Tell us about your PDF experience.

Power BI enterprise

Leverage the Power BI platform enterprise features and capabilities.

Power BI Premium

OVERVIEW

Introducing Power BI Premium

Power BI Premium features

CONCEPT

Power BI Premium architecture

Managing Premium capacities

Power BI for US government

HOW-TO GUIDE

Enroll a US government organization

Information protection

OVERVIEW

Data protection in Power BI

CONCEPT

Sensitivity labels

Microsoft Defender for Cloud Apps

HOW-TO GUIDE

Enable sensitivity labels

Apply sensitivity labels

Security

OVERVIEW

Power BI Security

CONCEPT

Power BI Desktop privacy levels

Row-level security (RLS)

HOW-TO GUIDE

Use service tags

Private endpoints

Bring your own encryption keys

Automation tools

REFERENCE

PowerShell cmdlets, REST APIs, and .NET Client library

Automatic aggregations

Article • 11/10/2023

Automatic aggregations use state-of-the-art machine learning (ML) to continuously optimize DirectQuery semantic models for maximum report query performance. Automatic aggregations are built on top of existing user-defined aggregations infrastructure first introduced with composite models for Power BI. Unlike user-defined aggregations, automatic aggregations don't require extensive data modeling and query-optimization skills to configure and maintain. Automatic aggregations are both self-training and self-optimizing. They enable model owners of any skill level to improve query performance, providing faster report visualizations for large models.

With automatic aggregations:

- Report visualizations are faster - An optimal percentage of report queries are returned by an automatically maintained in-memory aggregations cache instead of backend data source systems. Outlier queries that aren't returned by the in-memory cache are passed directly to the data source using DirectQuery.
- Balanced architecture - When compared to pure DirectQuery mode, most query results are returned by the Power BI query engine and in-memory aggregations cache. Query processing load on data source systems at peak reporting times can be significantly reduced, which means increased scalability in the data source backend.
- Easy setup - Model owners can enable automatic aggregations training and schedule one or more refreshes for the model. With the first training and refresh, automatic aggregations begin creating an aggregations framework and optimal aggregations. The system automatically tunes itself over time.
- Fine-tuning – With a simple and intuitive user interface in the model settings, you can estimate the performance gains for a different percentage of queries returned from the in-memory aggregations cache and make adjustments for even greater gains. A single slide bar control helps you easily fine-tune your environment.

Requirements

Supported plans

Automatic aggregations are supported for **Power BI Premium per capacity**, **Premium per user**, and **Power BI Embedded** models.

Supported data sources

Automatic aggregations are supported for the following data sources:

- Azure SQL Database
- Azure Synapse Dedicated SQL pool
- SQL Server 2019 or later
- Google BigQuery
- Snowflake
- Databricks
- Amazon Redshift

Supported modes

Automatic aggregations are supported for DirectQuery mode models. Composite model models with both import tables and DirectQuery connections are supported. Automatic aggregations are supported for the DirectQuery connection only.

Permissions

To enable and configure automatic aggregations, you must be the **Model owner**. Workspace admins can take over as owner to configure automatic aggregations settings.

Configuring automatic aggregations

Automatic aggregations are configured in model Settings. Configuring is simple - enable automatic aggregations training and schedule one or more refreshes. Before you configure automatic aggregations for your model, be sure to entirely read through this article. It provides a good understanding of how automatic aggregations work and can help you decide if automatic aggregations are right for your environment. When you're ready for step-by-step instructions on how to enable automatic aggregations training, configure a refresh schedule, and fine-tune for your environment, see Configure automatic aggregations.

Benefits

With DirectQuery, each time a model user opens a report or interacts with a report visualization, Data Analysis Expressions (DAX) queries are passed to the query engine and then to the backend data source as SQL queries. The data source must calculate and

return results for each query. Compared to import mode models stored in-memory, DirectQuery data source round trips can be both time and process intensive, often causing slow query response times in report visualizations.

When enabled for a DirectQuery model, automatic aggregations can boost report query performance by avoiding data source query round trips. Pre-aggregated query results are automatically returned by an in-memory aggregations cache rather than being sent to and returned by the data source. The amount of pre-aggregated data in the in-memory aggregations cache is a small fraction of the amount of data kept in fact and detail tables at the data source. The result isn't only better report query performance, but also reduced load on backend data source systems. With automatic aggregations, only a small portion of report and ad-hoc queries that require aggregations not included in the in-memory cache are passed to the backend data source, just like with pure DirectQuery mode.

Automatic query and aggregations management

While automatic aggregations eliminate the need to create user-defined aggregation tables and dramatically simplify implementing a pre-aggregated data solution, a deeper familiarity with the underlying processes and dependencies is helpful in understanding how automatic aggregations work. Power BI relies on the following to create and manage automatic aggregations.

Query log

Power BI tracks model and user report queries in a query log. For each model, Power BI maintains seven days of query log data. Query log data is rolled forward each day. The

query log is secure and not visible to users or through the XMLA endpoint.

Training operations

As part of the first scheduled model refresh operation for your selected frequency (Day or Week), Power BI first initiates a training operation that evaluates the query log to ensure aggregations in the in-memory aggregations cache adapt to changing query patterns. In-memory aggregation tables are created, updated, or dropped, and special queries are sent to the data source to determine aggregations to be included in the cache. Calculated aggregations data, however, isn't loaded into the in-memory cache during training - it's loaded during the subsequent refresh operation.

For example, if you choose a Day frequency and the schedule refreshes at 4:00AM, 9:00AM, 2:00PM, and 7:00PM, **only the 4:00AM refresh each day will include both a training operation *and* a refresh operation**. The subsequent 9:00AM, 2:00PM, and 7:00PM scheduled refreshes for that day are *refresh only operations* that update the existing aggregations in the cache.

While training operations evaluate past queries from the query log, the results are sufficiently accurate to ensure future queries are covered. There's no guarantee however

that future queries will be returned by the in-memory aggregations cache because those new queries could be different than those derived from the query log. Those queries not returned by the in-memory aggregations cache are passed to the data source by using DirectQuery. Depending on the frequency and ranking of those new queries, aggregations for them may be included in the in-memory aggregations cache with the next training operation.

The training operation has a 60-minute time limit. If training is unable to process the entire query log within the time limit, a notification is logged in the model Refresh history and training resumes the next time it's launched. The training cycle completes and replaces the existing automatic aggregations when the entire query log is processed.

Refresh operations

As described previously, after the training operation completes as part of the first scheduled refresh for your selected frequency, Power BI performs a refresh operation that queries and loads new and updated aggregations data into the in-memory aggregations cache and removes any aggregations that no longer rank high enough (as determined by the training algorithm). All subsequent refreshes for your chosen Day or Week frequency are *refresh only operations* that query the data source to update existing aggregations data in the cache. By using our previous example, the 9:00AM, 2:00PM, and 7:00PM scheduled refreshes for that day are refresh only operations.

Regularly scheduled refreshes throughout the day (or week) ensure aggregations data in the cache are more up to date with data at the backend data source. Through model

Settings, you can schedule up to 48 refreshes per day to ensure report queries that are returned by the aggregations cache are getting results based on the most recent refreshed data from the backend data source.

> ⊗ **Caution**
>
> Training and refresh operations are process and resource intensive for both the Power BI service and the data source systems. Increasing the percentage of queries that use aggregations means more aggregations must be queried and calculated from data sources during training and refresh operations, increasing the probability of excessive use of system resources and potentially causing timeouts. To learn more, see **Fine tuning**.

Training on demand

As mentioned earlier, a training cycle may not complete within the time limits of a single data refresh cycle. If you don't want to wait until the next scheduled refresh cycle that includes training, you can also trigger automatic aggregations training on-demand by selecting **Train and Refresh Now** in model Settings. By using **Train and Refresh Now** triggers both a training operation and a refresh operation. Check the model Refresh history to see if the current operation is finished before running another on-demand training and refresh operation, if necessary.

Refresh history

Each refresh operation is recorded in the model Refresh history. Important information about each refresh is shown, including the number of memory aggregations in the cache are consuming for the configured query percentage. To view refresh history, in the model Settings page, select **Refresh history**. If you want to drill down a little further, select **Show** details.

By regularly checking the refresh history you can ensure your scheduled refresh operations are completing within an acceptable period. Make sure refresh operations are successfully completing before the next scheduled refresh begins.

Training and refresh failures

While Power BI performs training and refresh operations as part of the first scheduled refresh for the day or week frequency you choose, these operations are implemented as separate transactions. If a training operation can't fully process the query log within its time limits, Power BI is going to proceed refreshing the existing aggregations (and regular tables in a composite model) using the previous training state. In this case, the refresh history will indicate the refresh succeeded and training is going to resume processing the query log the next time training launches. Query performance might be less optimized if client report query patterns changed and aggregations didn't adjust yet but the achieved performance level should still be far better than a pure DirectQuery model without any aggregations.

If a training operation requires too many cycles to finish processing the query log, consider reducing the percentage of queries that use the in-memory aggregations cache in model Settings. This will reduce the number of aggregations created in the cache, but allow more time for training and refresh operations to complete. To learn more, see Fine tuning.

If training succeeds but refresh fails, the entire refresh is marked as Failed because the result is an unavailable in-memory aggregations cache.

When scheduling refresh, you can specify email notifications if there are refresh failures.

User-defined and automatic aggregations

User-defined aggregations in Power BI can be manually configured based on hidden aggregated tables in the model. Configuring user-defined aggregations is often complex, requiring a greater level of data-modeling and query-optimization skills. Automatic aggregations on the other hand eliminate this complexity as part of an AI-driven system. Unlike user-defined aggregations that remain static, Power BI continuously maintains query logs and from those logs determines query patterns based on machine learning (ML) predictive modeling algorithms. Pre-aggregated data is calculated and stored in-memory based on query pattern analysis. With automatic aggregations, models are both self-training and self-optimizing. As client report query patterns change, automatic aggregations adjust, prioritizing and caching those aggregations used most often.

Because automatic aggregations are built on top of the existing user-defined aggregations infrastructure, it's possible to use both user-defined and automatic aggregations together in the same model. Skilled data modelers can define

aggregations for tables using DirectQuery, Import (with or without Incremental refresh), or Dual storage modes, while at the same time having the benefits of more automatic aggregations for queries over DirectQuery connections that don't hit the user-defined aggregation tables. This flexibility enables balanced architectures that can reduce query loads and avoid bottlenecks.

Aggregations created in the in-memory cache by the automatic aggregations training algorithm are identified as `System` aggregations. The training algorithm creates and deletes only those `System` aggregations as reporting queries are analyzed and adjustments are made to maintain the optimal aggregations for the model. Both user-defined and automatic aggregations are refreshed with refresh. Only those aggregations created by automatic aggregations and marked as system-generated aggregations are included in automatic aggregations processing.

Query caching and automatic aggregations

Power BI Premium also supports Query caching in Power BI Premium/Embedded to maintain query results. Query caching is a different feature from automatic aggregations. With query caching, Power BI Premium uses its local caching service to implement caching, whereas automatic aggregations are implemented at the model level. With query caching, the service only caches queries for the initial report page load, therefore query performance isn't improved when users interact with a report. In contrast, automatic aggregations optimize most report queries by pre-caching aggregated query results, including those queries generated when users interact with reports. Query caching and automatic aggregations can both be enabled for a model, but it's likely not necessary.

Monitor with Azure Log Analytics

Azure Log Analytics (LA) is a service within Azure Monitor which Power BI can use to save activity logs. With Azure Monitor suite, you can collect, analyze, and act on telemetry data from your Azure and on-premises environments. It offers long-term storage, an ad-hoc query interface, and API access to allow data export and integration with other systems. To learn more, see Using Azure Log Analytics in Power BI.

If Power BI is configured with an Azure LA account, as described in Configuring Azure Log Analytics for Power BI, you can analyze the success rate of your automatic aggregations. Among other things, you can determine if report queries are answered from the in-memory cache.

To use this ability, download the PBIT template and connect it to your log analytics account, as described in this Power BI blog post. In the report, you can view data at three different levels: Summary view, DAX query level view, and SQL query level view.

The following image shows the summary page for all the queries. As you can see, the marked chart shows the percentage of total queries that were satisfied by aggregations vs. the ones that had to utilize the data source.

The next step to dive deeper is to look at the use of aggregations at a DAX query level. Right-click a DAX query from the list (bottom left) > **Drill through** > **Query history**.

This will provide you with a list of all the pertinent queries. Drill through to the next level to show more aggregation details.

Application Lifecycle Management

From development to test and from test to production, models with automatic aggregations enabled have special requirements for ALM solutions.

Deployment pipelines

With deployment pipelines, Power BI can copy the models with their model configuration from the current stage into the target stage. However, automatic aggregations must be reset in the target stage as the settings do no get transferred from current to target stage. You can also deploy content programmatically, using the deployment pipelines REST APIs. To learn more about this process, see Automate your deployment pipeline using APIs and DevOps.

Custom ALM solutions

If you use a custom ALM solution based on XMLA endpoints, keep in mind that your solution might be able to copy system-generated and user-created aggregations tables as part of the model metadata. However, you must enable automatic aggregations after each deployment step at the target stage manually. Power BI will retain the configuration if you overwrite an existing model.

> **Note**
>
> If you upload or republish a model as part of a Power BI Desktop (.pbix) file, system-created aggregation tables are lost as Power BI replaces the existing model with all its metadata and data in the target workspace.

Altering a model

After altering a model with automatic aggregations enabled via XMLA endpoints, such as adding or removing tables, Power BI preserves any existing aggregations that can be and removes those that are no longer needed or relevant. Query performance could be impacted until the next training phase is triggered.

Metadata elements

Models with automatic aggregations enabled contain unique system-generated aggregations tables. Aggregations tables aren't visible to users in reporting tools. They're visible through the XMLA endpoint by using tools with Analysis Services client libraries version **19.22.5 and higher**. When working with models with automatic aggregations enabled, be sure to upgrade your data modeling and administration tools to the latest version of the client libraries. For SQL Server Management Studio (SSMS),

upgrade to SSMS version **18.9.2 or higher**. Earlier versions of SSMS aren't able to enumerate tables or script out these models.

Automatic aggregations tables are identified by a `SystemManaged` table property, which is new to the Tabular Object Model (TOM) in Analysis Services client libraries version 19.22.5 and higher. The following code snippet shows the `SystemManaged` property set to `true` for automatic aggregations tables and `false` for regular tables.

C#

```
using System;
using System.Collections.Generic;
using System.Linq;
using Microsoft.AnalysisServices.Tabular;

namespace AutoAggs
{
    class Program
    {
        static void Main(string[] args)
        {
            string workspaceUri = "<Specify the URL of the workspace where
your model resides>";
            string datasetName = "<Specify the name of your dataset>";

            Server sourceWorkspace = new Server();
            sourceWorkspace.Connect(workspaceUri);
            Database dataset =
sourceWorkspace.Databases.GetByName(datasetName);

            // Enumerate system-managed tables.
            IEnumerable<Table> aggregationsTables =
dataset.Model.Tables.Where(tbl => tbl.SystemManaged == true);


            if (aggregationsTables.Any())
            {
                Console.WriteLine("The following auto aggs tables exist in
this dataset:");
                foreach (Table table in aggregationsTables)
                {
                    Console.WriteLine($"\t{table.Name}");
                }
            }
            else
            {
                Console.WriteLine($"This dataset has no auto aggs tables.");
            }

            Console.WriteLine("\n\rPress [Enter] to exit the sample
app...");
            Console.ReadLine();
```

```
            }
        }
    }
```

Executing this snippet outputs automatic aggregations tables currently included in the model in a console.

Keep in mind, aggregations tables are constantly changing as training operations determine the optimal aggregations to include in the in-memory aggregations cache.

> **Important**
>
> Power BI fully manages automatic aggregations system-generated table objects. Do not delete or modify these tables yourself. Doing so can cause degraded performance.

Power BI maintains the model configuration outside of the model. The presence of a system-managed aggregations table in a model doesn't necessarily mean the model is in fact enabled for automatic aggregations training. In other words, if you script out a full model definition for a model with automatic aggregations enabled, and create a new copy of the model (with a different name/workspace/capacity), the new resulting model isn't enabled for automatic aggregations training. You still need to enable automatic aggregations training for the new model in model Settings.

Considerations and limitations

When using automatic aggregations, keep the following in mind:

- Aggregations do not support Dynamic M Query Parameters.
- The SQL queries generated during the initial training phase can generate significant load for the data warehouse. If training keeps finishing incomplete and you can verify on the data warehouse side that the queries are encountering a

timeout, consider temporarily scaling up your data warehouse to meet the training demand.

- Aggregations stored in the in-memory aggregations cache may not be calculated on the most recent data at the data source. Unlike pure DirectQuery, and more like regular import tables, there's a latency between updates at the data source and aggregations data stored in the in-memory aggregations cache. While there will always be some degree of latency, it can be mitigated through an effective refresh schedule.
- To further optimize performance, set all dimension tables to **Dual mode** and leave fact tables in DirectQuery mode.
- Automatic aggregations aren't available with Power BI Pro, Azure Analysis Services, or SQL Server Analysis Services.
- Power BI doesn't support downloading models with automatic aggregations enabled. If you uploaded or published a Power BI Desktop (*.pbix*) file to Power BI and then enabled automatic aggregations, you can no longer download the PBIX file. Make sure you keep a copy of the PBIX file locally.
- Automatic aggregations with external tables in Azure Synapse Analytics isn't supported. You can enumerate external tables in Synapse by using the following SQL query: `SELECT SCHEMA_NAME(schema_id) AS schema_name, name AS table_name FROM sys.external_tables`.
- Automatic aggregations are only available for models using enhanced metadata. If you want to enable automatic aggregations for an older model, upgrade the model to enhanced metadata first. To learn more, see Using enhanced model metadata.
- Don't enable automatic aggregations if the DirectQuery data source is configured for single sign-on and uses dynamic data views or security controls to limit the data a user is allowed to access. Automatic aggregations aren't aware of these data source-level controls, which makes it impossible to ensure correct data is provided on a per user basis. Training will log a warning in the refresh history that it detected a data source configured for single sign-on and skipped the tables that use this data source. If possible, disable SSO for these data sources to take full advantage of the optimized query performance automatic aggregations can provide.
- Don't enable automatic aggregations if the model contains only hybrid tables to avoid unnecessary processing overhead. A hybrid table uses both import partitions and a DirectQuery partition. A common scenario is incremental refresh with real-time data in which a DirectQuery partition fetches transactions from the data source that occurred after the last data refresh. However, Power BI imports aggregations during refresh. Automatic aggregations can't include transactions

that occurred after the last data refresh. Training will log a warning in the refresh history that it detected and skipped hybrid tables.

- Calculated columns aren't considered for automatic aggregations. If you use a calculated column in DirectQuery mode, such as by using the `COMBINEVALUES` DAX function to create a relationship based on multiple columns from two DirectQuery tables, the corresponding report queries won't hit the in-memory aggregations cache.
- Automatic aggregations are only available in the Power BI service. Power BI Desktop doesn't create system-generated aggregations tables.
- If you modify the metadata of a model with automatic aggregations enabled, query performance might degrade until the next training process is triggered. As a best practice, you should drop the automatic aggregations, make the changes, and then retrain.
- Don't modify or delete system-generated aggregations tables unless you have automatic aggregations disabled and are cleaning up the model. The system takes responsibility for managing these objects.

Community

Power BI has a vibrant community where MVPs, BI pros, and peers share expertise in discussion groups, videos, blogs and more. When learning about automatic aggregations, be sure to check out these other resources:

- Power BI Community
- Search "Power BI automatic aggregations" on Bing

See also

Configure automatic aggregations
User-defined aggregations
DirectQuery in Power BI
Analysis Services client libraries

Configure automatic aggregations

Article • 11/10/2023

Configuring automatic aggregations includes enabling training for a supported DirectQuery semantic model and configuring one or more scheduled refreshes. After several iterations of the training and refresh operations have run, you can return to semantic model settings to fine-tune the percentage of report queries that use the in-memory aggregations cache. Before completing these steps, be sure you fully understand the functionality and limitations described in Automatic aggregations.

Enable

You must have semantic model Owner permissions to enable automatic aggregations. Workspace admins can take over model owner permissions.

1. In semantic model Settings, expand **Scheduled refresh and performance optimization**.

2. Switch **Automatic aggregations training** to **On**. If the switch is greyed out, ensure Data source credentials are configured and you're signed in.

3. In **Refresh schedule**, specify a refresh frequency and time zone. If the Refresh schedule controls are disabled, verify the data source configuration including gateway connection (if necessary) and data source credentials.

4. Select **Add another time**, and then specify one or more refreshes.

You must schedule at least one refresh. The first refresh for the frequency you select will include both a *training* operation and a refresh that loads new and updated aggregations into the in-memory cache. Schedule more refreshes to ensure report queries that hit the aggregations cache are getting results that are most in-sync with the backend data source. For more information, see Refresh operations.

5. Select **Apply**.

On-demand train and refresh

The first *scheduled* refresh operation for your chosen frequency includes a training operation. If that training operation doesn't complete within the 60-minute time limit, the subsequent refresh operation won't load or update aggregations in the cache. The

next training operation won't run until the first refresh operation of your chosen frequency.

In such cases, you can manually run one or more *on-demand* training and refresh operations to fully complete the training and load or refresh aggregations in the cache. For example, when checking the Refresh history, if the first *scheduled* training and refresh operation for the day (frequency) doesn't complete within the time limit, and you don't want to wait for the next day's scheduled refresh that includes a training operation to run, you can run one or more on-demand train and refresh operations to fully process the data query log (train) and load aggregations to the cache (refresh).

To run an on-demand train and refresh operation, select **Train and Refresh Now**. Be sure to keep an eye on the refresh history to ensure the on-demand training operation completes successfully. If not, run another train and refresh operation until training completes successfully, and aggregations are loaded or refreshed in the cache.

Running **Train and Refresh Now** can be helpful for fine-tuning the percentage of report queries that will use aggregations from the in-memory cache. By running an on-demand train and refresh now operation, you can more quickly determine if your new percentage setting allows the training operation to complete within the time limit.

Keep in mind, training and refresh operations, whether scheduled or on-demand are process and resource intensive for both the data source and Power BI. Choose a time when resources are least impacted.

Fine-tuning

Both user-defined and system-generated aggregations tables are part of the model, contribute to the model size, and are subject to existing Power BI model size constraints. Aggregations processing also consumes resources and impacts model refresh durations. An optimal configuration strikes a balance between providing pre-aggregated results from the in-memory aggregations cache for the most frequently used report queries, while accepting slower results for outlier and ad-hoc queries in exchange for faster training and refresh times and a reduced burden on system resources.

Adjust the percentage

By default, the aggregations cache setting that determines the percentage of report queries that will use aggregations from the in-memory cache is 75%. Increasing the percentage means a greater number of report queries are ranked higher and therefore aggregations for them are included in the in-memory aggregations cache. While a higher percentage can mean more queries are answered from the in-memory cache, it

can also mean **longer training and refresh times**. Adjusting to a lower percentage, on the other hand, can mean shorter training and refresh times, and less resource utilization, but report visualization performance could diminish because fewer report queries would be answered by the in-memory aggregations cache, as those report queries instead must then roundtrip to the data source.

Before the system can determine the optimal aggregations to include in the cache, it must first know the report query patterns being used most often. Be sure to allow several iterations of the training/refresh operations to complete before adjusting the percentage of queries that will use the aggregations cache. This gives the training algorithm time to analyze report queries over a broader time period and self-adjust accordingly. For example, if you've scheduled refreshes for daily frequency, you might want to wait a full week. User reporting patterns on some days of the week can be different than others.

To adjust the percentage

1. In semantic model Settings, expand **Scheduled refresh and performance optimization**.

2. In **Query coverage**, use the **Adjust the percentage of queries that will use the aggregated caches** slider to increase or decrease the percentage to the desired value. As you adjust the percentage, the Query Performance Impact Lift chart provides estimated query response times.

3. Select **Train and Refresh Now** or **Apply**.

Estimate query performance impact

The **Query performance impact** lift chart provides estimated report query run times as a function of the percentage of queries that will use cached aggregations. The chart will initially show 0.0 for all metrics until at least one training/refresh operation is performed. After an initial training/refresh operation, the chart can help you determine if adjusting

the percentage of queries that use the in-memory aggregations cache can potentially further improve query response.

Threshold appears as a marker line on the lift chart and indicates the target query response time for your reports. You can then fine-tune the percentage of queries that will use the aggregations cache to determine a new query percentage that meets the desired threshold.

Metrics

DirectQuery - An estimated duration in seconds for a report query sent to and returned from the data source by using DirectQuery. Queries that can't be answered by the in-memory aggregations cache will typically be within this estimate.

Current query percentage - An estimated duration in seconds for report queries answered from the in-memory aggregations cache, based on the percentage setting for the most recent training/refresh operation.

New query percentage - An estimated duration in seconds for report queries answered from the in-memory aggregations cache for the newly selected percentage. As the percentage slider is changed, this metric reflects the potential change.

Disable

You must have model owner permissions to disable automatic aggregations. Workspace admins can take over model owner permissions.

1. To disable, switch **Automatic aggregations training** to **Off**.

When you disable training, you're prompted with an option to delete automatic aggregation tables.

If you choose *not* to delete existing automatic aggregation tables, the tables will remain in the model and continue to be refreshed. However, because training is disabled, no new aggregations will be added to them. Power BI will continue to use the existing tables to get aggregated query results when possible.

If you choose to delete the tables, the model is reverted to its original state without any automatic aggregations.

2. Select **Apply**.

See also

- Automatic aggregations
- User-defined aggregations
- DirectQuery in Power BI

Manage the Power BI Desktop sign-in form

Article • 02/28/2025

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 disables the dialog.

More questions? Ask the Power BI Community

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Track user activities in Power BI

Article • 12/26/2023

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 the Power BI activity log which is based on Power BI REST APIs.

You can track Microsoft Fabric user activities, including Power BI operations, using the audit log.

Prerequisites

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

Activity log

The Power BI activity log contains complete copy of the Power BI activities in a JSON array. You can find a list of all the Power BI activities in the Fabric operation list.

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%3AARUAAAAAAAAAFwAAAAAAAAA%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);
```

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='LDIwMjAtMDgtMTNUMDc6NTU6MDBaLDIwMjAtMDgtMTNUMDk6MDA6MDBaLDEsLA%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.

Related content

- Track user activities in Microsoft Fabric
- Operation list

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Bring your own encryption keys for Power BI

Article • 03/03/2025

By default, Power BI uses Microsoft-managed keys to encrypt your data. In Power BI Premium, you can also use your own keys for data at-rest that's imported into a semantic model. This approach is often described as *bring your own key* (BYOK). For more information, see Data source and storage considerations.

Why use BYOK?

BYOK makes it easier to meet compliance requirements that specify key arrangements with the cloud service provider, in this case Microsoft. With BYOK, you provide and control the encryption keys for your Power BI data at-rest at the application level. As a result, you can exercise control and revoke your organization's keys, should you decide to exit the service. By revoking the keys, the data becomes unreadable to the service within 30 minutes.

Data source and storage considerations

To use BYOK, you must upload data to the Power BI service from a Power BI Desktop (PBIX) file. You can't use BYOK in the following scenarios:

- Analysis Services Live Connection
- Excel workbooks, unless data is first imported into Power BI Desktop.

  > **Note**
  >
  > For Excel workbooks stored in SharePoint and OneDrive, you can use Customer Key.

- Push semantic models
- Streaming semantic models
- Power BI metrics don't currently support BYOK

BYOK applies only to semantic models. Push semantic models, Excel files, and CSV files that users can upload to the service aren't encrypted using your own key. To identify which items are stored in your workspaces, use the following PowerShell command:

```
PS C:\> Get-PowerBIWorkspace -Scope Organization -Include All
```

> **Note**
>
> This cmdlet requires Power BI management module v1.0.840. You can see which version you have by running `Get-InstalledModule -Name MicrosoftPowerBIMgmt`. Install the latest version by running `Install-Module -Name MicrosoftPowerBIMgmt`. You can get more information about the Power BI cmdlet and its parameters in Power BI PowerShell cmdlet module.

Configure Azure Key Vault

This section explains how to configure Azure Key Vault, a tool for securely storing and accessing secrets, like encryption keys. You can use an existing key vault to store encryption keys, or you can create a new one specifically for use with Power BI.

The following instructions assume basic knowledge of Azure Key Vault. For more information, see What is Azure Key Vault?

Configure your key vault in the following way:

1. Add the Power BI service as a service principal for the key vault, with wrap and unwrap permissions.
2. Create an RSA key with a 4096-bit length, or use an existing key of this type, with wrap and unwrap permissions.

   > **Important**
   >
   > Power BI BYOK supports RSA and RSA-HSM keys with a 4096-bit length.

3. Recommended: Check that the key vault has the *soft delete* option enabled.

Add the service principal

1. Log into the Azure portal and search for **Key Vaults**.
2. In your key vault, select **Access policies**, and then choose **Create**.

3. On the **Permissions** screen, under **Key permissions**, select **Unwrap Key** and **Wrap Key**, then choose **Next**.

4. On the **Principal** screen, search for and select *Microsoft.Azure.AnalysisServices*.

> **Note**
>
> If you can't find *Microsoft.Azure.AnalysisServices*, it's likely that the Azure subscription associated with your Azure Key Vault never had a Power BI resource associated with it. Try searching for the following string instead: 00000009-0000-0000-c000-000000000000.

5. Select **Next**, then **Review + create** > **Create**.

> **Note**
>
> To revoke Power BI access to your data, remove access rights to this service principal from your Azure Key Vault.

Create an RSA key

1. In your key vault, under **Keys**, select **Generate/Import**.

2. Select a **Key type** of *RSA* and an **RSA key size** of *4096*.

3. Select **Create**.

4. Under **Keys**, select the key you created.

5. Select the GUID for the **Current Version** of the key.

6. Check that **Wrap Key** and **Unwrap Key** are both selected. Copy the **Key Identifier** to use when you enable BYOK in Power BI.

Soft delete option

You should you enable soft-delete on your key vault to protect from data loss in case of accidental key, or key vault, deletion. To enable the *soft-delete* property, you must use PowerShell because this option isn't available yet in the Azure portal.

With Azure Key Vault properly configured, you're ready to enable BYOK on your tenant.

Configure the Azure Key Vault firewall

This section describes using the trusted Microsoft service firewall bypass, to configure a firewall around your Azure Key Vault.

> **Note**
>
> You can choose to enable firewall rules on your key vault. You can also choose to leave the firewall disabled on your key vault as per the default setting.

Power BI is a trusted Microsoft service. You can instruct the key vault firewall to allow access to all trusted Microsoft services, a setting that allows Power BI to access your key

vault without specifying endpoint connections.

To configure Azure Key Vault to allow access to trusted Microsoft services, follow these steps:

1. Search for **Key Vaults** in the Azure portal, then select the key vault you want to allow access from Power BI and all other trusted Microsoft services.

2. Select **Networking** from the left-side navigation panel.

3. Under **Firewalls and virtual networks**, select **Allow public access from specific virtual networks and IP addresses**.

4. Scroll down to the **Firewall** section. Select **Allow trusted Microsoft services to bypass this firewall**.

5. Select **Apply**.

Enable BYOK on your tenant

You enable BYOK at the tenant level by using PowerShell. First, install the Power BI administration package for PowerShell and introduce the encryption keys you created and stored in Azure Key Vault to your Power BI tenant. You then assign these encryption keys per Premium capacity for encrypting content in the capacity.

Important considerations

Before you enable BYOK, keep the following considerations in mind:

- At this time, you can't disable BYOK after you enable it. Depending on how you specify parameters for `Add-PowerBIEncryptionKey`, you can control how you use BYOK for one or more of your capacities. However, you can't undo the introduction of keys to your tenant. For more information, see Enable BYOK.
- You can't *directly* move a workspace that uses BYOK from a capacity in Power BI Premium to a shared capacity. You must first move the workspace to a capacity that doesn't have BYOK enabled.
- If you move a workspace that uses BYOK from a capacity in Power BI Premium to a shared capacity, reports and semantic models become inaccessible since they're encrypted with the Key. To avoid this situation, you must first move the workspace to a capacity that doesn’t have BYOK enabled.

Enable BYOK

To enable BYOK, you must be a Power BI admin, signed in using the `Connect-PowerBIServiceAccount` cmdlet. Then use Add-PowerBIEncryptionKey to enable BYOK, as shown in the following example:

PowerShell

```
Add-PowerBIEncryptionKey -Name'Contoso Sales' -
KeyVaultKeyUri'https://contoso-
vault2.vault.azure.net/keys/ContosoKeyVault/b2ab4ba1c7b341eea5ecaaa2wb54c4d2
'
```

To add multiple keys, run `Add-PowerBIEncryptionKey` with different values for `-Name` and `-KeyVaultKeyUri`.

The cmdlet accepts two switch parameters that affect encryption for current and future capacities. By default, neither of the switches are set:

- `-Activate`: Indicates that this key is used for all existing capacities in the tenant that aren't already encrypted.
- `-Default`: Indicates that this key is now the default for the entire tenant. When you create a new capacity, the capacity inherits this key.

> **Important**
>
> If you specify `-Default`, all of the capacities created on your tenant from this point are encrypted using the key you specify, or an updated default key. You can't undo the default operation, so you lose the ability to create a premium capacity in your tenant that doesn't use BYOK.

After you enable BYOK on your tenant, set the encryption key for one or more Power BI capacities:

1. Use Get-PowerBICapacity to get the capacity ID that's required for the next step.

   PowerShell

   ```
   Get-PowerBICapacity -Scope Individual
   ```

   The cmdlet returns output similar to the following output:

   ```
   Id               : xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
   DisplayName      : Test Capacity
   Admins           : adam@sometestdomain.com
   Sku              : P1
   State            : Active
   UserAccessRight  : Admin
   Region           : North Central US
   ```

2. Use Set-PowerBICapacityEncryptionKey to set the encryption key:

   PowerShell

   ```
   Set-PowerBICapacityEncryptionKey -CapacityId xxxxxxxx-xxxx-xxxx-xxxx-
   xxxxxxxxxxxx -KeyName 'Contoso Sales'
   ```

You have control over how you use BYOK across your tenant. For example, to encrypt a single capacity, call `Add-PowerBIEncryptionKey` without `-Activate` or `-Default`. Then call `Set-PowerBICapacityEncryptionKey` for the capacity where you want to enable BYOK.

Manage BYOK

Power BI provides additional cmdlets to help manage BYOK in your tenant:

- Use Get-PowerBICapacity to get the key that a capacity currently uses:

  PowerShell

  ```
  Get-PowerBICapacity -Scope Organization -ShowEncryptionKey
  ```

- Use Get-PowerBIEncryptionKey to get the key that your tenant currently uses:

  PowerShell

  ```
  Get-PowerBIEncryptionKey
  ```

- Use Get-PowerBIWorkspaceEncryptionStatus to see whether the semantic models in a workspace are encrypted and whether their encryption status is in sync with the workspace:

  PowerShell

  ```
  Get-PowerBIWorkspaceEncryptionStatus -Name'Contoso Sales'
  ```

  Note that encryption is enabled at the capacity level, but you get encryption status at the semantic model level for the specified workspace.

- Use Switch-PowerBIEncryptionKey to switch (or *rotate*) the version of the key being used for encryption. The cmdlet simply updates the `-KeyVaultKeyUri` for a key `-Name`:

  PowerShell

