Power BI administration

Administer Power BI for your organization.

Get started

GET STARTED

What is Power BI administration

Using the same account for Power BI and Azure

System administration

HOW-TO GUIDE

Manage the Power BI Desktop sign-in form

Add Power BI URLs to your allowlist

Add custom branding to the Power BI service

Find the default region for your organization

Where data is located when Power BI data is shared with your Microsoft 365 services

Monitoring

HOW-TO GUIDE

Track user activities in Power BI

Feature enablement

HOW-TO GUIDE

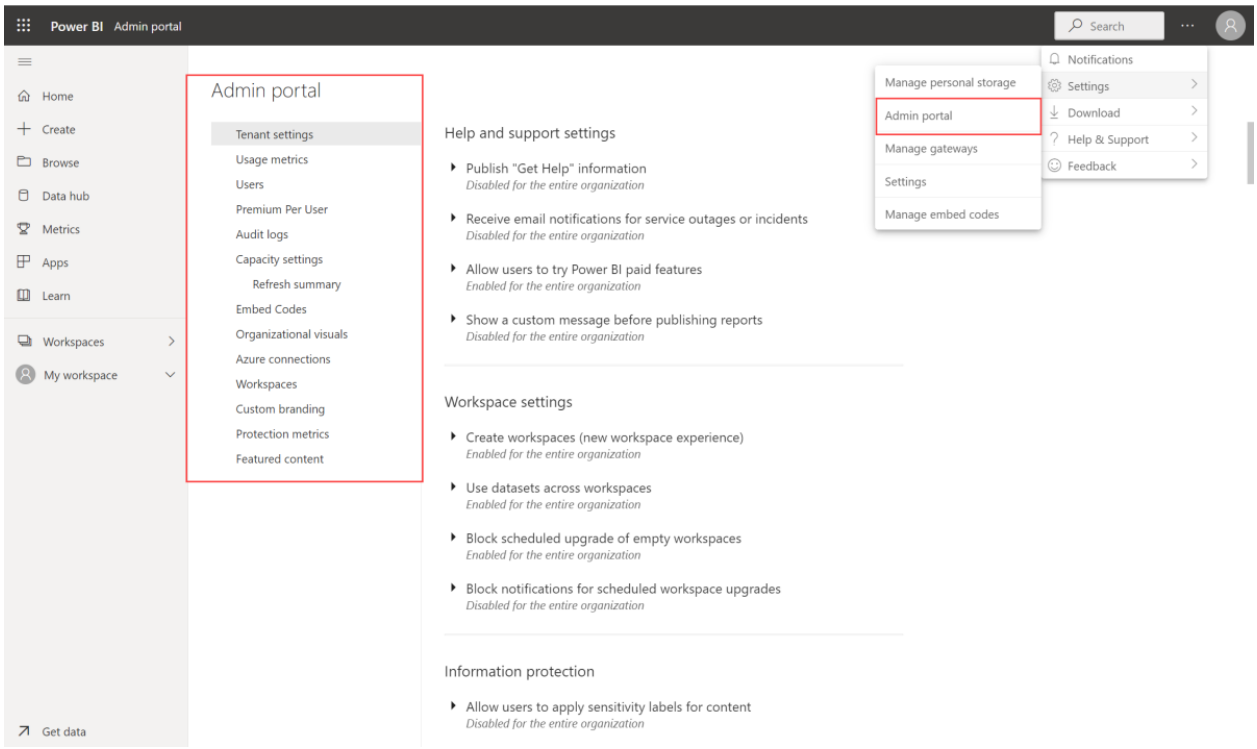
About the admin portal

Manage Power BI visuals admin settings

What is Power BI administration

Article • 11/21/2022 • 2 minutes to read

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



Administrator roles related to Power BI

There are several roles that work together to administer Power BI for your organization. Most admin roles are assigned in the Microsoft 365 admin center or by using PowerShell. The Power BI Premium Capacity and Power BI Embedded 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.

Type of administrator	Administrative scope	Power BI tasks
Global Administrator	Microsoft 365	Has unlimited access to all management features for the organization
		Assigns roles to other users
Billing Administrator	Microsoft 365	Manage subscriptions

Type of administrator	Administrative scope	Power BI tasks
		Purchase licenses
License Administrator	Microsoft 365	Assign or remove licenses for users
User admin	Microsoft 365	Create and manage users and groups
		Reset user passwords
Power Platform Administrator	Power Platform	Full access to Power BI management tasks
		Enable and disable Power BI features
		Report on usage and performance
		Review and manage auditing
Power BI Administrator	Power BI service	Full access to Power BI management tasks
		Enable and disable Power BI features
		Report on usage and performance
		Review and manage auditing
Power BI Premium Capacity Administrator	A single Premium capacity	Assign workspaces to the capacity
		Manage user permission to the capacity
		Manage workloads to configure memory usage
Power BI Embedded Capacity Administrator	A single Embedded capacity	Assign workspaces to the capacity
		Manage user permission to the capacity
		Manage workloads to configure memory usage

Administrative tasks and tools

Power BI admins work mostly in the Power BI Admin portal, but you should still be familiar with related tools and admin centers. Look at the table above to determine which role is required to do tasks using the tools listed here.

Tool	Typical tasks
Power BI Admin portal	Acquire and work with Premium capacity
	Ensure quality of service
	Manage workspaces
	Publish Power BI visuals
	Verify codes used to embed Power BI in other applications
	Troubleshoot data access and other issues
Microsoft 365 admin center	Manage users and groups
	Purchase and assign licenses
	Block users from accessing Power BI
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 Power BI resources
	Provision Power BI Embedded capacity
PowerShell cmdlets	Manage workspaces and other aspects of Power BI through scripts
Administrative APIs and SDK	Build custom admin tools. For example, Power BI Desktop can use these APIs to build reports based on data related to administration.

Next steps

Now that you know the basics of what's involved with Power BI administration, consult these articles to learn more:

- Use the Power BI admin portal
- About tenant settings
- Use PowerShell cmdlets

- Power BI administration FAQ
- Licensing the Power BI service for users in your organization
- Questions? Try asking the Power BI Community
- Suggestions? Contribute ideas to improve Power BI

Understanding Power BI administrator roles

Article • 11/21/2022 • 2 minutes to read

To administer Power BI for your organization, you must be in one of the following roles: Power BI administrator, Power Platform administrator, or global administrator. Microsoft 365 user administrators assign users to the Power BI administrator or Power Platform administrator roles in the Microsoft 365 admin center, or by using a PowerShell script. For more information, see Assign roles to user accounts with PowerShell.

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

> ⓘ **Note**
>
> In the Power BI documentation, *Power BI administrator* refers to users in either the Power BI administrator or Power Platform administrator roles. The documentation makes it clear when the global administrator role is required for a task.

Considerations and limitations

The Power BI administrator and Power Platform administrator roles don't provide the following capabilities:

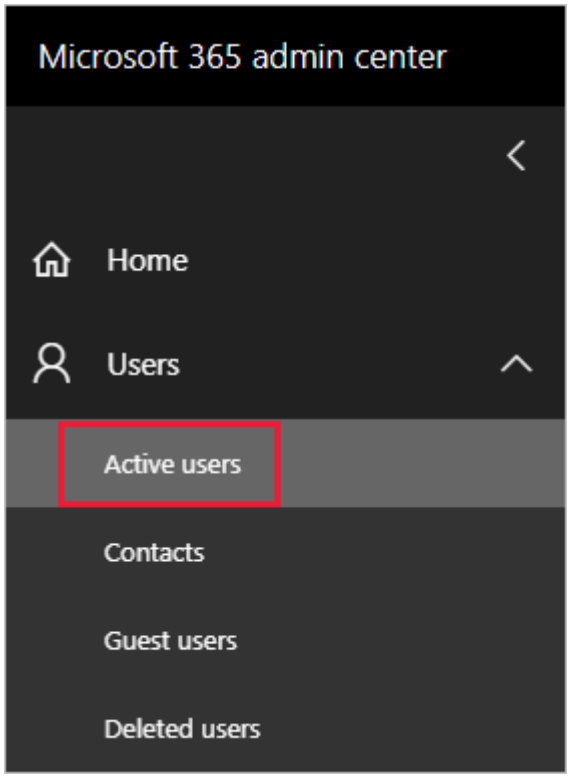
- Ability to modify users and licenses within the Microsoft 365 admin center.
- Access to the audit logs. For more information, see Track user activities in Power BI.

These capabilities require Microsoft 365 admin role assignments.

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

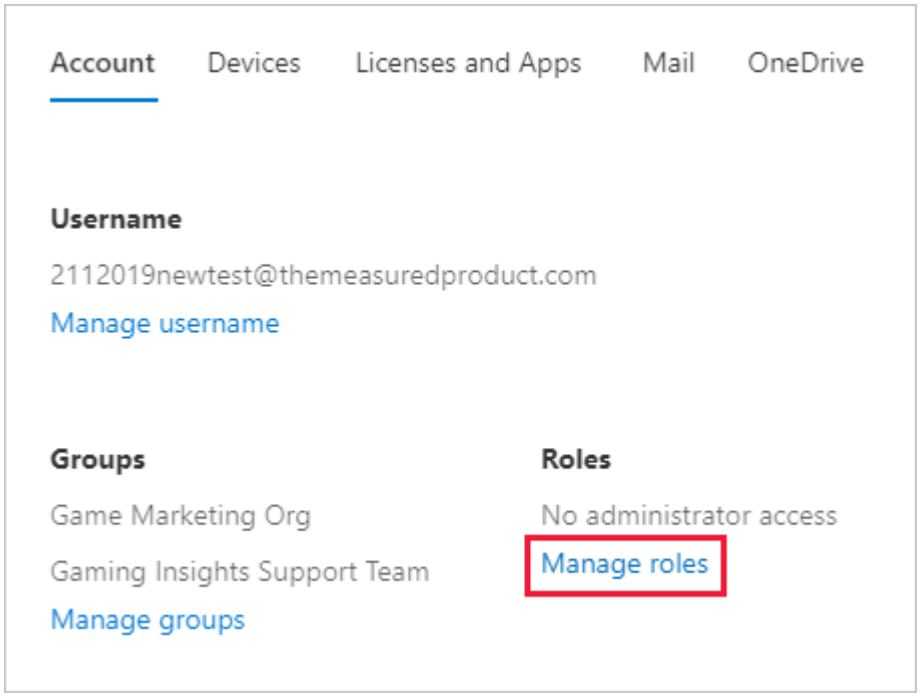
To assign users to an admin role in the Microsoft 365 admin center, follow these steps.

1. In the Microsoft 365 admin center, select **Users** > **Active Users**.

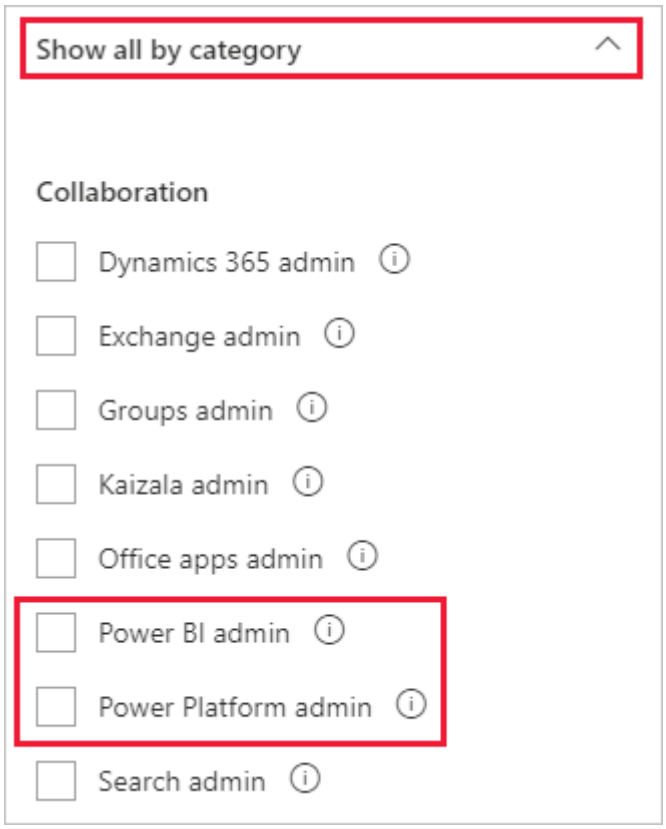


2. Select the user that you want to assign the role to.

3. Under **Roles**, select **Manage roles**.



4. Expand **Show all by category**, then select **Power BI 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 **Power BI administrator** role. You can run Get-AzureADDirectoryRole to get the **ObjectId**.

```
PowerShell

Get-AzureADDirectoryRole
```

```
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

Administering Power BI in your organization
Power BI admin portal

More questions? Try asking the Power BI Community

Using the same account for Power BI and Azure

Article • 12/27/2022 • 2 minutes to read

If you're a user of both Power BI and Azure, you might want to use the same sign-in for both services so that you don't need to type in your password twice.

Power BI signs you in with your organizational account, associated with your work or school email address. Azure signs you in with either a Microsoft Account or your organizational account.

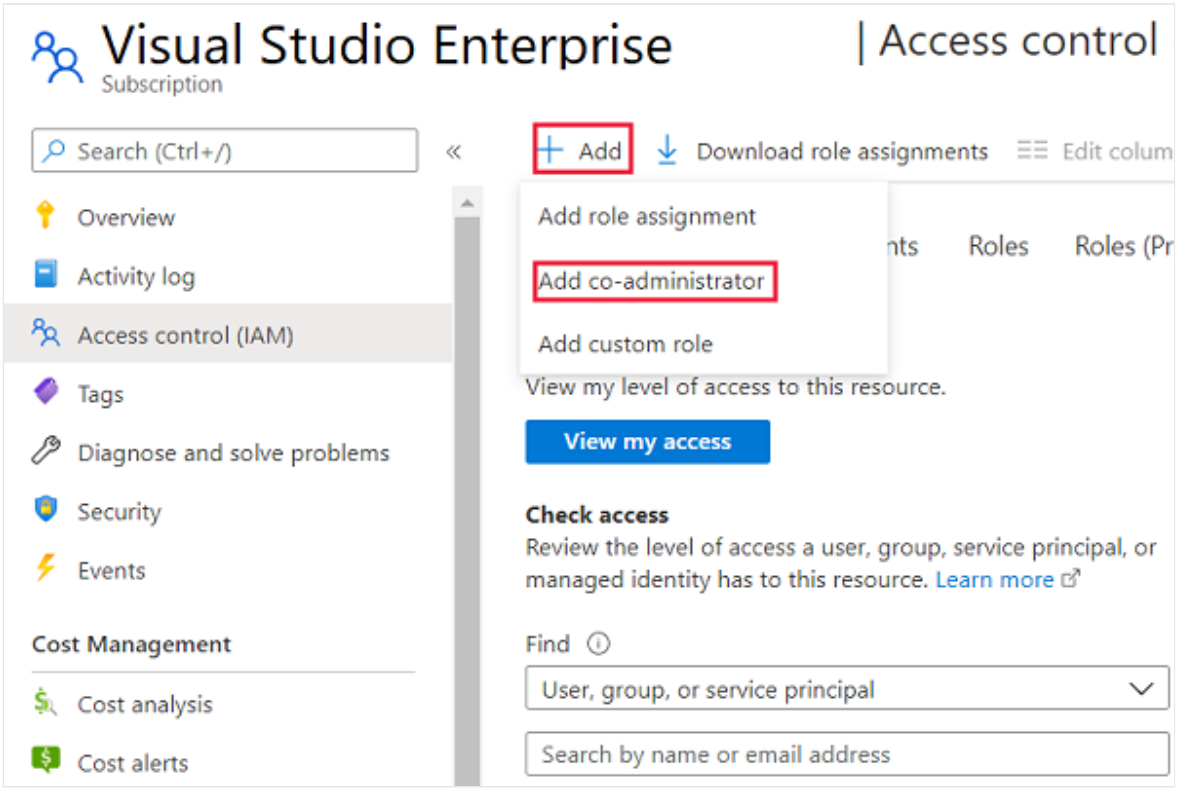
If you want to use the same sign-in for both Azure and Power BI, be sure to sign in to Azure with your organizational account.

What if I already sign in to Azure with my Microsoft Account?

You can add your organizational account as a co-administrator in Azure by following these steps:

1. Sign in to the Azure portal. If you're a user in multiple Azure directories, select **Subscriptions**. Then filter to view only the directory and subscriptions you want to edit.

2. In the nav pane, select **Access control (IAM)**, then choose **Add** > **Add co-administrator**.



3. Enter the email address associated with your organizational account, and select **Add**.

4. Next time you sign in to the Azure portal, use your organizational email address.

More questions? Try the Power BI Community

Administering Power BI - frequently asked questions (FAQ)

FAQ

This article addresses frequently asked questions for Power BI administration. For an overview of the Power BI administration, see What is Power BI administration?.

What's in this article

Sign up for Power BI section

- Using PowerShell
- How do users sign up for Power BI?
- How do individual users in my organization sign up?
- How can I prevent users from joining my existing organization?
- How can I allow users to join my existing organization?
- How do I check if I have the block on in the tenant?
- How can I prevent my existing users from starting to use Power BI?
- How can I allow my existing users to sign up for Power BI?

Administration of Power BI section

- How will this change the way I manage identities for users in my organization today?
- How do we manage Power BI?
- What is the process to manage a tenant created by Microsoft for my users?
- If I have multiple domains, can I control the Microsoft 365 tenant that users get added to?
- How do I remove Power BI for users that already signed up?
- How do I know when new users have joined my tenant?
- Are there any additional things I should prepare for?
- Where is my Power BI tenant located?
- What is the Power BI SLA (Service Level Agreement)?
- How does Power BI handle high availability and failover?

Security in Power BI section

- Does Power BI meet national, regional, and industry-specific compliance requirements?
- How does security work in Power BI?

Sign up for Power BI

Using PowerShell

Some of the procedures in this section require Windows PowerShell scripts. If you're not familiar with PowerShell, the PowerShell getting started guide can introduce you to the tool. To run the scripts, first install the latest 64-bit version of the Azure Active Directory PowerShell for Graph.

How do users sign up for Power BI?

As a Microsoft 365 administrator, you can sign up for Power BI through the Power BI website or the Purchase services page on the Microsoft 365 admin center. When a Microsoft 365 admin signs up for Power BI, they can assign user licenses to users who should have access.

Additionally, individual users in your organization might be able to sign up for Power BI through the Power BI website. When a user in your organization signs up for Power BI, the service automatically assigns a Power BI license. For more information, see Signing up for Power BI as an individual and Power BI licensing in your organization.

How do individual users in my organization sign up?

There are three scenarios that might apply to users in your organization:

- **Scenario 1**: Your organization already has an existing Microsoft 365 environment, and the user signing up for Power BI already has a Microsoft 365 account. In this scenario, if a user already has a work or school account in the tenant (for example, contoso.com) but doesn't yet have Power BI, Microsoft simply activates the Power BI (free) plan for that account. The user is automatically notified with information on how to use the Power BI service.

- **Scenario 2**: Your organization has an existing Microsoft 365 environment, but the user signing up for Power BI doesn’t have a Microsoft 365 account. In this scenario, the user has an email address in your organization’s domain (for example, contoso.com) but doesn't yet have a Microsoft 365 account. In this case, the user

can sign up for Power BI and is automatically given an account. This action lets the user access the Power BI service. For example, if an employee named Nancy uses their work email address (like nancy@contoso.com) to sign up, Microsoft automatically adds Nancy as a user in Contoso's Microsoft 365 environment and activates Power BI for that account.

- **Scenario 3**: Your organization doesn't have a Microsoft 365 environment connected to your email domain. There are no administrative actions required for your organization to take advantage of Power BI. The service adds users to a new, cloud-only user directory. You can also choose to take over as the Microsoft 365 Global admin for the tenant and manage them.

> **Important**
>
> If your organization has multiple email domains and you prefer all email address extensions to be in the same tenant, add all email address domains to an Azure Active Directory tenant before any users sign up. After you've created users, there's no automated mechanism to move users across tenants. For more information on this process, see **If I have multiple domains, can I control the Microsoft 365 tenant that users get added to?** later in this article and **Add a domain to Microsoft 365**.

How can I prevent users from joining my existing Microsoft 365 tenant?

There are steps you can take, as a global administrator, to prevent users from joining your existing Microsoft 365 tenant. If you block access, users' attempts to sign up fail, and a message appears that directs them to contact their organization's admin. You don't need to repeat this process if you have already disabled automatic license distribution (for example, through Office 365 Education for students, faculty, and staff).

Use the following PowerShell script to prevent new users from joining a managed tenant. For more information, see What is PowerShell?

PowerShell

```
$msolcred = get-credential
connect-msolservice -credential $msolcred

Set-MsolCompanySettings -AllowEmailVerifiedUsers $false
```

> **Note**
>
> Blocking access prevents new users in your organization from signing up for Power BI. Users that sign up for Power BI prior to disabling new signups for your organization still retain their licenses. To remove a user, see **How do I remove Power BI for users that already signed up?** later in this article.

How can I allow users to join my existing Microsoft 365 tenant?

Use the following PowerShell script to let new users join a managed tenant. (Learn more about PowerShell.)

```PowerShell
$msolcred = get-credential
connect-msolservice -credential $msolcred

Set-MsolCompanySettings -AllowEmailVerifiedUsers $true
```

How do I check if I have the block on in the tenant?

Use the following PowerShell script to check settings. *AllowEmailVerifiedUsers* should be false. (Learn more about PowerShell.)

```PowerShell
$msolcred = get-credential
connect-msolservice -credential $msolcred

Get-MsolCompanyInformation | fl allow*
```

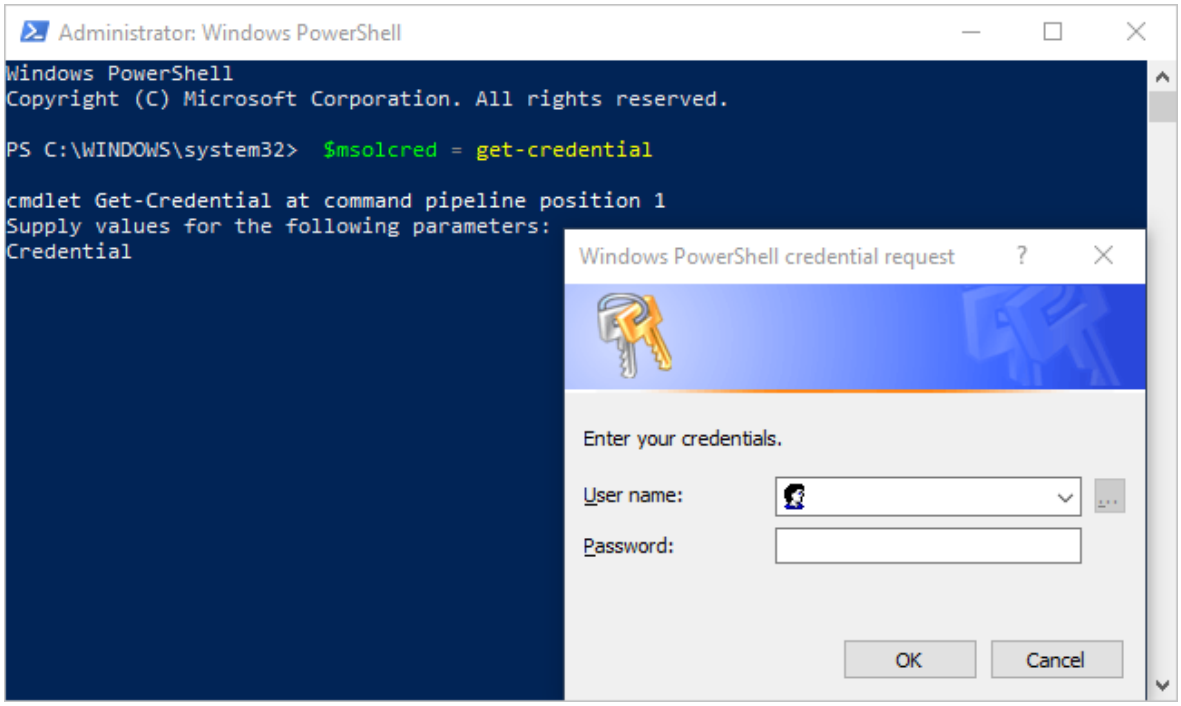
How can I prevent my existing users from starting to use Power BI?

The Azure AD setting that controls this is **AllowAdHocSubscriptions**. Most tenants have this set to *true*, which means it's enabled. If you acquired Power BI through a partner, this might be set to *false*, which means it's disabled.

Use the following PowerShell script to disable ad hoc subscriptions. For more information, see What is PowerShell?

1. Sign into Azure Active Directory by using your Microsoft 365 credentials. The first line of the following PowerShell script prompts you for your credentials. The second line connects to Azure Active Directory.

```powershell
$msolcred = get-credential
connect-msolservice -credential $msolcred
```



2. After you sign in, run the following command to see how your tenant is currently set up.

```powershell
Get-MsolCompanyInformation | fl AllowAdHocSubscriptions
```

3. Run the following command to enable (`$true`) or disable (`$false`) **AllowAdHocSubscriptions**.

```powershell
Set-MsolCompanySettings -AllowAdHocSubscriptions $false
```

> **Note**

Use the **AllowAdHocSubscriptions** flag to control several user capabilities in your organization, including the ability for users to sign up for the Azure Rights Management Service. Changing this flag affects all of these capabilities. With a setting of *false*, users can still sign up for an individual Power BI Pro trial.

How can I allow my existing users to sign up for Power BI?

To allow your existing users to sign up for Power BI, run the command listed for the previous question, but pass `$true` instead of `$false` in the last step.

Administration of Power BI

How will this change the way I manage identities for users in my organization today?

There are three scenarios that might apply to users in your organization:

- **Scenario 1**: If your organization already has an existing Microsoft 365 environment and all users in your organization have Microsoft 365 accounts, there's no change in how you manage identities.
- **Scenario 2**: If your organization already has an existing Microsoft 365 environment but not all users in your organization have Microsoft 365 accounts, we create a user in the tenant and assign licenses based on the user's work or school email address.

  As a result, the number of users you're managing at any particular time grows as users in your organization sign up for the service.
- **Scenario 3**: If your organization doesn't have a Microsoft 365 environment connected to your email domain, there's no change in how you manage identities.

  The service adds users to a new, cloud-only user directory that you can choose to take over as the Microsoft 365 Global admin and manage them.

How do we manage Power BI?

Power BI provides a Power BI admin portal for users in the Microsoft 365 Global Administrator role and users in the Power BI Service administrator role. To use the Power

BI admin portal, you must mark your account as a **Global Administrator** within Microsoft 365 or Azure Active Directory, or someone must assign the Power BI service administrator role to your user account. For more information, see Understanding the Power BI administrator role and Power BI Admin Portal. The portal provides the ability to control tenant-wide settings, view Power BI usage statistics and a link to the Microsoft 365 admin center to manage users and groups.

What is the process to manage a tenant created by Microsoft for my users?

When a self-service user signs up for a cloud service that uses Azure AD, the service adds them to an unmanaged Azure AD directory based on their email domain. You can claim and manage a tenant that someone created by using a process known as *admin takeover*. For more information, see Take over an unmanaged directory as administrator in Azure Active Directory. The type of takeover you do depends on whether there's an existing managed tenant associated with your domain:

- Power BI supports internal admin takeover. When you perform an *internal* admin takeover of an unmanaged Azure directory, you're added as the global administrator of the unmanaged directory. No users, domains, or service plans are migrated to any other directory you administer.
- Power BI no longer supports external admin takeover. When you perform an *external* admin takeover of an unmanaged Azure directory, you add the DNS domain name of the unmanaged directory to your managed Azure directory. External takeover will result in a loss of access to all Power BI content on the original unmanaged tenant. Power BI reports will need to be republished to the new tenant and Power BI dashboards and apps will need to be recreated in the new tenant.

If I have multiple domains, can I control the Microsoft 365 tenant that users get added to?

If you do nothing, the service creates a tenant for each user email domain and subdomain. If you want all users to be in the same tenant regardless of their email address extensions, create a target tenant ahead of time or use an existing tenant. Next, add all the existing domains and subdomains that you want consolidated within that tenant. Every user with email addresses ending in those domains and subdomains automatically join the target tenant when they sign up.

> **Important**
>
> After you've created users, there's no supported automated mechanism to move users across tenants. To learn about adding domains to a single Microsoft 365 tenant, see **Add your users and domain to Microsoft 365**.

How do I remove Power BI for users that already signed up?

If a user is signed up for Power BI, but you no longer want them to have access to Power BI, you can remove the Power BI license for that user.

1. Go to the Microsoft 365 admin center.
2. In the nav pane, select **Users** > **Active Users**.
3. Find the user you want to remove the license for, then select their name.

   You can perform bulk license management to users as well. To do that, select multiple users and select **Edit product licenses**.
4. On the user details page, next to **Product licenses**, select **Edit**.
5. Depending on what license you applied to their account, set **Power BI (free)** or **Power BI Pro** to **Off**.
6. Select **Save**.

How do I know when new users have joined my tenant?

Users who have joined your tenant via self-service sign-up get assigned a unique license that you can filter on within your active user pane in the admin dashboard. To create this new view, follow these steps.

1. Navigate to the Microsoft 365 admin center.
2. In the nav pane, select **Users** > **Active Users**.
3. On the **Views** menu, select **Add custom view**.
4. Name your new view, and under **Assigned product license**, select **Power BI (free)** or **Power BI Pro**.

You can only have one license selected per view. If you have both **Power BI (free)** and **Power BI Pro** licenses in your organization, you can create two views.

5. Enter any other conditions you want, then select **Add**.

6. After you create the new view, it's available from the **Views** menu.

Are there any additional things I should prepare for?

You might experience an increase in password reset requests. For information about this process, see Reset passwords in Microsoft 365 for business.

You can remove a user from your tenant via the standard process in the Microsoft 365 admin center. However, if the user still has an active email address from your organization, they can rejoin unless you block all users from joining.

Where is my Power BI tenant located?

For information about which data region your Power BI tenant is in, see Find the default region for your organization.

What is the Power BI SLA?

For information about the Power BI SLA (Service Level Agreement), see the Licensing Terms and Documentation article in the **Licensing** section of the Microsoft Licensing website.

How does Power BI handle high availability and failover?

For information about high availability and failover, see Power BI high availability, failover, and disaster recovery FAQ.

Security in Power BI

Does Power BI meet national, regional, and industry-specific compliance requirements?

To learn more about Power BI compliance, see the Microsoft Trust Center.

How does security work in Power BI?

Microsoft built Power BI on the foundation of Microsoft 365, which in turn builds on Azure services like Azure Active Directory. For an overview of Power BI architecture, see Power BI Security.

Next steps

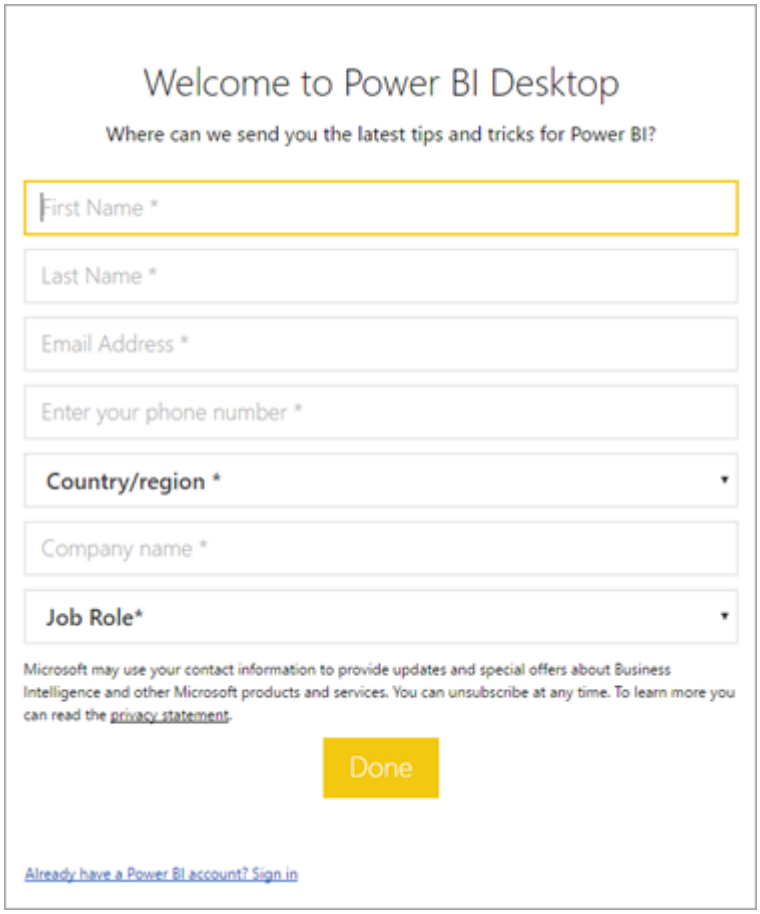
- About the admin portal
- Understanding Power BI administrator roles
- Sign up for or purchase the Power BI service as an individual
- Purchase and assign Power BI Pro user licenses
- What is Power BI Premium?
- How to purchase Power BI Premium
- Power BI Premium whitepaper
- Work or school account management
- Microsoft 365 group management

More questions? Try asking the Power BI Community

Administrators: Manage the Power BI Desktop sign-in form

Article • 01/06/2023 • 2 minutes to read

The first time Power BI Desktop is launched, a sign-in form is displayed. Information can be filled in, or sign in to Power BI to continue. Administrators manage this form by using a registry key.



Administrators use the following registry key to disable the sign-in form. This change can also be pushed to an entire organization by using global policies.

Console

```
Key: HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Microsoft Power BI
Desktop
valueName: ShowLeadGenDialog
```

You can also try the following key, which has been successful for some customers based on their configurations:

Console

