign users to roles by using PowerShell. To assign users to an admin role using PowerShell, follow the instructions in Assign admin roles to Microsoft 365 user accounts with PowerShell.

Related content

- What is the admin portal?
- What is the admin monitoring workspace?

Service interruption notifications

Article • 03/17/2024

It's important to have insight into the availability of your mission-critical business applications. Microsoft Fabric incident notification so you can optionally receive emails if there's a service disruption or degradation.

At this time, emails are sent for the following *reliability scenarios*:

- Open report reliability
- Model refresh reliability
- Query refresh reliability

Notifications are sent when there's an *extended delay* in operations like opening reports, semantic model refresh, or query executions. After an incident is resolved, you receive a follow-up email.

Enable notifications for service outages or incidents

A Fabric admin can enable notifications for service outages or incidents in the admin portal:

1. Identify or create an email-enabled security group that should receive notifications.
2. In the admin portal, select **Tenant settings**. Under **Help and support settings**, expand **Receive email notifications for service outages or incidents**.
3. Enable notifications, enter a security group, and select **Apply**.

Service health in Microsoft 365

This article describes how to receive service notifications through Fabric. You can also monitor Power BI service health through Microsoft 365. Opt in to receive email notifications about service health from Microsoft 365. Learn more in How to check Microsoft 365 service health.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Diagnostic query text storage

Article • 05/29/2024

Diagnostic query text storage is a Fabric feature that stores query text content for a limited period to help Fabric support teams to resolve issues that might arise from the use of some Fabric items. The feature is on by default. This article describes feature and how to disable it, if necessary or desired. Its target audience is Fabric administrators and others (for example, security and compliance teams) who want to understand the feature and its implications for data privacy and security.

Overview

To improve support and provide more effective troubleshooting, Microsoft might store the query text generated when users use Fabric items such as reports and dashboards. This data is sometimes necessary for debugging and resolving complex issues related to the performance and functionality of Fabric items such as semantic models.

What is stored query text

Query text refers to the text of the queries/commands (for example, DAX, MDX, TMSL, XMLA, etc.) that Fabric executes when users use Fabric items such as reports and dashboards, as well as external applications such as Excel, SQL Server Management Studio, etc. This information helps Fabric support teams understand the context and specific details of issues that arise, and facilitates quicker, more precise resolution.

Privacy and security

In compliance with Microsoft's stringent data protection standards, stored query text is securely handled within Fabric and retained for a limited period of time (less than 30 days). The data is used for approved investigations only. To prevent unauthorized use, access is strictly controlled and monitored. Access can also be protected by Customer Lockbox for Microsoft Azure if that feature is enabled.

Disabling diagnostic query text storage

Diagnostic query text storage is controlled by the tenant setting **Microsoft can store query text to aid in support investigation**. The feature is on by default. This means that

unless a Fabric admin changes the setting, Microsoft stores the query text associated with the use of some Fabric items in the organization.

If there are organizational requirements that don't permit the storage of query text, or if you wish to opt out of this feature for any other reason, you can turn the feature off. Go to the tenant settings, find the setting, and set the toggle to **Disabled**. See Microsoft can store query text to aid in support investigation for more information.

> **Note**
>
> The availability of stored query text enables high-quality support without any additional configuration on the part of Fabric administrators. It is thus not recommended to disable diagnostic query text storage unless there is a specific reason for doing so.

Implications of turning off diagnostic query text storage

Turning off diagnostic query text storage stops the storage of new query text data. This might adversely affect the ability of Fabric support teams to provide swift, efficient support should issues arise with your organization's reports or dashboards. Without access to the recent history of query text content, diagnosing and resolving problems might take longer, and it might not be possible to identify a root cause for some complex issues.

Further support

Contact Fabric support for further assistance regarding the query text storage feature.

Feedback

What is the admin monitoring workspace? (Preview)

Article • 09/17/2024

The admin monitoring workspace is a specialized environment designed for Fabric administrators to monitor and manage workloads, usage, and governance within their tenant. Using the resources available within the workspace, admins can perform tasks such as security audits, performance monitoring, capacity management, and more.

Prerequisites

To set up the admin monitoring workspace, a Fabric administrator role is required.

Installing the admin monitoring workspace

The admin monitoring workspace is automatically installed the first time an admin accesses it. Reports in the workspace appear as blank until the first data refresh. The first data refresh begins around five minutes after the workspace is installed, and usually completes within a few minutes.

To trigger the installation of the admin monitoring workspace, follow these steps:

1. Log into Fabric as an admin.
2. From the navigation menu, select **Workspaces**.
3. Select **Admin monitoring**. When selected for the first time, the workspace installation begins automatically and usually completes within a few minutes.

Sharing the admin monitoring workspace

Once set up, admins can share all reports in the workspace with users that aren't admins through a workspace viewer role. Admins can also share individual reports or semantic models with users that aren't admins through links or direct access.

Only admins can see the admin monitoring workspace at the top of the workspaces menu. Users that aren't admins can access the workspace's contents indirectly by using the *Browse* or *OneLake data hub* pages, or by bookmarking the workspace URL.

Managing the admin monitoring workspace

By default, the admin monitoring workspace is a Pro-licensed workspace. To take advantage of capacity benefits such as unlimited content sharing for the admin monitoring workspace, follow these steps:

1. Navigate to the **Admin portal**.
2. Navigate to the **Workspaces** page in the Admin portal.
3. Using the **Name** column filter, search for **Admin monitoring**.
4. Select the **Actions** button, then select **Reassign workspace**.
5. Select the desired **license mode**, then click **Save**.

Reports and semantic models

You can use the reports in the admin monitoring workspace for getting insights about user activity, content sharing, capacity performance, and more in your Fabric tenant. You can also connect to the semantic models in the workspace to create reporting solutions optimized for your organization's needs.

Considerations and limitations

- Only users whose admin roles are assigned directly can set up the admin monitoring workspace. If the workspace creator's admin role is assigned through a group, data refreshes in the workspace fail.
- The admin monitoring workspace is a read-only workspace. Workspace roles don't have the same capabilities as they do in other workspaces. Workspace users, including admins, aren't able to edit or view properties of items such as semantic models and reports in the workspace.
- Users with *build* permissions for a semantic model in the admin monitoring workspace are shown as having *read* permissions.
- Granular delegated admin privileges (GDAP) aren't supported.
- Once access is provided to the admin monitoring workspace or its underlying content, access can't be removed without reinitializing the workspace. However, sharing links can be modified as with a typical workspace.

Refreshes

The semantic models in the workspace are automatically refreshed once per day, around the same time that the workspace was installed for the first time.

To maintain the scheduled refresh process, consider the following limitations:

- If the user who first accessed the workspace is no longer an admin, scheduled refreshes in the workspace fail. This issue can be mitigated by having any other admin log into Fabric, as their credentials will automatically be assigned to all semantic models in the workspace to support any future data refreshes.
- If the admin who first accessed the workspace uses Privileged Identity Management (PIM), their PIM access must be active during the time of scheduled data refresh, otherwise the refresh fails.

Reinitializing the workspace

Occasionally, administrators may need to reinitialize the workspace, including to reset access to the workspace or its underlying content.

Admins can execute an API to reinitialize the workspace using the following steps:

1. Retrieve the ID of the admin monitoring workspace from the URL when viewing the workspace.
2. Execute the semantic model deletion API, first replacing the 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx' with the ID of your admin monitoring workspace.

   ```
   api.powerbi.com/v1/admin/workspaces/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx -Method Delete
   ```

3. Click the **Workspaces** menu and select **Admin monitoring** to trigger the reinitialization of the workspace, similar to the process of the first installation. On occasion, refreshing the page is also required.

Related content

- Admin overview
- Feature usage and adoption report

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Feature usage and adoption report (preview)

Article • 03/06/2025

The feature usage and adoption report is aimed at admins who want to understand how Fabric features are utilized across the organization. As an admin, the report insights can help you govern your Fabric tenant and take action when needed.

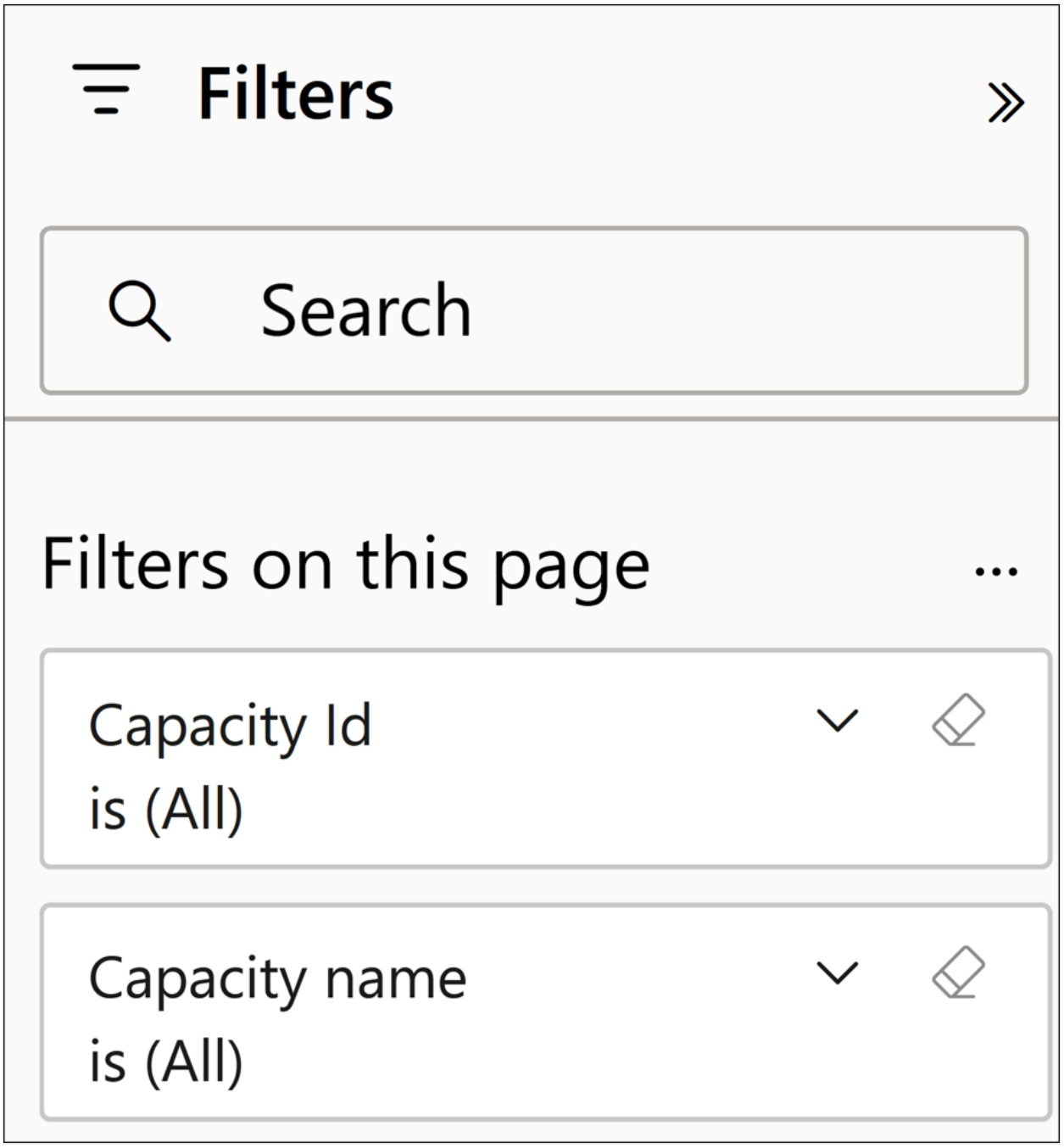
You can access the report from the Admin monitoring workspace. To access the workspace, you must be a Fabric administrator.

You can also have an admin share the report or semantic model directly with you. With build permissions to the semantic model, users can design a custom report that relies on the same underlying data.

Navigation

The report is designed for admins to analyze Fabric activity in various ways. Use the date range slicer to filter activity data across all pages for a specific range of time over the last 30 days.

Additionally, use the filter pane to filter activity data based on the desired analysis. Filters are available across different characteristics of activity, including capacity, user, and item-related info.



Report pages

The report is composed of five pages:

- **Activity Overview** - Provides a high-level overview of Fabric activity across the organization
- **Analysis** - Visualizes activity across different activity dimensions
- **Activity Details** - Shows detailed information on specific activity scenarios
- **Inventory** - Lists all Fabric items in your tenant
- **Item Details page** - Shows detailed information on specific inventory usage scenarios

Activity Overview page

The Activity Overview page helps you identify:

- Daily activities and user trends
- The most active capacities and workspaces
- Activities in your organization by your most or least active users

Example

In a large retail organization, you might use the Activity Overview page to check which capacities were most utilized in a given month. Using the date range slicer to filter to the month of December, you notice the *Sales and Marketing* capacity had nearly 1,000 activities while other capacities had under 200. To understand why this is happening, you then go to the Analysis page.

Analysis page

On the Analysis page, you can view:

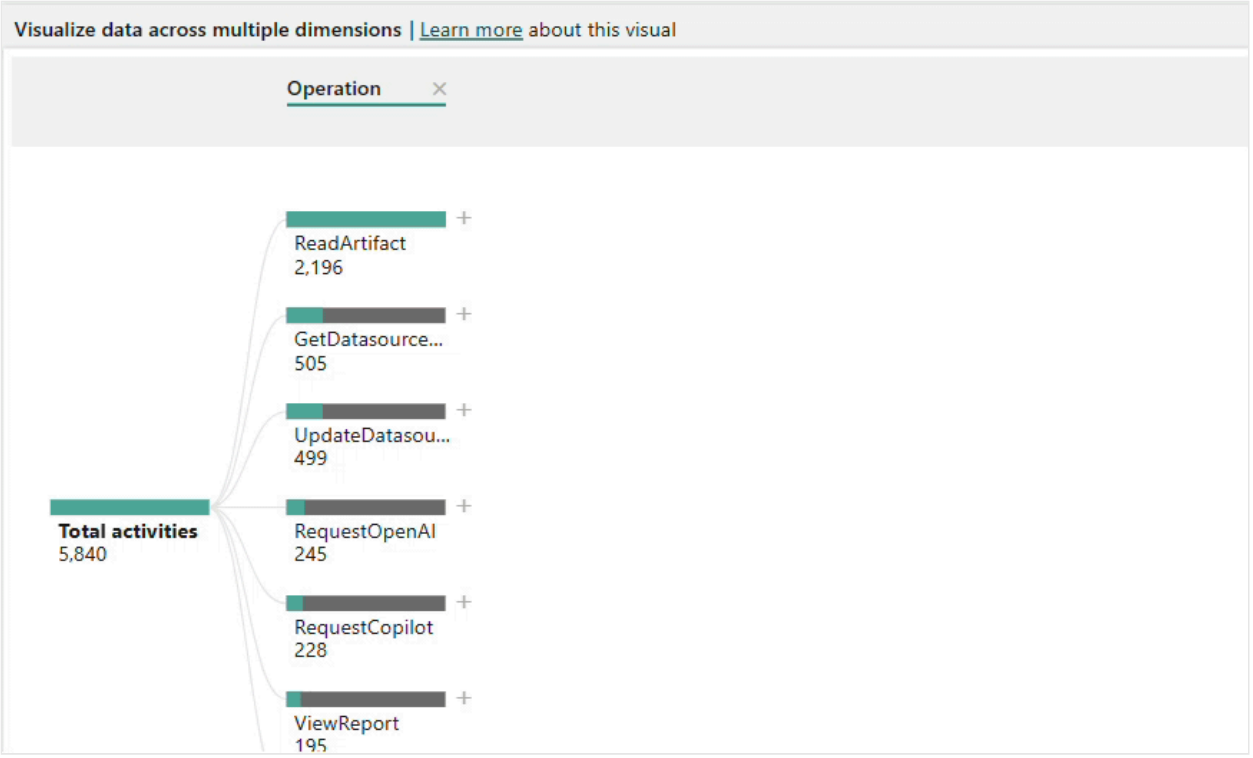
- A daily count of activity and users by date
- A decomposition tree to drill down into activity using dimensions such as operation, capacity, user, and more

Example

Continuing the example from the Activity Overview page, you use the Analysis page to investigate why the *Sales and Marketing* capacity had more activity in December than all other capacities. The decomposition tree reveals the most popular activity on the *Sales and Marketing* capacity was *ViewReport*, which signifies the viewing of a Power BI report. You then drill through to the Activity Details page to identify which reports were most frequently viewed that month on the *Sales and Marketing* capacity.

To drill through to the Activity Details page:

1. Right-click the visual element (such as Operation name) you want to drill through from.
2. Select *Drill through*.
3. Select *Activity Details*.



Activity Details page

The Activity Details page shows detailed information on specific activity scenarios. Users can access this page by drilling through from the Activity Overview or Analysis pages to display the following activity details:

- **Creation time** - The time the activity was registered
- **Capacity name** - The name of the capacity that the activity took place on
- **Capacity ID** - The ID of the capacity that the activity took place on
- **Workspace name** - The name of the workspace that the activity took place in
- **Workspace ID** - The ID of the workspace that the activity took place in
- **User (UPN)** - The user principal name of the user who conducted the activity
- **Operation** - The formal name of the operation
- **Total of activities** - The number of times the activity took place

Example

From the Analysis page, you drill through on frequently conducted *ViewReport* actions on the *Sales and Marketing* capacity in December. Using info from the Activity Details page, you discover that a new report titled "Unclosed Deals" was heavily viewed,

prompting further investigation to understand the report's impact on your organization's sales strategy.

Inventory page

The Inventory page displays all items in your Fabric tenant and how they're utilized. You can filter the Inventory page by:

- **Item type** - Including reports, dashboards, lakehouses, notebooks, and more
- **Workspace name** - The name of the workspace where the items are located
- **Activity status** - Indicates whether the item has been recently utilized
  - *Active* - At least one audit log activity was generated related to the item over the last 30 days
  - *Inactive* - No audit log activity was generated related to the item over the last 30 days

Example

The Inventory page also includes a decomposition tree visual to breakdown inventory by different factors such as capacity, user, workspace, and more. You can use the decomposition tree to decompose items by activity status; for example, displaying all inactive items by item name so that you can decide whether any of these items can be deleted.

Item Details page

The Item Details page shows information related to specific inventory usage scenarios.

Users can navigate to the Item Details page by drilling through from the Inventory page. To drill through, right-click a visual element (such as Item type) and then select the Item Details page from the *Drill through* menu.

After drilling through, you see the following information for the selected item types:

- **Capacity ID** - The ID of the capacity that the item is hosted on
- **Workspace ID** - The ID of the workspace that the item is located in
- **Workspace name** - The name of the workspace that the item is located in
- **Item ID** - The unique ID of the item

- **Item name** - The display name of the item
- **Item type** - The type of item such as report, dataset, app, and so on
- **Modified by** - The ID of the user that last modified the item
- **Activity status** - The status of an item whether it's active or inactive based on recent activity
- **Items** - The total number of items

Measures

The following measures are used in visuals throughout the report and are also available in the semantic model.

Measure calculations consider filter context, so measure values change as you apply filters or interact with other visuals.

Expand table

Measure name	Description
Active capacities	The number of capacities with audit activity.
Active users	The number of users who have generated audit activity.
Active workspaces	The number of workspaces with audit activity.
Activities	The number of audit activities generated.
Items	The count of items displayed.
Total activities	The number of audit activities generated. Reflected as 0 when no audit data is returned; used exclusively in card visuals.
Total items	The count of items displayed. Reflected as 0 when no items are returned; used exclusively in card visuals.

Considerations and limitations

This section lists the report's considerations and limitations.

Display

- Condensing the zoom slider on a date trend visual to a single day displays a misleading time range, as activities are aggregated by day and not by time.
- Using the *next level in the hierarchy* option on the *Most active Capacities* visual doesn't update the dynamic visual title.
- Items with the same name, or items deleted and recreated with the same name, might reflect as one item in certain visuals. To count the total number of unique items, use item IDs or the *Total items* measure.
- *NA* represents data that isn't available, which can happen when an audit event doesn't have complete information, or when that information isn't applicable for the event.
- The report retains information for 30 days, including the activities and metadata of deleted capacities, workspaces, and other items.
- Deleted workspaces with extended retention don't appear in the report after 30 days. They can be seen in the admin portal until they're permanently deleted.
- Items created and deleted within a 24 hour period may have incomplete information.

Pro and Premium Per User (PPU)

Semantic models in *Pro* and *Premium Per User* (PPU) workspaces are hosted on internal logical capacities. The usage of these capacities can be seen in this report.

- **Pro** - Appear as *Reserved Capacity for Pro Workspaces* with the capacity SKU value *Pro*.
- **PPU** - Appear as *Reserved Capacity for Premium Per User Workspaces* with the capacity SKU value *PPU*.

Counting logic

- All *My workspaces* are counted as separate records as part of the *Active workspaces* measure.

Related content

- What is the Admin monitoring workspace?

- Admin overview

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Content sharing report (preview)

07/02/2025

The *content sharing* report is aimed at admins who want to understand how Fabric items are distributed and shared across the organization. As an admin, the report insights can help you govern your Fabric tenant and take action if needed.

You can access the report from the Admin monitoring workspace. To access the workspace, you must be a Fabric administrator or a Microsoft 365 global administrator.

You can also have an admin share the report or semantic model directly with you. With build permissions to the semantic model, users can design a custom report that relies on the same underlying data.

Navigation

The report is designed for admins to analyze their Fabric inventory in various ways.

Use the slicers pane on the left side of the report to filter inventory on key attributes such as workspace, item type, and capacity. The filters pane on the right side of the report provides more options to further manipulate the data.

To switch pages, use the navigation buttons at the top right of the report.

Report pages

The report is composed of four pages:

- **Inventory Overview** - Provides a high-level overview of Fabric items across your organization
- **Analysis** - Visualizes inventory across different dimensions
- **Workspace** - Shows detailed inventory information for one or multiple workspaces
- **Details** - Lists all Fabric items in a tabular view

Inventory Overview page

The Inventory Overview page provides a high-level summary of how items are distributed in your organization.

Use the Inventory Overview page to quickly answer questions such as:

- Which workspaces in my tenant have the most items?
- Which Fabric item types are most commonly used in my organization?
- How are my items distributed by endorsement and sensitivity label?
- Is my organization effectively using domains to organize its Fabric inventory?

Analysis page

On the Analysis page, you're provided with a decomposition tree visual to aggregate and drill into your inventory.

Using the toggle at the bottom left of the page, you can decide whether to break down your inventory by total items or by total access count. Definitions for these measures are provided in the Measures section.

You can then break down either measure across different item-related dimensions, including item type, workspace name, endorsement, and more.

The Analysis page can be accessed directly using the page navigation buttons, or by drilling through from other pages in the report.

Example

In a large organization, the Analysis page can be helpful for analyzing item distribution. You can also drill into specific data points for a closer look at item distribution.

To drill into the details of a specific scenario from the decomposition tree visual:

1. With the *Analyze by* toggle set to *Total items*, you select the following dimensions: *Capacity name*, *Workspace name*, and *Item type*.
2. Right-click the data point on the decomposition tree visual that you want to drill into.
3. From the *Drill through* menu, select the Workspace or Details page.

After you drill through, the target page and its visuals are prefiltered to the subset of data selected from the Analysis page.

Workspace page

On the Workspace page, you're provided with details on how items within a specific workspace are shared. The Workspace page includes visuals that highlight certain scenarios such as:

- Most shared items by total access count
- Item distribution by endorsement and sensitivity label
- Items shared with the entire organization using links
- Item deleted within the last 28 days

Example

To drill into the details of a specific workspace:

1. Right-click any visual that uses the *Workspace name* field, then select the *Workspace* page from the *Drill through* menu.
2. After drilling through, you can see detailed metrics for the selected workspace, with the ability to drill through even further to the *Details* page.
3. Once on the Workspace page, users can select attributes from the available slicers or the filters pane to further manipulate the data.

In addition to drilling through, users can also access the *Workspace* page directly using the page navigation buttons.

Details page

The Details page highlights item distribution in a tabular format.

You can also navigate to the *Details* page by drilling through from other pages in the report. To drill through, right-click a value in any visual, then select the *Details* page from the *Drill through* menu. After drilling through to the *Details* page, you can see information for the specific subset of items.

You can export data from the Details page, or any other visual, by clicking *More options* in the visual header and selecting *Export data*.

You can also navigate directly to an item or its workspace using the hyperlinks in the data table.

> **Note**

Workspaces can only be accessed if you have a valid workspace role, else you are redirected to your *My workspace*. Item urls currently only support legacy Power BI items and some Fabric items.

Measures

The following measures are used in visuals throughout the *content sharing* report and are also available in the semantic model.

Expand table

Measure name	Description
Total items	The number of Fabric items across the entire tenant.
Total domains	The number of domains with items.
Total capacities	The number of capacities with items.
Total workspaces	The number of workspaces with items.
User access count	The number of individual users and service principals with access to an item.
Group access count	The number of group members and service principals with access to an item. Group owners aren't included in *group access counts*. Group access counts are calculated by flattening membership of all nested groups, so users aren't double counted if they're members of multiple groups in a nest. *Group access counts* also include +1 for each nested group in a nest.
Total access count	The number of individual users, service principals, and group members with access to an item. *Total access counts* for workspaces, capacities, and domains are a sum of access counts for all underlying items, not the container itself. *Total access counts* include both individual access to an item and access through a group, so users are double counted if they have access to an item in both scenarios.

Note

Access counts include access to an item through *Manage permissions*, or access inherited through a workspace role. Access counts also include service principals and sharing links for a specific persons or group.

Considerations and limitations

This section lists the report's considerations and limitations.

Display

- Items with the same name, or items deleted and recreated with the same name, might reflect as one item in certain visuals. To count the total number of unique items, use item IDs or the *Total items* measure.
- The report retains information for 28 days, including deleted capacities, workspaces, and other items.
- Deleted workspaces with extended retention don't appear in the report after 28 days. They can be seen in the admin portal until they're permanently deleted.
- Items created and deleted within a 24 hour period may have incomplete information.
- Reports and dashboards embedded in apps appear twice. Use the *Item ID* value to differentiate.

Pro and Premium Per User (PPU)

Semantic models in *Pro* and *Premium Per User* (PPU) workspaces are hosted on internal logical capacities.

- **Pro** - Appear as *Reserved Capacity for Pro Workspaces* with the capacity SKU value *Pro*.
- **PPU** - Appear as *Reserved Capacity for Premium Per User Workspaces* with the capacity SKU value *PPU*.

Counting logic

- All *My workspaces* are counted as separate records as part of the *Total workspaces* measure.
- Trial Fabric capacities are counted as separate records as part of the *Total capacities* measure. Trial capacities can be filtered out using the Capacity SKU filter with the value *FT1*.

Related content

- What is the Admin monitoring workspace?

- Admin overview

Use the Monitor hub

Article • 11/04/2024

The Microsoft Fabric *Monitor* hub enables users to monitor Microsoft Fabric activities from a central location. Any Fabric user can use the monitor hub, however, the monitor hub displays activities only for Fabric items you have permission to view.

The monitor hub displays activities for these Fabric items:

- Data pipelines
- Dataflows
- Datamarts
- Lakehouses
- Notebooks
- Semantic models
- Spark job definitions

View the monitor hub display

To open the monitor hub, In Fabric, select **Monitoring** from the navigation pane. The monitor hub displays information in a table form. Fabric activities are displayed according to their start time, with the newest activities at the top of the table. Each Fabric item displays a maximum of 100 activities. History is kept for 30 days and can be viewed using the *Historical view* option.

Interact with the monitor hub

You can use the monitor hub display options to find the activities you're interested in. This section describes the monitor hub controls.

Change the display order

You can change the order of the table's display by selecting each column title. The table is sorted according to your selection and the arrow next to the column header indicates the sorting order.

Configure table columns

Use the **Column options** button to add, remove and rearrange the columns displayed in the table.

- **Add** - Select a column from the *Column options* list.
- **Remove** - Remove the selection indicator from a column in the *Column options* list.
- **Rearrange** - In the *Column options* list, drag columns to your selected position.

Keyword search

Use the keyword search text box to search for specific activities according to their activity name. The search is performed on the loaded data, not on all the activities in the database.

Filter

Use the **Filter** button to filter the monitor hub table results. You can use a combination of any of the options listed below. Once you selected the options you want to filter for, select **Apply**. The monitor hub remembers your filter selection. If you leave the monitor hub, you'll see your selection when you next go to the hub.

Each time the table is refreshed, the recent 100 jobs are loaded in order, according to the filter option. By selecting *load more* you can load 50 more jobs.

- **Status** - Select the type of status you want the table to display. When no status is selected, item activities for all statuses are displayed.

  > ⓘ **Note**
  >
  > Each Fabric item has a unique set of operations and statuses. To display consistent results, the monitor hub might show a simplified version of an item's status. The exact status of an item, can be found in the details panel.

- **Start time** - Select the time period for the table to display. You can select a predetermined period, or use *Customize* to personalize the time period.
- **Item type** - Select the Fabric item types you want to table to display. When no item type is selected, item activities for all the item types are displayed.

- **Submitted by** - Select the owner of the Fabric item that the table displays activities for. When no owner is selected, activities for all item owners are displayed.
- **Location** - Select which workspaces to view item activities from. When no workspace is selected, item activities from all workspaces are displayed.

Take action

Providing you have the right permissions for the Fabric item displayed in the monitor hub table, you might be able to perform certain actions. The actions you can take depend on the type of item you're reviewing. To take action, select *More options* (**...**) next to the activity name, and from the menu, select the action you want to take.

Historical runs

You can view the history of a single Fabric item using the *Historical runs* option.

Select *More options* (**...**) next to the activity name of the item you're interested in, and from the menu, select *Historical runs*. The table displays up to 30 days of historical information for that item.

To return to the main display, select *Back to main view*.

View details

To view the details of an activity, hover over its activity name and select the *View detail* symbol (**i**).

Limitation

Dataflow Gen1 is not supported and isn't displayed in the table.

Related content

- Admin overview
- Browse the Apache Spark applications in the Fabric monitoring hub
- View refresh history and monitor your dataflows
- Feature usage and adoption report

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Track user activities in Microsoft Fabric

06/23/2025

Knowing who is taking what action on which item in Microsoft Fabric, can be critical in helping your organization fulfill requirements such as meeting regulatory compliance and records management. This article discusses tracking user activities using the audit log.

Prerequisites

You must be assigned the Audit Logs role in Exchange Online to access the audit log. By default, the Compliance Management and Organization Management role groups have roles assigned on the **Admin roles** page in the Exchange admin center. For more information about the roles that can view audit logs, see Requirements to search the audit log.

Access

To access the audit logs, go to Microsoft Purview.

Search the audit logs

You can search the audit logs using the Microsoft Purview filters. When you combine filters, the search results show only items that match all of the filter criteria. This section lists some of the available filters. For more information, review the Microsoft Purview documentation.

- **Date and time range** - Search the logs by date range using the *Start date* and *End date* fields. The default selection is the past seven days. The display presents the date and time in UTC format. For the maximum date range supported, please visit Microsoft Purview documentation.
- **Activities** - Your search returns the selected activities.
- **Users** - Search for activities performed by specific users. Enter one or more user names in the *Users* field. User names appear in email address format. Leave blank to return entries for all users (and service accounts) in your organization.
- **File, folder, or site** - Search by file name, folder name, or URL.

You can also use PowerShell to view audit logs. TO use PowerShell, Connect to Exchange Online PowerShell. You can also use the blog post Using Power BI Audit Log and PowerShell to assign Power BI Pro licenses as a reference.

Audit log list

Operation list includes a list of all the audit log entries.

Considerations and limitations

When capacity ID and capacity name aren't available in the audit logs, you can view them in the Microsoft Fabric Capacity Metrics app.

Related content

- Operation list

Operation list

Article • 05/18/2025

The following operations are available in the audit logs.

Expand table

Friendly name	Operation name	Notes
Abort copy blob operation	AbortCopyBlob	OneLake operation. Stops a pending Copy Blob operation, and leaves a destination blob with zero length and full metadata.
Accept an invitation to external data share	AcceptExternalDataShare	Accept an invitation to external data share
Add Admin Personal Workspace Access	AddAdminPersonalWorkspaceAccess	
Add Artifact To Pipeline	AddArtifactToPipeline	
Add Experiment Run	AddExperimentRun	
Add Model Version	AddModelVersion	
Add Tenant Key	AddTenantKey	
Add Tile	AddTile	Add Tile is dashboard activity, which is generated on adding visuals as tiles to a Power BI Dashboard
Add workload in a tenant or capacity	ExtensibilityActivationDynamic	Add a workload in a tenant or capacity from Workloads Hub
Add workload version in a tenant	ExtensibilityActivationStatic	Add a specific version of a workload in a tenant
Add workspace role	AddWorkspaceRoleViaAdminApi	Add workspace role
Added Power BI folder access	AddFolderAccess	Not currently used
Added Power BI group members	AddGroupMembers	
Added data source to Power BI gateway	AddDatasourceToGateway	
Added external resource	AddExternalResource	Registers or connects an external resource in the Fabric workspace.
Added link to external resource	AddLinkToExternalResource	Links a Fabric item to an external resource for reference or integration.
Added user to Power BI gateway cluster	AddUsersToGatewayCluster	Not currently used
Added user to Power BI gateway cluster datasource	AddUsersToGatewayClusterDatasource	
Admin Get Artifacts Byuser Id	AdminGetArtifactsByuserId	
Admin attached dataflow storage account to tenant	AdminAttachedDataflowStorageAccountToTenant	Not currently used
Analyze In Excel Dataset	AnalyzeInExcelDataset	
Analyze In Excel Report	AnalyzeInExcelReport	
Analyzed Power BI report	AnalyzeInExcel	Generated when a user selects Analyze in Excel on a report or semantic model in the service and successfully generates an Excel workbook
Analyzed Power BI semantic model	AnalyzedByExternalApplication	Generated when users interact with the service
Append block from URL	AppendBlockFromURL	OneLake operation. Writes a block of data from a URL to the en of an append blob (append blobs only)

Friendly name	Operation name	Notes
Append block to blob	AppendBlock	OneLake operation. Writes a block of data to the end of an append blob (append blobs only)
Append data to file	AppendDataToFile	OneLake operation. Uploads data to be append to a file (DFS).
Applied a change to model in Power BI	ApplyChangeToPowerBIModel	A user makes a change to an existing model. This occurs whenever any edit is made to the model (ex: write a DAX measure, manage relationships, etc.)
Applied sensitivity label to Power BI item	SensitivityLabelApplied	
Assign Workspace To Alm Pipeline	AssignWorkspaceToAlmPipeline	
Assigned a workspace to a deployment pipeline	AssignWorkspaceToPipeline	Not currently used
Attach Notebook Environment	AttachNotebookEnvironment	Attach the environment for Notebook.
Attach source in GraphQL artifact	AttachSourceGraphQL	Attach source in graphql artifact
Attached dataflow storage account	AttachedDataflowStorageAccount	
Auto bind user credentials to git	AutoBindGitCredentials	Auto bind existing user credentials for a git provider to a git connection
Binded Power BI semantic model to gateway	BindToGateway	
Binded monikers to Power BI datasources	BindMonikersToDatasources	
Branch Out in Git	BranchOutInGit	Branch out in Git is a workspace activity which is generated whe a new workspace is created, which is connected to a newly forked git branch based on the git branch that is connected to the origin workspace.
Cancel Datamart Batch	CancelDatamartBatch	
Cancel Dataset Refresh	CancelDatasetRefresh	
Cancel Publish Environment	CancelPublishEnvironment	Cancel publish environment
Cancel Running Artifact	CancelRunningArtifact	
Cancel Spark Application	CancelSparkApplication	
Cancel Sql Analytics Endpoint Lakehouse Batch	CancelSqlAnalyticsEndpointLakehouseBatch	Canceled a lakehouse SQL analytics endpoint batch. Previously named *Canceled a default warehouse* (Operation name: *CancelDefaultWarehouseBatch*)
Cancel Warehouse Batch	CancelWarehouseBatch	
Cancel Workspace Upgrades As Admin	CancelWorkspaceUpgradesAsAdmin	
Cancel mounted warehouse batch	CancelMountedWarehouseBatch	Generated when a mounted warehouse batch is canceled
Canceled Power BI dataflow refresh	CancelDataflowRefresh	
Changed Power BI gateway admins	ChangeGatewayAdministrators	
Changed Power BI gateway data source users	ChangeGatewayDatasourceUsers	
Changed Power BI semantic model connections	SetAllConnections	
Changed capacity state	ChangeCapacityState	

Friendly name	Operation name	Notes
Changed capacity user assignment	UpdateCapacityUsersAssignment	
Changed sensitivity label for Power BI item	SensitivityLabelChanged	
Check Scorecard Access	CheckScorecardAccess	Verifies the access permissions for a scorecard
Check access to file or blob	CheckAccessFileOrBlob	OneLake operation. Checks if the calling user has permission to perform the specified operation
Checkout Branch In Git	CheckoutBranchInGit	
Cleanup unused or corrupted files from dataflows' refreshes	CleanupDataflow	Cleanup unused or corrupted files from dataflows' refreshes
Clone Tile	CloneTile	
Co Author Notebook	CoAuthorNotebook	
Commit Notebook	CommitNotebook	
Commit To Git	CommitToGit	Commit To Git is an artifact activity, which is generated when users commit artifact to Git.
Completed an artifact access request action in Power BI	ArtifactAccessRequest	Tracks the notification sent to approvers when a request is created or denied.
Connect To Git	ConnectToGit	Connect To Git is a workspace activity, which is generated when users connect the workspace to Git.
Connected to Power BI semantic model from external app	ConnectFromExternalApplication	
Connected to a Warehouse or SQL analytics endpoint from an external app	ConnectWarehouseAndSqlAnalyticsEndpointLakehouseFromExternalApp	Previously named *Connected to a warehouse or default warehouse from an external app* (Operation name: *ConnectWarehouseAndDefaultWarehouseFromExternalAp*
Convert Personal Workspace To Workspace	ConvertPersonalWorkspaceToWorkspace	
Copied Power BI dashboard	CopyDashboard	
Copied Power BI report	CopyReport	
Copy Scorecard	CopyScorecard	
Copy blob	CopyBlob	OneLake operation. Copies a source blob to a destination blob i this storage account or in another storage account.
Create an SQL query from a Warehouse	CreateSqlQueryFromWarehouse	
Create Artifact	CreateArtifact	
Create Branch In Git	CreateBranchInGit	Create Branch In Git is a git provider activity, which is generated when users create branch in Git.
Create Cloud Datasource From Kind Path	CreateCloudDatasourceFromKindPath	Creates a cloud-based data source using a specific resource and path.
Create Cloud Datasource	CreateCloudDatasource	Establishes a new cloud data connection to external storage or services.
Create Data Sharing	CreateDataSharing	Create a new external data share
Create Datamart	CreateDatamart	Triggered when a new Datamart is created in a Workspace
Create Dataset By Quick Share	CreateDatasetByQuickShare	
Create Directory In Git	CreateDirectoryInGit	Create Directory In Git is a git provider activity, which is generated when users create directory in Git.

Friendly name	Operation name	Notes
Create Environment Resource	CreateEnvironmentResource	Create resources in environment
Create Fabric Identity for Workspace	CreateWorkspaceIdentityViaApi	Create a Fabric identity for a workspace
Create Folder	CreateFolder	Indicates a creation of a new workspace
Create Gateway Cluster User	CreateGatewayClusterUser	
Create Gateway Tenant Key	CreateGatewayTenantKey	
Create Goal Value Categories	CreateGoalValueCategories	
Create Hierarchy Goal Value	CreateHierarchyGoalValue	
Create Hierarchy Note	CreateHierarchyNote	
Create Lakehouse File	CreateLakehouseFile	
Create Lakehouse Folder	CreateLakehouseFolder	
Create Lakehouse Shortcut	CreateLakehouseShortcutLink	
Create Lakehouse Table	CreateLakehouseTable	
Create Link Goals	CreateLinkGoals	
Create Managed Private Endpoint	CreateManagedPrivateEndpoint	Create a private endpoint within a managed virtual network for workspace
Create Managed VNet	CreateManagedVNet	Create managed virtual network for a workspace
Create MetricSet Metric Endpoint	CreateMetricSetMetric	Create metric in a metricset endpoint
Create Notebook Resource	CreateNotebookResource	Create resources in notebook.
Create Org App	CreateOrgApp	
Create Personal Datasource	CreatePersonalDatasource	
Create Report From Lakehouse	CreateReportFromLakehouse	
Create Scorecard Hierarchy	CreateScorecardHierarchy	
Create Scorecard View	CreateScorecardView	
Create Semantic Metric Endpoint	CreateSemanticMetric	Create standalone semantic metric endpoint
Create Service Principal Profile	CreateServicePrincipalProfile	
Create Template App Package	CreateTemplateAppPackage	Create Template App Package is an app activity, which is generated on creation of a Template App Package
Create Temporary Upload Location	CreateTemporaryUploadLocation	Generated when a temporary upload URL is created.
Created visual query from a Warehouse	CreateVisualQueryFromWarehouse	
Create Warehouse	CreateWarehouse	
Create Workspace	CreateWorkspace	
Create a shortcut	CreateShortcut	OneLake operation. Part of Shortcut Controller
Create an external data share	CreateExternalDataShare	Create an external data share
Create blob from URL	PutBlobFromURL	OneLake operation. Creates a new blob or replaces an existing one where contents are from a URL.

Friendly name	Operation name	Notes
Create blob	PutBlob	OneLake operation. Creates a new blob or replaces an existing one.
Create block list	PutBlockList	OneLake operation. Commits a blob by specifying the set of block IDs that comprise the block blob.
Create block	PutBlock	OneLake operation. Creates a new block to be committed as pa of a block blob.
Create container	CreateContainer	OneLake operation. Creates a new workspace in OneLake
Create directory	CreateDirectory	OneLake operation. Creates a new directory.
Create file system	CreateFileSystem	OneLake operation. Creates a new workspace.
Create file	CreateFile	OneLake operation. Creates a new file.
Create gateway cluster data source from kind path JSON	CreateGatewayClusterDatasourceFromKindPath	Create gateway cluster data source from kind path JSON
Create or update data access roles	CreateOrUpdateDataAccessRoles	Creates or updates data access roles
Create subfolder	CreateSubfolder	
Create task flow	CreateTaskFlow	
Create virtual network data gateway proxy	CreateVirtualNetworkDataGatewayProxy	Create HTTP proxy for virtual network data gateway
Created Power BI app	CreateApp	
Created Power BI dashboard	CreateDashboard	
Created Power BI dataflow	CreateDataflow	
Created Power BI email subscription	CreateEmailSubscription	
Created Power BI gateway cluster datasource	CreateGatewayClusterDatasource	
Created Power BI gateway	CreateGateway	
Created Power BI group	CreateGroup	
Created Power BI report	CreateReport	
Created Power BI semantic model from external app	CreateDatasetFromExternalApplication	
Created Power BI semantic model	CreateDataset	
Created a Power BI metric value	CreateGoalValue	
Created a Power BI scorecard metric	CreateGoal	
Created a Power BI scorecard	CreateScorecard	
Created a visual query from an SQL analytics endpoint	CreateVisualQueryFromSqlAnalyticsEndpointLakehouse	
Created a Power BI template or a workspace for a template app	CreateTemplateApp	
Created an install ticket for installing Power BI template app	CreateTemplateAppInstallTicket	
Created an organizational custom visual	InsertOrganizationalGalleryItem	

Friendly name	Operation name	Notes
Created an SQL query from a SQL analytics endpoint	CreateSqlQueryFromSqlAnalyticsEndpointLakehouse	
Created deployment pipeline	CreateAlmPipeline	
Custom visual requested Azure AD access token	GenerateCustomVisualAADAccessToken	
Custom visual requested Office Web Apps access token	CustomVisualWACAccessToken	Not currently used
D L P Info	DLPInfo	
D L P Rule Match	DLPRuleMatch	
D L P Rule Undo	DLPRuleUndo	
Dataflow migrated to external storage account	DataflowMigratedToExternalStorageAccount	Not currently used
Dataflow permissions added	DataflowPermissionsAdded	Not currently used
Dataflow permissions removed	DataflowPermissionsRemoved	Not currently used
Delete Alm Pipeline Access As Admin	DeleteAlmPipelineAccessAsAdmin	
Delete Alm Pipeline Access	DeleteAlmPipelineAccess	
Delete Artifact	DeleteArtifact	
Delete Capacity Delegation settings	DeleteCapacityTenantSettingDelegation	Delete Capacity delegation settings.
Delete Datamart	DeleteDatamart	
Delete Domain	DeleteDataDomainAsAdmin	Delete Domain
Delete Domain's Folder Relation As Folder Owner	DeleteDataDomainFolderRelationsAsFolderOwner	Delete Domain's Folder Relation As Folder Owner
Delete Environment Resource	DeleteEnvironmentResource	Delete resources in environment
Delete Experiment Run	DeleteExperimentRun	
Delete Fabric Identity for Workspace	DeleteWorkspaceIdentityViaApi	Delete a Fabric identity for a workspace
Delete Folder	DeleteFolder	Indicated a deletion of a workspace
Delete Goal Current Value Rollup	DeleteGoalCurrentValueRollup	
Delete Goal Status Rules	DeleteGoalStatusRules	
Delete Goal Target Value Connection	DeleteGoalTargetValueConnection	
Delete Goal Target Value Rollup	DeleteGoalTargetValueRollup	
Delete Goal Value Categories	DeleteGoalValueCategories	
Delete Goal Value	DeleteGoalValue	
Delete Goals	DeleteGoals	
Delete Group Workspace	DeleteGroupWorkspace	
Delete Hierarchy Goal Value	DeleteHierarchyGoalValue	
Delete Hierarchy Note	DeleteHierarchyNote	

Friendly name	Operation name	Notes
Delete Lakehouse File	DeleteLakehouseFile	
Delete Lakehouse Folder	DeleteLakehouseFolder	
Delete Lakehouse Table	DeleteLakehouseTable	
Delete Link Goals	DeleteLinkGoals	
Delete Managed Private Endpoint	DeleteManagedPrivateEndpoint	Delete a private endpoint within a managed virtual network for workspace
Delete Managed VNet	DeleteManagedVNet	Delete managedvirtual network for a workspace
Delete MetricSet Metric Endpoint	DeleteMetricSetMetric	Delete metric in a metricset endpoint
Delete Model Version	DeleteModelVersion	Triggered when a Machine Learning Model version is removed
Delete Notebook Resource	DeleteNotebookResource	Update resources in notebook.
Delete Scorecard Hierarchy	DeleteScorecardHierarchy	Triggered when a scorecard hierarchy is deleted. That is, the hierarchy's metadata is deleted, not the values of the goals in it.
Delete Scorecard View	DeleteScorecardView	Triggered when a scorecard view (list, heatmap and compact) is deleted.
Delete Semantic Metric Endpoint	DeleteSemanticMetric	Delete standalone semantic metric endpoint
Delete Service Principal Profile As Admin	DeleteServicePrincipalProfileAsAdmin	
Delete Service Principal Profile	DeleteServicePrincipalProfile	
Delete Template App Package	DeleteTemplateAppPackage	Delete Template App Package is an app activity, which is generated on deletion of a Template App package
Delete Tile	DeleteTile	Delete Tile is a dashboard activity, which is generated on deletion of tiles from a Power BI Dashboard
Delete Warehouse	DeleteWarehouse	
Delete Workspace Via Admin Api	DeleteWorkspaceViaAdminApi	
Delete a shortcut	DeleteShortcut	OneLake operation. Part of Shortcut Controller
Delete admin monitoring folder via lockbox	DeleteAdminMonitoringFolderViaLockbox	
Delete admin usage dashboards via lockbox	DeleteAdminUsageDashboardsViaLockbox	
Delete all Domain's Folders Relations	DeleteAllDataDomainFoldersRelationsAsAdmin	Delete all Domain's Folders Relations
Delete blob	DeleteBlob	OneLake operation. Deletes a folder or file.
Delete configured credentials	DeleteGitProviderCredentials	Delete configured git provider credentials for a specific user
Delete container	DeleteContainer	OneLake operation. Deletes a workspace.
Delete file system	DeleteFileSystem	OneLake operation. Deletes a workspace.
Delete file	DeleteFileOrBlob	OneLake operation. Deletes a folder or file.
Delete source in GraphQL artifact	DeleteSourceGraphQL	Delete source in graphql artifact
Delete subfolder	DeleteSubfolder	
Delete usage metrics v2 package via lockbox	DeleteUsageMetricsv2PackageViaLockbox	
Delete virtual network data gateway proxy	DeleteVirtualNetworkDataGatewayProxy	Delete HTTP proxy for virtual network data gateway

Friendly name	Operation name	Notes
Delete workload package	ExtensibilityDeletePackage	Delete a workload package
Delete workspace role	DeleteWorkspaceRoleViaAdminApi	Delete workspace role
DeleteDelete Workspace Delegation settings	DeleteWorkspaceTenantSettingDelegation	Delete Workspace Delegation settings.
Deleted Power BI comment	DeleteComment	
Deleted Power BI dashboard	DeleteDashboard	
Deleted Power BI dataflow	DeleteDataflow	
Deleted Power BI email subscription	DeleteEmailSubscription	
Deleted Power BI folder access	DeleteFolderAccess	Not currently used
Deleted Power BI gateway cluster datasource	DeleteGatewayClusterDatasource	
Deleted Power BI gateway cluster	DeleteGatewayCluster	
Deleted Power BI gateway	DeleteGateway	
Deleted Power BI group	DeleteGroup	
Deleted Power BI metric	DeleteGoal	
Deleted Power BI note	DeleteNote	
Deleted Power BI report	DeleteReport	
Deleted Power BI scorecard	DeleteScorecard	
Deleted Power BI semantic model from external app	DeleteDatasetFromExternalApplication	
Deleted Power BI semantic model rows	DeleteDatasetRows	Indicates that the Push Datasets - Datasets DeleteRows API was called
Deleted Power BI semantic model	DeleteDataset	
Deleted Power BI template app or a workspace for a template app	DeleteTemplateApp	
Deleted a SQL query from a SQL analytics endpoint	DeleteSqlQueryFromSqlAnalyticsEndpointLakehouse	This audit event covers both deleting SQL and visual queries from the SQL analytics endpoint of the Lakehouse
Deleted SQL query from a Warehouse	DeleteSqlQueryFromWarehouse	Covers both deleting SQL and visual queries from the Warehous
Deleted an organizational custom visual	DeleteOrganizationalGalleryItem	
Deleted current value connection of Power BI metric	DeleteGoalCurrentValueConnection	
Deleted deployment pipeline	DeleteAlmPipeline	
Deleted link to external resource	DeleteLinkToExternalResource	
Deleted member of Power BI gateway cluster	DeleteGatewayClusterMember	
Deleted organizational Power BI content pack	DeleteOrgApp	
Deleted sensitivity label from Power BI item	SensitivityLabelRemoved	

Friendly name	Operation name	Notes
Deleted snapshot for user in Power BI tenant	DeleteSnapshot	Generated when a user deletes a snapshot that describes a semantic model
Deploy Model Version	DeployModelVersion	
Deploy user application in FunctionSet	DeployUserAppFunctionSet	Deploy user application through FunctionSet artifact
Deployed to a pipeline stage	DeployAlmPipeline	
Detect Customizations For Solution	DetectCustomizationsForSolution	
Determine if the user can share a datasource	DeterminePrincipalCanShareDatasource	Get the policy decision for the user to share a datasource
Disconnect From Git	DisconnectFromGit	Disconnect From Git is a workspace activity, which is generated when users disconnect the workspace from Git.
Discovered Power BI semantic model data sources	GetDatasources	
Downgrade Workspace	DowngradeWorkspace	
Download Environment Resource	DownloadEnvironmentResource	Download resources in environment
Download Notebook Resource	DownloadNotebookResource	Delete resources in notebook.
Download Spark App Log	DownloadSparkAppLog	
Downloaded Power BI report	DownloadReport	
Downloaded Exported Power BI artifact file	ExportArtifactDownload	An export of the .pptx or .pdf file is complete
Drop Lakehouse File	DropLakehouseFile	
Drop Lakehouse Folder	DropLakehouseFolder	
Drop Lakehouse Table	DropLakehouseTable	
Edit Artifact Endorsement	EditArtifactEndorsement	
Edit Report Description	EditReportDescription	
Edit Sql Analytics Endpoint Lakehouse Endorsement	EditSqlAnalyticsEndpointLakehouseEndorsement	Edited a lakehouse SQL analytics endpoint endorsement
Edit Tile	EditTile	Edit Tile is a dashboard activity, which is generated on changes or edits to settings for tiles in a Power BI Dashboard
Edit Warehouse Endorsement	EditWarehouseEndorsement	
Edit Widget Tile	EditWidgetTile	
Edit mounted warehouse endorsements	EditMountedWarehouseEndorsement	Generated when mounted warehouse endorsements are edited
Edited Power BI app endorsement	EditContentProviderProperties	
Edited Power BI certification permission	EditCertificationPermission	Not currently used
Edited Power BI dashboard	EditDashboard	Not currently used
Edited Power BI dataflow endorsement	EditDataflowProperties	
Edited Power BI report endorsement	EditReportProperties	

Friendly name	Operation name	Notes
Edited Power BI report	EditReport	
Edited Power BI semantic model endorsement	EditDatamartEndorsement	
Edited Power BI semantic model from external app	EditDatasetFromExternalApplication	
Edited Power BI semantic model properties	EditDatasetProperties	
Edited Power BI semantic model	EditDataset	
Enable/Disable AllowedInUntrustedContexts settings	AllowedInUntrustedContextsViaApi	Enable or disable AllowedInUntrustedContexts settings
Encrypted credentials for Power BI gateway datasource	EncryptCredentials	
Encrypted credentials using Power BI gateway cluster	EncryptClusterCredentials	
Evaluate Diagnostics Download	EvaluateDiagnosticsDownload	
Evaluate Diagnostics Query	EvaluateDiagnosticsQuery	
Evaluate chat response based on the data gateway diagnostics data	EvaluateDiagnosticsChat	Evaluate chat response based on the data gateway diagnostics data
Evaluate data sources against DMTS data policies	EvaluateDataSourcesAgainstTenantDlpPolicies	Evaluate data sources against DMTS data policies
Explore Dataset	ExploreDataset	
Export Package For Solution	ExportPackageForSolution	
Export Power BI activity events	ExportActivityEvents	
Export Scorecard	ExportScorecard	Exports a scorecard
Exported Power BI dataflow	ExportDataflow	
Exported Power BI item to another file format	ExportArtifact	
Exported Power BI report to another file format or exported report visual data	ExportReport	
Exported Power BI tile data	ExportTile	
Extract Template App Package	ExtractTemplateAppPackage	Extract Template App Package is an app activity, which is generated when users extract an existing Template App into another Power BI Template App Workspace
Fetch a shortcut's metadata	GetShortcut	OneLake operation. Part of Shortcut Controller
Finish Publish Environment	FinishPublishEnvironment	Finish publish environment
Flush data to file	FlushDataToFile	OneLake operation. Proxy calls
Follow Goal	FollowGoal	
Gateway Cluster S S O Test Connection	GatewayClusterSSOTestConnection	
Generate Custom Visual W A C Access Token	GenerateCustomVisualWACAccessToken	
Generate Multi Resource Embed Token	GenerateMultiResourceEmbedToken	

Friendly name	Operation name	Notes
Generate screenshot	GenerateScreenshot	
Generated Power BI Embed Token	GenerateEmbedToken	
Generated Power BI dataflow SAS token	GenerateDataflowSasToken	
Get All Private Link Services For Tenant	GetAllPrivateLinkServicesForTenant	
Get All Scorecards	GetAllScorecards	
Get Alm Pipeline Users As Admin	GetAlmPipelineUsersAsAdmin	
Get Alm Pipelines As Admin	GetAlmPipelinesAsAdmin	
Get Artifact Access By User Id Via Admin Api	GetArtifactAccessByUserIdViaAdminApi	
Get Artifact Link Shared To Whole Org As Admin	GetArtifactLinkSharedToWholeOrgAsAdmin	
Get Artifact Users Via Admin Api	GetArtifactUsersViaAdminApi	
Get Artifacts By Id Via Admin Api	GetArtifactsByIdViaAdminApi	
Get Artifacts Via Admin Api	GetArtifactsViaAdminApi	
Get Batch Lakehouse Table Details	GetBatchLakehouseTableDetails	
Get Cloud Supported Datasources	GetCloudSupportedDatasources	
Get Dashboards In Group As Admin	GetDashboardsInGroupAsAdmin	
Get Dataflow Users As Admin	GetDataflowUsersAsAdmin	
Get Dataflows In Group As Admin	GetDataflowsInGroupAsAdmin	
Get Dataset Info	GetDatasetInfo	Get the info of the dataset
Get Dataset Query Scale-Out Sync Status	GetDatasetQueryScaleOutSyncStatus	Get Dataset Query Scale-Out Sync Status is a dataset activity, which is generated when users request the sync status of a scale out-enabled Power BI dataset.
Get Dataset Users As Admin	GetDatasetUsersAsAdmin	
Get Datasets In Group As Admin	GetDatasetsInGroupAsAdmin	
Get Datasource Details With Credentials Async	GetDatasourceDetailsWithCredentialsAsync	
Get Dax Capabilities	GetDaxCapabilities	
Get Default Scorecard View	GetDefaultScorecardView	
Get Domain Delegation settings	DeleteDomainTenantSettingDelegation	Delete Domain Delegation settings.
Get Fabric Identity Token for Workspace	GetWorkspaceIdentityTokenViaApi	Get a Fabric identity token for a workspace
Get Fabric Identity for Workspace	GetWorkspaceIdentityViaApi	Get a Fabric identity for a workspace
Get Followed Goals	GetFollowedGoals	
Get Gateway Cluster	GetGatewayCluster	

Friendly name	Operation name	Notes
Get Gateway Clusters With Role Options	GetGatewayClustersWithRoleOptions	
Get Gateway Container I P Configuration	GetGatewayContainerIPConfiguration	
Get Gateway Container N S Lookup Details	GetGatewayContainerNSLookupDetails	
Get Gateway Container Test Net Connection Details	GetGatewayContainerTestNetConnectionDetails	
Get Gateway datasource limit status	GetGatewayDatasourceLimitStatus	Gets the datasource limit status of the gateway or tenant cloud gateway
Get Goal By Hierarchy Item Ids	GetGoalByHierarchyItemIds	
Get Goal Status Rules	GetGoalStatusRules	
Get Goal Value Categories	GetGoalValueCategories	
Get Groups As Admin	GetGroupsAsAdmin	Get Groups as Admin is a workspace activity, which is generated on retrieving list of Power BI workspaces using an API call.
Get Hierarchy Goal Values	GetHierarchyGoalValues	
Get Lakehouse Table Details	GetLakehouseTableDetails	
Get MetricSet Metric Endpoint	GetMetricSetMetric	Read metric in a metricset endpoint
Get Model Diagram Layouts	GetPowerBIDataModelDiagramLayouts	Get diagram layouts when open data model in web model view.
Get Model SAS Token via Lockbox	GetModelSASTokenViaLockbox	Gets the SAS Token for a given model in a tenant via Lockbox
Get My Goals	GetMyGoals	
Get Pending Change Status	GetPendingChangeStatus	
Get Power BI group users	GetGroupUsers	
Get Publish To Web Artifacts As Admin	GetPublishToWebArtifactsAsAdmin	
Get Relevant Measures	GetRelevantMeasures	
Get Reports As Admin	GetReportsAsAdmin	
Get Reports In Group As Admin	GetReportsInGroupAsAdmin	Get Reports in Group as Admin is a workspace activity, which is generated on retrieving the reports present inside a Power BI workspace using an API call.
Get Roles For Scorecard	GetRolesForScorecard	Gets the roles for a scorecard
Get Scorecard Additional Properties	GetScorecardAdditionalProperties	Gets the additional properties on a scorecard
Get Scorecard By Hierarchy Item Ids	GetScorecardByHierarchyItemIds	
Get Scorecard Hierarchies	GetScorecardHierarchies	
Get Scorecard Hierarchy Items	GetScorecardHierarchyItems	
Get Scorecard Hierarchy	GetScorecardHierarchy	
Get Scorecard View	GetScorecardView	
Get Scorecard Views	GetScorecardViews	
Get Scorecards As Admin	GetScorecardsAsAdmin	Get all the scorecards as an admin
Get Semantic Metric Endpoint	GetSemanticMetric	Read standalone semantic metric endpoint