  ```
  Switch-PowerBIEncryptionKey -Name'Contoso Sales' -
  KeyVaultKeyUri'https://contoso-
  vault2.vault.azure.net/keys/ContosoKeyVault/b2ab4ba1c7b341eea5ecaaa2wb5
  4c4d2'
  ```

  Note that the current key should be enabled.

Related content

- Overview of Power BI PowerShell cmdlet module.
- Ways to share your work in Power BI.
- Filter a report using query string parameters in the URL.

- Embed with report web part in SharePoint Online.
- Publish to web from Power BI.
- What is Power BI Premium?

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Distribute Power BI content to external guest users with Microsoft Entra B2B

Article • 01/28/2025

Power BI enables sharing content with external guest users through Microsoft Entra Business-to-Business (Microsoft Entra B2B). By using Microsoft Entra B2B, your organization enables and governs sharing with external users in a central place.

Another way to share content with external guest users is in-place semantic model sharing with Power BI. This allows you share content with external guest users that they can then access in their own home tenant. For more information about in-place semantic model sharing, see About Power BI in-place semantic model sharing with guest users in external organizations.

This article provides a basic introduction to Microsoft Entra B2B in Power BI. For more information, see Distribute Power BI content to external guest users using Microsoft Entra B2B.

Enable Invite external users to your organization setting

Make sure you enable the Invite external users to your organization feature in the Power BI admin portal before inviting guest users. Even when this option is enabled, the user must be granted the Guest Inviter role in Microsoft Entra ID to invite guest users.

> **Note**
>
> The **Invite external users to your organization** setting controls whether Power BI allows inviting external users to your organization. After an external user accepts the invite, they become a Microsoft Entra B2B guest user in your organization. They appear in people pickers throughout the Power BI experience. If the setting is disabled, existing guest users in your organization continue to have access to any items they already had access to and continue to be listed in people picker experiences. Additionally, if guests are added through the **planned invite** approach they'll also appear in people pickers. To prevent guest users from accessing Power BI, use a Microsoft Entra Conditional Access policy.

Who can you invite?

Most email addresses are supported for guest user invitations, including personal email accounts like gmail.com, outlook.com, and hotmail.com. Microsoft Entra B2B calls these addresses *social identities*.

> **Note**
>
> In Microsoft Entra ID, external users can be set to UserType Member. In Power BI, support for UserType Member is currently in preview. Note the following:
>
> - Microsoft Purview Information Protection isn't supported for external members. Admins in the provider tenant are advised not to enable information protection for external members.
>
> In some situations, external members may see errors during their first sign-in attempt on the provider tenant. To unblock these external members, grant them permission to a Power BI item, such as a workspace, semantic model, or report, and then have them sign in again.

Invite guest users

Guest users only require invitations the first time you invite them to your organization. To invite users, use planned or ad hoc invites.

To use ad hoc invites, use the following capabilities:

- Report and Dashboard sharing
- Report and Dashboard subscriptions
- App access list

Ad hoc invites aren't supported in the workspace access list. Use the planned invites approach to add these users to your organization. After the external user becomes a guest in your organization, add them to the workspace access list.

Planned invites

Use a planned invite if you know which users to invite. The Azure portal or PowerShell enables you to send the invites. You must be assigned the user admin role to invite people.

Follow these steps to send an invite in the Azure portal.

1. In the Azure portal, select Menu button then select **Microsoft Entra ID**.

2. Under **Manage**, select **Users** > **All users** > **New guest user**.

3. Scroll down and enter an **email address** and **personal message**.

4. Select **Invite**.

To invite more than one guest user, use PowerShell or create a bulk invite in Microsoft Entra ID. To use PowerShell for the bulk invite, follow the steps in Tutorial: Use PowerShell to bulk invite Microsoft Entra B2B collaboration users. To use the Azure portal for the bulk invite, follow the steps in Tutorial: Bulk invite Microsoft Entra B2B collaboration users.

The guest user must select **Get Started** in the email invitation they receive. The guest user is then added to the organization.

Ad hoc invites

To invite an external user at any time, add them to your dashboard or report through the share feature or to your app through the access page. Here's an example of what to do when inviting an external user to use an app.

The guest user gets an email indicating that you shared the app with them.

The guest user must sign in with their organization email address. They'll receive a prompt to accept the invitation after signing in. After they sign in, the app opens for the guest user. To return to the app, they should bookmark the link or save the email.

Discoverability for B2B content

Tenant switcher

If you have access to more than one tenant, you can switch between tenants using the tenant switcher.

1. Select your profile picture to open your account manager and choose **Switch**.

2. In the **Switch tenant (preview)** dialog, open the dropdown menu and choose the tenant you want to navigate to.

> **Note**
>
> The dropdown list displays a maximum of 50 tenants.

From external orgs tab

The discoverability for B2B content feature in Power BI makes accessing shared B2B content easy for consumers. Power BI users who are guest users in any other tenant have a tab on their home page (in their home tenant) called *From external orgs*. When you select the tab, it lists all the items shared with you from external tenants that you can access as a guest user. You can filter and sort through the list to find content easily, and see which organization is sharing a specific item with you. When you select an item on the tab, a new window opens and takes you to the relevant provider tenant where you can access the item.

Licensing

Licensing Requirements

The following table lists the licensing requirements for B2B access to Power BI. The columns on the left indicate the workspace type and the per user license for the user sharing data externally. The license limitations across Free user, Pro user, and PPU user outlines limitations for the user consuming the data from an external tenant. Also note to invite guest users, a Power BI Pro or Premium Per User (PPU) license is needed:

Expand table

Provider	**Provider**	**.**	**Consumer User Type**	**.**
Workspace Type	**User Type**	**Free User**	**Pro User**	**PPU User**
All Workspaces	Free User	Not Supported	Not Supported	Not Supported
Pro Workspace	Pro/PPU/PPU Trial	Not Supported	Supported	Supported
PPU Workspace	PPU User	Not Supported	Not Supported	Supported
PPU Workspace	PPU Trial User	Not Supported	Not Supported	Supported
PPC Workspace	Pro/PPU/PPU Trial	Supported	Supported	Supported

> **Note**
>
> Pro Trial users can't invite guest users in Power BI.

Steps to address licensing requirements

As noted previously, the guest user must have the proper licensing in place to view the content that you shared. There are a few ways to make sure the user has a proper license:

- Use Power BI Premium capacity.
- Assign a Power BI Pro or a Premium Per User (PPU) license.
- Use a guest's Power BI Pro or PPU license.

Use Power BI Premium capacity

Assigning the workspace to Power BI Premium capacity lets the guest user use the app without requiring a Power BI Pro license. Power BI Premium also lets apps take advantage of other capabilities like increased refresh rates and large model sizes.

Assign a Power BI Pro or Premium Per User (PPU) license to guest user

Assigning a Power BI Pro or PPU license from your organization to a guest user lets that guest user view content shared with them. For more information about assigning licenses, see Assign licenses to users on the Licenses page. Before assigning Pro or PPU licenses to guest users, consult the Product Terms site to ensure you're in compliance with the terms of your licensing agreement with Microsoft.

Guest user brings their own Power BI Pro or Premium Per User (PPU) license

The guest user may already have a Power BI Pro or PPU license that was assigned to them through their own organization.

To help allowed guests sign in to Power BI, provide them with the Tenant URL. To find the tenant URL, follow these steps.

1. In the Power BI service, in the header menu, select help (**?**), then select **About Power BI**.

2. Look for the value next to **Tenant URL**. Share the tenant URL with your allowed guest users.

Cross-cloud B2B

You can use Power BI's B2B capabilities across Microsoft Azure clouds by configuring Microsoft cloud settings for B2B collaboration. Read Microsoft cloud settings to learn how to establish mutual B2B collaboration between the following clouds:

- Microsoft Azure global cloud and Microsoft Azure Government
- Microsoft Azure global cloud and Microsoft Azure China 21Vianet

There are some limitations to the B2B experience that you should be aware of:

- Guest users may already have a Power BI license that was assigned to them through their own organization. But “Bring your own license” doesn’t work across different Microsoft Azure clouds for B2B guest users. A new license has to be assigned to these guest users by the provider tenant.

- New external users can't be invited to the organization through Power BI sharing, permissions, and subscription experiences.

- On the Home page, the “From external orgs” tab won't list content shared from other clouds.

- Cross-cloud sharing doesn't work when sharing with a security group. For instance, if a user using Power BI in a national cloud invites a security group from the public cloud or vice versa, access isn't granted. This is because the service can't resolve the members of these groups across clouds.

Admin Info for B2B Collaboration

The following tenant level settings in Power BI provide controls to admins. See Export and sharing admin settings for documentation on these settings:

- Guest users can access Microsoft Fabric
- Users can invite guest users to collaborate through item sharing and permissions
- Guest users can browse and access Fabric content
- Users can see guest users in lists of suggested people

There are also Microsoft Entra ID settings that can limit what external guest users can do within your organization. Those settings also apply to your Power BI environment. The following documentation discusses the settings:

- Manage External Collaboration Settings
- Allow or block invitations to B2B users from specific organizations

- Use Conditional Access to allow or block access

Additionally, to use in-place semantic model sharing, tenant admins need to enable the following settings:

- Guest users can work with shared semantic models in their own tenants
- Allow specific users to turn on external data sharing

Considerations and Limitations

- Information protection: See Sensitivity labels in Fabric and Power BI: Considerations and limitations.

- Some experiences aren't available to guest users even when they have higher-level permissions. To update or publish reports, guest users need to use the Power BI service, including Get Data, to upload Power BI Desktop files. The following experiences aren't supported:
  - Direct publishing from Power BI desktop to the Power BI service
  - Guest users can't use Power BI desktop to connect to service semantic models or dataflows in the Power BI service
  - Sending ad hoc invites isn't supported for workspace access lists
  - Guest users can't install a Power BI Gateway and connect it to your organization
  - Guest users can't install apps published to the entire organization
  - Guest users can't use Analyze in Excel
  - Guest users can't be @mentioned in commenting
  - Guest users who use this capability should have a work or school account

- Guest users using social identities experience more limitations because of sign-in restrictions.
  - They can use consumption experiences in the Power BI service through a web browser
  - They can't use the Power BI Mobile apps
  - They won't be able to sign in where a work or school account is required

- This feature isn't currently available with the Power BI SharePoint Online report web part.

- If you share directly to a guest user, Power BI sends them an email with the link. To avoid sending an email, add the guest user to a security group and share to the security group.

- If you disable the **Guest users can browse and access Fabric content** tenant setting, guest users continue to have any workspace role and item permissions

that they were previously granted, or will be granted, in the provider environment. For more information, see the Guest users can browse and access Fabric content tenant setting.

Related content

- For more detailed info, including how row-level security works, check out the whitepaper: Distribute Power BI content to external guest users using Microsoft Entra B2B.
- For information about Microsoft Entra B2B, see What is Microsoft Entra B2B collaboration?
- For information about in-place semantic model sharing, see Power BI in-place semantic model sharing with guest users in external organizations (preview).
- For information about government clouds, see Power BI for US Government.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Power BI high availability, failover, and disaster recovery FAQ

FAQ

This article explains how the Power BI service delivers high availability and provides business continuity and disaster recovery to its users. After reading this article, you should have a better understanding of how high availability is achieved, under what circumstances Power BI performs a failover, and what to expect from the service when it fails over.

What does "high availability" mean for Power BI?

Power BI is fully managed software as a service (SaaS). Power BI is resilient to infrastructure failures so that users can always access their reports. For information about SLAs, see Licensing Resources and Documents.

Power BI uses **Azure availability zones** to protect Power BI reports, applications, and data from datacenter failures. Availability zones are automatically applied and used for Power BI. Availability zones are fault-isolated locations within an Azure region that provide three or more distinct and unique locations within an Azure region that have redundant power, cooling, and networking. Availability zones allow Power BI customers to run critical applications with higher availability and fault tolerance to datacenter failures. Availability zones provide customers with the ability to withstand datacenter failures without triggering a Power BI failover.

For more information, see What are Azure regions and availability zones?

What is a Power BI failover?

Power BI's failover behavior is different based on the type of region you use.

- In regions with regional pairs, Power BI maintains multiple instances of each component in Azure datacenters (also known as regions) to guarantee business continuity. If there's an outage, or Power BI becomes inaccessible or inoperable in a region, Power BI fails all its components in that region to a backup instance. The failover restores availability and operability to the Power BI service instance in a

new region usually within the same geographic location. For more information, see the Microsoft Trust Center.

A failed-over Power BI service instance supports only *read operations*, which means the following operations aren't supported during failover: refreshes, report publish operations, dashboard or report modifications, and other operations that require changes to Power BI metadata (for example, inserting a comment in a report). Read operations, such as displaying dashboards and displaying reports (that aren't based on DirectQuery or Live Connect to on-premises data sources) continue to function normally.

- If you run Power BI components in a region without a regional pair, availability zones provide resiliency. Data isn't replicated to another region, and components don't fail over to another region.

To learn more about how Microsoft Fabric supports reliability, see Reliability in Microsoft Fabric.

How are backup instances kept in sync with my data?

All Power BI service components regularly sync their backup instances. There's a 15-minute targeted point-in-time sync for any content uploaded or changed in Power BI.

If there's a failover in a region with a regional pair, Power BI uses Azure storage geo-redundant replication and Azure SQL geo redundant replication to guarantee backup instances exist in other regions, and can be used.

In regions without a regional pair, Power BI uses Azure storage zone-redundant replication and Azure SQL zone redundancy to replicate data between availability zones.

To learn more about how Microsoft Fabric supports reliability, see Reliability in Microsoft Fabric.

Where are the failover clusters located?

Backup instances reside within the same geographic location (geo) that you select when your organization signs up for Power BI, except where noted in the Microsoft Trust Center. A geo can contain several regions, and Microsoft might replicate data to any of the regions within a specific geo for data resiliency. Microsoft doesn't replicate or

move customer data outside the geo. For a mapping of the geos offered by Power BI and the regions within them, see the Microsoft Trust Center.

How does Microsoft decide to fail over?

There are two different systems that indicate when a failover might be required:

- External and internal monitoring probes indicate a lack of availability or inability to operate properly. Indications might be based on outages detected in Power BI components or one or more of the services that Power BI depends on in a region.
- The Microsoft Azure central operations team reports on critical outages in a region.

In both cases, Power BI executive team members decide to fail over. The decision isn't automated. After the decision is made, failover is automatic.

How do I know Power BI is in failover mode?

A notification is posted on the Power BI support page. Notification information includes the major operations that aren't available, including publish, refresh, create dashboard, duplicate dashboard, and permission changes.

How long does it take Power BI to fail over?

For a zone failover, Power BI can complete the failover process in approximately 30 seconds and continues to function without limitations. For a regional failover, Power BI takes approximately 15 minutes to become operational again after the decision is made that a failover is required. The time to identify that a failover is required varies, based on the scenario that caused the failover.

Power BI uses Azure Storage GEO replication to perform the failover. Such replications usually have a return point of 15 minutes, however, Power BI can't guarantee a timeframe. For more information, see Azure storage redundancy.

What happens to workspaces and reports if my Premium capacity

becomes unavailable?

If a Premium capacity becomes unavailable, workspaces and reports remain accessible and visible to all.

When does my Power BI instance return to the original region?

Power BI service instances return to their original region when the issue that caused the failover is resolved. Check the Power BI support page: When the issue is resolved, the Power BI team removes the notification that describes the failover. At that point, operations should be back to normal.

Am I responsible for the availability of my Power BI solution?

If the Power BI solution used in your organization involves one of the following elements, you must take measures to guarantee that the solution remains highly available:

- If your organization uses Power BI Premium, ensure that the Premium capacity is sized to meet the load demands of your deployment. To help you plan for and meet this requirement, see the Power BI Premium Planning and Deployment white paper. To help with monitoring, new features are regularly added to the admin portal in Power BI and the Power BI Premium Capacity Metrics app.
- If your organization accesses on-premises data sources by using the on-premises data gateway, you must set up the gateway to support high availability, see Manage on-premises data gateway high availability clusters and load balancing. Use this guidance whether you're refreshing reports in import mode, or accessing data or data models by using DirectQuery or Live Connect.

Do gateways function in failover mode?

No. Data required from on-premises data sources (any reports and dashboards based on Direct Query and Live Connect) doesn't work during a failover. The gateway configuration doesn't change though. When the Power BI instance returns to its original state, the gateways return to normal functions.

If there's an extreme disaster in a primary region that prevents you from restoring a gateway for a considerable duration, the failed-over primary region allows read and write operations, so you can redeploy and configure a gateway against the new region.

You can choose to install a new gateway on a different machine or take over an existing gateway. Taking over the existing gateway should be simpler, because all the data sources associated with the old gateway are carried over to the new one.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Migrate Azure Analysis Services to Power BI

Article • 11/10/2023

This article describes the Microsoft Azure Analysis Services to Microsoft Power BI Premium migration feature in Power BI. This feature provides model database migration from Azure Analysis Services to semantic model in Power BI Premium, Power BI Premium Per User, and Power BI Embedded workspaces.

Before beginning a migration, be sure to review Migrate from Azure Analysis Services to Power BI Premium and Migration scenarios. These *Guidance* articles provide a detailed comparison of both platforms and can help you determine a migration strategy that best suits your organization.

After the migration, you can make modifications to the server properties in Analysis Services if needed.

Understanding migration

Prerequisites

Ensure each environment meets the following prerequisites:

In Azure Analysis Services

- The Azure Analysis Services server that you're migrating from and the Power BI workspace that you're migrating to must be in the same tenant.
- You must have Server administrator permissions and belong to the Owner and/or Contributor roles for the subscription.
- Azure Analysis Services must have an Azure Storage account with a container configured and backup enabled for the server as described in Azure Analysis Services database backup and restore.
- If Firewall is enabled for your server, ensure Allow access from the Power BI Service is set to On, or disable Firewall during migration.
- Your server must be started during migration. You can pause your server after migration is complete.

In Power BI

- To migrate to Power BI, you must have a Power BI Premium per Capacity, Power BI Premium per User, or Power BI Embedded license.
- You must have Workspace administrator permission. Power BI admins can view migrations for their tenant, however, they can't perform migrations unless they also have Workspace administrator permission.
- You must have an Azure Data Lake Storage Gen 2 (ADLS Gen 2) storage account in the same tenant and the workspace you're migrating to must be connected to that storage account. For the best performance, your ADLS Gen 2 storage should be located in the same region as the workspace capacity.
- Large semantic model storage format must be enabled for the workspace.
- The XMLA endpoint must be Enabled for read-write for the capacity.
- If a Microsoft on-premises data gateway is configured for the Azure Analysis Services server to connect to on-premises data sources, you must also install and configure a gateway in Power BI.

Pairing

When using the Azure Analysis Services to Power BI Premium migration feature in Power BI, after ensuring all prerequisites are met, you begin a migration by first creating a *connection* between an Azure Analysis Services server and a workspace. The connection is a unique pairing between a server resource in Azure Analysis Services and a workspace in Power BI. Only one pairing connection can exist between a particular server and workspace. When a migration pair is created, you can then migrate one or more model databases from the server to the workspace as a semantic model.

Migration

When migrating, a backup of the model database is created in the Azure storage account specified in the Azure Analysis Services server backup settings. The backup is then copied to the ADLS Gen 2 storage account connected to the workspace. The backup is then restored to the workspace. Build and Write permissions for the model are then configured.

Migration includes:

- Model metadata.

- Model data, as of the latest refresh.
- Model *roles* in Azure Analysis Services, such as those used for object-level and row-level security. UPNs are also included.
- Semantic model Build permissions are set for members of Read model roles.
- Semantic model Write permissions are set for members of Administrator model roles.

Migration doesn't include:

- Service principals configured for the Azure Analysis Services server and model database aren't included in the restored model in Power BI.
- Server redirection enabling client applications, tools, and automation processes to be automatically redirected to the newly migrated model in Power BI are not included in the migration step. Redirection is enabled separately, after migration is completed.

After migration, the model in Power BI is backwards compatible with the same tools used with Azure Analysis Services. Modifying model metadata requires XMLA endpoint-based client tools such as Visual Studio with Analysis Services projects, SQL Server Management Studio, ALM Toolkit, and Tabular Editor. Like other models in Power BI that have metadata modified through the XMLA endpoint, migrated models can't be downloaded as a Power BI Desktop file. To learn more about model management through the XMLA endpoint, see Advanced data model management.

Redirection

Server *redirection* enables XMLA endpoint-based client tools and automation processes to continue to work without having to change the server name reference in the connection string. Client applications, tools, and automation processes are automatically redirected to the migrated model in Power BI. If a server alias is configured for the Azure Analysis Services server, it too will redirect to the migrated model in Power BI.

Client applications and tools connecting to a migrated model must use the following minimum or higher Analysis Services client library versions:

Client library	File version	Product version
MSOLAP	2022.160.35.23	16.0.35.23
AMO	16.0.35.23	19.42.0.4
ADOMD	16.0.35.23	19.42.0.4

The following applications connecting to a migrated model through redirection must meet or exceed minimum versions:

Application	Minimum version
Microsoft Excel	16.0.15826.10000
PowerShell cmdlets	To be determined
Server Profiler	19.0.2
SQL Server Management Studio (SSMS)	19.0.2
Visual Studio with Analysis Services projects (SSDT)	3.0.6

> **Note**
>
> PowerShell cmdlets are currently pending release.

Server redirection for a migration can be enabled by using an On/Off setting. When you enable server redirection, the Azure Analysis Services server must exist and can't be paused. The current user must be both server administrator and workspace administrator.

When Redirection status for the migration shows Server Redirection Enabled, you can then pause your server in the Azure portal or by using the Azure Analysis Services REST API. Client applications, tools, and processes are redirected to the model in Power BI. You aren't billed while your server is paused. Deleting servers with server redirect is currently not supported. To learn more, see Enable redirection later in this article.

Rebind

Unlike server redirection, which redirects XMLA endpoint-based client tools to the new model in Power BI, *rebind* redirects live connect reports in the Power BI service to use the new model in Power BI.

Like server redirection, it's not something done for you automatically as part of the migration. It's something you have control over after your migration has completed. You can enable rebind, check the status of a rebind, or undo the rebind and revert reports back to querying model data in Azure Analysis Services. To learn more, see Enable rebind later in this article.

Important considerations

- Models migrated by using the Azure Analysis Services to Power BI Premium migration feature in Power BI can't be downloaded as a .pbix file. To modify model metadata, use Visual Studio, the open-source ALM Toolkit, or the open-source Tabular Editor.

- Table and PowerQuery M expressions having the same name are not allowed in Power BI models. Prior to migration, ensure model database tables and any PowerQuery M expressions in the model don't have the same name. For any duplicate names, you can rename either the expression or the table, however, in most cases it's easiest to rename the expression. If any duplicate names are present during migration, the restore operation will fail and an error is returned.

To migrate from Azure Analysis Services to Power BI

Before beginning a migration, first ensure prerequisites are met. Open pages for both your Azure Analysis Services server and Power BI in your browser.

Create a migration pairing

1. In Power BI, select **Settings** > **Azure Analysis Services migrations**.

2. On the **Azure Analysis Services to Power BI Premium** page, select **+ New Migration**.

3. On the **Create Azure Analysis Services migration** flyout, select **Connect to Azure**.

4. Select the Azure **Subscription**, **Resource group**, and **Server name** with one or more model databases you want to migrate.

5. In the **Workspace** listbox, select an existing workspace to migrate to, or to create a new workspace, select **Create a new Premium workspace**, and then enter a workspace name, description, and select a license mode.

   For example, if creating a new migration connection with a new PPU workspace, the Create AAS migration flyout should look like the below image:

6. Verify your settings, and then select **Create**.

Migrate

1. On the **Azure Analysis Services to Power BI Premium** page, select **All migrations** to refresh and show migration connection pairs created for your tenant.

2. Under **Azure Analysis Services Server**, select the server containing one or more model databases you want to migrate to the paired Power BI workspace.

3. In **Migration Details**, verify your Azure Analysis Services server and Power BI Premium workspace settings. Any prerequisites not met are shown. Model databases on the server that can be migrated are shown in **Semantic models**.

4. For each model database you want to migrate, under **Include in Migration**, toggle the slider button to **Yes**.

   Model databases are migrated in parallel, to reduce impact on your target capacity the maximum number of model databases that can be migrated concurrently is five.

5. Select **Migrate**. If prerequisites are met, migration will begin. The migration process can take some time while the source model database is saved to backup storage, copied to ADLS Gen 2 storage, and restored to the workspace. You can leave this page and continue to use Power BI while migration is in process.

   Server redirection isn't enabled during migration. Clients will continue to connect to the model database in Azure Analysis Services until server redirection is

enabled. Before enabling server redirection, it's recommended you thoroughly test connecting to the migrated model in Power BI.

Monitor migration

On the **Migration Details** page, in **Semantic models**, select the model database you are migrating to show the **Migration Details** flyout. The flyout shows important details about your migration including status and migration progress. Remember, migration can take some time depending on the size and complexity of the model database being migrated.

When the migration process is completed, any issues are shown.

Enable redirection

After a migration has successfully completed, you can then enable server redirection. When server redirection is complete, client applications and tools that meet the minimum version requirements along with automation processes are automatically redirected to the model in Power BI.

To enable redirection, on the **Azure Analysis Services to Power BI Premium** page, under **All migrations**, for the migration pair you want to redirect, in the **Server redirection enabled** column, set the slider to **Enable**.

Redirection can take some time. You can leave the page and continue to use Power BI while redirection is in process. To check the status of server redirection, select **More options**, and then select **Redirection status**.

The **Server Redirection** flyout shows the status of redirection.

To disable server redirection, on the **Azure Analysis Services to Power BI Premium** page, under **All migrations**, simply move the **Server Redirection Enabled** slider to Off.

Enable rebind

If you have reports in the Power BI service that connected to and queried your data model in Azure Analysis Services, after your migration has successfully completed, you can then rebind reports in the Power BI service to query the model in Power BI.

To rebind reports, on the **Azure Analysis Services to Power BI Premium** page, under **All migrations** > **Azure Analysis Services server**, select your server migration. Then, on the **Migration details** page, for your newly migrated model, select **Rebind reports**.

The rebind operation can take a few minutes to complete. To check the status of your rebind, select **Rebind status**.

To undo the rebind and revert reports back to querying model data in Azure Analysis Services, select **Undo rebind**.

Pause server

After you've verified a successful migration, you can **pause** your Azure Analysis Services server either in the Azure portal or by using the Azure Analysis Services REST API.

If your server remains started after you’ve enabled server redirection, existing Azure Analysis Services models can still be queried by setting the **AsAzureRedirection** connection string property to **Disabled**.

Community

Power BI has a vibrant community where MVPs, BI pros, and peers share expertise in discussion groups, videos, blogs and more. When learning about migration, be sure to check out these additional resources:

- Power BI Community
- Search "Migrate Azure Analysis Services to Power BI" on Bing

See also

Azure Analysis Services database backup and restore
Azure Data Lake Storage Gen 2 (ADLS Gen 2)

OneLake integration for semantic models

Article • 03/21/2025

With Microsoft OneLake integration for semantic models, data imported into model tables can also be automatically written to *Delta tables* in OneLake. The Delta format is the unified table format across all compute engines in Microsoft Fabric. OneLake integration exports the data with all key performance features enabled to provide more seamless data access with higher performance.

Data scientists, database analysts, app developers, data engineers, and other data consumers can then access the same data that drives your business intelligence and financial reports in Power BI. T-SQL, Python, Scala, PySpark, Spark SQL, R, and no-code/low-code solutions can all be used to query data from Delta tables.

Before implementing a OneLake integration solution in your organization, be sure to read Considerations and limitations later in this article.

Prerequisites

OneLake integration for semantic models is supported on Power BI Premium P and Microsoft Fabric F SKUs only. It's not supported on Power BI Pro, Premium Per User, or Power BI Embedded A/EM SKUs.

Before enabling OneLake integration, you must have one or more import semantic models in a workspace on a Power BI Premium or Fabric capacity. Import semantic model is a type of data model where data is fully imported into Power BI's in-memory storage, allowing fast and efficient querying.

Permissions

Model *contributor* (read, write, explore) permissions are required to access the contents of a model folder and create shortcuts linking to the folder in Lakehouse explorer.

Enable OneLake integration

In your semantic model settings, expand **OneLake integration**, click the slider to **On**, and then select **Apply**.

Admin portal

Global and tenant admins can control OneLake integration by using the following setting in the Power BI admin portal:

- **Users can create Fabric items** - enables production-ready Fabric features, including OneLake integration. This setting can be managed at both the organizational level and the capacity level. If disabled, users can't turn on OneLake integration for their semantic models, and any semantic models currently

configured for OneLake integration stop exporting import tables to OneLake. OneLake integration is enabled by default for the entire organization. The following image shows this setting enabled:

- **Semantic models can export data to OneLake** - enables semantic models configured for OneLake integration to send import tables to OneLake. Applies to the entire organization. The following image shows this setting enabled:

Refresh model

In order for model import data to be written to a Delta table in OneLake, at least one manual or scheduled refresh for the model must be run. Either run a manual refresh or wait for a scheduled refresh.

Export OneLake Delta tables

Delta tables can be exported in many ways. If your semantic model has XMLA read-write mode enabled, you can export programmatically by using the Tabular Object Model (TOM) and Tabular Model Scripting Language (TMSL).

For example, you can use SQL Server Management Studio (SSMS) to run the following TMSL command:

JSON

```
{
 "export": {
   "layout": "delta",
   "type": "full",
   "objects": [
     {
       "database": "<database name>"
     }
   ]
 }
}
```

Explore export files

After exporting, you can use OneLake file explorer, which integrates OneLake with your Windows File Explorer, to locate Delta table export files.

1. In OneLake file explorer, right click on the workspace folder, and then select **Sync from OneLake**.

2. Use Windows File Explorer to locate your data files. In the workspace folder, look for a subfolder with a name that matches your semantic model and ends with **.SemanticModel**. The semantic model folder includes every import-mode table in a subfolder that contains the Delta table's parquet files and log.

Shortcuts

By creating shortcuts for your semantic model Lakehouse tables, you can provide quick and easy access to them from other workloads in Fabric.

1. In Lakehouse Explorer, right-click **Tables**, and then select **New shortcut**.

2. In **New shortcut**, select **Microsoft OneLake**.

3. In **Select a data source type**, select your semantic model, and then select the tables you want to include.

Considerations and limitations

- Workspace Admins, Members, and Contributors, as well as Users with direct Write permission on a semantic model are granted Read permission on the exported artifact folder in OneLake.
- Users with Read permission on a semantic model get Read permission to the artifact folder in OneLake only if there are no RLS/OLS roles defined for the semantic model.
- Currency data types with values larger than 18 decimal points can have some precision loss when exported to Delta files.
- Semantic models in BYOK enabled workspaces aren't supported.
- Multi-Geo capacities aren't yet supported.
- Measures, DirectQuery tables, hybrid tables, calculation group tables, and system managed aggregation tables can't be exported to Delta format tables.
- Old versions of the delta tables are deleted after three days. Other execution engines which use an older but now deleted version of the data must move forward to an available version.

Related content

- What is OneLake?
- OneLake file explorer overview

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Purchase and assign Power BI paid user licenses

Article • 11/12/2024

This article is for administrators and explains how to purchase paid user licenses for Power BI and Fabric in the Microsoft 365 admin center. After purchasing, you assign licenses to users from either the Microsoft 365 admin center or from the Azure portal. Some organizations make licenses available for self-service upgrade and purchase by the organization's users. And, some organizations don't make licenses available for self-service or they might even put an alternate processes in place.

> **Note**
>
> The Power BI service is available as a standalone service and as one of the services that's integrated with Microsoft Fabric. Administration and licensing of the Power BI service is now integrated with Microsoft Fabric.

To learn about license types, including Pro and Premium Per User (PPU), see Licensing for Fabric and Power BI.

Prerequisites

- To purchase and assign licenses in the Microsoft 365 admin center, you must be a member of the Global or Billing admin role in Microsoft 365.
- To assign licenses in the Azure portal, you must be an owner of the Azure subscription that Power BI uses for Microsoft Entra lookups.

Purchase licenses in Microsoft 365

To purchase Power BI paid licenses in the Microsoft 365 admin center:

1. Using your administrator account, sign in to the Microsoft 365 admin center.
2. On the navigation menu, select **Home**, and then select **Subscriptions** > **Add more products**.
3. In the **View by category** section, search for **Power BI**.
4. Scroll to the license you want to purchase, and select **Details**.

5. Select the number of licenses you need and whether you want to be charged monthly or yearly.

6. Select **Buy**.

7. Complete the **Checkout** page and place your order.

8. To verify your purchase, on the navigation menu, select **Billing**, and then select **Your Products**.

> ⓘ **Note**
>
> To receive an invoice instead of using a credit card or bank account, work with your Microsoft Reseller or go through the Volume Licensing Service Center to add or remove licenses. For more information, see Manage subscription licenses.

Assign licenses from the Microsoft 365 admin center

To assign licenses to users, from **Billing**, select **Licenses**, and **Power BI Pro** or **Power BI Premium Per User**. For detailed information about assigning licenses from the Microsoft 365 admin center, see Assign Microsoft 365 licenses to users.

For guest users, see Use the licenses page to assign licenses to users. Before assigning paid licenses to guest users, contact your Microsoft account representative to make sure you're in compliance with the terms of your agreement.

Assign licenses from the Azure portal

Follow these steps to assign Power BI licenses to individual user accounts:

1. Sign in to the Azure portal.
2. Search for and select **Microsoft Entra ID**.

3. In the navigation pane, under **Manage**, select **Licenses**.
4. Select **Manage** again and choose **All products.**
5. Select the name of your product (for example, **Power BI Premium Per User** or **Power BI Pro**) and then choose **+ Assign**.
6. On the **Assign license** page, select a user, or select **+ Add users and groups**. Select one or more users from the list.
7. Select **Assignment options** and set the required options to **On**.
8. Select **Review + Assign**, and then select **Assign**.

Considerations and limitations

Self-service purchase, subscription, and license management capabilities for Fabric and Power BI are available for commercial cloud customers. For more information:

- Self-service purchase FAQ
- Enable or disable self-service sign-up and purchasing

Related content

- Power BI licensing in your organization
- Sign up for Power BI as an individual

More questions? Try asking the Power BI Community.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Organizational licenses and subscriptions for Fabric and Power BI

Article • 09/19/2024

There are two ways for users to get a license, from an administrator or by using self-service. This article is for the administrators, who purchase and manage services and licenses.

Billing administrators can sign up for the Power BI service and Fabric. After signing up and purchasing a subscription or a free trial, Billing, License, and User administrators assign licenses to users in their organization.

If you give them permissions, users in your organization can get one of the organization's licenses simply by signing in to Power BI (app.powerbi.com) or Fabric (app.fabric.microsoft.com). When a user signs in, they automatically receive a license. Administrators can set these permissions by following Enable and disable self-service.

> **Note**
>
> If you're an individual, you can sign up for your own free, Pro, Premium Per User, trial licenses or trial of a Fabric capacity. This process is called *self-service*. To learn more, see the self-service process.

Fabric and the Power BI service

Power BI is available as a standalone SaaS service and as one of the services integrated with Microsoft Fabric. Administration and licensing of the Power BI service is now integrated with Microsoft Fabric.

Licenses and subscriptions

Fabric and the Power BI service are both SaaS platforms and require licenses and at least one capacity subscription. There are some differences in how these licenses and capacities are acquired.

Power BI licenses

Use of the Power BI service requires a license and a capacity.

- Per user license - Per user licenses, allow users to work in the Power BI service. The options are Fabric (Free), Pro, and Premium Per User (PPU).
- Capacity subscription - There are two types of Power BI subscriptions for organizations: standard and Premium. Premium provides enhancements to Power BI, and a comprehensive portfolio of Premium features. Power BI Premium is a tenant-level Microsoft 365 subscription, available in a choice of SKUs (Stock Keeping Units).

Each Microsoft 365 E5 subscription includes standard capacity and a Pro license.

Fabric licenses

To access the Fabric SaaS platform, you need a license and a capacity.

- Per user license: Per user licenses allow users to work in Fabric. The options are Fabric (Free), Pro, and Premium Per User (PPU). The two Power BI licenses apply to using the Power BI workload in Fabric.
- Capacity license - An organizational license that provides a pool of resources for Fabric operations. Capacity licenses are divided into stock keeping units (SKUs). Each SKU provides a different number of capacity units (CUs) which are used to calculate the capacity's compute power. Fabric capacities are available for purchase and for trial.

Which admins can purchase licenses and subscriptions

Admin roles for purchasing licenses and subscriptions

You must belong to the Billing admin role to purchase or assign licenses for your organization. Admin roles are assigned from the Microsoft Entra admin center or the Microsoft 365 admin center. For more information about admin roles in Microsoft Entra ID, see View and assign administrator roles in Microsoft Entra ID. To learn more about admin roles in Microsoft 365, including best practices, see About admin roles.

Admin roles for managing licenses and subscriptions

After the licenses and subscriptions are purchased, License, or User admins can manage licenses for an organization. For details about these admin roles, see Admin roles.

Get Fabric or Power BI for your organization

Fabric and the Power BI service are available for organizations to purchase and to try for free. For detailed instructions, select the option you prefer.

> **Tip**
>
> If you're ready to make a purchase, use these links to find up-to-date pricing information.
>
> - Power BI Pricing & product comparison
> - Pricing options for Fabric

1. Purchase a Fabric subscription. If you're ready to purchase, your options include bulk purchasing for your organization or enabling your users to upgrade their own licenses.

   After you purchase a Fabric subscription, enable Fabric for your organization. Enabling Fabric includes setting up tenants and capacities.

2. Purchase a Power BI subscription and licenses. Power BI Pro is included in Microsoft 365 E5. Otherwise, you can purchase Pro or PPU licenses from the Microsoft pricing site, through Microsoft 365, or through a Microsoft partner. After your purchase, you can assign licenses to individual users or use self-service. For more information, see enabling your users to upgrade their own licenses.

3. Go directly to the sign-up wizard for Power BI Pro.

4. Start a free 60-day Fabric trial for your organization. The trial includes a trial capacity, 1 TB of storage, and access to all of the Fabric experiences and features.

5. Get free licenses for all of your users. The Fabric (Free) license doesn't include a Fabric capacity. The Fabric (Free) license includes access to the paid features of the Power BI service. Sign up on app.fabric.microsoft.com.

6. Start a free 30-day trial of Power BI Pro. The trial includes up to 25 licenses. When the trial expires, you receive a charge for the licenses.

View existing licenses

To see which users in your organization already have a license, see View and manage user licenses.

Enable and disable self-service sign-up and purchase

You purchased licenses or signed up for an organizational trial. Now, decide whether your users can assign themselves a license or give themselves an automatic license upgrade. Here are links to help you decide which settings to use.

Self-service

- When to use self-service sign-up and purchase
- Manage self-service purchases and trials
- Manage self-service license requests in the Microsoft 365 admin center
- Manage self-service sign-up subscriptions in the Microsoft 365 admin center
- How to combine self-service settings

Guest user licenses

You might want to distribute content to users who are outside of your organization. You can share content with external users by inviting them to view content as a guest. Microsoft Entra Business-to-business (Microsoft Entra B2B) enables sharing with external guest users. Prerequisites:

- The ability to share content with external users must be enabled.
- The guest user must have the proper licensing in place to view the shared content.

For more information about guest user access, see Distribute Power BI content to external guest users with Microsoft Entra B2B.

Other articles for admins

There are many other admin tasks related to licenses and subscriptions. Some of them are listed and linked here.

- Assign and manage licenses with Microsoft 365 and with the Azure portal.
- Remove or reassign a license, enable, disable a license
- Cancel a trial
- Takeover a license or tenant
- Handle expiring trials.
- Handle expiring licenses for Power BI

Power BI license expiration

There's a grace period after a Power BI license expires. For licenses that are part of a volume license purchase, the grace period is 90 days. If you bought the license directly, the grace period is 30 days. For license trials, there is no grace period.

Power BI has the same license lifecycle as Microsoft 365. For more information, see What happens to my data and access when my Microsoft 365 for business subscription ends.

Manage subscriptions included with Microsoft 365 E5 SKUs

A Microsoft 365 E5 subscription includes Power BI Pro licenses. To learn how to manage licenses, see Administration overview.

Related content

- Purchase and assign Power BI Pro licenses
- About self-service sign-up
- Business subscriptions and billing documentation
- Find Power BI users that are signed in
- Self service FAQ

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Administration overview

Article • 08/04/2024

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

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

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

Manage

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

Grant and manage licenses

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

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

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

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

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

Turn off self-service

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

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

Take over a subscription

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

View your subscriptions

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

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

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

Assign admin roles

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

Customize a Fabric tenant

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

according to the organizational functions, and workspaces can be created according to each function's divisions.

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

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

Add and remove users

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

Govern and secure data

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

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

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

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

Control

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

Delegate admin rights

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

Enable Fabric settings

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

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

Grant permissions

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

Monitor

An important part of an admin's role is to monitor what's going on in the organization. Fabric has several tools for monitoring different aspects of the platform usage. Monitoring enables your organization to comply with internal policies and external rules and regulations. You can also use monitoring to review consumption and billing, so that you can establish the best way to use your organizational resources. By analyzing what's happening in your organization, you can decide if you need to buy more resources, and potentially save money by using cheaper or fewer resources if that can be done.

Admin monitoring workspace

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

Monitoring hub

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

View audit logs

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

Understand consumption

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

Reviewing bills

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

Capabilities

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

Expand table

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

Related content

- Admin roles
- Security overview
- Governance and compliance overview

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Introduction to enabling and disabling self-service sign-up and purchasing

Article • 11/13/2024

Billing administrators can determine whether to enable or disable self-service sign-up. As a Billing administrator, you also determine whether users in your organization can make self-service purchases to get their own license.

Turning off self-service sign-up keeps users from exploring Power BI for data visualization and analysis. If you block individual sign-up, you may want to get Fabric (Free) licenses for your organization and assign them to all users.

Turning off self-service purchase keeps users from performing actions that require a paid license. These actions include sharing, exporting, and creating workspaces for collaboration.

This article is an overview of self-service in Power BI. To learn how to enable and disable self-service, see Instructions for enabling and disabling self-service sign-up and purchasing of licenses and subscriptions.

> **Note**
>
> If you acquired Power BI through a Microsoft Cloud Solution Provider (CSP), the settings might be disabled to block users from signing up individually. Your CSP can act as the admin for your organization, requiring that you contact them to help you change this setting.

When to use self-service sign-up and purchase

Use self-service when

- Your large and decentralized organization (work or school) gives individuals the flexibility to try or purchase SaaS (Software as a service) licenses for their own use.
- Your one-person or small organization purchases only one or a few Power BI Pro licenses.
- Individuals want to try Power BI and become proficient before purchasing a subscription for the entire organization.
- Current users with a free license want to create and share content and upgrade to a 60-day trial of the paid features of Power BI.

- Current users with a free license want to start a free trial of a Fabric capacity.

Disable self-service when

- Your organization has procurement processes that meet compliance, regulatory, security, and governance needs. Ensure that all licenses are approved and managed according to defined processes.
- Your organization has requirements for new Power BI Pro or Premium Per User licensees, such as mandatory training or user acknowledgment of data protection policies.
- Your organization prohibits use of Fabric or the Power BI service due to data privacy or other concerns and needs to closely control the assignment of Fabric (Free) licenses.
- You want to ensure that all Power BI Pro or Premium Per User licenses fall under an enterprise agreement that takes advantage of a negotiated or discounted licensing rate.
- Current users with a Fabric (Free) license are prompted to try or directly purchase a Fabric Pro license. Your organization might not want these users to upgrade because of security, privacy, or expense.

Related content

How-to instructions for enabling and disabling self-service sign-up and purchasing of licenses and subscriptions.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Sign up for Power BI with a new Microsoft 365 trial

Article • 08/27/2024

This article describes an alternative way to sign up for the Power BI service if you don't already have a work or school email account and don't already have an account that works with Microsoft 365.

You're unable to sign up for Power BI with your personal email address. You can still try out Power BI and Fabric with either an Office 365 or a Microsoft 365 trial. During the sign-up process, you create an "onmicrosoft" email work account. Use that new work account to sign up for the Power BI service and get a Fabric free or Power BI Pro license. Continue to use that work account even after you cancel your Office 365 or Microsoft 365 trial.

> **Note**
>
> You must use a credit or debit card when you sign up for the Microsoft 365 free trial. At the end of your free trial period, your trial subscription is automatically converted to a paid subscription. Your card isn't billed until the trial period ends. If you don't want to be charged, cancel your trial before you reach 30 days.

Sign up for a Microsoft 365 or an Office 365 trial

There are many trials available on the Microsoft 365 site at any time. Look for the **Try free for one month** buttons.

To follow along, sign up for an Office 365 E5 trial on the Microsoft 365 web site. If you don't already have an account, Microsoft walks you through the steps to create a new onmicrosoft work account.

1. On the Office 365 E5 option, select **Try for free**.
2. Follow the prompts to set up your trial. Enter a non-work and non-school email address, and select **Next** > **Set up account**.

3. After completing the sign-up process, Microsoft displays your new user name and domain, for example, *pradtannak@yourcompany.onmicrosoft.com*. Create a password, and then select **Next**.

You created a new onmicrosoft.com business account and started a free trial of Office 365. Your trial includes Power BI Pro.

A different way to try Power BI is to sign up for a trial of Microsoft 365. During the sign-up process, create an onmicrosoft.com account. Use the onmicrosoft.com account to sign up for a trial of the Power BI service as an individual.

Important considerations

If you have any issues when you sign in with the new account credentials, try using a private browser session.

When you use this sign-up method, you create a new organizational tenant, and you become the User and Billing administrator of the tenant. For more information, see What is Power BI administration. You can add new users to your tenant, then share with them, as described in the Microsoft 365 admin documentation.

If you'd like to use email with this new business account, enable email for your new account in Outlook. Alternatively, you can access your onmicrosoft email by going to the Microsoft account sign-in page and entering your email address and password. Use the Microsoft 365 portal and select **Admin** to update the email or add an alternate email address.

Related content

- Try or buy a Microsoft 365 for business subscription
- What is Power BI administration?
- Power BI licensing in your organization
- Signing up for Power BI as an individual

More questions? Ask the Power BI Community

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Sign-in to Microsoft Entra ID with email as an alternate login ID (Preview)

Article • 03/12/2025

> **Note**
>
> Sign-in to Microsoft Entra ID with email as an alternate login ID is a public preview feature of Microsoft Entra ID. For more information about previews, see Supplemental Terms of Use for Microsoft Azure Previews.

Many organizations want to let users sign in to Microsoft Entra ID using the same credentials as their on-premises directory environment. With this approach, known as hybrid authentication, users only need to remember one set of credentials.

Some organizations haven't moved to hybrid authentication for the following reasons:

- By default, the Microsoft Entra user Principal Name (UPN) is set to the same value as the on-premises UPN.
- Changing the Microsoft Entra UPN creates a mismatch between on-premises and Microsoft Entra environments that could cause problems with certain applications and services.
- Due to business or compliance reasons, the organization doesn't want to use the on-premises UPN to sign in to Microsoft Entra ID.

To move toward hybrid authentication, you can configure Microsoft Entra ID to let users sign in with their email as an alternate login ID. For example, if *Contoso* rebranded to *Fabrikam*, rather than continuing to sign in with the legacy `ana@contoso.com` UPN, email as an alternate login ID can be used. To access an application or service, users would sign in to Microsoft Entra ID using their non-UPN email, such as `ana@fabrikam.com`.

This article shows you how to enable and use email as an alternate login ID.

Before you begin

Here's what you need to know about email as an alternate login ID:

- The feature is available in Microsoft Entra ID Free edition and higher.
- The feature enables sign-in with *ProxyAddresses*, in addition to UPN, for cloud-authenticated Microsoft Entra users. More on how this applies to Microsoft Entra business-to-business (B2B) collaboration in the B2B section.
- When a user signs in with a non-UPN email, the `unique_name` and `preferred_username` claims (if present) in the ID token will return the non-UPN email.
  - If the non-UPN email in use becomes stale (no longer belongs to the user), these claims will return the UPN instead.
- The feature supports managed authentication with Password Hash Sync (PHS) or Pass-Through Authentication (PTA).
- There are two options for configuring the feature:
  - Home Realm Discovery (HRD) policy - Use this option to enable the feature for the entire tenant. At least the Application Administrator role is required.
  - Staged rollout policy - Use this option to test the feature with specific Microsoft Entra groups. When you first add a security group for staged rollout, you're limited to 200 users to avoid a UX time-out. After you've added the group, you can add more users directly to it, as required.

Preview limitations

In the current preview state, the following limitations apply to email as an alternate login ID:

- **User experience** - Users may see their UPN, even when they signed-in with their non-UPN email. The following example behavior may be seen:
  - User is prompted to sign in with UPN when directed to Microsoft Entra sign-in with `login_hint=<non-UPN email>`.
  - When a user signs-in with a non-UPN email and enters an incorrect password, the "*Enter your password*" page changes to display the UPN.
  - On some Microsoft sites and apps, such as Microsoft Office, the *Account Manager* control typically displayed in the upper right may display the user's UPN instead of the non-UPN email used to sign in.

- **Unsupported flows** - Some flows are currently not compatible with non-UPN emails, such as the following:

  - Microsoft Entra ID Protection doesn't match non-UPN emails with *Leaked Credentials* risk detection. This risk detection uses the UPN to match credentials that have been leaked. For more information, see How To: Investigate risk.
  - When a user is signed-in with a non-UPN email, they cannot change their password. Microsoft Entra self-service password reset (SSPR) should work as expected. During SSPR, the user may see their UPN if they verify their identity using a non-UPN email.

- **Unsupported scenarios** - The following scenarios are not supported. Sign-in with non-UPN email for:
  - Microsoft Entra hybrid joined devices
  - Microsoft Entra joined devices
  - Microsoft Entra registered devices
  - Single Sign-On and App Protection Policies on Mobile Platform
  - Legacy authentication such as POP3 and SMTP

- **Unsupported apps** - Some third-party applications may not work as expected if they assume that the `unique_name` or `preferred_username` claims are immutable or will always match a specific user attribute, such as UPN.

- **Logging** - Changes made to the feature's configuration in HRD policy are not explicitly shown in the audit logs.

- **Staged rollout policy** - The following limitations apply only when the feature is enabled using staged rollout policy:
  - The feature does not work as expected for users that are included in other staged rollout policies.
  - Staged rollout policy supports a maximum of 10 groups per feature.
  - Staged rollout policy does not support nested groups.
  - Staged rollout policy does not support dynamic membership groups.
  - Contact objects inside the group will block the group from being added to a staged rollout policy.

- **Duplicate values** - Within a tenant, a cloud-only user's UPN can be the same value as another user's proxy address synced from the on-premises directory. In this scenario, with the feature enabled, the cloud-only user will not be able to sign in with their UPN. More on this issue in the Troubleshoot section.

Overview of alternate login ID options

To sign in to Microsoft Entra ID, users enter a value that uniquely identifies their account. Historically, you could only use the Microsoft Entra UPN as the sign-in identifier.

For organizations where the on-premises UPN is the user's preferred sign-in email, this approach was great. Those organizations would set the Microsoft Entra UPN to the exact same value as the on-premises UPN, and users would have a consistent sign-in experience.

Alternate Login ID for AD FS

However, in some organizations the on-premises UPN isn't used as a sign-in identifier. In the on-premises environments, you would configure the local AD DS to allow sign-in with an alternate login ID. Setting the Microsoft Entra UPN to the same value as the on-premises UPN isn't an option as Microsoft Entra ID would then require users to sign in with that value.

Alternate Login ID in Microsoft Entra Connect

The typical workaround to this issue was to set the Microsoft Entra UPN to the email address the user expects to sign in with. This approach works, though results in different UPNs between the on-premises AD and Microsoft Entra ID, and this configuration isn't compatible with all Microsoft 365 workloads.

Email as an Alternate Login ID

A different approach is to synchronize the Microsoft Entra ID and on-premises UPNs to the same value and then configure Microsoft Entra ID to allow users to sign in to Microsoft Entra ID with a verified email. To provide this ability, you define one or more email addresses in the user's *ProxyAddresses* attribute in the on-premises directory. *ProxyAddresses* are then synchronized to Microsoft Entra ID automatically using Microsoft Entra Connect.

Expand table

Option	Description
Alternate Login ID for AD FS	Enable sign-in with an alternate attribute (such as Mail) for AD FS users.
Alternate Login ID in Microsoft Entra Connect	Synchronize an alternate attribute (such as Mail) as the Microsoft Entra UPN.
Email as an Alternate Login ID	Enable sign-in with verified domain *ProxyAddresses* for Microsoft Entra users.

Synchronize sign-in email addresses to Microsoft Entra ID

Traditional Active Directory Domain Services (AD DS) or Active Directory Federation Services (AD FS) authentication happens directly on your network and is handled by your AD DS infrastructure. With hybrid authentication, users can instead sign in directly to Microsoft Entra ID.

To support this hybrid authentication approach, you synchronize your on-premises AD DS environment to Microsoft Entra ID using Microsoft Entra Connect and configure it to use PHS or PTA. For more information, see Choose the right authentication method for your Microsoft Entra hybrid identity solution.

In both configuration options, the user submits their username and password to Microsoft Entra ID, which validates the credentials and issues a ticket. When users sign in to Microsoft Entra ID, it removes the need for your organization to host and manage an AD FS infrastructure.

One of the user attributes that's automatically synchronized by Microsoft Entra Connect is *ProxyAddresses*. If users have an email address defined in the on-premises AD DS environment as part of the *ProxyAddresses* attribute, it's automatically synchronized to Microsoft Entra ID. This email address can then be used directly in the Microsoft Entra sign-in process as an alternate login ID.

> **ⓘ Important**
>
> Only emails in verified domains for the tenant are synchronized to Microsoft Entra ID. Each Microsoft Entra tenant has one or more verified domains, for which you have proven ownership, and are uniquely bound to your tenant.
>
> For more information, see **Add and verify a custom domain name in Microsoft Entra ID**.

B2B guest user sign-in with an email address

Email as an alternate login ID applies to Microsoft Entra B2B collaboration under a "bring your own sign-in identifiers" model. When email as an alternate login ID is enabled in the home tenant, Microsoft Entra users can perform guest sign in with non-UPN email on the resource tenant endpoint. No action is required from the resource tenant to enable this functionality.

> **Note**
>
> When an alternate login ID is used on a resource tenant endpoint that does not have the functionality enabled, the sign-in process will work seamlessly, but SSO will be interrupted.

Enable user sign-in with an email address

> **Note**
>
> This configuration option uses HRD policy. For more information, see homeRealmDiscoveryPolicy resource type.

Once users with the *ProxyAddresses* attribute applied are synchronized to Microsoft Entra ID using Microsoft Entra Connect, you need to enable the feature for users to sign in with email as an alternate login ID for your tenant. This feature tells the Microsoft Entra login servers to not only check the sign-in identifier against UPN values, but also against *ProxyAddresses* values for the email address.

You can use either Microsoft Entra admin center or Graph PowerShell to set up the feature.

Microsoft Entra admin center

1. Sign in to the Microsoft Entra admin center as at least a Hybrid Identity Administrator.

2. Browse to **Identity** > **Hybrid management** > **Microsoft Entra Connect** > **Connect Sync**

3. Select Email as alternate login ID**.

4. Click the checkbox next to *Email as an alternate login ID*.

5. Click **Save**.

With the policy applied, it can take up to one hour to propagate and for users to be able to sign in using their alternate login ID.

PowerShell

> **Note**
>
> This configuration option uses HRD policy. For more information, see homeRealmDiscoveryPolicy resource type.

Once users with the *ProxyAddresses* attribute applied are synchronized to Microsoft Entra ID using Microsoft Entra Connect, you need to enable the feature for users to sign-in with email as an alternate login ID for your tenant. This feature tells the Microsoft Entra login servers to not only check the sign-in identifier against UPN values, but also against *ProxyAddresses* values for the email address.

1. Open a PowerShell session as an administrator, then install the *Microsoft.Graph* module using the `Install-Module` cmdlet:

   PowerShell
   ```
   Install-Module Microsoft.Graph
   ```

   For more information on installation, see Install the Microsoft Graph PowerShell SDK.

2. Sign-in to your Microsoft Entra tenant using the `Connect-MgGraph` cmdlet:

   PowerShell
   ```
   Connect-MgGraph -Scopes "Policy.ReadWrite.ApplicationConfiguration" -
   TenantId organizations
   ```

   The command will ask you to authenticate using a web browser.

3. Check if a *HomeRealmDiscoveryPolicy* already exists in your tenant using the `Get-MgPolicyHomeRealmDiscoveryPolicy` cmdlet as follows:

   PowerShell
   ```
   Get-MgPolicyHomeRealmDiscoveryPolicy
   ```

4. If there's no policy currently configured, the command returns nothing. If a policy is returned, skip this step and move on to the next step to update an existing policy.

   To add the *HomeRealmDiscoveryPolicy* to the tenant, use the `New-MgPolicyHomeRealmDiscoveryPolicy` cmdlet and set the *AlternateIdLogin* attribute to *"Enabled": true* as shown in the following example:

   PowerShell
   ```
   $AzureADPolicyDefinition = @(
     @{
   ```

```
      "HomeRealmDiscoveryPolicy" = @{
         "AlternateIdLogin" = @{
            "Enabled" = $true
         }
      }
   } | ConvertTo-JSON -Compress
)

$AzureADPolicyParameters = @{
  Definition            = $AzureADPolicyDefinition
  DisplayName           = "BasicAutoAccelerationPolicy"
  AdditionalProperties  = @{ IsOrganizationDefault = $true }
}

New-MgPolicyHomeRealmDiscoveryPolicy @AzureADPolicyParameters
```

When the policy has been successfully created, the command returns the policy ID, as shown in the following example output:

PowerShell

```
Definition
DeletedDateTime Description DisplayName                Id
IsOrganizationDefault
----------                                                          --
------------- ----------- -----------                --            ---
------------------
{{"HomeRealmDiscoveryPolicy":{"AlternateIdLogin":{"Enabled":true}}}}
BasicAutoAccelerationPolicy HRD_POLICY_ID True
```

5. If there's already a configured policy, check if the *AlternateIdLogin* attribute is enabled, as shown in the following example policy output:

PowerShell

```
Definition
DeletedDateTime Description DisplayName                Id
IsOrganizationDefault
----------                                                          --
------------- ----------- -----------                --            ---
------------------
{{"HomeRealmDiscoveryPolicy":{"AlternateIdLogin":{"Enabled":true}}}}
BasicAutoAccelerationPolicy HRD_POLICY_ID True
```

If the policy exists but the *AlternateIdLogin* attribute that isn't present or enabled, or if other attributes exist on the policy you wish to preserve, update the existing policy using the `Update-MgPolicyHomeRealmDiscoveryPolicy` cmdlet.

> **Important**
>
> When you update the policy, make sure you include any old settings and the new *AlternateIdLogin* attribute.

The following example adds the *AlternateIdLogin* attribute and preserves the *AllowCloudPasswordValidation* attribute that was previously set:

PowerShell

```
$AzureADPolicyDefinition = @(
  @{
     "HomeRealmDiscoveryPolicy" = @{
        "AllowCloudPasswordValidation" = $true
        "AlternateIdLogin" = @{
           "Enabled" = $true
        }
     }
  } | ConvertTo-JSON -Compress
)

$AzureADPolicyParameters = @{
  HomeRealmDiscoveryPolicyId = "HRD_POLICY_ID"
  Definition                 = $AzureADPolicyDefinition
  DisplayName                = "BasicAutoAccelerationPolicy"
  AdditionalProperties       = @{ "IsOrganizationDefault" = $true }
}

Update-MgPolicyHomeRealmDiscoveryPolicy @AzureADPolicyParameters
```

Confirm that the updated policy shows your changes and that the *AlternateIdLogin* attribute is now enabled:

PowerShell

```
Get-MgPolicyHomeRealmDiscoveryPolicy
```

> **Note**
>
> With the policy applied, it can take up to an hour to propagate and for users to be able to sign-in using email as an alternate login ID.

Removing policies

To remove an HRD policy, use the `Remove-MgPolicyHomeRealmDiscoveryPolicy` cmdlet:

