Microsoft Fabric documentation for admins

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

Get started

GET STARTED

Enable Microsoft Fabric for your organization

Governance in Microsoft Fabric

Security in Microsoft Fabric

OVERVIEW

What is Microsoft Fabric admin?

What is the admin portal?

HOW-TO GUIDE

Understand Microsoft Fabric admin roles

Tools and settings

OVERVIEW

Tenant admin settings for git integration

HOW-TO GUIDE

Track user activities in Fabric

Set up item certification

Enable service principal authentication for read-only admin APIs

Set up metadata scanning in your organization

Workspace settings

OVERVIEW

Workspace tenant settings

HOW-TO GUIDE

Manage workspaces

Admin monitoring workspace

OVERVIEW

What is the admin monitoring workspace?

Feature usage and adoption report

What is Microsoft Fabric admin?

Article • 06/15/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

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

- **Azure Active Directory 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.

Next steps

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

Enable Microsoft Fabric for your organization

Article • 06/15/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

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

> **Note**
>
> 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 be an early adopter of Microsoft Fabric.
- **A specific capacity** - Use this option if you want users in a specific capacity to try out Microsoft Fabric.

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

> **Tip**
>
> Unless an admin makes changes to the Microsoft Fabric admin switch settings, Microsoft Fabric will be turned on for all Power BI users on 1 July 2023.

Prerequisites

To enable Microsoft Fabric, you need to have one of the following admin roles:

- Microsoft 365 Global admin
- Power Platform admin

- Fabric admin

Enable for your tenant

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

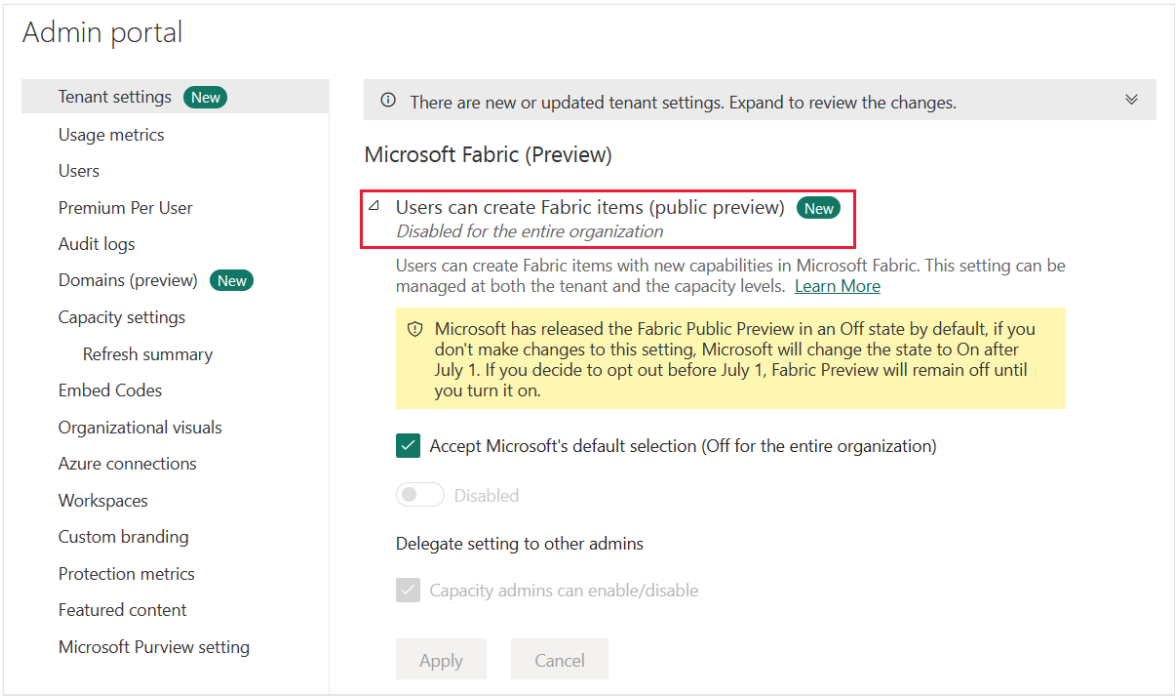
> ⓘ **Note**
>
> You, or other admins, can override the the Microsoft Fabric setting at the **capacity level**.

In your tenant, you can enable Microsoft Fabric for:

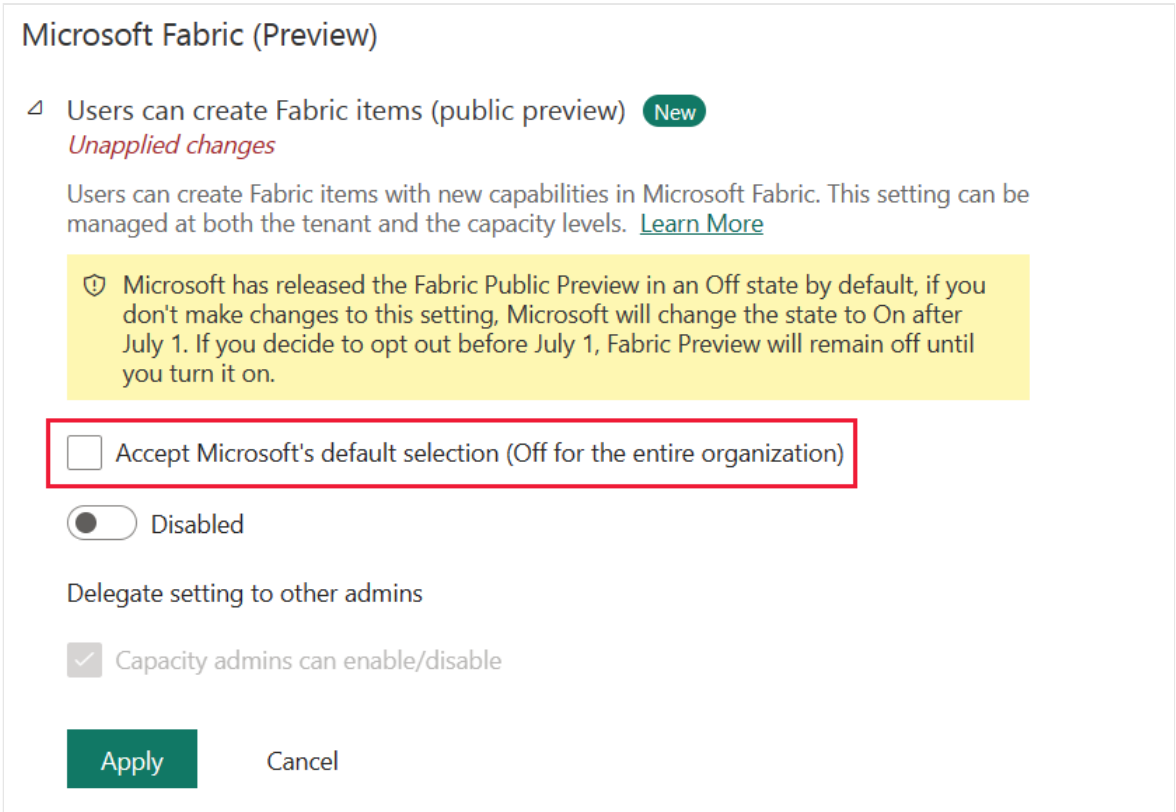
- **The entire organization** - In most cases your organization has one tenant, so selecting this option enables it for the entire organization. In organizations that have several tenants, if you want to enable Microsoft Fabric for the entire organization, you need to enable it in each tenant.
- **Specific 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.

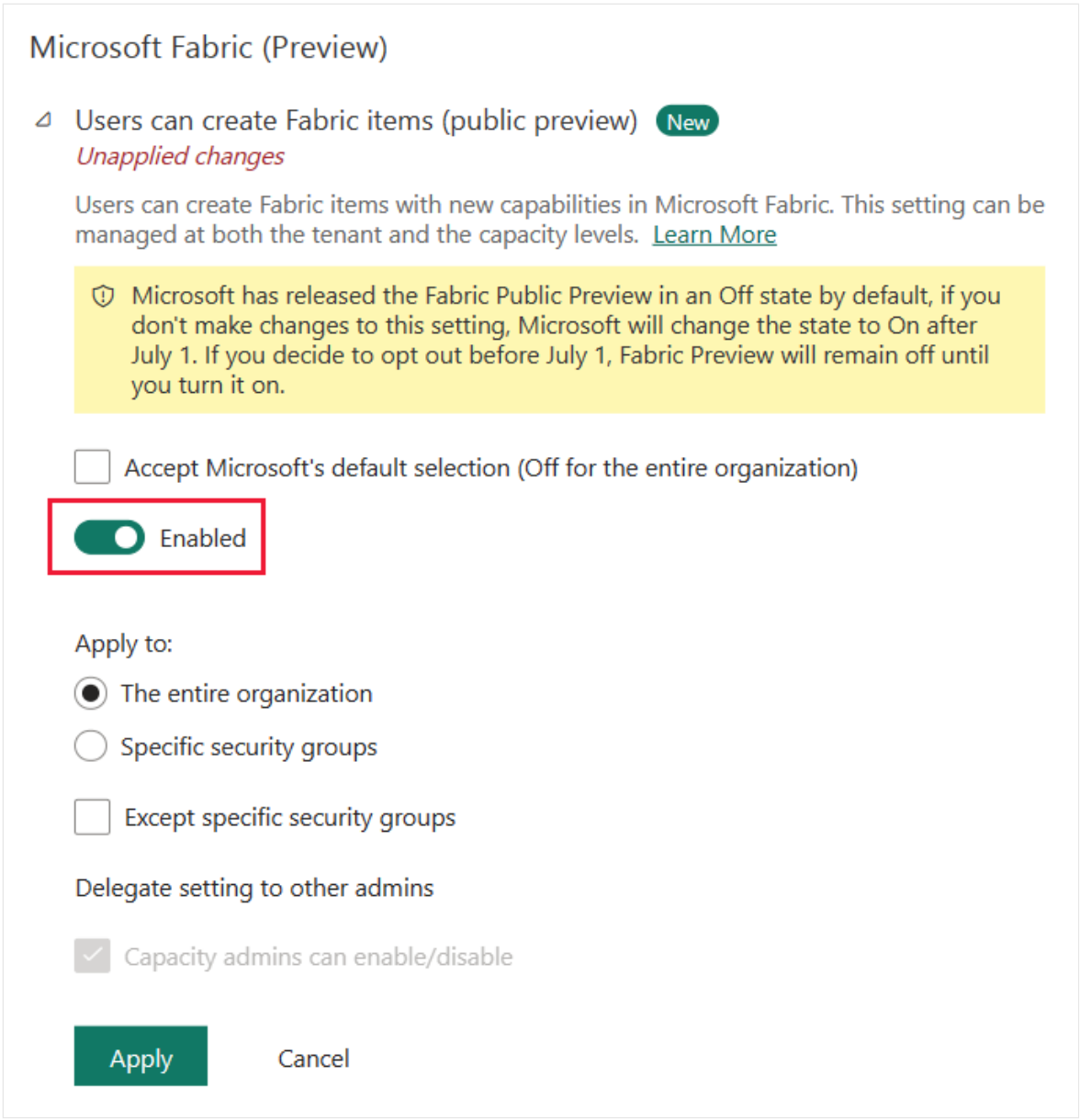
1. Navigate to the tenant settings in the admin portal and in *Microsoft Fabric (Preview)*, expand the **Users can create Fabric items (public preview)**.