Friendly name	Operation name	Notes
Get Service Principal Profile	GetServicePrincipalProfile	
Get Service Principal Profiles As Admin	GetServicePrincipalProfilesAsAdmin	
Get Service Principal Profiles	GetServicePrincipalProfiles	
Get Subscription Users By Dashboard Id As Admin	GetSubscriptionUsersByDashboardIdAsAdmin	
Get Subscription Users By Report Id As Admin	GetSubscriptionUsersByReportIdAsAdmin	
Get Subscriptions For User As Admin	GetSubscriptionsForUserAsAdmin	
Get Tenant Settings Via Admin Api	GetTenantSettingsViaAdminApi	
Get USEC roles for an artifact	GetArtifactRoles	OneLake operation.
Get Unused Artifacts	GetUnusedArtifacts	
Get User Datasource Limit Status	GetUserDatasourceLimitStatus	
Get User Datasources By Data Source Reference	GetUserDatasourcesByDataSourceReference	
Get Virtual Network	GetVirtualNetwork	
Get Workspace Users Via Admin Api	GetWorkspaceUsersViaAdminApi	
Get Workspaces By Id Via Admin Api	GetWorkspacesByIdViaAdminApi	
Get Workspaces Via Admin Api	GetWorkspacesViaAdminApi	
Get a task flow	GetTaskFlow	
Get access control list for file	GetAccessControlListForFile	OneLake operation. Returns the permissions list for a file.
Get all connections	GetAllConnections	Get all connections
Get all metric sets Endpoint	GetAllMetricSets	Get all metric sets endpoint
Get blob metadata	GetBlobMetadata	OneLake operation. Retrieves all user-defined metadata of an existing file or folder.
Get blob	GetBlob	OneLake operation. Reads or downloads a blob from OneLake, including its user-defined metadata and system properties.
Get block list	GetBlockList	OneLake operation. Retrieves the list of blocks that have been uploaded as part of a block blob.
Get data artifact table details	GetDataArtifactTableDetails	Get the details (for example, schema) for a data item table
Get datasource share policy	GetDatasourceShareTenantPolicy	Retrieve the datasource share policy set by the tenant
Get delegated capacity tenant setting overrides	GetCapacityDelegatedTenantSettingOverridesViaAdminApi	Get capacity delegated tenant setting overrides
Get delegated domain tenant setting overrides	GetDomainDelegatedTenantSettingOverridesViaAdminApi	Get domain delegated tenant setting overrides
Get delegated workspace tenant setting overrides	GetWorkspaceDelegatedTenantSettingOverridesViaAdminApi	Get workspace delegated tenant setting overrides
Get file or blob properties	GetFileOrBlobProperties	OneLake operation. Returns all system properties and user-defined metadata on the file or folder..
Get list of users part of the	GetDatasourceSharePrincipalsPolicy	Retrieve the datasource share principals that are part of policy

Friendly name	Operation name	Notes
datasource share policy		set by the tenant
Get path status	GetPathStatus	OneLake operation. Returns all system defined properties for a path.
Get properties	GetProperties	OneLake operation. Returns all system and user defined properties for a path
Get query text from secured telemetry store via Lockbox	GetQueryTextTelemetryViaLockbox	Retrieved query text from secured telemetry store via Azure Lockbox
Get refresh history via lockbox	GetRefreshHistoryViaLockbox	
Get single connection by ID	GetConnection	Get single connection by ID
Get the Details of a Moniker	DiscoverSystemDetailsOfMoniker	Get Moniker and related Data Sources information
Get the current set of DLP policies applied on the Tenant	GetTenantDlpPolicies	Get the current set of DLP policies applied on the Tenant
Get virtual network data gateway proxy	GetVirtualNetworkDataGatewayProxy	Get HTTP proxy info for virtual network data gateway
Goals Create Role	GoalsCreateRole	
Goals Delete Role	GoalsDeleteRole	
Goals Get Role	GoalsGetRole	
Goals Update Role	GoalsUpdateRole	
Import Package For Solution	ImportPackageForSolution	
Import file to Power BI ended	ImportArtifactEnd	Generated when importing Power BI Desktop files (.pbix). ImportSource indicates Power BI or OneDriveSharePoint. ImportType tells you if the file is new (Publish) or is being updated (Republish).
Import file to Power BI started	ImportArtifactStart	Generated when importing Power BI Desktop files (.pbix). When ImportSource is PowerBI, the file import originated from a Powe BI client or API. When ImportSource is OneDriveSharePoint, the file import originated from OneDrive or a SharePoint document library.
Imported file to Power BI	Import	
Initiate Cloud O Auth Login	InitiateCloudOAuthLogin	
Initiated Power BI gateway cluster authentication process	InitiateGatewayClusterOAuthLogin	
Insert Domain	InsertDataDomainAsAdmin	Insert Domain
Inserted Power BI note	InsertNote	
Inserted or updated current value connection of Power BI metric	UpsertGoalCurrentValueConnection	
Inserted or updated target value connection of Power BI metric	UpsertGoalTargetValueConnection	
Inserted snapshot for user in Power BI tenant	InsertSnapshot	Generated when user uploads a snapshot that describes their semantic model
Install Teams Analytics Report	InstallTeamsAnalyticsReport	
Installed Power BI app	InstallApp	
Installed Power BI template app	InstallTemplateApp	

Friendly name	Operation name	Notes
Instantiate App	InstantiateApp	
Lease blob	LeaseBlob	OneLake operation. Establishes and manages a lock on write an delete operations.
Lease container	LeaseContainer	OneLake operation. Establishes and manages a lock on write an delete operations.
Lease path	LeasePath	OneLake operation. Establishes and manages a lock on write an delete operations.
List Lakehouse Tables	ListLakehouseTables	
List blobs	ListBlob	OneLake operation. List all blobs in a workspace
List data access roles	ListDataAccessRoles	Returns a list of data access roles
List file paths	ListFilePath	OneLake operation. Lists all files in a path.
Load Lakehouse Table	LoadLakehouseTable	
Load Spark App Log	LoadSparkAppLog	
Manage Relationships	ManageRelationships	
Map Upn	MapUpn	
Migrated dataflow storage location	MigratedDataflowStorageLocation	Not currently used
Migrated workspace to a capacity	MigrateWorkspaceIntoCapacity	
Modify Workspace Capacity	ModifyWorkspaceCapacity	Modify Workspace Capacity is a capacity activity, which is generated on assigning a Power BI workspace to a capacity usin an API call or the UI.
Move Goals	MoveGoals	Moves goals within a scorecard
Move Scorecard	MoveScorecard	
Move items into subfolder	MoveItemsIntoSubfolder	
No Activity	NoActivity	
Opt In For P P U Trial	OptInForPPUTrial	
Override Sjd Spark Settings	OverrideSjdSparkSettings	
Patch Gateway Cluster	PatchGatewayCluster	
Patch Goal Value Categories	PatchGoalValueCategories	
Patch file system	PatchFileSystem	OneLake operation. Sets properties for a workspace.
Patched Power BI metric value	PatchGoalValue	
Patched Power BI metric	PatchGoal	
Patched Power BI note	PatchNote	
Patched Power BI scorecard	PatchScorecard	
Permanently delete Workspaces	DeleteWorkspacesPermanentlyAsAdmin	Generated when workspaces are permanently deleted by an admin
Pin Report Get Channels In Team	PinReportGetChannelsInTeam	
Pin Report Get User Joined Teams	PinReportGetUserJoinedTeams	
Pin Report To Teams Channel	PinReportToTeamsChannel	
Pin Tile	PinTile	

Friendly name	Operation name	Notes
Pin Widget Tile	PinWidgetTile	
Post Dataset Rows	PostDatasetRows	
Post Notebook Comment	PostNotebookComment	
Post configure credentials	PostGitProviderCredentials	Configure git provider credentials for a specific user
Posted Power BI comment	PostComment	
Preview Lakehouse Table	PreviewLakehouseTable	
Printed Power BI Dashboard	PrintDashboard	
Printed Power BI report page	PrintReport	
Promoted Power BI template app	PromoteTemplateAppPackage	
Provision Scorecard	ProvisionScorecard	
Publish/Unpublish a workload	ExtensibilityUpdatePublishingState	Publish or unpublish a workload, making it available or unavailable in Workloads Hub
PublishDataflow	PublishDataflow	Publish Dataflow
Published Power BI report to web	PublishToWebReport	
Put Table	PutTable	
Query blob contents	QueryBlobContents	OneLake operation. Applies a SQL statement on a blob's contents, only returning the specified subset.
Ran Power BI email subscription	RunEmailSubscription	
Re-encrypted credentials using Power gateway cluster	ReencryptCredentials	
Read Artifact	ReadArtifact	
Read Environment Resource	ReadEnvironmentResource	Read resources in environment
Read Experiment Run	ReadExperimentRun	
Read file or get blob	ReadFileOrGetBlob	OneLake operation. Reads a file in OneLake.
ReadDataflow	ReadDataflow	Read Dataflow
Rebind Report	RebindReport	
Received Power BI dataflow secret from Key Vault	ReceiveDataflowSecretFromKeyVault	
Refresh Datamart	RefreshDatamart	
Refresh Goal Current Value Rollup	RefreshGoalCurrentValueRollup	
Refresh Goal Target Value Rollup	RefreshGoalTargetValueRollup	
Refresh Lakehouse Data	RefreshLakehouseData	
Refresh Sql Analytics Endpoint Lakehouse Metadata	RefreshSqlAnalyticsEndpointLakehouseMetadata	Refreshed metadata for a lakehouse SQL analytics endpoint. Previously named *Refreshed metadata for a default warehouse* (Operation name: *RefreshDefaultWarehouseMetadata*)
Refresh mounted warehouse metadata	RefreshMountedWarehouseMetadata	Generated when mounted warehouse metadata is refreshed
Refreshed current value of Power BI metric	RefreshGoalCurrentValue	
Refreshed target value of Power BI metric	RefreshGoalTargetValue	

Friendly name	Operation name	Notes
Register workload development instance	ExtensibilityRegisterDevInstance	Register a development instance of a workload
Remove Admin Personal Workspace Access	RemoveAdminPersonalWorkspaceAccess	
Remove workload	ExtensibilityDeactivation	Remove a workload from a tenant or capacity
Removed Power BI group members	DeleteGroupMembers	
Removed a workspace from a deployment pipeline	UnassignWorkspaceFromPipeline	Not currently used
Removed data source from Power BI gateway	RemoveDatasourceFromGateway	
Removed user from Power BI gateway cluster datasource	RemoveGatewayClusterDatasourceUser	
Removed user from Power BI gateway cluster	RemoveGatewayClusterUser	
Removed workspace from a capacity	RemoveWorkspacesFromCapacity	
Rename Datamart	RenameDatamart	
Rename Lakehouse File	RenameLakehouseFile	
Rename Lakehouse Folder	RenameLakehouseFolder	
Rename Lakehouse Table	RenameLakehouseTable	
Rename Report	RenameReport	Rename Report is a report activity, which is generated on renaming the name of a Power BI Report through its settings
Rename Warehouse	RenameWarehouse	
Rename file or directory	RenameFileOrDirectory	OneLake operation. Renames a file or directory in OneLake.
Renamed Power BI dashboard	RenameDashboard	
Request Cognitive Service	RequestCognitiveService	Request Cognitive Service in ML workload.
Request Copilot features in Fabric	RequestCopilot	Request Copilot features in Fabric
Request OpenAI by Spark code in Fabric	RequestSparkCodeFirst	Request OpenAI by Spark code in Fabric
Request OpenAI model	RequestOpenAI	Request OpenAI models in ML workload.
Requested Power BI dataflow refresh	RequestDataflowRefresh	A dataflow refresh starts. The refresh can be scheduled or triggered manually from the portal or an API.
Requested Power BI semantic model refresh from external app	RefreshDatasetFromExternalApplication	
Requested Power BI semantic model refresh	RefreshDataset	
Requested SAS token for Power BI storage	AcquireStorageSASFromExternalApplication	
Requested account key for Power BI storage	AcquireStorageAccountKey	
Restore container	RestoreContainer	OneLake operation.
Restore deleted workspace	RestoreWorkspaceViaAdminApi	Restores the deleted workspace
Restored Power BI workspace	RestoreWorkspace	

Friendly name	Operation name	Notes
Resume Suspended Datamart	ResumeSuspendedDatamart	
Resume Suspended Sql Analytics Endpoint Lakehouse	ResumeSuspendedSqlAnalyticsEndpointLakehouse	Resumed a suspended lakehouse SQL analytics endpoint. Previously named *Resumed a suspended default warehouse* (Operation name: *ResumeSuspendedDefaultWarehouse*)
Resume Suspended Warehouse	ResumeSuspendedWarehouse	
Resume suspended mounted warehouse	ResumeSuspendedMountedWarehouse	Generated when a suspended mounted warehouse is resumed
Retrieved Power BI app users	GetAppUsersAsAdmin	
Retrieved Power BI apps for user	GetUserAppsAsAdmin	Not currently used
Retrieved Power BI apps	GetAppsAsAdmin	
Retrieved Power BI capacities for user	GetUserCapacitiesAsAdmin	Not currently used
Retrieved Power BI capacity users	GetCapacityUsersAsAdmin	
Retrieved Power BI dashboard tiles	GetDashboardTilesAsAdmin	
Retrieved Power BI dashboard users	GetDashboardUsersAsAdmin	
Retrieved Power BI dashboards for user	GetUserDashboardsAsAdmin	Not currently used
Retrieved Power BI dashboards	GetDashboardsAsAdmin	
Retrieved Power BI data sources for user	GetUserDatasourcesAsAdmin	Not currently used
Retrieved Power BI dataflows for user	GetUserDataflowsAsAdmin	Not currently used
Retrieved Power BI dataflows	GetDataflowsAsAdmin	
Retrieved Power BI gateway cluster datasource	GetGatewayClusterDatasource	
Retrieved Power BI gateway cluster datasources	GetGatewayClusterDatasources	
Retrieved Power BI gateway datasource users	GetDatasourceUsersAsAdmin	Not currently used
Retrieved Power BI gateway tenant key	GetGatewayTenantKeys	
Retrieved Power BI gateway tenant policy	GetGatewayTenantPolicy	
Retrieved Power BI gateway users	GetGatewayUsersAsAdmin	Not currently used
Retrieved Power BI gateways for user	GetUserGatewaysAsAdmin	Not currently used
Retrieved Power BI group users	GetGroupUsersAsAdmin	
Retrieved Power BI groups for user	GetUserGroupsAsAdmin	Not currently used
Retrieved Power BI imports	GetImportsAsAdmin	

Friendly name	Operation name	Notes
Retrieved Power BI metric value	GetGoalValue	
Retrieved Power BI metric	GetGoal	
Retrieved Power BI refresh history	GetRefreshHistory	
Retrieved Power BI refreshable by ID	GetRefreshablesForRefreshIdAsAdmin	
Retrieved Power BI refreshables for capacity	GetRefreshablesForCapacityAsAdmin	
Retrieved Power BI refreshables	GetRefreshablesAsAdmin	
Retrieved Power BI report users	GetReportUsersAsAdmin	
Retrieved Power BI reports for user	GetUserReportsAsAdmin	Not currently used
Retrieved Power BI scorecard by using report ID	GetScorecardByReportId	
Retrieved Power BI scorecard	GetScorecard	
Retrieved Power BI semantic models for user	GetUserDatasetsAsAdmin	Not currently used
Retrieved Power BI semantic models	GetDatasetsAsAdmin	
Retrieved Power BI tenant keys	GetTenantKeysAsAdmin	
Retrieved Power BI workspaces	GetWorkspaces	
Retrieved a model from Power BI	GetPowerBIDataModel	A user opens the Open data model experience or resyncs a data model.
Retrieved all Power BI gateway cluster datasources	GetAllGatewayClusterDatasources	
Retrieved all supported datasources for Power BI gateway cluster	GetGatewayClusterSupportedDatasources	
Retrieved allowed Power BI gateway regions	GetGatewayRegions	
Retrieved authentication details for Power BI gateway cluster datasource	GetGatewayClusterDatasourceOAuthDetails	
Retrieved data sources from Power BI dataflow	GetDataflowDatasourcesAsAdmin	
Retrieved data sources from Power BI semantic model	GetDatasetDatasourcesAsAdmin	
Retrieved links between semantic models and dataflows	GetDatasetToDataflowsLinksAsAdmin	
Retrieved list of Power BI gateway installer principals	GetGatewayInstallerPrincipals	
Retrieved list of datasource users for Power BI gateway cluster	GetGatewayClusterDatasourceUsers	
Retrieved list of modified workspaces in Power BI	GetModifiedWorkspacesAPI	

Friendly name	Operation name	Notes
tenant		
Retrieved member status of Power BI gateway cluster	GetGatewayClusterMemberStatus	
Retrieved metrics of Power BI scorecard	GetGoalsForScorecard	
Retrieved multiple Power BI gateway clusters	GetGatewayClusters	
Retrieved multiple Power BI metric values	GetGoalValues	
Retrieved multiple Power BI scorecards	GetScorecards	
Retrieved scan result in Power BI tenant	GetWorkspacesInfoResult	
Retrieved snapshots for user in Power BI tenant	GetSnapshots	Generated when user retrieves snapshots that describe a semantic model such as when a user visits the data hub
Retrieved status of Power BI gateway cluster datasource	GetGatewayClusterDatasourceStatus	
Retrieved status of Power BI gateway cluster	GetGatewayClusterStatus	
Retrieved upstream dataflows from Power BI dataflow	GetDataflowUpstreamDataflowsAsAdmin	
Retry lakehouse SQL analytics endpoint creation for a Lakehouse	RetryLakehouseSqlEndpointCreation	Retry SQL endpoint creation for a Lakehouse
Revoke an external data share	RevokeExternalDataShare	Revoke an external data share
Rotate Tenant Key	RotateTenantKey	
Rotated Power BI gateway tenant key	RotateTenantKeyEncryptionKey	
Run Artifact	RunArtifact	
Save Model Diagram Layouts	SavePowerBIDataModelDiagramLayouts	Save diagram layouts after update data model in web model view.
Saved an autogenerated report to Power BI	SaveAutogeneratedReport	After exploring an autogenerated Power BI report in an external application, a user saved it to the Power BI service.
Saved an autogenerated semantic model to Power BI	SaveAutogeneratedDataset	After exploring an autogenerated Power BI semantic model in a external application, a user saved it to the Power BI service.
Schedule Artifact	ScheduleArtifact	
Sent a scan request in Power BI tenant	GetWorkspacesInfoAPI	
Set Capacity Tenant Key	SetCapacityTenantKey	
Set D Q Refresh Schedule Of Dataset	SetDQRefreshScheduleOfDataset	
Set DirectQuery Refresh Schedule Of Dateset	SetDQRefreshScheduleOfDateset	
Set Lakehouse Endorsement	SetLakehouseEndorsement	
Set Lakehouse Sensitivity Label	SetLakehouseSensitivityLabel	
Set Model Refresh Schedule Of Dateset	SetModelRefreshScheduleOfDateset	

Friendly name	Operation name	Notes
Set Model Refresh Schedule Of Dataset	SetModelRefreshScheduleOfDataset	
Set Notebook Default Lakehouse	SetNotebookDefaultLakehouse	Set default lakehouse for notebook.
Set Sjd Retry Policy	SetSjdRetryPolicy	
Set access control for file	SetAccessControlForFile	OneLake operation. Sets permissions for a file.
Set blob expiry	SetBlobExpiry	OneLake operation. Set the expiration time for a blob.
Set blob metadata	SetBlobMetadata	OneLake operation. Set user-defined metadata for a blob.
Set blob properties	SetBlobProperties	OneLake operation. Set system properties for a blob.
Set blob tier	SetBlobTier	OneLake operation. Sets the tier of a blob.
Set container ACL	SetContainerAcl	OneLake operation. Sets permissions for a workspace.
Set container metadata	SetContainerMetadata	OneLake operation. Sets user-defined metadata for a workspace
Set dataflow storage location for a workspace	SetDataflowStorageLocationForWorkspace	
Set file properties	SetFileProperties	OneLake operation. Set user-defined properties for a file.
Set scheduled refresh on Power BI dataflow	SetScheduledRefreshOnDataflow	
Set scheduled refresh on Power BI semantic model	SetScheduledRefresh	
Share Artifact	ShareArtifact	
Share Datamart	ShareDatamart	
Share Lakehouse Table	ShareLakehouseTable	
Share Warehouse	ShareWarehouse	
Shared Power BI dashboard	ShareDashboard	
Shared Power BI report	ShareReport	
Shared Power BI semantic model	ShareDataset	
Start Notebook Session	StartNotebookSession	
Start Publish Environment	StartPublishEnvironment	Start publish environment
Started Power BI extended trial	OptInForExtendedProTrial	Not currently used
Started Power BI trial	OptInForProTrial	
Stop Notebook Session	StopNotebookSession	
Switch Branch Git	SwitchBranchInGit	Switch Branch Git is a workspace activity, which is generated when the user changes what git branch is connected to the workspace.
Sync Dataset Query Scale-Out Replicas	SyncDatasetQueryScaleOutReplicas	Sync Dataset Query Scale-Out Replicas is a dataset activity, whic is generated when users request a synchronization of the read replicas of a scale out-enabled Power BI dataset with its read/write replica.
Take Over Email Subscription	TakeOverEmailSubscription	
Tested Power BI gateway datasource connection with single sign-on	GatewayClusterDatasourceSSOTestConnection	
Took over Power BI semantic model	TakeOverDataset	

Friendly name	Operation name	Notes
Took over a Power BI datasource	TakeOverDatasource	
Took ownership of Power BI dataflow	TookOverDataflow	
Take over a Fabric item	TakeOverArtifact	
Trial License Extension	TrialLicenseExtension	Extend user trials by user list or tenant
Unassign Workspace From Alm Pipeline	UnassignWorkspaceFromAlmPipeline	
Undelete blob	UndeleteBlob	OneLake operation. Restore a soft deleted blob.
Undo Git	UndoGit	Undo Git is an artifact activity, which is generated when users undo changes done to artifact.
Unfollow Goal	UnfollowGoal	
Unpublished Power BI app	UnpublishApp	
Update Alm Pipeline Access As Admin	UpdateAlmPipelineAccessAsAdmin	
Update Alm Pipeline	UpdateAlmPipeline	
Update Artifact	UpdateArtifact	
Update Byo Resource Access	UpdateByoResourceAccess	
Update Capacity Delegation settings	UpdateCapacityTenantSettingDelegation	Update Capacity delegation settings.
Update Data Sharing	UpdateDataSharing	Update an existing external data share
Update Datamart Metadata	UpdateDatamartMetadata	
Update Datamart Settings	UpdateDatamartSettings	
Update Datamart	UpdateDatamart	
Update Dataset Parameters	UpdateDatasetParametersForSolution	Update Dataset Parameters is a dataset activity, which is generated when updates are made to a Power BI Dataset parameters
Update Dataset	UpdateDataset	Update Dataset is a dataset activity, which is generated when users updated the properties of a Power BI dataset.
Update Default Domain	UpdateDefaultDataDomainAsAdmin	Update Default Domain
Update Default Personal Workspace Capacity	UpdateDefaultPersonalWorkspaceCapacity	
Update Domain Access Permissions	UpdateDataDomainAccessAsAdmin	Update Data Domain Access Permissions
Update Domain Branding	UpdateDataDomainBrandingAsAdmin	Update Domain Branding
Update Domain Contributors Scope	UpdateDataDomainContributorsScopeAsAdmin	Update Domain Contributors Scope
Update Domain Delegation settings	UpdateDomainTenantSettingDelegation	Update Domain Delegation settings.
Update Domain	UpdateDataDomainAsAdmin	Update Domain
Update Domain's Folders Relations As Contributor	UpdateDataDomainFoldersRelationsAsContributor	Update Domain's Folders Relations As Contributor
Update Domain's Folders Relations	UpdateDataDomainFoldersRelationsAsAdmin	Update Domain's Folders Relations
Update Environment Resource	UpdateEnvironmentResource	Update resources in environment

Friendly name	Operation name	Notes
Update Environment Spark Settings	UpdateEnvironmentSparkSettings	Update environment spark settings
Update Experiment Run	UpdateExperimentRun	
Update Folder Access	UpdateFolderAccess	Indicates an update to workspace access settings
Update Folder	UpdateFolder	Indicates a workspace update
Update From Git	UpdateFromGit	Update From Git is an artifact activity, which is generated when users update artifact from Git.
Update Gateway Cluster Member	UpdateGatewayClusterMember	
Update Gateway Installer Principals	UpdateGatewayInstallerPrincipals	
Update Gateway Tenant Policy	UpdateGatewayTenantPolicy	
Update Goal Connection Settings	UpdateGoalConnectionSettings	
Update Goal Current Value Connection Owner	UpdateGoalCurrentValueConnectionOwner	
Update Goal Target Value Connection Owner	UpdateGoalTargetValueConnectionOwner	
Update Goals	UpdateGoals	
Update Group	UpdateGroup	
Update Hierarchy Goal Value	UpdateHierarchyGoalValue	
Update Hierarchy Note	UpdateHierarchyNote	
Update In Place Sharing Settings	UpdateInPlaceSharingSettings	
Update MetricSet Metric Endpoint	UpdateMetricSetMetric	Update metric in a metricset endpoint
Update Notebook Library	UpdateNotebookLibrary	
Update Notebook Resource	UpdateNotebookResource	Update resources in notebook.
Update Notebook Spark Property	UpdateNotebookSparkProperty	
Update Notification Settings	UpdateNotificationSettings	Update user notification settings for Notification Service Platform.
Update Report Content	UpdateReportContent	
Update Scorecard Dataset	UpdateScorecardDataset	
Update Scorecard Hierarchy	UpdateScorecardHierarchy	
Update Scorecard View	UpdateScorecardView	
Update Semantic Metric Endpoint	UpdateSemanticMetric	Update standalone semantic metric endpoint
Update Service Principal Profile	UpdateServicePrincipalProfile	
Update Sql Analytics Endpoint Lakehouse Settings	UpdateSqlAnalyticsEndpointLakehouseSettings	Updated settings for a lakehouse SQL analytics endpoint. Previously named *Updated a default warehouse* (Operation name: *UpdateDefaultWarehouse*)
Update Sql Analytics Endpoint Lakehouse	UpdateSqlAnalyticsEndpointLakehouse	Updated a lakehouse SQL analytics endpoint
Update USEC roles for an	UpdateArtifactRoles	OneLake operation.

Friendly name	Operation name	Notes
artifact		
Update Virtual Network	UpdateVirtualNetwork	
Update Warehouse Metadata	UpdateWarehouseMetadata	
Update Warehouse Settings	UpdateWarehouseSettings	
Update Warehouse	UpdateWarehouse	
Update Workspace Delegation settings	UpdateWorkspaceTenantSettingDelegation	Update Workspace Delegation settings.
Update capacity resource governance settings	UpdateCapacityResourceGovernanceSettings	Not currently in Microsoft 365 admin center
Update datasource share policy	UpdateDatasourceShareTenantPolicy	Set the datasource share policy set by the tenant
Update list of users part of the datasource share policy	UpdateDatasourceSharePrincipalsPolicy	Set the datasource share principals that are part of policy set by the tenant
Update mounted warehouse settings	UpdateMountedWarehouseSettings	Generated when mounted warehouse settings are updated
Update mounted warehouse	UpdateMountedWarehouse	Generated when mounted warehouse is updated
Update source in GraphQL artifact	UpdateSourceGraphQL	Update source in GraphQL artifact
Update subfolder	UpdateSubfolder	
Update task flow	UpdateTaskFlow	
Update the current set of DLP policies applied on the Tenant	UpdateTenantDlpPolicies	Update the current set of DLP policies applied on the Tenant
Update virtual network data gateway proxy	UpdateVirtualNetworkDataGatewayProxy	Update HTTP proxy for virtual network data gateway
Update workspace role	UpdateWorkspaceRoleViaAdminApi	Update workspace role
Updated Power BI access request settings	UpdateAccessRequestSettings	
Updated Power BI app	UpdateApp	
Updated Power BI dataflow	UpdateDataflow	
Updated Power BI discoverable model settings	UpdateDiscoverableModelSettings	Generated when a report is set to feature on home
Updated Power BI email subscription	UpdateEmailSubscription	
Updated Power BI gateway cluster datasource	UpdateGatewayClusterDatasource	
Updated Power BI gateway data source credentials	UpdateDatasourceCredentials	
Updated Power BI semantic model data sources	UpdateDatasources	
Updated Power BI semantic model parameters	UpdateDatasetParameters	
Updated Power BI workspace access	UpdateWorkspaceAccess	
Updated Power BI workspace	UpdateWorkspace	
Updated an organizational custom visual	UpdateOrganizationalGalleryItem	

Friendly name	Operation name	Notes
Updated capacity admin	UpdateCapacityAdmins	
Updated capacity custom settings	UpdateCapacityCustomSettings	
Updated capacity display name	UpdateCapacityDisplayName	
Updated credentials for Power BI gateway cluster	UpdateGatewayClusterDatasourceCredentials	
Updated dataflow storage assignment permissions	UpdatedDataflowStorageAssignmentPermissions	
Updated deployment pipeline access	UpdateAlmPipelineAccess	
Updated deployment pipeline configuration	SetConfigurationAlmPipeline	
Updated featured tables	UpdateFeaturedTables	
Updated organization's Power BI settings	UpdatedAdminFeatureSwitch	
Updated parameters for installed Power BI template app	UpdateInstalledTemplateAppParameters	
Updated settings for Power BI template app	UpdateTemplateAppSettings	
Updated snapshots for user in Power BI tenant	UpdateSnapshot	Generated when user updates snapshots that describe their semantic models
Updated testing permissions for Power BI template app	UpdateTemplateAppTestPackagePermissions	
Updated the Power BI datasource	UpdateDatasource	
Updated the Power BI gateway	UpdateGateway	
Updated workspace Analysis Services settings	SetASSeverPropertyOnWorkspaceFromExternalApplicationDetailedInfo	Not currently used
Upgrade Workspace	UpgradeWorkspace	
Upgrade Workspaces As Admin	UpgradeWorkspacesAsAdmin	
Upload workload package	ExtensibilityUploadPackage	Upload a workload package in a tenant
Upsert Datamart Parameters	UpsertDatamartParameters	
Upsert Goal Current Value Rollup	UpsertGoalCurrentValueRollup	
Upsert Goal Status Rules	UpsertGoalStatusRules	
Upsert Goal Target Value Rollup	UpsertGoalTargetValueRollup	
Upsert Goal Values	UpsertGoalValues	
Upsert Sql Analytics Endpoint Lakehouse Parameters	UpsertSqlAnalyticsEndpointLakehouseParameters	Upserted parameters for a lakehouse SQL analytics endpoint. Previously named *Updated parameters from a default warehouse* (Operation name: *UpsertDefaultWarehouseParameters*)
Upsert Warehouse Parameters	UpsertWarehouseParameters	
Upsert mounted warehouse parameters	UpsertMountedWarehouseParameters	Generated when mounted warehouse parameters are added or updated

Friendly name	Operation name	Notes
Used Power BI to explore data in an external application	ExploreDataExternally	Someone used Power BI to explore their data in an external application.
View Datamart	ViewDatamart	
View Spark App Input Output	ViewSparkAppInputOutput	
View Spark App Log	ViewSparkAppLog	
View Spark Application	ViewSparkApplication	
View Sql Analytics Endpoint Lakehouse	ViewSqlAnalyticsEndpointLakehouse	Viewed a lakehouse SQL analytics endpoint. Previously named *Viewed a default warehouse* (Operation name: *ViewDefaultWarehouse*)
View Warehouse	ViewWarehouse	
View mounted warehouse	ViewMountedWarehouse	Generated when mounted warehouse is fetched for viewing
Viewed Power BI dashboard	ViewDashboard	Some fields such as CapacityID and CapacityName, will return null if the report or dashboard is viewed from a Power BI app, rather than a Power BI workspace
Viewed Power BI dataflow	ViewDataflow	
Viewed Power BI metadata	ViewMetadata	
Viewed Power BI report	ViewReport	A report is also generated per page when exporting a report. Some fields such as CapacityID and CapacityName, will return null if the report or dashboard is viewed from a Power BI app, rather than a Power BI workspace.
Viewed Power BI tile	ViewTile	
Viewed Power BI usage metrics	ViewUsageMetrics	
disable workspace	DisableWorkspaceViaAdminApi	Disables the workspace

Considerations and limitations

When capacity ID and capacity name aren't available in the audit logs, you can view them in the Microsoft Fabric Capacity Metrics app.

Related content

Track user activities in Microsoft Fabric

Find users who signed in

10/09/2025

If you're an admin for your organization, you can use the Microsoft Entra admin center to view sign-in logs.

This guide shows you how to find sign-in logs specifically for Power BI. For more information about sign-in logs for other users and applications, see the Microsoft Entra sign-in logs documentation.

> **Note**
>
> The *Sign-in logs* report provides useful information, but it doesn't identify the type of license for each user. Use the Microsoft 365 admin center to view licenses.

Requirements

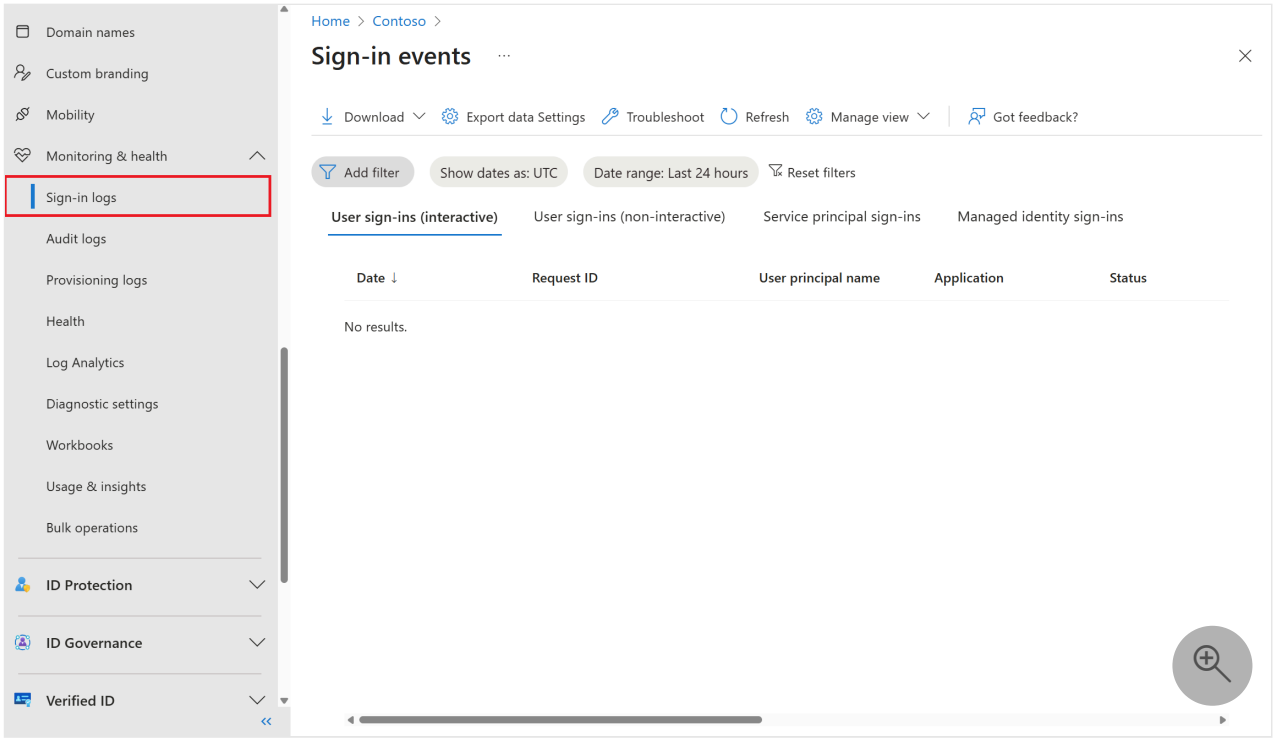
Any user can view a report of their own sign-ins. To see a report for all users, you must have a Fabric administrator role.

Use the Microsoft Entra admin center to view sign-ins

To view sign-in activity, follow these steps:

1. Sign in to the Microsoft Entra admin center, and then expand **Entra ID** from the left navigation pane.

2. From the left navigation pane under **Entra ID**, select **Monitoring & health** > **Sign-in logs**.

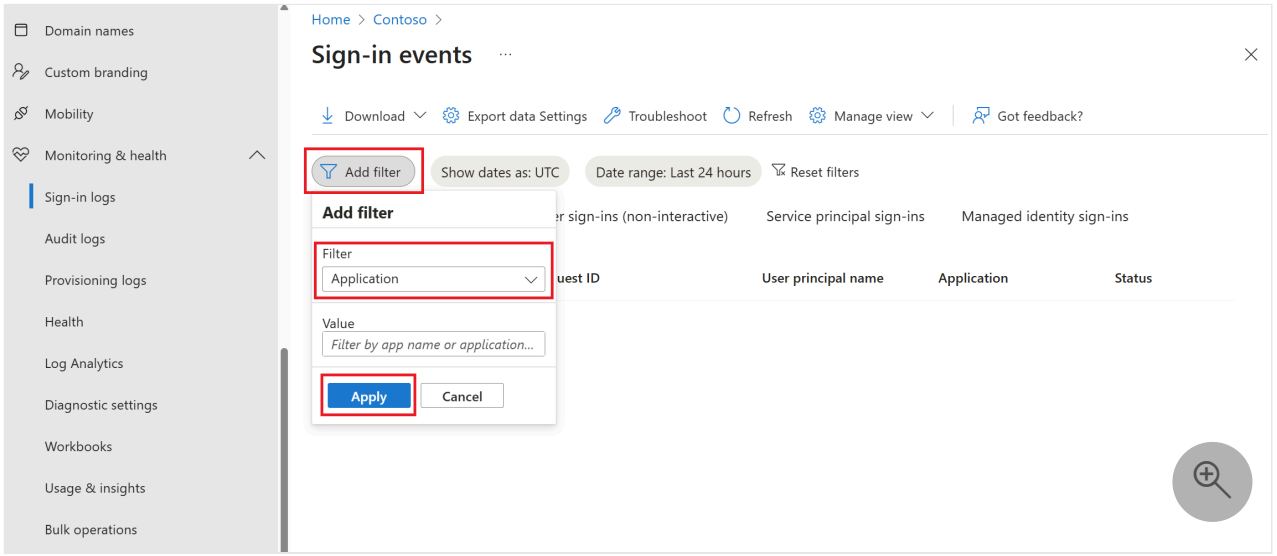


By default, all sign-ins from the last 24 hours for all users and all applications are shown.

3. To select a different time period, select **Date** in the working pane and choose from the available time intervals. For more information about available time intervals, see data retention.

4. To see only sign-ins to specific applications, add filters.

5. Select **Add filter** and then select **Application** as the field to filter by.



- To see only sign-in activity that's specific to Power BI service, enter **Microsoft Power BI**.

- To see only sign-in activity that's specific to the on-premises data gateway, enter **Power BI Gateway**.

6. Select **Apply**.

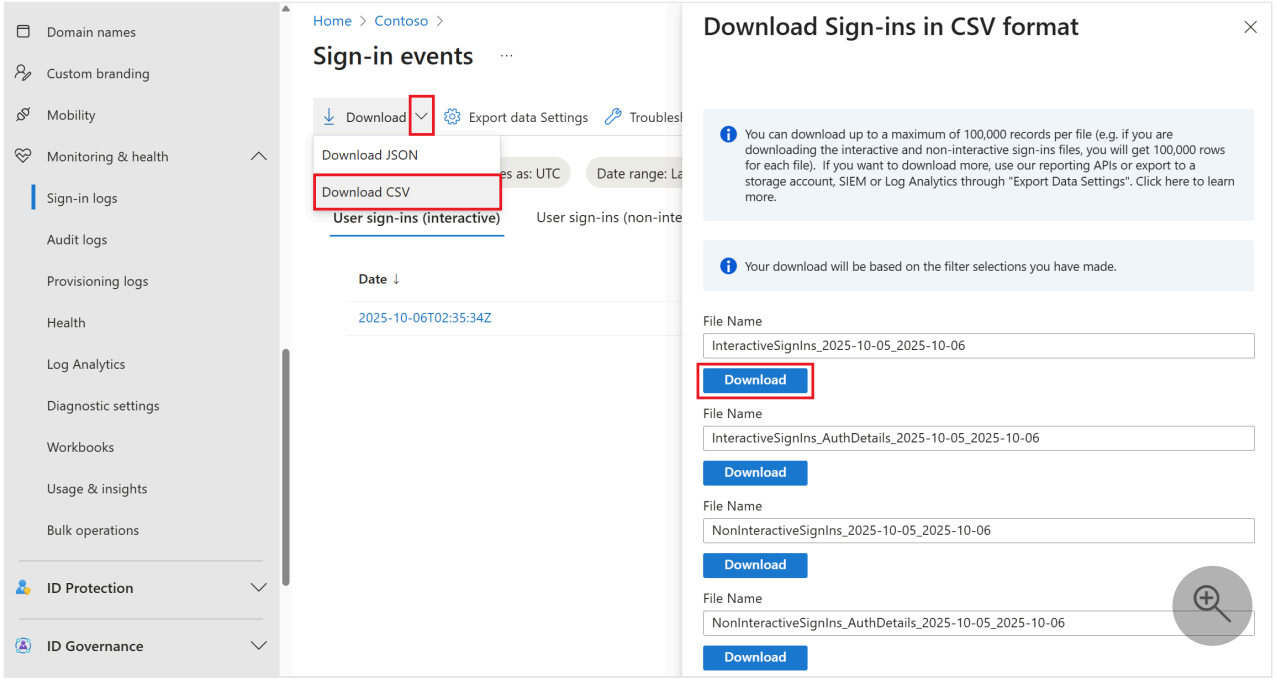
Export the data

You can download a sign-in report in either of two formats: a CSV file, or a JSON file. Use the following steps to download your report:

1. From the command bar for the **Sign-in events** page, select **Download** and then select one of the following options:

   - **Download JSON** to download a JSON file for the currently filtered data.
   - **Download CSV** to download a CSV file for the currently filtered data.

2. Decide what type of sign-ins you want to export, and then select **Download**.



> **Note**
>
> You can download up to a maximum of 100,000 records per file. For example, if you're downloading the interactive and non-interactive sign-ins files, you 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**.

Data retention

Sign-in-related data is available for up to seven days, unless your organization has a Microsoft Entra ID P1 or P2 license. If you use Microsoft Entra ID P1 or Microsoft Entra ID P2, you can see

data for the past 30 days. For more information, see How long does Microsoft Entra ID store reporting data?.

Related content

- Use the Monitoring hub
- Microsoft Entra sign-in logs

Add custom branding to the Power BI service

Article • 12/21/2023

As a Fabric admin, you can change the look and feel of the Power BI service to match your organization's own branding. With custom branding, you can change the theme color that appears in the top navigation bar, add your company logo, and bring your default landing page to life by adding a cover image.

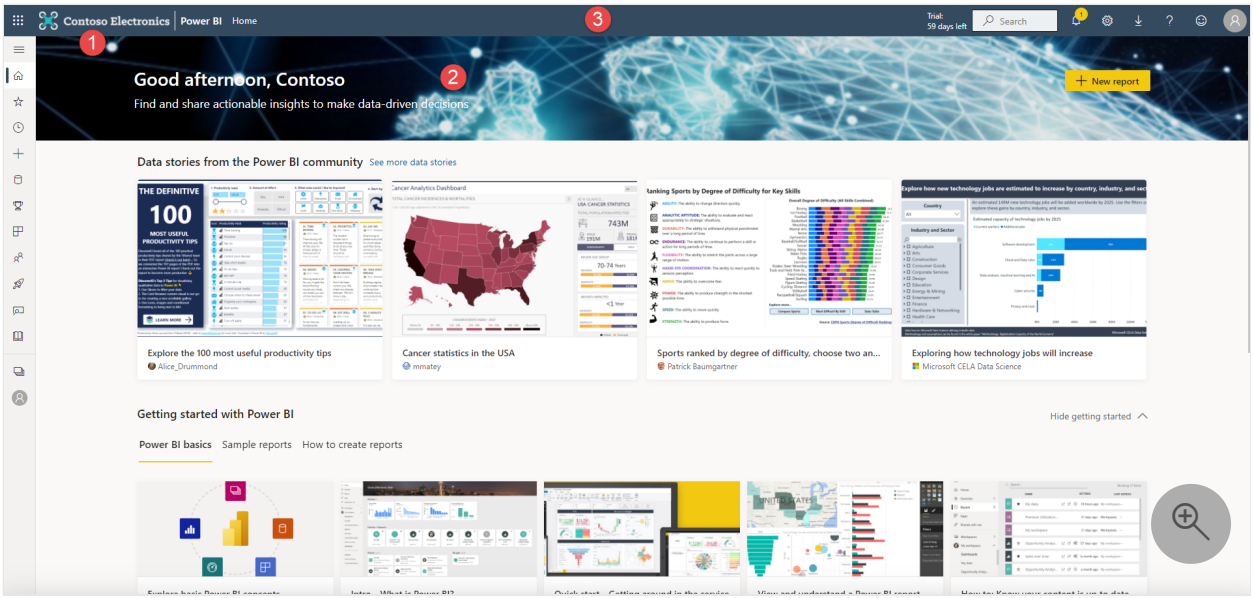
Custom branding changes the look of Power BI for your whole organization. Users can't override your custom branding with their own theme. Custom branding also appears to any external users who have access to your reports in B2B scenarios, helping to easily distinguish your organization.

Before you begin

- Make sure you're a Fabric administrator.
- Prepare your images for upload. You need these files:
  - A logo file that's saved in *.png* format, is 10 KB or smaller, and is at least 200 x 30 pixels. Choosing a PNG file makes sure your logo has a high-resolution appearance on all screens and at all zoom levels. The logo appears on every page.
  - A cover image that's saved in *.jpg* or *.png* format, is 1 MB or smaller, and is at least 1920 x 160 pixels. Get creative with your choice with an image that complements your theme color and feels welcoming. The cover image appears only at the top of Home.
- Identify the hex or decimal code for your theme color. Your theme color appears on every page and provides the background for your logo. Choose a color that complements your logo and cover image or that matches other custom branding in your organization.

The following image indicates where each of these elements appears in the Power BI service:

1. Logo
2. Cover image
3. Theme color

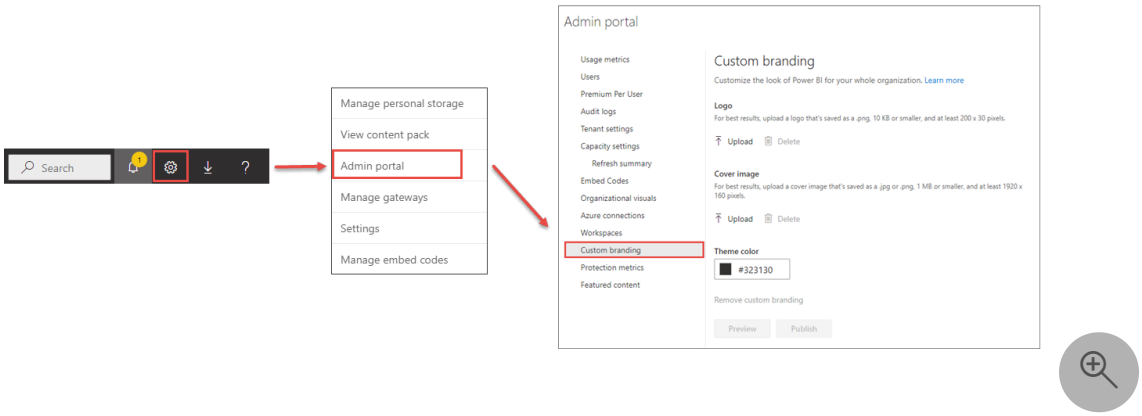


Add custom branding

Follow these steps to customize the look of Power BI for your whole organization:

1. Sign in to the Power BI service as a Fabric admin.

2. From the navigation bar, select **Settings** > **Admin portal** > **Custom branding**.



3. Upload a logo file.

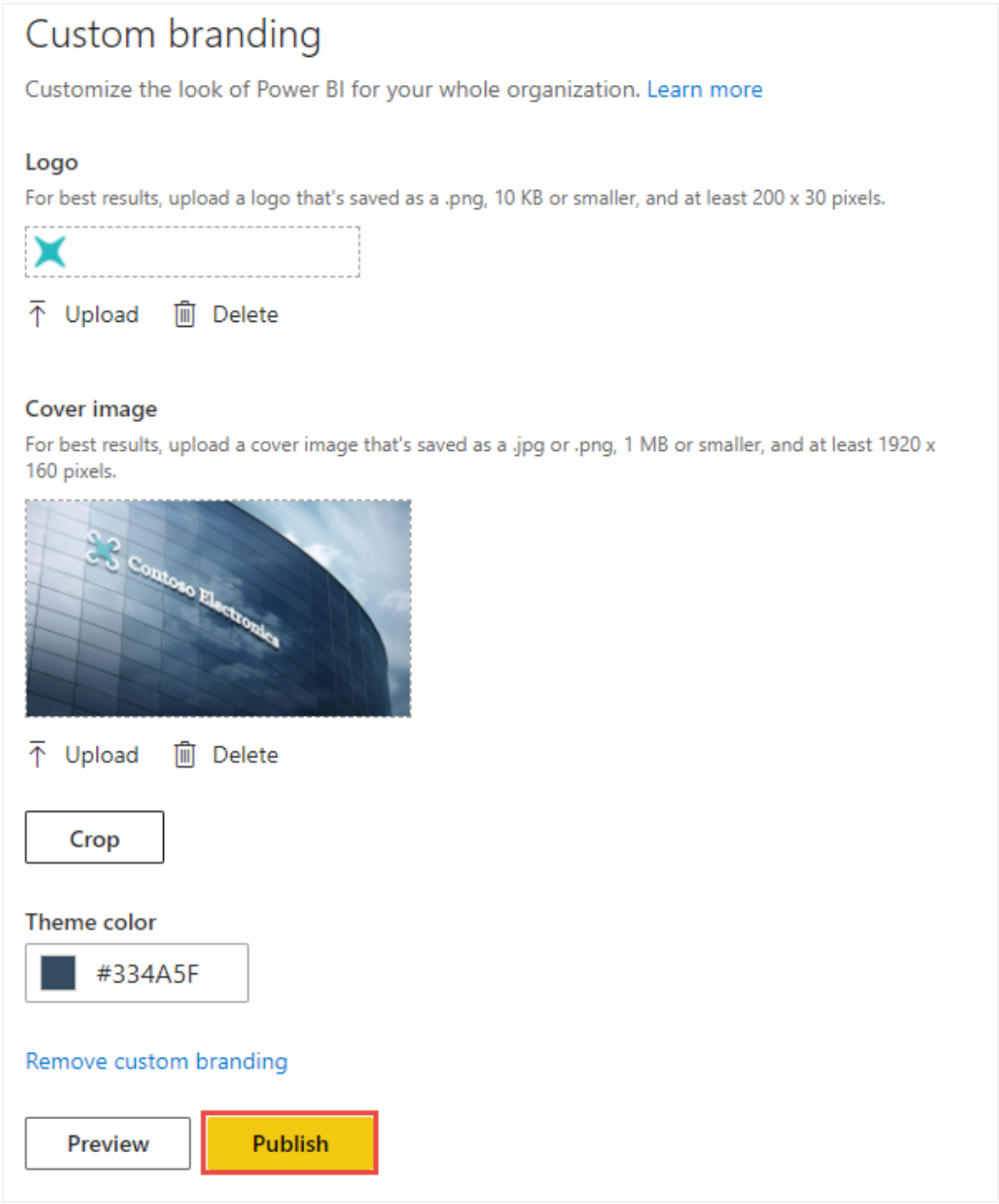
4. Upload a cover image file, then crop as needed to adjust how the image appears on the page.

5. Select your theme color by using the color picker or by typing the hex or decimal code.

6. Select **Preview** to see how your custom branding looks before you publish.

7. When you're happy with your settings, select **Publish** to make the custom branding the default appearance for all users in your organization. The custom

branding appears when you refresh your browser window.



Remove custom branding

Follow these steps to return the look of Power BI to the default settings:

1. Sign in to the Power BI service as a Fabric administrator.
2. From the navigation bar, select **Settings** > **Admin portal** > **Custom branding**.
3. Select **Remove custom branding**, then select **Publish** to go back to the Power BI default look.

Related content

Give your users a consistent online experience by applying custom branding to other services. Custom branding settings aren't shared between Microsoft 365 and Power BI, but your users will see branding that you apply to your organization's Microsoft Entra sign-in page.

- Add branding to your organization's Microsoft Entra sign-in page
- Customize the Microsoft 365 theme for your organization
- Add featured content to Power BI Home

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Manage Azure connections

08/20/2025

The Azure connections admin settings connect Azure services to Fabric. Using these settings, you can store your dataflows in your organization's Azure Data Lake Storage Gen2 (ADLS Gen2) account. You can review the benefits of this approach in Reasons to use the ADLS Gen 2 workspace or tenant connection. Workspace-level Log Analytics enables administrators and workspace owners to configure a Log Analytics connection to collect usage and performance logs for the workspace. You can review how the integration between Log Analytics and Power BI works.

The Azure connections admin settings have the following options:

- Tenant-level storage - Use to store dataflows in your organizations tenant settings. This setting can be configured if you want a central Data Lake storage place, or as a default storage place in addition to workspace level storage.
- Workspace-level storage permissions - Use to store dataflows in specific ADLS Gen 2 accounts, organized per workspace.
- Workspace-level log analytics permissions - Use to configure activity logging in Log Analytics.

To learn how to access the Fabric admin portal settings, see What is the admin portal?

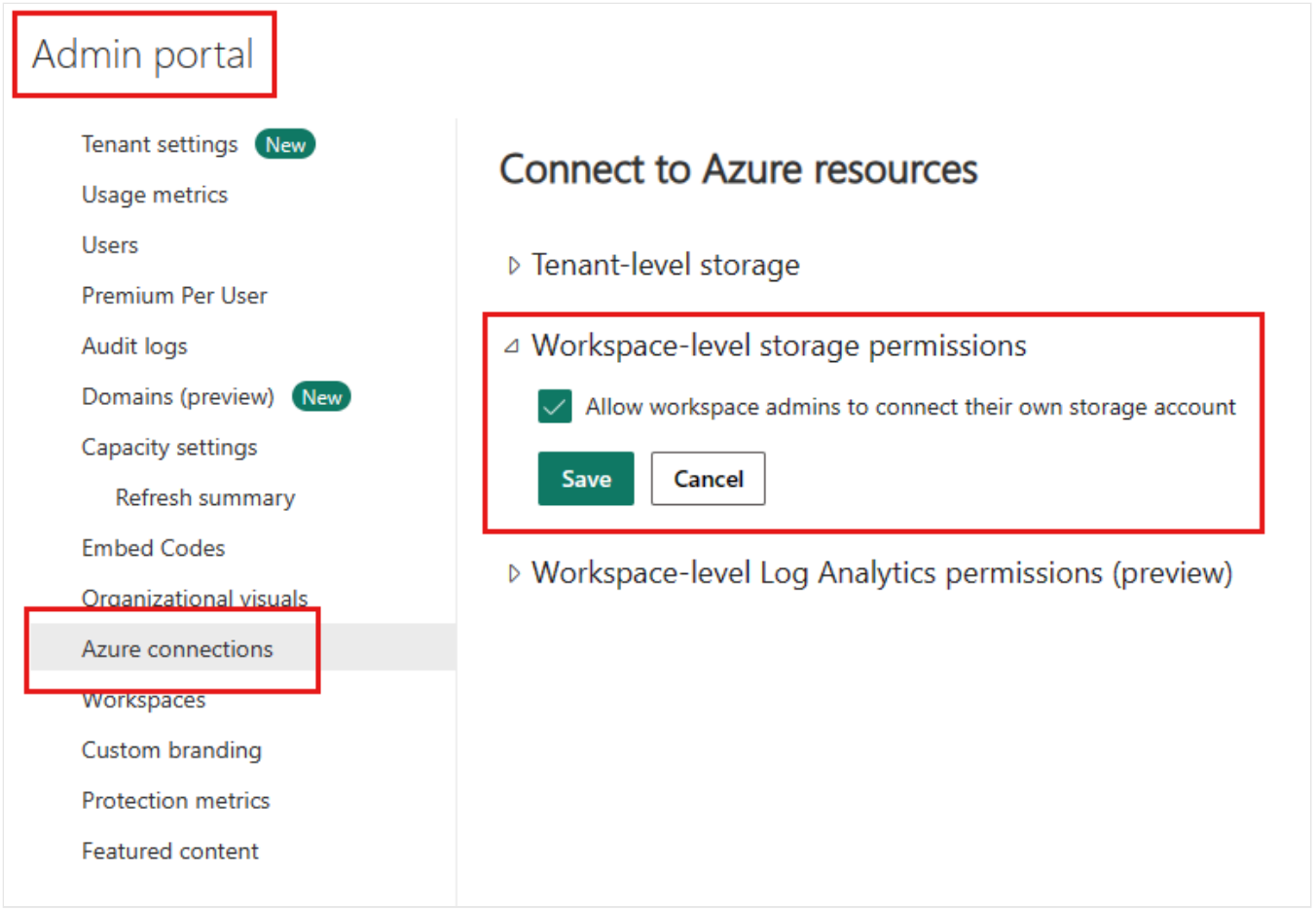
Tenant-level storage

By default, data used with Power BI is stored in internal storage provided by Power BI. With the integration of dataflows and Azure Data Lake Storage Gen2 (ADLS Gen2), you can store your dataflows in your organization's Azure Data Lake Storage Gen2 account. Storing dataflows in Azure Data Lake allows you to access them using the Azure portal, Azure Storage Explorer, and Azure APIs. For more information, see Configuring dataflow storage to use Azure Data Lake Gen 2.

Workspace-level storage permissions

By default, workspace admins can't connect their own storage account. This feature lets Fabric administrators turn on a setting that allows workspace admins to connect their own storage account.

To activate this feature, go to **Admin portal** > **Azure connections** > **Connect to Azure resources** > **Workspace-level storage permissions**, and check the **Allow workspace admins to connect their own storage account** checkbox.



Workspace-level log analytics permissions

Fabric administrators can find and configure activity logging in **Tenant settings** > **Audit and usage settings** > **Azure Log Analytics connections for workspace administrators**. For more information, see Allow workspace level logging from the admin portal

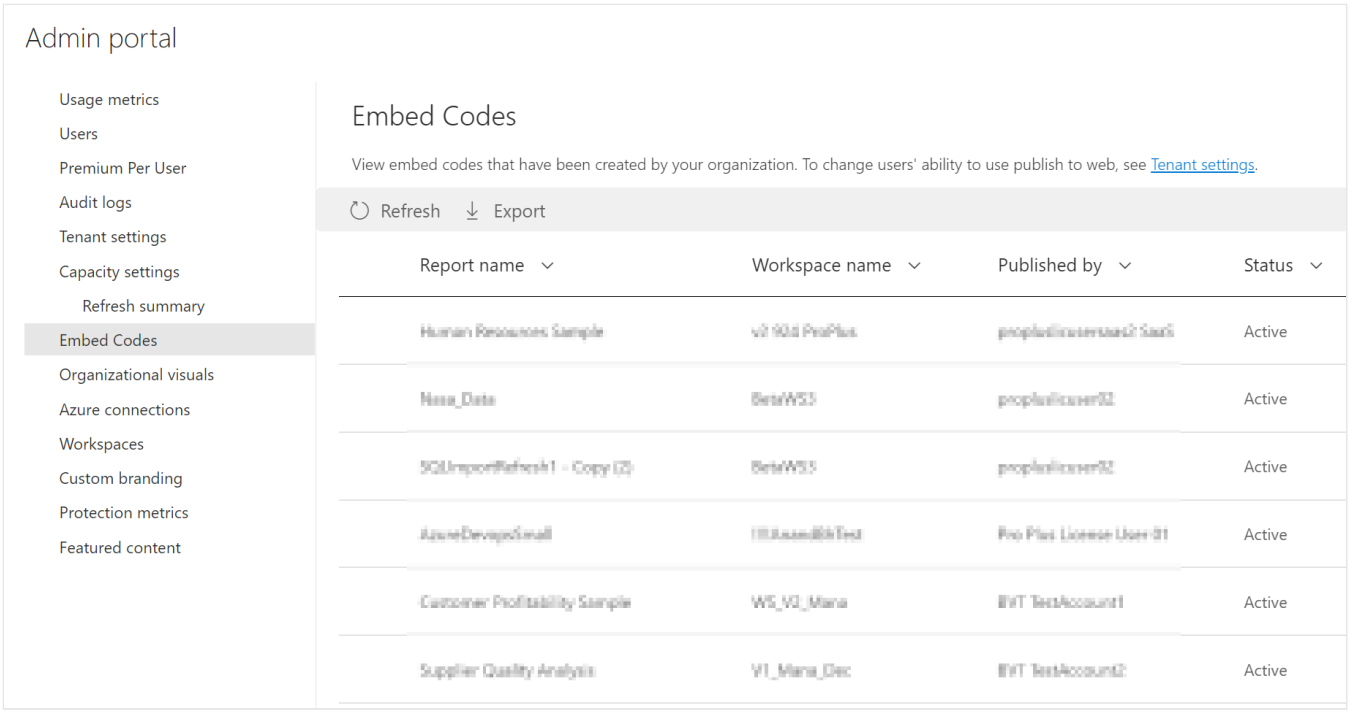
Related content

- What is the admin portal?
- Configuring dataflow storage to use Azure Data Lake Gen 2

Manage embed codes

Article • 05/23/2025

As a Fabric administrator, you can view the embed codes that are generated for sharing reports publicly, using the Publish to web from Power BI feature. You can also disable or delete embed codes.