```
PowerShell

Remove-MgPolicyHomeRealmDiscoveryPolicy -HomeRealmDiscoveryPolicyId
"HRD_POLICY_ID"
```

Enable staged rollout to test user sign-in with an email address

> **Note**
>
> This configuration option uses staged rollout policy. For more information, see featureRolloutPolicy resource type.

Staged rollout policy allows tenant administrators to enable features for specific Microsoft Entra groups. It is recommended that tenant administrators use staged rollout to test user sign-in with an email address. When administrators are ready to deploy this feature to their entire tenant, they should use HRD policy.

1. Open a PowerShell session as an administrator, then install the *Microsoft.Graph.Beta* module using the Install-Module cmdlet:

   ```
   PowerShell

   Install-Module Microsoft.Graph.Beta
   ```

   If prompted, select **Y** to install NuGet or to install from an untrusted repository.

2. Sign in to your Microsoft Entra tenant using the Connect-MgGraph cmdlet:

   ```
   PowerShell

   Connect-MgGraph -Scopes "Directory.ReadWrite.All"
   ```

   The command returns information about your account, environment, and tenant ID.

3. List all existing staged rollout policies using the following cmdlet:

   ```
   PowerShell
   ```

```
Get-MgBetaPolicyFeatureRolloutPolicy
```

4. If there are no existing staged rollout policies for this feature, create a new staged rollout policy and take note of the policy ID:

PowerShell

```
$MgPolicyFeatureRolloutPolicy = @{
Feature     = "EmailAsAlternateId"
DisplayName = "EmailAsAlternateId Rollout Policy"
IsEnabled   = $true
}
New-MgBetaPolicyFeatureRolloutPolicy @MgPolicyFeatureRolloutPolicy
```

5. Find the directoryObject ID for the group to be added to the staged rollout policy. Note the value returned for the *Id* parameter, because it will be used in the next step.

PowerShell

```
Get-MgBetaGroup -Filter "DisplayName eq 'Name of group to be added to
the staged rollout policy'"
```

6. Add the group to the staged rollout policy as shown in the following example. Replace the value in the *-FeatureRolloutPolicyId* parameter with the value returned for the policy ID in step 4 and replace the value in the *-OdataId* parameter with the *Id* noted in step 5. It may take up to 1 hour before users in the group can sign in to Microsoft Entra ID with email as an alternate login ID.

PowerShell

```
New-MgBetaDirectoryFeatureRolloutPolicyApplyToByRef `
   -FeatureRolloutPolicyId "ROLLOUT_POLICY_ID" `
   -OdataId
"https://graph.microsoft.com/v1.0/directoryObjects/{GROUP_OBJECT_ID}"
```

For new members added to the group, it may take up to 24 hours before they can sign in to Microsoft Entra ID with email as an alternate login ID.

Removing groups

To remove a group from a staged rollout policy, run the following command:

PowerShell

```
Remove-MgBetaPolicyFeatureRolloutPolicyApplyToByRef -FeatureRolloutPolicyId
"ROLLOUT_POLICY_ID" -DirectoryObjectId "GROUP_OBJECT_ID"
```

Removing policies

To remove a staged rollout policy, first disable the policy then remove it from the system:

PowerShell

```
Update-MgBetaPolicyFeatureRolloutPolicy -FeatureRolloutPolicyId
"ROLLOUT_POLICY_ID" -IsEnabled:$false
Remove-MgBetaPolicyFeatureRolloutPolicy -FeatureRolloutPolicyId
"ROLLOUT_POLICY_ID"
```

Test user sign-in with an email address

To test that users can sign in with email, go to https://myprofile.microsoft.com and sign in with a non-UPN email, such as `balas@fabrikam.com`. The sign-in experience should look and feel the same as signing-in with the UPN.

Troubleshoot

If users have trouble signing in with their email address, review the following troubleshooting steps:

1. Make sure it's been at least 1 hour since email as an alternate login ID was enabled. If the user was recently added to a group for staged rollout policy, make sure it's been at least 24 hours since they were added to the group.

2. If using HRD policy, confirm that the Microsoft Entra ID *HomeRealmDiscoveryPolicy* has the *AlternateIdLogin* definition property set to *"Enabled": true* and the *IsOrganizationDefault* property set to *True*:

   PowerShell

   ```
   Get-MgBetaPolicyHomeRealmDiscoveryPolicy | Format-List *
   ```

   If using staged rollout policy, confirm that the Microsoft Entra ID *FeatureRolloutPolicy* has the *IsEnabled* property set to *True*:

```
PowerShell

Get-MgBetaPolicyFeatureRolloutPolicy
```

3. Make sure the user account has their email address set in the *ProxyAddresses* attribute in Microsoft Entra ID.

Sign-in logs

You can review the sign-in logs in Microsoft Entra ID for more information. Sign-ins with email as an alternate login ID will emit `proxyAddress` in the *Sign-in identifier type* field and the inputted username in the *Sign-in identifier* field.

Conflicting values between cloud-only and synced users

Within a tenant, a cloud-only user's UPN may take on the same value as another user's proxy address synced from the on-premises directory. In this scenario, with the feature

enabled, the cloud-only user will not be able to sign in with their UPN. Here are the steps for detecting instances of this issue.

1. Open a PowerShell session as an administrator, then install Microsoft Graph by using the Install-Module cmdlet:

   PowerShell

   ```
   Install-Module Microsoft.Graph.Authentication
   ```

   If prompted, select **Y** to install NuGet or to install from an untrusted repository.

2. Connect to Microsoft Graph:

   PowerShell

   ```
   Connect-MgGraph -Scopes "User.Read.All"
   ```

3. Get affected users.

   PowerShell

   ```
   # Get all users
   $allUsers = Get-MgUser -All

   # Get list of proxy addresses from all synced users
   $syncedProxyAddresses = $allUsers |
       Where-Object {$_.ImmutableId} |
       Select-Object -ExpandProperty ProxyAddresses |
       ForEach-Object {$_ -Replace "smtp:", ""}

   # Get list of user principal names from all cloud-only users
   $cloudOnlyUserPrincipalNames = $allUsers |
       Where-Object {!$_.ImmutableId} |
       Select-Object -ExpandProperty UserPrincipalName

   # Get intersection of two lists
   $duplicateValues = $syncedProxyAddresses |
       Where-Object {$cloudOnlyUserPrincipalNames -Contains $_}
   ```

4. To output affected users:

   PowerShell

   ```
   # Output affected synced users
   $allUsers |
       Where-Object {$_.ImmutableId -And ($_.ProxyAddresses | Where-Object
   {($duplicateValues | ForEach-Object {"smtp:$_"}) -Contains $_}).Length
   ```

```
-GT 0} |
    Select-Object ObjectId, DisplayName, UserPrincipalName,
ProxyAddresses, ImmutableId, UserType

# Output affected cloud-only users
$allUsers |
    Where-Object {!$_.ImmutableId -And $duplicateValues -Contains
$_.UserPrincipalName} |
    Select-Object ObjectId, DisplayName, UserPrincipalName,
ProxyAddresses, ImmutableId, UserType
```

5. To output affected users to CSV:

PowerShell

```
# Output affected users to CSV
$allUsers |
    Where-Object {
        ($_.ImmutableId -And ($_.ProxyAddresses | Where-Object
{($duplicateValues | ForEach-Object {"smtp:$_"}) -Contains $_}).Length
-GT 0) -Or
        (!$_.ImmutableId -And $duplicateValues -Contains
$_.UserPrincipalName)
    } |
    Select-Object ObjectId, DisplayName, UserPrincipalName,
@{n="ProxyAddresses"; e={$_.ProxyAddresses -Join ','}},
@{n="IsSyncedUser"; e={$_.ImmutableId.Length -GT 0}}, UserType |
    Export-Csv -Path .\AffectedUsers.csv -NoTypeInformation
```

Next steps

To learn more about hybrid identity, such as Microsoft Entra application proxy or Microsoft Entra Domain Services, see Microsoft Entra hybrid identity for access and management of on-prem workloads.

For more information on hybrid identity operations, see how password hash sync or pass-through authentication synchronization work.

Feedback

Was this page helpful? Yes No

Provide product feedback

Close your account, cancel your subscription, end your trial

Article • 03/06/2025

You or your admin have options to close your account, cancel your subscription, or end your trial. Each of these actions has a different set of procedures and considerations.

End user

Most canceling, closing, and expiry is handled by an administrator. But there are some tasks that you can do as an end user. Being able to do these tasks yourself is possible if you signed up as an individual and your account or subscription isn't managed by your organization.

Cancel a Power BI license trial

If you signed up for a trial of a paid Power BI license, you can cancel that trial. Open your Account manager and select **Cancel trial**.

Cancel your license account

If you signed up for Power BI as an individual, and you don't want to use Power BI any longer, close your Power BI account. After you close your account, you can't sign in to Power BI. Also, as it states in the data retention policy in the Power BI Service Agreement, Power BI deletes any customer data you uploaded or created.

1. In Power BI, select the gear icon in the upper right, then select **Settings**.

2. On the **General** tab, select **Close Account**.

3. Select a reason for closing the account. You can also provide further information. Then select **Close account**.

4. Confirm that you want to close your account.

   You should see a confirmation that Power BI closed your account. You can reopen your account from here if necessary.

If your organization signed you up for Power BI, contact your admin. Ask them to unassign the license from your account.

Cancel a Fabric capacity trial that you started

If you signed up for a Fabric trial capacity, you can cancel that trial. Open your Account manager and select **Cancel trial**.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Power BI for US government customers

Article • 01/17/2025

This article is for US government customers who are deploying Power BI as part of a Microsoft 365 Government plan. Government plans are designed for the unique needs of organizations that must meet US compliance and security standards.

The Power BI service that's designed for US government customers differs from the commercial version of the Power BI service. These feature differences and capabilities are described in the following sections.

> **Note**
>
> Before you can get a Power BI US government subscription and assign licenses to users, you have to enroll in a Microsoft 365 Government plan. If your organization already has a Microsoft 365 Government plan, skip ahead to Buy a Power BI Pro subscription for government customers.

Government cloud instances

If you're a new customer, you have to validate your organization's eligibility before you can sign up for a Microsoft 365 Government plan. Get started by completing the Microsoft 365 for Government eligibility validation form.

Microsoft 365 provides different environments for government agencies to meet varying compliance requirements. To ensure that you're selecting the right plan for your organization, consult the Microsoft 365 US Government service description for each environment:

- Microsoft 365 Government Community Cloud (GCC) is designed for federal, state, and local government.
- Microsoft 365 Government Community Cloud High (GCC High) is designed for federal agencies, defense industry, aerospace industry, and other organizations that hold controlled unclassified information. This environment is suited for national/regional security organizations and companies that have International Traffic in Arms Regulations (ITAR) data or Defense Federal Acquisition Regulations Supplement (DFARS) requirements.
- The Microsoft 365 DoD environment is designed exclusively for the US Department of Defense.

> **Note**
>
> If you've already deployed Power BI to a commercial environment and want to migrate to the US government cloud, you'll need to add a new Power BI Pro or Premium Per User (PPU) subscription to your Microsoft 365 Government plan. Next, replicate the commercial data to the Power BI service for US government, remove commercial license assignments from user accounts, and then assign a Power BI Pro government license to the user accounts.

Buy a Power BI Pro subscription for government customers

After you deploy Microsoft 365, you can add a Power BI Pro subscription. To buy the Power BI Pro government service, follow the guidance in Enroll your US government organization. Buy enough licenses for all the users who need to use Power BI, and then assign the licenses to individual user accounts.

> **Important**
>
> Power BI US Government isn't available as a *Free* license. If you've purchased Power BI Premium, you don't have to assign licenses to users to allow them to consume content published to a Premium capacity. For all other access, including access to the admin portal and the ability to publish content to the Premium capacity, each user must be assigned a *Pro* or *Premium Per User (PPU)* license. If a user account has been assigned a Free license, the user is authorized to access only the commercial cloud and will encounter authentication and access issues.
>
> To review the differences between license types, see **Power BI service features by license type**.

Sign in to Power BI for US government

The URLs for connecting to Power BI differ for government users and commercial users. To sign in to the correct Power BI version, use one of the following URLs:

- **Commercial version**: https://app.powerbi.com
- **GCC**: https://app.powerbigov.us
- **GCC High**: https://app.high.powerbigov.us
- **DoD**: https://app.mil.powerbigov.us

Your account might be set up in more than one cloud. If your account is set up that way, when you sign in to Power BI Desktop, you can choose which cloud to connect to.

> **Tip**
>
> In this video, Using Power BI Desktop in government clouds, Technical Specialist Steve Winward shows how you can apply a registry setting to go directly to the right cloud endpoint for your environment. The registry key settings to bypass the global discovery endpoint are shared on GitHub.

Allow connections to Power BI

To use the Power BI service, you must allow connections to required endpoints on the internet. These destinations have to be reachable to enable communication between your own network, Power BI, and other dependent services.

The following table lists the required endpoints to add to your allowlist to enable connection to the Power BI service for general site usage. These endpoints are unique to the US government cloud. The Power BI service requires only Transmission Control Protocol (TCP) port 443 to be opened for the listed endpoints.

The endpoints for getting data, dashboard and report integration, Power BI visuals, and other optional services aren't unique to the US government cloud.

To add these URLs to your allowlist also, see Add Power BI URLs to your allowlist.

Authentication, identity, and administration for Power BI depend on connectivity to Microsoft 365 services. You also have to connect to Microsoft 365 to view audit logs. To identify the endpoints for these services, see "Microsoft 365 integration" in the following table:

Power BI URLs for general site usage

Expand table

Purpose	Destination
Back-end APIs	**GCC**: api.powerbigov.us **GCC High**: api.high.powerbigov.us **DoD**: api.mil.powerbigov.us
Back-end APIs	**GCC**: *.analysis.usgovcloudapi.net **GCC High**: *.high.analysis.usgovcloudapi.net

Purpose	Destination
	DoD: *.mil.analysis.usgovcloudapi.net
Back-end APIs	**All**: *.pbidedicated.usgovcloudapi.net
Content Delivery Network (CDN)	**GCC**: gov.content.powerapps.us **GCC High**: high.content.powerapps.us **DoD**: mil.content.powerapps.us
Microsoft 365 integration	**GCC**: Worldwide endpoints **GCC High**: US Government GCC High endpoints **DoD**: US Government DOD endpoints
Portal	**GCC**: *.powerbigov.us **GCC High**: *.high.powerbigov.us **DoD**: *.mil.powerbigov.us
Manage gateways, connections, and data policies (preview)	**GCC**: gatewayadminportal-gov.azure.us **GCC High**: gatewayadminportal-high.azure.us **DoD**: gatewayadminportal-mil.azure.us
Service telemetry	**All**: dc.services.visualstudio.us
Informational messages (optional)	**All**: arc.msn.com

Connect government and global Azure cloud services

Azure is distributed across multiple clouds. By default, you can enable firewall rules to open a connection to a cloud-specific instance, but cross-cloud networking is different. To communicate between services in the public cloud and services in the Government Community Cloud, you have to configure specific firewall rules. For example, if you want to access public cloud instances of an SQL database from your government cloud deployment of Power BI, you need a firewall rule in the SQL database. Configure specific firewall rules for SQL databases to allow connections to the Azure Government Cloud for the following datacenters:

- USGov Iowa
- USGov Virginia
- USGov Texas
- USGov Arizona

- US DoD East
- US DoD Central

To get the US government cloud IP ranges, download the Azure IP Ranges and Service Tags – US Government Cloud file. Ranges are listed for both Power BI and Power Query.

For more information about Microsoft Azure Government cloud services, see Azure Government documentation.

To set up firewalls for SQL databases, see Create and manage IP firewall rules.

Cross-Cloud B2B

You can use Power BI's B2B capabilities across Microsoft Azure clouds by configuring Microsoft cloud settings for B2B collaboration. Read Microsoft cloud settings to learn how to establish mutual B2B collaboration between the Microsoft Azure global cloud and Microsoft Azure Government.

There are some limitations to the B2B experience that you should be aware of:

- Guest users may already have a Power BI license that was assigned to them through their own organization. But “Bring your own license” doesn’t work across different Microsoft Azure clouds. A new license has to be assigned to these guest users by the provider tenant.

- New external users can be invited to the organization through Power BI sharing, permissions, and subscription experiences.

- On the Home page, the **From external orgs** tab won't list content shared from other clouds.

Power BI feature availability

To accommodate the requirements of government cloud customers, government plans differ from commercial plans in some respects. Our goal is to make all features available in government clouds within 30 days of general availability. In a few cases, underlying dependencies prevent us from making a feature available.

The following table lists features of Power BI that aren't yet available in a particular government environment or that are available with limited functionality. The table uses the following keys:

Expand table

Key	Description
✅	The feature is available in the environment, and any exceptions are defined in footnotes.
⊗	The feature isn't available in the environment, and we don't have an estimated time frame for delivery.

If a release is planned for an environment, we include the quarter of estimated availability.

> **Note**
>
> US Government customers who operate in an air-gapped cloud should consult feature parity documentation in that environment to discover feature availability.

Expand table

Feature	GCC	GCC High	DoD
Azure B2B collaboration between government and commercial cloud[1]	✅	✅	✅
Template apps[2]	✅	✅	✅
Embed in SharePoint Online by using the Power BI web part	✅	✅	✅
Data Loss Prevention policies	✅	✅	✅
Data Protection (MIP labels)	✅	✅	✅
Dataflows - Direct Query	✅	✅	Not planned
Dataflows - SQL Compute engine optimization	✅	✅	Not planned
Datamarts	Not planned	Not planned	Not planned
Power BI tab in Teams	✅	✅	✅
Large models	✅	✅	Not planned

Feature	GCC	GCC High	DoD
Call Quality Data Connector	✓ [3]	✓ [3]	✓ [3]
Bring your own storage (Azure Data Lake Gen 2)	✗	✓	✓
Autoscale	✗	✓	✓
Azure Maps	✗	✗	✗

[1] Although B2B collaboration is available for GCC, external users must be issued a license in that environment. Commercial cloud licenses aren't valid in GCC. For more information about known limitations with B2B collaboration for US government, see Compare Azure Government and global Azure.

[2] Because marketplace apps aren't available to US government cloud instances, template apps are limited to private and organizational apps.

[3] Call Quality Data Connector must be installed on an on-premises data gateway for compatibility with Power BI service. If the connector is not installed on an on-premises data gateway, usage is restricted to Power BI Desktop only.

For more information about support for Power BI components in Power Apps, see Power Apps US Government feature limitations.

Related content

- Article: Sign up for Power BI for US government
- Article: Microsoft Power Apps US Government
- Article: Power Automate US Government
- Video: Power BI US Government demo

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Enroll your US government organization in the Power BI service

Article • 12/12/2023

This article describes the US government enrollment process for the Power BI service. The process is intended for administrators who have authority to sign up their US government organization for Power BI. If you're not an admin, contact your administrator about getting a subscription to Power BI for US government organizations.

The Power BI service has a special US government version, which is part of the Microsoft 365 Government plans. The enrollment process that this article describes is different from the process for the commercial version of the Power BI service.

For more information, see Power BI for United States government customers.

> **Important**
>
> To maintain continuity of data access, US government customers must complete an explicit request for onboarding the following US government clouds:
>
> - Microsoft 365 Government Community Cloud (GCC)
> - Microsoft 365 Government Community Cloud High (GCC High)
> - Microsoft 365 Department of Defense (DoD)

Select the right sign-up process for your US government organization

Microsoft 365 provides different environments for government agencies to meet varying compliance requirements. The Microsoft 365 Government Community Cloud (GCC) is designed for federal, state, and local government. If your organization is in GCC, use the steps in this article to sign up and purchase services.

> **Important**
>
> Don't follow these instructions if you belong to one of the following clouds:

- **Microsoft 365 Government Community Cloud High (GCC High)**
- **Microsoft 365 Department of Defense (DoD)**

To purchase the Power BI service for these US government clouds, see **How do I buy Microsoft 365 Government?** and work with your reseller to ensure new services are properly associated with your tenant.

After you sign up for the Power BI service for the US government, work with your account team to start the allowlist process described in this article. That step is needed to fully enable your organization in the government community cloud.

Sign up for a new Microsoft 365 Government plan

If your organization is new to the government cloud community, get a Microsoft 365 Government plan with the following steps:

After this process is complete, follow the steps for existing Microsoft 365 Government customers to add a Power BI subscription.

> **Note**
>
> These steps should be performed by the global administrator.

1. Go to Microsoft 365 Government plans.
2. Select **Get started with a free trial**.
3. Under **My Organization is**, select your organization type.

4. Enter your business address and agree to the **Office 365 terms and conditions**.

5. Select **Submit** to start the onboarding process. Your Microsoft representative or partner can help with any questions.

Add Power BI to a Microsoft 365 Government plan

If your organization already has a Microsoft 365 Government plan, add a Power BI subscription.

1. Sign in to the Microsoft 365 admin center by using a global admin or billing admin account.

2. On the navigation menu, select **Billing**, and then select **Purchase services**.

3. Search or scroll to locate the Power BI Pro Government offer, and select **Buy Now**.

4. Complete your order.

5. Assign licenses to user accounts.

More sign-up information

Before you can use the Power BI service for the US government, you have to work with your Microsoft account team to have your organization added to the allowlist. The allowlist process is used by the Power BI engineering team to move customers from the commercial cloud environment into the secure, government community cloud. This step ensures that features available in the US government cloud work as expected.

To start the allowlist process, contact your Microsoft account team for assistance. Only administrators can request to be added to the allowlist. The process takes about three weeks. During this time, the Power BI engineering team makes appropriate changes to ensure your tenant operates properly in the US government cloud.

Next steps

Overview of Power BI for US government

How do I buy Microsoft 365 Government?

Power BI - operated by 21Vianet in China

Article • 04/03/2024

Microsoft Power BI service operated by 21Vianet is designed to comply with regulatory requirements in China. The services are a physically separated environment of cloud services operated and transacted currently by a local operator, Shanghai Blue Cloud Technology Co., Ltd ("21Vianet"). This operator is a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd. located in China.

Power BI feature availability

To accommodate the requirements of regional cloud customers, Power BI operated by 21Vianet plans differ from commercial plans in some respects. We attempt to make features available within 30 days of general availability. However in some cases, underlying dependencies prevent a feature from being available.

The following table lists features of Power BI that are **not** yet available in the Power BI operated by 21Vianet environment, or that are available with limited functionality.

Expand table

Product area	Feature or scenario	Commercial cloud status	21Vianet availability	More information
Power BI	Purview integration with Power BI	Generally available	Not available	
Power BI	Using Azure ExpressRoute to integrate an on-premises gateway	Generally available	Not available	Azure ExpressRoute for Office 365 isn't supported in the 21Vianet environment.
Power BI	Template app marketplace	Generally available	Not available	AppSource isn't available in China.
Power BI	Datamart	Public preview	Not available	
Power BI and Office	Teams - embed interactive Power BI report	Generally available	Not available	
Power BI scalability	Large models	Generally available	Generally available in China	

Product area	Feature or scenario	Commercial cloud status	21Vianet availability	More information
			East 2 and China North 2 only	
Power BI	Scorecards	Generally available	Not available for 21Vianet multi-geo capacities	

Related content

To learn more about Power BI operated by 21Vianet in China, see the following resources:

- Azure China 21Vianet
- Support site for 21Vianet (in Chinese)
- Power BI for US government customers

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Move between regions

Article • 02/07/2024

> **Important**
>
> At this time, we only offer the tenant migration service to customers with a P (Premium) SKU and F64 and above SKU. The location selected during sign-up determines your default data region. 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 Microsoft support to manage the migration for you.

> **Caution**
>
> This article describes how to request a move between regions and keep Power BI or 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 administration roles. We can't help identify your global administrator for you. Look for global administrator role holders in Microsoft 365 or Microsoft Entra ID 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.
- You must 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 some preparation steps you need to take.

Awareness

- **The end-to-end migration process might take up to six months**. We prioritize service reliability and deployment schedules can change, so we might need to reschedule during migration at any time. We can't guarantee successful migration due to inconsistent data or bugs.
- During the migration process, it's possible to encounter unforeseen issues that might result in multiple failures. Allow for multiple attempts to ensure a successful migration.
- Migration requires about six hours of down time. During migration, users can't access Power BI and an error message similar to the one shown in the following screenshot is displayed. 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 are deleted before migration starts. After the migration, PPU capacity is 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 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.
- Cross region workspace migration does not support semantic models in large model storage mode. To migrate a semantic model in large-model storage mode, please use backup restore. 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)
- If Fabric Metadata is linked to the Purview Data Map, it continues to be stored in the home region of the tenant. You can choose to delete the assets manually by navigating to Microsoft Purview and following the steps described here: Asset management in the Microsoft Purview Data Catalog.

Preparation steps

Our support team works 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.
  - To avoid conflicts during migration, delete any gateways that are already in the target region.
- 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.

- **All Fabric items have to be deleted individually** before deleting the capacity or workspace. Deleting the capacity or workspaces does not delete the Fabric items immediately.

- All Fabric trial capacities have to be deleted before the migration. To delete Fabric trial capacities, **the users who own** the trial capacity need to cancel the trial from the Me profile at least one and a half days before the migration.

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 or Fabric Admin & Management
   - Tell us what you need help with: **Move to a different region**

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

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

Expand table

Information needed	How to find the information
Tenant object ID	How to find your Microsoft Entra 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.

Information needed	How to find the information
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 reviews the submitted information, including your tenant object ID, current data region, and target data region. After details are confirmed, we 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 copies your data to the new region. Power BI isn't available to users during the move.

After the region move

When migration is complete, you can access Power BI in about 20-30 minutes. Support contacts 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. Recreate push datasets if they were deleted. 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. Update the connection string or redownload the ODC connection for datasets that didn't refresh. Excel workbooks that use the Analyze in Excel feature might fail to refresh. Follow the steps in Start in Power BI with Analyze in Excel if necessary.

5. Regenerate embedded links that didn't reconnect. 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 was 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 so that I don't 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 Microsoft Entra ID?

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. A global administrator must request the operation.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

What is Power BI Premium?

Article • 11/21/2024

This article describes Power BI Premium operations and considerations, to view a high level description of how Microsoft Fabric works, see Microsoft Fabric concepts and licenses.

Power BI Premium provides enhancements to Power BI, and a comprehensive portfolio of Premium features. The following table lists some of the Premium enhancements.

Expand table

Enhancement	Details
Purchase Premium for individuals in your organization	See Power BI Premium Per User (PPU).
Improved metrics	Capacity performance depends only on the amount of CPU usage. Metrics can be easily understood using the Microsoft Fabric Capacity Metrics app.
Autoscale	An optional feature that prevents slowdowns caused by throttling on overloaded capacities. When enabled, if the load on the capacity exceeds the capacity limits, autoscale automatically adds one v-core at a time for 24-hour periods. Additional v-cores are charged to your Azure subscription on a pay-as-you-go basis.

Capacities and SKUs

Capacity is a dedicated set of resources reserved for exclusive use. It offers dependable, consistent performance for your content.

Each capacity offers a selection of SKUs, and each SKU provides different resource tiers for computing power. The type of SKU you require, depends on the type of solution you wish to deploy.

Expand table

SKU	Capacity Units (CU)	Power BI SKU	Power BI v-cores
F2	2	N/A	N/A
F4	4	N/A	N/A
F8	8	EM1/A1	1
F16	16	EM2/A2	2
F32	32	EM3/A3	4

SKU	Capacity Units (CU)	Power BI SKU	Power BI v-cores
F64	64	P1/A4	8
F128	128	P2/A5	16
F256	256	P3/A6	32
F512[1]	512	P4/A7	64
F1024[1]	1,024	P5/A8	128
F2048[1]	2,048	N/A	N/A

[1] These SKUs aren't available in all regions. To request using these SKUs in regions where they're not available, contact your Microsoft account manager.

Subscriptions and licensing

Power BI Premium is a tenant-level Microsoft 365 subscription, available in two SKU (Stock-Keeping Unit) families.

Expand table

	P	EM
Range	P1-P5	EM1-EM3
Use	Enterprise features and embedding	Organizational embedding (embed for your organization)
Commitment	Monthly or yearly	Yearly
Billing	Monthly	Monthly
Additional information	Includes a license to install Power BI Report Server on-premises	EM1 and EM2 SKUs are available only through volume licensing plans. You can't purchase them directly.

Workspaces

Workspaces reside within capacities. Each Power BI user has a personal workspace known as *My Workspace*. Additional workspaces known as *workspaces* can be created to enable collaboration. By default, workspaces, including personal workspaces, are created in the shared capacity. When you have Premium capacities, both My Workspaces and workspaces can be assigned to Premium capacities.

Capacity administrators automatically have their My workspaces assigned to Premium capacities.

Semantic model SKU limitation

With *Power BI Premium* and Power BI Embedded, there are memory limits and other constraints for each SKU listed in the table below.

Expand table

SKU	Max memory (GB)[1, 2]	Max concurrent DirectQuery connections (per semantic model)[1]	Max DirectQuery parallelism[3]	Live connection (per second)[1]	Max memory per query (GB)[1]	Model refresh parallelism	Direct Lake rows per table (in millions)[1, 4]	Max Direct Lake model size on OneLake (GB)[1, 4]
F2	3	5	1	2	1	1	300	10
F4	3	5	1	2	1	2	300	10
F8	3	10	1	3.75	1	5	300	10
F16	5	10	1	7.5	2	10	300	20
F32	10	10	1	15	5	20	300	40
F64	25	50	4 - 8	30	10	40	1,500	Unlimited
F128	50	75	6 - 12	60	10	80	3,000	Unlimited
F256	100	100	8 - 16	120	10	160	6,000	Unlimited
F512	200	200	10 - 20	240	20	320	12,000	Unlimited
F1024	400	200	12 - 24	480	40	640	24,000	Unlimited
F2048	400	200		960	40	1,280	24,000	Unlimited

[1] The Microsoft Fabric Capacity Metrics app doesn't currently expose these metrics.

[2] The *Max memory (GB)* column represents an upper bound for the semantic model size. However, an amount of memory must be reserved for operations such as refreshes and queries on the semantic model. The maximum semantic model size permitted on a capacity might be smaller than the numbers in this column.

[3] DirectQuery parallelism can improve your query response times. The lower number indicates the default maximum number of queries that can be processed at the same time. The higher number indicates the maximum number of queries that can be processed at the same time. To change the default use the Model.MaxParallelismPerQuery property.

[4] These limits apply to Direct Lake tables and models, and are guardrails that affect fallback to DirectQuery. Direct Lake semantic models have additional constraints that are based on SKUs, as listed in fallback.

Semantic model memory usage

Semantic model operations such as queries are subject to individual memory limits. To illustrate the restriction, consider a semantic model with an in-memory footprint of 1 GB, and a user initiating an on-demand refresh while interacting with a report based on the same semantic model. Three separate actions determine the amount of memory attributed to the original semantic model, which may be larger than two times the semantic model size. The total amount of memory used by one Power BI item can't exceed the SKU's *Max memory per semantic model* allocation.

- **Loading the semantic model** - The first action is loading the semantic model into the memory.
- **Refreshing the semantic model** - The second action is refreshing the semantic model after it's loaded into the memory. The refresh operation will cause the memory used by the semantic model to more than double, because in addition to the memory used by the refresh operation, the original copy of data remains available for active queries while another copy is being processed by the refresh. Once the refresh transaction commits, the memory footprint is reduced.
- **Interacting with the report** - The third action is caused by the user's interaction with the report. During the semantic model refresh, report interactions will execute DAX queries. Each DAX query consumes a certain amount of temporary memory required to produce the results. Each query may consume a different amount of memory. The memory used to query the semantic model is added to the memory needed to load the semantic model, and refresh it.

Refreshes

Power BI Premium and Power BI Embedded don't require cumulative memory limits, and therefore concurrent semantic model refreshes don't contribute to resource constraints. However, refreshing individual semantic models is governed by existing capacity memory and CPU limits, and the model refresh parallelism limit for the SKU, as described in Capacities and SKUs.

You can schedule and run as many refreshes as required at any given time, and the Power BI service will run those refreshes at the time scheduled as a best effort.

Monitoring

When monitoring Power BI Premium and Power BI Embedded, you only need to take into consideration one aspect: *how much CPU your capacity requires to serve the load at any moment*. To monitor your capacity, use the Microsoft Fabric Capacity Metrics app app.

To install the app, see Install the Microsoft Fabric capacity metrics app. You can learn how to use the app in the article Microsoft Fabric Capacity Metrics.

Here's what happens when you exceed your CPU limit per the SKU size you purchased:

- **Power BI Premium** - If enabled, autoscale kicks in. If autoscale isn't enabled, your capacity throttles its interactive operations.
- **Power BI Embedded** - Your capacity throttles its interactive operations. To autoscale in Power BI Embedded, see Autoscaling in Power BI Embedded.

Paginated reports

When using *Power BI Premium* and Power BI Embedded, Power BI paginated reports benefit from the architectural and engineering improvements reflected in Power BI Premium.

- **Memory** - There's no memory management for Paginated reports.
- **SKU availability** - Paginated reports running on Power BI Premium can run reports across all available embedded and Premium SKUs, including the EM1-EM3 and A1-A3 SKUs. Billing is calculated per CPU hour, across a 24-hour period.
- **Enhanced security and code isolation** - Code isolation occurs at a per-user level, rather than at a per-capacity level.

Dataflows Gen1 and Gen2

Each SKU can run a set number of Dataflows parallel tasks, as listed in this table.

Expand table

Fabric SKU	Dataflow Gen1 parallel tasks	Dataflow Gen2 parallel tasks
F2	2	96
F4	2	96
F8	4	96
F16	8	96
F32	16	96
F64	32	384
F128	64	384
F256	64	384
F512	64	1536

Fabric SKU	Dataflow Gen1 parallel tasks	Dataflow Gen2 parallel tasks
F1024	64	1536
F2048	64	1536

To learn about Dataflow Gen2, see Getting from Dataflow Generation 1 to Dataflow Generation 2.

Considerations and limitations

The following known limitations currently apply to Power BI Premium.

- **Rendering visuals** - There's a 225-second limitation for rendering Power BI visuals. Visuals that take longer to render, will be timed-out and won't display.
- **Throttling** - Throttling can occur in Power BI Premium capacities. Concurrency limits are applied per session. An error message will appear when too many operations are being processed concurrently. To mitigate throttling, you can use autoscale. When autoscale is enabled, if CPU consumption exceeds the additional limits, throttling will still take place. To read more about throttling in Fabric, see The Fabric throttling policy.
- **Client library version** - Client applications and tools that connect to and work with semantic models on Premium capacities through the XMLA endpoint require Analysis Services client libraries. Most client applications and tools install the most recent client libraries with regular updates, so manually installing the client libraries isn't usually necessary. Regardless of the client application or tool version, the following minimum client library versions are required.

  Expand table

Client Library	Version
MSOLAP	15.1.65.22
AMO	19.12.7.0
ADOMD	19.12.7.0

  In some cases, manually installing the most recent client libraries may be necessary to reduce potential connection and operation errors. To learn more about verifying existing installed client library versions and manually installing the most recent versions, see Analysis Services client libraries.
- **Semantic models compatibility** - Some semantic models are incompatible with the Power BI service modern infrastructure:
  - Semantic models created in Power BI service from CSV files.

- Semantic models in the admin monitoring workspace and usage metrics models.
- Semantic models that still use 1103 compatibility level.
- Push semantic models.
- Semantic models that use deprecated features such as content packs.

Related content

- Power BI Premium Per User
- Managing Premium capacities
- Power BI Embedded

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Power BI Premium features

Article • 01/20/2025

This article lists the main Power BI Premium features. Most of the features apply to all the Power BI Premium licenses, including Premium Per User (PPU) and Power BI Embedded. When a feature only works with a specific license, the required license is indicated in the *description* field. If no license is listed, the feature works with any license.

Power BI Premium feature list

Expand table

Feature	Description
Asynchronous refresh	Perform asynchronous data-refresh operations
Automatic aggregations	Optimize DirectQuery datasets
Autoscale	Automatically add compute capability when your capacity is overloaded Available for Premium only, excluding EM SKUs
Backup and restore	Backup and restore data using XMLA endpoints
Bring your own key (BYOK)	Use your own keys to encrypt data Available for Premium and Embedded
Dataflows	• Perform in-storage computations • Optimize the use of dataflows • Use incremental refresh with dataflows • Reference other dataflows
Datamarts	Self-service solution enabling users to store and explore data that's loaded in a fully managed database
Deployment pipelines	Manage the lifecycle of your Power BI content
Direct Lake (preview)	Connect directly to your data lake without having to import its data
DirectQuery with dataflows	Connect directly to your dataflow without having to import its data
Hybrid tables	Incremental refresh augmented with real-time data
Insights (preview)	Explore and find insights such as anomalies and trends in your

Feature	Description
	reports
Model size limit	Available memory is set to: *Premium* - The limit of memory footprint of a single Power BI dataset; see the column *Max memory per dataset* in the Capacities and SKUs table *Premium Per User (PPU)* - See Considerations and limitations *Embedded* - See the column *Max memory per dataset* in the SKU memory and computing power table
Multi-geo	Deploy content to data centers in regions other than the home region of your tenant Available for Premium and Embedded
On-demand loading capabilities for large models	Improve report load time by loading datasets to memory on demand
Power BI Report Server	On-premises report server Available for Premium only, excluding EM SKUs
Refresh rate	The ability to refresh more than eight times a day
Query caching	Speed up reports by using local caching
Storage	Manage data storage
Unlimited content sharing	Share Power BI content with anyone Available for Premium only, excluding EM SKUs
Virtual network data gateway (preview)	Connect from Microsoft Cloud to Azure using a virtual network (VNet)
XMLA read/write	Enable XMLA endpoint

Related content

- What is Power BI Premium?

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Microsoft Fabric security fundamentals

Article • 01/15/2024

This article presents a big-picture perspective of the Microsoft Fabric security architecture by describing how the main security flows in the system work. It also describes how users authenticate with Fabric, how data connections are established, and how Fabric stores and moves data through the service.

The article is primarily targeted at Fabric administrators, who are responsible for overseeing Fabric in the organization. It's also relevant to enterprise security stakeholders, including security administrators, network administrators, Azure administrators, workspace administrators, and database administrators.

Fabric platform

Microsoft Fabric is an all-in-one analytics solution for enterprises that covers everything from data movement to data science, real-time analytics, and business intelligence (BI). The Fabric platform comprises a series of services and infrastructure components that support the common functionality for all Fabric experiences. Collectively, they offer a comprehensive set of analytics experiences designed to work together seamlessly. Experiences include Lakehouse, Data Factory, Fabric Data Engineering, Fabric Data Warehouse, Power BI, and others.

With Fabric, you don't need to piece together different services from multiple vendors. Instead, you benefit from a highly integrated, end-to-end, and easy-to-use product that's designed to simplify your analytics needs. Fabric was designed from the outset to protect sensitive assets.

The Fabric platform is built on a foundation of software as a service (SaaS), which delivers reliability, simplicity, and scalability. It's built on Azure, which is Microsoft's public cloud computing platform. Traditionally, many data products have been platform as a service (PaaS), requiring an administrator of the service to set up security, compliance, and governance for each service. Because Fabric is a SaaS service, many of these features are built into the SaaS platform and require no setup or minimal setup.

Architectural diagram

The architectural diagram below shows a high-level representation of the Fabric security architecture.

The architectural diagram depicts the following concepts.

1. A user uses a browser or a client application, like Power BI Desktop, to connect to the Fabric service.

2. Authentication is handled by Microsoft Entra ID, previously known as Azure Active Directory, which is the cloud-based identity and access management service that authenticates the user or service principal and manages access to Fabric.

3. The web front end receives user requests and facilitates sign-in. It also routes requests and serves front-end content to the user.

4. The metadata platform stores tenant metadata, which can include customer data. Fabric services query this platform on demand in order to retrieve authorization information and to authorize and validate user requests. It's located in the tenant home region.

5. The back-end capacity platform is responsible for compute operations and for storing customer data, and it's located in the capacity region. It leverages Azure core services in that region as necessary for specific Fabric experiences.

Fabric platform infrastructure services are multitenant. There is logical isolation between tenants. These services don't process complex user input and are all written in managed code. Platform services never run any user-written code.

The metadata platform and the back-end capacity platform each run in secured virtual networks. These networks expose a series of secure endpoints to the internet so that they can receive requests from customers and other services. Apart from these endpoints, services are protected by network security rules that block access from the public internet. Communication within virtual networks is also restricted based on the privilege of each internal service.

The application layer ensures that tenants are only able to access data from within their own tenant.

Authentication

Fabric relies on Microsoft Entra ID to authenticate users (or service principals). When authenticated, users receive access tokens from Microsoft Entra ID. Fabric uses these tokens to perform operations in the context of the user.

A key feature of Microsoft Entra ID is conditional access. Conditional access ensures that tenants are secure by enforcing multifactor authentication, allowing only Microsoft Intune enrolled devices to access specific services. Conditional access also restricts user locations and IP ranges.

Authorization

All Fabric permissions are stored centrally by the metadata platform. Fabric services query the metadata platform on demand in order to retrieve authorization information and to authorize and validate user requests.

For performance reasons, Fabric sometimes encapsulates authorization information into *signed tokens*. Signed tokens are only issued by the back-end capacity platform, and they include the access token, authorization information, and other metadata.

Data residency

In Fabric, a tenant is assigned to a home metadata platform cluster, which is located in a single region that meets the data residency requirements of that region's geography. Tenant metadata, which can include customer data, is stored in this cluster.

Customers can control where their workspaces are located. They can choose to locate their workspaces in the same geography as their metadata platform cluster, either explicitly by assigning their workspaces on capacities in that region or implicitly by using Fabric Trial, Power BI Pro, or Power BI Premium Per User license mode. In the latter case, all customer data is stored and processed in this single geography. For more information, see Microsoft Fabric concepts and licenses.

Customers can also create Multi-Geo capacities located in geographies (geos) other than their home region. In this case, compute and storage (including OneLake and experience-specific storage) is located in the multi-geo region, however the tenant metadata remains in the home region. Customer data will only be stored and processed in these two geographies. For more information, see Configure Multi-Geo support for Fabric.

Data handling

This section provides an overview of how data handling works in Fabric. It describes storage, processing, and the movement of customer data.

Data at rest

All Fabric data stores are encrypted at rest by using Microsoft-managed keys. Fabric data includes customer data as well as system data and metadata.

While data can be processed in memory in an unencrypted state, it's never persisted to permanent storage while in an unencrypted state.

Data in transit

Data in transit between Microsoft services is always encrypted with at least TLS 1.2. Fabric negotiates to TLS 1.3 whenever possible. Traffic between Microsoft services always routes over the Microsoft global network.

Inbound Fabric communication also enforces TLS 1.2 and negotiates to TLS 1.3, whenever possible. Outbound Fabric communication to customer-owned infrastructure prefers secure protocols but might fall back to older, insecure protocols (including TLS 1.0) when newer protocols aren't supported.

Telemetry

Telemetry is used to maintain performance and reliability of the Fabric platform. The Fabric platform telemetry store is designed to be compliant with data and privacy regulations for customers in all regions where Fabric is available, including the European Union (EU). For more information, see EU Data Boundary Services.

OneLake

OneLake is a single, unified, logical data lake for the entire organization, and it's automatically provisioned for every Fabric tenant. It's built on Azure and it can store any type of file, structured or unstructured. Also, all Fabric items, like warehouses and lakehouses, automatically store their data in OneLake.

OneLake supports the same Azure Data Lake Storage Gen2 (ADLS Gen2) APIs and SDKs, therefore it's compatible with existing ADLS Gen2 applications, including Azure Databricks.

For more information, see Fabric and OneLake security.

Workspace security

Workspaces represent the primary security boundary for data stored in OneLake. Each workspace represents a single domain or project area where teams can collaborate on data. You manage security in the workspace by assigning users to workspace roles.

For more information, see Fabric and OneLake security (Workspace security).

Item security

Within a workspace, you can assign permissions directly to Fabric items, like warehouses and lakehouses. Item security provides the flexibility to grant access to an individual Fabric item without granting access to the entire workspace. Users can set up per item permissions either by sharing an item or by managing the permissions of an item.

Compliance resources

The Fabric service is governed by the Microsoft Online Services Terms and the Microsoft Enterprise Privacy Statement.

For the location of data processing, refer to the *Location of Data Processing* terms in the Microsoft Online Services Terms and to the Data Protection Addendum.

For compliance information, the Microsoft Trust Center is the primary resource for Fabric. For more information about compliance, see Microsoft compliance offerings.

The Fabric service follows the Security Development Lifecycle (SDL), which consists of a set of strict security practices that support security assurance and compliance requirements. The SDL helps developers build more secure software by reducing the number and severity of vulnerabilities in software, while reducing development cost. For more information, see Microsoft Security Development Lifecycle Practices.

Related content

For more information about Fabric security, see the following resources.

- Security in Microsoft Fabric
- Microsoft Fabric end-to-end security scenario
- OneLake security overview
- Microsoft Fabric concepts and licenses

- Questions? Try asking the Microsoft Fabric community.
- Suggestions? Contribute ideas to improve Microsoft Fabric.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Power BI Premium Per User

FAQ

Organizations can use Power BI **Premium Per User** to license Premium features on a per-user basis. Premium Per User (PPU) includes all Power BI Pro license capabilities, and includes features such as XMLA endpoints, AI, and other capabilities only available to Premium subscribers.

The following sections describe using Premium Per User (PPU), administrative considerations, and expectations from a Premium Per User (PPU) license.

> **Note**
>
> This article contains all the information that was previously included in the Premium Per User FAQ article.

Using Premium Per User (PPU)

Premium Per User (PPU) gives organizations a way to license premium features on a per-user basis. PPU includes all Power BI Pro license capabilities, including features like AI, and other capabilities that were only available with a Premium capacity. With a PPU license, you don't need a separate Power BI Pro license because all Pro license capabilities are included.

You can use a Power BI individual trial to try PPU as long as your organization hasn't disabled individual trials with the Allow users to try Power BI paid features tenant setting.

The following table compares the features of Premium Per User (PPU) with Premium capacity:

Expand table

Feature description	Per User	Per Capacity
Model size limit	100 GB[1]	25-400 GB[1, 2]
Refresh rate limit per semantic model	48/day	48/day
AI capabilities (AutoML, Impact Analysis, Cognitive Services)	✓	✓
Advanced dataflows features, such as DirectQuery	✓	✓
Usage-based aggregate optimization	✓	✓
Deployment Pipelines	✓	✓
XMLA endpoint connectivity	✓	✓
Enhanced automatic page refresh	✓	✓
Incremental refresh	✓	✓
Multi-Geo support	X	✓
Unlimited distribution	X	✓
Power BI reports on-premises	X	✓
Bring Your Own Key (BYOK)	✓ *	✓

[1] The Model size limit represents an upper bound for the semantic model size. However, an amount of memory must be reserved for operations such as refreshes and queries on the semantic model. The maximum semantic model size permitted on a capacity might be smaller than the numbers shown here.

[2] Depending on the type of SKU you have. For more details, see Capacities and SKUs.

Note

Premium Per User (PPU) only supports BYOK when it's enabled across the entire tenant.

Some organizations choose to supplement their Premium capacity with Premium Per User (PPU) licenses. However, PPU isn't required to publish content to existing Premium capacities.

Administration of Premium Per User (PPU)

Administrators manage PPU licenses, users, and settings in the **Power BI Admin portal**. Admins can determine which per-user settings are exposed, which users can create PPU workspaces, which workspaces are Premium or Premium Per User, and other settings.

Once a Premium Per User (PPU) license is provisioned in a tenant, its features are available in any workspace where you turn them on.

Unlike Premium capacity settings, PPU licenses don't require memory management or CPU management, similar to how Pro licenses don't require such management. Tenant administrators can select feature settings for PPU licenses, but can't disable specific workloads.

You can move workspaces between Premium Per User (PPU) and Premium capacities as needed. Any such move requires a full refresh of datasets or dataflows in the workspace after you move it back to a Premium capacity. A limited set of APIs enable movement of workspaces, but they don't include actions such as turning off a workload.

Datasets in the *Large Dataset format* in Premium Per User (PPU) won't appear in the user interface.

End user experience

When a workspace is marked as a Premium Per User (PPU) workspace, it displays a diamond icon, as shown in the following image:

A Premium Per User (PPU) license is required to access content in a Premium Per User (PPU) workspace or app. This requirement includes scenarios where users are accessing the content through the XMLA endpoint, Analyze in Excel, Composite Models, and so on. You can give access to a workspace to users who don't have a PPU license. If they're eligible, they'll get a prompt for a trial license. If they aren't eligible, an admin must assign a license.

The following table describes who can access content with PPU.

		Users with this license type can view/access the content		
		Pro	Premium Per User	Premium Per Capacity User (no named license)
If you create/share Power BI content in the Power BI service in this type of workspace/app	Pro	Yes	Yes	No
	Premium Per User	No	Yes	No
	Premium Per Capacity	Yes	Yes	Yes

Premium Per User (PPU) works with Power BI embedded, in the same way as a Power BI Pro license. You can embed the content, and each user will need a PPU license to view it.

Email subscriptions and Premium Per User

Anyone with either a Premium Per User (PPU) license or a Pro license can receive the subscription and any attachment it includes, if the attachment is the same for all users. Pro users can't view the content in the product portal.

To add subscription capabilities that allow different data views for different recipients, a Premium capacity is required.

Users without a license can't view datasets, and reports that are built on these datasets, that were created in a PPU workspace. For example, users without a license can't access a report created from a Power BI dataset in a PPU workspace, and published in a non-PPU workspace. Similarly, content in a PPU workspace shared using **Publish to Web** isn't accessible to unlicensed users.

Power BI mobile works with any content published to a Premium Per User (PPU) app or workspace.

How can I purchase a PPU license?

To purchase Power BI Premium Per User, see Power BI pricing. Scroll to **Power BI Premium**, under **Per user** select **Buy now**.

Considerations and limitations

Considerations when working with Premium Per User licenses.

- Premium Per User is the lowest entry-point for Power BI Premium features. It's built upon the Premium platform with built-in mechanisms ensuring that PPU users can use the platform's ability to scale. PPU is designed to support enterprise workloads including Power BI items with size limits equivalent to that of a P3. For datasets, the 100-GB limit is documented in the Capacities and SKUs table.
- Your entire PPU tenant has the same 100-TB storage limit that is applied to a Premium capacity.
- PPU model refresh parallelism limits depend on the number of licenses your organization owns. The lowest PPU model refresh parallelism limit is 40, and the highest is 160.
- If your PPU trial expires, you and your users can still access the workspace, but content that requires the license is unavailable. You must then either move the workspace to a Premium capacity, or turn off the requirement.
- The export API for PPU is available for paginated reports, with a limit of one call every 5 minutes, per user. Power BI reports aren't supported.
- The Export Power BI report to file REST API isn't supported for PPU.
- The number of refreshes isn't restricted.
- The Power BI Premium metrics app isn't currently supported for PPU.
- You can't have a dataflow run in a PPU workspace, import it to a Power BI dataset in another workspace, and then allow users without a PPU license to access the content.
- Any workspace migrated from a PPU environment to a non-PPU environment (such as Premium or shared environments) must have its datasets refreshed before use. Reports opened after such migrations without being refreshed will fail with an error like: *This operation isn't allowed, as the database 'database name' is in a blocked state*. You might need to do a full refresh through SSMS to fix this.

- When using PPU you can't share data between tenants. For example, if you have a dataflow on a PPU capacity, you can't pull its data from a different tenant.

Next steps

What is Power BI Premium?

Microsoft Power BI Premium whitepaper

Planning a Power BI Enterprise Deployment whitepaper

Extended Pro Trial activation

Power BI Embedded FAQ

The Power BI Community

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

The Fabric throttling policy

Article • 07/10/2024

Throttling occurs when a tenant's capacity consumes more capacity resources than it has purchased. Too much throttling can result in a degraded end-user experience. A Microsoft Fabric tenant can create multiple capacities and assign workspaces to a specific capacity for billing and sizing.

Throttling is applied at the capacity level, meaning that while one capacity, or set of workspaces, might be experiencing reduced performance due to being overloaded, other capacities might continue running normally. In cases where features such as OneLake artifacts are produced in one capacity and consumed by another, the throttling state of the consuming capacity determines whether calls to the artifact are throttled.

Balance between performance and reliability

Fabric is designed to deliver lightning-fast performance to its customers by allowing operations to access more capacity unit (CU) resources than are allocated to the capacity. Tasks that might take several minutes to complete on other platforms can be finished in mere seconds on Fabric. To avoid penalizing users when operational loads surge, Fabric smooths or averages the CU usage of an operation over a minimum of five minutes, and even longer for high CU usage but short runtime requests. This behavior ensures you can enjoy consistently fast performance without experiencing throttling.

For background operations that have long runtimes and consume heavy CU loads, Fabric smooths their CU usage over a 24-hour period. Smoothing eliminates the need for data scientists and database administrators to spend time creating job schedules to spread CU load across the day to prevent accounts from freezing. With 24-hour CU smoothing, scheduled jobs can all run simultaneously without causing any spikes at any time during the day, and you can enjoy consistently fast performance without wasting time managing job schedules.

In-flight operations aren't throttled

When a capacity enters a throttled state, it only affects operations that are requested after the capacity has begun throttling. All operations, including long-running ones that were submitted before throttling began, are allowed to run to completion. This behavior gives you the assurance that operations are completed, even during surges in CU usage.

Throttle triggers and throttle stages

After smoothing, some accounts might still experience spikes in CU usage during peak reporting times. To help manage those spikes, admins can set up email alerts to be notified when a capacity consumes 100% of its provisioned CU resources. This pattern is an indication that the capacity might benefit from load balancing, and the admin should consider increasing the SKU size. It’s important to note that for F SKUs, you can manually increase and decrease them at any time in the admin settings. However, even when a capacity is operating at its full CU potential, Fabric doesn't apply throttling. This behavior ensures users have consistently fast performance without experiencing any disruptions.

The first phase of throttling begins when a capacity has consumed all its available CU resources for the next 10 minutes. For example, if you purchased 10 units of capacity and then consumed 50 units per minute, you would create a carryforward of 40 units per minute. After two and a half minutes, you would have accumulated a carryforward of 100 units, borrowed from future windows. At this point where all capacity is already exhausted for the next 10 minutes, Fabric initiates its first level of throttling, and all new interactive operations are delayed by 20 seconds upon submission. If the carryforward reaches a full hour, interactive requests are rejected, but scheduled background operations continue to run. If the capacity accumulates a full 24 hours of carryforward, the entire capacity is frozen until the carryforward is paid off.

Future smoothed consumption

> **Note**
>
> Microsoft tries to improve customer flexibility in using the service, while balancing the need to manage customer capacity usage. For this reason, Microsoft might change or update the Fabric throttling policy.

Expand table

Usage	Policy Limits	Platform Policy Experience Impact
Usage <= 10 minutes	Overage protection	Jobs can consume 10 minutes of future capacity use without throttling.
10 minutes < Usage <= 60 minutes	Interactive Delay	User-requested interactive jobs are delayed 20 seconds at submission.

Usage	Policy Limits	Platform Policy Experience Impact
60 minutes < Usage <= 24 hours	Interactive Rejection	User-requested interactive jobs are rejected.
Usage > 24 hours	Background Rejection	All requests are rejected.

Carryforward capacity usage reduction

Anytime a capacity has idle capacity, the system pays down the carryforward levels.

If you have 100 CU minutes and a carryforward of 200 CU minutes, and you don't have any operations running, it takes two minutes for you to pay off your carryforward. In this example, the system isn't throttled, as there are two minutes of carryforward. Throttling delays won't begin until 10 minutes of carryforward have accumulated.

If you need to pay down your carryforward faster, you can increase your SKU size temporarily to generate more idle capacity that is applied to your carryforward.

Throttling behavior is specific to Fabric

While most Fabric products follow the previously mentioned throttling rules, there are some exceptions.

For example, Fabric eventstreams have many operations that can run for years once they're started. Throttling new eventstream operations wouldn't make sense, so instead, the amount of CU resources allocated to keeping the stream open is reduced until the capacity is in good standing again.

Another exception is Real-Time Intelligence, which wouldn't be real-time if operations were delayed by 20 seconds. As a result, Real-Time Intelligence ignores the first stage of throttling with 20-second delays at 10 minutes of carryforward and waits until the rejection phase at 60 minutes of carryforward to begin throttling. This behavior ensures users can continue to enjoy real-time performance even during periods of high demand.

Similarly, almost all operations in the **Warehouse** category are reported as *background* to take advantage of 24-hour smoothing of activity to allow for the most flexible usage patterns. Classifying all data warehousing as *background* prevents peaks of CU utilization from triggering throttling too quickly. Some requests might trigger a string of operations that are throttled differently. This can make a background operation become subject to throttling as an interactive operation.

Interactive and background classifications for throttling and smoothing

Microsoft Fabric divides operations into two types, *interactive* and *background*. You can find descriptions of these and the distinctions between them in Fabric operations.

Some admins might notice that operations are sometimes classified as interactive and smoothed as background, or vice versa. This distinction happens because Fabric's throttling systems must apply throttling rules before a request begins to run. Smoothing occurs after the job has started running and CU consumption can be measured.

Throttling systems attempt to accurately categorize operations upon submission, but sometimes an operation's classification might change after throttling has been applied. When the operation begins to run, more detailed information about the request becomes available. In ambiguous scenarios, throttling systems try to err on the side of classifying operations as background, which is in the user's best interest.

Track overages and rejected operations

You can see if your capacity is overloading by reviewing the Utilization chart in the Microsoft Fabric Capacity Metrics app. A spike that goes over the line indicates an overload. To further investigate the overload, drill through to the timepoint page. You can then review both your interactive and background operations, and see which ones were responsible for overloading your capacity. You can also determine when the overloading events took place.

Since utilization exceeding 100% doesn't automatically mean throttling, you need to use the Throttling chart when evaluating overages. From there you can open a table that shows minutes to burndown, a chart with add, burndown, and cumulative percent, and more.

To view a visual history of any overutilization of capacity, including carryforward, cumulative, and burndown of utilization data, go to the Overages tab. You can change the overages visual scale to display 10 minutes, 60 minutes, and 24 hours. Carryforward only takes into account billable operations.

The Microsoft Fabric Capacity Metrics app drilldown allows admins to see operations that were rejected during a throttling event. There's limited information about these operations as they were never allowed to start. The admin can see the product, user, operation ID, and time the request was submitted. When a request is rejected, end users receive an error message that asks them to try again later.

Actions you can take to recover from overload situations

When your capacity is throttled to the point it's frozen, users receive an error if their action requires Fabric compute resources. For example, the error can say *Cannot load*

model due to reaching capacity limits. In such cases, you can use these strategies to recover your capacity from its frozen state.

- Wait until the overload state is over before issuing new requests.
- Upgrade the SKU of an F capacity.
- Pause/resume an F capacity.
- Autoscale a P capacity.
- Move lower priority or overconsuming workspaces out of the capacity.

Related content

- Install the Microsoft Fabric Capacity Metrics app to monitor Fabric capacities.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Backup and restore semantic models with Power BI Premium

Article • 09/03/2024

You can use the **Backup and Restore** feature with Power BI semantic models if you have a Power BI Premium or Premium Per User (PPU) license, similar to the backup and restore operations available in tabular models for Azure Analysis Services.

You can use SQL Server Management Studio (SSMS), Analysis Services cmdlets for PowerShell, and other tools to perform backup and restore operations in Power BI using XMLA endpoints. The following sections describe backup and restore concepts for Power BI semantic models, requirements, and considerations.

The ability to backup and restore Power BI semantic models provides a migration path from Azure Analysis Services workloads to Power BI Premium. Backup and restore also enables semantic model backups for multiple reasons, including corruption or loss, data retention requirements, and tenant movement, among others.

Using semantic model backup and restore

The **Backup and Restore** feature uses existing connections between Power BI and Azure, such as the ability to register an Azure Data Lake Gen2 (ADLS Gen2) storage account at

the tenant or workspace level to facilitate dataflow storage and operations. Since Backup and Restore uses the same connection, no other storage account is required.

You can perform offline backups, downloading the files from your ADLS Gen2 storage account. To download, use the file system, Azure Storage Explorer, .NET tools, and PowerShell cmdlets, such as the *Get-AzDataLakeGen2ItemContent* cmdlet. The following image shows a workspace with three semantic models and their corresponding backup files in Azure Storage Explorer.

To learn how to configure Power BI to use an ADLS Gen2 storage account, see configuring dataflow storage to use Azure Data Lake Gen 2.

Multi-geo considerations

Backup and Restore relies on the Azure connections infrastructure in Power BI to register an Azure Data Lake Gen2 (ADLS Gen2) storage account at the tenant or workspace level. You should provision the storage account in the region of your Power BI Premium capacity to avoid data transfer costs across regional boundaries. Check your data residency requirements before configuring your workspaces on a multi-geo Premium capacity with a storage account.

Who can perform backup and restore

With an ADLS Gen2 storage account associated with a workspace, workspace admins who have write or admin permissions can conduct *backups*. Users with these

permissions might be an admin, a member, or a contributor, or might not be part of the workspace level roles, but have direct write permission to the semantic model.

To *restore* an existing semantic model, users who have write or admin permission to the dataset can conduct a *restore* operation. To *restore* a new semantic model, the user must be an admin of the workspace.

To *browse the backup/restore filesystem* using Azure Storage Explorer (the *Browse...* button in SSMS), a user must be an admin, or a member or contributor of the workspace.

Power BI associates workspaces with their backup directories based on the workspace name. With owner permissions at the storage account level, you can download backup files or copy them from their original location to the backup directory of a different workspace, and restore them there if you're a workspace admin in the target workspace as well.

Storage account owners have unrestricted access to the backup files, so ensure storage account permissions are set and maintained carefully.

How to perform backup and restore

Backup and Restore requires using XMLA-based tools, such as SQL Server Management Studio (SSMS). There's no backup or restore facility or option in the Power BI user interface. Because of the XMLA dependency, **Backup and Restore** currently requires your semantic models to reside on a Premium or PPU capacity.

The storage account settings for **Backup and Restore** can be applied at either the **tenant** or the **workspace** level.

For **Backup and Restore**, Power BI creates a new container called *power-bi-backup* in your storage account, and creates a backup folder using the same name as your workspace in the *power-bi-backup* container. If you configure a storage account at the **tenant** level, Power BI only creates the *power-bi-backup* container. Power BI creates the backup folder at the time you attach the storage account to a workspace. If you configure a storage account at the **workspace** level, Power BI creates the *power-bi-backup* container and creates the backup folder.

During backup and restore, the following actions apply:

- Backup files are placed into the backup folder in the *power-bi-backup* container
- For restore, you must place the backup files (.abf files) into the folder before conducting a restore

If you rename a workspace, the backup folder in the *power-bi-backup* container is automatically renamed to match. However, if you have an existing folder with the same name as the renamed workspace, the automatic renaming for the backup folder fails.

Considerations and limitations

When using the **Backup and Restore** feature with Power BI, keep the following in mind.

- Power BI must be able to access your ADLS Gen2 directly. Your ADLS Gen2 can't be located in a VNET and the firewall can't be turned on.
- If your ADLS Gen2 is already working with **Backup and Restore**, and you disconnect and later reconfigure it to work with **Backup and Restore** again. You must first rename or move the previous backup folder, or the attempt will result in errors and failure.
- **Restore** only supports restoring the database as a **Large Model (Premium)** database.
- Only **enhanced format model (V3 model)** is allowed to be restored.
- When access to account key on your storage account is disabled, you might get this error: *Key based authentication is not permitted on this storage account*.
- The property, `ignoreIncompatibilities` for the `restore` command addresses Row-level security (RLS) incompatibilities between Azure Analysis Services (AAS) and Power BI Premium. Power BI Premium only supports the read permission for roles, but AAS supports all permissions. If you try to restore a backup file for which some roles don't have *read* permissions, you must specify the `ignoreIncompatibilities` property in the `restore` command. If not specified, restore can fail. When specified, the role without the *read* permission is dropped. Currently, there's no setting in SSMS that supports the `ignoreIncompatibilities` property, however, you can specify it in a `restore` command using Tabular Model Scripting Language (TMSL). For example:

JSON