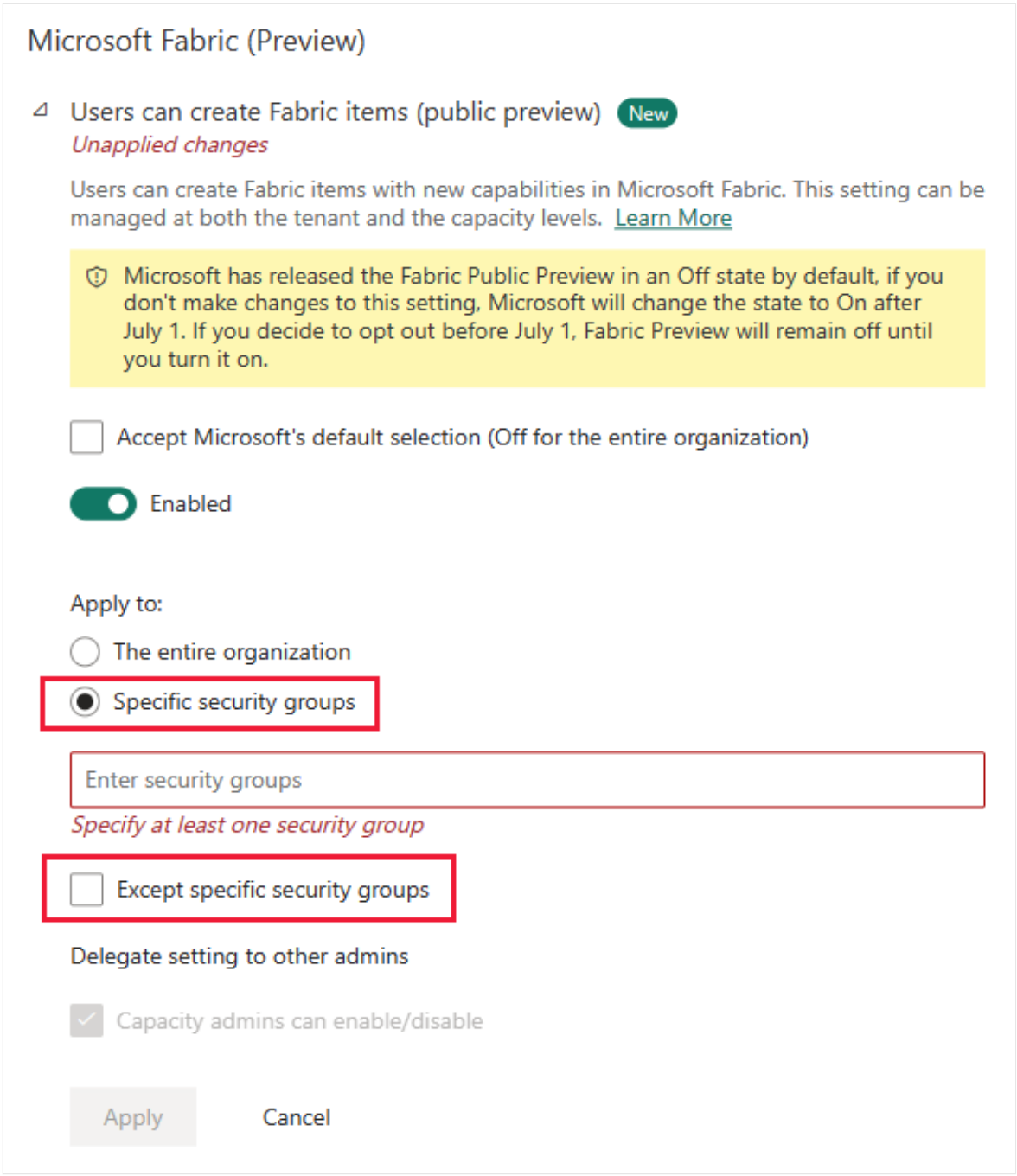
2. Uncheck the **Accept Microsoft's default selection (Off for the entire organization)** checkbox. You only need to uncheck the Microsoft's default selection when you enable the Microsoft Fabric setting for the first time.



3. Enable the **Users can create Fabric items (public preview)** switch.



4. (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 tenant, and exclude specific users.



5. Select **Apply**.

> **Note**
>
> The *Delegate settings to other admins* option, isn't available.

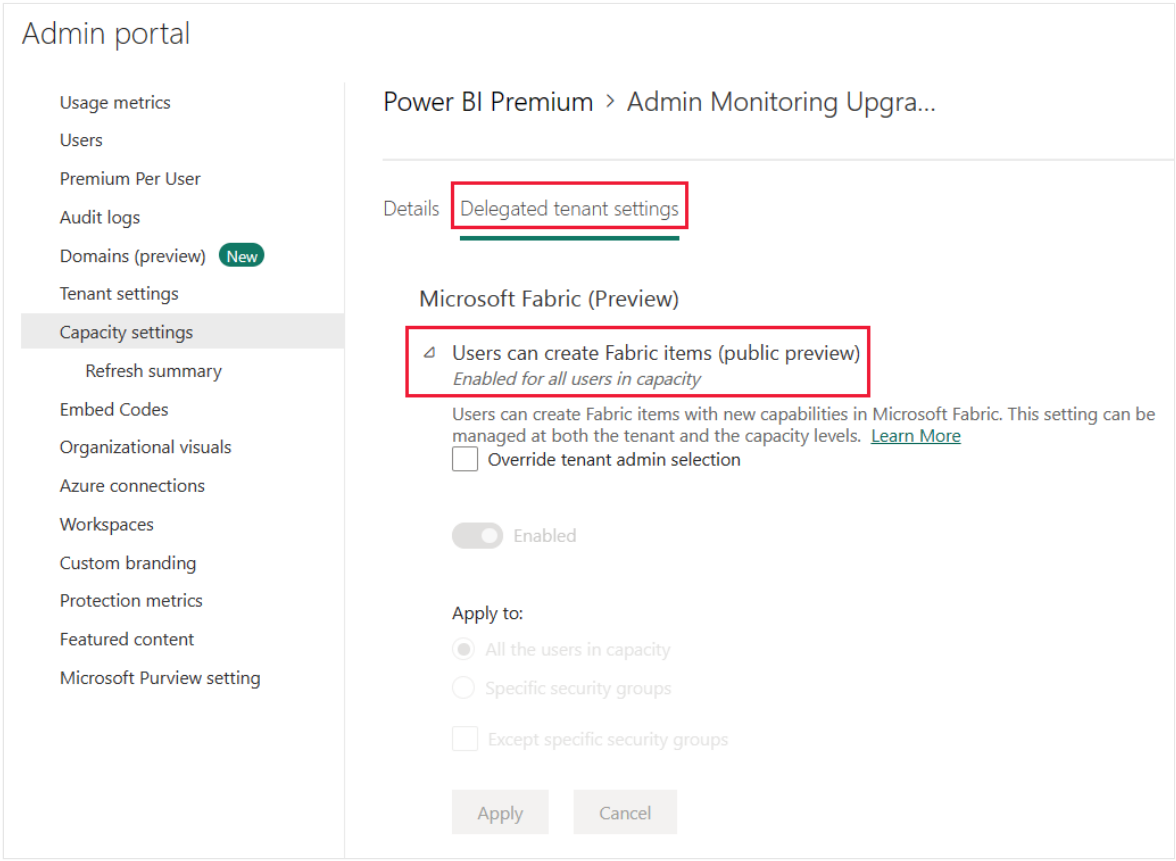
Enable for a capacity

Consider the Microsoft Fabric setting a recommendation for the entire organization. Capacity admins can override this setting, depending on their needs. For example, because Microsoft Fabric is a preview product, your organization decided not to enable it. However, your organization also has a group of highly advanced developers who

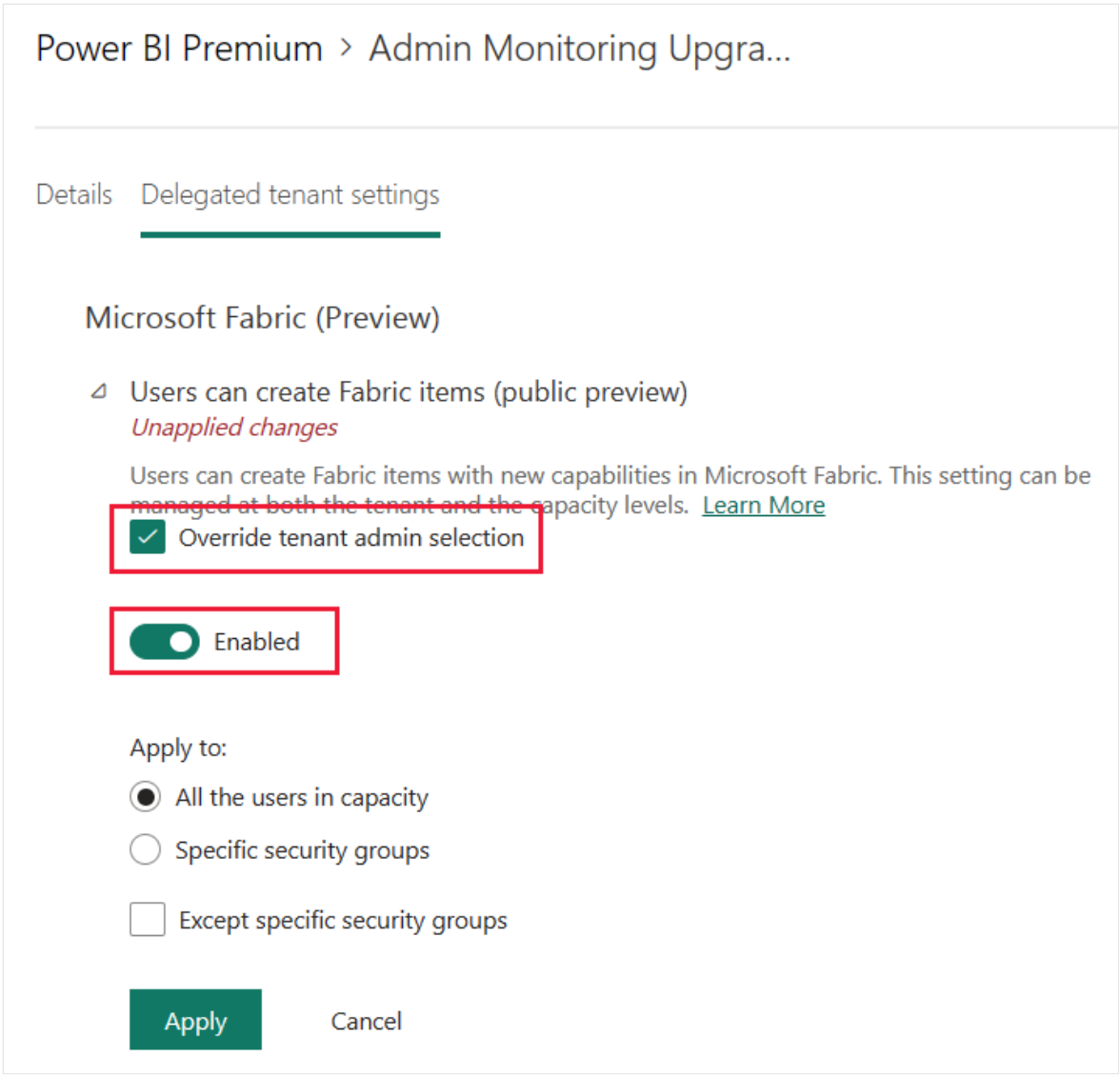
want to experiment with Microsoft Fabric. In such cases, Microsoft Fabric can be enabled at the capacity level.