To learn how to access the Fabric admin portal settings, see What is the admin portal?

Disable embed codes

You can disable the *Publish to web* feature, or allow embed codes to work only in your organization. If you disable *Publish to web*, the existing embed codes aren't deleted. When you reenable *Publish to web*, the existing embed codes become active again.

Disabling the embed codes is described in Publish to web.

Delete embed codes

To delete embed codes, select the codes you want to delete and then select **Delete**.

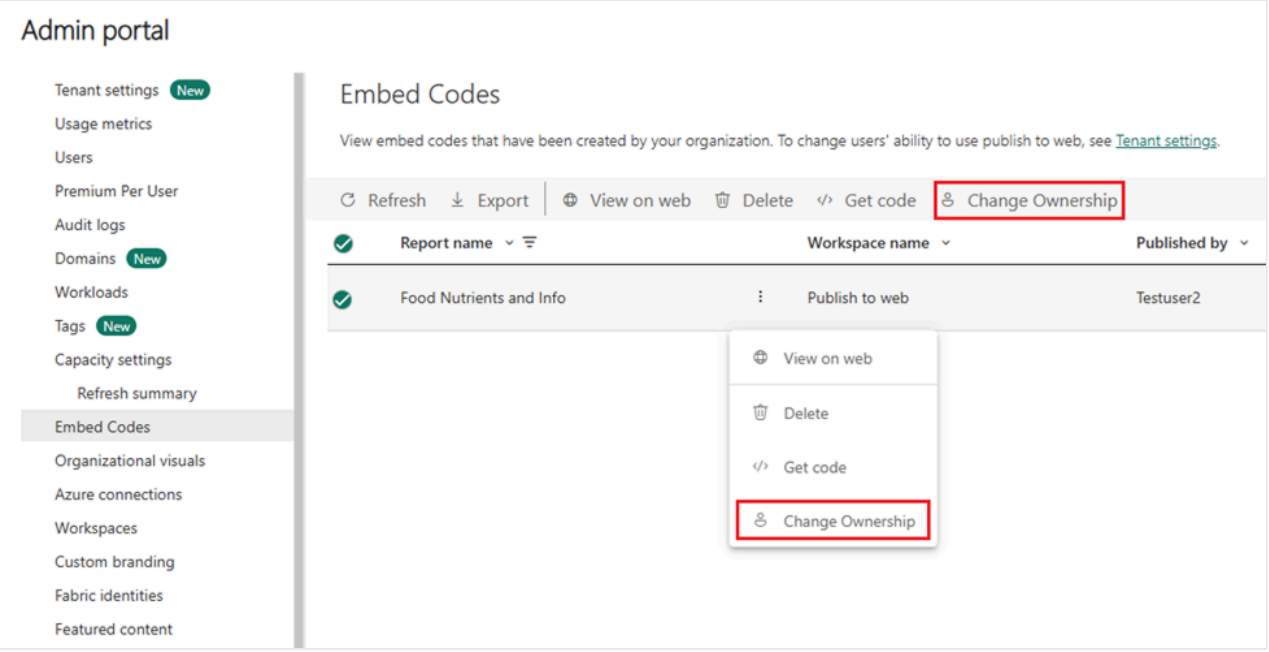
Transfer embed code ownership

Embed codes are linked directly to the publisher who creates them. This means that if the publisher loses access to the workspace where a report is published, users can no longer view

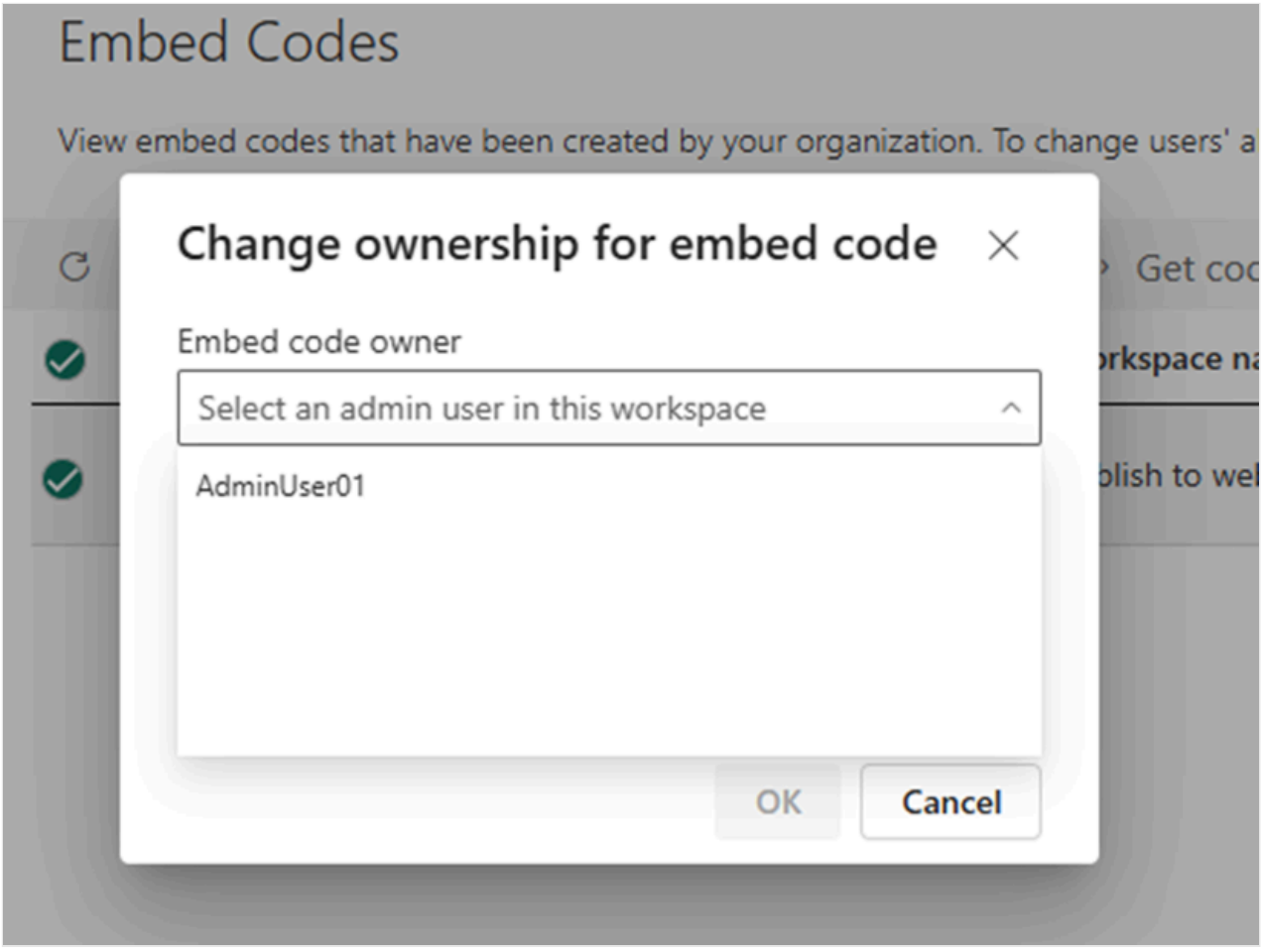
the embedded report. When a publisher leaves a workspace or an organization, Tenant admins can reassign ownership through the Admin portal, thereby restoring user access.

To change ownership from the Admin portal, follow these steps:

1. On the **Embed codes** page, select **Change ownership**.



2. Choose the new embed code owner from the dropdown menu, then select **OK**.



Related content

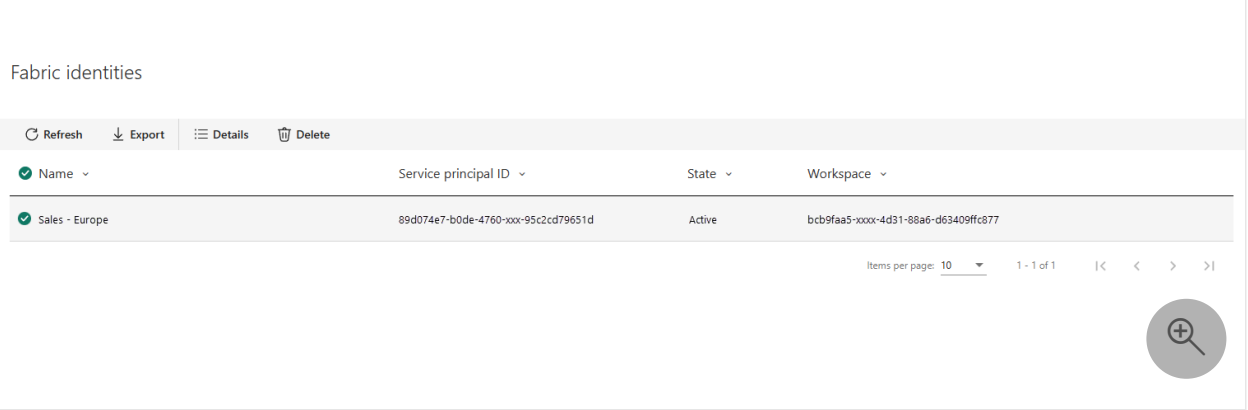
- Publish to web
- What is the admin portal?

Manage Fabric identities

Article • 11/07/2024

As a Fabric administrator, you can govern the Fabric identities that exist in your organization on the **Fabric identities** tab in the admin portal. For information about how to get to and use the admin portal, see How to get to the admin portal.

On the **Fabric identities** tab, you see a list of all the Fabric identities in your tenant.



The columns of the list of identities are described in following table.

Expand table

Column	Description
Name	The name of the identity.
Service principal ID	The object ID of the Enterprise application that is associated with the identity in Microsoft Entra.
State	The state of the identity. See workspace identity state values.
Workspace	The workspace ID.

View identity details

1. Select the radio button of the identity whose details you wish to view.
2. Select **Details** on the ribbon that appears. The **Details** side pane opens displaying the identity's details.

Expand table

Field	Description
Workspace name	The name of the workspace the identity is associated with.
State	The state of the identity.
State changed date	The date of the last change of state of the identity.
Service principal ID	The object ID of the Enterprise application that is associated with the identity in Microsoft Entra.
Application ID	The application ID of the Enterprise application that is associated with the identity in Microsoft Entra.
Tenant ID	The ID of the tenant the identity is defined in.
Role	The workspace role the identity has been assigned.

Delete an identity

> **⊗ Caution**
>
> Deleting a workspace identity breaks any Fabric item relying on that identity for trusted workspace access or authentication. Deleted identities can't be restored.

To delete an identity:

1. Select the radio button of the identity you want to delete.
2. Select **Delete** on the ribbon that appears.

Refresh the identities list

Select **Refresh** in the ribbon to refresh the list of identities.

Export the identities list as a .csv file

Select **Export** on the ribbon to download the list of identities as a *.csv* file.

Related content

- Workspace identity

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Manage featured content

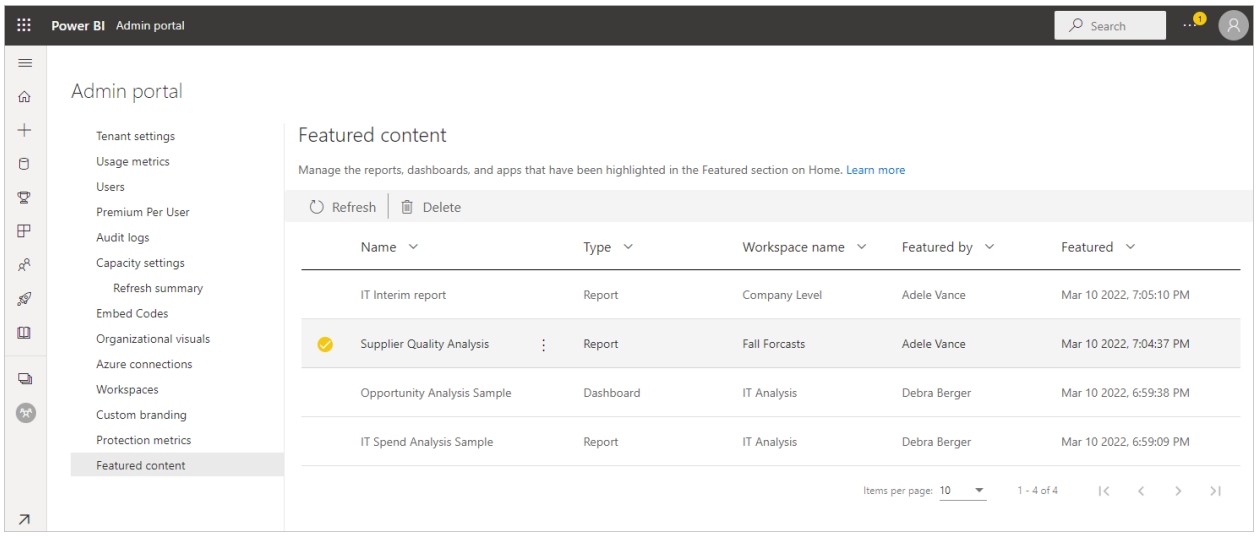
Article • 11/21/2023

If the *featured content* feature is enabled in your organization, users can feature content in the **Featured** section of the Power BI Home page. See Feature content on colleagues' Power BI Home page for details.

As a Fabric admin, you can monitor this featured content and remove it from the **Featured** section, if necessary. You can also disable the featured content feature entirely, in which case users will no longer be able to feature content. See the Enable/disable featured content section.

Monitor and manage featured content

In the admin portal, select **Featured content**.



Here you see a list of all featured items along with their relevant metadata. If something looks suspicious, or you want to clean up the **Featured** section, you can delete featured items as needed.

To delete an item, mouse over and select the item, and then click the trash can that appears in the top ribbon, or choose **More options (...)** > **Delete**. It's possible to select multiple items and then delete.

Enable/disable featured content

The featured content feature is enabled, disabled, and configured (for example, specifying who can feature content) via an admin setting. To learn more, see Featured content.

Related content

- Feature content on colleagues' Power BI Home page
- What is the admin portal?

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Manage organizational visuals

Article • 11/21/2023

The *organizational visuals* admin setting allows you to manage the list of Power BI visuals available in your organization. For more information and detailed instructions, see Organizational visuals.

Other Power BI visuals admin settings

All the Power BI visuals admin settings, including Power BI visuals tenant settings, are described in Manage Power BI visuals admin settings.

Related content

- What is the admin portal?
- Manage Power BI visuals admin settings

Feedback

Manage Power BI visuals admin settings

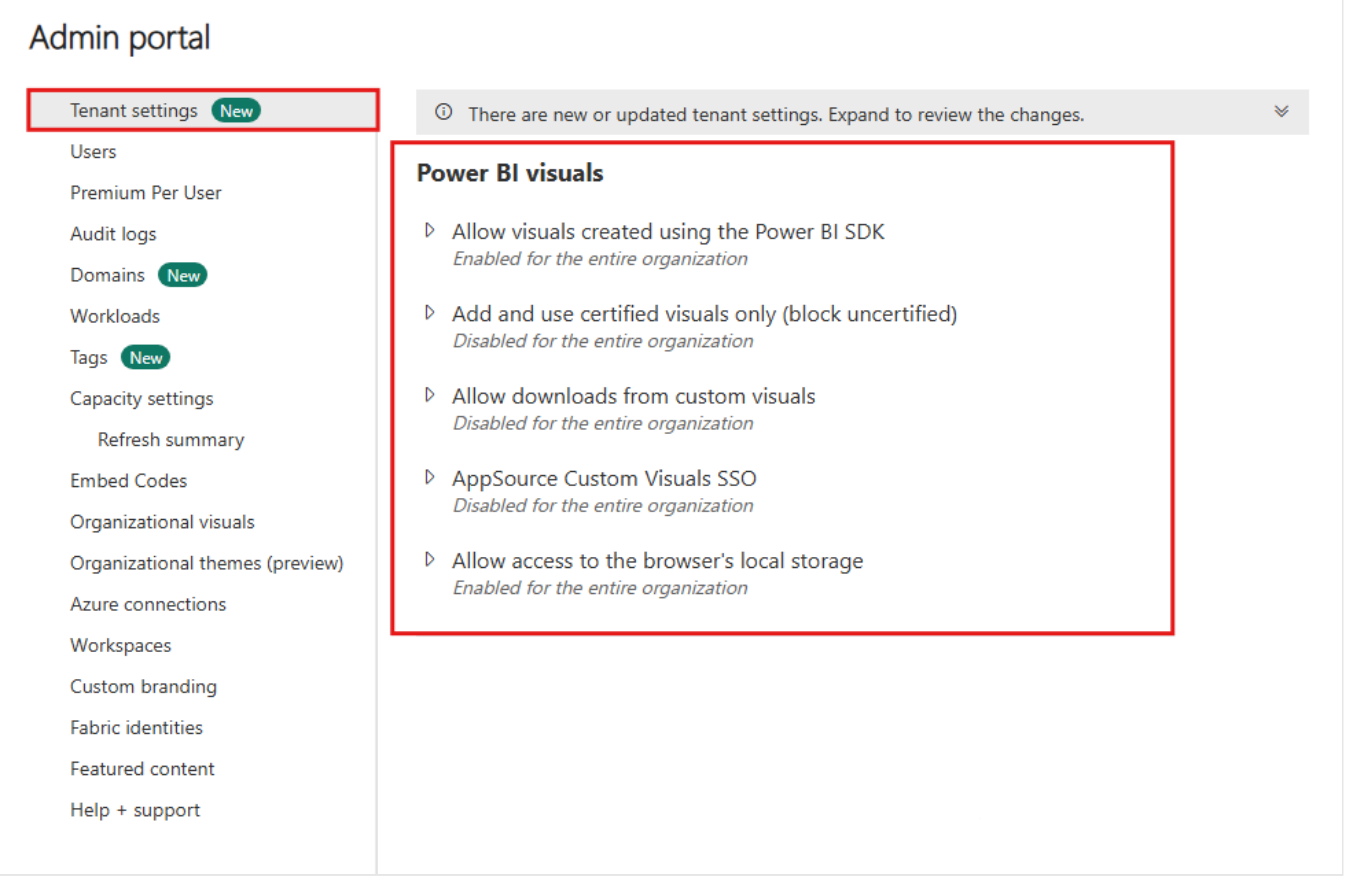
10/23/2025

As a Fabric administrator for your organization, you can control the type of Power BI visuals that users can access across the organization and limit the actions users can perform.

To manage Power BI visuals, you must be a Fabric administrator. For more information about the Fabric administrator role, see Understand Microsoft Fabric admin roles.

Power BI visuals tenant settings

To manage the tenant settings for Power BI visuals from the admin portal, go to **Tenant settings** and scroll down to **Power BI visuals**.



The UI tenant settings only affect the Power BI service. If you want these settings to take effect in Power BI Desktop, use group policies. A table at the end of each section provides details for enabling the setting in Power BI Desktop.

These settings allow you to control the following actions for Power BI visuals in your organization:

- Allow visuals created using the Power BI SDK
- Add and use certified Power BI visuals only

- Allow downloads from custom visuals
- AppSource Custom Visuals SSO
- Allow access to the browser's local storage

Visuals from AppSource or a file

Manage organizational access for the following types of Power BI visuals:

- Custom visuals that developers create by using the Power BI SDK and save as a *.pbiviz* file.
- Visuals that you download from AppSource.

This setting is disabled by default and doesn't affect visuals in the organizational store.

Use the following instructions to enable users in your organization to upload *.pbiviz* files, and add visuals from AppSource to their reports and dashboards:

1. Expand the **Allow visuals created using the Power BI SDK** settings.
2. Select **Enabled**.
3. Choose who can upload *.pbiviz* and AppSource visuals:
    - Select **The entire organization** option to allow everyone in your organization to upload *.pbiviz* files, and add visuals from AppSource.
    - Select the **Specific security groups** option to manage uploading *.pbiviz* files, and adding visuals from AppSource by using security groups. Add the security groups you want to manage to the *Enter security groups* text bar. The security groups you specify are excluded by default. If you want to include these security groups and exclude everyone else in the organization, select the **Except specific security groups** option.
4. Select **Apply**.

UI changes to tenant settings apply only to the Power BI service. To enable users in your organization to upload *.pbiviz* files, and add visuals from AppSource to their visualization pane in Power BI Desktop, use AD Group Policy.

Expand table

Key	Value name	Value
Software\Policies\Microsoft\Power BI Desktop\	EnableCustomVisuals	0 - Disable 1 - Enable (default)

Certified Power BI visuals

Certified Power BI visuals are visuals that meet the Microsoft Power BI team code requirements and testing. The tests check that the visual doesn't access external services or resources. However, Microsoft isn't the author of non-Microsoft visuals, so contact the author directly to verify the functionality of these visuals.

When you enable this setting, only certified Power BI visuals render in your organization's reports and dashboards. Power BI visuals from AppSource or files that aren't certified return an error message. This setting is disabled by default and doesn't apply to visuals in your organizational store.

1. From the admin portal, select **Add and use certified visuals only**.
2. Select **Enabled**.
3. Select **Apply**.

UI changes to tenant settings apply only to the Power BI service. To manage the certified visuals tenant setting in Power BI Desktop, use AD Group Policy.

Expand table

Key	Value name	Value
Software\Policies\Microsoft\Power BI Desktop\	EnableUncertifiedVisuals	0 - Disable 1 - Enable (default)

Export data to file

When you enable this setting, users can download data from a custom visual into a file on their storage device. This setting is separate from and not affected by download restrictions applied in your organization's export and sharing tenant settings. This setting is disabled by default and applies to all visuals including those visuals managed by your organizational store, Desktop, and web.

> **Note**
>
> When you enable this setting, a custom visual can export to files of the following types:
>
> - .txt
> - .csv
> - .json

- .tmplt
- .xml
- .pdf
- .xlsx

1. Expand the **Allow downloads from custom visuals** settings.
2. Select **Enabled**.
3. Choose who can download files:
    - Select **The entire organization** option to allow everyone in your organization to download data from a visual into a file.
    - Select the **Specific security groups** option to limit downloading files to specific security groups. Enter the security groups you want in the *Enter security groups* text bar. The security groups you specify are included by default. If you want to exclude these security groups and include everyone else in the organization, select the **Except specific security groups** option.
4. Select **Apply**.

UI changes to tenant settings apply only to the Power BI service. To enable users in your organization to download data from custom visuals in Power BI Desktop, use AD Group Policy.

Expand table

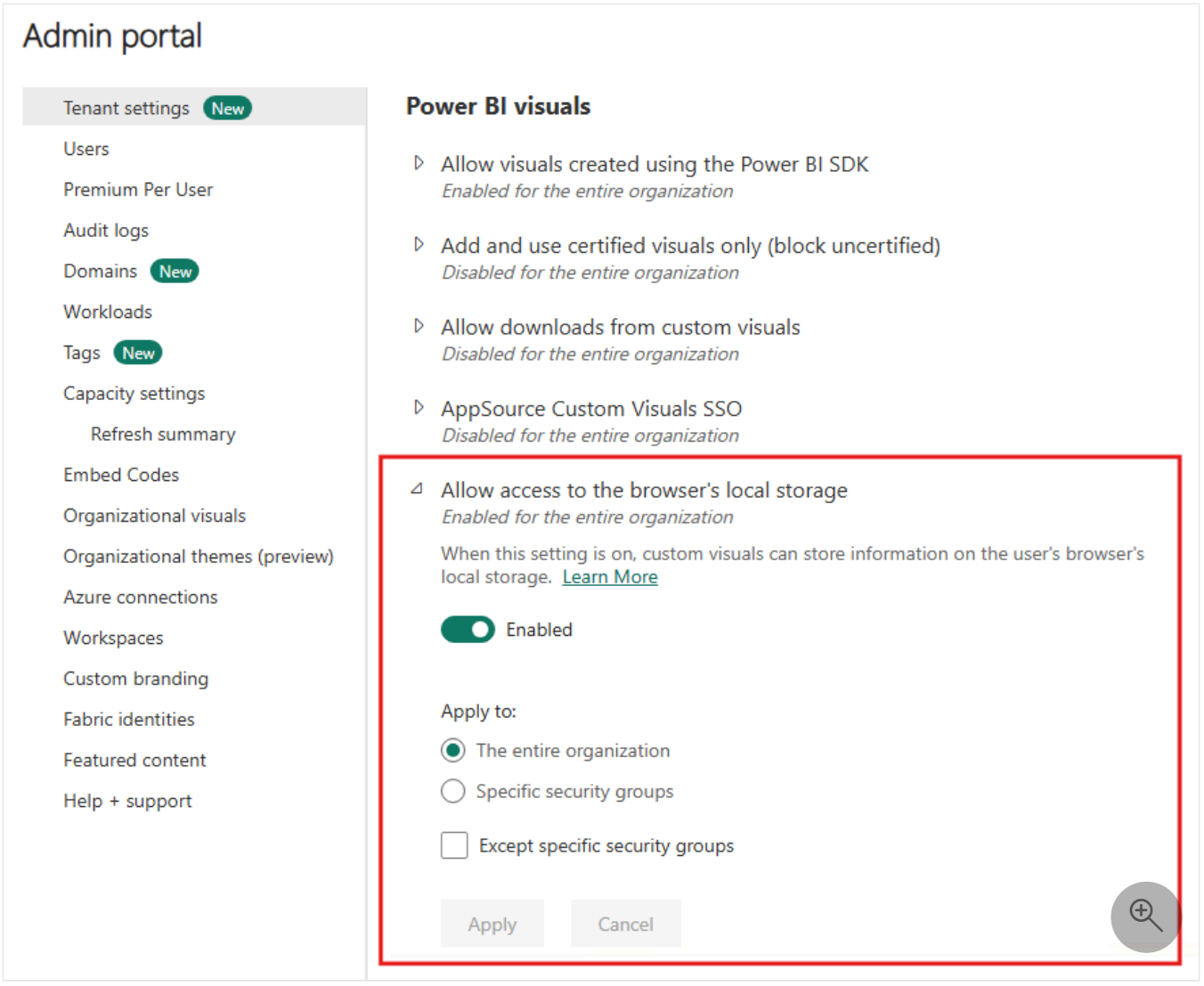
Key	Value name	Value
Software\Policies\Microsoft\Power BI Desktop\	AllowCVToExportDataToFile	0 - Disable 1 - Enable (default)

When `AllowCVToExportDataToFile` is set to *1*, the custom visual can export data to a file only if:

- The feature switch in the admin portal is enabled.
- The user is signed in.

Local storage

This setting enables visuals to store data on the browser's local storage which helps improve performance. This setting is separate from and not affected by download restrictions applied in your organization's export and sharing tenant settings. The setting is enabled by default and applies to all visuals, including those visuals managed by your organizational store, Desktop, and web.



To enable the local storage setting, follow these steps:

1. Expand the **Local storage** settings.

2. Select **Enabled**.

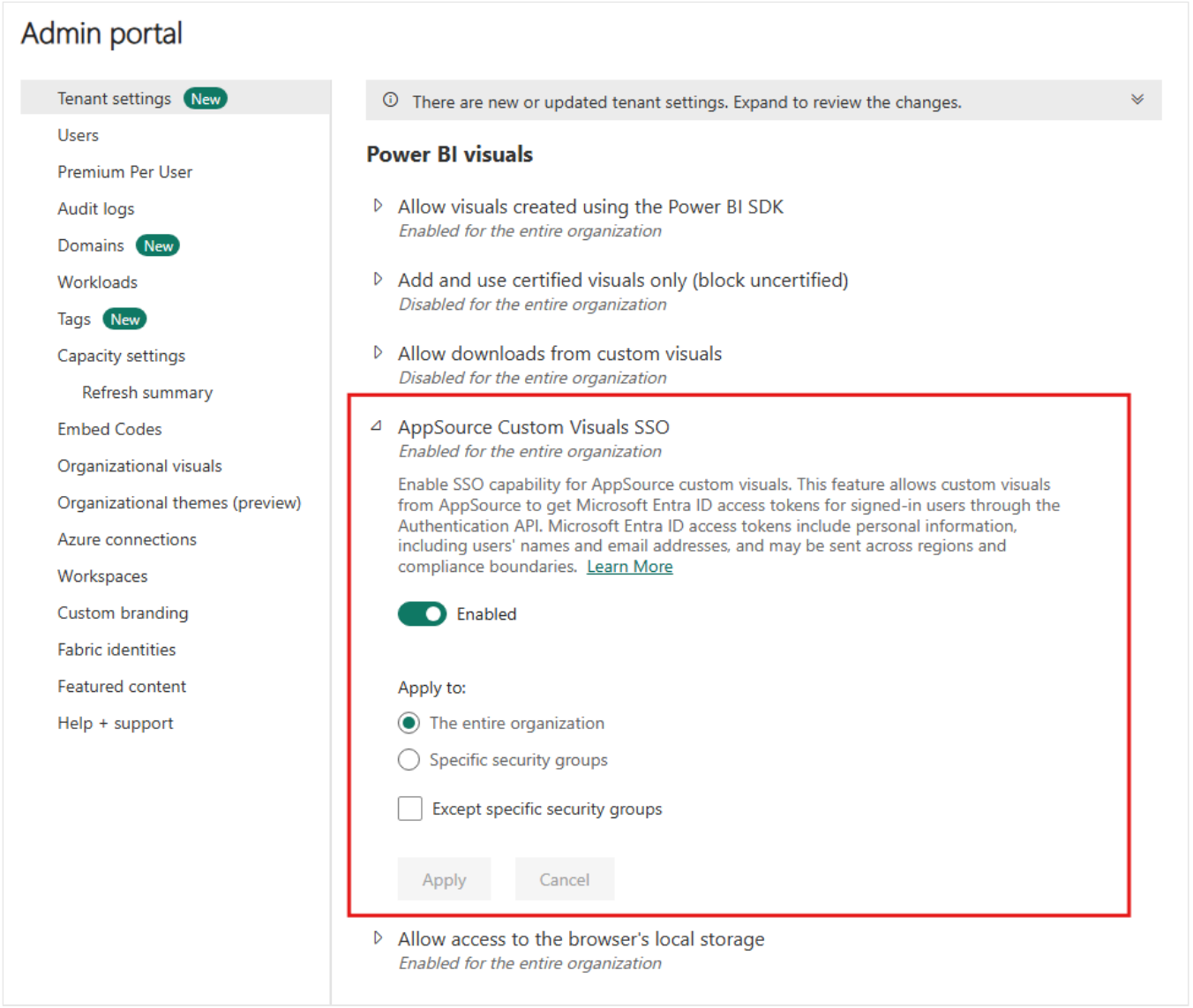
3. Choose who can render this API:

    - Select **The entire organization** option to allow visuals to store data on the local machine for every user in your organization.
    - Select the **Specific security groups** option to limit this privilege to specific security groups. Enter the security groups you want in the *Enter security groups* text bar. The security groups you specify are included by default. If you want to exclude these security groups and include everyone else in the organization, select the **Except specific security groups** option. Only a user listed in the permitted security group can render the API.

4. Select **Apply**.

AppSource Custom Visuals SSO

When you enable this setting, AppSource Custom Visuals can get Microsoft Entra ID (formerly known as Azure Active Directory) access tokens with restricted audiences for signed-in users by using the Authentication API. These tokens include personal information such as the user's name and email address. Custom Visuals can send these tokens across different regions and compliance boundaries, and they're fully responsible for handling the tokens they possess. The setting is disabled by default and applies to all AppSource Custom Visuals, including those visuals managed by your organizational store.



1. Expand the **Allow custom visuals to get user Microsoft Entra access tokens** settings.
2. Select **Enabled**.
3. Choose who can render this API:
    - Select **The entire organization** option to allow visuals to get Microsoft Entra access tokens for every user in your organization.
    - Select the **Specific security groups** option to limit getting access tokens to specific security groups. Enter the security groups you want in the *Enter security groups* text bar. The security groups you specify are included by default. If you want to exclude

these security groups and include everyone else in the organization, select the **Except specific security groups** option. Only a user listed in the permitted security group can render the API.

4. Select **Apply**.

Organizational visuals

As a Fabric admin, you can manage the list of Power BI visuals available in your organization's organizational store. The **Organizational visuals** tab, in the *Admin portal*, allows you to add and remove visuals and decide which visuals automatically display in the visualization pane of your organization's users. You can add to the list any type of visual including uncertified visuals and *.pbiviz* visuals, even if they contradict the tenant settings of your organization.

Organizational visuals settings automatically deploy to Power BI Desktop.

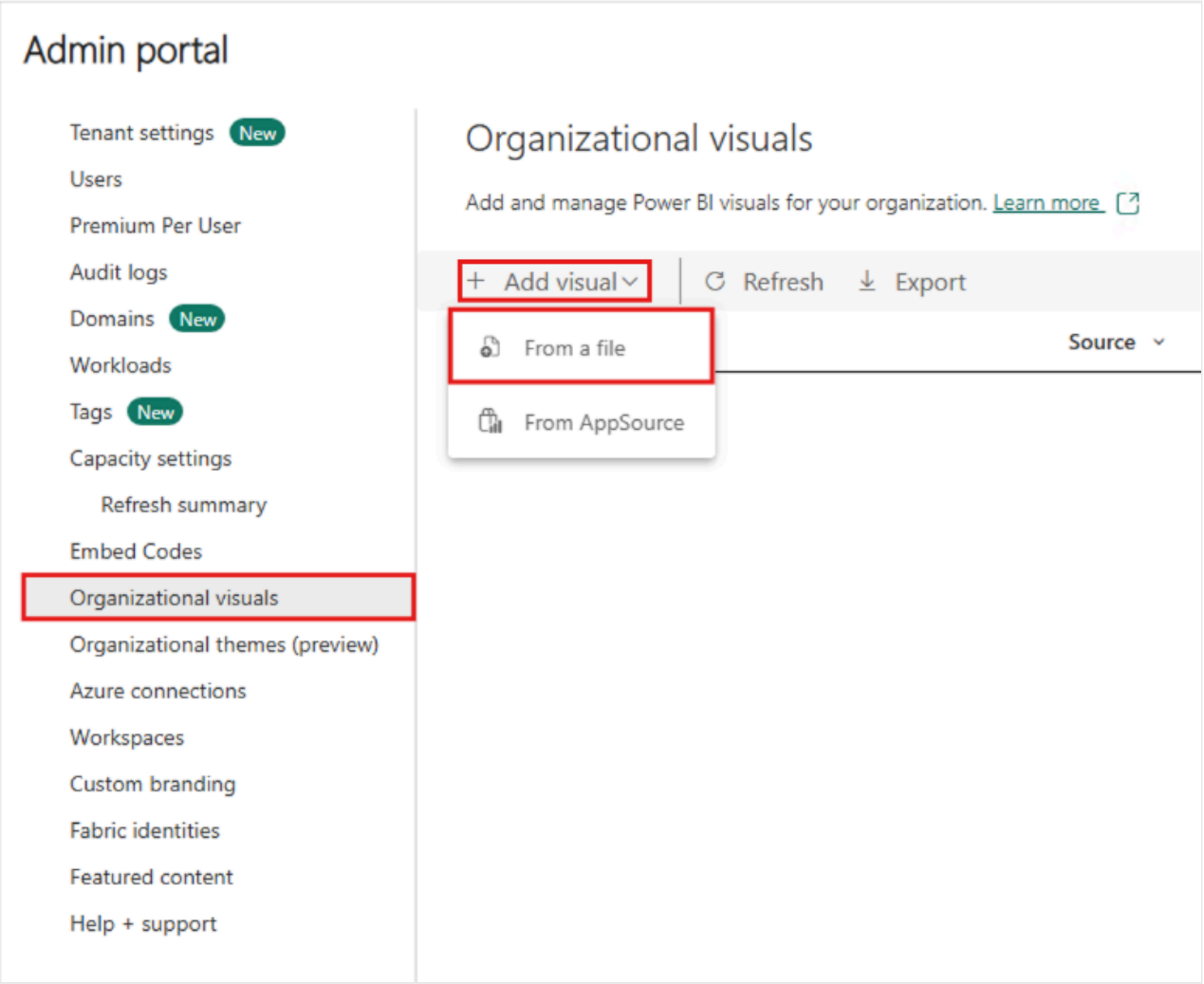
> ⓘ **Note**
>
> Power BI Report Server doesn't support organizational visuals.

Add a visual from a file

Use this method to add a new Power BI visual from a *.pbiviz* file.

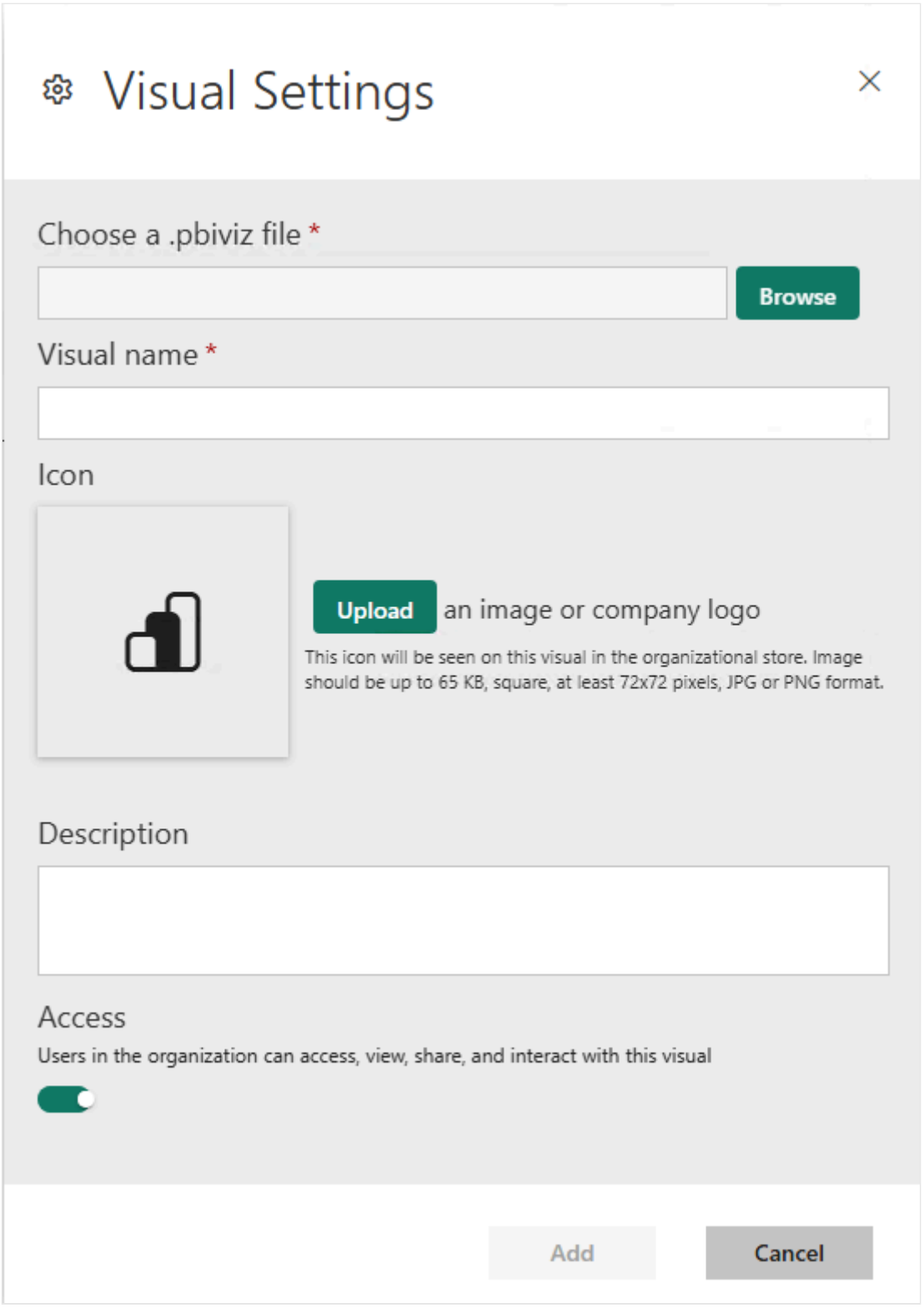
> ⚠ **Warning**
>
> A Power BI visual uploaded from a file could contain code with security or privacy risks. Make sure you trust the author and the source of the visual before deploying to the organization's repository.

1. Select **Add visual** > **From a file**.



2. Fill in the following fields:

- **Choose a .pbiviz file** - Select a visual file to upload.
- **Name your visual** - Give a short title to the visual, so that report authors can easily understand what it does.
- **Icon** - Upload an icon file to display in the visualization pane.
- **Description** - Provide a short description of the visual to give more context for the user.
- **Access** - Select whether users in your organization can access this visual. This setting is enabled by default.



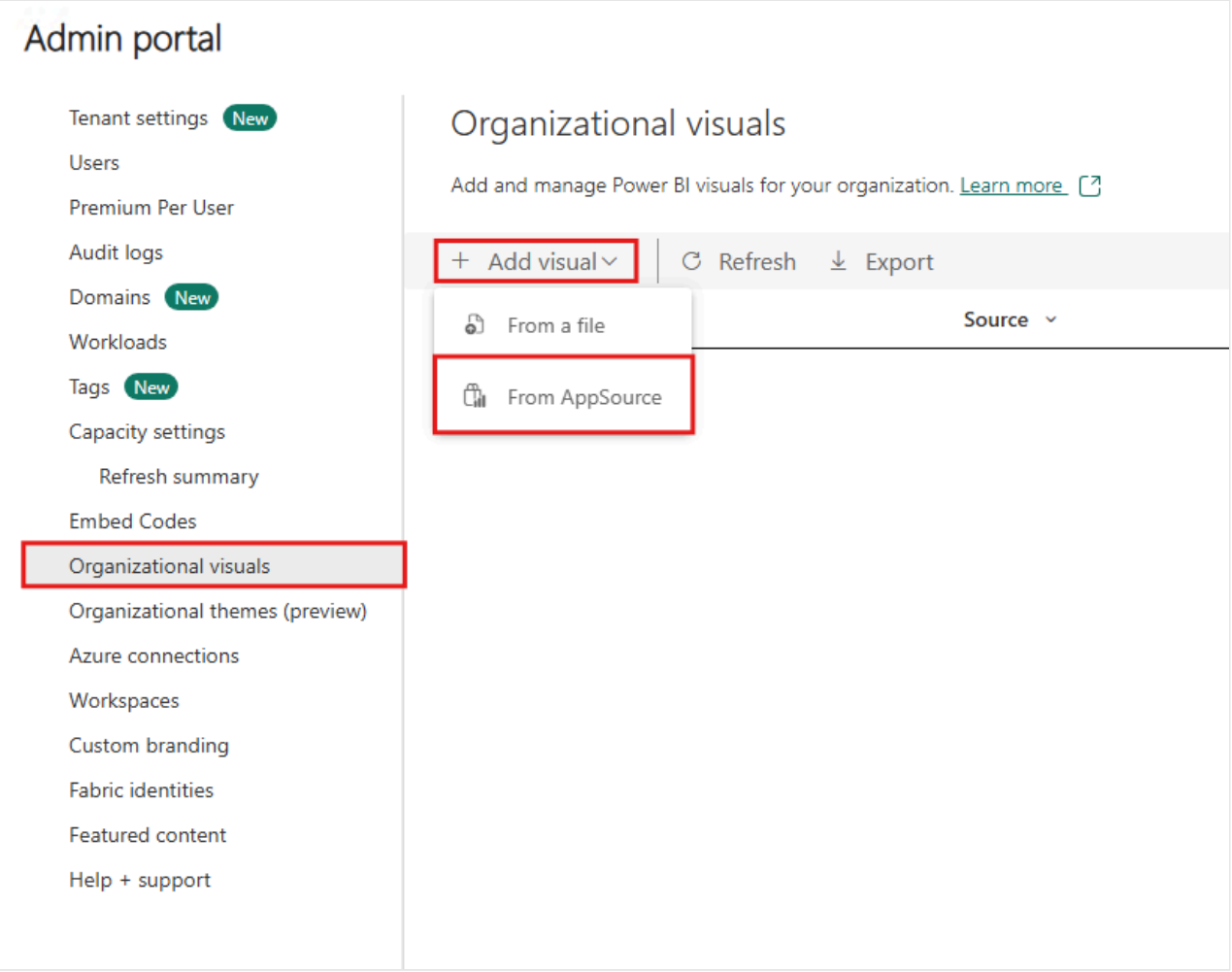
3. Select **Add** to start the upload request. After it uploads, the visual appears in the organizational visuals list.

Add a visual from AppSource

Use this method to add a new Power BI visual from AppSource.

AppSource Power BI visuals automatically update. Users in your organization always have the latest version of the visual.

1. Select **Add visual** > **From AppSource**.



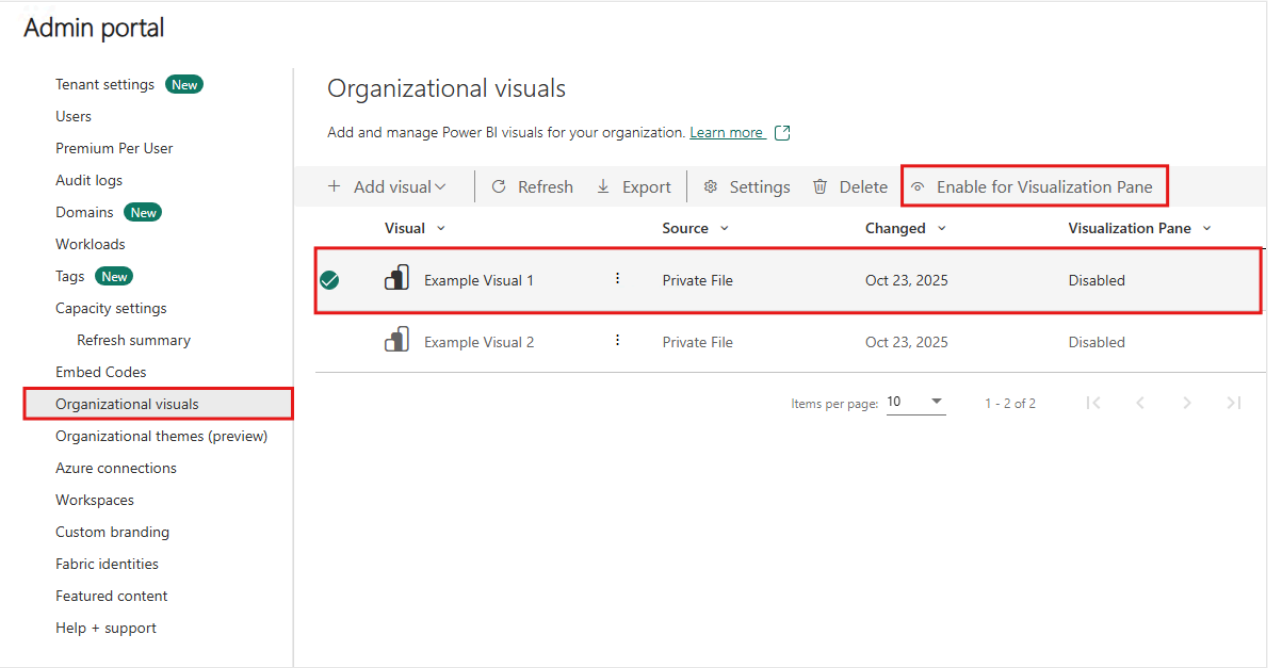
2. In the **Power BI visuals** window, find the AppSource visual you want to add, and select **Add**. After it uploads, the visual displays in the organizational visuals list.

Add a visual to the visualization pane

You can pick visuals from the organizational visuals page to automatically show on the visualization pane of all the users in your organization.

1. Select the visual you want to add.

2. Select **Enable for Visualization Pane**.



Delete a visual uploaded from a file

To permanently delete a visual, select the visual then select **Delete**.

> **Important**
>
> Deletion is irreversible. After the visual is deleted, it immediately stops rendering in existing reports. Even if you upload the same visual again, it doesn't replace the one that was deleted. However, users can import the new visual again and replace the instance they have in their reports.

Disable a *.pbiviz* visual

You can disable a *.pbiviz* visual from being available through the organizational store, while keeping it on the organizational visuals list.

1. Select the *.pbiviz* visual you want to disable, then select **Settings**.
2. In the **Access** section, disable the setting: **Users in the organization can access, view, share, and interact with this visual**.

After you disable the *.pbiviz* visual, the visual doesn't render in existing reports, and it displays the following error message:

```
This custom visual is no longer available. Contact your administrator for details.
```

> **Note**

.pbiviz visuals that are bookmarked continue working even after they're disabled.

Update a visual

AppSource visuals update automatically. After a new version is available from AppSource, it replaces an older version deployed via the organizational visuals list.

To update a *.pbiviz* visual, follow these steps to replace the visual.

1. Select the visual you want to add, then select **Settings**.
2. Select **Browse**, then select the *.pbiviz* file you want to use to replace the current visual.
3. Select **Update**.

Replace a visual from a file with a visual from AppSource

Sometimes an organization develops its own Power BI visual and distributes it internally. After some time, the organization might decide to make this visual public by uploading it to AppSource. To replace the visual uploaded from a file with the one from AppSource, use the following steps:

1. Add the visual from AppSource into the organizational store.
2. Open the report that contains this visual. Both the visual uploaded from a file and the AppSource visual are visible in the visualization pane.
3. In the report, highlight the visual uploaded from a file and in the visualization pane, select the AppSource visual to replace it. The visuals are swapped automatically. To verify that you're using the AppSource visual, in the visualization pane right-click the visual and select *about*.
4. Complete **step 3** for all the reports that contain the visual in your organization.
5. Delete the visual that you uploaded from a file.

Related content

- What is the admin portal?
- Visuals in Power BI
- Organizational visuals in Power BI

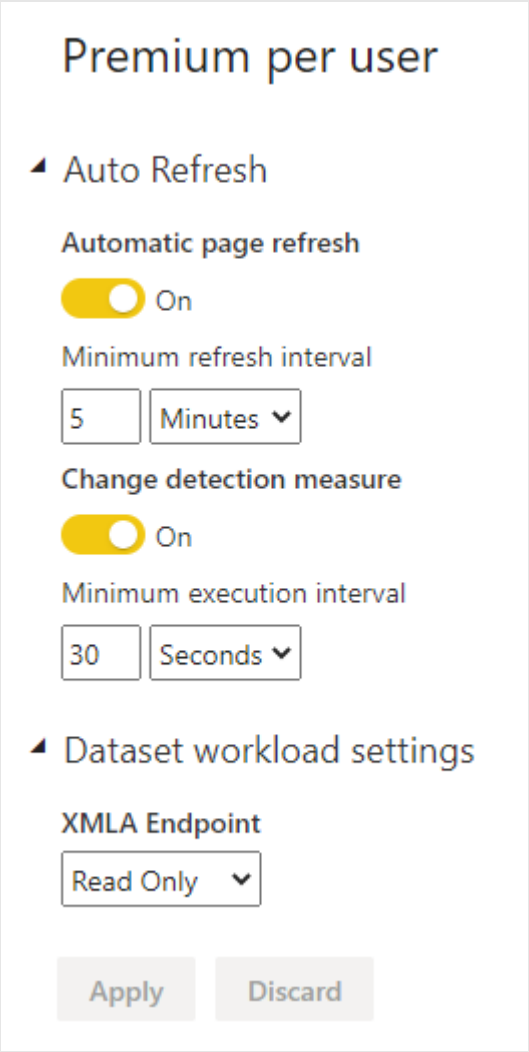
Manage Premium Per User

Article • 11/21/2023

Premium Per User (PPU) is a way to license Premium features on a per user basis. After the first user is assigned a PPU license, associated features can be turned on in any workspace. Admins can manage the auto refresh and semantic model workload settings that are shown to users and their default values. For example, access to the XMLA endpoint can be turned off, set to read only, or set to read and write.

PPU settings

You can configure the following PPU settings in the admin portal on the **Premium Per User** tab. To learn how to access the Fabric admin portal settings, see What is the admin portal?



Auto refresh

Automatic refresh enables your active report page to query for new data, during predefined intervals. By default, these settings are turned on. If you turn them off, PPU reports that use automatic refresh and change detection don't get updated automatically.

Use the following settings to override the *automatic refresh* settings in individual reports that reside on the PPU capacity. For example, when the *minimum refresh interval* setting is configured to refresh every 30 minutes, if you have a report that's set to refresh every five minutes, its setting will be overridden and the report is refreshed every 30 minutes instead.

- **Minimum refresh interval** - Use to specify a minimum value for the automatic refresh for all the reports in the PPU capacity. The Power BI service overrides any automatic refresh settings that are higher than this setting.
- **Change detection measure** - Use to specify a minimum value for all the reports in the PPU capacity that use change detection. The Power BI service overrides any change detection settings that are higher than this setting.

Semantic model workload settings

XMLA endpoints allow Microsoft and third-party apps and tools to connect to Power BI semantic models. Use this setting to determine if in the PPU capacity XMLA endpoints are turned off, or configured for read only or read and write.

Related content

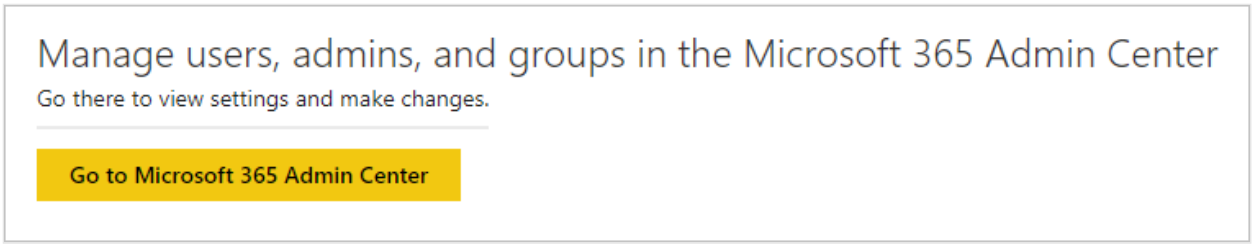
- What is the admin portal?
- Power BI Premium Per User FAQ
- Automatic page refresh in Power BI

Feedback

Manage users

Article • 11/20/2024

You manage Power BI users, groups, and admins in the Microsoft 365 admin center. The **Users** tab in the Fabric admin portal provides a link to the admin center.



Related content

- Administration overview
- Microsoft 365 admin center help
- Give users access to workspaces

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

View audit logs

Article • 02/28/2024

Go to the Fabric admin portal to access this feature. For information about how to get to and use the admin portal, see What is the admin portal?

You manage Power BI audit logs in the Microsoft Purview compliance portal. The Audit logs tab provides a link to the Microsoft Purview compliance portal. To learn more, see Track user activities in Power BI.

Related content

- What is the admin portal?

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

View refresh summary

Article • 11/21/2023

The refresh summary admin settings page lets you view your capacity's refresh history. You can also export the refresh history, and view details related to a specific refresh. The information in this page can help you investigate refresh errors, and establish a refresh schedule for the Power BI items that reside on your capacities.

To learn how to access the Fabric admin portal settings, see What is the admin portal?

Schedule

The schedule tab lists all the refreshes that took place in a specific capacity. Select the capacity you want to review from the *choose a capacity* dropdown menu. Use the *refresh* button to refresh the table's results, and the *export* button to export a .csv file.

To view details for a specific refresh instance, select the instance and then select **Details**.

History

The history tab lists all the refreshes that took place in all the capacities you're an admin of. The table headers allow you to sort the information and apply filters. Use the *refresh* button to refresh the table's results, and the *export* button to export a .csv file.

Related content

- What is the admin portal?

Feedback

Feature usage and adoption report (preview)

Article • 03/06/2025

The feature usage and adoption report is aimed at admins who want to understand how Fabric features are utilized across the organization. As an admin, the report insights can help you govern your Fabric tenant and take action when needed.

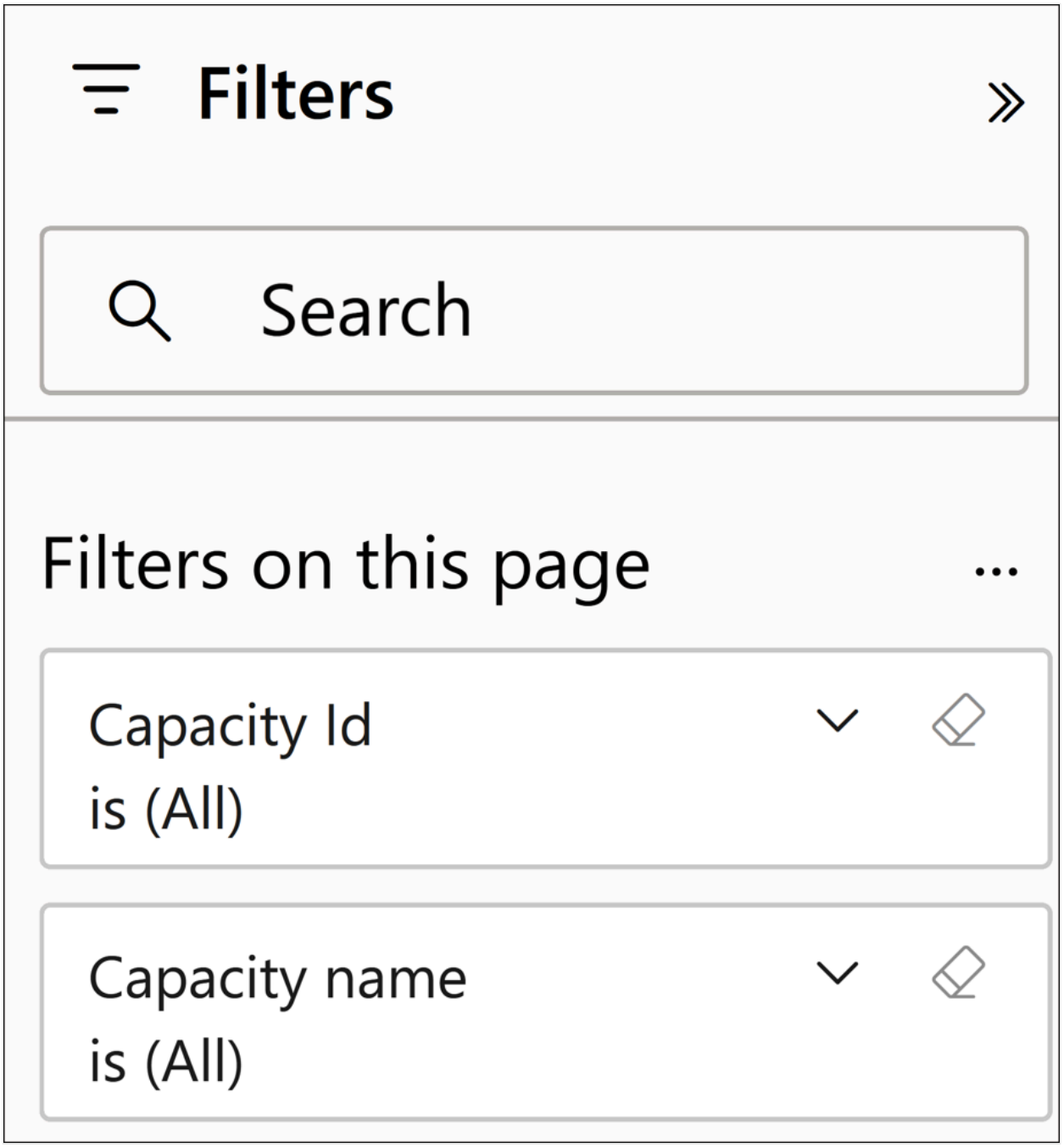
You can access the report from the Admin monitoring workspace. To access the workspace, you must be a Fabric administrator.

You can also have an admin share the report or semantic model directly with you. With build permissions to the semantic model, users can design a custom report that relies on the same underlying data.

Navigation

The report is designed for admins to analyze Fabric activity in various ways. Use the date range slicer to filter activity data across all pages for a specific range of time over the last 30 days.

Additionally, use the filter pane to filter activity data based on the desired analysis. Filters are available across different characteristics of activity, including capacity, user, and item-related info.