```
{
  "restore": {
    "database": "DB",
    "file": "/Backup.abf",
    "allowOverwrite": true,
    "security": "copyAll",
    "ignoreIncompatibilities": true
```

```
    }
  }
```

- You can restore a corrupt database. As long as you backup the database periodically, restoring the database is the most robust way to recover it. Use the following `restore` command in an XMLA query to restore a database:

  XML

  ```
  <Restore
xmlns="http://schemas.microsoft.com/analysisservices/2003/engine">
    <File>DatabaseBackup.abf</File>
    <DatabaseName>DatabaseName</DatabaseName>
    <AllowOverwrite>true</AllowOverwrite>
  </Restore>
  ```

- When restoring a database, you might get the following error:

  "*We cannot restore the semantic model backup right now because there is not enough memory to complete this operation. Please use the /forceRestore option to restore the semantic model with the existing semantic model unloaded and offline.*"

  In these cases, with the `restore` command, add the `forceRestore` property to trigger a forced restore operation. For example, when using TMSL:

  JSON

  ```
  {
    "restore": {
    "database": "DB",
    "file": "/Backup.abf",
    "allowOverwrite": true,
    "security": "copyAll",
    "forceRestore": true
    }
  }
  ```

Related content

- Analysis Services cmdlets for PowerShell
- Semantic model connectivity with the XMLA endpoint
- Configuring tenant and workspace storage

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Using Autoscale with Power BI Premium

Article • 05/15/2024

Power BI Premium offers scale and performance for Power BI content in your organization. Power BI Premium offers improvements such as enhanced performance, greater scale, improved metrics. In addition, Premium enables customers to automatically add compute capacity to avoid slowdowns under heavy use, using **Autoscale**.

Autoscale uses an Azure subscription to automatically use more v-cores (virtual CPU cores) when the computing load on your Power BI Premium subscription would otherwise be slowed by its capacity. This article describes the steps necessary to get Autoscale working for your Power BI Premium subscription and the conditions under which Autoscale is enabled. Autoscale only works with Power BI Premium.

To enable Autoscale, the following steps need to be completed:

1. Configure an Azure subscription to use with Autoscale.
2. Enable Autoscale in the Power BI Admin portal

The following sections describe the steps in detail.

> ⓘ **Note**

- Autoscale isn't available for Microsoft 365 Government Community Cloud (GCC), due to the use of the commercial Azure cloud. For more information about which features are available and which are not, see Power BI feature availability for U.S. Government customers.
- Power BI Embedded doesn't provide an out-of-the-box vertical Autoscale feature. To learn about alternative Autoscale options for Power BI Embedded, see Autoscaling in Power BI Embedded.

Configure an Azure subscription to use with Autoscale

To select and configure an Azure subscription to work with Autoscale, you need to have *contributor* rights for the selected Azure subscription. Any user with *Account admin* rights for the Azure subscription can add a user as a *contributor*. In addition, you must be an admin for the Power BI tenant to enable Autoscale.

To select an Azure subscription to work with Autoscale, take the following steps:

1. Sign on to the Azure portal and in the search box type and select **Subscriptions**.
2. From the **Subscriptions** page, select the subscription you want to work with Autoscale.

3. From the *Settings* selections for your selected subscription, select **Resource groups**.

4. Select **Create** to create a resource group to use with Autoscale.

5. Name your resource group and select **Review + create**. The following image shows an example resource group named *powerBIPremiumAutoscaleCores*. You can name your resource group whatever you want. Make a note of the name of the subscription, and the name of your resource group. You'll need to select it from a list when you configure Autoscale in the Power BI Admin portal.

6. Azure validates the information. After the validation process completes successfully, select **Create**. You receive a notification in the upper-right corner of the Azure portal when the action completes.

Enable Autoscale in the Power BI Admin portal

After you've selected the Azure subscription to use with Autoscale, and created a resource group as described in the previous section, you're ready to enable Autoscale and associate it with the resource group you created. The person configuring **Autoscale** must be at least a *contributor* for the Azure subscription to successfully complete these steps. You can learn more about assigning a user to a contributor role for an Azure subscription.

> **Note**
>
> After creating the subscription and enabling Autoscale in the admin portal, a `Microsoft.PowerBIDedicated/autoScaleVCores` resource is created. Make sure that you don't have any Azure policies that prevent Power BI Premium from provisioning, updating or deleting the `Microsoft.PowerBIDedicated/autoScaleVCores` resource.

The following steps show you how to enable and associate Autoscale with the resource group.

1. Open the **Power BI Admin portal** and select **Capacity settings** from the left pane. Information about your Power BI Premium capacity appears.

2. Select **Manage Autoscale** to enable and configure **Autoscale**. The **Autoscale settings** pane appears. Select **Enable Autoscale**.

3. Select the Azure subscription to use with Autoscale. Only subscriptions available to the current user are displayed, which is why you must be at least a *contributor* for the subscription. Once your subscription is selected, choose the **Resource group** you created in the previous section, from the list of resource groups available to the subscription. Assign the maximum number of v-cores to use for Autoscale, and then select **Save**.

4. Power BI applies your changes, then closes the pane and returns the view to **Capacity settings** with the settings you applied. The following image shows the maximum v-cores configured for Autoscale.

The following short video shows how quickly you can configure Autoscale for Power BI Premium:

When is Autoscale triggered?

You only pay for autoscale when it's triggered. Autoscale is triggered when interactive throttling is implemented on your capacity. When interactive operations on your capacity are delayed, autoscale v-cores are added to cover the overage. As long as the overage is not covered, v-cores are added to the capacity every 30 seconds, until the number of v-cores you allocated for autoscale is reached. Once an autoscale core is

added, it remains active for a minimum of 24 hours. After 24 hours, your capacity's throttling state is evaluated and if the capacity isn't throttled, autoscale usage returns to zero.

Disable Autoscale

To disable Autoscale, follow these steps:

1. Open the **Power BI Admin portal** and select **Capacity settings**.
2. Select the capacity you want to disable Autoscale for.
3. Select **Manage Autoscale**
4. Clear the **Enable Autoscale** checkbox.

Related content

What is Power BI Premium?

Power BI Premium FAQ

Power BI Premium Per User FAQ

Add or change Azure subscription administrators

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Configure workloads in a Premium capacity

Article • 09/25/2024

This article lists the workloads for Power BI Premium, and describes their capacities.

> **Note**
>
> Workloads can be enabled and assigned to a capacity by using the Capacities REST APIs.

Supported workloads

Query workloads are optimized for and limited by resources determined by your Premium capacity SKU. Premium capacities also support additional workloads that can use your capacity's resources.

The list of workloads below, describes which Premium SKUs supports each workload:

- **AI** - All SKUs are supported apart from the *EM1/A1* SKUs
- **Semantic models** - All SKUs are supported
- **Dataflows** - All SKUs are supported
- **Paginated reports** - All SKUs are supported

Configure workloads

You can tune the behavior of the workloads, by configuring workload settings for your capacity.

> **Important**
>
> All workloads are always enabled and cannot be disabled. Your capacity resources are managed by Power BI according to your capacity usage.

To configure workloads in the Power BI admin portal

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

2. From the page header, select ... > **Settings** > **Admin portal**.

3. Go to **Capacity settings** and from the **Power BI Premium** tab, select a capacity.

4. Expand **Workloads**.

5. Set the values for each workload according to your specifications.

6. Select **Apply**.

Monitor workloads

Use the Microsoft Fabric Capacity Metrics app to monitor your capacity's activity.

> **Important**
>
> If your Power BI Premium capacity is experiencing high resource usage, resulting in performance or reliability issues, you can receive notification emails to identify and resolve the issue. This can be a streamlined way to troubleshoot overloaded capacities. For more information, see Notifications.

AI (Preview)

The AI workload lets you use cognitive services and Automated Machine Learning in Power BI. Use the following settings to control workload behavior.

Expand table

Setting Name	Description
Max Memory (%)[1]	The maximum percentage of available memory that AI processes can use in a capacity.
Allow usage from Power BI Desktop	This setting is reserved for future use and doesn't appear in all tenants.
Allow building machine learning models	Specifies whether business analysts can train, validate, and invoke machine learning models directly in Power BI. For more information, see Automated Machine Learning in Power BI (Preview).
Enable parallelism for AI requests	Specifies whether AI requests can run in parallel.

[1] *Premium* doesn't require memory settings to be changed. Memory in Premium is automatically managed by the underlying system.

Semantic models

This section describes the following semantic models workload settings:

- Power BI settings
- Analysis Services server properties

Power BI settings

Use the settings in the table below to control workload behavior. Settings with a link have additional information that you can review in designated sections below the table.

Expand table

Setting Name	Description
Max Memory (%)[1]	The maximum percentage of available memory that semantic models can use in a capacity.
XMLA Endpoint	Specifies that connections from client applications honor the security group membership set at the workspace and app levels. For more information, see Connect to semantic models with client applications and tools.
Max Intermediate Row Set Count	The maximum number of intermediate rows returned by DirectQuery. The default value is 1000000, and the allowable range is between 100000 and

Setting Name	Description
	2147483646. The upper limit might need to be further constrained based on what the datasource supports.
Max Offline Semantic model Size (GB)	The maximum size of the offline semantic model in memory. This is the compressed size on disk. The default value is 0, which is the highest limit defined by SKU. The allowable range is between 0 and the capacity size limit.
Max Result Row Count	The maximum number of rows returned in a DAX query. The default value is 2147483647, and the allowable range is between 100000 and 2147483647.
Query Memory Limit (%)	The maximum percentage of available memory in the workload that can be used for executing an MDX or DAX query. The default value is 0, which results in SKU-specific automatic query memory limit being applied.
Query Timeout (seconds)	The maximum amount of time before a query times out. The default is 3600 seconds (1 hour). A value of 0 specifies that queries won't time out.
Automatic page refresh	On/Off toggle to allow premium workspaces to have reports with automatic page refresh based on fixed intervals.
Minimum refresh interval	If automatic page refresh is on, the minimum interval allowed for page refresh interval. The default value is five minutes, and the minimum allowed is one second.
Change detection measure	On/Off toggle to allow premium workspaces to have reports with automatic page refresh based on change detection.
Minimum execution interval	If change detection measure is on, the minimum execution interval allowed to poll for data changes. The default value is five seconds, and the minimum allowed is one second.

[1] *Premium* doesn't require memory settings to be changed. Memory in Premium is automatically managed by the underlying system.

Max Intermediate Row Set Count

Use this setting to control the impact of resource-intensive or poorly designed reports. When a query to a DirectQuery semantic model results in a very large result from the source database, it can cause a spike in memory usage and processing overhead. This situation can lead to other users and reports running low on resources. This setting allows the capacity administrator to adjust how many rows an individual query can fetch from the data source.

Alternatively, if the capacity can support more than the one million row default, and you have a large semantic model, increase this setting to fetch more rows.

This setting affects only DirectQuery queries, whereas Max Result Row Set Count affects DAX queries.

Max Offline Semantic model Size

Use this setting to prevent report creators from publishing a large semantic model that could negatively impact the capacity. Power BI can't determine actual in-memory size until the semantic model is loaded into memory. It's possible that a semantic model with a smaller offline size can have a larger memory footprint than a semantic model with a larger offline size.

If you have an existing semantic model that is larger than the size you specify for this setting, the semantic model will fail to load when a user tries to access it. The semantic model can also fail to load if it's larger than the Max Memory configured for the semantic models workload.

This setting is applicable for models in both small semantic model storage format (ABF format) and large semantic model storage format (PremiumFiles), although the offline size of the same model might differ when stored in one format vs another. For more information, see Large models in Power BI Premium.

To safeguard the performance of the system, an additional SKU-specific hard ceiling for max offline semantic model size is applied, regardless of the configured value. The additional SKU-specific hard ceiling in the below table does not apply to Power BI semantic models stored in large semantic model storage format.

Expand table

SKU	Limit[1]
F2	1 GB
F4	2 GB
F8/EM1/A1	3 GB
F16/EM2/A2	5 GB
F32/EM3/A3	6 GB
F64/P1/A4	10 GB
F128/P2/A5	10 GB

SKU	Limit[1]
F256/P3/A6	10 GB
F512/P4/A7	10 GB
F1024/P5/A8	10 GB
F2048	10 GB

[1]Hard ceiling for Max Offline semantic model size (small storage format).

Max Result Row Set Count

Use this setting to control the impact of resource-intensive or poorly designed reports. If this limit is reached in a DAX query, a report user sees the following error. They should copy the error details and contact an administrator.

This setting affects only DAX queries, whereas Max Intermediate Row Set Count affects DirectQuery queries.

Query Memory Limit

Use this setting to control the impact of resource-intensive or poorly designed reports. Some queries and calculations can result in intermediate results that use a lot of memory on the capacity. This situation can cause other queries to execute very slowly, cause eviction of other semantic models from the capacity, and lead to out of memory errors for other users of the capacity.

This setting applies to all DAX and MDX queries that are executed by Power BI reports, Analyze in Excel reports, as well as other tools that might connect over the XMLA endpoint.

Data refresh operations might also execute DAX queries as part of refreshing the dashboard tiles and visual caches after the data in the semantic model has been refreshed. Such queries might also potentially fail because of this setting, and this could

lead to the data refresh operation being shown in a failed state, even though the data in the semantic model was successfully updated.

The default setting is 0, which results in the following SKU-specific automatic query memory limit being applied.

Expand table

SKU	Automatic Query Memory Limit
F2	1 GB
F4	1 GB
F8/EM1/A1	1 GB
F16/EM2/A2	2 GB
F32/EM3/A3	5 GB
F64/P1/A4	10 GB
F128/P2/A5	10 GB
F256/P3/A6	10 GB
F512/P4/A7	20 GB
F1024/P5/A8	40 GB
F2048	40 GB

The query limit for a workspace that isn't assigned to a Premium capacity is 1GB.

Query Timeout

Use this setting to maintain better control of long-running queries, which can cause reports to load slowly for users.

This setting applies to all DAX and MDX queries that are executed by Power BI reports, Analyze in Excel reports, as well as other tools that might connect over the XMLA endpoint.

Data refresh operations might also execute DAX queries as part of refreshing the dashboard tiles and visual caches after the data in the semantic model has been refreshed. Such queries might also potentially fail because of this setting, and this could lead to the data refresh operation being shown in a failed state, even though the data in the semantic model was successfully updated.

This setting applies to a single query and not the length of time it takes to run all of the queries associated with updating a semantic model or report. Consider the following example:

- The **Query Timeout** setting is 1200 (20 minutes).
- There are five queries to execute, and each runs 15 minutes.

The combined time for all queries is 75 minutes, but the setting limit isn't reached because all of the individual queries run for less than 20 minutes.

Note that Power BI reports override this default with a much smaller timeout for each query to the capacity. The timeout for each query is typically about three minutes.

Automatic page refresh

When enabled, automatic page refresh allows users in your Premium capacity to refresh pages in their report at a defined interval, for DirectQuery sources. As a capacity admin, you can do the following:

- Turn automatic page refresh on and off
- Define a minimum refresh interval

To find the automatic page refresh setting:

1. In the Power BI Admin portal, select **Capacity settings**.

2. Select your capacity, and then scroll down and expand the **Workloads** menu.

3. Scroll down to the **Semantic models** section.

Queries created by automatic page refresh go directly to the data source, so it's important to consider reliability and load on those sources when allowing automatic page refresh in your organization.

Analysis Services server properties

Power BI Premium supports additional Analysis Services server properties. To review these properties, refer to Server properties in Analysis Services.

Admin portal switch

The Analysis Services XMLA-based server properties setting is enabled by default. When enabled, workspace admins can modify behaviors for an individual workspace. Modified properties apply only to that workspace. To toggle the Analysis Services server properties setting, follow the steps below.

1. Go to your capacity settings.
2. Select the capacity you want to disable the *Analysis Services server properties* in.
3. Expand **Workloads**.
4. Under *semantic models*, select the setting you want for the **Observe XMLA-based workspace settings (which might override capacity settings)** switch.

Dataflows

The dataflows workload lets you use dataflows self-service data prep, to ingest, transform, integrate, and enrich data. Use the following settings to control workload behavior in Premium. Power BI Premium doesn't require memory settings to be changed. Memory in Premium is automatically managed by the underlying system.

Enhanced dataflows compute engine

To benefit from the new compute engine, split ingestion of data into separate dataflows and put transformation logic into computed entities in different dataflows. This approach is recommended because the compute engine works on dataflows that reference an existing dataflow. It doesn't work on ingestion dataflows. Following this guidance ensures that the new compute engine handles transformation steps, such as joins and merges, for optimal performance.

Paginated reports

The paginated reports workload lets you run paginated reports, based on the standard SQL Server Reporting Services format, in the Power BI service.

Paginated reports offer the same capabilities that SQL Server Reporting Services (SSRS) reports do today, including the ability for report authors to add custom code. This allows authors to dynamically change reports, such as changing text colors based on code expressions.

Outbound connectivity

Outbound connectivity is turned on by default. It allows paginated reports to make requests for fetching external resources such as images, and call external APIs and Azure

functions defined using custom code in paginated reports. A Fabric administrator can disable this setting in the Power BI admin portal.

To get to the outbound connectivity settings, follow these steps:

1. In Power BI service, navigate to the admin portal.
2. From the **Power BI Premium** tab, select the capacity you want to disable the paginated reports outbound requests for.
3. Expand **Workloads**.

   The outbound connectivity switch is in the *paginated reports* section.

   - When **Outbound Connectivity Disable** is turned off, outbound connectivity is enabled.
   - When **Outbound Connectivity Disable** is turned on, outbound connectivity is disabled.
4. After you've made a change, select **Apply**.

The paginated reports workload is enabled automatically, and is always enabled.

Related content

Power BI Premium

Self-service data prep in Power BI with Dataflows

What are paginated reports in Power BI?

Automatic page refresh in Power BI Desktop (preview)

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Large semantic models in Power BI Premium

Article • 11/10/2023

Power BI semantic models can store data in a highly compressed in-memory cache for optimized query performance, enabling fast user interactivity. With Premium capacities, large semantic models beyond the default limit can be enabled with the **Large semantic model storage format** setting. When enabled, semantic model size is limited by the Premium *capacity* size or the maximum size set by the administrator.

Large semantic models can be enabled for all Premium P SKUs, Embedded A SKUs, and with Premium Per User (PPU). The large semantic model size limit in Premium is comparable to Azure Analysis Services, in terms of data model size limitations.

While required for semantic models to grow beyond 10 GB, enabling the Large semantic model storage format setting has other benefits. If you're planning to use XMLA endpoint-based tools for semantic model write operations, be sure to enable the setting, even for semantic models that you wouldn't necessarily characterize as a *large* semantic model. When enabled, the large semantic model storage format can improve XMLA write operations performance.

Large semantic models in the service don't affect the Power BI Desktop model upload size, which is still limited to 10 GB. Instead, semantic models can grow beyond that limit in the service on refresh.

> **Important**
>
> Power BI Premium does support large semantic models. Enable the **Large semantic model storage format** option to use semantic models in Power BI Premium that are larger than the default limit.

> **Note**
>
> Large semantic models in Power BI Premium are not available in the Power BI service for U.S. Government DoD customers. For more information about which features are available, and which are not, see **Power BI feature availability for U.S. Government customers**.

Enable large semantic models

Steps here describe enabling large semantic models for a new model published to the service. For existing semantic models, only step 3 is necessary.

1. Create a model in Power BI Desktop. If your semantic model will become larger and progressively consume more memory, be sure to configure Incremental refresh.

2. Publish the model as a semantic model to the service.

3. In the service > semantic model > **Settings**, expand **Large semantic model storage format**, set the slider to **On**, and then select **Apply**.

4. Invoke a refresh to load historical data based on the incremental refresh policy. The first refresh could take a while to load the history. Subsequent refreshes should be faster, depending on your incremental refresh policy.

Set default storage format

In supported regions, all new semantic models created in a workspace assigned to a Premium capacity can have the large semantic model storage format enabled by default. If the region doesn't support large semantic models, the *large semantic model storage format* option described below is disabled. You can see which regions are supported in the region availability section.

1. In the workspace, select **Settings** > **Premium**.

2. In **Default storage format**, select **Large semantic model storage format**, and then select **Save**.

Enable with PowerShell

You can also enable large semantic model storage format by using PowerShell. You must have capacity admin and workspace admin privileges to run the PowerShell cmdlets.

1. Find the semantic model ID (GUID). On the **Semantic models** tab for the workspace, under the semantic model settings, you can see the ID in the URL.

2. From a PowerShell admin prompt, install the MicrosoftPowerBIMgmt module.

```
PowerShell

Install-Module -Name MicrosoftPowerBIMgmt
```

3. Run the following cmdlets to sign in and check the semantic model storage mode.

```
PowerShell

Login-PowerBIServiceAccount

(Get-PowerBIDataset -Scope Organization -Id <Semantic model ID> -
Include actualStorage).ActualStorage
```

The response should be the following. The storage mode is ABF (Analysis Services backup file), which is the default.

```
Id                    StorageMode

--                    -----------

<Semantic model ID>         Abf
```

4. Run the following cmdlets to set the storage mode. It can take a few seconds to convert to Premium Files.

```
PowerShell

Set-PowerBIDataset -Id <Semantic model ID> -TargetStorageMode
PremiumFiles

(Get-PowerBIDataset -Scope Organization -Id <Semantic model ID> -
Include actualStorage).ActualStorage
```

The response should be the following. The storage mode is now set to Premium Files.

```
Id                    StorageMode

--                    -----------

<Semantic model ID>         PremiumFiles
```

You can check the status of semantic model conversions to and from Premium Files by using the Get-PowerBIWorkspaceMigrationStatus cmdlet.

Semantic model eviction

Semantic model eviction is a Premium feature that allows the sum of semantic model sizes to be significantly greater than the memory available for the purchased SKU size of the capacity. A single semantic model is still constrained to the memory limits of the SKU. Power BI uses dynamic memory management to evict inactive semantic models from memory. Semantic models are evicted so that Power BI can load other semantic models to address user queries.

> **Note**
>
> If you have to wait for an evicted semantic model to be reloaded, you might experience a noticeable delay.

On-demand load

On-demand load is enabled by default for large semantic models, and can provide significantly improved load time of evicted semantic models. With on-demand load, you get the following benefits during subsequent queries and refreshes:

- Relevant data pages are loaded on-demand (paged in to memory).
- Evicted semantic models are quickly made available for queries.

On-demand loading surfaces additional Dynamic Management View (DMV) information that can be used to identify usage patterns and understand the state of your models. For example, you can check the *Temperature* and *Last Accessed* statistics for each column in the semantic model, by running the following DMV query from SQL Server Management Studio (SSMS):

SQL

```
Select * from SYSTEMRESTRICTSCHEMA
($System.DISCOVER_STORAGE_TABLE_COLUMN_SEGMENTS, [DATABASE_NAME] =
'<Semantic model Name>')
```

Checking semantic model size

After loading historical data, you can use SSMS through the XMLA endpoint to check the estimated semantic model size in the model properties window.

You can also check the semantic model size by running the following DMV queries from SSMS. Sum the DICTIONARY_SIZE and USED_SIZE columns from the output to see the semantic model size in bytes.

SQL

```
SELECT * FROM SYSTEMRESTRICTSCHEMA
($System.DISCOVER_STORAGE_TABLE_COLUMNS,
 [DATABASE_NAME] = '<Semantic model Name>') //Sum DICTIONARY_SIZE (bytes)

SELECT * FROM SYSTEMRESTRICTSCHEMA
($System.DISCOVER_STORAGE_TABLE_COLUMN_SEGMENTS,
 [DATABASE_NAME] = '<Semantic model Name>') //Sum USED_SIZE (bytes)
```

Default segment size

For semantic models using the large semantic model storage format, Power BI automatically sets the default segment size to 8 million rows to strike a good balance

between memory requirements and query performance for large tables. This is the same segment size as in Azure Analysis Services. Keeping the segment sizes aligned helps ensure comparable performance characteristics when migrating a large data model from Azure Analysis Services to Power BI.

Considerations and limitations

Keep in mind the following restrictions when using large semantic models:

- **Download to Power BI Desktop**: If a semantic model is stored on Premium Files, downloading as a .pbix file will fail.
- **Supported regions**: Large semantic models are available in Azure regions that support Azure Premium Files Storage. Review the table in region availability to see a list of all the supported regions.
- **Setting maximum semantic model size**: Maximum semantic model size can be set by administrators. For more information, see *Max Memory* in Datasets.
- **Refreshing large semantic models**: Semantic models that are close to half the size of the capacity size (for example, a 12-GB semantic model on a 25-GB capacity size) may exceed the available memory during refreshes. Using the enhanced refresh REST API or the XMLA endpoint, you can perform fine grained data refreshes, so that the memory needed by the refresh can be minimized to fit within your capacity's size.
- **Push semantic models**: Push semantic models don't support the large semantic model storage format.
- **Pro isn't supported** - Large semantic models aren't supported in Pro workspaces. If a workspace is migrated from Premium to Pro, any semantic models with the *large semantic model storage format* setting, will fail to load.
- You can't use REST APIs to change the settings of a workspace to allow new semantic models to use the large semantic model storage format by default.

Region availability

Large semantic models in Power BI are only available in Azure regions that support Azure Premium Files Storage.

The following list provides regions where large semantic models in Power BI are available. Regions not in the following list aren't supported for large models.

> **Note**
>
> Once a large semantic model is created in a workspace, it must stay in that region. You cannot reassign a workspace with a large semantic model to a Premium capacity in another region.

Azure region	Azure region abbreviation
Australia East	australiaeast
Australia Southeast	australiasoutheast
Brazil South	brazilsouth
Canada East	canadaeast
Canada Central	canadacentral
Central India	centralindia
Central US	centralus
East Asia	eastasia
East US	eastus
East US 2	eastus2
France Central	francecentral
France South	francesouth
Germany North	germanynorth
Germany West Central	germanywestcentral
Japan East	japaneast
Japan West	japanwest
Korea Central	koreacentral
Korea South	koreasouth
North Central US	northcentralus
North Europe	northeurope
South Africa North	southafricanorth
South Africa West	southafricawest

Azure region	Azure region abbreviation
South Central US	southcentralus
Southeast Asia	southeastasia
Switzerland North	switzerlandnorth
Switzerland West	switzerlandwest
UAE Central	uaecentral
UAE North	uaenorth
UK South	uksouth
UK West	ukwest
West Europe	westeurope
West India	westindia
West US	westus
West US 2	westus2

Next steps

The following links provide information that can be useful for working with large models:

Azure Premium Files Storage

Configure Multi-Geo support for Power BI Premium

Bring your own encryption keys for Power BI

Incremental refresh for semantic models

Power BI Premium Generation 2

Automate Premium workspace and semantic model tasks with service principals

Article • 11/10/2023

Service principals are an Azure Active Directory (Azure AD) *app registration* you create within your tenant to perform unattended resource and service level operations. They're a unique type of user identity with an app name, application ID, tenant ID, and *client secret* or certificate for a password.

Power BI Premium uses the same service principal functionality as Power BI Embedded. To learn more, see Embedding Power BI content with service principals.

In Power BI Premium, you can use service principals with the XMLA (XML Analysis) endpoint to automate semantic model management tasks such as provisioning workspaces, deploying models, and semantic model refresh with:

- PowerShell.
- Azure Automation.
- Azure Logic Apps.
- Custom client applications.

Only new workspaces support XMLA endpoint connections by using service principals. Classic workspaces aren't supported. A service principal has only those permissions necessary to perform tasks on workspaces where it's assigned. Permissions are assigned through workspace access, much like regular UPN (user principal name) accounts.

To perform write operations, the capacity's Semantic models workload must have the XMLA endpoint enabled for read-write operations. Semantic models published from Power BI Desktop should have the enhanced metadata format feature enabled.

Create a service principal

Service principals are created as an app registration in the Azure portal or by using PowerShell. When creating your service principal, be sure to copy and save separately the app name, application (client) ID, directory (tenant) ID, and client secret. For steps on how to create a service principal, see:

- Create service principal - Azure portal
- Create service principal - PowerShell

Create an Azure AD security group

By default, service principals have access to any tenant settings they're enabled for. Depending on your admin settings, access can include specific security groups or the entire organization.

To restrict service principal access to specific tenant settings, you can allow access to specific security groups. Alternatively, you can create a dedicated security group for service principals, and exclude it from the desired tenant settings. To create a security group and add a service principal, see Create a basic group and add members using Azure Active Directory.

Enable service principals

Before you can start using service principals in Power BI, an admin must enable service principal access in the Power BI Admin portal.

1. Go to the Power BI Admin portal and then select **Tenant settings**.
2. Scroll to **Developer settings** and then expand **Allow service principals to use Power BI APIs**.
3. Select **Enabled**.
4. To apply permissions to a security group, select **Specific security groups (Recommended)**.
5. Enter the group name.
6. Select **Apply**.

Workspace access

In order for your service principal to have the necessary permissions to perform Premium workspace and semantic model operations, you must add the service principal as a workspace Member or Admin. Using workspace access in the Power BI service is described here, but you can also use the Add Group User REST API.

1. In the Power BI service for a workspace, select **More** > **Workspace access**.

2. Search by application name and then add the service principal as an **Admin** or **Member** to the workspace.

Connection strings for the XMLA endpoint

After you create a service principal, enable service principals for your tenant, and add the service principal to workspace access, use it as a user identity in connection strings with the XMLA endpoint. The difference is, instead of the `user id` and `password` parameters, you specify the application ID, tenant ID, and application secret.

`Data Source=powerbi://api.powerbi.com/v1.0/myorg/<workspace name>; Initial Catalog=<dataset name>;User ID=app:<appId>@<tenantId>;Password=<app_secret>;`

PowerShell

Open a PowerShell session to run the following example code.

Using SQLServer module

In the following example, `AppId`, `TenantId`, and `AppSecret` are used to authenticate a semantic model refresh operation:

PowerShell

```
Param (
        [Parameter(Mandatory=$true)] [String] $AppId,
        [Parameter(Mandatory=$true)] [String] $TenantId,
        [Parameter(Mandatory=$true)] [String] $AppSecret
       )
$PWord = ConvertTo-SecureString -String $AppSecret -AsPlainText -Force

$Credential = New-Object -TypeName
"System.Management.Automation.PSCredential" -ArgumentList $AppId, $PWord

Invoke-ProcessTable -Server
"powerbi://api.powerbi.com/v1.0/myorg/myworkspace" -TableName "mytable" -
DatabaseName "mydataset" -RefreshType "Full" -ServicePrincipal -
ApplicationId $AppId -TenantId $TenantId -Credential $Credential
```

Analysis Management Objects (AMO) and ADOMD.NET

When you connect with client applications and web apps, you can use AMO and ADOMD client libraries version 15.1.42.26 (June 2020) and later installable packages from NuGet to support service principals in connection strings by using the following syntax: `app:AppID` and password or `cert:thumbprint`.

In the following example, `appID` and `password` values are used to perform a model database refresh operation:

C#

```
string appId = "xxx";
string authKey = "yyy";
string connString = $"Provider=MSOLAP;Data
source=powerbi://api.powerbi.com/v1.0/<tenant>/<workspacename>;Initial
```