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

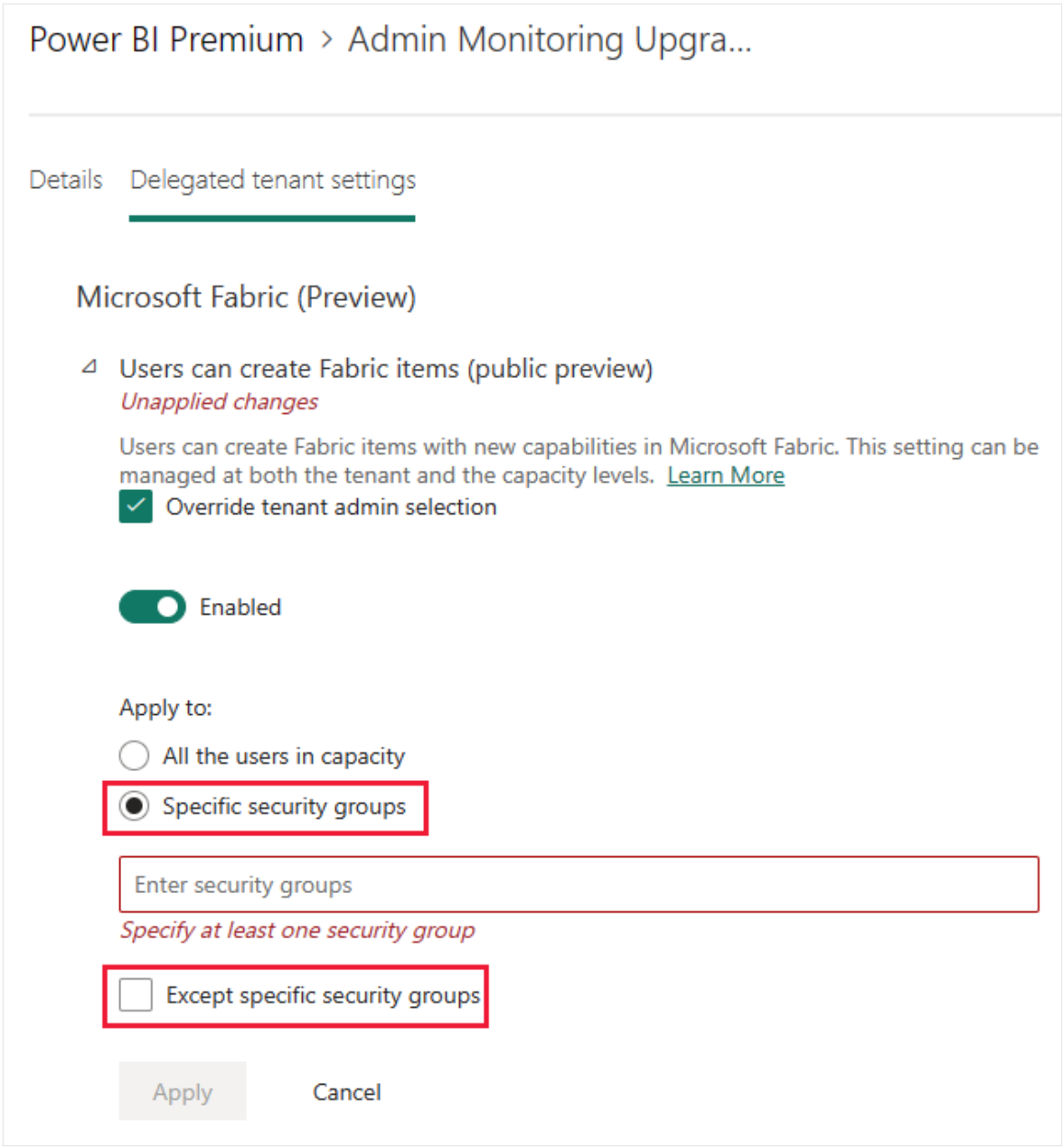
1. Navigate to the capacity settings in the admin portal.
2. Select the capacity you want to enable Microsoft Fabric for.
3. Select the **Delegate tenant settings** tab, and under *Microsoft Fabric (Preview)*, expand the **Users can create Fabric items (public preview)** setting.



4. Check the **Override tenant admin selection** checkbox and verify that the **Users can create Fabric items (public preview)** 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 (Preview)* 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.

Next steps

- Admin overview
- What is the admin portal?

Fabric region availability

Article • 05/23/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

Microsoft Fabric Public Preview is available in the Azure regions listed in this article. If your Microsoft Fabric home region isn't listed, you can still create a Microsoft Fabric capacity in a region that is supported. For more information, see Buy a Microsoft Fabric subscription.

To find out what your Fabric home region is, see Find your Fabric home region.

Asia Pacific

- AustraliaEast
- AustraliaSoutheast
- CentralIndia
- EastAsia
- JapanEast
- KoreaCentral
- SoutheastAsia
- SouthIndia

Europe

- NorthEurope
- WestEurope
- FranceCentral
- NorwayEast
- SwitzerlandNorth
- SwitzerlandWest
- UKSouth
- UKWest

Americas

- BrazilSouth
- CanadaCentral
- CanadaEast
- EastUS

- EastUS2
- NorthCentralUS
- SouthCentralUS
- WestUS
- WestUS2
- WestUS3

Middle East and Africa

- SouthAfricaNorth
- UAENorth

Next steps

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

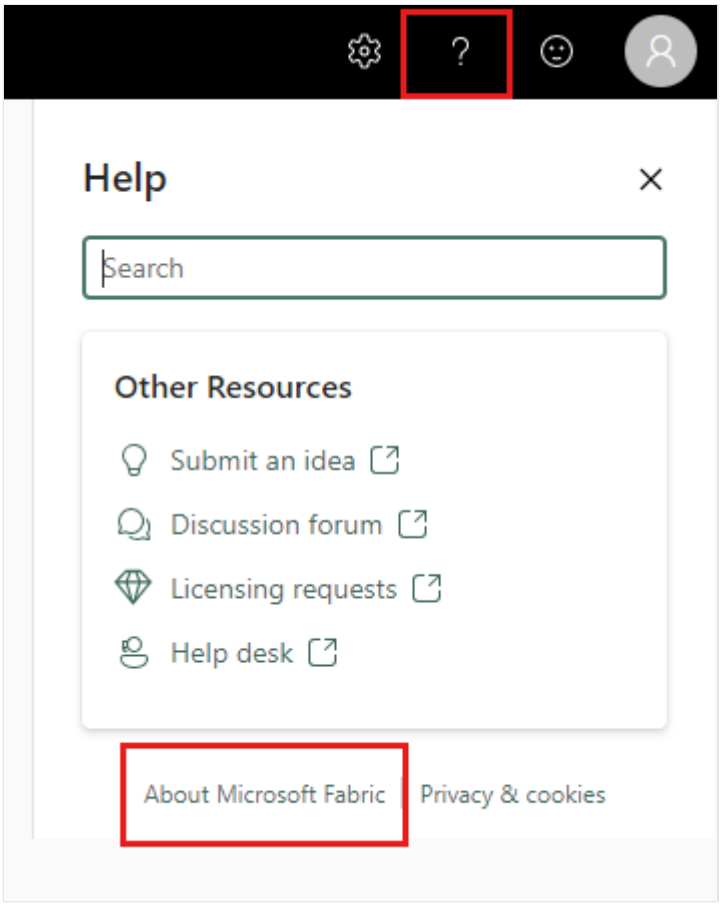
Find your Fabric home region

Article • 05/23/2023

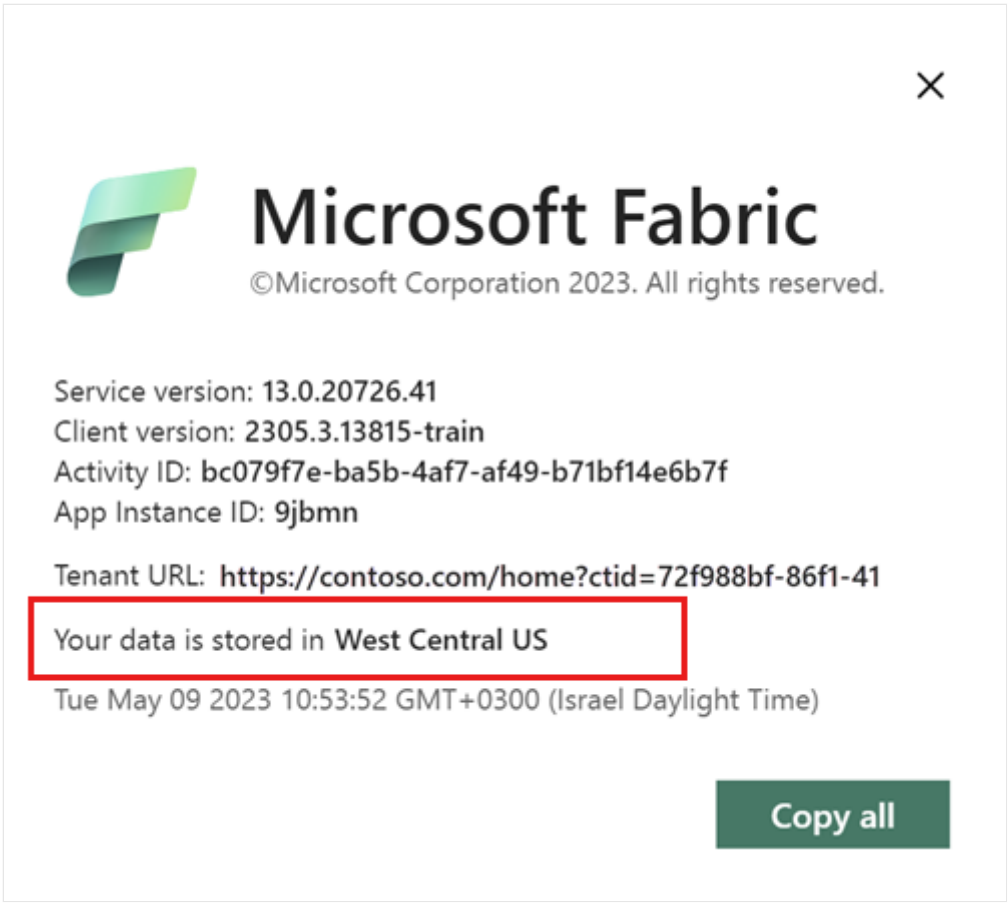
> **Important**
>
> Microsoft Fabric is in **preview**.

To find your Fabric home region, follow these steps:

1. Sign in to Fabric.
2. Open the Help pane and choose **About Microsoft Fabric**.



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 may also be using capacities in different regions for your workspaces.



Next steps

- Buy a Microsoft Fabric subscription
- Region availability

Understand Microsoft Fabric admin roles

Article • 06/20/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

To be a Microsoft Fabric admin for your organization, you must be in one of the following roles:

- Global administrator
- Power Platform administrator
- Fabric administrator

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. For more information, see Assign roles to user accounts with PowerShell.

Users in Fabric administrator and Power Platform administrator roles have full control over org-wide Microsoft Fabric settings and admin features, except for licensing. Once a user is assigned an admin role, they can access the admin portal. There, they have access to org-wide usage metrics and can control org-wide usage of Microsoft Fabric features. These admin roles are ideal for users who need access to the Fabric admin portal without also granting those users full Microsoft 365 administrative access.

Assign users to an admin role in the Microsoft 365 admin portal

To assign users to an admin role in the Microsoft 365 admin portal, follow these steps.

1. In the Microsoft 365 admin portal, select **Users** > **Active Users**.
2. Select the user that you want to assign the role to.
3. Under **Roles**, select **Manage roles**.
4. Expand **Show all by category**, then select **Fabric administrator** or **Power Platform administrator**.

5. Select **Save changes**.

Assign users to the admin role with PowerShell

You can also assign users to roles by using PowerShell. Users are managed in Azure Active Directory (Azure AD). If you don't already have the Azure AD PowerShell module, download and install the latest version.

1. Connect to Azure AD:

```
PowerShell

Connect-AzureAD
```

2. Get the **ObjectId** for the **Fabric administrator** role. You can run Get-AzureADDirectoryRole to get the **ObjectId**.

```
PowerShell

Get-AzureADDirectoryRole
```

> **Note**
>
> In the output produced by the PowerShell command, look for the *Power BI Service Administrator* in the DisplayName column. This is the legacy name for the *Fabric administrator*.

```
Output

ObjectId                             DisplayName
Description
--------                             -----------
-----------
00f79122-c45d-436d-8d4a-2c0c6ca246bf Power BI Service Administrator
Full access in the Power BI Service.
250d1222-4bc0-4b4b-8466-5d5765d14af9 Helpdesk Administrator
Helpdesk Administrator has access to perform..
3ddec257-efdc-423d-9d24-b7cf29e0c86b Directory Synchronization Accounts
Directory Synchronization Accounts
50daa576-896c-4bf3-a84e-1d9d1875c7a7 Company Administrator
Company Administrator role has full access t..
6a452384-6eb9-4793-8782-f4e7313b4dfd Device Administrators
Device Administrators
9900b7db-35d9-4e56-a8e3-c5026cac3a11 AdHoc License Administrator
Allows access manage AdHoc license.
```

```
a3631cce-16ce-47a3-bbe1-79b9774a0570 Directory Readers
Allows access to various read only tasks in ..
f727e2f3-0829-41a7-8c5c-5af83c37f57b Email Verified User Creator
Allows creation of new email verified users.
```

In this case, the role's **ObjectId** is 00f79122-c45d-436d-8d4a-2c0c6ca246bf.

3. Next, get the user's **ObjectId**. You can find that by running Get-AzureADUser.

PowerShell

```
Get-AzureADUser -ObjectId 'tim@contoso.com'
```

Output

```
ObjectId                             DisplayName UserPrincipalName
UserType
--------                             ----------- -----------------
--------
6a2bfca2-98ba-413a-be61-6e4bbb8b8a4c Tim         tim@contoso.com
Member
```

4. To add the member to the role, run Add-AzureADDirectoryRoleMember.

Parameter	Description
ObjectId	The Role ObjectId.
RefObjectId	The members ObjectId.