Report pages

The report is composed of five pages:

- **Activity Overview** - Provides a high-level overview of Fabric activity across the organization
- **Analysis** - Visualizes activity across different activity dimensions
- **Activity Details** - Shows detailed information on specific activity scenarios
- **Inventory** - Lists all Fabric items in your tenant
- **Item Details page** - Shows detailed information on specific inventory usage scenarios

Activity Overview page

The Activity Overview page helps you identify:

- Daily activities and user trends
- The most active capacities and workspaces
- Activities in your organization by your most or least active users

Example

In a large retail organization, you might use the Activity Overview page to check which capacities were most utilized in a given month. Using the date range slicer to filter to the month of December, you notice the *Sales and Marketing* capacity had nearly 1,000 activities while other capacities had under 200. To understand why this is happening, you then go to the Analysis page.

Analysis page

On the Analysis page, you can view:

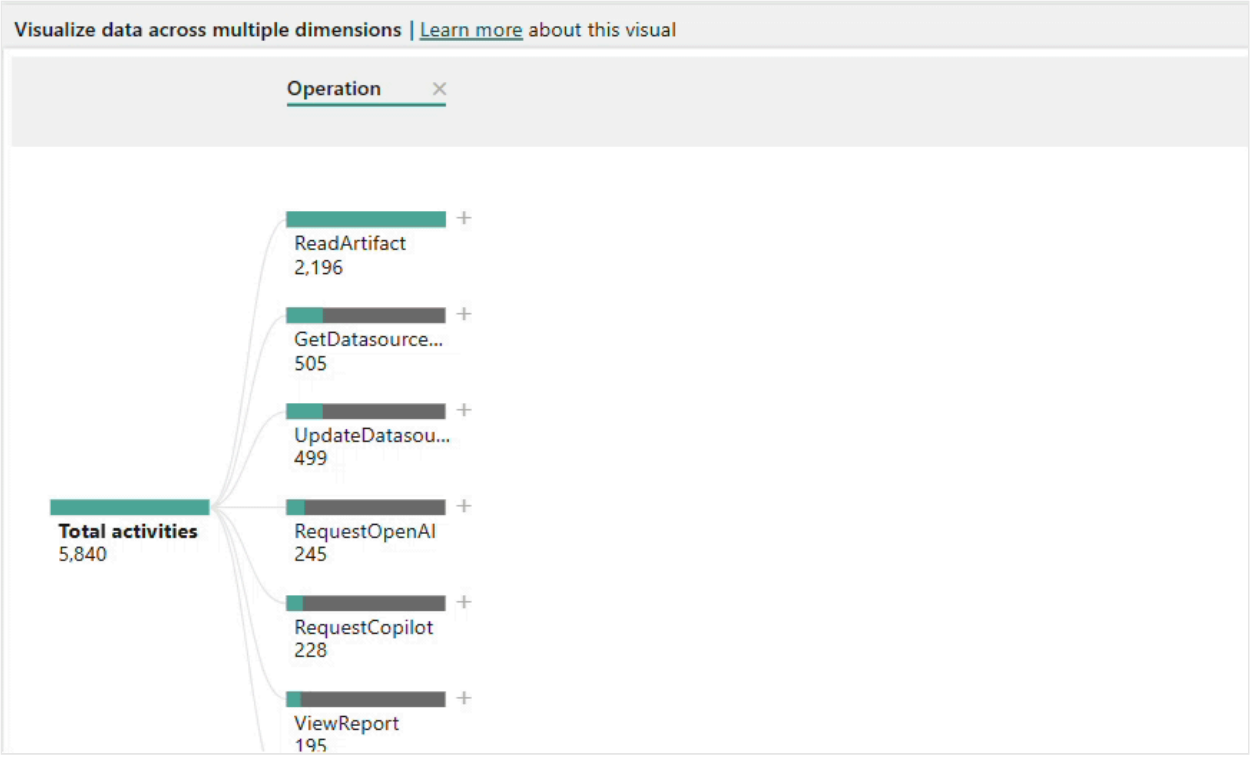
- A daily count of activity and users by date
- A decomposition tree to drill down into activity using dimensions such as operation, capacity, user, and more

Example

Continuing the example from the Activity Overview page, you use the Analysis page to investigate why the *Sales and Marketing* capacity had more activity in December than all other capacities. The decomposition tree reveals the most popular activity on the *Sales and Marketing* capacity was *ViewReport*, which signifies the viewing of a Power BI report. You then drill through to the Activity Details page to identify which reports were most frequently viewed that month on the *Sales and Marketing* capacity.

To drill through to the Activity Details page:

1. Right-click the visual element (such as Operation name) you want to drill through from.
2. Select *Drill through*.
3. Select *Activity Details*.



Activity Details page

The Activity Details page shows detailed information on specific activity scenarios. Users can access this page by drilling through from the Activity Overview or Analysis pages to display the following activity details:

- **Creation time** - The time the activity was registered
- **Capacity name** - The name of the capacity that the activity took place on
- **Capacity ID** - The ID of the capacity that the activity took place on
- **Workspace name** - The name of the workspace that the activity took place in
- **Workspace ID** - The ID of the workspace that the activity took place in
- **User (UPN)** - The user principal name of the user who conducted the activity
- **Operation** - The formal name of the operation
- **Total of activities** - The number of times the activity took place

Example

From the Analysis page, you drill through on frequently conducted *ViewReport* actions on the *Sales and Marketing* capacity in December. Using info from the Activity Details page, you discover that a new report titled "Unclosed Deals" was heavily viewed,

prompting further investigation to understand the report's impact on your organization's sales strategy.

Inventory page

The Inventory page displays all items in your Fabric tenant and how they're utilized. You can filter the Inventory page by:

- **Item type** - Including reports, dashboards, lakehouses, notebooks, and more
- **Workspace name** - The name of the workspace where the items are located
- **Activity status** - Indicates whether the item has been recently utilized
  - *Active* - At least one audit log activity was generated related to the item over the last 30 days
  - *Inactive* - No audit log activity was generated related to the item over the last 30 days

Example

The Inventory page also includes a decomposition tree visual to breakdown inventory by different factors such as capacity, user, workspace, and more. You can use the decomposition tree to decompose items by activity status; for example, displaying all inactive items by item name so that you can decide whether any of these items can be deleted.

Item Details page

The Item Details page shows information related to specific inventory usage scenarios.

Users can navigate to the Item Details page by drilling through from the Inventory page. To drill through, right-click a visual element (such as Item type) and then select the Item Details page from the *Drill through* menu.

After drilling through, you see the following information for the selected item types:

- **Capacity ID** - The ID of the capacity that the item is hosted on
- **Workspace ID** - The ID of the workspace that the item is located in
- **Workspace name** - The name of the workspace that the item is located in
- **Item ID** - The unique ID of the item

- **Item name** - The display name of the item
- **Item type** - The type of item such as report, dataset, app, and so on
- **Modified by** - The ID of the user that last modified the item
- **Activity status** - The status of an item whether it's active or inactive based on recent activity
- **Items** - The total number of items

Measures

The following measures are used in visuals throughout the report and are also available in the semantic model.

Measure calculations consider filter context, so measure values change as you apply filters or interact with other visuals.

Expand table

Measure name	Description
Active capacities	The number of capacities with audit activity.
Active users	The number of users who have generated audit activity.
Active workspaces	The number of workspaces with audit activity.
Activities	The number of audit activities generated.
Items	The count of items displayed.
Total activities	The number of audit activities generated. Reflected as 0 when no audit data is returned; used exclusively in card visuals.
Total items	The count of items displayed. Reflected as 0 when no items are returned; used exclusively in card visuals.

Considerations and limitations

This section lists the report's considerations and limitations.

Display

- Condensing the zoom slider on a date trend visual to a single day displays a misleading time range, as activities are aggregated by day and not by time.
- Using the *next level in the hierarchy* option on the *Most active Capacities* visual doesn't update the dynamic visual title.
- Items with the same name, or items deleted and recreated with the same name, might reflect as one item in certain visuals. To count the total number of unique items, use item IDs or the *Total items* measure.
- *NA* represents data that isn't available, which can happen when an audit event doesn't have complete information, or when that information isn't applicable for the event.
- The report retains information for 30 days, including the activities and metadata of deleted capacities, workspaces, and other items.
- Deleted workspaces with extended retention don't appear in the report after 30 days. They can be seen in the admin portal until they're permanently deleted.
- Items created and deleted within a 24 hour period may have incomplete information.

Pro and Premium Per User (PPU)

Semantic models in *Pro* and *Premium Per User* (PPU) workspaces are hosted on internal logical capacities. The usage of these capacities can be seen in this report.

- **Pro** - Appear as *Reserved Capacity for Pro Workspaces* with the capacity SKU value *Pro*.
- **PPU** - Appear as *Reserved Capacity for Premium Per User Workspaces* with the capacity SKU value *PPU*.

Counting logic

- All *My workspaces* are counted as separate records as part of the *Active workspaces* measure.

Related content

- What is the Admin monitoring workspace?

- Admin overview

Feedback

Was this page helpful? Yes No

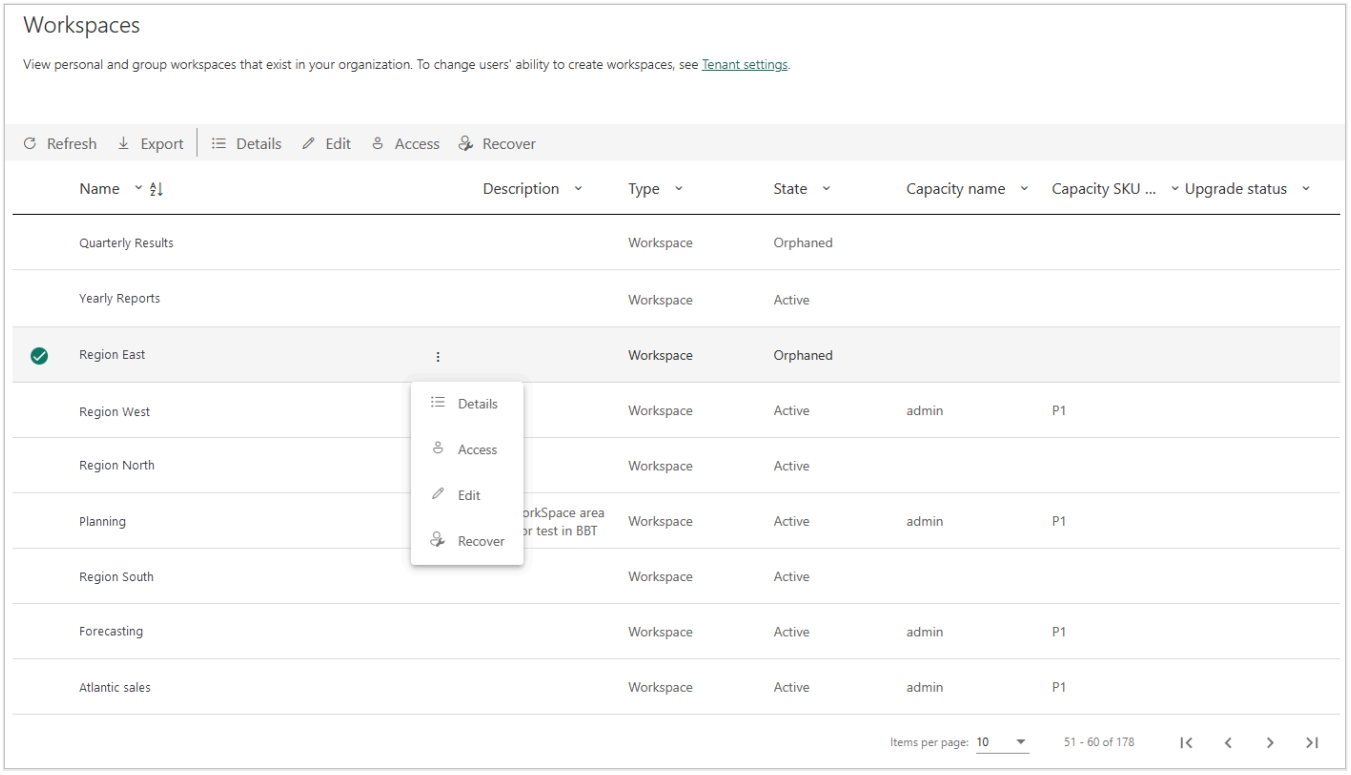
Provide product feedback | Ask the community

Manage workspaces

05/31/2025

As a Fabric administrator, you can govern the workspaces that exist in your organization on the **Workspaces** tab in the Admin portal. For information about how to get to and use the Admin portal, see About the Admin portal.

On the **Workspaces** tab, you see a list of all the workspaces in your tenant. Above the list, a ribbon provides options to help you govern the workspaces. These options also appear in the **More options (...)** menu of the selected workspace. The list of options varies depending on workspace type and status. All the options are described under workspace options.



The following table describes the columns of the list of workspaces.

Expand table

Column	Description
Name	The name given to the workspace.
Description	The information that is given in the description field of the workspace settings.
Type	The type of workspace. There are two types of workspaces: **Workspace** (also known as "app workspace") **Personal Group** ("My workspaces")

Column	Description
State	The state lets you know if the workspace is available for use. There are five states, **Active**, **Orphaned**, **Deleted**, **Removing**, and **Not found**. For more information, see Workspace states.
Capacity name	Name given to the workspace's capacity.
Capacity SKU Tier	The type of license used for the workspace's capacity. Capacity SKU Tiers include **Premium** and **Premium Per User (PPU)**. For more information about capacity tiers, see Configure and manage capacities in Premium.
Upgrade status	The upgrade status lets you know if the workspace is eligible for a Microsoft Fabric upgrade.

The table columns on the **Workspaces** tab correspond to the properties returned by the admin Rest API for workspaces. Personal workspaces are of type **PersonalGroup**, all other workspaces are of type **Workspace**. For more information, see Workspaces.

Workspace states

The following table describes the possible workspace states.

Expand table

State	Description
Active	A normal workspace. It doesn't indicate anything about usage or what's inside, only that the workspace itself is "normal".
Orphaned	A workspace with no admin user. You need to assign an admin.
Deleted	A deleted workspace. When a workspace is deleted, it enters a retention period. During the retention period, a Microsoft Fabric administrator can restore the workspace. See Workspace retention for detail. When the retention period ends, the workspace enters the *Removing* state.
Removing	At the end of a deleted workspace's retention period, it moves into the *Removing* state. During this state, the workspace is permanently removed. Permanently removing a workspace takes a short while, and depends on the service and folder content.
Not found	If the customer's API request includes a workspace ID for a workspace that doesn't belong to the customer's tenant, "Not found" is returned as the status for that ID.

Workspace options

The ribbon at the top of the list and the More options (...) menus of the individual workspaces provide options that to help you manage the workspaces. The Refresh and the Export options are always present, while the selection of other options that appear depends on the workspace type and status. All the options are described below.

Expand table

Option	Description
Refresh	Refreshes the workspace list.
Export	Exports the table as a *.csv* file.
Details	Lists the items that are contained in the workspace.
Edit	Enables you to edit the workspace name and description.
Access	Enables you to manage workspace access. You can use this feature to delete workspaces by first adding yourself to a workspace as an admin then opening the workspace to delete it.
Get access	Grants you temporary access to another user's MyWorkspace. See Gain access to any user's My workspace for detail.
Capacity	Enables you to assign the workspace to Premium capacity or to remove it from Premium capacity.
Recover	Enables you to restore an orphaned workspace.
Restore	Enables you to restore the MyWorkspace of a user that has left the organization, or a deleted collaborative workspace. For MyWorkspaces, see Restore a deleted My workspace as an app workspace. For collaborative workspaces, see Restore a deleted collaborative workspace
Permanently delete	Enables you to permanently delete a deleted collaborative workspace before the end of its retention period. See Permanently delete a deleted collaborative workspace during the retention period.

> **Note**
>
> Admins can also manage and recover workspaces using PowerShell cmdlets.
>
> Admins can also control users' ability to create new workspace experience workspaces and classic workspaces. See **Workspace settings** in this article for details.

Workspace item limits

Workspaces can contain a maximum of 1,000 Fabric and Power BI items. This includes both parent and child items.

Users attempting to create new items after this limit is reached get an error in the item creation flow. To develop a plan for managing item counts in workspaces, Fabric admins can review the total count of items per workspace in the admin monitoring workspace. See the total number of items in a workspace.

> **Note**
>
> If specific items have limits, those limits still apply, but the total number of items in the workspace is still capped at a 1000. For item specific limits, review the item type' documentation.

Workspace retention

By default, when a workspace is deleted, it isn't permanently and irrevocably deleted immediately. Instead, it enters a retention period during which it's possible to restore it. At the end of the retention period, it's removed permanently, and it will no longer be possible to recover it or its contents.

The retention period for personal workspaces (*My workspaces*) is 30 days.

The retention period for collaborative workspaces is configurable. The default retention period is seven days. However, Fabric administrators can change the length of the retention period by turning on the **Define workspace retention period** setting in the admin portal and specifying the desired retention period (from 7 to 90 days).

During the retention period, Fabric administrators can restore the workspace.

At the end of the retention period, the workspace is deleted permanently and it and its contents are irretrievably lost.

While a workspace is in the retention period, Fabric administrators can permanently delete it before the end of the retention period.

Configure the retention period for deleted collaborative workspaces

By default, deleted collaborative workspaces are retained for seven days. Fabric administrators can change the length of the retention period (from 7 to 90 days) using the **Define workspace retention period** tenant setting.

1. In the Fabric admin portal, go to **Workspace settings** > **Define workspace retention period**.
2. Turn on the setting and enter the number of days for desired retention period. You can choose anywhere from 7 to 90 days.
3. When done, select **Apply**.

> ⓘ **Note**
>
> When the **Define workspace retention period** setting is off, deleted collaborative workspaces automatically have a retention period of 7 days.
>
> This setting does not affect the retention period of *My workspaces*. *My workspaces* always have a 30-day retention period.

Restore a deleted collaborative workspace

While a deleted collaborative workspace is in a retention period, Fabric administrators can restore it and its contents.

1. In the Fabric admin portal, open the Workspaces page and find the deleted collaborative workspace you want to restore. Collaborative workspaces are of type *Workspace*. A workspace that is in a retention period has the status *Deleted*.
2. Select the workspace and then choose **Restore** from the ribbon, or select **More options (...)** and choose **Restore**.
3. In the Restore workspaces panel that appears, give a new name to the workspace and assign at least one user the Admin role in the workspace.
4. When done, select **Restore**.

Permanently delete a deleted collaborative workspace during the retention period

While a deleted collaborative workspace is in a retention period, Fabric administrators permanently delete it before the end of its retention period.

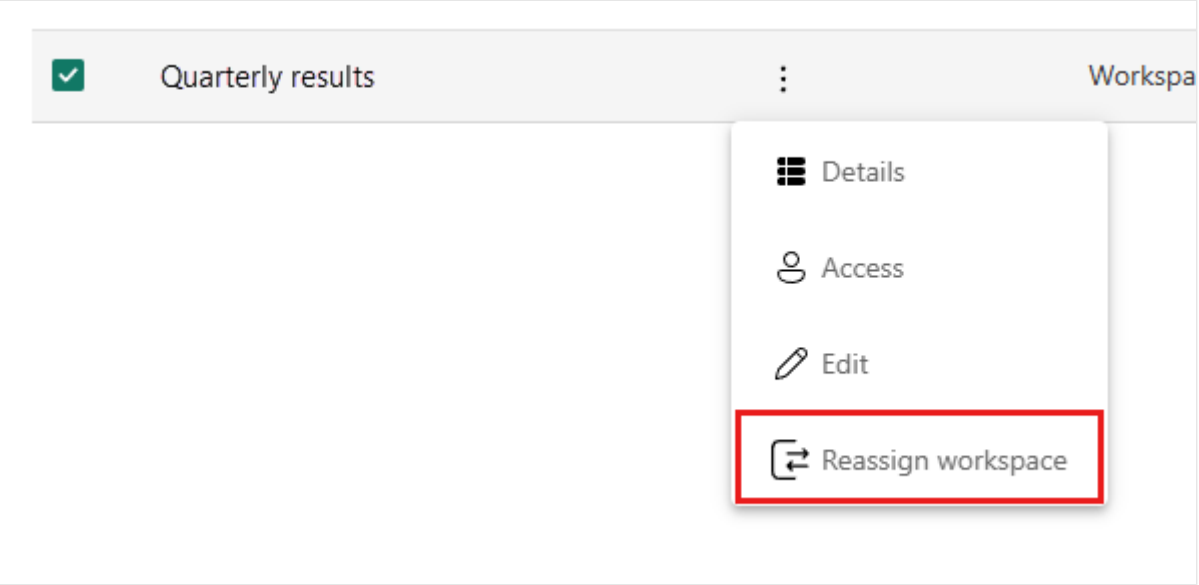
1. In the Fabric admin portal, open the Workspaces page and find the deleted collaborative workspace you want to restore. Collaborative workspaces are of type *Workspace*. A workspace that is in a retention period has the status *Deleted*.
2. Select the workspace and then choose **Permanently delete** from the ribbon, or select **More options (...)** and choose **Permanently delete**.

You're asked to confirm the permanent deletion. After you confirm, the workspace and its contents are no longer recoverable.

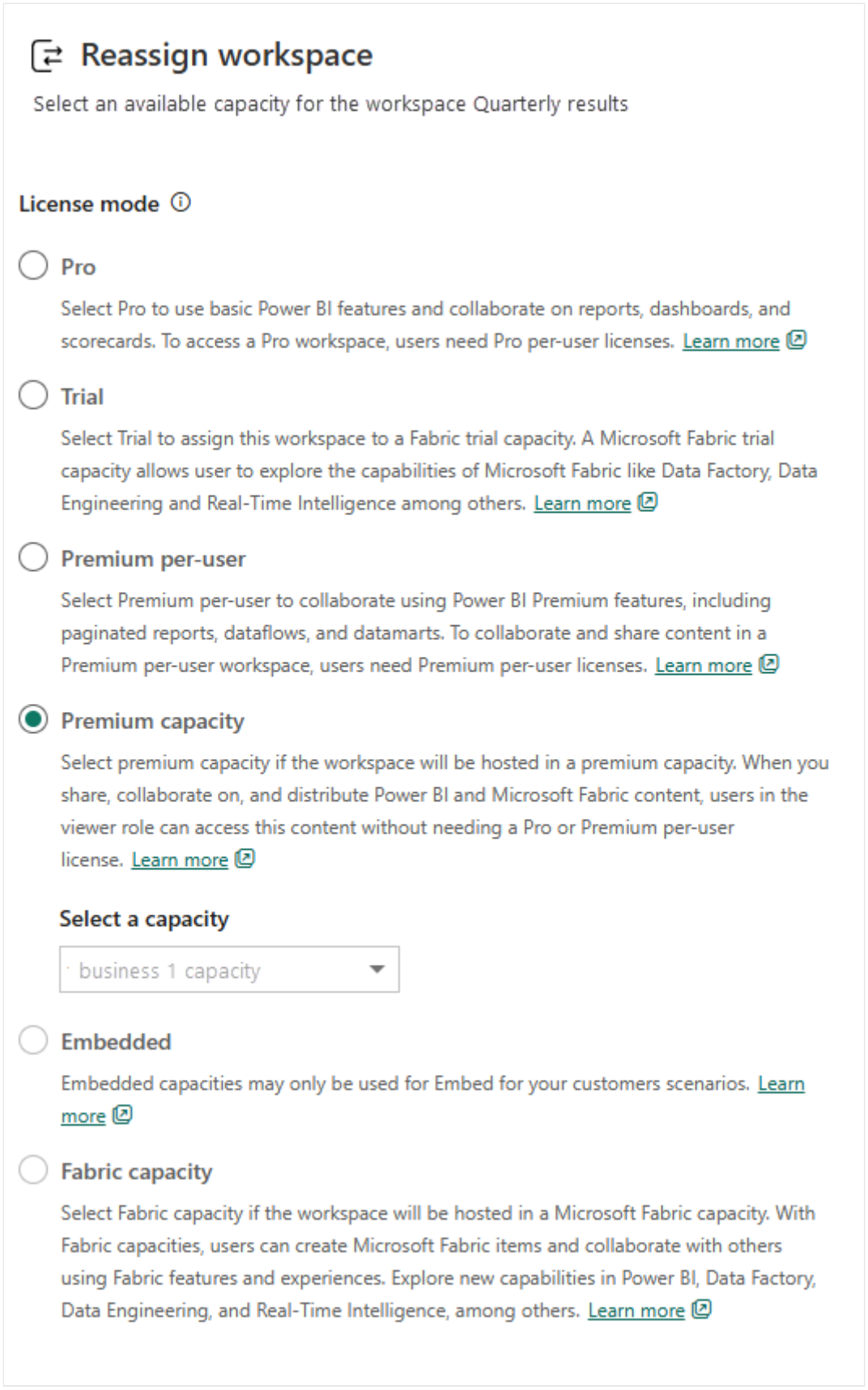
Reassign a workspace to a different capacity

Workspaces and the data they contain reside on capacities. You can move the workspace to a different capacity via the workspace license mode.

1. Go to **Admin portal** > **Workspaces**.
2. Find the workspace you want to move, open the options menu, and choose **Reassign workspace**.



3. On the Reassign workspace side pane that appears, select the desired license mode, and choose a capacity, if asked.



> **Note**
>
> The types of items contained in the workspace can affect the ability to change license modes and/or move the workspace to a capacity in a different region. See Moving data around for detail.

Govern My workspaces

Every Fabric user has a personal workspace called My workspace where they can work with their own content. While generally only My workspace owners have access to their My workspaces, Fabric admins can use a set of features to help them govern these workspaces. With these features, Fabric admins can:

- Gain access to the contents of any user's My workspace
- Designate a default capacity for all existing and new My workspaces
- Prevent users from moving My workspaces to a different capacity that might reside in noncompliant regions
- Restore deleted My workspaces as app workspaces

These features are described in the following sections.

Gain access to any user's My workspace

To gain access to a particular My workspace

1. In the Fabric Admin portal, open the Workspaces page and find the personal workspace you want to get access to.
2. Select the workspace and then choose **Get Access** from the ribbon, or select **More options (...)** and choose **Get Access**.

> **Note**
>
> Once access is obtained, the ribbon and the More options (...) menu will show **Remove Access** for the same My workspace. If you do not remove access by selecting one of these options, access will automatically be revoked for the admin after 24-hours. The My workspace owner's access remains intact.

Once you have access, the My workspace will show up in the list of workspaces accessible from the navigation pane. The icon  indicates that it's a My workspace.

Once you go inside the My workspace, you can perform any actions as if it's your own My workspace. You can view and make any changes to the contents, including sharing or unsharing. But you can't grant anyone else access to the My workspace.

Designate a default capacity for My workspaces

A Fabric admin or capacity admin can designate a capacity as the default capacity for My workspaces. To configure a default capacity for My workspaces, go to the details section in your capacity settings.

For details, see Designate a default capacity for My workspaces

Prevent My workspace owners from reassigning their My workspaces to a different capacity

Fabric admins can designate a default capacity for My workspaces. However, even if a My workspace has been assigned to Premium capacity, the owner of the workspace can still move it back to Pro license mode. Moving a workspace from Premium license mode to Pro license mode might cause the content contained in the workspace to be become noncompliant with respect to data-residency requirements, since it might move to a different region. To prevent this situation, the Fabric admin can block My workspace owners from moving their My workspace to a different license mode by turning on the **Block users from reassigning personal workspaces (My Workspace)** tenant setting. See Workspace settings for detail.

Restore a deleted My workspace as an app workspace

When users are deleted from the company's Active Directory, their My workspaces show up as Deleted in the State column on the Workspaces page in the Admin portal. Fabric admins can restore deleted My workspaces as app workspaces that other users can collaborate in.

During this restoration process, the Fabric admin needs to assign at least one Workspace admin in the new app workspace, as well as give the new workspace a name. After the workspace has been restored, it will show up as *Workspace* in the Type column on the Workspaces page in the Admin portal.

To restore a deleted My workspace as an app workspace

1. In the Fabric Admin portal, open the Workspaces page and find the deleted personal workspace you want to restore.
2. Select the workspace and then choose **Restore** from the ribbon, or select **More options (...)** and choose **Restore**.
3. In the Restore workspaces panel that appears, give a new name to the workspace and assign at least one user the Admin role in the workspace.
4. When done, select **Restore**.

After the deleted workspace has been restored as an app workspace, it's just like any other app workspace.

Moving data around

Workspaces and the data they contain reside on capacities, and can be moved around by assigning them to different capacities. Such movement might be to a capacity in the same region, or it might be to a capacity in a different region.

In the Fabric UI, workspaces can be moved to other capacities in the following ways:

- Fabric admins can reassign workspaces to a different capacity individually via the Workspaces page in the Fabric Admin portal.
- Fabric admins and capacity admins can reassign workspaces to a capacity in bulk via the **Workspaces assigned to this capacity** option in the capacity's settings.
- Workspace admins can reassign their workspace to a different capacity via the **License info option of the workspace settings**.

Restrictions on moving workspaces around

Moving workspaces from one capacity to another has the following restrictions:

- When you move a workspace, all jobs related to items in the workspace get canceled.

- Only movable item types can move between regions. **If you're reassigning a workspace to a capacity located in a different region, you must remove all non-movable items first, otherwise reassignment will fail**.

  The following items types are movable:
  - Report
  - Semantic model (small storage format)
  - Dashboard
  - Dataflow Gen1
  - Paginated Report
  - Datamart
  - Scorecard

  All other item types can't be moved between regions and must be removed from the workspace before you can migrate the workspace to a capacity in another region.

  After you've removed the non-movable items and the workspace is migrated to a different region, you can create new items of the non-movable type. It can take up to an hour after the migration before you will be able to do so.

- Only Power BI items can move from Premium capacity or Fabric capacity license mode to Pro or Premium Per User license mode (with exceptions as noted below). If you're

changing a workspace from Premium capacity or Fabric capacity license mode to Pro or Premium Per User license mode, you must remove all non-Power BI items and any Power BI items that can't be moved first, otherwise the license mode change will fail.

The following item types are considered Power BI items from the perspective of the workspace license mode.

- Report
- Semantic model (small storage format and large storage format)
- Dashboard
- Org app**
- Dataflow Gen1
- Paginated Report
- Metric set*
- Exploration**
- Datamart*
- Scorecard

*Can't move to Pro
**Can't move to Pro or Premium per user

All other item types must be removed from the workspace before you can change its license mode from Premium capacity or Fabric capacity to Pro or Premium Per User.

> **Note**
>
> If you have Dataflow Gen2 items in your workspace, note that their underlying staging lakehouse and staging warehouse items only become visible in the workspace UI after **all** Dataflow Gen2 items in the workspace have been deleted. These staging items are Fabric items as well, and as such their existance can prevent the workspace from being successfully migrated from one region to another. To ensure that your workspace can be successfully migrated across regions, first delete all Dataflow Gen2 items in the workspace, and then delete all the staging lakehouses and warehouses in the workspace that become visible.

Related content

- About the admin portal

Workspace tenant settings

06/01/2025

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Create workspaces

Workspaces are places where users collaborate on dashboards, reports, and other content. Microsoft Fabric admins can use the **Create workspaces** setting to designate which users in the organization can create workspaces. Admins can let everybody or nobody in an organization create workspaces. Workspace creation can also be limited to members of specific security groups. Learn more about workspaces.

List of workspaces

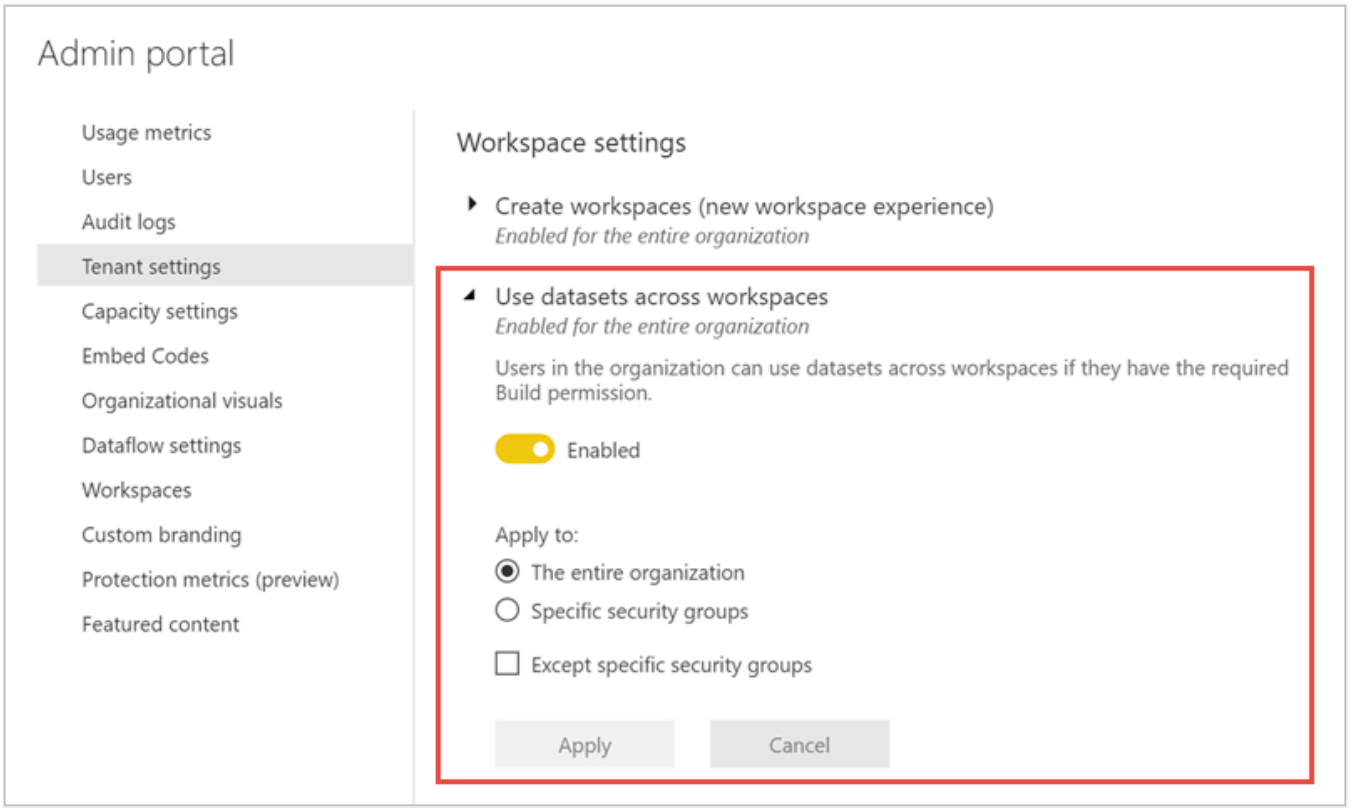
The admin portal has another section of settings about the workspaces in your tenant. In that section, you can sort and filter the list of workspaces and display the details for each workspace. See Manage workspaces for details.

Publish apps

In the admin portal, you also control which users have permissions to distribute apps to the organization. See Publish apps to the entire organization for details.

Use semantic models across workspaces

Admins can control which users in the organization can use semantic models across workspaces. When this setting is enabled, users still need the required Build permission for a specific semantic model.



For more information, see Intro to semantic models across workspaces.

Identify your workspace ID

The easiest way to find your workspace ID is in the URL of the Fabric site for an item in a workspace. As in Power BI, the Fabric URL contains the workspace ID, which is the unique identifier after `/groups/` in the URL, for example: `https://powerbi.com/groups/11aa111-a11a-1111-1abc-aa1111aaaa/...`. Alternatively, you can find the workspace ID in the Power BI Admin portal settings by selecting **Details** next to the workspace name.

Block users from reassigning personal workspaces (My Workspace)

Personal workspaces are the My workspaces that every user has for their personal content. Microsoft Fabric and capacity admins can designate a preferred capacity for My workspaces. By default, however, My workspace owners can still change the capacity assignment of their workspace. If a Microsoft Fabric or capacity admin designates a Premium capacity as the default capacity for My workspaces, but a My workspace owner then changes that capacity assignment back to shared capacity, this could result in non-compliance with data residency requirements.

To prevent such a scenario, the Microsoft Fabric admin can turn on the **Block users from reassigning personal workspaces (My Workspace)** tenant setting. When this setting is on, My

workspace owners can't change the capacity assignment of their My workspace.

To turn on the setting:

1. Go to the Microsoft Fabric Admin portal and select **Tenant settings**.
2. In the tenant settings, scroll down to the **Workspace settings** section.
3. Find the setting called **Block users from reassigning personal workspaces (My Workspace)**.

For more information, see Prevent My workspace owners from reassigning their My workspaces to a different capacity.

Related content

About tenant settings

Enable item certification

Article • 07/11/2024

Your organization can certify selected items to identify them an as authoritative sources for critical information. Currently, all Fabric items except Power BI dashboards can be certified.

As a Fabric admin, you're responsible for enabling and setting up the certification process for your organization. This means:

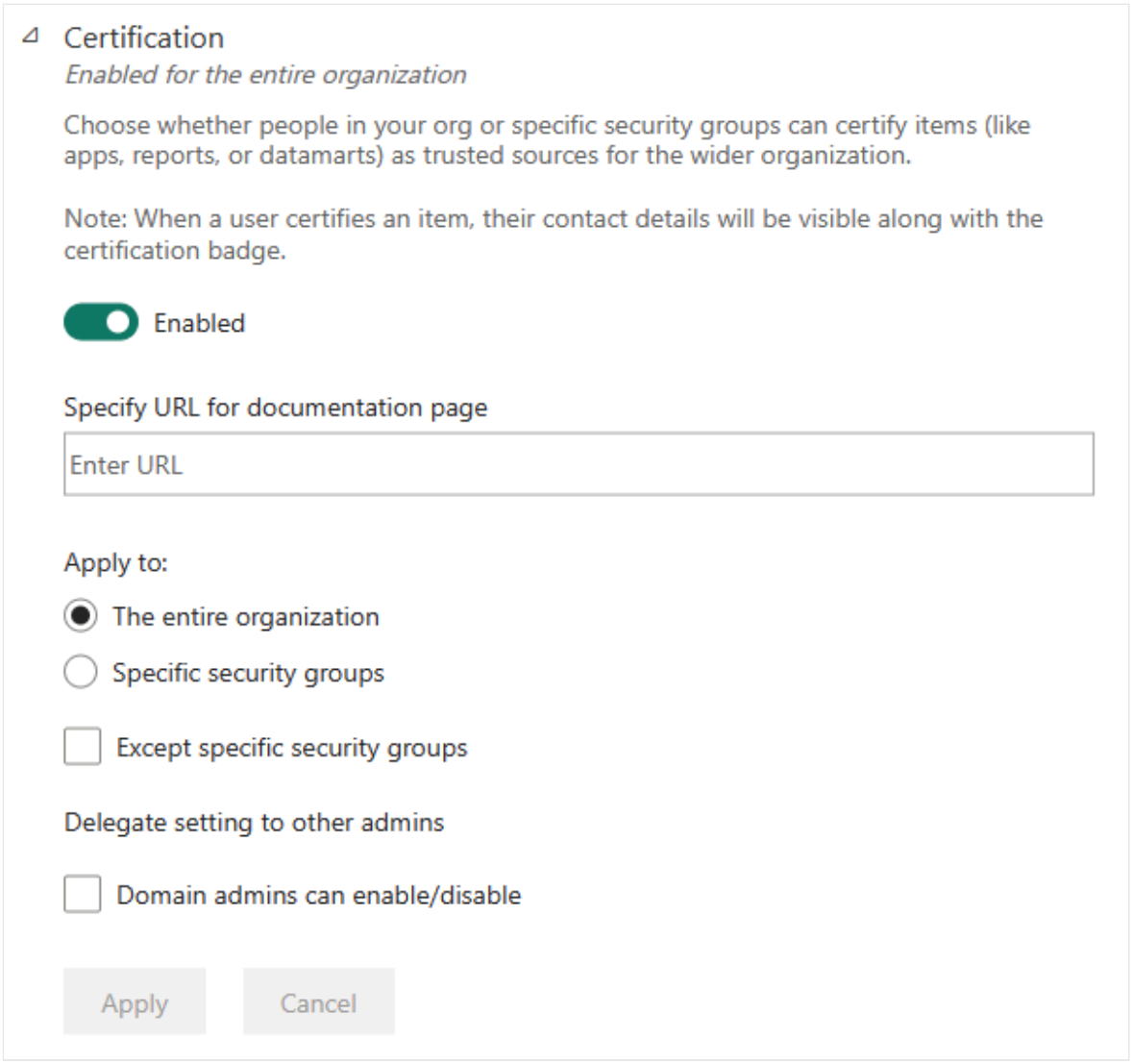
- Enabling certification on your tenant.
- Defining a list of security groups whose members will be authorized to certify items.
- Providing a URL that points to the documentation for the organization's item certification process, if such documentation exists.
- Deciding whether to delegate certification setup to domain administrators, so that they can set up certification specifically for their domain. When you delegate certification setup to domain administrators, the administrators of each domain can override any or all tenant-level certification settings, including enable/disable, for their domain.

Certification is part of Power BI's *endorsement* feature. For more information, see the endorsement overview.

Enable item certification

1. In the Admin portal, go to Tenant settings.

2. Under the Export and sharing settings section, expand the Certification section.



3. Set the toggle to **Enabled**.

4. If your organization has a published certification policy, provide its URL here. This becomes the **Learn more** link in the certification section of the endorsement settings dialog. If you don't supply a link, users who want to request certification of their item will be advised to contact their Fabric administrator.

5. Specify one or more security groups whose members will be authorized to certify items. These authorized certifiers will able to use the Certification button in the certification section of the endorsement settings dialog. This field accepts security groups only. You can't enter named users.

   If a security group contains subsecurity groups that you don't want to give certification rights to, you can check the **Except specific security groups** box and enter the names of those groups in a text box that will appear.

6. Check the **Domain admins can enable/disable** checkbox if you want domain administrators to be able to override any or all tenant-level certification settings.

> **Note**
>
> Selecting the checkbox enables domain admins to override any or all tenant-level certification settings, including enable/disable, even though the checkbox description only mentions enable/disable.

7. Select **Apply**.

Related content

- Read about endorsement in Fabric
- Enable master data endorsement
- Promote Fabric items
- Certify Fabric items

Feedback

Enable master data endorsement

Article • 07/11/2024

This article describes how to enable master data endorsement. Its target audience is Fabric administrators.

Master data endorsement is a way organizations can help its Fabric users find and use data that the organization regards as core, single-source-of-truth data, such as customer lists, product codes, etc. This is accomplished by qualified users applying a **Master data** badge to data items that they judge to contain that core, single-source-of-truth data.

As a Fabric administrator, you're responsible for enabling master data endorsement in your organization and specifying who in the organization is qualified to designate data items as master data.

For more information about endorsement and master data, see Endorsement overview.

Prerequisites

You must be a Fabric administrator to enable master data endorsement.

Enable master data endorsement

To enable master data endorsement, turn on the **Endorse master data (preview)** tenant setting and specify who is authorized to apply the **Master data** badge to data items.

1. Open the admin portal and go to the tenant settings.
2. Find and expand the **Endorse master data (preview)** tenant setting.
3. Switch the toggle to **Enabled**.
4. Specify who can apply the **Master data** badge to data items by choosing the appropriate options:
    - **The entire organization**: Everyone in the organization is authorized to apply the master data badge to data items.
    - **Specific security groups**: Only members of the specified security groups are authorized to apply the **Master data** badge to data items.
    - **Exclude specific security groups**: If you want to exclude particular users who are included in the option you chose, select the **Exclude specific security**

groups checkbox and provide the names of a security group or groups that include the users you want to exclude.

> **Note**
>
> Users who are authorized to apply the **Master data** badge must also have write permission on data items they wish to apply the badge to.

Related content

- Endorsement overview
- Enable item certification
- Endorse items
- Governance documentation

Feedback

Configure notifications

Article • 11/02/2023

Power BI Premium allows you to configure email notifications for your capacity. The emails are sent to the people you specify in the notifications settings.

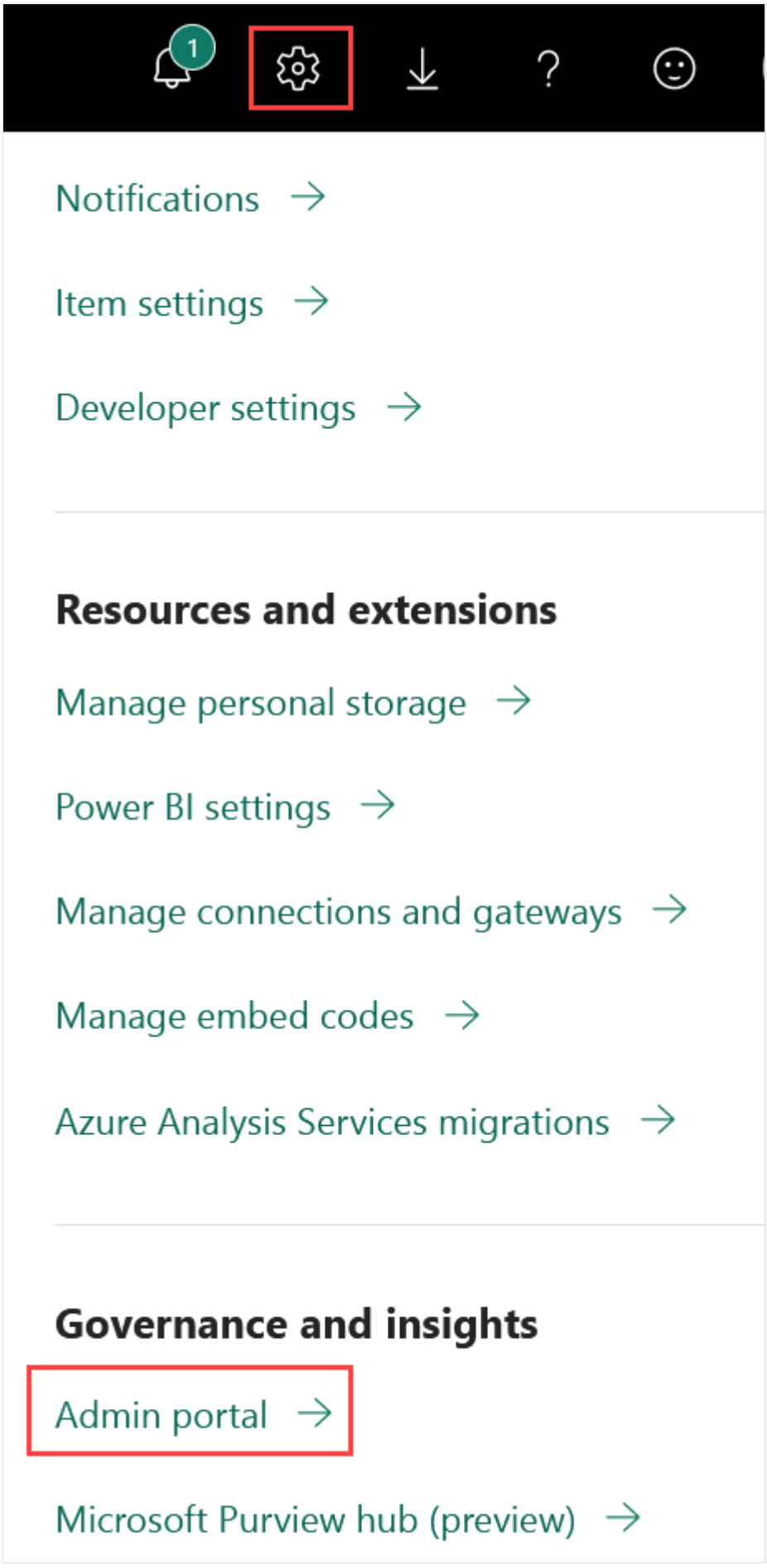
To calculate when to send emails, Power BI checks the capacity every 15 minutes. During the check, the last 15 to 30 minutes of capacity activity are examined.

> **Note**
>
> To configure email notifications, you must be a capacity administrator.

Configure capacity notifications

To configure the capacity notification emails, follow these steps:

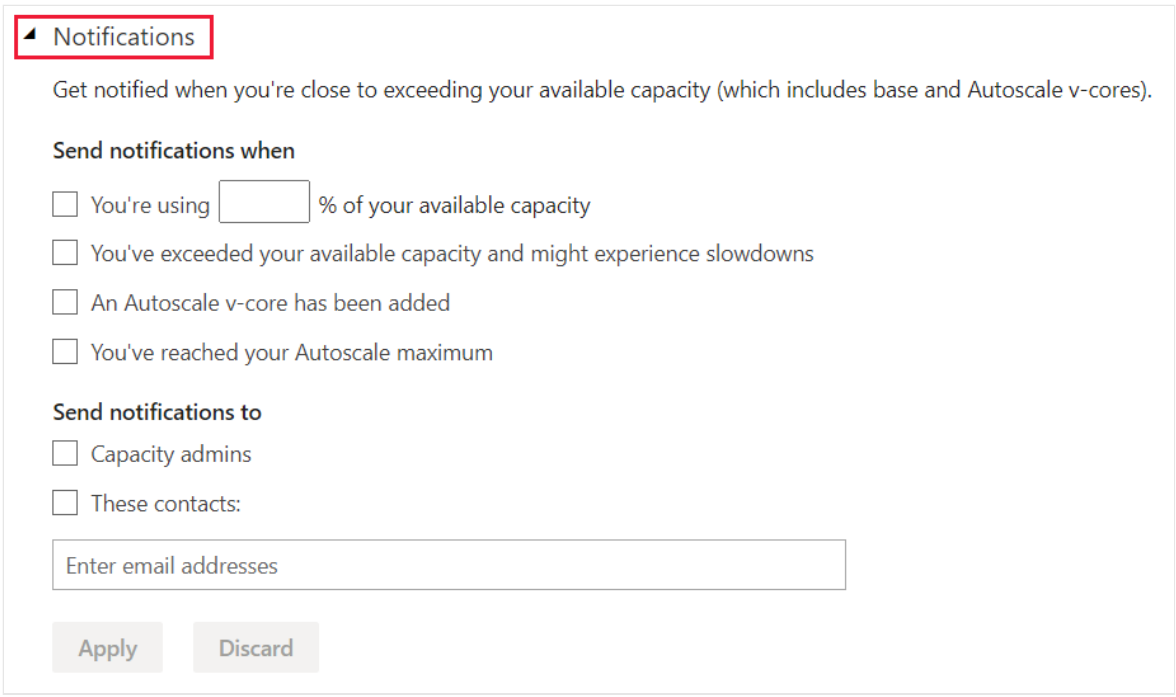
1. In the Power BI service, go to **Settings** > **Settings** > **Admin portal**.



2. In the *Admin portal*, select **Capacity settings**.

3. Select the capacity you want to configure notifications for.

4. Expand the **Notifications** section.



5. In the section **Send notifications when**, configure your required notifications as follows:

   - **You're using ___% of your available capacity** - A notification is sent after the capacity reaches the threshold you enter.
   - **You've exceeded your available capacity and might experience slowdowns** - A notification is sent after you reach your capacity limit. After the limit is reached, if you have autoscale enabled, autoscale starts. If you don't have autoscale enabled, throttling is applied to your capacity.
   - **An Autoscale v-core has been added** - A notification is sent after autoscale starts and every time a v-core is added.
   - **You've reached your Autoscale maximum** - A notification is sent when all the autoscale v-cores are fully utilized. Throttling is applied to your capacity if it continues to be overloaded.

6. In the section **Send notifications to**, select who you want the notifications to be emailed to:

   - **Capacity admins** - Email notifications are sent to all the admins of this capacity.
   - **These contacts** - Enter the emails of the contacts you want to receive notifications.

7. Select **Apply**.

Considerations and limitations

- Timestamps aren't included in notification emails.
- Notification emails don't list by how much a threshold was crossed.
- After a notification is sent, there's a three hour period in which new notifications won't be sent, even if your capacity crosses thresholds that are set to trigger these notifications. For example, if you configure your capacity to send a notification after you cross the 75% usage threshold, after that threshold is met you'll receive a notification. If the capacity goes below this threshold to 60%, and then right back over it in the next hour, you won't get another notification for crossing the 75% mark. If you have the autoscale notification turned on, and your capacity crosses the 100% threshold during these three hours, you get a notification that autoscale started.
- A 30-seconds window is applied to calculate your capacity usage. Due to a less granular calculation, capacity usage might appear differently in the Power BI Premium utilization and metrics app. As a result, you might not see the event your notification points to in the app. For example, a short spike in capacity activity that triggers a notification might not be seen at all in the Power BI Premium utilization and metrics app.

Next steps

- What is Power BI Premium?
- What is Microsoft Fabric admin?

Feedback

Set up metadata scanning in your organization

Article • 02/27/2025

Before metadata scanning can be run over an organization's Microsoft Fabric workspaces, it must be set up by a Fabric administrator. Setting up metadata scanning involves two steps:

1. Enabling service principal authentication for read-only admin APIs.
2. Enabling tenant settings for detailed semantic model metadata scanning.

Enable service principal authentication for read-only admin APIs

Service principal is an authentication method that can be used to let a Microsoft Entra application access Power BI APIs. With this authentication method, you don't have to maintain a service account with an admin role. Rather, to allow your app to use the Admin APIs, you just have to give your approval once as part of the tenant settings configuration.

To see how to enable service principal access to read-only Admin APIs, see Enable service principal authentication for read-only admin APIs.

If you don't want to enable service principal authentication, metadata scanning can be performed with standard delegated admin access token authentication.

Enable tenant settings for metadata scanning

Two tenant settings control metadata scanning:

- **Enhance admin APIs responses with detailed metadata**: This setting turns on Model caching and enhances API responses with low-level semantic model metadata (for example, name and description) for tables, columns, and measures.
- **Enhance admin APIs responses with DAX and mashup expressions**: This setting allows the API response to include DAX expressions and Mashup queries. This setting can only be enabled if the first setting is also enabled.

To enable these settings, go to **Admin portal** > **Tenant settings** > **Admin API settings**.

Related content

- Metadata scanning overview
- Enable service principal authentication for admin APIs
- Run metadata scanning
- Power BI REST Admin APIs

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Enable service principal authentication for admin APIs

This article shows how to enable service principal authentication for Power BI *read-only* admin APIs and Microsoft Fabric *update* admin APIs.

Service principal is an authentication method that can be used to let a Microsoft Entra application access Microsoft Fabric content and APIs.

When you create a Microsoft Entra app, a service principal object is created. The service principal object, also known simply as the service principal, allows Microsoft Entra ID to authenticate your app. Once authenticated, the app can access Microsoft Entra tenant resources.

Enable service principal authentication

To enable service principal authentication for Fabric APIs, follow these steps:

1. Create a Microsoft Entra app. You can skip this step if you already have a Microsoft Entra app you want to use. Take note of the app ID, which you need in later steps.

   > **Important**
   >
   > Make sure the app you use doesn't have any admin-consent required permissions for Fabric set on it in the Azure portal. See how to check whether your app has any such permissions.

2. Create a new Microsoft Entra Security Group and make sure to select **Security** as the Group type. You can skip this step if you already have a Microsoft Entra security group you'd like to use.

3. Add your app ID as a member of the security group you created. To do so:
   a. Navigate to **Azure portal** > **Microsoft Entra ID** > **Groups**, and choose the security group you created in *Step 2*.
   b. Select **Add Members**.

4. Enable the Fabric admin settings:
   a. Sign in to the Fabric admin portal. You need to be a Fabric admin to see the tenant settings page.
   b. Under **Admin API settings**, select the switch for the type of admin APIs you want to enable:

- **Service principals can access read-only admin APIs** (see supported Power BI admin APIs)
- **Service principals can access admin APIs used for updates** (see supported Fabric admin APIs)

5. Set the toggle to **Enabled**.

6. Select the **Specific security groups** radio button. In the text field that appears below it, add the security group you created in *Step 2*.

7. Select **Apply**.

Supported Power BI admin APIs for read-only

Service principal authentication is currently supported for the following read-only admin APIs.

- GetGroupsAsAdmin with $expand for dashboards, semantic models, reports, and dataflows
- GetGroupUsersAsAdmin
- GetDashboardsAsAdmin with $expand tiles
- GetDashboardUsersAsAdmin
- GetAppsAsAdmin
- GetAppUsersAsAdmin
- GetDatasourcesAsAdmin
- GetDatasetToDataflowsLinksAsAdmin
- GetDataflowDatasourcesAsAdmin
- GetDataflowUpstreamDataflowsAsAdmin
- GetCapacitiesAsAdmin
- GetCapacityUsersAsAdmin
- GetActivityLog
- GetModifiedWorkspaces
- WorkspaceGetInfo
- WorkspaceScanStatus
- WorkspaceScanResult
- GetDashboardsInGroupAsAdmin
- GetTilesAsAdmin
- ExportDataflowAsAdmin
- GetDataflowsAsAdmin
- GetDataflowUsersAsAdmin
- GetDataflowsInGroupAsAdmin
- GetDatasetsAsAdmin
- GetDatasetUsersAsAdmin

- GetDatasetsInGroupAsAdmin
- Get Power BI Encryption Keys
- Get Refreshable For Capacity
- Get Refreshables
- Get Refreshables For Capacity
- GetImportsAsAdmin
- GetReportsAsAdmin
- GetReportUsersAsAdmin
- GetReportsInGroupAsAdmin

How to check if your app has admin-consent required permissions

An app using service principal authentication that calls read-only admin APIs **must not** have any admin-consent required permissions for Power BI set on it in the Azure portal. To check the assigned permissions:

1. Sign into the **Azure portal**.
2. Select **Microsoft Entra ID**, then **Enterprise applications**.
3. Select the application you want to grant access to Power BI.
4. Select **Permissions**. There must be no admin-consent required permissions of type Application registered for the app.

Supported Fabric admin APIs for updates

The **Service principals can access admin APIs used for updates** setting applies to Fabric admin APIs, such as the Workspaces - Restore Workspace API.

To find out if a specific Fabric admin API supports service principal authentication, check the API's documentation in the Microsoft Fabric REST API reference. Look for the "Microsoft Entra supported identities" section, which indicates whether service principal authentication is supported.

Considerations and limitations

- The service principal can make rest API calls, but you can't open Fabric with service principal credentials.

- Fabric admin rights are required to enable service principal in the Admin API settings in the Fabric admin portal.

Related content

- Metadata scanning overview
- Set up metadata scanning
- Run metadata scanning

Last updated on 11/21/2025

Configure Multi-Geo support for Fabric

09/19/2025

Multi-Geo is a Microsoft Fabric feature that helps multinational customers address regional, industry-specific, or organizational data residency requirements. As a Fabric customer, you can deploy content to data centers in regions other than the home region of the Fabric tenant. A geo (geography) can contain more than one region. For example, the United States is a geo, and West Central US and South Central US are regions in the United States. You might choose to deploy content to any of the following geographies (geos) defined in the Azure geography map .

- Sovereign clouds support Multi-Geo across regions within that cloud.
- China North doesn't support Multi-Geo.
- Power BI Embedded supports Multi-Geo.
- Power BI Premium Per User (PPU) isn't supported for Multi-Geo.

Enable and configure

Enable Multi-Geo by selecting a region other than the default region when you're creating a new capacity. Once a capacity's created, it shows the region where it's currently located.

After you create a capacity, it remains in that region, and any workspaces created under it will have their content stored in that region.

Follow these steps to change the default capacity region when you're creating a new capacity.

Power BI Premium

1. In Fabric, select **settings** (⚙) and from the menu select **Admin portal**.
2. In the *Admin portal*, select **Capacity settings**.
3. Select **Set up new capacity**.
4. From the **Region** dropdown menu, select the region you want to use for this capacity.

Move workspaces between capacities

Follow the steps below to move workspaces from one capacity to another in the same region. During migration, certain operations might fail, such as publishing new semantic models or scheduled data refresh.

When you're performing a migration, don't delete or pause either the source or destination workspace capacities. Deleting or pausing a capacity during migration, can result in missing items. If you deleted or paused your capacity before the migration is finished and you have missing items in the migrated workspace, try migrating the workspace again.

1. Open the workspace settings.
2. From the side bar, select **License info**.
3. From the **License capacity** dropdown menu, select the capacity you want to move the workspace to.

Change the region of your existing content

To change the region for existing content, do one of the following:

- Create a new capacity and move your workspaces to the new capacities. Free users won't experience any downtime as long as the tenant has spare v-cores.
- Temporarily move your content to a shared capacity. You don't need extra v-cores, but free users will experience some downtime. After you create a new capacity in the desired region, move your workspaces to the new capacity.

Move content to your home region

To move workspaces to your home region, do one of the following:

- Delete the current capacity where the workspace is located. Workspaces in the deleted capacity are moved to a shared capacity in the home region.
- Move individual workspaces to a capacity located in the home tenant.

Large-storage format semantic models shouldn't be moved from the region where they were created. Reports based on a large-format semantic model won't be able to load the semantic model and will return a *Cannot load model* error. Move the large-storage format semantic model back to its original region to make it available again.