```
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Microsoft Power BI Desktop
valueName: ShowLeadGenDialog
```

A value of 0 will disable the dialog.

More questions? Try asking the Power BI Community

Manage Power BI visuals admin settings

Article • 12/20/2022 • 8 minutes to read

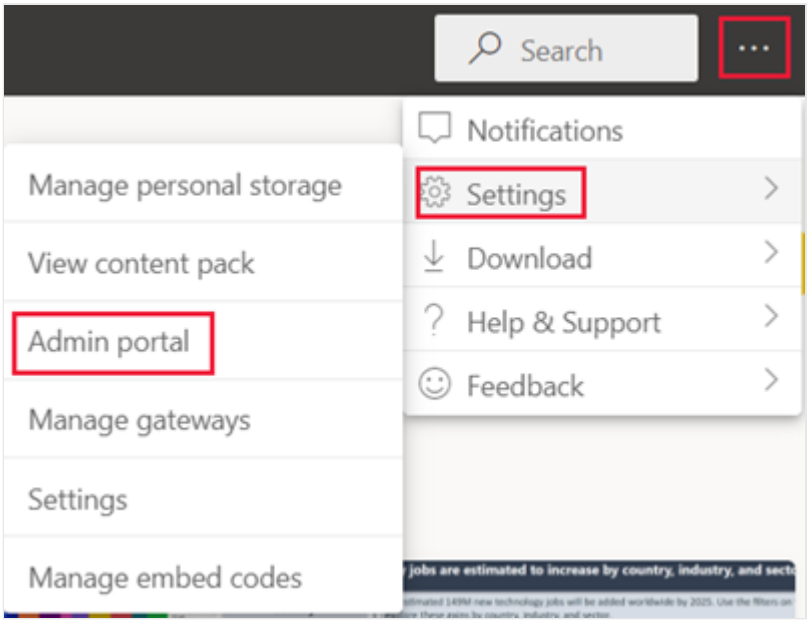
As a Power BI administrator for your organization, you can control the type of Power BI visuals users can access across the organization and limit the actions users can perform.

To manage Power BI visuals, you must be a Global Administrator in Office 365, or have been assigned the Power BI service administrator role. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles.

Access the Power BI admin portal settings

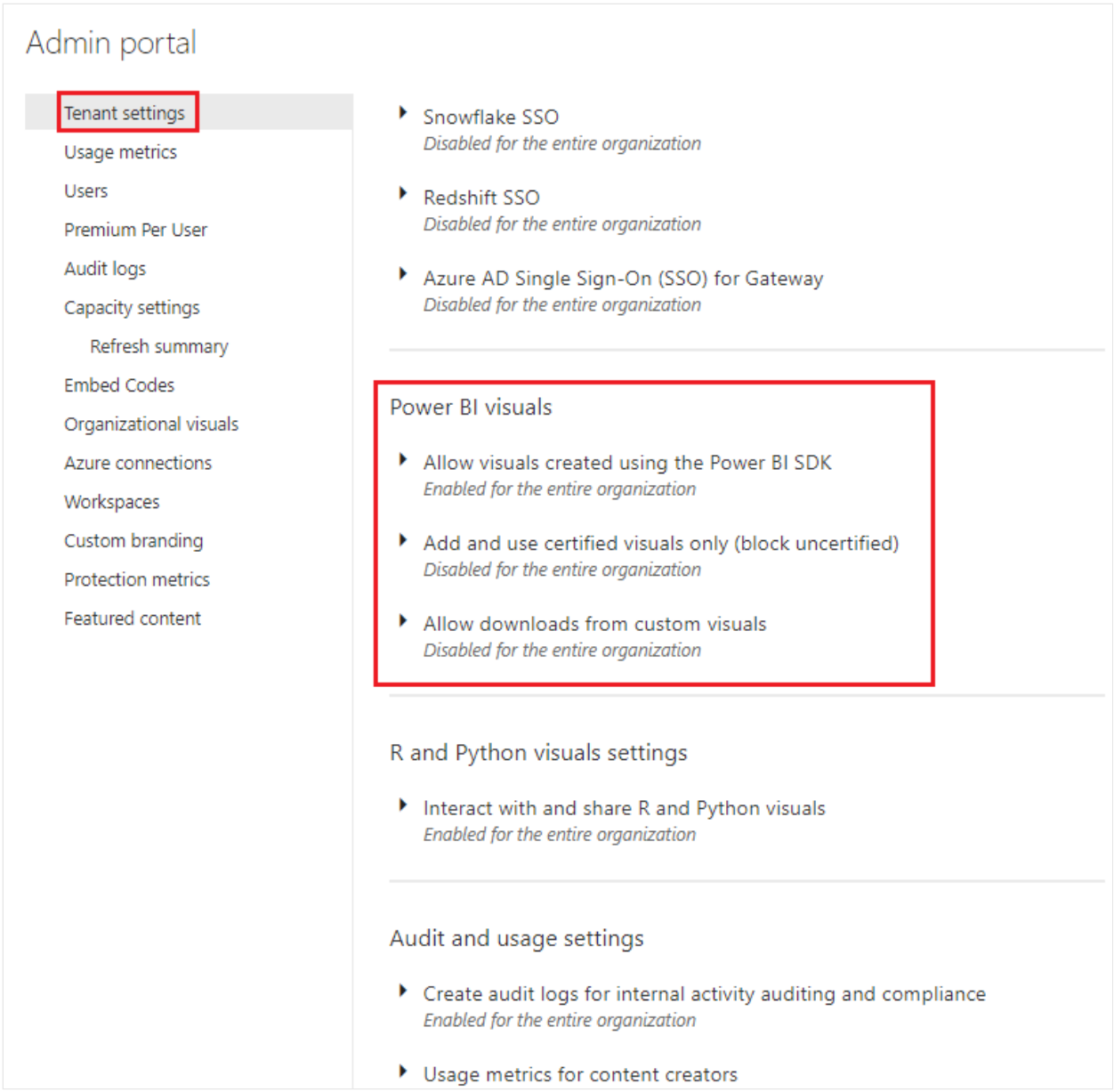
You have to be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI by using your admin account credentials.
2. From the page header, select ... > **Settings** > **Admin portal**.



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 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.

> ⓘ **Note**
>
> Changes to tenant settings do not affect Power BI visuals listed in the **organizational visuals** tab.

Visuals from AppSource or a file

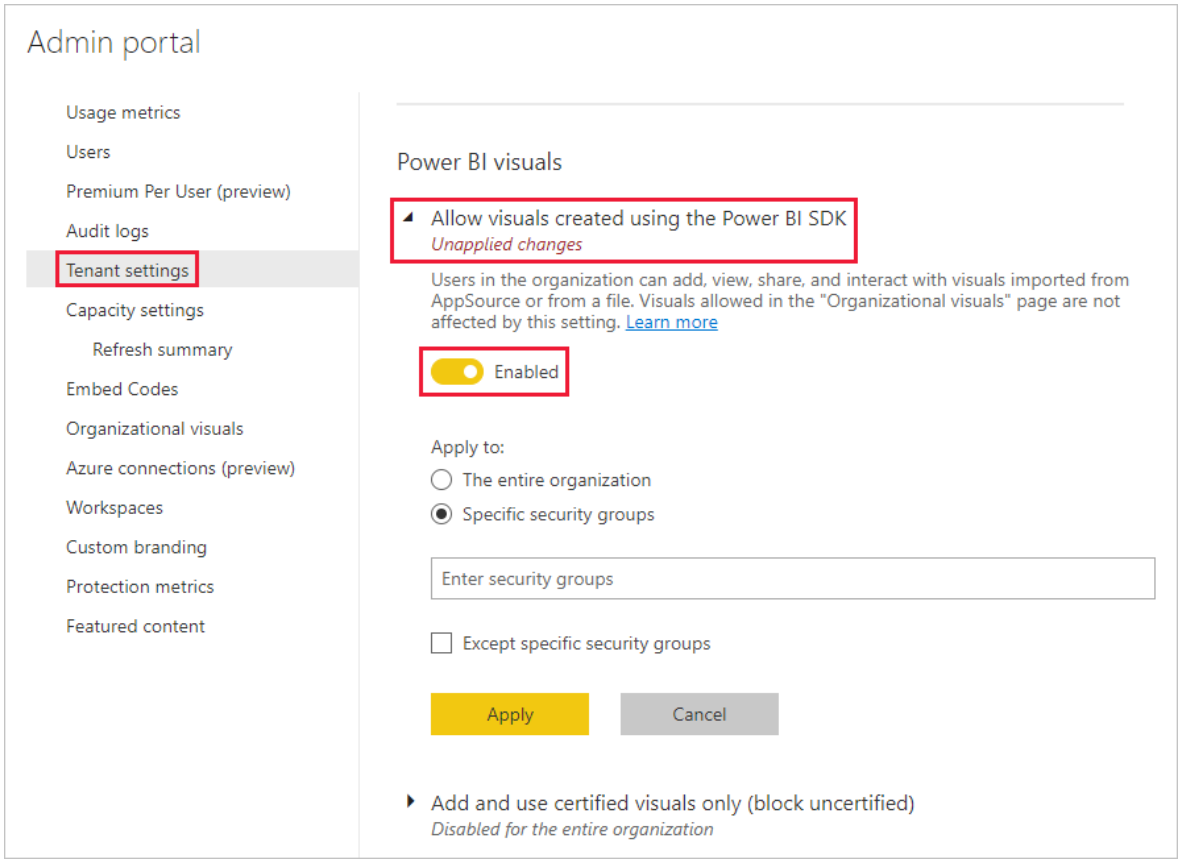
Manage organizational access for the following type of Power BI visuals:

- Custom visuals developers create by using the Power BI SDK and saved as a *.pbiviz* file.

- Visuals downloaded from AppSource.

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 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 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 Azure AD Group Policy.

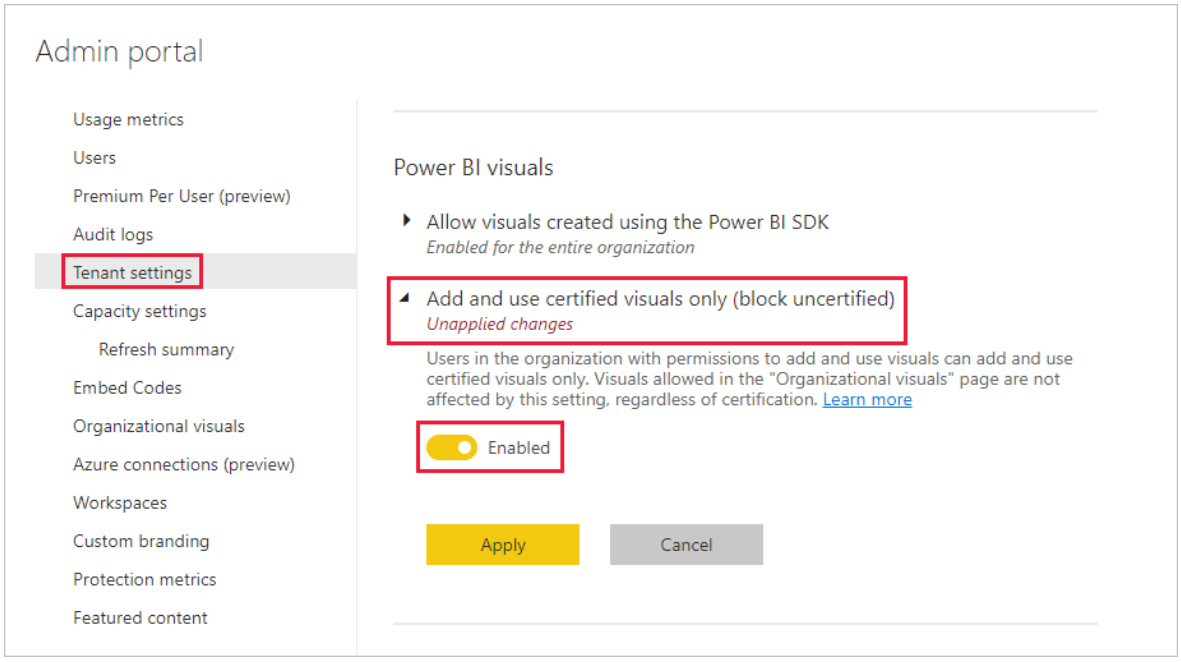
Key	Value name	Value
Software\Policies\Microsoft\Power BI Desktop\	EnableCustomVisuals	0 - Disable 1 - Enable (default)

Certified Power BI visuals

Certified Power BI visuals are visuals that meet the Microsoft Power BI team code requirements. They're tested to verify that they don't access external services or resources and that they follow secure coding patterns and guidelines.

When this setting is enabled, only certified Power BI visuals will render in your organization's reports and dashboards. Power BI visuals from AppSource or files that aren't certified will return an error message.

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

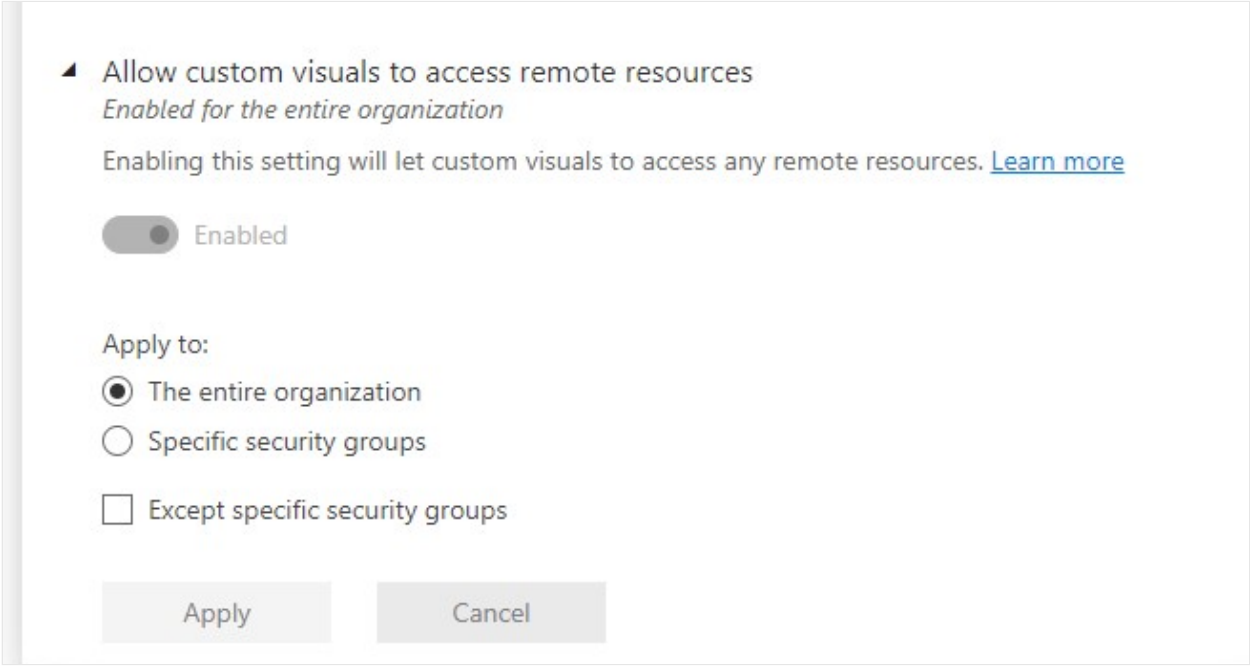


UI changes to tenant settings apply only to Power BI service. To manage the certified visuals tenant setting in Power BI Desktop, use Azure AD Group Policy.

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

Allow access to remote resources

When this setting is enabled, all visuals created with an API earlier than v4.6.0 will be able to access remote resources. Visuals created with API v4.6.0 and following versions will be able to access remote resources only if the visual's privileges setting allows it. If the visual's privileges setting doesn't allow access to remote resources, that visual won't be allowed access even if this admin setting is enabled.

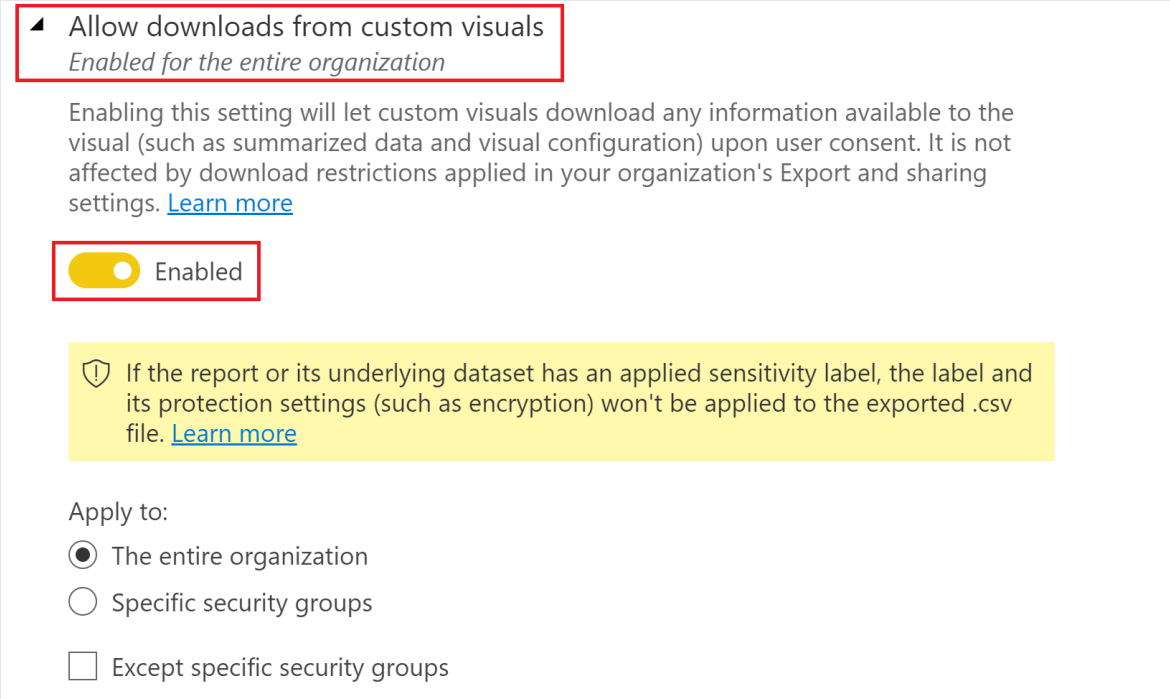


Export data to file

When this setting is enabled, 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.

> **Note**
>
> When this setting is enabled, 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 Power BI service. To enable users in your organization to download data from custom visuals in Power BI Desktop, use Azure AD Group Policy.

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 logged on.

Organizational visuals

As a Power BI 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 will 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 are automatically deployed to Power BI Desktop.

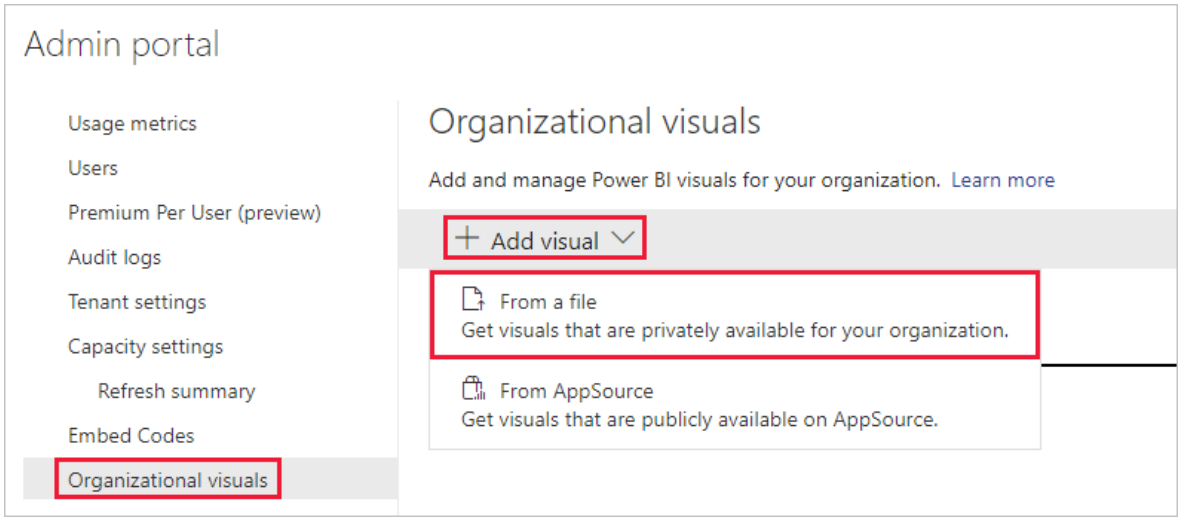
> ⓘ **Note**
>
> Organizational visuals are not supported in Power BI Report Server.

Add a visual from a file

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

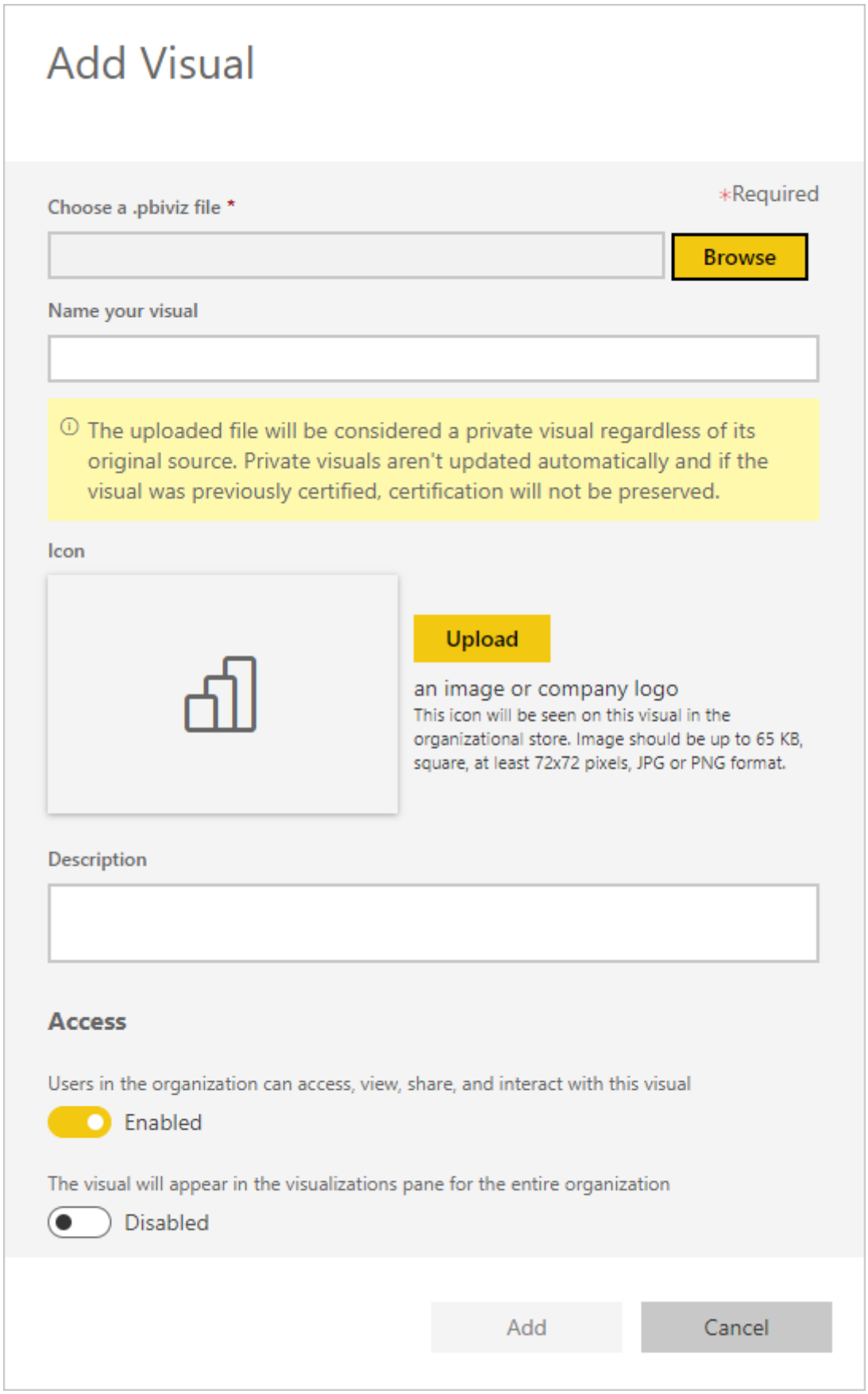
> ⚠ **Warning**
>
> A Power BI visual uploaded from a file could contain code with security or privacy risks. Make sure you trust the author and the source of the visual before deploying to the organization's repository.

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 be displayed in the visualization pane.
- **Description** - Provide a short description of the visual to give more context for the user.
- **Access** - This section has two options:
    - Select whether users in your organization can access this visual. This setting is enabled by default.
    - Select whether this visual will appear in the visualization pane of the users in your organization. This setting is disabled by default. For more information, see add a visual to the visualization pane.



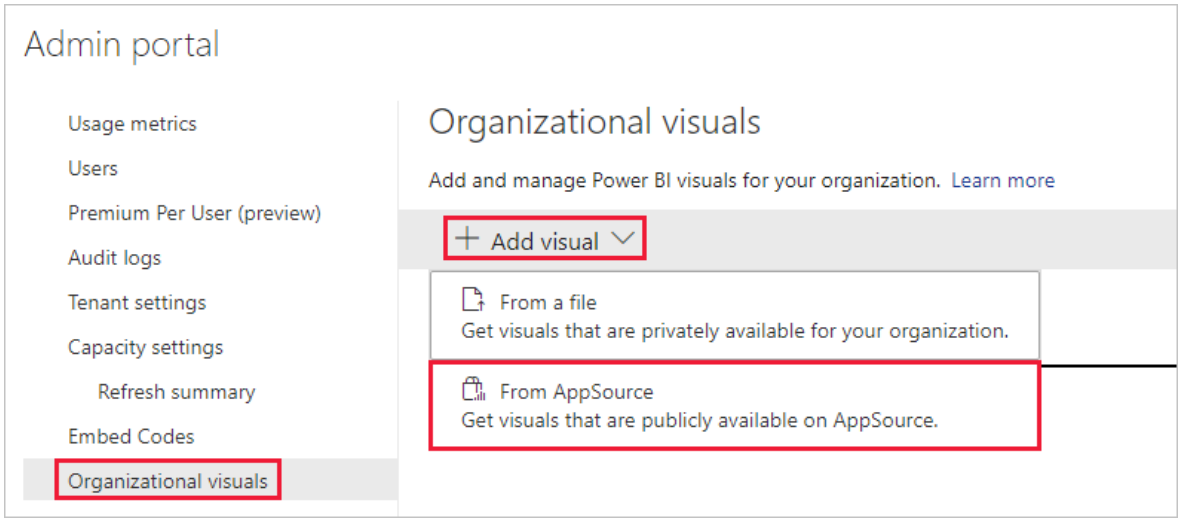
3. To initiate the upload request, select **Add**. After it's uploaded, the visual will display in the organizational visuals list.

Add a visual from AppSource

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

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

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

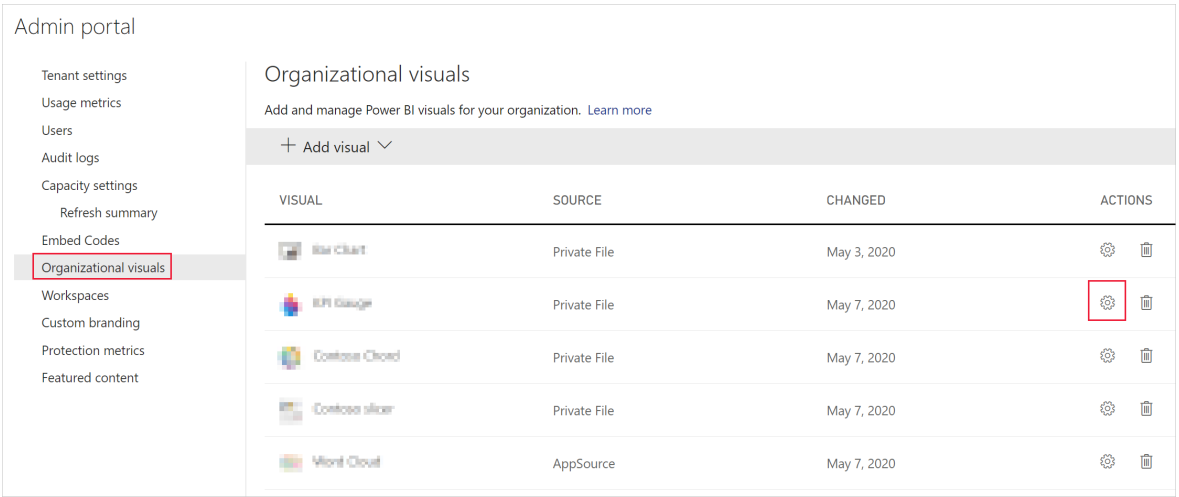


2. In the **Power BI visuals** window, find the AppSource visual you want to add, and select **Add**. After it's uploaded, the visual will display in the organizational visuals list.

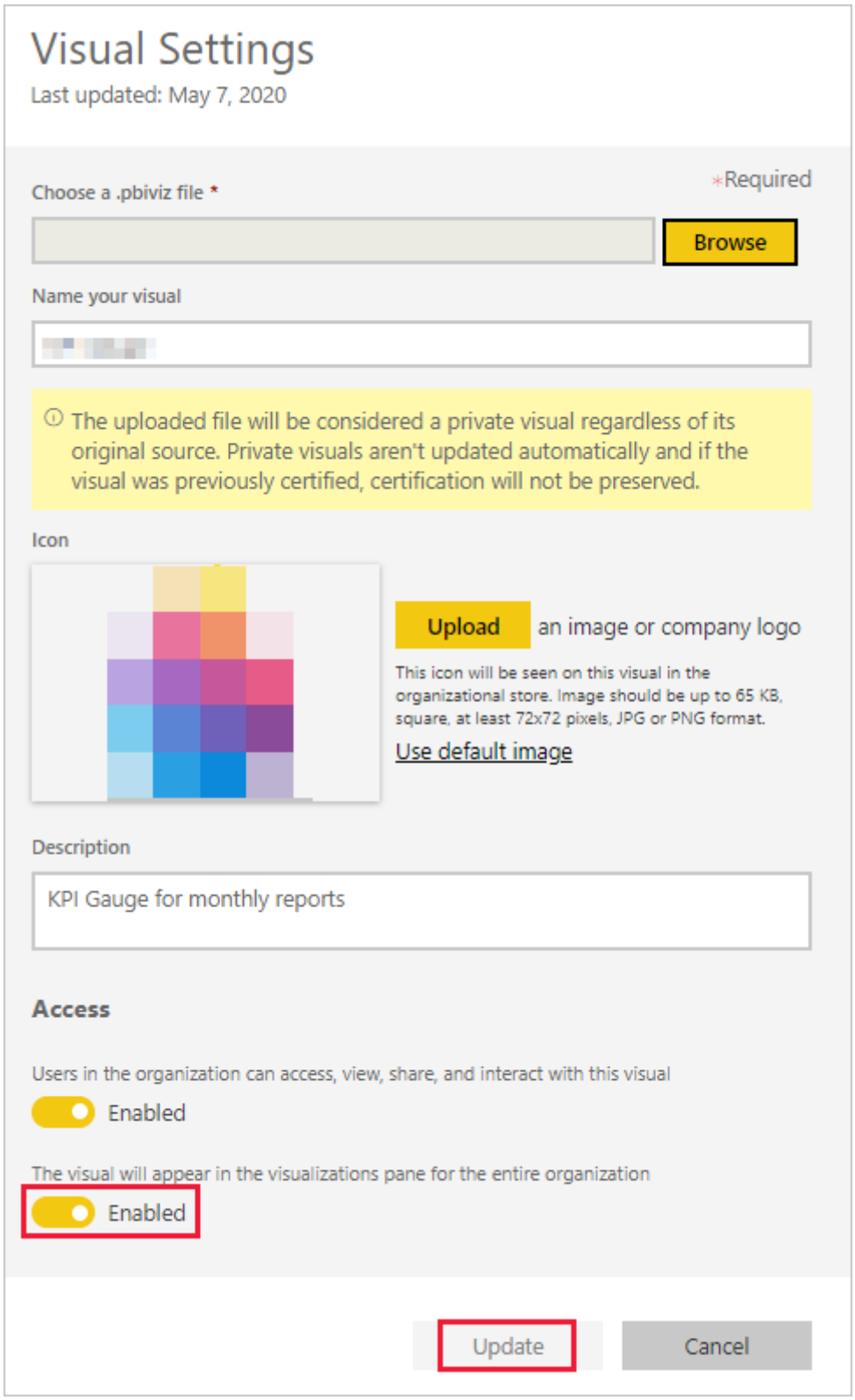
Add a visual to the visualization pane

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

1. In the row of the visual you want to add, select **settings**.



2. Enable the visualization pane setting and select **Update**.



Delete a visual uploaded from a file

To permanently delete a visual, select the trash bin icon for the visual in the repository.

> **ⓘ 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 won'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. In the row of the *.pbiviz* visual you want to disable, 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 won'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've been disabled.

Update a visual

AppSource visuals are updated automatically. After a new version is available from AppSource, it will replace an older version deployed via the organizational visuals list.

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

1. In the row of the visual you want to add, select **settings**.
2. Select **Browse**, and select the *.pbiviz* you want to replace the current visual with.
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 was uploaded from a file.

Next steps

Administering Power BI in the admin portal

Visuals in Power BI

Organizational visuals in Power BI

Add Power BI URLs to your allowlist

Article • 01/02/2023 • 3 minutes to read

The Power BI service requires connectivity to the internet. The endpoints listed in the tables in this article should be reachable for customers who use the Power BI service.

To use the Power BI service, you must be able to connect to the endpoints marked **required** in the tables in this article, and to any endpoints marked **required** on the linked sites. If the link to an external site refers to a specific section, you only need to review the endpoints in that section.

You can also add endpoints that are marked **optional** to allowlists for specific functionality to work.

The Power BI service requires only TCP Port 443 to be opened for the listed endpoints.

Wildcards (*) represent all levels under the root domain. N/A is used when information isn't available. The **Destination(s)** column lists domain names and links to external sites, which contain further endpoint information.

> **ⓘ Important**
>
> The information in this article doesn't apply to Power BI China operated by 21Vianet or Power BI for US government. Read **Connect government and global Azure cloud services** to learn more about communicating between cloud services.

Authentication

Power BI depends on the required endpoints in the Microsoft 365 authentication and identity sections. To use Power BI, you must be able to connect to the endpoints in the following linked site.

Row	Purpose	Destination(s)	Port(s)
1	**Required:** Authentication and identity	See the documentation for Microsoft 365 Common and Office Online URLs	N/A

General site usage

For the general use of Power BI, you must be able to connect to the endpoints and linked sites in the following table.

Row	Purpose	Destination(s)	Port(s)
1	**Required:** Backend APIs	api.powerbi.com	TCP 443
2	**Required:** Backend APIs	*.analysis.windows.net	TCP 443
3	**Required:** Backend APIs	*.pbidedicated.windows.net	TCP 443
4	**Required:** Content Delivery Network (CDN)	content.powerapps.com	TCP 443
5	**Required:** Microsoft 365 integration	See the documentation for Microsoft 365 Common and Office Online URLs	N/A
6	**Required:** Portal	*.powerbi.com	TCP 443
7	**Required:** Service telemetry	dc.services.visualstudio.com	TCP 443
8	**Optional:** Informational messages	arc.msn.com	TCP 443
9	**Optional:** NPS surveys	nps.onyx.azure.net	TCP 443

Administration

To perform administrative functions in Power BI, you must be able to connect to the endpoints in the following linked sites.

Row	Purpose	Destination(s)	Port(s)
1	**Required:** For managing users and viewing audit logs	See the documentation for Microsoft 365 Common and Office Online URLs	N/A

Getting data

To get data from specific data sources, such as OneDrive, you must be able to connect to the endpoints in the following table. Access to additional internet domains and URLs might be required for specific data sources that your organization uses.

Row	Purpose	Destination(s)	Port(s)
1	**Required:** AppSource (internal or external apps in Power BI)	appsource.microsoft.com *.s-microsoft.com	TCP 443
2	**Optional:** Import files From OneDrive personal	See the Required URLs and ports for OneDrive site	N/A
3	**Optional:** Power BI in 60-Seconds tutorial video	*.doubleclick.net *.ggpht.com *.google.com *.googlevideo.com *.youtube.com *.ytimg.com fonts.gstatic.com	TCP 443
4	**Optional:** PubNub streaming data sources	See the PubNub documentation	N/A

Dashboard and report integration

Power BI depends on certain endpoints to support your dashboards and reports. You must be able to connect to the endpoints and linked sites in the following table.

Row	Purpose	Destination(s)	Port(s)
1	**Required:** Excel integration	See the documentation for Microsoft 365 Common and Office Online URLs	N/A

Power BI visuals

Power BI depends on certain endpoints to view and access Power BI visuals. You must be able to connect to the endpoints and linked sites in the following table.

Row	Purpose	Destination(s)	Port(s)

Row	Purpose	Destination(s)	Port(s)
1	**Required:** Import a custom visual from the Marketplace interface or from a file	*.osi.office.net *.msecnd.net store.office.com web.vortex.data.microsoft.com store-images.s-microsoft.com	TCP 443
2	**Optional:** Bing Maps	bing.com platform.bing.com r.bing.com *.virtualearth.net	TCP 443
3	**Optional:** PowerApps	See the Required services section from the PowerApps system requirements site	N/A
4	**Optional:** Visio	See the documentation for Microsoft 365 Common and Office Online URLs, as well as SharePoint Online and OneDrive for Business	N/A

Related external sites

Power BI links to other related sites. These sites host documentation, support, new feature requests, and more. Access to these sites doesn't affect the functionality of Power BI, so adding them to allowlists is optional.

Row	Purpose	Destination(s)	Port(s)
1	**Optional:** Community site	community.powerbi.com oxcrx34285.i.lithium.com	TCP 443
2	**Optional:** Documentation site	learn.microsoft.com img-prod-cms-rt-microsoft-com.akamaized.net statics-uhf-eas.akamaized.net cdnssl.clicktale.net ing-district.clicktale.net	TCP 443
3	**Optional:** Download site (for Power BI Desktop and other products)	download.microsoft.com	TCP 443
4	**Optional:** External redirects	aka.ms go.microsoft.com	TCP 443

Row	Purpose	Destination(s)	Port(s)
5	**Optional:** Ideas feedback site	ideas.powerbi.com powerbi.uservoice.com	TCP 443
6	**Optional:** Power BI site - landing page, learn more links, support site, download links, partner showcase, and so on.	powerbi.microsoft.com	TCP 443
7	**Optional:** Power BI Developer Center	dev.powerbi.com	TCP 443
8	**Optional:** Support site	support.powerbi.com s3.amazonaws.com *.olark.com logx.optimizely.com mscom.demdex.net tags.tiqcdn.com	TCP 443

Share data with your Microsoft 365 services

Article • 10/21/2022 • 3 minutes to read

APPLIES TO: ✗ Power BI Desktop ✓ Power BI service

This article is aimed at Power BI administrators and decision makers who need to know how and where Power BI metadata is being used.

Power BI metadata sharing with Microsoft 365 services is a feature that allows metadata from Power BI 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 disabled by default.

When shared with Microsoft 365 services, Power BI content will be listed in the Most Recently Viewed list on the Office.com home page. The Power BI content affected includes reports, dashboards, apps, workbooks, paginated reports, and workspaces. The information required by the Most Recently Viewed functionality includes:

- The display name of the content
- When the content was last accessed
- The type of content that was accessed (report, dashboard etc.)

See the complete list of Power BI metadata that is shared with Microsoft 365 services.

How to turn on sharing with Microsoft 365 services

To enable sharing Power BI metadata with Microsoft 365 services, a Power BI administrator must turn on the **Share data with your Microsoft 365 services** tenant setting. Before turning on the experience, the administrator should review the list of data that will be shared with Microsoft 365.

Data residency

If Power BI and your Microsoft 365 services are in different geographic regions, information may flow outside the region it's stored in. By enabling this setting, the Power BI administrator explicitly opts in to this feature, and acknowledges enabling these cross-service capabilities may result in Power BI metadata flowing outside the

geographic region it's stored in. For more information, see Where data is located when Power BI data is shared with your Microsoft 365 services.

References:

- Where is my Power BI tenant located?
- Microsoft Privacy - Where is Your Data Located
- Where data is located when Power BI data is shared with your Microsoft 365 services

Data that will be shared with Microsoft 365

The tables below list the data that is shared with Microsoft 365 services.

Artifact metadata that is mainly used when using the "search" mechanism to look for Power BI content within your Microsoft 365 services

	Property	What is Shared	Example
1	TenantID	Azure AD Tenant Identifier	762049eb-7a69-4c39-bf19-75a5b7fcce1d
2	Artifact ID	Identifier for the Content Item (report, app, dashboard, scorecard etc.)	762049eb-7a69-4c39-bf19-75a5b7fcce1d
3	ACL	Access Control List with permissions and Azure AD User, Security Group and Distribution List Identifiers	{"accessType": "grant", "id" : "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee", "type" : "read" }
4	DisplayName	Display name for the report, dashboard, etc.	Retail Analysis Sample
5	Workspace name	Workspace name as per Create a workspace	Retail workspace
6	Workspace URL	Workspace URL	https://powerbi-df.analysis-df.windows.net/groups/8b5ac04e-89c1-4fc6-a364-e8411dfd8d17
7	Workspace ID	Workspace identifier	8b5ac04e-89c1-4fc6-a364-e8411dfd8d17
8	URL	Content Item URL for report, app, dashboard, scorecard etc.	https://powerbi-df.analysis-df.windows.net/groups/8b5ac04e-89c1-4fc6-a364-e8411dfd8d17/reports/762049eb-7a69-4c39-bf19-75a5b7fcce1d/ReportSection2

	Property	What is Shared	Example
9	SharingLinksURL	Sharing Link as per Share a report using a link	["https://app.powerbi.com/links/xyz123"]
10	IconURL		cdn.com/report.png
11	Description	Content description as per Report settings	Sample containing retail sales data
12	Owner/Creator	Azure AD User Principal Name of the User that Created the Content as per Azure AD user principal name	user1@griffin1.org
13	CreatedDate	Date the content was created	2011-06-30T23:32:46Z
14	LastModifiedDate	Last modified date for the content	2011-06-30T23:32:46Z
15	LastModifiedUser	Azure AD User Principal Name for the last person who modified the content	user1@griffin1.org

User activity that is leveraged for showing Power BI content within your "Recents" and "Recommended" sections at Office.com

	Property	What is Shared	Example
16	LastRefreshDate	Last refresh date for the content	2011-06-30T23:32:46Z
17	UserID	Azure AD User Principal Name for the user who acted on the content	user1@griffin1.org
18	Signal Type	The type of action the user took on the content (Viewed, Modified)	Viewed
19	ActorID	Users Azure AD ID for the user who acted on the content	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
20	StartTime/EndTime	Date/Time the user performed the action on the content	2011-06-30T23:32:46Z

Next steps

- Share data with your Microsoft 365 services tenant settings

- Where data is located when Power BI data is shared with your Microsoft 365 services

Got feedback? We'd love to hear it at Power BI Ideas.

Find the default region for your organization

Article • 12/05/2022 • 2 minutes to read

The region where your data is stored is important because it can affect the interactions you have with the Power BI service. For example, Power BI stores reports, connection information, data models, and the data inside those models in the service.

> **Note**
>
> This video might use earlier versions of Power BI Desktop or the Power BI service.

The first user in your organization to sign up for Power BI or Microsoft 365 chooses the country or region for the business identity. Azure Active Directory, the shared identity and access management service for the cloud, creates a tenant in the data center region closest to the selected country or region. Azure Active Directory is a multi-tenant service, and each organization is represented as an individual tenant in the data center.

The region you select during sign-up determines where data is stored. This region will be the same location for all users in your organization, no matter where they are. Ideally, the selected region will be in the same geographical area as most of your users. For more information about signing up for Power BI and choosing the data region, see Get a Power BI service subscription for your organization.

> **Important**

After sign-up you can't change the default data region yourself. For information about how to request a support-driven data region migration, see **Move between regions**.

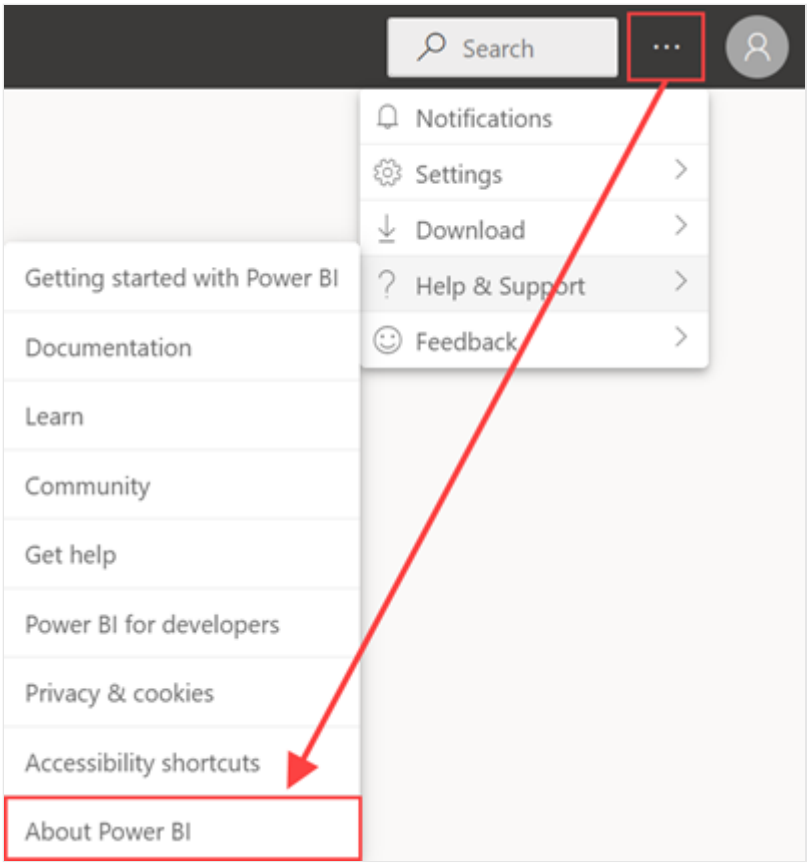
> **Note**
>
> Customers that have purchased Power BI Premium capacity can specify a data region for each capacity. The region for the capacity can be different than the default region. Learn more about how to configure this scenario in **Multi-Geo support for Power BI Premium**.

> **Note**
>
> There are some regions in which Power BI tenants are not initially established by default. If you prefer your Power BI tenant to be located in such a region, you can **move** your tenant to that region.

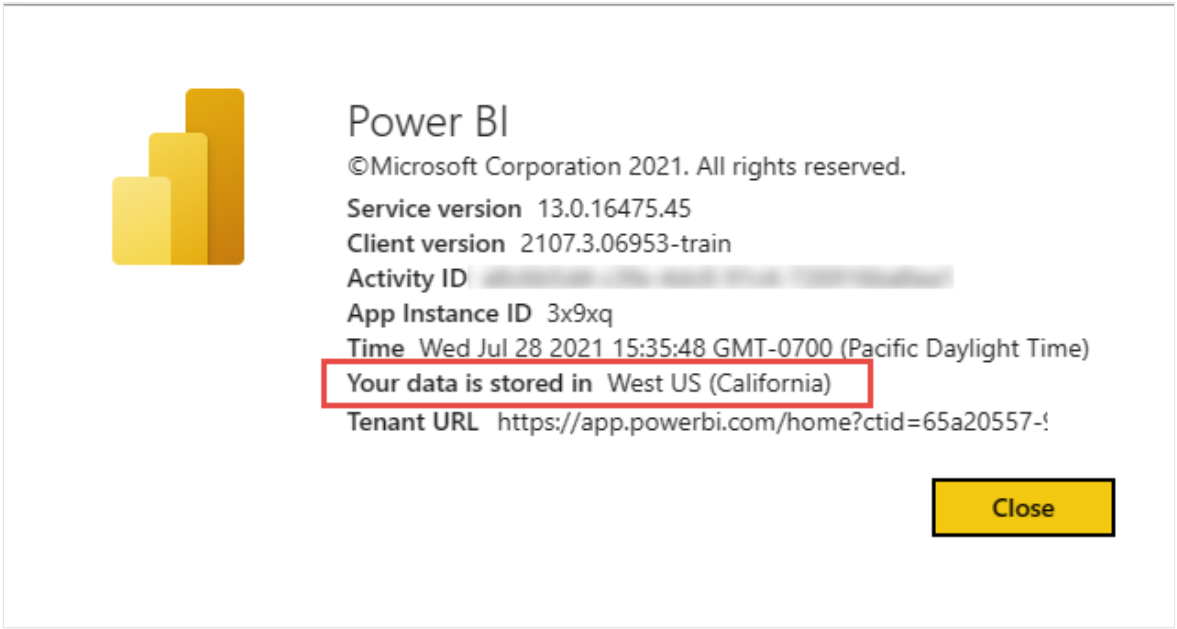
How to find the default region for your organization

To find the default data region for your organization, follow these steps:

1. Sign in to Power BI.
2. Select Settings in the upper right corner > **Help & Support** > **About Power BI**.



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.



Learn more

- International availability of Microsoft Power Platform
- Configure and manage capacities in Power BI Premium
- Move Power BI between regions

- Administrators learning catalog

More questions? Try the Power BI Community

Where data is located when Power BI data is shared with your Microsoft 365 services

Article • 10/21/2022 • 2 minutes to read

The Power BI administrator can use the **Allow your Microsoft 365 services to process or store Power BI data which may be outside of your Power BI tenant's geographic area** switch to share Power BI content on the Office.com home page. Power BI and Microsoft 365 are distinct and separately operated Microsoft cloud services each deployed according to their own service specific data center alignment rules, even when purchased together. Accordingly, your Microsoft 365 Services and Power BI service may not be deployed in the same geographic region. When this Power BI tenant setting is enabled, Power BI data shared with Microsoft 365 may be processed or stored in the Microsoft 365 region even if it is a different region than where Power BI is deployed.

What data is shared

To learn more about the data shared when you use this feature, see Data that will be shared with Microsoft 365.

Where Power BI data is stored

For more information about data storage locations, see Find the default region for your organization and Product Availability by Geography

Where Microsoft 365 data is 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.

Learn more

- Share data with your Microsoft 365 services admin settings
- Where your data is located

Move between regions

Article • 12/14/2022 • 8 minutes to read

Your default data region is determined by the location selected during sign-up. However, this region might not be optimal if most of your users are located in a different geographic location. You might want to move to another region to reduce latency or to ensure data governance. You can't move your organization's tenant between regions by yourself. Self-service migration of Power BI resources stored in Azure isn't supported. If you need to change your default data location from the current region to another region, you have to contact support to manage the migration for you.

> **ⓘ Important**
>
> This article describes how to request a move between regions and keep Power BI data. Be sure you're aware of what can't be moved and steps you have to do before and after the region move. Moving between regions is considered a tenant migration. You can request a different process to move your tenant to another region if data loss and reconfiguration is acceptable. To determine your current data region, follow the steps in **Find the default region for your organization**.

Prerequisites

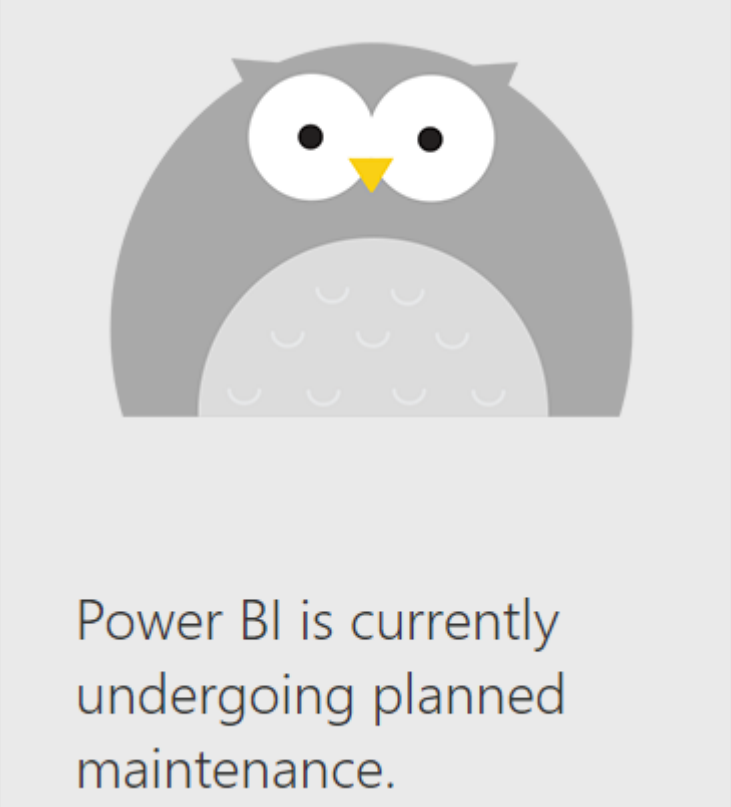
- The person who requests the data region move must be assigned the global administrator role. You can learn more about the different admin roles and what they can do in Understanding Power BI administrator roles. We can't help identify your global administrator for you. Look for global administrator role holders in Microsoft 365 or Azure Active Directory or ask your help desk.
- We must receive written approval confirming your awareness and agreement of the effect of the tenant migration on your organization.
- Provide a point of contact for after business hours during the migration.

Prepare

The migration process moves all tenant data to the new region. The GUID assigned to datasets, reports, dashboards, and other content don't change. However, there are some limitations you should be aware of and preparation steps you need to take.

Awareness

- The end-to-end migration process may take up to six months. We prioritize service reliability and deployment schedules can change, so we may need to reschedule during migration at any time. We can't guarantee successful migration due to inconsistent data or bugs.
- Migration requires about six hours of down time. During migration, users can't access Power BI and will see an error message similar to the one shown in the following screenshot. The actual down time depends on the volume of data to be migrated.



- Capacities and Premium workspaces can't be migrated.
- Power BI Premium Per User (PPU) capacity will be deleted before migration starts. After the migration, PPU capacity will be recreated at first PPU user sign-in. For more information about PPU licenses, see Power BI Premium Per User.
- After migration, Excel workbooks that use the Analyze in Excel feature might fail to refresh. You might need to update the connection string or redownload the ODC connection for that dataset. Follow the steps in Start in Power BI with Analyze in Excel if necessary.
- Push datasets might not be migrated. If they can't be migrated, you'll need to delete the datasets.
- You have to reconfigure data gateways after migration. To learn more about this step, read Migrate, restore, or take over an on-premises data gateway.

- Dataset and workspace storage modes shouldn't be changed one day before the migration. Changing the storage mode before the migration can leave the datasets unusable after the migration. For more information, read Dataset modes in the Power BI service and Manage data storage in Power BI workspaces.

- Some usage data collected before migration is unavailable after migration. Usage data in the following sources will be lost:
  - Power BI Activity Log
  - View count in Lineage view
  - Data protection metrics report
  - Usage metrics(preview)

Preparation steps

Our support team will work with you to verify that the following steps are done to prepare for the migration:

- We can't migrate capacities and Premium workspaces, so you have to delete all capacities before migration. After the region move, these resources can be recreated. If you move resources from a Premium workspace to a shared workspace, datasets larger than 1 GB can't be viewed until they're moved back to Premium capacity.

- Gateways should be deleted in the target region to avoid conflicts during migration.

- To keep user activity logs, follow the steps in Track user activities in Power BI. You can get log data from either the Power BI activity log or the Unified audit log.

Request a region move

To find out the best way to contact support, read Power BI support options. Most admins can use the **Help + support** experience in the Power Platform Admin Center to submit a service request. Use the following steps to get started:

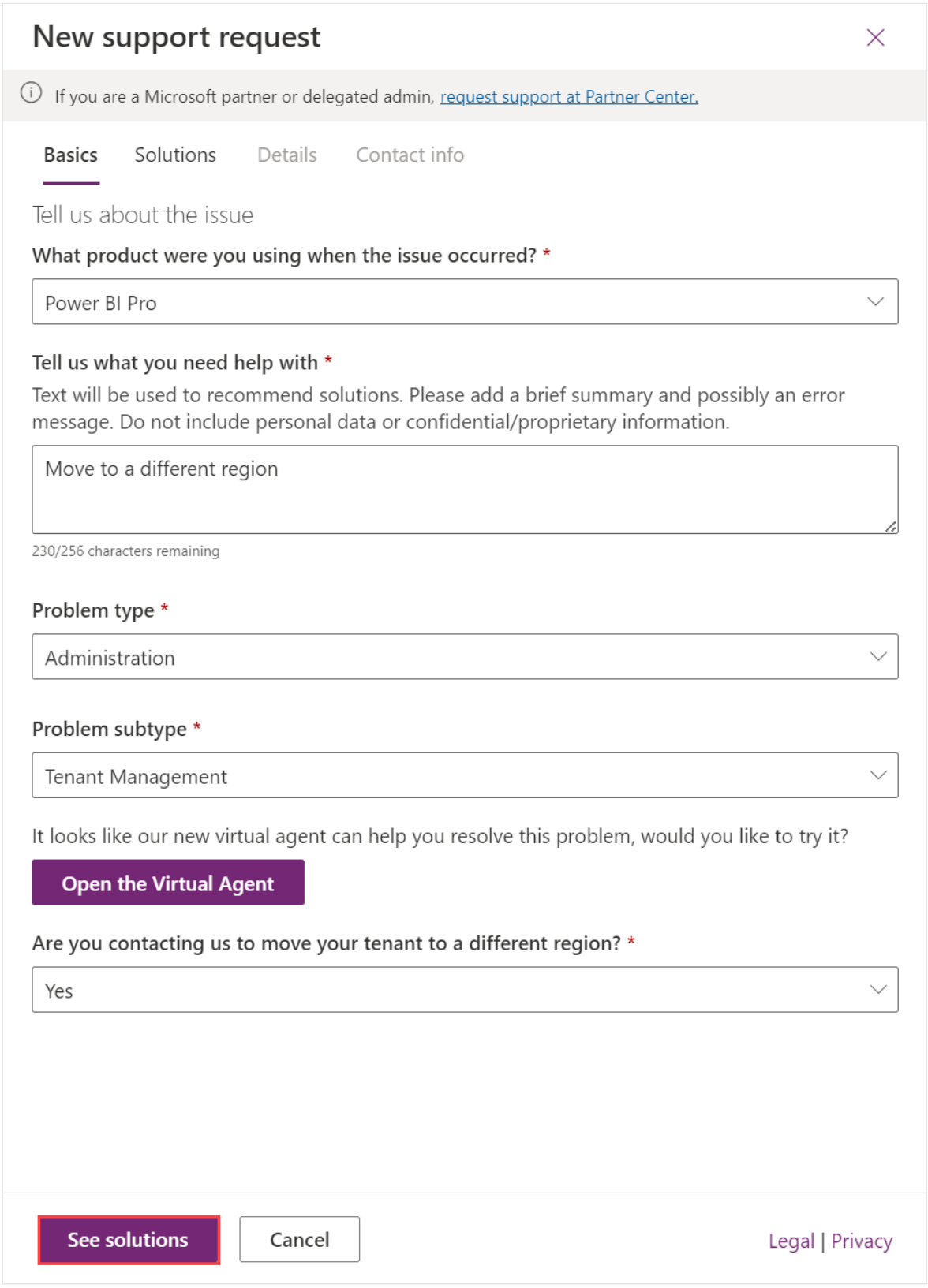
1. Go to Power Platform Admin Center Help + support and sign in using admin credentials.

2. Select **New support request**, then select the following options to request a region move:

   - Product: Power BI Pro
   - Tell us what you need help with: Move to a different region

- Problem type: Administration
- Problem Subtype: Tenant Management
- Are you contacting us to move your tenant to another region: Yes

Select **See solutions** to move to the next screen.



3. Select **Next** to continue to **Select your support plan**. Choose your support plan. Add a description and include the information in the following table:

Information needed	How to find the information
Tenant object ID	How to find your Azure Active Directory tenant ID
Current region	Find the default region for your organization
Proposed region	International availability of Microsoft Power Platform
Proposed date and time for migration	Give us three options in UTC time. The proposed dates should be at least two weeks later than when you submit the request.
Contact available after during off-business hours	Name, phone number, and email address

4. Under **Is the problem you're reporting related to a recent service change?**, choose N/A. Select a severity level, then select **Next**.

5. Add your contact information, then **Submit**.

Our support team will be in touch. The support team makes sure you're authorized to make this request, confirms your awareness of the issues listed earlier, and obtains written approval to confirm you want to move your tenant between regions.

Be sure to provide contact details for someone who can act as the point of contact for Support. The contact has to be available after business hours.

Support will review the submitted information, including your tenant object ID, current data region, and target data region. After details are confirmed, we'll coordinate the proposed migration time frame with you.

During the region move

- Don't do any manual or scheduled refreshes until after migration is complete.
- Support will copy your data to the new region. Power BI won't be available to users during the move.

After the region move

When migration is complete, you'll be able to access Power BI in about 20-30 minutes. Support will contact you to make sure everything is working.

Do the following steps to recreate the configuration of the original region:

1. Recreate capacities and move workspaces back to Premium. Read more about this step in Configure and manage capacities in Power BI Premium.
2. If push datasets were deleted, recreate them. For more information, see Real-time streaming in Power BI to learn how to push data into a dataset.
3. Reconfigure your data gateways. Follow the steps in Migrate, restore, or take over an on-premises data gateway.
4. Excel workbooks that use the Analyze in Excel feature might fail to refresh. You might need to update the connection string or redownload the ODC connection for that dataset. Follow the steps in Start in Power BI with Analyze in Excel if necessary.
5. Links to Power BI that are embedded in content might fail to connect when migration is complete. For example, an embedded link in SharePoint might result in a user error. To resolve this problem, you have to regenerate the embedded link in Power BI, and then update the locations where they're used. To fix this issue, follow the procedure in Embed a report web part in SharePoint Online.

To verify that the default region for data storage has been moved, follow the steps in Find the default region for your organization .

Frequently asked questions

Can I migrate back to the original region? If yes, what's the process and will I lose data?

No, you can't revert to using the old region.

Is my data deleted immediately from the old region? If not, how long is it kept and do I have access to it?

Data is retained in the old region for 30 days and is then deleted. Customers don't have access to data in the old region after migration.

What happens to my Microsoft 365 groups, SharePoint sites, etc.? Are they also migrated?

We only migrate Power BI-specific resources. Your Microsoft 365 groups and SharePoint sites aren't touched.

Can I request that some of my data be migrated to a different region?

No, migration of data to different regions isn't a supported scenario.

Does migration change any of my data or settings for Azure Active Directory?

No, migration doesn't affect anything outside of Power BI.

Can I use Power BI REST APIs for read-only operations during migration?

No, using Power BI during tenant migration activity isn't recommended.

Why do I need to provide three proposed migration dates?

We need to ensure that migration happens outside of the production deployment window. This time-frame is subject to change on a weekly basis. We can only confirm the actual migration date five days before the migration.

Can I request migration during weekdays (if my company allows) or on any public holiday recognized by my organization?

Yes, you can request migration during weekdays or public holidays.

How do I verify my data is now stored in the requested region?

Follow the steps in Find where data is stored. You should see the new region next to **Your data is stored in**.

Can I migrate or merge my Power BI tenant into a different tenant (for example, because of a company merger)?

No, migration from one tenant to another isn't possible.

After migration, is it normal to still see some refreshes happening from the old tenant location?

Refresh in the old region should stop after migration.

My allowlist contains Power BI IP ranges that are used to access some data sources. Do I need to update the IP ranges to match the new location?

Yes. Because it's a new location, the IP ranges are also changing, and the ranges need to be updated. Download the Azure IP Ranges JSON file to identify the needed IP ranges.

Is there a cost to have my tenant moved to a different region?

No, there's no cost charged for region migration. Customers that have any paid licenses can migrate. The operation must be requested by a global administrator.

Track Power BI service health in Microsoft 365

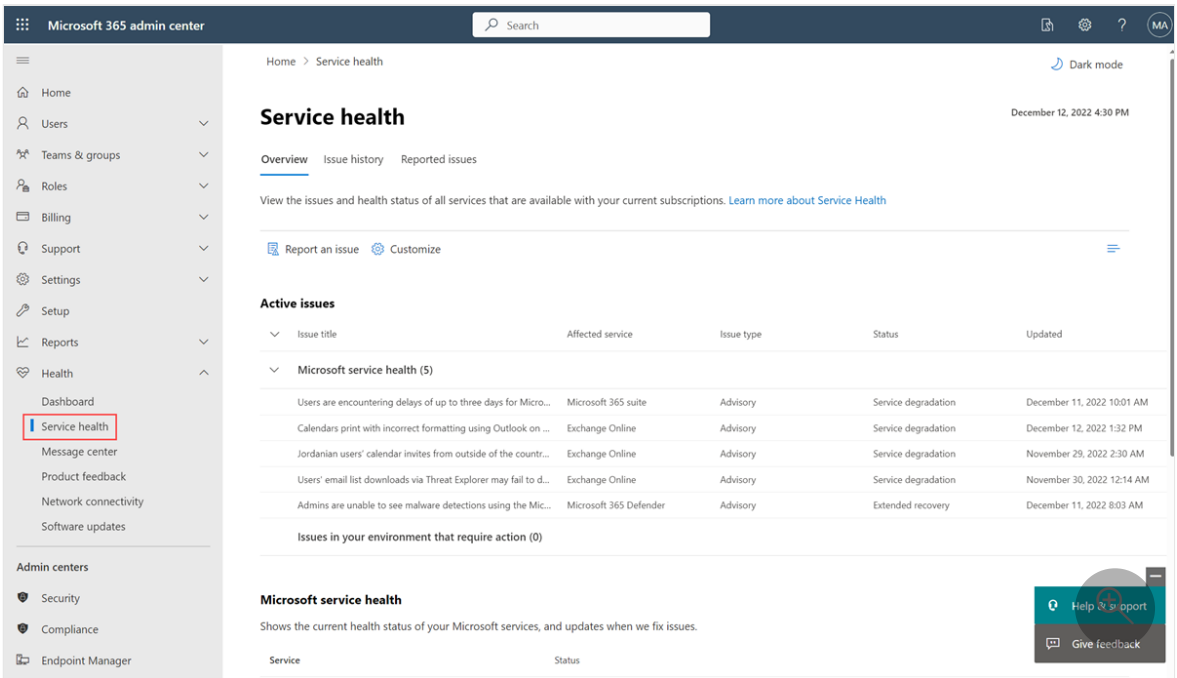
Article • 12/27/2022 • 2 minutes to read

The Microsoft 365 admin center provides important tools for Power BI admins. The tools include current and historical information about service health. To access service health information, you must be in one of the following roles:

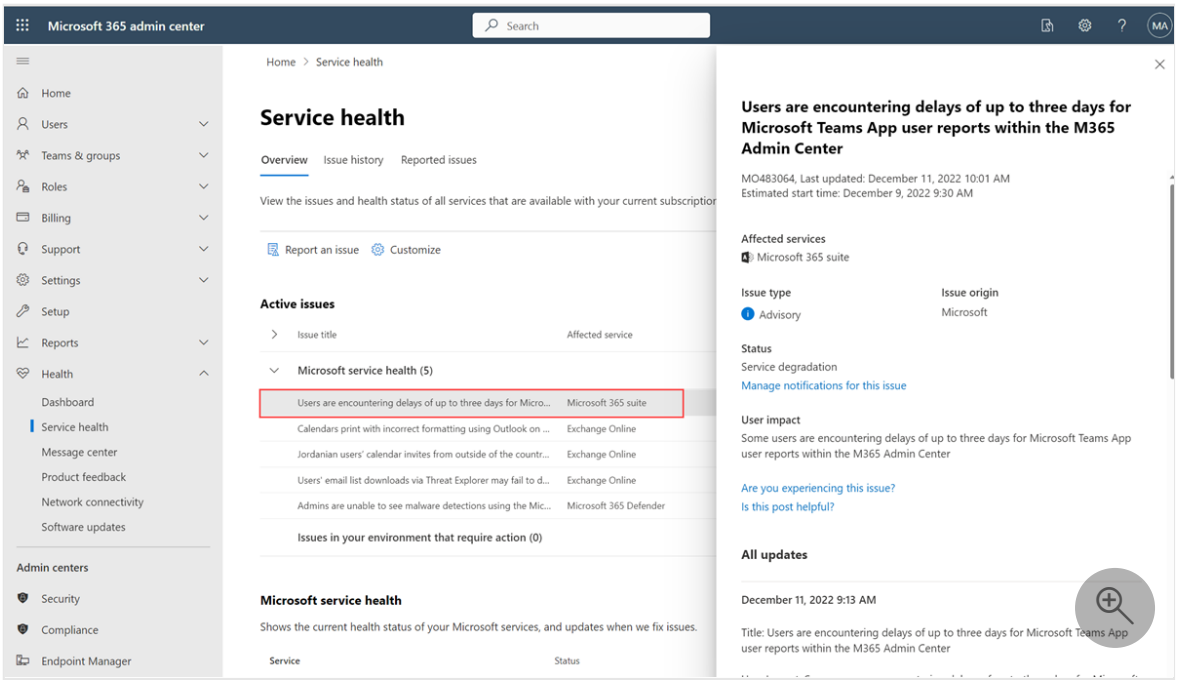
- Power BI Service Administrator
- Global Administrator

For more information about roles, see Administrator roles related to Power BI.

1. Sign in to the Microsoft 365 admin center.
2. From the nav pane, select **Show all** > **Health** > **Service health**. The Service health page appears. Active issues are listed on this overview page:



3. To see more information, select an item.



Scroll down to see more information, then close the pane when you're finished.

4. To see historical information across all services, select **Issue history**, and then select **Past 7 days** or **Past 30 days**.

5. To return to current service health, select **Overview**.

Find Power BI users who have signed in

Article • 12/27/2022 • 2 minutes to read

If you're an admin for your organization, and want to see who has signed in to Power BI, use the Azure Active Directory (Azure AD) access and usage reports, which are also known as the sign-in logs.

> ⓘ **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.

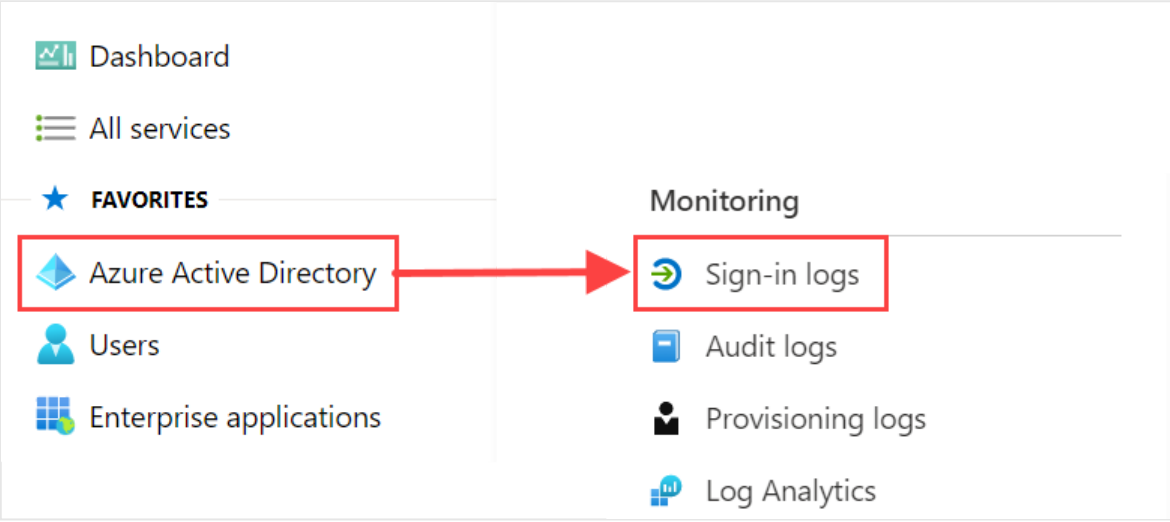
Requirements

Any user can view a report of their own sign-ins. To see a report for all users, you must be in one of the following roles: Global Administrator, Security Administrator, Security Reader, Global Reader, or Report Reader.

Use the Azure AD admin center to view sign-ins

To view sign-in activity, follow these steps:

1. Sign in to the Azure AD admin center, and then select **Azure Active Directory** from the portal menu.
2. From the resource menu, select **Monitoring** > **Sign-in logs**.



3. By default, all sign-ins from the last 24 hours for all users and all applications are shown. To select a different time period, select **Date** in the working pane and choose from the available time intervals. Only information from the last seven days is available. To see only sign-ins to Power BI, add filters:

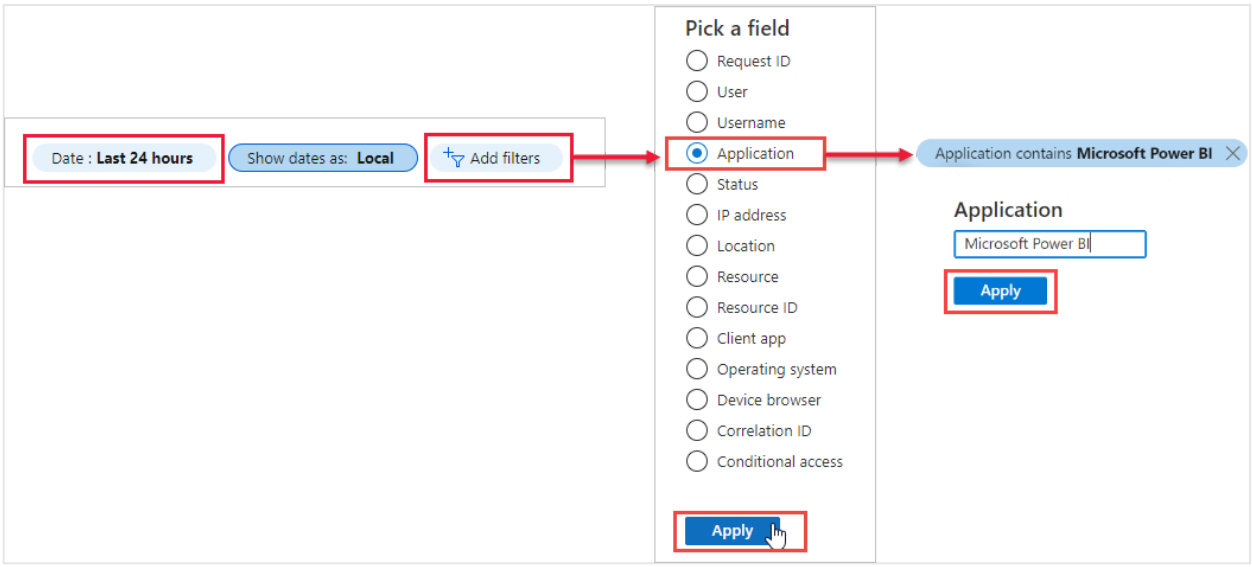
   a. Select **Add filter** > pick **Application** as the field to filter by, and select **Apply**.

   b. From the top of the working pane, select **Application contains**.

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

4. Select **Apply**.

Microsoft Power BI filters to sign-in activity related to the service. **Power BI Gateway** filters to sign-in activity specific to the on-premises data gateway.



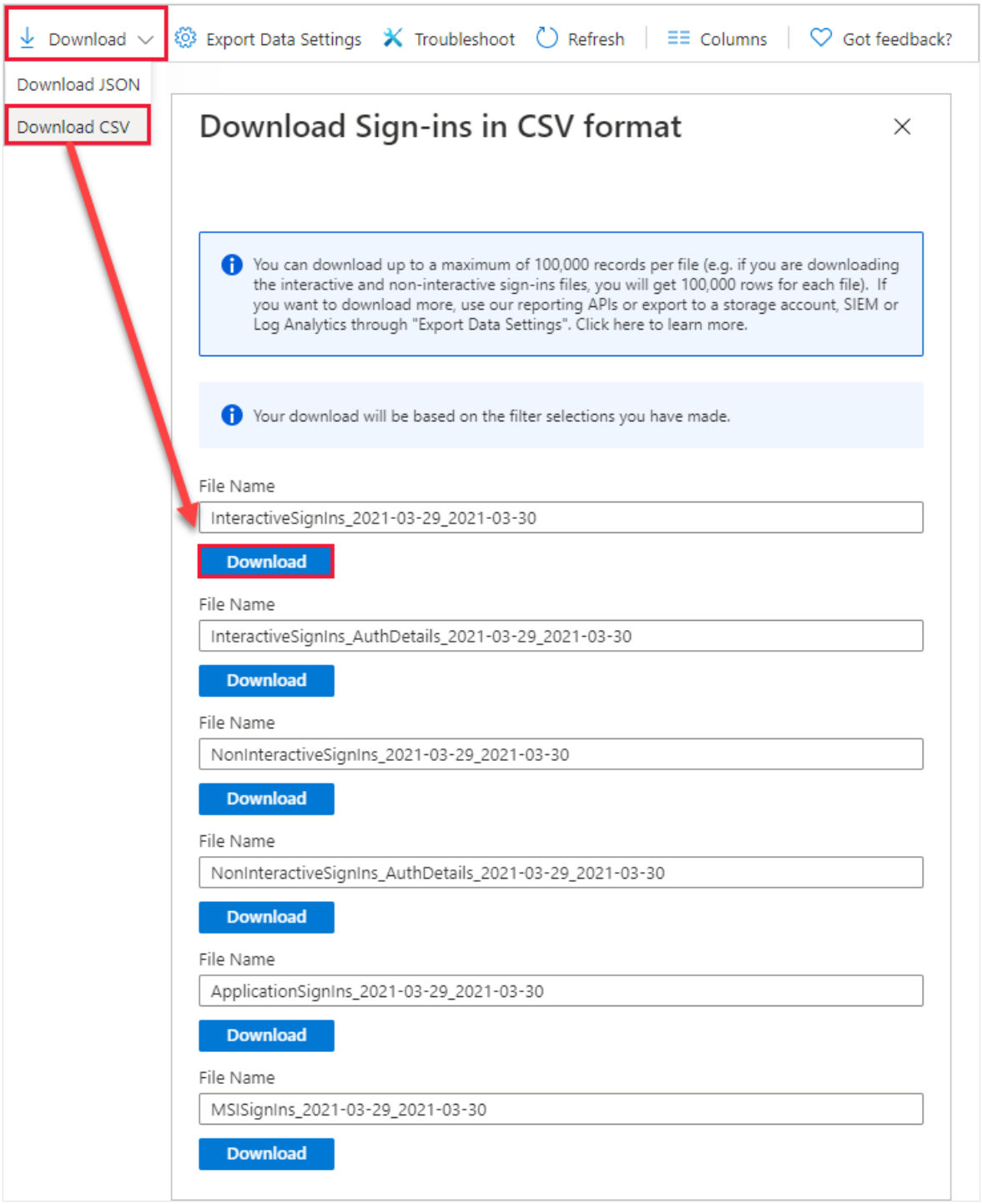
Export the data

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 logs** report, 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**.



Data retention

Sign-in-related data is available for up to seven days, unless your organization has an Azure AD premium license. If you use Azure AD Premium P1 or Azure AD Premium P2, you can see data for the past 30 days. For more information, see How long does Azure AD store reporting data?.

Next steps

Track user activities in Power BI

More questions? Try asking the Power BI Community

Track user activities in Power BI

Article • 11/21/2022 • 22 minutes to read

Knowing who is taking what action on which item in Power BI can be critical in helping your organization fulfill its requirements, like meeting regulatory compliance and records management. This article discusses two options to track user activity: The Power BI activity log and the unified audit log.

Choosing a log source

The Power BI activity log and unified audit log both contain a complete copy of the Power BI auditing data. However, we highly recommend using the Power BI activity log for the following reasons:

- The Power BI activity log contains only the Power BI activities structured list of records (JSON array).
- The global administrator role isn't needed to access the Power BI activity log.

The differences between log sources are summarized in the following table.

Unified audit log	Power BI activity log
Includes events from Power BI, plus events from SharePoint Online, Exchange Online, Dynamics 365, and other services.	Includes only the Power BI auditing events.
Only users with Audit Logs permissions have access, such as global administrators and auditors.	Global administrators, Power Platform administrators, and Power BI administrators have access.
Global administrators and auditors can search the unified audit log by using the Microsoft 365 Defender portal and the Microsoft Purview compliance portal.	There's no user interface to search the activity log yet.
Global administrators and auditors can download audit log entries by using Microsoft 365 Management APIs and cmdlets.	Global administrators, Power Platform administrators, and Power BI administrators can download activity log entries by using a Power BI REST API and management cmdlet.
Keeps audit data for 90 days	Keeps activity data for 30 days (public preview).
Keeps audit data, even if the tenant is moved to a different Azure region.	Doesn't keep activity data when the tenant is moved to a different Azure region.

Use the activity log

Power BI administrators can analyze usage for all Power BI resources at the tenant level by using custom reports that are based on the Power BI activity log. You download the activities by using a REST API or PowerShell cmdlet. Activity data can also be filtered by date range, user, and activity type.

> ⓘ **Note**
>
> You need to be familiar with the **Power BI Admin API** and **Power BI PowerShell modules**. PowerShell modules must be installed before you can run commands.
>
> There can be a lag of up to 30 minutes to retrieve Power BI events.

Activity log requirements

To access the Power BI activity log, you must meet these requirements:

- You have to be a global administrator or a Power BI administrator.
- Install the Power BI Management cmdlets locally or use the Power BI Management cmdlets in Azure Cloud Shell.

ActivityEvents REST API

You can use an administrative application based on the Power BI REST APIs to export activity events into a blob store or SQL database. You can then build a custom usage report on top of the exported data. In the **ActivityEvents** REST API call, you must specify a start date and end date and optionally a filter to select activities by activity type or user ID. Because the activity log could contain a large amount of data, the **ActivityEvents** API currently only supports downloading up to one day of data per request. In other words, the start date and end date must specify the same day, as in the following example. Make sure you specify the `DateTime` values in Coordinated Universal Time (UTC) format.