PowerShell

```
Add-AzureADDirectoryRoleMember -ObjectId 00f79122-c45d-436d-8d4a-
2c0c6ca246bf -RefObjectId 6a2bfca2-98ba-413a-be61-6e4bbb8b8a4c
```

To learn more about using PowerShell to assign admin roles, see AzureAD Directory Roles.

Next steps

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

What is the admin portal?

Article • 06/15/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

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.

The admin portal can be accessed by admins with the following roles:

- Global administrator
- Power Platform administrator
- Fabric administrator

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 table below with links to relevant documentation for each one.

Feature	Description
Tenant settings	Enable, disable, and configure Microsoft Fabric.
Usage metrics	View usage metrics related to your organization.
Users	Manage users in the Microsoft 365 admin portal.
Premium Per User	Configure auto refresh and dataset workload settings.
Audit logs	Audit Microsoft Fabric activities in the Microsoft Purview compliance portal.
Capacity settings	Manage Microsoft Fabric DC capacities.
Refresh summary	Schedule refresh on a capacity and view the details of refreshes that occurred.

Feature	Description
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.
Azure connections	Configure and manage connections to Azure resources.
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.
Protection metrics	Monitor and track sensitivity label usage and adoption 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 cog symbol and from the menu select **Admin portal**.

Next steps

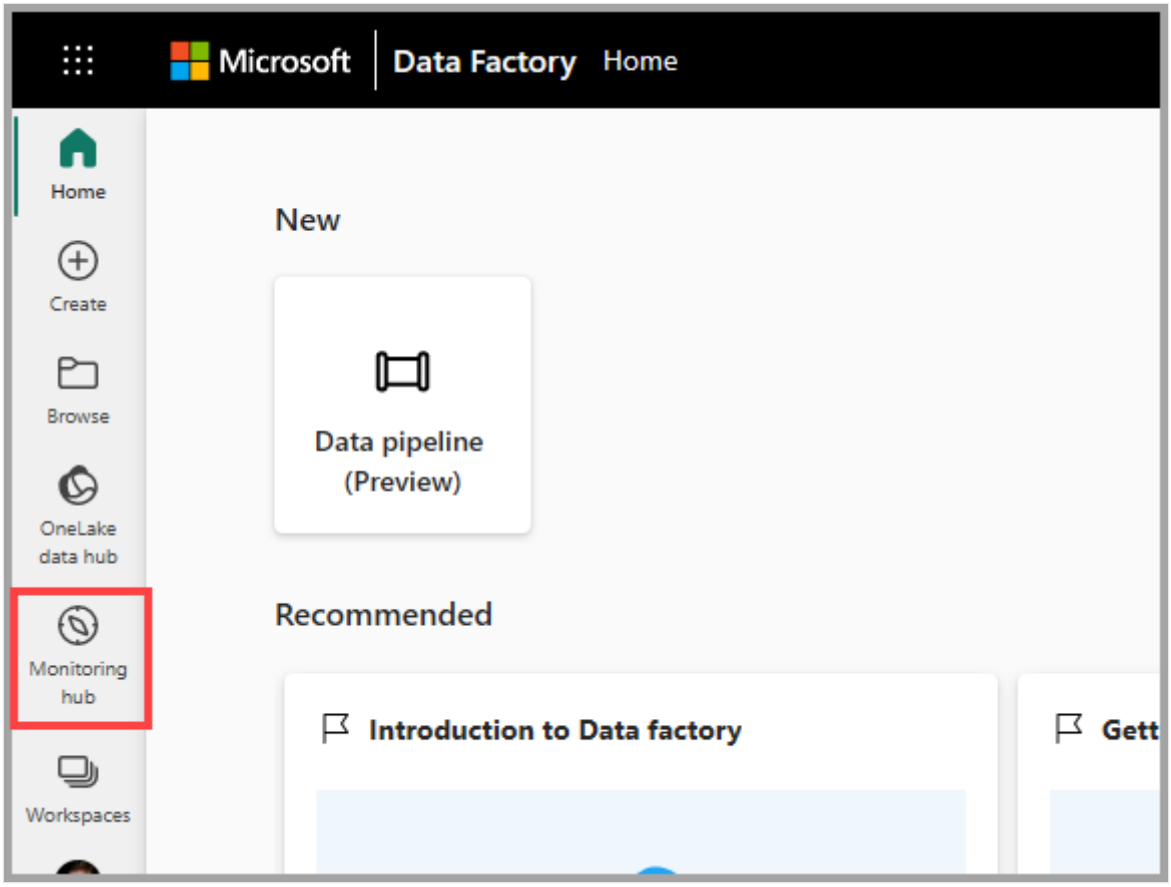
- What is the admin monitoring workspace?
- Workspace tenant settings
- Manage workspaces

Using Monitoring hub

Article • 05/23/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

Monitoring hub enables users to monitor various Microsoft Fabric activities, such as dataset refresh and Spark Job runs and many others, from a central location. You can access *Monitoring hub* by selecting its icon from the left pane.



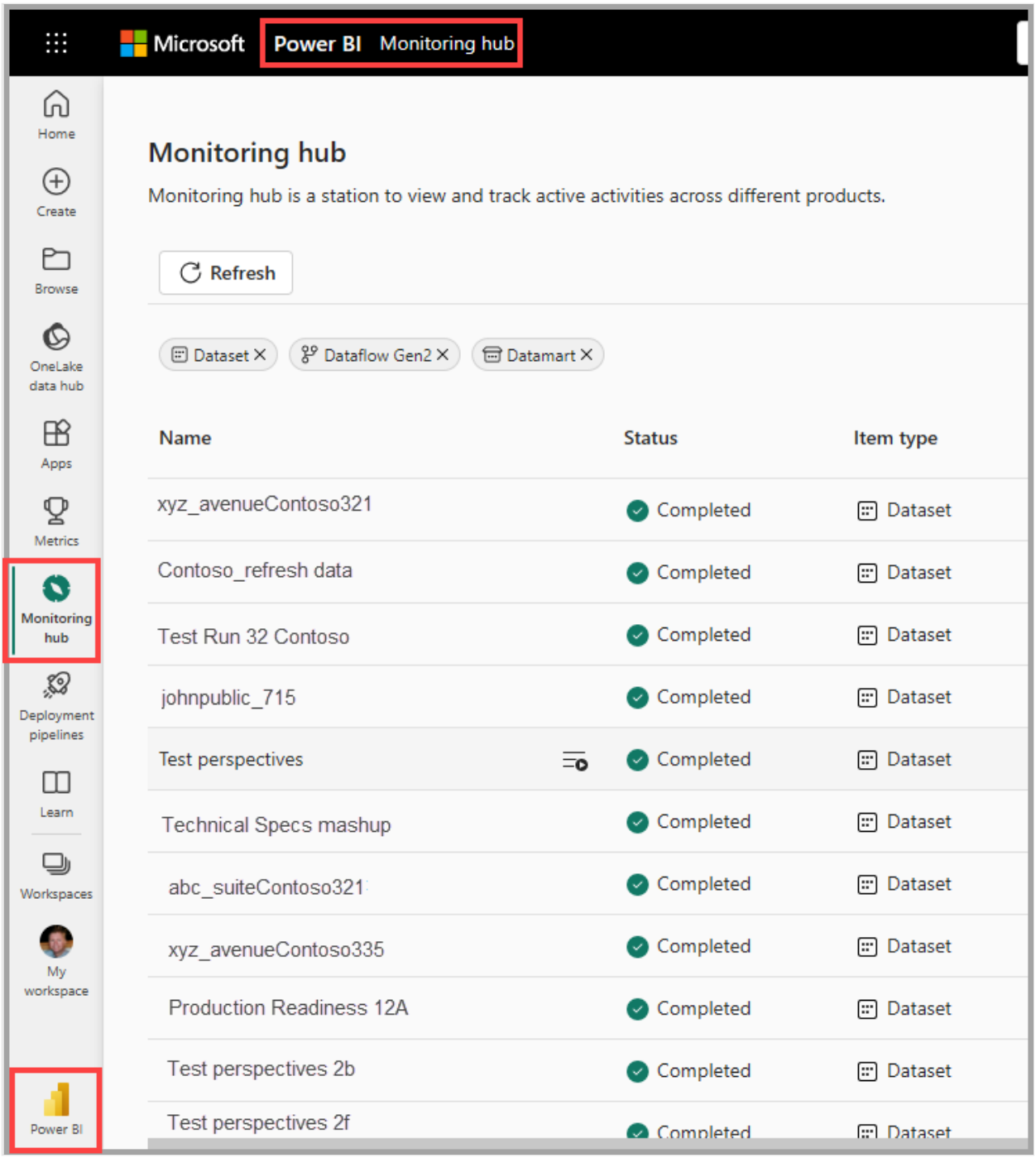
Monitoring hub is available for Power BI, Data Factory, Data Engineering and Data Science during the Microsoft Fabric public preview.

Prerequisites

Verify that the new workspace experience is enabled.

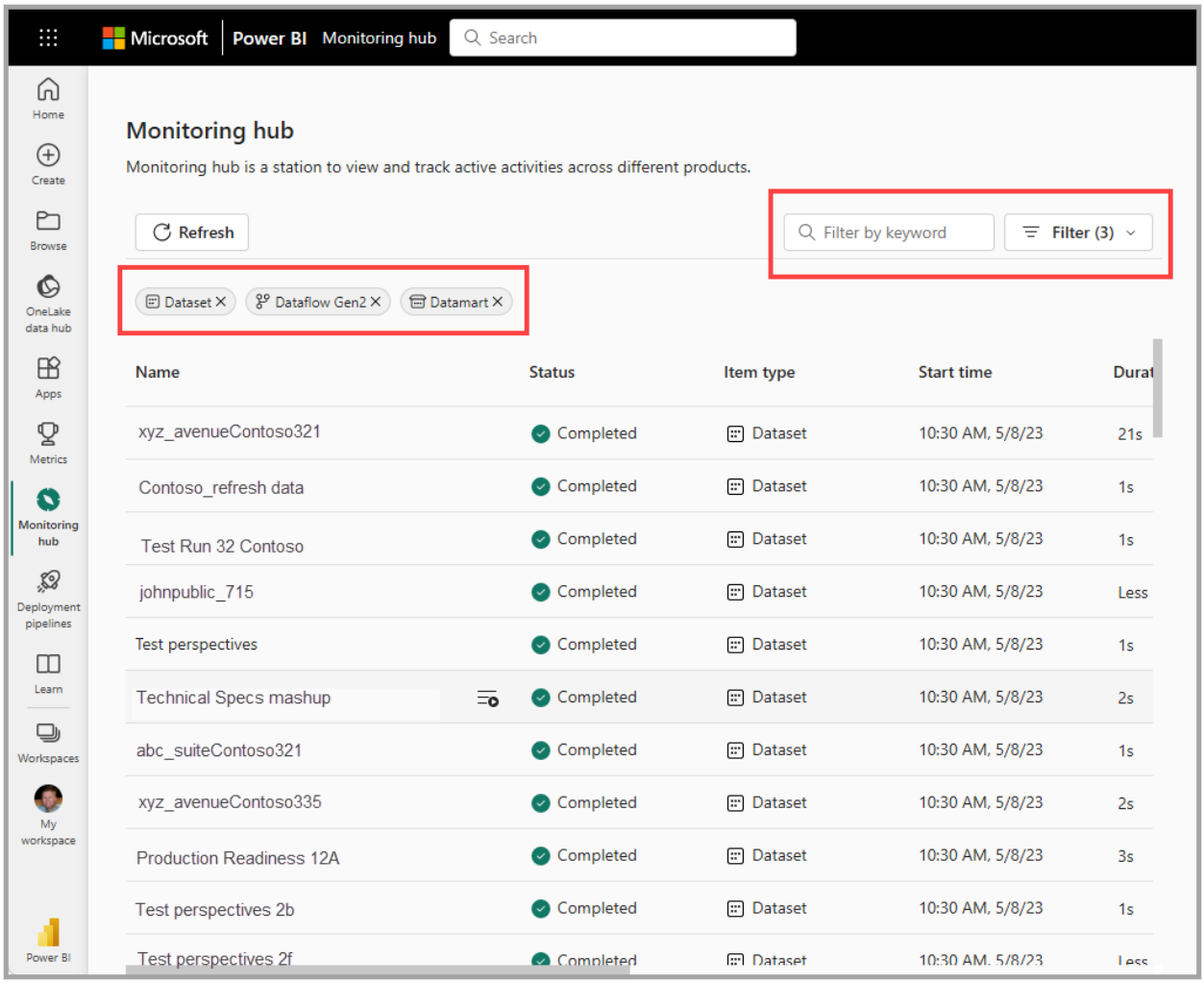
Using Monitoring hub

Monitoring hub shows activities based on which service is being used when Monitoring hub is selected. For example, if you're using Data Factory when you select Monitoring hub, a list of Data Factory activities is displayed. If you're using Power BI and then select Monitoring hub from the left pane, a list of Power BI related activities is displayed.