```
catalog=<datasetname>;User ID=app:{appId};Password={authKey};";
Server server = new Server();
server.Connect(connString);
Database db = server.Databases.FindByName("adventureworks");
Table tbl = db.Model.Tables.Find("DimDate");
tbl.RequestRefresh(RefreshType.Full);
db.Model.SaveChanges();
```

Next steps

Semantic model connectivity with the XMLA endpoint

Azure Automation

Azure Logic Apps

Power BI REST APIs

Semantic model connectivity with the XMLA endpoint

Article • 09/03/2024

Power BI Premium, Premium Per User, and Power BI Embedded workspaces use an *XMLA endpoint* to support open-platform connectivity from Microsoft and third-party client applications and tools.

XMLA endpoints

Workspaces use the XML for Analysis (XMLA) protocol for communications between client applications and the engine that manages your Power BI workspaces and semantic models. These communications are through what are commonly called XMLA endpoints. XMLA is the communication protocol used by the Microsoft Analysis Services engine, which runs Power BI's semantic modeling, governance, lifecycle, and data management. Data sent over the XMLA protocol is fully encrypted.

By default, *read-only* connectivity using the endpoint is enabled for the **Semantic models workload** in a capacity. With read-only, data visualization applications and tools can query semantic model model data, metadata, events, and schema.

Read-write operations using the endpoint can be enabled. Read-write provides more semantic model management, governance, advanced semantic modeling, debugging, and monitoring. When enabled, semantic models have more parity with Azure Analysis Services and SQL Server Analysis Services enterprise grade tabular modeling tools and processes.

Analysis Services server properties

Power BI Premium supports many Analysis Services server properties. To review these properties, refer to Server properties in Analysis Services.

Terms of use

Using the XMLA endpoint is subject to:

Single-user application - The application uses a single user account or app identity to access a Power BI semantic model through the XMLA endpoint. Examples of single-user applications include developer tools, admin scripts, and automated processes. These

applications can perform tasks such as data modeling and administrative tasks that alter the metadata of a semantic model, backup or restore operation, or trigger a data refresh. The user account or app identity that the client application uses to access a semantic model must have a valid Premium Per User (PPU) license unless the semantic model resides on a Premium capacity.

Multi-user application - The application provides multiple users with access to a Power BI semantic model. For example, a middle-tier application integrating a semantic model into a business solution and accessing the semantic model on behalf of its business users.

- Premium Per User (PPU) workspaces - The application must require each user to sign in to Power BI. For each user, the application uses an access token to access the semantic models. The application can't use a service account or other app identity to perform tasks on behalf of individual users. Each user must have their own Power BI account for opening reports, accessing semantic models, and executing queries.
- For Premium workspaces, the application can use either a service account or app identity on behalf of end users without requiring each user to sign in to Power BI.

Client applications and tools

Common applications and tools used with Azure Analysis Services and SQL Server Analysis Services that are now supported by Power BI Premium semantic models:

Microsoft Excel – Excel PivotTables are one of the most common tools used to summarize, analyze, explore, and present summary data from Power BI semantic models. Read-only is required for query operations. Requires the Click-to-Run version of Office 16.0.13612.10000 or higher.

Visual Studio with Analysis Services projects – Known as SQL Server Data Tools(SSDT). SSDT is an enterprise grade model authoring tool for Analysis Services tabular models. All Visual Studio 2017 and later editions including the free Community edition support Analysis Services projects extensions. Requires extension version 2.9.14 or higher to deploy tabular models to a Premium workspace. The model must be at the 1500 or higher compatibility level to deploy. Requires XMLA read-write on the semantic models workload. To learn more, see Tools for Analysis Services.

SQL Server Management Studio (SSMS) - Supports DAX, MDX, and XMLA queries. Perform fine-grain refresh operations and scripting of semantic model metadata using the Tabular Model Scripting Language (TMSL). Requires read-only for query operations.

Requires read-write for scripting metadata. Requires SSMS version **18.9** or higher. Download SSMS.

SQL Server Profiler – SQL Server Profiler installs with SSMS, it allows tracing and debugging of semantic model events. Although officially deprecated for SQL Server, Profiler is still included in SSMS and remains supported for Analysis Services and Power BI. Requires SQL Server Profiler version **18.9** or higher. Users must specify the semantic model (initial catalog) when connecting with the XMLA endpoint. To learn more, see SQL Server Profiler for Analysis Services.

Analysis Services Deployment Wizard – Installed with SSMS, this tool provides deployment of Visual Studio authored tabular model projects to Analysis Services and Premium workspaces. It can be run interactively or from the command line for automation. XMLA read-write is required. To learn more, see Analysis Services Deployment Wizard.

PowerShell cmdlets – Use Analysis Services cmdlets to automate semantic model management tasks like refresh operations. Requires XMLA read-write. Requires version **21.1.18256** or higher of the SqlServer PowerShell module. Azure Analysis Services cmdlets in the Az.AnalysisServices module aren't supported for Power BI semantic models. To learn more, see Analysis Services PowerShell Reference.

Power BI Report Builder - A tool for authoring paginated reports. Create a report definition that specifies the data to retrieve, where to get it, and how to display it. You can preview your report in Report Builder and then publish your report to the Power BI service. Requires XMLA read-only. To learn more, see Power BI Report Builder.

Tabular Editor - An open-source tool for creating, maintaining, and managing tabular models using an intuitive, lightweight editor. A hierarchical view shows all objects in your tabular model. Organizes objects by display folders with support for multi-select property editing and DAX syntax highlighting. Requires XMLA read-only for query operations. Requires read-write for metadata operations. To learn more, see tabulareditor.github.io.

DAX Studio – An open-source tool for DAX authoring, diagnosis, performance tuning, and analysis. Features include object browsing, integrated tracing, query execution breakdowns with detailed statistics, DAX syntax highlighting and formatting. Requires XMLA read-only for query operations. To learn more, see daxstudio.org.

ALM Toolkit - An open-source schema compare tool for Power BI semantic models, most often used for application lifecycle management (ALM) scenarios. Perform deployment across environments and retain incremental refresh historical data. Diff and merge metadata files, branches, and repos. Reuse common definitions between

semantic models. Requires read-only for query operations. Requires read-write for metadata operations. To learn more, see alm-toolkit.com.

Third party - Includes client data visualization applications and tools that can connect to, query, and consume semantic models in Premium workspaces. Most tools require the latest versions of MSOLAP client libraries, but some can use ADOMD. Read-only or read-write XMLA endpoint is dependent on the operations.

Client libraries

Client applications and tools don't communicate directly with the XMLA endpoint. Instead, they use *client libraries* as an abstraction layer. These are the same client libraries that applications use to connect to Azure Analysis Services and SQL Server Analysis Services. Microsoft applications like Excel, SQL Server Management Studio (SSMS), and Analysis Services projects extension for Visual Studio install all three client libraries and update them along with regular application and extension updates. Developers can use the client libraries to build custom applications. In some cases, particularly with third-party applications, if not installed with the application, it might be necessary to install newer versions of the client libraries. Client libraries are updated monthly. To learn more, see Client libraries for connecting to Analysis Services.

Optimize semantic models for write operations by enabling large models

When using the XMLA endpoint for semantic model management with write operations, it's recommended you enable the semantic model for large models. This reduces the overhead of write operations, which can make them considerably faster. For semantic models over 1 GB (after compression), the difference can be significant. To learn more, see Large models in Power BI Premium.

Enable XMLA read-write

By default, Premium capacity or Premium Per User semantic model workloads have the XMLA endpoint property setting enabled for read-only. This means applications can only query a semantic model. For applications to perform write operations, the XMLA Endpoint property must be enabled for read-write.

To enable read-write for a Premium capacity

1. Select **Settings** > **Admin portal**.

2. In the Admin portal, select **Capacity settings** > **Power BI Premium** > capacity name.

3. Expand **Workloads**. In the **XMLA Endpoint** setting, select **Read Write**. The XMLA Endpoint setting applies to *all workspaces and semantic models* assigned to the capacity.

To enable read-write for Premium Per User

1. Select **Settings** > **Admin portal**.
2. In the Admin portal, select **Premium Per User**.
3. Expand **Semantic model workload settings**. In the **XMLA Endpoint** setting, select **Read Write**.

Connecting to a Premium workspace

Workspaces assigned to a capacity have a connection string in URL format. For example:

`powerbi://api.powerbi.com/v1.0/[tenant name]/[workspace name]`.

Applications connecting to the workspace use the URL as if it were an Analysis Services server name. For example:

`powerbi://api.powerbi.com/v1.0/contoso.com/Sales Workspace`.

> ⓘ **Note**
>
> Connecting to a My Workspace by using the XMLA endpoint is currently not supported.

B2B and guest users

When users access a workspace in their home tenant, the tenant name section in the URL can be replaced by `myorg`. For example:

`powerbi://api.powerbi.com/v1.0/myorg/Sales Workspace`.

When B2B\guest users access workspaces in a different tenant, that tenant name must be specified in the data source URL. For example, when a contoso.com user is invited to the fabrikam.com tenant and granted permission to "Sales Workspace", they must use the below URL to connect:

`powerbi://api.powerbi.com/v1.0/fabrikam.com/Sales Workspace`.

To determine the primary domain name and ID of a tenant, sign into the Azure portal, select Microsoft Entra ID from the main menu, and then note the information on the Microsoft Entra Overview page. For more information, see Find the Microsoft Entra tenant ID and primary domain name.

To get the workspace connection URL

In workspace **Settings** > **Premium** > **Workspace Connection**, select **Copy**.

Connection requirements

Initial catalog

With some tools, such as SQL Server Profiler, you must specify an *Initial Catalog*, which is the semantic model (database) to connect to in your workspace. In the **Connect to Server** dialog, select **Options** > **Connection Properties** > **Connect to database**, enter the semantic model name.

Duplicate workspace names

Workspaces in Power BI validation prevents the creation or renaming of workspaces with duplicate names. When connecting to a workspace with the same name as another workspace, you might get the following message:

Cannot connect to `powerbi://api.powerbi.com/v1.0/[tenant name]/[workspace name]`.

To work around, in addition to the workspace name specify the ObjectIDGuid. You can copy the ObjectIDGuid from the workspace objectID in the URL. Append the objectID to the connection URL. For example:

`powerbi://api.powerbi.com/v1.0/myorg/Contoso Sales - 9d83d204-82a9-4b36-98f2-a40099093830`.

Duplicate semantic model name

To connect to a semantic model with the same name as another semantic model in the same workspace, append the semantic model guid to the semantic model name. You can get both semantic model name and guid when connected to the workspace in SSMS.

Delay in semantic models shown

When you connect to a workspace, changes from new, deleted, and renamed semantic models can take up to a few minutes to appear.

Unsupported semantic models

The following semantic models aren't accessible by using the XMLA endpoint. These semantic models won't appear under the workspace in SSMS or in other tools:

- Semantic models based on a live connection to an Azure Analysis Services or SQL Server Analysis Services model.
- Semantic models based on a live connection to a Power BI semantic model in another workspace. To learn more, see Intro to semantic models across workspaces.
- Semantic models with Push data by using the REST API.
- Semantic models in My Workspace.
- Excel workbook semantic models.

Server/workspace alias

Server name aliases, supported in Azure Analysis Services aren't supported for Premium workspaces.

Security

In addition to the XMLA Endpoint property being enabled read-write by the capacity admin, the tenant-level setting **Allow XMLA endpoints and Analyze in Excel with on-premises semantic models** must be enabled in the admin portal. If you need to generate Analyze in Excel (AIXL) files that connect to the XMLA endpoint, the tenant-level setting **Users can work with semantic models in Excel using a live connection** should also be enabled. These settings are both enabled by default.

Allow XMLA endpoints and Analyze in Excel with on-premises semantic models is an Integration setting.

Users can work with semantic models in Excel using a live connection is an Export and sharing setting.

The following table describes the implications of both settings:

Expand table

Setting	Allow XMLA endpoints and Analyze in Excel with on-premises semantic models = disabled	Allow XMLA endpoints and Analyze in Excel with on-premises semantic models = enabled
Users can work with semantic models in Excel using a live connection = disabled	XMLA: **disallowed** Analyze in Excel: **disallowed**	XMLA: **allowed** Analyze in Excel: **disallowed**
Users can work with semantic models in Excel using a live connection = enabled	XMLA: **disallowed** Analyze in Excel: **allowed**	XMLA: **allowed** Analyze in Excel: **allowed**

Access through the XMLA endpoint will honor security group membership set at the workspace/app level.

Workspace contributors and above have Write semantic model permissions, which are effectively the same as Analysis Services database admins. They can deploy new semantic models from Visual Studio and execute TMSL scripts in SSMS.

Users with Build semantic model permissions are equivalent to Analysis Services database readers. They can connect to and browse semantic models for data consumption and visualization. Row-level security (RLS) rules are honored and they cannot see internal semantic model metadata.

Operations that require Analysis Services server admin permissions (rather than database admin) in general are not supported.

Impersonation

User impersonation by using the EffectiveUserName connection string property is supported when connecting to Premium workspace semantic models. The account specified in EffectiveUserName must be in the tenant's Microsoft Entra ID and must have both **Read** and **Build** permissions for the semantic model being connected to. If the account doesn't have both Read and Build permissions, Power BI can't impersonate the user account. The connection will fail, and an error is returned.

You can also perform impersonation by specifying one or more workspace roles in the Roles connection string property. With the Roles property, you can test downgrading role members with Write permissions to Read permissions. The following Role permissions apply depending on the account of the user signed in:

- If the user performing impersonation *is* a workspace admin, which is effectively the same as a server admin in Analysis Services, they do not need to be a member of any of the specified roles.
- If the user performing impersonation *is not* a workspace admin, they must belong to one or more of the specified roles, otherwise a user not found or no permissions type error is returned.

Model roles

With the XMLA endpoint, roles, role membership, row-level security (RLS), and object-level security (OLS) can be defined for users in the tenant's Microsoft Entra ID. Model roles in Power BI are used only for RLS and OLS. Use the Power BI security model to control permissions beyond RLS and OLS.

For tabular model projects authored in Visual Studio, roles can be defined by using Role Manager in the model designer. For semantic models in Power BI, roles can be defined in Power BI Desktop prior to publishing to the service. Role membership is specified in the Power BI service. SSMS can also be used to create and manage roles. In most cases, role object definitions can be scripted by using TMSL to create or modify the Roles object. TMSL scripts can be executed in SSMS or with the Invoke-ASCmd PowerShell cmdlet.

The following limitations apply when working with roles through the XMLA endpoint:

- The only permission for a role that can be set for semantic models is Read permission. Other permissions are granted using the Power BI security model.
- Service Principals do not work with RLS and OLS, and cannot be added as model role members.
- Build permission for a semantic model is required for read access through the XMLA endpoint, regardless of the existence of semantic model roles.

Setting data source credentials

Metadata specified through the XMLA endpoint can create connections to data sources, but cannot set data source credentials. Instead, credentials can be set in the semantic model settings page in the Power BI Service.

Service principals

Service principals are a Microsoft Entra app registration you create within your tenant to perform unattended resource and service level operations. They're a unique type of user

identity with an app name, application ID, tenant ID, and client secret or certificate for a password. Power BI Premium uses the same service principal functionality as Power BI Embedded.

Service principals can be used with the XMLA endpoint to automate semantic model management tasks such as provisioning workspaces, deploying models, and semantic model refresh with:

- PowerShell
- Azure Automation
- Azure Logic Apps
- Custom client applications

To learn more, see Automate Premium workspace and semantic model tasks with service principals.

Deploy model projects from Visual Studio (SSDT)

Deploying a tabular model project in Visual Studio to a Premium workspace is much the same as deploying to an Azure or SQL Server Analysis Services server. The only differences are in the Deployment Server property specified for the project, and how data source credentials are specified so processing operations can import data from data sources into the new semantic model on the workspace.

To deploy a tabular model project authored in Visual Studio, set the workspace connection URL in the project **Deployment Server** property. In Visual Studio, in **Solution Explorer**, right-click the project > **Properties**. In the **Server** property, paste the workspace connection URL.

When the Deployment Server property is specified, the project can be deployed.

When deployed the first time, a semantic model is created in the workspace by using metadata from the model.bim. As part of the deployment operation, after the semantic model is created in the workspace from model metadata, processing to load data into the semantic model from data sources will fail.

Processing fails because unlike deploying to an Azure or SQL Server Analysis Server instance, where you are prompted for data source credentials as part of the deployment operation, when deploying to a Premium workspace data source credentials cannot be specified as part of the deployment operation. Instead, after metadata deployment has succeeded and the semantic model is created, data source credentials are then specified in the Power BI Service in semantic model settings. In the workspace, select **Semantic models** > **Settings** > **Data source credentials** > **Edit credentials**.

When data source credentials are specified, you can then refresh the semantic model in the Power BI service, configure schedule refresh, or process (refresh) from SQL Server Management Studio to load data into the semantic model.

The deployment **Processing Option** property specified in the project in Visual Studio is observed. However, if a data source has not had credentials specified in the Power BI service, even if the metadata deployment succeeds, processing will fail. You can set the property to **Do Not Process**, preventing any attempts to process as part of the deployment. You might want to set the property back to **Default** because once the data source credentials are specified in the data source settings for the new semantic model, processing as part of subsequent deployment operations will then succeed.

Connect with SSMS

Using SSMS to connect to a workspace is just like connecting to an Azure or SQL Server Analysis Services server. The only difference is you specify the workspace URL in server name, and you must use **Active Directory - Universal with MFA** authentication.

Connect to a workspace by using SSMS

1. In SQL Server Management Studio, select **Connect** > **Connect to Server**.

2. In **Server Type**, select **Analysis Services**. In **Server name**, enter the workspace URL. In **Authentication**, select **Active Directory - Universal with MFA**, and then in **User name**, enter your organizational user ID.

When connected, the workspace is shown as an Analysis Services server, and semantic models in the workspace are shown as databases.

To learn more about using SSMS to script metadata, see:

- Create Analysis Services scripts
- Tabular Model Scripting Language (TMSL)

Semantic model refresh

The XMLA endpoint enables a wide range of scenarios for fine-grain refresh capabilities using SSMS, automation with PowerShell, Azure Automation, and Azure Functions using TOM. For example, you can refresh certain incremental refresh historical partitions without having to reload all historical data.

Unlike configuring refresh in the Power BI service, refresh operations through the XMLA endpoint are not limited to 48 refreshes per day, and the scheduled refresh timeout is not imposed.

Date, time, and status for semantic model refresh operations that include a write transaction through the XMLA endpoint are recorded and shown in semantic model Refresh history.

> **Note**
>
> Refresh operations performed by the XMLA endpoint don't automatically refresh tile caches. Tile caches are only refreshed when a user accesses the report.

Dynamic Management Views (DMV)

Analysis Services DMVs provide visibility of semantic model metadata, lineage, and resource usage. DMVs available for querying in Power BI through the XMLA endpoint are limited to, at most, those that require database-admin permissions. Some DMVs, for example, aren't accessible because they require Analysis Services server-admin permissions.

Power BI Desktop authored semantic models

Enhanced metadata

XMLA write operations on semantic models authored in Power BI Desktop and published to a Premium workspace require enhanced metadata. To learn more, see Enhanced semantic model metadata.

> ⊗ **Caution**
>
> At this time, a write operation on a semantic model authored in Power BI Desktop prevents it from being downloaded back as a PBIX file. Be sure to retain your original PBIX file.

data source declaration

When connecting to data sources and querying data, Power BI Desktop uses Power Query M expressions as inline data source declarations. While supported in Premium workspaces, Power Query M inline data source declaration isn't supported by Azure Analysis Services or SQL Server Analysis Services. Instead, Analysis Services data modeling tools like Visual Studio create metadata using *structured* or *provider* data source declarations. With the XMLA endpoint, Premium also supports structured and provider data sources, but not as part of Power Query M inline data source declarations in Power BI Desktop models. To learn more, see Understanding providers.

Power BI Desktop in live connect mode

Power BI Desktop can connect to a Power BI Premium semantic model using a live connection. Using a live connection, data doesn't need to be replicated locally making it easier for users to consume semantic models. There are two ways users can connect:

- Select **Power BI semantic models**, and then select a semantic model to create a report. This is the **recommended** way for users to connect live to semantic models. This method provides an improved discover experience showing the endorsement level of semantic models. Users don't need to find and keep track of workspace URLs. To find a semantic model, users simply type in the semantic model name or scroll to find the semantic model they're looking for.

- Using **Get Data** > **Analysis Services**, specify a Power BI Premium workspace name as a URL, select **Connect live**, and then in Navigator, select a semantic model. In this case, Power BI Desktop uses the XMLA endpoint to connect live to the semantic model as though it were an Analysis Services data model.

Organizations that have existing reports connected live to Analysis Services data models, and intend to migrate to Premium semantic models only have to change the server name URL in **Transform data** > **Data source settings**.

Audit logs

When applications connect to a workspace, access through XMLA endpoints is logged in the Power BI audit logs with the following operations:

Expand table

Operation friendly name	Operation name
Connected to Power BI semantic model from an external application	ConnectFromExternalApplication
Requested Power BI semantic model refresh from an external application	RefreshDatasetFromExternalApplication
Created Power BI semantic model from an external application	CreateDatasetFromExternalApplication
Edited Power BI semantic model from an external application	EditDatasetFromExternalApplication
Deleted Power BI semantic model from an external application	DeleteDatasetFromExternalApplication

To learn more, see Auditing Power BI.

Considerations and limitations

Default Power BI semantic Models can't be modified using the XMLA endpoint.

Related content

For more information related to this article, see:

- Power BI usage scenarios: Advanced data model management
- Questions? Try asking the Power BI Community
- Suggestions? Contribute ideas to improve Power BI

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Fabric operations

Article • 03/20/2025

Each experience within Microsoft Fabric supports unique operations. An operation's consumption rate is what converts the usage of the experience's raw metrics into Compute Units (CU).

The Microsoft Fabric Capacity Metrics app's compute page provides an overview of your capacity's performance and lists Fabric operations that consume compute resources.

This article lists these operations by experience, and explains how they consume resources within Fabric.

Interactive and background operations

Microsoft Fabric divides operations into two types, *interactive* and *background*. This article lists these operations and explains the difference between them.

Interactive operations

On-demand requests and operations that can be triggered by user interactions with the UI, such as data model queries generated by report visuals, are classified as *interactive* operations. They're usually triggered by user interactions with the UI. For example, an interactive operation is triggered when a user opens a report or selects a slicer in a Power BI report. Interactive operations can also be triggered without interacting with the UI, for example when using SQL Server Management Studio (SSMS) or a custom application to run a DAX query.

Background operations

Longer running operations such as semantic model or dataflow refreshes are classified as *background* operations. They can be triggered manually by a user, or automatically without user interaction. Background operations include scheduled refreshes, interactive refreshes, REST-based refreshes and XMLA-based refresh operations. Users aren't expected to wait for these operations to finish. Instead, they might come back later to check the status of the operations.

How to read this document

Each experience has a table that lists its operations, with the following columns:

- **Operation** – The name of the operation. Visible in the Microsoft Fabric Capacity Metrics app.
- **Description** – A description of the operation.
- **Item** – The item that this operation can apply to. Visible in the Microsoft Fabric Capacity Metrics app.
- **Azure billing meter** – The name of the meter on your Azure bill that shows usage for this operation.
- **Type** – Lists the type of the operation. Operations are classified as interactive or background operations.

When more details regarding the consumption rate are available, a link to the document with this information is provided.

Fabric operations by experience

This section is divided into Fabric experience. Each experience had a table that lists its operations.

> **Important**
>
> Consumption rates are subject to change at any time. Microsoft will use reasonable efforts to provide notice via email or through in-product notification. Changes shall be effective on the date stated in Microsoft's Release Notes or Microsoft Fabric blog. If any change to a Microsoft Fabric Workload Consumption Rate materially increases the Capacity Units (CU) required to use a particular workload, customers might use the cancellation options available for the chosen payment method.

Copilot in Fabric

Copilot operations are listed in this table. You can find the consumption rates for Copilot in Copilot consumption.

Expand table

Operation	Description	Item	Azure billing meter	Type
Copilot in Fabric	Compute cost associated with input prompts and output completion	Multiple	Copilot in Fabric CU	Background

Data Factory

The Data Factory experience contains operations for Dataflows Gen2 and Pipelines.

Dataflows Gen2

You can find the consumption rates for Dataflows Gen2 in Dataflow Gen2 pricing for Data Factory in Microsoft Fabric.

Expand table

Operation	Description	Item	Azure billing meter	Type
Dataflow Gen2 Refresh	Compute cost associated with dataflow Gen2 refresh operation	Dataflow Gen2	Dataflows Standard Compute Capacity Usage CU	Background
High Scale Dataflow Compute - SQL Endpoint Query	Usage related to the dataflow Gen2 staging warehouse SQL endpoint	Warehouse	High Scale Dataflow Compute Capacity Usage CU	Background

Pipelines

You can find the consumption rates for Pipelines in Data pipelines pricing for Data Factory in Microsoft Fabric.

Expand table

Operation	Description	Item	Azure billing meter	Type
DataMovement	The amount of time used by the copy activity in a Data Factory pipeline divided by the number of data integration units	Pipeline	Data Movement Capacity Usage CU	Background
ActivityRun	A Data Factory data pipeline activity execution	Pipeline	Data Orchestration Capacity Usage CU	Background

Databases

One Fabric capacity unit = 0.383 SQL database vCores.

Expand table

Operation	Description	Item	Azure Billing Meter	Type
SQL Usage	Compute for all user-generated and system-generated SQL queries, modifications, and data processing operations within a database	Database	SQL database in Microsoft Fabric Capacity Usage CU	Interactive
Allocated SQL Storage	The dynamically allocated storage space for a SQL database in Fabric, used for storing tables, indexes, transaction logs, and metadata. Fully integrated with OneLake.	Database	SQL Storage Data Stored	Background

Data Warehouse

One Fabric Data Warehouse core (unit of compute for Data Warehouse) is equivalent to two Fabric Capacity Units (CUs).

Expand table

Operation	Description	Item	Azure billing meter	Type
Warehouse Query	Compute charge for all user generated and system generated T-SQL statements within a Warehouse	Warehouse	Data Warehouse Capacity Usage CU	Background
SQL Endpoint Query	Compute charge for all user generated and system generated T-SQL statements within the SQL analytics endpoint of a Lakehouse	Warehouse	Data Warehouse Capacity Usage CU	Background

Fabric API for GraphQL

GraphQL operations are made up of requests performed on API for GraphQL items by API clients. Each GraphQL request and response operation processing time is reported in Capacity Units (CUs) in seconds at the rate of ten CUs per hour.

Expand table

Operation	Description	Item	Azure billing meter	Type
Query	Compute charge for all generated GraphQL queries (reads) and mutations (writes) by clients within a GraphQL API	GraphQL	API for GraphQL Query Capacity Usage CU	Interactive

OneLake

One Lake compute operations represent the transactions performed on One Lake items. The consumption rate for each operation varies depending on its type. For more details, refer to One Lake consumption.

Expand table

Operation	Description	Item	Azure Billing Meter	Type
OneLake Read via Redirect	OneLake Read via Redirect	Multiple	OneLake Read Operations Capacity Usage CU	Background
OneLake Read via Proxy	OneLake Read via Proxy	Multiple	OneLake Read Operations via API Capacity Usage CU	Background
OneLake Write via Redirect	OneLake Write via Redirect	Multiple	OneLake Write Operations Capacity Usage CU	Background
OneLake Write via Proxy	OneLake Write via Proxy	Multiple	OneLake Write Operations via API Capacity Usage CU	Background
OneLake Iterative Write via Redirect	OneLake Iterative Write via Redirect	Multiple	OneLake Iterative Write Operations	Background
OneLake Iterative Read via Redirect	OneLake Iterative Read via Redirect	Multiple	OneLake Iterative Read Operations Capacity Usage CU	Background
OneLake Other Operations	OneLake Other Operations	Multiple	OneLake Other Operations	Background

Operation	Description	Item	Azure Billing Meter	Type
			Capacity Usage CU	
OneLake Other Operations via Redirect	OneLake Other Operations via Redirect	Multiple	OneLake Other Operations via API Capacity Usage CU	Background
OneLake Iterative Write via Proxy	OneLake Iterative Write via Proxy	Multiple	OneLake Iterative Write Operations via API Capacity Usage CU	Background
OneLake Iterative Read via Proxy	OneLake Iterative Read via Proxy	Multiple	OneLake Iterative Read Operations via API Capacity Usage CU	Background
OneLake BCDR Read via Proxy	OneLake BCDR Read via Proxy	Multiple	OneLake BCDR Read Operations via API Capacity Usage CU	Background
OneLake BCDR Write via Proxy	OneLake BCDR Write via Proxy	Multiple	OneLake BCDR Write Operations via API Capacity Usage CU	Background
OneLake BCDR Read via Redirect	OneLake BCDR Read via Redirect	Multiple	OneLake BCDR Read Operations Capacity Usage CU	Background
OneLake BCDR Write via Redirect	OneLake BCDR Write via Redirect	Multiple	OneLake BCDR Write Operations Capacity Usage CU	Background

Operation	Description	Item	Azure Billing Meter	Type
OneLake BCDR Iterative Read via Proxy	OneLake BCDR Iterative Read via Proxy	Multiple	OneLake BCDR Iterative Read Operations via API Capacity Usage CU	Background
OneLake BCDR Iterative Read via Redirect	OneLake BCDR Iterative Read via Redirect	Multiple	OneLake BCDR Iterative Read Operations Capacity Usage CU	Background
OneLake BCDR Iterative Write via Proxy	OneLake BCDR Iterative Write via Proxy	Multiple	OneLake BCDR Iterative Write Operations via API Capacity Usage CU	Background
OneLake BCDR Iterative Write via Redirect	OneLake BCDR Iterative Write via Redirect	Multiple	OneLake BCDR Iterative Write Operations Capacity Usage CU	Background
OneLake BCDR Other Operations	OneLake BCDR Other Operations	Multiple	OneLake BCDR Other Operations Capacity Usage CU	Background
OneLake BCDR Other Operations Via Redirect	OneLake BCDR Other Operations Via Redirect	Multiple	OneLake BCDR Other Operations via API Capacity Usage CU	Background

Power BI

The usage for each operation is reported in CU processing time in seconds. Eight CUs are equivalent to one Power BI v-core.

> **Note**
>
> The term *Semantic model* replaces the term *dataset*. You may still see the old term in the UI until it is completely replaced.
>
> We currently don't bill for R/Py visuals in Power BI.

Expand table

Operation	Description	Item	Azure billing meter	Type
Artificial intelligence (AI)	AI function evaluation	AI	Power BI Capacity Usage CU	Interactive
Background query	Queries for refreshing tiles and creating report snapshots	Semantic model	Power BI Capacity Usage CU	Background
Dataflow DirectQuery	Connect directly to a dataflow without the need to import the data into a semantic model	Dataflow Gen1	Power BI Capacity Usage CU	Interactive
Dataflow refresh	An on-demand or scheduled background dataflow refresh, performed by the service or with REST APIs.	Dataflow Gen1	Power BI Capacity Usage CU	Background
Semantic model on-demand refresh	A background semantic model refresh initiated by the user, using the service, REST APIs, or public XMLA endpoints	Semantic model	Power BI Capacity Usage CU	Background
Semantic model scheduled refresh	A scheduled background semantic model refresh, performed by the service, REST APIs, or public XMLA endpoints	Semantic model	Power BI Capacity Usage CU	Background
Full report email subscription	A PDF or PowerPoint copy of an entire Power BI report, attached to an email subscription	Report	Power BI Capacity Usage CU	Background
Interactive query	Queries initiated by an on-demand data request. For example, loading a model when opening a report, user interaction with a report, or querying a dataset before rendering. Loading a semantic model might be reported as a standalone interactive query operation.	Semantic model	Power BI Capacity Usage CU	Interactive
PublicApiExport	A Power BI report exported with the export report to file REST API	Report	Power BI Capacity Usage CU	Background
Render	A Power BI paginated report exported with the export paginated report to file REST API	Paginated report	Power BI Capacity Usage CU	Background
Render	A Power BI paginated report viewed in Power BI service	Paginated report	Power BI Capacity Usage CU	Interactive

Operation	Description	Item	Azure billing meter	Type
Web modeling read	A data model read operation in the semantic model web modeling user experience	Semantic model	Power BI Capacity Usage CU	Interactive
Web modeling write	A data model write operation in the semantic model web modeling user experience	Semantic model	Power BI Capacity Usage CU	Interactive
XMLA read	XMLA read operations initiated by the user, for queries and discoveries	Semantic model	Power BI Capacity Usage CU	Interactive
XMLA write	A background XMLA write operation that changes the model	Semantic model	Power BI Capacity Usage CU	Background
Power BI scripting visual execution	R and Py visuals run triggered by rendering Power BI report	Power BI scripting report	Spark memory optimized capacity (CU)	Interactive

Real-Time Intelligence

The Real-Time Intelligence experience contains operations for Eventstream, Fabric events and KQL Database and KQL Queryset.

Eventstream

You can find the consumption rates for Eventstream in Monitor capacity consumption for Microsoft Fabric Eventstream.

Expand table

Operation	Description	Item	Azure billing meter	Type
Eventstream Per Hour	Flat charge	Eventstream	Eventstream Capacity Usage CU	Background
Eventstream Data Traffic per GB	Data ingress & egress volume in default and derived streams (Includes 24-hour retention)	Eventstream	Eventstream Data Traffic Capacity Usage CU	Background
Eventstream Processor Per Hour	Computing resources consumed by the processor	Eventstream	Eventstream Processor Capacity Usage CU	Background
Eventstream Connectors Per vCore Hour	Computing resources consumed by the connectors	Eventstream	Eventstream Connector Capacity Usage CU	Background

Fabric events

You can find the consumption rates for Fabric events in Microsoft Fabric and Azure events capacity consumption.

Expand table

Operation	Description	Item	Azure billing meter	Type
Event Operations	Publish, delivery, and filtering operations	Multiple	Real-Time Intelligence - Event Operations	Background
Event Listener	Uptime of the event listener	Multiple	Real-Time Intelligence – Event Listener and Alert	Background

KQL Database and KQL Queryset

You can find the consumption rates for KQL Database in KQL Database consumption.

Expand table

Operation	Description	Item	Azure billing meter	Type
Eventhouse UpTime	Measure of the time that Eventhouse is Active	Eventhouse	Eventhouse Capacity Usage CU	Background

Spark

Two Spark VCores (a unit of computing power for Spark) equals one capacity unit (CU). To understand how Spark operations consume CUs, refer to spark pools.

Expand table

Operation	Description	Item	Azure billing meter	Type
Lakehouse operations	Users preview table in the Lakehouse explorer	Lakehouse	Spark Memory Optimized Capacity Usage CU	Background
Lakehouse table load	Users load delta table in the Lakehouse explorer	Lakehouse	Spark Memory Optimized Capacity Usage CU	Background
Notebook run	Notebook run manually by users	Notebook	Spark Memory Optimized Capacity Usage CU	Background
Notebook HC run	Notebook run under the high concurrency Spark session	Notebook	Spark Memory Optimized Capacity Usage CU	Background
Notebook scheduled run	Notebook run triggered by notebook scheduled events	Notebook	Spark Memory Optimized Capacity Usage CU	Background
Notebook pipeline run	Notebook run triggered by pipeline	Notebook	Spark Memory Optimized Capacity Usage CU	Background
Notebook VS Code run	Notebook runs in VS Code.	Notebook	Spark Memory Optimized Capacity Usage CU	Background
Spark job run	Spark batch job runs initiated by user submission	Spark Job Definition	Spark Memory Optimized Capacity Usage CU	Background
Spark job scheduled run	Batch job runs triggered by notebook scheduled events	Spark Job Definition	Spark Memory Optimized Capacity Usage CU	Background

Operation	Description	Item	Azure billing meter	Type
Spark job pipeline run	Batch job runs triggered by pipeline	Spark Job Definition	Spark Memory Optimized Capacity Usage CU	Background
Spark job VS Code run	Spark job definition submitted from VS Code	Spark Job Definition	Spark Memory Optimized Capacity Usage CU	Background

Related content

- What is the Microsoft Fabric Capacity Metrics app?
- Understand the metrics app compute page

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Troubleshoot XMLA endpoint connectivity

Article • 10/29/2024

XMLA endpoints in Power BI rely on the native Analysis Services communication protocol for access to Power BI semantic models. Because of this, XMLA endpoint troubleshooting is much the same as troubleshooting a typical Analysis Services connection. However, some differences around Power BI-specific dependencies apply.

Before you begin

Before troubleshooting an XMLA endpoint scenario, be sure to review the basics covered in Semantic model connectivity with the XMLA endpoint. Most common XMLA endpoint use cases are covered there. Other Power BI troubleshooting guides, such as Troubleshoot gateways - Power BI and Troubleshooting Analyze in Excel, can also be helpful.

Enabling the XMLA endpoint

The XMLA endpoint can be enabled on both Power BI Premium, Premium Per User, and Power BI Embedded capacities. On smaller capacities, such as an A1 capacity with only 2.5 GB of memory, you might encounter an error in Capacity settings when trying to set the XMLA Endpoint to **Read/Write** and then selecting **Apply**. The error states "There was an issue with your workload settings. Try again in a little while.".

Here are a couple things to try:

- Limit the memory consumption of other services on the capacity, such as Dataflows, to 40% or less, or disable an unnecessary service completely.
- Upgrade the capacity to a larger SKU. For example, upgrading from an A1 to an A3 capacity solves this configuration issue without having to disable Dataflows.

Keep in-mind, you must also enable the tenant-level Export data setting in the Power BI Admin Portal. This setting is also required for the Analyze in Excel feature.

Establishing a client connection

After enabling the XMLA endpoint, it's a good idea to test connectivity to a workspace on the capacity. To learn more, see Connecting to a Premium workspace. Also, be sure to read the section Connection requirements for helpful tips and information about current XMLA connectivity limitations.

Connecting with a service principal

If you've enabled tenant settings to allow service principals to use Power BI APIs, as described in Enable service principals, you can connect to an XMLA endpoint by using a service principal. Keep in mind the service principal requires the same level of access permissions at the workspace or semantic model level as regular users.

To use a service principal, be sure to specify the application identity information in the connection string as:

- **User ID** - *app:appid@tenantid*
- **Password**
  - *cert:thumbprint* (recommended for security)

    ```
    Data Source=powerbi://api.powerbi.com/v1.0/myorg/Contoso;Initial Catalog=PowerBI_Dataset;User ID=app:<appid>;Password=cert:<thumbprint>;
    ```

  - *application secret*

    ```
    Data Source=powerbi://api.powerbi.com/v1.0/myorg/Contoso;Initial Catalog=PowerBI_Dataset;User ID=app:<appid>;Password=<secret>;
    ```

If you receive the following error:

"We cannot connect to the semantic model due to incomplete account information. For service principals, make sure you specify the tenant ID together with the app ID using the format app:<appId>@<tenantId>, then try again."

Make sure you specify the tenant ID together with the app ID using the correct format.

It's also valid to specify the app ID without the tenant ID. However, in this case, you must replace the `myorg` alias in the data source URL with the actual tenant ID. Power BI can then locate the service principal in the correct tenant. But, as a best practice, use the `myorg` alias and specify the tenant ID together with the app ID in the User ID parameter.

Connecting with Microsoft Entra B2B

With support for Microsoft Entra business-to-business (B2B) in Power BI, you can provide external guest users with access to semantic models over the XMLA endpoint. Make sure the Share content with external users setting is enabled in the Power BI Admin portal. To learn more, see Distribute Power BI content to external guest users with Microsoft Entra B2B.

Deploying a semantic model

You can deploy a tabular model project in Visual Studio (SSDT) to a workspace assigned to a Premium capacity, much the same as to a server resource in Azure Analysis Services. However,

when deploying there are some additional considerations. Be sure to review the section Deploy model projects from Visual Studio (SSDT) in the semantic model connectivity with the XMLA endpoint article.

Deploying a new model

In the default configuration, Visual Studio attempts to process the model as part of the deployment operation to load data into the semantic model from the data sources. As described in Deploy model projects from Visual Studio (SSDT), this operation can fail because data source credentials cannot be specified as part of the deployment operation. Instead, if credentials for your data source aren't already defined for any of your existing semantic models, you must specify the data source credentials in the semantic model settings using the Power BI user interface (**Semantic models** > **Settings** > **Data source credentials** > **Edit credentials**). Having defined the data source credentials, Power BI can then apply the credentials to this data source automatically for any new semantic model, after metadata deployment has succeeded and the semantic model has been created.

If Power BI cannot bind your new semantic model to data source credentials, you will receive an error stating "Cannot process database. Reason: Failed to save modifications to the server." with the error code "DMTS_DatasourceHasNoCredentialError", as shown below:

To avoid the processing failure, set the **Deployment Options** > **Processing Options** to **Do not Process**, as shown in the following image. Visual Studio then deploys only metadata. You can then configure the data source credentials, and click on **Refresh now** for the semantic model in the Power BI user interface.

New project from an existing semantic model

Creating a new tabular project in Visual Studio by importing the metadata from an existing semantic model is not supported. However, you can connect to the semantic model by using SQL Server Management Studio, script out the metadata, and reuse it in other tabular projects.

Migrating a semantic model to Power BI

It's recommended you specify the 1500 (or higher) compatibility level for tabular models. This compatibility level supports the most capabilities and data source types. Later compatibility levels are backwards compatible with earlier levels.

Supported data providers

At the 1500 compatibility level, Power BI supports the following data source types:

- Provider data sources (legacy with a connection string in the model metadata).
- Structured data sources (introduced with the 1400 compatibility level).

- Inline M declarations of data sources (as Power BI Desktop declares them).

It's recommended you use structured data sources, which Visual Studio creates by default when going through the Import data flow. However, if you are planning to migrate an existing model to Power BI that uses a provider data source, make sure the provider data source relies on a supported data provider. Specifically, the Microsoft OLE DB Driver for SQL Server and any third-party ODBC drivers. For OLE DB Driver for SQL Server, you must switch the data source definition to the .NET Framework Data Provider for SQL Server. For third-party ODBC drivers that might be unavailable in the Power BI service, you must switch to a structured data source definition instead.

It's also recommended you replace the outdated Microsoft OLE DB Driver for SQL Server (SQLNCLI11) in your SQL Server data source definitions with the .NET Framework Data Provider for SQL Server.

The following table provides an example of a .NET Framework Data Provider for SQL Server connection string replacing a corresponding connection string for the OLE DB Driver for SQL Server.

Expand table

OLE DB Driver for SQL Server	.NET Framework Data Provider for SQL Server
`Provider=SQLNCLI11;Data Source=sqldb.database.windows.net;Initial Catalog=AdventureWorksDW;Trusted_Connection=yes;`	`Data Source=sqldb.database.windows.net;Initial Catalog=AdventureWorksDW2016;Integrated Security=SSPI;Encrypt=true;TrustServerCertificate=false`

Cross-referencing partition sources

Just as there are multiple data source types, there are also multiple partition source types a tabular model can include to import data into a table. Specifically, a partition can use a query partition source or an M partition source. These partition source types, in turn, can reference provider data sources or structured data sources. While tabular models in Azure Analysis Services support cross-referencing these various data source and partition types, Power BI enforces a more strict relationship. Query partition sources must reference provider data sources, and M partition sources must reference structured data sources. Other combinations are not supported in Power BI. If you want to migrate a cross-referencing semantic model, the following table describes supported configurations:

Expand table

Data source	Partition source	Comments	Supported with XMLA endpoint
Provider data source	Query partition	The AS engine uses the cartridge-based connectivity stack to access the data source.	Yes

Data source	Partition source	Comments	Supported with XMLA endpoint
	source		
Provider data source	M partition source	The AS engine translates the provider data source into a generic structured data source and then uses the Mashup engine to import the data.	No
Structured data source	Query partition source	The AS engine wraps the native query on the partition source into an M expression and then uses the Mashup engine to import the data.	No
Structured data source	M partition source	The AS engine uses the Mashup engine to import the data.	Yes

Data sources and impersonation

Impersonation settings you can define for provider data sources are not relevant for Power BI. Power BI uses a different mechanism based on semantic model settings to manage data source credentials. For this reason, make sure you select **Service Account** if you are creating a Provider Data Source.

Fine-grained processing

When triggering a scheduled refresh or on-demand refresh in Power BI, Power BI typically refreshes the entire semantic model. In many cases, it's more efficient to perform refreshes more selectively. You can perform fine-grained processing tasks in SQL Server Management Studio (SSMS) as shown below, or by using third-party tools or scripts.

Overrides in Refresh TMSL command

Overrides in Refresh command (TMSL) allow users choosing a different partition query definition or data source definition for the refresh operation.

Email subscriptions

Semantic models that are refreshed using an XMLA endpoint don't trigger an email subscription.

Errors on Premium capacity

Connect to Server error in SSMS

When connecting to a Power BI workspace with SQL Server Management Studio (SSMS), the following error may be displayed:

```
TITLE: Connect to Server
------------------------------
Cannot connect to powerbi://api.powerbi.com/v1.0/[tenant name]/[workspace name].
------------------------------
ADDITIONAL INFORMATION:
The remote server returned an error: (400) Bad Request.
Technical Details:
RootActivityId:
Date (UTC): 10/6/2021 1:03:25 AM (Microsoft.AnalysisServices.AdomdClient)
------------------------------
The remote server returned an error: (400) Bad Request. (System)
```

When connecting to a Power BI workspace with SSMS, ensure the following:

- The XMLA endpoint setting is enabled for your tenant's capacity. To learn more, see Enable XMLA read-write.
- The Allow XMLA endpoints and Analyze in Excel with on-premises semantic models setting is enabled in Tenant settings.
- You're using the latest version of SSMS. Download the latest.

Query execution in SSMS

When connected to a workspace in a Power BI Premium or a Power BI Embedded capacity, SQL Server Management Studio may display the following error:

```
Executing the query ...
Error -1052311437: We had to move the session with ID '<Session ID>' to another
Power BI Premium node. Moving the session temporarily interrupted this trace -
tracing will resume automatically as soon as the session has been fully moved to
the new node.
```

This is an informational message that can be ignored in SSMS 18.8 and higher because the client libraries will reconnect automatically. Note that client libraries installed with SSMS v18.7.1 or lower do not support session tracing. Download the latest SSMS.

Executing a large command using the XMLA endpoint

When executing a large command using the XMLA endpoint, you may encounter the following error:

```
Executing the query ...
Error -1052311437:
The remote server returned an error: (400) Bad Request.