Considerations and limitations

- Confirm that any movement you initiate between regions follows all corporate and government compliance requirements prior to initiating data transfer.

- When you're using Multi-Geo, the following items are stored in the region that isn't your home region:
  - SQL databases
  - Models (*.ABF* files) for import and DirectQuery semantic models
  - Query cache
  - R images

  These items remain in the home region of the tenant:
  - Push datasets
  - Dashboard/report metadata: tile names, tile queries, and any other data
  - Service buses for gateway queries or scheduled refresh jobs
  - Permissions
  - Semantic model credentials
  - Power BI Embedded Analytics Playground saved state
  - Metadata linked to Purview Data Map

- Cached data and queries stored in a remote region stays in that region at rest. Additionally, the data at rest is replicated to another region in the same Azure geography for disaster recovery if the Azure geography contains more than one region. Data in transit might go back and forth between multiple geographies.

- When moving data from one region to another, the source data might remain in the region from which the data was moved for up to 30 days. During that time end users don't have access to it. The data is removed from this region and destroyed during the 30-day period.

- Query text and query result traffic for imported and DirectQuery data models doesn't transit through the home region. However, the report metadata comes from the home region, and certain DNS routing states might take such traffic out of the region.

- Certain features such as screenshots, data alerts and others process data in the home region.

- The detailed semantic model metadata that is cached as part of enhanced metadata scanning is always stored in the home region, even if the scanned semantic model is located in a remote region.

- Detailed semantic model metadata lives in the home tenant.

- To use dataflows gen1 on Multi-Geo you must configure dataflow storage to use Azure Data Lake Storage (ADLS) Gen2.
- It's possible to create and maintain large-storage format semantic models in remote regions to meet data residency requirements. However, you can't move storage format semantic models to another region. Moving large-storage format semantic models from the region where they were created results in reports failing to load the semantic model. Move the large-storage semantic model back to its original region to make it available. If you must move such a model, deploy it as if it was a new model, and then delete the old model from the undesired region.
- Multi-Geo doesn't support Metrics in Power BI.
- Workspaces with non-Power BI Fabric items can't be moved between regions. You must delete all the non-Power BI Fabric items before moving a workspace to a different region. Once the workspace is moved, it can take up to 30 minutes before non-Power BI items can be created.

For more details, see Moving data around.

Related content

- What is Power BI Premium?
- Multi-Geo support for Power BI Embedded
- Moving data around

About tenant settings

08/22/2025

Tenant settings enable fine-grained control over the features that are made available to your organization. If you have concerns around sensitive data, some of our features might not be right for your organization, or you might only want a particular feature to be available to a specific group.

Tenant settings that control the availability of features in the Power BI user interface can help to establish governance policies, but they're not a security measure. For example, the **Export data** setting doesn't restrict the permissions of a Power BI user on a semantic model. Power BI users with read access to a semantic model have the permission to query this semantic model and might be able to persist the results without using the **Export data** feature in the Power BI user interface.

For a list and brief description of all the tenant settings, see the tenant settings index.

> **Note**
>
> It can take up to 15 minutes for a setting change to take effect for everyone in your organization.

New tenant settings

To help you quickly identify changes and respond, a message at the top of the tenant settings page appears when there's a change. The message lists new tenant settings and changes to existing ones.

You can identify new settings according to their *new* icon.

How to get to the tenant settings

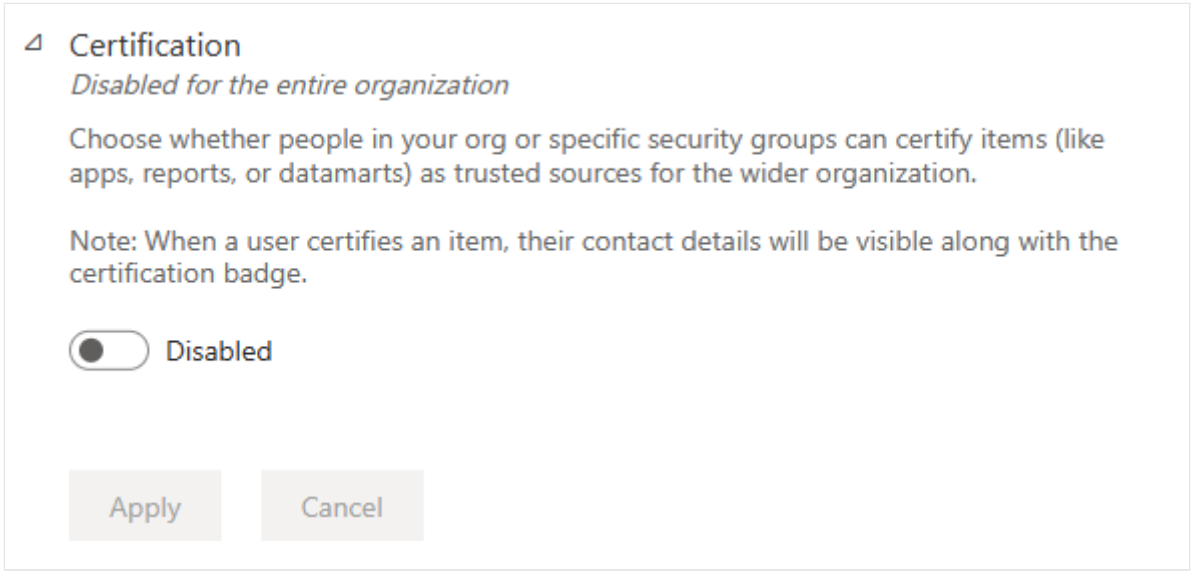
To get to the tenant settings:

1. Select the settings (gear) icon at the top of the Fabric portal.
2. In the side pane that appears, select **Admin portal** under the **Governance and insights** heading.
3. The admin portal opens. Select **Tenant settings**.

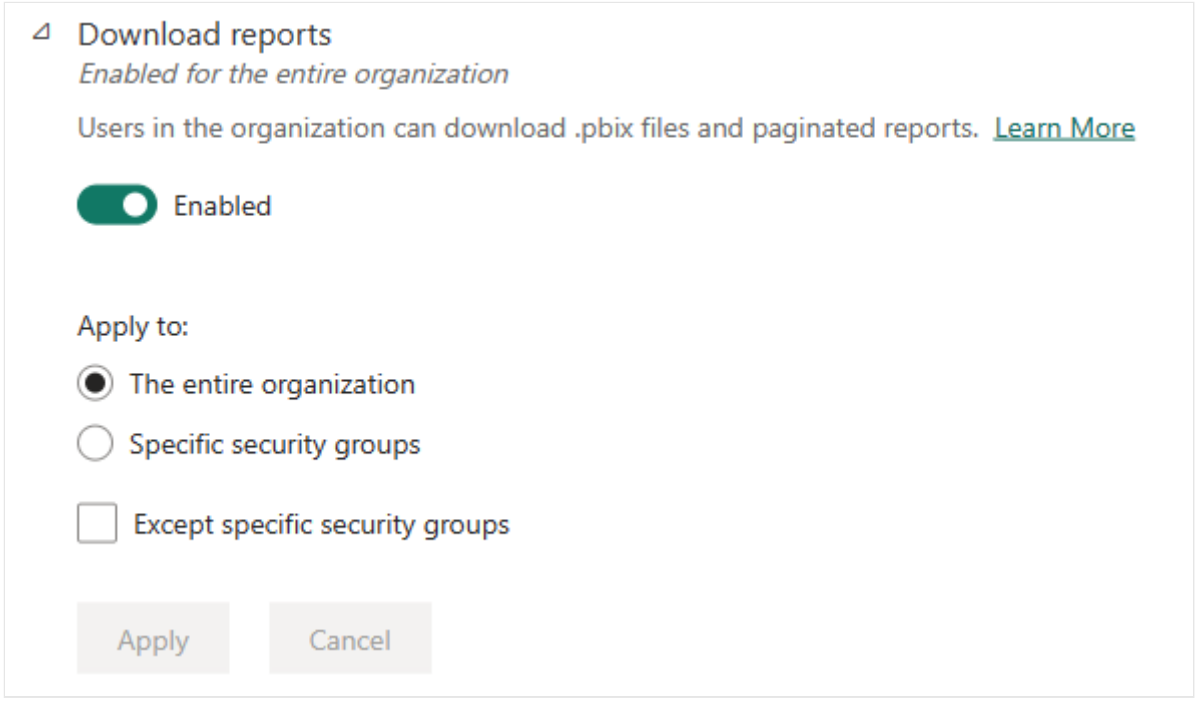
How to use the tenant settings

Many of the settings can have one of three states:

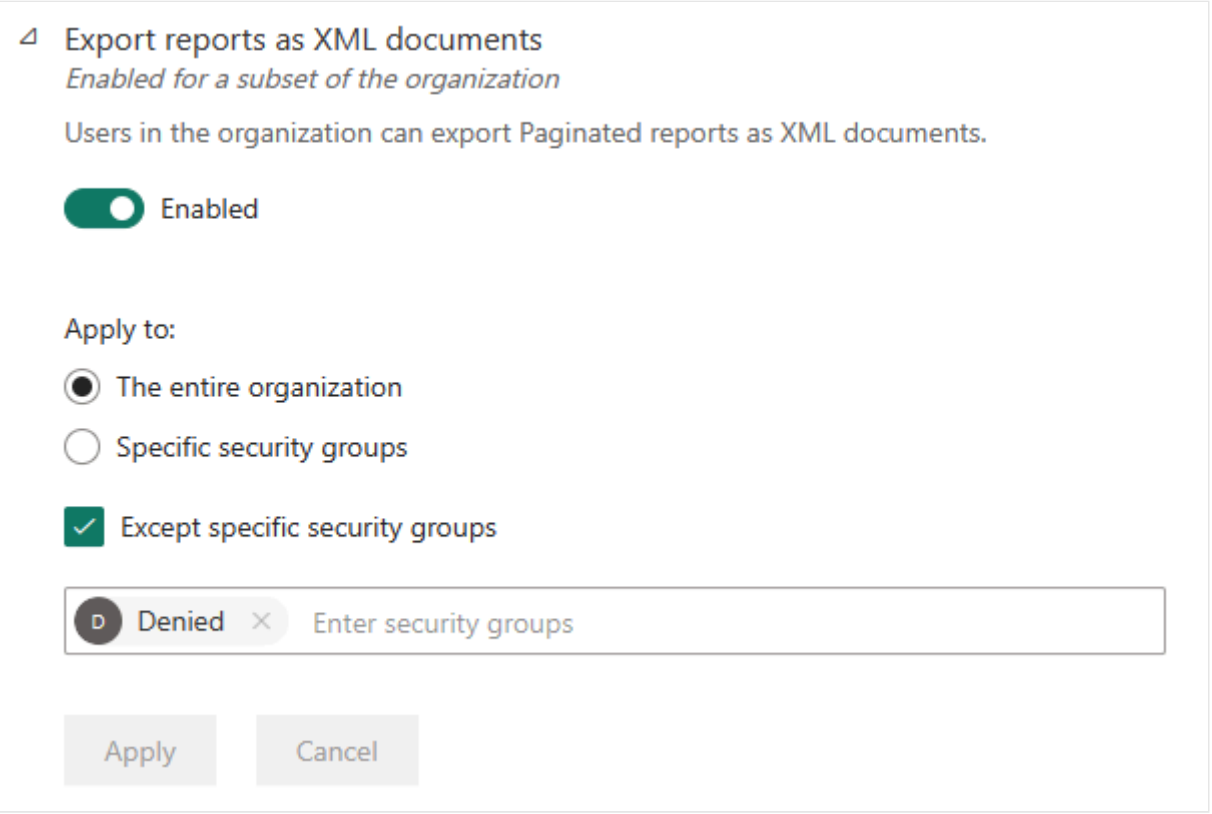
- **Disabled for the entire organization**: No one in your organization can use this feature.



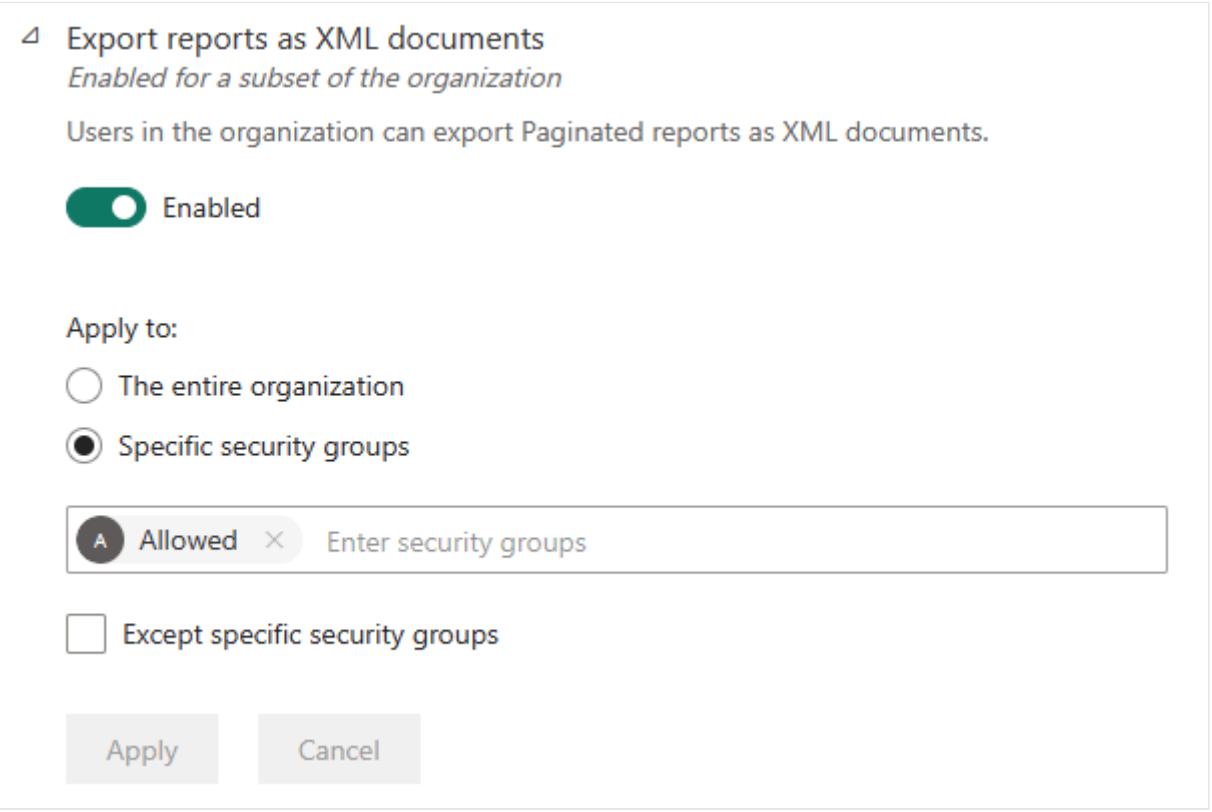
- **Enabled for the entire organization**: Everyone in your organization can use this feature.



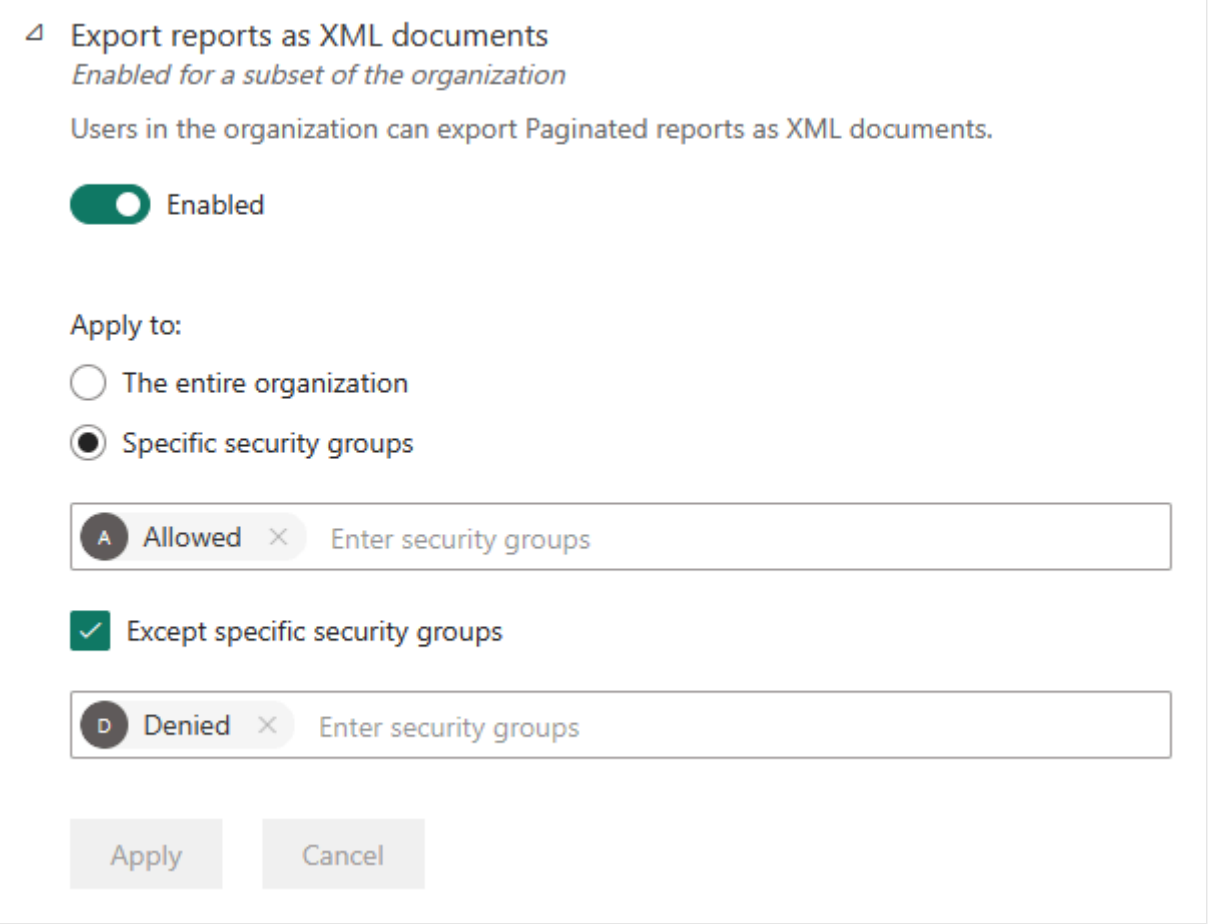
- **Enabled for the entire organization except for certain groups**: Everyone in your organization can use this feature except for users who belong to the specified groups.



- **Enabled for a subset of the organization**: Specific security groups in your organization are allowed to use this feature.



- **Enabled for specific groups except for certain groups**: Members of the specified security groups are allowed to use this feature, unless they also belong to an excluded group. This approach ensures that certain users don't have access to the feature even if they're in the allowed group. The most restrictive setting for a user applies.



Related content

- Use the Fabric REST API to list tenant settings
- What is the admin portal?
- Tenant settings index

Delegate tenant settings

Article • 04/21/2024

Microsoft Fabric allows organizations to delegate settings from the tenant to the capacity, and from the capacity to workspaces. Delegation allows the organization to give admins control over specific settings relevant to their area of responsibility. Delegation prevents centralized admins from becoming a bottle neck for teams across the organization that require control over specific settings.

Here are some key concepts related to delegating settings in Fabric:

- Tenant Settings - Global settings controlled by tenant administrators that impact the entire tenant.
- Domain - A logical grouping of workspaces aimed at facilitating data mesh architecture.
- Capacity - A dedicated compute resource. Capacity admins can delegate settings concerning the performance and consumption of compute resources.
- Workspace - Collaborative environments where Fabric items are stored and shared. Certain tenant settings can be delegated to workspaces through a domain or a capacity.

Domain, capacity and workspace admins can override tenant settings. Overriding tenant settings allows admins to modify their environment to meet specific requirements. When a setting is adjusted in a domain or capacity, it affects only the workspaces linked to those administrative units. Similarly, changes to a workspace impact only the items stored within that workspace.

Delegation design

A setting can be delegated either through domains or capacities, but not both. This ensures clarity in governance and prevents conflicts in the management of settings.

After delegating to a domain or capacity, certain settings can be further delegated to workspaces. This allows for finer granularity in control, empowering workspace owners to customize the settings to their requirements. Tenant admins can bypass domain and capacity admins and delegate directly to workspaces.

Delegate settings to workspaces

Follow these steps to delegate settings to workspaces:

1. Delegate tenant settings to a capacity or a domain.
2. Locate the setting you want to delegate to a workspace in your domain or capacity.
3. Select the option to delegate to a workspaces. Some settings can't be delegated to workspaces. In such cases, there isn't an option to delegate to a workspace.
4. Select **Apply**

Audit your delegated settings

The following activity events represent tenant setting changes:

- **UpdatedAdminFeatureSwitch** - Tenant delegation changes.
- **UpdateCapacityTenantSettingDelegation** - Capacity delegation changes.
- **UpdateDomainTenantSettingDelegation** - Domain delegation changes.
- **UpdateWorkspaceTenantSettingDelegation** - Workspace delegation changes.

Related content

- What is the admin monitoring workspace?
- Workspace tenant settings
- Manage workspaces

Tenant settings index

This article lists all Fabric tenant settings, along with a brief description of each, and links to relevant documentation, if available. For more information about tenant settings in general, see About tenant settings.

If you want to get to the tenant settings in the Fabric portal, see How to get to the tenant settings.

Microsoft Fabric

Expand table

Setting name	Description
Users can create Fabric items	Users can use production-ready features to create Fabric items. Turning off this setting doesn't impact users' ability to create Power BI items. This setting can be managed at both the tenant and the capacity levels. Learn More
Digital Twin Builder (preview)	Users can create digital twin builder items to build comprehensive digital twins of real world environments and processes, to enable big-picture data analysis and drive operational efficiency.
Enable Ontology item (preview)	Users can create ontologies to unify enterprise semantics across data, models and logic to operationalize decision intelligence with context-aware AI agents.
Users can discover and create org apps (preview)	Turn on this setting to let users create org apps as items. Users with access will be able to view them. By turning on this setting, you agree to the Preview Terms . If turned off, any org app items created will be hidden until this setting is turned on again. The prior version of workspace apps will still be available. Learn More
Product Feedback	This setting allows Microsoft to prompt users for feedback through in-product surveys within Microsoft Fabric and Power BI. Microsoft will use this feedback to help improve product features and services. User participation is voluntary. Learn More
Users can create and share Data agent item types (preview)	Users can create natural language data question and answer (Q&A) experiences using generative AI and then save them as Data agent items. Data agent items can be shared with others in the organization. Learn More
User can create Graph (preview)	Visualize your data with a Graph to drive deeper insights and reveal richer context at lightning speed. Learn More

Setting name	Description
Users can be informed of upcoming conferences featuring Microsoft Fabric when they are logged in to Fabric	Attending conferences can help your data teams learn in-depth about how to best use the Fabric platform for your business needs and build professional relationships with community members, Microsoft engineering and product teams, and the Fabric Customer Advisory Team (CAT). These conferences may be organized and hosted by third parties. Learn More
ML models can serve real-time predictions from API endpoints (preview)	With this setting on, users can get real-time predictions from model and version endpoints. Even with real-time endpoints turned off, batch predictions can still be generated. Learn More
Detect anomalies in Real-Time Intelligence (Preview)	This setting allows users to use statistical detection algorithms to detect anomalies in real-time data. Learn More
Users can create Maps (preview)	Users can build map items to analyze live geospatial data with interactive, real-time visualizations, helping uncover location-based insights.
Enable Operations Agents (Preview)	Users can create operations agents, which use Azure OpenAI to create operations plans and recommend actions to users in your organization in response to real-time data. By turning on this setting, you agree to the Preview Terms . Messages users send to operations agents will be processed through the Azure AI Bot Service, which processes data in the EU Data Boundary. Therefore, if your capacity\x{2019}s geographic boundary or national cloud boundary is outside the EU Data Boundary, data sent to operations agents can be processed outside your capacity\x{2019}s geographic boundary or national cloud boundary. This setting can be managed at both the tenant and the capacity levels. Learn More .
All Power BI users can see "Set alert" button to create Fabric Activator alerts	When enabled, all Power BI users will see the "Set alert" button in reports. However, only users with permission to create Fabric items can actually set up Fabric Activator alerts, which send real-time notifications based on predefined data conditions. Learn More
Enable Snowflake database item (preview)	Turn on this setting to allow users to create the Snowflake database item in Fabric, to serve as a default storage location for Iceberg tables written by Snowflake. Learn More

Help and support settings

Expand table

Setting name	Description
Publish "Get Help" information	Users in the organization can go to internal help and support resources from the Power BI help menu.
Receive email notifications for service outages or incidents	Mail-enabled security groups will receive email notifications if this tenant is impacted by a service outage or incident.
Users can try Microsoft Fabric paid features	When users sign up for a Microsoft Fabric trial, they can try Fabric paid features for free for 60 days from the day they signed up. Learn More
Show a custom message before publishing reports	When people attempt to publish a report, they'll see a custom message before it gets published.

Domain management settings

Expand table

Setting name	Description
Allow tenant and domain admins to override workspace assignments (preview)	Tenant and domain admins can reassign workspaces that were previously assigned to one domain to another domain.

Workspace settings

Expand table

Setting name	Description
Create workspaces	Users in the organization can create app workspaces to collaborate on dashboards, reports, and other content. Even if this setting is disabled, a workspace will be created when a template app is installed.
Use semantic models across workspaces	Users in the organization can use semantic models across workspaces if they have the required Build permission.
Block users from reassigning personal workspaces (My Workspace)	Turn on this setting to prevent users from reassigning their personal workspaces (My Workspace) from Premium capacities to shared capacities. Learn More
Define workspace retention period	Turn on this setting to define a retention period during which you can restore a deleted workspace and recover items in it. At the end of the retention period, the workspace is permanently deleted. By default, workspaces are always retained for a minimum of 7 days before they're permanently deleted.

Setting name	Description
	Turn off this setting to accept the minimum retention period of 7 days. After 7 days the workspace and items in it will be permanently deleted. Enter the number of days to retain a workspace before it's permanently deleted. My Workspace workspaces will be retained for 30 days automatically. Other workspaces can be retained for up to 90 days.
Automatically convert and store reports using Power BI enhanced metadata format (PBIR) (preview)	Enable this setting to automatically convert reports to PBIR format after editing and save them in the workspace. When this is activated, new reports will also be created in PBIR format. PBIR format provides source control-friendly file structures, enhancing co-development and boosting development efficiency for Power BI reports. Learn More

Information protection

Expand table

Setting name	Description
Allow users to apply sensitivity labels for content	With this setting enabled, Microsoft Purview Information Protection sensitivity labels published to users by your organization can be applied. All prerequisite steps must be completed before enabling this setting. Important: Sensitivity-label-based access control for Fabric and Power BI data and content is only enforced in the tenant where the labels were applied, in Power BI Desktop (.pbix) files, and in Excel, PowerPoint, and PDF files generated via supported export paths. Sensitivity-label-based access control is not supported in cross-tenant scenarios, such as external data sharing, or in any other export scenario, such as export to .csv or .txt formats. For more information, see Information protection in Microsoft Fabric: Access control. Note: Sensitivity label settings, such as encryption and content marking for files and emails, are not applied to content in Fabric. Learn More. Encryption is applied to content in supported export paths. Visit the Microsoft Purview portal to view sensitivity label settings for your organization.
Apply sensitivity labels from data sources to their data in Power BI	Only sensitivity labels from supported data sources will be applied. Please see the documentation for details about supported data sources and how their sensitivity labels are applied in Power BI. Learn about supported data sources

Setting name	Description
Automatically apply sensitivity labels to downstream content	With this setting enabled, whenever a sensitivity label is changed or applied to Fabric content, the label will also be applied to its eligible downstream content. Learn More
Allow workspace admins to override automatically applied sensitivity labels	With this setting enabled, workspace admins can change or remove sensitivity labels that were applied automatically by Fabric, for example, as a result of label inheritance. Learn More
Restrict content with protected labels from being shared via link with everyone in your organization	This setting will prevent content with protection settings in the sensitivity label from being shared via link with everyone in your organization. Learn More
Domain admins can set default sensitivity labels for their domains (preview)	Domain admins can set a default sensitivity label for their domains. The label they set will override your organization's default labels in Microsoft Purview, as long as it has a higher priority than the existing default labels set for your tenant. A domain's default label will automatically apply to new Fabric items created within the domain. Reports, semantic models, dataflows, dashboards, scorecards, and some additional item types aren't currently supported. Learn More
Allow Microsoft Purview to secure AI interactions	Allow Microsoft Purview to access, process, and store prompts and responses-including metadata-for data security and compliance outcomes such as sensitive info type (SIT) classification, reporting in Microsoft Purview Data Security Posture Management for AI, Audit, Insider Risk Management, Communication Compliance, and eDiscovery. Note: This is a Microsoft Purview paid capability and is not included in the Copilot in Fabric pricing. Learn More

Export and sharing settings

Expand table

Setting name	Description
External data sharing	Users can share a read-only link to data stored in OneLake with collaborators outside your organization. When you grant them permission to do so, users can share a link to data in lakehouses and additional Fabric items. Collaborators who receive the link can view, build on, and share the data both within and beyond their own Fabric tenants, using their organization's licenses and capacities. Learn More
Users can accept external data shares	Users can accept a read-only link to data from another organization's Fabric tenant. Users who accept an external share link can view, build on, and share the data, both inside and outside of your organization's tenant. For more

Setting name	Description
	information about the security limitations of this preview feature, view the feature documentation. Learn More
Guest users can access Microsoft Fabric	Guest users who've been added to your Microsoft Entra directory can access Microsoft Fabric and any Fabric items they have permissions to. Learn More
Users can invite guest users to collaborate through item sharing and permissions	Users can collaborate with people outside the organization by sharing Fabric items with them and granting them permission to access those items. After external users accept an invitation, they're added to your Microsoft Entra directory as guest users. Learn More
Guest users can browse and access Fabric content	Users can invite guest users to browse and request access to Fabric content. Learn More
Users can see guest users in lists of suggested people	With this setting on, users will see both users in your organization and guest users who've been added to your Microsoft Entra directory in lists of suggested people. With this setting off, users will see only users in your organization. Users can still share items with guests by providing their full email address. Learn More
Publish to web	People in your org can publish public reports on the web. Publicly published reports don't require authentication to view them. Go to Embed codes in the admin portal to review and manage public embed codes. If any of the codes contain private or confidential content remove them. Review embed codes regularly to make sure no confidential information is live on the web. Learn more about Publish to web
Copy and paste visuals	Users in the organization can copy visuals from a tile or report visual and paste them as static images into external applications.
Export to Excel	Users in the organization can export the data from a visualization or paginated report to an Excel file. Learn More
Export to .csv	Users in the organization can export data from a tile, visualization, or paginated report to a .csv file. Learn More
Download reports	Users in the organization can download .pbix files and paginated reports. Learn More
Users can work with semantic models in Excel using a live connection	Users can export data to Excel from a report visual or semantic model, or export a semantic model to an Excel workbook with Analyze in Excel, both options with a live connection to the XMLA endpoint. Learn More

Setting name	Description
Export reports as PowerPoint presentations or PDF documents	Users in the organization can export reports as PowerPoint files or PDF documents.
Export reports as MHTML documents	Users in the organization can export Paginated reports as MHTML documents.
Export reports as Word documents	Users in the organization can export Paginated reports as Word documents.
Export reports as XML documents	Users in the organization can export Paginated reports as XML documents.
Export reports as image files	Users in the organization can use the export report to file API to export reports as image files.
Print dashboards and reports	Users in the organization can print dashboards and reports.
Certification	Choose whether people in your org or specific security groups can certify items (like apps, reports, or datamarts) as trusted sources for the wider organization. Note: When a user certifies an item, their contact details will be visible along with the certification badge.
Endorse master data	Choose whether people in your org or specific security groups can endorse items (like lakehouses, warehouses, or datamarts) as one of the core sources for your organization's data records. Learn More Note: When someone endorses an item as master data, their name and email will show with the endorsement badge.
Users can set up email subscriptions	Users can create email subscriptions to reports and dashboards.
B2B guest users can set up and be subscribed to email subscriptions	B2B guest users can set up and be subscribed to email subscriptions. B2B guest users are external users that have been added to your Microsoft Entra ID. Turn this setting off to prevent B2B guest users from setting up or being subscribed to email subscriptions. Learn More
Users can send email subscriptions to external users	Users can send email subscriptions to external users. External users are users you've not added to your Microsoft Entra ID. Turn this setting off to prevent users from subscribing external users to email subscriptions. Learn More
Featured content	Users in the organization can promote their published content to the Featured section of Power BI Home.

Setting name	Description
Allow connections to featured tables	Users in the organization can access and perform calculations on data from featured tables. Featured tables are defined in the modeling view in Power BI Desktop and made available through data types gallery of Excel.
Allow shareable links to grant access to everyone in your organization	This setting will grant access to anyone in your organization with the link. It won't work for external users. Learn More
Enable Microsoft Teams integration	This setting allows people in the organization to access features associated with the Microsoft Teams and Power BI integration. This includes launching Teams experiences from the Power BI service like chats, the Power BI app for Teams, and receiving Power BI notifications in Teams. To completely enable or disable Teams integration, work with your Teams admin.
Install Power BI app for Microsoft Teams and Power BI agent for Microsoft 365 Copilot automatically	The Power BI app for Microsoft Teams and the Power BI agent for Microsoft 365 Copilot are automatically installed when users access Microsoft Fabric (if allowed in the Teams Admin Portal). Once installed, users get Teams notifications, can open all Fabric content, and more easily collaborate with colleagues. The Power BI agent can instantly find items users' want, generate answers to questions on the spot and summarize reports to highlight key insights. Learn More .
Enable Power BI add-in for PowerPoint	Let people in your org embed Power BI data into their PowerPoint presentations. This integration requires that your organization's Microsoft Office admin has enabled support for add-ins.
Allow DirectQuery connections to Power BI semantic models	DirectQuery connections allow users to make changes to existing semantic models or use them to build new ones. Learn More
Guest users can work with shared semantic models in their own tenants	Authorized guest users can discover semantic models shared with them in the OneLake data hub (in Power BI Desktop), and then work with these semantic models in their own Power BI tenants.
Allow specific users to turn on external data sharing	Turn off this setting to prevent all users from turning on external data sharing. If this setting is on, all or specific users can turn on the external data sharing option, allowing them to share data with authorized guest users. Authorized guest users can then discover, connect to, and work with these shared semantic models in their own Power BI tenants.

Discovery settings

Expand table

Setting name	Description
Make promoted content discoverable	Allow users in this org who can promote content to make content they promote discoverable by users who don't have access to it. Learn More
Make certified content discoverable	Allow users in the org who can certify content to make content they certify discoverable by users who don't have access to it. Learn More
Discover content	Allow users to find and request access to content they don't have access to if it was made discoverable by its owners. Learn More

App settings

Expand table

Setting name	Description
Create template organizational apps	Users in the organization can create template apps that use semantic models built on one data source in Power BI Desktop.
Push apps to end users	Users can share apps directly with end users without requiring installation from AppSource.
Publish apps to the entire organization	Users in the organization can publish apps to the entire organization.

Integration settings

Expand table

Setting name	Description
Allow XMLA endpoints and Analyze in Excel with on-premises semantic models	Users in the organization can use Excel to view and interact with on-premises Power BI semantic models. This also allows connections to XMLA endpoints.
Semantic Model Execute Queries REST API	Users in the organization can query semantic models by using Data Analysis Expressions (DAX) through Power BI REST APIs.
Use ArcGIS Maps for Power BI	Users in the organization can use the ArcGIS Maps for Power BI visualization provided by Esri.
Use global search for Power BI	Turn on this setting to let users use the global search bar at the top of the page.

Setting name	Description
Users can use the Azure Maps visual	With this setting on, users can create and view the Azure Maps visual. Your data may be temporarily stored and processed by Microsoft for essential services, including translating location names into latitudes and longitudes. Use of Azure Maps is subject to the following Terms of use.
Data sent to Azure Maps can be processed outside your tenant's geographic region, compliance boundary, or national cloud instance	Azure Maps services are currently not available in all regions and geographies. With this setting on, data sent to Azure Maps can be processed in a region where the service is available, which might be outside your tenant's geographic region, compliance boundary, or national cloud instance. Learn More
Data sent to Azure Maps can be processed by Microsoft Online Services Subprocessors	Some Azure Maps visual services, including the selection tool and the processing of location names within some regions, may require mapping capabilities provided in part by Microsoft Online Services subprocessors. Microsoft shares only necessary data with these Microsoft Online Services subprocessors, who may access data only to deliver the functions in support of online services that Microsoft has engaged them to provide and are prohibited from using data for any other purpose. Microsoft does not share the name of the customer or end user who submits the query. This feature is non-regional and the queries you provide may be stored and processed in the United States or any other country in which Microsoft or its subprocessors operate. Learn More
Map and filled map visuals	Allow people in your org to use the map and filled map visualizations in their reports.
Integration with SharePoint and Microsoft Lists	Users in the organization can launch Power BI from SharePoint lists and Microsoft Lists. Then they can build Power BI reports on the data in those lists and publish them back to the lists.
Dremio SSO	Enable SSO capability for Dremio. By enabling, user access token information, including name and email, will be sent to Dremio for authentication.
Snowflake SSO	Enable SSO capability for Snowflake. By enabling, user access token information, including name and email, will be sent to Snowflake for authentication. Learn More
Redshift SSO	Enable SSO capability for Redshift. By enabling, user access token information, including name and email, will be sent to Redshift for authentication.
Google BigQuery SSO	Enable SSO capability for Google BigQuery. By enabling, user access token information, including name and email, will be sent to Google BigQuery for authentication.
Microsoft Entra single sign-on for data gateway	Users can use Microsoft Entra single sign-on (SSO) to authenticate to on-premises data gateways and access data sources.

Setting name	Description
	With this setting on, user access token information, including names and emails, is sent to data sources to authenticate to the on-premises data gateway service. Learn More
Users can view Power BI files saved in OneDrive and SharePoint (preview)	Users in the organization can view Power BI files saved in OneDrive for Business or SharePoint document libraries. The permissions to save and share Power BI files in OneDrive and SharePoint document libraries are controlled by permissions managed in OneDrive and SharePoint. Learn More
Users can share links to Power BI files stored in OneDrive and SharePoint through Power BI Desktop (preview)	Users who have saved Power BI files (.pbix) to OneDrive and SharePoint can share links to those files using Power BI Desktop. Learn More
Enable granular access control for all data connections	Enforce strict access control for all data connection types. When this is turned on, shared items will be disconnected from data sources if they're edited by users who don't have permission to use the data connections. Learn More
Semantic models can export data to OneLake	Semantic models configured for OneLake integration can send import tables to OneLake. Once the data is in OneLake, users can include the exported tables in Fabric items, including lakehouses and warehouses. Learn More
Semantic model owners can choose to automatically update semantic models from files imported from OneDrive or SharePoint	Semantic model owners can choose to allow semantic models to be automatically updated with changes made to the corresponding Power BI files (.pbix) stored in OneDrive or SharePoint. File changes can include new and modified data connections. Turn off this setting to prevent automatic updates to semantic models. Learn More
ArcGIS GeoAnalytics for Fabric Runtime	Users in your organization can use Esri's ArcGIS GeoAnalytics for Fabric Runtime in Microsoft's Fabric Spark Runtime. ArcGIS GeoAnalytics delivers spatial analysis to your big data by extending Apache Spark with ready-to-use spatial SQL functions and analysis tools. Learn More
Allow non-Entra ID auth in Eventstream	Users can enhance the security of data streaming by disabling key-based authentication in Eventstream's Custom Endpoint, ensuring that only Microsoft Entra ID (formerly Azure Active Directory) authentication is allowed. This reduces the risk of unauthorized access to Fabric Eventstream through non-Entra ID authentication methods. Learn more
Users can create "Direct Lake on OneLake semantic models" (preview)	Users can create tables using "Direct Lake on OneLake" storage mode and have tables from one or more OneLake data sources in a Power BI semantic model when this setting is enabled. Direct Lake on OneLake storage mode does not require a SQL endpoint and does not support fallback to DirectQuery. If you disable this setting, you cannot create tables using Direct

Setting name	Description
	Lake on OneLake storage mode in semantic models. Existing semantic models using Direct Lake on OneLake storage mode are not affected and continue to use Direct Lake on OneLake. Learn More

Power BI visuals

Expand table

Setting name	Description
Allow visuals created using the Power BI SDK	Users in the organization can add, view, share, and interact with visuals imported from AppSource or from a file. Visuals allowed in the "Organizational visuals" page are not affected by this setting. Learn More
Add and use certified visuals only (block uncertified)	Users in the organization with permissions to add and use visuals can add and use certified visuals only. Visuals allowed in the "Organizational visuals" page are not affected by this setting, regardless of certification. Learn More
Allow downloads from custom visuals	Enabling this setting will let custom visuals download any information available to the visual (such as summarized data and visual configuration) upon user consent. It is not affected by download restrictions applied in your organization's Export and sharing settings. Learn More
AppSource Custom Visuals SSO	Enable SSO capability for AppSource custom visuals. This feature allows custom visuals from AppSource to get Microsoft Entra ID access tokens for signed-in users through the Authentication API. Microsoft Entra ID access tokens include personal information, including users' names and email addresses, and may be sent across regions and compliance boundaries. Learn More
Allow access to the browser's local storage	When this setting is on, custom visuals can store information on the user's browser's local storage. Learn More

R and Python visuals settings

Expand table

Setting name	Description
Interact with and share R and Python visuals	Users in the organization can interact with and share visuals created with R or Python scripts.

Audit and usage settings

Expand table

Setting name	Description
Usage metrics for content creators	Users in the organization can see usage metrics for dashboards, reports and semantic models that they have appropriate permissions to. Learn More
Per-user data in usage metrics for content creators	Usage metrics for content creators will expose display names and email addresses of users who are accessing content.
Show user data in the Fabric Capacity Metrics app and reports	With this setting on, active user data, including names and email addresses, are displayed in the Capacity Metrics app and reports. Learn More
Azure Log Analytics connections for workspace administrators	NO DESCRIPTION IN UI
Workspace admins can turn on monitoring for their workspaces (preview)	Workspace admins can turn on monitoring for their workspaces. When a workspace admin turns on monitoring, a read-only Eventhouse that includes a KQL database is created. After the Eventhouse and KQL database are added to the workspace, logging is turned on and data is sent to the database. Learn More
Microsoft can store query text to aid in support investigations	Query text for some items, including semantic models, is securely stored for usage during support investigations. Turn off this setting to stop the service from storing query text. Turning off this setting might negatively impact Microsoft's ability to provide support for the Fabric service. Learn More

Dashboard settings

Expand table

Setting name	Description
Web content on dashboard tiles	Users in the organization can add and view web content tiles on Power BI dashboards. Note: This may expose your org to security risks via malicious web content.

Developer settings

Expand table

Setting name	Description
Embed content in apps	Users in the organization can embed Power BI dashboards and reports in Web applications using "Embed for your customers" method. Learn More
Service principals can create workspaces, connections, and deployment pipelines	This setting allows service principals to create workspaces, connections, and deployment pipelines. To allow service principals to call the rest of Fabric public APIs, turn on the setting titled "Service principals can call Fabric public APIs". Learn More
Service principals can call Fabric public APIs	This setting allows service principals with the appropriate roles and item permissions to call Fabric public APIs. To allow service principals to create workspaces, connections, and deployment pipelines turn on the setting titled "Service principals can create workspaces, connections, and deployment pipelines". Learn More
Allow service principals to create and use profiles	Allow service principals in your organization to create and use profiles.
Block ResourceKey Authentication	For extra security, block using resource key based authentication. This means users not allowed to use streaming semantic models API using resource key.

Admin API settings

Expand table

Setting name	Description
Service principals can access read-only admin APIs	Web apps registered in Microsoft Entra ID can use service principals, rather than user credentials, to authenticate to read-only admin APIs. To allow an app to use a service principal as an authentication method, the service principal must be added to an allowed security group. Service principals included in allowed security groups will have read-only access to all the information available through admin APIs, which can include users' names and emails, and detailed metadata about semantic models and reports. Learn More
Service principals can access admin APIs used for updates	Web apps registered in Microsoft Entra ID can use service principals, rather than user credentials, to authenticate to admin APIs used for updates. To allow an app to use a service principal as an authentication method, add the service principal to an allowed security group. Service principals in allowed security groups have full access to the information available through admin APIs, including users' names and emails, and detailed metadata about items. Learn More

Setting name	Description
Enhance admin APIs responses with detailed metadata	Users and service principals allowed to call Power BI admin APIs may get detailed metadata about Power BI items. For example, responses from GetScanResult APIs will contain the names of semantic model tables and columns. Learn More Note: For this setting to apply to service principals, make sure the tenant setting allowing service principals to use read-only admin APIs is enabled. Learn More
Enhance admin APIs responses with DAX and mashup expressions	Users and service principals eligible to call Power BI admin APIs will get detailed metadata about queries and expressions comprising Power BI items. For example, responses from GetScanResult API will contain DAX and mashup expressions. Learn More Note: For this setting to apply to service principals, make sure the tenant setting allowing service principals to use read-only admin APIs is enabled. Learn More

Gen1 dataflow settings

Expand table

Setting name	Description
Create and use Gen1 dataflows	Users in the organization can create and use Gen1 dataflows. Learn More

Template app settings

Expand table

Setting name	Description
Publish template apps	Users in the organization can publish template apps for distribution to clients outside of the organization. Learn More .
Install template apps	Users in the organization can install template apps created outside the organization. When a template app is installed, an upgraded workspace is created. Learn More
Install template apps not listed in AppSource	Users in the organization who have been granted permission to install template apps which were not published to Microsoft AppSource. Learn More .

Q&A settings

Expand table

Setting name	Description
Review questions	Allow semantic model owners to review questions people asked about their data.
Synonym sharing	Allow people to share Q&A synonyms with your organization. Learn More

Explore settings (preview)

Expand table

Setting name	Description
Users with view permission can launch Explore	Explore is a light-weight visual data exploration experience that enables people to quickly and easily do ad hoc analysis. This setting allows people with view permission on a semantic model to launch Explore from that model and from items connected to it. Learn More

Semantic Model Security

Expand table

Setting name	Description
Block republish and disable package refresh	Disable package refresh, and only allow the semantic model owner to publish updates.

Advanced networking

Expand table

Setting name	Description
Tenant-level Private Link	Increase security by allowing people to use a Private Link to access your Fabric tenant. Someone will need to finish the set-up process in Azure. If that's not you, grant permission to the right person or group by entering their email. Learn More Set-up instructions Review the considerations and limitations section before enabling private endpoints.

Setting name	Description
Block Public Internet Access	For extra security, block access to your Fabric tenant via the public internet. This means people who don't have access to the Private Link won't be able to get in. Keep in mind, turning this on could take 10 to 20 minutes to take effect. Learn More Set-up instructions
Configure workspace-level inbound network rules	With this setting on, workspace admins can configure inbound private link access protection in workspace settings. When a workspace is configured to restrict inbound network access, existing tenant-level private links can no longer connect to these workspaces. Turning off this setting reverts all workspaces to their previous configuration. Learn More
Configure workspace-level outbound network rules	With this setting on, workspace admins can configure outbound access protection in workspace settings. Turning off this tenant setting also turns off outbound access protection in all the workspaces in the tenant. Learn More

Encryption

Expand table

Setting name	Description
Apply customer-managed keys	With this setting turned on, users can configure workspace level encryption using customer-managed keys to protect their data. When turned off, the default is to use Microsoft managed keys. Learn More

Metrics settings

Expand table

Setting name	Description
Create and use Metrics	Users in the organization can create and use Metrics

User experience experiments

Expand table

Setting name	Description
Help Power BI optimize your	Users in this organization will get minor user experience variations that the Power BI team is experimenting with, including content, layout, and design,

Setting name	Description
experience	before they go live for all users.

Share data with your Microsoft 365 services

Expand table

Setting name	Description
Share Fabric data with your Microsoft 365 services	When this setting is enabled, Microsoft Fabric data can be stored and displayed in Microsoft 365 services. Fabric data (including Power BI report titles, chart axis labels, Fabric data agent instructions, or open and sharing history) may be used to improve Microsoft 365 services like search results and recommended content lists. Learn More Users can browse or get recommendations only for content they have access to. Users will see metadata about Fabric items (including refresh dates and workspace names in search listings) and see item content (like chart axis labels or titles reflected in Copilot summarizations) to enhance Microsoft 365 services. This setting is automatically enabled only if your Microsoft Fabric and Microsoft 365 tenants are in the same geographical region. You may disable this setting. Where is my Microsoft Fabric tenant located?

Insights settings

Expand table

Setting name	Description
Receive notifications for top insights (preview)	Users in the organization can enable notifications for top insights in report settings
Show entry points for insights (preview)	Users in the organization can use entry points for requesting insights inside reports

Datamart settings

Expand table

Setting name	Description
Create Datamarts (preview)	Users in the organization can create Datamarts

Semantic model settings

Expand table

Setting name	Description
Users can edit semantic models in the Power BI service	Turn on this setting to allow users to edit semantic models in the service. This setting doesn't apply to DirectLake semantic models or editing a semantic model through an API or XMLA endpoint. Learn More

Scale-out settings

Expand table

Setting name	Description
Scale out queries for large semantic models	For semantic models that use the large semantic model storage format, Power BI Premium can automatically distribute queries across additional semantic model replicas when query volume is high.

OneLake settings

Expand table

Setting name	Description
Users can access data stored in OneLake with apps external to Fabric	Users can access data stored in OneLake with apps external to the Fabric environment, such as custom applications created with Azure Data Lake Storage (ADLS) APIs, OneLake File Explorer, and Databricks. Users can already access data stored in OneLake with apps internal to the Fabric environment, such as Spark, Data Engineering, and Data Warehouse. Learn More
Use short-lived user-delegated SAS tokens	OneLake SAS tokens enable applications to access data in OneLake through short-lived SAS tokens, based on a Microsoft Fabric user's Entra identity. These token's permissions can be further limited to provide least privileged access and cannot exceed a lifetime of one hour. Learn More

Setting name	Description
Authenticate with OneLake user-delegated SAS tokens	Allow applications to authenticate using a OneLake SAS token. Fabric users can create OneLake SAS by requesting a user delegation key. The tenant setting, Use short-lived user delegated SAS tokens, must be turned on to generate user delegation keys. The lifetimes of the user delegation keys and SAS tokens cannot exceed one hour. Learn More
Users can sync data in OneLake with the OneLake File Explorer app	Turn on this setting to allow users to use OneLake File Explorer. This app will sync OneLake items to Windows File Explorer, similar to OneDrive. Learn More
Enable Delta Lake to Apache Iceberg table format virtualization (preview)	Delta Lake tables will be virtually converted to have additional Iceberg table metadata. This allows different services/workloads to read your Delta Lake tables as Iceberg tables. Note: This setting controls a feature that is currently in preview. This setting will be removed in a future update when the feature is no longer in preview.
Include end-user identifiers in OneLake diagnostic logs	Control whether OneLake diagnostic logs capture end user identifiable information (EUII), such as email addresses and IP addresses. When enabled, these fields are recorded to support diagnostics, investigations, and usage analysis across your tenant. When disabled, these fields are redacted from new events. Learn More

Git integration

Expand table

Setting name	Description
Users can synchronize workspace items with their Git repositories	Users can import and export workspace items to Git repositories for collaboration and version control. Turn off this setting to prevent users from syncing workspace items with their Git repositories. Learn More
Users can export items to Git repositories in other geographical locations	The workspace and the Git repository may reside in different geographies. Turn on this setting to allow users to export items to Git repositories in other geographies.
Users can export workspace items with applied sensitivity labels to Git repositories	Turn on this setting to allow users to export items with applied sensitivity labels to their Git repositories.
Users can sync workspace items with GitHub repositories	Users can select GitHub as their Git provider and sync items in their workspaces with GitHub repositories.

Copilot and Azure OpenAI Service

Expand table

Setting name	Description
Users can use Copilot and other features powered by Azure OpenAI	When this setting is on, users can access Fabric features powered by Azure OpenAI, including Copilot and Fabric AI agents. Check documentation for the most recent list of these features. This setting can be managed at both the tenant and the capacity levels. Learn More For customers in the EU Data Boundary, this setting adheres to Microsoft Fabric's EU Data Boundary commitments. Learn More By turning on this setting, you agree to the Preview Terms for any AI features in preview.
Users can access standalone Copilot in Power BI and the Power BI agent (preview)	Users can find, analyze, and discuss Fabric items using a standalone, cross-item Copilot experience in Power BI and a Power BI agent in Microsoft 365. This setting requires the following tenant setting to be enabled: "Users can use Copilot and other features powered by Azure OpenAI." Learn More
Data sent to Azure OpenAI can be processed outside your capacity's geographic region, compliance boundary, or national cloud instance	This setting is only applicable for customers who want to use Copilot and AI features in Fabric powered by Azure OpenAI, and whose capacity's geographic region is outside of the EU Data Boundary or the United States. Learn More When this setting is on, data sent to Copilot and other generative AI features can be processed outside your capacity's geographic region, compliance boundary, or national cloud instance. Check documentation for the types of data this might include. This setting can be managed at both the tenant and the capacity levels. Learn More By turning on this setting, you agree to the Preview Terms for any AI features in preview.
Capacities can be designated as Fabric Copilot capacities	With this setting on, capacity admins can designate capacities as Fabric Copilot capacities. Copilot capacities are special capacity types that allow your organization to consolidate users' Copilot usage and billing on a single capacity. Learn More When users use Copilot features, capacity admins can see the names of the items associated with users' Copilot activity. Learn More
Data sent to Azure OpenAI can be stored outside your	This setting is only applicable for customers who want to use Copilot and AI features in Fabric powered by Azure OpenAI, and whose

Setting name	Description
capacity's geographic region, compliance boundary, or national cloud instance	capacity's geographic region is outside of the EU Data Boundary or the United States. Learn More When this setting is turned on, data sent to Azure OpenAI can be stored outside your capacity's geographic region, compliance boundary, or national cloud instance. Check documentation for the types of experiences and data this might include. Learn More By turning on this setting, you agree to the Preview Terms for any AI features in preview.
Only show approved items in the standalone Copilot in Power BI, and in the Power BI Agent experiences (preview)	When this is turned on, only apps, data agents, and items marked as "approved for Copilot" will appear in standalone Copilot and in the Power BI Agent. Users can still manually attach items to ask questions. Copilot item usage always subject to user permissions. Learn More

Azure Maps services

Expand table

Setting name	Description
Users can use Azure Maps services	When this setting is enabled, users can access the features powered by Azure Maps services. Learn More For customers in the EU Data Boundary, this setting adheres to Microsoft Fabric's EU Data Boundary commitments. Learn More Use of Azure Maps is subject to the following Terms of use.
Data sent to Azure Maps can be processed outside your capacity's geographic region, compliance boundary or national cloud instance	Azure Maps services are currently not available in all regions and geographies. With this setting on, data sent to Azure Maps can be processed in a region where the service is available, which might be outside your capacity's geographic region, compliance boundary, or national cloud instance. Learn More
Users can use Azure Maps Weather Services (Preview)	When this setting is enabled, users can access weather data from Azure Maps Weather, sourced from AccuWeather Learn More

Additional workloads

Expand table

Setting name	Description
Workspace admins can add and remove additional workloads (preview)	Workspace admins can add and remove workloads in their workspaces. If this setting is turned off, any existing workloads will stay added and items created with those workloads continue to work normally. When users interact with a workload, their data and access tokens, including name and email, are sent to the publisher. Sensitivity labels and protection settings including encryption aren't applied to items created with workloads. Learn More
Capacity admins and contributors can add and remove additional workloads	Capacity admins or individuals granted Contributor permission in Capacity settings can add and remove additional workloads in capacities. If this setting is turned off, any existing workloads will stay added and items created with those workloads continue to work normally. When users interact with a workload, their data and access tokens, including name and email, are sent to the publisher. Sensitivity labels and protection settings including encryption aren't applied to items created with workloads. Learn More
Workspace admins can develop partner workloads	Workspace admins can develop partner workloads with a local machine development environment. Turning off this feature will prevent developers from uploading to this workspace. Learn More
Users can see and work with additional workloads not validated by Microsoft	Turn on this setting to allow users to see and work with additional workloads not validated by Microsoft. Make sure that you only add workloads from publishers that you trust to meet your organization's policies. Learn More

Related content

- What is the admin portal?
- About tenant settings
- Use the Fabric REST API to list tenant settings

Last updated on 12/03/2025

Microsoft Fabric tenant settings

Microsoft Fabric tenant settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Users can create Fabric items

For more information, see Enable Microsoft Fabric for your organization.

Users can create and use ADF Mount items (preview)

Users can connect and test existing ADF pipelines in Microsoft Fabric. This setting can be managed at both the tenant and the capacity levels.

Users can create Healthcare Cohort items (preview)

For more information, see Overview of discover and build cohorts (preview) in healthcare data solutions.

User data functions (preview)

For more information, see What is Fabric User data functions (Preview)?.

SQL database (preview)

For more information, see SQL database in Microsoft Fabric (Preview).

Digital Twin Builder

For more information, see What is digital twin builder (preview)?.

Users can discover and create org apps (preview)

For more information, see Get started with org apps (preview).

Product Feedback

For more information, see Learn about Microsoft Fabric feedback.

Users can create and share Data agent item types (preview)

For more information, see Fabric data agent creation (preview).

Users can discover and use metrics (preview)

For more information, see Metric sets setting (preview).

Mirrored Azure Databricks Catalog

For more information, see Mirroring Azure Databricks Unity Catalog.

ML model endpoints for real-time predictions (preview)

For more information, see Serve real-time predictions with ML model endpoints.

Users can be informed of upcoming conferences featuring Microsoft Fabric when they are logged in to Fabric

When this feature is enabled, users who are signed in to Fabric in your org can receive notifications in the Fabric UI about upcoming conferences that feature Microsoft Fabric. This feature has no impact on billing or security. The setting is enabled by default.

All Power BI users can see "Set Alert" button to create Fabric Activator alerts

When this setting is enabled, all Power BI users will see the "Set Alert" button in web reports. This button allows users with Fabric permissions to create Activator alerts on their reports. When the setting is disabled, the "Set Alert" button will be visible only to Power BI users who have tenant-level Fabric Access.

Related content

- About tenant settings

Last updated on 11/21/2025

Product feedback

Article • 04/30/2024

Product feedback allows users to give Microsoft feedback about Microsoft Fabric. Product feedback is enabled by default.

Disable product feedback

Product feedback is configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

To disable product feedback, follow the following steps:

1. From the tenant settings, expand **Product feedback**.
2. Change the *Enabled* switch to **Disabled**.
3. Select, **Apply**.