Because there may be many records in Monitoring hub, filters are applied by default to limit the number of items initially displayed. For example, the following image shows Monitoring hub for Power BI, where filters are applied to only show *Dataset*, *Dataflow Gen2*, and *Datamart* items.

You can dismiss filters by selecting the *x* beside the filter button, and you can select different filters by using the filter drop-down in the upper right corner of the window. You can also filter by keyword.



The first seven columns in the list of items are shared across all Monitoring hub views. The columns after the first seven are specific to the viewing context, such as Power BI.

Getting detailed item information

When you select an item from the list, Monitoring hub displays detailed information about that item.

When you hover over an item's name, any available quick actions for the item type are displayed, such as stop, start, re-run, or other quick actions. You can also open a detail pane for the item itself when you hover, for example, *View run history* for datasets that are in Monitoring hub, to display their refresh activities.

Next steps

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

Track user activities in Fabric

Article • 05/23/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

Knowing who is taking what action on which item in Fabric can be critical in helping your organization fulfill its requirements, such as meeting regulatory compliance and records management.

In Fabric, user activities are logged in the Power BI activity log and in the unified audit log. You can retrieve them for tracking purposes in the same way as in Power BI, as described in Track user activities in Power BI. The following operations can be retrieved:

- For Power BI items: All currently available operations
- For all other Fabric items: Currently, only *create*, *read*, *update*, and *delete* operations.

Next steps

- Track user activities in Power BI

What is the admin monitoring workspace?

Article • 06/15/2023

> **ⓘ Important**
>
> Microsoft Fabric is in **preview**.

The *Admin monitoring* workspace is designed to provide admins with monitoring capabilities for their organization. Using the Admin monitoring workspace resources, admins can perform security and governance tasks such as audits and usage checks.

Prerequisites

To use the admin monitoring workspace, you need:

- To be an admin with one of these roles.
  - Microsoft 365 *Global administrator*
  - *Fabric administrator*
- A *Pro* license

Access the admin monitoring workspace

The Admin monitoring workspace is enabled for Microsoft Fabric admins that have the *Fabric admin* role. Admins can also share its content with other users.

The admin monitoring workspace is automatically installed during the first time any Microsoft Fabric admin accesses it. To access the admin monitoring workspace, follow these steps:

1. Log into Microsoft Fabric with your account.
2. From the left pane, select **Workspaces**.
3. Select **Admin monitoring**. When you select this option for the first time, the required items are automatically installed.

Reports and datasets

In the monitoring workspace, you can use the Feature Usage and Adoption report as is. You can also connect to this report's dataset, and create a solution that's optimized for your organization.

Manage access

There are several ways you can manage access to content of the admin monitoring workspace. If you're the admin of the workspace, you have a *member* workspace role and you can grant access to any of its items with or without share and build permissions.

- **Workspace** - Learn how to to give users access to the workspace in manage workspace. You can only grant other users a viewer role. Once a viewer role is provided, it can't be taken away.
- **Report** - You can share a report with other users.
- **Dataset** - You can share access to a dataset with other users. Once a dataset is shared, you can't unshare it.

Refreshes

The admin monitoring workspace is automatically refreshed once a day. The refresh takes place about 10 minutes after the admin workspace was accessed for the first time.

For the refresh to work, the admin that accessed the workspace for the first time, has to:

- Keep his *Global administrator* or *Fabric administrator* role. If the role of the admin who first accessed the workspace changes, the admin monitoring workspace will not be refreshed.
- If the workspace creator uses Privileged Identity Management (PIM), it has to be enabled during the scheduled refresh.

Considerations and limitations

- Sovereign clouds are not supported.
- The *admin Monitoring* workspace is a read-only workspace. Users, including workspace admins, are not able to edit or view properties of the items in the workspace, including datasets and reports.

Next steps

- Admin overview
- Feature usage and adoption report

Feature usage and adoption report

Article • 06/15/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

The Feature Usage and Adoption Report is a comprehensive analysis of usage and adoption of different features in your Microsoft Fabric tenant. As a Fabric admin you can share this report with others in your organization. You can also share the report's dataset, and use it to customize the report, or build a new report that relies on the same data.

You can access the report from the admin monitoring workspace. To see this workspace you need to be a Fabric administrator.

Navigation

The report is built to allow admins to analyze specific scenarios. Use the report date slicer to filter data for each page across the report. You can also use the filter pane to filter out information on the page, using available filters based on different scenarios.

Report pages

The *feature usage and adoption* report has three pages:

- **Activity Overview** - Provides a bird's eye view of activities and usage across the entire organization
- **Analysis** - Visualizes data across multiple activity dimensions
- **Activity Details** - Displays detailed information on specific or multiple capacity or workspace activities

Activity Overview page

Use the Activity Overview page to find out:

- What are the daily activities and user trends?

- Which capacities and workspaces are the most active?
- View activities in your organization.
- View activities in your organization by users or top active user.

For example, if you're working in a large retail organization, you may want to use the Activity Overview page to find out what capacities were utilized during December. You use the *Date* fields to filter the results for December, and notice that the *sales and marketing* capacity has almost 1,000 activities, while other capacities have under 200 activities each. You decide to further investigate this, and go to the Analysis page to try and understand why this is happening.

Analysis page

In the Analysis page, you can see a daily count of activities and users by date and a decomposition tree that automatically aggregates data and enables drilling down into dimensions in any order. Use the decomposition tree, to decompose the activities according to *operation* and *user*. You can use the additional available fields to decompose activities.

To view the details of a specific activity, drill through to the Activity Details:

1. Right-click the activity you want to drill through from.
2. Select *Drill through*.
3. Select *Activity Details*.

Continuing the example from the Activity Overview page, you turn to the Analysis page to understand why in December, the *sales and marketing* capacity has almost five times more activities than any other capacity. Using the *Date* fields, you filter the results for December. By reviewing the *Decomposition tree*, you see that almost all of the activities are for viewing a Power BI report. You decide to drill through to the Activity details page to understand which report is being extensively viewed.

Activity Details page

The Activity Details page shows information related to specific or multiple capacity or workspaces activities. You can only get to the *Activity Details* page from the page navigation menu, or by drilling through from the Activity Overview or Analysis pages. To drill through, right-click a result and then select the *Activity Details* page. After drilling through, you see the following information for the selected activities:

- **Creation time** - The time the activity was registered
- **Capacity name** - The name of the capacity that the activity took place in
- **Capacity ID** - The ID of the capacity that the activity took place in
- **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 (UPN) of the user who created the activity
- **Operation** - The name of the operation
- **Total of activities** - The number of times the activity was registered

To conclude the example given in the Activity Overview and Analysis pages, after drilling through from the *View Reports* log, in the Analysis page, you realize that a report titled *unclosed deals* has been heavily reviewed during December. After further inquiries, you learn that this is a new report and that many people in the organization reviewed in during December, to try and understand how sales could have been improved.

Considerations and limitations

This section lists the report's considerations and limitations.

Display

- The single data point across the zoom slider, displays a misleading date range for the total activities and users.
- When drilling down to a workspace, the *Expand All* feature doesn't update the *Most Active Capacities* visual title.
- Capacities with the same name and capacities that were deleted and recreated with the same name, are displayed as one capacity.
- *NA* represents data that isn't available in the *Audit* table. This can happen when an event doesn't have the dimension information, or when that information isn't applicable for the event.
- The report retains information for 30 days.

Counting logic

- All *MyWorkspaces* are counted as different records as part of the *Active Workspaces* total.
- When a capacity, workspace or item is deleted, its activities are counted in the report but appear as *(Blank)*.
- Capacities with the same name but different IDs are counted as separate records.

Next steps

- What is the admin monitoring workspace?
- Admin overview

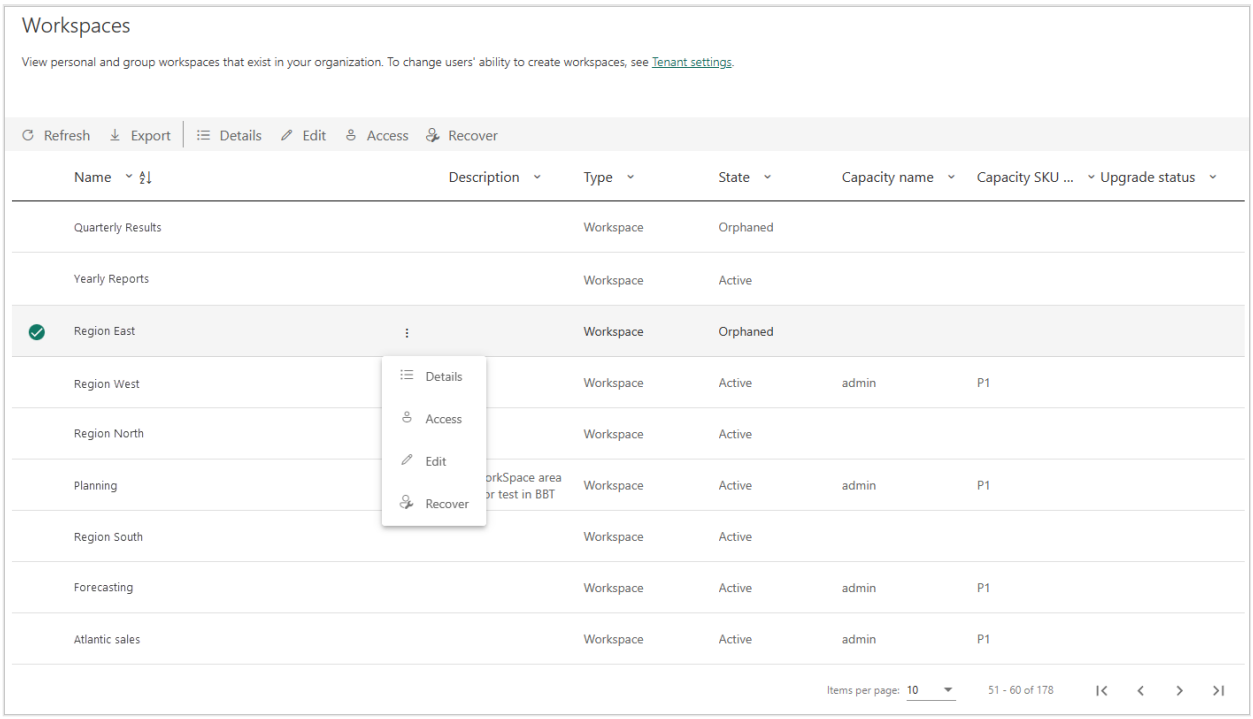
Manage workspaces

Article • 05/23/2023

> **ⓘ Important**
>
> Microsoft Fabric is in **preview**.

As a Microsoft 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 columns of the list of workspaces are described below

Column	Description
Name	The name given to the workspace.
Description	The information that is given in the description field of the workspace settings.

Column	Description
Type	The type of workspace. There are two types of workspaces:  **Workspace** (also known as "app workspace")  **Personal Group** ("My workspaces")
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 possible workspace states are described below.

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. A microsoft Fabric administrator can restore the workspace up to 30 days after it was deleted. When the 30 days pass, the workspace enters the *Removing* state. If you delete a *MyWorkspace* workspace, it moves to the *Removing* state immediately, without the 30 day grace period.
Removing	After you delete a workspace, and once the 30 day grace period passes, the workspace 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.

State	Description
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.

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. See Restore a deleted My workspace as an app workspace for detail.

> **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.