```
HTTP

https://api.powerbi.com/v1.0/myorg/admin/activityevents?startDateTime='2019-08-31T00:00:00'&endDateTime='2019-08-31T23:59:59'
```

If the number of entries is large, the **ActivityEvents** API returns only around 5,000 to 10,000 entries and a continuation token. Call the **ActivityEvents** API again with the

continuation token to get the next batch of entries, and so forth, until you've gotten all entries and no longer receive a continuation token. The following example shows how to use the continuation token:

HTTP

```
https://api.powerbi.com/v1.0/myorg/admin/activityevents?
continuationToken='%2BRID%3ARthsAIwfWGcVAAAAAAAAAA%3D%3D%23RT%3A4%23TRC%3A20
%23FPC%3AARUAAAAAAAAAFwAAAAAAAA%3D'
```

If the results include a continuation token, continue to call the API using that token to get the rest of the data until a continuation token is no longer returned. It's possible for a call to return a continuation token without any event entries. The following example shows how to loop with a continuation token returned in the response:

```
while(response.ContinuationToken != null)
{
   // Store the activity event results in a list for example
    completeListOfActivityEvents.AddRange(response.ActivityEventEntities);

    // Make another call to the API with continuation token
    response = GetPowerBIActivityEvents(response.ContinuationToken)
}
completeListOfActivityEvents.AddRange(response.ActivityEventEntities);
```

> **Note**
>
> It can take up to 24 hours for all events to show up, though full data is typically available much sooner.

If the time span between `startDateTime` and `endDateTime` exceeds 1 hour, it takes multiple requests to download the data through `continuationUri` in response.

The following example shows how to download data for 1 hour and 5 minutes:

HTTP

```
GET https://wabi-staging-us-east-
redirect.analysis.windows.net/v1.0/myorg/admin/activityevents?
startDateTime='2020-08-13T07:55:00Z'&endDateTime='2020-08-13T09:00:00Z'
{
  "activityEventEntities": […],
  "continuationUri": https://wabi-staging-us-east-
redirect.analysis.windows.net/v1.0/myorg/admin/activityevents?
```

```
continuationToken='LDIwMjAtMDgtMTNUMDc6NTU6MDBaLDIwMjAtMDgtMTNUMDk6MDA6MDBaL
DEsLA%3D%3D',
  "continuationToken":
"LDIwMjAtMDgtMTNUMDc6NTU6MDBaLDIwMjAtMDgtMTNUMDk6MDA6MDBaLDEsLA%3D%3D",
  "lastResultSet": false
}

GET https://wabi-staging-us-east-
redirect.analysis.windows.net/v1.0/myorg/admin/activityevents?
continuationToken='LDIwMjAtMDgtMTNUMDc6NTU6MDBaLDIwMjAtMDgtMTNUMDk6MDA6MDBaL
DEsLA%3D%3D'
{
  "activityEventEntities": [],
  "continuationUri": null,
  "continuationToken": null,
  "lastResultSet": false
}
```

To learn more about using the Power BI REST API, including examples of how to get audit activity events, see Admin - Get Activity Events in the Power BI REST API reference documentation.

Get-PowerBIActivityEvent cmdlet

Download activity events by using the Power BI Management cmdlets for PowerShell. The Get-PowerBIActivityEvent cmdlet automatically handles the continuation token for you. The `Get-PowerBIActivityEvent` cmdlet takes a *StartDateTime* and an *EndDateTime* parameter with the same restrictions as the **ActivityEvents** REST API. In other words, the start date and end date must reference the same date value because you can only retrieve the activity data for one day at a time.

The following script demonstrates how to download all Power BI activities. The command converts the results from JSON into .NET objects for straightforward access to individual activity properties. These examples show the smallest and largest timestamps possible for a day to ensure no events are missed:

PowerShell

```
Login-PowerBI

$activities = Get-PowerBIActivityEvent -StartDateTime '2019-08-31T00:00:00'
-EndDateTime '2019-08-31T23:59:59' | ConvertFrom-Json

$activities.Count
$activities[0]
```

Filter activity data

You can filter activity events by activity type and user ID. The following script demonstrates how to download only the event data for the **ViewDashboard** activity. For additional information about supported parameters, use the command `Get-Help Get-PowerBIActivityEvent`.

PowerShell

```
Login-PowerBI

$activities = Get-PowerBIActivityEvent -StartDateTime '2019-08-31T00:00:00'
-EndDateTime '2019-08-31T23:59:59' -ActivityType 'ViewDashboard' |
ConvertFrom-Json

$activities.Count
$activities[0]
```

> ⓘ **Note**
>
> A PowerShell sample is available to help you learn how to filter and retrieve Power BI activity log events. For more information, see **Access the Power BI activity log**.

Use the audit log

If your task is to track user activities across Power BI and Microsoft 365, you work with auditing in Microsoft Purview or use PowerShell. Auditing relies on functionality in Exchange Online, which automatically supports Power BI.

You can filter the audit data by date range, user, dashboard, report, dataset, and activity type. You can also download the activities in a comma-separated value (csv) file to analyze offline.

Audit log requirements

Meet these requirements to access audit logs:

- You must either be a global administrator or 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.

To give non-admin accounts access to the audit log, add the user as a member of one of these role groups. Another option is to create a custom role group in the Exchange admin center, assign the Audit Logs role to this group, and then add the non-admin account to the new role group. For more information, see Manage role groups in Exchange Online.

If you can't access the Exchange admin center from the Microsoft 365 admin center, go to https://outlook.office365.com/ecp, and sign in using your credentials.

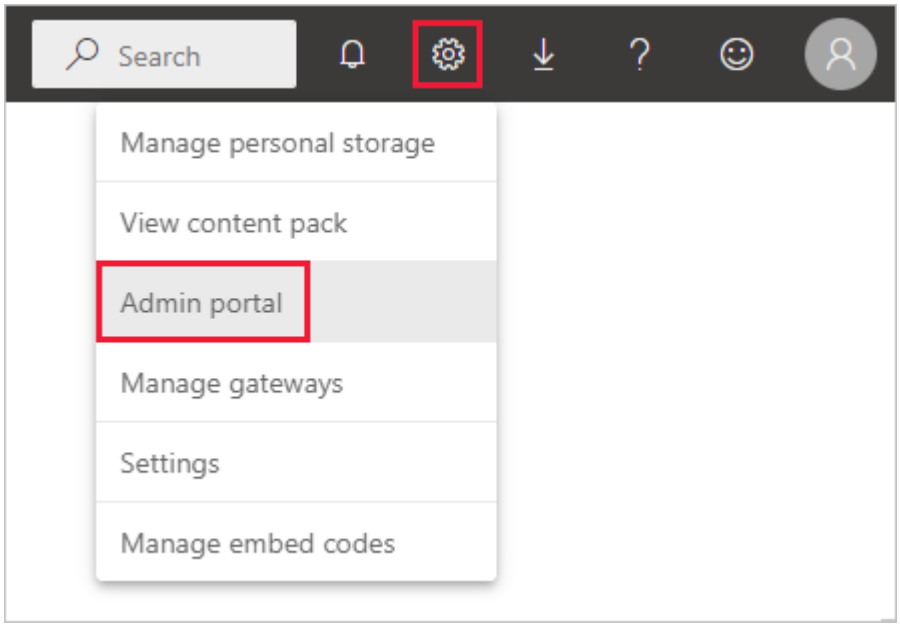
- If you have access to the audit log but aren't a global admin or Power BI Administrator, you can't get to the Power BI Admin portal. In this case, use a direct link to Microsoft Purview.

Access your audit logs

To access logs, first enable logging in Power BI. For more information, see Audit and usage settings in the admin portal documentation. There may be up to a 48-hour delay between the time you enable auditing and when you can view audit data. If you don't see data immediately, check the audit logs later. You might experience a similar delay between getting permission to view audit logs and being able to access the logs.

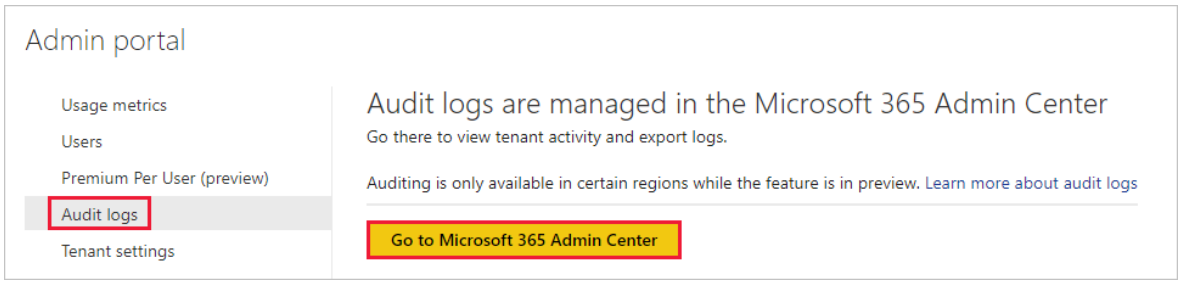
The Power BI audit logs are available directly through Microsoft Purview. There's also a link from the Power BI admin portal:

1. In Power BI, select **Settings** > **Admin portal**.



2. Select **Audit logs**.

3. Select **Go to Microsoft 365 Admin Center**.

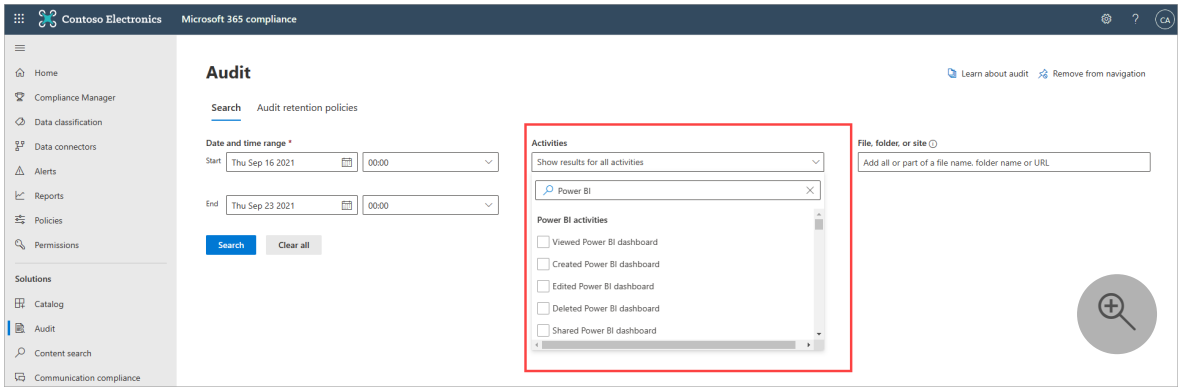


Search Power BI activities

Search for Power BI activities by following these steps. For a list of activities, see the list of activities audited by Power BI later in this article.

1. On the **Audit** page, under **Search**, select the drop-down for **Activities**.

2. Enter *Power BI* to go to the list of Power BI activities.



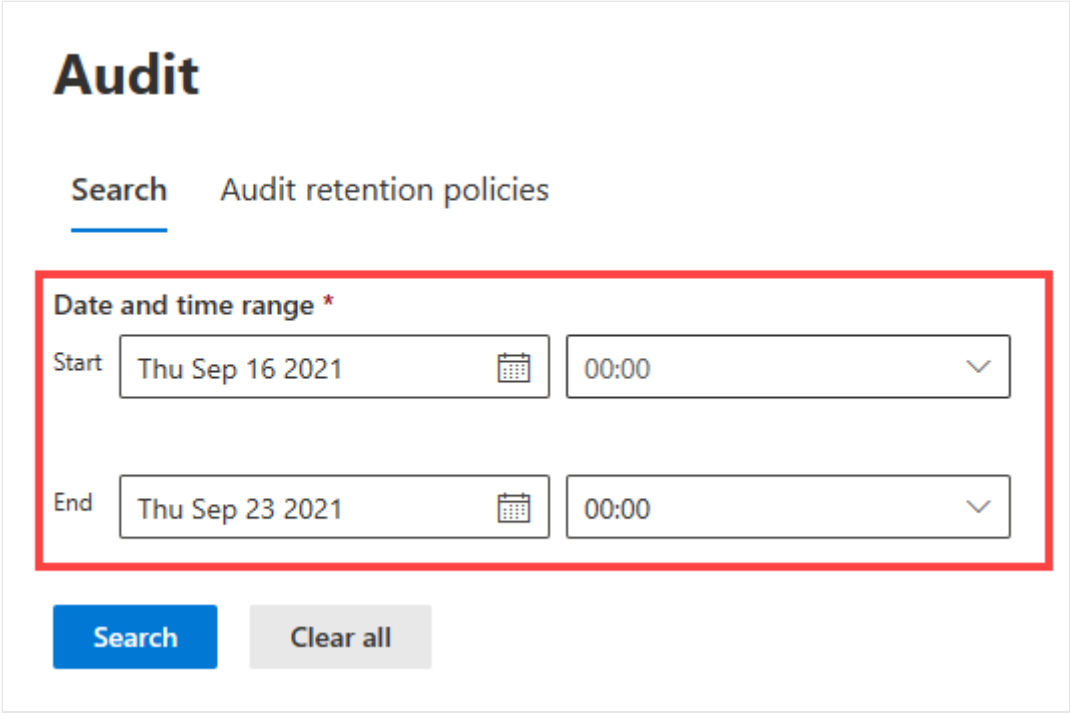
3. Select each of the Power BI activities that you want to track.

Your search will only return the selected Power BI activities.

Search the audit logs by date

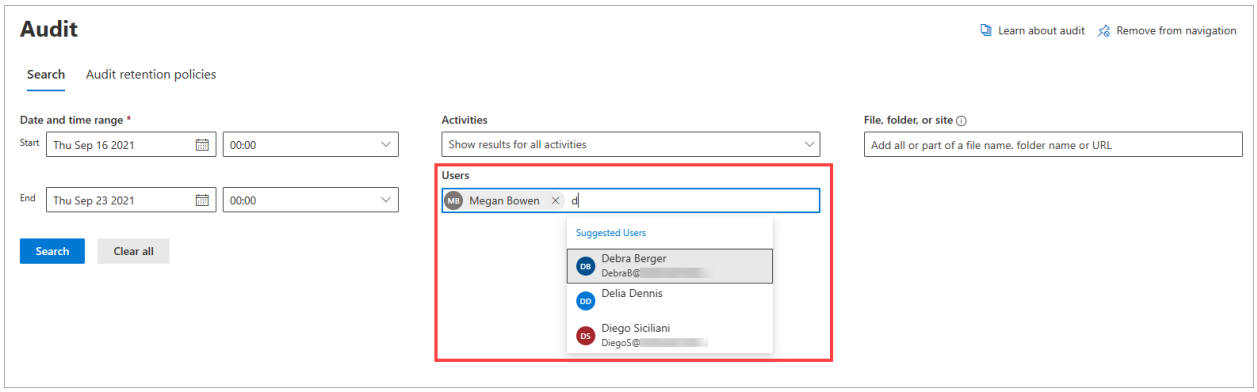
You can search the logs by date range using the **Start date** and **End date** fields. The default selection is the past seven days. The display presents the date and time in UTC format. The maximum date range that you can specify is 90 days.

You receive an error if the selected date range is greater than 90 days. If you're using the maximum date range of 90 days, select the current time for **Start date**. Otherwise, you'll receive an error saying that the start date is earlier than the end date. If you've turned on auditing within the last 90 days, the date range can't start before the date that auditing was turned on.



Search the audit logs by users

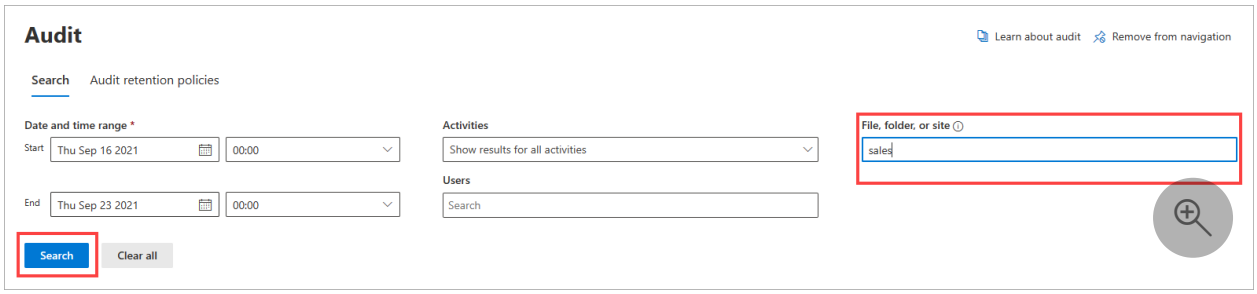
You can search for audit log entries for activities done by specific users. Enter one or more user names in the **Users** field. User names appear in email address format. This box should be left blank to return entries for all users (and service accounts) in your organization.



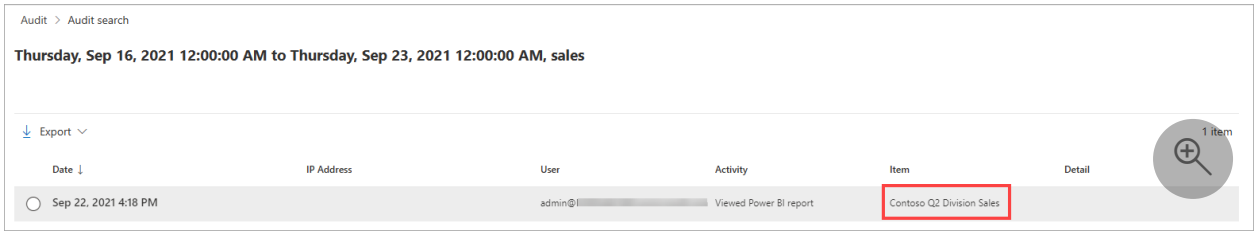
Search the audit logs by file, folder, or site

You can use the **File, folder, or site** field to determine who accessed a file, folder, or site, on the **Audit** page. Records can be searched by file name, folder name, or URL. Don't use any spaces or special characters. For example, you can enter all or part of the name of a dataset to find who has interacted with it recently.

In the example shown below, the search term *sales* was entered in the **File, folder, or site** field.



The search results for the "sales" filter show user activity for the Contoso Q2 Division Sales dataset.



Combine filters to narrow results

You can combine any of the filters included on the Audit page to refine the results that are returned. When you combine filters, the search results will show only items that match all of the filter criteria.

View search results

After you select **Search**, the search results load and display on the **Audit search** page. When the search finishes, the display shows the number of results found. **Audit search** displays a maximum of 1000 events. If more than 1000 events meet the search criteria, the app displays the newest 1000 events.

The following information is shown for each event returned by the search. Select a column header under **Results** to sort the results.

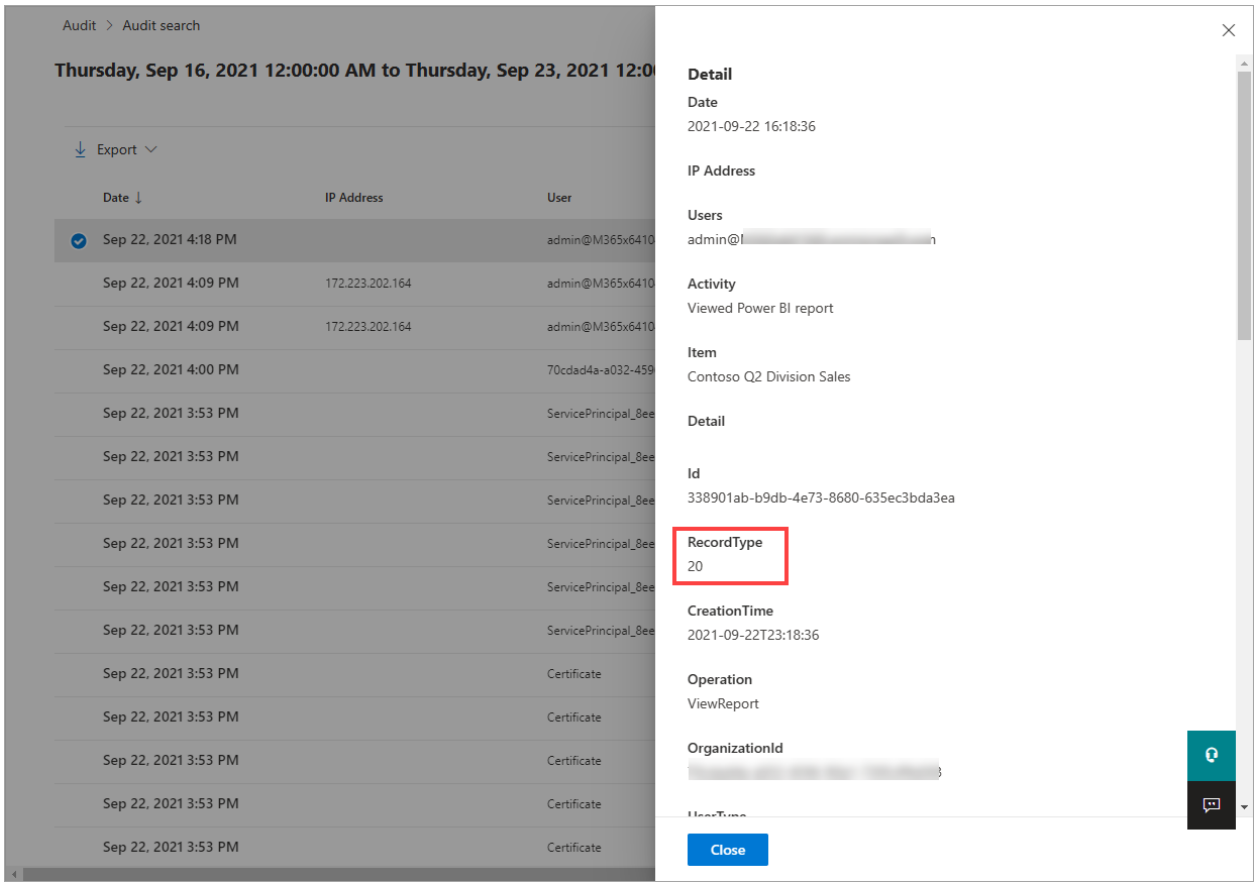
Column	Definition
Date	The UTC formatted date and time when the event occurred.
IP address	The IP address of the device used for the logged activity. The app displays the IP address in either an IPv4 or IPv6 address format.
User	The user (or service account) who did the activity.
Activity	The activity done by the user. This value corresponds to the activities that you selected in the **Activities** drop down list. For an event from the Exchange admin audit log, the value in this column is an Exchange cmdlet.

Column	Definition
Item	The object created or modified because of the corresponding activity. For example, the viewed or modified file, or the updated user account. Not all activities have a value in this column.
Detail	More detail about an activity. Again, not all activities have a value.

View the details for an event

To view more details about an event, select the event record in the list of search results. A **Detail** page appears that has the detailed properties from the event record. The **Detail** page displays properties depending on the Microsoft 365 service in which the event occurs.

All Power BI entries have a value of 20 for the **RecordType** property. For information about other properties, see Detailed properties in the audit log.

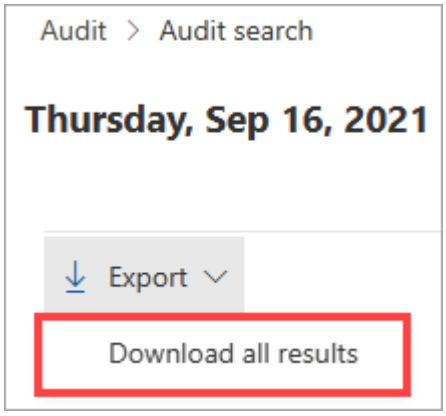


Export search results

To export the Power BI audit log search results to a csv file, follow these steps.

1. Do an audit search by following the steps in this article.

2. On the **Audit search** results page, select the drop-down next to **Export**. Then select **Download all results**. The results are saved in CSV format, and the file can be found in your **Downloads** folder.



Use PowerShell to search audit logs

You can also use PowerShell to access the audit logs. The following example shows how to connect to Exchange Online PowerShell V2 (EXO V2) and then use the Search-UnifiedAuditLog command to pull Power BI audit log entries. To run the script, an admin must assign you the appropriate permissions, as described in the Audit log requirements section. Read About the Exchange Online PowerShell V2 module and Connect to Exchange Online PowerShell to learn more about how this PowerShell module works.

You can download the EXO V2 module from the PowerShell gallery.

PowerShell

```
# The first command sets the execution policy for Windows computers and
allows scripts to run.
Set-ExecutionPolicy RemoteSigned

# The following command loads the Exchange Online management module.
Import-Module ExchangeOnlineManagement

# Next, you connect using your user principal name. A dialog will prompt you
for your
# password and any multi-factor authentication requirements.
Connect-ExchangeOnline -UserPrincipalName <user@contoso.com>

# Now you can query for Power BI activity. In this example, the results are
limited to
# 1,000, shown as a table, and the "more" command causes output to display
one screen at a time.
Search-UnifiedAuditLog -StartDate 09/16/2021 -EndDate 9/23/2021 -RecordType
PowerBIAudit -ResultSize 1000 | Format-Table | More
```

Use PowerShell to export audit logs

You can also use PowerShell to export the results of your audit logs search. The following example shows how to send from the Search-UnifiedAuditLog command and export the results using the Export-Csv cmdlet. To run the script, an admin must assign you the appropriate permissions, as described in the Audit log requirements section.

PowerShell