Related content

- Admin overview
- Learn about Microsoft Fabric feedback

Feedback

Was this page helpful? Yes No

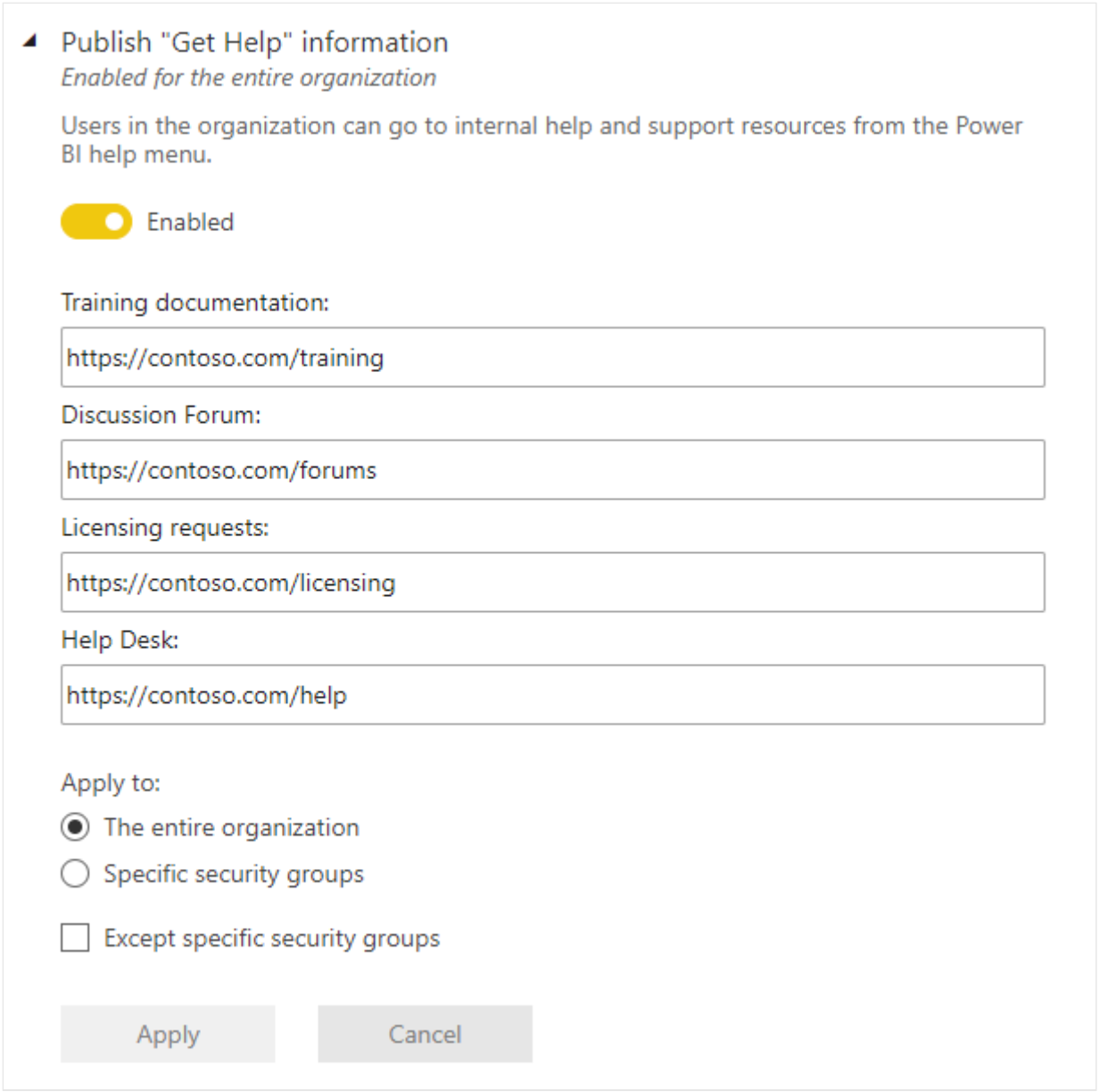
Provide product feedback | Ask the community

Help and support tenant settings

11/19/2024

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Publish "Get Help" information



Admins can specify internal URLs to override the destination of links on the Power BI help menu and for license upgrades. If custom URLs are set, users in the organization go to internal help and support resources instead of the default destinations. The following resource destinations can be customized:

- **Learn**. By default, this help menu link targets a list of all our Power BI learning paths and modules. To direct this link to internal training resources instead, set a custom URL for

Training documentation.

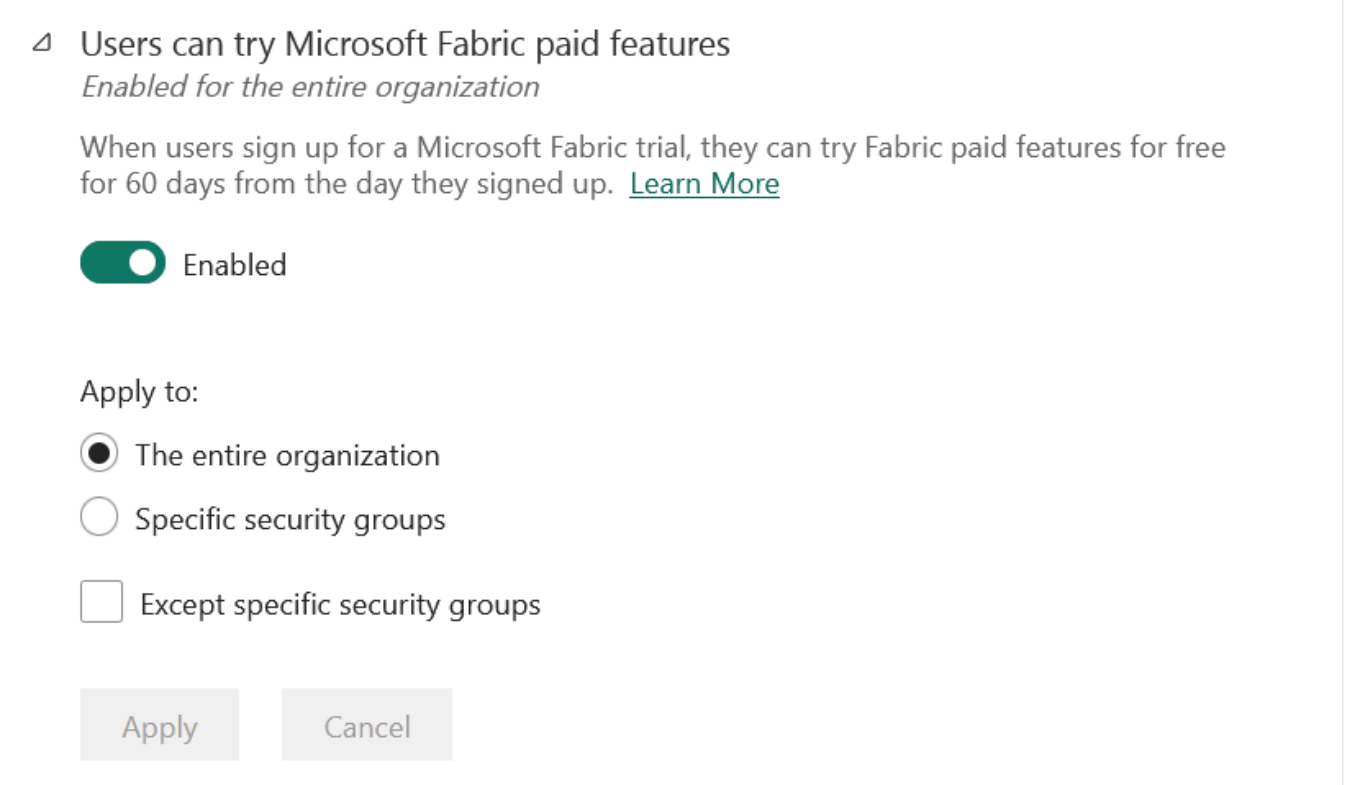
- **Community**. To take users to an internal forum from the help menu, instead of to the Fabric and Power BI Community, set a custom URL for **Discussion forum**.
- **Licensing upgrades**. Users with a Fabric (Free) license can be presented with the opportunity to upgrade to Power BI Pro (Pro) or Power BI Premium Per User (PPU). Users with a Fabric (Free) or Power BI Pro license can be presented with the opportunity to upgrade their account to a Power BI Premium Per User license. If you specify an internal URL for **Licensing requests**, you redirect users to an internal request and purchase flow and prevent self-service purchase. You might want to prevent users from buying licenses, but are okay with letting users start a Power BI individual trial or a trial of a Fabric capacity. For this scenario, see Users can try Microsoft Fabric paid features to separate the buy and try experiences.
- **Get help**. To take users to an internal help desk from the help menu, instead of to Microsoft Fabric In-Producy Support, set a custom URL for **Help Desk**.

> **Note**
>
> The Fabric In-product Support center and the option to open support cases to Microsoft (Get Microsoft Help) will always be available for Admins.

Receive email notifications for service outages or incidents

If this tenant is impacted by a service outage or incident, mail-enabled security groups receive email notifications. Learn more about Service interruption notifications.

Users can try Microsoft Fabric paid features



The setting to **Users can try Microsoft Fabric paid features** is enabled by default. This setting increases your control over how users get license upgrades. In scenarios where you block self-service purchase, this setting lets users use more features free for 60 days. Users can start a Power BI individual trial or a trial of a Fabric capacity. Changing **Users can try Microsoft Fabric paid features** from **enabled** to **disabled** blocks self-service trials of new licenses and of the Fabric capacity trial. It doesn't impact purchases that were already made.

The user's license upgrade and trial experience depends on how you combine license settings. The following table shows how the upgrade experience is affected by different setting combinations:

Expand table

Self-service purchase setting	Users can try Microsoft Fabric paid features	End-user experience
Enabled	Disabled	User can buy an upgraded license, but can't start a trial
Enabled	Enabled	User can start a free trial and can upgrade to a paid license
Disabled	Disabled	User sees a message to contact the IT admin to request a license
Disabled	Enabled	User can start a trial, but must contact the IT admin to get a paid license

> **Note**
>
> You can add an internal URL for licensing requests in **Help and support settings**. If you set the URL, it overrides the default self-service purchase experience. It doesn't redirect sign-up for a trial. Users who can buy a license in the scenarios described in the table are redirected to your internal URL.

To learn more, see Enable or disable self-service sign-up and purchasing.

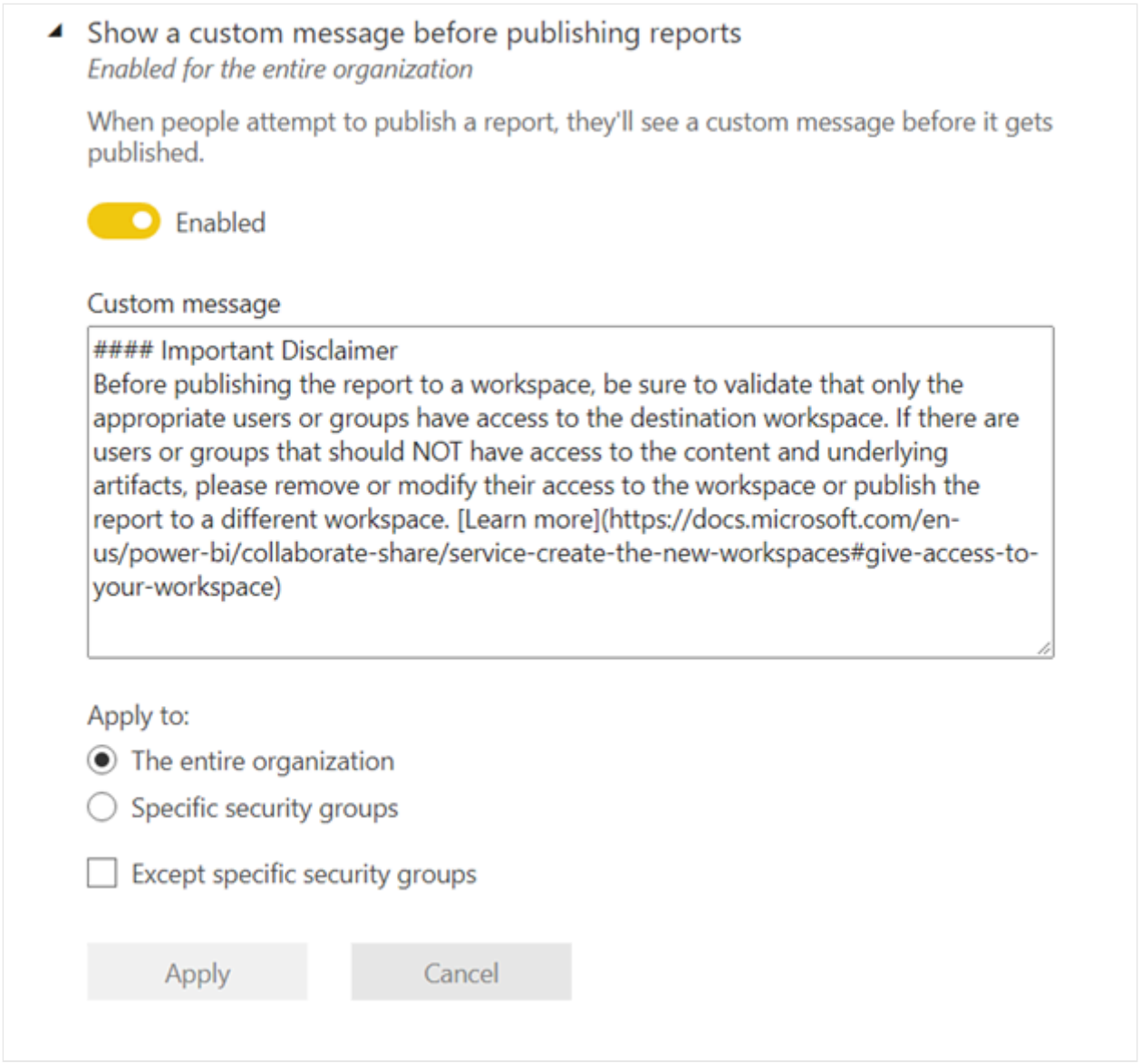
Show a custom message before publishing reports

Admins can provide a custom message that appears before a user publishes a report from Power BI Desktop. After you enable the setting, you need to provide a **custom message**. The custom message can be plain text or follow markdown syntax, as in the following example:

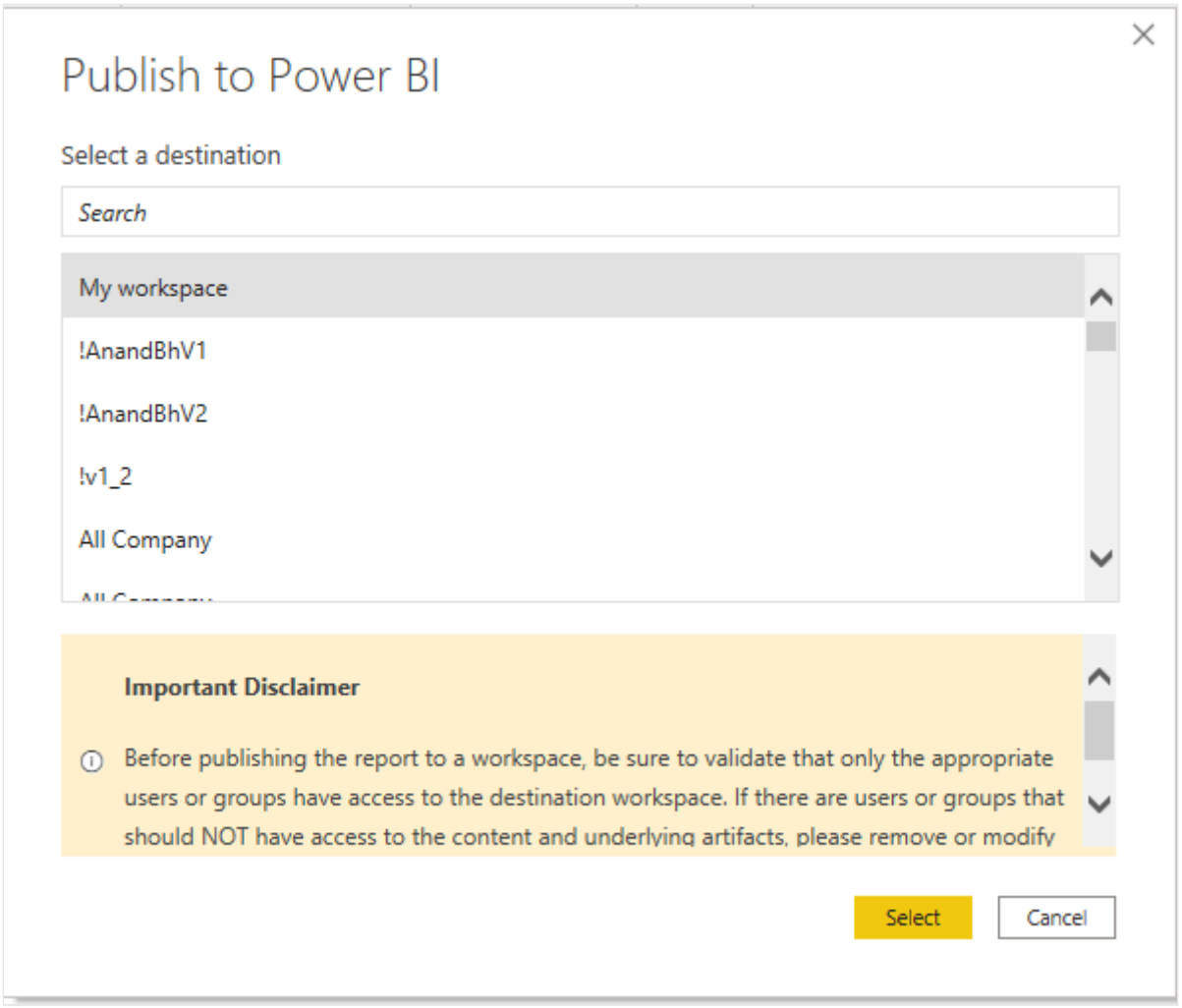
```markdown
### Important Disclaimer

Before publishing the report to a workspace, be sure to validate that the appropriate users or groups have access to the destination workspace. If some users or groups should *not* have access to the content and underlying artifacts, remove or modify their access to the workspace, or publish the report to a different workspace. Learn about [giving access to workspaces](/power-bi/collaborate-share/service-give-access-new-workspaces).
```

The **custom message** text area supports scrolling, so you can provide a message up to 5,000 characters.



When your users publish reports to workspaces in Power BI, they see the message you wrote.



As with other tenant settings, you can choose who the **custom message** applies to:

- **The entire organization**.
- **Specific security groups**.
- Or **Except specific security groups**.

Related content

- About tenant settings

Domain management tenant settings

Article • 05/02/2024

Domain management tenant settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Allow tenant and domain admins to override workspace assignments (preview)

This setting controls whether tenant and domain admins can override existing workspace domain assignments. When disabled, tenant and domain admins cannot reassign a workspace that is already assigned to a domain to another domain. When enabled, they can override such assignments. The setting is enabled by default. The domain REST APIs respect this setting.

To enable/disable the setting, go to **Admin portal** > **Tenant settings** > **Domain management settings**, expand **Allow tenant and domain admins to override workspace assignments (preview)** and set the toggle as desired.

Related content

- Fabric domains
- About tenant settings

Feedback

Workspace tenant settings

06/01/2025

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Create workspaces

Workspaces are places where users collaborate on dashboards, reports, and other content. Microsoft Fabric admins can use the **Create workspaces** setting to designate which users in the organization can create workspaces. Admins can let everybody or nobody in an organization create workspaces. Workspace creation can also be limited to members of specific security groups. Learn more about workspaces.

List of workspaces

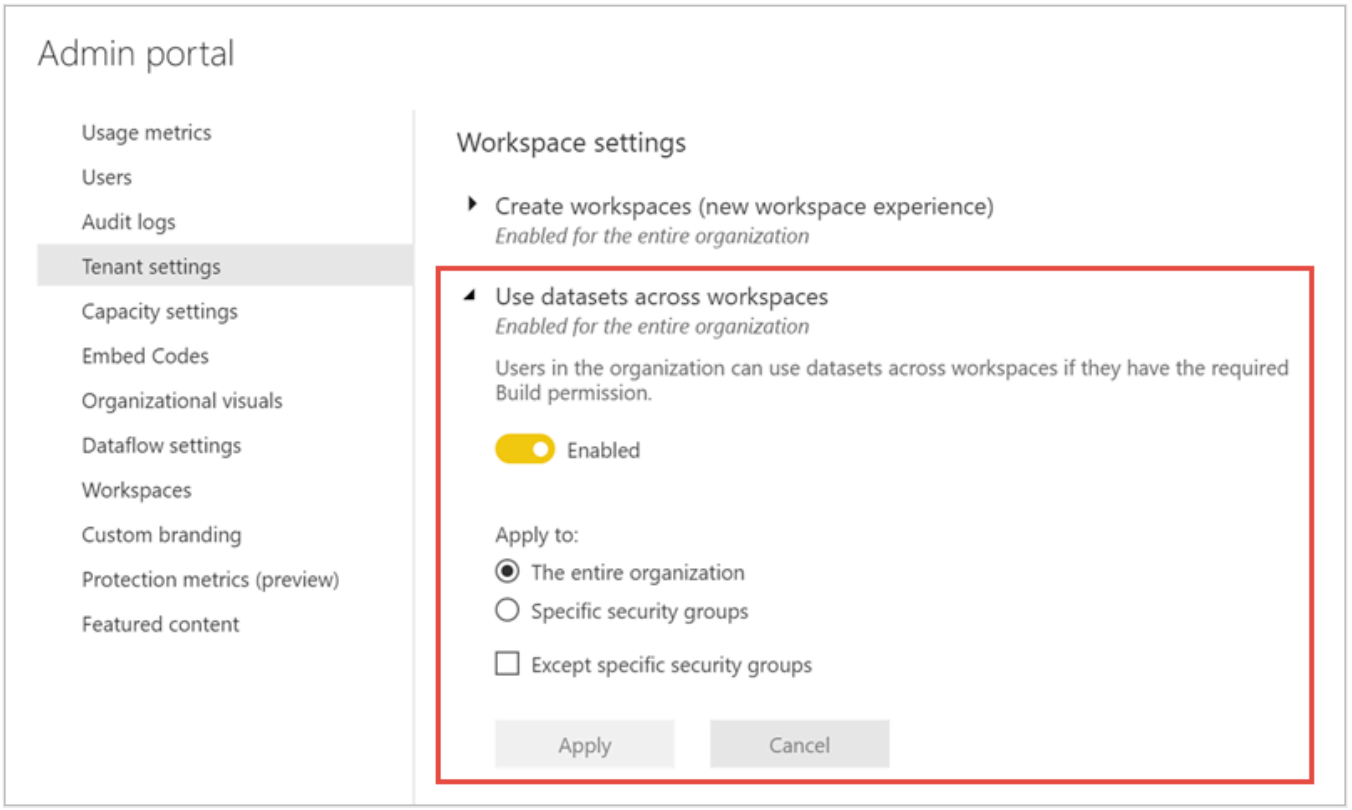
The admin portal has another section of settings about the workspaces in your tenant. In that section, you can sort and filter the list of workspaces and display the details for each workspace. See Manage workspaces for details.

Publish apps

In the admin portal, you also control which users have permissions to distribute apps to the organization. See Publish apps to the entire organization for details.

Use semantic models across workspaces

Admins can control which users in the organization can use semantic models across workspaces. When this setting is enabled, users still need the required Build permission for a specific semantic model.



For more information, see Intro to semantic models across workspaces.

Identify your workspace ID

The easiest way to find your workspace ID is in the URL of the Fabric site for an item in a workspace. As in Power BI, the Fabric URL contains the workspace ID, which is the unique identifier after `/groups/` in the URL, for example: `https://powerbi.com/groups/11aa111-a11a-1111-1abc-aa1111aaaa/...`. Alternatively, you can find the workspace ID in the Power BI Admin portal settings by selecting **Details** next to the workspace name.

Block users from reassigning personal workspaces (My Workspace)

Personal workspaces are the My workspaces that every user has for their personal content. Microsoft Fabric and capacity admins can designate a preferred capacity for My workspaces. By default, however, My workspace owners can still change the capacity assignment of their workspace. If a Microsoft Fabric or capacity admin designates a Premium capacity as the default capacity for My workspaces, but a My workspace owner then changes that capacity assignment back to shared capacity, this could result in non-compliance with data residency requirements.

To prevent such a scenario, the Microsoft Fabric admin can turn on the **Block users from reassigning personal workspaces (My Workspace)** tenant setting. When this setting is on, My

workspace owners can't change the capacity assignment of their My workspace.

To turn on the setting:

1. Go to the Microsoft Fabric Admin portal and select **Tenant settings**.
2. In the tenant settings, scroll down to the **Workspace settings** section.
3. Find the setting called **Block users from reassigning personal workspaces (My Workspace)**.

For more information, see Prevent My workspace owners from reassigning their My workspaces to a different capacity.

Related content

About tenant settings

Information protection tenant settings

Article • 03/03/2024

Information protection tenant settings help you to protect sensitive information in your Power BI tenant. Allowing and applying sensitivity labels to content ensures that information is only seen and accessed by the appropriate users. These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Allow users to apply sensitivity labels for content

With this setting enabled, specified users can apply sensitivity labels from Microsoft Purview Information Protection.

All prerequisite steps must be completed before enabling this setting.

Sensitivity label settings, such as encryption and content marking for files and emails, aren't applied to content. Sensitivity labels and protection are only applied to files exported to Excel, PowerPoint, or PDF files that are controlled by **Export to Excel** and **Export reports as PowerPoint presentation or PDF documents** settings. All other export and sharing options don't support the application of sensitivity labels and protection.

To learn more, see Sensitivity labels in Power BI.

To view sensitivity label settings for your organization, visit the Microsoft Purview compliance portal.

Apply sensitivity labels from data sources to their data in Power BI

When this setting is enabled, Power BI semantic models that connect to sensitivity-labeled data in supported data sources can inherit those labels, so that the data remains classified and secure when brought into Power BI.

To learn more about sensitivity label inheritance from data sources, see Sensitivity label inheritance from data sources (preview).

Automatically apply sensitivity labels to downstream content

When a sensitivity label is applied to a semantic model or report in the Power BI service, it's possible to have the label trickle down and be applied to content that's built from that semantic model or report.

To learn more, see Sensitivity label downstream inheritance.

Allow workspace admins to override automatically applied sensitivity labels

Fabric admins can enable the **Allow workspace admins to override automatically applied sensitivity labels** tenant setting. This makes it possible for workspace admins to override automatically applied sensitivity labels without regard to label change enforcement rules.

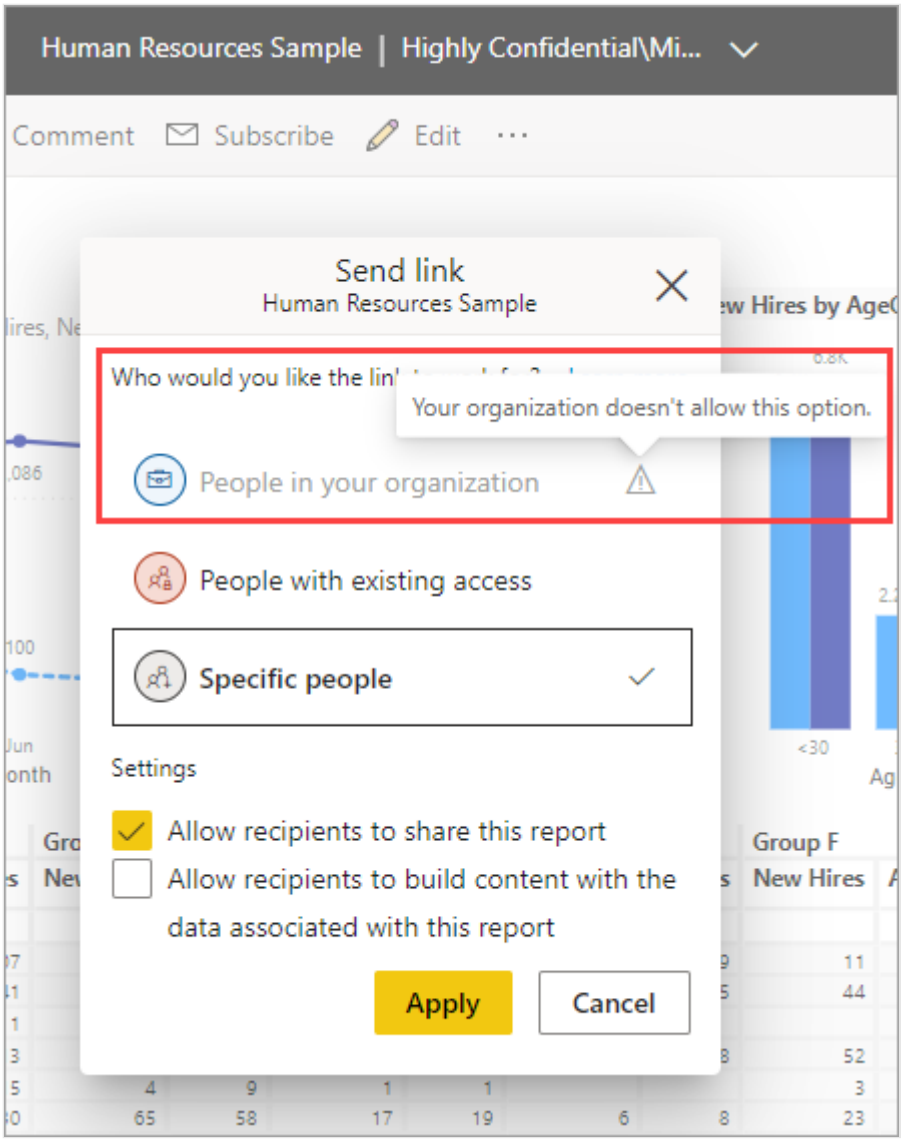
To learn more, see Relaxations to accommodate automatic labeling scenarios.

Restrict content with protected labels from being shared via link with everyone in your organization

When this setting is enabled, users can't generate a sharing link for **People in your organization** for content with protection settings in the sensitivity label.

> **Note**
>
> This setting is disabled if you haven't enabled both the **Allow users to apply sensitivity labels for Power BI content** setting and the **Allow shareable links to grant access to everyone in your organization** setting.

Sensitivity labels with protection settings include encryption or content markings. For example, your organization might have a *Highly Confidential* label that includes encryption and applies a *Highly Confidential* watermark to content with this label. Therefore, when this tenant setting is enabled and a report has a sensitivity label with protection settings, then users can't create sharing links for **People in your organization**:



To learn more about protection settings for sensitivity labels, see Restrict access to content by using sensitivity labels to apply encryption.

Increase the number of users who can edit and republish encrypted PBIX files (preview)

When enabled, users with restrictive sensitivity permissions on an encrypted sensitivity label can open, edit, publish, and republish PBIX files protected by that label, with restrictions (provided that the appropriate preview feature switch in Power BI Desktop is on).

Restrictive sensitivity permissions

Restrictive sensitivity permissions in this context means that the user must have all of the following usage rights:

- View Content (VIEW)

- Edit Content (DOCEDIT)
- Save (EDIT)
- Copy and extract content (EXTRACT)
- Allow Macros (OBJMODEL)

> **Note**
>
> Usage rights are granted to users by compliance admins in the Microsoft Purview compliance portal as part of sensitivity label definition.

Restrictions

The following are the restrictions that apply to users with restrictive sensitivity permissions:

- Users with restrictive sensitivity permissions can't export to formats that don't support sensitivity labels, such as CSV files.
- Users with restrictive sensitivity permissions can't change the label on the PBIX file.
- Users with restrictive sensitivity permissions can republish the PBIX file only to the original workspace they downloaded it from.

These restrictions ensure that protection is preserved and control of protection settings remains with users that have higher permission levels.

If a user tries to perform one of the restricted actions, they will see a warning informing them that they do not have the required permissions. If the **Increase the number of users who can edit and republish encrypted PBIX files (preview)** feature switch is enabled on the tenant, the user should check to see that the **Less elevated user support** preview feature switch in their Power BI Desktop app is on.

For more information, see Protected sensitivity labels in Fabric and Power BI.

Desktop preview feature switch for editing by users with restrictive sensitivity permissions

The **Less elevated user support** feature switch in Power BI Desktop must be selected in order for a user with restrictive sensitivity permissions to be able to open, edit, and publish/republish a PBIX file protected by an encrypted sensitivity label. Desktop users can select/unselect the switch by opening Power BI Desktop and navigating to **File** > **Options and settings** > **Options** > **Preview features**, finding the **Less elevated user support** preview feature, and selecting or unselecting the feature as desired.

Related content

- About tenant settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Map tenant settings

09/16/2025

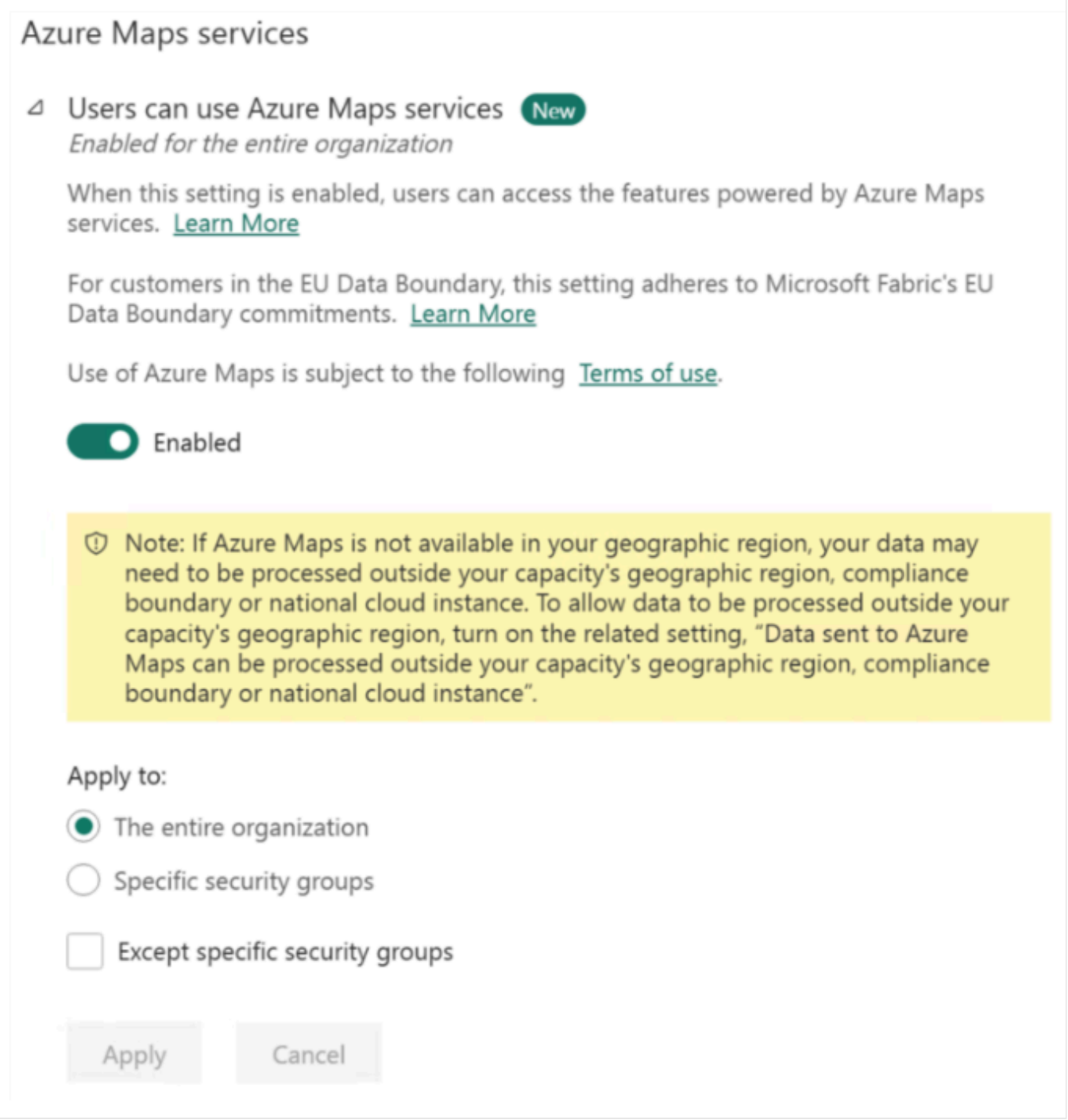
Tenant settings control whether members of your organization can use Map items. Administrators can enable or disable this feature to allow or restrict access. If enabled, users can create, view, and interact with Map items in their Fabric environment. If disabled, Map item functionality is unavailable to all users in the tenant.

Microsoft Fabric includes two tenant settings that determine whether Azure Maps services are available in Map items and Map visualizations. These settings affect user access to map-powered features, including Map items and Map visualizations within Notebooks.

Access to Azure Maps Services

When the **Users can use Azure Maps services** setting is enabled, users can access both the Map item and the Map visualization in Notebooks. These features, powered by Azure Maps, allow users to create location-aware reports, monitor real-time telemetry, and explore spatial data directly within Microsoft Fabric.

This setting determines whether members of your organization, or specific security groups, can access Azure Maps-powered experiences within Microsoft Fabric. When enabled, users can utilize features such as Interactive Maps and geospatial analytics across Fabric components like Map items, Map visualizations, and Notebooks. Disabling this setting restricts access to these location-aware capabilities, helping administrators manage data usage and compliance based on organizational needs.



Default: Enabled

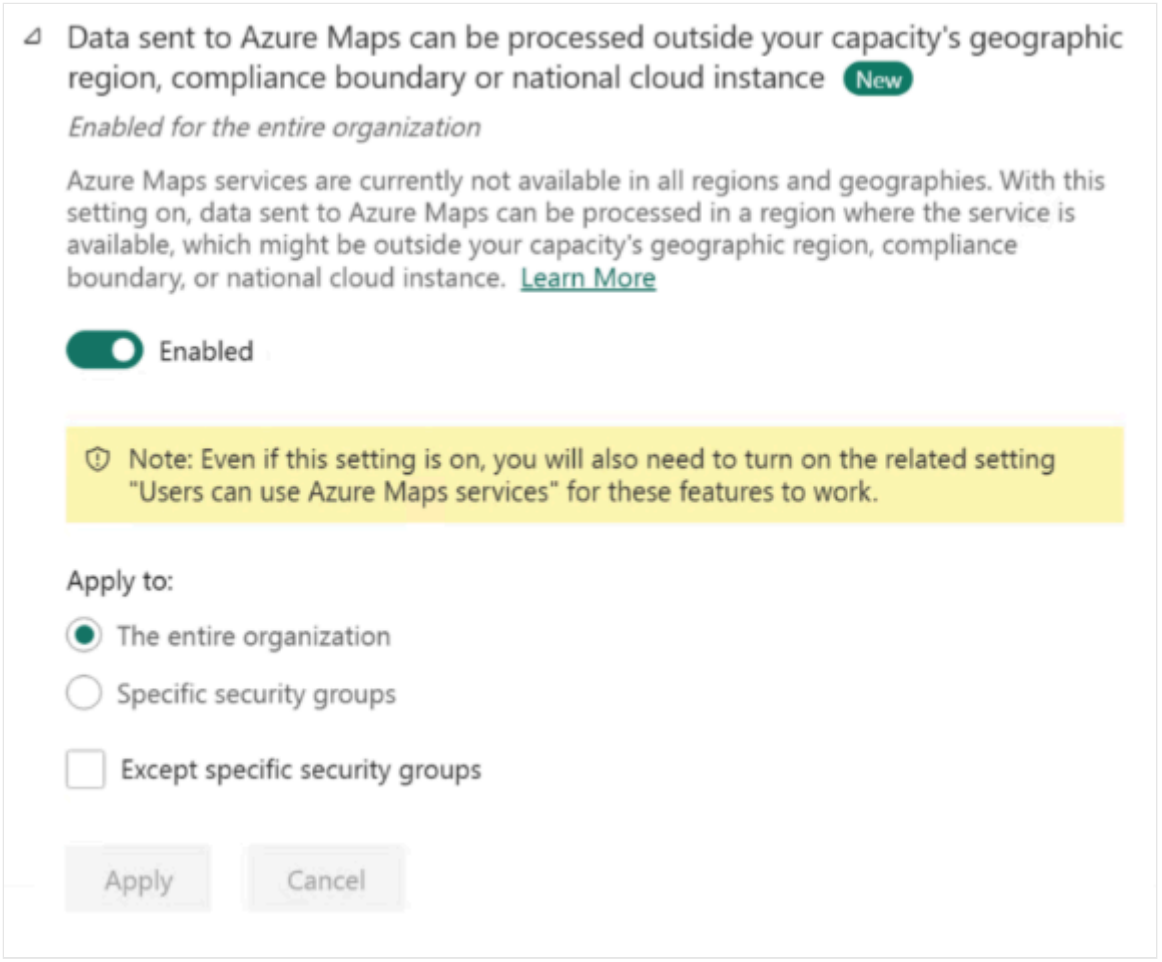
Configure global data processing

The **Data sent to Azure Maps can be processed outside your capacity's geographic region, compliance boundary or national cloud instance** setting is relevant only for customers who plan to use Map items and Map visualizations in Notebooks powered by Azure Maps, and whose capacity's geographic region is outside the supported Azure Maps service regions.

When enabled, this setting allows data sent to Azure Maps to be routed to the nearest available region, which may reside outside your organization's compliance boundary or

national cloud instance. This ensures uninterrupted access to Azure Maps capabilities in unsupported regions.

> **Note**
>
> This setting alone does not enable Azure Maps. You must also enable the setting **Users can use Azure Maps services**.



Default: Disabled

> **Note**
>
> Azure Maps does not process or transmit any customer names or personally identifiable information (PII).

Export and sharing tenant settings

Article • 05/26/2025

The export and sharing settings allow the Fabric administrator the flexibility to determine and allow Power BI content to export to formats within their organization's security and compliance guidelines. These settings also allow you to keep unauthorized export formats from being exported by users.

Sharing settings are also managed through these settings. You can determine how and who can share Power BI content in your organization, as well as determine settings for sharing content with users outside your organization. These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

External data sharing

When you turn on this setting, the users you specify will be able to share read-only links to data stored in your organization's OneLake storage with collaborators both outside and inside your organization. Collaborators who receive the link will be able to view, build on, and share the data both within and beyond their own Fabric tenants, using their organization's licenses and capacities.

External data sharing has important security considerations. For more information about external data sharing, see External data sharing.

To turn on external data sharing:

1. Go to the admin portal and open the **Tenant settings** tab.
2. Under the **Export and sharing settings** section, find and expand the **External data sharing (preview)** setting.
3. Set the toggle to **Enabled**.
4. Specify which users you want to be able to create external data shares.

Users can accept external data shares

When you turn on this setting, the users you specify will be able to accept read-only links to data from another organization’s Fabric tenant. Users who accept an external share link can view, build on, and share this data, both inside and outside of your organization. For more

information about external data sharing and its security considerations, see External data sharing.

To allow users to accept external data shares:

1. Go to the admin portal and open the **Tenant settings** tab.
2. Under the **Export and sharing settings** section, find and expand the **Users can accept external data shares (preview)** setting.
3. Set the toggle to **Enabled**.
4. Specify which users you want to be able to accept external data shares.

> ⓘ **Note**
>
> This setting is unrelated to the setting **Allow specific users to turn on external data sharing**, which refers to sharing Power BI semantic models via Entra B2B.

Guest users can access Microsoft Fabric

When you turn on this setting, Microsoft Entra Business-to-Business (Microsoft Entra B2B) guest users can access Fabric. If you turn off this setting, B2B guest users receive an error when trying to access Fabric and any Fabric items they have permissions to. Disabling this setting for the entire organization also prevents users from inviting guests to your organization. Use the specific security groups option to control which B2B guest users can access Fabric.

To learn more, see Distribute Power BI content to external guest users with Microsoft Entra B2B.

Users can invite guest users to collaborate through item sharing and permissions

This setting helps organizations choose whether new guest users can be invited to the organization through Fabric sharing, permissions, and subscription experiences.

To invite external users to your organization, the user must also have the Microsoft Entra Guest Inviter role. Once invited, external users become Microsoft Entra B2B guest users. This setting only controls the ability to invite through Fabric.

To learn more, see Invite guest users.

> ⓘ **Important**

This setting was previously called **Share content with external users**.

Guest users can browse and access Fabric content

This setting allows Microsoft Entra B2B guest users to have full access to the browsing experience using the left-hand navigation pane in the organization. Guest users who have been assigned workspace roles or specific item permissions continue to have those roles and/or permissions, even if this setting is disabled.

To learn more about sending Fabric content to Microsoft Entra B2B guest users, read Distribute Power BI content to external guest users with Microsoft Entra B2B.

Users can see guest users in lists of suggested people

This setting helps organizations limit visibility of external users in sharing experiences. When disabled, Microsoft Entra guest users aren't shown in people picker suggested users lists. This helps prevent accidental sharing to external users and seeing which external users have been added to your organization through Power BI sharing UIs.

> **Important**
>
> When the setting is set to disabled, you can still give permission to a guest user by providing their full email address in people pickers.

Publish to web

People in your organization can publish public reports on the web. Publicly published reports don't require authentication to view them.

Only admins can allow the creation of new publish-to-web embed codes. Go to Embed codes in the admin portal to review and manage public embed codes. If any of the codes contain private or confidential content remove them. Review embed codes regularly to make sure no confidential information is live on the web.

The **Publish to web** setting in the admin portal gives options for which users can create embed codes. Admins can set **Publish to web** to **Enabled** and **Choose how embed codes work** to **Allow only existing embed codes**. In that case, users can create embed codes, but they have to contact the admin to allow them to do so.

Users see different options in the UI based on the **Publish to web** setting.

Expand table

Feature	Enabled for entire organization	Disabled for entire organization	Specific security groups
Publish to web under report **More options (...)** menu	Enabled for all	Not visible for all	Only visible for authorized users or groups.
Manage embed codes under **Settings**	Enabled for all	Enabled for all	Enabled for all - **Delete** option only for authorized users or groups. - **Get codes** enabled for all.
Embed codes within admin portal	Status has one of the following values: - Active - Not supported - Blocked	Status displays **Disabled**	Status has one of the following values: - Active - Not supported - Blocked If a user isn't authorized based on the tenant setting, status displays **infringed**.
Existing published reports	All enabled	All disabled	Reports continue to render for all.

Learn more about publishing to the web.

Copy and paste visuals

Turn on this setting to allow users in the organization to copy visuals from a tile or report visual and paste them as static images into external applications.

Export to Excel

Users in the organization can export the data from a visualization to an Excel file.

To learn more, see Export the data that was used to create a visualization.

> **Note**

Fabric automatically applies a sensitivity label on the exported file and protects it according to the label's file encryption settings.

Export to .csv

Users in the organization can export data from a tile, visualization, or paginated report to a *.csv* file.

To turn this setting on or off:

1. Still in the **Export and sharing settings** section of the **Tenant Settings**, find the setting called **Export to .csv**.
2. Turn the switch on or off.
3. Under **Apply to**, select the scope of users that the setting will affect.
4. Select **Apply** to save your changes.

Download reports

Users in the organization can download .pbix files and paginated reports.

To learn more, see Download a report from the Power BI service to Power BI Desktop.

Users can work with Power BI semantic models in Excel using a live connection

Turn this setting on to allow users to export data to Microsoft Excel from a Power BI visual or semantic model, or export a semantic model to an Excel workbook with Analyze in Excel, both options with a live connection to the XMLA endpoint.

To learn more, see Create Excel workbooks with refreshable Power BI data.

Export reports as PowerPoint presentations or PDF documents

This setting lets users export reports as PowerPoint presentations or PDF documents.

- Learn how to export PowerPoint presentations.
- Learn how to export PDF documents.

Export reports as MHTML documents

Users in the organization can export paginated reports as MHTML documents when this setting is turned on.

Export reports as Word documents

This setting lets users in the organization export paginated reports as Microsoft Word documents.

To learn more, see Export Power BI paginated report to Microsoft Word.

Export reports as XML documents

This setting lets users in the organization export paginated reports as XML documents.

To learn more, see Export Power BI paginated report to XML.

Export reports as image files

Users in the organization can use the *export report to file* API to export reports as image files.

To learn more, see Export Power BI paginated report to an Image File.

Print dashboards and reports

This setting lets users in the organization print dashboards and reports.

To learn more, see Print from the Power BI service.

Certification

Choose whether people in your organization or specific security groups can certify items like apps, reports, or datamarts as trusted sources for the wider organization.

> **Important**
>
> When a user certifies an item, their contact details are visible along with the certification badge.

Read Enable content certification for more details.

Users can set up email subscriptions

This setting lets users create email subscriptions to reports and dashboards. Read Email subscriptions for reports and dashboards in the Power BI service to learn more.

B2B guest users can set up and be subscribed to email subscriptions

There may be instances that admin may want B2B guest users to receive email subscriptions but not other external users. Use this setting to allow B2B guest users to set up and subscribe themselves to email subscriptions.

If this setting is off, only users in your organization can create and receive email subscriptions.

> ⓘ **Important**
>
> The **Allow email subscriptions to be sent to external users** switch will be automatically turned off if the **B2B guest users can set up and be subscribed to email subscriptions** switch is turned off. This is because B2B users are external users that have been granted elevated permissions to get content. Since B2B guest users have higher permissions than other external users, if they can't get the email subscription neither can the other external users.

Users can send email subscriptions to guest users

Users can send email subscriptions to guest users. With this setting off, users in your organization can't subscribe guest users to subscription emails.

Featured content

This setting lets you enable or disable the ability of users in your organization to promote their published content to the **Featured** section of the Power BI Home page. By default, anyone with the Admin, Member, or Contributor role in a workspace in your organization can feature content on Power BI Home.

To learn more, see Feature content on colleagues' Power BI Home page.

You can also manage featured content on the **Featured content** page in the Admin portal. Go to Manage featured content for more details.

Allow connections to featured tables

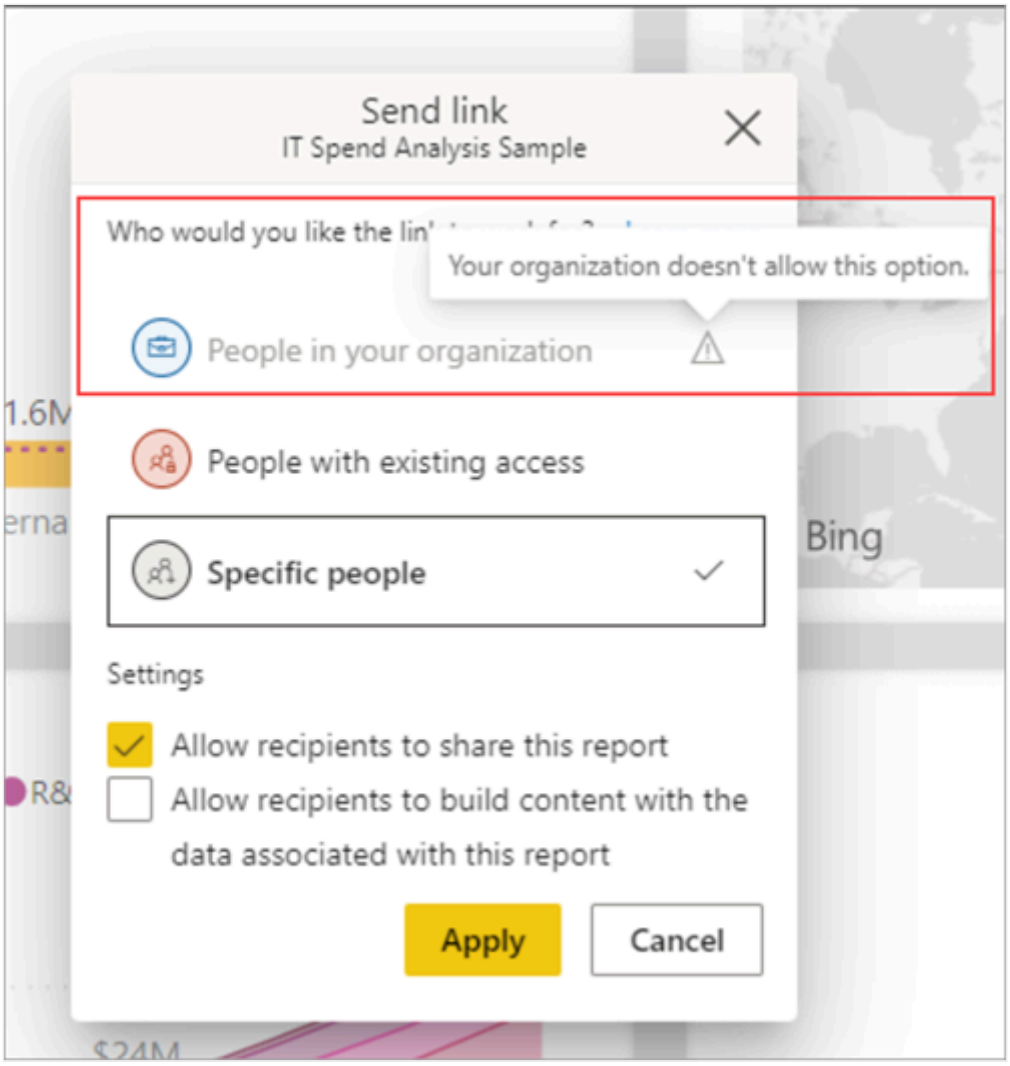
This setting lets Fabric admins control who in the organization can use featured tables in the Excel Data Types Gallery. Read more about Power BI featured tables in Excel.

> **Note**
>
> Connections to featured tables are also disabled if the **Allow live connections** setting is set to Disabled.

Allow shareable links to grant access to everyone in your organization

This tenant setting is available for admins looking to disable creating shareable links to **People in your organization**.

If this setting is turned off for a user with permissions to share a report, that user can only share the report via link to **Specific people** or **People with existing access**. The following image shows what that user sees if they attempt to share the report via link:



To learn more, see Link settings.

Enable Microsoft Teams integration

This setting allows organizations to access features that work with Microsoft Teams and the Power BI service. These features include launching Teams experiences from Power BI like chats, the Power BI app for Teams, and getting Power BI notifications from Teams. To completely enable or disable Teams integration, work with your Teams admin.

Read more about collaborating in Microsoft Teams with Power BI.

Install Power BI app for Microsoft Teams automatically

Automatic installation makes it easier to install the Power BI app for Microsoft Teams, without needing to change Microsoft Teams app setup policies. This change speeds up the installation and removes admin hassles of configuring and maintaining infrastructure needed by an app setup policy.

When the app is installed, users receive notifications in Teams and can more easily discover and collaborate with colleagues. The Power BI app for Teams provides users with the ability to open all Fabric content.

Automatic installation happens for a user under the following conditions:

- The Power BI app for Microsoft Teams is set to **Allowed** in the Microsoft Teams admin portal.
- The Power BI tenant setting **Install Power BI app for Microsoft Teams automatically** is **Enabled**.
- The user has a Microsoft Teams license.
- The user opens the Power BI service in a web browser.

When the app is installed, users receive notifications in Teams and can more easily discover and collaborate with colleagues. The Power BI app for Teams provides users with the ability to open all Fabric content.

To learn more, see Add the Power BI app to Microsoft Teams.

Enable Power BI add-in for PowerPoint

The Power BI add-in for PowerPoint makes it possible for users to add live, interactive data from Power BI to a PowerPoint presentation. See About the Power BI add-in for PowerPoint for more detail.

When this setting is on (default), entry points for opening a new PowerPoint presentation with the add-in already loaded are available in Power BI. When this setting is off, the entry points in Power BI are unavailable.

This integration requires that your organization's Microsoft Office admin has enabled support for add-ins.

> **Note**
>
> If you turn this setting off, that doesn't prevent people from using the add-in starting from PowerPoint. To completely block adding live Power BI report pages to PowerPoint slides using the add-in, the add-in must be turned off in both Power BI and PowerPoint.

Allow DirectQuery connections to Power BI semantic models

When this setting is turned on (default), users can use DirectQuery to connect to Azure Analysis Services or Power BI datasets.

To learn more about DirectQuery, see Use DirectQuery in Power BI Desktop.

If you turn this switch off, it effectively stops users from publishing new composite models on Power BI semantic models to the service. Existing reports that leverage a composite model on a Power BI semantic model continue to work, and users are still able to create composite models using Desktop, but they can't publish to the service.

To learn more about composite models, see Use composite models in Power BI Desktop.

> **Note**
>
> Live connections to Power BI semantic models aren't affected by this switch, nor are live or DirectQuery connections to Azure Analysis Services. These continue to work regardless of whether the setting is on or off. In addition, any published reports that leverage a composite model on a Power BI semantic model continue to work even if the setting has been turned off after they were published.

Guest users can work with shared semantic models in their own tenants

When this setting is turned on, Microsoft Entra B2B guest users of semantic models shared with them by users in your organization can access and build on those semantic models in their own tenant.

This setting is off by default for customers. If this setting is disabled, a guest user can still access the semantic model in the provider tenant but not in their own tenant.

Allow specific users to turn on external data sharing

As a Fabric admin, you can specify which users or user groups in your organization can share semantic models externally with guests from a different tenant through the in-place mechanism. Authorized guest users can then discover, connect to, and work with these shared semantic models in their own tenants.

Disabling this setting prevents any user from sharing semantic models externally by blocking the ability of users to turn on external sharing for semantic models they own or manage.

> **Note**
>
> This setting relates to sharing Power BI semantic models via Entra B2B capabilities. It is unrelated to the **External data sharing (preview)** and **Users can accept external data shares (preview)** tenant settings, which control the external data sharing feature. The external data sharigin feature enables sharing data from an organization's OneLake storage locations to external Fabric tenants, and uses secure Fabric-to-Fabric communication channels rather than Entra B2B.

Users can deliver reports to OneDrive and SharePoint in Power BI

Users can deliver reports to OneDrive or SharePoint. If the **Users can set up subscriptions** setting is also turned on, users can use subscriptions to schedule delivery of these reports to OneDrive or SharePoint.

Related content

- About tenant settings
- Tenant settings index

Discovery tenant settings

Article • 11/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Discoverability is a feature that semantic model owners can use to make their endorsed content discoverable by users who don't yet have access to it.

Make promoted content discoverable

Allow users in this organization who can promote content to make content they promote discoverable by users who don't have access to it. You can also specify users and/or groups to exclude from the permitted groups.

To learn more, see Semantic model discoverability.

Make certified content discoverable

Allow users in the organization who can certify content to make content they certify discoverable by users who don't have access to it.

Discover content

Allow users to find and request access to content they don't have access to if it was made discoverable by its owners.

To learn more, see Find recommended items.

Related content

- About tenant settings

Feedback

App tenant settings

Article • 11/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Create template organizational apps

Users in the organization can create template apps that use semantic models built on one data source in Power BI Desktop.

To learn more, see Create a template app in Power BI.

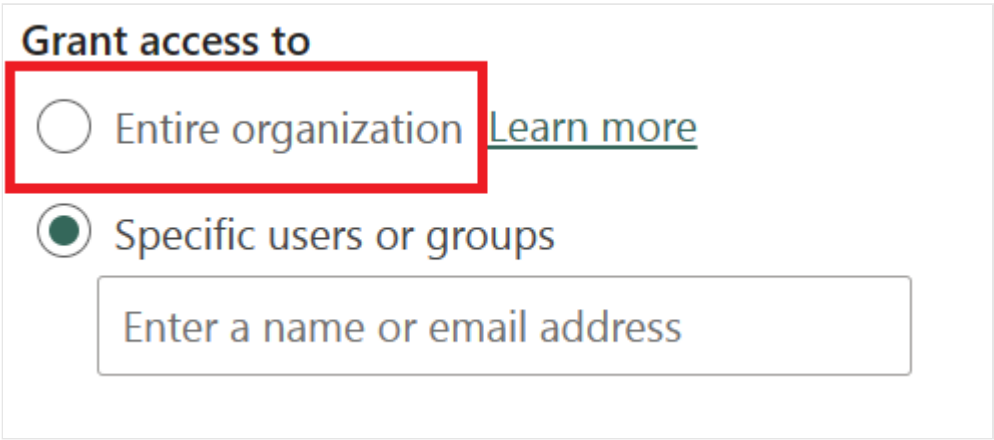
Push apps to end users

Admins can allow report creators to share apps directly with end users, without requiring installation from AppSource. In the admin portal, the setting is **Push apps to end users**.

To learn more, see Automatically install apps for end users.

Publish apps to the entire organization

Admins use this setting to decide which users can publish apps to the entire organization, rather than specific groups. The following image shows the **Entire organization** option when creating an app.



To learn more, see Publish an app in Power BI.

Related content

- About tenant settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Configure Fabric data agent tenant setting

07/21/2025

To use a data agent in Microsoft Fabric, you must configure the required tenant settings. Additionally, if your Fabric data agent uses a Power BI semantic model as a data source, specific tenant settings must be enabled to allow connectivity. This guide walks you through the necessary configurations for a seamless setup.

Accessing tenant settings

To configure the required settings, you need administrative privileges to access the **Admin Portal** in Microsoft Fabric.

1. **Sign in to Microsoft Fabric** with an admin account.
2. **Open the Admin Portal**:
    - Select the gear icon in the top-right corner.
    - Select **Admin Portal**.
3. **Navigate to Tenant Settings**:
    - In the Admin Portal, select **Tenant settings** from the left-hand navigation pane.

Once you are in **Tenant Settings**, you can proceed with enabling the necessary configurations.

> ⓘ **Note**
>
> The tenant settings might need up to one hour to take effect after you enable them.