Govern My workspaces

Every Microsoft 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, Microsoft Fabric admins can use a set of features to help them govern these workspaces. With these features, Microsoft 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 may reside in non-compliant 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 Microsoft 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'll be able to 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 Microsoft Fabric admin or capacity admin can designate a capacity as the default capacity for My workspaces. For details, see Designate a default capacity for My workspaces

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

Microsoft Fabric admins can designate a default capacity for My workspaces. However, even if a My workspace has been assigned to Premium capacity, the owner the workspace can still move it back to Pro, which is in Shared capacity. Moving a workspace from Premium capacity to Shared capacity might cause the content contained in the workspace to be become non-compliant with respect to data-residency requirements, since it might move to a different region. To prevent this situation, the Microsoft Fabric admin can block My workspace owners from moving their My workspace to a different capacity by turning off the **Users can reassign personal workspaces** tenant admin setting. See Workspace settings for detail.

Restore a deleted My workspace as an app workspace

When users leave the company, their My workspaces show up as Deleted in the State column on the Workspaces page in the Admin portal. Microsoft Fabric admins can restore deleted My workspaces as app workspaces that other users can collaborate in.

During this restoration process, the Microsoft 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 Microsoft 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 between capacities in different regions, or between different capacity types, such as Premium and shared.

In Microsoft Fabric, such movement currently has the following restrictions:

- Non Power BI Fabric items can't move from Premium to shared capacity.
- Non Power BI Fabric items can't move between regions.

This means the following:

- **Moving a workspace from one capacity to another within the same region**

  If the workspace has non Power BI Fabric items, you can only move it from one Premium capacity to another Premium capacity. If you want to move the workspace from Premium to shared capacity, you won't be able to do so unless you delete all non-Power BI Fabric items first.

  If the workspace has no non Power BI Fabric items (that is, it has only Power BI items) moving the workspace from Premium to shared is supported.

- **Moving a workspace from one capacity to a capacity in a different region**

  If the workspace has non Power BI Fabric items, you won't be able to move it unless you delete all non-Power BI Fabric items first.

  If the workspace has no non-Power BI Fabric items (that is, it has only Power BI items) moving the workspace to another capacity in a different region is supported.

Next steps

About the Admin portal

Workspace tenant settings

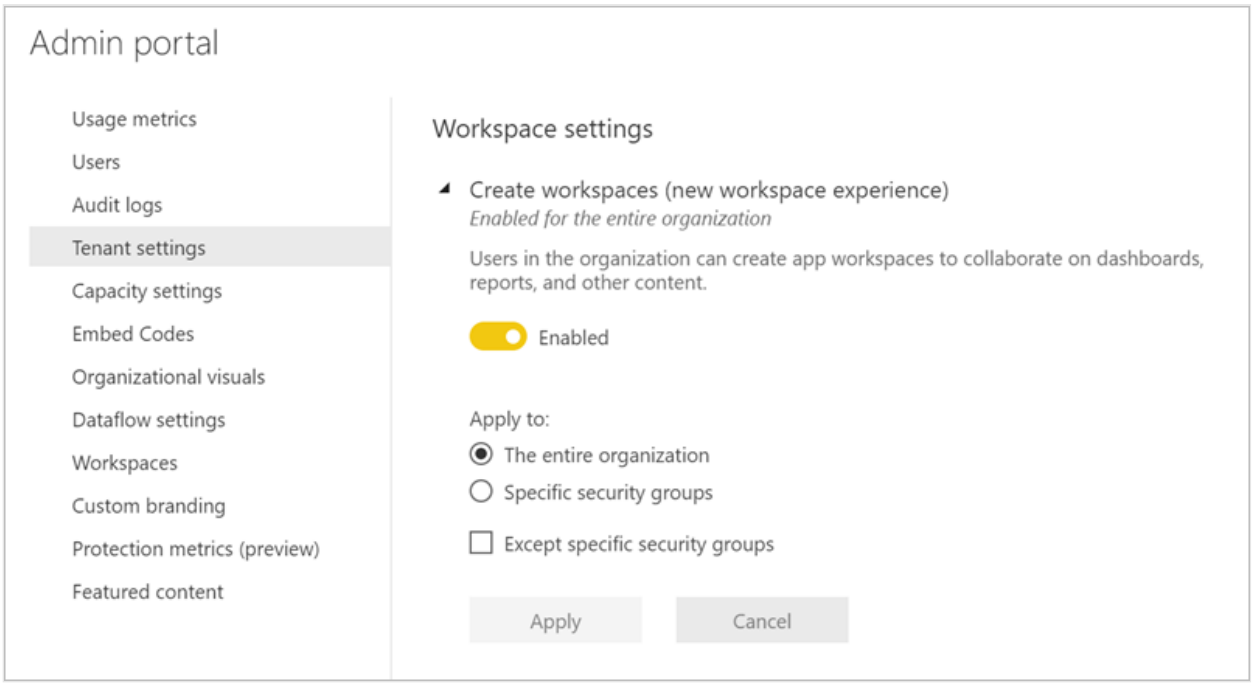
Article • 05/23/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

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.



For classic workspaces based on Microsoft 365 Groups, administration continues to occur in admin portal and Azure Active Directory.

> **Note**
>
> The **Create workspaces** setting defaults to allowing only users who can create Microsoft 365 Groups to create the new Microsoft Fabric workspaces. Be sure to set

a value in the Microsoft Fabric admin portal to ensure appropriate users can create them.

List of workspaces

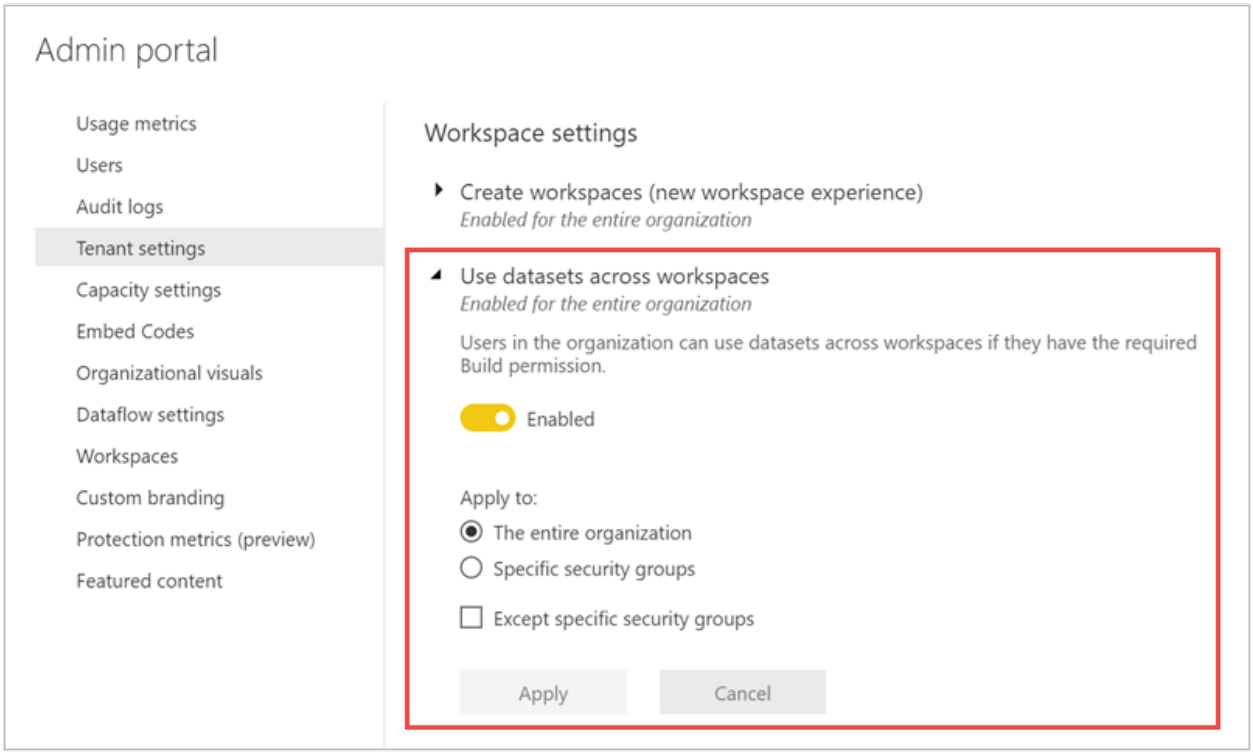
The admin portal has another section of settings about the workspaces in your tenant. In that section, you can sort and filter the list of workspaces and display the details for each workspace. See Workspaces in this article for details.

Publish content packs and apps

In the admin portal, you also control which users have permissions to distribute apps to the organization. See Publish content packs and apps to the entire organization in this article for details.

Use datasets across workspaces

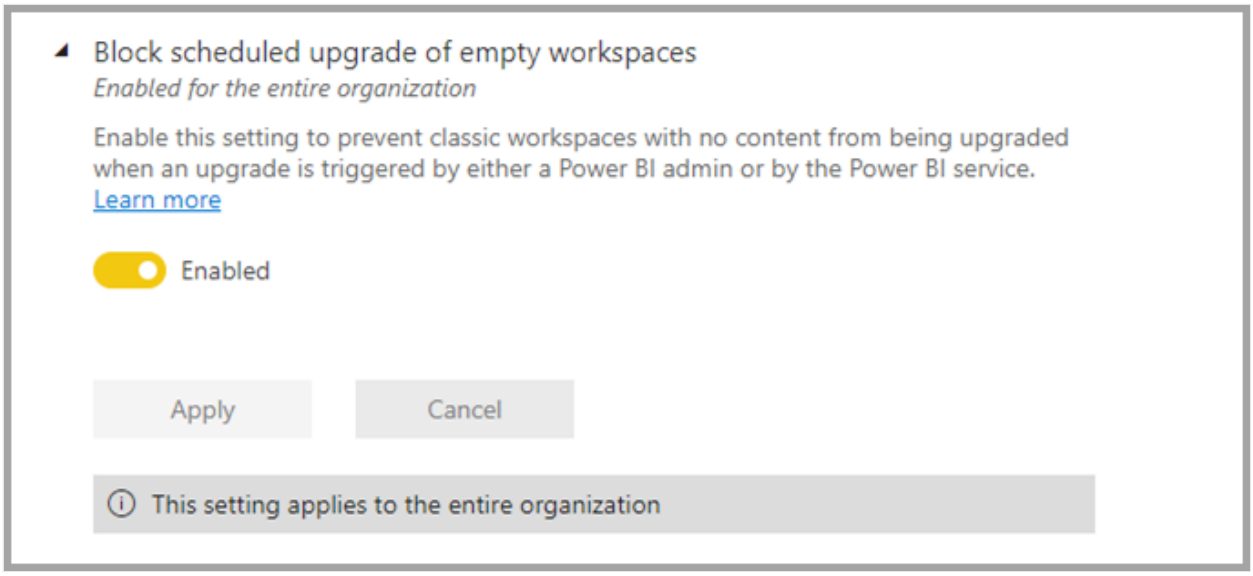
Admins can control which users in the organization can use datasets across workspaces. When this setting is enabled, users still need the required Build permission for a specific dataset.



For more information, see Intro to datasets across workspaces.

Block scheduled upgrade of empty workspaces

To reduce the impact of maintaining empty classic workspaces that were automatically created, empty classic workspaces are deleted by default as part of the upgrade process. However, admins can prevent deleting empty workspaces by disabling the following setting in the Admin portal.



Additional notes on deletion of empty workspaces:

- Only empty v1 workspaces will be deleted during upgrade. Empty v2 workspaces will not be deleted. Deletion of empty workspaces can be prevented by using the tenant setting described previously in this article.
- Office 365 groups associated with empty v1 workspaces aren't deleted. Read more about workspaces.

Users can reassign personal workspaces

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 off the **Users can reassign personal workspaces** tenant setting. When this setting is off, My workspace owners can't change the capacity assignment of their My workspace.

To turn off 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 **Users can reassign personal workspaces**. By default, this setting is on, which means that any My workspace owner can reassign their My workspace capacity. To prevent users from being able to reassign the capacity of their My workspace, turn the setting off.