```
Set-ExecutionPolicy RemoteSigned

Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -UserPrincipalName <user@contoso.com>
Search-UnifiedAuditLog -StartDate 09/16/2021 -EndDate 9/23/2021 -RecordType
PowerBIAudit -ResultSize 1000 | Export-Csv -Path
"c:\temp\PowerBIAuditLog.csv" -NoTypeInformation
```

For more information on connecting to Exchange Online, see Connect to Exchange Online PowerShell. For another example of using PowerShell with audit logs, see Using Power BI audit log and PowerShell to assign Power BI Pro licenses.

Operations available in the audit and activity logs

The following operations are available in both the audit and activity logs.

> **Note**
>
> We recently added many Power BI activities to the audit and activity logs. Friendly names can be found in Microsoft Purview, and we'll continue to update this list to identify the operation names used in REST API and PowerShell queries.

Friendly name	Operation name	Notes
Added data source to Power BI gateway	AddDatasourceToGateway	

Friendly name	Operation name	Notes
Added external resource	AddExternalResource	
Added link to external resource	AddExternalResourceLink	
Added Power BI folder access	AddFolderAccess	Not currently used
Added Power BI group members	AddGroupMembers	
Added user to Power BI gateway cluster	AddUsersToGatewayCluster	
Added user to Power BI gateway cluster datasource	AddUsersToGatewayClusterDatasource	
Admin attached dataflow storage account to tenant	AdminAttachedDataflowStorageAccountToTenant	Not currently used
Analyzed Power BI dataset	AnalyzedByExternalApplication	Generated when users interact with the service

Friendly name	Operation name	Notes
Analyzed Power BI report	AnalyzeInExcel	Generated when a user selects **Analyze in Excel** on a report or dataset in the service and successfully generates an Excel workbook
Applied sensitivity label to Power BI item	SensitivityLabelApplied	
Assigned a workspace to a deployment pipeline	AssignWorkspaceToPipeline	
Attached dataflow storage account	AttachedDataflowStorageAccount	
Binded monikers to Power BI datasources	BindMonikerstoDatasources	
Binded Power BI dataset to gateway	BindToGateway	
Canceled Power BI dataflow refresh	CancelDataflowRefresh	
Changed capacity state	ChangeCapacityState	

Friendly name	Operation name	Notes
Changed capacity user assignment	UpdateCapacityUsersAssignment	
Changed Power BI dataset connections	SetAllConnections	
Changed Power BI gateway admins	ChangeGatewayAdministrators	
Changed Power BI gateway data source users	ChangeGatewayDatasourceUsers	
Changed sensitivity label for Power BI item	SensitivityLabelChanged	
Connected to Power BI dataset from external app	ConnectFromExternalApplication	
Copied Power BI dashboard	CopyDashboard	
Copied Power BI report	CopyReport	
Created a Power BI scorecard metric	CreateGoal	
Created a Power BI metric value	CreateGoalValue	
Created a Power BI scorecard	CreateScorecard	

Friendly name	Operation name	Notes
Created an organizational custom visual	InsertOrganizationalGalleryItem	
Created deployment pipeline	CreateAlmPipeline	
Created install ticket for installing Power BI template app	CreateTemplateAppInstallTicket	
Created Power BI app	CreateApp	
Created Power BI dashboard	CreateDashboard	
Created Power BI dataflow	CreateDataflow	
Created Power BI dataset	CreateDataset	
Created Power BI dataset from external app	CreateDatasetFromExternalApplication	
Created Power BI email subscription	CreateEmailSubscription	
Created Power BI folder	CreateFolder	
Created Power BI gateway	CreateGateway	

Friendly name	Operation name	Notes
Created Power BI gateway cluster datasource	CreateGatewayClusterDatasource	
Created Power BI group	CreateGroup	
Created Power BI report	CreateReport [1]	
Created Power BI template app	CreateTemplateApp	
Created workspace for Power BI template app	CreateTemplateApp	
Custom visual requested Azure AD access token	GenerateCustomVisualAADAccessToken	
Custom visual requested Office Web Apps access token	CustomVisualWACAccessToken	
Dataflow migrated to external storage account	DataflowMigratedToExternalStorageAccount	Not currently used
Dataflow permissions added	DataflowPermissionsAdded	Not currently used
Dataflow permissions removed	DataflowPermissionsRemoved	Not currently used

Friendly name	Operation name	Notes
Deleted an organizational custom visual	DeleteOrganizationalGalleryItem	
Delete admin monitoring folder via lockbox	DeleteAdminMonitoringFolderViaLockbox	
Delete admin usage dashboards via lockbox	DeleteAdminUsageDashboardsViaLockbox	
Delete usage metrics v2 package via lockbox	DeleteUsageMetricsv2PackageViaLockbox	
Deleted deployment pipeline	DeleteAlmPipeline	
Deleted current value connection of Power BI metric		
Deleted link to external resource	DeleteExternalResourceLink	
Deleted member of Power BI gateway cluster		
Deleted organizational Power BI content pack	DeleteOrgApp	
Deleted Power BI comment	DeleteComment	

Friendly name	Operation name	Notes
Deleted Power BI dashboard	DeleteDashboard	Not currently used
Deleted Power BI dataflow	DeleteDataflow	Not currently used
Deleted Power BI dataset	DeleteDataset	
Deleted Power BI dataset from external app	DeleteDatasetFromExternalApplication	
Deleted Power BI dataset rows	DeleteDatasetRows	Indicates that the Push Datasets - Datasets DeleteRows API was called
Deleted Power BI email subscription	DeleteEmailSubscription	
Deleted Power BI folder	DeleteFolder	
Deleted Power BI metric	DeleteGoal	
Deleted Power BI folder access	DeleteFolderAccess	Not currently used
Deleted Power BI gateway	DeleteGateway	

Friendly name	Operation name	Notes
Deleted Power BI gateway cluster		
Deleted Power BI gateway cluster datasource	DeleteGatewayClusterDatasource	
Deleted Power BI metric	DeleteGoal	
Deleted Power BI group	DeleteGroup	
Deleted Power BI note	DeleteNote	
Deleted Power BI scorecard	DeleteScorecard	
Deleted Power BI report	DeleteReport	
Deleted Power BI template app	DeleteTemplateApp	
Deleted sensitivity label from Power BI item	SensitivityLabelRemoved	
Deleted snapshot for user in Power BI tenant	DeleteSnapshot	Generated when a user deletes a snapshot that describes a dataset

Friendly name	Operation name	Notes
Deleted workspace for Power BI template app	DeleteTemplateApp	
Deployed to a pipeline stage	DeployAlmPipeline	
Discovered Power BI dataset data sources	GetDatasources	
Downloaded Power BI report	DownloadReport	
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 dataset	EditDataset	
Edited Power BI dataset endorsement	EditDatasetProperties	
Edited Power BI dataset from external app	EditDatasetFromExternalApplication	
Edited Power BI dataset properties	EditDatasetProperties	

Friendly name	Operation name	Notes
Edited Power BI report	EditReport	
Edited Power BI report endorsement	EditReportProperties	
Encrypted credentials for Power BI gateway datasource		
Encrypted credentials using Power BI gateway cluster		
Export Power BI activity events	ExportActivityEvents	
Exported Power BI item to another file format	ExportArtifact	
Exported Power BI dataflow	ExportDataflow	
Exported Power BI report to another file format	ExportReport	
Exported Power BI report visual data	ExportReport	
Exported Power BI tile data	ExportTile	

Friendly name	Operation name	Notes
Generated Power BI dataflow SAS token	GenerateDataflowSasToken	
Generated Power BI Embed Token	GenerateEmbedToken	
Generate screenshot	GenerateScreenshot	
Get Power BI group users	GetGroupUsers	
Get refresh history via lockbox	GetRefreshHistoryViaLockbox	
Imported file to Power BI	Import	
Initiated Power BI gateway cluster authentication process		
Inserted or updated current value connection of Power BI metric	UpsertGoalCurrentValueConnection	
Inserted or updated target value connection of Power BI metric		
Inserted Power BI note	InsertNote	

Friendly name	Operation name	Notes
Inserted snapshot for user in Power BI tenant	InsertSnapshot	Generated when user uploads a snapshot that describes their dataset
Installed Power BI app	InstallApp	
Installed Power BI template app	InstallTemplateApp	
Mapped user principal names for tenant		
Migrated dataflow storage location	MigratedDataflowStorageLocation	
Migrated workspace to a capacity	MigrateWorkspaceIntoCapacity	
Patched Power BI metric	PatchGoal	
Patched Power BI metric value	PatchGoalValue	
Patched Power BI note	PatchNote	
Patched Power BI scorecard	PatchScorecard	
Posted Power BI comment	PostComment	
Printed Power BI Dashboard	PrintDashboard	

Friendly name	Operation name	Notes
Printed Power BI report page	PrintReport	
Promoted Power BI template app	PromoteTemplateAppPackage	
Published Power BI report to web	PublishToWebReport [2]	
Ran Power BI email subscription	RunEmailSubscription	
Received Power BI dataflow secret from Key Vault	ReceiveDataflowSecretFromKeyVault	
Re-encrypted credentials using Power gateway cluster		
Refreshed current value of Power BI metric		
Refreshed target value of Power BI metric		
Removed a workspace from a deployment pipeline	UnassignWorkspaceFromPipeline	
Removed data source from Power BI gateway	RemoveDatasourceFromGateway	

Friendly name	Operation name	Notes
Removed Power BI group members	DeleteGroupMembers	
Removed user from Power BI gateway cluster		
Removed user from Power BI gateway cluster datasource		
Removed workspace from a capacity	RemoveWorkspacesFromCapacity	
Renamed Power BI dashboard	RenameDashboard	
Requested account key for Power BI storage	AcquireStorageAccountKey	
Requested Power BI dataflow refresh	RequestDataflowRefresh	Not currently used
Requested Power BI dataset refresh	RefreshDataset	
Requested Power BI dataset refresh from external app	RefreshDatasetFromExternalApplication	

Friendly name	Operation name	Notes
Requested SAS token for Power BI storage	AcquireStorageSASFromExternalApplication	
Restored Power BI workspace	RestoreWorkspace	
Retrieved all Power BI gateway cluster datasources	GetAllGatewayClusterDatasources	
Retrieved all supported datasources for Power BI gateway cluster		
Retrieved allowed Power BI gateway regions	GetGatewayRegions	
Retrieved authentication details for Power BI gateway cluster datasource		
Retrieved data sources from Power BI dataset	GetDatasetDatasourcesAsAdmin	
Retrieved data sources from Power BI dataflow	GetDataflowDatasourcesAsAdmin	

Friendly name	Operation name	Notes
Retrieved metrics of Power BI scorecard	GetGoal	
Retrieved links between datasets and dataflows	GetDatasetToDataflowsLinksAsAdmin	
Retrieved list of datasource users for Power BI gateway cluster		
Retrieved list of modified workspaces in Power BI tenant	GetModifiedWorkspacesAPI	
Retrieved list of Power BI gateway installer principals		
Retrieved member status of Power BI gateway cluster	GetGatewayClusterMemberStatus	
Retrieved multiple Power BI gateway clusters		
Retrieved multiple Power BI metric values	GetGoalValues	

Friendly name	Operation name	Notes
Retrieved multiple Power BI scorecards	GetScorecards	
Retrieved Power BI app users	GetAppUsersAsAdmin	
Retrieved Power BI apps	GetAppsAsAdmin	
Retrieved Power BI apps for user	GetUserAppsAsAdmin	
Retrieved Power BI capacities for user	GetUserCapacitiesAsAdmin	
Retrieved Power BI capacity users	GetCapacityUsersAsAdmin	
Retrieved Power BI dashboards	GetDashboardsAsAdmin	
Retrieved Power BI dashboard tiles	GetDashboardTilesAsAdmin	
Retrieved Power BI dashboard users	GetDashboardUsersAsAdmin	
Retrieved Power BI dashboards for user	GetUserDashboardsAsAdmin	
Retrieved Power BI dataflows	GetDataflowsAsAdmin	

Friendly name	Operation name	Notes
Retrieved Power BI dataflows for user	GetUserDataflowsAsAdmin	
Retrieved Power BI datasets	GetDatasetsAsAdmin	
Retrieved Power BI datasets for user	GetUserDatasetsAsAdmin	
Retrieved Power BI data sources for user	GetUserDatasourcesAsAdmin	
Retrieved Power BI gateway cluster datasource		
Retrieved Power BI gateway cluster datasources		
Retrieved Power BI gateway datasource users	GetDatasourceUsersAsAdmin	
Retrieved Power BI gateway tenant key		
Retrieved Power BI gateway tenant policy		

Friendly name	Operation name	Notes
Retrieved Power BI gateway users	GetGatewayUsersAsAdmin	
Retrieved Power BI gateways for user	GetUserGatewaysAsAdmin	
Retrieved Power BI metric	GetGoal	
Retrieved Power BI metric value	GetGoalValue	
Retrieved Power BI group users	GetGroupUsersAsAdmin	
Retrieved Power BI groups for user	GetUserGroupsAsAdmin	
Retrieved Power BI imports	GetImportsAsAdmin	
Retrieved Power BI refresh history	GetRefreshHistory	
Retrieved Power BI refreshable by ID	GetRefreshablesForRefreshIdAsAdmin	
Retrieved Power BI refreshables	GetRefreshablesAsAdmin	
Retrieved Power BI refreshables for capacity	GetRefreshablesForCapacityAsAdmin	

Friendly name	Operation name	Notes
Retrieved Power BI report users	GetReportUsersAsAdmin	
Retrieved Power BI reports for user	GetUserReportsAsAdmin	
Retrieved Power BI scorecard	GetScorecard	
Retrieved Power BI scorecard by using report ID	GetScorecardByReportId	
Retrieved Power BI tenant keys	GetTenantKeysAsAdmin	
Retrieved Power BI workspaces	GetWorkspaces	
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 dataset such as when a user visits the data hub
Retrieved status of Power BI gateway cluster	GetGatewayClusterStatus	

Friendly name	Operation name	Notes
Retrieved status of Power BI gateway cluster datasource		
Retrieved upstream dataflows from Power BI dataflow	GetDataflowUpstreamDataflowsAsAdmin	
Rotated Power BI gateway tenant key		
Sent a scan request in Power BI tenant	GetWorkspacesInfoAPI	
Set dataflow storage location for a workspace	SetDataflowStorageLocationForWorkspace	
Set scheduled refresh on Power BI dataflow	SetScheduledRefreshOnDataflow	
Set scheduled refresh on Power BI dataset	SetScheduledRefresh	
Shared Power BI dashboard	ShareDashboard	
Shared Power BI dataset	ShareDataset	
Shared Power BI report	ShareReport	

Friendly name	Operation name	Notes
Started Power BI extended trial	OptInForExtendedProTrial	Not currently used
Started Power BI trial	OptInForProTrial	
Tested Power BI gateway datasource connection with single sign-on		
Took over a Power BI datasource	TakeOverDatasource	
Took over Power BI dataset	TakeOverDataset	
Took ownership of Power BI dataflow	TookOverDataflow	
Unpublished Power BI app	UnpublishApp	
Update capacity resource governance settings	UpdateCapacityResourceGovernanceSettings	Not currently in Microsoft 365 admin center
Updated an organizational custom visual	UpdateOrganizationalGalleryItem	
Updated capacity admin	UpdateCapacityAdmins	
Updated capacity display name	UpdateCapacityDisplayName	

Friendly name	Operation name	Notes
Updated capacity custom settings	UpdateCapacityCustomSettings	
Updated credentials for Power BI gateway cluster		
Updated dataflow storage assignment permissions	UpdatedDataflowStorageAssignmentPermissions	
Updated deployment pipeline access	UpdateAlmPipelineAccess	
Updated deployment pipeline configuration	SetConfigurationAlmPipeline	
Updated featured tables	UpdateFeaturedTables [3]	
Updated organization's Power BI settings	UpdatedAdminFeatureSwitch	
Updated parameters for installed Power BI template app	UpdateInstalledTemplateAppParameters	
Updated Power BI access request settings		

Friendly name	Operation name	Notes
Updated Power BI app	UpdateApp	
Updated Power BI dataflow	UpdateDataflow	
Updated Power BI dataset data sources	UpdateDatasources	
Updated Power BI dataset parameters	UpdateDatasetParameters	
Updated Power BI discoverable model settings	UpdateDiscoverableModelSettings	Generated when a report is set to feature on home
Updated Power BI gateway data source credentials	UpdateDatasourceCredentials	
Updated Power BI email subscription	UpdateEmailSubscription	
Updated Power BI folder	UpdateFolder	
Updated Power BI folder access	UpdateFolderAccess	
Updated Power BI gateway cluster datasource		

Friendly name	Operation name	Notes
Updated Power BI gateway data source credentials	UpdateDatasourceCredentials	
Updated Power BI workspace	UpdateWorkspace	
Updated Power BI workspace access	UpdateWorkspaceAccess	
Updated snapshots for user in Power BI tenant	UpdateSnapshot	Generated when user updates snapshots that describe their datasets
Updated the Power BI gateway		
Updated the Power BI datasource		
Updated settings for Power BI template app	UpdateTemplateAppSettings	
Updated testing permissions for Power BI template app	UpdateTemplateAppTestPackagePermissions	
Updated workspace Analysis Services settings	SetASSeverPropertyOnWorkspaceFromExternalApplicationDetailedInfo	

Friendly name	Operation name	Notes
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	

[1] Publishing from Power BI Desktop to the service is a CreateReport event in the service.

[2] PublishToWebReport refers to the Publish to web feature.

[3] UpdateFeaturedTables refers to Power BI featured tables in Excel.

[4] Publishing from Power BI Report Builder to the service doesn't record an event.

Next steps

- What is Power BI administration?
- Power BI Admin Portal
- Access the Power BI activity log
- Questions? Try asking the Power BI Community
- Suggestions? Contribute ideas to improve Power BI

Set up Data in space for your organization (preview)

Article • 07/19/2022 • 3 minutes to read

Data in space is a feature of the Power BI mobile apps that enables Power BI reports to be pinned in augmented reality to real-world locations, where the people who need to access those reports on location can find them.

When Data in space is set up, specified people in the organization can pin reports to locations in the real world. Using the Power BI mobile app's camera, they scan and map a location and pin a report there. Afterwards, the people who need to access the report can scan the area with their mobile app's camera and find the pinned reports in augmented reality at the place they were pinned. They can then tap the report to open it. For more information about Data in space, see the Data in space overview.

This article explains how to set up Data in space in your organization. Data in space uses Azure Spatial Anchors for storing location-mapping data, so the article includes references and notes concerning creating and configuring the required Azure Spatial Anchors resource.

See Next steps for a general overview of the Data in space feature, or for information about pinning, finding, and accessing data in space.

Setup overview

Setting up Data in space for your organization involves three steps:

1. Creating an Azure Spatial Anchors resource.
2. Connecting Power BI to the Azure Spatial Anchors resource.
3. Assigning users in the organization to roles so that they can use the Data in space feature.

Step 1 must be performed first. Steps 2 and 3 can be performed in any order.

Supported operating systems

Data in space is currently supported for iOS.

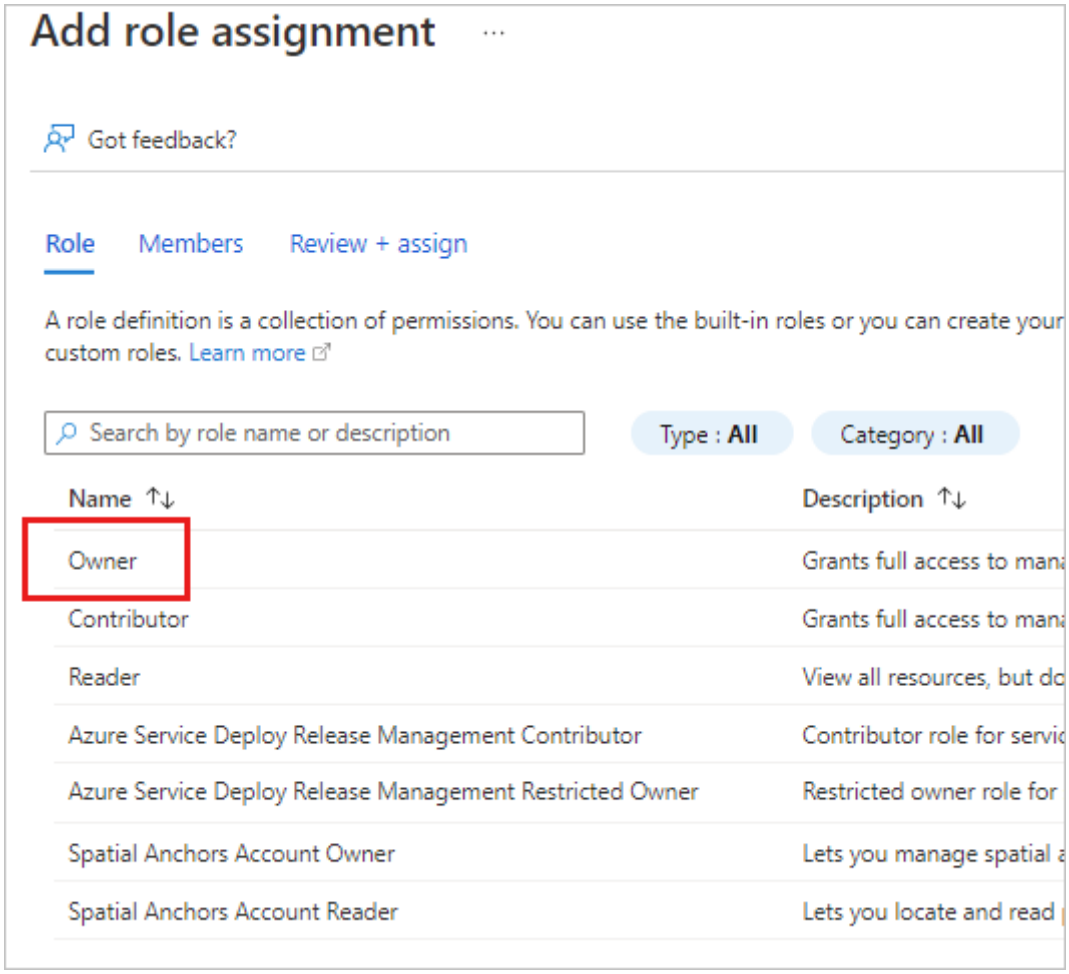
Create an Azure Spatial Anchors resource

This step requires that you have a role that gives you `Microsoft.Authorization/roleAssignments/write` permissions, such as **User Access Administrator** or **Owner**. For more information, see Assign Azure roles using the Azure portal.

In the Azure portal, create an Azure Spatial Anchor resource for Power BI. See Create an Azure Spatial Anchors account for detail.

When configuring the resource:

- Be sure to assign the **Owner** role to the Power BI admin who, in step 2, is going to connect Power BI to the Azure Spatial Anchors resource you're creating.



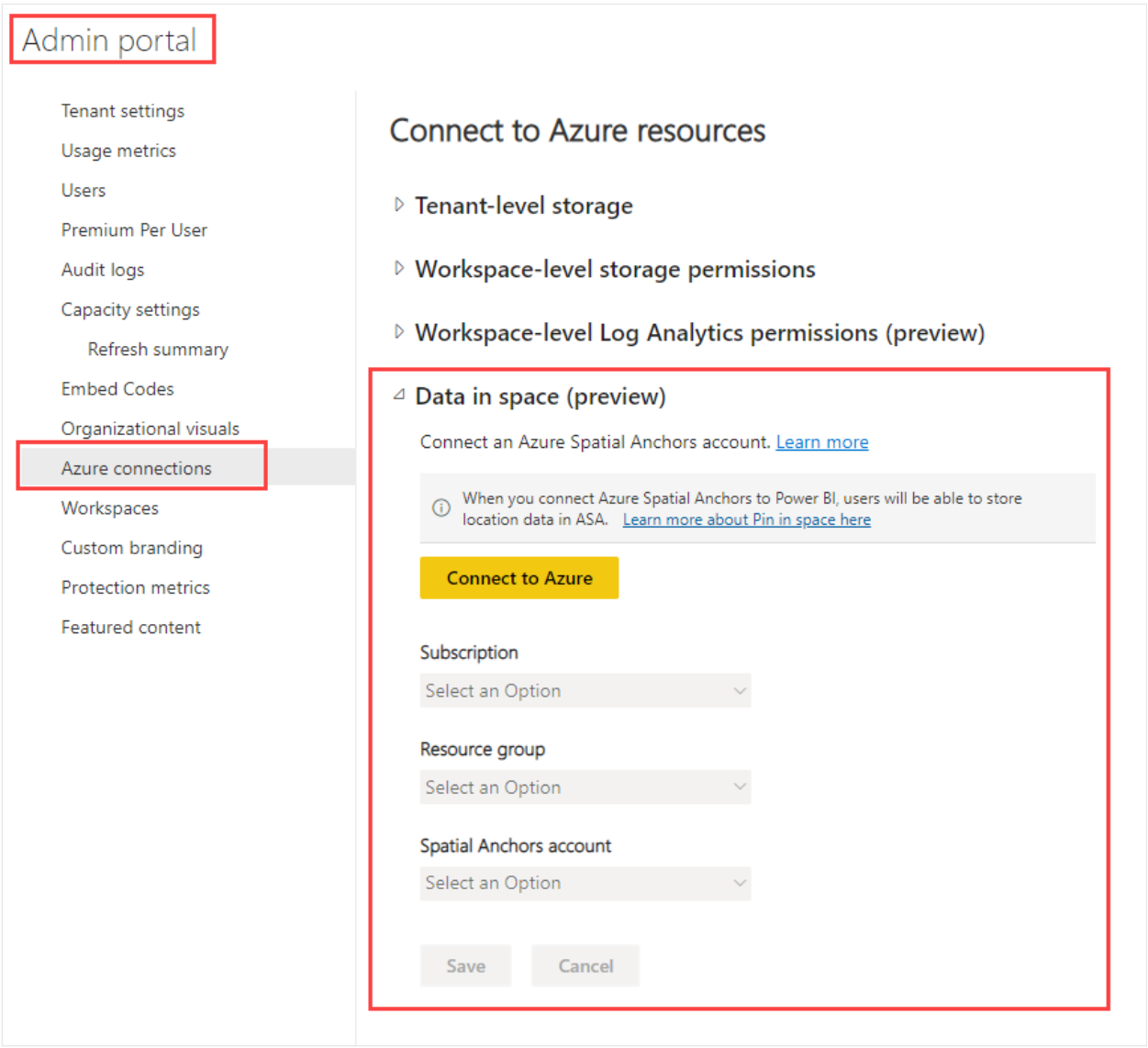
- Be sure that the person who is going to assign users roles in step 3 has a role in the Azure Spatial Anchors resource that gives them `Microsoft.Authorization/roleAssignments/write` permissions, such as **User Access Administrator** or **Owner**. For more information, see Assign Azure roles using the Azure portal.

Connect Power BI to the Azure Spatial Anchors resource

This step requires that you have both of the following:

- A Power BI administrator role in Power BI.
- An Owner role in the Azure Spatial Anchors resource.

Go to **Admin portal** > **Azure Connections** > **Data in space (preview)** and add the connection details.



> ⓘ **Note**
>
> You can connect Power BI to only one Azure Spatial Anchors service.

Assign users to Spatial Anchors Account roles in the Azure Spatial Anchors resource

In this step, you assign users in the organization to roles that will enable them to use the data in space feature.

To perform this step, you must have a role in the Azure Spatial Anchors resource that gives you `Microsoft.Authorization/roleAssignments/write` permissions, such as **User Access Administrator** or **Owner**. For more information, see Assign Azure roles using the Azure portal.

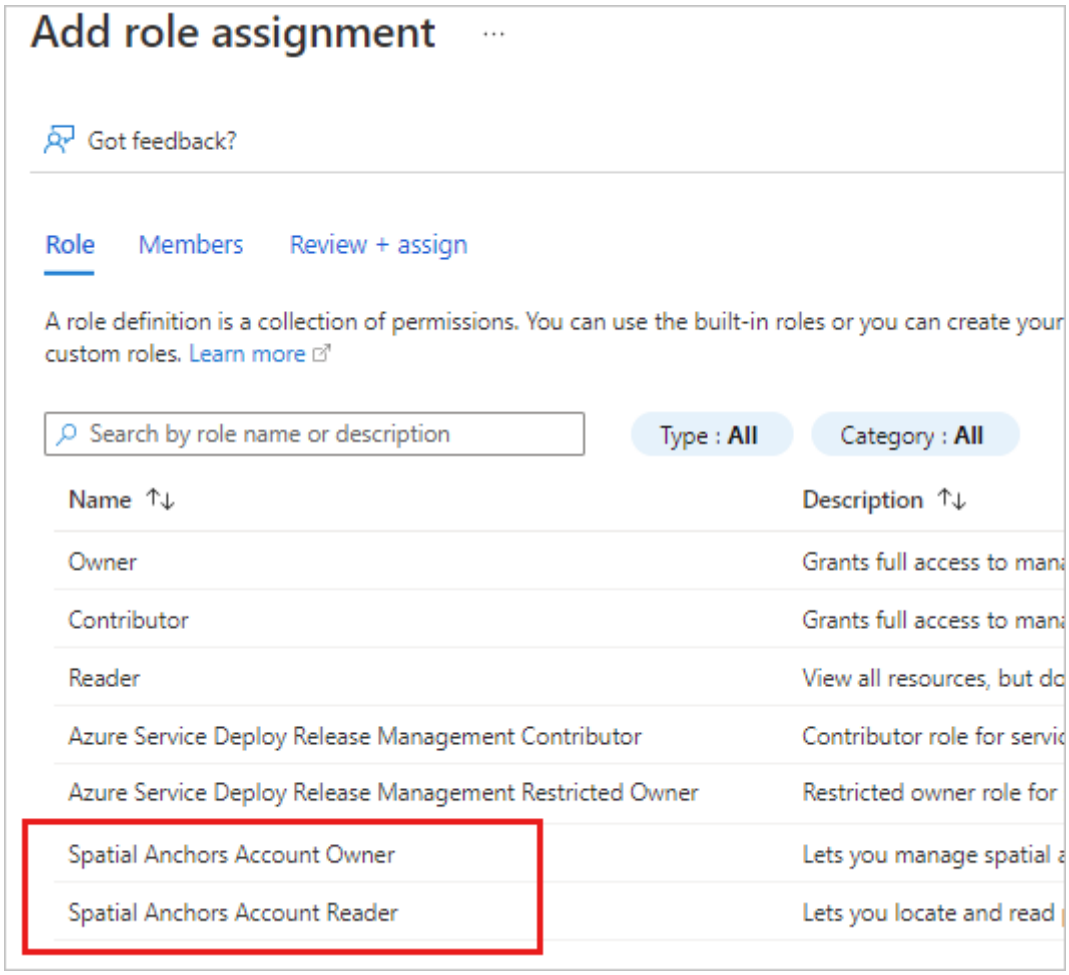
After the Azure Spatial Anchors resource has been created, assign users to Spatial Anchors Account roles in the Azure Spatial Anchors resource:

- If you want a user to be able to create, edit, scan and delete anchors in Power BI mobile app, assign them the **Spatial Anchors Account Owner** role. Users with this role will get the "Data in Space Writer" role in the mobile app.

  > **ⓘ Important**
  >
  > Do not confuse the **Spatial Anchors Account Owner** that you assign users to in this step with the **Owner** role in the Azure Spatial Anchors resource that gives you the write permissions you need to perform this step.

- If you want a user only to be able to scan/search for anchors created by others. assign them the **Spatial Anchors Account Reader** role. Users with this role will get the "Data in Space Reader" role in the mobile app.