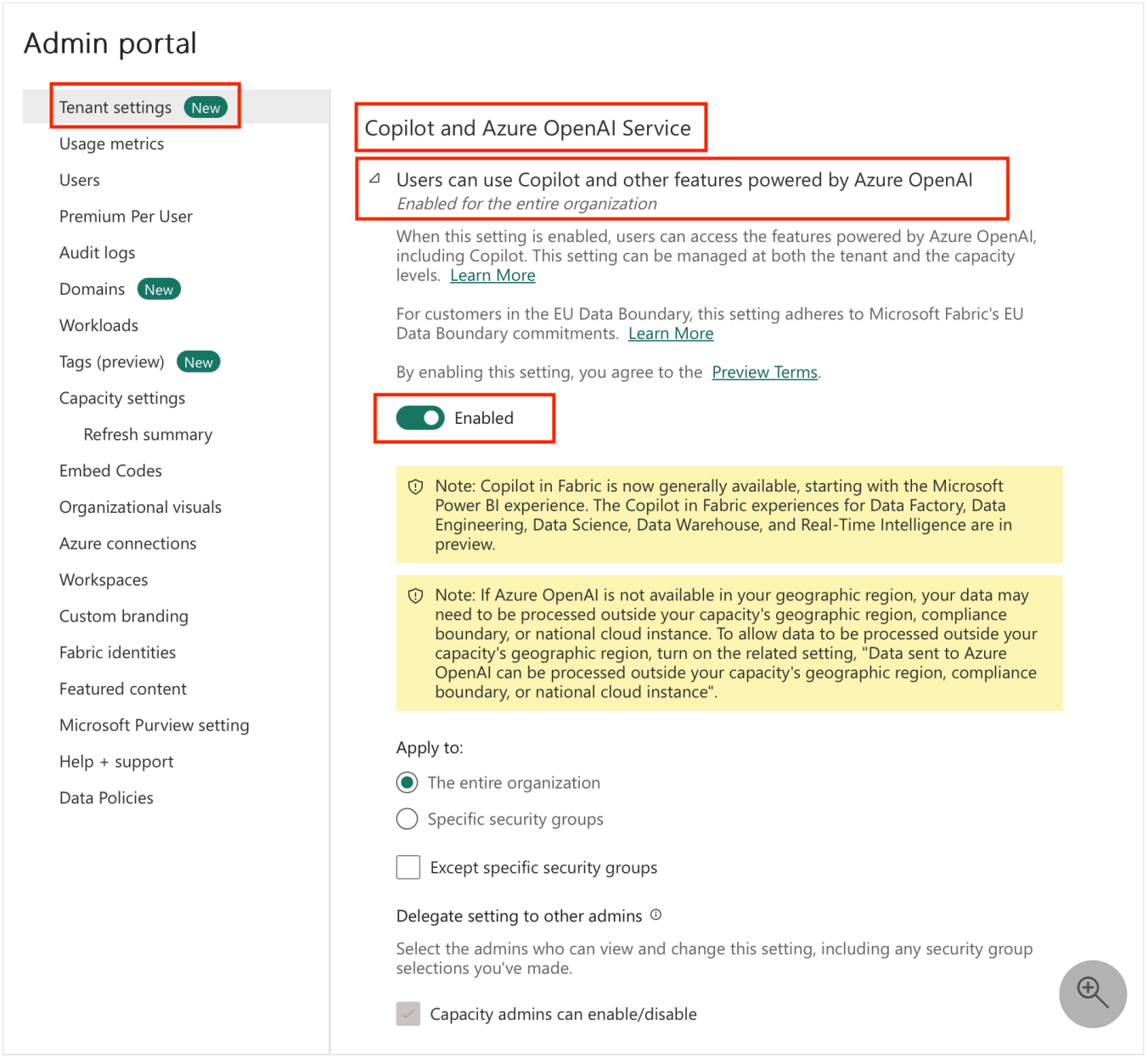
Enable Copilot and Azure OpenAI tenant switch

For a Fabric data agent to function properly, the **Copilot and Azure OpenAI Service** tenant settings must be enabled. These settings control user access and data processing policies.

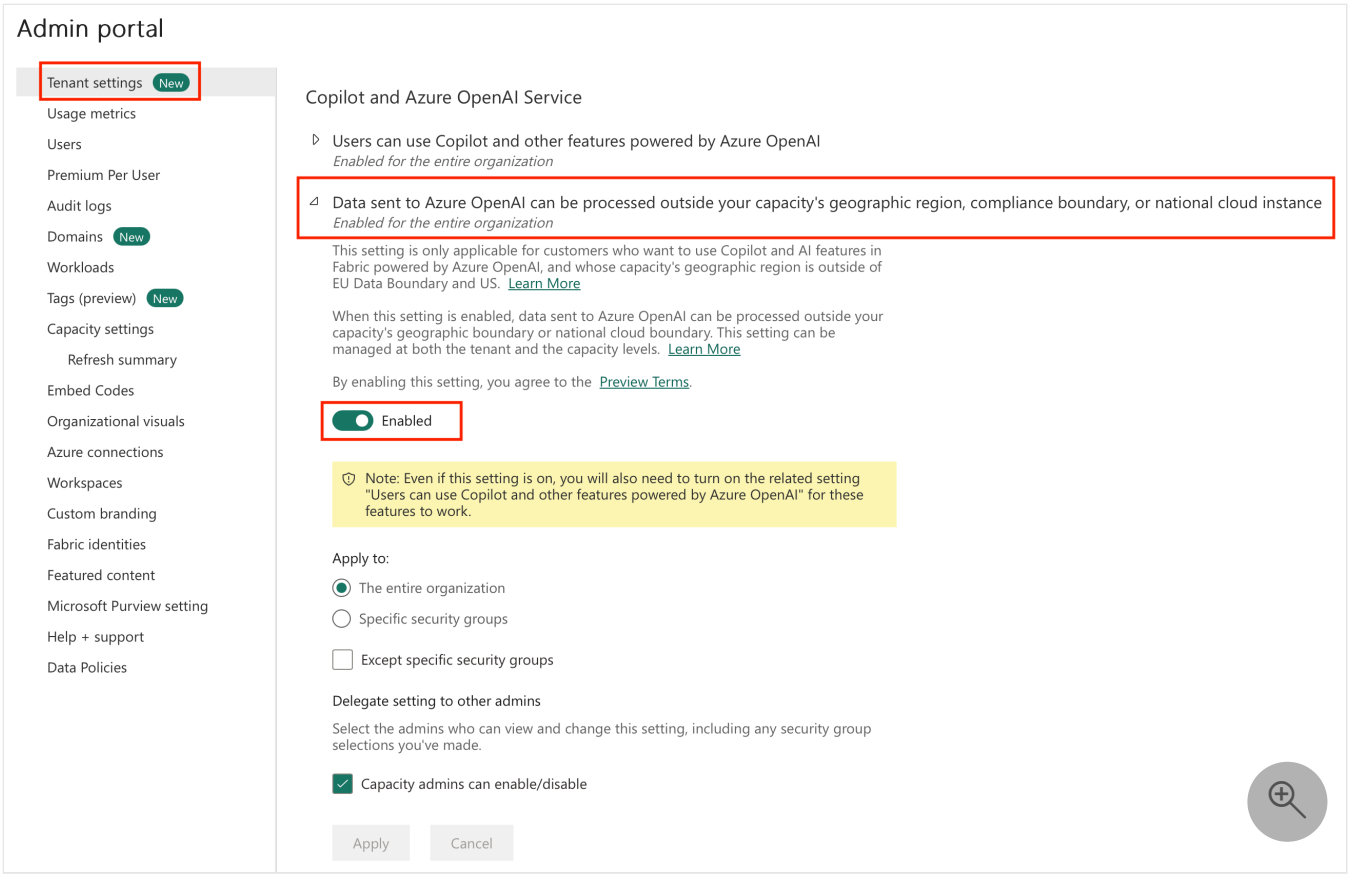
Required settings

- **Users can use Copilot and other features powered by Azure OpenAI**:
    - This must be enabled to allow users to access Copilot-powered features, including Fabric data agent. This setting can be managed at both the tenant and the capacity levels. For more information, see Overview of Copilot in Fabric.

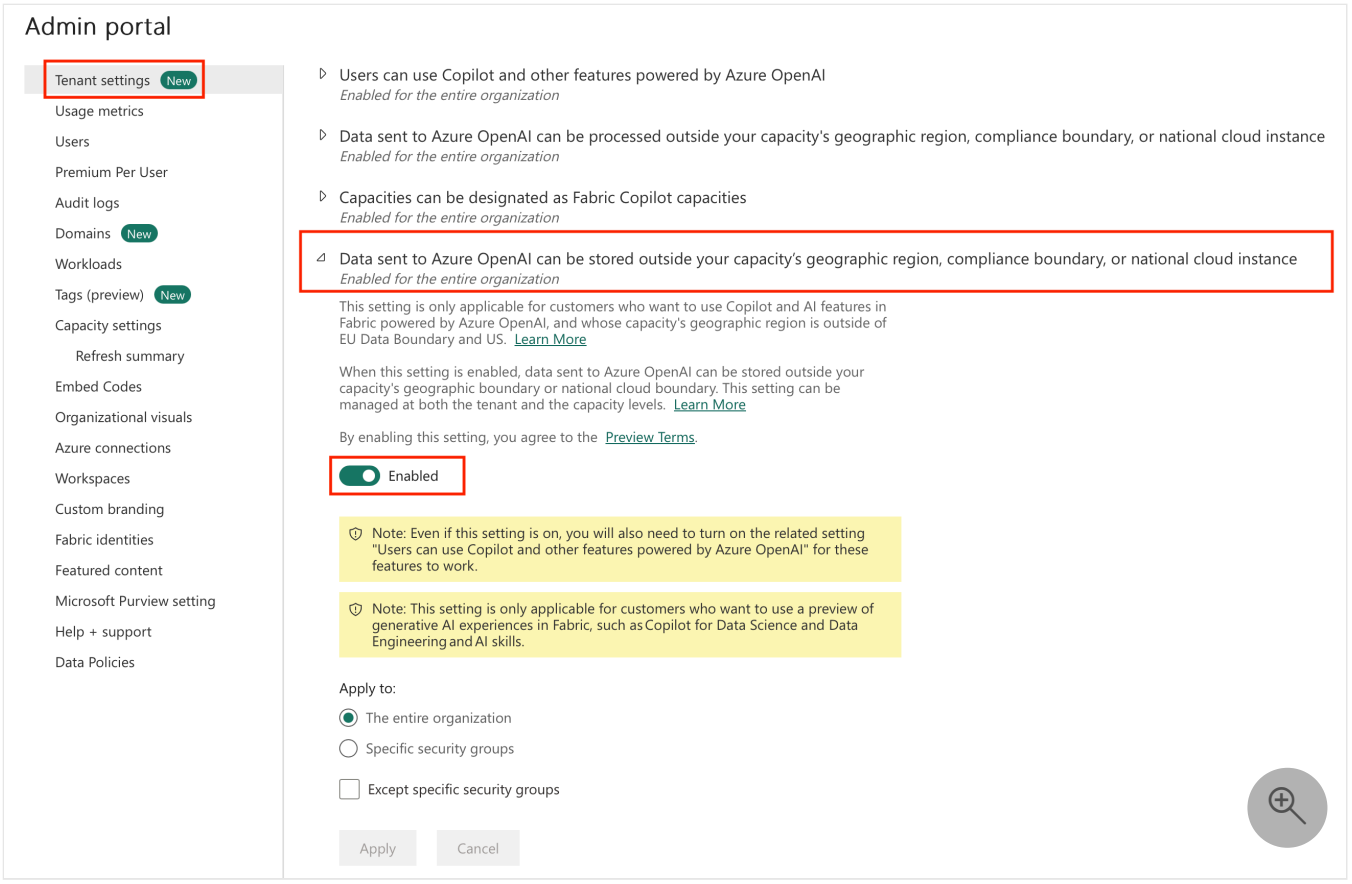
- To enable this setting, check the option in **Tenant Settings** as shown in the next screenshot:



- **Data sent to Azure OpenAI can be processed outside your capacity's geographic region, compliance boundary, or national cloud instance**
  - Required for customers using Fabric data agent whose capacity's geographic region is outside of the EU data boundary and the US.
  - To enable this setting, check the option in **Tenant Settings** as shown in the next screenshot:



- **Data sent to Azure OpenAI can be stored outside your capacity's geographic region, compliance boundary, or national cloud instance**
  - Required for customers using Fabric data agent whose capacity's geographic region is outside of the EU data boundary and the US.
  - To enable this setting, check the option in **Tenant Settings** as shown in the next screenshot:

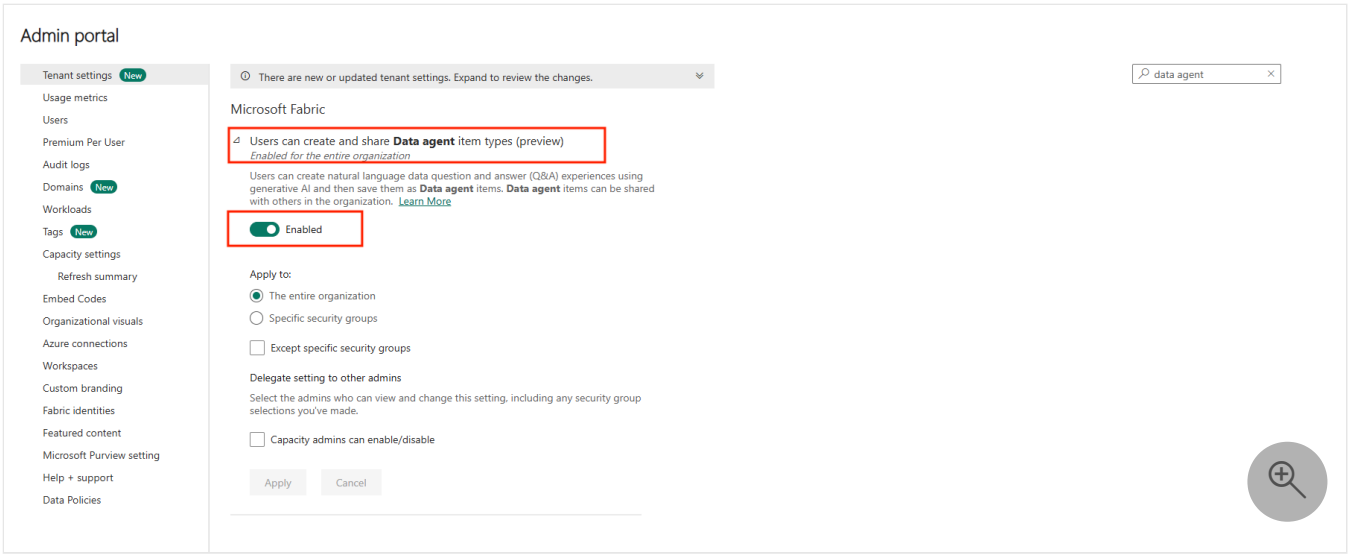


Enable Fabric data agent tenant settings

By default, the Fabric data agent feature is disabled at the tenant level. To allow users to create and share Fabric data agent items, administrators must enable this setting. This activation allows users to craft natural language Q&A experiences using generative AI, and then share the Fabric data agent within the organization.

Steps to enable Fabric data agent

1. In **Tenant Settings**, locate the **Fabric data agent** section.
2. To enable this setting, check the option in **Tenant Settings** as shown in the next screenshot:

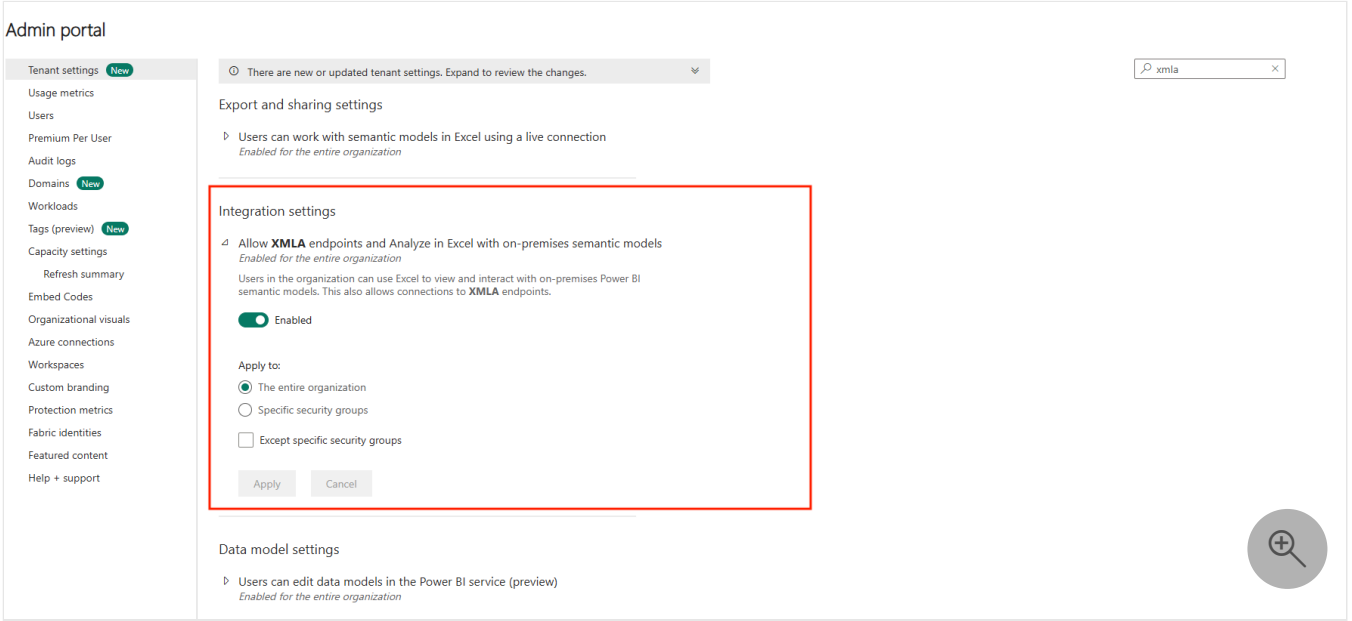


Enable integration of Power BI semantic models via XMLA endpoints

Fabric data agents can query and manage Power BI semantic models programmatically via XMLA (XML for Analysis) endpoints. To enable this functionality, XMLA endpoints must be configured correctly.

Steps to enable XMLA endpoints

1. In **Tenant Settings**, navigate to the **Integration settings** section.
2. Locate **Allow XMLA endpoints and Analyze in Excel with on-premises datasets** and then enable it, as shown in the next screenshot:



Related content

- Data agent concept
- About tenant settings

Copilot tenant settings

10/15/2025

Fabric Copilot settings are controlled by the **Copilot and Azure OpenAI Service** tenant settings group. There are multiple settings governing user access and data processing policies, and some of them are enabled by default whereas others require the Fabric administrator to enable them.

For information about how to get to the Fabric tenant settings, see About tenant settings - How to get to the tenant settings.

Settings enabled by default

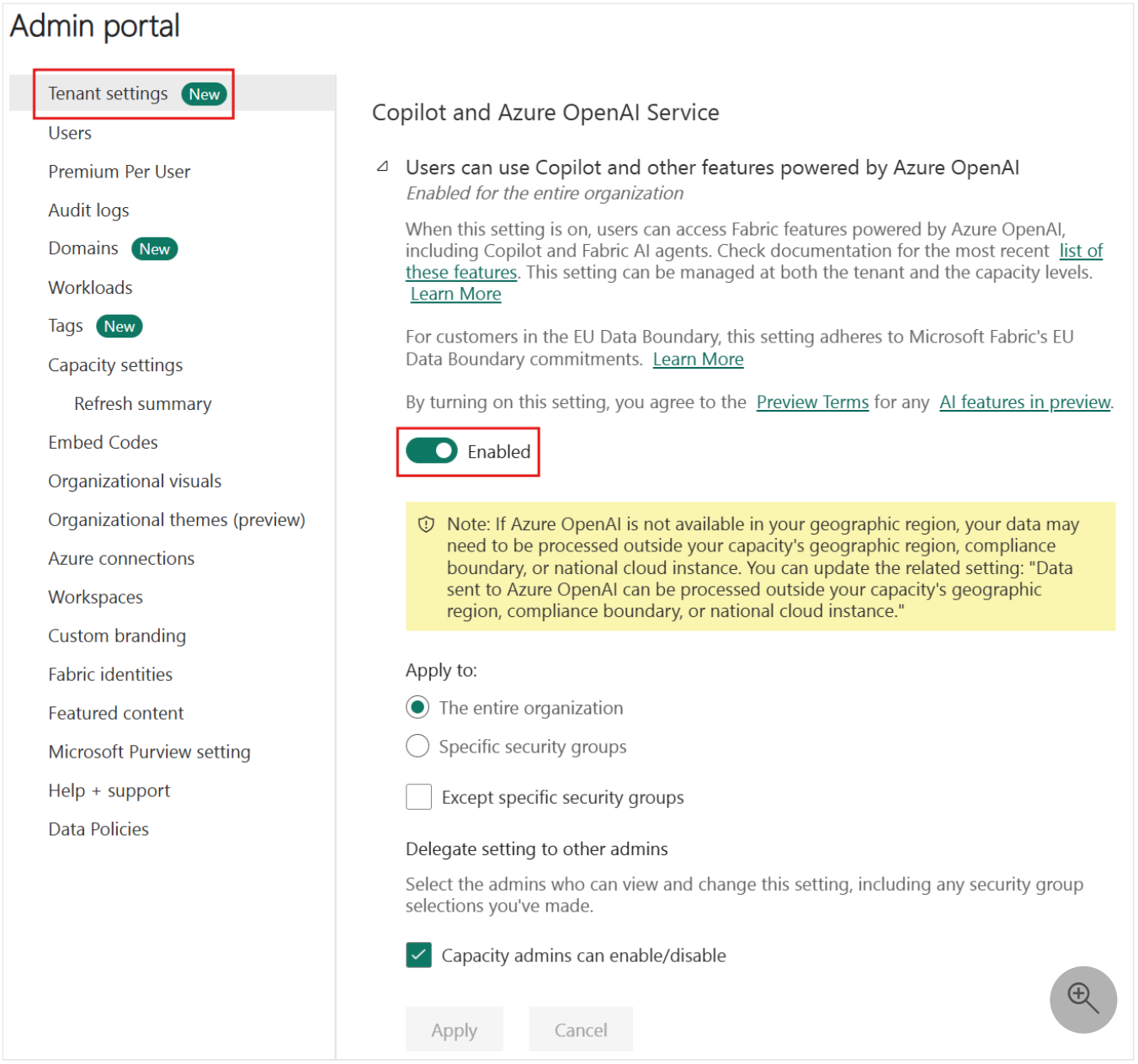
- Users can use Copilot and other features powered by Azure OpenAI

Settings disabled by default

- Capacities can be designated as Fabric Copilot capacities
- Data sent to Azure OpenAI can be processed outside your capacity's geographic region, compliance boundary, or national cloud instance
- Data sent to Azure OpenAI can be stored outside your capacity's geographic region, compliance boundary, or national cloud instance
- Users can access a standalone, cross-item Power BI Copilot experience (preview)
- Only show AI-prepped items in the standalone Copilot in Power BI experience (preview)

Users can use Copilot and other features powered by Azure OpenAI

When this setting is enabled, users can access the features powered by Azure OpenAI, including Copilot, as shown in the following screenshot:



This setting can be managed at both the tenant and the capacity levels. When this setting is enabled, the service may execute background jobs at no charge to the tenant capacity to support end user experiences. For more information, see Overview of Copilot in Fabric.

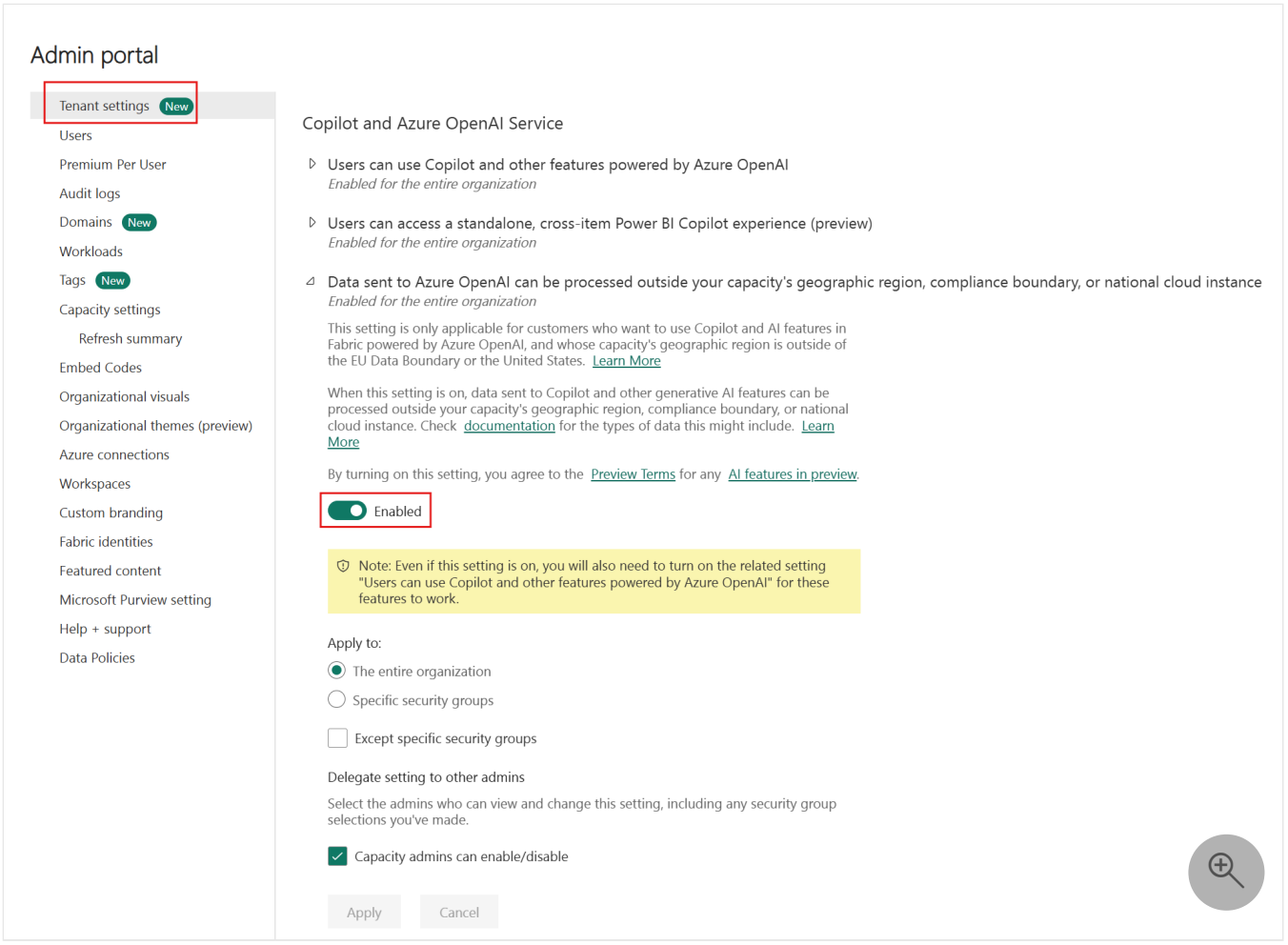
Default: Enabled

Data sent to Azure OpenAI can be processed outside your capacity's geographic region, compliance boundary, or national cloud instance

This setting is only applicable for customers who want to use Copilot and AI features in Fabric powered by Azure OpenAI, and whose capacity's geographic region is outside of the EU data boundary and the US. When this setting is enabled, service background jobs may execute

across geographic boundaries at no charge to the tenant capacity to support end user experiences.

The following screenshot shows how to make this setting:

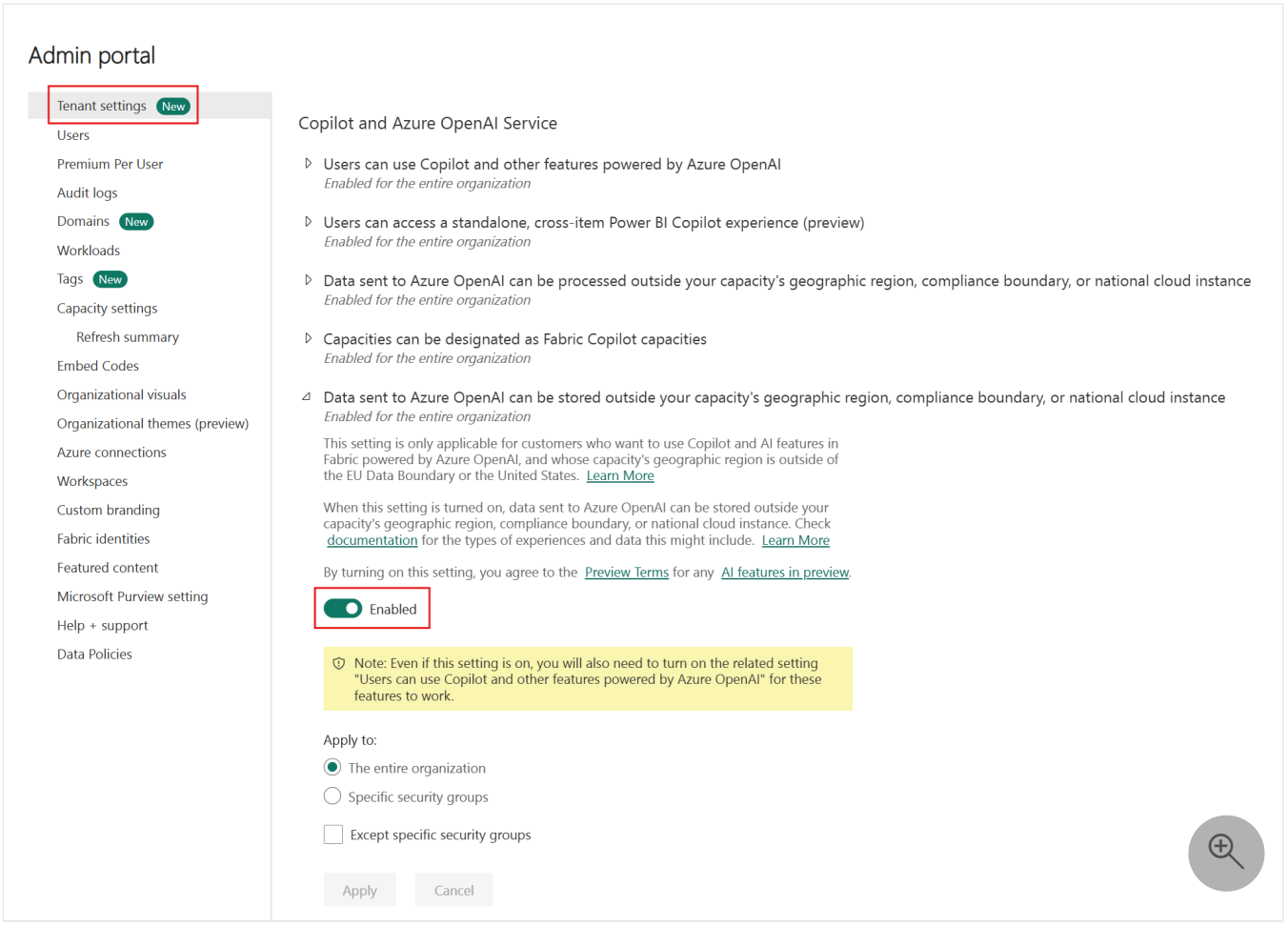


For more information, visit the Available regions resource.

Default: Disabled

Data sent to Azure OpenAI can be stored outside your capacity's geographic region, compliance boundary, or national cloud instance

This setting is only applicable for customers who want to use Copilot in Notebooks and the Data agent Feature in Fabric powered by Azure OpenAI, and whose capacity's geographic region is outside of the EU data boundary and the US. The following screenshot shows how to make this setting:



For more information, visit the Available regions resource.

Default: Disabled

Conversation history stored outside your capacity's geographic region, compliance boundary, or national cloud instance

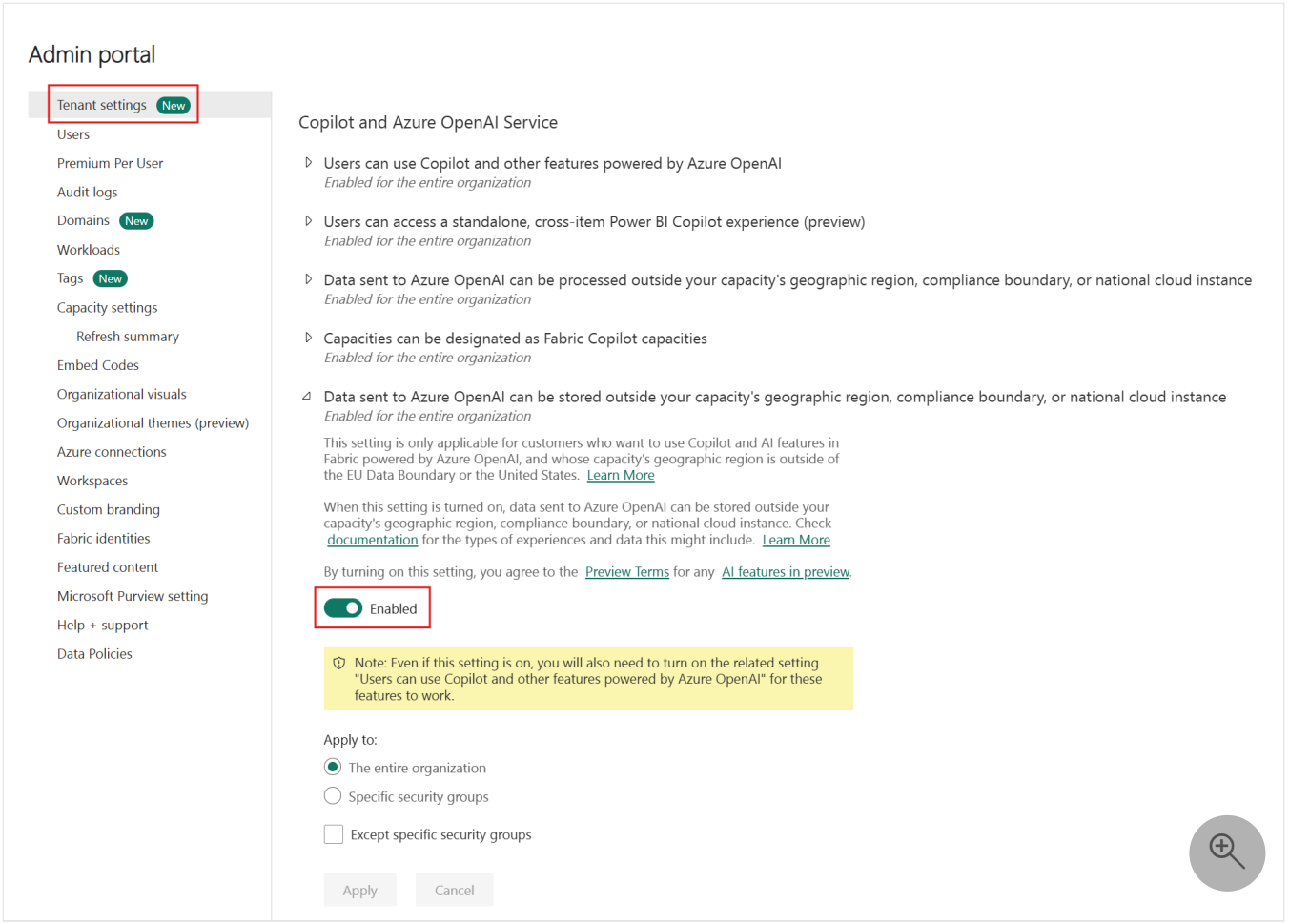
Note that this setting is **only** applicable for customers who want to use Copilot in Notebooks and Fabric data agents (formerly known as Data agent) powered by Azure OpenAI, and whose capacity's geographic region is outside of the EU data boundary and the US.

In order to use fully conversational agentic AI experiences, the agent needs to store conversation history across user sessions. This ensures that the AI agent keeps context about what a user asked in previous sessions and is a desired behavior in many agentic experiences. Experiences such as Copilot in Notebooks and Fabric data agents are AI experiences that store conversation history across the user's sessions. **This history is stored inside the Azure security boundary, in the same region and in the same Azure OpenAI resources that process all your Fabric AI requests.** The difference in this case is that the conversation history is stored for as

log as the user allows. For experiences that don't store conversation history across sessions, no data is stored. Prompts are only processed by Azure OpenAI resources that Fabric uses.

Your users can delete their conversation history at any time, simply by clearing the chat. This option exists both for Copilot in Notebooks and data agents. If the conversation history isn't manually removed, it is stored for 28 days.

The following screenshot shows how to enable this setting:

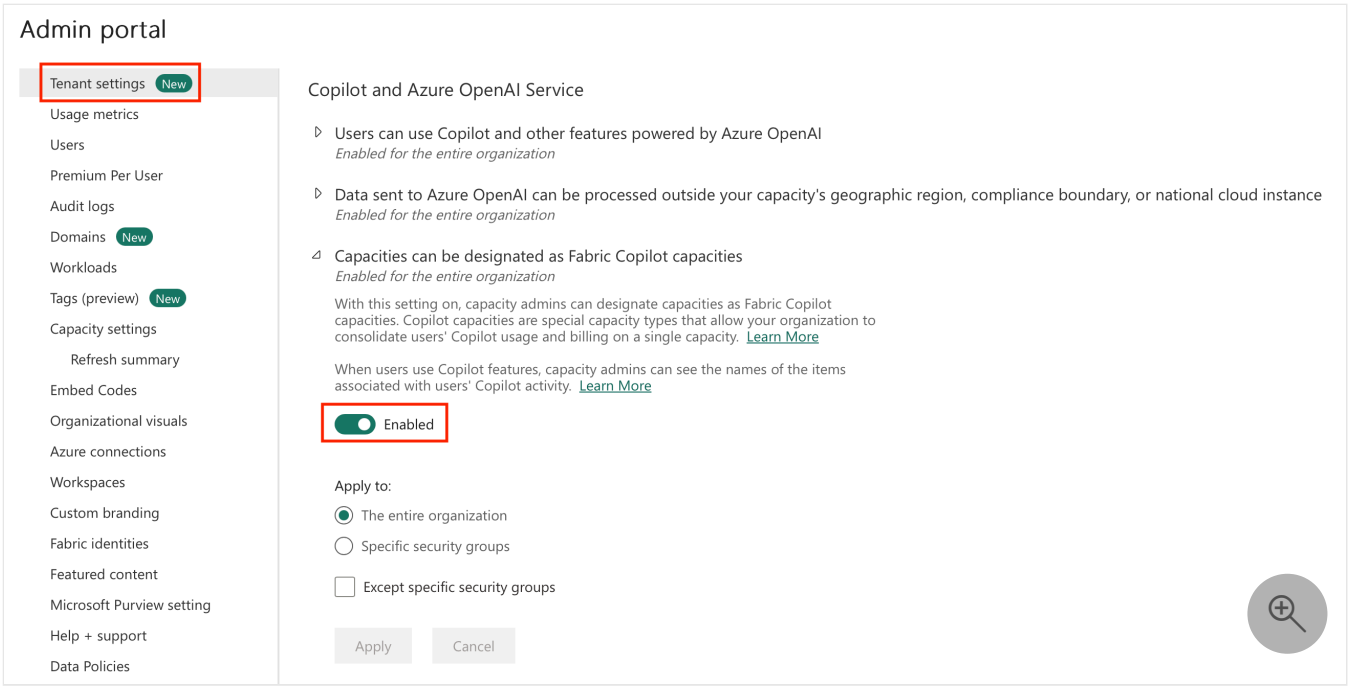


For more information, visit the Available regions resource.

Default: Disabled

Capacities can be designated as Fabric Copilot capacities

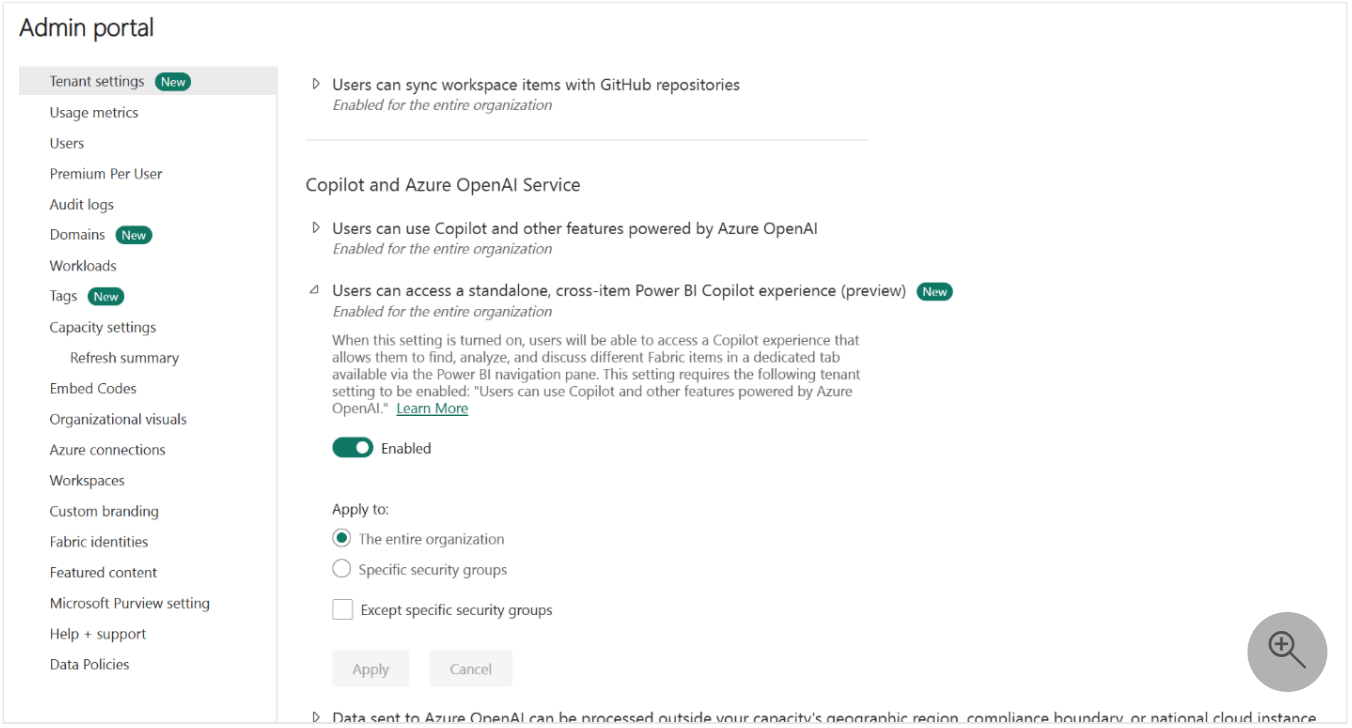
Copilot capacities enable users' usage and billing to be consolidated under a single capacity. Fabric administrators can assign specific groups or the entire organization to manage capacities as Fabric Copilot capacities. Capacity administrators must designate user access to each Copilot capacity and can view item names linked to users' Copilot activity in the Fabric capacity metrics app.



Default: Disabled

Users can access a standalone, cross-item Power BI Copilot experience (preview)

You can enable copilot as a standalone experience for Fabric. Enabling this setting allows users to access the standalone Copilot experience from the left navigation. The Azure OpenAI setting must be enabled at the tenant level to use the standalone experience. This setting also affects the Power BI agent. Turn on this setting to enable the Power BI agent in Microsoft 365. To learn more, see standalone Copilot experience.

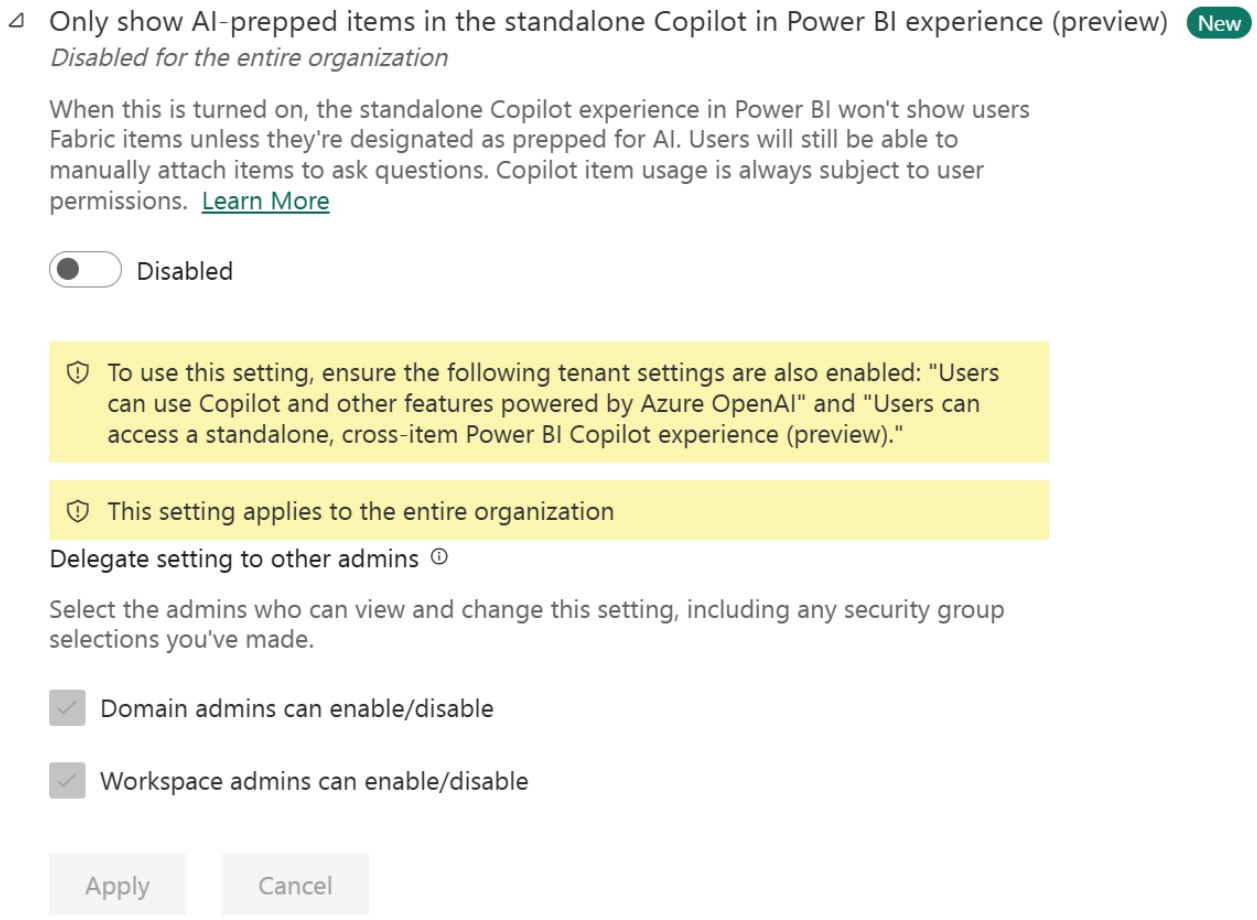


Default: Disabled

Only show AI-prepped items in the standalone Copilot in Power BI experience (preview)

Tenant admins can default Copilot search to be limited to items that have prepped for AI. This setting is delegated to workspace admins by default, allowing workspace admins to make broader content findable by Copilot search when appropriate.

Note that this setting is applicable in the standalone Power BI Copilot as well as the Power BI agent. If this setting is turned on for standalone Copilot, it is also mandatory for the Power BI agent. To learn more, see standalone Copilot experience.



Default: Disabled

Related content

- Copilot in Fabric and Power BI overview
- About tenant settings

Integration tenant settings

09/02/2025

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Allow XMLA endpoints and Analyze in Excel with on-premises datasets

When enabled, users in the organization can use Excel to view and interact with on-premises Power BI semantic models. This also allows connections to XMLA endpoints.

To learn more, see Create Excel workbooks with refreshable Power BI data.

Dataset Execute Queries REST API

When enabled, users in the organization can query semantic models by using Data Analysis Expressions (DAX) through Power BI REST APIs.

To learn more, see Datasets - Execute Queries.

Use ArcGIS Maps for Power BI

When enabled, users in the organization can use the ArcGIS Maps for Power BI visualization provided by Esri.

To learn more, see Create ArcGIS maps in Power BI.

Use global search for Power BI

When enabled, users in the organization can use external search features that rely on Azure Search.

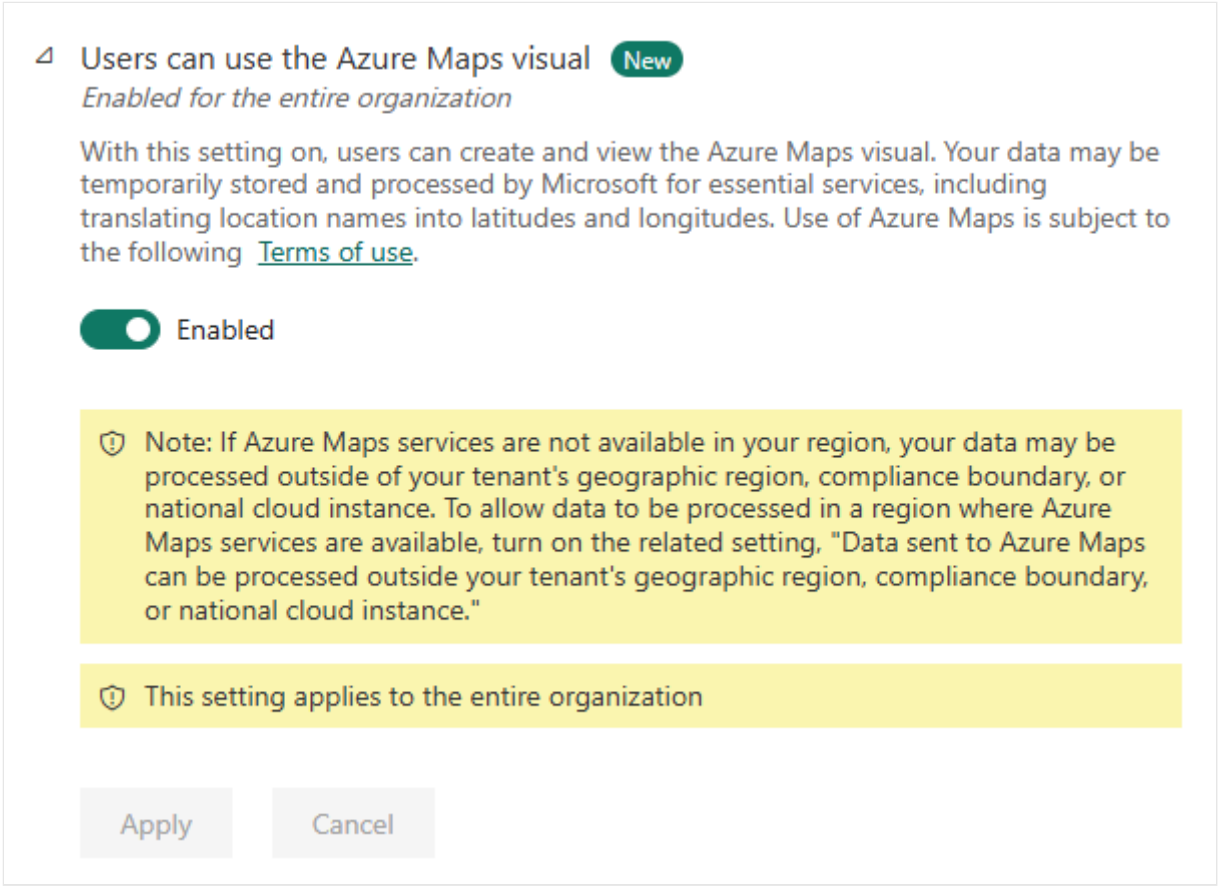
To learn more, see Navigation for Power BI business users: global search.

Use Azure Maps Visual

When enabled, users in the organization can create and view reports that use the Azure Maps visual.

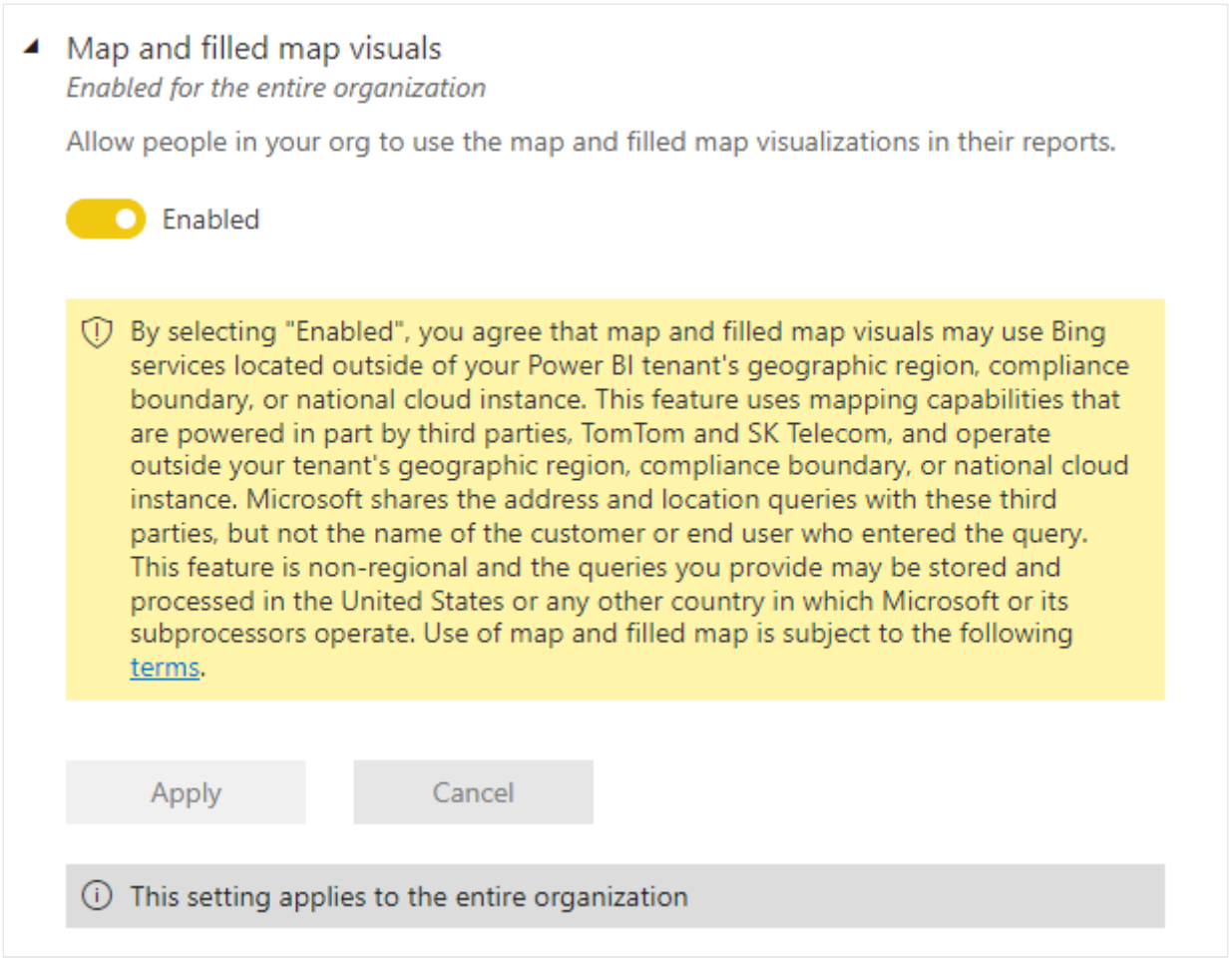
- Microsoft temporarily stores and processes your data for essential services like translating locations into latitudes and longitudes.
- If Azure Maps services are unavailable in your region, your data can be processed outside your tenant's geographic region, compliance boundary, or national cloud instance.

To learn more, see Get started with Azure Maps Power BI visual.



Map and filled map visuals

When enabled, users in the organization can use map and filled map visualizations in their reports.



> **Note**
>
> In a future release, Power BI plans to deprecate older map visuals and migrate existing reports to Azure Maps. Learn about converting to Azure Maps.

Integration with SharePoint and Microsoft Lists

Users in the organization can create Fabric reports directly from SharePoint and Microsoft Lists. Then they can build Fabric reports on the data in those lists and publish them back to the lists, to be visible to others who can access the list.

This setting is enabled by default. Even if the feature is disabled, in SharePoint and Microsoft Lists users can still see **Power BI** > **Visualize the list**, and any existing reports, on the **Integrate** menu. If they select **Visualize the list**, they go to an error page explaining that their admin disabled the feature.

Learn more about creating reports from SharePoint and Microsoft Lists.

Dremio SSO

Enable SSO capability for Dremio. By enabling, user access token information, including name and email, is sent to Dremio for authentication.

To learn more, see Microsoft Entra ID-based Single Sign-On for Dremio Cloud and Power BI.

Snowflake SSO

For semantic model owners to be able to enable single sign-on for DirectQuery connections to Snowflake in semantic model settings, a Fabric admin must enable the **Snowflake SSO** setting. This setting approves sending Microsoft Entra credentials to Snowflake for authentication for the entire organization.

To learn more, see Connect to Snowflake in the Power BI Service.

Redshift SSO

Enable SSO capability for Redshift. By enabling, user access token information, including name and email, is sent to Redshift for authentication.

To learn more, see Overview of single sign-on for on-premises data gateways in Power BI.

Google BigQuery SSO

Enable SSO capability for Google BigQuery. By enabling, user access token information, including name and email, is sent to Google BigQuery for authentication.

To learn more, see Google BigQuery (Azure AD).

Oracle SSO

Enable SSO capability for Oracle. By enabling, user access token information, including name and email, is sent to Oracle for authentication.

To learn more, see Overview of single sign-on for on-premises data gateways in Power BI.

Microsoft Entra Single Sign-On (SSO) for Gateway

This setting enables Microsoft Entra SSO through on-premises data gateways to cloud data sources that rely on Microsoft Entra ID-based authentication. It gives seamless Microsoft Entra SSO connectivity to Azure-based data sources, such as Azure Synapse Analytics (SQL DW),

Azure Data Explorer, Snowflake on Azure, and Azure Databricks through an on-premises data gateway.

This feature is important for users who work with reports that require SSO connectivity in DirectQuery mode to data sources deployed in an Azure virtual network (Azure VNet). When you configure SSO for an applicable data source, queries execute under the Microsoft Entra identity of the user that interacts with the Power BI report.

An important security-related consideration is that gateway owners have full control over their on-premises data gateways. This means that it's theoretically possible for a malicious gateway owner to intercept Microsoft Entra SSO tokens as they flow through an on-premises data gateway (this isn't a concern for VNet data gateways because they're maintained by Microsoft).

Because of this possible threat, the Microsoft Entra SSO feature is disabled by default for on-premises data gateways. As a Fabric admin, you must enable the **Microsoft Entra Single Sign-On (SSO) for Gateway** tenant setting in the Fabric admin portal before data sources can be enabled for Microsoft Entra SSO on an on-premises data gateway. Before enabling the feature, make sure to restrict the ability to deploy on-premises data gateways in your organization to appropriate administrators.

To learn more, see Microsoft Entra SSO.

Power Platform Solutions Integration (Preview)

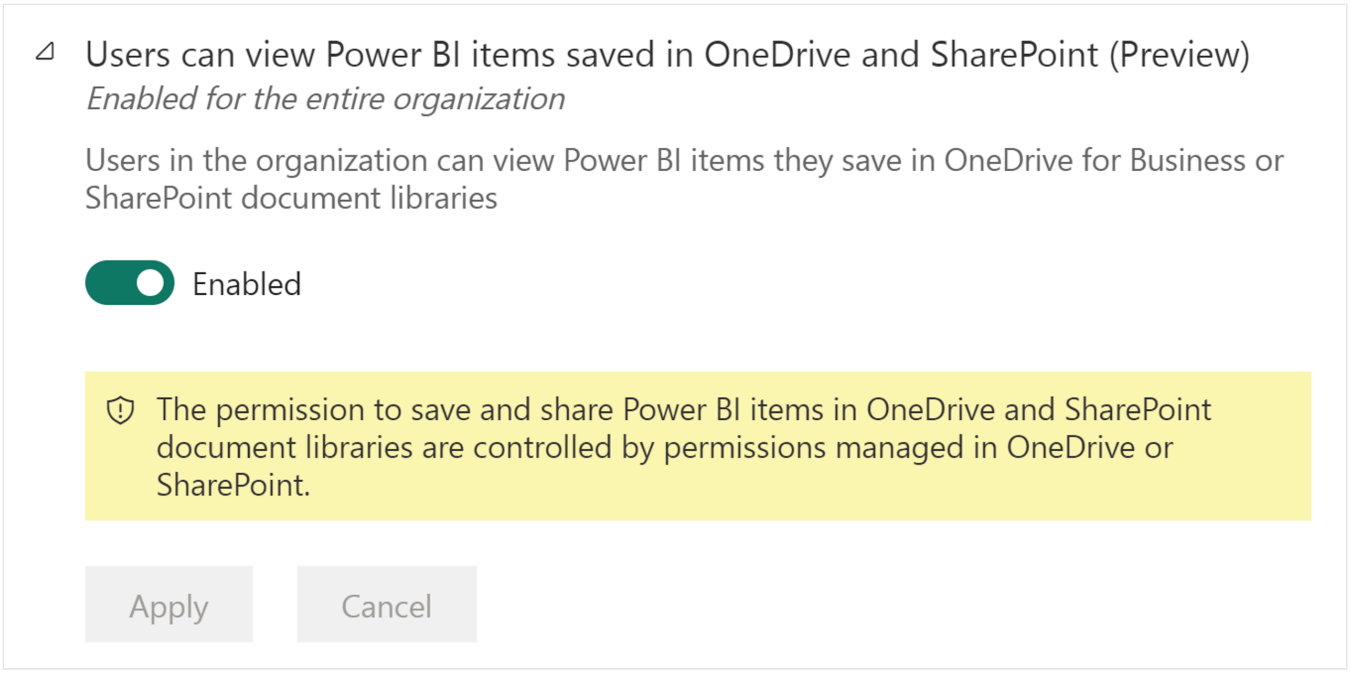
This setting enables the Power BI/Power Platform Solutions integration from the Power BI side. Admin settings also have to be turned on in Power Platform.