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

Next steps

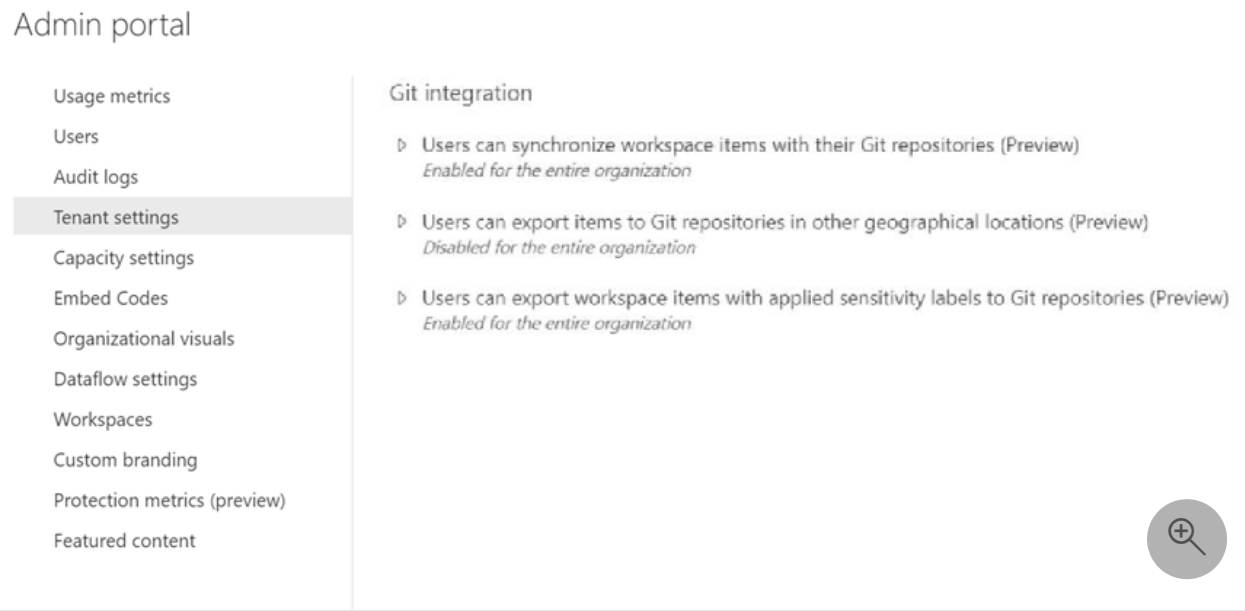
About tenant settings

Tenant admin settings for git integration

Article • 05/23/2023

> **ⓘ Important**
>
> Microsoft Fabric is in **preview**.

The git integration tenant admin 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.



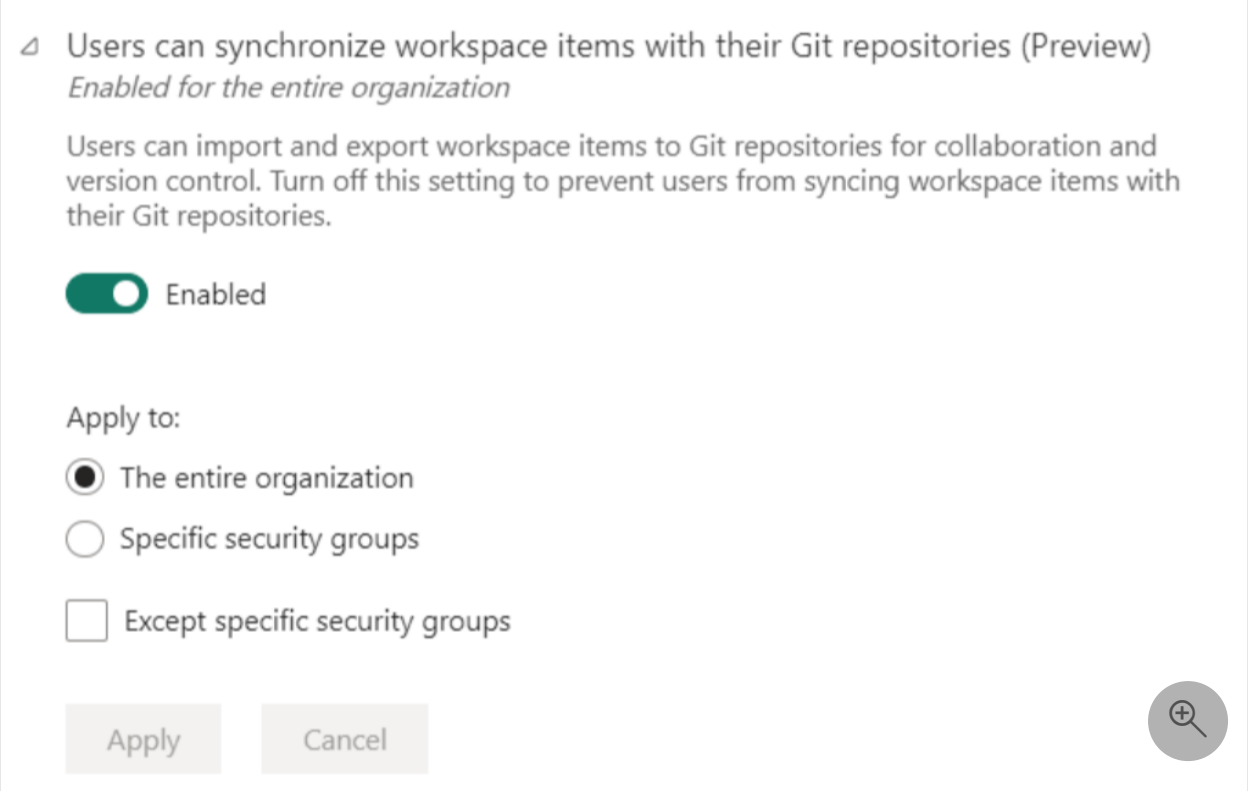
> **ⓘ Important**
>
> The switches that control git integration are part of Microsoft Fabric and will only work if the **Fabric admin switch** is turned on. If Fabric is disabled, git integration can't work regardless of the status of these switches.

These settings are only visible to the tenant admin.
There are three settings relating to git integration:

- Enable the git integration feature
- Enable git actions on workspaces residing in other geographical locations
- Enable export of items that have sensitivity labels

Enable git integration feature

Enable this setting to allow users to synchronize a workspace with a 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.

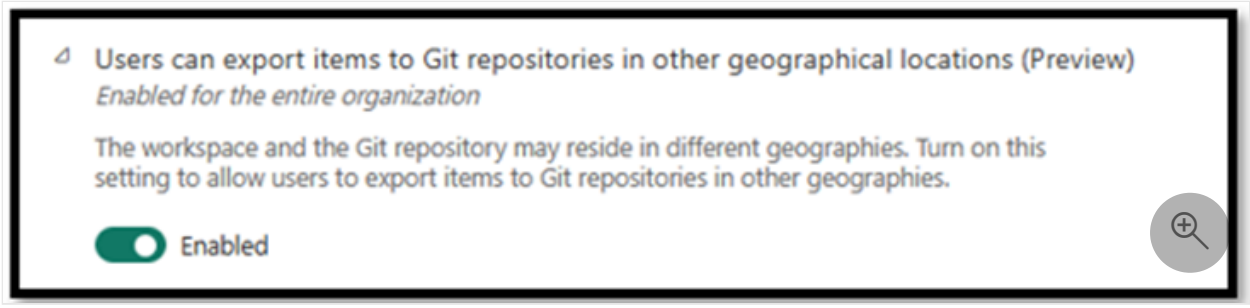


Learn more about git integration.

Enable git actions on workspaces residing in other geographical locations

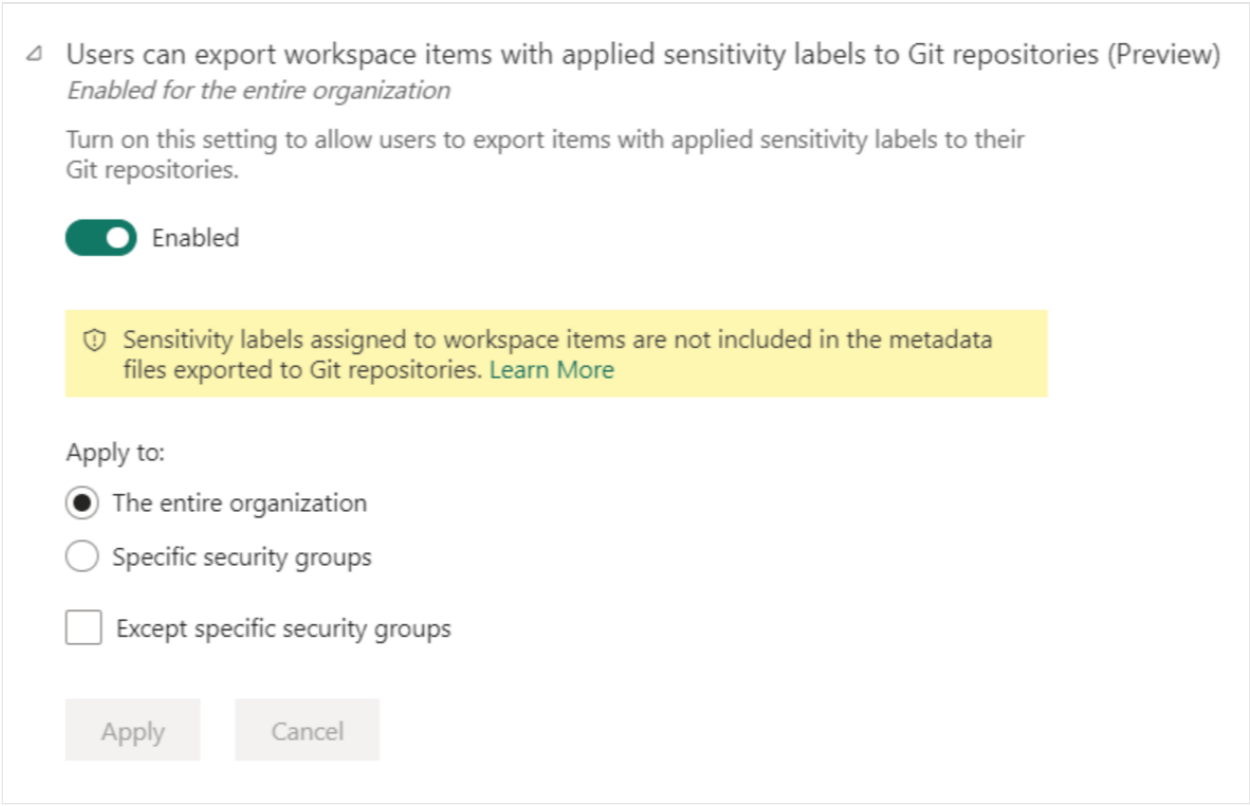
If a workspace capacity is in one geographic location (for example, Central US) while the Azure DevOps repo is in another location (for example, West Europe), the Fabric admin can decide whether to allow users to commit metadata (or perform other git actions) to another geographical location. Only the 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.



Enable export of items that have sensitivity labels

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.

Next steps

- About tenant settings
- About git integration

Set up item certification

Article • 06/15/2023

> **Important**
>
> Microsoft Fabric is in **preview**.