The image below shows where to find **Spatial Anchors Account Owner** and **Spatial Anchors Account Reader** roles in the Azure Spatial Anchors resource configuration in the Azure portal.



> **Note**
>
> Only role-assignable groups can be assigned to Spatial Anchors Account roles. For more information about role-assignable groups, see **Create a role-assignable group in Azure Active Directory**.

Next steps

- Data in space overview
- Pin Power BI reports to locations in the real world
- Find and access Power BI reports pinned to locations in the real world

About the admin portal

Article • 10/24/2022 • 2 minutes to read

The admin portal includes settings that govern Power BI for all users in your organization. For example, you can view usage metrics, access the Microsoft 365 admin center, and control how users interact with Power BI.

The full admin portal can be accessed by global admins and users who have the Power BI administrator role. If you're not in one of these roles, you only see **Capacity settings** in the portal. For more information about the Power BI service administrator role, see Understanding the Power BI admin role.

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.

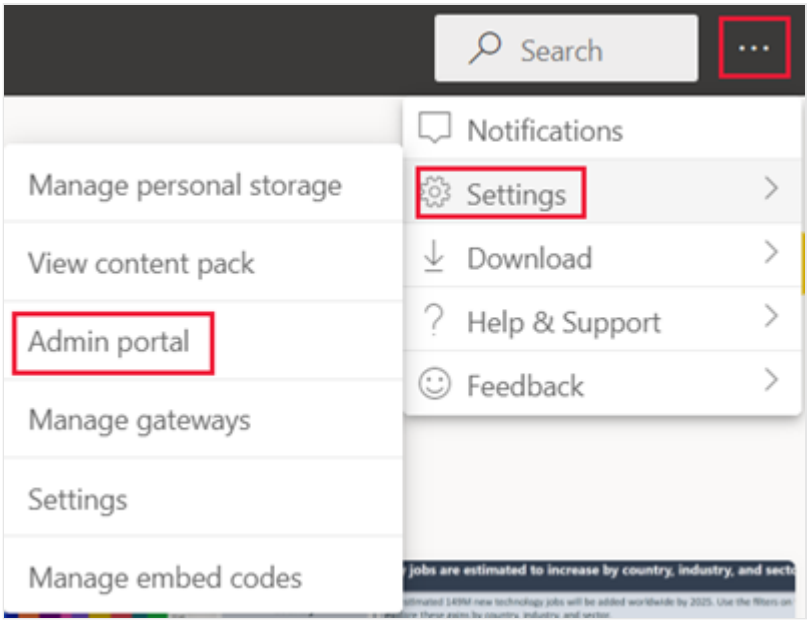
Feature	Description
Tenant settings	Enable, disable, and configure Power BI.
Usage metrics	View metrics about Power BI usage in your organization.
Users	Manage users in the Microsoft 365 admin center.
Premium Per User	Configure auto refresh and dataset workload settings.
Audit logs	Audit Power BI activities in the Microsoft Purview compliance portal.
Capacity settings	Manage any Power BI Premium capacities (EM or P SKU) that have been purchased for your organization
Refresh summary	Schedule refresh on a capacity and also view the details of refreshes that have 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.
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 Power BI service to match your organization's own branding.
Protection metrics	View a metric to monitor and track sensitivity label usage and adoption in your organization.
Featured content	Manage all the reports, dashboards, and apps that have been promoted to the Featured section on Power BI Home across your organization.

How to get to the admin portal

You must be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding the Power BI admin role. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI using your admin account credentials.
2. From the page header, select ... > **Settings** > **Admin portal**.



Next steps

About tenant settings

Manage Azure connections

Article • 12/19/2022 • 2 minutes to read

The Azure connections admin settings connect Azure services to Power BI. 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.

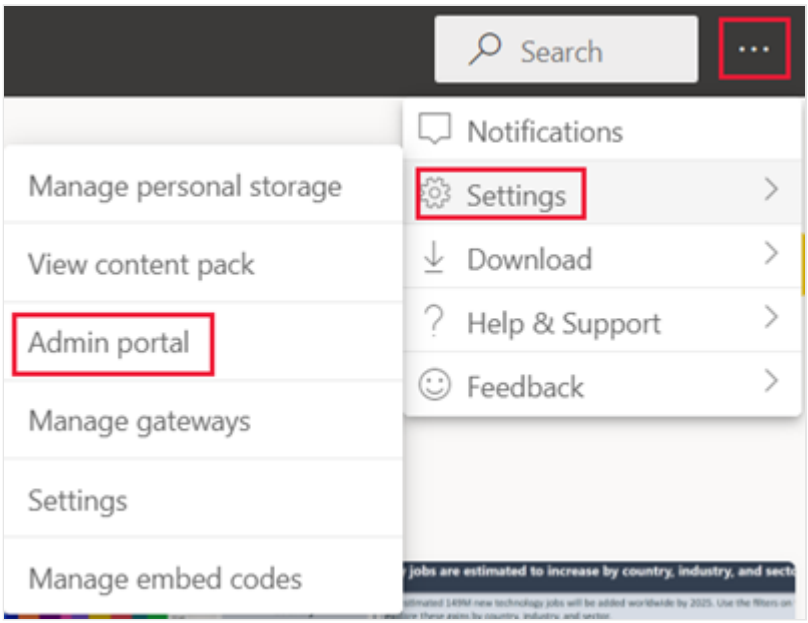
The Azure connections admin settings have the following options:

- 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.

Access the Power BI admin portal settings

You have to be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI by using your admin account credentials.
2. From the page header, select ... > **Settings** > **Admin portal**.



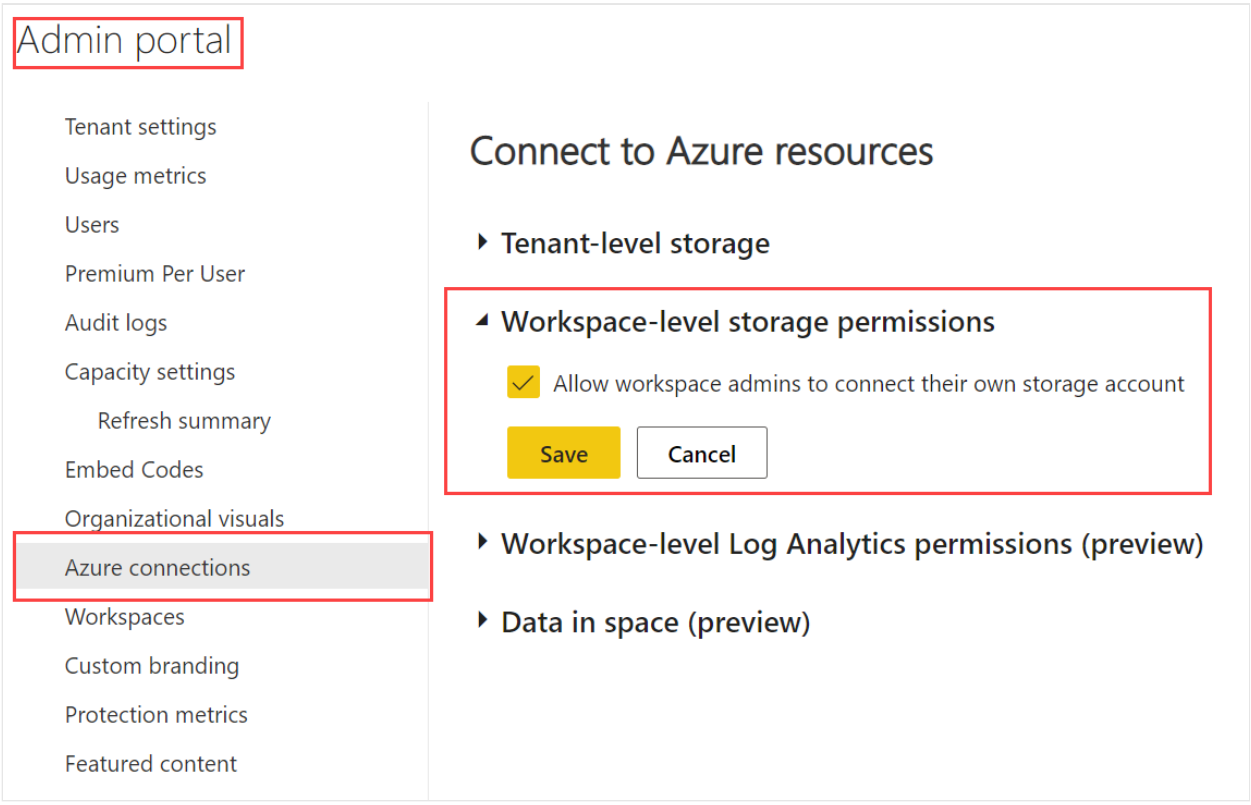
Tenant-level storage

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 Power BI 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.



Next steps

About the Admin portal

Configuring dataflow storage to use Azure Data Lake Gen 2

Add custom branding to the Power BI service

Article • 11/29/2022 • 2 minutes to read

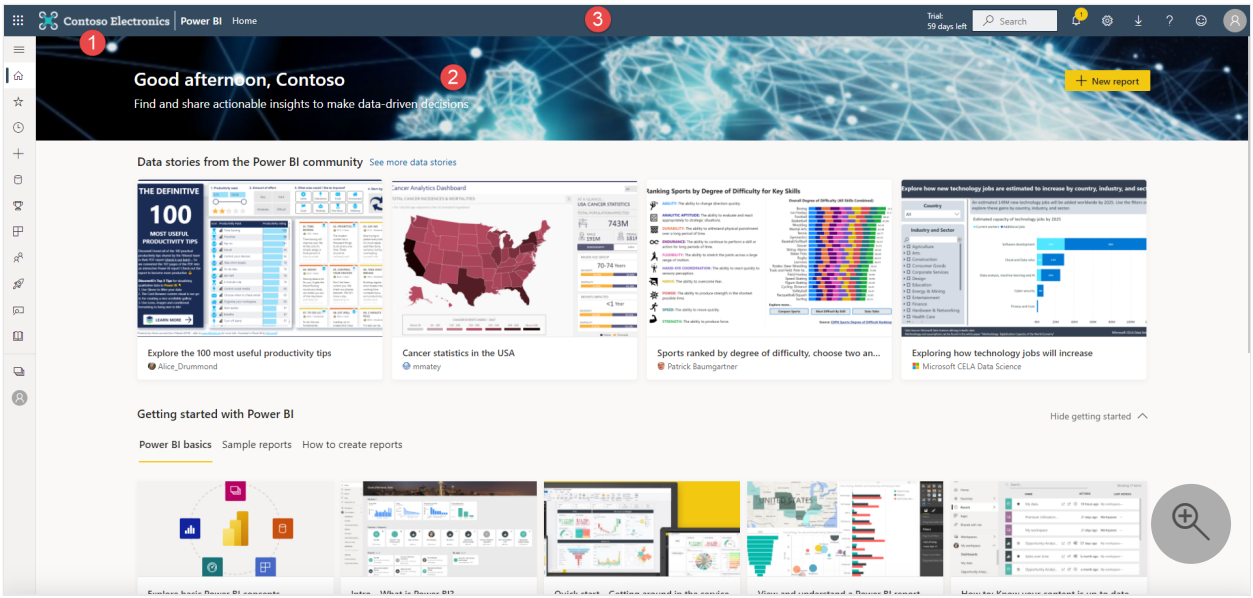
As a Power BI admin, you can change the look and feel of the Power BI service to match your organization's own branding. With custom branding, you can change the theme color that appears in the top navigation bar, add your company logo, and bring your default landing page to life by adding a cover image.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

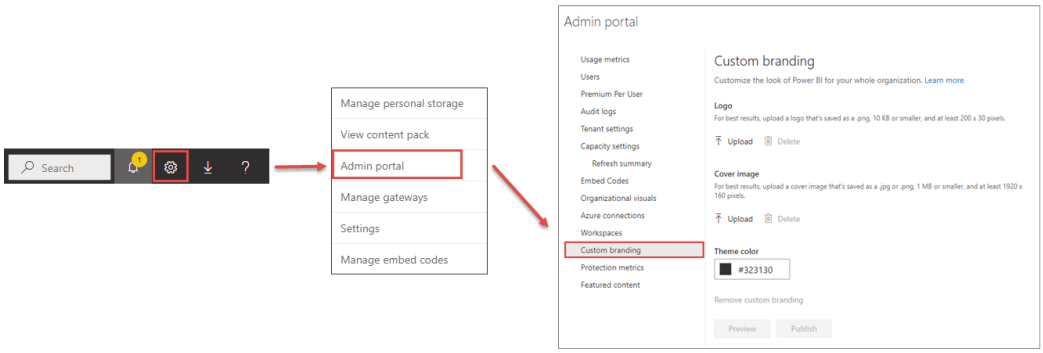


Add custom branding

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

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

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



3. Upload a logo file.

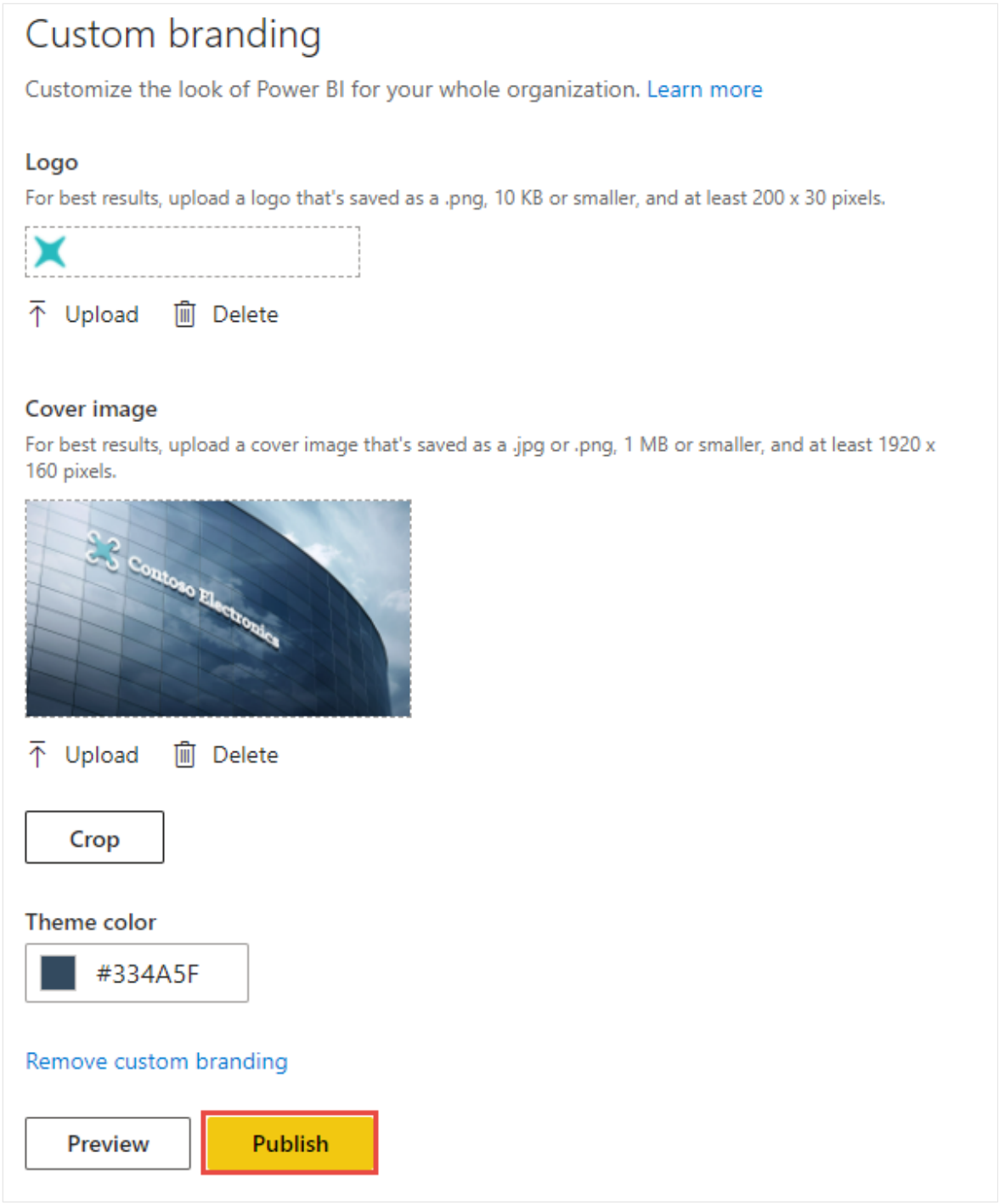
4. Upload a cover image file, then crop as needed to adjust how the image appears on the page.

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 Power BI 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.

Next steps

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 Azure Active Directory sign-in page.

Add branding to your organization's Azure Active Directory sign-in page

Customize the Microsoft 365 theme for your organization

Add featured content to Power BI Home

Manage Capacity settings

Article • 12/08/2022 • 2 minutes to read

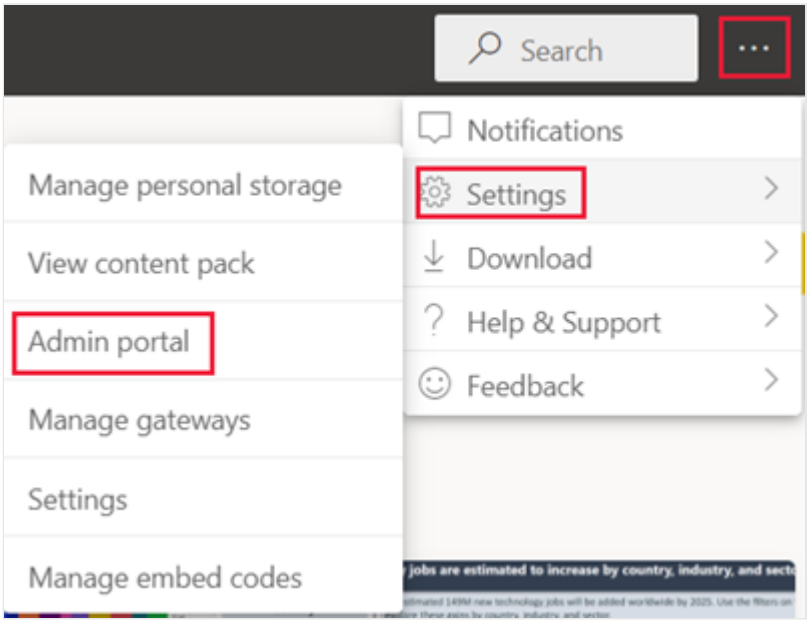
Capacity is a dedicated set of resources reserved for exclusive use. Premium and Embedded capacities offer a dependable and consistent performance for your content. Here are some settings that you can configure when managing your organization's capacity settings:

- Creating new capacities
- Deleting capacities
- Managing capacity permissions
- Changing the size of the capacity

Access the Power BI admin portal settings

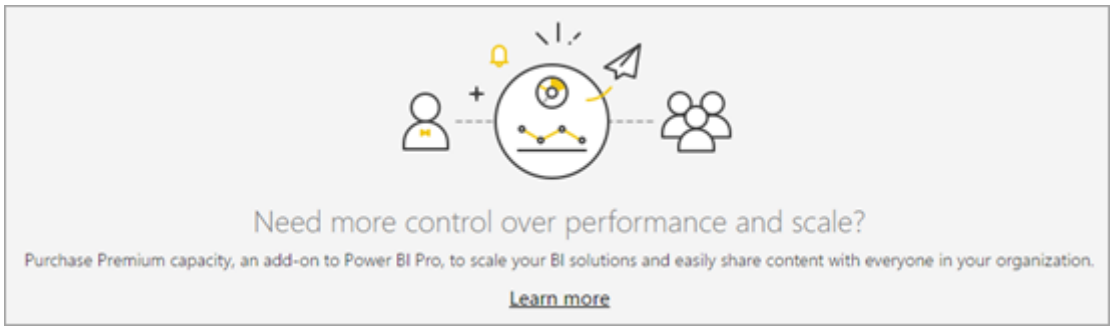
You have to be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI by using your admin account credentials.
2. From the page header, select ... > **Settings** > **Admin portal**.



Power BI Premium

The **Power BI Premium** tab enables you to manage any Power BI Premium capacities (EM or P SKU) that have been purchased for your organization. All users within your organization can see the **Power BI Premium** tab, but they only see contents within it if they're assigned as either a *Capacity admin* or a user that has assignment permissions. If a user doesn't have any permissions, the following message appears:



To understand more about the concepts of capacity management, see Managing Premium Gen2 capacities.

The capacity management process is described in Configure and manage capacities in Power BI Premium.

Power BI Embedded

The **Power BI Embedded** tab enables you to view your Power BI Embedded (A SKU) capacities that you've purchased for your customer. Because you can only purchase A SKUs from Azure, you manage embedded capacities in Azure from **the Azure portal**.

For more information about Power BI Embedded, see:

- Power BI Embedded SKUs - Capacity and SKUs in Power BI embedded analytics
- Create a Power BI Embedded capacity in Azure - Create Power BI Embedded capacity in the Azure portal
- Scale a capacity in Azure - Scale your Power BI Embedded capacity in the Azure portal
- Pause and start a capacity Azure - Pause and start your Power BI Embedded capacity in the Azure portal

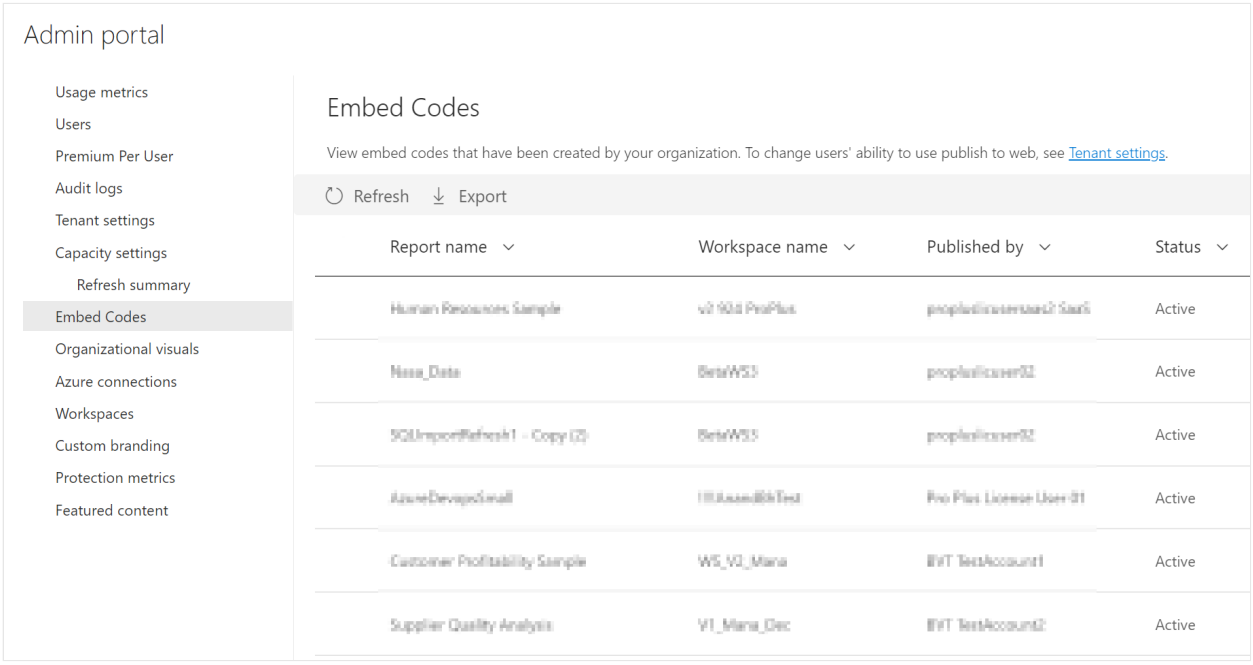
Next steps

About the Admin portal

Manage embed codes

Article • 06/20/2022 • 2 minutes to read

As an 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.

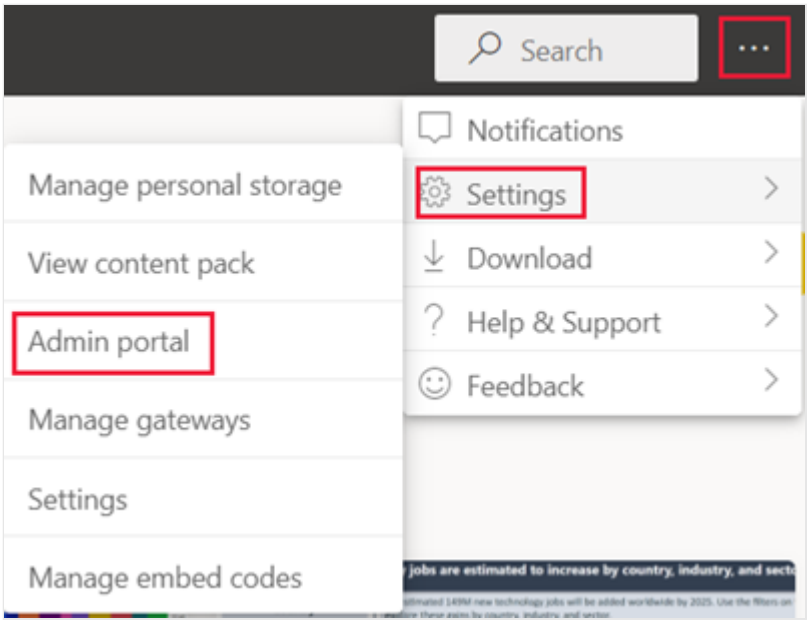


Access the Power BI admin portal settings

You have to be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI by using your admin account credentials.

2. From the page header, select ... > **Settings** > **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 will 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**.

Next steps

- Publish to web from Power BI
- Publish to web
- About the Admin portal

Manage featured content

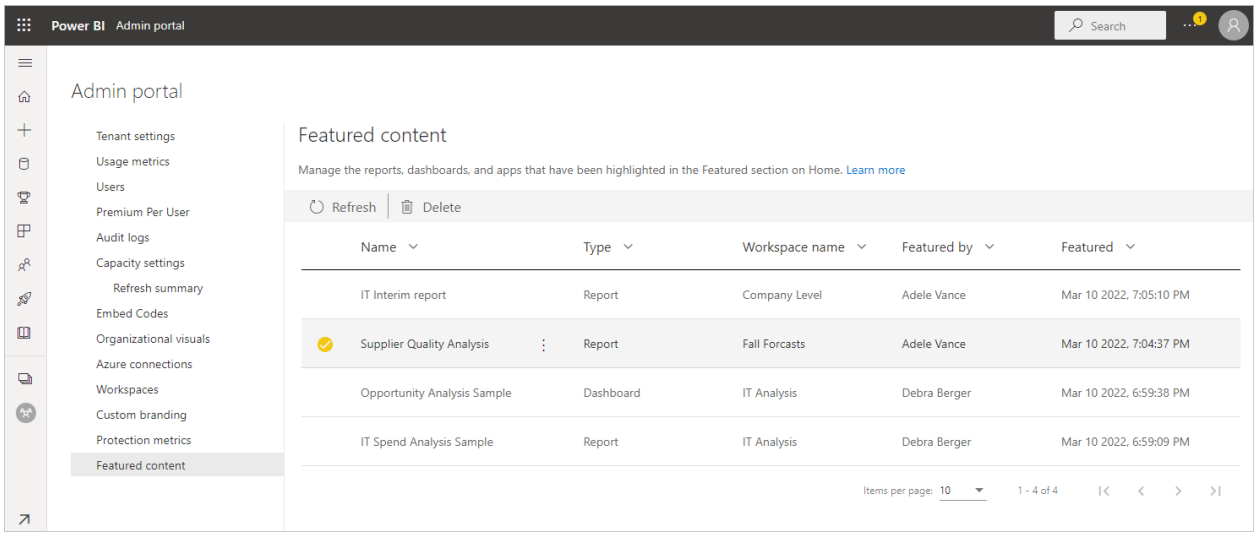
Article • 06/14/2022 • 2 minutes to read

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 Power BI 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 Enable/disable featured content below.

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, mouseover and select the item, and then click the trash can that appears in the top ribbon, or choose **More options (...)** > **Delete**. It is 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. See Featured content for detail.

Next steps

- Enable/disable featured content
- Feature content on colleagues' Power BI Home page
- About the Admin portal

Manage organizational visuals

Article • 12/19/2022 • 2 minutes to read

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.

Next steps

About the Admin portal

Manage Power BI visuals admin settings

Manage Premium Per User

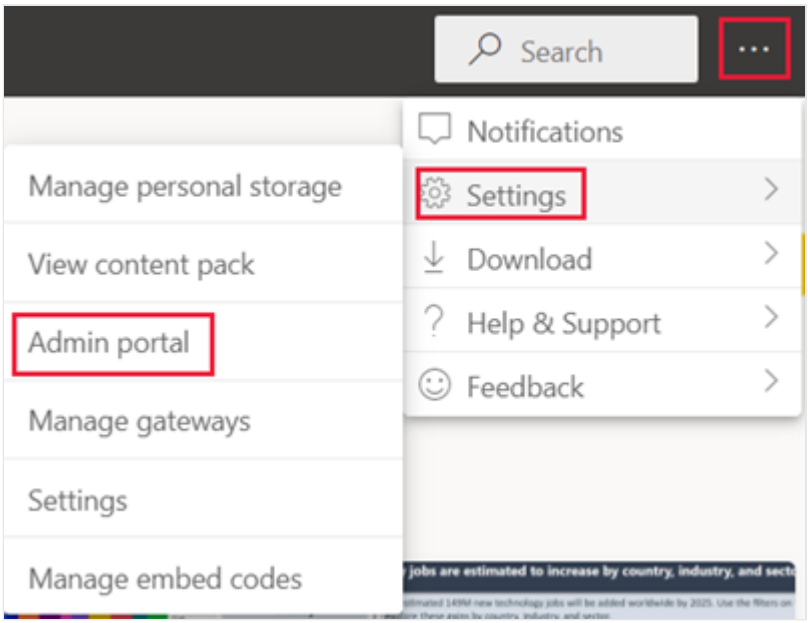
Article • 12/19/2022 • 2 minutes to read

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 dataset 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.

Access the Power BI admin portal settings

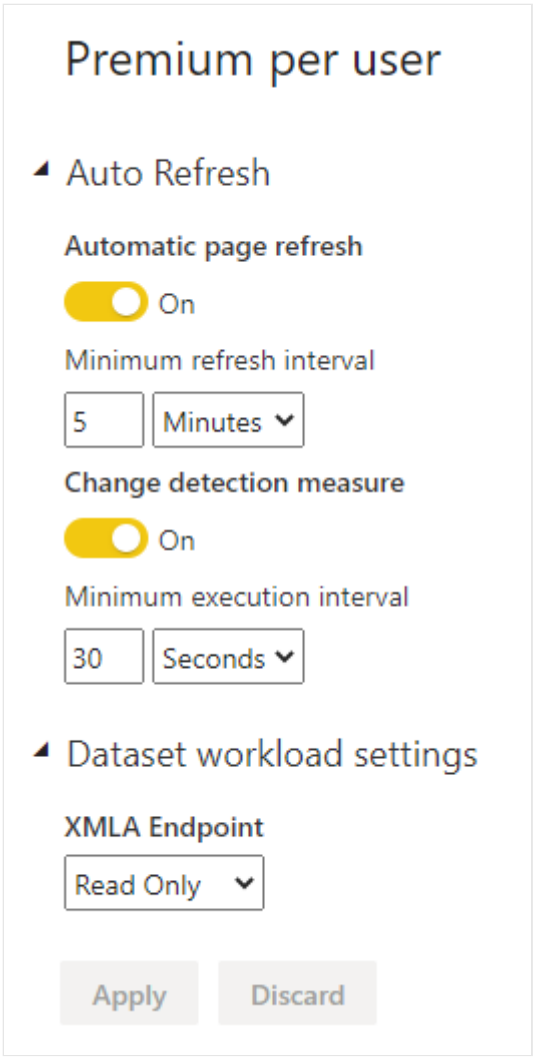
You have to be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI by using your admin account credentials.
2. From the page header, select ... > **Settings** > **Admin portal**.



PPU settings

You can configure the following PPU settings in the admin portal on the **Premium Per User** tab.



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 won'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 will be 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. Power BI service will override 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. Power BI service will override any change detection settings that are higher than this setting.

Dataset workload settings

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

Next steps

About the Admin portal

Power BI Premium Per User FAQ

Automatic page refresh in Power BI

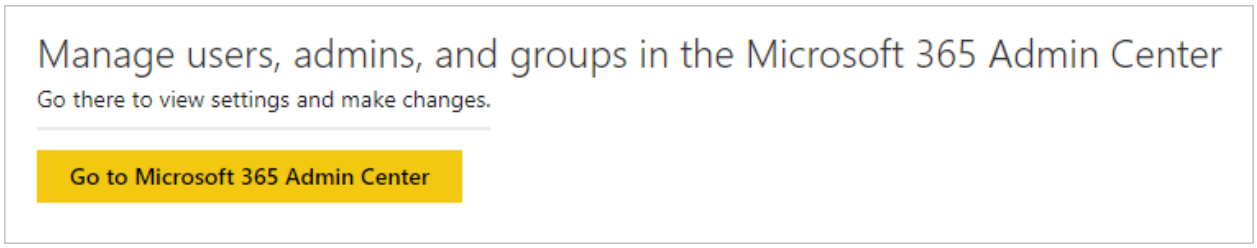
Dataset connectivity with the XMLA endpoint

Manage users

Article • 12/05/2022 • 2 minutes to read

Go to the **Admin portal** to access this feature. For information about how to get to and use the Admin portal, see About the Admin portal.

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



Next steps

- About the Admin portal

View audit logs

Article • 11/22/2022 • 2 minutes to read

Go to the **Admin portal** to access this feature. For information about how to get to and use the Admin portal, see About 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.

To use audit logs, make sure the **Create audit logs for internal activity auditing and compliance** setting is enabled.

Next steps

- About the Admin portal

View information protection metrics

Article • 06/14/2022 • 2 minutes to read

After you enable information protection for Power BI, data protection metrics can be displayed in the admin portal. The report shows how sensitivity labels help protect your content.

Opening the protection metrics report

You must have a Power BI administrator role to open and view the report. To view the report, go to **Settings** > **Admin portal**, and choose **Protection metrics**.

See Data protection metrics report for details about the report.

Next steps

- Data protection metrics report
- Sensitivity labels in Power BI
- About the Admin portal

View refresh summary

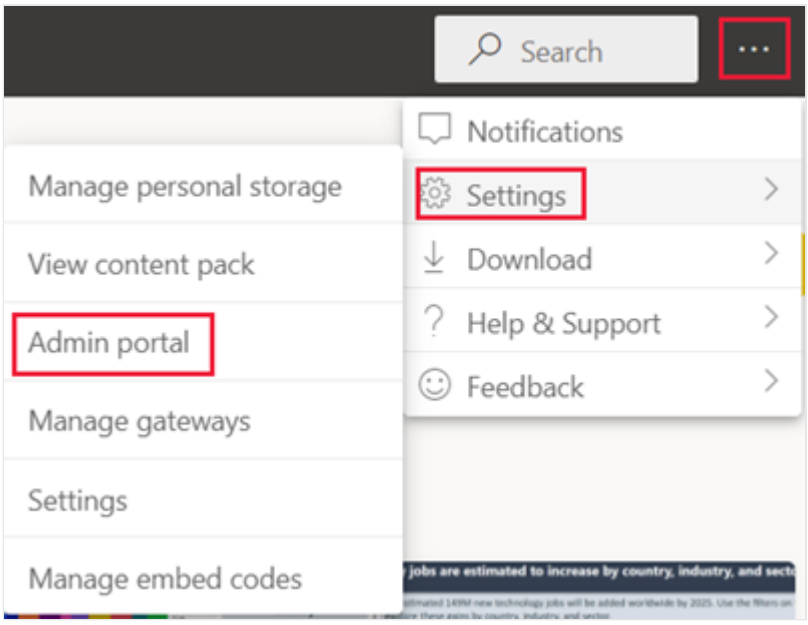
Article • 06/20/2022 • 2 minutes to read

The refresh summary admin settings page, lets you view your capacity's refresh history. You can also export the refresh history, and view additional 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.

Access the Power BI admin portal settings

You have to be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI by using your admin account credentials.
2. From the page header, select ... > **Settings** > **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 additional 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.

Next steps

About the Admin portal

View usage metrics

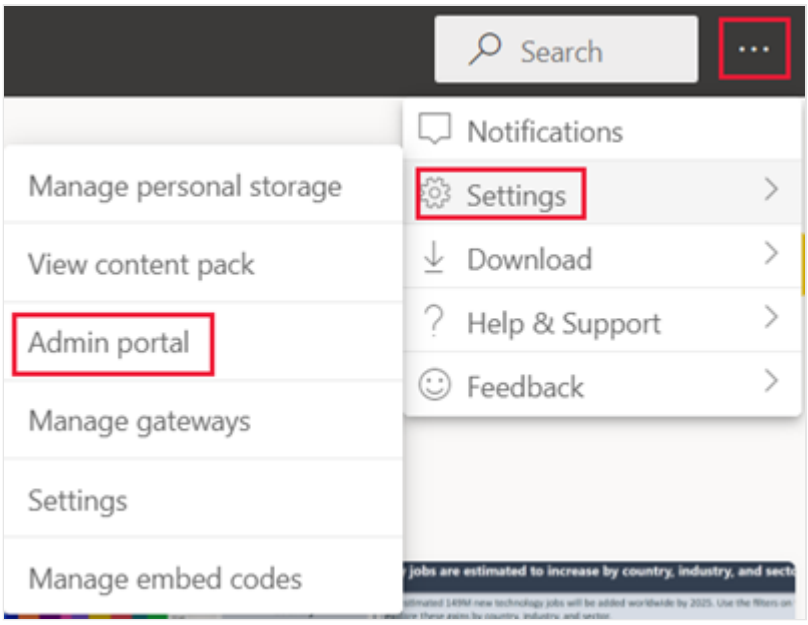
Article • 11/22/2022 • 2 minutes to read

The *usage metrics* page in the Power BI admin settings allows you to monitor Power BI usage for your organization. It also shows which users and groups in your organization are the most active in Power BI. With this information, you can get real insights into how people are using Power BI across your organization.

Access the Power BI admin portal settings

You have to be a global admin or Power BI service admin to access the Power BI admin portal. For more information about the Power BI service administrator role, see Understanding Power BI administrator roles. To get to the Power BI admin portal, follow these steps:

1. Sign in to Power BI by using your admin account credentials.
2. From the page header, select ... > **Settings** > **Admin portal**.



Usage metrics dashboard

The first time you access the dashboard, or when you revisit after a long period of not viewing the dashboard, you might see a loading screen before the dashboard appears. After the dashboard loads, you see two sections of tiles. The first section, at the top of the page, includes usage data for individual users. The second section, at the bottom of the page, has similar information for groups. This section lets you see which groups in your organization are most active and what kind of content they're consuming.

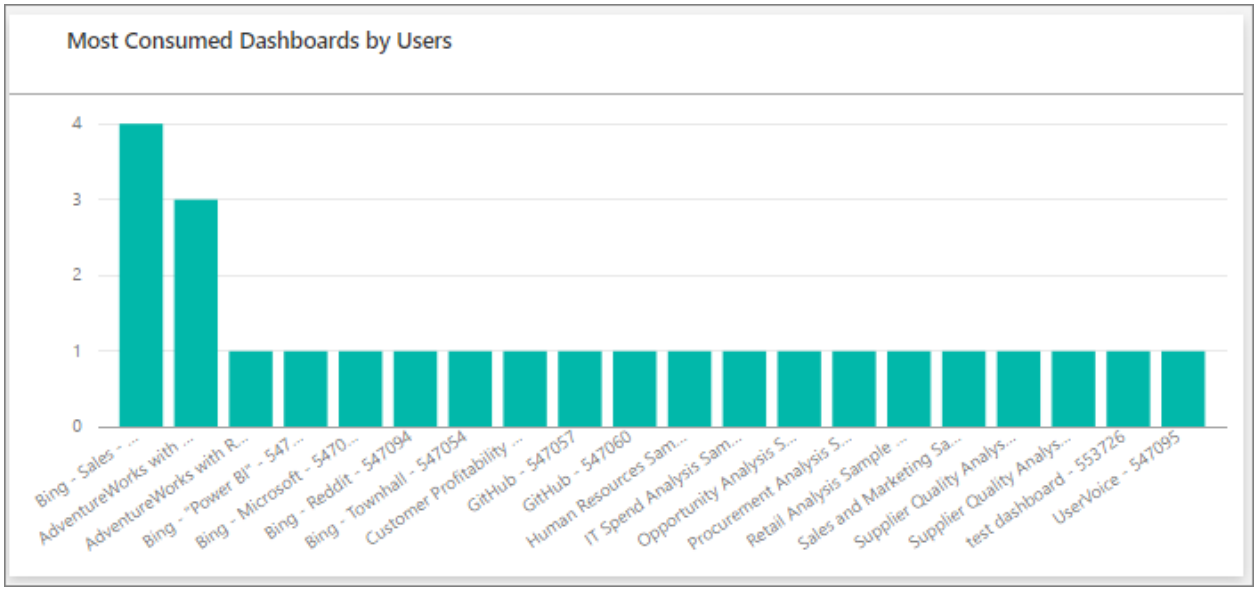
The following sections of the article show a breakdown of what you can see in each tile.

Number of users

This tile is in the first section of the report. It shows a distinct count of all dashboards, reports, and datasets in a workspace, and it refers to users. The second section of the report contains a similar tile that refers to groups.

Consumed dashboards

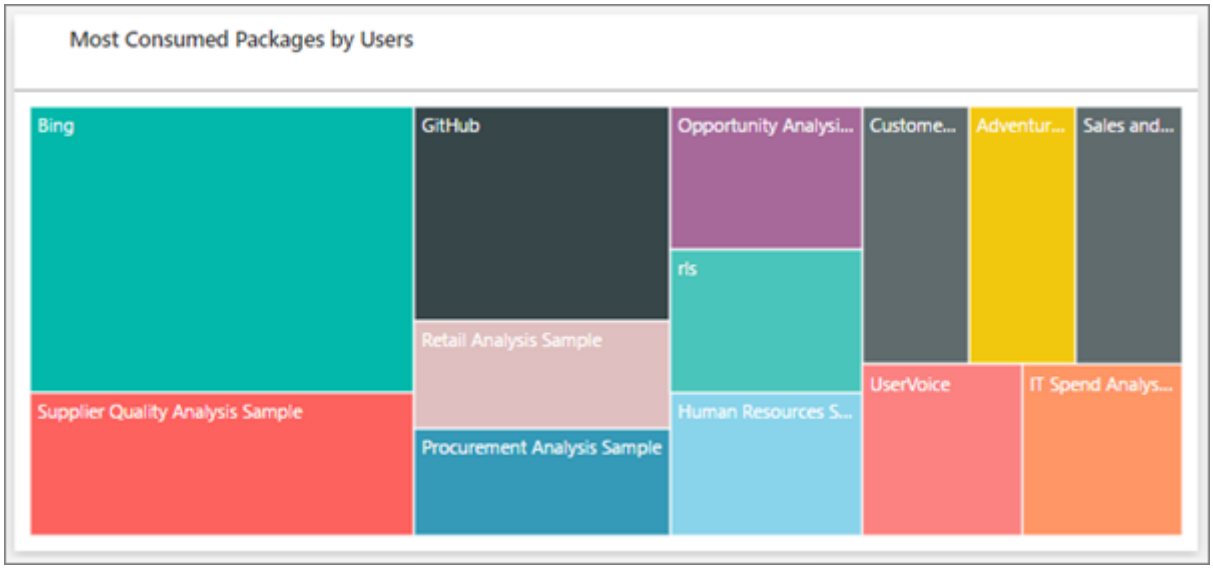
This tile shows a list of the most consumed dashboards. The tile in the first section refers to the number of users who consumed the dashboards. The report's second section has a similar tile that refers to the number of groups. For example, if you have a dashboard that you shared with three users and you also added it to an app that two different users connected to, the dashboard's count would be six: you, three shared users, and two app users.



Consumed packages

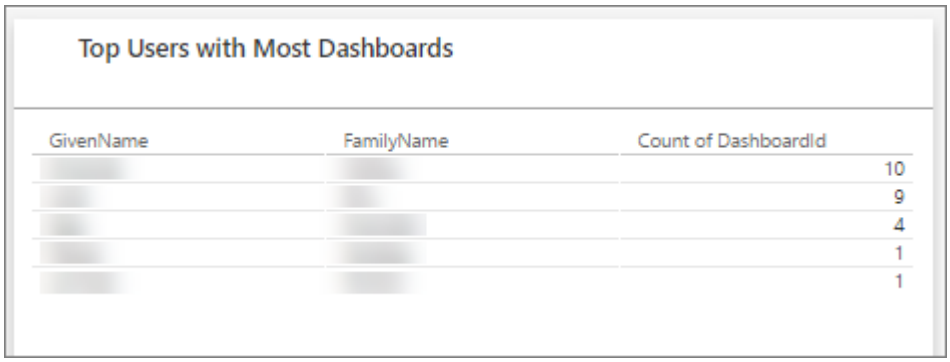
This tile shows a breakdown of the most popular content. The tile in the first section shows content users connected to. The report the second section shows a tile that

displays content groups connected to. The content includes anything the users could reach using the Get Data process, such as SaaS template apps, files, or databases.



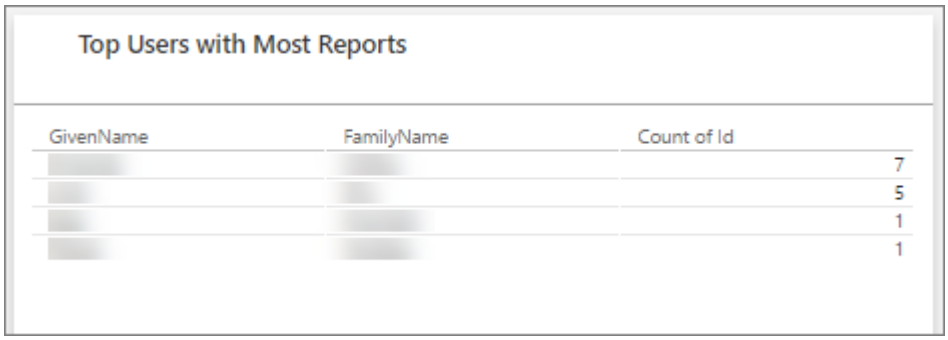
Top users or groups based on dashboards

This tile shows a view of your top users based on how many dashboards they have. Each entry includes dashboards they created themselves and dashboards shared with them. The report in the second section shows a tile that displays top groups based on the number of dashboards they have.



Top users or groups based on reports

This tile shows a view of your top users based on how many reports they have. The report in the second section shows a tile that displays top groups based on the number of reports they have.



Next steps

About the admin portal

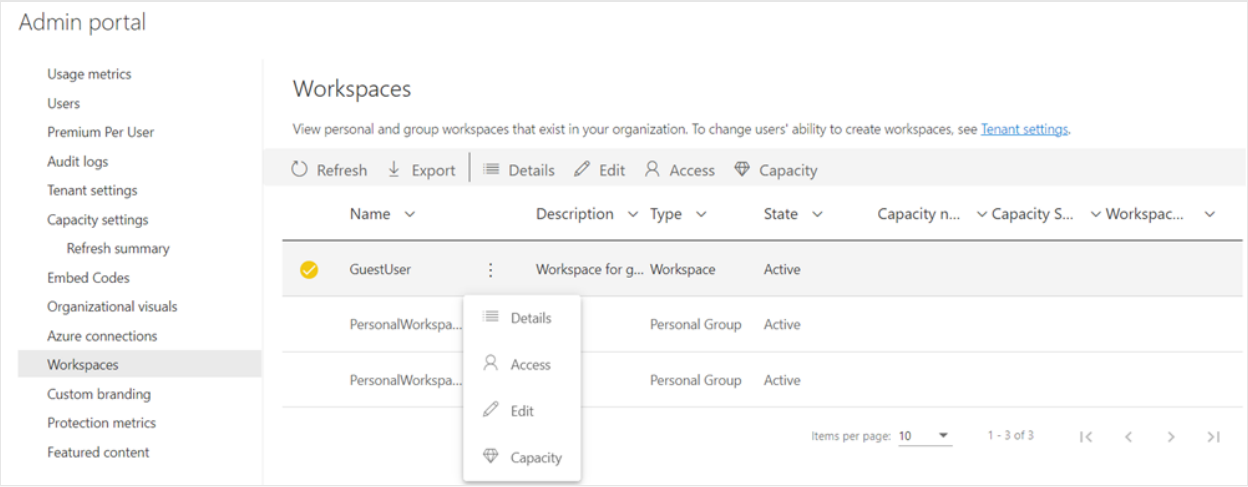
View workspaces

Article • 11/24/2022 • 2 minutes to read

Go to the **Admin portal** to access this feature. For information about how to get to and use the Admin portal, see About the Admin portal.

As an administrator, you can view the workspaces that exist in your organization on the **Workspaces** tab. On this tab, you can perform these actions:

- Refresh the list of workspaces and their details.
- Export the data about the workspaces to a .csv file.
- See details about a workspace, including its ID, its users and their roles, and its dashboards, reports, and datasets.
- Edit the list of people who have 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.
- Edit the Name and Description fields.
- Upgrade classic workspaces to the new workspace experience.



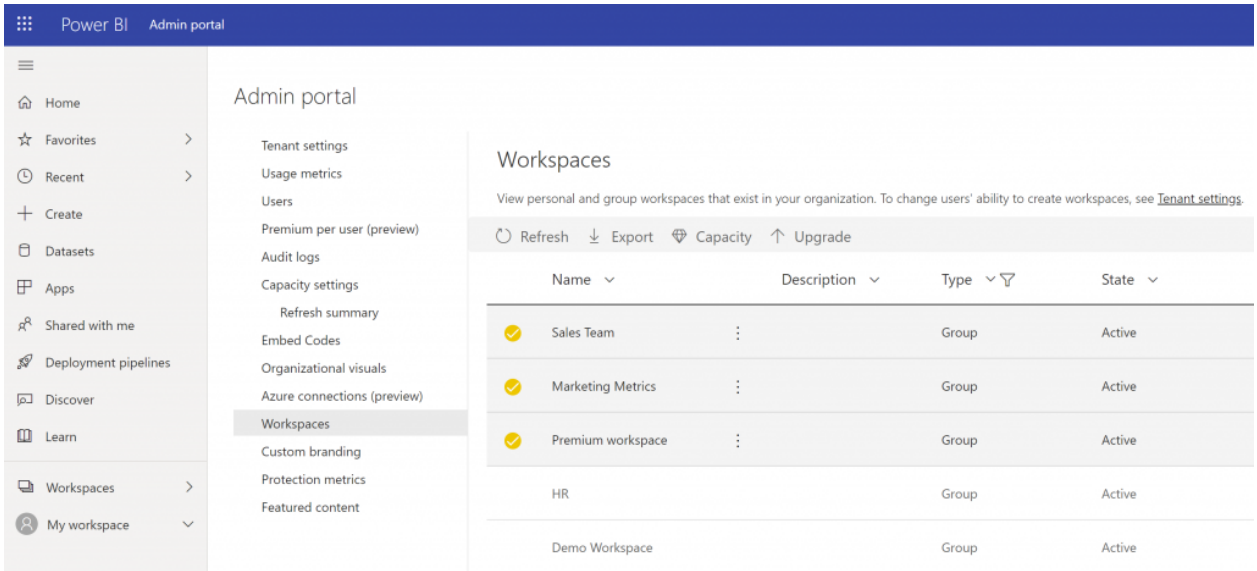
Admins can also control users' ability to create new workspace experience workspaces, and classic workspaces. See Workspace settings in this article for details.

The table columns on the **Workspaces** tab correspond to the properties returned by the Power BI admin Rest API for workspaces. Personal workspaces are of type **PersonalGroup**, classic workspaces are of type **Group**, and the new workspace experience workspaces are of type **Workspace**. For more information, see Workspaces in Power BI.

On the **Workspaces** tab, you see the *state* for each workspace. The following table gives more details about the meaning of those states.

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 Power BI administrator can restore the workspace up to 90 days after it was deleted. When the 90 days pass, the workspace enters the *Removing* state. If you delete a *MyWorkspace* workspace, it moves to the *Removing* state immediately, without the 90 days grace period.
Removing	After you delete a workspace, and once the 90 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.
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.

Admins can also manage and recover workspaces using either the admin portal or PowerShell cmdlets.



Next steps

- About the Admin portal

About tenant settings

Article • 10/24/2022 • 2 minutes to read

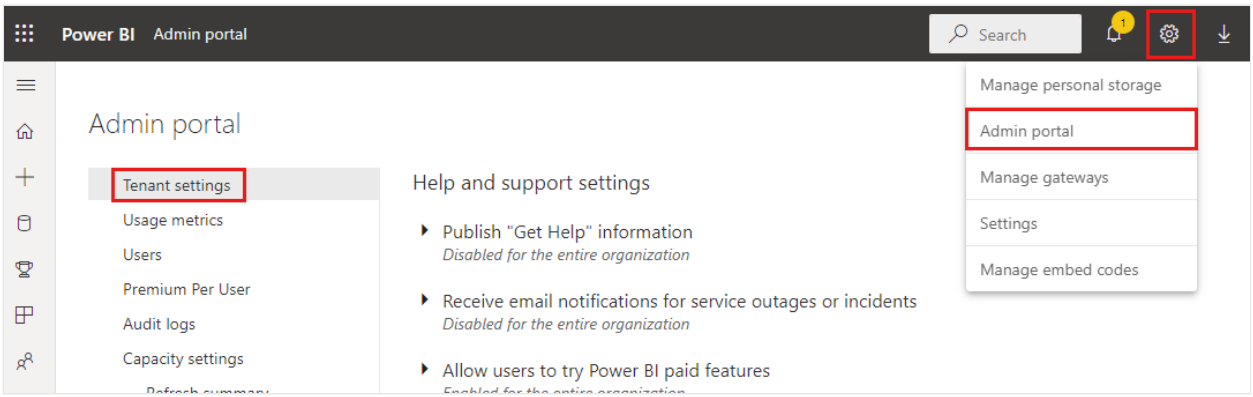
Tenant settings enable fine-grained control over the features that are made available to your organization. If you have concerns around sensitive data, some of our features may not be right for your organization, or you may only want a particular feature to be available to a specific group.

> **Note**
>
> 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 dataset. Power BI users with read access to a dataset have the permission to query this dataset and might be able to persist the results without using the **Export data** feature in the Power BI user interface.

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

How to get to the tenant settings

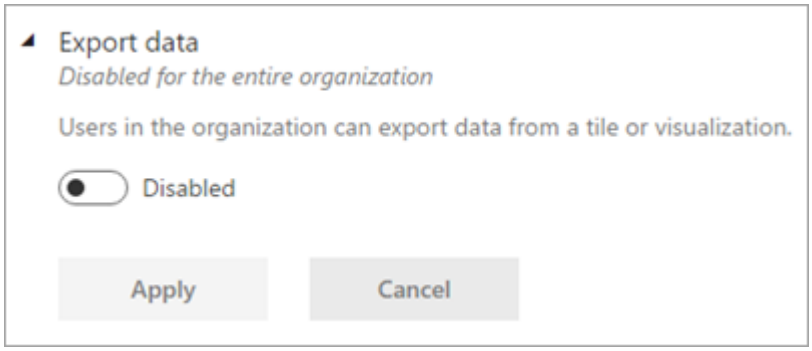
Go to the Admin portal and select Tenant settings.



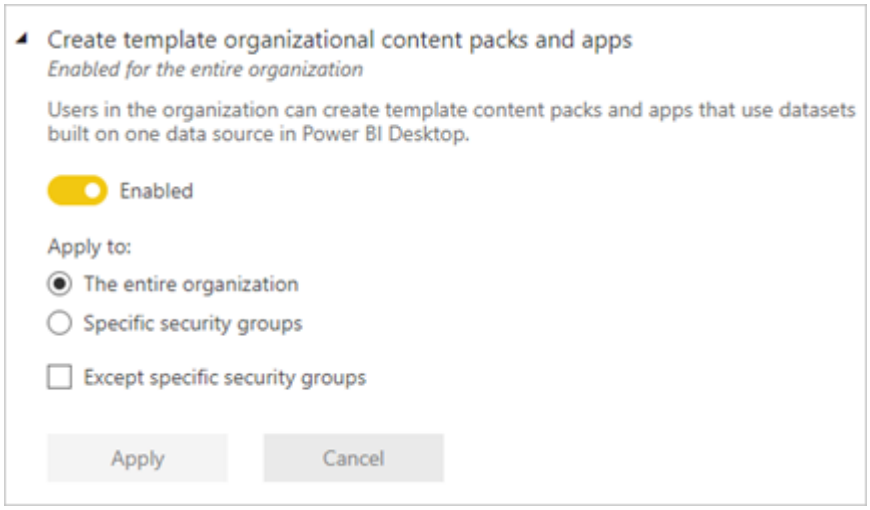
How to use the tenant settings

Many of the settings can have one of three states:

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

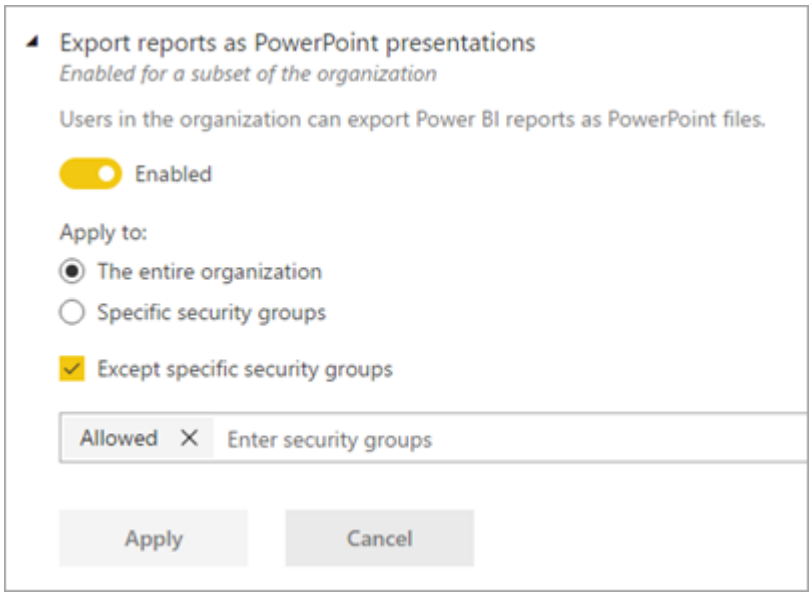


- **Enabled for the entire organization**: Everyone in your organization can use this feature.

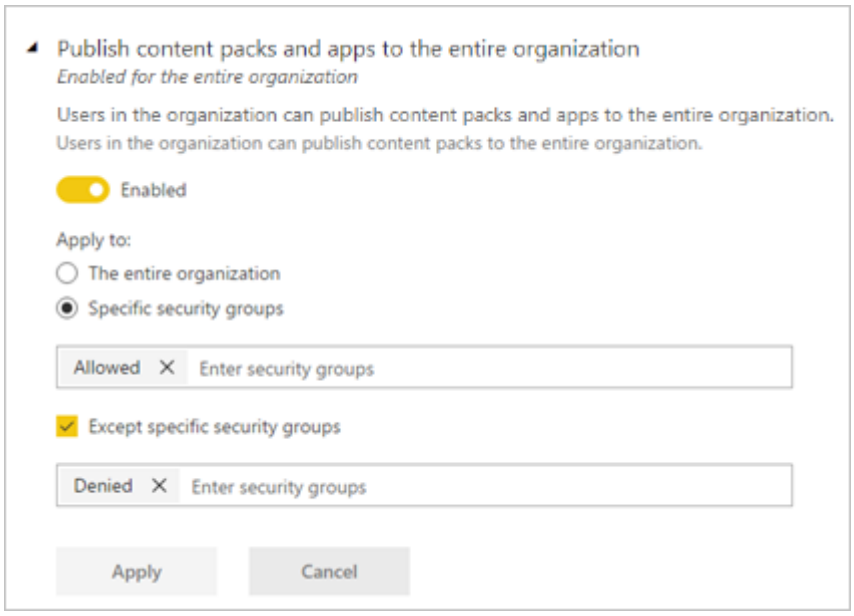


- **Enabled for a subset of the organization**: Specific security groups in your organization are allowed to use this feature.

  You can also enable a feature for your entire organization, **Except specific security groups**.



You can also combine settings to enable the feature only for a specific group of users and also disable it for a group of users. Using 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.



Tenant setting sections

The sections of the tenant settings page are listed in the table below.

- Help and support settings
- Workspace settings
- Information protection
- Export and sharing settings
- Discovery settings
- Content pack and app settings
- Integration settings
- Power BI visuals
- R and Python visuals settings
- Audit and usage settings
- Dashboard settings
- Developer settings
- Admin API settings
- Dataflow settings
- Template app settings
- Q&A settings
- Dataset Security
- Advanced networking
- Metrics settings

- User experience experiments
- Share data with your Microsoft 365 services
- Insights settings
- Quick measure suggestions settings

Next steps

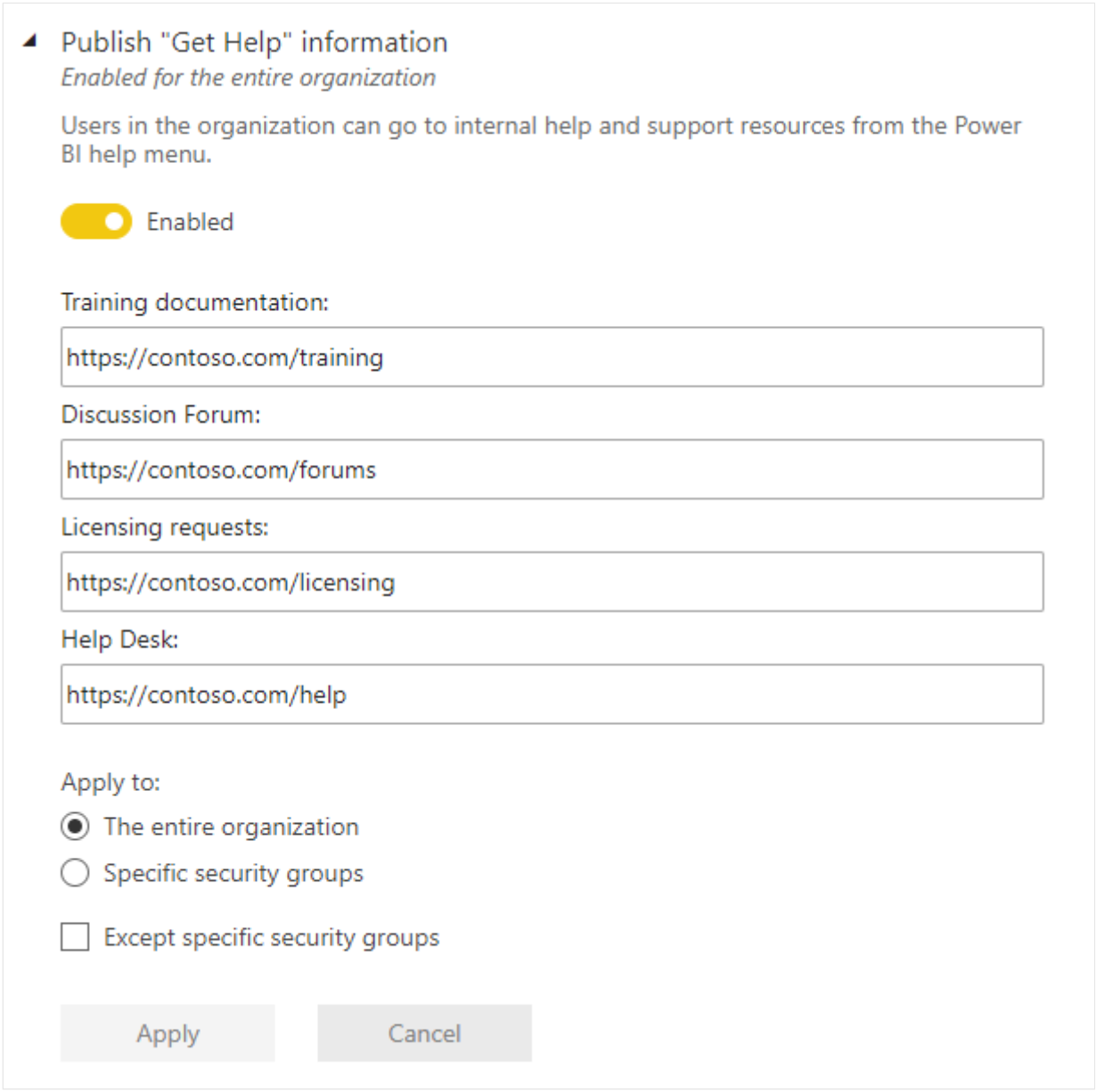
About the Admin portal

Help and support tenant settings

Article • 12/08/2022 • 3 minutes to read

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

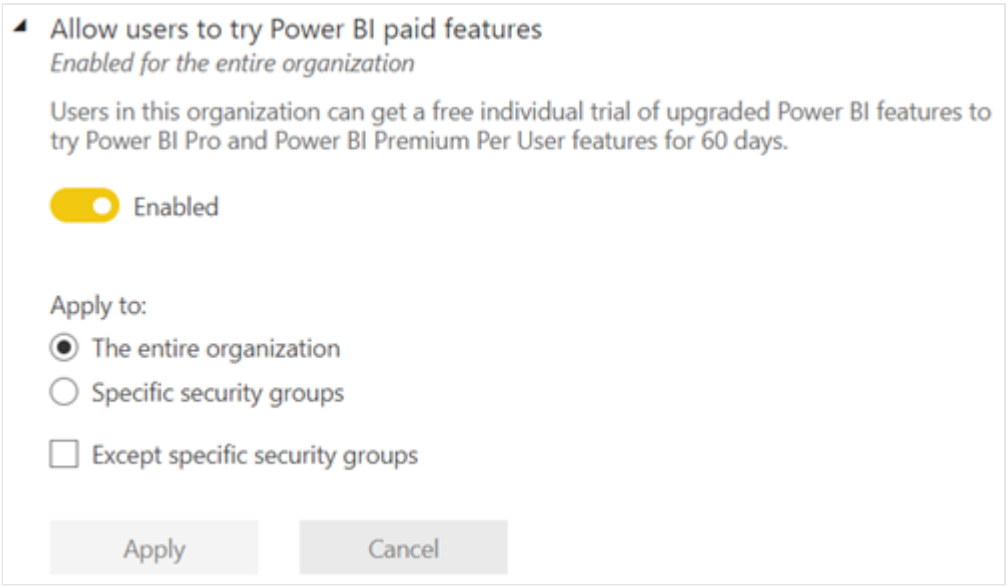
custom URL for **Training documentation**.

- **Community**. To take users to an internal forum from the help menu, instead of to the Power BI Community, set a custom URL for **Discussion forum**.
- **Licensing upgrades**. Users with a Power BI (free) license may be presented with the opportunity to upgrade their account to Power BI Pro while using the service. Users who already hold a Power BI Pro license may be prompted to upgrade 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. If you want to prevent users from buying licenses, but are okay with letting users start a Power BI Pro or Power BI Premium Per User trial, see Allow users to try Power BI 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 Power BI Support, set a custom URL for **Help Desk**.

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. Learn more about Service interruption notifications.

Allow users to try Power BI paid features



The setting to **Allow users to try Power BI paid features** is enabled by default. This setting increases your control over how users get license upgrades. In scenarios where you have blocked self-service purchase, this setting lets users use more features free for

60 days. Users who have a Power BI (free) license can start a Power BI Pro trial. Users with a Power BI Pro license can start a Power BI Premium Per User trial. The user's license upgrade experience depends on how you combine license settings. The table below shows how the upgrade experience is affected by different setting combinations:

Self-service purchase setting	Allow user to try Power BI 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 signup for a trial license. Users who can buy a license in the scenarios described in the table above are redirected to your internal URL.

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

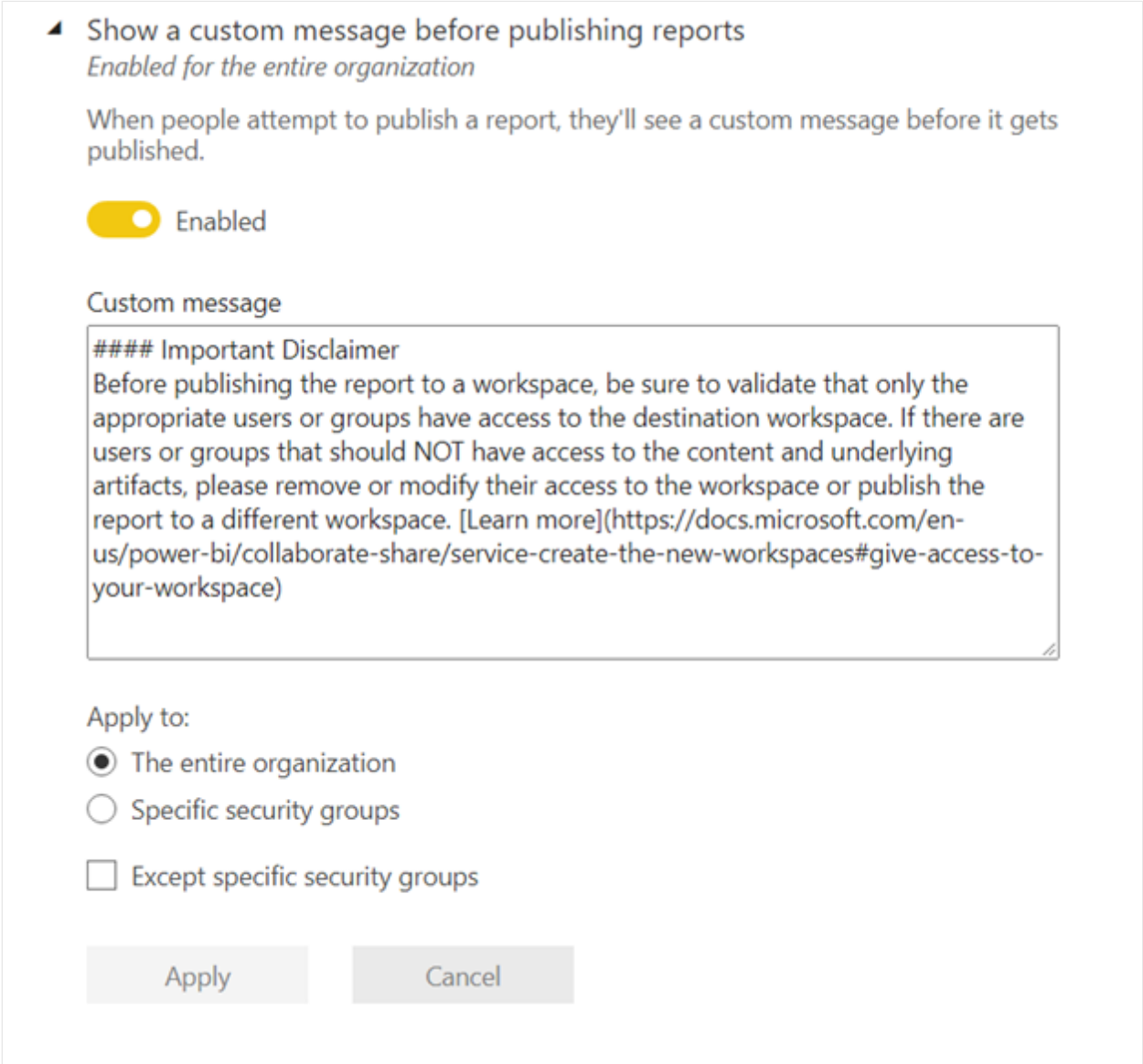
Show a custom message before publishing reports

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 message:

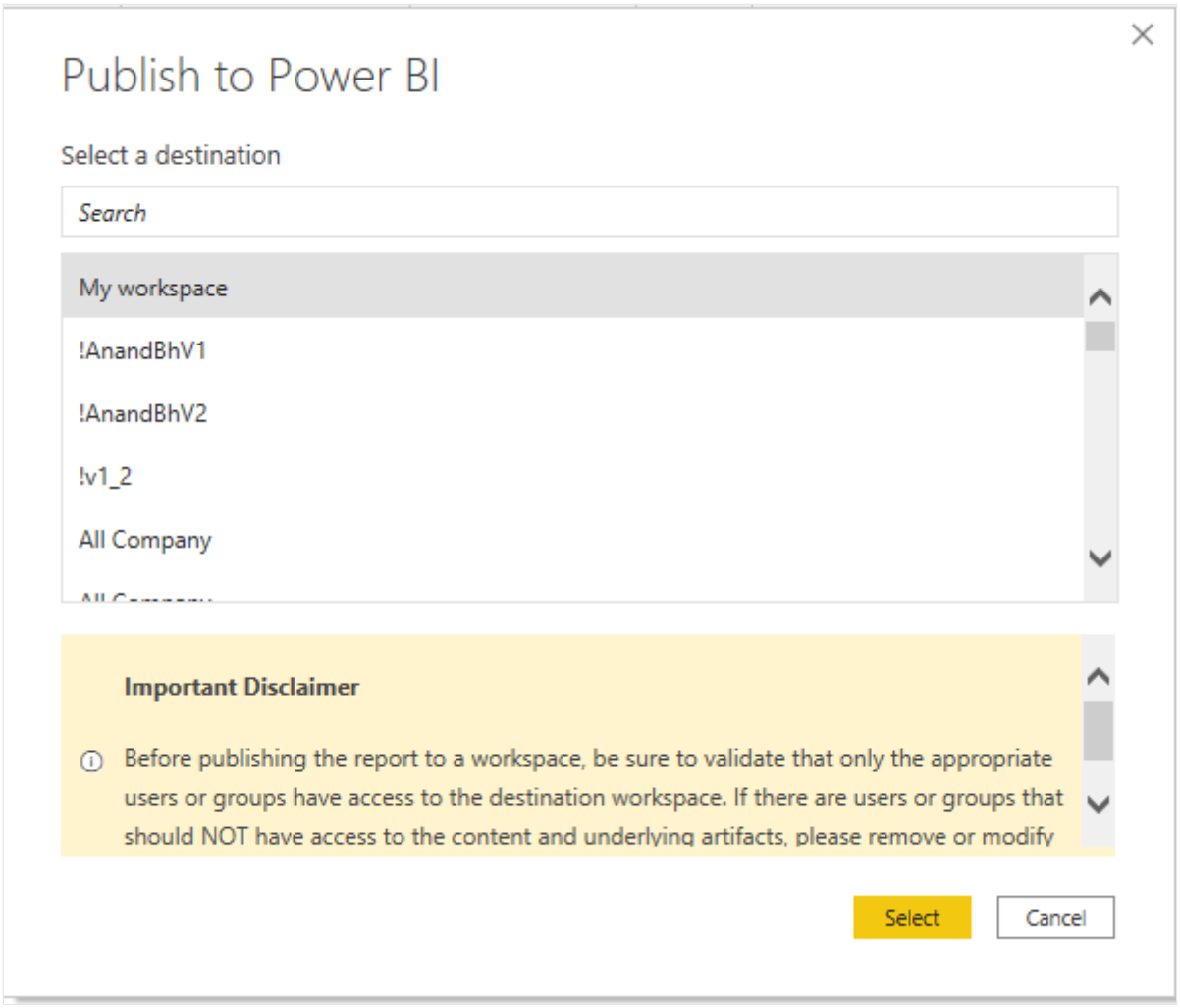
```markdown
### Important Disclaimer