When the integration is enabled, when Power BI components are created in a Power Apps solution, a special Power BI workspace dedicated to the Power Apps environment is created in Power BI to store copies of the Power BI report and semantic model that are being to create the component.

To learn more, see Power BI content management in Power Apps solutions and About Power BI in Power Apps Solutions.

Users can view Power BI files saved in OneDrive and SharePoint (Preview)

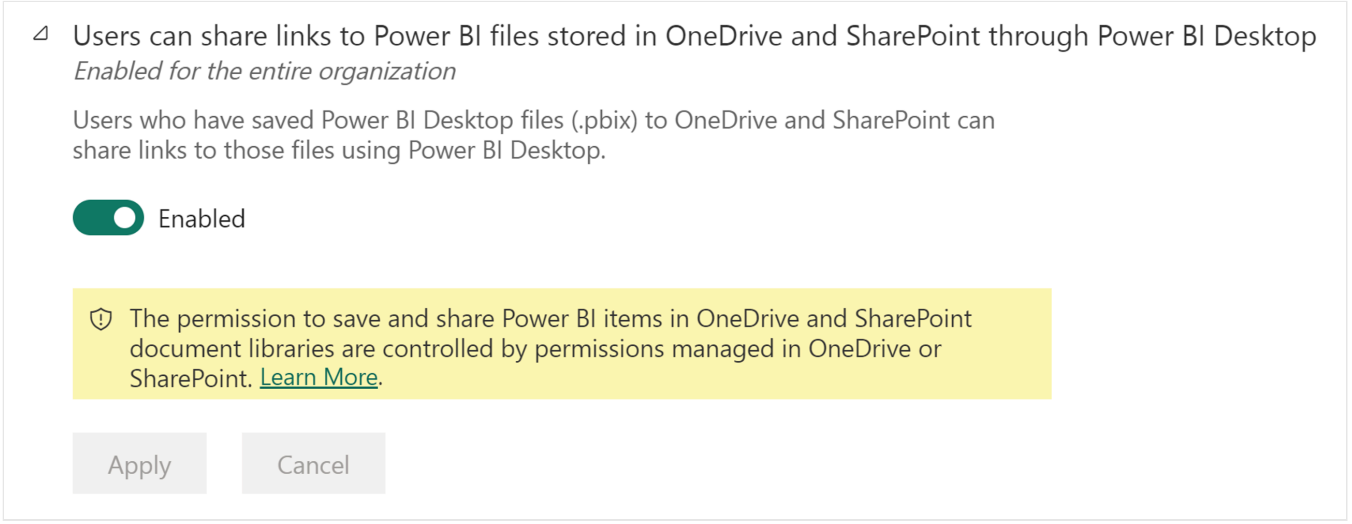
This setting allows users to view Power BI files saved in OneDrive for Business and SharePoint Online document libraries in their browser without needing to download the file and open in Power BI Desktop on their local machine. When enabled, the setting applies to all users in your organization. This setting is on by default.



Learn more about viewing Power BI files saved in OneDrive and SharePoint.

Users can share links to Power BI files stored in OneDrive and SharePoint through Power BI Desktop

Users can share links to Power BI Desktop files (.pbix) saved to OneDrive and SharePoint through Power BI Desktop. Sharing uses standard OneDrive and SharePoint sharing functionality. When enabled, this setting applies to all users in your organization.



During public preview, if a user enables share through the Power BI Desktop menu, but the admin setting is disabled for the tenant, a **Share** button still appears in Power BI Desktop, but the user is notified that the capability is disabled when they attempt to share.

Learn more about sharing links through Power BI Desktop.

Related content

- About tenant settings

Power BI visuals tenant settings

Article • 12/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

All the Power BI visuals admin settings, including Power BI visuals tenant settings, are described in Manage Power BI visuals admin settings.

- Allow visuals created using the Power BI SDK
- Add and use certified visuals only (block uncertified)
- Allow downloads from custom visuals
- Allow custom visuals to get user Microsoft Entra ID access tokens

Allow visuals created using the Power BI SDK

Users in the organization can add, view, share, and interact with visuals imported from AppSource or from a file. Visuals allowed in the *Organizational visuals* page aren't affected by this setting.

To learn more, see Visuals from AppSource or a file.

Add and use certified visuals only (block uncertified)

Users in the organization with permissions to add and use visuals can add and use certified visuals only. Visuals allowed in the *Organizational visuals* page aren't affected by this setting, regardless of certification.

To learn more, see Certified Power BI visuals.

Allow downloads from custom visuals

Enabling this setting lets custom visuals download any information available to the visual (such as summarized data and visual configuration) upon user consent. It's not affected by download restrictions applied in your organization's Export and sharing settings.

To learn more, see Export data to file.

Allow custom visuals to get user Microsoft Entra ID access tokens

Enabling this setting lets custom visuals obtain Microsoft Entra ID (formerly known as Azure AD) access tokens for signed-in users, facilitating single sign-on authentication.

To learn more, see Obtain Microsoft Entra access token.

Related content

- About tenant settings

Feedback

R and Python visuals tenant settings

Article • 11/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Interact with and share R and Python visuals

Users in the organization can interact with and share visuals created with R or Python scripts.

- Create and use R visuals in Power BI.
- Create Power BI visuals with Python.

> **Note**
>
> This setting applies to the entire organization and can't be limited to specific groups.

Related content

- About tenant settings

Feedback

Audit and usage tenant settings

Article • 05/01/2025

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Usage metrics for content creators

When this setting is enabled, users in the organization can see usage metrics for dashboards, reports and semantic models that they have appropriate permissions to.

To learn more, see Monitor usage metrics in the workspaces.

Per-user data in usage metrics for content creators

When this setting is enabled, content creator account information (such as user name and email address) will be exposed in the metrics report. If you don't wish to gather this information for all users, you can disable the feature for specified security groups or for an entire organization. Account information for the excluded users then shows in the report as *Unnamed*.

Per-user data is enabled for usage metrics by default.

Show user data in the Fabric Capacity Metrics app and reports

When this setting is enabled, active user data, including names and email addresses, is displayed in the Microsoft Fabric Capacity Metrics app and reports. This setting is enabled by default.

Azure Log Analytics connections for workspace administrators

Power BI integration with Azure Log Analytics enables Fabric administrators and Premium workspace owners to connect their Premium workspaces to Azure Log Analytics to monitor the connected workspaces.

When the setting is enabled, administrators and Premium workspace owners can configure **Azure Log Analytics for Power BI**.

Workspace admins can turn on monitoring for their workspaces

When this setting is enabled, workspace admins can turn on monitoring for their workspaces. When a workspace admin turns on monitoring, a read-only Eventhouse that includes a KQL database is created. After the Eventhouse and KQL database are added to the workspace, logging is turned on and data is sent to the database. Enable workspace monitoring, a feature that allows workspace admins to monitor their workspace.

Microsoft can store query text to aid in support investigation

When this setting is enabled, Microsoft can store the query text generated when users use Fabric items such as reports and dashboards. This data is sometimes necessary for debugging and resolving complex issues related to the performance and functionality of Fabric Items such as semantic models. The setting is enabled by default.

Storing and retaining query text data can have implications for data security and privacy. While it is recommended to leave the setting on to facilitate support, if there are organizational requirements that don't permit storing query text, or if you wish to opt out of this feature for any other reason, you can turn off the feature as follows:

1. Go to the tenant settings tab in the admin portal.
2. Find the setting **Microsoft can store query text to aid in support investigation**. It is in the Audit and usage section. You can use the search box on the tenant settings tab to help find it.
3. Set the toggle to **Disabled**.

For more information about the diagnostic query text storage feature, see Diagnostic query text storage.

Related content

- About tenant settings

Dashboard tenant settings

Article • 01/08/2024

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Web content on dashboard tiles

If this setting is enabled, users in the organization can add and view web content tiles on Power BI dashboards.

To learn more, see Add images, videos, and more to your dashboard.

> **Note**
>
> Enabling this feature could expose your organization to security risks via malicious web content. Due to these security risks, the setting is disabled by default.

Related content

- About tenant settings

Feedback

Was this page helpful? Yes No

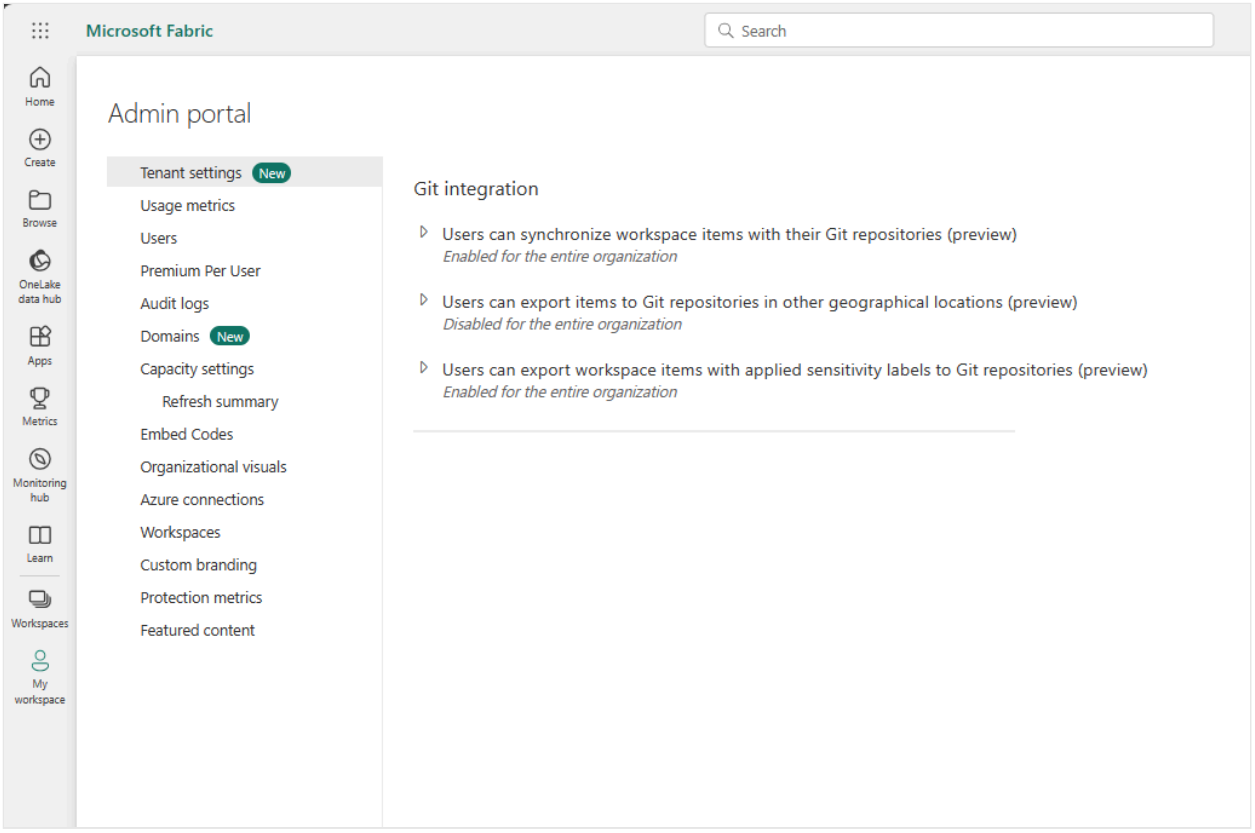
Provide product feedback | Ask the community

Git integration tenant settings

Article • 07/11/2024

The Git integration tenant admin settings are configured in the tenant settings section of the admin portal.
The tenant admin can choose to delegate control of these switches to the workspace admin or capacity admin. If the tenant admin enables delegation, the capacity admin can override the tenant admin's decision to enable or disable the switch. The workspace admin can override the tenant and the capacity settings.

For information about how to get to and use tenant settings, see About tenant settings.

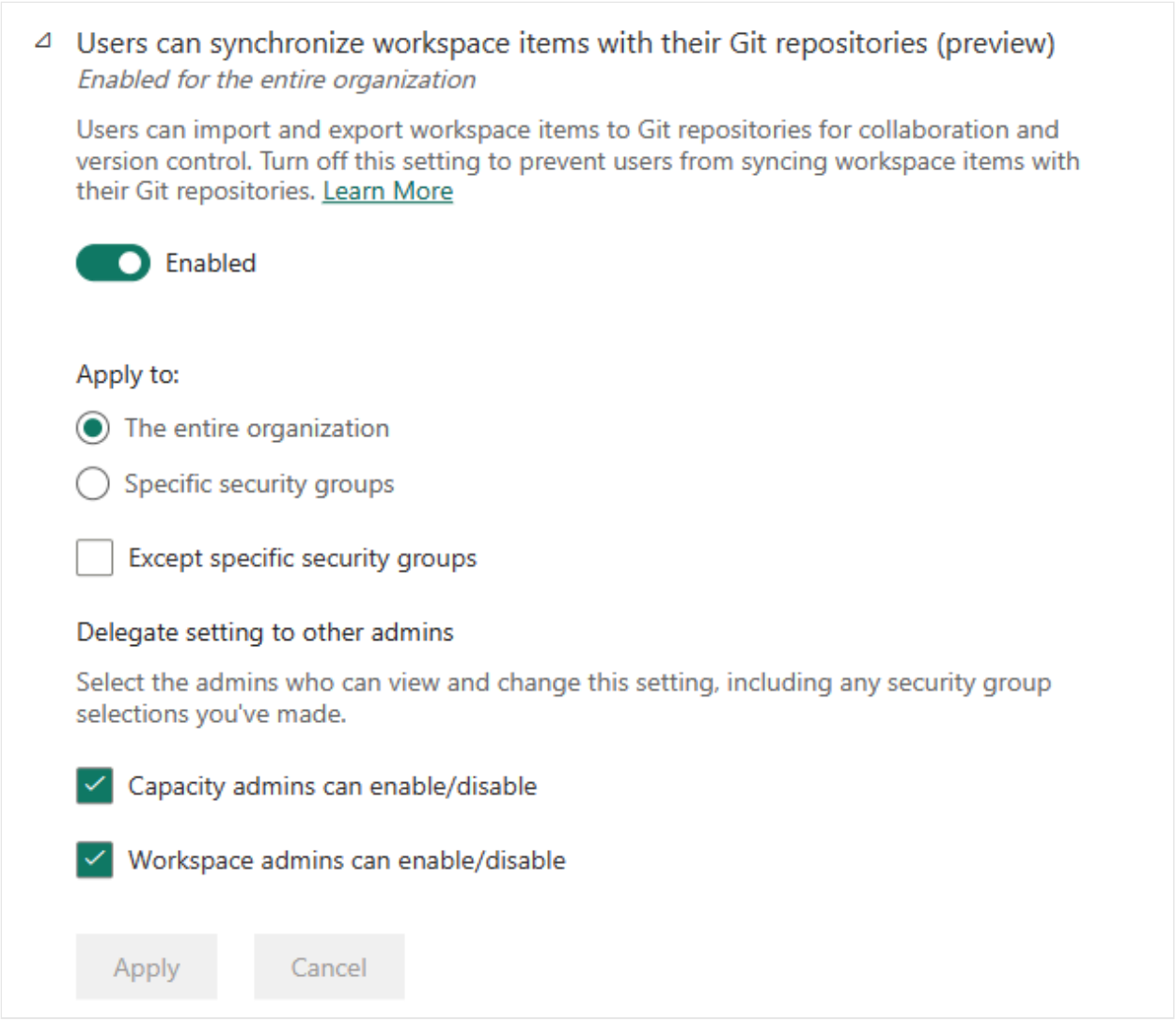


Important

The switches that control Git integration are part of Microsoft Fabric and only work if the Fabric admin switch is turned on. If Fabric is disabled, Git integration doesn't work regardless of the status of these switches.

Users can synchronize workspace items with their Git repositories (Preview)

Users can synchronize a workspace with an Azure Git repository, edit their workspace, and update their Git repos using the Git integration tool. You can enable Git integration for the entire organization, or for a specific group.
This switch is **enabled** by default. Disable it to prevent users from syncing workspace items with their Git repositories.



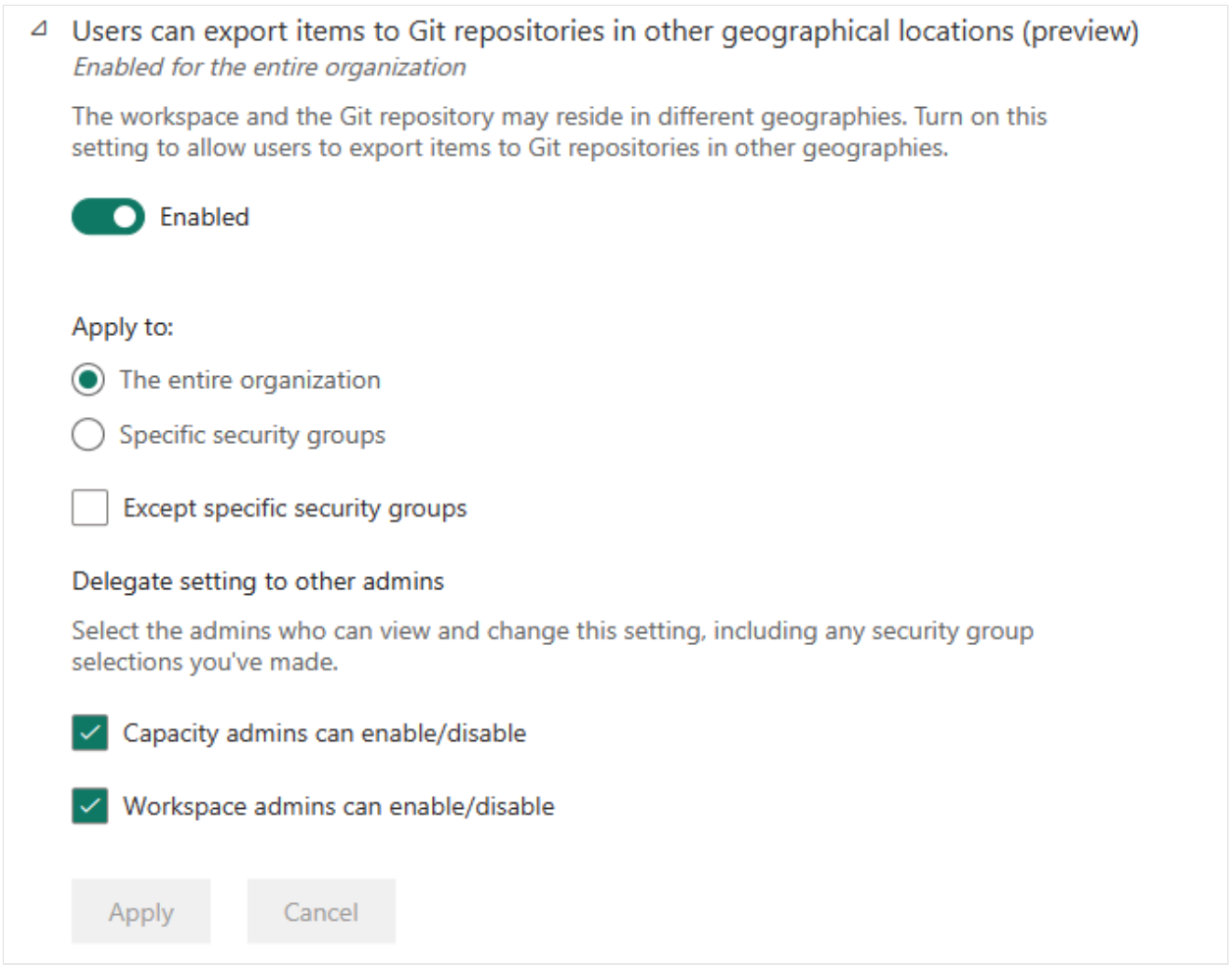
To learn more, see Introduction to Git integration.

To get started with Git integration, see Manage a workspace with Git.

Users can export items to Git repositories in other geographical locations (Preview)

If a workspace capacity is in one geographic location (for example, Central US) while the *Azure DevOps* repo is in another location (for example, West Europe), the Fabric admin can decide whether to allow users to commit metadata (or perform other Git actions) to another geographical location. Only the metadata of the item is exported. Item data and user related information are not exported.

Enable this setting to allow all users, or a specific group or users, to export metadata to other geographical locations.

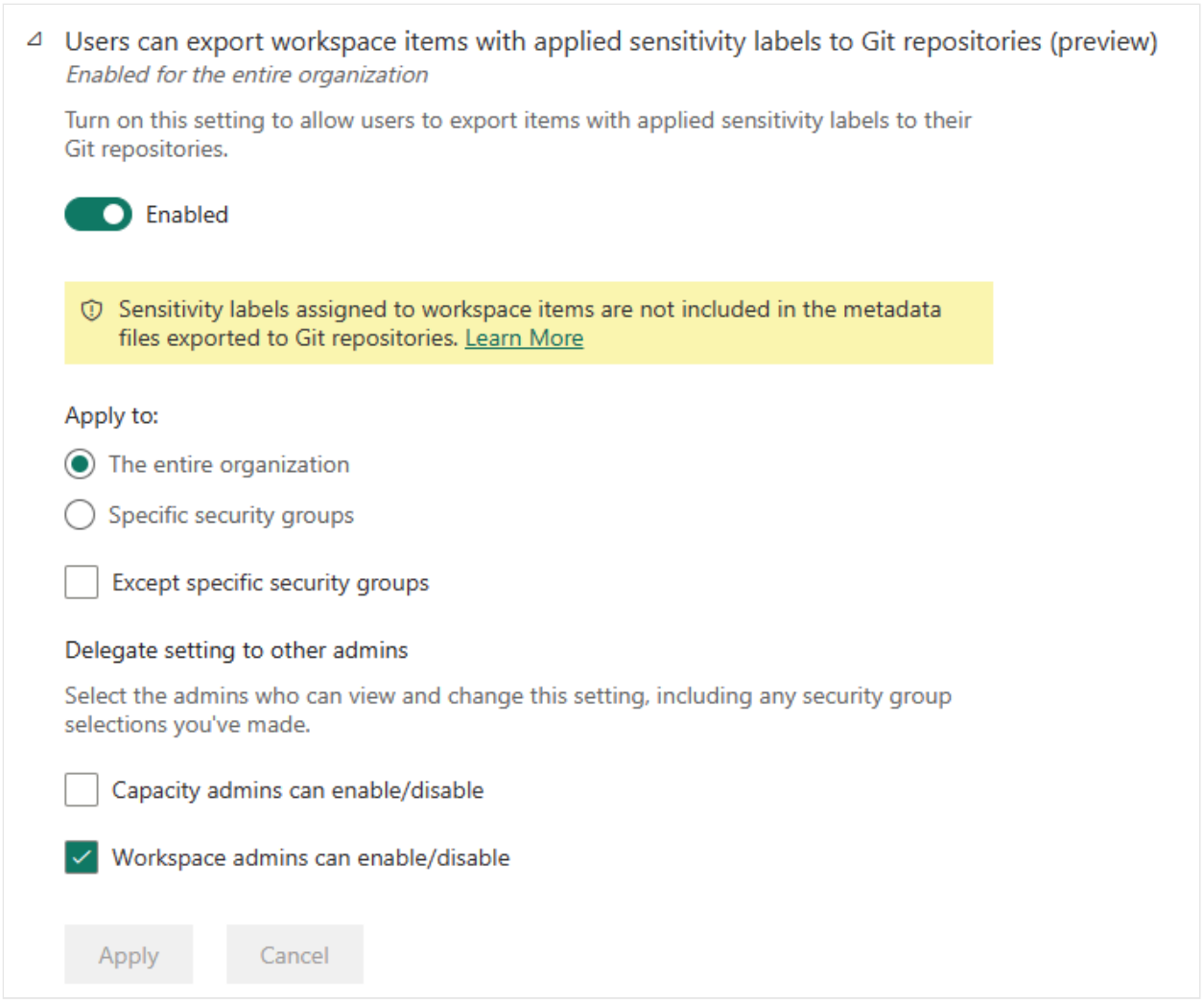


> **Note**
>
> GitHub doesn't support enforcement of this switch.

Users can export workspace items with applied sensitivity labels to Git repositories (Preview)

Sensitivity labels aren't included when exporting an item. Therefore, the Fabric admin can choose whether to block the export of items that have sensitivity labels, or to allow it even though the sensitivity label won't be included.

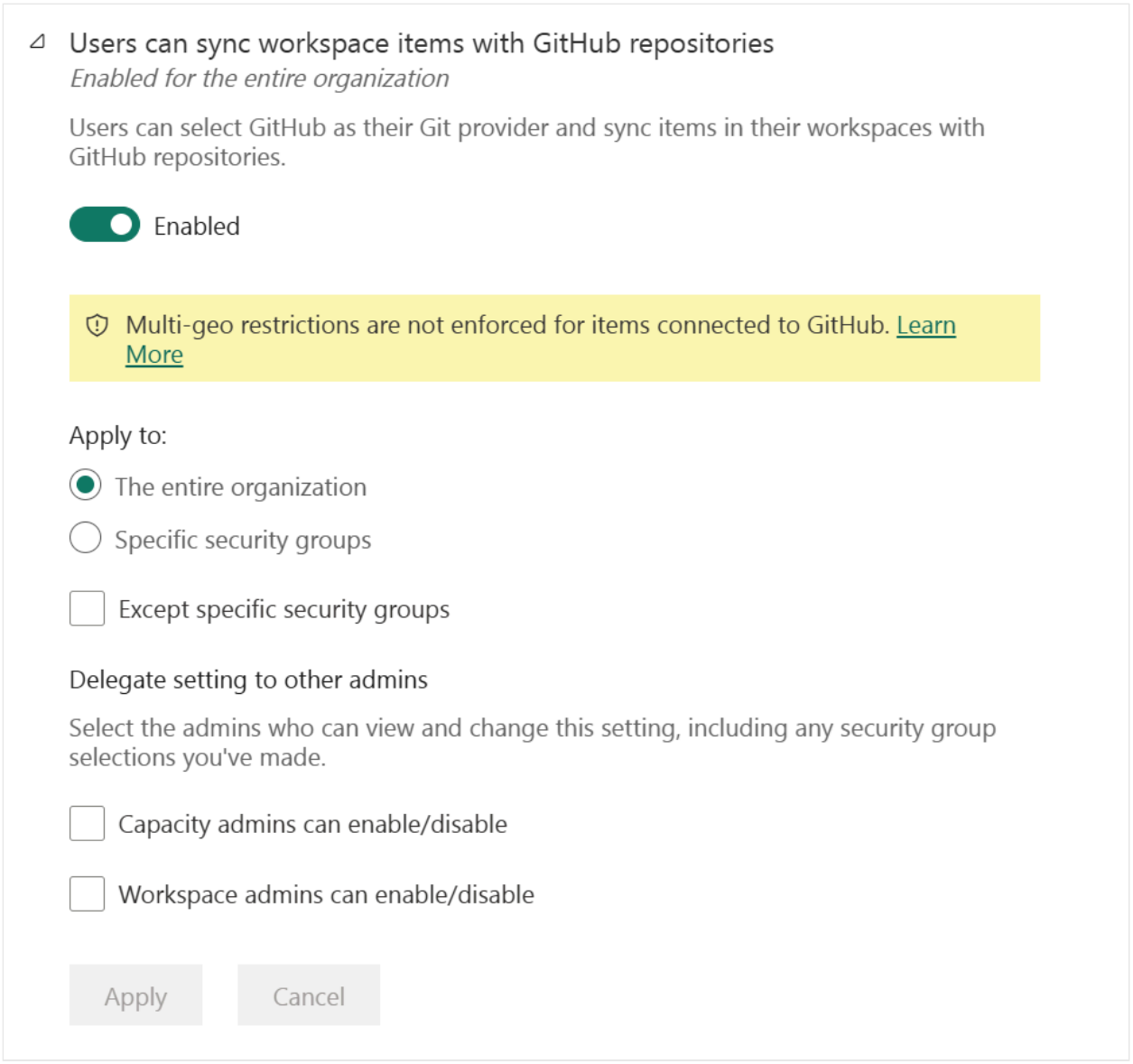
Enable this setting to allow all users, or a specific group of users, to export items without their sensitivity labels.



Learn more about sensitivity labels.

Users can sync workspace items with GitHub repositories (Preview)

Users can synchronize a workspace with their GitHub repository, edit their workspace, and update their GitHub repos using the Git integration tool. You can enable Git integration for the entire organization, or for a specific group.
This switch is **disabled** by default. Enable it to allow users to sync workspace items with their Git repositories.



To learn more, see Introduction to Git integration.

To get started with Git integration, see Manage a workspace with Git.

Related content

- About tenant settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Developer tenant settings

Article • 05/19/2025

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

To manage Power BI developer settings, you must be a Fabric administrator. For more information about the Fabric administrator role, see Understand Microsoft Fabric admin roles.

> **Note**
>
> The developer settings in the Admin portal are different from and not related to the developer mode setting for debugging visuals.

Embed content in apps

Users in the organization can embed Power BI dashboards and reports in software as a service (SaaS) applications. Disabling this setting prevents users from being able to use the REST APIs to embed Power BI content within their application.

To learn more, see What is Power BI embedded analytics?.

Learn about the Embed for your customers method to build an app that uses non-interactive authentication against Power BI.

Service principals can use Fabric APIs

> **Note**
>
> This setting is being rolled out and might not be available in your tenant. Once removed, these settings will replace it:
>
> - Service principals can create workspaces, connections, and deployment pipelines
> - Service principals can call Fabric public APIs

Web apps registered in Microsoft Entra ID use an assigned service principal to access Power BI APIs without a signed-in user. To allow an app to use service principal authentication, its service principal must be included in an allowed security group.

Service principals can create workspaces, connections, and deployment pipelines

Use a service principal to access these Fabric APIs that aren't protected by a Fabric permission model.

- Create Workspace
- Create Connection
- Create Deployment Pipeline

To allow an app to use service principal authentication, its service principal must be included in an allowed security group. You can control who can access service principals by creating dedicated security groups and using these groups in other tenant settings.

This setting is disabled by default for new customers.

Service principals can call Fabric public APIs

Use a service principal to access Fabric public APIs that include create, read, update, and delete (CRUD) operations, and are protected by a Fabric permission model.

To allow an app to use service principal authentication, its service principal must be included in an allowed security group. You can control who can access service principals by creating dedicated security groups and using these groups in other tenant settings.

This setting is enabled by default for new customers.

Allow service principals to create and use profiles

An app owner with many customers can use service principal profiles as part of a multitenancy solution to enable better customer data isolation and establish tighter security boundaries between customers.

To learn more, see Service principal profiles for multitenancy apps.

Block ResourceKey Authentication

For extra security, you can block the use of resource key-based authentication. The Block ResourceKey Authentication setting applies to streaming and PUSH datasets. If disabled, users

will not be allowed send data to streaming and PUSH datasets using the API with a resource key.

This setting applies to the entire organization. You can't apply it only to a select security group.

Related content

- About tenant settings

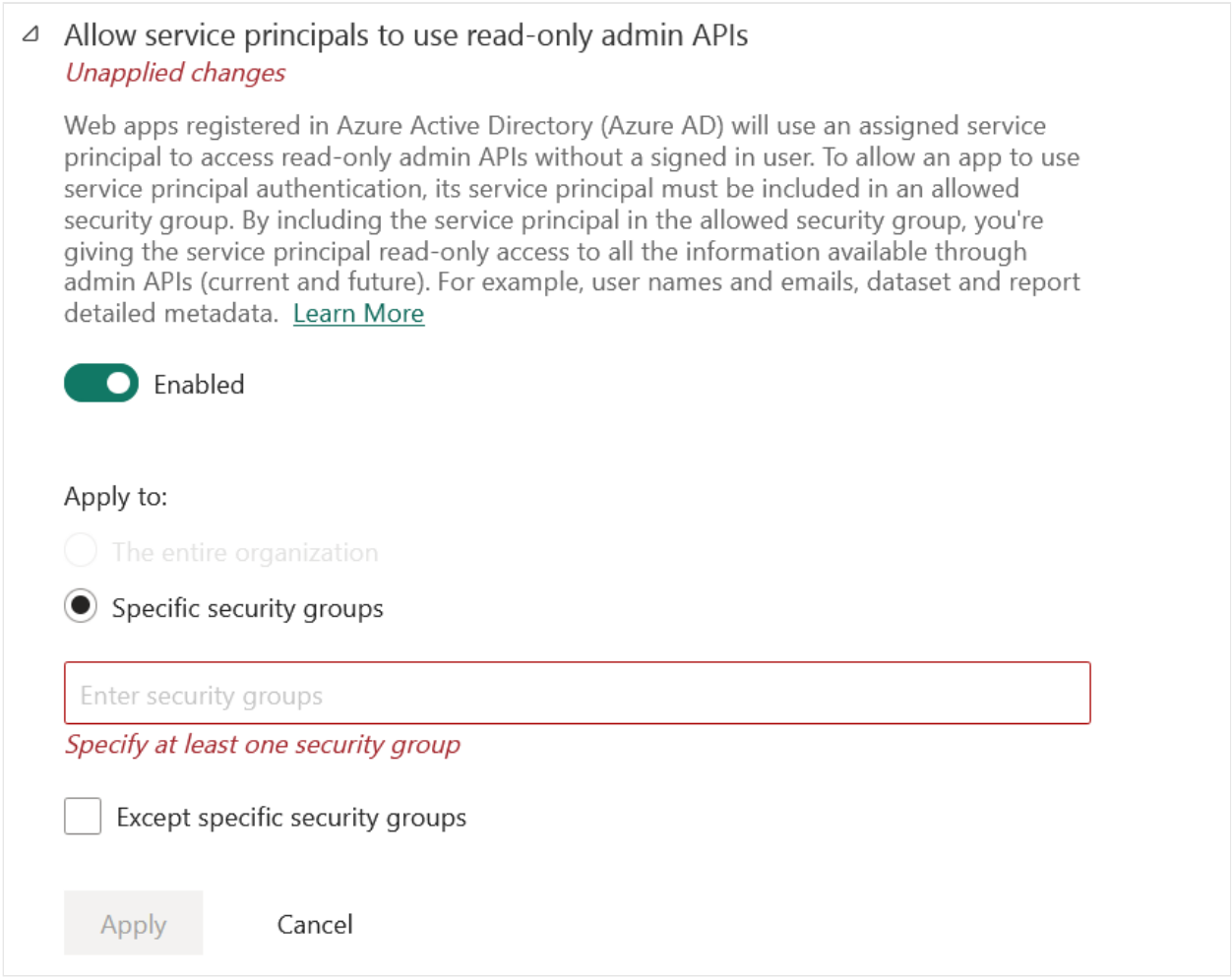
Admin API tenant settings

Article • 12/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Allow service principals to use read-only admin APIs

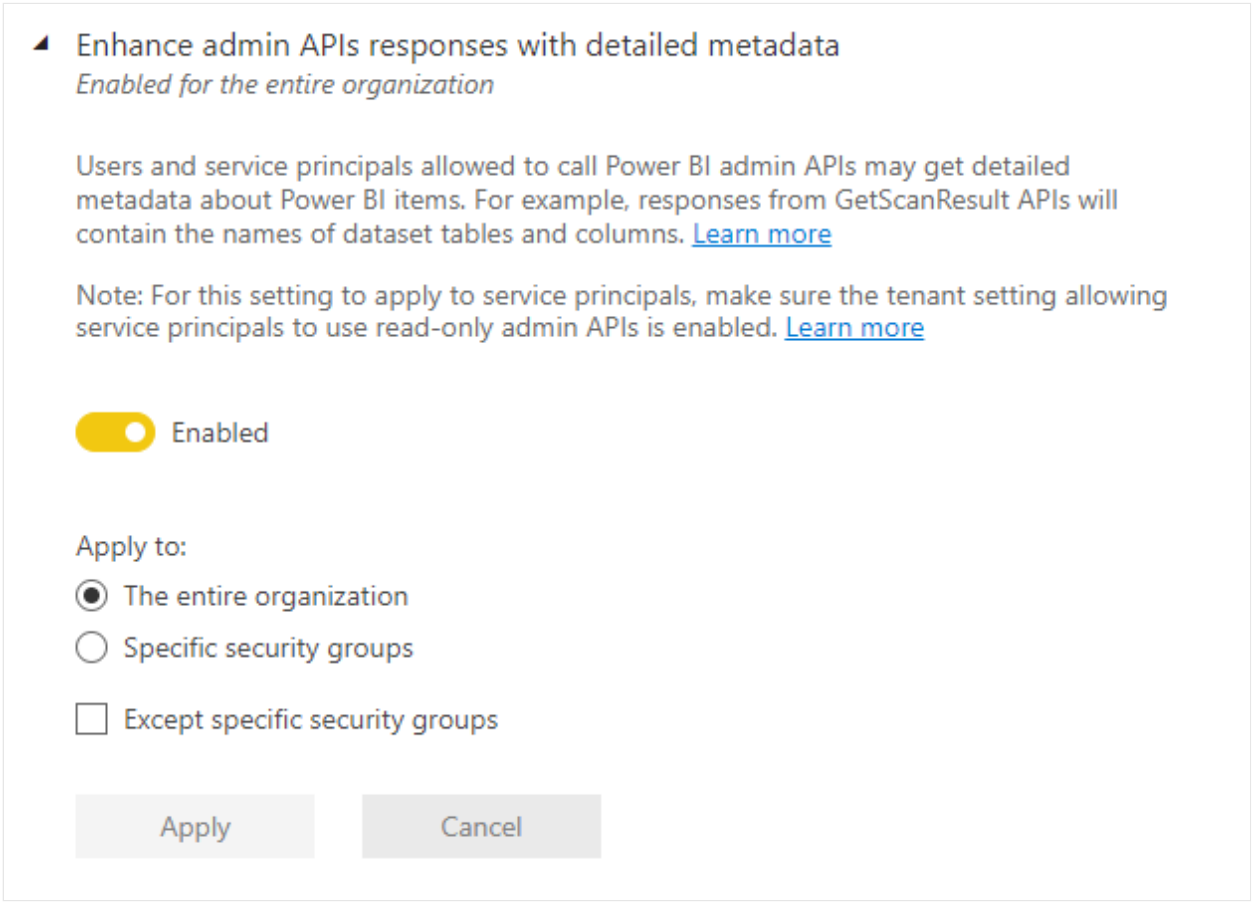
Web apps registered in Microsoft Entra ID use an assigned service principal to access read-only admin APIs without a signed-in user. To allow an app to use service principal authentication, its service principal must be included in an allowed security group. By including the service principal in the allowed security group, you're giving the service principal read-only access to all the information available through admin APIs (current and future). For example, user names and emails, semantic model, and report detailed metadata.



To learn more, see Allow service principals to use read-only admin APIs

Enhance admin APIs responses with detailed metadata

Users and service principals allowed to call Power BI admin APIs might get detailed metadata about Power BI items. For example, responses from GetScanResult APIs contain the names of semantic model tables and columns.



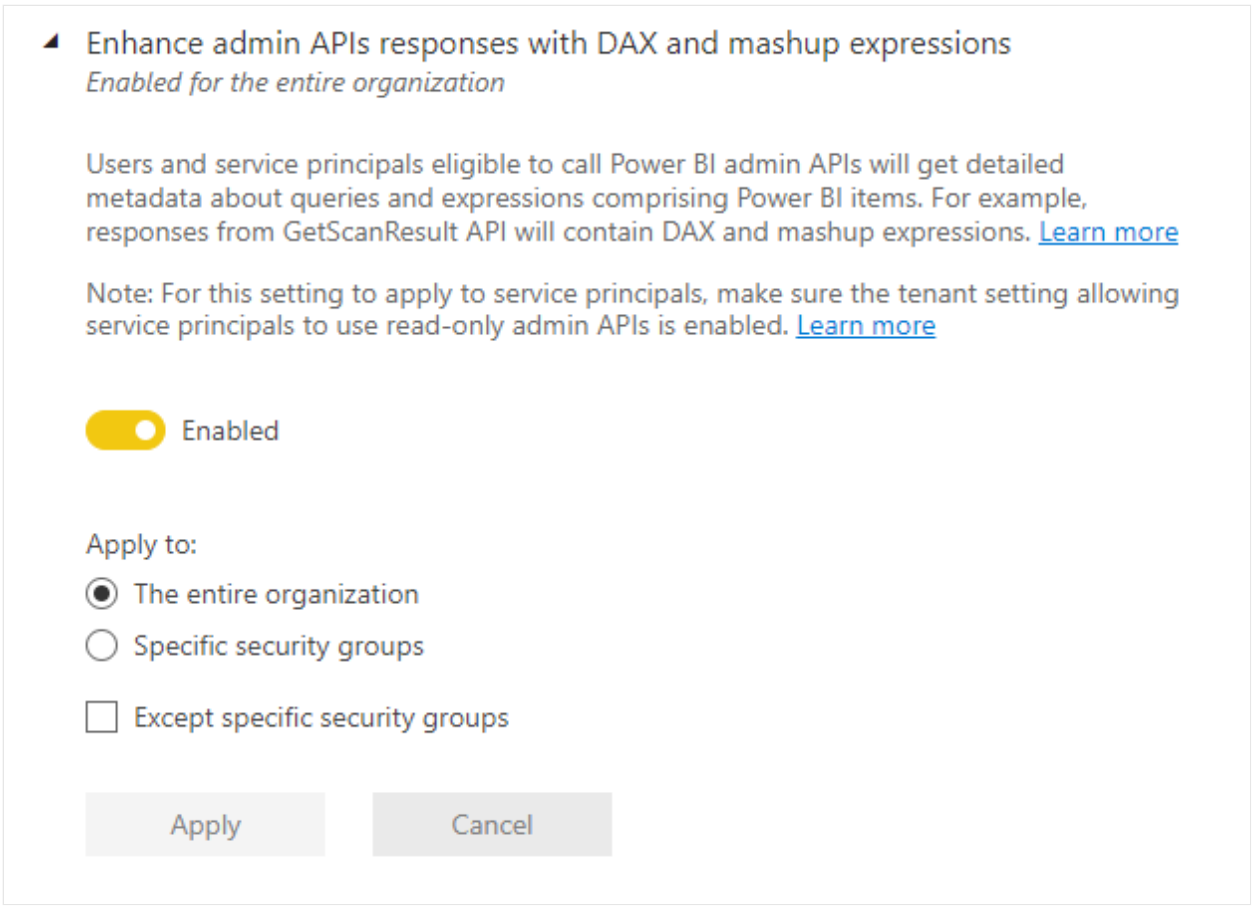
To learn more, see Metadata scanning.

> **Note**
>
> For this setting to apply to service principals, make sure the tenant setting **Allow service principals to use read-only admin APIs** is enabled. To learn more, see **Set up metadata scanning**.

Enhance admin APIs responses with DAX and mashup expressions

Users and service principals eligible to call Power BI admin APIs get detailed metadata about queries and expressions comprising Power BI items. For example, responses from

GetScanResult API contain DAX and mashup expressions.



To learn more, see Metadata scanning.

> **Note**
>
> For this setting to apply to service principals, make sure the tenant setting **Allow service principals to use read-only admin APIs** is enabled. To learn more, see **Set up metadata scanning**.

Related content

- About tenant settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Gen 1 dataflow tenant settings

Article • 11/02/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Create and use Gen1 dataflows

Users in the organization can create and use dataflows. For an overview of dataflows, see Introduction to dataflows and self-service data prep. To enable dataflows in a Premium capacity, see Configure workloads.

> **Note**
>
> This setting applies to the entire organization and can't be limited to specific groups.

Next steps

- About tenant settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Template app tenant settings

Article • 11/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Publish template apps

Users in the organization can create template apps workspaces. Control which users can publish template apps or distribute them to clients outside your organization by way of Microsoft AppSource or other distribution methods.

To learn more about template apps, see What are Power BI template apps?.

Install template apps

Users in the organization can download and install template apps **only** from Microsoft AppSource. Control which specific users or security groups can install template apps from AppSource.

To learn about AppSource, see What is Microsoft AppSource?.

Install template apps not listed in AppSource

Control which users in the organization can download and install template apps **not** listed on Microsoft AppSource.

Related content

- About tenant settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Q&A tenant settings

Article • 11/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Review questions

When this setting is enabled, semantic model owners can review questions end-users ask about their data.

To learn more, see Intro to Q&A tooling to train Power BI Q&A.

Synonym sharing

When this setting is enabled, users can share Q&A synonyms as suggested terms with everyone in your organization.

To learn about synonyms, see Field synonyms.

> **Note**
>
> If you disable this setting and apply the changes, and then later re-enable synonym sharing, it might take a few weeks to reshare all the synonyms within your organization.

Related content

- About tenant settings

Feedback

Semantic model security tenant setting

Article • 04/21/2025

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Block republish and disable package refresh

Disable package refresh, and only allow the semantic model owner to publish updates. When using the XMLA Endpoint, a user can discover only those semantic models for which they are the owner.

To learn more about semantic model security, see Semantic model permissions.

Related content

- About tenant settings

Advanced networking tenant settings

Article • 11/02/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Azure Private Link

Increase security by allowing people to use a Private Link to access your Power BI tenant. Someone will need to finish the set-up process in Azure. If that's not you, grant permission to the right person or group by entering their email.

To learn how to set up Private Link, see Private endpoints for secure access to Power BI.

Block Public Internet Access

For extra security, block access to your Power BI tenant via the public internet. This means people who don't have access to the Private Link won't be able to get in. Keep in mind, turning this on could take 10 to 20 minutes to take effect.

To learn more, see Private endpoints for secure access to Power BI.

Next steps

- About tenant settings

Feedback

Encryption tenant setting

10/15/2025

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Apply customer-managed keys

Customer-managed keys (CMK) are encryption keys that you create, own, and manage in your Azure Key Vault (AKV). By using a CMK, you can supplement default encryption with an extra encryption layer. You can use customer-managed keys for greater flexibility to manage access controls or to meet specific regulatory compliance.

Enable CMK for Fabric workspaces tenant setting

By default, the CMK feature is disabled at the tenant level. This means that workspace administrators cannot enable CMK until the tenant administrator enables the setting. CMK can be enabled and disabled for the workspace while the tenant setting is on. Once the tenant setting is turned off, you can no longer enable CMK for workspaces in that tenant or disable CMK for workspaces that already have CMK turned on in that tenant.

To learn how to set up CMK encryption, see customer-managed keys for Fabric workspaces.

Related content

- About tenant settings

Metrics Hub tenant settings

Article • 11/25/2024

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Create and use Metrics

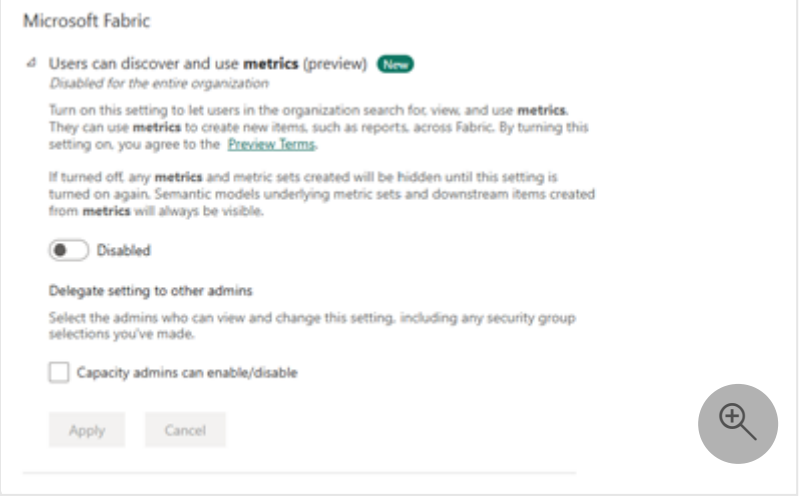
Users in the organization can create and use metrics in Power BI.

To learn more, see Get started with metrics in Power BI.

Metric sets setting (preview)

To turn on the Metrics hub for your organization, the Power BI or Fabric tenant admin should turn on the tenant admin setting for Metrics in your organization. After you turn on the setting, the new Metric set area within the metrics hub visible. The Metric set setting is disabled by default. Turning on this setting shows the new metric hub UI (metric sets) in the classic metric hub experience, allowing users to create, browse, and consume metrics and metric sets.

To turn on the Metrics set setting:



1. Make sure you are in Fabric tenant settings and use the Search feature to find the metric set settings.
2. Toggle the **Users can discover and use metrics** switch to on.
3. Specify who can access metric sets in Power BI.
4. Select Apply to save your changes.

Related content

- About tenant settings

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

User experience experiments tenant settings

Article • 11/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Help Power BI optimize your experience

Enabling this feature allows the Power BI team to gather early feedback and to make data-driven decisions as to which in-product experience is received more positively by users.

When this feature is enabled, individual users in the same organization might get minor variations in the user experience, including content, layout, and design, before these variations go live for all users. This means that different users in the same tenant might have slightly different experiences.

Related content

- About tenant settings

Feedback

Share data with your Microsoft 365 services

This article is aimed at Fabric administrators and decision makers who need to know how and where Fabric metadata is being used.

Fabric metadata sharing with Microsoft 365 services is a feature that allows metadata from Fabric to be shared with Microsoft 365 services (typically via Microsoft Graph) and combined with data from across Microsoft 365, Windows, and Enterprise Mobility + Security (EMS) to build apps for organizations and consumers that interact with millions of users. The feature is enabled by default when your Fabric home tenant and Microsoft 365 tenant are in the same geographical region.

When shared with Microsoft 365 services, Fabric content will be listed in the Quick Access list on the Office.com home page. The Fabric content affected includes reports, dashboards, apps, workbooks, paginated reports, and workspaces. The information required by the Quick Access functionality includes:

- The display name of the content
- When the content was last accessed
- The type of content that was accessed (report, app, dashboard, scorecard, etc.)

See more about the Fabric data that is shared with Microsoft 365 services.

Data residency

Fabric and Microsoft 365 are distinct and separately operated Microsoft cloud services, each deployed according to its own service-specific data center alignment rules, even when purchased together. As a result, it's possible that your Microsoft 365 Services and your Fabric service are not deployed in the same geographic region.

By default, Fabric metadata is available only in the region where the Fabric tenant is located. However, you can allow Fabric to share metadata across regions by turning on a toggle switch in the **Users can see Microsoft Fabric metadata in Microsoft 365** tenant setting. For more information, see How to turn sharing with Microsoft 365 services on and off.

Where is Fabric data stored?

For more information about data storage locations, see Find the default region for your organization and Product Availability by Geography.

Where is Microsoft 365 data stored?

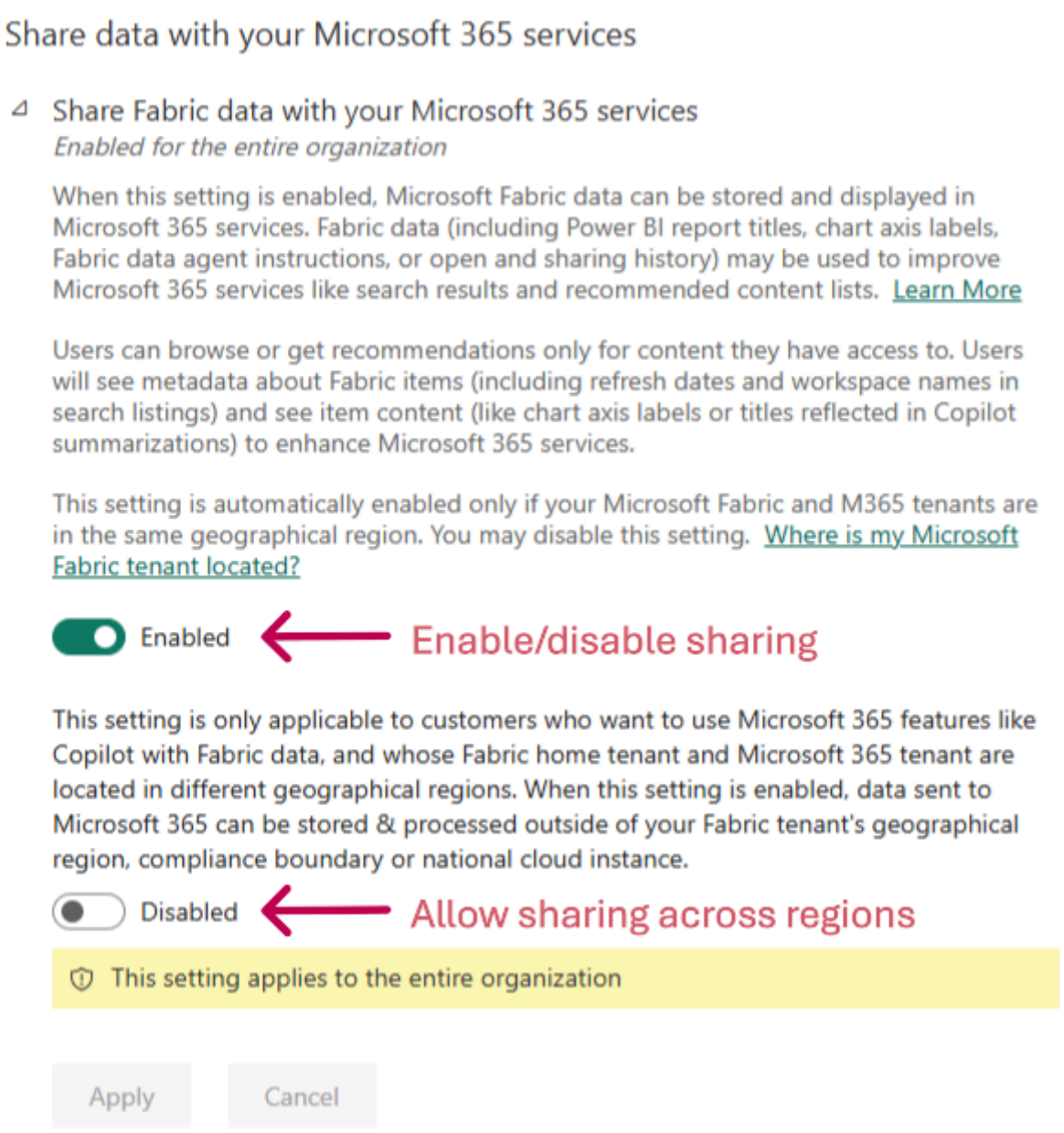
For more information about data storage for Microsoft 365, see Where your Microsoft 365 customer data is stored and Multi-Geo Capabilities in Microsoft 365.

How to turn sharing with Microsoft 365 services on and off

Sharing metadata with Microsoft 365 services is controlled by the **Share Fabric data with your Microsoft 365 services** tenant setting. The setting is **Enabled** by default. To turn off the feature, or to turn it on again after it's been turned off, go to **Admin portal** > **Tenant settings** > **Share Fabric data with your Microsoft 365 services** and set the toggle as appropriate. Once the setting is enabled or disabled, it may take up to 24 hours for you to see changes.

By default, Fabric data is available only in the region where the Fabric tenant is located. To allow Fabric to share metadata across regions, set the second toggle switch to **Enabled**. When you enable the second toggle, you acknowledge that Fabric data may flow outside the geographic region it's stored in.

> **Note**
>
> The second toggle is visible only when the main sharing toggle is enabled.



Data that is shared with Microsoft 365

The tables below lists examples of the data that is shared with Microsoft 365 services.

Item metadata that is mainly used when using the "search" mechanism to look for Fabric content within your Microsoft 365 services

Expand table

Property	What is Shared	Example
TenantID	Microsoft Entra tenant Identifier	aaaabbbb-0000-cccc-1111-dddd2222eeee
ItemType	Fabric category for the item	Report

Property	What is Shared	Example
DisplayName	Display name for the item	Retail Analysis Sample
Description	Content description in the servics (e.g. Report settings)	Sample containing retail sales data
URL	Content Item URL for the item	https://powerbi-df.analysis-df.windows.net/groups/8b5ac04e-89c1-4fc6-a364-e8411dfd8d17/reports/aaaabbbb-0000-cccc-1111-dddd2222eeee/ReportSection2
ACL	Access Control List with permissions and Microsoft Entra user, Security Group and Distribution List Identifiers	{"accessType": "grant", "id" : "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee", "type" : "read" }
WorkspaceName	Workspace name as per Create a workspace	Retail workspace
WorkspaceURL	Link to navigate to the Workspace in the service	https://powerbi-df.analysis-df.windows.net/groups/8b5ac04e-89c1-4fc6-a364-e8411dfd8d17
Creator	Microsoft Entra user principal name of the person that created the content	user1@fourthcoffee.com
CreatedDate	Date the content was created	2011-06-30T23:32:46Z
LastModifiedUser	Microsoft Entra user principal name for the last person who modified the content	user1@fourthcoffee.com
LastModifiedDate	Last modified date for the content	2011-06-30T23:32:46Z
PageNames	Display names for pages within the report	Sales Summary, Regional details, Returns
ChartTitles	Display names for visualizations in the report layout	Regional sales over time
FieldNames	Names of columns and measures used in the report	revenue, date, product_category

User activity that is mainly leveraged for showing Fabric content within your "Recents" and "Recommended" sections at Office.com

Expand table

Property	What is Shared	Example
LastRefreshDate	Last refresh date for the content	2011-06-30T23:32:46Z
UserID	Microsoft Entra user principal name for the user who acted on the item	user1@fourthcoffee.com
SignalType	The type of action the user took on the content	Viewed
ActorID	Microsoft Entra ID for the user who acted on the item	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
StartTime/EndTime	Date/Time the user performed the action on the content	2011-06-30T23:32:46Z

Related content

- About tenant settings

Last updated on 12/06/2025

Insights tenant settings

Article • 11/21/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Receive notifications for top insights (preview)

Users in the organization can enable notifications for top insights in report settings.

To learn more about insights, see Find Insights in your reports.

Show entry points for insights (preview)

Users in the organization can use entry points for requesting insights inside reports.

To learn more about insights, see Find Insights in your reports.

Related content

- About tenant settings

Feedback

Datamart tenant settings

Article • 11/21/2023

Datamart tenant settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Create Datamarts (Preview)

When this setting is on, specified users in the organization can create datamarts.

For more information, see Administration of datamarts.

Related content

- About tenant settings
- Administration of datamarts

Feedback

Data model tenant settings

Article • 11/21/2023

Fabric administrators can enable or disable data model editing in the service for the entire organization or for specific security groups, using the setting described in this article. This setting is configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Users can edit data models in the Power BI service (preview)

Users can edit data models in the Power BI service (preview) tenant settings. This setting doesn't apply to DirectLake datasets or editing a dataset through an API or XMLA endpoint.

To learn more, see Enabling data model editing in the admin portal.

Related content

- About tenant settings
- Edit data models in the Power BI service(preview)

Feedback

Quick measure suggestions tenant settings

Article • 11/02/2023

These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Allow quick measure suggestions (preview)

When enabled, users use natural language to generate suggested measures. Quick measure suggestions assist creation of DAX measures using natural language instead of using templates or writing DAX from scratch.

To learn more, see Quick measure suggestions.

Allow user data to leave their geography

Quick measure suggestions are currently processed in the US. When this setting is enabled, users get quick measure suggestions for data outside the US.

To learn more, see Limitations and considerations.

Next steps

- About tenant settings

Feedback

Scale-out tenant settings

Article • 11/21/2023

Scale-out tenant settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Scale out queries for large semantic models (Preview)

For semantic models that use the large semantic model storage format, Power BI Premium can automatically distribute queries across other semantic model replicas when query volume is high. Scale-out is enabled on a tenant by default.

For more information, see Power BI semantic model scale-out.

Related content

- About tenant settings

Feedback

OneLake tenant settings

Article • 11/21/2023

OneLake tenant settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Users can access data stored in OneLake with apps external to Fabric

Users can access data stored in OneLake with apps external to the Fabric environment, such as custom applications created with Azure Data Lake Storage (ADLS) APIs, OneLake File Explorer, and Databricks. Users can already access data stored in OneLake with apps internal to the Fabric environment, such as Spark, Data Engineering, and Data Warehouse.

To learn more, see Allow apps running outside of Fabric to access data via OneLake.

Users can sync data in OneLake with the OneLake File Explorer app

Turn on this setting to allow users to use OneLake File Explorer. This app will sync OneLake items to Windows File Explorer, similar to OneDrive.

To learn more, see OneLake File Explorer.

Related content

- About tenant settings

Feedback