Technical Details:
RootActivityId: 3716c0f7-3d01-4595-8061-e6b2bd9f3428
Date (UTC): 11/13/2020 7:57:16 PM
Run complete
```

When using SSMS v18.7.1 or lower to perform a long running (>1 min) refresh operation on a semantic model in a Power BI Premium or a Power BI Embedded capacity, SSMS may display this error even though the refresh operation succeeds. This is due to a known issue in the client libraries where the status of the refresh request is incorrectly tracked. This is resolved in SSMS 18.8 and higher. Download the latest SSMS.

This error can also occur when a very large request needs to be redirected to a different node in the Premium cluster. It's often seen when you try to create or alter a semantic model using a large TMSL script. In such cases, the error can usually be avoided by specifying the Initial Catalog to the name of the database before executing the command.

When creating a new database, you can create an empty semantic model, for example:

JSON

```
{
  "create": {
    "database": {
      "name": "DatabaseName"
    }
  }
}
```

After you create the new semantic model, specify the Initial Catalog and then make changes to the semantic model.

Other client applications and tools

Client applications and tools such as Excel, Power BI Desktop, SSMS, or external tools connecting to and working with semantic models in Power BI Premium capacities may cause the following error: **The remote server returned an error: (400) Bad Request.**. The error can be caused especially if an underlying DAX query or XMLA command is long running. To mitigate potential errors, be sure to use the most recent applications and tools that install recent versions of the Analysis Services client libraries with regular updates. Regardless of

application or tool, the minimum required client library versions to connect to and work with semantic models in a Premium capacity through the XMLA endpoint are:

Expand table

Client Library	Version
MSOLAP	15.1.65.22
AMO	19.12.7.0
ADOMD	19.12.7.0

Editing role memberships in SSMS

When using the SQL Server Management Studio (SSMS) v18.8 to edit a role membership on a semantic model, SSMS may display the following error:

```
Failed to save modifications to the server.
Error returned: ‘Metadata change of current operation cannot be resolved, please
check the command or try again later.’
```

This is due to a known issue in the app services REST API. This will be resolved in an upcoming release. In the meantime, to get around this error, in **Role Properties**, click **Script**, and then enter and execute the following TMSL command:

JSON

```
{
  "createOrReplace": {
    "object": {
      "database": "AdventureWorks",
      "role": "Role"
    },
    "role": {
      "name": "Role",
      "modelPermission": "read",
      "members": [
        {
          "memberName": "xxxx",
          "identityProvider": "AzureAD"
        },
        {
          "memberName": “xxxx”
          "identityProvider": "AzureAD"
        }
      ]
    }
```

```
    }
  }
```

Publish Error - Live connected semantic model

When republishing a live connected semantic model utilizing the Analysis Services connector, the following error, "**There is an existing report/semantic model with the same name. Please delete or rename the existing semantic model and retry.**" may be shown.

This is due to the semantic model being published having a different connection string but having the same name as the existing semantic model. To resolve this issue, either delete or rename the existing semantic model. Also be sure to republish any apps that are dependent on the report. If necessary, downstream users should be informed to update any bookmarks with the new report address to ensure they access the latest report.

Live connected semantic model cannot be loaded

Users trying to create a new Live Connected model or open an existing Live Connected model, using the March 2024 or later versions of Power BI Desktop, may encounter an error similar to the following: "***We couldn't connect to your model in the Power BI service. The dataset may have been deleted, renamed, moved, or it is possible that you don't have permission to access it.***"

The error may occur when a proxy is configured in the user's environment and the proxy is preventing access to the Power BI service. Beginning with the March 2024 version of Power BI Desktop, the user's environment must allow connections to the Power BI service at endpoint ***.pbidedicated.windows.net** or the corresponding Power BI service endpoints for sovereign clouds.

To validate whether the issue is a result of proxy settings, try the **SQL Server Analysis Services** connector in Power BI Desktop or any first-party or third-party external tool, such as **SQL Server Management Studio**, to connect to any premium workspace.

Refer to the establishing a client connection section in this article for more information about testing general XML/A connectivity.

Excel workbook fails to open

Excel workbook might fail to open with error, "**Initialization of the data source failed. Check the database server or contact your database administrator.**". If the workbook contains a connection to a Power BI semantic model, then check if the connection string contains the property "**Catalog Rebound=True**". If the property is found, remove it, save the workbook, and try opening it again.

The "**Catalog Rebound=True**" property is automatically added by the Analysis Services OLE DB Provider (MSOLAP) in newer versions of Excel when the connection to Power BI semantic model is optimized by the provider. Because the property is persisted to the workbook, when the same workbook is opened in Excel that's using an older version of the provider that doesn't support the optimization, then Excel will fail to open the workbook.

"**Catalog Rebound**" is meant for internal use only.

Workspace/server alias

Unlike Azure Analysis Services, server name aliases **are not supported** for Premium workspaces.

DISCOVER_M_EXPRESSIONS

The DMV DISCOVER_M_EXPRESSIONS data management view (DMV) is currently not supported in Power BI using the XMLA Endpoint. Applications can use the Tabular object model (TOM) to obtain M expressions used by the data model.

Resource governing command memory limit in Premium

Premium capacities use resource governing to ensure no single semantic model operation can exceed the amount of available memory resources for the capacity - determined by SKU. For example, a P1 subscription has an *effective memory limit* per item of 25 GB, for a P2 subscription the limit is 50 GB, and for a P3 subscription the limit is 100 GB. In addition to semantic model (database) size, the effective memory limit also applies to underlying semantic model command operations like Create, Alter, and Refresh.

The effective memory limit for a command is based on the lesser of the capacity's memory limit (determined by SKU) or the value of the DbpropMsmdRequestMemoryLimit XMLA property.

For example, for a P1 capacity, if:

- DbpropMsmdRequestMemoryLimit = 0 (or unspecified), the effective memory limit for the command is 25 GB.
- DbpropMsmdRequestMemoryLimit = 5 GB, the effective memory limit for the command is 5 GB.
- DbpropMsmdRequestMemoryLimit = 50 GB, the effective memory limit for the command is 25 GB.

Typically, the effective memory limit for a command is calculated on the memory allowed for the semantic model by the capacity (25 GB, 50 GB, 100 GB) and how much memory the semantic model is already consuming when the command starts executing. For example, a semantic model using 12 GB on a P1 capacity allows an effective memory limit for a new command of 13 GB. However, the effective memory limit can be further constrained by the DbPropMsmdRequestMemoryLimit XMLA property when optionally specified by an application. Using the previous example, if 10 GB is specified in the

DbPropMsmdRequestMemoryLimit property, then the command's effective limit is further reduced to 10 GB.

If the command operation attempts to consume more memory than allowed by the limit, the operation can fail, and an error is returned. For example, the following error describes an effective memory limit of 25 GB (P1 capacity) has been exceeded because the semantic model already consumed 12 GB (12288 MB) when the command started execution, and an effective limit of 13 GB (13312 MB) was applied for the command operation:

"Resource governing: This operation was canceled because there wasn't enough memory to finish running it. Either increase the memory of the Premium capacity where this semantic model is hosted or reduce the memory footprint of your semantic model by doing things like limiting the amount of imported data. More details: consumed memory 13312 MB, memory limit 13312 MB, database size before command execution 12288 MB. Learn more: `https://go.microsoft.com/fwlink/?linkid=2159753`."

In some cases, as shown in the following error, "consumed memory" is 0 but the amount shown for "database size before command execution" is already greater than the effective memory limit. This means the operation failed to begin execution because the amount of memory already used by the semantic model is greater than the memory limit for the SKU.

"Resource governing: This operation was canceled because there wasn't enough memory to finish running it. Either increase the memory of the Premium capacity where this semantic model is hosted or reduce the memory footprint of your semantic model by doing things like limiting the amount of imported data. More details: consumed memory 0 MB, memory limit 25600 MB, database size before command execution 26000 MB. Learn more: `https://go.microsoft.com/fwlink/?linkid=2159753`."

To potentially avoid exceeding the effective memory limit:

- Upgrade to a larger Premium capacity (SKU) size for the semantic model.
- Reduce the memory footprint of your semantic model by limiting the amount of data loaded with each refresh.
- For refresh operations through the XMLA endpoint, reduce the number of partitions being processed in parallel. Too many partitions being processed in parallel with a single command can exceed the effective memory limit.

Related content

- Semantic model connectivity with the XMLA endpoint
- Automate Premium workspace and semantic model tasks with service principals
- Troubleshooting Analyze in Excel
- Tabular model solution deployment

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Power BI Premium FAQ

FAQ

Power BI Premium transitioned to Microsoft Fabric. Learn about the transition and its impact.

Power BI Premium transition to Microsoft Fabric

What's Microsoft Fabric?

Microsoft Fabric is a platform that allows users to get, create, share, and visualize data using an array of tools. Power BI is a visualization tool, and is one of Fabric's experiences.

What's Power BI Premium per capacity?

Power BI Premium per capacity is another name for Power BI Premium. Power BI requires two types of licenses, a *per capacity* license and a *per user license*. For this reason, Power BI Premium is sometimes referred to as Power BI Premium per capacity.

What's happening to Power BI Premium?

Power BI Premium transitioned to Microsoft Fabric. Power BI Premium is now part of Fabric. You can use Power BI in Fabric alongside all the other Fabric workloads. Because of this change, the Power BI Premium SKUs are being retired.

Can I use Power BI without Fabric?

Power BI is part of the Fabric platform. To use Power BI without any of the other Fabric experiences, disable the *Users can create Fabric items* tenant switch.

Can I buy Power BI Premium?

No. P SKUs are no longer available for purchase they can only be renewed. To use the Power BI Premium features, you need to buy an F SKU. Purchasing an F SKU allows you to use all the Fabric features and the Power BI Premium features. You can read more about this transition in the Power BI Premium P SKU.

How do I buy Microsoft Fabric?

To buy Fabric, start with the Microsoft Fabric pricing page.

How do I renew a P SKU?

At the time of your next contract renewal, talk to your Microsoft representative about renewing your contract using an F SKU instead of your P SKU.

I'm using Power BI Premium, how does the transition impact me?

At the end of your current agreement with Microsoft, work with your Microsoft account representatives to migrate your P SKU purchase to an F SKU purchase. No immediate action is required. You can continue using your existing Power BI Premium capacity until the time of your next renewal.

How do I migrate my Power BI Premium content to Fabric?

To transfer your content to Fabric, you need to reassign your workspaces to a Fabric capacity. Workspaces can be assigned to a new capacity in the admin portal or the workspace pane. To accelerate the transfer process, admins can reassign workspaces to a Fabric capacity in bulk.

If I take no action, is my Power BI Premium capacity be automatically converted to a Fabric capacity?

No. Work with your Microsoft account representative to buy a Fabric capacity at the time of your next renewal. Then reassign your workspaces to the new Fabric capacity.

What happens to my Fabric and Power BI items once I cancel my P SKU capacity and purchase an F SKU capacity?

You can access your Power BI items for 90 days after your P SKU capacity subscription ends. During these 90 days, migrate your workspaces to your new F SKU capacity

without losing access to your existing work. However, once the workspace is reassigned, all currently active jobs are canceled. Rerun those jobs after migration. Migration doesn't impact scheduled jobs.

Is Power BI Embedded included with Fabric's F SKUs?

Yes, when you buy an F SKU you also get Power BI Embedded.

How do P SKUs compare to F SKUs?

Stock Keeping Units (SKUs) indicate how much compute power your capacity has. You can find a comparison between P and F SKUs in Capacity license.

How do I know what F SKU size I need?

To estimate the size of the capacity you need, work with your Microsoft account representatives. Your representatives can recommend which SKU to buy, according to your current consumption. You can use a Fabric trial to measure your capacity consumption. The Microsoft Fabric Capacity Metrics app can help you analyze your capacity's consumption.

Do I need a Power BI Pro license with Fabric?

To create Power BI reports and consume content, you need a Power BI Pro license. With an F64 or higher SKU, you can view content with a Microsoft Fabric free license, if the content is in the capacity. Fabric items that aren't Power BI items, don't require a Pro license. For more information about user licenses in Fabric, see Per user licenses.

How can I continue to access Power BI Report Server without P SKUs?

Power BI Report Server is available through two different licenses: Fabric reserved license and SQL Server Enterprise Edition with Software Assurance.

What are the key differences between F SKUs and P SKUs?

This table lists the key differences between F SKUs and P SKUs.

Expand table

Capability	P1 or higher	F64 or higher
Commitment	Monthly or yearly	Monthly, yearly and pay as you go
Pricing	Global	Regional
Power BI Report Server	Included	Included with a reserved license
Power BI Embedded	Included when buying EM SKUs	Included
Azure features*	Not included	Included

* Fabric has Azure features such Trusted workspace access and Managed Private Endpoint that are only available with F SKUs.

Power BI Premium operations

How can I control the costs of autoscaling?

Autoscaling is an optional feature of Power BI Premium, and is subject to two limits, each if which is configured by Power BI administrators:

- **Proactive limit** - a proactive limit sets the rate of expenses that Autoscale can generate, by limiting the number of autoscale v-cores a capacity can use. For example, by setting a maximum autoscale of v-cores to one v-core, you ensure that the maximum charge you can incur is 30 days of autoscaling with one v-core.
- **Reactive limit** - you can also set a reactive limit to the cost for autoscaling, by setting an expenditure limit on the Azure subscription used with autoscale. To set a reactive limit, do the following:
  - Set an Azure Policy to restrict the resource group to resources of type `microsoft.powerbidedicated/autoscalevcores` only.

- Create an Action Group within your Azure budget which calls a custom Azure PowerShell Runbook to get and delete all resources in the resource group.

How does resource utilization cause Premium to autoscale?

Power BI Premium evaluates your level of utilization by aggregating utilization records every 30 seconds. Each evaluation is composed of two different aggregations: *Interactive utilization* and *background utilization*.

Interactive utilization is evaluated by considering all the interactive operations that completed on or near the current half-minute evaluation cycle.

Background utilization is evaluated by considering all the background operations that completed during the past 24 hours, where each background operation contributes only 1/2,880 of its total CPU cost (there are 2,880 evaluation cycles in each 24-hour period).

A capacity consists of a defined number of v-cores. The Microsoft Fabric Capacity Metrics app tracks the utilization of your capacity v-cores. The CPU usage reported in the app drives the need to autoscale.

If you have a P1 subscription with eight v-cores, each evaluation cycle quota is 240 (8 × 30) seconds of CPU utilization. If the sum of both utilizations exceeds the total v-quota in your capacity, your capacity autoscales using an additional v-core for the next 24 hours.

Autoscale always looks at your current capacity size to evaluate how much resource you use. If you autoscaled using one v-core, your maximum capacity is now at 270 (240 + 1 × 30) seconds of CPU time in an evaluation cycle.

Autoscale always makes sure that no single interactive operation can consume all of your capacity, and you must have two or more interactive operations taking place in a single evaluation cycle to initiate autoscale.

What happens to traffic during overload if I don't autoscale?

During overload, if you don't autoscale throttling is applied.

How is the overload score calculated?

Overload events that take place in the middle of the day are likely to affect many users. Overload events that take place in the middle of the night will probably affect only a handful of users. The overload score is designed to help you differentiate between these two overload events, so that you can single out the Power BI items (such as reports and datasets) that most impact your users.

The overload score is calculated in two steps:

1. The amount of CPU seconds belonging to interactive queries affected by an overload event is summed.

2. The value form step 1 is multiplied by the count of interactive operations that are affected by throttling.

How can I use my utilization data to predict my capacity needs?

Your metrics report dataset retains 30 to 45 days of data. Use the report to indicate how close you're to your capacity's maximum resources. If you save monthly snapshots, compare them to indicate trends of growth and extrapolate the rate to reach 100% utilization of your resources.

How can my utilization data inform me I should turn on autoscale?

Utilization data doesn't currently indicate whether requests were throttled due to capacity being in *interactive request delay* mode. The information is added to the utilization app so admins can determine whether users experienced delays, and to what extent the delays are due to overload without autoscaling.

How can I get notified that I'm approaching my max capacity?

The **Capacity management** page in the Power BI admin portal has a utilization notification checkbox. Users can choose the threshold at which an alert is triggered (default is 80%) and the email address to which utilization alerts should be sent.

How much data is Power BI storing? How can I retain more?

The Power BI service stores over 90 days of utilization data. Users who need longer data retention can use Bring Your Own Log Analytics (BYOLA) to store more utilization data.

How do I get visibility into resources of Premium beyond CPU time?

Customers don't have visibility through utilization data to the memory footprint of their operations, and can't know ahead of time whether any of their operations is subject to failures.

How do I use utilization data to perform chargebacks?

On the left side of the utilization report, a bar chart visual displays utilization information between workspaces for the time span of the report. The bar chart visual can be used for chargebacks, providing each workspace represents a different business unit, cost center, or other entity to which chargebacks can apply.

How does Power BI report CPU usage?

When you buy a capacity, you get a predefined number of v-cores, as listed in Capacities and SKUs.

The Microsoft Fabric Capacity Metrics app helps you understand how your capacity is performing by displaying your capacity's CPU usage levels. To provide a way of measuring your capacity's performance, The app reports CPU usage for the number of v-cores your capacity has. Power BI makes throttling and autoscale decisions based on the data displayed in the app.

Premium Per User (PPU)

Where can I learn more about Premium Per User (PPU)?

For information about Premium Per User (PPU), see the Power BI Premium Per User article.

Next steps

The following articles provide more information about Power BI Premium:

- What is Power BI Premium?
- Using Autoscale with Power BI Premium
- Extended Pro Trial activation
- Power BI Embedded FAQ

More questions? Try asking the Power BI Community

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Data protection in Power BI

Article • 11/14/2023

Overview

Power BI plays a key role in bringing data insights to everyone in an organization. However, as data becomes more accessible to inform decisions, risk of accidental oversharing or misuse of business-critical information increases.

Microsoft has world-class security capabilities to help protect customers from threats. Over 3,500 security researchers along with sophisticated AI models reason every day over 6.5+ trillion signals globally to help protect customers against threats at Microsoft.

Data protection capabilities in Power BI build on Microsoft's strengths in security and enable customers to empower every user with Power BI and better protect their data no matter how or where it is accessed.
https://www.youtube-nocookie.com/embed/zEx0449K7F8

The pillars of Power BI's data protection capabilities and how they help you protect your organization's sensitive data are listed below:

- **Sensitivity labels from Microsoft Purview Information Protection**
  - **Classify and label sensitive Power BI data** using the same sensitivity labels from Microsoft Purview Information Protection that are used in Office and other Microsoft products.
  - **Enforce governance policies even when Power BI content is exported** to Excel, PowerPoint, PDF, and other supported export formats to help ensure data is protected even when it leaves Power BI.

- **Microsoft Defender for Cloud Apps**
  - **Monitor and protect user activity on sensitive data in real time** with alerts, session monitoring, and risk remediation using Defender for Cloud Apps.
  - **Empower security administrators** who use data protection reports and security investigation capabilities with Defender for Cloud Apps to enhance organizational oversight.

- **Microsoft 365 data loss prevention**
  - **Data loss prevention policies for Power BI** enable central security teams to use Microsoft 365 data loss prevention policies to enforce the organization's DLP policies on Power BI. DLP policies for Power BI currently support detection of sensitive info types and sensitivity labels on semantic models, and can trigger

automatic risk remediation actions such as alerts to security admins in Microsoft 365 compliance portal and policy tips for end users.

Read more about sensitivity labels from Microsoft Purview Information Protection, Microsoft Defender for Cloud Apps, and Microsoft 365 data loss prevention.

Give us your feedback

The product team would love to get your **feedback** about Power BI's information protection capabilities and its integration with Microsoft Purview Information Protection. Help us meet your information protection needs! Thanks!

Next steps

- Learn about sensitivity labels in Power BI and how to use them
- Set up and use Defender for Cloud Apps controls in Power BI
- Learn about data loss prevention
- Power BI implementation planning: Information protection and data loss prevention

Sensitivity labels in Power BI

Article • 02/16/2025

This article describes the functionality of sensitivity labels from Microsoft Purview Information Protection in Power BI.

For information about enabling sensitivity labels on your tenant, including licensing requirements and prerequisites, see Enable data sensitivity labels in Power BI.

For information about how to apply sensitivity labels on your Power BI content and files, see How to apply sensitivity labels in Power BI.

Give us your feedback

The product team would love to get your **feedback** about Power BI's information protection capabilities and its integration with Microsoft Purview Information Protection. Help us meet your information protection needs! Thanks!

Introduction

Sensitivity labels from Purview Information Protection provide a simple way for your users to classify critical content in Power BI without compromising productivity or the ability to collaborate. They can be applied in both Power BI Desktop and the Power BI service, making it possible to protect your sensitive data from the moment you first start developing your content on through to when it's being accessed from Excel via a live connection. Sensitivity labels are retained when you move your content back and forth between Desktop and the service in the form of .pbix files.

In the Power BI service, sensitivity labels can be applied to semantic models, reports, dashboards, and dataflows. When labeled data leaves Power BI, either via export to Excel, PowerPoint, PDF, or .pbix files, or via other supported export scenarios such as Analyze in Excel or live connection PivotTables in Excel, Power BI automatically applies the label to the exported file and protects it according to the label's file encryption settings. This way your sensitive data can remain protected, even when it leaves Power BI.

In addition, sensitivity labels can be applied to .pbix files in Power BI Desktop, so that your data and content is safe when it's shared outside Power BI (for example, so that only users within your organization can open a confidential .pbix that has been shared or attached in an email), even before it has been published to the Power BI service. See Restrict access to content by using sensitivity labels to apply encryption for more detail.

Sensitivity labels on reports, dashboards, semantic models, and dataflows are visible from many places in the Power BI service. Sensitivity labels on reports and dashboards are also visible in the Power BI iOS and Android mobile apps and in embedded visuals. In Desktop, you can see the sensitivity label in the status bar.

A protection metrics report available in the Power BI admin portal gives Power BI admins full visibility over the sensitive data in the Power BI tenant. In addition, the Power BI audit logs include sensitivity label information about activities such as applying, removing, and changing labels, as well as about activities such as viewing reports, dashboards, etc. This gives Power BI and security admins visibility over sensitive data consumption for the purposes of monitoring and investigating security alerts.

Important considerations

In the Power BI service, sensitivity labeling **does not** affect access to content. Access to content in the service is managed solely by Power BI permissions. While the labels are visible, any associated encryption settings (configured in the Microsoft Purview compliance portal) aren't applied. They're applied only to data that leaves the service via a supported export path, such as export to Excel, PowerPoint, or PDF, and download to .pbix.

In Power BI Desktop, sensitivity labels with encryption settings **do** affect access to content. If a user doesn't have sufficient permissions according to the encryption settings of the sensitivity label on the .pbix file, they won't be able to open the file. In addition, in Desktop, when you save your work, any sensitivity label you've added and its associated encryption settings will be applied to the saved .pbix file.

Sensitivity labels and file encryption **are not** applied in non-supported export paths. The Power BI admin can block export from non-supported export paths.

> **Note**
>
> Users who are granted access to a report are granted access to the entire underlying semantic model, unless row-level security (RLS) limits their access. Report authors can classify and label reports using sensitivity labels. If the sensitivity label has protection settings, Power BI applies these protection settings when the report data leaves Power BI via a supported export path such as export to Excel, PowerPoint, or PDF, download to .pbix, and **Save** (Desktop). Only authorized users will be able to open protected files.

Supported export paths

Applying sensitivity labels and their associated protection to data that leaves the Power BI service is currently supported for the following export paths:

- Export to Excel, PDF files, and PowerPoint.
- Analyze in Excel from the Power BI service, which triggers download of an Excel file with a live connection to a Power BI semantic model.
- PivotTable in Excel with a live connection to a Power BI semantic model, for users with Microsoft 365 E3 and above.
- Download to .pbix (Service)

> **Note**
>
> When using **Download the .pbix** in the Power BI service, if the downloaded report and its semantic model have different labels, the more restrictive label will be applied to the .pbix file.
>
> In Power BI Desktop, sensitivity label support in Export to PDF is a preview feature that is on by default. It is possible to turn it off. See Desktop considerations and limitations for more information.

How sensitivity labels work in Power BI

When you apply a sensitivity label to Power BI content and files, it's similar to applying a tag on that resource that has the following benefits:

- **Customizable** - you can create categories for different levels of sensitive content in your organization, such as Personal, Public, General, Confidential, and Highly Confidential.
- **Clear text** - since the label is in clear text, it's easy for users to understand how to treat the content according to sensitivity label guidelines.
- **Persistent** - after a sensitivity label has been applied to content, it accompanies that content when it's exported to Excel, PowerPoint and PDF files, downloaded to .pbix, or saved (in Desktop) and becomes the basis for applying and enforcing policies.

Here's a quick example of how sensitivity labels in Power BI work. The image below shows how a sensitivity label is applied on a report in the Power BI service, then how the data from the report is exported to an Excel file, and finally how the sensitivity label and its protections persist in the exported file.

The sensitivity labels you apply to content persist and roam with the content as it's used and shared throughout Power BI. You can use the labeling to generate usage reports and to see activity data for your sensitive content.

Sensitivity labels in Power BI Desktop

Sensitivity labels can also be applied in Power BI Desktop. This makes it possible to protect your data from the moment you first start developing your content. When you save your work in Desktop, the sensitivity label you applied, along with any associated encryption settings, is applied to the resulting .pbix file. If the label has encryption settings, the file is thus protected wherever it goes and however it's transmitted. Only users with the necessary RMS permissions will be able to open it.

> **Note**
>
> Some limitations may apply. See Considerations and limitations.

If you apply a sensitivity label in Desktop, when you publish your work to the service, or when you upload a .pbix file of that work to the service, the label travels with the data into the service. In the service, the label will be applied to both the semantic model and the report that you get with the file. If the semantic model and report already have sensitivity labels, you can choose to keep those labels or to overwrite them with the label coming from Desktop.

If you upload a .pbix file that has never been published to the service before, and that has the same name as a report or semantic model that already exists on the service, the

upload will succeed only if the uploader has the RMS permissions necessary to change the label.

The same is also true in the opposite direction - when you download to .pbix in the service and then load the .pbix into Desktop, the label that was in the service will be applied to the downloaded .pbix file and from there be loaded into Desktop. If the report and semantic model in the service have different labels, the more restrictive of the two will be applied to the downloaded .pbix file.

When you apply a label in Desktop, it shows up in the status bar.

Learn how to apply sensitivity labels to Power BI content and files.

Sensitivity label inheritance upon creation of new content

When new reports and dashboards are created in the Power BI service, they automatically inherit the sensitivity label previously applied on parent semantic model or report. For example, a new report created on top of a semantic model that has a "Highly Confidential" sensitivity label will automatically receive the "Highly Confidential" label as well.

The following image shows how a semantic model's sensitivity label is automatically applied on a new report that is built on top of the semantic model.

> **Note**
>
> If for any reason the sensitivity label can't be applied on the new report or dashboard, Power BI **will not** block creation of the new item.

Sensitivity label inheritance from data sources

Power BI semantic models that connect to sensitivity-labeled data in supported data sources can inherit those labels so that the data remains classified and secure when brought into Power BI. Currently, Azure Synapse Analytics (formerly SQL Data Warehouse) and Azure SQL Database are supported. See Sensitivity label inheritance from data sources to learn how inheritance from data sources works and how to enable it for your organization.

Sensitivity label downstream inheritance

When a sensitivity label is applied to a semantic model or report in the Power BI service, it's possible to have the label trickle down and be automatically applied to content that is built from that semantic model or report as well. This capability is called downstream inheritance.

Downstream inheritance is a critical link in Power BI's end-to-end information protection solution. Together with inheritance from data sources, inheritance upon creation of new content, inheritance upon export to file, and other capabilities for applying sensitivity

labels, downstream inheritance helps ensure that sensitive data remains protected throughout its journey through Power BI, from data source to point of consumption.

Read more about downstream inheritance

Data loss prevention (DLP) policies

Power BI leverages Microsoft 365 data loss prevention to enable central security teams to use data loss prevention policies to enforce their organization's DLP policies in Power BI. See Data loss prevention policies for Fabric and Power BI for detail.

Default label policy

To help ensure comprehensive protection and governance of sensitive data, organizations can create default label policies for Power BI that automatically apply default sensitivity labels to unlabeled content. Currently, default label policies are supported in Power BI Desktop only. For more information, see Default label policy.

Mandatory label policy

To help ensure comprehensive protection and governance of sensitive data, organizations can require users to apply labels to their sensitive Power BI content. Such a policy is called a mandatory label policy. For more information, see Mandatory label policy for Power BI.

Admin APIs for setting and removing labels programmatically

To meet compliance requirements, organizations are often required to classify and label all sensitive data in Power BI. This task can be challenging for tenants that have large volumes of data in Power BI. To make the task easier and more effective, Power BI has admin REST APIs that admins can use to set and remove sensitivity labels on large numbers of Power BI artifacts programatically. See the following:

- Admin - InformationProtection SetLabelsAsAdmin
- Admin - InformationProtection RemoveLabelsAsAdmin

Auditing for activity on sensitivity labels

Whenever a sensitivity label on a semantic model, report, dashboard, or dataflow is applied, changed, or removed, that activity is recorded in the audit log for Power BI. You can track these activities in the unified audit log or in the Power BI activity log. See Audit schema for sensitivity labels in Power BI for detail.

Sensitivity labels and protection on exported data

When data is exported from Power BI to Excel, PDF files, or PowerPoint files, Power BI automatically applies a sensitivity label on the exported file and protects it according to the label's file encryption settings. This way your sensitive data remains protected no matter where it is.

A user who exports a file from Power BI has permissions to access and edit that file according to the sensitivity label settings; they don't get owner permissions to the file.

> **Note**
>
> When using **Download the .pbix** in the Power BI service, if the downloaded report and its semantic model have different labels, the more restrictive label will be applied to the .pbix file.

Sensitivity labels and protection aren't applied when data is exported to .csv, files or any other unsupported export path.

Applying a sensitivity label and protection to an exported file doesn't add content marking to the file. However, if the label is configured to apply content markings, the markings are automatically applied by the Azure Information Protection unified labeling client when the file is opened in Office desktop apps. The content markings aren't automatically applied when you use built-in labeling for desktop, mobile, or web apps. See When Office apps apply content marking and encryption for more detail.

Export fails if a label can't be applied when data is exported to a file. To check if export failed because the label couldn't be applied, select the report or dashboard name at the center of the title bar and see whether it says "Sensitivity label can't be loaded" in the info dropdown that opens. This can happen as the result of a temporary system issue, or if the applied label has been unpublished or deleted by the security admin.

Sensitivity label inheritance in Analyze in Excel

When you create a PivotTable in Excel with a live connection to a Power BI semantic model (you can do this either from Power BI through Analyze In Excel or from Excel), the semantic model's sensitivity label is inherited and applied to your Excel file, along with any associated protection. If the label on the semantic model later changes to a more restrictive one, the label applied on the linked Excel file will automatically update upon data refresh.

Sensitivity labels in Excel that were manually set aren't automatically overwritten by the semantic model's sensitivity label. Rather, a banner notifies you that the semantic model has a sensitivity label and recommends that you apply it.

> **Note**
>
> If the semantic model's sensitivity label is less restrictive than the Excel file's sensitivity label, no label inheritance or update takes place. An Excel file never inherits a less restrictive sensitivity label.

Sensitivity label persistence in embedded reports and dashboards

You can embed Power BI reports, dashboards, and visuals in business applications such as Microsoft Teams and SharePoint, or in an organization's website. When you embed a

visual, report or dashboard that has a sensitivity label applied to it, the sensitivity label will be visible in the embedded view, and the label and its protection will persist when data is exported to Excel.

The following embedding scenarios are supported:

- Embed for your organization
- Microsoft 365 apps (for example, Teams and SharePoint)
- Secure URL embedding (embedding from the Power BI service)

Sensitivity labels in paginated reports

Sensitivity labels can be applied to paginated reports hosted in the Power BI service. After uploading a paginated report to the service, you apply the label to the report just as you would to a regular Power BI report. See Sensitivity label support for paginated reports for detail.

Sensitivity labels in deployment pipelines

Sensitivity labels are supported in deployment pipelines. See the deployment pipeline documentation for details about how sensitivity labels are handled as content is deployed from stage to stage.

Sensitivity labels in the Power BI mobile apps

Sensitivity labels can be viewed on reports and dashboards in the Power BI mobile apps. An icon near the name of the report or dashboard indicates that it has a sensitivity label, and the type of label and its description can be found in the report or dashboard's info box.

Label change enforcement

Power BI restricts permission to change or remove sensitivity labels from Purview Information Protection that have file encryption settings to authorized users only. See Sensitivity label change enforcement for detail.

Supported clouds

Sensitivity labels are supported for tenants in global (public) clouds, and the following national/regional clouds:

- US Government: GCC, GCC High, DoD
- China

Sensitivity labels aren't currently supported in other national/regional clouds.

Licensing and requirements

See Licensing and requirements.

Sensitivity label creation and management

Sensitivity labels are created and managed in the Purview compliance portal.

To access sensitivity labels in either of these centers, navigate to **Classification** > **Sensitivity labels**. These sensitivity labels can be used by multiple Microsoft services such Azure Information Protection, Office apps, and Office 365 services.

> **Important**
>
> If your organization uses Azure Information Protection sensitivity labels, you need to migrate them to one of the previously listed services in order for the labels to be used in Power BI.

Custom help link

To help your users understand what your sensitivity labels mean or how they should be used, you can provide a *Learn more* URL that appears at the bottom of the sensitivity label menu that you see when you're applying a sensitivity label.

See Custom help link for sensitivity labels for detail.

Considerations and limitations

General

- Power BI doesn't support sensitivity labels of the following types:
  - Do Not Forward
  - User-defined, where users are allowed to assign permissions when they manually apply a sensitivity label to content.
  - HYOK (hold your own key)

The *Do Not Forward* and *user-defined* types refer to labels defined in the Micosoft Purview portal.

- Don't use parent labels. A parent label is a label that has sublabels. You can't apply parent labels, but a label that is already applied may become a parent label if it acquires sublabels. If you come across an item that has a parent label, apply the appropriate sublabel. To change a parent label, you must have sufficient usage rights on the label.

  If an item has a parent label, note the following behavior:
  - Parent labels won't be inherited.
  - Mandatory label policies won't be applied to items that have a parent label. This means users won't be required to apply a meaningful label in order to save the item, and the item will escape mandatory label policies designed to promote total coverage.
  - If you try to export data from an item that has a parent label, export will fail.
  - It's possible to publish a *.pbix* file that has a parent label, but if the parent label is protected, publish will fail. The solution is to apply a suitable sublabel.

- Data sensitivity labels aren't supported for template apps. Sensitivity labels set by the template app creator are removed when the app is extracted and installed, and sensitivity labels added to artifacts in an installed template app by the app consumer are lost (reset to nothing) when the app is updated.

- In the Power BI service, if a semantic model has a label that has been deleted from the label admin center, you will not be able to export or download the data. In Analyze in Excel, a warning will be issued and the data will be exported to an .odc file with no sensitivity label.

- Get data and refresh scenarios from encrypted Excel (*.xlsx*) files are supported, unless the file is stored behind a gateway, in which case the Get data/refresh action will fail. Get data and refresh actions from an Excel file that is stored behind a gateway and that has an *unprotected* sensitivity label will succeed, but the sensitivity label won't be inherited. See Sensitivity label inheritance from data sources for detail.

- Information protection in Power BI doesn't support **B2B** and **multi-tenant scenarios**.

Power BI service

- Sensitivity labels can be applied only on dashboards, reports, semantic models, dataflows, and paginated reports. They aren't currently available for workbooks.

- Sensitivity labels on Power BI assets are visible in the workspace list, lineage, favorites, recents, and apps views; labels aren't currently visible in the "shared with me" view. Note, however, that a label applied to a Power BI asset, even if not visible, will always persist on data exported to Excel, PowerPoint, PDF, and PBIX files.

- Import of sensitivity-labeled *.pbix* files (both protected and unprotected) stored on OneDrive or SharePoint Online, as well as on-demand and automatic semantic model refresh from such files, is supported, except for the following scenarios:
  - Protected live-connected *.pbix* files and protected Azure Analysis Services *.pbix* files. Refresh will fail. Neither report content nor label will be updated.
  - Labeled unprotected Live Connect *.pbix* files: Report content will be updated but label won't be updated.
  - When the *.pbix* file has had a new sensitivity label applied that the semantic model owner doesn't have usage rights to. In this case, refresh will fail. Neither report content nor label will be updated.
  - If the semantic model owner's access token for OneDrive/SharePoint has expired. In this case, refresh will fail. Neither report content nor label will be updated.

Power BI Desktop

- Directly publishing a protected .pbix file from Power BI Desktop to the Power BI service is not supported for guest users, even if they have higher-level permissions. To update or publish reports from a protected .pbix file, guest users need to start from the Power BI service, using **Get Data**, for example.

- Power BI Desktop for Power BI Report Server doesn't support information protection. If you try to open a protected .pbix file, the file won't open and you'll receive an error message. Sensitivity-labeled .pbix files that aren't encrypted can be opened as normal.

- Users with a free license can't open protected .pbix files.

- To open a protected .pbix file, a user with an appropriate license must also have **Full control** and/or **Export** usage rights for the relevant label. See more detail.

  The user who sets the label gets Full control and can never be locked out unless connectivity fails and authentication can't take place.

  In rare cases, it may happen that no one has the necessary usage rights for the relevant label except the person that set the label. Then, if that one person leaves the organization or changes aliases within the organization, all access to the .pbix file will be lost. The solution for regaining access to the file in such cases is to either change or remove the sensitivity label on the file using the set/remove sensitivity label Admin APIs. Contact your Power BI admin for assistance (only admins can run the Admin APIs).

- "Publish" or "Get data" of a protected .pbix file requires that the label on the .pbix file be in the user's label policy. If the label isn't in the user's label policy, the Publish or Get data action will fail.

- Power BI supports publishing or importing a .pbix file that has an **unprotected** sensitivity label to the service via APIs running under a service principal. Publishing or importing a .pbix file that has a **protected** sensitivity label to the service via APIs running under a service principal **is not** supported and will fail. To mitigate, users can remove the label and then publish using service principals.

- Power BI Desktop users may experience problems saving their work when internet connectivity is lost, such as after going offline. With no internet connection, some actions related to sensitivity labels and rights management might not complete properly. In such cases it's recommended to go back online and try saving again.

- In general, when you protect a file with a sensitivity label that applies encryption, it's good practice to use another encryption method as well, such as pagefile encryption, NTFS encryption, BitLocker instances, antimalware, etc.

- Temp files aren't encrypted.

- **Export to PDF in Desktop** supports sensitivity labels as a preview feature that is on by default. To turn off the preview feature, go to **File** > **Options and settings** > **Options** > **Preview features**, and uncheck **Enable setting sensitivity label on exported PDF**. If you turn off the preview feature, when you export a file that has a sensitivity label to PDF, the PDF won't receive the label and no protection will be applied.

- Exporting a report with a protected sensitivity label from the Power BI service to a .pbix file might fail if the .pbix file size starts to exceed 6 GB.

- If you overwrite a labeled semantic model or report in the service with an unlabeled .pbix file, the labels in the service will be retained.

Related content

This article provided an overview of data protection in Power BI. The following articles provide more details about data protection in Power BI.

- Enable sensitivity labels in Power BI
- How to apply sensitivity labels in Power BI
- Using Microsoft Defender for Cloud Apps controls in Power BI
- Protection metrics report
- Power BI implementation planning: Information protection for Power BI

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Enable sensitivity labels in Fabric

Article • 11/16/2023

In order for sensitivity labels from Microsoft Purview Information Protection to be used in Fabric, they must be enabled on the tenant. This article shows Fabric admins how to do this. For an overview about sensitivity labels in Fabric, see Sensitivity labels in Fabric. For information about applying sensitivity labels in Fabric, see Apply sensitivity labels to Fabric items

When sensitivity labels are enabled:

- Specified users and security groups in the organization can apply sensitivity labels to their Fabric content. In the Fabric service, this means any Fabric item. In Power BI Desktop, it means their *.pbix* files.
- In the service, all members of the organization can see those labels. In Desktop, only members of the organization who have the labels published to them can see the labels.

Enabling sensitivity labels requires an Azure Information Protection license. See Licensing and requirements for detail.

Give us your feedback

The product team would love to get your **feedback** about Fabric's information protection capabilities and its integration with Microsoft Purview Information Protection. Help us meet your information protection needs! Thanks!

Licensing and requirements

- An Azure Information Protection Premium P1 or Premium P2 license is required to apply or view sensitivity labels from Purview Information Protection. Azure Information Protection can be purchased either standalone or through one of the Microsoft licensing suites. See Azure Information Protection pricing for detail.

> **Note**
>
> If your organization uses Azure Information Protection sensitivity labels, they need to be migrated to the Purview Information Protection Unified Labeling platform in order for the them to be used in Fabric. **Learn more about migrating sensitivity labels**.

- To be able to apply labels to Power BI Fabric items, a user must have a Power BI Pro or Premium Per User (PPU) license in addition to one of the Azure Information Protection licenses mentioned above.
- Office apps have their own licensing requirements for viewing and applying sensitivity labels.
- Before enabling sensitivity labels on your tenant, make sure that sensitivity labels have been defined and published for relevant users and groups. See Create and configure sensitivity labels and their policies for detail.
- Customers in China must enable rights management for the tenant and add the Microsoft Purview Information Protection Sync Service service principle, as described in steps 1 and 2 under Configure Azure Information Protection for customers in China.
- Using sensitivity labels in Desktop requires the Desktop December 2020 release or later.

> **Note**
>
> If you try to open a protected .pbix file with a Desktop version earlier than December 2020, it will fail, and you'll be prompted to upgrade your Desktop version.

Enable sensitivity labels

Sensitivity labels must be enabled in your tenant before they can be used in both in the Fabric service and in Power BI Desktop. This section describes how to enable them in the Fabric tenant settings.

To enable sensitivity labels on your tenant:

1. Go to the Fabric admin portal.
2. Choose **Tenant settings** on the navigation pane.
3. Find the **Information protection** section and expand **Allow users to apply sensitivity labels for content**.
4. Turn on the toggle switch.
5. Define who can apply and change sensitivity labels on Fabric items:

- Select **The entire organization** if you want everyone in the organization to be able to apply and change labels on items. This is the default setting.
- Select **Specific security groups** if you want to allow this capability for only certain users. Make sure that the security group(s) you specify contain only users who you want to be able to apply and change sensitivity labels on items.

6. If you want certain users not to be able to apply and change sensitivity labels on items, mark the **Except specify security groups** checkbox and specify a security group(s) that contains just those users.
7. When done, press **Apply**.

> **Important**
>
> Users who this setting allows to apply and change sensitivity labels must also have *create* and *edit* permissions on any item they wish to apply or change a label on.

Troubleshooting

Fabric uses sensitivity labels from Microsoft Purview Information Protection. Thus if you encounter an error message when trying to enable sensitivity labels, it might be due to one of the following reasons:

- Sensitivity labels haven't been migrated to the Microsoft Purview Information Protection version supported by Fabric.
- No sensitivity labels from Microsoft Purview Information Protection have been defined in the organization.

Considerations and limitations

For a list of sensitivity label limitations in Fabric and Power BI, see Sensitivity labels in Power BI.

Next steps

This article described how to enable sensitivity labels in Fabric. The following articles provide more details about data protection in Fabric.

- Overview of sensitivity labels

- Apply sensitivity labels to Fabric items
- Using Microsoft Defender for Cloud Apps controls in Power BI

How to apply sensitivity labels in Power BI

Article • 11/16/2023

Sensitivity labels from Microsoft Purview Information Protection on your reports, dashboards, semantic models, dataflows, and **.pbix** files can guard your sensitive content against unauthorized data access and leakage. Labeling your data correctly with sensitivity labels ensures that only authorized people can access your data. This article shows you how to apply sensitivity labels in the Power BI service and in Power BI Desktop.

For more information, see Sensitivity labels in Power BI.

Give us your feedback

The product team would love to get your **feedback** about the Power BI information protection capabilities and its integration with Microsoft Purview Information Protection. Help us meet your information protection needs! Thanks!

Apply sensitivity labels in the Power BI service

In the Power BI service, you can apply sensitivity labels to reports, dashboards, semantic models, and dataflows.

Here are the requirements to apply sensitivity labels in the Power BI service:

- You must have a Power BI Pro or Premium Per User (PPU) license and edit permissions on the content you want to label. Note: If you have a Free license, you can apply sensitivity labels on the content in your *My workspace*, provided that the other requirements listed here have been met.
- Sensitivity labels must be enabled for your organization. Contact your Power BI admin for information about your configuration.
- You must belong to a security group that has permissions to apply sensitivity labels, as described in Enable sensitivity labels in Power BI.
- All licensing and other requirements must be met.

View sensitivity labels

When data protection is enabled on your tenant, sensitivity labels appear in the **Sensitivity** column in the list view of dashboards, reports, semantic models, and dataflows.

Set the sensitivity label on a report or dashboard

You can apply or change the sensitivity label on a report or dashboard by following these steps:

1. On the **More options...** menu for a report or dashboard, select **Settings**.
2. In the **Settings** side pane, go to the **Sensitivity label** section.
3. Select the appropriate sensitivity label in the drop-down list.
4. Select **Save** to apply the modified settings.

The following image shows how to set the sensitivity label for a dashboard to *Highly Confidential\Any User (No Protection)*:

> **Note**
>
> If the **Sensitivity label** setting isn't available, you might not have the correct **usage rights** to change the setting. If you're not able to change a sensitivity label, consider asking the person who originally applied the label to make the change. You can also contact the Microsoft 365/Office security administrator and request the necessary usage rights for the label.

Set the sensitivity label on a semantic model or dataflow

You can apply or change the sensitivity label on a semantic model or dataflow by following similar steps:

1. On the **More options...** menu for a semantic model or dataflow, select **Settings**.
2. In the **Settings** view, select the **Semantic models** or **Dataflows** tab, depending on your configuration.
3. Expand the **Sensitivity label** section.
4. Select the appropriate sensitivity label in the drop-down list.
5. Select **Apply** to save the modified settings.

The following images show how to set the sensitivity label for a semantic model to *General*:

> **Note**
>
> If the **Sensitivity label** setting isn't available, you might not have the correct **usage rights** to change the setting. If you're not able to change a sensitivity label, consider asking the person who originally applied the label to make the change. You can also contact the Microsoft 365/Office security administrator and request the necessary usage rights for the label.

Apply sensitivity labels in Power BI Desktop

Here are the requirements to apply sensitivity labels in Power BI Desktop:

- You must have a Power BI Pro or Premium Per User (PPU) license.
- Sensitivity labels must be enabled for your organization. Contact your Power BI admin for information about your configuration.
- You must belong to a security group that has permissions to apply sensitivity labels, as described in Enable sensitivity labels in Power BI.
- All licensing and other requirements must be met.
- You must be signed in.

Watch the following short video on how to apply sensitivity labels and then try it out yourself.

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

https://www.microsoft.com/en-us/videoplayer/embed/RE4M5Gj?postJsllMsg=true

Set the sensitivity label on a file

To apply a sensitivity label on a file you're working on, select the **Sensitivity** option on the toolbar. Select the appropriate sensitivity label in the drop-down list.

> **Note**
>
> If the **Sensitivity** option isn't available, you might not have an appropriate license, or you might not belong to a security group that has permissions to apply sensitivity labels, as described in **Enable sensitivity labels in Power BI**.
>
> If a specific sensitivity label isn't available, you might not have the correct **usage rights** to change the setting. If you're not able to change a sensitivity label, consider asking the person who originally applied the label to make the change. You can also contact the Microsoft 365/Office security administrator and request the necessary usage rights for the label.

After you apply the sensitivity label, it's visible in the status bar.

Work with sensitivity labels on uploaded or downloaded files

When you publish a .pbix file to the Power BI service from Power BI Desktop, or when you upload a .pbix file to the Power BI service directly via the **OneLake data hub**, the .pbix file's label is applied to both the report and the semantic model that are created in the service.

If the .pbix file you're publishing or uploading replaces existing assets (that is, the file has the same name as the .pbix file), you see a dialog prompt. At the prompt, choose whether to keep the labels on the assets or have the .pbix file's label overwrite those labels. If the .pbix file is unlabeled, the labels in the service are retained.

When you download a .pbix file from the Power BI service by using the **Download this file** option, if both the report and semantic model to download have labels and the two labels are different, the label applied to the .pbix file is the more restrictive of the two.

Remove sensitivity labels

You can remove sensitivity labels only in Power BI Desktop.

To remove a sensitivity label from a .pbix file, select the **Sensitivity** option on the toolbar. Select the current sensitivity label setting in the drop-down list. The sensitivity label is removed from the file.

Considerations and limitations

For more information, see Sensitivity labels in Power BI.

Next steps

This article described how to apply sensitivity labels in Power BI. The following articles provide more details about data protection in Power BI.

- Overview of sensitivity labels in Power BI
- Enable sensitivity labels in Power BI
- Using Microsoft Defender for Cloud Apps controls in Power BI

Sensitivity label change enforcement

Article • 01/16/2024

Power BI restricts permission to change or remove sensitivity labels from Microsoft Purview Information Protection that have file encryption settings to authorized users only.

Authorized users are:

- The user who applied the sensitivity label.
- Users who have been assigned at least one of the following usage rights to the label in the labeling admin center (Microsoft Purview compliance portal):
  - OWNER
  - EXPORT
  - EDIT and EDITRIGHTSDATA

Users who try to change a label and can't should ask the person who applied the label to perform the modification, or they can contact their Microsoft 365/Office security administrator and ask to be granted the necessary usage rights.

Relaxations to accommodate automatic labeling scenarios

Power BI supports several capabilities, such as label inheritance from data sources and downstream inheritance, which automatically apply sensitivity labels to content. These automated scenarios can result in situations where no user has been set as the RMS label issuer for a label on an item. This means that there is no user who is guaranteed to be able to change or remove the label.

In such cases, the usage rights requirements for changing or removing the label are relaxed - a user needs just one of the following usage rights to be able to change or remove the label:

- OWNER
- EXPORT
- EDIT

If no user has even these usage rights, nobody will be able to change or remove the label from the item, and access to the item is potentially endangered.

To avoid this situation, the Power BI admin can enable the **Allow workspace admins to override automatically applied sensitivity labels (preview)** tenant setting. This makes it possible for workspace admins to override automatically applied sensitivity labels without regard to label change enforcement rules.

To enable this setting, go to: **Admin portal** > **Tenant settings** > **Information protection**.

Related content

- Sensitivity label overview

Custom help link for sensitivity labels

Article • 01/16/2024

To help your organization's Power BI users understand and use your sensitivity labels, you can provide a *Learn more* link pointing to your organization's custom web page that users will see when they're applying or being prompted to apply sensitivity labels. The image below is an example that shows how the *Learn more* link appears when applying a sensitivity label in Power BI Desktop.

Define a custom help link

You can define a custom help link for sensitivity labels in two ways:

- Using the Security & Compliance Center PowerShell Set-LabelPolicy command. This creates a Power BI dedicated help link.

  PowerShell