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:

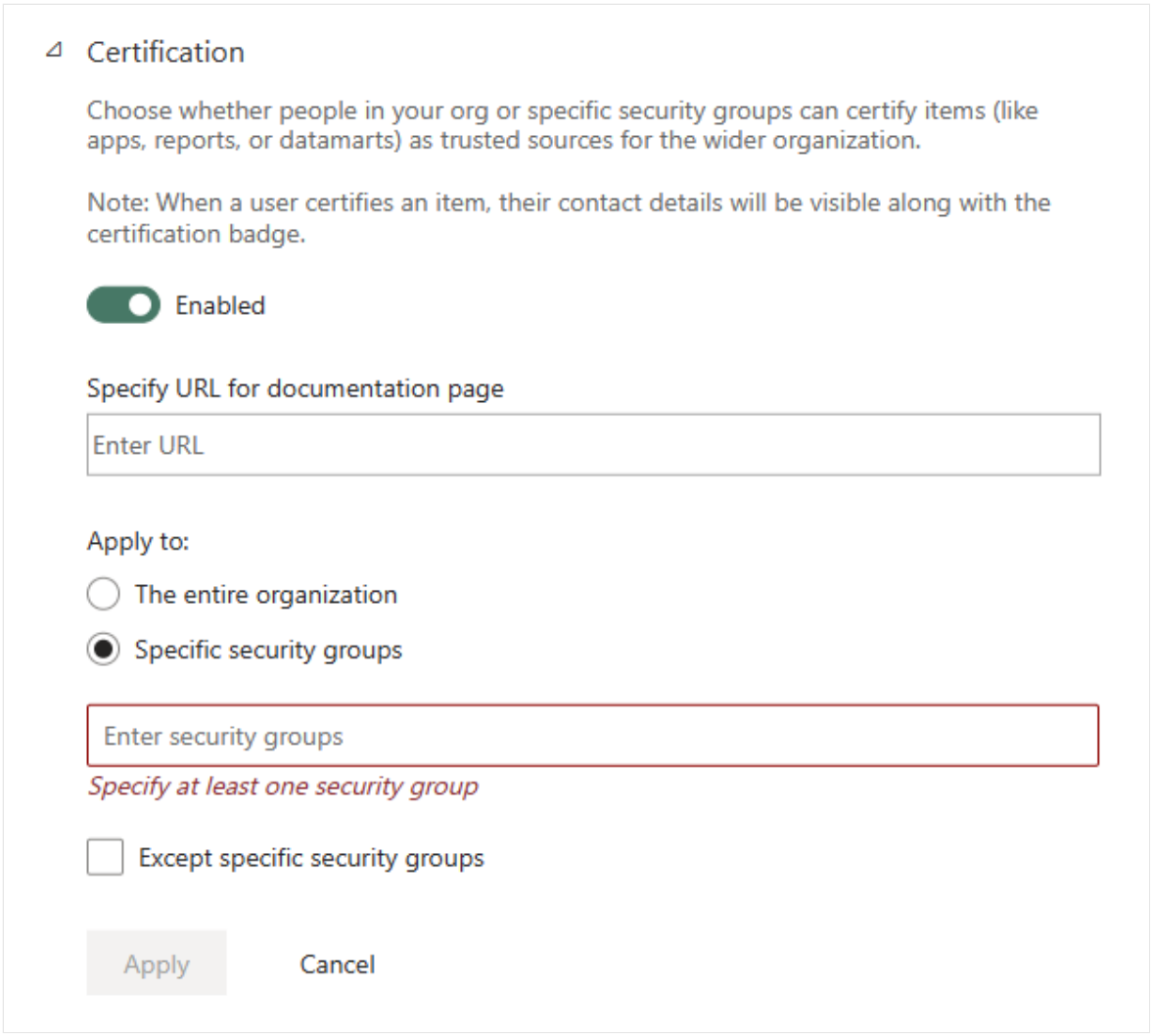
- Enabling certification on your tenant.
- Defining a list of security groups whose members will be authorized to certify items.
- Providing a URL that points to the documentation for the organization's item certification process, if such documentation exists.

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

Set up 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 name(s) of those group(s) in a text box that will appear.

6. Select **Apply**.

Next steps

- Read about endorsement in Fabric
- Promote Fabric items
- Certify Fabric items

Set up metadata scanning in your organization

Article • 06/15/2023

> **ⓘ Important**
>
> Microsoft Fabric is in **preview**.

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 dataset metadata scanning.

Enable service principal authentication for read-only admin APIs

Service principal is an authentication method that can be used to let an Azure AD 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 dataset 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**.

Next steps

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

Enable service principal authentication for read-only admin APIs

Article • 05/23/2023

Service principal is an authentication method that can be used to let an Azure Active Directory (Azure AD) application access Microsoft Fabric content and APIs.

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

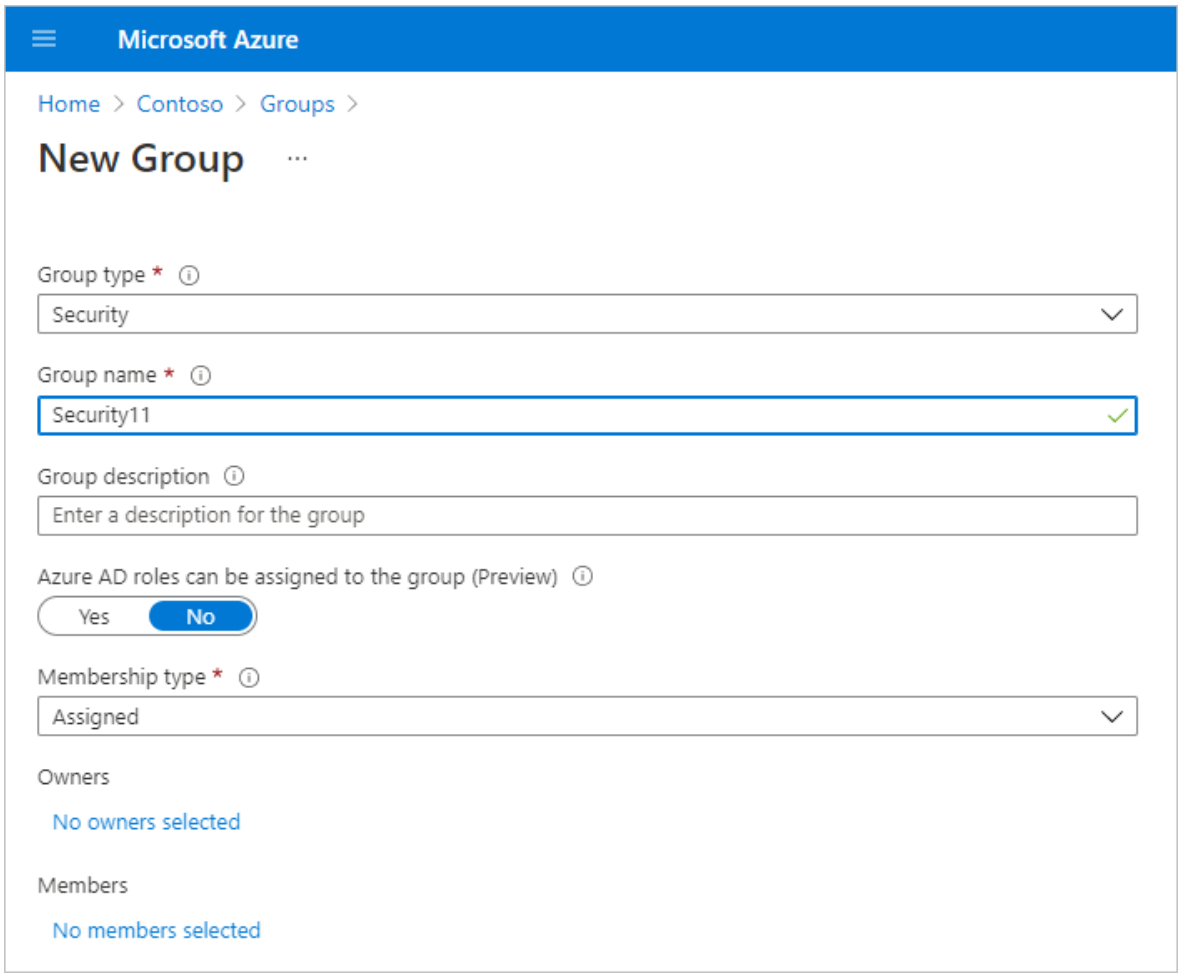
Method

To enable service principal authentication for Power BI read-only APIs, follow these steps:

1. Create an Azure AD app. You can skip this step if you already have an Azure AD app you want to use. Take note of the App-Id for later steps.

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

2. Create a new **Security Group** in Azure Active Directory. Read more about how to create a basic group and add members using Azure Active Directory. You can skip this step if you already have a security group you would like to use. Make sure to select **Security** as the Group type.



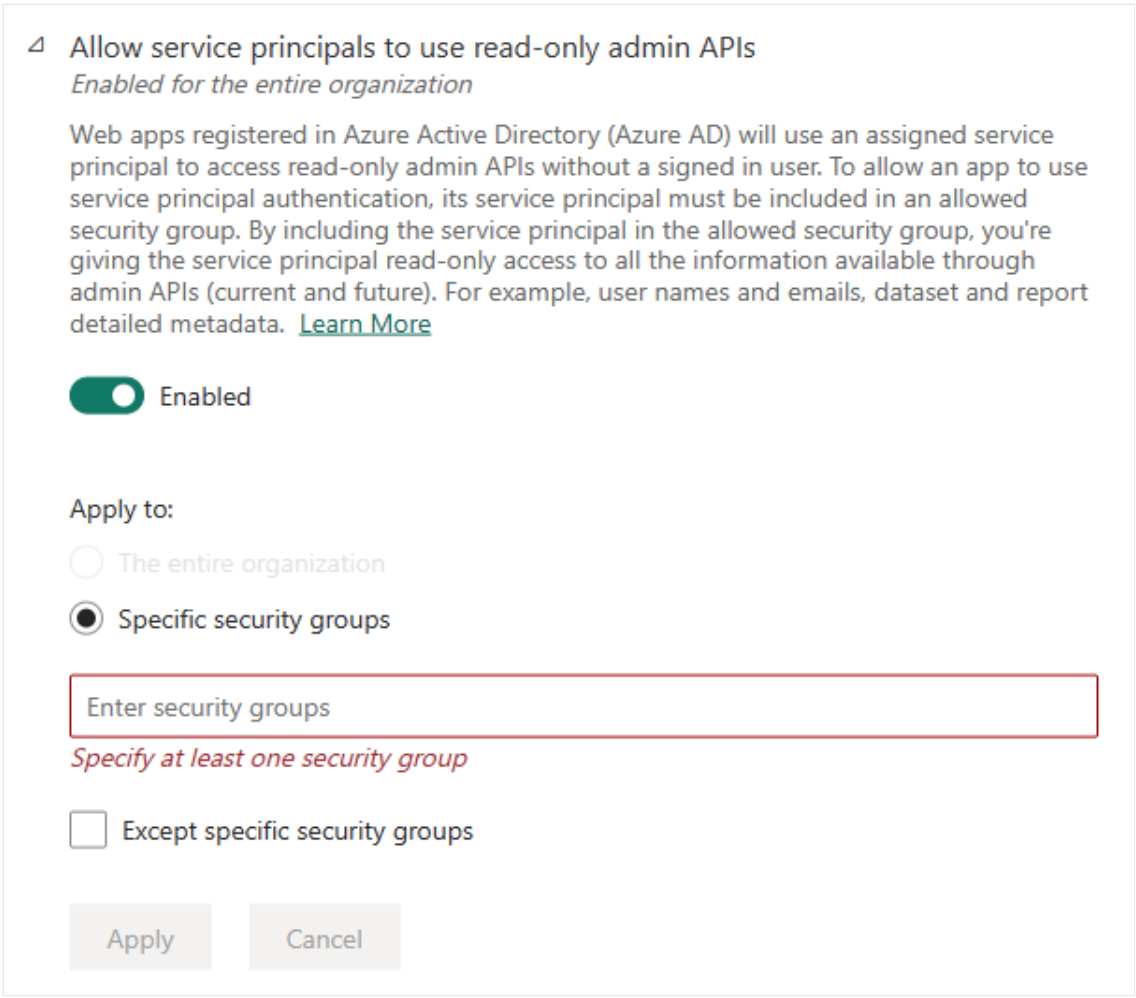
3. Add your App-Id as a member of the security group you created. To do so:
   a. Navigate to **Azure portal** > **Azure Active Directory** > **Groups**, and choose the security group you created in Step 2.
   b. Select **Add Members**.

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

4. Enable the Fabric admin settings:

   a. Log in to the Fabric admin portal. You need to be a Fabric admin to see the tenant settings page.

   b. Under **Admin API settings**, you'll see **Allow service principals to use read-only Power BI admin APIs**. Set the toggle to Enabled, and then select the **Specific security groups** radio button and add the security group you created in Step 2 in the text field that appears below it.



5. Start using the read-only admin APIs. See the list of supported APIs below.

> **ⓘ Important**
>
> 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. **See how to check whether your app has any such permissions**.

Supported APIs

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

- GetGroupsAsAdmin with $expand for dashboards, datasets, 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: [POWER BI?]

1. Sign into the **Azure portal** as a Global Administrator, an Application Administrator, or a Cloud Application Administrator.
2. Select **Azure Active Directory**, then **Enterprise applications**.
3. Select the application you want to grant access to Power BI. [POWER BI?]

4. Select **Permissions**. There must be no admin-consent required permissions of type Application registered for the app.

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.

Next steps

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