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]
(../collaborate-share/give-access-new-workspaces.md).
```

The **Custom message** text area does support 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've written.



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**.

Next steps

- About tenant settings

Workspace tenant settings

Article • 10/03/2022 • 2 minutes to read

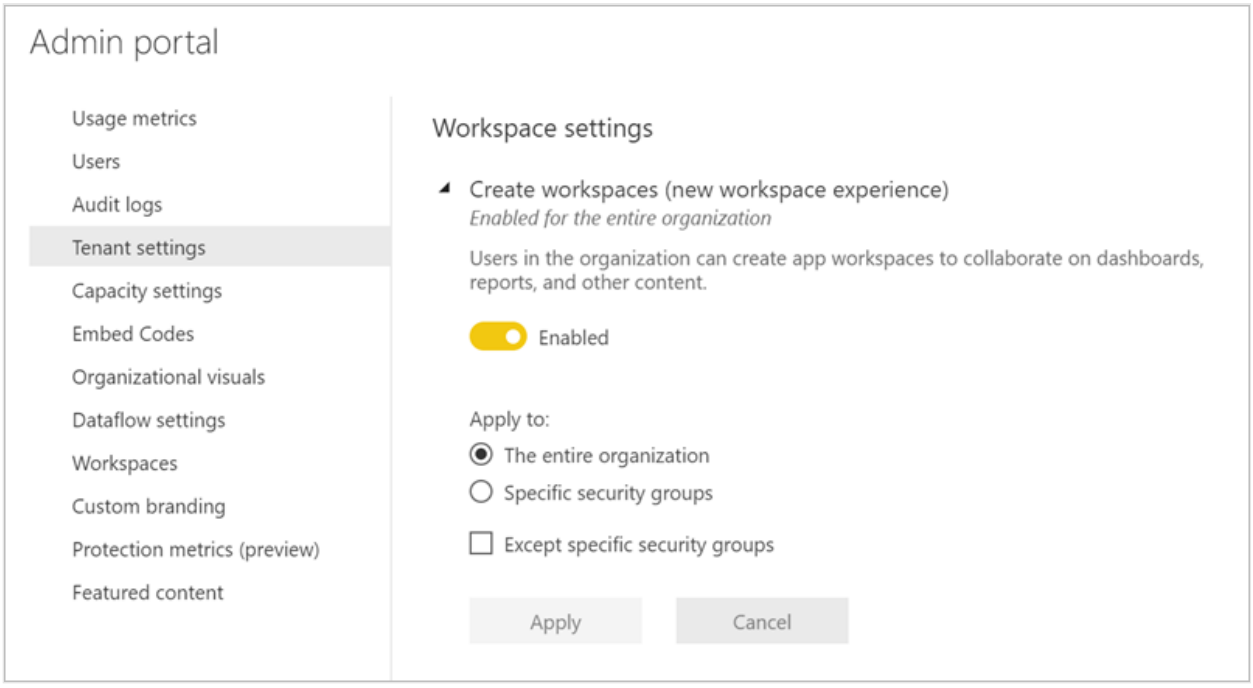
These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

In **Tenant settings**, the admin portal has three sections for controlling workspaces:

- Create the new workspace experiences.
- Use datasets across workspaces.
- Block upgrading empty classic workspaces.

Create the new workspaces

Workspaces are places where users collaborate on dashboards, reports, and other content. Admins use the **Create workspaces (new workspace experience** setting to indicate which users in the organization can create workspaces. Admins can let everybody or nobody in an organization create new workspace experience 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 (new workspace experience)** setting defaults to allowing only users who can create Microsoft 365 Groups to create the new Power BI workspaces. Be sure to set a value in the Power BI admin portal to ensure appropriate users can create them.

List of workspaces

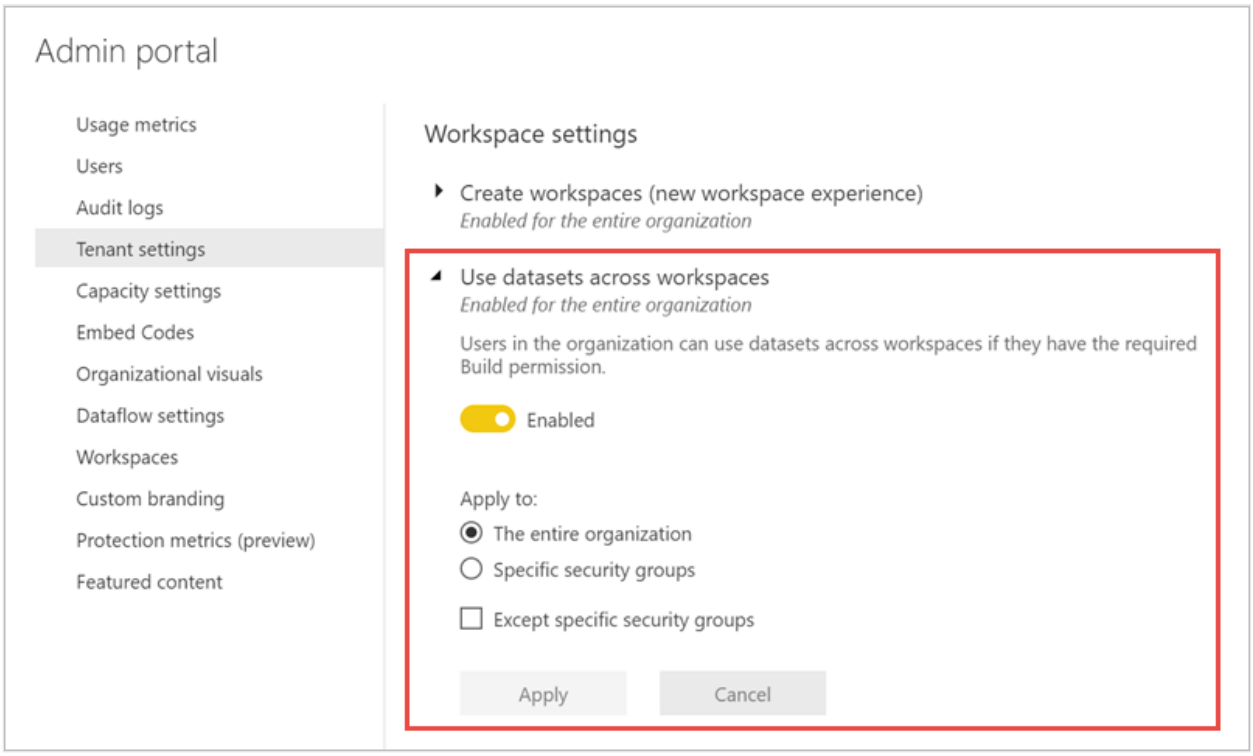
The admin portal has another section of settings about the workspaces in your tenant. In that section, you can sort and filter the list of workspaces and display the details for each workspace. See Workspaces in this article for details.

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

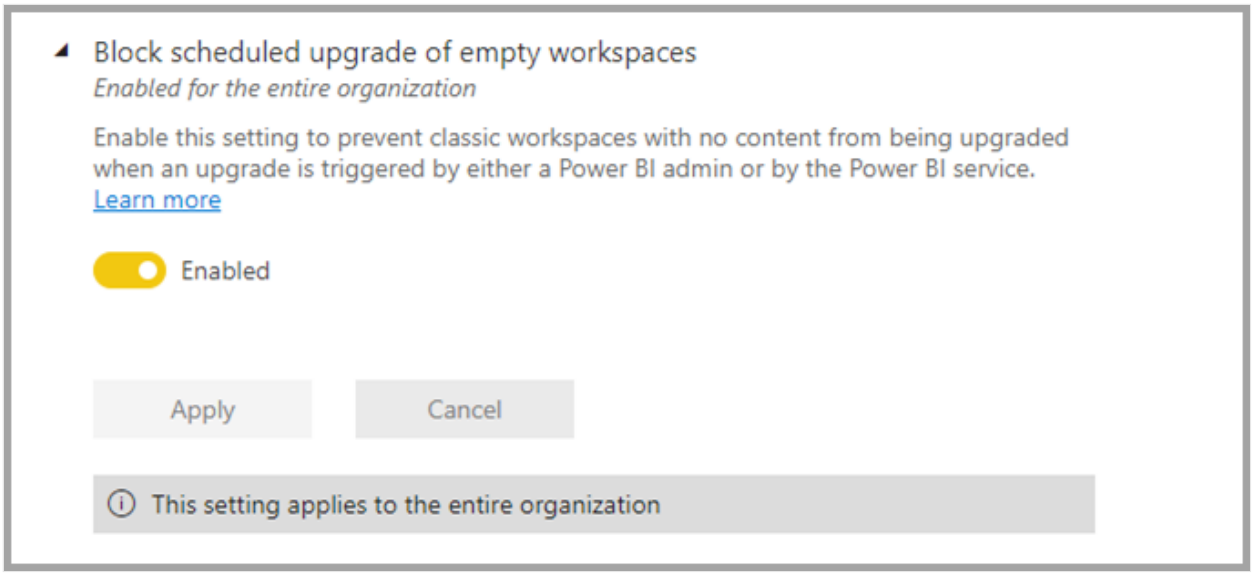
Admins can control which users in the organization can use datasets across workspaces. When this setting is enabled, users still need the required Build permission for a specific dataset.



For more information, see Intro to datasets across workspaces.

Empty classic 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 will not be deleted.Read more about the new workspace experience workspaces.

Next steps

- About tenant settings

Information protection tenant settings

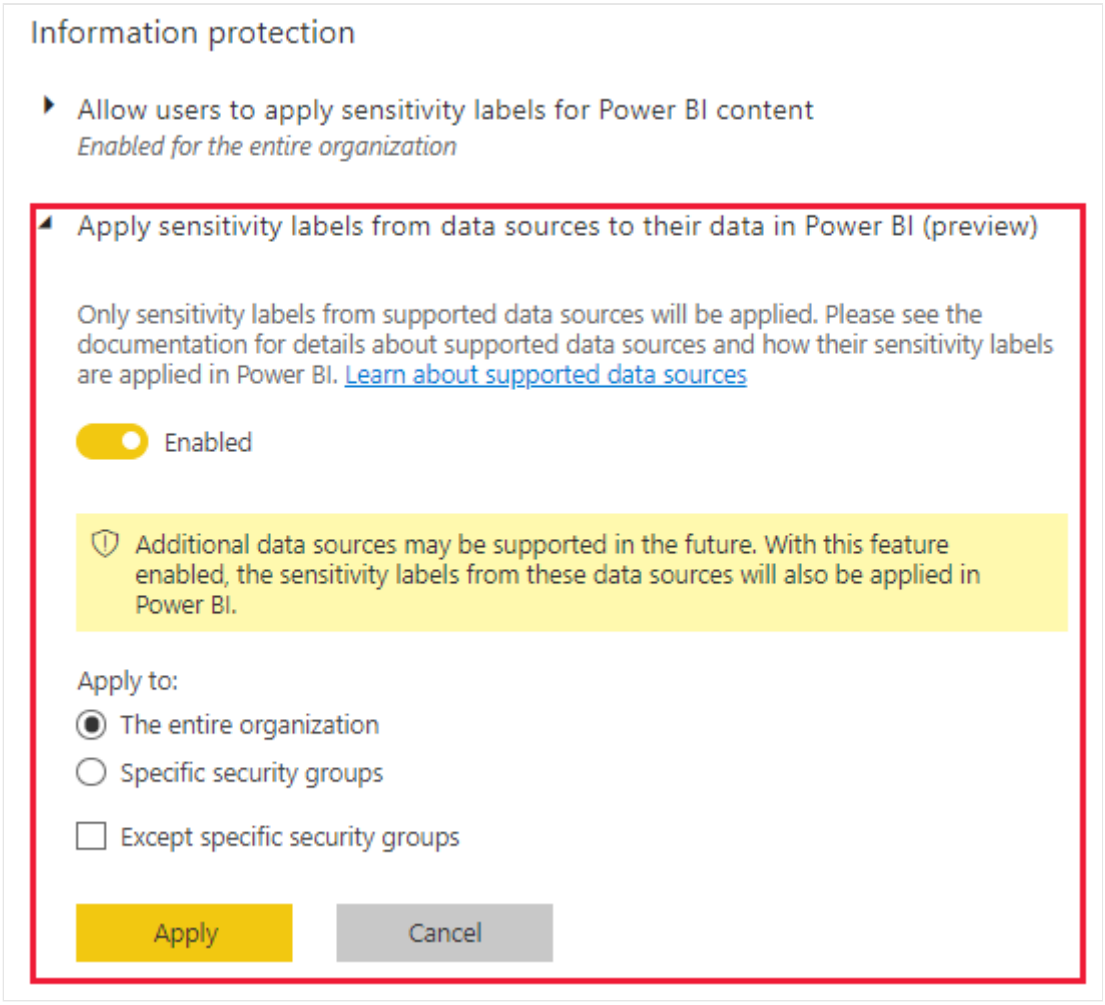
Article • 10/03/2022 • 2 minutes to read

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 sensitivity labels from data sources to their data in Power BI (preview)

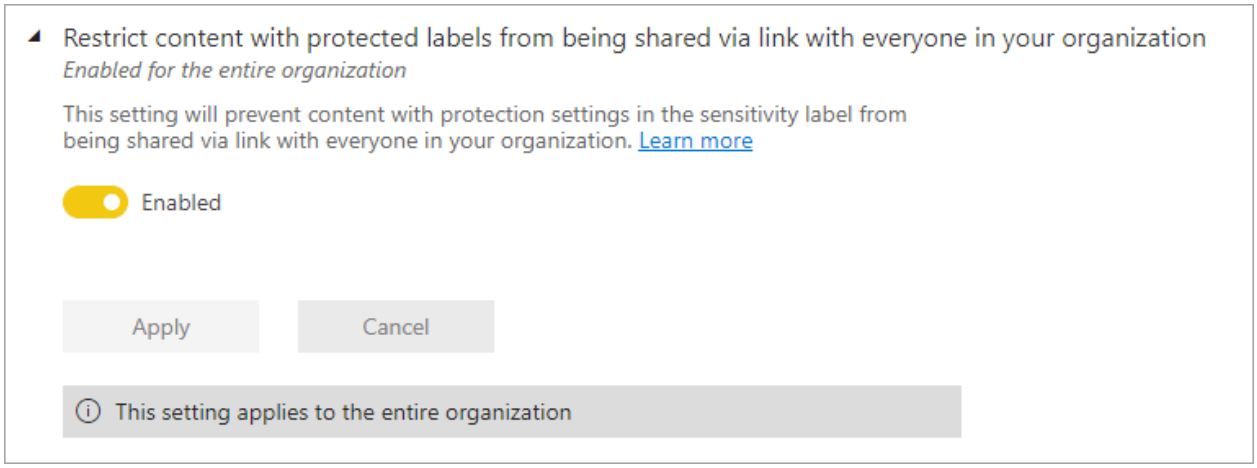
When this setting is enabled, Power BI datasets that connect to sensitivity-labeled data in supported data sources can inherit those labels, so that the data remains classified and secure when brought into Power BI. For detail about sensitivity label inheritance from data sources, see Sensitivity label inheritance from data sources (preview).

To enable sensitivity label inheritance from data sources go to the Power BI tenant settings, and enable the toggle under **Information protection** > **Apply sensitivity labels from data sources to their data in Power BI (preview)**:



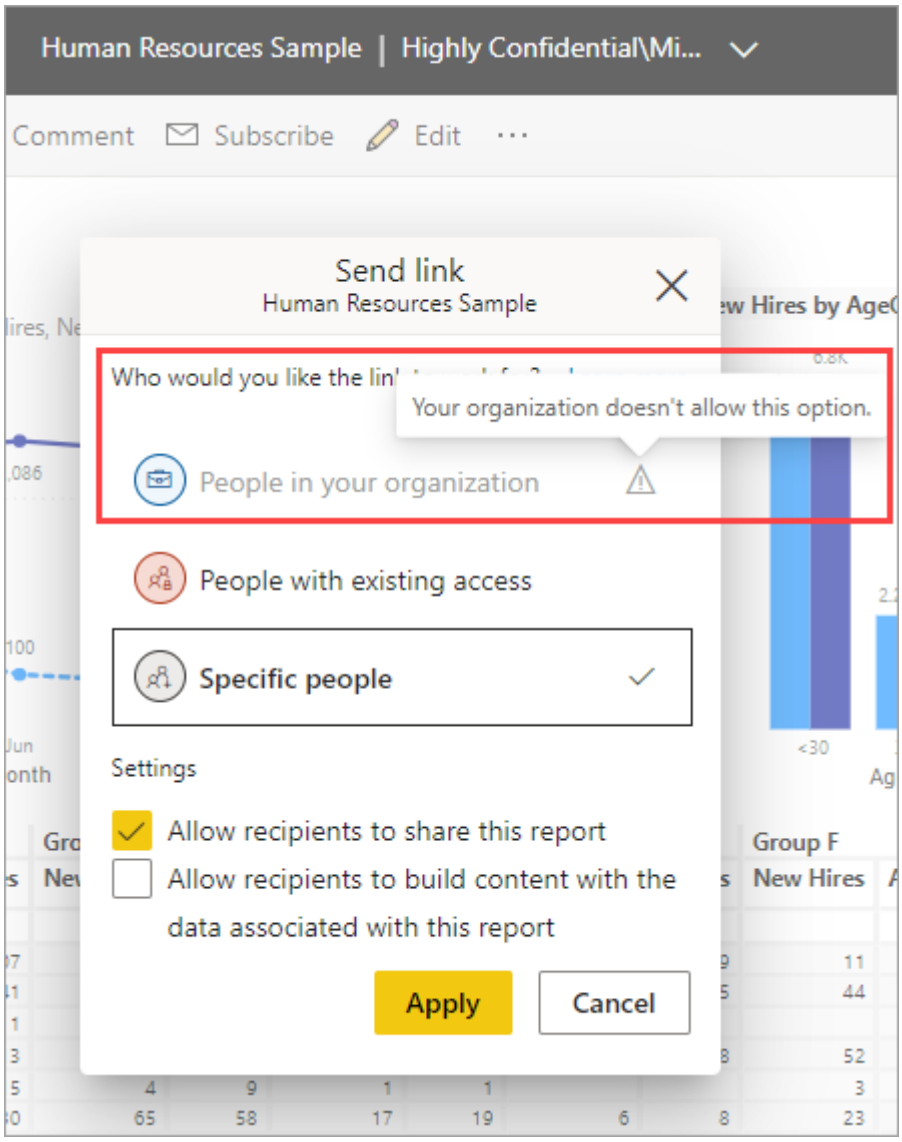
Restrict content with protected labels from being shared via link with everyone in your organization

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 may 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, check out the Microsoft 365 article Restrict access to content by using sensitivity labels to apply encryption.

Next steps

- About tenant settings

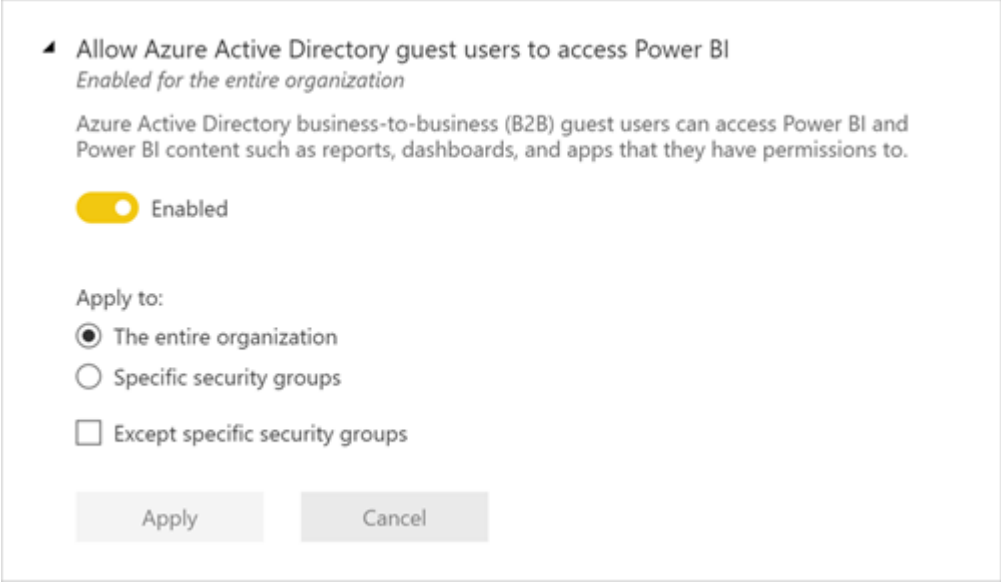
Export and sharing tenant settings

Article • 10/03/2022 • 9 minutes to read

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.

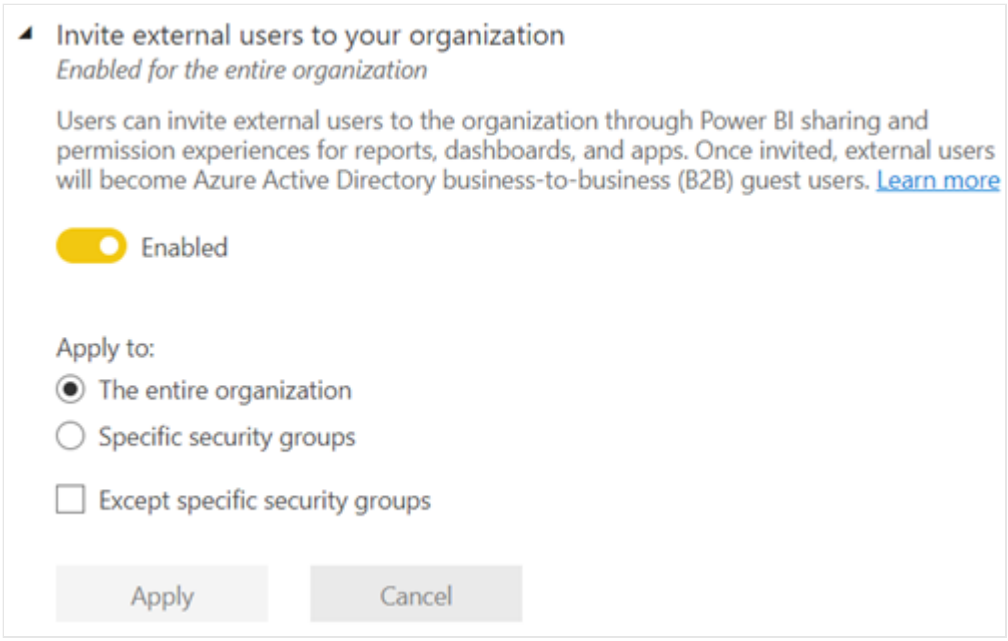
Allow Azure Active Directory guest users to access Power BI

Enabling this setting allows Azure Active Directory Business-to-Business (Azure AD B2B) guest users to access Power BI. If you disable this setting, guest users receive an error when trying to access Power BI. 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 guest users can access Power BI.



Invite external users to your organization

The **Invite external users to your organization** setting helps organizations choose whether new external users can be invited to the organization through Power BI sharing, permissions, and subscription experiences. If the setting is disabled, an external user who isn't already a guest user in the organization, can't be added to the organization through Power BI.



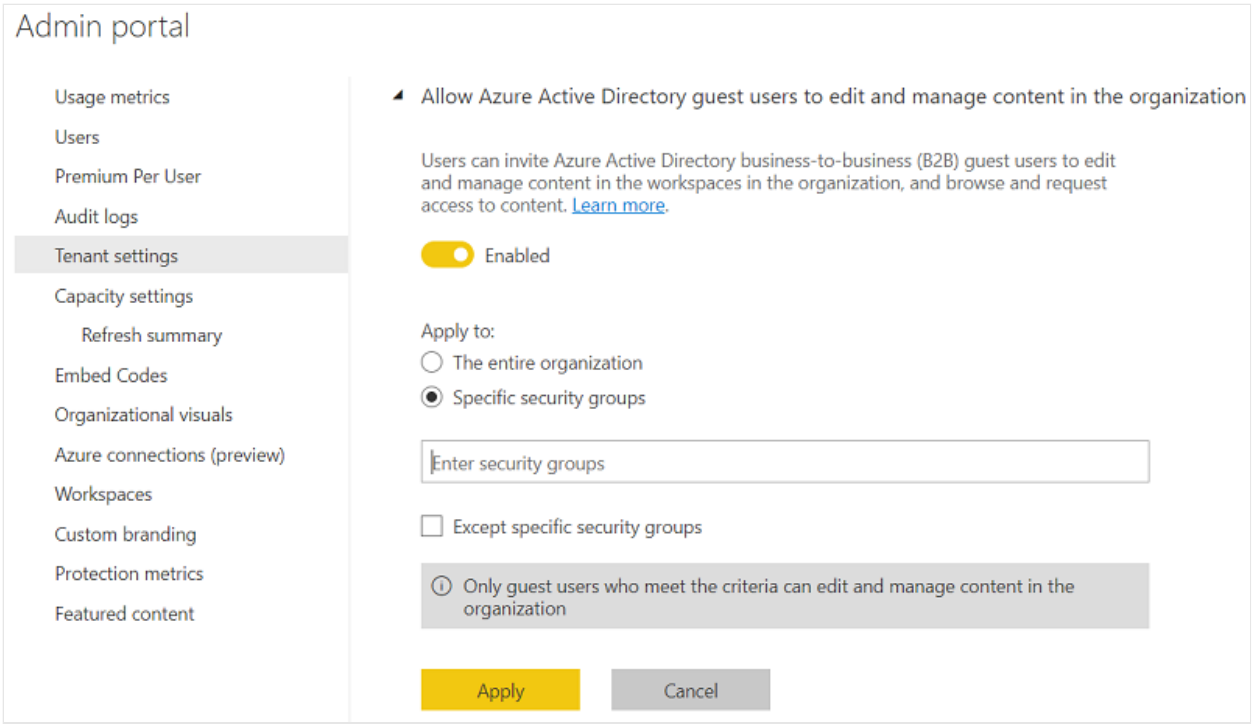
> **ⓘ Important**
>
> This setting was previously called "Share content with external users". The revised name reflects more accurately what the setting does.

To invite external users to your organization, a user also needs the Azure Active Directory Guest Inviter role. This setting only controls the ability to invite through Power BI.

Allow external guest users to edit and manage content in the organization

Azure AD B2B guest users can edit and manage content in the organization. Learn more

The following image shows the option to Allow Azure Active Directory external guest users to edit and manage content in the organization.

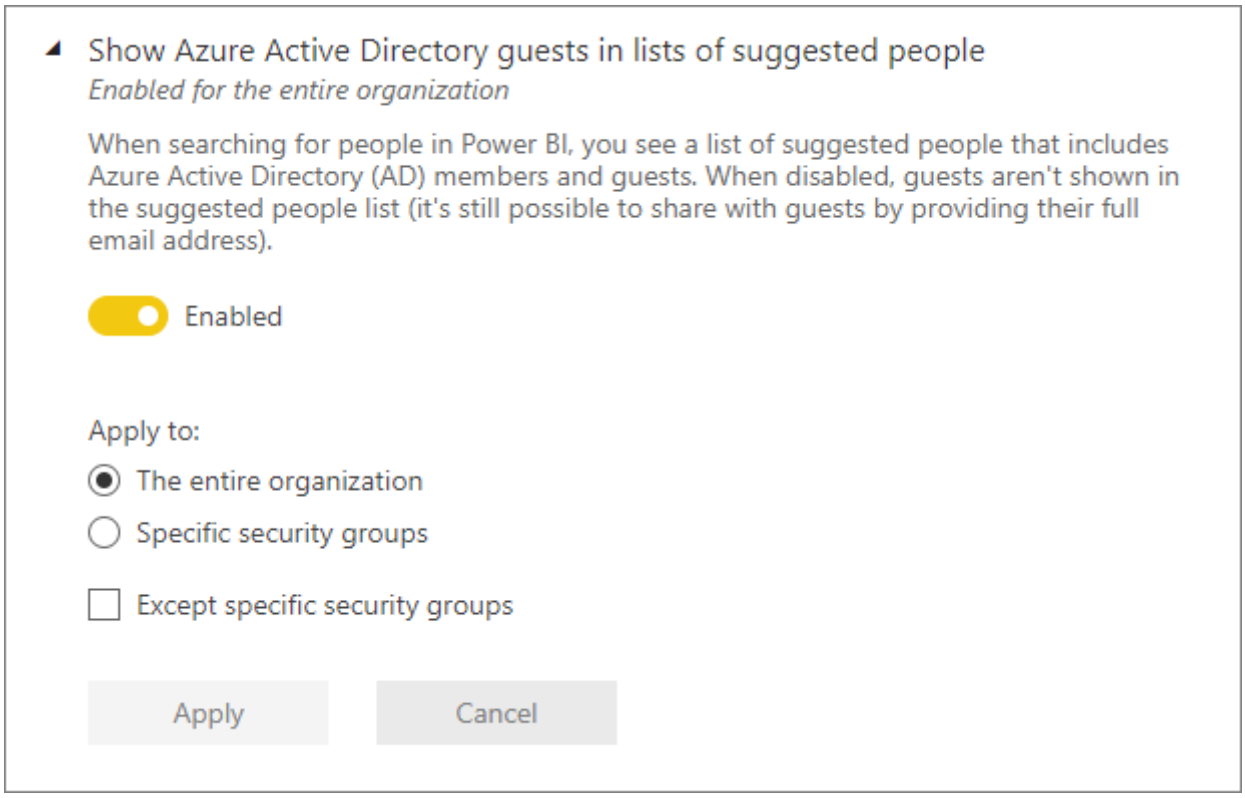


In the admin portal, you also control which users have permissions to invite external users to the organization. See Share content with external users in this article for details.

Show Azure Active Directory guests in lists of suggested people

The **Show Azure Active Directory guests in lists of suggested people** setting helps organizations limit visibility of external users in sharing experiences. When disabled, Azure Active Directory (Azure AD) guest users are not 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.

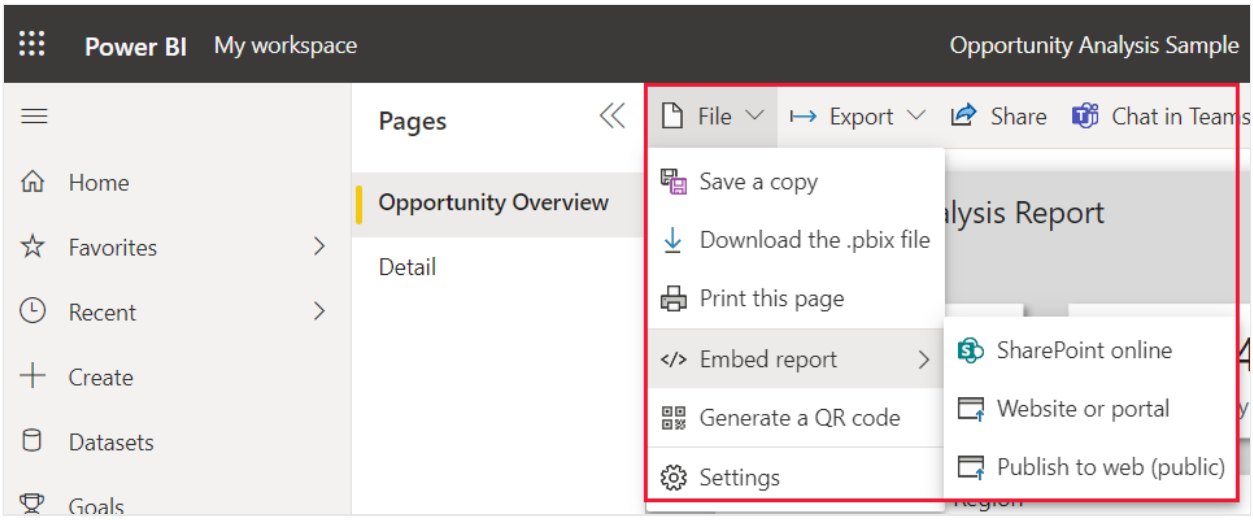


Publish to web

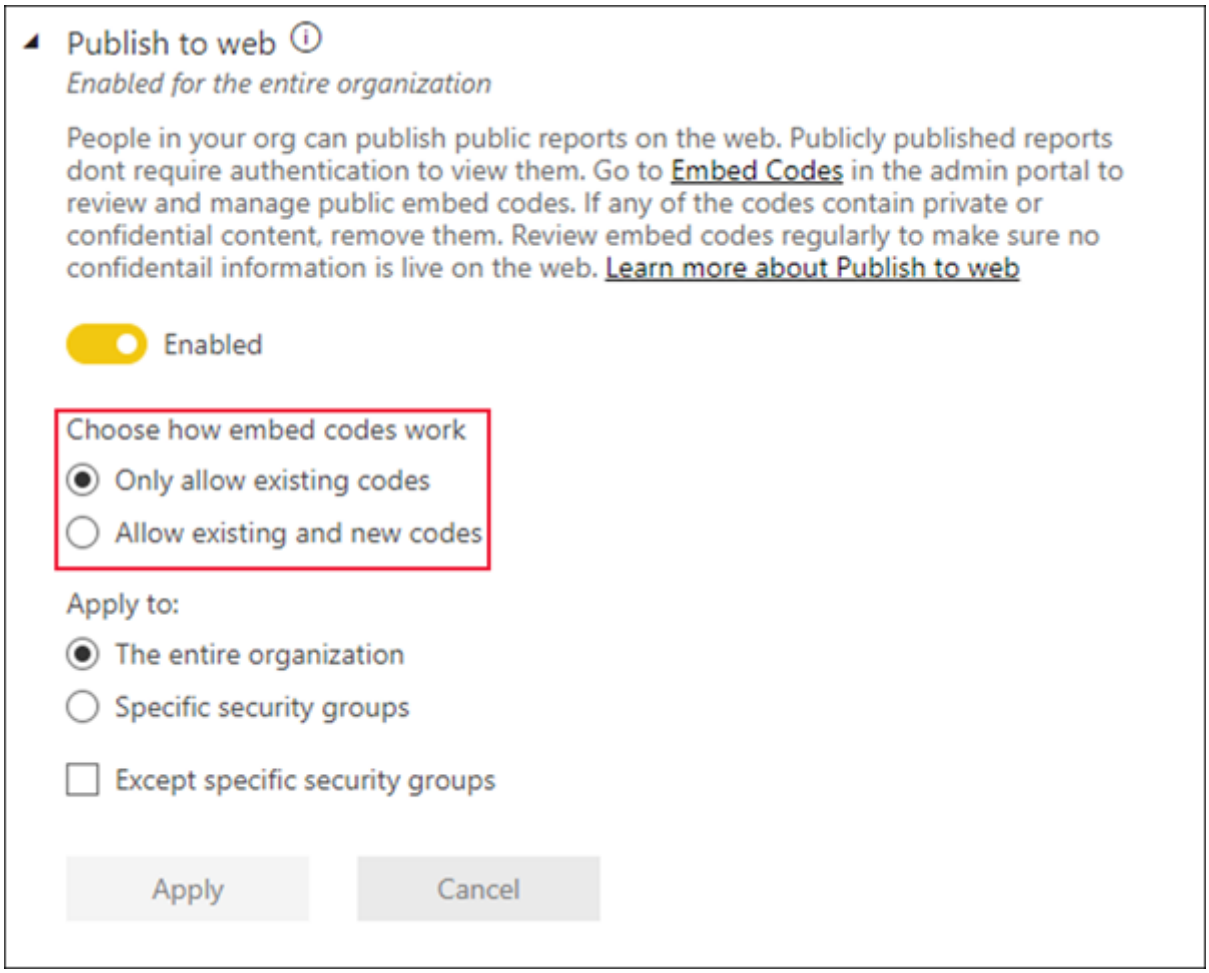
As a Power BI admin, the **Publish to web** setting gives you options that let users create embed codes to publish reports to the web. This functionality makes the report and its data available to anyone on the web. Learn more about publishing to the web.

> ⓘ **Note**
>
> Only Power BI admins can allow creating new publish to web embed codes. Organizations may have existing embed codes. See the **Embed codes** section of the admin portal to review currently published reports.

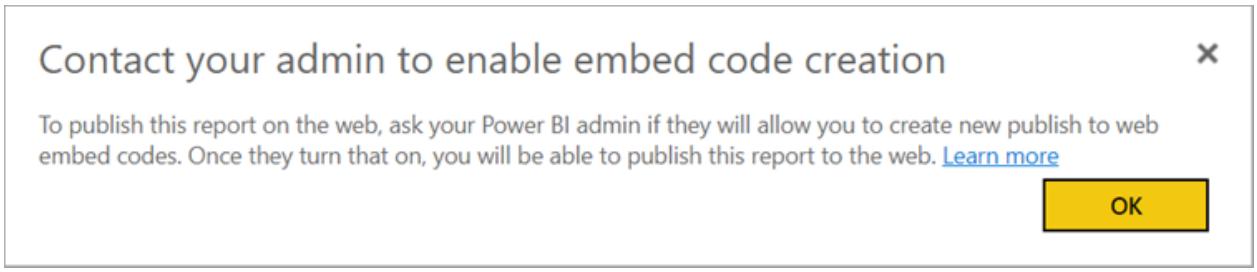
You can find **Publish to web** under **File** > **Embed report** when the **Publish to web** setting is enabled.



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 Power BI admin to allow them to do so.

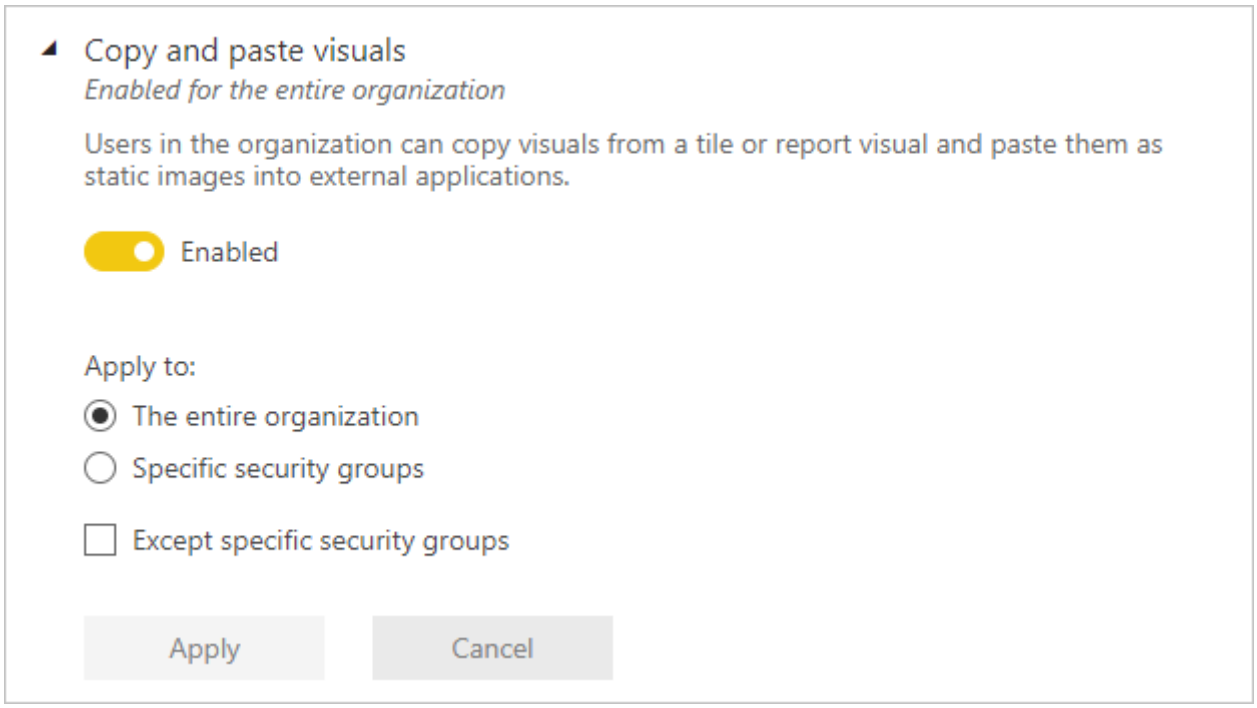


Users see different options in the UI based on what the **Publish to web** setting is.

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.

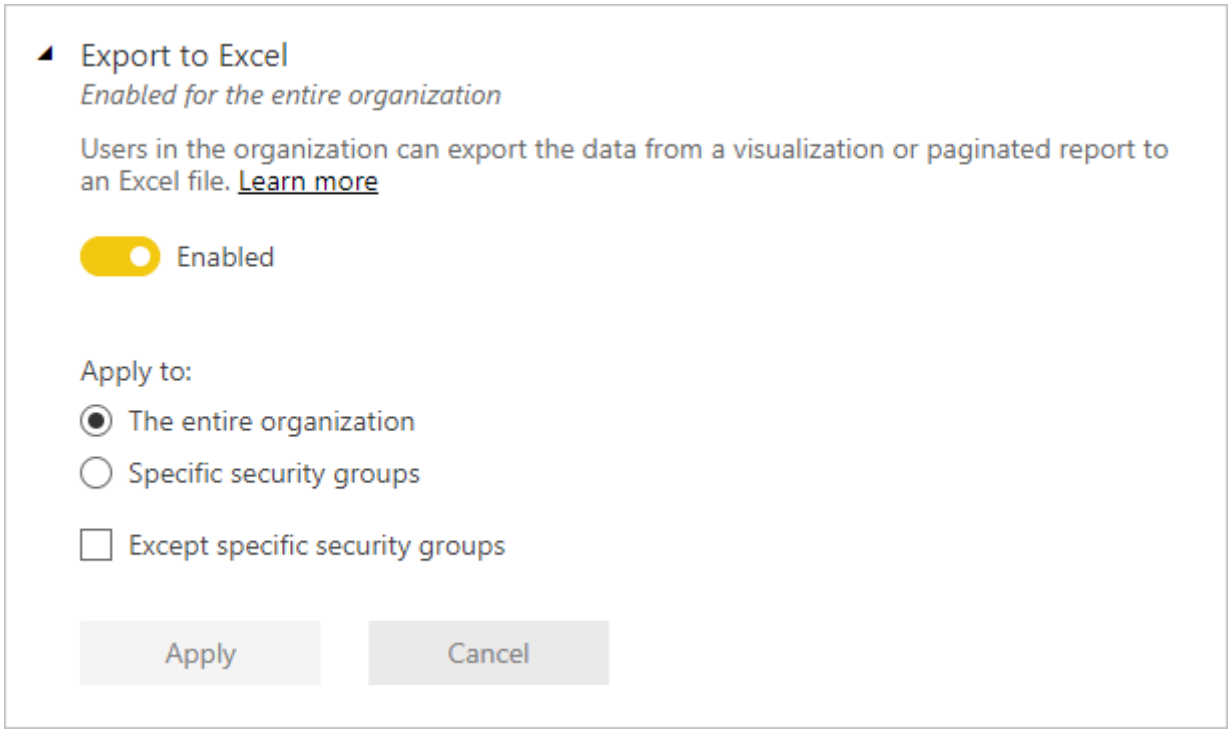
Copy and paste visuals

Users in the organization can copy visuals from a tile or report visual and paste them as static images into external applications.



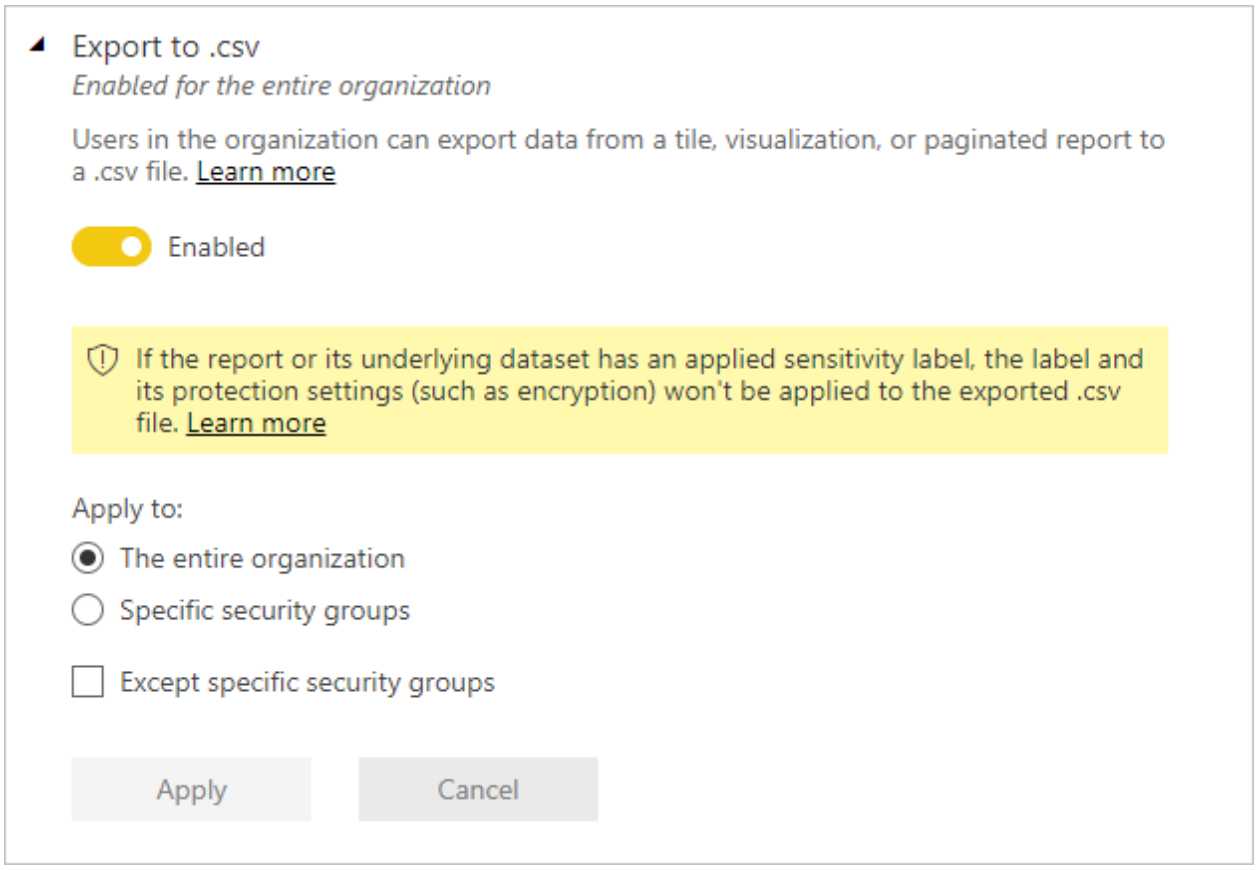
Export to Excel

Users in the organization can export the data from a visualization to an Excel file.



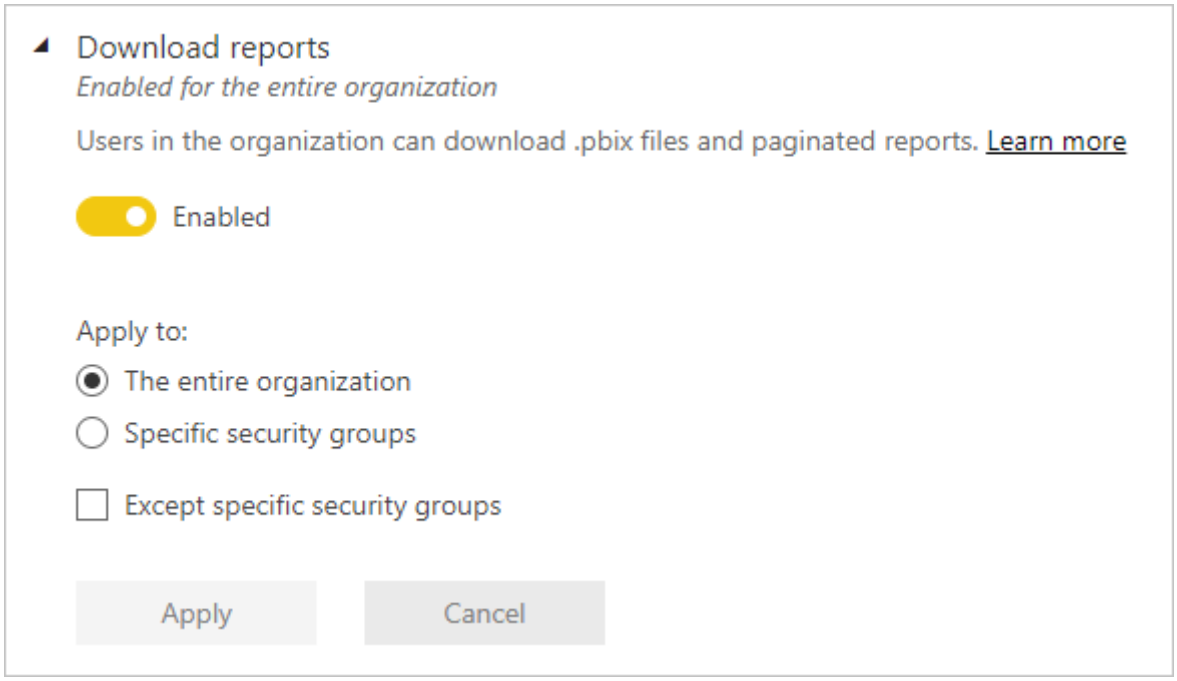
Export to .csv

Users in the organization can export data from a tile, visualization, or paginated report to a .csv file.



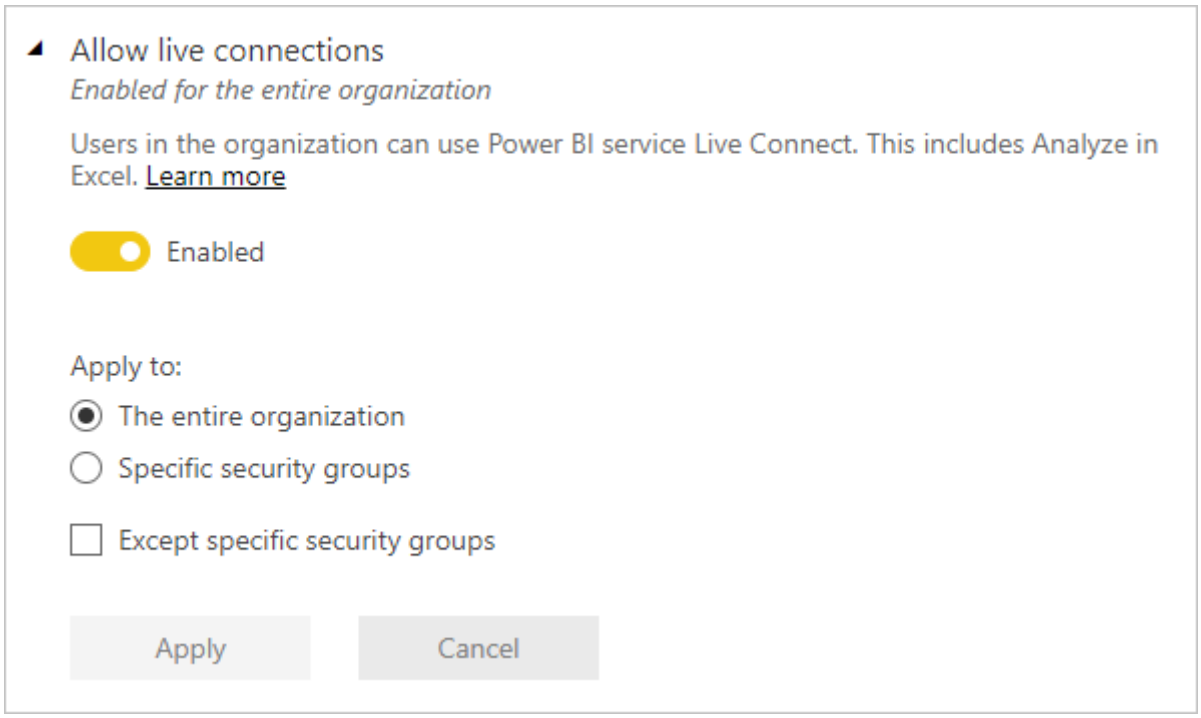
Download reports

Users in the organization can download .pbix files and paginated reports.



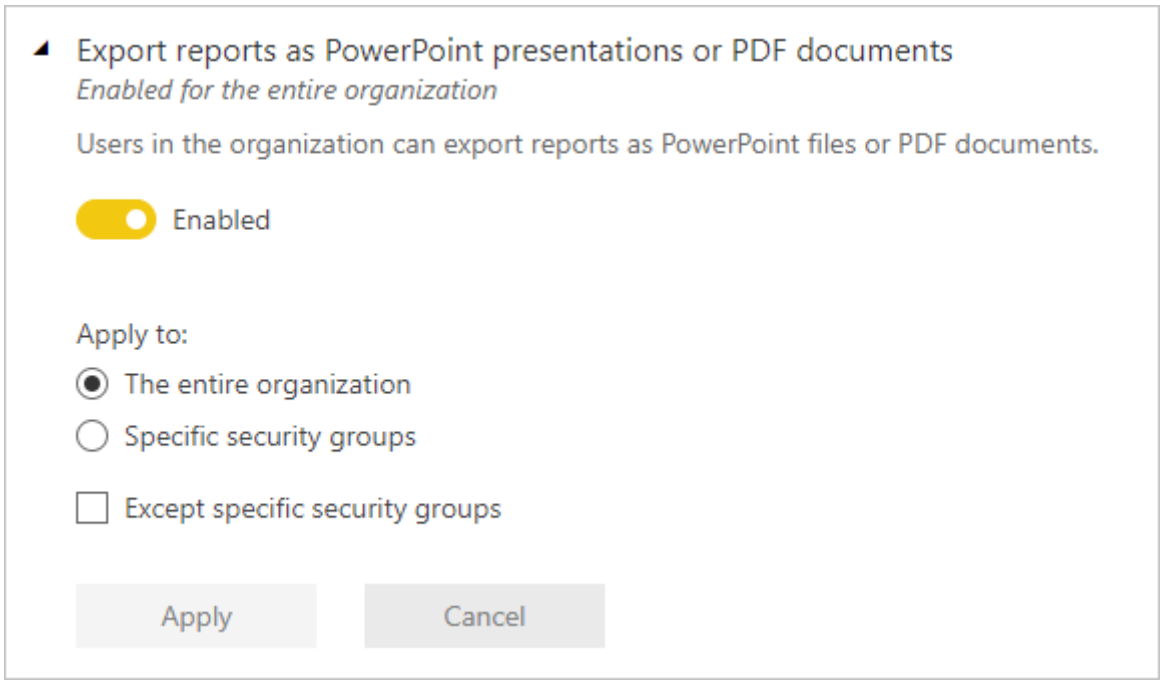
Allow live connections

Users in the organization can use Power BI service Live Connect. Allowing live connections also allows users to Analyze in Excel.



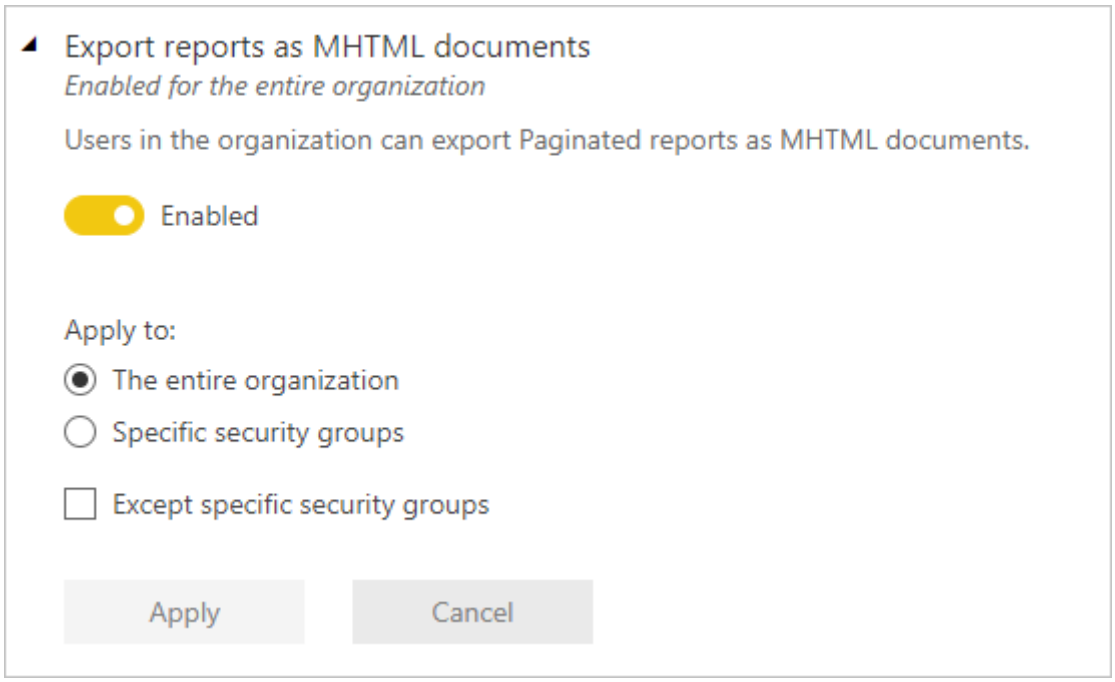
Export reports as PowerPoint presentations or PDF documents

Users in the organization can export reports as PowerPoint files or PDF documents.



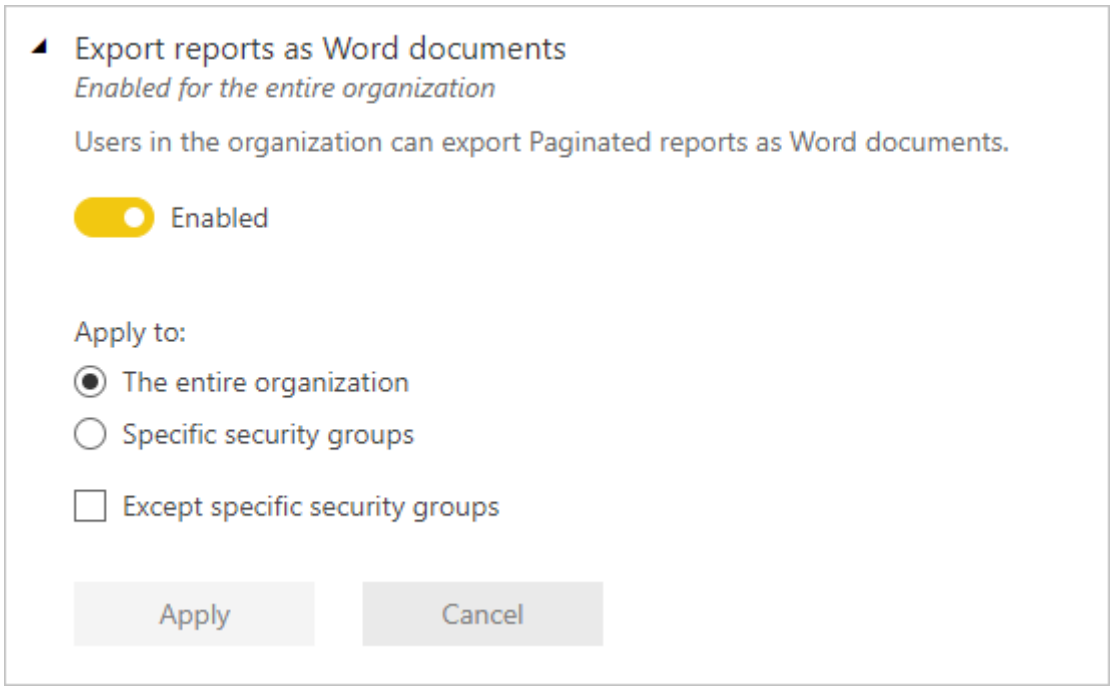
Export reports as MHTML documents

Users in the organization can export Paginated reports as MHTML documents.



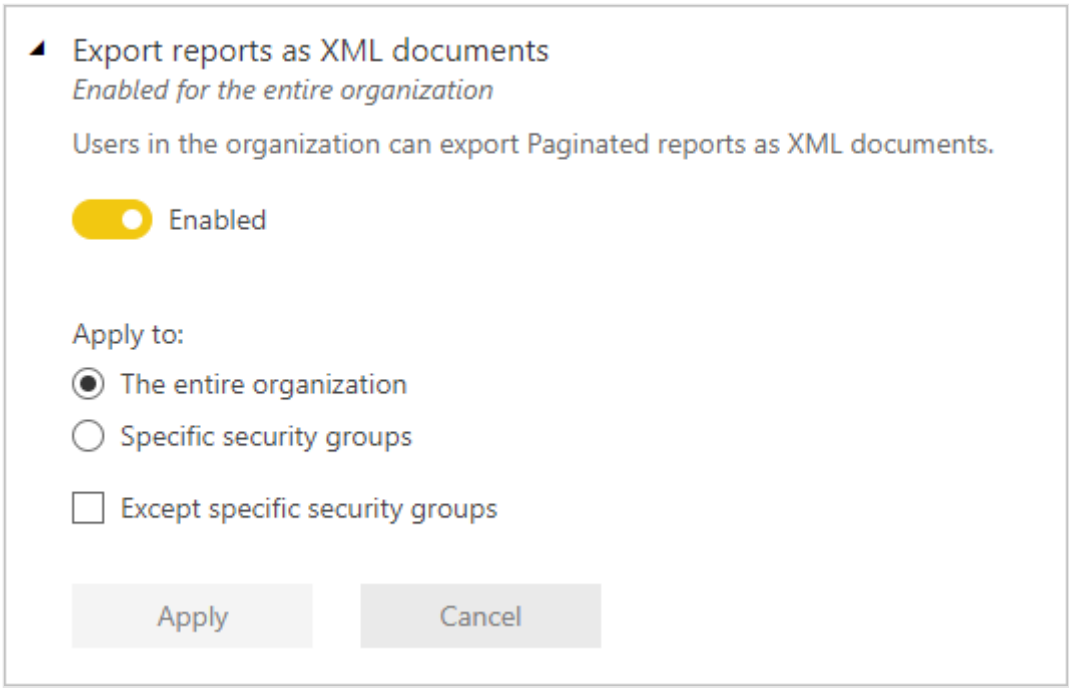
Export reports as Word documents

Users in the organization can export Paginated reports as Word documents.



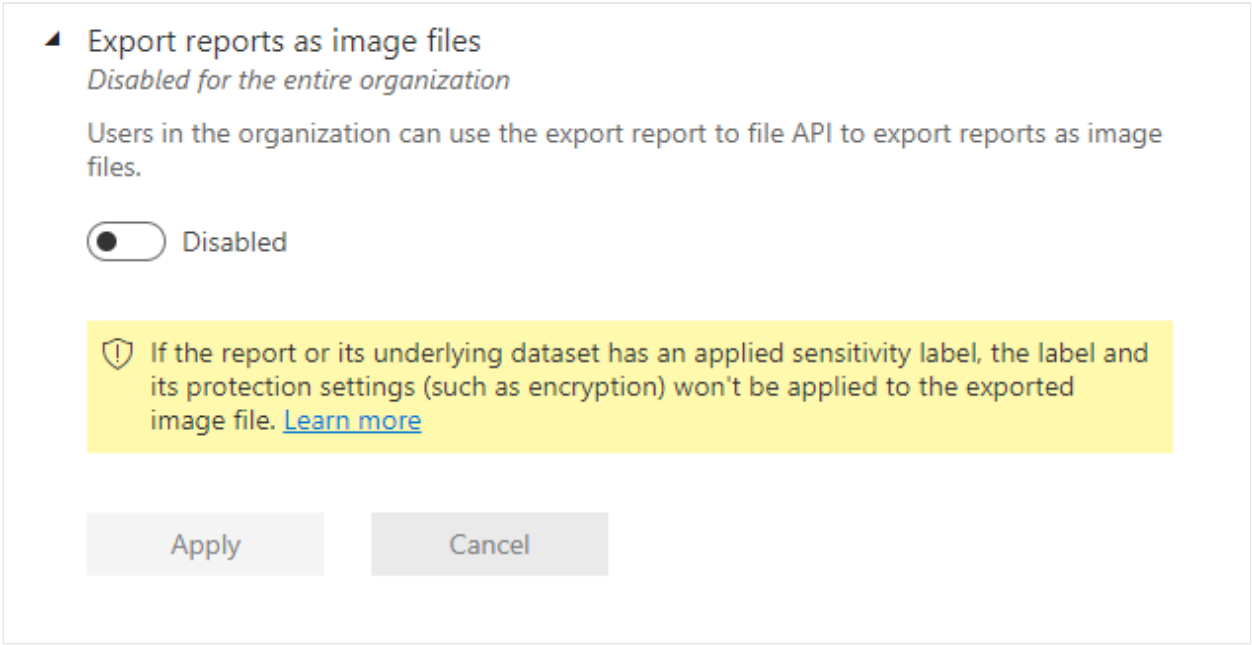
Export reports as XML documents

Users in the organization can export Paginated reports as XML documents.

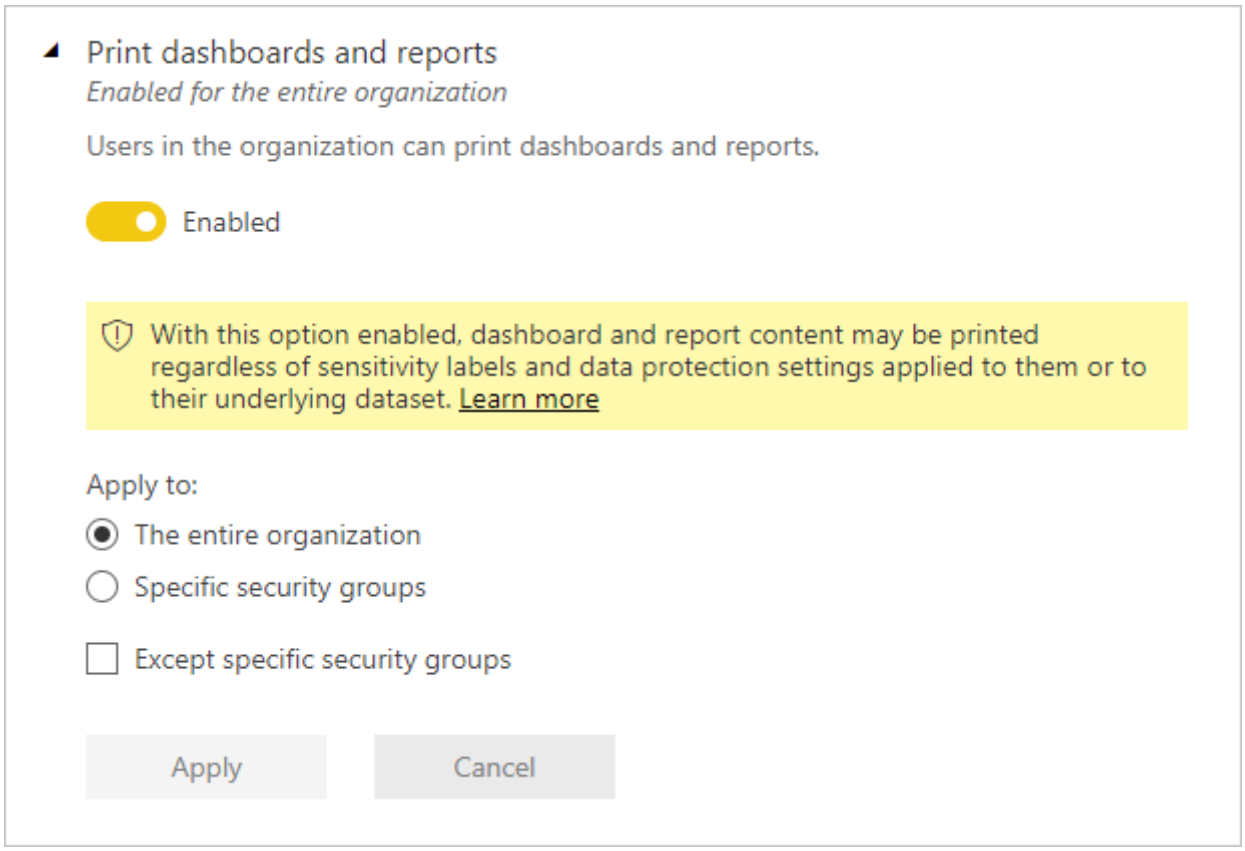


Export reports as image files

Users in the organization can use the export report to file API to export reports as image files.



Print dashboards and reports

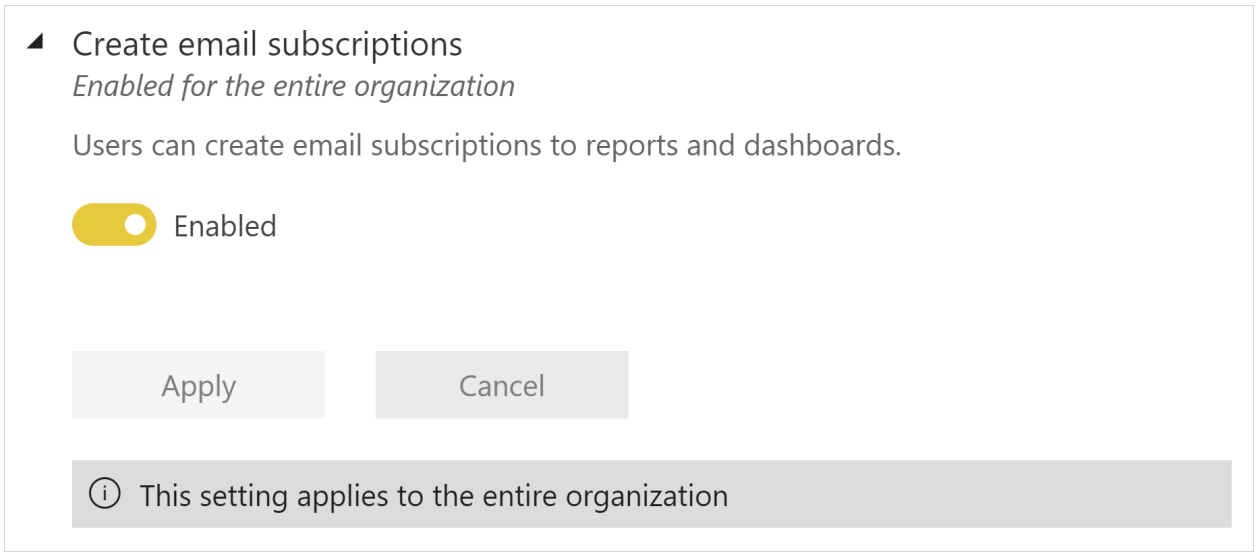


Certification

Allow users in this org to certify datasets, dataflows, reports, and apps. See Enable content certification for details.

Create email subscriptions

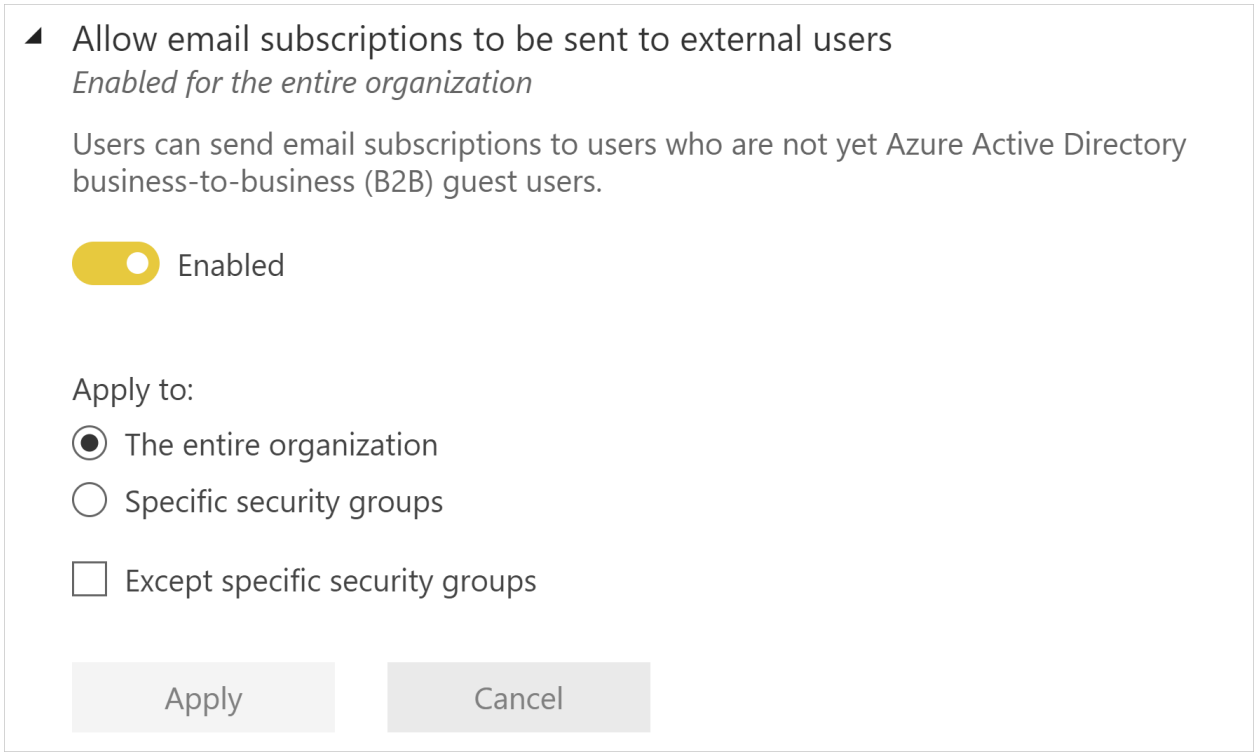
Users can create email subscriptions to reports and dashboards. Learn more about subscriptions.



Allow email subscriptions to be sent to external users

The **Allow email subscriptions to be sent to external users** setting helps organizations choose whether external users can be included as recipients of email subscriptions.

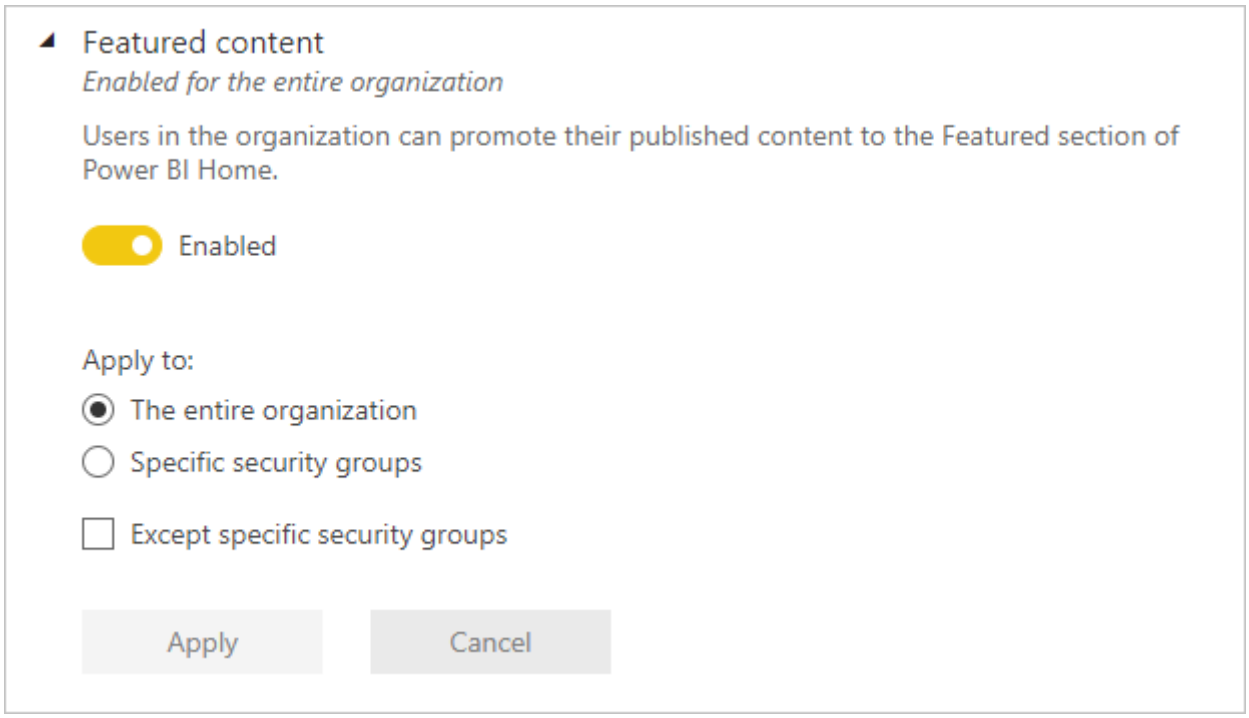
External users are users outside of the organization that have not been added as Azure Active Directory business-to-business (B2B) guest users. If this setting is turned off, an external user who isn't already a guest user in the organization can't be included as a recipient of an email subscription.



Featured content

By default, anyone with the Admin, Member, or Contributor role in a workspace in your organization can feature content on Power BI Home. See Feature content on colleagues' Power BI Home page for details.

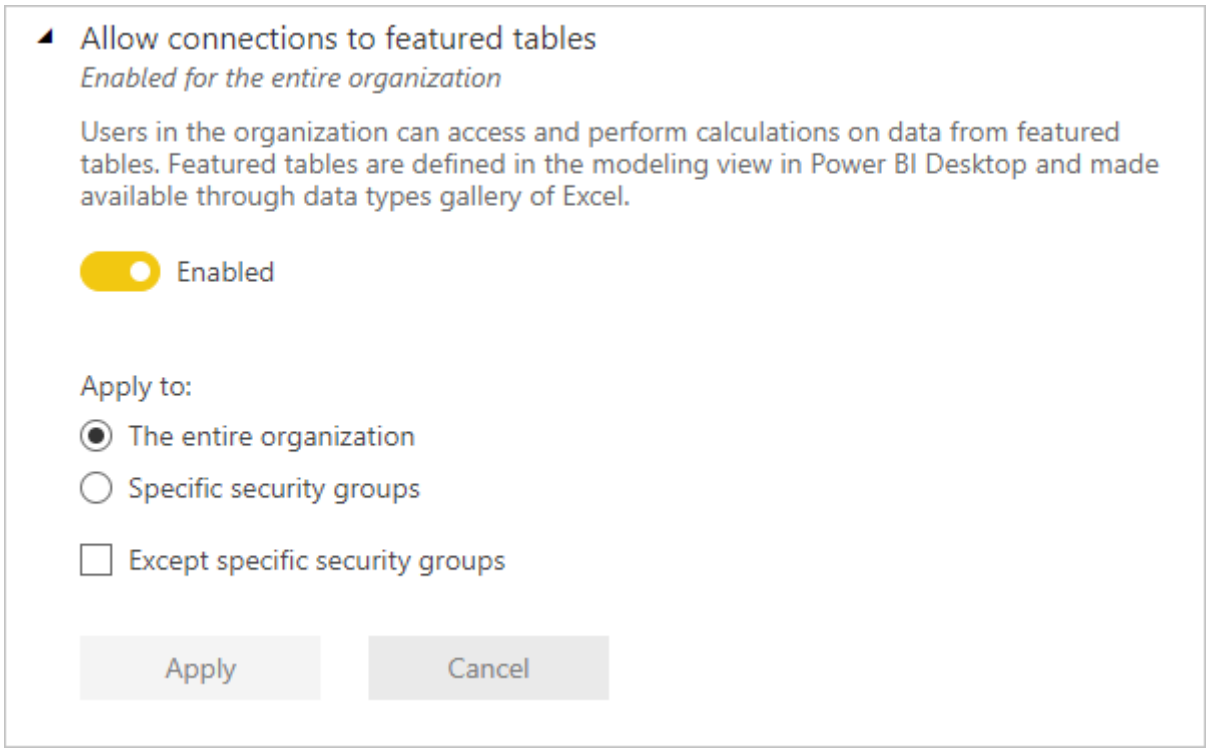
This setting enables you enable/disable the ability of users in your organization to promote their published content to the **Featured** section of the Power BI Home page.



Featured content can be managed on the **Featured content** page in the Admin portal. See Manage featured content.

Allow connections to featured tables

This setting lets Power BI admins control who in the organization can use featured tables in the Excel Data Types Gallery.