  ```
  Set-LabelPolicy -Identity "<policy name>" -AdvancedSettings
  @{powerbicustomurl=https://<your link>}
  ```

- If a dedicated custom help link for Power BI isn't set, Power BI uses the custom help link defined for Office 365 apps. The custom help link is defined in the Microsoft Purview compliance portal. For more information, see What label policies can do.

If a user has more than one label policy, the custom URL is always taken from the policy with the highest priority, so be sure to configure the custom URL on that policy.

Related content

- Sensitivity labels in Power BI

Audit schema for sensitivity labels in Power BI

Article • 11/22/2022

Whenever a sensitivity label on a dataset, report, dashboard, or dataflow is applied, changed, or removed, that activity is recorded in the audit log for Power BI. You can track these activities in the unified audit log or in the Power BI activity log. For more information, see Track user activities in Power BI.

This article documents the information in the Power BI auditing schema that's specific to sensitivity labels. It covers the following activity keys:

- SensitivityLabelApplied
- SensitivityLabelChanged
- SensitivityLabelRemoved

SensitivityLabelEventData

Field	Type	Must appear in the schema	Description
SensitivityLabelId	Edm.Guid		The guid of the new label. This field is only present when the activity key is SensitivityLabelApplied or SensitivityLabelChanged.
OldSensitivityLabelId	Edm.Guid		The guid of the label on the item before the action. This field is only present when the activity key is SensitivityLabelChanged or SensitivityLabelRemoved.
ActionSource	Edm.Enum	Yes	This field indicates whether the label change is the result of an automatic or manual process.
ActionSourceDetail	Edm.Enum	Yes	This field gives more detail about what caused the action to take place.
LabelEventType	Edm.Enum	Yes	This field indicates whether the action resulted in a more restrictive label, less restrictive label, or a label of the same degree of sensitivity.

ArtifactType

This field indicates the type of item the label change took place on.

Value	Field
1	Dashboard
2	Report
3	Dataset
7	Dataflow

ActionSource

This field indicates whether the label change is the result of an automatic or manual process.

Value	Meaning	Description
2	Auto	An automatic process performed the action.
3	Manual	A manual process performed the action.

ActionSourceDetail

This field gives more detail about what caused the action to take place.

Value	Meaning	Description
0	None	There are no other details.
3	AutoByInheritance	The label change took place as a result of an automatically triggered inheritance process.
4	AutoByDeploymentPipeline	The label change took place automatically as a result of the deployment pipeline process.
5	PublicAPI	The label change action was performed by one of the following Power BI public admin REST APIs: setLabels, removeLabels.

LabelEventType

This field indicates whether the action resulted in a more restrictive label, less restrictive label, or a label of the same degree of sensitivity.

Value	Meaning	Description
1	LabelUpgraded	A more restrictive label was applied to the item.
2	LabelDowngraded	A less restrictive label was applied to the item.
3	LabelRemoved	The label was removed from the item.
4	LabelChangedSameOrder	The label was replaced by another label with the same level of sensitivity.

Next steps

- Sensitivity labels in Power BI
- Track user activities in Power BI

Get started with Data loss prevention policies for Fabric and Power BI

Article • 11/19/2024

This article describes Microsoft Purview Data Loss Prevention (DLP) policies in Fabric. The target audience is Fabric administrators, security and compliance teams, and Fabric data owners.

Overview

To help organizations detect and protect their sensitive data, Fabric supports Microsoft Purview Data Loss Prevention (DLP) polices. When a DLP policy for Fabric detects a supported item type containing sensitive information, a policy tip can be attached to the item that explains the nature of the sensitive content, and an alert can be registered on the data loss prevention **Alerts** page in the Microsoft Purview portal for monitoring and management by administrators. In addition, email alerts can be sent to administrators and specified users.

This article describes how DLP in Fabric works, lists considerations and limitations as well as licensing and permissions requirements, and explains how DLP CPU usage is metered. For more information, see:

- Respond to a DLP policy violation in Fabric to see how to respond when a policy tip tells you your lakehouse or semantic model has a DLP policy violation.
- Monitor DLP policy violations in Fabric to see how to sign in to the Microsoft Purview portal to see details about DLP violation alerts.

> **Tip**
>
> Get started with Microsoft Security Copilot to explore new ways to work smarter and faster using the power of AI. Learn more about Microsoft Security Copilot in Microsoft Purview.

Considerations and limitations

- DLP policies for Fabric are defined in the Microsoft Purview portal.
- DLP policies apply to workspaces. Only workspaces hosted in Fabric or Premium capacities are supported. For more information, see Microsoft Fabric concepts and

licenses.

- DLP evaluation workloads impact capacity. Currently, DLP for Fabric is available at no additional cost, but this is subject to change. Check this document and the Fabric blog for updates.
- DLP policy templates aren't yet supported for Fabric DLP policies. When creating a DLP policy for Fabric, choose the "custom policy" option.
- Fabric DLP policy rules currently support sensitivity labels and sensitive info types as conditions.
- DLP policies for Fabric aren't supported for sample semantic models, streaming datasets, or semantic models that connect to their data source via DirectQuery or live connection. This includes semantic models with mixed storage, where some of the data comes via import-mode and some comes via DirectQuery.
- DLP policies for Fabric apply only on data in Lakehouse Tables/ folder stored in Delta format.
- DLP policies for Fabric support all the primitive Delta types except *timestamp_ntz*.
- DLP policies for Fabric aren't supported for the following Delta Parquet data types:
  - Binary, timestamp_ntz, Struct, Array, List, Map, Json, Enum, Interval, Void.
  - Data with LZ4, Zstd, and Gzip compression codecs.
- Exact data match (EDM) classifiers and trainable classifiers aren't supported by DLP for Fabric. If you select an EDM or trainable classifier in the condition of a policy, the policy will yield no results even if the semantic model or lakehouse does in fact contain data that satisfies the EDM or trainable classifier. Other classifiers specified in the policy will return results, if any.
- DLP policies for Fabric aren't supported in the China North region. See How to find the default region for your organization to learn how to find your organization's default data region.
- Azure capacities aren't supported for DLP in Fabric in the following clusters:
  - WUS3
  - WUS2
  - SCUS
- Onboarding a new tenant to DLP can take a few hours, depending on the number of supported workspaces that are being onboarded.

Licensing and permissions

SKU/subscriptions licensing

Before you get started with DLP for Power BI, you should confirm your Microsoft 365 subscription. For full licensing guidance, see Microsoft 365 guidance for security & compliance.

Permissions

Data from DLP for Fabric can be viewed in Activity explorer. There are four roles that grant permission to Activity explorer; the account you use for accessing the data must be a member of any one of them.

To view the Activity explorer, the account you use for accessing the data must be a member of any of the following roles or above.

- Compliance administrator
- Security administrator
- Compliance data administrator

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. This helps improve security for your organization. Global Administrator is a highly privileged role that should only be used in scenarios where a lesser privileged role can't be used.

Supported item types

DLP policies for Fabric currently support (*preview*) the following item types.

- Semantic models
- Lakehouses

See Considerations and limitations for exceptions.

How do DLP policies for Fabric work

You define a DLP policy in the data loss prevention section of the Microsoft Purview portal. In the policy, you specify the sensitivity labels and/or sensitive info types you want to detect. You also specify the actions that will happen when the policy detects a semantic model or lakehouse that contains sensitive data of the kind you specified. DLP policies for Fabric support three actions:

- User notification via policy tips.
- Alerts. Alerts can be sent by email to administrators and users. Additionally, administrators can monitor and manage alerts on the **Alerts** tab in the Purview portal.

- Restrict access. When a supported item type violates a policy configured with the restrict access action, access to the item is restricted, either to the data owners or to members of the organization, depending on how the policy is configured. All other users will lose access to the item.

> ⓘ **Note**
>
> The restrict access action is only enforced on semantic models.

When a semantic model or lakehouse is evaluated by DLP policies, if it matches the conditions specified in a DLP policy, the actions specified in the policy occur. DLP policies are initiated by the following actions:

Semantic models:

A semantic model is evaluated against DLP policies whenever one of the following events occurs:

- Publish
- Republish
- On-demand refresh
- Scheduled refresh

> ⓘ **Note**
>
> DLP evaluation of the semantic model doesn't occur if either of the following is true:
>
> - The initiator of the event (publish, republish, on-demand refresh, scheduled refresh) is an account using service principal authentication.
> - The semantic model owner is a service principal.

Lakehouse:

A lakehouse is evaluated against DLP policies When the data within a lakehouse undergoes a change, such as getting new data, connecting a new source, adding or updating existing tables, and more.

What happens when an item is flagged by a Fabric DLP policy

When a DLP policy detects an issue with an item:

- If "user notification" is enabled in the policy, the item will be marked in Fabric with an icon that indicates that a DLP policy has detected an issue with the item. Hover over the icon to display a hover card that provides an option to see the full details in a side panel. For more information about what you see in the side panel, see Respond to a DLP violation in Fabric.

For semantic models, opening the details page will show a policy tip that explains the policy violation and how the type of sensitive information detected should be handled. Selecting **View all** opens a side panel with all the policy details.

> **Note**
>
> If you hide the policy tip, it doesn't get deleted. It will appear the next time you visit the page.

For lakehouses, the indication will appear in the header in edit mode, and opening the fly out makes it possible to see more details about the policy tips affecting the lakehouse. Selecting **View all** opens a side panel with all the policy details.

- If alerts are enabled in the policy, an alert will be recorded on the data loss prevention **Alerts** page in the Microsoft Purview portal, and (if configured) an email will be sent to administrators and/or specified users. For more information, see Monitor and manage DLP policy violations.

Configure a DLP policy for Power BI/Fabric

Follow the procedures in Create and Deploy data loss prevention policies and use the custom template.

> **Important**
>
> When you select the locations for your DLP policy for Power BI/Fabric, select only the Power BI/Fabric location. Do not select any other locations, this configuration is not supported.

See also

- Learn about data loss prevention
- Sensitivity labels in Power BI
- Audit schema for sensitivity labels in Power BI
- Configure a DLP policy for Fabric.
- Respond to a DLP policy violation in Fabric.
- Monitor and manage DLP policy violations
- Learn about data loss prevention

Feedback

Was this page helpful? Yes No

Configure data loss prevention policies for Fabric

Article • 11/19/2024

Data loss prevention policies for Fabric help organizations protect their sensitive data by detecting upload of sensitive data in supported item types. When a policy violation occurs, data owners can see this indicated, and alerts can be sent to data owners and security admins, and violations can be investigated. For more information, see Get started with Data loss prevention policies for Fabric and Power BI.

This article describes how to configure Purview data loss prevention (DLP) policies for Fabric. The target audience is compliance administrators who are responsible for data loss prevention in their organization.

Prerequisites

The account you use to create DLP policies must be a member of one of these role groups

- Compliance administrator
- Compliance data administrator
- Information Protection
- Information Protection Admin
- Security administrator

SKU/subscriptions licensing

Before you get started with DLP for Fabric and Power BI, you should confirm your Microsoft 365 subscription. The admin account that sets up the DLP rules must be assigned one of the following licenses:

- Microsoft 365 E5
- Microsoft 365 E5 Compliance
- Microsoft 365 E5 Information Protection & Governance
- Purview capacities

Configure a DLP policy for Fabric

1. Open the data loss prevention policies page in the Microsoft Purview portal and select + **Create policy**.

> ⓘ **Note**
>
> The + **Create policy** option is only available if the prerequistes have been met.

2. Choose the **Custom** category and then the **Custom policy** template. When done, select **Next**.

> ⓘ **Note**
>
> No other categories or templates are currently supported.

3. Name the policy and provide a meaningful description. When done, select **Next**.

4. Select **Next** when you get to the Assign admin units page. Admin units are not supported for DLP in Fabric and Power BI.

5. Select **Fabric and Power BI workspaces** as the location for the DLP policy. All other locations will be disabled, as DLP policies for Fabric and Power BI only support this location.

By default the policy will apply to all workspaces. However, you can specify particular workspaces to include in the policy as well as workspaces to exclude from the policy. To specify specific workspaces for inclusion or exclusion, select **Edit**.

> **Note**
>
> DLP actions are supported only for workspaces hosted in Fabric or Premium capacities.

After you've enabled Fabric and Power BI as the DLP location for the policy and chosen which workspaces the policy will apply to, select **Next**.

6. The **Define policy settings** page appears. Choose **Create or customize advanced DLP rules** to begin defining your policy.

When done, select **Next**.

7. On the **Customize advanced DLP rules** page, you can either start creating a new rule or choose an existing rule to edit. Select **Create rule**.

8. The **Create rule** page appears. On the create rule page, provide a name and description for the rule, and then configure the other sections, which are described following the image below.

Conditions

In the condition section, you define the conditions under which the policy will apply to supported item types. Conditions are created in groups. Groups make it possible to construct complex conditions.

1. Open the conditions section. Choose **Add condition** if you want to create a simple or complex condition, or **Add group** if you want to start creating a complex condition.

   For more information about using the condition builder, see Complex rule design.

2. If you chose **Add condition**, next choose **Content contains**, then **Add**, and then either **Sensitive info types** or **Sensitivity labels**.

If you started with **Add group**, you'll eventually get to **Add condition**, after which you continue as described above.

When you choose either **Sensitive info types** or **Sensitivity labels**, you'll be able to choose the particular sensitivity labels or sensitive info types you want to detect from a list that will appear in a sidebar.

When you select a sensitive info type as a condition, you then need to specify how many instances of that type must be detected in order for the condition to be considered as met. You can specify from 1 to 500 instances. If you want to detect 500 or more unique instances, enter a range of '500' to 'Any'. You also can select the degree of confidence in the matching algorithm. Select the info button next to the confidence level to see the definition of each level.

You can add additional sensitivity labels or sensitive info types to the group. To the right of the group name, you can specify **Any of these** or **All of these**. This determines whether matches on all or any of the items in the group is required for the condition to hold. If you specified more than one sensitivity label, you'll only be able to choose **Any of these**, since Fabric and Power BI items can't have more than one label applied.

The image below shows a group (Default) that contains two sensitivity label conditions. The logic Any of these means that a match on any one of the sensitivity labels in the group constitutes *true* for that group.

You can use the **Quick summary** toggle to get the logic of the rule summarized in a sentence.

You can create more than one group, and you can control the logic between the groups with **AND** or **OR** logic.

The image below shows a rule containing two groups, joined by **OR** logic.

Here's the same rule shown as a quick summary.

Actions

If you want the policy to restrict access to items that trigger the policy, expand the **Restrict access or encrypt the content in Microsoft 365 locations** section and select **Block users from receiving email, or accessing shared SharePoint, OneDrive, and Teams files, and Power BI items.**. Then choose whether to block everyone or only people in your organization.

When you enable the restrict access action, user overrides are automatically allowed.

> **Note**

The restrict access action is enforced on semantic models only.

User notifications

The user notifications section is where you configure your policy tip. Turn on the toggle, select the **Notify users in Office 365 service with a policy tip or email notifications** check box, and then select the **Policy tips** checkbox. Write your policy tip in the text box that appears.

User overrides

If you enabled user notifications and selected the **Notify users in Office 365 service with a policy tip** checkbox, owners of items that have DLP policy violations (owners - that is, users with an Admin or Member role in the workspace where the item is located) will be able to respond to violations on the Data loss prevention policies side pane, which they can display from a button or a link on the policy tip. The selection of response options they have depends on the choices you make in the **User overrides** section.

The options are described below.

- **Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions** (automatically selected when you've enabled user notifications and selected the **Notify users in**

Office 365 service with a policy tip checkbox): Users will be able to either report the issue as a false positive or override the policy.

- **Require a business justification to override**: Users will be able to either report the issue as a false positive or override the policy. If they choose to override, they'll need to provide a business justification.
- **Override the rule automatically if they report it as a false positive**: Users will be able to report the issue as a false positive and automatically override the policy, or they can just override the policy without reporting it as a false positive.
- If you select both **Override the rule automatically if they report it as a false positive** and **Require a business justification to override**, users will be able to report the issue as a false positive and automatically override the policy, or they can just override the policy without reporting it as a false positive, but they'll have to provide a business justification.

Overriding a policy means that from now on the policy will no longer check the item for sensitive data.

Reporting an issue as a false positive means that the data owner believes that the policy has mistakenly identified non-sensitive data as sensitive. You can use false positives to fine tune your rules.

Any action the user takes is logged for reporting.

Incident reports

Assign a severity level that will be shown in alerts generated from this policy. Enable (default) or disable email notification to admins, specify users or groups for email notification, and configure the details about when notification will occur.

Additional options

Considerations and limitations

- DLP policy templates aren't yet supported for Fabric DLP policies. When creating a DLP policy for Fabric, choose the *custom policy* option.
- Fabric DLP policy rules currently support sensitivity labels and sensitive info types as conditions.

Related content

- Create and Deploy data loss prevention policies
- Get started with Data loss prevention policies for Fabric and Power BI
- Respond to a DLP policy violation
- Monitor DLP policy violations

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Respond to a DLP policy violation in Fabric and Power BI

Article • 11/19/2024

When a supported item type you own violates a DLP policy for Fabric and Power BI, a violation icon on the item in the OneLake data hub or workspace list view appears. Hover over the icon and select **Show full details** to display a side panel that displays the details of your item's DLP policy violations and provides options for responding to them. Alternatively:

- From a semantic model details page, select the **View all** button on the policy tip.
- In a lakehouse's edit mode, select the policy violation notice in the header and then select **View all** in the policy violation section of the flyout that appears.

This article describes the information you see on the side pane and the actions you can take regarding the violations.

View an item's DLP violations

The data loss prevention side pane lists the name of the item and all the DLP policy issues detected by a content scan of that item. You can select the item's name if you want to view the item's details.

Each DLP policy issue is shown on a card. The card shows you the policy tip, indicates what kind of sensitive data was detected, and offers actions you can take if you believe the data was falsely identified.

Violations of policies configured with the restrict access action are indicated in red and indicate who access is restricted to.

Take action on the violation

The action or combination of actions you see might vary depending on the policy configuration. The possible actions are:

- **Report an issue**: Report the issue as a false positive (that is, report that the policy has mistakenly identified nonsensitive data as sensitive).
- **Override**: Override the policy. Overriding a policy means that this policy will no longer check this item for sensitive data. Depending on the policy configuration,

you might be required to provide a justification for the override.

- **Report and override**: Report the issue as a false positive and override the policy.

> **Note**
>
> Any action you take will be recorded in the audit log where it can be reviewed by security admins.
>
> The purpose of the policy tip is to flag sensitive information found in your item. If you own this data and determine that it shouldn't be in the item, when you remove the data from the item, the next time the item is evaluated, the policy tip will be removed, since the sensitive data will no longer be found.

Related content

- Get started with Data loss prevention policies for Fabric and Power BI
- Configure a DLP policy for Fabric and Power BI
- Monitor and manage DLP policy violations
- Learn about data loss prevention

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Power BI Security

Article • 02/28/2025

For detailed information about Power BI security, see the Power BI Security white paper.

To plan for Power BI security, see the Power BI implementation planning security series of articles. It expands upon the content in the Power BI Security white paper. While the Power BI security white paper focuses on key technical topics such as authentication, data residency, and network isolation, the primary goal of the series is to provide you with considerations and decisions to help you plan for security and privacy.

The Power BI service is built on **Azure**, Microsoft's cloud computing infrastructure and platform. The architecture of the Power BI service is based on two clusters:

- The Web Front End (**WFE**) cluster. The **WFE** cluster manages the initial connection and authentication to the Power BI service.
- The **Back-End** cluster. Once authenticated, the **Back-End** handles all subsequent user interactions. Power BI uses Microsoft Entra ID to store and manage user identities. Microsoft Entra ID also manages data storage and metadata using Azure BLOB and Azure SQL Database, respectively.

Power BI Architecture

The **WFE** cluster uses Microsoft Entra ID to authenticate clients, and provide tokens for subsequent client connections to the Power BI service. Power BI uses the **Azure Traffic Manager** (Traffic Manager) to direct user traffic to the nearest datacenter. Traffic Manager directs requests using the DNS record of the client attempting to connect, authenticate, and to download static content and files. Power BI uses the **Azure Content Delivery Network** (CDN) to efficiently distribute the necessary static content and files to users based on geographical locale.

The **Back-End** cluster determines how authenticated clients interact with the Power BI service. The **Back-End** cluster manages visualizations, user dashboards, semantic models, reports, data storage, data connections, data refresh, and other aspects of interacting with the Power BI service. The **Gateway Role** acts as a gateway between user requests and the Power BI service. Users don't interact directly with any roles other than the **Gateway Role**. **Azure API Management** eventually handles the **Gateway Role**.

> ⓘ **Important**
>
> Only **Azure API Management** and **Gateway** roles are accessible through the public Internet. They provide authentication, authorization, DDoS protection, throttling, load balancing, routing, and other capabilities.

Data Storage Security

Power BI uses two primary repositories for storing and managing data:

- Data uploaded from users is typically sent to **Azure Blob Storage**.
- All metadata including items for the system itself are stored in the **Azure SQL Database**.

The dotted line shown in the **Back-End** cluster diagram, clarifies the boundary between the two components that are accessible by users shown on the left of the dotted line. Roles that are only accessible by the system are shown on the right. When an authenticated user connects to the Power BI Service, the connection and any request by the client is accepted and managed by the **Gateway Role** which then interacts on the user's behalf with the rest of the Power BI Service. For example, when a client attempts to view a dashboard, the **Gateway Role** accepts that request, and then separately sends a request to the **Presentation Role** to retrieve the data needed by the browser to display the dashboard. Eventually, connections and client requests are handled by **Azure API Management**.

User Authentication

Power BI uses Microsoft Entra ID to authenticate users who sign in to the Power BI service. Sign-in credentials are required whenever a user attempts to access secure resources. Users sign in to the Power BI service using the email address with which they established their Power BI account. Power BI uses the same credentials as the *effective username* and passes it to resources whenever a user attempts to connect to data. The *effective username* is then mapped to a User Principal Name and resolves to the associated Windows domain account against which authentication is applied.

For organizations that used work email addresses for Power BI sign-in, for example `david@contoso.com`, the *effective username* to UPN mapping is straightforward. For organizations that didn't use work email addresses, for example `david@contoso.onmicrosoft.com` mapping between Microsoft Entra ID and on-premises credentials requires directory synchronization to work properly.

Platform security for Power BI also includes multitenant environment security, networking security, and the ability to add other Microsoft Entra ID-based security measures.

Data and Service Security

For more information, see Microsoft Trust Center, Products and services that run on trust.

As described earlier, on-premises AD servers use a Power BI sign-in to map to a UPN for credentials. However, users must understand the sensitivity of the data they share. After you securely connect to a data source, and then share reports, dashboards, or semantic models with others, the recipients are granted access to the report. Recipients don't have to sign in to the data source.

An exception is connecting to **SQL Server Analysis Services** using the **On-premises data gateway**. Dashboards are cached in Power BI, but access to underlying reports or semantic models initiates authentication for each user that attempts to access the report or semantic model. Access will only be granted if the user has sufficient credentials to access the data. For more information, see On-premises data gateway in-depth.

Enforcing TLS version usage

Network and IT administrators can enforce the requirement for using current Transport Layer Security (TLS) for any secured communication on their network. Windows provides support for TLS versions over the Microsoft Schannel Provider, for more information, see Protocols in the TLS/SSL (Schannel SSP).

This enforcement is implemented by administratively setting registry keys. For enforcement details, see Managing SSL/TLS Protocols and Cipher Suites for AD FS.

Power BI Desktop requires TLS (Transport Layer Security) version 1.2 (or higher) to secure your endpoints. Web browsers and other client applications that use TLS versions earlier than TLS 1.2 won't be able to connect. If a newer version of TLS is required, Power BI Desktop respects the registry key settings described in those articles, and only creates connections meeting the version requirement of TLS allowed based on those registry settings, when present.

For more information about setting these registry keys, see Transport Layer Security (TLS) registry settings.

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Power BI Desktop privacy levels

Article • 03/15/2024

In **Power BI Desktop**, privacy levels specify isolation levels that determine the degree to which one data source is isolated from other data sources. Although a restrictive isolation level blocks information from being exchanged between data sources, it can reduce functionality and performance.

Data source settings

To configure data source settings:

1. Select **File**, and then select **Options and settings**.
2. Select **Data source settings**.
3. Select a data source from the list, and then select **Edit Permissions**.
4. Under **Privacy Levels**, select a privacy level.
5. Select **OK**, and then select **Close**.

The following table describes data source privacy levels:

Expand table

Setting	Description	Example data sources
Private	Data sources set to **Private** contain sensitive or confidential information. Visibility can be restricted to authorized users. Data from a private data source won't fold in to other data sources, including other private data sources.	Facebook data, a text file containing stock awards, or a workbook containing employee review information.
Organizational	Data sources set to **Organizational** can fold in to private and other organizational data sources. They can't fold in to public data sources. Visibility is set to a trusted group.	A Microsoft Word document on an intranet SharePoint site with permissions enabled for a trusted group.
Public	Files, internet data sources, and workbook data can be set to **Public**. Data can fold in to other data sources. Visibility is available to everyone.	Free data from the Azure Marketplace, data from a Wikipedia page, or a local file containing data copied from a public web page.

Caution

Configure a data source containing highly sensitive or confidential data as **Private**.

Privacy levels

To configure privacy options for a file:

1. Select **File**, and then select **Options and settings**.
2. Select **Options**.
3. Under **Current File**, select **Privacy**.
4. Under **Privacy Levels**, select a privacy level.
5. Select **OK**.

The following table describes privacy level settings:

Expand table

Setting	Description
Combine data according to your Privacy Level settings for each source (Default)	When selected, data is combined according to your privacy levels setting. Merging data across Privacy isolation zones will result in some data buffering.
Ignore the Privacy Levels and potentially improve performance	When selected, data is combined ignoring your privacy level setting. Ignoring the privacy setting can reveal sensitive or confidential data to an unauthorized user. This setting might improve performance and functionality.

Caution

- **Ignore the Privacy Levels and potentially improve performance** doesn't work in the Power BI service. Reports created in Power BI Desktop with this setting and published to the Power BI service don't adhere to the setting. However, the privacy levels are available on the personal gateway.
- Power BI Desktop can't ensure the privacy of data merged into another Power BI Desktop file.

Related content

- Power BI implementation planning: Content creator security planning
- Questions? Try asking the Power BI Community
- Suggestions? Contribute ideas to improve Power BI

Use service tags with Power BI

Article • 01/20/2024

You can use *Azure service tags* with Power BI to enable an Azure SQL Managed Instance (MI) to allow incoming connections from the Power BI service. In Azure, a *service tag* is a defined group of IP addresses that you can configure to be automatically managed, as a group, to minimize the complexity of updates or changes to network security rules. By using service tags with Power BI, you can enable a SQL Managed Instance to allow incoming connections from the Power BI service.

The following configurations are necessary to successfully enable the endpoints for use in the Power BI service:

1. Enable a public endpoint in the SQL Managed Instance.
2. Create a Network Security Group rule to allow inbound traffic.
3. Enter the credentials in Power BI.

The following sections look at each of these steps in turn.

Enable a public endpoint

The first part of the process is to enable a public endpoint in the SQL Managed Instance. Take the following steps:

1. Sign in to the Azure portal and navigate to your SQL Managed Instance.

2. On the left side of the page, select **Networking**.

3. Slide **Public endpoint (data)** to **Enable**, then set the **Minimum TLS version** to **1.2**. The following image shows the screen in the Azure portal.

4. Select **Save** to save your settings.

Create a network security group rule

The next collection of steps requires that you create a *Network Security Group (NSG)* rule to allow inbound traffic for the Power BI service. This action can be completed in the Azure portal by leveraging the "Source service tag" of Power BI or by using either the *command-line interface (CLI)* or PowerShell.

> **Note**
>
> The priority of the rule you set must be higher than the 4096 *deny_all_inbound* rule, which means the priority value must be lower than 4096. In the following example, a priority value of 400 is used.

The following *CLI script* is provided as a reference example. For more information, see az network nsg rule. You might need to change multiple values for the example to work properly in your situation. A PowerShell script is provided afterward.

Azure CLI

```
#login to azure
az login

#set subscription that contains SQL MI instance
$subname = "mysubscriptionname"
az account set --subscription $subname
```

```
#set NSG rule for inbound PowerBI traffic

#update $RG to your resource group name
$rg = 'myresourcegroup'
#update $nsg to your Network Security Group name
$nsg = 'nsgresourcename'
# Name the NSG rule
$rule = 'allow_inbound_PowerBI'
#set the priority - this must be higher priority (lower number) than the
deny_all_inbound rule
$priority = 400
#specifiy the service tag to use
$servicetag = 'PowerBI'
#specify the public endpoint port defined in step 1
$port = 3342
#set the rule to inbound direction
$direction = 'Inbound'
#set the access type to "Allow"
$access = 'Allow'
#Set the protocol as TCP
$protocol = 'tcp'
#Provide a description for the rule
$desc = 'Allow PowerBI Access to SQL MI for Direct Query or Data Refresh.'

#create the NSG rule
az network nsg rule create -g $rg \
--nsg-name $nsg -n $rule --priority $priority \
--source-address-prefixes $servicetag --destination-address-prefixes '*' \
--destination-port-ranges $port --direction $direction --access $access \
--protocol $protocol --description $desc
```

The following *PowerShell* script is provided as another reference to create the NSG rule. For more information, see Add a network security group rule in PowerShell. You might need to change multiple values for the example to work properly in your situation.

PowerShell

```
#login to azure
Login-AzAccount

#get your subscription ID
Get-AzSubscription

####
#Script to create Network Security Group Rule
###

#enter your subscription ID
Set-AzContext -SubscriptionId "yoursubscriptionID"

#Provide the resource group for your Network Security Group
```

```
$RGname="yourRG"
#Enter the port for the SQL Managed Instance Public Endpoint
$port=3342
#name the NSG rule
$rulename="allow_inbound_PowerBI"
#provide the name of the Network Security Group to add the rule to
$nsgname="yourNSG"
#set direction to inbound to allow PowerBI to access SQL MI
$direction ="Inbound"
#set the priority of the rule. Priority must be higher (ie. lower number)
than the deny_all_inbound (4096)
$priority=400
#set the service tags for the source to \u201cPowerBI\u201d
$serviceTag = "PowerBI"

# Get the NSG resource
$nsg = Get-AzNetworkSecurityGroup -Name $nsgname -ResourceGroupName $RGname

# Add the inbound security rule.
$nsg | Add-AzNetworkSecurityRuleConfig -Name $rulename -Description "Allow
app port" -Access Allow `
    -Protocol * -Direction $direction -Priority $priority -
SourceAddressPrefix $serviceTag -SourcePortRange * `
    -DestinationAddressPrefix * -DestinationPortRange $port

# Update the NSG.
$nsg | Set-AzNetworkSecurityGroup
```

Enter the credentials in Power BI

The last part of the process is entering the credentials in the Power BI service.

1. Sign in to the Power BI service and navigate to the workspace containing the dataset(s) that are using SQL Managed Instance. In the following example, that workspace is called *ASAdataset* and the dataset is called *Contoso SQL MI Demo*.

2. Select **Settings** from the top-right corner, then choose **Settings** from the dropdown menu.

3. Under **Datasets**, expand the **Data source credentials** section.

4. Select the **Edit credentials** link. In the dialog box that appears, enter valid credentials.

Save your settings and exit. Your SQL Managed Instance is now configured to allow incoming connections from the Power BI service.

Related content

- What is Power BI Premium?
- Enable a public endpoint in the SQL Managed Instance
- az network nsg rule
- Add a network security group rule in PowerShell

Private links for secure access to Fabric

Article • 01/17/2025

You can use private links to provide secure access for data traffic in Fabric. Azure Private Link and Azure Networking private endpoints are used to send data traffic privately using Microsoft's backbone network infrastructure instead of going across the internet.

When private link connections are used, those connections go through the Microsoft private network backbone when Fabric users access resources in Fabric.

To learn more about Azure Private Link, see What is Azure Private Link.

Enabling private endpoints has an impact on many items, so you should review this entire article before enabling private endpoints.

What is a private endpoint?

Private endpoint guarantees that traffic going *into* your organization's Fabric items (such as uploading a file into OneLake, for example) always follows your organization's configured private link network path. You can configure Fabric to deny all requests that don't come from the configured network path.

Private endpoints *don't* guarantee that traffic from Fabric to your external data sources, whether in the cloud or on-premises, is secured. Configure firewall rules and virtual networks to further secure your data sources.

A private endpoint is a single, directional technology that lets clients initiate connections to a given service but doesn't allow the service to initiate a connection into the customer network. This private endpoint integration pattern provides management isolation since the service can operate independently of customer network policy configuration. For multitenant services, this private endpoint model provides link identifiers to prevent access to other customers' resources hosted within the same service.

The Fabric service implements private endpoints and not service endpoints.

Using private endpoints with Fabric provides the following benefits:

- Restrict traffic from the internet to Fabric and route it through the Microsoft backbone network.
- Ensure only authorized client machines can access Fabric.

- Comply with regulatory and compliance requirements that mandate private access to your data and analytics services.

Understand private endpoint configuration

There are two tenant settings in the Fabric admin portal involved in Private Link configuration: **Azure Private Links** and **Block Public Internet Access**.

If Azure Private Link is properly configured and **Block public Internet access** is **enabled**:

- Supported Fabric items are only accessible for your organization from private endpoints, and aren't accessible from the public Internet.
- Traffic from the virtual network targeting endpoints and scenarios that support private links are transported through the private link.
- Traffic from the virtual network targeting endpoints and scenarios that *don't* support private links will be blocked by the service, and won't work.
- There might be scenarios that don't support private links, which therefore will be blocked at the service when **Block Public Internet Access** is enabled.

If Azure Private Link is properly configured and **Block public Internet access** is **disabled**:

- Traffic from the public Internet will be allowed by Fabric services.
- Traffic from the virtual network targeting endpoints and scenarios that support private links are transported through the private link.
- Traffic from the virtual network targeting endpoints and scenarios that *don't* support private links are transported through the public Internet, and will be allowed by Fabric services.
- If the virtual network is configured to block public Internet access, scenarios that don't support private links will be blocked by the virtual network, and won't work.

Private Link in Fabric experiences

OneLake

OneLake supports Private Link. You can explore OneLake in the Fabric portal or from any machine within your established virtual network using OneLake file explorer, Azure Storage Explorer, PowerShell, and more.

Direct calls using OneLake regional endpoints don't work via private link to Fabric. For more information about connecting to OneLake and regional endpoints, see How do I connect to OneLake?.

Warehouse and Lakehouse SQL analytics endpoint

Accessing a Warehouse or the SQL analytics endpoint of a Lakehouse in the Fabric portal is protected by private link. Customers can also use Tabular Data Stream (TDS) endpoints (for example, SQL Server Management Studio, Azure Data Studio) to connect to Warehouse via private link.

Visual query in Warehouse doesn't work when the **Block Public Internet Access** tenant setting is enabled.

SQL database

Accessing a SQL database or the SQL analytics endpoint in the Fabric portal is protected by private link. Customers can also use Tabular Data Stream (TDS) endpoints (for example, SQL Server Management Studio or Visual Studio Code) to connect to SQL database via private link. For more information on connecting to a SQL database, see Authentication in SQL database in Microsoft Fabric.

Lakehouse, Notebook, Spark job definition, Environment

Once you've enabled the **Azure Private Link** tenant setting, running the first Spark job (Notebook or Spark job definition) or performing a Lakehouse operation (Load to Table, table maintenance operations such as Optimize or Vacuum) will result in the creation of a managed virtual network for the workspace.

Once the managed virtual network has been provisioned, the starter pools (default Compute option) for Spark are disabled, as these are prewarmed clusters hosted in a shared virtual network. Spark jobs run on custom pools that are created on-demand at the time of job submission within the dedicated managed virtual network of the workspace. Workspace migration across capacities in different regions isn't supported when a managed virtual network is allocated to your workspace.

When the private link setting is enabled, Spark jobs won't work for tenants whose home region doesn't support Fabric Data Engineering, even if they use Fabric capacities from other regions that do.

For more information, see Managed VNet for Fabric.

Dataflow Gen2

You can use Dataflow gen2 to get data, transform data, and publish dataflow via private link. When your data source is behind the firewall, you can use the VNet data gateway to

connect to your data sources. The VNet data gateway enables the injection of the gateway (compute) into your existing virtual network, thus providing a managed gateway experience. You can use VNet gateway connections to connect to a Lakehouse or Warehouse in the tenant that requires a private link or connect to other data sources with your virtual network.

Pipeline

When you connect to Pipeline via private link, you can use the data pipeline to load data from any data source with public endpoints into a private-link-enabled Microsoft Fabric lakehouse. Customers can also author and operationalize data pipelines with activities, including Notebook and Dataflow activities, using the private link. However, copying data from and into a Data Warehouse isn't currently possible when Fabric's private link is enabled.

ML Model, Experiment, and AI skill

ML Model, Experiment, and AI skill supports private link.

Power BI

- If internet access is disabled, and if the Power BI semantic model, Datamart, or Dataflow Gen1 connects to a Power BI semantic model or Dataflow as a data source, the connection will fail.
- Publish to Web isn't supported when the tenant setting **Azure Private Link** is enabled in Fabric.
- Email subscriptions aren't supported when the tenant setting **Block Public Internet Access** is enabled in Fabric.
- Exporting a Power BI report as PDF or PowerPoint isn't supported when the tenant setting **Azure Private Link** is enabled in Fabric.
- If your organization is using Azure Private Link in Fabric, modern usage metrics reports will contain partial data (only Report Open events). A current limitation when transferring client information over private links prevents Fabric from capturing Report Page Views and performance data over private links. If your organization had enabled the **Azure Private Link** and **Block Public Internet Access** tenant settings in Fabric, the refresh for the dataset fails and the usage metrics report doesn't show any data.

- Copilot isn't currently supported for Private Link or closed network environments.

Eventhouse

Eventhouse supports Private Link, allowing secure data ingestion and querying from your Azure Virtual Network via a private link. You can ingest data from various sources, including Azure Storage accounts, local files, and Dataflow Gen2. Streaming ingestion ensures immediate data availability. Additionally, you can utilize KQL queries or Spark to access data within an Eventhouse.

Limitations:

- Ingesting data from OneLake isn't supported.
- Creating a shortcut to an Eventhouse isn't possible.
- Connecting to an Eventhouse in a data pipeline isn't possible.
- Ingesting data using queued ingestion isn't supported.
- Data connectors relying on queued ingestion aren't supported.
- Querying an Eventhouse using T-SQL isn't possible.

Healthcare data solutions (preview)

Customers can provision and utilize Healthcare data solutions in Microsoft Fabric through a private link. Within a tenant that has been enabled with a private link, customers can deploy Healthcare data solution capabilities to execute comprehensive data ingestion and transformation scenarios for their clinical data. This includes the ability to ingest healthcare data form various sources, such as Azure Storage accounts, and more.

Azure and Fabric Events

Azure and Fabric events support private link such that when the **Block Public Internet Access** tenant setting is enabled:

- Any new configuration to consume Azure events, like Azure Blob Storage events, would be blocked.
- Existing configurations that are consuming Azure events will start losing any new events.

Other Fabric items

Other Fabric items, such as Eventstream, don't currently support Private Link, and are automatically disabled when you turn on the **Block Public Internet Access** tenant setting in order to protect compliance status.

Microsoft Purview Information Protection

Microsoft Purview Information Protection doesn't currently support Private Link. This means that in Power BI Desktop running in an isolated network, the **Sensitivity** button is grayed out, label information won't appear, and decryption of *.pbix* files will fail.

To enable these capabilities in Desktop, admins can configure service tags for the underlying services that support Microsoft Purview Information Protection, Exchange Online Protection (EOP), and Azure Information Protection (AIP). Make sure you understand the implications of using service tags in a private links isolated network.

Other considerations and limitations

There are several considerations to keep in mind while working with private endpoints in Fabric:

- Fabric supports up to 450 capacities in a tenant where Private Link is enabled.
- When capacity is newly created, it won't support private link until its endpoint is reflected in the private DNS zone. This can take up to 24 hours.
- Tenant migration is blocked when Private Link is turned on in the Fabric admin portal.
- Customers can't connect to Fabric resources in multiple tenants from a single virtual network, but rather only the last tenant to set up Private Link.
- Private link doesn't support in Trial capacity. When accessing Fabric via Private Link traffic, trial capacity won't work.
- Any uses of external images or themes aren't available when using a private link environment.
- Each private endpoint can be connected to one tenant only. You can't set up a private link to be used by more than one tenant.
- **For Fabric users**: On-premises data gateways aren't supported and fail to register when Private Link is enabled. To run the gateway configurator successfully, Private

Link must be disabled. Learn more about this scenario. VNet data gateways will work. For more information, see these considerations.

- **For non-PowerBI (PowerApps or LogicApps) Gateway users**: The on-premises data gateway isn't supported when Private Link is enabled. We recommend exploring the use of the VNET data gateway, which can be used with private links.
- Private Links won't work with VNet Data Gateway download diagnostics.
- Private links resource REST APIs don't support tags.
- The following URLs must be accessible from the client browser:
  - Required for auth:
    - `login.microsoftonline.com`
    - `aadcdn.msauth.net`
    - `msauth.net`
    - `msftauth.net`
    - `graph.microsoft.com`
    - `login.live.com`, though this may be different based on account type.
  - Required for the Data Engineering and Data Science experiences:
    - `http://res.cdn.office.net/`
    - `https://aznbcdn.notebooks.azure.net/`
    - `https://pypi.org/*` (for example, `https://pypi.org/pypi/azure-storage-blob/json`)
    - local static endpoints for condaPackages
    - `https://cdn.jsdelivr.net/npm/monaco-editor*`

Related content

- Set up and use secure private endpoints
- Managed VNet for Fabric
- Conditional Access
- How to find your Microsoft Entra tenant ID

Feedback

Was this page helpful? Yes No

Private endpoints for secure access to Power BI for on-premises clients

Article • 08/23/2023

If you've configured private links for secure access to data in Power BI, using Azure Private Links and Azure Networking private endpoints as described in Private endpoints for secure access to Fabric, then you can also enable Azure Virtual Machines to access the Power BI service through private IP addresses.

You can extend your on-premises networks to the Azure Virtual Network (VNet) using an ExpressRoute circuit, or a site-to-site VPN, to access and use services deployed in the Azure Virtual Networks with private connections.

Understand private endpoints for on-premises clients

When access to the Power BI service from the Virtual Network is already established, described in Private endpoints for secure access to Fabric, with few further steps you can extend private access to the Power BI service to on-premises clients.

This article describes the steps you must take to configure such private connectivity between the Azure VNet and the on-premises networks. To successfully complete the configuration, you must already have an ExpressRoute connection successful established, with established communication between the on-premises networks and Azure VNet. For more details about ExpressRoute setup, see Create and modify an ExpressRoute circuit.

The following network diagram shows how the configuration works.

The network diagram includes a handful of components:

- The Azure VNet
- **Private DNS zone** for the name resolution of Power BI URLs in private endpoint IP Addresses
- **Azure DNS private resolver** to extend the naming resolution of Azure private DNS zones to the on-premises network
- The **ExpressRoute Gateway, ExpressRoute Connection**, and **ExpressRoute circuit** to establish the connectivity between the on-premises network and Azure VNet
- The **on-premises DNS server** for local naming resolution and to forward the DNS requests for the Power BI service to the Azure Private DNS resolver

The following sections describe the steps required to configure connectivity to your existing private endpoints configuration for on-premises clients.

Configure connections for on-premises clients

The following list provides an overview of the steps necessary to configure access to the Power BI service from on-premises, through ExpressRoute private peering. Sections following this list provide more detail and examples to help with configuration.

An overview of the necessary steps is described in the following steps:

1. In the Azure Virtual Network, create a subnet for hosting the ExpressRoute Gateway. The network assigned to the subnet needs to be at least /27 or larger (/26, /25, and so on), as described in the ExpressRoute documentation. The name assignment to the subnet *must* be **GatewaySubnet**; changing or modifying the subnet name will disable your configuration.
2. Deploy an ExpressRoute gateway in the **GatewaySubnet**. You can deploy the ExpressRoute Gateway in various ways, including in the Azure management portal, PowerShell, Azure CLI, or using REST APIs.
3. Verify your ExpressRoute circuit is already deployed and working, and that private peering is properly configured. To verify, follow the tutorial that explains how to create Azure private peering.
4. Create a connection, the steps for which are described in this tutorial, to link the ExpressRoute Gateway in the VNet to the ExpressRoute circuit.
5. Verify the on-premises hosts or VMs can successfully access the workload or workloads. You can begin by using a simple PING test, but a better verification is to use applications (such as an HTTP/HTTPS connection between on-premises client and a web server in an Azure VM).
6. In the Azure VNet, create two subnets to host the endpoints of the Azure DNS Private Resolver: one subnet for inbound endpoints, one subnet for outbound endpoints.
7. Inside the Azure Virtual Network create an Azure DNS Private Resolver. Inside the Azure DNS Private Resolver, configure the **inbound endpoint**. The inbound endpoint in the Azure DNS Private Resolver enables you to query Azure DNS Private Zones for the Power BI services from an on-premises network.
8. Configure on-premises DNS Servers with Condition Forwarders for the naming resolution associated to the DNS Private Zones for the Power BI service.

While many of the previous steps are self explanatory, some merit more explanation. The following sections provide more detail for some of the previous configuration steps.

Step 6: Create two subnets to host endpoints

The **Azure DNS Private Resolver** uses two subnets: one subnet for the inbound endpoint, and another subnet for the outbound endpoint. For the endpoint subnets of the DNS Private Resolver, you must assign the delegation to **Microsoft.Network/dnsResolvers**. The subnets can only be delegated to **Microsoft.Network/dnsResolvers** and can't be used for other services. Without such delegation, the inbound endpoint creation will fail.

The following screenshot shows how to configure delegation.

The following screenshot shows another screen demonstrating the delegation.

Step 7: Create An Azure DNS Private Resolver

To create an **Azure DNS Private Resolver**, to do the Azure Marketplace and search for *DNS private resolver*, and select the result shown in the following screenshot.

Configure the Azure DNS Private Resolver to the VNet. The DNS Private Resolver and the VNet must exist in the same Azure region.

The Azure DNS Private Resolver is based on two components: inbound endpoints and outbound endpoint. For naming resolution of Power BI URLs in the on-premises hosts/VMs, only the inbound endpoint is required. The following image shows where you can configure the inbound endpoints.

An inbound endpoint enables name resolution from on-premises devices using an IP address that's part of your private VNet address space. In the **Azure Management** portal, in the DNS private resolver, select **inbound endpoints** as shown in the previous image, then select **Add an endpoint** as shown in the following screenshot.

Next you assign an *endpoint name* and select the subnet you defined in previous step, as shown in the following screenshot:

Once the process of deployment of inbound endpoint is completed, an IP address is automatically associated to the inbound endpoint.

In this example, and shown in the previous screenshot, the IP address assigned to the inbound endpoint is 10.7.2.4. That assigned IP address is used in step 8 as Conditional Forwarder IP in the on-premises DNS server, described in more detail in the following section.

Step 8: Configure on-premises DNS servers

To properly resolve your Azure Private DNS zones from on-premises, define the Conditional Forwarders associated with the Power BI service in your on-premises DNS server configuration.

The IP address of each Conditional Forwarder points to the IP address of the inbound endpoint in the Azure DNS Private Resolver.

The following screenshot shows an example of DNS Conditional Forwarder entries in Windows server.

Verification of successful configuration

As final step for your configuration, sign in to the on-premises Windows client and perform a verification by using nslookup. If properly configured, you'll receive a response similar to the following message.

```
C:\ > nslookup <tenant-object-id-without-hyphens>-
api.privatelink.analysis.windows.net
Server:  UnKnown
Address:  10.1.21.10           <- IP address of on-premises DNs server
Non-authoritative answer:
Name:    <tenant-object-id-without-hyphens>-
api.privatelink.analysis.windows.net
Address:  10.7.0.5
```

The Power BI service URL is translated into the private IP that's assigned to the private endpoint, which is configured in the VNet and connected to the Power BI service.

Considerations and limitations

- You must configure private endpoints before enabling private endpoints for on-premises clients. See Private endpoints for secure access to Fabric for more information.

Related content

- Private endpoints for secure access to Fabric
- Create and modify an ExpressRoute circuit
- ExpressRoute documentation
- ExpressRoute gateway
- How to create Azure private peering
- Azure DNS Private Resolver

More questions? Ask the Power BI Community.

Configure mobile apps with Microsoft Intune

Article • 01/16/2023

Microsoft Intune enables organizations to manage devices and applications. The Power BI mobile applications for iOS and Android integrate with Intune. This integration enables you to manage the application on your devices, and to control security. Through configuration policies, you can control items like requiring an access pin, how data is handled by the application, and even encrypting application data when the app isn't in use.

The Microsoft Power BI mobile app allows you to get access to your important business information. You can view and interact with your dashboards and reports for all your organization's managed devices and app business data. For more information about supported Intune apps, see Microsoft Intune protected apps.

General mobile device management configuration

This article assumes that Intune is configured properly and you have devices enrolled with Intune. This article isn't meant as a full configuration guide for Intune. For more information about Intune, see What is Intune?.

Microsoft Intune can co-exist with Mobile Device Management (MDM) within Microsoft 365. If you're using MDM, the device will show as enrolled with MDM, but is available to manage in Intune.

Before end users use the Power BI app on their devices, an Intune admin must add the app to Intune and assign the app to end users.

> **Note**
>
> After you configure Intune, background data refresh is turned off for the Power BI mobile app on your iOS or Android device. Power BI refreshes the data from the Power BI service on the web when you open the app.

Step 1: Add the Power BI app to Intune

To add the Power BI app to Intune, follow the steps in the appropriate article:

- Add iOS store apps to Microsoft Intune
- Add Android store apps to Microsoft Intune

Step 2: Assign the app to your end users

After you've added the Power BI app to Microsoft Intune, assign the app to users and devices. It's important to note that you can assign an app to a device whether or not the device is managed by Intune.

To assign the Power BI app to users and devices, follow the steps in Assign apps to groups with Microsoft Intune.

Step 3: Create and assign app protection policies

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is in the app. A managed app is an app that has APP applied to it, and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allow you to manage and protect your organization's data in an app. With MAM without enrollment (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any device, including personal devices in bring-your-own-device (BYOD) scenarios. For more information, see App protection policies overview.

To create and assign an app protection policy for the Power BI app, follow the steps in How to create and assign app protection policies.

Step 4: Use the application on a device

Managed apps are apps that your company's support team can set up to help protect company data that you can access from the app. When you access company data in a managed app on your device, you might notice that the app works a little differently than what you expect. For example, you might not be able to copy and paste protected company data, or you might not be able to save that data to certain locations.

To understand how your end users can use the Power BI app on their device, review the steps in the following articles:

- Work or school apps for iOS
- Managed work and school apps for Android

Next steps

- How to create and assign app protection policies
- What are the Power BI mobile apps

More questions? Ask the Power BI Community

Power BI semantic model scale-out

Article • 11/13/2024

Semantic model scale-out helps Power BI deliver fast performance while your reports and dashboards are consumed by a large audience. Semantic model scale-out uses your Premium capacity to host one or more read-only *replicas* of your *primary* semantic model. By increasing throughput, the read-only replicas ensure performance doesn't slow down when multiple users submit queries at the same time.

When Power BI creates read-only replicas, it separates them from the primary read-write semantic model. The read-only replicas serve Power BI report and dashboard queries, and the read-write semantic model is used when write and refresh operations are performed. During write and refresh operations, the read-only replicas continue to serve your reports and dashboard queries without being disrupted. By default, the read-only and read-write semantic models are automatically synchronized so that the read-only replicas are kept up-to-date. However, you can disable automatic sync, and choose to synchronize manually at the command line or by script.

The following table shows the required synchronization for each refresh method when Power BI semantic model scale-out is *enabled*, and automatic synchronization is *disabled*:

Expand table

Refresh method	Sync
OnDemand UI	Always syncs
Scheduled Refresh	Always syncs
Basic REST API	Manual sync required [1]
Advanced REST API	Manual sync required [1]
XMLA	Manual sync required [1]

1 - With `autoSyncReadOnlyReplicas` in `queryScaleOutSettings` set to false.

Replica management

Scale-out creates one read-write semantic model replica, and as many read-only replicas as needed. All write operations are directed to the read-write replica. This includes queries on sessions that target the read-write replica explicitly, that is, don't use `?`

`readonly` in the connection string. These queries can cause high interactive CPU usage on the read-write replica. In such cases, a new replica isn't created because the query load targeting the read-write replica can't be distributed to read-only replicas.

The number of read-only replicas is determined based on the number of CUs that your queries consume. If the demand exceeds the compute resources currently available on a node where the model is loaded, and stays high, an additional read-only replica might be created on another node to distribute the load. The total number of CUs consumed by all replicas combined, however, can't exceed the maximum number of CUs that a single model is allowed to consume on your given capacity SKU.

For example, a given semantic model on an F64 capacity will have enough resources on a single node to consume all allowed CUs on that SKU. Therefore, F64 capacities typically do not scale out beyond a single read-only replica. On the other hand, F256 and F1024+ capacities are more likely to create a second read-only replica because a single node may not be sufficient to provide all the CUs that are allowed to be used on an F256/F1024+ capacity.

QSO is designed to leverage the available compute power of a given capacity SKU as efficiently and seamlessly as possible with the least number of read-only replicas, and without management overhead for semantic model owners.

However, the current load on a capacity might by high enough to cause throttling if more replicas are added. Throttling prevents additional read-only replicas from reaching a sustained high CPU usage. In such cases, a new scale out read-only replica isn't created.

A replica is removed when CU usage for the model reduces sufficiently and consistently stays low enough.

Prerequisites

By default, scale-out is enabled for your tenant, but it's not enabled for semantic models in your tenant. To enable scale-out for a semantic model, you must use the Power BI REST APIs. Before enabling, the following prerequisites must be met:

- The **Scale-out queries for large semantic models** setting for your tenant is enabled (default).
- Your workspace resides on a Power BI Premium capacity:
  - Premium Per User (PPU)
  - Power BI Premium P SKUs

- Power BI A SKUs for Power BI Embedded (also known as embed for your customers).
- Fabric F SKUs

- The Large semantic model storage format setting is enabled.
- To manage semantic models by using the REST API, use Power BI Management cmdlets. Install by opening PowerShell in Administrator mode, and running the command:

```
PowerShell
Install-Module -Name MicrosoftPowerBIMgmt
```

- The following (or higher) app, library, and service versions support connecting to read-only replicas:

Expand table

App, library or service	Version
Microsoft Analysis Services OLE DB Provider for Microsoft SQL Server (MSOLAP)	16.0.20.201 (March 2022)
Microsoft.AnalysisServices.AdomdClient (ADOMD.NET)	19.36.0 (March 2022)
Power BI Desktop	June 2022
SQL Server Management Studio (SSMS)	19.0
Tabular Editor 2	2.16.6
Tabular Editor 3	3.2.3
DAX Studio	3.0.0

Configure scale-out for a semantic model

To learn how to enable or disable scale-out for a semantic model, or get scale-out status by using PowerShell and the REST APIs, see Configure semantic model scale-out.

Connect to a specific semantic model type

When scale-out is enabled, the following connections are retained:

- By default, Power BI Desktop connects to a read-only replica.
- Live connection reports connect to a read-only replica.
- XMLA client applications connect to the read-write semantic model by default.
- Refreshes in the Power BI service and refreshes using the Enhanced Refresh REST API connect to the read-write semantic model.

You can connect to a read-only replica or the read-write semantic model by appending one of the following strings to the semantic model's URL:

- **Read-only** - `?readonly`
- **Read-write** - `?readwrite`

Disable semantic model scale-out for your tenant

Power BI semantic model scale-out is enabled by default for a tenant. Power BI tenant admins can disable this setting. To disable semantic model scale-out for the tenant, do the following:

1. Go to your tenant settings.
2. In **Scale-out settings**, expand **Scale-out queries for large semantic models**.
3. Toggle the switch to **Disabled**.
4. Select **Apply**.

Considerations and limitations

- Client applications can connect to a read-only replica through the XMLA endpoint, provided they support the mode specified in the connection string. Client applications can also connect to the read-write instance by using the XMLA endpoint.

- Manual and scheduled refreshes are always automatically synchronized with the latest version of the read-only replicas. REST API refreshes respect the automatic sync configuration. If automatic sync is disabled, your semantic model must be synced with the read-only replicas by using the manual sync REST API.

- With automatic sync disabled, XMLA updates and refreshes must be synced with the read-only semantic model copies by using the sync REST API.

- When deleting a Power BI scale-out semantic model, and creating another semantic model with the same name, allow five minutes to pass before creating the new semantic model. It might take Power BI a while to remove the replicas of the primary semantic model.

- When Power BI semantic model scale-out is enabled and `autoSyncReadOnlyReplicas=false`, changes to the following features, are not supported:
  - Adding or deleting roles
  - Updating the set of role memberships for any role

  - Modifying a data source
  - Deleting data sources used by a DirectQuery or a Dual table
  - Changes to object-level security (OLS) or dynamic row-level security (RLS) expressions

  To make changes to these features, disable scale-out and allow a few minutes for the change to take place before reenabling.

- Discovering role memberships using the Dynamic Management View (DMV) TMSCHEMA_ROLE_MEMBERSHIPS rowset, doesn't return any results when run against the read-only replica.

- Reports that use a Live connection always connect to the read-only replica, even if the connection string uses `?readwrite`. However, in Power BI Desktop, live connection reports using `?readwrite` connect to the read-write replica.

- The DBSCHEMA_CATALOGS and DISCOVER_XML_METADATA the Dynamic Management View (DMV) rowsets, return read-write replica information when using `?readonly` in the connection string.

- SQL server profiler doesn't work with the `?readonly` connection string.

- These operations trigger auto-sync even when auto sync is turned off (`AutoSync=Off`).
  - Migrating a workspace from one capacity to another.
  - Switching (or rotating) the version of the key used for Bring your own encryption keys (BYOK).
  - Moving a semantic model's workspace from a capacity that doesn't use BYOK to a capacity that uses BYOK.
  - Moving a semantic model's workspace from a capacity that uses BYOK to a capacity that doesn't uses BYOK.
  - Restoring a semantic model using the public XMLA endpoint.

- Disabling Large semantic model storage format disables scale-out and loses all sync information.

Related content

- Configure semantic model scale-out

- Tutorial: Test semantic model scale-out

- Synchronize scale-out replicas

- Compare semantic model scale-out replicas

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Configure semantic model scale-out

Article • 11/28/2023

You can enable scale-out in Power BI service, or using the Power BI Datasets REST APIs. Before configuring semantic model, read the Power BI semantic model scale-out overview.

Enable scale-out in Power BI service

To enable scale-out for your semantic model in Power BI service, follow these steps:

1. In Power BI service, open the workspace with the semantic model you want to enable scale-out for.
2. Select the semantic model's *more options* (...).
3. From the menu, select **Settings**.
4. In the setting's page, enable the Large semantic model storage format if it's not enabled.
5. Enable *Query scale-out* and select *Apply*.

Enable scale-out using the Datasets REST APIs

This section describes using the Power BI Datasets REST APIs to configure semantic model scale-out.

Get datasetId

To get the datasetId, use Get-PowerBIDataset. You must specify a workspaceId and semantic model name.

PowerShell

```
Login-PowerBI | Out-Null

$workspaceId = '<enter workspaceId>'

$datasetId = Get-PowerBIDataset -WorkspaceId $workspaceId `
    | Where{$_.Name -match "<enter semantic model name>"} `
    | Select-Object -ExpandProperty Id -First 1 `
    | ForEach-Object {$_.Guid}

Write-Host
Write-Host "Workspace Id: $workspaceId"
Write-Host "Dataset Id: $datasetId"
```

Get current scale-out configuration

Before configuring semantic model scale-out, determine the current configuration.

PowerShell

```
###
# Get current scale-out configuration
###
Login-PowerBI | Out-Null

$workspaceId = '<enter workspaceId>'

$datasetId = Get-PowerBIDataset -WorkspaceId $workspaceId `
    | Where{$_.Name -match "<enter semantic model name>"} `
    | Select-Object -ExpandProperty Id -First 1 `
    | ForEach-Object {$_.Guid}

$response = Invoke-PowerBIRestMethod -Url
"groups/$workspaceId/datasets/$datasetId" -Method Get | ConvertFrom-Json

$response.queryScaleOutSettings | Format-List

if ($response.queryScaleOutSettings.maxReadOnlyReplicas -eq -1 `
    -or $response.queryScaleOutSettings.maxReadOnlyReplicas -gt 0)
{
    Write-Host "Semantic model scale-out is enabled."
}
else
{
```

```
    Write-Host "Semantic model scale-out is disabled."
}
```

Enable semantic model scale-out

To enable semantic model scale-out, set `maxReadOnlyReplicas` to `-1`, or any non-0 value. A value of `-1` allows Power BI to create as many read-only replicas as your Power BI capacity supports. You can also explicitly set the replica count to a value lower than that of the capacity maximum. Setting `maxReadOnlyReplicas` to `-1` is recommended.

PowerShell

```
###
# Enable scale-out
###
Login-PowerBI | Out-Null

$workspaceId = '<enter workspaceId>'

$datasetId = Get-PowerBIDataset -WorkspaceId $workspaceId `
    | Where{$_.Name -match "<enter semantic model name>"} `
    | Select-Object -ExpandProperty Id -First 1 `
    | ForEach-Object {$_.Guid}

Invoke-PowerBIRestMethod -Url "groups/$workspaceId/datasets/$datasetId" `
    -Method Patch -Body '{ "queryScaleOutSettings": { "maxReadOnlyReplicas":
-1 }}'

Invoke-PowerBIRestMethod -Url "groups/$workspaceId/datasets/$datasetId" -
Method Get `
    | ConvertFrom-Json | Select-Object - expandProperty queryScaleOutSettings
`
    | ForEach {
        if($_.maxReadOnlyReplicas -eq -1)
        {
            Write-Host "Success! Semantic model scale-out has been enabled."
        } else
        {
            Write-Host "Something went wrong! Semantic model scale-out is
still disabled." -ForegroundColor Red
        }
     }
```

Disable semantic model scale-out

To disable semantic model scale-out, set `maxReadOnlyReplicas` to `0`.

PowerShell

```
###
# Disable scale-out
###
Login-PowerBI | Out-Null

$workspaceId = '<enter workspaceId>'

$datasetId = Get-PowerBIDataset -WorkspaceId $workspaceId `
    | Where{$_.Name -match "<enter semantic model name>"} `
    | Select-Object -ExpandProperty Id -First 1 `
    | ForEach-Object {$_.Guid}

Invoke-PowerBIRestMethod -Url "groups/$workspaceId/datasets/$datasetId" `
    -Method Patch -Body '{ "queryScaleOutSettings": { "maxReadOnlyReplicas":
0 }}'

Invoke-PowerBIRestMethod -Url "groups/$workspaceId/datasets/$datasetId" -
Method Get `
    | ConvertFrom-Json | Select-Object - expandProperty queryScaleOutSettings
`
    | ForEach {
        if($_.maxReadOnlyReplicas -eq 0)
        {
            Write-Host "Success! Semantic model scale-out has been
disabled."
        } else
        {
            Write-Host "Something went wrong! Semantic model scale-out is
still enabled." -ForegroundColor Red
        }
     }
```

Related content

- Power BI semantic model scale-out
- Tutorial: Test semantic model scale-out
- Synchronize scale-out replicas
- Compare semantic model scale-out replicas

Test semantic model scale-out

Article • 01/16/2024

This article describes how you can test the semantic model scale-out feature.

Step 1 - Create a scale-out query

1. Open Power BI Desktop and sign into your account.

2. Select **Transform data** to open the Power BI *Power Query Editor*.

3. In the Power BI *Power Query Editor*, select **New Source**.

4. In the *Get Data* pop-up window, select **Blank Query** and select **Connect**.

5. Select *Query 1*, and then select **Advanced editor**.

6. Enter the following *M Formula language* code.

```
let
    Source = "Dataset last refreshed:",
    #"Converted to Table" = #table(1, {{Source}}),
    #"Renamed Columns" = Table.RenameColumns(#"Converted to Table",
{{"Column1", "RefreshInfo"}})
in
    #"Renamed Columns"
```

7. Select **Done**.

8. In the *Power Query Editor* select **Close & Apply**.

Step 2 - Create a time column

1. In Power BI Desktop select **Data**.

2. In the *Fields* pane, select **Query 1**.

3. Select **New column**.

4. Enter the following DAX expression to define a new calculated column.

DAX

```
Time = NOW()
```

5. Select **Report**.

6. Select **Publish** and in the *Microsoft Power BI Desktop* pop-up window, select **Save**.

7. in the *Publish to Power BI* pop-up window, select the workspace you want to enable scale-out for, and then select **Select**.

Step 3 - Connect to the read-write semantic model (optional)

By default, Power BI Desktop connects to a read-only replica. To connect to the read-write semantic model, follow these steps:

1. In SQL Server Management Studio (SSMS), expand *Databases* and select the uploaded Power BI semantic model.

2. Run a simple DAX query such as:

```
DAX

Evaluate Query1
```

Step 4 - Validate the read/write connection (optional)

If you followed step 3, you're connected to the read-write semantic model. You can validate this connection by following these steps:

1. In SQL Server Management Studio (SSMS), right-click your semantic model, select **Process Database**.

2. In the *Process Database* dialog box, select **OK**.

3. Once the process completes successfully, select **Close** and close the *Process Database* window.

4. In the DAX query window, execute the query *Evaluate Query1* again. SQL Server Management Studio (SSMS) shows the latest refresh time because it's connected to the *read/write* replica.

Related content

- Power BI semantic model scale-out
- Configure semantic model scale-out
- Synchronize scale-out replicas
- Compare semantic model scale-out replicas

Synchronize scale-out replicas

Article • 09/22/2024

This article describes how to synchronize a semantic model scale-out replicas by using PowerShell at the command line or by script.

When you're working against the primary read-write semantic model, and semantic model users are using the read-only replicas, you can perform semantic model metadata updates and refreshes without affecting them. However, changes to the semantic model model and refreshes take place in the primary semantic model. To copy the changes to the read-only replicas, it must be synchronized with the read-write semantic model.

By default, the `autoSyncReadOnlyReplicas` parameter is set to `true` - Power BI synchronizes the replicas automatically. You can disable auto sync by setting `autoSyncReadOnlyReplicas` to `false`. However, you can choose to sync manually by using `syncStatus` and `sync` REST APIs.

To check the sync status of your replicas, use the `SyncStatus` REST API. This article describes the PowerShell commands for using this API.

Check replica sync status

PowerShell

```
###
# Check the scale-out replica sync status
###
Login-PowerBI | Out-Null

$workspaceId = '<enter workspaceId>'

$datasetId = Get-PowerBIDataset -WorkspaceId $workspaceId `
    | Where{$_.Name -match "<enter semantic model name>"} `
    | Select-Object -ExpandProperty Id -First 1 `
    | ForEach-Object {$_.Guid}

$response = Invoke-PowerBIRestMethod -Url
"groups/$workspaceId/datasets/$datasetId/queryScaleOut/syncStatus" -Method
Get | ConvertFrom-Json
$response | Format-List

if ($response.commitVersion -eq $response.minActiveReadVersion)
{
    Write-Host "Semantic model read-write and read-only replicas are in
sync."
```

```
}
else
{
    Write-Host "Semantic model read-write and read-only replicas are not in
sync." -ForegroundColor Red
}
```

If the sync status API returns an empty response or if **scaleOutStatus** is set to "**Unavailable**", try to load the semantic model's read-write replica or perform a refresh on the model to get the latest sync status.

To learn more, see Datasets - Get Query Scale Out Sync Status In Group in the Power BI REST API reference.

Disable automatic replica synchronization

PowerShell

```
###
# Disable automatic scale-out replica sync
###
Login-PowerBI | Out-Null

$workspaceId = '<enter workspaceId>'

$datasetId = Get-PowerBIDataset -WorkspaceId $workspaceId `
    | Where{$_.Name -match "<enter semantic model name>"} `
    | Select-Object -ExpandProperty Id -First 1 `
    | ForEach-Object {$_.Guid}

Invoke-PowerBIRestMethod -Url "groups/$workspaceId/datasets/$datasetId" `
    -Method Patch -Body '{ "queryScaleOutSettings": {
"autoSyncReadOnlyReplicas": false }}'

Invoke-PowerBIRestMethod -Url "groups/$workspaceId/datasets/$datasetId" -
Method Get `
    | ConvertFrom-Json | Select-Object -ExpandProperty queryScaleOutSettings
`
    | ForEach {
        if($_.autoSyncReadOnlyReplicas -eq $false)
        {
            Write-Host "Success! Automatic replica synchronization has been
disabled."
        } else
        {
            Write-Host "Something went wrong! Automatic replica
synchronization is still enabled." -ForegroundColor Red
```

```
        }
    }
```

Perform a manual replica sync (script)

PowerShell

```
###
# Perform a manual replica sync
###
Login-PowerBI | Out-Null

$workspaceId = '<enter workspaceId>'

$datasetId = Get-PowerBIDataset -WorkspaceId $workspaceId `
    | Where{$_.Name -match "<enter semantic model name>"} `
    | Select-Object -ExpandProperty Id -First 1 `
    | ForEach-Object {$_.Guid}

$response = Invoke-PowerBIRestMethod -Url
"groups/$workspaceId/datasets/$datasetId/queryScaleOut/sync" -Method Post -
Body "" | ConvertFrom-Json

Write-Host 'Synchronizing the scale-out replicas...' -NoNewLine

while ($response.commitVersion -ne $response.minActiveReadVersion)
{
    Write-Host '.' -NoNewLine
    Start-Sleep -Seconds 10

    $response = Invoke-PowerBIRestMethod -Url
"groups/$workspaceId/datasets/$datasetId/queryScaleOut/syncStatus" -Method
Get | ConvertFrom-Json
}

Write-Host 'Completed'
$response
```

To learn more, see Datasets - Trigger Query Scale Out Sync In Group in the Power BI REST API reference.

Perform a manual replica sync (command line)

Follow these steps to sync the replicas by using Windows PowerShell:

1. Open PowerShell and log into Power BI by running this command:

```
PowerShell

Login-PowerBI
```

2. Get your workspace Ids by running the command below. Replace `<WorkspaceName>` with the name of your workspace.

```
PowerShell

Get-PowerBIWorkspace -Name "<WorkspaceName>"  # Replace <WorkspaceName>
with the name of your workspace
```

3. Get the semantic model Id by running the command below. Replace `<WorkspaceId>` with the Id of your workspace.

```
PowerShell

Get-PowerBIDataset -WorkspaceId "<WorkspaceId>"  # Replace
<WorkspaceId> with the Id of your workspace
```

4. Check the sync status of your semantic model by using the command below. Replace the values of `<WorkspaceId>` and `<DatasetId>` accordingly.

```
PowerShell

Invoke-PowerBIRestMethod -Url
'groups/<WorkspaceId>/datasets/<DatasetId>/queryScaleOut/syncStatus' -
Method Get | ConvertFrom-Json | Format-List  # Replace <WorkspaceId>
with the Id of your workspace and <DatasetId> with the Id of your
semantic model
```

In the output, the `minActiveReadVersion` and `minActiveReadTimestamp` values refer to the read-only replica. The `commitVersion` and `commitTimestamp` values, refer to the read-write semantic model. A difference between them, indicates the read-only replica represents an older version of the semantic model.

5. Sync the read-write semantic model and read-only replicas by using the following command. Replace the values of `<WorkspaceId>` and `<DatasetId>` accordingly.

```
PowerShell

Invoke-PowerBIRestMethod -Url
'groups/<WorkspaceId>/datasets/<DatasetId>/queryScaleOut/sync' -Method
Post -Body "" | ConvertFrom-Json | Format-List  # Replace <WorkspaceId>
```

```
with the Id of your workspace and <DatasetId> with the Id of your
semantic model
```

The sync status information in the output indicates the read-write semantic model and the read-only replicas are out of sync, which is expected because you just triggered the sync.

6. To verify the sync is complete, run the `syncStatus` command in *step 4* again. You might need to run the command a few times depending on the length of the time that's required to sync the semantic model copies. When the sync is complete, check the values of `syncStartTime` and `syncEndTime` to see how long the sync took.

To learn more, see Datasets - Trigger Query Scale Out Sync In Group in the Power BI REST API reference.

Related content

- Power BI semantic model scale-out
- Configure semantic model scale-out
- Tutorial: Test semantic model scale-out
- Compare semantic model scale-out replicas

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

Compare semantic model scale-out replicas

Article • 11/28/2023

This article provides a few Visual Studio app examples for comparing semantic model properties when Power BI semantic model scale-out is enabled.

The `syncStatus` REST API shows if the read-write semantic model and read-only replicas are in sync. You can also use the Tabular Object Model (TOM) to build a custom application that connects to both semantic models and compares timestamps, metadata, and query results between them.

App 1 - Check the database object properties

Use the code below to build an app that checks the LastUpdate, LastProcessed and LastSchemaUpdate properties of your semantic models. Before the app performs the checks, it needs to call the `Refresh()` method, to get the replica's metadata.

Replace `<WorkspaceUrl>` with your workspace's URL, and `<Semantic modelName>` with your semantic model's name.

TypeScript

```
string workspaceUrl = "<WorkspaceUrl>";  // Replace <WorkspaceUrl> with the
URL of your workspace
string datasetName = "<Semantic modelName>";  // Replace <Semantic
modelName> with the name of your semantic model
using (var workspace_readwrite = new
Microsoft.AnalysisServices.Tabular.Server())
using (var workspace_readonly = new
Microsoft.AnalysisServices.Tabular.Server())
{
    workspace_readwrite.Connect(workspaceUrl + "?readwrite");
    workspace_readonly.Connect(workspaceUrl + "?readonly");
    var datasetRW = workspace_readwrite.Databases.FindByName(semantic
modelName);
    var datasetRO = workspace_readonly.Databases.FindByName(semantic
modelName);

    if (datasetRW == null || datasetRO == null)
    {
        throw new ApplicationException("Database cannot be found!");
    }
    datasetRW.Refresh();
    datasetRO.Refresh();
```

```
    Console.WriteLine($"LastUpdated: {datasetRW.LastUpdate} (readwrite)
{datasetRO.LastUpdate} (readonly)");
    Console.WriteLine($"LastProcessed: {datasetRW.LastProcessed} (readwrite)
{datasetRO.LastProcessed} (readonly)");
    Console.WriteLine($"LastSchemaUpdate: {datasetRW.LastSchemaUpdate}
(readwrite) {datasetRO.LastSchemaUpdate} (readonly)\n");
}
Console.WriteLine("Test completed. Press any key to exit.");
Console.Read();
```

App 2 - Compare the semantic model's metadata

Use the code below to compare the metadata of the primary read-write semantic model with the metadata of a read-only replica. Replace `<WorkspaceUrl>` with your workspace's URL, and `<DatasetName>` with your semantic model's name.

TypeScript

```
string workspaceUrl = "<WorkspaceUrl>";  // Replace <WorkspaceUrl> with the
URL of your workspace
string datasetName = "<DatasetName>";  // Replace <DatasetName> with the
name of your semantic model
using (var workspace_readwrite = new
Microsoft.AnalysisServices.Tabular.Server())
using (var workspace_readonly = new
Microsoft.AnalysisServices.Tabular.Server())
{
    workspace_readwrite.Connect(workspaceUrl + "?readwrite");
    workspace_readonly.Connect(workspaceUrl + "?readonly");
    var datasetRW = workspace_readwrite.Databases.FindByName(datasetName);
    var datasetRO = workspace_readonly.Databases.FindByName(datasetName);

    if (datasetRW == null || datasetRO == null)
    {
        throw new ApplicationException("Database cannot be found!");
    }

    string tmslRW =
Microsoft.AnalysisServices.Tabular.JsonSerializer.SerializeDatabase(datasetR
W);
    string tmslRO =
Microsoft.AnalysisServices.Tabular.JsonSerializer.SerializeDatabase(datasetR
O);

    if (tmslRW != tmslRO)
    {
        Console.WriteLine("The replicas are out of sync.\n");
    }
    else
```

```
    {
        Console.WriteLine("The replicas are in sync.\n");
    }
}
Console.WriteLine("Test completed. Press any key to exit.");
Console.Read();
```

App 3 - Query the semantic model data

Use `ADOMD.NET` to query the data in the replicas. Replace `<WorkspaceUrl>` with your workspace's URL, and `<DatasetName>` with your semantic model's name.

TypeScript

```
string workspaceUrl = "<WorkspaceUrl>";  // Replace WorkspaceUrl with the
URL of your workspace
string datasetName = "<DatasetName>";  // Replace DatasetName with the name
of your semantic model
string daxQuery = "Evaluate SUMMARIZECOLUMNS(RefreshTimeTable[Time])";
using (var connectionRW = new
Microsoft.AnalysisServices.AdomdClient.AdomdConnection())
using (var connectionRO = new
Microsoft.AnalysisServices.AdomdClient.AdomdConnection())
{
    connectionRW.ConnectionString = $"Data Source={workspaceUrl}?
readwrite;Catalog={datasetName}";
    connectionRO.ConnectionString = $"Data Source={workspaceUrl}?
readonly;Catalog={datasetName}";
    connectionRW.Open();
    connectionRO.Open();
    var cmd = new
Microsoft.AnalysisServices.AdomdClient.AdomdCommand(daxQuery);
    string resultRW = string.Empty;
    string resultRO = string.Empty;
    cmd.Connection = connectionRW;
    using (var reader = cmd.ExecuteReader())
    {
        while (reader.Read())
        {
            resultRW = reader.GetString(0);
        }
    }

    cmd.Connection = connectionRO;
    using (var reader = cmd.ExecuteReader())
    {
        while (reader.Read())
        {
            resultRO = reader.GetString(0);
        }
    }
```

```
    if (resultRW != resultRO)
    {
        Console.WriteLine("The replicas are out of sync.\n");
    }
    else
    {
        Console.WriteLine("The replicas are in sync.\n");
    }
}
Console.WriteLine("Test completed. Press any key to exit.");
Console.Read();
```

Next steps

- Power BI semantic model scale-out
- Configure semantic model scale-out
- Tutorial: Test semantic model scale-out
- Synchronize scale-out replicas

Semantic model operations

Article • 11/20/2024

Semantic model operation logs are part of the workspace monitoring logs and are registered in the Eventhouse KQL database, which is part of the Real-Time Intelligence solution. You can use these logs to monitor the usage and performance of your workspace.

Semantic model operation logs

Analysis services engine process events such as the start of a batch or transaction. For example, execute query and process partition. Typically used to monitor the performance, health and usage of Power BI's data engine. Contains information from the entire tenant.

Use semantic model logs to:

- Identify periods of high or unusual Analysis Services engine activity by capacity, workspace, report, or user.
- Analyze query performance and trends, including external DirectQuery operations.
- Analyze semantic model refresh duration, overlaps, and processing steps.
- Analyze custom operations sent using the Premium XMLA endpoint.

This table lists the semantic model logs. For more information on the events and drill-down into the `ExecutionMetrics` event, see Events and schema.

Expand table

ColumnName	ColumnType	Description
ApplicationContext	dynamic	Property bag of unique identifiers providing details about the application executing the request. For example, report ID.
ApplicationName	string	Contains the name of the client application that created the connection to the server. This column is populated with the values passed by the application rather than the displayed name of the program.
CallerIpAddress	string	Called IP address
CapacityId	string	Unique identifier of the capacity hosting the artifact being operated on.

ColumnName	ColumnType	Description
Category	string	Category of the events, like Audit/Security/Request.
CorrelationId	string	The ID for correlated events. Can be used to identify correlated events between multiple tables.
CpuTimeMs	long	Amount of CPU time (in milliseconds) used by the event.
CustomerTenantId	string	Fabric tenant identifier
DatasetMode	string	The mode of the semantic model. Import, DirectQuery, or Composite.
DurationMs	long	Amount of time (in milliseconds) taken by the operation.
EventText	string	Contains verbose information associated with the operation, for example, DAX Query.
ExecutingUser	string	The user running the operation.
Identity	dynamic	Information about user and claims.
ItemId	string	Unique identifier of the resource logging the data.
ItemKind	string	Type of artifact logging the operation, for example, semantic model.
ItemName	string	The name of the Power BI artifact logging this operation.
Level	string	Contains the severity level of the operation being logged. Success, informational, warning, or error.
OperationDetailName	string	More details about the operation
OperationId	string	Unique identifier of the operation or the request. Same as `XmlaRequestId`
OperationName	string	The operation associated with the log record.
ProgressCounter	long	Progress counter
Region	string	Contains the Fabric region
ReplicaId	string	Replica identifier that will let you identify the replica when Query Scale Out (QSO) is

ColumnName	ColumnType	Description
		enabled. Read-write replica always has ReplicaId='AAA' and read-only replicas have ReplicaId starting 'AAB' onwards. For non-QSO enabled semantic models the ReplicaId is always 'AAA'
Status	string	Status of the operation.
StatusCode	int	Status code of the operation. It covers success and failure.
Timestamp	datetime	The timestamp (UTC) of when the log was generated.
User	string	The user associated with the running operation. Used when an end-user identity must be impersonated on the server.
WorkspaceId	string	Unique identifier of the workspace containing the item being operated on.
WorkspaceMonitoringTableName	string	Name of the table the events are available in Fabric Workspace monitoring
WorkspaceName	string	Name of the Fabric workspace containing the item.
XmlaObjectPath	string	Object path. A comma-separated list of parents, starting with the object's parent.
XmlaProperties	string	Properties of the XMLA request
XmlaSessionId	string	Analysis services session identifier

Feedback

Was this page helpful? Yes No

Provide product feedback | Ask the community

PowerShell cmdlets, REST APIs, and .NET Client library for Power BI administration

Article • 03/09/2022

Power BI enables administrators to script common tasks with PowerShell cmdlets. It also exposes REST APIs and provides a .NET client library for developing administrative solutions. This topic shows a list of cmdlets and the corresponding APIs and REST API endpoint. For more information, see:

- PowerShell download and documentation
- REST API documentation
- .NET Client library download

> Cmdlets below should be called with `-Scope Organization` to operate against the tenant for administration.

Cmdlet name	Aliases	API	REST API endpoint	Description
`Get-PowerBIDatasource`	N/A	`Datasets_GetDataSourcesAsAdmin`	/v1.0/myorg/admin/datasets/{datasetkey}/datasources	Gets the data sources for a given dataset.
`Get-PowerBIDataset`	N/A	`Datasets_GetDatasetsAsAdmin`	/v1.0/myorg/admin/datasets	Gets the full list of datasets in a Power BI tenant.
`Get-PowerBIWorkspace`	`Get-PowerBIGroup`	`Groups_GetGroupsAsAdmin`	/v1.0/myorg/admin/groups	Gets the full list of workspaces in a Power BI tenant.
`Add-PowerBIWorkspaceUser`	`Add-PowerBIGroupUser`	`Groups_AddUserAsAdmin`	/v1.0/myorg/admin/groups/{groupId}/users	Adds a user as a member to a given workspace.
`Remove-PowerBIWorkspaceUser`	`Remove-PowerBIGroupUser`	`Groups_DeleteUserAsAdmin`	/v1.0/myorg/admin/groups/{groupId}/users/{user}	Removes a user from the membership list of a given workspace.
`Restore-PowerBIWorkspace`	`Restore-PowerBIGroup`	`Groups_RestoreDeletedGroupAsAdmin`	/v1.0/myorg/admin/groups/{groupId}/restore	Restores a deleted workspace.
`Set-PowerBIWorkspace`	`Set-PowerBIGroup`	`Groups_UpdateGroupAsAdmin`	/v1.0/myorg/admin/groups/{groupId}	Updates the properties of a given workspace.
`Get-PowerBIDataset -WorkspaceId`	N/A	`Groups_GetDatasetsAsAdmin`	/v1.0/myorg/admin/groups/{group_id}/datasets	Gets the datasets within a given workspace.
`Get-PowerBIReport`	N/A	`Reports_GetReportsAsAdmin`	/v1.0/myorg/admin/reports	Gets the full list of reports in a Power BI tenant.

Cmdlet name	Aliases	API	REST API endpoint	Description
`Get-PowerBIDashboard`	N/A	`Dashboards_GetDashboardsAsAdmin`	/v1.0/myorg/admin/dashboards	Gets the full list of dashboards in a Power BI tenant.
`Get-PowerBIDashboard -WorkspaceId`	N/A	`Groups_GetDashboardsAsAdmin`	/v1.0/myorg/admin/groups/{group_id}/dashboards	Gets the dashboards within a given workspace.
`Get-PowerBITile`	`Get-PowerBIDashboardTile`	`Dashboards_GetTilesAsAdmin`	/v1.0/myorg/admin/dashboards/{dashboard_id}/tiles	Gets the tiles of a given dashboard.
`Get-PowerBIReport`	N/A	`Groups_GetReportsAsAdmin`	/v1.0/myorg/admin/groups/{group_id}/reports	Gets the reports within a given workspace.
`Get-PowerBIImport`	N/A	`Imports_GetImportsAsAdmin`	/v1.0/myorg/admin/imports	Gets the full list of imports in a Power BI tenant.
`Connect-PowerBIServiceAccount`	`Login-PowerBI` & `Login-PowerBIServiceAccount`	N/A	N/A	Login to Power BI and start a session.
`Disconnect-PowerBIServiceAccount`	`Logout-PowerBI` & `Logout-PowerBIServiceAccount`	N/A	N/A	Logout of Power BI and close the existing session.
`Invoke-PowerBIRestMethod`	N/A	N/A	N/A	Send arbitrary REST API calls to Power BI.
`Get-PowerBIAccessToken`	N/A	N/A	N/A	Obtain the Power BI access token in a session.
`Resolve-PowerBIError`	N/A	N/A	N/A	Get detailed error information for unsuccessful cmdlet calls.

Microsoft Power BI Cmdlets for Windows PowerShell and PowerShell Core

Article • 09/15/2021

Welcome to the PowerShell reference for Microsoft Power BI. Here you will find resources for PowerShell modules targeting Power BI.

PowerShell modules

Below is a table of the Power BI PowerShell modules covered in this reference.

Expand table

Description	Module Name	PowerShell Gallery link
Rollup module for Power BI Cmdlets	MicrosoftPowerBIMgmt	MicrosoftPowerBIMgmt v1.2.1111
Admin module for Power BI Cmdlets	MicrosoftPowerBIMgmt.Admin	MicrosoftPowerBIMgmt.Admin v1.2.1111
Capacities module for Power BI Cmdlets	MicrosoftPowerBIMgmt.Capacities	MicrosoftPowerBIMgmt.Capacities v1.2.1111
Data module for Power BI Cmdlets	MicrosoftPowerBIMgmt.Data	MicrosoftPowerBIMgmt.Data v1.2.1111
Profile module for Power BI Cmdlets	MicrosoftPowerBIMgmt.Profile	MicrosoftPowerBIMgmt.Profile v1.2.1111
Reports module for Power BI	MicrosoftPowerBIMgmt.Reports	MicrosoftPowerBIMgmt.Reports v1.2.1111
Workspaces module for Power BI	MicrosoftPowerBIMgmt.Workspaces	MicrosoftPowerBIMgmt.Workspaces v1.2.1111

Supported environments and PowerShell versions

- Windows PowerShell v3.0 and up with .NET 4.7.1 or above.
- PowerShell Core (v6) and up on any OS platform supported by PowerShell Core.

Installation

The cmdlets are available on PowerShell Gallery and can be installed in an elevated PowerShell session:

```PowerShell
Install-Module -Name MicrosoftPowerBIMgmt
```

Optionally you could install individual modules (based on your needs) instead of the rollup module, for example if you only wanted the Workspaces module:

```PowerShell
Install-Module -Name MicrosoftPowerBIMgmt.Workspaces
```

If you have an earlier version, you can update to the latest version by running:

```PowerShell
Update-Module -Name MicrosoftPowerBIMgmt
```

Uninstall

If you want to uninstall all the Power BI PowerShell cmdlets, run the following in an elevated PowerShell session:

```PowerShell
Get-Module MicrosoftPowerBIMgmt* -ListAvailable | Uninstall-Module -Force
```

Usage

Two scopes are supported by cmdlets that interact with Power BI entities:

- Individual is used to access entities that belong to the current user.
- Organization is used to access entities across the entire company. Only Power BI tenant admins are allowed to use.

If the -Scope parameter doesn't exist on the cmdlet, the entity doesn't support an Administrative API.

Log in to Power BI

```PowerShell
Connect-PowerBIServiceAccount   # or use aliases: Login-PowerBIServiceAccount, Login-PowerBI
```

Get workspaces

Get workspaces for the user. By default (i.e. without `-First` parameter) it shows the first 100 workspaces assigned to the user:

```PowerShell
Get-PowerBIWorkspace
```

Use the `-All` parameter to show all workspaces assigned to the user:

```PowerShell
Get-PowerBIWorkspace -All
```

If you are a tenant administrator, you can view all workspaces in your tenant by adding `-Scope Organization`:

```PowerShell
Get-PowerBIWorkspace -Scope Organization -All
```

Update a workspace

Update the name or description of a user's workspace:

```PowerShell
Set-PowerBIWorkspace -Scope Organization -Id "3244f1c1-01cf-457f-9383-6035e4950fdc" -Name "Test Name" -Description "Test Description"
```

Add a new user to a workspace

Add a user to a given workspace:

PowerShell

```
Add-PowerBIWorkspaceUser -Scope Organization -Id 3244f1c1-01cf-457f-9383-6035e4950fdc -UserEmailAddress john@contoso.com -AccessRight Admin
```

Remove a user from a given workspace

Remove user's permissions from a given workspace:

PowerShell

```
Remove-PowerBIWorkspaceUser -Scope Organization -Id 3244f1c1-01cf-457f-9383-6035e4950fdc -UserEmailAddress john@contoso.com
```

Get workspace migration status

Get Power BI workspace migration status:

PowerShell

```
Get-PowerBIWorkspaceMigrationStatus -Id 038f9a64-1fcd-42f2-957a-13a63b3d3235
```

Restore a workspace

To view deleted workspaces as a tenant administrator:

PowerShell

```
Get-PowerBIWorkspace -Scope Organization -Deleted -All
```

Restore a deleted workspace:

PowerShell

```
Restore-PowerBIWorkspace -Id "3244f1c1-01cf-457f-9383-6035e4950fdc" -RestoredName "TestWorkspace" -AdminEmailAddress "john@contoso.com"
```

Recover an orphaned workspace

A workspace becomes orphaned when it has no assigned administrators. If you are a tenant administrator, run the following to view all orphaned workspaces:

```PowerShell
Get-PowerBIWorkspace -Scope Organization -Orphaned -All
```

To correct this issue, use:

```PowerShell
Add-PowerBIWorkspaceUser -Scope Organization -Id f2a0fae5-1c37-4ee6-97da-c9d31851fe17 -UserPrincipalName 'john@contoso.com' -AccessRight Admin
```

Get reports

Get all reports for the user:

```PowerShell
Get-PowerBIReport
```

If you are a tenant administrator, you can view all reports in your tenant by using assigning `-Scope Organization`:

```PowerShell
Get-PowerBIReport -Scope Organization
```

Get dashboards

Get dashboards for the user:

```PowerShell
Get-PowerBIDashboard
```

If you are a tenant administrator, you can view all dashboards in your tenant by adding `-Scope Organization`:

```PowerShell
Get-PowerBIDashboard -Scope Organization
```

Get tiles

Get tiles within a dashboard:

PowerShell

```
Get-PowerBITile -DashboardId 9a58d5e5-61bc-447c-86c4-e221128b1c99
```

Get imports

Get Power BI imports:

PowerShell

```
Get-PowerBIImport
```

Create a report

Create a report in Power BI by uploading a *.pbix file:

PowerShell

```
New-PowerBIReport -Path .\newReport.pbix -Name 'New Report'
```

By default, the report is placed in the user's My Workspace. To place in a different workspace, use the `-WorkspaceId` or `-Workspace` parameters:

PowerShell

```
New-PowerBIReport -Path .\newReport.pbix -Name 'New Report' -WorkspaceId
f95755a1-950c-46bd-a912-5aab4012a06d
```

Export a report

Export a Power BI report to *.pbix file:

PowerShell

```
Export-PowerBIReport -Id b48c088c-6f4e-4b7a-b015-d844ab534b2a -OutFile
.\exportedReport.pbix
```

If the workspace exists outside the My Workspace, export with the `WorkspaceId` or `-Workspace` parameter:

```
PowerShell
Export-PowerBIReport -Id b48c088c-6f4e-4b7a-b015-d844ab534b2a -OutFile
.\exportedReport.pbix -WorkspaceId 3bdd9735-0ab5-4f21-bd5d-87e7f1d7fb84
```

Get datasets

Get Power BI datasets:

```
PowerShell
Get-PowerBIDataset
```

Update dataset storage mode

Set Power BI dataset to use Premium Files for storage mode:

```
PowerShell
Set-PowerBIDataset -Id 038f9a64-1fcd-42f2-957a-13a63b3d3235 -
TargetStorageMode PremiumFiles
```

Get datasources

Get Power BI datasources for a dataset:

```
PowerShell
Get-PowerBIDatasource -DatasetId 65d7d7e5-8af0-4e94-b20b-50a882ae15e1
```

Get tables

Get Power BI tables contained within a dataset:

```
PowerShell
Get-PowerBITable -DatasetId 65d7d7e5-8af0-4e94-b20b-50a882ae15e1
```

Call the Power BI Rest API

For Power BI API that lacks corresponding cmdlets, you can reuse the authenticated session from `Connect-PowerBIServiceAccount` to make custom REST requests:

PowerShell

```
Invoke-PowerBIRestMethod -Url 'reports/4eb4c303-d5ac-4a2d-bf1e-39b35075d983/Clone' -Method Post -Body ([pscustomobject]@{name='Cloned report'; targetModelId='adf823b5-a0de-4b9f-bcce-b17d774d2961'; targetWorkspaceId='45ee15a7-0e8e-45b0-8111-ea304ada8d7d'} | ConvertTo-Json -Depth 2 -Compress)
```

If you want to use the authenticated session outside of PowerShell, get the access token by using:

PowerShell

```
Get-PowerBIAccessToken -AsString
```

Troubleshooting errors

To get more information about an error returned back from the cmdlets, use:

PowerShell

```
Resolve-PowerBIError -Last
```

This information can be useful for opening support tickets for Power BI.

Issues and feedback

If you find any bugs or would like to see certain functionality implemented for the PowerShell Cmdlets for Power BI, please file an issue.

If your issue is broader than just the PowerShell cmdlets, please submit your feedback to the Power BI Community or the official Power BI Support site.

Feedback

Was this page helpful?

Yes No