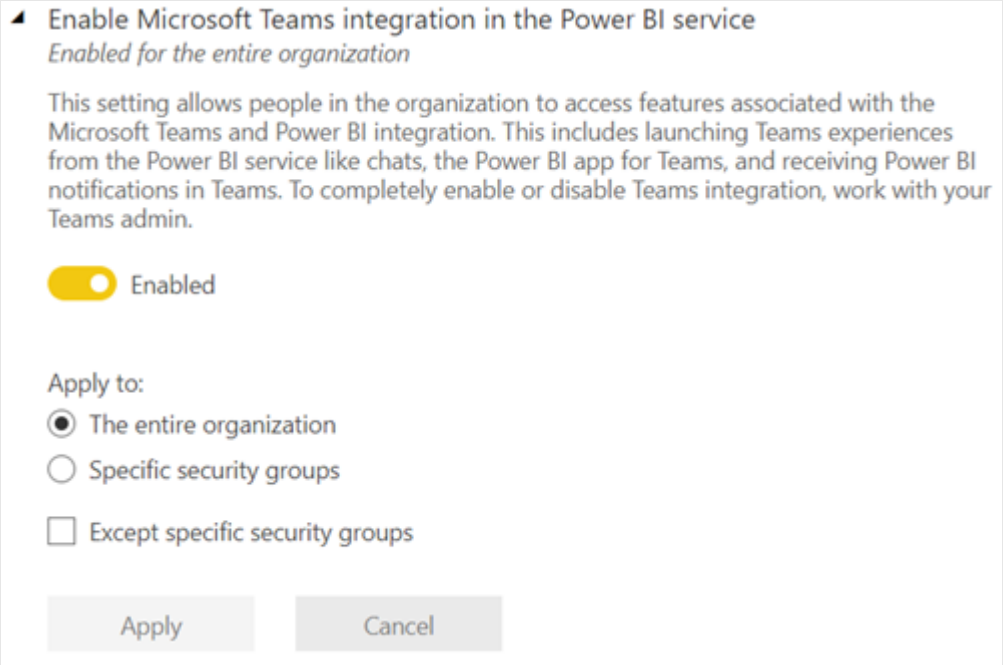
> **Note**

Connections to featured tables are also disabled if the **Allow live connections** setting is set to Disabled.

Read more about Power BI featured tables in Excel.

Microsoft Teams integration in the Power BI service

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 the Power BI app for 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.

The **Install Power BI app for Microsoft Teams automatically** tenant setting is added to the Power BI admin portal so Power BI admins can control the auto-install behavior. By

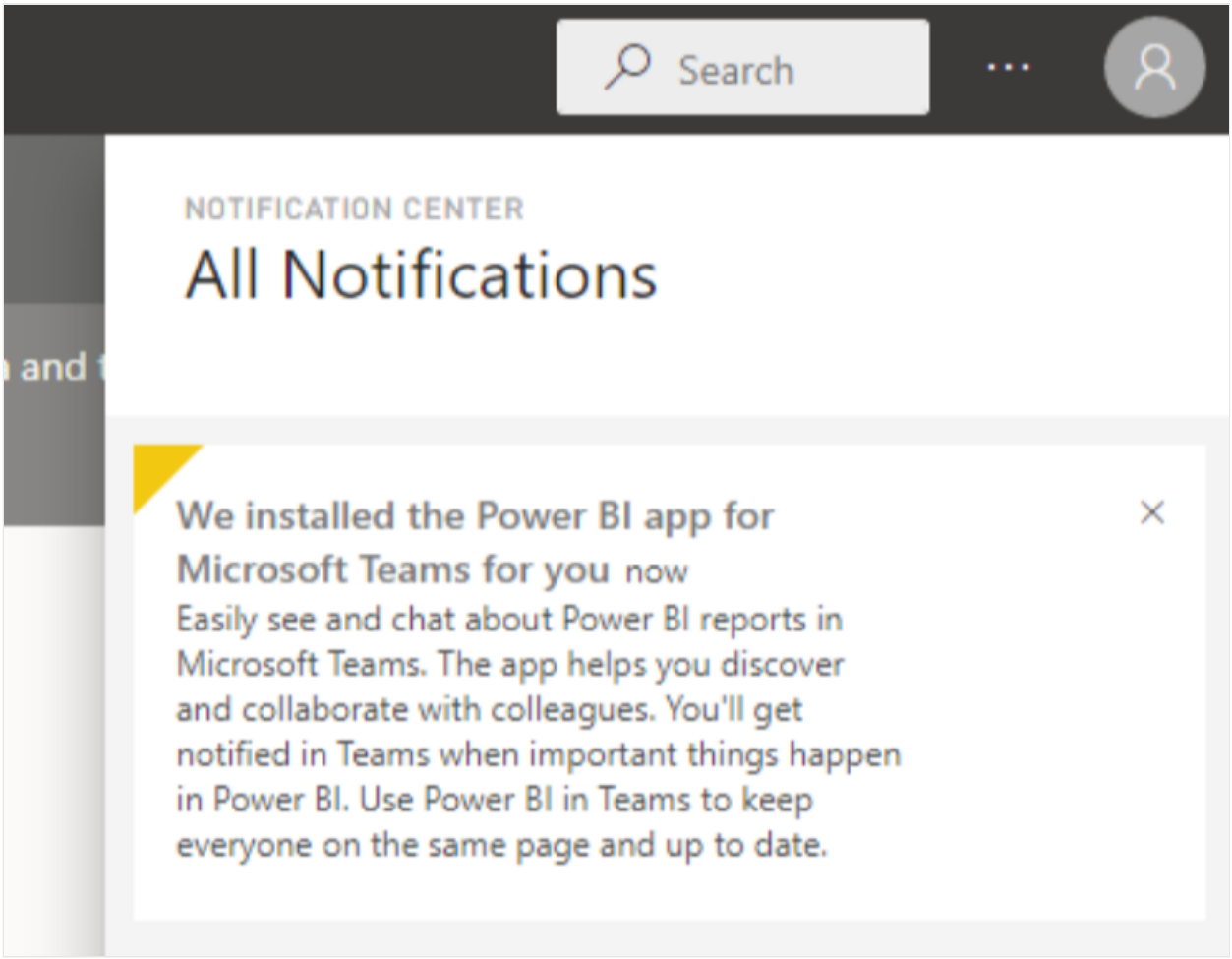
default, the auto-install is enabled.

The 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 (e.g. app.powerbi.com) in a web browser.

Initially, auto-install applies to new users the first time they visit the Power BI service in a web browser. Automatic installation will start occurring after November 1, 2021 for users who visit the Power BI service and meet the criteria.

When auto-install occurs, users see the following notification in the Power BI service notification pane.



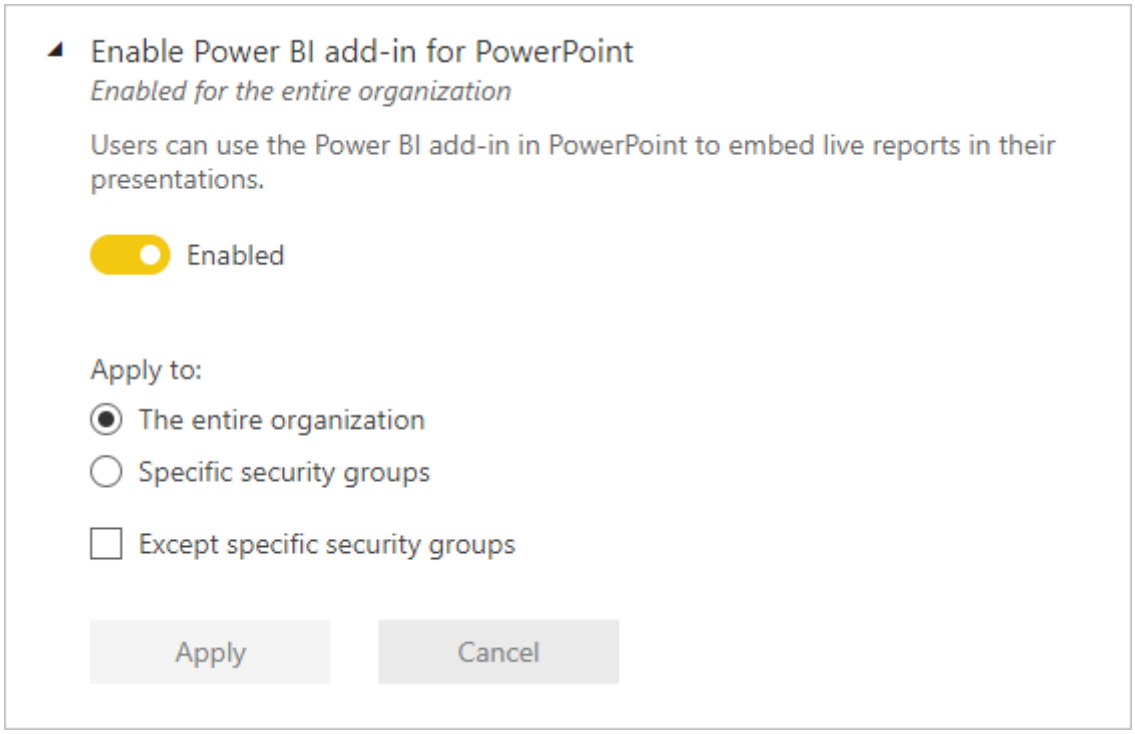
Read more about the Power BI app for Microsoft Teams.

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.

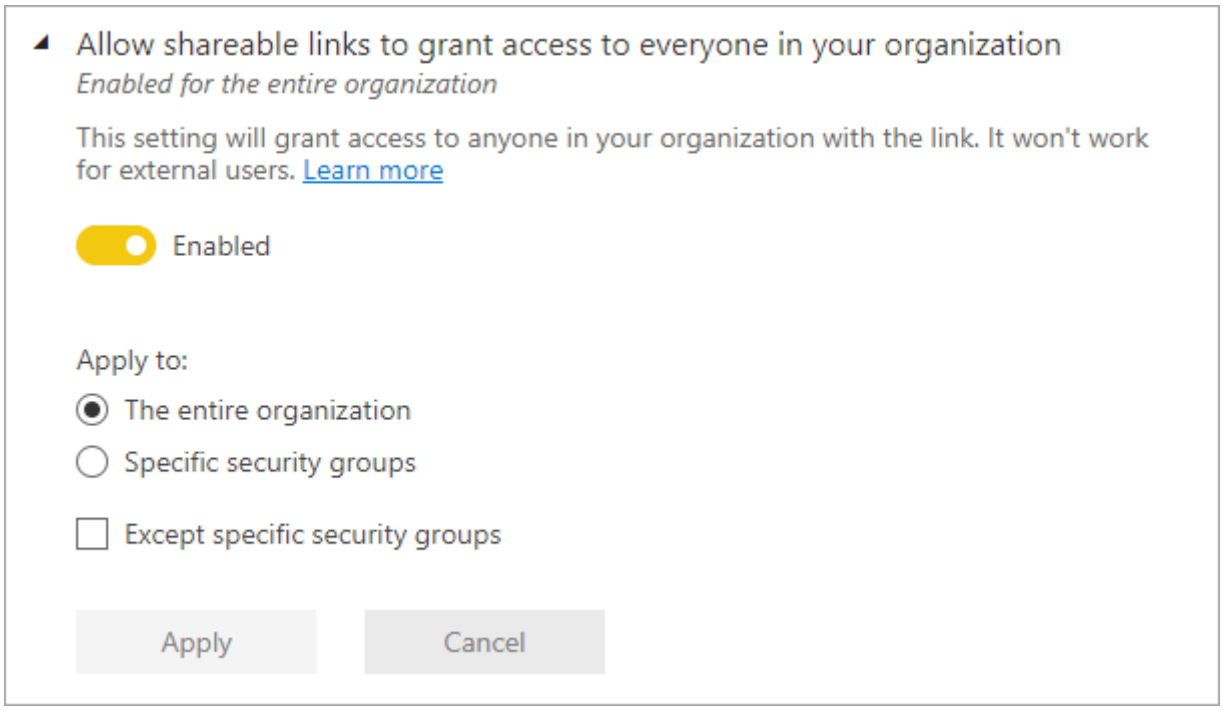
When this setting is enabled (default), entry points for opening a new PowerPoint presentation with the add-in already loaded are available in Power BI. When this setting is disabled, the entry points in Power BI are unavailable.

> **Note**
>
> Disabling this setting does not 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 disabled in both Power BI and PowerPoint.



Allow shareable links to grant access to everyone in your organization

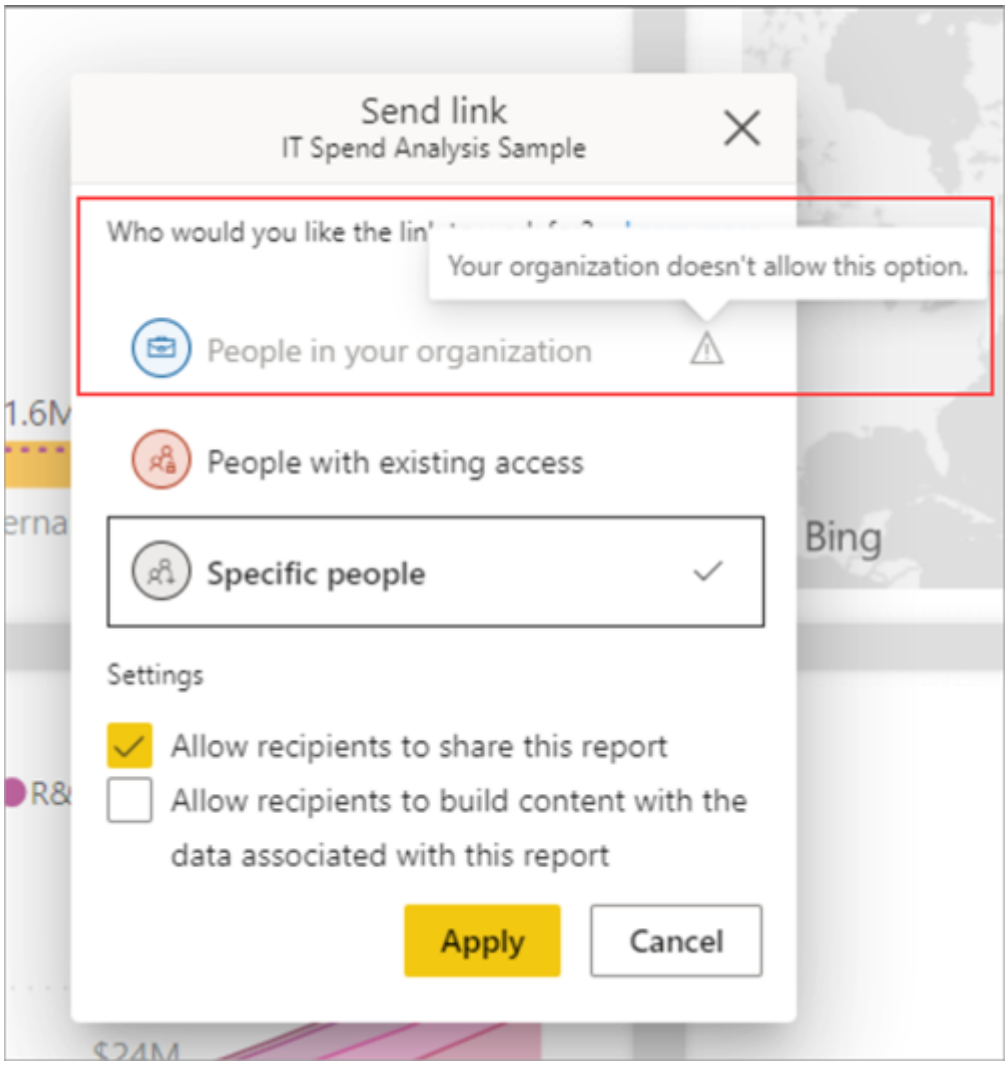
This tenant setting is available for admins looking to disable creating shareable links to **People in your organization**. You can find this option in the Admin portal by navigating to **Tenant settings** > **Export and sharing settings** > **Allow shareable links to grant access to everyone in your organization**.



As with other tenant settings, you can enable sharing links to **People in your organization** for:

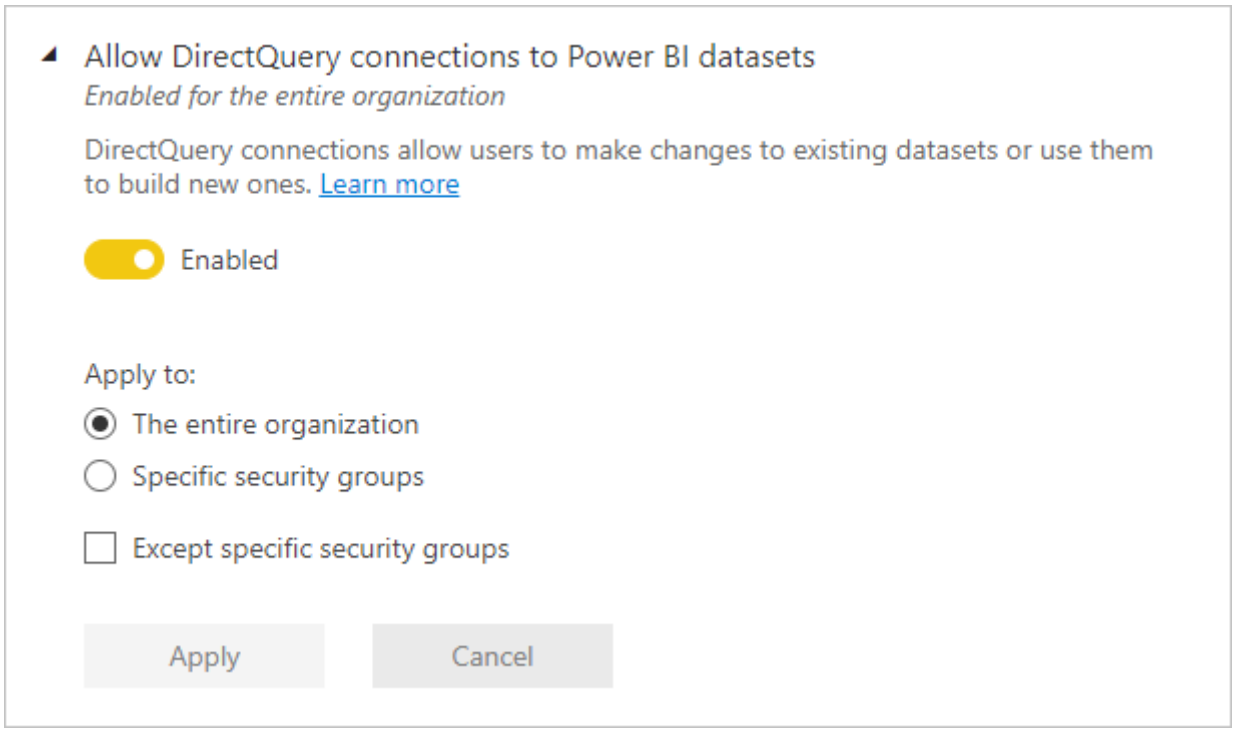
- **The entire organization**
- **Specific security groups**
- Or **Except specific security groups**

If this setting is disabled for a user with share permissions to a report, that user can only share the report via link to **Specific people** or **People with existing access**.



Allow DirectQuery connections to Power BI datasets

When this setting is enabled (default), users can use DirectQuery to connect to Azure Analysis Services or Power BI datasets. See Using DirectQuery for Power BI datasets and Azure Analysis Services for more detail.



Disabling this switch effectively stops users from publishing new composite models on Power BI datasets to the service. Existing reports that leverage a composite model on a Power BI dataset will continue to work, and users will still be able to create composite models using Desktop, but they will not be able to publish to the service.

> **Note**
>
> Live connections to Power BI datasets are not affected by this switch, nor are live or DirectQuery connections to Azure Analysis Services. These will continue to work regardless of whether the setting is enabled or disabled. In addition, any published reports that leverage a composite model on a Power BI dataset will continue to work even if the setting has been disabled after they were published.

Allow guest users to work with shared datasets in their own tenants

When this setting is turned on, Azure AD B2B guest users of datasets shared with them by users in your organization will be able to access and build on those datasets in their own tenant. See Use in-place dataset sharing to enable external users to view and share datasets in their own tenants (preview) - Admin info for detailed information.

Allow specific users to turn on external data sharing

As a Power BI admin, you can specify which users or user groups in your organization can share datasets externally with guests from a different tenant through the in-place mechanism. Disabling this setting prevents any user from sharing datasets externally by blocking the ability of users to turn on external sharing for datasets they own or manage. See Use in-place dataset sharing to enable external users to view and share datasets in their own tenants (preview) - Admin info for detailed information.

Next steps

- About tenant settings

Discovery tenant settings

Article • 10/03/2022 • 2 minutes to read

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 dataset owners can use to make their endorsed content discoverable by users who don't yet have access to it. See Discoverability for more detail.

Next steps

- About tenant settings

Content pack and app tenant settings

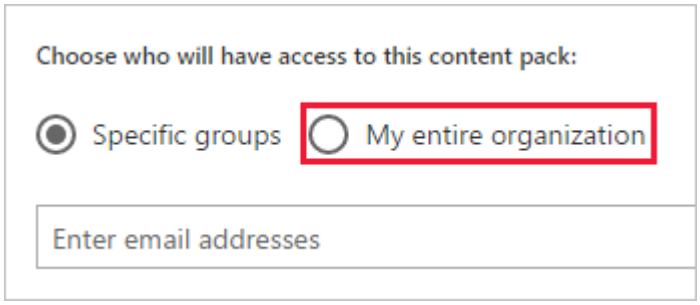
Article • 10/03/2022 • 2 minutes to read

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 content packs and apps to the entire organization

Admins use this setting to decide which users can publish content packs and apps to the entire organization, rather than specific groups. Learn more about publishing apps.

The following image shows the **My entire organization** option when creating a content pack.

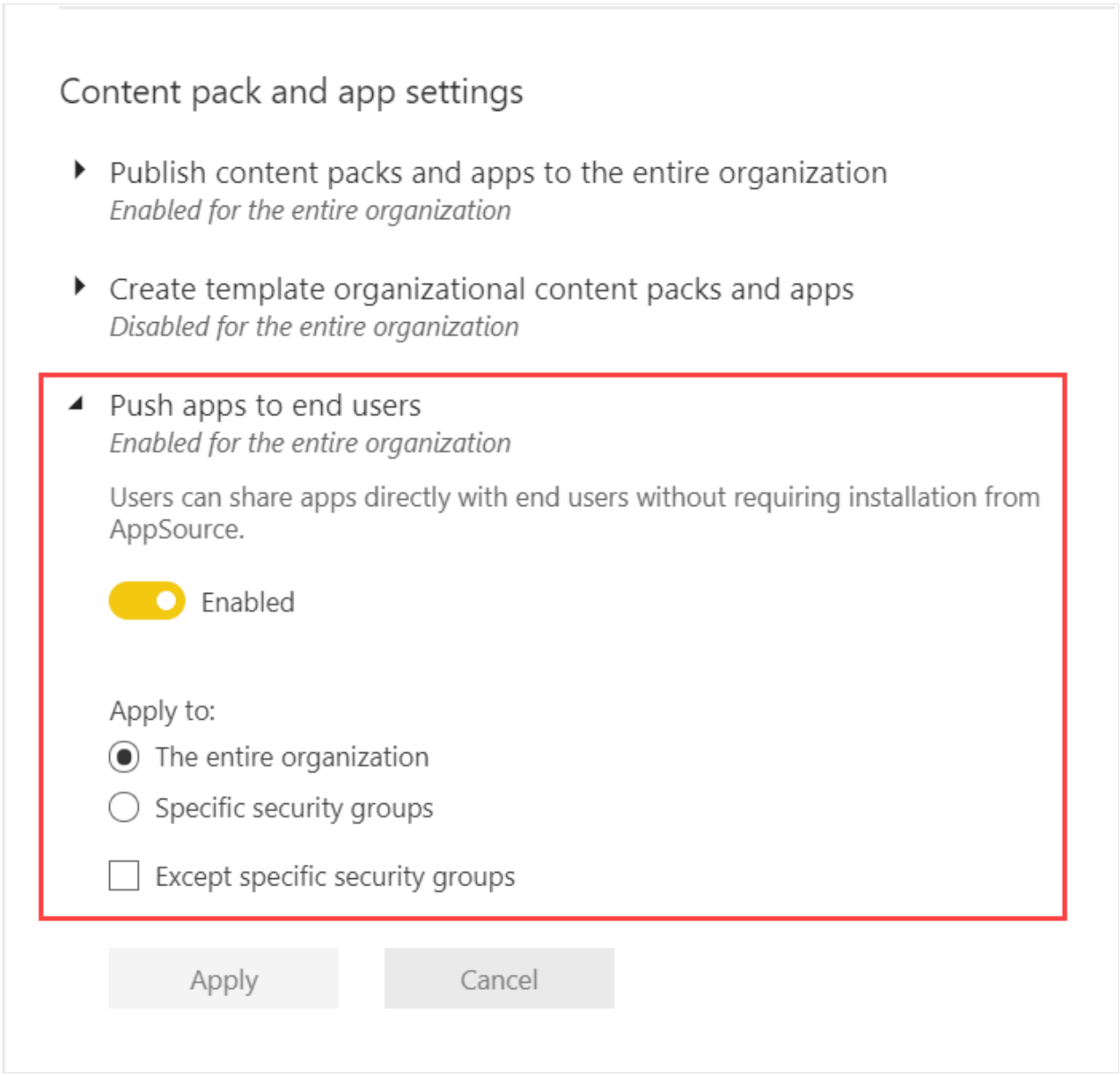


Create template apps and organizational content packs

Users in the organization can create template apps and organizational content packs that use datasets built on one data source in Power BI Desktop. Learn more about template apps.

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**. Learn more about automatically installing apps for end users.



Next steps

- About tenant settings

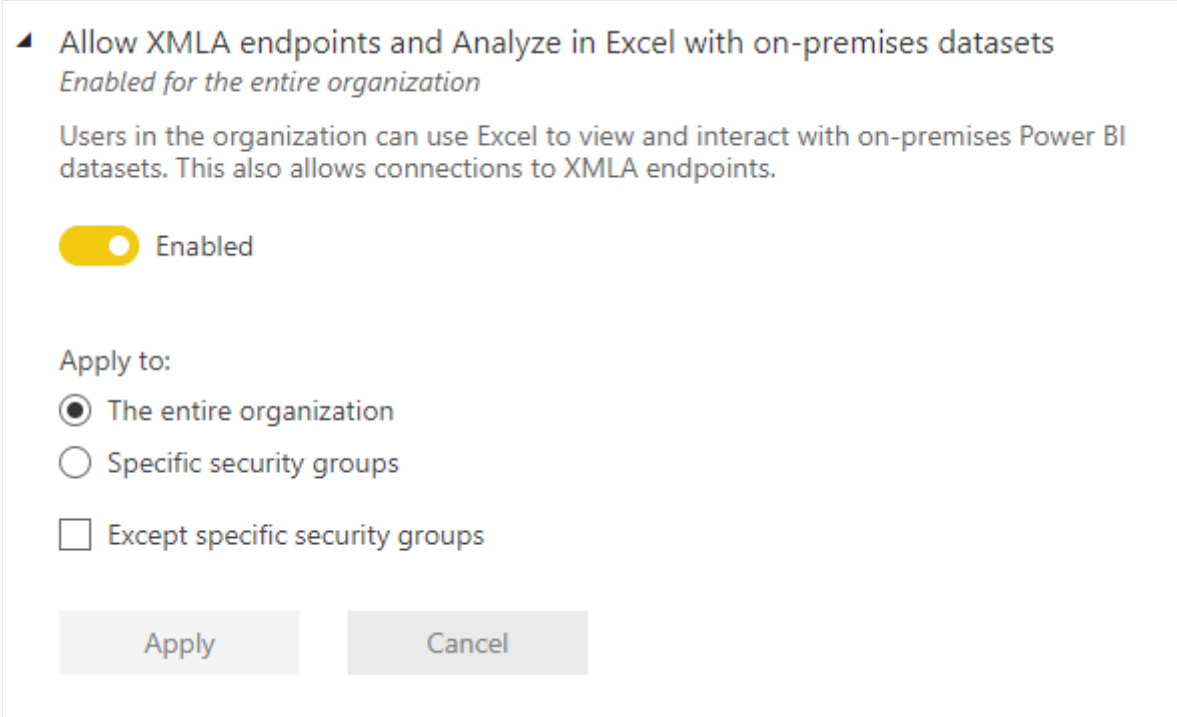
Integration tenant settings

Article • 10/03/2022 • 3 minutes to read

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.

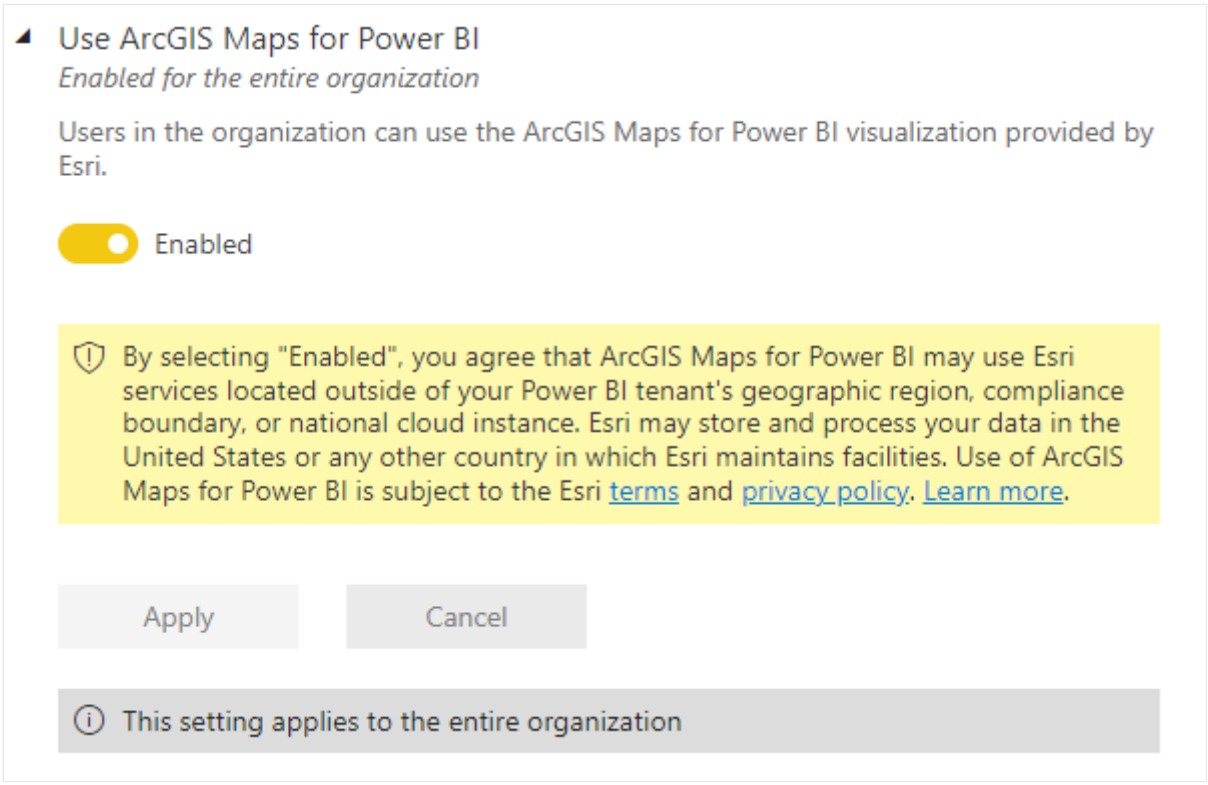
Allow XMLA endpoints and Analyze in Excel with on-premises datasets

When enabled, users in the organization can use Excel to view and interact with on-premises Power BI datasets. This also allows connections to XMLA endpoints. Learn more about analyzing in Excel.



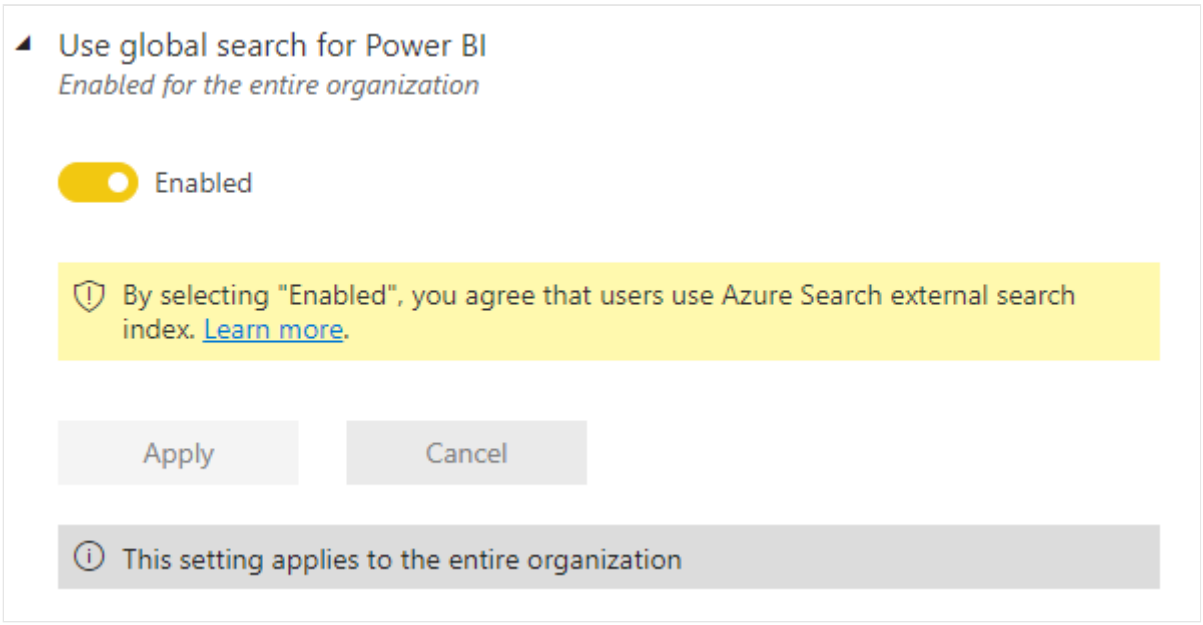
Use ArcGIS Maps for Power BI

When enabled, users in the organization can use the ArcGIS Maps for Power BI visualization provided by Esri. Learn more about ArcGIS maps.



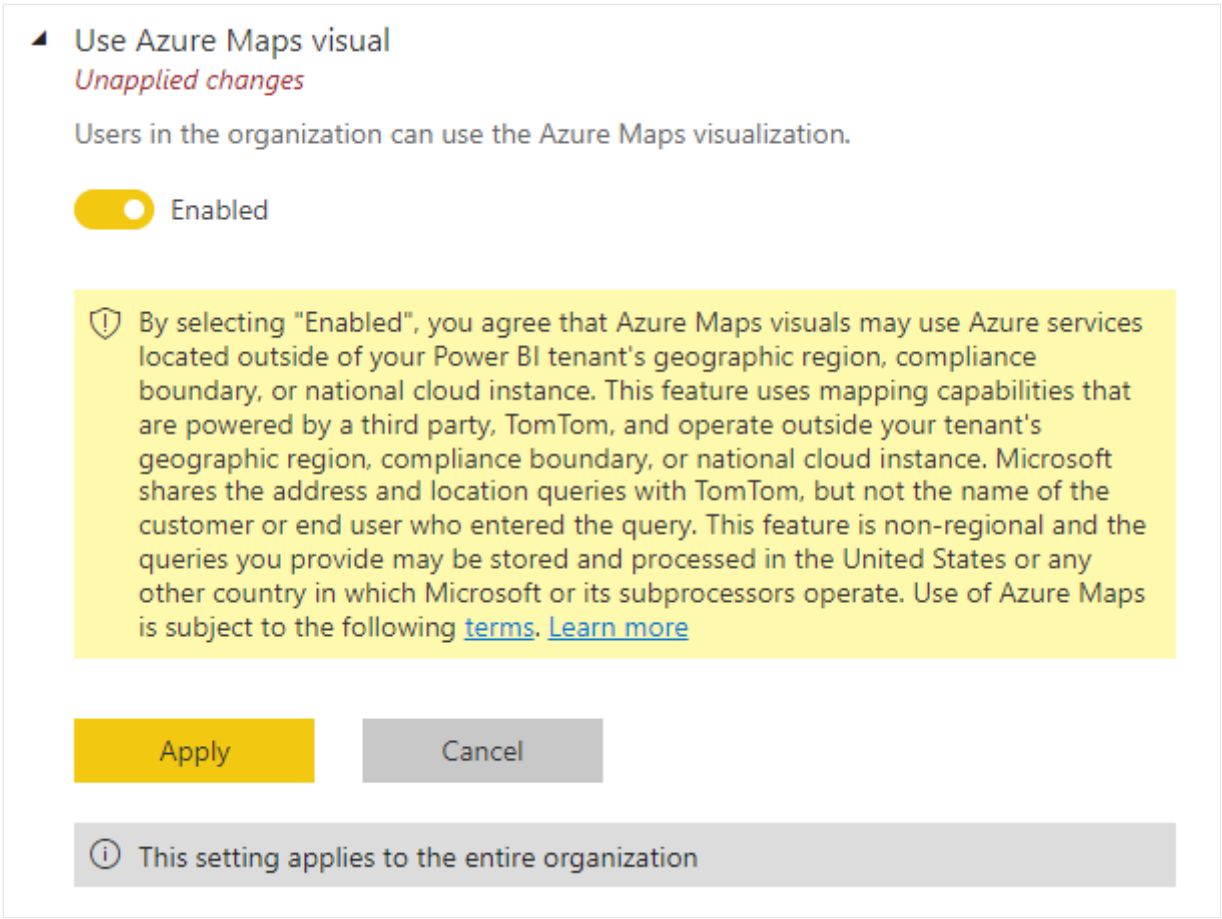
Use global search for Power BI

When enabled, users in the organization can use external search features that rely on Azure Search. See Navigation for Power BI business users: global search for more information.



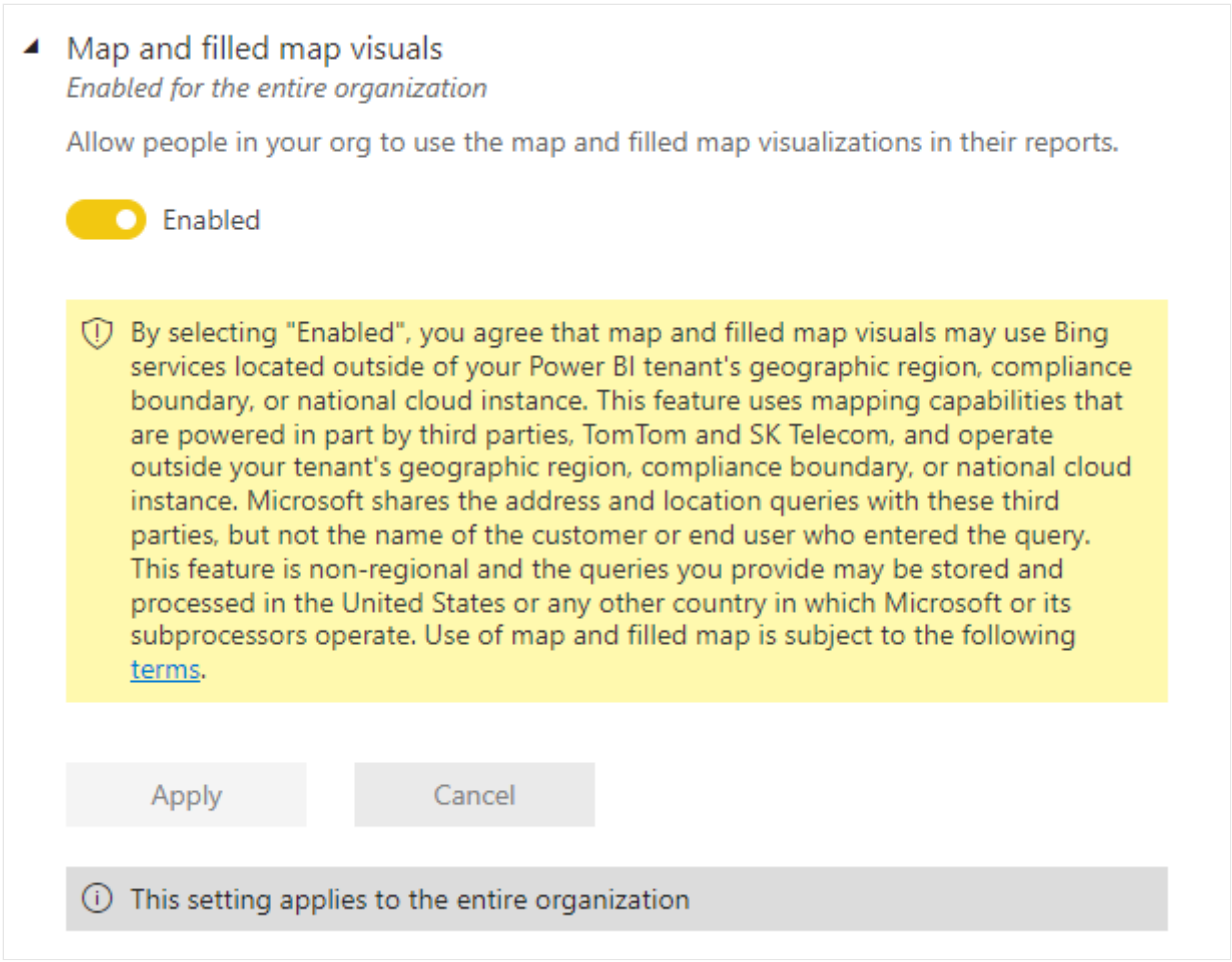
Use Azure Maps Visual

When enabled, users in the organization can use the Azure Maps visual for Power BI. See Get started with Azure Maps Power BI visual for more information.



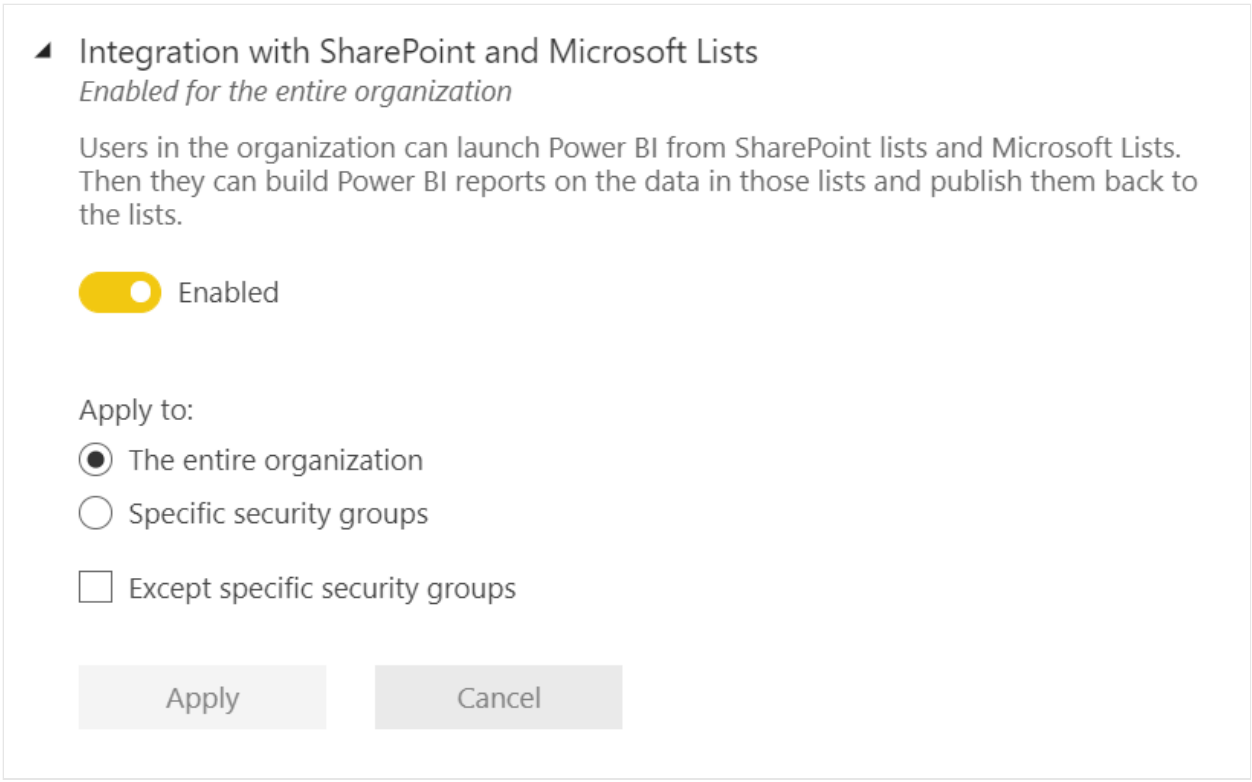
Map and filled map visuals

When enabled, users in the organization can use map and filled map visualizations in their reports.



Integration with SharePoint and Microsoft Lists

Users in the organization can create Power BI reports directly from SharePoint and Microsoft Lists. Then they can build Power BI 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 in **Tenant settings** > **Integration settings**.

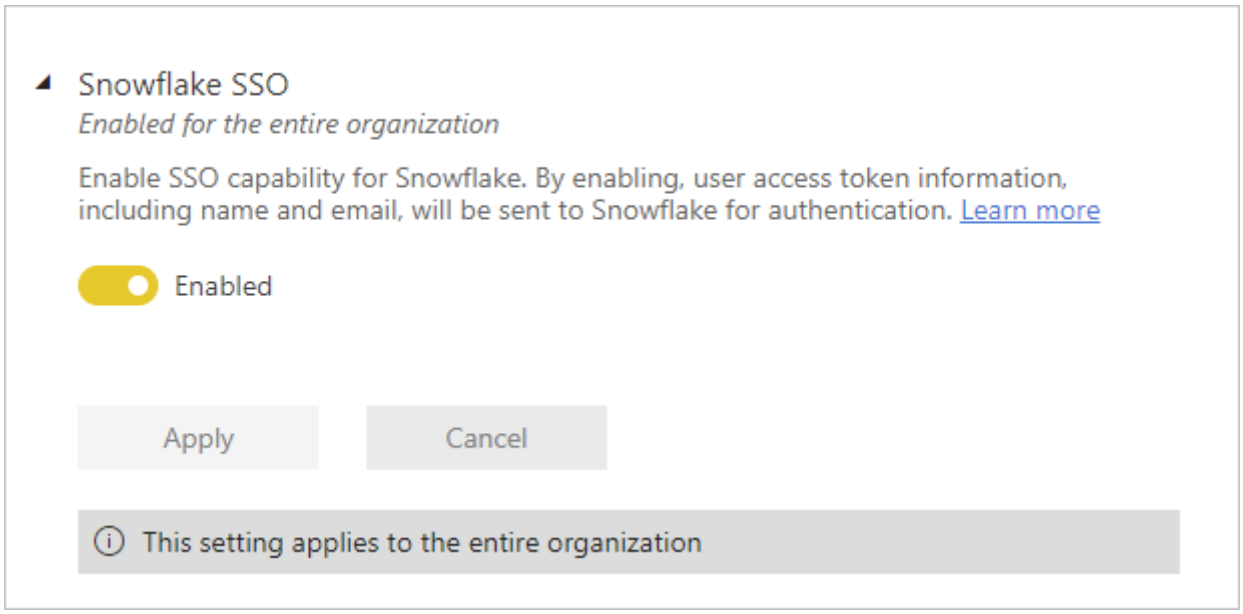


This feature is on by default. Even if the feature is disabled, in SharePoint and Microsoft Lists users will still see **Power BI** > **Visualize the list**, and any existing Power BI reports, on the **Integrate** menu. If they select **Visualize the list**, they go to an error page explaining that their admin has disabled the feature.

Learn more about creating reports from SharePoint and Microsoft Lists.

Snowflake (SSO)

For dataset owners to be able to enable single sign-on for DirectQuery connections to Snowflake in dataset settings, a Power BI admin must enable the **Snowflake SSO** setting. This setting approves sending Azure AD credentials to Snowflake for authentication for the entire organization. See Connect to Snowflake in Power BI Service for more detail.



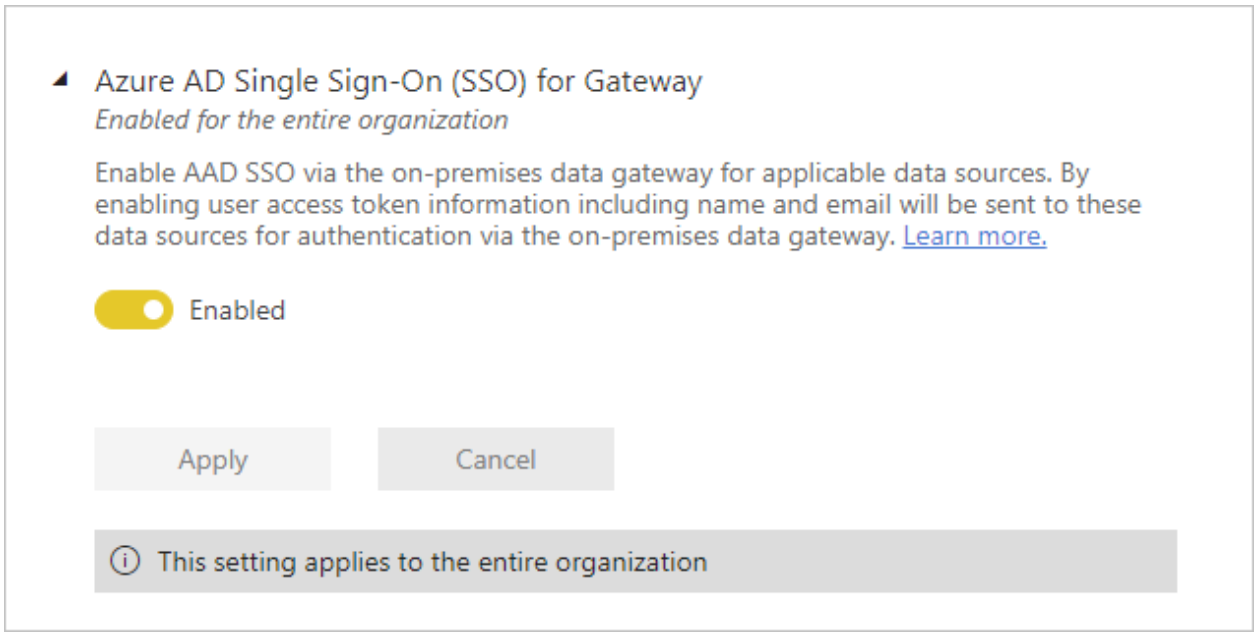
Azure AD Single Sign-On (SSO) for Gateway

This setting enables Azure Active Directory (Azure AD) single sign-on (SSO) through on-premises data gateways to cloud data sources that rely on Azure AD-based authentication. It gives seamless Azure AD 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 Azure AD 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 Azure AD 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 Azure AD single sign-on feature is disabled by default for on-premises data gateways. As a Power BI admin, you must enable the **Azure AD Single Sign-On (SSO) for Gateway** tenant setting (shown below) in the Power BI admin portal before data sources can be enabled for Azure AD 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.



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 dataset that are being to create the component. For more detail, see Power BI content management in Power Apps solutions and About Power BI in Power Apps Solutions.

This setting is on by default. To change the setting, go to the Power BI Admin portal, select **Tenant settings** > **Integration settings** > **Power Platform Solutions Integration (Preview)**, and set the toggle as desired.

Next steps

- About tenant settings

Power BI visuals tenant settings

Article • 10/03/2022 • 2 minutes to read

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.

Next steps

- About tenant settings

R and Python visuals tenant settings

Article • 10/03/2022 • 2 minutes to read

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. Learn more about R visuals.

> **Note**
>
> This setting applies to the entire organization and cannot be limited to specific groups.

Next steps

- About tenant settings

Audit and usage tenant settings

Article • 10/24/2022 • 2 minutes to read

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 audit logs for internal activity auditing and compliance

Users in the organization can use auditing to monitor actions taken in Power BI by other users in the organization. Learn more

This setting must be enabled for audit log entries to be recorded. There can be up to a 48-hour delay between enabling auditing and being able to view audit data. If you don't see data immediately, check the audit logs later. There can be a similar delay between getting permission to view audit logs and being able to access the logs.

> **Note**
>
> This setting applies to the entire organization and cannot be limited to specific groups.

Usage metrics for content creators

When this setting is on, users in the organization can see usage metrics for dashboards, reports, and datasets that they have appropriate permissions for. Learn more about usage metrics.

To turn on this setting, go to **Admin portal** > **Tenant settings** > **Audit and usage settings** and turn on the **Usage metrics for content creators** setting.

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. Learn more about usage metrics.

Per-user data is enabled for usage metrics by default, and content creator account information is included in the metrics report. If you do not 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 will then show in the report as *Unnamed*.

Azure Log Analytics connections for workspace administrators

Power BI integration with Azure Log Analytics enables Power BI administrators and Premium Workspace owners to connect their Premium Workspaces to Azure Log Analytics to monitor the connected workspaces. Power BI administrators can enable this feature by going to **Admin Portal** > **Tenant settings** > **Audit and usage settings** and turning on the **Azure Log Analytics connections for workspace administrators** setting. When the switch is on, administrators and Premium Workspace owners can configure **Azure Log Analytics for Power BI**.

Next steps

- About tenant settings

Dashboard tenant settings

Article • 10/03/2022 • 2 minutes to read

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

Users in the organization can add and view web content tiles on Power BI dashboards. Learn more

> **Note**
>
> This may expose your org to security risks via malicious web content.

Next steps

- About tenant settings

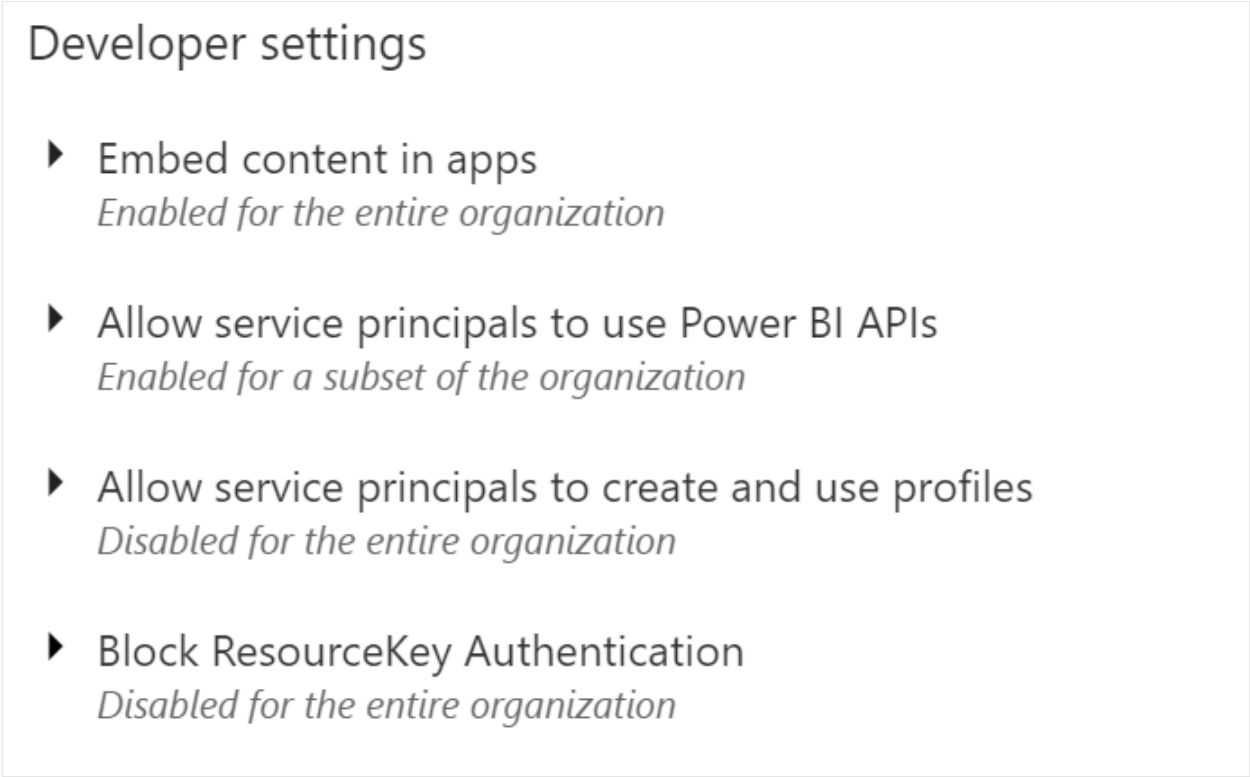
Developer tenant settings

Article • 10/03/2022 • 2 minutes to read

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.

You can:

- Embed content in apps
- Allow service principals to use Power BI APIs
- Allow service principals to create and use profiles
- Block ResourceKey Authentication



To manage Power BI developer settings, you must be a Global Admin in Office 365, or have been assigned the Power BI service administrator role. For more information about the Power BI service administrator role, see Understanding the Power BI admin role.

> **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. Learn more.

Allow service principals to use Power BI APIs

Web apps registered in Azure Active Directory (Azure AD) will 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.

You can control who can access service principals by creating dedicated security groups and using these groups in any Power BI tenant level-settings. Learn more.

Allow service principals to create and use profiles

An app owner with many customers can use service principal profiles as part of a multi-tenancy solution to enable better customer data isolation and establish tighter security boundaries between customers. Learn more.

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.

Next steps

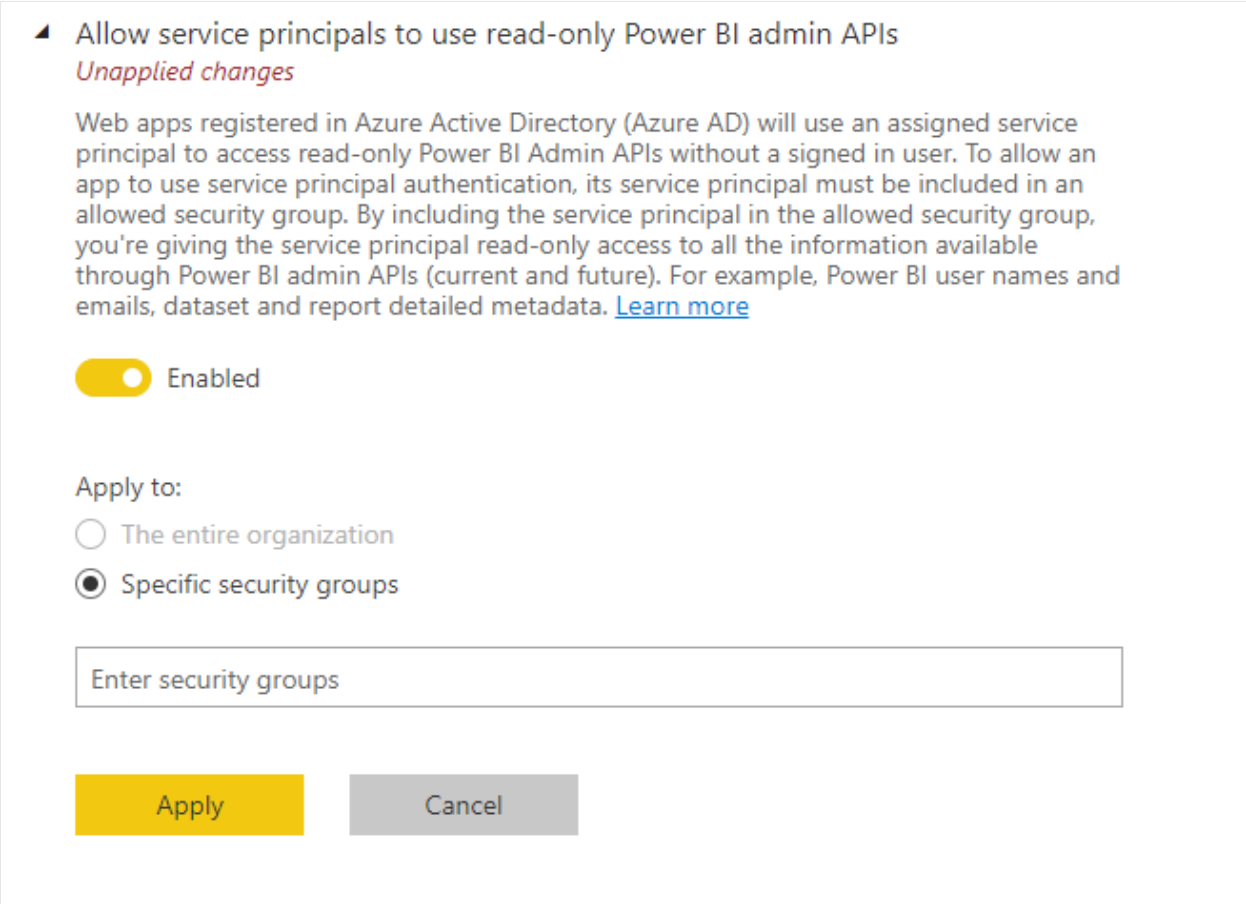
About tenant settings

Admin API tenant settings

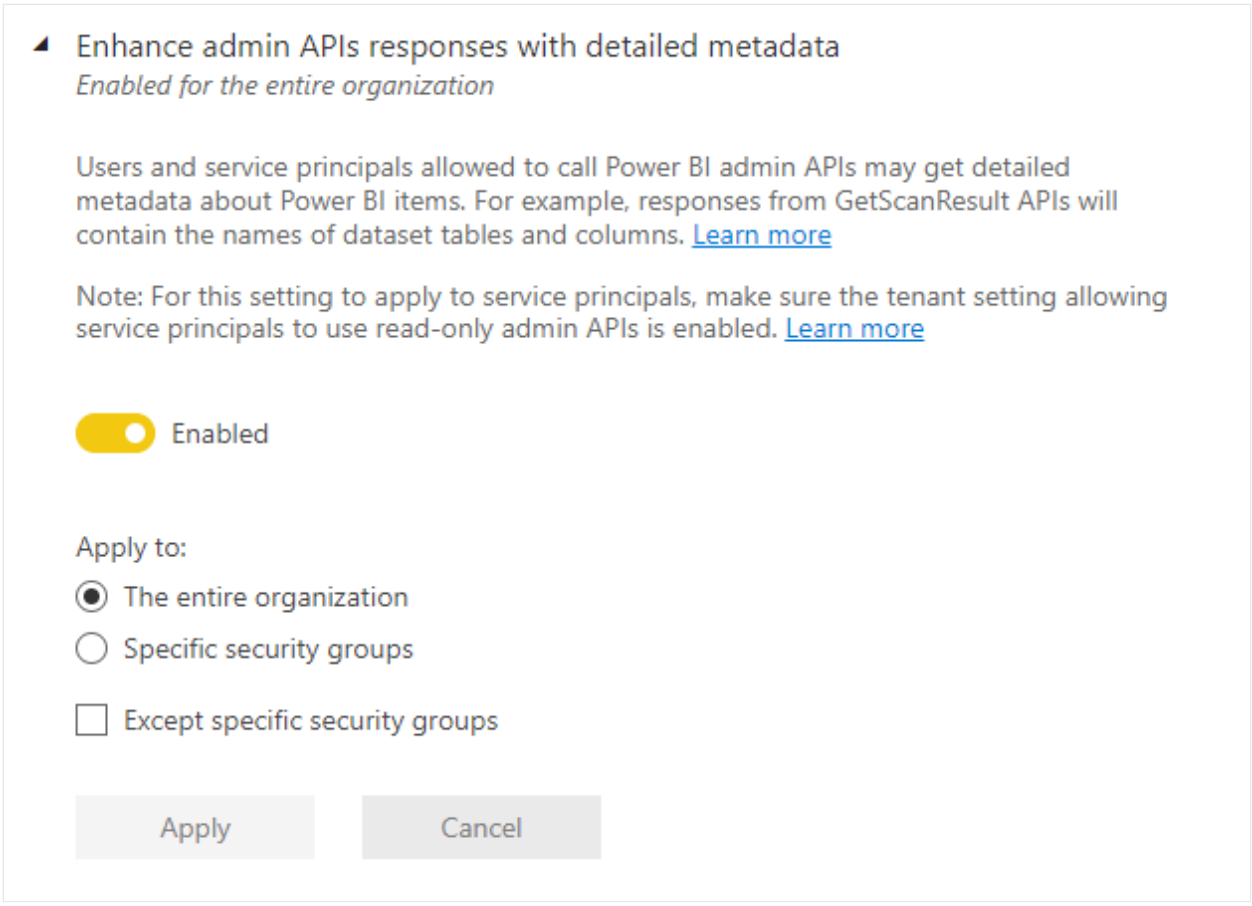
Article • 10/03/2022 • 2 minutes to read

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.

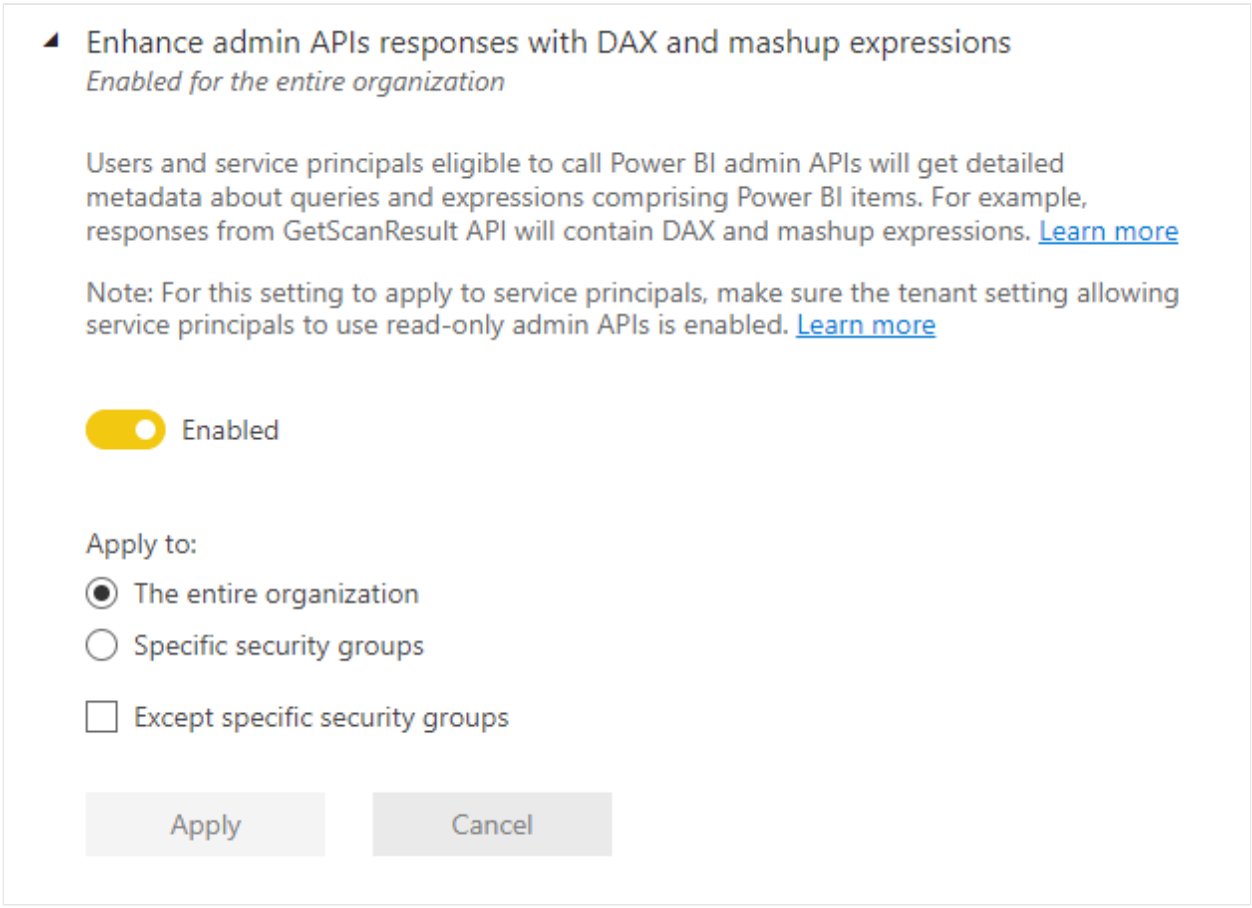
Allow service principals to use read-only Power BI admin APIs



Enhance admin APIs responses with detailed metadata



Enhance admin APIs responses with DAX and mashup expressions



Next steps

- About tenant settings

Dataflow tenant settings

Article • 10/03/2022 • 2 minutes to read

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 dataflows

Users in the organization can create and use dataflows. For an overview of dataflows, see Self-service data prep in Power BI. To enable dataflows in a Premium capacity, see Configure workloads.

> **Note**
>
> This setting applies to the entire organization and cannot be limited to specific groups.

Next steps

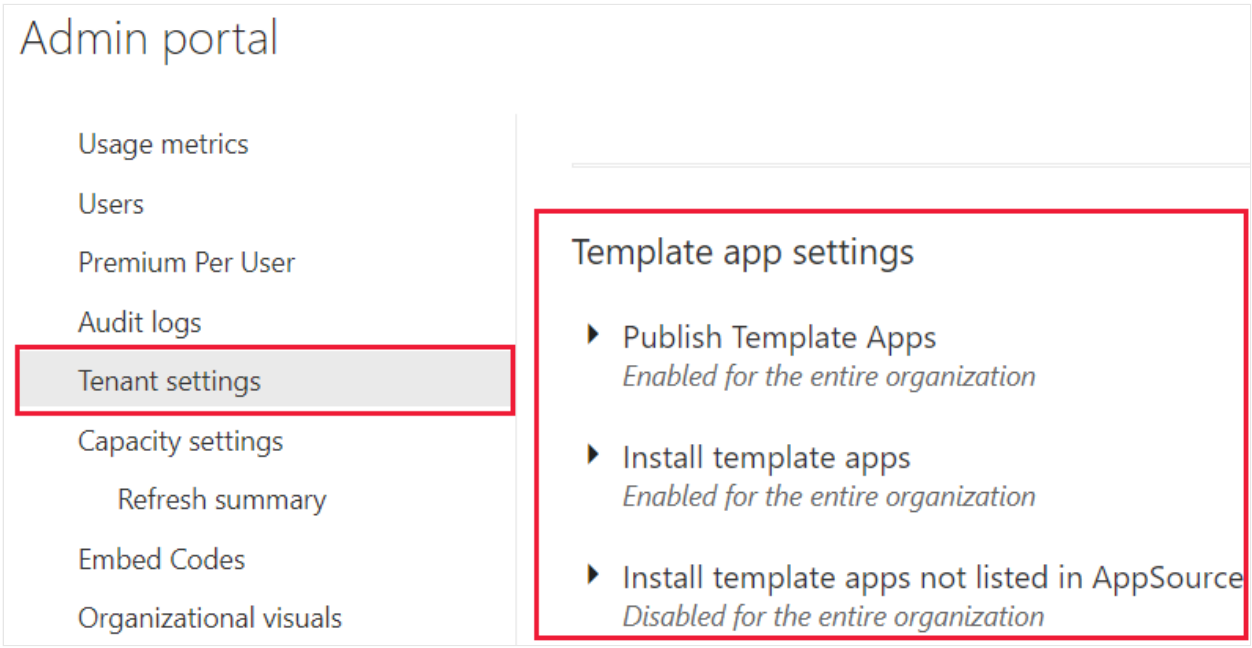
- About tenant settings

Template app tenant settings

Article • 10/03/2022 • 2 minutes to read

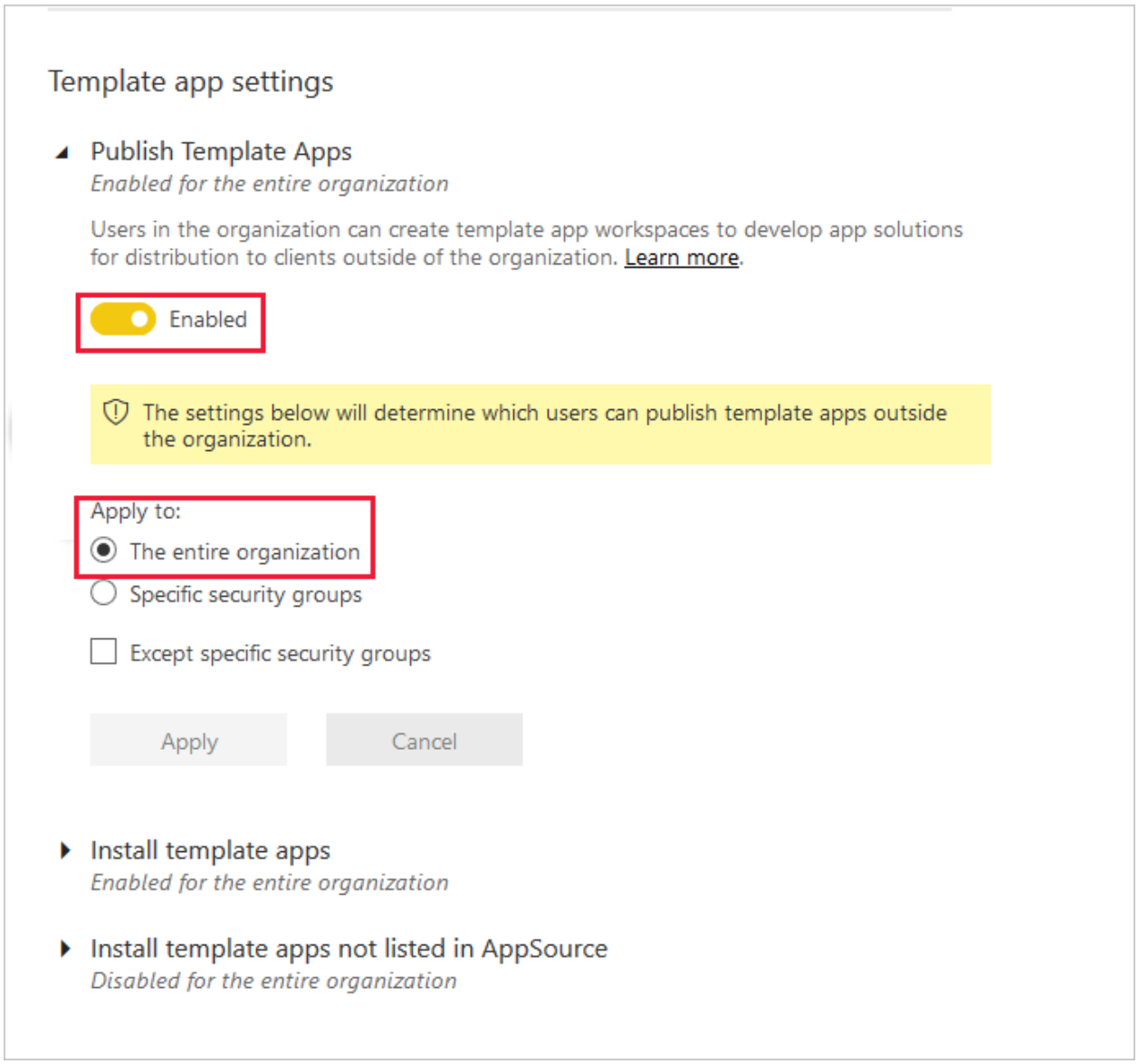
These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Three settings control template apps ability to publish or install template apps.



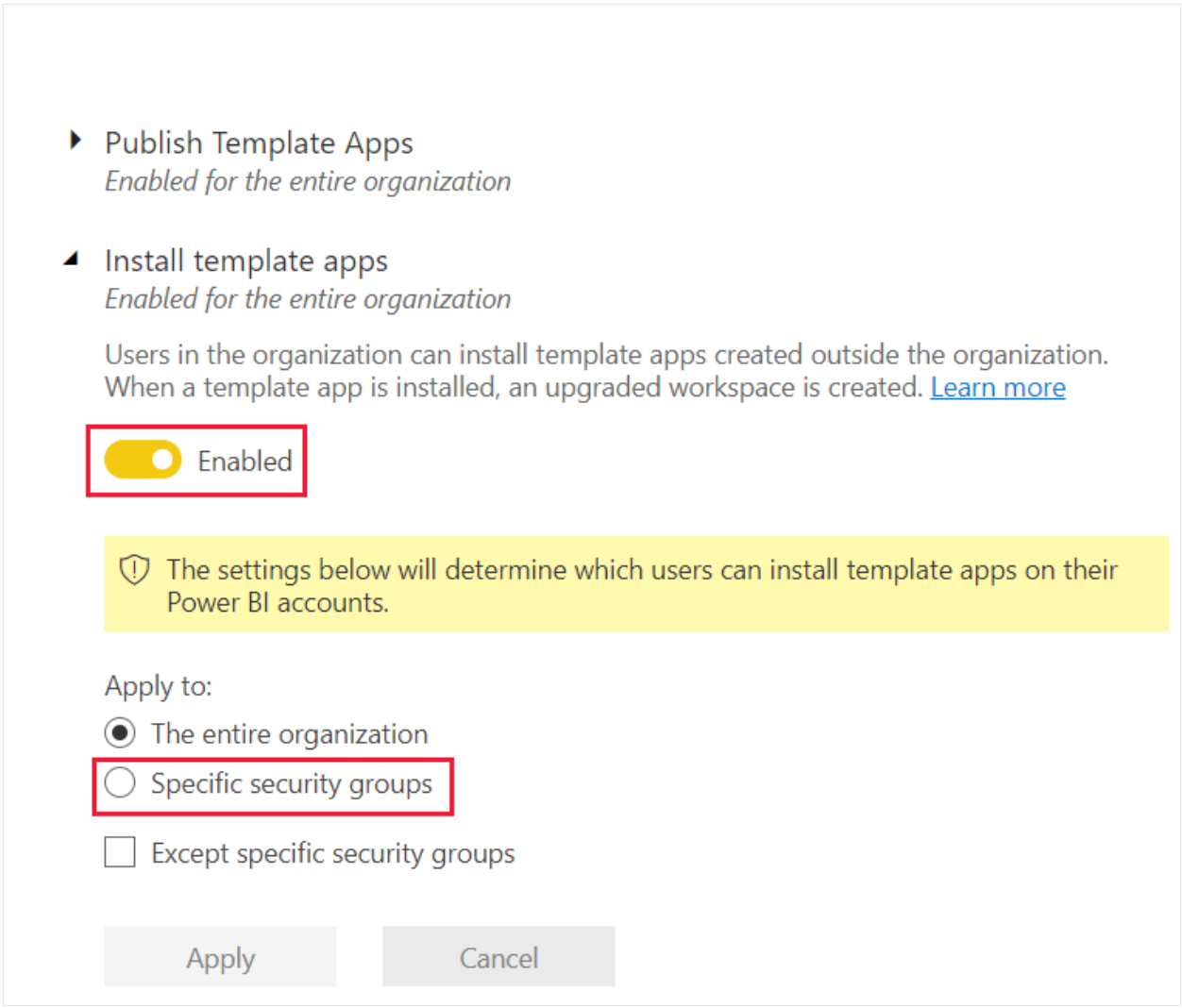
Publish Template Apps

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 AppSource or other distribution methods.



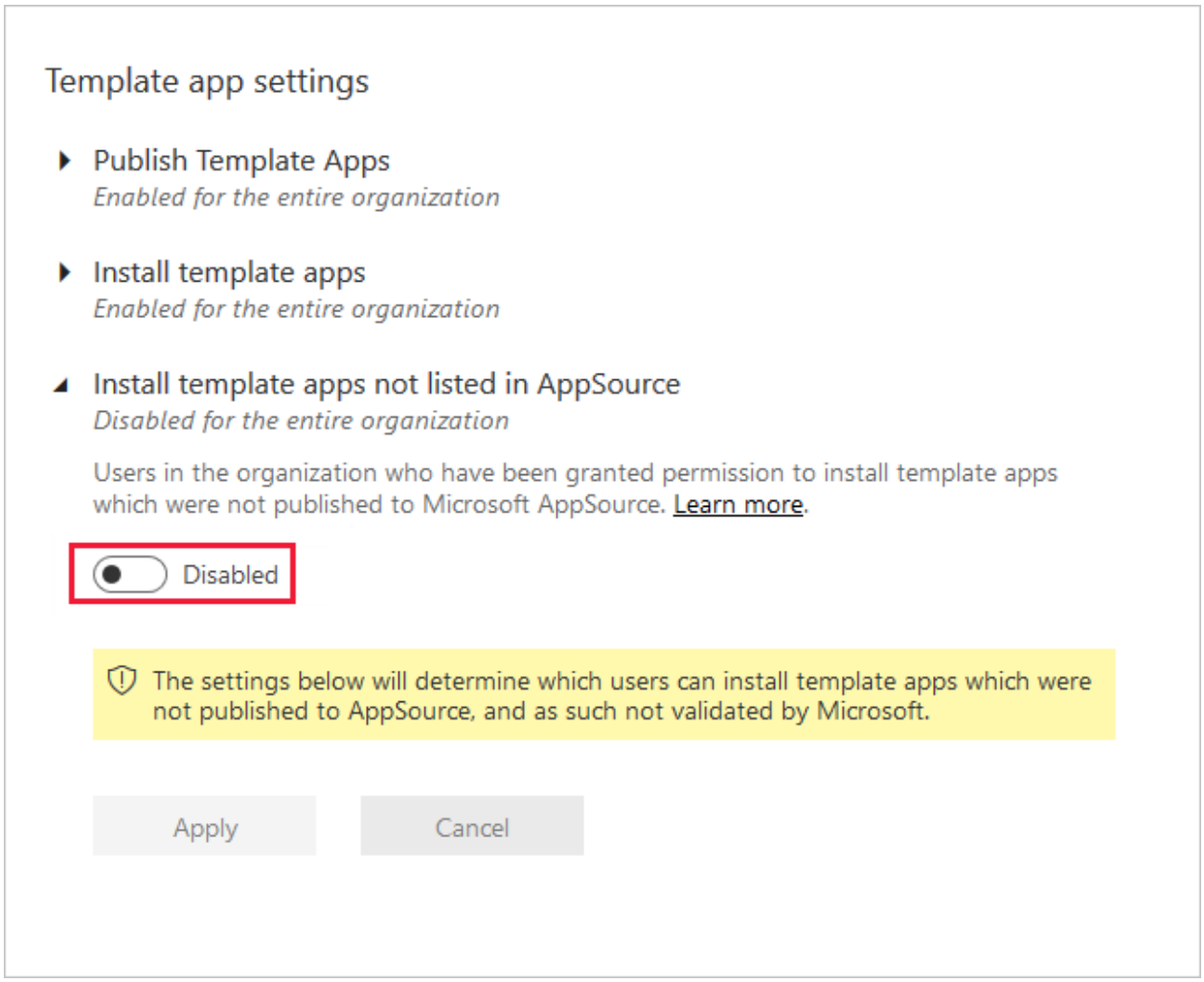
Install template apps listed on AppSource

Users in the organization can download and install template apps **only** from AppSource. Control which specific users or security groups can install template apps from AppSource.



Install template apps not listed on AppSource

Control which users in the organization can download and install template apps **not listed on** AppSource.



Next steps

- About tenant settings

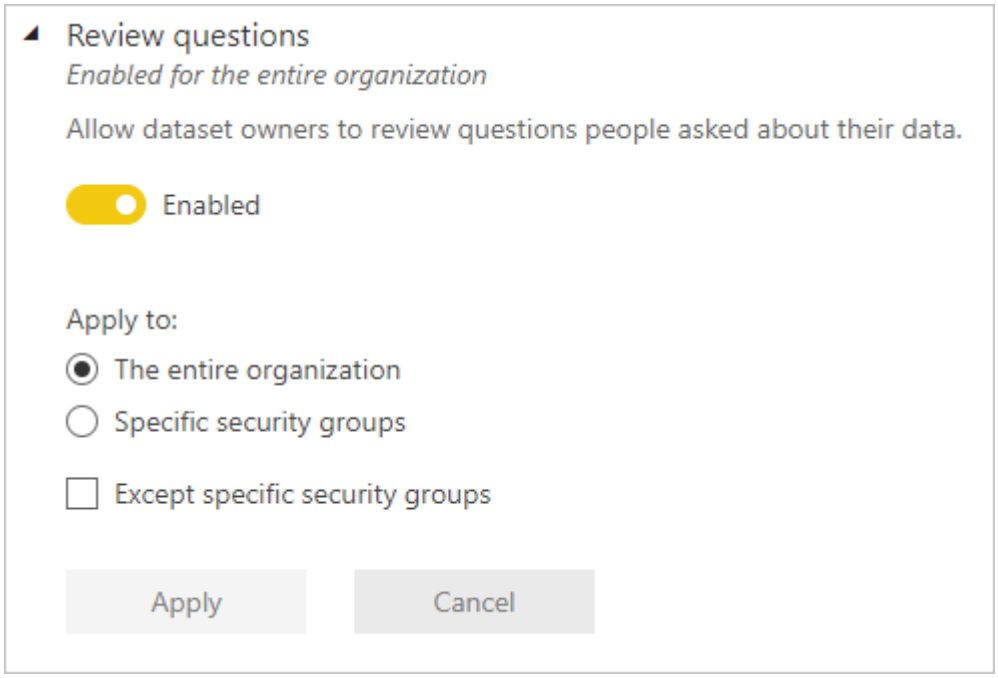
Q&A tenant settings

Article • 10/03/2022 • 2 minutes to read

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.

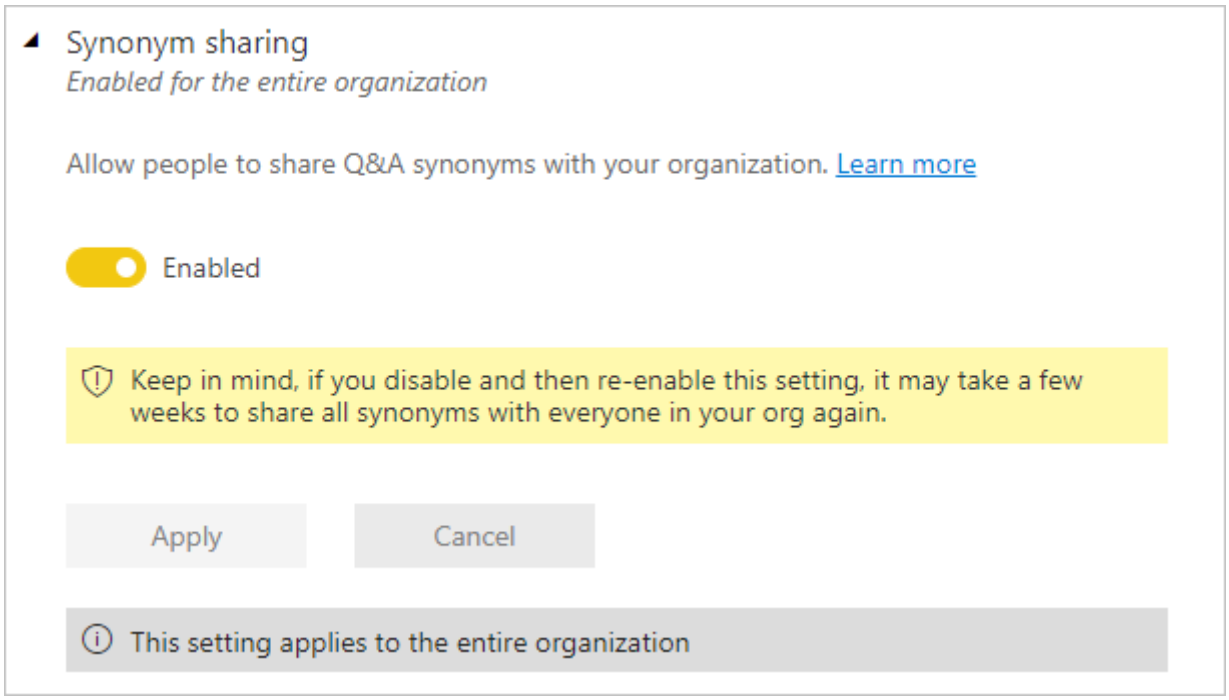
Review questions

When this setting is enabled, dataset owners can review questions end-users ask about their data.



Synonym sharing

When this setting is enabled, users can share Q&A synonyms as suggested terms with everyone in your organization.



> **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.

Next steps

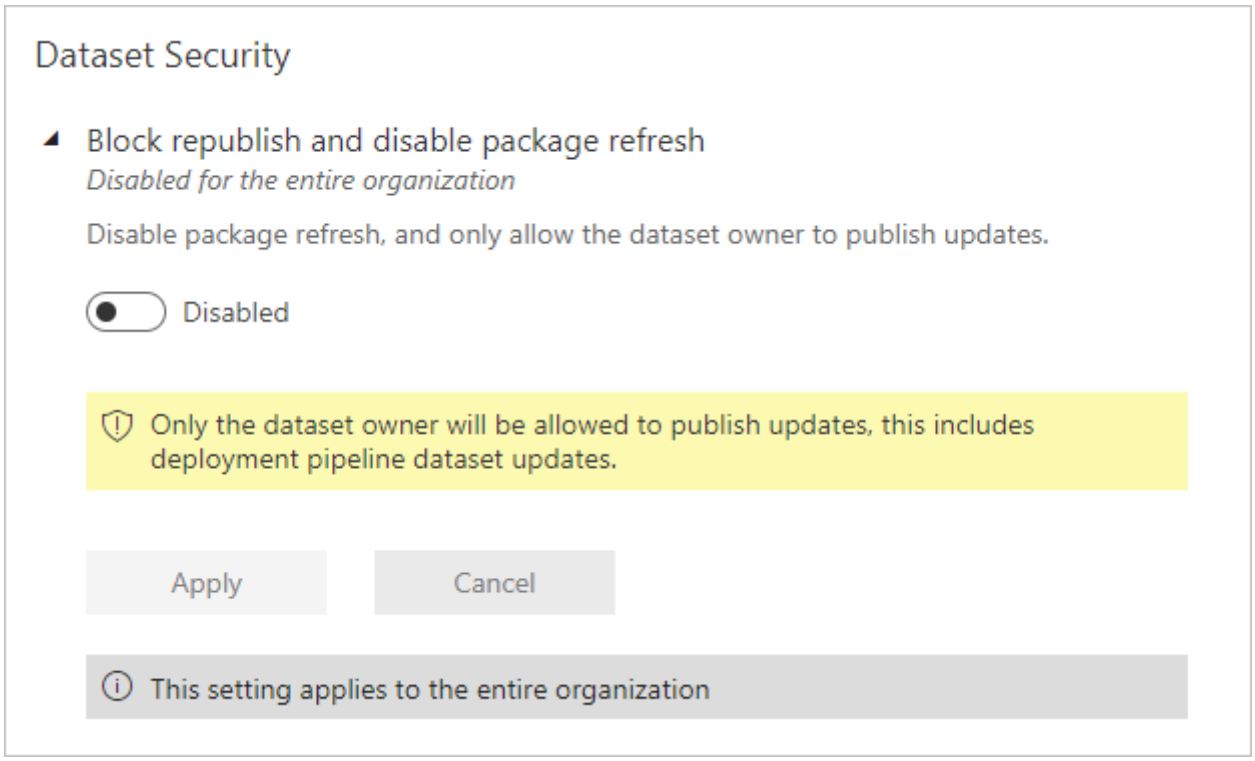
- About tenant settings

Dataset Security tenant setting

Article • 10/03/2022 • 2 minutes to read

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



Next steps

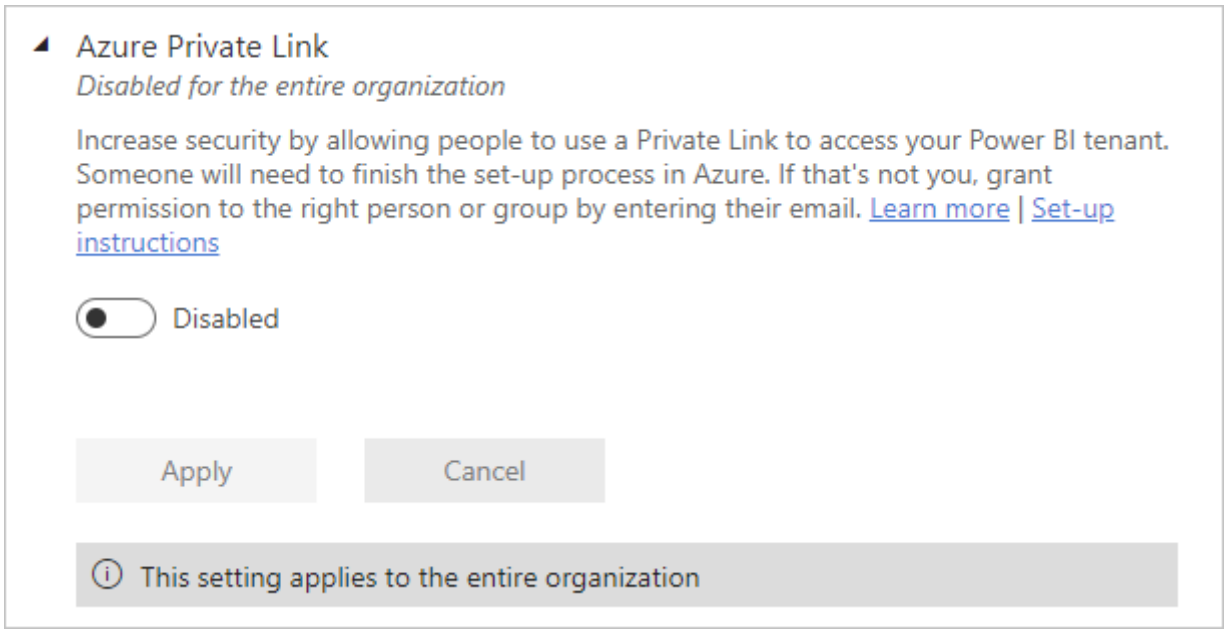
- About tenant settings

Advanced networking tenant settings

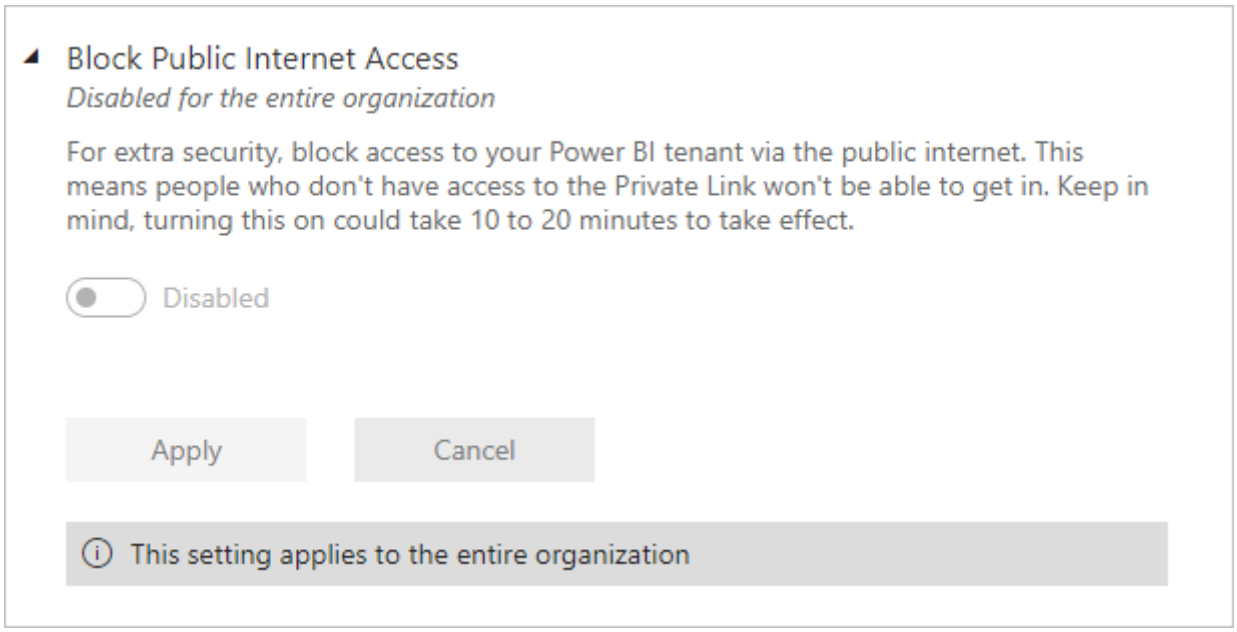
Article • 10/03/2022 • 2 minutes to read

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



Block Public Internet Access



Next steps

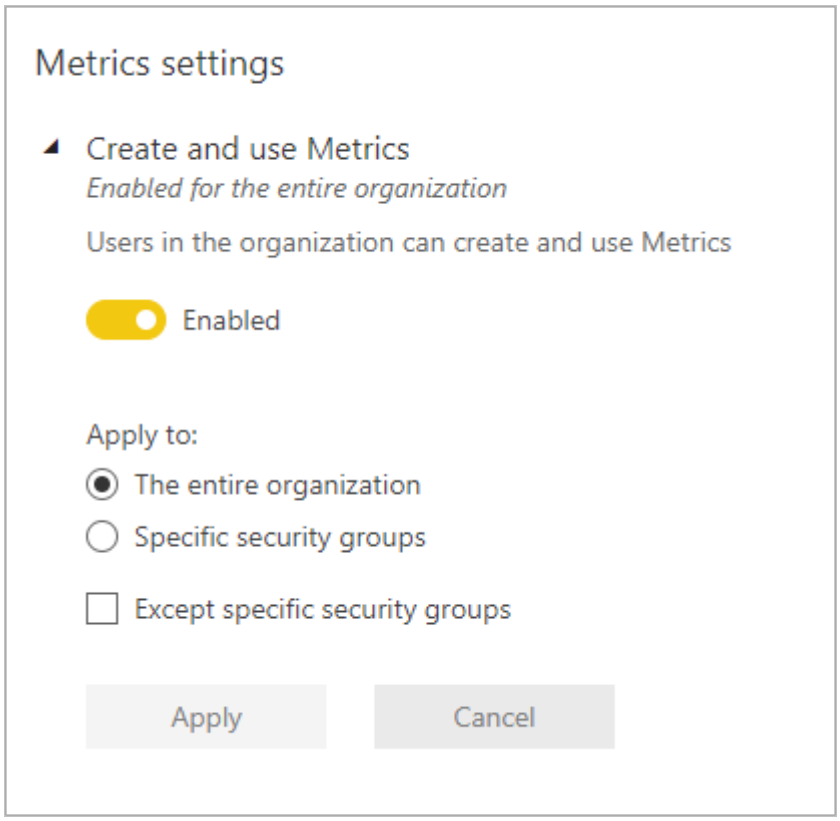
- About tenant settings

Metrics tenant settings

Article • 10/03/2022 • 2 minutes to read

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



Next steps

- About tenant settings

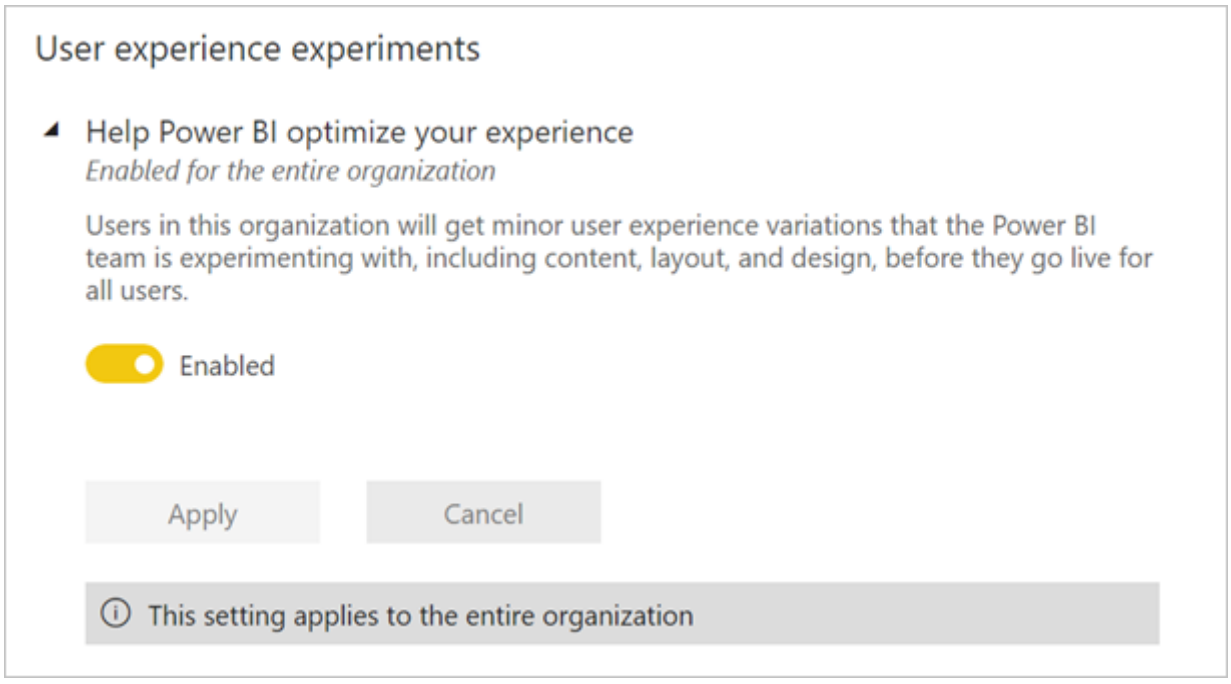
User experience experiments tenant settings

Article • 10/03/2022 • 2 minutes to read

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

When this feature is enabled, individual users in the same organization might get minor variations in the user experience, including content, layout, and design. This means different users in the same tenant might have slightly different experiences before they go live for all users. 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.



Next steps

- About tenant settings

Share data with your Microsoft 365 services tenant settings

Article • 10/21/2022 • 2 minutes to read

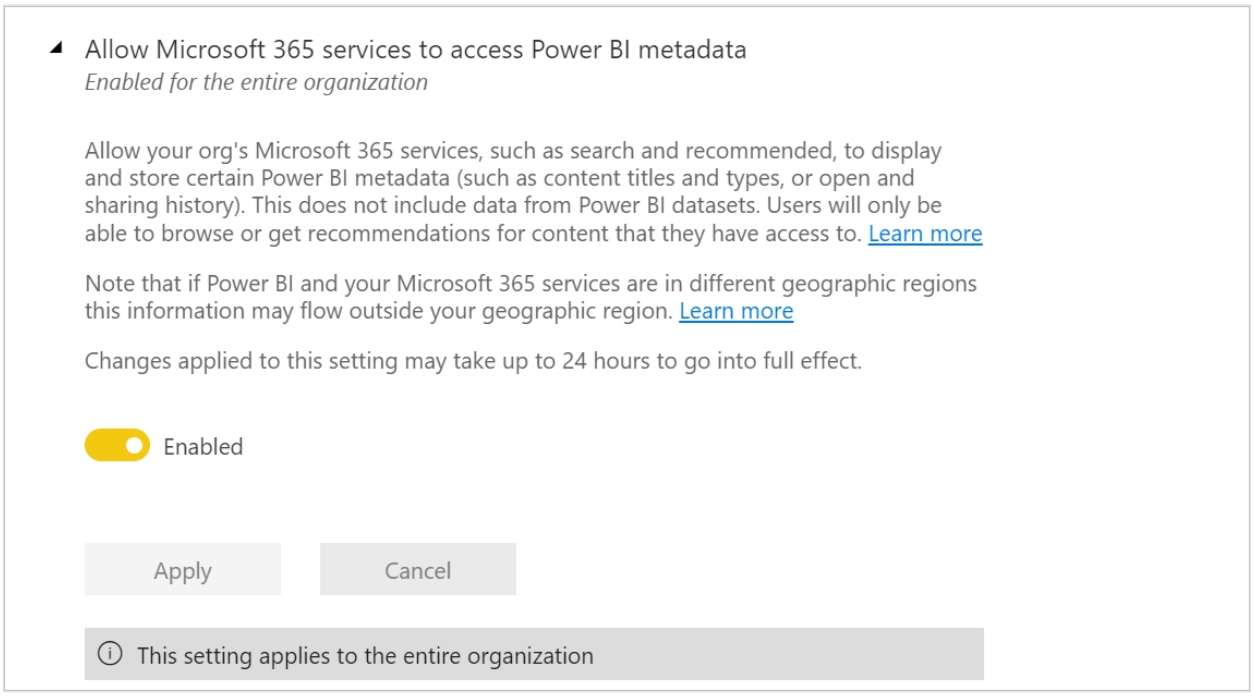
These settings are configured in the tenant settings section of the Admin portal. For information about how to get to and use tenant settings, see About tenant settings.

Allow Microsoft 365 services to access Power BI metadata

This setting controls whether Power BI metadata is shared with your Microsoft 365 services. For more information about this feature, see Share data with your Microsoft 365 services. In particular, review the list of what metadata is shared.

If Power BI and your Microsoft 365 services are in different geographic regions, information may flow outside the region it is stored in. By enabling this setting, you are explicitly opting in to this feature, and acknowledging that enabling these cross-service capabilities may result in Power BI metadata flowing outside the geographic region it is stored in. See Where data is located when Power BI data is shared with your Microsoft 365 services for more detail.

To turn on the feature, go to **Admin portal** > **Tenant settings** > **Share data with your Microsoft 365 services.** Expand the switch and set the toggle switch to **Enabled**. Because of the data residency considerations, it is disabled by default.



Next steps

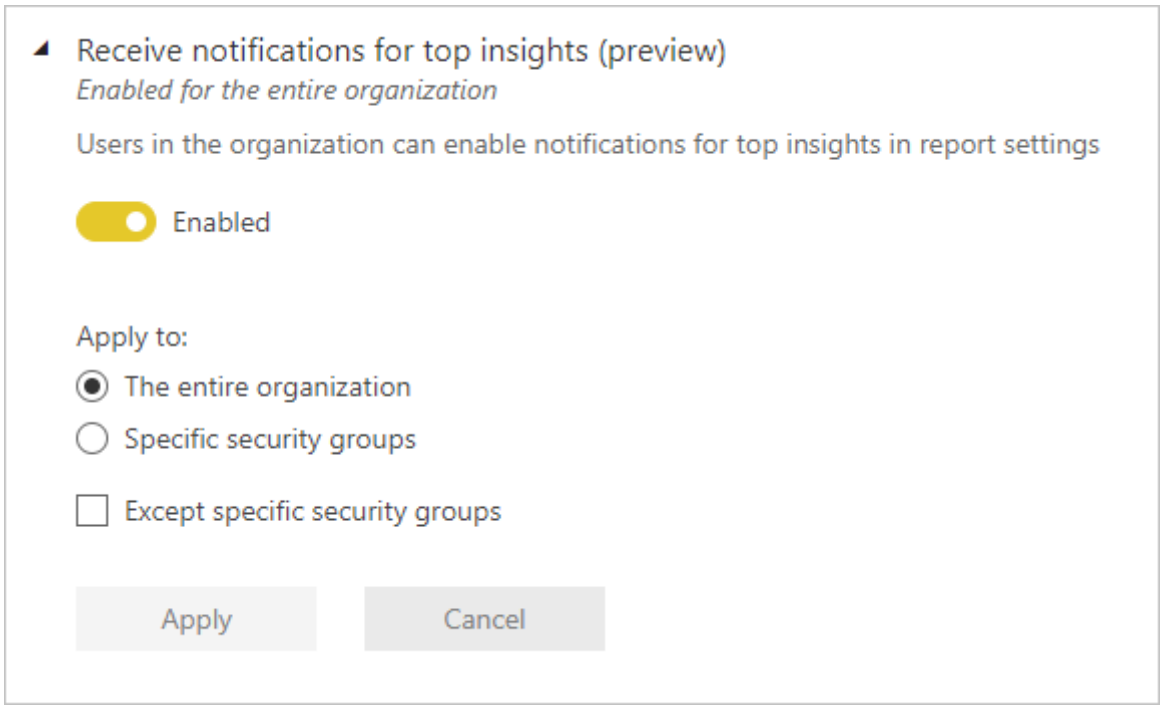
- Share data with your Microsoft 365 services
- Where data is located when Power BI data is shared with your Microsoft 365 services
- About tenant settings

Insights tenant settings

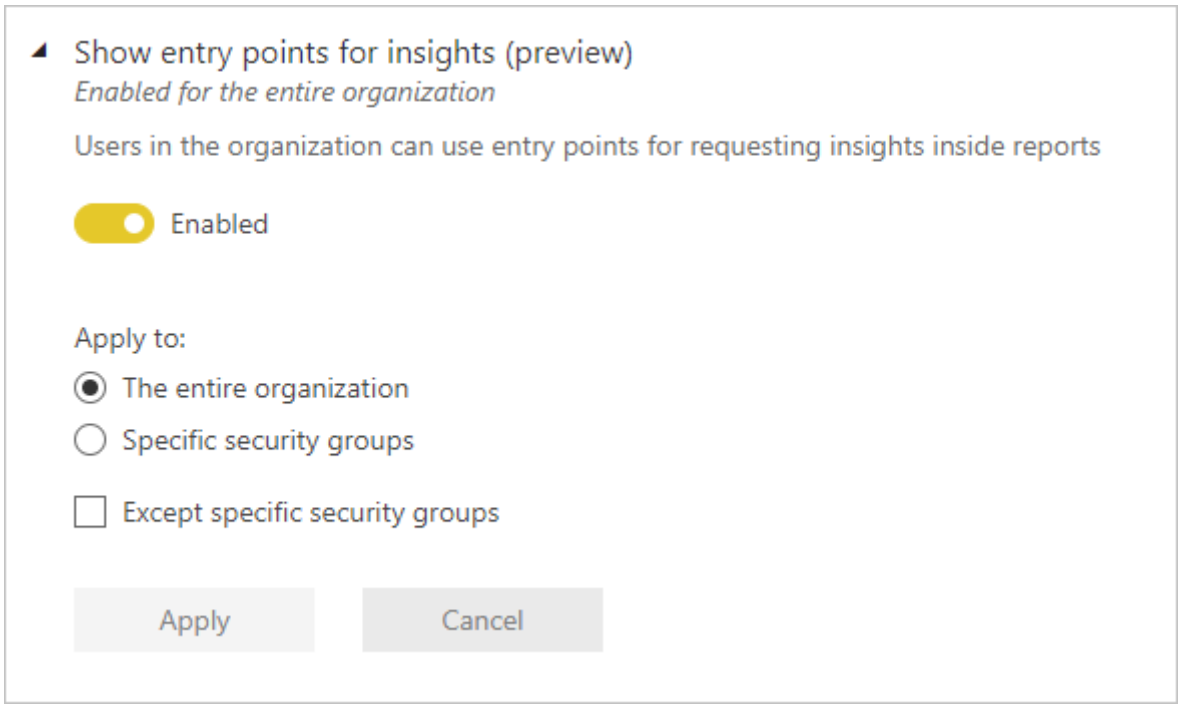
Article • 10/03/2022 • 2 minutes to read

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)



Show entry points for insights (preview)



Next steps

- About tenant settings

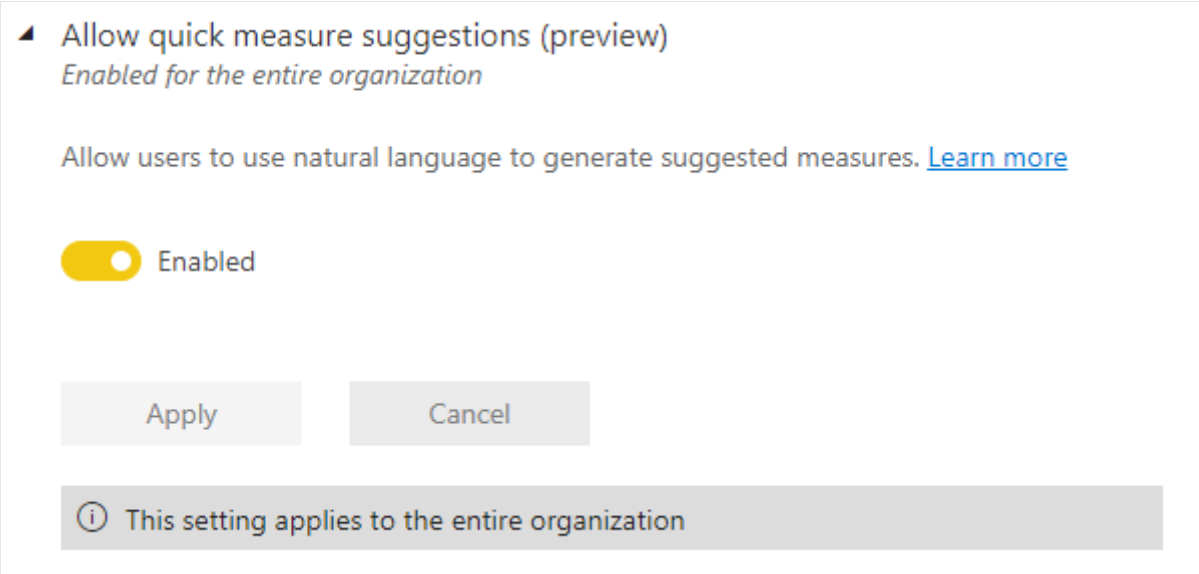
Quick measure suggestions tenant settings

Article • 10/03/2022 • 2 minutes to read

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.

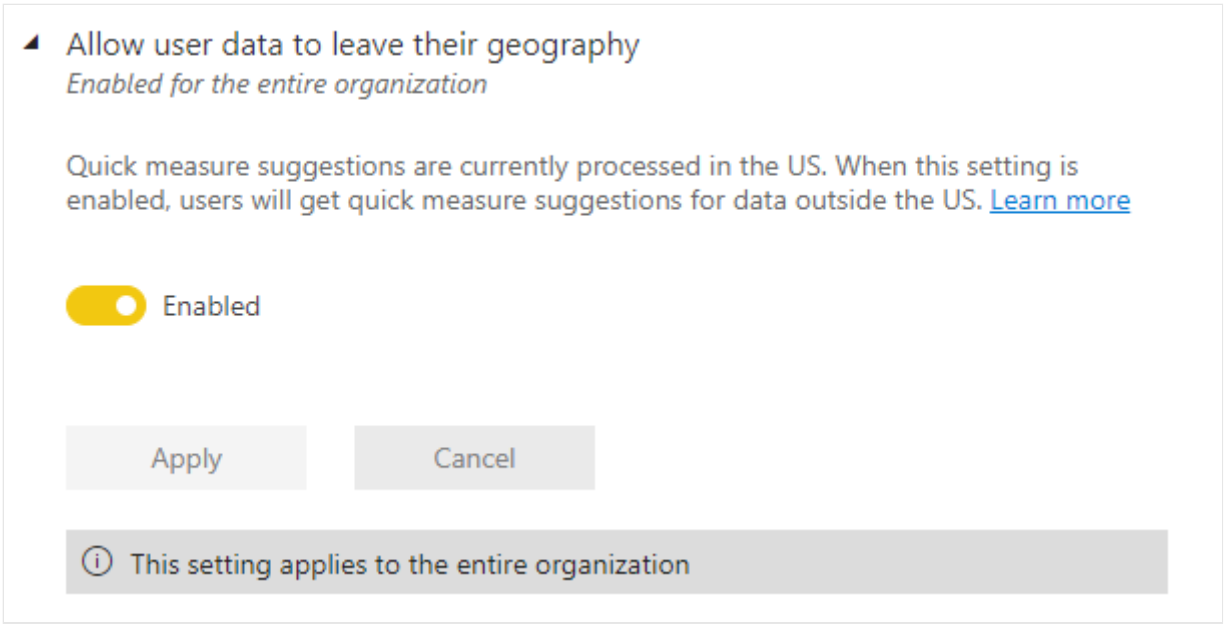
Allow quick measure suggestions (preview)

When enabled, users use natural language to generate suggested measures. See more information.



Allow use data to leave their geography

Quick measure suggestions are currently processed in the US. When this setting is enabled, users will get quick measure suggestions for data outside the US. See more information.



Next steps

- About tenant settings